|  |  |
| --- | --- |
| **Project Name:** | **AIM 2.0** |
| **Sprint:** | **2** |
| **Task Name:** | **AV2-206 Spike Sample user Onboarding Use Case (External)** |

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

The process touch following external systems:

1. JM CRM System
2. Azure AD B2C for external 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

## **AV2-229:** **Configure CRM records for external 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 external users to access AIM 2.0 portal.

* External User

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 external user getting onboarded and accessing portal sign-up page for first time, the system will divert user for Azure AD B2C authentication.

**AV2-231: Create User Roles in CRM and assign**

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.

(Other than the above mentioned information to be created in CRM, roles based access can be defined in Azure AD B2C. To implement role-based access control ( RBAC) for an Application and for an API (hosted in API Management) in Azure AD and B2C, we need to add custom roles into the Azure AD/B2C application manifest file. The application manifest contains a definition of all the attributes of an application object in the Microsoft identity)

## **AV2-232:** **Configure external user in Azure AD B2C for authentication**

To set up Azure AD B2C authentication for external user, either the user record should be created in AD or the system flow will generate the record at run time during sign up process.

If a user is setup in CRM and AD has no record for the same, user will be displayed following screen during the sign up process:

Graphical user interface, text

Description automatically generated

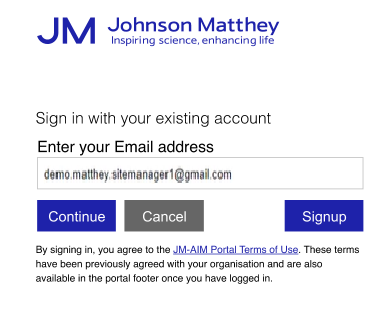
The information taken in screen above will be used to create user in Azure AD.

(Process of setting up portal for AD B2C Authentication is provided in separate user story AV2-41 Understanding the authentication API that can be used for Methanol. This document will cover creation of policies, creation of user flows etc. steps)

**AV2-233: Develop UI/UX flow for first time user login (External User Onboarding)**

Use journey for the external 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.



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 external user will then be displayed Azure AD B2C authentication screen for creation of record in AD.

Graphical user interface, text

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. User onboarding for external user will begin with Azure AD B2C authentication screen requesting for information for record/account creation. Additional call to CRM API will be made to check user role.
2. On successful signup and login, the user will be displayed login page based on role and what is accessible for the user.

**AV2-234: API Development for Token Generation Call**

User opens AIM 2.0 portal page to access the dashboards.

The system calls for domain identification based on email address provided. As the user is external, the system will invoke Azure AD B2C authentication. An API call will be generated to initiate this process.

API call for Token generation is not required to be made explicitly. It will happen internally based on setup done in Azure B2C.

Example of the calls flow:

A screenshot of a computer

Description automatically generated

Once the user enters password to the screen, an API call such as given in example below will be made:

<https://b2ctntdeveulevoshared001.b2clogin.com/b2ctntdeveulevoshared001.onmicrosoft.com/B2C_1A_MethanolDevsignup_signin/SelfAsserted?tx=StateProperties=eyJUSUQiOiI5ZjA3OGEyMy01MjVhLTRlM2EtYTY4Yi0zYThkNThhMGJiZGUifQ&p=B2C_1A_MethanolDevsignup_signin>

with payload

request\_type=RESPONSE&signInName=demo.matthey.sitemanager1%40gmail.com&password=Password!1

Once the API returns an output, API call to generate Token will be made:

<https://b2ctntdeveulevoshared001.b2clogin.com/b2ctntdeveulevoshared001.onmicrosoft.com/b2c_1a_methanoldevsignup_signin/oauth2/v2.0/token>

with following payload:

