

Project Name SailPoint IAM Implementation

Prepared For: SMWE

Prepared By: NTT Data

Date:



**Copyright**

**Confidentiality**

**Disclaimer**

# Document Control

## General Properties

Author(s):

Contributors(s):

Data Classification:

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author(s) | Summary of changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Distribution

This document has been distributed to:

|  |  |  |
| --- | --- | --- |
| Name | Organization | Title / Role |
|  |  |  |
|  |  |  |

## Approvals

This document requires following approvals:

|  |  |  |
| --- | --- | --- |
| Approver | Date Approved | Title / Organization |
|  |  |  |
|  |  |  |

# 

Contents

[Document Control 3](#_Toc525115090)

[A. General Properties 3](#_Toc525115091)

[B. Revision History 3](#_Toc525115092)

[C. Distribution 3](#_Toc525115093)

[D. Approvals 3](#_Toc525115094)

[1. Executive Summary 6](#_Toc525115095)

[1.1 Business Goals 6](#_Toc525115096)

[1.2 Value Proposition 6](#_Toc525115097)

[1.3 Critical Success Factors (CSFs) 6](#_Toc525115098)

[1.4 Deployment Strategy 7](#_Toc525115099)

[2. Requirements 8](#_Toc525115100)

[2.1 Review of Scope and Requirements 8](#_Toc525115101)

[2.2 Functional Requirements 8](#_Toc525115102)

[2.3 Non-Functional Requirements 9](#_Toc525115103)

[2.4 Availability / Capacity 9](#_Toc525115104)

[3. Use Cases 10](#_Toc525115105)

[4. Solution Overview 11](#_Toc525115106)

[4.1 System Context 11](#_Toc525115107)

[4.2 Architectural Overview 12](#_Toc525115108)

[4.4 Information Flows 14](#_Toc525115109)

[4.5 Data Types 16](#_Toc525115110)

[4.6 Architectural Decisions 16](#_Toc525115111)

[4.6.1 Architectural Decision – CloudSOC SpanVA Placement 16](#_Toc525115112)

[5. Physical Architecture 18](#_Toc525115113)

[5.1 Production Environment 18](#_Toc525115114)

[6. Operational Model 19](#_Toc525115115)

[6.1 Production and Disaster Recovery 19](#_Toc525115116)

[6.2 User Access & Authorization 19](#_Toc525115117)

[6.3 Policies 20](#_Toc525115118)

[6.4 Reports 20](#_Toc525115119)

[6.5 Connectivity Diagrams 20](#_Toc525115120)

[6.5.1 Solution Connectivity Diagram 20](#_Toc525115121)

[7. Appendix 21](#_Toc525115122)

[7.1 Definitions 21](#_Toc525115123)

# Executive Summary

.

## Business Goals

.

## Value Proposition

## Critical Success Factors (CSFs)

The key success factors for the project are:

## Deployment Strategy

Based on the number of Users, SMWE Implementation is categorized into the Small to Medium size Enterprise wrt Deployment footprint.

These installations fit most small\medium size enterprises and start to separate the UI and Batch/Task layers for performance benefits, typically designating one UI host and one or two batch/task hosts. Often, installations at this scale have a substantial volume of data to process during account aggregation tasks. This scale of installation requires the separation and dedication of a relational database host. Medium footprint installations exploit the fact that Task/Batch servers can act as UI servers in the event that the singleton UI server should fail. Load Balancing systems used with medium configurations should be configured to preferentially route UI traffic to the UI server and only route UI traffic to the Task/Batch servers in the event of UI server failure or saturation.

Hardware recommendation for SMWE installation:

1 x IdentityIQ Batch/Task host with:

• 4-Core Processor

• 8GB of RAM

• 64 bit OS

• 40GB of local block storage space for binaries and logs

1 x IdentityIQ UI host, with:

• 4-Core Processor

• 8GB of RAM

• 64 bit OS

• 40GB of local block storage space for binaries and logs

1 x Dedicated DB Server host, with:

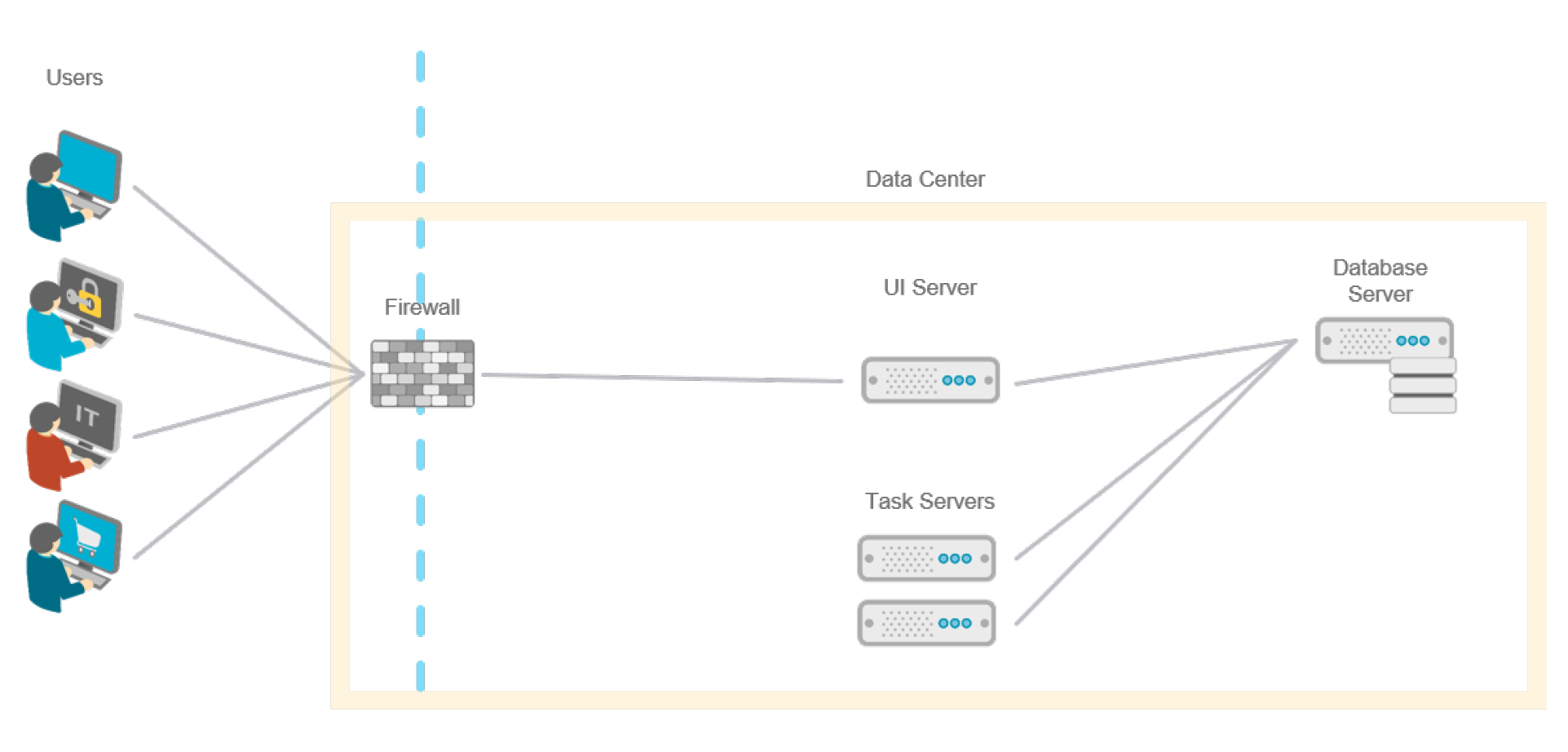
• 4-Core Processor

• 64GB of RAM

• 64 bit OS

• 500GB of RAID protected DB storage plus 20 of RAID protected storage for OS files

SMWE will have 1 Dev\QA Env and 1 Prod Env, both having the similar hardware configuration.



# Requirements

## Review of Scope and Functional Requirements

**Ultipro:**

Ultipro is the HR system of SMWE holding the Employee Source of truth records.

Ultipro will not be considered as a target system for User provisioning from SailPoint.

Ultipro will send Daily file feeds for the following events, with appropriate status:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Event** | **Account Status** | **Fields** |
| 1 | Recruitment Completion | PreEmployment | FirstName, LastName, Personal Email, Mobile Number, Date of Joining, Status, RecordCreationDate |
| 2 | Date of Joining | Active | All agreed fields |
| 3 | Job code change, Department Change, Promotion, etc. | Active | All agreed fields |
| 4 | Separation | Terminate | All agreed fields |

Upon a user Termination, his HR Manager will disable the user account in SailPoint.

