

## 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

The screenshot displays the 'Create new user' interface in the Microsoft Entra admin center. The breadcrumb navigation shows 'Home > Users >'. The title is 'Create new user' with a close button. Below the title, it says 'Create a new internal user in your organization'. A descriptive text states: 'Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)'. The 'Identity' section contains the following fields and options:

- User principal name \***: A text box with 'admin-emergency' and a dropdown menu with 'frcay1gmail.onmicrosoft.com'. A link 'Domain not listed? [Learn more](#)' is present.
- Mail nickname \***: A text box with 'admin-emergency'. A checkbox 'Derive from user principal name' is checked.
- Display name \***: A text box with 'admin-emergency'.
- Password \***: A text box with masked characters. A checkbox 'Auto-generate password' is checked.
- Account enabled**: A checkbox that is checked.

At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next: Properties >'. A 'Give feedback' link is located at the bottom left.

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.

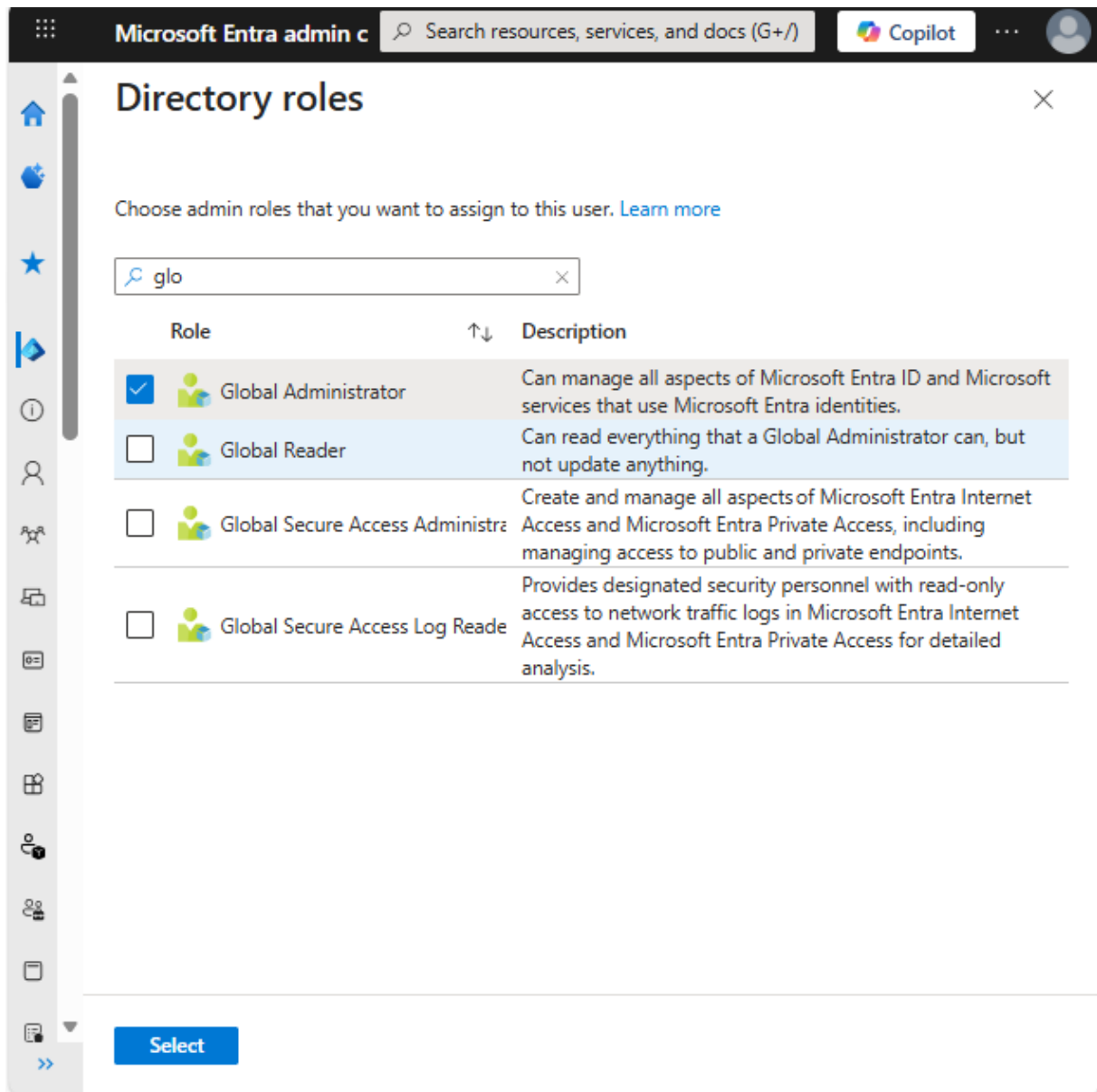


Figure 2 Directory Roles

## 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.

Microsoft Entra admin center

Home > Users > Répertoire par défaut > Conditional Access | Policies >

## New

Conditional Access policy

decisions, and enforce organizational policies. [Learn more](#)

**Name \***  
Require MFA for Admins ✓

**What does this policy apply to?**  
Users and groups

**Include** **Exclude**

Select the users and groups to exempt from the policy

☐ Guest or external users

☐ Directory roles

☒ Users and groups

Select excluded users and groups

3 users

- AD admin-emergency  
admin-emergency@frcay1g...
- AS Asay  
asay@frcay1gmail.onmicroso...
- BO Boubacar  
Boubacar@frcay1gmail.onmi...

**Assignments**

Users or agents (Preview)

All users included and specific users excluded

