Organization banner logo

Phase One

Implementation Design

for

HD Supply

DRAFT

**CONFIDENTIAL**

**FOR HD SUPPLY INTERNAL USE ONLY**

Table of Contents

[1. Document History 2](#_Toc1400783623)

[2. Project Overview 3](#_Toc1102163684)

[2.1. Assumptions 4](#_Toc515266060)

[2.2. Exclusions 4](#_Toc877794256)

[2.3. Design Constraints 4](#_Toc190862551)

[3. Logical Architecture 4](#_Toc1783823452)

[3.1. Logical Architecture – As-Is 5](#_Toc1811876216)

[3.2. Logical Architecture – To-Be 5](#_Toc1313055183)

[4. IdentityIQ Deployment Architecture 6](#_Toc592551628)

[4.1. Single Facility Architecture: Standard "2 Tier" Enterprise Web Application Architecture 7](#_Toc925468222)

[5. IdentityIQ Deployment Configuration 10](#_Toc856719385)

[5.1. Branding 11](#_Toc935761033)

[5.2. Login Configuration 11](#_Toc604388675)

[5.3. Identity Attributes 13](#_Toc1426799354)

[5.4. IdentityIQ Application Access Control 13](#_Toc942611028)

[5.5. Audit Configuration 14](#_Toc57558055)

[6. Email Templates 18](#_Toc1255673283)

[6.1. EMT01: Mandatory: Contractor Compliance Program Checklist 19](#_Toc1235798811)

[6.2. EMT02: Manager Mail (User Onboarding) 20](#_Toc1411434455)

[6.3. EMT03: Manager Mail (Contractor Offboarding) 20](#_Toc980499564)

[6.4. EMT04: Contractor Expiration Reminders (On Day 30,14,7,6,5,4,3,2,1) 20](#_Toc173165132)

[6.5. EMT05: Approval Email 21](#_Toc79240313)

[6.6. EMT06: Requestor Email 22](#_Toc161136401)

[6.7. EMT07: Service Account/Non-Person Account Creation 22](#_Toc157108960)

[6.8. EMT08: Privileged Account Creation 23](#_Toc453966148)

[6.9. EMT09: AD Group Creation 23](#_Toc1646906810)

[7. Application Configuration 24](#_Toc1430863479)

[7.1. Workday 24](#_Toc593992191)

[7.2. Active Directory 28](#_Toc1513235182)

[7.3. Microsoft Entra ID 42](#_Toc433251954)

[7.4. Salesforce 47](#_Toc1596101665)

[7.5. SAP GRC 50](#_Toc1661099765)

[7.6. CyberArk 59](#_Toc818578717)

[8. Life Cycle Events 61](#_Toc1273783425)

[8.2. Pre-Hire 61](#_Toc1480332483)

[8.3. Joiner 62](#_Toc1875871562)

[8.4. Mover 63](#_Toc1723767955)

[8.5. Leaver 64](#_Toc1615596848)

[8.6. C2Hire 70](#_Toc1405269892)

[8.7. Rehire 71](#_Toc1136173950)

[8.8. LOA 72](#_Toc1872318144)

[8.9. ReturnFromLOA 73](#_Toc400893747)

[9. Contractor Management 74](#_Toc1964630530)

[9.1. Quick Link 75](#_Toc1172786498)

[9.2. Workflow Steps 75](#_Toc1960972458)

[9.3. HDS-Select Operation 76](#_Toc1559220240)

[9.4. New contractor 76](#_Toc628421892)

[9.5. Edit/Extend/Terminate Existing Contractor 78](#_Toc583222006)

[9.6. HDS Contractor Submit Request 79](#_Toc1066170177)

[10. Service Account Management 79](#_Toc824168617)

[10.1. Identify/Load Service Accounts 79](#_Toc307198496)

[10.2. Service Account Provisioning Policies 82](#_Toc477106230)

[10.3. Request Service Account 83](#_Toc790033488)

[10.4. Modify Service Account 85](#_Toc1764745489)

[10.5. Manage Service Account 87](#_Toc2132387585)

[10.6. Request Service Access 88](#_Toc1893069837)

[11. Privileged Account Management 88](#_Toc624404724)

[11.1. Privileged Account Provisioning Policies 89](#_Toc1182108068)

[11.2. Request Privileged Account 90](#_Toc974123714)

[12. Group Management 92](#_Toc1235638534)

[12.1. Create New Group 93](#_Toc27350065)

[12.2. Change Group Owner 95](#_Toc1354674979)

[13. Security/Legal Hold 97](#_Toc956686830)

[14. Out of Office 100](#_Toc645105518)

[15. Roles 102](#_Toc1021483077)

[15.1. IT\_Role 103](#_Toc1733241575)

[15.2. Business Role 103](#_Toc1643842752)

[16. Role Importer 103](#_Toc1498073600)

[17. Reports 104](#_Toc1779180879)

[17.1. Custom Reports 105](#_Toc417202773)

[18. Request Access 105](#_Toc2029074431)

[19. Certifications and Access Reviews 106](#_Toc1470125651)

[20. Task Configuration 107](#_Toc363040405)

[20.1. Aggregations 107](#_Toc132791031)

[20.2. Aggregation Tasks 109](#_Toc700038353)

[20.3. Task Scheduling 118](#_Toc565185644)

[21. Appendix 119](#_Toc742485648)

[21.1. Identity Attribute Matrix 120](#_Toc404422102)

[21.2. References 121](#_Toc1028709964)

[21.3. Audit Configuration 122](#_Toc430422536)

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Editor | Notes |
| 0.1 | 22/04/2024 | Kumar Gaurav | Initial draft |
| 0.2 | 23/05/2024 | Jitesh Jain | Edit & Review |
|  |  |  |  |

# Project Overview

CyberSolve will provide technical services to design, install, and integrate SailPoint IdentityIQ (IIQ) software with HD Supply systems and associated processes enabling comprehensive Identity & Access Management (IAM) capabilities. CyberSolve will work directly with HD Supply staff to complete the following:

* Design, architect, and implement IdentityIQ in the Dev, QA, and Production environments
* Integrations configured for:
  + Workday
  + Active Directory
  + Active Directory Privileged
  + Microsoft Entra ID
  + Salesforce
  + SAP GRC
* Workflows configured for:
  + Joiner
  + Mover/Transfers
  + Leaver
  + C2Hire
  + Reinstate
  + Contractor Management
  + Secondary Account Management
  + Group Management
  + Security Hold
  + Out of Office

## Assumptions

* The application team would provide the required support for this integration promptly.
* Trusted source (Workday) will provide clean and complete data feed.

## Exclusions

1. This design excludes the following integrations which might have been implemented on AD+ currently:
   1. RightFax
   2. Mobile Devices
   3. Drive Mappings
   4. Mail Forwarding
   5. AutoBill TXT BKP
   6. Bitlocker Recovery Keys
   7. SailPoint does not support adding photos to Identity Cube.

## Design Constraints

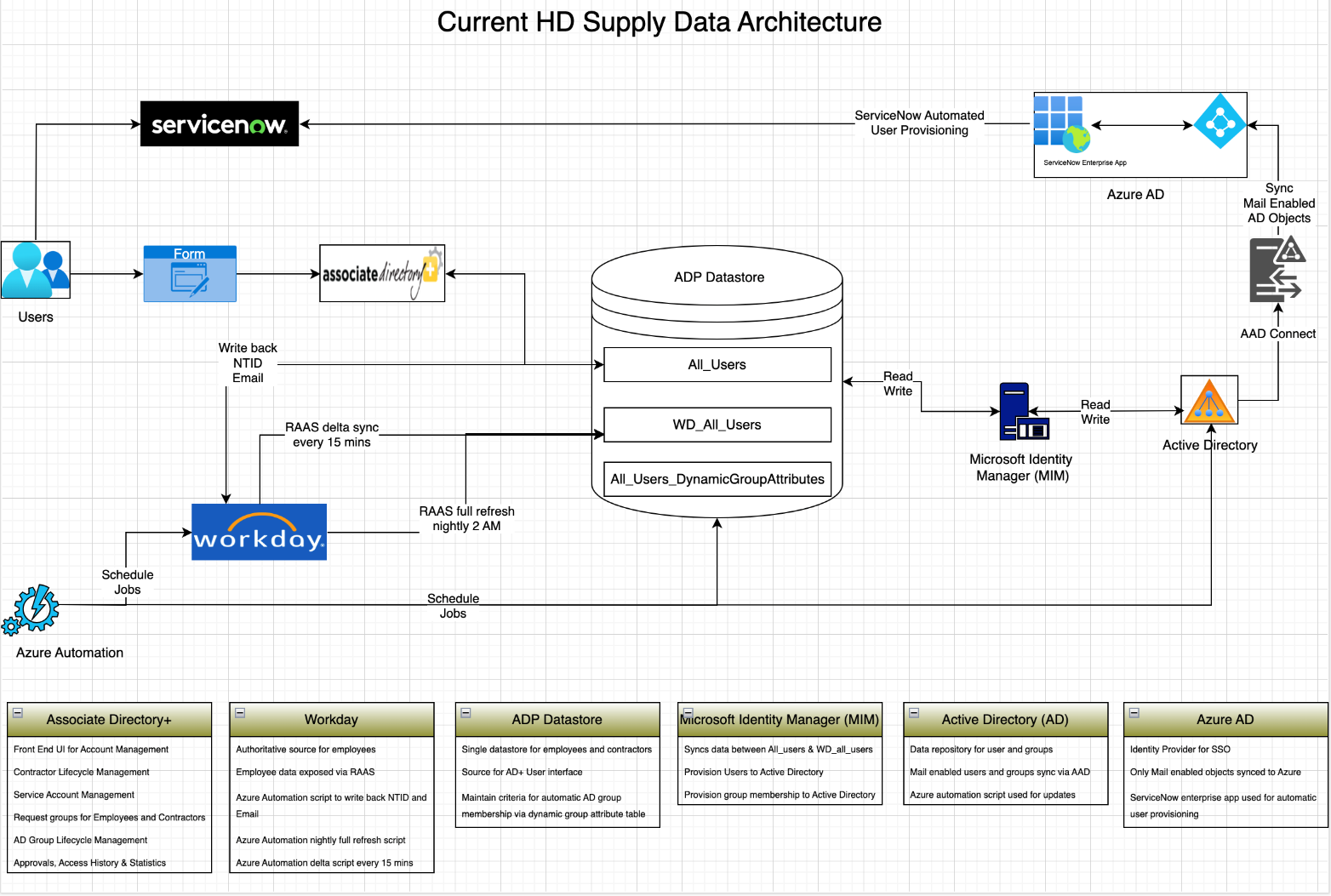
1. SailPoint Connectors: The implementation will be constrained by the available options for integration with authoritative and target applications. In some cases, these connectors can be modified to expand their capabilities using available API.

# Logical Architecture

The diagrams below illustrate the high-level integration points between IdentityIQ and its associated upstream and downstream systems for the current phase. These diagrams also include some contextual information for internal IdentityIQ application functions. These same diagrams will apply for each respective IdentityIQ environment (Dev, QA, and Production) with the only difference being the number of servers in each respective pool.

## Logical Architecture – As-Is

This diagram below illustrates the current state of HDS applications and tools used for Identity Life Cycle Management. One of the goals for this project is to phase out existing tools and replace them with newer IGA technologies using tools like SailPoint IdentityIQ.



## Logical Architecture – To-Be

This diagram below illustrates the future state of HDS IGA applications and flow of data between various systems.

A diagram of a company's supply chain

Description automatically generated

# IdentityIQ Deployment Architecture

Many different deployment architectures can be used with Java applications like IdentityIQ. Some of those architectures are recommended for IdentityIQ deployments, some are not recommended, and some are not supported at all.

These response-time statistics apply to any selected architecture as benchmarks for system performance:  
Average round-trip ping time for a 1k data block from all application servers to the database should be 300 microseconds or less

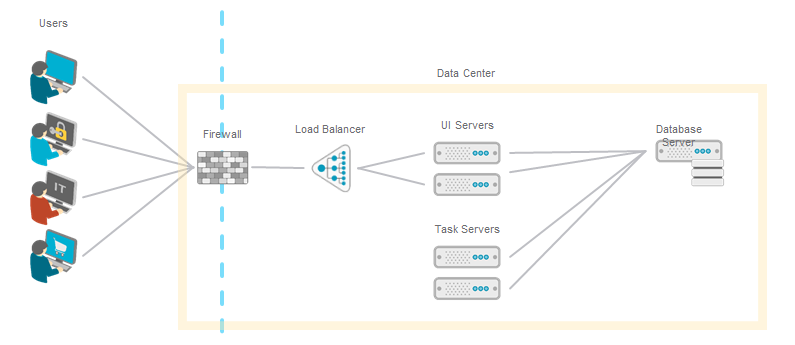
* Average round-trip commit time for a 1k data block should be 9ms or less
* Average round-trip commit time for a 4k data block should be 17ms or less
* Average round-trip commit time for an 8k data block should be 20ms or less

**NOTE**: If you are deploying IdentityIQ in the cloud, most of these recommendations are still relevant, but there are some variances.  Refer to [IdentityIQ on AWS - Performance and Architecture Recommendations](https://community.sailpoint.com/t5/Other-Documents/IdentityIQ-on-AWS-Performance-and-Architecture-Recommendations/ta-p/75218) and [IdentityIQ on Azure - Architecture and Performance Recommendations](https://community.sailpoint.com/t5/Other-Documents/IdentityIQ-on-Azure-Architecture-and-Performance-Recommendations/ta-p/74073) for more details for that scenario.

**NOTE:** Containerization does not affect these recommendations. If the OS version, JVM version and Servlet container requirements align with recommendations, the containerized server deployment is supported.  Therefore, when you see the word "server" in the following discussion and diagrams you can assume it means "server or container".  Refer to [Best Practices: Containerized IdentityIQ Deployments](https://community.sailpoint.com/docs/DOC-12543)  for more details.

HD Supply will be using Single Facility Architecture: Standard "2 Tier" Enterprise Web Application Architecture for deployment of IdentityIQ.

## Single Facility Architecture: Standard "2 Tier" Enterprise Web Application Architecture



This is what JEE architects call a “two tier enterprise web application architecture.”  It separates the users from the web servers with a firewall.  It does not separate the application servers from the relational database with any LAN or WAN network traversal.  All network components, including the UI Servers, Task Ethernet, or faster network segment.  This type of architecture IS RECOMMENDED for use with IdentityIQ.  Successful and performant IdentityIQ installations use single-facility architectures like this. Servers, and Database Server, reside in the same data center, preferably on the same Gigabit.

HD Supply IdentityIQ Servers

Below table list the server and infrastructure used for HDS IdentityIQ deployment.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Environment Type | Hostname | IP Address | Purpose | OS | CPU | RAM (GB) | Storage (GB ) |
| DEV | cfmslpiq01wd0s.hds.hdsupply.com | 10.244.64.236 | IQService | Windows Server 2022 Standard | 8 | 8 | 50 |
| DEV | cfmslpiq02wd0s.hds.hdsupply.com | 10.244.65.48 | SSB | Windows Server 2022 Standard | 8 | 8 | 50 |
| DEV | cfmsailpt01ld0s.hdsupply.net | 10.244.65.100 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| DEV | cfmsailpt02ld0s.hdsupply.net | 10.244.65.101 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| DEV | cfmsailpt03ld0s.hdsupply.net | 10.244.65.102 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| DEV | cfmsailpt04ld0s.hdsupply.net | 10.244.65.103 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| DEV | Iiqdevdb.hds.hdsupply.com | 10.244.64.164 | IIQ Databases | GCP Compute Engine MSSQL 2019 | 16 | 64 | 500 |
| QA | cfmslpiq01wqas.hds.hdsupply.com | 10.244.65.79 | IQService | Windows Server 2022 Standard | 8 | 8 | 50 |
| QA | cfmslpiq02wq0s.hds.hdsupply.com | 10.244.64.51 | IQService | Windows Server 2022 Standard | 8 | 8 | 50 |
| QA | cfmsailui01lq0s.hdsupply.net | 10.244.68.122 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| QA | cfmsailui02lq0s.hdsupply.net | 10.244.68.123 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| QA | cfmsailpt01lq0s.hdsupply.net | 10.244.68.120 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| QA | cfmsailpt02lq0s.hdsupply.net | 10.244.68.121 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| QA | iiqqadb.hds.hdsupply.com | 10.244.64.136 | IIQ Databases | GCP Compute Engine MSSQL 2019 | 16 | 64 | 500 |
| PROD | cfmslpiq01wp0s.hds.hdsupply.com | 10.244.1.112 | IQService | Windows Server 2022 Standard | 8 | 8 | 50 |
| PROD | cfmslpiq02wp0s.hds.hdsupply.com | 10.244.1.149 | IQService | Windows Server 2022 Standard | 8 | 8 | 50 |
| PROD | cfmsailui01lp0s.hdsupply.net | 10.244.3.246 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| PROD | cfmsailui02lp0s.hdsupply.net | 10.244.3.247 | IIQ UI | RHEL 8.9 | 4 | 16 | 70 |
| PROD | cfmsailpt01lp0s.hdsupply.net | 10.244.3.244 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| PROD | cfmsailpt02lp0s.hdsupply.net | 10.244.3.245 | IIQ Task hosts | RHEL 8.9 | 4 | 16 | 70 |
| PROD | iiqproddb.hds.hdsupply.com |  | IIQ Databases | GCP Compute Engine MSSQL 2019 | 16 | 64 | 500 |

# IdentityIQ Deployment Configuration

## Branding

The IdentityIQ user interface can be customized to include custom corporate branding, giving the application a look and feel that matches other enterprise applications. The files modified to implement custom branding in IdentityIQ are located under the IdentityIQ installation directory. Common alterations to default branding include updating logos and altering the color scheme.

### Branding at HD Supply

* Alternate color scheme by performing the following customizations in the /ui/css/ui-custom.css file:
  + Primary Color – Updated to #FFCC33
  + Primary Color (accent) – Updated to #FFCC33
  + Secondary Color – Updated to #FFCC33
  + Secondary Color (accent) – Updated to #FFCC33
* Alternate Logos by performing the following customizations:
  + TopLogo1:



* + loginLogo:



## Login Configuration

User access to the IdentityIQ application is controlled through an authentication process in which the user’s sign-on credentials are validated against an authentication source. The IdentityIQ web application can be configured by a system administrator or implementer to perform this authentication in one of three ways:

* Internal IdentityIQ authentication (default)
* Pass-Through Authentication (PTA)
* Single Sign-On (SSO)

By default, IdentityIQ authenticates users against its internal user identity records with passwords stored in IdentityIQ. However, Pass-Through Authentication and Single Sign-On can be enabled and configured through the IdentityIQ user interface. In fact, IdentityIQ is not limited to using just one authentication mechanism at a time; multiple authentication methods can be used together in a "failover" configuration.

### Authentication Method Processing Order

IdentityIQ attempts to authenticate users by all enabled methods before reporting login failure to the user. The methods are executed in this order (skipping any disabled methods):

1. Single Sign On (Rule-based or SAML)
2. Pass-Through Authentication
3. Internal IdentityIQ Authentication

### SSO Authentication

IdentityIQ supports two (2) different options for single sign-on (SSO) configuration: rule-based and Security Assertion Markup Language (SAML). SSO streamlines the login process for users even further than pass-through authentication by allowing the user to bypass signing in to each system entirely, once they have completed the initial sign-on to the authenticating application.

#### Rule-Based Single Sign-On

In rule-based Single Sign-On (SSO) configurations, when the user accesses the IdentityIQ web application, the authentication source recognizes it as a secure resource, requires the user to authenticate to it (if the user has not already done so), and passes a “token” containing contextual information in the HTTP header to IdentityIQ. The SSOAuthenticationRule validates that information and maps the user to the appropriate IdentityIQ Identity.

The diagram below is a visual representation of the rule-based Single Sign-On authentication process for IdentityIQ:

Diagram

Description automatically generated

#### SAML Single Sign-On

In SAML SSO, the authorization request can be initiated with the Service Provider (i.e., the application itself: IdentityIQ) or with the SSO authentication application (known as the Identity Provider). In either case, the Identity Provider handles authentication of the user and provides a signed XML <Response>, or Assertion. This response contains information that IdentityIQ can match to an identity to determine the user's proper authorization to IdentityIQ functionality.

This diagram illustrates how IdentityIQ interacts with the Identity Provider to authenticate users in the case of an IdP-initiated request:

Diagram

Description automatically generated

### Pass-Through Authentication

With Pass-Through Authentication, the user logs in to the IdentityIQ application through the normal IdentityIQ login page but the system validates the user’s credentials against an external source, “passing” the ID and password “through” to the authorizing system instead of consulting IdentityIQ’s internal records.

Once validated, the user account is mapped to an IdentityIQ Identity to complete the login process. The external source is commonly an LDAP directory or Active Directory. Maintaining a single repository against which all corporate systems validate user logins allows the company’s employees to access all of their corporate systems with a single username and password combination instead of having to keep track of separate usernames and passwords for each application.

The diagram below is a visual representation of the Pass-Through Authentication process for IdentityIQ:

Diagram

Description automatically generated

### Login Configuration at HD Supply

HD Supply IdentityIQ instance will be configured to use HD Supply Single Sign-On (SSO). HD Supply users will authenticate into Azure AD identity provider, then federate into IdentityIQ to perform their tasks. Upon authentication from IDP (Azure AD), the SAML token will be generated and map to an identity. This means to sign-on to IdentityIQ, a user will need both an account in Azure AD, the appropriate permission and an Identity in IdentityIQ.

Azure AD will be onboarded to the IGA Solution as a downstream system, and an account in Azure AD will be considered a birthright access for all Identities.

It will be making use of Azure Active Directory SAML Authentication to provide all identities authentication to IdentityIQ.

As authentication provider is Azure AD, inactive users should be blocked at Azure AD. It is assumed that when AD account is disabled, account is synced to Azure AD and the associated Azure AD account of the leaver is made inactive making it impossible to authenticate to Azure AD.

## Identity Attributes

Please see the “Identity Attribute Matrix” section of the Appendix for an in-depth review of the identity attributes in IdentityIQ and their associated mappings from upstream systems to downstream systems.

## IdentityIQ Application Access Control

IdentityIQ uses a security model based on rights that are granted to users to control access to product features. These rights (also called SPRights) turn on or off menus, tools, pages, and tabs in the UI, and thus can limit the actions users can take within IdentityIQ.

Capabilities group one or more access rights within IdentityIQ and are used to group rights logically by job function, streamlining their assignment to users or workgroups.

Rights tend to be limited and granular, and are often used in combination to provide full access to a feature or area of the UI. The granular nature of rights helps administrators fine-tune access—allowing them, for example, to give read-or-view-only privileges to some users in a given feature, but to allow other users full access to that feature, including creating, editing, and deleting data.

There are several ways capabilities can be assigned to users, or used in other ways in IdentityIQ:

* Identities can have capabilities assigned directly to them. This is done via Identities  Identity Warehouse  User Rights tab.
* Workgroups can have capabilities assigned to them and users who are members of the workgroup inherit the capabilities. This is done via Setup  Groups  Workgroups tab.
* Certifications can include the capabilities assigned to users as part of the access being reviewed and certified.
* Quicklink Populations can include assigned capabilities as part of their membership criteria; in other words, you can create Quicklink Populations (dynamic scopes) based on assigned capabilities.

### IdentityIQ Application Access Control at HD Supply

For the current phase, there will be two (2) groups of users: end users and administrators. To that end, we will leverage two (2) mechanisms to provide these two groups with their required level of access, QuickLink Populations, and Workgroups. Following these two mechanisms, as opposed to manually granting access to user’s identities directly, allows for more streamlined review and administration of IdentityIQ platform access and is in-line with best practices.

#### End Users

Your typical end users will be permitted to login to the IdentityIQ platform and be able to perform a small set of operations against their own identity and, if they are a manager, will be permitted to perform a small set of operations against the users that report to them based on the data from your authoritative source systems.

#### Administrators

To ensure IdentityIQ administrators could review data across the platform and perform any required technical operations tasks, a workgroup will be created which will be assigned the “SystemAdministrator” Capability. This means that any user who is a part of this workgroup will be granted full administrative rights to the IdentityIQ platform.

#### Workgroup Matrix

|  |  |  |
| --- | --- | --- |
| Workgroup Name | Capabilities | Description |
| HDS Administrators | System Administrator | This workgroup grants all members full administrative privileges to the IdentityIQ platform. |

## Audit Configuration

IdentityIQ can capture audit records on a variety of actions which occur in the system. Each installation may have different requirements for the types of activities that need to be audited, so IdentityIQ provides auditing flexibility through system configurations.

The built-in auditing options can be turned on and off through the IdentityIQ user interface on the Audit Configuration page. Additional audit records can be added programmatically by rules and workflows.

In addition to true audit events, IdentityIQ also logs system messages, provisioning transactions, and can be configured to automatically purge system data after a configurable period of time. While not all object types can be configured for automated data retention adherence, the vast majority of those critical to a typical IdentityIQ installation can be configured in this manner.

Refer the list of audit actions, along with their associated descriptions, in [Audit Configuration](#_Audit_Configuration) in Appendix section, that captures the out-of-the-box options for auditing in IdentityIQ.

### Provisioning Transactions

IdentityIQ 7.1 introduced a new administrative user interface page where administrative users (those with the System Administrator capability in IdentityIQ) can view data about provisioning transactions which have occurred in the IdentityIQ installation (whether from an automated process, a request, or a certification decision). This page can optionally display all provisioning transactions which are processed through IdentityIQ.

By default, the Provisioning Transactions table only displays failed provisioning transactions because the Provisioning Transactions log is configured to only store failures.

To change this configuration:

* Navigate to the Gear menu  Global Settings  IdentityIQ Configuration  Miscellaneous page.
* In the Provisioning Transaction Log Settings section, change Maximum Log Level to Retry or Success.
  + Retry means the system will log provisioning transactions that return a Failure result or a Retry result (an error message indicating a temporary condition that means a later retry of the provisioning operation will likely succeed and should therefore be auto-retried after a delay interval).
  + Success means the system will log all provisioning transactions, regardless of their provisioning result status values.

When setting Maximum Log Level to Success, the provisioning transaction log will record high volumes of records. Consequently, it is particularly important in that case to also set the Days before provisioning transaction event deletion value to the number of days you want to retain these records so they will be automatically purged after that time. Leaving that attribute as the default "0" means these records will never be deleted by the system, which would fill your database quickly. Even when using a Retry or Failure maximum log level, this value should be set to purge records you no longer need.

#### Provisioning Transaction at HD Supply

Taking each of these points into consideration, along with the positives of having a full set of provisioning transaction data available, it is our recommendation to configure the Provisioning Transaction Table to store data for all transactions (set Maximum Log Level to “Success” and check the Enabled Provisioning Transaction Log box) and to have this data pruned after being stored for sixty (60) days (set Days before provisioning transcation event deletion to “60”):

Graphical user interface, text

Description automatically generated

This will allow administrators to reference historical data for a reasonable period of time to support any incidents that come up but will be pruned often enough where it should not impact overall platform performance.

### SysLogs

IdentityIQ as an application is configured to write events out to a log file on each server running IdentityIQ. In addition, IdentityIQ can also be configured to store these events in its internal database for future reference.

Long term, it is best practice to read and store these logged events into a central Security Information & Event Management (SIEM) tool of some kind for any future reporting purposes.

In the near term, it is our recommendation to enable Syslog storage at the “Error” level with a retention period of sixty (60) days to match the suggested retention period for Provisioning Transactions (as described above):

Graphical user interface, application

Description automatically generated

### Audit Events

IdentityIQ can capture audit records on a variety of actions which occur in the system.

