M365 Administration Runbook #004

How to Set Up Conditional Access Policies

Policy design & documentation - requires Entra ID P1 (not available in this lab)

Lab Environment | Entra ID P1 Required | 45 min | Theoretical

Jean Claude Munyakazi

IT Systems Administrator | Berlin, Germany | munyakazi.org

⚠ Lab Limitation - Licence Not Available

This runbook was NOT executed in the live lab tenant.

Reason: Conditional Access requires Entra ID P1 (M365 Business Premium, E3 or E5). This lab runs on M365 Business Standard - Conditional Access is not available at this licence tier.

What this runbook contains:

→ Policy design based on Microsoft official documentation

→ Step-by-step configuration as it would be performed with the correct licence

→ Screenshots replaced with placeholder frames - no live tenant access

→ All scenarios and best practices sourced from Microsoft Learn documentation

Real-world note: In production, Conditional Access would be the first policy configured after MFA. It is included here to demonstrate understanding of the full M365 security stack.

What You Will Learn

HOW CONDITIONAL ACCESS WORKS

IF user attempts to sign in
AND conditions are met (location, device, risk)
THEN grant / block / require MFA

3 Policies built in this Runbook:
→ Block sign-in from outside Germany
→ Require MFA for admin accounts
→ Block legacy authentication protocols

POLICY 1

Block non-Germany sign-ins

Any sign-in from outside Germany is blocked. MOS operates from Berlin only.

POLICY 2

Require MFA for admins

All admin directory roles must complete MFA at every sign-in.

POLICY 3

Block legacy authentication

POP3, IMAP, SMTP bypass MFA - block these protocols entirely.

Lab Note: This runbook was designed on M365 Business Standard which does NOT include Entra ID P1. The Conditional Access menu was not accessible in this lab. All steps and policies documented here are based on Microsoft documentation and represent intended configuration - they were not executed in the live tenant.

Prerequisites

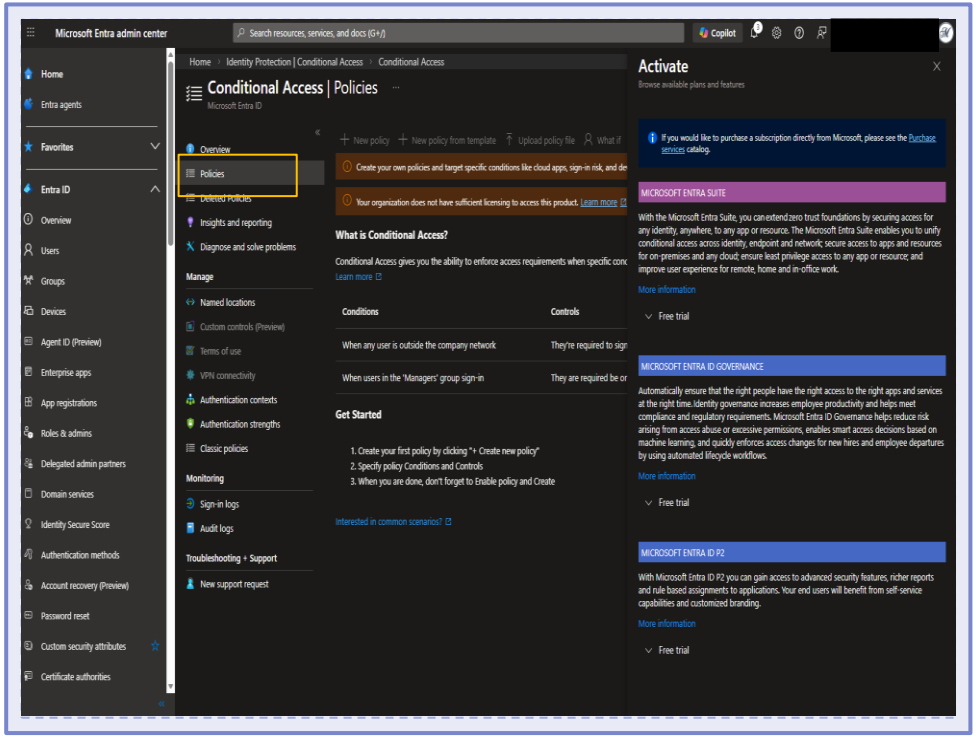
Requirement	Details
Admin Role	Conditional Access Administrator or Global Administrator
Licence Required	Entra ID P1 - NOT available in M365 Business Standard (used in this lab). This runbook documents the design and intended configuration only.
Access URL	entra.microsoft.com → Protection → Conditional Access
MFA Configured	Complete Runbook #002 before setting up CA policies
Warning	Test in Report-only mode first - a wrong policy can lock everyone out
Break-glass account	Always exclude one emergency admin account from all CA policies

