

Microsoft Entra Conditional Access documentation

Learn how to configure and test Microsoft Entra Conditional Access

About Conditional Access

OVERVIEW

[What is Conditional Access?](#)

CONCEPT

[What are conditions?](#)

[How can I define locations?](#)

[Conditional Access service dependencies](#)

Deploy Conditional Access

CONCEPT

[Plan a Conditional Access deployment](#)

HOW-TO GUIDE

[Block legacy authentication](#)

[Troubleshooting using the What If tool](#)

Common Conditional Access policies

CONCEPT

[Common Conditional Access policies](#)

HOW-TO GUIDE

Require MFA for administrators

Require MFA for Azure management

Block legacy authentication

Risk-based Conditional Access (Requires Microsoft Entra ID P2)

Require trusted location for MFA registration

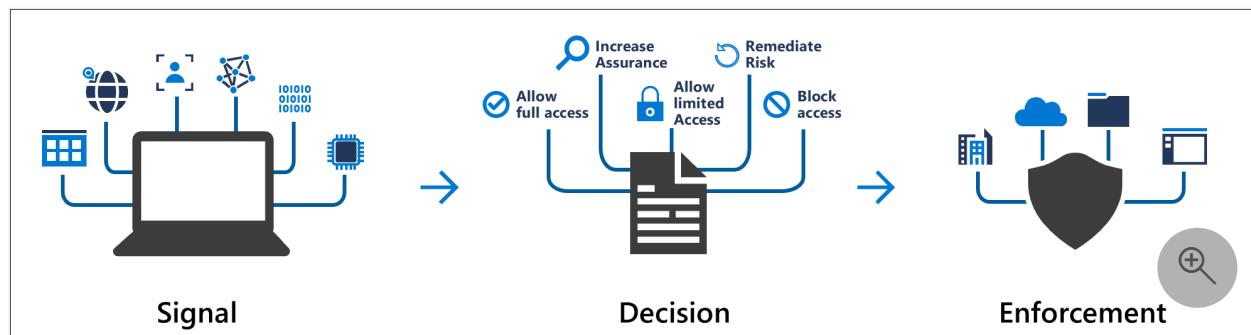
Block access by location

Require compliant device

What is Conditional Access?

Article • 03/04/2025

Modern security extends beyond an organization's network perimeter to include user and device identity. Organizations now use identity-driven signals as part of their access control decisions. Microsoft Entra Conditional Access brings signals together, to make decisions, and enforce organizational policies. Conditional Access is Microsoft's [Zero Trust policy engine](#) taking signals from various sources into account when enforcing policy decisions.



Conditional Access policies at their simplest are if-then statements; **if** a user wants to access a resource, **then** they must complete an action. For example: If a user wants to access an application or service like Microsoft 365, then they must perform multifactor authentication to gain access.

Administrators are faced with two primary goals:

- Empower users to be productive wherever and whenever
- Protect the organization's assets

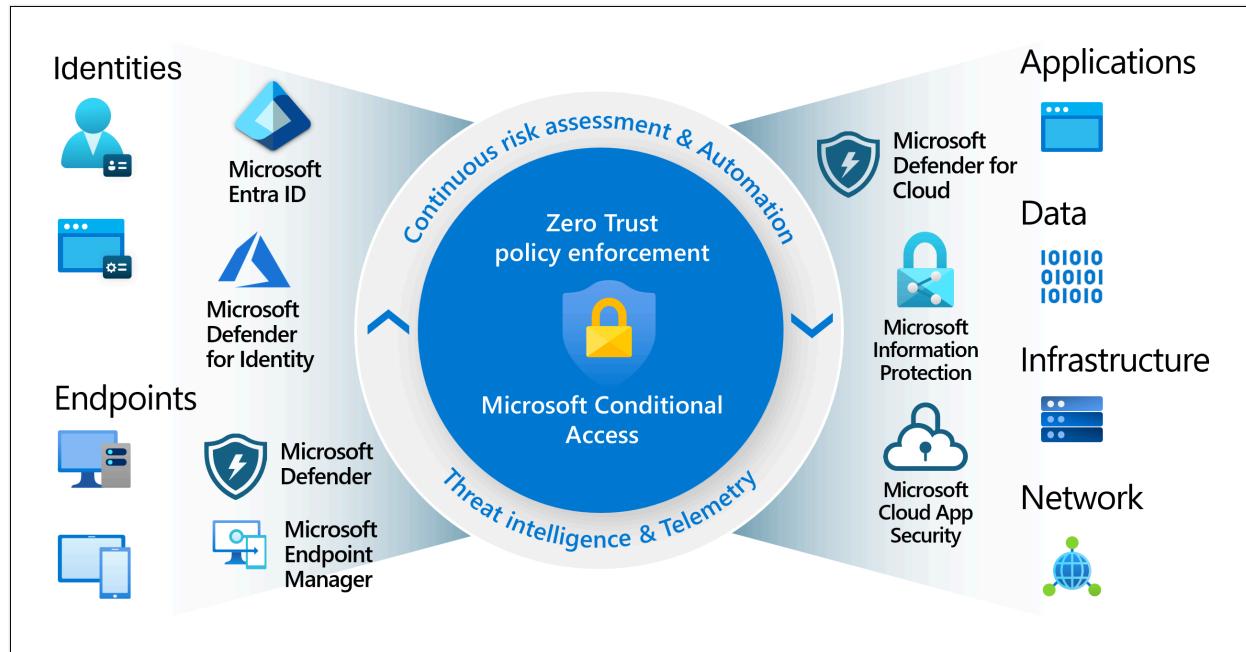
Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.

ⓘ Important

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Common signals

Conditional Access takes signals from various sources into account when making access decisions.



These signals include:

- User or group membership
 - Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
- IP Location information
 - Organizations can create trusted IP address ranges that can be used when making policy decisions.
 - Administrators can specify entire countries or regions IP ranges to block or allow traffic from.
- Device
 - Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
 - Use filters for devices to target policies to specific devices like privileged access workstations.
- Application
 - Users attempting to access specific applications can trigger different Conditional Access policies.
- Real-time and calculated risk detection
 - Signals integration with [Microsoft Entra ID Protection](#) lets Conditional Access policies identify and remediate risky users and sign-in behavior.
- [Microsoft Defender for Cloud Apps](#)
 - Lets user application access and sessions be monitored and controlled in real time. This integration increases visibility and control over access to and activities done within your cloud environment.

Common decisions

- Block access
 - Most restrictive decision
- Grant access
- Less restrictive decision that can require one or more of the following options:
 - Require multifactor authentication
 - Require authentication strength
 - Require device to be marked as compliant
 - Require Microsoft Entra hybrid joined device
 - Require approved client app
 - Require app protection policy
 - Require password change
 - Require terms of use

Commonly applied policies

Many organizations have [common access concerns](#) that Conditional Access policies can help with, such as:

- Requiring multifactor authentication for users with administrative roles
- Requiring multifactor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for security information registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications

Admins can create policies from scratch or start from a template policy in the portal or using the Microsoft Graph API.

Administrator experience

Administrators with the [Conditional Access Administrator](#) role can manage policies.

Conditional Access is found in the [Microsoft Entra admin center](#) ↗ under **Protection > Conditional Access**.

The screenshot shows the Microsoft Entra admin center Conditional Access Overview page. The left sidebar includes sections for Home, Overview, Policies, Insights and reporting, Diagnose and solve problems, Manage (Named locations, Custom controls, Terms of use, VPN connectivity, Authentication context, Authentication strengths, Classic policies), Monitoring (Sign-in logs, Audit logs), Troubleshooting + Support (New support request), and a bottom section for Security Alerts (Preview). The main content area features a Policy Snapshot summary with 5 Enabled, 17 Report-only, and 9 Off policies. It also displays sections for Devices (88% from unmanaged or non-compliant devices) and Applications (Browse unprotected apps). A General Alerts section highlights Named Locations (IPv6 update suggestion) and Security Alerts (Preview) showing 69% of sign-ins out of scope and 69% lacking multifactor authentication.

- The **Overview** page provides a summary of policy state, users, devices, and applications, as well as general and security alerts with suggestions.
- The **Coverage** page provides a synopsis of applications with and without Conditional Access policy coverage over the last seven days.
- The **Monitoring** page allows administrators to see a graph of sign-ins that can be filtered to see potential gaps in policy coverage.

Conditional Access policies on the **Policies** page can be filtered by administrators based on items like the actor, target resource, condition, control applied, state, or date. This filtering ability lets administrators find specific policies based on their configuration quickly.

License requirements

Using this feature requires Microsoft Entra ID P1 licenses. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID](#).

Customers with [Microsoft 365 Business Premium licenses](#) also have access to Conditional Access features.

Risk-based policies require access to [Microsoft Entra ID Protection](#), which requires P2 licenses.

Other products and features that interact with Conditional Access policies require appropriate licensing for those products and features.

When licenses required for Conditional Access expire, policies aren't automatically disabled or deleted. This lets customers migrate away from Conditional Access policies without a sudden change in their security posture. Remaining policies can be viewed and deleted, but no longer updated.

[Security defaults](#) help protect against identity-related attacks and are available for all customers.

Zero Trust

This feature helps organizations to align their [identities](#) with the three guiding principles of a Zero Trust architecture:

- Verify explicitly
- Use least privilege
- Assume breach

To find out more about Zero Trust and other ways to align your organization to the guiding principles, see the [Zero Trust Guidance Center](#).

Next steps

- [Building a Conditional Access policy piece by piece](#)
- [Plan your Conditional Access deployment](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Tutorial: Secure user sign-in events with Microsoft Entra multifactor authentication

Article • 03/04/2025

Multifactor authentication is a process in which a user is prompted for additional forms of identification during a sign-in event. For example, the prompt could be to enter a code on their cellphone or to provide a fingerprint scan. When you require a second form of identification, security is increased because this additional factor isn't easy for an attacker to obtain or duplicate.

Microsoft Entra multifactor authentication and Conditional Access policies give you the flexibility to require MFA from users for specific sign-in events.

Important

This tutorial shows an administrator how to enable Microsoft Entra multifactor authentication. To step through the multifactor authentication as a user, see [Sign in to your work or school account using your two-step verification method](#).

If your IT team hasn't enabled the ability to use Microsoft Entra multifactor authentication, or if you have problems during sign-in, reach out to your Help desk for additional assistance.

In this tutorial you learn how to:

- ✓ Create a Conditional Access policy to enable Microsoft Entra multifactor authentication for a group of users.
- ✓ Configure the policy conditions that prompt for MFA.
- ✓ Test configuring and using multifactor authentication as a user.

Prerequisites

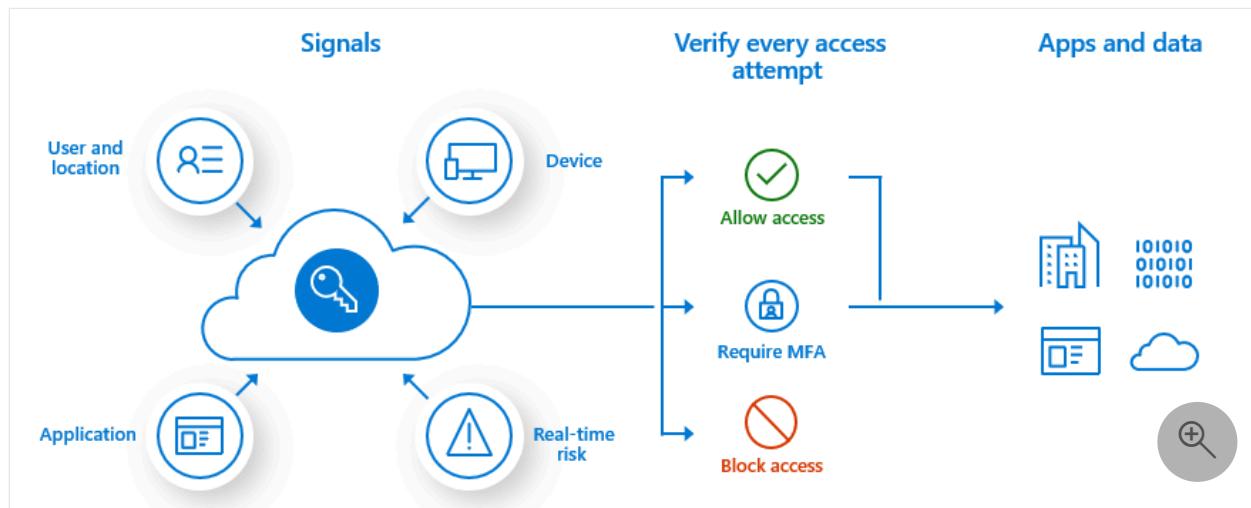
To complete this tutorial, you need the following resources and privileges:

- A working Microsoft Entra tenant with Microsoft Entra ID P1 or trial licenses enabled.
 - If you need to, [create one for free](#).

- An account with at least the [Conditional Access Administrator](#) role. Some MFA settings can also be managed by an [Authentication Policy Administrator](#).
- A non-administrator account with a password that you know. For this tutorial, we created such an account, named *testuser*. In this tutorial, you test the end-user experience of configuring and using Microsoft Entra multifactor authentication.
 - If you need information about creating a user account, see [Add or delete users using Microsoft Entra ID](#).
- A group that the non-administrator user is a member of. For this tutorial, we created such a group, named *MFA-Test-Group*. In this tutorial, you enable Microsoft Entra multifactor authentication for this group.
 - If you need more information about creating a group, see [Create a basic group and add members using Microsoft Entra ID](#).

Create a Conditional Access policy

The recommended way to enable and use Microsoft Entra multifactor authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.



Conditional Access policies can be applied to specific users, groups, and apps. The goal is to protect your organization while also providing the right levels of access to the users who need it.

In this tutorial, we create a basic Conditional Access policy to prompt for MFA when a user signs in. In a later tutorial in this series, we configure Microsoft Entra multifactor authentication by using a risk-based Conditional Access policy.

First, create a Conditional Access policy and assign your test group of users as follows:

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.

2. Browse to **Protection > Conditional Access > Overview**, select **+ Create new policy**.

The screenshot shows the Microsoft Entra admin center interface. At the top, there's a breadcrumb navigation: Home > Security | Conditional Access >. Below it is the title "Conditional Access | Overview" with a Microsoft Entra ID icon. A red box highlights the "+ Create new policy" button in the top right corner of the main content area. The navigation bar below includes tabs for Overview, Policies, Getting started, Overview (which is underlined), Coverage, Monitoring (Preview), and Tutorials. There are also links for Refresh and Got feedback?.

1. Enter a name for the policy, such as *MFA Pilot*.

2. Under **Assignments**, select the current value under **Users or workload identities**.

The screenshot shows the "New Conditional Access policy" creation page. At the top, there's a breadcrumb navigation: Home > Conditional Access >. The title is "New" with a "Conditional Access policy" subtitle. Below it is a descriptive text: "Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies." with a "Learn more" link. The "Name *" field has a placeholder "Example: 'Device compliance app policy'". The "Assignments" section is expanded, showing a red box around the "Users or workload identities" section. Inside, it says "0 users or workload identities selected". The "Cloud apps or actions" section is also visible below it.

3. Under **What does this policy apply to?**, verify that **Users and groups** is selected.

4. Under **Include**, choose **Select users and groups**, and then select **Users and groups**.

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities (i)

Specific users included

✖ "Select users and groups" must be configured

Cloud apps or actions (i)

No cloud apps, actions, or authentication contexts selected

Conditions (i)

0 conditions selected

Access controls

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

What does this policy apply to?

Users and groups

Include None All users Select users and groups All guest and external users (i) Directory roles (i) Users and groups

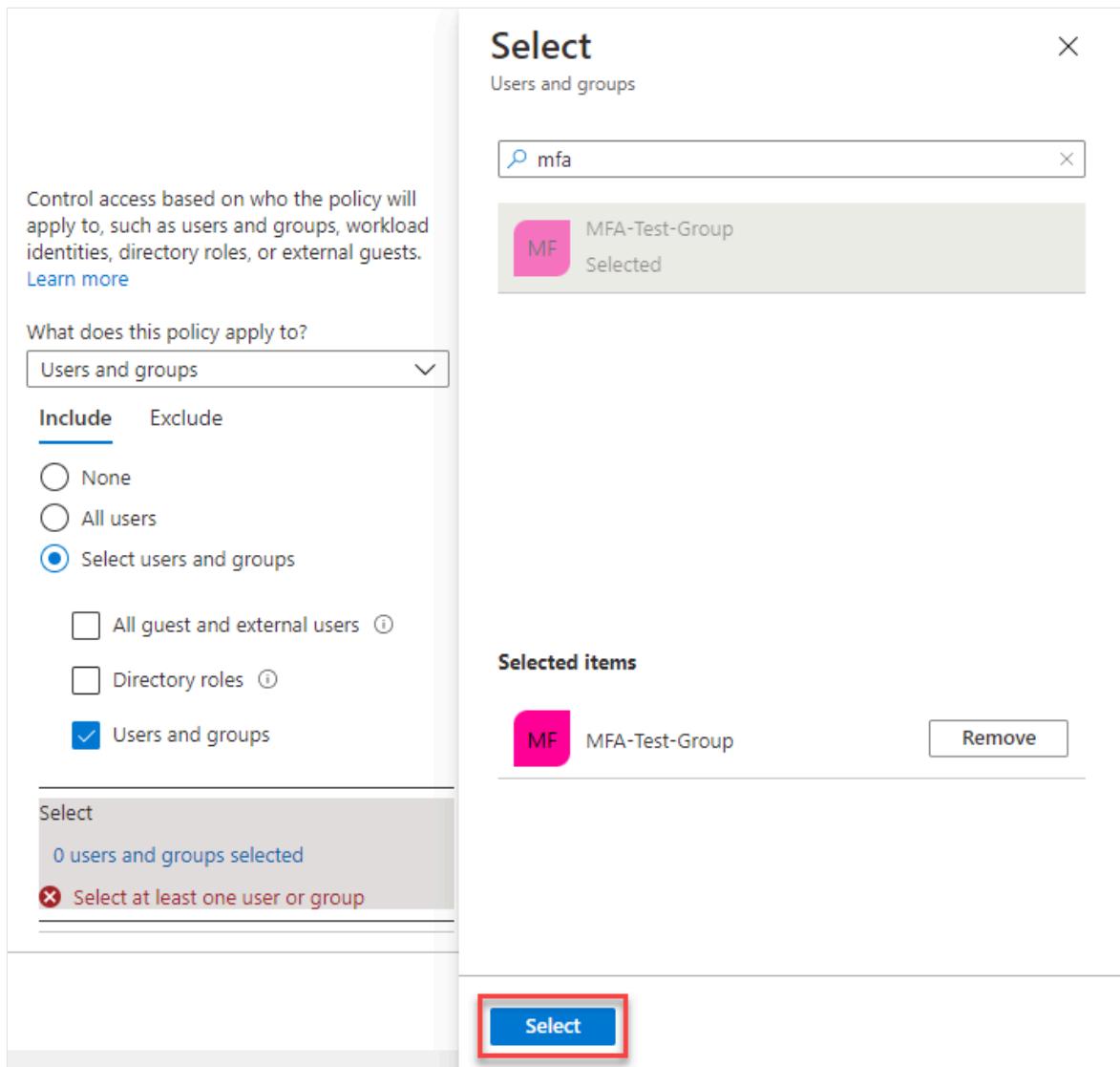
Select

0 users and groups selected

✖ Select at least one user or group

Since no one is assigned yet, the list of users and groups (shown in the next step) opens automatically.

5. Browse for and select your Microsoft Entra group, such as *MFA-Test-Group*, then choose **Select**.



We've selected the group to apply the policy to. In the next section, we configure the conditions under which to apply the policy.

Configure the conditions for multifactor authentication

Now that the Conditional Access policy is created and a test group of users is assigned, define the cloud apps or actions that trigger the policy. These cloud apps or actions are the scenarios that you decide require additional processing, such as prompting for multifactor authentication. For example, you could decide that access to a financial application or use of management tools require an additional prompt for authentication.

Configure which apps require multifactor authentication

For this tutorial, configure the Conditional Access policy to require multifactor authentication when a user signs in.

1. Select the current value under **Cloud apps or actions**, and then under **Select what this policy applies to**, verify that **Cloud apps** is selected.

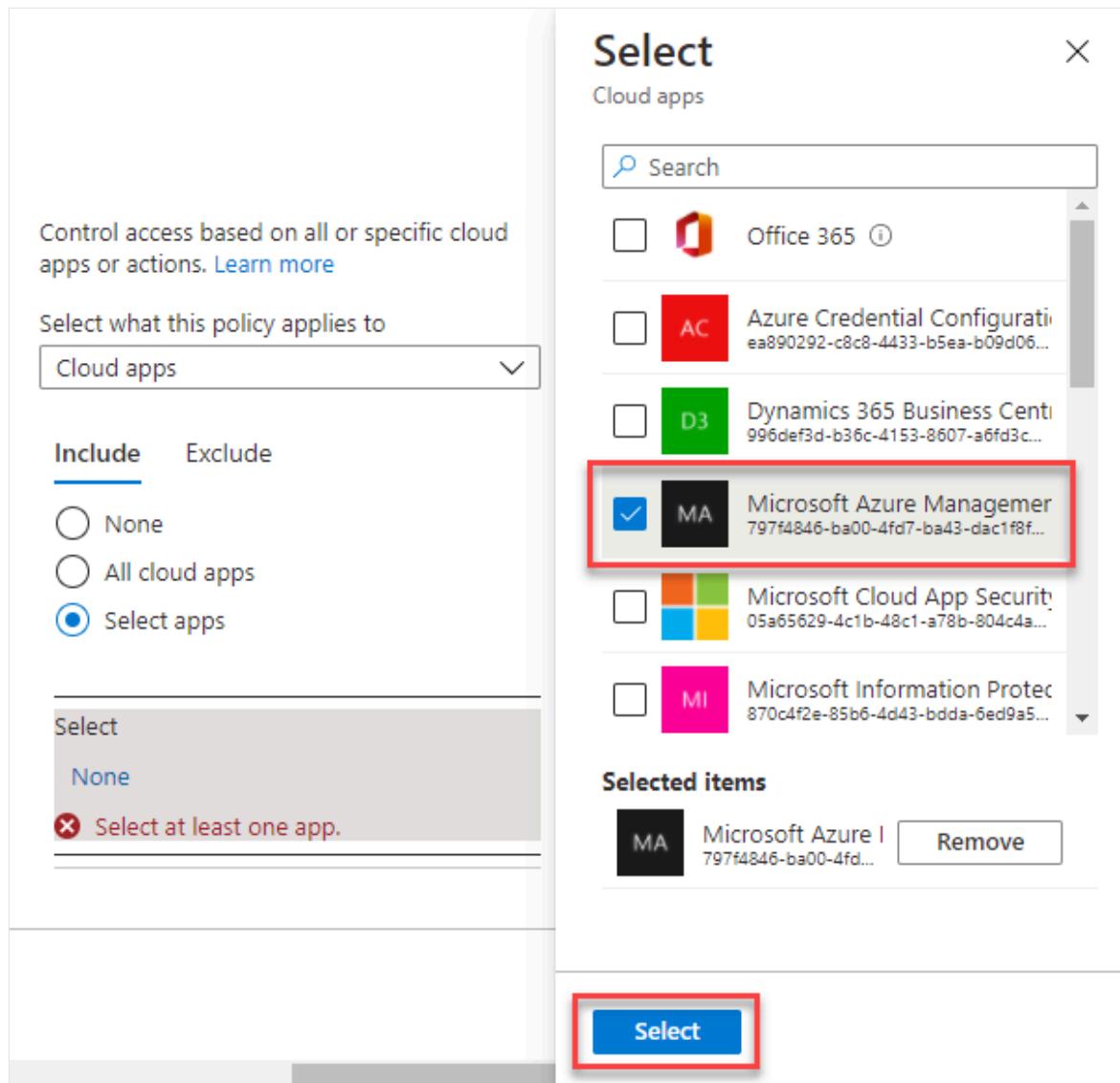
2. Under **Include**, choose **Select resources**.

Since no apps are yet selected, the list of apps (shown in the next step) opens automatically.

 **Tip**

You can choose to apply the Conditional Access policy to **All resources** (formerly 'All cloud apps') or **Select resources**. To provide flexibility, you can also exclude certain apps from the policy.

3. Browse the list of available sign-in events that can be used. For this tutorial, select **Windows Azure Service Management API** so that the policy applies to sign-in events. Then choose **Select**.



The screenshot shows the 'Select' dialog box for choosing cloud apps. On the left, there's a summary section with a link to learn more about controlling access based on all or specific cloud apps. Below it is a dropdown for 'Select what this policy applies to' set to 'Cloud apps'. Under 'Include', the 'Select apps' radio button is selected. A note at the bottom says 'Select at least one app.' On the right, a list of apps is shown with checkboxes. One checkbox for 'Microsoft Azure Manager' is checked and highlighted with a red box. At the bottom right of the list is a 'Selected items' section with a single item: 'Microsoft Azure I' with a 'Remove' button. At the very bottom right of the entire dialog is a large blue 'Select' button, also highlighted with a red box.

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select

None

Select at least one app.

Cloud apps

Office 365 ⓘ

AC Azure Credential Configuration
ea890292-c8c8-4433-b5ea-b09d06...

D3 Dynamics 365 Business Central
996def3d-b36c-4153-8607-a6fd3c...

MA Microsoft Azure Manager
797f4846-ba00-4fd7-ba43-dac1f8f...

Microsoft Cloud App Security
05a65629-4c1b-48c1-a78b-804c4a...

MI Microsoft Information Protection
870c4f2e-85b6-4d43-bdd4-6ed9a5...

Selected items

MA Microsoft Azure I
797f4846-ba00-4fd...

Remove

Select

Configure multifactor authentication for access

Next, we configure access controls. Access controls let you define the requirements for a user to be granted access. They might be required to use an approved client app or a device that's hybrid-joined to Microsoft Entra ID.

In this tutorial, configure the access controls to require multifactor authentication during a sign-in event.

1. Under **Access controls**, select the current value under **Grant**, and then select **Grant access**.

The screenshot shows the Microsoft Conditional Access Overview page with a 'New' policy named 'MFA Pilot'. The 'Access controls' section is expanded, showing the 'Grant' tab selected. The 'Grant' tab has a red box around it. Inside the tab, the 'Grant access' radio button is selected, also with a red box around it. Below it, other options like 'Require multifactor authentication' and 'Require password change' are listed with checkboxes. At the bottom of the tab, there are two radio buttons for 'For multiple controls': 'Require all the selected controls' (selected) and 'Require one of the selected controls'. The 'Create' button is at the bottom left, and the 'Select' button is at the bottom right.

2. Select **Require multifactor authentication**, and then choose **Select**.

Grant

X

Control access enforcement to block or grant access. [Learn more](#)

- Block access
- Grant access

- Require multifactor authentication** ⓘ

ⓘ Consider testing the new "Require authentication strength". [Learn more](#)

- Require authentication strength** ⓘ

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

- Require device to be marked as compliant** ⓘ

- Require Microsoft Entra hybrid joined device** ⓘ

- Require approved client app** ⓘ
[See list of approved client apps](#)

- Require app protection policy** ⓘ
[See list of policy protected client apps](#)

- Require password change** ⓘ

For multiple controls

- Require all the selected controls**
- Require one of the selected controls**

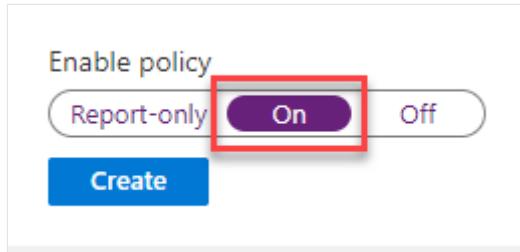
Select

Activate the policy

Conditional Access policies can be set to **Report-only** if you want to see how the configuration would affect users, or **Off** if you don't want to use policy right now.

Because a test group of users is targeted for this tutorial, let's enable the policy, and then test Microsoft Entra multifactor authentication.

1. Under **Enable policy**, select **On**.



2. To apply the Conditional Access policy, select **Create**.

Test Microsoft Entra multifactor authentication

Let's see your Conditional Access policy and Microsoft Entra multifactor authentication in action.

First, sign in to a resource that doesn't require MFA:

1. Open a new browser window in InPrivate or incognito mode and browse to <https://account.activedirectory.windowsazure.com>.

Using a private mode for your browser prevents any existing credentials from affecting this sign-in event.

2. Sign in with your non-administrator test user, such as *testuser*. Be sure to include @ and the domain name for the user account.

If this is the first instance of signing in with this account, you're prompted to change the password. However, there's no prompt for you to configure or use multifactor authentication.

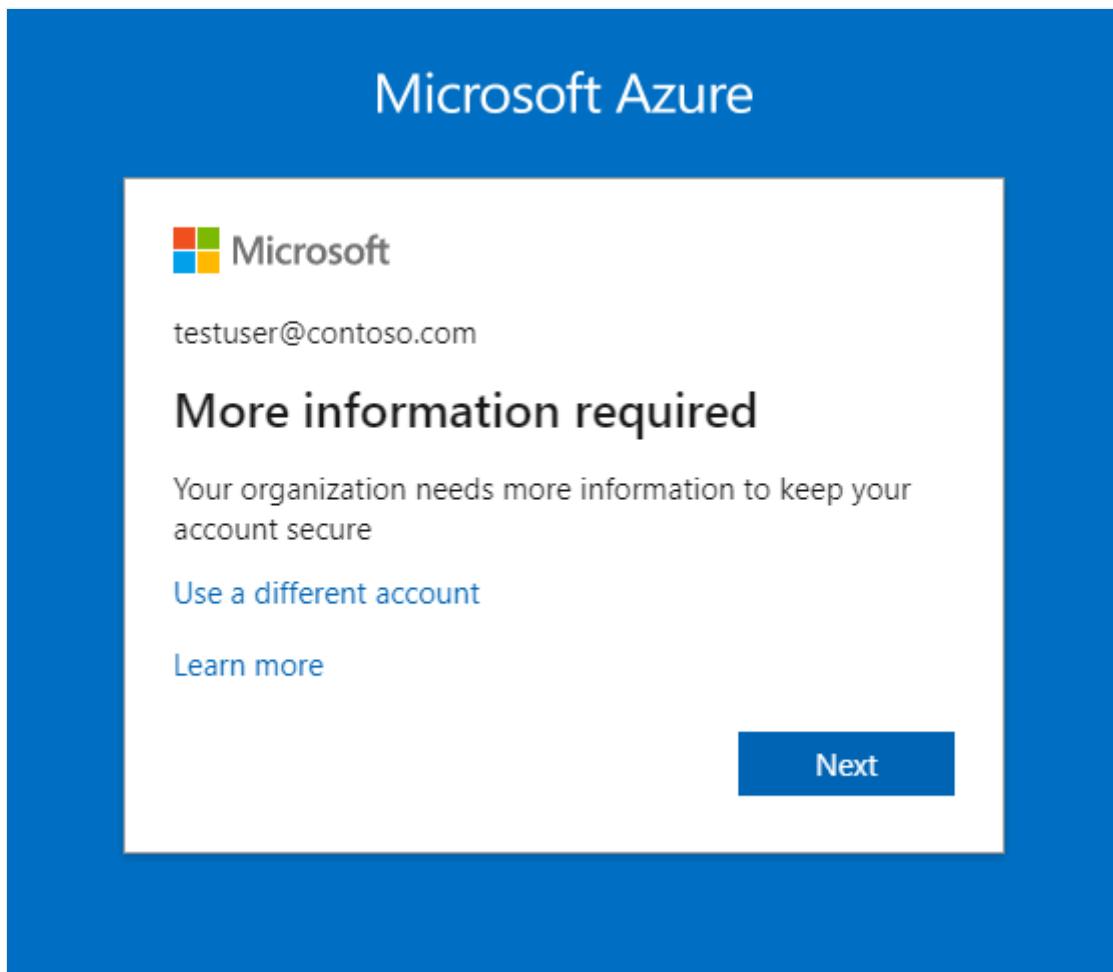
3. Close the browser window.

You configured the Conditional Access policy to require additional authentication for sign in. Because of that configuration, you're prompted to use Microsoft Entra multifactor authentication or to configure a method if you haven't yet done so. Test this new requirement by signing in to the Microsoft Entra admin center:

1. Open a new browser window in InPrivate or incognito mode and sign in to the [Microsoft Entra admin center](#).

2. Sign in with your non-administrator test user, such as *testuser*. Be sure to include @ and the domain name for the user account.

You're required to register for and use Microsoft Entra multifactor authentication.



3. Select **Next** to begin the process.

You can choose to configure an authentication phone, an office phone, or a mobile app for authentication. *Authentication phone* supports text messages and phone calls, *office phone* supports calls to numbers that have an extension, and *mobile app* supports using a mobile app to receive notifications for authentication or to generate authentication codes.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?—

- Receive notifications for verification
- Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

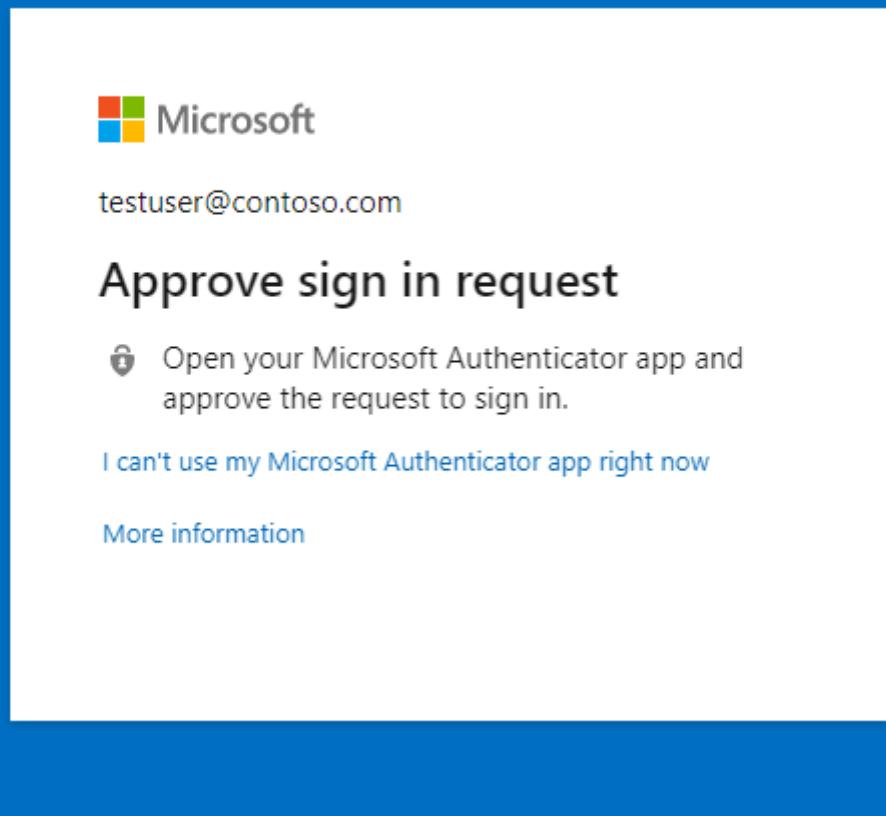
Set up

Please configure the mobile app.

Next

4. Complete the instructions on the screen to configure the method of multifactor authentication that you've selected.
5. Close the browser window, and sign in to the [Microsoft Entra admin center](#) again to test the authentication method that you configured. For example, if you configured a mobile app for authentication, you should see a prompt like the following.

Microsoft Azure



6. Close the browser window.

Clean up resources

If you no longer want to use the Conditional Access policy that you configured as part of this tutorial, delete the policy by using the following steps:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Policies > Conditional Access**, and then select the policy that you created, such as **MFA Pilot**.
3. select **Delete**, and then confirm that you want to delete the policy.

A screenshot of the Microsoft Entra admin center interface. The navigation path is Home > Contoso > Security > Conditional Access. Below this, a policy named "MFA Pilot" is listed as a "Conditional Access policy". A red box highlights the "Delete" button, which is located at the bottom left of the policy card.

Next steps

In this tutorial, you enabled Microsoft Entra multifactor authentication by using Conditional Access policies for a selected group of users. You learned how to:

- ✓ Create a Conditional Access policy to enable Microsoft Entra multifactor authentication for a group of Microsoft Entra users.
- ✓ Configure the policy conditions that prompt for multifactor authentication.
- ✓ Test configuring and using multifactor authentication as a user.

[Enable password writeback for self-service password reset \(SSPR\)](#)

Feedback

Was this page helpful?

 Yes

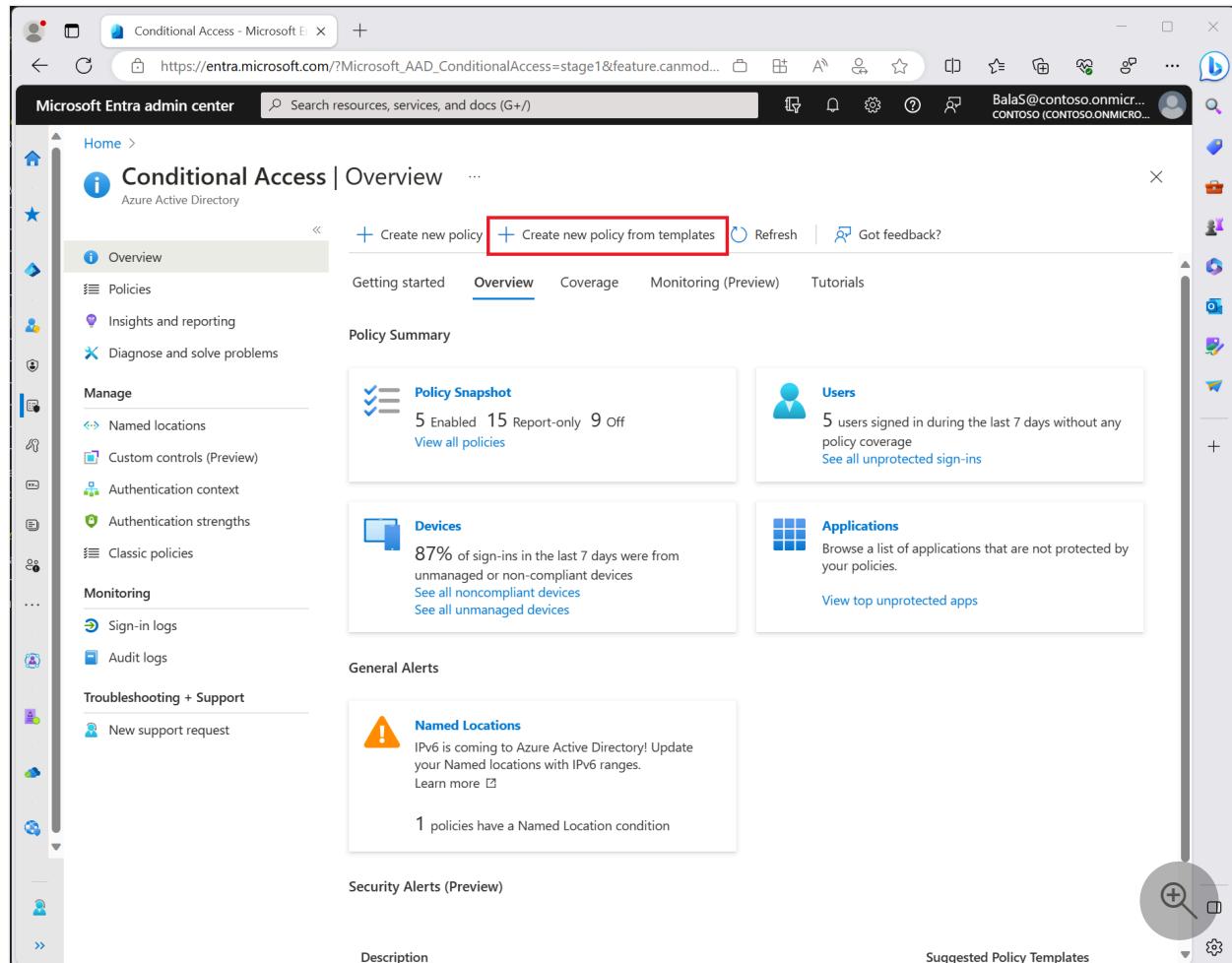
 No

[Provide product feedback ↗](#)

Conditional Access policy templates

Article • 10/22/2024

Conditional Access templates provide a convenient method to deploy new policies aligned with Microsoft recommendations. These templates are designed to provide maximum protection aligned with commonly used policies across various customer types and locations.



The screenshot shows the Conditional Access Overview page in the Microsoft Entra admin center. The top navigation bar includes the Microsoft Entra admin center logo, a search bar, and a user profile for 'BalaS@contoso.onmicrosoft.com'. The main content area has a title 'Conditional Access | Overview' and a sub-section 'Azure Active Directory'. On the left, there's a sidebar with links like 'Overview', 'Policies', 'Insights and reporting', 'Diagnose and solve problems', 'Manage' (with 'Named locations', 'Custom controls (Preview)', 'Authentication context', 'Authentication strengths', 'Classic policies'), 'Monitoring' (with 'Sign-in logs', 'Audit logs'), and 'Troubleshooting + Support' (with 'New support request'). The main content area features several cards: 'Policy Snapshot' (5 Enabled, 15 Report-only, 9 Off), 'Users' (5 users signed in during the last 7 days without any policy coverage, with a link to 'See all unprotected sign-ins'), 'Devices' (87% of sign-ins in the last 7 days were from unmanaged or non-compliant devices, with links to 'See all noncompliant devices' and 'See all unmanaged devices'), and 'Applications' (Browse a list of applications that are not protected by your policies, with a link to 'View top unprotected apps'). Below these are 'General Alerts' (with a 'Named Locations' warning about IPv6 coming to Azure Active Directory) and 'Security Alerts (Preview)'. At the bottom right is a 'Suggested Policy Templates' section with a magnifying glass icon. The 'Create new policy from templates' button in the top navigation bar is highlighted with a red box.

Template categories

Conditional Access policy templates are organized into the following categories:

Secure foundation

Microsoft recommends these policies as the base for all organizations. We recommend these policies be deployed as a group.

- [Require multifactor authentication for admins](#)
- [Securing security info registration](#)
- [Block legacy authentication](#)

- Require multifactor authentication for admins accessing Microsoft admin portals
- Require multifactor authentication for all users
- Require multifactor authentication for Azure management
- Require compliant or Microsoft Entra hybrid joined device or multifactor authentication for all users
- Require compliant device

Find these templates in the [Microsoft Entra admin center](#) > **Protection** > **Conditional Access** > **Create new policy from templates**. Select **Show more** to see all policy templates in each category.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Create new policy from template' and the URL 'https://entra.microsoft.com/?Microsoft_AAD_ConditionalAccess=stage1&feature.canmodifystamps=true&if...'. The main title is 'Create new policy from templates'. Below it, there's a 'Select a template' section with a search bar and tabs: 'Secure foundation' (selected), 'Zero Trust', 'Remote work', 'Protect administrator', and 'Emerging threats'. A red box highlights the 'Show more' button at the bottom left of the template list. The list contains six items:

- Require multifactor authentication for admins**
Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
[Learn more](#)
- Securing security info registration**
Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
[Learn more](#)
- Block legacy authentication**
Block legacy authentication endpoints that can be used to bypass multifactor authentication.
[Learn more](#)
- Require multifactor authentication for all users**
Require multifactor authentication for all user accounts to reduce risk of compromise.
[Learn more](#)
- Require multifactor authentication for guest access**
Require guest users perform multifactor authentication when accessing your company resources.
[Learn more](#)
- Require multifactor authentication for Azure management**
Require multifactor authentication to protect privileged access to Azure management.
[Learn more](#)

At the bottom, there are buttons for 'Review + create', '< Previous', 'Next: Review + Create >', and a circular icon with a plus sign and a magnifying glass.

ⓘ Important

Conditional Access template policies will exclude only the user creating the policy from the template. If your organization needs to exclude other accounts, you will be able to modify the policy once they are created. You can find these policies in the [Microsoft Entra admin center](#) > **Protection** > **Conditional Access** > **Policies**. Select a policy to open the editor and modify the excluded users and groups to select accounts you want to exclude.

By default, each policy is created in [report-only mode](#), we recommend organizations test and monitor usage, to ensure intended result, before turning on each policy.

Organizations can select individual policy templates and:

- View a summary of the policy settings.
- Edit, to customize based on organizational needs.
- Export the JSON definition for use in programmatic workflows.
 - These JSON definitions can be edited and then imported on the main Conditional Access policies page using the [Upload policy file](#) option.

Other common policies

- [Require multifactor authentication for device registration](#)
- [Block access by location](#)
- [Block access except specific apps](#)

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or break-glass accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Next steps

- [Simulate sign in behavior using the Conditional Access What If tool.](#)

- Use report-only mode for Conditional Access to determine the results of new policy decisions.
-

Feedback

Was this page helpful?

 Yes

 No

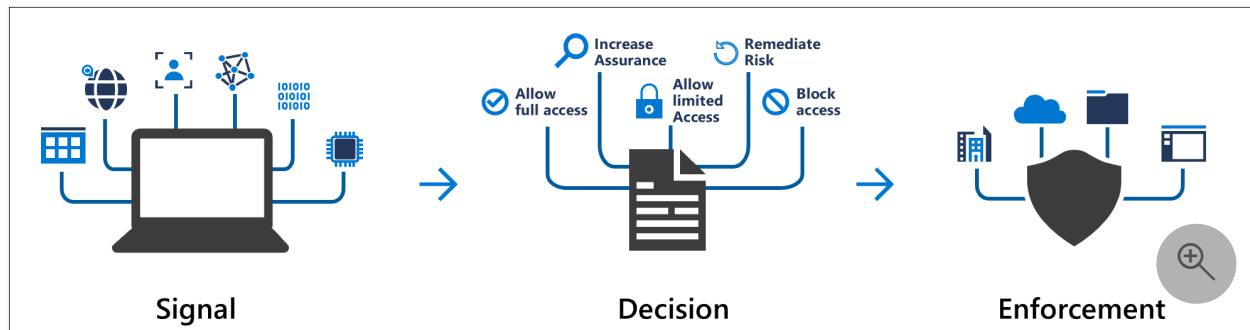
Provide product feedback ↗

Building a Conditional Access policy

Article • 05/06/2024

As explained in the article [What is Conditional Access](#), a Conditional Access policy is an if-then statement, of **Assignments** and **Access controls**. A Conditional Access policy brings signals together, to make decisions, and enforce organizational policies.

How does an organization create these policies? What is required? How are they applied?



Multiple Conditional Access policies might apply to an individual user at any time. In this case, all policies that apply must be satisfied. For example, if one policy requires multifactor authentication and another requires a compliant device, you must complete MFA, and use a compliant device. All assignments are logically **ANDed**. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

If a policy where "Require one of the selected controls" is selected, we prompt in the order defined, as soon as the policy requirements are satisfied, access is granted.

All policies are enforced in two phases:

- **Phase 1:** Collect session details
 - Gather session details, like network location and device identity necessary for policy evaluation.
 - Phase 1 of policy evaluation occurs for enabled policies and policies in [report-only mode](#).
- **Phase 2:** Enforcement
 - Use the session details gathered in phase 1 to identify any requirements that aren't met.
 - If there's a policy that is configured with the **block** grant control, enforcement stops here and the user is blocked.
 - The user is prompted to complete more grant control requirements that weren't satisfied during phase 1 in the following order, until policy is satisfied:

1. Multifactor authentication
 2. Device to be marked as compliant
 3. Microsoft Entra hybrid joined device
 4. Approved client app
 5. App protection policy
 6. Password change
 7. Terms of use
 8. Custom controls
- Once all grant controls are satisfied, apply session controls (App Enforced, Microsoft Defender for Cloud Apps, and token Lifetime)
 - Phase 2 of policy evaluation occurs for all enabled policies.

Assignments

The assignments portion controls the who, what, and where of the Conditional Access policy.

Users and groups

[Users and groups](#) assign who the policy include or exclude when applied. This assignment can include all users, specific groups of users, directory roles, or external guest users.

Target resources

[Target resources](#) can include or exclude cloud applications, user actions, or authentication contexts that are subjected to the policy.

Network

[Network](#) contains IP addresses, geographies, and [Global Secure Access' compliant network](#) to Conditional Access policy decisions. Administrators can choose to define locations and mark some as trusted like those for their organization's primary network locations.

Conditions

A policy can contain multiple [conditions](#).

Sign-in risk

For organizations with [Microsoft Entra ID Protection](#), the risk detections generated there can influence your Conditional Access policies.

Device platforms

Organizations with multiple device operating system platforms might enforce specific policies on different platforms.

The information used to calculate the device platform comes from unverified sources such as user agent strings that can be changed.

Client apps

The software the user is employing to access the cloud app. For example, 'Browser' and 'Mobile apps and desktop clients'. By default, all newly created Conditional Access policies apply to all client app types even if the client apps condition isn't configured.

Filter for devices

This control allows targeting specific devices based on their attributes in a policy.

Access controls

The access controls portion of the Conditional Access policy controls how a policy is enforced.

Grant

[Grant](#) provides administrators with a means of policy enforcement where they can block or grant access.

Block access

Block access does just that, it blocks access under the specified assignments. The block control is powerful and should be wielded with the appropriate knowledge.

Grant access

The grant control can trigger enforcement of one or more controls.

- Require multifactor authentication
- Require device to be marked as compliant (Intune)
- Require Microsoft Entra hybrid joined device
- Require approved client app
- Require app protection policy
- Require password change
- Require terms of use

Administrators can choose to require one of the previous controls or all selected controls using the following options. The default for multiple controls is to require all.

- Require all the selected controls (control and control)
- Require one of the selected controls (control or control)

Session

[Session controls](#) can limit the experience of users.

- Use app enforced restrictions:
 - Currently works with Exchange Online and SharePoint Online only.
 - Passes device information to allow control of experience granting full or limited access.
- Use Conditional Access App Control:
 - Uses signals from Microsoft Defender for Cloud Apps to do things like:
 - Block download, cut, copy, and print of sensitive documents.
 - Monitor risky session behavior.
 - Require labeling of sensitive files.
- Sign-in frequency:
 - Ability to change the default sign in frequency for modern authentication.
- Persistent browser session:
 - Allows users to remain signed in after closing and reopening their browser window.
- Customize continuous access evaluation
- Disable resilience defaults

Simple policies

A Conditional Access policy must contain at minimum the following to be enforced:

- **Name** of the policy.

- **Assignments**
 - **Users and/or groups** to apply the policy to.
 - **Cloud apps or actions** to apply the policy to.
- **Access controls**
 - **Grant or Block** controls

New □ X

Info

*** Name**
Example: 'Device compliance app policy'

Assignments

Users and groups >
0 users and groups selected

Cloud apps or actions >
No cloud apps or actions sele...

Conditions >
0 conditions selected

Access controls

Grant >
0 controls selected

Session >
0 controls selected

Enable policy

On Off

Create

The article [Common Conditional Access policies](#) includes some policies that we think would be useful to most organizations.

Related content

- [Create a Conditional Access policy](#)

- Managing device compliance with Intune
- Microsoft Defender for Cloud Apps and Conditional Access

Conditional Access: Users, groups, and workload identities

Article • 05/21/2024

A Conditional Access policy must include a user, group, or workload identity assignment as one of the signals in the decision process. These identities can be included or excluded from Conditional Access policies. Microsoft Entra ID evaluates all policies and ensures that all requirements are met before granting access.

<https://www.youtube-nocookie.com/embed/5DsW1hB3Jqs>

Include users

This list of users typically includes all of the users an organization is targeting in a Conditional Access policy.

The following options are available to include when creating a Conditional Access policy.

- None
 - No users selected
- All users
 - All users that exist in the directory including B2B guests.
- Select users and groups
 - Guest or external users
 - This selection provides several choices that can be used to target Conditional Access policies to specific guest or external user types and specific tenants containing those types of users. There are [several different types of guest or external users that can be selected](#), and multiple selections can be made:
 - B2B collaboration guest users
 - B2B collaboration member users
 - B2B direct connect users
 - Local guest users, for example any user belonging to the home tenant with the user type attribute set to guest
 - Service provider users, for example a Cloud Solution Provider (CSP)
 - Other external users, or users not represented by the other user type selections
 - One or more tenants can be specified for the selected user types, or you can specify all tenants.
 - Directory roles

- Allows administrators to select specific [built-in directory roles](#) used to determine policy assignment. For example, organizations might create a more restrictive policy on users actively assigned a privileged role. Other role types aren't supported, including administrative unit-scoped roles and custom roles.
- Conditional Access allows administrators to select some [roles that are listed as deprecated](#). These roles still appear in the underlying API and we allow administrators to apply policy to them.
- Users and groups
 - Allows targeting of specific sets of users. For example, organizations can select a group that contains all members of the HR department when an HR app is selected as the cloud app. A group can be any type of user group in Microsoft Entra ID, including dynamic or assigned security and distribution groups. Policy is applied to nested users and groups.

Important

When selecting which users and groups are included in a Conditional Access Policy, there is a limit to the number of individual users that can be added directly to a Conditional Access policy. If there are a large amount of individual users that are needed to be added directly to a Conditional Access policy, we recommend placing the users in a group, and assigning the group to the Conditional Access policy instead.

If users or groups are a member of over 2048 groups their access may be blocked. This limit applies to both direct and nested group membership.

Warning

Conditional Access policies do not support users assigned a directory role [scoped to an administrative unit](#) or directory roles scoped directly to an object, like through [custom roles](#).

Note

When targeting policies to B2B direct connect external users, these policies will also be applied to B2B collaboration users accessing Teams or SharePoint Online who are also eligible for B2B direct connect. The same applies for policies targeted to B2B collaboration external users, meaning users accessing Teams shared channels

will have B2B collaboration policies apply if they also have a guest user presence in the tenant.

Exclude users

When organizations both include and exclude a user or group, the user or group is excluded from the policy. The exclude action overrides the include action in policy. Exclusions are commonly used for emergency access or break-glass accounts. More information about emergency access accounts and why they're important can be found in the following articles:

- [Manage emergency access accounts in Microsoft Entra ID](#)
- [Create a resilient access control management strategy with Microsoft Entra ID](#)

The following options are available to exclude when creating a Conditional Access policy.

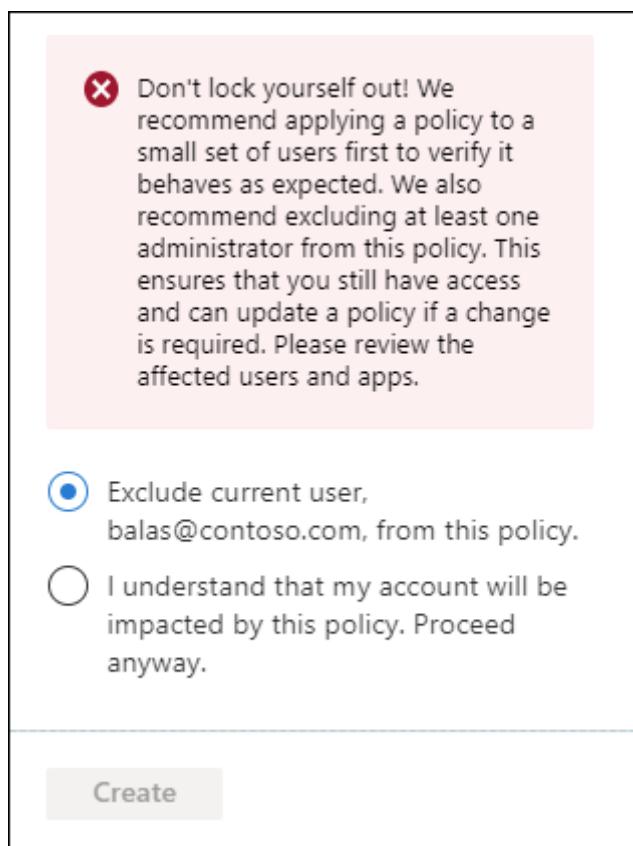
- Guest or external users
 - This selection provides several choices that can be used to target Conditional Access policies to specific guest or external user types and specific tenants containing those types of users. There are [several different types of guest or external users that can be selected](#), and multiple selections can be made:
 - B2B collaboration guest users
 - B2B collaboration member users
 - B2B direct connect users
 - Local guest users, for example any user belonging to the home tenant with the user type attribute set to guest
 - Service provider users, for example a Cloud Solution Provider (CSP)
 - Other external users, or users not represented by the other user type selections
 - One or more tenants can be specified for the selected user types, or you can specify all tenants.
- Directory roles
 - Allows administrators to select specific [Microsoft Entra directory roles](#) used to determine assignment.
- Users and groups
 - Allows targeting of specific sets of users. For example, organizations can select a group that contains all members of the HR department when an HR app is selected as the cloud app. A group can be any type of group in Microsoft Entra ID, including dynamic or assigned security and distribution groups. Policy is applied to nested users and groups.

Preventing administrator lockout

To prevent administrator lockout, when creating a policy applied to **All users** and **All apps**, the following warning appears.

Don't lock yourself out! We recommend applying a policy to a small set of users first to verify it behaves as expected. We also recommend excluding at least one administrator from this policy. This ensures that you still have access and can update a policy if a change is required. Please review the affected users and apps.

By default the policy provides an option to exclude the current user from the policy, but an administrator can override as shown in the following image.



If you do find yourself locked out, see [What to do if you're locked out?](#)

External partner access

Conditional Access policies that target external users might interfere with service provider access, for example granular delegated admin privileges [Introduction to granular delegated admin privileges \(GDAP\)](#). For policies that are intended to target service provider tenants, use the **Service provider user** external user type available in the **Guest or external users** selection options.

Workload identities

A workload identity is an identity that allows an application or service principal access to resources, sometimes in the context of a user. Conditional Access policies can be applied to single tenant service principals registered in your tenant. Third party SaaS and multi-tenanted apps are out of scope. Managed identities aren't covered by policy.

Organizations can target specific workload identities to be included or excluded from policy.

For more information, see the article [Conditional Access for workload identities](#).

Next steps

- [Conditional Access: Cloud apps or actions](#)
- [Conditional Access common policies](#)

Conditional Access: Target resources

Article • 02/04/2025

Target resources (formerly Cloud apps, actions, and authentication context) are key signals in a Conditional Access policy. Conditional Access policies allow administrators to assign controls to specific applications, services, actions, or authentication context.

- Administrators can choose from the list of applications or services that include built-in Microsoft applications and any [Microsoft Entra integrated applications](#) including gallery, non-gallery, and applications published through [Application Proxy](#).
- Administrators might choose to define policy not based on a cloud application but on a [user action](#) like **Register security information** or **Register or join devices**, allowing Conditional Access to enforce controls around those actions.
- Administrators can target [traffic forwarding profiles](#) from Global Secure Access for enhanced functionality.
- Administrators can use [authentication context](#) to provide an extra layer of security in applications.

The screenshot shows the Microsoft Entra admin center Conditional Access Overview page. On the left, a sidebar lists various administrative tasks like User management, Group management, and Identity protection. The main area is titled 'New' and 'Conditional Access policy'. It includes sections for 'Assignments' (0 users or workload identities selected), 'Target resources' (No target resources selected), 'Network' (Not configured), 'Conditions' (0 conditions selected), 'Access controls' (Grant 0 controls selected), and 'Session' (0 controls selected). A note indicates that to create a Conditional Access policy targeting members with Global Secure Access (GSA), GSA must be deployed in the tenant. At the bottom, there's an 'Enable policy' section with a 'Report-only' button, an 'On' switch, an 'Off' switch, and a 'Create' button.

Microsoft cloud applications

Many of the existing Microsoft cloud applications are included in the list of applications you can select from.

Administrators can assign a Conditional Access policy to these Microsoft cloud applications. Some apps like [Office 365](#) and [Windows Azure Service Management API](#) include multiple related child apps or services.

ⓘ Important

Applications that are available to Conditional Access go through an onboarding and validation process. These applications don't include all Microsoft apps. Many applications are backend services that aren't meant to have policy directly applied to them. If you're looking for an application that is missing, you can contact the specific application team or make a request on [UserVoice](#).

Office 365

Microsoft 365 provides cloud-based productivity and collaboration services like Exchange, SharePoint, and Microsoft Teams. Microsoft 365 cloud services are deeply integrated to ensure smooth and collaborative experiences. This integration can cause confusion when creating policies as some apps such as Microsoft Teams have dependencies on others such as SharePoint or Exchange.

The Office 365 suite makes it possible to target these services all at once. We recommend using the new Office 365 suite, instead of targeting individual cloud apps to avoid issues with [service dependencies](#).

Targeting this group of applications helps to avoid issues that might arise because of inconsistent policies and dependencies. For example: The Exchange Online app is tied to traditional Exchange Online data like mail, calendar, and contact information. Related metadata might be exposed through different resources like search. To ensure that all metadata is protected by as intended, administrators should assign policies to the Office 365 app.

Administrators can exclude the entire Office 365 suite or specific Office 365 cloud apps from the Conditional Access policy.

A complete list of all services included can be found in the article [Apps included in Conditional Access Office 365 app suite](#).

Windows Azure Service Management API

When you target the Windows Azure Service Management API application, policy is enforced for tokens issued to a set of services closely bound to the portal. This grouping includes the application IDs of:

- Azure Resource Manager
- Azure portal, which also covers the Microsoft Entra admin center
- Azure Data Lake
- Application Insights API
- Log Analytics API

Because the policy is applied to the Azure management portal and API services, or clients with an Azure API service dependency, can indirectly be impacted. For example:

- Azure CLI
- Azure Data Factory portal
- Azure DevOps
- Azure Event Hubs
- Azure PowerShell
- Azure Service Bus
- Azure SQL Database
- Azure Synapse
- Classic deployment model APIs
- Microsoft 365 admin center
- Microsoft IoT Central
- SQL Managed Instance
- Visual Studio subscriptions administrator portal

 **Note**

The Windows Azure Service Management API application applies to [Azure PowerShell](#), which calls the [Azure Resource Manager API](#). It doesn't apply to [Microsoft Graph PowerShell](#), which calls the [Microsoft Graph API](#).

For more information on how to set up a sample policy for Windows Azure Service Management API, see [Conditional Access: Require MFA for Azure management](#).

 **Tip**

For Azure Government, you should target the Azure Government Cloud Management API application.