The built-in auditing options can be turned on and off through the IdentityIQ user interface on the Audit Configuration page. Additional audit records can be added programmatically by rules and workflows.

Out-of-the-box, IdentityIQ is configured to maintain audit records around events that are most often critical to track and report against for organizations of various industries. As an example, IdentityIQ is configured out-of-the-box to maintain audit records around Access Request events including who made the original request, who the request was for, and who approved the request.

In addition to the events enabled out-of-the-box, we recommend enabling audit tracking for the following General Actions:

* Login Failure
* Import File
* Email Sent
* Email Failure

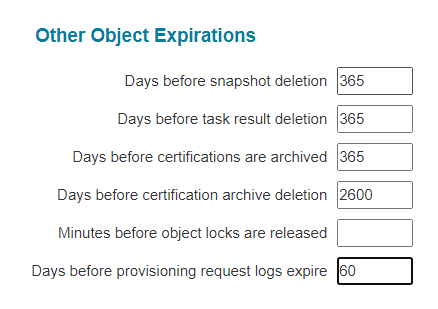
We recommend enabling these specific events primarily to support administrators and their ability to evaluate end user incidents and perform other operations specific activities.

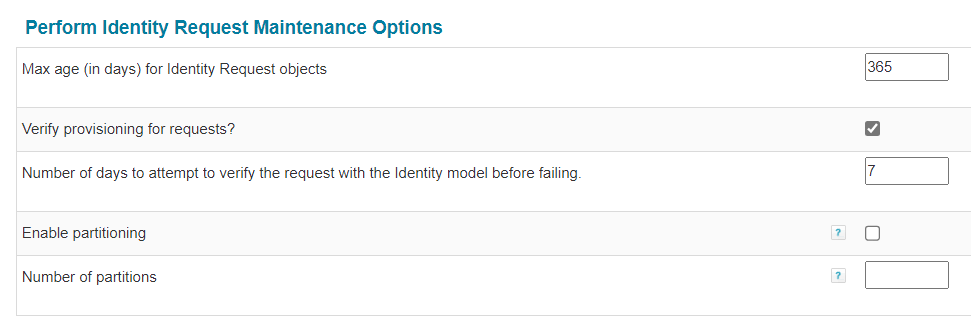
It is important to note that Audit data accumulates in the system indefinitely. There is no task or option to prune this data.  Depending on your data retention requirements, you can create a custom task to prune the data, or manually prune this table using a simple SQL query to archive and delete the old records every X days.

Other actions can and should be enabled as new functionality is deployed to the IdentityIQ platform. For more information regarding what options are available to audit out-of-the-box, please see the “Audit Configuration” section of the Appendix.

### Other Data Retention

In addition to Audit Events, SysLogs, and Provisioning Transactions, IdentityIQ can also be configured to automatically prune a subset of object types after a configurable amount of time. While a few of these settings will not be used until future phases, it is recommended that we configure the “Other Object Expirations” portion of the product and Max age (in days) for Identity Request objects in Perform Identity Request Maintenance task as follows:





These settings should be reviewed in greater detail before deploying any access certification related functionality.

# Email Templates

## EMT01: Mandatory: Contractor Compliance Program Checklist

| When | Contractor identity is created |
| --- | --- |
| From | SailPoint |
| To | User’s HD supply email and User’s contractor company email |
| Cc | Manager and infoseccompliance@hdsupply.com |
| Subject | Mandatory: Contractor Compliance Program Checklist |
| Body | Display Name: ${display name}  As part of the on-boarding process for HD Supply contractors, you are required to complete all assigned security awareness training courses, and review all relevant HD Supply policies within 30 days of on-boarding. Your hiring manager is obligated to ensure that you complete your training as soon as possible.   * Please visit the [Contractor Compliance](https://hdsnprd.service-now.com/myportal?id=mp_kb_article_view&sys_kb_id=d193cdaddb515f84937151295e961937) page on MyPortal to review and initiate the required tasks that you will need to complete. It is recommended that you complete the tasks in the order presented. * Access to the Proofpoint training portal will be automatically provisioned for you by the HDS Information Security team. A separate welcome email will be sent to your HD Supply email address with directions on accessing the portal. Please send an email to [infoseccompliance@hdsupply.com](mailto:infoseccompliance@hdsupply.com) if you don’t receive the welcome email from the HDS InfoSec team with a link to the platform within 48 hours. * Attest to completion of the review of all policies and training material within the Proofpoint attestation form presented upon successful completion of your Proofpoint training. * Any questions or concerns regarding this policy, or any related information-security policies or issues, should be directed to the Information Security Team, by email to [infosec@hdsupply.com](mailto:infosec@hdsupply.com).   **Note:** These requirements must be followed by all contractors. You may be subject to disciplinary action, up to and including termination of network access, if these requirements are not followed. Any exceptions to this policy must be approved by your engagement/hiring manager.  THIS IS AN AUTOMATED MESSAGE, DO NOT REPLY DIRECTLY TO THIS MESSAGE AS IT IS SENT FROM AN UNMONITORED MAILBOX |

## EMT02: Manager Mail (User Onboarding)

| When | User is onboarded to SailPoint |
| --- | --- |
| From | SailPoint |
| To | Manager |
| Subject | New {Employee/Contractor} Account Details: ${Display Name} |
| Body | New {Employee/Contractor} Account Details: ${Display Name}  First Name: ${First Name}  Last Name: ${Last Name}  Display Name: ${Display Name}  HDS ID: ${Network ID}  Password: ${AD Password}  Expiration Date: ${Contractor End Date} (Only for Contractor)  Thanks, SailPoint Team |

## EMT03: Manager Mail (Contractor Offboarding)

|  |  |
| --- | --- |
| When | User is offboarded from SailPoint |
| From | SailPoint |
| To | Manager |
| Subject | Contractor terminated: ${Display Name} |
| Body | Contractor ${Display Name} has been terminated successfully.  First Name: ${First Name}  Last Name: ${Last Name}  Display Name: ${Display Name}  HDS ID: ${networkid}  Expiration Date: ${Contractor End Date}  Thanks, SailPoint Team |

## EMT04: Contractor Expiration Reminders (On Day 30,14,7,6,5,4,3,2,1)

|  |  |
| --- | --- |
| When | Contractor offboarding reminder |
| From | SailPoint |
| To | User |
| Cc | Manager |
| Subject | Your account is going to expire in ${Number of expiry days} days. |
| Body | \*\* Your HDS Domain Account is set to expire in ${Number of expiry days} days. \*\*  Display Name: ${Display Name}  HDS ID: ${Network ID}  Expiration Date: ${Contractor End Date}  Manager Email: ${Manager Email}  Should your account require an extension, you or your Manager must [click here](https://myhdsaccess-dev.hdsupply.net/identityiq/home.jsf) and perform the following steps:   1. Login to SailPoint. 2. Click on the 3 lines on the left-hand side and click on Contractor Management. Select Manage Contractor. 3. Select ‘Extend Contractor’. Select the contractor from the drop down. 4. Update the end date on the next page and submit the request.   If you are the User, an email will be sent to your Manager requesting their approval.  If you are the Manager, an email will be sent to your Manager requesting their approval.  Once the approvals have been received, an email will be sent to you with your account status.  Thanks, SailPoint Team |

## EMT05: Approval Email

|  |  |
| --- | --- |
| When | Approval pending in SailPoint for user |
| From | SailPoint |
| To | Manager |
| Subject | Work item assigned: $workItemName |
| Body | Dear {manager display name},  There are new work item(s) assigned to you in SailPoint. Below are the details:  Workitem Name: ${workitemname}  Requester: ${REQUESTER\_NAME}  User: ${USER\_FULL\_NAME}  Requested Item: ${item.name}  Application: ${applicationName}  Based on your review, approve/reject the request on SailPoint. Please mark your decision in <TBD>days.  Thanks, SailPoint Team |

## EMT06: Requestor Email

|  |  |
| --- | --- |
| When | Access Request submitted for user |
| From | SailPoint |
| To | Requester |
| Subject | Your request for ${user displayname} has been submitted successfully. |
| Body | Dear {manager display name},  Your request for user ${User display name} has been submitted successfully.  Requestid: ${requestid}  Thanks, SailPoint Team |

## EMT07: Service Account/Non-Person Account Creation

|  |  |
| --- | --- |
| When | Service/Non-Person Account is created |
| From | SailPoint |
| To | Requestor, manager |
| Subject | ${Service/Non-Person Account Display Name} $ {Service/Non-Person} Account Information |
| Body | New {Service/Non-Person} Account Details: ${Service/Non-Person Account Display Name}  Name: ${Service/Non-Person Account Display Name}  AccountID: ${sAMAccountName}  Password: ${password}  Manager/Owner: ${owner}  Thanks, SailPoint Team |

## EMT08: Privileged Account Creation

|  |  |
| --- | --- |
| When | Privileged Account is created |
| From | SailPoint |
| To | User |
| Subject | ${Privileged Account Display Name} Privileged Account Information |
| Body | New Privilege Account Details: ${Privileged Account Display Name}  Name: ${Privileged Account Display Name}  AccountID: ${sAMAccountName}  Password: ${password}  If you have any issues, please [contact us](mailto:SN-AG-IT-INF-L3-APPLICATIONS@hdsupply.com).  Thanks, SailPoint Team |

## EMT09: AD Group Creation

| When | AD Group is created |
| --- | --- |
| From | SailPoint |
| To | Requestor, owner |
| Subject | ${AD Group} Information |
| Body | New AD Group has been created:  Display Name: ${AD Group Display Name}  Value: ${ AD Group Value}  Members: ${memberlist}  Owners: ${owner list}  Thanks, SailPoint Team |

# Application Configuration

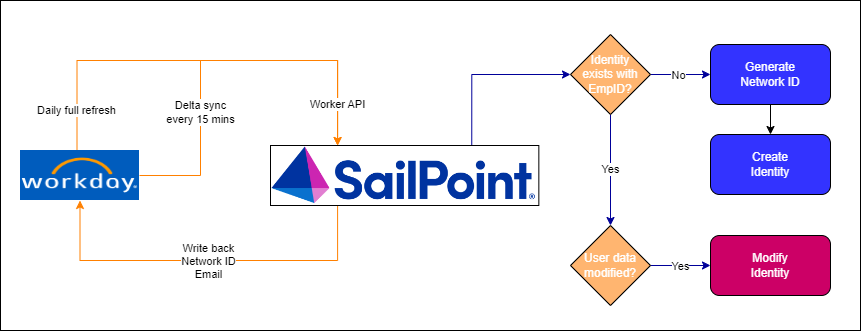
The applications detailed below will be configured within IdentityIQ. Each application, as defined in IdentityIQ, represents a connection with a unique schema to a unique data source.

1. Workday
2. Active Directory
3. Active Directory Privileged
4. Microsoft Entra ID
5. Salesforce
6. SAP GRC

## Workday

Workday is a cloud-based software that offers applications for financial management, enterprise resource planning, and human capital management. The Workday application will function as the authoritative source for Employees at HD Supply. The source will be configured using the SailPoint IdentityIQ Workday connector. SailPoint will perform delta aggregation every 15 minutes and full aggregation every midnight of accounts. No group will be aggregated. SailPoint will write back Network ID and Email attribute values to Workday.

### Process Flow



### Configuration Details

|  |  |
| --- | --- |
| Parameter | Value |
| Name | Workday |
| Owner | <TBD> |
| Application Type | Workday |
| Description | Fetches employee data from Workday |
| Authoritative Application | True |

### Connection Settings

|  |  |  |
| --- | --- | --- |
| Attribute Name | Development | Production |
| Authentication Type | Basic Authentication | Basic Authentication |
| Workday URL | https://wd2-impl-services1.workday.com/ccx/service/hdsupply\_preview/Human\_Resources |  |
| Effective Time Zone | America/New\_York | America/New\_York |
| Effective Date Offset | 14 | 14 |
| Termination Offset | 35 | 35 |

### Account Schema

|  |  |  |
| --- | --- | --- |
| Account Attribute | Description | Type |
| USERID | Worker ID | String |
| FILENUMBER | Employee ID | String |
| MANAGER\_ID | Manager ID | String |
| EMAIL\_ADDRESS\_HOME | Home email address of the worker. | String |
| ADDITIONAL\_EMAIL\_ADDRESS\_HOME | Additional home email address of the worker. | String |
| EMAIL\_ADDRESS\_WORK | Work email address of the worker. | String |
| ADDITIONAL\_EMAIL\_ADDRESS\_WORK | Additional work email address of the worker. | String |
| ADDRESS\_HOME | Home address of the worker. | String |
| ADDRESS\_WORK | Work address of the worker. | String |
| FIRST\_NAME | First name | String |
| LAST\_NAME | Last name | String |
| CLASS | Combination of Position, Time Type and Employment Type | String |
| DEPARTMENT | Cost center | String |
| JOBCODE | Job profile | String |
| JOBTITLE | Business title | String |
| LOCATION | Work Location of the worker. | String |
| COST\_CENTER\_HIERARCHY | Cost center hierarchy of the worker. | String |
| HIREDATE | Hire date | String |
| FULLPARTTIME | Type of employment full time or part time. | String |
| TERMINATION\_DATE | Termination date | String |
| TEAM | Team in the organization data of the worker. | String |
| DIVISION | Sales channel in the organization data of worker. | String |
| POSTAL\_CODE | Postal Code | String |
| COUNTRY | Business site's country of a worker. | String |
| CITY | Business site's city of a worker. | String |
| ON\_LEAVE | Leave status of the worker whether on leave | String |
| LEGAL\_MIDDLE\_NAME | Legal Middle Name | String |
| MIDDLE\_NAME | Middle Name | String |
| WORKER\_NAME | Worker Name | String |
| POSITION | Position of the Worker | String |
| BUSINESS\_SITE\_LOCATION\_ID | Business site location ID | String |
| EMPLOYEE\_TYPE | Employee Type | String |
| CONTRACT\_END\_DATE | Contract end date of worker. | String |
| ORGANIZATION\_NAME | Business Unit Name. | String |
| COMPANY\_NAME | The company under which worker belongs. | String |
| LAST\_DAY\_OF\_WORK | Last working day of a worker. | String |
| COST\_CENTER\_REFERENCE\_ID | Reference ID of organization type COST CENTER. | String |
| ADDRESS\_LINE\_1 | Business site's Address\_line\_1 of worker. | String |
| STATE | Business site's state. | String |
| COST\_CENTER | Represent the organization name whose type is COST\_CENTER | String |
| FUTURE\_DATE | Represent date of hiring/termination/onboarding incase its in future | String |
| FUTURE\_ACTION | Represent action for worker who will be getting hire/terminate/onboard in future. e.g Hire Employee | String |
| HOME\_TELEPHONE | Represent home phone of the worker with device type telephone | String |
| HOME\_MOBILE | Represent home phone of the worker with device type mobile | String |
| WORK\_MOBILE | Represent work phone of the worker with device type mobile | String |
| WORK\_TELEPHONE | Represent work phone of the worker with device type telephone | String |
| ACQUISITIONID | acquisition id of the user | String |
| ORIGHIREDATE | original hire date of the user | String |
| PREFERREDLNAME | Preferred Last name | String |
| JOBFAMILY | Job Family | String |
| JOB\_SUB\_FUNC | Job Sub Function | String |
| COST\_CENTER\_ID | Represent the organization code whose type is COST\_CENTER | String |
| EMPL\_STATUS | Employee status | String |
| COMPANY\_CODE | Company Code | String |
| NETWORK\_ID | network Id | String |
| ORGANIZATION\_CODE | Organization code | String |
| TERMINATED | Terminated | String |
| ONLEAVE | On Leave | String |
| ACTIVE | Active | String |
| PRIMARY\_TERMINATION\_REASON\_REFERENCE | Primary Termination Reason Reference | String |

### Identity Attributes Mapping

Please refer to the “[Identity Attribute Matrix](#_Identity_Attribute_Matrix)” section of the Appendix for more information on each of the attributes coming from Workday and how they relate to attributes in downstream systems.

### Account Correlation

|  |  |  |
| --- | --- | --- |
| Application Attribute | Operator | Identity Attribute |
| USERID | Equals | Name |

### Manager Correlation

|  |  |  |
| --- | --- | --- |
| Application Attribute | Operator | Identity Attribute |
| MANAGER\_ID | Equals | Name |

### Aggregation Schedule

Please see the “[Aggregations](#_Task_Scheduling)” portion of the “Task Configuration” section below for more information regarding the Workday aggregation schedules.

### Rules

#### Creation Rule

|  |  |
| --- | --- |
| Rule Name | Description |
| HDS-Workday-IdentityCreation | Fetch USERID and FILENUMBER attributes from Workday account. If USERID exists then set USERID as the name of the identity else set FILENUMBER as the name of the identity. |

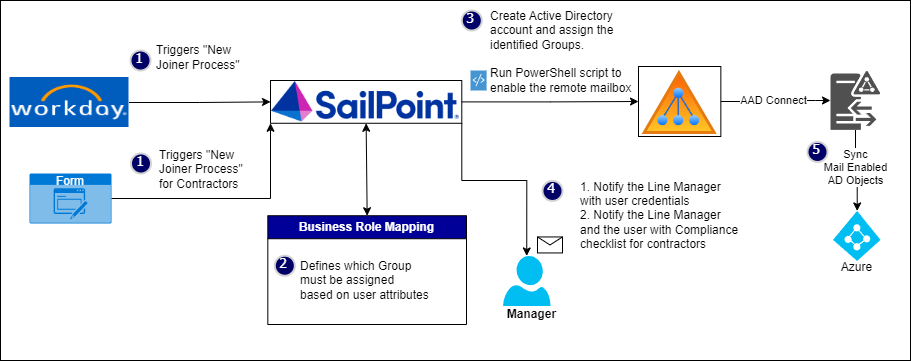
## Active Directory

The Active Directory (AD) application serves as the primary directory application for all user types at HD Supply. This application will be configured using SailPoint IdentityIQ Active Directory – Direct connector.

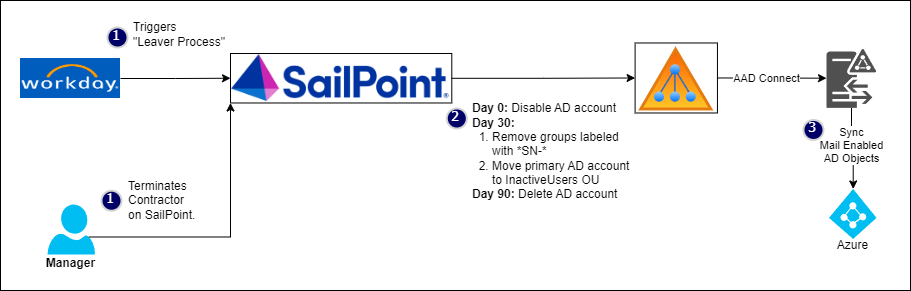
Since HD Supply doesn’t have a classification of privileged and normal groups, it is recommended to manage all the regular accounts and privileged accounts using a single application.

### Process Flow

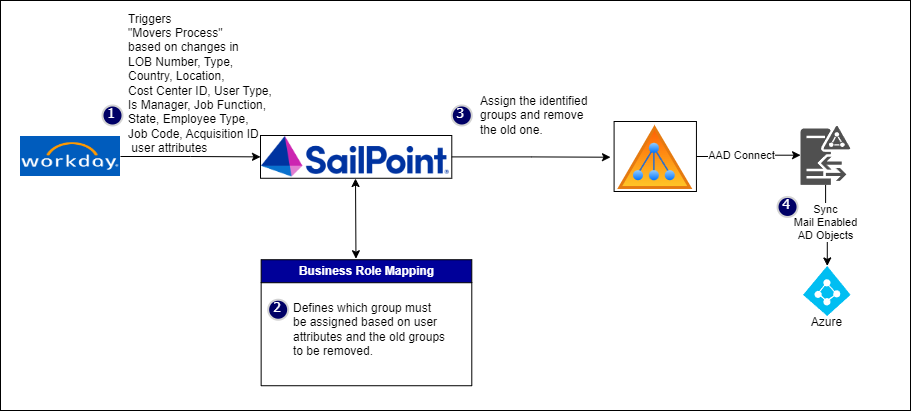
##### New Joiner Process



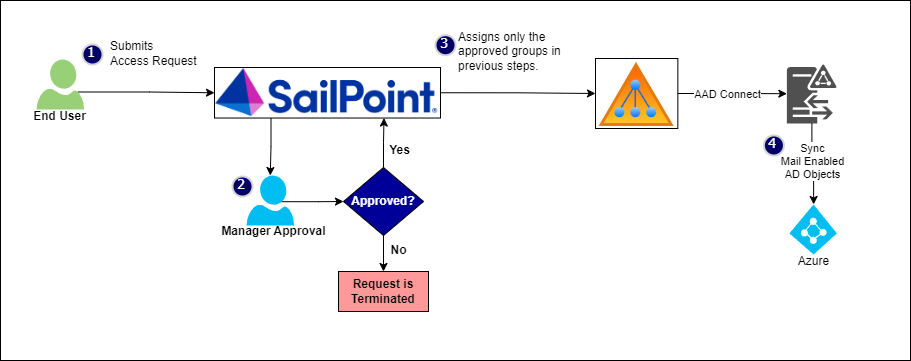
##### Leaver Process



##### Mover Process



##### Access Request



### Application Configuration

#### 7.2.1.1. Configuration Details

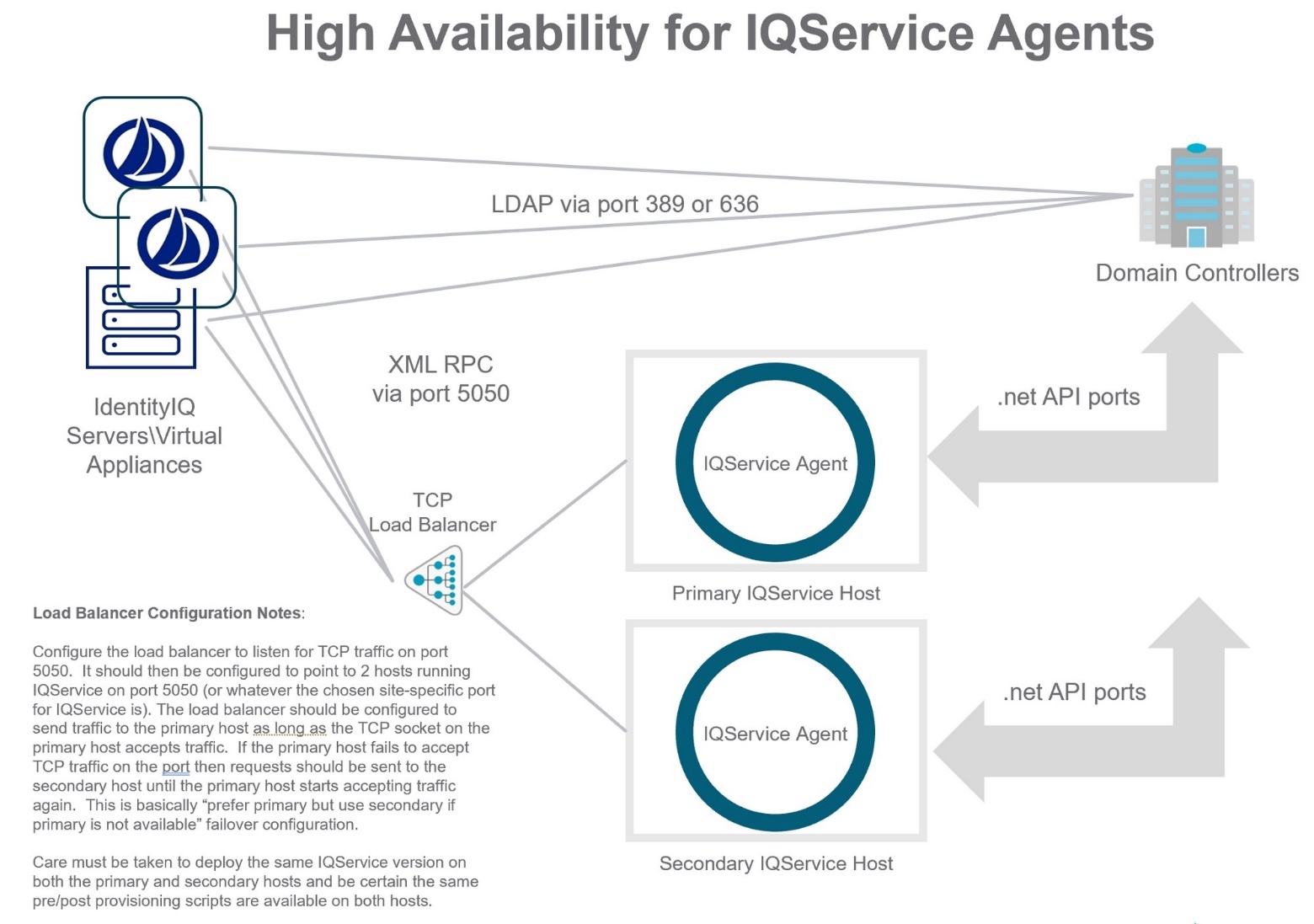
|  |  |
| --- | --- |
| Parameter | Value |
| Name | Active Directory |
| Owner | <TBD> |
| Type | Active Directory – Direct |
| Action(s) | Aggregation of accounts and entitlements  Create accounts and assign entitlements |
| Authoritative Application | False |

#### 7.2.1.2 IQService Configuration

Installations of IdentityIQ provisioning to Active Directory, Lotus Notes, SharePoint Server, Windows Local, and a few other various target systems will use the IQService windows provisioning agent as an intermediary to provision to systems that require integration with a Windows-based API.

IQService is a windows based agent written in .net languages. It leverages APIs provided in Windows environments to provide provisioning services for IdentityIQ's Java-based technologies. IQService is installed as a service running on a Windows OS based host. By default, it listens on TCP port 5050 for requests from IdentityIQ systems.

