

*IdentityIQ Accelerator Pack Implementation*

Table of Contents

Overview 4

Terminology 4

Application Terminology 4

Role Terminology 5

Entitlement Terminology 6

Accelerator Pack Mappings and Extended Attributes 6

Hibernate Mappings 6

Identity Mappings 13

Accelerator Pack Features 15

Email Feature 15

Triggers Feature 19

Global Feature 23

Operations Feature 29

Aggregation Feature 33

Mine Provisioning Policies Feature 36

Joiner Feature 37

Leaver Feature 41

Mover Feature 43

Manager Certification Allow Exception Feature 45

Certification Feature 46

Native Change Detection Feature 48

Approvals (Accounts and Access) Feature 50

Policy Violation Feature 55

Attribute Synchronization Feature 57

Password Synchronization Feature 59

IdentityIQ Ownership and Access Feature 60

New Account Dependency Entitlements Feature 64

Privileged Account Feature 65

Service Account Feature 66

Create Identity Feature 68

Edit Identity Feature 71

Registration Feature 74

Provisioning Feature 76

Ticket Integration Feature 78

Epic Feature 82

Reports Feature 83

Persona Feature 85

Batch Feature 88

Simplified Logical Applications Feature 89

Auditing Feature 90

Self Service Onboarding Wizard Feature 91

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta | Initial Draft |
| Version 1 | 3/15/18 |  | Dave Smizik | Initial Draft Review |
| Version 2 | 5/14/18 |  | Cathy Mallet | Minor editorial cleanup |

# Overview

At an enterprise level, IdentityIQ will be used as a centralized repository for any access assigned to or removed from person and non-person identities within an organization. The access can be assigned/removed during joiner, mover, and leaver processes and it can be granted manually using request access process. This document will outline the implementation of Accelerator Pack features.

# Terminology

It is important to start any implementation using some standard terms for identity and access management implementation.

## Application Terminology

In IdentityIQ, access is governed and managed by an application construct. Both technology and Infrastructure access is managed by the same construct. Auto assignment of access on applications is done by business roles. Please see Role Terminology for more explanation.

1. **Birthright (Infrastructure/Technology Application) Access:** This access is automated via **Birthright Roles**. Access is assigned automatically based on population (for example, employee population and contractor population). Here are some of the examples for this type of application: Mainframe, Unix, AD, Exchange, Database Servers, RSA, etc. These applications could be SaaS or On-premises applications. This access is related to Infrastructure/Technology Applications.
2. **Birthright Human Resource Business Application Access:** This access is automated via **Birthright Roles.** Access is assigned automatically based on population (for example, employee population). This access is related to mostly HR applications (for example, Payroll, Benefits, Concur, Work Force Time Keeping, Workday, etc.) These applications could be SaaS or On-premises applications.
3. **Automated OR Requested Vertical Business Application Access**: This access can be requested or automated via **Business Roles aka RBAC Roles**. Access can be assigned automatically based on population and Identity Cube profile attributes (for example, Employee Population + Job Title). This access can be requested for Contractor Populations. These applications could be SaaS or On-premises applications. These applications are usually Industry Vertical based applications (for example, finance, banking, security, healthcare applications, etc.) The access of these applications is dependent on **Infrastructure/Technology Application for authorization**.

## Role Terminology

There are two categories of roles that are used within an IdentityIQ Implementation.

1. **Birthright Roles:** Mainly used for Automation of IT/Infrastructure.This is assigned during Joiner (including Rehire) Lifecycle Events. This is usually based on type of population (for example, employee, contractor, students, etc). This access cannot be requested manually. This access gets excluded from certifications, too, as it does not need to be reviewed. This automation can be applied to **Employees as well as Non-Employee Populations**. **In the case of Health Care, this is just at the persona level**. This is usually done at **Phase 1 Implementation of IAM program**.
2. **Business Roles (aka RBAC Roles):** These roles are assigned via the IdentityIQ Role Engine. Assignment is based on population and population attributes (for example, job code, location, etc.). There are two main scenarios where RBAC Roles are used
   1. **Automation of Human Resource/Vertical Business Application Roles)** This is done by putting **matching criteria on the business roles**. That matching criteria is mostly based on HR profile attributes and is automatically assigned based on the HR data. This access can also be requested manually from the shopping cart. This access gets excluded from certifications, too. This is usually done only for **Employee Populations**. This is usually done at **Phase 2 Implementation of IAM program**.
   2. **Abstraction of Roles (RBAC Roles):** This involves bundling of entitlements into IdentityIQ Business roles. In this case, the requestor doesn’t need to know all the entitlements that are required to get access on a business application; this simplifies the shopping cart experience for end-users during access requests. This includes infrastructure access, too. Abstraction of access into Roles, or RBAC, is done as the **IAM program matures** over time.

There are four main differences between birthright roles and business (RBAC) roles

1. Birthright Roles cannot be requested, as compared to Business Roles aka RBAC Roles
2. Once Birthright Roles are defined, assignment of these roles doesn’t change. However, Business Roles aka RBAC Roles assignment can change based on compliance need
3. Birthright Roles are only related to Infrastructure/IT Access, whereas Business Roles are related to the Business Access required for an individual to fulfill their job responsibilities.
4. Role Mining is often used for the creation of Business Roles, but is not used in the creation of Birthright roles.

Within Accelerator Pack, Business Roles can be further classified into two categories at the enterprise level

1. **Business Application Roles**: The scope of this role is confined to **ONLY** one business application and/or Technology or Infrastructure. The Business Role is made up of IT and Permitted Roles. IT/Permitted Roles are made up of application entitlements (groups, authorizations, etc.). This is an organizational role within the Accelerator Pack.
2. **Enterprise Roles:** The scope of this role is across **MULTIPLE** business applications and/or Technology or Infrastructure. The Enterprise Role is made up of multiple Business roles. The Business Role is made up of IT and Permitted Roles. IT/Permitted Roles is made up of application entitlement profiles. This is an organizational role within Accelerator Pack.

**Please Note:** Over time, Business Application Roles get migrated to Enterprise Roles as organizations mature in their RBAC model.

## Entitlement Terminology

1. **Owner:** The Owner of an application may or may not be same as the business approver. The owner certifies access on their applications and is responsible for data quality and cleanup of orphan/terminated accounts
2. **Business Approver:** They are responsible for approving access requests made for their application

# Accelerator Pack Mappings and Extended Attributes

For any IdentityIQ implementation, identity mappings and extended attributes need to be built out and configured to construct applications, entitlements, roles, and Identity Cubes within the system. Accelerator Pack is packaged with certain set of extended attributes for various feature.

## Hibernate Mappings

### Description

Configuring of the IdentityIQ Hibernate mappings is required for any customer implementation of IdentityIQ. These mappings are used to add customer specific extended attributes. Accelerator Pack ships with some pre-built extended attributes that are defined in these mappings. These extended attributes can be removed from the Hibernate mappings, if some specific Accelerator Pack features are not required.

### Accelerator Pack Configuration

There are no configurations required on Hibernate mappings. However, there may be some instances where some of the advanced Accelerator Pack features are not required during Phase 1 implementation. In this case, these mappings can be configured to remove undesired extended attributes for those features.

### Application Extended Attributes

The following Hibernate mappings, required for Accelerator Pack, are made on the ApplicationExtended.hbm.xml.

|  |  |
| --- | --- |
| Feature Name | Extended Attribute Name |
| Aggregation, Certification, Cart Access Request, Leaver, Reporting Feature | busApp  This attribute is used to categorize IdentityIQ applications and makes a clear distinction between business and infrastructure/technology types of applications. As a result of the categorization, during an access request of Business Roles, the business application approval scheme gets a preference over infrastructure/technology applications. Also, during certification, if an application is a business application, all the access on the application gets included by default during the certification campaign. During termination, the Business Application leaver scheme for business roles wins over IT/Infrastructure Applications |
| Leaver, Reporting Feature | terminationProcess  This attribute is used for termination options that are displayed during application onboarding and the selected option gets executed during a termination life cycle event |
| Leaver, Reporting Feature | loaProcess  This attribute is used for leave of absence options that are displayed during application onboarding and the selected option gets executed during a leave of absence life cycle event |
| Leaver, Reporting Feature | ltdProcess  This attribute is used for long term disability options that are displayed during application onboarding and the selected option gets executed during a long term disability life cycle event |
| Mover, Reporting Feature | moverProcess  This attribute is used for mover options that are displayed during application onboarding and the selected option gets executed during a mover life cycle event |
| Native Change, Reporting Feature | nativeChangeProcess  This attribute is used for mover options that are displayed during application onboarding and the selected option gets executed during a native change life cycle event |
| Cart Access Request, Reporting, Leaver Feature | appBusApprovers  This attribute on applications is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |
| Cart Access Request, Reporting, Leaver Feature | additionalAppBusApprovers  This attribute on applications is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |
| Joiner, Reporting Feature | joinerEnabled  This attribute is used during application onboarding to categorize an application as a birthright application. During the joiner lifecycle event, applications that are joiner enabled will result in a new account for the joiner |
| Joiner, Reporting Feature | rehireProcess  This attribute is used for rehire options that are displayed during application onboarding and the selected option gets executed during a rehire life cycle event |
| Joiner, Reporting Feature | rtwloaProcess  This attribute is used for return to work from leave of absence options that are displayed during application onboarding and the selected option gets executed during a return to work leave of absence life cycle event |
| Joiner, Reporting Feature | rtwltdProcess  This attribute is used for return to work from long term disability options that are displayed during application onboarding and the selected option gets executed during a return to work long term disability life cycle event |
| Joiner, Reporting Feature | reverseleaverProcess  This attribute is used for reverse leaver options that are displayed during application onboarding and the selected option gets executed during a reverse leaver life cycle event |
| Cart Access Request, Reporting, Policy Violation Feature | softPolicyviolations  This attribute is used to categorize policy violations for an application that can allow a requestor to submit a request. These violations are executed during a cart access request for preventive checks |
| Cart Access Request, Reporting, Policy Violation Feature | hardPolicyviolations  This attribute is used to categorize policy violations for an application that cannot allow a requestor to submit a request. These violations are executed during a cart access request for preventive checks |
| Privileged Account, Reporting Feature | enablepswexpNotification  This attribute is used to enable password change notification for privileged accounts on the application |
| Privileged Account, Reporting Feature | afterPassExpProcess  This attribute is used for password expiration options that are displayed during application onboarding for privileged accounts. This option is executed when a password is not reset in time. The time frame is defined by the application for the privileged accounts during application onboarding |

### ManagedAttribute Extended Attributes

The following Hibernate mappings, required for Accelerator Pack, are made on the ManagedAttributeExtended.hbm.xml

|  |  |
| --- | --- |
| Cart Access Request, Reporting, Leaver Feature | entBusApprovers  This attribute on entitlements is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |
| Cart Access Request, Reporting, Leaver Feature | additionalEntBusApprovers  This attribute on entitlements is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |
| Logical Applications, Certifications, Cart Access Request, Reporting Feature | entAppName  This is used to tag entitlements as logical applications. In the case of Infrastructure/Technology type applications, entitlements that are not tagged with this attribute are excluded from the certification campaign. Also, this attribute is shown during an access request. |
| Privileged Account, Cart Access Request, Aggregation, Reporting Feature | entPrivileged  This attribute is used to tag entitlements as privileged. Only Privileged entitlements can be assigned to Privileged Accounts. Tagging of entitlements as privileged is either done via the Aggregation Feature or can be done manually using the Entitlement catalog |
| Joiner, Certifications, Access Request, Aggregation, Reporting Feature | isBirthright  This attribute is used to mark entitlements as birthright. These entitlements will be excluded from certification campaign. Also, these entitlements will not show up on access request screens |
| Aggregation, Reporting Feature | manualOverride  This attribute is used to manually override marking entitlements privileged, birthright, and not requestable (Only for Infrastructure/Technology entitlements that are not tied to Logical or Business Applications) during aggregation. This is done via the Entitlement Catalog |

### Bundle Extended Attributes

The following Hibernate mappings, required for Accelerator Pack, are made on the BundleExtended.hbm.xml and the CertificationExtended.hbm.xml.

|  |  |
| --- | --- |
| Joiner, Certifications, Access Request, Reporting Feature | isBirthright  This attribute is used to mark roles as birthright. These roles will be excluded from the certification campaign. Also, these roles will not show up on the access request screens |
| Privileged Account, Cart Access Request, Reporting Feature | rolePrivileged  This attribute is used to tag roles as privileged. Only Privileged roles can be assigned to Privileged Accounts. Tagging of roles as privileged is done manually using the Role Administrative Page |
| Logical Applications, Certifications, Cart Access Request, Reporting Feature | appName  This is used to tag roles as logical applications. In the case of Infrastructure/Technology type applications, roles that are not tagged with this attribute are excluded from the certification campaign. Also, this attribute is shown during the access request. |
| Cart Access Request Feature, Leaver, Reporting Feature | roleBusApprovers  This attribute on applications is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |
| Cart Access Request Feature, Leaver, Reporting Feature | additionalRoleBusApprovers  This attribute on applications is used for the access request approval scheme. Also, during a termination life cycle event, ownership gets reassigned to the owner’s manager |

### Link and Certification Extended Attributes

The following Hibernate mappings, required for Accelerator Pack, are made on the LinkExtended.hbm.xml and the CertificationExtended.hbm.xml.

|  |  |
| --- | --- |
| Aggregation, Reporting Feature | disabledAccount  Marks Applications accounts as disabled. No, Aggregation Identification is required, if the connector is smart enough to identify disabled accounts on its own.  This attribute provides disable account status search functionality on many pages of IdentityIQ |
| Aggregation, Reporting Feature | lockedAccount  Marks Applications accounts as locked. No Aggregation Identification is required, if the connector is smart enough to identify locked accounts on its own.  This attribute provides lock account status search functionality on many pages of IdentityIQ |
| Aggregation, Reporting Feature | sAccount  Marks Applications accounts as service accounts.  This attribute provides service account search functionality on many pages of IdentityIQ |
| Privileged Account, Aggregation, Password, Mover, Joiner, Attribute Sync, Reporting Feature | psAccount  Marks application accounts as privileged or secondary accounts. It is done via the Aggregation Feature or can be done manually via the Edit Link on the Application Accounts Page.  The Mover, Joiner, Attribute Sync, and Password Features uses this attribute to perform operations either on primary accounts or all accounts.  The Privileged Account Feature uses this for assigning privileged access to privileged accounts. It uses this attribute to identify privileged accounts and send out password expiration notifications |
| Privileged Account | apAccounttype  The Privileged Account Feature uses this for validations on access request where privileged access account type on either roles or entitlements matches privileged account type |

### Identity Extended Attributes

The following Hibernate mappings, required for Accelerator Pack, are made on the IdentityExtended.hbm.xml.

|  |  |
| --- | --- |
| Create, Edit, Registration Feature | middleName  This attribute is used on the create, edit, and registration form |
| Create, Edit Feature | ctrexpDt  This attribute is used for lifecycle events on Contractor Expiration Date |
| Create, Edit Feature | ctrMgr  This attribute is used for lifecycle event notifications to Contractor Manager |
| Service Account, Leaver Feature | saccountOwnerone  This attribute is used for service account ownership. Ownership is reassigned to the owner’s manager on termination. This ownership can be overridden by an extended rule |
| Service Account, Create, Aggregation, Reporting Feature | serviceCube  This attribute is used to mark cubes as service cubes. This can be done on the Create Form or it can be done via the Aggregation Feature |
| Persona, Joiner, Mover, Leaver, Create, Edit, Reporting Feature | relationships  This attribute is used to maintain cube persona relationships from multiple authoritative sources. Also, it can be populated on the Create Form and modified on the Edit Form |
| Persona, Certification, Reporting Feature | mgrrelationships  This attribute is used to maintain cube personas and their manager relationships from multiple authoritative sources. It is helpful during a certification campaign where a primary manager can delegate or reassign certification item to other managers using this as a reference or index. |
| Joiner Feature | needsJoiner  This attribute is used for implicit joiner events. |

### As Built Configuration

Please describe all the hibernate changes that are applied for the [Customer] that is not Accelerator Pack specific>

|  |  |
| --- | --- |
| Hibernate File Name | Hibernate File Changes |
|  |  |

## Identity Mappings

### Description

This is required for setting up Identity Cube enterprise wide attributes within IdentityIQ. These cube attributes are populated via values originating in authoritative sources. This may require a BeanShell coding skill set to configure cube mapping logic.