client\_id: faf5c562-7e57-491f-9dd0-f819d3176995

redirect\_uri: https://dev-levo.matthey.com/methanol

scope: openid profile offline\_access

code: eyJraWQiOiJCem9mNExaVm1Ock1lOTFEWUtXMGJOTnVfVTFvYmdjR0NHY3lUZTF6MWlBIiwidmVyIjoiMS4wIiwiemlwIjoiRGVmbGF0ZSIsInNlciI6IjEuMCJ9.cLR9wS2A2IwN0cTltGrlfFM1bLsB4G46WIlUd8EopM-RhyqA34JAHbrczkzueWH9vnzQ1upPrgkdlWGF1nWrqvVZ09TNBQcdU31VPxTDaQQW0kJ7Y6fvfDHGWmtVj6TzNlNV7F3MDJrJOJJO\_MQzV4z-DUGeHPCHaa6VXpRESzIRmkVlf3TDMZqs9-hxETOwCkH\_q0oc2srDXgX5r31HBCPtP92XkIdBmsWdu2T5mdDen3dK0FN3NDQyI4V5LqYIkKHVvnbMvCRrHEcotwa8jP1x5Amg3C8sJBpWNjoMjTHjbQ1VJmsqst0IFY7i6XS0xS\_KuOP5nb2PAX8\_WPOztg.D6ib688bP\_uBOkiM.japgEtyfAPIjHivwcjl-nOK0LHuE1bfbmZg6QqYVPCxIqkakPMUkP2bQkpVCJOTX4ztdHRgkreYnpDWhZoLIa3Mzlpy-JJqsNU8JqpRqP-P6g292ZOyLSyLa32rI0qnfV9ugW1QMMBCD3aP8o9k5Ts2DrU5RlyQ4zptUg9FMAP3LB64DldQsmDpDq5psr383a1x2\_2x5h50hfs5hEkwf\_gMiZk2eyKAift3rkzpRvkpbcTXdKeffTaicoJGK4B\_0HUGoL4B5uI2067HvZMY1zH8fa71SzsvO1M6IKzgNUpw\_WY2Q3-Ch-M34YJvhywzboQAiOllEelX2SwsztiHGL5GWVKdZpv5sdVky1b1jVlUo3kOkh1rIm8GSINPBl0VAID-bqxk2w3WMsww4YhLD1DIYTh\_iAUp75gbWmUaISfEOKgksoPbWqm7roMiLAqQWN48wF9PFnvmdrHhCqsSnnb\_awV6FsnoksDyPTmDml4w7sWX55CrmQz\_\_8xFy7Le35DYMThtXjx87BFaa02-JodV7yxeEMjLkh0k\_liDR2SVZ6moUHtpEcUaRmgPwtimVxQTH5v-N0ORbwRaCgI0UHZVKO9MkADncrVzSwtbylXv5MSVOMdXu9dQyQNSKZ9pAtwTHT2Y7YtKNaJ8UyxZUckZD\_jHdFJcnqv1Xfw0l4uFliNiNillue0Gdwkv76cgxBU-w8MnaqOTduZ7SfeHXVsc-GXnb\_QdY16XxWyeXiZaM5QBuRRxQVtVJlqAApP0-iBL57m0xppLuz\_81QPMaRJCbWGOSicV1tx-rGjSe-UxmKuHmUmzicuUi18TrjI3QWPUOni9OE8NE0mjKJ\_xGaPFXDSerbX1FL\_qSOejzlEYN-9D7GyFnrK3dZFkKD6Uo40Hn9mn4HFaufUwWQiMr6MBxtsBnsvxtvYb7-LGYAS6Tx89BRWG3uCfLluWZcwAp2dInXBAlXvtCsMIVMa1b1ZTzPIBg-WioDyFqMC2wNAouC-mTCOkaOWYTgCJN9Gw1JDK9akuYAuN-yOu9ajAg\_fdm6mewBTjt25v-Ad5ZMYn9Yzw0D3Aby137MTfD7oOMI-Pryp2L-5MJf6wYG4ydXlicNg\_Qb4\_pjDld6pKoGKweZSnEnPY\_wEZS-7Tkziy84wD86AwQsUu9EsyAK6Am\_95rh9vfzdfEcv2OFj9x4RFQ-2bMtgMcupISfwLp9U007DGGd30Spp2HLJAQOv5rZ28FF8nk4v2JVdJiZ-dahJD6IHn5Z8oS0XiQzOJrXoXy2klhUpSTFvQ\_fsp56MYNAsgdGHPgikxYD23LkPm4Q8O5cDA9Z2zag6AWiq\_IbmgyXsMhU-y1XSRFR07TU3TbCMvsE4GFHDAcZnh8SG3NTogjk1og-CDJc8-ddIiFmQ8hQL2g65eZi-bw\_UnyzDPRN3UeTea82bxLYcsNaX2m5XxKhd2SukKM6TD7Pa9FdQJEt1xInRezR4LvCSUqWqnZ3IJqBTuUXuvt55IQZkkJSn8RzyD1tX19lxdahD8Q8mIFMytI0Xz97wj0604JCNpIMZTB68GCh-psv2FRl9IfQDpsVV8oOSx9r6ugW33FfH\_jsQf8m\_Q3Vjb0pglLn3tkBvqc-v2qTlRnSzXKVd-fARQgWg5m4E9veqJZHiPL8dwoz\_dgpscI3I3jzeU7G9V0Ljha0nmoYUfOyAkgWjhVydBfuXuXyh6ErJ8fMZVF7BvfeefAbUsKzzYNpB2CcyTL8Av5ShIgJNLvWqufJmZxKSnqlTxkQZTohiIW6EKW4zV9xpVk\_uJl07-5YxMm0P2daDuIMekX2Qzt9Udf2ssBa-Prwkn\_Q1\_EfJuygpD4gDMRSLu4UJ5I8KadTKjIsMNHvzBA2U7SV32pd1H1FHgZWTdSXam2wLp8PWo.hVSFDlygJFiiADNLuwHQVw

