

*IdentityIQ Accelerator Pack Best Practices*

## Overview

This document outlines the industry standards and best practices that are built into the Accelerator Pack program. Accelerator Pack was designed to allow customers to take advantage of preconfigured, best practice use cases that are recommended for SailPoint customers. Accelerator Pack provides the ability to get to production quicker and add more features and applications more effectively by ensuring customers follow our best practices. Each section of this document explains the reasoning behind each feature, and how it aligns with industry best practices, and why our customers should adopt these features that are part of Accelerator Pack.

## Approval Feature

This feature makes a clear distinction **between approvers and owners**.

* Owners are responsible for **certifying access and ensuring that no terminated identity has access** within an organization, from a governance perspective.
* Approvers are responsible for approving access and taking the responsibility for an identity who has been given access based on this approval. This is extremely important from auditing and security perspective. Approvers must be held **responsible** in case an identity who has approved access does anything malicious.
* Sometimes an organization’s governance practices are not mature enough to require a clear distinction between ownership and responsibility. In this case, Accelerator Pack has the flexibility to make approvers also be owners.

There is a maximum of five levels of approvals and a minimum of one level of approval within this feature. However, it is not usually recommended to have five levels of approval, for two reasons:

1. It is not easy to manage this many approval levels within the enterprise. It entails a lot of operational cost.
2. The enterprise needs to identify at least two approvers, from an auditing and security perspective. The approvers are responsible for any access that is being granted to an individual within enterprise. Having too many approval levels disrupts the whole concept of responsibility.

Based on industry best practices, there is no need to have more than three levels of approval. Here is the mapping of Accelerator Pack Levels with Industry Approval Levels.

The Data Custodian and Data Steward for an application play a huge role in data governance. Data Stewards are mainly responsible for content, quality, business controls related to compliance and governance, etc. Data Custodians are accountable and responsible for data audits, security, backups, restores, implementation of business controls, etc.

|  |  |
| --- | --- |
| Accelerator Pack Approval Level | Industry Standard Approvals |
| Manager Approval | Supervisor or Manager Approval |
| Application Approval Level 1 | Data Custodian Primary Level |
| Application Approval Level 2 | Data Custodian Secondary Level |
| Entitlement Approval Level 1/ Role Approval Level 1 | Data Stewardship Primary Level |
| Entitlement Approval Level 2 | Data Stewardship Primary Level |
| Service Owner Level 1  Or  Service Owner Level 2 | Service Account (Non-Interactive/Device/Shared Accounts) Primary Owner is either a Data Custodian or Data Steward  Service Account (Non-Interactive/Device/Shared Accounts) Secondary Owner is either a Data Custodian or Data Steward |

Here are some of the best practices that must be followed for approval levels:

1. Business Application Regular Account Access must have at least Manager approval; for example, a financial application’s business user access within a banking and insurance vertical, or an electronic medical records (EMR) application’s business user access within a health care vertical. Manager must own the responsibility of access for his/her direct reports. Data Custodian approval may be required in the case access may pose some security threats to the organization. Data Stewardship approval may be required in the case access is related to regulatory compliances from (PHI, PII, PCI, etc.)
2. Business Application Privileged Account Access must have Manager and Data Custodian or Data Stewardship approval; for example, a financial application’s administrative access within a banking and insurance vertical, or an electronic medical records application’s administrative access within a health care vertical.
3. Business Application Service Account Access must have one level of approval from the owner of the account; for example, non-interactive accounts to access records on the business application’s critical data via APIs.
4. Logical Business Application Regular Account Access must have Manager approval. These are the applications that are dependent on Infrastructure/Technology Authentication and Authorization. In some cases, it may require Data Custodian approval or Data Stewardship approval for same reasons as described above for Business Application Regular Account Access
5. Infrastructure / Technology Privileged Account Access must have Managers and Data Custodian or Data Stewardship approval for example data and server administrative access.
6. Infrastructure / Technology Service Account Access must have ownership approval from its owner either Data Custodian or Data Stewardship approval.