The Joiner Lifecycle Event is pre-configured with the Accelerator Pack. There are two AND conditions for the joiner workflow to be kicked off.

1. Condition One: A “needsJoiner” extended attribute is used to ensure that the Joiner Lifecycle Event is processed only once. This is used as an implicit Joiner Lifecycle Event. Before the Joiner event, the value of this attribute is “NEEDS PROCESSING”, and once the event is processed, the value of this attribute is set to “JOINER PROCESSED”.
   1. The creation rule “**Rule-FrameWork-Creation-Joiner-Authoritative-Source**” is automatically set on all authoritative source applications. This rule is automatically saved either during “**Configure Triggers**” or onboarding of authoritative source applications “**Self Service Onboarding Wizard**”. This rule sets the value of a “needsJoiner” extended attribute to ”NEEDS PROCESSING” for all new Identity Cubes. Also, this rule sets Identity Cube Type to Contractor, Employee, or Service Account if application, marks it as authoritative and the follow attributes are enabled on the application
      1. authoritativeEmployee
      2. authoritativeNonEmployee
      3. authoritativeServiceAccount
2. Condition Two: The Identity Cube must not be part of the population “New Joiner Has At Least One Birthright Account

### Accelerator Pack Configuration

There are two attributes that need to be configured on the “Identity Mappings” page for Persona Feature.

1. For the Persona Feature, the Multi-valued attribute “relationships” is required to handle personas in IdentityIQ. This attribute is set using the “**Rule-IdentityAttribute-Relationships**” rule. Persona relationships comes from multiple authoritative sources. This rule must be configured as a global rule using the Identity Mappings page.
2. For the Persona Feature, the Multi-valued attribute “mgrrelationships” is required for handling managers from different personas in IdentityIQ. This attribute is set using the “**Rule-Framework-IdentityAttribute-Manager-Global-Index**” rule. Manager Persona relationships comes from multiple authoritative sources. This rule must be configured as a global rule using the Identity Mappings page. Configure following rules

|  |  |  |
| --- | --- | --- |
| Extended Attribute Name | Identity Mapping Rules | Description |
| relationships | Global Rule: Rule-IdentityAttribute-Relationships | This is used for the Persona Feature |
| mgrrelationships | Global Rule: Rule-Framework-IdentityAttribute-Manager-Global-Index | This is used for the Persona Feature |

### Built In Functionality

The creation rule “**Rule-FrameWork-Creation-Joiner-Authoritative-Source**” is packaged with the Accelerator Pack. An additional creation logic must be done using Additional Accelerator Pack Creation Rule

|  |  |  |
| --- | --- | --- |
| Extended Attribute Name | Authoritative Application Creation Rule | Description |
| needsJoiner | Creation Rule: Rule-IdentityAttribute-Relationships | This is used for the Joiner Feature |

### As Built Configuration

<Please describe all the configuration and implementation changes that are applied to Identity Mappings for the [Customer] that are not Accelerator Pack specific>

Please describe all the configuration and implementation changes that are applied to the Authoritative Application Creation Rule for the [Customer] that are not Accelerator Pack specific>

# Accelerator Pack Features

The overall goal of this program is to onboard applications into IdentityIQ and **enforce enterprise wide standard policies and procedures** from access and account management perspective. IdentityIQ is extended to implement Accelerator Pack Features. There are certain steps that are required for configuring every feature for Accelerator Pack implementation, which are listed below.

## Email Feature

### Description

This is required for any customer implementation. Mostly it requires applying HTML header, footer, and Style Sheets so that emails sent from IdentityIQ have the same look and feel as other emails sent by the organization.

### Accelerator Pack Configuration

* Server Root Path must be defined using OOTB Mail Settings
* There are four files that needs to be configured for all Accelerator Pack Email Notifications

|  |  |
| --- | --- |
| File Name and Object Name | Description |
| EmailTemplate-FrameworkHeader(Required) | HTML Header defined in this file will be applied to all IdentityIQ Email Templates |
| EmailTemplate-FrameworkFooter(Required) | HTML Footer defined in this file will be applied to all IdentityIQ Email Templates |
| EmailTemplate-FrameworkStyleSheet (Required) | HTML Style Sheet defined in this file will be applied to all IdentityIQ Email Templates |
| Custom-Framework-EmailTextMapping (Optional) | Additional Email Instructions can be defined in a custom Artifact. It starts with Request Type, Template Name, Application Name, Operation and finally new instructions. Here is an example from the configuration of the Cart Request Completion Email Template  Application name can be authoritative or non-authoritative. **All application attributes and provisioning plan attributes can be defined with velocity syntax in the Custom-Framework-EmailTextMapping artifact.**  Operation can be AccountRequest Operation or constant “none”. This constant is used for authoritative applications   * CART REQUEST FEATURE (Request Type) * EmailTemplate-FrameworkRequestCompletion (Template Name * IdentityIQ (Application Name) * Create (Account Operation) or “None” * Please Follow Registration Instructions (Additional Cart Request Completion Instructions) |

* This feature needs to be configured to identify “from” address for an email template. This is configured via the “Global Definition” QuickLink for the field “Email Notifications Verification” on the QuickLink form. This field is a list of Authoritative Sources that helps Accelerator Pack to identify Human Populations for Email Notifications from IdentityIQ. The configuration that is done via QuickLink is saved in a “**Custom-Framework-Common-Settings**” custom artifact

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| authSourceAppName | Comma separated authoritative source names | Empty |

* This feature can be configured to override Joiner/Rehire Email and Leaver/Reverse Leaver Email from Manager to Work Group . This is configured using the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| wgJoinerRehireEmail | WorkGroup to recieve Joiner and Rehire Email | Empty |
| wgLeaverReverseLeaverEmail | WorkGroup to receive Leaver and Reverse Leaver Email | Empty |

* Manager Notificationsfor LifeCycle Events Joiner, Rehire, Reverse Leaver, and Leaver can be cce’d to any workgroup using Global Definition “CC Email To Workgroup” configuration. In case, there is a requirement to cc email to different workgroups as per population, an extended rule “CC Email Rule” can be used.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| apCCEmailWorkgroup | Email to Workgroup is applied to Lifecycle Events Joiner, Rehire, Reverse Leaver, and Leaver | Empty |
| apCCEmailRule | This option gets precedence over above option. This rule output (Comma separated email addresses) is used. CC Email Rule is applied to Lifecycle Events Joiner, Rehire, Reverse Leaver, Leaver, LOA, LTD, Joiner LOA, Joiner LTD, Epic/SER, Attribute Synchronization, and Mitigation Expiration | Empty |

* Email References for request submission, completion, auto rejection, rejection, batch completion. This is configured via the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |  |
| --- | --- | --- | --- |
| Property Name | Description | Default Settings | |
| RequestSubmission | Request Submission Email | EmailTemplate-FrameworkRequestSubmission |
| RequestCompletion | Request Completion Email | EmailTemplate-FrameworkRequestCompletion |
| BatchCompletion | Batch Completion Email | EmailTemplate-FrameworkBatchCompletion |
| AutoRejection | Auto Rejection Email | EmailTemplate-FrameworkAutoRejection |
| Rejection | Request Rejection Email | EmailTemplate-FrameworkRejection |
| PSAPasswordExpiration | Privileged Account Expiration Notifications | EmailTemplate-FrameworkPSAPasswordExpiration |

### As Built Configuration

* <Please describe all the configuration changes that are applied to the following objects for the [Customer]>

|  |  |
| --- | --- |
| File Name and Object Name | Description |
| EmailTemplate-FrameworkHeader |  |
| EmailTemplate-FrameworkFooter |  |
| EmailTemplate-FrameworkStyleSheet |  |
| Custom-Framework-EmailTextMapping |  |

* <Please list all the configuration changes that are applied to the “**Custom-Framework-Common-Settings**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Triggers Feature

### Description

This is required for setting up life cycle events for automated provisioning workflows (e.g. Joiner, Leaver, Mover, etc.). These events are triggered based on changes on Identity Attributes coming from Authoritative Sources.

### Accelerator Pack Configuration

The “**Configure Triggers**” QuickLink is used to set up Life Cycle Events. These triggers can be configured based on an extended attribute changes (either in string or date format) and/or population aka GroupDefinition.

The Joiner Lifecycle event is pre-configured based on an internal extended attribute called “**needsJoiner**” and the “**New Joiner Has Atleast One Birthright Account**” population. These two triggers are configured using AND conditions.

### Built In Functionality

A packaged QuickLink Workflow that has a User Interface to add/remove triggers for following workflows

* Joiner Workflow
* Joiner Rehire Workflow
* Joiner Return to Work from LOA (Leave of Absence) Workflow
* Joiner Return to Work from LTD (Long Term Disability) Workflow
* Joiner Reverse Leaver Workflow
* Leaver Termination Workflow
* Leaver LOA (Leave of Absence) Workflow
* Leaver LTD (Long Term Disability) Workflow
* Mover Workflow

By default, all lifecycle events are enabled to be configured in a custom artifact called “Custom-Triggers-User-Interface-Form”.

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Lifecycle Event Key | Lifecycle Event Name | Disabled |
| Custom-Triggers-User-Interface-Form | joinerProcess | JOINER FEATURE | false |
| Custom-Triggers-User-Interface-Form | rehireProcess | JOINER REHIRE FEATURE | false |
| Custom-Triggers-User-Interface-Form | reverseleaverProcess | REVERSE LEAVER FEATURE | false |
| Custom-Triggers-User-Interface-Form | rtwltdProcess | JOINER LTD FEATURE | false |
| Custom-Triggers-User-Interface-Form | rtwloaProcess | JOINER LOA FEATURE | false |
| Custom-Triggers-User-Interface-Form | moverProcess | MOVER FEATURE | false |
| Custom-Triggers-User-Interface-Form | terminationProcess | LEAVER FEATURE | false |
| Custom-Triggers-User-Interface-Form | loaProcess | LEAVER LOA FEATURE | false |
| Custom-Triggers-User-Interface-Form | ltdProcess | LEAVER LTD FEATURE | false |

By default, the Joiner Lifecycle Event is pre-configured with two implicit events. These implicitly must not be removed, and a customer specific joiner trigger can be added as an additional trigger to existing implicit triggers.

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Trigger Name | Triggers Definition | Operation Between Triggers |
| Custom-Triggers | JOINER FEATURE | * Trigger ONE   + Attribute: GROUPDEFINITION   + New Value: Group Definition: New Joiner Has Atleast One Birthright Account   + Old Value: IGNORE * Trigger TWO   + Attribute: needsJoiner   + New Value: NEEDS PROCESSING   + Old Value: IGNORE | AND |

### As Built Configuration

<Please describe all the configuration changes that are applied to the following objects for the [Customer]>

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Lifecycle Event Key | Lifecycle Event Name | Disabled |
| Custom-Triggers-User-Interface-Form | joinerProcess | JOINER FEATURE | <> |
| Custom-Triggers-User-Interface-Form | rehireProcess | JOINER REHIRE FEATURE | <> |
| Custom-Triggers-User-Interface-Form | reverseleaverProcess | REVERSE LEAVER FEATURE | <> |
| Custom-Triggers-User-Interface-Form | rtwltdProcess | JOINER LTD FEATURE | <> |
| Custom-Triggers-User-Interface-Form | rtwloaProcess | JOINER LOA FEATURE | <> |
| Custom-Triggers-User-Interface-Form | moverProcess | MOVER FEATURE | <> |
| Custom-Triggers-User-Interface-Form | terminationProcess | LEAVER FEATURE | <> |
| Custom-Triggers-User-Interface-Form | loaProcess | LEAVER LOA FEATURE | <> |
| Custom-Triggers-User-Interface-Form | ltdProcess | LEAVER LTD FEATURE | <> |

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Trigger Name | Triggers Definition | Operation Between Triggers |
| Custom-Triggers | JOINER FEATURE | * Trigger ONE   + Attribute: GROUPDEFINITION   + New Value: Group Definition: New Joiner Has Atleast One Birthright Account   + Old Value: IGNORE * Trigger TWO   + Attribute: needsJoiner   + New Value: NEEDS PROCESSING   + Old Value: IGNORE * <Additional Trigger> | AND |
| Custom-Triggers | <> | <> | <> |

## Global Feature

### Description

This feature is required for applying Accelerator Pack “Global Definition” QuickLink for all features and applications within IdentityIQ.

### Accelerator Pack Configuration

A “**Global Definition**” QuickLink can be used to set up various Feature options. The workgroup “Business Analyst” members need to be configured to have access to this QuickLink.

### Built In Functionality

Here is the list of things that are packaged with this feature

* Global Definition QuickLink
  + Operations Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see [Operations Feature](#Operations Feature)
    - Error Email Notifications Work Group: Default is “**Operations**” Workgroup
    - Staging Workgroup for Lifecycle Events: Default is “**Operations**” Workgroup
    - Workgroup to bypass batch approvals: Default is “**Operations**” Workgroup
    - Email References. Please see [Operations Feature](#Operations Feature)
  + Termination Reassignments Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see [IdentityIQ Ownership and Access Feature](#IdentityIQ Ownership and Access Feature)
    - By default, Artifacts Reassignment to Manager
      * If no manager is defined on a cube, artifacts are reassigned to the **No Manager Found** workgroup. If reassignment to manager is turned OFF, artifacts are reassigned to the **No Reassignment** workgroup.
      * The Artifacts Reassignment Rule overrides the manager reassignment
    - By default, Business Approvers Reassignment to Manager
      * In case no manager is defined on a cube, business approvers get reassigned to **No Manager Found** workgroup. In case reassignment to manager is turned OFF, business approvers ownership is reassigned to **No Reassignment** workgroup.
      * Business Approvers Reassignment Rule overrides manager reassignment
  + Existing Workflow References
    - Object Name Custom-Framework-Common-Settings where default settings are stored
    - By default, Wait Time for Lifecycle Event Workflows is 60 seconds
    - By default, Existing Workflow for Interactive Access Request is empty
    - By default, Existing Workflow for Interactive Account Request is empty
    - By default, Existing Workflow for Batch Access Request is empty
    - By default, Existing Workflow for Batch Account Request is empty
  + Email Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored
    - By default, Separate Joiner Email for Password is ON. Please see the [Joiner Feature](#Joiner Feature)
    - List of Authoritative Sources to Identify Human Population for Email Notifications from IdentityIQ: This needs to be configured. Please see [Email Feature](#Email Feature)
    - Override Joiner and Rehire Email from Manager to WorkGroup
    - Override Leaver and Reverse Leaver Email from Manager to WorkGroup
    - Email References. Please see [Email Feature](#Email Feature)
  + Approval Access and Accounts Request Feature
    - Object Name Custom-ApprovalFrameWorkMappings where default settings are stored. Please see the [Approvals (Accounts and Access) Feature](#Approvals (Accounts and Access) Feature)
    - By default, Split of Requests at various approvals levels is OFF
    - Notification Scheme for all access and account request approvals. Here are the default options:
      * Total Number of Hours Before First Reminder: 24 Hours
      * Total Number of Reminders Before First Escalation: 3 Reminders
      * Reminder Frequency: 24 Hours
      * Auto Rejection of Approval Item: 168 Hours
      * Notification Scheme: Both Reminders and Escalations
      * Approval Notifications: Send Notifications
      * Escalation Options: No Reassignment Send an Email to Owner's Manager and cc the Owner
    - Enable Electronic Signature
      * Default is OFF
    - Email References. Please see the [Approvals (Accounts and Access) Feature](#Approvals (Accounts and Access) Feature)
  + Service Accounts Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see [Service Account Feature](#Service Account Feature)
    - By default, Account Ownership Reassignment to Manager
      * If no manager is defined on a service cube, account ownership gets reassigned to the **No Manager Found** workgroup. If reassignment to the manager is turned OFF, ownership is reassigned to the **No Reassignment** workgroup.
      * Service Account Owner Reassignment Rule overrides manager reassignment
  + Snapshot Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| requestSnapshot | List of entry points within Accelerator Pack that is configured to take an Identity Snapshot before workflow plan execution. This is executed within Accelerator Pack Workflows where requestType is any of the items from the list | * LEAVER FEATURE * IMMEDIATE TERMINATION FEATURE |

