National College of Ireland

Configuration Manual

MSc Research Project
Cybersecurity

Tushar Kaushik
Student ID: 19236158

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Tushar Kaushik……

Student ID: ……19236158……

Programme: ……MSc Cybersecurity…… **Year:** …2021-2022..

Module: ……MSc Internship……

Lecturer: ……Prof. Vikas Sahni……

Submission Due Date: ……07/01/2022……

Project Title: Implementing an IDaaS for Microsoft Active Directory using SensiPass® Three-factor Dynamic Digital Signature

Word Count: ……1307……**Page Count:** ……14……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Tushar Kaushik……

Date: ……06/01/2022……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Tushar Kaushik
Student ID: 19236158

1 Introduction

SensiPass® application was created as a three-factor dynamic digital signature authentication provider. The backend of which was deployed on AWS Lambda service and the database used was Aurora. Changes were made to the core to provide an extension for SAML based identity provider. The code cannot be displayed because the changes had been made in the existing code of the application and there is an NDA signed with the company.

2 Tools/Languages

Backend - The languages used for core development are Java, JavaScript, and MySQL. AWS Lambda and Aurora MySQL database is used along with API Gateway for creating application API service.

Java 8: Java is used for the coding in Lambda to make changes in the backend.

JavaScript ES2015 and HTML5: JavaScript and HTML was used to create a session token page.

AWS Lambda: AWS Lambda is considered as one of the leading service providers when it comes to serverless computing. Stateless functions coded in languages like Node.js, C#, Go, Python and Java can be easily executed in the Lambda. Since the functions are designed in a stateless manner (i.e., The functions are created without making any assumptions about the infrastructure), elasticity is provided automatically by the platform. (Giménez-Alventosa et al., 2019)

Aurora Database: It's a cloud-based relational database that combines MySQL and PostgreSQL compatibility. It produces five times the output of normal MySQL and three times the output of conventional PostgreSQL uses the same hardware. Storage space that auto-scales up to 64TB per database instance and is fault-tolerant, distributed, and self-healing. (Mukherjee, 2019)

API Gateway: The Amazon API Gateway service allows you to create, deploy, maintain, analyse, and secure REST, HTTP, and WebSocket APIs at any scale. API builders can design APIs that connect to AWS or other web services, along with data stored in the Amazon Web Services Cloud.[1]

[1] https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html

3 Description

Screenshots of various components created has been shown below. However, some parts could not be disclosed and had been stroked off because of the NDA signed.

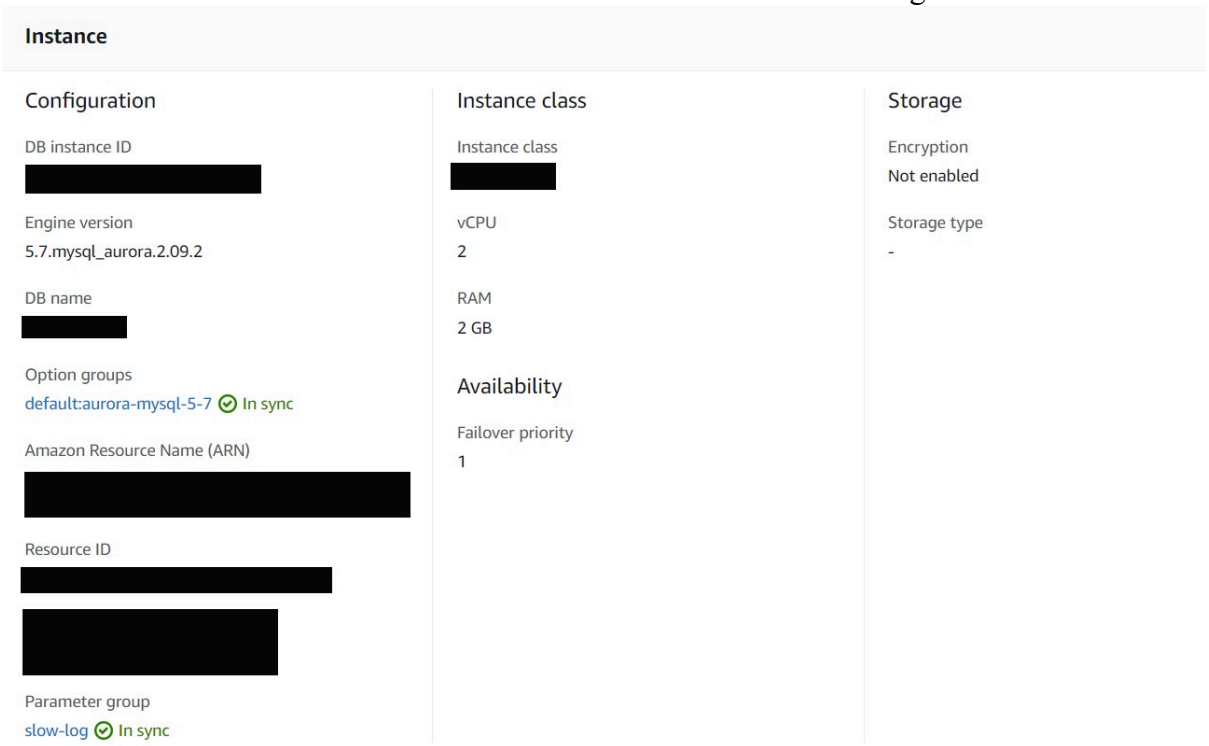

Figure 1: Aurora Db details

Details of the Aurora database has been shown above. The figure depicts the various specifications used to create the database instance.

