



# Steps to setup MFA & granular CA policy for SharePoint sites

# Contents

- Pre-Requisite ..... 2
- Step 1: Configure Conditional Access Policy in Azure..... 2
  - To Block Access ..... 4
  - To Restrict Access ..... 4
- Step 2: Connect the Azure Policy to a SharePoint site..... 5
  - Testing..... 5
- Step 3: (Optional) Terms of use ..... 5
- Step 4: (Optional) Sign-in Frequency ..... 8
  - Scenarios: ..... 8
- Known limitation in preview ..... 9

## Pre-Requisite

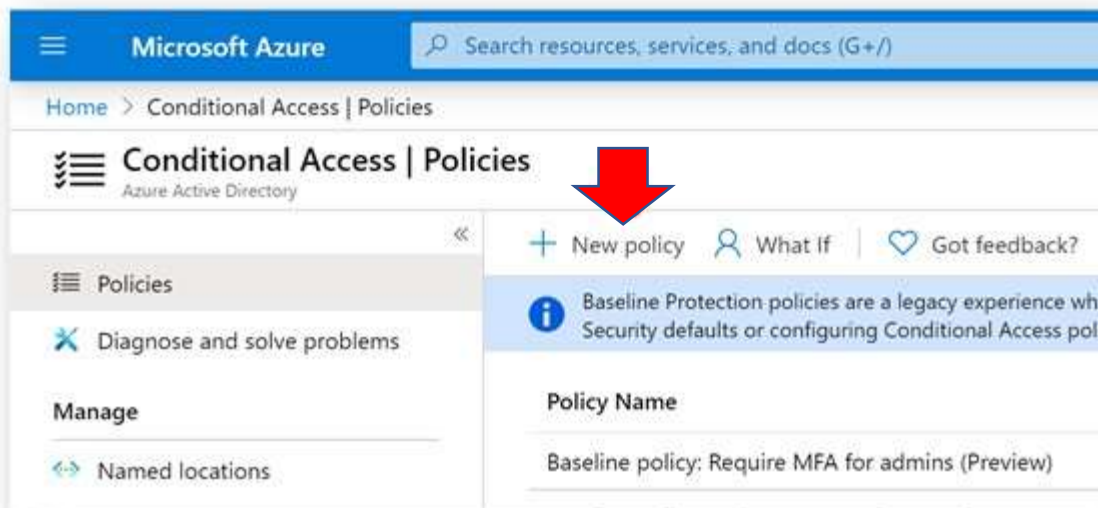
- Minimum license requirement AAD P1
- We recommend testing in a dev/test environment
- Download and install latest SPO PowerShell from here <https://www.microsoft.com/en-us/download/details.aspx?id=35588>
- Install-Module -Name Microsoft.Online.SharePoint.PowerShell -RequiredVersion 16.0.19927.12000

## Step 1: Configure Conditional Access Policy in Azure

1. Sign-in to the below AAD URL  
[https://portal.azure.com/?causeractions=true&caaccessrequirementsactions=true#blade/Microsoft\\_AAD\\_IAM/ConditionalAccessBlade/Policies](https://portal.azure.com/?causeractions=true&caaccessrequirementsactions=true#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies)

NOTE: Above URL required. Direct navigation will provide preview features

2. Click on “New Policy”



3. Name your policy, then under Assignments expand Users and Groups. Select the users and groups you wish to assign the policy to.

NOTE: To prevent lock we do not recommend using the “All Users” option

4. Open Cloud *apps or actions* and select the *User actions* option. For the **Granular MFA** preview feature you will need to select *Accessing secured app data*.

A. Selecting this option opens three levels that are called *Authentication Tags*. Each tag can be associated with a different policy set for assignment. The levels will be associated as follows:

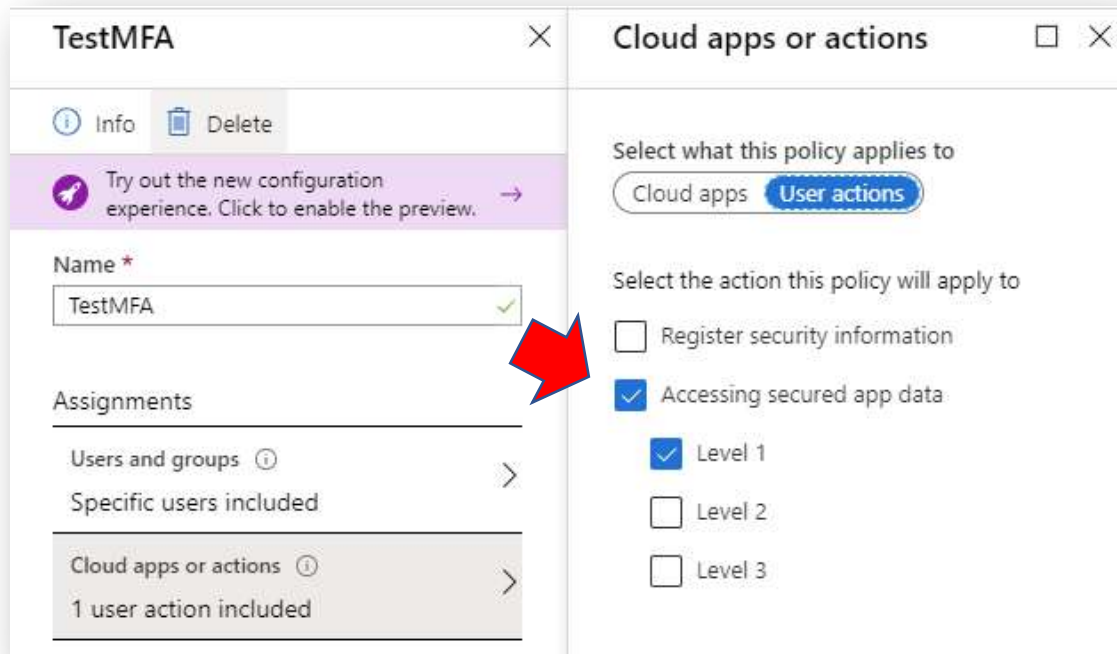
Level 1 urn:microsoft:req1

Level 2 urn:microsoft:req2

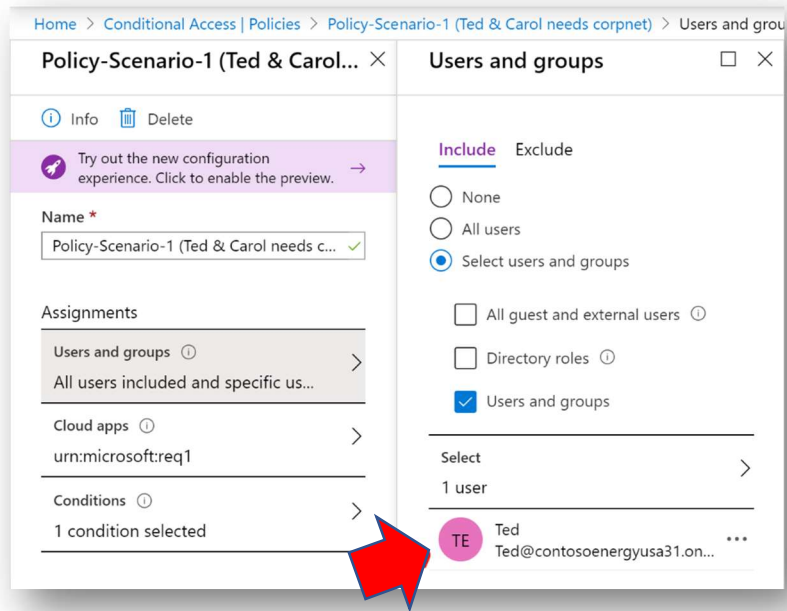
Level 3 urn:microsoft:req3

NOTE: These assignments will be used again later in the process

B. Multiple policies can share the same tag based on your requirements. For instance, you may have one policy one for “compliant devices” and a second policy for “trusted network”, both policies can use the same tag. Tags will be assigned to a site collection and all policies that reference that tag will be evaluated.



NOTE: For testing purposes this document will outline adding a single user in a simple CA policy



5. Under **Access Controls** click *Grant* to open the options panel.

#### To Block Access

1. Under Grant → Select the *Block* access option
2. Click Select

**NOTE:** This will restrict access to site, regardless of permissions, to users who have this policy assigned

#### To Restrict Access

1. Select the Grant access option
2. Choose the condition **Require multi-factor authentication**
3. Click Select



6. Under **Enable policy**, choose "ON" to activate the policy.

## Step 2: Connect the Azure Policy to a SharePoint site

To make use of this policy it must be linked to a sites collection. A single policy can be linked to multiple sites. Linking a policy to a specific site must done using PowerShell