* + Certification Feature
    - Object Names Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess, Custom-Mover-Settings, and Custom-Native-Change-Settings where default settings are stored
    - Exclude Privileged Access from Certifications. Please see [Certification Feature](#Certification Feature)
      * By default, it is OFF
    - Native Change Certification Staging. Please see the [Native Change Detection Feature](#Native Change Detection Feature)
      * By default, it is ON
    - Native Change Redirect To Security Group. Please see the [Native Change Detection Feature](#Native Change Detection Feature)
      * By default, it is OFF
    - Native Change Include Privileged Access Only. Please see the [Native Change Detection Feature](#Native Change Detection Feature)
      * By default, it is OFF
    - Mover Certification Staging. Please see the [Mover Feature](#Mover Feature)
      * By default, it is ON
    - Include Only Privileged Access. Please see the [Certification Feature](#Certification Feature)
      * Group Membership Certification
      * Entitlement Owner Certification
      * Application Owner Certification
    - Post Mover and Mitigation Workflow Extension Rule
    - Email References. Please see the [Manager Certification Allow Exception Feature](#Manager Certification Allow Exception Feature)
    - Exclude Simple Logical Applications for Mover and Manager Certification. Please see the [Certification Feature](#Certification Feature)
  + Policy Violations Feature
    - Object Name Custom-PolicyViolation-AllowDenyExceptions where default settings are stored. Please see the [Policy Violation Feature](#Policy Violation Feature)
      * Add/Remove Multiple Applications Soft Policy Violations
      * Add/Remove Multiple Applications Hard Policy Violations
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see the [Policy Violation Feature](#Policy Violation Feature)
      * Turn ON/OFF Preventive Policy Violations
  + Ticket Integration Feature
    - Object Name Custom-Ticket-Settings where default settings are stored. Please see the [Ticket Integration Feature](#Ticket Integration Feature)
    - Default Polling Time: 720 Minutes or 1 day
    - Default Maximum Checks: 3
    - Default Optimistic Provisioning: True
  + Provisioning Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see the [Provisioning Feature](#Provisioning Feature)
    - Retries and Intervals for all application provisioning
    - Default Retry Wait Time: 720 Minutes or 1 day
    - Default Number of Retries: 3
    - Target Aggregation
    - Post Wrapper Workflow Extension Rule
    - Wrapper Interceptor Plan Rule
    - Wrapper Interceptor Project Rule
  + Leaver Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see the [Leaver Feature](#Leaver Feature)
    - Post LOA, LTD, and Leaver Workflow Extension Rule
    - Email References. Please see the [Leaver Feature](#Leaver Feature)
  + Attribute Synchronization Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see the [Attribute Synchronization Feature](#_Attribute_Synchronization_Feature)
    - Post Attribute Synchronization Workflows Extension Rule
  + Joiner Feature
    - Object Name Custom-Framework-Common-Settings where default settings are stored. Please see the [Joiner Feature](#Joiner Feature)
    - Extension Rehire Rule Before Plan Creation
    - Post Joiner, Rehire, RTW LOA, RTW LTD, Reverse Leaver Workflows Extension Rule
    - Email References. Please see the [Joiner Feature](#Joiner Feature)
  + Persona Feature
    - Object Name Custom-Persona-Settings where default settings are stored. Please see the [Persona Feature](#Persona Feature)
    - By Default, Persona Triggers are OFF
    - Add/Remove Relationships to be ignored for Mover Certification
  + Epic Feature
    - Define Epic and SER Application Name and ID attributes
    - Object Name Custom-Epic-SER-Settings where default settings are stored. Please see the [Epic Feature](#Epic Feature)
  + Password Feature
    - Object Name Custom-Identity-Verification-Form-Settings where default settings are stored. Please see the [Password Synchronization Feature](#Password Synchronization Feature)
    - Add/Remove Identity Verification Attributes
  + Create Identity Feature
    - Object Name Custom-ApprovalFrameWorkMappings and Custom-Framework-Common-Settings where default settings are stored. Please see the [Create Identity Feature](#Create Identity Feature)
    - Create Service Cube Accounts ON/OFF
      * By default, it is ON
    - Manager Approval for Contractors/ Service Account Cube Owner Approval ON/OFF
      * By default, manager approval is required
    - Workgroup Approval Name
      * By default, it is empty
  + Edit Identity Feature
    - Object Name Custom-ApprovalFrameWorkMappings and Custom-Framework-Common-Settings where default settings are stored. Please see the [Edit Identity Feature](#Edit Identity Feature)
    - Edit Service Cube Accounts ON/OFF
      * By default, it is ON
    - Manager Approval for Contractor / Service Account Cube Owner Approval ON/OFF
      * By default, manager approval is required
    - Workgroup Approval Name
      * By default, it is empty
  + Register Identity Feature
    - Object Name Custom-ApprovalFrameWorkMappings where default settings are stored. Please see the [Registration Feature](#Registration Feature)
    - Manager Approval for Contractors ON/OFF
      * By default, manager approval is required
    - Workgroup Approval Name
      * By default, it is empty
  + Self Service Onboarding Wizard Feature
    - Object Name Custom-SmartServices-SelfService-Form-Settings where default settings are stored. Please see the [Self Service Onboarding Wizard Feature](#Self Service Onboarding Wizard Feature)
    - Hide/Show Feature Forms
    - Add/Remove list of connector class names that **supports** and doesn’t require Aggregation Feature Disable/Lock definitions
    - Add/Remove list of connector class names that requires Provisioning Definition for Lock/Unlock/Enable/Disable/Password

### As Built Configuration

<Please list all the configuration changes that are applied to the “**Custom-Framework-Common-Settings**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Operations Feature

### Description

This feature offers tools for performing operational activities within IdentityIQ. Examples include restoring access, launching lifecycle events, and immediate termination. Three QuickLinks will be accessible to this feature. It is scoped to only the “Operations” Workgroup

* Terminate Identity Access
* Recover Identity Access
* Process Identity Event

### Accelerator Pack Configuration

Here is the list of configuration items

* An error notification workgroup can be configured via the “Global Definition” QuickLink. This workgroup receives an error notification when there is any error during the execution of Accelerator Pack Workflows/Rules. The configuration that is done via QuickLink is saved in a custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| errorNotificationWorkGroup | Error Notification Group | Operations |

* All Accelerator Pack Lifecycle Events can be staged for workgroup approvals via the “Global Definition” QuickLink. This workgroup receives approval notifications and approval work items during the execution of Accelerator Pack Lifecycle Event Workflows. The configuration that is done via QuickLink is saved in a custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| temporaryApprovalsWorkGroup | Staged Lifecycle Event WorkGroup | Operations |

* Need to configure group email on Operations Workgroup
* Need to configure group email on No Manager Found Workgroup. This workgroup is used by the following features, if a **manager is not found on** the **cube**
  + Leaver
  + Approval
  + Mover Certification
  + Native Change
  + Ticket Integration
  + Cart Request Manager Approval
  + Service Cube Ownership
  + IdentityIQ Artifacts Ownership
  + Cart Request Business Approvers
  + Email Notifications
* Need to configure group email on No Service Account Owner Workgroup. This workgroup is used by the following features, if the **primary and secondary service account owners are not found on** the **cube**
  + Service Account Owner Certification
  + Access/Account Approvals for Service Account Cube
* Email References are configured via the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| OperationsAttributeSync | Operational Attribute Synchronization Email | EmailTemplate-FrameworkOperationsAttributeSync |
| apSendEmailToOperations | Send Email To Operations on all Attribute Synchronization Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsSER | Operational Epic/SER Email | EmailTemplate-FrameworkOperationsSER |
| apSendEmailToOperationsEpicSER | Send Email To Operations on all Epic/SER Linking Unlinking Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsRTWLOA | Operational Return To Work Leave of Absence Email | EmailTemplate-FrameworkOperationsRTWLOA |
| apSendEmailToOperationsRLOA | Send Email To Operations on all RTW LOA Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsRTWLTD | Operational Return To Work Long Term Disability Email | EmailTemplate-FrameworkOperationsRTWLTD |
| apSendEmailToOperationsRLTD | Send Email To Operations on all RTW LTD Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsLOA | Operational Leave of Absence Email | EmailTemplate-FrameworkOperationsLOA |
| apSendEmailToOperationsLOA | Send Email To Operations on all LOA Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsLTD | Operational Long-Term Disability Email | EmailTemplate-FrameworkOperationsLTD |
| apSendEmailToOperationsLTD | Send Email To Operations on all LTD Provisioning Actions. Otherwise, only error emails are sent out | OFF |
| OperationsNativeChange | Operational Native Change Email | EmailTemplate-FrameworkOperationsNativeChange |
| apSendEmailToOperationsNC | Send Email To Operations on all Native Change Provisioning Actions. Otherwise, only error emails are sent out | OFF |

### Built In Functionality

List of things that are packaged with this feature:

* Terminate Identity Access QuickLink: This is used, from the UI, for immediate termination of the identity
* Recover Identity Access QuickLink: This is used, from the UI, to recover access of an identity that has been removed by mistake
* Process Identity Event QuickLink. This is used, from the UI, to process the below Lifecycle Events manually
  + Joiner Feature
    - New Joiner
    - Rehire
    - Reverse Leaver
    - Return to Work LOA
    - Return to Work LTD
  + Leaver Feature
    - LOA
    - LTD
  + EPIC/SER
    - Linking
    - Unlinking
  + Native Change Feature
    - Redirect To Security Group, instead of Manager
    - Include Privileged Access Only
  + Mover Feature
    - Certification
    - Automation Allow Exception
  + Attribute Sync Feature
* Error Email Notifications To Operations Team on All Provisioning Failures
* The Batch Request Administrator capability is assigned to the Operations Work Group or workgroup defined using Global Definition . This capability bypasses the approval scheme for access and account requests.

### As Built Configuration

* Please fill in the group email settings on the workgroups for the [Customer]

|  |  |
| --- | --- |
| Work Group Name | Group Email Settings |
| Operations | <> |
| No Manager Found | <> |

* <Please list all the configuration changes that are applied to the the “**Custom-Framework-Common-Settings**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Aggregation Feature

### Description

This feature first requires an implementer to follow the IdentityIQ connector guide to connect to an application using service account credentials, and to set up application schema attributes. Once the application is created in IdentityIQ, it will show up on the **Self Service Onboarding Wizard**.

### Accelerator Pack Configuration

The main goal behind the aggregation feature is to classify data during aggregation. Once an application is connected it can be configured using the **Self Service Onboarding Wizard** QuickLink or the **IdentityIQ Administrative Application Wizard** for Aggregation Feature. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being on boarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

This feature performs data classification and data validation functions. For data classification, **Java Regular Expressions** are supported using the IdentityIQ Application Administrative Wizard, and simple **String Operations** are supported using the Self Service Onboarding Wizard.

Mappings or configuration done via the Self Service Onboarding Wizard saves the aggregation rules on the application implicitly. Mappings or configuration done via the IdentityIQ Administrative Application Wizard requires aggregation rules to be selected and saved on the application explicitly.

This feature is applied to both authoritative and non-authoritative applications.

Here is the list of primary functions that are performed by the Aggregation Feature:

* Classifies or categorizes Applications as either Business or Infrastructure/Technology.
* Classifies or categorizes the authoritative application as employee, contractors or service account repository
* Classifies regular accounts, service accounts, and privileged accounts found on the application during aggregation. It is used to define disable and lock status of an account on the application, in case the **connector does not set disable/lock statusof accounts implicitly**. The “**Rule-Framework-RapidAppOnBoarding-Customization-Rule**” rule is saved on the application during data classification.
* Correlates regular, privileged accounts to regular cubes and service accounts to service cubes. If the correlation logic requires OR condition on regular accounts, the application must be configured using the **IdentityIQ Correlation Tab** onthe **Application Page**. This can be done from the IdentityIQ Administrative Page. The “**Rule-FrameWork-Correlation**” rule is saved on the application during data classification. This rule uses Correlation Configuration and Java Regular Expression/String Operations if defined on the application
* Classifies Birthright Entitlements. If the Joiner Feature enabled, these entitlements will not show up on the access request “Add Access” and Certification screens. The “**Rule-FrameWork-Promote-Managed-Attribute**” rule is saved on the application during data classification. For direct group or entitlement aggregations, the “**Rule-FrameWork-Group-Refresh**” rule must be used as a Group Refresh Rule on Aggregation of groups or entitlements. This can be done from the **IdentityIQ Administration Task Page**.
* Classifies Privileged Entitlements. If the Privileged Account Feature enabled, these entitlements will not show under the “Manage Access” QuickLink; instead they will appear under the “Manage Privileged Access” Quicklink. The “**Rule-Framework-Promote-Managed-Attribute**” rule is saved on the application during data classification. For direct group or entitlements aggregations, the “**Rule-FrameWork-Group-Refresh**” rule must be used as a Group Refresh Rule on Aggregation of groups or entitlements. This can be done from the **IdentityIQ Administration Task Page**
* If the Logical Application Feature is enabled, the “**Rule-FrameWork-Group-Refresh**” rule and the “**Rule-FrameWork-Promote-Managed-Attribute**” rule categorize Infrastructure/Technology Application Entitlements and make them non-requestable, if there is no association of entitlements with the Logical Application
* If the Service Account Feature is enabled, the “**Rule-FrameWork-Creation**” rule is saved on the application during Self Service Application Onboarding. It creates service accounts as cubes in IdentityIQ with the naming convention <Application Name (Only Alphanumeric Characters)>+<Service Account Identifier Attribute Value>
* Marking Entitlements not requestable, birthright, and privileged can be manually overridden via the Entitlement Catalog “**Manual Override**” functionality. This is useful only when birthright, privileged and business application are identified using the **Self Service Onboarding Wizard** orthe **Application Administrative Page** andthe operations team would want to override the identification manually
* As an alternative to the Aggregation Feature for birthright and privileged entitlements automation via expressions, the IdentityIQ Entitlement Catalog and Role Administrative Pagescan be used
  + To configure privileged entitlements/roles
  + To configure birthright entitlements/roles
* Validates Flat File Connector Data. It performs two functions. The “**Rule-FrameWork-Preiterate-DelimitedFile**” rule is saved on application during Self Service Onboarding of flat file applications. Here is the list of functions that are performed by this rule:
  + Validates Required Schema Attributes
    - Application Schema attributes must be marked as **required** to validate the required header fields. This needs to be done from the **IdentityIQ Debug Page**
  + Converts Index key to upper case in case merge is required and the file is not sorted
    - This merges the flat file data properly, otherwise the last record wins and results in inaccurate aggregated data.
* Configure “Email Notification Template” “**EmailTemplate-Framework-TaskStatus**” on all aggregation tasks
* Classification of Employee Repository for Authoritative Applications
  + Rule-FrameWork-Creation-Joiner-Authoritative-Source sets User Type to Employee during authoritative contractor application
* Classification of Service Account Repository for Authoritative Applications
  + Provisioning of Contractors to the authoritative source using the Create Identity Form
  + Provisioning of Service Accounts to the authoritative source using the Create Identity Form
  + Rule-FrameWork-Creation-Joiner-Authoritative-Source sets User Type to Contractor during authoritative contractor application
* Classification of Contractor Repository for Authoritative Applications
  + Provisioning of Contractors to the authoritative source using the Edit Identity Form
  + Provisioning of Service Accounts to the authoritative source using the Edit Identity Form
  + Rule-FrameWork-Creation sets User Type to Service Account during authoritative service account application
* Set list of aggregation definition connectors. Please see

[Self Service Onboarding Wizard Feature](#Self Service Onboarding Wizard Feature)

### Built In Functionality

All the rules defined below are packaged with the Accelerator Pack Aggregation Feature

* Creation Rule
* Correlation Rule
* Customization Rule
* Group Refresh Rule
* Promote Managed Attribute Rule
* Delimited File Pre-Iterate Rule

### As Built Configuration

<Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>

## Mine Provisioning Policies Feature

### Description

Provisioning policies are required to create and modify accounts on the application. Sometimes, start date, end date, password change date, and comments are required during account modifications on the target system. Mining of provisioning policies allows for a head start in the creation of provisioning polices for applications.

Aggregation on a given application must be completed successfully before this feature can be used to build a provisioning policy for that application. This feature creates provisioning policies based on a single baseline account on an application. It compares identity data and account data and generates provisioning policies.

