Project: Azure Security: Emergency Access ("Break-Glass") Implementation

Author	Saidou Abdou Ahmadou
Date	January 30, 2026

1. Executive Summary

To align with Microsoft's Identity Security standards, this project implements a resilient "Break-Glass" strategy. The goal is to prevent total tenant lockout during MFA service outages by configuring a cloud-only emergency account with high-priority Conditional Access exclusions.

2. The Configuration

Step 1: Identity Creation

Objective: Create a dedicated account independent of on-premise infrastructure.

- **Action:** Provisioned a cloud-only Global Administrator (admin-emergency) on the *.onmicrosoft.com domain. This ensures the account remains accessible even if on-premise federation or DNS services fail.
- **Account:** admin-emergency@frcay1gmail.onmicrosoft.com

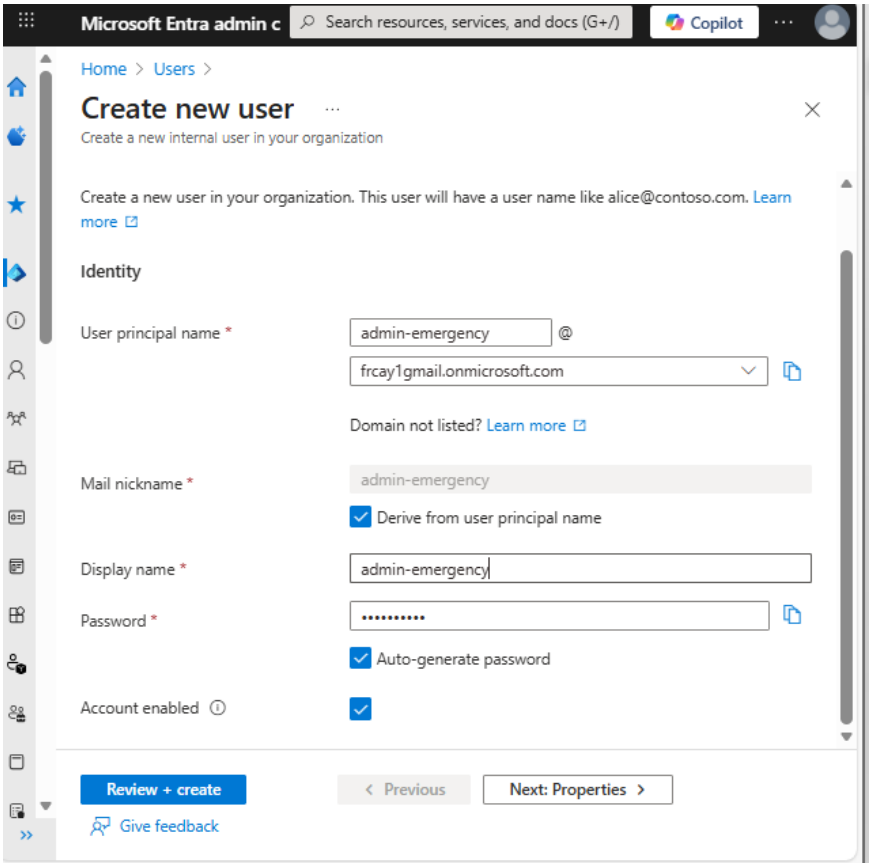

Figure 1 User Creation

Step 2: Role Assignment

Objective: Grant sufficient privileges for tenant recovery.

- **Action:** Assigned the permanent **Global Administrator** role. This account is strictly reserved for emergency recovery scenarios and is monitored for any unauthorized usage.

