

*IdentityIQ Accelerator Pack Self Service Wizard Feature*

Table of Contents

1. Overview 3

2. Initial Application Form 3

3. Aggregation Form Feature 3

4. Joiner Form Feature 5

5. Leaver Form Feature 7

6. Mover Form Feature 8

7. Native Change Form Feature 8

8. Attribute Synchronization Form Feature 8

9. Approval Form Feature 9

10. Privileged Account Form Feature 9

11. Password Synchronization Form Feature 10

12. Policy Violation Form Feature 10

13. New Account Dependency Entitlements Form Feature 11

14. Ticket Integration Form Feature 11

15. Provisioning Form Feature 11

16. Application Changes 12

**Document Revision History**

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

## Overview

The Self Service Wizard Feature built within the Accelerator Pack supports the configuration of the following features

* Aggregation
* Joiner
* Leaver
* Mover
* Native Change
* Attribute Synchronization
* Approval
* Privileged Account
* Password Synchronization
* New Account Dependency Entitlements
* Policy Violation
* Ticket Integration
* Provisioning

## Initial Application Form

All applications are shown on the form. In case, system scoping is enabled, only scoped applications will be shown to the user.

## Aggregation Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used to configure both authoritative and non-authoritative applications.

Authoritative applications can be configured for the following functions:

* Correlation Rule
  + Application Attribute: accountCorrelationAttrExpression
* Contractor Repository
  + Field Visibility is controlled by by the ObjectConfig Application Attribute: authoritativeNonEmployee
* Service Account Repository
  + Field Visibility is controlled by the ObjectConfig Application Attribute: authoritativeStudent
* Account Disable
  + Field Visibility is controlled by the QuickLink “Global Definition”, Exclude Connectors from Aggregation Disable Definition
  + Field Validation to ensure Disable Account Value is entered when Disable Account Attribute is selected
  + Application Attribute: accountDisableAttrExpression
* Account Lock
  + Field Visibility is controlled by the QuickLink “Global Definition”, Exclude Connectors from Aggregation Lock Definition
  + Field Validation to ensure Lock Account Value is entered when Lock Account Attribute is selected
  + Application Attribute: accountLockAttrExpression

Non-Authoritative applications can be configured for the following functions:

* Is Business Application
  + Field Visbility is controlled by ObjectConfig Application Attribute: busApp
* Correlation Rule
  + Application Attribute: accountCorrelationAttrExpression
* Account Disable
  + Field Visibility is controlled by the QuickLink “Global Definition”, Exclude Connectors from Aggregation Disable Definition
  + Field Validation to ensure Disable Account Value is entered when Disable Account Attribute is selected
  + Application Attribute: accountDisableAttrExpression
* Account Lock
  + Field Visibility is controlled by QuickLink “Global Definition”, Exclude Connectors from Aggregation Lock Definition
  + Field Validation to ensure Disable Account Value is entered when Disable Account Attribute is selected
  + Application Attribute: accountLockAttrExpression
* Privileged Account
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: privilegedAccountAttrExpression
  + Field Validation to ensure Privileged Account Value is entered when Privileged Account Attribute is selected
  + Application Attribute: privilegedAccountAttrExpression
* Privileged Entitlement
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: privilegedEntAttrExpression
  + Field Validation to ensure Privileged Entitlement Value is entered when Privileged Entitlement Attribute is selected
  + Application Attribute: privilegedEntAttrExpression
* Birthright Entitlement
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER FEATURE
  + Application Attribute: birthrightEntAttrExpression
  + Field Validation to ensure Birthright Entitlement Value is entered when Birthright Entitlement Attribute is selected
* Service Account
  + Field Visibility is controlled by ObjectConfig Application Attribute: serviceAccountAttrExpression
  + Field Validation to ensure Service Account Value is entered when Service Account Attribute is selected
* Service Account Name Generation
  + Field Visibility is controlled by ObjectConfig Application Attribute: apAppendApplicationName
* Service Account Name Generation Attribute Name
  + Field Visibility is controlled by ObjectConfig Application Attribute: apServiceAccountUniqueName

