



Parasoft SFTP Client Tool

About the Plugin

The SFTP Client tool is a custom tool extension for Parasoft SOAtest and Virtualize. It is a standard implementation of SFTP V3. The client performs a single SFTP session of up to 10 commands using Public Key authentication. Raw SFTP traffic is supplied as an output to the tool—much as it is with the FTP Client tool. Any failures during tool execution are reported as Quality Tasks; if failures occur, server connections are closed and tool execution terminates.

Implementation

The SFTP Client tool is implemented as `com.parasoft.soavirt.tool.sftp.client-1.0.0.jar`, which depends upon:

- **Parasoft SOAtest & Virtualize Custom Extension Utility Package:** `com.parasoft.soavirt.util.jar`
- **Java Secure Channel:** `jsch-0.1.50.jar`

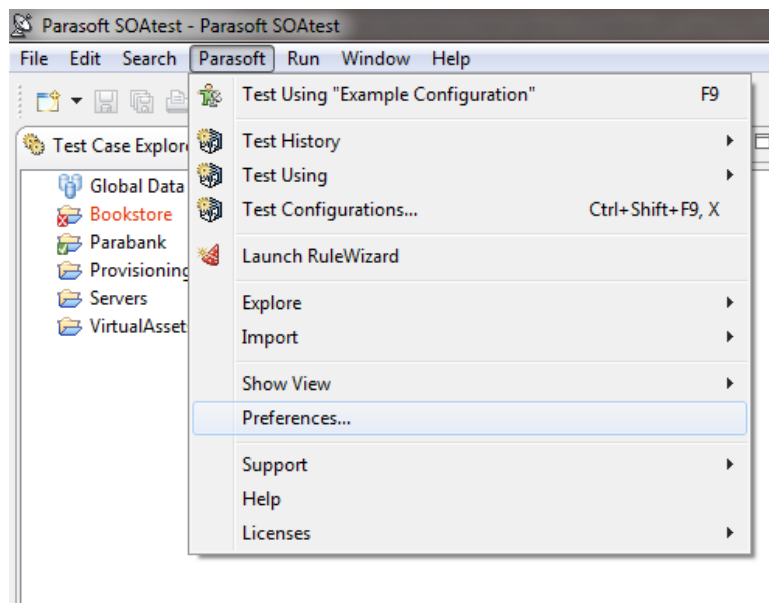
Note that `jsch-0.1.50.jar` is packaged with the tool's jar file and `com.parasoft.soavirt.util.jar` is available separately on Marketplace.

Installation

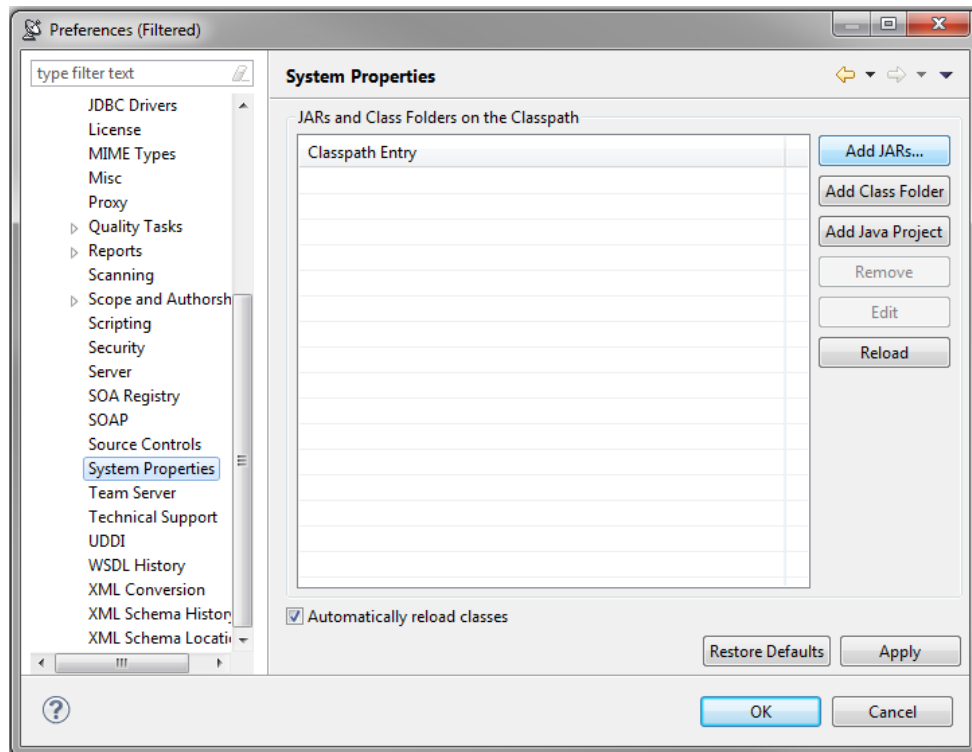
The tool can be installed from the UI or command line.

UI Installation

1. Choose **Parasoft > Preferences**.



2. In the System Properties preferences page, click **Add JARs**.



3. In the file chooser that opens, select **com.parasoft.soavirt.tool.sftp.client-1.0.0.jar**. Once this jar file is added to the SOAtest/Virtualize classpath, all of the required dependencies will be loaded.
4. Restart SOAtest/Virtualize.

