



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Web Services and Applications Deployment Guide

CORS filter

CORS filter

Web Services supports Cross-Origin Resource Sharing (CORS) filter, which allows applications to request resources from another domain. For general information and background on CORS, see [Cross-Origin Resource Sharing](#).

Important

CORS must be enabled for the screen recording options to be available in the Speechminer Web UI when the using Microsoft Internet Explorer web browser.

To set up Cross-Origin Resource Sharing, make sure you set the [crossOriginSettings](#) option in the `serverSettings` section of the **application.yaml** file on each of your Web Services nodes (**server-settings.yaml** if you're installing Web Services and Applications version 8.5.201.09 or earlier). It specifies the configuration for cross-origin resource sharing in Web Services. Make sure this option has the **exposedHeaders** setting with a value that includes X-CSRF-HEADER,X-CSRF-TOKEN.

For example, your configuration might look like this:

```
crossOriginSettings:
  corsFilterCacheTimeToLive: 120
  allowedOrigins: http://*.genesys.com, http://*.genesyslab.com
  allowedMethods: GET,POST,PUT,DELETE,OPTIONS
  allowedHeaders: "X-Requested-With,Content-Type,Accept,Origin,Cookie,authorization,ssid,surl,ContactCenterId,X-CSRF-TOKEN"
  allowCredentials: true
  exposedHeaders: "X-CSRF-HEADER,X-CSRF-TOKEN"
```

For more information about CORS in the Web Services API, see [Cross-Origin Resource Sharing](#).

Next step

- [Back to Configuring security](#)