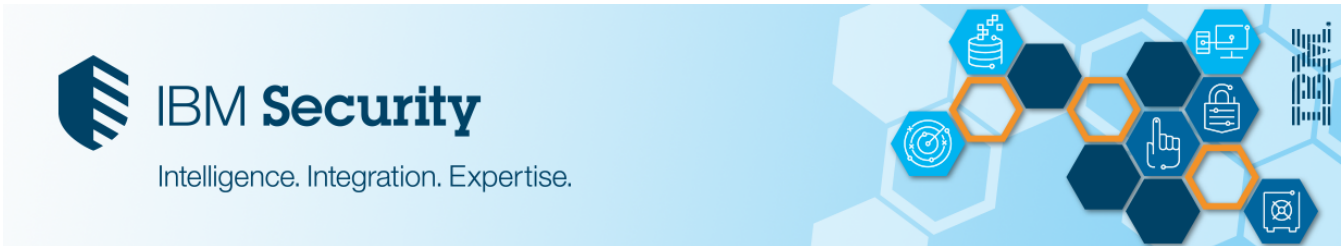


IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

IGI Attribute Permissions Lab (Lab03)

5.2.x

David Edwards

Version 0.2
July 2017

Document Purpose

This document provides the instructions for running the IGI Attribute Permissions lab.

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
23 Feb 2017	0.1	David Edwards	Initial version
31 Jul 2017	0.2	David Edwards	Updated to IGI 5.2.3 with Trg Image v4

Table of Contents

1 Introduction to the Lab

Accounts and account attributes are critical to identity management, often entitlements involve some account group membership. Some systems, like RACF and ACF2 on the mainframe, also use other account attributes to assign rights to the user. For example, an account may be flagged with OPERATIONS or AUDITOR rights.

IGI 5.2.2 added the ability to flag an attribute as a permission and then treat that permission as another permission for identity governance; review in certification campaigns, map to business activities and SoD rules, and request and review them as access rights.

This lab will explore this new attribute-permission capability introduced with IGI 5.2.2; identifying the permission attributes, managing identities with them and reviewing them in a certification campaign.

The parts of the lab are:

1. Define permission attributes
2. Manage permission attributes on users
3. Review attribute-permissions in a certification campaign

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 applications, accounts, targets, attributes and permissions
- Ability to create certification datasets and campaigns, run campaigns and review access
- Basic unix/linux shell operations (login/ssh, cd, running commands)

This knowledge can be gained via the introductory (Foundation) training.

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 this lab.

3 Lab Instructions

3.1 Part 1 – Define Permission Attributes

This part of the lab will define some account attributes as permissions, which we will use in later parts of the lab.

> The system we will use is LDAP and the schema (inetOrgPerson) doesn't have any attributes that are used for access rights, so we will re-purpose some attributes. We are just doing this to show how the mechanisms work. For live deployments you would be working with attributes that are actually permissions.

The steps we will follow:

- Import and configure account attributes
- Import and configure attribute permissions
- Publish the permissions

To support this section, you should review the section "Accounts" in the IGI Knowledge Center (online documentation) at https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.3/com.ibm.igi.doc/CrossIdeas_Topics/AGC/GestioneCfgPwd.html

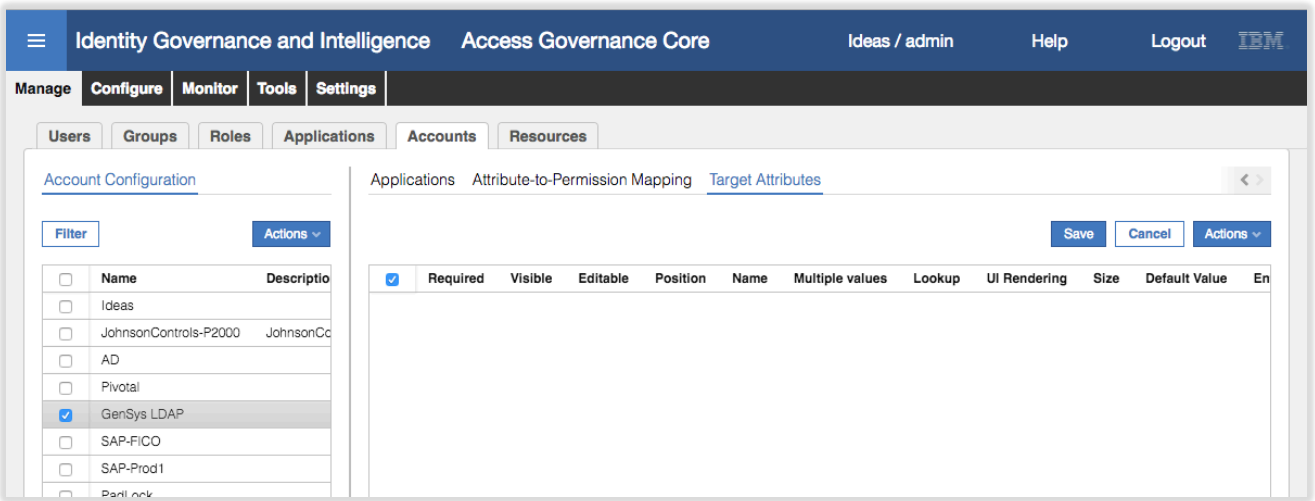
3.1.1 Import and Configure Account Attributes

This section will identify some account attributes that can be viewed in the IGI UI.

> This is not technically required to define attribute-permissions, but it will allow us to see the values/set and changed in the IGI Administration Console.

The steps are:

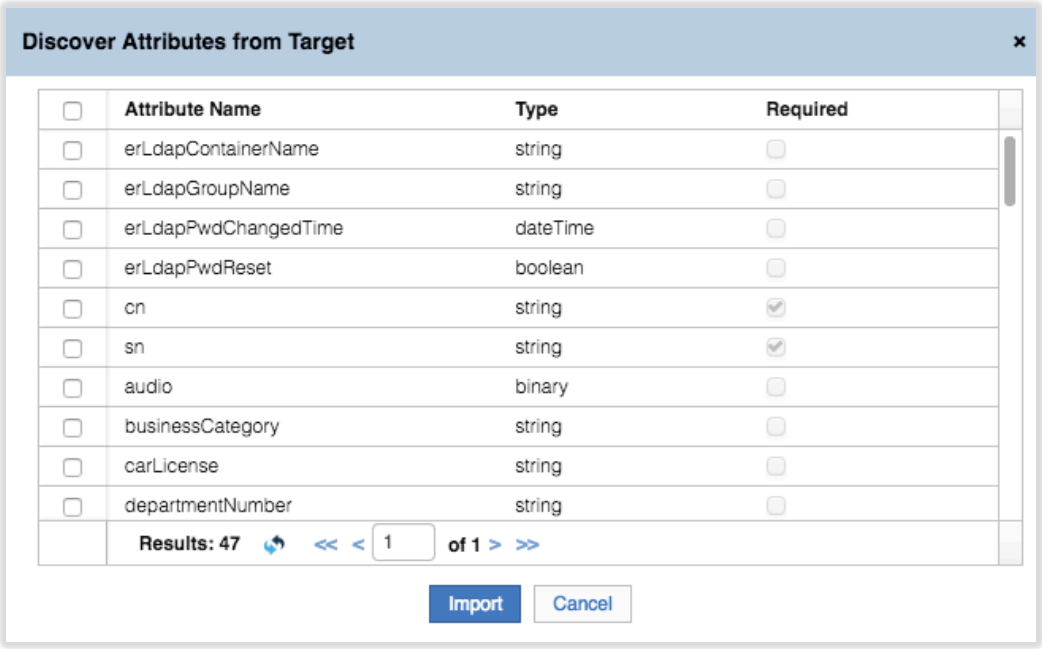
☐ Open the **IGI Administrative Console** (`admin`/`admin`)
☐ Open **Access Governance Core**
☐ Go to **Manage > Accounts**
☐ Select the `GenSys LDAP` account and select the **Target Attributes** tab (you may need to use the right arrow icon to see the tab)



No attributes are currently exposed for this account.

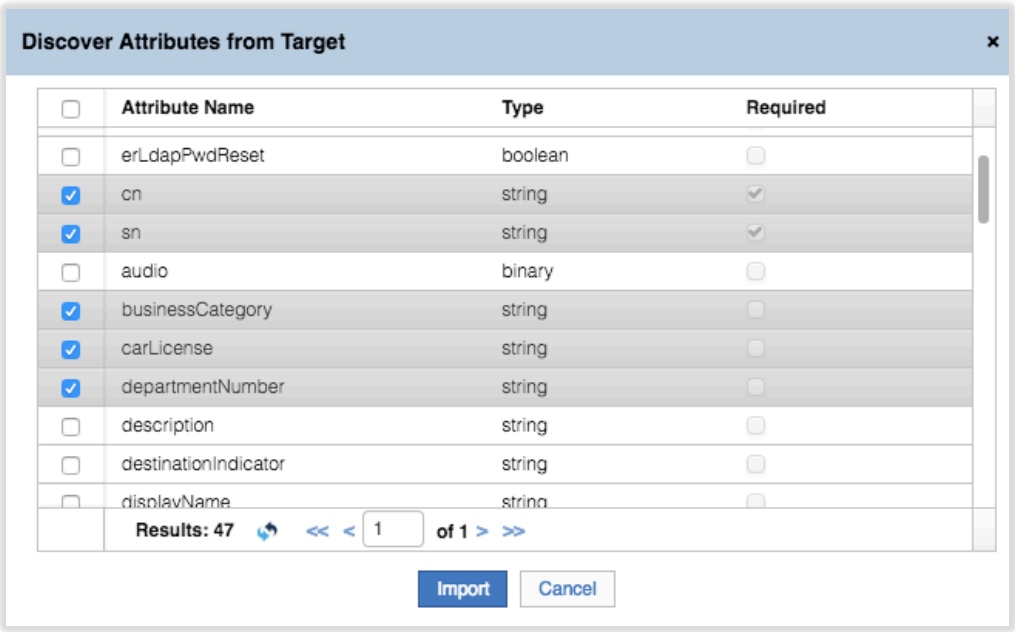
☐ Select **Actions > Discover Account Attributes from Target**

There may be a delay, but a dialog will display showing all the attributes available for this account type.



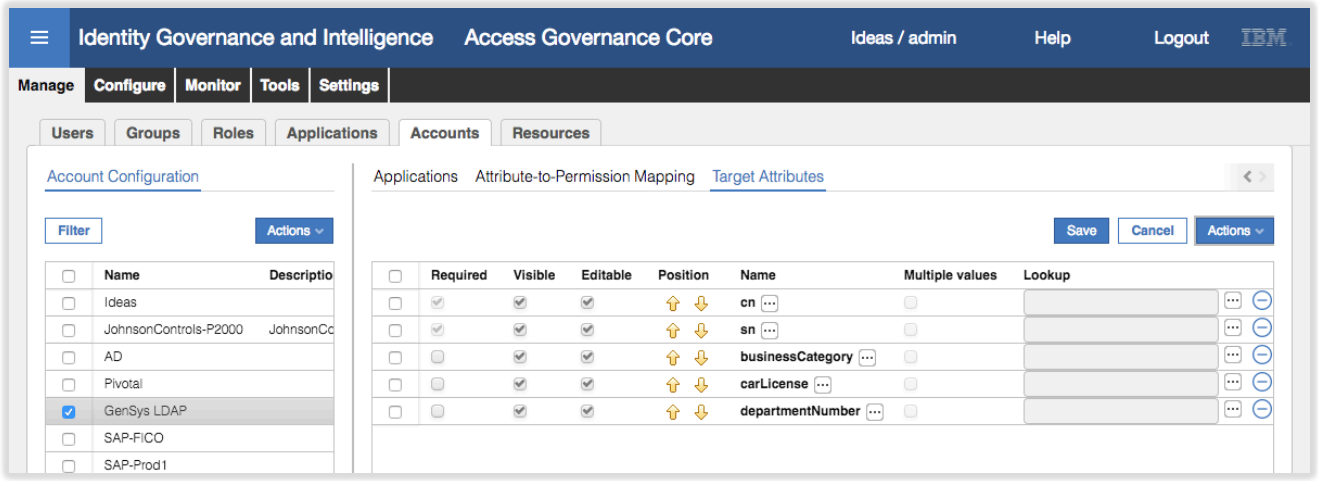
You should see that both cn (Common Name) and sn (Surname) are flagged as Required. This means they are mandatory account attributes (the LDAP inetOrgPerson object requires cn and sn).