## Joiner Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Activate Joiner
  + Application Attribute: joinerEnabled
* Restore Only Primary Account on Rehire
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER REHIRE FEATURE
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: rehirePrimaryaccount
* Rehire Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER REHIRE FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: rehireProcess
* Birthright Population
  + Application Attribute: joinerPopulationRegex
* Birthright Roles
  + Read Only Field
  + Only displays Matching Profile Application Name Birthright Roles
  + Rule “Rule-Self-Service-Birthright-Roles” displays matching selected population birthright roles
  + Application Attribute: joinerRoles
* Reverse Leaver Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event REVERSE LEAVER FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: reverseleaverProcess
* Return to Work Leave of Absence Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER LOA FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: rtwloaProcess
* Return to Work Long Term Disability Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER LTD FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: rtwltdProcess
* Joiner Email Instructions
  + Value from Custom Artifact Custom-Framework-EmailTextMapping
    - Email Template: EmailTemplate-FrameworkJoinerManager
    - Request Type: JOINER FEATURE
    - Application: Selected Application
    - Operation:Create
* Joiner Password Email Instructions
  + Field Visibility is controlled by the QuickLink “Global Definition”, Separate Joiner Temporary Password Email
  + Value from Custom Artifact Custom-Framework-EmailTextMapping
    - Email Template: EmailTemplate-FrameworkPasswordJoinerManager
    - Request Type: JOINER FEATURE
    - Application: Selected Application
    - Operation:Create
  + Initial onboarding of an application, Password Field from Create Provisioning Policy is saved to Custom Artifact
  + Field Validation to ensure the Create Provisioning Policy is defined with the Password Field
* Rehire Email Instructions
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER REHIRE FEATURE
  + Value from Custom Artifact Custom-Framework-EmailTextMapping
    - Email Template: EmailTemplate-FrameworkJoinerManager
    - Request Type: JOINER REHIRE FEATURE
    - Application: Selected Application
    - Operation:Create
* Rehire Password Email Instructions
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event JOINER REHIRE FEATURE
  + Field Visibility is controlled by the QuickLink “Global Definition”, Separate Joiner Temporary Password Email
  + Value from Custom Artifact Custom-Framework-EmailTextMapping
    - Email Template: EmailTemplate-FrameworkPasswordJoinerManager
    - Request Type: JOINER REHIRE FEATURE
    - Application: Selected Application
    - Operation:Create
  + Initial onboarding of an application, the Password Field from Create Provisioning Policy is saved to Custom Artifact
  + Field Validation to ensure Create Provisioning Policy is defined with the Password Field
* Process Attribute Synchronization After Rehire
  + Application Attribute: apAfterRehireAttrSync
  + Field Visibility is controlled by Joiner Rehire and Attribute Synchronization Feature Enablement
    - LifeCycle Event JOINER REHIRE FEATURE
    - LifeCycle Event ATTRIBUTE SYNCHRONIZATION FEATURE

## Leaver Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions

* Move Account on Termination
  + Application Attribute: moveAccountContainer
* Leaver Options
  + Rule “Rule-Self-Service-Onboard-ApplicationLeaverOptions” displays all options that contains “Remove Entitlements”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard or If option doesn’t contain word “Remove”
  + Application Attribute: terminationProcess
* Postpone By X Days
  + Application Attribute: xDays
  + Field Validation to ensure value is required if selected “Leaver Options” field value contains “X Days”
* Postpone By X Days
  + Application Attribute: xDeleteDays
* Scramble Password Attribute Name
  + Application Attribute: scramblePasswordAttr
* Comment Attribute
  + Application Attribute: commentsAttr
* Comment Value
  + Application Attribute: commentsValue
* Leave of Absence Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event LEAVER LOA FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: loaProcess
* Long Term Disability Options
  + Field Visibility is controlled by Joiner Feature Enablement
    - LifeCycle Event LEAVER LTD FEATURE
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: ltdProcess
* Remove Entitlement Exception
  + Application Attribute: removeEntitlementLeaverExceptionExpression
  + Field Validation to ensure Entitlement Value is entered when Entitlement Attribute is selected

