9160 boul. Leduc
Suite 410
Brossard, Quebec
J4Y 0E3, Canada
1.877.322.1368

www.solabs.com

HOW TO CONFIGURE AZURE FOR INTERACTION WITH SOLABS QM 10

Status: Approved & Effective
Effective Date: 2024-06-14
Control Number: TINS000077
Version: 12.0

DOCUMENT INFORMATION TABLE

Name	How to configure Azure for interaction with SOLABS QM 10
Document Type	Technical Instructions
Description	Technical instructions on how to configure MS Azure in order to interact with SOLABS QM.
Control Number	TINS000077
Version (Internal Version)	12.0 (12.0)
Effective Date	2024-06-14
Next Review Date	N/A
Reason for Change	Add step to make it clear that users or groups will have to be selected to allow them to use the SSO App. Also, some reformatting/typo corrections.
Additional Information	*< empty >*
Legacy Number	*< empty >*
Area	*< empty >*
ISO Reference	null
Originator (Author)	pdemers@solabs.com (Pascal Demers)
Document Owner	FCT_Head of Engineering
Document Coordinator	N/A
Unique ID	f748b19d-4ee8-4061-ade6-aa6f1d4afb37

EFFECTIVE

RELATED ITEMS

N/A

© SOLABS QM

9160 boul. Leduc
Suite 410
Brossard, Quebec
J4Y 0E3, Canada
1.877.322.1368

www.solabs.com

HOW TO CONFIGURE AZURE FOR INTERACTION WITH SOLABS QM 10

Status: Approved & Effective
Effective Date: 2024-06-14
Control Number: TINS000077
Version: 12.0

APPROVAL TABLE

Status[1]	Selected for Approval username (Full Name), *Title*	Approved By username (Full Name)	Meaning	Approval Date
APP	pdemers@solabs.com (Pascal Demers), *N/A*	pdemers@solabs.com (Pascal Demers)	Originator (Author)	2024-06-13 17:03:27 UTC-04:00
APP	Any, *Head of Engineering*	kevin.b.langlois@solabs.com (Kevin Byrne-Langlois)	Approver	2024-06-14 09:27:17 UTC-04:00
APP	Any, *Head of Product & Quality Management*	mboire@solabs.com (Martine Boire)	Approver	2024-06-14 09:32:40 UTC-04:00

[1] Legend:
NS: Not Started
AWA: Awaiting Approval
APP: Approved
REJ: Rejected
STO: Stopped

EFFECTIVE

© SOLABS QM

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

EFFECTIVE

CREQ NUMBER:	**CREQ-** _____
INSTANCE	INTERNAL: ☐ QUALIF: ☐ SANDBOX: ☐ 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 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. IF MFA IS ENABLED FOR USERS, OF THE AZURE ACTIVE DIRECTORY, A PREMIUM SUBSCRIPTION TO AZURE WILL BE REQUIRED, ALLOWING BYPASS FOR OPERATIONS DONE FROM THE QM10 BACKEND.
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	10.10.0+

EFFECTIVE

2. EXECUTION

QM Graph Api application configuration for the SOLABS QM10 instances:

1. ☐ Go to the Entra Id Portal: https://entra.microsoft.com/
2. ☐ Under **Manage**, click on **App Registrations.**
3. ☐ Click on **+ New registration.**
4. ☐ Enter the desired Name (ex.: SOLABSQM Graph).
5. ☐ Select the 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, under **Allow public client flows,** set **Enable the following mobile and desktop flows** to **Yes.**
10. ☐ Click **Save**.
11. ☐ Click on **API permissions.**
12. ☐ Click **+ Add a permission** > **Microsoft Graph** >
13. ☐ Click on **Delegated permissions.**
14. ☐ Search **User.Read** and choose **User.Read – Sign in and read user profile.**

15. ☐ Click on **Application permissions.**
16. ☐ Search **User.Read.all** and choose **User.Read.all – Read all users full profiles.**
17. ☐ Click **Add permissions.**
18. ☐ Click on **Grant admin consent.**
19. ☐ Click on **Certificates & secrets.**
20. ☐ Click **+ New client secret.**
21. ☐ Give it a description and choose its expiration, then click **Add.**
22. ☐ Take note of the value in the list (it will not be shown again afterward), you will need to provide it to SOLABS.