Microsoft Admin Portals

When a Conditional Access policy targets the Microsoft Admin Portals cloud app, the policy is enforced for tokens issued to application IDs of the following Microsoft administrative portals:

- Azure portal
- Exchange admin center
- Microsoft 365 admin center

- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Intune admin center
- Microsoft Purview compliance portal
- Microsoft Teams admin center

We're continually adding more administrative portals to the list.

 **Note**

The Microsoft Admin Portals app applies to interactive sign-ins to the listed admin portals only. Sign-ins to the underlying resources or services like Microsoft Graph or Azure Resource Manager APIs aren't covered by this application. Those resources are protected by the [Windows Azure Service Management API](#) app. This grouping enables customers to move along the MFA adoption journey for admins without impacting automation that relies on APIs and PowerShell. When you're ready, Microsoft recommends using a [policy requiring administrators perform MFA always](#) for comprehensive protection.

Other applications

Administrators can add any Microsoft Entra registered application to Conditional Access policies. These applications might include:

- Applications published through [Microsoft Entra application proxy](#)
- [Applications added from the gallery](#)
- [Custom applications not in the gallery](#)
- [Legacy applications published through app delivery controllers and networks](#)
- Applications that use [password based single sign-on](#)

 **Note**

Since Conditional Access policy sets the requirements for accessing a service, you aren't able to apply it to a client (public/native) application. In other words, the policy isn't set directly on a client (public/native) application, but is applied when a client calls a service. For example, a policy set on SharePoint service applies to all clients calling SharePoint. A policy set on Exchange applies to the attempt to access the email using Outlook client. That is why client (public/native) applications aren't available for selection in the app picker and Conditional Access option isn't

available in the application settings for the client (public/native) application registered in your tenant.

Some applications don't appear in the picker at all. The only way to include these applications in a Conditional Access policy is to include **All resources** (formerly 'All cloud apps').

Understanding Conditional Access for different client types

Conditional Access applies to resources not clients, except when the client is a confidential client requesting an ID token.

- Public client
 - Public clients are those that run locally on devices like Microsoft Outlook on the desktop or mobile apps like Microsoft Teams.
 - Conditional Access policies don't apply to the public client itself, but apply based on the resources requested by the public clients.
- Confidential client
 - Conditional Access applies to the resources requested by the client and the confidential client itself if it requests an ID token.
 - For example: If Outlook Web requests a token for scopes `Mail.Read` and `Files.Read`, Conditional Access applies policies for Exchange and SharePoint. Additionally, if Outlook Web requests an ID token, Conditional Access also applies the policies for Outlook Web.

To view [sign-in logs](#) for these client types from the Microsoft Entra admin center:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Add a filter for **Client credential type**.
4. Adjust the filter to view a specific set of logs based on the client credential used in the sign-in.

For more information see the article [Public client and confidential client applications](#).

All resources

Applying a Conditional Access policy to **All resources** (formerly 'All cloud apps') without any app exclusions results in the policy being enforced for all token requests from web sites and services including [Global Secure Access traffic forwarding profiles](#). This option includes applications that aren't individually targetable in Conditional Access

policy, such as `Windows Azure Active Directory` (00000002-0000-0000-c000-000000000000).

Important

Microsoft recommends creating a baseline multifactor authentication policy targeting all users and all resources (without any app exclusions), like the one explained in [Require multifactor authentication for all users](#).

Conditional Access behavior when an all resources policy has an app exclusion

If any app is excluded from the policy, in order to not inadvertently block user access, certain low privilege scopes are excluded from policy enforcement. These scopes allow calls to the underlying Graph APIs, like `Windows Azure Active Directory` (00000002-0000-0000-c000-000000000000) and `Microsoft Graph` (00000003-0000-0000-c000-000000000000), to access user profile and group membership information commonly used by applications as part of authentication. For example: when Outlook requests a token for Exchange, it also asks for the `User.Read` scope to be able to display the basic account information of the current user.

Most apps have a similar dependency, which is why these low privilege scopes are automatically excluded whenever there's an app exclusion in an **All resources** policy. These low privilege scope exclusions don't allow data access beyond basic user profile and group information. The excluded scopes are listed as follows, consent is still required for apps to use these permissions.

- Native clients and Single page applications (SPAs) have access to the following low privilege scopes:
 - Azure AD Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`
 - Microsoft Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`,
`People.Read`
- Confidential clients have access to the following low privilege scopes, if they're excluded from an **All resources** policy:
 - Azure AD Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`,
`User.Read.All`, `User.ReadBasic.All`
 - Microsoft Graph: `email`, `offline_access`, `openid`, `profile`, `User.Read`,
`User.Read.All`, `User.ReadBasic.All`, `People.Read`, `People.Read.All`,
`GroupMember.Read.All`, `Member.Read.Hidden`

For more information on the scopes mentioned, see [Microsoft Graph permissions reference](#) and [Scopes and permissions in the Microsoft identity platform](#).

Protecting directory information

If the [recommended baseline MFA policy without app exclusions](#) can't be configured due to business reasons, and your organization's security policy must include these low privilege scopes, the alternative is to create a separate Conditional Access policy targeting `Windows Azure Active Directory` (00000002-0000-0000-c000-000000000000). Windows Azure Active Directory (also called Azure AD Graph) is a resource representing data stored in the directory such as users, groups, and applications. The Windows Azure Active Directory resource is included in **All resources** but can be individually targeted in Conditional Access policies by using the following steps:

1. Sign in to the [Microsoft Entra admin center](#) as an [Attribute Definition Administrator](#) and [Attribute Assignment Administrator](#).
2. Browse to **Protection > Custom security attributes**.
3. Create a new attribute set and attribute definition. For more information, see [Add or deactivate custom security attribute definitions in Microsoft Entra ID](#).
4. Browse to **Identity > Applications > Enterprise applications**.
5. Remove the **Application type** filter and search for **Application ID** that starts with 00000002-0000-0000-c000-000000000000.
6. Select **Windows Azure Active Directory > Custom security attributes > Add assignment**.
7. Select the attribute set and attribute value that you plan to use in the policy.
8. Browse to **Protection > Conditional Access > Policies**.
9. Create or modify an existing policy.
10. Under **Target resources > Resources (formerly cloud apps) > Include**, select > **Select resources > Edit filter**.
11. Adjust the filter to include your attribute set and definition from earlier.
12. Save the policy

All internet resources with Global Secure Access

The **All internet resources with Global Secure Access** option allows administrators to target the [internet access traffic forwarding profile](#) from [Microsoft Entra Internet Access](#).

These profiles in Global Secure Access enable administrators to define and control how traffic is routed through Microsoft Entra Internet Access and Microsoft Entra Private Access. Traffic forwarding profiles can be assigned to devices and remote networks. For

an example of how to apply a Conditional Access policy to these traffic profiles, see the article [How to apply Conditional Access policies to the Microsoft 365 traffic profile](#).

For more information about these profiles, see the article [Global Secure Access traffic forwarding profiles](#).

User actions

User actions are tasks that a user performs. Currently, Conditional Access supports two user actions:

- **Register security information:** This user action allows Conditional Access policy to enforce when users who are enabled for combined registration attempt to register their security information. More information can be found in the article, [Combined security information registration](#).

Note

When administrators apply a policy targeting user actions for register security information, if the user account is a guest from [Microsoft personal account \(MSA\)](#), using the control 'Require multifactor authentication', will require the MSA user to register security information with the organization. If the guest user is from another provider such as [Google](#), access is blocked.

- **Register or join devices:** This user action enables administrators to enforce Conditional Access policy when users [register](#) or [join](#) devices to Microsoft Entra ID. It provides granularity in configuring multifactor authentication for registering or joining devices instead of a tenant-wide policy that currently exists. There are three key considerations with this user action:
 - [Require multifactor authentication](#) is the only access control available with this user action and all others are disabled. This restriction prevents conflicts with access controls that are either dependent on Microsoft Entra device registration or not applicable to Microsoft Entra device registration.
 - [Client apps](#), [Filters for devices](#), and [Device state](#) conditions aren't available with this user action since they're dependent on Microsoft Entra device registration to enforce Conditional Access policies.

Warning

When a Conditional Access policy is configured with the **Register or join devices** user action, you must set **Identity > Devices > Overview > Device Settings** -

Require Multifactor Authentication to register or join devices with Microsoft Entra to No. Otherwise, Conditional Access policies with this user action aren't properly enforced. More information about this device setting can found in [Configure device settings](#).

Authentication context

Authentication context can be used to further secure data and actions in applications. These applications can be your own custom applications, custom line of business (LOB) applications, applications like SharePoint, or applications protected by Microsoft Defender for Cloud Apps.

For example, an organization might keep files in SharePoint sites like the lunch menu or their secret BBQ sauce recipe. Everyone might have access to the lunch menu site, but users who have access to the secret BBQ sauce recipe site might need to access from a managed device and agree to specific terms of use.

Authentication context works with users or [workload identities](#), but not in the same Conditional Access policy.

Configure authentication contexts

Authentication contexts are managed under **Protection > Conditional Access > Authentication context**.

The screenshot shows the 'Conditional Access | Authentication context' page in the Azure portal. The left sidebar includes links for Policies, Insights and reporting, Diagnose and solve problems, Manage (with Named locations, Custom controls (Preview), Terms of use, VPN connectivity, and Authentication context selected), Classic policies, Troubleshooting + Support (Virtual assistant (Preview)), and New support request. The main content area has a 'Get started' section explaining authentication context's purpose and a 'Configuration steps' table:

Item	Documentation
Configure authentication contexts	Learn more
Assign Conditional Access policies to the authentication context	Learn more
Tag resources with an authentication context	Learn more

A magnifying glass icon is in the bottom right corner of the main content area.

Create new authentication context definitions by selecting **New authentication context**.

Organizations are limited to a total of 99 authentication context definitions **c1-c99**.

Configure the following attributes:

- **Display name** is the name that is used to identify the authentication context in Microsoft Entra ID and across applications that consume authentication contexts. We recommend names that can be used across resources, like *trusted devices*, to reduce the number of authentication contexts needed. Having a reduced set limits the number of redirects and provides a better end to end-user experience.
- **Description** provides more information about the policies, used by administrators and those applying authentication contexts to resources.
- **Publish to apps** checkbox when checked, advertises the authentication context to apps and makes them available to be assigned. If not checked the authentication context is unavailable to downstream resources.
- **ID** is read-only and used in tokens and apps for request-specific authentication context definitions. Listed here for troubleshooting and development use cases.

Add to Conditional Access policy

Administrators can select published authentication contexts in their Conditional Access policies under **Assignments > Cloud apps or actions** and selecting **Authentication context** from the **Select what this policy applies to** menu.

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Authentication context



Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security.

[Learn more](#)

Select the authentication contexts this policy will apply to



Strong Authentication

Delete an authentication context

When you delete an authentication context, make sure no applications are still using it. Otherwise access to app data is no longer protected. You can confirm this prerequisite by checking sign-in logs for cases when the authentication context Conditional Access policies are being applied.

To delete an authentication context, it must have no assigned Conditional Access policies and must not be published to apps. This requirement helps prevent the accidental deletion of an authentication context that is still in use.

Tag resources with authentication contexts

For more information about authentication context use in applications, see the following articles.

- Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites
- Microsoft Defender for Cloud Apps
- Custom applications

Next steps

- Conditional Access: Conditions
 - Conditional Access common policies
 - Client application dependencies
-

Feedback

Was this page helpful?

 Yes

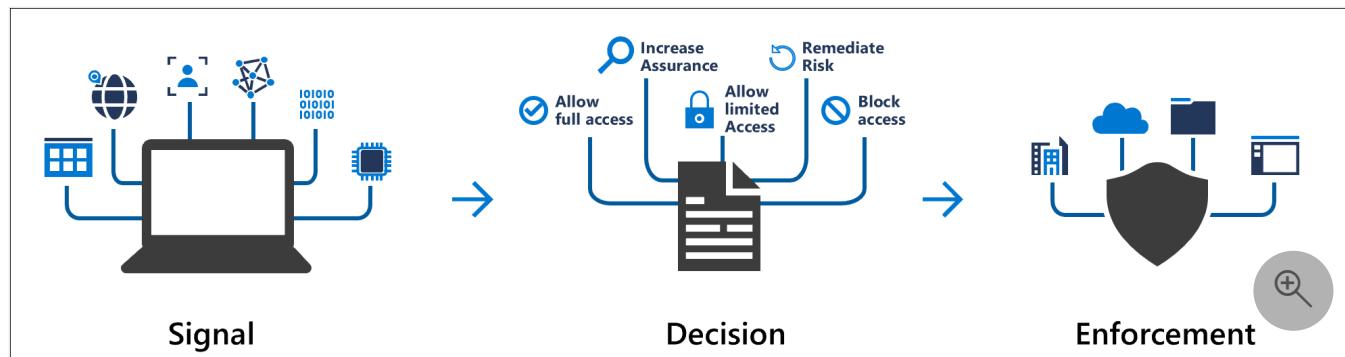
 No

Provide product feedback 

Conditional Access: Network assignment

Article • 04/28/2025

Administrators can create policies that target specific network locations as a signal along with other conditions in their decision making process. They can include or exclude these network locations as part of their policy configuration. These network locations might include public IPv4 or IPv6 network information, countries/regions, unknown areas that don't map to specific countries/regions, or [Global Secure Access' compliant network](#).



! Note

Conditional Access policies are enforced after first-factor authentication completes. Conditional Access isn't intended to be an organization's frontline of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Organizations might use these locations for common tasks such as:

- Requiring multifactor authentication for users accessing a service when they're off the corporate network.
- Blocking access from specific countries your organization never operates from.

A user's location is found using their public IP address or the GPS coordinates provided by the Microsoft Authenticator app. Conditional Access policies apply to all locations by default.

💡 Tip

The **Location** condition moved and was renamed **Network**. Initially, this condition appears at both the **Assignment** level and under **Conditions**.

Updates or changes appear in both locations. The functionality remains the same, and existing policies using **Location** continue to work without changes.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Favorites, Identity, Protection, Identity governance, Verified ID, Permissions Management, Global Secure Access (Preview), and Learn & support. The main area is titled 'Conditional Access | Overview > New > Session Management > Conditional Access | Policies > New'. It's a step-by-step wizard for creating a new policy. The current step is 'Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.' A 'Name' field contains 'Block top secret app outside office'. Below it, under 'Assignments', there's a 'Users' section with 'All users included and specific users excluded' and a 'Target resources' section with '1 app included'. Under 'Conditions', there's one condition selected: 'Network NEW'. A tooltip for this condition states: 'All Compliant Network locations* does not work with "Require app protection policy" or "Require approved client app" grant controls. Learn more'. Below the conditions, there's an 'Access controls' section with 'Grant' set to 'Block access'. Under 'Session', there are '0 controls selected'. At the bottom, there's an 'Enable policy' section with 'Report-only' set to 'On' and a 'Create' button.

When configured in policy

When you configure the location condition, you can distinguish between:

- Any network or location
- All trusted networks and locations
- All Compliant Network locations
- Selected networks and locations

Any network or location

Selecting **Any location** applies a policy to all IP addresses, including any address on the Internet. This setting isn't limited to IP addresses you configure as named locations. When you select **Any location**, you can exclude specific locations from a policy. For example, apply a policy to all locations except trusted locations to set the scope to all locations except the corporate network.

All trusted networks and locations

This option applies to:

- All locations marked as trusted locations.

- Multifactor authentication trusted IPs, if configured.

Multifactor authentication trusted IPs

Using the trusted IPs section of multifactor authentication's service settings isn't recommended. This control accepts only IPv4 addresses and is intended for specific scenarios covered in the article [Configure Microsoft Entra multifactor authentication settings](#).

If you have these trusted IPs configured, they show up as **MFA Trusted IPs** in the list of locations for the location condition.

All Compliant Network locations

Organizations with access to Global Secure Access features see another location listed, consisting of users and devices that comply with your organization's security policies. For more information, see [Enable Global Secure Access signaling for Conditional Access](#). It can be used with Conditional Access policies to perform a compliant network check for access to resources.

Selected networks and locations

With this option, select one or more named locations. For a policy with this setting to apply, a user must connect from any of the selected locations. When you choose **Select**, a list of defined locations opens. This list shows the name, type, and whether the network location is marked as trusted.

How are these locations defined?

Locations exist in the [Microsoft Entra admin center](#) under **Entra ID > Conditional Access > Named locations**. Admins with at least the [Conditional Access Administrator](#) role can create and update named locations.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes sections like Home, Favorites, Identity, Protection, Conditional Access (which is currently selected), Authentication methods, Password reset, Custom security attributes, Risky activities, Show more, Identity governance, Verified ID, Permissions Management, Global Secure Access (Preview), Get started, and Learn & support. The main content area is titled 'Conditional Access | Named locations' and shows a list of named locations. The list includes:

Name	Location type	Trusted	Conditional Access policies
All Compliant Network locations	Network Access	No	Require Compliant Network
Contoso - Blocked Countries List	Countries (IP)		Not configured in any policy yet
Contoso - GPS Blocked Countries	Countries (GPS)		Not configured in any policy yet
Contoso HQ	IP ranges	No	Not configured in any policy yet

There are also buttons for '+ Countries location', '+ IP ranges location', 'Configure multifactor authentication trusted IPs', and a 'Refresh' button.

Named locations might include an organization's headquarters network ranges, VPN network ranges, or ranges you want to block. Named locations contain IPv4 address ranges, IPv6 address ranges, or countries.

IPv4 and IPv6 address ranges

To define a named location by public IPv4 or IPv6 address ranges, provide:

- A **Name** for the location.
- One or more public IP ranges.
- Optionally **Mark as trusted location**.

Named locations defined by IPv4 or IPv6 address ranges have these limitations:

- No more than 195 named locations.
- No more than 2000 IP ranges per named location.
- Only CIDR masks greater than /8 are allowed when defining an IP range.

For devices on a private network, the IP address isn't the client IP of the user's device on the intranet (like 10.55.99.3), it's the address used by the network to connect to the public internet (like 198.51.100.3).

Trusted locations

Administrators can optionally mark IP-based locations, like your organization's public network ranges, as trusted. This marking is used by features in several ways.

- Conditional Access policies can include or exclude these locations.
- Sign-ins from trusted named locations improve the accuracy of Microsoft Entra ID Protection's risk calculation.

Locations marked as trusted can't be deleted without first removing the trusted designation.

Countries

Organizations can determine a geographic country or region location by IP address or GPS coordinates.

To define a named location by country or region, do the following:

- Provide a **Name** for the location.
- Choose to determine location by IP address or GPS coordinates.
- Add one or more countries/regions.
- Optionally choose to **Include unknown countries/regions**.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is visible with sections like Home, Favorites, Identity, Protection, Conditional Access, and others. The main content area is titled 'Conditional Access | Policies > New > Conditional Access' under 'Named locations'. A red box highlights the '+ Countries location' button. To the right, a modal window titled 'New location (Countries)' is open. It contains a note about IPv4 and IPv6 mapping, a 'Name' input field, and a dropdown for 'Country lookup method' with three options: 'Determine location by IP address (IPv4 and IPv6)', 'Determine location by IP address (IPv4 and IPv6)', and 'Determine location by GPS coordinates'. The middle option is also highlighted with a red box. Below these are search and filter fields, and a list of countries with checkboxes. A 'Create' button is at the bottom right of the modal.

When selecting **Determine location by IP address**, Microsoft Entra ID resolves the user's IPv4 or **IPv6** address to a country or region, based on a periodically updated mapping table.

When selecting **Determine location by GPS coordinates**, users must have the Microsoft Authenticator app installed on their mobile device. Every hour, the system contacts the user's Microsoft Authenticator app to collect the GPS location of their mobile device.

- The first time the user must share their location from the Microsoft Authenticator app, they receive a notification in the app. The user must open the app and grant location permissions. For the next 24 hours, if the user is still accessing the resource and granted the app permission to run in the background, the device's location is shared silently once per hour.
- After 24 hours, the user must open the app and approve the notification.
- Every time the user shares their GPS location, the app does jailbreak detection using the same logic as the Microsoft Intune MAM SDK. If the device is jailbroken, the location isn't considered valid, and the user isn't granted access.
 - The Microsoft Authenticator app on Android uses the Google Play Integrity API to facilitate jailbreak detection. If the Google Play Integrity API is unavailable, the request is denied and the user isn't able to access the requested resource unless the Conditional Access policy is disabled. For more information about the Microsoft Authenticator app, see the article [Common questions about the Microsoft Authenticator app](#).
- Users can modify the GPS location as reported by iOS and Android devices. As a result, the Microsoft Authenticator app denies authentications where the user might be using a different location than the actual GPS location of the mobile device where the app is installed. Users who modify the location of their device get a denial message for GPS location-based based policies.
- The country code returned depends on the device platform API: For example one platform might report US for Puerto Rico, while another reports PR.

 **Note**

A Conditional Access policy with GPS-based named locations in report-only mode prompts users to share their GPS location, even though they aren't blocked from signing in.

GPS location can be used with [passwordless phone sign-in](#) only if MFA push notifications are also enabled. Users can use Microsoft Authenticator to sign in, but they also need to approve subsequent MFA push notifications to share their GPS location.

GPS location doesn't work when only [passwordless authentication methods](#) are set.

Multiple Conditional Access policies might prompt users for their GPS location before all are applied. Because of the way Conditional Access policies are applied, a user might be denied

access if they pass the location check but fail another policy. For more information about policy enforcement, see the article [Building a Conditional Access policy](#).

Important

Users might receive prompts every hour letting them know that Microsoft Entra ID is checking their location in the Authenticator app. This feature should only be used to protect very sensitive apps where this behavior is acceptable or where access must be restricted for a specific country/region.

Include unknown countries/regions

Some IP addresses can't be mapped to a specific country or region. To capture these IP locations, check the box **Include unknown countries/regions** when defining a geographic location. This option allows you to choose if these IP addresses should be included in the named location. Use this setting when the policy using the named location should apply to unknown locations.

Common questions

Is there Graph API support?

Graph API support for named locations is available. For more information, see the [namedLocation API](#).

What if I use a cloud proxy or VPN?

When you use a cloud hosted proxy or VPN solution, the IP address Microsoft Entra ID uses while evaluating a policy is the IP address of the proxy. The X-Forwarded-For (XFF) header that contains the user's public IP address isn't used because there's no validation that it comes from a trusted source. This lack of validation could allow faking an IP address.

When a cloud proxy is in place, a policy that requires a [Microsoft Entra hybrid joined or compliant device](#) can be easier to manage. Keeping an up-to-date list of IP addresses used by your cloud-hosted proxy or VPN solution is nearly impossible.

We recommend organizations utilize Global Secure Access to enable [source IP restoration](#) to avoid this change in address and simplify management.

When is a location evaluated?

Conditional Access policies evaluate when:

- A user initially signs in to a web app, mobile or desktop application.
- A mobile or desktop application that uses modern authentication, uses a refresh token to acquire a new access token. By default, this check occurs once an hour.

This check means for mobile and desktop applications using modern authentication, a change in location is detected within an hour of changing the network location. For mobile and desktop applications that don't use modern authentication, the policy applies on each token request. The frequency of the request can vary based on the application. Similarly, for web applications, policies apply at initial sign-in and are good for the lifetime of the session at the web application. Because of differences in session lifetimes across applications, the time between policy evaluation varies. Each time the application requests a new sign-in token, the policy is applied.

By default, Microsoft Entra ID issues a token on an hourly basis. After users move off the corporate network, within an hour the policy is enforced for applications using modern authentication.

When you might block locations?

A policy that uses the location condition to block access is considered restrictive, and should be done with care after thorough testing. Some instances of using the location condition to block authentication might include:

- Blocking countries/regions where your organization never does business.
- Blocking specific IP ranges, such as:
 - Known malicious IPs before a firewall policy can be changed.
 - Highly sensitive or privileged actions and cloud applications.
 - Based on user specific IP range like access to accounting or payroll applications.

Related content

- [Configure an example Conditional Access policy using location.](#)

Conditional Access: Conditions

Article • 03/12/2025

Within a Conditional Access policy, an administrator can use one or more signals to enhance their policy decisions.

The screenshot shows the Microsoft Entra admin center interface for creating a new Conditional Access policy. On the left, there's a vertical sidebar with various icons representing different administrative functions. The main area shows the 'New Conditional Access policy' screen. At the top, there's a breadcrumb navigation: Home > Conditional Access | Policies >. Below that, the title 'New' is followed by a 'Conditional Access policy' subtitle. A large red box highlights the 'Conditions' section, which is described as controlling access based on signals from conditions like risk, device platform, location, client apps, or device state. This section includes fields for User risk (set to 'Not configured'), Sign-in risk (set to 'Not configured'), Insider risk (set to 'Not configured'), Device platforms (set to 'Not configured'), Locations (set to 'Not configured'), Client apps (set to 'Not configured'), Filter for devices (set to 'Not configured'), and Authentication flows (set to 'Not configured'). Other sections visible include 'Assignments' (with 0 users and groups selected), 'Target resources' (with no target resources selected), 'Network' (marked as NEW), 'Conditions' (0 conditions selected), 'Access controls' (Grant: 0 controls selected, Session: 0 controls selected), and 'Enable policy' (Report-only, On, Off). A 'Create' button is at the bottom right.

Multiple conditions can be combined to create fine-grained and specific Conditional Access policies.

When users access a sensitive application, an administrator might factor multiple conditions into their access decisions, such as:

- Sign-in risk information from ID Protection
- Network location
- Device information

User risk

Administrators with access to [ID Protection](#) can evaluate user risk as part of a Conditional Access policy. User risk represents the probability that a given identity or account is compromised. More information about user risk is found in the articles [What is risk](#) and [How To: Configure and enable risk policies](#).

Sign-in risk

Administrators with access to [ID Protection](#) can evaluate sign-in risk as part of a Conditional Access policy. Sign-in risk represents the probability that a given authentication request wasn't made by the identity owner. More information about sign-in risk is found in the articles [What is risk](#) and [How To: Configure and enable risk policies](#).

Insider risk

Administrators with access to [Microsoft Purview adaptive protection](#) can incorporate risk signals from Microsoft Purview into Conditional Access policy decisions. Insider risk takes into account your data governance, data security, and risk and compliance configurations from Microsoft Purview. These signals are based on contextual factors like:

- User behavior
- Historical patterns
- Anomaly detections

This condition lets administrators use Conditional Access policies to take actions like blocking access, requiring stronger authentication methods, or requiring terms of use acceptance.

This functionality involves incorporating parameters that specifically address potential risks arising from within an organization. By configuring Conditional Access to consider

Insider Risk, administrators can tailor access permissions based on contextual factors such as user behavior, historical patterns, and anomaly detection.

For more information, see the article [Configure and enable an insider risk based policy](#).

Device platforms

Conditional Access identifies the device platform by using information provided by the device, such as user agent strings. Since user agent strings can be modified, this information is unverified. Use of device platform should be paired with Microsoft Intune device compliance policies or as part of a block statement. The default is to apply to all device platforms.

Conditional Access supports the following device platforms:

- Android
- iOS
- Windows
- macOS
- Linux

If you block legacy authentication using the **Other clients** condition, you can also set the device platform condition.

Selecting macOS or Linux device platforms isn't supported when selecting **Require approved client app** or **Require app protection policy** as the only grant controls or when you choose **Require all the selected controls**.

Important

Microsoft recommends having a Conditional Access policy for unsupported device platforms. For example, to block access to your corporate resources from **Chrome OS** or any other unsupported clients, configure a policy with a Device platforms condition that includes any device and excludes supported device platforms and Grant control set to Block access.

Locations

The locations condition moved.

Client apps

By default, all newly created Conditional Access policies apply to all client app types even if the client apps condition isn't configured.

ⓘ Note

The behavior of the client apps condition was updated in August 2020. If you have existing Conditional Access policies, they remain unchanged. However, if you select an existing policy, the **Configure** toggle is removed and the client apps the policy applies to are selected.

ⓘ Important

Sign-ins from legacy authentication clients don't support multifactor authentication (MFA) and don't pass device state information, so they're blocked by Conditional Access grant controls, like requiring MFA or compliant devices. If you have accounts which must use legacy authentication, you must either exclude those accounts from the policy, or configure the policy to only apply to modern authentication clients.

The **Configure** toggle when set to **Yes** applies to checked items, when set to **No** it applies to all client apps, including modern and legacy authentication clients. This toggle doesn't appear in policies created before August 2020.

- Modern authentication clients
 - Browser
 - These include web-based applications that use protocols like SAML, WS-Federation, OpenID Connect, or services registered as an OAuth confidential client.
 - Mobile apps and desktop clients
 - This option includes applications like the Office desktop and phone applications.
- Legacy authentication clients
 - Exchange ActiveSync clients
 - This selection includes all use of the Exchange ActiveSync (EAS) protocol. When policy blocks the use of Exchange ActiveSync, the affected user receives a single quarantine email. This email provides information on why they're blocked and includes remediation instructions if able.
 - Administrators can apply policy only to supported platforms (such as iOS, Android, and Windows) through the Conditional Access Microsoft Graph API.

- Other clients
- This option includes clients that use basic/legacy authentication protocols that don't support modern authentication.
- SMTP - Used by POP and IMAP client's to send email messages.
- Autodiscover - Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.
- Exchange Online PowerShell - Used to connect to Exchange Online with remote PowerShell. If you block Basic authentication for Exchange Online PowerShell, you need to use the Exchange Online PowerShell Module to connect. For instructions, see [Connect to Exchange Online PowerShell using multifactor authentication](#).
- Exchange Web Services (EWS) - A programming interface used by Outlook, Outlook for Mac, and third-party apps.
- IMAP4 - Used by IMAP email clients.
- MAPI over HTTP (MAPI/HTTP) - Used by Outlook 2010 and later.
- Offline Address Book (OAB) - A copy of address list collections that are downloaded and used by Outlook.
- Outlook Anywhere (RPC over HTTP) - Used by Outlook 2016 and earlier.
- Outlook Service - Used by the Mail and Calendar app for Windows 10.
- POP3 - Used by POP email clients.
- Reporting Web Services - Used to retrieve report data in Exchange Online.

These conditions are commonly used to:

- Require a managed device
- Block legacy authentication
- Block web applications but allow mobile or desktop apps

Supported browsers

This setting works with all browsers. However, to satisfy a device policy, like a compliant device requirement, the following operating systems and browsers are supported.

Operating Systems and browsers out of mainstream support aren't shown on this list:

[+] Expand table

Operating Systems	Browsers
Windows 10 +	Microsoft Edge, Chrome , Firefox 91+
Windows Server 2022	Microsoft Edge, Chrome
Windows Server 2019	Microsoft Edge, Chrome

Operating Systems	Browsers
iOS	Microsoft Edge, Safari (see the notes)
Android	Microsoft Edge, Chrome
macOS	Microsoft Edge, Chrome, Firefox 133+ ↗ , Safari
Linux Desktop	Microsoft Edge

These browsers support device authentication, allowing the device to be identified and validated against a policy. The device check fails if the browser is running in private mode or if cookies are disabled.

ⓘ Note

Microsoft Edge 85+ requires the user to be signed in to the browser to properly pass device identity. Otherwise, it behaves like Chrome without the [Microsoft Single Sign On extension ↗](#). This sign-in might not occur automatically in a hybrid device join scenario.

Safari is supported for device-based Conditional Access on a managed device, but it can't satisfy the **Require approved client app** or **Require app protection policy** conditions. A managed browser like Microsoft Edge satisfies approved client app and app protection policy requirements. On iOS with non-Microsoft MDM solutions, only the Microsoft Edge browser supports device policy.

[Firefox 91+ ↗](#) is supported for device-based Conditional Access, but "Allow Windows single sign-on for Microsoft, work, and school accounts" needs to be enabled.

[Chrome 111+ ↗](#) is supported for device-based Conditional Access, but "CloudApAuthEnabled" needs to be enabled.

macOS devices using the Enterprise SSO plugin require the [Microsoft Single Sign On ↗](#) extension to support SSO and device-based Conditional Access in Google Chrome.

macOS devices using the Firefox browser must be running macOS version 10.15 or newer and have the [Microsoft Enterprise SSO plug-in installed](#) and [configured appropriately](#).

Why do I see a certificate prompt in the browser

On Windows 7, iOS, Android, and macOS devices are identified using a client certificate. This certificate is provisioned when the device is registered. When a user first signs in through the browser the user is prompted to select the certificate. The user must select this certificate before using the browser.

Chrome support

Windows

For Chrome support in **Windows 10 Creators Update (version 1703)** or later, install the [Microsoft Single Sign On](#) extension or enable Chrome's [CloudAPAuthEnabled](#). These configurations are required when a Conditional Access policy requires device-specific details for Windows platforms specifically.

To automatically enable the CloudAPAuthEnabled policy in Chrome, create the following registry key:

- Path: `HKEY_LOCAL_MACHINE\Software\Policies\Google\Chrome`
- Name: `CloudAPAuthEnabled`
- Value: `0x00000001`
- PropertyType: `DWORD`

To automatically deploy the Microsoft Single Sign On extension to Chrome browsers, create the following registry key using the [ExtensionInstallForcelist](#) policy in Chrome:

- Path:
`HKEY_LOCAL_MACHINE\Software\Policies\Google\Chrome\ExtensionInstallForcelist`
- Name: `1`
- Type: `REG_SZ (String)`
- Data:
`ppnbnppeolgkicgegkbkjmhlideopiji;https://clients2.google.com/service/update2/c
rx`

For Chrome support in **Windows 8.1 and 7**, create the following registry key:

- Path:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AutoSelectCertificateForUrl`
- Name: `1`
- Type: `REG_SZ (String)`

- Data: `{"pattern": "https://device.login.microsoftonline.com", "filter": {"ISSUER": {"CN": "MS-Organization-Access"}}}`

macOS

macOS devices using the Enterprise SSO plugin require the [Microsoft Single Sign On](#) extension to support SSO and device-based Conditional Access in Google Chrome.

For MDM based deployments of Google Chrome and extension management, refer to [Set up Chrome browser on Mac](#) and [ExtensionInstallForcelist](#).

Supported mobile applications and desktop clients

Administrators can select **Mobile apps and desktop clients** as client app.

This setting has an effect on access attempts made from the following mobile apps and desktop clients:

[Expand table](#)

Client apps	Target Service	Platform
Dynamics CRM app	Dynamics CRM	Windows 10, Windows 8.1, iOS, and Android
Mail/Calendar/People app, Outlook 2016, Outlook 2013 (with modern authentication)	Exchange Online	Windows 10
MFA and location policy for apps. Device-based policies aren't supported.	Any My Apps app service	Android and iOS
Microsoft Teams Services - this client app controls all services that support Microsoft Teams and all its Client Apps - Windows Desktop, iOS, Android, WP, and web client	Microsoft Teams	Windows 10, Windows 8.1, Windows 7, iOS, Android, and macOS
Office 2016 apps, Office 2013 (with modern authentication), OneDrive sync client	SharePoint	Windows 8.1, Windows 7
Office 2016 apps, Universal Office apps, Office 2013 (with modern authentication), OneDrive sync client	SharePoint Online	Windows 10
Office 2016 (Word, Excel, PowerPoint, OneNote only).	SharePoint	macOS

Client apps	Target Service	Platform
Office 2019	SharePoint	Windows 10, macOS
Office mobile apps	SharePoint	Android, iOS
Office Yammer app	Yammer	Windows 10, iOS, Android
Outlook 2019	SharePoint	Windows 10, macOS
Outlook 2016 (Office for macOS)	Exchange Online	macOS
Outlook 2016, Outlook 2013 (with modern authentication), Skype for Business (with modern authentication)	Exchange Online	Windows 8.1, Windows 7
Outlook mobile app	Exchange Online	Android, iOS
Power BI app	Power BI service	Windows 10, Windows 8.1, Windows 7, Android, and iOS
Skype for Business	Exchange Online	Android, iOS
Azure DevOps Services (formerly Visual Studio Team Services, or VSTS) app	Azure DevOps Services (formerly Visual Studio Team Services, or VSTS)	Windows 10, Windows 8.1, Windows 7, iOS, and Android

Exchange ActiveSync clients

- Administrators can only select Exchange ActiveSync clients when assigning policy to users or groups. Selecting **All users**, **All guest and external users**, or **Directory roles** causes all users to be subject of the policy.
- When administrators create a policy assigned to Exchange ActiveSync clients, **Exchange Online** should be the only cloud application assigned to the policy.
- Administrators can narrow the scope of this policy to specific platforms using the **Device platforms** condition.

If the access control assigned to the policy uses **Require approved client app**, the user is directed to install and use the Outlook mobile client. In the case that **Multifactor authentication**, **Terms of use**, or **custom controls** are required, affected users are blocked, because basic authentication doesn't support these controls.

For more information, see the following articles:

- [Block legacy authentication with Conditional Access](#)
- [Requiring approved client apps with Conditional Access](#)

Other clients

By selecting **Other clients**, you can specify a condition that affects apps that use basic authentication with mail protocols like IMAP, MAPI, POP, SMTP, and older Office apps that don't use modern authentication.

Device state (deprecated)

This condition was deprecated. Customers should use the **Filter for devices** condition in the Conditional Access policy, to satisfy scenarios previously achieved using the device state condition.

 **Important**

Device state and filters for devices can't be used together in Conditional Access policy. Filters for devices provide more granular targeting including support for targeting device state information through the `trustType` and `isCompliant` property.

Filter for devices

When administrators configure filter for devices as a condition, they can include or exclude devices based on a filter using a rule expression on device properties. The rule expression for filter for devices can be authored using rule builder or rule syntax. This experience is similar to the one used for rules for dynamic membership groups. For more information, see the article [Conditional Access: Filter for devices](#).

Authentication flows (preview)

Authentication flows control how your organization uses certain authentication and authorization protocols and grants. These flows might provide a seamless experience to devices that might lack local input devices like shared devices or digital signage. Use this control to configure transfer methods like [device code flow or authentication transfer](#).

Next steps

- Conditional Access: Grant
 - Common Conditional Access policies
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Conditional Access: Grant

Article • 02/27/2025

Within a Conditional Access policy, an administrator can use access controls to grant or block access to resources.

The screenshot shows the 'Grant' configuration page in the Microsoft Azure portal. The URL is https://portal.azure.com/?Microsoft_AAD_IAM_ca.showrequireauthstrength=true&Microsoft_AAD_IAM_... . The page title is 'Grant - Microsoft Azure'. The left sidebar shows the navigation path: Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies > Require Phish-Resistant MFA for Admins. The main content area is titled 'Require Phish-Resistant MFA for Admins' and is described as a 'Conditional Access policy'. It includes sections for 'Name' (Require Phish-Resistant MFA for Admins), 'Assignments' (Users or workload identities, Specific users included and specific users excluded), 'Cloud apps or actions' (All cloud apps), 'Conditions' (0 conditions selected), 'Access controls' (Grant, 1 control selected), and 'Session' (0 controls selected). The 'Grant' section is selected. Under 'Grant', the 'Control access enforcement to block or grant access' section has 'Grant access' selected. Under 'Access controls', 'Require authentication strength' is checked, while 'Require multifactor authentication' is unchecked. A warning message states: "⚠️ 'Require authentication strength' cannot be used with 'Require multifactor authentication'". Other available controls include 'Require device to be marked as compliant', 'Require Hybrid Azure AD joined device', 'Require approved client app', 'Require app protection policy', 'Require password change', and 'Contoso App - Terms of Use'. At the bottom, there are options for 'Enable policy' (Report-only, On, Off) and a 'Save' button. A 'Select' button and a magnifying glass icon are also present.

Block access

The control for blocking access considers any assignments and prevents access based on the Conditional Access policy configuration.

Block access is a powerful control that you should apply with appropriate knowledge. Policies with block statements can have unintended side effects. Proper testing and validation are vital before you enable the control at scale. Administrators should use tools such as [Conditional Access report-only mode](#) and [the What If tool in Conditional Access](#) when making changes.

Grant access

Administrators can choose to enforce one or more controls when granting access. These controls include the following options:

- Require multifactor authentication ([Microsoft Entra multifactor authentication](#))
- Require authentication strength
- Require device to be marked as compliant ([Microsoft Intune](#))
- Require Microsoft Entra hybrid joined device
- Require approved client app
- Require app protection policy
- Require password change

When administrators choose to combine these options, they can use the following methods:

- Require all the selected controls (control *and* control)
- Require one of the selected controls (control *or* control)

By default, Conditional Access requires all selected controls.

Require multifactor authentication

Selecting this checkbox requires users to perform Microsoft Entra multifactor authentication. You can find more information about deploying Microsoft Entra multifactor authentication in [Planning a cloud-based Microsoft Entra multifactor authentication deployment](#).

[Windows Hello for Business](#) satisfies the requirement for multifactor authentication in Conditional Access policies.

Require authentication strength

Administrators can choose to require [specific authentication strengths](#) in their Conditional Access policies. These authentication strengths are defined in the **Microsoft Entra admin center > Protection > Authentication methods > Authentication strengths**. Administrators can choose to create their own or use the built-in versions.

Require device to be marked as compliant

Organizations that deploy Intune can use the information returned from their devices to identify devices that meet specific policy compliance requirements. Intune sends compliance information to Microsoft Entra ID so Conditional Access can decide to grant

or block access to resources. For more information about compliance policies, see [Set rules on devices to allow access to resources in your organization by using Intune](#).

A device can be marked as compliant by Intune for any device operating system or by a third-party mobile device management system for Windows devices. You can find a list of supported third-party mobile device management systems in [Support third-party device compliance partners in Intune](#).

Devices must be registered in Microsoft Entra ID before they can be marked as compliant. You can find more information about device registration in [What is a device identity?](#).

The **Require device to be marked as compliant** control:

- Only supports Windows 10+, iOS, Android, macOS, and Linux Ubuntu devices registered with Microsoft Entra ID and enrolled with Intune.
- Microsoft Edge in InPrivate mode on Windows is considered a noncompliant device.

 **Note**

On Windows, iOS, Android, macOS, and some third-party web browsers, Microsoft Entra ID identifies the device by using a client certificate that is provisioned when the device is registered with Microsoft Entra ID. When a user first signs in through the browser, the user is prompted to select the certificate. The user must select this certificate before they can continue to use the browser.

You can use the Microsoft Defender for Endpoint app with the approved client app policy in Intune to set the device compliance policy to Conditional Access policies.

There's no exclusion required for the Microsoft Defender for Endpoint app while you're setting up Conditional Access. Although Microsoft Defender for Endpoint on Android and iOS (app ID dd47d17a-3194-4d86-bfd5-c6ae6f5651e3) isn't an approved app, it has permission to report device security posture. This permission enables the flow of compliance information to Conditional Access.

Require Microsoft Entra hybrid joined device

Organizations can choose to use the device identity as part of their Conditional Access policy. Organizations can require that devices are Microsoft Entra hybrid joined by using this checkbox. For more information about device identities, see [What is a device identity?](#)

When you use the [device-code OAuth flow](#), the required grant control for the managed device or a device state condition isn't supported. This is because the device that is performing authentication can't provide its device state to the device that is providing a code. Also, the device state in the token is locked to the device performing authentication. Use the **Require multifactor authentication** control instead.

The **Require Microsoft Entra hybrid joined device** control:

- Only supports domain-joined Windows down-level (before Windows 10) and Windows current (Windows 10+) devices.
- Doesn't consider Microsoft Edge in InPrivate mode as a Microsoft Entra hybrid joined device.

Require approved client app

Organizations can require that an approved client app is used to access selected cloud apps. These approved client apps support [Intune app protection policies](#) independent of any mobile device management solution.

Warning

The approved client app grant is retiring in early March 2026. Organizations must transition all current Conditional Access policies that use only the Require Approved Client App grant to Require Approved Client App or Application Protection Policy by March 2026. Additionally, for any new Conditional Access policy, only apply the Require application protection policy grant. For more information, see the article [Migrate approved client app to application protection policy in Conditional Access](#).

To apply this grant control, the device must be registered in Microsoft Entra ID, which requires using a broker app. The broker app can be Microsoft Authenticator for iOS, or either Microsoft Authenticator or Microsoft Company Portal for Android devices. If a broker app isn't installed on the device when the user attempts to authenticate, the user is redirected to the appropriate app store to install the required broker app.

The following client apps support this setting. This list isn't exhaustive and is subject to change:

- Microsoft Azure Information Protection
- Microsoft Cortana
- Microsoft Dynamics 365
- Microsoft Edge

- Microsoft Excel
- Microsoft Power Automate
- Microsoft Invoicing
- Microsoft Kaizala
- Microsoft Launcher
- Microsoft Lists
- Microsoft Office
- Microsoft OneDrive
- Microsoft OneNote
- Microsoft Outlook
- Microsoft Planner
- Microsoft Power Apps
- Microsoft Power BI
- Microsoft PowerPoint
- Microsoft SharePoint
- Microsoft Skype for Business
- Microsoft Stream
- Microsoft Teams
- Microsoft To Do
- Microsoft Visio
- Microsoft Word
- Microsoft Yammer
- Microsoft Whiteboard
- Microsoft 365 Admin

Remarks

- The approved client apps support the Intune mobile application management feature.
- **The Require approved client app requirement:**
 - Only supports the iOS and Android for device platform condition.
 - Requires a broker app to register the device. The broker app can be Microsoft Authenticator for iOS, or either Microsoft Authenticator or Microsoft Company Portal for Android devices.
- Conditional Access can't consider Microsoft Edge in InPrivate mode an approved client app.
- Conditional Access policies that require Microsoft Power BI as an approved client app don't support using Microsoft Entra application proxy to connect the Power BI mobile app to the on-premises Power BI Report Server.

- WebViews hosted outside of Microsoft Edge don't satisfy the approved client app policy. For example: If an app is trying to load SharePoint in a webview, app protection policies fail.

See [Require approved client apps for cloud app access with Conditional Access](#) for configuration examples.

Require app protection policy

In Conditional Access policy, you can require that an [Intune app protection policy](#) is present on the client app before access is available to the selected applications. These mobile application management (MAM) app protection policies allow you to manage and protect your organization's data within specific applications.

To apply this grant control, Conditional Access requires that the device is registered in Microsoft Entra ID, which requires using a broker app. The broker app can be either Microsoft Authenticator for iOS or Microsoft Company Portal for Android devices. If a broker app isn't installed on the device when the user attempts to authenticate, the user is redirected to the app store to install the broker app. The Microsoft Authenticator app can be used as the broker app but doesn't support being targeted as an approved client app. App protection policies are generally available for iOS and Android, and in public preview for Microsoft Edge on Windows. [Windows devices support no more than three Microsoft Entra user accounts in the same session](#). For more information about how to apply policy to Windows devices, see the article [Require an app protection policy on Windows devices \(preview\)](#).

Applications must meet certain requirements to support app protection policies. Developers can find more information about these requirements in the section [Apps you can manage with app protection policies](#).

The following client apps support this setting. This list isn't exhaustive and is subject to change. If your app isn't in the list, check with the application vendor to confirm support:

- Adobe Acrobat Reader mobile app
- iAnnotate for Office 365
- Microsoft Cortana
- Microsoft Dynamics 365 for Phones
- Microsoft Dynamics 365 Sales
- Microsoft Edge
- Microsoft Excel
- Microsoft Power Automate

- Microsoft Launcher
- Microsoft Lists
- Microsoft Loop
- Microsoft Office
- Microsoft OneDrive
- Microsoft OneNote
- Microsoft Outlook
- Microsoft Planner
- Microsoft Power BI
- Microsoft PowerApps
- Microsoft PowerPoint
- Microsoft SharePoint
- Microsoft Stream Mobile Native 2.0
- Microsoft Teams
- Microsoft To Do
- Microsoft Word
- Microsoft Whiteboard Services
- MultiLine for Intune
- Nine Mail - Email and Calendar
- Notate for Intune
- Provectus - Secure Contacts
- Viva Engage (Android, iOS, and iPadOS)

 **Note**

Kaizala, Skype for Business, and Visio don't support the **Require app protection policy** grant. If you require these apps to work, use the **Require approved apps** grant exclusively. Using the "or" clause between the two grants will not work for these three applications.

See [Require app protection policy and an approved client app for cloud app access with Conditional Access](#) for configuration examples.

Require password change

When user risk is detected, administrators can employ the user risk policy conditions to have the user securely change a password by using Microsoft Entra self-service password reset. Users can perform a self-service password reset to self-remediate. This process closes the user risk event to prevent unnecessary alerts for administrators.

When a user is prompted to change a password, they're first required to complete multifactor authentication. Make sure all users register for multifactor authentication, so they're prepared in case risk is detected for their account.

Warning

Users must have previously registered for multifactor authentication before triggering the user risk policy.

The following restrictions apply when you configure a policy by using the password change control:

- The policy must be assigned to **All resources**. This requirement prevents an attacker from using a different app to change the user's password and resetting their account risk by signing in to a different app.
- **Require password change** can't be used with other controls, such as requiring a compliant device.
- The password change control can only be used with the user and group assignment condition, cloud app assignment condition (which must be set to "all"), and user risk conditions.

Terms of use

If your organization created terms of use, other options might be visible under grant controls. These options allow administrators to require acknowledgment of terms of use as a condition of accessing the resources that the policy protects. You can find more information about terms of use in [Microsoft Entra terms of use](#).

Multiple grant controls

When multiple grant controls are applied to a user, it's important to understand that Conditional Access policies follow a specific validation order by design. For example, if a user has two policies requiring multifactor authentication (MFA) and Terms of Use (ToU), Conditional Access first validates the user's MFA claim and then the ToU.

- If a valid MFA claim isn't present in the token, you see an "interrupt" (pending MFA) and a failure for ToU in the logs, even if the ToU was already accepted in a previous sign-in.
- Once multifactor authentication is completed, a second log entry appears, validating the ToU. If the user already accepted the ToU, you see success for both MFA and ToU.

- If a valid MFA claim is present in the token, a single log shows success for both MFA and ToU.

If multiple policies are applied to a user requiring MFA, Device State, and ToU, the process is similar. The validation order is MFA, Device State, and then ToU.

Custom controls (preview)

Custom controls are a preview capability of Microsoft Entra ID. When you use custom controls, your users are redirected to a compatible service to satisfy authentication requirements that are separate from Microsoft Entra ID. For more information, check out the [Custom controls](#) article.

Next steps

- [Conditional Access: Session controls](#)
- [Conditional Access common policies](#)
- [Report-only mode](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Conditional Access: Session

Article • 08/13/2024

Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications.

The screenshot shows the Microsoft Azure Conditional Access PolicyBlade interface. On the left, there's a navigation pane with 'Home', 'Contoso | Security', 'Security | Conditional Access', and 'Conditional Access | Policies'. Below that, it says 'New ... Conditional Access policy'. The main area has sections for 'Name *' (with 'Example: 'Device compliance app policy''), 'Assignments' (with 'Users 0 users and groups selected'), 'Cloud apps or actions' (with 'No cloud apps, actions, or authentication contexts selected'), 'Conditions' (with '0 conditions selected'), 'Access controls' (with 'Grant 0 controls selected'), and 'Session' (with '0 controls selected'). At the bottom, there's an 'Enable policy' section with radio buttons for 'Report-only' (selected), 'On', and 'Off', and a 'Create' button. On the right, under the heading 'Session', it says 'Control access based on session controls to enable limited experiences within specific cloud applications. Learn more'. It lists several options with checkboxes: 'Use app enforced restrictions' (which has a note: 'This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more'), 'Use Conditional Access App Control', 'Sign-in frequency', 'Persistent browser session', 'Customize continuous access evaluation', 'Disable resilience defaults', and 'Require token protection for sign-in sessions (Preview)'. There's also a 'Select' button at the bottom right.

Application enforced restrictions

Organizations can use this control to require Microsoft Entra ID to pass device information to the selected cloud apps. The device information allows cloud apps to know if a connection is from a compliant or domain-joined device and update the session experience. When selected, the cloud app uses the device information to provide users with a limited or full experience. Limited when the device isn't managed or compliant and full when the device is managed and compliant.

For a list of supported applications and how to configure policies, see the following articles:

- [Idle session timeout for Microsoft 365](#).
- [Enabling limited access with SharePoint Online](#)

- Enabling limited access with Exchange Online

Conditional Access application control

Conditional Access App Control uses a reverse proxy architecture and is uniquely integrated with Microsoft Entra Conditional Access. Microsoft Entra Conditional Access allows you to enforce access controls on your organization's apps based on certain conditions. The conditions define what user or group of users, cloud apps, and locations and networks a Conditional Access policy applies to. After you determine the conditions, you can route users to [Microsoft Defender for Cloud Apps](#) where you can protect data with Conditional Access App Control by applying access and session controls.

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to refine filters and set actions to take. With the access and session policies, you can:

- Prevent data exfiltration: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.
- Protect on download: Instead of blocking the download of sensitive documents, you can require documents to be labeled and protected with Azure Information Protection. This action ensures the document is protected and user access is restricted in a potentially risky session.
- Prevent upload of unlabeled files: Before a sensitive file is uploaded, distributed, and used, it's important to make sure that the file has the right label and protection. You can ensure that unlabeled files with sensitive content are blocked from being uploaded until the user classifies the content.
- Monitor user sessions for compliance (Preview): Risky users are monitored when they sign into apps and their actions are logged from within the session. You can investigate and analyze user behavior to understand where, and under what conditions, session policies should be applied in the future.
- Block access (Preview): You can granularly block access for specific apps and users depending on several risk factors. For example, you can block them if they're using client certificates as a form of device management.
- Block custom activities: Some apps have unique scenarios that carry risk, for example, sending messages with sensitive content in apps like Microsoft Teams or Slack. In these kinds of scenarios, you can scan messages for sensitive content and block them in real time.

For more information, see the article [Deploy Conditional Access App Control for featured apps](#).

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. Administrators can select a period of time (hours or days) or choose to require reauthentication every time.

Sign-in frequency setting works with apps that implement OAUTH2 or OIDC protocols according to the standards. Most Microsoft native apps for Windows, Mac, and Mobile including the following web applications follow the setting.

- Word, Excel, PowerPoint Online
- OneNote Online
- Office.com
- Microsoft 365 Admin portal
- Exchange Online
- SharePoint and OneDrive
- Teams web client
- Dynamics CRM Online
- Azure portal

For more information, see the article [Configure authentication session management with Conditional Access](#).

Persistent browser session

A persistent browser session allows users to remain signed in after closing and reopening their browser window.

For more information, see the article [Configure authentication session management with Conditional Access](#).

Customize continuous access evaluation

[Continuous access evaluation](#) is auto enabled as part of an organization's Conditional Access policies. For organizations who wish to disable continuous access evaluation, this configuration is now an option within the session control within Conditional Access. Continuous access evaluation policies can be scoped to all users or specific users and groups. Admins can make the following selection while creating a new policy or while editing an existing Conditional Access policy.

- **Disable** only work when **All cloud apps** are selected, no conditions are selected, and **Disable** is selected under **Session > Customize continuous access evaluation**

in a Conditional Access policy. You can choose to disable all users or specific users and groups.

The screenshot shows the Microsoft Azure portal interface for creating a new Conditional Access policy named "Conditional Access Documentation". The left sidebar lists policy components: Assignments, Cloud apps or actions, Conditions, Access controls, and Session. The "Session" section is currently selected and expanded, showing various configuration options. A callout box provides information about app enforced restrictions, stating it only works with supported apps like Office 365, Exchange Online, and SharePoint Online. Other options shown include "Use Conditional Access App Control", "Sign-in frequency", "Persistent browser session", "Customize continuous access evaluation" (which is checked), and "Disable". At the bottom right of the configuration area is a "Select" button with a magnifying glass icon.

Session

Control access based on session controls to enable limited experiences within specific cloud applications.

Learn more

Use app enforced restrictions ⓘ

i This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

Use Conditional Access App Control ⓘ

Sign-in frequency ⓘ

Persistent browser session ⓘ

Customize continuous access evaluation ⓘ

Disable

See list of supported clients and resource providers

Disable resilience defaults (Preview) ⓘ

Select

Disable resilience defaults

During an outage, Microsoft Entra ID extends access to existing sessions while enforcing Conditional Access policies.

If resilience defaults are disabled, access is denied once existing sessions expire. For more information, see the article [Conditional Access: Resilience defaults](#).

Require token protection for sign-in sessions (preview)

Token protection (sometimes referred to as token binding in the industry) attempts to reduce attacks using token theft by ensuring a token is usable only from the intended device. When an attacker is able to steal a token, by hijacking or replay, they can impersonate their victim until the token expires or is revoked. Token theft is thought to be a relatively rare event, but the damage from it can be significant.

The preview works for specific scenarios only. For more information, see the article [Conditional Access: Token protection \(preview\)](#).

Use Global Secure Access security profile

Using a security profile with Conditional Access unifies identity controls with network security in Microsoft's Security Service Edge (SSE) product, [Microsoft Entra Internet Access](#). Selecting this Session control allows you to bring identity and context awareness to security profiles, which are groupings of various policies created and managed in Global Secure Access.

Related content

- [Conditional Access common policies](#)
- [Report-only mode](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Analyze Conditional Access Policy Impact

Article • 03/12/2025

Conditional Access helps organizations stay secure by applying the right security access controls under the right circumstances. Understanding the impact of these policies can be challenging, especially when deploying new policies. This article explains how to analyze Conditional Access policy impact using report-only mode and other tools.

There are several options available to administrators based on report-only mode. Report-only mode is a policy state letting administrators test most Conditional Access policies before enabling them.

- Conditional Access policies can be evaluated in report-only mode except for items included in the "User Actions" scope.
- During sign-in, policies in report-only mode are evaluated but not enforced.
- Results are logged in the **Conditional Access** and **Report-only** tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

<https://www.youtube-nocookie.com/embed/NZbPYfhb5Kc>

⚠️ Warning

Policies in report-only mode that require a compliant device might prompt users on macOS, iOS, and Android devices to select a device certificate during policy evaluation, even though device compliance isn't enforced. These prompts might repeat until the device is compliant. To prevent end users from receiving prompts during sign-in, exclude device platforms Mac, iOS, and Android from report-only policies that perform device compliance checks.

Policy evaluation results

When a policy is evaluated for a given sign-in, there are several possible results:

 Expand table

Result	Description
Report-only: Success	All configured policy conditions, required non-interactive grant controls, and session controls were satisfied. For example, a multifactor authentication requirement is satisfied by an MFA claim already present in the token, or a compliant device policy is satisfied by performing a device check on a compliant device.
Report-only: Failure	All configured policy conditions were satisfied but not all the required non-interactive grant controls or session controls were satisfied. For example, a policy applies to a user where a block control is configured, or a device fails a compliant device policy.
Report-only: User action required	All configured policy conditions were satisfied but user action would be required to satisfy the required grant controls or session controls. With report-only mode, the user isn't prompted to satisfy the required controls. For example, users aren't prompted for multifactor authentication challenges or terms of use.
Report-only: Not applied	Not all configured policy conditions were satisfied. For example, the user is excluded from the policy or the policy only applies to certain trusted named locations.
Success	Sign-in events where the policy applied, the requirements were met, and the policy would allow the sign-in to proceed. The sign-in might still be blocked by a different policy.
Failure	Sign-in events where the policy applied, the requirements weren't met, and the policy would block the sign-in. This might be by design, like when sign-ins from a specific location are blocked, or accidental when the policy is misconfigured.
Not applied	Sign-in events where the policy wasn't applied, for example, the user was excluded.

Reviewing results

Administrators can use several options to review the potential results of policies in their environment:

- Workbooks
- Sign-in logs
- Policy impact (Preview)

Policy impact (Preview)

The policy impact view of Conditional Access lets admins with at least the Security Reader role see a snapshot of information about the potential or existing impacts of policies on interactive sign-ins in your organization. This functionality lets you explore

impact over a period of the past 24 hours, 7 days, or 1 month. Additionally, you can see and link to a sampling of sign-in events for further detail.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with various icons. The main area shows a policy configuration for 'Multifactor authentication for all'. The 'View policy impact (Preview)' button is highlighted with a red box. To the right, the 'Policy impact (Preview)' section is displayed, featuring a chart titled 'Sign-in activity over time' showing data from Feb 10 to Mar 12. The chart has three stacked areas: green (Success), orange (Failure), and grey (Not applied). Below the chart, success rates are summarized: Total sign-ins (100%), Success (73.89%), Failure (2.72%), and Not applied (23.39%). A table titled 'Sample sign-ins on February 25, 2025 where policy controls were not met' lists three entries:

Date	User	Application
2/25/2025, 10:21:08 PM	Harri Kalda	Azure Portal
2/25/2025, 9:49:46 PM	Harri Kalda	Azure Portal
2/25/2025, 9:48:20 PM	Harri Kalda	Microsoft App Access P...

Workbooks

Administrators can create multiple policies in report-only mode, so it's necessary to understand both the individual impact of each policy and the combined impact of multiple policies evaluated together. The [Conditional Access Insights and Reporting workbook](#) lets administrators visualize Conditional Access policy, it queries and monitor the impact of a policy for a given time range, set of applications, and users. Administrators can customize workbooks to suit their specific needs.

Sign-in logs

For deeper evaluation of Conditional Access policies and their application at a specific sign-in, administrators might investigate individual sign-in events. Each of these events includes details of what Conditional Access policies were enabled versus were in report-only mode, and applied or didn't apply.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar includes sections for Overview, Policies, Insights and reporting, Diagnose and solve problems, Manage (Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication contexts, Authentication strengths, Classic policies), Monitoring (Sign-in logs, Audit logs), and Troubleshooting + Support. The main content area is titled 'Activity Details: Sign-ins' and shows a table of sign-in logs. The table has columns for Policy Name, Grant Controls, Session Controls, and Result. A red box highlights the 'Report-only' tab in the top navigation bar and the 'Sign-in logs' link in the left sidebar.

Policy Name	Grant Controls	Session Controls	Result
REPORT ONLY - All Users - Phi...	Require authentication strength	Report-only: Success	...
Block access to Office Apps for...	Block	Report-only: Not applied	...
BLOCK - Copilot Test	Block	Report-only: Not applied	...

Using these options

After administrators confirm the settings using [report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- [Configure report-only mode on a Conditional Access policy](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

Microsoft Entra Conditional Access optimization agent

Article • 04/30/2025

The Conditional Access optimization agent helps you ensure all users are protected by policy. It recommends policies and changes based on best practices aligned with [Zero Trust](#) and Microsoft's learnings.

In preview, the agent evaluates policies requiring multifactor authentication (MFA), enforces device based controls (device compliance, app protection policies, and Domain Joined Devices), and blocks legacy authentication and device code flow.

The agent also evaluates all existing enabled policies to propose potential consolidation of similar policies.

