### **Chavali Krishna Chandra Aakhyath**

* **Project Name:** Zero Trust Access Architecture on Azure
* **Duration:** 1 Week (6–7 Days)
* **Objective:** Build a working Zero Trust model using Azure AD, Conditional Access, PIM, and Governance tools, then document it as a portfolio project.

### **Tools and Services Used:**

* Azure Active Directory (Entra ID)
* Conditional Access
* Azure AD Identity Protection
* Privileged Identity Management (PIM)
* Access Reviews
* Entitlement Management (Access Packages)
* Azure Monitor + Workbooks
* Log Analytics Workspace
* Azure Alerts

**Day 1 – Setup**

**Tasks:**

* Create Azure Free Trial – <https://azure.microsoft.com/en-in/free>
* Set up 3 users: admin@, user1@, guestuser@
* Create 2 groups: IT-Admins, App-Users
* Document: Tenant name, region, domain name
* Draw rough ZT model (users, apps, policies)

### **Day 2 – Conditional Access**

**Tasks:**

* Policy 1: Require MFA for All Admins
* Policy 2: Block legacy authentication
* Policy 3: Block non-compliant devices
* Policy 4 (Optional): Require MFA outside India
* Test each policy (use InPrivate/Incognito)
* Screenshot: Policy config + sign-in logs

### **Day 3 – PIM**

**Tasks:**

* Enable Azure AD Privileged Identity Management
* Make admin1@ eligible for Global Administrator
* Set up approval + justification
* Test activation (time limit + email alert)
* Screenshot: PIM role activation workflow

### **Day 4 – Identity Protection & Access Governance**

**Tasks:**

* Enable Azure AD Identity Protection
* Policy: Block high-risk users
* Access Package: Create package for App-Users with approval flow
* Set Access Review to expire after 14 days
* Screenshot: Access package flow, risky sign-in alert

### **Day 5 – Monitoring & Alerting**

**Tasks:**

* Open Azure Monitor > Workbooks > Sign-in Activity
* Add filters: MFA, location, device platform
* Add alert for “Impossible Travel” scenario
* (Optional) Connect to Sentinel
* Screenshot: Dashboard + sample alert email

#### Day 1 - Doc:

Tenant Name: Default Directory

Domain: [techieguy361gmailcom.onmicrosoft.com](http://techieguy361gmailcom.onmicrosoft.com)

Region: India

Users Created: admin, guest user, user1

Groups created: IT-Admins, App-Users

Zero Trust layout:

+------------------------------+

| Identity Provider |

| (Azure AD / Entra ID) |

+-------------+----------------+

|

Authenticate via:

- MFA

- Conditional Access

- PIM (Privileged Roles)

|

v

+-----------------------------+

| Access Policies |

| - CA: Geo/IP/device/user |

| - Risk-based access |

| - App Protection Policies |

+-------------+---------------+

|

+---------+--------+

| Azure AD Joined |

| Devices (Intune) |

+---------+--------+

|

+-------------------------------+

| Application Access |

| - Office 365, SaaS, IaaS/PaaS |

| - Protected via App Proxy |

| - Group-based access control |

+-------------------------------+

|

+---------+---------+

| Monitoring & Logs |

| - Azure Monitor |

| - Defender for ID |

| - Sentinel (SIEM) |

+--------------------+

#### Day2- Doc:

MFA enabled for **admin**

CA policy **Admin Portal MFA** created with target user & app

Behavior difference between **admin** and **user**

* Admin is allowed to Azure Portal with MFA prompt while User is allowed to Azure Portal with MFA prompt only when security default is enabled (here it is disabled to use CA). Admin is enforced to MFA while user is not. CA policy is targeted to Admin. Risk exposure is lower to admin and higher to user as Admin has MFA enforced.