☐ Select the following attributes: `cn, sn, businessCategory, carLicense, departmentNumber`



☐ Click **Import**

☐ On the **Accounts > Target Attributes** page check that all five attributes are Visible



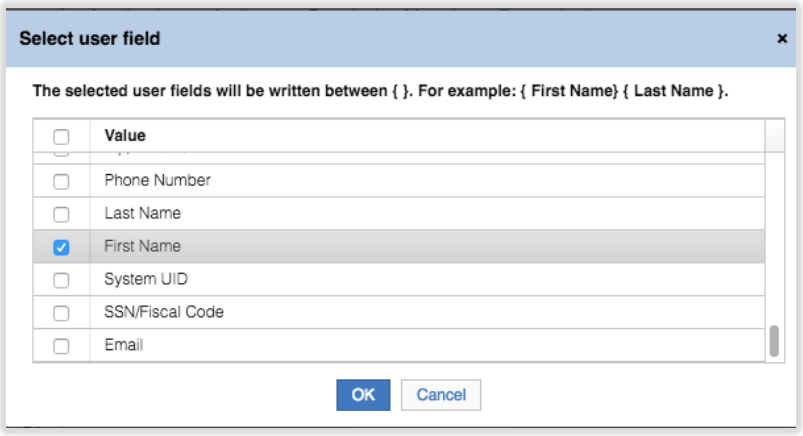
☐ Select the ellipses (…) button beside each of the fivw attributes and set the English label as follows:

cn	Common Name
sn	Surname
businessCategory	Auditor Flag
carLicense	Operations Flag
departmentNumber	Default Access

The new labels do not appear in the **Target Attributes** view, you still only see the attribute name. To see the labels you need to view an account, which we will do momentarily.

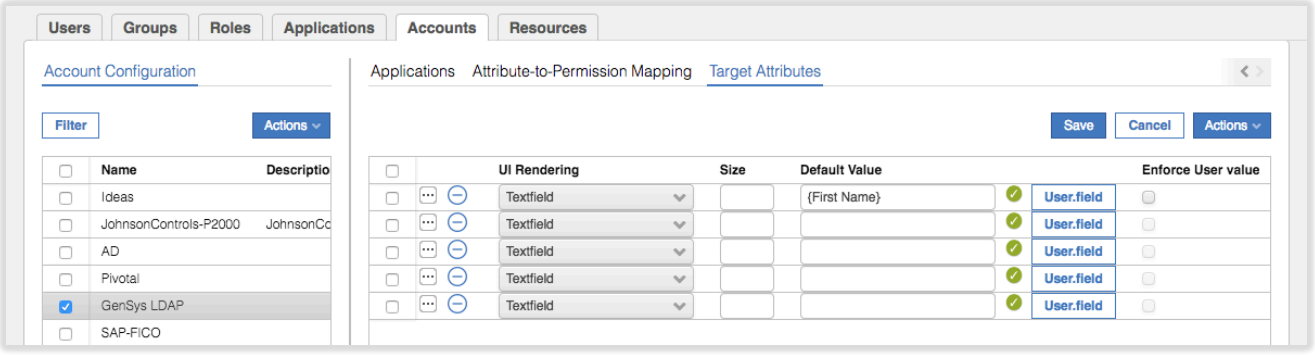
☐ Leave the **UI Rendering** for all four as Textfield
☐ Scroll across to see the Default Value column
☐ Click the User.field button in the “cn” row (the first row)

This button presents the Select user field dialog. This dialog presents the IGI User object fields (attributes) that we can use to define the default account (target) attribute values.



☐ Select the `First Name` value and click **OK**

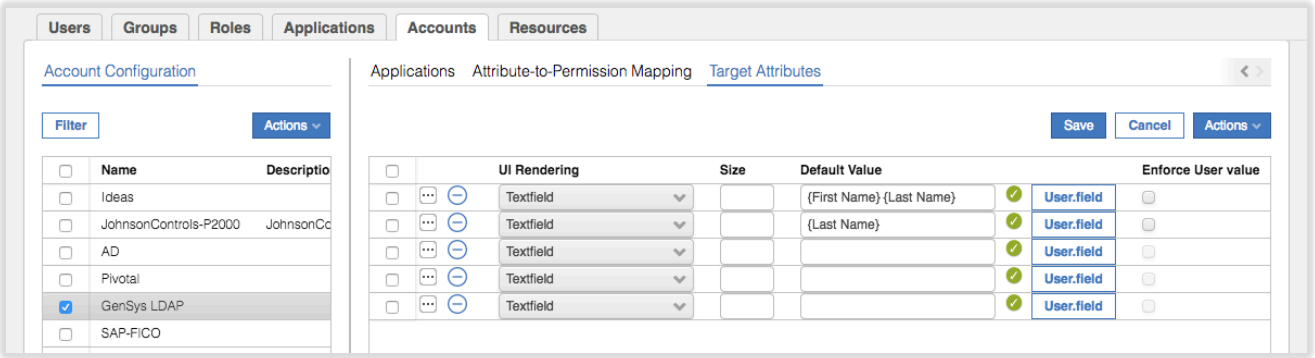
This inserts the text {First Name} into the Default Value field.



☐ Go to the **Default Value** field and type a `space` then `{Last Name}` after `{First Name}` (so the default value will be first+ +last)

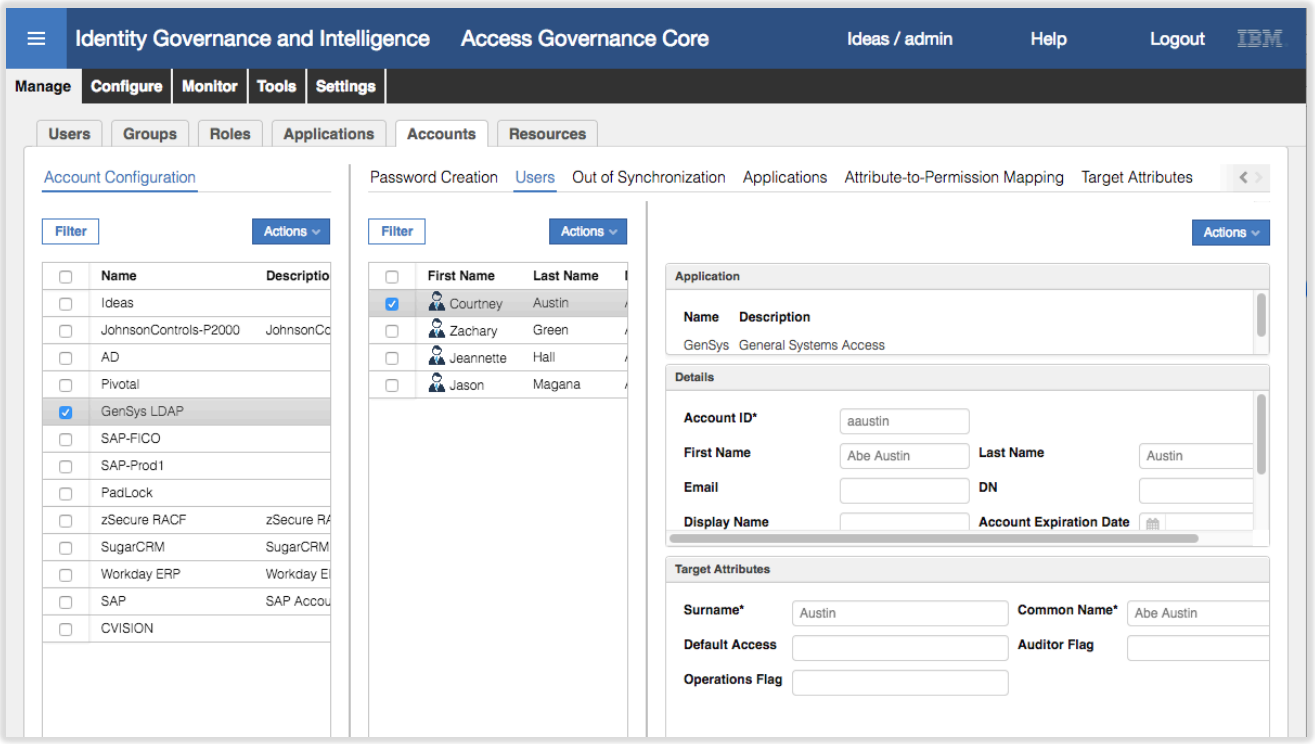
☐ Use the **User.field** button on the second line (sn attribute) and select Last Name

The Default Values should look like this.



☐ Click **Save**

☐ Still within the **Accounts** tab, click on the **Users** tab and select the user `Courtney Austin`



Ignore the fact that Courtney Austin has an LDAP account of Abe Austin (due to the data in the demo system).

You can see the five attributes (and any values this account has) in the bottom right of the view. You can also see that they have the English label we set earlier, not the attribute name.

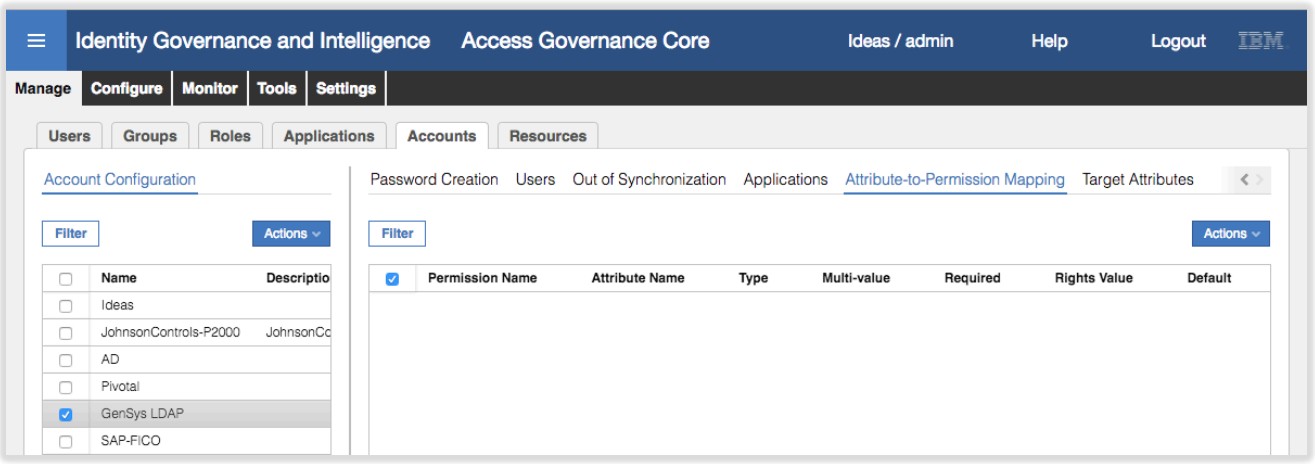
This concludes setting up the attributes, we will now go make these attributes into permissions.

3.1.2 Import and Configure Attribute Permissions

This section will define three attribute permissions; repurposing the businessCategory, carLicense and departmentNumber attributes.

