Configuring TLS for iWD

Configuration options

12/20/2025

Contents

Configuration options

Standard Genesys TLS configuration options

Use the configuration options described in the TLS List of Parameters in the *Platform SDK Developer's Guide*.

Certificate password configuration (iWD specific)

There are two ways to set certificate passwords.

Application and Host level options (strongly recommended)

Section	Name	Client/Server Side	Default value	Description
tls-keystore	password	• Simple TLS: SERVER • Mutual TLS: BOTH	N/A	Keystore password
tls-keystore-entry	password	• Simple TLS: SERVER • Mutual TLS: BOTH	N/A	Keystore entry password
tls-truststore	password	• Simple TLS: CLIENT • Mutual TLS: BOTH	N/A	Trusted certificates storage password

In this case passwords are automatically encrypted in the configuration database and masked in the GAX UI.

> **Important**
> Passwords set at the Application and Host levels using the parameters above are

applied to all secured connections of these Applications and Hosts respectively. So every connection MUST use certificates with the same passwords.

Connection/port level options

Important

Passwords set using the parameters below are NOT encrypted in the configuration database and can be viewed in GAX UI. Genesys strongly recommends not using these parameters. The options are to be used only if connection level configuration cannot be avoided.

If it is necessary to define passwords at the connection/port level, use the following parameters.

Name	Client/Server Side	Default value	Description
keystore-password	Simple TLS—Server Mutual TLS—Both.	N/A	Keystore password
keystore-entry-password	Simple TLS—Server Mutual TLS—Both.	N/A	Keystore entry password
tls-truststore	Simple TLS—Client Mutual TLS—Both.	N/A	Trusted certificates storage password