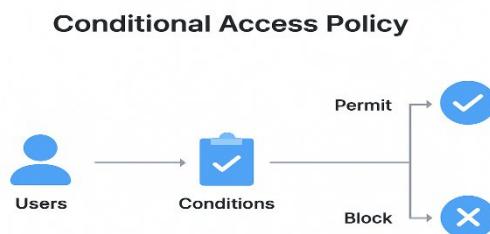


Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Conditional Access Policy (Microsoft):

What is Conditional Access Policy: Conditional Access Policy is one of the most powerful tools in Microsoft 365 security. It helps organizations protect against password theft, risky sign-ins, and unauthorized device access by enforcing conditions that must be met before granting access to company resources.



Purpose: As part of Cybersecurity protection/mitigation, conditional access acts as part of an organization's cybersecurity defense strategy. Its primary purpose is to protect and prevent access from:

- Password Theft
- Risky Sign-ins
- Unmanaged Devices

Conditional Access in Microsoft 365 – Real-World Scenarios:

Conditional Access in Microsoft 365 is where **Security** gets real and **controls the Risk**.

We will learn how to Secure your Business Data:

- Control access for contractors and temporary staff (browser-only access)
- Protect sensitive sites like Finance and HR with authentication contexts
- Automatically block compromised users with high-risk policies
- Manage sign-in frequency and persistent browser sessions for better security

These are practical examples we can implement straight away, designed to help you tighten security without breaking productivity.

Application/Technical Configuration:

Policy 1: Control access for contractors and temporary staff (browser-only access).

Create a policy to **CA-Contractors - All Apps - Block Mobile & Desktops Apps**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Contractors
- Target Resources > All resources (Formerly “All cloud apps”)
- Conditions > Client Apps > Configure Click Yes > Untick Browser
- Click Grant > Block Access

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with various navigation links like 'Overview', 'Users', 'Groups', etc. The main area is titled 'New Conditional Access policy'. It has several sections: 'Assignments' (Users: Specific users included), 'Target resources' (No target resources selected), 'Network' (NEW, Not configured), 'Conditions' (0 conditions selected, highlighted with a red arrow), 'Access controls' (Grant: 0 controls selected), 'Session' (0 controls selected), and 'Client apps' (Not configured). On the right, there's a panel titled 'Client apps' with a description: 'Control user access to target specific client applications not using modern authentication.' Below it is a 'Configure' button with 'Yes' and 'No' options. Further down, it says 'Select the client apps this policy will apply to' and lists 'Modern authentication clients' (Browser is unchecked, indicated by a red arrow) and 'Legacy authentication clients' (Mobile apps and desktop clients, Exchange ActiveSync clients, Other clients are checked). At the bottom right of the main area, there's a 'Enable policy' button.

- The purpose of this policy is specifically for the **admins**, while regular staff can use the **Required strong MFA**.

Policy 2: CA-Contractors - SharePoint & OneDrive APP Enforce Restriction

Create a policy to **CA-Contractors - SharePoint & OneDrive APP Enforce Restriction**. Click in Microsoft 365 Admin Center > **Conditional Access > Policies > New Policy**

- Select User > Select Users and Group > Select the Group of Users which is CA - Contractors.
- Target Resources > **Include: Select resources** > Select specific resources: **Office 365** (This includes SharePoint and One Drive)
- Session > Tick/Check Use app enforce restrictions (**They can view, but they can't download, it's like a read only.**)

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like 'Overview', 'Users', 'Groups', etc. The main area is titled 'New Conditional Access policy' and shows a policy named 'CA-Contractors - SharePoint & OneDrive ...'. Under the 'Session' section, there's a checkbox for 'Use app enforced restrictions' which is checked. Other options like 'Use Conditional Access App Control', 'Sign-in frequency', etc., are listed below. A red arrow points to the 'Session' section.

- click Create

Policy 3: Entra High Risk User Policy (This is like a Digital Kill Switch) in policy.

