



IBM Security

Intelligence. Integration. Expertise.



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	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 – Define Permission Attributes.....	6
3.1.1 Import and Configure Account Attributes.....	6
3.1.2 Import and Configure Attribute Permissions	10
3.2 Part 2 – Request Attribute-Permissions with Access Request Mgmt.....	16
3.2.1 Requesting Attribute-Permissions	16
3.2.2 Checking the Requested Attribute-Permissions	19
3.3 Part 3 – Review Attribute-Permissions with Access Certification.....	21
3.3.1 Setup Dataset and Campaign.....	21
3.3.2 Review and Update Access in the Campaign.....	21
3.3.3 Review Changes Resulting from Campaign	23
Notices	27

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/GestionCfgPwd.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)

	Required	Visible	Editable	Position	Name	Multiple values	Lookup	UI Rendering	Size	Default Value	Enabled
<input checked="" type="checkbox"/>					GenSys LDAP						

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.

Discover Attributes from Target

<input type="checkbox"/>	Attribute Name	Type	Required
<input type="checkbox"/>	erLdapContainerName	string	<input type="checkbox"/>
<input type="checkbox"/>	erLdapGroupName	string	<input type="checkbox"/>
<input type="checkbox"/>	erLdapPwdChangedTime	dateTime	<input type="checkbox"/>
<input type="checkbox"/>	erLdapPwdReset	boolean	<input type="checkbox"/>
<input type="checkbox"/>	cn	string	<input checked="" type="checkbox"/>
<input type="checkbox"/>	sn	string	<input checked="" type="checkbox"/>
<input type="checkbox"/>	audio	binary	<input type="checkbox"/>
<input type="checkbox"/>	businessCategory	string	<input type="checkbox"/>
<input type="checkbox"/>	carLicense	string	<input type="checkbox"/>
<input type="checkbox"/>	departmentNumber	string	<input type="checkbox"/>

Results: 47 << < 1 of 1 > >

Import **Cancel**

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

Discover Attributes from Target

<input type="checkbox"/>	Attribute Name	Type	Required
<input type="checkbox"/>	erLdapPwdReset	boolean	<input type="checkbox"/>
<input checked="" type="checkbox"/>	cn	string	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	sn	string	<input checked="" type="checkbox"/>
<input type="checkbox"/>	audio	binary	<input type="checkbox"/>
<input checked="" type="checkbox"/>	businessCategory	string	<input type="checkbox"/>
<input checked="" type="checkbox"/>	carLicense	string	<input type="checkbox"/>
<input checked="" type="checkbox"/>	departmentNumber	string	<input type="checkbox"/>
<input type="checkbox"/>	description	string	<input type="checkbox"/>
<input type="checkbox"/>	destinationIndicator	string	<input type="checkbox"/>
<input type="checkbox"/>	displayName	string	<input type="checkbox"/>

Results: 47 << < 1 of 1 > >

Import **Cancel**

- Click **Import**
- On the **Accounts > Target Attributes** page check that all five attributes are Visible

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 menu includes 'Manage', 'Configure' (which is currently selected), 'Monitor', 'Tools', and 'Settings'. Below this, a secondary navigation bar has tabs for 'Users', 'Groups', 'Roles', 'Applications', 'Accounts' (selected), and 'Resources'. On the left, a sidebar titled 'Account Configuration' lists various accounts with checkboxes and dropdown menus for filtering and actions. The main content area is titled 'Target Attributes' and contains a table with columns: Required, Visible, Editable, Position, Name, Multiple values, and Lookup. The table lists attributes like cn, sn, businessCategory, carLicense, and departmentNumber, each with a '...' button for localization.

- Select the ellipses (...) button beside each of the five attributes and set the English label as follows:

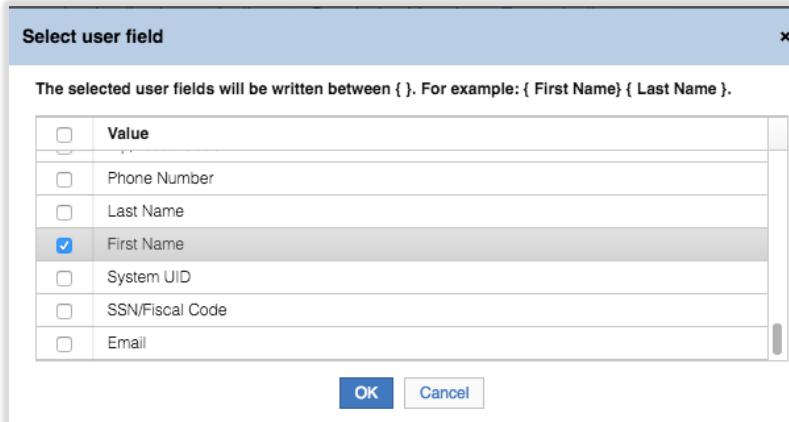
cn	Common Name
sn	Surname
businessCategory	Auditor Flag
carLicense	Operations Flag
departmentNumber	Default Access

The screenshot shows the 'Attribute Localization' dialog box. It has tabs for English, Italian, German, French, Spanish, Portuguese, Chinese, Japanese, and Chinese. The English tab is selected. Below the tabs, there is a 'Label' section with a text input field containing 'Common Name'.

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.

	UI Rendering	Size	Default Value	Enforce User value
<input type="checkbox"/>	Textfield		{First Name}	User.field
<input type="checkbox"/>	Textfield			User.field
<input type="checkbox"/>	Textfield			User.field
<input type="checkbox"/>	Textfield			User.field
<input type="checkbox"/>	Textfield			User.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.