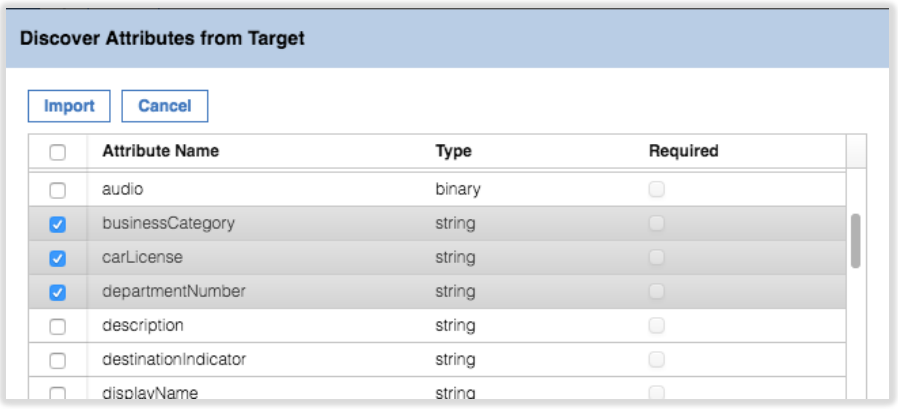
The steps are:

- ☐ If not there already, open the **IGI Administrative Console** (`admin`/`admin`) and **Access Governance Core**, go to **Manage > Accounts**
- ☐ Select the `GenSys LDAP` account and select the **Attribute-to-Permission Mapping** tab (you may need to use the right)

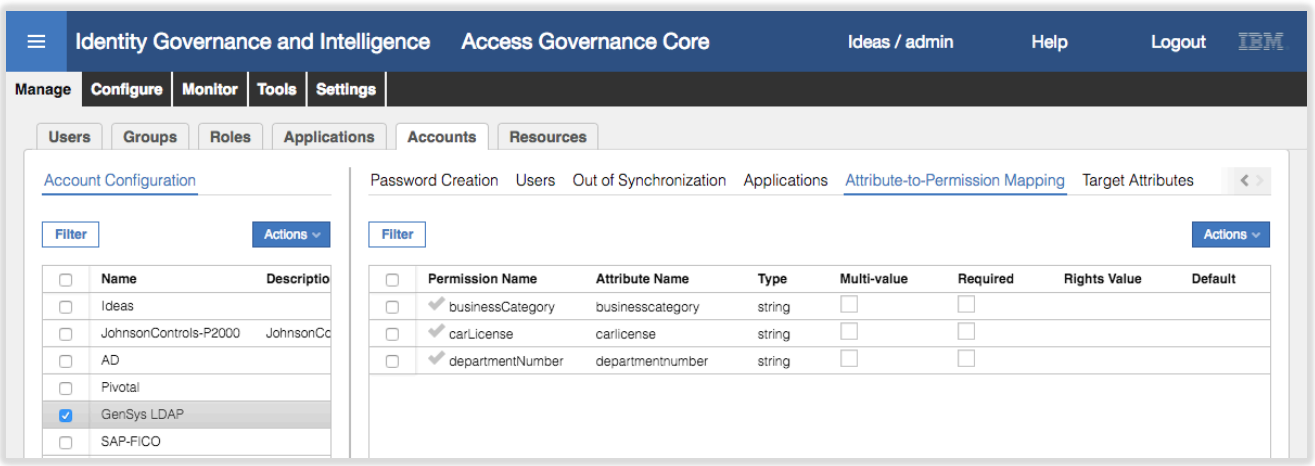


There are no attribute permissions defined.

☐ Select **Actions > Discover Account attributes from Target**
☐ Select the three attributes; `businessCategory`, `carLicense`, and `departmentNumber`



☐ Click **Import**
☐ Click **OK** on the Information dialog

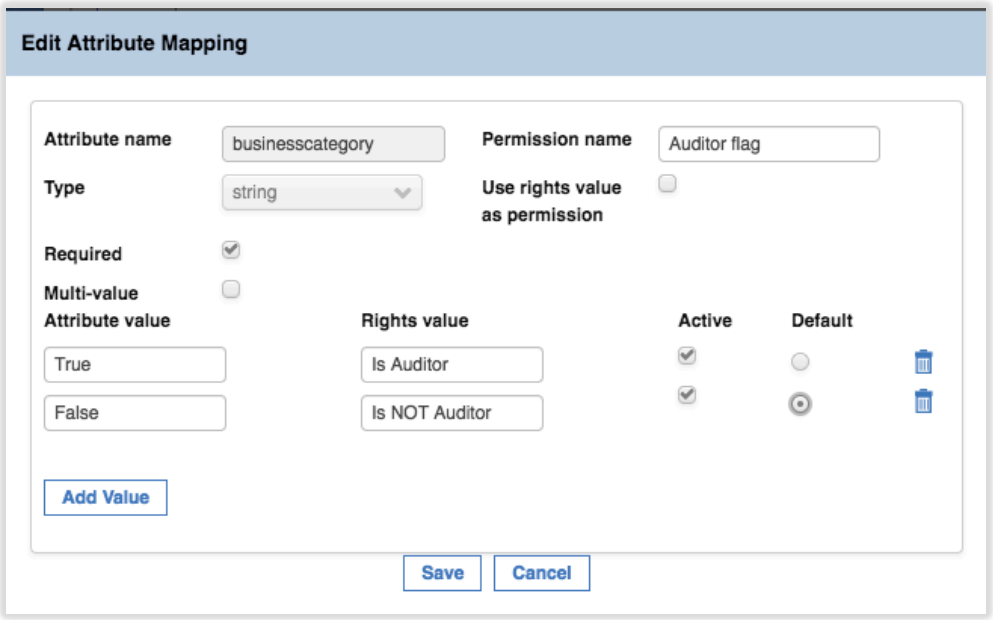


The Attribute-to-Permission Mapping tab now shows the three new attributes. Note the following:

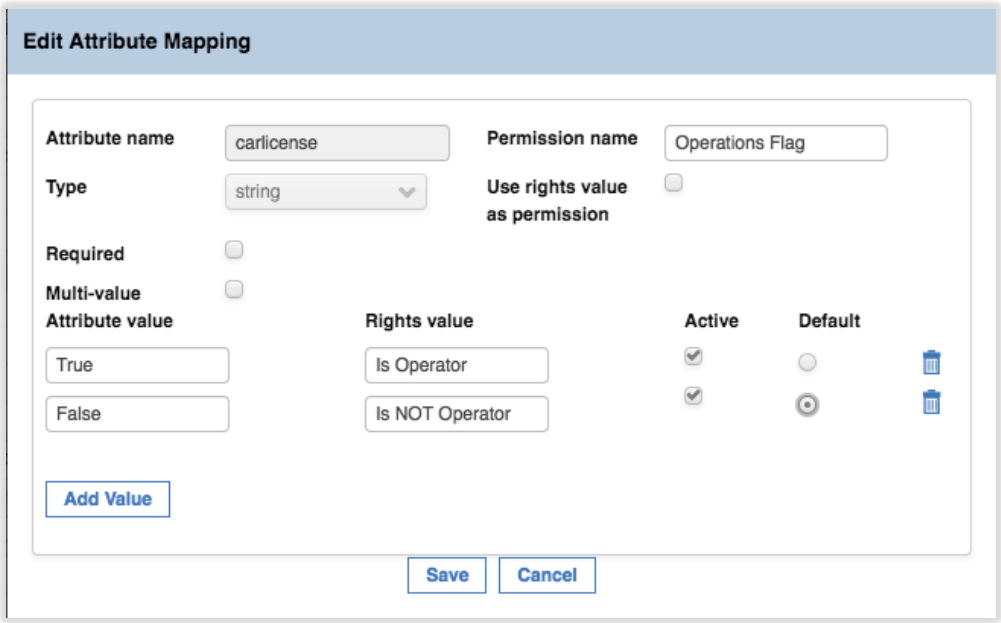
- There is a greyed-out tick beside each – this indicates the permission has not been enabled
- The Permission Name is the Attribute Name (we will change this)
- Each has a Type of string – this has come from the attribute type on the target
- Each could be flagged as multi-valued – note that the Adapter must be able to handle/process a multi-valued attribute (the LDAP adapter we were using won't do it for the three attributes we are using)
- Each has the option of Required or not
- Each can (will) have Rights Values – this list will be populated as we define each permission
- Each can have a Default value.

We will work through each Permission and setup the appropriate values.

☐ Select the `businessCategory` permission and select **Actions > Edit**
☐ On the Edit Attribute Mapping dialog enter the following values:
  - Permission name = "Auditor flag"
  - Required = selected (this is important for later)
  - Attribute value/Rights value (click Add Value) = True / Is Auditor
  - Attribute value/Rights value (click Add Value) = False / In NOT Auditor
  - Select Default for the False attribute value

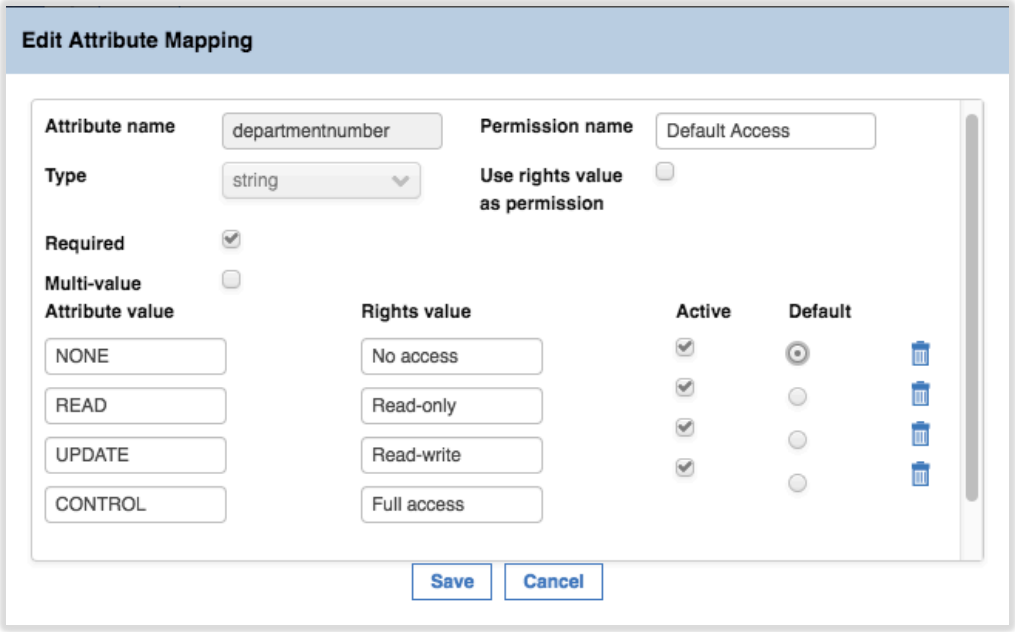


- ☐ Click **Save** and click **OK** on the Information dialog
- ☐ Select the `carLicense` permission and select **Actions > Edit**
- ☐ On the Edit Attribute Mapping dialog enter the following values:
  - Permission name = “Operations Flag”
  - Required = NOT selected (this is important for later)
  - Attribute value/Rights value (click Add Value) = True / Is Operator
  - Attribute value/Rights value (click Add Value) = False / In NOT Operator
  - Select Default for the False attribute value



- ☐ Click **Save** and click **OK** on the Information dialog
- ☐ Select the `departmentNumber` permission and select **Actions > Edit**
- ☐ On the Edit Attribute Mapping dialog enter the following values:
  - Permission name = “Default Access”
  - Required = selected (this is important for later)
  - Add four Attribute values; NONE / No access, READ / Read-only, UPDATE / Read-write, CONTROL / Full access

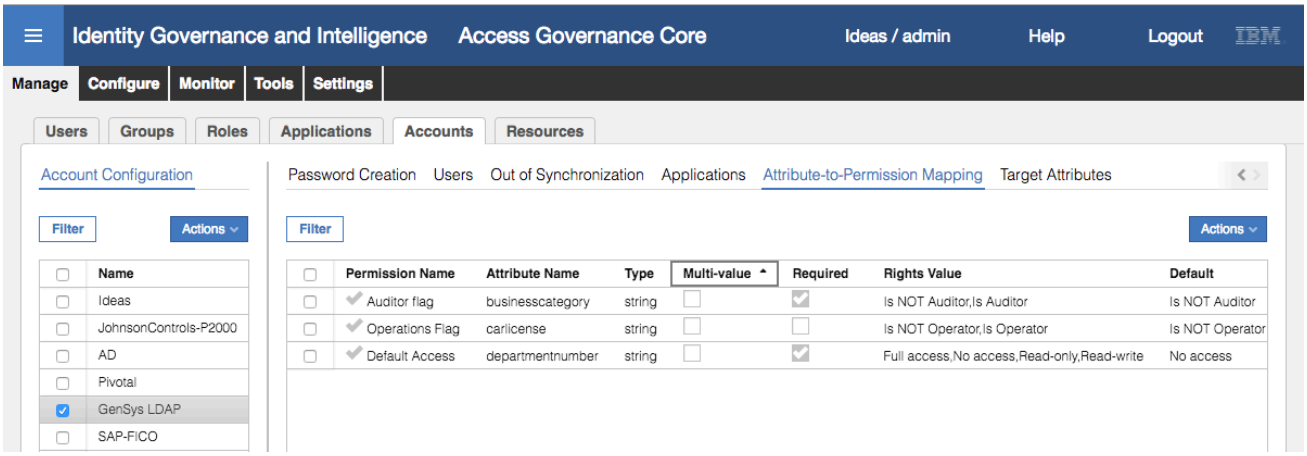
- Select Default for the NONE / No access attribute value



