Application Management

Version: 8.3

Revised: October 2022

Copyright and Trademark Notices

Contents

Aggregation

Aggregation is the process by which data about identities and their access is read from your enterprise systems into IdentityIQ. IdentityIQ aggregates Account data (which includes information about identities and their accounts and entitlements on the outside systems) and Account Group data (which includes account groups and application object types that are the basis for creating entitlements that represent group membership).

IdentityIQ uses configured applications to connect to these enterprise systems, and uses tasks to do the work of reading the data into IdentityIQ and correlating it to identities stored in IdentityIQ

Aggregation and Applications

A configured Application is the component that lets IdentityIQ communicate with an enterprise system. The enterprise system is the source of information about accounts and account groups, which will be read into IdentityIQ.

Applications use a system-specific connector type (such as JDBC, LDAP, Active Directory, Azure, Workday, et cetera) to set up a connection to the system that is the source of the data. The configuration options are flexible; many elements of the configuration depend on the connector type, but they all have several things in common:

- **Connection parameters** – the information IdentityIQ needs in order to communicate with the data source. This typically includes a path to the data source and credentials for logging in/authenticating, but may include more.
- **Account schema** – how IdentityIQ defines and organizes the data that is being read in.
- **Correlation logic** – how IdentityIQ maps data from the source system to what is stored in IdentityIQ.

For more information on configuring applications, see the *IdentityIQ Application Configuration Guide* and the **Connectors & Integrations** section on the SailPoint Product Documentation portal.

What Data Is Aggregated?

Account aggregation is the process through which account data from a configured application is read into IdentityIQ and stored in Link (account) objects connected to Identities. Aggregation is an integral part of every IdentityIQ installation. Account aggregation reads in information about identities, which typically includes:

- **Account information** – the accounts the identity has on the system being aggregated.
- **Entitlements** – the access the identity has on the systems that it has accounts on.
- *From authoritative sources*: information about the identity, such as name, department, email address, et cetera.

Account Group aggregation is used to create entitlements (managedAttributes) representing an application's group objects. See Entitlement Catalog.

Authoritative and Non-Authoritative Data Sources

The enterprise systems that provide information about identities and their access may be numerous, and information about identities may not always be synchronized across all systems. For this reason, some sources of data are designated as **authoritative** sources. An authoritative source is any repository for employee information for your enterprise that represents the primary and most trusted information about identities, such as a human resources application. This is in contrast to **non-authoritative** sources that may contain some accurate information about identities but is not considered the system of record for information about the identity itself.

A simple example is when an employee's name changes – Pat Smith becomes Pat Jones. In this example, Human Resources will change the employee's name, and perhaps the email address, in an authoritative source, such as

Active Directory. The changes then need to be propagated out to other accounts that the user has, such as JIRA, Sales Force, Outlook, etc.

A system is designated as an authoritative source by checking the **Authoritative Application** flag in the application configuration for that source. For more information, see the *IdentityIQ Application Configuration Guide.*

Note that your organization can have multiple authoritative sources.

Delta Aggregation

Delta aggregation is the process of only aggregating accounts or account groups that have changed since the last aggregation.

Delta aggregation can be run as an alternative to a full aggregation, which brings in all accounts or account groups, regardless of whether they are unchanged since the last aggregation.

Using delta aggregation to bring in only the changes can be much faster than full aggregations, and can allow processes to occur at a much more rapid pace.

The option to enable delta aggregation is set in the aggregation task. You can set this option in the tasks for aggregating accounts and for aggregating account groups. However, delta aggregation requires support by the connector; not all connector types support delta aggregation.

For more information on aggregation tasks, see Tasks for Aggregation .

Tasks for Aggregation

Tasks drive the actual work of retrieving info from the data source. There is a task type for aggregating accounts, and a task type for aggregating groups. You use the task type as a template to set up your own specific tasks, and you can have many defined tasks for each type – for example, it typical to have a separate account aggregation task for each one of your source systems.