Create a policy for All users - All Apps - High Risk - Block Access. Click in Microsoft 365 Admin Center > Conditional Access > Policies > New Policy

- Select User > All users (be extra careful not to block your admin account) > Click Exclude > Click All Admin Group of User you create e.g. CA – Break Glass (These are the group of Admin users inside) or your account as an Administrator.
- Target Resources > All resources (Formerly “All cloud apps”)
- Conditions > User risk > Configure = Yes > Click/Tick High > Done

The screenshot shows the Microsoft Entra admin center interface. The 'User risk' section is selected, showing a 'Configure' button with 'Yes' selected and a checkbox for 'High' which is checked. Other options like 'Medium' and 'Low' are available but unchecked. A red arrow points to the 'Yes' button and another red arrow points to the 'High' checkbox.

- Click Grant > Click Block

Policy 4: Protecting Sensitive Data with Authentication Contexts. Require compliant device conditional access policy.

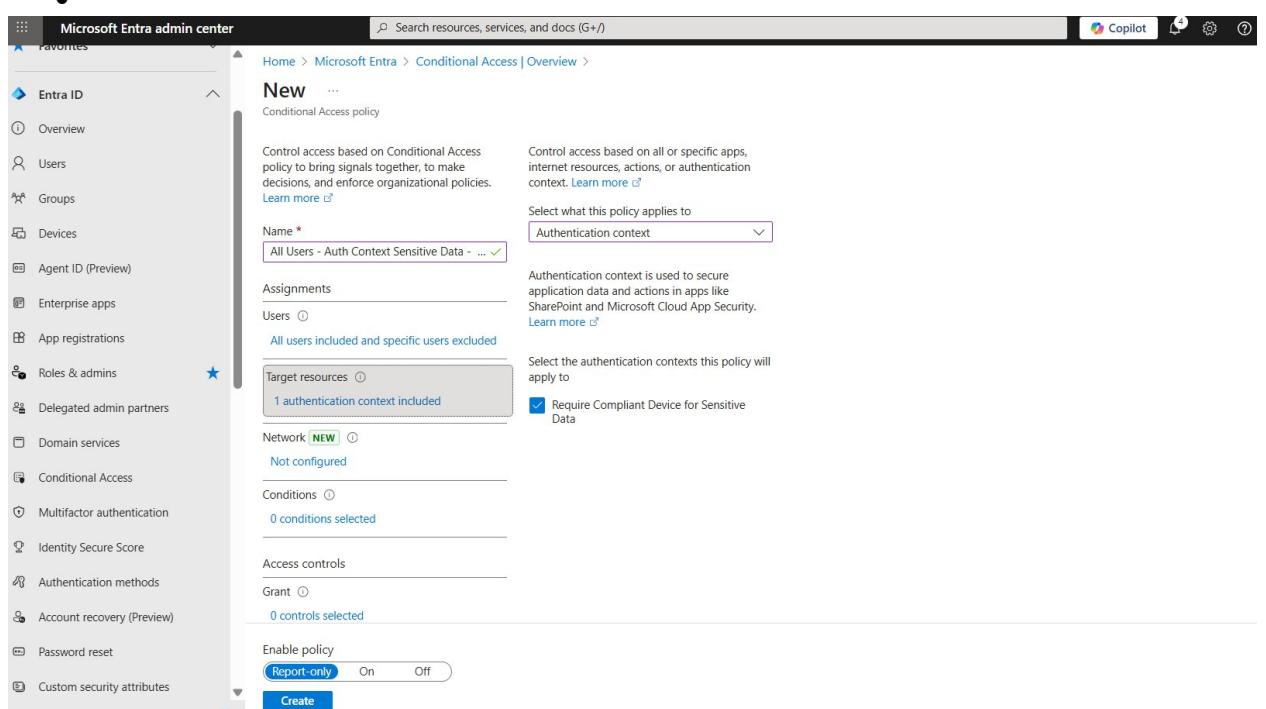
What is Authentication Context? = Think this as a trigger in any sensitive data or content like: Finance, HR and, Legal. When someone tries to open this, we will enforce an extra security rule. Now, on this we will target specific sites.

