sgcWebSockets 4.3.7

Table of Contents

Introduction

WebSockets represent a long-awaited evolution in client/server web technology. They allow a long-held single TCP socket connection to be established between the client and server which allows for bi-directional, full duplex, messages to be instantly distributed with little overhead resulting in a very low latency connection.

Both the WebSocket API and the well as native WebSocket support in browsers such as Google Chrome, Firefox, Opera and a prototype Silverlight to JavaScript bridge implementation for Internet Explorer, there are now WebSocket library implementations in Objective-C, .NET, Ruby, Java, node.js, ActionScript and many other languages.

The Internet wasn't built to be all that dynamic. It was conceived to be a collection of HyperText Markup Language (HTML) pages linking to one another to form a conceptual web of information. Over time the static resources increased in number and richer items, such as images, began to be part of the web fabric. Server technologies advanced allowing for dynamic server pages - pages whose content was generated based on a query.

Soon the requirement to have more dynamic web pages lead to the availability of Dynamic HyperText Markup Language (DHTML) all thanks to JavaScript (let's pretend VBScript never existed). Over the following years, we saw cross frame communication in an attempt to avoid page reloads followed by HTTP Polling within frames. Things started to get interesting with the introduction of LiveConnect, then the forever frame technique, and finally, thanks to Microsoft, we ended up with the XMLHttpRequest object and therefore Asynchronous JavaScript and XML (AJAX). In turn, AJAX made XHR Long-Polling and XHR Streaming possible. But none of these solutions offered a truly standardised cross-browser solution to real-time bi-directional communication between a server and a client.

Finally, WebSockets represent a standard for bi-directional real-time communication between servers and clients. Firstly in web browsers, but ultimately between any server and any client. The standards first approach means that as developers we can finally create functionality that works consistently across multiple platforms. Connection limitations are no longer a problem since WebSockets represent a single TCP socket connection. Cross-domain communication has been considered from day one and is dealt with within the connection handshake. This means that services such as Pusher can easily use them when offering a massively scalable real-time platform that can be used by any website, web, desktop or mobile application.

WebSockets don't make AJAX obsolete but they do supersede Comet (HTTP Long-polling/HTTP Streaming) as the solution of choice for true real-time functionality. AJAX should still be used for making short-lived web service calls, and if we eventually see a good uptake in CORS supporting web services, it will get even more useful. WebSockets should now be the go-to standard for real-time functionality since they offer low latency bi-directional communication over a single connection. Even if a web browser doesn't natively support the WebSocket object there are polyfill fallback options which all but guarantee any web browser can actually establish a WebSocket connection.

sgcWebSockets is a complete package providing access to WebSockets protocol, allowing to create WebSockets Servers, Intraweb Clients or WebSocket Clients in VCL, Firemonkey, Linux and FreePascal applications.

- Fully functional **multithreaded WebSocket server** according to **RFC 6455**.
- Supports **Firemonkey** (**Windows** and **MacOS**).
- Supports **NEXTGEN Compiler** (IOS and Android Support).
- Supports **LINUX Compiler**.
- Supports **Lazarus / FreePascal.**
- Supports **CBuilder.**

- Supports **Chrome**, **Firefox, Safari, Opera and Internet Explorer** (including **iPhone**, **iPad** and **iPod**)
- Supports **Microsoft HTTP Server API** and **IOCP** for high-performance Windows Servers.
- **Multiple Threads** Support. **Indy Servers** support **IOCP** or default Indy one thread per connection model.
- Supports **Message Compression** using PerMessage_Deflate extension **RFC 7692**.
- Supports **Text** and **Binary** Messages.
- Supports **Server** and **Client Authentication**. **OAuth2** is fully supported.
- **Server** component providing **WebSocket** and **HTTP connections** through the **same port**.
- **Proxy Server** component allowing to Web Browsers to connect to any TCP server.
- **WebBroker Server** which supports **DataSnap, HTTP** and **WebSocket** connections using the same port.
- **Load Balancing** Server.
- Client WebSocket based on WinHTTP API.
- Client WebSocket supports connections through **Socket.IO Servers**.
- **FallBack** support through Adobe **Flash** for old Web Browsers like Internet Explorer from 6+.
- Supports **Server-Sent Events** (Push Notifications) over HTTP Protocol.
- **WatchDog** and **HeartBeat** built-in support.
- **Client WebSocket** supports connections through **HTTP Proxy Servers** and **SOCKS Proxy Servers.**
- **Events** Available: OnConnect, OnDisconnect, OnMessage, OnError, OnHandshake
- **Built-in sub-protocols**: JSON-RPC 2.0, Dataset, Presence, WebRTC, MQTT (3.1.1 and 5.0) and WAMP (1.0 and 2.0)
- Client **Built-in API**: **Blockchain**, **Bitfinex**, **Pusher, SignalR Core, Huobi, CEX, Bitmex and Bittrex**.
- Support for JSON parsers: **Delphi JSON** and **XSuperObject**.
- **Built-in Javascript libraries** to support browser clients.
- **Easy** to setup
- **Javascript Events** for full control
- **Async Events** using Ajax
- **SSL/TLS Support** for Server / Client Components (OpenSSL libraries required). OpenSSL 1.1.1 libraries are supported. Client supports **SChannel** for Windows.

Main components available are:

- **TsgcWebSocketClient:** Non-visual component, used to establish a WebSocket connection with a WebSocket server, based on Indy LIbrary.
- **TsgcWebSocketServer:** Non-visual component, it's used to manage client threaded connections. Supports RFC 6455. Based on Indy library.
- **TsgcWebSocketHTTPServer:** Non-visual component, it's used to manage client threaded connections. Supports RFC 6455. Supports HTTP Requests using a unique port for WebSocket and HTTP Connections. Based on Indy library.
- **TsgcWSHTTPWebBrokerBridgeServer:** Non-visual component, the server which allows combine HTTP, DataSnap and WebSocket requests using the same server and port.
- **TsgcWebSocketLoadBalancerServer:** Non-visual component, it's used to distribute messages across several back-up servers. Based on Indy library.
- **TsgcWebSocketClient_WinHTTP:** Non-visual component, used to establish a WebSocket connection with a WebSocket server based on WinHTTP API.
- **TsgcWebsocketProxyServer:** Non-visual component, used to translate WebSocket connections to normal TCP connections. Based on Indy library.

- **TsgcIWWebSocketClient:** Non-visual component, used on Intraweb forms to establish a WebSocket connection with a WebSocket Server.

Overview

Versions Support

Delphi supported IDE

- Delphi 7 (* only supported if upgraded to Indy 10, Intraweb is not supported)
- Delphi 2007
- Delphi 2009
- Delphi 2010
- Delphi XE
- Delphi XE2
- Delphi XE3
- Delphi XE4
- Delphi XE5
- Delphi XE6
- Delphi XE7
- Delphi XE8
- Delphi 10 Seattle
- Delphi 10.1 Berlin
- Delphi 10.2 Tokyo
- Delphi 10.3 Rio

CBuilder supported IDE

- CBuilder 2010
- CBuilder XE
- CBuilder XE2
- CBuilder XE3
- CBuilder XE4
- CBuilder XE5
- CBuilder XE6
- CBuilder XE7
- CBuilder XE8
- CBuilder 10 Seattle
- CBuilder 10.1 Berlin
- CBuilder 10.2 Tokyo
- CBuilder 10.3 Rio

AppMethod supported IDE

- AppMethod 2014

FreePascal supported IDE

- Lazarus

HTML supported IDE

- HTML5 Builder

Trial Version

Compiled *.dcu files provided with free version are using default Indy and Intraweb version. If you have upgraded any of these packets, probably it won't work or you need to buy full source code version.

Indy Package

Some components use Indy as TCP/IP library (like TsgcWebSocketClient or TsgcWebSocketServer), this means that Indy is needed in order to install sgcWebSockets Package. By default, sgcWebSockets uses Indy library built-in with Rad Studio, but we provide a custom indy version which has more features than Indy: support for OpenSSL API 1.1, ALPN protocol...