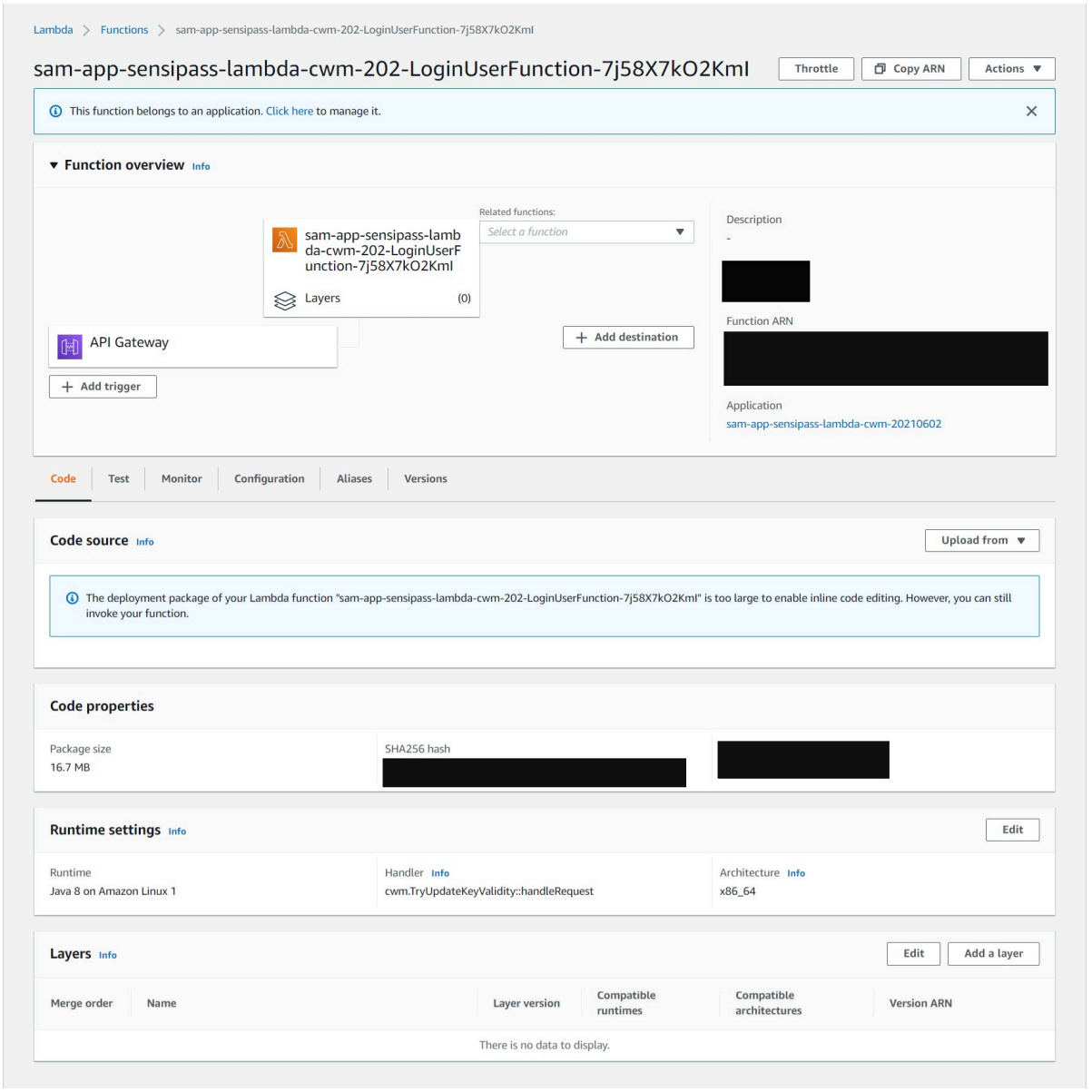

Figure 2: Functions in Lambda

Figure 2 depicts the overview of the function created in AWS to implement the extension of API.