	UI Rendering	Size	Default Value	Enforce User value
<input type="checkbox"/>	Textfield		{First Name} {Last Name}	User.field
<input type="checkbox"/>	Textfield		{Last Name}	User.field
<input type="checkbox"/>	Textfield			User.field
<input type="checkbox"/>	Textfield			User.field
<input type="checkbox"/>	Textfield			User.field

- Click **Save**
- Still within the **Accounts** tab, click on the **Users** tab and select the user Courtney Austin

The screenshot shows the IBM Security Access Governance Core interface. In the top navigation bar, 'Identity Governance and Intelligence' and 'Access Governance Core' are selected. The left sidebar has 'Manage' selected. The main content area has 'Accounts' selected. On the left, a list of accounts includes 'Ideas', 'JohnsonControls-P2000', 'AD', 'Pivotal', 'GenSys LDAP' (selected), 'SAP-FICO', 'SAP-Prod1', 'PadLock', 'zSecure RACF', 'SugarCRM', 'Workday ERP', 'SAP', and 'CVISION'. On the right, a detailed view for the 'GenSys LDAP' account shows a table of users (Courtney Austin, Zachary Green, Jeannette Hall, Jason Magana) and their attributes (First Name, Last Name). Below this is a 'Details' section with fields for Account ID (aaustin), First Name (Abe Austin), Last Name (Austin), Email (DN), Display Name, and Account Expiration Date. At the bottom is a 'Target Attributes' section with fields for Surname (Austin), Common Name (Abe Austin), Default Access, Auditor Flag, and Operations Flag.

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)

The screenshot shows the 'Attribute-to-Permission Mapping' tab for the 'GenSys LDAP' account. The table has columns for Permission Name, Attribute Name, Type, Multi-value, Required, Rights Value, and Default. There are no rows in the table.

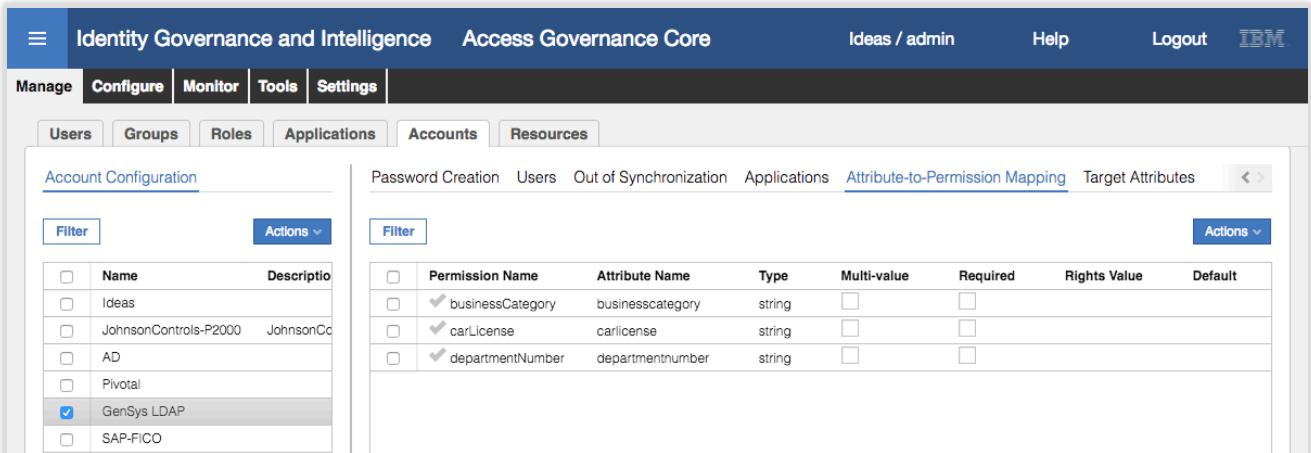
There are no attribute permissions defined.

- Select **Actions > Discover Account attributes from Target**
- Select the three attributes: businessCategory, carLicense, and departmentNumber

Discover Attributes from Target

<input type="checkbox"/>	Attribute Name	Type	Required
<input type="checkbox"/>	audio	binary	<input type="checkbox"/>
<input checked="" type="checkbox"/>	businessCategory	string	<input type="checkbox"/>
<input checked="" type="checkbox"/>	carLicense	string	<input type="checkbox"/>
<input checked="" type="checkbox"/>	departmentNumber	string	<input type="checkbox"/>
<input type="checkbox"/>	description	string	<input type="checkbox"/>
<input type="checkbox"/>	destinationIndicator	string	<input type="checkbox"/>
<input type="checkbox"/>	displayName	string	<input type="checkbox"/>

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



The screenshot shows the IBM Security Access Governance Core interface. At the top, there's a navigation bar with tabs for Identity Governance and Intelligence, Access Governance Core, Ideas / admin, Help, Logout, and IBM. Below the navigation bar, there's a secondary navigation bar with tabs for Manage, Configure, Monitor, Tools, Settings, Users, Groups, Roles, Applications, Accounts, and Resources. The Accounts tab is selected. On the left, there's a sidebar titled "Account Configuration" with a "Filter" button and an "Actions" dropdown. It lists several accounts: Ideas, JohnsonControls-P2000, AD, Pivotal, GenSys LDAP (which is selected), and SAP-FICO. On the right, there's a main content area with tabs for Password Creation, Users, Out of Synchronization, Applications, Attribute-to-Permission Mapping (which is selected), and Target Attributes. Under the "Attribute-to-Permission Mapping" tab, there's a "Filter" button and an "Actions" dropdown. A table lists three attributes: businessCategory, carLicense, and departmentNumber, each with a checked checkbox in the "Permission Name" column. The columns include Permission Name, Attribute Name, Type, Multi-value, Required, Rights Value, and Default.