Prerequisites

- You must be assigned the [Security Administrator](#) or [Global Administrator](#) role during the preview. These roles also have [access to Security Copilot by default](#).
- You must have at least [Microsoft Entra ID P1](#).
- You must have available [security compute units \(SCU\)](#). On average, each agent run consumes less than one SCU.
- Device-based controls require [Microsoft Intune licenses](#).

Limitations

- During the preview, avoid using an account to set up the agent that requires role activation with Privileged Identity Management. Using an account that doesn't have standing permissions might cause authentication failures for the agent.
- Once agents are started, they can't be stopped or paused. It might take a few minutes to run.
- For policy consolidation, each agent run only looks at four similar policy pairs
- The agent currently runs as the user who enables it.
- In preview, you should only run the agent from the Microsoft Entra admin center.

Getting started

1. Sign in to the [Microsoft Entra admin center](#) ↗ as at least a [Security Administrator](#).
2. From the new home page, select **Go to agents** from the agent notification card.

The Microsoft Entra admin center home page displays various tenant statistics and administrative tools. The 'Security Copilot agents are here' section is highlighted with a red box. Other visible sections include 'Contoso Outdoors' (Primary domain: contosoutdoors.ms), 'Connie Wilson' (My Entra role assignments), and '55 users at high risk'. The page also features a 'Shortcuts' bar and a 'Get the most out of your licenses and subscriptions' section.

3. Select **View details** under the Conditional Access Optimization Agent, then select **Start agent** to begin your first run.

The Microsoft Entra admin center shows the 'Conditional Access Optimization Agent' overview. The 'View details' button for the agent is highlighted with a red box. The right pane provides detailed information about the agent, including its purpose, trigger, permissions, identity, products, plugins, roles with access, and a 'Start agent' button.

4. When the agent overview page loads, you see most recent and next scheduled runtimes, performance highlights, recent suggestions, and recent activity.

The screenshot shows the Microsoft Entra admin center interface. At the top, there are tabs for 'Conditional Access Optimization' and 'Microsoft Security Copilot'. The main content area is titled 'Conditional Access Optimization Agent (Preview)'. It includes sections for 'Agent is active' (status: finished running on April 25, 2025 at 7:12 PM), 'Performance highlights' (unprotected users: 0, sign-ins protected discovered: 0, security compute units used: 0.00), 'Recent suggestions' (no suggestions yet), and 'Recent activity' (run started: 4/25/25, 7:12:14 PM, 0 suggestions, status: Complete). On the left, there's a sidebar with icons for Home, Security Copilot agents, Microsoft Entra, and Security. Below the sidebar, there are sections for 'About this agent' (description of the agent's function), 'Products' (Conditional Access), and 'Plugins' (Microsoft Entra). A search bar is located in the bottom right corner.

5. Selecting a suggestion allows you to see the proposed change, make edits, see [potential policy impact](#).
6. Newly created policies are created in report-only mode. As a best practice organizations should exclude their break-glass accounts from policy to avoid being locked out due to misconfiguration.

💡 Tip

Policies created by the agent are tagged with **Conditional Access Optimization Agent** in the Conditional Access policies pane.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Reviewing results

The agent might run and:

- Not identify any unprotected users or recommend any changes
- Suggest creation of a new Conditional Access policy in report-only mode
- Suggest adding newly created users to an existing policy

Providing feedback

Use the **Give Microsoft feedback** button at the top of the agent window to provide feedback to Microsoft about the agent.

Settings

The agent is configured to run every 24 hours based on when it's initially configured. Toggling **Trigger** to off under the settings page of the agent and back on at a specific time reconfigures the agent to run at that time.

Use the checkboxes under **Objects** to specify what the agent should monitor when making policy recommendations. By default the agent looks for both new users and applications in your tenant over the previous 24 hour period.

The agent runs under the **Identity and permissions** of the user who enabled the agent in your tenant. Because of this requirement you should avoid using an account that requires elevation like those that use PIM for just-in-time elevation.

You can tailor policy to your needs using the optional **Custom Instructions** field. This allows you to provide a prompt to the agent as part of its execution. For example: "The user "Break Glass" should be excluded from policies created." When you save the custom instruction prompt Security Copilot will attempt to interpret and the results appear in the settings page.

Remove agent

If you no longer wish to use the Conditional Access optimization agent, you can remove it using the **Remove agent** button at the top of the agent window.

Related content

- [Conditional Access policy templates](#)
- [Learn more about Microsoft Security Copilot](#)

What are service dependencies in Microsoft Entra Conditional Access?

Article • 06/14/2024

With Conditional Access policies, you can specify access requirements to websites and services. For example, your access requirements can include requiring multifactor authentication (MFA) or [managed devices](#).

When you access a site or service directly, the impact of a related policy is typically easy to assess. For example, if you have a policy that requires multifactor authentication (MFA) for SharePoint Online configured, MFA is enforced for each sign-in to the SharePoint web portal. However, it isn't always straight-forward to assess the impact of a policy because there are cloud apps with dependencies to other cloud apps. For example, Microsoft Teams can provide access to resources in SharePoint Online. So, when you access Microsoft Teams in our current scenario, you're also subject to the SharePoint MFA policy.

Tip

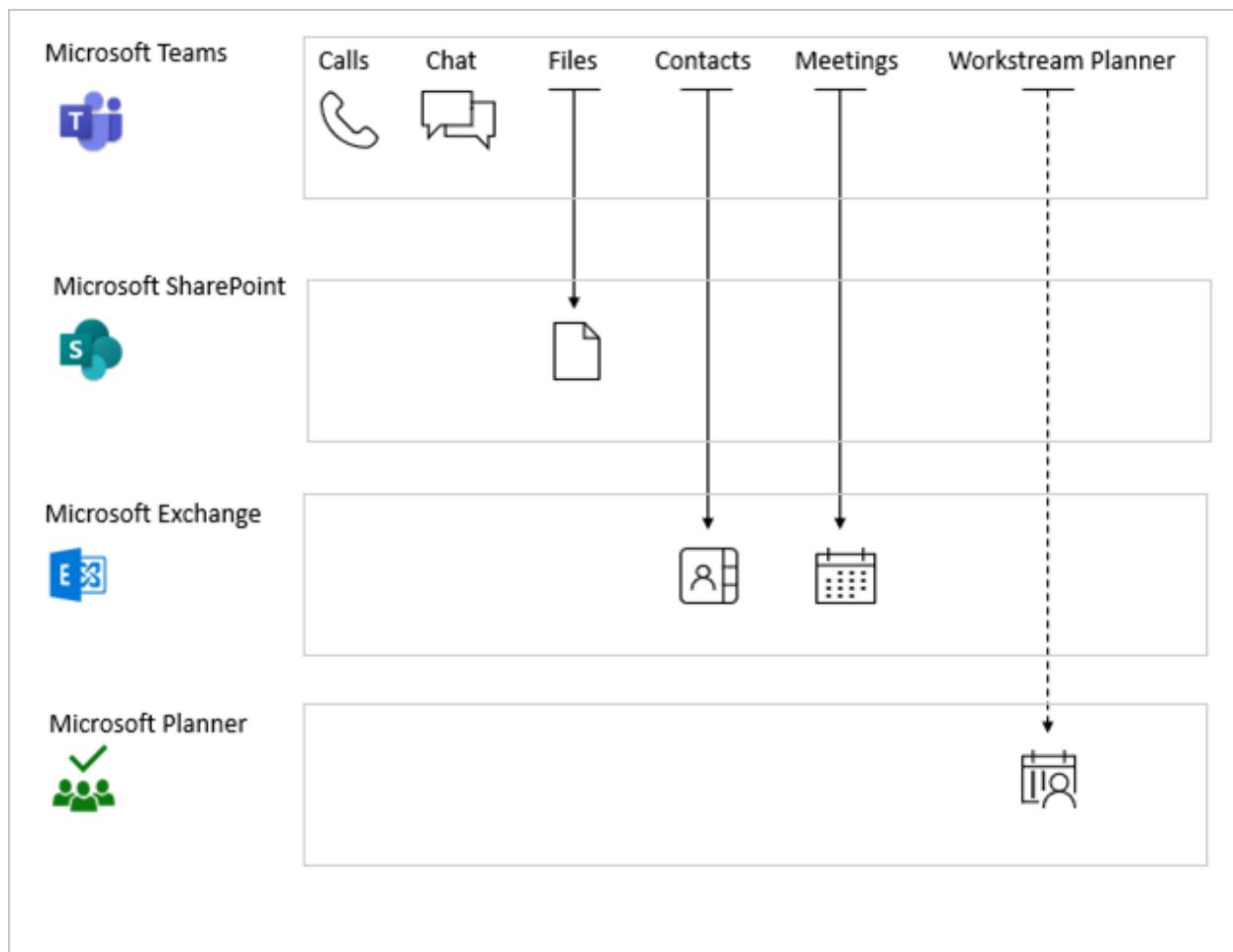
Using the [Office 365](#) app will target all Office apps to avoid issues with service dependencies in the Office stack.

Policy enforcement

If you have a service dependency configured, the policy can apply using early-bound or late-bound enforcement.

- **Early-bound policy enforcement** means a user must satisfy the dependent service policy before accessing the calling app. For example, a user must satisfy SharePoint policy before signing into Microsoft Teams.
- **Late-bound policy enforcement** occurs after the user signs into the calling app. Enforcement is deferred to when calling app requests a token for the downstream service. Examples include Microsoft Teams accessing Planner and Office.com accessing SharePoint.

The following diagram illustrates Microsoft Teams service dependencies. Solid arrows indicate early-bound enforcement the dashed arrow for Planner indicates late-bound enforcement.



As a best practice, you should set common policies across related apps and services whenever possible. Having a consistent security posture provides you with the best user experience. For example, setting a common policy across Exchange Online, SharePoint Online, and Microsoft Teams reduces prompts that might arise from different policies being applied to downstream services.

A great way to accomplish a common policy with applications in Microsoft 365 is to use the [Office 365 app](#) instead of targeting individual applications.

The below table lists some more service dependencies, where the client apps must satisfy. This list isn't exhaustive.

[\[+\] Expand table](#)

Client apps	Downstream service	Enforcement
Azure Data Lake	Windows Azure Service Management API (portal and API)	Early-bound
Microsoft Classroom	Exchange	Early-bound
	SharePoint	Early-bound
Microsoft Teams	Exchange	Early-bound

Client apps	Downstream service	Enforcement
	MS Planner	Late-bound
	Microsoft Stream	Late-bound
	SharePoint	Early-bound
	Skype for Business Online	Early-bound
	Microsoft Whiteboard	Late-bound
Office Portal	Exchange	Late-bound
	SharePoint	Late-bound
Outlook groups	Exchange	Early-bound
	SharePoint	Early-bound
Power Apps	Windows Azure Service Management API (portal and API)	Early-bound
	Windows Azure Active Directory	Early-bound
	SharePoint	Early-bound
	Exchange	Early-bound
Power Automate	Power Apps	Early-bound
Project	Dynamics CRM	Early-bound
Skype for Business	Exchange	Early-bound
Visual Studio	Windows Azure Service Management API (portal and API)	Early-bound
Microsoft Forms	Exchange	Early-bound
	SharePoint	Early-bound
Microsoft To Do	Exchange	Early-bound
SharePoint	SharePoint Online Web Client Extensibility	Early-bound
	SharePoint Online Web Client Extensibility Isolated	Early-bound
	SharePoint Client Extensibility web application principal (where present)	Early-bound

Troubleshooting service dependencies

The Microsoft Entra sign-in log is a valuable source of information when troubleshooting why and how a Conditional Access policy applied in your environment. For more information about troubleshooting unexpected sign-in outcomes related to Conditional Access, see the article [Troubleshooting sign-in problems with Conditional Access](#).

Next steps

To learn how to implement Conditional Access in your environment, see [Plan your Conditional Access deployment in Microsoft Entra ID](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Conditional Access: Filter for applications

Article • 10/29/2024

Currently Conditional Access policies can be applied to all apps or to individual apps. Organizations with a large number of apps might find this process difficult to manage across multiple Conditional Access policies.

Application filters for Conditional Access allow organizations to tag service principals with custom attributes. These custom attributes are then added to their Conditional Access policies. Filters for applications are evaluated at token issuance runtime, a common question is if apps are assigned at runtime or configuration time.

In this document, you create a custom attribute set, assign a custom security attribute to your application, and create a Conditional Access policy to secure the application.

Assign roles

Custom security attributes are security sensitive and can only be managed by delegated users. One or more of the following roles should be assigned to the users who manage or report on these attributes.

Expand table

Role name	Description
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.
Attribute Definition Administrator	Define and manage the definition of custom security attributes.
Attribute Definition Reader	Read the definition of custom security attributes.

Assign the appropriate role to the users who manage or report on these attributes at the directory scope. For detailed steps, see [Assign a role](#).

Important

By default, **Global Administrator** and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Create custom security attributes

Follow the instructions in the article, [Add or deactivate custom security attributes in Microsoft Entra ID](#) to add the following **Attribute set** and **New attributes**.

- Create an **Attribute set** named *ConditionalAccessTest*.
- Create **New attributes** named *policyRequirement* that **Allow multiple values to be assigned** and **Only allow predefined values to be assigned**. We add the following predefined values:
 - legacyAuthAllowed
 - blockGuestUsers
 - requireMFA
 - requireCompliantDevice
 - requireHybridJoinedDevice
 - requireCompliantApp

The screenshot shows the Microsoft Azure portal interface for creating a new attribute. The URL in the browser is https://portal.azure.com/#Microsoft_AAD_IAM_ca.appFil.... The page title is "policyRequirement - Microsoft A". The user is signed in as "BalaS@contoso.onmicrosoft.com (CONTOSO (CONTOSO.ONMICRO...))". The breadcrumb navigation shows: Home > Contoso | Custom security attributes (Preview) > ConditionalAccessTest | Active attributes > policyRequirement.

The form fields for the attribute "policyRequirement" are as follows:

- Attribute name: policyRequirement
- Description: (empty)
- Data type: String
- Allow multiple values to be assigned: Yes (radio button selected)
- Only allow predefined values to be assigned: Yes (radio button selected)
- Predefined values (table):

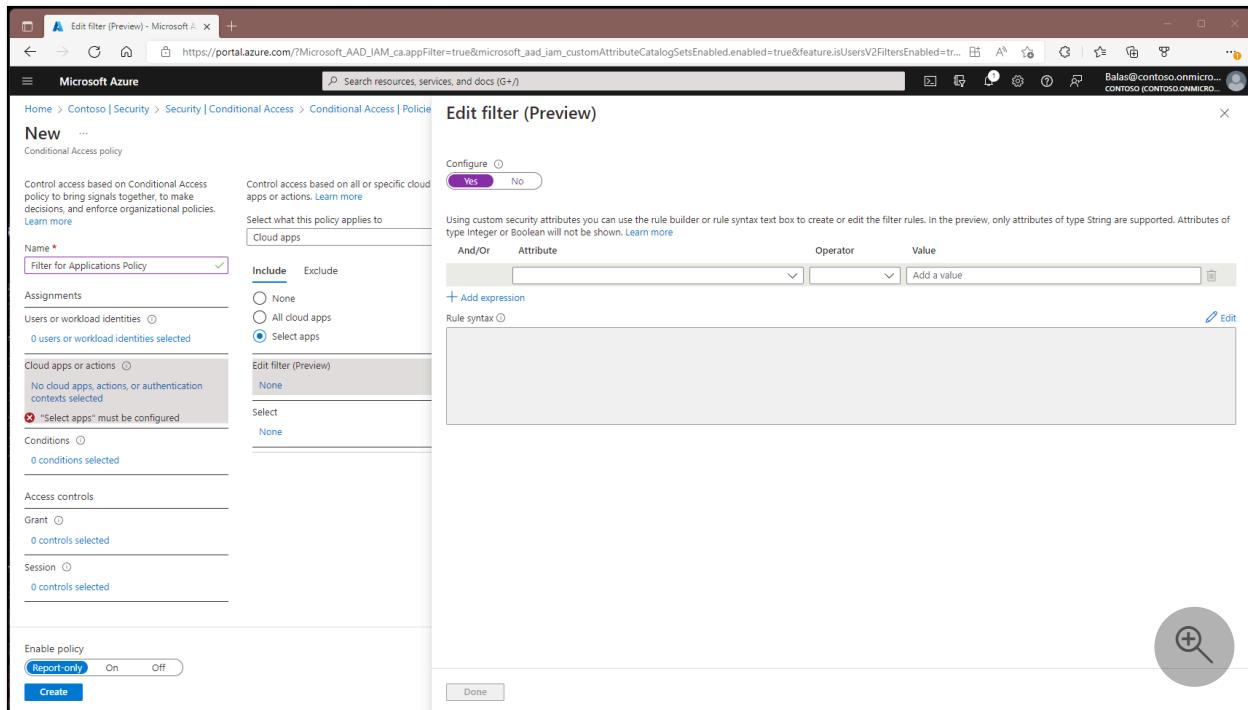
Value	Is active?
requireSAW	✓
requireCompliantApp	✓
requireHybridJoinedDevice	✓
requireCompliantDevice	✓
requireMFA	✓
blockGuestUsers	✓
legacyAuthAllowed	✓

At the bottom left is a "Save" button, and at the bottom right is a circular icon with a plus sign and a magnifying glass.

(!) Note

Conditional Access filters for applications only works with custom security attributes of type "string". Custom Security Attributes support creation of Boolean data type but Conditional Access Policy only supports "string".

Create a Conditional Access policy



1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator** and [Attribute Definition Reader](#).
2. Browse to **Protection > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - c. Select **Done**.
6. Under **Target resources**, select the following options:
 - a. Select what this policy applies to **Cloud apps**.
 - b. Include **Select resources**.
 - c. Select **Edit filter**.
 - d. Set **Configure** to **Yes**.

- e. Select the **Attribute** we created earlier called *policyRequirement*.
 - f. Set **Operator** to **Contains**.
 - g. Set **Value** to **requireMFA**.
 - h. Select **Done**.
7. Under **Access controls > Grant**, select **Grant access**, **Require multifactor authentication**, and select **Select**.
 8. Confirm your settings and set **Enable policy to Report-only**.
 9. Select **Create** to create to enable your policy.

After administrators confirm the settings using [report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Configure custom attributes

Step 1: Set up a sample application

If you already have a test application that makes use of a service principal, you can skip this step.

Set up a sample application that, demonstrates how a job or a Windows service can run with an application identity, instead of a user's identity. Follow the instructions in the article [Quickstart: Get a token and call the Microsoft Graph API by using a console app's identity](#) to create this application.

Step 2: Assign a custom security attribute to an application

When you don't have a service principal listed in your tenant, it can't be targeted. The Office 365 suite is an example of one such service principal.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator** (~/identity/role-based-access-control/permissions-reference.md#conditional-access-administrator) and **Attribute Assignment Administrator**.
2. Browse to **Identity > Applications > Enterprise applications**.
3. Select the service principal you want to apply a custom security attribute to.
4. Under **Manage > Custom security attributes**, select **Add assignment**.
5. Under **Attribute set**, select **ConditionalAccessTest**.
6. Under **Attribute name**, select **policyRequirement**.
7. Under **Assigned values**, select **Add values**, select **requireMFA** from the list, then select **Done**.

8. Select Save.

Step 3: Test the policy

Sign in as a user who the policy would apply to and test to see that MFA is required when accessing the application.

Other scenarios

- Blocking legacy authentication
- Blocking external access to applications
- Requiring compliant device or Intune app protection policies
- Enforcing sign in frequency controls for specific applications
- Requiring a privileged access workstation for specific applications
- Require session controls for high risk users and specific applications

Related content

[Conditional Access templates](#)

[Determine effect using Conditional Access report-only mode](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra Conditional Access: Token protection (Preview)

Article • 04/29/2025

Token protection (sometimes referred to as token binding in the industry) attempts to reduce attacks using token theft by ensuring a token is usable only from the intended device. When an attacker is able to steal a token, by hijacking or replay, they can impersonate their victim until the token expires or is revoked. Token theft is thought to be a relatively rare event, but the damage from it can be significant.

Token protection creates a cryptographically secure tie between the token and the device (client secret) it's issued to. Without the client secret, the bound token is useless. When a user registers a Windows 10 or newer device in Microsoft Entra ID, their primary identity is [bound to the device](#). What this means: A policy can ensure that only bound sign-in session (or refresh) tokens, otherwise known as Primary Refresh Tokens (PRTs) are used by applications when requesting access to a resource.

Important

Token protection is currently in public preview. For more information about previews, see [Universal License Terms For Online Services](#). With this preview, we're giving you the ability to create a Conditional Access policy to require token protection for sign-in tokens (refresh tokens) for specific services. We support token protection for sign-in tokens in Conditional Access for desktop applications accessing Exchange Online and SharePoint Online on Windows devices.

Important

The following changes have been made to Token Protection since the initial public preview release:

- **Sign In logs output:** The value of the string used in `enforcedSessionControls` and `sessionControlsNotSatisfied` changed from `Binding` to `SignInTokenProtection` in late June 2023. Queries on Sign In Log data should be updated to reflect this change.
- Devices that are joined to Microsoft Entra using certain methods are no longer supported. See the [known limitations section](#) for a complete list.
- Error code change: The Token protection Conditional Access policy error code is changing from 53003 to 530084 to better identify errors related to token protection.

- Token protection now supports the Windows App, extending protection to Windows 365 and Azure Virtual Desktop.

TESTING - Token Protection

Conditional Access policy

Delete View policy information View policy impact (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
TESTING - Token Protection

Assignments

Users or workload identities [\(i\)](#)
[Specific users included](#)

Target resources [\(i\)](#)
[2 resources included](#)

Network [\(NEW\)](#) [\(i\)](#)
[Not configured](#)

Conditions [\(i\)](#)
[2 conditions selected](#)

Access controls

Grant [\(i\)](#)
[0 controls selected](#)

Session [\(i\)](#)

Require token protection for sign-in sessions (Preview)

Enable policy
[Report-only](#) [On](#) [Off](#)

Save Select

Session

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions [\(i\)](#)
 Use Conditional Access App Control [\(i\)](#)
 Sign-in frequency [\(i\)](#)
 Persistent browser session [\(i\)](#)
 Customize continuous access evaluation
 Disable resilience defaults [\(i\)](#)
 Require token protection for sign-in sessions (Preview) [\(i\)](#)

Info The control "Require token protection for sign-in sessions" only works with supported devices and applications. Unsupported devices and client applications will be blocked. [Learn more](#)

Use Global Secure Access security profile [\(i\)](#)

Info This option only works with Global Secure Access resources.

Requirements

Using this feature requires Microsoft Entra ID P2 licenses. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID](#).

Note

Token protection enforcement is part of Microsoft Entra ID Protection and requires Microsoft Entra ID P2 licenses at general availability.

The following devices and applications support accessing resources on which a token protection Conditional Access policy is applied:

Supported devices:

- Windows 10 or newer devices that are Microsoft Entra joined, Microsoft Entra hybrid joined, or Microsoft Entra registered. See the [known limitations section](#) for unsupported device types.
- Windows Server 2019 or newer that are hybrid Microsoft Entra joined.

Supported applications:

- OneDrive sync client version 22.217 or newer
- Teams native client version 1.6.00.1331 or newer
- Power BI desktop version 2.117.841.0 (May 2023) or newer
- [Exchange PowerShell module version 3.7.0 or newer](#)
- Microsoft Graph PowerShell version 2.0.0 or newer with [EnableLoginByWAM option](#)
- Visual Studio 2022 or newer when using the 'Windows authentication broker' Sign-in option
- Windows App version 2.0.379.0 or newer

Known limitations

- Office perpetual clients aren't supported.
- The following applications don't support signing in using protected token flows and users are blocked when accessing Exchange and SharePoint:
 - PowerShell modules accessing SharePoint
 - PowerQuery extension for Excel
 - Extensions to Visual Studio Code which access Exchange or SharePoint
- The following Windows client devices aren't supported:
 - Surface Hub
 - Windows-based Microsoft Teams Rooms (MTR) systems
- [External users](#) who meet the token protection device registration requirements in their home tenant are supported. However, users who don't meet these requirements see an unclear error message with no indication of the root cause.

- Devices registered with Microsoft Entra ID using the following methods are unsupported:
 - Microsoft Entra joined [Azure Virtual Desktop session hosts](#).
 - Windows devices deployed using [bulk enrollment](#).
 - [Cloud PCs deployed by Windows 365](#) that are Microsoft Entra joined.
 - Power Automate hosted machine groups that are [Microsoft Entra joined](#).
 - Windows Autopilot devices deployed using [self-deploying mode](#).
 - Windows virtual machines deployed in Azure using the virtual machine (VM) extension that are enabled for [Microsoft Entra ID authentication](#).
- New [Microsoft Entra registered devices](#) on Windows versions before 24H2 might be blocked if users don't perform a fresh sign-in during registration. If blocked, users must re-register the device.

To identify the impacted devices due to unsupported registration types listed previously, inspect `tokenProtectionStatusDetails` attribute in the Sign-in logs. Token requests that are blocked due to an unsupported device registration type, can be identified with a `signInSessionStatusCode` value of 1003.

To prevent any disruption for new onboarding, you can modify the token protection Conditional Access policy by adding a device filter condition that excludes any devices that fall in the previously described deployment category. For example, to exclude:

- Cloud PCs that are Microsoft Entra joined, you can use `systemLabels -eq "CloudPC"` and `trustType -eq "AzureAD"`.
- Azure Virtual Desktops that are Microsoft Entra joined, you can use `systemLabels -eq "AzureVirtualDesktop"` and `trustType -eq "AzureAD"`.
- Power Automate hosted machine groups that are Microsoft Entra joined, you can use `systemLabels -eq "MicrosoftPowerAutomate"` and `trustType -eq "AzureAD"`.
- Windows virtual machines in Azure that are Microsoft Entra joined, you can use `systemLabels -eq "AzureResource"` and `trustType -eq "AzureAD"`.

Deployment

For users, the deployment of a Conditional Access policy to enforce token protection should be invisible when using compatible client platforms on registered devices and compatible applications.

To minimize the likelihood of user disruption due to app or device incompatibility, we highly recommend:

- Start with a pilot group of users, and expand over time.

- Create a Conditional Access policy in [report-only mode](#) before moving to enforcement of token protection.
- Capture both Interactive and Non-interactive sign in logs.
- Analyze these logs for long enough to cover normal application use.
- Add known good users to an enforcement policy.

This process helps to assess your users' client and app compatibility for token protection enforcement.

Create a Conditional Access policy

Users who perform specialized roles like those described in [Privileged access security levels](#) are possible targets for this functionality. We recommend piloting with a small subset to begin.

The steps that follow help create a Conditional Access policy to require token protection for Exchange Online and SharePoint Online on Windows devices.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Entra ID > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select the users or groups who are testing this policy.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**
 - a. Under **Select**, select the following applications supported by the preview:
 - i. Office 365 Exchange Online
 - ii. Office 365 SharePoint Online
 - iii. If you deployed Windows App in your environment, include:
 - i. Azure Virtual Desktop
 - ii. Windows 365
 - iii. Windows Cloud Login

Warning

Your Conditional Access policy should only be configured for these applications. Selecting the **Office 365** application group might result in unintended failures.

This change is an exception to the general rule that the **Office 365** application group should be selected in a Conditional Access policy.

b. Choose **Select**.

7. Under **Conditions**:

a. Under **Device platforms**:

i. Set **Configure** to **Yes**.

ii. **Include > Select device platforms > Windows**.

iii. Select **Done**.

b. Under **Client apps**:

i. Set **Configure** to **Yes**.

 **Warning**

Not configuring the **Client Apps** condition, or leaving **Browser** selected might cause applications that use MSAL.js, such as Teams Web to be blocked.

ii. Under Modern authentication clients, only select **Mobile apps and desktop clients**.

Leave other items unchecked.

iii. Select **Done**.

8. Under **Access controls > Session**, select **Require token protection for sign-in sessions** and select **Select**.

9. Confirm your settings and set **Enable policy** to **Report-only**.

10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Tip**

Since Conditional Access policies requiring token protection are currently only available for Windows devices, it's necessary to secure your environment against potential policy bypass when an attacker might appear to come from a different platform.

In addition, you should configure the following policies:

- [**Block access from unknown platforms**](#)
- [**Require device compliance for all known platforms**](#)

Capture logs and analyze

Monitor Conditional Access enforcement of token protection before and after enforcement using features like [Policy impact \(Preview\)](#), [Sign-in logs](#), or [Log Analytics](#).

Sign-in logs

Use Microsoft Entra sign-in log to verify the outcome of a token protection enforcement policy in report only mode or in enabled mode.

The screenshot shows the Microsoft Entra admin center Conditional Access Policy details page. The policy is named "TESTING - Token Protection" and is set to Enabled. The result of the policy enforcement is Failure. The policy has assignments for a user (Flip Schoonen) and a resource (Office 365 SharePoint Online), both of which matched. Under Conditions, the sign-in risk is None (Not configured), the device platform is Windows10 (Matched), the network location is Westerville, US (173.88.126.146) (Not configured), the client app is Browser (Matched), the device is Unknown (Not configured), and user risk is Not configured. In the Access controls section, under Session Controls, it shows "Not satisfied" with a note: "Require token protection for sign-in sessions (Preview)". A red box highlights this note.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Entra ID > Monitoring & health > Sign-in logs**.
3. Select a specific request to determine if the policy is applied or not.
4. Go to the **Conditional Access** or **Report-Only** pane depending on its state and select the name of your policy requiring token protection.
5. Under **Session Controls** check to see if the policy requirements were satisfied or not.
6. To find more details about the binding state of the request, select the pane **Basic Info** and see the field **Token Protection - Sign In Session**. Possible values are:

- a. Bound: the request was using bound protocols. Some sign-ins might include multiple requests, and all requests must be bound to satisfy the token protection policy. Even if an individual request appears to be bound, it doesn't ensure compliance with the policy if other requests are unbound. To see all requests for a sign-in, you can filter all requests for a specific user or look by correlationid.
- b. Unbound: the request wasn't using bound protocols. Possible `statusCodes` when request is unbound are:
- i. 1002: The request is unbound due to the lack of Microsoft Entra ID device state.
 - ii. 1003: The request is unbound because the Microsoft Entra ID device state doesn't satisfy Conditional Access policy requirements for token protection. This error could be due to an unsupported device registration type, or the device wasn't registered using fresh sign-in credentials.
 - iii. 1005: The request is unbound for other unspecified reasons.
 - iv. 1006: The request is unbound because the OS version is unsupported.
 - v. 1008: The request is unbound because the client isn't integrated with the platform broker, such as Windows Account Manager (WAM).

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Sign-in events' section with a 'User sign-ins (interactive)' tab selected. A date range selector shows 'Last 24 hours'. The main area displays activity details for a specific sign-in session. A red box highlights the 'Token Protection - Sign In Session' status, which is listed as 'Unbound (statusCode: 1002)'. Other visible details include Home tenant ID, Client app (Browser), Client credential type (Client assertion), Service principal ID, Original transfer method (None), Resource service principal ID, Unique token identifier, Token issuer type (Microsoft Entra ID), Token issuer name, Incoming token type (None), Authentication Protocol (None), Latency (67ms), Flagged for review (No), and User agent.

Activity Details: Sign-ins	
Home tenant ID	64376ee2-9871-401c-a9ab-1ce83eb7c486
Home tenant name	
Client app	Browser
Client credential type	Client assertion
Service principal ID	c4e6495d-cda3-4e2b-a10f-8c86dd75031d
Original transfer method	None
Token Protection - Sign In Session	Unbound (statusCode: 1002)
Service principal name	
Resource service principal ID	0ea27b70-01bf-446f-bcf9-0e34d0ec73d1
Unique token identifier	ueNINYcYM0GILnjUQRcOAA
Token issuer type	Microsoft Entra ID
Token issuer name	
Incoming token type	None
Authentication Protocol	None
Latency	67ms
Flagged for review	No
User agent	

Log Analytics

You can also use [Log Analytics](#) to query the sign-in logs (interactive and non-interactive) for blocked requests due to token protection enforcement failure.

Here's a sample Log Analytics query searching the non-interactive sign-in logs for the last seven days, highlighting **Blocked** versus **Allowed** requests by **Application**. These queries are only samples and are subject to change.

(!) Note

Sign In logs output: The value of the string used in "enforcedSessionControls" and "sessionControlsNotSatisfied" changed from "Binding" to "SignInTokenProtection" in late June 2023. Queries on Sign In Log data should be updated to reflect this change. The examples cover both values to include historical data.

Kusto

```
//Per Apps query
// Select the log you want to query (SigninLogs or AADNonInteractiveUserSignInLogs
)
//SigninLogs
AADNonInteractiveUserSignInLogs
// Adjust the time range below
| where TimeGenerated > ago(7d)
| project Id,ConditionalAccessPolicies, Status,UserPrincipalName, AppDisplayName,
ResourceDisplayName
| where ConditionalAccessPolicies != "[]"
| where ResourceDisplayName == "Office 365 Exchange Online" or ResourceDisplayName
=="Office 365 SharePoint Online" or ResourceDisplayName == "Azure Virtual Desktop"
or ResourceDisplayName == "Windows 365" or ResourceDisplayName == "Windows Cloud
Login"
| where ResourceDisplayName == "Office 365 Exchange Online" or ResourceDisplayName
=="Office 365 SharePoint Online"
//Add userPrincipalName if you want to filter
// | where UserPrincipalName ==<user_principal_Name>
| mv-expand todynamic(ConditionalAccessPolicies)
| where ConditionalAccessPolicies ["enforcedSessionControls"] contains
'["Binding"]' or ConditionalAccessPolicies ["enforcedSessionControls"] contains
'["SignInTokenProtection"]'
| where ConditionalAccessPolicies.result != "reportOnlyNotApplied" and
ConditionalAccessPolicies.result != "notApplied"
| extend SessionNotSatisfyResult =
ConditionalAccessPolicies["sessionControlsNotSatisfied"]
| extend Result = case (SessionNotSatisfyResult contains 'SignInTokenProtection'
or SessionNotSatisfyResult contains 'SignInTokenProtection', 'Block', 'Allow')
| summarize by Id,UserPrincipalName, AppDisplayName, Result
| summarize Requests = count(), Users = dcount(UserPrincipalName), Block =
countif(Result == "Block"), Allow = countif(Result == "Allow"), BlockedUsers =
dcountif(UserPrincipalName, Result == "Block") by AppDisplayName
| extend PctAllowed = round(100.0 * Allow/(Allow+Block), 2)
| sort by Requests desc
```

The result of the previous query should be similar to the following screenshot:

Results Chart

AppDisplayName	Requests	Users	Block	Allow	BlockedUsers	PctAllowed
> Microsoft Office	4,574	37	42	4,532	1	99.08
> Microsoft Edge	3,336	25	174	3,162	4	94.78
> Microsoft Application Command Service	1,603	31	0	1,603	0	100
> Graph Files Manager	1,423	22	0	1,423	0	100
> Microsoft Edge Enterprise New Tab Page	1,015	15	0	1,015	0	100
> Microsoft Bing Search for Microsoft Edge	969	15	0	969	0	100
> Universal Store Native Client	930	37	0	930	0	100
> Office UWP PWA	916	15	0	916	0	100
> Microsoft Authentication Broker	890	33	0	890	0	100
> OneDrive SyncEngine	651	7	0	651	0	100



The following query example looks at the non-interactive sign-in log for the last seven days, highlighting **Blocked** versus **Allowed** requests by **User**.

Kusto

```
//Per users query
// Select the log you want to query (SigninLogs or AADNonInteractiveUserSignInLogs
)
//SigninLogs
AADNonInteractiveUserSignInLogs
// Adjust the time range below
| where TimeGenerated > ago(7d)
| project Id,ConditionalAccessPolicies, UserPrincipalName, AppDisplayName,
ResourceDisplayName
| where ConditionalAccessPolicies != "[]"
| where ResourceDisplayName == "Office 365 Exchange Online" or ResourceDisplayName
=="Office 365 SharePoint Online" or ResourceDisplayName == "Azure Virtual Desktop"
or ResourceDisplayName == "Windows 365" or ResourceDisplayName == "Windows Cloud
Login"
| where ResourceDisplayName == "Office 365 Exchange Online" or ResourceDisplayName
=="Office 365 SharePoint Online"
//Add userPrincipalName if you want to filter
// | where UserPrincipalName ==<user_principal_Name>
| mv-expand todynamic(ConditionalAccessPolicies)
| where ConditionalAccessPolicies ["enforcedSessionControls"] contains
'["Binding"]' or ConditionalAccessPolicies ["enforcedSessionControls"] contains
'["SignInTokenProtection"]'
| where ConditionalAccessPolicies.result != "reportOnlyNotApplied" and
ConditionalAccessPolicies.result != "notApplied"
| extend SessionNotSatisfyResult =
ConditionalAccessPolicies.sessionControlsNotSatisfied
| extend Result = case (SessionNotSatisfyResult contains 'SignInTokenProtection'
or SessionNotSatisfyResult contains 'SignInTokenProtection', 'Block','Allow')
| summarize by Id, UserPrincipalName, AppDisplayName, ResourceDisplayName,Result
| summarize Requests = count(), Block = countif(Result == "Block"), Allow =
countif(Result == "Allow") by UserPrincipalName,
AppDisplayName,ResourceDisplayName
```

```
| extend PctAllowed = round(100.0 * Allow/(Allow+Block), 2)  
| sort by UserPrincipalName asc
```

The following query example looks at the non-interactive sign-in log for the last seven days, highlighting users that are using devices, where Microsoft Entra ID device state doesn't satisfy Token protection CA policy requirements.

Kusto

```
AADNonInteractiveUserSignInLogs  
// Adjust the time range below  
| where TimeGenerated > ago(7d)  
| where TokenProtectionStatusDetails != ""  
| extend parsedBindingDetails = parse_json(TokenProtectionStatusDetails)  
| extend bindingStatus = tostring(parsedBindingDetails["signInSessionStatus"])  
| extend bindingStatusCode =  
tostring(parsedBindingDetails["signInSessionStatusCode"])  
| where bindingStatusCode == 1003  
| summarize count() by UserPrincipalName
```

End user experience

A user that registered or enrolled their device doesn't experience any differences in the sign in experience on a token protection supported application when the token protection requirement is enabled.

A user that hasn't registered or enrolled their device, or when using an unsupported application when the token protection requirement is enabled will see the following screenshot after authenticating.



Register or enroll your device

To access this app, website, or service, you'll need to register or enroll your device. [Learn More](#)

Contact your admin if you run into issues.

[More details](#)

A user that isn't using a supported application when the token protection requirement is enabled will see the following screenshot after authenticating.



Sorry, a security policy is preventing access

An organization security policy requiring token protection is preventing this application from accessing the resource. You may be able to use a different application.

[More details](#)

[OK](#)

Related content

[What is a Primary Refresh Token?](#)

Conditional Access: Authentication flows

Article • 05/06/2025

Microsoft Entra ID supports various authentication and authorization flows to provide a seamless experience across all application and device types. Some authentication flows are higher risk than others. To give you more control over your security posture, Conditional Access lets you control certain authentication flows. This control begins with explicitly targeting [device code flow](#).

Device code flow

Device code flow lets you sign into devices that lack local input devices, like shared devices or digital signage. Device code flow is a high-risk authentication method that can be part of a phishing attack or used to access corporate resources on unmanaged devices. Configure device code flow control along with other controls in Conditional Access policies. For example, if device code flow is used for Android-based conference room devices, block device code flow everywhere except for Android devices in a specific network location.

Allow device code flow only where necessary. Microsoft recommends blocking device code flow wherever possible.

Authentication transfer

Authentication transfer is a flow that lets users seamlessly transfer authenticated state from one device to another. For example, users might see a QR code in the desktop version of Outlook that, when scanned on their mobile device, transfers their authenticated state to the mobile device. This capability provides a simple, intuitive experience that reduces friction for users.

Protocol tracking

To ensure Conditional Access policies are accurately enforced on specified authentication flows, we use functionality called protocol tracking. This tracking is applied to the session using device code flow or authentication transfer. In these cases, the sessions are considered protocol tracked. Any protocol tracked sessions are subject to policy enforcement if a policy exists. Protocol tracking state is sustained through subsequent refreshes. Nondevice code flow or authentication transfer flows can be subject to enforcement of authentication flows policies if the session is protocol tracked.

For example:

1. You configure a policy to block device code flow everywhere except for SharePoint.
2. You use device code flow to sign-in to SharePoint, as allowed by the configured policy. At this point, the session is considered protocol tracked
3. You try to sign in to Exchange within the context of the same session using any authentication flow not just device code flow.
4. You're blocked by the configured policy due to the protocol tracked state of the session

Sign-in logs

When configuring a policy to restrict or block device code flow, it's important to understand if and how device code flow is used in your organization. Creating a Conditional Access policy in report-only mode or filtering the sign-in logs for device code flow events with the **authentication protocol** filter can help.

To aid in troubleshooting protocol tracking related errors, we've added a new property called **original transfer method** to the **activity details** section of the Conditional Access **sign-in logs**. This property displays the protocol tracking state of the request in question. For example, for a session in which device code flow was performed previously the **original transfer method** is set to **Device code flow**.

Enforcement of Authentication Flows policies on Device Registration Service resource

Starting early September 2024, Microsoft began enforcing authentication flows policies on Device Registration Service. This applies only to policies which target **all resources** in the resource picker. If your organization currently uses Device Code Flow for device registration purposes, and you have an authentication flows policy targeting **all resources**, you need to exempt the Device Registration Resource from the scope of your Conditional Access policy to avoid impact. You can find the Device Registration Service resource in the [Target Resources](#) option present within the Conditional Access policy configuration experience. To exempt Device Registration Service via Conditional Access UX, you need to go to **Target Resources > Exclude > Select excluded cloud apps > Device Registration Service**. For API, you need to update your policy by excluding the Client ID for Device Registration Service: 01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9.

If you're unsure whether your organization uses Device Code Flow against Device Registration Service, you can utilize the Microsoft Entra [Sign-in logs](#) to check. There, you can filter for the Device Registration Service client ID in the **Resource ID** filter, and narrow it down to Device Code Flow usage by utilizing the **Device code** option within the **Authentication Protocol** filter.

Troubleshooting unexpected blocks

If you have a sign-in unexpectedly blocked by a Conditional Access policy, you should confirm whether the policy was an authentication flows policy. You can do this confirmation by going to **sign-in logs**, clicking on the blocked sign-in, and then navigating to the **Conditional Access** tab in the **Activity details: sign-ins** pane. If the policy enforced was an authentication flows policy, select the policy to determine which authentication flow was matched.

If device code flow was matched but device code flow wasn't the flow performed for that sign-in, the refresh token was protocol tracked. You can verify this case by clicking on the blocked sign-in and searching for the **Original transfer method** property in the **Basic info** portion of the **Activity details: sign-ins** pane.

 **Note**

Blocks due to protocol tracked sessions are expected behavior for this policy. There's no recommended remediation.

Related content

- [Block authentication flows with Conditional Access policy](#)
- [Conditional Access: Conditions](#)

Conditional Access: Authentication transfer (Preview)

Article • 03/05/2024

Authentication Transfer is a new authentication flow that simplifies the cross-device sign-in from PC to mobile for Microsoft apps. Authentication transfer allows you to transfer an authentication from one device to another, like desktop to mobile.

Authentication transfer increases user engagement by connecting them on more than one platform. Users can use a QR code in an authenticated app on their PC to sign-in to a mobile app.

The screenshot shows the Microsoft Entra admin center interface. On the left, a sidebar lists various administrative tasks. The main area displays a 'Conditional Access | Policies' page. A specific policy, 'Block authentication transfer', is selected. The right pane is titled 'Authentication flows' and contains configuration options. Under 'Transfer methods', the 'Authentication transfer' checkbox is checked and highlighted with a red box. In the 'Authentication flows (Preview)' section, 'Not configured' is listed. At the bottom right, there is a 'Save' button.

Authentication transfer and Conditional Access

During authentication transfer, all Microsoft Entra Conditional Access policies get evaluated. Authentication transfer only transfers authentication claims it doesn't transfer

device related claims.

- With authentication transfer, if users perform multifactor authentication (MFA) on their PC, they aren't required to perform MFA on their mobile device.
- With authentication transfer, Conditional Access policies get evaluated before transferring the authentication. If a policy isn't met for the mobile device, the user is prompted to sign in manually.
 - Authentication Transfer bypasses 3rd party mobile device management (MDM) solutions when transferring authentication to mobile devices.
- With authentication transfer, users must reauthenticate on mobile apps if they signed in with protected session tokens, like the Primary Refresh Token.

Authentication transfer in sign-in logs

Administrators can check the sign-in logs to see if their users are using authentication transfer to sign-in. Usage of authentication transfer appears under **Authentication Details** in the Microsoft Entra Sign-in logs. Administrators see events back to back, with the first being a QR code as the authentication method.

Manage authentication transfer for specific users and apps

Authentication transfer is enabled by default for all users. Administrators can manage authentication transfer using Conditional Access policies and the condition [authentication flows](#). This condition can restrict authentication transfer use to specific users, apps, or to turn off the functionality.

Authentication transfer checks all applicable Conditional Access policies before signing the user into a mobile app. If the required conditions aren't met, the user is prompted to authenticate on the mobile app.

To create a policy that uses the authentication transfer condition, see the article [Block authentication transfer with Conditional Access policy](#).

Related content

- [Block authentication transfer with Conditional Access policy](#)
- [Conditional Access: Conditions](#)

Conditional Access for workload identities

Article • 04/25/2025

Conditional Access policies historically applied only to users when they access apps and services like SharePoint Online. We're now extending support for Conditional Access policies to be applied to service principals owned by the organization. We call this capability Conditional Access for workload identities.

A [workload identity](#) is an identity that allows an application or service principal access to resources, sometimes in the context of a user. These workload identities differ from traditional user accounts as they:

- Can't perform multifactor authentication.
- Often have no formal lifecycle process.
- Need to store their credentials or secrets somewhere.

These differences make workload identities harder to manage and put them at higher risk for compromise.

Important

Workload Identities Premium licenses are required to create or modify Conditional Access policies scoped to service principals. In directories without appropriate licenses, existing Conditional Access policies for workload identities continue to function, but can't be modified. For more information, see [Microsoft Entra Workload ID](#).

Note

Policy can be applied to single tenant service principals that are registered in your tenant. Third party SaaS and multi-tenanted apps are out of scope. Managed identities aren't covered by policy. Managed identities could be included in an [access review](#) instead.

Conditional Access for workload identities enables blocking service principals:

- From outside of known public IP ranges.
- Based on risk detected by Microsoft Entra ID Protection.
- In combination with [authentication contexts](#).

Implementation

Create a location-based Conditional Access policy

Create a location based Conditional Access policy that applies to service principals.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Entra ID > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **What does this policy apply to?**, select **Workload identities**.
 - b. Under **Include**, choose **Select service principals**, and select the appropriate service principals from the list.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**. The policy applies only when a service principal requests a token.
7. Under **Conditions > Locations**, include **Any location** and exclude **Selected locations** where you want to allow access.
8. Under **Grant**, **Block access** is the only available option. Access is blocked when a token request is made from outside the allowed range.
9. Your policy can be saved in **Report-only** mode, allowing administrators to estimate the effects, or policy is enforced by turning policy **On**.
10. Select **Create** to complete your policy.

Create a risk-based Conditional Access policy

Create a risk-based Conditional Access policy that applies to service principals.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Favorites, Identity, Protection, Identity governance, Verified ID, Permissions Management, Global Secure Access (Preview), and Learn & support. The main content area is titled 'Conditional Access | Overview' and shows a 'New' policy being created. The policy name is 'Workload identity risk policy'. Under 'Assignments', 'Users' is selected, and 'Specific users included' is chosen. In the 'Target resources' section, 'All cloud apps' is selected. The 'Conditions' section is highlighted with a red box and shows '1 condition selected'. Under 'Access controls', 'Grant' is selected, and 'Block access' is listed. The 'Session' section shows '0 controls selected'. At the bottom, there's an 'Enable policy' row with three options: 'Report-only' (disabled), 'On' (selected and highlighted with a red box), and 'Off'. A 'Create' button is also present. A search bar and a magnifying glass icon are at the bottom right.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Entra ID > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **What does this policy apply to?**, select **Workload identities**.
 - b. Under **Include**, choose **Select service principals**, and select the appropriate service principals from the list.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**. The policy applies only when a service principal requests a token.
7. Under **Conditions > Service principal risk**
 - a. Set the **Configure** toggle to **Yes**.

- b. Select the levels of risk where you want this policy to trigger.
 - c. Select **Done**.
8. Under **Grant**, **Block access** is the only available option. Access is blocked when the specified risk levels are seen.
 9. Your policy can be saved in **Report-only** mode, allowing administrators to estimate the effects, or policy is enforced by turning policy **On**.
 10. Select **Create** to complete your policy.

Roll back

If you wish to roll back this feature, you can delete or disable any created policies.

Sign-in logs

The sign-in logs are used to review how policy is enforced for service principals or the expected affects of policy when using report-only mode.

1. Browse to **Entra ID > Monitoring & health > Sign-in logs > Service principal sign-ins**.
2. Select a log entry and choose the **Conditional Access** tab to view evaluation information.

Failure reason when Conditional Access blocks a Service Principal: "Access has been blocked due to Conditional Access policies."

Report-only mode

To view results of a location-based policy, go to the **Report-only** tab of events in the **Sign-in report**, or use the **Conditional Access Insights and Reporting** workbook.

To view results of a risk-based policy, refer to the **Report-only** tab of events in the **Sign-in report**.

Reference

Finding the objectID

You can get the objectID of the service principal from Microsoft Entra Enterprise Applications. The Object ID in Microsoft Entra App registrations can't be used. This identifier is the Object ID of the app registration, not of the service principal.

1. Browse to **Entra ID > Enterprise apps**, find the application you registered.

2. From the **Overview** tab, copy the **Object ID** of the application. This identifier is the unique to the service principal, used by Conditional Access policy to find the calling app.

Microsoft Graph

Sample JSON for location-based configuration using the Microsoft Graph beta endpoint.

JSON

```
{  
  "displayName": "Name",  
  "state": "enabled OR disabled OR enabledForReportingButNotEnforced",  
  "conditions": {  
    "applications": {  
      "includeApplications": [  
        "All"  
      ],  
      "clientApplications": {  
        "includeServicePrincipals": [  
          "[Service principal Object ID] OR ServicePrincipalsInMyTenant"  
        ],  
        "excludeServicePrincipals": [  
          "[Service principal Object ID]"  
        ]  
      },  
      "locations": {  
        "includeLocations": [  
          "All"  
        ],  
        "excludeLocations": [  
          "[Named location ID] OR AllTrusted"  
        ]  
      }  
    },  
    "grantControls": {  
      "operator": "and",  
      "builtInControls": [  
        "block"  
      ]  
    }  
  }  
}
```

Next steps

- [Using network location in a Conditional Access policy](#)
- [What is Conditional Access report-only mode?](#)

Continuous access evaluation

Article • 03/14/2024

Token expiration and refresh are a standard mechanism in the industry. When a client application like Outlook connects to a service like Exchange Online, the API requests are authorized using OAuth 2.0 access tokens. By default, access tokens are valid for one hour, when they expire the client is redirected to Microsoft Entra to refresh them. That refresh period provides an opportunity to reevaluate policies for user access. For example: we might choose not to refresh the token because of a Conditional Access policy, or because the user is disabled in the directory.

Customers express concerns about the lag between when conditions change for a user, and when policy changes are enforced. Microsoft experimented with the "blunt object" approach of reduced token lifetimes but found they degrade user experiences and reliability without eliminating risks.

Timely response to policy violations or security issues really requires a "conversation" between the token issuer Microsoft Entra, and the relying party (enlightened app). This two-way conversation gives us two important capabilities. The relying party can see when properties change, like network location, and tell the token issuer. It also gives the token issuer a way to tell the relying party to stop respecting tokens for a given user because of account compromise, disablement, or other concerns. The mechanism for this conversation is continuous access evaluation (CAE), an industry standard based on [Open ID Continuous Access Evaluation Profile \(CAEP\)](#). The goal for critical event evaluation is for response to be near real time, but latency of up to 15 minutes might be observed because of event propagation time; however, IP locations policy enforcement is instant.

The initial implementation of continuous access evaluation focuses on Exchange, Teams, and SharePoint Online.

To prepare your applications to use CAE, see [How to use Continuous Access Evaluation enabled APIs in your applications](#).

Key benefits

- User termination or password change/reset: User session revocation is enforced in near real time.
- Network location change: Conditional Access location policies are enforced in near real time.
- Token export to a machine outside of a trusted network can be prevented with Conditional Access location policies.

Scenarios

There are two scenarios that make up continuous access evaluation, critical event evaluation and Conditional Access policy evaluation.

Critical event evaluation

Continuous access evaluation is implemented by enabling services, like Exchange Online, SharePoint Online, and Teams, to subscribe to critical Microsoft Entra events. Those events can then be evaluated and enforced near real time. Critical event evaluation doesn't rely on Conditional Access policies so it's available in any tenant. The following events are currently evaluated:

- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Microsoft Entra ID Protection

This process enables the scenario where users lose access to organizational SharePoint Online files, email, calendar, or tasks, and Teams from Microsoft 365 client apps within minutes after a critical event.

 **Note**

SharePoint Online doesn't support user risk events.

Conditional Access policy evaluation

Exchange Online, SharePoint Online, Teams, and MS Graph can synchronize key Conditional Access policies for evaluation within the service itself.

This process enables the scenario where users lose access to files, email, calendar, or tasks from Microsoft 365 client apps or SharePoint Online immediately after network location changes.

 **Note**

Not all client app and resource provider combinations are supported. See the following tables. The first column of this table refers to web applications launched via web browser (i.e. PowerPoint launched in web browser) while the remaining four columns refer to native applications running on each platform described. Additionally, references to "Office" encompass Word, Excel, and PowerPoint.

 Expand table

	Outlook Web	Outlook Win32	Outlook iOS	Outlook Android	Outlook Mac
SharePoint Online	Supported	Supported	Supported	Supported	Supported
Exchange Online	Supported	Supported	Supported	Supported	Supported

 Expand table

	Office web apps	Office Win32 apps	Office for iOS	Office for Android	Office for Mac
SharePoint Online	Not Supported *	Supported	Supported	Supported	Supported
Exchange Online	Not Supported	Supported	Supported	Supported	Supported

 Expand table

	OneDrive web	OneDrive Win32	OneDrive iOS	OneDrive Android	OneDrive Mac
SharePoint Online	Supported	Not Supported	Supported	Supported	Not Supported

 Expand table

	Teams web	Teams Win32	Teams iOS	Teams Android	Teams Mac
Teams Service	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported
SharePoint Online	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported
Exchange Online	Partially supported	Partially supported	Partially supported	Partially supported	Partially supported

* Token lifetimes for Office web apps are reduced to 1 hour when a Conditional Access policy is set.

Note

Teams is made up of multiple services and among these the calls and chat services don't adhere to IP-based Conditional Access policies.

Continuous access evaluation is also available in Azure Government tenants (GCC High and DOD) for Exchange Online.

Client Capabilities

Client-side claim challenge

Before continuous access evaluation, clients would replay the access token from its cache as long as it wasn't expired. With CAE, we introduce a new case where a resource provider can reject a token when it isn't expired. To inform clients to bypass their cache even though the cached tokens

haven't expired, we introduce a mechanism called **claim challenge** to indicate that the token was rejected and a new access token need to be issued by Microsoft Entra. CAE requires a client update to understand claim challenge. The latest versions of the following applications support claim challenge:

 Expand table

	Web	Win32	iOS	Android	Mac
Outlook	Supported	Supported	Supported	Supported	Supported
Teams	Supported	Supported	Supported	Supported	Supported
Office	Not Supported	Supported	Supported	Supported	Supported
OneDrive	Supported	Supported	Supported	Supported	Supported

Token lifetime

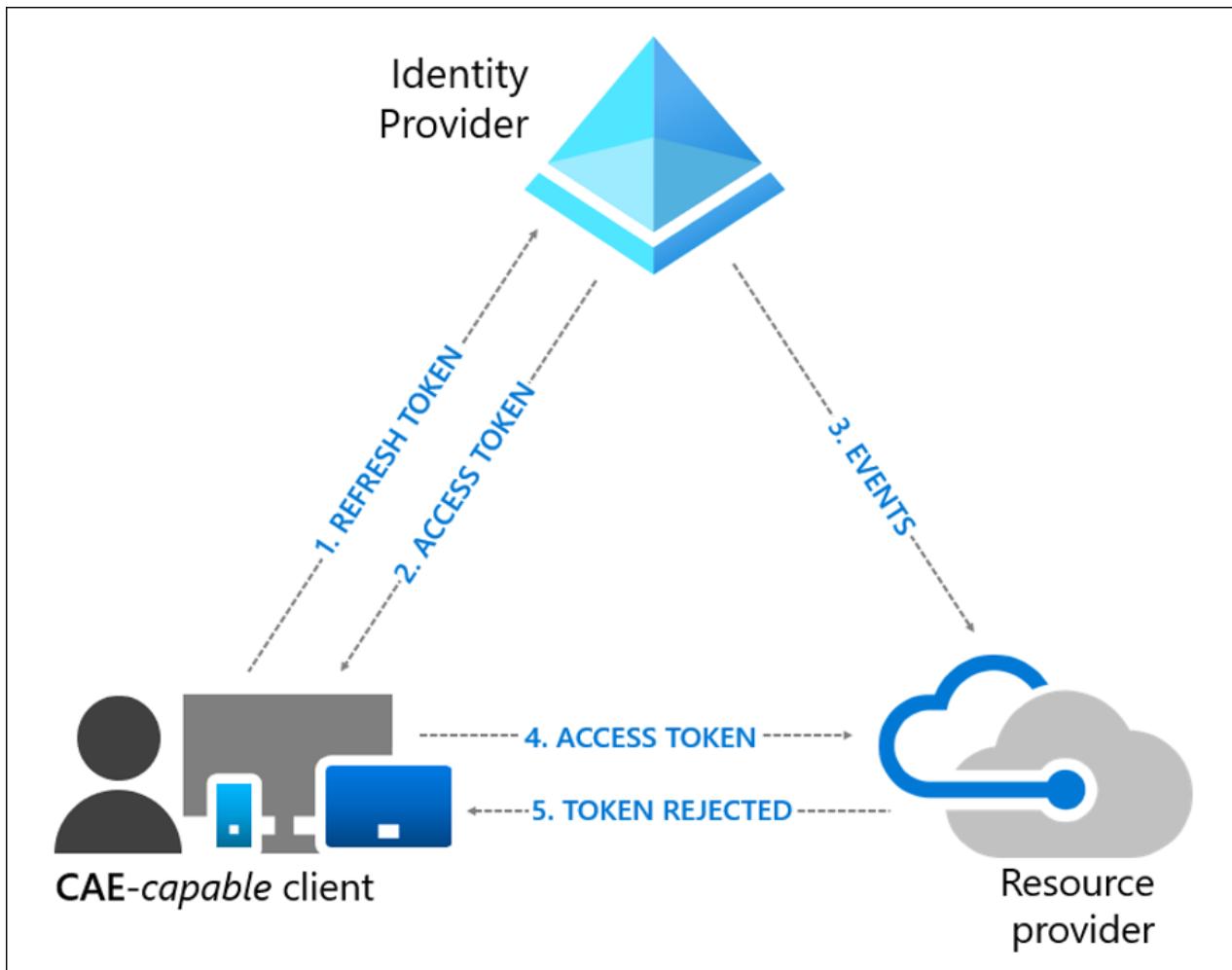
Because risk and policy are evaluated in real time, clients that negotiate continuous access evaluation aware sessions no longer rely on static access token lifetime policies. This change means that the configurable token lifetime policy isn't honored for clients negotiating CAE-aware sessions.

Token lifetime increases to long-lived, up to 28 hours, in CAE sessions. Critical events and policy evaluation drive revocation, not just an arbitrary time period. This change increases the stability of applications without affecting security posture.

If you aren't using CAE-capable clients, your default access token lifetime remains 1 hour. The default only changes if you configured your access token lifetime with the [Configurable Token Lifetime \(CTL\)](#) preview feature.

Example flow diagrams

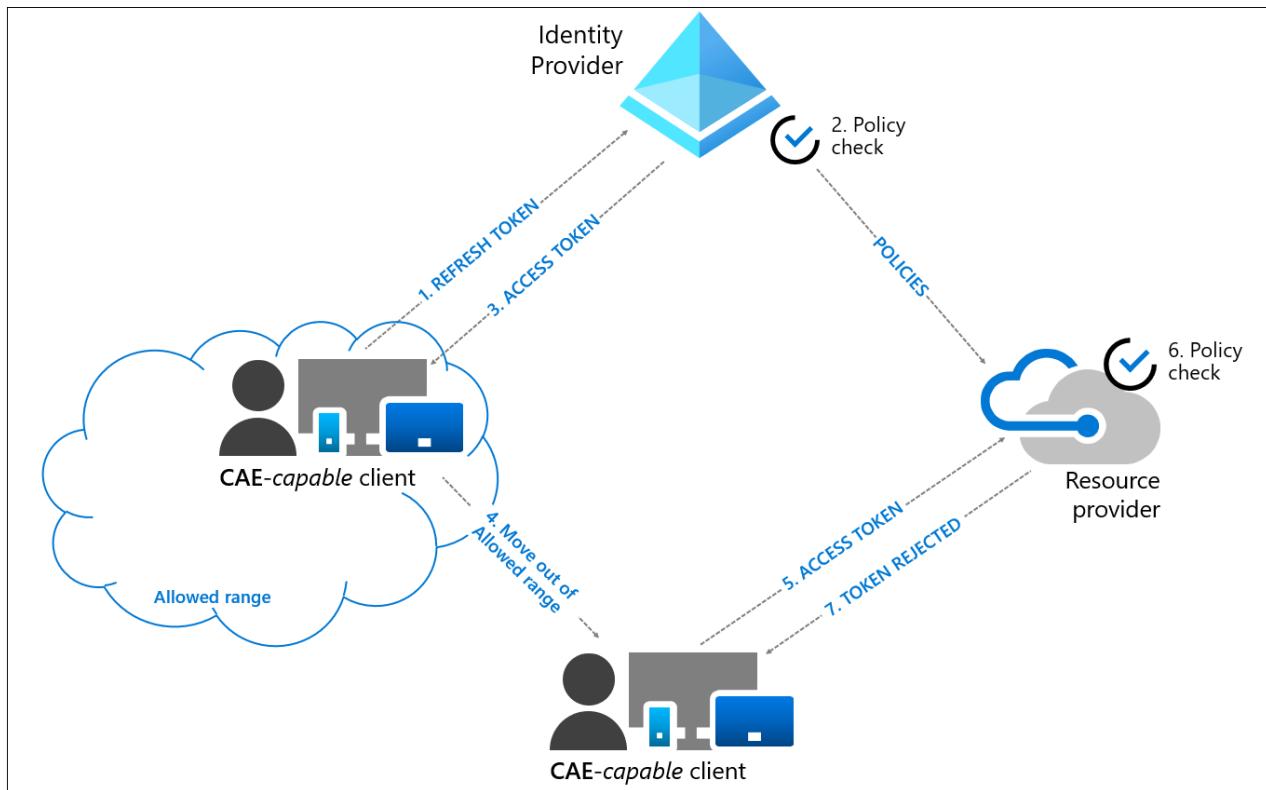
User revocation event flow



1. A CAE-capable client presents credentials or a refresh token to Microsoft Entra asking for an access token for some resource.
2. An access token is returned along with other artifacts to the client.
3. An Administrator explicitly [revokes all refresh tokens for the user](#), then a revocation event is sent to the resource provider from Microsoft Entra.
4. An access token is presented to the resource provider. The resource provider evaluates the validity of the token and checks whether there's any revocation event for the user. The resource provider uses this information to decide to grant access to the resource or not.
5. In this case, the resource provider denies access, and sends a 401+ claim challenge back to the client.
6. The CAE-capable client understands the 401+ claim challenge. It bypasses the caches and goes back to step 1, sending its refresh token along with the claim challenge back to Microsoft Entra. Microsoft Entra then reevaluates all the conditions and prompts the user to reauthenticate in this case.