QM SSO Application configuration for the instance:

23. ☐ From the main page App registrations, under **Applications**, click on **Enterprise applications.**
24. ☐ Click on **+ New application.**
25. ☐ Click on **+ Create you own application.**
26. ☐ Enter the desired Name (based on the type of instance to which this app will be used for) and Supported account type.
27. ☐ Make sure to select the option **Integrate any other application you don't find in the gallery (Non-gallery).**
28. ☐ Click **Create.**
29. ☐ Click on **Single sign-on.**
30. ☐ Select **SAML**
31. ☐ Click **Edit** in the **Basic SAML Configuration**.
32. ☐ In the **Identifier (Entity ID**), enter the URL of the SOLABS QM Instance. (Ex.: https://clientX.solabs.com/QMXXX/) provided by SOLABS (Note the trailing **/** at the end: it is mandatory).
33. ☐ In the **Reply URL (Assertion Consumer Service URL)** enter the same URL, with **?useSamlRoute=true** appended at the end (ex.: https://clientX.solabs.com/QMXXX?useSamlRoute=true).
34. ☐ Click **Save**.
35. ☐ Under the **SAML Certificates** section, download the **Certificate (Base64)**, you will need to send it to SOLABS.
36. ☐ Click on **Users and Group.**
37. ☐ Click **Add User/Group** then add group(s) or specific users that will need to be authenticated through Azure using this SSO Application.

Optional

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

38. ☐ Click on **Properties.**
39. ☐ Set **Enabled for users to sign-in?** to **Yes**.

40. ☐ Upload the SOLABS QM app logo (provided on demand by SOLABS), for the instance to which this app relates, through the "Logo" field.
41. ☐ Set **Assignment required?** To **Yes**. (Users will have to be assigned to be able to access the App.)
42. ☐ Set **Visible to users?** to **Yes**.
43. ☐ Click **Save**

Azure application configuration for Production instance:

EFFECTIVE

44. ☐ Repeat step 1 to 42 but use a different name at steps 5 and 26 and to better indicate that this is for the Production environment.

MFA Bypass

Notes:

- *Because there are certain operations that are done through the SOLABS QM10 backend (without user interactions), it is important for MFA to be disabled for request coming form the SOLABS QM public IP.*
- *This is **required** if MFA is enabled for users of the Azure Active Directory that will be accessing SOLABS QM.*
- *The configuration depends on how MFA is enabled for each user.*
- *One of the Conditional Access configurations is required when MFA is enabled through a Conditional Access policy.*
- *The Trusted IPs configuration is required when MFA is enabled at the user level (Per-user MFA)*
- *Both configurations could have to be set in place if both methods are used for different users that would be required to access QM10.*

Important:

- *An Azure Premium subscription is required to have access to these options.*
- *These are minimal guidelines which could be implemented differently based on the customer's own Azure configuration/knowledge.*

EFFECTIVE

Conditional Access – Exclude QM10 Location:

45. ☐ Go to the Entra Id Portal: https://entra.microsoft.com/
46. ☐ Under **Protection**, select **Security Center**.
47. ☐ Select **Named Location**.
48. ☐ Select **+ IP ranges location.**
49. ☐ Enter a **name** for this location. (ex.: SOLABS)
50. ☐ Click **+** and enter the **IP range** provided by SOLABS and click Add.
51. ☐ Click **Save**.
52. ☐ Select **Conditional Access.**
53. ☐ Select the Conditional Access policy related to the MFA.
54. ☐ Under **Assignments**, select **Conditions**.
55. ☐ Select **Locations**.
56. ☐ Under **Exclude**, select **Selected locations** and click on **Select**.
57. ☐ Select the **Named Location** created above.
58. ☐ Click **Select**.
59. ☐ Click **Save**.

AND / OR

MFA Trusted IP – Add SOLABS IP to trusted list:

60. ☐ Go to the Entra Id Portal: https://entra.microsoft.com/

61. ☐ Under **Protection**, select **Security Center**.
62. ☐ Select **Named locations**.
63. ☐ Click on **Configure multifactor authentication trusted IPs**.
64. ☐ Under **Trusted IPs** check the box next to **Skip multi-factor authentication for requests from federated users on my intranet**.
65. ☐ 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.
66. ☐ Click **Save**.

Sending information to SOLABS

67. ☐ Fill the **FORM000019 – Azure Configuration Parameters Form**
68. ☐ Send the form to SOLABS.

3. COMMENTS

EFFECTIVE