### Accelerator Pack Configuration

Mine Provisioning Policies is accessed by using the “**Mine Provisioning Policies**” QuickLink. Any unmined fields and additional attributes that are required to be populated for Disable, Enable, Change Password, Unlock, Delete Provisioning Policies must be created using the **IdentityIQ Administrative Application Wizard**. Sometimes this may require some **implementation effort**. This can be done via Java or BeanShell coding.

An Agent-based Connector (for example, Active Directory) may require **PowerShell scripts coding**.

### Built In Functionality

All the rules defined below are generated dynamically with the Accelerator Pack Mine Provisioning Policies Feature, and are part of the overall provisioning policy that is created using the feature.

* Provisioning Policy Rules are auto-generated per application
  + Start Date
  + End Date
  + Comment with IdentityIQ Request Id
  + Password Change Date
  + Random Password Generator
  + Mined Schema Fields
* The Mine Provisioning Policies QuickLink is packaged with this feature

### As Built Configuration

<Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>

## Joiner Feature

### Description

This is required for creating infrastructure/technology accounts (for example,Active Directory and Exchange) when a new identity joins the organization and is found in one of the authoritative sources.

### Accelerator Pack Configuration

Once the application is connected, aggregated, and provisioning polices mined, this feature can be configured using the **Self Service Onboarding Wizard** QuickLink or the **IdentityIQ Administrative Application Wizard**. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

**IdentityIQ Role and Advanced Analytics Administration Pages** can be used to create Joiner populations and Joiner Birthright Roles. This is not required for the Joiner Feature. If there are no Joiner Birthright Roles and Joiner Populations, every new joiner gets a new Infrastructure/Technology account.

* If required, Joiner Birthright Roles must be configured using the Role Administration Page
  + They must be of role type “**Birthright Roles**”
  + They must be configured with the extended attribute “**isBirthright**” value as “True”
  + All the entitlements of the Birthright Role must be configured with the extended attribute “**isBirthright**” value as “TRUE”
  + They must have an **assignment rule set up as a population.** This population must match the identity population defined on the application. This ensures that every population gets its own birthright role (for example, the employee population gets an employee birthright role and the contractor population gets a contractor birthright role)
* If required, Joiner populations must be configured using the Advanced Analytics Page
  + Multiple Joiner Populations can be configured for an application
* If required, application provisioning policy field data can be added to the joiner email templates via the Debug page. This needs to be done on the custom artifact “**Custom-Framework-EmailTextMapping**”. Joiner Email Instructions can be added via the **Self Service Onboarding Wizard QuickLink** for an application

|  |  |  |
| --- | --- | --- |
| Email Template Name | Description | Default Settings |
| Default - EmailTemplate-FrameworkJoinerManager (JOINER FEATURE) | Email for Account on Joiner | Empty  This is defined per application |
| Default - EmailTemplate-FrameworkPasswordJoinerManager(JOINER FEATURE) | Email for Password on Joiner | Empty  This is defined per application |
| Default - EmailTemplate-FrameworkJoinerManager(JOINER REHIRE FEATURE) | Email for Account on Joiner | Empty  This is defined per application |
| Deafult - EmailTemplate-FrameworkPasswordJoinerManager(JOINER REHIRE FEATURE) | Email for Password on Joiner | Empty  This is defined per application |

* If required, Additional Password Email to manager needs to be configured via the **“Global Definition” QuickLink.** This is a recommended approach for email notifications on Joiner. The changes are saved in a custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| additionalPasswordEmail | Separate Email for Password on Joiner | TRUE |

* Email References are configured via the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| JoinerManager | Joiner /Rehire Email | EmailTemplate-FrameworkJoinerManager |
| PasswordJoinerManager | Joiner/Rehire Password Email | EmailTemplate-FrameworkPasswordJoinerManager |
| ReverseLeaver | Reverse Leaver Email | EmailTemplate-FrameworkReverseLeaver |

### Accelerator Pack Implementation

If the requirements for return to work leave of absence, return to work long term disability, rehire, reverse leaver are not met via drop down options, an **Extended Rule** can be implemented for each task per application. The Extended rule option is not provided on the Self Service Onboarding Wizard. Therefore, this configuration can be done only from the IdentityIQ Application Administrative Wizard. The name of the rule must be applied to the fields “**Rehire Extended Rule**” , “**Reverse Termination Extended Rule**”, “**Return To Work From** **Leave Of Absence Extended Rule**”, and “**Return To Work From** **Long Term Disability Extended Rule**”.

The “**Extended Rule**” option must be selected for the fields “**Rehire Options**”, “**Reverse Leaver Options**”, “**Return To Work From** **Long Term Disability Options**”, and “**Return To Work From** **Leave of Absence Options**”.

If required within Joiner Feature Workflows, the post workflow rules can be implemented for exceptional use cases. The names/references of these rules are stored in a custom artifact “**Custom-Framework-Common-Settings**”.

The name/reference of these rules is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| rehireBeforePlanRule | This is used within Rehire Workflow before plan execution | Empty |
| postRehireRule | This is used within Rehire Workflow after plan execution | Empty |
| postJoinerRule | This is used within Joiner Workflow after plan execution | Empty |
| postRTWLOARule | This is used within RTW LOA Workflow after plan execution | Empty |
| postRTWLTDRule | This is used within RTW LTD Workflow after plan execution | Empty |
| postReverseLeaverRule | This is used within Reverse Leaver Workflow after plan execution | Empty |

### Built In Functionality

Here is the list of things that are packaged with the Joiner Feature

* Joiner Workflow
* Rehire Workflow
* Reverse Leaver Workflow
* Return to Work Leave of Absence Workflow
* Return to Work Long Term Disability Workflow
* Email Templates

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list all the configuration changes that are applied to the object “**Custom-Framework-EmailTextMapping**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* Please list all the rule implementation details for the [Customer]

## Leaver Feature

### Description

This is required for removing all access of a terminated identity. This is triggered by an Authoritative Source Termination Lifecycle event or Immediate Termination or when all relationships/personas are dropped (In case of Person Feature).

Accelerator Pack offers a QuickLink for Immediate Termination: “Terminate Identity Access”. This Quicklink workflow and leaver lifecycle event workflow uses the same leaver feature setting options that are configured on an application.

### Accelerator Pack Configuration

Once an application is connected, aggregated, and provisioning polices are mined, this feature is ready to be used via the **Self Service Onboarding Wizard QuickLink. This feature can be configured by** **the** **IdentityIQ Administrative Application Wizard.** The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

If there are some exceptions in terms of removing all access, the **“Remove Entitlement Exceptions**” option can be configured to handle such a use case. Java Regular Expressions can be used to exclude some access that matches the expression. It can be defined via the IdentityIQ Application Administrative Wizard. A Simple String Operation expression can be defined using the Self-Service Onboarding Wizard for exclusion.

### Accelerator Pack Implementation

If the requirements for leaver, leave of absence, or long-term disability are not met via drop down options, an **Extended Rule** can be implemented for each task per application. The Extended rule option is not provided on the Self-Service Onboarding Wizard. Therefore, this configuration can be done only from the IdentityIQ Application Administrative Wizard. The name of the rule must be applied to the fields “**Termination Extended Rule**”, “**Long Term Disability Extended Rule**”, “**Leave Of Absence Extended Rule**” and the “**Extended Rule**” option must be selected for fields “**Termination Options**”, “**Long Term Disability Options**”, and “**Termination Options**”.

If required within Leaver Feature Workflows, the post workflow rules can be implemented for exceptional use cases. The names/references of these rules are stored in a custom artifact “**Custom-Framework-Common-Settings**”.

* The name/reference of these rules is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postLeaverRule | This is used within Leaver Workflow after plan execution | Empty |
| postLOARule | This is used within LOA Workflow after plan execution | Empty |
| postLTDRule | This is used within LTD Workflow after plan execution | Empty |

* Email References for request submission, completion, auto rejection, rejection, batch completion. This is configured via the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| LeaverManager | Leaver Email | EmailTemplate-FrameworkLeaverManager |
| LeaverManagerOwnershipRemoval | Leaver Reassignment Email | EmailTemplate-FrameworkLeaverManagerOwnershipRemoval |

### Built In Functionality

Here is the list of things that are packaged with Leaver Feature

* Leaver Workflow
* Leave of Absence Workflow
* Long Term Disability Workflow
* Terminate Identity QuickLink
  + Same behavior as Leaver Workflow
* Email Templates
  + Leaver Email Template
  + Reassignment Email Templates
    - IdentityIQ Artifacts Reassignment Email Template
    - Business Approvers Reassignment Email Template
    - Service Account Ownership Reassignment Email Template
* Service Account Ownership, Business Approvers, and IdentityIQ Artifacts Ownership Reassignment To Manager

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* Please list all the rule implementation details for the [Customer]
* Please list all the configuration changes that are applied to the the “**Custom-Framework-Common-Settings**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Mover Feature

### Description

This is required for certifying access of an Identity that has moved within an organization or, in the of Persona Feature, when one of the personas has been dropped from the Identity.

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard** QuickLink or the **IdentityIQ Administrative Application Wizard**. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* **Please see the** **Mover Design Document**
* Use the Entitlement Catalog to configure display name and description
* Use the Entitlement Catalog to configure birthright access, if the aggregation feature cannot identify birthright access
* Use the Entitlement Catalog to configure privileged access if the aggregation feature cannot identify privileged access
* Use the Entitlement Catalog to configure logical application
* Use the Role Administration to configure birthright, privileged access, and logical application
* Staging of mover certifications can be configured using the “**Global Definition**” QuickLink. This configuration is saved within a custom artifact “**Custom-** **Custom-Mover-Settings**”. Please see the table below for default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| stagingEnabled | Mover Certifications Staging | True |

### Accelerator Pack Implementation

If the **before mover** requirements are not met via drop down options, an **Extended Rule** can be implemented per application. The Extended rule option is not provided on the Self Service Onboarding Wizard. The name of the rule must be applied to the field “**Before Mover Extended Rule**” and the “**Extended Rule**” option must be selected for “**Before Mover Certification Options**”.

If required within Mover Workflow, a post mover rule can be implemented for exceptional use cases. The name/reference of this rule is stored in a custom artifact “**Custom-Framework-Common-Settings**”.

The name/reference of this rule is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postMoverRule | This is used within Mover Workflow after plan execution | Empty |

### Built In Functionality

Here is the of things that are packaged with the Mover Feature. Packaged Certification Campaign:

* Before Certification Move Account Rule
  + Move Account in LDAP Before Mover Campaign
* Supports Multiple Accounts for Account Move Before Mover Campaign

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-Mover-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* Please list all the rule implementation details for the [Customer]

## Manager Certification Allow Exception Feature

### Description

This feature is used to automate revocation of access that has been approved by the manager with some time limit on it during certification (in other words, when the manager performs the “Allow Exception” action on a certification item during **mover certification**).

### Accelerator Pack Configuration

The **“Automated Account Mitigation Options**” option of the Mover feature can be configured using the **Self Service Onboarding Wizard** **QuickLink or** the **IdentityIQ Administrative Application Wizard.** This is applied to accounts that have no access and are being extended or kept by managers for some time during an Identity move. Depending upon what option has been selected, the account can either be disabled or deleted.

The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

### Accelerator Pack Implementation

If required within Mitigation Workflow, a post mitigation rule can be implemented for exceptional use cases. The name/reference of this rule is stored in a custom artifact “**Custom-Framework-Common-Settings**”.

The name/reference of this rule is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postMitigationRule | This is used within Mitigation Workflow after plan execution | Empty |

* Email References for request submission, completion, auto rejection, rejection, batch completion. This is configured via the “Global Definition” QuickLink . These configurations are saved in a “**Custom-Framework-Common-Settings**” custom artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| MitigationExpiration | Allow Exception Automation Email | EmailTemplate-FrameworkMitigationExpiration |

### Built In Functionality

There is an allow exception automated revocation Lifecycle Event named “MANAGER CERTIFICATION ALLOW EXCEPTION FEATURE” and a workflow is tied to this event.

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* Please list all the configuration changes that are applied to the the “**Custom-Framework-Common-Settings**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Certification Feature

### Description

This is required for certifying access of an Identity using the following types of certifications

* Manager
* Account Group Membership
* Mover Certification
* Entitlement Owner
* Application Owner

### Accelerator Pack Configuration

This feature can be configured using the **“Global Definition” QuickLink**.

* Exclusion of Privileged Access (Only for Manager and Mover Certifications)
* Exclusion of Simplified Logical applications (Only for Manager and Mover Certifications)
* ONLY privileged access for Account Group Membership , Entitlement Owner, and Application Owner certification
  + These configurations are saved within a custom artifact “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**”. Please see the table below for default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| LogicalBusinessApps | List of Logical Applications that needs to be excluded for Mover Certification | Empty |
| excludePrivilegedAccess | Exclude Privileged Access Mover Certification | FALSE |
| excludePrivilegedAccessRegularCert | Exclude Privileged Access Manager Certification | FALSE |
| includeOnlyPrivilegedAccessAccountGroupMemCert | Include Only Privileged Access Account Group Membership Certification | FALSE |
| includeOnlyPrivilegedAccessEntitlementOwnerCert | Include Only Privileged Access Entitlement Owner Certification | FALSE |
| includeOnlyPrivilegedAccessApplicationOwnerCert | Include Only Privileged Access Entitlement Owner Certification | FALSE |

### Built In Functionality

Here is the list of things that are packaged with the Mover Feature Packaged Certification Campaign

* Manager/Mover Exclusion Rule
  + Exclude Birthright and Automated RBAC access
  + Exclude Privileged Access (Optional)
  + Exclude IT/Technology Application Access with no Logical Application Association
  + Exclude Extended Attribute Logical Applications
* Account Group Membership Exclusion Rule
  + Include Extended Attribute Logical Applications
* Entitlement Owner Exclusion Rule
  + Include Extended Attribute Logical Applications
* Advance Certifications for Service Accounts
  + Pre-Delegation Rule
  + Population for Service Cubes
* System Configuration Rule
  + Populate Logical Application (Business Application Name) Column on Certification
  + Populate Privileged Access Column on Certification
* Certification Email Templates
* Additional Recipient Rule to cc Manager on Escalation

### As Built Configuration

Please list all the configuration changes that are applied to the object “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**” object for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Native Change Detection Feature

### Description

This is used to remove/add access that is not being assigned or unassigned within IdentityIQ.

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard** QuickLink or **IdentityIQ Administrative Application Wizard**. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* Redirect Native Change Certification To Security Group using the “**Global Definition**” QuickLink. This configuration is saved within a custom artifact “**Custom-Native-Change-Settings**”. Please see the table below for default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| securityGroupName | Security Officer Group Name | Empty |

* Staging of native change certifications can be configured using the “**Global Definition**” QuickLink. This configuration is saved within a custom artifact “**Custom-Native-Change-Settings**”. Please see the table below for default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| stagingEnabled | Native Change Certifications Staging | False |

* Include Only Privileged Access for Native Change Certification can be configured using the “**Global Definition**” QuickLink. This configuration is saved within a custom artifact “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**”. Please see the table below for default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| includeOnlyPrivilegedAccessNativeChangeCert | Include Only Privileged Access | False |

### Accelerator Pack Implementation

If required within Native Change Workflow, a post native change rule can be implemented for exceptional use cases. The name/reference of this rule is stored in a custom artifact “**Custom-Framework-Common-Settings**”.

The name/reference of this rule is saved using the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postNativeChangeRule | This is used within Native Change Workflow after plan execution | Empty |

### Built In Functionality

Here is the list of things that are packaged with Native Change Detection Feature, Packaged Native Change Certification Campaign.

* Exclusion Rule
  + Exclude Existing Access that is controlled by IdentityIQ
* Native Change Email Templates
* Additional Recipient Rule to cc Manager on Escalation

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-Native-Change-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list all the configuration changes that are applied to the object “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Approvals (Accounts and Access) Feature

### Description

This is required for any access that is assigned and unassigned to/from an Identity within IdentityIQ.

### Accelerator Pack Configuration

This feature needs to be configured for application level approvals using the **Self Service Onboarding Wizard QuickLink**.