User condition change flow

In the following example, a Conditional Access Administrator configured a location based Conditional Access policy to only allow access from specific IP ranges:



1. A CAE-capable client presents credentials or a refresh token to Microsoft Entra asking for an access token for some resource.
2. Microsoft Entra evaluates all Conditional Access policies to see whether the user and client meet the conditions.
3. An access token is returned along with other artifacts to the client.
4. User moves out of an allowed IP range.
5. The client presents an access token to the resource provider from outside of an allowed IP range.
6. The resource provider evaluates the validity of the token and checks the location policy synced from Microsoft Entra.
7. In this case, the resource provider denies access, and sends a 401+ claim challenge back to the client. The client is challenged because it isn't coming from an allowed IP range.
8. The CAE-capable client understands the 401+ claim challenge. It bypasses the caches and goes back to step 1, sending its refresh token along with the claim challenge back to Microsoft Entra. Microsoft Entra reevaluates all the conditions and denies access in this case.

Exception for IP address variations and how to turn off the exception

In step 8 above, when Microsoft Entra reevaluates the conditions, it denies access because the new location detected by Microsoft Entra is outside the allowed IP range. This isn't always the case. Due to [some complex network topologies](#), the authentication request can arrive from an allowed egress IP address even after the access request received by the resource provider arrived from an IP address that isn't allowed. Under these conditions, Microsoft Entra interprets that the client continues to be in an allowed location and should be granted access. Therefore, Microsoft Entra

issues a one-hour token that suspends IP address checks at the resource until token expiration. Microsoft Entra continues to enforce IP address checks.

If you're sending traffic to non-Microsoft 365 resources through Global Secure Access, resource providers aren't aware of the source IP address of the user as [source IP restoration](#) isn't currently supported for these resources. In this case, if the user is in the trusted IP location (as seen by Microsoft Entra), Microsoft Entra issues a one-hour token that suspends IP address checks at the resource until token expiration. Microsoft Entra continues to enforce IP address checks correctly for these resources.

Standard vs. Strict mode. The granting of access under this exception (that is, an allowed location detected between Microsoft Entra ID with a disallowed location detected by the resource provider) protects user productivity by maintaining access to critical resources. This is standard location enforcement. On the other hand, Administrators who operate under stable network topologies and wish remove this exception can use [Strict Location Enforcement \(Public Preview\)](#).

Enable or disable CAE

The CAE setting moved to Conditional Access. New CAE customers can access and toggle CAE directly when creating Conditional Access policies. However, some existing customers must go through migration before they can access CAE through Conditional Access.

Migration

Customers who configured CAE settings under Security before must migrate settings to a new Conditional Access policy.

The following table describes the migration experience of each customer group based on previously configured CAE settings.

[Expand table](#)

Existing CAE Setting	Is Migration Needed	Auto Enabled for CAE	Expected Migration Experience
New tenants that didn't configure anything in the old experience.	No	Yes	Old CAE setting is hidden given these customers likely didn't see the experience before general availability.
Tenants that explicitly enabled for all users with the old experience.	No	Yes	Old CAE setting is greyed out. Since these customers explicitly enabled this setting for all users, they don't need to migrate.
Tenants that explicitly enabled some users in	Yes	No	Old CAE settings are greyed out. Clicking Migrate launches the new Conditional Access policy wizard, which includes All users , while excluding users and

Existing CAE Setting	Is Migration Needed	Auto Enabled for CAE	Expected Migration Experience
their tenants with the old experience.			groups copied from CAE. It also sets the new Customize continuous access evaluation Session control to Disabled .
Tenants that explicitly disabled the preview.	Yes	No	Old CAE settings are greyed out. Clicking Migrate launches the new Conditional Access policy wizard, which includes All users , and sets the new Customize continuous access evaluation Session control to Disabled .

More information about continuous access evaluation as a session control can be found in the section, [Customize continuous access evaluation](#).

Limitations

Group membership and Policy update effective time

Changes made to Conditional Access policies and group membership made by administrators could take up to one day to be effective. The delay is from replication between Microsoft Entra and resource providers like Exchange Online and SharePoint Online. Some optimization has been done for policy updates, which reduce the delay to two hours. However, it doesn't cover all the scenarios yet.

When Conditional Access policy or group membership changes need to be applied to certain users immediately, you have two options.

- Run the [revoke-mgusersign PowerShell command](#) to revoke all refresh tokens of a specified user.
- Select "Revoke Session" on the user profile page to revoke the user's session to ensure that the updated policies are applied immediately.

IP address variation and networks with IP address shared or unknown egress IPs

Modern networks often optimize connectivity and network paths for applications differently. This optimization frequently causes variations of the routing and source IP addresses of connections, as seen by your identity provider and resource providers. You might observe this split path or IP address variation in multiple network topologies, including, but not limited to:

- On-premises and cloud-based proxies.
- Virtual private network (VPN) implementations, like [split tunneling](#).
- Software defined wide area network (SD-WAN) deployments.
- Load balanced or redundant network egress network topologies, like those using [SNAT](#).
- Branch office deployments that allow direct internet connectivity for specific applications.

- Networks that support IPv6 clients.
- Other topologies, which handle application or resource traffic differently from traffic to the identity provider.

In addition to IP variations, customers also might employ network solutions and services that:

- Use IP addresses that might be shared with other customers. For example, cloud-based proxy services where egress IP addresses are shared between customers.
- Use easily varied or undefinable IP addresses. For example, topologies where there are large, dynamic sets of egress IP addresses used, like large enterprise scenarios or [split VPN](#) and local egress network traffic.

Networks where egress IP addresses might change frequently or are shared might affect Microsoft Entra Conditional Access and Continues Access Evaluation (CAE). This variability can affect how these features work and their recommended configurations. Split Tunneling might also cause unexpected blocks when an environment is configured using [Split Tunneling VPN Best Practices](#). Routing [Optimized IPs](#) through a Trusted IP/VPN might be required to prevent blocks related to *insufficient_claims* or *Instant IP Enforcement check failed*.

The following table summarizes Conditional Access and CAE feature behaviors and recommendations for different types of network deployments and resource providers (RP):

[\[+\] Expand table](#)

Network Type	Example	IPs seen by Microsoft	IPs seen by RP	Applicable Conditional Access Configuration (Trusted Named Location)	CAE enforcement	CAE access token	Recommendations
1. Egress IPs are dedicated and enumerable for both Microsoft Entra and all RP traffic	All to network traffic to Microsoft Entra and RPs egresses through 1.1.1.1 and/or 2.2.2.2	1.1.1.1	2.2.2.2	1.1.1.1 2.2.2.2	Critical Events IP location Changes	Long lived – up to 28 hours	If Conditional Access Named Locations are defined, ensure that they contain all possible egress IPs (seen by Microsoft Entra and all RP)
2. Egress IPs are dedicated and enumerable for Microsoft Entra, but not for RP traffic	Network traffic to Microsoft Entra egresses through 1.1.1.1. RP traffic	1.1.1.1	x.x.x.x	1.1.1.1	Critical Events	Default access token lifetime – 1 hour	Don't add non dedicated or nonenumerable egress IPs (x.x.x.x) into Trusted Named Location Conditional Access

Network Type	Example	IPs seen by Microsoft Entra	IPs seen by RP	Applicable Conditional Access Configuration (Trusted Named Location)	CAE enforcement	CAE access token	Recommendations
	egresses through x.x.x.x						rules as it can weaken security
3. Egress IPs are non-dedicated/shared or not enumerable for both Microsoft Entra and RP traffic	Network traffic to Microsoft Entra egresses through y.y.y. RP traffic egresses through x.x.x.x	y.y.y.y	x.x.x.x	N/A -no IP Conditional Access policies/Trusted Locations are configured	Critical Events	Long lived – up to 28 hours	Don't add non dedicated or nonenumerable egress IPs (x.x.x.x/y.y.y.y) into Trusted Named Location Conditional Access rules as it can weaken security

Networks and network services used by clients connecting to identity and resource providers continue to evolve and change in response to modern trends. These changes might affect Conditional Access and CAE configurations that rely on the underlying IP addresses. When deciding on these configurations, factor in future changes in technology and upkeep of the defined list of addresses in your plan.

Supported location policies

CAE only has insight into [IP-based named locations](#). CAE doesn't have insight into other location conditions like [MFA trusted IPs](#) or country/region-based locations. When a user comes from an MFA trusted IP, trusted location that includes MFA Trusted IPs, or country/region location, CAE won't be enforced after that user moves to a different location. In those cases, Microsoft Entra issues a one-hour access token without instant IP enforcement check.

i Important

If you want your location policies to be enforced in real time by continuous access evaluation, use only the [IP based Conditional Access location condition](#) and configure all IP addresses, **including both IPv4 and IPv6**, that can be seen by your identity provider and resources provider. Do not use country/region location conditions or the trusted ips feature that is available in Microsoft Entra multifactor authentication's service settings page.

Named location limitations

When the sum of all IP ranges specified in location policies exceeds 5,000, CAE can't enforce user change location flow in real time. In this case, Microsoft Entra issues a one-hour CAE token. CAE continues enforcing [all other events and policies](#) besides client location change events. With this change, you still maintain stronger security posture compared to traditional one-hour tokens, since [other events](#) are still evaluated in near real time.

Office and Web Account Manager settings

[\[+\] Expand table](#)

Office update channel	DisableADALatopWAMOverride	DisableAADWAM
Semi-Annual Enterprise Channel	If set to enabled or 1, CAE isn't supported.	If set to enabled or 1, CAE isn't supported.
Current Channel or Monthly Enterprise Channel	CAE is supported whatever the setting	CAE is supported whatever the setting

For an explanation of the office update channels, see [Overview of update channels for Microsoft 365 Apps](#). The recommendation is that organizations don't disable Web Account Manager (WAM).

Coauthoring in Office apps

When multiple users are collaborating on a document at the same time, CAE might not revoke their access to the document immediately based on policy change events. In this case, the user loses access completely after:

- Closing the document
- Closing the Office app
- After 1 hour when a Conditional Access IP policy is set

To further reduce this time, a SharePoint Administrator can reduce the maximum lifetime of coauthoring sessions for documents stored in SharePoint Online and Microsoft OneDrive, by [configuring a network location policy](#). Once this configuration is changed, the maximum lifetime of coauthoring sessions is reduced to 15 minutes, and can be adjusted further using the SharePoint Online PowerShell command [Set-SPOTenant -IPAddressWACTokenLifetime](#).

Enable after a user is disabled

If you enable a user right after disabling, there's some latency before the account is recognized as enabled in downstream Microsoft services.

- SharePoint Online and Teams typically have a 15-minute delay.
- Exchange Online typically has a 35-40 minute delay.

Push notifications

An IP address policy isn't evaluated before push notifications are released. This scenario exists because push notifications are outbound and don't have an associated IP address to be evaluated against. If a user selects that push notification, for example an email in Outlook, CAE IP address policies are still enforced before the email can display. Push notifications display a message preview, which isn't protected by an IP address policy. All other CAE checks are done before the push notification being sent. If a user or device has its access removed, enforcement occurs within the documented period.

Guest users

CAE doesn't support Guest user accounts. CAE revocation events and IP based Conditional Access policies aren't enforced instantaneously.

CAE and Sign-in Frequency

Sign-in Frequency is honored with or without CAE.

Related content

- [How to use Continuous Access Evaluation enabled APIs in your applications](#)
- [Claims challenges, claims requests, and client capabilities](#)
- [Conditional Access: Session](#)
- [Monitor and troubleshoot continuous access evaluation](#)

Strictly enforce location policies using continuous access evaluation (preview)

Article • 03/15/2024

Strictly enforce location policies is a new enforcement mode for continuous access evaluation (CAE), used in Conditional Access policies. This new mode provides protection for resources, immediately stopping access if the IP address detected by the resource provider isn't allowed by Conditional Access policy. This option is the highest security modality of CAE location enforcement, and requires that administrators understand the routing of authentication and access requests in their network environment. See our [Introduction to continuous access evaluation](#) for a review of how CAE-capable clients and resource providers, like the Outlook email client and Exchange Online evaluate location changes.

[+] Expand table

Location enforcement mode	Recommended network topology	If the IP address detected by the Resource isn't in the allowed list	Benefits	Configuration
Standard (Default)	Suitable for all topologies	A short-lived token is issued only if Microsoft Entra ID detects an allowed IP address. Otherwise, access is blocked	Falls back to the pre-CAE location detection mode in split tunnel network deployments where CAE enforcement would affect productivity. CAE still enforces other events and policies.	None (Default Setting)
Strictly enforced location policies	Egress IP addresses are dedicated and enumerable for both Microsoft Entra ID and all resource provider traffic	Access blocked	Most secure, but requires well understood network paths	<ol style="list-style-type: none">1. Test IP address assumptions with a small population2. Enable "Strictly enforce" under Session controls

Configure strictly enforced location policies

Step 1 - Configure a Conditional Access location based policy for your target users

Before administrators create a Conditional Access policy requiring strict location enforcement, they must be comfortable using policies like the one described in [Conditional Access location based policies](#). Policies like this one should be tested with a subset of users before proceeding to the next step. Administrators can avoid discrepancies between the allowed and actual IP addresses seen by Microsoft Entra ID during authentication, by testing before enabling strict enforcement.

Step 2 - Test policy on a small subset of users

The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The left sidebar shows 'New' and 'Conditional Access policy'. The main area has sections for 'Name' (Strict location enforcement policy), 'Assignments' (All users included and specific users excluded), 'Target resources' (2 apps included), 'Conditions' (1 condition selected), 'Access controls' (Grant, Block access), and 'Session' (Use continuous access evaluation - Strict location). The 'Session' section is highlighted with a red box. On the right, there's a 'Session' configuration panel with options like 'Use app enforced restrictions', 'Use Conditional Access App Control', 'Sign-in frequency', 'Persistent browser session', and 'Customize continuous access evaluation' (which is checked and highlighted with a red box). Under 'Customize continuous access evaluation', there are radio buttons for 'Disable' and 'Strictly enforce location policies (Preview)', with 'Strictly enforce location policies' selected. Other options in this panel include 'See list of supported clients and resource providers', 'Disable resilience defaults', and 'Require token protection for sign-in sessions (Preview)'. At the bottom, there are 'Enable policy' (On/Off switch) and 'Create' buttons.

After enabling policies requiring strict location enforcement on a subset of test users, validate your testing experience using the filter **IP address (seen by resource)** in the Microsoft Entra sign-in logs. This validation allows administrators to find scenarios

where strict location enforcement might block users with an unallowed IP seen by the CAE-enabled resource provider.

Before administrators turn on Conditional Access policies requiring strict location enforcement, they should:

- Ensure all authentication traffic towards Microsoft Entra ID and access traffic to resource providers are from dedicated egress IPs that are known.
 - Like Exchange Online, Teams, SharePoint Online, and Microsoft Graph
- Ensure that all IP addresses from which their users can access Microsoft Entra ID and resource providers are included in their [IP-based named locations](#).
- Ensure that they aren't sending traffic to non-Microsoft 365 applications through Global Secure Access.
 - [Source IP restoration](#) isn't supported for these non-Microsoft 365 applications. Enabling strict location enforcement with Global Secure Access blocks access even if the user is in a trusted IP location.
- Review their Conditional Access policies to ensure that they don't have any policies that don't support CAE. For more information, see [CAE-supported CA policies](#).

If administrators don't perform this validation, their users might be negatively impacted. If traffic to Microsoft Entra ID or a CAE supported resource is through a shared or undefinable egress IP, don't enable strict location enforcement in your Conditional Access policies.

Step 3 - Use the CAE Workbook to Identify IP addresses that should be added to your named locations

If you haven't already, create a new Azure Workbook using the public template "Continuous Access Evaluation Insights" to identify IP mismatch between IP address seen by Microsoft Entra ID and **IP address (seen by resource)**. In this case, you might have a split-tunnel network configuration. To ensure your users aren't accidentally locked out when strict location enforcement is enabled, administrators should:

- Investigate and identify any IP addresses identified in the CAE Workbook.
- Add public IP addresses associated with known organizational egress points to their defined [named locations](#).

The screenshot shows the Azure Active Directory Workbooks interface. On the left, there's a navigation pane with options like 'Cross-tenant synchronization', 'Azure AD Connect', 'Custom domain names', 'Mobility (MDM and MAM)', 'Password reset', 'Company branding', 'User settings', 'Properties', and 'Security'. Below that is a 'Monitoring' section with 'Sign-in logs', 'Audit logs', 'Provisioning logs', 'Health (Preview)', 'Log Analytics', 'Diagnostic settings', and 'Workbooks' (which is selected). Other sections include 'Usage & Insights', 'Bulk operation results (Preview)', 'Troubleshooting + Support', and 'New support request'. The main content area is titled 'Continuous access evaluation token insights' and contains a sub-section 'IP address mismatch CAE per Sign-in'. It says, 'The continuous access evaluation (CAE) workbook allows administrators to monitor CAE usage insights for their tenants.' A red box highlights a table showing 'Potential IP address mismatch between Azure AD & resource provider'. The table has two columns: 'Total sign-ins' (4.34k) and 'Mismatched IPs sign-ins' (12). Below this is another table titled 'IP address mismatch seen by Azure AD and resource provider', also with a red box around it. This table lists sign-ins from Anna Traver and Tenney Bartenfelder, showing details like Request DateTime, RequestId, Is CAE Tok..., IP seen by Azure AD, and IP seen by Resource.

The following screenshot shows an example of a client's access to a resource being blocked. This block is due to policies requiring CAE strict location enforcement being triggered revoking the client's session.

The screenshot shows a Microsoft sign-in error page. At the top is the Microsoft logo and the email address annatraver@woodgrove.ms. The main message is 'You cannot access this right now'. Below it, a text block says: 'Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.' At the bottom, there are two links: 'Sign out and sign in with a different account' and 'More details'.

This behavior can be verified in the sign-in logs. Look for **IP address (seen by resource)** and investigate adding this IP to **named locations** if experiencing unexpected blocks from Conditional Access on users.

Activity Details: Sign-ins

X

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Location	Quincy, Washington, US					
IP address	51.143.90.94					
IP address (seen by resource)	73.193.97.10					
Autonomous system number	8075					
Named location type	Location name					
Named location	United States Office Locatoins - GPS					
Named location	Woodgrove NOAM					
Named location	ProsAllow					
Named location	Praveen Strict Locations					

Looking at the **Conditional Access Policy details** tab provides more details of blocked sign-in events.

Conditional Access Policy details

X

↑ Previous ↓ Next

Policy: Strict Location CA Policy
Policy state: Enabled
Result: Failure

Assignments

User

Anna Traver ✓ Matched



Application

Office 365 Exchange Online ✓ Matched



Conditions

Sign-in risk

None ● Not configured

Device platform

Windows 10 ● Not configured

Location

Quincy, US ✓ Matched

Location included



IP seen by Azure AD
51.143.90.94 ✗ Not matched

IP seen by resource provider

73.193.97.10 ✓ Matched

Client app

Browser ● Not configured

Device

Unknown ● Not configured

User risk

● Not configured

Access controls

Grant Controls

✗ Block

Block



Session Controls

✓ Enforced

ContinuousAccessEvaluation



Step 4 - Continue deployment

Repeat steps 2 and 3 with expanding groups of users until Strictly Enforce Location Policies are applied across your target user base. Roll out carefully to avoid impacting user experience.

Troubleshooting with Sign-in logs

Administrators can investigate the Sign-in logs to find cases with IP address (seen by resource).

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Global Reader**.
 2. Browse to **Identity > Monitoring & health > Sign-in logs**.
 3. Find events to review by adding filters and columns to filter out unnecessary information.
- a. Add the **IP address (seen by resource)** column and filter out any blank items to narrow the scope. The **IP address (seen by resource)** is blank when that IP seen by Microsoft Entra ID matches the IP address seen by the resource.

Date	Request ID	User	Application	IP address	Conditional Access	IP address (seen by resource)
6/14/2023, 10:37:59 PM	855f667a-1a26...	Anna Traver	Office 365 Exchange Online	51.143.90.94	Failure	73.193.97.10
6/14/2023, 10:33:23 PM	cbbfb826a-071d...	Anna Traver	Office 365 Exchange Online	51.143.90.94	Failure	73.193.97.10
6/14/2023, 10:33:21 PM	8b343e26-ca70...	Anna Traver	Office 365 Exchange Online	51.143.90.94	Success	73.193.97.10

IP address (seen by resource) contains filter isn't empty in the following examples:

Initial authentication

1. Authentication succeeds using a CAE token.

Status	Success
Continuous access evaluation	Yes
Additional Details	MFA requirement satisfied by claim in the token

2. The **IP address (seen by resource)** is different from the IP address seen by Microsoft Entra ID. Although the IP address seen by the resource is known, there's no enforcement until the resource redirects the user for reevaluation of the IP address seen by the resource.

Activity Details: Sign-ins

X

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Location	Quincy, Washington, US					
IP address	51.143.90.94					
IP address (seen by resource)	73.193.97.10					
Autonomous system number	8075					
Named location type	Location name					
Named location	United States Office Locatoins - GPS					
Named location	Woodgrove NOAM					
Named location	ProsAllow					
Named location	Praveen Strict Locations					

3. Microsoft Entra authentication is successful because strict location enforcement isn't applied at the resource level.

Conditional Access Policy details

X

↑ Previous	Next ↓
Policy: Strict Location CA Policy Policy state: Enabled Result: Not Applied	
Assignments	
User Anna Traver ✓ Matched	
Application Office 365 Exchange Online ✓ Matched	
Conditions	
Sign-in risk None ● Not configured	
Device platform Windows 10 ● Not configured	
Location Quincy, US ✗ Not matched Location excluded	
IP seen by Azure AD 51.143.90.94 ✗ Not matched	
IP seen by resource provider 73.193.97.10 ● Not configured	
Client app Browser ● Not configured	
Device Unknown ● Not evaluated	
User risk Not configured	

Resource redirect for reevaluation

1. Authentication fails and a CAE token isn't issued.

Activity Details: Sign-ins

X

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Date	6/14/2023, 10:33:23 PM					
Request ID	cbfb826a-071d-484b-a0fd-726424ca0700					
Correlation ID	e210e228-cb8c-9f5f-5c64-51264636a86f					
Authentication requirement	Multifactor authentication					
Status	Failure					
Continuous access evaluation	No					
Sign-in error code	53003					
Failure reason	Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.					
Additional Details	If this is unexpected, see the conditional access policy that applied to this request in the Azure Portal.					

2. IP address (seen by resource) is different from the IP seen by Microsoft Entra ID.

Activity Details: Sign-ins

X

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	...
Location	Quincy, Washington, US					
IP address	51.143.90.94					
IP address (seen by resource)	73.193.97.10					
Autonomous system number	8075					
Named location type	Location name					
Named location	United States Office Locatoins - GPS					
Named location	Woodgrove NOAM					
Named location	ProsAllow					
Named location	Praveen Strict Locations					

3. Authentication isn't successful because IP address (seen by resource) isn't a known named location in Conditional Access.

Conditional Access Policy details

X

↑ Previous ↓ Next

Policy: Strict Location CA Policy
Policy state: Enabled
Result: Failure

Assignments

User

Anna Traver ✓ Matched



Application

Office 365 Exchange Online ✓ Matched



Conditions

Sign-in risk

None ● Not configured

Device platform

Windows 10 ● Not configured

Location

Quincy, US ✓ Matched

Location included



IP seen by Azure AD
51.143.90.94 ✗ Not matched

IP seen by resource provider
73.193.97.10 ✓ Matched

Client app

Browser ● Not configured

Device

Unknown ● Not configured

User risk

● Not configured

Access controls

Grant Controls

✗ Block

Block



Session Controls

✓ Enforced

ContinuousAccessEvaluation



Related content

- Continuous access evaluation in Microsoft Entra ID
- Claims challenges, claims requests, and client capabilities
- How to use continuous access evaluation enabled APIs in your applications
- Monitor and troubleshoot sign-ins with continuous access evaluation

Continuous access evaluation for workload identities

Article • 02/27/2024

Continuous access evaluation (CAE) for [workload identities](#) provides security benefits to your organization. It enables real-time enforcement of Conditional Access location and risk policies along with instant enforcement of token revocation events for workload identities.

Continuous access evaluation doesn't currently support managed identities.

Scope of support

Continuous access evaluation for workload identities is supported only on access requests sent to Microsoft Graph as a resource provider. More resource providers will be added over time.

Service principals for line of business (LOB) applications are supported.

We support the following revocation events:

- Service principal disable
- Service principal delete
- High service principal risk as detected by Microsoft Entra ID Protection

Continuous access evaluation for workload identities supports [Conditional Access policies that target location and risk](#).

Enable your application

Developers can opt in to Continuous access evaluation for workload identities when their API requests `xms_cc` as an optional claim. The `xms_cc` claim with a value of `cp1` in the access token is the authoritative way to identify a client application is capable of handling a claims challenge. For more information about how to make this work in your application, see the article, [Claims challenges, claims requests, and client capabilities](#).

Disable

In order to opt out, don't send the `xms_cc` claim with a value of `cp1`.

Organizations who have Microsoft Entra ID P1 or P2 can create a [Conditional Access policy to disable continuous access evaluation](#) applied to specific workload identities as an immediate stop-gap measure.

Troubleshooting

When a client's access to a resource is blocked due to CAE being triggered, the client's session is revoked, and the client needs to reauthenticate. This behavior can be verified in the sign-in logs.

The following steps detail how an admin can verify sign in activity in the sign-in logs:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs > Service Principal Sign-ins**. You can use filters to ease the debugging process.
3. To see activity details, select an entry. The **Continuous access evaluation** field indicates whether a CAE token was issued in a particular sign-in attempt.

Related content

- [Register an application with Microsoft Entra ID and create a service principal](#)
- [How to use Continuous Access Evaluation enabled APIs in your applications](#)
- [Sample application using continuous access evaluation](#)
- [Securing workload identities with Microsoft Entra ID Protection](#)
- [What is continuous access evaluation?](#)

Conditional Access adaptive session lifetime policies

Article • 03/03/2025

Conditional Access adaptive session lifetime policies help organizations restrict authentication sessions in complex deployments. Scenarios include:

- Resource access from an unmanaged or shared device
- Access to sensitive information from an external network
- High impact users
- Critical business applications

Conditional Access provides adaptive session lifetime policy controls, letting you create policies that target specific use cases within your organization without affecting all users.

Before diving into details on how to configure the policy, let's examine the default configuration.

User 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.

The Microsoft Entra ID default configuration for user sign-in frequency is a rolling window of 90 days. Asking users for credentials often seems sensible, but it can backfire. Users trained to enter their credentials without thinking can unintentionally supply them to a malicious credential prompt.

It might sound alarming to not ask a user to sign back in, but any violation of IT policy revokes the session. Some examples include (but aren't limited to) a password change, a noncompliant device, or account disable. You can also explicitly [revoke users' sessions using Microsoft Graph PowerShell](#). The Microsoft Entra ID default configuration comes down to "don't ask users to provide their credentials if security posture of their sessions didn't change."

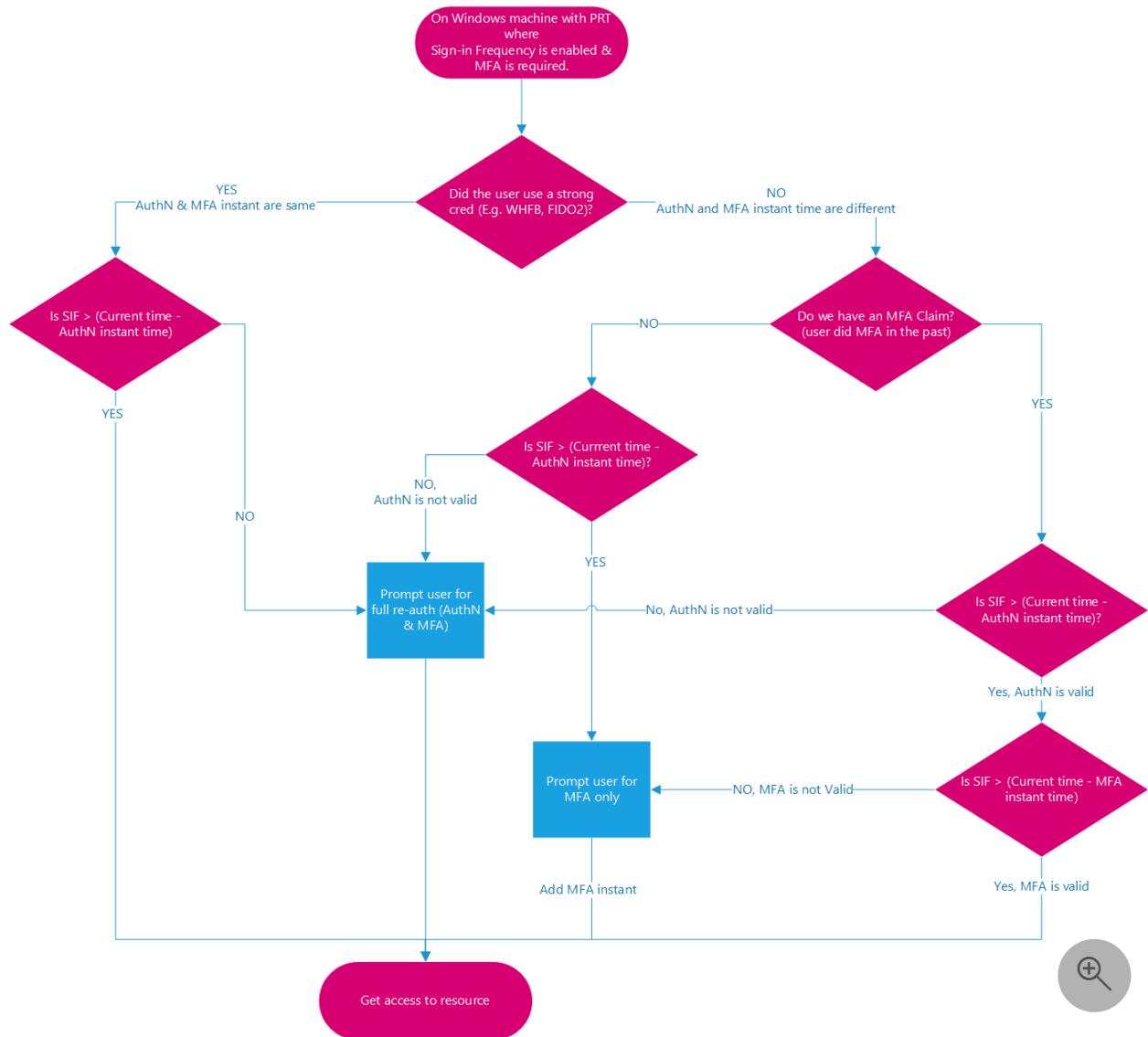
The sign-in frequency setting works with apps that implement OAuth2 or OIDC protocols according to the standards. Most Microsoft native apps, like those for Windows, Mac, and Mobile including the following web applications comply with the setting.

- Word, Excel, PowerPoint Online
- OneNote Online
- Office.com
- Microsoft 365 Admin portal
- Exchange Online
- SharePoint and OneDrive
- Teams web client
- Dynamics CRM Online
- Azure portal

Sign-in frequency (SIF) works with non-Microsoft SAML applications and apps that implement OAuth2 or OIDC protocols, as long as they don't drop their own cookies and are redirected back to Microsoft Entra ID for authentication on a regular basis.

User sign-in frequency and multifactor authentication

Sign-in frequency previously applied only to the first factor authentication on devices that were Microsoft Entra joined, Microsoft Entra hybrid joined, and Microsoft Entra registered. There was no easy way for customers to reinforce multifactor authentication on those devices. Based on customer feedback, sign-in frequency now applies to multifactor authentication (MFA) as well.



User sign-in frequency and device identities

On Microsoft Entra joined and Microsoft Entra hybrid joined devices, unlocking the device or signing in interactively refreshes the Primary Refresh Token (PRT) every 4 hours. The last refresh timestamp recorded for the PRT compared with the current timestamp must be within the time allotted in SIF policy for the PRT to satisfy SIF and grant access to a PRT that has an existing MFA claim. On [Microsoft Entra registered devices](#), unlocking or signing in wouldn't satisfy the SIF policy because the user isn't accessing a Microsoft Entra registered device via a Microsoft Entra account. However, the [Microsoft Entra WAM](#) plugin can refresh a PRT during native application authentication using WAM.

Note

The timestamp captured from user log-in isn't necessarily the same as the last recorded timestamp of PRT refresh because of the 4-hour refresh cycle. The case when it's the same is when the PRT expired and a user log-in refreshes it for 4

hours. In the following examples, assume SIF policy is set to 1 hour and the PRT is refreshed at 00:00.

Example 1: When you continue to work on the same doc in SPO for an hour

- At 00:00, a user signs in to their Windows 11 Microsoft Entra joined device and starts work on a document stored on SharePoint Online.
- The user continues working on the same document on their device for an hour.
- At 01:00, the user is prompted to sign in again. This prompt is based on the sign-in frequency requirement in the Conditional Access policy configured by their administrator.

Example 2: When you pause work with a background task running in the browser, then interact again after the SIF policy time elapsed

- At 00:00, a user signs in to their Windows 11 Microsoft Entra joined device and starts to upload a document to SharePoint Online.
- At 00:10, the user gets up and takes a break locking their device. The background upload continues to SharePoint Online.
- At 02:45, the user returns from their break and unlocks the device. The background upload shows completion.
- At 02:45, the user is prompted to sign in when they interact again. This prompt is based on the sign-in frequency requirement in the Conditional Access policy configured by their administrator since the last sign-in happened at 00:00.

If the client app (under activity details) is a browser, we defer sign-in frequency enforcement of events and policies on background services until the next user interaction. On confidential clients, sign-in frequency enforcement on non-interactive sign-ins is deferred until the next interactive sign-in.

Example 3: With four hour refresh cycle of primary refresh token from unlock

Scenario 1 - User returns within cycle

- At 00:00, a user signs into their Windows 11 Microsoft Entra joined device and starts work on a document stored on SharePoint Online.
- At 00:30, the user gets up and takes a break locking their device.
- At 00:45, the user returns from their break and unlocks the device.

- At 01:00, the user is prompted to sign in again. This prompt is based on the sign-in frequency requirement in the Conditional Access policy configured by their administrator, 1 hour after the initial sign-in.

Scenario 2 - User returns outside cycle

- At 00:00, a user signs into their Windows 11 Microsoft Entra joined device and starts work on a document stored on SharePoint Online.
- At 00:30, the user gets up and takes a break locking their device.
- At 04:45, the user returns from their break and unlocks the device.
- At 05:45, the user is prompted to sign in again. This prompt is based on the sign-in frequency requirement in the Conditional Access policy configured by their administrator. It's now 1 hour after the PRT was refreshed at 04:45, and over 4 hours since the initial sign-in at 00:00.

Require reauthentication every time

There are scenarios where customers might want to require a fresh authentication, every time a user performs specific actions like:

- Accessing sensitive applications.
- Securing resources behind VPN or Network as a Service (NaaS) providers.
- Securing privileged role elevation in PIM.
- Protecting user sign-ins to Azure Virtual Desktop machines.
- Protecting risky users and risky sign-ins identified by Microsoft Entra ID Protection.
- Securing sensitive user actions like Microsoft Intune enrollment.

When administrators select **Every time**, it requires full reauthentication when the session is evaluated. For example, if the user closed and opened their browser during the session lifetime, they aren't prompted for reauthentication. Sign-in frequency set to every time works best when the resource has the logic to identify when a client should get a new token. These resources redirect the user back to Microsoft Entra only once the session expires.

Administrators should limit the number of applications they enforce a policy requiring users to reauthenticate every time with. Triggering reauthentication too frequently can increase security friction to a point that it causes users to experience MFA fatigue and open the door to phishing. Web applications usually provide a less disruptive experience than their desktop counterparts when require reauthentication every time is enabled. We factor for five minutes of clock skew when every time is selected in policy, so that we don't prompt users more often than once every five minutes.

- For applications in the Microsoft 365 stack, we recommend using [time-based user sign-in frequency](#) for a better user experience.
- For the Azure portal and the Microsoft Entra admin center, we recommend either using [time-based user sign-in frequency](#) or to [require reauthentication on PIM activation](#) using authentication context for a better user experience.

Persistence of browsing sessions

A persistent browser session lets users stay signed in after closing and reopening their browser window.

The Microsoft Entra ID default for browser session persistence lets users on personal devices choose whether to persist the session by showing a **Stay signed in?** prompt after successful authentication. If browser persistence is configured in AD FS using the guidance in the article [AD FS single sign-on settings](#), we comply with that policy and persist the Microsoft Entra session as well. You can also configure whether users in your tenant see the **Stay signed in?** prompt by changing the appropriate setting in the [company branding pane](#).

In persistent browsers, cookies stay stored in the user's device even after a user closes the browser. These cookies could have access to Microsoft Entra artifacts, and those artifacts are usable until token expiration regardless of the Conditional Access policies placed on the resource environment. So, token caching can be in direct violation of desired security policies for authentication. While it might seem convenient to store tokens beyond the current session, doing so can create a security vulnerability by allowing unauthorized access to Microsoft Entra artifacts.

Configuring authentication session controls

Conditional Access is a Microsoft Entra ID P1 or P2 capability and requires a premium license. If you want to learn more about Conditional Access, see [What is Conditional Access in Microsoft Entra ID?](#).

Warning

If you're using the [configurable token lifetime](#) feature currently in public preview, note that we don't support creating two different policies for the same user or app combination: one with this feature and another with the configurable token lifetime feature. Microsoft retired the configurable token lifetime feature for refresh and session token lifetimes on January 30, 2021, and replaced it with the Conditional Access authentication session management feature.

Before enabling sign-in frequency, make sure other reauthentication settings are disabled in your tenant. If "Remember MFA on trusted devices" is enabled, disable it before using sign-in frequency, as using these two settings together might lead to prompting users unexpectedly. To learn more about reauthentication prompts and session lifetime, see the article, [Optimize reauthentication prompts and understand session lifetime for Microsoft Entra multifactor authentication](#).

Next steps

- [Configure session lifetimes in Conditional Access policies](#)
- To configure Conditional Access policies for your environment, see the article [Plan a Conditional Access deployment](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Conditional Access: Filter for devices

Article • 04/08/2025

When administrators create Conditional Access policies, the ability to target or exclude specific devices in their environment is a common task. The condition filter for devices gives administrators the ability to target specific devices. Administrators can use [supported operators and properties for device filters](#) along side the other available assignment conditions in your Conditional Access policies.

The screenshot shows the Microsoft Azure portal interface with the title 'Filter for devices - Microsoft Azure'. The URL is https://portal.azure.com/#blade/Microsoft_AAD_IAM/PolicyBlade/ConfigureFilterForDevicesBlade. The user is signed in as 'BalaS@contoso.onmicrosoft.com (CONTOSO (CONTOSO.ONMICRO...))'. On the left, there's a sidebar with navigation links like Home, Identity, Conditional Access, Control access policy, Assignments, Users and groups, Cloud apps or services, Conditions, Access controls, Grant, Enable policy, and Report-only. The 'Report-only' option is selected. The main content area is titled 'Filter for devices' and has a sub-section 'New'. It says 'Configure a filter to apply policy to specific devices.' with a 'Learn more' link. Below that is a 'Configure' section with 'Yes' and 'No' buttons, where 'Yes' is selected. The next section is 'Devices matching the rule:' with two options: 'Include filtered devices in policy' (radio button) and 'Exclude filtered devices from policy' (radio button, which is selected). A note says 'You can use the rule builder or rule syntax text box to create or edit the filter rule.' Below this is a table with columns 'And/Or', 'Property', 'Operator', and 'Value'. There's one row: 'And/Or' is 'ExtensionAttribute1', 'Property' is 'Equals', and 'Value' is 'SAW'. Below the table is a '+ Add expression' button. Under 'Rule syntax', there's a text box containing 'device.extensionAttribute1 -eq "SAW"' with an 'Edit' button next to it. At the bottom are 'Create' and 'Done' buttons.

Common scenarios

There are multiple scenarios that organizations can now enable using filter for devices condition. The following scenarios provide examples of how to use this new condition.

- **Restrict access to privileged resources.** For this example, let's say you want to allow access to Windows Azure Service Management API from a user who:
 - o Is assigned a [privileged role](#).

- Completed multifactor authentication.
 - Is on a device that is [privileged or secure admin workstations](#) and attested as compliant.
 - For this scenario, organizations would create two Conditional Access policies:
 - Policy 1: All users with an administrator role, accessing the Windows Azure Service Management API cloud app, and for Access controls, Grant access, but require multifactor authentication and require device to be marked as compliant.
 - Policy 2: All users with an administrator, accessing the Windows Azure Service Management API cloud app, excluding a filter for devices using rule expression device.extensionAttribute1 equals SAW and for Access controls, Block. Learn how to [update extensionAttributes on a Microsoft Entra device object](#).
- **Block access to organization resources from devices running an unsupported Operating System.** For this example, lets say you want to block access to resources from Windows OS version older than Windows 10. For this scenario, organizations would create the following Conditional Access policy:
 - All users, accessing all resources, excluding a filter for devices using rule expression device.operatingSystem equals Windows and device.operatingSystemVersion startsWith "10.0" and for Access controls, Block.
 - **Do not require multifactor authentication for specific accounts on specific devices.** For this example, lets say you want to not require multifactor authentication when using service accounts on specific devices like Teams Phones or Surface Hub devices. For this scenario, organizations would create the following two Conditional Access policies:
 - Policy 1: All users excluding service accounts, accessing all resources, and for Access controls, Grant access, but require multifactor authentication.
 - Policy 2: Select users and groups and include group that contains service accounts only, accessing all resources, excluding a filter for devices using rule expression device.extensionAttribute2 not equals TeamsPhoneDevice and for Access controls, Block.

Note

Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory. The best way to target policies for unregistered devices is by using the negative operator since the configured filter rule would apply. If you were to use a positive operator, the filter rule would only apply when a device exists in the directory and the configured rule matches the attribute on the device.

Create a Conditional Access policy

Filter for devices is an optional control when creating a Conditional Access policy.

The following steps help create two Conditional Access policies to support the first scenario under [Common scenarios](#).

Policy 1: All users with an administrator role, accessing the Windows Azure Service Management API cloud app, and for Access controls, Grant access, but require multifactor authentication and require device to be marked as compliant.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **Directory roles**, then all roles with administrator in the name.

Warning

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](../role-based-access-control/manage-roles-portal.md) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
- c. Select **Done**.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**, choose **Windows Azure Service Management API**, and select **Select**.
7. Under **Access controls > Grant**, select **Grant access, Require multifactor authentication, and Require device to be marked as compliant**, then select **Select**.
8. Confirm your settings and set **Enable policy** to **On**.
9. Select **Create** to create to enable your policy.

Policy 2: All users with an administrator role, accessing the Windows Azure Service Management API cloud app, excluding a filter for devices using rule expression device.extensionAttribute1 equals SAW and for Access controls, Block.

1. Select **New policy**.

2. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
3. Under **Assignments**, select **Users or workload identities**.

- a. Under **Include**, select **Directory roles**, then all roles with administrator in the name

 **Warning**

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](#) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
- c. Select **Done**.
4. Under **Target resources** > **Resources (formerly cloud apps)** > **Include** > **Select resources**, choose **Windows Azure Service Management API**, and select **Select**.
5. Under **Conditions**, **Filter for devices**.
 - a. Toggle **Configure** to **Yes**.
 - b. Set **Devices matching the rule** to **Exclude filtered devices from policy**.
 - c. Set the property to `ExtensionAttribute1`, the operator to `Equals` and the value to `SAW`.
 - d. Select **Done**.
6. Under **Access controls** > **Grant**, select **Block access**, then select **Select**.
7. Confirm your settings and set **Enable policy** to **On**.
8. Select **Create** to create to enable your policy.

 **Warning**

Policies that require compliant devices may prompt users on Mac, iOS, and Android to select a device certificate during policy evaluation, even though device compliance is not enforced. These prompts may repeat until the device is made compliant.

Setting attribute values

Setting extension attributes is made possible through the Microsoft Graph API. For more information about setting device attributes, see the article [Update device](#).

Filter for devices Graph API

The filter for devices API is available in Microsoft Graph v1.0 endpoint and can be accessed using the endpoint <https://graph.microsoft.com/v1.0/identity/conditionalaccess/policies/>. You can configure a filter for devices when creating a new Conditional Access policy or you can update an existing policy to configure the filter for devices condition. To update an existing policy, you can do a patch call on the Microsoft Graph v1.0 endpoint by appending the policy ID of an existing policy and executing the following request body. The example here shows configuring a filter for devices condition excluding devices that aren't marked as SAW devices. The rule syntax can consist of more than one single expression. To learn more about the syntax, see [rules for dynamic membership groups for groups in Microsoft Entra ID](#).

JSON

```
{  
  "conditions": {  
    "devices": {  
      "deviceFilter": {  
        "mode": "exclude",  
        "rule": "device.extensionAttribute1 -ne \"SAW\""  
      }  
    }  
  }  
}
```

Supported operators and device properties for filters

The following device attributes can be used with the filter for devices condition in Conditional Access.

Note

Microsoft Entra ID uses device authentication to evaluate device filter rules. For a device that is unregistered with Microsoft Entra ID, all device properties are considered as null values and the device attributes cannot be determined since the device does not exist in the directory. The best way to target policies for unregistered devices is by using the negative operator since the configured filter rule would apply. If you were to use a positive operator, the filter rule would only apply when a device exists in the directory and the configured rule matches the attribute on the device.

 Expand table

Supported device attributes	Supported operators	Supported values	Example
deviceid	Equals, NotEquals, In, NotIn	A valid deviceid that is a GUID	(device.deviceid -eq "aaaaaaaa- 0000-1111-2222- bbbbbbbbbbbb")
displayName	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	Any string	(device.displayName -contains "ABC")
deviceOwnership	Equals, NotEquals	Supported values are "Personal" for bring your own devices and "Company" for corporate owned devices	(device.deviceOwnership -eq "Company")
enrollmentProfileName	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	This is set by Microsoft Intune based on the profile the device was enrolled under at the time of enrollment. It's a string value created by Microsoft Intune admin, and matches the Windows Autopilot, Apple Automated Device Enrollment (ADE), or Google enrollment profile applied to the device.	(device.enrollmentProfileName -startsWith "AutoPilot Profile")
isCompliant	Equals, NotEquals	Supported values are "True" for compliant devices and "False" for non compliant devices	(device.isCompliant -eq "True")
manufacturer	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	Any string	(device.manufacturer - startsWith "Microsoft")

Supported device attributes	Supported operators	Supported values	Example
mdmAppId	Equals, NotEquals, In, NotIn	A valid MDM application ID	(device.mdmAppId -in ["00001111-aaaa-2222-bbbb-3333cccc4444"])
model	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	Any string	(device.model -notContains "Surface")
operatingSystem	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	A valid operating system (like Windows, iOS, or Android)	(device.operatingSystem -eq "Windows")
operatingSystemVersion	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	A valid operating system version (like 6.1 for Windows 7, 6.2 for Windows 8, or 10.0 for Windows 10 and Windows 11)	(device.operatingSystemVersion -in ["10.0.18363", "10.0.19041", "10.0.19042", "10.0.22000"])
physicalIds	Contains, NotContains	As an example all Windows Autopilot devices store ZTID (a unique value assigned to all imported Windows Autopilot devices) in device physicalIds property.	(device.physicalIds -contains "[ZTID]:value")
profileType	Equals, NotEquals	A valid profile type set for a device. Supported values are: RegisteredDevice (default),	(device.profileType -eq "Printer")

Supported device attributes	Supported operators	Supported values	Example
		SecureVM (used for Windows VMs in Azure enabled with Microsoft Entra sign-in), Printer (used for printers), Shared (used for shared devices), IoT (used for IoT devices)	
systemLabels	Contains, NotContains	List of labels applied to the device by the system. Some of the supported values are: AzureResource (used for Windows VMs in Azure enabled with Microsoft Entra sign-in), M365Managed (used for devices managed using Microsoft Managed Desktop), MultiUser (used for shared devices)	(device.systemLabels -contains "M365Managed")
trustType	Equals, NotEquals	A valid registered state for devices. Supported values are: AzureAD (used for Microsoft Entra joined devices), ServerAD (used for Microsoft Entra hybrid joined devices), Workplace (used for Microsoft Entra registered devices)	(device.trustType -eq "ServerAD")
extensionAttribute1-15	Equals, NotEquals, StartsWith, NotStartsWith, EndsWith, NotEndsWith, Contains, NotContains, In, NotIn	extensionAttributes1-15 are attributes that customers can use for device objects. Customers can update any of the extensionAttributes1 through 15 with custom values and use them in the filter for devices condition in Conditional Access. Any string value can be used.	(device.extensionAttribute1 -eq "SAW")

 **Important**

Customers should avoid using Entra device properties (ones that can be modified or manipulated by an end user) just on its own when creating a device filter rule. As an example, use of displayName that can be modified by end user or model, manufacturer, etc. sourced from registry entries that can be manipulated by the end user. Microsoft recommends using these properties in conjunction (use of AND clause) with some of the other properties on the device that are not modifiable by the end user when creating a device filter rule in Conditional Access.

Warning

Devices must be Microsoft Intune managed, compliant, or Microsoft Entra hybrid joined for a value to be available in extensionAttributes1-15 at the time of the Conditional Access policy evaluation.

Note

When building complex rules or using too many individual identifiers like deviceId for device identities, keep in mind "The maximum length for the filter rule is 3072 characters".

Note

The `Contains` and the `NotContains` operators work differently depending on attribute types. For string attributes such as `operatingSystem` and `model`, the `Contains` operator indicates whether a specified substring occurs within the attribute. For string collection attributes such as `physicalIds` and `systemLabels`, the `Contains` operator indicates whether a specified string matches one of the whole strings in the collection.

Policy behavior with filter for devices

The filter for devices condition in Conditional Access evaluates policy based on device attributes of a registered device in Microsoft Entra ID and hence it's important to understand under what circumstances the policy is applied or not applied. The following table illustrates the behavior when a filter for devices condition is configured.

 Expand table

Filter for devices condition	Device registration state	Device filter Applied
Include/exclude mode with positive operators (Equals, StartsWith, EndsWith, Contains, In) and use of any attributes	Unregistered device	No
Include/exclude mode with positive operators (Equals, StartsWith, EndsWith, Contains, In) and use of attributes excluding extensionAttributes1-15	Registered device	Yes, if criteria are met
Include/exclude mode with positive operators (Equals, StartsWith, EndsWith, Contains, In) and use of attributes including extensionAttributes1-15	Registered device managed by Intune	Yes, if criteria are met
Include/exclude mode with positive operators (Equals, StartsWith, EndsWith, Contains, In) and use of attributes including extensionAttributes1-15	Registered device not managed by Intune	Yes, if criteria are met. When extensionAttributes1-15 are used, the policy applies if device is compliant or Microsoft Entra hybrid joined
Include/exclude mode with negative operators (NotEquals, NotStartsWith, NotEndsWith, NotContains, NotIn) and use of any attributes	Unregistered device	Yes
Include/exclude mode with negative operators (NotEquals, NotStartsWith, NotEndsWith, NotContains, NotIn) and use of any attributes excluding extensionAttributes1-15	Registered device	Yes, if criteria are met
Include/exclude mode with negative operators (NotEquals, NotStartsWith, NotEndsWith, NotContains, NotIn) and use of any attributes including extensionAttributes1-15	Registered device managed by Intune	Yes, if criteria are met
Include/exclude mode with negative operators (NotEquals, NotStartsWith, NotEndsWith, NotContains, NotIn) and use of any attributes including extensionAttributes1-15	Registered device not managed by Intune	Yes, if criteria are met. When extensionAttributes1-15 are used, the policy applies if device is compliant or Microsoft Entra hybrid joined

Related content

- [Back to school – Using Boolean algebra correctly in complex filters](#)

- Update device Graph API
- Conditional Access: Conditions
- Common Conditional Access policies

Troubleshoot Conditional Access Policies with the What If Tool

Article • 04/28/2025

The [Conditional Access What If policy tool](#) helps you understand the result of [Conditional Access](#) policies in your environment. It can be useful when simulating uncommon scenarios, enabling you to design more comprehensive security policies. Instead of manually testing your policies with multiple sign-ins, this tool helps you simulate a sign-in for a user or service principal. The simulation estimates how your policies affect this sign-in and generates a report.

The **What If** tool and [APIs](#) let you quickly determine the policies that apply to a specific user or single-tenant service principal. Use this information to troubleshoot issues, understand which policies apply to specific sign-in conditions, and test complex sign-in scenarios.

How it works

The Conditional Access What If tool is powered by the [What If Evaluation API](#). To use the tool, start by configuring the conditions of the sign-in scenario you want to simulate. The configuration should include:

- The user or single tenant service principal you want to test.
- The cloud apps, user action they would attempt to perform, or sensitive data protected by authentication context they would attempt to access.
- The sign-in conditions under which access would be attempted.

Important

The What If tool doesn't test for [Conditional Access service dependencies](#). For example, if you're using **What If** to test a Conditional Access policy for Microsoft Teams, the result doesn't consider any policy that applies to Office 365 Exchange Online, a Conditional Access service dependency for Microsoft Teams.

Next, initiate a simulation run that evaluates your settings. Only policies that are enabled or in report-only mode are included in an evaluation run.

When the evaluation finishes, the tool generates a report of the affected policies. To gather more information about a Conditional Access policy, use [Conditional Access per-policy reporting](#) or the [Conditional Access insights and reporting workbook](#) for details about policies in report-only mode or currently enabled.

Run the What If tool

You can find the **What If** tool in the **Microsoft Entra admin center > Entra ID > Conditional Access > Policies > What If**.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has sections like Overview, Policies (which is selected), Insights and reporting, Diagnose and solve problems, Manage (Named locations, Custom controls, Terms of use, VPN connectivity, Authentication contexts, Authentication strengths, Classic policies), Monitoring (Sign-in logs, Audit logs), Troubleshooting + Support (New support request). The top navigation bar includes 'Sign in', 'Conditional Access - Microsoft Entra', 'Home - Microsoft Defender', a search bar, and user info 'FlScho@microsoftlearn... MICROSOFTLEARNSECURITYDOCS'. The main content area is titled 'Conditional Access | Policies' and shows 'All policies' (8 total) and 'Microsoft-managed policies' (0 total). It includes a search bar and a 'Add filter' button. Below is a table of policies:

Policy name	State	Creation date	Modified date
BLOCK - Copilot Test	Report-only	2/25/2025, 11:58:32 AM	2/25/2025, 12:09:52 PM
Block access to Office Apps for users with Insider Risk (Preview)	Report-only	2/11/2025, 10:51:15 AM	...
Block legacy authentication	On	3/18/2025, 10:09:05 AM	3/18/2025, 10:09:32 AM
Multifactor authentication	On	2/11/2025, 12:02:37 PM	...
REPORT ONLY - All Users - Phishing Resistant MFA Strength	Report-only	2/14/2025, 11:10:10 AM	2/14/2025, 11:14:49 AM
Reauthentication on signin risk	On	2/11/2025, 12:04:14 PM	...
Secure password change on high user risk	On	2/11/2025, 12:04:51 PM	...
Security info registration	On	2/11/2025, 12:03:35 PM	...

To run the **What If** evaluation, provide the conditions you want to evaluate.

Conditions

The following conditions are required: identity, target resource, device platform, and client app. All other conditions are optional and are assumed to be set to **none** by default if no value is provided. For definitions of these conditions, see the article [Building a Conditional Access policy](#).

What if

X

Policies

[Info](#) | [Preview features](#) | [Got feedback?](#)

[\(i\)](#) To revert to the classic What if experience, click here.

Test the impact of Conditional Access on a user or service principal when signing in under certain conditions.

[Learn more](#)

Identity

Select identity type *

User ▼ *

User *

[Edit user](#)

Target resource

Select target type *

Cloud apps ▼ *

Cloud apps *

[+ Select cloud apps](#)

Sign-in conditions

Device platform

[Select device platform...](#) ▼

Client apps

[Select a client app...](#) ▼

Authentication flow

[Select authentication flow...](#) ▼

Insider risk

[Select Insider risk...](#) ▼

Sign-in risk

[Select sign-in risk...](#) ▼

Service principal risk (Preview)

[Select service principal risk...](#) ▼

IP address

Country

[Select country...](#) ▼

Filter for devices

Property	Value	Delete
Select a property... ▼	<i><Pick a property and operator first></i>	

[What if](#)

[Reset](#)



Evaluation

Start an evaluation by clicking **What If**. The evaluation result provides you with a report that consists of:

- An indicator showing whether classic policies exist in your environment.
- Policies that apply to your user or workload identity.
- Policies that don't apply to your user or workload identity.

Policies that will apply		Policies that will not apply	
<input type="text"/> Search			
Policy Name ↑↓	Grant controls ↑↓	Session controls ↑↓	State ↑↓
CA003: Block legacy authentication	Block access		On
CA004: Require multi-factor authentication for all users	Require multifactor authentication		Report-only
CA006: Require multi-factor authentication for Azure	Require multifactor authentication		On
CA007: Require multi-factor authentication for risky sign-in	Require multifactor authentication		On
CA008: Require password change for high-risk users	Require multifactor authentication AND Require password change		Report-only
CA011: No persistent browser session		Sign-in frequency - 1 hour AND P...	Report-only

The list of policies that apply also includes **grant controls** and **session controls** that must be satisfied.

The list of policies that don't apply includes the reasons why these policies don't apply. For each listed policy, the reason represents the first condition that wasn't satisfied.

Has filter indicates whether the policy has app filters that use custom security attributes.

Key differences between the What If evaluation API and the legacy experience

The What If Evaluation API is a Microsoft Graph API that is called by the Conditional Access experience. The What If tool powered by the [What If Evaluation API](#) is currently in public preview. The API is different from the legacy What If evaluation in a few ways:

1. The What-if API is a public and fully supported API (once the API is generally available).
The API can be used through the Conditional Access UX and the MS Graph API.
2. The logic aligns with the authentication logic used during sign-in to provide more accurate policy evaluation.
3. The What-if API expects all sign-in parameters to be defined for the evaluation to provide the most accurate results. If your tenant has policies with specific conditions and the sign-in details for those conditions aren't provided, the What If API can't evaluate those conditions.

Note

For application specification, provide the App ID. Groups of apps, such as **Office 365** or **Microsoft Admin Portals**, don't result in a match.

Examples

This example highlights key differences:

Suppose you have a Conditional Access policy with the following configuration:

- User: All users
- Resource: Office 365
- Location: United States
- Sign-in risk: High

 Expand table

Example	Parameters	Result based on legacy What If evaluation	Result based on the new What If evaluation API
1	UserId = "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb"	Applies	Does not apply
2	UserId = "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb" ApplicationId = "00000003-0000-0ff1-ce00-000000000000"	Applies	Does not apply
3	UserId = "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb" ApplicationId = "00000003-0000-0ff1-ce00-000000000000" Location = "US"	Applies	Applies
4	UserId = "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb" ApplicationId = "00000003-0000-0ff1-ce00-000000000000" Location = "US" Sign-in Risk = "High"	Applies	Applies

Related content

- Learn more about Conditional Access policy application by using the policies report-only mode in [Conditional Access insights and reporting](#).
- To configure Conditional Access policies for your environment, see [Conditional Access common policies](#).

Add, test, or remove protected actions in Microsoft Entra ID

Article • 03/30/2025

[Protected actions](#) in Microsoft Entra ID are permissions that have been assigned Conditional Access polices that are enforced when a user attempts to perform an action. This article describes how to add, test, or remove protected actions.

ⓘ Note

You should perform these steps in the following sequence to ensure that protected actions are properly configured and enforced. If you don't follow this order, you might get unexpected behavior, such as [getting repeated requests to reauthenticate](#).

Prerequisites

To add or remove protected actions, you must have:

- Microsoft Entra ID P1 or P2 license
- [Conditional Access Administrator](#) or [Security Administrator](#) role

Step 1: Configure Conditional Access policy

Protected actions use a Conditional Access authentication context, so you must configure an authentication context and add it to a Conditional Access policy. If you already have a policy with an authentication context, you can skip to the next section.

1. Sign in to the [Microsoft Entra admin center](#).
2. Select **Protection > Conditional Access > Authentication context > Authentication context**.
3. Select **New authentication context** to open the **Add authentication context** pane.
4. Enter a name and description and then select **Save**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Favorites, Identity, Applications, and Roles & admins. The main area is titled 'Conditional Access | Authentication contexts'. A sub-menu on the right shows 'Get started' and 'Configuration steps'. The 'Step' section includes 'Configure authentication contexts', 'Assign Conditional Access policies to the authentication context', and 'Tag resources with an authentication context'. A separate 'Add authentication context' dialog is open, prompting for a name ('Multifactor authentication'), a description ('Require multifactor authentication'), and a checkbox for 'Publish to apps'. The ID field is set to 'c1'.

