

# Zero-Trust Identity & Access Hub

Portfolio Lab By THATO KGOLE

Date: November 2025

Cloud Platform: Microsoft Azure

## Overview

This Project demonstrates the implementation of a Zero-Trust security model in Azure by focusing on identity and access management. The goal is to secure resources by controlling who can access them, under what conditions, and with what privileges.

## Problem Statement

Many organizations face risks of unauthorized access and data breaches. Traditional perimeter-based security is insufficient, as users may access from multiple locations or devices.

## ***SOLUTION***

Step 1: Create a Resource Group

To group all related content

[Home](#) > [Resource Manager | Resource groups](#) >

## Create a resource group ...

Basics   Tags   Review + create

 [Automation Link](#)

### Basics

Subscription	ZEMBE
Resource group name	ZeroTrustHub
Region	South Africa North

### Tags

None

---

[Previous](#)

[Next](#)

[Create](#)

---

## Step 2: Add user

To give permission and access later



[Home](#) > [Default Directory | Users](#) > [Users](#) >

## Create new user ...

Create a new internal user in your organization

[Basics](#)   [Properties](#)   [Assignments](#)   [Review + create](#)

### Basics

User principal name	AliceJohnson@zembecloudcomputinggmail.onmicrosoft.com 
Display name	Alice Johnson
Mail nickname	AliceJohnson
Password	..... 
Account enabled	Yes

### Properties

User type	Member
-----------	--------

### Assignments

Administrative units

Groups

Roles

[Create](#)


[< Previous](#)

[Next >](#)

## Step 3: Create Groups

### To assign access all at once

## New Group ...

 Got feedback?

Group type \*

Security

Group name \*

AdminTeam

Group description

Enter a description for the group

Membership type

Assigned

Owners

No owners selected

Members

No members selected

Create

### Step 4: Add User Groups

Add members

Try changing or adding filters if you don't see what you're looking for.

Search

94 results found

All Users Groups Devices Enterprise applications

	Name	Type	Details
<input type="checkbox"/>	AR AAD Request Verification Service - P	Enterprise ap...	c728155f-7b2a-4502-a08b-b8af9b269319
<input type="checkbox"/>	A AdminTeam	Group	
<input checked="" type="checkbox"/>	AJ Alice Johnson	User	AliceJohnson@zembeccloudcomputinggmail.c
<input type="checkbox"/>	A aciapi	Enterprise ap...	c5b17a4f-cc6f-4649-9480-684280a2af3a
<input type="checkbox"/>	TK Thato Kgole	User	zembeccloudcomputing@gmail.com
<input type="checkbox"/>	AD AKS Deployment Safeguards	Enterprise ap...	589ce44b-ca13-4384-89e2-dd4e642a4b37

Selected (1)

Reset

AJ Alice Johnson

AliceJohnson@zembeccloudcomputinggm...

Select


### Step 5: Enable MFA For extra Security Measures

[Home](#) > [Default Directory | Users](#) > [Users](#) >

## Per-user multifactor authentication ...

 Bulk update |  Got feedback?

[Users](#) | [Service settings](#)

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive [Conditional Access policies](#). [Learn more](#) 

Before you begin, take a look at the [multifactor authentication deployment guide](#). 

☒ Enable MFA ☐ Disable MFA ☐ Enforce MFA  User MFA settings

Status: All View: Sign-in allowed users  Reset filters

<input type="checkbox"/>	Name 	UPN	Status
<input checked="" type="checkbox"/>	Alice Johnson	Alice.Johnson@zembeccloudcomputinggmail.onmicrosoft.c	disabled
<input type="checkbox"/>	Thato Kgole	zembeccloudcomputing_gmail.com#EXT#@zembeccloud.c	disabled

### Step 6: Create Conditional Access Policy

**Goal > To restrict access to admins based on location, device and require MFA**

**Action Taken > Conceptually created AdminAccessPolicy**

**Limitation > Could not enforce conditions because Conditional access requires Azure AD Premium P1 features**

### Step 7: Privileged Identity Management (PIM)

**Goal > Allow temporary admin privileges for safe operations**

**Action Taken > Conceptually assigned Alice as eligible for Global Admin.**

**Limitation > Require P2 for activation**