



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Genesys Voice Platform

[https Section](#)

## https Section

- [https.certificate.algorithm](#)
- [https.client.authentication](#)
- [https.connector.type](#)
- [https.keystore.path](#)
- [https.keystore.type](#)
- [https.protocol](#)
- [https.random.algorithm](#)
- [https.security.provider](#)
- [password](#)

### https.certificate.algorithm

**Default Value:** SunX509

**Valid Values:** Name of HTTPS algorithm

**Changes Take Effect:** at start/restart

The SSL algorithm used for the configured keystore.

### https.client.authentication

**Default Value:** none

**Valid Values:**  
**none**

No certificate request, so client-side authentication is disabled.

**required**

A certificate is requested and the server will require a valid, non-empty certificate response to establish the connection. (Only works for BIO connector type).

**preferred**

A certificate is requested, but the server will still establish the connection if the certificate response is empty.

**Changes Take Effect:** at start/restart

HTTPS client authentication requirements.

## https.connector.type

**Default Value:** 2

**Valid Values:**

**NIO**

Non-blocking NIO connector (Refer to Jetty's JavaDoc for class `org.mortbay.jetty.security.SslSelectChannelConnector` for more information).

**BIO**

Blocking BIO connector (Refer to Jetty's JavaDoc for class `org.mortbay.jetty.security.SslSocketConnector` for more information).

**Changes Take Effect:** at start/restart

The type of Jetty connector to use

## https.keystore.path

**Default Value:** `${user.home}/.keystore`

**Valid Values:** A directory path

**Changes Take Effect:** at start/restart

The path to the keystore file, which will be used for all the HTTPS connectors.

## https.keystore.type

**Default Value:** JKS

**Valid Values:** A HTTPS keystore type

**Changes Take Effect:** at start/restart

The type of keystore, which defines the file format that the security implementation supports.

## https.protocol

**Default Value:** TLS

**Valid Values:**

## **SSL**

Supports some version of SSL.

## **SSLv2**

Supports SSL version 2 or higher.

## **SSLv3**

Supports SSL version 3; may support other versions.

## **TLS**

Supports some versions of TLS.

## **TLSv1**

Supports TLS version 1; may support other versions.

**Changes Take Effect:** at start/restart

The cryptographic protocol to use.

## https.random.algorithm

**Default Value:**

**Valid Values:** Name of the RNG (Random Number Generator) algorithm

**Changes Take Effect:** at start/restart

Refer to the JDK JavaDoc for class `java.security.SecureRandom` for more information.

## https.security.provider

**Default Value:**

**Valid Values:** Name of Java security provider

**Changes Take Effect:** at start/restart

Refer to the JDK JavaDoc for class `java.security.Provider` for more information.

## password

**Default Value:**

**Valid Values:** A string

**Changes Take Effect:** at start/restart

The password for the keystore file.