Installation

Delphi / CBuilder / Lazarus

1. Unzip the files included into a directory {$DIR}

2. From Delphi\CBuilder:

Add the directory where the files are unzipped {$DIR} to the Delphi\CBuilder library path under Tools, Environment options, Directories

All Delphi\CBuilder Versions

Add the directory {$DIR}\source to the library path

For specific Delphi version

Delphi 7 : Add the directory {$DIR}\libD7 to the library path
Delphi 2007 : Add the directory {$DIR}\libD2007 to the library path
Delphi 2009 : Add the directory {$DIR}\libD2009 to the library path
Delphi 2010 : Add the directory {$DIR}\libD2010 to the library path
Delphi XE : Add the directory {$DIR}\libDXE to the library path
Delphi XE2 : Add the directory {$DIR}\libDXE2\$(Platform) to the library path
Delphi XE3 : Add the directory {$DIR}\libDXE3\$(Platform) to the library path
Delphi XE4 : Add the directory {$DIR}\libDXE4\$(Platform) to the library path
Delphi XE5 : Add the directory {$DIR}\libDXE5\$(Platform) to the library path
Delphi XE6 : Add the directory {$DIR}\libDXE6\$(Platform) to the library path
Delphi XE7 : Add the directory {$DIR}\libDXE7\$(Platform) to the library path
Delphi XE8 : Add the directory {$DIR}\libDXE8\$(Platform) to the library path
Delphi 10 : Add the directory {$DIR}\libD10\$(Platform) to the library path
Delphi 10.1 : Add the directory {$DIR}\libD10_1\$(Platform) to the library path
Delphi 10.2 : Add the directory {$DIR}\libD10_2\$(Platform) to the library path
Delphi 10.3 : Add the directory {$DIR}\libD10_3\$(Platform) to the library path

For specific CBuilder version

C++ Builder 2010 : Add the directory {$DIR}\libD2010 to the library path
C++ Builder XE : Add the directory {$DIR}\libDXE to the library path
C++ Builder XE2 : Add the directory {$DIR}\libDXE2\$(Platform) to the library path
C++ Builder XE3 : Add the directory {$DIR}\libDXE3\$(Platform) to the library path
C++ Builder XE4 : Add the directory {$DIR}\libDXE4\$(Platform) to the library path
C++ Builder XE5 : Add the directory {$DIR}\libDXE5\$(Platform) to the library path
C++ Builder XE6 : Add the directory {$DIR}\libDXE6\$(Platform) to the library path
C++ Builder XE7 : Add the directory {$DIR}\libDXE7\$(Platform) to the library path
C++ Builder XE8 : Add the directory {$DIR}\libDXE8\$(Platform) to the library path
C++ Builder 10 : Add the directory {$DIR}\libD10\$(Platform) to the library path

C++ Builder 10.1 : Add the directory {$DIR}\libD10_1\$(Platform) to the library path
C++ Builder 10.2 : Add the directory {$DIR}\libD10_2\$(Platform) to the library path
C++ Builder 10.3 : Add the directory {$DIR}\libD10_3\$(Platform) to the library path

For all CBuilder versions, Add dcp\$(Platform) to the library path (contains .bpi files)

For AppMethod

AppMethod : Add the directory {$DIR}\libAppMethod\$(Platform) to the library path

3. From Delphi

Choose

File, Open and browse for the correct Packages\sgcWebSockets.groupproj (First compile sgcWebSocketsX.dpk and then install dclsgcWebSocketsX.dpk)

packages files for Delphi

sgcWebSocketsD7.groupproj : Delphi 7
sgcWebSocketsD2007.groupproj : Delphi 2007
sgcWebSocketsD2009.groupproj : Delphi 2009
sgcWebSocketsD2010.groupproj : Delphi 2010
sgcWebSocketsDXE.groupproj : Delphi XE
sgcWebSocketsDXE2.groupproj : Delphi XE2
sgcWebSocketsDXE3.groupproj : Delphi XE3
sgcWebSocketsDXE4.groupproj : Delphi XE4
sgcWebSocketsDXE5.groupproj : Delphi XE5
sgcWebSocketsDXE6.groupproj : Delphi XE6
sgcWebSocketsDXE7.groupproj : Delphi XE7
sgcWebSocketsDXE8.groupproj : Delphi XE8
sgcWebSocketsD10.groupproj : Delphi 10
sgcWebSocketsD10_1.groupproj : Delphi 10.1
sgcWebSocketsD10_2.groupproj : Delphi 10.2
sgcWebSocketsD10_3.groupproj : Delphi 10.3

4. From CBuilder

Choose

File, Open and browse for the correct Packages\sgcWebSockets.groupproj (First compile sgcWebSocketsX.dpk and then install dclsgcWebSocketsX.dpk)

packages files for CBuilder

sgcWebSocketsC2010.groupproj : C++ Builder 2010
sgcWebSocketsCXE.groupproj : C++ Builder XE
sgcWebSocketsCXE2.groupproj : C++ Builder XE2
sgcWebSocketsCXE3.groupproj : C++ Builder XE3
sgcWebSocketsCXE4.groupproj : C++ Builder XE4
sgcWebSocketsCXE5.groupproj : C++ Builder XE5
sgcWebSocketsCXE6.groupproj : C++ Builder XE6
sgcWebSocketsCXE7.groupproj : C++ Builder XE7

sgcWebSocketsCXE8.groupproj : C++ Builder XE8
sgcWebSocketsC10.groupproj : C++ Builder 10
sgcWebSocketsC10_1.groupproj : C++ Builder 10.1
sgcWebSocketsC10_2.groupproj : C++ Builder 10.2
sgcWebSocketsC10_3.groupproj : C++ Builder 10.3

5. From AppMethod

Choose
File, Open and browse for the correct Packages\sgcWebSockets.groupproj
(First compile sgcWebSocketsX.dpk and then install dclsgcWebSocketsX.dpk)

packages files for AppMethod

sgcWebSocketsAppMethod.groupproj : AppMethod

6. From Lazarus

Choose : File, Open and browse Packages\sgcWebSocketsLazarus.lpk (First compile and then install)

Compiled files are located on Lazarus Directory, inside this, there is a Indy directory with latest Indy source version.

Tested with Lazarus 1.6.4 and Indy 10.5.9.4930

7. Demos

All demos are available in subdirectory Demos. Just open the project and run it. Intraweb demos may need to modify some units due to different Intraweb Versions.

HTML5 Builder

1. Copy "esegece" directory into HTML5 Builder's RPCL directory.

C:\Program Files\Embarcadero\HTML5 Builder\5.0\rpcl

2. From HTML5 Builder

go to Home > Packages and press button "Add Package"

Locate your package file (sgcWebSockets.package.php), select it and click Open.

3. If you start a new project you will see a new palette called "SGC - WebSockets", drop a sgcWebSocket component on a Form and configure required properties.

4. Demos

All demos are available in subdirectory Demos. Just open the project and run it.

Install

Configure Install

In the source folder, there is a file called sgcVer.inc which includes all compiler defines for all Delphi, CBuilder and Lazarus IDEs. Here you can customize your configuration for Intraweb, Indy...

For every Delphi version, there is a section where you can configure all compiler defines, an example for Delphi 10.3

```
{$IFDEF VER330} { Delphi  10.3 }
  {$DEFINE D2006}
  {$DEFINE D2007}
  {$DEFINE D2009}
  {$DEFINE D2010}
  {$DEFINE DXE}
  {$DEFINE DXE2}
  {$DEFINE DXE3}
  {$DEFINE DXE4}
  {$DEFINE DXE5}
  {$DEFINE DXE6}
  {$DEFINE DXE7}
  {$DEFINE DXE8}
  {$DEFINE D10}
  {$DEFINE D10_1}
  {$DEFINE D10_2}
  {$DEFINE D10_3}
  {$DEFINE INDY10_1}
  {$DEFINE INDY10_2}
  {$DEFINE INDY10_5_5}
  {$DEFINE INDY10_5_7}
  {$DEFINE INDY10_6}
  {$DEFINE INDY10_6_2_5366}

  {$IFNDEF BCB}
    {$IFNDEF MACOS}
    {$IFNDEF ANDROID}
      {$DEFINE IWIX}
      {$DEFINE IWXI}
      {$DEFINE IWXIV}
    {$ENDIF}
    {$ENDIF}
{$IFNDEF NEXTGEN}
  {$DEFINE SGC_JSON_INTF}
{$ENDIF}
  {$ENDIF}
{$ENDIF}
```

Indy

There are some compiler defines for Indy library. This depends on Indy version installed, by default is configured for Indy package included with Delphi. Indy version is gsIdVersion parameter of IdVers.inc Indy file.

