Marathon Petroleum Corporation Requirement Document

**Prepared by:**

**Simeio Solutions**

Table of Contents

[2 Document Revision History: 4](#_Toc17816792)

[3 Required Approvals: 4](#_Toc17816793)

[4 Project Overview: 5](#_Toc17816794)

[5 Stakeholders: 5](#_Toc17816795)

[6 Products and Tools: 5](#_Toc17816796)

[7 Key Decisions: 6](#_Toc17816797)

[8 Assumptions: 6](#_Toc17816798)

[9 Password Policy: 7](#_Toc17816799)

[10 Non-Functional Requirements: 8](#_Toc17816800)

[10.1 Development Servers & Specifications: 8](#_Toc17816801)

[10.2 Test Servers & Specifications: 8](#_Toc17816802)

[10.3 Production Servers & Specifications: 8](#_Toc17816803)

[11 Functional Requirements: 9](#_Toc17816804)

[12 Holding Table Reference: 11](#_Toc17816805)

[12.1 User Types: 12](#_Toc17816806)

[12.2 Mandatory Attributes: 13](#_Toc17816807)

[13 User Processes: 13](#_Toc17816808)

[13.1 User Creation: Employee (Incremental Recon Job): 13](#_Toc17816809)

[13.2 User Creation: Employee (Non-Incremental Recon Job for All Users): 14](#_Toc17816810)

[13.3 User Creation: Non-Employee: 14](#_Toc17816811)

[13.4 User Update: Employee (Incremental/Non-Incremental Recon Job): 15](#_Toc17816812)

[13.5 User Update: Non-Employee: 15](#_Toc17816813)

[13.6 User Enable/Disable: Employee (Incremental/Non-Incremental Recon Job): 16](#_Toc17816814)

[13.7 User Enable/Disable: Non-Employee 16](#_Toc17816815)

[13.8 User Termination: Employee: 17](#_Toc17816816)

[13.9 Password Reset: 17](#_Toc17816817)

[13.10 Certification of Non-Employee Identity: 18](#_Toc17816818)

[13.11 Emergency Termination: 18](#_Toc17816819)

[13.12 Provisioning of Service Accounts: 19](#_Toc17816820)

[14 Organization Processes: 20](#_Toc17816821)

[14.1 Organization Creation/Update: 20](#_Toc17816822)

[15 UDF Value Loader: 20](#_Toc17816823)

[15.1 Create/Update Lookups: 20](#_Toc17816824)

[16 Active Directory: 21](#_Toc17816825)

[16.1 AD User Account Provisioning: 21](#_Toc17816826)

[16.2 AD User Account De-Provisioning: 21](#_Toc17816827)

[16.3 AD User Account Termination: 22](#_Toc17816828)

[16.4 AD Data Sync to IAM: 22](#_Toc17816830)

[16.5 AD Password Reset: 22](#_Toc17816831)

[17 IAMGoldTables: 23](#_Toc17816832)

[17.1 User Creation/Update/Delete in “user\_id”: 23](#_Toc17816833)

[17.2 Organization Creation/Update/Delete in “org\_id”: 23](#_Toc17816834)

[18 Polaris: 23](#_Toc17816835)

[18.1 Provisioning User Accounts in Polaris DB: 23](#_Toc17816836)

[18.2 De-Provisioning User Accounts in Polaris DB: 24](#_Toc17816837)

[18.3 Polaris Password Reset: 25](#_Toc17816838)

[18.4 Access Requests for Polaris DB: 25](#_Toc17816839)

[19 SAP: 26](#_Toc17816840)

[19.1 Provisioning User Accounts in SAP: 26](#_Toc17816841)

[19.2 SAP Role Request and SOD Check: 26](#_Toc17816842)

[19.3 De-Provisioning User Accounts in SAP: 27](#_Toc17816843)

[19.4 Password Synchronization to SAP: 28](#_Toc17816844)

[19.5 Provisioning Non-Employee Accounts in SAP: 28](#_Toc17816845)

[20 Targeted AD Attribute Sync (TADA): 29](#_Toc17816846)

[20.1 TADA Provisioning: 29](#_Toc17816847)

[21 Other: 30](#_Toc17816848)

[21.1 Delegation of User’s IAM Permissions: 30](#_Toc17816849)

[21.2 Organization Admin Permission for Supervisors: 30](#_Toc17816850)

# Document Revision History:

| **Version** | **Version Date** | **Summary of Changes** | **Author** |
| --- | --- | --- | --- |
| 0.1 | 07-08-2019 | Initial Draft | Simeio Solutions |
| 0.6 | 16-08-2019 | Reviewed by team | Simeio Solutions |
| 1.0 | 22-08-2019 | Final review by Amit and Tonnie | Simeio Solutions |
| 1.1 | 27-08-2019 | Minor updates and review by Wes and Linda | MPC |
| 1.2 | 30-08-2019 | Accepted all updates. ready for Signoff | Simeio Solutions |

# Required Approvals:

|  |  |  |
| --- | --- | --- |
| Name of Person | Date | Approval |
| Wes Vollmar | 8/30/2019 | Wes Vollmar |
| Robert Calmus | 9/4/2019 | Robert Calmus |
| Dennis Longdon | 9/6/2019 | Dennis Longdon |
|  |  |  |

# Project Overview:

Saviynt is a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise resources. Saviynt is designed to manage user access privileges across all of a firm's resources, throughout the entire identity management lifecycle -- from initial creation of access privileges to dynamically adapting to changes in business requirements.

As a next phase to IAM implementation, MPC is in process of designing user provisioning as a birthright access to users. User will be auto-provisioned to a set of roles and accounts based on applicable group of attributes (policies) when a new user is on-boarded. Account and entitlement assignments may change as users’ identity attributes change in the enterprise as a result of promotions, transfers, or other organizational changes. Saviynt automatically provisions these changes in the target systems based on roles/policies.