Microsoft 365 Admin Center > Conditional Access > Authentication Contexts

- Click New authentication context > Name: Require Compliant Device for Sensitive Data > Click Save

Now, we will go back to Conditional Access

- Create new policy for **All Users - Auth Context Sensitive Data - Require Compliant Device**. Click in Conditions > Client apps > Configure Yes > Uncheck the browser > Click Done
- Select User > **All users (be extra careful not to block your admin account)** > Click Exclude > Click All Admin Group of User you create e.g. CA – Break Glass (These are the group of Admin users inside) or your account as an Administrator.
- **Click Target Resources** > Select what this policy applies to Choose in dropdown the **Authentication context** > **Click/Tick require Compliant Device for Sensitive Data**



- **Click Grant > Click Grant access > Tick Require authentication strength: Phishing-resistant MFA > Require device to be marked as compliant**

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Overview, Users, Groups, Devices, etc. The main area is titled 'New ... Conditional Access policy' and shows a step-by-step configuration process. The 'Name' field is set to 'All Users - Auth Context Sensitive Data'. Under 'Assignments', it says 'Users' and 'All users included and specific users excluded'. In the 'Grant' section, the 'Grant access' radio button is selected. Other options shown include 'Require authentication strength' (selected), 'Phishing-resistant MFA' (selected), and 'Require device to be marked as compliant'.

- Click Create

Now, once applied we will configure this with our **PowerShell (run as admin)**, copy and paste below.

```
Connect-SPOService -Url https://hawthornebell-admin.sharepoint.com

Set-SPOSite -Identity https://hawthornebell.sharepoint.com/sites/Finance |
    -ConditionalAccessPolicy AuthenticationContext |
        -AuthenticationContextName "Require Compliant Device for Sensitive Data"

Get-SPOSite -Identity https://hawthornebell.sharepoint.com/sites/Finance |
    Format-List Url,ConditionalAccessPolicy.AuthenticationContextName
```

Policy 5: How long people can stay sign-in: Sign-in Frequency & Persistent Browser sessions

Now, we will go back to Conditional Access

- Create new policy for **All Users – Browser Sessions – Sign-in Frequency**.
- Select User > **All users** (be extra careful not to block your admin account) > Click Exclude > Click All Admin Group of User you create e.g. CA – Break Glass (These are the group of Admin users inside) or your account as an Administrator.
- **Click Target Resources** > All resources (formerly 'All cloud apps')
- **Session > Click Sign-in frequency (8 | hours) > Click Persistent browser session (Never Persistent)**

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, and Authentication methods. The main content area shows a 'Conditional Access | Overview' page with a 'New' button. Under 'Assignments', it says 'All users included and specific users excluded'. Under 'Target resources', it says 'All resources (formerly 'All cloud apps')' and 'Network [NEW] (Not configured)'. Under 'Conditions', it says '0 conditions selected'. Under 'Access controls', it says 'Grant (0 controls selected)'. Under 'Session', it says '0 controls selected'. At the bottom, there's an 'Enable policy' section with 'Report-only' set to 'On' and a 'Create' button. On the right, a 'Session' configuration pane is open, showing 'Use app enforced restrictions' (unchecked), 'Sign-in frequency' (checked), 'Periodic reauthentication' (selected, value 8, unit Hours), 'Every time' (radio button), 'Persistent browser session' (checked), 'Never persistent' (selected), and other optional settings like 'Customize continuous access evaluation' and 'Disable resilience defaults'. A red arrow points to the 'Sign-in frequency' checkbox, and another red arrow points to the 'Persistent browser session' checkbox.

Sources:

1. Advanced Conditional Access for IT Pros | Complete Guide
<https://www.youtube.com/watch?v=DkCq8wWN9Sc>

2. How to Set Up Conditional Access in Microsoft 365 (Step-by-Step) By Jonathan Edwards
<https://www.youtube.com/watch?v=5oMaZink7kc>

”When you train Smarter, you defend Stronger”
 Leonard Estos