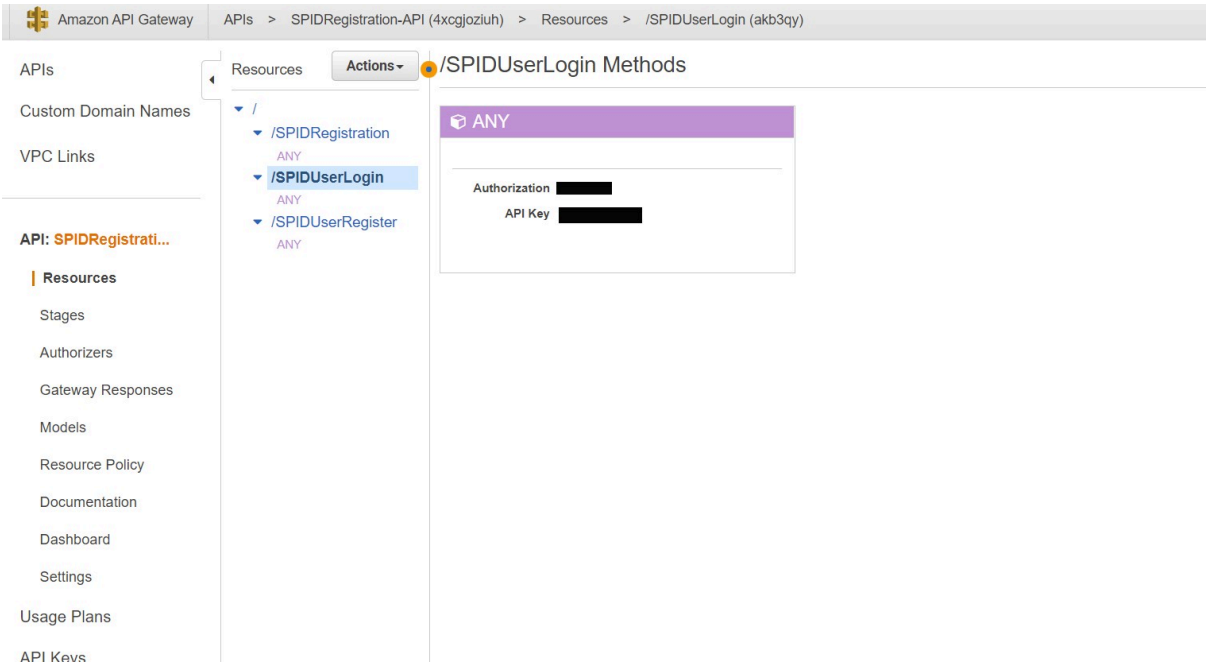

Figure 3: Details of API

In Figure 3, the details of API are shown in the Amazon API gateway section. Here, the login and user registration functions can be seen.

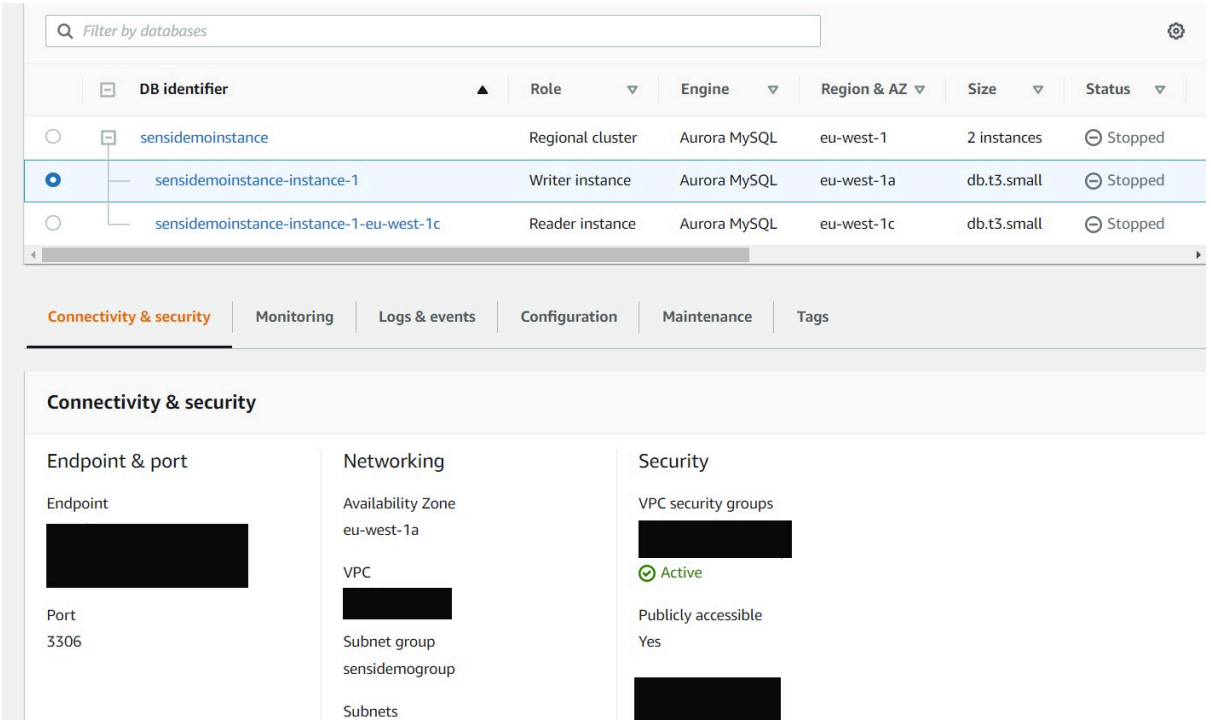

Figure 4: Demo instances created

Here the demo database instances were created with Aurora MySQL database.

