PHASE 17: Zero Trust & Conditional Access (CA)

Implement identity-first security using Microsoft Entra ID (formerly Azure AD) to enforce Conditional Access, device compliance, MFA, and geo-blocking — just like in real-world enterprise Zero Trust architectures.

Enforce access control based on device health, user risk, location, and compliance using built-in Entra ID Conditional Access.

I. Step-by-Step Setup

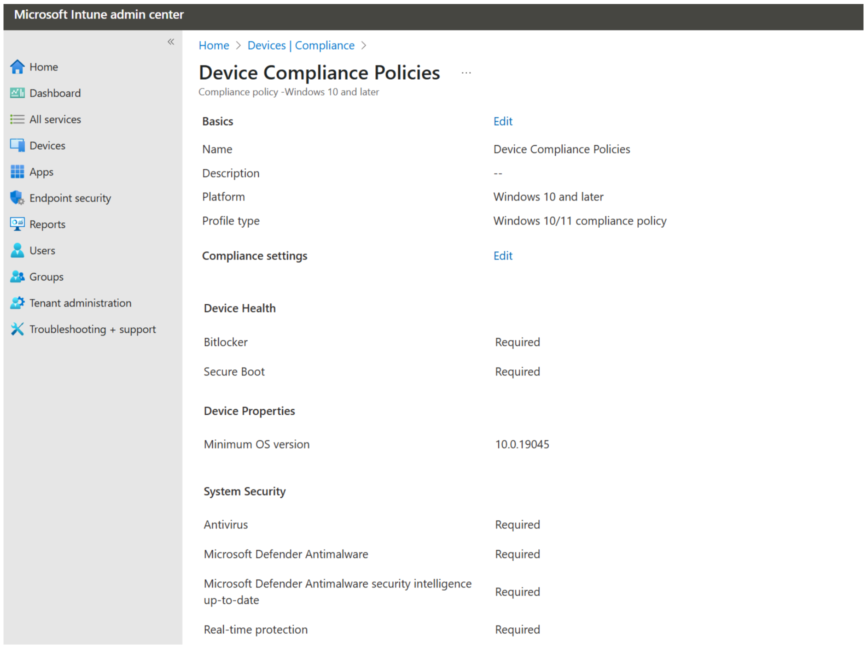
Step 1: Define Device Compliance Policies in Intune

Go to: https://endpoint.microsoft.com → Devices → Compliance policies

Create a policy for Windows 10/11:

- Require BitLocker enabled
- Require Antivirus (Microsoft Defender)
- Minimum OS version: 10.0.19045
- Require secure boot
- Mark as "Not Compliant" if not met

Assign it to: "Cloud Devices" group



Device Compliance Policies

Compliance policy -Windows 10 and later

Basics

Name	Device Compliance Policies
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings

Device Health

Bitlocker	Required
Secure Boot	Required

Device Properties

Minimum OS version	10.0.19045

System Security

Antivirus	Required
Microsoft Defender Antimalware	Required
Microsoft Defender Antimalware security intelligence up-to-date	Required
Real-time protection	Required

⏱ Wait 30 mins to apply

Step 2: Create Conditional Access Policy – Block Non-Compliant Devices

Go to: https://entra.microsoft.com → Protection → Conditional Access → + New policy

