Application Management

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

Entitlement Catalog **1**

Add or Edit Entitlement Parameters 1

Approval Requirement for Changes to Entitlements 2

Deleting a Managed Entitlement 2

Import and Export 2

Standard Properties 3

Members 4

Access 4

Classifications 5

Associated Roles 5

View Entitlement Catalog **6**

Activity Target Categories **7**

Entitlement Catalog

> The terms "account group" and "application object" are use interchangeably in this document but have the same meaning. Some applications can have multiple application objects. An account group can be the name of one of those objects.

Use the Entitlement Catalog page to view and manage all of your managed attributes including entitlements, account groups/application objects and permissions.

Managed attributes can be specific to one application or shared among multiple applications of the same type. Managed attributes can also be defined in multiple languages.

A managed attribute is the value of an account attribute that has been promoted to a first-class object in the IdentityIQ database so the system can track other data related to these attributes, such asa description or an owner. Any attribute can become managed, but the most common attribute to be managed is one holding group memberships.

A managed attribute is indicated by checking the **Managed** box in the account schema on the Application Definition page.

As accounts are aggregated, IdentityIQ detects the values for each managed attribute and promotes these to ManagedAttribute objects. For example if location is managed, and we aggregate three accounts with locations Austin, Dallas, and Houston, there are three ManagedAttribute objects for those values. If the attribute is multi-valued, such as groups or memberOf, IdentityIQ creates one ManagedAttribute for each value in the list.

The expectation is that most of the attributes that are managed are entitlement attributes, which usually means a group attribute. Because of this, the language in the product is oriented around the word entitlement. For example we refer to manage entitlements and the entitlement catalog. It is possible, however, to have managed attributes that are not entitlements, but it is unusual.

Managed attributes that are also groups have additional features. If the connector supports group aggregation, IdentityIQ can import the definitions of those groups and store them in the ManagedAttribute object. Managed attributes for groups have editable tabs that contain the definition of the group that can, optionally, be used for provisioning. If a groups managed attribute is available for provisioning, any change made on the Object Properties tab is sent to a connector to modify the target application.

> The additional Object Properties tab is only available if Lifecycle Manager is installed and the Enable Account Group Management options was selected during Lifecycle Manager configuration. See the Lifecycle Manager documentation for more information.

Add or Edit Entitlement Parameters

> You can only add new managed attributes of type entitlement.

Open the Edit page by clicking **New Entitlement** or clicking on an existing managed attribute from the list.

The Edit page enables you to change properties on a managed attribute. The **Save** button at the bottom of the page launches a business process that persists the changes to the managed attribute. The title and content of this page varies depending on the type of attribute being edited. If necessary, the business process launches provisioning.

Approval Requirement for Changes to Entitlements

Beginning with version 8.2 of IdentityIQ, the default behavior is to *require an approval* when an entitlement is changed. The approval path is managed by the Entitlement Update business process. This business process identifies an **approver**, which by default is the owner of the entitlement. If no owner has been specified for the entitlement, the approval is routed to the **fallback approver**, which by default is the owner of the application that is the source for the entitlement.

If you don't want to require approvals for changes to entitlement, you can edit the business process to disable approvals:

1. Click **Setup > Business Processes**
2. Select the **Entitlement Update** business process.
3. Click the **Process Variables** tab.
4. Edit the **approver** variable to set the **Initial Value** to **String**. Make sure that the **Value** field is blank.
5. **Save** the change. Note that if you re-open the **approver** value to verify your changes, no type of **Initial Value** will show as selected.
6. Edit the **fallbackApprover** variable in the same manner, changing **Initial Value** to **String** and making sure the **Value** field is blank.
7. **Save** your change.

For more information on IdentityIQ business processes, see the IdentityIQ **Business Processes** documentation.

Deleting a Managed Entitlement

Deleting a managed entitlement does not directly remove the entitlement from the product. Instead, a group update business process is launched as a task.

You can track the progress of this task on the **Setup > Tasks > Task Results** tab.

Import and Export

Use the **Import** and **Export** buttons to import new managed attributes from a CSV file or to export existing managed attributes to a CSV file. Each option opens a dialog with instruction on how to continue.

The import and export processes are handled with tasks in IdentityIQ and can be tracked on the Task Results page. See the **Tasks** documentation for more information.

The import data file must be in a CSV format that is defined by comments at the top of the file. A comment line containing a comma-separated set of values defines the properties corresponding to the CSVs on subsequent lines. The imported Entitlements' properties will be set accordingly.

The properties on this line can be any of the following:

- application
- attribute
- value
- displayName

- requestable
- owner
- scope

An example of this type of comment

```
# value, displayName
```

A line containing an assignment statement defines default values for the imported Entitilements' properties.

Here is an example of this type of comment:

```
# application=Active_Directory
```

Import attribute descriptions

For importing attribute descriptions, you must also declare the language used. To get an example of the description format do the following:

There might be a size limit set on the imported entitlement description during the configuration of IdentityIQ. If you run into issues, contact your administrator.

