Table of Contents

[1 Overview 2](#_Toc1116132)

[2 Simple and Create Policy Mapping Format 2](#_Toc1116133)

[3 Attribute Synchronization Lifecycle Event Priority 3](#_Toc1116134)

[4 Advanced Extended Rule Format 3](#_Toc1116135)

[5 Evaluate Create Provisioning Policy 3](#_Toc1116136)

[6 Rename / Move LDAP Account (DN AND/OR CN Change) 4](#_Toc1116137)

[7 Only Primary Account 4](#_Toc1116138)

[8 Attribute Synchronization Process 4](#_Toc1116139)

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta |  |
| Version 2 | 4/16/18 |  | Cathy Mallet | Minor cleanup edit |

# Overview

The purpose of this document is to explain the technical details of the Attribute Synchronization Feature that is bundled with the Accelerator Pack. This feature is configured via the Self-Service Onboarding Wizard or the IdentityIQ Debug Page.

# Simple and Create Policy Mapping Format

The mapping of Identity Cube attributes to application schema attributes is supported from the Self-Service Onboarding Wizard. Every application can be subscribed to Identity Cube attribute changes. This is done by mapping application schema attribute names to Identity Cube attribute names.

Mappings that are done from the Self-Service Onboarding Wizard can be defined directly in the “**Custom-FrameworkAttributeSyncMapping**” custom artifact. Multiple schema attributes for an application can be mapped to a single Identity Cube attribute.

Here is an example of the identity cube attribute as source and application schema attribute as target format:

<entry key="[Cube Attribute Name]">

<value>

<List>

<String>[Application Name]:[Schema Attribute Name]</String>

<String>[Application Name]:[Schema Attribute Name]</String>

</List>

</value>

</entry>

Here is an example of application create policy as source and application schema attribute as target format:

<entry key="CREATEPOLICY">

<value>

<List>

<String>[Application Name]:[Schema Attribute Name]</String>

<String>[Application Name]:[Schema Attribute Name]</String>

</List>

</value>

</entry>

**Please Note:** String, List, and Boolean source and target attribute types are supported for both formats

# Attribute Synchronization Lifecycle Event Priority

The Joiner, Joiner Rehire, and Leaver Lifecycle Events has priority over Attribute Synchronization . In case an identity is eligible for Joiner or Joiner Rehire or Leaver, Attribute Synchronization Lifecycle Event will not be kicked off. Mover Lifecycle event has priority over Attribute Synchronization Lifecycle Event.

There are before and after mover Attribute Synchronization options on an application.

1. Process Attribute Synchronization Before Mover Certification: See Mover documentation.
2. Process Attribute Synchronization After Rehire: See Joiner documentation.

Also, Attribute Synchronization can be kicked off in parallel at global level with Mover and Joiner Rehire using Global Definitions configuration.

# Advanced Extended Rule Format

This format is not supported from the Self-Service Onboarding Wizard. Every application can define and refer to a rule name to synchronize each Identity Cube attribute change. This is defined in the “**Custom-FrameworkAttributeSyncMapping**” custom artifact. This rule is executed for each application Link object. Here is an example of a rule reference that can be defined in the customer artifact.

<entry key="[Cube Attribute Name]">

<value>

<List>

<String>RULE:[Application Name]:[Rule Name]</String>

<String>RULE:[Application Name]:[Rule Name]</String>

</List>

</value>

</entry>

The following input parameters are passed to these kinds of rules and can be used to build account requests per application. These account requests get merged into the overall attribute synchronization provisioning plan.

These rules must validate and ensure old value from Link Object and new value generated from rule is different.

**Please Note:** String, List, and Boolean source and target attribute types are supported for this format

**Input Parameters:**

|  |  |
| --- | --- |
| Parameter Name | Description |
| identityName | Identity Name Being Processed |
| applicationName | Application Name Being Processed |
| nativeId | Native Id of Account Being Processed |
| secondaryAccount | Link Object “psAccount” value |

**Output:**

List of AccountRequest Objects

# Evaluate Create Provisioning Policy

This option is used to get the source attribute values from the Create provisioning policy defined on an application instead of from the target attribute value from the Identity Cube. When turned on, this option eliminates the need to write separate rules for attribute synchronization, which may have been already defined on the Create provisioning policy of an application. This attribute is of type string with a value of either true or false. This attribute is defined on an application by the “Evaluate Create Provisioning Policy” display name, and an internal name, “evaluateCreateprovpolicy”. This option is only applicable for Simple and Create Policy Mapping Format. Please see [Simple and Create Policy Mapping Format](#Simple and Create Policy Mapping Format). This is **required** to be checked for applications where target mapping is selected as “CREATEPOLICY”.

# Rename / Move LDAP Account (DN AND/OR CN Change)

The attribute is of type string with a value of either true or false. This attribute is defined on an application by the “Rename / Move LDAP Account (DN AND/OR CN Change)” display name, and an internal name, “renameLDAPaccount”. It is used to rename the LDAP “cn” attribute and/or “dn” attribute. The new “cn” and “dn” attribute value is extracted from the Create provisioning policy for native identity defined on an application. When this option is checked, a new account request by the attribute “AC\_NewName” and “AC\_NewParent” is injected into the attribute synchronization provisioning plan.

# Only Primary Account

Any account that is not privileged is considered a primary account. When this option is checked, only the primary account is synchronized with identity attribute changes. If it is not checked, all accounts are synchronized. This option is only applicable for Simple and Create Policy Mapping Format. Please see [Simple and Create Policy Mapping Format](#Simple and Create Policy Mapping Format)

# Notify Operations

By Default, Attribute Synchronization Email is sent out to Operations on provisioning failures only. A Global Definition Configuration "Notify Operations on Attribute Synchronization for an Identity" can be used to send out email to Operations on Attribute Synchronization provisioning action.

In case, there is a requirement to cc Attribute Synchronization email, an extended rule can be used and referenced using Global Definituion configuration “CC Email Rule.

# Attribute Synchronization Process

This process starts with an event which is detected from the “ATTRIBUTE SYNCHRONATION FEATURE” Identity Lifecycle event. It is based on changes in Identity Cube’s old and new attributes. This event kicks off the Attribute Synchronization Workflow.

The same process can be kicked off manually by the “Process Identity Event” Operations QuickLink. This QuickLink is accessible to the “Operations” workgroup.

This workflow builds a provisioning plan based on a list of Identity Cube attributes that are defined in the custom artifact.

* Build Provisioning Plan for **changed** Identity attribute or **cleared** identity attribute
  + For each source attribute, if source is not “CREATEPOLICY”, get the source attribute value from Identity cube
  + For each source attribute, if “Evaluate Create Provisioning Policy” is enabled and source is “CREATEPOLICY”, get the source attribute value from Create Provisioning Policies. Please see [Evaluate Create Provisioning Policy](#Evaluate Create Provisioning Policy)
  + For each source attribute, if “Is Primary Account” is enabled, synchronize the Identity Cube attribute value or provisioning policy value to only the primary account, or else synchronize to all accounts. Please see [Only Primary Account](#Only Primary Account)

Additional Processing performed by the workflow

* Target aggregation on the application that has the “Rename LDAP Account” option enabled

