

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 shows the Microsoft Entra admin center interface for creating a new user. The 'Identity' section is selected. The 'User principal name' field contains 'admin-emergency' followed by '@' and a dropdown menu showing 'frcay1gmail.onmicrosoft.com'. Below it, the 'Mail nickname' field is 'admin-emergency' with a checked checkbox for 'Derive from user principal name'. The 'Display name' field is 'admin-emergency'. The 'Password' field contains '*****' with a checked checkbox for 'Auto-generate password'. The 'Account enabled' checkbox is checked. At the bottom, there are 'Review + create' and 'Next: Properties' buttons, along with a 'Give feedback' link.

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.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Microsoft Entra admin c', a search bar ('Search resources, services, and docs (G+/)'), 'Copilot' (with a person icon), and a three-dot menu. On the left is a vertical sidebar with various icons. The main content area is titled 'Directory roles' and contains a message: 'Choose admin roles that you want to assign to this user.' Below is a search bar with 'glo' typed in. A table lists four roles:

Role	Description
<input checked="" type="checkbox"/> Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.
<input type="checkbox"/> Global Reader	Can read everything that a Global Administrator can, but not update anything.
<input type="checkbox"/> Global Secure Access Administra	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.
<input type="checkbox"/> Global Secure Access Log Read	Provides designated security personnel with read-only access to network traffic logs in Microsoft Entra Internet Access and Microsoft Entra Private Access for detailed analysis.

At the bottom left is a 'Select' button.

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.

New Conditional Access policy decisions, and enforce organizational policies. Learn more [↗](#)

Name * What does this policy apply to?

Assignments Select the users and groups to exempt from the policy

Target resources

Network Select excluded users and groups

Conditions 3 users

Access controls admin-emergency
admin-emergency@friday1g... ***

Grant Asay
asay@friday1gmail.onmicroso... ***

Session Boubacar
Boubacar@friday1gmail.onmi... ***

Enable policy

⚠️ 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.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Entrra agents, Favorites, Entrra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Account recovery (Preview), Password reset, and Custom security attributes. The main area is titled "Users | Sign-in logs" and displays a table of sign-in logs. The table has columns for Date, Request ID, User, Application, Status, Sign-in error co..., IP address, Location, Conditional Acc..., and Agent Type. The data shows multiple successful sign-ins (Status: Success) from different sources (Azure Portal, Office365 Shell WCS...) over a period of time (1/30/2026 to 1/26/2026). All entries in the Conditional Acc... and Agent Type columns are listed as "Not Applied" and "Not Agentic".

Date	Request ID	User	Application	Status	Sign-in error co...	IP address	Location	Conditional Acc...	Agent Type
1/30/2026 12:38:57 ...	00b01600-545b-439...	Asay	Azure Portal	Success	0	2c0f2a008a2b510...	Namey, Namey, NE	Not Applied	Not Agentic
1/30/2026 12:35:47 ...	ad20cc1a-1d05-4c13...	Asay	Azure Portal	Success	0	2c0f2a008a2b510...	Namey, Namey, NE	Not Applied	Not Agentic
1/30/2026 12:34:08 ...	69bc3c15-4712-4cd...	Asay	Azure Portal	Success	0	2c0f2a008a2b510...	Namey, Namey, NE	Not Applied	Not Agentic
1/30/2026 12:32:41 ...	074cd99d-e20a-48d...	Asay	Azure Portal	Success	0	2c0f2a008a2b510...	Namey, Namey, NE	Not Applied	Not Agentic
1/30/2026 12:31:02 ...	193586a8-b11f-434...	Asay	Azure Portal	Success	0	2c0f2a008a2b510...	Namey, Namey, NE	Not Applied	Not Agentic
1/26/2026 10:46:05 ...	be0dd992-5591-40a...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Namey, Namey, NE	Not Applied	Not Agentic
1/26/2026 10:46:04 ...	1d5a2454-93d4-42f...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Namey, Namey, NE	Not Applied	Not Agentic
1/26/2026 10:45:40 ...	bef6dd92-5591-40a...	Asay	Office365 Shell WCS...	Success	0	197.214.27.193	Namey, Namey, NE	Not Applied	Not Agentic
1/26/2026 10:45:40 ...	e4a4c95d-bf2c-4b1d...	Asay	Microsoft 365 Admin...	Success	0	197.214.27.193	Namey, Namey, NE	Not Applied	Not Agentic

Figure 4 Sign-in Logs