The following diagram illustrates the most common deployment architecture for IQService:



Diagram

Description automatically generated

For communication between IQService and a domain controller, SailPoint recommends at least the following ports must be opened:

* LDAP Ports 389 and 636
* Kerberos port 88
* Active Directory Web Services 9389
* Active Directory port 3268
* Active Directory port 3269
* Active Directory DNS port 53
* Active Directory Replication, Login services port 445
* Kerberos Passwords, port 464
* Authentication port UDP 137
* Authentication port TCP 139

#### 7.2.1.3 Connection Settings

|  |  |  |
| --- | --- | --- |
| Attribute | Development | Production |
| IQ Service Configuration | | |
| IQService Host | cfmslpiq01wd0s.hds.hdsupply.com  LB: myhdsaccess-dev-iq.hdsupply.net |  |
| IQService Port | 5050 | 5050 |
| Use TLS | TRUE | TRUE |
| Forest Configuration | | |
| Forest Name | hdsupply | hdsupply |
| Global Catalog Server | NA | NA |
| Authentication and Security | Simple | Simple |
| Use TLS | TRUE | TRUE |
| Resource Forest | FALSE | FALSE |
| Domain Configuration | | |
| Forest Name | hdsupply | hdsupply |
| Domain DN | DC=hdsdev,DC=hdsupply,DC=com | DC=hds,DC=hdsupply,DC=com |
| Authentication and Security | Simple | Simple |
| Use TLS | TRUE | TRUE |
| Domain Controllers | cfmdevdc50wsbs.**hdsdev.hdsupply.com -10.244.71.196**  cfmdevdc51wsbs.**hdsdev.hdsupply.com -10.244.71.197**  **devaddc01.hdsdev.hdsupply.com – 10.244.65.76** | Cf**madc50wp0s.hds.hdsupply.com – 10.244.64.1** |
| Exchange Configuration | | |
| Exchange Forest |  |  |
| Exchange Host |  |  |
| Account Forest |  |  |
| Use TLS |  |  |
| User Search Scope | | |
| Search DN | OU=Users,OU=HDS,DC=hdsdev,DC=hdsupply,DC=com | OU=Users,OU=HDS,DC=hds,DC=hdsupply,DC=com |
| Search DN | OU=Admins,DC=hdsdev,DC=hdsupply,DC=com | OU=Admins,DC=hds,DC=hdsupply,DC=com |
| Search DN | OU=ServiceAccounts,DC=hdsdev,DC=hdsupply,DC=com | OU=AdminsKali,DC=hds,DC=hdsupply,DC=com |
| Search DN |  | OU=ServiceAccounts,DC=hds,DC=hdsupply,DC=com |
| Search filter | NA | NA |
| Group Search Scope | | |
| Search DN | OU=Groups,DC=hdsdev,DC=hdsupply,DC=com | OU=Groups,DC=hds,DC=hdsupply,DC=com |
| Search filter | NA | NA |

#### Account Schema

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Type |
| businessCategory | business category | String |
| carLicense | vehicle license or registration plate | String |
| cn | common name(s) for which the entity is known by | String |
| departmentNumber | identifies a department within an organization | String |
| description | descriptive information | String |
| destinationIndicator | destination indicator | String |
| displayName | preferred name to be used when displaying entries | String |
| distinguishedName | distinguished name for which the entity is known by | String |
| employeeNumber | numerically identifies an employee within an organization | String |
| employeeType | type of employment for a person | String |
| facsimileTelephoneNumber | Facsimile (Fax) Telephone Number | String |
| givenName | first name(s) for which the entity is known by | String |
| homePhone | home telephone number | String |
| homePostalAddress | home postal address | String |
| initials | initials of some or all of names, but not the surname(s). | String |
| internationalISDNNumber | international ISDN number | String |
| l | city | String |
| mail | RFC822 Mailbox | String |
| manager | DN of manager | String |
| mobile | mobile telephone number | String |
| o | organization this object belongs to | String |
| ou | organizational unit this object belongs to | String |
| pager | pager telephone number | String |
| physicalDeliveryOfficeName | Physical Delivery Office Name | String |
| postOfficeBox | Post Office Box | String |
| postalAddress | postal address | String |
| postalCode | postal code | String |
| preferredDeliveryMethod | preferred delivery method | String |
| preferredLanguage | preferred written or spoken language for a person | String |
| registeredAddress | registered postal address | String |
| roomNumber | room number | String |
| secretary | DN of secretary | String |
| seeAlso | DN of related object | String |
| sn | last (family) name(s) for which the entity is known by | String |
| st | state or province which this object resides in | String |
| street | street of this object | String |
| streetAddress | street address of this object | String |
| telephoneNumber | Telephone Number | String |
| teletexTerminalIdentifier | Teletex Terminal Identifier | String |
| telexNumber | Telex Number | String |
| title | title associated with the entity | String |
| uid | user identifier | String |
| userPrincipalName | user principal name | String |
| objectClass | object classes of the entity | String |
| memberOf | Group Membership | group |
| objectSid | Windows Security Identifier | String |
| objectguid | Object globally unique identifier | String |
| objectType | Type of Active Directory object | String |
| sAMAccountName | sAMAccountName | String |
| accountFlags | List of the flags enabled on an account | String |
| department | User's department | String |
| msNPCallingStationID | CallingStationID | String |
| msRADIUSFramedRoute | Static Routes for Dial-In connection | String |
| msNPAllowDialin | Is dial-in allowed | String |
| msRADIUSCallbackNumber | Callback Number | String |
| msRADIUSFramedIPAddress | Define Static IP Address | String |
| externalEmailAddress | External email address of Mail User | String |
| mailNickname | Exchange Alias | String |
| homeMDB | Exchange Database | String |
| msExchHideFromAddressLists | Hide from Exchange address lists | String |
| msRTCSIP-UserEnabled | User enabled for Skype for Business Server | boolean |
| SipAddress | Skype for Business sipAddress | String |
| RegistrarPool | Skype for Business Registrar pool | String |
| LyncPinSet | Skype for Business user pin set status | String |
| LyncPinLockedOut | Skype for Business user pin lock status | String |
| DialPlan | Skype for Business user dial plan name | String |
| dNSHostName | Fully Qualified Domain Name for the Service Account | String |
| msDS-ManagedPasswordInterval | Password change interval in days for the Managed Service Account | String |
| msDS-SupportedEncryptionTypes | Supported Encryption Types for the Managed Service Account | String |
| msDS-GroupMSAMembership | Principals allowed to use Group Managed Service Account | String |
| msDS-AllowedToActOnBehalfOfOtherIdentity | Principals that can act on the behalf of Group Managed Service Account | String |
| servicePrincipalName | Service principal names for the Service Account | String |
| shadowAccountDN | DistinguishedName of the Linked Mailbox shadow account | String |
| shadowAccountGuid | ObjectGuid of the Linked Mailbox shadow account | String |
| msExchRecipientTypeDetails | Type of the Microsoft Exchange recipient object | String |
| msDS-PrincipalName | Name of the entity in the format "NetBIOS domain name\sAMAccountName" | String |
| extensionAttribute1 | extensionAttribute1 | String |
| extensionAttribute2 | extensionAttribute2 | String |
| extensionAttribute3 | extensionAttribute3 | String |
| extensionAttribute4 | extensionAttribute4 | String |
| extensionAttribute5 | extensionAttribute5 | String |
| extensionAttribute6 | extensionAttribute6 | String |
| extensionAttribute7 | extensionAttribute7 | String |
| extensionAttribute8 | extensionAttribute8 | String |
| extensionAttribute9 | extensionAttribute9 | String |
| extensionAttribute10 | extensionAttribute10 | String |
| extensionAttribute11 | extensionAttribute11 | String |
| extensionAttribute12 | extensionAttribute12 | String |
| extensionAttribute13 | extensionAttribute13 | String |
| extensionAttribute14 | extensionAttribute14 | String |
| extensionAttribute15 | extensionAttribute15 | String |
| smtp | smtp | String |
| employeeID | stores the networkID for the user | String |
| name | stores the networkID for the user | String |
| company | company | String |
| co | country of the user | String |

#### Identity Attributes Mapping

Please refer to the “[Identity Attribute Matrix](#_Identity_Attribute_Matrix)” section of the Appendix for more information on each of the attributes coming from Workday and how they relate to attributes in Active Directory.

#### Correlation Configuration

Please refer to Active Directory [Correlation rule](#_Correlation_Rule) for correlation logic.

### Aggregation Schedule

Please see the “[Aggregations](#_Task_Scheduling)” portion of the “Task Configuration” section below for more information regarding the Active Directory aggregation schedules.

### Provisioning Policies

This section captures information sent to the downstream application on a per attribute, per operation level. As an example, the Create Account Provisioning Policy outlines the attributes required to be sent to Active Directory when creating a new user account. Note that these tables are not 100% inclusive of all attributes that must be set as there are other mechanisms that could account for specific attributes, e.g. the PowerShell After Create rule will capture Exchange/Email specific processing.

A custom object, HDS-AzureLicenseJobCodes, will be created based on the exported data from tbl\_ AzureLicenseJobCodes table in ADP database as a one-time activity. The data in the custom object will be added as a map as per below structure. This custom object will be used for calculating the value for extensionAttribute8 attribute.

1010 —>

JC1 —>E3

JC2 —>E3

JC3 —>E5

**HR should send an email notification to SailPoint Administrator for addition of any new job code along with the required Azure license name.**

#### Create Account

| Attribute | OOTB | Field Type | Value or Mapping |
| --- | --- | --- | --- |
| cn | True | String | Network ID |
| company |  |  | Company |
| co | True | String | Country 3 ISO Code i.e. USA |
| department | True | String | Cost Center Id |
| description | True | String | Network ID for Employees  “Contractor” for Contractors |
| displayName | True | String | Display Name |
| distinguishedName | True | String | Calculated based on Network ID and LOB Number.  CN=<Network ID>,OU=<LOB Number>,OU=Users,OU=HDS,DC=hds,DC=hdsupply,DC=com  e.g. CN=1011865,OU=1010,OU=Users,OU=HDS,DC=hds,DC=hdsupply,DC=com |
| employeeID | True | String | Employee ID |
| extensionAttribute1 | True | String | LOB Number |
| extensionAttribute4 | True | String | Network ID |
| extensionAttribute7 | True | String | Not required for Employees  Calculated, manager’s email address for Contractors |
| extensionAttribute8 | True | String | Get the Azure license value from custom object HDS-AzureLicenseJobCodes based on LOB number and jobcode.  If not found, then use below logic:  “E3” if Job Family starts with “D” or “E” or “M” or “P” or “V”,  “E1” if Job Family starts with “S” or “U”,  else “F3” |
| extensionAttribute9 | True | String | Network ID |
| extensionAttribute10 | True | String | sync – It is set to sync for mail enabled accounts. Regular accounts of employees, contractors and non-person accounts are mail enabled.  Setting this attribute value to sync, synchronizes the AD accounts to Azure using AAD connect. |
| extensionAttribute5 | True | String | Mobile Number |
| givenName | True | String | First Name |
| initials | True | String | Middle Initial stripped down to a single character  e.g. “Daniel” becomes “D” |
| L | True | String | City |
| mail | True | String | Calculated, [firstName.lastName@hdsupply.com](mailto:firstName.lastName@christushealth.org)  Duplicate check performed. If already reserved, the next value will have a numeric value starting from 2 appended to it. This duplicate check will be repeated until the next available combination is found.  e.g. [firstName.lastName2@hdsupply.com](mailto:firstName.lastName2@hdsupply.com) or [firstName.lastName3@hdsupply.com](mailto:firstName.lastName3@hdsupply.com)  Additionally, some historical email data may not be in sequence and suffix might be missing. For example – there might be 2 users with name Dennis Lilly and there is email address could be  [Dennis.lilly@hdsupply.com](mailto:Dennis.lilly@hdsupply.com)  [Dennis.lilly4@hdsupply.com](mailto:Dennis.lilly4@hdsupply.com)  In the above example, suffixes 2 and 3 are missing. In such cases, if another user with name Dennis Lilly shows up, then email address should be Dennis.Lilly5@hdsupply.com |
| mailNickName | True | String | Calculated, same as NetworkID |
| manager | True | String | Calculated, manager’s distinguishedName from their primary Active Directory account  e.g. CN=tw053515,OU=1010,OU=Users,OU=HDS,DC=hds,DC=hdsupply,DC=com |
| password | True | Secret, String | During the creation process, a random password will be generated based on password policy. |
| pwdLastSet | True | Integer, Interval | “0”  NOTE: Setting this value to 0 is the same as checking the reset password on the next login box. |
| postalCode | True | String | Postal Code |
| sAMAccountName | True | String | Network ID |
| sn | True | String | Last Name |
| st | True | String | State |
| streetAddress | True | String | Address |
| sn | True | String | Last Name |
| title | True | String | Blank for Employees  “Contractor” for Contractors |
| telephoneNumber | True | String | Work Phone |
| userPrincipalName | True | String | Calculated, matching email. [firstName.lastName@hdsupply.com](mailto:firstName.lastName@christushealth.org)  Duplicate check performed. If already reserved, the next value will have a numeric value appended to it. This duplicate check will be repeated until the next available combination is found.  e.g. [firstName.lastName1@hdsupply.com](mailto:firstName.lastName1@christushealth.org) or [firstName.lastName2@hdsupply.com](mailto:firstName.lastName2@christushealth.org) |
| msExchHideFromAddressLists | False | String | Set to True when Account is disabled  Set to False when Account is enabled |
| accountType | False | String | Values: Primary, Privileged, Service and Non-Person (Maintained internally in SailPoint) |

### Password Policy

| Rule | Value |
| --- | --- |
| passwordHistory | 24 |
| passwordMinAge | 2 |
| passwordMinLength | 12 |
| passwordMinNumeric | 1 |
| passwordMinSpecial | 1 |
| passwordMinUpper | 1 |
| checkPasswordsAgainstIdentityAttributes | true |

### Rules

#### Correlation Rule

The Correlation Rule is used to select the existing Identity to which the aggregated account information should be connected.

|  |  |
| --- | --- |
| Rule Name | Description |
| HDS-Active Directory-Correlation | Use below logic for correlation of aggregated accounts to the existing identity:   * Identity attribute Network ID matches with account attribute sAMAccountName * If account attribute sAMAccountName ends with ‘r’, then remove ‘r’ from last letter of sAMAccountName and check if it matches with Identity attribute Network ID * If account attribute sAMAccountName ends with ‘k’, then remove ‘k’ from last letter of sAMAccountName and check if it matches with Identity attribute Network ID * If account attribute sAMAccountName starts with “svc\_” or “np\_” , then check if identity with name “ZZ:AD:” plus sAMAccountName exists |

#### Native After Create Rule and Native After Modify Rule

Before and After Scripts, also called Native Rules, are scripts that are sent through the connector to the IQService host machine to run before and after provisioning. Before Scripts can modify the request object (containing the provisioning request) and After Scripts can modify the result object (containing the provisioning result); both can perform custom actions or manipulations on those objects. Scripts can be written in any scripting language, including both object-oriented languages like PowerShell and non-object-oriented languages like Perl.

| Rule Name | Description |
| --- | --- |
| HDS-ConnectorAfterCreate | The Native After Create Rule will evaluate the request as well as the output from the Before Provisioning Rule to perform any required exchange processing. Of note, these rules will run PowerShell scripts to enable remote mailboxes in accordance with the current mailbox creation process today. |
|  | The Native After Modify Rule will evaluate the request as well as the output from the Before Provisioning Rule to perform any required exchange processing. Of note, these rules will run PowerShell scripts to enable remote mailboxes in accordance with the current mailbox creation process today.  If account description contains “Out of Office”, then set the Out of Office for Mailbox.  Use PS command:  Set-MailboxAutoReplyConfiguration -Identity UserName -AutoReplyState Scheduled -StartTime {start Time} -EndTime {end Time} -InternalMessage {internal message}  where UserName {SamAccountName}, {start Time}, {end Time} and {internal message} should be passed from before provisioning rule. |

#### Logiplex Split Rule

The LogiPlex Split Rule is in fact a rule of type ResourceObjectCustomization, but is run before the

actual customization rule is applied. It will receive slightly different inputs and the expected output is

also different.

|  |  |
| --- | --- |
| Rule Name | Description |
| HDS-LogiPlex-Split-Rule | This rule will inspect the account and group objects received from Active Directory server. It will check the name of groups and create applications based on that. The custom object 'HDS-LogiPlex-App-Criteria' defines the criteria which will segregate the groups to different applications based on the group naming conventions. All other groups will be related to the main application, Active Directory.  Similarly, it will check accounts, and the group membership will be segregated to different accounts based on the group naming conventions defined in the same custom object mentioned above. Refer Section 7.2.7 on details on logiplex connector. |

#### Logiplex Provisioning Rule

The LogiPlex Provisioning Rule is in fact a rule of type CompositeRemediation (Logical Provisioning

Rule). It accepts a provisioning plan and can modify the plan for the real target application and then

return the modified provisioning plan.

|  |  |
| --- | --- |
| Rule Name | Description |
| HDS-LogiPlex-Provisioning-Rule | The goal of this rule is to merge changes for sub-applications into the main application. It is important to understand that the plan will, after successful provisioning, also be applied to the identity cube. So, the plan must be modified in such a way that whatever will change ends up in the original plan object.  Also, when there are multiple accounts on the main application for an identity, then it is important to choose which account should be picked up when provisioning for a sub application. That is also taken care of in this rule and is finally merged to the original plan object. Refer Section 7.2.7 on details on logiplex connector. |

### Logiplex Connector Changes

Active Directory is also being used as a logiplex connector for AD based applications. For this the following changes were made on the application xml:

* connector value is updated to ‘sailpoint.services.standard.connector.LogiPlexConnector’
* logiPlexAggregationRule entry was added, with value as "HDS-LogiPlex-Split-Rule"
* logiPlexProvisioningRule entry was added, with value as "HDS-LogiPlex-Provisioning-Rule"
* logiPlexMasterConnector entry was added, with value as ‘sailpoint.connector.ADLDAPConnector’
* logiPlexUseGetObject entry was added, with value as ‘true’
* logiPlexSimulateProvisioning entry was added, with value as ‘false’

This Active Directory application will act as Proxy Application (master/main application) for other sub applications and provisioning will happen through this master/main application. The ‘HDS-ActiveDirectory-GroupAggregation’ Task and ‘HDS-ActiveDirectory-AccountAggregation’ Task will be used for logiplex sub application creation and their group creation. For more informaton on logiplex application, please refer https://community.sailpoint.com/t5/Professional-Services/PSLabs-LogiPlex-Connector/ta-p/172304

## Microsoft Entra ID

Microsoft Entra ID (Azure AD) is Microsoft’s cloud-based identity and access management service. It simplifies and secures access to resources within an organization, whether they are on-premises or in the cloud. Microsoft Entra ID manages access to applications, devices, and data. This application will be configured using SailPoint IdentityIQ Azure Active Directory connector.

Microsoft Entra ID application will support following features:

Account Management for User and User in Federated Domain

The Microsoft Entra ID connector supports managing the following group types as an entitlement and as separate group objects. These different types of groups are created for different purpose which are described as follows:

* Microsoft 365 groups (formerly Office 365 groups) are used for collaboration between internal and external users of the company.
* Distribution Lists (Distribution groups) are used for sending notifications to a group of people.
* Security groups are used for granting access to resources such as SharePoint sites.
* Mail-enabled security groups are used for granting access to resources such as SharePoint and emailing notifications to those users.

The following table describes different conditions or configurations depending on which connector will aggregate /able to provision distinct types of groups:

|  |  |  |
| --- | --- | --- |
| **Group Types** | **Aggregation** | **Provisioning** |
| Security | Yes | Yes |
| Mail-Enabled Security | Yes | No |
| Office 365 | Yes | Yes |
| Distribution Lists | Yes | No |

### Application Configuration

#### Configuration Details

|  |  |
| --- | --- |
| Parameter | Value |
| Name | Microsoft Entra ID |
| Owner | HDS-WG-APPOWNER-AZURE-ACTIVE-DIRECTORY |
| Type | Azure Active Directory |
| Action(s) | Aggregation of accounts and entitlements  Create accounts and assign entitlements |
| Authoritative Application | False |

#### Connection Settings

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | Development | QA | Production |
| Connector Credentials | | | |
| Authentication Method | OAuth 2.0 | OAuth 2.0 | OAuth 2.0 |
| Grant Type | Client Credentials | Client Credential | Client Credentials |
| Domain Name | hdsupplydev.onmicrosoft.com | hdsupplydev.onmicrosoft.com | hdsupplyinc.onmicrosoft.com |
| Additional Configuration | | | |
| IQService Host | myhdsaccess-dev-iq.hdsupply.net | myhdsaccess-qa-iq.hdsupply.net | myhdsaccess-iq.hdsupply.net |
| IQService Port | 5051 | 5051 | 5051 |
| Use TLS for IQService | TRUE | TRUE | TRUE |
| Manage Microsoft Office 365 Groups | TRUE | TRUE | TRUE |
| Enable Microsoft Teams Notifications | FALSE | FALSE | FALSE |
| User Filters |  |  |  |
| Advanced User Filter |  |  |  |
| Group Filters |  |  |  |
| Advanced Group Filter |  |  |  |

#### Account Schema

Add below additional attributes to Account schema.

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute Name | Type | Description | Properties |
| accountEnabled | boolean | True if the account is enabled; otherwise, false |  |
| assignedLicenses | string | The licenses that are assigned to the user | Multi-valued |
| assignedPlans | string | The plans that are assigned to the user | Multi-valued, Entitlement, Managed |
| city | string | The city in which the user is located |  |
| country | string | The country/region in which the user is located |  |
| department | string | The name for the department in which the user works |  |
| dirSyncEnabled | string | Indicates whether this object was synced from the on-premises directory |  |
| disabledPlans | string | The plans that are not assigned to user | Multi-valued |
| displayName | string | The name displayed in the address book for the user |  |
| facsimileTelephoneNumber | string | The telephone number of the user's business fax machine |  |
| givenName | string | First name of user |  |
| groups | string | Groups assigned to a user | Multi-valued, Entitlement, Managed |
| appRoleAssignments | string | Application roles assigned to a user | Multi-valued, Entitlement, Managed |
| immutableId | string | This property is used to associate an on-premises ActiveDirectory user account to their Azure AD user object |  |
| jobTitle | string | The user's job title |  |
| lastDirSyncTime | string | Indicates the last time at which the object was synced with the on-premises directory |  |
| mail | string | The SMTP address for the user, for example, "[john@contoso.onmicrosoft.com](mailto:john@contoso.onmicrosoft.com)" |  |
| mailNickname | string | The mail alias for the user |  |
| signInNames | string | Specifies the collection of sign-in names for a local account in an Azure Active Directory B2C tenant | Multi-valued |
| userIdentities | string | Specifies the collection of userIdentities for a social user account in an Azure Active Directory B2C tenant | Multi-valued |
| creationType | string | Indicates whether the user account is a local account for an Azure Active Directory B2C tenant |  |
| mobile | string | The primary cellular telephone number for the user |  |
| objectId | string | The unique identifier for the user |  |
| onPremisesSecurityIdentifier | string | Contains the on-premises security identifier (SID) for the user that was synchronized from on-premises to the cloud |  |
| otherMails | string | A list of additional email addresses for the user | Multi-valued |
| passwordPolicies | string | Specifies password policies for the user |  |
| physicalDeliveryOfficeName | string | The office location in the user's place of business |  |
| postalCode | string | The ZIP OR postal code for the user's postal address |  |
| preferredLanguage | string | Preferred written or spoken language for a person |  |
| proxyAddresses | string | Proxy addresses, for example: ["SMTP: [bob@contoso.com](mailto:bob@contoso.com)", "smtp: [bob@sales.contoso.com](mailto:bob@sales.contoso.com)"] | Multi-valued |
| roles | string | Administrator Role assigned to user | Multi-valued, Entitlement, Managed |
| sipProxyAddress | string | Specifies the voice over IP (VOIP) session initiation protocol (SIP) address for the user |  |
| state | string | The state or province in the user's address |  |
| streetAddress | string | The street address of the user's place of business |  |
| surname | string | Last name of the user |  |
| telephoneNumber | string | The primary telephone number of the user's place of business |  |
| usageLocation | string | A two letter country code indicating usage location |  |
| userPrincipalName | string | The user principal name (UPN) of the user |  |
| userType | string | Type of the user |  |
| manager | string | Manager of the user |  |
| channels | string | List of channel membership of a user | Multi-valued, Entitlement, Managed |
| azureEligibleRoles | string | List of Azure Eligible Roles | Multi-valued, Entitlement, Managed |
| azureActiveRoles | string | List of Azure Active Roles | Multi-valued, Entitlement, Managed |
| azureADEligibleRoles | string | List of Azure AD Eligible Roles | Multi-valued, Entitlement, Managed |
| azureADActiveRoles | string | List of Azure AD Active Roles | Multi-valued, Entitlement, Managed |
| accessPackages | string | List of Access Packages assigned to the user | Multi-valued, Entitlement, Managed |

#### Correlation

Correlation is required to match the accounts from the source system to identities in IdentityIQ. It describes in which order which identity attribute should be compared with which account attribute.

|  |  |  |
| --- | --- | --- |
| Identity Attribute | Operator | Account Attribute |
| upn | = | userPrincipalName |
| networkid | = | mailNickName |

### Aggregation Schedule

Please see the “[Aggregations](#_Aggregations)” portion of the “Task Configuration” section below for more information regarding the Microsoft Entra ID aggregation schedules.

### Rules

#### Correlation Rule

|  |  |
| --- | --- |
| Rule Name | Description |
| HDS-Microsoft Entra ID-Correlation | Logic to correlate R-accounts having email access:  Identity attribute Network ID plus ‘r@hdsupply.com’ equals account attribute userPrincipalName |

## Salesforce

The Salesforce application provides customer relationship management (CRM) service and provides enterprise applications focused on customer service, marketing automation, analytics, and application development. The integration of Salesforce with SailPoint IdentityIQ will allow users in the sales, dc, customer care, credit, and marketing departments to be given coarse grained access to salesforce in an automated manner eliminating delays or errors.

### Application Configuration

#### Configuration Details

|  |  |
| --- | --- |
| Parameter | Value |
| Name | Salesforce |
| Owner | <TBD> |
| Type | Salesforce |
| Action(s) | Aggregation of accounts and entitlements  Create accounts and assign entitlements |
| Authoritative Application | False |

#### Connection Settings

|  |  |  |
| --- | --- | --- |
| Attribute Name | Dev / QA | Production |
| Salesforce URL | Dev: <https://hdsupplyfm--hdsfull.sandbox.my.salesforce.com/services/Soap/u/>  QA: <https://hdsupplyfm--hdsqa.sandbox.my.salesforce.com/services/Soap/u/> |  |
| Authentication Type | Basic Authentication |  |
| Manage Active Accounts Only |  |  |
| Exclude Frozen Accounts |  |  |
| Create Contact on User Creation |  |  |
| Search Query For User |  |  |
| Search Query For Profile |  |  |

#### Account Schema

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Type |
| Id | Internal salesforce id. | String |
| Alias | User's assigned alias. | String |
| City | User's city. | String |
| CommunityNickname | DisplayNames for user's online communities. | String |
| CompanyName | User's company name. | String |
| CallCenterId | User's call center. | String |
| Country | User's country. | String |
| Department | User's department. | String |
| Email | User's Email address. | String |
| Division | User's division. | String |
| EmployeeNumber | User's employee number. | String |
| Extension | User's telephone extension. | String |
| Street | The street address associated with the User. | String |
| Fax | User's fax number. | String |
| IsActive | Flag that indicates if the user is active in Salesforce. | boolean |
| IsFrozen | Flag that indicates if the user is frozen in Salesforce. | boolean |
| Username | Contains the name that a user enters to log into the API or the user interface. | String |
| FirstName | User's first name. | String |
| LastName | User's last name. | String |
| EmailEncodingKey | Encoding that should be used during email communications. | String |
| Name | User's fullname. | String |
| UserPermissionsMarketingUser | Maps to the Marketing User Flag. | boolean |
| UserPermissionsOfflineUser | Maps to the Offline user Flag. | boolean |
| UserPermissionsSFContentUser | Maps to Sales Anywhere User. | boolean |
| Phone | User's phone number. | String |
| ProfileId | ID of the profile assigned to a user. | group |
| ProfileName | Name of the profile assigned to a user. | String |
| PublicGroups | Public groups are the entitlements for user. | PublicGroups |
| QueueNames | Queues assigned to the user. | String |
| ReceivesAdminInfoEmails | Receive the salesforce.com administrator newsletter. | String |
| Role | The Role assigned to a user. |  |
| UserType | This is user type of salesforce user i.e Standard, Partner, AutomatedProcess. | String |
| State | User's state. | String |
| Title | User's title. | String |
| ReceivesInfoEmails | Receive the salesforce.com newsletter. | String |
| PermissionSet | PermissionSet assigned to a user. | PermissionSet |
| PermissionSetGroup | PermissionSetGroup assigned to a user. | PermissionSetGroup |
| PermissionSetLicense | PermissionSetLicense assigned to a user. | PermissionSetLicense |
| ManagedPackage | Managed Package assigned to a user. | ManagedPackage |
| CollaborationGroup | Collaboration Group Id assigned to a user. | CollaborationGroup |
| UserLicense | User's license. | String |
| LanguageLocaleKey | The user's language. | String |
| LocaleSidKey | This is the user's locale. | String |
| TimeZoneSidKey | The timezone of the user. | String |
| FederationIdentifier | A Federation IDs is an identifier that is unique within a salesforce Organization. | String |
| ManagerId | User's manager id. | String |
| Workday\_Department\_ID\_\_c | Workday Department ID | String |
| Workday\_Department\_Name\_\_c | Workday Department Name | String |
| Workday\_Title\_\_c | Workday Title | String |
| TERRITORY\_EFFECTIVE\_DATE\_DEL\_\_C | TERRITORY EFFECTIVE DATE DEL | String |
| HOME\_STREET\_\_C | HOME STREET | String |
| HOME\_CITY\_\_C | HOME CITY | String |
| HOME\_ZIP\_\_C | HOME ZIP | String |
| SHIP\_ADDRESS\_\_C | SHIP ADDRESS | String |
| SHIP\_CITY\_\_C | SHIP CITY | String |
| SHIP\_ST\_\_C | SHIP ST | String |
| SHIP\_ZIP\_\_C | SHIP ZIP | String |

#### Correlation

|  |  |  |
| --- | --- | --- |
| Identity Attribute | Operator | Account Attribute |
| Network ID | = | EMPLOYEENUMBER |
| Employee ID | = | EMPLOYEENUMBER |
| Email | = | FederationIdentifier |

### Aggregation Schedule

Please see the “[Aggregations](#_Aggregations)” portion of the “Task Configuration” section below for more information regarding the Salesforce aggregation schedules.