Current Applications which is in scope for this implementation are:

* SAP HR
* Active Directory
* TADA
* 6 SAP Applications
* Polaris DB
* IAMGold DB

When a user’s employment is terminated, Saviynt ensures that all their accounts are disabled or de-provisioned, according to the enterprise policies configured in IAM. Automatic assignment and provisioning of accounts and entitlements increases employee productivity by eliminating long manual cycles typically required to provision accounts manually. Similarly, automatic de-provisioning of accounts and entitlements ensures compliance to key regulatory requirements by ensuring that terminated employees are not able to access key corporate applications after termination.

# Stakeholders:

|  |  |
| --- | --- |
| **Name** | **Title** |
| **Robert Calmus** | IAM Supervisor |
| **Dennis Longdon** | IAM Cybersecurity Architect |
| **Wesley Vollmar** | IAM Cybersecurity Architect |

# Products and Tools:

MPC has purchased Saviynt IGA to build the IAM solution. Currently, MPC is utilizing IAM 11gR2PS3.

# Key Decisions:

* Current requirements were chosen to be gathered through demonstration/review with the IAM Admin team via reverse engineering the current IAM configuration.
* Simeio will vet all use cases gathered from IAM and design the similar solution in the Saviynt platform. Current use cases might not be implemented in the same way in new Saviynt platform.
* As Saviynt doesn’t support a lot of customization within the tool, Simeio will highlight steps and functionality to be built in Saviynt in our Design Documents.
* The MPC “PIC” will continue to be the primary user login attribute from the **PicsAvailable** table going forward.
* The new implementation will provision the same systems and access that the current IAM system provisions.
* Workflows for request approvals will be implemented in the new platform to match the current IAM design.
* Saviynt will be the request portal for SAP role requests and provisioning/de-provisioning.
* A portal for non-employee account creation/management will be available, defined further in the Design Document.
* Existing users, accounts, and roles will be imported into the new platform as a data migration task from IAM, so that new accounts are not provisioned for existing users at the migration.
* Password synchronization will be configured for the connected user accounts on the new platform.
* Quarterly non-Employee identity certifications will continue to be processed in the Saviynt governance module.

# Assumptions:

Several key business assumptions were considered during reverse engineering of technical components of this phase:

* MPC HRIS is responsible for ensuring accuracy and completeness of the information in the HRIS system.
* An employee belongs to only one HR legal entity under a given employee number as its primary identifier.
* MPC Network Team is responsible for providing the network connectivity and target system high availability.

# Password Policy:

This is the configured IAM password policy:

|  |  |
| --- | --- |
| **Policy Item** | **Configured Value** |
| Minimum Length | 9 |
| Warn After(days) | 113 |
| Disallow past Passwords | 24 |
| Expires After(days) | 120 |
| Minimum Numeric Characters | 1 |
| Maximum Alphabet Characters | 2 |
| Minimum Upper Case Characters | 1 |
| Minimum Lower Case Characters | 1 |
| Maximum Incorrect Login attempts counter | 10 |
| Lock Duration | 30 |
| Disallow First Name | Yes |
| Disallow Last Name | Yes |
| Disallow user ID | Yes |

# Non-Functional Requirements:

* Data replication / reconciliation should handle potential issues between the data nodes in odd cases of up/down.
* TLS 1.2 for all data communication.
* Saviynt or Simeio standard SDLC and security procedures on all custom code.
* OVA-based image will be shared by team with Saviynt version 5.3.1 and CentOS 7.0 installed and pre-configured.
* Database used is Maria DB which is similar to MySQL and has capability to support Galera clustering.
* DBs per environment will be configured as master/slave, supporting synchronous replication.
* Saviynt servers can be configured as UI app server for user traffic and UI jobs server for task jobs.
* Multi-site active/passive architecture for all layers.

## Development Servers & Specifications:

* 2x Web Server: 2x Xenon vCPU, 16GB RAM
* 2x App Server – Saviynt Security Manager: 2x Xenon vCPU, 8GB RAM
* 2x Identity Audit & WF DB – MySQL: 2x Xenon vCPU, 8GB RAM

## Test Servers & Specifications:

* 4x Web Server: 4x Xenon vCPU, 32GB RAM
* 4x App Server – Saviynt Security Manager: 4x Xenon vCPU, 16GB RAM
* 2x Identity Audit & WF DB – MySQL: 4x Xenon vCPU, 16GB RAM

## Production Servers & Specifications:

* 4x Web Server: 4x Xenon vCPU, 32GB RAM
* 4x App Server – Saviynt Security Manager: 4x Xenon vCPU, 16GB RAM
* 2x Identity Audit & WF DB – MySQL: 4x Xenon vCPU, 16GB RAM

**Note:** Physical and virtual servers both ok, Dedicated DB servers for Galera Cluster: Any modern HD will provide sufficient local storage, preferable SSD storage for DB; 1-10 GB of data storage depending on the archive frequency and transaction rates.

# Functional Requirements:

This section describes the functional requirements for Saviynt Security Manager (SSM) implementation at MPC.