## Aggregation Feature

This feature **forces customers to classify and categorize data before aggregation**. This helps approvers, certifiers, and owners make the right decisions during approvals and certifications. At a high level, it offers following industry standards:

1. Provides 360-degree visibility of the **types** of accounts found in the application (e.g., regular, privileged, and service accounts).
2. Requires Infrastructure/Technology owners to classify or categorize access as birthright and privileged; for example, any Active Directory Security Group could be identified as birthright access, and Active Directory Security Group “Domain Admins” could be identified as privileged access.
3. Sets up industry standard approval levels and sets up **account type** certification campaigns.

## Certification Feature

This feature provides **complete visibility into accounts and their type of access, either regular or privileged,** to managers and owners on certification campaigns. This helps managers and owners to pay more attention to the privileged access during the certification campaign and not just rubber stamp the whole campaign. Organizations must train managers to certify the business application’s privileged access with utmost attention.

1. Manager certifies regular accounts and their regular access. This feature excludes Birthright and Automated RBAC (Role Based Control Access). Birthright access is excluded because this access is required for an Identity to be functional within an Organization to do his/her job. Automated RBAC Business Role access is excluded because this access gets added and removed based on assignment criteria that is established and agreed by an organization using Role Mining Tool. As organizations mature in the Automated RBAC model, the need for frequent manager certifications becomes very minimal and there is less access to certify because this access is automatically added and removed based on role based access control.
2. Entitlement and /or Application owners get complete visibility into privileged and regular access.
3. Advanced Certification Service Account owners certify only service accounts.
4. Any Requested/Approved RBAC Role is included in the certifications

## Joiner Feature

Birthright Roles are assigned automatically when someone joins the organization. Some examples of birthright applications are Active Directory, Exchange, etc. This is mainly done using IdentityIQ populations during a Joiner LifeCycle event. These roles are made up of Infrastructure/Technology profiles.

RBAC Business Roles are assigned either automatically using automated assignment criteria or using request access processes. For automated assignment, the assignment criteria is mined using IdentityIQ’s Role Mining tool. These roles are made up of Business and Infrastructure/Technology profiles.

This feature makes **a clear distinction between** **Business roles (RBAC Roles) and Birthright roles, and between Business and Infrastructure/Technology applications**. This encourages organizations to look at IAM implementation from RBAC perspective. The primary focus for Birthright Roles is automation for infrastructure/technology accounts and access, whereas the primary focus of RBAC Business Roles is geared towards least privileged access. Having a clear distinction between RBAC Business and Birthright Roles helps organizations to mature their IAM program with Role Based Access Control.

For Joiner Emails, this feature encourages and enables organizations to **send a welcome email for new account information, and a separate email with temporary password information**. Per industry standards, **it is advised to not to send the password and account in a single email unless the email is encrypted**.

## Leaver Feature

Per industry standards, all access must be removed when someone leaves the organization. This feature ensures all access is removed. All Accelerator Pack Leaver configuration options for an applications **have, at a minimum, the removal of access at the entitlement level.** This ensures that if the same identity comes back to the organization in either the same or a different position, access is re-requested, which will require approvals **again**. As a result, the approver takes the responsibility for rehired identities access. For Automated Birthright and RBAC Business Roles, access is reassigned without any approvals.

Any pending action item that is related to access (for example, certification or approval), and anything related to ownership in IdentityIQ, is very critical from a security perspective. Upon termination, this feature ensures all these critical items are acted upon appropriately.