1. Open the [SharePoint Online Management Shell](#)
2. Type: **\$cred = get-credential**
3. Enter credentials with Admin Access
4. Type: **connect-SPOservice -credential \$cred -Url <admin site url>**
5. Use the command Set-SPOsite to link the policy:

```
Set-SPOsite -Identity https://contosoenergyusa31.sharepoint.com/sites/Finance -  
ConditionalAccessPolicy ProtectionLevel -ProtectionLevelName "urn:microsoft:req1"
```

**NOTE:** The PowerShell command uses the level references listed previously in this document

6. Once complete allow time for propagation (<5 min)

## Testing

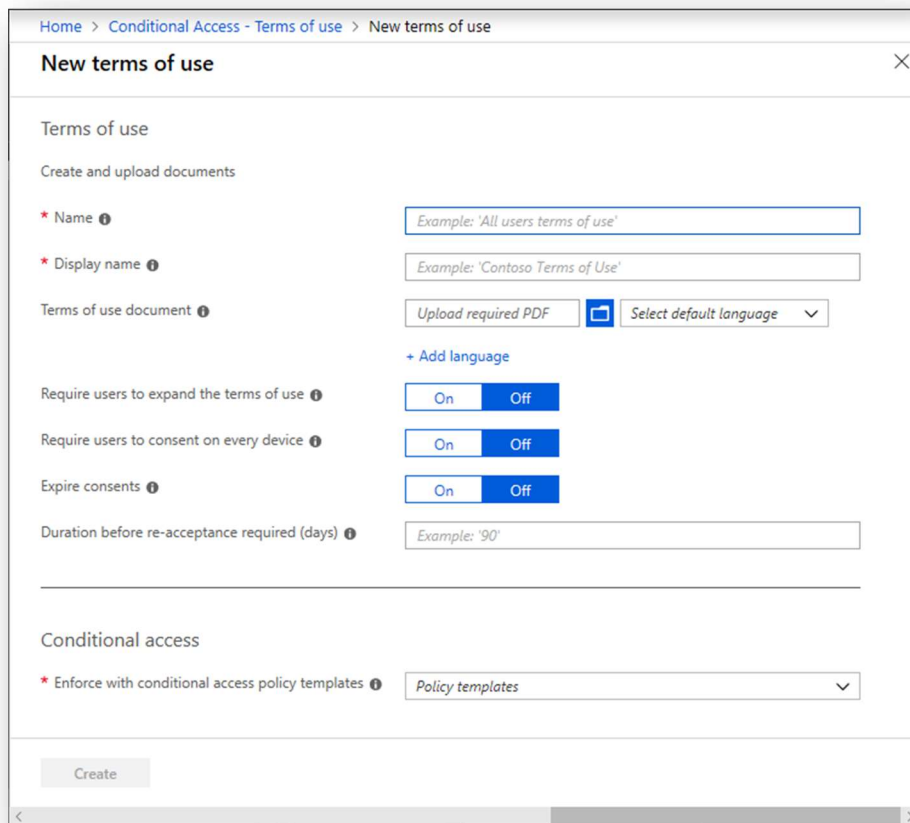
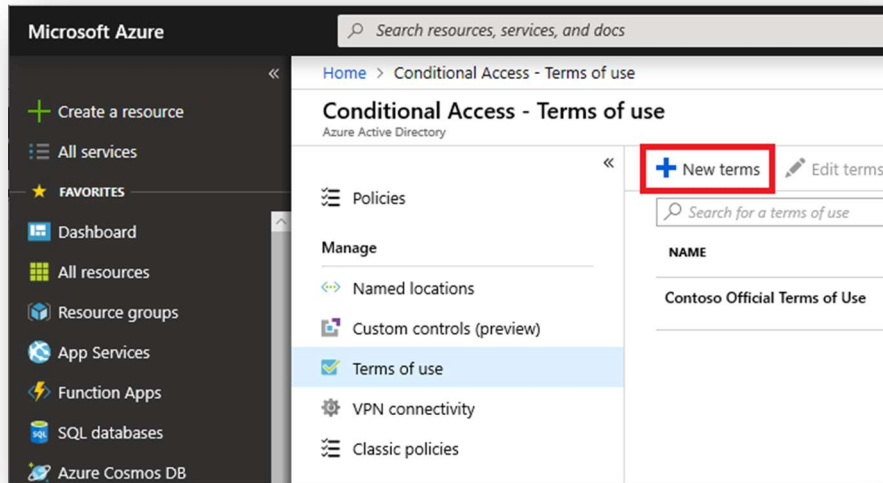
1. Ensure that user you are testing has permission to the site the policy was assigned to.
2. Open a browser to portal.office.com
3. Sign in as a user that was assigned the policy created from the steps list above.
4. Click the SharePoint app tile
  1. If no MFA policy was previously configured, the user will be able to access the SharePoint Home page without further required action
5. Navigate to the site URL the policy was linked to previously.
  1. The user will be presented with an MFA Prompt for additional security access
    - a. If the user had not previously been configured for MFA, they will be required to follow on-screen instructions to complete the process
  2. If Block Access was assigned, the user should not gain access to the site.

