

# Cross-Origin Resource Sharing (CORS)

By default, for security reasons, the SCIM interface is published for any server application, but not for client-side (javascript) applications.

In order to allow client-side applications to query or modify SCIM objects, the CORS protocol states how to define the restrictions that apply to client-side applications. CORS settings can be tuned adding two parameters:

| Parameter                       | Value  |
|---------------------------------|--|
| <b>soffid.scim.cors.origin</b>  | Set a comma separated list of DNS domains allowed to perform SCIM operations.<br>Set to * to allow access from any domain  |
| <b>soffid.scim.cors.methods</b> | Set a comma-separated list of allowed operations.<br>By default, it is set to <b>GET, OPTIONS, HEAD</b><br>To allow any operation, set it to <b>GET, POST, PUT, PATCH, DELETE, OPTIONS, HEAD</b> |

These parameters can be changed in real-time for any tenant. Mind that setting these values for the master tenant applies to master tenant, but also applies as default values for any child tenant.

---

Revision #1

Created 12 May 2023 06:37:23 by Gabriel Buades

Updated 12 May 2023 06:46:18 by Gabriel Buades