

Configuration Manual

MSc Research Project
Cybersecurity

Sujit Mourya
Student ID: x19239343

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Sujit Mourya

Student ID: x19239343

Programme: MSc Cybersecurity

Year: 2021-2022

Module: MSc Internship

Supervisor: Prof. Vikas Sahni

Submission

Due Date: 07/01/2022

Project Title: Implementing an IDaaS for Azure Active Directory using Azure Conditional Access Policies

Word Count: 1481 **Page Count:** 13

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: Sujit Mourya

Date: 05/01/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
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 the computer.	<input type="checkbox"/>

Assignments 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

Sujit Mourya
X19239343

1 Introduction

The Configuration Manual document contains the details about the research paper's technical details, tools, and technologies. This Configuration Manual also contains various steps that would allow to replicate the implementation process on the Azure AD. The methods contain the different service creation and configuration of the relevant sections in the Azure Active Directory portal.

2 Tools / Services / Pre-requisites

The Tools, Services and Pre-requisites for the implementation of the Azure AD is explained as below.

2.1 Backend

The backend integration of Azure AD with SensiPass requires an API endpoint. The backend API code was written in Java 8 and hosted on AWS Lambda. The API Gateway was used with Lambda for the endpoint creation. AWS Aurora was used to store the API request data for logging purpose. The coding for the backend changes has been done by Tushar (SensiPass colleague from same internship). The mobile application created at SensiPass was built on core Java (version 8) and used Android Studio latest to write the code.

2.2 Frontend

The frontend of the multi-factor authentication page was built on Node.js v16.13.0, JavaScript and HTML. The QR code contains a socket connection with the time-bound auto refresh that changes the QR code.

2.3 Services

Microsoft Azure standard user account is required to create the Azure AD service.

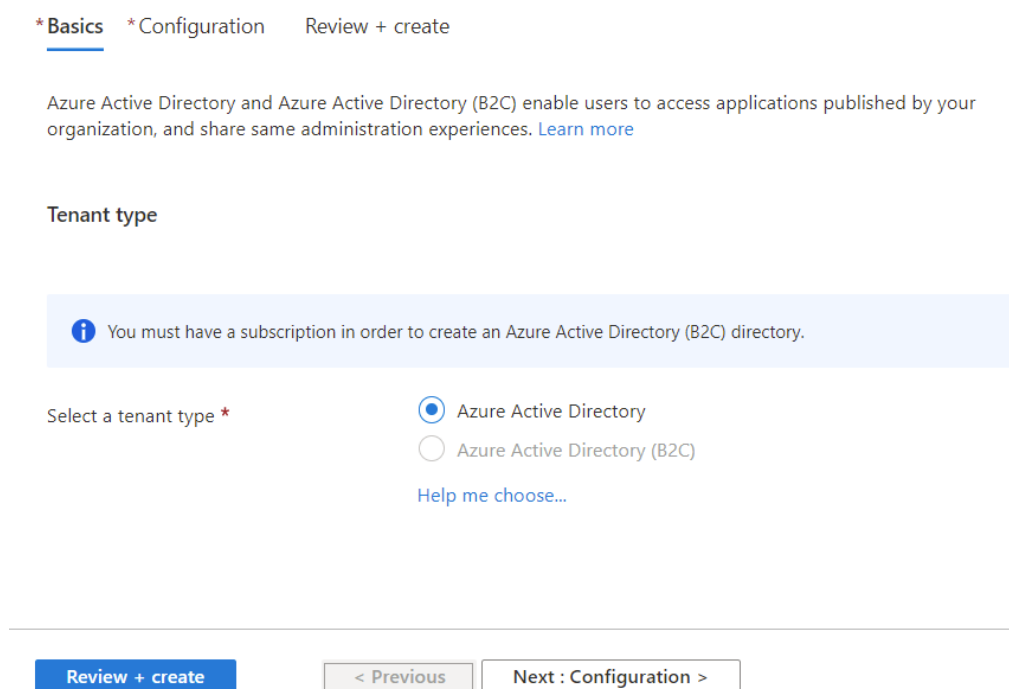
2.4 Pre-requisites

To create custom policies, Device Risk, Sign-in Risk and target specific conditions, the Azure AD premium is required. The following types of Azure AD premium are available, Enterprise Mobility + Security E5 / Azure Active Directory Premium P1 and Azure Active Directory Premium P2. The current implementation of Azure AD was done through the Free trial of Azure AD Premium.¹

3 Setting and Configuration of Microsoft Azure AD

The settings and configurations contain the steps required to setup conditional access on Azure AD. It requires creation of tenant, users, groups, and custom policy.²

