

Identity and Access Management

Securing Microsoft 365 with Entra ID in Azure

1. Executive Summary

Identity and Access Management (IAM) is the foundation of modern cybersecurity. At its core, IAM answers one critical question: Who are you, and what are you allowed to do? Microsoft Entra ID (formerly Azure Active Directory) is Microsoft's cloud-native IAM platform that provides the identity backbone for Microsoft 365 environments.

This report documents the hands-on configuration of Microsoft Entra ID through a structured project exercise, and explains how each capability — user provisioning, group management, external collaboration, audit logging, and role-based access control — directly strengthens an organization's security posture.

The screenshots embedded throughout this report are taken directly from the project environment and correspond to each task completed.

2. How Entra ID Enhances Microsoft 365 Security

2.1 Part 1 — Environment Setup & Global Administrator Verification

The first step in any IAM implementation is establishing a secure baseline. In this project, a Microsoft Entra ID tenant was created under the Default Directory, and Global Administrator status was confirmed before any configuration work began. Global Administrator is the highest-privilege role in Entra ID — it can manage every aspect of the directory, including creating users, assigning roles, and configuring security policies.

The screenshot below shows the Entra admin center home page confirming the Default Directory, the logged-in administrator with the Global Administrator badge, and the initial state of the tenant before any users or groups were created.

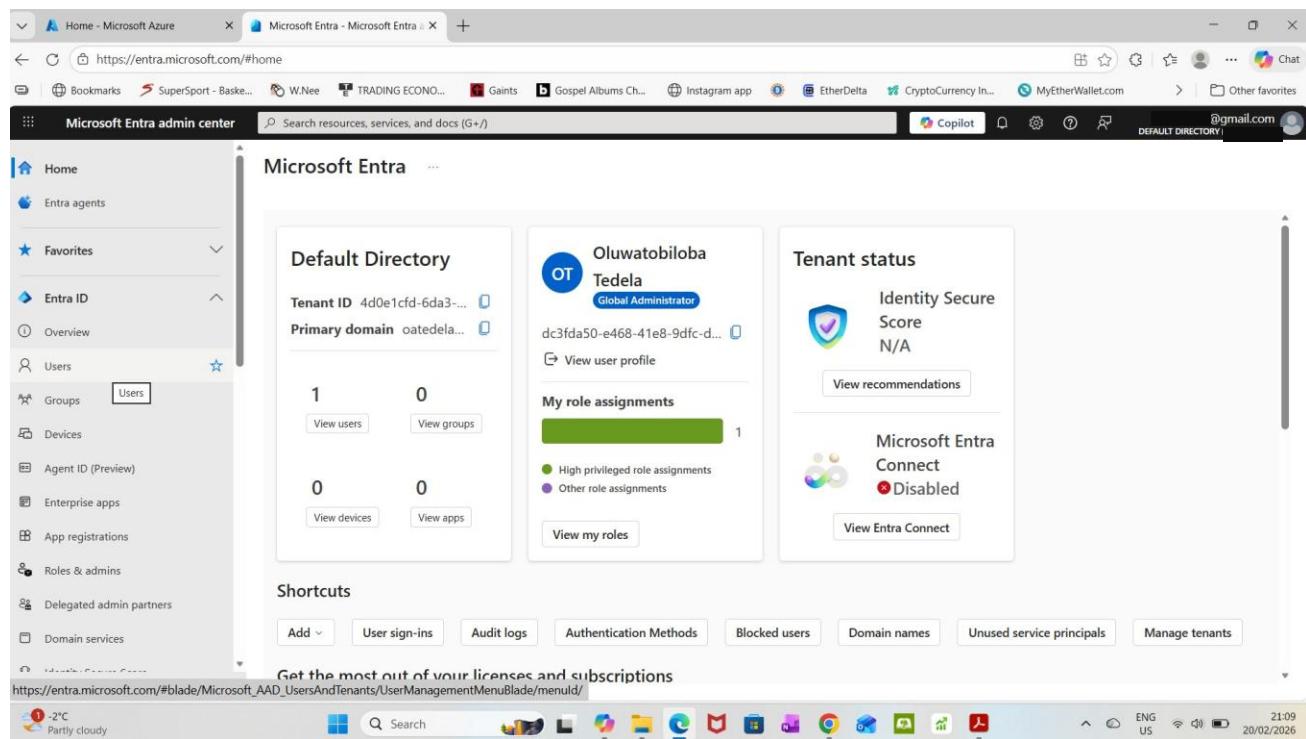


Figure 1: Microsoft Entra admin center — Default Directory confirmed, Global Administrator role verified

2.2 Part 2 — User Provisioning and Role-Based Access Control

Centralized identity management means every person in an organization has one identity that works across all connected services. In this project, three internal users DevUser1, DevUser2, and DevUser3 — were created in the Default Directory. The screenshot below shows the new user creation form for DevUser1, with an auto-generated secure password and the account enabled immediately.