5. Select Policies > New policy to create a new policy.

6. Create a new policy and select your authentication context.

For more information, see [Conditional Access: Cloud apps, actions, and authentication context](#).

The screenshot shows the 'New Conditional Access Policy' dialog. At the top, it says 'Home > Conditional Access | Policies > New'. The 'Name *' field contains 'Require multifactor authentication'. A dropdown menu under 'Select what this policy applies to' is set to 'Authentication context', with other options like 'Cloud apps' and 'User actions' available. Below this, a list of 'Authentication contexts' shows '1 authentication context included'. The 'Conditions' section indicates '0 conditions selected'. The 'Access controls' section is collapsed. At the bottom, the 'Enable policy' switch is set to 'On'. A large blue 'Create' button is at the bottom left.

Step 2: Add protected actions

To add protection actions, assign a Conditional Access policy to one or more permissions using a Conditional Access authentication context.

1. Select **Protection > Conditional Access > Policies**.
2. Make sure the state of the Conditional Access policy that you plan to use with your protected action is set to **On** and not **Off** or **Report-only**.
3. Select **Identity > Roles & admins > Protected actions**.

The screenshot shows the 'Protected actions' page in the Microsoft Entra ID for workforce interface. The left sidebar has sections for 'All roles', 'Protected actions' (which is selected), 'Diagnose and solve problems', 'Activity' (with 'Access reviews' and 'Audit logs'), 'Troubleshooting + Support', and 'New support request'. The main area has a search bar and a table with no results found. At the top, there are buttons for '+ Add protected actions', 'Refresh', 'Manage view', 'Remove', 'Preview features', and 'Got feedback?'. A red box highlights the '+ Add protected actions' button.

4. Select **Add protected actions** to add a new protected action.
- If **Add protected actions** is disabled, make sure you're assigned the Conditional Access Administrator or Security Administrator role. For more information, see [Troubleshoot protected actions](#).

5. Select a configured Conditional Access authentication context.
6. Select **Select permissions** and select the permissions to protect with Conditional Access.

The screenshot shows the 'Add protected actions' page. The left sidebar shows 'Conditional Access authentication context' set to 'Phishing resistant' and 'Permissions' section with 'No permissions added'. The main area has a search bar and a table with 7 actions found. The table has columns: 'Permission' (checkboxes), 'Description'. Some permissions are checked: 'microsoft.directory/conditionalAccessPolicies/basic/update', 'microsoft.directory/conditionalAccessPolicies/create', and 'microsoft.directory/conditionalAccessPolicies/delete'. A red box highlights the 'Select permissions' button.

7. Select **Add**.
8. When finished, select **Save**.

The new protected actions appear in the list of protected actions

Step 3: Test protected actions

When a user performs a protected action, they'll need to satisfy Conditional Access policy requirements. This section shows the experience for a user being prompted to satisfy a policy. In this example, the user is required to authenticate with a FIDO security key before they can update Conditional Access policies.

1. Sign in to the [Microsoft Entra admin center](#) as a user that must satisfy the policy.
2. Select **Protection > Conditional Access**.
3. Select a Conditional Access policy to view it.

Policy editing is disabled because the authentication requirements haven't been satisfied. At the bottom of the page is the following note:

Editing is protected by an additional access requirement. Click here to reauthenticate.

Require MFA for all cloud apps

X

Conditional Access policy

 Delete  View policy information (Preview)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name

Require MFA for all cloud apps

Assignments

Users 

[Specific users included](#)

Cloud apps or actions 

Enable policy

 Report-only  On  Off

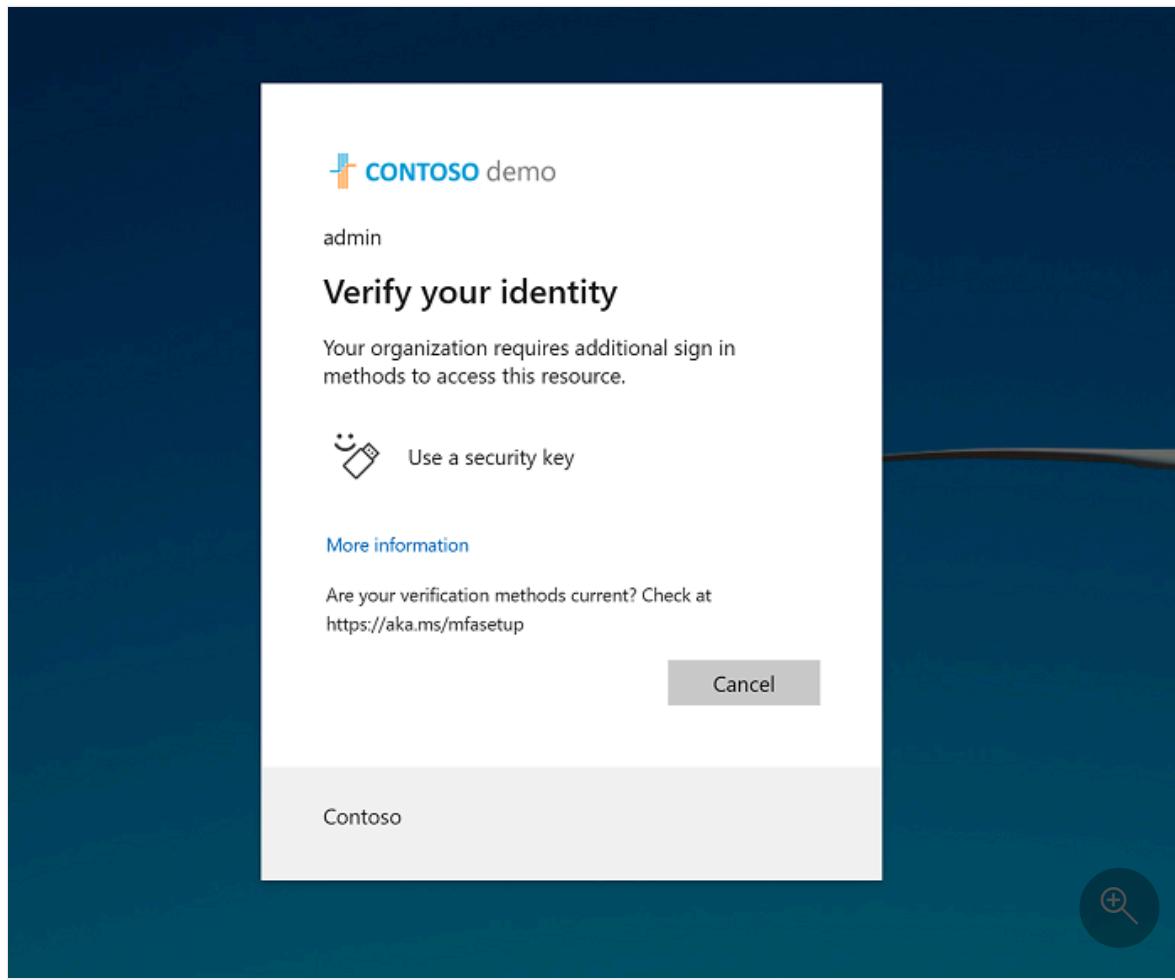
 Editing is protected by an additional access requirement. Click here to reauthenticate.

 Save



4. Select **Click here to reauthenticate**.

5. Complete the authentication requirements when the browser is redirected to the Microsoft Entra sign-in page.



After completing the authentication requirements, the policy can be edited.

6. Edit the policy and save changes.

Require MFA for all cloud apps

Conditional Access policy

X

 [Delete](#) [View policy information \(Preview\)](#)

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

Require MFA for all cloud apps

Assignments

Users

[Specific users included](#)

Cloud apps or actions

[All cloud apps](#)

Conditions

Enable policy

Report-only On Off
[Save](#)

Remove protected actions

To remove protection actions, unassign Conditional Access policy requirements from a permission.

1. Select Identity > Roles & admins > Protected actions.

2. Find and select the permission Conditional Access policy to unassign.

... > MOD Demo Platform UnifiedApiConsumer | Users and groups > Conditional Access | Authentication contexts > Roles and administrators | Protected actions > Roles and administrators

Roles and administrators | Protected actions ...

Contoso - Microsoft Entra ID for workforce

[Add protected actions](#) [Refresh](#) [Manage view](#) [Remove](#) [Preview features](#) [Got feedback?](#)

Protected actions are role permissions with Conditional Access applied for added security. Conditional Access requirements are enforced when a user performs the protected action.

[Learn more](#)

Search by name or description

2 actions found

Permission	Description	Conditional Ac
<input type="checkbox"/> microsoft.directory/conditionalAccessPolicies/basic/update	Update basic properties for Conditional Access policies	
<input checked="" type="checkbox"/> microsoft.directory/conditionalAccessPolicies/create	Create Conditional Access policies	

[New support request](#)

3. On the toolbar, select Remove.

After you remove the protected action, the permission won't have a Conditional Access requirement. A new Conditional Access policy can be assigned to the permission.

Microsoft Graph

Add protected actions

Protected actions are added by assigning an authentication context value to a permission. Authentication context values that are available in the tenant can be discovered by calling the [authenticationContextClassReference](#) API.

Authentication context can be assigned to a permission using the [unifiedRbacResourceAction](#) API beta endpoint:

HTTP

```
https://graph.microsoft.com/beta/roleManagement/directory/resourceNamespaces  
/microsoft.directory/resourceActions/
```

The following example shows how to get the authentication context ID that was set on the `microsoft.directory/conditionalAccessPolicies/delete` permission.

HTTP

```
GET  
https://graph.microsoft.com/beta/roleManagement/directory/resourceNamespaces  
/microsoft.directory/resourceActions/microsoft.directory-  
conditionalAccessPolicies-delete-delete?  
$select=authenticationContextId,isAuthenticationContextSettable
```

Resource actions with the property `isAuthenticationContextSettable` set to true support authentication context. Resource actions with the value of the property `authenticationContextId` is the authentication context ID that has been assigned to the action.

To view the `isAuthenticationContextSettable` and `authenticationContextId` properties, they must be included in the select statement when making the request to the resource action API.

Troubleshoot protected actions

Symptom - No authentication context values can be selected

When attempting to select a Conditional Access authentication context, there are no values available to select.

The screenshot shows the 'Add protected actions' interface. At the top, there's a breadcrumb navigation: Home > Roles and administrators | Protected actions >. The main title is 'Add protected actions' with a three-dot ellipsis. Below the title is a note: 'Select a Conditional Access authentication context and then the permissions you want to protect with that authentication context.' A 'Learn more' link is provided. The first section is 'Conditional Access authentication context *', which has a dropdown menu labeled 'Select' with a red box around it. To the left is 'Permissions ⓘ' and to the right is '+ Select permissions'. Below this is a table with columns 'Permission' and 'Description'. A message 'No permissions added' is displayed. At the bottom left is a 'Save' button, and at the bottom right is a circular search icon with a magnifying glass and a plus sign.

Cause

No Conditional Access authentication context values have been enabled in the tenant.

Solution

Enable authentication context for the tenant by adding a new authentication context. Ensure **Publish to apps** is checked, so the value is available to be selected. For more information, see [Authentication context](#).

Symptom - Policy isn't getting triggered

In some cases, after a protected action has been added, users may not be prompted as expected. For example, if policy requires multifactor authentication, a user may not see a sign-in prompt.

Cause 1

The user hasn't been assigned to the Conditional Access policies used for protected action.

Solution 1

Use Conditional Access [What If](#) tool to check if the user has been assigned policy. When using the tool, select the user and the authentication context that was used with the protected action. Select What If and verify the expected policy is listed in the **Policies that will apply** table. If the policy doesn't apply, check the policy user assignment condition, and add the user.

Cause 2

The user has previously satisfied policy. For example, the completed multifactor authentication earlier in the same session.

Solution 2

Check the [Microsoft Entra sign-in events](#) to troubleshoot. The sign-in events include details about the session, including if the user has already completed multifactor authentication. When troubleshooting with the sign-in logs, it's also helpful to check the policy details page, to confirm an authentication context was requested.

Symptom - Policy is never satisfied

When you attempt to perform the requirements for the Conditional Access policy, the policy is never satisfied and you keep getting requested to reauthenticate.

Cause

The Conditional Access policy wasn't created or the policy state is **Off** or **Report-only**.

Solution

Create the Conditional Access policy if it doesn't exist or and set the state to **On**.

If you aren't able to access the Conditional Access page because of the protected action and repeated requests to reauthenticate, use the following link to open the Conditional Access page.

- [https://aka.ms/MSALProtectedActions ↗](https://aka.ms/MSALProtectedActions)

Symptom - No access to add protected actions

When signed in you don't have permissions to add or remove protected actions.

Cause

You don't have permission to manage protected actions.

Solution

Make sure you're assigned the [Conditional Access Administrator](#) or [Security Administrator](#) role.

Symptom - Error returned using PowerShell to perform a protected action

When using PowerShell to perform a protected action, an error is returned and there's no prompt to satisfy Conditional Access policy.

Cause

Microsoft Graph PowerShell supports step-up authentication, which is required to allow policy prompts. Azure PowerShell isn't supported for step-up authentication.

Solution

Make sure you're using Microsoft Graph PowerShell.

Next steps

- [What are protected actions in Microsoft Entra ID?](#)
- [Conditional Access authentication context](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

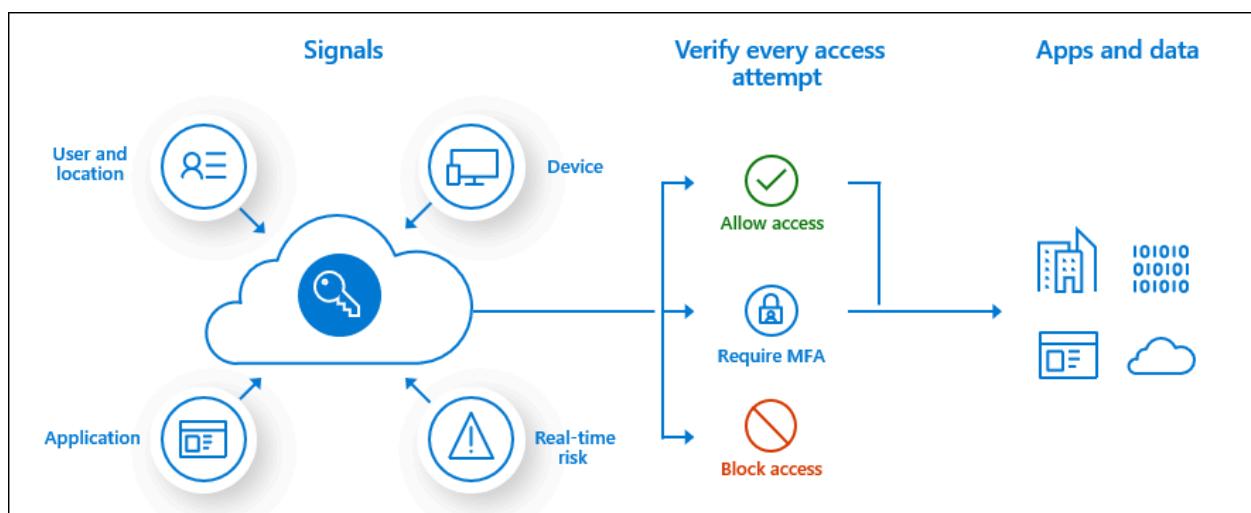
Plan a Conditional Access deployment

Article • 09/18/2024

Planning your Conditional Access deployment is critical to achieving your organization's access strategy for apps and resources. Conditional Access policies provide great configuration flexibility. However, this flexibility also means you should plan carefully to avoid undesirable results.

[Microsoft Entra Conditional Access](#) combines signals such as user, device, and location to automate decisions and enforce organizational access policies for resources. These Conditional Access policies help you balance security and productivity, enforcing security controls when needed and staying out of the user's way when not.

Conditional Access is the basis of [Microsoft's Zero Trust security policy engine](#).



Microsoft provides [security defaults](#) that ensure a basic level of security enabled in tenants that don't have Microsoft Entra ID P1 or P2. With Conditional Access, you can create policies that provide the same protection as security defaults, but with granularity. Conditional Access and security defaults aren't meant to be combined as creating Conditional Access policies prevent you from enabling security defaults.

Prerequisites

- A working Microsoft Entra tenant with Microsoft Entra ID P1, P2, or trial license enabled. If needed, [create one for free](#).
- Microsoft Entra ID P2 is required to include Microsoft Entra ID Protection risk in Conditional Access policies.
- Administrators who interact with Conditional Access must have one of the following role assignments depending on the tasks they're performing. To follow

the [Zero Trust principle of least privilege](#), consider using [Privileged Identity Management \(PIM\)](#) to just-in-time activate privileged role assignments.

- Read Conditional Access policies and configurations
 - [Security Reader](#)
 - Create or modify Conditional Access policies
 - [Conditional Access Administrator](#)
- A test user (not an administrator) that allows you to verify policies work as expected before deploying to real users. If you need to create a user, see [Quickstart: Add new users to Microsoft Entra ID](#).
- A group that the test user is a member of. If you need to create a group, see [Create a group and add members in Microsoft Entra ID](#).

Communicating change

Communication is critical to the success of any new functionality. You should proactively communicate with your users how their experience changes, when it changes, and how to get support if they experience issues.

Conditional Access policy components

Conditional Access policies answer questions about who can access your resources, what resources they can access, and under what conditions. Policies can be designed to grant access, limit access with session controls, or to block access. You [build a Conditional Access policy](#) by defining the if-then statements like:

[] [Expand table](#)

If an assignment is met	Apply the access controls
If you're a user in Finance accessing the Payroll application	Require multifactor authentication and a compliant device
If you aren't a member of Finance accessing the Payroll application	Block access
If your user risk is high	Require a multifactor authentication and a secure password change

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Ask the right questions

Here are some common questions about [Assignments and Access Controls](#). Document the answers to questions for each policy before building it out.

Users or workload identities

- Which users, groups, directory roles, or workload identities are included in or excluded from the policy?
- What emergency access accounts or groups should be excluded from policy?

Cloud apps or actions

Will this policy apply to any application, user action, or authentication context? If yes:

- What applications or services will the policy apply to?
- What user actions are subject to this policy?
- What authentication contexts will this policy be applied to?

Filter for applications

[Using filter for applications to include or exclude applications instead of individually specifying them](#) helps organizations:

- Easily scale and target any number of applications.

- Easily manage applications with similar policy requirements.
- Reduce the number of individual policies.
- Reduce errors while editing policies: No need to add/remove applications manually from the policy. Just manage the attributes.
- Overcome policy size constraints.

Conditions

- Which device platforms are included in or excluded from the policy?
- What are the organization's known network locations?
 - What locations are included in or excluded from the policy?
- What client app types are included in or excluded from the policy?
- Do you need to target specific device attributes?
- If using [Microsoft Entra ID Protection](#), do you want to incorporate sign-in or user risk?

Block or grant controls

Do you want to grant access to resources by requiring one or more of the following?

- Multifactor authentication
- Device marked as compliant
- Using a Microsoft Entra hybrid joined device
- Using an approved client app
- App protection policy applied
- Password change
- Terms of Use accepted

Block access is a powerful control that you should apply with appropriate knowledge. Policies with block statements can have unintended side effects. Proper testing and validation are vital before you enable the control at scale. Administrators should use tools such as [Conditional Access report-only mode](#) and [the What If tool in Conditional Access](#) when making changes.

Session controls

Do you want to enforce any of the following access controls on cloud apps?

- Use app enforced restrictions
- Use Conditional Access App control
- Enforce sign-in frequency

- Use persistent browser sessions
- Customize continuous access evaluation

Combining policies

When creating and assigning policies, you must take into account how access tokens work. [Access tokens](#) grant or deny access based on whether the users making a request have been authorized and authenticated. If the requestor can prove they're who they claim to be, they can access the protected resources or functionality.

Access tokens are issued by default if a Conditional Access policy condition does not trigger an access control.

This policy doesn't prevent the app having its own ability to block access.

For example, consider a simplified policy example where:

Users: FINANCE GROUP

Accessing: PAYROLL APP

Access control: Multifactor authentication

- User A is in the FINANCE GROUP, they're required to perform multifactor authentication to access the **PAYROLL APP**.
- User B is **not** in the FINANCE GROUP, is issued an access token and is allowed to access the **PAYROLL APP** without performing multifactor authentication.

To ensure users outside of finance group can't access the payroll app, a separate policy could be created to block all other users, like the following simplified policy:

Users: Include All Users / Exclude FINANCE GROUP

Accessing: PAYROLL APP

Access control: Block access

Now when User B attempts to access the **PAYROLL APP** they're blocked.

Recommendations

Taking into account our learnings in the use of Conditional Access and supporting other customers, here are a few recommendations based on our learnings.

Apply Conditional Access policies to every app

Ensure that every app has at least one Conditional Access policy applied. From a security perspective it's better to create a policy that encompasses All cloud apps, and then exclude applications that you don't want the policy to apply to. This practice ensures you don't need to update Conditional Access policies every time you onboard a new application.

💡 Tip

Be very careful in using block and all apps in a single policy. This could lock admins out, and exclusions cannot be configured for important endpoints such as Microsoft Graph.

Minimize the number of Conditional Access policies

Creating a policy for each app isn't efficient and leads to difficult administration. Conditional Access has a limit of 195 policies per-tenant. This 195 policy limit includes Conditional Access policies in any state including report-only mode, on, or off.

We recommend that you **analyze your apps and group them into applications that have the same resource requirements for the same users**. For example, if all Microsoft 365 apps or all HR apps have the same requirements for the same users, create a single policy and include all the apps to which it applies.

Conditional Access policies are contained in a JSON file and that file is bound to a size limit we don't expect a single policy to grow beyond. If you use a long list of GUIDs in your policy, you might hit this limit. If you encounter these limits, we recommend alternatives like:

- Use groups or roles to include or exclude Users instead of listing each user individually.
- Use filter for applications to include or exclude applications instead of individually specifying them.

Configure report-only mode

By default, each policy created from template is created in report-only mode. We recommended organizations test and monitor usage, to ensure the intended result, before turning on each policy.

Enable policies in report-only mode. Once you save a policy in report-only mode, you can see the effect on real-time sign-ins in the sign-in logs. From the sign-in logs, select

an event and navigate to the **Report-only** tab to see the result of each report-only policy.

You can view the aggregate affects of your Conditional Access policies in the **Insights and Reporting workbook**. To access the workbook, you need an Azure Monitor subscription and you need to [stream your sign-in logs to a log analytics workspace](#).

Plan for disruption

To reduce the risk of lockout during unforeseen disruptions, [plan resilience strategies](#) for your organization.

Enable protected actions

Enabling [protected actions](#) puts another layer of security on attempts to create, modify, or delete Conditional Access policy. Organizations can require a fresh multifactor authentication or other grant control before modifying policy.

Set naming standards for your policies

A naming standard helps you to find policies and understand their purpose without opening them in the Azure admin portal. We recommend that you name your policy to show:

- A Sequence Number
- The cloud apps it applies to
- The response
- Who it applies to
- When it applies

<SN>-	<Cloud app>:	<Response>	For	<Principal>	When	<Conditions>
-------	--------------	------------	-----	-------------	------	--------------

Example: A policy to require MFA for marketing users accessing the Dynamics CRP app from external networks might be:

CA01 -	Dynamics CRP:	Require MFA	For	marketing	When	On external networks
--------	---------------	-------------	-----	-----------	------	----------------------

A descriptive name helps you to keep an overview of your Conditional Access implementation. The Sequence Number is helpful if you need to reference a policy in a conversation. For example, when you talk to an administrator on the phone, you can ask them to open policy CA01 to solve an issue.

Naming standards for emergency access controls

In addition to your active policies, implement disabled policies that act as secondary [resilient access controls in outage or emergency scenarios](#). Your naming standard for the contingency policies should include:

- ENABLE IN EMERGENCY at the beginning to make the name stand out among the other policies.
- The name of disruption it should apply to.
- An ordering sequence number to help the administrator to know in which order policies should be enabled.

Example: The following name indicates that this policy is the first of four policies to enable if there's an MFA disruption:

- EM01 - ENABLE IN EMERGENCY: MFA Disruption [1/4] - Exchange SharePoint: Require Microsoft Entra hybrid join For VIP users.

Block countries/regions from which you never expect a sign-in

Microsoft Entra ID allows you to create [named locations](#). Create the list of countries/regions that are allowed, and then create a network block policy with these "allowed countries/regions" as an exclusion. This option creates less overhead for customers who are based in smaller geographic locations. **Be sure to exempt your emergency access accounts from this policy.**

Deploy Conditional Access policies

When you're ready, deploy your Conditional Access policies in phases.

Build your Conditional Access policies

Refer to [Conditional Access policy templates](#) and [Common security policies for Microsoft 365 organizations](#) for a head start. These templates are convenient way to deploy Microsoft recommendations. Make sure you exclude your emergency access accounts.

Evaluate the policy impact

We recommend that you use the following tools to evaluate the effect of your policies both before and after making changes. A simulated run gives you a good idea of the effect a Conditional Access policy has, it doesn't replace an actual test run in a properly configured development environment.

- [Report-only mode](#) and the Conditional Access insights and Reporting workbook.
- The [What If tool](#)

Test your policies

Ensure you test the exclusion criteria of a policy. For example, you might exclude a user or group from a policy that requires MFA. Test if the excluded users are prompted for MFA, because the combination of other policies might require MFA for those users.

Perform each test in your test plan with test users. The test plan is important to have a comparison between the expected results and the actual results. The following table outlines some example test cases. Adjust the scenarios and expected results based on how your Conditional Access policies are configured.

[\[+\] Expand table](#)

Policy	Scenario	Expected Result
Risky sign-ins	User signs into App using an unapproved browser	Calculates a risk score based on the probability that the sign-in wasn't performed by the user. Requires user to self-remediate using MFA
Device management	Authorized user attempts to sign in from an authorized device	Access granted
Device management	Authorized user attempts to sign in from an unauthorized device	Access blocked
Password change for risky users	Authorized user attempts to sign in with compromised credentials (high risk sign-in)	User is prompted to change password or access is blocked based on your policy

Deploy in production

After you confirm impact using [report-only mode](#), an administrator can move the [Enable policy](#) toggle from [Report-only](#) to [On](#).

Roll back policies

In case you need to roll back your newly implemented policies, use one or more of the following options:

- **Disable the policy.** Disabling a policy makes sure it doesn't apply when a user tries to sign in. You can always come back and enable the policy when you would like to use it.
- **Exclude a user or group from a policy.** If a user is unable to access the app, you can choose to exclude the user from the policy.

Caution

Exclusions should be used sparingly, only in situations where the user is trusted. Users should be added back into the policy or group as soon as possible.

- If a policy is disabled and no longer required, **delete it**.

Troubleshoot Conditional Access policies

If a user has an issue with a Conditional Access policy, collect the following information to facilitate troubleshooting.

- User Principal Name
- User display name
- Operating system name
- Time stamp (approximate is ok)
- Target application
- Client application type (browser vs client)
- Correlation ID (this ID is unique to the sign-in)

If the user received a message with a More details link, they can collect most of this information for you.

Once you collect the information, see the following resources:

- [Sign-in problems with Conditional Access](#) – Understand unexpected sign-in outcomes related to Conditional Access using error messages and Microsoft Entra sign-in log.
- [Using the What-If tool](#) - Understand why a policy was or wasn't applied to a user in a specific circumstance or if a policy would apply in a known state.

Related content

- [Learn more about Multifactor authentication](#)
 - [Learn more about Microsoft Entra ID Protection](#)
 - [Manage Conditional Access policies with Microsoft Graph API](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Block legacy authentication with Conditional Access

Article • 04/01/2025

Microsoft recommends that organizations block authentication requests using legacy protocols that don't support multifactor authentication. Based on Microsoft's analysis more than 97 percent of credential stuffing attacks use legacy authentication and more than 99 percent of password spray attacks use legacy authentication protocols. These attacks would stop with basic authentication disabled or blocked.

Customers without licenses that include Conditional Access can make use of [security defaults](#) to block legacy authentication.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to block legacy authentication requests. This policy is put in to [Report-only mode](#) to start so administrators can determine the impact they have on existing users. When administrators are comfortable that the policy applies as they intend, they can switch to [On](#) or stage the deployment by adding specific groups and excluding others.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose any accounts that must maintain the ability to use legacy authentication. Microsoft recommends you exclude at least one account to prevent yourself from being locked out due to misconfiguration.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Conditions > Client apps**, set **Configure** to **Yes**.
 - a. Check only the boxes **Exchange ActiveSync clients** and **Other clients**.
 - b. Select **Done**.
8. Under **Access controls > Grant**, select **Block access**.
 - a. Select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

ⓘ Note

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Identify legacy authentication use

To understand if your users have client apps that use legacy authentication, administrators can check for indicators in the sign-in logs with the following steps:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Reports Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Add the **Client App** column if it isn't shown by clicking on **Columns > Client App**.
4. Select **Add filters > Client App** > choose all of the legacy authentication protocols and select **Apply**.
5. Also perform these steps on the **User sign-ins (non-interactive)** tab.

Filtering shows you sign-in attempts made by legacy authentication protocols. Clicking on each individual sign-in attempt shows you more details. The **Client App** field under the **Basic Info** tab indicates which legacy authentication protocol was used. These logs indicate users who are using clients that depend on legacy authentication.

Additionally, to help triage legacy authentication within your tenant use the [Sign-ins using legacy authentication workbook](#).

Related content

- [Deprecation of Basic authentication in Exchange Online](#)
- [How to set up a multifunction device or application to send email using Microsoft 365](#)
- [How modern authentication works for Office client apps](#)
- [Connect to Exchange Online PowerShell](#)

Feedback

Was this page helpful?



[Provide product feedback](#)

Require phishing-resistant multifactor authentication for administrators

Article • 10/22/2024

Accounts that are assigned privileged administrative roles are frequent targets of attackers. Requiring phishing-resistant multifactor authentication (MFA) on those accounts is an easy way to reduce the risk of those accounts being compromised.

⊗ Caution

Before creating a policy requiring phishing-resistant multifactor authentication, ensure your administrators have the appropriate methods registered. If you enable this policy without completing this step you risk locking yourself out of your tenant. Administrators can [Configure Temporary Access Pass to register passwordless authentication methods](#) or follow the steps in [Register a passkey \(FIDO2\)](#).

Microsoft recommends you require phishing-resistant multifactor authentication on the following roles at a minimum:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

Organizations might choose to include or exclude roles based on their own requirements.

Organizations can use this policy in conjunction with features like Privileged Identity Management (PIM) and its ability to [require MFA for role activation](#).

Authentication strength

The guidance in this article helps your organization create an MFA policy for your environment using authentication strengths. Microsoft Entra ID provides three [built-in authentication strengths](#):

- Multifactor authentication strength (less restrictive)
- Passwordless MFA strength
- **Phishing-resistant MFA strength** (most restrictive) recommended in this article

You can use one of the built-in strengths or create a [custom authentication strength](#) based on the authentication methods you want to require.

For external user scenarios, the MFA authentication methods that a resource tenant can accept vary depending on whether the user is completing MFA in their home tenant or in the resource tenant. For more information, see [Authentication strength for external users](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

Warning

If you use [external authentication methods](#), these are currently incompatible with authentication strength and you should use the [Require multifactor authentication](#) grant control.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **Directory roles** and choose at least the previously listed roles.

Warning

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](#) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Cloud apps > Include**, select **All cloud apps**.
7. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select **Phishing-resistant MFA strength** from the list.
 - b. Select **Select**.
8. Confirm your settings and set **Enable policy to Report-only**.
9. Select **Create** to create to enable your policy.

After administrators confirm the settings using [report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- Microsoft Entra built-in roles
 - Conditional Access templates
 - Configure Microsoft Entra role settings in Privileged Identity Management
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Require multifactor authentication for all users

Article • 04/01/2025

As Alex Weinert, the Director of Identity Security at Microsoft, mentions in his blog post [Your Pa\\$\\$word doesn't matter ↗](#):

Your password doesn't matter, but MFA does! Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA.

Authentication strength

The guidance in this article helps your organization create an MFA policy for your environment using authentication strengths. Microsoft Entra ID provides three [built-in authentication strengths](#):

- **Multifactor authentication strength** (less restrictive) recommended in this article
- Passwordless MFA strength
- Phishing-resistant MFA strength (most restrictive)

You can use one of the built-in strengths or create a [custom authentication strength](#) based on the authentication methods you want to require.

For external user scenarios, the MFA authentication methods that a resource tenant can accept vary depending on whether the user is completing MFA in their home tenant or in the resource tenant. For more information, see [Authentication strength for external users](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or break-glass accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).

- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require all users do multifactor authentication, using the authentication strength policy, [without any app exclusions](#).

Warning

External authentication methods are currently incompatible with authentication strength. You should use the Require multifactor authentication grant control.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**:
 - i. Select **Users and groups**
 - i. Choose your organization's emergency access or break-glass accounts.

- ii. If you use hybrid identity solutions like Microsoft Entra Connect or Microsoft Entra Connect Cloud Sync, select **Directory roles**, then select **Directory Synchronization Accounts**
 - ii. You might choose to exclude your guest users if you're targeting them with a [guest user specific policy](#).
6. Under **Target resources** > **Resources (formerly cloud apps)** > **Include**, select All resources (formerly 'All cloud apps').

 **Tip**

Microsoft recommends all organizations create a baseline Conditional Access policy that targets: All users, all resources without any app exclusions, and requires multifactor authentication.

- 7. Under **Access controls** > **Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Multifactor authentication strength** from the list.
 - b. Select **Select**.
- 8. Confirm your settings and set **Enable policy** to **Report-only**.
- 9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Named locations

Organizations might choose to incorporate known network locations known as **Named locations** in their Conditional Access policies. These named locations might include trusted IP networks like those for a main office location. For more information about configuring named locations, see the article [What is the location condition in Microsoft Entra Conditional Access?](#)

In the previous example policy, an organization might choose to not require multifactor authentication if accessing a cloud app from their corporate network. In this case they could add the following configuration to the policy:

1. Under **Assignments**, select **Network**.
 - a. Configure **Yes**.
 - b. Include **Any network or location**.

- c. Exclude All trusted networks and locations.
2. Save your policy changes.

Related content

- Conditional Access templates
 - Use report-only mode for Conditional Access to determine the results of new policy decisions.
 - Windows subscription activation
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Require multifactor authentication strength for external users

Article • 04/01/2025

Authentication strength is a Conditional Access control that lets you define a specific combination of multifactor authentication (MFA) methods that an external user must complete to access your resources. This control is especially useful for restricting external access to sensitive apps in your organization. For example, you can create a Conditional Access policy, require a phishing-resistant authentication strength in the policy, and assign it to guests and external users.

Microsoft Entra ID provides three [built-in authentication strengths](#):

- **Multifactor authentication strength** (less restrictive) recommended in this article
- Passwordless MFA strength
- Phishing-resistant MFA strength (most restrictive)

You can use one of the built-in strengths or create a [custom authentication strength](#) based on the authentication methods you want to require.

In external user scenarios, the MFA authentication methods that a resource tenant can accept vary depending on whether the user is completing MFA in their home tenant or in the resource tenant. For details, see [Authentication strength for external users](#).

ⓘ Note

Currently, you can only apply authentication strength policies to external users who authenticate with Microsoft Entra ID. For email one-time passcode, SAML/WS-Fed, and Google federation users, use the [MFA grant control](#) to require MFA.

Configure cross-tenant access settings to trust MFA

Authentication strength policies work together with [MFA trust settings](#) in your cross-tenant access settings to determine where and how the external user must perform MFA. A Microsoft Entra user first authenticates with their own account in their home tenant. Then when this user tries to access your resource, Microsoft Entra ID applies the authentication strength Conditional Access policy and checks to see if you enabled MFA trust.

- If MFA trust is enabled, Microsoft Entra ID checks the user's authentication session for a claim indicating that MFA was fulfilled in the user's home tenant.
- If MFA trust is disabled, the resource tenant presents the user with a challenge to complete MFA in the resource tenant using an acceptable authentication method.

The authentication methods that external users can use to satisfy MFA requirements are different depending on whether the user is completing MFA in their home tenant or the resource tenant. See the table in [Conditional Access authentication strength](#).

ⓘ Important

Before you create the Conditional Access policy, check your cross-tenant access settings to make sure your inbound MFA trust settings are configured as intended.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Create a Conditional Access policy

Use the following steps to create a Conditional Access policy that applies an authentication strength to external users.

Warning

If you use [external authentication methods](#), these are currently incompatible with authentication strength and you should use the [Require multifactor authentication](#) grant control.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, choose **Select users and groups**, and then select **Guest or external users**.
 - i. Select the types of [guest or external users](#) you want to apply the policy to.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps)**, under **Include or Exclude**, select any applications you want to include in or exclude from the authentication strength requirements.
7. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the appropriate built-in or custom authentication strength from the list.
 - b. Select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- [Conditional Access templates](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Protect security info registration with Conditional Access policy

Article • 04/01/2025

Securing when and how users register for Microsoft Entra multifactor authentication and self-service password reset is possible with user actions in a Conditional Access policy. This feature is available to organizations who enable [combined registration](#). This functionality allows organizations to treat the registration process like any application in a Conditional Access policy and use the full power of Conditional Access to secure the experience. Users signing in to the Microsoft Authenticator app or enabling passwordless phone sign-in are subject to this policy.

Some organizations in the past might have used trusted network location or device compliance as a means to secure the registration experience. With the addition of [Temporary Access Pass](#) in Microsoft Entra ID, administrators can provide time-limited credentials to their users that allow them to register from any device or location. Temporary Access Pass credentials satisfy Conditional Access requirements for multifactor authentication.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a policy to secure registration

The following policy applies to the selected users, who attempt to register using the combined registration experience. The policy requires users to be in a trusted network location and do multifactor authentication, or use Temporary Access Pass credentials.

Warning

If you use [external authentication methods](#), these are currently incompatible with authentication strength and you should use the [Require multifactor authentication](#) grant control.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. In Name, Enter a Name for this policy. For example, **Combined Security Info Registration with TAP**.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.

Warning

Users must be enabled for the [combined registration](#).

- b. Under **Exclude**.

- i. Select **All guest and external users**.

Note

Temporary Access Pass does not work for guest users.

- ii. Select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > User actions**, check **Register security information**.
7. Under **Conditions > Locations**.
 - a. Set **Configure** to **Yes**.
 - i. **Include Any location**.
 - ii. **Exclude All trusted locations**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the appropriate built-in or custom authentication strength from the list.
 - b. Select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Administrators have to issue Temporary Access Pass credentials to new users so they can satisfy the requirements for multifactor authentication to register. Steps to accomplish this task, are found in the section [Create a Temporary Access Pass in the Microsoft Entra admin center](#).

Organizations might choose to require other grant controls with or in place of **Require multifactor authentication** at step 8a. When selecting multiple controls, be sure to select the appropriate radio button toggle to require **all** or **one** of the selected controls when making this change.

Guest user registration

For [guest users](#) who need to register for multifactor authentication in your directory you might choose to block registration from outside of [trusted network locations](#) using the following guide.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. In **Name**, Enter a Name for this policy. For example, **Combined Security Info Registration on Trusted Networks**.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All guest and external users**.
6. Under **Target resources > User actions**, check **Register security information**.

7. Under **Conditions** > **Locations**.
 - a. Configure **Yes**.
 - b. Include **Any location**.
 - c. Exclude **All trusted locations**.
8. Under **Access controls** > **Grant**.
 - a. Select **Block access**.
 - b. Then choose **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- [Microsoft Entra built-in roles](#)
- [Conditional Access templates](#)
- [Require users to reconfirm authentication information](#)

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Require multifactor authentication for elevated sign-in risk

Article • 04/03/2025

Most users have a normal behavior that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in. You might want to block that user or maybe ask them to perform multifactor authentication to prove that they're really who they say they are.

A sign-in risk represents the probability that a given authentication request isn't the identity owner. Organizations with Microsoft Entra ID P2 licenses can create Conditional Access policies incorporating [Microsoft Entra ID Protection sign-in risk detections](#).

The Sign-in risk-based policy protects users from registering MFA in risky sessions. If users aren't registered for MFA, their risky sign-ins are blocked, and they see an AADSTS53004 error.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Enable with Conditional Access policy

1. Sign in to the Microsoft Entra admin center  as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - c. Select **Done**.
6. Under **Cloud apps or actions > Include**, select **All resources** (formerly 'All cloud apps').
7. Under **Conditions > Sign-in risk**, set **Configure** to **Yes**.
 - a. Under **Select the sign-in risk level this policy will apply to**, select **High** and **Medium**. [This guidance is based on Microsoft recommendations and might be different for each organization](#)
 - b. Select **Done**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Multifactor authentication** authentication strength from the list.
 - b. Select **Select**.
9. Under **Session**.
 - a. Select **Sign-in frequency**.
 - b. Ensure **Every time** is selected.
 - c. Select **Select**.
10. Confirm your settings and set **Enable policy** to **Report-only**.
11. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Passwordless scenarios

For organizations that adopt [passwordless authentication methods](#) make the following changes:

Update your passwordless sign-in risk policy

1. Under **Users**:
 - a. **Include**, select **Users and groups** and target your passwordless users.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - c. Select **Done**.
2. Under **Cloud apps or actions > Include**, select **All resources** (formerly 'All cloud apps').
3. Under **Conditions > Sign-in risk**, set **Configure** to **Yes**.
 - a. Under **Select the sign-in risk level this policy will apply to**, select **High** and **Medium**. For more information on risk levels, see [Choosing acceptable risk levels](#).
 - b. Select **Done**.
4. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Passwordless MFA** or **Phishing-resistant MFA** based on which method the targeted users have.
 - b. Select **Select**.
5. Under **Session**:
 - a. Select **Sign-in frequency**.
 - b. Ensure **Every time** is selected.
 - c. Select **Select**.

Related content

- [Require reauthentication every time](#)
- [Remediate risks and unblock users](#)
- [Conditional Access common policies](#)
- [User risk-based Conditional Access](#)
- [Determine effect using Conditional Access report-only mode](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Require a secure password change for elevated user risk

Article • 04/01/2025

Microsoft works with researchers, law enforcement, various security teams at Microsoft, and other trusted sources to find leaked username and password pairs. Organizations with Microsoft Entra ID P2 licenses can create Conditional Access policies incorporating [Microsoft Entra ID Protection user risk detections](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Enable with Conditional Access policy

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - c. Select **Done**.
6. Under **Cloud apps or actions > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Conditions > User risk**, set **Configure** to **Yes**.
 - a. Under **Configure user risk levels needed for policy to be enforced**, select **High**.
This guidance is based on Microsoft recommendations and might be different for each organization
 - b. Select **Done**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Multifactor authentication** authentication strength from the list.
 - b. Select **Require password change**.
 - c. Select **Select**.
9. Under **Session**.
 - a. Select **Sign-in frequency**.
 - b. Ensure **Every time** is selected.
 - c. Select **Select**.
10. Confirm your settings and set **Enable policy** to **Report-only**.
11. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Passwordless scenarios

For organizations that adopt [passwordless authentication](#) methods make the following changes:

Update your passwordless user risk policy

1. Under **Users**:

- a. **Include**, select **Users and groups** and target your passwordless users.
2. Under **Access controls** > **Block** access for passwordless users.

Tip

You might need to have two policies for a period of time while deploying passwordless methods.

- One that allows self-remediation for those not using passwordless methods.
- Another that blocks passwordless users at high risk.

Remediate and unblock passwordless user risk

1. Require administrator [investigation and remediation](#) of any risk.
2. Unblock the user.

Related content

- [Require reauthentication every time](#)
- [Remediate risks and unblock users](#)
- [Conditional Access common policies](#)
- [Sign-in risk-based Conditional Access](#)
- [Determine effect using Conditional Access report-only mode](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Require multifactor authentication for device registration

Article • 04/03/2025

Use the [Conditional Access user action](#) to enforce policy when users register or join devices to Microsoft Entra ID. This control provides granularity in configuring multifactor authentication for registering or joining devices instead of a tenant-wide policy that currently exists. Administrators can customize this policy to fit the security needs of their organization.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Create a Conditional Access policy

Warning

If you use [external authentication methods](#), these methods are currently incompatible with authentication strength and you should use the [Require multifactor authentication](#) grant control.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > User actions**, select **Register or join devices**.
7. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Multifactor authentication** authentication strength from the list.
 - b. Select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Warning

When a Conditional Access policy is configured with the **Register or join devices** user action, you must set **Identity > Devices > Overview > Device Settings - Require Multifactor Authentication** to register or join devices with Microsoft Entra to **No**. Otherwise, Conditional Access policies with this user action aren't properly enforced. More information about this device setting can found in [Configure device settings](#).

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation sidebar with links like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices (selected), Applications, and Learn & support. The main content area is titled "Devices | Device settings" for "Contoso - Microsoft Entra ID". It includes sections for Overview, All devices, Manage (Device settings selected), Activity (Audit logs, Bulk operation results (Preview)), Troubleshooting + Support (New support request, Diagnose and solve problems), and Microsoft Entra join and registration settings. In the "Manage" section, there are two tabs: "All" (selected) and "Selected". Under "All", it says "No member selected". Below this, there are sections for "Users may join devices to Microsoft Entra" (All selected) and "Users may register their devices with Microsoft Entra" (All selected). A link "Learn more on how this setting works" is present. At the bottom, under "Troubleshooting + Support", there is a "Require Multifactor Authentication to register or join devices with Microsoft Entra" section with a "Yes" button (selected) and a "No" button. A warning message states: "⚠ You already require Multifactor Authentication to register or join devices with Microsoft Entra in a Conditional Access policy. To correctly enforce the Conditional Access policy, set this to No. See Conditional Access policies." A magnifying glass icon is shown next to the warning message.

Related content

- [Conditional Access authentication strength](#)
- [Determine effect using Conditional Access report-only mode](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)
- [Manage device identities using the Microsoft Entra admin center](#)

Feedback

Was this page helpful?



Provide product feedback ↗

Require device compliance with Conditional Access

Article • 04/01/2025

Microsoft Intune and Microsoft Entra work together to secure your organization through [device compliance policies](#) and Conditional Access. Device compliance policies are a great way to ensure user devices meet minimum configuration requirements. The requirements can be enforced when users access services protected with Conditional Access policies.

Some organizations might not be ready to require device compliance for all users. These organizations might instead choose to deploy the following policies:

- Require compliant or Microsoft Entra hybrid joined device for their administrators
- Require a compliant device, Microsoft Entra hybrid joined device, **OR** multifactor authentication for all users
- Block unknown or unsupported device platforms
- Disable browser persistence

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require devices accessing resources be marked as compliant with your organization's [Intune compliance policies](#).

Warning

Without a compliance policy created in Microsoft Intune, this Conditional Access policy won't function as intended. Create a compliance policy first and ensure you have at least one compliant device before proceeding.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**:
 - i. Select **Users and groups**
 - i. Choose your organization's emergency access or break-glass accounts.
 - ii. If you use hybrid identity solutions like Microsoft Entra Connect or Microsoft Entra Connect Cloud Sync, select **Directory roles**, then select **Directory Synchronization Accounts**
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Access controls > Grant**.
 - a. Select **Require device to be marked as compliant**.
 - b. Select **Select**.
8. Confirm your settings and set **Enable policy to Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Note

You can enroll your new devices to Intune even if you select **Require device to be marked as compliant for All users and All resources (formerly 'All cloud apps')** using the previous steps. The **Require device to be marked as compliant** control doesn't block Intune enrollment.

Known behavior

On iOS, Android, macOS, and some non-Microsoft web browsers, Microsoft Entra ID identifies the device using a client certificate that is provisioned when the device is registered with Microsoft Entra ID. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

Subscription activation

Organizations that use the [Subscription Activation](#) feature to enable users to "step-up" from one version of Windows to another, might want to exclude the Windows Store for Business, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f from their device compliance policy.

Related content

- [Create a compliance policy in Microsoft Intune](#)
- [Conditional Access grant controls](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

Block authentication flows with Conditional Access policy

Article • 04/01/2025

The following steps help create Conditional Access policies to restrict how device code flow and authentication transfer are used within your organization.

Device code flow policies

ⓘ Note

To bolster security posture, Microsoft recommends blocking or restricting device code flow wherever possible.

You should always start by configuring a policy in [report-only mode](#) to determine the potential effect on your organization.

We recommend organizations get as close as possible to a unilateral block on device code flow. Organizations should consider creating a policy to audit the existing use of device code flow and determine if it is still necessary.

For organizations that have no established use of device code flow, blocking can be done with the following Conditional Access policy:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select the users you want to be in-scope for the policy (**all users recommended**).
 - b. Under **Exclude**:
 - i. Select **Users and groups** and choose your organization's emergency access or break-glass accounts and any other necessary users this exclusion list should be audited regularly.
5. Under **Target resources > Resources (formerly cloud apps) > Include**, select the apps you want to be in-scope for the policy (**All resources (formerly 'All cloud apps')** recommended).
6. Under **Conditions > Authentication Flows**, set **Configure** to **Yes**.

- a. Select **Device code flow**.
 - b. Select **Done**.
7. Under **Access controls > Grant**, select **Block access**.
 - a. Select **Select**. 8. Confirm your settings and set **Enable policy** to **Report-only**.
 9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Authentication transfer policies

Use the **Authentication flows** condition in Conditional Access to manage the feature.

You might want to block [authentication transfer](#) if you don't want users to transfer authentication from their PC to a mobile device. For example, if you don't allow Outlook to be used on personal devices by certain groups. Blocking authentication transfer can be done with the following Conditional Access policy:

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access**.
3. Select **Create new policy**.
4. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users** or user groups you would like to block for authentication transfer.
 - b. Under **Exclude**:
 - i. Select **Users and groups** and choose your organization's emergency access or break-glass accounts and any other necessary users this exclusion list should be audited regularly.
5. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')** or apps you would like to block for authentication transfer.
6. Under **Conditions > Authentication Flows**, set **Configure** to **Yes**
 - a. Select **Authentication transfer**.
 - b. Select **Done**.
7. Under **Access controls > Grant**, select **Block access**.
 - a. Select **Select**.
8. Confirm your settings and set **Enable policy** to **Enabled**.
9. Select **Create** to create to enable your policy.

Related content

- [Conditional Access: Authentication flows](#)
 - [Conditional Access: Authentication transfer](#)
 - [Conditional Access: Conditions](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Require approved client apps or app protection policy

Article • 04/03/2025

People regularly use their mobile devices for both personal and work tasks. While making sure staff can be productive, organizations also want to prevent data loss from applications on devices they may not manage fully.

With Conditional Access, organizations can restrict access to [approved \(modern authentication capable\) client apps with Intune app protection policies](#). For older client apps that may not support app protection policies, administrators can restrict access to [approved client apps](#).

⚠ Warning

App protection policies are supported on iOS and Android where applications meet specific requirements. **App protection policies are supported on Windows in preview for the Microsoft Edge browser only.** Not all applications that are supported as approved applications or support application protection policies. For a list of some common client apps, see [App protection policy requirement](#). If your application is not listed there, contact the application developer. In order to require approved client apps or to enforce app protection policies for iOS and Android devices, these devices must first register in Microsoft Entra ID.

ⓘ Note

Require one of the selected controls under grant controls is like an **OR** clause. This is used within policy to enable users to utilize apps that support either the **Require app protection policy** or **Require approved client app** grant controls. **Require app protection policy** is enforced when the app supports that grant control.

For more information about the benefits of using app protection policies, see the article [App protection policies overview](#).

The following policies are put in to **Report-only mode** to start so administrators can determine the impact they'll have on existing users. When administrators are comfortable that the policies apply as they intend, they can switch to **On** or stage the deployment by adding specific groups and excluding others.

Require approved client apps or app protection policy with mobile devices.

The following steps help create a Conditional Access policy requiring an approved client app **or** an app protection policy when using an iOS/iPadOS or Android device. This policy prevents the use of Exchange ActiveSync clients using basic authentication on mobile devices. This policy works in tandem with an [app protection policy created in Microsoft Intune](#).

Organizations can choose to deploy this policy using the following steps or using the [Conditional Access templates](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access**.
3. Select **Create new policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and exclude at least one account to prevent yourself from being locked out. If you don't exclude any accounts, you can't create the policy.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Conditions > Device platforms**, set **Configure** to **Yes**.
 - a. Under **Include**, **Select device platforms**.
 - b. Choose **Android** and **iOS**.
 - c. Select **Done**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require approved client app** and **Require app protection policy**
 - b. For multiple controls select **Require one of the selected controls**
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Tip**

Organizations should also deploy a policy that [blocks access from unsupported or unknown device platforms](#) along with this policy.

Block Exchange ActiveSync on all devices

This policy blocks all Exchange ActiveSync clients using basic authentication from connecting to Exchange Online.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access**.
3. Select **Create new policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and exclude at least one account to prevent yourself from being locked out. If you don't exclude any accounts, you can't create the policy.
 - c. Select **Done**.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **Select resources**.
 - a. Select **Office 365 Exchange Online**.
 - b. Select **Select**.
7. Under **Conditions > Client apps**, set **Configure** to **Yes**.
 - a. Uncheck all options except **Exchange ActiveSync clients**.
 - b. Select **Done**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require app protection policy**
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related Content

- [App protection policies overview](#)
- [Conditional Access common policies](#)
- [Migrate approved client app to application protection policy in Conditional Access](#)

Feedback

Was this page helpful?

 Yes

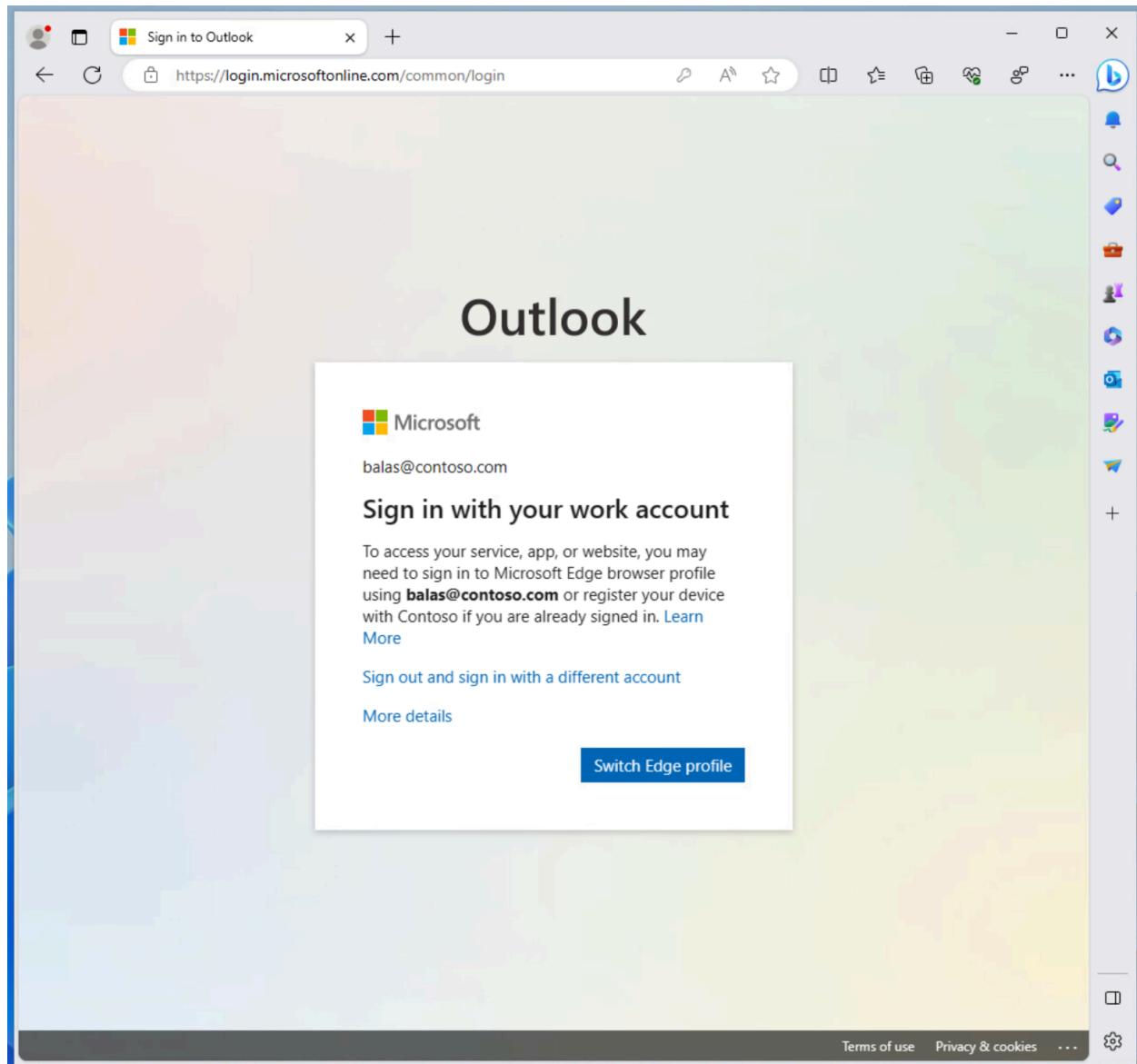
 No

[Provide product feedback ↗](#)

Require an app protection policy on Windows devices

Article • 04/01/2025

App protection policies apply [mobile application management \(MAM\)](#) to specific applications on a device. These policies allow for securing data within an application in support of scenarios like bring your own device (BYOD).



Prerequisites

- We support applying policy to the Microsoft Edge browser on devices running Windows 11 and Windows 10 version 20H2 and higher with KB5031445.
- [Configured app protection policy targeting Windows devices](#).
- Currently unsupported in sovereign clouds.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Create a Conditional Access policy

The following policy is put in to [Report-only mode](#) to start so administrators can determine the impact they have on existing users. When administrators are comfortable that the policy applies as they intend, they can switch to **On** or stage the deployment by adding specific groups and excluding others.

Require app protection policy for Windows devices

The following steps help create a Conditional Access policy requiring an app protection policy when using a Windows device accessing the Office 365 apps grouping in Conditional Access. The app protection policy must also be configured and assigned to your users in Microsoft Intune. For more information about how to create the app protection policy, see the article [App protection policy settings for Windows](#). The following policy includes multiple controls allowing devices to either use app protection policies for mobile application management (MAM) or be managed and compliant with mobile device management (MDM) policies.



Tip

App protection policies (MAM) support unmanaged devices:

- If a device is already managed through mobile device management (MDM), then Intune MAM enrollment is blocked, and app protection policy settings aren't applied.
- If a device becomes managed after MAM enrollment, app protection policy settings are no longer applied.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose at least your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **Office 365**.
7. Under **Conditions**:
 - a. **Device platforms** set **Configure** to **Yes**.
 - i. Under **Include**, Select **device platforms**.
 - ii. Choose **Windows** only.
 - iii. Select **Done**.
 - b. **Client apps** set **Configure** to **Yes**.
 - i. Select **Browser** only.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require app protection policy** and **Require device to be marked as compliant**.
 - b. For multiple controls select **Require one of the selected controls**
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

Note

If you set to **Require all the selected controls** or just use the **Require app protection policy** control alone, you need to make sure that you only target unmanaged devices or that the devices are not MDM managed. Otherwise, the

policy will block access to all applications since it cannot assess whether the application is compliant as per policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

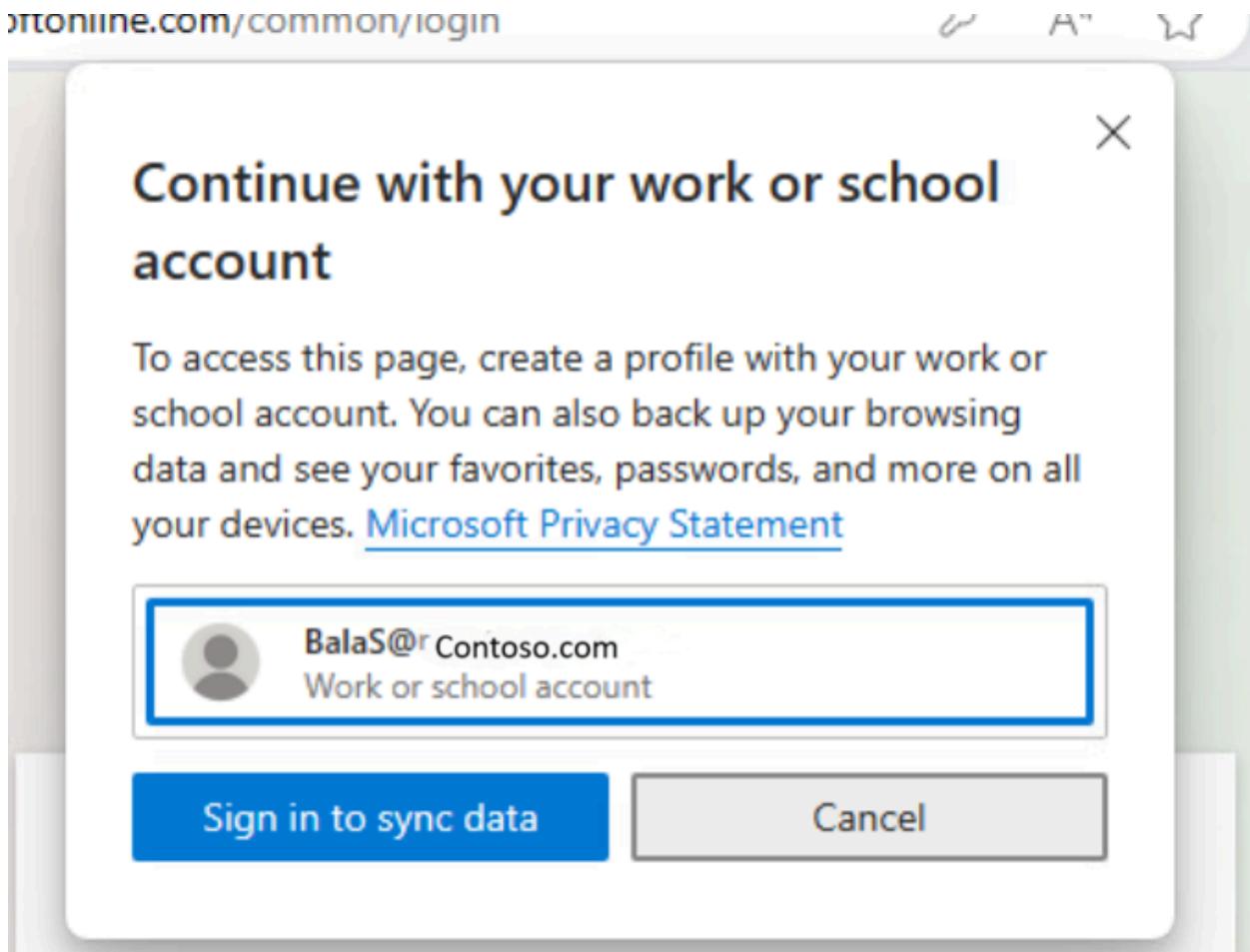
 **Tip**

Organizations should also deploy a policy that [blocks access from unsupported or unknown device platforms](#) along with this policy.