☐ Click **Save** and click **OK** on the Information dialog

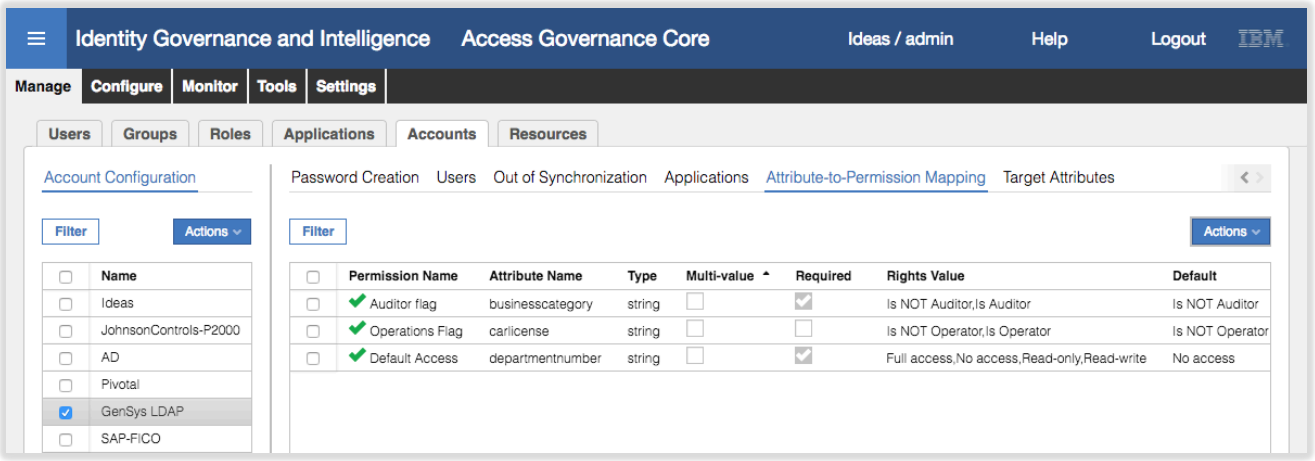
The Attribute-to-Permission Mapping view will show the three attributes updated with:

- A different permission name,
- Whether the permission is required or not,
- The rights values, and
- The default value.



The last thing to do is Enable the permissions so they will show up in the Roles view.

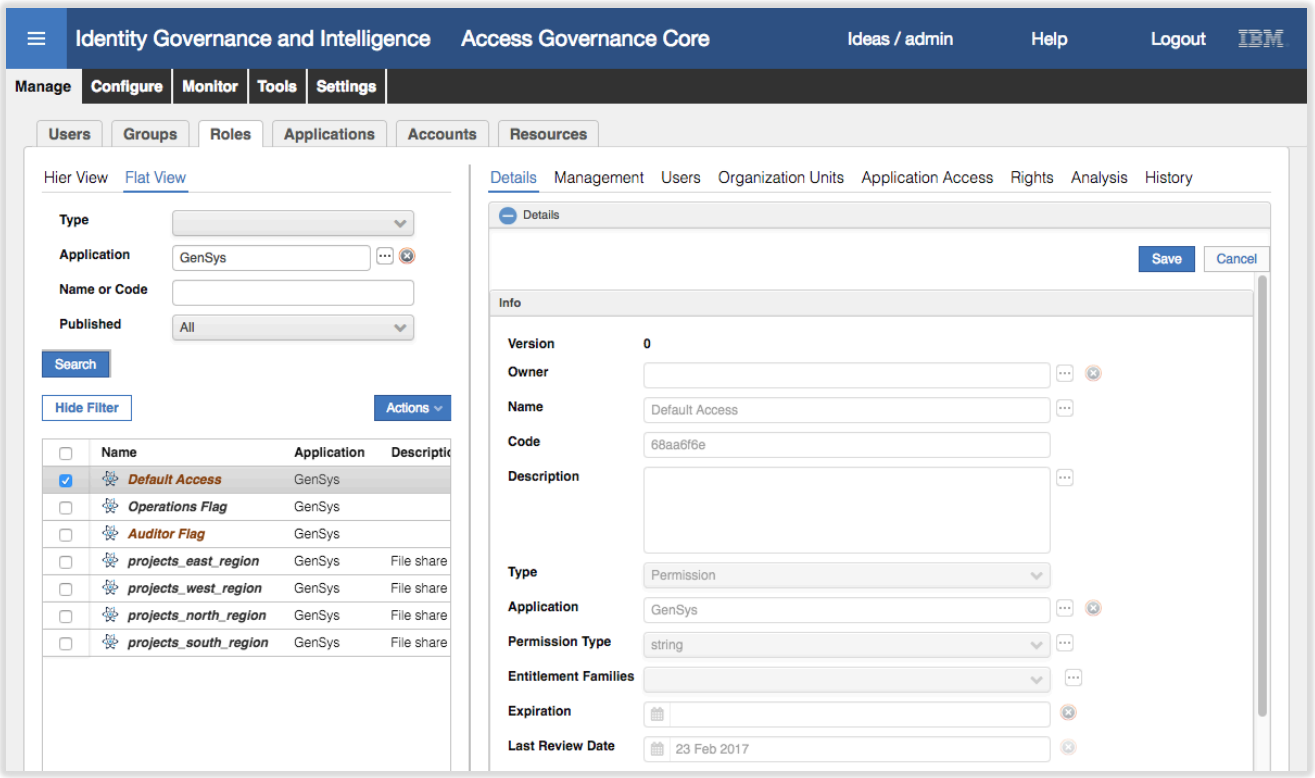
☐ Select all three Permissions and select **Actions > Enable**
☐ Click **OK** on the Information dialog



All three now have a green tick indicating they are enabled

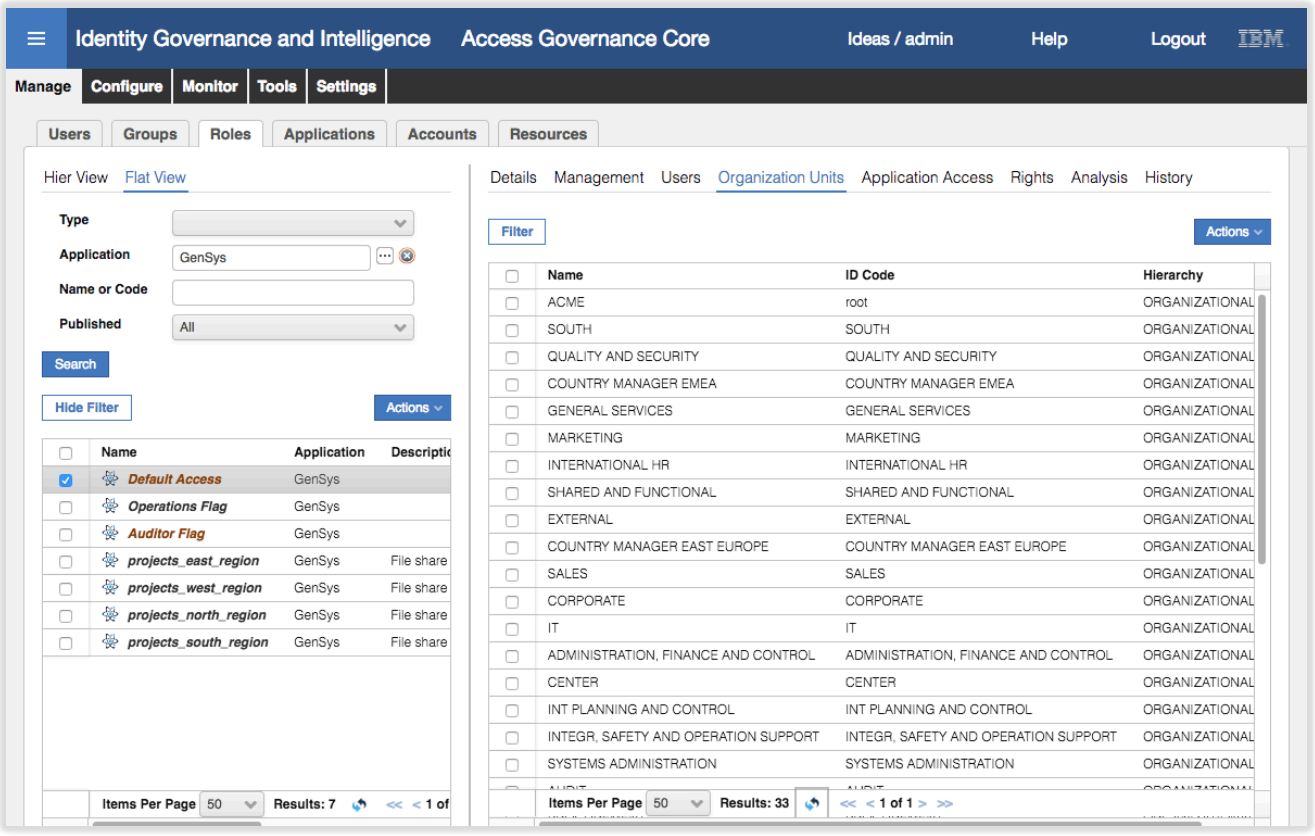
Next, we need to check the new Permissions and set the visibility.

- ☐ Go to **Manage > Roles** within **Access Governance Core**
- ☐ Filter to see permissions from the GenSys application



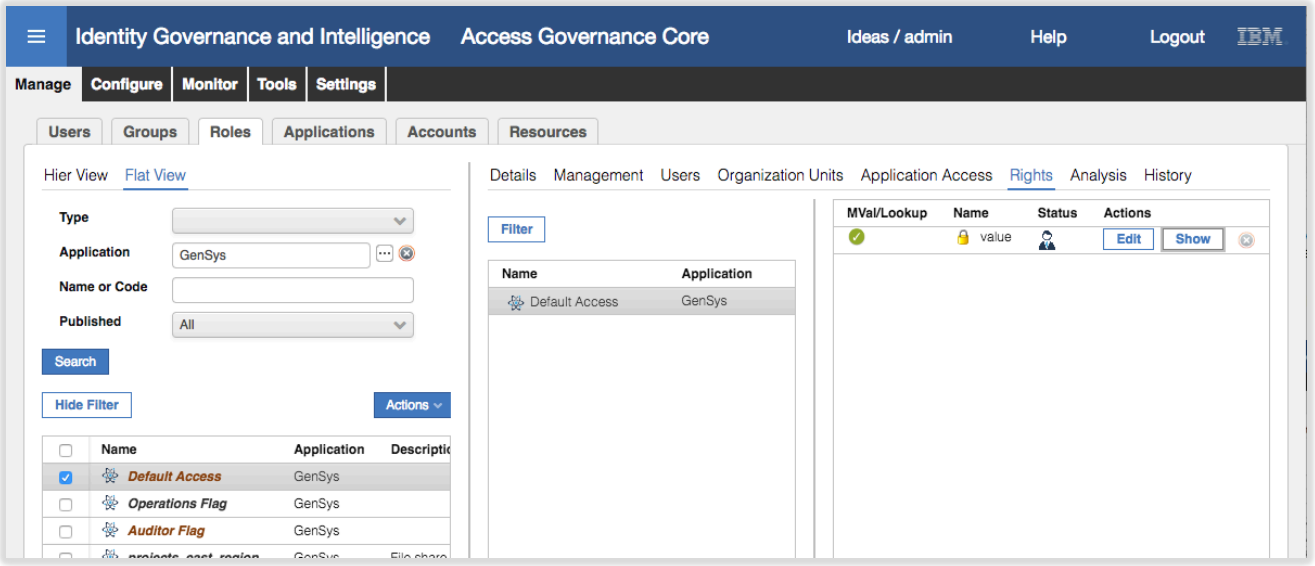
Notice that all three new Permissions are bold+italic indicating that they are published. The two that we set with Required are shown in brown (Default Access and Auditor Flag). We need to set the visibility.

