Final Summary: Azure PIM Implementation Project

Project Name

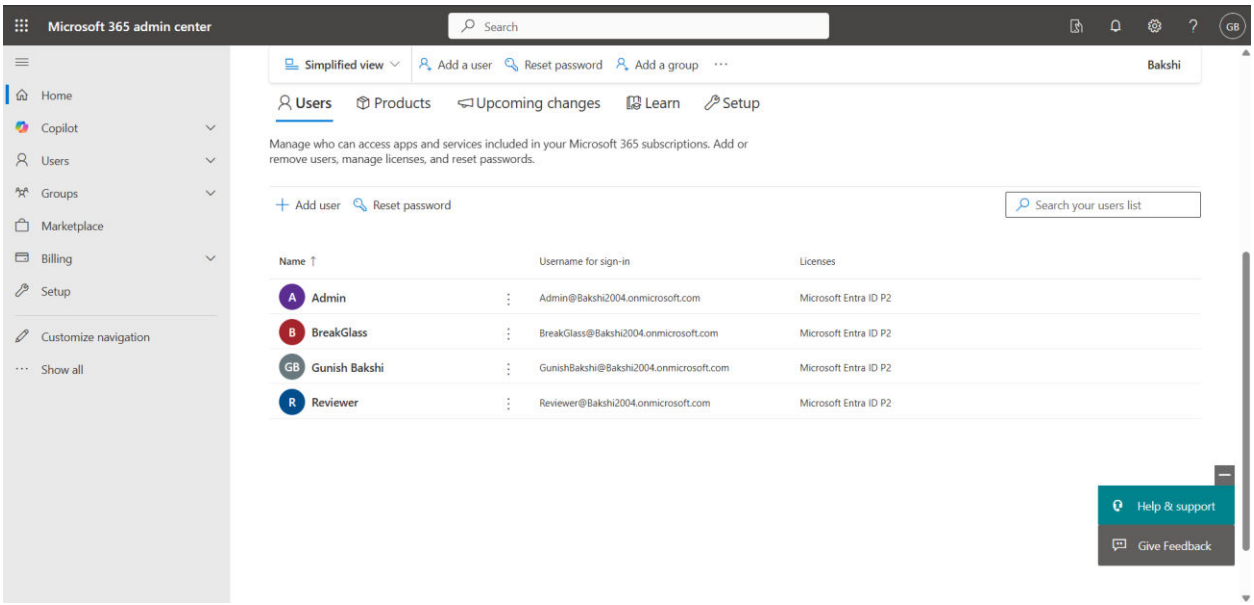
Enhancing Security with Microsoft Entra Privileged Identity Management (PIM)

Objective Recap

This project aimed to secure privileged identities by leveraging Microsoft Entra PIM features such as Just-In-Time access, approval workflows, access reviews, and emergency break-glass accounts. The configuration enforces least-privilege principles and enhances governance across Entra roles and privileged access groups.

Accounts Used

Account	Role	Purpose
GunishBakshi@Bakshi2004.onmicrosoft.com	Global Administrator	Main configuration and management account
admin@Bakshi2004.onmicrosoft.com	Entra Role Administrator	Used to assign and activate roles
reviewer@Bakshi2004.onmicrosoft.com	Privileged Role Administrator	Used to approve JIT access requests
breakglass@Bakshi2004.onmicrosoft.com	Permanent Global Administrator	Used as break-glass account



Steps Completed

Step	Title	Status
1	Overview and Setup Prerequisites for Roles and Licenses	Completed
2	Explore Just-In-Time (JIT) Activation	Completed
3	Configure Entra Roles in PIM: Settings and Assignments	Completed
4	Configure Azure Resources in PIM: Settings and Assignments	Completed
5	Configure Privileged Access Groups	Completed
6	Set Up PIM Requests and Approval Process	Completed
7	Analyze PIM Audit History and Reports	Completed
8	Create and Manage Break-Glass Accounts	Completed
9	Explore Eligible vs Active Roles	Completed
10	Configure Role Time Limits and Access Reviews	Completed

Security Improvements Achieved

- All privileged roles are now time-bound and require JIT activation
- MFA and approval workflows added for role elevation
- Privileged Access Groups streamline access for teams
- Break-glass account created and tested for emergencies
- Regular access reviews scheduled to validate need for privileged access
- Audit logs regularly reviewed to ensure transparency and traceability

Next Steps

- Integrate with ServiceNow for ticket-based activation
- Automate alerting on unusual elevation patterns using Sentinel
- Use Conditional Access policies to further restrict activation context
- Export audit logs to Log Analytics for long-term retention