Sign in to Windows devices

When users attempt to sign in to a site that is protected by an app protection policy for the first time, they're prompted: To access your service, app, or website, you might need to sign in to Microsoft Edge using `username@domain.com` or register your device with `organization` if you're already signed in.

Clicking on **Switch Edge profile** opens a window listing their Work or school account along with an option to **Sign in to sync data**.

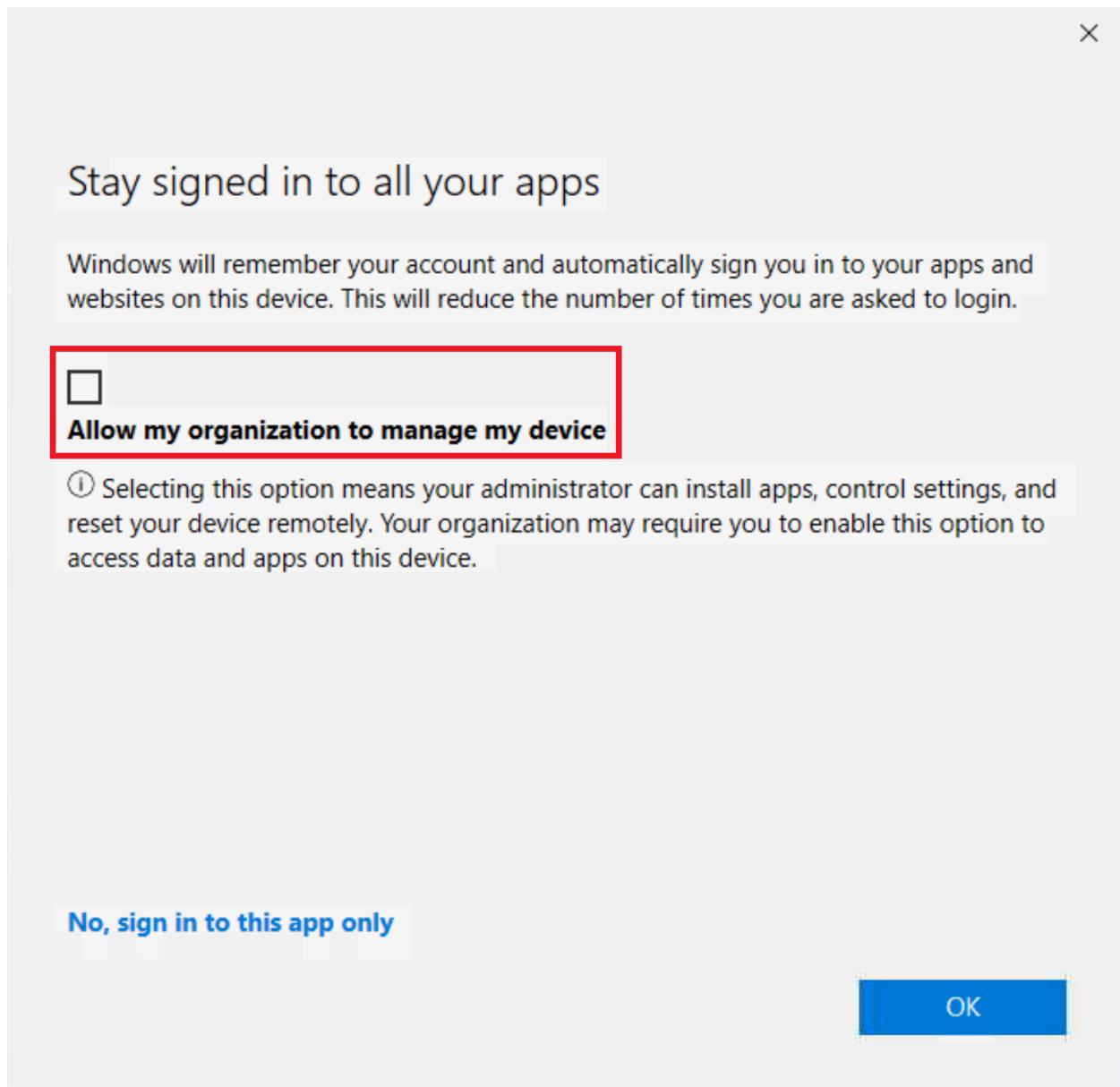


This process opens a window offering to allow Windows to remember your account and automatically sign you in to your apps and websites.

 **Caution**

You must **CLEAR THE CHECKBOX Allow my organization to manage my device**. Leaving this checked enrolls your device in mobile device management (MDM) not mobile application management (MAM).

Don't select **No, sign in to this app only**.



After selecting **OK**, you might see a progress window while policy is applied. After a few moments, you should see a window saying **You're all set**, app protection policies are applied.

Troubleshooting

Common issues

In some circumstances, after getting the "you're all set" page you might still be prompted to sign in with your work account. This prompt might happen when:

- Your profile is added to Microsoft Edge, but MAM enrollment is still being processed.
- Your profile is added to Microsoft Edge, but you selected "this app only" on the heads up page.
- You enrolled into MAM but your enrollment expired or you aren't compliant with your organization's requirements.

To resolve these possible scenarios:

- Wait a few minutes and try again in a new tab.
- Contact your administrator to check that Microsoft Intune MAM policies are applying to your account correctly.

Existing account

There's a known issue where there's a pre-existing, unregistered account, like `user@contoso.com` in Microsoft Edge, or if a user signs in without registering using the Heads Up Page, then the account isn't properly enrolled in MAM. This configuration blocks the user from being properly enrolled in MAM.

Next steps

- [What is Microsoft Intune app management?](#)
- [App protection policies overview](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Use application enforced restrictions for unmanaged devices

Article • 04/01/2025

This policy can help organizations accomplish the following initiatives:

- Block or limit access to a specific SharePoint site or OneDrive
- Limit access to email attachments in Outlook on the web and the new Outlook for Windows
- Enforce idle session timeout on unmanaged devices

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or break-glass accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

1. Sign in to the Microsoft Entra admin center  as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps)**, select the following options:
 - a. Under **Include**, choose **Select resources**.
 - b. Choose **Office 365**, then select **Select**.
7. Under **Access controls > Session**, select **Use app enforced restrictions**, then select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Next steps

[Conditional Access templates](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions](#).

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) 

Block unknown or unsupported device platform

Article • 04/03/2025

Users are blocked from accessing company resources when the device type is unknown or unsupported.

The [device platform condition](#) is based on user agent strings. Conditional Access policies using this condition should be used with another policy, like one requiring device compliance or app protection policies, to mitigate the risk of user agent spoofing.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Conditions**, select **Device platforms**
 - a. Set **Configure** to **Yes**.
 - b. Under **Include**, select **Any device**
 - c. Under **Exclude**, select **Android, iOS, Windows, and macOS**.

 **Note**

For this exclusion, select any platforms that your organization uses, and leave the others unselected.

- d. Select, **Done**.
8. Under **Access controls > Grant**, select **Block access**, then select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Next steps

- [Conditional Access templates](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions](#).

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Require compliant device or Microsoft Entra hybrid joined device for administrators

Article • 04/01/2025

Accounts that are assigned administrative rights are a target for attackers. Requiring users with these highly privileged rights to perform actions from devices marked as compliant or Microsoft Entra hybrid joined can help limit possible exposure.

More information about device compliance policies can be found in the article, [Set rules on devices to allow access to resources in your organization using Intune](#).

Requiring a Microsoft Entra hybrid joined device is dependent on your devices already being Microsoft Entra hybrid joined. For more information, see the article [Configure Microsoft Entra hybrid join](#).

Microsoft recommends you require phishing-resistant multifactor authentication on the following roles at a minimum:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

Organizations can choose to include or exclude roles as they see fit.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require multifactor authentication, devices accessing resources be marked as compliant with your organization's Intune compliance policies, or be Microsoft Entra hybrid joined.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **Directory roles** and choose at least the previously listed roles.

 **Warning**

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](#) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Access controls > Grant**.
 - a. Select **Require device to be marked as compliant**, and **Require Microsoft Entra hybrid joined device**
 - b. **For multiple controls** select **Require one of the selected controls**.
 - c. Select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Note**

You can enroll your new devices to Intune even if you select **Require device to be marked as compliant** for **All users** and **All resources (formerly 'All cloud apps')** using the previous steps. **Require device to be marked as compliant** control does not block Intune enrollment.

Known behavior

On Windows 7, iOS, Android, macOS, and some non-Microsoft web browsers, Microsoft Entra ID identifies the device using a client certificate that is provisioned when the device is registered with Microsoft Entra ID. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

Subscription activation

Organizations that use the [Subscription Activation](#) feature to enable users to "step-up" from one version of Windows to another, might want to exclude the Windows Store for Business, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f from their device compliance policy.

Related content

- Microsoft Entra built-in roles
 - Conditional Access templates
 - Device compliance policies work with Microsoft Entra ID
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Require a compliant device, Microsoft Entra hybrid joined device, or multifactor authentication for all users

Article • 04/01/2025

Organizations who deploy Microsoft Intune can use the information returned from their devices to identify devices that meet compliance requirements such as:

- Requiring a PIN to unlock
- Requiring device encryption
- Requiring a minimum or maximum operating system version
- Requiring a device isn't jailbroken or rooted

Policy compliance information is sent to Microsoft Entra ID where Conditional Access decides to grant or block access to resources. More information about device compliance policies can be found in the article, [Set rules on devices to allow access to resources in your organization using Intune](#)

Requiring a Microsoft Entra hybrid joined device is dependent on your devices already being Microsoft Entra hybrid joined. For more information, see the article [Configure Microsoft Entra hybrid join](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access

policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.

- If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require multifactor authentication, devices accessing resources be marked as compliant with your organization's Intune compliance policies, or be Microsoft Entra hybrid joined.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**:
 - i. Select **Users and groups**
 - i. Choose your organization's emergency access or break-glass accounts.
 - ii. If you use hybrid identity solutions like Microsoft Entra Connect or Microsoft Entra Connect Cloud Sync, select **Directory roles**, then select **Directory Synchronization Accounts**
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
 - a. If you must exclude specific applications from your policy, you can choose them from the **Exclude** tab under **Select excluded cloud apps** and choose **Select**.
7. Under **Access controls > Grant**.
 - a. Select **Require multifactor authentication**, **Require device to be marked as compliant**, and **Require Microsoft Entra hybrid joined device**
 - b. For multiple controls select **Require one of the selected controls**.
 - c. Select **Select**.
8. Confirm your settings and set **Enable policy to Report-only**.

9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Note**

You can enroll your new devices to Intune even if you select **Require device to be marked as compliant** for **All users** and **All resources** (formerly 'All cloud apps') using the previous steps. **Require device to be marked as compliant** control doesn't block Intune enrollment and the access to the Microsoft Intune Web Company Portal application.

Known behavior

On iOS, Android, macOS, and some non-Microsoft web browsers, Microsoft Entra ID identifies the device using a client certificate that is provisioned when the device is registered with Microsoft Entra ID. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.

Subscription activation

Organizations that use the Subscription Activation feature to enable users to "step-up" from one version of Windows to another and use Conditional Access policies to control access need to exclude one of the following cloud apps from their Conditional Access policies using **Select Excluded Cloud Apps**:

- [Universal Store Service APIs and Web Application, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f](#).
- [Windows Store for Business, AppID 45a330b1-b1ec-4cc1-9161-9f03992aa49f](#).

Although the app ID is the same in both instances, the name of the cloud app depends on the tenant.

When a device is offline for an extended period of time, the device might not reactivate automatically if this Conditional Access exclusion isn't in place. Setting this Conditional Access exclusion ensures that Subscription Activation continues to work seamlessly.

Starting with Windows 11, version 23H2 with [KB5034848](#) or later, users are prompted for authentication with a toast notification when Subscription Activation needs to

reactivate. The toast notification shows the following message:

Your account requires authentication

Please sign in to your work or school account to verify your information.

Additionally, in the **Activation** pane, the following message might appear:

Please sign in to your work or school account to verify your information.

The prompt for authentication usually occurs when a device is offline for an extended period of time. This change eliminates the need for an exclusion in the Conditional Access policy for Windows 11, version 23H2 with [KB5034848](#) or later. A Conditional Access policy can still be used with Windows 11, version 23H2 with [KB5034848](#) or later if the prompt for user authentication via a toast notification isn't desired.

Next steps

[Conditional Access templates](#)

[Determine effect using Conditional Access report-only mode](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

[Device compliance policies work with Microsoft Entra ID](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Require reauthentication and disable browser persistence

Article • 04/03/2025

Protect user access on unmanaged devices by preventing browser sessions from remaining signed in after the browser is closed and setting a sign-in frequency to 1 hour.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).

2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Conditions > Filter for devices**, set **Configure** to **Yes**.
 - a. Under **Devices matching the rule:**, set to **Include filtered devices in policy**.
 - b. Under **Rule syntax** select the **Edit** pencil and paste the following expressing in the box, then select **Apply**.
 - i. device.trustType -ne "ServerAD" -or device.isCompliant -ne True
 - c. Select **Done**.
8. Under **Access controls > Session**
 - a. Select **Sign-in frequency**, specify **Periodic reauthentication**, and set the duration to **1** and the period to **Hours**.
 - b. Select **Persistent browser session**, and set **Persistent browser session** to **Never persistent**.
 - c. Select, **Select**
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Next steps

[Conditional Access templates](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Require multifactor authentication for Intune device enrollments

Article • 03/03/2025

Applies to:

- Android
- iOS/iPadOS
- macOS
- Windows 10
- Windows 11

You can use Intune together with Microsoft Entra Conditional Access policies to require multifactor authentication (MFA) during device enrollment. If you require MFA, employees and students wanting to enroll devices must first authenticate with a second device and two forms of credentials. MFA requires them to authenticate using two or more of these verification methods:

- Something they know, such as a password or PIN.
- Something they have that can't be duplicated, such as a trusted device or phone.
- Something they are, such as a fingerprint.

If a device isn't compliant, the device user is prompted to make the device compliant before enrolling in Microsoft Intune.

Prerequisites

To implement this policy, you must assign Microsoft Entra ID P1 or later to users.

Configure Intune to require multifactor authentication at device enrollment

Complete these steps to enable multifactor authentication during Microsoft Intune enrollment.

 **Important**

Don't configure **Device based access rules** for Microsoft Intune enrollment.

1. Sign in to the [Microsoft Intune admin center](#).

2. Go to Devices.
3. Expand **Manage devices**, and then select **Conditional Access**. This Conditional Access area is the same as the Conditional Access area available in the Microsoft Entra admin center. For more information about the available settings, see [Building a Conditional Access policy](#).
4. Choose **Create new policy**.
5. Name your policy.
6. Select the **Users** category.
 - a. Under the **Include** tab, choose **Select users or groups**.
 - b. Additional options appear. Select **Users and groups**. A list of users and groups opens.
 - c. Browse and select the Microsoft Entra users or groups you want to include in the policy. Then choose **Select**.
 - d. To exclude users or groups from the policy, select the **Exclude** tab and add those users or groups like you did in the previous step.
7. Select the next category, **Target resources**. In this step, you select the resources that the policy applies to. In this case, we want the policy to apply to events where users or groups try to access the Microsoft Intune Enrollment app.
 - a. Under **Select what this policy applies to**, choose **Resources (formerly cloud apps)**.
 - b. Select the **Include** tab.
 - c. Choose **Select resources**. Additional options appear.
 - d. Under **Select**, choose **None**. A list of resources open.
 - e. Search for **Microsoft Intune Enrollment**. Then choose **Select** to add the app.

For Apple automated device enrollments using Setup Assistant with modern authentication, you have two options to choose from. The following table describes the difference between the *Microsoft Intune* option and *Microsoft Intune Enrollment* option.

 [Expand table](#)

Cloud app	MFA prompt location	Automated Device Enrollment notes
Microsoft Intune	Setup Assistant, Company Portal app	With this option, MFA is required during enrollment and each time the user signs into the Company Portal app or website. The MFA prompts appear on the Company Portal sign-in page.
Microsoft Intune Enrollment	Setup Assistant	With this option, MFA is required during device enrollment and appears as a one-time MFA prompt on the Company Portal sign-in page.

 **Note**

The Microsoft Intune Enrollment cloud app isn't created automatically for new tenants. To add the app for new tenants, a Microsoft Entra administrator must create a service principal object, with app ID d4ebce55-015a-49b5-a083-c84d1797ae8c, in PowerShell or Microsoft Graph.

8. Select the **Grant** category. In this step, you grant or block access to the Microsoft Intune Enrollment app.
 - a. Choose **Grant access**.
 - b. Select **Require multifactor authentication**.
 - c. Select **Require device to be marked as compliant**.
 - d. Under **For multiple controls**, select **Require all the selected controls**.
 - e. Choose **Select**.
9. Select the **Session** category. In this step, you can make use of session controls to enable limited experiences within the Microsoft Intune Enrollment app.
 - a. Select **Sign-in frequency**. Additional options appear.
 - b. Choose **Every time**.
 - c. Choose **Select**.
10. For **Enable policy**, select **On**.
11. Select **Create** to save and create your policy.

After you apply and deploy this policy, device users enrolling their devices see a one-time MFA prompt.

 **Note**

A second device or a Temporary Access Pass is required to complete the MFA challenge for these types of corporate-owned devices:

- Android Enterprise fully managed devices
- Android Enterprise corporate-owned devices with a work profile
- iOS/iPadOS devices enrolled via Apple automated device enrollment
- macOS devices enrolled via Apple automated device enrollment

The second device is required because the primary device can't receive calls or text messages during the provisioning process.

Require MFA for administrators

Article • 04/03/2025

Accounts that are assigned administrative rights are targeted by attackers. Requiring multifactor authentication (MFA) on those accounts is an easy way to reduce the risk of those accounts being compromised.

Microsoft recommends you require phishing-resistant multifactor authentication on the following roles at a minimum:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

Organizations can choose to include or exclude roles as they see fit.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or **break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic

access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.

- If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require those assigned administrative roles to perform multifactor authentication. Some organizations might be ready to move to stronger authentication methods for their administrators. These organizations might choose to implement a policy like the one described in the article [Require phishing-resistant multifactor authentication for administrators](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **Directory roles** and choose at least the previously listed roles.

⚠ Warning

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](#) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.

6. Under Target resources > Resources (formerly cloud apps) > Include, select All resources (formerly 'All cloud apps').
7. Under Access controls > Grant, select Grant access, Require multifactor authentication, and select Select.
8. Confirm your settings and set Enable policy to Report-only.
9. Select Create to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- [Microsoft Entra built-in roles](#)
 - [Conditional Access templates](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Require multifactor authentication for guest access

Article • 04/01/2025

Require guest users perform multifactor authentication when accessing your organization's resources. Some organizations might be ready to move to stronger authentication methods for their guest users. These organizations might choose to implement a policy like the one described in the article [Require multifactor authentication strength for external users](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

1. Sign in to the Microsoft Entra admin center  as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All guest and external users**
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
 - a. Under **Exclude**, select any applications that don't require multifactor authentication.
7. Under **Access controls > Grant**, select **Grant access**, **Require multifactor authentication**, and select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Next steps

[Conditional Access templates](#)

Use report-only mode for Conditional Access to determine the results of new policy decisions.

Feedback

Was this page helpful?



Yes



No

[Provide product feedback !\[\]\(30bfb0e300a4285fd19011628f0d7066_img.jpg\)](#)

Require multifactor authentication for admins accessing Microsoft admin portals

Article • 04/01/2025

Microsoft recommends securing access to any Microsoft admin portals like Microsoft Entra, Microsoft 365, Exchange, and Azure. Using the [Microsoft Admin Portals](#) app organizations can control interactive access to Microsoft admin portals.

Microsoft recommends you require phishing-resistant multifactor authentication on the following roles at a minimum:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access** or break-glass accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).

- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **Directory roles** and choose at least the previously listed roles.

⚠ Warning

Conditional Access policies support built-in roles. Conditional Access policies are not enforced for other role types including [administrative unit-scoped](#) or [custom roles](#).

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include, Select resources**, select **Microsoft Admin Portals**.
7. Under **Access controls > Grant**, select **Grant access, Require authentication strength**, select **Multifactor authentication**, then select **Select**.

8. Confirm your settings and set **Enable policy** to **Report-only**.

9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- Microsoft Entra built-in roles
 - Conditional Access templates
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Require MFA for Azure management

Article • 04/03/2025

Organizations use many Azure services and manage them from Azure Resource Manager based tools like:

- Azure portal
- Azure PowerShell
- Azure CLI

These tools can provide highly privileged access to resources that can make the following changes:

- Alter subscription-wide configurations
- Service settings
- Subscription billing

To protect these privileged resources, Microsoft recommends requiring multifactor authentication for any user accessing these resources. In Microsoft Entra ID, these tools are grouped together in a suite called [Windows Azure Service Management API](#). For Azure Government, this suite should be the Azure Government Cloud Management API app.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.

- If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Create a Conditional Access policy

The following steps help create a Conditional Access policy to require users who access the [Windows Azure Service Management API](#) suite do multifactor authentication.

Caution

Make sure you understand how Conditional Access works before setting up a policy to manage access to Windows Azure Service Management API. Make sure you don't create conditions that could block your own access to the portal.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**, choose **Windows Azure Service Management API**, and select **Select**.
7. Under **Access controls > Grant**, select **Grant access, Require multifactor authentication**, and select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Next steps

[Conditional Access templates](#)

Use report-only mode for Conditional Access to determine the results of new policy decisions.

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Protect AI with Conditional Access policy

Article • 04/03/2025

Generative Artificial Intelligence (AI) services like [Microsoft Security Copilot](#) and [Microsoft 365 Copilot](#) when used appropriately bring value to your organization.

Protecting these services from misuse can be accomplished with existing features like Microsoft Entra Conditional Access policy.

Applying Conditional Access policy to these Generative AI services can be accomplished through your existing policies that target all resources for [all users](#), [risky users](#) or [sign-ins](#), and users with [insider risk](#).

This article shows you how to target specific Generative AI services like Microsoft Security Copilot and Microsoft 365 Copilot for policy enforcement.

Create targetable service principals using PowerShell

To individually target these Generative AI services, organizations must create the following service principals to make them available in the Conditional Access app picker. The following steps show how to add these service principals using the [New-MgServicePrincipal](#) cmdlet, part of the [Microsoft Graph PowerShell SDK](#).

PowerShell

```
# Connect with the appropriate scopes to create service principals
Connect-MgGraph -Scopes "Application.ReadWrite.All"

# Create service principal for the service Enterprise Copilot Platform
# (Microsoft 365 Copilot)
New-MgServicePrincipal -AppId fb8d773d-7ef8-4ec0-a117-179f88add510

# Create service principal for the service Security Copilot (Microsoft
# Security Copilot)
New-MgServicePrincipal -AppId bb5ffd56-39eb-458c-a53a-775ba21277da
```

Create Conditional Access policies

As an organization adopting services like Microsoft 365 Copilot and Microsoft Security Copilot, you want to ensure access is only by those users who meet your security

requirements. For example:

- All users of Generative AI services must complete phishing-resistant MFA
- All users of Generative AI services must access from a compliant device when insider risk is moderate
- All users of Generative AI services are blocked when insider risk is elevated

 **Tip**

The following Conditional Access policies target the [standalone experiences, not embedded experiences](#).

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts and Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

All users of Generative AI services must complete phishing-resistant MFA

The following steps help create a Conditional Access policy to require all users do multifactor authentication using the authentication strength policy.

 **Warning**

If you use [external authentication methods](#), these are currently incompatible with authentication strength and you should use the [Require multifactor authentication](#) grant control.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude** select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**, select:
 - a. **Enterprise Copilot Platform** fb8d773d-7ef8-4ec0-a117-179f88add510
(Microsoft 365 Copilot)
 - b. **Security Copilot** bb5ffd56-39eb-458c-a53a-775ba21277da (Microsoft Security Copilot)
7. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require authentication strength**, then select the built-in **Phishing-resistant MFA** authentication strength from the list.
 - b. Select **Select**.
8. Confirm your settings and set **Enable policy** to **Report-only**.
9. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

All users of Generative AI services must access from a compliant device when insider risk is moderate

 **Tip**

Configure [adaptive protection](#) before you create the following policy.

Without a [compliance policy created in Microsoft Intune](#) this Conditional Access policy will not function as intended. Create a compliance policy first and ensure you have at least one compliant device before proceeding.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**
 - b. Under **Exclude**:
 - i. Select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - ii. Select **Guest or external users** and choose the following:
 - i. **B2B direct connect users**.
 - ii. **Service provider users**.
 - iii. **Other external users**.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**, select:
 - a. **Enterprise Copilot Platform** fb8d773d-7ef8-4ec0-a117-179f88add510 (Microsoft 365 Copilot)
 - b. **Security Copilot** bb5ffd56-39eb-458c-a53a-775ba21277da (Microsoft Security Copilot)
7. Under **Conditions > Insider risk**, set **Configure** to **Yes**.
 - a. Under **Select the risk levels that must be assigned to enforce the policy**.
 - i. Select **Moderate**.
 - ii. Select **Done**.
8. Under **Access controls > Grant**.
 - a. Select **Require device to be marked as compliant**.
 - b. Select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

All users of Generative AI services are blocked when insider risk is elevated

 **Tip**

Configure [adaptive protection](#) before you create the following policy.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**:
 - i. Select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - ii. Select **Guest or external users** and choose the following:
 - i. **B2B direct connect users**.
 - ii. **Service provider users**.
 - iii. **Other external users**.
6. Under **Target resources > Resources (formerly cloud apps) > Include > Select resources**, select:
 - a. **Enterprise Copilot Platform** fb8d773d-7ef8-4ec0-a117-179f88add510 (Microsoft 365 Copilot)
 - b. **Security Copilot** bb5ffd56-39eb-458c-a53a-775ba21277da (Microsoft Security Copilot)
7. Under **Conditions > Insider risk**, set **Configure** to **Yes**.
 - a. Under **Select the risk levels that must be assigned to enforce the policy**.
 - i. Select **Elevated**.
 - ii. Select **Done**.
8. Under **Access controls > Grant**, select **Block access**, then select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related content

- Use report-only mode for Conditional Access to determine the results of new policy decisions.
- Secure Generative AI with Microsoft Entra
- Microsoft Purview data security and compliance protections for generative AI apps
- Considerations for Microsoft Purview AI Hub and data security and compliance protections for Copilot
- Apply principles of Zero Trust to Microsoft Copilot

- Apply principles of Zero Trust to Microsoft 365 Copilot
 - Apply principles of Zero Trust to Microsoft Security Copilot
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Block access for users with insider risk

Article • 04/01/2025

Most users have a normal behavior that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in. You might want to block that user or ask them to review a specific [terms of use policy](#). Microsoft Purview can provide an [insider risk signal](#) to Conditional Access to refine access control decisions. Insider risk management is part of [Microsoft Purview](#). You must enable it before you can use the signal in Conditional Access.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, Show more, Protection (Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes), Risky activities, Learn & support, and a Done button. The main content area displays a Conditional Access policy titled "Block access to Office365 apps for users with insider risk". The policy details include:

- Name:** Block access to Office365 apps for users with insider risk
- Assignments:** All users included and specific users excluded
- Target resources:** 1 app included
- Network:** NEW (Not configured)
- Conditions:** 1 condition selected
- Access controls:** Grant (Block access), Session (0 controls selected)
- Enable policy:** Report-only (On)

A modal window titled "Insider risk" is open on the right, explaining that it assesses user activity in Microsoft Purview Insider Risk Management. It includes a "Configure" section with "Yes" selected, and a "Select the risk levels that must be assigned to enforce the policy" section where "Elevated" is checked. A note at the bottom states: "The insider risk condition requires configuration in Adaptive Protection. Go to Microsoft Purview".

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.

- More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Template deployment

Organizations can choose to deploy this policy using the steps outlined below or using the [Conditional Access templates](#).

Block access with Conditional Access policy

Tip

Configure [adaptive protection](#) before you create the following policy.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**:
 - i. Select **Users and groups** and choose your organization's emergency access or break-glass accounts.
 - ii. Select **Guest or external users** and choose the following:
 - i. **B2B direct connect users**.
 - ii. **Service provider users**.
 - iii. **Other external users**.

6. Under Target resources > Resources (formerly cloud apps) > Include, select All resources (formerly 'All cloud apps').
7. Under Conditions > Insider risk, set Configure to Yes.
 - a. Under Select the risk levels that must be assigned to enforce the policy.
 - i. Select Elevated.
 - ii. Select Done.
8. Under Access controls > Grant, select Block access, then select Select.
9. Confirm your settings and set Enable policy to Report-only.
10. Select Create to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Some administrators might create other Conditional Access policies that use other access controls, like terms of use on lower levels of insider risk.

Related content

- [Dynamically mitigate risks with adaptive protection](#)
- [Insider risk as a condition](#)
- [Determine effect using Conditional Access report-only mode](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Require terms of use to be accepted before accessing Microsoft Admin Portals

Article • 04/03/2025

Organizations might want to require users to accept [terms of use \(ToU\)](#) before accessing certain applications in their environment. This example helps you create a policy requiring terms of use to be accepted as part of the initial sign in process for administrators who access any of the [Microsoft Admin Portals](#).

Create your terms of use

This section provides you with the steps to create a sample terms of use document. When you create a terms of use document, you select a value for **Enforce with Conditional Access policy templates**. Selecting **Custom policy** opens a dialog to create a new Conditional Access policy as soon as your terms of use is created.

1. Create a new terms of use document and save it as a PDF file.
2. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
3. Browse to **Protection > Conditional Access > Terms of use**.
4. In the menu on the top, select **New terms**.
5. In the **Name** textbox, provide a name for your terms of use policy.
6. Upload your terms of use PDF file.
 - a. Select your default language.
 - b. In the **Display name** textbox, type the name you want to be displayed.
7. For **Require users to expand the terms of use**, select **On**.
8. For **Enforce with Conditional Access policy templates**, select **Custom policy**.
9. Select **Create**.

Create a Conditional Access policy

This section shows how to create the required Conditional Access policy.

To configure your Conditional Access policy:

1. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
2. Under **Assignments**, select **Users or workload identities**.

- a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
3. Under **Target resources > Resources (formerly cloud apps)**, select the following options:
 - a. Under **Include**, choose **Select resources**.
 - b. Select **Microsoft Admin Portals**, and then choose **Select**.
 4. Under **Access controls**, select **Grant**.
 - a. Select **Grant access**.
 - b. Select the terms of use you created previously and choose **Select**.
 5. Confirm your settings and set **Enable policy** to **Report-only**.
 6. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Test your Conditional Access policy

In the previous section, you created a Conditional Access policy requiring terms of use be accepted when accessing any of the [Microsoft Admin Portals](#).

To test your policy, try to sign in to the [Microsoft Entra admin center](#) using a test account. You should see a dialog that requires you to accept your terms of use.

Related content

[Microsoft Entra terms of use](#)

[Conditional Access templates](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Block access by location

Article • 04/03/2025

With the location condition in Conditional Access, you can control access to your cloud apps based on the network location of a user. The location condition is commonly used to block access from countries/regions where your organization knows traffic shouldn't come from. For more information about IPv6 support, see the article [IPv6 support in Microsoft Entra ID](#).

ⓘ Note

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Named locations**.
3. Choose the type of location to create.
 - **Countries location or IP ranges location**.
 - Give your location a name.
4. Provide the **IP ranges** or select the **Countries/Regions** for the location you're specifying.
 - If you select IP ranges, you can optionally **Mark as trusted location**.
 - If you choose Countries/Regions, you can optionally choose to include unknown areas.
5. Select **Create**

More information about the location condition in Conditional Access can be found in the article, [What is the location condition in Microsoft Entra Conditional Access](#)

Create a Conditional Access policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.

3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**.
7. Under **Network**.
 - a. Set **Configure** to **Yes**
 - b. Under **Include**, select **Selected networks and locations**
 - i. Select the blocked location you created for your organization.
 - ii. Click **Select**.
8. Under **Access controls** > select **Block Access**, and click **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Related Content

- [Conditional Access templates](#)
- [Determine effect using Conditional Access report-only mode](#)
- [Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Block access example policy

Article • 04/03/2025

For organizations with a conservative cloud migration approach, the block all policy is an option that can be used.

✖ Caution

Misconfiguration of a block policy can lead to organizations being locked out.

Policies like these can have unintended side effects. Proper testing and validation are vital before enabling. Administrators should utilize tools such as [Conditional Access report-only mode](#) and [the What If tool in Conditional Access](#) when making changes.

User exclusions

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policies:

- **Emergency access or break-glass** accounts to prevent lockout due to policy misconfiguration. In the unlikely scenario all administrators are locked out, your emergency-access administrative account can be used to log in and take steps to recover access.
 - More information can be found in the article, [Manage emergency access accounts in Microsoft Entra ID](#).
- **Service accounts** and **Service principals**, such as the Microsoft Entra Connect Sync Account. Service accounts are non-interactive accounts that aren't tied to any particular user. They're normally used by back-end services allowing programmatic access to applications, but are also used to sign in to systems for administrative purposes. Calls made by service principals won't be blocked by Conditional Access policies scoped to users. Use Conditional Access for workload identities to define policies targeting service principals.
 - If your organization has these accounts in use in scripts or code, consider replacing them with [managed identities](#).

Create a Conditional Access policy

The following steps help create Conditional Access policies to block access to all apps except for [Office 365](#) if users aren't on a trusted network. These policies are put in to

[Report-only mode](#) to start so administrators can determine the impact on existing users.

When administrators are comfortable that the policies apply as they intend, they can switch them to **On**.

The first policy blocks access to all apps except for Microsoft 365 applications if not on a trusted location.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
6. Under **Target resources > Resources (formerly cloud apps)**, select the following options:
 - a. Under **Include**, select **All resources (formerly 'All cloud apps')**.
 - b. Under **Exclude**, select **Office 365**, select **Select**.
7. Under **Conditions**:
 - a. Under **Conditions > Location**.
 - i. Set **Configure** to **Yes**
 - ii. Under **Include**, select **Any location**.
 - iii. Under **Exclude**, select **All trusted locations**.
 - b. Under **Client apps**, set **Configure** to **Yes**, and select **Done**.
8. Under **Access controls > Grant**, select **Block access**, then select **Select**.
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

The following policy is created to require multifactor authentication or a compliant device for users of Microsoft 365.

1. Select **Create new policy**.
2. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
3. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.

- b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.
4. Under **Target resources** > **Resources (formerly cloud apps)** > **Include** > **Select resources**, choose **Office 365**, and select **Select**.
5. Under **Access controls** > **Grant**, select **Grant access**.
 - a. Select **Require multifactor authentication** and **Require device to be marked as compliant** select **Select**.
 - b. Ensure **Require one of the selected controls** is selected.
 - c. Select **Select**.
6. Confirm your settings and set **Enable policy** to **Report-only**.
7. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Note**

Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

Next steps

[Conditional Access templates](#)

[Determine effect using Conditional Access report-only mode](#)

[Use report-only mode for Conditional Access to determine the results of new policy decisions.](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft-managed Conditional Access policies

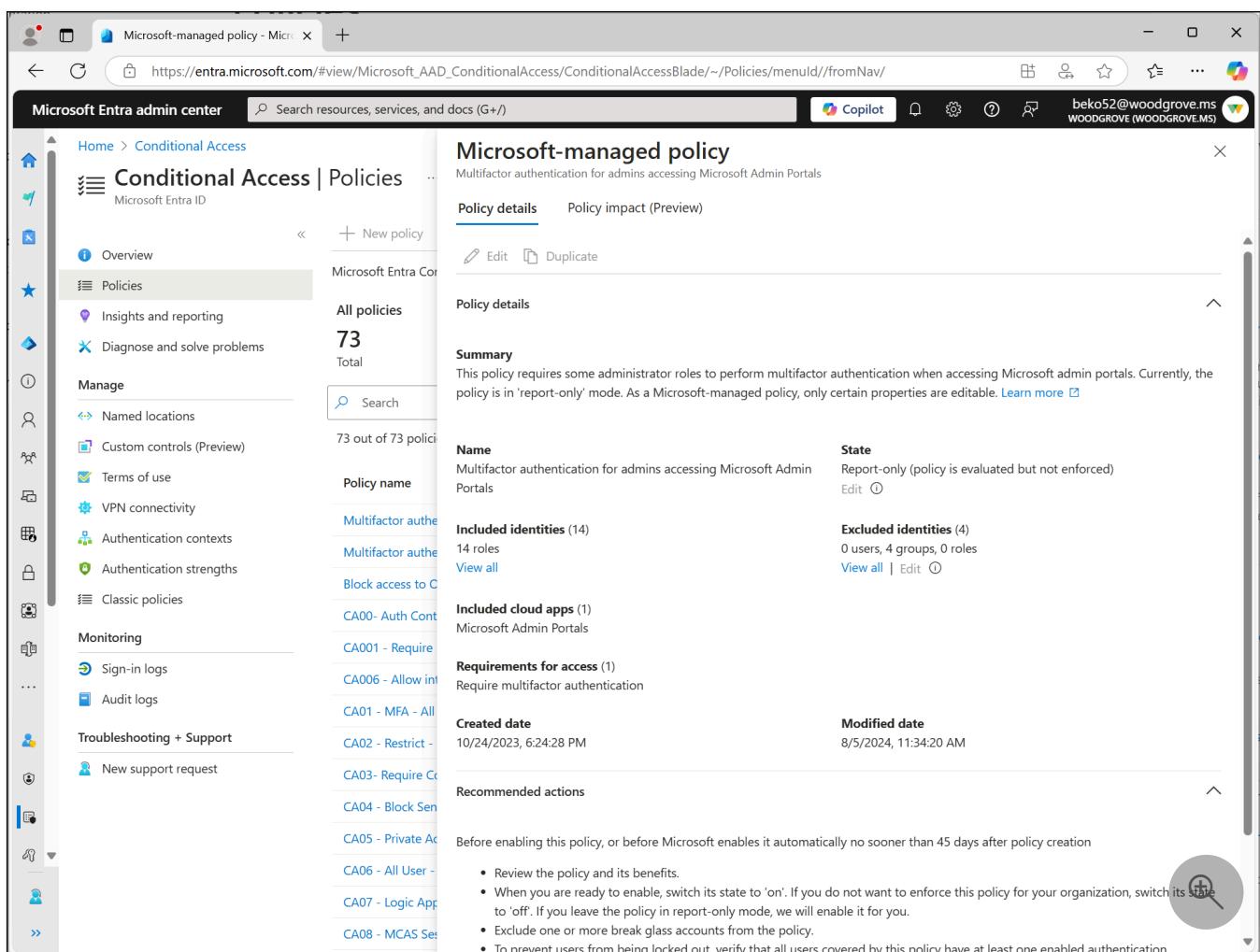
Article • 04/21/2025

As mentioned in the [Microsoft Digital Defense Report](#) from October 2023,

...threats to digital peace have reduced trust in technology and highlighted the urgent need for improved cyber defenses at all levels...

...at Microsoft, our more than 10,000 security experts analyze over 65 trillion signals each day... driving some of the most influential insights in cybersecurity. Together, we can build cyber resilience through innovative action and collective defense.

As part of this work, we're making Microsoft-managed policies available in Microsoft Entra tenants around the world. These [simplified Conditional Access policies](#) require multifactor authentication, which a [recent study](#) finds reduces the risk of compromise by more than 99%.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various icons and links like Home, Conditional Access, Policies, Insights and reporting, Diagnose and solve problems, Manage, Monitoring, and Troubleshooting + Support. The main content area is titled "Conditional Access | Policies". It displays a summary of 73 policies, with 73 out of 73 policies listed. A specific policy named "Multifactor authentication for admins accessing Microsoft Admin Portals" is selected. The "Policy details" tab is active, showing the policy name, state (Report-only), included identities (14 roles), excluded identities (4 users, 0 groups, 0 roles), included cloud apps (Microsoft Admin Portals), requirements for access (Require multifactor authentication), and creation and modification dates. Below this, a "Recommended actions" section provides instructions for enabling the policy.

How Microsoft-managed policies work

Administrators with at least the [Conditional Access Administrator](#) role assigned find these policies in the [Microsoft Entra admin center](#) under **Protection > Conditional Access > Policies**.

You can edit the state of a policy and what identities the policy should exclude. Exclude your [break-glass or emergency access accounts](#) from managed policies just like other Conditional Access policies. Consider duplicating these policies if you need to make more changes than what's allowed in the Microsoft-managed policies.

Microsoft enables these policies no less than 45 days after they're introduced in your tenant if they're left in the **Report-only** state. You can turn on these policies sooner, or opt out by setting the policy state to **Off**. Customers are notified through emails and [Message center](#) posts 28 days before the policies are enabled.

Note

In some cases, policies might be enabled faster than 45 days. If this change applies to your tenant:

- It's mentioned in emails and Microsoft 365 message center posts you receive about Microsoft-managed policies.
- It's mentioned in the policy details in the Microsoft Entra admin center.

Policies

These Microsoft-managed policies allow administrators to make simple modifications like excluding users or turning them from report-only mode to on or off. Organizations can't rename or delete any Microsoft-managed policies. As administrators get more comfortable with Conditional Access policy, they might choose to duplicate the policy to create custom versions.

As threats evolve, Microsoft might update these policies to use new features, functionality, or improve their effectiveness

- [Block legacy authentication](#)
- [Block device code flow](#)
- [Multifactor authentication for admins accessing Microsoft Admin portals](#)
- [Multifactor authentication for all users](#)
- [Multifactor authentication for per-user multifactor authentication users](#)
- [Multifactor authentication and reauthentication for risky sign-ins](#)

Block legacy authentication

This policy blocks sign-in attempts using legacy authentication and legacy authentication protocols. These authentications might come from older clients like Office 2010, or clients that use protocols like IMAP, SMTP, or POP3.

Based on Microsoft's analysis, more than 99 percent of password spray attacks use these legacy authentication protocols. These attacks would stop with basic authentication disabled or blocked.

Block device code flow

This policy blocks device code flow, where a user initiates authentication on one device, completes on another, and their token is sent back to the original device. This type of authentication is common where users can't enter their credentials, like smart TVs, Microsoft Teams Room devices, IoT devices, or printers.

Device code flow is rarely used by customers, but is frequently used by attackers. Enabling this Microsoft-managed policy for your organization helps remove this attack vector.

Multifactor authentication for admins accessing Microsoft Admin portals

This policy covers [14 admin roles](#) that are highly privileged, who access the [Microsoft Admin Portals](#), and requires them to perform multifactor authentication.

This policy applies to Microsoft Entra ID P1 and P2 tenants where security defaults aren't enabled.

💡 Tip

Microsoft-managed policies requiring multifactor authentication differ from the [announcement of mandatory multifactor authentication for Azure sign-ins made in 2024](#), which started gradual rollout in October of 2024. For more information, see [Planning for mandatory multifactor authentication for Azure and other admin portals](#).

Multifactor authentication for all users

This policy covers all users in your organization and requires them to use multifactor authentication whenever they sign in. In most cases, the session persists on the device, and

users don't need to complete multifactor authentication when they interact with another application.

Multifactor authentication for per-user multifactor authentication users

This policy covers users [per-user MFA](#), a configuration that Microsoft no longer recommends. [Conditional Access](#) offers a better admin experience with many extra features. Consolidating all multifactor authentication policies to Conditional Access can help you be more targeted in requiring multifactor authentication, lowering end user friction while maintaining security posture.

This policy targets:

- Organizations with Microsoft Entra ID P1 and P2 licensed users
- Organizations where security defaults aren't enabled
- Organizations with less than 500 per-user MFA enabled or enforced users

To apply this policy to more users, duplicate it and change the assignments.

💡 Tip

Using the **Edit** pencil at the top to modify the Microsoft-managed per-user multifactor authentication policy might result in a **failed to update** error. To work around this issue, select **Edit** under the **Excluded identities** section of the policy.

Multifactor authentication and reauthentication for risky sign-ins

This policy covers all users and requires multifactor authentication and reauthentication when we detect high-risk sign-ins. High-risk in this case means something about the way the user signed in is out of the ordinary. These high-risk sign-ins might include travel that is highly abnormal, password spray attacks, or token replay attacks. For more information, see [What are risk detections](#).

This policy targets Microsoft Entra ID P2 tenants where security defaults aren't enabled. The policy covers users in two different ways, depending on if you have more P2 licenses than users or if you have more users than P2 licenses. Guest users aren't included in the policy.

- If all your active users have MFA and your P2 licenses equal or exceed the total active users, the policy covers *All Users*.

- *All Users* could include service accounts or break-glass accounts, so you might want to exclude them.
- If some active users don't have MFA, or if there aren't enough P2 licenses to cover all MFA-registered users, we create and assign the policy to a security group called "Conditional Access: Risky sign-in multifactor authentication" that is capped to your available P2 licenses.
 - The policy applies only to that security group, so you can scope the policy by modifying the group itself.
 - To populate the group, we select users who can satisfy MFA, prioritizing users with a directly assigned P2 license.
 - This setup ensures that the policy doesn't block legitimate users and that you're getting maximum value on your P2 licenses.

To prevent attackers from taking over accounts, Microsoft blocks risky users from registering for multifactor authentication.

Security defaults policies

The following policies are available for when you upgrade from using security defaults.

- [Block legacy authentication](#)
- [Require multifactor authentication for Azure management](#)
- [Require multifactor authentication for admins](#)
- [Require multifactor authentication for all users](#)

Block legacy authentication

This policy blocks legacy authentication protocols from accessing applications. Legacy authentication refers to an authentication request made by:

- Clients that don't use modern authentication (for example, an Office 2010 client)
- Any client that uses older mail protocols such as IMAP, SMTP, or POP3
- Any sign-in attempts to use legacy authentication.

Most observed compromising sign-in attempts come from legacy authentication. Because legacy authentication doesn't support multifactor authentication, attackers can bypass multifactor authentication requirements by using older protocols.

Require multifactor authentication for Azure management

This policy covers all users when they're trying to access various Azure services managed through the Windows Azure Service Management API including:

- Azure portal
- Microsoft Entra admin center
- Azure PowerShell
- Azure CLI

Users must complete multifactor authentication to access these resources.

Require multifactor authentication for admins

This policy applies to users with highly privileged admin roles:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

These accounts must use multifactor authentication to sign in to any application.

Require multifactor authentication for all users

This policy applies to all users in your organization and requires multifactor authentication for every sign-in. In most cases, sessions persist on devices, so users don't need to complete multifactor authentication when interacting with other applications.

Monitor and review

The managed policy and the sign-in logs are the two places where you can see the effect of these policies on your organization.

Review the **Policy impact** tab of the managed policy to see a summary of how the policy affects your environment.

Microsoft-managed policy

Multifactor authentication for admins accessing Microsoft Admin Portals

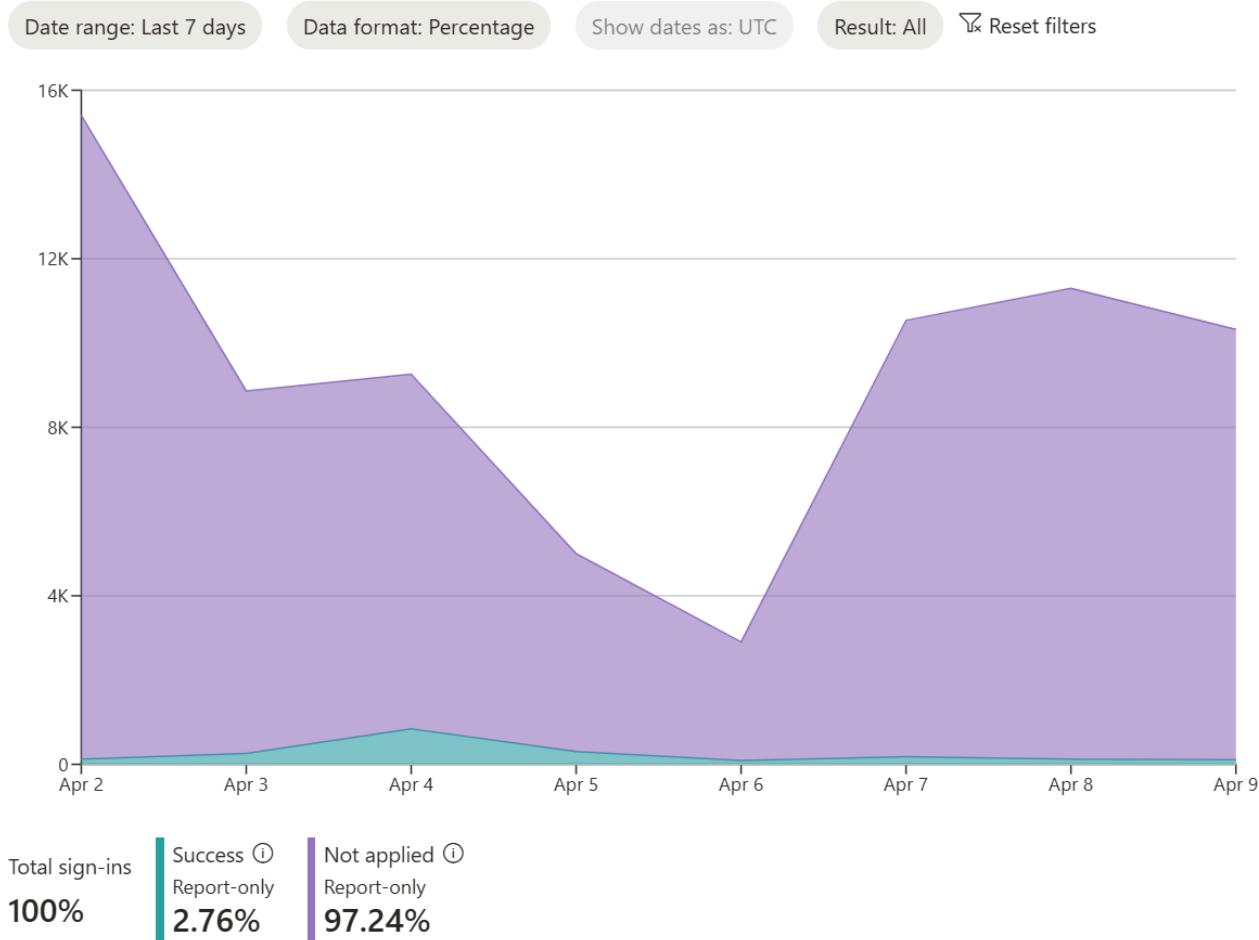
Policy details

Policy impact (Preview)

X

To view more information about the impact of your Conditional Access policies, visit [Conditional Access Insights and reporting page](#).

Sign-in activity over time



Sample sign-ins on April 9, 2025 where policy did not apply

Here are examples of sign-in events where the Conditional Access policy wouldn't apply if enabled.

Analyze the **Microsoft Entra sign-in logs** to see details about how the policies affect sign-in activity.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Use some or all of the following filters:
 - **Correlation ID** when you have a specific event to investigate.
 - **Conditional Access** to see policy failure and success.
 - **Username** to see information related to specific users.
 - **Date** scoped to the time frame in question.
4. Select a specific sign-in event, then select **Conditional Access**.

- To investigate further, select the **Policy Name** to drill down into the configuration of the policies.

5. Explore the other tabs to see the **client user** and **device details** that were used for the Conditional Access policy assessment.

Common questions

What is Conditional Access?

Conditional Access is a Microsoft Entra feature that allows organizations to enforce security requirements when accessing resources. Conditional Access is commonly used to enforce multifactor authentication, device configuration, or network location requirements.

These policies can be thought of as logical if then statements.

If the assignments (users, resources, and conditions) are true, then apply the access controls (grant and/or session) in the policy. If you're an administrator, who wants to access one of the Microsoft admin portals, then you must perform multifactor authentication to prove it's really you.

What if I want to make more changes?

Administrators might choose to make further changes to these policies by duplicating them using the **Duplicate** button in the policy list view. This new policy can be configured in the same way as any other Conditional Access policy with starting from a Microsoft recommended position. Be careful not to lower your security posture with those changes.

What administrator roles are covered by these policies?

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator

- Security Administrator
- SharePoint Administrator
- User Administrator

What if I use a different solution for multifactor authentication?

Multifactor authentication using [external authentication methods](#) satisfies the MFA requirements of Microsoft-managed policies.

When multifactor authentication is completed via a federated identity provider (IdP), it might satisfy Microsoft Entra ID MFA requirements depending on your configuration. For more information, see [Satisfy Microsoft Entra ID multifactor authentication \(MFA\) controls with MFA claims from a federated IdP](#).

What if I use Certificate-Based Authentication?

Depending on your Certificate-Based Authentication (CBA) configuration, it can function as [single or multifactor authentication](#).

- If your organization configures CBA as single-factor, users must use a second authentication method to satisfy MFA. For more information on the allowed combinations of authentication methods to MFA with single-factor CBA, see [MFA with single factor certificate-based authentication](#).
- If your organization configures CBA as multifactor, users can complete MFA with their CBA authentication method.

What if I use custom controls?

[Custom controls don't satisfy multifactor authentication claim requirements](#). If your organization uses custom controls you should [migrate to external authentication methods](#), the replacement of custom controls. Your external authentication provider must support external authentication methods and provide the necessary configuration guidance for integration.

How do I monitor when Microsoft makes a change to these policies or adds a new one?

Administrators with **AuditLog.Read.All** and **Directory.Read** permissions can query the audit log for entries initiated by **Microsoft Managed Policy Manager** in the **Policy** category. For example, use [Graph Explorer](#) to find entries with this query string:

```
https://graph.microsoft.com/v1.0/auditLogs/directoryAudits?  
$filter=initiatedBy/app/displayName eq 'Microsoft Managed Policy Manager' and category eq  
'Policy'.
```

Related content

- [Deploy other commonly used policies from templates](#)
- [Configure and use Conditional Access report-only mode](#)

Conditional Access insights and reporting

Article • 04/14/2025

The Conditional Access insights and reporting workbook enables you to understand the impact of Conditional Access policies in your organization over time. During sign-in, one or more Conditional Access policies might apply, granting access if certain grant controls are satisfied or denying access otherwise. Because multiple Conditional Access policies might be evaluated during each sign-in, the insights and reporting workbook lets you examine the impact of an individual policy or a subset of all policies.

Prerequisites

To enable the insights and reporting workbook, your tenant must have:

- A Log Analytics workspace to retain sign-in logs data.
- Microsoft Entra ID P1 licenses to use Conditional Access.

Users must have at least the Security Reader role assigned and Log Analytics workspace Contributor roles assigned.

Stream sign-in logs from Microsoft Entra ID to Azure Monitor logs

If you haven't integrated Microsoft Entra logs with Azure Monitor logs, you need to take the following steps before the workbook loads:

1. [Create a Log Analytics workspace in Azure Monitor](#).
2. [Integrate Microsoft Entra logs with Azure Monitor logs](#).

How it works

To access the insights and reporting workbook:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Reader](#).
2. Browse to **Protection > Conditional Access > Insights and reporting**.

Get started: Select parameters

The insights and reporting dashboard lets you see the impact of one or more Conditional Access policies over a specified period. Start by setting each of the parameters at the top of the workbook.

The screenshot shows the Microsoft Azure Conditional Access Insights and reporting page. The left sidebar includes sections for Overview (Preview), Policies (with Insights and reporting selected), Diagnose and solve problems, Manage (Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context, Authentication strengths (Preview), Classic policies), Monitoring (Sign-in logs, Audit logs), and Troubleshooting + Support (New support request). The main content area displays User sign-ins and Service principal sign-ins. It features filters for Conditional Access policy (Select all enabled policies - All ...), Time range (Last 24 hours), App (All apps), and Data view (users). Below these filters is an Impact summary section with four cards: Total users (86), Success users (57), Failure users (39), and Not applied users (38). A magnifying glass icon is located in the bottom right corner of the impact summary area.

Conditional Access policy: To view their combined impact, select one or more Conditional Access policies. Policies are separated into two groups: **Enabled** and **Report-only** policies. By default, all **Enabled** policies are selected. These policies are the policies currently enforced in your tenant.

Time range: Select a time range from 4 hours to as far back as 90 days. If you select a time range further back than when you integrated the Microsoft Entra logs with Azure Monitor, only sign-ins after the time of integration appear.

User: By default, the dashboard shows the impact of the selected policies for all users. To filter by an individual user, type the name of the user into the text field. To filter by all users, type **All users** into the text field or leave the parameter empty.

App: By default, the dashboard shows the impact of the selected policies for all apps. To filter by an individual app, type the name of the app into the text field. To filter by all apps, type **All apps** into the text field or leave the parameter empty.

Data view: Select whether you want the dashboard to show results in terms of the number of users or number of sign-ins. An individual user might have hundreds of sign-ins to many apps with many different outcomes during a given time range. If you select the data view to be users, a user could be included in both the **Success** and **Failure** counts. For example, if there

are 10 users, 8 of them might have a result of success in the past 30 days and 9 of them might have a failure in the past 30 days.

Impact summary

Once the parameters are set, the **Impact summary** loads. The summary shows how many users or sign-ins during the time range resulted in **Success**, **Failure**, **User action required** or **Not applied** when the selected policies were evaluated.



Total: The number of users or sign-ins during the time period where at least one of the selected policies was evaluated.

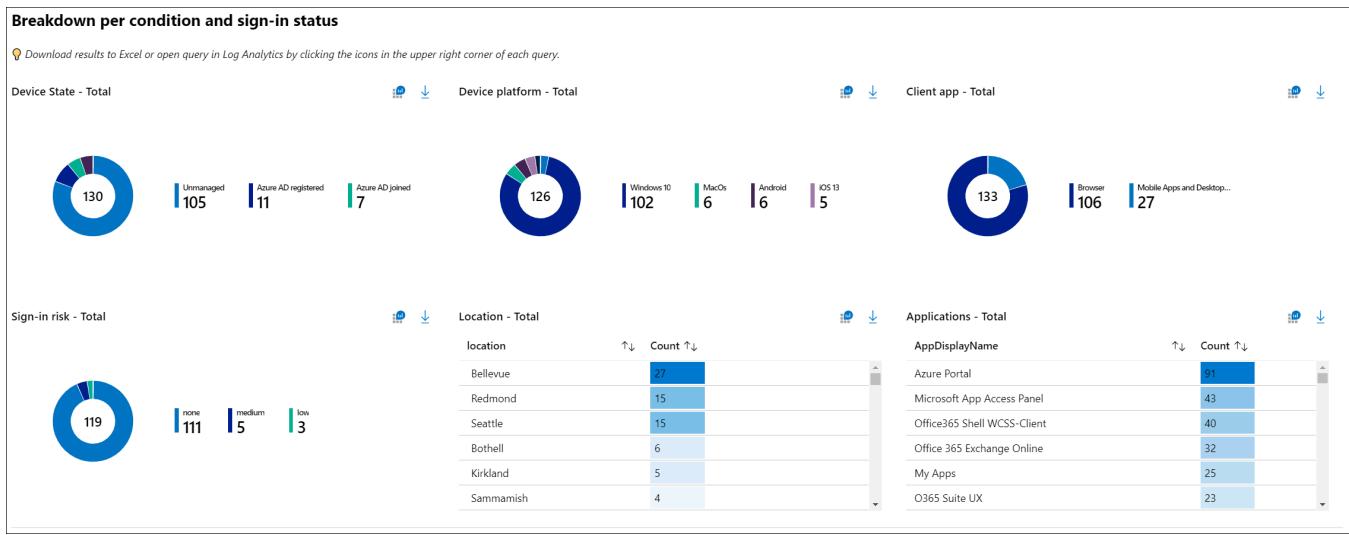
Success: The number of users or sign-ins during the time period where the combined result of the selected policies was **Success** or **Report-only: Success**.

Failure: The number of users or sign-ins during the time period where the result of at least one of the selected policies was **Failure** or **Report-only: Failure**.

User action required: The number of users or sign-ins during the time period where the combined result of the selected policies was **Report-only: User action required**. User action is required when an interactive grant control, such as multifactor authentication is required. Since interactive grant controls aren't enforced by report-only policies, success or failure can't be determined.

Not applied: The number of users or sign-ins during the time period where none of the selected policies applied.

Understanding the impact



View the breakdown of users or sign-ins for each of the conditions. You can filter the sign-ins of a particular result (for example, Success or Failure) by selecting one of the summary tiles at the top of the workbook. You can see the breakdown of sign-ins for each of the Conditional Access conditions: device state, device platform, client app, location, application, and sign-in risk.

Sign-in details

Sign-in Details

To investigate sign-in details of a specific user, filter by username at the top of the workbook

User sign-in count - Total	Sign-in events - Total
UserDisplayName	TimeGenerated
On-Premises Directory Synchronization Service Account	4/30/2020, 10:22:43 AM
	4/30/2020, 10:20:51 AM
	4/30/2020, 10:11:24 AM
	4/30/2020, 10:11:16 AM
	4/30/2020, 10:11:12 AM
	4/30/2020, 10:10:22 AM
	4/30/2020, 9:52:08 AM
	4/30/2020, 9:22:02 AM
	4/30/2020, 8:52:06 AM
	4/30/2020, 8:52:01 AM

You can also investigate the sign-ins of a specific user by searching for sign-ins at the bottom of the dashboard. The query displays the most frequent users. Selecting a user filters the query.

! Note

When downloading the sign-in logs, choose JSON format to include Conditional Access report-only result data.

Improve workbook performance

The standard Conditional Access insights and reporting workbook can capture a large amount of data with the default settings. The amount of data captured can affect the performance of the workbook so some queries might take longer to load or even time out. To improve performance, you can create a transformation in Azure Monitor.