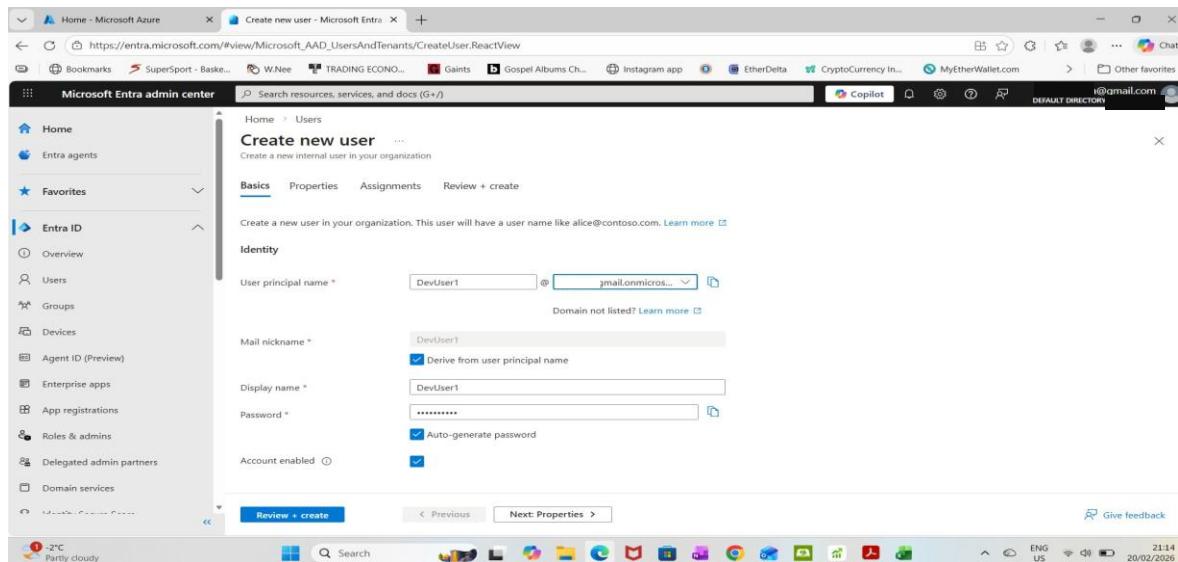


Figure 2: Create new user form — DevUser1 being provisioned with auto-generated password

Role-Based Access Control (RBAC) is the principle of least privilege in action: give users only the permissions they need for their role. DevUser1 was assigned the User Administrator role — a scoped role that allows managing user accounts and group memberships without granting broader administrative privileges. This limits the blast radius if DevUser1's account is ever compromised.

Figure 3: Directory roles panel — User Administrator role selected and assigned to DevUser1

Once all three users were created, the Users list confirmed all accounts were successfully provisioned in the Default Directory. Note that each user has the type 'Member' (internal users), and each has an @###gmail.onmicrosoft.com identity tied to the tenant.

Display name	User principal name	User type	Is Agent	On-premises sync	Identities
DevUser1	DevUser1@...	Member	No	No	gmail.onmicrosoft.com
DevUser2	DevUser2@...	Member	No	No	gmail.onmicrosoft.com
DevUser3	DevUser3@...	Member	No	No	gmail.onmicrosoft.com
Oluwatobiloba Tedela	...	Member	No	No	MicrosoftAccount

Figure 4: Users list — DevUser1, DevUser2, DevUser3, and admin account (4 users total at this stage)

2.3 Part 2 — Group-Based Access Control

Managing permissions for individuals doesn't scale. Security groups solve this by bundling users and applying permissions to the entire group. When a user joins or leaves a group, their access updates automatically. The Groups overview below shows the starting point before the AppDevTeam group was created.

