



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.

Web Services and Applications Deployment Guide

Password encryption

Password encryption

For added security, consider encrypting your passwords in the **application.yaml** file. This feature is only supported for JAR (Spring Boot) distributables.

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	<ul style="list-style-type: none"> keyStorePassword keyManagerPassword trustStorePassword
serverSettings	<ul style="list-style-type: none"> opsUserPassword cmePassword jksPassword webDAVPassword
serverSettings > samlSettings	<ul style="list-style-type: none"> encryptionKeyPassword signingKeyPassword tlsKeyPassword
serverSettings > accountManagement > smtpServer	<ul style="list-style-type: none"> password
cassandraCluster	<ul style="list-style-type: none"> password truststorePassword

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==
```

Password encryption

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