Mail server connection configuration - CustomerID

Mail server connection is originally configured in the file `win32.config` (or `linux.config` in Linux installations). If these settings need to be changed after installation, it is best to do the changes both to the `win32.config/linux.config` configuration file and directly to WildFly configuration.

The following table explains the different mail server settings:

Property Name	Description
mail.host	The address of the SMTP server to be used. It can either be the host name or the IP address of the mail server.
mail.port	The port of the SMTP server to be used.
mail.username	The user name to use when connecting to the mail server. Can be left empty if no user needs to be defined when contacting the mail server.
mail.password	Password for the SMTP server, if required.
mail.from	The email address from which emails from Ubisecure CustomerID seem to be coming from. You need to double the @ character. For example: noReplies@@example.com
mail.ssl	If true, SSL is used.

The issuer of the mail server SSL certificate must be trusted by the Java environment by adding it to the Java truststore.

Adding Mail Server Certificate to Java Truststore

The usage of SSL is recommended when making the SMTP connection from Ubisecure CustomerID to a mail server. You must add the certificate of the issuer to the Ubisecure CustomerID trust store.

In Windows the Java certificate storage is by default in the following file:

- `%JRE_HOME%\lib\security\cacerts`

The SMTP server issuer certificate can be added to the Java certificate store using the `keytool` command. Here are example commands for Windows and Linux installations:

Listing 1. Windows

```
cd %JRE_HOME%\lib\security
set keytool="%JRE_HOME%\bin\keytool"
%keytool% –importcert –keystore cacerts –trustcacerts –alias <any alias e.g. mailserverca> -file <insert issuer
certificate filename here> -storepass changeit
```

Listing 2. Linux

```
cd $JRE_HOME/lib/security
keytool –importcert –keystore cacerts –trustcacerts –alias <any alias e.g. mailserverca> –file <insert issuer
certificate filename here> -storepass changeit
```

Check the validity time of the issuer certificate and record in your system maintenance calendar a task to check this well before it expires and ensure it is updated as required.