Criar uma política de autenticação com restrição por sistema operacional.

Uma **política de autenticação com restrição por sistema operacional** no Azure AD (via **Acesso Condicional**) serve para **controlar** ou **bloquear** o acesso a aplicativos e recursos com base no **tipo de sistema operacional** do dispositivo que o usuário está a usar no momento do login.

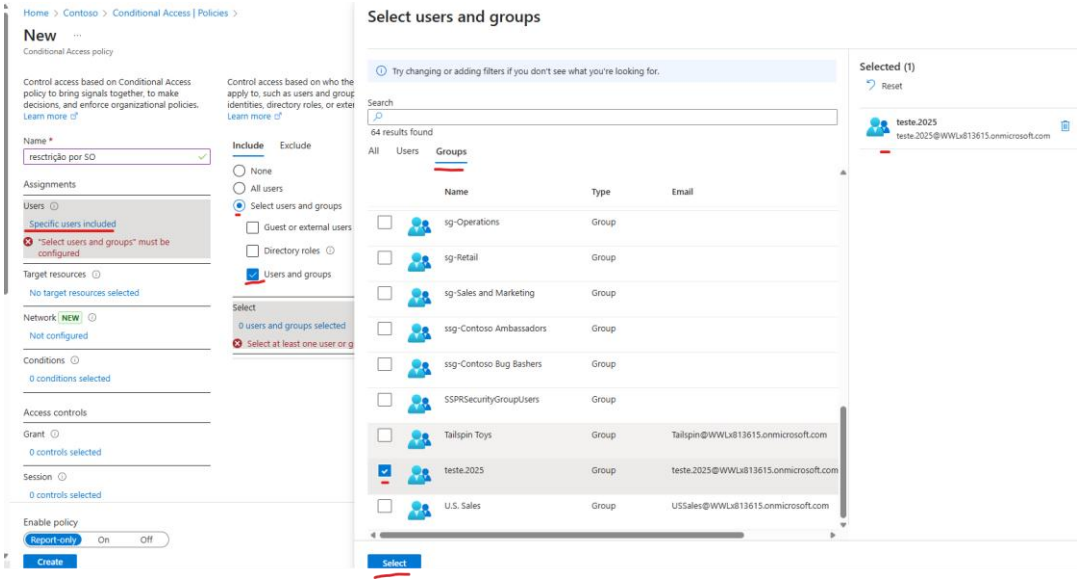
Para que serve na prática:

- Bloquear dispositivos não suportados
- Garantir conformidade de segurança
- Restringir dispositivos móveis
- Evitar riscos de malware e vulnerabilidades

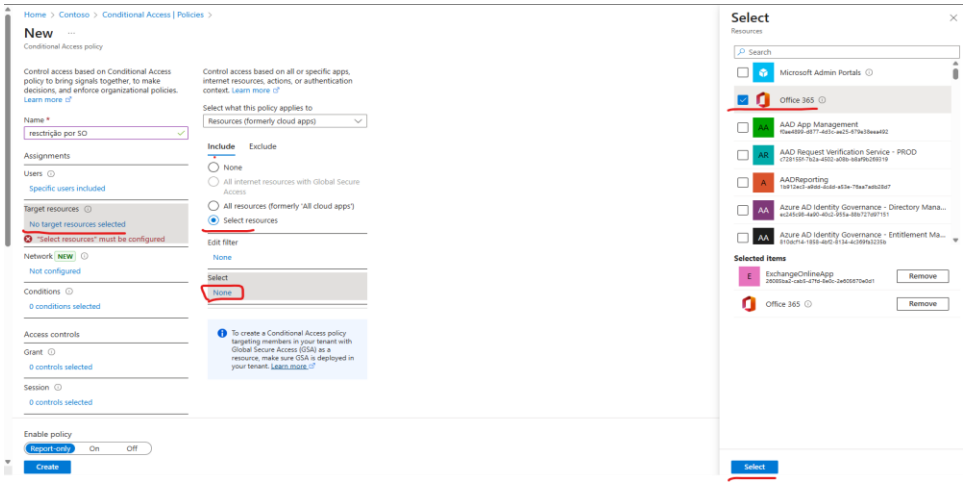
Exemplo real:
Se a sua organização quer que o Teams, o Outlook e o SharePoint só sejam usados em **Windows corporativo**, você cria a política para permitir apenas **Windows** e bloquear todos os outros sistemas (macOS, Linux, iOS, Android).