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

Edit Attribute Mapping

Attribute name	businesscategory	Permission name	Auditor flag										
Type	string	Use rights value as permission	<input type="checkbox"/>										
Required	<input checked="" type="checkbox"/>												
Multi-value	<input type="checkbox"/>												
Attribute value	<table border="1"> <tr> <td>True</td> <td>Is Auditor</td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td>False</td> <td>Is NOT Auditor</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="radio"/></td> <td><input type="button" value="Delete"/></td> </tr> </table>			True	Is Auditor	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="Delete"/>	False	Is NOT Auditor	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="button" value="Delete"/>
True	Is Auditor	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="Delete"/>									
False	Is NOT Auditor	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="button" value="Delete"/>									
<input type="button" value="Add Value"/>													
<input type="button" value="Save"/> <input type="button" value="Cancel"/>													

- 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

Edit Attribute Mapping

Attribute name	carlicense	Permission name	Operations Flag										
Type	string	Use rights value as permission	<input type="checkbox"/>										
Required	<input type="checkbox"/>												
Multi-value	<input type="checkbox"/>												
Attribute value	<table border="1"> <tr> <td>True</td> <td>Is Operator</td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td><input type="button" value="Delete"/></td> </tr> <tr> <td>False</td> <td>Is NOT Operator</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="radio"/></td> <td><input type="button" value="Delete"/></td> </tr> </table>			True	Is Operator	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="Delete"/>	False	Is NOT Operator	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="button" value="Delete"/>
True	Is Operator	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="button" value="Delete"/>									
False	Is NOT Operator	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="button" value="Delete"/>									
<input type="button" value="Add Value"/>													
<input type="button" value="Save"/> <input type="button" value="Cancel"/>													

- 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

Edit Attribute Mapping

Attribute name	departmentnumber	Permission name	Default Access
Type	string	Use rights value as permission	<input type="checkbox"/>
Required	<input checked="" type="checkbox"/>		
Multi-value	<input type="checkbox"/>		
Attribute value	Rights value	Active	Default
NONE	No access	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>
READ	Read-only	<input checked="" type="checkbox"/>	<input type="radio"/>
UPDATE	Read-write	<input checked="" type="checkbox"/>	<input type="radio"/>
CONTROL	Full access	<input checked="" type="checkbox"/>	<input type="radio"/>

Save **Cancel**

- 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 screenshot shows the 'Attribute-to-Permission Mapping' section of the interface. On the left, there's a sidebar with 'Account Configuration' and a list of accounts. In the main area, there are tabs for 'Password Creation', 'Users', 'Out of Synchronization', 'Applications', 'Attribute-to-Permission Mapping' (which is selected), and 'Target Attributes'. Below these tabs is a 'Filter' button and an 'Actions' dropdown. A table lists permissions with their details:

	Permission Name	Attribute Name	Type	Multi-value	Required	Rights Value	Default
<input type="checkbox"/>	<input checked="" type="checkbox"/> Auditor flag	businesscategory	string	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Is NOT Auditor,Is Auditor	Is NOT Auditor
<input type="checkbox"/>	<input checked="" type="checkbox"/> Operations Flag	carlicense	string	<input type="checkbox"/>	<input type="checkbox"/>	Is NOT Operator,Is Operator	Is NOT Operator
<input type="checkbox"/>	<input checked="" type="checkbox"/> Default Access	departmentnumber	string	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Full access,No access,Read-only,Read-write	No access

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

The screenshot shows the 'Attribute-to-Permission Mapping' section. On the left, there's a list of accounts with checkboxes. On the right, a table lists permissions with columns for Permission Name, Attribute Name, Type, Multi-value, Required, Rights Value, and Default. The 'Default Access' permission is selected.

	Permission Name	Attribute Name	Type	Multi-value	Required	Rights Value	Default
<input type="checkbox"/>	Auditor flag	businesscategory	string	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Is NOT Auditor,Is Auditor	Is NOT Auditor
<input type="checkbox"/>	Operations Flag	caricense	string	<input type="checkbox"/>	<input type="checkbox"/>	Is NOT Operator,Is Operator	Is NOT Operator
<input type="checkbox"/>	Default Access	departmentnumber	string	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Full access,No access,Read-only,Read-write	No access

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

The screenshot shows the 'Role Management' section. On the left, a list of roles is shown with checkboxes. On the right, a detailed view of the 'Default Access' role is displayed, including fields for Version, Owner, Name, Code, Description, Type, Application, Permission Type, Entitlement Families, Expiration, and Last Review Date.