- ☐ With `Default Access` selected, go to the **Organization Units** tab
- ☐ As you would for any Role/Permission, add the Org Unit of `ACME` (with default = no, enabled = yes and hierarchy selected) so it's visible to all users in the entire organization.
- ☐ Click **OK** on the Information dialog



☐ Repeat the process to set visibility to the `ACME` Org Unit (with hierarchy) for both `Operations Flag` and `Auditor Flag` permissions

☐ With the `Default Access` permission selected, go to the Rights tab and select the `Default Access` permission



This panel allows further policy to be applied to rights values for this permission. More details can be found in the IGI Knowledge Center: https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.3/com.ibm.igi.doc/CrossIdeas_Topics/AGC/GestioneRuoli_Rights.html

We will not alter any of the values here.

These permissions are now ready to use in Access Request Management.

> One point on the attribute permission rights; they are not common rights that can be applied to any permission (as you see in AGC -> Configure -> Rights Lookup).

This concludes the import and configuration of the attribute rights. The next two parts of the lab will add them as access for a user and run a certification campaign.

3.2 Part 2 – Request Attribute-Permissions with Access Request Mgmt

This part of the lab will request these new permissions and see what they look like in IGI. We will perform the initial steps for user Courtney Austin, who has a manager of Shirley Chang, then check the changes as an administrator.

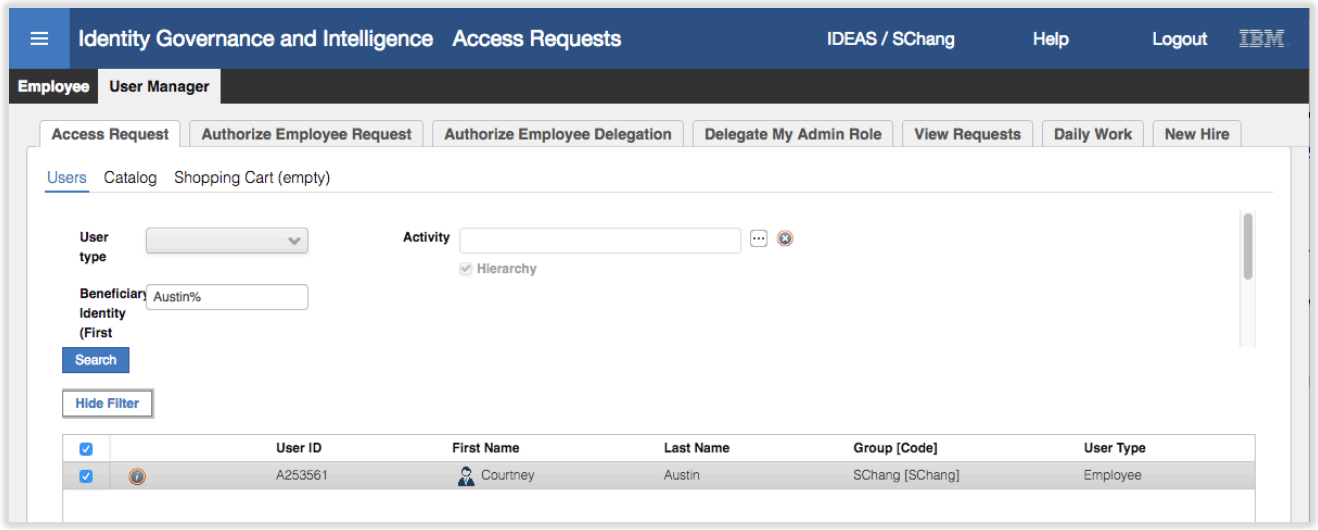
3.2.1 Requesting Attribute-Permissions

Steps:

☐ Log into the **IGI Service Center** (`SChang` / `Passw0rd`)

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

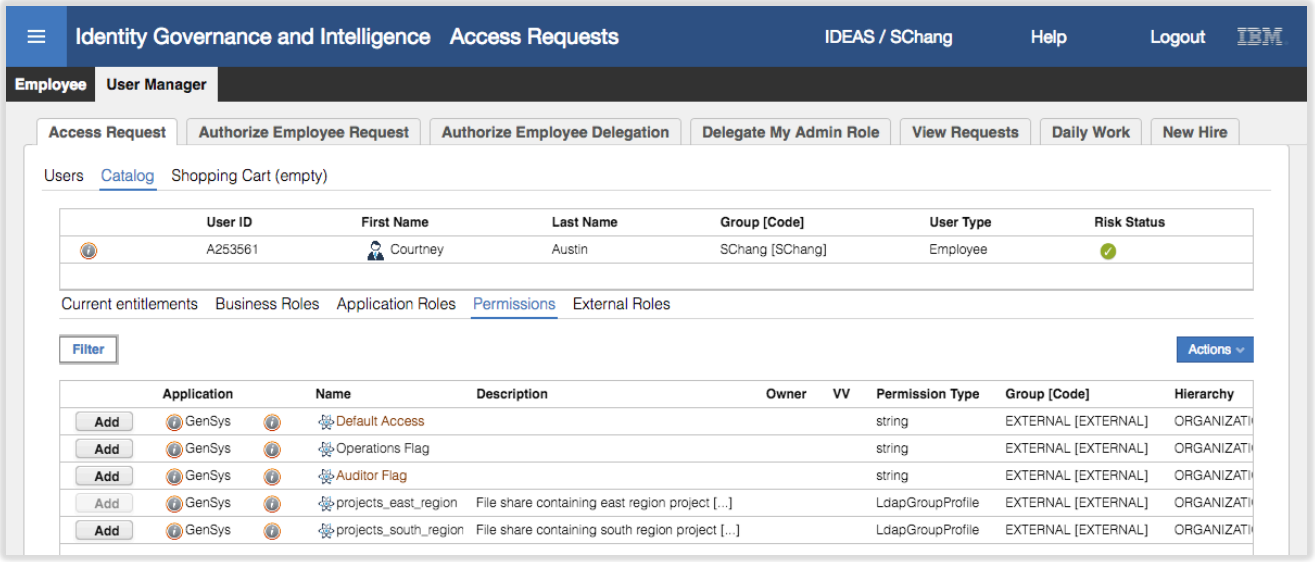
☐ Find and select `Courtney Austin`



☐ Click **Next**

Currently Courtney only has a single entitlement; the projects_east_region group in GenSys. We need to add the three new permissions.

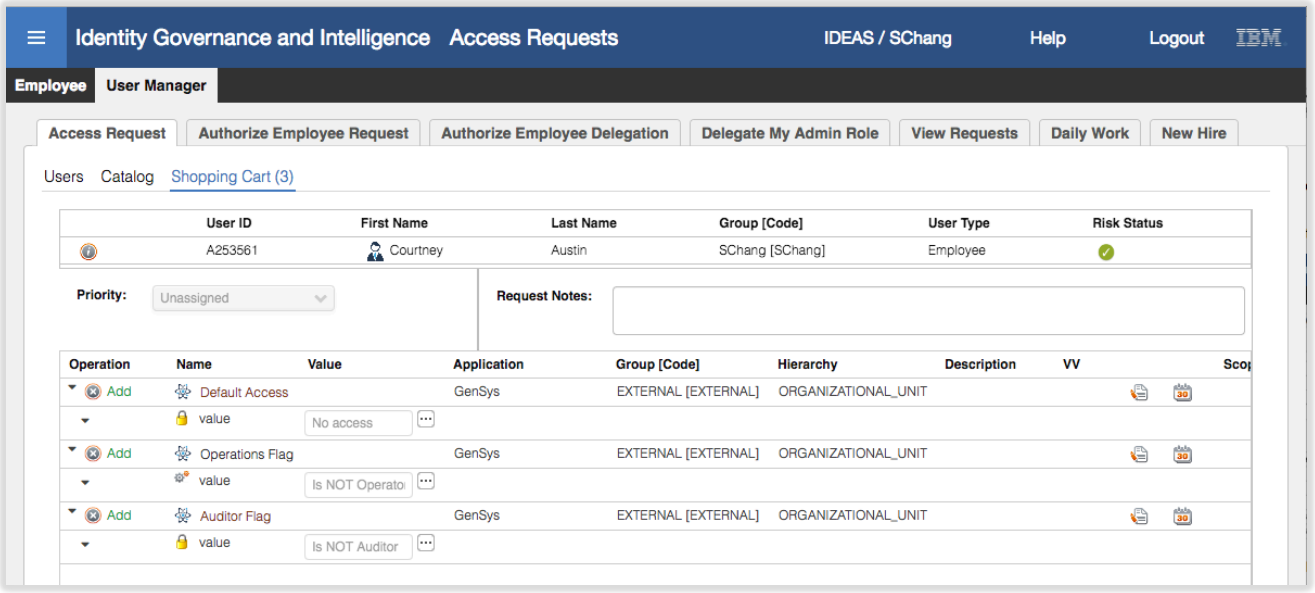
☐ Click the **Permissions** tab and when prompted select the `GenSys` application



The three permissions are shown, including highlighting the two required attributes (in brown typeface).

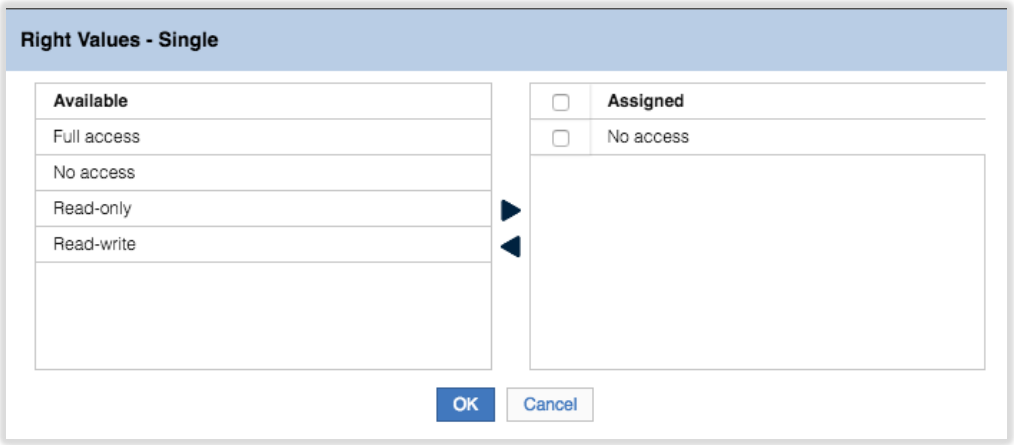
☐ Click the **Add** button for all three permissions
☐ Click **Next** to go to the Shopping Cart tab

The Shopping Cart view shows the three permissions selected with an additional line showing the rights on the permissions. The padlock means the permission is required. The default values are pre-selected.



For example, the “Default Access” permission has a default value of “No access” selected.

☐ Click on the ellipses icon **[…]** for the `Default Access` value

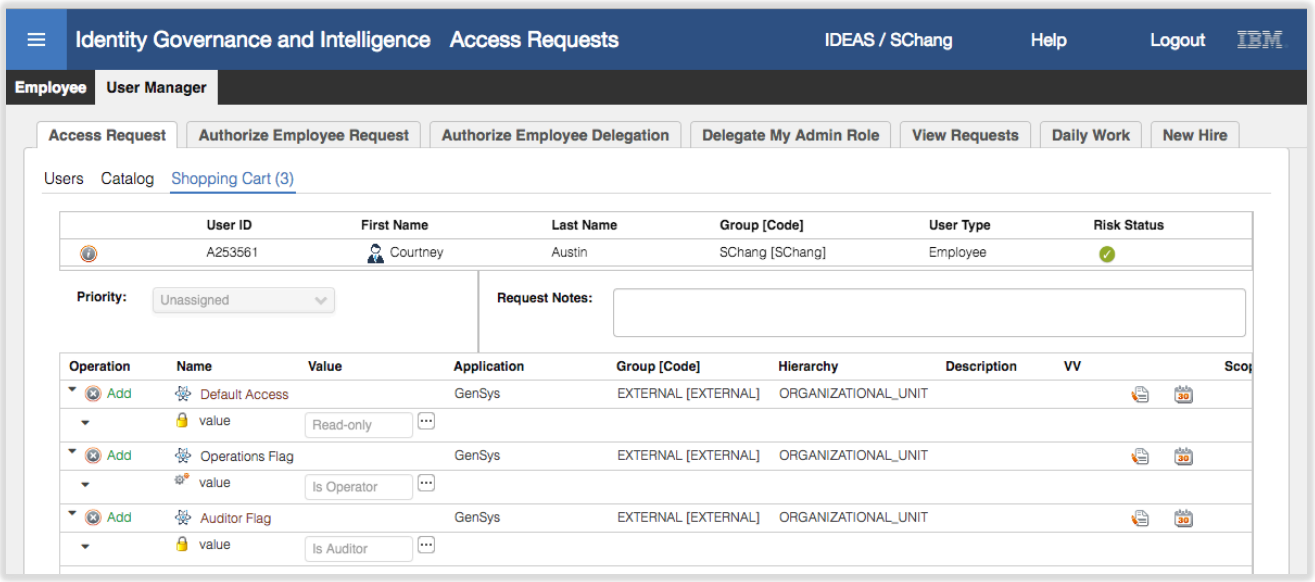


☐ Select the `Read-only` value on the left and click the **right arrow**.

