Web Services API Reference

Cross-Origin Resource Sharing

4/13/2025

Cross-Origin Resource Sharing

This is part of the API Basics section of the Web Services API.

Overview

Cross-Origin Resource Sharing (CORS) is a specification that enables open access across domain-boundaries.

Each contact center can define their own allow origin list through Web Services access control settings.

Web Services will filter an incoming request by merging global `allowOrigins` and contact center access control settings by using an `Admin` account.

Operations

The following operations are available for this group:

Operation	Description	Permissions
GET	Retrieves an array of settings	Contact Center Admin
POST	Creates a new setting in this group. `allowedOrigins` is the only valid setting.	Contact Center Admin
PUT	Updates a setting.	Contact Center Admin
DELETE	Removes a setting.	Contact Center Admin

Settings

Attribute name	Description
allowedOrigins	An array of valid "origins" for this contact center. The CORS filter will use this list to validate incoming requests.

> **Tip**
> Wildcards are allowed in the context of a domain name for `allowedOrigins`, but `"*"`

> by itself is not permitted.

Examples

Retrieve access control settings

```
GET /settings/access-control {
   settings:[
{
  “name”:”allowedOrigins”,
  “value”: ["https://cloud.genGWS.com", "https://*.genGWS.com"]
}
]
```

Add "genesys.com" to the list of domains

```
PUT /settings/access-control {
   settings:
{
  “name”:”allowedOrigins”,
  “value”: ["https://cloud.genGWS.com", "https://*.genGWS.com", "https://*.genesys.com"]
}
```

> **Important**
> When sending the above, the entire array must be sent