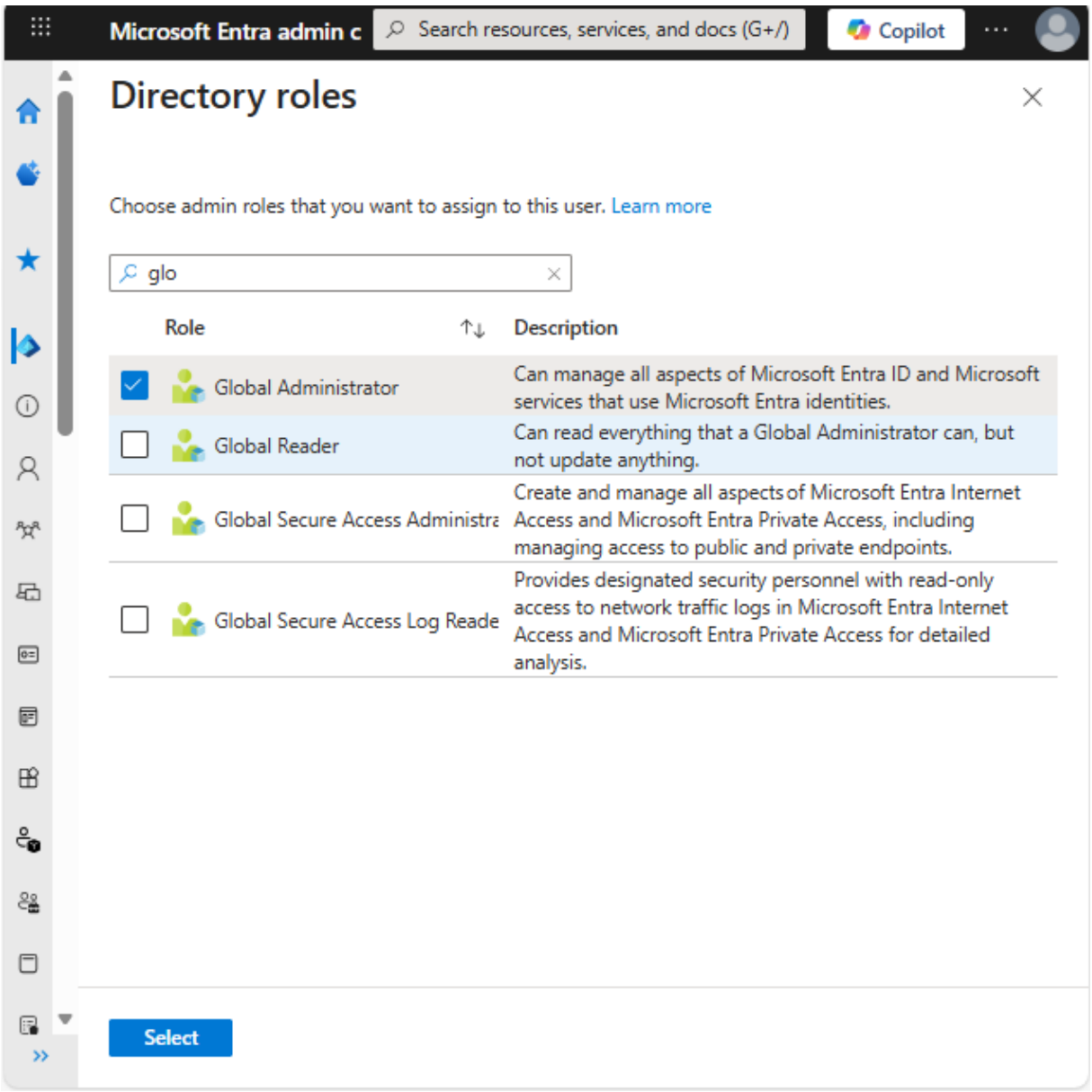

Figure 2 Directory Roles

Step 3: Security Baseline & Exclusion

Objective: Enforce security for the organization while exempting the emergency account.

- **Action:** Designed a "Baseline - Require MFA" Conditional Access policy for the tenant. Configured a critical **Exclusion Group** for the emergency identity, ensuring it bypasses MFA enforcement during service disruptions.

