Table of Contents

[1 Overview 2](#_Toc1123266)

[2 Service Account Identification 2](#_Toc1123267)

[3 Service Cube Naming 2](#_Toc1123268)

[4 Service Cube Creation 3](#_Toc1123269)

[5 Service Account Correlation 3](#_Toc1123270)

[6 Service Account Lock/Disable Identification 4](#_Toc1123271)

[7 Service Account Cube Attributes 4](#_Toc1123272)

[8 Service Account Link Attribute 4](#_Toc1123273)

[9 Service Account Owners 4](#_Toc1123274)

[10 Service Account Cube Access Approval 4](#_Toc1123275)

[11 Service Account Leaver Process 5](#_Toc1123276)

[12 Service Account Certification 5](#_Toc1123277)

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta |  |
| Version 2 | 5/4/18 |  | Cathy Mallet | Minor edit |

# Overview

The purpose of this document is to explain the technical details of the Service Account Feature that is bundled with the Accelerator Pack.

# Service Account Identification

Service Accounts can be identified using the application attribute “**serviceAccountAttrExpression**”. There are two types of String format that are supported for this attribute. One is with String Comparison Operation and another one with Java Regular Expression.

An example of String Format with Operation “**[Schema Attribute Name]#IIQService#[Schema Attribute Value]#IIQService#[Operation]**”. This format is automatically set from the Self-Service Onboarding Wizard.

|  |  |
| --- | --- |
| String Tokens and Separators | Description |
| [Schema Attribute Name] | Application Schema Attribute Name |
| #IIQService# (Token Separator) | Token to Separate Application Schema Attribute Name and Schema Attribute Value |
| [Schema Attribute Value] | Application Schema Attribute Value |
| #IIQService# (Token Separator) | Token to Separate Schema Attribute Value and Operation |
| [Operation] | STARTSWITH  ENDSWITH  CONTAINS  EQUALS |

An example of String Format with Java Regular Expression “**[Schema Attribute Name]#IIQService#[Java Regular Expression]**”.

|  |  |
| --- | --- |
| String Tokens and Separators | Description |
| [Schema Attribute Name] | Application Schema Attribute Name |
| #IIQService# (Token Separator) | Token to Separate Application Schema Attribute Name and Java Regular Expression |
| [Java Regular Expression] | This is executed against the Application Schema Attribute Value obtained from Application Schema Attribute Name on the “Link” Object |

# Service Cube Naming

There are two options that can be configured on an application for cube name generation.

* Service Account Unique Name Attribute: The selected attribute value on Link Object is used for cube name. By default, Service Account Identification attribute value is used for cube name
* Append Application Name To Service Account Cube Name: If enabled, application name will be appended to service cube name

# Service Cube Creation

The “**Rule-Framework-Creation**” Creation Rule creates service Identity Cubes for each service account. The “**Rule-Framework-Creation**” rule must be selected as a creation rule on an application. This rule is automatically set from the Self-Service Onboarding Wizard.

This rule identifies service accounts using “**serviceAccountAttrExpression**” and creates a separate Cube for service accounts with following attributes

* Cube Name: See [Service Cube Naming](#_Service_Cube_Naming)
* First Name: [Application Name (only alpha numeric, special characters are removed)]
* Last Name: [Schema Attribute Name Value from Link]
* Service Cube (Extended Attribute): TRUE
* Correlated (Internal Attribute): True
* CorrelatedOverride (Internal Attribute):True
* Type:Service Account



# Service Account Correlation

The “**Rule-Framework-Correlation**” rule must be selected as a correlation rule on an application. This rule is automatically set from the Self-Service Onboarding Wizard. This rule identifies service accounts using “**serviceAccountAttrExpression**” on an application and correlates them to service account Cubes that are created using ” **Rule-Framework-Creation**” rule. Any unmatched account will end up as an uncorrelated Cube. All the string operation comparisons are case insensitive

**Please Note:** This rule correlates service/non-interactive/shared accounts to service Cubes first and then correlates privileged/secondary/interactive, and regular/primary accounts to authoritative source Cubes. Please see the **Accelerator Pack Aggregation Document** Section **Account Correlation Identification** andsection **Aggregation Data Flow.**