Name: Block Access – Non-Compliant Devices

✔ Users: Include → All users

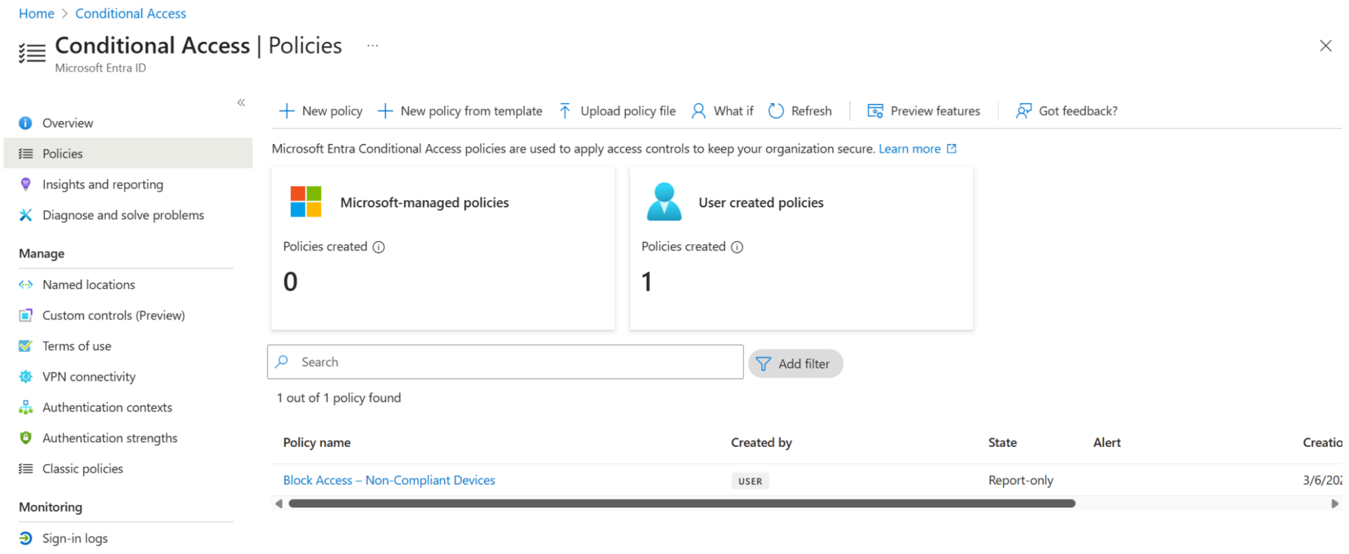
✔ Target apps: All cloud apps

✔ Conditions → Device plateform → Include All

✔ Grant access: Require device to be marked as compliant

→ Block if not compliant

✔ Session: None



Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

Microsoft-managed policies
Policies created
0

User created policies
Policies created
1

1 out of 1 policy found

Policy name	Created by	State	Alert	Creatio
Block Access – Non-Compliant Devices	USER	Report-only		3/6/20

Result: Only Intune-compliant, enrolled devices will access M365.

Step 3: Geo-IP Blocking – Block Login from Outside Country

Still in Conditional Access → + New policy

Name: Block Foreign Sign-Ins

✔ Users: All users

✔ Cloud apps: All

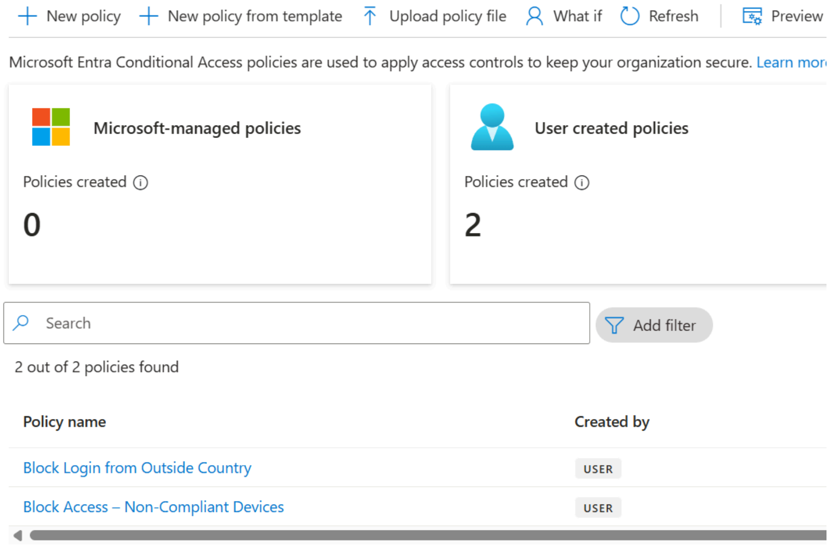
✔ Conditions → Locations:

→ Include: All locations

→ Exclude: Canada (or your current country)

✔ Grant: Block access

✔ Enable: On



Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn mor

Microsoft-managed policies

Policies created ⓘ

0

User created policies

Policies created ⓘ

2

2 out of 2 policies found

Policy name	Created by
Block Login from Outside Country	USER
Block Access – Non-Compliant Devices	USER

Result: Sign-ins from outside Canada will be denied (ideal for small teams)

Step 4: Require MFA for Admin Roles

Name: Enforce MFA for Admins

✔ Users: Roles → Include → All admin roles

✔ Apps: All

✔ Conditions → Sign-in risk = Medium and above

✔ Grant: Require MFA

✔ Enable: On

⏱ You can also enable Microsoft Entra Identity Protection for more granular risk-based CA (available in E5)

Step 5: Block Legacy Authentication (POP/IMAP/SMTP Basic)

Name: Block Legacy Auth

✔ Users: All

✔ Client Apps → Other clients (legacy)

✔ Grant → Block access

Legacy protocols like:

- Outlook 2010 or older
- Basic SMTP/POP (unauthenticated)
- Mobile clients that don't support modern auth

This is a major security gap closed in real companies.

Step 6: Test Policy with Break-Glass Account

Create an emergency admin account excluded from all CA:

- Name: breakglassadmin@dipeshcorp.onmicrosoft.com
- Strong password, store in your password vault
- Exclude from CA policies to avoid lockout
- No MFA — used only for emergency portal access

Step 7: Monitor CA Effectiveness

Go to: https://entra.microsoft.com → Monitoring → Sign-in logs

Filter by: Failure reason: Conditional Access & Result: Blocked, MFA Required, Compliant

You’ll see why logins failed or were granted.