#### Day 3- Doc:

**Enabled Microsoft Entra PIM**

* Navigated to Microsoft Entra > Identity Governance > Privileged Identity Management
* Activated PIM for Azure AD roles

**Assigned admin... as an *Eligible* Global Administrator**

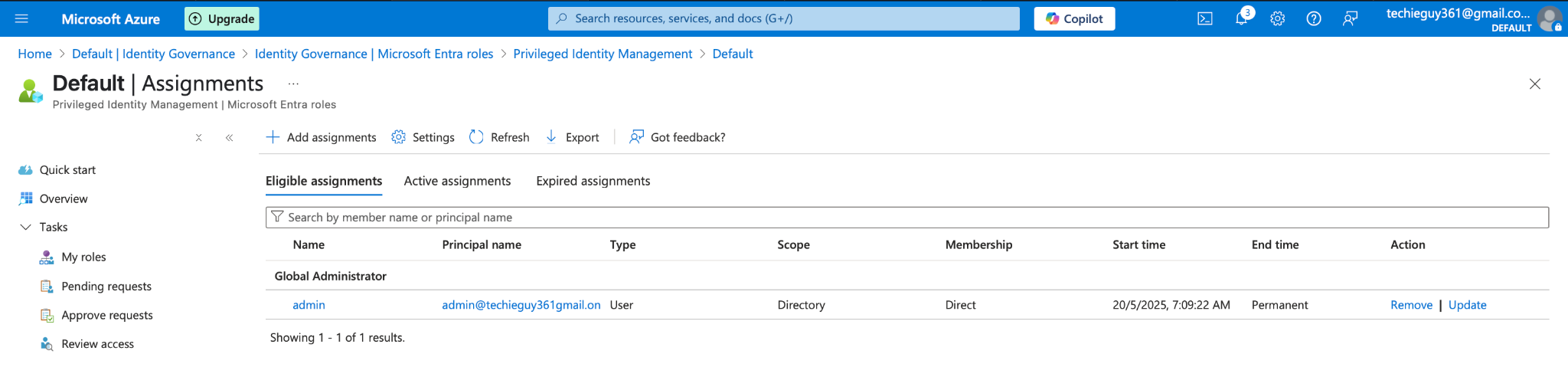
* Role assigned: Global Administrator
* Assignment type: Eligible

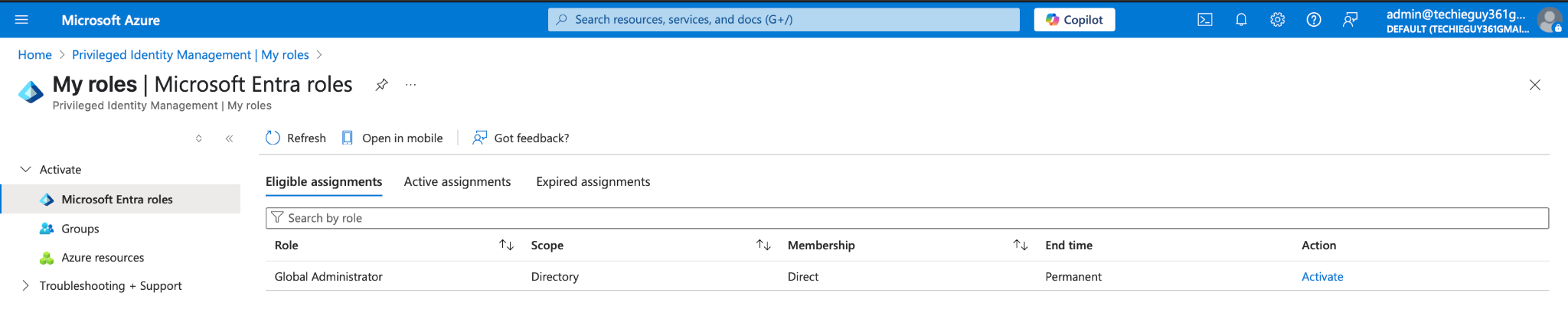
**Configured Role Settings for Global Administrator**

