T-Server for Cisco UCM Deployment Guide

TLS Support

4/9/2025

TLS Support

Contents

CTI-level communication between T-Server and the Genesys Java Telephony API (JTAPI) process and the Cisco CTIManager can now be encrypted. Communication between T-Server and the Cisco CTIManager can traverse multiple network paths. Each link within T-Server communicates over a TCP connection to a Genesys JTAPI process and each JTAPI process communicates over a TCP connection to the Cisco CTIManager. Because T-Server for Cisco UCM supports multiple links, the number of network paths (CTI/TCP connections) is twice that of the number of links (2 links - 4 TCP connections, 3 links - 6 TCP connections).

This feature enables secure communication over TCP sockets originating and terminating between the JTAPI process and the Cisco CTIManager. JTAPI provides the necessary functionality required to provide two-way authentication and secure communication between JTAPI and Cisco CTIManager. This functionality is dependent on client server certificates, and is out of scope of this document.

Securing communication with JTAPI

Securing communication with JTAPI requires communication to:

1. Cisco TFTP server to obtain the trusted server certificate (using the `tls-tftp-host` and `tls-tftp-port` configuration options).
2. Cisco CAPF server to obtain the client certificates (using the `tls-capf-host` and `tls-capf-port` configuration options).

When T-Server starts, all required certificates are automatically downloaded by the Genesys JTAPI process and stored in the local folder specified by the `tls-cert-path` configuration option. These downloaded certificates are encrypted based on the password defined by the `password` option.

Each connection/link between JTAPI and CTIManager requires its own unique client certificate. To obtain a client certificate for a particular link, an authorization code and an instance ID are required. Two link-level options, `tls-auth-code` and `tls-instance-id`, represent the authorization code and the instance ID, respectively, for TLS-enabled configurations.

The authorization code is required only for the initial download of the client certificates.

The instance ID provides a method to associate a specific certificate with a specific link and is configured in the Cisco UCM database. There is a one-to-one relationship between a link and an instance ID. Using the same instance ID on different links simultaneously might cause the certificate to be invalidated by Cisco.

Note: The first initial download of the server certificate is considered trusted. For this reason, it is recommended that the initial T-Server run, after configuring TLS, be done in a secure network (environment).

Feature Configuration

To enable TLS communication:

1. Obtain the certificates.

1. Configure the following options in the **`link-tls`** section:
   - `password`
   - `tls-cert-path`
   - `tls-capf-host`
   - `tls-capf-port`
   - `tls-tftp-host`
   - `tls-tftp-port`
2. Configure the following options in the link section specified by the **`link-`*`n`*`-name`** option:
   - `tls-auth-code`
   - `tls-instance-id`
3. Start T-Server.
4. Check that certificates were obtained and are located in the directory specified in `tls-cert-path`.
5. Stop T-Server.
6. Remove the `tls-auth-code` option from the link section.

2. Run T-Server with the secure connection.

1. Ensure that the link section contains only the TLS-related option `tls-instance-id`.
2. Start T-Server.

To disable TLS communication, remove one or more of the mandatory TLS options.

Configuration Options

password

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: After restart

Specifies a passphrase used to encrypt the local key store for certificates.

tls-cert-path

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid local path

Changes Take Effect: After restart

Specifies the local directory path where certificates should be installed.

tls-capf-host

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid address
Changes Take Effect: After restart

Specifies the hostname or IP address of the Cisco UCM CAPF server. Defined by switch configuration.

tls-capf-port

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid port
Changes Take Effect: After restart

Specifies the port number on which the CAPF server is running. Defined by switch configuration (typically defaults to 3804).

tls-tftp-host

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: After restart

Specifies the hostname or IP address of the Cisco UCM TFTP server.

tls-tftp-port

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid port
Changes Take Effect: After restart

Specifies the port number on which the TFTP server is running. Defined by switch configuration (typically defaults to 69).

tls-instance-id

Section: Specified by `link-<n>-name`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: Immediately – changing this option will cause the link to drop and reconnect

Specifies the application instance ID, as configured on the switch side (Cisco UCM). Each TLS link requires a unique ID.

tls-auth-code

Section: Specified by `link-<n>-name`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: Immediately – changing this option will cause the link to drop and reconnect

Specifies the authorization string configured in Cisco UCM. This code is used only once for client certificate download.