GVP Documentation Supplement

Remove support for SSLv2

5/6/2025

Remove support for SSLv2

SUMMARY: Remove support for SSL v2.

The next publication of the Genesys Media Server 8.5 Deployment Guide will include this revision:

CHAPTER: Appendix A: Deploying the T-Server-CUCM to Media Server Connector
SECTION: Secure Communications
CHANGE TO MAKE
Two changes:
1). On page 21, remove SSL v2.
2). On page 133, add the following section "Secure Communications" before the section "Supported Media Operations".

Secure Communications
UCMC supports the following protocols for secure SIP communications:

- Secure SIP (SIPS) — SIP over the Transport Layer Security (TLS) protocol for media service requisition between UCMC and Resource Manager.
- Non-secure SIP — SIP over User Datagram Protocol (UDP) and Transport Control Protocol (TCP) for media service request messaging between UCMC and Resource Manager.
- Secure Socket Layer (SSL) — SSL version 3 (SSL v3), SSL version 23 (SSL v23), TLS v1, TLS v1.1, and TLS v1.2.

Note: SSL version 2 (SSL v2) is no longer supported.

Key and Certificate Authentication (this is sub section of **Secure Communications**)
UCMC ships with a generic private key and SSL certificate. Default SIP transports for TLS are configured in the UCMC Application object. Therefore, basic security is implemented without having to configure it.

For more stringent security, UCMC 8.1.5 and above supports using the attributes of the **sip.transport.configuration** option to configure a password for key and certificate authority to perform server authentication.

Note: password=[password] Applicable to SIPS only and is optional. The password is associated with the certificate and key pair, and is required only if the key file is password protected.

For more information about obtaining SSL keys and certificates, and configuring UCMC to use SIPS in your deployment, see the section on enabling secure communications in the GVP 8.5 User's Guide.