Upon job code\Department change the users access review will be triggered to the HR Manager to validate if the access needs to be retained\modified\removed.

Fields that Ultipro file feed will have: (TBD SMWE BA)

|  |  |  |
| --- | --- | --- |
| **FIELD** | **FIELD TITLE** | **LENGTH** |
| 1 | FIRST\_NAME | 30 |
| 2 | MI | 5 |
| 3 | LAST\_NAME | 30 |
| 4 | SUFFIX | 5 |
| 5 | Known As | 40 |
| 6 | Candidate Ref# | 20 |
| 7 | PAYROLL\_AREA | 2 |
| 8 | POSITION\_NUM | 8 |
| 9 | POSITION\_DESC | 40 |
| 10 | REPORTS\_TO\_POS\_NUM | 8 |
| 11 | GRADE | 4 |
| 12 | PERSONNEL\_NUM | 8 |
| 13 | ORG\_UNIT\_NUM | 8 |
| 14 | COST\_CENTER\_NUM | 10 |
| 15 | COST\_CENTER\_DESC | 40 |
| 16 | JOB\_NUM | 8 |
| 17 | JOB\_DESC | 40 |
| 18 | PERS\_AREA | 4 |
| 19 | PERS\_AREA\_DESC | 30 |
| 20 | PERS\_SUBAREA | 4 |
| 21 | PERS\_SUBAREA\_DESC | 15 |
| 22 | LOA\_INDICATOR | 1 |
| 23 | EMPLOYEE\_GROUP | 1 |
| 24 | BUILDING\_NAME | 60 |
| 25 | CITY\_ENGLISH | 40 |
| 26 | STATE | 3 |
| 27 | ZIP\_CODE | 10 |
| 28 | INTERNAL\_MAIL\_CD | 30 |
| 29 | BLDG\_ADDR\_1 | 60 |
| 30 | BLDG\_ADDR\_2 | 40 |
| 31 | WORK\_NUM | 20 |
| 32 | FAX\_NUM | 20 |
| 33 | COUNTRY\_CD | 3 |
| 34 | MOBILE\_NUM | 30 |
| 35 | PAGER\_NUM | 30 |
| 36 | COMPANY\_CODE | 4 |
| 37 | COMPANY\_NAME |  |
| 38 | Start Date | 8 |
| 39 | Separation Date | 8 |
| 40 | Status Indicator | 1 |
| 41 | Assistant Name | 62 (max) |
| 42 | Assistant Phone | 30 |
| 43 | NTID | 30 |
| 44 | Email address | 241 |
| **45** | **Employee Type** | **1** |
| 46 | FILE\_CREATION\_DATE\_TIME | 14 |

Attributes to be added additionally:

* User account Type (Privileged, etc)
* Office365LicenseType
* Site code (3 letter location code used for the OU in AD)

**Active Directory:**

AD Groups List:



AD Groups associated with IS Authorization form Applications:



AD Groups with standard naming and group owners template to be filled by SMWE BA:



AD Provisioning Approval process:

Any user provisioning request to an AD group, will go thru 2 step approval process; HR Manager provides first level of approval after which request is passed to the Group owner(s) one of whose approval will be required. (Group owner information will have to be captured in the format as mentioned in above templae)

Birthright access:

For Phase 1 implementation, upon new user creation the account will be placed in the appropriate Domain users OU as mentioned in below section.

All other access will be provisioned as per the Manager’s selection in Service Now forms.

Organization Unity (OU) where to place users:

Domain Users OU and sub OU's based on site (Job Location)

Domain Users\CSM\ - Chateau Ste Michelle WDV

Domain Users\COL\ - Columbia Crest

**Assumption** (to be validated by SMWE BA, once the Ultipro attributes are finalized)

Site code will be part of the fields sent by Ultipro\Contractor creation.

Correlation:

Existing employee user types have Employee Number as Unique Id.

New employees will be created after checking for matching First name, Last Name, Middle Name, Personal Email, Mobile Number for uniqueness.

Later the Employee number will flow in from Ultipro and if Employee Number is present, that will be used for correlation.

New Contractor user types will be created after checking for matching First name, Last Name, Middle Name, Personal Email, Mobile Number for uniqueness. Same will be used to match existing contractors also.

Application Questionnaire:



|  |  |
| --- | --- |
| 2.1.01 | Manage (create, update and delete) the following types of accounts from the IAM system per Altria's naming standards. Accounts will be aggregated from the target applications and will be correlated automatically using correlation rule configured in the application configuration. Accounts can be updated through access/account request. Permission to update the accounts will be managed based upon defined policy.  Type of accounts:  • Generic Account \* Regular User Account • Training Account • Kiosk account (sitename, Kiosk) • Admin account (A\_) • Test account \* Phone and Shared Phone account \* E account \* Conference accounts \* Service account (S\_) [Service Account OU]. \* Mailbox accounts (Exchange or O365) \* Unique IDs (an account with no AD record; used for SAP Other systems) |
| 2.1.02 | Following AD account creations, provision the user’s home Directory and home Drive attributes and permissions. |
| 2.1.05 | Schedule a task in SailPoint to disable the user accounts (regular, admin and test) that have not logged into Windows for over 90 days for only interactive logon |
| 2.1.06 | The IdM Tool will manage provision and requested deprovisioning of AD 'contact objects' |
| 2.1.07 | Create workflow/approval process for the below entitlement request for <APP>  If user creates entitlement request, create workflow/approval process for <app> for user entitlement request in SailPoint with the report manager approval and provision the requested OU (entitlement)  If Manager requested the change, no approval is required  For Non-employee request the same, both manager approval and manager delegate approvals are mandatory for provisioning |
| 2.1.08 | Automate the leaver process in SailPoint to disable the user’s personal accounts and remove all the company data/systems. Send the email notification to terminated user’s manager about the disabled accounts |
| 2.1.10 | IIQ’s LCM module will be capable of handling access request with multiple entitlements. Approval scheme will be set as per defined, and approvals will be generated through Approval Assignment Rule. Provisioning will occur as per the approval decisions.  From Quicklink Population page in IIQ, multiple entitlement selection will be configured. |
| 2.1.12 | Leaver workflow need to be implemented, which will perform the deactivation of the accounts automatically as the identity state is updated in the HR Auth Source. Identities will not be deleted from the leaver process. When the Altria Record Management process is completed along with all the legal holds are cleared, HR source will be updated and based on that a task will be configured for account deletion. |
| 2.1.13 | Terminated users must not be visible in Global Address List (GAL). |
| 2.1.15 | After the HR auth source is updated with the identity state to be terminated for an user, at the time of auth source aggregation, leaver workflow will be launched –   * Initially password will be reset and notification will be sent to the manager with the new random password * After 5 days accounts will be disabled |
| 2.1.16 | The account creation follows Altria’s standard for constructing the following AD attributes:  • samAccountName (obtained from Active Directory) • displayName • cn • password is randomly generated and changed on first use  Provisioning policy will created and set under the application configuration. Provisioning policy will map identity data to the AD account attributes. |
| 2.1.17 | Place the users in the appropriate OU, based on the Site code.  Organization Unity (OU) where to place users:  Domain Users OU and sub OU's based on site (Job Location)  Domain Users\CSM\ - Chateau Ste Michelle WDV  Domain Users\COL\ - Columbia Crest |
| 2.1.18 | IAM system (SailPoint) must send the notification email to User/Manager/Requestor once the AD account is provisioned in SailPoint. Email template must follow the Altria’s standards. Manager email |
| 2.1.20 | Create the following AD attributes for shared mailbox accounts: • mail Nickname (in case email was selected) • mail (in case email was selected) \* assign ownership of shared mailbox account \* auto-create the ad group associated with the mailbox and assign user's permissions |
|  | licenses should be removed when O365 account is disabled |
| 2.1.22 | The turnaround time on access provisioning and deprovisioning will be less than 1 hour after approvals or the appropriate event trigger. Alert thresholds will be established to avoid unplanned impacts by scenario. |
| 2.1.23 | Automate the following access recertification process for AD  - Group / DL membership  - Group / DL ownership  - Auxiliary Account ownership (service, mailbox, phone, etc.)  - Auxiliary Account validity and purpose  - Group /DL validity and purpose  - Group Attribute validation (Privacy, Privileged, etc.)  Schedule recertification for the below  - Group / DL membership  - Group / DL ownership  - Auxiliary Account ownership (service, mailbox, phone, etc.)  - Auxiliary Account validity and purpose  - Group /DL validity and purpose  - Group Attribute validation (Privacy, Privileged, etc.) |
| 2.1.24 | Primary and secondary owners can manage ownership of AD Groups. The secondary owner will be able to edit everything except primary owner. |
| 2.1.25 | In SailPoint, assign and manage owners for system account such as service accounts, shared mailboxes , etc., |
| 2.1.26 | LCM module of IIQ will be capable of handling below challenges by enabling all the features of access request page through QuickLink Population configuration page –  - Create multiple accounts  - Bulk add/remove from Groups / DLs   - Bulk changes to accounts (i.e. bulk disable) |
| 2.1.26 | As part of leaver process, disable/remove PCI group access |
| 2.1.27 | IdM system must track shared mailbox access ownership, there must be primary and can have secondary owners |
| No Number | Capture the group & description details and include them in email template while send to approver for approval. |
| No Number | Conference room Account creation |
| No Number | The IAM System needs to provide business labels that are searchable for access to information in human readable, business friendly formats. |
| NEW | Support change to email address based on Operating company changes and name changes.   Make new address the primary in Outlook  Move previous primary address to a secondary for 90 days  Send email to end user of change and the expiration of the previous  Send reminder email to end user of expiration of secondary addresses |
|  | **Directory Services -- Active Directory Group Management** |
| 4.1.02 | Extended attributes will be created for the managed attributes in IIQ to manage Distribution & Security groups with attributes such as privileges, file share controls and classifications etc. |
| 4.1.03 | Users with specific capabilities (HelpDesk\Managers? – TBD SMWE BA) should be able to create new groups for AD and provision it in the AD |
| 4.1.04 | On board all AD groups in SailPoint |
| 4.1.05 | Customize the welcome message, departure message, all email notifications in SailPoint as per Altria’s standards |
| 4.1.06 | An Extended Attribute will be created to store Expiration Date of an user account. This attribute will sync with the HR source value, or can be modified using a custom form in the IIQ. Custom should only be only available to the designated person or a workgroup. Through a custom run rule task in IIQ, expiration notice will be sent to the user’s manager/group owner prior to the expiration as follow:  o 30 days prior  o 10 days prior  o 3 days prior • On expiration date IIQ will launch the Leaver workflow to delete the group and disable the user account, unless the expiration date is extended. At the same time a notification is sent to the user/group owner. |
| 4.1.07 | AD Group owners will have the automatic privilege to modify the group attributes in IIQ. But proper extended attributes must be configured in IIQ to store all the required groups attributes. |
| 4.1.08 | When new groups are created thru SailPoint, system should ensure it has at least 1 owner and should have the Manager level capability in SailPoint assigned. (Capability matrix for SMWE users – SMWE BA) |
| 4.1.09 | Distribution Lists must have at least 1 owner at any employee level |
| 4.1.13 | Group Owners will be able to modify the following attributes of their groups: o Member o Expiration Date o Description o Owner |

