SailPoint IdentityIQ Logical Connector

The following topics are discussed in this document:

Configuration Parameters

This section contains the information that this connector uses to connect and interact with the application. Logical applications do not have connection attributes, by default. If you have defined custom logical connectors there might be connection attributes on this tab.

Use this tab to test your logical application connection.

Schema Attributes

The application schema is used to configure the objects returned from a connector. When a connector is called, the schema is supplied to the methods on the connector interface. This connector currently supports two types of objects, account and group. Account objects are used when building identities Link objects. The group schema is used when building AccountGroup objects which are used to hold entitlements shared across identities.

Logical applications enable you to pull schema attribute information from the tier applications from which it is compiled. When you use this feature the schema attribute information is automatically added to the attributes table and you can edit it as needed.

Click **New Tier Attribute** to display the Select Source Attribute dialog and select the tier application and attribute to pull into the logical application.

Additional Information

This section describes the additional information related to the Logical Connector.

Logical Connector - Tiers Tab

This section contains the information that this connector uses to build the relationships between the tier applications that make up a logical application. For an identity to have an account on a logical application they must have the required, matching accounts on all tier applications. For example an identity, Lori Ferguson, might

be represented by the attribute `dbid` on one tier and `username` on another. You must correlate those attributes, either manually or with a correlation rule, to create accounts on the logical application.

Add Tiers to a Logical Application

You must define the tier applications that are contained within the logical application and identify the application to be used as the primary tier application.

To add a tier application, select the application from the Select an Application drop-down list and click **Add Tier**. Click the arrow to right of the field to display all applications configured to work with IdentityIQ or type the first few letters of an application name to display a list of applications with names containing that letter string. You can add as many applications as required.

Specify the primary tier application by selecting it in the Primary Tier column. The primary tier application is the application containing all of the attributes to which the attributes on the other tiers will correlate. Every account on the logical application must have an account on the primary tier application. In some instances this might be a human resources application containing all of the identities. A logical application can only have one primary tier application.

To remove tier applications, select the application using the selection boxes in the left-most column and click **Remove Selected**.

Correlate Tier Application Attributes

Use the logical application tier attribute mapping, or correlation, panel to either manually map attributes for correlation or assign an existing correlation rule. For an identity to have an account on a logical application they must have the required, matching, accounts on all tier applications. Map the attributes on each application that should have matching values.

To manually map attributes on the tier applications do the following:

1. Select a non-primary tier application in the application list. The selected application is highlighted and any mapped correlation attributes are displayed in the attribute correlation panel.
   If you select the primary tier application a note is displayed stating that no correlation is required on the primary tier.
2. Click **Add Attribute** to display a row in which to add the new attribute.
3. Click on the row to activate either the **Tier Attribute** or **Primary Tier Attribute** field.
4. Select an attribute from the drop-down list in both columns.
5. Click **Save Changes** or continue mapping attributes for the applications.

To use an existing correlation rule, open the Use Correlation Rule panel and select a rule from the **Correlation Rule** drop-down list. The rule should contain all of the attribute mapping required for this logical application.

The Tiers tab contains the following information:

Attribute	Description
Account Rule	Select an existing account rule from the drop-down list. The logical application rule defines the requirements that must be met before an identity is assigned an account on this logical application. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**

Attribute	Description
Provisioning Rule	Select an existing provisioning rule from the drop-down list. The logical provisioning rule defines how provision requests for the logical application account or any of the accounts with which it is comprised are handled. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**
Application	The tier applications that make up the logical application.
Primary Tier	Designate one tier application as the primary tier application. The primary tier application is the application containing all of the attributes to which the attributes on the other tiers will correlate. Every account on the logical application must have an account on the primary tier application. In some instances this might be a human resources application containing all of the identities in IdentityIQ. **Note: A logical application can only have one primary tier application.**
Tier Attribute	Attributes from the selected tier application whose values must match the values of the associated attributes from the primary tier application.
Primary Tier Attribute	Attributes on the primary tier application to which the attribute values from the tier applications must match.
Account Matching	Use account matching to select attributes and permissions from existing application tiers as the parameters for your logical application. This panel contains the following: **Application Items** — Click **Add Attribute** to include application attributes in your account matching parameters. Click **Add Permission** to include application permissions in you account matching parameters. **Operation** — choose the AND / OR operator to include multiple attributes / permissions **Type** — indicates either Attribute or Permission **Application** — indicates the application from which the attribute or permission is being matched **Name** — select an attribute from the drop-down list or input the permission name into the field **Value** — input the value of the attribute or permission **Group/Ungroup/Delete Selected** — use the check box to select line items on which to perform the respective action

Defining Logical Connectors

Use the following procedure to define a logical connector.

1. Define all tier applications.
2. Perform the following tasks on each tiered application:
    a. Run aggregation task.
    b. Run entitlement correlation task.
    c. Scan for missing entitlements or define new managed entitlements.

3. Define the logical application
    a. Define application tiers
    b. Discover schema attributes from selected tier applications for editing.
    c. Scan for missing entitlements using the filters from the selected tiered applications fro editing.
4. Run aggregation task on your newly defined logical application.
5. (*Optional*) Run Account-Group Aggregation task on the newly defined logical application.
   This will update the logical application entitlements to have the configured display value for the respective groups. The tier application information used to update the entitlement is based upon the logical applications configured “Group Attribute” from its Account Schema.

Logical Application Filtering

Logical applications use the **Find missing entitlement** scan on the Managed Entitlements tab as filtering action using the Account Matching criteria provided on the Tiers tab. This gives a more focused starting point instead of using all of the entitlement values from the selected application tiers.

For example, a new logical application uses the “memberOf” attribute in Active Directory. There are likely thousands of values that are assigned in an enterprise. With specific criteria defined in Account Matching, only the values you are interested in appear for easier editing.