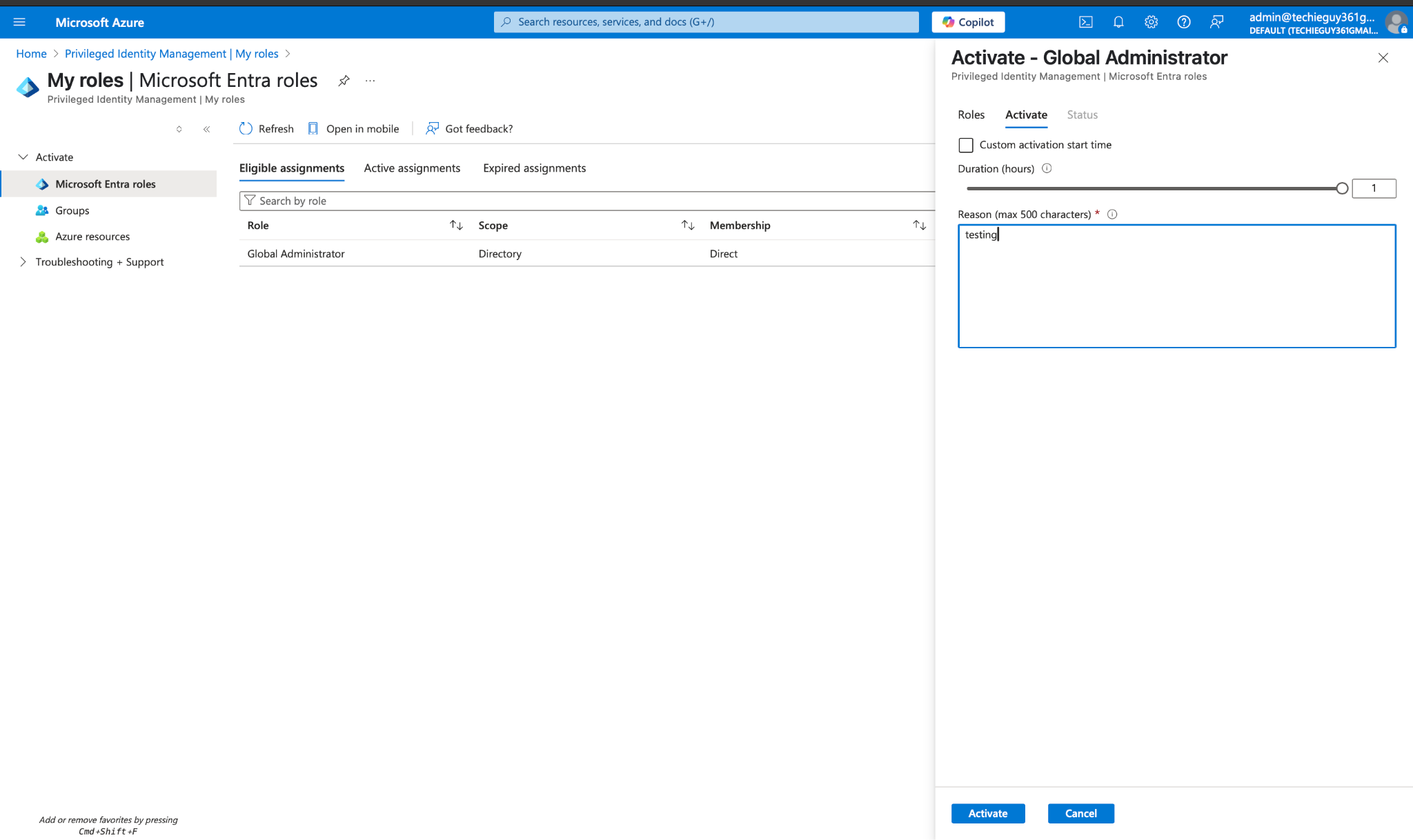
* Activation Duration: 1 hour
* Required MFA on role activation
* Required justification for access
* Approval not added (optional)

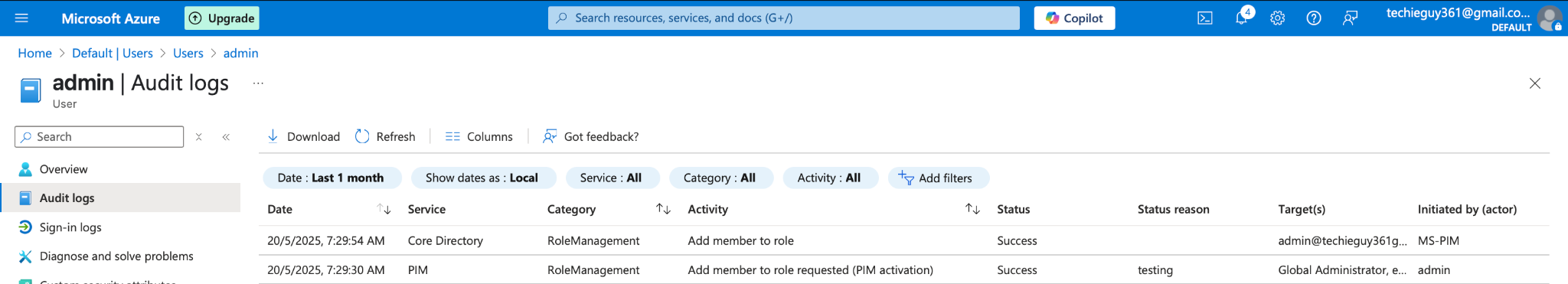
**Tested Just-in-Time (JIT) Access Flow**