**User Processes:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 13.1 | Creating employee from incremental recon job |
| FR: 13.2 | Creating employee from non-incremental recon job for all users |
| FR: 13.3 | Creating non-employee users |
| FR: 13.4 | Updating employees using incremental/non-incremental recon job |
| FR: 13.5 | Updating non-employee |
| FR: 13.6 | Enabling or disabling of employee using incremental or non-incremental recon job |
| FR: 13.7 | Enabling or disabling of non-employee |
| FR: 13.8 | Terminating the employee |
| FR: 13.9 | Resetting of password |
| FR: 13.10 | Certification of non-employee identity |
| FR: 13.11 | Emergency termination |
| FR: 13.12 | Provisioning of service accounts |

**Organization Processes:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 14.1 | Creating or updating the organization record |

**UDF Value Loader:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 15.1 | Create/update lookups |

**Active Directory:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 16.1 | Provisoning user accounts in Active Directory |
| FR: 16.2 | De-provisoning user accounts in Active Directory |
| FR: 16.3 | Terminating/Deleting user accounts in Active Directory |
| FR: 16.4 | Data synchronization of relevant changes in AD to IAM |
| FR: 16.5 | Change a user password in Active Directory |

**IAMGoldTables:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 17.1 | User creation or update in IAMGoldTables.dbo.user\_id |
| FR: 17.2 | Organization creation or update in IAMGoldTables.dbo.org\_id |

**Polaris:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 18.1 | Provisoning users in Polaris DB |
| FR: 18.2 | De-provisoning users in Polaris DB |
| FR: 18.3 | Change a user password in Polaris DB |
| FR: 18.4 | Access request for Polaris DB |

**SAP:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 19.1 | Provisioning employee user accounts in SAP |
| FR: 19.2 | Assignment of SAP access |
| FR: 19.3 | De-provisioning of user accounts in SAP |
| FR: 19.4 | Change a user password in SAP |
| FR: 19.5 | Provisioning non-employee user accounts in SAP |

**Targeted AD Attribute Sync (TADA):**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 20.1 | Custom data sync and provisioning with TADA |

**Other:**

| **FR#** | **Requirements** |
| --- | --- |
| FR: 21.1 | Delegation of user’s IAM permissions |
| FR: 21.2 | Org Admin permissions for supervisors |

# Holding Table Reference:

In Marathon we are using below staging/holding tables to provide/store employee data to IAM, as well as define some important lookups/mappings for various systematic processes.

|  |  |
| --- | --- |
| **Table Name** | **Description** |
| HOLD\_EMPL\_CURRENT | This table holds user/employee information for current active employees (Note: Archive table also exists for historical documentation of table contents) |
| HOLD\_EMPL\_HIRE | This table holds user/employee information for employees to start within 21 days (Note: Archive table also exists for historical documentation of table contents) |
| VW\_DBAT\_SAP\_TRUSTED\_RECON | View that combines the current and future employees into a single view for selection for the employee feed. Some filtering is done in this view |
| VW\_DBAT\_SAP\_TRUSTED\_RECON\_INCREMENTAL | View that combines the current and future employees into a single view for selection for the employee feed. Filtering occurs on this view to limit down to just updated users within a configurable number of days |
| PicsAvailable | This table contains assigned and available PICs for assignment |
| HOLD\_ORG\_CURRENT | Table that contains all current organizations from SAP (Note: Archive table also exists for historical documentation of table contents) |
| HOLD\_PSEUDO\_ORG\_CURRENT | Table that contains manually maintained organizations that do not exist in SAP |
| VW\_ORG\_CURRENT | View that combines the SAP and pseudo orgs for selection for the org feed |
| Location | This table contains Office code for the selectable list of locations, as well as mapping into OU and assignment to home drive location |
| Shares | This table holds the mapping for OUs to home drive location and share folder assignment |
| Partner | This table contains Partner code for the selectable list of external partners |
| JobCategory | This table contains Job category for the selectable list of jobs a contractor is performing |
| Risks | This table holds risks and risk owners for communication of daily risks that have occurred through approved role assignments |
| Risks\_Notifications | This table holds a log of the risk notification sent to risk owners, as auditable documentation that the notification occurred |
| ManualProvisioning | This table holds roles, contacts, and instructions for manual role assignment activities, triggered by completed role assignments for the day |
| Config | Table for configuration values that are commonly queried and used within our DBAT views or custom processes |

## User Types:

MPC has defined these current user types for IAM-managed identities.

|  |  |
| --- | --- |
| **Code** | **Decode** |
| B - Batch ID | B - Batch ID |
| Contractor | Contractor |
| D1-Function Outsourced Indefinitely | Function Outsourced Indefinitely |
| D2-G - Group/Shared | G - Group/Shared |
| D3-Individual Independent Contractor – Self Employed | Individual Independent Contractor – Self Employed |
| D4-Leased Workers | Leased Workers |
| D5-Outsourced Project - Billed on Hourly Basis | Outsourced Project - Billed on Hourly Basis |
| D7-Speedway store account | Speedway store account |
| EMP | Employee |
| OTHER | ZZZ-Other |
| D6-Outsourced Project - Billed on Project Basis | Outsourced Project - Billed on Project Basis |
| Test Non-Employee ID | ZZZ-Test Non-Employee ID |
| RPA Account | RPA Account |
| Andeavor Contractor | Andeavor Contractor |

## Mandatory Attributes:

The below fields are the mandatory attributes that MPC uses for all user types within IAM.

|  |  |
| --- | --- |
| **User Types** | **Mandatory Attributes** |
| B - Batch ID | First Name |
| Contractor | Last Name |
| Function Outsourced Indefinitely | Organization |
| G - Group/Shared | User Type |
| Individual Independent Contractor – Self Employed | Last4 Digits of SSN/International ID |
| Leased Workers | Birthdate (MMDD) |
| Outsourced Project - Billed on Hourly Basis | Office Location |
| Speedway store account | MUID (generated by IAM at creation) |
| Employee |  |
| ZZZ-Other |  |
| Outsourced Project - Billed on Project Basis |  |
| ZZZ-Test Non-Employee ID |  |
| RPA Account |  |
| Andeavor Contractor |  |

# User Processes:

Two jobs are required for loading the employee data

* Incremental is periodic scheduler job, which runs every 2 hours
* Full is an unscheduled job, runs weekly (manually), usually on Friday