Function name	Description	Package type	Runtime	Code size
[redacted]	-	Zip	Java 8 on Amazon Linux 1	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 2	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 2	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 1	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 1	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 2	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 1	13.8 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 1	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 1	16.7 MB
[redacted]	-	Zip	Java 8 on Amazon Linux 2	16.7 MB

Figure 5: Functions

Different functions for the application were created. This includes the previous functions which were already present and the new functions which were created for the implementation.

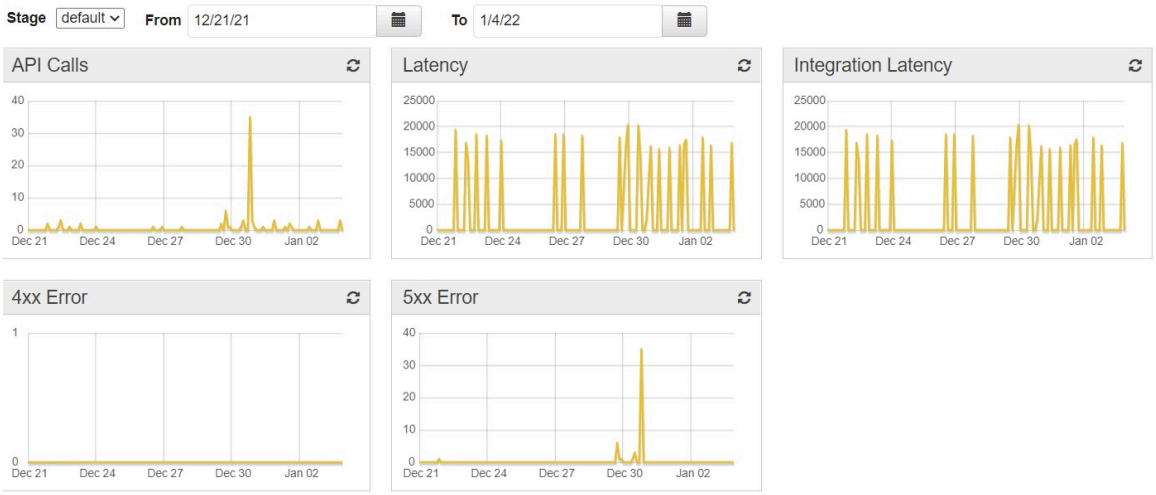

Figure 6: Various Stats

Step 1: In Figure 7, SensiPass will require the read access to the user's Azure active directory tenant.

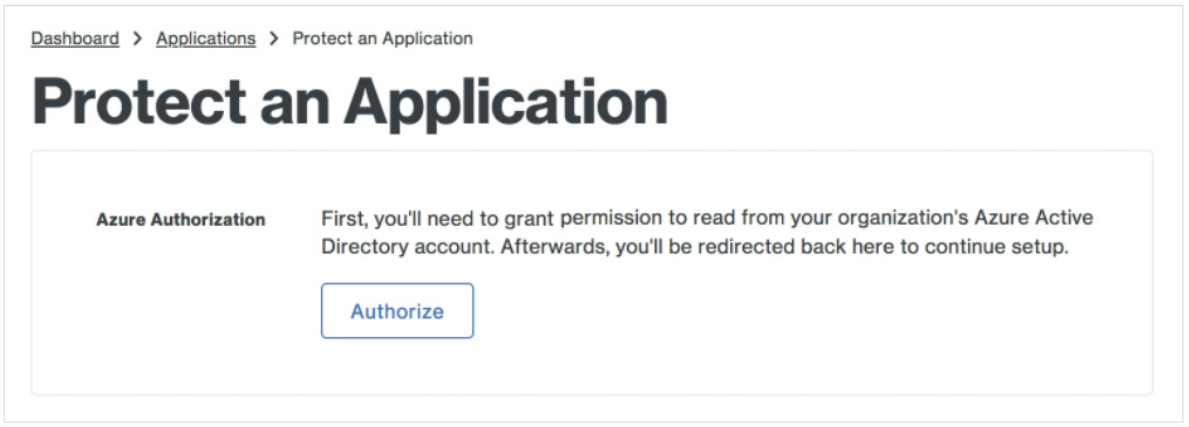

Figure 7: Read permission

Step 2: A sign in with the Azure account will be required.