Before proceeding with this optional step, review the [Transformation in Azure Monitor](#) article for a general overview and cost considerations.

To identify the results to keep or exclude from the transformation, use the following Kusto query in Log Analytics:

```
Kusto

SignInLogs
| extend CAPResult_CF = extract_all(@"(\\{[^{}]*""result"":""(success|failure)""[^{}]*\\})", tostring(ConditionalAccessPolicies))
| project-away ConditionalAccessPolicies
```

The query looks specifically at Conditional Access policies that result in a success or failure. Other values you can include in the query include `notApplied`, `reportOnlySuccess`, `reportOnlyFailure`, `reportOnlyNotApplied`, and `notEnabled`.

To create the Data Collection Rule (DCR) for Sign-in logs:

1. Sign in to the [Azure portal](#) as at least a **Monitoring Contributor**.
2. Browse to **Log Analytics workspaces** and select your workspace.
3. Go to **Settings > Tables** > select **SignInLogs**.
4. Open the menu on the right and select **Create transformation**.
5. Follow the prompts to create the transformation, selecting **Transformation editor** to change any of the details included in the transformation.

Once the transformation is created and deployed successfully, the Conditional Access insights and reporting workbook should load faster. The transformation only applies to new sign-in logs ingested after the transformation is created. Other workbooks that also pull from this table are affected by the transformation.

Keep in mind that if you exclude certain policy results from the transformation, you won't see any of those results in the workbook once the transformation is running.

Configure a Conditional Access policy in report-only mode

To configure a Conditional Access policy in report-only mode:

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Policies**.
3. Select an existing policy or create a new policy.
4. Under **Enable policy** set the toggle to **Report-only** mode.
5. Select **Save**

Tip

Editing the **Enable policy** state of an existing policy from **On** to **Report-only** disables existing policy enforcement.

Troubleshooting

Why are queries failing due to a permissions error?

In order to access the workbook, you need the proper permissions in Microsoft Entra ID and Log Analytics. To test whether you have the proper workspace permissions by running a sample log analytics query:

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Security Reader**.
2. Browse to **Identity > Monitoring & health > Log Analytics**.
3. Type `SigninLogs` into the query box and select **Run**.
4. If the query doesn't return any results, your workspace might not be configured correctly.

The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a navigation bar with 'New Query 1*', '+', 'Example queries', 'Query explorer', and a gear icon. Below the navigation is a header with 'ContosoLogAnalytics' and 'Select scope'. A red box highlights the 'SigninLogs' tab under 'Queries'. The main area shows a search bar and a 'Group by: Solution' dropdown. On the left, there's a 'Favorites' section and a tree view under 'LogManagement' with nodes like 'Operation', 'Usage', etc. A red box highlights the 'SigninLogs' node. The right side displays the query results for 'SigninLogs' with a time range of 'Last hour'. The results table has columns: TimeGenerated [UTC], ResourceId, OperationName, and Ope... (partially visible). The results show five records from May 26, 2020, at various times, all labeled 'Sign-in activity' with a value of '1.0'.

TimeGenerated [UTC]	ResourceId	OperationName	Ope...
5/26/2020, 4:25:02.474 PM	/tenants/ffffaaaa-5555-bbbb-6666-cccc7777ddd/providers/Micro...	Sign-in activity	1.0
5/26/2020, 4:25:02.474 PM	/tenants/ffffaaaa-5555-bbbb-6666-cccc7777ddd/providers/Micro...	Sign-in activity	1.0
5/26/2020, 4:25:07.403 PM	/tenants/ffffaaaa-5555-bbbb-6666-cccc7777ddd/providers/Micro...	Sign-in activity	1.0
5/26/2020, 4:55:02.734 PM	/tenants/ffffaaaa-5555-bbbb-6666-cccc7777ddd/providers/Micro...	Sign-in activity	1.0
5/26/2020, 4:55:07.562 PM	/tenants/ffffaaaa-5555-bbbb-6666-cccc7777ddd/providers/Micro...	Sign-in activity	1.0

For more information about how to stream Microsoft Entra sign-in logs to a Log Analytics workspace, see the article [Integrate Microsoft Entra logs with Azure Monitor logs](#).

Why are the queries in the workbook failing?

Customers notice queries sometimes fail if the wrong or multiple workspaces are associated with the workbook. To fix this problem, select **Edit** at the top of the workbook and then the Settings gear. Select and then remove workspaces that aren't associated with the workbook. There should be only one workspace associated with each workbook.

Why is the Conditional Access policies parameter empty?

The list of policies is generated by looking at the policies evaluated for the most recent sign-in event. If there are no recent sign-ins in your tenant, you might need to wait a few minutes for the workbook to load the list of Conditional Access policies. Empty results can happen immediately after configuring Log Analytics or if a tenant doesn't have recent sign-in activity.

Why is the workbook taking a long time to load or returning zero results?

Depending on the time range selected and the size of your tenant, the workbook might be evaluating an extraordinarily large number of sign-in events. For large tenants, the volume of sign-ins might exceed the query capacity of Log Analytics. Try shortening the time range to 4 hours, then see if the workbook loads. Review the [Improve workbook performance](#) section for more information about how to improve performance.

Can I save my parameter selections or customize the workbook?

You can save your parameter selections and customize the workbook at the top of the workbook. Browse to **Identity > Monitoring & health > Workbooks > Conditional Access Insights and reporting**. Here you find the workbook template, where you can edit the workbook and save a copy to your workspace, including the parameter selections, in **My reports** or **Shared reports**. To start editing the queries, select **Edit** at the top of the workbook.

Related content

- [Conditional Access report-only mode](#)
- For more information about Microsoft Entra workbooks, see the article, [How to use Azure Monitor workbooks for Microsoft Entra reports](#).
- [Conditional Access common policies](#)

Microsoft Entra terms of use

Article • 03/15/2024

Microsoft Entra terms of use policies provide a simple method to present information to end users. Organizations can use terms of use along with Conditional Access policies to require employees or guests to accept your terms of use policy before getting access. These terms of use statements can be generalized or specific to groups or users and provided in multiple languages. Administrators can determine who has or hasn't accepted terms of use with the provided logs or APIs.

ⓘ Note

This article provides steps about how to delete personal data from the device or service and can be used to support your obligations under the GDPR. For general information about GDPR, see the [GDPR section of the Microsoft Trust Center](#) and the [GDPR section of the Service Trust portal](#).

Prerequisites

To use and configure Microsoft Entra terms of use policies, you must have:

- Microsoft Entra ID P1 licenses.
- Administrators who need to read terms of use configuration and Conditional Access policies need at least the [Security Reader](#) role assigned.
- Administrators who need to Create or modify terms of use and Conditional Access policies need at least the [Conditional Access Administrator](#) role assigned.
- A terms of use document in PDF format. The PDF file can be any content you decide to display. To support users on mobile devices, the recommended font size in the PDF is 24 point.

Service limits

You can add no more than 40 terms per tenant.

Add terms of use

Once you complete your terms of use policy document, use the following procedure to add it.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.

2. Browse to **Protection > Conditional Access > Terms of use.**

3. Select, **New terms.**

The screenshot shows the 'New terms of use' configuration page in the Microsoft Entra admin center. The left sidebar has a 'Conditional Access' icon selected. The main area is titled 'New terms of use'. It contains the following fields:

- Name ***: Contoso Terms of Use
- Terms of use document ***: "Contoso ToU.pdf"
- Language**: English
- Display name**: Terms of Use
- Require users to expand the terms of use**: On
- Require users to consent on every device**: Off
- Expire consents**: Off
- Duration before re-acceptance required (days)**: Example: '90'
- Conditional access**: Enforce with conditional access policy templates *: Create conditional access policy later

A large blue 'Create' button is at the bottom left.

4. In the **Name** box, enter a name for the terms of use policy.

5. For **Terms of use document**, browse to your finalized terms of use policy PDF and select it.

6. Select the language for your terms of use policy document. The language option allows you to upload multiple terms of use policies, each with a different language. The version of the terms of use policy that an end user sees is based on their browser preferences.

7. In the **Display name** box, enter a title that users see when they sign in.

8. To require end users to view the terms of use policy before accepting them, set **Require users to expand the terms of use** to **On**.
9. To require end users to accept your terms of use policy on every device they're accessing from, set **Require users to consent on every device** to **On**. Users might be required to install other applications if this option is enabled. For more information, see [Per-device terms of use](#).
10. If you want to expire terms of use policy consents on a schedule, set **Expire consents** to **On**. When set to On, two more schedule settings are displayed.
 - a. Use the **Expire starting on** and **Frequency** settings to specify the schedule for terms of use policy expirations. The following table shows the result for a couple of example settings:

[+] Expand table

Expire starting on	Frequency	Result
Today's date	Monthly	Starting today, users must accept the terms of use policy and then reaccept every month.
Date in the future	Monthly	Starting today, users must accept the terms of use policy. When the future date occurs, consents expire, and then users must reaccept every month.

For example, if you set the expire starting on date to **Jan 1** and frequency to **Monthly**, this example is how expirations might occur for two users:

[+] Expand table

User	First accept date	First expire date	Second expire date	Third expire date
Alice	Jan 1	Feb 1	Mar 1	Apr 1
Bob	Jan 15	Feb 1	Mar 1	Apr 1

- b. Use the **Duration before re-acceptance required (days)** setting to specify the number of days before the user must reaccept the terms of use policy. This option allows users to follow their own schedule. For example, if you set the duration to **30** days, this example is how expirations might occur for two users:

[+] Expand table

User	First accept date	First expire date	Second expire date	Third expire date
Alice	Jan 1	Jan 31	Mar 2	Apr 1
Bob	Jan 15	Feb 14	Mar 16	Apr 15

It's possible to use the **Expire consents** and **Duration before re-acceptance required (days)** settings together, but typically you use one or the other.

Important

Users whose consent has expired regardless of the setting used, **Expire consents** or **Duration before re-acceptance required (days)** are prompted to re-accept the terms only if their session has expired.

- Under **Conditional Access**, use the **Enforce with Conditional Access policy template** list to select the template to enforce the terms of use policy.

 Expand table

Template	Description
Custom policy	Select the users, groups, and apps that the terms of use policy is applied to.
Create Conditional Access policy later	This terms of use policy appears in the grant control list when creating a Conditional Access policy.

Important

Conditional Access policy controls (including terms of use policies) do not support enforcement on service accounts. We recommend excluding all service accounts from the Conditional Access policy.

Custom Conditional Access policies enable granular terms of use policies, down to a specific cloud application or group of users. For more information, see [Quickstart: Require terms of use to be accepted before accessing cloud apps](#).

- Select **Create**.

If you selected a custom Conditional Access template, then a new screen appears that allows you to create the custom Conditional Access policy. You should now see your new terms of use policies.

Per-device terms of use

The **Require users to consent on every device** setting enables you to require end users to accept your terms of use policy on every device they're accessing from. The end user's device must be registered in Microsoft Entra ID. When the device is registered, the device ID is used to enforce the terms of use policy on each device. Their experience is dependent on permissions to join devices and the platform or software used. For more information, see [device identity in Microsoft Entra ID](#).

Per-device terms of use have the following constraints:

- The Microsoft Intune Enrollment app `Application ID: d4ebce55-015a-49b5-a083-c84d1797ae8c` isn't supported. Ensure that it's excluded from any Conditional Access policy requiring Terms of Use.
- Microsoft Entra B2B users aren't supported.

Policy changes

Conditional Access policies take effect immediately. When this enforcement happens, the administrator might see errors in the Microsoft Entra admin center. The administrator must sign out and sign in to satisfy the new policy.

Important

Users in scope will need to sign-out and sign-in in order to satisfy a new policy if:

- a Conditional Access policy is enabled on a terms of use policy
- or a second terms of use policy is created

Edit terms of use details

You can edit some details of terms of use policies, but you can't modify an existing document. The following procedure describes how to edit the details.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select the terms of use policy you want to edit.
4. Select **Edit terms**.

5. In the Edit terms of use pane, you can change the following options:

- **Name** – the internal name of the terms of use that isn't shared with end users.
- **Display name** – the name that end users can see when viewing the terms of use.
- **Require users to expand the terms of use** – Setting this option to **On** forces the end user to expand the terms of use policy document before accepting it.
- You can **update an existing terms of use** document.
- You can **add a language** to an existing terms of use.

6. Once you're done, select **Save** to save your changes.

If there are other settings you would like to change, you must create a new terms of use policy.

Update the version or PDF of an existing terms of use

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select the terms of use policy you want to edit.
4. Select **Edit terms**.
5. For the language that you would like to update a new version, select **Update** under the action column
6. In the pane on the right, upload the pdf for the new version
7. There's also a toggle option here **Require reaccept** if you want to require your users to accept this new version the next time they sign in.
 - If you require your users to reaccept, next time they try to access the resource defined in your Conditional Access policy they'll be prompted to accept this new version.
 - If you don't require your users to reaccept, their previous consent stays current and only new users who haven't consented before or whose consent expires see the new version. Until the session expires, **Require reaccept** doesn't require users to accept the new terms of use. If you want to ensure reaccept, delete and recreate or create a new terms of use for this case.

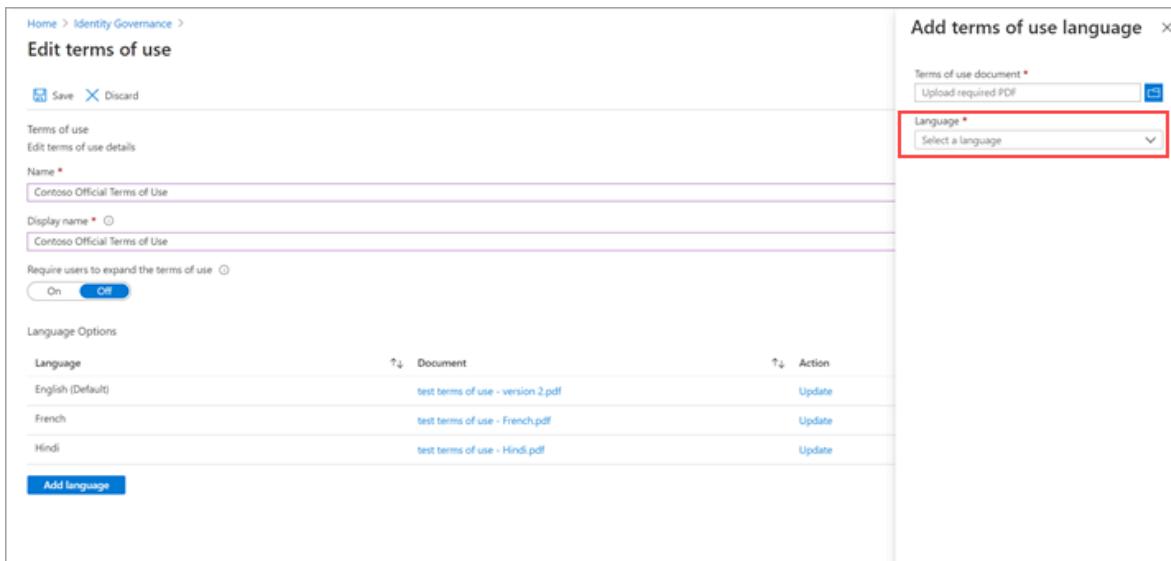
The screenshot shows the Microsoft Entra admin center interface. On the left, under 'Edit terms of use', there are fields for 'Name' (Contoso Official Terms of Use) and 'Display name' (Contoso Official Terms of Use). A toggle switch for 'Require users to expand the terms of use' is set to 'On'. Below this is a table for 'Language Options' with rows for English (Default), French, and Hindi, each with a 'test terms of use - [language].pdf' file in the 'Document' column and an 'Update' button in the 'Action' column. At the bottom of this section is a blue 'Add language' button. On the right, a separate pane titled 'Update terms of use version' shows a 'Terms of use document' field with 'Upload required PDF' and a 'Language' dropdown set to 'English'. A red box highlights the 'Require re-accept' toggle switch, which is currently set to 'Off'.

8. Once you upload your new pdf and decide on reaccept, select Add at the bottom of the pane.
9. You see the most recent version under the Document column.

Add a language

The following procedure describes how to add a language to your terms of use.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select the terms of use policy you want to edit.
4. Select **Edit Terms**.
5. Select **Add language** at the bottom of the page.
6. In the **Add terms of use language** pane, upload your localized PDF, and select the language.



7. Select **Add language**.
8. Select **Save**
9. Select **Add** to add the language.

View previous versions of a terms of use

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select the terms of use policy for which you want to view a version history.
4. Select **Languages and version history**.
5. Select **See previous versions**.
6. You can select the name of the document to download that version.

View report of who has accepted and declined

The **Terms of use** blade shows a count of the users who accepted and declined. These counts and who accepted/declined are stored for the life of the terms of use policy.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Terms of use**.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view under 'Conditional Access' with nodes like 'Overview', 'Policies', 'Insights and reporting', 'Diagnose and solve problems', 'Manage' (with 'Named locations', 'Custom controls (Preview)', and 'Terms of use' selected), 'VPN connectivity', 'Authentication contexts', 'Authentication strengths', and 'Classic policies'. The main content area is titled 'Terms of use document details' for 'Contoso Terms of Use'. It shows settings such as 'Require users to expand the terms of use' (On), 'Require users to consent on every device' (Off), 'Expire consents' (Off), and 'Users accepted' (0). There are tabs for 'Details' and 'Languages and version history'.

3. For a terms of use policy, select the numbers under **Accepted** or **Declined** to view the current state for users.
 - a. By default, the next page will show you the current state of each user's acceptance to the terms of use.
 - b. If you would like to see the previous consent events, you can select **All** from the **Current State** drop-down. Now you can see each user's events in details about each version and what happened.
 - c. Alternatively, you can select a specific version from the **Version** drop-down to see who accepted that specific version.
4. To view the history for an individual user, select the ellipsis (...) and then **View History**. In the view history pane, you see a history of all the accepts, declines, and expirations.

User acceptance record deletion

User acceptance records are deleted when:

- An admin explicitly deletes the terms of use.
 - When this change happens, all the acceptance records associated with that specific terms of use are also deleted.
- The tenant loses its Microsoft Entra ID P1 or P2 licenses.
- The tenant is deleted.

View Microsoft Entra audit logs

If you want to view more activity, Microsoft Entra terms of use policies include audit logs. Each user consent triggers an event in the audit logs that is stored for 30 days. You can view these logs in the portal or download as a .csv file.

To get started with Microsoft Entra audit logs, use the following procedure:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select a terms of use policy.
4. Select **View audit logs**.
5. On the Microsoft Entra audit logs screen, you can filter the information using the provided lists to target specific audit log information.

You can also select **Download** to download the information in a .csv file for use locally.

The screenshot shows the Microsoft Entra admin center interface. The URL in the browser is https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConditionalAccess/TermsOfUse. The page title is "Audit Logs". The main content area displays a table of audit logs for a "Terms Of Use" service. The table has columns: Date, Service, Category, Activity, Status, and Status reason. There are four rows of data:

Date	Service	Category	Activity	Status	Status reason
3/8/2024, 2:41:37 PM	Terms Of Use	Policy	Create Terms Of Use	Success	
3/8/2024, 1:38:23 PM	Terms Of Use	Policy	Delete Terms Of Use	Success	
3/8/2024, 1:37:58 PM	Terms Of Use	Policy	Delete Terms Of Use	Success	
3/8/2024, 1:37:46 PM	Terms Of Use	Policy	Edit Terms Of Use	Success	

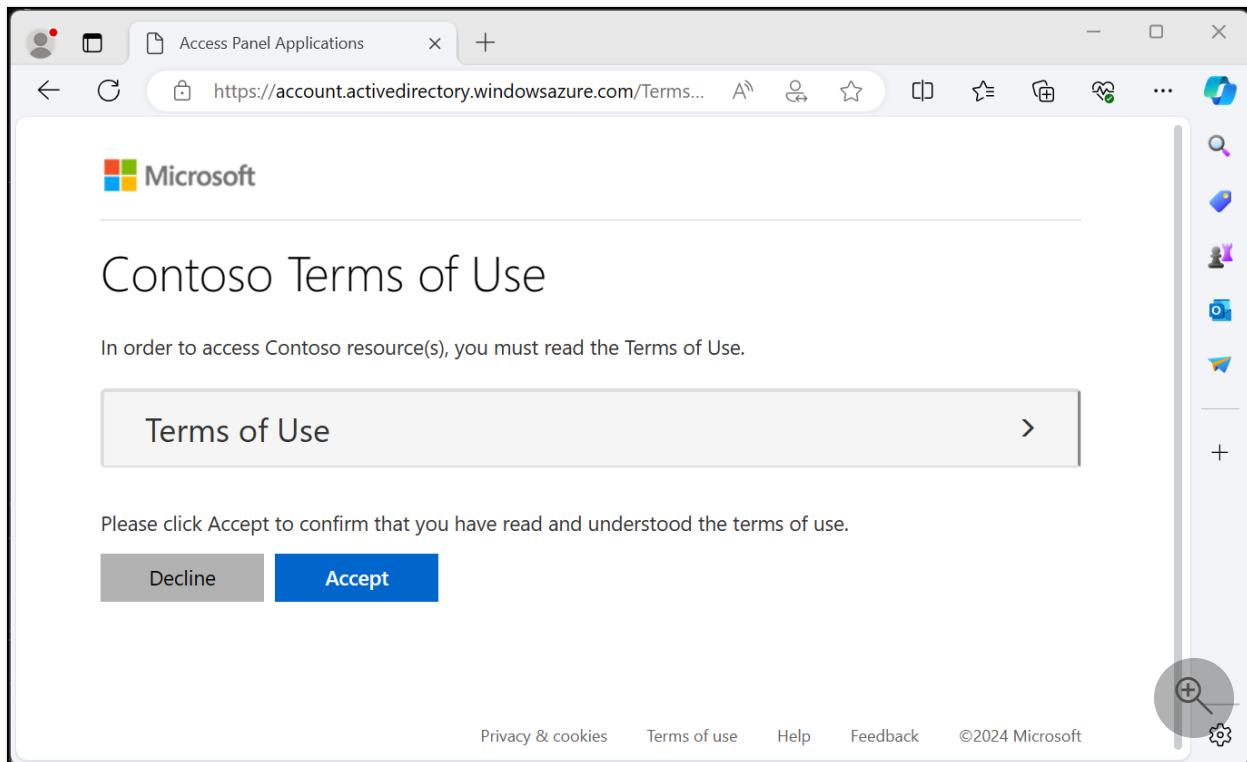
If you select a log, a pane appears with more activity details.

The screenshot shows the Microsoft Entra admin center interface. The title bar reads "Audit Log Details - Microsoft Ent..." and the URL is "https://entra.microsoft.com/#view/Micro...". The main content area is titled "Audit Log Details" and displays an "Activity" record. The activity details are as follows:

Activity	Target(s)	Modified Properties
Activity		
Date	3/8/2024, 2:41 PM	
Activity Type	Create Terms Of Use	
Correlation ID	8f637fef-a8d2-47ee-90b0-af837149bd71	
Category	Policy	
Status	success	
Status reason		
User Agent		
Initiated by (actor)		
Type	User	
Display Name	BalaS	
Object ID	f74e3dc5-134f-4182-8e2c-fd28b75a4318	
User Principal Name	BalaS@contoso.onmicrosoft.com	
Additional Details		
What User Will See	Contoso Terms of Use	
Required Upon	Access to resources	

What terms of use looks like for users

Once a terms of use policy is created and enforced, users, who are in scope, see the following screen during sign-in.



Users can view the terms of use policy and, if necessary, use buttons to zoom in and out. Users are only required to accept the terms of use policy once, and they won't see the terms of use policy again on later sign-ins.

How users can review their terms of use

Users can review and see the terms of use policies that they've accepted by using the following procedure.

1. Sign in to <https://myaccount.microsoft.com/>.
2. Select **Settings & Privacy**.
3. Select **Privacy**.
4. Under **Organization's notice**, select **View** next to the terms of use statement you want to review.

Delete terms of use

You can delete old terms of use policies using the following procedure.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Terms of use**.
3. Select the terms of use policy you want to remove.
4. Select **Delete terms**.
5. In the message that appears asking if you want to continue, select **Yes**.

- a. You should no longer see your terms of use policy.

B2B guests

Using Conditional Access and terms of use policies, you can enforce a policy directly towards B2B guest users. During the invitation redemption flow, the user is presented with the terms of use policy.

Terms of use policies are only displayed when the user has a guest account in Microsoft Entra ID. SharePoint Online currently has an [external sharing recipient experience](#) to share a document or a folder that doesn't require the user to have a guest account. In this case, a terms of use policy isn't displayed.

Support for cloud apps

Terms of use policies can be used for different cloud apps, such as Azure Information Protection and Microsoft Intune. This support is currently in preview.

Azure Information Protection

You can configure a Conditional Access policy for the Azure Information Protection app and require a terms of use policy when a user accesses a protected document. This configuration triggers a terms of use policy before a user accessing a protected document for the first time.

Microsoft Intune Enrollment

You can configure a Conditional Access policy for the Microsoft Intune Enrollment app and require a terms of use policy before enrollment of a device in Intune. For more information, see the Read [Choosing the right Terms solution for your organization blog post](#).

Note

The Intune Enrollment app is not supported for [Per-device terms of use](#).

For iOS/iPadOS Automated device enrollment, adding a custom URL to the Microsoft Entra Terms of Use policy doesn't allow for users to open the policy from the URL in Setup Assistant to read it. The policy can be read by the user after Setup

Assistant is completed from the Company Portal website, or in the Company Portal app.

Frequently asked questions

Q: Why do I see two sign-ins for my users? One interrupt and one success.

A: Administrators might see two sign-ins when users haven't yet accepted a terms of use policy, this scenario is by design. These entries share a correlation ID.

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication requir...
3/11/2024, 4:22:07 PM	cfe1119-9e72-467f-9efc...	BalaS	Azure Portal	Success	173.88.126.146	Westerville, Ohio, US	Success	Single-factor authentication
3/11/2024, 4:22:06 PM	31fb37b7-581a-4d9f-aaf...	BalaS	AAD Terms Of Use	Success	173.88.126.146	Westerville, Ohio, US	Not Applied	Single-factor authentication
3/11/2024, 4:21:59 PM	b0ea636e-286e-46e9-ad1...	BalaS	My Profile	Success	173.88.126.146	Westerville, Ohio, US	Not Applied	Single-factor authentication
3/11/2024, 4:21:59 PM	ea47f0c9-201e-46f4-a4c6...	BalaS	My Profile	Success	173.88.126.146	Westerville, Ohio, US	Not Applied	Single-factor authentication
3/11/2024, 4:21:56 PM	8c1f3924-4211-48f9-9ae4...	BalaS	AAD Terms Of Use	Success	173.88.126.146	Westerville, Ohio, US	Not Applied	Single-factor authentication
3/11/2024, 4:21:55 PM	cfe1119-9e72-467f-9efc...	BalaS	AAD Terms Of Use	Success	173.88.126.146	Westerville, Ohio, US	Not Applied	Single-factor authentication
3/11/2024, 4:21:54 PM	cfe1119-9e72-467f-9efc...	BalaS	Azure Portal	Interrupted	173.88.126.146	Westerville, Ohio, US	Failure	Single-factor authentication
2/11/2024, 4:20:06 PM	4622dd0d-1b0e-4d93-bbe...	BalaS	AuditHistory	Success	173.88.126.146	Westerville, Ohio, US	Success	Single-factor authentication

One sign-in is interrupted since the user can't provide proof of acceptance of the terms of use policy in their token. The **additional details** field in the sign-in log includes the following message:

The user is required to satisfy additional requirements before finishing authentication, and was redirected to another page (such as terms of use or a third party MFA provider). This code alone does not indicate a failure on your users part to sign in. The sign in logs may indicate that this challenge was successfully passed or failed.

If the user accepts the terms of use policy, the other sign-in is successful.

Q: I cannot sign in using PowerShell when terms of use is enabled.

A: Terms of use can only be accepted when authenticating interactively.

Q: How do I see when/if a user has accepted a terms of use?

A: On the Terms of use blade, select the number under **Accepted**. You can also view or search the accepted activity in the Microsoft Entra audit logs. For more information, see View report of who accepted and declined and [View Microsoft Entra audit logs](#).

Q: How long is information stored?

A: The user counts in the terms of use report and who accepted/declined are stored for the life of the terms of use. The Microsoft Entra audit logs are stored for 30 days.

Q: Why do I see a different number of consents in the terms of use details overview versus the Microsoft Entra audit logs?

A: The terms of use details overview data is stored for the lifetime of the terms of use policy. The Microsoft Entra audit logs are stored for 30 days.

Q: Why do I see a different number of consents in the terms of use details overview versus the exported CSV report?

A: The terms of use details overview reflect aggregated acceptances of the current version of the policy (updated once every day). If expiration is enabled or a terms of use agreement is updated (with reacceptance required), the count on the details overview is reset since the acceptances are expired, this page shows the count of the current version. All acceptance history is still captured in the CSV report.

Q: If hyperlinks are in the terms of use policy PDF document, will end users be able to click them?

A: Yes, end users are able to select hyperlinks to other pages but links to sections within the document aren't supported. Also, hyperlinks in terms of use policy PDFs don't work when accessed from the Microsoft Entra My Apps/MyAccount portal.

Q: Can a terms of use policy support multiple languages?

A: Yes. An administrator can upload multiple PDF documents and tag those documents with a corresponding language. When end users sign in, we look at their browser language preference and display the matching document. If there's no match, we display the default document, which is the first document that is uploaded.

Q: When is the terms of use policy triggered?

A: A terms of use policy triggers during the sign-in experience.

Q: What applications can I target a terms of use policy to?

A: You can create a Conditional Access policy on the enterprise applications using modern authentication. For more information, see [enterprise applications](#).

Q: Can I add multiple terms of use policies to a given user or app?

A: Yes, by creating multiple Conditional Access policies targeting those groups or applications. If a user falls in scope of multiple terms of use policies, they must accept one policy at a time.

Q: What happens if a user declines the terms of use policy?

A: The user is blocked from getting access to the application. The user would have to sign in again and accept the terms to get access.

Q: Is it possible to unaccept a terms of use policy that was previously accepted?

A: You can [review previously accepted terms of use policies](#), but currently there isn't a way to unaccept.

Q: What happens if I'm also using Intune terms and conditions?

A: If you configure both Microsoft Entra terms of use and [Intune terms and conditions](#), the user is required to accept both. For more information, see the [Choosing the right Terms solution for your organization](#) blog post .

Q: What endpoints does the terms of use service use for authentication?

A: Terms of use utilize the following endpoints for authentication:

<https://tokenprovider.termsfuse.identitygovernance.azure.com>  ,

<https://myaccount.microsoft.com>  , and

<https://account.activedirectory.windowsazure.com>  . If your organization has an allowlist of URLs for enrollment, you need to add these endpoints to your allowlist, along with the Microsoft Entra endpoints for sign-in.

Related content

- [Example policy to require terms of use to be accepted before accessing Microsoft Admin Portals](#)

Configure adaptive session lifetime policies

Article • 11/12/2024

⚠️ Warning

If you are using the [configurable token lifetime](#) feature currently in public preview, please note that we don't support creating two different policies for the same user or app combination: one with this feature and another one with configurable token lifetime feature. Microsoft retired the configurable token lifetime feature for refresh and session token lifetimes on January 30, 2021 and replaced it with the Conditional Access authentication session management feature.

Before enabling Sign-in Frequency, make sure other reauthentication settings are disabled in your tenant. If "Remember MFA on trusted devices" is enabled, be sure to disable it before using Sign-in frequency, as using these two settings together may lead to prompting users unexpectedly. To learn more about reauthentication prompts and session lifetime, see the article, [Optimize reauthentication prompts and understand session lifetime for Microsoft Entra multifactor authentication](#).

Policy deployment

To make sure that your policy works as expected, the recommended best practice is to test it before rolling it out into production. Ideally, use a test tenant to verify whether your new policy works as intended. For more information, see the article [Plan a Conditional Access deployment](#).

Policy 1: Sign-in frequency control

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

5. Choose all required conditions for customer's environment, including the target cloud apps.

! Note

It is recommended to set equal authentication prompt frequency for key Microsoft Office apps such as Exchange Online and SharePoint Online for best user experience.

6. Under Access controls > Session.

- a. Select Sign-in frequency.

- i. Choose Periodic reauthentication and enter a value of hours or days or select Every time.

The screenshot shows the Microsoft Entra admin center interface for creating a new Conditional Access policy. The left pane displays the policy structure: Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies > New. The right pane is titled 'Session' and contains the following configuration:

- Name:** Sign-in frequency
- Assignments:** Users or workload identities (Specific users included)
- Cloud apps or actions:** 1 app included
- Conditions:** 0 conditions selected
- Access controls:** Grant (0 controls selected)
- Session:** 0 controls selected (highlighted with a red box)
- Enable policy:** Report-only (selected), On, Off

The 'Session' tab is active, showing the following settings:

- Use app enforced restrictions
- Use Conditional Access App Control
- Sign-in frequency
 - Periodic reauthentication
 - 0
 - Select units (dropdown menu)
 - Every time

A yellow warning box indicates: "⚠ Some of the applications currently selected are not compatible with the 'Sign-in frequency' option of 'Every time'".

Other session options listed but not selected include:

- Persistent browser session
- Customize continuous access evaluation
- Disable resilience defaults

7. Save your policy.

Policy 2: Persistent browser session

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Conditional Access Administrator**.

2. Browse to **Protection > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Choose all required conditions.

 **Note**

This control requires to choose "All Cloud Apps" as a condition. Browser session persistence is controlled by authentication session token. All tabs in a browser session share a single session token and therefore they all must share persistence state.

6. Under **Access controls > Session**.

- a. Select **Persistent browser session**.

 **Note**

Persistent Browser Session configuration in Microsoft Entra Conditional Access overrides the "Stay signed in?" setting in the company branding pane for the same user if you have configured both policies.

- b. Select a value from dropdown.

7. Save your policy.

Policy 3: Sign-in frequency control every time risky user

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and choose your organization's emergency access or break-glass accounts.

- c. Select Done.
6. Under Cloud apps or actions > Include, select All resources (formerly 'All cloud apps').
7. Under Conditions > User risk, set Configure to Yes.
 - a. Under Configure user risk levels needed for policy to be enforced, select High.
This guidance is based on Microsoft recommendations and might be different for each organization
 - b. Select Done.
8. Under Access controls > Grant, select Grant access.
 - a. Select Require authentication strength, then select the built-in Multifactor authentication authentication strength from the list.
 - b. Select Require password change.
 - c. Select Select.
9. Under Session.
 - a. Select Sign-in frequency.
 - b. Ensure Every time is selected.
 - c. Select Select.
10. Confirm your settings and set Enable policy to Report-only.
11. Select Create to create to enable your policy.

After administrators confirm your settings using [report-only mode](#), they can move the Enable policy toggle from Report-only to On.

Validation

Use the [What If tool](#) to simulate a sign-in from the user to the target application and other conditions based on how you configured your policy. The authentication session management controls show up in the result of the tool.

Prompt tolerance

We factor for five minutes of clock skew when **every time** is selected in policy, so that we don't prompt users more often than once every five minutes. If the user completed MFA in the last 5 minutes, and they hit another Conditional Access policy that requires reauthentication, we don't prompt the user. Over-prompting users for reauthentication can impact their productivity and increase the risk of users approving MFA requests they didn't initiate. Use "Sign-in frequency – every time" only for specific business needs.

Known issues

- If you configure sign-in frequency for mobile devices: Authentication after each sign-in frequency interval could be slow, it can take 30 seconds on average. Also, it could happen across various apps at the same time.
- On iOS devices: If an app configures certificates as the first authentication factor and the app has both Sign-in frequency and [Intune mobile application management policies](#) applied, end-users are blocked from signing in to the app when the policy triggers.

Next steps

- If you're ready to configure Conditional Access policies for your environment, see the article [Plan a Conditional Access deployment](#).
-

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Use audit logs to troubleshoot Conditional Access policy changes

Article • 04/25/2025

The Microsoft Entra audit log is a valuable source of information when troubleshooting why and how Conditional Access policy changes happened in your environment.

Audit log data is only kept for 30 days by default, which might not be long enough for every organization. Organizations can store data for longer periods by changing diagnostic settings in Microsoft Entra ID to:

- Send data to a Log Analytics workspace
- Archive data to a storage account
- Stream data to Event Hubs
- Send data to a partner solution

Find these options under **Entra ID > Monitoring & health > Diagnostic settings > Edit setting**. If you don't have a diagnostic setting, follow the instructions in the article [Create diagnostic settings to send platform logs and metrics to different destinations](#) to create one.

Use the audit log

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Entra ID > Monitoring & health > Audit logs**.
3. Select the **Date** range you want to query.
4. From the **Service** filter, select **Conditional Access** and select the **Apply** button.

The audit logs display all activities, by default. Open the **Activity** filter to narrow down the activities. For a full list of the audit log activities for Conditional Access, see the [Audit log activities](#).

5. To view the details, select a row. The **Modified Properties** tab lists the modified JSON values for the selected audit activity.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation pane includes sections like Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, Audit logs (which is selected and highlighted with a red box), Provisioning logs, Health (Preview), and Learn & support.

The main content area is titled "Audit Logs" and shows a table of audit log entries. The table has columns for Date, Target(s), and Modified Properties. A red box highlights the "Modified Properties" tab and the first row of the table, which details a policy change:

Target	Property Name	Old Value	New Value
access pol...	ConditionalAcc...	<code>{"id": "d18e74a5-7c8c-4e69-afe2-6ef5450de4fd", "displayName": "access policy", "createdDateTime": "2024-03-22T16:07:09.2359994+00:00", "modifiedDateTime": "2024-03-22T16:18:28.2477554+00:00", "state": "enabled", "conditions": {"applications": [{"applicationFilter": "null", "users": [{"includeUsers": ["All"], "excludeUsers": []}, {"includeGroups": [], "excludeGroups": []}, {"includeLocations": [{"includeLocations": ["All"], "excludeLocations": []}, {"userRiskLevels": [{"userRiskLevels": ["All"], "signlnRiskLevels": []}], "clientAppTypes": [{"clientAppTypes": ["all"], "servicePrincipalRiskLevels": []}], "grantControls": {"operator": "OR", "builtinControls": ["mfa"], "customAuthenticationFactors": [{"termsOfUse": []}]}]}]}]</code>	<code>{"id": "d18e74a5-7c8c-4e69-afe2-6ef5450de4fd", "displayName": "access policy", "createdDateTime": "2024-03-22T16:07:09.2359994+00:00", "modifiedDateTime": "2024-03-22T16:18:28.2477554+00:00", "state": "enabled", "conditions": {"applications": [{"applicationFilter": "null", "users": [{"includeUsers": ["All"], "excludeUsers": []}, {"includeGroups": [], "excludeGroups": []}, {"includeLocations": [{"includeLocations": ["All"], "excludeLocations": []}, {"userRiskLevels": [{"userRiskLevels": ["All"], "signlnRiskLevels": []}], "clientAppTypes": [{"clientAppTypes": ["all"], "servicePrincipalRiskLevels": []}], "grantControls": {"operator": "OR", "builtinControls": ["mfa"], "customAuthenticationFactors": [{"termsOfUse": []}]}]}]}}</code>

Use Log Analytics

Log Analytics allows organizations to query data using built in queries or custom created Kusto queries, for more information, see [Get started with log queries in Azure Monitor](#).

The screenshot shows the Microsoft Azure Log Analytics workspace for the Contoso tenant. The left sidebar includes sections like Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, Mobility (MDM and MAM), Password reset, Company branding, User settings, Properties, Security, Monitoring, Sign-in logs, Audit logs, Provisioning logs, and Log Analytics (which is selected and highlighted with a red box).

The main area displays a Kusto query results table. A red box highlights the query itself:

```

1 AuditLogs
2 | where OperationName == "Update conditional access policy"

```

The results table shows two records from the last 12 hours:

TimeGenerated [Local Time]	ResourceID	OperationName
2024-03-22T16:07:09.2359994+00:00	IPCGraph_f5afdf5ee-0e51-409f-829f-46b25bb6006a_YA45U_6628328	Update conditional access policy
2024-03-22T16:18:28.2477554+00:00	IPCGraph_f5afdf5ee-0e51-409f-829f-46b25bb6006a_YA45U_6628328	Update conditional access policy

Each record has expanded rows for TargetResources and modifiedProperties, also highlighted with red boxes:

- TargetResources:**
 - Id: 334e26e9-9622-4e0a-a424-102ed4b185b3
 - InitiatedBy: user:f74e3dc5-134f-4182-8e2c-fd28b75a4318
 - LoggedByService: Conditional Access
 - Result: success
 - ResultReason: <null>
- modifiedProperties:**
 - displayName: Common Policy - Require MFA for Azure management
 - id: 334e26e9-9622-4e0a-a424-102ed4b185b3
 - modifiedProperties: [{"id": "334e26e9-9622-4e0a-a424-102ed4b185b3", "oldValue": "Common Policy - Require MFA for Azure management"}]
 - oldValue: "Common Policy - Require MFA for Azure management"
 - newValue: "Common Policy - Common Policy - Require MFA for Azure management"

Once enabled find access to Log Analytics in the **Entra ID > Monitoring & health > Log Analytics**. The table of most interest to Conditional Access Administrators is **AuditLogs**.

Kusto

AuditLogs

```
| where OperationName == "Update Conditional Access policy"
```

Changes can be found under **TargetResources > modifiedProperties**.

Reading the values

The old and new values from the audit log and Log Analytics are in JSON format. Compare the two values to see the changes to the policy.

Old policy example:

JSON

```
{
  "conditions": {
    "applications": {
      "applicationFilter": null,
      "excludeApplications": [
      ],
      "includeApplications": [
        "797f4846-ba00-4fd7-ba43-dac1f8f63013"
      ],
      "includeAuthenticationContextClassReferences": [
      ],
      "includeUserActions": [
      ]
    },
    "clientAppTypes": [
      "browser",
      "mobileAppsAndDesktopClients"
    ],
    "servicePrincipalRiskLevels": [
    ],
    "signInRiskLevels": [
    ],
    "userRiskLevels": [
    ],
    "users": {
      "excludeGroups": [
        "eedad040-3722-4bcb-bde5-bc7c857f4983"
      ],
      "excludeRoles": [
      ],
      "excludeUsers": [
      ]
    }
  }
}
```

```

        ],
        "includeGroups": [
        ],
        "includeRoles": [
        ],
        "includeUsers": [
            "All"
        ]
    }
},
"displayName": "Common Policy - Require MFA for Azure management",
"grantControls": {
    "builtInControls": [
        "mfa"
    ],
    "customAuthenticationFactors": [
    ],
    "operator": "OR",
    "termsOfUse": [
        "a0d3eb5b-6cbe-472b-a960-0baacbd02b51"
    ]
},
"id": "334e26e9-9622-4e0a-a424-102ed4b185b3",
"modifiedDateTime": "2021-08-09T17:52:40.781994+00:00",
"state": "enabled"
}

```

Updated policy example:

JSON

```
{
    "conditions": {
        "applications": {
            "applicationFilter": null,
            "excludeApplications": [
            ],
            "includeApplications": [
                "797f4846-ba00-4fd7-ba43-dac1f8f63013"
            ],
            "includeAuthenticationContextClassReferences": [
            ],
            "includeUserActions": [
            ]
        },
        "clientAppTypes": [
            "browser",
            "mobileAppsAndDesktopClients"
        ],
        "servicePrincipalRiskLevels": [
        ],
        "signInRiskLevels": [

```

```
        ],
        "userRiskLevels": [
        ],
        "users": {
            "excludeGroups": [
                "eedad040-3722-4bcb-bde5-bc7c857f4983"
            ],
            "excludeRoles": [
            ],
            "excludeUsers": [
            ],
            "includeGroups": [
            ],
            "includeRoles": [
            ],
            "includeUsers": [
                "All"
            ]
        }
    },
    "displayName": "Common Policy - Require MFA for Azure management",
    "grantControls": {
        "builtInControls": [
            "mfa"
        ],
        "customAuthenticationFactors": [
        ],
        "operator": "OR",
        "termsOfUse": [
        ]
    },
    "id": "334e26e9-9622-4e0a-a424-102ed4b185b3",
    "modifiedDateTime": "2021-08-09T17:52:54.9739405+00:00",
    "state": "enabled"
}
```

In the previous example, the updated policy doesn't include terms of use in grant controls.

Related content

- [What is Microsoft Entra monitoring?](#)
- [Install and use the log analytics views for Microsoft Entra ID](#)

Troubleshooting sign-in problems with Conditional Access

Article • 03/04/2025

Use this article to troubleshoot unexpected sign-in outcomes related to Conditional Access using error messages and Microsoft Entra sign-in logs.

Select "all" consequences

The Conditional Access framework provides great configuration flexibility. However, great flexibility also means that you should carefully review each configuration policy before releasing it to avoid undesirable results. In this context, pay special attention to assignments affecting complete sets such as **all users / groups / cloud apps**.

Organizations should avoid the following configurations:

For all users, all resources:

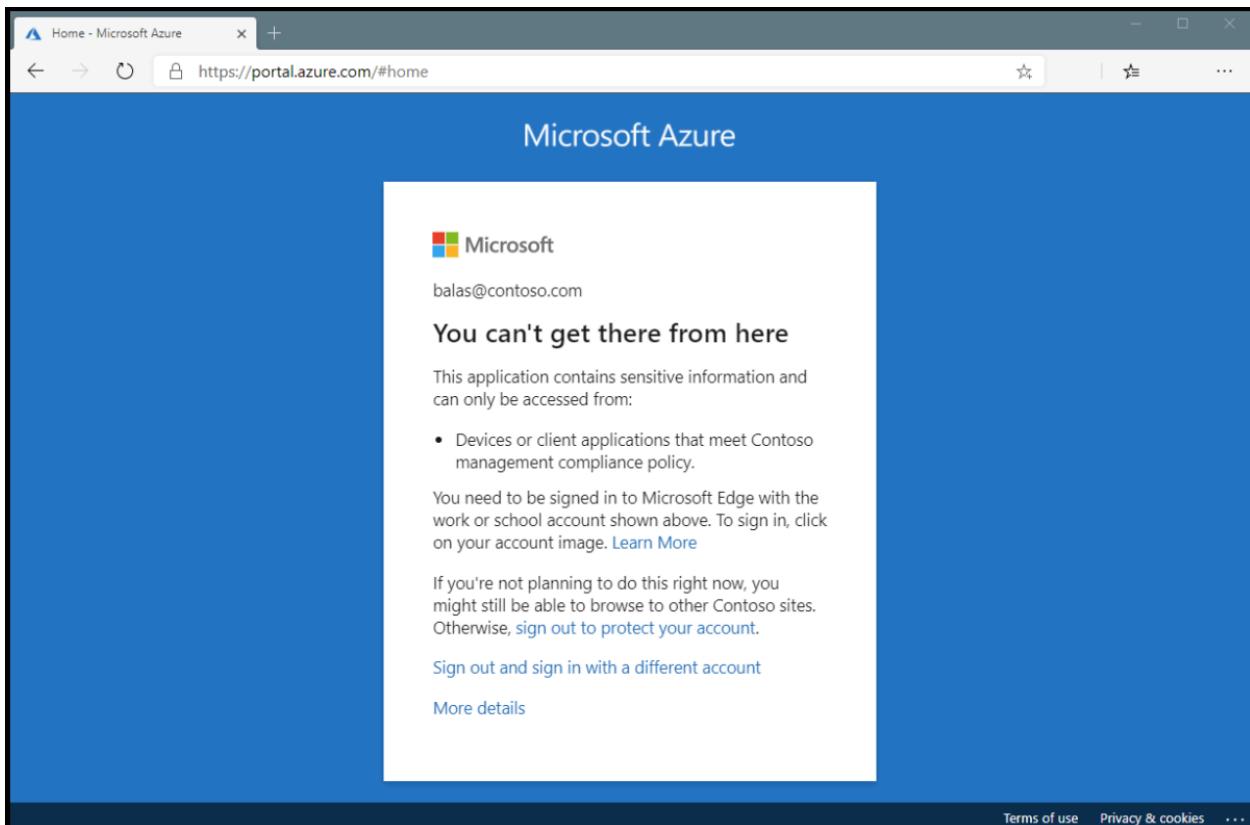
- **Block access** - This configuration blocks the entire organization.
- **Require device to be marked as compliant** - For users that haven't enrolled their devices yet, this policy blocks all access including access to the Intune portal. If you're an administrator without an enrolled device, this policy blocks you from getting back in to change the policy.
- **Require Hybrid Microsoft Entra domain joined device** - This policy also has the potential to block access for all users in your organization if they don't have a Microsoft Entra hybrid joined device.
- **Require app protection policy** - This policy also has the potential to block access for all users in your organization if you don't have an Intune policy. If you're an administrator without a client application that has an Intune app protection policy, this policy blocks you from getting back into portals such as Intune and Azure.

For all users, all resources, all device platforms:

- **Block access** - This configuration blocks your entire organization.

Conditional Access sign-in interrupt

Review the error message that appears. For problems signing in when using a web browser, the error page itself has detailed information. This information alone might describe the problem and suggest a solution.

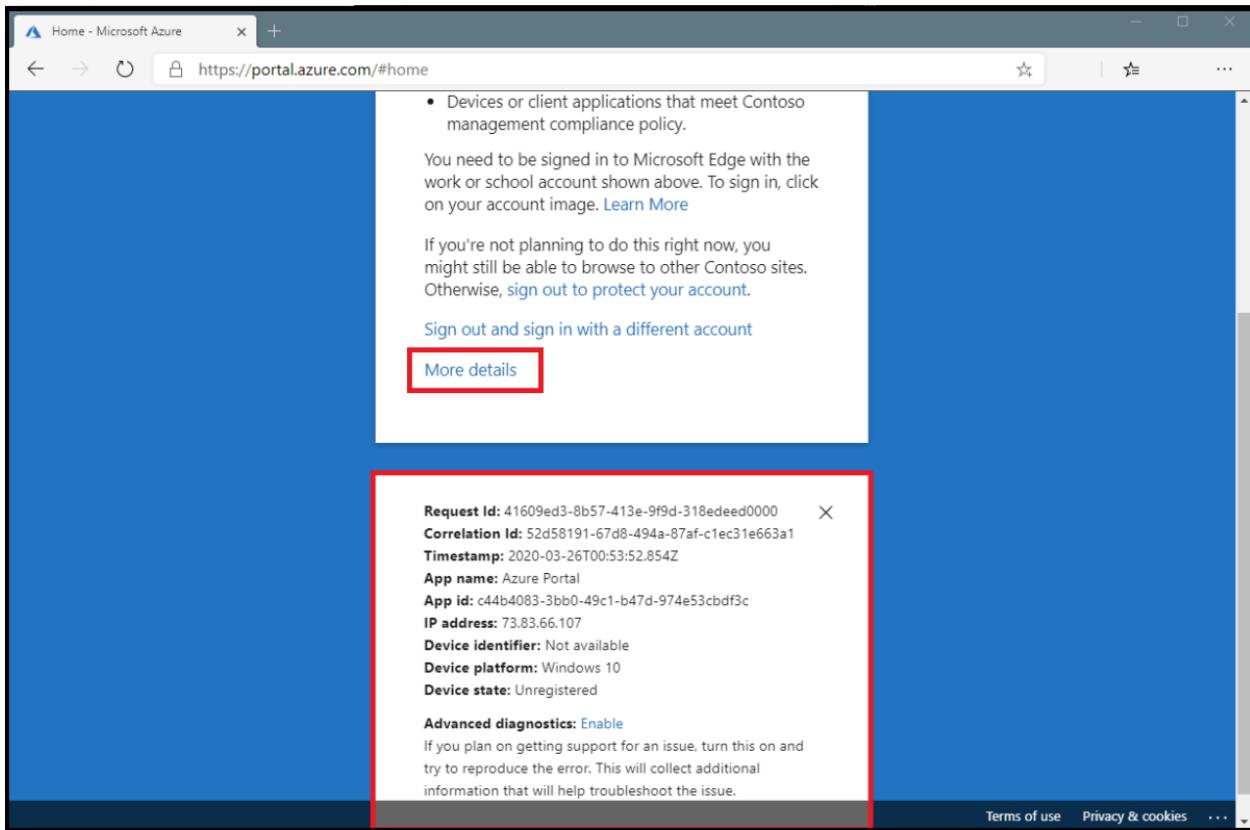


In the above error, the message states that the application can only be accessed from devices or client applications that meet the company's mobile device management policy. In this case, the application and device don't meet the policy.

Microsoft Entra sign-in events

The second method to get detailed information about the sign-in interruption is to review the Microsoft Entra sign-in events to see which Conditional Access policy or policies were applied and why.

More information can be found about the problem by clicking **More Details** in the initial error page. Clicking **More Details** reveals troubleshooting information that is helpful when searching the Microsoft Entra sign-in events for the specific failure event the user saw or when opening a support incident with Microsoft.



To find out which Conditional Access policy or policies applied and why, follow these steps.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Reports Reader**.
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Find the event for the sign-in to review. Add or remove filters and columns to filter out unnecessary information.
 - a. Narrow the scope by adding filters like:
 - i. **Correlation ID** when you have a specific event to investigate.
 - ii. **Conditional Access** to see policy failure and success. Scope your filter to show only failures to limit results.
 - iii. **Username** to see information related to specific users.
 - iv. **Date** scoped to the time frame in question.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, and the main area is titled "Sign-in events". At the top right, there are download, export, troubleshoot, refresh, column settings, and feedback links. A message box says "Want to switch back to the default sign-ins experience? Click here to leave the preview." Below this, there are filter buttons for date (Last 24 hours), show dates as (Local), status (Failure, highlighted with a red box), and add filters. The table below has tabs for User sign-ins (interactive), User sign-ins (non-interactive), Service principal sign-ins, and Managed identity. The "User sign-ins (interactive)" tab is selected. The columns are Date, Request ID, User, Application, and Status. One row is shown: Date 3/21/2024, 1:01:18 PM, Request ID a0a0a0a0-bbbb-ccc..., User MOD Administrator, Application Microsoft App Acces..., Status Failure.

4. After finding the sign-in event that corresponds to the user's sign-in failure, select the **Conditional Access** tab. The Conditional Access tab shows the specific policy or policies that resulted in the sign-in interruption.
 - a. Information in the **Troubleshooting and support** tab might provide a clear reason as to why a sign-in failed such as a device that didn't meet compliance requirements.
 - b. To investigate further, drill down into the configuration of the policies by clicking on the **Policy Name**. Clicking the **Policy Name** shows the policy configuration user interface for the selected policy for review and editing.
 - c. The **client user** and **device details** that were used for the Conditional Access policy assessment are also available in the **Basic Info**, **Location**, **Device Info**, **Authentication Details**, and **Additional Details** tabs of the sign-in event.

Policy not working as intended

Selecting the ellipsis on the right side of the policy in a sign-in event brings up policy details. This option gives administrators additional information about why a policy was successfully applied or not.

The left side provides details collected at sign-in and the right side provides details of whether those details satisfy the requirements of the applied Conditional Access policies. Conditional Access policies only apply when all conditions are satisfied or not configured.

If the information in the event isn't enough to understand the sign-in results or adjust the policy to get desired results, use the sign-in diagnostic tool. The sign-in diagnostic is under **Basic info > Troubleshoot Event**. For more information about the sign-in diagnostic, see [What is the sign-in diagnostic in Microsoft Entra ID](#). You can also [use the What If tool to troubleshoot Conditional Access policies](#).

If you need to submit a support incident, provide the request ID and time and date from the sign-in event in the incident submission details. This information allows Microsoft support to find the specific event you're concerned about.

Common Conditional Access error codes

[Expand table](#)

Sign-in Error Code	Error String
53000	DeviceNotCompliant
53001	DeviceNotDomainJoined
53002	ApplicationUsedIsNotAnApprovedApp
53003	BlockedByConditionalAccess

Sign-in Error Code	Error String
53004	ProofUpBlockedDueToRisk
53009	Application needs to enforce Intune protection policies

More information about error codes can be found in the article [Microsoft Entra authentication and authorization error codes](#). Error codes in the list appear with a prefix of `AADSTS` followed by the code seen in the browser, for example `AADSTS53002`.

Service dependencies

In some scenarios, users are blocked because cloud apps depend on resources blocked by Conditional Access policy.

To determine the service dependency, check the sign-in log for the application and resource called by the sign-in. In the following screenshot, the application called is **Azure Portal** but the resource called is **Windows Azure Service Management API**. To target this scenario appropriately all the applications and resources should be similarly combined in Conditional Access policy.

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	3/22/2024, 11:56:26 AM				
Request ID	0x00000-0000-0000-x00x-0xxx0x00x0				
Correlation ID	0x00000-0000-0000-x00x-0xxx0x00x0				
Authentication requirement	Single-factor authentication				
Status	Success				
Continuous access evaluation	No				

Follow these steps:

Troubleshoot Event [Launch the Sign-in Diagnostic](#).
1. Review the diagnosis and act on suggested fixes.

User	MOD Administrator
Username	admin@contoso.com
User ID	0x00000-0000-0000-x00x-0xxx0x00x0
Sign-in identifier	admin@contoso.com
User type	Member
Cross tenant access type	None

Application	Azure Portal
Application ID	0x00000-0000-0000-x00x-0xxx0x00x0
Resource	Windows Azure Service Management API
Resource ID	0x00000-0000-0000-x00x-0xxx0x00x0

Resource tenant ID: 0x00000-0000-0000-x00x-0xxx0x00x0
Home tenant ID: 0x00000-0000-0000-x00x-0xxx0x00x0
Home tenant name:

What to do if you're locked out

If you're locked out due to an incorrect setting in a Conditional Access policy:

- Check if there are other administrators in your organization who aren't blocked yet. An administrator with access can disable the policy that is impacting your sign-in.
- If none of the administrators in your organization can update the policy, submit a support request. Microsoft support can review and upon confirmation update the Conditional Access policies that are preventing access.

Next steps

- [Use the What If tool to troubleshoot Conditional Access policies](#)
 - [Sign-in activity reports](#)
 - [Troubleshooting Conditional Access using the What If tool](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Troubleshooting Conditional Access using the What If tool

Article • 08/13/2024

The [What If tool](#) in Conditional Access is powerful when trying to understand why a policy was or wasn't applied to a user in a specific circumstance or if a policy would apply in a known state.

The What If tool is located in the **Microsoft Entra admin center > Protection > Conditional Access > Policies > What If**.

What If



Policies

[Info](#) [Preview features](#) | [Got feedback?](#)

Test the impact of Conditional Access on a user when signing in under certain conditions. [Learn more](#)

User or Workload identity [i](#)

[No user or service principal selected](#)

✗ User or Service principal required

Cloud apps, actions, or authentication context [i](#)

[Any cloud app](#)

IP address [i](#)

Enter IP address (ex: 40.77.182.32)

Country [i](#)

Select country...



Device platform [i](#)

Select device platform...



Client apps [i](#)

Select a client app...



Device state (deprecated) [i](#)

Select device state...



Filter for devices [i](#)

Property

Value

<Pick a property and operator first>

<Pick a property and operator first>

What If

Reset

Gathering information

The What If tool requires only a **User or Workload identity** to get started.

The following additional information is optional but helps narrow the scope for specific cases.

- Cloud apps, actions, or authentication context
- IP address
- Country/Region
- Device platform
- Client apps
- Device state
- Sign-in risk
- User risk level
- Service principal risk (Preview)
- Filter for devices

This information can be gathered from the user, their device, or the Microsoft Entra sign-in log.

Generating results

Input the criteria gathered in the previous section and select **What If** to generate a list of results.

At any point, you can select **Reset** to clear any criteria input and return to the default state.

Evaluating results

Policies that will apply

This list shows which Conditional Access policies would apply given the conditions. The list includes both the grant and session controls that apply including policies in report-only mode. Examples include requiring multifactor authentication to access a specific application.

Policies that won't apply

This list shows Conditional Access policies that wouldn't apply if the conditions applied. The list includes any policies and the reason why they don't apply including policies in report-only mode. Examples include users and groups that might be excluded from a policy.

Use case

Many organizations create policies based on network locations, permitting trusted locations and blocking locations where access shouldn't occur.

To validate that a configuration is appropriate, an administrator could use the What If tool to mimic access, from a location that should be allowed and from a location that should be denied.

The screenshot shows the 'What If' configuration page for Conditional Access Policies. It includes fields for User or Workload identity (set to Adele Vance), Cloud apps, actions, or authentication context (set to Any cloud app), IP address (set to 192.168.0.0), Country (set to United States), Device platform, Client apps, Device state (deprecated), and a Filter for devices section. Below this is an 'Evaluation result' section showing 'Policies that will apply' (access policy) and 'Policies that will not apply' (Require multifactor authentication). A search bar and filter options are also present.

In this instance, the user would be blocked from accessing any cloud app on their trip to North Korea as Contoso blocked access from that location.

This test could be expanded to incorporate other data points to narrow the scope.

Related content

- [What is Conditional Access report-only mode?](#)
- [What is Microsoft Entra ID Protection?](#)
- [What is a device identity?](#)
- [How it works: Microsoft Entra multifactor authentication](#)

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Monitor and troubleshoot continuous access evaluation

Article • 06/27/2024

Administrators can monitor and troubleshoot sign in events where [continuous access evaluation \(CAE\)](#) is applied in multiple ways.

Continuous access evaluation sign-in reporting

Administrators can monitor user sign-ins where continuous access evaluation (CAE) is applied. This information is found in the Microsoft Entra sign-in logs:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Reader](#).
2. Browse to **Identity > Monitoring & health > Sign-in logs**.
3. Apply the **Is CAE Token** filter.

Date	Request ID	Conditional Access	Authentication requir...
4/3/2023, 1:37:40 PM	46541c5c-4bba-4ec9-93	Not Applied	Single-factor authentication
4/3/2023, 1:37:21 PM	b7cd83ea-ed5e-49cd-bc	Not Applied	Single-factor authentication
4/3/2023, 1:36:03 PM	d60cf2d4-dc50-42fe-8d	Success	Multifactor authentication
4/3/2023, 1:36:00 PM	56a197d6-2b4c-4cf0-bf	Success	Multifactor authentication
4/3/2023, 1:35:58 PM	56a197d6-2b4c-4cf0-bf	Failure	Multifactor authentication
4/3/2023, 1:35:55 PM	83e6eb91-c7ea-4818-92	Failure	Multifactor authentication
4/3/2023, 1:35:17 PM	81d9b590-a9b7-40c8-96	Success	Multifactor authentication
4/3/2023, 1:35:15 PM	01c82799-905a-47db-93	Success	Multifactor authentication
4/3/2023, 1:35:15 PM	65389f71-d5ac-46eb-84	Success	Multifactor authentication
4/3/2023, 1:35:15 PM	aaf3a880-d51a-44a5-b5	Success	Multifactor authentication

From here, admins are presented with information about their user's sign-in events. Select any sign-in to see details about the session, like which Conditional Access policies applied and if CAE enabled.

