Microsoft Entra ID (Azure) Conditional Access

www.thecyphere.com

info@thecyphere.com

Learn how Entra ID (Azure AD) Conditional Access Policies provide flexibility in managing resource access, allowing precise enforcement of security measures when and where necessary.

Conditional access, signals and decisions

Conditional Access Policies are a set of rules and criteria that organisations can configure to control and enforce access to their resources.

Think of **'if-then'** statements, if a user wants to access this, then this action needs to be completed.

These policies allow you to define who can access what, under which conditions, based on signals taken from various sources before decisions are taken to block or grant access.

Various sources for signals include:

- User/group memberships
- IP Location info
- Device, application
- Entra ID protection
- Defender for cloud apps

Conditional access templates

16 pre-defined Conditional Access policy templates across five categories are ready to be deployed. These templates align with Microsoft's best practices for access control policies.

Risks addressed with conditional access policies

Require MFA

- Unauthorised access
- Credential theft
- Privilege escalation
- Insider threats
- Compliance risks
- Improved remote access security

Securing security info registration

- Unauthorised access
- Account takeover
- Brute force attacks
- Spam and fraudulent accounts
- Data privacy violations
- Identity theft
- Compliance violations
- Account lockout

Require multifactor authentication

- Phishing attacks
- Unauthorised access
- Credential theft
- Account compromise
- Insider threats

Blocking legacy authentication

- Credential theft
- Unauthorised access
- Brute force attacks
- Account compromise
- Security weaknesses

Require a compliant device, Microsoft Entra hybrid joined device or MFA

- Unauthorised access
- Device non-compliance
- Account compromise
- Security vulnerabilities

User risk-based password change

- Weak passwords
- Credential theft
- Unauthorised access
- Account compromise
- Insider threats

Block access for unknown or unsupported device platform

- Unauthorised access
- Device compatibility issues
- Account compromise
- Security weaknesses

Require approved client apps or app protection policy

- Unauthorised access
- Data leakage
- Insecure application use
- Account compromise
- Security weaknesses

Use application-enforced restrictions for unmanaged devices

- Unauthorized access
- Data exposure
- Device security
- Account Compromise
- Security Weaknesses

Require reauthentication and disable browser persistence

- Unauthorised access
- Session hijacking
- Account compromise
- Security weaknesses

5 categories of conditional access policy templates

Microsoft added pre-defined templates across these categories:

1. Secure foundation
2. Zero Trust architecture
3. Remote work
4. Protect administrator
5. Emerging threats

User exclusions

- Exclude emergency access or brkea-glass accounts to prevent a tenant-wide lockout.
- Exclude service accounts and principals due to their non-interactive nature; consider managed identities or targeted policies.

How to deploy without impact on users?

Configure Report-only mode before deployment to determine the impact on end users

Troubleshoot using what-if tool to simulate conditional access. Access it here:

Entra admin center > Protection > Conditional Access > Policies > What If.

LIKE THIS?

Share ♻ with your network

For consultation, reach out:

www.thecyphere.com
info@thecyphere.com