Enabling Token Protection in Entra ID Conditional Access

> **Licensing -** Microsoft Entra ID P1 is required for Token Protection.

> Browser-based sessions NOT supported (only native apps). Deploy in Report-only mode first to prevent app/device disruption. MDM is required for macOS/iOS preview support.

> The 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. - According to Microsoft Learn.

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

Capture logs and analyze

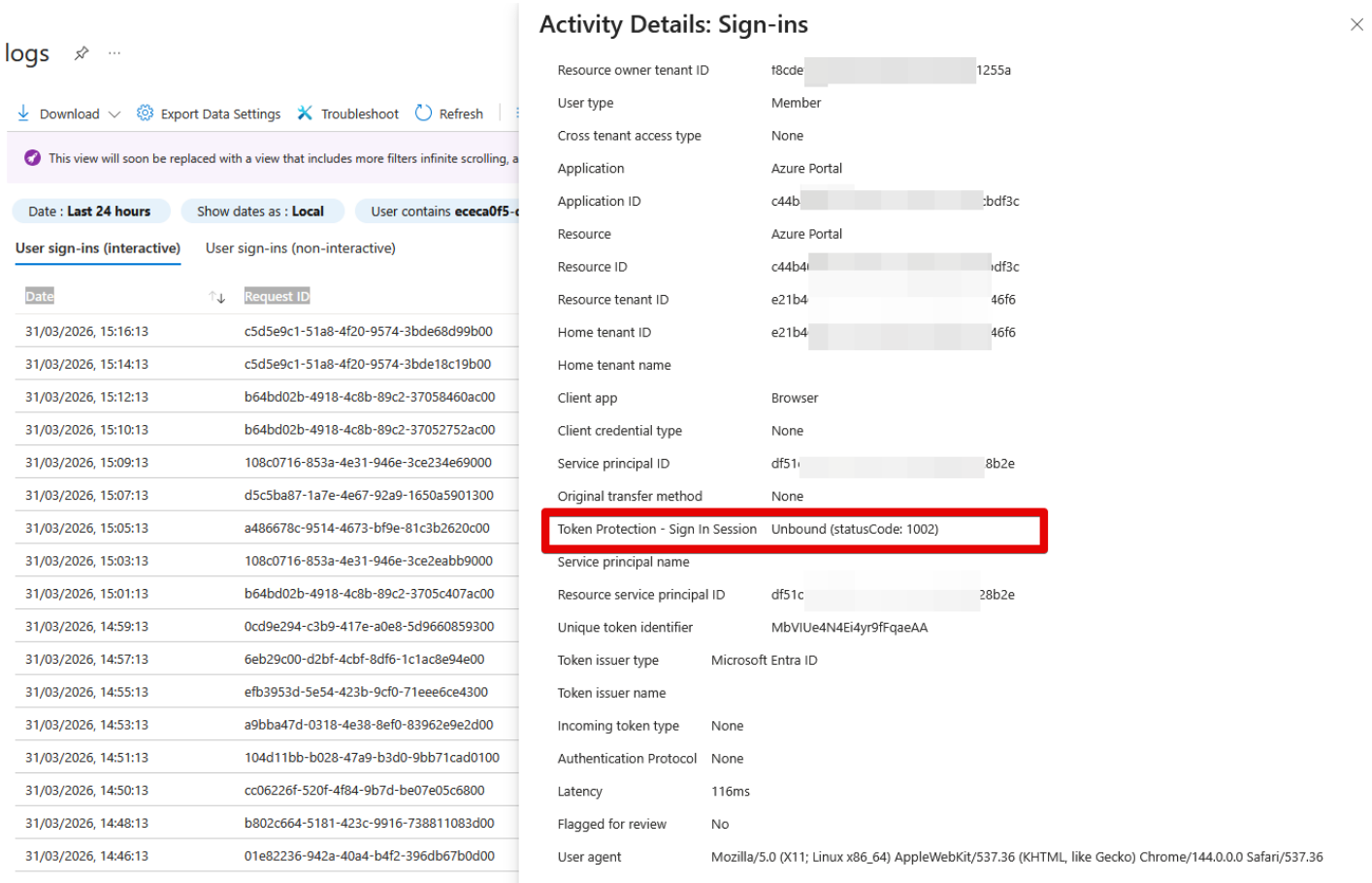
Monitor Conditional Access enforcement of token protection before and after enforcement by using features like Policy impact, Sign-in logs, and Log Analytics.

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.

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:
    1. 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 correlation ID.

2. Unbound: the request wasn't using bound protocols. Possible `statusCodes` when request is unbound are:
    1. 1002: The request is unbound due to the lack of Microsoft Entra ID device state.
    2. 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.
    3. 1005: The request is unbound for other unspecified reasons.
    4. 1006: The request is unbound because the OS version is unsupported.
    5. 1008: The request is unbound because the client isn't integrated with the platform broker, such as Windows Account Manager (WAM).



Revision #6
Created 2026-03-19 11:29:04 UTC by AK. Udofeh
Updated 2026-03-31 14:31:14 UTC by AK. Udofeh