Solution

Define locations

Step 1: Sign in to the Azure portal

Step 2: Named locations

Step 3: Location selection

Step 4: Specify the countries or regions

Create a Conditional Access policy

Step 1: Sign in to the Azure portal

Step 2: Create new policy

Step 3: New policy

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 *

| Block access from designated countries | ✓ |

Assignments

Users ⓘ

0 users and groups selected

Step 4: User assignments

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more ⬀

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more ⬀

Name *

Block access from designated countries ✓

Assignments

Users ⓘ

All users

Include　Exclude

◯ None

◉ All users

◯ Select users and groups

Target resources ⓘ

No target resources selected

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Learn more ⬀

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Enable policy

[Report-only]　On　Off

⚠ It looks like you're about to manage your organization's security configurations. That's great! You must first disable security defaults before enabling a Conditional Access policy.

Create

Step 5: Cloud app assignments

Step 6: Condition assignments

Step 7: Blocked location

Step 8: Blocked access

Step 9: Report-only

Step 10: Create

Notifications

Dismiss all ⌄

✅ **Successfully created 'Block access from designated countries'** ✕

Successfully created 'Block access from designated countries'

a few seconds ago