Total groups	Dynamic groups
0	0

M365 groups	Cloud groups
0	0

Security groups	On-premises groups
0	0

Figure 5: Groups overview — Security group creation initiated in Default Directory

The AppDevTeam security group was created and DevUser1 and DevUser2 were added as members during group creation. The screenshot below shows the 'Add members' dialog with both DevUser1 and DevUser2 selected (highlighted in blue on the right panel), ready to be assigned to the AppDevTeam group.

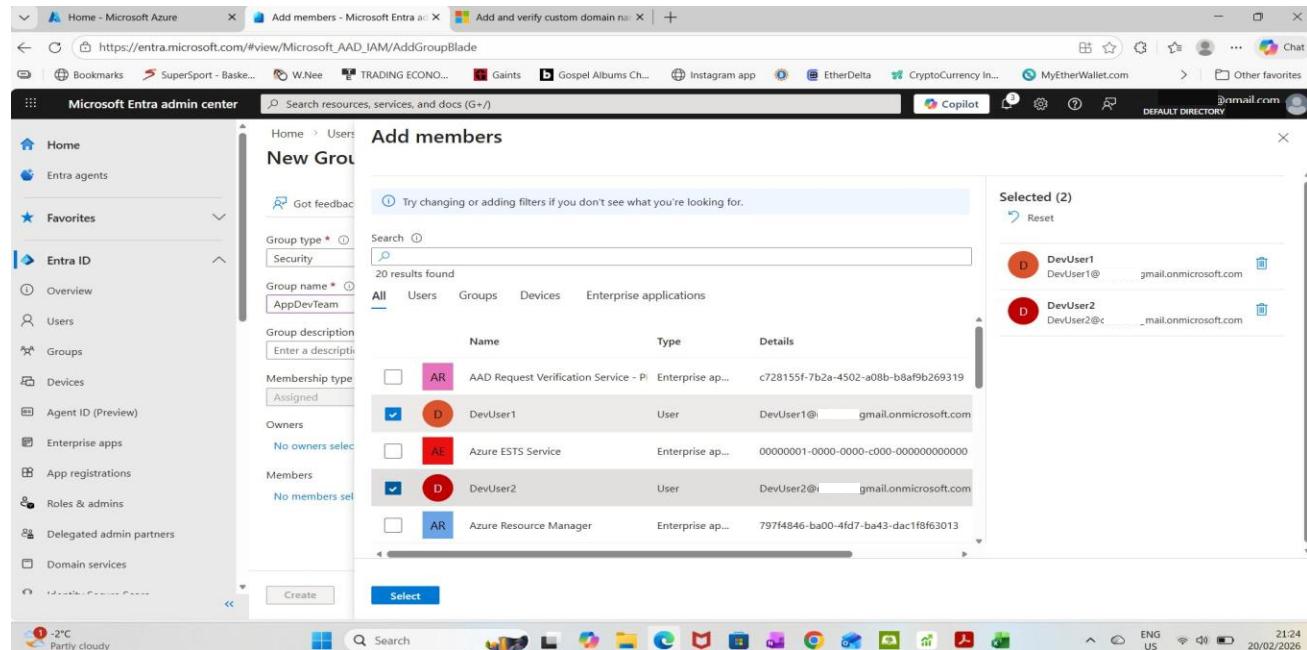


Figure 6: Add members dialog — DevUser1 and DevUser2 selected as AppDevTeam members

2.4 Part 3 — External Collaboration (B2B Guest Access)

Modern organizations regularly collaborate with contractors, partners, and vendors who need temporary access to internal resources. Entra ID's B2B (Business-to-Business) capability allows external users to be invited as guests using their own existing identity. This approach is more secure than creating internal accounts for external users because the external user manages their own credentials, their home organization's security policies apply to their authentication, and access can be instantly revoked without managing a separate password.