**Exchange\O365:**

SMWE has a hybrid environment for Mailboxes which includes an on-Premise Exchange Server and O365 in the cloud. AD Connect\Sync is used to sync between these.

Current Process:

Exchange Server Version:

|  |  |  |  |
| --- | --- | --- | --- |
| Exchange Server 2013 CU5 | May 27, 2014 | 15.0.913.22 | 15.00.0913.022 |

Name                : SMWECSMCAS1

Edition             : StandardEvaluation

AdminDisplayVersion : Version 15.0 (Build 913.22)

ServerRole          : Mailbox, ClientAccess

Site                : ustis.com/Configuration/Sites/SMWECSM

New Process\Requirements:

All the mailbox provisioning, Distribution Lists, Name changes, O365 licensing will be done thru SailPoint, as listed in the business requirements above. The licensing level to be used is selected by the Manager while raising the IT request thru Service Now. So O365 provisioning will trigger once the Service Now form is submitted with these details for New Users.

**JDE:**

Current Access Request Process:



Compliance\Reporting:



Current report includes the below fields from JDE.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User/Role | User Name | Profile - Date Last Change | Profile - Enabled User | Profile - Changed By | Profile - Program ID | Profile - Date Updated |

While doing Data Aggregation from JDE, the above fields needs to be pulled (besides other IAM specific fields)

Application questionnaire



**Service Now:**

OTB Service Catalog Integration type is not used in the current implementation, due to the current version’s limitation on Business Role based access request Catalog; There is no option to show up the Application and its entitlements, which is planned for a future version, but SailPoint is not sure of this features’ release date.

Service Desk Integration Module will be used to raise new Request tickets or update tickets.

Version:

Service Now is upgraded to Madrid version currently and SailPoint 8.0 version supports this version.

Current Process:

HR Manager fills out the below IS Authorization form when a new user joins and attaches it to an IT ticket in Service Now and an IT technician manually decodes the document selection and creates further tickets to respective groups for provisioning.



New Process:

This manual form will be replaced with Service Now forms and automated provisioning thru SailPoint will happen for in-scope applications.

Service now forms will use the below mapping to map certain application role selections to their corresponding AD groups, to provision.



For those in-scope applications like JDE, JDE defined roles will be sent as entitlements to SailPoint.

Application Questionnaire:



**Contractors:**

Current Process:

Contractors are currently maintained in excel sheet and account created in AD based on Service Now ticket.

New Process:

Contractors will be created directly in SailPoint by the HR Manager. Initial loading of Contractors will happen thru a file feed.

Attributes for Contactors include Contract Expiration Date (besides other user fields – TBD SMWE BA).

Correlation:

New Contractor user types will be created after checking for matching First name, Last Name, Middle Name, Personal Email, Mobile Number for uniqueness. Same will be used to match existing contractors also.

Initial Load:

Similar to employee file feed, we will need a file with all the contractor information to be aggregated into the system. SMWE BA needs to get this file.

Proposed Fields

Contract Agencies Tab

The Contract Agencies tab is a form used to manage all the contract agencies with which an organization works in a single place.

|  |  |
| --- | --- |
| **Fields** | **Description** |
| Agency Name | The agency’s name |
| Agency ID | The agency’s unique ID (auto-increment) |
| Domain | The agency’s domain |
| Contract Person | The name of the agency contact |
| Telephone | The agency’s phone number |
| Email | The agency’s email address |
| Address | The agency’s mailing address |

Department Tab

Manage departments within an organization that are using the defined vendors from the previous tab in a single place.

|  |  |
| --- | --- |
| **Fields** | **Description** |
| Department Name | The department name |
| Department ID | The department unique ID (auto-increment) |
| Contract Agencies | List of contract agencies associated with this department |
| Assignment Manager | The manager of the assignment |
| Account Sponsor | The access approver and review for this department |
| Account Administrator | The administrator of this department |

Assignments Tab

Manage the relationships between contract agencies and their contractors with the departments that are using their services to provide better visibility into when contracts are expiring so that governance can be tied to those events efficiently.

|  |  |
| --- | --- |
| **Fields** | **Description** |
| Assignment Name | The assignment name |
| Assignment ID | The assignment’s unique ID (auto-increment) |
| Expiry Date | The date the assignment expires |
| Departments | The departments connected to this assignment |
| Contract Agencies | The contract agency connected to the assignment |

**Other User Types:**

There are different employee types; question is open to SMWE; this section needs to be updated based on their response. (TBD – SMWE BA)

**Compliance:**

JDE Access Review

AD Access Review

**Reporting:**

Termination report

SoX control report - JDE

Periodicity:

Termination reports are sent weekly.