1

Policy 1 - Block Non-Germany Sign-ins

Restrict tenant access to Germany only via Named Locations

STEP 1 Open Conditional Access



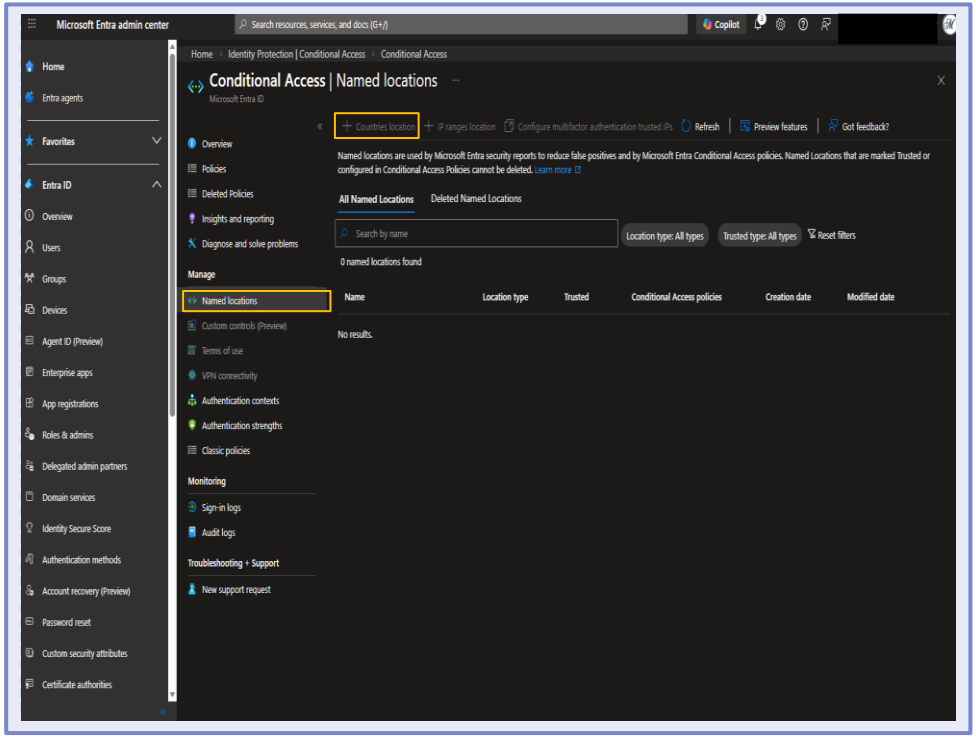
INSTRUCTIONS

- Go to: entra.microsoft.com
- Left menu: Protection → Conditional Access

→ **Conditional Access overview loads**

- Click: Policies in the sub-menu

STEP 2 Create Named Location: Germany



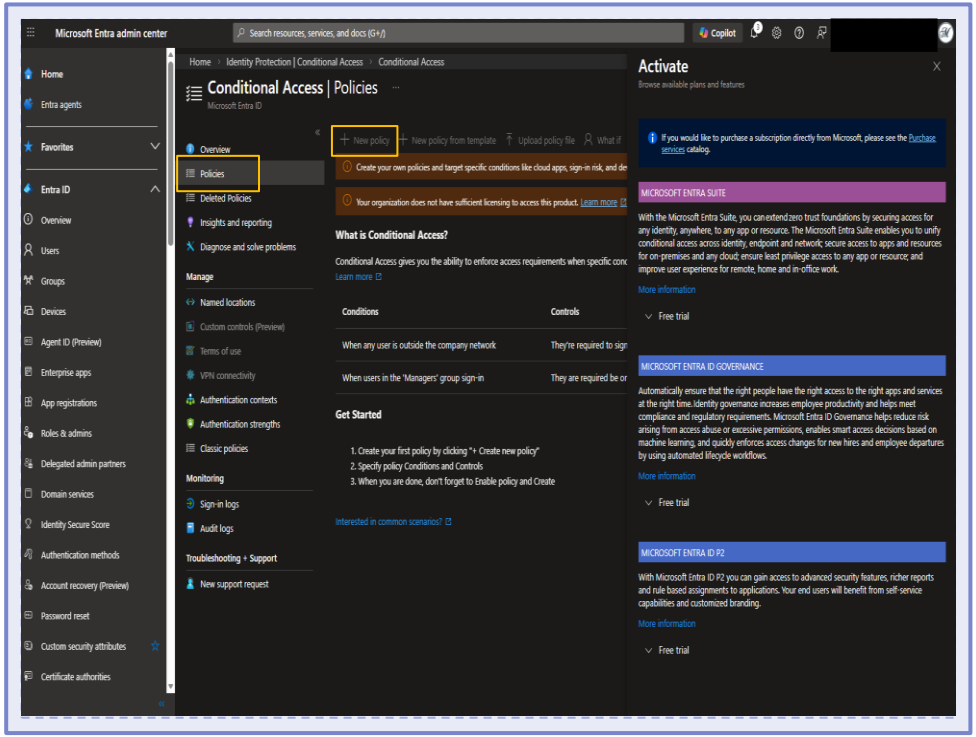
INSTRUCTIONS

- In left menu click: Named locations
- Click + Countries location
- Name: Germany Only
- Select: Germany from the list
- Leave 'Include unknown countries' unchecked