x-client-SKU: msal.js.browser

x-client-VER: 2.15.0

x-client-OS:

x-client-CPU:

x-ms-lib-capability: retry-after, h429

x-client-current-telemetry: 5|865,0,,,|,

x-client-last-telemetry: 5|0|||0,0

code\_verifier: ihYFdIOl1zQDg6jiGiG-phzCJXGda7ggDsgy0P5cxuE

grant\_type: authorization\_code

client\_info: 1

client-request-id: be411851-a900-4a46-b02d-9ceb23270a2e

X-AnchorMailbox: Oid:e4951ac7-b06b-425b-ba09-a74ddeaee44b-b2c\_1a\_methanoldevsignup\_signin@57dd950a-e033-47e9-a77f-717d580ca48f

This API will return a Token, which is used in all other calls after this and redirection will happen on desired URL (for example - dev-levo.matthey.com/methanol)

**Example -------**

{"id\_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ik8yZ1pwekhsYzFhbk45LWdHLTUyUHhWRFN4U3VKbTFSWXJtUHVhLURDLTgifQ..Agj5tjUf34vB-Gk1YjhmK-ezGqF0DUvP6snsvLCULSdJ-gjFBBaucYpVoXhWzDudYqiOBu1N0Ck14FUs0o6BZhMmWTip1zkDAwxmRLb3Rv-QQHkzgMbKFVh\_tG6PMxwMSjWSO0JXLpmYq0IVseseV7ccg-1zZzomBy2-7Box5LdmQUOK2QMhkGH2FOpJd14nTLm5HZ62jwMXgV0YnXJb4kC253v3Ao\_04xeFhx74c2zbBBu6chMxqB63a9ewKp4sJmBF728UBaAiKxeP4Eqk899N6kghmYQ27nkCDj-kAsBhgsbqXGbWeW\_SEqfw-FTSelqPwoTUZAx9FuCe9w69Aw","token\_type":"Bearer","not\_before":1642681773,"client\_info":"eyJ1aWQiOiJlNDk1MWFjNy1iMDZiLTQyNWItYmEwOS1hNzRkZGVhZWU0NGItYjJjXzFhX21ldGhhbm9sZGV2c2lnbnVwX3NpZ25pbiIsInV0aWQiOiI1N2RkOTUwYS1lMDMzLTQ3ZTktYTc3Zi03MTdkNTgwY2E0OGYifQ","scope":"","refresh\_token":"eyJraWQiOiJCem9mNExaVm1Ock1lOTFEWUtXMGJOTnVfVTFvYmdjR0NHY3lUZTF6MWlBIiwidmVyIjoiMS4wIiwiemlwIjoiRGVmbGF0ZSIsInNlciI6IjEuMCJ9.p1\_jSGz4O9gPKhoRcOslrG6cqyZ3EjdQaDuhN4RtVvekMMRUieROf31RNA1C3oKuoletSiY4Jl7HS5ZsRTF9ebqYhi2ZiOxcNU7oVjz8qjkaPv5x1Yu6lkU02\_9vnoZTEgm3LXjB9gTLMqB9qS6Yazwqd3O93SByc3u3r20Wdp3sK\_z-5-bCPDcQA0qGQgia5YICqccoXJh9Wc9Y5jT4INZxV3wEzgWkS6c8cABZ8KKC9KasnxJcIytXWhArkpnMP5wcVuO5kqlzv1ElcbiCseWaZpHArBgMe80smHZQLGRQ0XjriIlSotGg7y8ZUIRTIcl7-wj2yXbD-8GaNFtoqQ.NETKPKLkZJdeEoXS.IFlFlkFNIdAUb1YDciLfkAqgYKfwsTtv\_YOeX0y5YlswhrtR2WAk2HMWWMK7nuljiUZJ5dzCs2RdK-XLfDkGpqutF2V3Tjx7eoABqJ2ibfxUyMOYmZNNTfNNiC8seLNQ46jf7kd7gbNAz0qjnV58Mqi1LEc0nO-G8m3nfnb20phR5fPqAdq0XmG6hl8nxA8DXpMy1xDdrsrzGzl7\_TnCJ9K\_ocuI7pQ1XvywHxqA2lZthFFGhtKyvSHTPkR2pT6xt4BVH\_E9InphyCypDVe\_-naOIJ-OAkVMZ3inhV1vLXvrxUfIpTpcgU71aR0RJ4OacWseXIIbyDFp4quC19UStgaK0Y3506gJXNglBKGjt1mXQm3W6D4-XN-rj