

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:

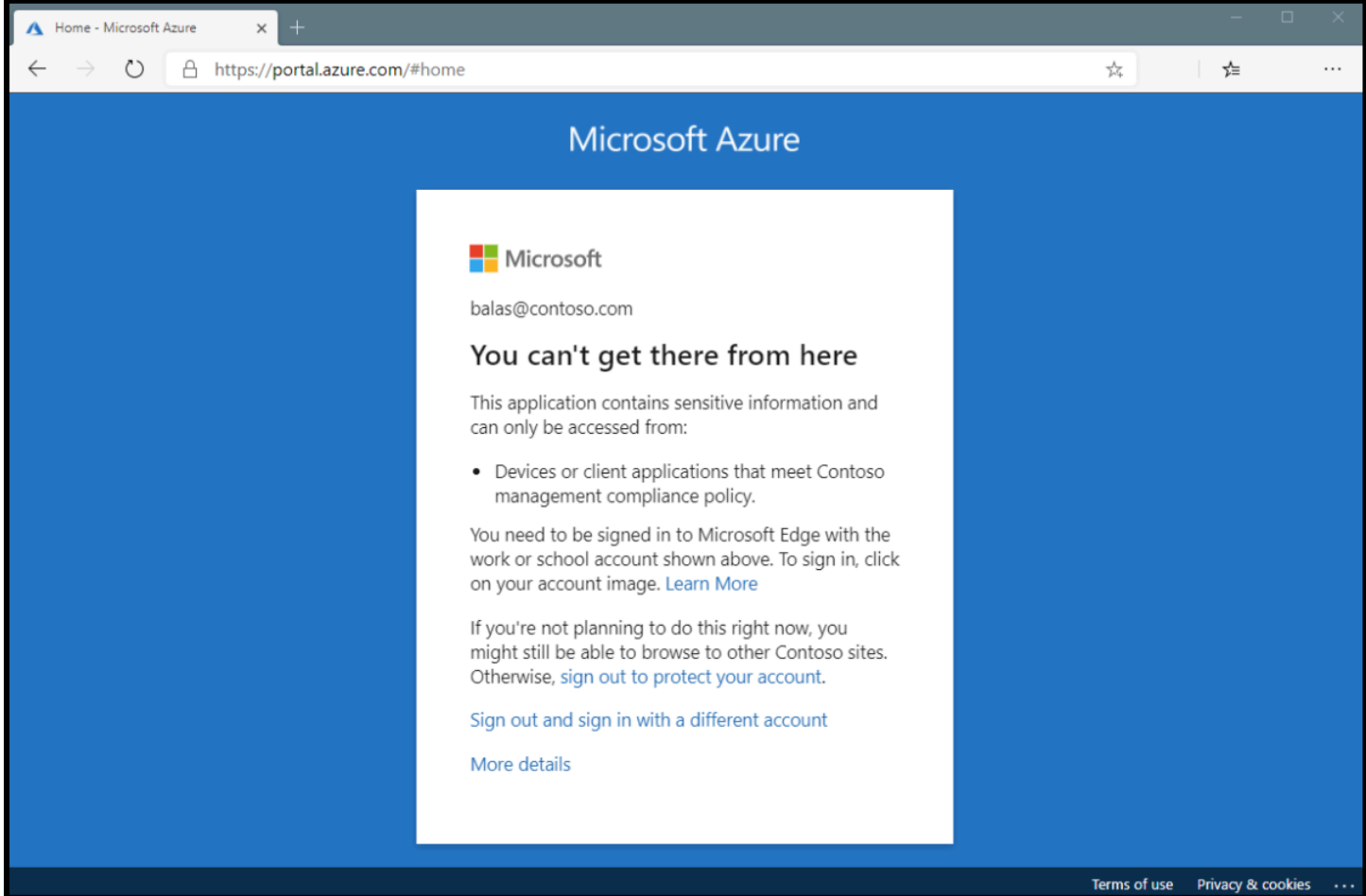
- **Block access** - This configuration blocks the entire organization.
- **Require device to be marked as compliant** - For users that haven't enrolled their devices yet, this policy blocks all access including access to the Intune portal. If you're an administrator without an enrolled device, this 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.

