Microsoft Skype for Business Deployment Guide

Transport Layer Security

4/4/2025

Transport Layer Security

Contents

> **Important**
>
> Beginning with version 9.0.000.03, TLS 1.2 is supported supported fully. The minimum security protocol level is configurable and TLS 1.1 and earlier protocols are disabled by default.

T-Server supports the standard Transport Layer Security (TLS) Protocol, which offers confidentiality, integrity protection, and data compression to client/server applications. T-Server also supports TLS connections with Management Framework, T-Library clients, and between internal T-Server components (T-Server and UCMA Connector). Any matching TLS certificates can be used for secure connection (not just produced by Genesys). For a detailed description of how the TLS protocol works, see the relevant RFCs:

- RFC 5246—The Transport Layer Security (TLS) Protocol
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)

You can also find a more general description of TLS and how Genesys uses the protocol in the *Genesys Security Deployment Guide*.

> **Important**
>
> When creating the secure port that will be used for High Availability in the Primary and Backup T-Server applications, make sure that in the **Connection Protocol** box the value addp is provided—High Availability via TLS will only work when the Connection Protocol is addp.

Configuring TLS Between T-Server and Connector

From release 9.0, the Connector is fully integrated with Genesys configuration layer and a secure connection can be configured between Connector and T-Server by configuring the Connector port as secure. For more information on configuring secure connections between Genesys components, please see the Secure Connections (TLS) page of the *Genesys Security Deployment Guide*.