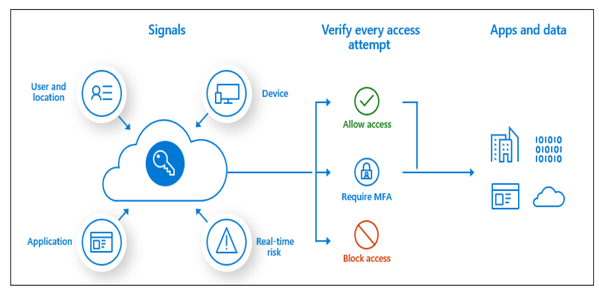
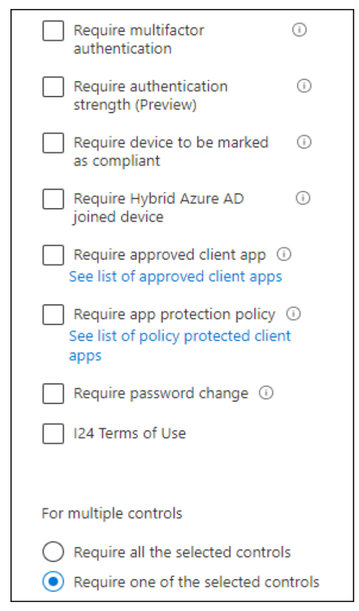
Conditional Access troubleshooting flowchart



Rules:
All policies are enforced in two phases:
In the first phase, all policies are evaluated and all access controls that aren't satisfied are collected.
In the second phase, you are prompted to satisfy the requirements you haven't met.
If one of the policies blocks access, you are blocked and not prompted to satisfy other policy controls. If none of the policies blocks you, you are prompted to satisfy either one or all selected policy controls in the following order. (see picture on the right)

1. Multi-factor authentication
2. Approved client app/app protection policy
3. Managed device (compliant or hybrid Azure AD join)
4. Terms of use
5. Custom controls



External MFA providers and terms of use come next. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

Block access thrumps all other configuration settings

Assignments

Enable policy

Start → Is the policy enabled? (No → Is the policy in Report-only mode or turned off?)
- Turned off → This policy not applicable
- Report-only → View possible applicability in Azure AD sign-in logs or Log Analytics Workbooks
- Yes → Users or workload identities

Users or workload identities

Policy applies to? (Yes / Yes)
- Policy effectively assigned to user? (Yes → Cloud apps or actions; No → Policy effectively assigned to Service Pricipal?)
- Policy effectively assigned to Service Pricipal? (Yes → Cloud apps or actions; No → This policy not applicable)

Cloud apps or actions

Policy applies to? (Authentication context / Cloud apps)
- Authentication context → Is the Authentication Context applicable? (No → Conditions; Yes → Are we registering security information or registering or joining device?)
- Are we registering security information or registering or joining device? (User Actions; No → Conditions; Yes → This policy not applicable)
- Cloud apps → Is the cloud app targeted? (No → Conditions; Yes → This policy not applicable)

Assigned to user / *Workload identity*

Conditions

User risk specified? → Sign-in risk specified? → Device Platforms specified? → Locations specified? → Client apps specified and applicable? → Filter for devices: specified?

Each "specified?" (Yes) → "… applicable?"; each "… applicable?" (No) → This policy not applicable.

Service Principal risk (Preview) specified? / Locations (Preview) specified? (Yes) → Risk applicable? (No → This policy not applicable; Yes → Access Controls)

Access Controls

Grant

Grant or Block?
- Block → Access is blocked, no other policies evaluated
- Additional controls required?

Or
- Multifactor authentication required? (Yes → Multifactor authentication satisfied?)
- Authentication Strength required? (Yes → Authentication strength satisfied?)

Other controls needed? (No → Session controls; Yes →)

And/Or
- Approved client app required? (Yes → Approved client app satisfied?)
- App Protection policy required? (Yes → App Protection policy satisfied?)

Other controls needed? (No → Session controls; Yes →)

Or
- Compliant device required? (Yes → Device Compliant?)
- Hybrid AD joined device required? (Yes → Device Hybrid AD Joined?)

Other controls needed? (No → Session controls; Yes →)

Terms of use acceptance required? (Yes → Terms of use accepted?)

Other controls needed? (No → Session controls; Yes →)

Password change required? (Yes → Password changed?)

Other controls needed? (No → Session controls; Yes →)

Custom controls? (Yes → Custom controls satisfied?)

Custom controls satisfied? (Yes → Session controls; No → Access is blocked, no other policies evaluated)

Access is granted, other policies will be evaluated

Are session controls specified? (No → Access is granted, other policies will be evaluated; Yes → Session controls)

Session controls

App enforced restrictions selected? (Yes → App enforced restrictions applied to session)

Conditional Access App Control selected? (Yes → Session routed to Microsoft Defender for Cloud Apps)

Sign-in frequency selected? (Yes → Sign-in frequency specified is applied to session)

Persistent browser session selected? (Yes → Browser persistence settings is applied to session)

Customize continuous access evaluation selected? (Yes → Continuous access evaluation is disabled)

Disable resilience defaults selected? (Yes → Resilience defaults are disabled)