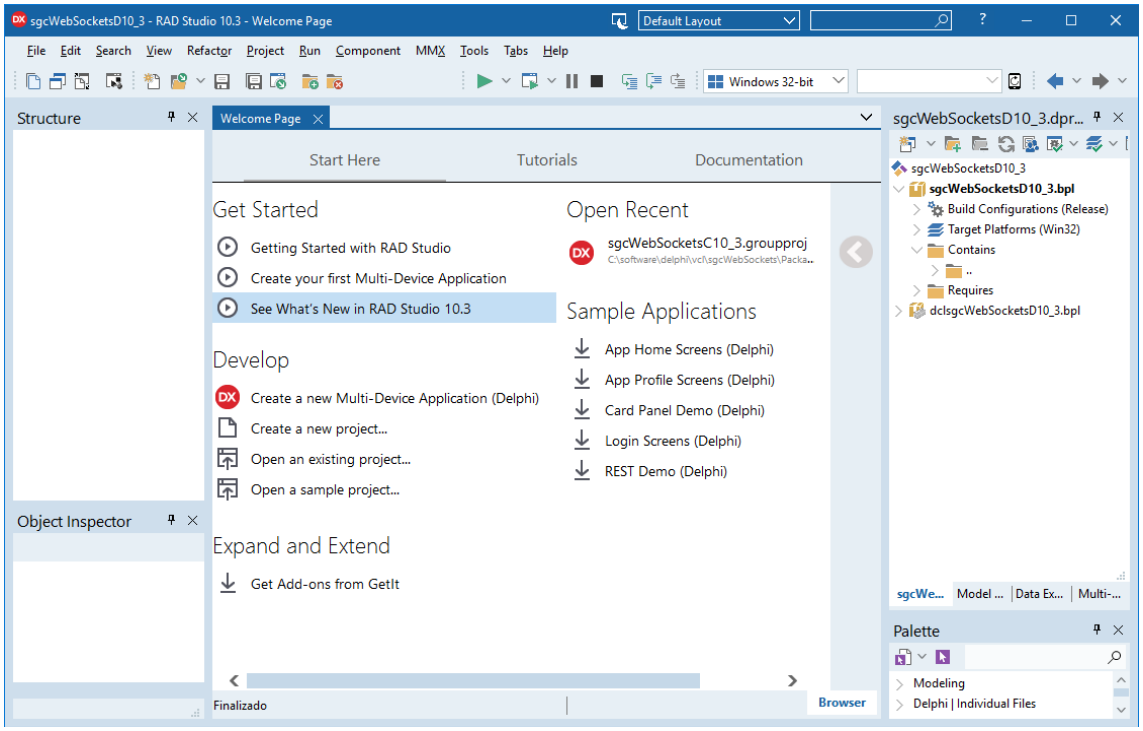
Intraweb

If Intraweb is not installed, just comment compiler defines for Intraweb (those who starts with IW...)

Install Package

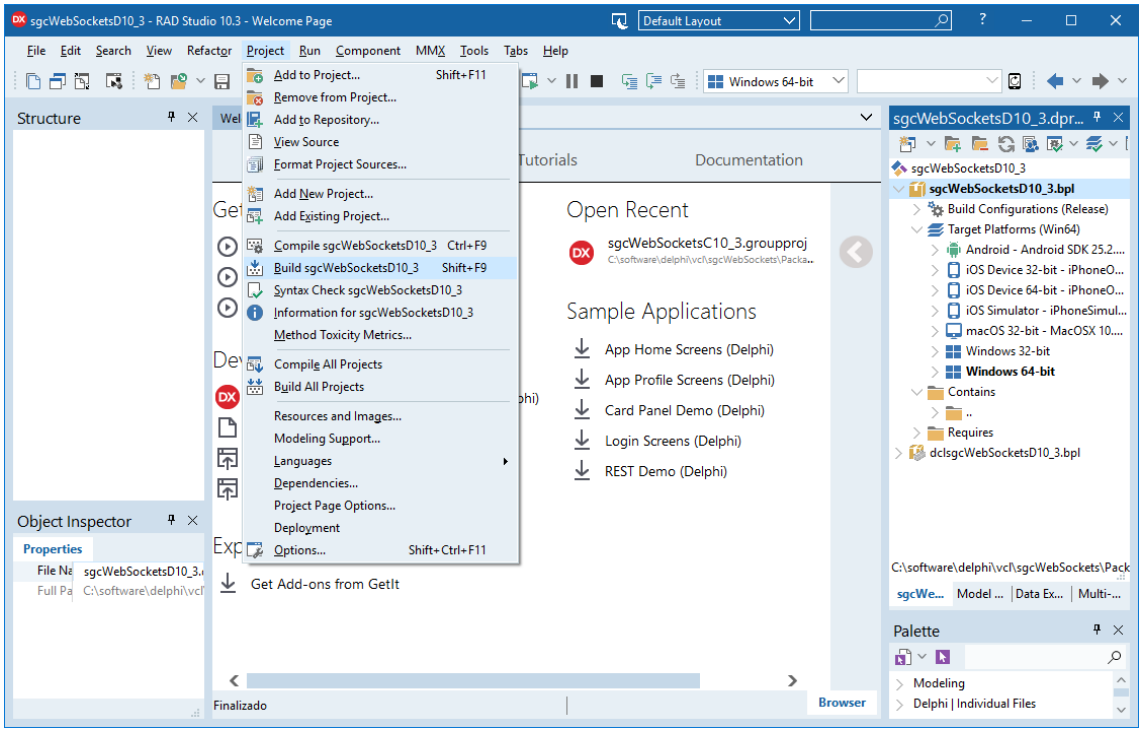
Follow next steps to install sgcWebSockets package, screenshots use Delphi 10.3 version.

1. Open sgcWebSocketsD10_3 group project.

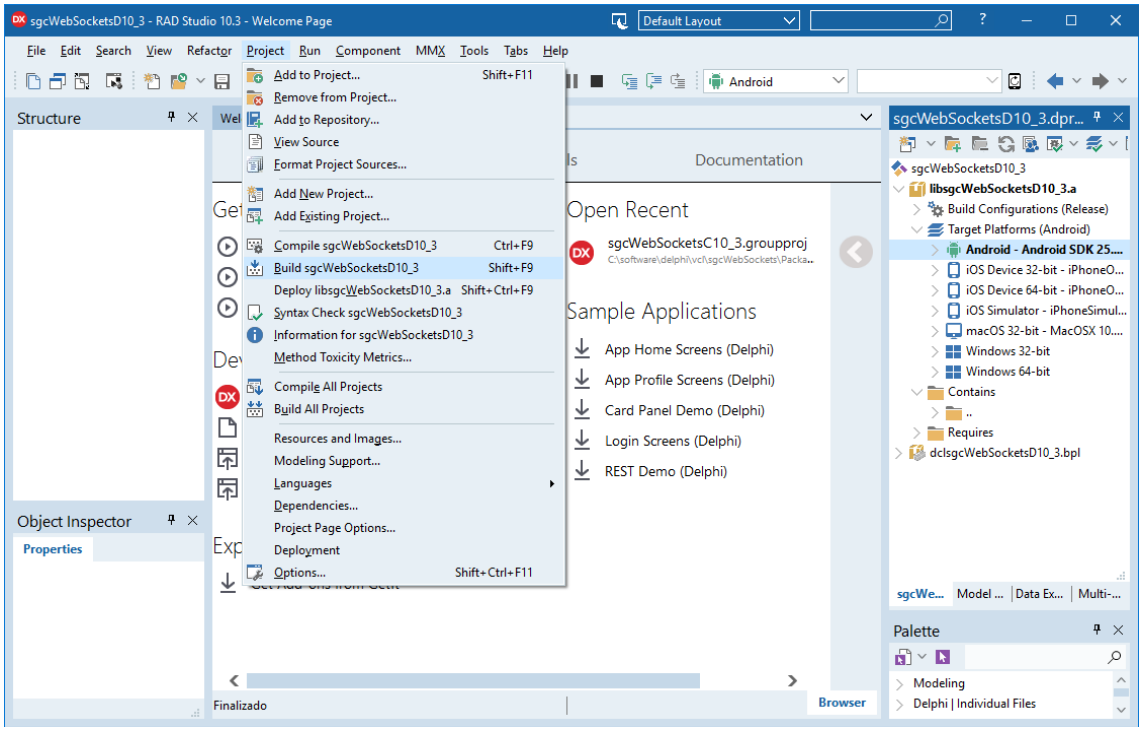


2. Now we must **compile first runtime packages** (name starts with sgcWebSockets). There is one package for every target platform and this depends of Delphi version, so **select target platform one by one and build** every package.