Passos a seguir:

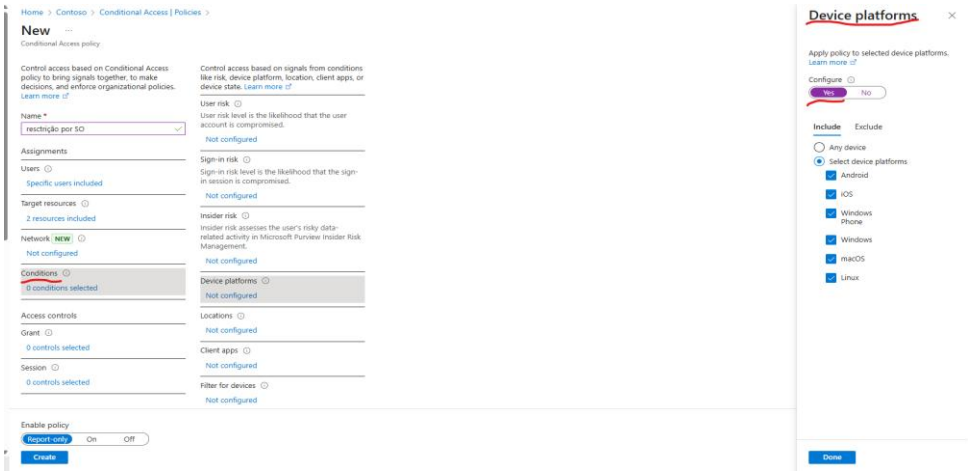
1. **Aceder ao Portal Microsoft Entra**
   - Inicie sessão com uma conta **Administrador Global** ou **Administrador de Segurança**.
2. **Acesso Condicional**
   - Vá para **Acesso Condicional → Políticas**.
   - Clique em + **Nova política**.
3. **Nomear a Política**
4. **Atribuir a política a Utilizadores ou Grupos**

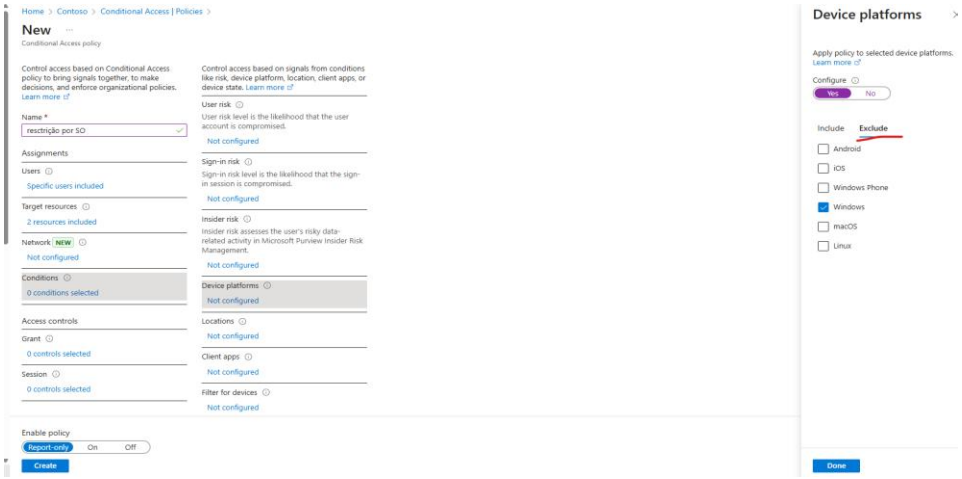


5. **Selecionar Aplicações**
    - Em **Atribuições** → Aplicações ou ações em nuvem, escolha Selecionar aplicações.
    - Escolha as aplicações que quer proteger (por exemplo: **Office 365**, **Exchange Online** ou **Todas as aplicações na nuvem**).



6. **Configurar Plataforma do Dispositivo (SO)**
    - **Em Condições → Plataformas de dispositivos, ative** a condição**.**
    - Em **Incluir**, marque o(s) sistema(s) operacional(is) que quer **alvo da política** (Windows, macOS, iOS, Android).
    - Se o objetivo for **bloquear** certos SO:
    - Em **Excluir**, selecione o SO que deseja **permitir**.





7. **Definir Controlo de Acesso**
    - Em **Controlos de acesso** → Conceder, **selecione Bloquear acesso** (ou "Exigir dispositivo compatível.
8. **Ativar a Política**
    - Defina **Ativar política → Ligado**.