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

Identity Governance and Intelligence Access Governance Core

Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Hier View Flat View

Type: Application: GenSys

Name or Code:

Published: All

Search

Actions

<input type="checkbox"/>	Name	Application	Description
<input checked="" type="checkbox"/>	Default Access	GenSys	
<input type="checkbox"/>	Operations Flag	GenSys	
<input type="checkbox"/>	Auditor Flag	GenSys	
<input type="checkbox"/>	projects_east_region	GenSys	File share
<input type="checkbox"/>	projects_west_region	GenSys	File share
<input type="checkbox"/>	projects_north_region	GenSys	File share
<input type="checkbox"/>	projects_south_region	GenSys	File share

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

Details Management Users Organization Units Application Access Rights Analysis History

Filter

<input type="checkbox"/>	Name	ID Code	Hierarchy
<input type="checkbox"/>	ACME	root	ORGANIZATIONAL
<input type="checkbox"/>	SOUTH	SOUTH	ORGANIZATIONAL
<input type="checkbox"/>	QUALITY AND SECURITY	QUALITY AND SECURITY	ORGANIZATIONAL
<input type="checkbox"/>	COUNTRY MANAGER EMEA	COUNTRY MANAGER EMEA	ORGANIZATIONAL
<input type="checkbox"/>	GENERAL SERVICES	GENERAL SERVICES	ORGANIZATIONAL
<input type="checkbox"/>	MARKETING	MARKETING	ORGANIZATIONAL
<input type="checkbox"/>	INTERNATIONAL HR	INTERNATIONAL HR	ORGANIZATIONAL
<input type="checkbox"/>	SHARED AND FUNCTIONAL	SHARED AND FUNCTIONAL	ORGANIZATIONAL
<input type="checkbox"/>	EXTERNAL	EXTERNAL	ORGANIZATIONAL
<input type="checkbox"/>	COUNTRY MANAGER EAST EUROPE	COUNTRY MANAGER EAST EUROPE	ORGANIZATIONAL
<input type="checkbox"/>	SALES	SALES	ORGANIZATIONAL
<input type="checkbox"/>	CORPORATE	CORPORATE	ORGANIZATIONAL
<input type="checkbox"/>	IT	IT	ORGANIZATIONAL
<input type="checkbox"/>	ADMINISTRATION, FINANCE AND CONTROL	ADMINISTRATION, FINANCE AND CONTROL	ORGANIZATIONAL
<input type="checkbox"/>	CENTER	CENTER	ORGANIZATIONAL
<input type="checkbox"/>	INT PLANNING AND CONTROL	INT PLANNING AND CONTROL	ORGANIZATIONAL
<input type="checkbox"/>	INTEGR, SAFETY AND OPERATION SUPPORT	INTEGR, SAFETY AND OPERATION SUPPORT	ORGANIZATIONAL
<input type="checkbox"/>	SYSTEMS ADMINISTRATION	SYSTEMS ADMINISTRATION	ORGANIZATIONAL

Items Per Page: 50 Results: 33 << < 1 of 1 > >>

- 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

Identity Governance and Intelligence Access Governance Core

Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Hier View Flat View

Type: Application: GenSys

Name or Code:

Published: All

Search

Actions

<input type="checkbox"/>	Name	Application	Description
<input checked="" type="checkbox"/>	Default Access	GenSys	
<input type="checkbox"/>	Operations Flag	GenSys	
<input type="checkbox"/>	Auditor Flag	GenSys	
<input type="checkbox"/>	projects_east_region	GenSys	File share

Details Management Users Organization Units Application Access Rights Analysis History

Filter

MVal/Lookup	Name	Status	Actions
<input checked="" type="checkbox"/>	Default Access	GenSys	Edit Show

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/CrossIideas_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

User ID	First Name	Last Name	Group [Code]	User Type
A253561	Courtney	Austin	SChang [SChang]	Employee

- 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

Identity Governance and Intelligence Access Requests

IDEAS / SChang Help Logout IBM

User Manager

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

Users Catalog Shopping Cart (empty)

User ID	First Name	Last Name	Group [Code]	User Type	Risk Status
A253561	Courtney	Austin	SChang [SChang]	Employee	

Current entitlements Business Roles Application Roles Permissions External Roles

Permissions

Filter Actions

Application	Name	Description	Owner	VV	Permission Type	Group [Code]	Hierarchy
Add GenSys	Default Access	Default Access			string	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Add GenSys	Operations Flag	Operations Flag			string	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Add GenSys	Auditor Flag	Auditor Flag			string	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Add GenSys	projects_east_region	File share containing east region project [...]	LdapGroupProfile		EXTERNAL [EXTERNAL]	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Add GenSys	projects_south_region	File share containing south region project [...]	LdapGroupProfile		EXTERNAL [EXTERNAL]	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT

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.

Identity Governance and Intelligence Access Requests

IDEAS / SChang Help Logout IBM

User Manager

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

Users Catalog Shopping Cart (3)

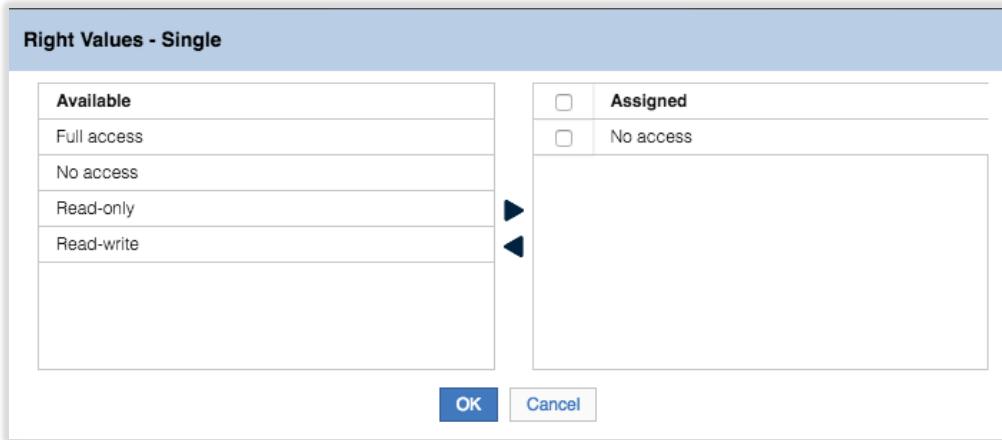
User ID	First Name	Last Name	Group [Code]	User Type	Risk Status
A253561	Courtney	Austin	SChang [SChang]	Employee	