## User Creation: Employee (Incremental Recon Job):

|  |  |
| --- | --- |
| **UC FR: 13.1:** | **Creating employee from incremental recon job** |
| **Actor(s):** | * DB Connector (Employee only) * DBATSAPTrustedRecon Incremental User Reconciliation Scheduler |
| **Description:** | This case covers the addition and change of multiple records within the Identity Management system |
| **Narrative:** | 1. User record will be picked up from the view VW\_DBAT\_SAP\_TRUSTED\_RECON\_INCREMENTAL. 2. Each record will be evaluated before being processed. 3. The create request validate basic user details like First Name, Last Name, User type, Last 4 Digits of SSN, Birthdate (MMDD), Organization, Location, etc. 4. Organization code will be used to evaluate the new user manager in the system. 5. After successful user creation in IAM, the user profile is available in IAM and the system will send user PIC and password format notification to the user’s manager via email. 6. On an unsuccessful creation, the IAM system will log an error message with missing info. |
| **Frequency:** | Every 2 hours |

## User Creation: Employee (Non-Incremental Recon Job for All Users):

|  |  |
| --- | --- |
| **UC FR: 13.2:** | **Creating employee from non-incremental recon job for all users** |
| **Actor(s):** | * DB Connector (Employee only) * DBATSAPTrustedRecon Trusted Resource User Reconciliation Scheduler |
| **Description:** | This case covers the addition and change of multiple records within the Identity Management system |
| **Narrative:** | 1. All User record will be picked up from the view VW\_DBAT\_SAP\_TRUSTED\_RECON 2. Each record will be evaluated before being processed. 3. The create request validate basic user details like First Name, Last Name, User type, Last 4 Digits of SSN, Birthdate (MMDD), Organization, Location, etc. 4. Organization code will be used to evaluate the new user manager in the system. 5. After successful user creation in IAM, the user profile is available in IAM and the system will send user PIC and password format notification to the user’s manager via email. 6. On an unsuccessful creation, the IAM system will log an error message with missing info. |
| **Frequency:** | Weekly |

## User Creation: Non-Employee:

|  |  |
| --- | --- |
| **UC FR: 13.3:** | **Creating non-employee users** |
| **Actor(s):** | * Any MPC user * IAM Self-Service Portal |
| **Description:** | This use case covers the addition of a non-employee record within the Identity Management system |
| **Narrative:** | 1. The user logs into IAM system through GUI console and selects option for Non-Employee account creation 2. User submits basic user information like First Name, Last Name, User Type, Last 4 Digits of SSN, Birthdate (MMDD), Organization, Location, Contract Company (Partner), etc. 3. During request, the requester may choose if the non-employee should have Internet access and/or Exchange/Skype access 4. The create request validates basic user details like First Name, Last Name, User Type, Last 4 Digits of SSN, Birthdate (MMDD), Organization, Location, etc. 5. After successful user creation in IAM, the user profile is available in IAM and the system will send user PIC and password format notification to the user’s manager via email 6. If the creation is unsuccessful, an error message will be displayed highlighting the missing or incorrect information. |
| **Frequency:** | As required |

## User Update: Employee (Incremental/Non-Incremental Recon Job):

|  |  |
| --- | --- |
| **UC FR: 13.4:** | **Updating employees using incremental/non-incremental recon job** |
| **Actor(s):** | * DB Connector (Employee) * DBATSAPTrustedRecon Trusted Resource User Reconciliation Scheduler * DBATSAPTrustedRecon Incremental User Reconciliation Scheduler |
| **Description:** | This use case covers the update of multiple employee records within the Identity Management system |
| **Narrative:** | 1. Each record will be evaluated before being processed. 2. Each user record is matched against Employee Number -> Last Name/SSN/Birthdate fields (in that order) 3. If match found for User, then a status attribute will be used to determine which records need to be disabled/enabled 4. Organization code will be used to determine if the user has a new manager to be transferred under 5. All other attributes will update the user’s record |
| **Frequency:** | Incremental every 2 hours. Full weekly |

## User Update: Non-Employee:

|  |  |
| --- | --- |
| **UC FR: 13.5:** | **Updating non-employee** |
| **Actor(s):** | * IAM Self-Service Portal |
| **Description:** | This use case covers the enabling/disabling of multiple records within the Identity Management system |
| **Narrative:** | 1. The user logs into IAM browses to the Manage -> Users tile 2. User searches for and finds the user they’d like to update 3. On the search list or on the user page user finds and enter the details that needs to be updated and click update button in bottom 4. User submits updates to basic user information like First Name, Last Name, User Type, Organization, Location, Contract Company (Partner), etc. Note: SSN/Birthdate cannot be edited, only entered on creation. 5. During request, the requester may change if the non-employee should have Internet access and/or Exchange/Skype access 6. The update request validates basic user details like First Name, Last Name, User Type, Organization, Location, etc. 7. If not an organization admin (which is the supervisor or delegate) for the user’s current organization, an update user request is submitted for approval by the organization supervisor. If the requester is a system admin or org admin, the request is auto- approved, and the user is immediately updated |
| **Frequency:** | As needed |

## User Enable/Disable: Employee (Incremental/Non-Incremental Recon Job):

|  |  |
| --- | --- |
| **UC FR: 13.6:** | **Enabling or disabling of employee using incremental/non-incremental recon job** |
| **Actor(s):** | * DB Connector (Employee) * DBATSAPTrustedRecon Trusted Resource User Reconciliation Scheduler * DBATSAPTrustedRecon Incremental User Reconciliation Scheduler |
| **Description:** | The use case covers the enabling/disabling of multiple records within the Identity Management system. |
| **Narrative:** | 1. Job will be used to query the view for user records 2. Each record will be evaluated before being processed. 3. Each user record is matched against the Employee Number -> Last Name/SSN/Birthdate fields (in that order) 4. If match found in for User record a status attribute will be used to determine which records need to be disabled/enabled 5. All other attributes will update the user’s record. 6. Once updated, the user profile will show Active/Disabled. If Disabled, all connected accounts will also be disabled, but assigned roles will NOT be removed |
| **Frequency:** | Incremental every 2 hours. Full weekly |