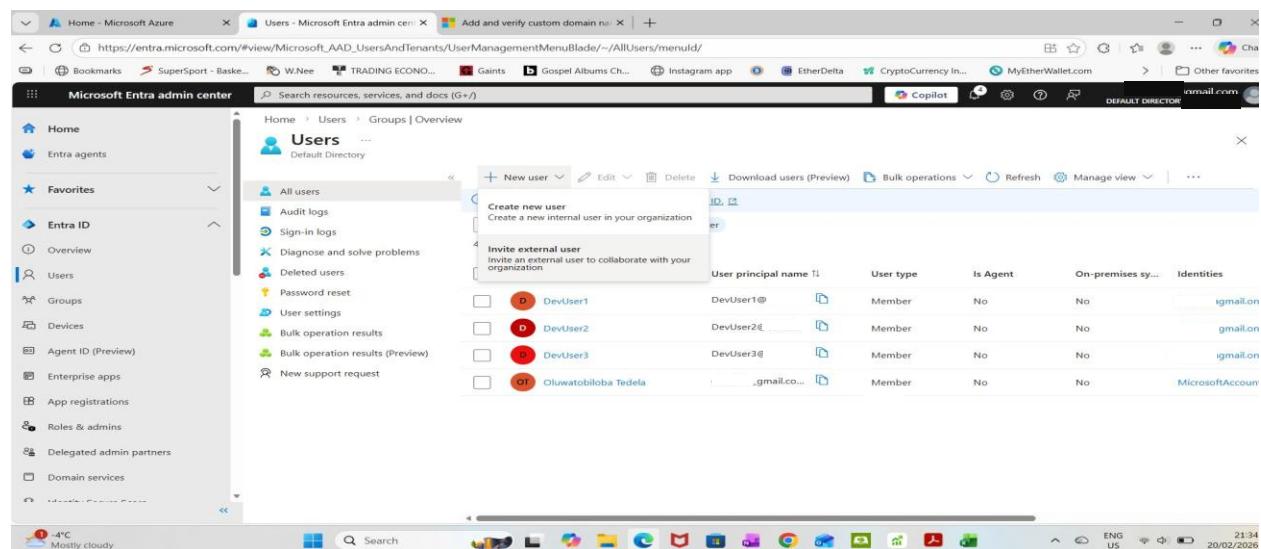


Figure 7: Invite external user option — B2B guest invitation initiated from the Users panel

After the invitation was sent, the external user was added to the AppDevTeam group, granting them the same resource access as internal members while keeping their identity separate from the internal directory.

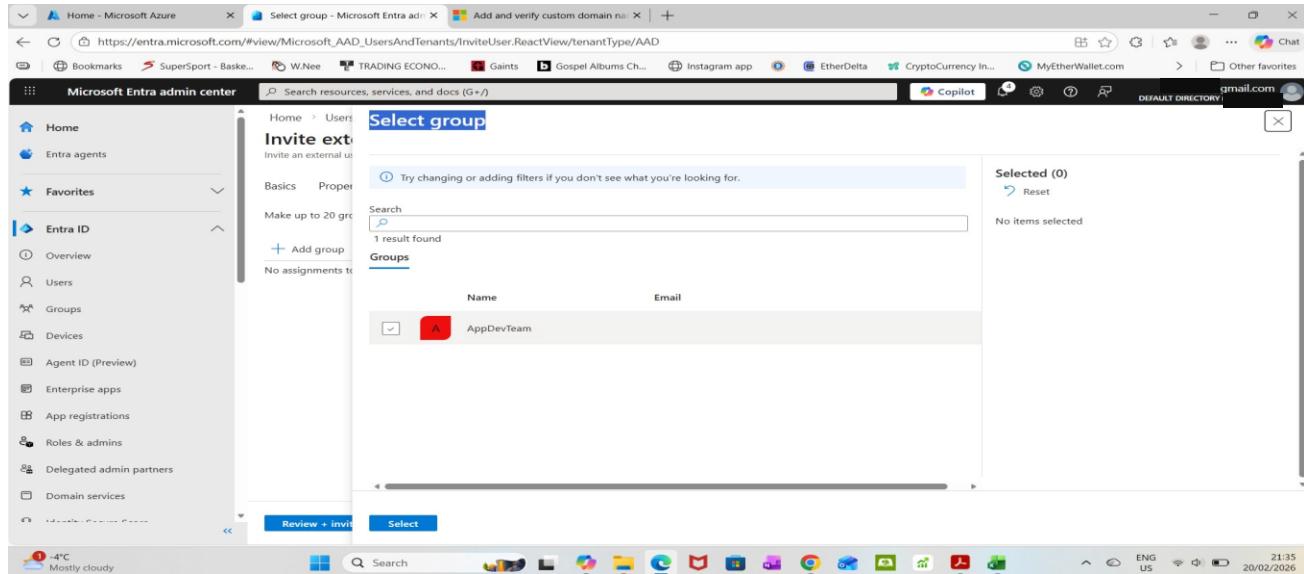


Figure 8: Select group dialog — AppDevTeam selected to add the external (guest) user as a member

