# Deployment Guide

## Security Tips for Third-Party Components

12/18/2025

# Security Tips for Third-Party Components

Web Engagement can't do its job without the help of these third-party Java-based applications:

- Cassandra
- Elasticsearch

Because Genesys doesn’t create these products, we can't control their dependencies. This means that they are subject to vulnerabilities that would not otherwise affect Web Engagement. Please pay attention to the following recommendations as you are securing your Web Engagement environment.

## Cassandra

Be sure that:

- This cluster is located in the secure zone.
- Access to Cassandra hosts (default ports 9042, 9160, 7000, 7001) is granted only for a limited set of client connections.

By default, Cassandra will not open a JMX port, but if you do need to open one, please consider that an open JMX connection is a security exposure, so pay attention to securing the JMX port by taking care of things like these:

- Limit access to specific IP addresses.
- Apply authentication parameters.

## Elasticsearch

GWE 8.5.2 relies on the external Elasticsearch 6.8 that is installed by customers. However, X-Pack security is not currently supported by GWE. Be sure that:

- Elasticsearch cluster is located in the secure zone.
- Access to Elasticsearch hosts (default ports 9200, 9300) is granted only for a limited set of IP addresses.