|  |  |
| --- | --- |
| **Project Name:** | **AIM 2.0** |
| **Sprint:** | **2** |
| **Task Name:** | **AV2-205 Spike Sample user Onboarding Use Case (Internal)** |

This is spike understanding user process that needs to be followed to onboard an internal user to be able to access AIM 2.0 solution.

The process touch following external systems:

1. JM CRM System
2. OKTA for internal user authentication
3. Azure Subscription to create Tenant for the AIM 2.0 portal (there can be different environments such as PROD, DEV, TEST etc.), identity framework with custom policies for user authorizations.

Diagram

Description automatically generated

## **AV2-222:** **Configure CRM records for internal user**

TSE or designated person will ensure user record/account information is created in CRM system for the AIM 2.0 to refer for user onboarding and login sessions.

The details captured will be verified and will be approved by CRM TSE group.

Following roles will be defined and used for internal users to access AIM 2.0 portal.

* Internal - Technical and field services
* Internal - Account / sales managers
* Internal - Customer services

Once the user information is setup in CRM, an invitation will be sent to the user to sing-up to the portal. (The information submitted by user in front-end during sign-up process will initiate account creation in Azure AD B2C)

Following information will be captured for the user record creation in CRM:

1. User name
2. Email address (with confirm email address process)
3. User role
4. Refinery information
5. Additional company access

Get Role API called to pick role information from CRM system.

Text

Description automatically generated

In case of an internal user getting onboarded and accessing portal sign-up page for first time, the system will divert user for OKTA authentication.

## **AV2-223:** **Setup OKTA authentication for internal user login**

To set up Okta system authentication for internal user, the information needs to be added to OKTA.

OKTA will provide secrete key to be created as policy key in Azure AD B2C for the OKTA access.

(Currently we can utilize the OKTA policy that is being used by Methanol as it is already being shared. We only need to add logic to ensure system can differentiate if user is logging to Methanol, AIM2.0 or any other system)

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

The Azure Tenant custom policy will ensure diversion of internal user to OKTA screen based on the policy criterions and domain information.

The user once enters information to the login screen (Email address), the system will identify if the domain being used by user is registered for internal users or the user should be considered external user. After that the portal will first give a call API to find out information about user role (from CRM) and divert the user to go through OKTA or Azure AD B2C.

Sample call to API that redirects to OKTA authentication:

Graphical user interface, text, application, email

Description automatically generated

On successful authentication of user, system then checks for user authorization from CRM system. If the user record does not exist in CRM, the user will be displayed error message indicating they need to contact Administrator to set up their record in CRM system.

Graphical user interface

Description automatically generated with medium confidence

## **AV2-224:** **Master: CRM - confirm if separate access policies for internal users are required**

The user account needs to be setup in CRM and no other specific policy is required to be setup.

The roles will drive the decision making that will enable the portal to display landing page for the user.

The user information from CRM will be fetched by APIs such as one mentioned in above point (to fetch account information and roles data).

**AV2-225: Setup first time login UI/UX flow**

Use journey for the internal user being onboarded for the first time will be as given below:

1. The user account will be created in CRM system by TSE and an invitation will be sent for signing up to AIM 2.0 portal
2. The user will be presented with user login screen.

Graphical user interface, application, Teams

Description automatically generated

User will click on the ‘Signup’ button to enter information.

1. Set up related to Tenant and custom policies is completed in the Azure AD B2C and available for utilization. The custom policies are used to check if the email provided by user is external or internal. Based on this, the user will be directed to OKTA or Azure AD.

Text

Description automatically generated

Text

Description automatically generated

Based on the information the internal user will then be displayed OKTA authentication screen.

Graphical user interface, application

Description automatically generated

1. In case if the user email is not already registered with the AIM system (no account setup done in CRM), the user will be displayed following message:

Graphical user interface

Description automatically generated with medium confidence

1. If the user record is created by TSE in CRM. OKTA authentication additional call to API will be made to check user role and in addition the user will be presented with screen to submit information to create Azure AD record.

Graphical user interface, text, application

Description automatically generated

If user wants to register for the portal access

Graphical user interface, text

Description automatically generated

User information should be present in CRM. The information taken in screen above will be used to create user in Azure AD.

Here onwards, Azure AD will always cross check with CRM for user record/information existence.

If the user is internal user and has not been registered in CRM, the OKTA screen will be shown to them.

Graphical user interface, application, Teams

Description automatically generated

If the user is not setup in CRM or no site is assigned to user, the they will get following screen:

Graphical user interface, application, Teams

Description automatically generated

User Authentication and Authorization

Graphical user interface, text, application

Description automatically generated

1. On successful signup and login, the user will be displayed login page based on role and what is accessible for the user.

**AV2-226: Create API to fetch User Role**

Graphical user interface, application

Description automatically generated

JWT token will indicate role and other information for the user. It will also indicate if user has access to any particular site related information. The site id(s) will be in encrypted format and business validation will be able to retrieve site id from the information to check if valid site id is provided for access.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

**AV2-227: Create data structure for first time user login**

Following data structures are created and operated in CRM & AIM 2.0 locally to facilitate operations:

1. User information table in CRM

Graphical user interface

Description automatically generated with medium confidence

1. Roles information in CRM

Text

Description automatically generated Text

Description automatically generated with medium confidence

1. Customer and sites information.

**AV2-228: APIs integration with UI/UX for User Onboarding functionality implementation**

Various APIs such as:

Account information fetch from CRM

Roles information fetch from CRM

Customer information fetch from CRM

Sites information fetch from CRM

Loaders information fetch from CRM

Loader data fetch

Alerts/Events fetch

Etc. will be developed to integrate them with front-end.

Every API will satisfy criteria to provide maximum security to the data being used, screen display based on user authorization and authentication and optimization for the given functionality.