→ **Click Create**

STEP 3

Create the Block Policy



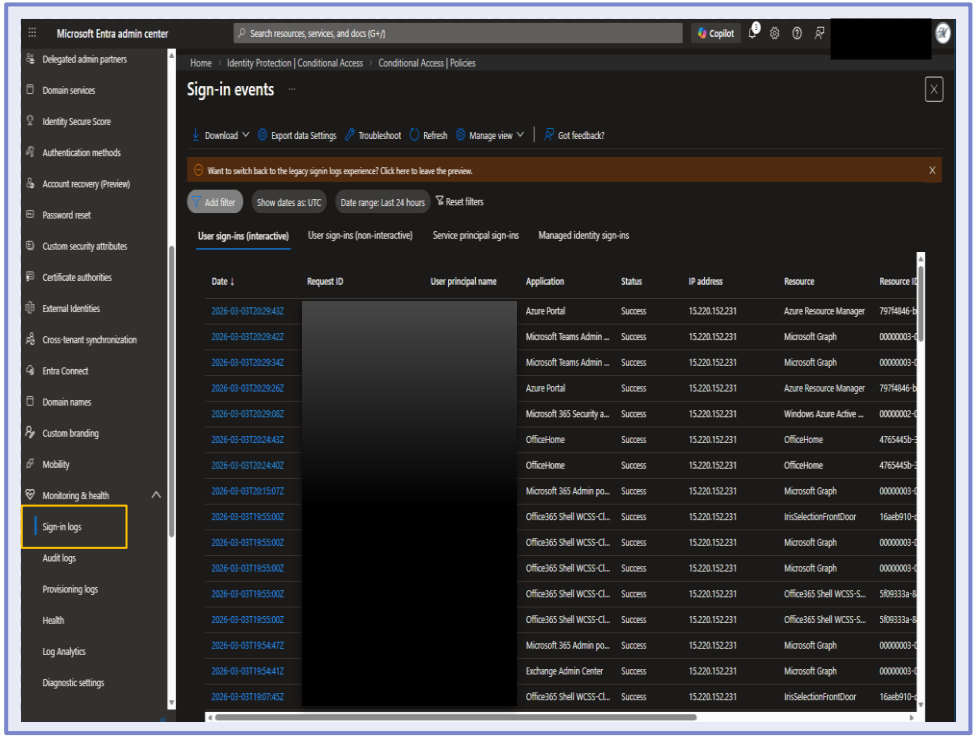
INSTRUCTIONS

- Policies → + New policy
- Name: MOS-CA-001-Block-Non-Germany
- Users: All users (exclude your admin break-glass account)
- Conditions → Locations: Include Any location, Exclude Germany Only
- Grant: Block access
- State: Report-only first

→ Click Create

STEP 4

Enable After Testing



INSTRUCTIONS

- Monitor Report-only for 24-48 hours
- Check: Monitoring → Sign-in logs for expected blocked sign-ins
- Confirm no legitimate Germany users would be blocked
- Change State: On when satisfied