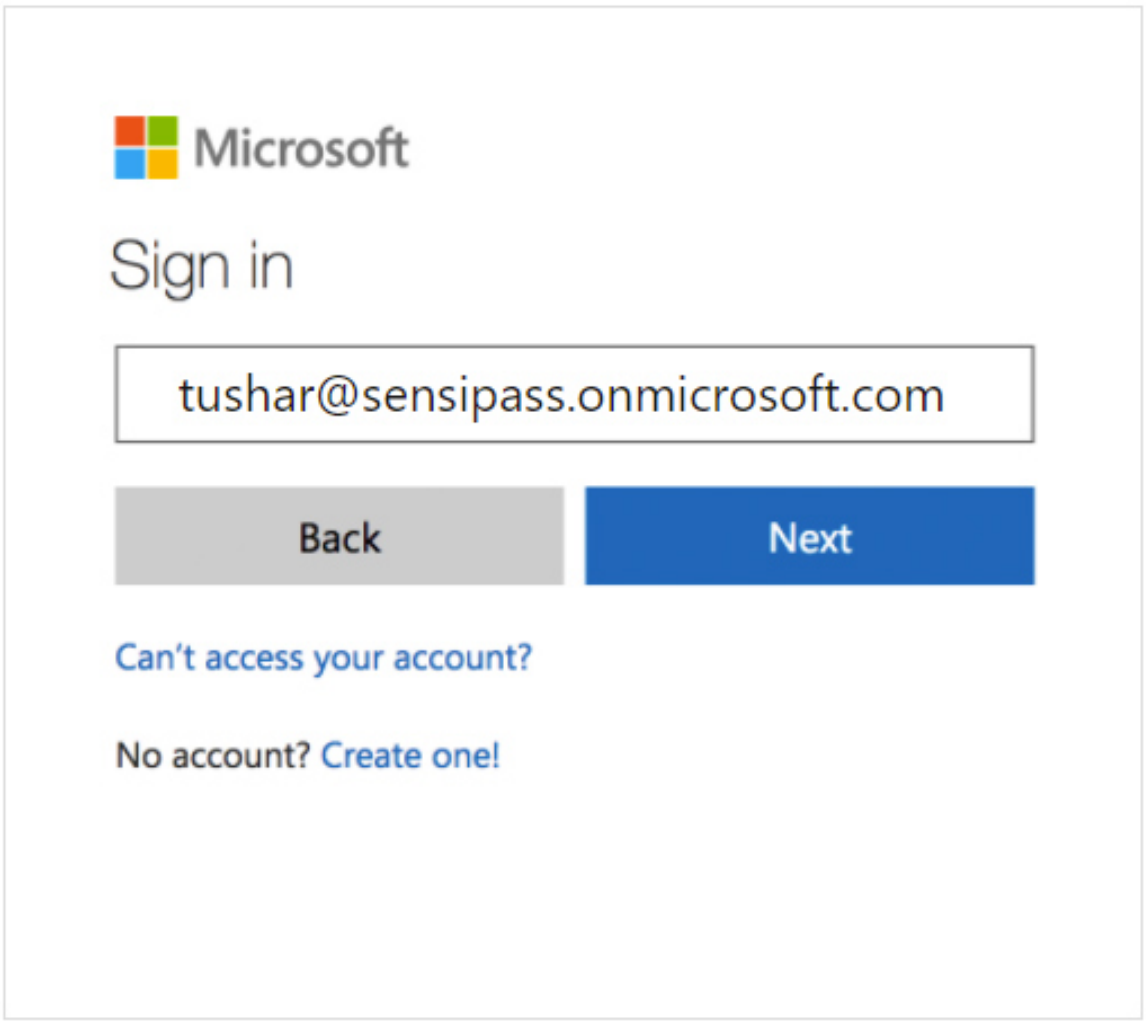

Figure 8: Sign in

Step 3: Once the sign in is completed, the user shall click on Accept and give SensiPass the necessary rights which were needed to read and access the Azure active directory tenant.

