Genesys Administrator Extension Deployment Guide

Cross-site Scripting and Cookies

5/10/2025

Cross-site Scripting and Cookies

Contents

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 Tomcat 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" />
```

Load Balance for Apache Tomcat

The following information applies to Apache Tomcat Configuration for communication by using the AJP protocol with a Web Server in front of it that is acting as a load balancer (for example, Apache Web Server. AJP is a protocol).

You might have to configure Load Balancing to accommodate the use of the `HttpOnly` and `Secure` flags.

In the `$CATALINA_HOME/conf/server.xml` file, make the following adjustment to support the Apache JServ Protocol (AJP) on the default connector:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" secure="true"/>
```