## Step 3: (Optional) Terms of use

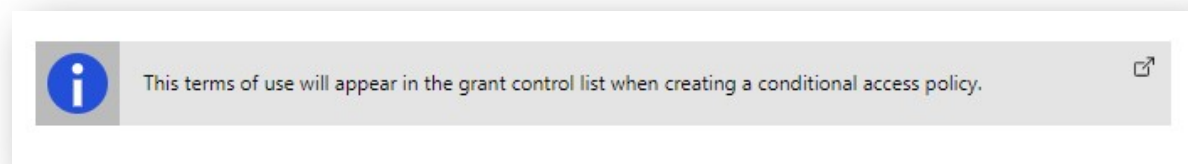
Along with the granular control for MFA on a site collection, you can attach a [Terms of Use](#) policy to your granular per site policy. This will allow you to outline specific guidelines that detail the extra layer of security and usage.

1. Sign in to Azure as a Global Administrator, Security Administrator, or Conditional Access Administrator.

2. Navigate to **Terms of use** at <https://aka.ms/catou>.
3. Click **New terms**.



4. In the **Name** box, enter a name for the terms of use that will be used in the Azure portal.
5. In the **Display name** box, enter a title that users see when they sign in.
6. For **Terms of use document**, browse to your finalized terms of use PDF and select it.
7. Select the language for your terms of use document. The language option allows you to upload multiple terms of use, each with a different language. The version of the terms of use that an end user will see will be based on their browser preferences.
8. To require end users to view the terms of use prior to accepting them, set **Require users to expand the terms of use to On**.
9. For **Enforce with conditional access policy templates** select *Create conditional access policy later* from the drop down.



10. Create your policy as outlined in [Step 1](#). Under **Access Controls** you will now see your Terms of Use policies. Select the desired terms policy

**Grant**

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Secure Site A

Secure Site A

For multiple controls

Require all the selected controls

Require one of the selected controls

**NOTE:** For more additional Terms of Use configuration options see this [link](#).

## Step 4: (Optional) Sign-in Frequency

Along with the granular control for MFA on a site collection, you can utilize session management with your Conditional Access policy with Sign-in frequency. Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

1. Create your policy as outlined in [Step 1](#).
2. Go to Access Controls > Session and click Sign-in frequency.
3. Enter the required value of days and hours in the first text box.
4. Select a value of Hours or Days from dropdown.
5. Click Select.
6. Save your policy.

The screenshot shows the 'Session' configuration page in Azure AD. The 'Sign-in frequency' option is checked and highlighted with a callout box. The callout box shows a text input field containing '1' and a dropdown menu set to 'Hours'. Below this, the 'Persistent browser session' option is unchecked.

### Scenarios:

- SharePoint Online site with no policy applied
  - User 1 logs in and connects to SiteA
  - User 1 locks computer with session open and active for 1+ hours
  - User 1 opens device, refreshes page and continues to work with no reauthentication required
- SharePoint Online site with session management policy applied
  - User 1 logs in and connects to SecureSiteB
  - User 1 is present with MFA security requirements
  - User 1 locks computer with session open and active for 1+ hours
  - User 1 opens device, refreshes page
  - User 1 is required to enter credentials
  - User 1 is present with MFA security requirements

## Known limitation in preview

- OneDrive Sync client will not be able to sync libraries in a site with this policy applied
- Office files will only load in the Office Web Apps (Word, Excel, PowerPoint)
- The Teams App (desktop and web) will not load the files. To interact with the files, direct navigation to the site in SharePoint is required.
- OWA will not be able to add file attachments to an email pulling from the site. To send a file located in the site collection, navigate to the site URL and use the “Share” options to send a link. Access is subject to the policy.
- Workflows will no longer on the site. Workflow authentication does not work MFA requirements.