Application, entitlement, and role level approval can be configured **using** the **IdentityIQ Administrative Application Wizard, Entitlement Catalog, and Role Administration Pages.**

The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* Approvers can be comma separated Workgroups or Identity Cubes. Only workgroups can be selected as approvers at the application level from the Self Service Onboarding Wizard.
  + Manage Access Request and Manage Privileged Access Approvals
    - Maximum 5 Level (Regular Cubes) , Maximum 6 Level (Service Cubes) and Minimum 1 Level Approval. Maximum levels can be extended using extension rules
      * Initial Manager Level Approval for Contractor Cube
      * If a manager is not defined, the request is redirected to the “No Manager Found” Work Group
    - Initial Service Account Owner Level Approvals for Service Account Cube
      * Owner/Administrator
      * If owners are not defined, the request is redirected to the “No Service Account Owner” Work Group
    - 1st and 2nd Application Approval Level
    - 1st and 2nd Entitlement Approval Level or 1st and 2nd Level Role Approval Level
  + Manage Account Approvals
    - Minimum 1 Level Approval
      * Regular or Privileged Accounts
    - Minimum 1 and Maximum 2 Level Approval level for Service Accounts
      * Maximum Approval levels are in Serial mode
      * Service Account Primary Owner and Service Account Secondary Owner
      * If owners are not defined, the request is redirected to the “No Service Account Owner” Work Group
  + The Workgroup must be created via the IdentityIQ Administrative Workgroups page. The name of the Workgroup must start with application name. Otherwise, the workgroup will not show up on the Self-Service Onboarding form.
  + Workgroup membership can be managed by the **IdentityIQ** application or needs to be configured via the **IdentityIQ Administrative Workgroups** page.
  + Applications that require the requestor form must create a Role under the Organizational Role “**Form Roles**” and create a form via **IdentityIQ Administrative Forms** Page
    - The Application name must be defined on the Role. This can be done via a non-indexed extended attribute “formappName”. These roles are just shell roles and they must not be configured with any IT roles. These roles must start with the application name. The application name will be **automatically** set on the Form Role using the Self Service Onboarding Wizard
    - The Form name must start with the application name. Any field on the form that matches with the application schema field will be provisioned directly to an application and the unmatched field will be provisioned to an application “**Extended Form**”. This application will generate a manual action item within IdentityIQ. This behavior can be overridden via the **Ticket Integration Feature**
  + Approvals can be split into multiple provisioning plans. This requires picking a split point. The split point can be configured and enabled via the “Global Definition” QuickLink.
  + Implicit Approvals
    - By default, implicit approvals are turned off. Requests can be auto-approved where requestor or requestee is same as approver. If electronic signatures are enabled, implicit approvals are not used.
  + Electronic Signatures can be enabled via the “Global Definition” QuickLink
    - Configure Electronic Signature Text on configuration object “**ElectronicSignature**” **via Debug Page**
  + On termination, Business Approvers Reassignment can be configured via the “Global Definition” QuickLink
  + Notification Schemes can be configured via “Global Definition”. Here are the default settings for the scheme:
    - Approval Notifications are turned ON. This can be turned OFF for Lower environment testing
    - Notification Scheme
      * Both Reminders and Escalations
    - 1st Reminder After 24 Hours
    - 3 Reminders After Every 24 hours
    - 1st Escalation After 3 Reminders
      * Reminder Cycle Restarts (3 Reminders After Every 24 Hours)
      * Escalation email is copied to Manager
    - Auto Rejection After 7 Days or 168 Hours
* The “Global Definition” QuickLink can be used to configure these approval settings. These settings are saved in a custom artifact “**Custom-ApprovalFrameWorkMappings**”. Here is the table that lists the default settings.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| Split Eligibility | This is used for splitting the request that eliminates the dependency of provisioning of cart items that has different approval path | This is False or OFF for all levels of approval   * RoleBusApprovers * AdditionalRoleBusApprovers * AdditionalEntitlementBusApprovers * AdditionalApplicationBusApprovers * ApplicationBusApprovers * EntitlementBusApprovers * BatchOwners * Operations |
| Default WorkItem Config | This is a notification scheme that is applied to all approval work items | * disableApprovalNotifications=false * notifyEmailTemplate= EmailTemplate-FrameworkApproval * reminderEmailTemplate=EmailTemplate-FrameworkReminder * escalationEmailTemplate=EmailTemplate-FrameworkEscalation * accountSelectionNotifyEmailTemplate =EmailTemplate-FrameworkAccountSelectionNotification * escalationStyle=both * hoursBetweenReminders=24 * hoursTillEscalation=24 * hoursTillExpiration=168 * maxReminders=3 * escalationRule=Rule-FrameworkEscalationType * escalationType=emailToManager   + Possible values:   + sameLevel: execute rule defined in escalationSameLevelRule entry   + directManager: escalate to work item owner's direct manager   + emailToManager: does not escalate item, but sends an email to owner's manager and cc's the owner * electronicSignature=No Electronic Signature Required * escalationSameLevelRule= |

### Accelerator Pack Implementation

This feature offers an extended rule to handle exceptional use cases to implement customers’ requirements

* Approval Extended Rules can be implemented to omit or override approvals
* The Requestor Form Extended rule can be implemented to generate a dynamic requestor form instead of a static requestor form or can be omitted for an application
* Escalation Extended Rule can be implemented for peer level escalations
* On Termination, Extended Rule Business Approvers Reassignment can be implemented to override default manager reassignment. This must be implemented and configured **only** **when cube names are used as business approvers**
* GRC Rule “Accelerator Pack GRC Dates Rule” can be used to set dates on requested access items. This rule is called from provisioning workflow “Interactive Request Provision with retries”
* An accelerator pack workflow “Accelerator Pack GRC Integration” can be implemented for any GRC system integration for preventive policy violation checks, polling of policy on GRC system, and provisioning to the requested end system. This workflow is called after approval work items are acted upon the requested items

### Built In Functionality

* Maximum 5 Approval Level for Regular cubes and 6 Approval Level for Service Cubes. However maximum level can be extended using extension rules
  + Manager Approval
  + Service Owner Approval
    - Two Levels
  + Two levels at application
  + Two levels at entitlement
  + Two levels at Role
* Configuration of Requestor Form per Application
* Split Approval Level Configuration
* Email Templates
  + Submission
  + Approval
  + Rejection
  + Auto Rejection
  + Completion
  + Business Approvers Reassignment
* Service Account Owners Approval for Service Accounts and Access Request
* Manager Forward when Manager is Inactive for Access and Accounts Request
* No Manager Found Workgroup Forward when Manager Not Found for Access and Accounts Request
* No Service Account Owner Forward when Primary and Secondary Service Account Owners Not Found for Access and Accounts Request
* Auto Manager Approval when Requestor is Manager for Access and Accounts Request
* Service Owner Approval Service Cubes for Access and Accounts Request
* Auto Rejection After Work Item Expiration for Access and Accounts Request
* All Emails are sent to Requestor and copied to Requestee (Requestee is not copied in case of Immediate Termination)

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-ApprovalFrameWorkMappings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Policy Violation Feature

### Description

This is required for any application that requires strict controls around access that is being requested from IdentityIQ. Control can be soft or hard stop access request, or it could be an eligibility type policy violation. Soft means requests can be submitted, and hard means requests cannot be submitted. Eligibility type means only certain sets of population can be allowed have access on this application. Usually, this type is always hard stop.

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard QuickLink or IdentityIQ Administrative Application Wizard**. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* Multiple Accounts Single Entitlement
  + Create and Configure Advanced policy that starts with application name
  + Create Custom Artifact for any Single Entitlement Exception that starts with application name (Optional)
  + Configure Application using Self Service Onboarding Wizard or IdentityIQ Administrative Application Wizard to set this policy as hard or soft stop
* Multiple Account Toxic Combinations Multiple Entitlements
  + Create and Configure Advanced Policy that starts with application name
  + Create and Configure Custom Artifact Toxic Combination that starts with application name (Required)
  + Configure Application using Self Service Onboarding Wizard or IdentityIQ Administrative Application Wizard to set this policy as hard or soft stop
* Eligibility Policy Violation
  + Create and Configure Population using Advanced Analytics that starts with application name
    - Instead of population, Java Regular Expression can be used from IdentityIQ Application Administrative Page
  + Create and Configure Advanced Policy that starts with application name
  + Configure Application using Self Service Onboarding Wizard or IdentityIQ Administrative Application Wizard to set this policy as hard or soft stop
* Single account applications must use the out of the box IdentityIQ Policy Administration Page
* Configure the custom artifact “**Custom-PolicyViolation-AllowDenyExceptions**” for any policy violation that is across multiple applications for hard and soft stop. This can be configured using the “**Global Definition**” QuickLink.

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Value |
| Empty | Policy Across Multiple Applications | Either “Allow Exception” or “Deny Exception” |

* Configure the custom artifact “**Custom-Framework-Common-Settings**” to turn on preventive policy violations check during access request. This can be configured using the “**Global Definition**” QuickLink.

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Value |
| policyScheme | Either can be Interactive or None.  Interactive means preventive policy violations are turned on | interactive |
| policyDenyFilter | Global Filter for Hard Preventive Access Request | Empty |
| policySoftFilter | Global Filter for Soft Preventive Access Request | Empty |

### Built In Functionality

* Hard and Soft Stop Policy Violation Configuration
* Eligibility Policy Violation Configuration
* Supports Multiple Accounts Single and Toxic Combination Policy Violations Configuration
* Advanced Policy Rule Java Library
  + Built in Library for Multiple Accounts Single Entitlement, Toxic Combinations, and Eligibility Type Policy Violations

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-PolicyViolation-AllowDenyExceptions**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Value |
|  |  |  |

* <Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Value |
|  |  |  |

## Attribute Synchronization Feature

### Description

This feature is used to synchronize Identity Cube attribute changes coming from authoritative sources to target system attributes. Also, it can be used to synchronize attributes from target systems. For example, (Active Directory / Exchange) to authoritative sources (for example Workday)

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard QuickLink**.

Mapping of Identity Cube source attributes to target system attributes needs to be configured via the **Self Service Onboarding Wizard**. These mappings are saved in a custom artifact “**Custom-FrameworkAttributeSyncMapping**”.

### Accelerator Pack Implementation

* Extended Rules can be used to support complicated synchronizations per application. These rules must be defined and referenced in the custom artifact “**Custom-FrameworkAttributeSyncMapping**” via the **Debug Page**.
* The name/reference of these rules is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postAttributeSyncRule | This is used within Attribute Synchronization Workflow after plan execution | Empty |

* Parlallel Lifecycle Events saved using the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| attributeSyncParallelMover | Execute Mover and Attribute Synchronization in Parallel | Empty |
| attributeSyncParallelRehire | Execute Rehire and Attribute Synchronization in Parallel | Empty |

### Built In Functionality

* Supports Multiple accounts synchronization
* Supports Workflow driven attribute synchronization
* Supports Create provisioning policy synchronization
* Extended Rules Support for complicated Synchronization

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list all the configuration changes that are applied to the object “**Custom-FrameworkAttributeSyncMapping**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Identity Cube Attribute Name | Description | Application Schema Attribute Name Mappings |
|  |  |  |

## Password Synchronization Feature

### Description

This feature is used to synchronize enterprise directory passwords to target applications. This is used where either applications don’t support single sign on integration or there is some kind of synchronization hybrid model (for example Active Directory and Azure).

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard QuickLink or IdentityIQ Administrative Application Wizard** for Target Application Mappings. The configurations applied through these wizards for this feature are saved on a selected application artifact that is being on boarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* The “**Global Definition**” QuickLink can be used to configure Identity Cube Attributes for verification process. This process is executed by the Help Desk. Changes made from the QuickLink are saved to a custom artifact “**Custom-Identity-Verification-Form-Settings**”. Attributes that are **excluded** by default are

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| needsJoiner | This is used for Joiner Feature | True |
| saccountOwnerone | Service Account Feature Attribute | True |
| serviceCube | Service Account Feature Attribute | True |

**Please Note:** The Out of Box Manage Passwords QuickLink can be used for Service Accounts/Service Cube Password Changes.

* The “Self Service Onboarding” QuickLink can be used to set password synchronization target aplications **per application**. These changes are saved on the selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template.

### Built In Functionality

* Supports Multiple Accounts Password Synchronization
* Supports Multiple Enterprise Directory Password Synchronization
* Password Interceptor
* Change Password Email Templates
* **Change Password** QuickLink
  + Accessible To End User
  + Accessible To Help Desk
    - Identity Verification Based on Cube Attributes

### As Built Configuration

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* <Please list all the configuration changes that are applied to the object “**Custom-Identity-Verification-Form-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## IdentityIQ Ownership and Access Feature

### Description

This feature is used to manage IdentityIQ access using a **loopback connector**. The access on IdentityIQ application is workgroup membership and capabilities. On Termination, all this access gets removed from IdentityIQ. Also, ownership of IdentityIQ Artifacts gets reassigned to the terminated Identity’s manager

### Accelerator Pack Configuration

The IdentityIQ application is packaged with this feature named “IdentityIQ Access”. This application is onboarded with the Accelerator Pack Features that are listed in [Built In Functionality](#Built in Functionality).

The list of configuration items for this feature are

* Need to configure group email on the No Reassignment Workgroup. This workgroup is used when there is no new owner for IdentityIQ items that are owned by the terminated identity
* Configure list of IdentityIQ Artifacts and Business Approvers that needs to be reassigned on termination using the “**Global Definition**” QuickLink. Changes are saved to a custom artifact “**Custom-Framework-Common-Settings**”. Here is the table of default settings:

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| removeIIQArtifactsOwnership | Enable IdentityIQ Artifacts Reassignment | True |
| reassignOwnershipToManager | On Termination, Reassign IdentityIQ Artifacts To Manager | True |
| reassignmentRule | Override Ownership Reassignment to Manager for IdentityIQ Artifacts via Rule. Rule must return cube or workgroup | Empty |
| sailpointArtifacts | List of IdentityIQ Artifacts to Reassign | * Bundle: Reassignment of Role ownership * Application: Reassignment of Application ownership * Policy: Reassignment of Policy ownership * ManagedAttribute: Reassignment of Entitlement ownership * GroupDefinition: Reassignment of Population ownership * CertificationDefinition: Reassignment of Certification Campaign ownership * TaskDefinition: Reassignment of Reports ownership * Identity: Reassignment of Workgroup ownership * WorkItem: Reassignment of pending certifications, pending approvals, pending forms, etc. |
| businessApproversremoveOwnership | Enable Business Approvers Artifacts Reassignment | True |
| businessApproversToManager | On Termination, Reassign Business Approvers To Manager | True |
| businessApproversreassignmentRule | Override Ownership Reassignment to Manager for Business Approvers via Rule. Rule must return cube or workgroup | Empty |
| sailpointBusinessApproversArtifacts | List of IdentityIQ Business Approver Attributes to Reassign | * appBusApprovers * additionalAppBusApprovers * entBusApprovers * additionalEntBusApprovers * roleBusApprovers |

* Workgroup members need to be added to the following groups
  + IdentityIQ Read Only Access Approvers: Approvers who are responsible for read only access in IdentityIQ

### Accelerator Pack Implementation

On Termination, the Reassignment Extended Rule can be implemented to override default manager reassignment.

### Built In Functionality

* Onboarded IdentityIQ Application named “IdentityIQ”
  + Aggregation Feature
    - Privileged Account Identification
      * Name EQUALS spadmin
    - Privileged Entitlement Identification
      * Capabilities.name EQUALS SystemAdministrator
  + Joiner Feature
    - Enable Immediately Option for Rehire
    - Enable Immediately Option for Return To Work Leave of Absence
    - Enable Immediately Option for Return To Work Long Term Disability
    - Enable Immediately Option for Reverse Leaver
  + Termination Feature
    - Disable and Remove Entitlements
      * Capabilities and Workgroups
    - Disable Option for Leave of Absence
    - Disable Option for Long Term Disability
  + Mover Feature
    - Mover Certification
      * Disable Account with no access on Revocation
  + IdentityIQ Artifacts Reassignment Email Template
  + Approvals Feature
    - Bundle for Read Only Access in In IdentityIQ “Read Only IdentityIQ Access”
      * WorkGroup “IdentityIQ Read Only Access Approvers” as 1st Level Role Approvers on this role

### As Built Configuration

* <Please list “IdentityIQ” application onboarding settings for the [Customer] that are changed for this feature. Please use the Accelerator Pack Application Onboarding Template>
* Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* Please fill in the group email settings on the workgroups for the [Customer]

|  |  |
| --- | --- |
| Work Group Name | Group Email Settings |
| No Reassignment | <> |

## New Account Dependency Entitlements Feature

### Description

This feature offers **new** account and authorization synchronization between Business Applications and/or IT/Infrastructure Technology Applications.