3.1 Create a tenant



The screenshot shows the 'Create a tenant' - Basics page in the Azure portal. At the top, there are three tabs: '* Basics' (selected), '* Configuration', and 'Review + create'. Below the tabs, a message states: 'Azure Active Directory and Azure Active Directory (B2C) enable users to access applications published by your organization, and share same administration experiences. [Learn more](#)'. Under the heading 'Tenant type', there is a light blue information box that says: 'You must have a subscription in order to create an Azure Active Directory (B2C) directory.' Below this, the 'Select a tenant type' section has two radio button options: 'Azure Active Directory' (which is selected) and 'Azure Active Directory (B2C)'. A link 'Help me choose...' is located below the radio buttons. At the bottom of the page, there are three buttons: 'Review + create' (in blue), '< Previous' (disabled), and 'Next : Configuration >' (disabled).

Figure 1. Create a Tenant - Basics

A new tenant can be created using the 'Create a tenant' page. The form asks for various details such as Tenant type.

¹ <https://azure.microsoft.com/en-in/services/active-directory>

² <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

* Basics * **Configuration** Review + create

Directory details
Configure your new directory

Organization name * ⓘ ✓

Initial domain name * ⓘ ✓
sensipass3fa.onmicrosoft.com

Country/Region ⓘ ▼

✓ Datacenter location - United States
Datacenter location is based on the country/region selected above.

[Review + create](#) [< Previous](#) [Next : Review + create >](#)

Figure 2. Create a Tenant - Configuration

The configuration step includes the Organization name and Domain name. The country/region is the server location for the Active Directory. Click Review + create to see the selected options.

3.2 Create a User

Home > SensiPass AD > Users >

New user ...

SensiPass AD

Got feedback?

☒

Create user

Create a new user in your organization. This user will have a user name like `alice@sensipass.onmicrosoft.com`.
[I want to create users in bulk](#)

☐

Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * ⓘ @ ▼
[The domain name I need isn't shown here](#)

Name * ⓘ

First name

Last name

Groups and roles

[Create](#)

Figure 3. Create a user form

A new user creation page has two options. Create user form and Invite User form. The create user form has a different field identity, password, groups, roles, settings, and job info.

New user ...

SensiPass AD

[Got feedback?](#)

☐ **Create user**
Create a new user in your organization. This user will have a user name like `alice@sensipass.onmicrosoft.com`.
[I want to create users in bulk](#)

☒ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

Name ⓘ

Email address * ⓘ

First name

Last name

Personal message

Figure 4. Create a User by Invite

The user by Invite link allows users out of the organisation to join the Azure AD. The username and Email Id is filled for inviting users.

3.3 Create a Group

A new group is created through a 'Create a Group' page. The different options such as Group type, Group name and Group descriptions are mentioned in the form.

[Home](#) > [SensiPass AD](#) > [Groups](#) >

New Group ...

Group type * ⓘ

Security

Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type ⓘ

Assigned

Owners

[No owners selected](#)

Members

[No members selected](#)

Create

Figure 5. Create a User by Invite

3.4 Create a new policy for Conditional Access

Creating a new Conditional Access policy requires Azure AD premium. The creation form takes name of the policy, apps, access controls and sessions value. The policy will be enabled if the user enables the policy and finally save the policy.

3.4.1 Custom new policy for conditional access

Sensipass 3-factor auth

Conditional Access policy

Delete

policy to bring signals together, to make decisions, and enforce organizational policies.
 [Learn more](#)

Name *

Sensipass 3-factor auth

Assignments

Users or workload identities

0 users or workload identities selected

Cloud apps or actions

1 app included

Enable policy

Report-only

On

Off

It looks like you're about to manage your organization's security configurations. That's great! You must first disable Security defaults before enabling a Conditional Access policy.

Save

Figure 6. Create a new policy for Conditional Access

Creating a custom new policy for conditional requires the unique name and different configurations and settings.

3.4.2 User or workload identities selection

Home > cybeardcloud.com > Security > Conditional Access >

Sensipass 3-factor auth

Conditional Access policy

Delete

Learn more

Name *

Sensipass 3-factor auth

Assignments

Users or workload identities

Specific users included

"Select users and groups" must be configured.

Cloud apps or actions

1 app included

Conditions

4 conditions selected

Access controls

Grant

Enable policy

Report-only

On

Off

It looks like you're about to manage your organization's security configurations. That's great! You must first disable Security defaults before enabling a Conditional Access policy.

Save

What does this policy apply to?

Users and groups

Include

Exclude

☐ None
 ☐ All users
 ☒ Select users and groups

☐ All guest and external users
 ☐ Directory roles
 ☒ Users and groups

Select

0 users and groups selected

Select at least one user or group.

