

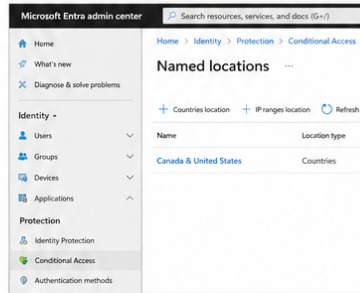
Microsoft 365 Conditional Access – Safe Zones (Canada & US)

Block sign-ins from outside Canada & United States unless traveling

Goal: Allow access from Canada and the United States. Block access from other countries unless the user is traveling (exception).

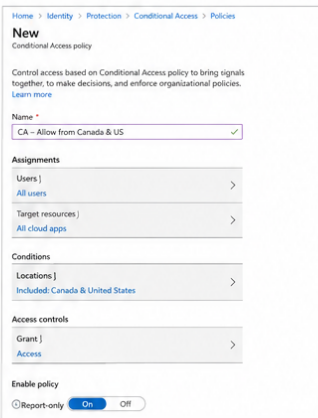
1 Create Named Location – Canada & United States

1. Go to Microsoft Entra admin center (entra.microsoft.com)
2. Identity > Protection > Conditional Access > Named locations
3. Click + Country location
4. Name: "Canada & United States"
5. Include: Canada, United States
6. Click **Create**



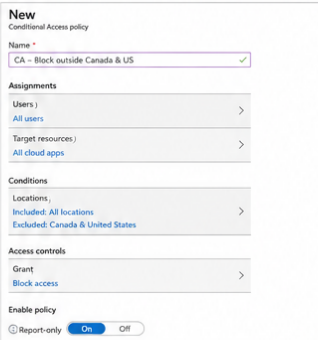
2 Create Conditional Access Policy – Allow from Safe Zone

1. Go to Identity > Protection > Conditional Access > Policies
2. Click + New policy
3. Name: "CA – Allow from Canada & US"
4. Assignments
 - Users: All users
 - Cloud apps: All cloud apps
5. Conditions > Locations
 - Include: Canada & United States
 - Exclude: Leave blank
6. Access controls
 - Grant: Access
 - Session: 0 controls selected
7. Enable policy: On
8. Create



3 Create Conditional Access Policy – Block outside Safe Zone

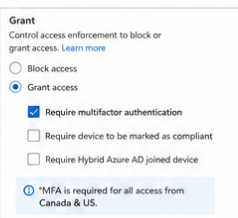
1. Click + New policy
2. Name: "CA – Block outside Canada & US"
3. Assignments
 - Users: All users
 - Cloud apps: All cloud apps
4. Conditions > Locations
 - Include: All locations
 - Exclude: Canada & United States
5. Access controls
 - Grant: Block access
6. Enable policy: On
7. Create



4 Require MFA for All Access

Ensure MFA is required in the "Allow" policy.

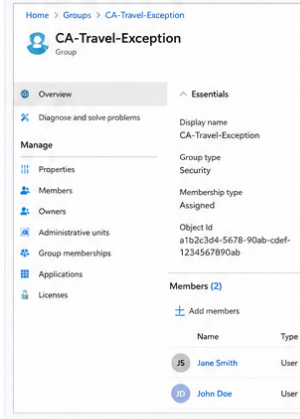
- Access controls > Grant > Require multifactor authentication = **Yes**
- This enforces MFA for all sign-ins from Canada & US.



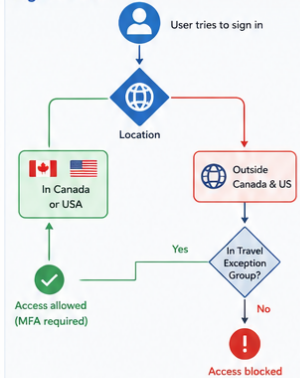
Travel Exception Process

When a user needs to travel internationally:

1. User requests access by emailing IT.
2. IT adds the user to a security group "CA-Travel-Exception".
3. Create an exception policy:
 - Users: CA-Travel-Exception group
 - Conditions > Locations: All locations
 - Grant: **Require MFA** (or Access + MFA)
 - Place this policy above the Block policy.
4. Remove user from group after travel.



Sign-in Flow



Monitoring & Best Practices

- Monitor sign-ins: Entra admin center > Identity > Monitoring & health > Sign-in logs
- Start policies in Report-only mode, test, then switch to On.
- Keep the Travel Exception group membership reviewed and time-bound.
- Use least privilege and enforce MFA for all access.