> Notice that it replaces the No access value on the right. This is because this is a single-valued attribute permission. If multi-valued had been selected when the Permission was defined, multiple values could be moved to the Assigned side.

☐ Click **OK**

☐ For both the `Operations Flag` and the `Auditor Flag`, change the values to `Is Operator` and `Is Auditor` respectively



☐ **Submit** the request

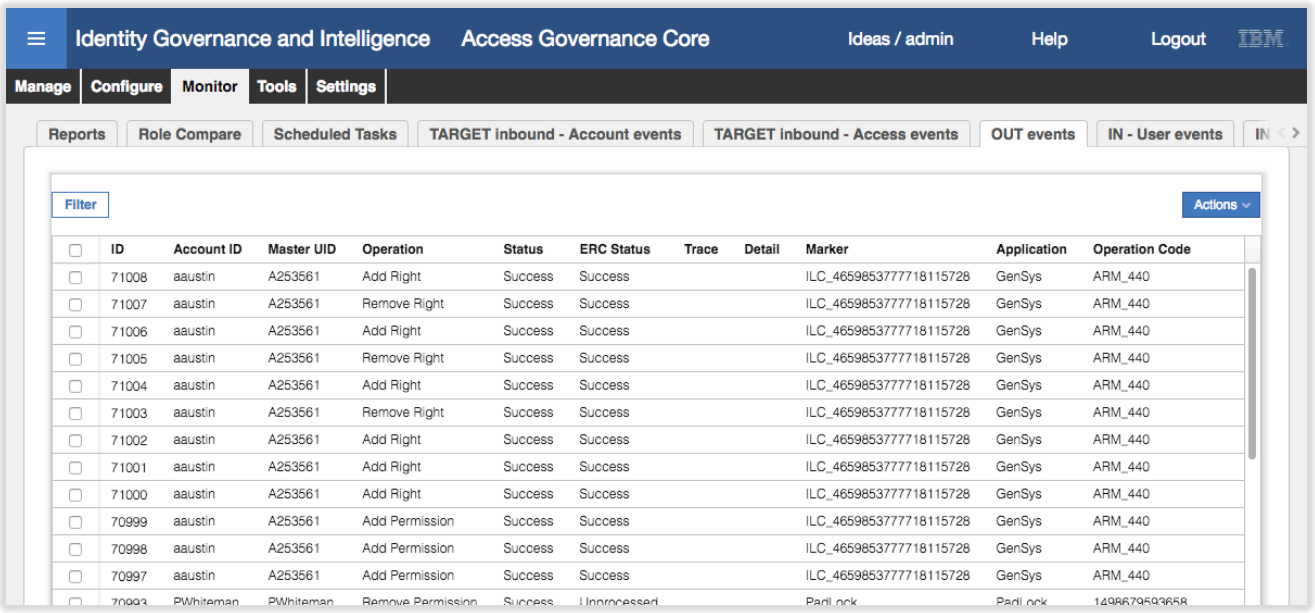
☐ The workflow for this requires the Application Owner to approve. Log out and log in as `RPeterson` (`Passw0rd`) and approve this access request.

Notice that he only see's the permissions not the rights.

3.2.2 Checking the Requested Attribute-Permissions

With the access request submitted and approved, we need to check its progress through IGI and to the target LDAP.

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

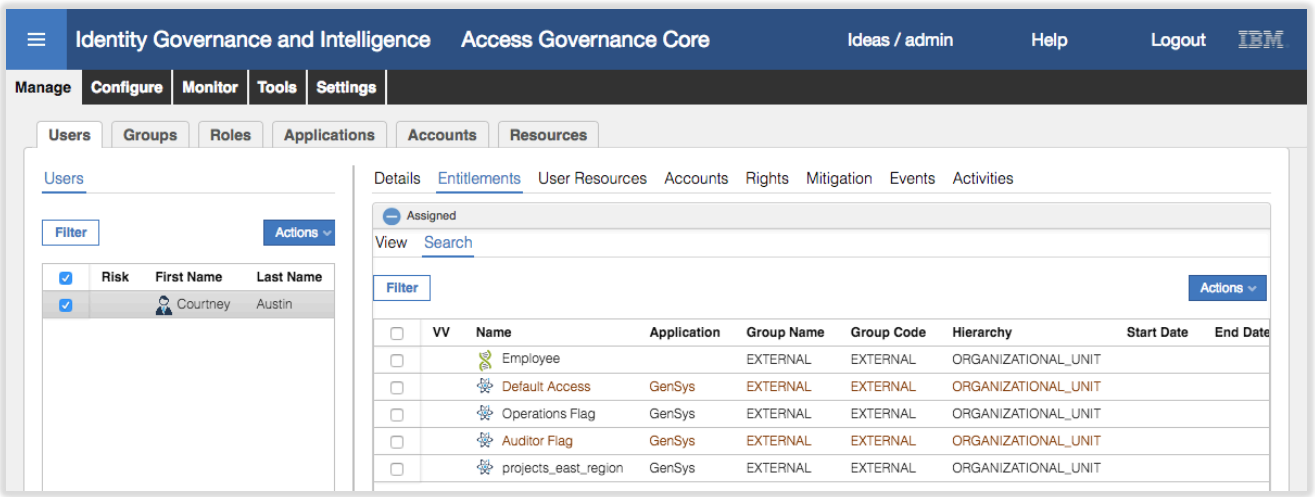


You should see several events relating to adding permissions and rights.

Ignore the “Remove Right” events and the extra “Add Permission” events as they relate to how IGI handles the access and how the adapter processes the events.

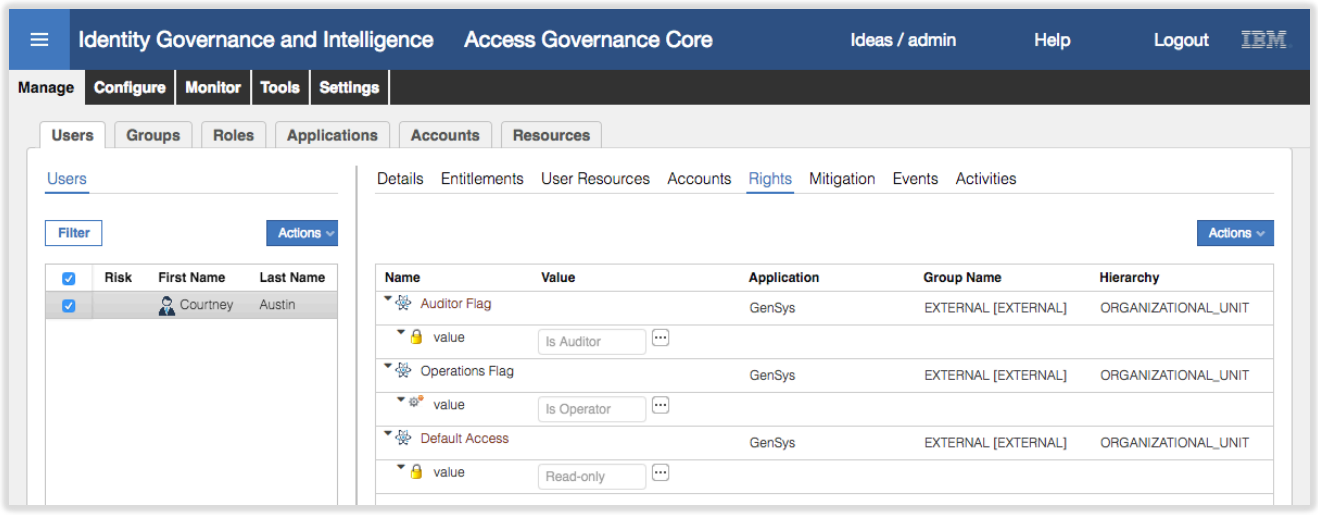
The Status and ERC Status should be Success. The Status result is for the internal IGI processing, the ERC Status is for the external event processing (in this case by the Broker and LDAP adapter).

- ☐ Go to **Manage > Users**
- ☐ Find and select `Courtney Austin` (e.g filter on “`Austin%`”)
- ☐ Go to the **Entitlements** tab



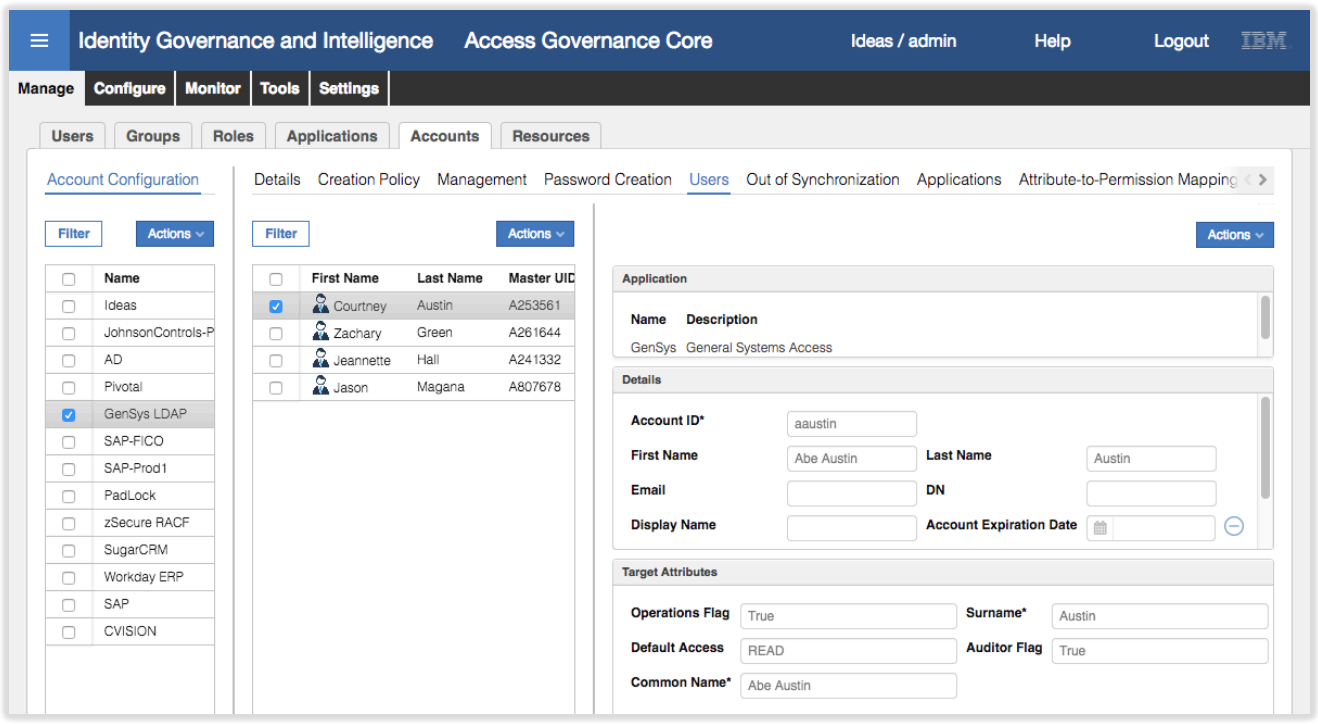
This view shows all the entitlements for Courtney. However, the view does not show the rights on the permissions.