2.5 Part 4 — Reporting: User and Group Export

Visibility into who has access to what is a fundamental security requirement. Entra ID provides built-in reporting and bulk export capabilities that allow administrators to generate snapshots of all users, their roles, and group memberships. These reports are critical for access reviews, compliance audits, and detecting unauthorized changes.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes 'Home', 'Entra agents', 'Favorites', 'Entra ID', 'Overview', 'Users', 'Groups', 'Devices', 'Agent ID (Preview)', 'Enterprise apps', 'App registrations', 'Roles & admins', 'Delegated admin partners', and 'Domain services'. The main area is titled 'Users' and shows a list of users: DevUser1, DevUser2, DevUser3, Oluwatobiloba Tedela, and Tobi. To the right, a 'Download users' panel is open, prompting the user to select filters and providing options to download 'AllUsersAndRoles.csv'. The status bar at the bottom right shows the date as 20/02/2026 and the time as 22:20.

Figure 9: Download users panel — 'AllUsersAndRoles' report initiated for all 5 users

Similarly, the AppDevTeam group members were exported. The group now shows 3 members: DevUser1, DevUser2 (internal), and Tobi (the external guest user). The download panel shows 'GroupAndMemberships' as the report filename.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has sections for Home, Entra agents, Favorites, and Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services). The main area shows the 'AppDevTeam | Members' group. The 'Members' tab is selected in the navigation pane. A table lists three members:

Name	Type	Email
DevUser1	User	
DevUser2	User	
Tobi	User	@gmail.com

A 'Start bulk operation' button is visible on the right side of the screen.

Figure 10: AppDevTeam members with export — DevUser1, DevUser2, and guest user Tobi; 'GroupAndMemberships' report exported

2.6 Part 5 — Security: Consent Governance and Identity Secure Score

One of the most overlooked attack vectors in Microsoft 365 environments is OAuth consent phishing — where users are tricked into granting malicious applications access to their data. Entra ID's consent governance policies prevent this by restricting which applications users can authorize. The screenshot below shows the Identity Secure Score dashboard, which provides a quantitative measure of the tenant's security posture against Microsoft's best practices.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has sections for Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, Account recovery (Preview), Password reset, and Custom security attributes. The main area shows the 'Security | Identity Secure Score' dashboard. The score is displayed as 'N/A'. A chart titled 'Score History' shows a line starting at 100 and dropping to 50. Below the chart, there are four tabs: All (0), Security (0), Best practice (0), and Microsoft Defender for Identity (0). A 'Search by recommendation' field and a 'Priority' filter are also present.

Figure 11: Security | Identity Secure Score — Score shown as N/A on the Free tier (scores require P1/P2 licensing)
The Enterprise Applications panel provides the entry point for managing how applications integrate with the directory. From here, Consent and permissions policies were configured to prevent unauthorized application access.