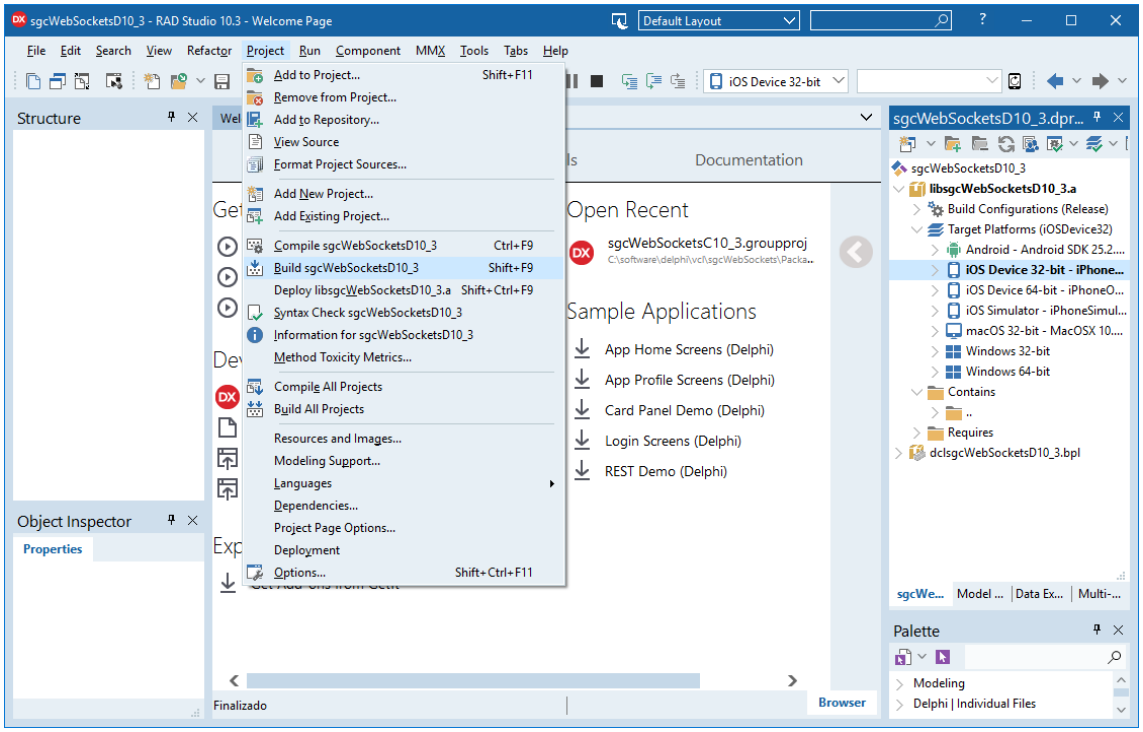
3. Select win64 as Target platform and build package.



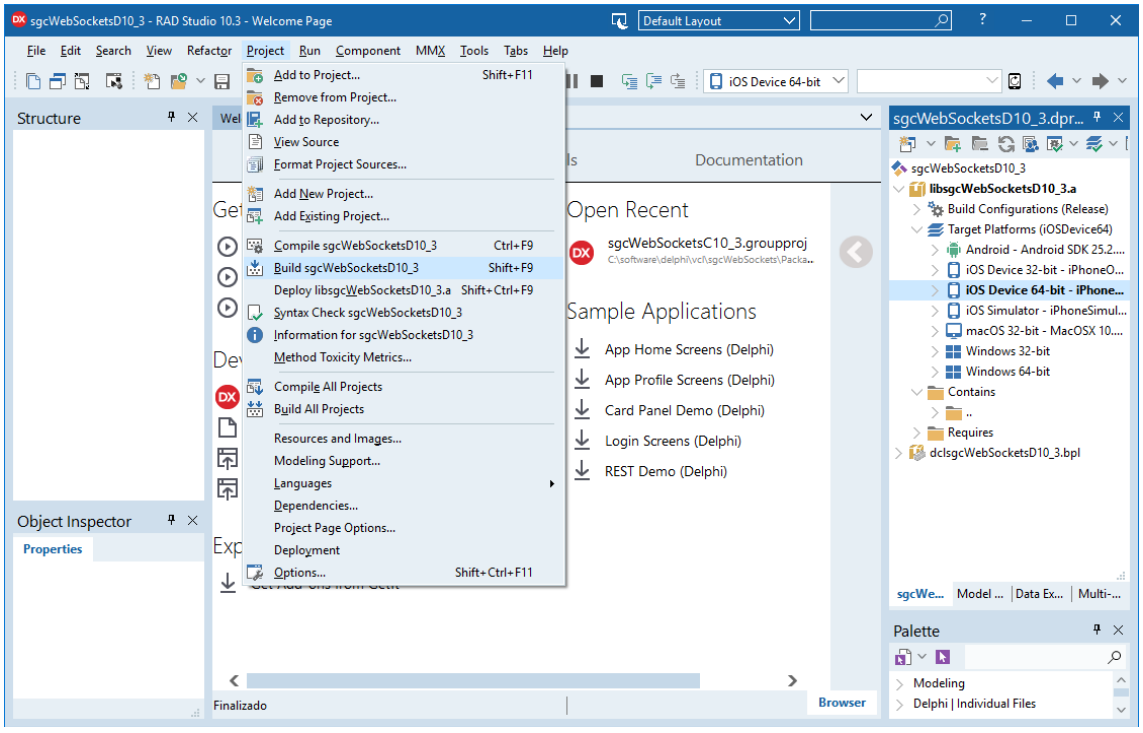
4. Select Android as Target Platform and build package.



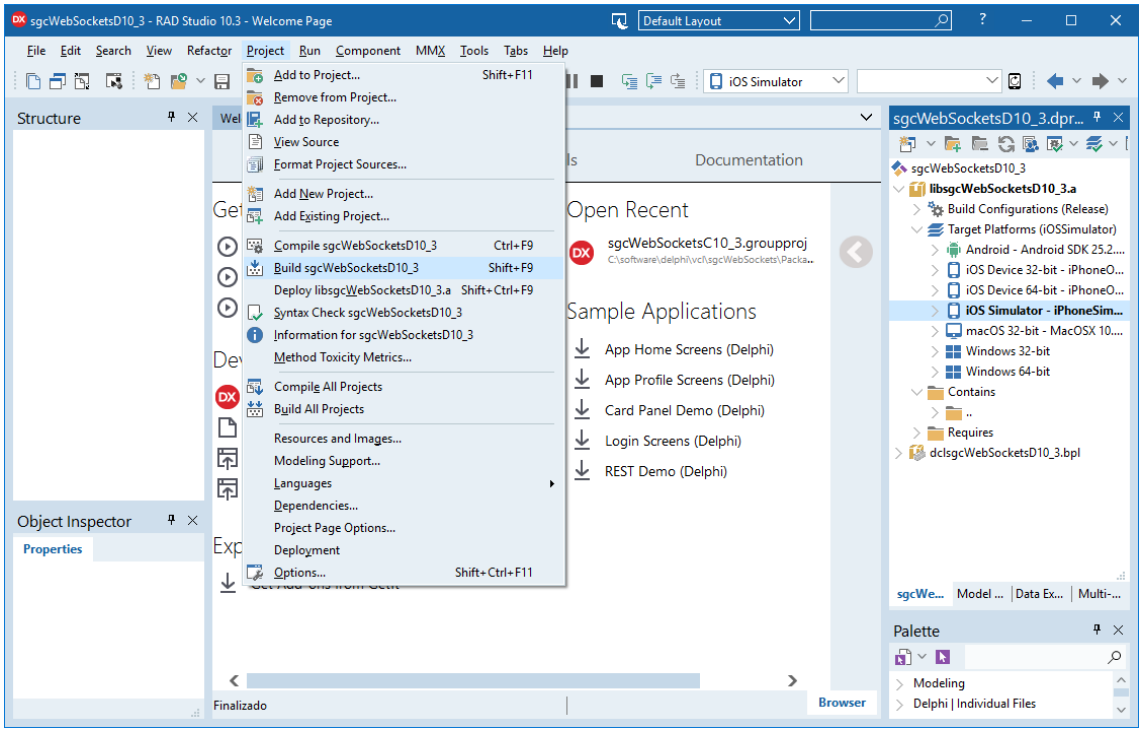
5. Select **iOS Device 32** as Target Platform and build package.



