

Advanced Server Configuration Options

The following is a list of advanced configuration options you can specify in a properties file. For details on working with properties files, as well as the most commonly-used options, see [Server Configuration](#).

In this section:

- [General Virtualize Options](#)
- [Proxy Options](#)
- [Security Options](#)

General Virtualize Options

- [misc.character.encoding](#)
- [misc.default.timeout](#)
- [misc.project.file.format](#)
- [misc.automatically.backup.project.files](#)
- [misc.warn.file.size](#)
- [traffic.wizard.xpath.ignores](#)
- [xml.conversion.data.model.directories](#)

misc.character.encoding

Specifies the character encoding; valid values are any encodings available on the JVM being used. The default is UTF-8.

misc.default.timeout

The default timeout in milliseconds. Allows you to customize the length of delay after which Virtualize should consider your HTTP, JMS, or MQ requests to be "timed out." The default is 30000 milliseconds. Specifically applies to the Message Forward Tool.

misc.project.file.format

Specifies what file format to use for saving project files (e.g., .pva, .pvn, .changetemplate). Project files can be saved in three formats—XML, binary, and compressed XML. The default is XML.

misc.automatically.backup.project.files

Tells Virtualize to automatically back up and save the project files you are working on. The default is false.

misc.warn.file.size

Specifies the threshold at which the REST API will return an error about large .pva file size. You can then reduce the file size (and prevent performance problems) by dividing it into smaller files. The default is 20.

traffic.wizard.xpath.ignores

Lets you globally indicate that you want certain values (such as timestamps) ignored whenever:

- you are creating parameterized .pvas from traffic, and
- request body correlations are configured automatically.

Exclusions are specified in the format:

```
traffic.wiz-ard.xpath.ignores=[element name 1]:[value pattern 1];[element name 2]:[value pattern 2];[element name 3]:[value pattern 3]
```

Default Value

```
*:[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}([.][0-9]{1,3})?(([-+][0-9]{2}:[0-9]{2})Z)?
```

Example Usage

```
traffic.wiz-ard.xpath.ignores=*[0-9]{4}-[0-9]{2}-[0-9]{2}T[0-9]{2}:[0-9]{2}:[0-9]{2}([.][0-9]{1,3})?(([-+][0-9]{2}:[0-9]{2})|Z)?;uuid:[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}
```

Backslashes in Regular Expressions Must be Escaped

When the backslash character (\) is used in the regular expression, it needs to be escaped. For example, the regex [d], which represents a single digit, would be entered as [\\d].

xml.conversion.data.model.directories

Specifies a comma-separated list of directories where fixed length data model files are located (for use in Fixed Length responders).

Proxy Options

- [proxy.enable.proxy](#)
- [proxy.use.system.proxy.configuration](#)
- [proxy.use.automatic.configuration.script](#)
- [proxy.enable.proxy.authentication](#)
- [proxy.same.proxy.server.for.all.protocols](#)
- [proxy.automatic.configuration.script.location](#)
- [proxy.http](#)
- [proxy.http.port](#)
- [proxy.ftp](#)
- [proxy.ftp.port](#)
- [proxy.secure](#)
- [proxy.secure.port](#)
- [proxy.username](#)
- [proxy.password](#)
- [proxy.exceptions](#)

proxy.enable.proxy

Enables/disables the application of Windows and IE proxy settings.

If Windows/IE are properly configured so that the proxy accesses the relevant websites, set this option to `false` and set the [proxy.use.system.proxy.configuration](#) option to `true`. Otherwise, set this option to `true` and set the other relevant proxy properties.

The default is `false`.

This option specifically applies to the [Message Forward](#) tool.

proxy.use.system.proxy.configuration

If Windows and IE (which use the same settings) are configured to properly use the proxy to access the relevant websites, set this property to `true`.

The default is `true`.

This option specifically applies to the [Message Forward](#) tool.

proxy.use.automatic.configuration.script

Enables/disables ability to use an automatic configuration script. Set this to `true` and enter the proxy address with [proxy.automatic.configuration.script.location](#) setting.

The default is `false`.

This option specifically applies to the [Message Forward](#) tool.

proxy.enable.proxy.authentication

If your proxy server requires authentication, set this property to true, then enter a valid user name and password with proxy.username and proxy.password. The default is false.

This option specifically applies to the [Message Forward](#) tool.

proxy.same.proxy.server.for.all.protocols

If you want to use the same proxy server for all protocols, set this property to true, then enter the address and port of the proxy server you want to use in the proxy.http, proxy.ftp, proxy.secure, and proxy.*.port properties. The default is true.

This option specifically applies to the [Message Forward](#) tool.

proxy.automatic.configuration.script.location

The value should be a URL to the script: either an HTTP(S) URL or a file URL. File URLs should be formatted as "file:/" followed by the file system path where the proxy autoconfiguration script lives. For example, on Windows this could be file://c:/Users/user/scripts/proxy.pac. On Linux, it might be file:///home/machine/scripts/proxy.pac.

This option specifically applies to the [Message Forward](#) tool.

proxy.http

Address of the http proxy to use. If the same proxy server will be used for all protocols, this is the value that will be used.

This option specifically applies to the [Message Forward](#) tool.

proxy.http.port

Port of the http proxy to use. If the same proxy server will be used for all protocols, this is the value that will be used.

This option specifically applies to the [Message Forward](#) tool.

proxy.ftp

Address of the ftp proxy to use.

This option specifically applies to the [Message Forward](#) tool.

proxy.ftp.port

Port of the ftp proxy to use.

This option specifically applies to the [Message Forward](#) tool.

proxy.secure

Address of the secure proxy to use.

This option specifically applies to the [Message Forward](#) tool.

proxy.secure.port

Port of the secure proxy to use.

This option specifically applies to the [Message Forward](#) tool.

proxy.username

Username to use when proxy authentication is enabled.

This option specifically applies to the [Message Forward](#) tool.

proxy.password

Password to use when proxy authentication is enabled.

This option specifically applies to the [Message Forward](#) tool.

proxy.exceptions

If you want to allow Web traffic from designated IP addresses to pass through directly (avoiding the proxy), enter those IP addresses in this property. If you enter multiple addresses, use a semicolon (;) to separate the entries.

This option specifically applies to the [Message Forward](#) tool.

Security Options

- [security.mq.ssl.trust.store.location](#)
- [security.mq.ssl.key.store.location](#)
- [security.mq.ssl.key.store.password](#)

security.mq.ssl.trust.store.location

Specifies the location of the trust store to be used for Server-Side SSL (authentication of the Queue Manager by the client).

This option specifically applies to the [Message Forward](#) tool.

security.mq.ssl.key.store.location

Specifies the location of the key store to be used for Client-Side SSL (authentication of the client by the Queue Manager).

This option specifically applies to the [Message Forward](#) tool.

security.mq.ssl.key.store.password

Specifies the MQ SSL Key Store password.

This option specifically applies to the [Message Forward](#) tool.