Command Line Installation

Add the **com.parasoft.soavirt.tool.sftp.client-1.0.0.jar** file to the **system.properties.classpath** property in your localsettings properties file. For example:

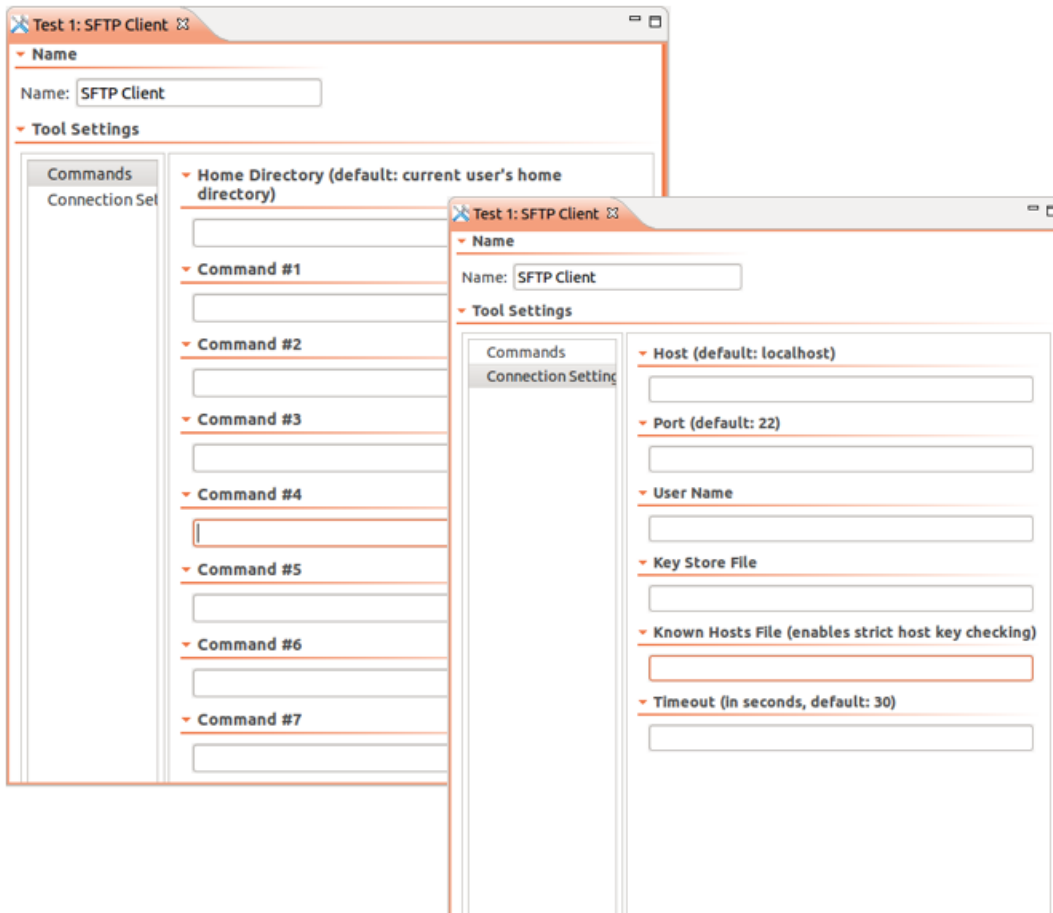
```
system.properties.classpath=<path to jar>/com.parasoft.soavirt.tool.sftp.client-1.0.0.jar
```

Once the classpath is modified, all of the required dependencies will be loaded.

Usage

SFTP Client tools can be added as standalone tools via the Add Test wizard, or chained to the output of another tool via the Add Output wizard.

Configuration options cover commands and connection settings.



The image displays two overlapping screenshots of the 'Test 1: SFTP Client' configuration window. The left window shows the 'Commands' tab, which includes a 'Name' field set to 'SFTP Client', a 'Tool Settings' section with a 'Home Directory' field, and seven 'Command' slots (Command #1 through Command #7). The right window shows the 'Connection Settings' tab, which includes a 'Name' field set to 'SFTP Client', a 'Tool Settings' section with fields for 'Host' (default: localhost), 'Port' (default: 22), 'User Name', 'Key Store File', 'Known Hosts File' (with a note: 'enables strict host key checking'), and 'Timeout' (in seconds, default: 30).

Commands Configuration Options

Option	Description
Home Directory	Defines the user's local home directory. This directory is <i>not</i> the same as the user's remote home directory, which is configured on the server side. If empty, the system's current user's home directory will be used.
Command #1 - #10	Specifies the series of SFTP commands to be performed during the SFTP session. The commands will be executed in the order in which they are listed here. They should be typed exactly as if they were being performed in an interactive SFTP console. At least one of these fields must be defined in order for this tool to be enabled.

Connection Settings Configuration Options

Option	Description
Host	Defines the hostname or IP address for connecting to the server. If empty, the default value (localhost) will be used.
Port	Defines the port for connecting to the server. If empty, the default value (22) will be used.
User Name	Defines the username for connecting to the server. If empty, the tool will remain disabled.
Key Store File	Defines the absolute path to the user's private key file, which should be in PEM format. If empty, the tool will remain disabled.
Known Hosts File	Defines the absolute path to a known hosts file, which should be formatted as a standard OpenSSH known hosts file. If a known hosts file is defined, then strict host key checking will be enabled. If the host key is not found in the known hosts file, the connection to the server will be closed. If empty, strict host key checking will remain disabled.
Timeout	Defines how many seconds to wait to connect to the SSH server (as well as the underlying SFTP channel) before timing out and closing all connections. If empty, the default value (30 seconds) will be used.