Troubleshooting sign-in problems with Conditional Access

- 1 contributor - MicrosoftGuyJFlo

The information in this article can be used to troubleshoot unexpected sign-in outcomes related to Conditional Access using error messages and Azure AD sign-ins log.

Select "all" consequences

The Conditional Access framework provides you with a 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, you should 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 cloud apps:

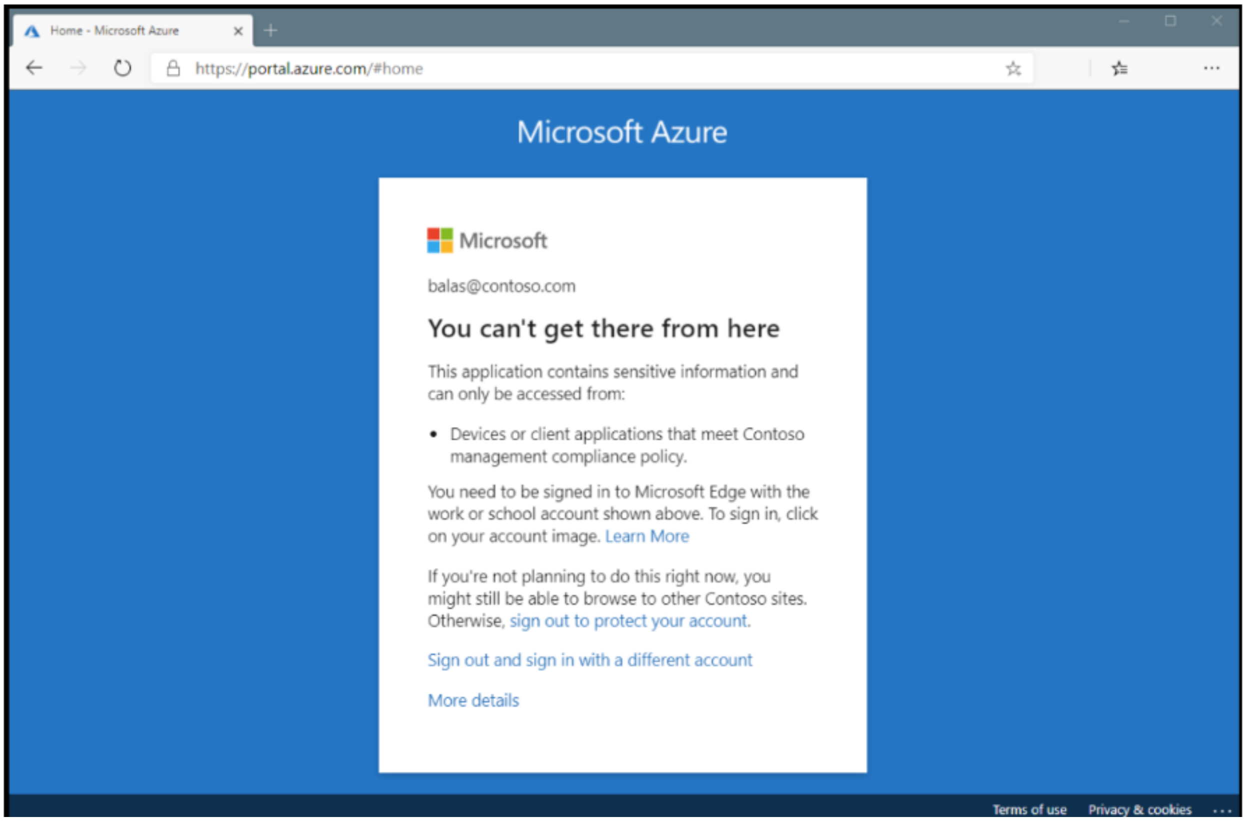
- **Block access** - This configuration blocks your entire organization.
- **Require device to be marked as compliant** - For users that haven't enrolled their devices yet, this policy blocks all access including access to the Intune portal. If you're an administrator without an enrolled device, this policy blocks you from getting back into the Azure portal to change the policy.
- **Require Hybrid Azure AD domain joined device** - This policy block access has also the potential to block access for all users in your organization if they don't have a hybrid Azure AD joined device.
- **Require app protection policy** - This policy block access has also 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 cloud apps, all device platforms:

- **Block access** - This configuration blocks your entire organization.

Conditional Access sign-in interrupt

The first way is to 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 may describe what the problem is and that may suggest a solution.



balas@contoso.com

You can't get there from here

This application contains sensitive information and can only be accessed from:

- Devices or client applications that meet Contoso management compliance policy.

You need to be signed in to Microsoft Edge with the work or school account shown above. To sign in, click on your account image. Learn More

If you're not planning to do this right now, you might still be able to browse to other Contoso sites. Otherwise, sign out to protect your account.

Sign out and sign in with a different account

More details

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 that policy.

Azure AD sign-in events

The second method to get detailed information about the sign-in interruption is to review the Azure AD 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** will reveal troubleshooting information that is helpful when searching the Azure AD 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 do the following.

1. Sign in to the **Azure portal** as a global administrator, security administrator, or global reader.
2. Browse to **Azure Active Directory** > **Sign-ins**.
3. Find the event for the sign-in to review. Add or remove filters and columns to filter out unnecessary information.
    1. Add filters to narrow the scope:
        1. **Correlation ID** when you have a specific event to investigate.
        2. **Conditional access** to see policy failure and success. Scope your filter to show only failures to limit results.
        3. **Username** to see information related to specific users.
        4. **Date** scoped to the time frame in question.

4. Once the sign-in event that corresponds to the user's sign-in failure has been found select the **Conditional Access** tab. The Conditional Access tab will show the specific policy or policies that resulted in the sign-in interruption.
    1. Information in the **Troubleshooting and support** tab may provide a clear reason as to why a sign-in failed such as a device that didn't meet compliance requirements.
    2. To investigate further, drill down into the configuration of the policies by clicking on the **Policy Name**. Clicking the **Policy Name** will show the policy configuration user interface for the selected policy for review and editing.
    3. 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 details

Selecting the ellipsis on the right side of the policy in a sign-in event brings up policy details. This 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, the sign-in diagnostic tool can be used. The sign-in diagnostic can be found under **Basic info** > **Troubleshoot Event**. For more information about the sign-in diagnostic, see the article What is the sign-in diagnostic in Azure AD.

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 will allow Microsoft support to find the specific event you're concerned about.

Conditional Access error codes

Sign-in Error Code	Error String
53000	DeviceNotCompliant
53001	DeviceNotDomainJoined
53002	ApplicationUsedIsNotAnApprovedApp
53003	BlockedByConditionalAccess
53004	ProofUpBlockedDueToRisk

What to do if you're locked out of the Azure portal?

If you're locked out of the Azure portal due to an incorrect setting in a Conditional Access policy:

- Check is there are other administrators in your organization that aren't blocked yet. An administrator with access to the Azure portal 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.