Report sent To:

For the in-scope applications, Termination report is sent to below users:

Kreta, Marty - E1 JDE profile

\*Services Coordinator, IT (Donna Skipworth)

--- E1 JDE Profile

\*Systems Analyst ( Dustin Harper)

--- Office 365/Outlook

Sample reports:

JDE main report fields:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User/Role | User Name | Profile - Date Last Change | Profile - Enabled User | Profile - Changed By | Profile - Program ID | Profile - Date Updated |

Other reports will be added as per the requirements below.

|  |  |
| --- | --- |
|  | **Auditing & Reporting** |
|  | SailPoint must provide the information/reports required for security audit |
|  | Create a customized report in SailPoint for the below   * Identity updates * Entitlement added/changes/updates/removals * Self-administration * Historical reports for password changes * Schedule a task/job to send the import reports to key people such as app owners, internal auditors, admins |
|  | Create customized report to provide the historical changes/updates/  For example, user had access to the particular entitlements/resources/applications |
| 8.1.01a | Custom report need to be created to preview all the access and account requests (create, update, delete) performed and the report will contain requester, requestee, all the approvers and time for each of the action. |
| 8.1.02 | Ability to archive data and for future reference after 3 years in accorodance with Altria Records Retention Policies, or in alignment with legal hold requirements |
| 8.1.03 | Access recertification campaigns will be configured to felicitate below cases – • Verify that users have been given appropriate permissions to accomplish their business tasks for the following types of accounts   o AD accounts and associated groups.  • Be able to see all the access rights that a user has and all the users that have a specific access.  • Provide a process for conducting recertification campaign.  • Allow for the removal of unneeded access durring recertifcation • Allow IDM System custodians to use the IdM system to monitor the progress of the recertification • Ability to send reminders to recertification recipients if there is no action taken. • Ability to deny role ownership and transfer it to someone else  • Ensure campaign activities are logged to allow for:  o Analysis of the actions taken in the course of the recertifcation campaign.  o Prove to auditors that attestation campaign was done and that unneeded access rights were actually removed. |
| 8.1.05a | Users will have to privilege to self-certify their access. Cases that will be taken under consideration –  • Users should see what accounts they have • Group owners should see what groups they own in AD • Account owners should see what accounts they own • Manager should see what access their direct reports have |
|  | Users will have to privilege to self-certify their access. Cases that will be taken under consideration –  • Users will see what JDE roles and privileged access they have • Role owners will see what roles they own • Account owners will see what accounts they own • Manager will see what access their direct reports have \* JDE users can see the validity dates of other users for access troubleshooting |
| 8.1.08 | Reports to be created to review specific access which users are having. IIQ will provide a dashboard to run query to get the access related data on the identities. |
| 8.1.05 | Manager Recertification process for AD Accounts will implemented. |
| 8.1.09 | Specific users and workgroups will have access to extract reports out of the reporting database based on criteria such as: • Date range • Requestor • Target • Approver  It will be configured by assigning capabilities. |
| 8.1.10 | Proper transparency and accountability will be provided, by enabling auditing to track all actions requested and performed relative to the following operations: • Active Directory, SAP, or JDE access provisioning/de-provisioning • Group or Role owner change |
| No Number | Support views showing all approvals you have completed, as manager or resource owner |
| 4.1.08 | Audit will be enabled in IIQ for every group ownership change. |

**Password Management:**

AD Password Complexity:

*Min 8 characters, one uppercase, 1 lowercase, 1 special character*

AD Password Policy:

TBD - SMWE BA

JDE Password Complexity:

*Minimum passowrd length = 8, minimum number of numerics = 1, minimum number of alpha = 1, minimum number of special characters = 1*

Service Now, O365:

These applications use Active Directory credentials for authentication, so same AD password complexity rules will be applicable.

Self Service Password Security Questions:

Default questions will be used for now. TBD – SMWE BA.

All other password management requirements are as detailed below.

|  |  |
| --- | --- |
|  | **End User Self Service - Password Management** |
|  | Self-service workflow should be implemented to facilitate forgot password feature with OTP. OTP shall only be sent once the user verifies his/her identity correctly by answering pre-configured questions. |
|  | Users with HelpDesk or System Administrator capability in IIQ, will be able to reset password for other users or service accounts. Users will have to set a new password after logging in. |
|  | Users with HelpDesk or System Administrator capability in IIQ, will be able to disable or enable accounts of other users, as well as service accounts. |
|  | Set Password Interceptor module of IIQ to perform password synchronization of the selected target systems. |
|  | Self-service workflow to be enabled for self-registration with user-defined questions answers. |
|  | Support for pre-defined challenge-response questions and answers |
|  | Self-service workflow will enabled to facilitate the Forgot Password Reset feature.  user will be allowed to reset password and IdM/target account will be unlocked after correctly answering three out of five; user account will be locked if more than two questions are answered incorrectly |
|  | Web-based GUI interface will be invoked for desktop password reset |
|  | IVR and/or telephony interface for resetting passwords |
|  | Self-service password reset application may be encapsulated as a portlet |
|  | **Password Management – Delegated Password Administration** |
| 7.1.01 | Delegated Administrators (e.g., Help Desk, Data Center) will be able to reset IIIQ password (create a new one-time password) without knowledge of current password by validating the user’s identifying information Identifying Information in the IIQ system against the information provided by the user. |
| 7.1.03 | Users permanently locked out can be unlocked by IIQ users with Capability such as – • Helpdesk,  • System Administrators, • User’s manager. |
| 7.1.08 | Users cannot register or reset passwords directly from the Internet Remote network access must be employed to gain access to the registration and self-service password reset functionality |
| 7.1.09 | New users should be prompted and/or reminded regularly to perform the self-service registration until the registration process is completed. |
| 7.1.10 | VPN users need to receive an email notification when their password is about to expire • 10 days before • 5 days before  • 1 day before |
| 7.1.11 | Passwords for AD and SAP personal accounts should be synchronized from the user's AD regular account (excluding the system accounts owned by that user such as service accounts and shared mailboxes, firefighter, etc.) |
| 7.1.12 | After an assisted password reset, by the service desk or administrators the user will be forces to change their password on the next login. |
| 7.1.13 | Users will reset their password through the IdM portal or through the Windows Ctr+Alt+Delt interface |
| 7.1.14 | During registration, questions are displayed to the user for the purpose of validating the user for password resets. |
| 7.1.15 | The user must answer 5 questions in order to register. (User can change their questions/answers at a future date if they re-register.) |
| 7.1.16 | Users must answer two questions from the five they have registered before their password will be reset. |
| 7.1.17 | Registration questions must not allow the same answer to multiple questions. |
| 7.1.18 | The answers to the registration questions must be between three and fifty characters (3-50 characters). |
| 7.1.19 | Users will be temporarily locked out for 5 minutes after answering security questions incorrectly 2 times. |
| 7.1.20 | On first logon of a newly created user account, the user is required to do a password reset. |
| NEW | Ability to generate a standard security word/date or send to end user (and/or manager). |
|  | **Password Management – Password Automation** |
|  | SailPoint Desktop Password Reset MSI needs to be installed in every users workstations to facilitate desktop password reset in case of account lock-out or forgot password.  If the user forgets password, at the time of logging in to desktop, under the Password field, Forgot Password link is what the user needs to click. Once it is clicked SailPoint application will launch to capture password reset question-answers and based on the user’s input it will enable user to reset the desktop password. |

**Workflow\Provisioning Requirements:**

Access requests require 2 level of approval: HR Manager and Application Owner.

