

# 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**

## ⚠ 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.

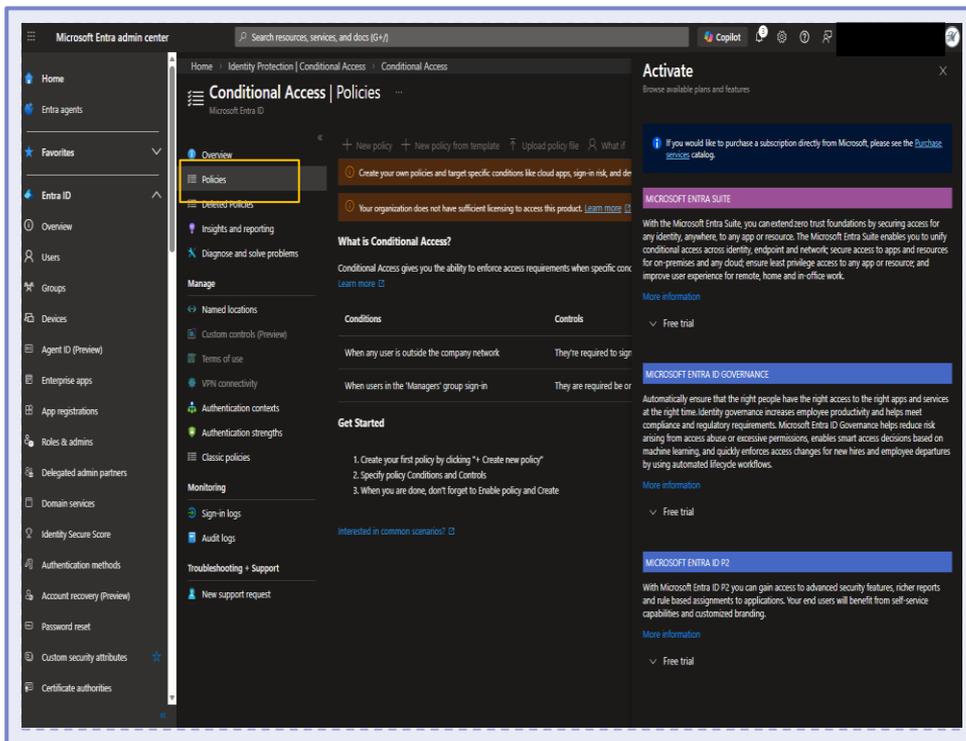
## Prerequisites

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

The screenshot shows the Microsoft Entra admin center interface. The left-hand navigation pane is visible, with the 'Policies' option under the 'Conditional Access' section highlighted with a yellow box. The main content area displays the 'Conditional Access | Policies' page, including an 'Activate' section, a 'What is Conditional Access?' section, and a 'Get Started' section with a numbered list of steps.

**INSTRUCTIONS**

- Go to: [entra.microsoft.com](https://entra.microsoft.com)
- Left menu: Protection → Conditional Access  
→ **Conditional Access overview loads**
- Click: Policies in the sub-menu

