Web Services and Applications Deployment Guide

CSRF protection

4/10/2025

CSRF protection

Web Services provides protection against Cross Site Request Forgery (CSRF) attacks. For general information and background on CSRF, see the OWASP CSRF Prevention Cheat Sheet.

To set up Cross Site Request Forgery protection, set the following options 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) :

- enableCsrfProtection — determines whether CSRF protection is enabled on the Web Services node.
- crossOriginSettings — 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:

```
enableCsrfProtection: true
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"
    allowCredentials: true
    exposedHeaders: "X-CSRF-HEADER,X-CSRF-TOKEN"
```

For more information about CSRF protection in the Web Services API, see Cross Site Request Forgery Protection.

Next step

- Back to Configuring security