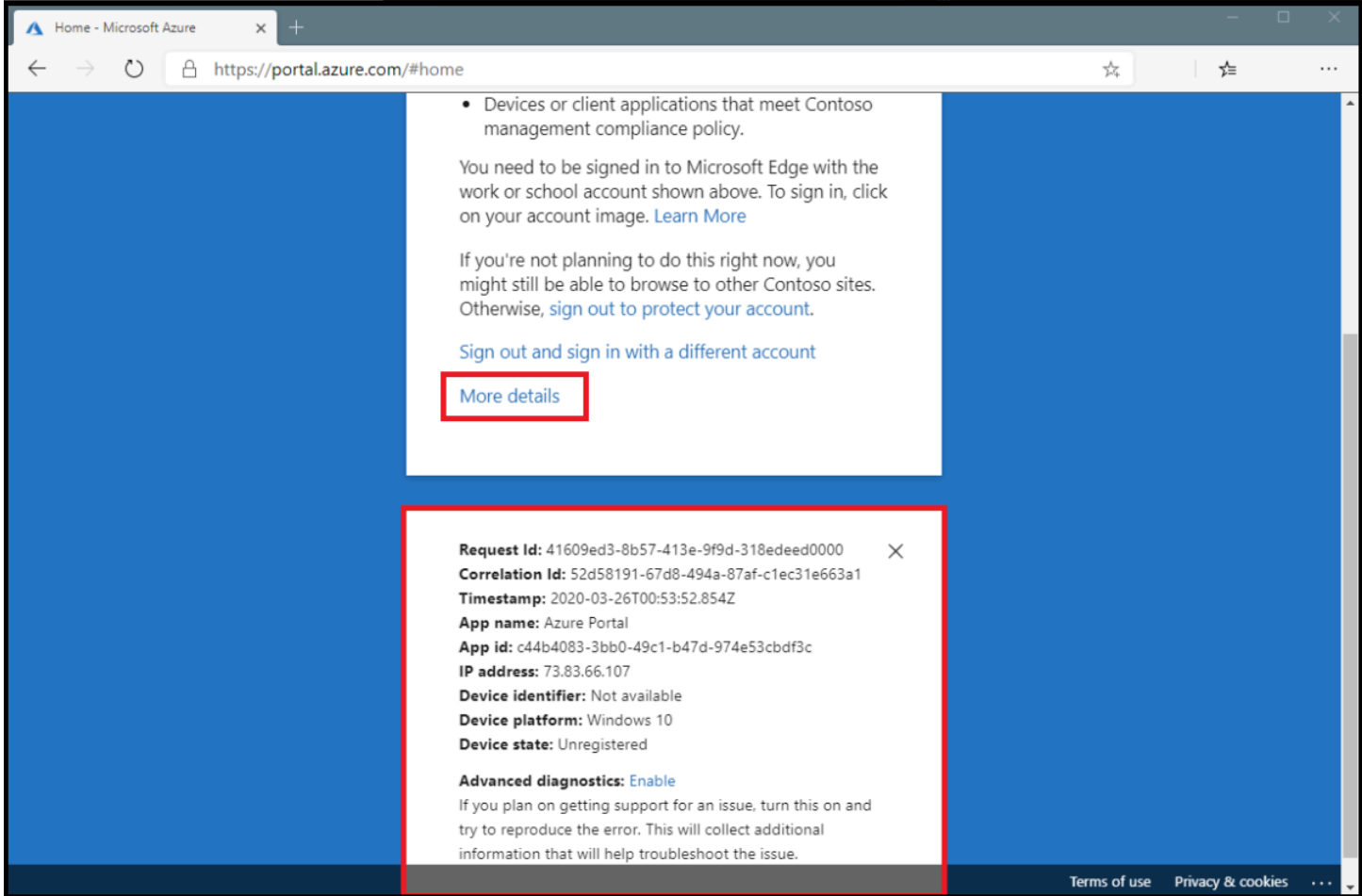


In the above error, the message states that the application can only be accessed from devices or client applications that meet the company's mobile device management policy. In this case, the application and device don't meet the policy.

