Genesys Knowledge Center Deployment Guide

Cross Origin Resource Sharing (CORS) Filter

3/6/2026

Contents

Cross Origin Resource Sharing (CORS) Filter

What is CORS?

Since the browser Same Origin Policy prevents a web page from making an XMLHttpRequest to another domain, the Genesys Knowledge Center supports Cross Origin Resource Sharing (CORS) to allow the web application to interact with the Knowledge Center APIs across domains.

For a simple request — one that uses either GET or POST and whose body is text/plain — the request is sent with an extra header called Origin. The Origin header contains the origin URI (scheme, domain name or address, and port, as per RFC 6454) of the requesting page so that the server can easily determine whether or not it should serve a response. An example Origin header might look like this:

`Origin:` http://www.genesys.com:8080

If the server decides that the request should be allowed, it either sends an Access-Control-Allow-Origin header echoing back the same origin that was sent or '*' if it is a public resource.

For example:

`Access-Control-Allow-Origin:` http://www.genesys.com:8080

If this header is missing, or the value of this header does not match the value of Origin header, then the browser disallows the request. If all is well, then the browser processes the response.

For general information and background on CORS, see Cross-Origin Resource Sharing.

Configuring CORS Filter

Knowledge Center supports the CORS pre-flight OPTIONS requests.

Types of requests:

- A CORS request is an HTTP request that includes an `Origin` header.
- A CORS-preflight request is a CORS request that checks to see if the CORS protocol is understood. It uses `OPTIONS` as method.

Allowed-Origins

To set up Cross-Origin Resource Sharing, make sure you set the `allowedOrigins` option in the `cross-origin` section of Knowledge Center Cluster application. Knowledge Center will use the provided list of domains to validate the `Origin` header of the request and respond with `Access-Control-Allow-Origin` in response.

> **Important**
>
> By default `cross-origin/allowedOrigins` is set to * which makes it possible to use Knowledge Center APIs from any web resource. Before going into production mode, the default value of this option MUST be updated with the most precise list of origins in which API access is allowed.

`allowedOrigins` option must be set as a comma-separated list of allowed domains. For example:

```
allowedOrigins=http://*.genesys.com,http://*.genesyslab.com
```

Other CORS options

All options are collected in section `cross-origin` (default), however the name of this section can be changed. **Note:** Genesys Knowledge Center has two application servers, while CMS and every other application have their own section: `gks.cross-origin` and `cms.cross-origin`.

Option	Description	Default value
skipCheckControlRequestHeaders	Allow pass **CROSS** preflight request with out check Access-Control-Request-Headers.	false **for Genesys Knowledge Center:** true
preflightMaxAge	The number of seconds that preflight requests can be cached by the client.	1800 seconds, or 30 minutes **for Genesys Knowledge Center:** 3600 seconds, or 60 minutes
passBlockedRequestToChain	Allow pass next chain if this request is **CROSS** request but not allowed by origin, method, or header.	true
exposedHeaders	A whitelist of additional response headers to be exposed to the browser tab beyond the default headers.	Cache-Control,Content-Language,Content-Type,Expires,Last-Modified,Pragma **for Genesys Knowledge Center:** gkc_agentId,gkc_apiClientId,gkc_apiClientMediaType, gkc_customerId,gkc_interactionId,gkc_sessionId, ContactCenterID,Authorization,contentType
enable	Boolean value that allows `cross-origin` filter.	true
emptyAllowedFor	A comma-separated list of requested URLs that are allowed to access this server application in the case when there is no	.* (any request)

Option	Description	Default value
	Origin and **Referer**. This option is affected if `allowOrigin` does not contain "*" (any origin).	
disableHttpOptionsRequest	Boolean value that disables the **OPTIONS** http request if it is `true`. If it is `false` we cannot use preflight requests.	false
checkReferer	Boolean value; will answer **Referrer** canonized to **Origin** instead of **Origin** for use with native **CrossOrigin** check. If this option is enabled: • Origin present and Referrer present and both are valid (filter recognizes them as allowed for CrossOrigin), so CrossOrigin headers are added to response. • Origin absent and Referrer present and valid, so CrossOrigin headers are added to response. • Origin present and Referrer present and one of them is invalid, so CrossOrigin headers are not added to response.	true
chainPreflight	If `true`, preflight requests are chained to their target resource for normal handling (as an **OPTION** request). Otherwise the filter responds to the preflight.	true
allowedOrigins	A comma-separated list of origins (for example, instrumented web sites) allowed to access this server application. If an allowed origin contains one or more "*" characters (for example http://*.domain.com) this can be interpreted as a regular expression.	"*" (any origin)
allowedMethods	a comma-separated list of **HTTP** methods that are allowed to be used when accessing the resources (for preflight requests).	GET,POST,HEAD **for Genesys Knowledge Center:** GET,POST,HEAD,PUT,DELETE, ATCH
allowedHeaders	a comma separated list of **HTTP** headers that are allowed to be	X-Requested-With,Content-Type,Accept,Origin

Option	Description	Default value
	specified when accessing the resources (for preflight requests).	**for Genesys Knowledge Center:** gkc_agentId,gkc_apiClientId,gkc_apiClientMediaType, gkc_customerId,gkc_interactionId,gkc_sessionId, ContactCenterID,Authorization,contentType,Content-Type
allowCredentials	A boolean indicating if the resource allows requests with credentials.	false **for Genesys Knowledge Center:** true

For morel information and background on CORS and response headers, see Cross Origin Resource Sharing Standard.