Genesys Security Deployment Guide

Federal Information Processing Standards (FIPS)

4/15/2025

Contents

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards, also known as FIPS, are a set of standards created by the United States federal government for use in computer systems of non-military government agencies and their contractors. They are concerned primarily with interoperability of different systems, portability of data and software, and computer security.

A FIPS standard is developed only when there are no voluntary standards in existence to address federal requirements. In some cases, the standards are modified and updated restatements of technical standards already in use, such as those of the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO).

Generally speaking, the Genesys implementation of TLS is considered to be consistent with FIPS 140-2, based on FIPS capabilities of the underlying libraries.

Supporting Components

The following Genesys components support data security using FIPS:

- Management Framework (except on Apple OS)
- Genesys Security Pack on UNIX
- Workforce Management
- Network T-Servers
- Media T-Servers
- Performance Manager Advisors CCA-ME
- eServices (partial)
- Composer (except on connections to/from the Web Request Block)
- Genesys Rules System
- Outbound Contact
- intelligent Workload Distribution (iWD)
- Interaction Concentrator
- Genesys Info Mart
- Workspace Desktop Edition
- Orchestration Server
- Platform SDK

Genesys Voice Platform

Genesys Voice Platform (GVP) components support data security using FIPS, but some GVP components will require an additional step to enable it. These components use the security library directly and require the additional configuration option **FIPS Mode Enabled** to control their usage. Refer to the *Genesys Voice Platform User's Guide* for more information.

Enabling FIPS in your Environment

Enabling FIPS depends on the operating system that is running in your environment, as follows:

Windows

> **Important**
> FIPS is disabled by default

To set up a FIPS-compliant set of ciphers to be used on Windows, configure the operating system as described in Windows documentation at: http://support.microsoft.com/kb/811833

Then, to enable or disable FIPS, set the following registry variable to `1` (enable) or `0` (disable), as appropriate:

- On Windows 2012 and Windows 8:
  HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy
- On Windows 2008, Windows Vista, and Windows 7:
  HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled

UNIX or Linux

Starting in release 8.1.1, the Genesys Security Pack contains both the original non-FIPS and FIPS-consistent shared libraries. To specify which library to use (FIPS or non-FIPS), set the given environment variables (and related variables) to the location of the library (**<install directory>**) to be used, as follows:

- To use the FIPS library, do one of the following, as appropriate:
  - On AIX platforms, set both the LD_LIBRARY_PATH and LIB_PATH environment variables to either:
    - **<install directory>/fips140_lib32** (for 32-bit libraries)

      or

    - **<install directory>/fips140_lib64** (for 64-bit libraries)
  - On Solaris 64-bit platforms, set both the LD_LIBRARY_PATH and LD_LIBRARY_PATH_64 environment variables to **<install directory>/fips140_lib64**.
  - On Linux platforms that use the Genesys Security Pack version 8.5.100.30 or later, use the following procedure. For Linux with Genesys Security Pack versions prior to 8.5.100.30, use the regular configuration(s) specified in the later section of this page.
    - Run the `fipsinstall.sh` script provided in the **fips140_lib64** directory. This runs the FIPS module self-test and generates proper OpenSSL configuration files which are mandatory for using the FIPS module.
    - Set both the LD_LIBRARY_PATH and OPENSSL_MODULES environment variables to **<install directory>/fips140_lib64** and OPENSSL_CONF variable to **<install directory>/fips140_lib64/openssl.cnf**.

    Note: The master OpenSSL configuration file (**openssl.cnf**) configured in **OPENSSL_CONF** is not included in the installation package but it is generated dynamically by the **fipsinstall.sh** script along with the **fipsmodule.cnf** configuration for FIPS.
  - On all other platforms (including Linux with Genesys Security Pack version prior to 8.5.100.30), set only the LD_LIBRARY_PATH environment variable to **<install directory>/fips140_lib32** (for 32-bit libraries) or **<install directory>/fips140_lib64** (for 64-bit libraries).
- To use the non-FIPS library, set the LD_LIBRARY_PATH environment variable to **<install directory>**.

Platform SDK for .NET

To enable FIPS in an application built using Platform SDK for .NET, use the same procedure as you do for configuring the common library for IIRC.

Platform SDK for Java

To enable FIPS in a Genesys Java environment, you must set up the Java Runtime Environment (JRE) to be compliant with FIPS, as described in the Platform SDK Java documentation.

To configure a FIPS-enabled service-provider, refer to Platform SDK FIPS documentation.