* Signed in as admin
* Activated Global Admin role through PIM
* Provided justification and completed MFA
* Verified access to privileged areas (e.g., Azure AD, Conditional Access)









#### Day 4- Doc:

##### Objective:

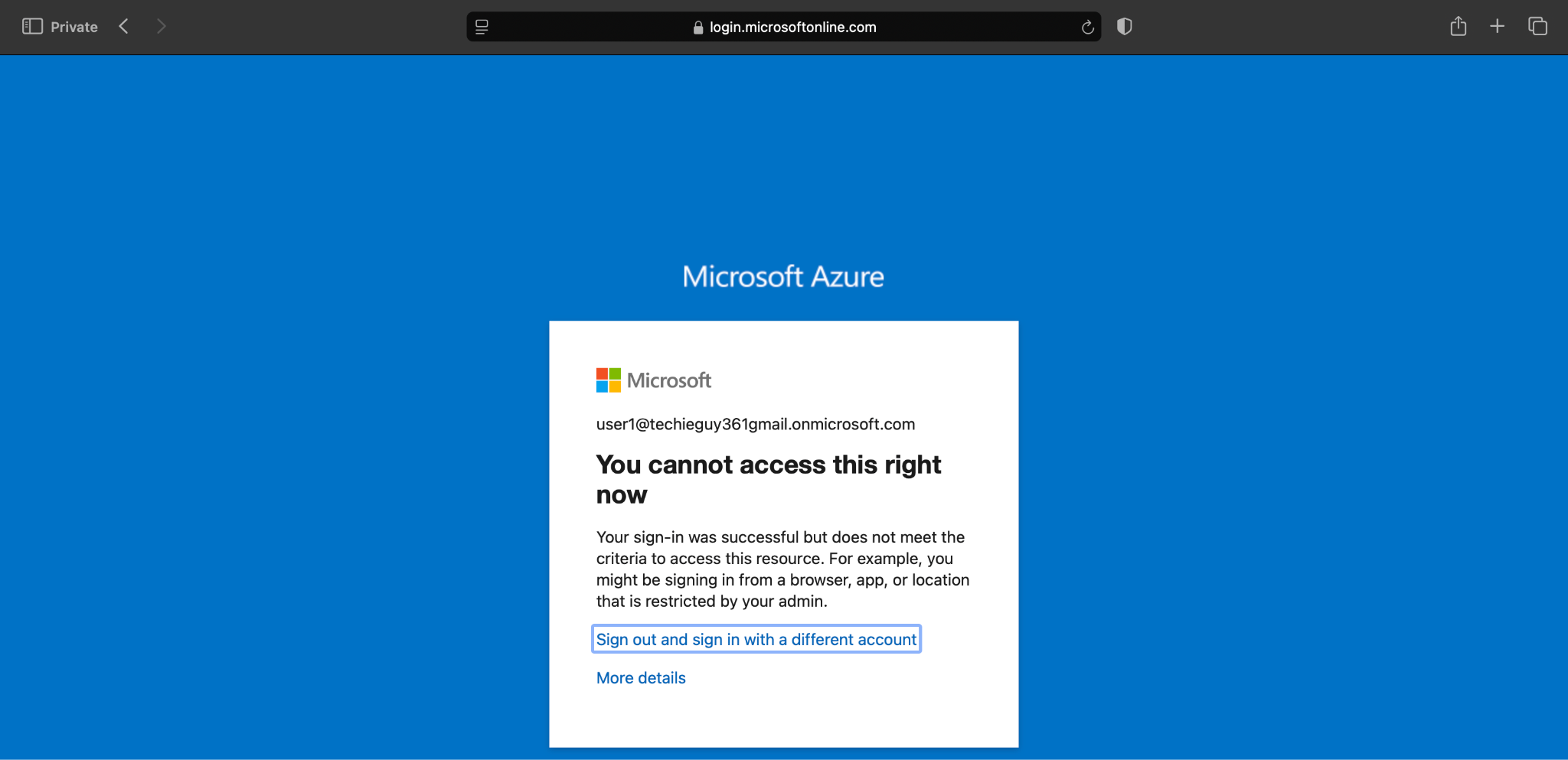
To restrict access to Microsoft Azure services based on **device compliance**, **sign-in risk**, and **user risk**, using **Conditional Access** and **Identity Protection**.

