

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-understand-cors-issues#option-3-update-http-headers>

Option 5: Extend the lifetime of the access token

Some CORS issues can't be resolved, such as when your app redirects to *login.microsoftonline.com* to authenticate, and the access token expires. The CORS call then fails. A workaround for this scenario is to extend the lifetime of the access token, to prevent it from expiring during a user's session. For more information about how to do this, see [Configurable token lifetimes in Azure AD](#).

Fiddler:

The screenshot shows the Fiddler Classic interface. The left pane displays a list of HTTP requests. The right pane shows the details of a selected request, including headers, response, and cache information.

#	Result	Protocol	Host	URL
467	200	HTTPS	clientservices.googleapis.com	/chrome-variations/seed?osname=win&ch...
468	200	HTTP	Tunnel to safebrowsing.googleapis.com	/safebrowsing.googleapis.com:443
469	200	HTTPS	safebrowsing.googleapis.com	/v4/threatlist/updates:fetch?req=Ch4K...
470	200	HTTP	Tunnel to nxgensiabeluat.johnsoncontrols.com	nxgensiabeluat.johnsoncontrols.com:443
471	200	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
472	200	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu?SWECmd=G...
473	200	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
474	200	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
475	200	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
476	200	HTTP	Tunnel to content-autofill.googleapis.com	content-autofill.googleapis.com:443
477	200	HTTPS	content-autofill.googleapis.com	/v1/pages/ChVdaHjvWUvMTAYtJAUNTA...
478	200	HTTP	Tunnel to www.google.com	www.google.com:443
479	200	HTTP	Tunnel to www.google.com	www.google.com:443
480	200	HTTP	Tunnel to clientservices.googleapis.com	clientservices.googleapis.com:443
481	304	HTTPS	clientservices.googleapis.com	/chrome-variations/seed?osname=win&ch...
482	200	HTTP	Tunnel to nxgensiabeluat.johnsoncontrols.com	nxgensiabeluat.johnsoncontrols.com:443
483	302	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
484	200	HTTP	Tunnel to login.microsoftonline.com	login.microsoftonline.com:443
485	200	HTTPS	login.microsoftonline.com	/a1f1e214-7ded-45b6-81a1-9e8ae3459641/...
486	302	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
487	200	HTTP	Tunnel to login.microsoftonline.com	login.microsoftonline.com:443
488	200	HTTPS	login.microsoftonline.com	/a1f1e214-7ded-45b6-81a1-9e8ae3459641/...
489	302	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
490	200	HTTP	Tunnel to login.microsoftonline.com	login.microsoftonline.com:443
491	200	HTTPS	login.microsoftonline.com	/a1f1e214-7ded-45b6-81a1-9e8ae3459641/...
492	302	HTTPS	nxgensiabeluat.johnsoncontrols.com	/siebel/app/openservice/enu
493	200	HTTP	Tunnel to login.microsoftonline.com	login.microsoftonline.com:443
494	200	HTTPS	login.microsoftonline.com	/a1f1e214-7ded-45b6-81a1-9e8ae3459641/...

The right pane shows the details of the selected request (485). The Request Headers section includes:

- Access-Control-Request-Headers: x-requested-with
- Access-Control-Request-Method: GET
- Referer: https://nxgensiabeluat.johnsoncontrols.com/

The Security section shows:

- Origin: https://nxgensiabeluat.johnsoncontrols.com
- Sec-Fetch-Dest: empty
- Sec-Fetch-Mode: cors
- Sec-Fetch-Site: cross-site

The Transport section shows:

- Connection: keep-alive
- Host: login.microsoftonline.com

The Response Headers section shows:

- HTTP/1.1 200 OK
- Cache-Control: no-store, no-cache
- Date: Fri, 17 Jun 2022 22:41:23 GMT
- Expires: -1
- Pragma: no-cache

CORS error browser> Inspect

The screenshot shows the browser's developer tools with the 'Console' tab selected. It displays several error messages related to CORS (Cross-Origin Resource Sharing) policy violations. The errors indicate that the response to a preflight request doesn't pass access control checks because the 'Access-Control-Allow-Origin' header is not present on the requested resource.

```
Access to XMLHttpRequest at 'https://login.microsoftonline.com/a1f1e214-7ded-45b6-81a1-9e8ae3459641/oauth-3EndOfStateParam%23&client-request-id=48ff21f7-15da-4dba-a6b3-f8351884791f' (redirected from 'https://nxgensiabeluat.johnsoncontrols.com/siebel/app/openservice/enu') from origin 'https://nxgensiabeluat.johnsoncontrols.com' has been blocked by CORS policy: Response to preflight request doesn't pass access control check: No 'Access-Control-Allow-Origin' header is present on the requested resource.
GET https://login.microsoftonline.com/a1f1e214-7ded-45b6-81a1-9e8ae3459641/oauth-3EndOfStateParam%23&client-request-id=48ff21f7-15da-4dba-a6b3-f8351884791f net::ERR_FAILED
Access to XMLHttpRequest at 'https://login.microsoftonline.com/a1f1e214-7ded-45b6-81a1-9e8ae3459641/oauth-3EndOfStateParam%23&client-request-id=48ff21f7-15da-4dba-a6b3-f8351884791f' (redirected from 'https://nxgensiabeluat.johnsoncontrols.com/siebel/app/openservice/enu') from origin 'https://nxgensiabeluat.johnsoncontrols.com' has been blocked by CORS policy: Response to preflight request doesn't pass access control check: No 'Access-Control-Allow-Origin' header is present on the requested resource.
GET https://login.microsoftonline.com/a1f1e214-7ded-45b6-81a1-9e8ae3459641/oauth-3EndOfStateParam%23&client-request-id=48ff21f7-15da-4dba-a6b3-f8351884791f net::ERR_FAILED
Access to XMLHttpRequest at 'https://login.microsoftonline.com/a1f1e214-7ded-45b6-81a1-9e8ae3459641/oauth-3EndOfStateParam%23&client-request-id=48ff21f7-15da-4dba-a6b3-f8351884791f' (redirected from 'https://nxgensiabeluat.johnsoncontrols.com/siebel/app/openservice/enu') from origin 'https://nxgensiabeluat.johnsoncontrols.com' has been blocked by CORS policy: Response to preflight request doesn't pass access control check: No 'Access-Control-Allow-Origin' header is present on the requested resource.
```