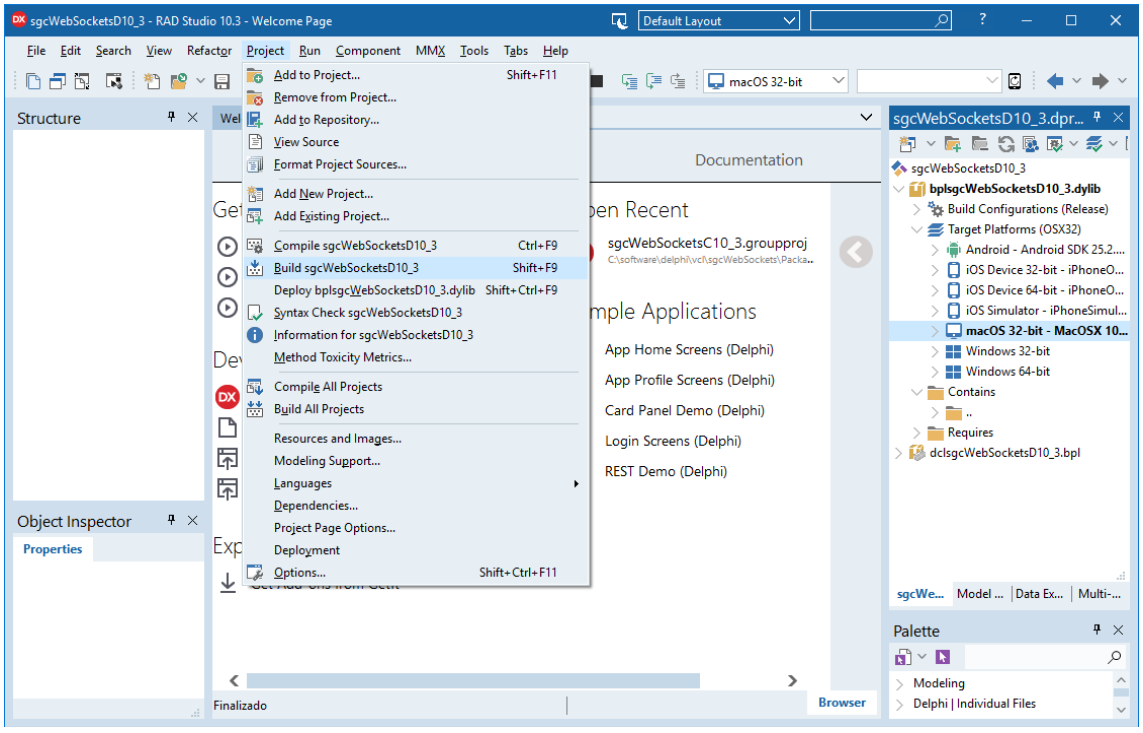
6. Select **iOS Device 64** as Target Platform and build package.



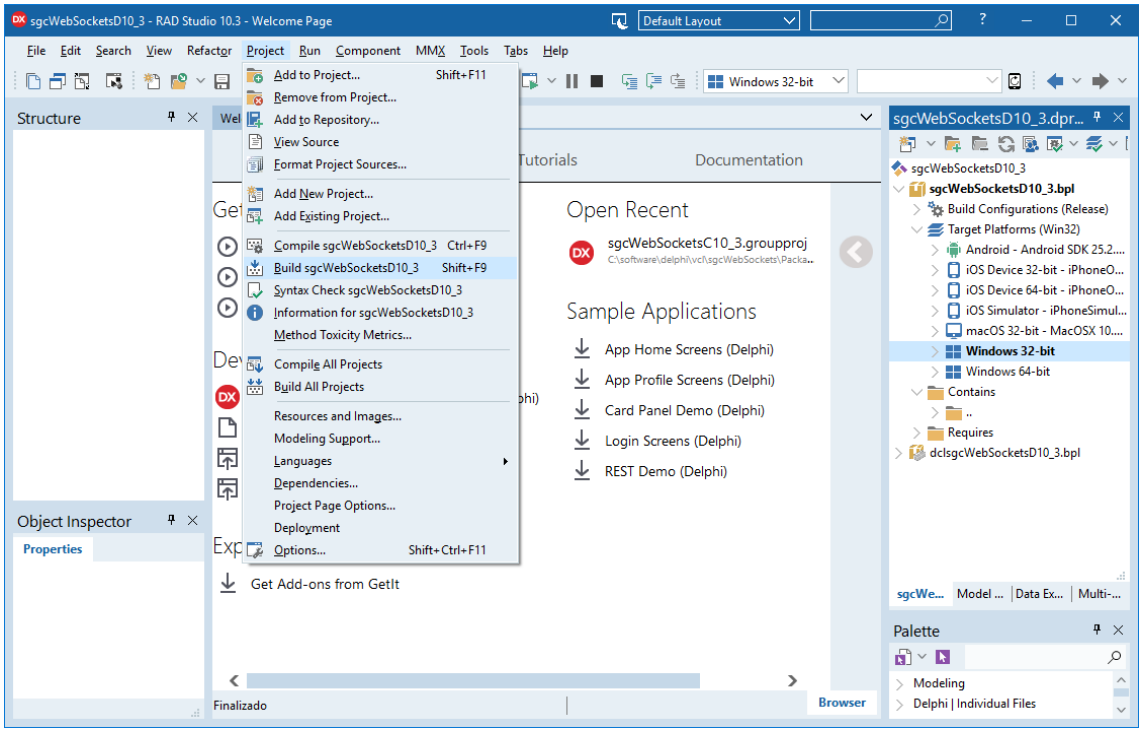
7. Select **iOS Device** Simulator as Target Platform and build package.



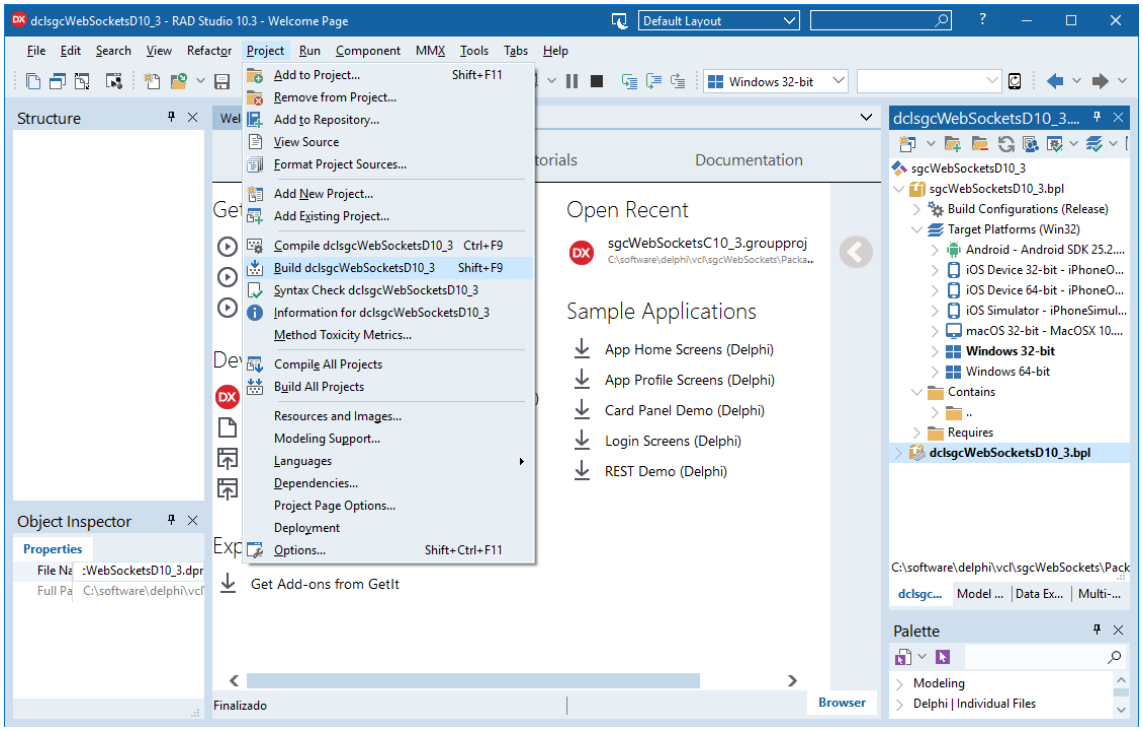
8. Select **MacOS 32** as Target Platform and build package.