Select

Users and groups

Search

SensiPass Users

Selected

Sujit Mourya

x19239343@student.ncirl.ie

Sujit Mourya

sujitmourya@outlook.com mourya

sujitmourya_outlook.com#EXT#@sujitmouryaoutlook.onmicrosoft.com

Selected items

SU

SensiPass Users

Remove

Select

Figure 7. User or workload identities selection

7

Selection of custom users and groups makes conditional access to be targeted for set of users. The options can be used to select SensiPass users and trigger MFA to those users only.³

3.4.3 Cloud apps or actions selection

Home > cybearcloud.com > Security > Conditional Access >

Sensipass 3-factor auth

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Sensipass 3-factor auth

Assignments

Users or workload identities ⓘ

Specific users included

✖ "Select users and groups" must be configured

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

4 conditions selected

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

☐ None

☐ All cloud apps

☒ Select apps

Select

Zendesk

10152947-266f-4ef1-998e-05482c3201...

Enable policy

Report-only On Off

⚠ It looks like you're about to manage your organization's security configurations. That's great! You must first disable Security defaults before enabling a Conditional Access policy.

Save

Figure 8. Cloud apps or actions selection

Different apps can be targeted for conditional access. Here Zendesk was used to target the 3-factor authentication, so when user access this app, it will trigger an authentication on SensiPass app.

3.4.4 Selection of Conditions for a Policy

³ <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

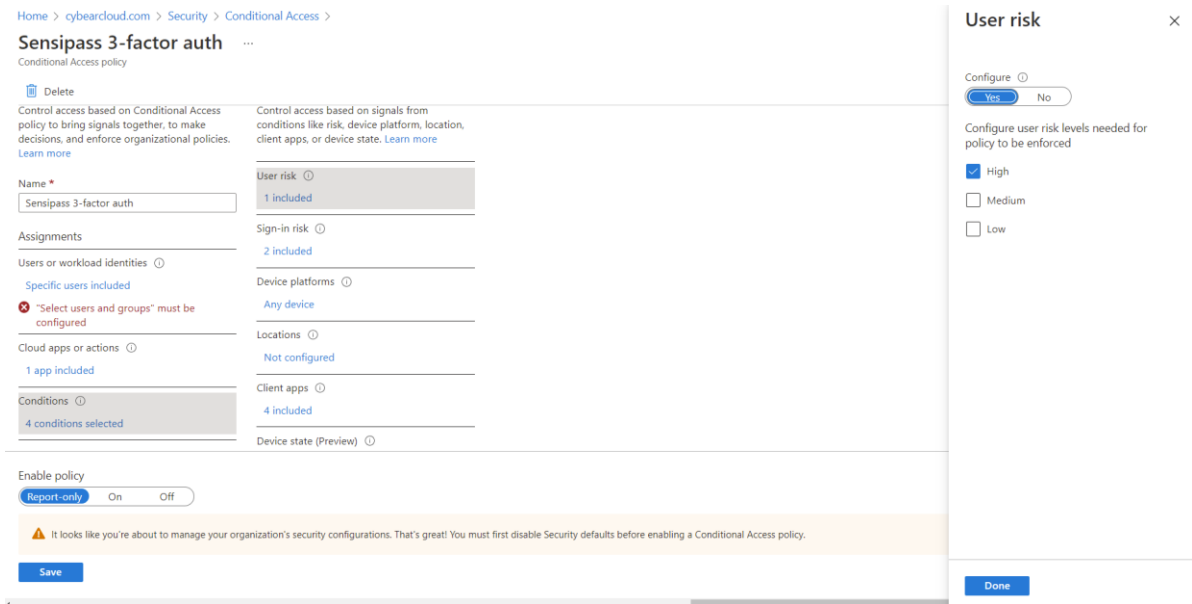


Figure 9. Selection of Conditions for a Policy

Different conditions such as user risk, sign in risk, locations and client apps can be targeted through this settings.

