GVP Documentation Supplement

CTIC TLS 1.2 Support

5/8/2025

Contents

CTIC TLS 1.2 Support

SUMMARY: Add TLS 1.2 Support information to the user guide.

DOCUMENT: The next publication of the GVP 8.5 User's Guide will include these revisions.

CHAPTER: Chapter 10: Configuring the CTI Connector

SECTION: CTI Connector TLS 1.2 Support

Add a new section title "CTI Connector TLS 1.2 Support", and add the following information to the section:

CTI Connector (CTIC) supports TLS 1.2 for connection with:

- IVRServer
- Resource Manager (RM)
- Configuration Server and Message Server

TLS 1.2 is not supported for connections with Cisco ICM and LCA.

CTIC TLS 1.2 for IVRServer

CTIC supports TLS 1.2 for IVRServer. To enable TLS, set the secured parameter to true in the “IServer_Sample” section. The following TLS parameters are configured in the “IServer_Sample” section:

- **certificate**=[cert path and filename]—This parameter is mandatory for using TLS, and it denotes the path and the filename of the TLS certificate to be used.
- **key**=[key path and filename]—This denotes the path and the filename of the TLS key to be used.
- **type**=[Type of secure transport]—This denotes the type of secure transport to be used. The value can be TLSv1_2, TLSv1_1, or TLSv1. The default is TLSv1_2.
- **password**=[password]—This denotes the password associated with the certificate and key pair, and is required only if the key file is password protected.
- **cafile**=[CA cert path and filename]—This denotes the path and the filename of the certificate to be used for verifying the peer (IVRServer).
- **verifypeer**=true—This parameter turns on peer certificate verification. When enabled, CTIC verifies the IVRServer certificate with the ca certificate configured in the cafile parameter. If peer certificate verification fails, connection is not made with the IVRServer.
- **verifydepth**=[max depth for the certificate chain verification]—This parameter is applicable only to peer certificate authentication, and sets the maximum depth for the certificate chain verification.
- **Secured** = [Boolean true/false] When this parameter is set to `true`, TLS is enabled for CTIC-IVR connection. Setting this parameter to `false` disables TLS.

CTIC TLS 1.2 for RM

CTIC supports SIP over a secured transport layer from RM. CTIC supports TLSv1.2.

Example:

sip.transport2 tls:any:5081 cert=$InstallationRoot$/config/GEN-C8-232.pem key=$InstallationRoot$/config/GEN-C8-232_key.pem type=TLSv1_2 cafile=$InstallationRoot$/config/cert_authority.pem

`sip.transport.<n>`—This parameter defines how TLS is enabled in the SIP stack.

`type:ip:port`

where:

- **type** must be set to tls.
- **ip** is the IP address of the network interface that accepts incoming SIP messages. If ip is an IPv6 address, [] must be used. For example:
- To define a transport to listen to all IPv4 interfaces, set the value of ip to any or any4.
- To define a transport to listen to all IPv6 interfaces, set the value of ip to [any6].
- port is the port number where the SIP stack accepts incoming SIP messages.

`[parameters]` defines SIPS-TLS transport parameters. For example:

- **cert**=[cert path and filename]—This parameter is applicable to SIPS only and mandatory if using SIPS, and denotes the path and the filename of the TLS certificate to be used.
- **key**=[key path and filename]—This parameter is applicable to SIPS only and mandatory if using SIPS, and denotes the path and the filename of the TLS key to be used.
- **type**=[Type of secure transport]—This parameter is applicable to SIPS only and is optional. This denotes the type of secure transport to be used and the value can be TLSv1_2, TLSv1_1, TLSv1, SSLv3, or SSLv23. Default is TLSv1_2.
- **password**=[password]—This is applicable to SIPS only and is optional, and denotes the password associated with the certificate and key pair. This is required only if key file is password protected.
- **cafile**=[CA cert path and filename]—Mandatory for TLS mutual authentication. This denotes the path and the filename of the certificate to be used for verifying the peer.
- **verifypeer**=true—This parameter is mandatory for TLS mutual authentication, and turns on the TLS mutual authentication.
- **verifydepth**=[max depth for the certificate chain verification]—This parameter is applicable only to TLS mutual authentication, and sets the maximum depth for the certificate chain verification. For the default Genesys certificate provided, the recommended value is 1.

CTIC TLS 1.2 for Configuration Server and Message Server

CTIC supports TLS connection to Configuration Server and Message Server through secure ports exposed by Configuration Server.