Restricting Users to Specific App Access & by Location in Microsoft Entra ID

Field	Details
Document Type	Runbook
Applies To	Entra ID, Managed Applications
Audience	Identity Administrators
Author	AK. Udofeh
Last Updated	July 2026

Overview
This configuration restricts a specific user or group to accessing only a defined set of target applications, while simultaneously ensuring those allowed applications can only be accessed from a trusted network location.

It is important because it prevents compromised credentials from being used outside corporate boundaries or on unapproved applications. This mitigates the risk of data exfiltration from unauthorised applications and blocks lateral movement from untrusted geographic locations or IP addresses.

Prerequisites

- **Licenses**: Microsoft Entra ID P1 or P2.
- **Roles**: Conditional Access Administrator or Global Administrator.
- **Dependencies**: A pre-configured Named Location (IP range or country-based) in Entra ID.
- **Preparation**: Identify the exact user(s), the specific allowed application, and ensure a break-glass administrator account is excluded from testing.

Step 1: Navigation & Entry Point

1. Log in to the **Microsoft Entra admin center** (https://entra.microsoft.com).
2. Expand the left menu and navigate to **Protection** > **Conditional Access**.
3. Click on **Policies** > **New policy**.

Step 2: Scope Configuration (Policy 1 & 2)
You must create two separate policies to achieve this setup without logic conflicts.

For Policy 1 (Block Unapproved Apps) & Policy 2 (Location Restrict App):

1. Under **Assignments**, click on **Users**.
2. Under **Include**, choose **Select users and groups**.
3. Check **Users and groups** and select your target restricted user.
4. Under **Exclude**, ensure your global emergency access ("break-glass") account is listed.

Step 3: Target Resources
For Policy 1 (Block Unapproved Apps):

1. Under **Target resources**, select **Cloud apps**.
2. Under **Include**, select **All cloud apps**.
3. Under **Exclude**, select **Select excluded cloud apps** and choose your `[Target Allowed App]` (e.g., Office 365).

For Policy 2 (Location Restrict App):

1. Under **Target resources**, select **Cloud apps**.
2. Under **Include**, select **Select apps** and choose the identical `[Target Allowed App]` excluded in Policy 1.
3. Leave the **Exclude** tab completely empty.

Step 4: Core Network Configuration (Policy 2 Only)

1. In Policy 2, go to **Conditions** > **Network**.
2. Set **Configure** to **Yes**.
3. Under the **Include** tab, select **Any location**.
4. Under the **Exclude** tab, select **Selected locations**.
5. Choose your pre-configured trusted **`[Named Location]`**.

Step 5: Access Control Enforcement
For both Policy 1 and Policy 2:

1. Under **Access controls**, click on **Grant**.

2. Select the radio button for **Block access**.
3. Click **Select**.

> Policy 1 blocks all other apps everywhere. Policy 2 blocks the allowed app everywhere except inside your named location.

Step 6: Testing & What If Validation

1. Set the **Enable policy** toggle at the bottom of both policies to **Report-only** and click **Save**.
2. In the Conditional Access menu, click **What If** at the top.
3. Under **User**, select your test user.
4. Under **Cloud apps**, select your `[Target Allowed App]`.
5. Under **IP address**, type an external/untrusted IP address and click **What If**.
6. Verify under **Policies that will apply** that Policy 2 shows a "Block" result.
7. Change the **IP address** to your trusted corporate IP and run the tool again; Policy 2 should now appear under **Policies that will not apply**.

Step 7: Monitoring & Validation

1. Navigate to **Identity** > **Monitoring & health** > **Sign-in logs**.
2. Filter by the targeted user's name.
3. Click on a specific sign-in row and open the **Conditional Access** tab.
4. Review the policies listed to confirm they are evaluating as **Success** (meaning the logic triggered correctly) or **Not Applied** based on the location and app targeted.

Step 8: Enforcement & Go-Live

1. Open Policy 1 and Policy 2.
2. Change the **Enable policy** toggle from *Report-only* to **On**.
3. Click **Save**.
4. Monitor the live **Sign-in logs** closely for the next 24 hours to catch any unexpected user disruption or overlooked application dependencies.

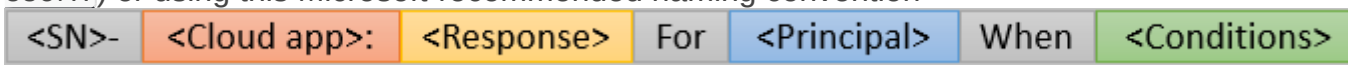
> **Important Considerations**

- **Admin Lockout**: Forgetting to exclude a break-glass account while testing broad "Block" rules can result in total tenant lockout if the scope is accidentally applied to all users.

- **Baseline Services**: Blocking "All cloud apps" can sometimes restrict access to background Microsoft utilities like the Entra ID Enrollment service or My Apps portal; verify user workflow dependencies during the report-only phase.
- **IPv6 Mismatches**: If your network provider or user device utilises IPv6 and only IPv4 was added to the Named Location, the user will be blocked unexpectedly.

Best Practices

- **Use Descriptive Names**: Name your policies clearly using a standard prefix (e.g., `CA-Strict-Block-NonTargetApps-UserX` and `CA-Strict-LocationRestrict-TargetApp-UserX`) or using this Microsoft-recommended naming convention

  Dynamic IPs: Avoid using country-based locations if precision is required, as cellular networks often map to incorrect geographic regions. Use explicit public egress IP ranges.
- **Review Cycle**: Audit named locations quarterly to ensure deprecated office IPs or altered remote boundaries are removed or updated.

Summary

- **Implementation**: A two-policy Conditional Access architecture that isolates a user's app catalog and restricts their remaining allowed workload to a trusted network boundary.
- **Impact**: Enforces true zero-trust containment on high-risk or specialised accounts, ensuring data cannot be accessed from outside designated corporate perimeters.

Revision #1
Created 2026-07-20 14:24:36 UTC by AK. Udofeh
Updated 2026-07-20 15:21:17 UTC by AK. Udofeh