Priority: Unassigned Request Notes:

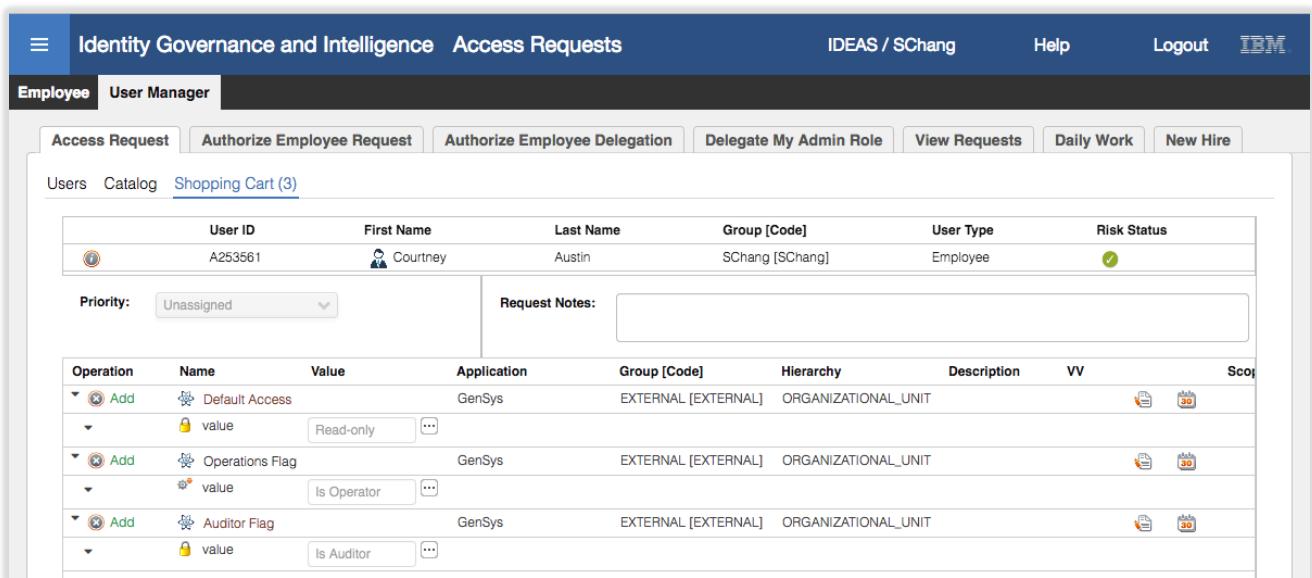
Operation	Name	Value	Application	Group [Code]	Hierarchy	Description	VV	Scope
Add	Default Access	No access	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT	Default Access		
Add	Operations Flag	No access	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT	Operations Flag		
Add	Auditor Flag	No access	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT	Auditor Flag		

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



The screenshot shows the "Identity Governance and Intelligence Access Requests" application. The top navigation bar includes "IDEAS / SChang", "Help", "Logout", and the IBM logo. The main menu has "Employee" and "User Manager" tabs, with "User Manager" being active. Below the menu is a toolbar with links: "Access Request", "Authorize Employee Request", "Authorize Employee Delegation", "Delegate My Admin Role", "View Requests", "Daily Work", and "New Hire". The main content area displays an "Access Request" for user "A253561" (Courtney Austin, Group [Code]: SChang [SChang], User Type: Employee). The "Priority" is set to "Unassigned". The "Request Notes" field is empty. The "Scope" section shows icons for "Document" and "Email". The "Details" table lists three items:

Operation	Name	Value	Application	Group [Code]	Hierarchy	Description	VV	Scope	
Add	Default Access	Read-only	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT				
Add	Operations Flag	Is Operator	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT				
Add	Auditor Flag	Is Auditor	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT				

- 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**

The screenshot shows the 'OUT events' tab in the 'Monitor' section of the Access Governance Core interface. The table displays various audit events:

ID	Account ID	Master UID	Operation	Status	ERC Status	Trace	Detail	Marker	Application	Operation Code
71008	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71007	aaustin	A253561	Remove Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71006	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71005	aaustin	A253561	Remove Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71004	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71003	aaustin	A253561	Remove Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71002	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71001	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
71000	aaustin	A253561	Add Right	Success	Success	ILC_465985377718115728			GenSys	ARM_440
70999	aaustin	A253561	Add Permission	Success	Success	ILC_465985377718115728			GenSys	ARM_440
70998	aaustin	A253561	Add Permission	Success	Success	ILC_465985377718115728			GenSys	ARM_440
70997	aaustin	A253561	Add Permission	Success	Success	ILC_465985377718115728			GenSys	ARM_440
70993	PWhitman	PWhitman	Remove Permission	Success	Unprocessed				Padl ock	149867959365

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).

