

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).

The screenshot shows the Microsoft Entra ID logs interface. On the left, the 'logs' view is active, displaying a table of sign-in events. The table has columns for 'Date' and 'Request ID'. The right pane shows 'Activity Details: Sign-ins' for a specific event. A red box highlights the 'Token Protection - Sign in Session' entry, which has a status of 'Unbound (statusCode: 1002)'. Below this, the 'User agent' field shows 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36'.

Date	Request ID
31/03/2026, 15:16:13	c5d5e9c1-51a8-4f20-9574-3bde68d99b00
31/03/2026, 15:14:13	c5d5e9c1-51a8-4f20-9574-3bde18c19b00
31/03/2026, 15:12:13	b64bd02b-4918-4c8b-89c2-37058460ac00
31/03/2026, 15:10:13	b64bd02b-4918-4c8b-89c2-37052752ac00
31/03/2026, 15:09:13	108c0716-853a-4e31-946e-3ce234e69000
31/03/2026, 15:07:13	d5c5ba87-1a7e-4e67-92a9-1650a5901300
31/03/2026, 15:05:13	a486678c-9514-4673-bf9e-81c3b2620c00
31/03/2026, 15:03:13	108c0716-853a-4e31-946e-3ce2eabb9000
31/03/2026, 15:01:13	b64bd02b-4918-4c8b-89c2-3705c407ac00
31/03/2026, 14:59:13	0cd9e294-c3b9-417e-a0e8-5d9660859300
31/03/2026, 14:57:13	6eb29c00-d2bf-4cbf-8df6-1c1ac8e94e00
31/03/2026, 14:55:13	efb3953d-5e54-423b-9cf0-71eee6ce4300
31/03/2026, 14:53:13	a9bba47d-0318-4e38-8ef0-83962e9e2d00
31/03/2026, 14:51:13	104d11bb-b028-47a9-b3d0-9bb71cad0100
31/03/2026, 14:50:13	cc06226f-520f-4f84-9b7d-be07e05c6800
31/03/2026, 14:48:13	b802c664-5181-423c-9916-738811083d00
31/03/2026, 14:46:13	01e82236-942a-40a4-b4f2-396db67bd000

Property	Value
Resource owner tenant ID	t8cde...1255a
User type	Member
Cross tenant access type	None
Application	Azure Portal
Application ID	c44b...:bdf3c
Resource	Azure Portal
Resource ID	c44b4...df3c
Resource tenant ID	e21b4...46f6
Home tenant ID	e21b4...46f6
Home tenant name	
Client app	Browser
Client credential type	None
Service principal ID	df51...8b2e
Original transfer method	None
Token Protection - Sign in Session	Unbound (statusCode: 1002)
Service principal name	
Resource service principal ID	df51c...28b2e
Unique token identifier	MbVIUe4N4Ei4yr9FqaeAA
Token issuer type	Microsoft Entra ID
Token issuer name	
Incoming token type	None
Authentication Protocol	None
Latency	116ms
Flagged for review	No
User agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36

Revision #6

Created 2026-03-19 11:29:04 UTC by AK. Udofeh

Updated 2026-03-31 14:31:14 UTC by AK. Udofeh