Genesys Mobile Services Deployment Guide

Transport Layer Security

4/24/2025

Transport Layer Security

Genesys Mobile Services (GMS) supports Transport Layer Security (TLS), which enables cryptographic and trusted communications between Genesys clients and servers.

TLS features to note:

- Upgrade mode for Configuration Server
- No mutual TLS mode where server and client exchange their certificate (only server certificate is checked)

See the *Genesys Security Deployment Guide* for additional information about TLS.

Chat Server Specifics

GMS has no direct connection to Chat Server.

To implement TLS to Chat Server: this is the connection from Web API Server to Chat Server that must be configured using the same TLS option as what is described from direct connection from GMS to Message Server or Stat Server.

In background, for each Chat polling (5s/chat session):

- GMS requests to load-balancer for Chat Server information.
- GMS gets ChatServer host:port, TLS information, and build connection.
- If connection is secured, GMS must be configured with certificate on host or application level (it is not possible on the connection level).

Summary

The following table summarizes the GMS TLS connection support for Genesys servers.

GMS connect to	TLS support	Comment
Configuration Server	Yes	Upgrade mode only.
Message Server	Yes	TLS server port must be enabled.
Statistics Server	See comments.	Not configured at startup, but should work.
Chat Server	Yes	Connection information returned by Web API Server Load-Balancer.

GMS connect to	TLS support	Comment
Orchestration Server	No	An HTTP connection. Not configured at startup (that is, not in the GMS Connection tab). Note: GMS uses HTTPClientFactory, and a TLS option can be set (section gms, option http.ssl_trust_all, value=false, true).
Web API Server	No	An HTTP connection. Not configured at startup (that is, not in the GMS Connection tab). Note: GMS uses HTTPClientFactory, and a TLS option can be set (section gms, option http.ssl_trust_all, value=false, true).