There are multiple sign-in requests for each authentication. Some are on the interactive tab, while others are on the non-interactive tab. CAE is only marked true for one of the requests it can be on the interactive tab or non-interactive tab. Admins must check both tabs to confirm whether the user's authentication is CAE enabled or not.

Searching for specific sign-in attempts

Sign-in logs contain information on success and failure events. Use filters to narrow your search. For example, if a user signed in to Teams, use the Application filter and set it to Teams. Admins might need to check the sign-ins from both interactive and non-interactive tabs to locate the specific sign-in. To further narrow the search, admins might apply multiple filters.

Continuous access evaluation workbooks

The continuous access evaluation insights workbook allows administrators to view and monitor CAE usage insights for their tenants. The table displays authentication attempts with IP mismatches. This workbook can be found as template under the Conditional Access category.

Accessing the CAE workbook template

Log Analytics integration must be completed before workbooks are displayed. For more information about how to stream Microsoft Entra sign-in logs to a Log Analytics workspace, see the article [Integrate Microsoft Entra logs with Azure Monitor logs](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Reader](#).
2. Browse to **Identity > Monitoring & health > Workbooks**.
3. Under **Public Templates**, search for **Continuous access evaluation insights**.

The **Continuous access evaluation insights** workbook contains the following table:

Potential IP address mismatch between Microsoft Entra ID and resource provider

The potential IP address mismatch between Microsoft Entra ID & resource provider table allows admins to investigate sessions where the IP address detected by Microsoft Entra ID doesn't match with the IP address detected by the resource provider.

This workbook table sheds light on these scenarios by displaying the respective IP addresses and whether a CAE token was issued during the session.

Continuous access evaluation insights per sign-in

The continuous access evaluation insights per sign-in page in the workbook connects multiple requests from the sign-in logs and displays a single request where a CAE token

was issued.

This workbook can come in handy, for example, when: A user opens Outlook on their desktop and attempts to access resources inside of Exchange Online. This sign-in action might map to multiple interactive and non-interactive sign-in requests in the logs making issues hard to diagnose.

IP address configuration

Your identity provider and resource providers might see different IP addresses. This mismatch might happen because of the following examples:

- Your network implements split tunneling.
- Your resource provider is using an IPv6 address and Microsoft Entra ID is using an IPv4 address.
- Because of network configurations, Microsoft Entra ID sees one IP address from the client and your resource provider sees a different IP address from the client.

If this scenario exists in your environment, to avoid infinite loops, Microsoft Entra ID issues a one-hour CAE token and doesn't enforce client location change during that one-hour period. Even in this case, security is improved compared to traditional one-hour tokens since we're still evaluating the other events besides client location change events.

Admins can view records filtered by time range and application. Admins can compare the number of mismatched IPs detected with the total number of sign-ins during a specified time period.

To unblock users, administrators can add specific IP addresses to a trusted named location.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Protection > Conditional Access > Named locations**. Here you can create or update trusted IP locations.

Note

Before adding an IP address as a trusted named location, confirm that the IP address does in fact belong to the intended organization.

For more information about named locations, see the article [Using the location condition](#).

Related content

- [Integrate Microsoft Entra logs with Azure Monitor logs](#)
 - [Using the location condition](#)
 - [Continuous access evaluation](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#) ↗

Migrate approved client app to application protection policy in Conditional Access

Article • 04/25/2025

In this article, you learn how to migrate from the approved client app Conditional Access grant to the application protection policy grant. App protection policies provide the same data loss and protection as approved client app policies, but with other benefits. For more information about the benefits of using app protection policies, see the article [App protection policies overview](#).

The approved client app grant is retiring in early March 2026. Organizations must transition all current Conditional Access policies that use **only** the Require Approved Client App grant control to Require Approved Client App **or** Application Protection Policy by March 2026. Additionally, for any new Conditional Access policy, only apply the Require application protection policy grant.

After March 2026, Microsoft will stop enforcing require approved client app control, and it will be as if this grant isn't selected. Use the following steps before March 2026 to protect your organization's data.

Edit an existing Conditional Access policy

Require approved client apps or app protection policy with mobile devices

The following steps make an existing Conditional Access policy require an approved client app or an app protection policy when using an iOS/iPadOS or Android device. This policy works in tandem with an app protection policy created in Microsoft Intune.

Organizations can choose to update their policies using the following steps.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Entra ID > Conditional Access > Policies**.
3. Select a policy that uses the approved client app grant.
4. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require approved client app** and **Require app protection policy**
 - b. **For multiple controls** select **Require one of the selected controls**
5. Confirm your settings and set **Enable policy** to **Report-only**.
6. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

Repeat the previous steps on all of your policies that use the approved client app grant.

Warning

Not all applications that are supported as approved applications are supported by application protection policies. For a list of some common client apps, see [App protection policy requirement](#). If your application is not listed there, contact the application developer.

Create a Conditional Access policy

Require app protection policy with mobile devices

The following steps help create a Conditional Access policy requiring an approved client app or an app protection policy when using an iOS/iPadOS or Android device. This policy works in tandem with an [app protection policy created in Microsoft Intune](#).

Organizations can choose to deploy this policy using the following steps.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Entra ID > Conditional Access > Policies**.
3. Select **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
 - a. Under **Include**, select **All users**.
 - b. Under **Exclude**, select **Users and groups** and exclude at least one account to prevent yourself from being locked out. If you don't exclude any accounts, you can't create the policy.
6. Under **Target resources > Resources (formerly cloud apps) > Include**, select **All resources (formerly 'All cloud apps')**
7. Under **Conditions > Device platforms**, set **Configure** to **Yes**.
 - a. Under **Include**, Select **device platforms**.
 - b. Choose **Android and iOS**
 - c. Select **Done**.
8. Under **Access controls > Grant**, select **Grant access**.
 - a. Select **Require approved client app** and **Require app protection policy**
 - b. For multiple controls select **Require one of the selected controls**
9. Confirm your settings and set **Enable policy** to **Report-only**.
10. Select **Create** to create to enable your policy.

After administrators evaluate the policy settings using [policy impact or report-only mode](#), they can move the **Enable policy** toggle from **Report-only** to **On**.

 **Note**

If an app does not support **Require app protection policy**, end users trying to access resources from that app will be blocked.

Next steps

For more information on application protection policies, see:

[App protection policies overview](#)

Apps included in Conditional Access Office 365 app suite

Article • 04/17/2025

The following list is provided as a reference and includes a detailed list of services and applications that are included in the Conditional Access [Office 365](#) app.

- App Studio for Microsoft Teams
- Augmentation Loop
- Call Recorder
- Connectors
- DataSecurityInvestigation
- Device Management Service
- EDU Assignments
- EnrichmentSvc
- Enterprise Copilot Platform
- Groups Service
- IC3 Gateway
- IC3 Gateway Non Cae
- Insights Services
- INT Augmentation Loop 1P
- Legacy Smart Compose
- Loop
- Loop Web Application
- Loop Web Service
- M365 Admin Services
- M365 Auditing Public Protected Web API app
- M365ChatClient
- make.gov.powerapps.us
- make.powerapps.com
- Media Analysis and Transformation Service
- Media Analysis and Transformation Service
- Message Recall
- Messaging Async Media
- MessagingAsyncMediaProd
- Microsoft 365 Reporting Service
- Microsoft Discovery Service
- Microsoft Exchange Online Protection
- Microsoft Flow Portal
- Microsoft Flow Portal GCC

- Microsoft Forms
- Microsoft Forms Web
- Microsoft Forms Web
- Microsoft Information Protection API
- Microsoft Office
- Microsoft Office 365 Portal
- Microsoft People Cards Service
- Microsoft Planner
- Microsoft Planner Client
- Microsoft SharePoint Online - SharePoint Home
- Microsoft Stream Portal
- Microsoft Stream Service
- Microsoft Teams
- Microsoft Teams - T4L Web Client
- Microsoft Teams - Teams And Channels Service
- Microsoft Teams Analytics
- Microsoft Teams Chat Aggregator
- Microsoft Teams Graph Service
- Microsoft Teams Mailhook
- Microsoft Teams Retail Service
- Microsoft Teams Services
- Microsoft Teams Targeting Application
- Microsoft Teams UIS
- Microsoft Teams Web Client
- Microsoft Todo web app
- Microsoft To-Do web app
- Microsoft Virtual Events Portal
- Microsoft Virtual Events Services
- Microsoft Visio Data Visualizer
- Microsoft Whiteboard Services
- MSAI Substrate Meeting Intelligence
- Natural Language Editor
- O365 Diagnostic Service
- O365 Suite UX
- O365 Suite UX PathFinder
- OCPS Checkin Service
- Office 365
- Office 365 Exchange Microservices
- Office 365 Exchange Online
- Office 365 Search Service
- Office 365 SharePoint Online

- Office Collab Actions
- Office Delve
- Office Hive
- Office Hive Fairfax
- Office MRO Device Manager Service
- Office Online Add-in SSO
- Office Online Augmentation Loop SSO
- Office Online Core SSO
- Office Online Loki SSO
- Office Online Maker SSO
- Office Online Print SSO
- Office Online Search SSO
- Office Online Service
- Office Online Speech SSO
- Office Scripts Service
- Office Scripts Service - INT
- Office Scripts Service - Local
- Office Scripts Service - Test
- Office Shredding Service
- Office.com
- Office365 Shell DoD WCSS-Client
- Office365 Shell WCSS-Client
- OfficeClientService
- OfficeHome
- OfficePowerPointSGS
- OfficeServicesManager
- Olympus
- OMEX External
- One Outlook Web
- OneDrive
- OneDrive SyncEngine
- OneNote
- Outlook Browser Extension
- Outlook Service for Exchange
- PowerApps Service
- Project for the web
- ProjectWorkManagement
- ProjectWorkManagement_AdminTools
- ProjectWorkManagement_USGov
- Protection Center
- Reply-At-Mention

- SharePoint eSignature
- SharePoint eSignature PPE
- SharePoint Online Web Client Extensibility
- SharePoint Online Web Client Extensibility Isolated
- Skype and Teams Tenant Admin API
- Skype for Business
- Skype for Business Online
- Skype Presence Service
- Sway
- Targeted Messaging Service
- Teams CMD Services Artifacts
- Teams Walkie Talkie Service
- Teams Walkie Talkie Service - GCC
- Viva Engage

conditionalAccessPolicy resource type

Article • 07/23/2024

Namespace: microsoft.graph

Represents a Microsoft Entra Conditional Access policy. Conditional access policies are custom rules that define an access scenario. For more information, see the [Conditional access documentation](#).

Methods

[+] [Expand table](#)

Method	Return Type	Description
List	conditionalAccessPolicy collection	Get all of the conditionalAccessPolicies objects in the organization.
Create	conditionalAccessPolicy	Create a new conditionalAccessPolicy object.
Get	conditionalAccessPolicy	Read properties and relationships of a conditionalAccessPolicy object.
Update	conditionalAccessPolicy	Update a conditionalAccessPolicy object.
Delete	None	Delete a conditionalAccessPolicy object.

Properties

[+] [Expand table](#)

Property	Type	Description
conditions	conditionalAccessConditionSet	Specifies the rules that must be met for the policy to apply. Required.
createdDateTime	DateTimeOffset	The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Readonly.
displayName	String	Specifies a display name for the conditionalAccessPolicy object.
grantControls	conditionalAccessGrantControls	Specifies the grant controls that must be

Property	Type	Description
		fulfilled to pass the policy.
id	String	Specifies the identifier of a conditionalAccessPolicy object. Read-only.
modifiedDateTime	DateTimeOffset	The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Readonly.
sessionControls	conditionalAccessSessionControls	Specifies the session controls that are enforced after sign-in.
state	conditionalAccessPolicyState	Specifies the state of the conditionalAccessPolicy object. Possible values are: <code>enabled</code> , <code>disabled</code> , <code>enabledForReportingButNotEnforced</code> . Required.

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON
<pre>{ "conditions": {"@odata.type": "microsoft.graph.conditionalAccessConditionSet"}, "createdDateTime": "String (timestamp)", "displayName": "String", "grantControls": {"@odata.type": "microsoft.graph.conditionalAccessGrantControls"}, "id": "String (identifier)", "modifiedDateTime": "String (timestamp)", "sessionControls": {"@odata.type": "microsoft.graph.conditionalAccessSessionControls"}, "state": "string" }</pre>

namedLocation resource type

Article • 07/22/2024

Namespace: microsoft.graph

This is the base class that represents a Microsoft Entra ID named location. Named locations are custom rules that define network locations which can then be used in a Conditional Access policy.

Methods

[] [Expand table](#)

Method	Return Type	Description
List	namedLocation collection	Get all the namedLocation objects in the organization.
Get	namedLocation	Read the properties and relationships of a namedLocation object.
Delete	None	Delete a namedLocation object.

Properties

[] [Expand table](#)

Property	Type	Description
createdDateTime	DateTimeOffset	The Timestamp type represents creation date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only.
displayName	String	Human-readable name of the location.
id	String	Identifier of a namedLocation object. Read-only.
modifiedDateTime	DateTimeOffset	The Timestamp type represents last modified date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only.

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON

```
{  
  "createdDateTime": "String (timestamp)",  
  "displayName": "String",  
  "id": "String (identifier)",  
  "modifiedDateTime": "String (timestamp)"  
}
```

Related content

- [What is Conditional Access?](#)
- [Using the location condition in a Conditional Access policy](#)

countryNamedLocation resource type

Article • 07/23/2024

Namespace: microsoft.graph

Represents a Microsoft Entra ID named location defined by countries and regions. Named locations are custom rules that define network locations which can then be used in a Conditional Access policy.

Inherits from [namedLocation](#)

Methods

 [Expand table](#)

Method	Return Type	Description
List	countryNamedLocation collection	Get all the countryNamedLocation objects in the organization.
Create	countryNamedLocation	Create a new countryNamedLocation object.
Get	countryNamedLocation	Read the properties and relationships of a countryNamedLocation object.
Update	countryNamedLocation	Update a countryNamedLocation object.
Delete	None	Delete a countryNamedLocation object.

Properties

 [Expand table](#)

Property	Type	Description
countriesAndRegions	String collection	List of countries and/or regions in two-letter format specified by ISO 3166-2. Required.
countryLookupMethod	countryLookupMethodType	Determines what method is used to decide which country the user is located in. Possible values are <code>clientIpAddress</code> (default) and <code>authenticatorAppGps</code> . Note: <code>authenticatorAppGps</code> is not yet

Property	Type	Description
		supported in the Microsoft Cloud for US Government.
createdDateTime	DateTimeOffset	The Timestamp type represents creation date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only. Inherited from namedLocation .
displayName	String	Human-readable name of the location. Required. Inherited from namedLocation .
id	String	Identifier of a namedLocation object. Read-only. Inherited from namedLocation .
includeUnknownCountriesAndRegions	Boolean	<code>true</code> if IP addresses that don't map to a country or region should be included in the named location. Optional. Default value is <code>false</code> .
modifiedDateTime	DateTimeOffset	The Timestamp type represents last modified date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only. Inherited from namedLocation .

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON

```
{
  "countriesAndRegions": ["String"],
```

```
"countryLookupMethod": "String",
"createdDateTime": "String (timestamp)",
"displayName": "String",
"id": "String (identifier)",
"includeUnknownCountriesAndRegions": true,
"modifiedDateTime": "String (timestamp)"
}
```

Related content

- [What is Conditional Access?](#)
- [Using the location condition in a Conditional Access policy](#)

ipNamedLocation resource type

Article • 05/24/2024

Namespace: microsoft.graph

Represents a Microsoft Entra ID named location defined by IP ranges. Named locations are custom rules that define network locations that can then be used in a Conditional Access policy.

Inherits from [namedLocation](#)

Methods

 [Expand table](#)

Method	Return Type	Description
List	ipNamedLocation collection	Get all the ipNamedLocation objects in the organization.
Create	ipNamedLocation	Create a new ipNamedLocation object.
Get	ipNamedLocation	Read the properties and relationships of an ipNamedLocation object.
Update	ipNamedLocation	Update an ipNamedLocation object.
Delete	None	Delete an ipNamedLocation object.

Properties

 [Expand table](#)

Property	Type	Description
createdDateTime	DateTimeOffset	The Timestamp type represents creation date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only. Inherited from namedLocation .
displayName	String	Human-readable name of the location. Required.
id	String	Identifier of a namedLocation object. Read-only. Inherited from namedLocation .

Property	Type	Description
ipRanges	ipRange collection	List of IP address ranges in IPv4 CIDR format (for example, 1.2.3.4/32) or any allowable IPv6 format from IETF RFC5969. Required.
isTrusted	Boolean	<code>true</code> if this location is explicitly trusted. Optional. Default value is <code>false</code> .
modifiedDateTime	DateTimeOffset	The Timestamp type represents last modified date and time of the location using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is <code>2014-01-01T00:00:00Z</code> . Read-only. Inherited from namedLocation .

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON
<pre>{ "createdDateTime": "String (timestamp)", "displayName": "String", "id": "String (identifier)", "ipRanges": [{"@odata.type": "microsoft.graph.ipRange"}], "isTrusted": true, "modifiedDateTime": "String (timestamp)" }</pre>

Related content

- [What is Conditional Access?](#)
- [Using the location condition in a Conditional Access policy](#)

conditionalAccessTemplate resource type

Article • 12/03/2024

Namespace: microsoft.graph

Represents a Microsoft recommended template of best practice configurations for Microsoft Entra [conditional access policies](#). For more information, see [Conditional Access policy templates](#).

Inherits from [entity](#).

Methods

 [Expand table](#)

Method	Return type	Description
List	conditionalAccessTemplate collection	Get a list of the conditionalAccessTemplate objects and their properties.
Get	conditionalAccessTemplate	Read the properties and relationships of a conditionalAccessTemplate object.

Properties

 [Expand table](#)

Property	Type	Description
description	String	The user-friendly name of the template.
details	conditionalAccessPolicyDetail	Complete list of policy details specific to the template. This property contains the JSON of policy settings for configuring a Conditional Access policy.
id	String	Immutable ID of a template. Inherited from entity .
name	String	The user-friendly name of the template.
scenarios	templateScenarios	List of conditional access scenarios that the template is recommended for. The possible values are: new, secureFoundation, zeroTrust, remoteWork, protectAdmins, emergingThreats, unknownFutureValue. This is a multi-valued enum. Supports \$filter (has).

Relationships

None.

JSON representation

The following JSON representation shows the resource type.

JSON

```
{  
  "@odata.type": "#microsoft.graph.conditionalAccessTemplate",  
  "description": "String",  
  "details": {  
    "@odata.type": "microsoft.graph.conditionalAccessPolicyDetail",  
    "id": "String (identifier)",  
    "name": "String",  
    "scenarios": "String"  
  }  
}
```

Custom controls (preview)

Article • 12/05/2024

Custom controls are a preview capability of the Microsoft Entra ID. When using custom controls, your users are redirected to a compatible service to satisfy authentication requirements outside of Microsoft Entra ID. To satisfy this control, a user's browser is redirected to the external service, performs any required authentication, and is then redirected back to Microsoft Entra ID. Microsoft Entra ID verifies the response and, if the user was successfully authenticated or validated, the user continues in the Conditional Access flow.

ⓘ Note

As Nitika Gupta mentioned in her blog post [Public preview: External authentication methods in Microsoft Entra ID ↗](#):

...External authentication methods are the replacement of custom controls, and they provide several benefits over the custom controls approach. These include:

1. External authentication method integration, which uses industry standards and supports an open model
2. External authentication methods are managed the same way as Entra methods
3. External authentication methods are supported for a wide range of Entra ID use cases (including PIM activation)

For more information, see the article [Manage an external authentication method in Microsoft Entra ID \(Preview\)](#).

Creating custom controls

⊗ Caution

Custom controls can't be used with:

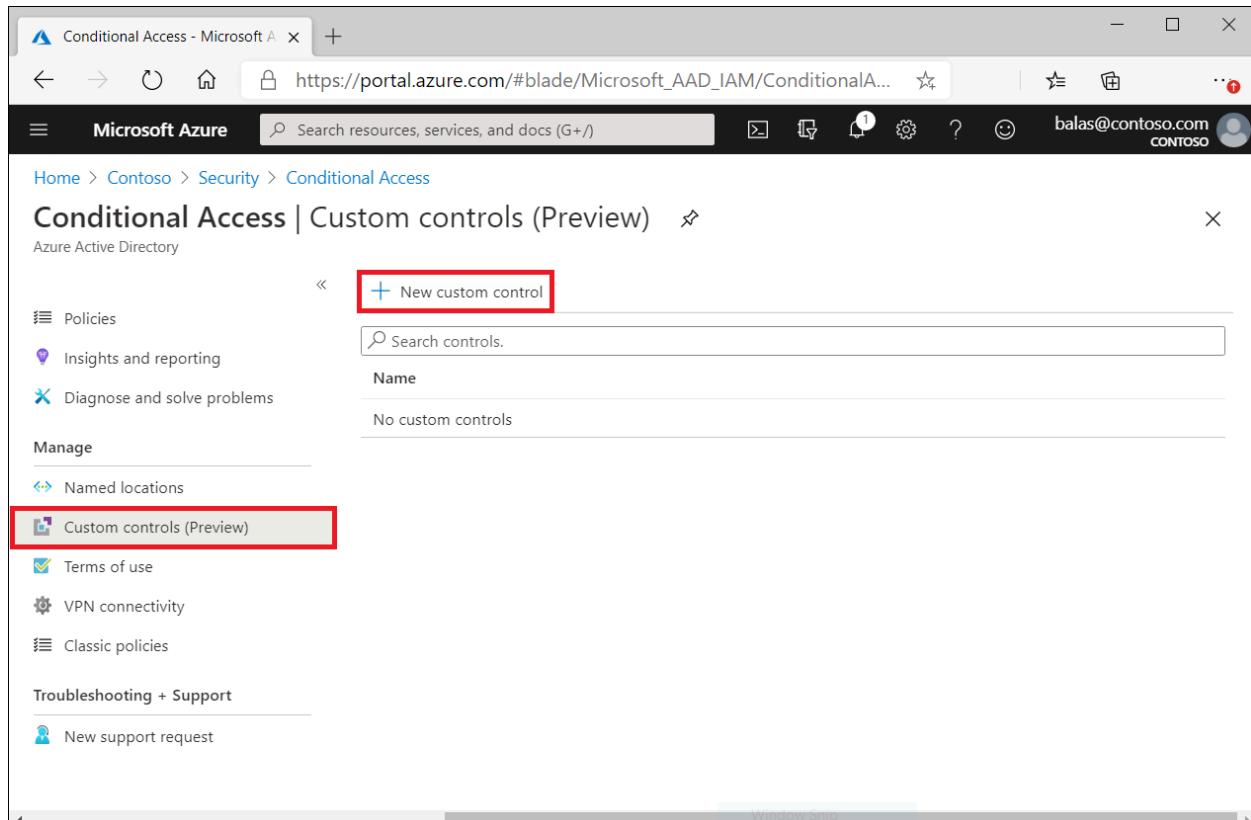
- Microsoft Entra ID Protection's automation requiring multifactor authentication
- Microsoft Entra self-service password reset (SSPR)
- Satisfying multifactor authentication claim requirements

- Sign-in frequency controls
- Privileged Identity Manager (PIM)
- Intune device enrollment
- Cross-tenant trusts
- Joining devices to Microsoft Entra ID.

Custom Controls works with a limited set of approved authentication providers. To create a custom control, you should first contact the provider that you wish to utilize. Each non-Microsoft provider has its own process and requirements to sign up, subscribe, or otherwise become a part of the service, and to indicate that you wish to integrate with Conditional Access. At that point, the provider gives you a block of data in JSON format. This data allows the provider and Conditional Access to work together for your tenant, creates the new control and defines how Conditional Access can tell if your users have successfully performed verification with the provider.

Copy the JSON data and then paste it into the related textbox. Don't make any changes to the JSON unless you explicitly understand the change you're making. Making any change could break the connection between the provider and Microsoft and potentially lock you and your users out of your accounts.

The option to create a custom control is in the **Manage** section of the **Conditional Access** page.



Clicking **New custom control** opens a blade with a textbox for the JSON data of your control.

The screenshot shows a Microsoft Azure browser-based interface. The title bar says "New custom control - Microsoft". The address bar shows the URL "https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/controlsCustomize". The top navigation bar includes "Microsoft Azure", a search bar, and user information for "balas@contoso.com CONTOSO". Below the navigation is a breadcrumb trail: "Home > Contoso > Security > Conditional Access > New custom control". A large text area titled "Enter the JSON for customized controls given by your claim providers." contains a JSON code block. At the bottom of the blade is a blue "Create" button.

```
[{"Name": "", "AppId": "00000000-0000-0000-0000-000000000000", "ClientId": "00000000-0000-0000-0000-000000000000", "DiscoveryUrl": "", "Controls": [{"Id": "", "Name": "", "claimsRequested": [{"Type": "", "Value": "", "Values": null}]}]}
```

Deleting custom controls

To delete a custom control, you must first ensure that it isn't being used in any Conditional Access policy. Once complete:

1. Go to the Custom controls list
2. Select ...
3. Select **Delete**.

Editing custom controls

To edit a custom control, you must delete the current control and create a new control with the updated information.

Known limitations

Custom controls can't be used with Microsoft Entra ID Protection's automation requiring Microsoft Entra multifactor authentication, Microsoft Entra self-service password reset (SSPR), satisfying multifactor authentication claim requirements, with sign-in frequency controls, to elevate roles in Privileged Identity Manager (PIM), as part of Intune device enrollment, for cross-tenant trusts, or when joining devices to Microsoft Entra ID.

Related content

- [Upcoming changes to Custom Controls ↗](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

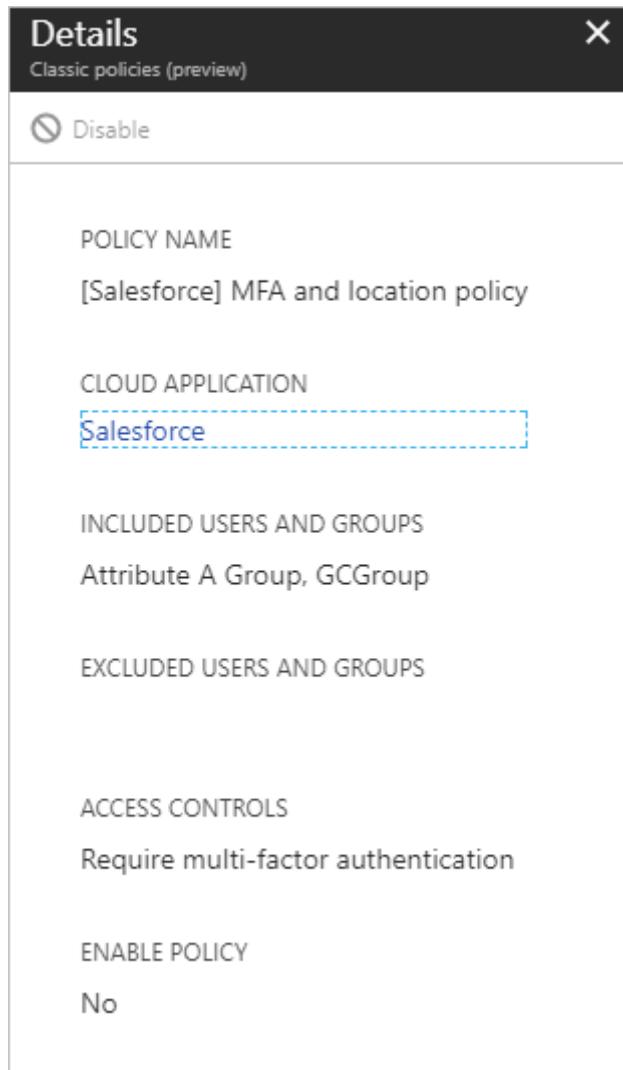
Migrate from a classic policy

Article • 04/25/2025

This article shows an example of how to migrate a classic policy that requires **Multifactor authentication** for a cloud app.

💡 Tip

As of the August 2023 Intune service release (2308), classic Conditional Access policies are no longer created for the [Microsoft Defender for Endpoint connector](#). If your tenant has a classic Conditional Access policy that was previously created for integration with Microsoft Defender for Endpoint, it can be deleted.

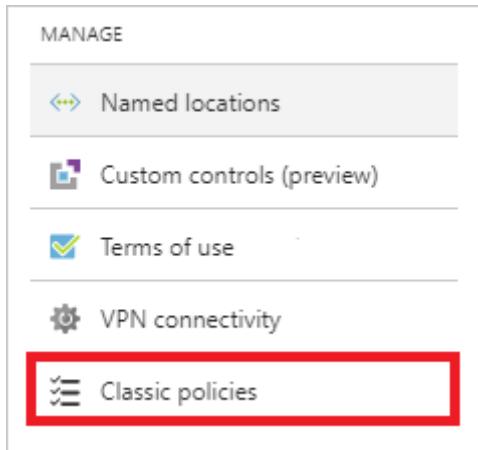


⚠️ Warning

Once disabled a classic policy can't be re-enabled.

Open a classic policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Conditional Access Administrator**.
2. Browse to **Entra ID > Conditional Access > Classic policies**.



3. In the list of classic policies, select the policy you wish to migrate. Document the configuration settings so that you can re-create with a new Conditional Access policy.

For examples of common policies and their configuration, see the article [Common Conditional Access policies](#).

Disable the classic policy

To disable your classic policy, select **Disable** in the **Details** view.

 **Warning**

Once disabled a classic policy can't be re-enabled.

Details X

Classic policies (preview)

POLICY NAME
[Office 365 Exchange Online] MFA and location policy

INCLUDE/EXCLUDE GROUPS
By excluding groups, you can perform phased migration of policies.

Groups ⓘ >

1 group included

CLOUD APPLICATION
[Office 365 Exchange Online](#)

ACCESS CONTROLS
Require multi-factor authentication when not at work

ENABLE POLICY
Yes

Next steps

[Conditional Access template policies](#)

Microsoft Entra releases and announcements

Article • 04/30/2025

This article provides information about the latest releases and change announcements across the Microsoft Entra family of products over the last six months (updated monthly). If you're looking for information that's older than six months, see: [Archive for What's new in Microsoft Entra](#).

Get notified about when to revisit this page for updates by copying and pasting this URL:

`https://learn.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us` into your  feed reader.

April 2025

Public Preview - Conditional Access Optimization Agent in Microsoft Entra

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

[Conditional Access Optimization Agent in Microsoft Entra](#) monitors for new users or apps not covered by existing policies, identifies necessary updates to close security gaps, and recommends quick fixes for identity teams to apply with a single selection. For more information, see: [Microsoft Entra Conditional Access optimization agent](#).

Public Preview - Microsoft Entra ID Governance: Suggested access packages in My Access

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

In December 2024, we introduced a new feature in My Access: a curated list of suggested access packages. Users view the most relevant access packages, based on their peers' access packages and previous assignments, without scrolling through a long list. By May 2025, suggestions will be enabled by default and we'll introduce a new card in the Microsoft Entra

Admin Center Entitlement Management control configurations for admins to see My Access settings. We recommend admins turn on the peer-based insights for suggested access packages via this setting. For more information, see: [Suggested access packages in My Access \(Preview\)](#).

Public Preview - Conditional Access What If evaluation API

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Conditional Access What If evaluation API – Leverage the What If tool using the Microsoft Graph API to programmatically evaluate the applicability of conditional access policies in your tenant on user and service principal sign-ins. For more information, see: [conditionalAccessRoot: evaluate](#).

Public Preview - Manage refresh tokens for mover and leaver scenarios with Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now customers can configure a Lifecycle workflows task to automatically revoke access tokens when employees move within, or leave, the organization. For more information, see: [Revoke all refresh tokens for user \(Preview\)](#).

General Availability - Use managed identities as credentials in Microsoft Entra apps

Type: New feature

Service category: Managed identities for Azure resources

Product capability: Identity Security & Protection

You can now use managed identities as federated credentials for Microsoft Entra apps, enabling secure, secret-less authentication in both single- and multi-tenant scenarios. This eliminates the need to store and manage client secrets or certificates when using Microsoft Entra app to access Azure resources across tenants. This capability aligns with Microsoft's

Secure Future Initiative [🔗](#) pillar of protecting identities and secrets across systems. Learn how to configure this capability in the [official documentation](#).

Plan for change - Roll out of Application Based Authentication on Microsoft Entra Connect Sync

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

What is changing

Microsoft Entra Connect creates and uses a [Microsoft Entra Connector account](#) to authenticate and sync identities from Active Directory to Microsoft Entra ID. The account uses a locally stored password to authenticate with Microsoft Entra ID. To enhance the security of the Microsoft Entra Connect application sync process, we will, in the coming week roll out support for "Application based Authentication" (ABA), which uses a Microsoft Entra ID application based identity and Oauth 2.0 client credential flow to authenticate with Microsoft Entra ID. To enable this, Microsoft Entra Connect will create a single tenant 3rd party application in customer's Microsoft Entra ID tenant, register a certificate as the credential for the application, and authorize the application to perform on-premises directory synchronization

The Microsoft Entra Connect Sync .msi installation file for this change will be exclusively available in the Microsoft Entra admin center within the [Microsoft Entra Connect pane](#) [🔗](#).

Check our [version history page](#) in the next week for more details of the change.

March 2025

Microsoft Entra Permissions Management end of sale and retirement

Type: Plan for change

Service category: Other

Product capability: Permissions Management

Effective April 1, 2025, Microsoft Entra Permissions Management (MEPM) will no longer be available for sale to new Enterprise Agreement or direct customers. Additionally, starting May

1, it will not be available for sale to new CSP customers. Effective October 1, 2025, we will retire Microsoft Entra Permissions Management and discontinue support of this product.

Existing customers will retain access to this product until September 30, 2025, with ongoing support for current functionalities. We have partnered with Delinea to provide an alternative solution, [Privilege Control for Cloud Entitlements \(PCCE\)](#), that offers similar capabilities to those provided by Microsoft Entra Permissions Management. The decision to phase out Microsoft Entra Permissions Management was done after deep consideration of our innovation portfolio and how we can focus on delivering the best innovations aligned to our differentiating areas and partner with the ecosystem on adjacencies. We remain committed to delivering top-tier solutions across the Microsoft Entra portfolio. For more information, see: [Important change announcement: Microsoft Entra Permissions Management end of sale and retirement](#).

Public Preview - Track and investigate identity activities with linkable identifiers in Microsoft Entra

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft will standardize the linkable token identifiers, and expose them in both Microsoft Entra and workflow audit logs. This allows customers to join the logs to track, and investigate, any malicious activity. Currently linkable identifiers are available in Microsoft Entra sign in logs, Exchange Online audit logs, and MSGraph Activity logs.

For more information, see: [Track and investigate identity activities with linkable identifiers in Microsoft Entra \(preview\)](#).

General Availability- Conditional Access reauthentication policy

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Require reauthentication every time can be used for scenarios where you want to require a fresh authentication, every time a user performs specific actions like accessing sensitive

applications, securing resources behind VPN, or Securing privileged role elevation in PIM. For more information, see: [Require reauthentication every time](#).

General Availability- Custom Attributes support for Microsoft Entra Domain Services

Type: New feature

Service category: Microsoft Entra Domain Services

Product capability: Microsoft Entra Domain Services

Custom Attributes for Microsoft Entra Domain Services is now Generally Available. This capability allows customers to use Custom Attributes in their managed domains. Legacy applications often rely on custom attributes created in the past to store information, categorize objects, or enforce fine-grained access control over resources. For example, these applications might use custom attributes to store an employee ID in their directory and rely on these attributes in their application LDAP calls. Modifying legacy applications can be costly and risky, and customers might lack the necessary skills or knowledge to make these changes. Microsoft Entra Domain Services now supports custom attributes, enabling customers to migrate their legacy applications to the Azure cloud without modification. It also provides support to synchronize custom attributes from Microsoft Entra ID, allowing customers to benefit from Microsoft Entra ID services in the cloud. For more information, see: [Custom attributes for Microsoft Entra Domain Services](#).

Public Preview - Conditional Access Per-Policy Reporting

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Conditional Access Per-Policy Reporting enables admins to easily evaluate the impact of enabled and report-only Conditional Access policies on their organization, without using Log Analytics. This feature surfaces a graph for each policy in the Microsoft Entra Admin Center, visualizing the policy's impact on the tenant's past sign-ins. For more information, see: [Policy impact \(Preview\)](#).

Public Preview - Limit creation or promotion of multitenant apps

Type: New feature

Service category: Directory Management

Product capability: Developer Experience

A new feature has been added to the [App Management Policy Framework](#) that allows restriction on creation or promotion of multitenant applications, providing administrators with greater control over their app environments.

Administrators can now configure tenant default or custom app policy using the new '[audiences](#)' restriction to block new app creation if the signInAudience value provided in the app isn't permitted by the policy. In addition, existing apps can be restricted from changing their signInAudience if the target value isn't permitted by the policy. These policy changes are applied during app creation or update operations, offering control over application deployment and usage. For more information, see: [audiencesConfiguration resource type](#).

General Availability - Download Microsoft Entra Connect Sync on the Microsoft Entra admin center

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Identity Governance

The Microsoft Entra Connect Sync .msi installation files are also available on Microsoft Entra admin center within the [Microsoft Entra Connect pane](#). As part of this change, we'll stop uploading new installation files on the [Microsoft Download Center](#).

General Availability - New Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows

Type: Changed feature

Service category: Conditional Access

Product capability: Access Control

As part of our ongoing commitment to enhance security and protect our customers from evolving cyber threats, we're rolling out two new Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows. These policies are aligned to the secure by default principle of our broader [Secure Future Initiative](#), which aims to provide robust security measures to safeguard your organization by default.

Deprecated - Upgrade your Microsoft Entra Connect Sync version to avoid impact on the Sync Wizard

Type: Deprecated

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

As announced in the Microsoft Entra What's New [Blog](#) and in Microsoft 365 Center communications, customers should upgrade their connect sync versions to at least [2.4.18.0](#) for commercial clouds and [2.4.21.0](#) for non-commercial clouds before April 7, 2025. A breaking change on the Connect Sync Wizard will affect all requests that require authentication such as schema refresh, configuration of staging mode, and user sign in changes. For more information, see: [Minimum versions](#).

February 2025

General Availability - Authentication methods migration wizard

Type: New feature

Service category: MFA

Product capability: User Authentication

The authentication methods migration guide in the Microsoft Entra Admin Center lets you automatically migrate method management from the [legacy MFA and SSPR policies](#) to the [converged authentication methods policy](#). In 2023, it was announced that the ability to manage authentication methods in the legacy MFA and SSPR policies would be retired in September 2025. Until now, organizations had to manually migrate methods themselves by using [the migration toggle](#) in the converged policy. Now, you can migrate in just a few selections by using the migration guide. The guide evaluates what your organization currently has enabled in both legacy policies, and generates a recommended converged policy configuration for you to review and edit as needed. From there, confirm the configuration, and we set it up for you and mark your migration as complete. For more information, see: [How to migrate MFA and SSPR policy settings to the Authentication methods policy for Microsoft Entra ID](#).

Public Preview - Enhanced user management in Admin Center UX

Type: New feature

Service category: User Management

Product capability: User Management

Admins are now able to multi-select and edit users at once through the Microsoft Entra Admin Center. With this new capability, admins can bulk edit user properties, add users to groups, edit account status, and more. This UX enhancement will significantly improve efficiency for user management tasks in the Microsoft Entra admin center. For more information, see: [Add or update a user's profile information and settings in the Microsoft Entra admin center.](#)

Public Preview – QR code authentication, a simple and fast authentication method for Frontline Workers

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're thrilled to announce public preview of QR code authentication in Microsoft Entra ID, providing an efficient and simple authentication method for frontline workers.

You see a new authentication method 'QR code' in Microsoft Entra ID Authentication method Policies. You can enable and add QR code for your frontline workers via Microsoft Entra ID, My Staff, or MS Graph APIs. All users in your tenant see a new link 'Sign in with QR code' on navigating to <https://login.microsoftonline.com> > 'Sign-in options' > 'Sign in to an organization' page. This new link is visible only on mobile devices (Android/iOS/iPadOS). Users can use this auth method only if you add and provide a QR code to them. QR code auth is also available in BlueFletch and Jamf. MHS QR code auth support is generally available by early March.

The feature has a 'preview' tag until it's generally available. For more information, see: [Authentication methods in Microsoft Entra ID - QR code authentication method \(Preview\).](#)

Public Preview - Custom SAML/WS-Fed External Identity Provider Support in Microsoft Entra External ID

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

By setting up federation with a custom-configured identity provider that supports the SAML 2.0 or WS-Fed protocol, you enable your users to sign up and sign in to your applications using their existing accounts from the federated external provider.

This feature also includes domain-based federation, so a user who enters an email address on the sign-in page that matches a predefined domain in any of the external identity providers will be redirected to authenticate with that identity provider.

For more information, see: [Custom SAML/WS-Fed identity providers \(preview\)](#).

Public Preview - External Auth Methods support for system preferred MFA

Type: New feature

Service category: MFA

Product capability: 3rd Party Integration

Support for external auth methods as a supported method begins rolling out at the beginning of March 2025. When this is live in a tenant where system preferred is enabled and users are in scope of an external auth methods policy, those users will be prompted for their external authentication method if their most secure registered method is Microsoft Authenticator notification. External Authentication Method will appear as third in the list of most secure methods. If the user has a Temporary Access Pass (TAP) or Passkey (FIDO2) device registered, they'll be prompted for those. In addition, users in the scope of an external auth methods policy will have the ability to delete all registered second factor methods from their account, even if the method being deleted is specified as the default sign in method or is system preferred. For more information, see: [System-preferred multifactor authentication - Authentication methods policy](#).

General Availability - Granular Microsoft Graph permissions for Lifecycle workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now new, lesser privileged permissions can be used for managing specific read and write actions in Lifecycle workflows scenarios. The following granular permissions were introduced in Microsoft Graph:

- LifecycleWorkflows-Workflow.ReadBasic.All
- LifecycleWorkflows-Workflow.Read.All
- LifecycleWorkflows-Workflow.ReadWrite.All
- LifecycleWorkflows-Workflow.Activate
- LifecycleWorkflows-Reports.Read.All
- LifecycleWorkflows-CustomExt.Read.All
- LifecycleWorkflows-CustomExt.ReadWrite.All

For more information, see: [Microsoft Graph permissions reference](#).

January 2025

Public Preview - Manage Lifecycle Workflows with Microsoft Security CoPilot in Microsoft Entra

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Customers can now manage, and customize, Lifecycle Workflows using natural language with Microsoft Security CoPilot. Our Lifecycle Workflows (LCW) Copilot solution provides step-by-step guidance to perform key workflow configuration and execution tasks using natural language. It allows customers to quickly get rich insights to help monitor, and troubleshoot, workflows for compliance. For more information, see: [Manage employee lifecycle using Microsoft Security Copilot \(Preview\)](#).

General Availability - Microsoft Entra PowerShell

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Manage and automate Microsoft Entra resources programmatically with the scenario-focused Microsoft Entra PowerShell module. For more information, see: [Microsoft Entra PowerShell module now generally available ↗](#).

General Availability - Improving visibility into downstream tenant sign-ins

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Security wants to ensure that all customers are aware of how to notice when a partner is accessing a downstream tenant's resources. Interactive sign-in logs currently provide a list of sign in events, but there's no clear indication of which logins are from partners accessing downstream tenant resources. For example, when reviewing the logs, you might see a series of events, but without any additional context, it's difficult to tell whether these logins are from a partner accessing another tenant's data.

Here's a list of steps that one can take to clarify which logins are associated with partner tenants:

1. Take note of the "ServiceProvider" value in the CrossTenantAccessType column:

- This filter can be applied to refine the log data. When activated, it immediately isolates events related to partner logins.

2. Utilize the "Home Tenant ID" and "Resource Tenant ID" Columns:

- These two columns identify logins coming from the partner's tenant to a downstream tenant.

After seeing a partner logging into a downstream tenant's resources, an important follow-up activity to perform is to validate the activities that might have occurred in the downstream environment. Some examples of logs to look at are Microsoft Entra Audit logs for Microsoft Entra ID events, Microsoft 365 Unified Audit Log (UAL) for Microsoft 365 and Microsoft Entra ID events, and/or the Azure Monitor activity log for Azure events. By following these steps, you're able to clearly identify when a partner is logging into a downstream tenant's resources and subsequent activity in the environment, enhancing your ability to manage and monitor cross-tenant access efficiently.

To increase visibility into the aforementioned columns, Microsoft Entra will begin enabling these columns to display by default when loading the sign-in logs UX starting on March 7, 2025.

Public Preview - Auditing administrator events in Microsoft Entra Connect

Type: New feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

We have released a new version of Microsoft Entra Connect, version 2.4.129.0, that supports the logging of the changes an administrator makes on the Connect Sync Wizard and PowerShell. For more information, see: [Auditing administrator events in Microsoft Entra Connect Sync \(Public Preview\)](#).

Where supported, we'll also autoupgrade customers to this version of Microsoft Entra Connect in February 2025. For customers who wish to be autoupdated, [ensure that you have auto-upgrade configured](#).

For upgrade-related guidance, see [Microsoft Entra Connect: Upgrade from a previous version to the latest](#).

Public Preview - Flexible Federated Identity Credentials

Type: New feature

Service category: Authentications (Logins)

Product capability: Developer Experience

Flexible Federated Identity Credentials extend the existing Federated Identity Credential model by providing the ability to use wildcard matching against certain claims. Currently available for GitHub, GitLab, and Terraform Cloud scenarios, this functionality can be used to lower the total number of FICs required to manage similar scenarios. For more information, see: [Flexible federated identity credentials \(preview\)](#).

General Availability - Real-time Password Spray Detection in Microsoft Entra ID Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Traditionally, password spray attacks are detected post breach or as part of hunting activity. Now, we've enhanced Microsoft Entra ID Protection to detect password spray attacks in real-

time before the attacker ever obtains a token. This reduces remediation from hours to seconds by interrupting attacks during the sign-in flow.

Risk-based Conditional Access can automatically respond to this new signal by raising session risk, immediately challenging the sign-in attempt, and stopping password spray attempts in their tracks. This cutting-edge detection, now Generally Available, works alongside existing detections for advanced attacks such as Adversary-in-the-Middle (AitM) phishing and token theft, to ensure comprehensive coverage against modern attacks. For more information, see: [What is Microsoft Entra ID Protection?](#)

General Availability - Protected actions for hard deletions

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Customers can now configure Conditional Access policies to protect against early hard deletions. Protected action for hard deletion protects hard deletion of users, Microsoft 365 groups, and applications. For more information, see: [What are protected actions in Microsoft Entra ID?](#).

Public Preview - Elevate Access events are now exportable via Microsoft Entra Audit Logs

Type: New feature

Service category: RBAC

Product capability: Monitoring & Reporting

This feature enables administrators to export and stream Elevate Access events to both first-party and third-party SIEM solutions via Microsoft Entra Audit logs. It enhances detection and improves logging capabilities, allowing visibility into who in their tenant has utilized Elevate Access. For more information on how to use the feature, see: [View elevate access log entries](#).

Deprecated - Action Required by February 1, 2025: Azure AD Graph retirement

Type: Deprecated

Service category: Azure AD Graph

Product capability: Developer Experience

The Azure AD Graph API service was [deprecated] in 2020. [Retirement of the Azure AD Graph API service](#) began in September 2024, and the next phase of this retirement starts February 1, 2025. This phase will impact new and existing applications unless action is taken. The latest updates on Azure AD Graph retirement can be found here: [Take action by February 1: Azure AD Graph is retiring](#).

Starting from February 1, both new and existing applications will be prevented from calling Azure AD Graph APIs, unless they're configured for an extension. You might not see impact right away, as we're rolling out this change in stages across tenants. We anticipate full deployment of this change around the end of February, and by the end of March for national cloud deployments.

If you haven't already, it's now urgent to review the applications on your tenant to see which ones depend on Azure AD Graph API access, and mitigate or migrate these before the February 1 cutoff date. For applications that haven't migrated to Microsoft Graph APIs, [an extension](#) can be set to allow the application access to Azure AD Graph through June 30, 2025.

Microsoft Entra Recommendations are the best tool to identify applications that are using Azure AD Graph APIs in your tenant and require action. Reference this blog post: Action required: [Azure AD Graph API retirement](#) for step by step guidance.

General Availability - Microsoft Entra Connect Version 2.4.129.0

Type: Changed feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

On January 15, 2025, we released Microsoft Entra Connect Sync Version 2.4.129.0 which supports auditing administrator events. More details are available in the [release notes](#). We'll automatically upgrade eligible customers to this latest version of Microsoft Entra Connect in February 2025. For customers who wish to be auto-upgraded, [ensure that you have auto-upgrade configured](#).

Deprecated - Take action to avoid impact when legacy MSOnline and AzureAD PowerShell modules retire

Type: Deprecated

Service category: Legacy MSOnline and AzureAD PowerShell modules

Product capability: Developer Experience

As announced in Microsoft Entra [change announcements](#) and in the Microsoft Entra [Blog](#), the MSOnline, and Microsoft Azure AD PowerShell modules (for Microsoft Entra ID) retired on March 30, 2024.

The retirement for MSOnline PowerShell module starts in early April 2025, and ends in late May 2025. If you're using MSOnline PowerShell, you must take action by March 30, 2025 to avoid impact after the retirement by migrating any use of MSOnline to [Microsoft Graph PowerShell SDK](#) or [Microsoft Entra PowerShell](#).

Key points

- MSOnline PowerShell will retire, and stop working, between early April 2025 and late May 2025
- AzureAD PowerShell will no longer be supported after March 30, 2025, but its retirement will happen in early July 2025. This postponement is to allow you time to finish the MSOnline PowerShell migration
- To ensure customer readiness for MSOnline PowerShell retirement, a series of temporary outage tests will occur for all tenants between January 2025 and March 2025.

For more information, see: [Action required: MSOnline and AzureAD PowerShell retirement - 2025 info and resources](#).

December 2024

General Availability - What's new in Microsoft Entra

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

What's new in Microsoft Entra offers a comprehensive view of Microsoft Entra product updates including product roadmap (like Public Previews and recent GAs), and change announcements (like deprecations, breaking changes, feature changes and Microsoft-managed policies). It's a one stop shop for Microsoft Entra admins to discover the product updates.

Public Preview - Microsoft Entra ID Governance: Approvers can revoke access in MyAccess

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

For Microsoft Entra ID Governance users, approvers of access package requests can now revoke their decision in MyAccess. Only the person who took the approve action is able to revoke access. To opt into this feature, admins can go to the [Identity Governance settings page](#), and enable the feature. For more information, see: [What is the My Access portal?](#).

General Availability - Expansion of SSPR Policy Audit Logging

Type: New feature

Service category: Self Service Password Reset

Product capability: Monitoring & Reporting

Starting Mid-January, we are improving the audit logs for changes made to the SSPR Policy.

With this improvement, any change to the SSPR policy configuration, including enablement or disablement, will result in an audit log entry that includes details about the change made. Additionally, both the previous values and current values from the change will be recorded within the audit log. This additional information can be found by selecting an audit log entry and selecting the Modified Properties tab within the entry.

These changes are rolled out in phases:

- Phase 1 includes logging for the Authentication Methods, Registration, Notifications, and Customization configuration settings.
- Phase 2 includes logging for the On-premises integration configuration settings.

This change occurs automatically, so admins take no action. For more information and details regarding this change, see: [Microsoft Entra audit log categories and activities](#).

General Availability - Update Profile Photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

Users can now update their profile photo directly from their MyAccount portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Temporary Access Pass (TAP) support for internal guest users

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra ID now supports issuing Temporary Access Passes (TAP) to internal guest users. TAPs can be issued to internal guests just like normal members, through the Microsoft Entra ID Admin Center, or natively through Microsoft Graph. With this enhancement, internal guests can now seamlessly onboard, and recover, their accounts with time-bound temporary credentials.

For more information, see: [Configure Temporary Access Pass to register passwordless authentication methods](#).

Public Preview - Microsoft Entra ID Governance: access package request suggestions

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

Opt-In As communicated [earlier](#), we're excited to introduce a new feature in [My Access](#): a curated list of suggested access packages. This capability allows users to quickly view the most relevant access packages (based off their peers' access packages and previous requests) without scrolling through a long list. In December you can [enable the preview in the Opt-in Preview Features for Identity Governance](#). From January, this setting is enabled by default.

Public Preview - Security Copilot embedded in Microsoft Entra

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

We've announced the public preview of Microsoft Security Copilot embedded in the Microsoft Entra admin Center. This integration brings all identity skills previously made generally available for the Security Copilot standalone experience in April 2024, along with new identity capabilities for admins and security analysts to use directly within the Microsoft Entra admin center. We've also added brand new skills to help improve identity-related risk investigation. In December, we broaden the scope even further to include a set of skills specifically for App Risk Management in both standalone and embedded experiences of Security Copilot and Microsoft Entra. These capabilities allow identity admins and security analysts to better identify, understand, and remediate the risks impacting applications and workload identities registered in Microsoft Entra.

With Security Copilot now embedded in Microsoft Entra, identity admins get AI-driven, natural-language summaries of identity context and insights tailored for handling security incidents, equipping them to better protect against identity compromise. The embedded experience also accelerates troubleshooting tasks like resolving identity-related risks and sign-in issues, without ever leaving the admin center.

Public Preview - Security Copilot in Microsoft Entra: App Risk skills

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Identity admins and security analysts managing Microsoft Entra ID registered apps can identify and understand risks through natural language prompts. Security Copilot has links to the Microsoft Entra Admin Center for admins to take needed remediation actions. For more information, see: [Assess application risks using Microsoft Security Copilot in Microsoft Entra](#).

Public Preview - Provision custom security attributes from HR sources

Type: New feature

Service category: Provisioning

Product capability: Inbound to Entra ID

With this feature, customers can automatically provision "*custom security attributes*" in Microsoft Entra ID from authoritative HR sources. Supported authoritative sources include: Workday, SAP SuccessFactors, and any HR system integrated using API-driven provisioning.

Public Preview - Sign in with Apple

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: Extensibility

This new feature adds Apple to our list of preconfigured social identity providers. As the first social identity provider implemented on the eSTS platform, it introduces a "*Sign in with Apple*" button to the sign-in options, allowing users to access applications with their Apple accounts. For more information, see: [Add Apple as an identity provider \(preview\)](#).

General Availability - Microsoft Entra External ID Custom URL Domains

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Lifecycle Management

This feature allows users to customize their Microsoft default sign in authentication endpoint with their own brand names. Custom URL Domains help users to change Ext ID endpoint < tenant-name >.ciamlogin.com to login.contoso.com.

General Availability - Privileged Identity Management integration in Azure Role Based Access Control

Type: New feature

Service category: RBAC

Product capability: Access Control

Privileged Identity Management (PIM) capabilities are now integrated into the Azure Role Based Access Control (Azure RBAC) UI. Before this integration, RBAC admins could only manage standing access (active permanent role assignments) from the Azure RBAC UI. With this integration, just-in-time access and timebound access, which are functionalities supported

by PIM, are now brought into the Azure RBAC UI for customers with either a P2, or Identity Governance, license.

RBAC admins can create assignments of type eligible and timebound duration from the Azure RBAC add role assignment flow, see the list of different states of role assignment in a single view, as well as convert the type and duration of their role assignments from the Azure RBAC UI. In addition, end users now see all their role assignments of different state straight from the Azure RBAC UI landing page, from where they can also activate their eligible role assignments. For more information, see: [List role assignments at a scope](#).

General Availability - Dedicated new 1st party resource application to enable Active Directory to Microsoft Entra ID sync using Microsoft Entra Connect Sync or Cloud Sync

Type: Changed feature

Service category: Provisioning

Product capability: Directory

As part of ongoing security hardening, Microsoft deployed Microsoft Entra AD Synchronization Service, a dedicated first-party application to enable the synchronization between Active Directory and Microsoft Entra ID. This new application, with Application ID `6bf85cfa-ac8a-4be5-b5de-425a0d0dc016`, was provisioned in customer tenants that use Microsoft Entra Connect Sync or the Microsoft Entra Cloud Sync service.

November 2024

Public Preview - Universal Continuous Access Evaluation

Type: New feature

Service category: Provisioning

Product capability: Network Access

Continuous Access Evaluation (CAE) revokes, and revalidates, network access in near real-time whenever Microsoft Entra ID detects changes to the identity. For more information, see: [Universal Continuous Access Evaluation \(Preview\)](#).

Public Preview - Microsoft Entra new store for certificate-based authentication

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft Entra ID has a new scalable PKI (Public Key Infrastructure) based CA (Certificate Authorities) store with higher limits for the number of CAs and the size of each CA file. PKI based CA store allows CAs within each different PKI to be in its own container object allowing administrators to move away from one flat list of CAs to more efficient PKI container based CAs. PKI-based CA store now supports up to 250CAs, 8KB size for each CA and also supports issuers hints attribute for each CA. Administrators can also upload the entire PKI and all the CAs using the "Upload CBA PKI" feature or create a PKI container and upload CAs individually. For more information, see: [Step 1: Configure the certificate authorities with PKI-based trust store \(Preview\)](#).

Public Preview - Updating profile photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

On November 13, 2024, users received the ability to update their profile photo directly from their [MyAccount](#) portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Microsoft Entra Health Monitoring, Health Metrics Feature

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Entra health monitoring, available from the Health pane, includes a set of low-latency pre-computed health metrics that can be used to monitor the health of critical user scenarios

in your tenant. The first set of health scenarios includes MFA, CA-compliant devices, CA-managed devices, and SAML authentications. This set of monitor scenarios will grow over time. These health metrics are now released as general availability data streams with the public preview of an intelligent alerting capability. For more information, see: [What is Microsoft Entra Health?](#)

General Availability - Microsoft Entra Connect Sync Version 2.4.27.0

Type: Changed feature

Service category: Provisioning

Product capability: Identity Governance

On November 14, 2025, we released Microsoft Entra Connect Sync Version 2.4.27.0 that uses the OLE DB version 18.7.4 that further hardens our service. Upgrade to this latest version of connect sync to improve your security. More details are available in the [release notes](#).

Changed feature - expansion of WhatsApp as an MFA one-time passcode delivery channel for Microsoft Entra ID

Type: Changed feature

Service category: MFA

Product capability: User Authentication

In late 2023, Microsoft Entra ID started using WhatsApp as an alternate channel to deliver multifactor authentication (MFA) one-time passcodes to users in India and Indonesia. We saw improved deliverability, completion rates, and satisfaction when using the channel in both countries. The channel was temporarily disabled in India in early 2024. Starting early December 2024, we'll be re-enabling the channel in India, and expanding its use to more countries.

Starting December 2024, users in India, and other countries can start receiving MFA text messages via WhatsApp. Only users that are enabled to receive MFA text messages as an authentication method, and already have WhatsApp on their phone, get this experience. If a user with WhatsApp on their device is unreachable or doesn't have internet connectivity, we'll quickly fall back to the regular SMS channel. In addition, users receiving OTPs via WhatsApp for the first time will be notified of the change in behavior via SMS text message.

If you don't want your users to receive MFA text messages through WhatsApp, you can disable text messages as an authentication method in your organization or scope it down to only be

enabled for a subset of users. Note that we highly encourage organizations move to using more modern, secure methods like Microsoft Authenticator and passkeys in favor of telecom and messaging app methods. For more information, see: [Text message verification](#).

Retirement - MFA Fraud Alert will be retired on March 1st 2025

Type: Deprecated

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra multifactor authentication (MFA) fraud alert allows end users to report MFA voice calls, and Microsoft Authenticator push requests, they didn't initiate as fraudulent.

Beginning March 1, 2025, MFA Fraud Alert will be retired in favor of the replacement feature

[Report Suspicious Activity](#) which allows end users to report fraudulent requests, and is also

integrated with [Identity Protection](#) for more comprehensive coverage and remediation.

To ensure users can continue reporting fraudulent MFA requests, organizations should migrate to using Report Suspicious Activity, and review how reported activity is remediated based on their Microsoft Entra licensing. For more information, see: [Configure Microsoft Entra multifactor authentication settings](#).

Public Preview - Microsoft Entra Health Monitoring, Alerts Feature

Type: Changed feature

Service category: Other

Product capability: Monitoring & Reporting

Intelligent alerts in Microsoft Entra health monitoring notify tenant admins, and security engineers, whenever a monitored scenario breaks from its typical pattern. Microsoft Entra's alerting capability watches the low-latency health signals of each scenario, and fires a notification if an anomaly is detected. The set of alert-ready health signals and scenarios will grow over time. This alerts feature is now available in Microsoft Entra Health as an API-only public preview release (UX release is scheduled for February 2025). For more information, see: [How to use Microsoft Entra Health monitoring alerts \(preview\)](#).

General Availability - Log analytics sign-in logs schema is in parity with MSGraph schema

Type: Plan for change

Service category: Authentications (Logins)

Product capability: Monitoring & Reporting

To maintain consistency in our core logging principles, we've addressed a legacy parity issue where the Azure Log Analytics sign-in logs schema didn't align with the MSGraph sign-in logs schema. The updates include fields such as ClientCredentialType, CreatedDateTime, ManagedServiceIdentity, NetworkLocationDetails, tokenProtectionStatus, SessionID, among others. These changes take effect in the first week of December 2024.

We believe this enhancement provides a more consistent logging experience. As always, you can perform pre-ingestion transformations to remove any unwanted data from your Azure Log Analytics storage workspaces. For guidance on how to perform these transformations, see:

[Data collection transformations in Azure Monitor](#).

Deprecated - MIM hybrid reporting agent

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Monitoring & Reporting

The hybrid reporting agent, used to send a MIM Service event log to Microsoft Entra to surface in password reset and self-service group management reports, is deprecated. The recommended replacement is to use Azure Arc to send the event logs to Azure Monitor. For more information, see: [Microsoft Identity Manager 2016 reporting with Azure Monitor](#).
