FIXEdge Admin REST API

Overview

FIXEdge Admin REST API is intended to be a pragmatic tool for on-the-fly tuning of the most common FIXEdge properties.

It offers REST interface to handle the following properties of FIXEdge:

1. Referring to FIX message log:
    a. Retrieve FIX message log of specific / all sessions
    b. Output the acquired contents to text
2. Get FIX session list:
    a. Retrieve the list of session definitions and their states
    b. Output the acquired contents to text
3. Session Control

    a. Start and stop sessions
    b. Get session status (since FIXEdge 6.9.0)
    c. Get session statistics (since FIXEdge 6.9.0)
    d. Restart session (since FIXEdge 6.9.0)
4. Reset sequence No.

    a. Reset FIX sequence No. (incoming and outgoing)
5. Set sequence No.

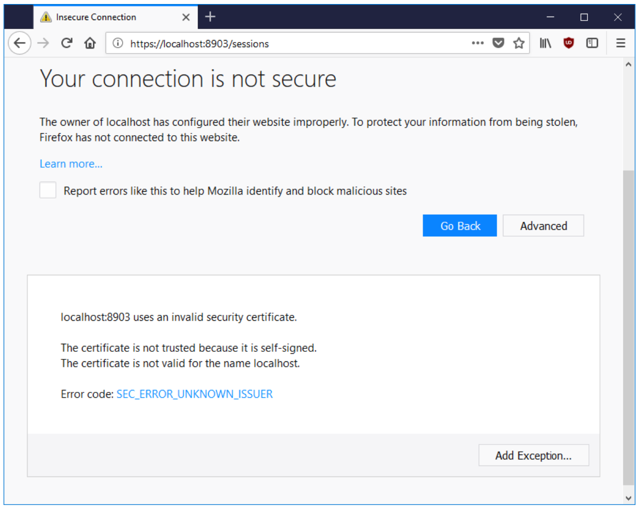
    a. Set an arbitrary value for the sequence number of a specific session
6. Reload BL_Config.xml
7. Send messages to session output queue

Installation

FIXEdge Admin REST API is a part of FIXEdge Server and is introduced in version 6.4.0 of FIXEdge. It's needed to enable AdminRESTAPI.Enabled parameter and set the values for all required AdminRESTAPI fields in FIXEdge.properties (See the "Properties" section).

Admin REST API is available via HTTPS protocol only so it's needed to configure a certificate and a private key which it uses for encryption. FIXEdge packages contain self-signed certificate and private key that can be used by Admin REST API. You can set up your own a self-signed certificate for the servers you're connecting to as described in the "Configuration of Admin REST API with self-signed SSL certificate" section below.

Note: when you're connecting to a server that uses a self-signed certificate, you will be displayed a warning (see figure below). Click on the "Add Exception..." button to add the certificate to a set of trusted certificates.



Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

localhost:8903 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is not valid for the name localhost.

Error code: SEC_ERROR_UNKNOWN_ISSUER

If you use cURL to query Admin REST API you need to add parameter *--insecure*, e.g.

curl --insecure https://fixedge.host:8903/sessions

Configuration parameters

The properties can be configured in `FIXEdge.properties:`

Field	Type	Description	Required
AdminRESTAPI.Enabled	bool	is admin REST API enabled or not	No, default = false
AdminRESTAPI.ServerMode	enum	admin REST API server modes: • HTTPS • HTTP	No, default = HTTPS
AdminRESTAPI.BindAddress	string	define specific network interface for listening ⓘ The parameter was introduced in FIXEdge 6.9.0	No, default = "0.0.0.0" (all interfaces)
AdminRESTAPI.Port	int	TCP port to listen	Yes (if **AdminRESTAPI.Enabled** = true)
AdminRESTAPI.HTTPSServer.Port	int	TCP port to listen ⓘ Property is deprecated, use **AdminRESTAPI.Port** instead	No
AdminRESTAPI.HTTPSServer.PrivateKey	string	path to SSL private key file	Yes (if **AdminRESTAPI.ServerMode** = HTTPS)
AdminRESTAPI.HTTPSServer.Certificate	string	path to SSL certificate file	Yes (if **AdminRESTAPI.ServerMode** = HTTPS)
AdminRESTAPI.HTTPSServer.CertificateAuthority	string	path to the file or directory containing the CA/root certificates. Can be empty if the OpenSSL builtin CA certificates are used	No

Example:

```
AdminRESTAPI.Enabled = true
AdminRESTAPI.Port = 8903
AdminRESTAPI.HTTPSServer.PrivateKey = ../FIXEdge1/conf/AdminRESTAPI.key
AdminRESTAPI.HTTPSServer.Certificate = ../FIXEdge1/conf/AdminRESTAPI.crt
```

Configuration of Admin REST API with self-signed SSL certificate:

You need OpenSSL or LibreSSL installed on your system to follow this instruction. For Windows systems you can get OpenSSL from Cygwin (www.cygwin.com).

1. Create CA root key
   openssl genrsa -out rootCA.key 2048
2. Create root certificate
   openssl req -x509 -new -key rootCA.key -days 10000 -out rootCA.crt
   Answer the questions that openssl asks. The duration of certificate will be 10000 days.
3. Generate certificate signed with the created CA
   openssl genrsa -out AdminRESTAPI.key 2048
4. Create certificate signing request
   openssl req -new -key AdminRESTAPI.key -out AdminRESTAPI.csr
5. Sign the certificate with the root certificate
   openssl x509 -req -in AdminRESTAPI.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out AdminRESTAPI.crt -days 5000

Documentation

FIXEdge Administrative REST API and SDK Documentation