



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.

Web Services and Applications Deployment Guide

HTTPS for Platform Service

HTTPS for Platform Service

The following configuration are required at the Platform Service for accepting a HTTPS connection.

Server-side configuration for GWS Platform Service

To enable HTTPS at the server-side,

1. Configure the following TLS-specific settings.

Name	Mandatory	Default Value	Description
GWS_SERVER_TLS_REQUIRED	No	false	Determines if TLS is required. Change to true if a certificate is also provided. Note: Once TLS is enabled, Platform Service accepts only HTTPS requests.
GWS_SERVER_TLS_PROVIDER	No	rustls	Specifies the TLS provider. Possible values: rustls, native.
GWS_SERVER_TLS_HANDSHAKE_TIMEOUT	Yes (if TLS is enabled)	10000 (ms)	Specifies the timeout (in milliseconds) for TLS handshake. Default is 10000 ms (10 seconds).
GWS_SERVER_TLS_CERT_PATH	Yes (if TLS is enabled)	-	Specifies the path to the TLS certificate.
GWS_SERVER_TLS_KEY_PATH	Yes (if TLS is enabled)	-	Specifies the path to the TLS key.
GWS_AUTH_TOKEN_IDLE_TIME	No	-	Specifies the idle time (in seconds) before an auth token is considered inactive. If absent, all tokens remain active until expiration.
GWS_SERVER_TLS_CERT_PASSWORD	No	""	Specifies the password for the TLS certificate, if applicable.

2. After you enable TLS for the Platform Service, ensure to update the health check URL in the `get_version()` function within `/usr/bin/gws-service-platform` to use HTTPS. For example, `RESPONSE=$(curl -XGET -skLS https://${GWS_HOST}:${GWS_PORT}${GWS_HEALTH_CHECK_URL} 2>&1)`

3. Update monitoring services, such as Grafana, to send requests to the Platform Service using the HTTPS endpoint after enabling TLS.

Client-side (GWS 8.6) configuration

To establish a HTTPS connection with Platform Service, configure the Platform Service URL in the **application.yaml** file as shown in the following settings:

```
serverSettings:
  platformSettings:
    platformServiceUrl: https://<ip>:<port>
```

Also, make sure that configured CA (Certification Authority) certificates are added to the JKS (Java KeyStore) file.

```
serverSettings:
  caCertificate: /opt/ca_cert.jks #location of the file
  jksPassword: pa$$word #password for the keystore
```