



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.

Genesys Administrator Extension Deployment Guide

Cross-site Scripting and Cookies

12/14/2025

Cross-site Scripting and Cookies

Contents

- [1 Cross-site Scripting and Cookies](#)
 - [1.1 Securing Server-side Cookies](#)

You can configure your system to improve the protection of Genesys Administrator Extension against Cross-site Scripting (XSS) attacks by configuring the `HttpOnly` and `Secure` flags on your HTTP server to further enhance the existing GAX security. These flags tell browsers how to handle cookies.

Server-side cookies can be tagged with `HttpOnly` and `Secure` flags to tell the browser how to deal with them. To achieve a maximum level of security, administrators must make this configuration on the Application Server.

Securing Server-side Cookies

HttpOnly

Setting the `HttpOnly` flag on cookies forces the browser to prevent (disallow) scripts from accessing the cookies. This prevents JavaScript that might be introduced through an XSS attack into a browser page to access cookie data and send it to a different person. Stolen cookie data can also be used to hijack a browser session.

Secure Flag

With the `Secure` flag set, cookies are transmitted only from the browser to the server when the connection is secured by using the HTTPS protocol. This setting is applicable to HTTPS connections only. Therefore, you must configure GAX to use an HTTPS connector, not an HTTP connector.

Setup

Follow these recommendations to configure the `HttpOnly` and `Secure` flags.

HttpOnly

Open and edit the following file: `$CATALINA_HOME/conf/context.xml`

To set the `HttpOnly` flag, add the following attribute:

```
useHttpOnly="true"
```

The main tag should be:

```
<Context useHttpOnly="true">
```

Instead of: `<Context>`

Secure Flag

Open and edit the following file: `$CATALINA_HOME/conf/server.xml`

To set the `Secure` flag, add the following attribute to the HTTPS connector:

```
secure="true"
```

The flag must not be applied to any non-HTTPS connectors. If you apply the flag to an HTTP connection, it will become unusable for Genesys Administrator Extension.

The following is an example of a valid connector:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
maxThreads="150" scheme="https" secure="true"  
keystoreFile="/home/gcti/keystore.key" keystorePass="genesys"  
clientAuth="false" sslProtocol="TLS" />
```