|  |  |
| --- | --- |
|  | **Resource Provisioning – Workflow & Automation** |
|  | Access request workflow status can be checked through the Access Request review page in IIQ. This page will only be available to the IIQ System Admins. |
|  | Approver will require to authenticate first to login to IIQ and then he/she can access the inbox and perform the workflow activity. |
|  | IIQ will be configured to trigger email notifications after various task completions, such as aggregation, refresh identities etc. |
|  | Access request feature of the LCM module IIQ will be enabled and managers or System Admins or HelpDesk persons will be able to raise access request which will in turn kick off the LCM Provisioning workflow. |
|  | Events need to be defined to for specific identity attribute change, so that, once that attribute gets updated IIQ will kick off dedicated workflow to perform required tasks. |
|  | Events need to be created in IIQ to facilitate Automated Account De-activation, by launching specific workflow. Workflow may or may not require approvals. |
|  | Accounts can also be requested to be de-activated by the users having correct rights in IIQ. |
|  | Leaver workflow need to be implemented in IIQ to facilitate the leaver process. Leaver process will occur in two steps –   1. Identity will be inactivated, and all the user accounts will be deactivated 2. After 30 days all the target accounts will be removed from the identity 3. After all the legal process completion for exit, identity will be deleted from the IIQ database |
|  | Leaver workflow will remove the groups from the user’s target account before deleting the account. |
|  | Support removal of user accounts and user ID (person object) from identity management system upon deletion, with notification or pending workflow approval |
|  | Custom Task need to be implemented in IIQ which will find the service accounts having inactive administrator/owner who are marked to be Terminated as well. After finding those service accounts, IIQ will launch workflow for each of them to update their administrator/owner. Workflow will assign secondary owners as primary or it send workitem to the manager of the current owner to select a new owner. |
|  | Native rules to be developed which will take care of the platform-specific entities required along with account provisioning. |
|  | IIQ will be configured to provide assurance of account creation on target system (retry of failed creation, failure reporting mechanism, commit and rollback capabilities) |
| 3.1.12 | “Create” event needs to be configured in IIQ. Then, once the an identity is created in IIQ, immediately the event will be launched to perform the birthright provisioning. |
| 3.1.19 | Reminder, escalation and expiration must be configured in IIQ’s LCM Provisioning workflow.  Reminder will be sent everyday to the owner of the workitem.  Escalation will happen after 10 days of workitem creation, for no-action, and the new owner of the approval will be manager’s manager.  Expiration will occur after 6 days of the escalation. Workitem will completed and the approval will be cancelled automatically. Requester and the requestee will get the notification.  \*\*Escalation must not go to VPs or above. |
| 3.1.20 | At the time of requesting for new access user will be able to add business justification through comment or even he/she can add attachment as well. Comment or the uploaded attachment from the requester will be forwarded to the approver and will be audited as well. |
| 3.1.23 | Managers or any user will be able to enable Out Of Office delegation and will be able to select another user based on the scoped population. |
| 3.1.24 | Managers will have the ability to delegate their approval to another manager and set the expiration date for the delegation. Delegates should be notified of delegation assignments and expirations. |
| 3.1.26 | Provisioning policies will be configured in IIQ where target account name will be generated based on defined rules. |
| 3.1.27 | Attribute change event needs to be defined in IIQ which will capture the company change of an identity and launch appropriate workflow. Workflow will update users’ OU in active directory as well as it will audit the change. |
| 3.1.28 | Attribute change event needs to be defined in IIQ which will capture the change of type of an identity (from employee to contractor and vice versa) and launch the appropriate workflow. Workflow will update users’ OU in active directory as well as it will audit the change. |
|  | Approvals can be routed to workgroups as well as single identity |
| 11.1.11 | Bulk upload and approvals will be enabled in IIQ, including extension of valid account dates. |
| 3.1.29 | Mirroring another users’ access profile, will be enabled in IIQ. |
| 3.1.29 | Mover workflow will change the UPN of the user while migrating it from one OU to another as well as that will be updated in the O365 profile for rejoining. |

**Delegated Administration\Self Service:**

|  |  |
| --- | --- |
|  | **Resource Provisioning – Delegated Administration/employee self service** |
| New | Few entitlements should be provisioned directly without any approval. Each and every entitlement will have a start and end date and the identities will have the entitlements for its duration of access only. |
| 11.1.01 | Self service workflows should be implemented so that users should have access to: • User profile (e.g. security word / date; security questions / answers) • User access management  • Group management for AD • Role owner management for connected systems (e.g., SAP, JDE) • Group ownership management  • Password reset  • Reporting / Workflow Status  • Auxiliary access management ( SAP System accounts, SAP Firefighter ID and SAP Emergency ID, etc.) |
| 11.1.02 | End-users should be able to the check the status for their respective access requests. (i.e. completed or pending). Also, the administrators can check status for access requests generated by end users. |
| 11.1.04 | Requesters, Service Desk Analysts and Administrators will have the ability to cancel requests. |
| 11.1.09 | The system should be interactive and user-friendly.  For this, quick links and forms should be implemented which would trigger a workflow in background. |
| 11.1.10 | Once end users are logged into the systems, they must only see options that they have access to and only be able to perform the operations that they have been explicitly granted permissions. |
|  | Security administrators (e.g., administrators) should be able to raise a ticket in servicenow for capturing of new contractor data. |
|  | Support dynamic delegation to specific identity administrators based on a user’s attribute values (cost center, job code, etc.) |
|  | Administrators should get regular reminders and notification to perform work-flow tasks. |
|  | Users should be able to register themselves for specific services |
| NEW | Administrators will have the ability to reassign the approval task to another manager. And they won’t be able to assign to themselves. |

## Non-Functional Requirements

|  |  |  |
| --- | --- | --- |
| BR- 1.12 |  |  |
| BR- 1.13 |  |  |
| BR-1.16 |  |  |
| BR-1.17 |  |  |

## Availability / Capacity

# Use Cases

This section contains the details of the use cases which have been requested by Altria.

Employee Creation Flow

Pre-conditions:

* The user has not been employed by SMWE.
* The user does not have an account in UltiPro.
* The user does not have an IdentityIQ account.
* The user does not have an account in Active Directory.
* The user does not have an email account (Exchange).
* The onboarding (Joiner) process will be triggered when the recruitment module in UltiPro sends file feed with ‘Pre Employment’ status. (Frequency - Daily once)
* The onboarding (Joiner) process will check status of account and if its Active, then based on matching rules will change status of the ‘Pre Employment’ account to “Active”.
* While sending the user with Active Status, Employee number, Network User Id (samAccountName) also will be sent from Ultipro.
* The user will have a location associated to them in UltiPro.

## Main Success Scenario:

1. Data aggregation of UltiPro file feed with PreEmployment status will bring newly created accounts into IdentityIQ.
2. An identity (cube) will be created in IdentityIQ.
3. The UltiPro attributes populate the IdentityIQ Identity attributes. (TBD based on attributes)
4. A Network ID will be generated by IdentityIQ; User id naming rules: firsttwolettersfirstname, firstletterlastname, twonumericalcharacters
5. User is created in Active Directory and placed in the Domain users OU based on the site code\location attribute.
6. User Account will be set to disabled, until the Start Date
7. Generate a ServiceNow Service Request Ticket (SNOW) to request for a laptop. (Request details – TBD SMWE BA)
8. Network User Id (samAccountName) is sent in a file to be used by HR to fill it in Ultipro.
9. A notification will be sent to Hiring Manager with the User Id, Temporary Password.
10. On start date, account status will change to Active and will be enabled.
11. On the day of joining after I-9 verification, Ultipro fill send another file feed with Active Status and other attributes filled; this information will be updated in IdentityIQ.
12. If User doesn’t join or I-9 verification doesn’t go thru, HR needs to disable the account explicitly in SailPoint; this will trigger user account to be disabled in Active Directory.
13. Mailbox in Office365 will be created when Service Now form (along with any other access required) is filled out by Manager, based on the license level he selects for the user.

**User access request – Onboarding form in ServiceNow**

1. Manager fills out the service now form selecting the application and roles required
2. Upon form submission, depending on the applications selected, approvals need to happen. TBD SMWE BA: Approvals on SailPoint for SailPoint integrated applications vs Approvals on ServiceNow side.
3. SailPoint workflows are launched upon submission
4. For those applications that require further tickets, Service Now form code will create other IT Tickets as per requirement (TBD Service Now Development team)

(below needs to be finalized during Blueprint Review – TBD SMWE BA)

Approvals on SailPoint:

*Pros:*

1. Leverage the workflow capabilities of SailPoint
2. Governance features will be utilized – out of the box, Auditing is available
3. Reports can be generated on all the access changes, approvals etc.
4. Delegation option on approvals can be configured

*Cons:*

1. Users (Managers) may need to understand the SailPoint UI

Approval on ServiceNow:

*Pros:*

1. User experience

*Cons:*

1. Governance feature, reporting etc are not leveraged to its potential and auditing spread across systems.
2. Difficult to correlate access provisioned vs request approvals.

Employee Job \ Department Change Flow

Pre-Conditions:

* Network User Id, Employee Number are present in Ultipro
* User account is in Active status in Ultipro
* The user account is already loaded into SailPoint

## Main Success Scenario:

1. HR updates user account with profile changes in Ultipro
2. Daily file feed includes user updates along with all the attributes.
3. LCM workflow triggered in SailPoint
4. If Job code, Job Title, Department, Location attributes changes, then Manager is notified thru email to recertify users access in SailPoint.

Employee Termination Flow

## Main Success Scenario:

1. Manager\HR logs into SailPoint and disables the user account.
2. HR Sets user account status to Terminate in Ultipro.
3. Daily file feed includes users with Terminate status, Last worked date
4. Leaver workflow triggered in SailPoint
5. De-provision access for integrated applications, Set status to Terminate in Sailpoint, Reset AD Password and send it to Manager
6. If Termination date is > xx (configured date), then delete account in AD and soft delete in SailPoint (set user account status to Deleted and remove other attributes)
7. If Termination date is > xx, delete the O365 account and revoke license.

