GENESYS™

Web Services and Applications Deployment Guide

Password encryption

5/4/2025

Password encryption

For added security, consider encrypting your passwords in the **application.yaml** file.

The following table identifies which passwords can be encrypted and where you can find them in the **application.yaml** file:

File section	Settings
jetty > ssl	- keyStorePassword - keyManagerPassword - trustStorePassword
serverSettings	- opsUserPassword - cmePassword - jksPassword - webDAVPassword
serverSettings > samlSettings	- encryptionKeyPassword - signingKeyPassword - tlsKeyPassword
serverSettings > accountManagement > smtpServer	password
serverSettings > elasticSearchSettings > transportClient	- password - keyStorePassword - keyPassword
db	password
spring > data > redis	password

Procedure: Encrypting passwords

Start

1. Run the GWS application with the **--encrypt** parameter followed by the password you need to encrypt. For example:

   ```
   $ java -jar gws.jar --encrypt ops
   CRYPT:an03xPrxLAu9p==
   ```

   The GWS application only encrypts and prints the password. The server won't actually start.

2. Copy the printed encrypted password and paste into the **application.yaml** file. For example:

   ```
   opsUserName: ops
   opsUserPassword: CRYPT:an03xPrxLAu9p==
   ```

   The server only decrypts passwords that start with the **CRYPT:** prefix. Passwords without the **CRYPT:** prefix are considered plain text and remain unmodified.

End