1. All access request approval work items that are pending for the terminated identity’s decision are reassigned to the identity’s manager
2. All pending decisions on access requests for the terminated identity get canceled immediately
3. All Challenge Response Questions and Answers are cleared out
4. All IdentityIQ Items that are owned by the terminated identity are reassigned to the identity’s manager
5. Service Account ownership is reassigned to account owner’s manager

## Mover Feature

During a Mover campaign, manager can take three actions:

* Approve Access: This means keeping the selected access as it is on an application
* Deny Access: This means revoking the selected access on an application
* Allow Exceptions: This means keeping access, but only for certain time, on an application

This feature offers **Timely** **Automated Removal of “Allow Exceptions”** that are allowed on a Mover campaign. As a result, no one gets more access than what is required. This aligns with industry security standards and RBAC standards. From an access point of view, no one should have more access than what is required for their job.

## Mine Provisioning Policies Feature

This feature helps organizations to **discover** and build their account creation and modification polices. Organizations have large sets of applications and as a result, account creation and modification process requirements can be cumbersome and time consuming. This feature helps customers get started building the business processes used when creating and modifying accounts.

## Native Change Feature

This feature offers **Timely Automated Reversal of Native Changes,** which take place on a system integrated with IdentityIQ that are considered high risk to organization's security. Once IdentityIQ takes full control over an application’s access, any access-related changes outside IdentityIQ must be immediately acted upon.

## Create/Edit Identity Feature

For Non-Employee / Student creation, Accelerator Pack provide a UI to create these Identities using the **same Joiner Feature standards and processes**.

For service account creation, this feature **forces organizations to pick at least one owner who will be responsible for the service account**. Also, it ensures that IdentityIQ becomes an authoritative source for service account ownership, and regular access reviews on service accounts can be assigned to service account owners.

## Registration Feature

For Non-Employee / Student registration, the **same Joiner Feature standards are followed**.

## Privileged Account Feature

These accounts are correlated to Identity cubes that have regular/primary accounts. This feature **creates a segregation of access assignments between regular and privileged accounts**. As per industry standards, it prevents regular accounts from gaining privileged access, and provides functionality to **enforce more frequent password changes on privileged accounts**.

## Service Account Feature

This feature creates a separate Identity Cube for a service account. In this way, there is **complete request access visibility for that Identity Cube within IdentityIQ**. This feature ensures that there is **primary and secondary ownership on Non - Interactive / Shared /Device accounts.** In this way, if any malicious activities are performed by these accounts, there is someone to be held responsible and accountable.

## Change Password Feature

This feature makes a **clear distinction between managing service account passwords and changing enterprise passwords for regular accounts**. Enterprise users don’t understand the whole password synchronization process and want to have a single password to use. As a result, segregation of password management for service accounts and regular users is extremely important from the end-user’s perspective.

## Email Feature

This feature **ensures that emails from IdentityIQ are only sent to members of the Employee population**. Since employees are responsible for approving and certifying access, it is considered a risk to the organization if non-employees are receiving emails for approval and certification action items.

## Operations Feature

This feature offers four main functionalities.

* **Timely recovery of access that shouldn’t have been removed from the identity**. This is absolutely critical in the health care vertical, since access could be related to Electronic Medical Records and this may impact critical operations such as performing surgery on a patient.
* **Staging of automated events using temporary approvals**. This is a feature that serves as a safeguard in the first weeks of a deployment, when data quality is uncertain. In this situation, no one gets more access just because the system was not implemented properly. As organizations grow comfortable with the data and system processing, staging can be completely turned off.
* **Operational recovery mechanisms** where automated events can be kicked off manually.
* **Immediate Termination** that utilizes the Leaver Feature industry standards but is launched by a properly scoped admin from the UI.

## Batch Feature

This feature **allows organizations to enforce the same Identity Governance procedures during batch requests that are available during standard event-based processing**. Batch access requests follows same approval scheme that is used for cart requests. In this way, **IdentityIQ has complete visibility into access given to Non-Employees or Students**. In some cases, this feature is used for recovery. As a result, it allows the Operations team to bypass approvals.