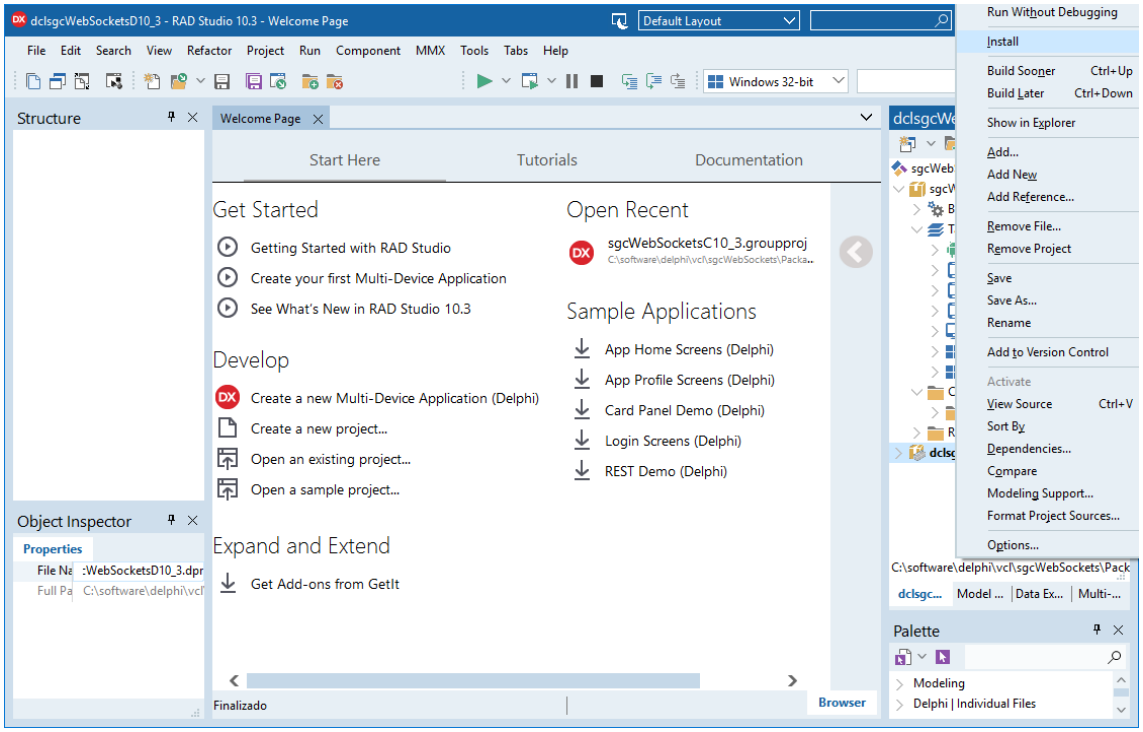


9. Select **Win32** as Target Platform and build package.

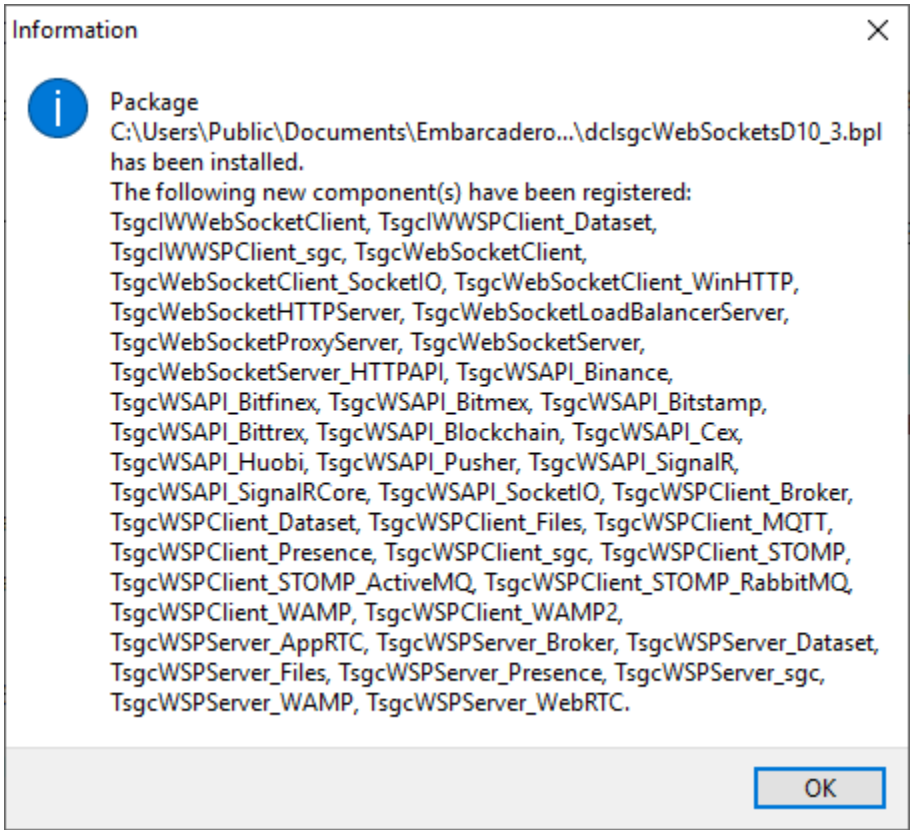


10. Once all runtime packages are compiled, select **design time package** (name starts with dcl) and first **build** and then **install** (design time packages only have Win32 as target platform).





11. If installation is **successful** you will see a message with all components installed.



Install Errors

Sometimes you may get some errors installing components.