## User Enable/Disable: Non-Employee

|  |  |
| --- | --- |
| **UC FR: 13.7:** | **Enabling or disabling of non-employee** |
| **Actor(s):** | * IAM Self-Service Portal * Any MPC user |
| **Description:** | This use case covers the enabling/disabling of a non-employee record within the Identity Management system. |
| **Narrative:** | 1. The user logs into IAM through GUI console and browses to the Manage -> Users tile 2. User searches for and finds the user they’d like to enable/disable 3. On the search list or on the user page, the user will choose the “Enable” or “Disable” button 4. User enters a justification and/or effective date and submits the request 5. If not an organization admin (which is the supervisor or delegate) for the user’s current organization, an enable/disable user request is submitted for approval by the organization supervisor. If the requester is a system admin or org admin, the request is auto- approved, and the user is immediately enabled/disabled |
| **Frequency:** | As required |

## User Termination: Employee:

|  |  |
| --- | --- |
| **UC FR: 13.8:** | **Terminating the employee** |
| **Actor(s):** | * DB Connector (Employee) |
| **Description:** | This use case covers the termination and disabling of an employee record within the Identity Management system. |
| **Narrative:** | 1. IAM ‘Disable Deleted SAP Users’ job will query the records, the OIM employee user records with the **VW\_DBAT\_SAP\_TRUSTED\_RECON** view   If any employee records are NOT matched to records in the **VW\_DBAT\_SAP\_TRUSTED\_RECON** view, the users are: Disabled, moved to the “Terminated\_Users” organization, and moved to the “Other” user type (so they might be re-hired as a contractor later)   1. Once terminated, the user profile will show Disabled. All connected accounts will also be disabled, but assigned roles will NOT be removed |
| **Frequency:** | Every 2 hours |

## Password Reset:

|  |  |
| --- | --- |
| **UC FR: 13.9:** | **Resetting of password** |
| **Actor(s):** | * User |
| **Description:** | This use case covers the password reset and synchronization for a user within the Identity Management system. |
| **Narrative:** | 1. When user (Employee, Non-Employee) created in IAM system Initial default password is communicated with user manager through email notification 2. The password is synchronized with connected application like AD, SAP, etc. (initially and synchronized as the password is changed later) 3. User can change their password with the password reset link available on IAM identity login page or the reset password button 4. On a successful password reset, process will change password in IAM and synchronize to the connected accounts 5. On an unsuccessful password reset, it will have triggered error with info |
| **Frequency:** | As required |

## Certification of Non-Employee Identity:

|  |  |
| --- | --- |
| **UC FR: 13.9:** | **Certification of non-employee identity** |
| **Actor(s):** | * Supervisors |
| **Description:** | This use case covers the how a non-employee is confirmed with his availability in the organization |
| **Narrative:** | 1. Every quarter an email is sent to the supervisors for the certification of their non-employees 2. Once the supervisors get the email they need to confirm it if the non-employee is still actively working in the organization 3. If the non-employee is working, then the supervisor can mark the user as reviewed and complete 4. If the non-employee is not actively working with MPC, then the supervisor can revoke the identity, and all his rights will be revoked immediately 5. If the supervisor will not respond in the given time, then cybersecurity will act on it and will revoke the identity |
| **Frequency:** | Every Quarter |

## Emergency Termination:

|  |  |
| --- | --- |
| **UC FR: 13.9:** | **Emergency termination** |
| **Actor(s):** | * Supervisors * HR * User |
| **Description:** | This use case describes how a user is terminated in the emergency condition |
| **Narrative:** | 1. The supervisor or HR will raise a request to the service desk for the emergency termination 2. On receiving the request Updates ZTAB table, ZEMPL\_SUSPENDED, with ee# 3. Data Services job looks for ee# in ZTAB table and writes out action = SU and status = Inactive 4. IAM detects the SU action like an LOA 5. Identity updated to reflect inactive status 6. Provisioned system user accounts are all disabled (SAP, POLARIS, AD), but a full termination does not occur yet |
| **Frequency:** | Every 2 hours |

## Provisioning of Service Accounts:

|  |  |
| --- | --- |
| **UC FR: 14.1:** | **Provisioning of service accounts** |
| **Actor(s):** | * End UserOrg Admin |
| **Description:** | This use case covers the provisioning of service accounts that are not representative of a person |
| **Narrative:** | 1. The user will submit a request for a new user, choosing the type as a batch or service account and submitting some different information on the user form (not including SSN/Birthdate, and asking for the user account name) 2. Once the request has been made, it will go for the approval of the Org Admin for the chosen organization 3. If the org admin approves, then the user identity is created and provisioned to the appropriate end systems, following birthright access 4. If the org admin denies the request, then the identity is not created |
| **Frequency:** | As required |

# Organization Processes:

We have one scheduler job in IAM for loading organization data into IAM [**Organization Loader**]

* Periodic scheduler job, which runs every 2 hours

## Organization Creation/Update:

|  |  |
| --- | --- |
| **UC FR: 14.1:** | **Creating or Updating the organization record** |
| **Actor(s):** | * DB Connector * Organization Loader Scheduler |
| **Description:** | This use case covers the creation and update of organization records within the Identity Management system |
| **Narrative:** | 1. Organization record is brought in from HR and pulled from the VW\_ORG\_CURRENT view 2. IAM ‘Organization Loader’ job will query the view for org records Organization records are matched against table 3. If it does not find a match, then the organization record will be created as a new organization in IAM 4. If any match found, then the existing organization will be updated with the organization details (in case of any change) 5. Once the organization is determined as a new or updated org, the organization data is mapped against the IAM table fields to serve as list of values |
| **Frequency:** | Every 2 hours |