## Persona Feature

This feature allows organizations, such as higher education and health care, to properly model and govern access where a single Identity may have more than one job function. With the Persona Feature, IdentityIQ **only removes access from a identity when all the relationships/personas of an Identity are terminated/dropped**. It generates **mover events when one of the relationship/persona is dropped**. As a result, it follows industry standards to ensure a identity doesn’t have additional access. It forces the Primary Manager to certify access and delegate/reassign access to secondary managers in case they don’t want to take responsibility on that. It generates **joiner events when a new relationship and persona is added to an Identity.** All the persona/relationship related LifeCycle events follow Joiner, Mover, and Leaver standards that are describe above.

## Entitlement Dependency Feature

This feature resolves account and authorization dependencies between Business Applications and/or IT/Infrastructure Technology. Here are two use case examples where this feature will be heavily used:

* Many Business Applications rely on IT/Infrastructure technology authorization. This creates a dependency between Business Application New Account creation and IT/Infrastructure Authorization
  + For example some Business Applications requires Active Directory Security Group Authroization for every new account on that application. Accounts cannot login to that application’s modules, portals, etc. without Active Directory Security Group Authorization
* This has become an industry norm. **Many SSO solution providers offer Unified Application Catalog** (for example, VMWare Workspace ONE Azure SSO, etc.). The Authorization on these Launchpads is basically having the application in their catalog. This creates a dependency between SSO Business Application Catalog Items and Business Application New Account creation
  + For example, SSO Launchpads (VMWare Workspace ONE, Azure Single Sign-On, etc.) requires business application to be automatically assigned to an Identity as catalog item on creation of new account on that business application

## Self Service Onboarding Feature

This feature provides an enterprise-centric view of the applications, which is the core to a full rapid onboarding process for an application. This allows organizations to **enforce standard access control options on every application that is on boarded into IdentityIQ**. Anything that falls outside of the standard option can be flagged as a security risk to the organization, or it may turn out to be an exception to the enterprise polices.

## Policy Violations Feature

This feature **helps organizations onboard their segregation of duties (SOD) as functions on access from different applications, in both a preventive and a detective fashion. During an access request, this feature offers both hard and soft preventive policies for an application**.

Hard-stop policies prevent people from gaining access which is not allowed by SOD. Soft-stop polices allow a requestor to submit requests that require approval. If approved, after some period of time this access gets revoked by the policy owner.

## Simplified Logical Applications Feature

Logical applications are business applications that are dependent on Infrastructure/Technology applications for authentication and authorization. Many organizations struggle with the problem of rapidly onboarding logical applications and ensuring that the proper security controls are applied. This feature **simplifies the whole concept of logical applications in IdentityIQ and doesn’t impose Role methodology on customers**. It uses metadata (extended attributes) on IT/Infrastructure technology entitlements to display business application names on certifications and access requests.

## Triggers Feature

Often, organizations change/upgrade their authoritative sources or migrate them to the cloud, as well as adding additional authoritative sources for certain sets of populations (such as non-employees and/or students in health care or higher education). Changes in authoritative sources and consolidation of contractor/non-employee population data is very common.

This feature **provides flexibility to organizations to allow them to change their event policies** **without any code change** in IdentityIQ, based on a change or addition of authoritative sources to the organization.

## Ticket Integration Feature

This feature helps organizations to define standards for application integration that require manual tickets for provisioning. It **encourages customers to create** **dedicated assignment groups in the ticketing system for each application**. As a result, it provides complete visibility into the provisioning part of the ticketing system, in terms of “who is doing what”.

Also, it provides hooks for post-ticket completion, where additional steps may be required for account and access provisioning to be considered fully complete.

## Epic SER Linking Feature

This feature is **required for any Epic Integration within the health care space**. Health care Providers must have SER (Scheduled Resource) assigned to them on the Epic employee record. This feature **links Epic Employee records and SER records** via the out-of-the-box Epic connector, based on Epic and SER authoritative sources.