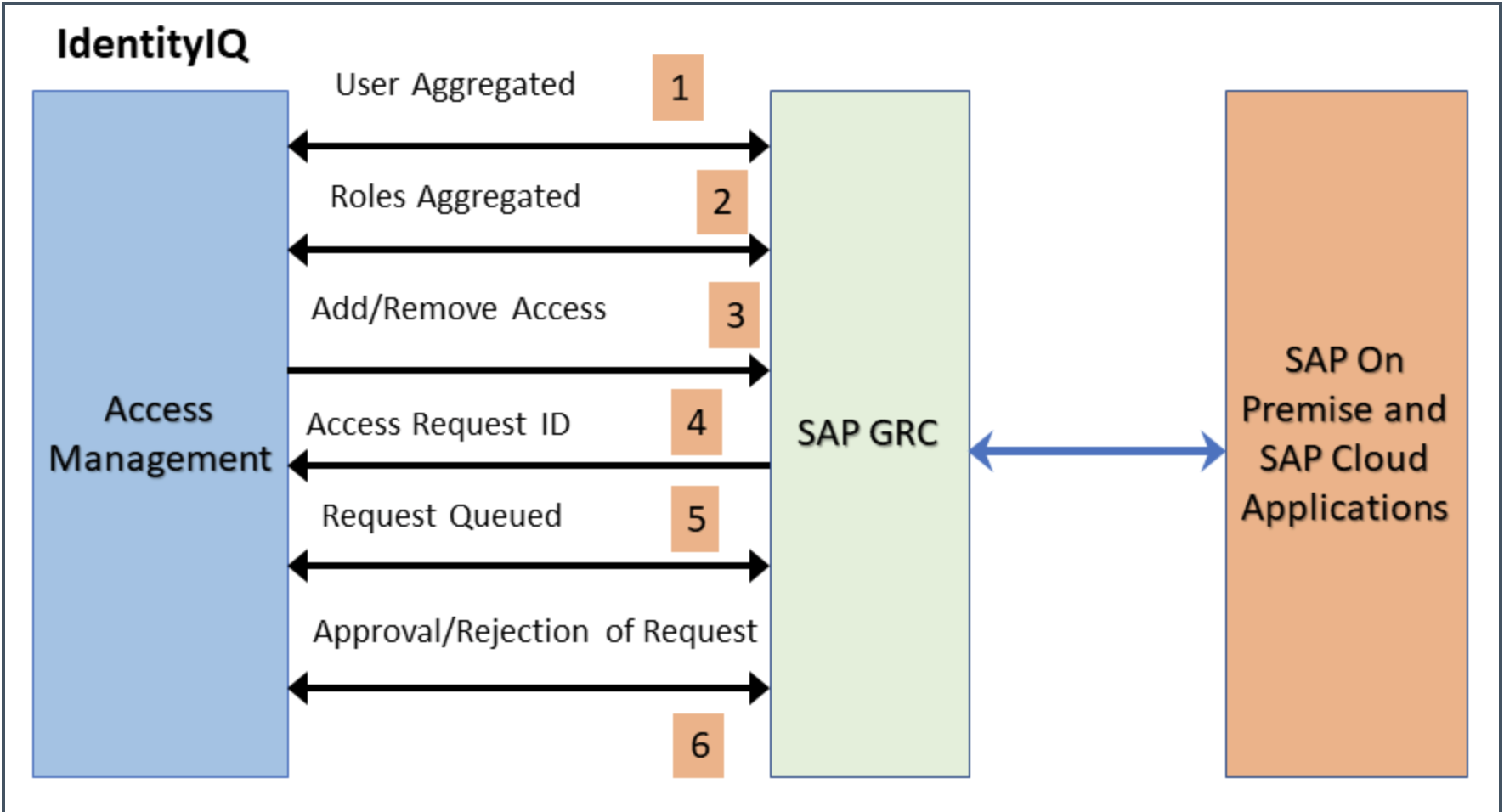
## SAP GRC

SAP GRC (governance, risk, and compliance) is a set of solutions and products that help to manage enterprise resources in a way that minimizes risk, builds trust, and lowers compliance costs. Products like SAP Risk Management, SAP Process Control, and SAP Audit Management let you automate GRC activities, improve control and visibility, monitor risks and enforce controls, and coordinate GRC through a unified technology platform.

The integration of SAP GRC application with SailPoint IdentityIQ will allow relevant users, identified by specific attributes, to be given coarse grained access to SAP GRC system. The fine-grained access into downstream SAP ecosystem will continue to be managed within SAP GRC as an SAP satellite systems.

**Integration Mode: Access Management**

This integration is used to aggregate all the Users and Roles from the systems (SAP SCM, JAVA, SAP ERP HCM, and so on) connected to SAP GRC and facilitates their provisioning by creating requests in GRC irrespective if there is risk present or not, as illustrated in the following figure:



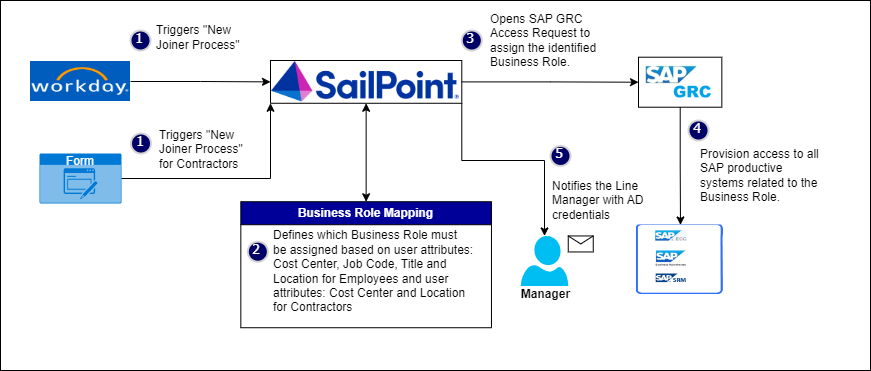
The figure explains the following methods:

* User Aggregated from the GRC connected system.
* Roles Aggregated from the GRC connected system.
* Request sent for adding or removing access to the connected system.
* Access Request ID created in GRC.
* Requests wait and are queued until a response is issued by SAP GRC.
* On the basis of the response returned from SAP GRC (approval or rejection in GRC), SAP GRC provisions or rejects the request, and the corresponding status is maintained in the SAP GRC source.

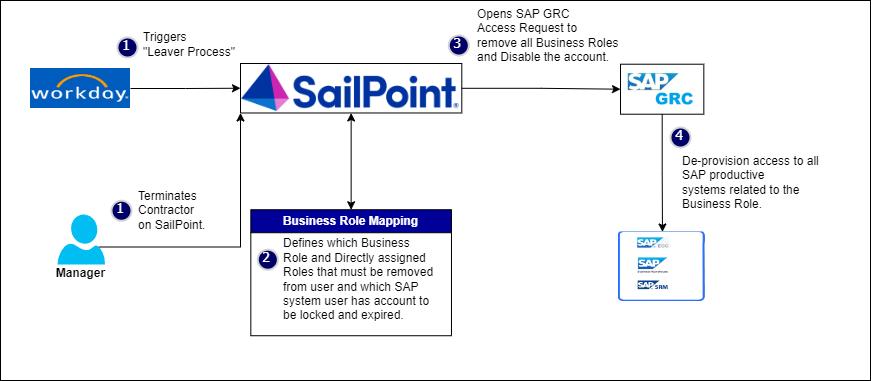
### Process Flow

Below diagrams outline the SailPoint - SAP GRC integration process flow for New Joiner, Leaver, Movers, Access Requests, Leave of Absence and Return from Leave of Absence.

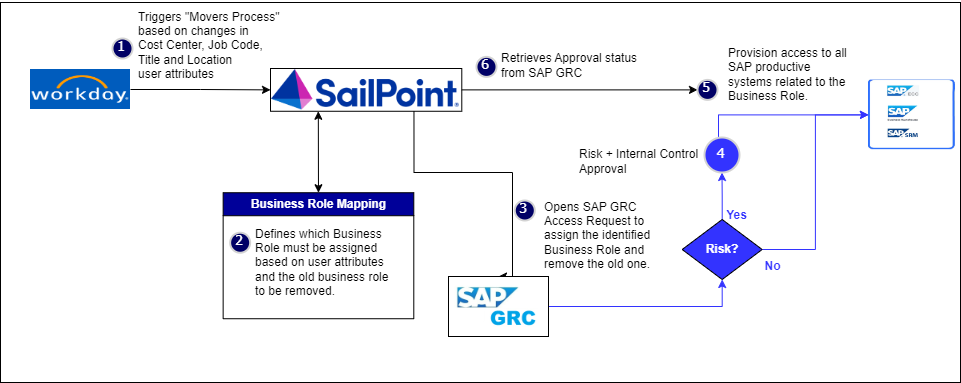
#### New Joiner Process



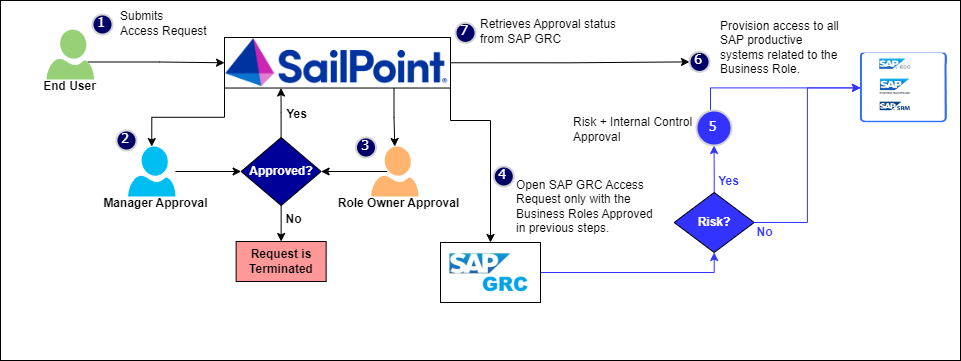
#### Leaver Process



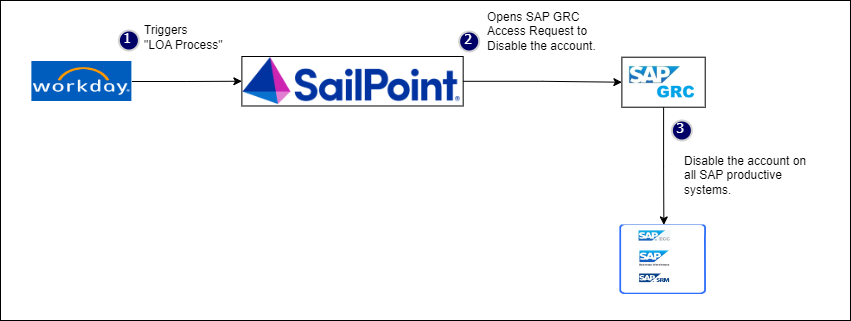
#### Mover Process



#### Access Request



#### Leave of Absence



#### Return from Leave of Absence



### Application Configuration

#### Configuration Details

|  |  |
| --- | --- |
| Parameter | Value |
| Name | SAP GRC |
| Owner | WG-SAPGRC-GRD2IIQ |
| Type | SAP GRC |
| Action(s) | Aggregation of accounts and business roles  Create accounts, assign/remove business roles  Disable accounts, Enable Accounts |
| Authoritative Application | False |

#### Connection Settings

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute Name | Dev | QA | Production |
|  | | | |
| Integration Mode | Access Management |  | Access Management |
| Host | sgrdpas.hdsupply.net |  |  |
| System Number | 00 |  |  |
| Client Number | 300 |  |  |
| Client Language | EN |  |  |
|  | | | |
| User Access | http://sgrdpas.hdsupply.net:8000/sap/bc/srt/rfc/sap/grac\_user\_acces\_ws/300/zns\_ws/zns\_ws |  |  |
| Request Details | http://sgrdpas.hdsupply.net:8000/sap/bc/srt/rfc/sap/grac\_request\_details\_ws/300/zreq\_details/zreq\_details |  |  |
| Search Roles | http://sgrdpas.hdsupply.net:8000/sap/bc/srt/rfc/sap/grac\_search\_roles\_ws/300/zsrch\_roles\_ws/zsrch\_roles\_ws |  |  |
| Role Details | http://sgrdpas.hdsupply.net:8000/sap/bc/srt/rfc/sap/grac\_role\_details\_ws/300/zrole\_details\_ws/zrole\_details\_ws |  |  |
|  | | | |
| Name | /SAILPOIN/SAIL\_READ\_TABLE |  |  |
| Page Size |  |  |  |
| Aggregation Delimiter |  |  |  |
|  | | | |
| Role Type | BUS |  |  |
| Business Process |  |  |  |
| Sub Process |  |  |  |
|  | | | |
| Access Request Priority | 006 |  | 006 |
| Disable Operation Configuration | | | |
| Disable Operation | Disable all systems connected to SAP GRC |  | Disable all systems connected to SAP GRC |
| Read-only Systems to Bypass | LDAP2GRD |  |  |
| Remove all roles when account is disabled | FALSE |  |  |
| Access Request Type Mapping | | | |
| Disable Account | 023 |  |  |
| Create Account | 034 |  |  |
| Modify Account | 002 |  |  |
| Enable Account | 035 |  |  |
| Provisioning Actions for Role | | | |
| Assign | 006 |  |  |
| Remove | 009 |  |  |
| Provisioning Actions for System | | | |
| Disable User | 004 |  |  |
| Enable User | 005 |  |  |
| Create User | 001 |  |  |
| Change & Lock User | 023 |  |  |
| Modify User | 002 |  |  |
| Change & Unlock User | 024 |  |  |

#### Account Schema

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Type |
| First Name | First name of the user | String |
| Last Name | Last name of the user | String |
| User ID | Id of the user | String |
| Email | Email of the user | String |
| Phone | Telephone number of the user | String |
| Department | Department of the user | String |
| Manager ID | Manager Id of the user | String |
| User Group | User group assigned to a user | String |
| User Type | Type of the user | String |
| Valid From | Valid from date of the user | String |
| Valid To | Valid to date of the user | String |
| Status | User Status (per connector) | String |
| System | System ID of the connector/source with highest sequence (priority) maintained in the data source configuration from SPRO. | String |
| Roles | Roles assigned to a user | group |

#### Group Schema

|  |  |  |
| --- | --- | --- |
| Attribute Name | Description | Type |
| Role UUID | Role universally unique identifier | String |
| Role Name | Name of the role | String |
| Role Desc | Role description | String |
| System | System to which role belongs | String |
| Role Type | Type of the role | String |
| Role Type Desc | Role type description | String |
| Landscape | Role landscape | String |
| Role Owner | Owner of the role | String |
| Business Process | Business Process to which role belongs | String |
| Sub Process | Sub Process to which role belongs | String |
| Role Status | Role Status | String |
| Associated Child Roles | Roles associated with the Composite or Business role | String, multi-valued |

#### Identity Attributes Mapping

Please refer to the “[Identity Attribute Matrix](#_Identity_Attribute_Matrix)” section of the Appendix for more information on each of the attributes coming from Workday and how they relate to attributes in SAP GRC.

#### Correlation

Correlation is required to match the accounts from the source system to identities in IdentityIQ. It describes in which order which identity attribute should be compared with which account attribute.

|  |  |  |
| --- | --- | --- |
| Identity Attribute | Operator | Account Attribute |
| Network ID | = | User ID |
| Email | = | Email |

### Manage Firefighter ID Access

Access to Firefighter IDs will be managed in SAP GRC. A soft link for SAP GRC Firefighter Access Request will be created in SailPoint IdentityIQ using Quicklink. Users who need access to Firefighter IDs will login to SailPoint and click on the Manage Firefighter Access quicklink and the user will be redirected to SAP GRC Firefighter access page.

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Dev | QA | Production |
| Quicklink Category | Manage Access |  | Manage Access |
| Quicklink Name | Manage Firefighter Access |  | Manage Firefighter Access |
| SAP Firefighter IDs URL |  |  |  |

### Aggregation Schedule

Please see the “[Aggregations](#_Aggregations)” portion of the “Task Configuration” section below for more information regarding the SAP GRC aggregation schedules.

### Birthright Roles

### Provisioning Policies

This section captures information sent to the downstream application on a per attribute, per operation level. As an example, the Create Account Provisioning Policy outlines the attributes required to be sent to SAP GRC when creating a new user account.

#### Create Account

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute | OOTB | Field Type | Value or Mapping |
| User ID | True | String | Network ID |
| First Name | True | String | First Name |
| Last Name | True | String | Last Name |
| Email | True | String | Email |
| Manager ID | True | String | Manager’s Network ID |
| Department | True | String | Location |

## CyberArk

This is a Logiplex Connector based application. This uses ‘Active Directory – Direct connector’an ‘Active Directory’ as Proxy Application.

Note: If a user having multiple AD accounts (primary and admin) requests CyberArk Access, triggering a create request on CyberArk, the CyberArk access would be added on the primary AD account. The CyberArk account would be seen on the primary AD account.

### Groups in scope

1. All entitlements that start with:

CN=GSC-CyberArkUsers-U0\5c ,OU=SecurityOnly,OU=1000,OU=Groups,DC=hdsdev,DC=hdsupply,DC=com

CN=GSC-CyberArkAudit-U0,OU=SecurityOnly,OU=1000,OU=Groups,DC=hdsdev,DC=hdsupply,DC=com

CN=GSC-CyberArkEPM-U0,OU=SecurityOnly,OU=1000,OU=Groups,DC=hdsdev,DC=hdsupply,DC=com

CN=GSC-CyberArkManager-U0,OU=SecurityOnly,OU=1000,OU=Groups,DC=hdsdev,DC=hdsupply,DC=com

CN=GSC-CyberArkVaultAdmin-U0,OU=SecurityOnly,OU=1000,OU=Groups,DC=hdsdev,DC=hdsupply,DC=com

CN=CY-

CN= HDS-MULE-NC-SEC-SAP

### Pre-requisite

Active Directory application to provide all the following API in working condition before start of the development:

a. Get User - One User

b. Update User Account

i. Assign Entitlement

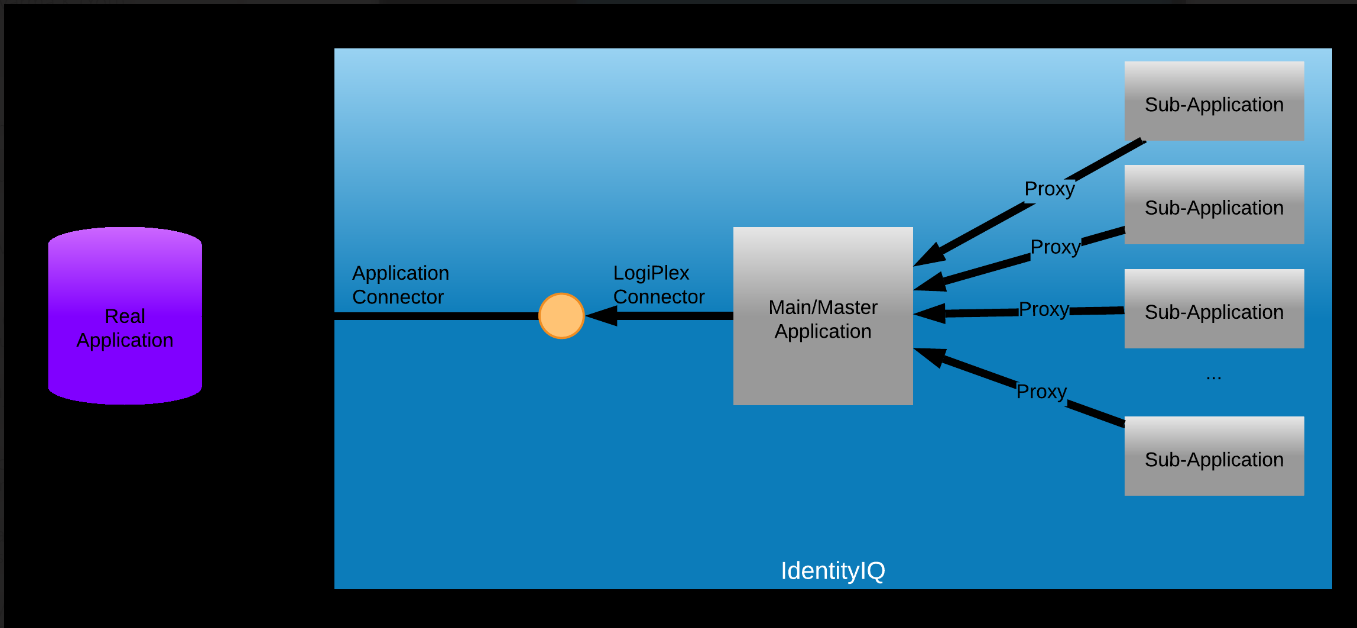
ii. Unassign Entitlement

c. Delete User Account

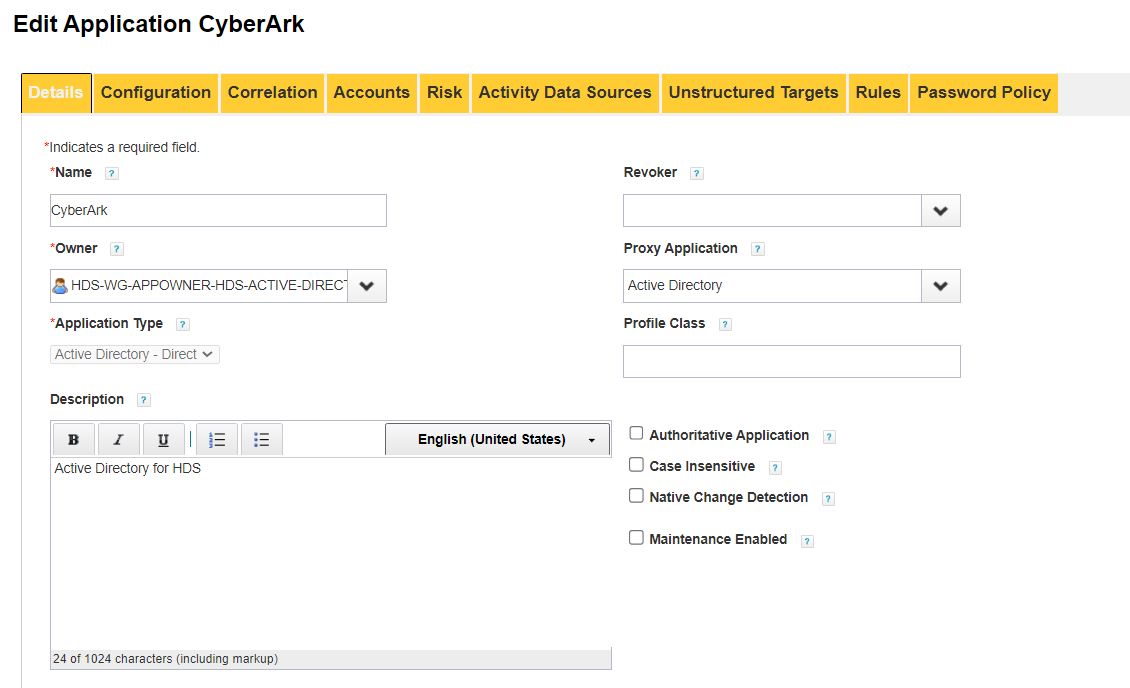
d. Account Aggregation - Get All Users

e. Group Aggregation

### Architecture Diagram



### Application Configuration



## ServiceNow

This is a Logiplex Connector based application. This uses ‘Active Directory – Direct connector’an ‘Active Directory’ as Proxy Application.

Note: If a user having multiple AD accounts (primary and admin) requests ServiceNow Access, triggering a create request on ServiceNow, the ServiceNow access would be added on the primary AD account. The ServiceNow account would be seen on the primary AD account.