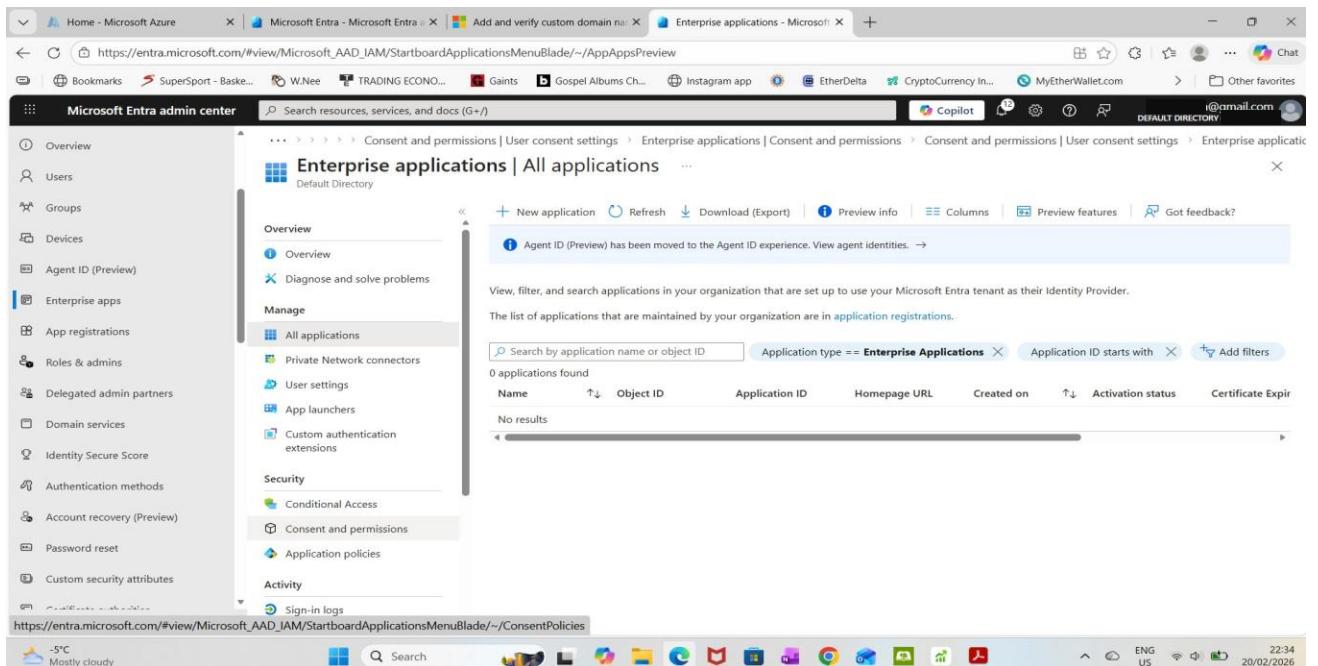


Figure 12: Enterprise Applications — Consent and permissions management accessed for security configuration

The most critical security change in Part 5 was setting user consent to 'Do not allow user consent.' This means users cannot independently grant third-party applications access to organizational data — all app consent must go through an administrator. This eliminates the OAuth phishing attack surface entirely.

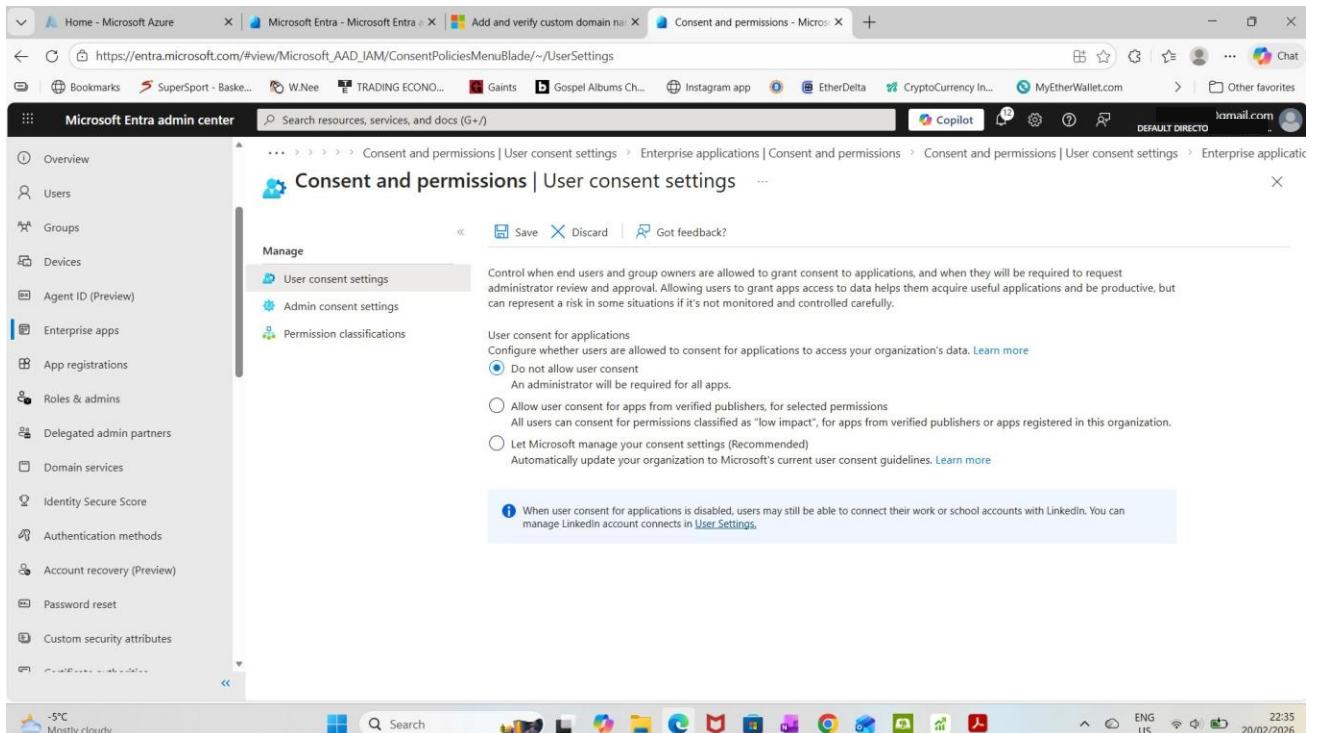


Figure 13: User consent settings — 'Do not allow user consent' enabled; administrator approval required for all application access