**Target resources**

No target resources selected

**Network** NEW

Not configured

**Conditions**

0 conditions selected

**Access controls**

**Grant**

0 controls selected

**Session**

0 controls selected

**Enable policy**

Report-only **On** Off

⚠ It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy.

Create

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.

Microsoft Entra admin center

Home > Users

Users | Sign-in logs

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date: Last 7 days Show dates as: Local Status: Success Add filters

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User	Application	Status	Sign-in error co...	IP address	Location	Conditional Acc...	Agent Type
1/30/2026, 12:36:57 ...	00b01608-5458-439...	Asay	Azure Portal	Success	0	2c0f2a809e2b6f10c...	Niamey, Niamey, NE	Not Applied	Not Agentic
1/30/2026, 12:35:47 ...	ad20c1a-1d05-4c13...	Asay	Azure Portal	Success	0	2c0f2a809e2b6f10c...	Niamey, Niamey, NE	Not Applied	Not Agentic
1/30/2026, 12:34:08 ...	89b3c215-4712-4ed...	Asay	Azure Portal	Success	0	2c0f2a809e2b6f10c...	Niamey, Niamey, NE	Not Applied	Not Agentic
1/30/2026, 12:32:41 ...	074cd99d-420a-48d...	Asay	Azure Portal	Success	0	2c0f2a809e2b6f10c...	Niamey, Niamey, NE	Not Applied	Not Agentic
1/30/2026, 12:31:02 ...	193586a8-b11f-434a...	Asay	Azure Portal	Success	0	2c0f2a809e2b6f10c...	Niamey, Niamey, NE	Not Applied	Not Agentic
1/26/2026, 10:46:05 ...	becdd92-9591-40a...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Niamey, Niamey, NE	Not Applied	Not Agentic
1/26/2026, 10:46:04 ...	1d5a2454-a93d-442f...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Niamey, Niamey, NE	Not Applied	Not Agentic
1/26/2026, 10:46:04 ...	becdd92-9591-40a...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Niamey, Niamey, NE	Not Applied	Not Agentic
1/26/2026, 10:45:40 ...	e4a4c95d-472c-4b1d...	Asay	Microsoft 365 Admin...	Success	0	197.214.27.193	Niamey, Niamey, NE	Not Applied	Not Agentic

Figure 4 Sign-in Logs