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.

Deployment Guide

Security Tips for Third-Party Components

12/20/2025

Contents

Security Tips for Third-Party Components

Web Engagement and Data Processing Server can't do their jobs without the help of these third-party Java-based applications:

- Cassandra
- Elasticsearch
- Spark

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.

Spark

Genesys Data Processing Server comes with Spark, which runs separately outside of the Data Processing Server JVM process. Be sure to limit your Spark-related connections, by verifying for example, that:

- Ports are opened only for specific IP addresses
- JMX is controlled in the appropriate way

Cassandra

Genesys recommends that you use an external Cassandra cluster. 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

In Web Engagement 8.5.1, the Elasticsearch nodes are running in the same JVM as the Cassandra nodes. This means that most Cassandra-related security measures will automatically be applied to Elasticsearch.

However, Elasticsearch also opens additional ports (by default 9200 and 9300), so these ports must also be secured.