An admin consent workflow was then configured: users can request access to new applications, but a designated reviewer must approve before any access is granted. DevUser3 was selected as the reviewer, as shown below.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Overview, Users, Groups, Devices, etc. The main area is titled "Select admin consent request reviewers". It has a search bar and a table listing users. The user "DevUser3" is highlighted with a blue selection bar and checked in the "Selected reviewers" list on the right. The status bar at the bottom shows it's 22:37 on 20/02/2026.

Figure 14: Select admin consent reviewers — DevUser3 assigned as the consent request reviewer

The consent request expiry was adjusted from the default 30 days (shown below left) to 2 days (shown below right), ensuring stale or unreviewed requests expire quickly and do not accumulate as an ongoing risk.

This screenshot shows the "Consent and permissions | Admin consent settings" page. In the "Admin consent requests" section, the "Users can request admin consent to apps they are unable to consent to" option is set to "Yes". The "Who can review admin consent requests" section shows "Users" selected under "Reviewer type" and "1 user selected" under "Reviewers". The "Selected users will receive email notifications for requests" and "Selected users will receive request expiration reminders" options are both set to "Yes". At the bottom, the "Consent request expires after (days)" field is set to 30. The status bar at the bottom shows it's 22:37 on 20/02/2026.

Figure 15: Admin consent settings — default expiry of 30 days (before adjustment)

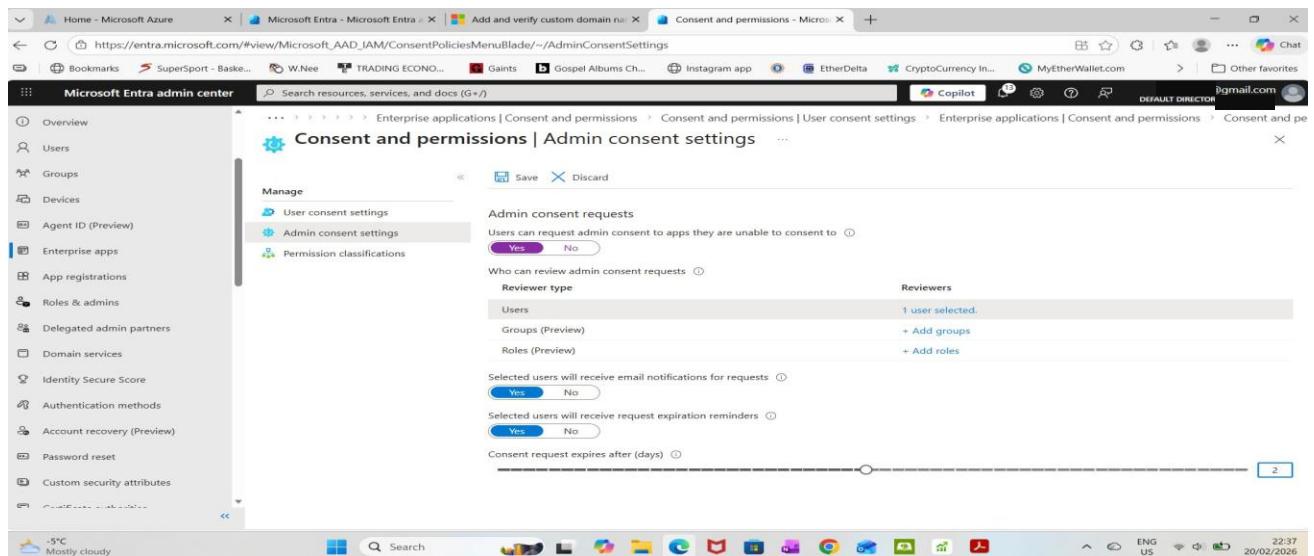


Figure 16: Admin consent settings — expiry reduced to 2 days, DevUser3 confirmed as reviewer (1 user selected)

2.7 Part 6 — Monitoring: Audit Logs and Sign-in Events

Security without visibility is ineffective. Entra ID provides two critical monitoring capabilities. Audit Logs are a tamper-proof record of every administrative action, who created a user, who changed a role, who modified a policy, and exactly when. Sign-in Logs record every authentication attempt, who signed in, from where, on which device, and whether it succeeded or failed.