3.4.5 Selecting Device Target for Conditions

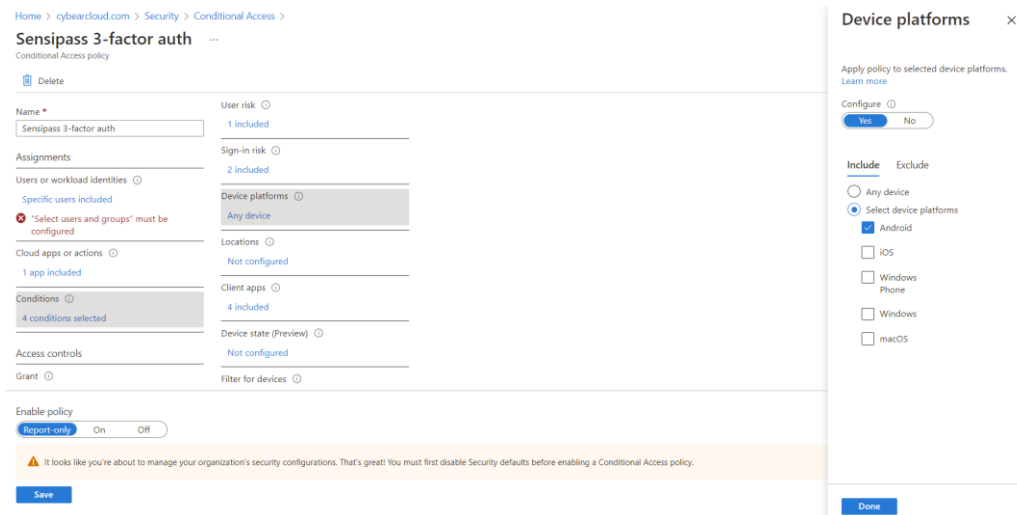


Figure 10. Selecting Device Target for Conditions

Different types of devices can be targeted such Android and iOS for MFA authentication. For now, Android was enabled as the SensiPass is only available on Android.

3.4.6 Json setting customised control for claim providers

Home > cybearcloud.com > Security > Conditional Access >

SensipassAuth ...

Enter the JSON for customized controls given by your claim providers.

```
{
  "Name": "SensiPassAuth",
  "AppId": "00000200-0100-4000-0600-000700000000",
  "ClientId": "00001000-0010-2000-0002-000000000003",
  "DiscoveryUrl": "https://sensipass.com/azure-auth/3fa",
  "controls": [
    {
      "Id": "SensipassAuth",
      "Name": "SensipassAuth",
      "ClaimsRequested": [
        {
          "Type": "SensipassAuth",
          "Value": "MFADone",
          "Values": null
        }
      ],
      "Claims": null
    }
  ]
}
```

Save

Figure 12. Json setting customised control for claim providers

Custom Json settings can be used for providing the claim providers details for multi-factor authentication. Different keys in the Json provides the parameters for the API endpoints at SensiPass. The settings contains the AppId and ClientId for security settings and claims for verification at SensiPass end.

3.4.7 Grant selection for custom policy

Home > cybearcloud.com > Security > Conditional Access >

Sensipass 3-factor auth ...

Conditional Access policy

Delete

Specific users included

✖ "Select users and groups" must be configured

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

4 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

⚠ It looks like you're about to manage your organization's security configurations. That's great! You must first disable Security defaults before enabling a Conditional Access policy.

Save

https://aka.ms/rapolicygrant

Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)

☐ Require password change ⓘ

☒ SensipassAuth

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

Select

Figure 11. Grant selection for custom policy

The grant policy is used to select the newly created customised controls in the previous step. The 'SensipassAuth' is enabled in the screenshot, which allows the triggering of custom controls for the Multi-factor authentication.

3.5 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: Sujit Mourya

Student number: 19239343

Company: Sensipass Ltd.

Month Commencing: Oct-Dec 2021

Role Description:

The primary objective of the internship was to research around the 3-factor authentication finding a research gap in the field of Identity and Access Management. The security recommendations for AWS services and the necessary modifications proposal for SensiPass. Building architecture for SensiPass for integrating the Azure Active Directory as an Identity-as-a-service model.

List of Tasks performed:

- Understanding and Creation of the Tasks on click-up.
- Scheduling and prioritizing the tasks according to the deadlines.
- Identifying different components and services at SensiPass.
- AWS cloud security recommendations
- Meeting with internal stakeholders for understanding architecture and the project requirements.
- Understanding the SensiPass core architecture through its patent and official documents.
- Designing and building a framework for integrating Azure AD and SensiPass
- Understanding the architecture of the Azure AD through official documentation.
- Studying the research gap of 3-factor authentication for SensiPass.
- Coordinating with the team members for knowledge transfer and technical understanding.
- Brainstorming with Mike for different concepts around 3-factor authentication and the latest innovation in IAM.

Employer comments

Sujit 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 utilised our communications and management tools, demonstrate knowledge of our technology and integrated well with our development team remotely and in our offices. He further provided insights into a broader architecture and development options for a new user administration component currently in design. 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. Mourya.

Student Signature:



Sujit Mourya
Date: 04-01-2022

Industry Supervisor Signature:



Mike Hill
Date: 04-01-2022

References