



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.

- ☐ Require multi-factor authentication ⓘ
- ☐ Require device to be marked as compliant ⓘ
- ☐ Require Hybrid Azure AD 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 (Preview) ⓘ
- ☐ I24 Terms of Use

Block access trumps all other configuration settings