→ Non-Germany sign-ins are now blocked

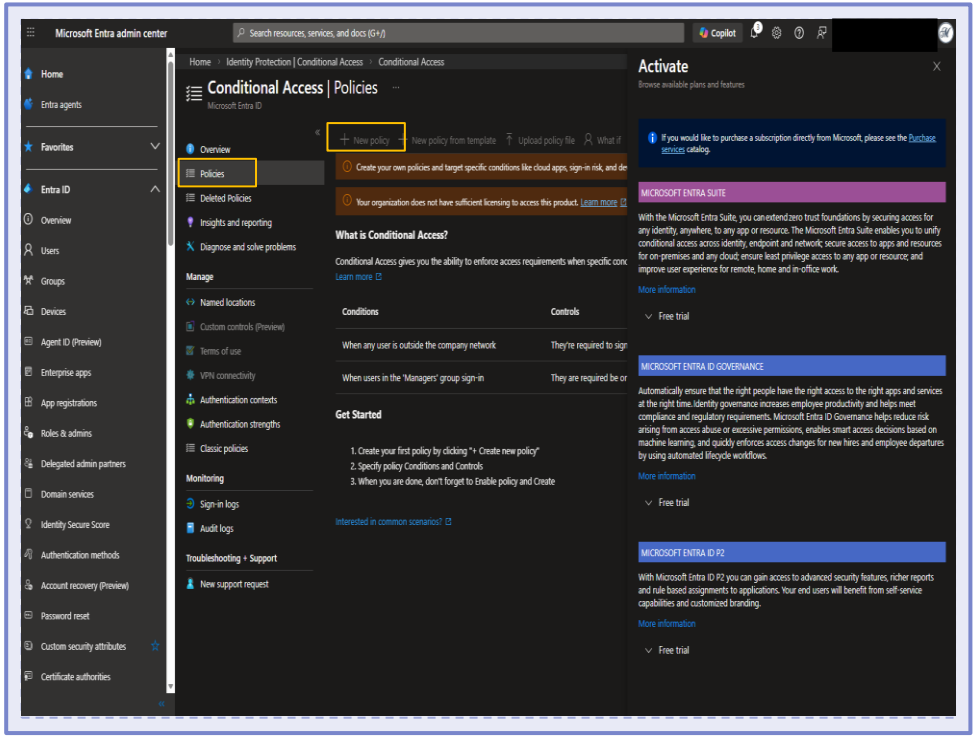
2

Policy 2 - Require MFA for Admins

Force MFA on every admin sign-in via Conditional Access

STEP 1

Create MFA for Admins Policy

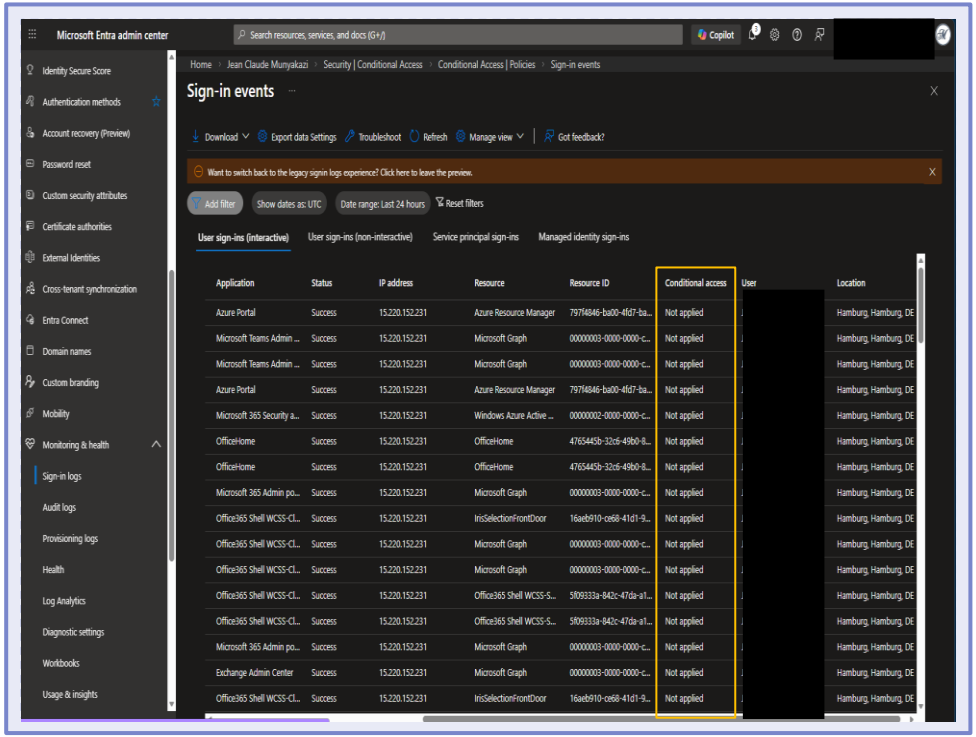


INSTRUCTIONS

- Policies → + New policy
- Name: MOS-CA-002-Require-MFA-Admins
- Users → Include: Directory roles
- Select: Global Administrator, User Administrator, SharePoint Administrator
- Grant: Require multifactor authentication
- State: Report-only first