You can also have more than one aggregation task for a given system - for example, one that runs daily to only pick up changes from that day (Delta Aggregation), and a more thorough one that runs monthly to refresh *all* your data from that specific source.

The aggregation tasks can be configured with options that determine which of the task's available actions are performed in the aggregation.

An **Account aggregation task** is responsible for:

- reading the account data from the designated data source
- creating a Link object to represent the account or updating an existing Link object with any data changes for the account
- associating the accounts (Links) to an existing Identity in the system or creating new Identities to hold the accounts

There are several additional options that an Account aggregation task can be configured to perform, such as:

- deleting any Links for accounts that no longer exist
- recalculating active scopes for the installation when scoping is enabled
- executing some of the Identity Refresh task options

An **Account Group aggregation** task aggregates information about groups. Group aggregation can only be done for applications which have a group schema defined. IdentityIQ aggregates group data from one application at a time, repeating this process for each application specified in the aggregation task (in the “applications” parameter of the task).

Other tasks make updates based on aggregated data, and therefore should be run after aggregation:

- **Identity Refresh**: This task scans all identities to ensure that all identity information is up-to-date and accurate. Identity Refresh scans are also used to detect and report on policy violations, which may arise due to changes in account or group associations.
- **Effective Access Indexing**: Effective Access is any indirect access that was granted through another object, such as a nested group, an unstructured target, or another role. This task indexes effective access so that it can be shown on a single view of an identity.

For more information, see the *IdentityIQ Tasks Guide*.

Correlation

Correlation refers to how IdentityIQ maps data from the source system to authoritative identities stored in IdentityIQ. Correlation logic can be implemented in a variety of ways, including:

- Through direct mapping of attributes – for example, the application's account attribute “mail” is mapped directly to the identity's attribute “email”
- Using conditions that assign application accounts to existing identities by defining attribute conditions. For example, the root account on Unix typically does not have any identifying attributes that can help when trying to correlate it to an existing identity using direct attribute mapping, so you can use a condition, such as whether the identity is a Unix application owner, to drive the correlation
- Through rules – custom BeanShell rules let you create your own specialized logic for correlation.

For more information about correlation, see the *IdentityIQ Application Configuration Guide*, the *IdentityIQ Identity Management Guide*, and the *IdentityIQ Rapid Setup Guide*.

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 as a description or an owner. Any attribute can become managed, but the most common attribute to be managed is one holding group memberships.

What Is Included in the Entitlement Catalog

The Entitlement Catalog lists the managed attributed in your IdentityIQ instance. A managed attribute is indicated by checking the **Managed** box for the attribute, 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 you aggregate three accounts with locations Austin, Dallas, and Houston, there will be 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 "managing 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.

Requestable Attributes

When Lifecycle Manager is enabled, items in the Entitlement Catalog can be flagged as Requestable by checking the **Requestable**option in the item's standard properties. The Entitlement Catalog shows a check icon in this Requestable column for all attributes that can be requested. See Standard Properties.

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.

Add or Edit Entitlement Parameters

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

Open the Edit page by clicking **Add 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.
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

Field	Description
	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.

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.

Elevated Access

IdentityIQ has the capability of protecting sensitive access with the Elevated Access feature. Administrators, application owners, or entitlement owners can classify specific roles or entitlements as having elevated access.

Classifying a role or entitlement as allowing elevated access provides clear visibility to users when they request, certify, or approve the role or entitlement. When a role or an entitlement has elevated access, it is displayed with a badge (a check mark inside a shield icon) to alert the user to the elevated access status. This helps ensure that the item is treated with appropriate care.

A property on these items makes it possible to include them in reports, to facilitate auditing and to help identify high risk areas. Audit activities can focus on this access by leveraging these reports.

You can create workflows to handle elevated access items, by incorporating the "iiqElevatedAccess" property from a role or entitlement

Role Configuration

1. To add the elevated access flag to roles, navigate to **Setup > Roles**. Once at the Role Management screen, find the appropriate role that needs Elevated Access.
2. Scroll to the bottom of the Role Information and click **Edit Role**.
3. Select **Elevated Access**.
4. Click **Submit**.