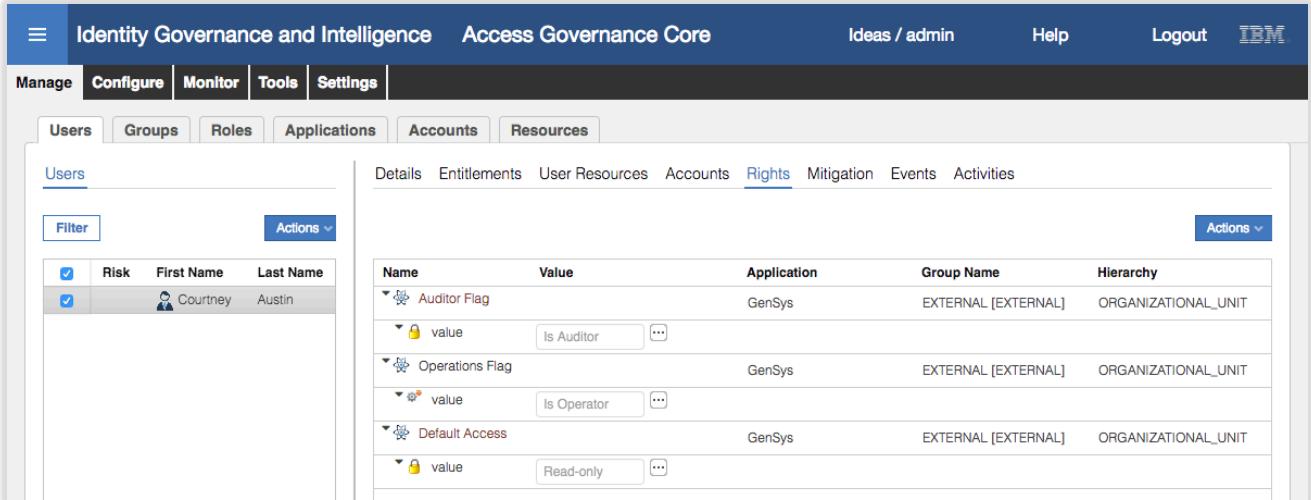
- Go to **Manage > Users**
- Find and select Courtney Austin (e.g filter on “Austin%”)
- Go to the **Entitlements** tab

The screenshot shows the 'Entitlements' tab for the user Courtney Austin in the 'Accounts' section of the Access Governance Core interface. The table displays the entitlements assigned to her:

VV	Name	Application	Group Name	Group Code	Hierarchy	Start Date	End Date
	Employee	EXTERNAL	EXTERNAL		ORGANIZATIONAL_UNIT		
	Default Access	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT		
	Operations Flag	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT		
	Auditor Flag	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT		
	projects_east_region	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT		

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

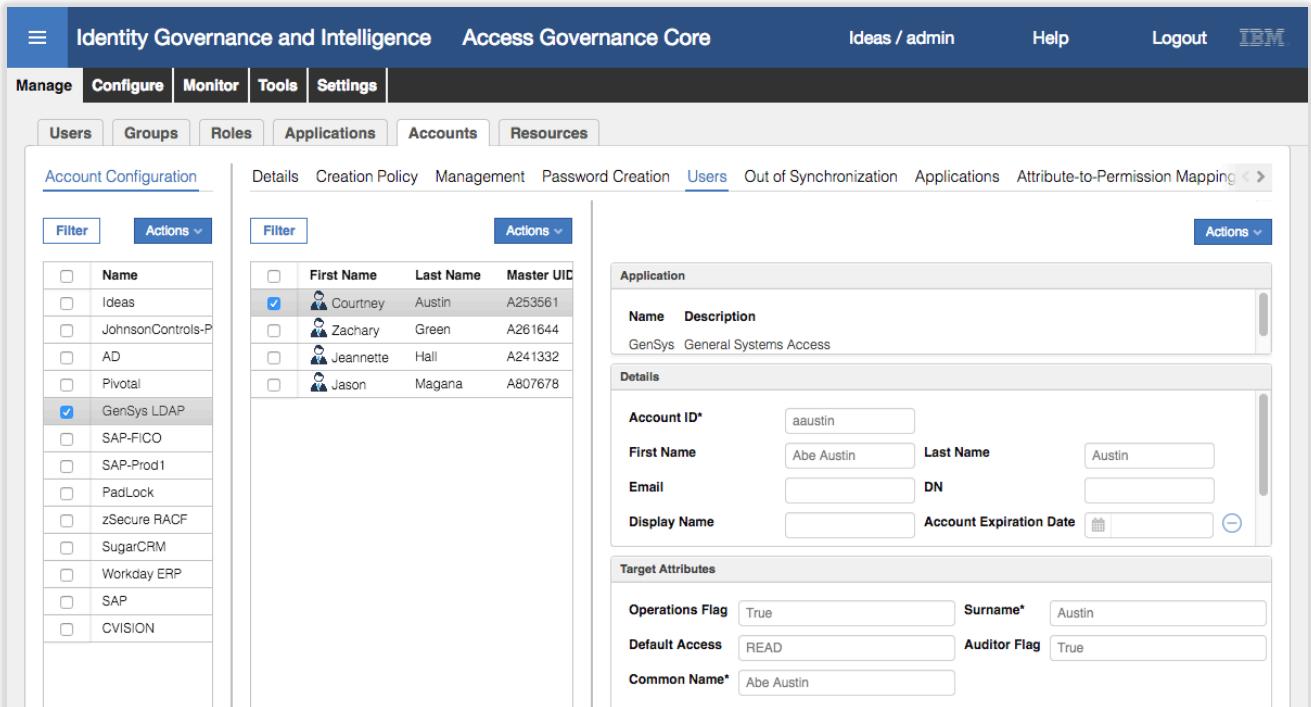


The screenshot shows the Access Governance Core interface. In the top navigation bar, the 'Rights' tab is selected. On the left, there's a sidebar with 'Manage' and 'Configure' sections, and a 'Users' tab is active. The main content area displays a table of rights for the user 'Courtney'. The columns include Name, Value, Application, Group Name, and Hierarchy. The rights listed are:

Name	Value	Application	Group Name	Hierarchy
Auditor Flag	Is Auditor	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Operations Flag	Is Operator	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT
Default Access	Read-only	GenSys	EXTERNAL [EXTERNAL]	ORGANIZATIONAL_UNIT

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



The screenshot shows the Access Governance Core interface with the 'Accounts' tab selected. On the left, the 'Account Configuration' sidebar has 'GenSys LDAP' selected. The main content area shows a list of users under 'Details' tab, with 'Courtney' selected. To the right, the 'Target Attributes' section is expanded, showing the following settings:

Attribute	Value
Operations Flag	True
Default Access	READ
Auditor Flag	True
Common Name*	Abe Austin

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

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

Campaign: GenSys User Entitlement Review [?](#)

User View

Filter

Actions	U...	Master UID	Type	First Name	Last Name	SOD	User Details	OU Name	% Completion
?		A253561	Employee	Courtney	Austin	? 30	EXTERNAL		0% [0/ 4]
?		A807678	Employee	Jason	Magan	? 30	COUNTRY MANAGER EAST EUROPE		0% [0/ 1]

- View entitlements for Courtney Austin
- Expand each of the **Entitlements** (click the arrow beside the entitlement name)

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

User View

Campaign: GenSys User Entitlement Review [?](#) **Inspected User:** Courtney Austin [A253561] [?](#)

Back **Filter**

Actions	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description
Approve Revoke ? GenSys	Default Access		EXTERNAL	? ORGANIZATIONAL_UNIT	
Approve Revoke ? GenSys	Operations Flag		EXTERNAL	? ORGANIZATIONAL_UNIT	
Approve Revoke ? GenSys	Auditor flag		EXTERNAL	? ORGANIZATIONAL_UNIT	
Approve Revoke ? GenSys	projects_east_region		EXTERNAL	? ORGANIZATIONAL_UNIT	File share containing east region

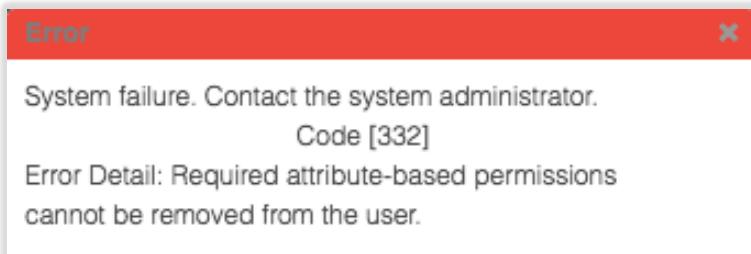
The three attribute-permissions are shown.

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`).

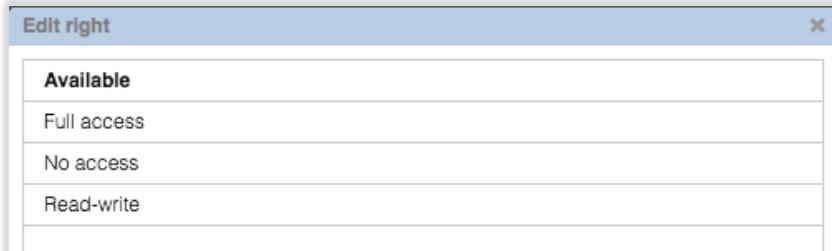
- Click the main **Revoke** (under Actions column, not the greyed-out one) button beside `Default Access`

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.

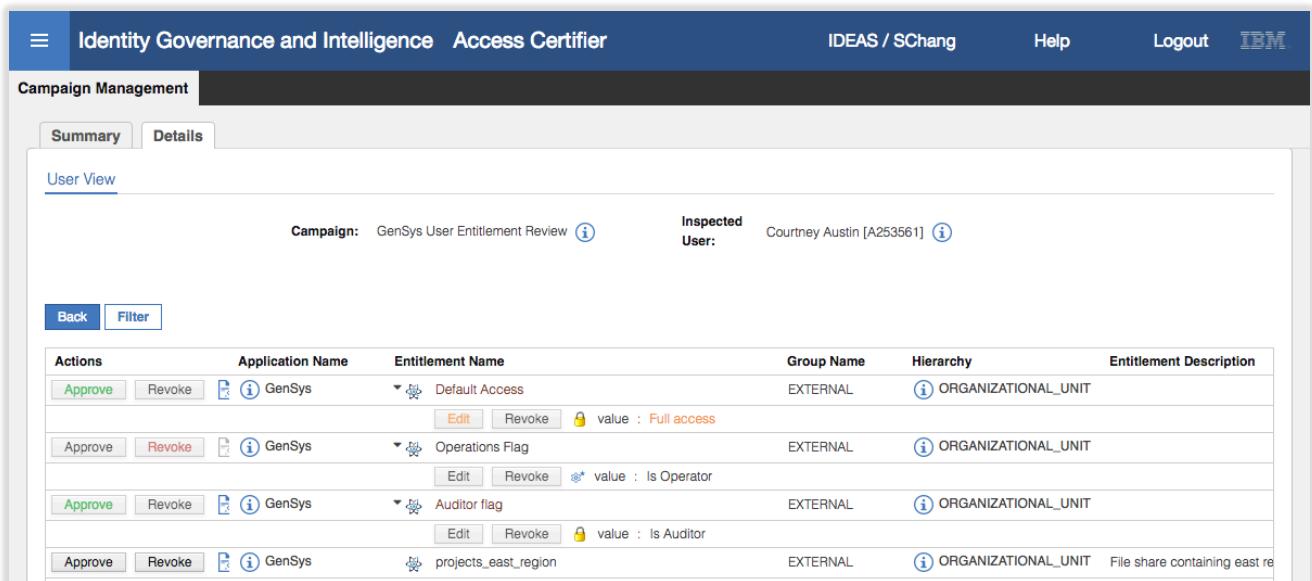
- Click **OK** to close the error dialog
- Expand the Default Access permission again and click the **Edit** button