→ Click Create

STEP 2 Review and Enable



INSTRUCTIONS

- Monitor Report-only 24-48 hours
- Check sign-in logs confirm admin accounts trigger MFA
- Change State: On when satisfied

→ **All admin roles now require MFA at every sign-in**

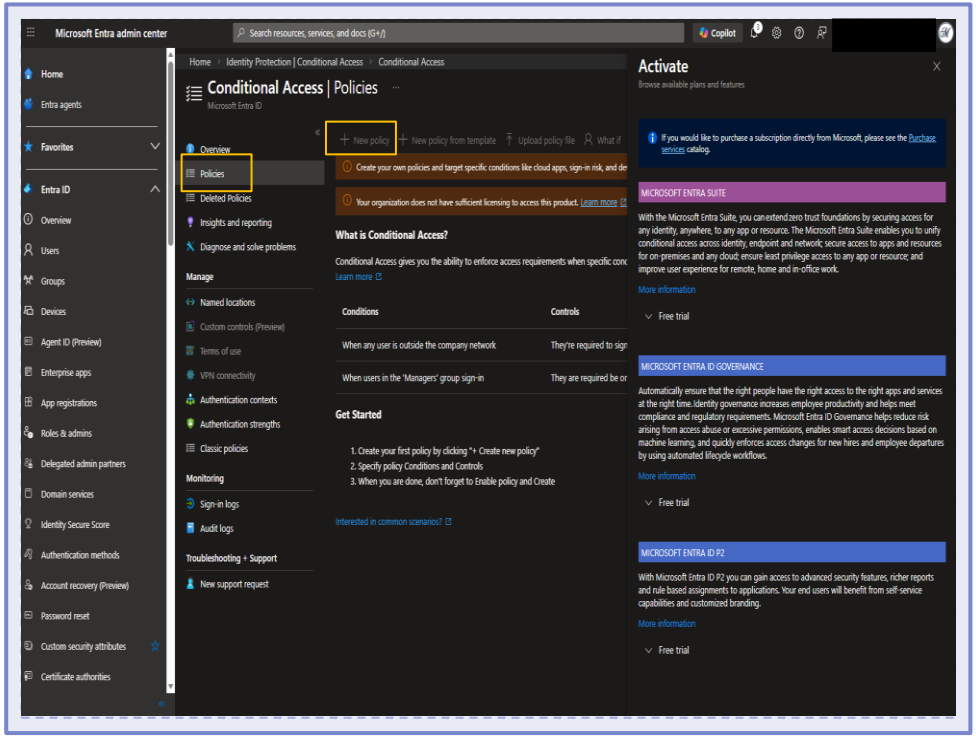
3

Policy 3 - Block Legacy Authentication

Eliminate protocols that cannot support MFA

STEP 1

Create Block Legacy Auth Policy



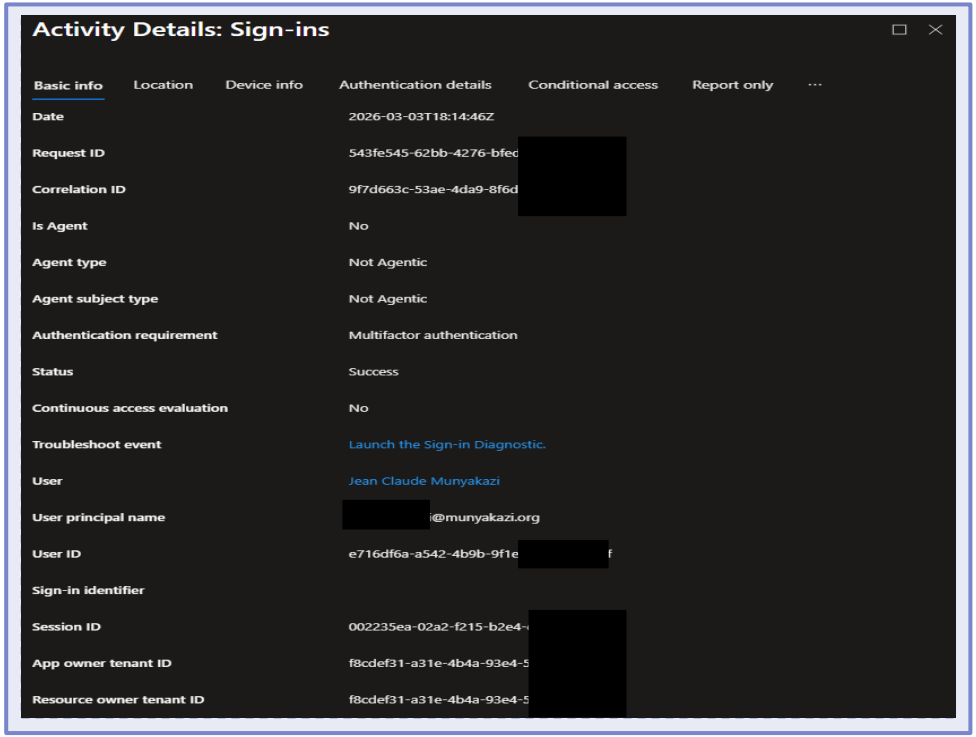
INSTRUCTIONS

- Policies → + New policy
- Name: MOS-CA-003-Block-Legacy-Auth
- Users: All users
- Conditions → Client apps: check Exchange ActiveSync and Other clients
- Grant: Block access
- State: Report-only first

→ **Click Create**

STEP 2

Enable After Verification



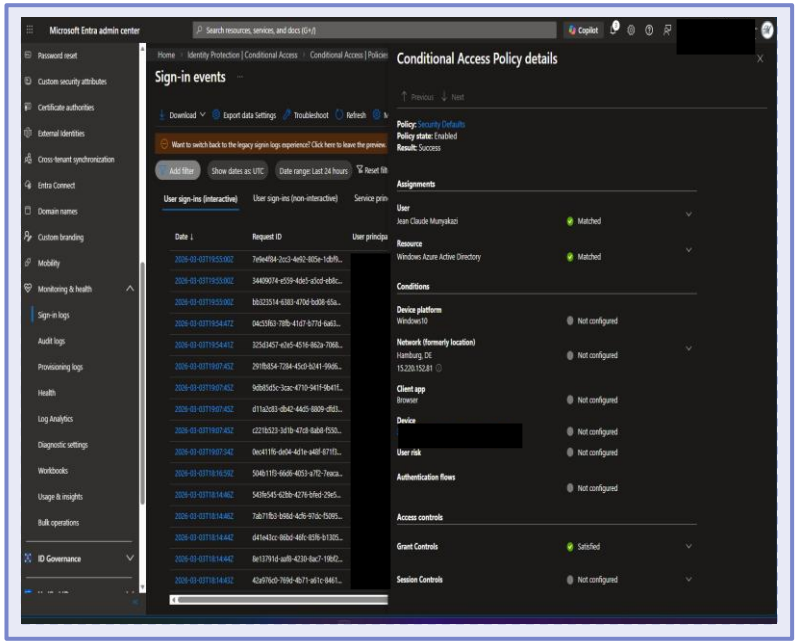
INSTRUCTIONS

- Check sign-in logs for any legitimate legacy client usage
- Update any old mail clients before enabling
- Change State: On when ready

→ **All legacy authentication blocked across the tenant**

Verification Checklist

- 3 CA policies visible in Conditional Access → Policies with correct names
- Named location 'Germany Only' exists under Named locations
- Policy 1: Any location → Block, with Germany Only excluded
- Policy 2: Admin directory roles → Require MFA
- Policy 3: Legacy client apps → Block access
- All 3 policies tested in Report-only before being set to Enabled



Common Errors & Fixes

Error	Cause & Fix
Conditional Access not visible	Entra ID P1 licence required - not in M365 Business Standard
Policy locked me out	Use break-glass account to sign in and disable the policy immediately
Report-only shows too many blocked	Refine conditions - check location scope or user exclusions before enabling
Named location not in conditions	Refresh the page after creating - named locations may take a moment to appear
Admin not prompted for MFA	Confirm policy targets the correct directory role and is set to Enabled
Legacy auth policy breaks email sync	Update mail clients to modern authentication before enabling this policy

What's Next

Access policies are live. Now learn how to safely remove access.

#005	#006	#001
Disable / Offboard User	**Configure SSPR**	**Review: Create Users**
Block sign-in and preserve mailbox for a departing employee	Let users reset their own passwords without the helpdesk	Return to user creation to onboard the next batch of staff
20 min	30 min	30 min

All runbooks available at: munyakazi.org/m365-runbook