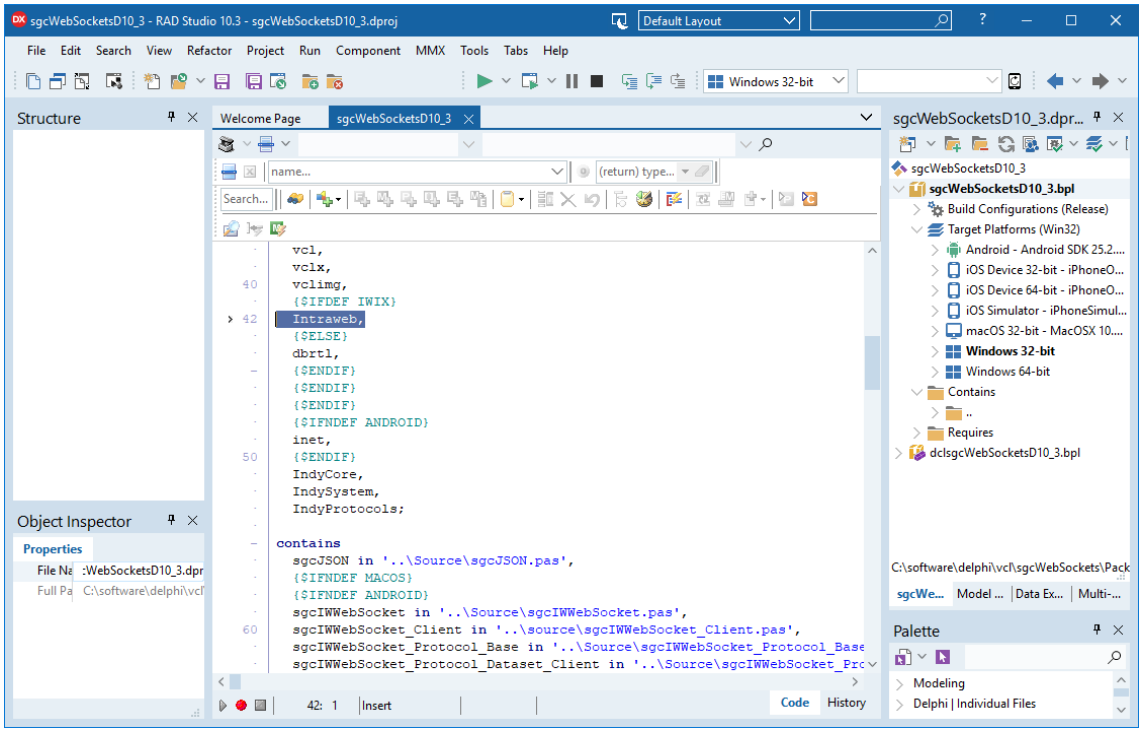
Intraweb package not found

sgcWebsockets is compiled using the **default Intraweb version** provided with Delphi. If you don't have Intraweb installed, you can **modify sgcVer.inc** file (located in Source folder). Search your Delphi version and **comment all compiler defines for Intraweb** (starts with IW).
Example: for Delphi 10.3 comment all compiler defines for Intraweb

```
{$IFDEF VER330} { Delphi  10.3 }
  {$DEFINE D2006}
  {$DEFINE D2007}
  {$DEFINE D2009}
  {$DEFINE D2010}
  {$DEFINE DXE}
  {$DEFINE DXE2}
  {$DEFINE DXE3}
  {$DEFINE DXE4}
  {$DEFINE DXE5}
  {$DEFINE DXE6}
  {$DEFINE DXE7}
  {$DEFINE DXE8}
  {$DEFINE D10}
  {$DEFINE D10_1}
  {$DEFINE D10_2}
  {$DEFINE D10_3}
  {$DEFINE INDY10_1}
  {$DEFINE INDY10_2}
  {$DEFINE INDY10_5_5}
  {$DEFINE INDY10_5_7}
  {$DEFINE INDY10_6}
  {$DEFINE INDY10_6_2_5366}

  {$IFNDEF BCB}
    {$IFNDEF MACOS}
    {$IFNDEF ANDROID}
      {.$DEFINE IWIX}
      {.$DEFINE IWXI}
      {.$DEFINE IWXIV}
    {$ENDIF}
    {$ENDIF}
{$IFNDEF NEXTGEN}
  {$DEFINE SGC_JSON_INTF}
{$ENDIF}
  {$ENDIF}
{$ENDIF}
```

If Intraweb is installed but it's a different version from the default that comes with Delphi, maybe your Intraweb package has a different name. Then open sgcWebSockets runtime package and **change Intraweb name** in project source.



Indy Package not found

sgcWebSockets requires Indy to install components in your IDE. Trial installation is compiled against Indy library provided with Delphi / CBuilder, so if you get a message like this:

> [DCC Fatal Error] dclsgcWebSocketsDX.dpk(31): E2202 Required package 'IndyCore' not found

Most probably you have a **newer Indy version**, so in order to install trial you must delete this version and install built-in indy version using Delphi / CBuilder setup.

If you have full source code, then you only must check:

1. Required Indy packages: IndyCore, IndySystem and IndyProtocols. If you have a newer Indy version, most probably packages have a different name (including version), so access to menu **"Component / Install Packages"** and check which name have Indy packages and change accordingly in the project.

2. sgcWebSockets supports several Indy versions, there are compiler defines to allow compile for every Indy version. Open **sgcVer.inc**, located in the source folder, and change accordingly for your Indy version (is gsIdVersion of IdVers.inc Indy file). Some compiler defines:

```
{$DEFINE INDY10_1}
{$DEFINE INDY10_2}
{$DEFINE INDY10_5_5}
{$DEFINE INDY10_5_7}
{$DEFINE INDY10_6}
{$DEFINE INDY10_6_2_5366}
```

c00000005 ACCESS_VIOLATION in CBuilder

If you compile a project using CBuidler and you get this error, set the following options in your project:

Project > Options > C++ Linker
uncheck "Link with Dynamic RTL"

Project > Options > Packages > Runtime Packages
uncheck "Link with runtime packages"

Unable to find package import: sgcWebSocketsCXXX.bpi in CBuilder Win64

When you compile runtime package for win64, you must compile Release and Debug.

Ambiguous reference System.ZLib.hpp and IdZLib.hpp CBuilder

sgcWebSockets uses Indy for some components and Indy doesn't make use of ZLib unit, uses its own copy of ZLib: IdZLib, IdZLibHeaders... the project is linking to ZLib and indy ZLib units, so when compile, compiler doesn't know which is the correct reference because names are the same. There are 2 solutions:

1. Search where is included a link to System.ZLib.hpp and delete or move after IdZLibHeaders.hpp
2. Use the following conditional defines NO_USING_NAMESPACE_SYSTEM_ZLIB or DELPHIHEADER_NO_IMPLICIT_NAMESPACE_USE in your projects options to avoid the use of System.Zlib.hpp

QuickStart

QuickStart

Let's start with a basic example where we need to create a Server WebSocket and 2 client WebSocket types: Application Client and Web Browser Client.

WebSocket Server

1. Create a new Window Forms Application
2. Drop a TsgcWebSocketServer onto a Form.
3. On Events Tab, Double click OnMessage Event, and type following code:

```
procedure OnMessage(Connection: TsgcWSConnection; const Text: string);
begin
  ShowMessage('Message Received From Client: ' + Text);
end;
```

4. Drop a Button onto the Form, Double Click and type this code:

```
TsgcWebSocketServer1.Active := True;
```

WebSocket Client

1. Create a new Window Forms Application
2. Drop a TsgcWebSocketClient onto a Form and configure Host and Port Properties to connect to Server.
3. Drop a TButton in a Form, Double Click and type this code:

```
TsgcWebSocketClient1.Active := True;
```

4. Drop a Button onto the Form, Double Click and type this code:

```
TsgcWebSocketClient1.WriteData('Hello Server From VCL Client');
```

Web Browser Client

1. Create a new HTML file

2. Open file with a text editor and copy following code:

```
<html>
<head>
<script type="text/javascript"
src="http://host:port/sgcWebSockets.js"></script>
</head>
<body>
```

```
<a href="javascript:var socket = new
sgcWebSocket('ws://host:port');">Open</a>
<a href="javascript:socket.send('Hello Server From Web
Browser');">Send</a>
</body>
</html>
```

You need to replace host and port in this file for your custom Host and Port!!

3. Save File and that's all, you have configured a basic WebSocket Web Browser Client.

How To Use

1. Start Server Application and press button to start WebSocket Server to listen new connections.

2. Start Client Application and press button1 to connect to server and press button2 to send a message. On Server Side, you will see a message with text sent by Client.

3. Open then HTML file with your Web Browser (Chrome, Firefox, Safari or Internet Explorer 10+), press Open to open a connection and press send, to send a message to the server. On Server Side, you will see a message with a text sent by Web Browser Client.

Linux Compiler

Simple Server example (listening on port 5000).

```
program sgcWebSockets_linux;

{$APPTYPE CONSOLE}

{$R *.res}

uses
  System.SysUtils, sgcWebSocket;

var
  oServer: TsgcWebSocketServer;

begin
  try
    oServer := TsgcWebSocketServer.Create(nil);
    oServer.Port := 5000;
    oServer.Active := True;

    while oServer.Active do
      Sleep(10);
  except
    on E: Exception do
      Writeln(E.ClassName, ': ', E.Message);
  end;
```

```
end.
```

Linux (Lazarus)

If you compile a Lazarus project for Linux and you get this message:

```
Semaphore init failed (possibly too many concurrent threads)
```

Just add **cthreads** unit to your project file.

WebBrowser Test

TsgcWebSocketServer implements a built-in Web page where you can test WebSocket Server connection with your favourite Web Browser.