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.



The screenshot shows the Identity Governance and Intelligence Access Certifier interface. At the top, it says "Identity Governance and Intelligence Access Certifier" and "Campaign Management". Below that, there are tabs for "Summary" and "Details", with "Summary" selected. Under "User View", it shows a campaign named "GenSys User Entitlement Review" and an inspected user "Courtney Austin [A253561]". There are "Back" and "Filter" buttons. A table lists entitlements for the user:

Actions	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description
Approve	GenSys	Default Access	EXTERNAL	ORGANIZATIONAL_UNIT	
Approve	GenSys	Operations Flag	EXTERNAL	ORGANIZATIONAL_UNIT	
Approve	GenSys	Auditor flag	EXTERNAL	ORGANIZATIONAL_UNIT	
Approve	GenSys	projects_east_region	EXTERNAL	ORGANIZATIONAL_UNIT	File share containing east re

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**

The screenshot shows the IGI Access Governance Core interface. At the top, there are tabs for 'Identity Governance and Intelligence' and 'Access Governance Core'. Below the tabs, a navigation bar includes 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. A secondary navigation bar below it includes 'Reports', 'Role Compare', 'Scheduled Tasks', and several event-related tabs: 'TARGET inbound - Account events', 'TARGET inbound - Access events', 'OUT events', 'IN - User events', and 'IN >'. A 'Filter' button is located at the top left of the main content area. The main content displays two tables. The first table lists events with columns: ID, Account ID, Master UID, Operation, Status, ERC Status, Trace, Detail, Marker, Application, and C. The second table lists entitlements with columns: n Code, ATTR1, ATTR2, ATTR3, ATTR4, ATTR5, and Event Date.

ID	Account ID	Master UID	Operation	Status	ERC Status	Trace	Detail	Marker	Application	C
71011	aaustin	A253561	Remove Permission	Success	Error	java.lang.NullPointerException		ILC_4659853777718115728	GenSys	A
71010	aaustin	A253561	Remove Right	Success	Success			ILC_4659853777718115728	GenSys	A
71009	aaustin	A253561	Add Right	Success	Success			ILC_4659853777718115728	GenSys	A
71008	aaustin	A253561	Add Right	Success	Success			ILC_4659853777718115728	GenSys	A

n Code	ATTR1	ATTR2	ATTR3	ATTR4	ATTR5	Event Date
224440901399153_SChang	Operations Flag	string	Operations Flag	1	PERMISSION	31-Jul-2017 03:19:19
321091088189363_SChang	value	Read-only	Default Access	1	PERMISSION	31-Jul-2017 03:19:19
321091088189363_SChang	value	Full access	Default Access	1	PERMISSION	31-Jul-2017 03:19:19
	value	Read-only	Default Access	1	PERMISSION	31-Jul-2017 02:26:19

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

The screenshot shows the IGI Access Governance Core interface with the 'Entitlements' tab selected for a user named Courtney. The left panel shows a list of users with a filter for 'Courtney' and an 'Actions' dropdown. The right panel displays entitlement details, including assigned entitlements like 'Employee', 'Default Access', 'Auditor Flag', and 'projects_east_region', along with their respective application, group name, group code, and hierarchy.

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

VV	Name	Application	Group Name	Group Code	Hierarchy
	Employee	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT	
	Default Access	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT
	Auditor Flag	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT
	projects_east_region	GenSys	EXTERNAL	EXTERNAL	ORGANIZATIONAL_UNIT

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security Access Governance Core. In the left pane, under 'Manage > Accounts', the 'Users' tab is selected. A table lists users with columns: Risk, First Name, Last Name, Master UID, and Org.Unit. One row for 'Courtney' is selected, showing Austin as the Last Name and A253561 as the Master UID. In the right pane, under 'Rights', a table shows account permissions for 'Courtney'. The 'Auditor Flag' permission has a value of 'Is Auditor', and the 'Default Access' permission has a value of 'Full access'.

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 screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security Access Governance Core. In the left pane, under 'Manage > Accounts', the 'Applications' tab is selected. A table lists applications with a column for 'Name'. The 'GenSys LDAP' application is selected. In the right pane, under 'Details', a detailed view of the 'GenSys' application is shown. It includes fields for 'Account ID*', 'First Name', 'Last Name', 'Email', 'Display Name', 'Operations Flag', 'Default Access', and 'Common Name*'. The 'Operations Flag' is set to 'True', and the 'Default Access' is set to 'CONTROL'.

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  
telephononenumber=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:

© 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.