Genesys Mobile Services Deployment Guide

Transport Layer Security for Third-Party Servers

4/23/2025

Transport Layer Security for Third-Party Servers

Contents

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

TLS features include:

- 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.

Supported TLS versions

The list of supported TLS versions depends on the latest third-party Jetty library embedded in GMS. As a best practice, Genesys recommends using the latest GMS version available as GMS third-party libraries are updated regularly to fix issues and vulnerabilities. For further details about TLS usage in Jetty, read the *Configuring SSL/TLS* section in Jetty Official Documentation.

> **Important**
>
> - TLSv1.0 and TLSv1.1 are no longer supported in the latest Jetty versions and therefore should not be used with GMS.

For further details about TLS versions, you can also check the Transport Layer Security Wikipedia page.

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.

TLS Customization

To disable SSL 2.0 and SSL 3.0, edit the JDK security configuration file:

- Open the `jdk-17.x/conf/security/java.security` file and update the following list:
- `jdk.tls.disabledAlgorithms=SSLv2,SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA,`

Starting in GMS 8.5.227+, to modify the list of supported TLS protocols, open the `etc/jetty-ssl-context.xml` file and edit the properties as follows:

```
<Set name="SniRequired">
   <Property name="jetty.sslContext.sniRequired" default="false"/>
</Set>
<Set name="IncludeProtocols">
   <Array type="String">
       <Item>TLSv1.3</Item>
       <Item>TLSv1.2</Item>
   </Array>
</Set>
<Set name="ExcludeProtocols">
   <Array type="String">
       <Item>TLSv1</Item>
       <Item>TLSv1.1</Item>
       <Item>SSLv3</Item>
   </Array>
</Set>
```

> **Important**
>
> Do not try to authorize protocols that the Jetty third-party library do not support. Genesys recommends using the above configuration as a best practice.

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	Yes	No special procedures. Statistics Server is configured to listen to a TLS port using certificates. In the GMS Connections tab, add StartServer TLS connection (one-way or two-way "mutual" authentication) and copy server certificates on GMS hosts if

GMS connection to	TLS support	Comment
		needed.
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 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).