## STEP 2

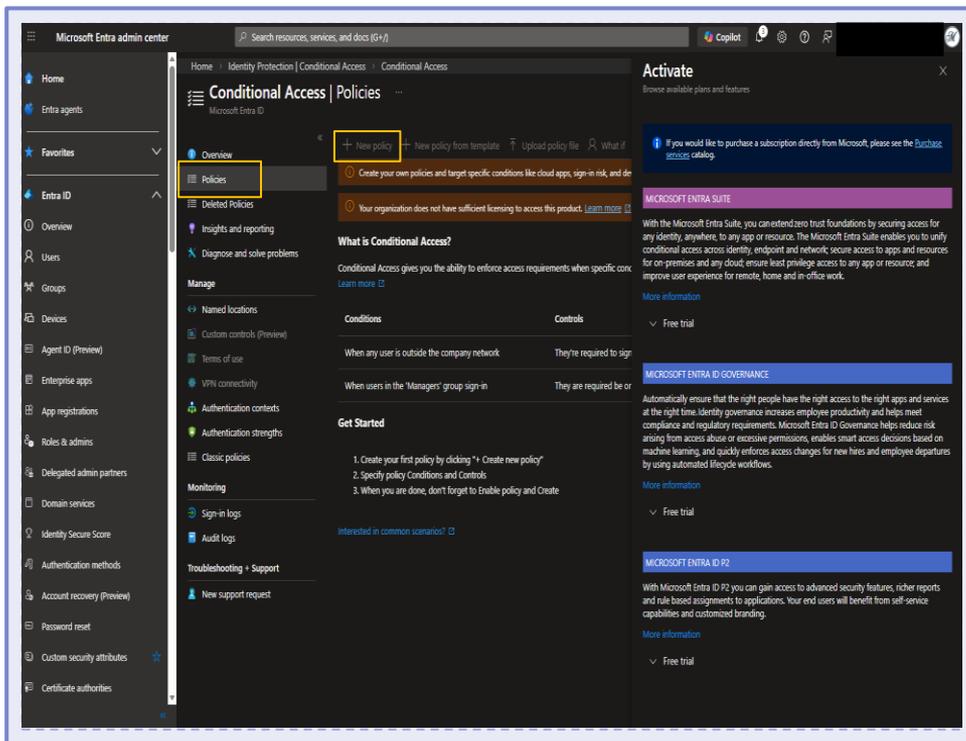
## Create Named Location: Germany

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane is visible, with 'Named locations' selected and highlighted. The main content area is titled 'Named locations' and includes a '+ Countries location' button, a search bar, and a table with the following columns: Name, Location type, Trusted, Conditional Access policies, Creation date, and Modified date. The table currently displays 'No results'.

## 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



The screenshot shows the Microsoft Entra admin center interface. The left navigation pane is visible, with the 'Policies' link under 'Conditional Access' highlighted. The main content area displays the 'Activate' section, which includes a 'New policy' button (highlighted with a yellow box) and a 'Free trial' button. Below this, there are sections for 'MICROSOFT ENTRA SUITE', 'MICROSOFT ENTRA ID GOVERNANCE', and 'MICROSOFT ENTRA ID P2', each with a 'Free trial' button.

### 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

The screenshot shows the Microsoft Entra admin center interface. The left navigation pane has 'Sign-in logs' highlighted. The main content area displays the 'Sign-in events' page with a table of user sign-in events. The table has columns for Date, Request ID, User principal name, Application, Status, IP address, Resource, and Resource ID. The events listed are all successful sign-ins for various applications like Azure Portal, Microsoft Teams Admin, OfficeHome, and Office365 Shell WCSS-CL.

Date	Request ID	User principal name	Application	Status	IP address	Resource	Resource ID
2026-03-03T20:29:43Z			Azure Portal	Success	15.220.152.231	Azure Resource Manager	797f4846-b...
2026-03-03T20:29:42Z			Microsoft Teams Admin ...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T20:29:34Z			Microsoft Teams Admin ...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T20:29:26Z			Azure Portal	Success	15.220.152.231	Azure Resource Manager	797f4846-b...
2026-03-03T20:29:08Z			Microsoft 365 Security a...	Success	15.220.152.231	Windows Azure Active ...	00000002-f...
2026-03-03T20:26:43Z			OfficeHome	Success	15.220.152.231	OfficeHome	4765445b-b...
2026-03-03T20:24:40Z			OfficeHome	Success	15.220.152.231	OfficeHome	4765445b-b...
2026-03-03T20:15:07Z			Microsoft 365 Admin po...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T19:55:00Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	InsSelectionFromDoor	16a68910-f...
2026-03-03T19:55:00Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T19:55:00Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T19:55:00Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	Office365 Shell WCSS-S...	509333a-b...
2026-03-03T19:55:00Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	Office365 Shell WCSS-S...	509333a-b...
2026-03-03T19:54:47Z			Microsoft 365 Admin po...	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T19:54:41Z			Exchange Admin Center	Success	15.220.152.231	Microsoft Graph	00000003-f...
2026-03-03T19:07:45Z			Office365 Shell WCSS-CL...	Success	15.220.152.231	InsSelectionFromDoor	16a68910-f...