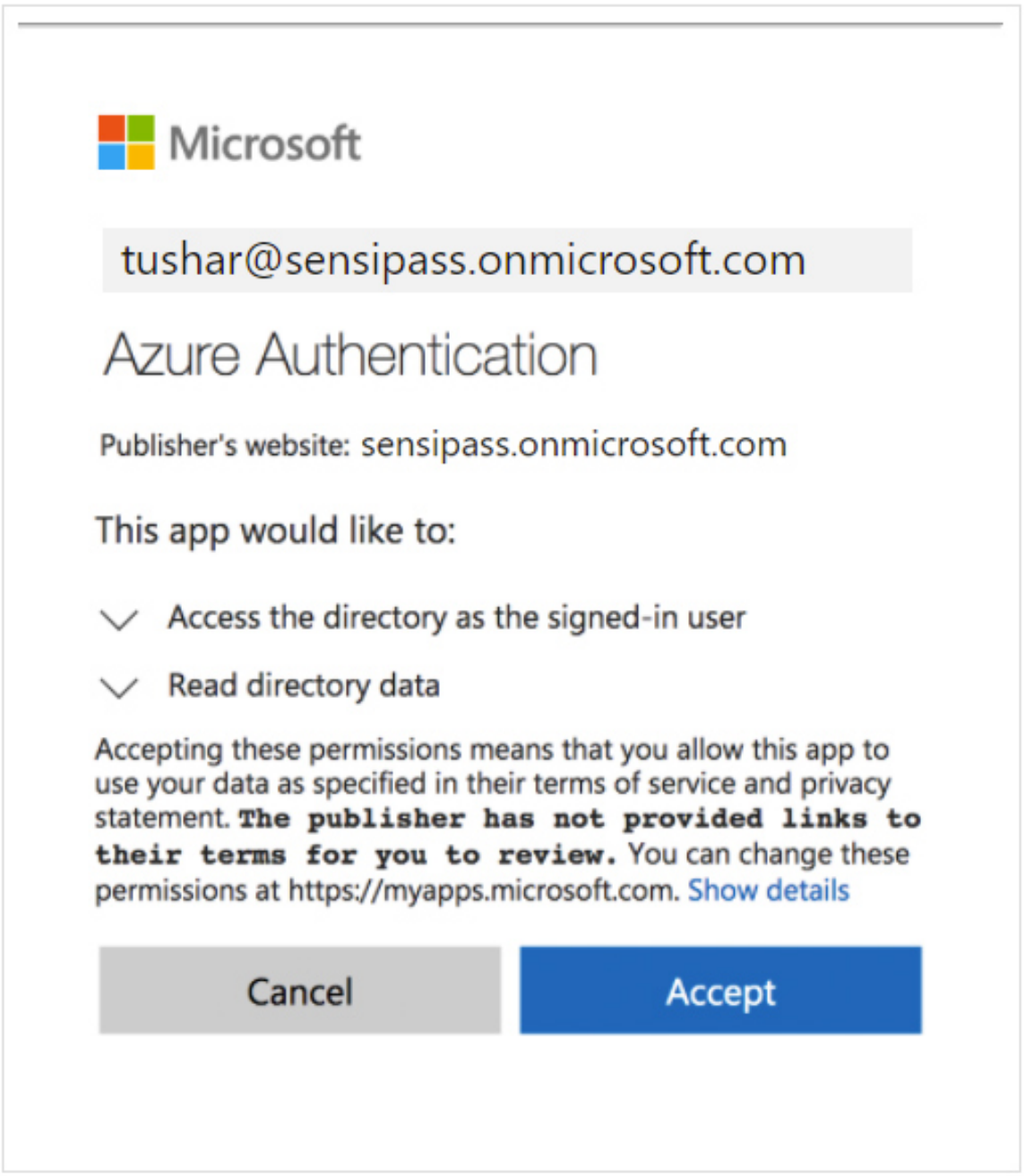

Figure 9: Permissions for the tenant access

Step 4: To complete the SensiPass authentication setup the above shown JSON text will be provided to Azure.

