Genesys Rules System Deployment Guide

Configuring GRS for Secure Sockets Layer (SSL)

5/1/2025

Contents

- 1 Configuring GRS for Secure Sockets Layer (SSL)
  - 1.1 Introduction
  - 1.2 Setting up GRAT in SSL Mode
  - 1.3 Setting up GRE in SSL mode

Configuring GRS for Secure Sockets Layer (SSL)

Introduction

Purpose

This topic describes how set to up GRAT and/or GRE in SSL (Secure Sockets Layer) mode using the Java *Keytool* utility which should be available if Java is installed. In these steps, Keytool is used to generate the self-signed certificate and update Java's keystore to add the certificate. The browser is used to download the public certificate.

Supported Configurations

Supported configurations are:

- GRAT in SSL mode and GRE in non-SSL mode
- GRAT in non-SSL mode and GRE in SSL mode
- Both GRAT and GRE in SSL mode

Changes in GRE's Communication Port in Configuration

- Make sure the correct SSL communication port is provided. In Tomcat, by default, 8080 is a non-SSL port and 8443 is for SSL.
- The value for the Connection Protocol in the GRE Port must remain as `http` (**NOT** to be changed to `https`).
- The listening mode must be set to `Secured`.

Setting up GRAT in SSL Mode

> **Important**
>
> The steps here demonstrate how to create a self-signed certificate and use it for SSL. For security reasons, it is very important that you consult your organization's IT Security Administrator to check whether you must use a certificate signed by an external CA (Certificate Authority) like VeriSign or Thawte.

1. **[+] Create the Certificate if it is not already available.**

   On GRAT, use Keytool utility to create a self-signed certificate to be used for SSL.

   ```
   keytool -genkey -alias <alias name> -keyalg <security key algorithm> -validity 360
   ```

   > **Important**
   >
   > When prompted for input `What is your first and last name?`, enter the name of GRAT's Host object in Configuration Server. It must be either GRAT's hostname or the IP address. The value entered here is used in the commonName (CN) property of the certificate.

   For example:

   ```
   /usr/local/java/jdk1.7.0_79/jre/bin/keytool -genkey -alias linux-grat -keyalg RSA
   ```

   A self-signed certificate will be created by file name `.keystore` in the user's home directory. If the certificate must be signed by an external CA (Certificate Authority), a CSR needs to be created and submitted to the CA. You can use Keytool to create a CSR. Please see Java documentation for a complete list of Keytool options.

2. **[+] Enable SSL in the server configuration by using the Certificate and disable non-SSL mode.**

   For example, to enable SSL in the case of Tomcat, the SSL configuration in `.../[TOMCAT_HOME]/conf/server.xml` looks like this:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
   ```

```
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="/home/certificates/.keystore" keystorePass="changeit"/>
```

Where:

- `keystoreFile` is the path to the certificate file generated in step 1.
- `keystorePass` is the password created for the certificate in step 1.

3. **[+] On the GRE machine, get the public certificate of GRAT.**
   a. Open GRAT's link `https://[ GRAT IP address]:[SSL port number]/genesys-rules-authoring/index.jsp` in your browser.
   b. When it shows the warning about certificates, accept the certificate to be added in the browser's Trusted Certificates list.
   c. Once the certificate has been downloaded by the browser, export it using the browser's export certificate feature.

<toggledisplay linkstyle font-size:larger showtext="[+] BROWSER DETAILS" hidetext="[-] BROWSER DETAILS">

Browser	Procedure
IE 11	1. When the GRAT application is open in Internet Explorer using HTTPS, click the **Lock** icon in the address bar. (It is located beside the refresh icon on the right side in the address bar.) 2. Navigate to the **View Certificates link > Details** tab. 3. Click the **Copy to File...** button. 4. Select the format `DER encoded binary X.509 (.CER)` and click **Next**. 5. Enter the file name into which you want to save the certificate. Click **Next**, then **Finish**. OR 1. Navigate to **Internet Options > Content > Certificates**. 2. Locate the certificate. 3. Select the certificate and export it selecting `DER encoded binary X.509 (.CER)` format from the three format choices.

Browser	Procedure
Firefox 40.02	1. When the GRAT application is open in Firefox using HTTPS, click the **Lock** icon in the address bar. (It is located just before "https") 2. Click **More information...**. 3. Navigate to the **Security Tab > View Certificate button > Details Tab**. 4. Click the **Export...** button. OR 1. Navigate to **Options > Advanced > Certificates**. 2. Locate the certificate. 3. Select the certificate and export it.
Chrome 44.0	1. When the GRAT application is open in Chrome using HTTPS, click the **Lock** icon in the address bar. (It is located just before "https"). 2. In the popup that opens, navigate to **Connection tab > Certificate information link > Details** tab. 3. Click **Copy to File...**. 4. In the Certificate Export Wizard, enter the file name to which you want to save the certificate. Click **Next**, then **Finish**. OR 1. Navigate to **Customize > Settings >**. 2. Enter `certificate` in **Search Settings** and press the enter key. 3. Click **Manage Certificates...**. 4. Locate the certificate.

Browser	Procedure
	5. Select the certificate and export it.

4. **[+] On the GRE machine, add the public certificate to Java Keystore using the Java Keytool.**

   ```
   keytool -import -alias <alias> -keystore <cacerts_file> -trustcacerts -file <certificate_filename>
   ```

   > **Important**
   > This will prompt for the Java Keystore password. The default password for Java Keystore is changeit

   For example:

   ```
   /usr/local/java/jdk1.7.0_79/jre/bin/keytool -import -alias linux-grat -keystore /usr/local/java/jdk1.7.0_79/jre/lib/security/cacerts
    -trustcacerts -file /home/certificates/linux-grat
   ```

   Where:

   - `alias` is the alias to be used for this certificate.
   - `keystore` is the path to Java's Keystore in which we want to add the certificate. Make sure to update the Keystore of Java that is used by the Server.
   - `file` is the path to the certificate file (exported in step 3) that we can to add into Java Keystore.

5. **As for GRE**, repeat step 3 and 4 for any other Java clients of GRAT which would need to use HTTPS to send requests to GRAT.

Setting up GRE in SSL mode

The procedure to set up GRE in SSL mode is similar to the procedure for GRAT. In step 3, use:

```
https://[ GRE IP address]:[SSL port number]/genesys-rules-engine/status.jsp
```

to get GRE's public certificate on the GRAT machine.

Similar to the steps above, where you added GRAT's public certificate to GRE's Java keystore, for GRE you need to add GRE's public certificate (exported from the browser) to GRAT's Java Keystore.