### Groups in scope

1. All entitlements that start with:

CN=SN-

### Pre-requisite

Active Directory application to provide all the following API in working condition before start of the development:

a. Get User - One User

b. Update User Account

i. Assign Entitlement

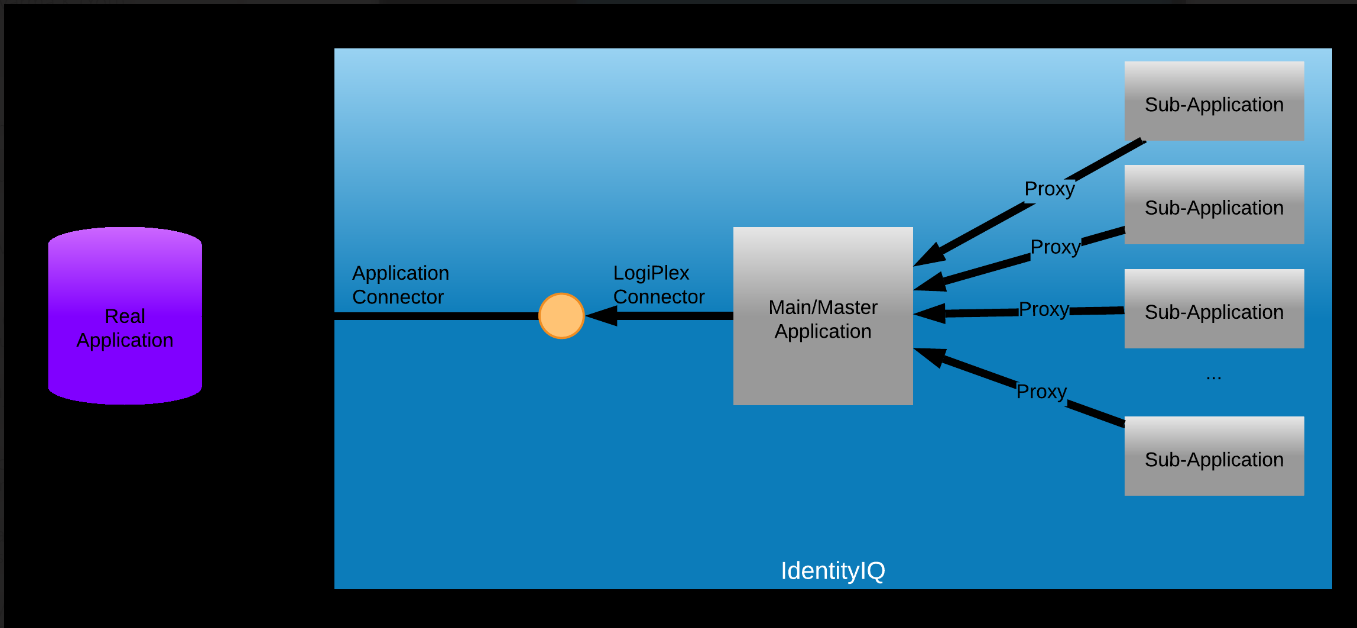
ii. Unassign Entitlement

c. Delete User Account

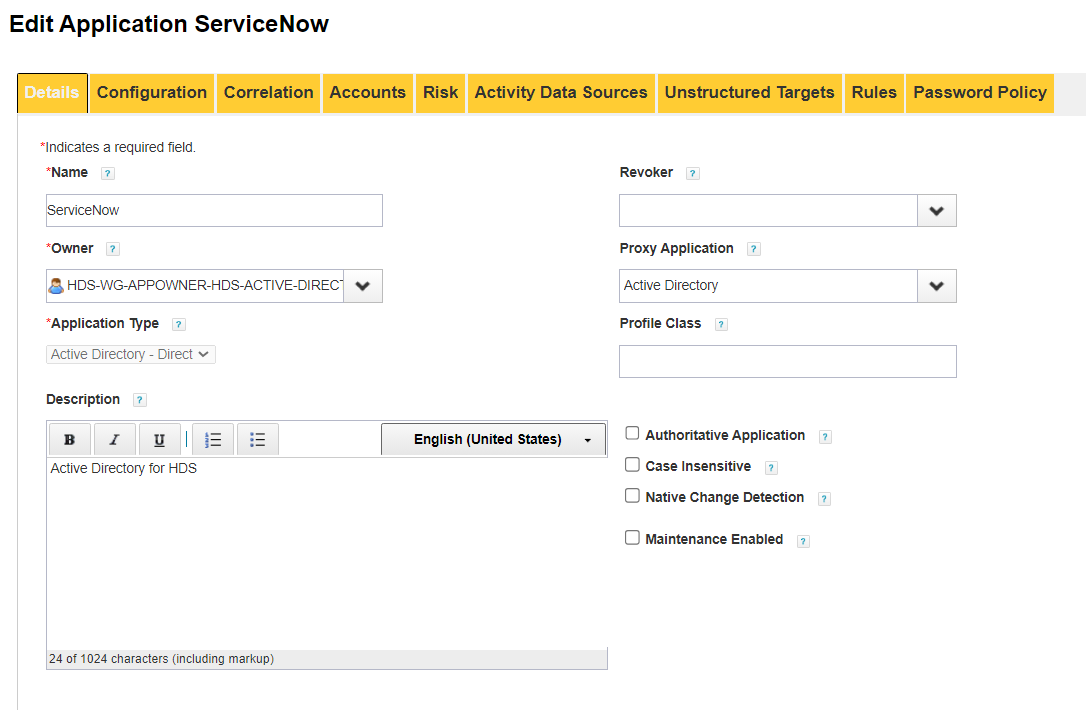
d. Account Aggregation - Get All Users

e. Group Aggregation

### Architecture Diagram



### Application Configuration



## SnowFlake

This is a Logiplex Connector based application. This uses ‘Active Directory – Direct connector’an ‘Active Directory’ as Proxy Application.

Note: If a user having multiple AD accounts (primary and admin) requests SnowFlake Access, triggering a create request on ServiceNow, the SnowFlake access would be added on the primary AD account. The SnowFlake account would be seen on the primary AD account.

### Groups in scope

1. All entitlements that start with:

CN=HDS-EDP-

### Pre-requisite

Active Directory application to provide all the following API in working condition before start of the development:

a. Get User - One User

b. Update User Account

i. Assign Entitlement

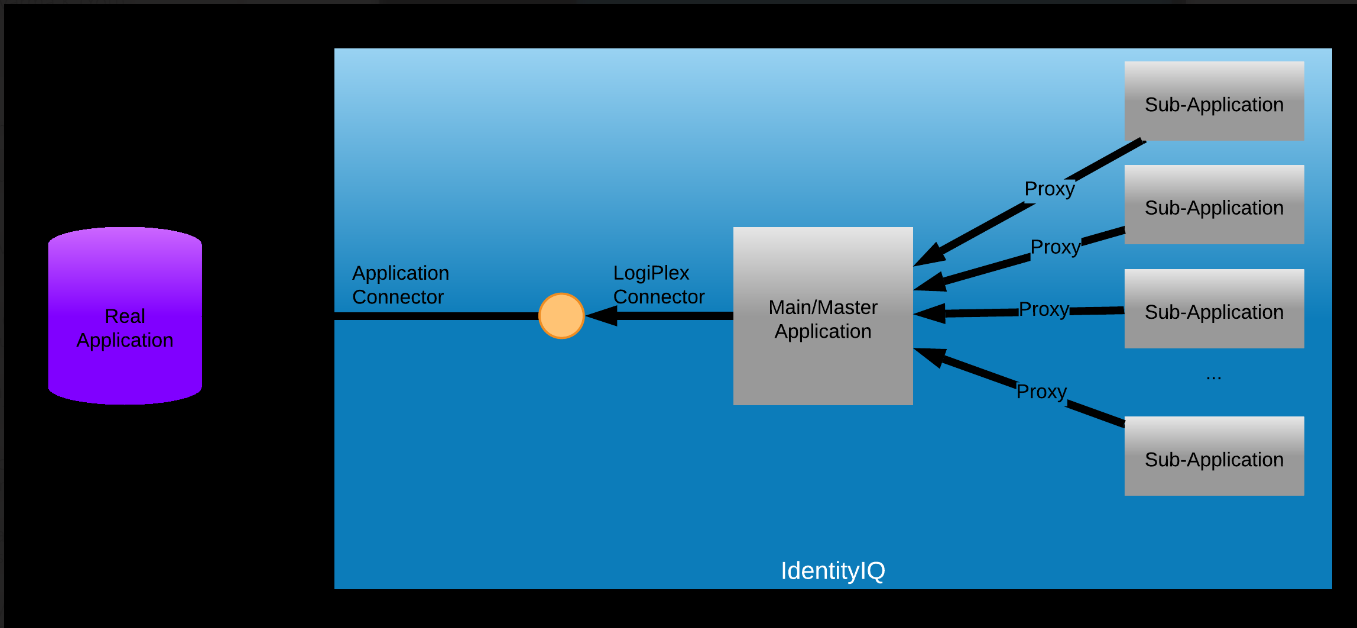
ii. Unassign Entitlement

c. Delete User Account

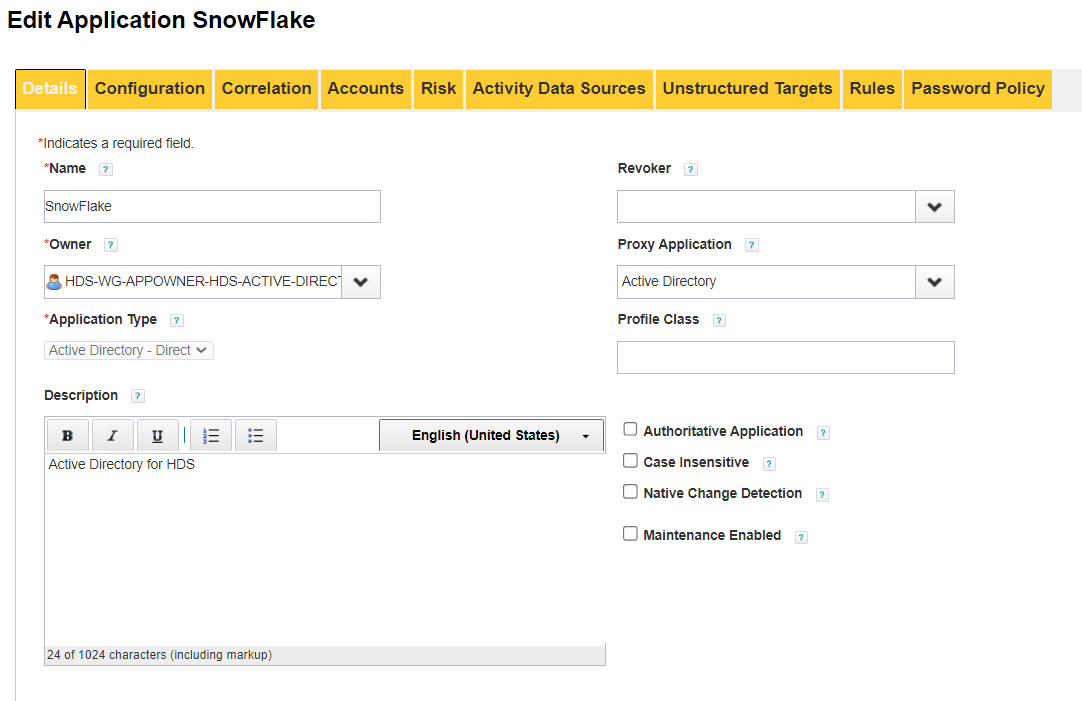
d. Account Aggregation - Get All Users

e. Group Aggregation

### Architecture Diagram



### Application Configuration



# Life Cycle Events

Lifecycle Events are workflows that are launched, usually as a result of a refresh task. The most common Lifecycle Events are Joiner (on-boarding), Leaver (termination), and Mover (transfer). Each lifecycle event consists of a triggering mechanism and a workflow. The triggering mechanism is often a rule that evaluates the previous Identity with the new Identity and determines whether the given event should be launched. The workflow is what gets launched.

Each process triggered via Lifecycle Event will provision or deprovision access as per business requirements. The following sections will describe each Lifecycle event and its associated requirements.

## Pre-Hire

The pre-hire lifecycle event is a data-driven process to create new identity records in IdentityIQ and associated Active Directory, Salesforce and SAP GRC accounts leveraging birthright and business roles.

The Joiner lifecycle event will be comprised of two (2) components:

* Pre-Hire Identity Trigger
  + This portion of the event determines which identities meet the criteria for the Joiner workflow
* Pre-Hire Workflow
  + This portion of the event houses the technical and business logic used to control what happens when an identity is selected for joiner processing

### Pre-Hire Identity Trigger

The Pre-hire Identity Trigger will evaluate the following items to determine if a user is eligible for joiner processing:

* If Identity is of Type = “Employee”, Employee Status is ’Pre-Hire’ and LifeCycleAction is empty?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for joiner processing
* If the identity is of Type = “Contractor”, Employee Status is ’Pre-Hire’ and LifeCycleAction is empty?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for joiner processing

### Workflow

Once IdentityIQ determines that an identity is marked for joiner processing, the HDS-RapidSetup-Pre-Hire Workflow will be triggered individually for that identity. The following explains different joiner workflow steps:

* Calculate Birthirght roles on the user and create a plan
* Active Directory create request is added to the plan for both Employees and Contractors identity types.
* After a new account is created in Active Directory, the Joiner workflow will send an email notification [EMT02](#_EMT02:_Manager_Mail) to the user’s manager that includes the following data points:
  + AD Account Display Name
  + Network ID
  + Password

## Joiner

The Joiner lifecycle event is a data-driven process to create new identity records in IdentityIQ and associated Active Directory, Salesforce and SAP GRC accounts leveraging birthright and business roles.

The Joiner lifecycle event will be comprised of two (2) components:

* Joiner Identity Trigger
  + This portion of the event determines which identities meet the criteria for the Joiner workflow
* Joiner Workflow
  + This portion of the event houses the technical and business logic used to control what happens when an identity is selected for joiner processing

### Joiner Identity Trigger

The Joiner Identity Trigger will evaluate the following items to determine if a user is eligible for joiner processing:

* If Identity is of Type = “Employee”, Employee Status is ’Active’ and LifeCycleAction is ‘Pre-Hire'?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for joiner processing
* If the identity is of Type = “Contractor”, Employee Status is ’Active’ and LifeCycleAction is ‘Pre-Hire'?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for joiner processing

### Workflow

Once IdentityIQ determines that an identity is marked for joiner processing, the HDS-LifecycleEvent-Joiner Workflow will be triggered individually for that identity. The following explains different joiner workflow steps:

* Calculate Birthirght roles on the user and create a plan
* Active Directory create request is added to the plan for both Employees and Contractors identity types.
* If the pre-hire was not triggered for the user, after a new account is created in Active Directory through joiner process, an email notification [EMT02](#_EMT02:_Manager_Mail) is sent to the user’s manager that includes the following data points:
  + AD Account Display Name
  + Network ID
  + Password
* If the pre-hire was triggered on the user, then AD account creation and email sending steps are skipped.
* For contractor identities, email notification [EMT01](#_EMT01:_Mandatory:_Contractor) for “Mandatory: Contractor Compliance Program Checklist” is sent to the manager, contractor’s external email address and compliance team workgroup email.
* In case there is a GRC related birthright access on the user, it is provisioned one hour after the AD account provisioning completes.

## Mover

The Mover lifecycle event is a data-driven process to provision/deprovision the user’s access to associated downstream accounts, based on the defined matching criteria on roles and entitlements, whenever there is change in identity’s attributes like job code, cost center, department, etc.

Mover / Transfer of the users will be performed using Refresh Identity Cube task. The attributes will be synchronized to the target applications and the provision/deprovision the user’s access to associated downstream accounts, based on the defined matching criteria on roles and entitlements performed with following options enabled on the task:

* Refresh Identity Cube
  + Refresh identity attributes: Checked
  + Refresh assigned, detected roles and promote additional entitlements: Checked
  + Synchronize attributes: Checked

Mover Implementation:

OOTB Rapid setup configuration is used to achieve Mover Functionality.

OOTB RapidSetup – Mover Workflow is customized by adding a new step to Refresh Identity with Attribute Synch Enabled and the workflow is renamed as “HDS-Rapidsetup-Mover”.

In the Rapid Setup Configuration: Mover process is enabled, joiner processing is checked in, certifications are not enabled, and attributes required for trigger are added in the trigger filter conditions with OR. Refer this [JIRA](https://hdsdigital.atlassian.net/browse/IAM-152) for list of attributes used to trigger the Mover Workflow.

Whenever any attribute listed in these conditions is CHANGED, mover is triggered, Rapid Setup – Mover LifeCycleEvent is launched.

Workflow starts processing to check to add/remove existing birthright roles and it creates access request with flow as “Lifecycle Mover”

At the end, it runs the refresh for the Identity, with attribute synchronization option enabled for any attributes provisioning to target if there’s any change.

## Leaver

The Leaver workflow is a data-driven process to process the termination of identity records in IdentityIQ and any associated downstream accounts correlated to the terminated user’s identity cube.

System Access for employees is calculated based on attribute values of the Identity from Workday in the table below. User’s access is disabled when System Access = “N” and the access is enabled when System Access = “Y”

For Contractor, System Access = “N” when contractor’s end date is in past, or the contractor is terminated else System Access = “Y”

|  |  |  |  |
| --- | --- | --- | --- |
| **Employee Type** | **Country** | **Employee Status** | **System Access** |
|  |  | T (Terminated Immediately) | N |
|  |  | T (Retired/Deceases) | N |
|  |  | A (Active) | Y |
|  |  | U (Termed with pay) | N |
|  |  | N (Future Dated Hire) | N |
|  |  | Q (Retired with Pay) | N |
|  |  | R (Retired Without Pay) | N |
| Hourly | Not Canada | P (On Paid Leave) | N |
| Hourly | Canada | P (On Paid Leave) | Y |
| Salaried | Any country | P (On Paid Leave) | Y |
| Hourly | Not Canada | L (On Unpaid Leave) | N |
| Hourly | Canada | L (On Unpaid Leave) | Y |
| Salaried | Any country | L (On Unpaid Leave) | Y |
|  |  | D (Deceased) | N |

The Leaver is a three-step process, which will perform the following actions according to the schedule below:

* Day 0:
* Disable AD account when Employee status changes to ‘Terminated’ or ‘Immediate Termination’.
* For SAP GRC application, on the day of termination, disable user’s account and remove all the access.
* For Salesforce application, on the day of termination,

Set NULL values to blank out the below fields:

* MANAGER
* MANAGERID
* TERRITORY\_EFFECTIVE\_DATE\_DEL\_\_C
* TERRITORYID\_\_C
* CALLCENTERID
* EXTENSION
* PHONE
* FAX
* MOBILEPHONE
* TEAM\_\_C
* OFFICE\_PHONE\_\_C

Set the values of below fields:

* Mgr At Termination: ID of manager
* USERPERMISSIONSSUPPORTUSER: FALSE
* LAST\_DAY\_\_C: Termination Date
* DIGITAL\_QUOTING\_USER\_\_C: FALSE

Prefix NOTES field with below information:

* Last Day
* Title
* Team
* Manager
* Terrid
* Deactivation Date

Note: If HR Status = “T” and Termination Reason = “Terminated Immediately” then disable all the access immediately else disable the access after midnight of last working day.

A Lifecyle Event, Leaver Disable will be configured which will get triggered when Employee Status changes to ‘Terminated’ or ‘Immediate Termination’. It will be configured to call HDS-RapidSetup-Leaver Disable WF to perform above operations.

* Day 30:

Remove security groups labeled with \*SN-\* from regular account and privileged account. The regular AD account will be moved to Inactive Users OU. The privileged AD account will remain in Admin Users OU.

A Lifecyle Event, Leaver InactiveOU will be configured which will get triggered when termination date of the identity is more than 30 days and LifecycleAction is ‘Leaver Disable’. It will be configured to call HDS-LifecycleEvent-LeaverInactiveOU WF to perform above operations.

* Day 90:

Delete both the regular and privileged AD accounts on the user.

* + If the account was re-enabled and/or moved out of the Inactive Users OU, don’t do anything as a part of this event.

A Lifecyle Event Leaver Delete, will be configured which will get triggered when termination date of the identity is more than 90 days and LifecycleAction is ‘Leaver InactiveOU’. It will be configured to call HDS-LifecyleEvent- LeaverDeleteW F to perform above operations.

#### HDS-LCE-Leaver

Identity Trigger

The Identity Trigger, Leaver Disable, will evaluate the following items to determine if a user is eligible for processing of disable access:

* Did the Employee Status attribute value of the Identity change to ‘Terminated’ or ‘Immediate Termination’ and for ‘Terminated’ scenario, if the EOD is reached. (Also check if previous LifecycleAction is either Joiner or Pre-Hire)
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for processing

Workflow

Once IdentityIQ determines that an identity is marked for disable access processing, the HDS- RapidSetup -LeaverDisable workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Build Plan** –
  + For Active Directory application, build a plan to disable both regular and privileged account of the user. Set
* For SAP GRC application, build a plan to disable user’s account and remove all the access when user is terminated.
* For Salesforce application, build a plan to perform below operations when user is terminated:

|  |  |
| --- | --- |
| Field | Action |
| MobilePhone | BLANK |
| Phone | BLANK |
| Office\_Phone\_\_C | BLANK |
| Mgr\_at\_Termination\_\_c | Take the current manager ID and put the User ID in the Mgr\_at\_Termination\_\_c field |
| Extension | BLANK |
| CallCenterId | BLANK |
| TerritoryId\_\_C | BLANK |
| profileId | Change to 00e70000000wM7d which is profile name “Inactive” |
| Digital\_Quoting\_User\_\_c | BLANK |
| UserPermissionsSupportUser | Blank, or set the checkbox to false |
| Last\_Day\_\_c | Last day worked from Workday |
| Team\_\_c | BLANK |
| Territory\_Effective\_Date\_del\_\_c | BLANK |
| IsActive | Set to boolean False |
| UserRoleId | Set to 00E70000000xe9o which is Role name “Terminated” |
| ManagerId | BLANK |
| Fax | BLANK |
| Notes\_\_C | Add to the beginning of the existing notes on its own line what was done. In this format: SR: Last day worked 7/24/2024 Former info: e-Business Customer Care Associate, TEAM: , Manager: Martell Rogers, TerrID: , Deactivated: 7/31/2024 1:19:48 PM per RITM0569142 |

Prefix NOTES field with below information:

* Last Day
* Title
* Team
* Manager
* Terrid
* Deactivation Date
* **Initialize** – Call the SP Identity Request Initialize subprocess WF to initialize the request, this includes auditing, building the approvalset, compiling the plan into project and checking policy violations.
* **Provision** – Call the SP Identity Request Provision subprocess WF that will process the approval decisions and do provisioning. This includes calling any configured provisioning connectors and building manual actions.
* **Finalize** – Call the SP Identity Request Finalize subprocess WF that can audit/finalize the request.

#### HDS-LCE-RemoveAccessAfter30Days

Identity Trigger

The Identity Trigger, Leaver InactiveOU, will evaluate the following items to determine if a user is eligible for processing of disable access:

* Is termination date of the identity more than 30 days and less than 31 days in past and LifecycleAction is Leaver Disable?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for processing

Once IdentityIQ determines that an identity is marked to remove access after 30 days, the HDS-LifecycleEvent- LeaverInactiveOU workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Build Plan** – When user is of type “Employee” or user is of type “Contractor”, build a plan to move the regular AD account to Inactive Users OU. Remove only ‘SN-’ group membership from both regular and priviledged accounts.
* **Initialize** – Call the SP Identity Request Initialize subprocess WF to initialize the request, this includes auditing, building the approvalset, compiling the plan into project and checking policy violations.
* **Provision** – Call the SP Identity Request Provision subprocess WF that will process the approval decisions and do provisioning. This includes calling any configured provisioning connectors and building manual actions.
* **Finalize** – Call the SP Identity Request Finalize subprocess WF that can audit/finalize the request.

#### HDS-LCE-DeleteAccountAfter90Days

Identity Trigger

The Identity Trigger, Leaver Delete will evaluate the following items to determine if a user is eligible for processing of deleting account:

* Is termination date of the identity more than 90 days and less than 91 days in past and Lifecycle Action is Levaver InactiveOU?
  + If yes, proceed to execute the workflow
  + If no, stop here and do not return the identity for processing

Once IdentityIQ determines that an identity is marked to delete account after 90 days, the HDS-LifecycleEvent- Delete workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Build Plan** – Build a plan to delete both regular AD account and priviledged AD account.
* **Initialize** – Call the SP Identity Request Initialize subprocess WF to initialize the request, this includes auditing, building the approvalset, compiling the plan into project and checking policy violations.
* **Provision** – Call the SP Identity Request Provision subprocess WF that will process the approval decisions and do provisioning. This includes calling any configured provisioning connectors and building manual actions.
* **Finalize** – Call the SP Identity Request Finalize subprocess WF that can audit/finalize the request.

## C2Hire

For C2Hire, the contractor’s identity will be terminated from IdentityIQ. The C2Hire will be onboarded as a new employee in Workday.

The C2Hire’s contractor identity will be offboarded from IdentityIQ and all the access will be removed as per Leaver process.

The C2Hire’s new Identity will be aggregated from Workday and all the birthright provisioning to downstream applications will be performed as the Joiner process.

## Rehire

The Rehire lifecycle event is a data-driven process to process the return of employees after termination. The identity is enabled in IdentityIQ and access to any associated downstream accounts is enabled for below applications:

Active Directory

SAP GRC

### Identity Trigger

The Identity Trigger, Rehire, will evaluate the following items to determine if a user is eligible for processing of rehire:

* For contractor,
  + HR Status changed from T to A
  + Termination date is in future
* For employees,
  + HR Status changed from T to A
  + Employee ID has not changed

**Identity Trigger Configuration**

|  |  |
| --- | --- |
| Attribute | Value |
| Event Type | Rule |
| Rule | HDS-IdentityTrigger-Rehire |
| Business Process | HDS-LifecycleEvent-Rehire |

**Included Identities Match List Filter**

|  |  |
| --- | --- |
| Attribute | Value |
| Type | Employee or contractor |
| HR Status | A |

### Workflow

Once IdentityIQ determines that an identity is marked for rehire processing, the HDS-LifecycleEvent-Rehire workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Initialize** – Set Life Cycle Action to Joiner.
* **Launch Joiner** – If the user does not have Active Directory account, and if hire date is in future launch HDS-RapidSetup-PreHire WF else launch HDS-LifecycleEvent-Joiner WF and Stop.
* **Move AD Account From InActiveOU** – If the user had Active Directory Account and is in InActive OU, then build plan move the OU to Users OU.
* Build Plan To Enable Accounts – Build plan to enable Active Directory and SAP GRC accounts.
* **Provision** – Call LCM Provisioning subprocess WF to process the plan.
* **Send Email** – Send an email to IAM operations team for any provisioning error.

## LOA

The LOA lifecycle event is a data-driven process, to disable the access of the employees who is hourly and not in Canada and goes on Leave of Absence. The access of these employees is disabled on below applications:

Active Directory

SAP GRC

### Identity Trigger

The Identity Trigger, LOA, will evaluate the following items to determine if a user is eligible for processing of LOA:

**Identity Trigger Configuration**

|  |  |
| --- | --- |
| Attribute | Value |
| Event Type | Attribute Change |
| Attribute | System Access |
| Previous Value Filter | Y |
| New Value Filter | N |
| Business Process | HDS-LifecycleEvent-LOA |

**Included Identities Match List Filter**

|  |  |
| --- | --- |
| Attribute | Value |
| Type | employee |
| HR Status | A |
| Employee Status | OnLeave |

### Workflow

Once IdentityIQ determines that an identity is marked for LOA processing, the HDS-LifecycleEvent-LOA workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Set Lifecycle Action** – Set Lifecycle Action of the identity to “LOA”
* **Build Plan** – Build Provisioning plan to disable the accounts on the application listed above.
* **Provision** – Call LCM Provisioning WF to provision the disable account operation on the target applications.
* **Send Email** – Send an email to IAM operations team for any provisioning error.

## ReturnFromLOA

The ReturnFromLOA lifecycle event is a data-driven process, to enable the access of the employees who is hourly and not in Canada and returns from Leave of Absence. The access of these employees is enabled on below applications:

Active Directory

SAP GRC

### Identity Trigger

The Identity Trigger, ReturnFromLOA, will evaluate the following items to determine if a user is eligible for processing of ReturnFromLOA:

**Identity Trigger Configuration**

|  |  |
| --- | --- |
| Attribute | Value |
| Event Type | Attribute Change |
| Attribute | Employee Status |
| Previous Value Filter | OnLeave |
| New Value Filter | Active |
| Business Process | HDS-LifecycleEvent-ReturnFromLOA |

**Included Identities Match List Filter**

|  |  |
| --- | --- |
| Attribute | Value |
| Type | employee |
| HR Status | A |
| System | Y |

### Workflow

Once IdentityIQ determines that an identity is marked for ReturnFromLOA processing, the HDS-LifecycleEvent- ReturnFromLOA workflow will be triggered individually for that identity. The workflow will have the following steps:

* **Set Lifecycle Action** – Set Lifecycle Action of the identity to “Joiner”
* **Build Plan** – Build Provisioning plan to enable the accounts on the application listed above.
* **Provision** – Call LCM Provisioning WF to provision the enable account operation on the target applications.
* **Send Email** – Send an email to IAM operations team for any provisioning error.

# Contractor Management

Contractor identities/accounts are accounts of an external individual who will access the organization's systems, applications or resources. The contractor identity/account in SailPoint will be active for a specific duration, until the contract expires. Contractor identity can be identified by the type attribute value of identity i.e contractor.

Contractor Management includes:

Requesting new contractors

Edit existing contractors

Extending contract duration

Terminating contractor

A custom quick link and workflow will be developed for contingent workforce management. The workflow will include dynamic forms with which SailPoint will get the data and will build a plan to create a new identity cube for the contractor or managing the contractor identity/accounts.

