

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

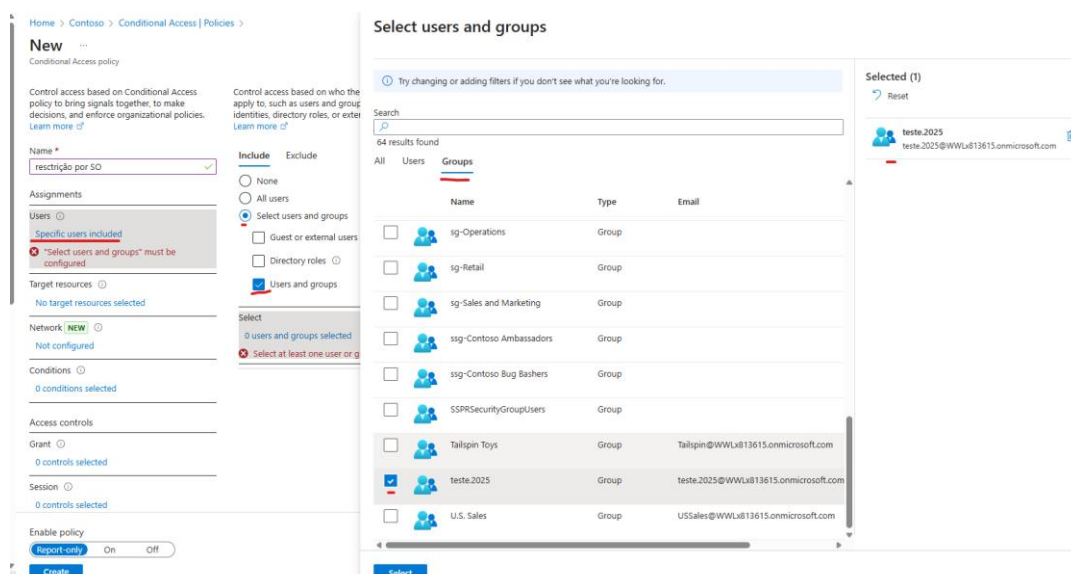
- Inicie sessão com uma conta **Administrador Global** ou **Administrador de Segurança**.

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**).

Home > Contoso > 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 *
restrição por SO

Assignments

Users
Specific users included

Target resources
No target resources selected
Select resources must be configured

Network
Not configured

Conditions
0 conditions selected

Access controls
Grant
0 controls selected

Session
0 controls selected

Enable policy
Report only On Off

Create

Select what this policy applies to
Resources (formerly cloud apps)

Include Exclude

None
All internet resources with Global Secure Access

All resources (formerly 'All cloud apps')
Select resources

Exit filter
None

Select
None

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. [Learn more](#)

Select

Resources

Search

- Microsoft Admin Portals
- Office 365
- AAD App Management
- AAD Request Verification Service - PROD
- AADReporting
- Azure AD Identity Governance - Directory Mana...
- Azure AD Identity Governance - Entitlement Ma...

Selected items

- ExchangeOnlineApp
- Office 365

Select

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**.

Home > Contoso > 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 *
restrição por SO

Assignments

Users
Specific users included

Target resources
2 resources included

Network
Not configured

Conditions
0 conditions selected

Access controls
Grant
0 controls selected

Session
0 controls selected

Enable policy
Report only On Off

Create

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk
Not configured

Sign-in risk
Not configured

Insider risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Filter for devices
Not configured

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure
Yes No

Include Exclude

Any device
Select device platforms

- Android
- iOS
- Windows Phone
- Windows
- macOS
- Linux

Done

Home > Contoso > 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 *
restrição por SO ✓

Assignments

Users ☐
Specific users included

Target resources ☐
2 resources included

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

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ☐ Yes ☐ No

Include ☒ Exclude

☐ Android
☐ iOS
☐ Windows Phone
☒ Windows
☐ macOS
☐ Linux

Done

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.

Home > Contoso > 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 *
restrição por SO ✓

Assignments

Users ☐
Specific users included

Target resources ☐
2 resources included

Network **NEW** ☐
Not configured

Conditions ☐
1 condition 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
☐ Require authentication strength
☐ 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
☐ Require password change

For multiple controls
☒ Require all the selected controls
☐ Require one of the selected controls

Select

Home > Contoso > Conditional Access

Conditional Access | Policies —

Microsoft Entra ID

Overview

[+ 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](#)

Policy name	Created by	State	Alert	Creation date	Modified da
Bloquear logins fora de Angola	USER	Report-only		8/13/2025, 10:24:21 PM	8/13/2025, 1
restrição por SO	USER	On		8/14/2025, 12:40:41 PM	