These logs are the foundation of incident response. If a security event occurs, audit and sign-in logs answer the key forensic questions: What happened? When? Who did it? The audit log below shows all actions performed during the project session, including CreateBulkJob (user provisioning), RoleManagement (role assignments), and B2C Authentication (external user validation) — all with a status of Success.

Date	Service	Category	Activity	Status	Status Reason
20/02/2026, 22:33:57	Core Directory	AuthorizationPolicy	Update authorization p...	Success	
20/02/2026, 22:33:57	Core Directory	RoleManagement	Update role	Success	
20/02/2026, 22:33:57	Core Directory	RoleManagement	Add role from template	Success	
20/02/2026, 22:25:43	B2C	Authentication	Validate user authenticatio...	Success	Token is valid
20/02/2026, 22:25:38	AAD Management UX	DirectoryManagement	DeleteBulkJob	Success	
20/02/2026, 22:25:33	AAD Management UX	DirectoryManagement	DeleteBulkJob	Success	
20/02/2026, 22:20:30	AAD Management UX	DirectoryManagement	CreateBulkJob	Success	
20/02/2026, 22:19:27	Self-service Group Man...	GroupManagement	GroupsODataV4_Get	Success	OK
20/02/2026, 22:19:17	Self-service Group Man...	GroupManagement	GroupsODataV4_Get	Success	OK

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has 'Monitoring & health' selected, with 'Audit logs' under 'Sign-in logs'. The main area is titled 'Audit Logs'. It shows a table of audit events with columns: Date, Service, Category, Activity, Status, and Status Reason. The table lists several events, mostly from 'Core Directory' and 'AAD Management UX', involving actions like 'Update authorization', 'Update role', 'Add role from template', 'Validate user authentication', 'DeleteBulkJob', 'CreateBulkJob', and 'GroupsODataV4_Get'. All events show a 'Status' of 'Success'. The status bar at the bottom shows the date as 20/02/2026.

Figure 17: Audit Logs — Complete activity trail showing user creation, role management & B2C authentication events

The Sign-in events log confirms successful logins by the administrator account.

Date	Request ID	User principal name	Application	Status	IP address	Resource
2026-02-21T02:09:45Z	d30bef66-1647-49e6-9806-a382...	@gmail.com	Azure Portal	Success	5	Azure Resource #
2026-02-21T01:06:05Z	cc9fde2b-9169-42ee-a6dc-e5b7...	@gmail.com	Azure Portal	Success	5	Azure Resource #
2026-02-21T01:05:26Z	cad1da38-4eea-41db-90c6-6ccf2...	@gmail.com	Azure Portal	Success	5	Azure Resource #
2026-02-21T01:05:23Z	cc9fde2b-9169-42ee-a6dc-e5b7...	@gmail.com	Azure Portal	Success	1 ... 5	Azure Resource #

Figure 18: Sign-in events Successful authentication sessions for the administrator account across the project session

3. Project Deliverables Summary

The following table maps each project part to the action performed and the figure number in this report:

Part	Action	Figure	Key Outcome
1	Verified Default Directory & Global Admin status	Fig. 1	Secure baseline established
2	Created DevUser1-3; assigned User Administrator to DevUser1; created AppDevTeam security group with DevUser1 & DevUser2	Fig. 2–6	RBAC & centralized identity in place
3	Invited external user (Tobi) via B2B; added to AppDevTeam	Fig. 7–8	Secure external collaboration enabled
4	Generated AllUsersAndRoles and GroupAndMemberships CSV reports	Fig. 9–11	Audit-ready user and group reports
5	Blocked user consent; set DevUser3 as reviewer; set 2-day expiry on consent requests	Fig. 12–17	OAuth phishing surface eliminated
6	Reviewed audit logs and sign-in events for suspicious activity	Fig. 17–18	Full monitoring visibility confirmed

4. Conclusion

Identity is the new perimeter. Microsoft Entra ID provides a comprehensive, layered approach to securing Microsoft 365 environments by controlling who can access what, under which conditions, and with full visibility into every action taken. The capabilities demonstrated in this project — from basic user provisioning to external collaboration, consent governance, and audit logging — each address a specific, real-world category of security risk.