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.

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home >

Sign-in events

Download Export Data Settings Troubleshoot Refresh Columns Got feedback

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : Last 24 hours Show dates as : Local Status : Failure Add filters

User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins Managed identity

Date	Request ID	User	Application	Status
3/21/2024, 1:01:18 PM	a0a0a0a0-bbbb-ccc...	MOD Administrator	Microsoft App Acces...	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.

Microsoft Entra admin center

Search resources, services, and docs (G+)

admin@M365BV646824...
CONFOSO (M365BV646824) ON...

Users
Groups
Devices
Applications
Roles & admins
Billing
Settings
Protection
Identity governance
External Identities
User experiences
Hybrid management
Monitoring & health
Sign-in logs
Audit logs
Provisioning logs
Health (Preview)
Log Analytics
Diagnostic settings
Learn & support

Home >
Sign-in events

Download Export Data Settings Troubleshoot

Want to switch back to the default sign-ins experience?

Date: Last 24 hours Show dates as: Local

User sign-ins (interactive) User sign-ins (non-interactive)

Date	Request ID	User
3/22/2024, 12:19:14 ...	e7c295e5-7473-495...	MOD A
3/22/2024, 12:19:10 ...	87d962b3-bd71-4ce...	MOD A
3/22/2024, 12:07:52 ...	11d8de98-e2b5-4a0...	MOD A
3/22/2024, 12:05:00 ...	4c41a892-57d5-4d2...	MOD A
3/22/2024, 11:56:26 ...	9ae140a9-5610-422...	MOD A
3/22/2024, 11:55:33 ...	d1003fe3-8ba2-4cf4...	MOD A
3/22/2024, 11:55:26 ...	32b8f352-d674-499f...	MOD A
3/22/2024, 11:48:01 ...	94fade41-55f9-40a4...	MOD A
3/22/2024, 9:17:08 AM	0b5b4030-9724-411...	MOD A
3/21/2024, 1:01:42 PM	276c6131-b763-495...	MOD A
3/21/2024, 1:01:35 PM	e7c295e5-7473-495...	MOD A
3/21/2024, 1:01:31 PM	8be49135-c0c0-462...	MOD A
3/21/2024, 1:01:18 PM	0c010a0b-ddec-40f5...	MOD A
3/21/2024, 1:00:59 PM	e712db1f-d26e-45d...	MOD A
3/21/2024, 1:00:50 PM	2f05d340-adec-4648...	MOD A

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only

Search

Policy Name	Grant Controls	Session Controls	Result
access policy	Require multifactor authentica...		Success


A sign-in can also be interrupted (e.g. blocked, multifactor authentication challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.

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

Sign-in Error Code	Error String
53003	BlockedByConditionalAccess
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.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane shows the 'Sign-in logs' section selected. The main area is divided into two panes. The left pane, titled 'Sign-in events', shows a list of sign-in events with columns for Date, Request ID, and User. The right pane, titled 'Activity Details: Sign-ins', shows details for a specific sign-in event. The 'Basic info' tab is active, displaying fields such as Date, Request ID, Correlation ID, Authentication requirement, Status, Continuous access evaluation, User, Username, User ID, Sign-in identifier, User type, Cross tenant access type, Application, Application ID, Resource, Resource ID, Resource tenant ID, Home tenant ID, and Home tenant name. The 'Application' field is highlighted with a red box, showing 'Azure Portal'. The 'Resource' field is also highlighted with a red box, showing 'Windows Azure Service Management API'.

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](#)