Criar política de MFA para um grupo específico

O MFA (*Multi-Factor Authentication* ou Autenticação Multifator) é um método de segurança que exige que o usuário prove a identidade usando mais de um fator de autenticação ao fazer login.

Pré-requisitos

- Licença **Azure AD Premium P1** ou superior.
- Conta com permissão de **Administrador de Segurança** ou **Administrador Global**.
- Grupo já criado no **Microsoft Entra ID** (Azure AD) com os usuários desejados.

Como funciona

Em vez de depender apenas da senha (algo que você sabe), o MFA combina outros fatores, por exemplo:

- Algo que você sabe → senha, PIN.
- Algo que você tem → celular, token físico, aplicativo de autenticação (Microsoft Authenticator, Google Authenticator).
- Algo que você é → biometria (impressão digital, reconhecimento facial).

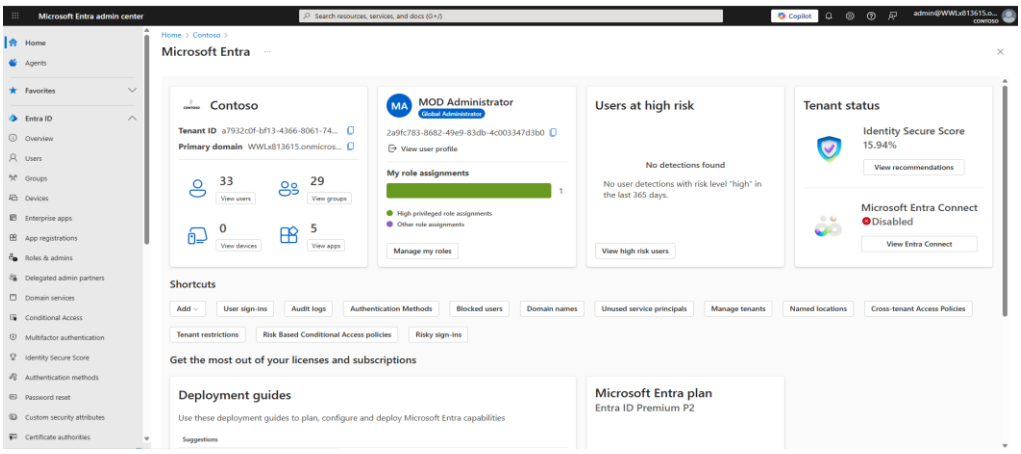
Exemplo:
Você digita sua senha no Microsoft 365 → recebe um código no seu celular ou uma notificação no app Authenticator → só depois o acesso é liberado.

Passos a seguir para criar politica de MFA para grupos específicos:

1. Acessar o Microsoft Entra Admin Center

   - Vá para: https://entra.microsoft.com.

   - Faça login com conta de administrador.

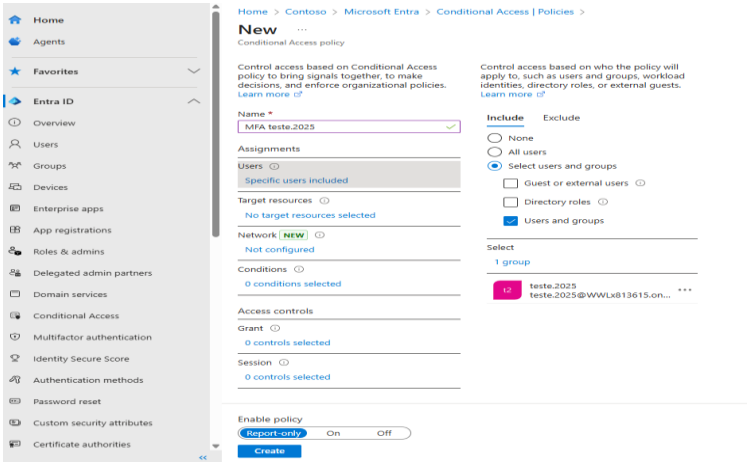


2. Criar a política de Conditional Access

    - No menu esquerdo, clique em **Acesso condicional** (*Conditional Access*).
    - Clique em **política + Nova política** (*+ New policy*).
    - **Nome:** dê um nome claro, exemplo: teste.2025

3. Usuários ou identidades de trabalho (*Users*):

    - Selecione **Selecionar usuários e grupos**
    - Marque **Grupos** e selecione o grupo que deve ter MFA obrigatório