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard** **or IdentityIQ Administrative Application Wizard QuickLink.** Extended Rule Option is excluded from the Self-Service Onboarding Wizard**.** The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

Mappings or configuration done via the Self Service Onboarding Wizard saves the after-provisioning rule “**Rule-AccountCreation-Dependency-Framework**” on the application.

Mappings or configuration done via IdentityIQ Administrative Application Wizard require the after provisioning rule to be selected and saved on the application explicitly.

Existing after-provisioning rule on applications must be **configured via the** **debug page** to merge this feature’s rule libraries and method.

### Accelerator Pack Implementation

The Extended Rule can be implemented to omit this dependency provisioning conditionally. This implemented rule name must be applied to the **Conditional Omit Dependency Application Entitlements Rule** field via the Administrative or Self-Service Wizard.

### Built In Functionality

* After provisioning Rule **Rule-AccountCreation-Dependency-Framework**
  + Referenced Library Rule-AccountCreationDependency-RuleLibrary
  + Referenced Library Rule-Framework-AfterBeforeProvisionRuleLibrary
  + Invokes Method addAccountCreateDependencyRequests(plan, application.getName())

### As Built Configuration

<Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>

## Privileged Account Feature

### Description

This feature is used to validate cart/batch access request. It allows privileged access to be applied to privileged accounts only. It sends out email notifications to privileged account owners to reset their passwords more frequently. Privileged access can be configured to be excluded from manager certifications and access request approvals. Privileged accounts can be configured to be excluded from password synchronization, attribute synchronization, account rename, and account move.

### Accelerator Pack Configuration

This feature can be configured using the **Self Service Onboarding Wizard** **or IdentityIQ Administrative Application Wizard QuickLink.** The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

* Schedule Task “**Privileged Account Password Expiration Notification**” for password reset notifications
* The “**Global Definition**” QuickLink can be used to exclude Privileged Access from Manager Certifications. Changes are saved to a custom artifact “**Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess**”
* Here is the list of things that can be configured by Wizard.
* Exclude Privileged Accounts from Password Change (Password Synchronization Feature)
* Exclude Privileged Accounts from Move/Rename and Attribute Changes (Attribute Synchronization Feature)
* Exclude Privileged Accounts from Account Move (Mover Feature)
* Exclude Privileged Accounts from Account Move (Joiner Feature)
* Omit Manager’s Approval
* Enable Password Reset Notifications
  + Password Notification Before Expiration in X Days
  + Password Reset in X Days
  + Action on Account After Password Expiration in X Days
  + Action After Password Expiration Option
  + Password Format Option
  + Password Attribute

### Accelerator Pack Implementation

The Extended Rule can be used to calculate password age on the application. This implemented rule name must be applied to the field “**Password Expiration Date Rule**” and the “**Extended Rule**” option must be selected for the field “**Password Expiration Date Format Options”**. The Extended rule option is not provided on the Self Service Onboarding Wizard. Therefore, this configuration can be done only from the IdentityIQ Application Administrative Wizard.

Account Mapping Rule needs to be implemented to set Privileged Account Type during aggregation

### Built In Functionality

* Separate QuickLink “**Manage Privileged Access**” to manage privileged access
* Privileged access is filtered out from out of the box “**Manage Access**” QuickLink
* Task Definition to Send out Password Notifications
  + Password Notification Email Template
* Workflow to take action after Password Expiration. Action is based on selected options
* Interactive Request Email Templates
* Access and Batch Request Validations
  + Apply Privileged Access to Privileged Accounts Only
  + Primary Account must exist before privileged access request
  + Force New Privileged Account Creation for Privileged Access

### As Built Configuration

<Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>

## Service Account Feature

### Description

This feature provides Advanced Certification Campaign functionality where primary or secondary service account owners can certify service accounts. On termination, service account ownership is reassigned to the manager.

### Accelerator Pack Configuration

* Need to configure group email on No Service Account Owner Workgroup. This workgroup is used when **primary and secondary service account owners are not found on cube for the following use cases**
  + Service Account Owner Certification (Advanced Certification)
  + Access/Account Approvals for Service Account Cube
* Configure a list of IdentityIQ Artifacts and Business Approvers that needs to be reassigned on termination using the “**Global Definition**” QuickLink. Changes are saved to a custom artifact “**Custom-Framework-Common-Settings**”. Here is the table of default settings:

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| serviceAccountremoveOwnership | Enable Service Account Ownership Reassignment | True |
| serviceAccountreassignOwnershipToManager | On Termination, Reassign Service Account Ownership To Manager | True |
| serviceAccountreassignmentRule | Override Ownership Reassignment to Manager for Service Accounts via Rule. Rule must return cube or workgroup | Empty |
| serviceAccountOwnerAttrs | List of Service Account Ownership Attributes to Reassign | **Comma Separated** List   * saccountOwnerone * administrator |

### Accelerator Pack Implementation

On Termination, Extended Rule Service Account Ownership Reassignment can be implemented to override default manager reassignment.

### Built In Functionality

* Pre-Delegation Rule “Rule-Framework-ServiceCubes-CertificationPreDelegation” for Advanced Certifications
* Workgroup “No Service Account Owner” for Advanced Certifications
* Manager Reassignment for Service Account Ownership
* Email Templates
  + Reassignment Email Template
  + Certification Email Templates
* Create Service Account Identity Cubes
  + Please see [Create Identity Feature](#Create Identity Feature)
* Edit Service Account Identity Cubes
  + Please see [Edit Identity Feature](#Edit Identity Feature)
* Manage Request Access
  + Service Cube Access and Approvals. Please see [Approvals Feature](#Approvals Feature)
* Manage Accounts
  + Create Service Cube Accounts and Approvals. Please see [Approvals Feature](#Approvals Feature)

### As Built Configuration

* Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* Please fill in the group email settings on the workgroups for the [Customer]

|  |  |
| --- | --- |
| Work Group Name | Group Email Settings |
| No Service Account Owner | <> |

## Create Identity Feature

### Description

This feature is used to Create Identity Cubes for Service Accounts and Contractors.

### Accelerator Pack Configuration

Same [Joiner Feature](#Joiner Feature) configurations will be applied to this feature for Contractor’s Joiner access.

QuickLink “Global Definition” can be used to configure following things

* Turn Contractor Sponsor or Service Account Owner/Administrator Approval ON/OFF for Service Accounts and Contractors. These settings are stored in custom artifact “**Custom-ApprovalFrameWorkMappings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| CREATE IDENTITY FEATURE | This enables manager approval for service accounts or contractor creation | <String>ManagerOrServiceAccountOwner</String>  <String>Workgroup</String> |

* Turn ON/OFF Service Account Fields on create form and set up Contractor Expiration date format. These settings are stored in custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| createServiceCubes | This option shows Service Account fields on form “Accelerator Pack Create Identity” | TRUE |
| createEditCtrDateFormat | The default date format for contractor expiration date | MM/dd/yyyy K:m:s a z |

The contractor cube attributes that can be populated during Identity Creation are:

* Unique Cube Name\*: The value of this attribute can be manually entered or implemented using rule “Rule-FrameWork-Generate-Unique-Id”
* Last Name\*: Entered Last Name
* First Name\*: Entered First Name
* Middle Name: Entered Middle Name
* Email\*: Entered Email
* Contractor Sponsor/Manager\*: Entered Sponsor/Manager
* Contractor Expiration Date\*: Entered Date
* Contractor/Profile Manager\*: Entered Manager
* Type\*: Contractor

The Service Account cube attributes that can be populated during Identity Creation are:

* Unique Cube Name\*: The value of this attribute can be manually entered or implemented using rule “Rule-FrameWork-Generate-Unique-Id”
* Application Name\*: Selected Application Name
* Last Name\*: Auto-generated on the form with the value same as of attribute “Unique Cube Name” or can be manually entered
* First Name\*: Auto-generated on the form with the value same as of selected attribute< Application Name (Only Alpha Numeric Characters) or can be manually entered
* Service Account Owner\*: Selected Identity. This is used for IdentityIQ version 7.2
* Administrator\*: Selected Identity. This is used for IdentityIQ version 7.3
* Type\*: Service Accounts

### Accelerator Pack Implementation

Generation of Unique Id for contractor and service account cubes can be implemented within the Rule “Rule-FrameWork-Generate-Unique-Id”.

The “Accelerator Pack Create Identity” form can be modified to add additional fields for contractor cube creation.

The same form is used for service account cubes. If the Service Account Feature is enabled, any additional field for service account added to the form must be hidden for the contractors. Please using the following hidden script on the field

### <Attributes><Map><entry key="hidden"><value><Script><Source><![CDATA[

### if(form!=null && form.getField("type")!=null)

### {String isServiceHumanCube=form.getField("type").getValue();

### if (null != isServiceHumanCube && isServiceHumanCube.equalsIgnoreCase("contractor"))

### {return false;}else{return true;}}else{return true;}]]></Source>

### </Script></value> </entry></Map></Attributes>

### Built In Functionality

* Form “Accelerator Pack Create Identity” to create service account and contractor
* This uses the Joiner Feature for contractors to assign joiner access
* Email Templates
* Provisioning to Contractors, and Service Account Repository

### As Built Configuration

<Please list all the configuration changes that are applied to the object “**Custom-ApprovalFrameWorkMappings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

<Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Edit Identity Feature

### Description

This feature is used to Edit Identity Cubes for Service Accounts and Contractors.

### Accelerator Pack Configuration

The same [Attribute Sync Feature](#Attribute Sync Feature) configurations will be applied to this feature for contractor attribute changes to the downstream systems.

The same [Leaver Feature](#_Leaver_Feature) configurations will be applied to contractor cubes on contractor expiration date change only if leaver trigger is set up on expiration date.

The same [Mover Feature](#_Mover_Feature) configurations will be applied to contractor cubes on contractor expiration date change only if mover trigger is set up on expiration date.

The “Global Definition” QuickLink can be used to configure the following things:

* Turn Contractor Sponsor/Manager or Service Account Owner/Administrator Approval ON/OFF for Service Accounts and Contractors. These settings are stored in the custom artifact “**Custom-ApprovalFrameWorkMappings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| EDIT IDENTITY FEATURE | This enables manager approval for service or contractor cube modification | <String>ManagerOrServiceAccountOwner</String>  <String>Workgroup</String> |

* Turn ON/OFF Service Account Cube field “Administrator” on edit form. These settings are stored in the custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| editServiceCubes | This option shows Service Cube modification fields on form “Accelerator Pack Edit Identity” | TRUE |

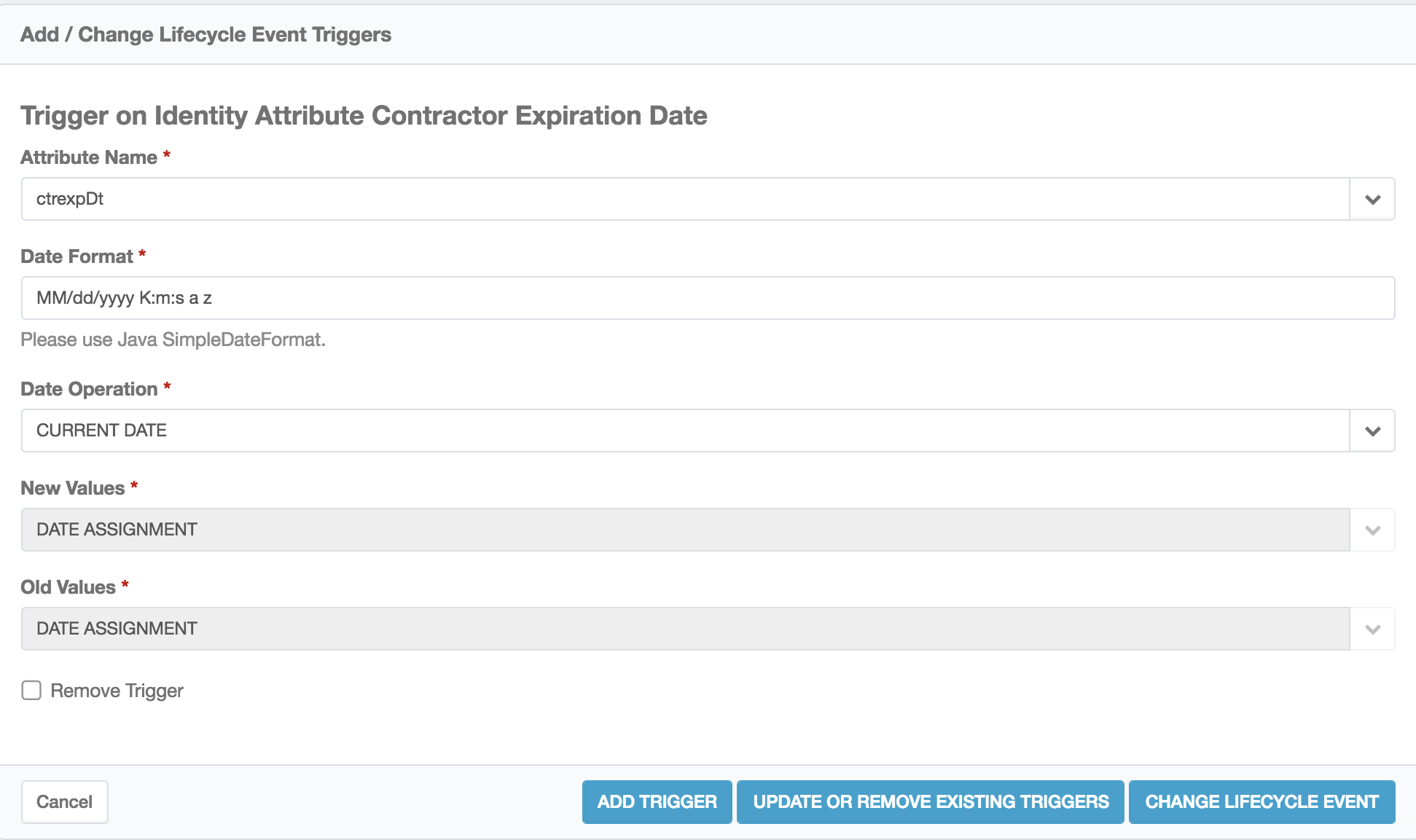
The contractor cube attributes that can be edited from IdentityIQ are:

* Last Name\*: Entered Last Name
* First Name\*: Entered First Name
* Middle Name: Entered Middle Name
* Email\*: Entered Email
* Contractor Expiration Date\*: Entered Date
* Contractor Sponsor/Manager\*: Entered Sponsor (Used for Approvals)
* Contractor/Profile Manager\*: Entered Manager

