eServices Deployment Guide

Deploying an E-Mail System in Secured Mode

5/4/2025

Contents

Deploying an E-Mail System in Secured Mode

This section describes how to configure an e-mail system to work in secured mode using TLS/SSL. This applies to POP3, IMAP4, and SMTP. The purpose is to generate and install a public/private key pair.

Configuring TLS/SSL for E-mail Server

This section describes procedures for configuring your E-mail Server application to work with TLS/SSL.

1. Generating the .truststore file

Prerequisites: The corporate e-mail server is configured to work in secured mode.

Steps:

1. From the certificate on the Corporate E-mail Server, extract the public key. The following is an example of extracting a public key using keytool:

   ```
   keytool -export -v -alias hostname.example.com -file <certificate_name>.cer -keystore
   <certificate_name>.truststore
   -storepass <certificate_password> keytool -import -alias hostname.example.com -file
   <certificate_name>.cer -keystore client.truststore -storepass <certificate_password>
   ```

   At this point, the **client.truststore** file contains the public key.
2. Copy it to the host on which E-mail Server is running.

2. Modifying the E-mail Server startup command line on Windows

Prerequisites: The **.truststore** file has been created.

Steps:

1. Open **JavaEmailServerDriver.ini** in a text editor.
2. In the **[JavaArgs]** section, add the following: `-Djavax.net.ssl.trustStore=<path to certificate>`
3. Save and close the file.

3. Modifying the E-mail Server startup command line on UNIX

Prerequisites: The **.truststore** file has been created.

Steps:

1. Locate the E-mail Server startup file (**emailServer.sh**).
2. Open the file in a text editor and modify the startup command line so E-mail Server can locate the **.truststore** file. For example:

```
java -Djavax.net.ssl.trustStore=”<path to certificate>” --Xmx512M ....
```

3. Save and close the file.

4. Configuring E-mail Server's POP, IMAP, and SMTP Ports

Prerequisites: The **.truststore** file has been generated and E-mail Server's startup command line has been modified.

Steps:

1. In Configuration Manager or Genesys Administrator, open the properties for your E-mail Server application.
2. In the Options tab, locate the **[pop-client]** section for IMAP and configure the **type**, **port**, and **enable-ssl** options. For example:

```
[pop-client1]
type = IMAP
port = 993 (the default SSL port for IMAP)
pop-connection-security = ssl-tls
```

3. Locate the **[pop-client]** section for POP3 and configure the **type**, **port**, and **enable-ssl** options. For example:

```
[pop-client2]
type = POP3
port = 995 (the default SSL port for POP3)
pop-connection-security = ssl-tls
```

4. Locate the **[smtp-client]** section and configure the **port** and **enable-ssl** options. For example:

```
port = 465 (the default SSL port for SMTP)
smtp-connection-security = ssl-tls
```

5. Save your changes.
6. (Optional) If the application has already started, restart the application to apply the changes.

Configuring TLS 1.2 for E-mail Server

Prerequisites:

- E-mail Server must run on JDK 1.8 or later.
- Ensure JDK 1.8 or later is installed. For example:
  - On the UNIX platform, the installed **emailServer.sh** (/usr/local/genesys/eservices/esj/emailServer.sh) must have JAVACMD pointing to JDK 8 or later, as follows:

    ```
    JAVACMD=/usr/lib/jvm/jre1.8.0_161/bin/java
    ```

  - On the Windows platform, the installed **JavaEmailServerDriver.ini** file must have the JVMPath reference to JDK 8 or later, as follows:

    ```
    JVMPath=C:\Programs\java\x64\jdk\jre\bin\server\jvm.dll
    ```

Steps:

1. Follow procedures in Configuring TLS/SSL for E-mail Server to generate a certificate with **trustStore**, to modify the E-mail Server startup command line on Windows and/or UNIX, and to configure E-mail Server's POP, IMAP, and SMTP ports.
2. Configure the following E-mail Server KVPs:

   ```
   [pop-client]
   mail.pop3s.ssl.protocols="TLSv1.2"
   (OR)
   mail.imaps.ssl.protocols="TLSv1.2"

   [smtp-client]
   mail.smtps.ssl.protocols="TLSv1.2"
   ```

   Note: The **pop-client** configuration must be added to all **pop-client-*** sections.

Troubleshooting:

To address possible issues on the Windows platform, consider completing the following steps:

1. Disable TLS 1.0 if necessary. See details in Microsoft documentation.
2. Enable TLS 1.2. See an example in this documentation.
3. Create an SSL self-signed certificate with **openssl**.
4. Add this self-signed certificate to the mail server (for example, set up an hMailServer with this certificate and add TCP/IP ports for IMAP-993, POP3-995, and SMTP-587 by following these instructions).
5. Verify the TLS version for the expected ports using **openssl**. For example:

   ```
   C:\> openssl s_client -connect <domainName>:993
   ```

   Example of the expected result:

   ```
   SSL-Session:
       Protocol  : TLSv1.2
       Cipher    : 0000
       Session-ID:
       Session-ID-ctx:
       Master-Key:
       Key-Arg   : None
       PSK identity: None
       PSK identity hint: None
       SRP username: None
       Start Time: 1526325099
   ```

```
Timeout   : 300 (sec)
Verify return code: 0 (ok)
```

Configuring the Corporate E-mail Server

Configure TLS/SSL in the Corporate E-mail Server. Follow the constructor recommendations to generate a certificate and configure TLS/SSL on ports POP3, IMAP and SMTP.

The following is an example of generation of a certificate with keytool (keytool is a Java utility that is available with the JRE. The utility can be found in <eServices_Install_Dir>/jre/bin for UNIX operating systems, and in <eServices_Install_Dir>\jre\bin for Windows operating systems):

```
keytool -genkey -v -alias hostname.example.com -dname
“CN=hostname.example.com,OU=IT,O=ourcompany,C=FR” -keypass <certificate_password>
-keystore <certicate_name>.keystore -storepass <certificate_password> -keyalg “RSA” -sigalg
“SHA1withRSA” -keysize 2048 -validity 3650
```

The arguments used in this command are the following:

- `-alias`—Defines an alias in keystore, to store the key.
- `-dname`—Distinguished Name, a comma-separated list made up of the following, in the following order:
  - CN—Common Name. This must be the name of the host where the corporate e-mail server is running. It must be the host name used in E-mail Server's settings; for example, if connecting to a POP 3 server, the option server in the pop-client section must have this value.
  - OU—Organizational Unit Name
  - O—Organization Name
  - L—Locality Name (city)
  - S—State
  - C—Country Name

> **Important**
>
> - The abbreviations are not case-sensitive.
> - Only CN is required.

- `-keypass`—Password of the key of the certificate.
- `-keystore`—Specifies the keystore used.
- `-storepass`—Password of the keystore.
- `-keyalg`—Algorithm used to generate the key. Possible values are DSA and RSA. More information is available at `http://docs.oracle.com/javase`.

- `-sigalg`—Specifies the algorithm used to sign the key.
- `-keysize`—Specifies the size of the key.
- `-validity`—Defines the validity of the certificate, in days. The value in the example is 3,650 days, or 10 years.