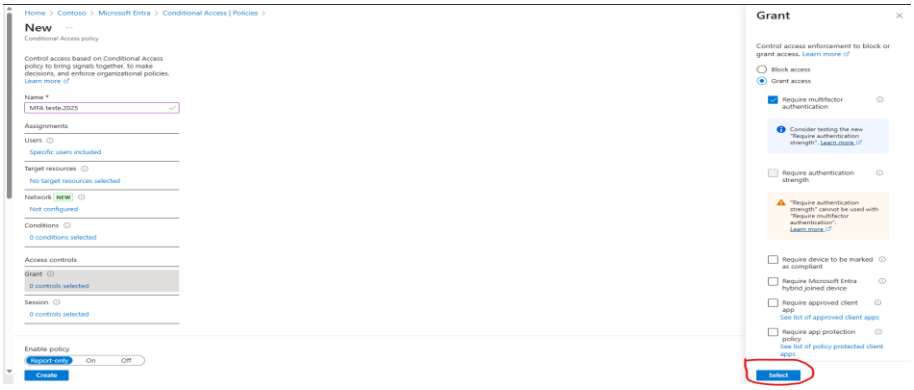
4. Escolher as aplicações-alvo

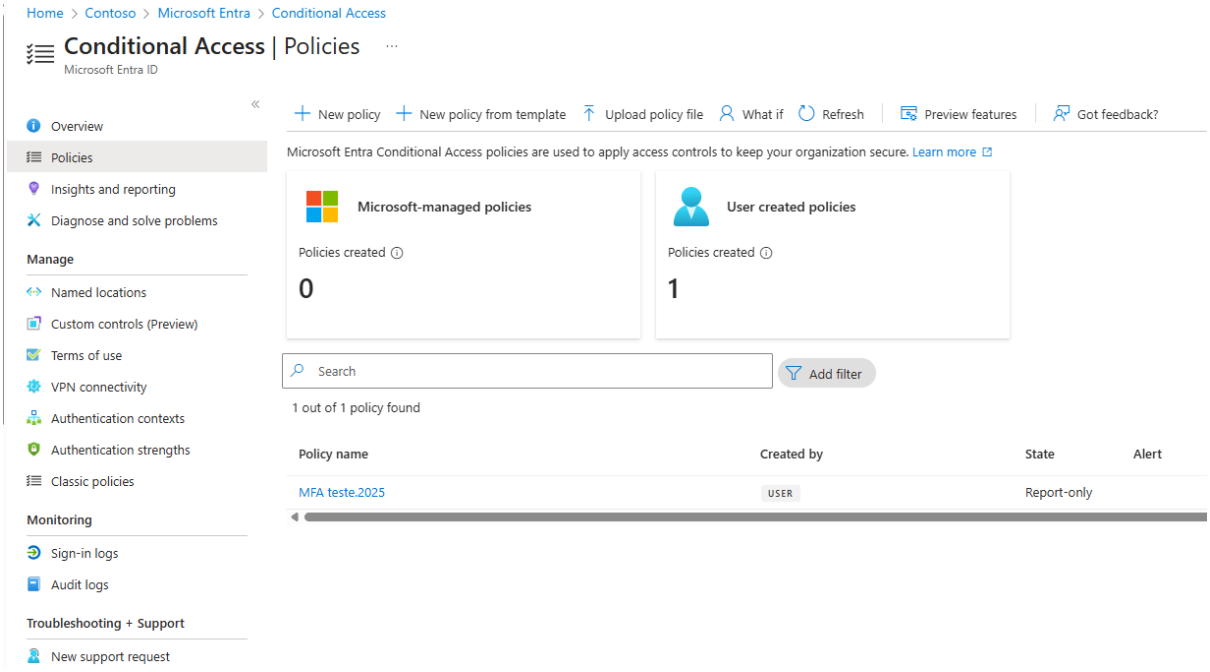
    - Em **Atribuições → Aplicativos** (*Cloud apps or actions*):
    - Pode deixar **Todos os aplicativos na nuvem** ou escolher apps específicos (ex.: Microsoft 365).

5. Configurar o MFA

    Em **Condições → Conceder** (*Grant*):

    - Selecione **Conceder acesso** (*Grant access*).
    - Marque **Exigir autenticação multifator** (*Require multi-factor authentication*).
    - Clique em **Selecionar**.


Home > Contoso > Microsoft Entra > Conditional Access | Policies >
New
Conditional Access policy
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
MFA teste.2025
Assignments
Users
Specific users included
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
Create
Grant
Control access enforcement to block or grant access. Learn more
Block access
Grant access
Require multifactor authentication
Consider testing the new "Require authentication strength". Learn more
Require authentication strength
"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more
Require device to be marked as compliant
Require Microsoft Entra hybrid joined device
Require approved client app
See list of approved client apps
Require app protection policy
See list of policy protected client apps
Select


Home > Contoso > Microsoft Entra > Conditional Access
Conditional Access | Policies
Microsoft Entra ID
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
New policy
New policy from template
Upload policy file
What if
Refresh
Preview features
Got feedback?
Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more
Microsoft-managed policies
Policies created
0
User created policies
Policies created
1
Search
Add filter
1 out of 1 policy found
Policy name
Created by
State
Alert
MFA teste.2025
USER
Report-only