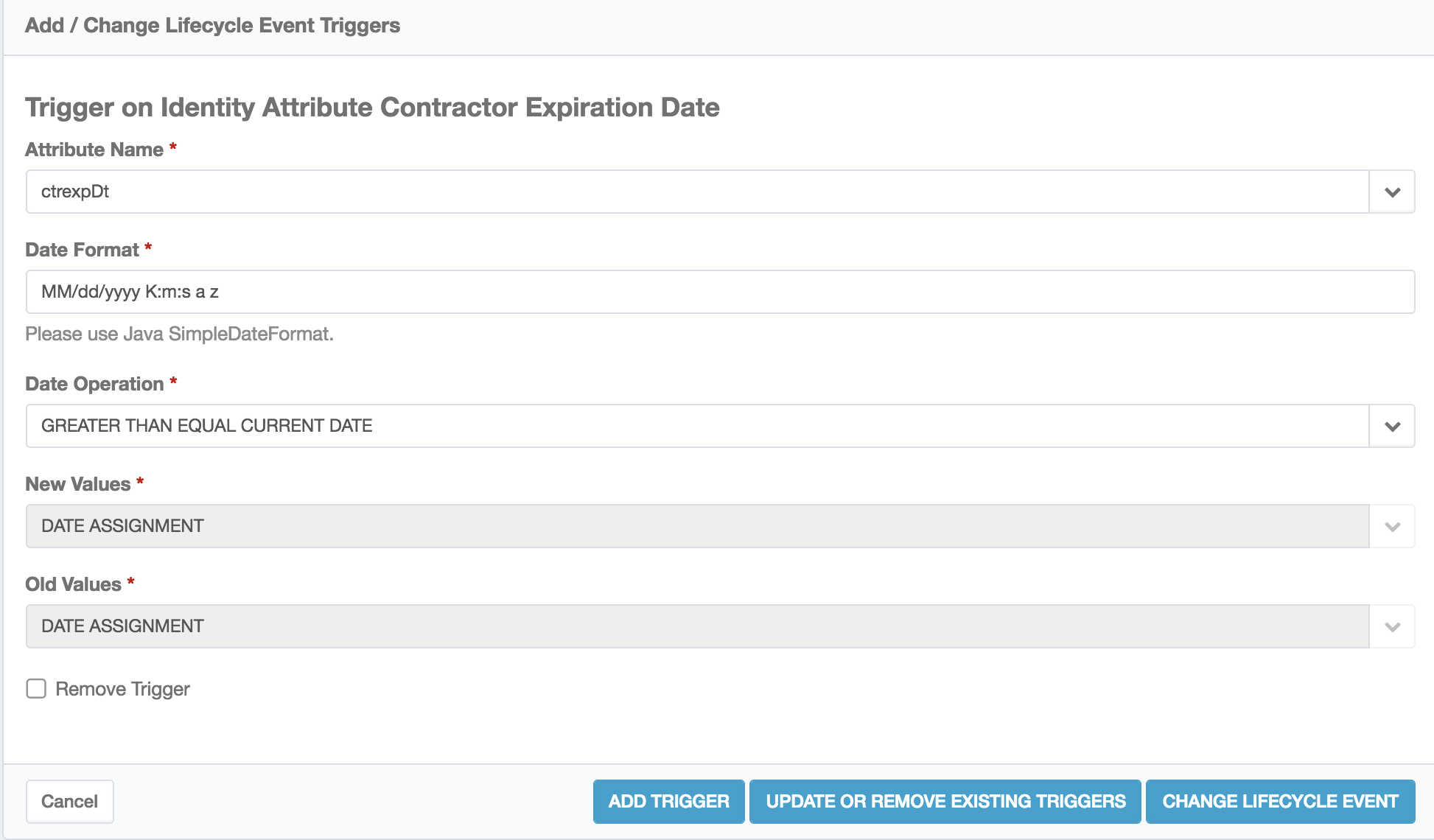
The service account cube attributes that can be edited from IdentityIQ are:

* Last Name\*: Entered Last Name
* First Name\*: Entered First Name
* Service Account Owner\*: Selected Identity. This is used for IdentityIQ version 7.2
* Administrator\*: Selected Identity. This is used for IdentityIQ version 7.3

**Contractor Leaver Trigger Configuration:** If required, Please use QuickLink “Lifecycle Triggers” to configure leaver trigger for contractors as shown in the below screen shot.

****

**Contractor Mover Trigger Configuration:** If required, Please Use QuickLink “Lifecycle Triggers” to configure mover trigger for contractors as shown in the below screen shot..



### Accelerator Pack Implementation

The “Accelerator Pack Edit Identity” form can be modified to add additional fields for contractors.

The same form is used for service account cubes. If Service Account Cube Modification is enabled, any additional field added to the form for service accounts must be hidden for contractors. Please using the following hidden script on the service account field

### <Attributes><Map><entry key="hidden"><value><Script>

### <Source><![CDATA[

### if(form!=null && form.getField("serviceCube")!=null)

### {String isServiceCube=form.getField("serviceCube").getValue();

### if (null != isServiceCube && isServiceCube.equalsIgnoreCase("TRUE")) {return true;}

### else{return false;}}else{return true;}

### ]]></Source></Script></value></entry></Map></Attributes>

### Built In Functionality

* The “Accelerator Pack Edit Identity” form to edit service account and contractor cubes
* This uses the Attribute Synchronization Feature for contractor attribute synchronization to downstream steams
* Email Templates
* Provisioning to Contractors, and Service Account Repository

### As Built Configuration

<Please list all the configuration changes that are applied to the object “**Custom-ApprovalFrameWorkMappings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

<Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

<Please list all the configuration changes that are applied to the object “**Custom-Triggers**” for the [Customer]>

|  |  |  |  |
| --- | --- | --- | --- |
| Object Name | Trigger Name | Triggers Definition | Operation Between Triggers |
| Custom-Triggers | LEAVER FEATURE | <Defined in Custom-Triggers XML> | <Defined in Custom-Triggers XML> |
| Custom-Triggers | MOVER FEATURE | <Defined in Custom-Triggers XML> | <Defined in Custom-Triggers XML> |

## Registration Feature

### Description

This feature is used to Register Identity for Non-Employee Population.

### Accelerator Pack Configuration

The same [Joiner Feature](#Joiner Feature) configurations will be applied to this feature as for Joiner access.

QuickLink “Global Definition” can be used to configure following things

* Turn ON/OFF Manager Approval. These settings are stored in custom artifact “**Custom-ApprovalFrameWorkMappings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| REGISTRATION IDENTITY FEATURE | This enables manager approval for contractor cube registration | <String>ManagerOrServiceAccountOwner</String>  <String>Workgroup</String> |

The cube attributes that can be populated during Identity Registration are:

* Unique Identity\*: The value of this attribute can be manually entered or implemented using the “Rule-FrameWork-Registration-Generate-Unique-Id” rule
* Last Name\*: Entered Last Name
* First Name\*: Entered First Name
* Middle Name: Entered Middle Name
* Manager\*: Entered Manager
* Email\*: Entered Email
* Contractor Manager\*: Entered Manager

### Accelerator Pack Implementation

Generation of Unique Id for contractors can be implemented within the Rule “Rule-FrameWork-Registration-Generate-Unique-Id”.

The “Accelerator Pack Register Identity” form can be modified to add additional fields for the registration.

### Built In Functionality

* Form “Accelerator Pack Registration Identity” to register cubes
* This feature uses the Joiner Feature to assign joiner access to newly registered cubes
* Email Templates

### As Built Configuration

<Please list all the configuration changes that are applied to the object “**Custom-ApprovalFrameWorkMappings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Provisioning Feature

### Description

This feature is used to set up provisioning retries, time interval between provisioning retries, and a list of provisioning retry errors. These parameters per application can be configured using the **Self Service Onboarding Wizard** QuickLink or the **Debug Page.** The configurations applied through the wizard for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

### Accelerator Pack Configuration

* The “Global Definition” QuickLink can be used to set global provisioning retries, and time interval between provisioning retries. This applies to all applications that have some sort of provisioning mechanism. Creation of ticket for an application is also considered to be a provisioning action. These settings are stored in a custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| provisioningRetryThreshold | The interval in minutes to wait to retry the request | 720 |
| provisioningMaxRetries | The maximum number of retries that will be attempted before failure of the provisioning | 3 |
| postWrapperRule | This rule is executed after wrapper workflow execution | Empty |
| interceptorPlanRule | This rule is executed before wrapper workflow plan compilation | Empty |
| interceptorProjectRule | This rule is executed before wrapper workflow project provisioning | Empty |

* The “Global Definition” QuickLink can be used to set Target Aggregation settings that are stored in Custom-Framework-Common-Settings

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| targetAggregationAttributes | List of attributes that requires Target Aggregation. This is executed within Accelerator Pack Workflows where the provisioning plan contains any of the item from the list | * AC\_NewName * AC\_NewParent |

* The “Self Service Onboarding” QuickLink can be used to set provisioning retries, and time interval between provisioning retries **per application**. These changes are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template
* Configure list of provisioning definition connectors. Please see

[Self Service Onboarding Wizard Feature](#Self Service Onboarding Wizard Feature)

**Please Note:** Application Provisioning Settings will override Global settings

### Accelerator Pack Implementation

If required within Wrapper Workflow, the post workflow rule can be implemented for exceptional use cases. The names/reference of this rule is stored in a custom artifact “**Custom-Framework-Common-Settings**”.

The name/reference of this rule is saved via the **“Global Definition” QuickLink**. The changes are saved in a custom “**Custom-Framework-Common-Settings**” artifact.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| postWrapperRule | This is used within “Workflow-FrameWork-Wrapper” Workflow after post provisioning | Empty |

### As Built Configuration

* <Please list all the configuration changes that are applied to the object “**Custom-Framework-Common-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use the Accelerator Pack Application Onboarding Template>
* Please list all the rule implementation details for the [Customer]

## Ticket Integration Feature

### Description

This feature provides a user interface to set up applications for ticket integration.

It is also used to set up assignment group, ticket polling, and ticket retries per application using the **Self Service Onboarding Wizard QuickLink**. These can also be configured using the **IdentityIQ Administrative Application Wizard.** The configurations applied through these wizards for this feature are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template for application attribute names.

**An a**fter provisioning rule can be implemented and set up per application using only **IdentityIQ Administrative Application Wizard.**

### Accelerator Pack Configuration

The ”Configure Ticket Integration” QuickLink provides a user interface to set up connection settings for ticket integration and set up applications for ticket integration. The form fields of this user interface are configured using custom artifact “Custom-SmartServices -TicketIntegration-Form-Settings”. The configuration is based on key parameters for each type of integration. These settings are stored in custom object “**Custom-SmartServices-TicketIntegration-Form-Settings**” artifact. This custom artifact can be configured from the debug page if there is any upgrade/patch change to the integrations.

* Common Executor- Key Parameter in Custom Artifact is “commonExecutor”. This key defines common fields that will be displayed for all integrations
  + Remedy – Key Parameter in Custom Artifact is “RemedyIntegrationExecutor”. This key defines only Remedy Ticket Integration fields that will be displayed on the form
  + ServiceNow - Key Parameter in Custom Artifact is “ServiceNowIntegrationExecutor”. This key defines only ServiceNow Ticket Integration fields that will be displayed on the form
  + HP Service Manger- Key Parameter in Custom Artifact is “HPServiceManagerIntegrationExecutor”. This key defines only HP Service Manager Ticket Integration fields that will be displayed on the form
  + Accelerator Pack Simulated Ticket Integration (Used for Testing)– Key Parameter in Custom Artifact is “SmartServicesTicketIntegrationExecutor”. This key defines only Accelerator Pack Simulated Ticket Integration fields that will be displayed on the form

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| ServiceNowIntegrationExecutor | This key has comma separated QuickLink form field names for ServiceNow Ticket Integration | keystorePath,keystorePass,keystoreType,alias,keyPass,catalogItem,catalogItemList,username,password,authType |
| HPServiceManagerIntegrationExecutor | This key has comma separated QuickLink form field names for HP Service Manager Ticket Integration | multipleProvisioningSteps,lastProvisioningStep, checkStatusProvisioningStep,catalogItem,catalogItemList,username,password,committedClosureCode,failureClosureCode,inProcessClosureCode |
| RemedyIntegrationExecutor | This key has comma separated QuickLink form field names for Remedy Ticket Integration | basicAuthType,httpUserName,httpUserPass |
| SmartServicesTicketIntegrationExecutor | This key has comma separated QuickLink form field names for Accelerator Pack Simulated Testing Ticket Integration | Empty |
| commonExecutor | This key has comma separated QuickLink form field names for all Ticket Integration Systems | executor,universalManager,planInitializerRule,multipleTicket,groupTicketBy,retryableErrors,noProvisioningRequests,provisioningRequestExpiration,managedResources,operations,defaultAssignmentGroupName,defaultRequestedBy,inProcess,failure,committed,ticketStatus,ticketId |

* The “Global Definition” QuickLink can be used to set Global Ticket Polling and Ticket Retries. This will apply to all applications that are integrated via tickets. The changes are saved in a custom artifact “**Custom-Ticket-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| provisioningMaxStatusChecks | The maximum number of retries that will be attempted before failure of the provisioning | 3 |
| provisioningStatusCheckInterval | The interval in minutes to retry the check status call | 720 |
| optimisticProvisioningTicket | This applies ticket provisioning optimistically to Identity cube after ticket completion | True |

**Please Note:** Application Ticket Polling and Retry Settings will override Global settings

* The “Self Service Onboarding” QuickLink can be used to set Assignment Group Name, Ticket Polling, and Ticket Retries **per application**. These changes are saved on a selected application artifact that is being onboarded. Please see the Accelerator Pack Application Onboarding template.
* The “Configure Ticket Integration” QuickLink can be used to set default Assignment Group Name and default Requestor (for Lifecycle Events or Background Events). These changes are saved on the selected IntegrationConfig

|  |  |
| --- | --- |
| Property Name | Description |
| defaultAssignmentGroupName | The default assignment group for ticket assignment on ticketing system. |
| defaultRequestedBy | The default requestor in case of background/system events in IdentityIQ |

**Please Note:** The Application Assignment Group Name will override the default Assignment Group Name and if the request is interactive will override the default requestor.

### SOAP Envelope Configuration

The SOAP Envelope for the “provisioning” entry and the “getRequestStatus” entry in the integration configuration must be configured with the following velocity parameters.

* Requestor Identity Attributes
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘requester<attributename>’)}
* Requestee Identity Attributes
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘requestor<attributename>’)}
* Requestee’s Manager’s Identity Attributes
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘manager<attributename>’)}
* Assignment Group Name for the requested Application
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘assignmentGroupName’)}
* IdentityIQ Request Id
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘identityRequestId’)}
* “requestType” variable initialized from the workflows
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘requestType’)}
* “flow” variable initialized from the workflows
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘flow’)}
* “source” variable initialized from the workflows
  + Referenced in SOAP Envelope as $!{provisioningPlan.getArguments().get(‘source’)}

### Accelerator Pack Implementation

An after Provisioning Rule can be implemented per application. An Extended Rule can be used to do some post ticket provisioning on an application. This implemented rule name must be applied to the field “**After Ticket Provisioning Extended Rule**” and the “**Extended Rule**” option must be selected for the field “**After Ticket Provisioning Options”**. The Extended rule option is not provided on the Self Service Onboarding Wizard. Therefore, this configuration can be done only from IdentityIQ Application Administrative Wizard.

### Built In Functionality

* User Interface to Ticket Based Applications
* After Provisioning Rule for Ticket Integrated Applications
* Plan Initializer Rule “Rule-Framework-Plan-Initializer” inserts data elements into the provisioning plan arguments. These data elements are needed for the ticket content and the content is configured via the debug page on the Integration Configuration object.
* Accelerator Pack Simulated Ticket Integration Testing

### As Built Configuration

* <Please list all the configuration changes that are applied to the object “**Custom-SmartServices-TicketIntegration-Form-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list all the configuration changes that are applied to the object “**Custom-Ticket-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* Please list all the configuration changes that are applied to the “IntegrationConfig” object “**[Name of the Object]**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

* <Please list each application’s onboarding settings for the [Customer] that are configured for this feature. Please use Accelerator Pack Application Onboarding Template>

## Epic Feature

### Description

This feature establishes a link between EMP records from an Epic feed and SER records from an SER feed based, on an Identity Lifecycle Event. This event is triggered based on two conditions:

* A new SER ID Record from the SER Feed for an EMP record on Epic
* A change in a SER Record. This change is detected by comparing the existing SER ID on an EMP record from Epic and the SER ID from SER Feed

### Accelerator Pack Configuration

Use the “Global Definition” QuickLink to configure Epic and SER application names and their attributes. The changes made from this QuickLink are saved to a “**Custom-Epic-SER-Settings**” custom artifact. Please see the table below for default settings that are packaged with this feature.

