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.

# Genesys Security Deployment Guide

## Securing Application Protocol Connections

5/7/2025

# Contents

# Securing Application Protocol Connections

This topic describes how to secure connections between components that connect via a specific protocol.

## Securing Connections Between Distributed Solution Control Servers

To have secure connections between Solution Control Servers in Distributed mode, the connections between all of the Solution Control Servers must be secured. To accomplish this, on each SCS in the distributed configuration, secure the port to which the other distributed servers connect.

Refer to Configuring TLS on Other Genesys Servers for details about how to secure connections between Solution Control Servers.

## Session Initiation Protocol (SIP)

To secure connections using SIP, refer to the Genesys SIP Server Deployment Guide.

## Other Protocols

To secure connections with components using protocols in this section or otherwise described in this document, refer to the Deployment Guide for the appropriate component.

### Configuring Secure Connections to Java/PSDK-Based Applications

Secure connections to Java/PSDK-based applications (such as Universal Contact Server) running on UNIX are configured in the same way as described in Other Genesys Servers, with one exception:

- If you are running Java/PSDK-based applications on the same host as C++-based applications, do not use the host certificate to secure data exchange at the application or port level. Although both types of applications use a PEM file for their private key, the internal format differs—Java/PSDK uses PKCS#8 and C++ uses RSA. Instead, use the application's certificate to enable secure data exchange on all secure ports of that application.