Genesys Security Deployment Guide

Certificate Generation and Installation

12/20/2025

Certificate Generation and Installation

This chapter provides an overview of the process of certificate generation using the open source OpenSSL tool and Windows Certificate Services, and how to manage those certificates on a Windows platform using Microsoft Management Console (MMC).

Keep in mind that the actual process of certificate generation in a specific environment is highly dependent on the security policies of your IT organization and tools used, and can, therefore, be different from the process described in this chapter. Genesys recommends that you consult with your network administrator before generating certificates for secure data exchange between Genesys components.

Important

- Although you can use OpenSSL to generate certificates on both UNIX and Windows, Windows Certificate Services is available only on the Windows Server operating system. Nevertheless, the certificates generated by both methods can be used for secure data exchange between applications that run on both Windows and UNIX operating systems.
- Genesys recommends that you use OpenSSL if you intend to run any applications that might require secure connections on UNIX. If you intend to run all your applications on Windows, Windows Certificate Services is recommended.
- When configuring simple TLS, certificates are optional for Genesys 8.x client applications.
- The security certificates used in Genesys TLS must be valid and compatible with (acceptable to) OpenSSL.