Microsoft Skype for Business Deployment Guide

Transport Layer Security

5/3/2025

Transport Layer Security

Contents

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*.

Configuring TLS Between T-Server and Connector

Configuring the TLS Connection for the Connector

The UCMA Connector supports two different ways of configuring TLS connection:

- The value of the certificate thumbprint, or its *friendly* name can be configured in the **[startupOptions]** section of the connector's configuration file. For example:

```
<startupOptions>
   <add key="connectorCertificate" value="416af925efade88309cdf203813e1e3b19f6"/>
     </startupOptions>
```

- The value of certificate thumbprint, or its *friendly* name can be provided in the command line. The command line option name is **–connectorCertificate**. For example:

```
Mslync_connector.exe –connectorCertificate "416af925efade88309cdf203813e1e3b19f6"
```

> **Important**
>
> The option in the command line takes precedence over the value set in the configuration file.

Configuring the TLS Connection for T-Server

T-Server uses the Application-level conn-certificate option for configuring the secure connection. The value of the option is used each time T-Server performs a connection to any connector. In the **[TServer]** section of the T-Server Application object, set the **conn-certificate** option to a valid thumbprint—for example, `416af925efade88309cdf203813e1e3b19f6c283`, or `6a f9 25 ef ad e8 83 09 cd f2 03 81 3e 1e 3b 19 f6 c2 83`.

Note that you can provide two formats for the thumbprint. As shown in the above example, both

forms are acceptable as long as the value corresponds to the thumbprint of a valid certificate available in the Certificate store. The spaces are for convenience.