## Quick Link

The quick link will be built with the following options:

* **QuickLinkCategory Display Name** – Contingent Workforce Management
* **Display Name** – Contractor Management
* **Action** – workflow
* **Workflow Name** – HDS-ContractorManagementWorkflow
* **Visibility** – All employees will be able to access the quicklink but the operations to be performed on/for contractor may differ.

## Workflow Steps

The workflow HDS-ContractorManagementWorkflow will handle the management of contractor identities. The workflow will have following steps:

* **Build Form**
  + Get the Contractor operation to be performed using SelectOperation form displayed initially.
  + Display form based on the operation selected and select contractor if required, on which the operation needs to be performed. Get and set variable to form.
  + Transition to Enter Form
* **Enter Form**
  + Display form, tied to an identityModel object that will contain the values entered on the form
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit (next), Back (back), Cancel Request (cancel)
  + Transition to - Build Plan on Approved (next)

- Enter Form on Rejected (back)

- End on Cancel Request (cancel).

Note: the workflow must be transient for cancel to work.

* **Generate Employee Number**
  + The employee number for the contractor will be generated using the DB sequence [identityiq].[USER\_ID\_SEQ]. The Network Id of the Contractor will be the same as the employee number. The employee number sequence for Contractors in Dev starts from 8000000 and from 9000000 in Prod.
* **Build Plan**
  + Dynamically build a provisioning plan using the identity model
* **Provision**
  + Call Sub-Process HDS-LCM Create and Update of type LCMIdentity. This will Initialize, Approve, and Provision the plan
* **Close Request**
  + Update the links with any required account attributes

## HDS-Select Operation

HDS-SelectOperationForm is the first menu option form displayed for contractor management that will be visible to all the employees. The form, HDS-SelectOperationForm is developed with the following fields:

* **Select Operation –** Combobox to display list of below operations
  + New Contractor
  + Edit
  + Extend
  + Terminate

Here, in “Select Operation” dropdown only the Managers and administrators will be able to see all the 4 options. However, for employees only “New Contractor” option would be visible.

* **Select Identity –** Combobox to display list of Identities
  + This field will be hidden by default or if the selected operation is “Request New Contractor”. It will be visible for other selected operations.
  + Identities of type “Contractor” will be displayed in drop down according to the operation selected and manager hierarchy.

## New contractor

To request a new contractor identity in SailPoint, the forms HDS-RequestNewContractorForm and HDS-ReviewRequestNewContractorForm are displayed to the requestor. HDS-RequestNewContractorForm, has two sections and will take inputs from requestor and HDS- ReviewRequestNewContractorForm will display all the details submitted by requester to review/confirm the provided details. The forms are developed with the following fields:

### Form

#### HDS-RequestNewContractorForm

**Requester’s Information**

**Display Name** – Read only, showing display name of the requester

**Type** – Read only, Text, showing type of requester

**User Status** – Read only, Text, showing user status of requester

**LOB** – Read only, Text, showing LOB of requester

**Title** – Read only, Text, showing title of requester

**Employee ID** – Read only, showing employee ID of requester

**Contractor Information**

**Contractor Company** –Text, Required

**Contractor Company Email** –Text, Required

**First Name** –Text, Required

**Middle Name** –Text

**Last Name** –Text, Required

**LOB** – Combobox, values: “FM”, Required

**Manager Name** – Combobox, display list of all active managers, Required

**Cost Center ID –** Text, Read Only, Required

**HDS Work Address** – Combobox, display list of HDS work addresses fetched from HDS-WorkLocationDetails custom object. Required

**Start Date** – Date Range, Required

**End Date** – Date Range, Required

**Business Reason** –Text Area, Required.

**Form Validation:**

**Contractor Company Email:**

field value should not exist in SailPoint already.

field value domain should not be @hdsupply.com, @hdsupplydev.com, @hdsdev.hdsupply.com.

#### HDS-ReviewRequestNewContractorForm

The form HDS-ReviewRequestNewContractorForm is developed with all the fields in read only format.

**Requester’s Information**

**Display Name** – Read only, showing display name of the requester

**Type** – Read only, Text, showing type of requester

**User Status** – Read only, Text, showing user status of requester

**LOB** – Read only, Text, showing LOB of requester

**Title** – Read only, Text, showing title of requester

**Employee ID** – Read only, showing employee ID of requester

**Contractor Information**

**Contractor Company** –Read only, Text, Required

**Contractor Company Email** –Read only, Text, Required

**First Name** –Read only, Text, Required

**Middle Name** –Read only, Text

**Last Name** –Read only, Text, Required

**LOB** – Read only, Combobox, values: “FM”, Required

**Manager Name** – Read only, Combobox, display list of all active managers, Required

**Cost Center ID –** Read only, Text, Read Only, Required

**HDS Work Address** – Read only, Combobox, display list of HDS work addresses fetched from HDS-WorkLocationDetails custom object. Required

**Start Date** – Read only, Date Range, Required

**End Date** – Read only, Date Range, Required

**Business Reason** –Read only, Text Area, Required.

## Edit/Extend/Terminate Existing Contractor

The form, HDS-ModifyExistingContractorForm is used for Edit, Extend and Terminate operations. Also, the form HDS-ReviewModifyExistingContractorForm will display all the details submitted by requester to review. The forms are developed with the following fields:

### Form

#### HDS-ModifyExistingContractorForm

* + **Select Identity** – Read Only
  + **Contractor Company** – Read Only
  + **Contractor Company Email** – Read Only
  + **First Name** –Read Only
  + **Middle Name** –Read Only
  + **Last Name** –Read Only
  + **LOB** – Read Only
  + **Manager Name** – Combobox, Required, display current manager and list of all active managers
  + **Cost Center** – Combobox, Required, displays a list of cost centers associated with current manager’s cost center hierarchy.
  + **HDS Work Address** – Combobox, display current work address and list of HDS work address fetched from HDS-Work Address Locations custom object, Read only for Extend Contractor
  + **Start Date – Hidden for Edit Contractor operation, Read only for Extend Contractor**
  + **End Date – Hidden for Edit Contractor operation, Editable for Extend Contractor**
  + **Business Reason** – Text Area, Required

#### HDS-ReviewModifyExistingContractorForm

The form HDS-ReviewModifyExistingContractorForm is developed with all the fields in read only format.

* + **Select Identity** – Read Only
  + **Contractor Company** – Read Only
  + **Contractor Company Email** – Read Only
  + **First Name** –Read Only
  + **Middle Name** –Read Only
  + **Last Name** –Read Only
  + **LOB** – Read Only
  + **Manager Name** – Read only, Combobox, Required, display current manager and list of all active managers
  + **Cost Center** – Read only, Combobox, Required, displays a list of cost centers associated with current manager’s cost center hierarchy.
  + **HDS Work Address** – Read only, Combobox, display current work address and list of HDS work address fetched from HDS-Work Address Locations custom object, Read only for Extend Contractor
  + **Start Date – Hidden for Edit Contractor operation, Read only for Extend Contractor**
  + **End Date – Hidden for Edit Contractor operation, Editable for Extend Contractor**
  + **Business Reason** – Read only, Text Area, Required

## HDS Contractor Expiry Notification

Managers should be notified in advance when contractor is about to expire in the system so that manager can extend the contractor in advance if required.

Expiry Notification would be sent out to the Manager on day 30, 14, 7, 6, 5, 4, 3, 2, 1 before expiration date to take appropriate actions.

Expiry Notification is implemented using an Advanced Policy “HDS-ContractorExpirationPolicy” in IdentityIQ and should be executed once a day only by running/scheduling “Check Active Policies” Task.

# Service Account Management

The term “service account” can be used to describe several categories of system accounts. The key characteristic of a service account is its persistence beyond the tenure of an individual with the organization; that is: it should not be tied to an individual user and should not be deleted or disabled when a user leaves the organization.

At HD Supply, we have two types of service account:

Service Account

Non-Person Account

Each service account will be represented as a standalone identity cube in IdentityIQ.

Service Account Management includes loading and identifying existing accounts, creation of new accounts/cubes, managing account ownership, managing account access, and deletion of accounts.

## Identify/Load Service Accounts

Service Accounts include all accounts used by more than one user and generally not deleted when anyone leaves. Each service account will be stored in a single, individual cube. The cube will only contain the service account, and the name of the cube will reflect:

* It is not a user
* The name of the application on which service account is created
* The name of the account

A prefix should be added to split out the secondary cubes on the Identity Warehouse page. The unique name will be set in the Creation of secondary accounts for each given application. The naming scheme of the cube will be as follows:

**$appName + “:” + $accountName**

$appName is the name of the application. For Active Directory application, $appName is “Active Directory”

$accountName will be based on application-specific logic. For Active Directory, $accountName will prefix with “svc\_” for service accounts and “np\_” for non-person accounts.

### Active Directory Service Accounts

The Account Type link attribute will distinguish the account from regular accounts. The attribute value will be determined by the following logic:

The following breaks down the different service account types:

|  |  |
| --- | --- |
| Type | Value |
| Service Accounts | service |
| Non-Person Accounts | non-person |

#### Correlation Logic

Correlation is required to match the accounts from the source system to identities in IdentityIQ. It describes in which order which identity attribute should be compared with which account attribute.

|  |  |  |
| --- | --- | --- |
| Identity Attribute | Operator | Account Attribute |
| Network ID | = | sAMAccountName |

#### Load Service Account

Existing Service Accounts will be imported to IdentityIQ using Batch Request.

A workgroup will be created for each service account with “WG-” as prefix followed by service account name. The owners of the service account will be added as members to the workgroup. This workgroup will be added as administrator to the Service Account Identity cube.

The following is a sample csv file to import the Workgroups for service account owners using HDS-WorkgroupImporter task:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| workgroup\_name | workgroup\_owner | workgroup\_description | workgroup\_email | workgroup\_members |
| WG-svc\_ACDHDBNP | tp019656 | Owner of Service Account: svc\_ACDHDBNP |  | tp019656 |
| WG-svc\_ACPHDBP | tp019656 | Owner of Service Account: svc\_ACPHDBP |  | tp019656 |
| WG-svc\_AD-ContractorExp | ae083298 | Owner of Service Account: svc\_AD-ContractorExp |  | ae083298 |
| WG-svc\_adext01 | ms024737 | Owner of Service Account: svc\_adext01 |  | ms024737 |

The following is a sample csv file to create service account identity cubes using Batch Request:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| operation | name | type | administrator | lob | lobnumber | networkid | inactive |
| CreateIdentity | Active Directory:svc\_ACDHDBNP | service | WG-svc\_ACDHDBNP | FM1US | 1010 | svc\_ACDHDBNP |  |
| CreateIdentity | Active Directory:svc\_ACPHDBP | service | WG-svc\_ACPHDBP | FM1US | 1010 | svc\_ACPHDBP |  |
| CreateIdentity | Active Directory:svc\_activecontrol | service |  | FM1US | 1010 | svc\_activecontrol | TRUE |
| CreateIdentity | Active Directory:svc\_AD-ContractorExp | service | WG-svc\_AD-ContractorExp | FM1US | 1010 | svc\_AD-ContractorExp |  |

## Service Account Provisioning Policies

Service Accounts have different attribute requirements from regular user accounts. The following details the provisioning policy requirements:

### AD Provisioning Policy

The following attributes will be provisioned during the creation of the service accounts, as per account type listed below:

##### Service Account

|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| sAMAccountName | “svc\_” + accountName from form (would be validated for uniqueness) |
| CN | sAMAccountName |
| distinguishedName | “CN=<sAMAccountName>, OU=<LOB Number>, OU=ServiceAccounts,DC=hds,DC=hdsupply,DC=com” |
| UserPrincipalName | <[sAMAccountName>@hdsupply.com](mailto:sAMAccountName@hdsupply.com) |
| Description | <Purpose of account>:Application Name-<Application Name>:Owners-<list of owners> |
| displayName | Display name value provided by user |
| extensionAttribute1 | LOB Number ie 1010 |
| manager | DistinguishedName of first owner in the list |
| userAccountControl | 66048 |

##### Non-Person Account

|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| sAMAccountName | “np\_” + accountName from form (would be validated for uniqueness) |
| CN | sAMAccountName |
| distinguishedName | “CN=<sAMAccountName>, OU=Exchange, OU=ServiceAccounts,DC=hds,DC=hdsupply,DC=com” |
| mail | <[sAMAccountName>@hdsupply.com](mailto:sAMAccountName@hdsupply.com) |
| UserPrincipalName | <[sAMAccountName>@hdsupply.com](mailto:sAMAccountName@hdsupply.com) |
| Description | <Purpose of account>:Application Name-<Application Name>:Owners-<list of owners> |
| displayName | Display name value provided by user |
| extensionAttribute1 | LOB Number ie 1010 |
| extensionAttribute10 | sync |
| manager | DistinguishedName of first owner in the list |
| userAccountControl | 66048 |

## Request Service Account

A custom quick link and workflow will be developed to allow users to request a Service/Non-Person account. The workflow will include a dynamic form and will build a plan to create a new identity cube for each service account. A workgroup will be created for each service account, all the service account owners will be added as members of the workgroup and this workgroup will be attached to the identity cube as Administrator. A lifecycle event HDS-ServiceAccountJoiner will be triggered on creation of identity cube for Service/Non-Person which will provision the service/non-person account on Active Directory application.

Request Service Account requires InfoSec approval.

### Process Flow

**Request Service Account**

A diagram of a company

Description automatically generated

### Quick Link

The quicklink, HDS-ServiceAccountManagement, will be built with the following options:

* **Display Name** – Request Service Account
* **Action** – workflow
* **Workflow Name** – HDS-ServiceAccountManagement
* **Visibility** – All users

### Form

The form, HDS-ServiceAccountManagement, will be developed with the following fields:

|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| Account Type | Radio Button with below value:   * Servcie Account * Non-Person Account |
| Prefix | “svc\_” if account type selected is Service Account  “np\_” if account type selected is Non-Person Account |
| SAM Account Name | Text Field. Validation to allow sAMAccountName length to be maximum 20 characters |
| Display Name | Text Field |
| Account Owners | Muti-valued. Identity drop down to select Active Employee Type Users |
| Description | Text Field |
| LOB | Text Drop down. Allowed value: FM1US |
| Application Name | Text Field. Help text: Name of the Application for which Service Account is requested |
| Mailed Enabled Account | Read Only Checkox. Enabled only when Non-Person account type is selected. Checked by default. |

### Workflow

Two workflows will be developed for creation of Service/Non-Person Accounts:

* 1. HDS-ServiceAccountManagement
  2. HDS-IdentityLifecycle-ServiceAccountJoiner

##### HDS-ServiceAccountManagement

This workflow will be executed when a user clicks on Request Service Account quicklink. It will have the following steps:

* **Build Form**
  + Get and set form variable to form, HDS-ServiceAccountManagement
  + Transition to Enter Form
* **Enter Form**
  + Display form, tied to an identityModel object that will contain the values entered on the form
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit (next), Back (back), Cancel Request (cancel)
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plan**
  + Dynamically build a provisioning plan using the identity model.
* **Provision**
  + Call HDS-LCM Create and Update WF. This will Initialize, Approve and Provision the plan.
* **Create Account Owner Workgroup**
  + Create a workgroup with name WG-<service account name>
  + Add selected owners as member of the workgroup.
  + Set the workgroup as administrator of service account identity.

**Send Email**

Send an email to IAM operations team for any provisioning error

##### HDS-IdentityLifecycle-ServiceAccountJoiner

This workflow will be executed as a Joiner event for Request Service Account. It will have the following steps:

* **Create Plan**
  + Build a provisioning plan using the attribute values on Service Account Identity cube.
* **Provision**
  + Call LCM Provisioning WF. This will Initialize and Provision the plan.
* **Generate Work Item for PAM**
  + Create an Approval Set for the Service Account.
  + Call HDS-GenerateWorkItemForPAM WF to generate a Work Item and assign it to CyberArk Administrator workgroup to vault the credentials.

**Send Email**

Send an email to IAM operations team for any provisioning error

## Modify Service Account

A custom quicklink “Modify Service Account” will be created to enable/disable the service account, and edit the attributes - **Display Name, Account Owners, Description and Application Name** for which Service Account is created. Service account owners can modify only the service accounts they own. It does not require any approval.

### Quick Link

The quicklink, HDS-ModifyServiceAccount, will be built with the following options:

* **Display Name** – Modify Service Account
* **Action** – workflow
* **Workflow name** – HDS-ModifyServiceAccount

### Form

The form, HDS-ModifyServiceAccount, will be developed with the following fields:

|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| Select Service Account | Identity drop down. Displays the list of Service Account Identities, owner by the requester |
| Select Operation | Text Drop down. Allowed Values:  Enable  Disable  Edit |
| SAM Account Name | Text Field. Read Only |
| Display Name | Text Field |
| Account Owners | Muti-valued. Identity drop down to select Active Employee Type Users |
| Description | Text Field |
| LOB | Text Drop down. Read Only |
| Application Name | Text Field. Help text: Name of the Application for which Service Account is requested |
| Business Justification | Text Area |
| Mailed Enabled Account | Read Only Checkox. Enabled only when Non-Person account type is selected. Checked by default. |

### Workflow

The workflow, HDS-ModifyServiceAccount, will be executed when a user clicks on Modify Service Account quicklink. It will have the following steps:

* **Build Form**
  + Get and set form variable to form, HDS-ModifyServiceAccount
  + Transition to Enter Form
* **Enter Form**
  + Display form, tied to an identityModel object that will contain the values entered on the form
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit (next), Back (back), Cancel Request (cancel)
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plan**
  + Dynamically build a provisioning plan using the identity model.
* **Provision**
  + Call HDS-LCM Create and Update WF. This will Initialize and Provision the plan.
* **Modify Workgroup**
  + This step will be executed, if there is a change in Service Account Owner.
  + Update members of the workgroup.
* **Generate Work Item for PAM**
  + This step will be executed, if there is a change in Service Account Owner.
  + Create an Approval Set for the modified Service Account.
  + Call HDS-GenerateWorkItemForPAM WF to generate a Work Item and assign it to CyberArk Administrator workgroup to update the service account owners.

**Send Email**

Send an email to IAM operations team for any provisioning error

## Request Service Access

A custom quicklink “Manage Service Accounts” will be created to request access to roles/entitlements for the Service Account. It uses IdentityIQ OOB feature of Request Access. Service account owners can request access for only the service accounts they own. It requires entitlement owner approval, if present.

The quicklink, HDS-RequestServiceAccess, will be built with the following options:

* **Display Name** – Request Service Access
* **Action** – requestAccess

# Privileged Account Management

Privileged Account Management refers to managing access to privileged or high-level accounts and critical or sensitive accounts and systems.

At HD Supply, we have two types of privileged account:

R-Account

K-Account

The Account Type link attribute will distinguish the account from regular accounts. The attribute value will be determined by the following logic:

The following breaks down the different privileged account types:

|  |  |
| --- | --- |
| Type | value |
| R-Account | privileged |
| K-Account | privileged |

**Since the privileged accounts are added directly to the users, the lifecycle of privileged accounts would follow the standard process of the user.**

## Privileged Account Provisioning Policies

Privileged Accounts have different attribute requirements from regular user accounts. The following details the provisioning policy requirements:

### AD Provisioning Policy

The following attributes will be provisioned during the creation of the secondary accounts, as per account type listed below:

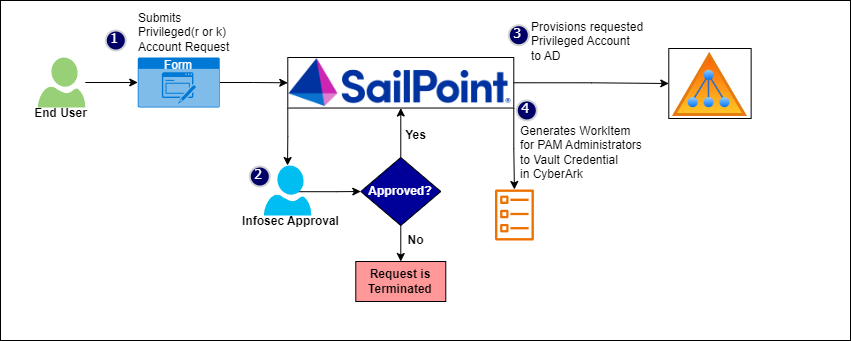
|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| sAMAccountName | For R-Account: <Network ID> + ‘r’  For K-Account: <Network ID> + ‘k’ |
| CN | <SAMAccountName> |
| distinguishedName | For R-Account: “CN=<sAMAccountName>, OU=Admins,DC=hdsdev,DC=hdsupply,DC=com”  For K-Account: “CN=<sAMAccountName>, OU=Adminskali,DC=hdsdev,DC=hdsupply,DC=com” |
| UserPrincipalName | <[sAMAccountName>@hdsupply.com](mailto:sAMAccountName@hdsupply.com) |
| Description | For R-Account: SOC Approved Admin Account  For K-Account: Kali Linux account for <FirstName> + “ " + <LastName> |
| displayName | For R-Account: Admin - <FirstName> + “ " + <LastName>  For K-Account: KaliLinux - <FirstName> + “ " + <LastName> |
| extensionAttribute1 | LOB Number ie 1010 |
| extensionAttribute9 | <SAMAccountName> |
| givenName | <FirstName> |
| sn | <LastName> |
| memberOf | GSC-CyberArkUsers-U0 |
| employeeID | <Employee ID> |

## Request Privileged Account

A custom quick link and workflow will be developed to allow users to request a new privileged account. The workflow will include a dynamic form and will build a plan to provision the privileged account on Active Directory application. It will generate a manual work item and assign to IAM Administrator workgroup to vault the privileged account in CyberArk.

### Process Flow

**Request Privileged Account**



### Quick Link

The quicklink, HDS-PrivilegedAccountManagement, will be built with the following options:

* **Display Name** – Request Service Account
* **Action** – workflow
* **Workflow Name** – HDS-PrivilegedAccountManagement
* **Visibility** – All users

### Form

The form, HDS-PrivilegedAccountManagement, will be developed with the following fields:

|  |  |
| --- | --- |
| Attribute | Value or Mapping |
| Account Type | Radio Button with below value:   * R-Account * K-Account |
| Select Identity | Identity Drop Down  For R-Account, All active Employee and Contractor  For K-Account, Identities with costcenterhierarchy = “Information Security” |
| SAM Account Name | Text Field, Read Only. Validation to allow sAMAccountName length to be maximum 20 characters |
| Display Name | Text Field, Read Only |
| Description | Text Field, Read Only |
| LOB | Text Field, Read Only |

### Workflow

The workflow, HDS-PrivilegedAccountManagement, will be executed when a user clicks on Request Privileged Account quicklink. It will have the following steps:

* **Build Form**
  + Get and set form variable to form, HDS-PrivilegedAccountManagement
  + Transition to Enter Form
* **Enter Form**
  + Display form, tied to an identityModel object that will contain the values entered on the form
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel
  + Provide buttons: Submit (next), Back (back), Cancel Request (cancel)
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plan**
  + Dynamically build a provisioning plan using the identity model.
* **Provision**
  + Call HDS-LCM Create and Update WF. This will Initialize, Approve and Provision the plan.
* **Generate Work Item for PAM**
  + Create an Approval Set for the Privileged Account.
  + Call HDS-GenerateWorkItemForPAM WF to generate a Work Item and assign it to CyberArk Administrator workgroup to vault the credentials.

**Send Email**

Send an email to IAM operations team for any provisioning error

# Group Management

Group Management includes loading and identifying existing groups, creation of new groups, managing group ownership, termination of owners, and deletion of groups.

## Create New Group

A custom quick link and workflow will be developed to allow users to create new group / distribution list. The quick link will use the OOTB Select Identities to search for owner identities. The workflow will include a dynamic form and will build a plan to create a group / distribution list on the target.

### Quick Link

The quick link will be built with the following options:

* **Action** – workflow
* **Workflow name** – HDS-Create Group
* **forceAllowSelf** – true
* **hideAllowOthers** – true
* **Visibility – All employees**

### Workflow Steps

The workflow will have the following steps:

* **Build Form**
  + Get and set form variable to form, HDS-Create Group
  + Transition to Enter Form
* **Enter Form**
  + Display form, tied to an identityModel object that will contain the values entered on the form
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit (next), Back (back), Cancel Request (cancel)
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plan**
  + Dynamically build a provisioning plan using the identity model.
  + A workgroup with name Workgroup\_<Group name> will be created and all the selected owner identities will be added to this workgroup.
* **Provision**
  + Call SP Provision Processor WF sub. This will Initialize, Approve (auto in this case), and Provision the plan
* **Close Request**
  + Update the links with any required group attributes
  + Append to the emailArgsList a map of:
    - To – Owner Identity’s email
    - Template – HDS-New Group Created
    - All other attributes in the target group request
* **Send Emails**
  + Call the SP Send Emails WF sub, passing in the emailArgsList

### Form

The form, HDS-Create Group, will be developed with the following fields:

* Group Name: text
* Description: text
* Display Name: text
* LOB: Combobox
* Type: Combobox, values: Group and Distribution List
* Mail : for DL and mail enabled security groups
* Owner: Multiselect of active employee identities
  + Filter out all inactive, all non-user accounts, and “Contractor” employee type
* Add/Remove members
  + Add/Remove – Primary accounts
  + Add/Remove – Admin-R accounts

## Change Group Owner

A custom quick link and workflow will be developed to allow the users to change the owner of groups. The quick link will use the OOTB Select Identities to search for owner identities. The workflow will include a dynamic form and will update the group’s owner on the target account.

### Quick Link

The quick link will be built with the following options:

* **Action** – workflow
* **Workflow name** – HDS-Change Secondary Account Owner
* **forceAllowOthers** – true
* **hideAllowSelf** – true
* **Visibility** – All employees

### Workflow Steps

The workflow will have the following steps:

* **Build Form**
  + Get and set variable to form, HDS-Change Group Owner
  + Transition to Enter Form
* **Enter Form**
  + Display form, that will return a list of the groups and the new owner identity
  + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit, Back, Cancel Request
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plans**
  + For each identity in the group list, dynamically build a provisioning
  + Add each plan to a list
  + Transition to Launch Requests
* **Launch Requests**
  + Loop the plans in the list
  + For each, launch the workflow, Process Group Owner Update WF, passing in the plan and identityName.
* **Provision**
  + Call SP Provision Processor WF sub. This will Initialize, Approve (auto in this case), and Provision the plan
* **Close Request**
  + Update the links with any required group attributes
  + Append to the emailArgsList a map of:
    - To – New and Old Owner Identity’s email
    - Template – HDS-Group Owner Changed
    - List all groups that were updated
* **Send Emails**
  + Call the SP Send Emails WF sub, passing in the emailArgsList

### Process Group Owner Update Workflow

The workflow will receive a plan and identityName. It will be a wrapper workflow to simply call the SP Provision Processor Sub.

### Form

The form, HDS- Change Group Owner, will be developed with the following fields:

* **Current Accounts** – Multi-select of all owned accounts
* **Current Owner Identity** – Read Only, showing current owner
* **New Owner Identity** – Identity drop down
  + Filter out all inactive, all non-user accounts, and “Contractor” employee type

# Security/Legal Hold

In some cases when employee/contractor leaves organization, HDS would like to identify and preserve relevant data for any anticipated litigation. Legal Hold gives HDS an advantage in preparing for a hold, responding to a regulatory agency, or negotiating with opposing counsel with Legal Hold.

A legal hold process would be built in SailPoint IIQ to flag users as legal hold and preserve their data.

