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 Rules System Deployment Guide

Installing GRAT

2/23/2025

Installing GRAT

Contents

Genesys Administrator

Genesys recommends that you configure the GRAT by using Genesys Administrator. If you use Genesys Administrator, you can deploy the installation package from within Genesys Administrator.

Configuration Manager

You can configure the GRAT by using Configuration Manager if you are using an older version of Configuration Server, prior to 8.0.2, where Roles are not supported. If you use Configuration Manager, you will have to:

1. **Create the applications**.
2. **Run the setup program manually**.

Non-English Environments

When operating the GRAT in a non-English environment, you will need to configure the **URIEncoding** option to properly operate and integrate with the Genesys Framework environment. By default, Tomcat uses ISO-8859-1 character encoding when decoding URLs received from a browser. If you wish to use characters not included in this character set, you will need to set the **URIEncoding** option to UTF-8 in the **server.xml** file on the Connector that is used for the Genesys Rules Authoring Tool.

For example:

```
<Connector connectionTimeout="20000" port="8080" protocol="HTTP/1.1" redirectPort="8443"
URIEncoding="UTF-8" useBodyEncodingForURI="true"/>
```

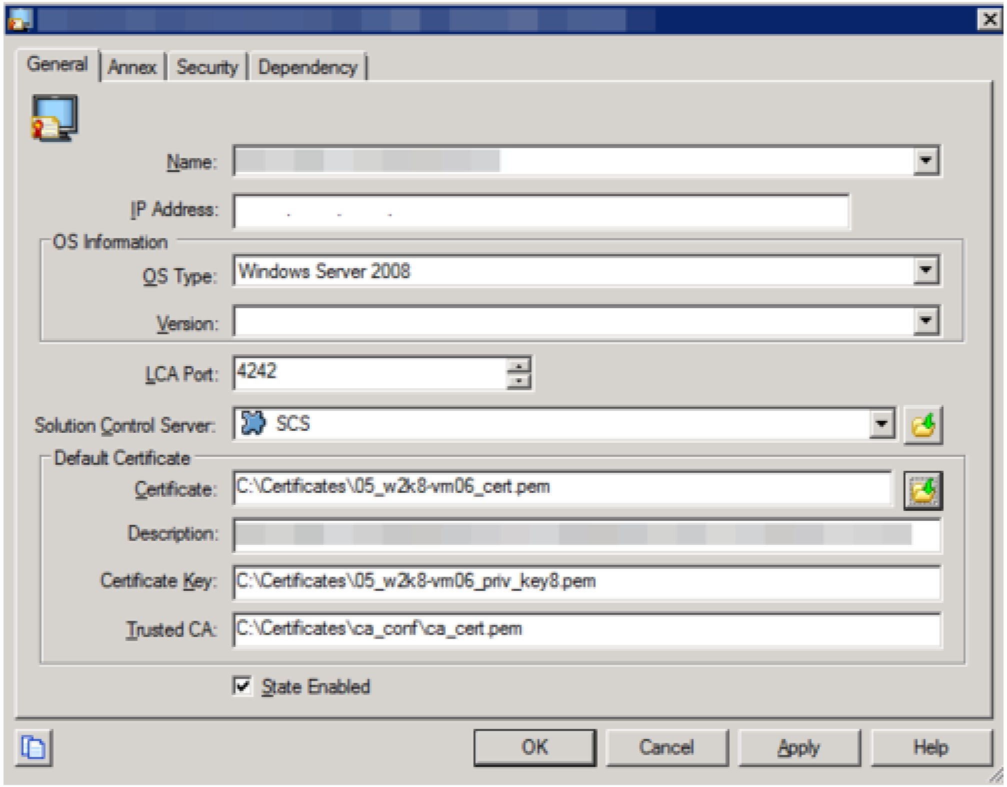
Security Certificates in Initial Release of 8.5.1

GRE and GRAT applications are unable to understand thumbprint certificates from the Windows Microsoft Certificate Store while connecting to Configuration Server or Message Server. Consequently they cannot establish a TLS connection to either Configuration Server or Message Server, and a security error is generated, such as this:

```
15:14:31.445 Alarm 21363 [ServerConnectionMonitor][Thread-2]: connect(): caught exception
while
opening connection to server '<GRAT/GREServerVersion>'. Nested exception: Could not configure
TLS.
```

Workaround

Create certificates in .PEM format and private-keys in PKCS#8 format—see the example below.



Name: [redacted]

IP Address: . . .

OS Information

OS Type: Windows Server 2008

Version:

LCA Port: 4242

Solution Control Server: SCS

Default Certificate

Certificate: C:\Certificates\05_w2k8-vm06_cert.pem

Description: [redacted]

Certificate Key: C:\Certificates\05_w2k8-vm06_priv_key8.pem

Trusted CA: C:\Certificates\ca_conf\ca_cert.pem

☑ State Enabled

Paths to the physical certificates can be configured either on the Application or the Connection level, but not on the Host level (despite this being a general Genesys recommendation). For Host level certificates, if GRAT and GRE are located on the same host as Configuration Server or Message Server or other C++ applications, the secured connection will not be established because C++ based applications do not accept PKCS#8 format.

You can convert private-key from PEM to PKCS#8 format using the following OpenSSL command:

```
openssl pkcs8 -topk8 –nocrypt -in tradfile.pem -out p8file.pem
```