# Conditional Access as Code via GitHub Actions

Conditional Access as Code with Terraform and GitHub Actions

This project demonstrates how to implement Conditional Access Policies as Code using:

* Terraform
* Azure Active Directory (Microsoft Entra)
* GitHub Actions for CI/CD

The goal is to automate the deployment of Conditional Access policies in a secure, repeatable, and auditable way using Infrastructure as Code (IaC). To perform this lab you have the Microsoft Entra P2 subscription.

## Use Case:

Block Non-Compliant Devices from Untrusted Locations. This use case creates a Conditional Access policy that:

* Applies to all users, excluding guests and external users.
* Applies when sign-in risk is medium or high.
* Blocks access from devices not compliant with organizational policy.
* Excludes access from trusted locations.
* Requires Multi-Factor Authentication (MFA).
* Includes session control configurations.

## Tech Stack:

* Terraform: IaC for Azure resources
* Azure AD Provider: Provision Conditional Access policies
* GitHub Actions: Automate the CI/CD workflow

## Project Structure:

├── .github/workflows/

│ └── deploy.yml # GitHub Actions CI/CD pipeline

├── main.tf # Conditional Access policy definition

├── variables.tf # Required input variables

├── providers.tf # AzureAD provider setup

├── README.md # Project documentation

## Prerequisites:

Azure AD App Registration with the following:

* API permissions: Policy.ReadWrite.ConditionalAccess
* A client secret (store the value, not the ID)
* Assign Required Directory Role: At least Security Administrator or Conditional Access Administrator

## Create GitHub Secrets:

ARM\_CLIENT\_ID: App (client) ID

ARM\_CLIENT\_SECRET: Client secret value (not ID!)

ARM\_TENANT\_ID: Tenant (directory) ID

Now create the following .tf files:

* main.tf
* variables.tf
* providers.tf

And create the GitHub actions workflow:

* .github/workflows/deploy.yaml

For code of these .tf files, clone the repo:

## https://github.com/Anisa-BiBi/conditional\_access.git

## How It Works:

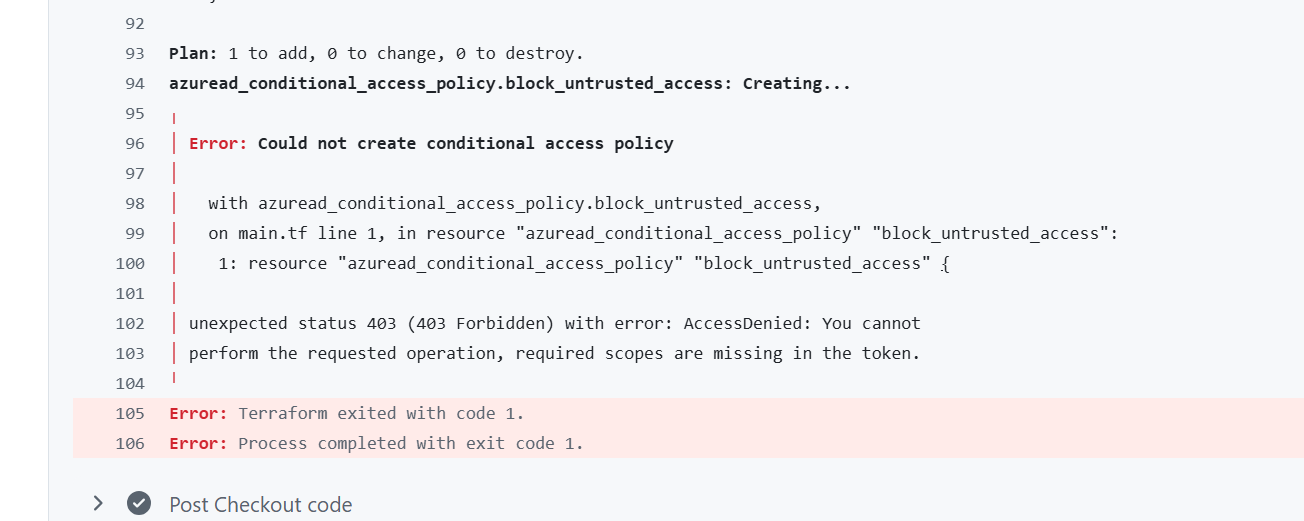
* GitHub Actions triggers on Push to main
* Manual workflow\_dispatch
* Terraform authenticates using secrets from GitHub
* A Conditional Access Policy is created or updated based on main.tf

## Testing the Setup:

* Push a change to main
* Or manually trigger from GitHub Actions → "Deploy Conditional Access Policy"
* Check Azure Portal → Azure AD → Security → Conditional Access → Policies

## Note:

CDX and student account of azure portal have less permissions. This above policy implementation might give an error.



So don’t need to worry just used other tenant that have subscription with more resources and permissions.