**INSTRUCTIONS**

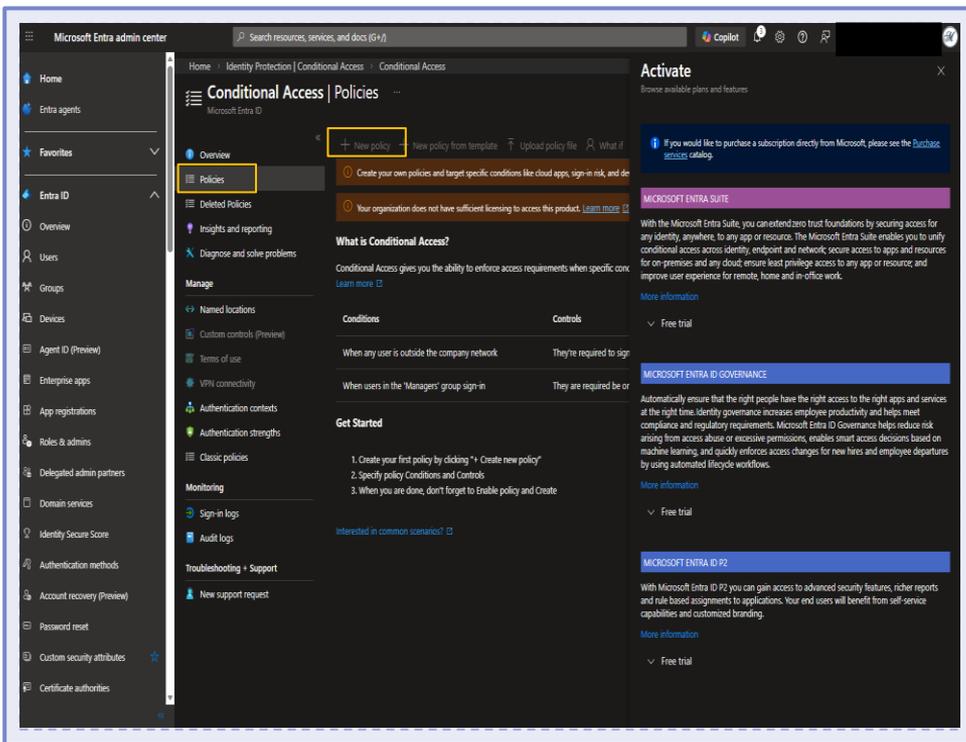
- Monitor Report-only for 24-48 hours
- Check: Monitoring → Sign-in logs for expected blocked sign-ins
- Confirm no legitimate Germany users would be blocked
- Change State: On when satisfied

→ 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

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane shows the 'Policies' link under the 'Conditional Access' section, which is highlighted with a yellow box. The main content area is titled 'Activate' and includes a 'New policy' button, also highlighted in yellow. Below the button, there are sections for 'What is Conditional Access?', 'Conditions', 'Controls', and 'Get Started'. The 'Get Started' section provides a three-step guide: 1. Create your first policy by clicking 'Create new policy', 2. Specify policy Conditions and Controls, and 3. When you are done, don't forget to Enable policy and Create.

**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

The screenshot shows the Microsoft Entra admin center interface. The main content area is titled 'Sign-in events' and displays a table of sign-in events. The table has the following columns: Application, Status, IP address, Resource, Resource ID, Conditional access, User, and Location. The 'Conditional access' column is highlighted in yellow, and all entries in this column are 'Not applied'. The table contains 18 rows of data, including sign-ins for Azure Portal, Microsoft Teams Admin, Office365 Shell, and Exchange Admin Center.

