SIP Feature Server Deployment Guide

TLS Configuration

4/3/2026

Contents

TLS Configuration

Create Certificate and Keystores

Create Java truststore and keystore objects in the path: **<SIP Feature Server installed directory>/etc**.

- Your keystore typically contains certificates that Feature Server uses on its listening port(s) along with the private key.
- Your truststore might contain additional trusted certificate authorities required by Feature Server to validate certificates when connecting to remote servers via TLS.

Follow the documentation instructions of your operating system and Java version that you use in your environment to make your keystore and truststore.

The following example command allows you to create a **pks12 keystore** using certificates and keys in the **pem** format that will hold self-signed certificate and a key, and protected by **password** string using the Java keytool and OpenSSL executables on the Linux platform:

```
cat ../certs/priv_key.pem ../certs/cert.pem ../certs/ca.pem >certstore.pem
openssl pkcs12 -export -in certstore.pem -name 'fs-selfsigned' -noiter -nomaciter -out
keystore.pkcs12 -passout pass:password || { echo "failed cert  conversion to pkcs12
keystore"; extit 1; }
keytool -list -keystore keystore.pkcs12 -storepass password
```

Enable SIP Feature Server secure listening ports

SIP Feature Server uses Jetty application server internally to manage HTTP/HTTPS interface with other Genesys applications. This section describes steps to configure the underlying Jetty server to use the TLS listening port.

> **Important**
>
> SIP Feature Server's Dial plan module listening port does not support secure mode.

HTTPS configuration

This section provides information on HTTPS configuration. The HTTPS configuration settings such as settings in **start.ini**, **TrustStore and keystore configuration paths**, and **Generate obfuscated passwords** differ for SIP Feature Server 8.1.204 and earlier versions. These changes are noted in the headers of respective sections.

Configuration of start.ini for SIP Feature Server 8.1.204 and later

Remove the '#' symbol in the **start.ini** file to enable the HTTPS and SSL parameters listed as follows:

- Enable HTTPS module
  `--modules=https`
- Enable SSL module
  `--modules=ssl`
- Configure https port
  `jetty.ssl.port=8443`
- Configure HTTPS idle timeout
  `jetty.ssl.idleTimeout=30000`

Configuration of start.ini for SIP Feature Server 8.1.203 and earlier

Remove the '#' symbol or add the following lines to the end of the **start.ini** file to enable the HTTPS and SSL parameters:

- Enable HTTPS module
  `--module=https`
- Configure https port
  `https.port=8443`
- Configure HTTPS idle timeout
  `https.timeout=30000`
- Enable SSL module
  `--module=ssl`

Configuration of jetty-ssl-context.xml

In the **jetty-ssl-context.xml** file, you can configure protocols acceptable by Feature Server on its HTTPS port, for example:

```
<Set name="IncludeProtocols">
  <Array type="java.lang.String">
    <Item>TLSv1.2</Item>
  </Array>
</Set>
<Set name="ExcludeProtocols">
  <Array type="java.lang.String">
    <Item>TLSv1.1</Item>
    <Item>SSLv3</Item>
  </Array>
</Set>
```

> **Important**
>
> When TLS is enabled in SIP Feature Server, configure the SIP Feature Server host

certificates in the GAX truststore.

Truststore and keystore configuration paths for SIP Feature Server 8.1.204 and later

Jetty defines main configuration rules for truststore and keystore paths in the **jetty-ssl-context.xml** file. By default, it defines the path as relative to **<FS Installation directory>**. The default values of Truststore and Keystore path parameters in **jetty-ssl-context.xml** are as follows:

- ```
  <Set name="KeyStorePath">
    <Call name="resolvePath" class="org.eclipse.jetty.xml.XmlConfiguration">
      <Arg><Property name="jetty.base" default="."/></Arg>
      <Arg><Property name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
  default="etc/keystore" /></Arg>
    </Call>
  </Set>
  ```

- ```
  <Set name="TrustStorePath">
    <Call name="resolvePath" class="org.eclipse.jetty.xml.XmlConfiguration">
      <Arg><Property name="jetty.base" default="."/></Arg>
      <Arg><Property name="jetty.sslContext.trustStorePath"
  deprecated="jetty.sslContext.trustStoreAbsolutePath,jetty.truststore" default="etc/
  keystore"/></Arg>
    </Call>
  </Set>
  ```

You can define absolute paths in **start.ini** by using **jetty.sslContext.keyStorePath** and **jetty.sslContext.trustStorePath** variables. In this case, the **jetty-ssl-context.xml** file must be modified as follows:

- `<Set name="KeyStorePath"><Property name="jetty.sslContext.keyStorePath"/></Set>`
- `<Set name="TrustStorePath"><Property name="jetty.sslContext.trustStorePath"/></Set>`

Important

The keystore file must not be removed from the **<FS Installation directory>/etc/** folder.

Configuring the following keystore and truststore configuration in the **start.ini** file will override the configuration in the **jetty-ssl-context.xml** file.