**Simulated Device Compliance via Conditional Access**

* Created CA policy **“Block Unmanaged Device Platforms”**
  + **Users**: user1@<yourtenant>
  + **Cloud apps**: Microsoft Azure Management
  + **Conditions > Device platforms**: Android, iOS, macOS, Linux
  + **Grant**: Block access
* Verified that sign-ins from non-Windows platforms receive a “Blocked by Conditional Access” message.

**Configured Risk-Based Access (Identity Protection)**

* Navigated to **Microsoft Entra ID > Protection > Identity Protection**
* Created **User risk policy**:
  + **Assignment**: user1@<yourtenant>
  + **Action**: Block access if user risk = High
  + **Enable policy**: On
* Created **Sign-in risk policy**:
  + **Assignment**: user1@<yourtenant>
  + **Action**: Require MFA if sign-in risk = Medium or higher
  + **Enable policy**: On
* Tested by simulating a risky sign-in (e.g., impossible travel via VPN) and confirmed MFA challenge or block.



#### **Test Results**

* **Platform block**:
  + Attempted login from iOS simulator → **Access blocked**
* **User risk block**:
  + Simulated high-risk account compromise → **Sign-in blocked**
* **Sign-in risk MFA**:
  + Simulated medium-risk event → **MFA prompt appeared**

Created an Access Package for App-Users group with 14-day expiration and approval flow. Enabled access review post-assignment. This simulates Zero Trust governance with just-in-time access and lifecycle control.

#### Day 5 - Doc:

### Objective:

#### Implement monitoring and alerting for Zero Trust access visibility using Azure Monitor, Log Analytics, and custom dashboards.

#### 

### Tasks Completed:

#### 1. Log Analytics Setup

#### Created a Log Analytics Workspace named ZT-Logs

#### Region: US-East

#### Connected Azure AD Sign-in Logs and Audit Logs to the workspace via Diagnostic Settings

#### 2. Custom Workbook Created

#### Tool Used: Azure Monitor → Workbooks

#### Name: ZT Sign-in Activity Tracker

#### Data Source: Log Analytics Workspace (ZT-Logs)

#### Query Used:

#### kusto

#### CopyEdit

#### SigninLogs

#### | where TimeGenerated > ago(7d)

#### | project TimeGenerated, UserPrincipalName, Location, DeviceDetail, Status, ConditionalAccessStatus, AuthenticationRequirement, MFA = tostring(AuthenticationDetails[0].authenticationMethod), AppDisplayName

#### | sort by TimeGenerated desc

#### 

#### 3. Filters Added

#### Location (to detect sign-ins from risky regions)

#### Device OS (platform-level filtering)

#### MFA method used

#### 4. Alert Created

#### Alert for "Impossible Travel" scenario:

#### Triggered when the same user signs in from two locations in a short time window

#### Action group: Email to admin for investigation

### Summary

#### What is Zero Trust?

#### “Zero Trust is a security framework requiring all users, inside or outside the network, to be authenticated, authorized, and continuously validated before being granted access to applications and data.”

#### Implementation Flow:

#### Identity Setup ➝ Conditional Access ➝ PIM ➝ Governance ➝ Monitoring ➝ Alerts

#### Key Policies Implemented:

#### Block legacy auth

#### Require MFA for admins

#### Block non-compliant devices

#### Sign-in risk-based access control

#### Governance:

#### Just-in-time role activation via PIM

#### App-user access package with approval flow

#### 14-day access review

#### Monitoring:

#### Custom workbook for sign-in activity

#### Alert for impossible travel

#### Risk-based login analysis

#### 