# SMTP Listener 1.1

The SMTP Listener is a custom message listener extension for Parasoft Virtualize. It stands up a temporary SMTP server that notifies Virtualize on a per-message basis allowing users to accept or reject, with a custom rejection message, the incoming message and perform validations and post-processing as needed.

In this section:



## Installation

This tool can be installed from the UI or the command line.

### Installing from the UI

1. Choose **Parasoft> Preferences**.
2. Choose **System Properties** and click **Add JARs**.
3. In the file chooser, select com.veritualize.listener.smtp-<version>.jar.
4. Click **Apply** and restart Virtualize.

### Installing from the Command Line

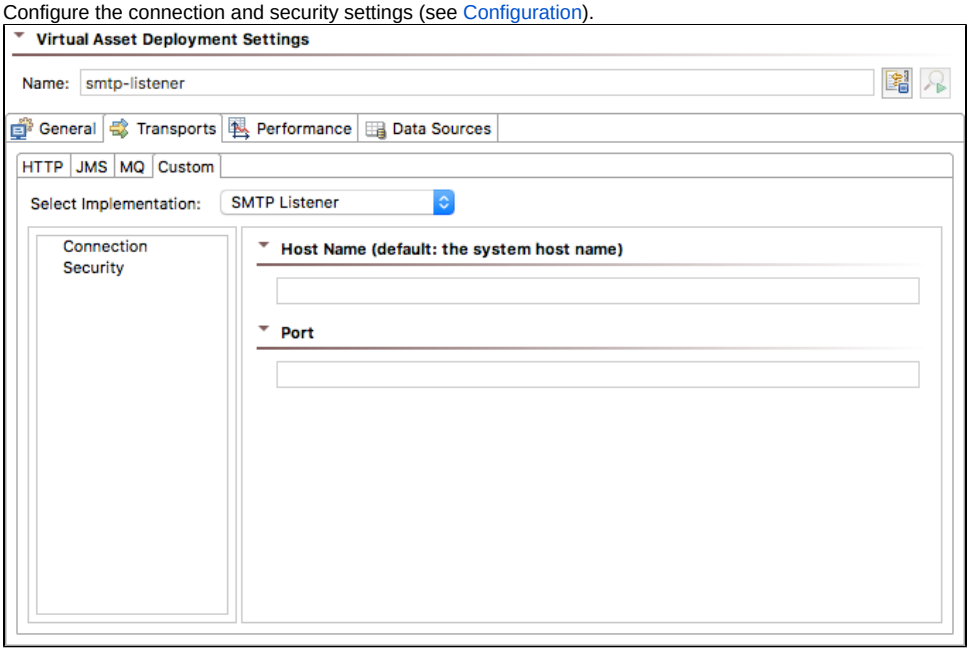
Add the com.parasoft.virtualize.listener.smtp-<version>.jar file to the system.properties.classpath property in your localsettings properties file. For example:

```
system.properties.classpath=<path to jar>/com.parasoft.virtualize.listener.smtp-1.1.0.jar
```

## Usage

You can select and configure the listener in the Virtual Asset configuration panel.

1. In the Virtualize Server view, choose the virtual asset you want to configure to use with the custom message listener.
2. Choose Transports> Custom in the Virtual Asset Deployment Settings. If multiple listeners are installed, use the Select Implementation drop-down menu to select **SMTPListener**.
3. Configure the connection and security settings (see Configuration).




4. Save your changes.

## Configuration

You can configure the following settings.

## Connection Settings

| | |
|---|---|
| **Host Name** | Defines the hostname for the SMTP server. If empty, the system default hostname will be used. |
| **Port** | Defines the port for the SMTP server. If empty, the listener will not start. |

## Security Settings

| | |
|---|---|
| **User Properties File** | Specifies the absolute path to a properties file used to define username and password combinations. The passwords are stored in plain text. The properties file should be configured in the following format:<br><br>`<username>=<password>`<br><br>*If this field is left empty user authentication will be disabled.* |
| **Enable Transport Layer Security** | Enables/disables transport layer security. If set to `true`, all connections to the server will be encrypted. Enabling TLS requires a properly configured Key Store and Trust Store.<br><br>Default is `false`. |
| **Key Store File** | Specifies the absolute path to a keystore file. The keystore file must be in a standard format (e.g., JKS, PKCS12, etc.). If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.keyStore will be used. *TLS must be enabled for this property to have any effect*. |
| **Key Store Type** | Defines the type of keystore file supplied in the Key Store File setting. If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.keyStoreType will be used. *TLS must be enabled for this property to have any effect*. |
| **Key Store Password** | Defines the password for the keystore supplied in the Key Store File setting. If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.keyStorePassword will be used. *TLS must be enabled for this property to have any effect*. |
| **Enable Client Authentication** | Enables/disables client authentication when TLS is enabled. If set to `true`, all connections will require the server to authenticate the clients' certificate. The Trust Store File must be properly configured with the client certificate as a “Trusted” certificate. *TLS must be enabled for this property to have any effect*.<br><br>Default is `false`. |
| **Trust Store File** | Specifies the absolute path to the keystore file used for verifying the authenticity (“trust”) of client certificates. The keystore file must be in a standard format (e.g., JKS, PKCS12, etc.). If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.trustStore will be used. *TLS must be enabled for this property to have any effect*. |
| **Trust Store Type** | Defines the type of keystore file supplied in the Trust Store File setting. If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.trustStoreType will be used. *TLS must be enabled for this property to have any effect.* |
| **Trust Store Password** | Defines the password for the keystore supplied in the Trust Store File setting. If TLS is enabled and no value is defined, the JVM system property javax.net.ssl.trustStorePassword will be used. *TLS must be enabled for this property to have any effect.* |