# UDF Value Loader:

We have one scheduler job in IAM for loading lookup data into IAM [**Load UDF Lookup Values**]

* Unscheduled job, which is run manually (as needed)

## Create/Update Lookups:

|  |  |
| --- | --- |
| **UC FR: 15.1:** | **Create/Update lookups** |
| **Actor(s):** | * DB Connector * Load UDF lookup Values Scheduler |
| **Description:** | This use case covers loading the Location, Job Category, and Partner lookups into the Identity Management system |
| **Narrative:** | 1. Data is manually maintained in the applicable holding tables:   Location, Partner, JobCategory outside of IAM   1. The Load UDF Lookup Values job executes to pick up those values to push them to OIM 2. If values are not found, then they will be created as new 3. If a value match is found, then existing list of values will be updated (if necessary). Note: the update is mainly only enabled/disabled status, as most of the encoded values are the same as the decoded |
| **Frequency:** | As required |

# Active Directory:

## AD User Account Provisioning:

|  |  |
| --- | --- |
| **UC FR: 16.1:** | **Provisioning user accounts in Active Directory** |
| **Actor(s):** | * IAM Active Directory Connector |
| **Description:** | This use case covers the provisioning of users in Active Directory |
| **Narrative:** | 1. All of the users who are created in IAM will be provisioned to AD as birthright access 2. If the identity status is active for the user, then that user will be provisioned to AD 3. For employees we also provide an AD group for Internet access, as default 4. For non-employees we provide the Internet access AD group only if they were enabled for it on their IAM profile (which gave them the Internet access role) 5. The OU will be assigned to the user based on location, using a manually-maintained lookup in IAM 6. On a successful creation of the AD account, the account will be visible in the IAM system |
| **Frequency:** | As required |

## AD User Account De-Provisioning:

|  |  |
| --- | --- |
| **UC FR: 16.2:** | **De-provisioning user accounts in Active Directory** |
| **Actor(s):** | * IAM Active Directory Connector |
| **Description:** | This use case covers the de-provisioning of user accounts in Active Directory |
| **Narrative:** | 1. All the users whose identity status is disabled will be “de-provisioned” from AD, which is configured as a user disable 2. On a successful de-provisioning in AD, we are able to see user account status as disabled in AD and disabled in the IAM system 3. On an unsuccessful de-provisioning of the AD account, it will log an error and the user’s account status will remain in provisioned state |
| **Frequency:** | As required |

## AD User Account Termination:

|  |  |
| --- | --- |
| **UC FR: 16.3:** | **Terminating/Deleting user accounts in Active Directory** |
| **Actor(s):** | * IAM Active Directory Connector |
| **Description:** | This use case covers the termination of user accounts in Active Directory |
| **Narrative:** | 1. Disabled AD accounts with an end date >90 days will be terminated/deleted in Active Directory (after completing a hold order check for that user) |
| **Frequency:** | As required |

## AD Data Sync to IAM:

|  |  |
| --- | --- |
| **UC FR: 16.4:** | **Data synchronization of relevant changes in AD to IAM** |
| **Actor(s):** | * IAM Active Directory Connector * IAM AD reconciliation Job |
| **Description:** | This use case covers the synchronization of relevant attributes like email address and display name between Active Directory and IAM |
| **Narrative:** | 1. The email address and display name are configured in AD through other means, so are not triggered/calculated by IAM 2. The IAM Active Directory User reconciliation job will run periodically and synchronize the differences between AD and the IAM system 3. On a successful update, the user profile is updated with any changes from AD 4. On an unsuccessful recon, an error message will be posted to the log and the user will not be updated in IAM |
| **Frequency:** | As required |

## AD Password Reset:

|  |  |
| --- | --- |
| **UC FR: 16.5:** | **Change a user password in Active Directory** |
| **Actor(s):** | * End user |
| **Description:** | This use case covers the password change process for Active Directory |
| **Narrative:** | 1. User will generally change their password with Ctrl+Alt+Del, which is then picked up by AD-installed component and synchronized to IAM 2. After the new password is synchronized with IAM, the modified password will be synchronized with all connected applications for which the user has an account |
| **Frequency:** | As required |

# IAMGoldTables:

## User Creation/Update in “user\_id”:

|  |  |
| --- | --- |
| **UC FR: 17.1:** | **User creation or update in IAMGoldTables.dbo.user\_id** |
| **Actor(s):** | * Custom .NET Application |
| **Description:** | This use case covers the propagation of user data into the IAMGoldTables database |
| **Narrative:** | 1. The application will synchronize any changes between IAM and the IAM Gold Tables 2. Any new users are to be inserted in the user\_id table 3. Disable users are updated in the user\_id table as disabled status(They won’t be deleted) 4. The before and after values of each field is to be added to the user\_id\_history table for any insert/update/delete action 5. On a successful creation in dbo.user\_id table, we are able to query the user details in dbo.user\_id table or the connected OData services 6. Upon completion of the job, a notification is sent to the IAM support team to identify the run settings and number of records added/updated/deleted 7. On an unsuccessful creation in dbo.user\_id table, the Db connector will log an error |
| **Frequency:** | As required |

