



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.

Configuring TLS for iWD

iWD Web connections

12/14/2025

Contents

- 1 iWD Web connections
 - 1.1 REST server
 - 1.2 PSDK client to Interaction Server, Message Server
 - 1.3 PSDK client to Configuration Server

iWD Web connections

REST server

1. Open **GAX -> Applications -> <iWD Web Server app> -> ports -> default**
2. Fill Certificate and Trusted CA fields with JKS keystore and truststore files.
3. Add Transport parameters **tls-mutual=1, keystore-password, truststore-password, provider=JKS**. The final string should look like this:
 - `tls=1;certificate=/genesys/TLS/keystore.jks;trusted-ca=/genesys/TLS/truststore.jks;keystore-password=KSPASSWD;truststore-password=TSPASSWD;tls-mutual=1;provider=JKS`

PSDK client to Interaction Server, Message Server

1. Open **GAX -> Applications -> <iWD Web Server app> -> connections .**
2. Change the connection to the Interaction Server application to a Secured port.
3. Make sure it has a secured connection to the Message Server application.

PSDK client to Configuration Server

1. Open **GAX -> Applications -> <iWD Web app> -> connections .**
2. Open the connection to Configuration Server and add the following transport parameters:
 - For Linux:
 - `certificate=<path to PEM certificate file>;certificate-key=<path to PEM certificate key file>;trusted-ca=<path to PEM certificate truststore file>;tls-mutual=1`
 - For Windows:
 - `certificate=<certificate_thumbprint>;trusted-ca=<truststore_thumbprint>;tls-mutual=1`