A custom quick link and workflow will be developed to allow users to set an identity to Security Hold. The workflow will include a dynamic form and will build a plan to set the account to security hold.

### Quick Link

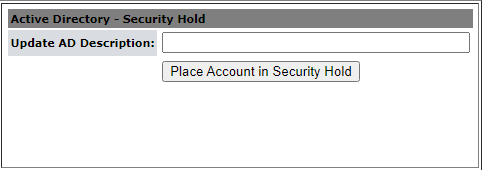
The quick link will be built with the following options:

* **Action** – workflow
* **Workflow name** – HDS-Security Hold
* **forceAllowSelf** – false
* **allowSelf** – true
* **Visibility** – Manager

### Workflow Steps

The workflow will have the following steps:

* **Build Form**
  + Get and set variable to form, HDS-Security Hold
  + Transition to Enter Form
* **Enter Form**
  + Display form, that will return a list of the identity. Select the identity to be moved to Security Hold



* + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit, Back, Cancel Request
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plans**
  + For the identity selected in the form, dynamically build a provisioning plan account request:
    - Target account – Disable the primary account, move active directory account to OU=”SecurityHold,OU=Users,DC=hds,DC=hdsupply,DC=com”, set Description value from the form
    - Retain only O365 access, email, share drives and teams group membership
  + Transition to Launch Requests
* **Launch Requests**
  + Launch the workflow, Process Secondary Account Owner WF, passing in the plan and identityName.
* **Close Request**
  + Update the links with any required account attributes

### Form

#### HDS-Security Hold

The form, HDS-Security Hold, will be developed with the following fields:

* **Select Identity –** Identity drop down
* **Security Hold** – Checkbox
* **Description** – Text, prefix with “INVESTIGATION – “

# Out of Office

In some cases, associates go on paid/unpaid leave and managers need the ability to set out of office notification on their mailbox.

An Out of Office process would be built in SailPoint IIQ to allow managers to select their subordinates and set out of office notifications on their mailbox.

A custom quick link and workflow will be developed to allow managers to set up Out of Office for their subordinate’s mailbox. The workflow will include a dynamic form and will build a plan to set the Out of Office for account.

### Quick Link

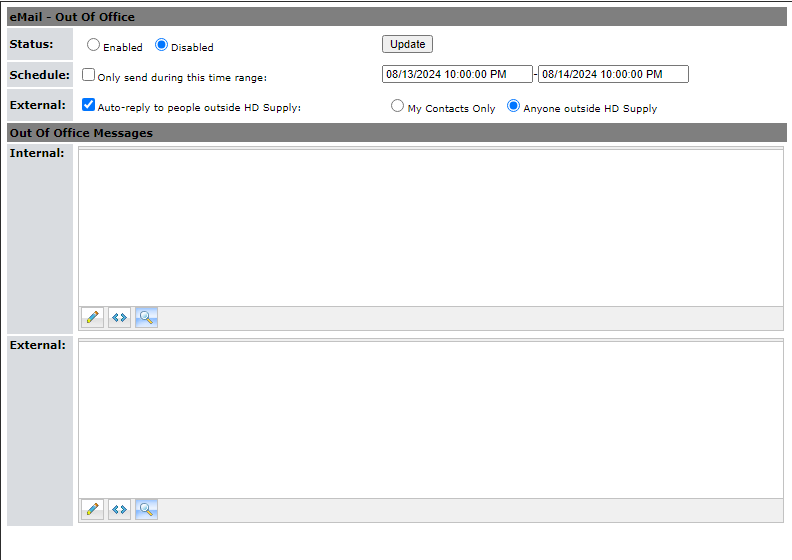
The quick link will be built with the following options:

* **Action** – workflow
* **Workflow name** – HDS-Out of Office
* **forceAllowSelf** – false
* **allowSelf** – true
* **Visibility** – Manager, System Administrator, Helpdesk

### Workflow Steps

The workflow will have the following steps:

* **Build Form**
  + Get and set variable to form, HDS-Out of Office
  + Transition to Enter Form
* **Enter Form**
  + Display form, that will return a list of the identity. Select the identity to setup out of office message and capture details as shown below:



* + Transition to Confirm if Approved
  + Transition to end if Rejected
* **Confirm**
  + Display a confirmation form, dynamically showing all values in the identityModel (make more static if the display doesn’t work out)
  + Provide buttons: Submit, Back, Cancel Request
  + Transition to Build Plan on Approved (next), Enter Form on Rejected (back) and end on Cancel Request (cancel). Note: the workflow must be transient for cancel to work.
* **Build Plans**
  + Dynamically build a provisioning plan using the identity model.
* **Launch Requests**
  + Launch workflow. This will Initialize, Approve (auto in this case), and Provision the plan
* **Close Request**
  + Update the links with any required account attributes

### Form

#### HDS-Out of Office

The form, HDS-Out of Office, will be developed with the following fields:

* **Select Identity –** Identity drop down
* **Description** – Text, prefix with “Out of Office”
* **Out of Office** – Checkbox
* **Scheduled** – Checkbox
* **StartTime** – Date Range
* **EndTime** – Date Range
* **InternalMessage** – Textarea
* **ExternalMessage** – Textarea

# Roles

IdentityIQ's Role functionality is used to model a company's structure and business operations. Roles are designed to be highly flexible and customizable, allowing them to be used to model a wide array of business structures and functions.

By default, there are four (4) types of Roles configured in IdentityIQ:

* **Organizational:** organize and manage the role hierarchy
* **Business:** identify job functions or titles
* **IT:** encapsulate sets of system Entitlements
* **Entitlement:** represent individual system Entitlements

At HD Supply, IdentityIQ’s Role functionality can be used to deliver Birthright access such that users, when they first join the organization, are automatically provisioned the access they need to perform their designated job function.

Tying this function back to the role types configured in IdentityIQ, there would be one or more “Business” roles assigned to an identity in IdentityIQ, each with one or more required “IT” roles that contain the entitlements required to be provisioned based on the users who are assigned the “Business” role.

## IT\_Role

The IT roles being deployed for the current phase, including their associated entitlements, are captured in the “IT role” sheet in the attached excel file.

[IT Role Mapping](https://hdsupplyinc.sharepoint.com/:x:/r/teams/fm-infosec-iam/Shared%20Documents/General/Sailpoint%20IIQ%20Implementation/02%20Design/HD%20Supply%20Roles%20Mapping.xlsx?d=wec81429136de4142b69e3b306d63d588&csf=1&web=1&e=iI5rDe)

NOTE: As of this initial draft, the following details are examples only and will need to be reviewed prior to Go-Live.

## Business Role

The business roles being deployed for the current phase, including their associated IT roles, are captured in the “Business Role” sheet attached excel file.

[Business Role Mapping](https://hdsupplyinc.sharepoint.com/:x:/r/teams/fm-infosec-iam/Shared%20Documents/General/Sailpoint%20IIQ%20Implementation/02%20Design/HD%20Supply%20Roles%20Mapping.xlsx?d=wec81429136de4142b69e3b306d63d588&csf=1&web=1&e=iI5rDe)

NOTE: As of this initial draft, the following details are examples only and will need to be reviewed prior to Go-Live.

# Role Importer

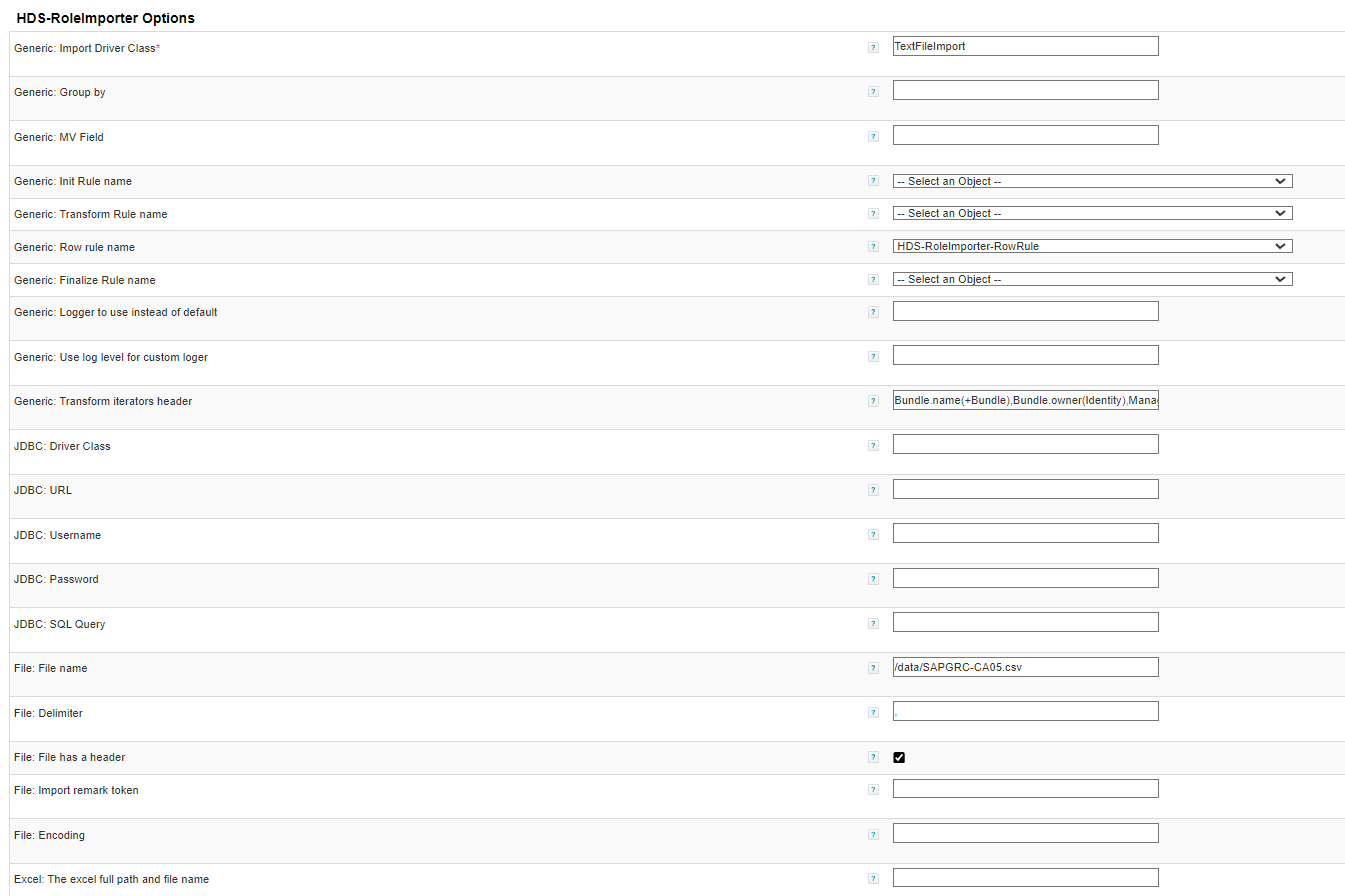
Role Importer is a customized Generic Importer utility which allows for the rapid development of miscellaneous data imports into IdentityIQ. With role importer you can import data from different sources such as a delimited text file, excel spreadsheet or a JDBC database. The primary advantage of using a role importer is that we don’t need to write iterators, just use a Rule to process a row of data at a time. In IdentityIQ, we have defined a rule “HDS-RoleImporter-RowRule”, that will read and process a row of data at a time, handling multiple operations.

Below is the Role importer task defined:

**Task Name** – HDS-RoleImporter

**Source** – File (.csv)

**Row Rule** – HDS-RoleImporter-RowRule



In project HD Supply, we are using role importer to import roles from a csv file to avoid creation of each and every role through manual intervention. Below are the operations that we can perform using the role importer:

**Create** – to create roles

**Update** – to update roles

**Delete** – to delete roles

**AddEntitlement** – to add entitlements to the role

**RemoveEntitlement** – to remove entitlements from the role

**AddMatchlist** – to define role assignment criteria based on identity attributes

**RemoveMatchlist** – to remove certain criteria for role assignment

**AddFilter** – to define role assignment criteria based on a pre-defined population

**RemoveFilter** – to remove the population criteria defined for role assignment.

You can access the file here - [hds-roleimporter.csv](https://hdsupplyinc.sharepoint.com/:x:/r/teams/fm-infosec-iam/Shared%20Documents/General/Sailpoint%20IIQ%20Implementation/01%20Discovery/hds-roleimporter.csv?d=w2ac0cc4b42264165a8624b79e2bc6f6e&csf=1&web=1&e=79bdu3)

User Guide for Generic Importer – [Generic Importer](https://community.sailpoint.com/t5/Services-Standard-Deployment/SSD-Generic-Importer-User-Guide/ta-p/78253)

# Migration

## Contractor Migration

In this process we are migrating the contractor records from AD Plus to SailPoint using a csv file. Existing contractor records present in the ADP database need to be imported into SailPointIIQ. Below is the SQL query to fetch the contractor records from ADP database:

**SQL Query:**

SELECT 'CreateIdentity' as operation

,ISNULL([SAMAccount],'') as name

,ISNULL(lower([UserType]),'') as type

,ISNULL([LOB],'') as lobnumber

,case when LOB = '1010' then 'FM1US' when LOB ='1000' then 'GC1US' when LOB='1040' then 'HIS' else ISNULL(lob,'') end as lob

,ISNULL([FirstName],'') as firstname

,ISNULL([MiddleName],'') as middleinitial

,ISNULL([LastName],'') as lastname

,ISNULL([PreferedName],'') as preferredname

,ISNULL([LOC],'') as location

,ISNULL([Address1],'') as address

,ISNULL([Address2],'') as address2

,ISNULL([City],'') as city

,ISNULL([State],'') as state

,ISNULL([Zip],'') as zipcode

,ISNULL([Phone],'') as workphone

,ISNULL([Mobile],'') as mobilephone

,ISNULL([SAMAccount],'') as employeeid

,ISNULL([JobTitle],'') as title

,ISNULL([Email],'') as email

,ISNULL(substring(ManagerDN,4, CHARINDEX(',', ManagerDN)-4),'') as manager

,ISNULL([ContractorCompany],'') as contractorcompany

,ISNULL([ContractorEmail],'') as contractorcompanyemail

,ISNULL(try\_parse(whencreated as date),'') as hiredate

,ISNULL(try\_parse(expirationDate as date),'') as terminationdate

,case when try\_parse(expirationDate as date) is not null and datediff(day, GETDATE(),try\_parse(expirationDate as date)) >0 then 'Joiner' else 'Leaver Disable'end as lifecycleaction

,case when LicenseOverride is not null then LicenseOverride else ISNULL(LicenseAssigned,'') end as licenseassigned

,ISNULL([SAMAccount],'') as networkid

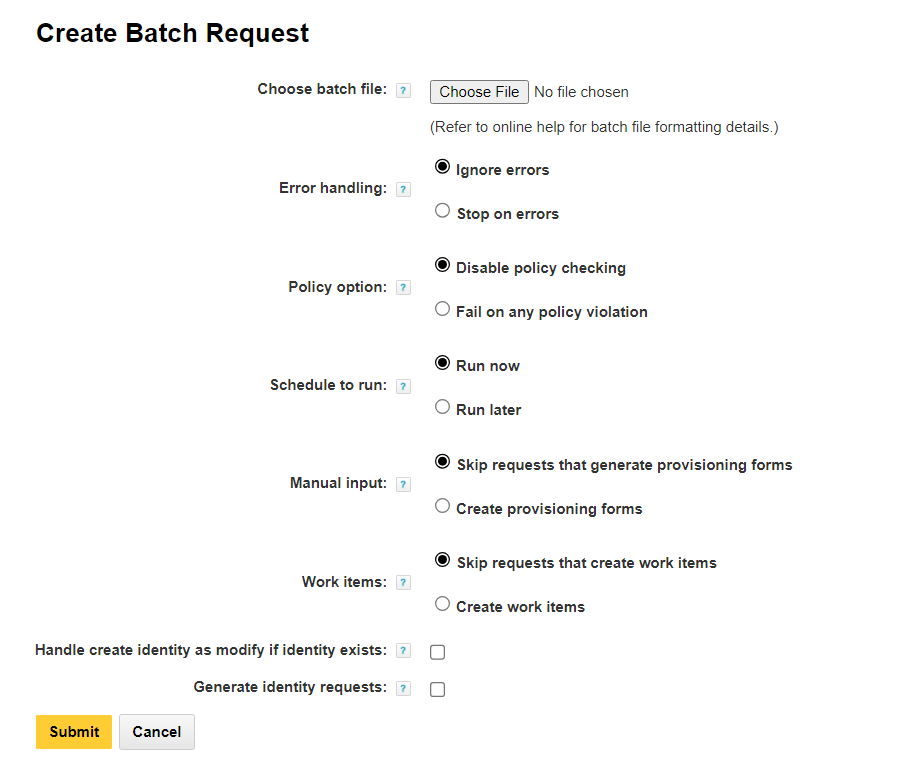
FROM [ADP].[dbo].[tbl\_All\_Users]

where UserType='Contractor'

and expirationDate is not null

The above query returns the contractor records that we can export into a csv file. Here, is the sample file [SampleContractor](https://hdsupplyinc.sharepoint.com/:x:/r/teams/fm-infosec-iam/Shared%20Documents/General/Sailpoint%20IIQ%20Implementation/01%20Discovery/SampleContractor.csv?d=w3e45e42a6fdd450ba89b234446571c86&csf=1&web=1&e=am8JaD)

SailPoint IdentityIQ provides a feature to import and process bulk data into IIQ, known as batch requests. This feature can only be accessed by users with system administrator capability, therefore login as a user having system administrator privileges. Click on Setup Menu >> Batch Requests >> Add New Batch Request >> below page is to be displayed, upload the file to be processed and validate options as below then Submit.



**Note:**

Ensure that the checkbox is disabled for option “Handle create identity as modify if identity exists”.

## Service Account Migration

In Service Account Migration we are migrating the Service account records from Active Directory to SailPoint using a csv file. Service Account migration process can be defined in two steps, where

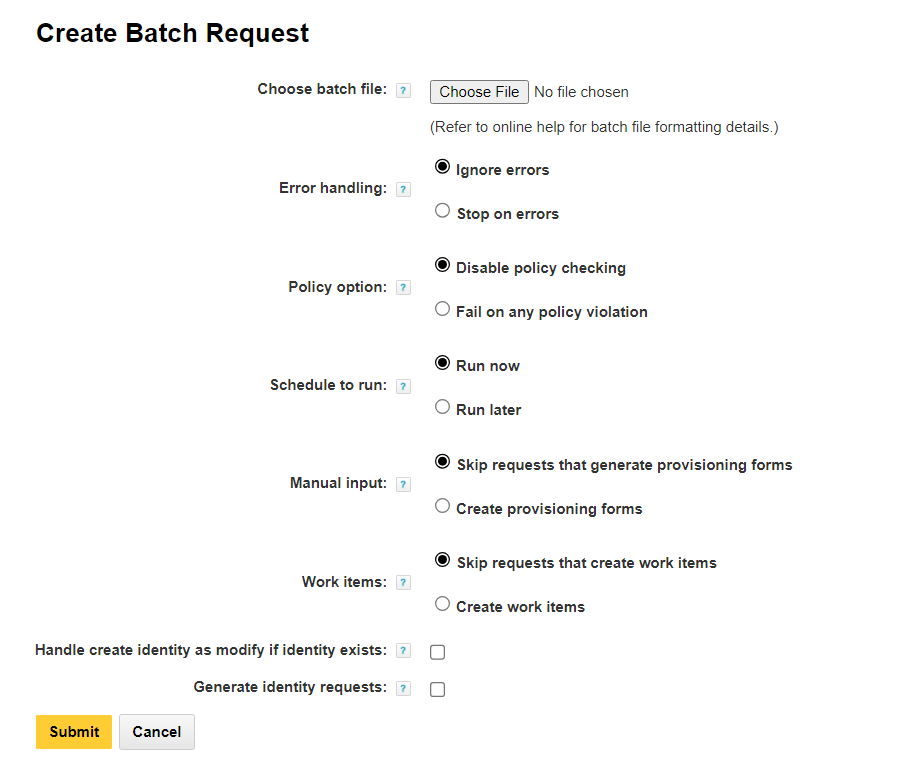
Step 1: Create workgroup for Service Account Owner

Here, is the sample file for Service Accounts – [ServiceAccountsSample.csv](https://hdsupplyinc.sharepoint.com/:x:/r/teams/fm-infosec-iam/Shared%20Documents/General/Sailpoint%20IIQ%20Implementation/01%20Discovery/ServiceAccountSample.csv?d=w3d347bb9a8a84c5e921ac7c467ba5ed1&csf=1&web=1&e=jphQ3R)

Step 2: Create Service Account identity

We can have some service account records present in a csv file that we need to import into SailPointIIQ for creating and managing the service accounts in a more efficient and convenient way.

SailPoint IdentityIQ provides a feature to import and process bulk data into IIQ, known as batch requests. This feature can only be accessed by users with system administrator capability, therefore login as a user having system administrator privileges. Click on Setup Menu >> Batch Requests >> Add New Batch Request >> below page is to be displayed, upload the file to be processed and validate options as below then Submit.



# Reports

Reports provide an at-a-glance view of the data in IdentityIQ, which helps the organization manage system access and the compliance process. IdentityIQ includes a standard set of core reports in template form. Individual users and organizations can customize and save instances of these templates and run these reports on a scheduled or ad-hoc basis. Additionally, custom reports can be created to meet the needs of each customer. IdentityIQ includes a reporting architecture that simplifies the process of creating custom reports. Basic reports can be created quickly through an XML specification. A variety of hooks are available for introducing more complex logic where it is needed to produce the desired report output. The standard report templates that are part of the product are modeled with this same XML specification structure and can serve as helpful examples of how custom reports should be structured.

To access the Reports page, from the Navigation menu bar, go to Intelligence > Reports.

IdentityIQ includes a number of standard reports for monitoring and managing compliance and provisioning activities. These reports can be run with or without filter criteria. For example, the Uncorrelated Accounts Report can run with no filters and return the list of uncorrelated accounts for all applications in the system, or you can set filters on the report, to restrict the results to a subset of applications.

The unfiltered, standard version of each report is listed on, and can be run from, the Report page's Reports tab. If you add filters to the standard report, that report configuration is saved as a customized report on the My Reports tab.

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs.The provided reports are displayed on the Reports tab. The following types of report templates are provided:

* **Detailed Reports** – include key data about specific areas in IdentityIQ. The information can be presented in table or grid format. The results can be exported to a .csv file and used in spreadsheets.
* **Archived Reports** – include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file
* **Summary Report** – include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs. Use scope to control access to your report results.

All reports use a set of standard properties for basic information such as naming and descriptions, and for setting controls, such as scoping and requiring sign-off. The Report Layout configuration procedure is the same for all reports.

The reports are divided in to the following categories:

* Access Review and Certification Reports
* Activity Reports: User Activity Detailed Report
* Administration Reports
* Application Status Report
* Configured Resource Reports
* Identity and User Reports
* Lifecycle Manager Reports
* Policy Violation Report
* Risk Reports
* Role Management Reports

## Custom Reports

<TBD>

# Request Access

Request Access includes Role and Entitlement requests. If you are working with a single user, a third tab, Current Access displays that you can use to request the removal of Roles or Entitlements. Use the Lifecycle Manager Request Roles feature to generate requests that:

* Add the appropriate role to the specified identities.
* Provision the entitlements the role requires.
* Provision permitted roles, if added to the request when prompted.
* Deprovision by removing roles from an identity

This option generates a provisioning request to remove the role assignment from the identities and the entitlements the role requires if another role does not need the entitlements.

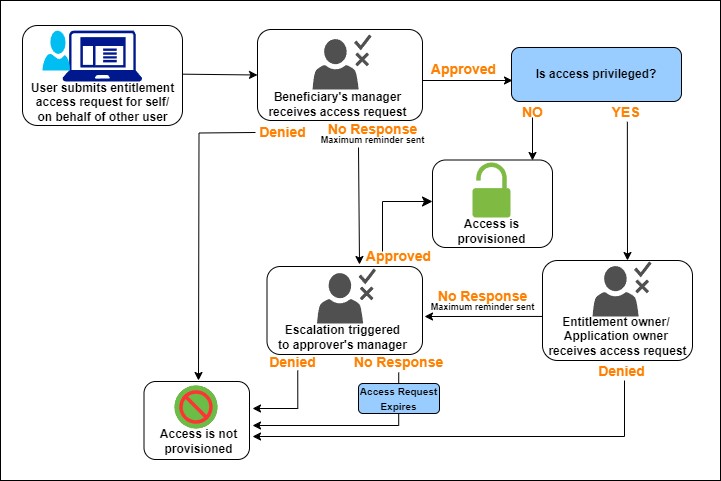
Use the Lifecycle Manager Request Entitlements feature to generate requests to:

* Add the entitlement to the specified identity.
* Revoke an identity's current entitlements.

This option generates a provisioning request that removes the access from the source application or applications.

By default, when you request a new entitlement on an application and the user already has an account on that application, the entitlement is added to the existing account.

Request Access will follow below approval flow at HD Supply:



# Certifications and Access Reviews

In IdentityIQ, certifications let you automate the review and approval of identity access privileges. In a certification, IdentityIQ collects fine-grained access or entitlement data, and formats the information into interactive reports, which are sent to the appropriate reviewers as access reviews. You can also use certifications to validate things like roles and account groups.

Certifications typically consist of multiple access reviews. For example, when you schedule a Manager Certification, a type of certification that asks managers to review and validate their direct reports' access, it will consist of an individual access review for each of the managers you choose to include as part of the campaign. However, it is possible to configure a certification such that it includes only one access review – for example, you might schedule a Manager Certification for just one specific manager, which means that there would only be one access review making up that certification.

When you configure the certification, you can set it up to annotate each access review with descriptive language that highlights changes, flags anomalies, and highlights where policy violations appear. The access reviews enable reviewers to:

* Approve access for identities
* Approve account group permissions and membership
* Approve role composition and membership
* Take corrective actions, such as revoking entitlements that violate policy
* Forward, reassign, or delegate all or part of the access review to another reviewer

For all corrective actions, IdentityIQ can fulfill certification revocations through automated or manual means, depending on the individual applications' connector configurations. IdentityIQ can also be configured to integrate with ticketing systems or other provisioning systems to fulfill provisioning requests.

Below certifications will be configured for HD Supply

**Manager Certifications** – Certify that a manager's direct reports have the right entitlements they need to do their job, and no more than that. You can configure a Manager Certification to include all managers in the company, or only specific managers. You can also configure which applications you want to certify as part of the Manager Certification.

**Entitlement Owner Certifications** – Certify that all identities that have access to entitlements for which the reviewer is responsible are correct.

# Task Configuration

## Aggregations

### Account Aggregation

Account Aggregation is the process through which account data from a configured application is read into IdentityIQ and stored in Link (account) objects connected to Identities. Aggregation is an integral part of every IdentityIQ installation. The aggregation process is driven by an IdentityIQ task—specifically an account aggregation task—which can read data from one or more applications. The options specified for the aggregation task determine which of the available actions are performed in the aggregation.

An account aggregation task is responsible for:

* Reading the account data from the designated data source (e.g., a delimited file, a database table, the native application’s data structure, etc.)
* Creating a Link object to represent the account or updating an existing Link object with any data changes for the account
* Associating the accounts (Links) to an existing Identity in the system or creating new Identities to hold the accounts

There are a number of additional options that an aggregation task can be configured to perform, such as:

* Correlating Identities to their appropriate manager Identity based on data values in the feed
* Deleting any Links for accounts that no longer exist
* Recalculating active scopes for the installation when scoping is enabled
* Executing some of the identity refresh task options

IdentityIQ aggregates data from one application at a time, repeating this process for each application specified in the aggregation task (in the “applications” attribute). This diagram shows the actions executed for each application named in the aggregation task definition:

Diagram

Description automatically generated

At HD Supply, IdentityIQ will need to consume account information (via Account Aggregation) for each application mentioned in the “Application Configuration” section above. For details on scheduling of these aggregation tasks, please see the “Scheduling” section below.