Application	Status	IP address	Resource	Resource ID	Conditional access	User	Location
Azure Portal	Success	15.220.152.231	Azure Resource Manager	797f4846-ba00-4f07-ba...	Not applied		Hamburg, Hamburg, DE
Microsoft Teams Admin ...	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Microsoft Teams Admin ...	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Azure Portal	Success	15.220.152.231	Azure Resource Manager	797f4846-ba00-4f07-ba...	Not applied		Hamburg, Hamburg, DE
Microsoft 365 Security a...	Success	15.220.152.231	Windows Azure Active ...	00000002-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
OfficeHome	Success	15.220.152.231	OfficeHome	4765445b-32c6-49b0-8...	Not applied		Hamburg, Hamburg, DE
OfficeHome	Success	15.220.152.231	OfficeHome	4765445b-32c6-49b0-8...	Not applied		Hamburg, Hamburg, DE
Microsoft 365 Admin po...	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	IntSelectionFrontDoor	16ae8910-c668-4161-9...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	Office365 Shell WCSS-S...	5f09333a-842c-47da-a1...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	Office365 Shell WCSS-S...	5f09333a-842c-47da-a1...	Not applied		Hamburg, Hamburg, DE
Microsoft 365 Admin po...	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Exchange Admin Center	Success	15.220.152.231	Microsoft Graph	00000003-0000-0000-c...	Not applied		Hamburg, Hamburg, DE
Office365 Shell WCSS-CL	Success	15.220.152.231	IntSelectionFrontDoor	16ae8910-c668-4161-9...	Not applied		Hamburg, Hamburg, DE

### 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

Microsoft Entra center

Home > Identity Protection > Conditional Access > Conditional Access

### Conditional Access | Policies

Microsoft Entra ID

Overview Policies Deleted Policies Insights and reporting Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication contexts
- Authentication strengths

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

### Activate

Browse available plans and features

If you would like to purchase a subscription directly from Microsoft, please see the [Purchase services catalog](#).

#### MICROSOFT ENTRA SUITE

With the Microsoft Entra Suite, you can extend zero trust foundations by securing access for any identity, anywhere, to any app or resource. The Microsoft Entra Suite enables you to unify conditional access across identity, endpoint and network, secure access to apps and resources for on-premises and any cloud, ensure least privilege access to any app or resource, and improve user experience for remote, home and in-office work.

[More information](#)

Free trial

#### MICROSOFT ENTRA ID GOVERNANCE

Automatically ensure that the right people have the right access to the right apps and services at the right time. Identity governance increases employee productivity and helps meet compliance and regulatory requirements. Microsoft Entra ID Governance helps reduce risk arising from access abuse or excessive permissions, enables smart access decisions based on machine learning, and quickly enforces access changes for new hires and employee departures by using automated lifecycle workflows.

[More information](#)

Free trial

#### MICROSOFT ENTRA ID P2

With Microsoft Entra ID P2, you can gain access to advanced security features, richer reports and rule-based assignments to applications. Your end users will benefit from self-service capabilities and customized branding.

[More information](#)

Free trial

### What is Conditional Access?

Conditional Access gives you the ability to enforce access requirements when specific conditions are met.