☐ With `Courtney` still selected, Click on the **Rights** tab



This shows the values (rights) for each attribute-permission. We can now check the account values.

☐ Go to **Manage > Accounts** and select the `GenSys LDAP` account
☐ Click on the **Users** tab
☐ Select `Courtney` and look at the **Target Attributes** in the right pane



This shows the **Operations Flag** and **Auditor Flag** set to `True` and the **Default Access** set to `READ`, as expected.

To confirm we can go into a terminal session and check the LDAP record.

☐ Go to the IGI Data Server VM console or start a SSH session as `igi` (password `igi`)
☐ Run the following LDAP search command to see the account information

```
/opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b ou=users,ou=gsa,dc=apps "(cn=aaustin)"
```

```
MacBook-Pro-2:~ davidedw$ ssh igi@192.168.42.60
igi@192.168.42.60's password:
Last login: Sun Feb 19 04:42:10 2017
[igi@igi ~]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
ou=users,ou=gsa,dc=apps "(cn=aaustin)"
cn=aaustin,ou=users,ou=gsa,DC=APPS
telephonenumber=1-512-124-8643
userpassword=p1Ehm2GD
objectclass=inetorgperson
objectclass=organizationalperson
objectclass=person
objectclass=top
givenname=Abe
employeenumber=qw123453
title=Accounts receivable
sn=Austin
cn=Abe Austin
cn=aaustin
carlicense=True
departmentnumber=READ
businesscategory=True
[igi@igi ~]$
```

The last three lines confirm the attribute values have been applied to the account.

The last part of the lab will use a certification campaign to verify and update the attribute-permission values.

3.3 Part 3 – Review Attribute-Permissions with Access Certification

In this part of the lab we will use a certification campaign to review and update the attribute permissions given to Courtney in the last part.

3.3.1 Setup Dataset and Campaign

We need to setup a campaign dataset and certification campaign and launch it. These steps are only summarized; you should know how to do this from prior training.

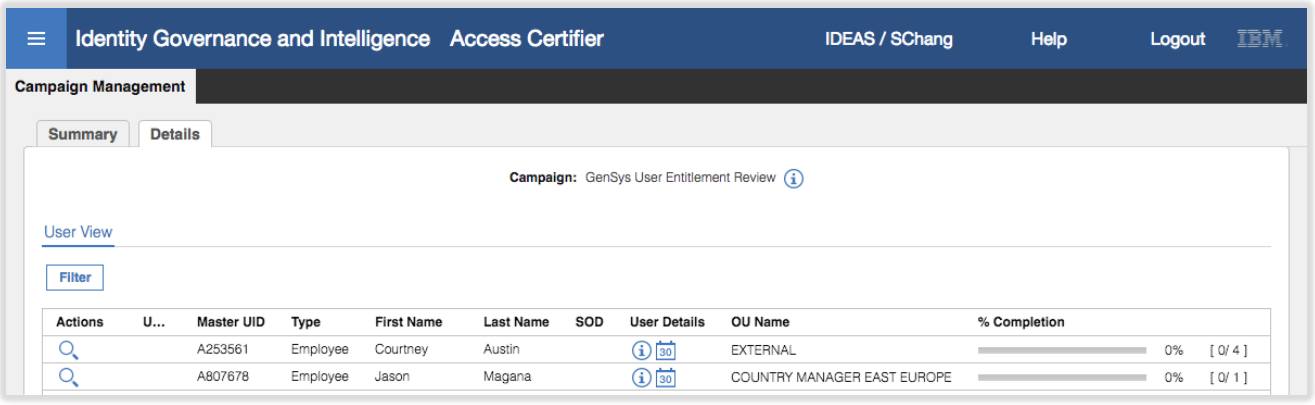
- ☐ Setup a new certification dataset (non-default values);
  - Details - Campaign Name: “GenSys-only”,
  - Details - Campaign Type: “User Assignment”,
  - Applications -> White List -> “GenSys”.
- ☐ Setup a new certification campaign (non-default values) – Save at each step!;
  - Details - Campaign Name: “GenSys User Entitlement Review”
  - Details - Campaign Type: “User Assignment”
  - Details - Certification Dataset: GenSys-only
  - Supervisors – add Myriam Brewer as the supervisor
  - Reviewers – Scope: User Hierarchy of Managers
  - Reviewers – Default Reviewer: David Fox (DFox)
  - Fulfillment – Physical deletion with 0 grace days (**this is important!!!!**)
  - Everything else can be left as default
- ☐ Launch the campaign and wait for it to start

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

3.3.2 Review and Update Access in the Campaign

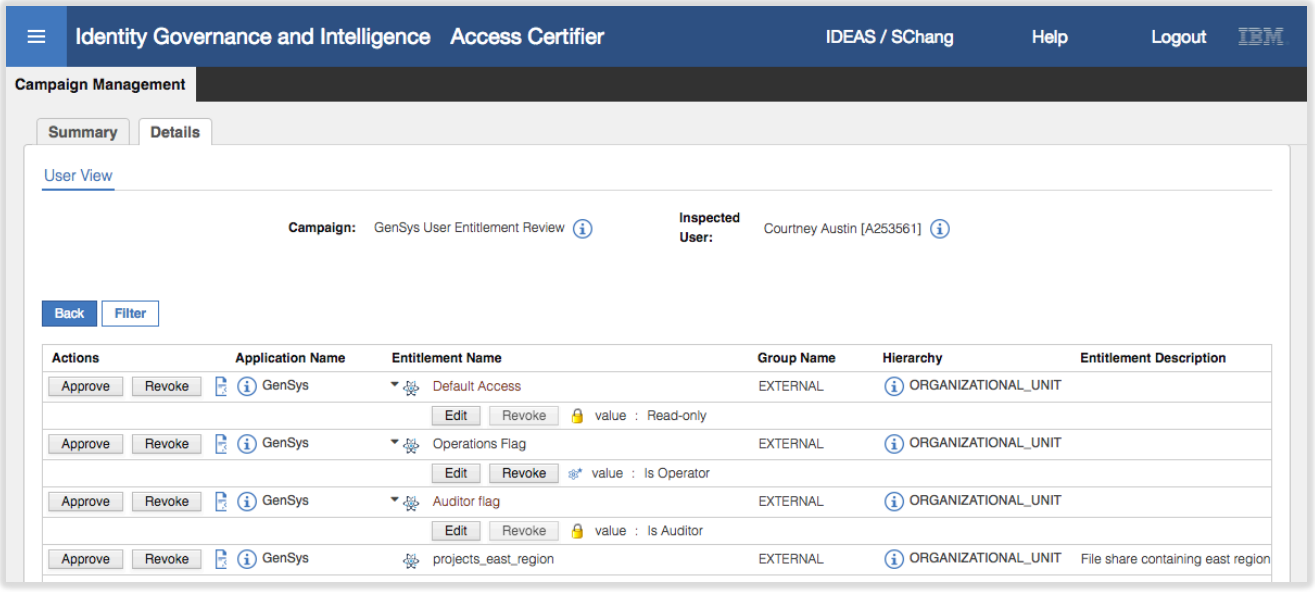
Steps:

- ☐ Log into the **Service Center** as `SChang` (`Passw0rd`)
- ☐ Go to **Access Certifier** and select the `GenSys User Entitlement Review` campaign



☐ View entitlements for `Courtney Austin`

☐ Expand each of the **Entitlements** (click the arrow beside the entitlement name)



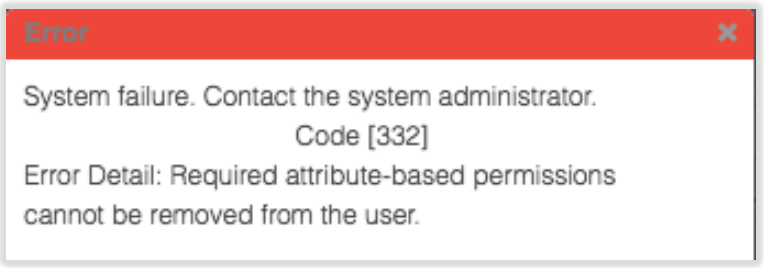
The three attribute-permissions are shown.

> Depending on your screen resolution you may not see the permission values (the rights values). If this is the case, hover your mouse pointer on the title line between “Entitlement Name” and “Group Name [Code] and move it until it changes to the resize icon and you can move Group Name [Code] to the right until you see the rights values.

Notice that the value Revoke buttons are greyed-out for the two required permissions (`Default Access` and `Auditor Flag`).

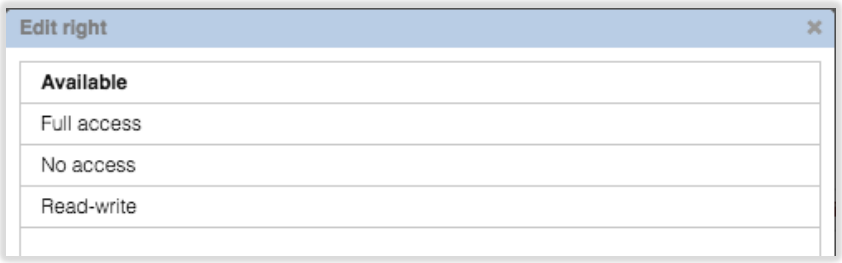
☐ Click the main **Revoke** (under Actions column, not the greyed-out one) button beside `Default Access`

You should see an error dialog



This indicates that you can't revoke an attribute-permission that is marked as required. This is why the value Revoke buttons are greyed-out.

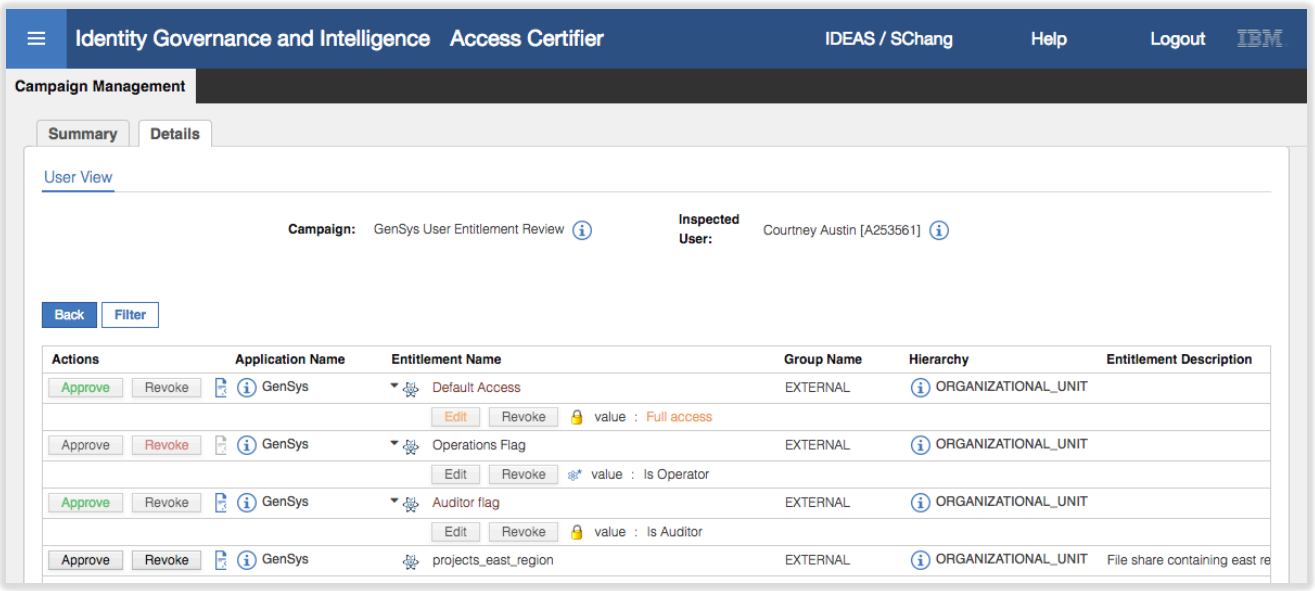
- ☐ Click **OK** to close the error dialog
- ☐ Expand the `Default Access` permission again and click the **Edit** button



This dialog shows the other values available (Read-only) is the current value so is not shown

- ☐ Select `Full access` and click **OK**
- ☐ Click **Approve** for the permission
- ☐ Click **Revoke** for the `Operations Flag`
- ☐ **Approve** the `Auditor Flag` permission

If you expand all three permissions again you should see that `Default Access` has been edited (Edit button now orange) and the changed value is shown in orange also. The other two values are unchanged, so remain black.