### Group Aggregation

The group aggregation process is used to create managedAttributes representing an application’s group objects. It is far simpler than account aggregation. As with account aggregation, slight variations in the logic occur based on whether the application is a logical application, a multiplexed application, or a normal application. Also like account aggregation, the task’s specific processing is determined by the arguments specified for the task.

Group aggregation can only be done for applications which have a group schema defined and a group attribute defined for the account schema. IdentityIQ aggregates group data from one application at a time, repeating this process for each application specified in the aggregation task (in the “applications” attribute). This diagram shows the actions executed for each application named in the group aggregation task definition:

Diagram

Description automatically generated

At HD Supply, IdentityIQ will need to consume group information (via Group Aggregation) for Active Directory (to support group requests via ServiceNow Service Catalog, birthright roles, future access certifications, etc.), ServiceNow (to support the ServiceNow Integration modules), and EPIC. For details on scheduling of these group aggregation tasks, please see the “Task Scheduling” section below.

### Identity Refresh

The Identity Refresh task of IdentityIQ is a critical component of any IdentityIQ installation. Identity Refresh tasks are used to update Identity attribute details, synchronize attributes to downstream systems, evaluate workflow triggers, and evaluate policies, as well as over a dozen other operations for the system. Configuring a set of Identity Refresh tasks for an installation is an important technical task that requires understanding of all of the options available and the specific functions and performance impacts they have.

At HD Supply, the Identity refresh task will primarily be used to ensure that identity data is accurately kept up to date based on data feeds from upstream and downstream systems, trigger lifecycle events, and evaluate role assignment criteria.

## Aggregation Tasks

### HDS-Workday-AccountAggregation-FullSync

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-Workday-AccountAggregation-FullSync |
| Description | Aggregate Accounts from Workday Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Workday |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | No |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts |  |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | No |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-Workday-AccountAggregation-DeltaSync

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-Workday-AccountAggregation-DeltaSync |
| Description | Aggregate Account deltas from Workday Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | No |
| Application to Scan | No |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | Yes |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts | No |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | Yes |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-Active Directory-AccountAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-Active Directory-AccountAggregation |
| Description | Aggregate Accounts from Active Directory Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Active Directory |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | No |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts |  |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | No |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-Active Directory-AccountGroupAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-Active Directory-AccountGroupAggregation |
| Description | Aggregate Groups from Active Directory Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Active Directory |
| Filter object types to scan | No |
| Enable Delta Aggregation | No |
| Detect deleted account groups | Yes |
| Automatically promote descriptions to this locale | No |
| Description attribute (default "description") | No |
| Group Aggregation Refresh Rule | No |
| Promote Classifications | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |

### HDS-Microsoft Entra ID-AccountAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS- Microsoft Entra ID-AccountAggregation |
| Description | Aggregate Accounts from Microsoft Entra ID Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Microsoft Entra ID |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | No |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts |  |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | No |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-Microsoft Entra ID-AccountGroupAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS- Microsoft Entra ID-AccountGroupAggregation |
| Description | Aggregate Groups from Microsoft Entra ID Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Microsoft Entra ID |
| Filter object types to scan | No |
| Enable Delta Aggregation | No |
| Detect deleted account groups | Yes |
| Automatically promote descriptions to this locale | No |
| Description attribute (default "description") | No |
| Group Aggregation Refresh Rule | No |
| Promote Classifications | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |

### HDS-Salesforce-AccountAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS- Salesforce-AccountAggregation |
| Description | Aggregate Accounts from Salesforce Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Salesforce |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | No |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts |  |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | No |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-Salesforce-AccountGroupAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS- Microsoft Entra ID-AccountGroupAggregation |
| Description | Aggregate Groups from Salesforce Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | Salesforce |
| Filter object types to scan | No |
| Enable Delta Aggregation | No |
| Detect deleted account groups | Yes |
| Automatically promote descriptions to this locale | No |
| Description attribute (default "description") | No |
| Group Aggregation Refresh Rule | No |
| Promote Classifications | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |

### HDS-SAP GRC-AccountAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-SAP GRC-AccountAggregation |
| Description | Aggregate Accounts from SAP GRC Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | SAP GRC |
| Refresh Assigned and Detected Roles | No |
| Check Active Policies | No |
| Only create links if they can be correlated to an existing identity. | No |
| Refresh Identity Risk Scorecards | No |
| Maintain Identity Histories | No |
| Enable Delta Aggregation | No |
| Detect Deleted Accounts | Yes |
| Maximum deleted accounts |  |
| Refresh Assigned Scope | No |
| Disable Auto Creation of Scopes | No |
| Disable Optimization of unchanged accounts | No |
| Promote managed attributes | No |
| Disable auto creation of applications | No |
| Disable marking the identity as needing a refresh | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |
| Sequential Execution - Terminate on error | No |
| Actions to include in the task result | Deselect all option |

### HDS-SAP GRC-AccountGroupAggregation

|  |  |
| --- | --- |
| Task Option | Value |
| Task Name | HDS-SAP GRC-AccountGroupAggregation |
| Description | Aggregate Groups from SAP GRC Application. |
| Allow Concurrency | No |
| Require Sign-Off | No |
| Host | NA |
| Application to Scan | SAP GRC |
| Filter object types to scan | No |
| Enable Delta Aggregation | No |
| Detect deleted account groups | Yes |
| Automatically promote descriptions to this locale | No |
| Description attribute (default "description") | No |
| Group Aggregation Refresh Rule | No |
| Promote Classifications | No |
| Enable Partitioning | No |
| Terminate when maximum number of errors is exceeded | No |

## Task Scheduling

|  |  |
| --- | --- |
| Task Name | Schedule |
| HDS-Workday-AccountAggregation-FullSync | <TBD> |
| HDS-Workday-AccountAggregation-DeltaSync | Every 15 minutes |
| HDS-Active Directory-AccountAggregation | <TBD> |
| HDS-Active Directory-AccountGroupAggregation | <TBD> |
| HDS-Active Directory Privileged-AccountAggregation | <TBD> |
| HDS-Active Directory-AccountGroupAggregation | <TBD> |
| HDS- Microsoft Entra ID-AccountAggregation | <TBD> |
| HDS- Microsoft Entra ID-AccountGroupAggregation | <TBD> |
| HDS- Salesforce-AccountAggregation | <TBD> |
| HDS- Microsoft Entra ID-AccountGroupAggregation | <TBD> |
| HDS- SAP GRC-AccountAggregation | <TBD> |
| HDS- SAP GRC-AccountGroupAggregation | <TBD> |
| HDS-RemoveAccessAfter30Days | <TBD> |
| HDS-DeleteAccountAfter90Days | <TBD> |

NOTE: The above schedules will be subject to change as performance considerations are evaluated throughout the development and testing phases.

# Appendix

This section covers any miscellaneous information relating to the topics discussed above.

## Identity Attribute Matrix

The Microsoft Excel spreadsheet attached includes the mapping from the source system through IdentityIQ and to downstream systems, as well as any associated transformation logic required along the way.

[HD Supply Identity Attributes.xlsx](https://hdsupplyinc.sharepoint.com/teams/fm-infosec-iam/_layouts/15/Doc.aspx?sourcedoc=%7BCE11DB47-1DC2-4528-8166-82CFF73C440B%7D&file=HD%20Supply%20IdentityMappings_v1.xlsx&action=default&mobileredirect=true&DefaultItemOpen=1)

## References

* IdentityIQ Deployment Architectures

[Recommended IdentityIQ Deployment Architectures - Compass (sailpoint.com)](https://community.sailpoint.com/t5/Technical-White-Papers/Recommended-IdentityIQ-Deployment-Architectures/ta-p/74263)

* IQService Installation and Configuration

[IQService - Compass (sailpoint.com)](https://community.sailpoint.com/t5/Other-Documents/IQService/ta-p/158011)

* Workday – Required Permissions

[Required Permissions (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/workday/help/integrating_workday/administrator_permission.html)

* Active Directory – Required Permissions

[Required Permissions (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/active_directory/help/integrating_active_directory/required_permissions.html)

* Microsoft Entra ID – Required Permissions

[Required Permissions (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/microsoft/entra_id/help/integrating_entra_id/administrator_permission.html)

* Microsoft Entra ID – Last Login for Accounts feature

[Last Login for Accounts (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/microsoft/entra_id/help/integrating_entra_id/last_login_for_accounts.html)

* Microsoft Entra ID – Multi-Factor Authentication (MFA) Management feature

[Multi-Factor Authentication (MFA) Management (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/microsoft/entra_id/help/integrating_entra_id/mfa_management.html)

* Salesforce – Required Permissions

[Required Permissions (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/salesforce/help/integrating_salesforce/required_permission.html)

* SAP GRC – Required Permissions

[Required Permissions (sailpoint.com)](https://documentation.sailpoint.com/connectors/identityiq/sap/grc/help/integrating_sap_grc/required_permissions.html)

* Reports

[Reports (sailpoint.com)](https://documentation.sailpoint.com/identityiq/help/reports/reports.html)

* Certifications and Access Reviews

[Certifications and Access Reviews (sailpoint.com)](https://documentation.sailpoint.com/identityiq/help/certification/certification_and_access_reviews.html)

* Request Access

[Requesting Access (sailpoint.com)](https://documentation.sailpoint.com/identityiq/help/lcm/requestaccess.html)

* Lifecycle Events

[Lifecycle Events (sailpoint.com)](https://documentation.sailpoint.com/identityiq/help/lcm/define_lifecycle_events.html)

## Audit Configuration

The table below captures a list of audit actions, along with their associated descriptions, that captures the out-of-the-box options for auditing in IdentityIQ.

| Audit Category | Auditable Action | Description | Enabled? |
| --- | --- | --- | --- |
| General System Actions | Login | Creates an audit table entry for every successful IdentityIQ login, recording the username | yes |
| General System Actions | Logout | Creates an audit table entry for every successful IdentityIQ logout, recording the username | yes |
| General System Actions | Login Failure | Creates an audit table record for every failed login attempt, recording the username | yes |
| General System Actions | Session Timeout | Creates an audit table entry for every IdentityIQ logout caused by the session timing out, recording the username | yes |
| General System Actions | Import File | Records name of every file imported through the UI import option: **gear** icon > **Global Settings** (or in 6.4 and prior **System Setup)** > **Import from File,** or the console | yes |
| General System Actions | Run Task | Generates an audit record for each task run, recording the task name and the name of the user who launched it (Scheduler if it was a scheduled task) | yes |
| General System Actions | Email Sent | Creates an audit record for each email sent by the system, recording the recipient email address and message subject. This audit entry does not indicate successful delivery or valid email address; it just means the email was successfully launched by IdentityIQ. | yes |
| General System Actions | Email Failure | Creates an audit record any time email sending fails due to an IdentityIQ configuration problem or server connection error; failure reasons could include: incorrect email setup, failure to connect to the SMTP server, no email address configured, etc.; records the intended recipient email address, subject, and the error message | yes |
| General System Actions | Delegate Certification Item | Creates an audit record when a certification item is delegated to another user, recording the delegator, new owner, the name of the delegated item, and the delegation comments | yes |
| General System Actions | Delegation Completion | Records completion of delegation work items; shows the Identity completing the item and the work item number | yes |
| General System Actions | Delegation Revocation | Captures when a delegation work item is revoked by the delegator, returning the certification items to the original certification; records the revoker’s name, the former delegate, the work item number, and information about what was in the delegated (identity name, role name, etc.) as well as the certificationEntity and workItem IDs | yes |
| General System Actions | Reassign Certification | Records an audit log entry when one or more certification entities are reassigned to another certifier; shows the original certifier, the new certifier, and the reassignment comments, as well as the original certification and reassignment certification IDs | yes |
| General System Actions | Rescind Certification | Logs an entry when a certification reassignment is recalled by the original certifier; includes name of parent certification, owner name, and the name of the certifier from whom the reassignment was recalled, and IDs for the recalled and parent certification | no |
| General System Actions | Remediate Certification Item | Creates an audit entry when a policy violation is corrected or a certification item is remediated, resulting in a remediation action; the remediation requestor and target identity are both shown, as are the owner of the remediation and the type of remediation action (Provisioning Request or WorkItem); for policy violation remediations, the policy and rule violated are also shown | no |
| General System Actions | Certification Signoff | Generates an audit record when a certification is signed off, recording the certification name and the certifier; if a certification includes a signoff approver rule, only the last person to sign off generates this audit event; any others in the chain generate certification signoff approval events (see below) | yes |
| General System Actions | Certification Signoff Approval | Creates an audit record when a certification is signed off and a configured signoff approver rule routes the certification to another approver; records the certification name, the name of the person signing off, and the name of the user to whom the certification was sent for approval | no |
| Workflow and Work Item Auditing | Escalate Work Item | Logs the old owner name and new owner name when a work item escalation occurs | no |
| Workflow and Work Item Auditing | Expire Work Item | Logs an audit record when a workItem reaches notification timeout and can no longer be escalated | no |
| Workflow and Work Item Auditing | Approve Work Item | Deprecated in favor of Update Role / Disable Role set of audit events; will be removed from AuditConfig in a future release | no |
| Workflow and Work Item Auditing | Reject Work Item | Deprecated in favor of Update Role / Disable Role set of audit events; will be removed from AuditConfig in a future release | no |
| Workflow and Work Item Auditing | Start Workflow Process | Creates an audit entry every time a workflow is launched; the name of the launched workflow is recorded | yes |
| Workflow and Work Item Auditing | Update Role | Triggered by the Role Modeler – Owner Approval workflow; creates an audit event when a role modification undergoes approval (whether approved or rejected – shows “success” if approved, “failure” if rejected) | yes |
| Workflow and Work Item Auditing | Disable Role | Triggered by the Role Modeler – Owner Approval workflow; creates an audit event when a disabled role undergoes approval (whether approved or rejected) | yes |
| Workflow and Work Item Auditing | WorkItem Forwarded | Records an audit event when a user forwards a workItem to another user; includes the original owner, the new owner, the workItem number and ID, and any forwarding comments | no |
| Workflow and Work Item Auditing | Assign Work Item | Deprecated audit event; will be removed from the AuditConfig in a future release | no |
| Workflow and Work Item Auditing | Assign Remediation Item | Deprecated audit event; will be removed from the AuditConfig in a future release | no |
| Perform Maintenance Task Statistics Logging | Prune Histories | Logs deletion of history snapshots | no |
| Perform Maintenance Task Statistics Logging | Prune Task Results | Logs deletion of task results | no |
| Perform Maintenance Task Statistics Logging | Prune Requests | Logs deletion of request queue items | no |
| Perform Maintenance Task Statistics Logging | Prune Syslog Events | Logs deletion of events recorded in the syslog table | no |
| Perform Maintenance Task Statistics Logging | Prune Certifications | Logs deletion of certifications | no |
| Perform Maintenance Task Statistics Logging | Archive Certifications | Logs archiving of certifications (when archiving is enabled) | no |
| Perform Maintenance Task Statistics Logging | Prune Certification Archives | Logs deletion of certification archives | no |
| Perform Maintenance Task Statistics Logging | Finish Certifications | Logs count of certifications progressed to the “finished” state | no |
| Perform Maintenance Task Statistics Logging | Scan Remediations | Logs the number of certifications scanned for remediations to determine whether the requested remediation activities have been completed | no |
| Perform Maintenance Task Statistics Logging | Forward Inactive [User] Work Items | Logs the number of workItems found assigned to inactive users and forwarded to another user (using the inactive user workItem escalation rule) | no |
| Perform Maintenance Task Statistics Logging | Denormalize Scopes | Logs the number of scopes that were denormalized to correct scope paths recorded on other system objects. Objects record the full path to their assigned scopes but if the scope hierarchy changes, these paths become “dirty” and must be denormalized to regain optimal performance. | no |
| Perform Maintenance Task Statistics Logging | Certifications Phased | Logs the number of certifications moved to the next appropriate phase | no |
| Perform Maintenance Task Statistics Logging | Certification Items Phased | Logs the number of certification items (in continuous certifications) that were moved to their next appropriate phase; Certification items in continuous certifications phase individually rather than as a whole certification | no |
| Perform Maintenance Task Statistics Logging | Continuous Certifications Processed | Logs the number of continuous certifications found and processed | no |
| Perform Maintenance Task Statistics Logging | Continuous Certification Items Required | Logs the number of continuous certification items moved to a Certification Required state | no |
| Perform Maintenance Task Statistics Logging | Continuous Certification Items Overdue | Logs of the number of continuous certification items moved to a Certification Overdue state | no |
| Perform Maintenance Task Statistics Logging | Prune Provisioning Transactions | Logs deletion of provisioning transactions (these are visible on the Administrator Console page under the gear menu) | no |
| Provisioning-Related Audits | Provision | Creates an audit event for any provisioning result (entitlement adds, removals, account updates, etc.); indicates the requester, the user to whom the provisioning action applies, and the status (or the error message if it fails) | yes |
| Provisioning-Related Audits | Provisioning Expansion | Creates an audit entry when a provisioning plan gets expanded into component parts that each must be provisioned separately; for example, when a role gets connected to an Identity, it may require creation of an account and then addition of entitlements on that account, each of which would be a separate provisioning action and would therefore get its own separate audit entry; includes details about the specific provisioning action. | yes |
| Identity Event Audits | Identity Manually Correlated | Not currently used in logging audit events; manual correlation of accounts to identities creates an event for Link manually moved from one identity to another (see next item) | yes |
| Identity Event Audits | Link manually moved from one identity to another | Creates an audit record when an uncorrelated account gets manually correlated or when an account is moved from one Identity to another with the **Move Account** option on an Identity Cube’s Application Accounts page | yes |
| Identity Event Audits | Identity Event | When an Identity Lifecycle Event occurs this will trigger an Audit entry Example Create a new Identity via LCM | yes |
| Identity Event Audits | Role sunrise | Creates an audit record when a role is auto-activated on a sunrise (activation) date specified for the role; only applicable when role sunrise/sunset activation is configured | no |
| Identity Event Audits | Role sunset | Creates an audit record when a role is auto-deactivated on a sunset (deactivation) date specified for the role; only applicable when role sunrise/sunset activation is configured | no |
| Policy Violation Audits | Allow Exception on Violation | Records an audit event when a policy violation exception is allowed in a certification or through the **My Work** (or in version 6.4 and prior, **Manage) > Policy Violations** page; shows the user who allowed it, the user for whom it was allowed, the violated rule, the exception expiration date, and the comments entered for the exception | no |
| Policy Violation Audits | Correct Violation | Audits when a policy violation is corrected (e.g. by removing conflicting access); records the names of the user making the correction and the user who was in violation, the violated policy and rule names, and the remediation actions taken | no |
| Policy Violation Audits | Delegate Violation | Creates an audit record when a user delegates responsibility for addressing a policy violation to another user | no |
| Plugin Audits | Plugin Installed | Creates an audit event when a user installs a Plugin; records the Plugin name (Target) and the user who installed the Plugin (Source) | yes |
| Plugin Audits | Plugin Upgraded | Creates an audit event when a user upgrades a Plugin | yes |
| Plugin Audits | Plugin Uninstalled | Creates an audit event when a user uninstalls a Plugin; records the Plugin name (Target) and the user who uninstalled the Plugin (Source) | yes |
| Plugin Audits | Plugin Enabled | Creates an audit event when a user enables a Plugin; records the Plugin name (Target) and the user who enabled the Plugin (Source) | yes |
| Plugin Audits | Plugin Disabled | Creates an audit event when a user disables a Plugin; records the Plugin name (Target) and the user who disabled the Plugin (Source) | yes |
| Plugin Audits | Plugin Configuration Changed | Creates an audit event when a user changes the configuration for a Plugin; records the Plugin name (Target), the user who changed the Plugin (Source), and the attributes' new values | yes |
| Alerts | Alert Processed | Creates an audit event when an alert record is evaluated against the IdentityIQ alert definitions. Only applicable when IdentityIQ is aggregating alerts from another system (e.g. SecurityIQ) | no |
| Alerts | Alert Action Created | Creates an audit event when IdentityIQ has triggered a certification, email, or workflow in response to alert processing | no |
| LCM Event Actions | Approve Line Item | Generates an audit entry when a user approves a pending access request item; records the requester, the approver, and several pieces of information about the access requested (account name, username, requested access, etc.) | yes |
| LCM Event Actions | Accounts Request Started | Creates an audit entry when an account-related request is entered through LCM; the entry shows the requester, the user for whom the request was made, the application name, and (except for create requests) the account name | yes |
| LCM Event Actions | Comment Added | Creates an audit entry showing all work item comments recorded on a work item as it is processed; does not apply to certification work items, only LCM request work items; generates one comment audit entry containing all comments from the work item when the work item is completed | no |
| LCM Event Actions | Create | Creates an audit event when a Create Identity action occurs through LCM; records all attributes provided on creation | yes |
| LCM Event Actions | Delete | Adds an audit entry when an account is deleted through an LCM request; records the requesting user, the application, and the account name (native identity) | yes |
| LCM Event Actions | Disable | Logs an audit event when an account is disabled through LCM, recording the requesting user, the application, and the account (native identity) | yes |
| LCM Event Actions | Enable | Creates an audit record when an account is enabled through LCM | yes |
| LCM Event Actions | Entitlement Added | Creates an audit record when an Entitlement is added through an LCM request; records the requester, the affected Identity, the application, and the attribute name/value that make up the requested entitlement | yes |
| LCM Event Actions | Entitlement Removed | Logs an audit record when an Entitlement is removed through an LCM request; includes the requester, application, account name, and attribute name/value of access to remove | yes |
| LCM Event Actions | Entitlements Request Started | Does not currently create AuditEvents automatically; LCM workflow could be modified to add auditEvents for this action if desired | yes |
| LCM Event Actions | Expired Password Start | Creates an audit event when a pass-through authentication login password has expired (on the native system) and is changed through IdentityIQ. NOTE: Expired password resets of internally stored IdentityIQ passwords do not generate this audit event. | yes |
| LCM Event Actions | Forgot Password Start | Creates an audit entry to record a password reset through the Forgot Password feature (only available with pass-through authentication); records the identity name and the account name on the pass-through-authentication system | yes |
| LCM Event Actions | Identity Create Request Started | Creates an audit entry when a user submits a Create Identity request through LCM; logs identity name, workflow used to process the request, where the request came from, and the operation (Create) | yes |
| LCM Event Actions | Identity Edit Request Started | Creates an audit entry when a user submits a Create Identity request through LCM; logs identity name, workflow used to process the request, where the request came from, and the operation (Create) | yes |
| LCM Event Actions | Manual Provisioning | Logs an audit entry when a request through LCM requires a manual workItem to complete the provisioning activity; records the performer, operation (e.g. add, remove), application, account name on which action is performed, attribute name/value of access removed/added, and the requester | yes |
| LCM Event Actions | Modify | Creates an audit record when an Identity is edited through the LCM Edit Identity option. Records the user making the change, the affected IdentityIQ account (Identity name), and the new and previous attribute value in the change. | yes |
| LCM Event Actions | Password Request Start | Logs an audit entry when a password change request is initiated through LCM | yes |
| LCM Event Actions | Password Changed | Creates an audit entry when the password for a managed application is changed through IdentityIQ; this includes password changes on the pass-through authentication application through the Forgot Password feature as well as LCM requests to change password | yes |
| LCM Event Actions | Password Change Failure | Creates an audit entry when a user attempts to change a password for a managed application through IdentityIQ, but the password update fails. Records the error details. | yes |
| LCM Event Actions | Forgot Password Changed | Audit events for this action are currently only generated as Forgot Password Start events (see *above*). | yes |
| LCM Event Actions | Expired Password Changed | Audit events for this action are currently only generated as Expired Password Start events (see *above*). | yes |
| LCM Event Actions | Provisioning Complete | Creates an audit entry when a provisioning request is set to Complete by the Perform Identity Request Maintenance task; reports the provisioning requester, the identity to which the request pertains, the application and account, the attribute/value for the entitlement, and the operation (e.g. add/remove) | yes |
| LCM Event Actions | Provisioning Failure | Logs an audit record when a provisioning request ends in failure | yes |
| LCM Event Actions | Registration Started | Creates an audit event when a user who does not have an IdentityIQ account requests a new IdentityIQ account through the self-service registration process | yes |
| LCM Event Actions | Reject Line Item | Generates an audit entry when a user rejects a pending access request item (role or entitlement); records the requester, the approver, and several pieces of information about the access requested (account name, username, requested access, etc.) | yes |
| LCM Event Actions | Role Added | Creates an audit event when a role is added through an LCM request; records the requester, the affected Identity, and the role added | yes |
| LCM Event Actions | Role Removed | Creates an audit event when a role is removed as a result of an LCM request; records the requester, the affected Identity, and the role removed | yes |
| LCM Event Actions | Roles Request Started | Does not currently create AuditEvents automatically; LCM workflow could be modified to add AuditEvents for this action if desired | yes |
| LCM Event Actions | Unlock | Creates an audit event when a locked application account is unlocked through LCM | yes |
| LCM Event Actions | Access Request Started | Records an audit event when an LCM Access Request is created, showing the application, account, attribute name, and attribute value in the request | yes |
| Authentication-related Audits | Identity Locked | Records the username in an audit entry when a user’s IdentityIQ account gets temporarily locked, either because they entered an incorrect password too many times or because they entered incorrect challenge question answers too many times | yes |
| Authentication-related Audits | Identity Unlocked | Records the username in an audit entry when a user's locked IdentityIQ account gets unlocked | yes |
| Authentication-related Audits | Authentication Answer Incorrect | Creates an audit event showing the username when a user attempts to authenticate through challenge questions (Forgot Password functionality) and fails to answer the required number of questions correctly | yes |
| Miscellaneous | Password Policy Changed | Creates an audit event when an application's password policy has changed; records the source (who created the new password policy), the application, the password policy name (attribute value), and the policy attributes (minimum number of characters, maximum number of letters, etc.) | yes |
| Miscellaneous | Server Up/Down | Creates an audit event when an application server shuts down or starts up (Target = either "Server Up" or "Server Down") | yes |
| Miscellaneous | API Configuration Changed | Creates an audit event when an OAuth client configuration (for SCIM API authentication) is created or edited; records the Source, application, and attributes, along with the type of change that occurred | yes |
| Miscellaneous | Emergency Termination launched | Emergency Termination | yes |
| Miscellaneous | hds\_HSPasswordResetEvent | Password reset | yes |
| Miscellaneous | Entitlement Management Modify | Entitlement Management - Modify | yes |
| Miscellaneous | Entitlement Management Create | Entitlement Management - Create | yes |
| Miscellaneous | Shared Mailbox Account Creation | Shared Mailbox Account - Create | yes |
| Miscellaneous | hds-Joiner | Joiner Event | yes |
| Miscellaneous | hds-RLOA | Return From Leave of Absence event | yes |
| Miscellaneous | hds-Leaver | Leaver event | yes |
| Miscellaneous | hds-Leaver-Delete | Leaver – Delete event | yes |
| Miscellaneous | hds-Mover | Mover event | yes |
| Miscellaneous | Batch Request | Batch Request | yes |
| Miscellaneous | Privileged Account Creation | Privileged Account - Create | yes |
| Miscellaneous | Privileged Account Creation Failure | Privileged Account – Create Failed | yes |