



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

Specific connection configuration details

Contents

- 1 Specific connection configuration details
 - 1.1 Assumptions/Prerequisites
 - 1.2 ActiveMQ
 - 1.3 JDBC configuration
 - 1.4 Windows certificates import
 - 1.5 Framework configuration
 - 1.6 Host configuration
 - 1.7 Troubleshooting

Specific connection configuration details

iWD follows the common Genesys approach and recommends using Host-level configuration with PEM-files on Linux and Windows certificates on Windows for all PSDK connections, REST clients and JMS client. For REST servers, Connection-level configuration with JKS-files is recommended. For JDBC clients the recommended way is to use JKS files and configure connection via JVM options.

Assumptions/Prerequisites

- You have generated certificates with associated private and public keys.
- You have Java keystore and truststore files with the same keys.

Please find more information about certificates [here](#).

ActiveMQ

To configure SSL in ActiveMQ, please refer to the vendor's ActiveMQ documentation.

Sample ActiveMQ SSL configuration

The following is an example of how you might configure SSL for ActiveMQ.

1. Copy **keystore.jks** and **truststore.jks** into the **<Apache ActiveMQ installation directory>/conf** folder.
2. Open the **<Apache ActiveMQ installation directory>/conf/activemq.xml** file and add the following lines:

```
<transportConnectors>
  ...
  <transportConnector name="ssl"
uri="ssl://0.0.0.0:61617?trace=true&edClientAuth=true"/>
  ...
</transportConnectors>
<sslContext>
  <sslContext keyStore="file:${activemq.base}/conf/keystore.jks"
keyStorePassword="YourKeyStorePassword"
trustStore="file:${activemq.base}/conf/truststore.jks"
trustStorePassword="YourTrustStorePassword" />
</sslContext>
```

3. Change keystore and truststore passwords accordingly.
4. Restart ActiveMQ.

JDBC configuration

Please read the [Configuring database connections](#) topic.

Windows certificates import

For the Windows certificates installation procedure please see the [Windows certificates](#) topic.

Framework configuration

Configuration Server

Configure the auto-upgrade port as described in [Securing core framework connections](#) topic.

Interaction Server, UCS, Message Server

Configure secured ports as described [here](#).

Host configuration

1. Open **GAX -> Hosts -> <your_host> ->** and fill the certificate fields with your PEM certificate files.

The screenshot shows the GAX Configuration page with the 'Configuration' tab selected. The breadcrumb trail is 'Home > Hosts > Hosts > [Host Name] Properties'. The 'General' tab is active, showing various configuration fields:

- Name ***: [Redacted]_int.genesyslab.com
- IP Address**: [Empty field]
- OS Type ***: RedHat Enterprise Linux AS/Intel (dropdown)
- Version**: 1
- LCA Port ***: 4999
- Solution Control Server**: scs
- Certificate**: /genesys/TLS/02_[Redacted]_cert.pem
- Certificate Description**: [Empty field]
- Certificate Key**: /genesys/TLS/02_[Redacted]_priv_key.pem
- Trusted CA**: /genesys/TLS/ca_cert.pem
- Tenant**: Environment
- State Enabled**: ☒

2. Open the **Options** tab and add the following options:

- **[security]/tls** = true
- **[security]/mutual-tls** = true

The screenshot shows the GAX Configuration page with the 'Options' tab selected. The breadcrumb trail is 'Home > Hosts > Hosts > [Host Name] Properties'. The 'Options' tab is active, showing a table of configuration options:

Name	Section	Key	Value
conf			
security			
security \ certificate	security	certificate	/genesys/TLS/02_[Redacted]_cert.pem
security \ certificate-key	security	certificate-key	/genesys/TLS/02_[Redacted]_priv_key.pem
security \ trusted-ca	security	trusted-ca	/genesys/TLS/ca_cert.pem
security \ tls	security	tls	true
security \ mutual-tls	security	mutual-tls	true

Troubleshooting

If you start receiving ESP Server is not connected interaction errors and tasks, do the following:

1. Go to the ErrorHeld queue, add the `tls=1` transport parameter to the connection between Interaction Server and GRE or the GRE cluster application and GRE nodes.
2. Add the `tls=1` transport parameter to the connection between Interaction Server and Universal Contact Server.