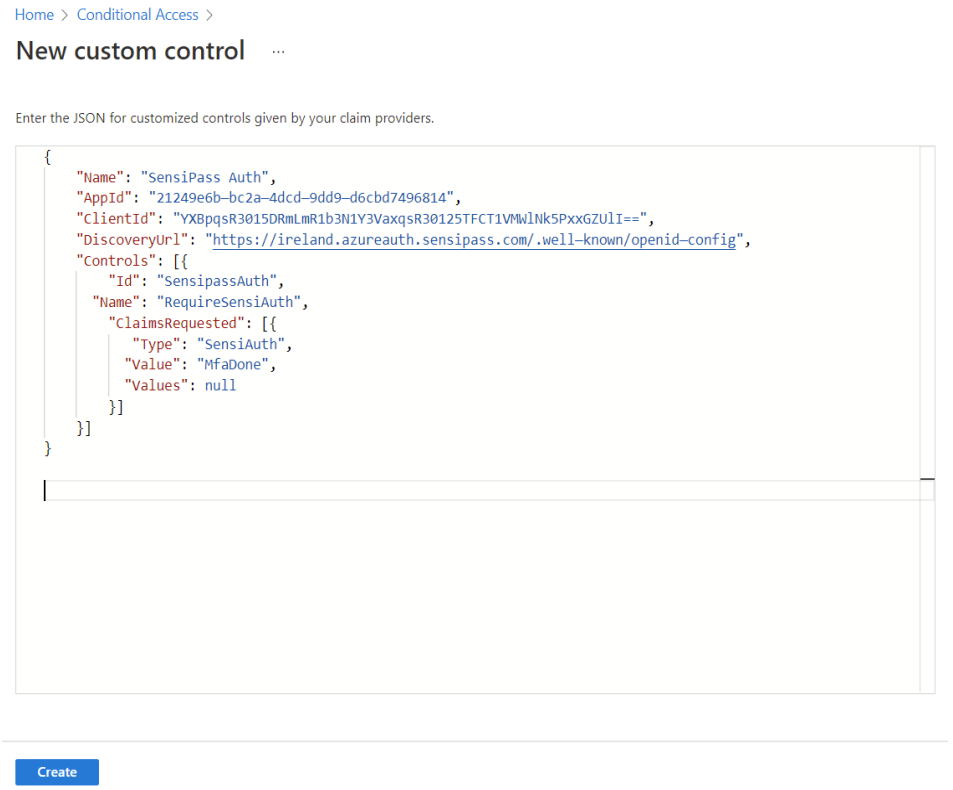

Figure 10: Custom Control Configuration in Azure AD Conditional Access

The next step, Microsoft Azure configuration will be done by my internship colleague Sujit Mourya.

Continuing with my part ahead,

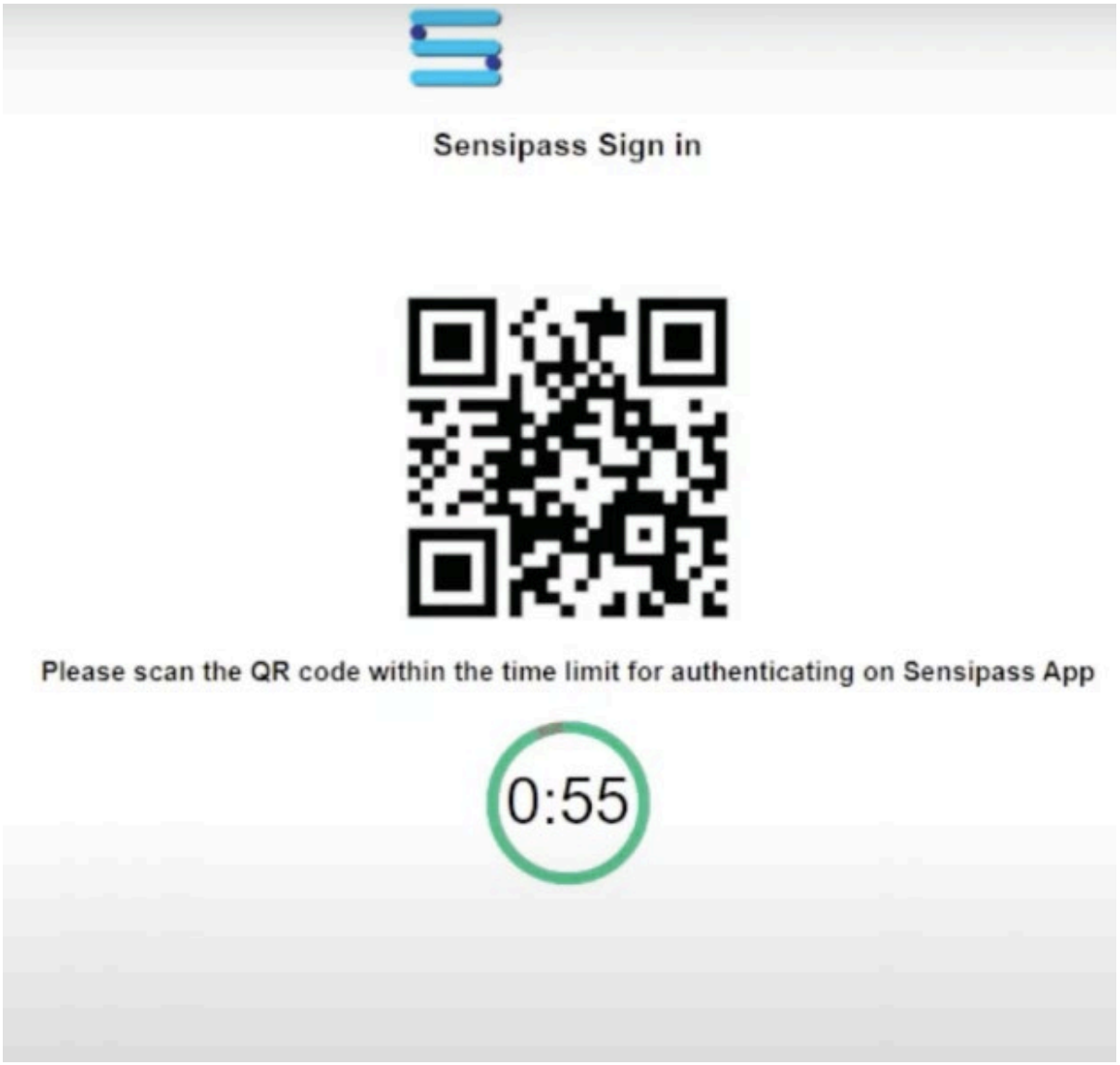

Figure 11: Session token (QR code) generated

In Figure 11, a session token in the form of a QR code had been created to provide proximity to the user. Proximity helps the user to maintain confidentiality and makes sure that even if the user gives access to someone then also the authentication will not be breached. As the token is generated for a very short time and in front of the valid user.