## Mover Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Mover Options
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: moverProcess
* Before Mover Options
  + Rule “Rule-Self-Service-Onboard-ApplicationOptions” displays all options except “Extended Rules”
    - Hide if “Extended Rules” is configured via Apllication Administrative Wizard
  + Application Attribute: beforemoverAccount
* Move Only Primary Account
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: beforemoverPrimaryaccount
* Automated Allow Exception Account Revocation Options
  + Field Visibility is controlled by Mover Feature Enablement
    - LifeCycle Event MANAGER CERTIFICATION ALLOW EXCEPTION FEATURE
  + Application Attribute: moverRevocation
* Process Attribute Synchronization Before Mover Certification
  + Application Attribute: apBeforeMoverAttrSync
  + Field Visibility is controlled by Mover and Attribute Synchronization Feature Enablement
    - LifeCycle Event MOVER FEATURE
    - LifeCycle Event ATTRIBUTE SYNCHRONIZATION FEATURE
* Process Joiner After Mover Certification
  + Application Attribute: apAfterMoverJoiner
  + Field Visibility is controlled by Joiner Rehire and Attribute Synchronization Feature Enablement
    - LifeCycle Event MOVER FEATURE
    - LifeCycle Event JOINER FEATURE

## Native Change Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following function:

* Native Change Options
  + Application Attribute: nativeChangeProcess

## Attribute Synchronization Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Authoritative and Non-Authoritative applications can be configured for the following functions:

* Synchronize Only Primary Accounts
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: primarySyncaccounts
* Rename / Move Move LDAP Account
  + Application Attribute: renameLDAPaccount
* Evaluate Create Provisioning Policy for Synchronization
  + Application Attribute: evaluateCreateprovpolicy
* Source Attributes
  + Read Only List
  + List of Identity Cube Attributes and CREATEPOLICY
* Target Attributes
  + Read Only List
  + List of Application Schema Attributes
    - Except Entitlement Attributes
* Source to Target Mappings
  + Field Validation to ensure
    - Source attribute matches either the Identity Cube Attribute or CREATEPOLICY
    - Target attribute matches the application schema attribute
    - Source and Target Attribute Mappings are separated by “:”
    - Mappings Saved to Custom Artifact Custom-FrameworkAttributeSyncMapping
    - Exclude “EXCH\_” source attributes validation

## Approval Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* 1st Level Business Approvers
  + Filter:Workgroup Name must start with application name
  + Application Attribute: appBusApprovers
* 2nd Level Business Approvers
  + Filter:Workgroup Name must start with application name
  + Application Attribute: additionalAppBusApprovers
* Request Form
  + Filter:Form Name must start with application name
  + Application Attribute: displayFormRule
* Request Form Role
  + Filter:Bundle Name must start with application name
  + Application Attribute: requestorFormRole
* Omit Manager's Approval for Privileged Access
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: omitmanagerPrivgaccess
* Validate Request for Privileged and Non-Privileged Access
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: enablepsaValidation

## Privileged Account Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition” and ObjectConfig Application Attribute: enablepswexpNotification. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Enable Password Expiration Notification
  + Application Attribute: enablepswexpNotification
* Password Reset After X Days
  + Application Attribute: xdaysresetPwd
* Password Expiration Application Attribute
  + Application Attribute: pwdexpAttr
* Password Before Expiration Days (Daily Notfications)
  + Application Attribute: beforepwdexpAttr
* Password After Expiration Days (Action on Account)
  + Application Attribute: afterpwdexpAttr
* After Password Expiration Options
  + Application Attribute: afterPassExpProcess
* Password Expiration Date Format Options
  + Application Attribute: pwdexpAttrexpression
* Scramble Password Application Attribute
  + Application Attribute: scramPwdattr

## Password Synchronization Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions

* Target Applications Password Creation / Modification Synchronization
  + Application Attribute: targetpasswordSync
* Detect Change Password on Primary Account
  + Field Visibility is controlled by Privileged Account Feature Enablement
    - ObjectConfig Application Attribute: primarypasswordSyncaccounts
* Is Enterprise Directory
  + Application Attribute: entDir