## Organization Creation/Update/Delete in “org\_id”:

|  |  |
| --- | --- |
| **UC FR: 17.2:** | **Organization creation or update in IAMGoldTables.dbo.org\_id** |
| **Actor(s):** | * Custom .NET Application |
| **Description:** | This use case covers the propagation of organization data into the IAMGoldTables database |
| **Narrative:** | 1. The application will synchronize any changes between IAM and the IAM Gold Tables 2. Any new/ organizations in IAM are inserted/updated/ in the org\_id table 3. If the organization is disabled then it is marked as deleted in the org\_id table 4. No history is tracked for this table 5. On a successful creation in dbo.org\_id table, we are able to query the org details in dbo.org\_id table 6. On an unsuccessful creation in dbo.org\_id table, the IAM DB connector will log an error. |
| **Frequency:** | Every 2 hours |

# Polaris:

## Provisioning User Accounts in Polaris DB:

|  |  |
| --- | --- |
| **UC FR: 18.1:** | **Provisioning users in Polaris DB** |
| **Actor(s):** | * Any MPC User * IAM Self-Service Portal * IAM DB Connector |
| **Description:** | This use case covers the provisioning of user accounts in Polaris |
| **Narrative:** | 1. Several Polaris roles have been defined in IAM for Polaris DB access 2. Access policies assigned to those roles define what accounts and DB roles should be assigned to the user 3. Access requests for a Polaris role are initiated in IAM using the IAM Self-Service Portal and the access request interface 4. The access will be requested in the form of business roles and will be routed for role owner approval 5. No risk checking occurs for Polaris roles, currently 6. After approval and assignment of the Polaris role to a user a Polaris DB account will be created, and Oracle roles are assigned to the user profile 7. The Polaris DB account is mapped with attributes like username, ref id, profile name, global DN, password, etc. 8. An email notification is sent to the user once the process creates the user account in Polaris with user login and password information a further email is to be sent to the Polaris team, so that they can complete another provisioning task to add a user to a database table of users 9. On a successful creation in Polaris, we are able to see user account in Polaris DB, as well as the assigned roles 10. On an unsuccessful creation of the account, IAM will log an error message |
| **Frequency:** | As required |

## De-Provisioning User Accounts in Polaris DB:

|  |  |
| --- | --- |
| **UC FR: 18.1:** | **De-provisioning users in Polaris DB** |
| **Actor(s):** | * Any MPC User * IAM Self-Service Portal * IAM DB Connector |
| **Description:** | This use case covers the de-provisioning of user accounts in Polaris |
| **Narrative:** | 1. Access requests to remove a Polaris role are initiated in IAM using the IAM Self-Service Portal and the access request interface 2. New request raised to remove an assigned Polaris role 3. The request is a removal, so is auto-approved 4. After removal, eval policy flag triggers and revokes the Polaris DB account and Oracle roles from the user profile 5. The Polaris DB account and role assignments are deleted from the Polaris database 6. An email is sent to the user to tell them access was removed from their account. A further email is sent to the Polaris team, so that they can complete another de-provisioning task to remove the user from a database table of users 7. On a successful deletion in Polaris, the user account and assigned roles will all be deleted 8. On an unsuccessful deletion of the account, OIM will throw/log an error message |
| **Frequency:** | As required |

## Polaris Password Reset:

|  |  |
| --- | --- |
| **UC FR: 18.3:** | **Change a user password in Polaris DB** |
| **Actor(s):** | * End user |
| **Description:** | This use case covers the password reset process for Polaris |
| **Narrative:** | 1. When a Polaris DB account is successfully created by IAM, the custom process sends an email notification to the user containing the user login and password details 2. If end users want to reset their password for the Polaris account, they reset their password using Polaris GUI password reset 3. No password synchronization is currently in place for Polaris accounts |
| **Frequency:** | As required |

## Access Requests for Polaris DB:

|  |  |
| --- | --- |
| **UC FR: 18.4:** | **Access request for Polaris DB** |
| **Actor(s):** | * Any MPC User * OIM Self-Service Portal * OIM DBUM Connector |
| **Description:** | The use case covers the access request of user accounts in Polaris DB |
| **Narrative:** | 1. Access requests for a Polaris role are initiated in OIM using the OIM Self-Service Portal and the access request interface 2. The access will be requested in the form of business roles and will be routed for role owner approval 3. No risk checking occurs for Polaris roles, currently 4. After approval and assignment of the Polaris role to a user a Polaris DB account will be created, and Oracle roles are assigned to the user profile 5. The Polaris DB account is mapped with attributes like username, ref id, profile name, global DN, password, etc. 6. On a successful creation in Polaris, we are able to see user account in Polaris DB, as well as the assigned roles |
| **Frequency:** | As required |

# SAP:

## Provisioning User Accounts in SAP:

|  |  |
| --- | --- |
| **UC FR: 19.1:** | **Provisioning employee user accounts in SAP** |
| **Actor(s):** | * Role Based (Birthright access for employees) * IAM SAP Connector |
| **Description:** | The use case covers the provisioning of user accounts in SAP |
| **Narrative:** | 1. SAP roles are available in IAM for provisioning accounts into 6 SAP applications 2. The user account will by default match the user’s PIC, unless the SAP account was created in the past with a legacy account (based on the user’s name) 3. Birthright provisioning is done with the ‘SAP Basic Account Provisioning’ roles. The employee role is auto-assigned by rule. 4. All 6 SAP applications have an account access policy attached to the role for assignment of a SAP account in each system 5. In the employee role, ECC has a parameter access policy attached to the role, for HR-required parameters to be assigned 6. No risks are possible on these accounts or roles, so risk checking is not required |
| **Frequency:** | As required |