1. Go to the Entitlement Catalog page, **Applications >Entitlement Catalog**.
2. Click **Import**.
3. Choose an file to import.
4. Click **Import**.

A message is displayed at the bottom of the browser window when the import is complete. From there, you can view or save the imported descriptions.

Standard Properties

The Standard Properties tab is common to all managed attributes, regardless of type.

Field	Description
Application	The application associated with the attribute.
Type	Application object type.
Attribute	This field is read-only when editing an existing managed attribute. This field has different behavior based on the selected type: • **Entitlement** - this field is labeled **Attribute**, and the input is a suggest box populated with all attributes in the selected application's account schema. • **Group** - this field is also labeled **Attribute**, but no input choice is provided. The attribute is set to the reference attribute defined in the application's group schema. • **Permission** - this field is labeled **Target** and the input is a free-form text box.

Field	Description
Value	This field is only displayed for groups and entitlements. This field is read-only when editing an existing managed attribute. For groups with provisioning enabled, this field contains information on how the value was derived. The attribute value represented by the managed attribute.
Display Value	This field is only displayed for groups and entitlements. The value used to concisely represent this managed attribute in IdentityIQ. In many cases, this is the same as the value. Sometimes (when the value is an LDAP domain, for instance) this only contains a small, relevant portion of the value. No provisioning is launched when this field is changed.
Requestable	This option is only displayed if you have SailPoint Lifecycle Manager enabled. Indicates whether or not the entitlement can be requested from the Lifecycle Manager.
Elevated Access	When editing an entitlement, select Elevated Access to display when an entitlement has this feature.
Description	A localized description. You must Save the description before changing languages to enter another description. Use the language selector to enter description in multiple languages. The drop-down list displays any languages supported by your instance of IdentityIQ. The description displayed throughout the product is dependent on the language associated with the user's browser. If only one description is entered, that will be the description used by default.
Owner	The owner of the managed attribute. No provisioning is launched when this field is changed.
This tab might contain additional extended attributes that were defined as part of the configuration process. Extended attributes only apply to IdentityIQ's representation of the managed attribute and no provisioning is launched by them.	

Members

This is a read-only tab that lists all of the Identities with detected roles with profiles that match the edited managed attribute. This tab only pertains to Group type managed attributes.

Access

This is a read-only tab that lists any effective access for the entitlement.

Classifications

This tab lists any classifications that have been assigned to the entitlement. Classifications flag and categorize entitlements, most typically to identify entitlements that permit access to sensitive or protected data such as financial, personal, or health-related information. You can also add and remove classifications on this tab.

To add classifications to the entitlement, choose the entitlement(s) from **Assign Classifications to this Entitlement** and click **Add**. You can add as many classifications to the entitlement as you wish.

To remove classifications from the entitlement, check the classifications to remove, then click **Remove Selected**.

For more information, see the **Classifications** documentation.

Associated Roles

The Associated Roles tab is included for any entitlement that is *directly* provisioned by a role. It lists the roles that directly provision the entitlement, showing the **Display Name** and **Description** of the role.

For more information on Associated Roles and how they can help you visualize the relationship between roles and the access they provide, see Understanding Relationships Between Roles and Entitlements/Permissions.

View Entitlement Catalog

From this page you can add new managed attributes and edit the existing manage attributes. You can also use this page to import lists of managed attributes into IdentityIQ or export them back out to other applications.

Column	Description
Application	The application to which the managed attribute belongs.
Attribute	The attribute (in the case of an Entitlement or Group) or target (in the case of a Permission) that the managed attribute represents.
Display Name	Display name of the managed attribute. If no display name was defined, this field displays the value of the attribute. When an application has Elevated Access, the display name will have the Elevated Access icon next to it.
Name	The raw attribute value for the managed attribute. This column is hidden by default.
Type	The type of managed attribute that is shown. There are two types: Entitlement and Permission. However, entitlements can be marked with the boolean group property if they represent a group object type for the application. Since applications can have more than one group object type, the object type name, for example Group or Role, is shown here for those managed attributes.
Description	The description for the locale that is specified in the combination box between the search area and the grid.
Owner	The Identity who owns the managed attribute.
Requestable	Any managed attribute that can be requested has a check icon in this column.
Last Refreshed	The date and time that the managed attribute was last modified. This column is hidden by default.

Activity Target Categories

Use this page to create or edit target categories that point to the activity targets defined on your applications.

A target is a specific object within a data source that is acted upon. For example, a target might be a machine name for a login action, or a file name for a create action.

The targets specified here are used to populate lists on the Activity Search page. These targets can be grouped with targets specified on other applications to create categories of targets. For example, if you have inventory applications at three different locations and a procurement database on each, you can set each procurement database as a target, create a Procurement category, and then collect activity for all three procurement databases using a single activity search.