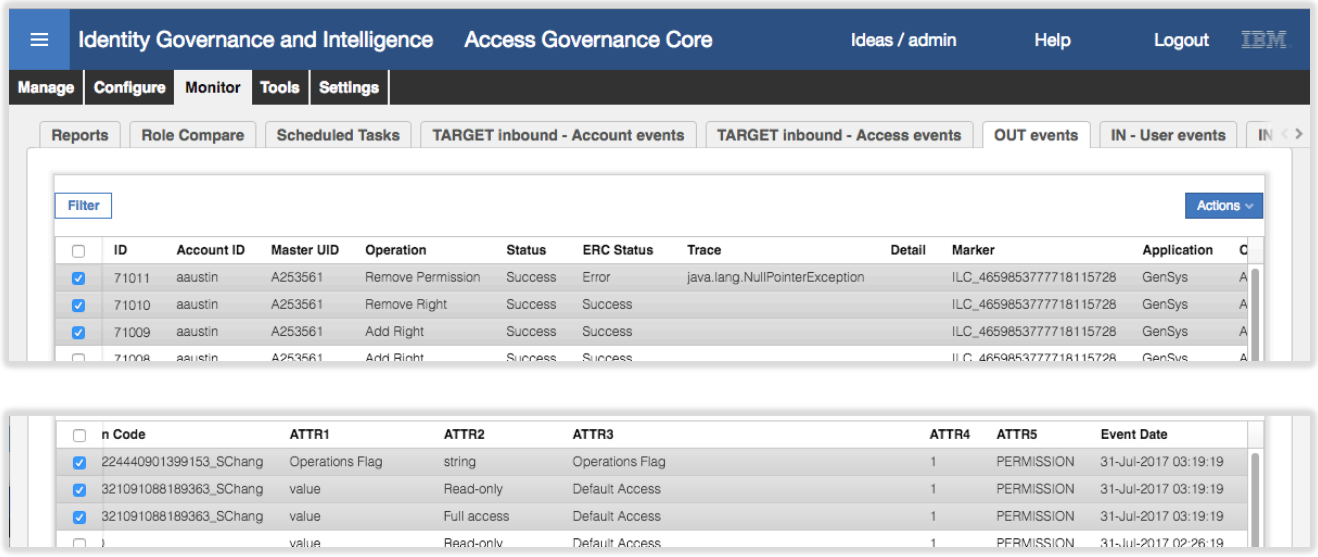


As we set the campaign to process each approve/revoke as it's done by the manager, there should be changes processed by IGI and the adapter immediately.

3.3.3 Review Changes Resulting from Campaign

We will now switch back to the administrator to check for completion of the changes.

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

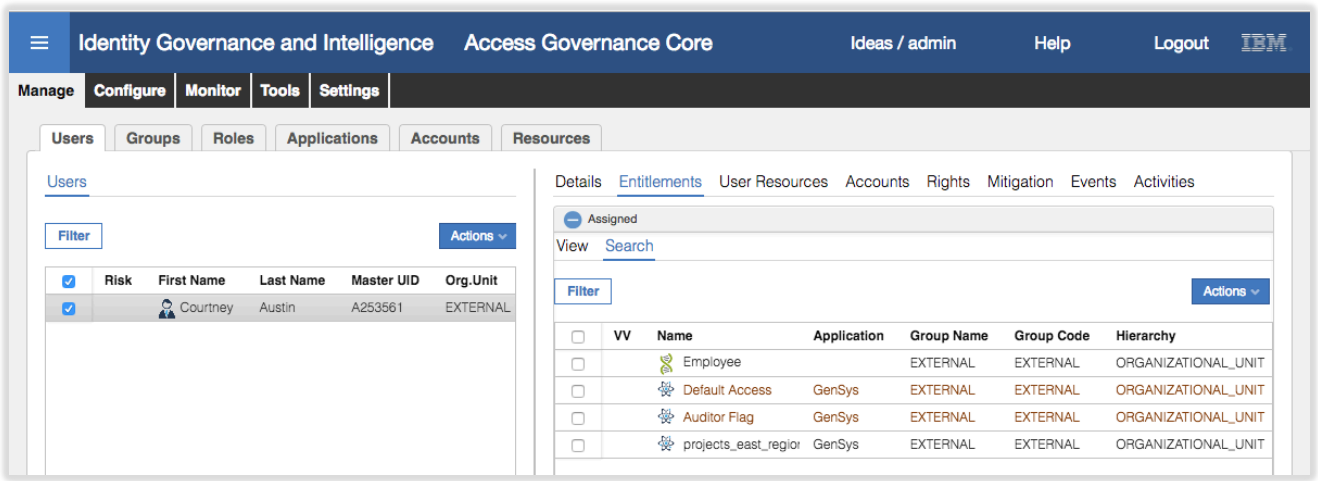


You should see events related to the campaign changes (highlighted above). Two relate to the `Default Access` permission, where the `Read-only` right is removed and the `Full access` right is being added.

> There appears to be an issue with removing the right on the `Operations Flag` attribute. You would expect that if the non-default value was Revoked then IGI would revert to the Default value. This may be a bug that needs to be resolved, but won't affect the rest of the lab.

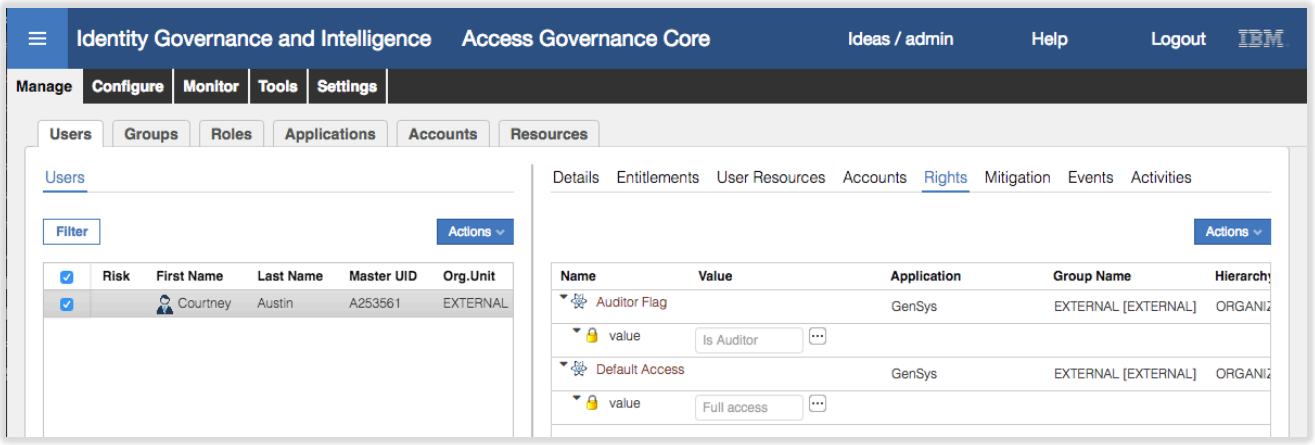
Were all the changes from the campaign applied? We need to go check the user's permissions and rights.

- ☐ Go to **Manage > Users**
- ☐ Find and select `Courtney Austin` (e.g filter on "`Austin%`")
- ☐ Go to the **Entitlements** tab



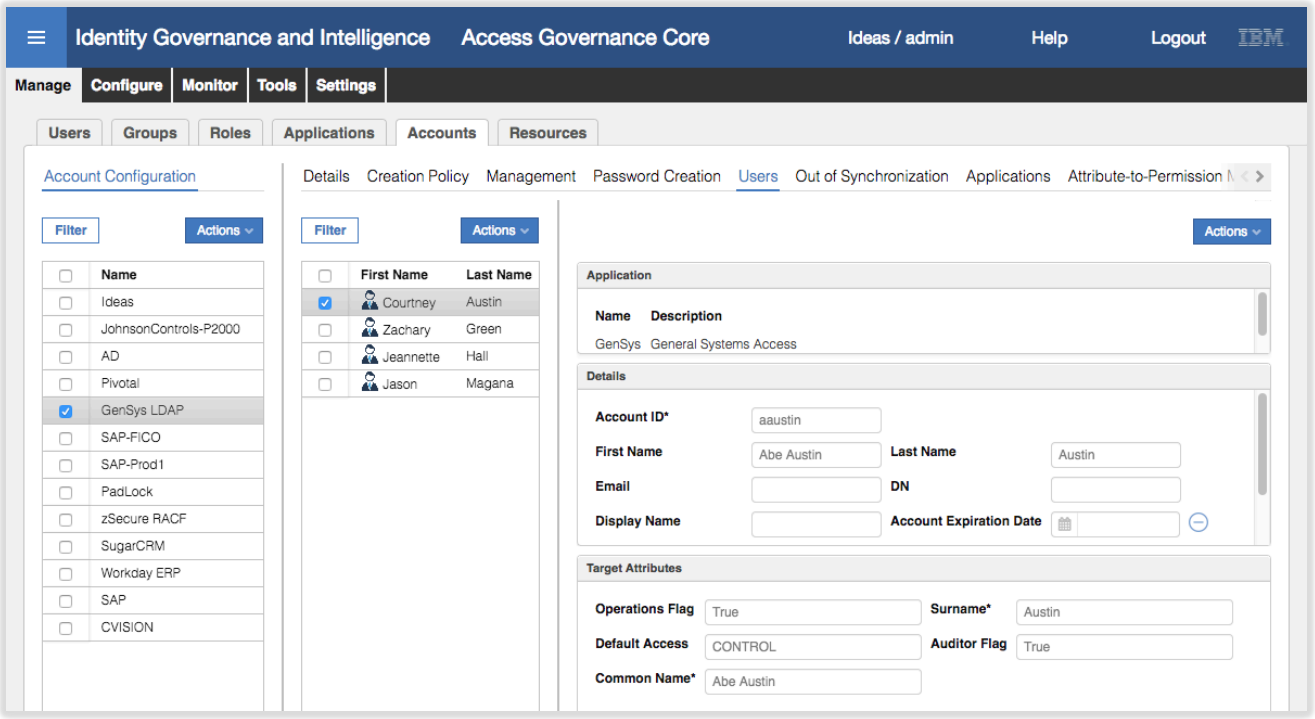
This view shows all the entitlements for `Courtney`. We can see that the `Operations Flag` permission has been removed.

- ☐ With `Courtney` still selected, Click on the **Rights** tab



We can see she has the `Is Auditor` value for the `Auditor Flag` permission (unchanged, as expected) and `Full Access` for the `Default Access` permission (changed, as expected).

- ☐ Go to **Manage > Accounts** and select the `GenSys LDAP` account
- ☐ Click on the **Users** tab
- ☐ Select `Courtney` and look at the **Account Attributes** in the right pane



The Operations Flag attribute has NOT been removed. The Auditor Flag value remains as “True”.

Running the LDAP query command also confirms the only change to the account was the change to departmentnumber to CONTROL.

```
[igi@igidb ~]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
ou=users,ou=gsa,dc=apps "(cn=aaustin)"
cn=aaustin,ou=users,ou=gsa,DC=APPS
telephonenumber=1-512-124-8643
userpassword=p1Ehm2GD
objectclass=inetorgperson
objectclass=organizationalperson
objectclass=person
objectclass=top
givenname=Abe
employeenumber=qw123453
title=Accounts receivable
sn=Austin
cn=Abe Austin
cn=aaustin
carlicense=True
businesscategory=True
departmentnumber=CONTROL
```

This completes this lab.

Care should be taken with choosing the settings for the attribute-permissions. Of note:

- Setting an attribute-permission as `not required` will mean the entire account attribute can be removed. If you need to have a default setting, you should make the attribute required.
- Once an attribute-permission has been marked as `required` and the permission is assigned to a user, the permission cannot be removed from the user.

End of Document

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at ibm.com/legal/copytrade.shtml.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

International Business Machines Corporation
New Orchard Road Armonk, NY 10504
Produced in the United States of America 01-2016