Conditions	Controls
When any user is outside the company network	They're required to sign in
When users in the 'Managers' group sign in	They are required by or

### Get Started

1. Create your first policy by clicking "Create new policy"
2. Specify policy Conditions and Controls
3. When you are done, don't forget to Enable policy and Create

[Interested in common scenarios?](#)

## 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

## Activity Details: Sign-ins

Basic info	Location	Device info	Authentication details	Conditional access	Report only	...
Date			2026-03-03T18:14:46Z			
Request ID			543fe545-62bb-4276-bfec			
Correlation ID			9f7d663c-53ae-4da9-8f6d			
Is Agent			No			
Agent type			Not Agentic			
Agent subject type			Not Agentic			
Authentication requirement			Multifactor authentication			
Status			Success			
Continuous access evaluation			No			
Troubleshoot event			<a href="#">Launch the Sign-in Diagnostic.</a>			
User			<a href="#">Jean Claude Munyakazi</a>			
User principal name			██████████@munyakazi.org			
User ID			e716df6a-a542-4b9b-9f1e-██████████			
Sign-in identifier						
Session ID			002235ea-02a2-f215-b2e4-██████████			
App owner tenant ID			f8cdef31-a31e-4b4a-93e4-5-██████████			
Resource owner tenant ID			f8cdef31-a31e-4b4a-93e4-5-██████████			

## 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

The screenshot displays the Microsoft Entra admin center interface, specifically the 'Conditional Access Policy details' page for 'Sign-in events'. The policy is named 'Security Defaults' and is currently 'Enabled' with a 'Success' result. The policy is assigned to the user 'Jean Claude Munyakazi' and applies to the 'Windows Azure Active Directory' resource. The policy conditions are configured as follows:

- Device platform:** Windows 10 (Not configured)
- Network (formerly location):** Hamburg, DE (Not configured)
- Client app:** Browser (Not configured)
- Device:** (Not configured)
- User risk:** (Not configured)
- Authentication flows:** (Not configured)
- Access controls:** Grant Controls (Satisfied), Session Controls (Not configured)

The 'Sign-in events' table shows a list of recent sign-in attempts with columns for Date, Request ID, and User principal name. The first row shows a successful sign-in on 2024-10-03T19:55:00Z for user 'jean@munyakazi.com' from '193.50.135.100'.

Date	Request ID	User principal
2024-10-03T19:55:00Z	7d64284-2c23-462c-805c-1d8f...	jean@munyakazi.com
2024-10-03T19:55:00Z	3483074-6519-4665-650f-d96c...	jean@munyakazi.com
2024-10-03T19:55:00Z	bb23214-6383-4736-bd88-61a...	jean@munyakazi.com
2024-10-03T19:54:47Z	0ac3383-788b-4147-6718-6463...	jean@munyakazi.com
2024-10-03T19:54:41Z	3254347-4345-4516-6a29-7996...	jean@munyakazi.com
2024-10-03T19:07:42Z	29f8a54-7384-4504-9341-996b...	jean@munyakazi.com
2024-10-03T19:07:42Z	9db85d5c-3aac-4719-941f-9841f...	jean@munyakazi.com
2024-10-03T19:07:42Z	671a203-0842-4445-8009-d511...	jean@munyakazi.com
2024-10-03T19:07:42Z	02216523-3d18-4718-ba88-f55b...	jean@munyakazi.com
2024-10-03T19:07:34Z	0ec4118-6d44-4d1e-a6d7-6711...	jean@munyakazi.com
2024-10-03T19:16:59Z	5046110-4649-4013-917c-76ca...	jean@munyakazi.com
2024-10-03T18:14:46Z	3436545-6236-4276-6160-29e5...	jean@munyakazi.com
2024-10-03T18:14:46Z	7ab717b3-b96d-4c6-91c-5595...	jean@munyakazi.com
2024-10-03T18:14:44Z	641443c-880d-461-639b-d135...	jean@munyakazi.com
2024-10-03T18:14:44Z	8e137914-6d8-423b-ba67-196f...	jean@munyakazi.com
2024-10-03T18:14:42Z	42a796d3-769d-4671-a81c-9461...	jean@munyakazi.com

## Common Errors & Fixes

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

## Disable / Offboard User

Block sign-in and preserve mailbox for a departing employee

20 min

#006

## Configure SSPR

Let users reset their own passwords without the helpdesk

30 min

#001

## Review: Create Users

Return to user creation to onboard the next batch of staff

30 min