## SAP Role Request and SOD Check:

|  |  |
| --- | --- |
| **UC FR: 19.2:** | **Assignment of SAP access** |
| **Actor(s):** | * Any MPC User * IAM Self-Service Portal * IAM SAP Connector * IAM SOD Check |
| **Description:** | The use case covers the request, SOD check, and approval of SAP roles |
| **Narrative:** | 1. Roles will be defined in IAM for SAP Enterprise and Functional roles 2. Access policies assigned to those roles define what roles (and sometimes AD groups) should be assigned across the 6 SAP systems and AD 3. For any removal requests, the request is auto-approved, and the role is immediately removed from the user, notifying them via email that access has been removed from their account 4. Access requests for SAP roles are initiated in IAM using the Self-Service Portal and the access request interface 5. The access will be requested in the form of Enterprise or Functional business roles and will be routed for role owner approval after being checked for risks. Note: Entitlements cannot currently be requested directly 6. When any SAP role is requested, in IAM the system needs to perform a SOD check for that particular user and role 7. If a critical risk is found for a requested entitlement, the request containing a role that provides that entitlement will be rejected 8. If a high risk is found for a requested entitlement, the request is updated with the risk results from that entitlement, to provide info to the approver 9. Any low/medium risk is ignored 10. If not rejected by critical risk, IAM will request approval from the role approver group, notifying them via email 11. After approval has been received and the SAP access has been provisioned the attributed SAP roles are visible in the user’s profile |
| **Frequency:** | As required |

## De-Provisioning User Accounts in SAP:

|  |  |
| --- | --- |
| **UC FR: 19.3:** | **De-provisioning user accounts and or roles in SAP** |
| **Actor(s):** | * Rule Based (Employee-Birthright Access DE provisioning) * Remove access request in IAM |
| **Description:** | This use case covers the de-provisioning of employee accounts in SAP |
| **Narrative:** | 1. If a user is disabled in IAM their attributed SAP accounts are automatically disabled as well. Disabled user accounts are not deleted from SAP 2. All role removal requests are auto-approved and the roles are immediately removed from the user, notifying them via email that access has been removed from their account 3. Risk checking is not performed on removal requests |
| **Frequency:** | As required |

## Password Synchronization to SAP:

|  |  |
| --- | --- |
| **UC FR: 19.4:** | **Change a user password in SAP** |
| **Actor(s):** | * End User |
| **Description:** | This use case covers the password reset/synchronization process for SAP accounts |
| **Narrative:** | 1. When a user changes their password in IAM or in AD the password will synchronize to all SAP systems 2. If necessary, the user can also update their SAP password, per system, in the SAP GUI by entering their user name and choosing “New Password”. **This password will NOT synchronize to IAM or any other system** 3. On an unsuccessful password change, the IAM system will log an error, but the user is not notified. |
| **Frequency:** | As required |

## Provisioning Non-Employee Accounts in SAP:

|  |  |
| --- | --- |
| **UC FR: 19.5:** | **Provisioning non-employee user accounts in SAP** |
| **Actor(s):** | * Role Based (Access for non-employees) * IAM SAP Connector |
| **Description:** | The use case covers the provisioning of user accounts in SAP. These are very similar roles to employees, but do not provide ECP parameters and are not auto-provisioned as birthright |
| **Narrative:** | 1. SAP roles are available in IAM for provisioning accounts into 6 SAP applications 2. The user account will by default match the user’s PIC, unless the SAP account was created in the past with a legacy account (based on the user’s name) 3. All 6 SAP applications have an account access policy attached to the role for assignment of a SAP account in each system 4. All 6 SAP applications have a role access policy attached for assignment of a base SAP access role in each system 5. No risks are possible on these accounts or roles, so risk checking is not required |
| **Frequency:** | As required |

# Targeted AD Attribute Sync (TADA):

The TADA system manages user access to email, skype, Citrix and users Home-drive

TADA updates the Active directory account of a user with relevant information.

## TADA Provisioning:

|  |  |
| --- | --- |
| **UC FR: 20.1:** | **Custom data sync and provisioning with TADA** |
| **Actor(s):** | * IAM System (Birth Right) * Custom program (TADA) |
| **Description:** | This use case covers updating user account information in TADA |
| **Narrative:** | 1. TADA will query user identity data as source to its configured fields and tasks 2. TADA will take that data and populate fields in AD accordingly    1. Fields include (see TADA documentation for the complete and current listing):   company  department  displayName  division  employeeNumber  l  extensionAttribute13  mailNickname  mobile  extensionAttribute6  physicalDeliveryOfficeName  telephoneNumber  extensionAttribute3  uid  postalCode  extensionAttribute2  st  manager  title   1. User tasks will also execute to    1. Provision Exchange/Skype    2. Update Exchange/Skype account status    3. Provision Citrix    4. Double-check and correct user status (including accounts such as -extra, -staging, and -azure)    5. Push user data such as email, PIC, and SAP Account to SAP |
| **Frequency:** | As required |

# Other:

## Delegation of User’s IAM Permissions:

|  |  |
| --- | --- |
| **UC FR: 21.1:** | **Delegation of user’s IAM permissions** |
| **Actor(s):** | * User * Proxy User |
| **Description:** | This use case covers how a user can set up a proxy for him/her in case of their absence (or unfortunately chosen desire NOT to perform actions on users in IAM, such as with executives) |
| **Narrative:** | 1. The user will set up a delegate for the proxy rights in case of their absence 2. The user can delegate the rights to any selected user 3. Once the delegate is set all new access requests will go to the delegated user. Previous request will stay in the user’s queue |
| **Frequency:** | As required |

## Organization Admin Permission for Supervisors:

|  |  |
| --- | --- |
| **UC FR: 21.2:** | **Organization admin permission for supervisors** |
| **Actor(s):** | * Org Admin / Supervisor |
| **Description:** | This use case covers how an Org Admin is entitled with the special rights |
| **Narrative:** | 1. A user can be set up as an Admin for a specific organization, which is automatically given to an organization supervisor, but also can be assigned directly for delegation 2. Once the user is given the admin rights he can:  * Approve new account requests for Non-Employees * Approve new account requests for Service accounts * Modify users that are within his/her organizations * Reset passwords for users within his/her organizations |
| **Frequency:** | As required |