



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 Mobile Services Deployment Guide

Transport Layer Security for Third-Party Servers

5/9/2025

Transport Layer Security for Third-Party Servers

Contents

- **1 Transport Layer Security for Third-Party Servers**
 - 1.1 TLS Interconnections in GMS Cluster
 - 1.2 GMS TLS Connections with other Genesys Servers

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.

TLS Interconnections in GMS Cluster

To use SSL/TLS for all incoming GMS connections for one node or for a cluster of nodes, you must set up your nodes to use the SSL/TLS port, by using the following options:

- `server/web_scheme = https` (to change from the default http protocol)
- `server/web_port = 443` (or 8443, instead of using 80 or 8080)

Instead of using SSL/TLS certificates, you can also make GMS trust everything with the following option: `gms/http.ssl_trust_all=true`

GMS now supports secure connections towards eServices, Chat Server, E-mail Server Java, and Universal Contact Server. To implement TLS to Chat Server, you must set up the trust server mode described above.

GMS TLS Connections with other Genesys Servers

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

GMS connection to	TLS support	Comment
Configuration Server	Yes	Upgrade mode only.
Message Server	Yes	TLS server port must be enabled.
Statistics Server	No	Not implemented.
Chat Server	Yes	TLS between GSG/GMS and Chat Server in trust server mode (do not check the certificate).
Universal Contact Server	Yes	TLS between GSG/GMS and Universal Contact Server in trust server mode (do not check the certificate).
E-mail Server Java	Yes	TLS between GSG/GMS and E-mail Server Java in trust server

GMS connection to	TLS support	Comment
		mode (do not check the certificate).
Orchestration Server	Yes	You can set up an HTTPS 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	Yes	You can set up an HTTPS 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).
Universal Routing Server	Yes	You can set up an HTTPS 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).