## Policy Violation Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Allow Access Request Policy Names
  + Filter:Policy Name must start with application name
  + Application Attribute: softPolicyviolations
* Deny Access Request Policy Names
  + Filter:Policy Name must start with application name
  + Application Attribute: hardPolicyviolations
* Multiple Accounts Policy Type Options
  + Application Attribute: policyType
* Single Entitlement Exceptions Artifact Name
  + Filter:Custom Name must start with application name
  + Application Attribute: policytypeExceptions
* Toxic Combinations Artifact Name
  + Filter:Custom Name must start with application name
  + Application Attribute: txCombinationName
* Eligibility Policy Violation Population Identification
  + Filter:Group Definition Name must start with application name
  + Application Attribute: eligibilityExpression

## New Account Dependency Entitlements Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Dependency Application
  + Application Attribute: accountCreateEntitlements
* Dependency Application Entitlements
  + Application Attribute: accountCreateEntitlements

**Please Note:** Both Field Values are concatenated and saved on an application for the attribute accountCreateEntitlements

## Ticket Integration Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Assignment Group Name
  + Application Attribute: assignmentGroupname
* Maximum Status Check on Ticket
  + Application Attribute:provisioningMaxStatusChecks
* Minutes Wait Between Status Checks
  + Application Attribute: provisioningStatusCheckInterval

## Provisioning Form Feature

This feature’s form visibility and read/write form mode is controlled via the QuickLink “Global Definition”. This is used for non-authoritative applications only.

Non-Authoritative applications can be configured for the following functions:

* Soft Delete
  + Set “deleteToDisable” property on Application’s ProvisioningConfig
* Maximum Retries
  + Application Attribute: provisioningMaxRetries
* Minutes Wait Between Retries
  + Application Attribute: provisioningRetryThreshold
* Retryable Errors
  + Application Attribute: retryableErrors
* LDAP Lock Attribute
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Lock Definition
  + Application Attribute: lockAttr
* LDAP Lock Value
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Lock Definition
  + Application Attribute: lockVal
* LDAP Unlock Attribute
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Unlock Definition
  + Application Attribute: unlockAttr
* LDAP Unlock Value
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Unlock Definition
  + Application Attribute: unlockVal
* LDAP Unlock Action
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Unlock Definition
  + Application Attribute: unlockAction
* LDAP Disable Attribute
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Disable Definition
  + Application Attribute: revokeAttr
* LDAP Disable Value
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Disable Definition
  + Application Attribute: revokeVal
* LDAP Disable Action
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Disable Definition
  + Application Attribute: revokeAction
* LDAP Enable Attribute
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Enable Definition
  + Application Attribute: restoreAttr
* LDAP Enable Value
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Enable Definition
  + Application Attribute: restoreVal
* LDAP Password Attribute
  + Field Visibility is controlled by QuickLink “Global Definition”, Incldue Connectors from Provisioning Password Definition
  + Application Attribute: passwordAttr

## Application Changes

Configurations done using the Self Service Onboarding Wizard save changes to following artifacts

1. Selected Application Object
   1. Extended and Non-Extended Attributes are saved on the application
   2. Rules are saved on application (Only if there are not any existing rules on the application)
      1. Customization Rule
         1. Rule-Framework-RapidAppOnBoarding-Customization-Rule
      2. Creation Rule
         1. Rule-FrameWork-Creation-Joiner-Authoritative-Source (Only for Authoritative Applications)
         2. Rule-FrameWork-Creation (Service Account Feature Enabled and Application is not Authoritative)
      3. Correlation Rule
         1. Rule-FrameWork-Correlation
      4. Managed Attribute Rule
         1. Rule-FrameWork-Promote-Managed-Attribute
      5. After Provisioning Rule
         1. Rule-AccountCreation-Dependency-Framework (Only if New Account Entitlement Depency Feature is configured)
         2. Rule-Audit-Framework
      6. PreIterate Rule (Only for Delimited File)
         1. Rule-FrameWork-Preiterate-DelimitedFile
2. Custom Object
   1. Joiner and Rehire Email and Password Instructions
      1. Custom-Framework-EmailTextMapping
   2. Attribute Synchronization Mappings
      1. Custom-FrameworkAttributeSyncMapping