Contractor Creation Flow

Contractors are directly created in SailPoint.

Contractor Job \ Department Change Flow

Contractor Termination Flow

# Solution Overview

## System Context

## Architectural Overview

The Architecture Overview describes the high-level conceptual elements that are part of the solution and the ways in which they interact. This is represented in the form of an architecture overview diagram and accompanying descriptions.

**Overview Diagram**



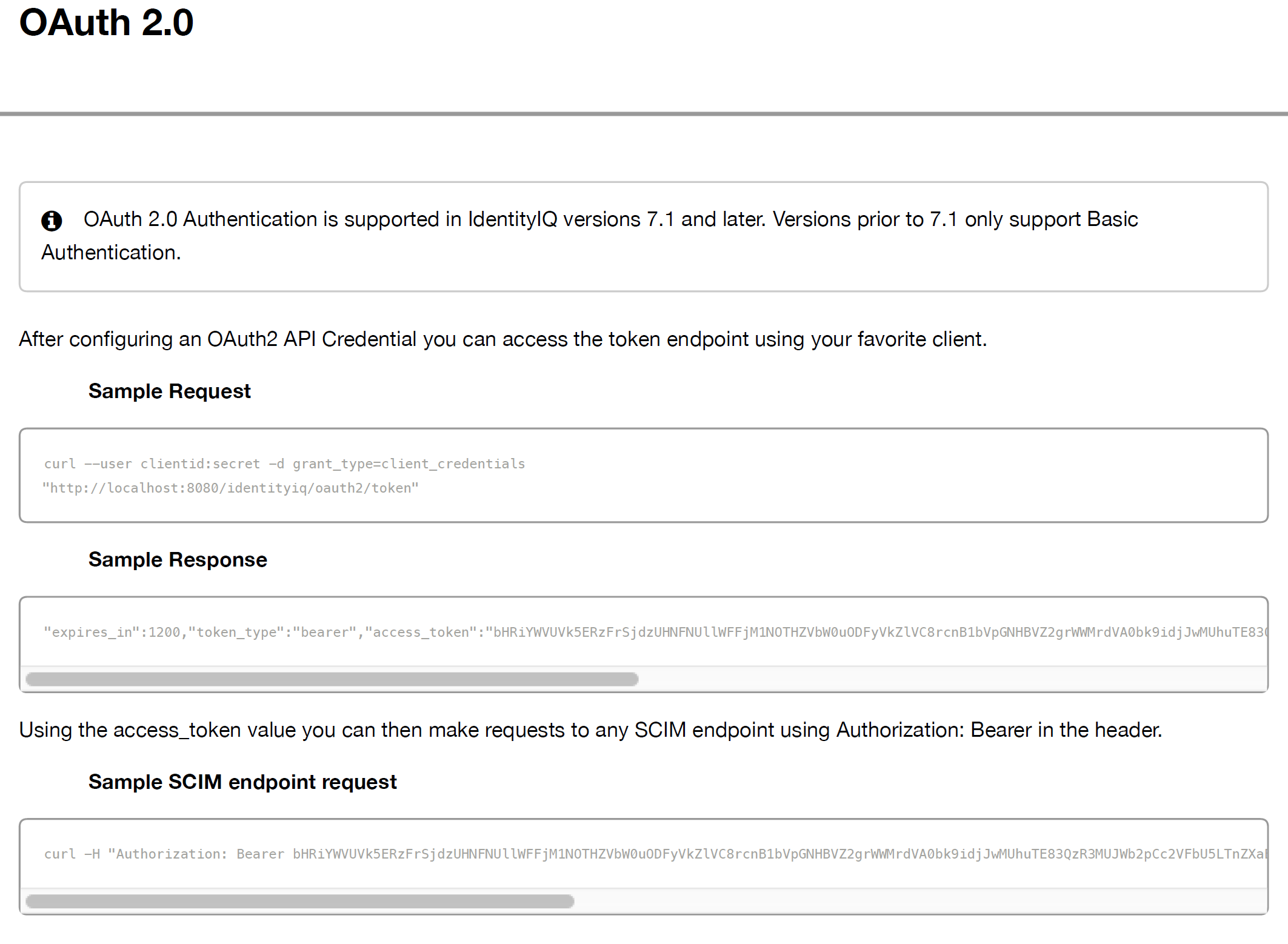
**Authentication:**

This section describes how the Sailpoint web application UI users will be authenticated.

Users will use AD to Authenticate;

Capabilities will be configured based on defined users role (users’ SailPoint role information will be collected by SMWE BA).

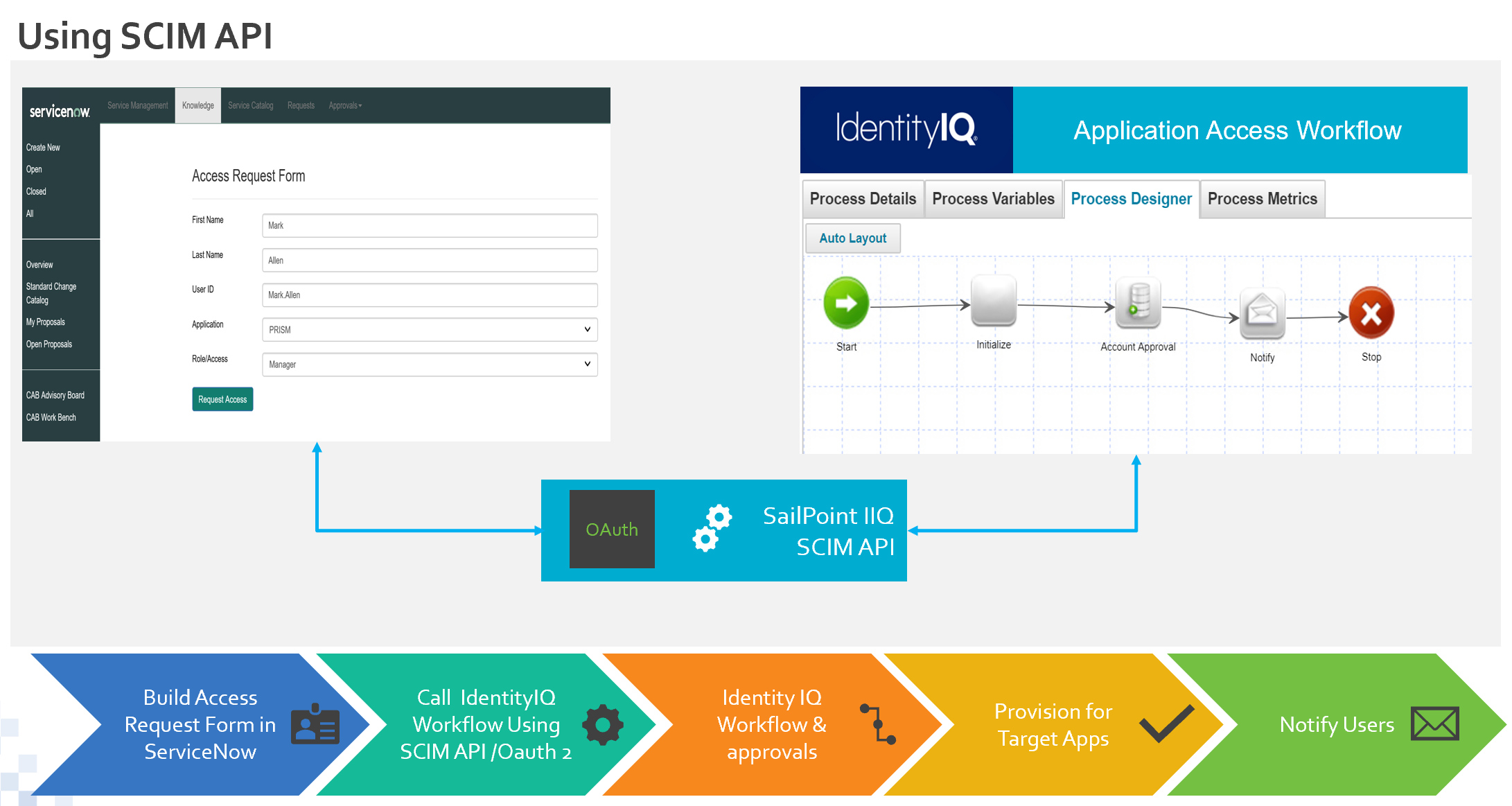
SCIM API Authentication:



**Contractors:**

SailPoint 7.3 and later supports a new plugin type – Contractor plugin. We can leverage this to support the Contractor type.