2N6tizeYBdYCJK0b7qdtpi5mevu4wFD9DrjtQ9D1F959edDXIxAgNRN3YxBSeAR5d4kq3Dy\_Bn03yX5k5AWmlhwWKFs87K0ZFA\_nl7Rkt9KPhNRqghJVJ1Lv5HyNA3UlzyYs6a4Lkd9b\_gYFowNXkrYKSBsjZzSEUM\_OCdmrc8AAQsRpjc-wc0wccgAVKzwjpWKxT68caE5yvufyt9k\_rn0eNvJ51hUX48wH1tYHFScMsLp4B6F92lONg\_qm-0Bfv0d9GzLTIXFBAG9aKg8yh8Ciuc6zdh9JzC46Y3qGDOeaH\_rwJXhkfWSBWRVBuPzmC9AxNkOW7Gi-tc2AnKl1Od6yccIlNVPY3L31qQwLMUR-oc7\_aOomVD7aB1LalAMBwtZBgSVibG5G\_hNFSoOC2BvkF3mytn6BbXilpvnKj2X3DFmYEnvVKXAsz2IuzyPNs38o9euzr8vBZZNGraZRz92ySItB1iYO73tjudUq4TsJ\_u3mF3o8I0yUOgEK5aOfNlJ-jLW\_ockkPhDqrXAKHnj4msP4gv7YweSGPaOQmiMC5kItYdpB\_szQeG\_D5ZdMvS6WY3j5cdyJc8CpNJpjvys\_0fyjTr16acROd3RVCAF9Dq5SrgeFBKXijqQ1EYtPOudEWtPTtK0wNrLmrGCYr5RycvXAy60i49dKSwB57sB8Au3AMJJ3TegchkkhWIojvPKDhDcXt\_6RJbV68vkbbL48EBRnwQtaKQbcWq2QdzWMT23PVmJVkIOugcco9AhdXoo\_PmEQahmlXzh8NMJnBy6nqW4yaMpegghlLpifTzB996VycG1j-otTlFNdy3PkYO9tuFWTUGW4BHHt4WHAb-ZZ4rsAr5-JzrvnY6PdKsy57VX8SHj2rFcreUg45tq1jTMcWhsUd\_js3ZcseFfoueS5bHFYzlN7dkN33U6pHuUQq7RbIkfl72eAhGMXiK3oOfVj2CcMEgjo\_6YeukZIeaPMqQcXr7ru4JgkWBnzndjQJrZl9cgOT4q8Lseqp0lIvBK-h2R0WFBgacQ3hlIZ7gI6jaOgWf23HCJI93KpQO5TFgQvvoXymwk9gasGoogQcuiL3letM1WjkHIJd5uk6Qj1M5CDL6\_6H\_hlkvCfZekvtIJ6myDf185NkdZLM5h\_HbMOKg3zMH5Wb88JyCCWxHFb0Y4ZfQNXdYo6hFf3h17exHAJMIbkTqci5fzWUcQi9jMl0UNbwwYkj3ZKz8iNOhS31Ri456\_wBq2jwMjTv7mJ\_lOyFXu7a6O7BF8e0YjY-qMOYi6cUyy9M0Ect\_z28B4FjzTBCxyCuq6DSgp1pdHn7NZLNPf15ddWgCfXxki3Sow5STqNgGsCORRfMfE1hhG1xX0Zew42UjFIjYSs-SRQLCDN7y8ArbnLmvyrlSgpxFxxo2ehdRfct2H22JojPs2N-XiovaruoXxSrsqcu1ys\_za.0Lg1GI9dt8aruVIbV71utw","refresh\_token\_expires\_in":86400}

**AV2-235: API Development for Azure AD B2C Authentication**

For external user, the automatic validation will happen as AD B2C facilitates the same. The Token will be transferred to calls internally which will be authenticated at Azure’s API Management Services end for every call based on policy setup as given below:

Graphical user interface, application

Description automatically generated with medium confidence

**AV2-236: API development 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

## **AV2-237:** **UI/UX, API Integration for external user onboarding**

This point is covered across the different subtasks detailed above.

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

This point is covered in AV2-234 and AV2-236