Entitlement Configuration

1. To add the elevated access flag to entitlements, navigate to **Applications > Entitlement Catalog**. Once at the Entitlement Catalog screen, select the appropriate entitlement.
2. Select **Elevated Access**.
3. Click **Save**.

The following are locations where a user can see or edit elevated access:

- Manage User Access
- Access Reviews
- Targeted Certification: Additional Settings
- Identity Warehouse
- Identity Details
- Entitlement Catalog - Advanced Search
- Role Editor
- Entitlement Details Dialog
- Role Details Dialog
- Work Items

- Role Search Criteria
- Reports
- Match List

Supporting Active Directory Native Move/Rename

In many places in IdentityIQ, the default identifier for Active Directory accounts and groups is Distinguished Name (DN). Some native changes, such as when an account or group is moved within the Active Directory OU or when a person's name changes, result in a change to the DN.

Beginning with version 8.3, IdentityIQ uses the Active Directory GUID, a globally unique identifier, to determine when an account or group object's DN has changed. When a change is detected, the object is updated, and the change is propagated to all DN references throughout IdentityIQ.

When a changed DN is updated on aggregation, IdentityIQ creates an event to propagate the changes to these areas:

For account groups:

- Bundle/Profile
- Policy
- Form
- Rule
- GroupDefinition
- Identity
- Dynamic Scope
- PasswordPolicy/PasswordPolicyHolder
- Widgets

For accounts:

- Form
- Rule
- GroupDefinition
- Identity

If a DN has been updated in response to a native move or rename, the DN is also replaced with the new one in the Provisioning plan at provisioning time, to ensure that there will be no errors on provisioning.

Disabling the Propagation of DN Changes

The propagation behavior is enabled by default. If you want to disable it, to prevent the propagation of changes throughout IdentityIQ, follow these steps.

1. Navigate to **gear icon > Global Settings > IdentityIQ Configuration > Miscellaneous** tab.
2. In the **Native Identity Change Event Propagation Settings** section, uncheck the **Enable Native Identity Change Event** propagation checkbox.
3. **Save** your changes.

Customizing How DN Changes Are Propagated

System administrators can customize the areas where DN changes are propagated by editing the **Native Identity Change Propagation** object in the Debug pages. This object is a **Request Definition** object.

Rename Detection in the Account Aggregation Task

The Account Aggregation task includes an option to **Enable rename detection on managed attributes** This option affects aggregation from Active Directory. It enables IdentityIQ to detect when an account group DN has changed due to being renamed. IdentityIQ determines whether a DN is new or is a rename of an existing DN, by examining the relevant account group's GUID or UUID. Enabling this option can prevent unintended changes to access that is based on assignment rules which use DN as assignment criteria.

Note that when a change is made in Active Directory to an OU which contains accounts or groups (such as renaming or moving it), a delta aggregation does not pick up the changes. This is due to a limitation in Microsoft DirSync Control.To avoid this issue, perform a full aggregation to capture the changes and update the child objects. You might have to do this regularly to ensure the data is up to date.

For more information, see the IdentityIQ **Tasks** documentation.

Handling Duplicate Distinguished Names in Active Directory

During aggregation, if IdentityIQ detects two Active Directory accounts or account groups with the same Distinguished Name but different UUIDs, it will update the UUID to the most recent value, and treat the two accounts or account groups as the same. This handles the case where an account or group is accidentally deleted and re-added. Consequently, it is not advisable to re-use the same DN with a different meaning. IdentityIQ will not detect this as an account or account group change to any attribute but UUID.

Handling Future Actions

If there are future actions that may be impacted by a DN move or rename, such as a sunset date on an entitlement, or a mitigation end date for a policy violation, be cautious about pruning events. Otherwise, if a DN changes for an account included a sunrise/sunset action, IdentityIQ may not perform the provisioning action because it will contain the "old" DN. This is particularly important for dates far in the future.

In policy violation mitigations, if the DN on an account changes during the mitigation period, the next time Check Policy Violations is run, the policy violation can re-appear and need to be mitigated again.