**Service Now – SailPoint API:**



**Components:**

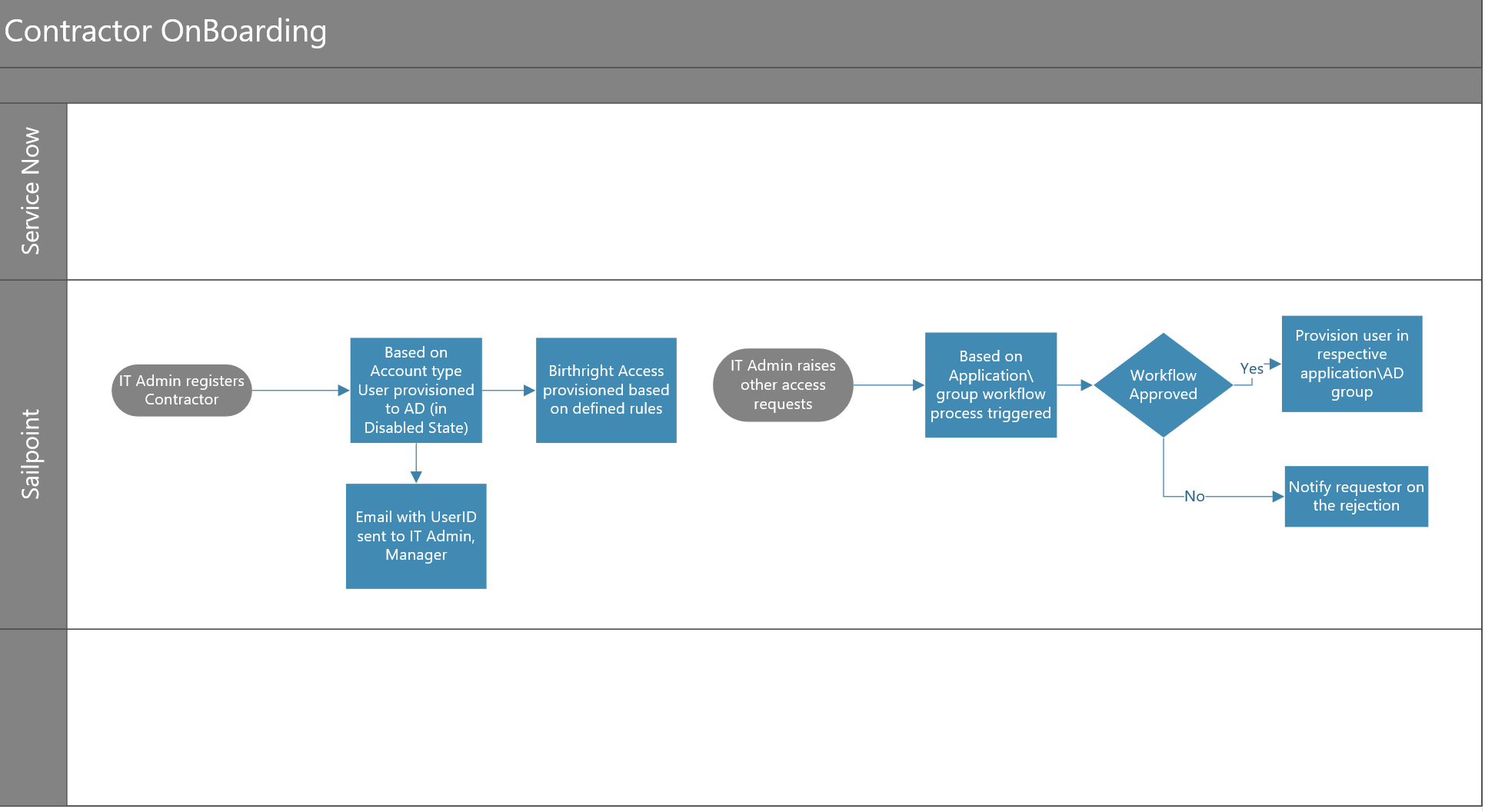
The following table below indicates the architectural components of the solution:

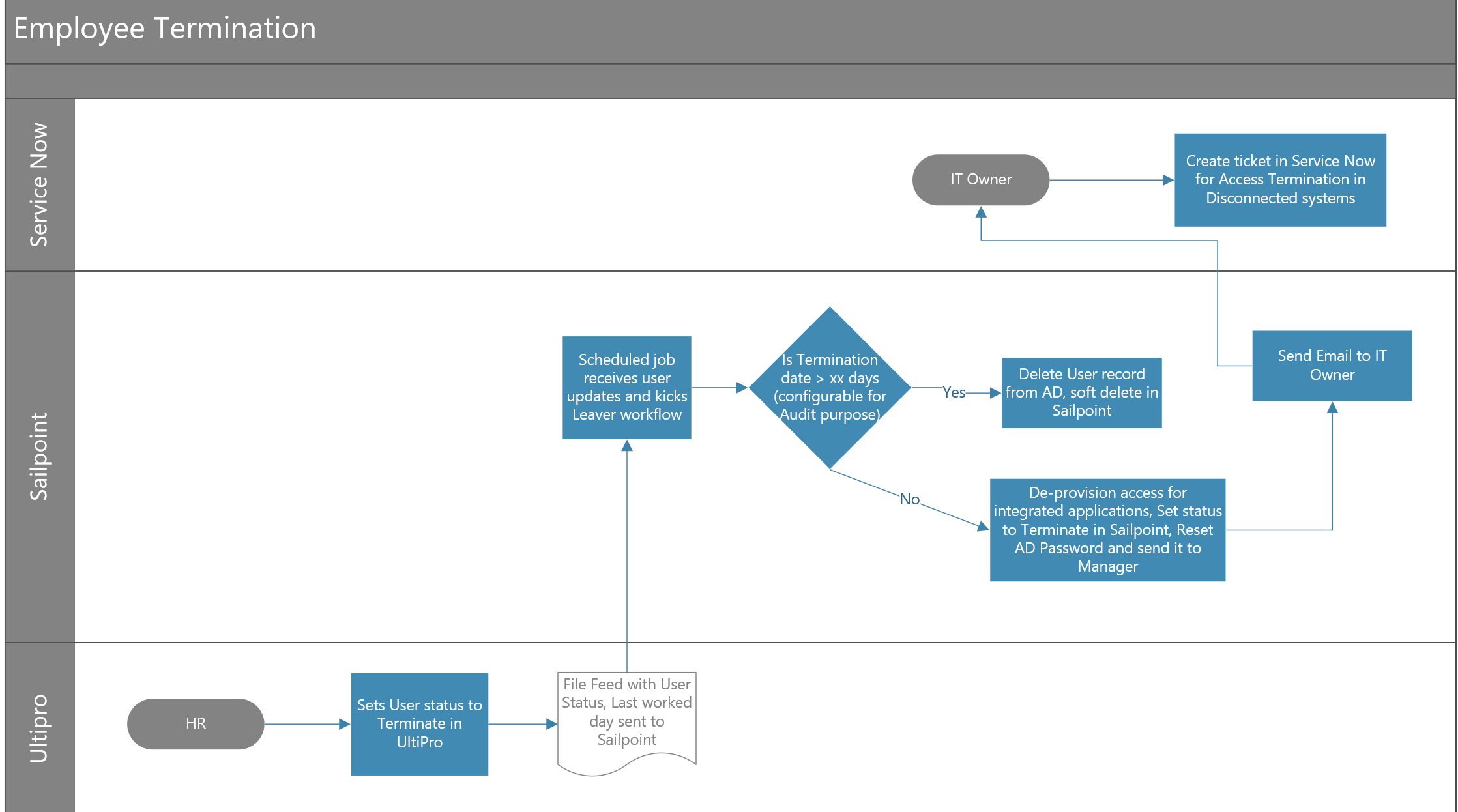
|  |  |  |
| --- | --- | --- |
| **Component** | **Component Owner** | **Description** |
| Application Server |  | TomCat |
| Task Server |  | IIQ Batch Server |
| Database |  | IIQ Sql Server database |
| IQ Service |  | Windows Service to provision in AD |