# Service Account Lock/Disable Identification

Please see the **Accelerator Pack Aggregation Document** Section **Account Disable Status Identification and Account Lock Status Identification.**

# Service Account Cube Attributes

Identity ObjectConfig is extended with an extended attribute “**serviceCube**”. This extended attribute and OOTB attribute “**type**” of cube is populated using rule “**Rule-Framework-Creation**”. This rule must be defined or merged with every application that is on boarded in IdentityIQ. This rule is defined automatically during onboarding of authoritative applications via QuickLink Self-Service Onboarding.

# Service Account Link Attribute

Link ObjectConfig is extended with an ”**sAccount**” extended attribute to indicate if an account is a service account or not. This attribute is populated using the global rule “**Rule-FrameWork-SA**”

This rule promotes the resource object attribute “IIQService” value calculated during aggregation to this extended attribute. The resource object attribute is calculated by the customization rule “Rule-Framework-RapidAppOnBoarding-Customization-Rule” defined on every application that is onboarded in IdentityIQ.

# Service Account Owners

Identity ObjectConfig is extended with two attributes to maintain the relationship of service account owners on an Identity Cube

* saccountOwnerone (Required): This attribute holds the Service Account Owner value. This is used for IdentityIQ 7.2 version
  + OR
* administrator: This attribute holds the administrator value. This is used for IdentityIQ 7.3 version

The value of these attributes can be set in three different ways:

* + Using Identity mapping rules for an authoritative source service account repository
  + Create Identity QuickLink
    - This can be used to create a service account Identity Cube and ownership information can be pushed to the service account authoritative source repository.
  + Edit Identity QuickLink
    - This can be used to edit a service account Identity Cube and ownership changes can be pushed to the service account authoritative source repository.

**Please Note:** A push to the repository is conditional and can be done only if the application is configured for provisioning, with provisioning policies and the value of the “authoritativeServiceAccount” attribute on the application is configured to be “true”. This value of the attribute “authoritativeServiceAccount” can be set via the Self-Service Onboarding Wizard.

# Service Account Cube Access Approval

The approval process for service Cubes goes through following sequence

1. Service Account Owner (IdentityIQ 7.2) or Administrator (IdentityIQ 7.3+) Approval, if one of these are not defined, the request is redirected to No Service Account Owner Work Group
2. 1st and 2nd Level Application Business Approvers (If defined)
3. 1st and 2nd Level Entitlement Business Approvers (If defined) - for Entitlements Request or 1st Level Role Approval – Roles Request

# Service Account Leaver Process

On Termination, Service Account Ownership or Administartor Ownership is Reassigned to Manager. If no manager is defined on a Service Cube, account ownership gets reassigned to the **No Manager Found** workgroup. If reassignment to manager is turned OFF, ownership is reassigned to the **No Reassignment** workgroup. The Service Account Owner Reassignment Rule overrides manager reassignment as described above.

Please Note: This is not applicable if Service Account Owner or Administrator is defined as a orkgroup.

# Service Account Certification

For **IdentityIQ 7.2,** a “**Rule-Framework-ServiceCubes-CertificationPreDelegation**” pre-delegation rule must be set on Advanced Certification to reassign the service accounts certification to the service account owner. If owner is not defined on a service Cube, the certification is redirected to the No Service Account Owner Work Group.

The “Service Cubes” Population must be defined on the Advanced Certification to limit the scope of certification to service Cubes. Please see below for population definition and composite filters.

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE GroupDefinition PUBLIC "sailpoint.dtd" "sailpoint.dtd">

<GroupDefinition indexed="true" name="Service Cubes" private="true">

<Description/>

<GroupFilter>

<CompositeFilter operation="AND">

<Filter matchMode="START" operation="LIKE" property="serviceCube" value="TRUE" ignoreCase="true"/>

</CompositeFilter>

</GroupFilter>

<Owner>

<Reference class="sailpoint.object.Identity" name="spadmin"/>

</Owner>

</GroupDefinition>

For **IdentityIQ 7.3+, Targeted Certifications can be used.**