Introduction to Azure PIM Project

Project Overview

This project covers the end-to-end setup and configuration of Microsoft Entra Privileged Identity Management (PIM) in an Azure environment. PIM is a security feature within Microsoft Entra ID (formerly Azure AD) that enables Just-in-Time (JIT) access, approval workflows, time-bound role assignments, and access auditing for highly privileged accounts.

The purpose is to reduce the risk of excessive, unnecessary, or misused access permissions and ensure tighter control over administrative actions within the organization.

Goals of the Project

- Enable Just-In-Time (JIT) activation for highly privileged roles

- Configure MFA, approval, ticketing, and time-limit settings for elevated access

- Set up and test Privileged Access Groups

- Configure and test Break-Glass accounts for emergency use

- Perform Access Reviews and analyze audit logs

- Document the entire implementation with screenshots

Accounts Used

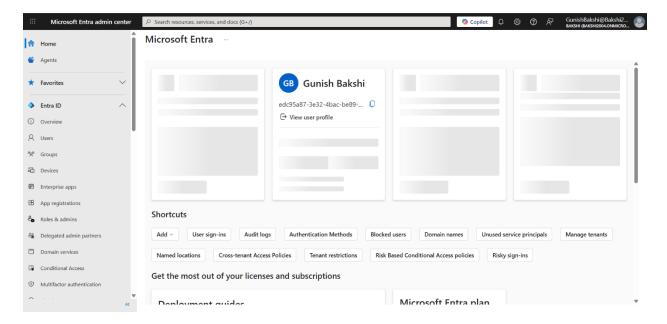| Account	Role	Purpose
GunishBakshi@Bakshi2004.onmicrosoft.com	Global Administrator	Main account used to configure and manage PIM
Admin@Bakshi2004.onmicrosoft.com	Eligible Global Administrator	The account used to send requests and to have the main control of the System.
reviewer@Bakshi2004.onmicrosoft.com	Privileged Role Administrator	Used to approve JIT access requests
breakglass@Bakshi2004.onmicrosoft.com	Permanent Global Administrator	Emergency break-glass account with non-expiring access

Tools and Services Required

- Microsoft Entra ID (Azure AD)
- Microsoft Entra PIM (Privileged Identity Management)
- Identity Governance & Access Reviews
- Azure Portal
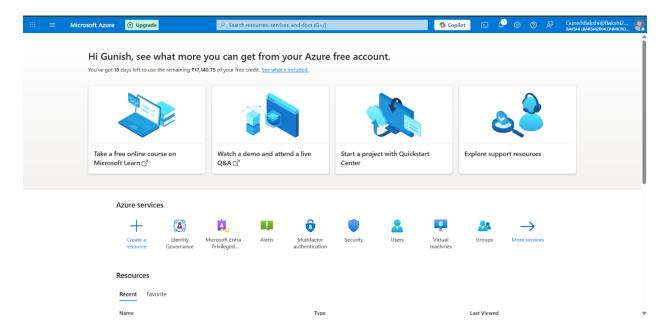- Microsoft Word for documentation

Project Methodology

This implementation is structured into multiple steps. Each step is documented separately and includes:

- Configuration instructions

- Screenshots (with placeholders)

- Descriptions of actions taken

- Final validation results

- Microsoft Entra

- **Azure Portal**