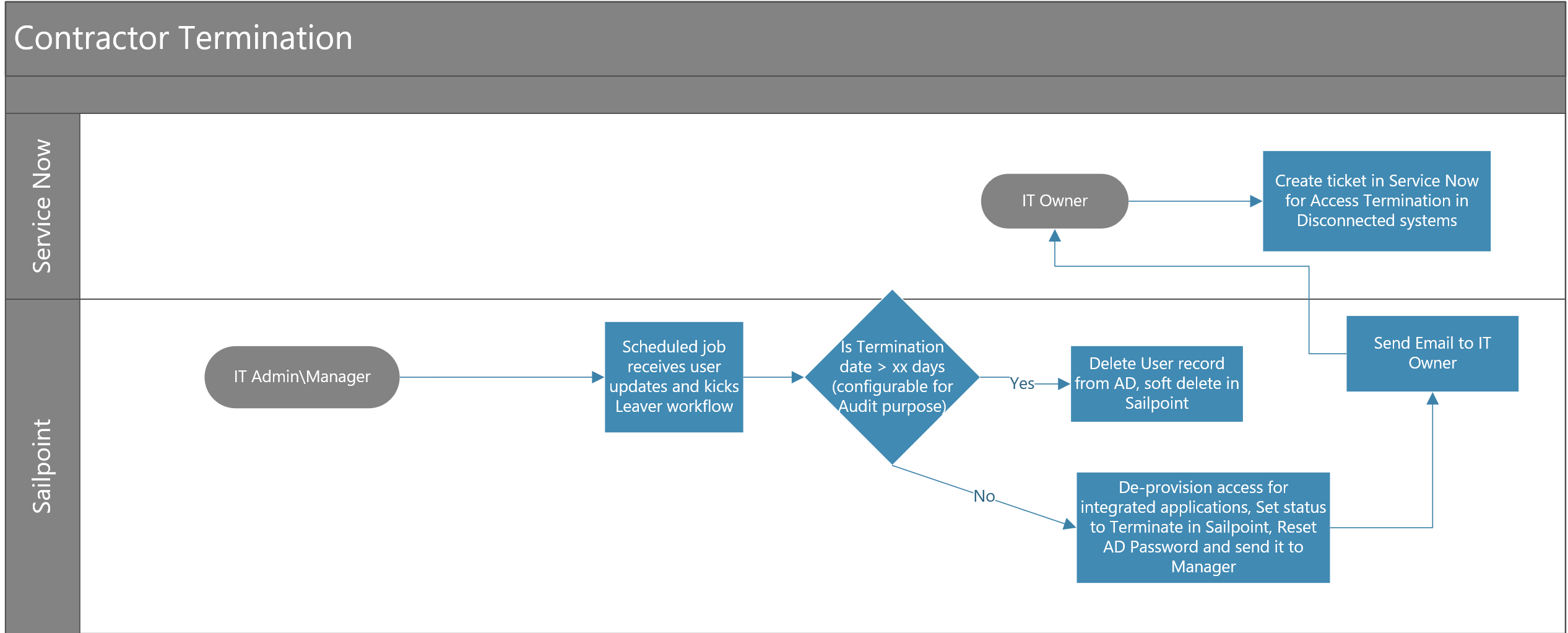
## 

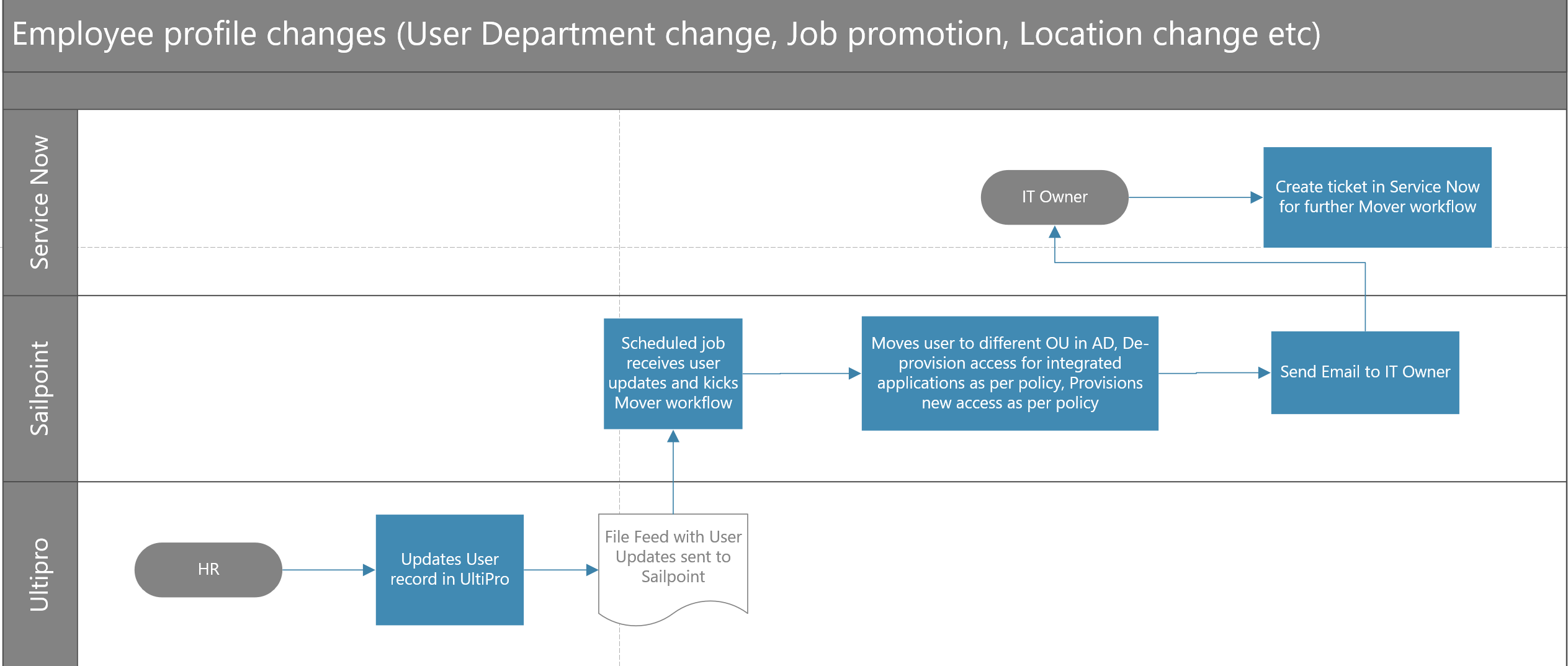
## Information Flows











## Data Types

This section depicts the types of data that will be utilized in the system at a high level.

## Architectural Decisions

## Architectural Decision

| **Architectural Decision ID** | **Subject Area** | **Source**  **(Project or Program)** |
| --- | --- | --- |
| **AD01** |  |  |
| **Issue or Problem** |  | |
| **Architectural Decision** |  | |
| **Assumptions** |  | |
| **Motivation** |  | |

* + 1. **Architectural Decision**

| **Architectural Decision ID** | **Subject Area** | **Source**  **(Project or Program)** |
| --- | --- | --- |
| **AD02** |  |  |
| **Issue or Problem** |  | |
| **Architectural Decision** |  | |
| **Assumptions** |  | |
| **Motivation** |  | |

# Physical Architecture

## Production Environment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Site** | **Device Name** | **IP** | **Model** | **Description** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table: Hardware / Servers Allocated for Production Environments

# Operational Model

## Production and Disaster Recovery

.

## User Access & Authorization

TBD SMWE BA – based on roles needed – like HelpDesk, Manager, User etc.

The following table below shows the user accounts that created.

| **Username** | **User Role** | **Email** |
| --- | --- | --- |
| <email\_address> | SysAdmin | <email\_address> |
| <email\_address> | Admin | <email\_address> |
| <email\_address> | Audit Read Only | <email\_address> |
| <email\_address> | Protect Read Only | <email\_address> |
| <email\_address> | Investigate Read Only | <email\_address> |
| <email\_address> | User | <email\_address> |

## Policies

TBD – SMWE BA (Action item in MoM to Altria\SMWE)

## Reports

|  |  |
| --- | --- |
| **Report** | **Description** |
| Termination Report | All user types including Employees, Contractors |
| Sox Control Report | JDE |
| AD User Group Membership Report | Group membership of Users |
| User based Access Report | All access that a user has (in-scope Apps) |
| Application based Access Report | All users who have access to the particular application (in-scope Apps) |

## Connectivity Diagrams

# Appendix

## Definitions

The following standard definitions are used in this document:

| **Term** | **Details** |
| --- | --- |
|  |  |
|  |  |
|  |  |