- Setup path to keystore (relative to **<FS Installation directory>** by default):

  ```
  jetty.sslContext.keyStorePath=etc/keystore
  ```

- Setup path truststore (relative to **<FS Installation directory>** by default):

```
jetty.sslContext.keyStorePassword=OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4
```

- Set the obfuscated passwords for keystore (For more details, see the **Generate Obfuscated passwords** topic in this section.):

```
jetty.sslContext.keyStorePassword=OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4
jetty.sslContext.keyManagerPassword=OBF:1u2u1wml1z7s1z7a1wnl1u2g
jetty.sslContext.trustStorePassword=OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4
```

Truststore and keystore configuration paths for SIP Feature Server 8.1.203 and earlier

Jetty defines main configuration rules for truststore and keystore paths in the **jetty-ssl-context.xml** file. By default, it defines the path as relative to <FS Installation directory>. The default values of Truststore and Keystore path parameters in **jetty-ssl-context.xml** are as follows:

- <Set name="KeyStorePath"><Property name="jetty.base" default="." />/<Property name="jetty.keystore" default="etc/keystore"/></Set>
- <Set name="TrustStorePath"><Property name="jetty.base" default="." />/<Property name="jetty.truststore" default="etc/keystore"/></Set>

You can define absolute paths in start.ini by using "jetty.keystore" and "jetty.truststore" variables. In this case, jetty-ssl-context.xml file must be modified as follows:

- <Set name="KeyStorePath"><Property name="jetty.keystore"/></Set>
- <Set name="TrustStorePath"><Property name="jetty.truststore"/></Set>

> **Important**
>
> The keystore file must not be removed from the <FS Installation directory>/etc/ folder.

Configuring the following keystore and truststore configuration in the **start.ini** file will override the configuration in the **jetty-ssl-context.xml** file.

- Setup path to keystore (relative to <FS Installation directory> by default):
  ```
  jetty.keystore=etc/keystore
  ```
- Setup path truststore (relative to <FS Installation directory> by default):
  ```
  jetty.truststore=etc/keystore
  ```
- Set the obfuscated passwords for keystore (For more details, see **Generate Obfuscated passwords** topic in this section.):
  ```
  jetty.keystore.password=OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4

  jetty.keymanager.password=OBF:1u2u1wml1z7s1z7a1wnl1u2g

  jetty.truststore.password=OBF:1vny1zlo1x8e1vnw1vn61x8g1zlu1vn4
  ```

Generate obfuscated passwords for SIP Feature Server 8.1.204 and later

1. Navigate to <FS Installation directory> in Linux Shell or Windows Command prompt.

2. Run the following command to run the Jetty's password utility to obfuscate your passwords:
```
java -cp lib/jetty-http-xxx.jar:lib/jetty-util-
xxx.jar org.eclipse.jetty.util.security.Password your_Password
```

- Where -xxx signifies the version of Jetty that you have installed.
- On Linux, use a colon (:) instead of a semi-colon (;) to separate the two JAR names.

For example:
```
{FS Installation directory}>java -cp lib/jetty-http-12.0.8.jar;lib/jetty-
util-12.0.8.jar org.eclipse.jetty.util.security.Password 123456 123456
OBF:19iy19j019j219j419j619j8
MD5:e10adc3949ba59abbe56e057f20f883e
```

Generate obfuscated passwords for SIP Feature Server 8.1.203 and earlier

1. Navigate to <FS Installation directory> in Linux Shell or Windows Command prompt.
2. Run the following command to run the Jetty's password utility to obfuscate your passwords:
```
java -cp lib/jetty-http-xxx.jar:lib/jetty-util-
xxx.jar org.eclipse.jetty.util.security.Password your_Password
```

- Where -xxx signifies the version of Jetty that you have installed.
- On Linux, use a colon (:) instead of a semi-colon (;) to separate the two JAR names.

For example:
```
{FS Installation directory}>java -cp lib/jetty-http-9.2.10.v20150310.jar;lib/
jetty-util-9.2.10.v20150310.jar org.eclipse.jetty.http.security.Password 123456
123456
OBF:19iy19j019j219j419j619j8
MD5:e10adc3949ba59abbe56e057f20f883e
```

Configuration of jetty-ssl.xml

In order for the HTTPS connection to select the port as per the configuration, enable the following configuration in the **jetty-ssl.xml** file:

```
<Set name="host"><Property name="jetty.ssl.host" deprecated="jetty.host" /></Set>
<Set name="port"><Property name="jetty.ssl.port" deprecated="ssl.port" default="8443" /></Set>
```

Configuration of TLS connections to backend servers

If you want SIP Feature Server to make secure connections with Genesys backend servers (such as Configuration Server and SIP Server), make sure you configure the following:

- In the **<SIP Feature Server installed directory>/launcher.xml** file (or **launcher_64.xml** for Linux), set the parameter **ssl_encryption** (com.genesyslab.voicemail.application.encryption) to `true`. If you use this option then ensure that Feature Server application object is configured with connections to other Genesys backend servers pointing to their secure ports.
- You can future limit TLS handshake protocol, used by Feature Server, when communicating with remote

servers, by specifying the parameter **ssl_versions** (jdk.tls.client.protocols) with the value of protocol in the **<SIP Feature Server installed directory>/launcher.xml** file (or **launcher_64.xml** for Linux). For example, you can set the value as TLSv1.2. **Note:** Genesys does not recommend you to force specific handshake protocol. You can rely on auto-negotiation of TLS protocol that will select highest possible version of transport layer protocol between Feature Server and remote backend server(s).

- In the **<SIP Feature Server installed directory>/launcher.xml** file (or **launcher_64.xml** file for Linux), configure keystore type(s), path(s), and passwords (if in use) prepared as described in Create certificate and key stores. Use the following parameters to configure these values:
  - **cert_store_file**
  - **cert_store_type**
  - **key_store_file**
  - **key_store_type**