How to configure the Microsoft Azure feature in SOLABS QM 10 – Azure side

CREQ NUMBER:	**CREQ-** _____
INSTANCE	INTERNAL: ☐ QUALIF: ☐ TEST: ☐ VALIDATION: ☐ PRODUCTION: ☐
BACKUP REQUIRED: YES: ☐ NO: ☒	SOLABS DB: ☐ SOLABS QM APP FOLDER: ☐
CLIENT:	

EXECUTED BY:							
REVIEWED BY:							
	NAME		SIGNATURE		INITIALS		DATE

1. INTRODUCTION

PURPOSE OF THIS DOCUMENT:

Define the steps required to configure an Azure directory in order to enable a SOLABS QM instance to connect to it.

OBJECTIVE	Configure the Azure directory so SOLABS QM 10 can be connected to it.
ASSUMPTIONS	THE CLIENT HAS MICROSOFT AZURE (WITH THE APPROPRIATE LICENSE TO MANAGE USERS AND APPS) AND SOLABS QM DEPLOYED.
TYPE OF ACCESS REQUIRED	Administrative rights in the Azure administration console.
APPLICABLE TO THE FOLLOWING OPERATING SYSTEMS	N/A
SYSTEM DOWNTIME REQUIRED	N/A
ESTIMATED EXECUTION TIME	45 minutes
ROLL-BACK PROCEDURE	Revert configuration
Applicable SOLABS QM version	N/A

2. EXECUTION

Azure application configuration for Validation instance:

1. ☐ Go to the Azure Portal: https://portal.azure.com/
2. ☐ Select **Azure Active Directory.**
3. ☐ Under **Manage**, click on **App Registrations.**
4. ☐ Click on **+ New registration.**
5. ☐ Enter the desired Name (based on the type of instance to which this app will be used for) and Supported account type.
6. ☐ Click **Register.**
7. ☐ Take note of the **Application (client) ID** and the **Directory (tenant) ID**, you will need to provide it to SOLABS.
8. ☐ Click on **Authentication.**
9. ☐ Under the Advanced setting section, set **Allow public client flows** to **Yes.**
10. ☐ Click on **API permissions.**
11. ☐ Click **+ Add a permission** > **Microsoft Graph** > **Application permissions.**
12. ☐ Search **User.Read.all** and choose **User.Read.all – Read all users full profiles.**
13. ☐ Click **Add permissions.**
14. ☐ Click on **Grant admin consent.**
15. ☐ Click on **Certificates & secrets.**
16. ☐ Click **+ New client secret.**
17. ☐ Give it a description and choose its expiration, then click **Add.**

18. ☐ Take note of the value in the list (it will not be shown again afterward), you will need to provide it to SOLABS.

Optional

If users are to access the app from the Azure portal directly, perform the following steps:

19. ☐ Click on **Branding.**
20. ☐ In the Home page URL, enter the URL of the SOLABS QM Instance. (Ex.: https://clientX.solabs.com/QM-VAL)
21. ☐ Upload the SOLABS QM app logo (provided on demand by SOLABS), for the instance to which this app relates, through the "Upload New Logo" field.

Azure application configuration for Production instance:

22. ☐ Repeat step 1 to 21 but use a different name at step 5 to better indicate that this is for the Production environment.

MFA Bypass

Notes:

- *This is **required** if MFA is enabled for users of the Azure Active Directory that will be accessing SOLABS QM.*
- *Perform only one of the two configurations (Trusted IPs or Conditional Access).*
- *These are minimal guidelines which could be implemented differently based on the customer's own Azure configuration/knowledge.*

Configuring Trusted IP:

23. ☐ Go to the Azure Portal: https://portal.azure.com/
24. ☐ Select **Azure Active Directory.**
25. ☐ Select **Security.**
26. ☐ Select **Named locations.**
27. ☐ Click on **Configure MFA trusted IPs**
28. ☐ Under **trusted ips** check the box next to **Skip multi-factor authentication for requests from federated users on my intranet**.
29. ☐ In the text area under **Skip multi-factor authentication for requests from following range of IP address subnet**, enter the IP address that will be provided by SOLABS.
30. ☐ Click **save.**

OR

Conditional Access:

31. ☐ Go to the Azure Portal: https://portal.azure.com/
32. ☐ Select **Azure Active Directory.**
33. ☐ Select **Security.**
34. ☐ Select **Conditional Access**

35. ☐ Click **+ New policy.**
36. ☐ Enter the desired name for this policy (ex.: *SOLABS QM MFA Bypass*).
37. ☐ Under Assignments, select **Users and groups.**
38. ☐ Under **Include**, select **All users.**
39. ☐ Under Assignments, select **Cloud apps or actions.**
40. ☐ Under **Include**, click **Select apps** and select both SOLABS QM Apps (Val and Prod).
41. ☐ Click **Select.**
42. ☐ Under Assignments, select **Conditions.**
43. ☐ Select **Client apps.**
44. ☐ Under **Configure**, click **Yes** and make sure that only **Browser** is checked.
45. ☐ Click **Done.**
46. ☐ Under **Access controls**, select **Session.**
47. ☐ Check **Sign-in frequency.**
48. ☐ Enter **1** and select **Hours**.
49. ☐ Click **Select.**
50. ☐ Under **Enable policy**, click **On**.
51. ☐ Click **Save.**

Create a SAML application

Notes:
The following section is optional and should be used done only when SAML needs be enabled.

52. ☐ Using the values below, follow the guidelines from Microsoft to enable SAML on applications registered through the "App Registrations Experience".

For the Validation instance:

Values to set:
- Identifier (Entity ID): solabsqm_val
- Reply URL: [ENTER SOLABS QM10 VAL URL HERE]
- Sign-on URL: [ENTER SOLABS QM10 VAL URL HERE]
- Name Identifier Value: user.principalname

Value to retrieve and send to SOLABS:
- SAML Signing Certificate (Raw)
- Login URL

For the Production instance:

Values to set:
- Identifier (Entity ID): solabsqm
- Reply URL: [ENTER SOLABS QM10 PROD URL HERE]

- Sign-on URL: [ENTER SOLABS QM10 PROD URL HERE]
- Name Identifier Value: user.principalname

Value to retrieve and send to SOLABS:

- SAML Signing Certificate (Raw)
- Login URL

Send information to SOLABS

53. ☐ Fill the form
54. ☐ Send the form to SOLABS along with the certificates that were created on step 20.

3. COMMENTS