Table of Contents

[1 Overview 2](#_Toc518380330)

[2 Simplified Logical Applications 2](#_Toc518380331)

[3 Business Application Access 2](#_Toc518380332)

[4 System Certification Item Rule 2](#_Toc518380333)

[5 Certification Exclusion Rule 2](#_Toc518380334)

[5.1 Certification Email Templates 3](#_Toc518380335)

[5.2 Certification Additional Recipient Rule 3](#_Toc518380336)

[5.3 Algorithm of Manager Certification Exclusion Rule 3](#_Toc518380337)

[5.4 Algorithm of Account Group Membership Certification Exclusion Rule 4](#_Toc518380338)

[5.5 Algorithm of Entitlement Owner Certification Exclusion Rule 4](#_Toc518380339)

.

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta |  |
| Version 2 | 6/1/18 |  | Cathy Mallet | Minor edit |

# Overview

The purpose of this document is to explain the Certification Feature that is packaged with Accelerator Pack. The feature requir some configuration in IdentityIQ for email templates, notification schemes and simplified logical applications. These configurations are outlined in the Accelerator Pack Implementation Guide.

# Simplified Logical Applications

There are three ways logical applications can be managed in IdentityIQ

* Logical Connectors
* Roles
* Extended Attributes

Accelerator Pack leverages extended attributes on roles and entitlements to manage logical applications. As a result, a custom artifact is used to include/exclude logical applications during ad-hoc or scheduled certifications. The logical applications originate from Infrastructure/Technology applications. The internal name of the attribute on the role is “appName” and on entitlements is “entAppName”.

**Please Note:** Multiple business application names can be stored on Infrastructure/Technology roles/entitlements using a comma separator. This can be used in cases where an entitlement or role is being shared across multiple Infrastructure/Technology applications. This is mostly seen in cases of technologies with multiple instances.

# Business Application Access

This is just a simple true or false value attribute on an application named “Business Application”. During the certification process, **all** access associated with business applications will be included on **manager certification** as compared to Infrastructure/Technology applications.

# System Certification Item Rule

There is a certification item rule that copies the logical application name from roles and entitlements to the certification item attribute “Custom1”. The name of the rule is “Rule-Framework-Certification-Item-Rule”.

Also, this rule copies the “entPrivileged” and “rolePrivileged” extended attribute values from entitlements and roles to the certification item attribute “Custom2”.

# Certification Exclusion Rule

There are three exclusion rules that are packaged with Accelerator Pack for various certifications types. Here is the mapping of exclusion rules for the certification types.

|  |  |
| --- | --- |
| Certification Type | Exclusion Rule |
| Manager | Rule-FrameWorkCertificationExclusionManager |
| Account Group Membership | Rule-FrameworkCertificationAccountGroupMembershipExclusion |
| Entitlement Owner | Rule-FrameworkCertificationEntitlementOwnerExclusion |

## Certification Email Templates

The following email templates can be selected during certification configuration. These email templates are packaged with Accelerator Pack

* EmailTemplate-Framework-CertificationDecisionChallengedNotification
* EmailTemplate-Framework-CertificationSignOffApproval
* EmailTemplate-Framework-ChallengeAccepted
* EmailTemplate-Framework-ChallengeCreationNotification
* EmailTemplate-Framework-ChallengeDecisionExpiration
* EmailTemplate-Framework-ChallengeExpiration
* EmailTemplate-Framework-ChallengePeriodEnd
* EmailTemplate-Framework-ChallengePeriodStart
* EmailTemplate-Framework-ChallengeRejected
* EmailTemplate-Framework-MitigationExpiration
* EmailTemplate-FrameworkAccessReviewBulkReassignment
* EmailTemplate-FrameworkAccessReviewDelegation
* EmailTemplate-FrameworkAccessReviewDelegationCompletion
* EmailTemplate-FrameworkAccessReviewDelinquent
* EmailTemplate-FrameworkAccessReviewReminder
* EmailTemplate-FrameworkAccessReviewStart

## Certification Additional Recipient Rule

The rule “Rule-FrameworkEmailRecipientCcFirstManager” can be defined on a certification escalation scheme. This rule copies escalation emails to the recipient’s manager. This rule is also packaged with Accelerator Pack.

## Algorithm of Manager Certification Exclusion Rule

* Exclusions
  + Excludes Privileged Roles and Entitlements, if this is configured to be excluded in the custom artifact “Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess” (detected using extended attributes “entPrivileged” and “rolePrivileged”)
  + Excludes Application’s Birthright Roles and Entitlements (detected using an extended attribute “isBirthright”)
  + Excludes Assigned RBAC Roles (assigned via assignment rules)
  + Excludes Logical Application Roles and Logical Application Entitlements for Infrastructure/ Technology Applications if no logical application is defined on them (if no value for an extended attribute “appName” on roles and no value for an extended attribute “entAppName” on entitlements)
  + Excludes Logical Application Roles and Logical Application Entitlements, if the logical application name does match the exclusion list
  + Excludes Logical Application Entitlement and Logical Application Role, if one of the logical application names separated by commas matches the exclusion list of logical applications from custom artifact “Custom-Framework-Exclusion-Logical-BusinessApplications-PrivilegedAccess”
* Inclusions
  + Include All Business Application’s roles and entitlements (detected using Boolean extended attribute “busApp”)
    - A Role is included if it has at least one business application defined on profiles
  + Includes Business Application accounts with no entitlements
  + Includes Logical Application accounts with no entitlements, if the logical application name does not match the exclusion list of logical applications
  + Includes Logical Application Entitlement and Logical Application Role, if the logical application name does not match the exclusion list
  + Includes Policy Violation, if configured

## Algorithm of Account Group Membership Certification Exclusion Rule

* Exclusions
  + Exclude Non-Privileged Access, If Certification is configured to show only privileged access
* Inclusions
  + Business Applications and Infrastructure/Platform applications will need to be manually selected using the certification setting “Certification Included Applications”

## Algorithm of Entitlement Owner Certification Exclusion Rule

* Exclusions
  + Exclude Non-Privileged Access, If Certification is configured to show only privileged access
* Inclusions
  + Business Applications and Infrastructure/Platform applications will need to be manually selected using the certification setting “Certification Included Applications”

## Algorithm of Application Owner Certification Exclusion Rule

* Exclusions
  + Exclude Non-Privileged Access, If Certification is configured to show only privileged access
* Inclusions
  + Business Applications and Infrastructure/Platform applications will need to be manually selected using the certification setting “Certification Included Applications”