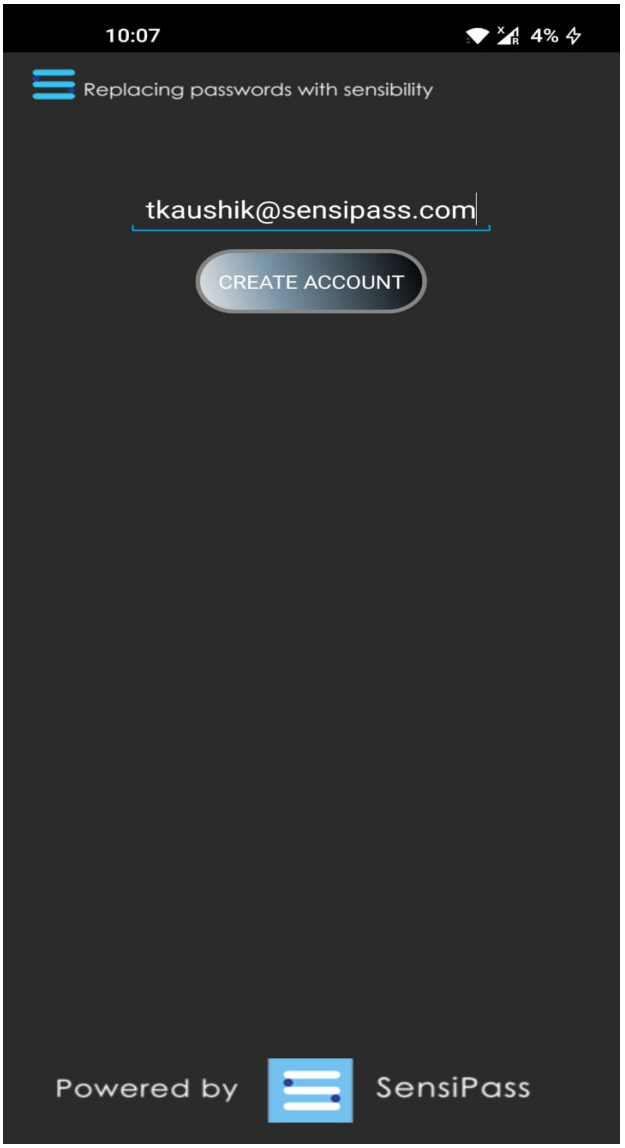

Figure 6: Registration Page

Figure 12 shows the registration page from where the QR code leads the user for authentication and enter their BioGlyph.

4 Monthly Internship Activity Report

Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Tushar Kaushik Company: SensiPass Ltd.

Student number: 19236158

Month Commencing: October – December 2021

Role description:

The primary goal was to study the SensiPass architecture and research on three-factor authentication. Security recommendations for AWS and the required modifications for SensiPass. Following are the list of tasks performed:

- Providing Security recommendations for AWS Lambda and Aurora database.
- Building and designing a framework for integrating Microsoft Azure Active Directory and SensiPass three-factor dynamic digital signature.
- Get an understanding of SensiPass core working architecture by studying its patent and official documents.
- Learning about the latest innovation in the domain of multifactor authentication.
- Learning the Azure AD architecture by performing a thorough research from official documents.
- Coordinating with the team members for the knowledge transfer and technical understanding.
- Meeting with internal stake holders for understanding architecture and the project requirements.
- Creation of tasks on click up while keeping up with scheduling and prioritizing deadlines.

Employer comments

Tushar entered into a Confidentiality Agreement with SensiPass on 15 September 2021 and effectively began his internship in the beginning of October. During this time, he effectively utilized our communications and management tools, demonstrate knowledge of our technology, and integrated well with our development team remotely and in our offices. Ultimately, he provided value in the final report he created as well as in his insights and comments along the way. We are looking forward to continuing a working relationship with Mr. Kaushik.

Student Signature: 

Date: 6 Januaary 2022

Industry Supervisor Signature: 

Date: 6 January 2022

References

[1] Giménez-Alventosa, V., Moltó, G., Caballer, M., 2019. A framework and a performance assessment for serverless MapReduce on AWS Lambda. Future Generation Computer Systems 97, 259–274. https://doi.org/10.1016/j.future.2019.02.057

[2] Mukherjee, S., 2019. Benefits of AWS in Modern Cloud. SSRN Journal. https://doi.org/10.2139/ssrn.3415956