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| epicAppName | Epic Application Name | Empty |
| epicIdAttr | Epic Provider Id Attribute | LinkedProviderID |
| serAppName | SER Application Name | Empty |
| serIdAttr | SER Provider ID Attribute. The ID from this attribute is linked to an EMP record on the Epic Application on attribute “LinkedProviderID” | Empty |

### Built In Functionality

* EMP-SER Linking Lifecycle Event
* In case of Provisioning Failures
  + Email Provisioning Failures to “Operations” Work Group
  + Manual Linking/Unlinking of SER Record by “Operations” Work Group

### As Built Configuration

Please list all the configuration changes that are applied to the object “**Custom-Epic-SER-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Reports Feature

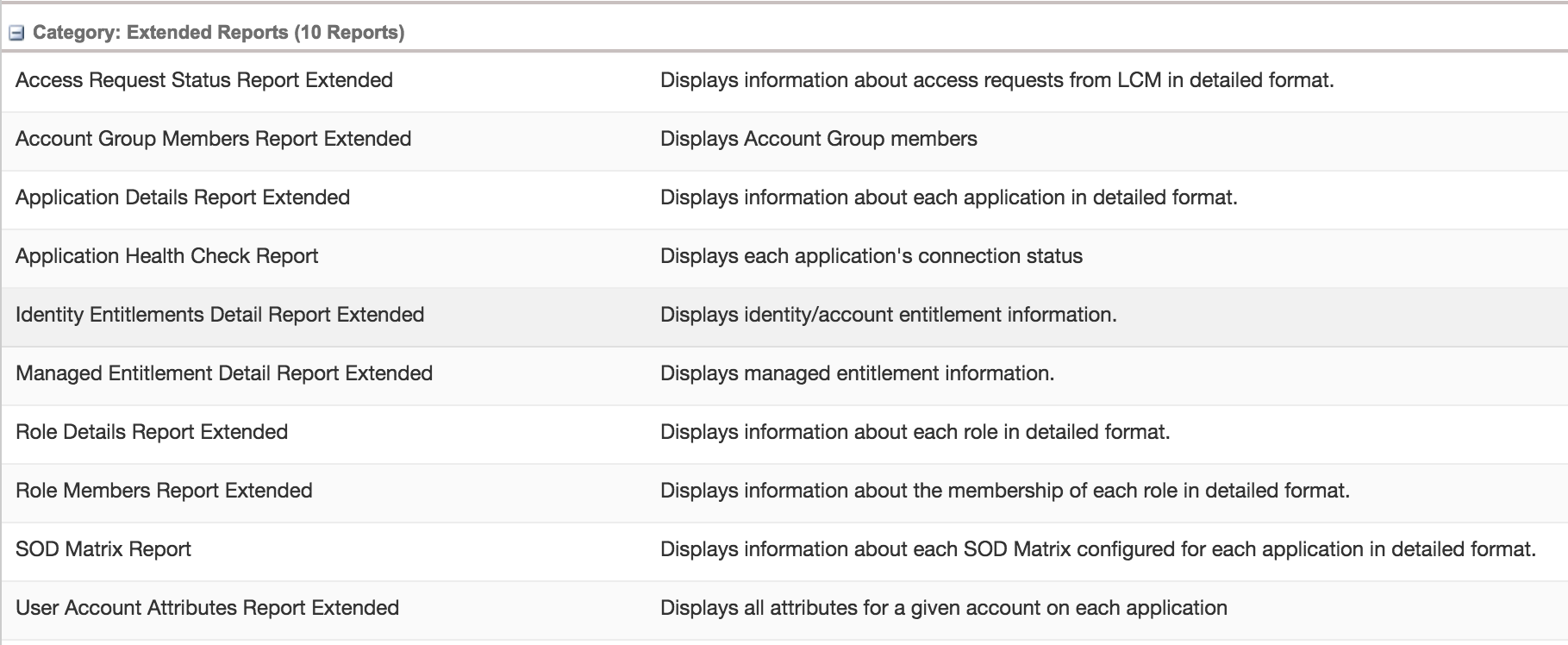
### Description

This feature extends out of the box reports with extended attributes. It contains two new additional reports.

* Application Health Check Monitoring
  + This tests the application’s basic connectivity, accounts connectivity, and group connectivity
* Application Multiple Accounts Policy Violation Composition
  + This report shows policy violations composition for multiple accounts on an application configured via application custom artifacts
    - Application only permits 1 entitlement per account
    - Entitlements cannot be assigned together per account

### Accelerator Pack Configuration

Please refer “**IdentityIQ Accelerator Pack Extended Reports.xlsx**” to configure reports of category “Extended Reports”.



### Built In Functionality

* New Report “Application Health Check Report”
* New Report “SOD Matrix Report”
* User Account Attributes Report Extended
* Application Details Report Extended
* Identity Entitlements Detail Report Extended
* Managed Entitlement Detail Report Extended
* Role Details Report Extended
* Role Members Report Extended
* Account Group Members Report Extended
* Access Request Status Report Extended
  + Extended with new flow values
    - Lifecycle
      * All Lifecycle Events
    - External
      * REST/SCIM Workflow Invocation
    - Interceptor
      * Password Interceptor Workflow
    - NewAccountDependency
      * New Account Entitlements Dependency
    - PasswordExpiration
      * Privileged Account Password Expirations
    - Recovery
      * Operational Recover Tool
    - PasswordsChangeRequest
      * Quick Link Change Password

### As Built Configuration

<Please list any additional configuration changes that are applied to the reports that are listed above for the [Customer]>

|  |  |
| --- | --- |
| Report Name | Report Configurations |
|  |  |

## Persona Feature

### Description

This feature manages Lifecycle Events for an Identity that has personas or multiple relationships within an organization. Joiner, Mover, and Lever Lifecycle events are triggered based on persona changes on an Identity. Also, Lifecycle events can be configured to be triggered based on Employee Authoritative Source.

* Joiner (OR Condition between following events)
  + New Persona
    - OR
  + Employee Authoritative Source Trigger
* Joiner Rehire
  + Addition of Persona
    - OR
  + Employee Authoritative Source Trigger
* Joiner Return To Work Leave of Absence
  + Employee Authoritative Source Trigger
* Joiner Return To Work Long Term Disability
  + Employee Authoritative Source Trigger
* Joiner Reverse Leaver
  + Addition of All Personas that were dropped
* Leaver
  + Drop of All Personas

Leaver Leave of Absence

* + Employee Authoritative Source Trigger
* Leaver Long Term Disability
  + Employee Authoritative Source Trigger
* Mover (OR Condition between following events)
  + Drop of Persona
    - OR
  + Employee Authoritative Source Trigger

### Accelerator Pack Configuration

ObjectConfig: Identity must be extended with two attributes “relationships” and “mgrrelationships”.

“Rule-Framework-IdentityAttribute-Manager-Global-Index” can be defined as global rule on extended attribute “mgrrelationships”. “Rule-Framework-IdentityAttribute-Relationships” can be defined as global rule on extended attribute “relationships”. The following attribute names must be configured within the rules.

**EMPLOYEE APPLICATION ATTRIBUTES**

employeeSource - Employee Application Name.

employeeStatusAttribute - Employee Application Attribute Name for Status.

employeeLOA - Employee Application Leave of Absence Attribute Name. This can be comma separated values.

employeeLTD - Employee Application Long Term Disability Attribute Name. This can be comma separated values.

managerIdEmployee - Employee Application Manager Id Attribute Name.

**NON- EMPLOYEE APPLICATION ATTRIBUTES**

nonEmployeeSource – Non-Employee Application Name.

nonEmployeeTypeAttr – Non-Employee Type Attribute Name for Non-Employee Application.

managerIdNonEmployee- Non-Employee Application Manager Id Attribute Name.

**STUDENT APPLICATION ATTRIBUTES**

educationSource – Student Application Name.

managerIdStudent - Student Application Education Coordinate Id Attribute Name

appointmentAttr - Student Application Appointment Attribute Name

schoolNameAttr - Student Application School Attribute Name

campusCodeAttr - Student Application Campus Attribute Name

programNameAttr - Student Application Program Attribute Name

Use the “Configure Triggers” QuickLink to configure Lifecycle Events for Employee Population (for example, Joiner, Mover, and LOA/LTD).

Use the “Global Definition” QuickLink

* Turn ON Persona Lifecycle Event
  + By Default, it is OFF
* Ignore relationship drop for Mover Lifecycle Event
  + By Default, it is an empty list
* All these settings are stored in a custom object artifact named “**Custom-Persona-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| enabledPersona | This is used to turn on Persona Lifecycle Events   * New Persona (Joiner Lifecycle Event) * Addition of Persona (Joiner Rehire Lifecycle Event) * Drop of Persona (Mover Lifecycle Event) * All Persona Drop (Leaver Lifecycle Event) * All Persona Add (Reverse Leaver Lifecycle Event) | False |
| moverRelationshipsDropIgnore | Ignore Relationship Drop For Mover Certification or Leaver (For All Persona Drops). This is compared against relationships attribute on an Identity Cube using STARTS WITH operation. Relationship added here must be in the format Relationship [INACTIVE], where Relationship is the name of the relationship from authoritative sources. | Empty List |

### Built In Functionality

* Identity Mapping Rules to populate Identity Cube extended attributes. These rules must be defined on persona extended attributes
  + Rule-Framework-IdentityAttribute-Relationships
    - This rule populates an extended attribute by display name “Relationships” and name “relationships”
  + Rule-Framework-IdentityAttribute-Manager-Global-Index
    - This rule populates an extended attribute by display name “Global Manager Index Relationships” and name “mgrrelationships”. During a certification campaign, this attribute can be used by the Primary Manager as a reference to delegate or reassign certification items to other managers
* Identity Reports are extended with attributes “Relationships” and “Global Manager Index Relationships”
* Certification screens would show “Relationships” and “Global Manager Index Relationships” on an Identity Cube and this helps primary manager to delegate or reassign items to secondary manager

Identity Mapping persona rules Rule-Framework-IdentityAttribute-Relationships and Rule-Framework-IdentityAttribute-Manager-Global-Index **can be used as references to implement customer specific rules**.

**Note: It is important to build relationships in following formats**

<Persona Name>[ACTIVE or INACTIVE or SUSPENDED]

### As Built Configuration

<Please list all the configuration changes that are applied to the object “**Custom-Persona-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Batch Feature

### Description

This feature follows the same approval scheme as access and account requests. The approval scheme is bypassed for the “Operations” Work Group.

### OOTB Configuration

If there is a requirement to have batch approvals for any batch request this can be done using the out of the box configuration “Batch Request Approver”. This will be the first level of approval for any batch request. Afterwards there will be additional approvals for each batch items if the requestor is not a member of the “Operations” Work Group. Batch Item requests go through the same approval scheme as cart requests and account items requested using the “Manage Accounts”, “Manage User Access”, and “Manage Privileged Access” QuickLinks.

### Accelerator Pack Configuration

Here is the list of configuration items

* System Configuration for Additional Batch Approver. This is done using Batch Request Approver - Require batch request approval
* Batch approval can be skipped for workgroup members. Workgroup is defined via the “Global Definition” QuickLink. The configuration that is done via QuickLink is saved in a custom artifact “**Custom-Framework-Common-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| byPassBatchApprovals | Approvals will by bypassed for group members | Operations |

### Built In Functionality

* Privileged Service Access and Account Validations
  + Privileged Access must be assigned to a privileged account
  + Regular access must be assigned to a regular account
  + Regular accounts must exist before we request privileged access
* Batch Request Form Validations
  + Fail on any policy violation required
  + Create Provisioning Forms required
  + Generate Identity Requests required
  + Create Work Items required
* Email Templates
* Same Approval Scheme for Access and Account request unless the requestor is a member of the Operations Work Group
* Additional Batch Approval

### As Built Configuration

## Simplified Logical Applications Feature

### Description

Accelerator Pack leverages extended attributes on roles and entitlements to manage logical applications. Role/Entitlements extended attributes are displayed and used for filtering during access request and certifications. No additional aggregation is required for this kind of approach other than Infrastructure/Platform/Technology application for example AD, Databases, Servers. The logical applications originate/tagged entitlements/roles of these applications. This feature supports simple extended attribute based Logical Business Applications. The display name of this extended attribute on roles and entitlements is “Logical Business Application Name”.

The logical business application is set on roles and entitlements using out of the box IdentityIQ Role and Entitlement Catalog Administrative Pages.

The attribute “Logical Business Application Name” on roles and entitlements can also be defined with multiple applications by using comma separator on the attribute between logical business application names.

### Built In Functionality

* Simple Extended Attribute Logical Applications
  + Extended Attribute on Roles
  + Extended Attribute on Entitlements
* Reports are extended with “Logical Business Application Name” attribute

### As Built Configuration

<Please list all the logical applications that are applied to the roles and entitlements for the [Customer]>. Please make sure **display name of the entitlements and roles contains the logical application name.** This is required because currently out of the box there is no easy way to display an extended attribute based logical application name on the approval work items.

|  |  |  |
| --- | --- | --- |
| Logical Application Name | Entitlement Catalog csv | Role Name csv |
|  |  |  |

## Auditing Feature

### Description

This feature is used to audit provisioning actions on the end systems. This is done via an after provisioning rule on every application and an after provisioning step in the Accelerator Pack Wrapper workflow “Workflow-FrameWork-Wrapper”.

### Accelerator Pack Configuration

By default, here is the list of Audit Configuration that is enabled.

* Accelerator PackLifecycle Event
* Accelerator Pack Lifecycle Certification Event
* Accelerator Pack Interactive Requests
* Accelerator Pack Operational Requests
* Accelerator Pack Background Service Requests
* Accelerator Pack Automated Assignment Event
* Accelerator Pack Policy Violation Requests
* Accelerator Pack Certification Revocation Requests
* Accelerator Pack Webservices Request

The out of th box Audit Configuration Link can be used to disable Accelerator Pack Audits

### As Built Configuration

<Please list all the audit changes that are applied to the object “**AuditConfig**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |

## Self Service Onboarding Wizard Feature

### Description

This feature is used to onboard applications using the “Self Service Onboarding” QuickLink.

### Accelerator Pack Configuration

* The Workgroup “ROAD” members needs to be configured to have access to this QuickLink
* The “Global Definition” QuickLink can be used to configure:
  + Hide and Show the following forms on the wizard
    - Joiner
    - Leaver
    - Mover
    - Native Change
    - Approval Access and Accounts
    - Privileged Account
    - Password Synchronization
    - Attribute Synchronization
    - New Account Entitlement Dependency
    - Policy Violation
    - Provisioning
    - Ticket Integration
    - Confirmation
  + Switch Onboarding Form Mode
    - Read Only
    - Read and Update
  + Add/Remove the list of connector names that support disable and lock operations internally. This is an exclusion list. Once configured, the Aggregation Feature form on the Self Service Onboarding Wizard **will not show** disable and lock fields during application onboarding. Here is the default list that is packaged with this feature:
    - **ADLDAPConnector**
    - **LoopbackConnector**
  + Add/Remove the list of connector names that require provisioning definition. This is an inclusion list. Provisioning definition means defining lock/unlock/enable/disable /password attributes, values, and LDAP operations. Once configured, the Provisioning Feature on the Self Service Onboarding Wizard **will show** the fields that connectors are configured for. Here is the default list that is packaged with this feature:
    - **LDAPConnector**

All these settings are stored in a custom object artifact called “**Custom-SmartServices-SelfService-Form-Settings**”

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Default Settings |
| roadReadOnly | Onboarding Form | False (Disabled) |
| roadJoiner | Joiner Feature | False (Enabled) |
| roadLeaver | Leaver Feature | False (Enabled) |
| roadMover | Mover Feature | False (Enabled) |
| roadNativeChange | Native Change Feature | False (Enabled) |
| roadAttrSync | Attribute Synchronization Feature | False (Enabled) |
| roadCartRequest | Approval Feature | False (Enabled) |
| roadAggregation | Aggregation Feature | False (Enabled) |
| roadPSA | Privileged Account Feature | False (Enabled) |
| roadPassword | Password Synchronization Feature | False (Enabled) |
| roadPolicyViolation | Policy Violation Feature | False (Enabled) |
| roadSSO | New Account Dependency Entitlements Feature | False (Enabled) |
| roadTicketintegration | Ticket Integration Feature | False (Enabled) |
| roadProvisioning | Provisioning Feature | False (Enabled) |
| roadConfirmation | Confirmation Page | False (Enabled) |
| roadSupportedAggregationDisableConnectors | Connectors that tag accounts with disable status internally | * ADLDAPConnector * LoopbackConnector |
| roadSupportedAggregationLockConnectors | Connectors that tag accounts with disable status internally | * ADLDAPConnector * LoopbackConnector |
| roadDefineProvisioningLockConnectors | Connectors that require provisioning definition for lock operation | * LDAPConnector |
| roadDefineProvisioningUnLockConnectors | Connectors that require provisioning definition for unlock operation | * LDAPConnector |
| roadDefineProvisioningDisableConnectors | Connectors that require provisioning definition for disable operation | * LDAPConnector |
| roadDefineProvisioningEnableConnectors | Connectors that require provisioning definition for enable operation | * LDAPConnector |
| roadDefineProvisioningPasswordConnectors | Connectors that require provisioning definition for password operation | * LDAPConnector |

### Built In Functionality

* QuickLink “Self Service Onboarding”
* Form and Workflow for Self Service Onboarding

### As Built Configuration

<Please list all the configuration changes that are applied to the object “**Custom-SmartServices-SelfService-Form-Settings**” for the [Customer]>

|  |  |  |
| --- | --- | --- |
| Property Name | Description | Settings |
|  |  |  |