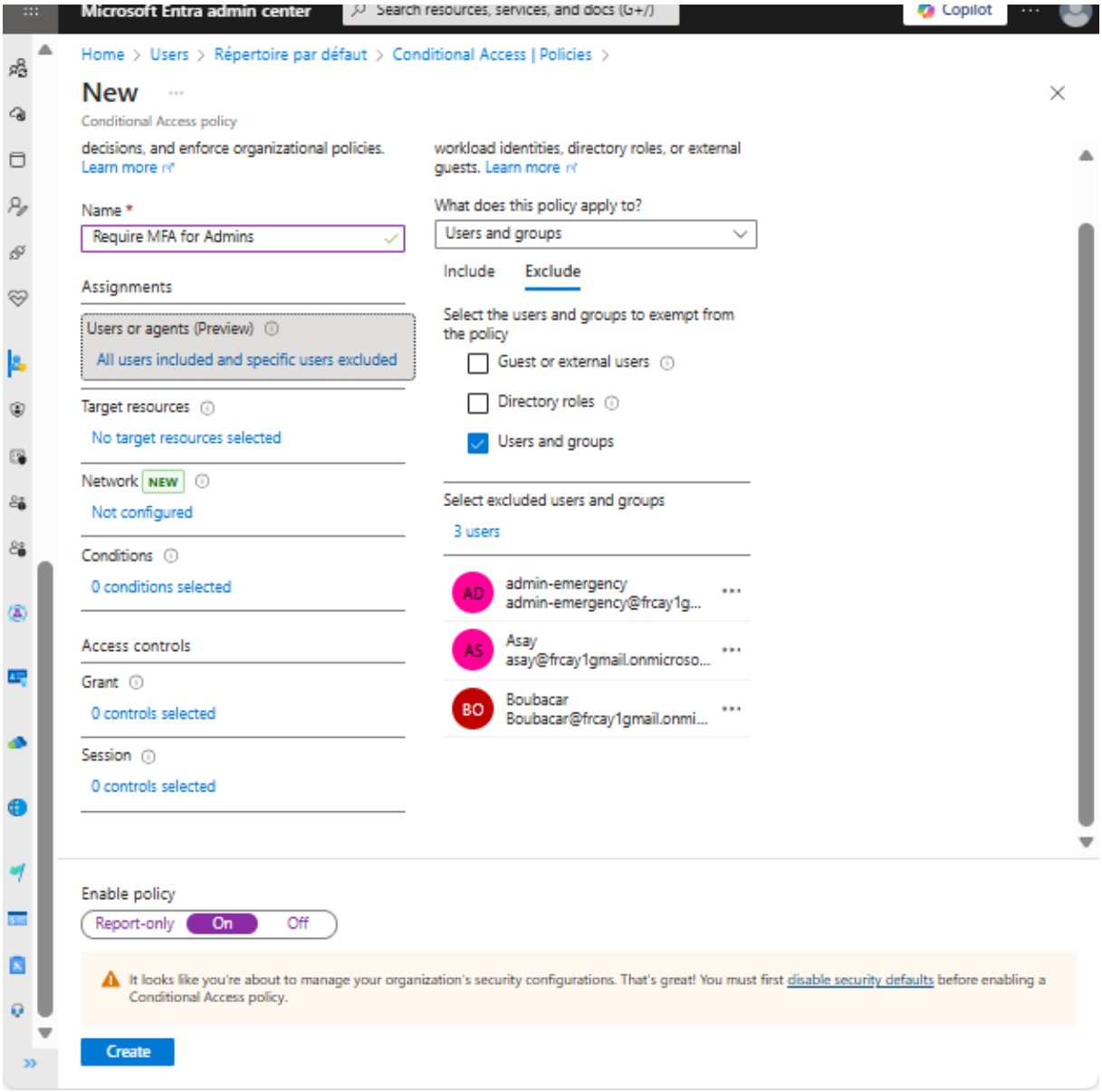

Figure 3 Conditional Access Exclusion

3. Validation

Step 4: Sign-In Test

Objective: Verify that the exclusion logic functions correctly.

- **Action:** Conducted a sign-in simulation using a test administrator account (Asay) to confirm the MFA bypass logic.

- **Result:** The Sign-in Logs confirm that Conditional Access was **"Not Applied"**, successfully granting access without an MFA prompt due to the configured exclusion.

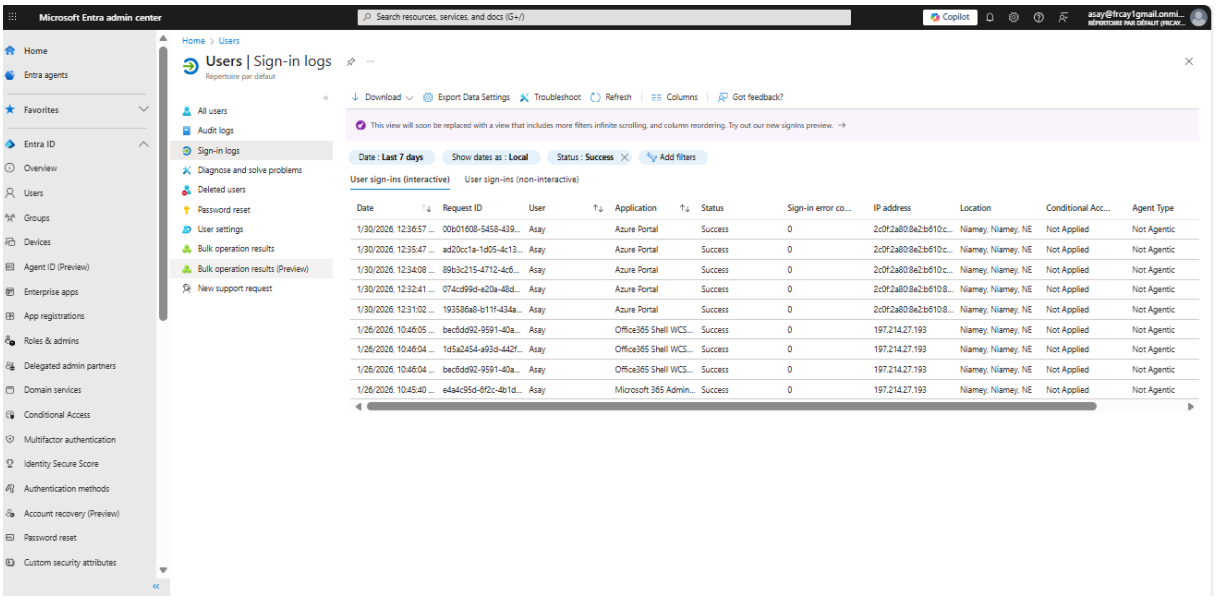

Figure 4 Sign-in Logs