



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

CSRF protection

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:

- **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](#)