To access to this Test Page, you need to type this URL:

```
http://host:port/sgcWebSockets.html
```

Example: if you have configured your WebSocket Server on IP 127.0.0.1 and uses port 80, then you need to type:

```
http://127.0.0.1:80/sgcWebSockets.html
```

In this page, you can test the following WebSocket methods:

Open
Close
Status
Send

To disable WebBrowser HTML Test pages, just set in
TsgcWebSocketServer.Options.HTMLFiles = false;

Fast Performance Server

TsgcWebSocketServer and TsgcWebSocketHTTPServer are based on Indy library, so every connection is handled by a thread, so if you have 1000 concurrent connections, you will have, at least, 1000 threads to handle these connections. When performance is important, you must do some "tweaks" to increase performance and improve server work. **From sgcWebSockets 4.3.3 Indy servers support IOCP too**, you can read more.

Use the following tips to increase server performance.

1. Set in Server component property **NotifyEvents := neNoSync**. This means that events are raised in the context of connection thread, so there is no synchronization mechanism. If you must access to VCL controls or shared objects, use your own synchronization mechanisms.

2. Set in Server component property **Optimizations.Connections.Enabled := True**. If you plan to have more than 1000 concurrent connections in your server, and you call Server.WriteData method a lot, enable this property. Basically, it saves connections in a cache list where searches are faster than accessing to Indy connections list.

    2.1 CacheSize: is the number of connections stored in a fast cache. Default value = 100.
    2.2 GroupLevel: creates internally several lists split by the first character, so if you have lots of connections, searches are faster. Default value = 1.

3. Set in Server component property **Optimizations.Channels.Enabled := True**. Enabling this property, channels are saved in a list where searches are faster than previous method.

4. Set in Server component property **Optimizations.ConnectionsFree.Enabled := True**. If this property is enabled, every time there is a disconnection, instead of destroying TsgcWSConnection, the object is stored in a List and every X seconds, all objects stored in this list are destroyed.

    4.1 Interval: number of seconds where all disconnected connections stored in a list are destroyed. By default is 60.

5. By default, sgcWebSockets uses **Critical Sections** to protect access to shared objects. But you can use TMonitor or SpinLocks instead of critical sections. Just compile your project with one of the following compiler defines

    3.1 {$DEFINE SGC_SPINLOCKS}
    3.2 {$DEFINE SGC_TMONITOR}

6. Use latest **FastMM4**, you can download from: https://github.com/pleriche/FastMM4
   FastMM4 is a very good memory manager, but sometimes doesn't scale well with multi-threaded applications. Use the following compiler define in your application:

    {$DEFINE UseReleaseStack}

   Then, add FastMM4 as the first unit in your project uses and compile again. For a high concurrent server, you will note an increase in performance.
   This tweak does the following: If a block cannot be released immediately during a FreeMem call the block will be added to a list of blocks that will be freed later, either in the background cleanup thread or during the next call to FreeMem.

Custom Sub-Protocols

A client can request that the server use a specific subprotocol by including the subprotocol name in its handshake. If it is specified, the server needs to include one of the selected subprotocol values in its response for the connection to be established.

In order to create your own subprotocol, you must inherit from TsgcWSProtocol_Client_Base and TsgcWSProtocol_Server_Base in order to create your custom subprotocols.

```
//Client Example Code

unit sgcWebSocket_Protocol_Example_Client;

interface

{$I sgcVer.inc}
{$IFDEF SGC_PROTOCOLS}

uses
  sgcWebSocket_Protocol_Base_Client, Classes, sgcWebSocket_Classes;

type
  TsgcWSProtocol_Example_Client = class(TsgcWSProtocol_Client_Base)
  { from TsgcWSComponent }
  protected
    procedure DoEventConnect(aConnection: TsgcWSConnection); override;
    procedure DoEventMessage(aConnection: TsgcWSConnection; const
Text: string);
        override;
    procedure DoEventDisconnect(aConnection: TsgcWSConnection; Code:
Integer);
        override;
  { from TsgcWSComponent }
  public
    constructor Create(aOwner: TComponent); override;
  end;
{$ENDIF}

implementation

{$IFDEF SGC_PROTOCOLS}

constructor TsgcWSProtocol_Example_Client.Create(aOwner: TComponent);
begin
  inherited;
  // ... here add your protocol name
  FProtocol := 'MyProtocol';
end;

procedure TsgcWSProtocol_Example_Client.DoEventConnect(aConnection:
    TsgcWSConnection);
begin
  inherited;
  // ... add your own code when client connects to server
end;

procedure TsgcWSProtocol_Example_Client.DoEventDisconnect(aConnection:
```

```
    TsgcWSConnection; Code: Integer);
begin
  // ... add your own code when client disconnects from server
  inherited;
end;

procedure TsgcWSProtocol_Example_Client.DoEventMessage(aConnection:
    TsgcWSConnection; const Text: string);
begin
  // ... process messages received from server
  // ... you can send a message to server using WriteData('your
message') method
end;
{$ENDIF}

end.

// Server Example Code

unit sgcWebSocket_Protocol_Example_Server;

interface

{$I sgcVer.inc}
{$IFDEF SGC_PROTOCOLS}

uses
  sgcWebSocket_Protocol_Base_Server, Classes, sgcWebSocket_Classes;

type
  TsgcWSProtocol_Example_Server = class(TsgcWSProtocol_Server_Base)
  { from TsgcWSComponent }
  protected
    procedure DoEventConnect(aConnection: TsgcWSConnection); override;
    procedure DoEventMessage(aConnection: TsgcWSConnection; const
Text: string);
        override;
    procedure DoEventDisconnect(aConnection: TsgcWSConnection; Code:
Integer);
        override;
  { from TsgcWSComponent }
  public
    constructor Create(aOwner: TComponent); override;
  end;
{$ENDIF}

implementation

{$IFDEF SGC_PROTOCOLS}
constructor TsgcWSProtocol_Example_Server.Create(aOwner: TComponent);
begin
  inherited;
  // ... here add your protocol name
  FProtocol := 'MyProtocol';
end;

procedure TsgcWSProtocol_Example_Server.DoEventConnect(aConnection:
    TsgcWSConnection);
begin
  inherited;
  // ... add your own code when a client connects to server
```

```
end;

procedure TsgcWSProtocol_Example_Server.DoEventDisconnect(aConnection:
    TsgcWSConnection; Code: Integer);
begin
  // ... add your own code when a client disconnects from server
  inherited;
end;

procedure TsgcWSProtocol_Example_Server.DoEventMessage(aConnection:
    TsgcWSConnection; const Text: string);
begin
  inherited;
  // ... process messages received from clients
  // ... you can answer to client using WriteData(aConnection.Guid,
'your message') method
  // ... you can send a message to all clients using BroadCast('your
message') method
end;
{$ENDIF}

end.

//Implementation
// Once your custom subprotocol is implemented, then you only need to
assign to your Client or Server websocket component. Example:

procedure InitalizeClient;
var
  oClient: TsgcWebSocketClient;
  oProtocol: TsgcWSProtocol_Example_Client;
begin
  oClient := TsgcWebSocketClient.Create(nil);
  oProtocol := TsgcWSProtocol_Example_Client.Create(nil);
  oProtocol.Client := oClient;
end;


procedure InitalizeServer;
var
  oServer: TsgcWebSocketServer;
  oProtocol: TsgcWSProtocol_Example_Server;
begin
  oClient := TsgcWebSocketServer.Create(nil);
  oProtocol := TsgcWSProtocol_Example_Server.Create(nil);
  oProtocol.Server := oServer;
end;
```

OpenSSL

OpenSSL is a software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end. It is widely used by Internet servers, including the majority of HTTPS websites.

This library is required by components based on Indy Library when a secure connection is needed. If your application requires OpenSSL, you must have necessary files in your file system before deploying your application:

Platform	API 1.0	API 1.1	Static/Dynamic Linking
Windows (32-bit and 64-bit)	libeay32.dll and ssleay32.dll	libcrypto-1_1.dll and libssl-1_1.dll	Dynamic
OSX	libcrypto.dylib, libssl.dylib	libcrypto.1.1.dylib, libssl.1.1.dylib	Dynamic
iOS Device (32-bit and 64-bit)	libcrypto.a and libssl.a	libcrypto.a and libssl.a	Static
iOS Simulator	libcrypto.dylib, libssl.dylib	libcrypto.1.1.dylib, libssl.1.1.dylib	Dynamic
Android Device	libcrypto.so, libssl.so	libcrypto.so, libssl.so	Dynamic

Windows

There is one version for 32 bits and another for 64 bits. You must copy these libraries in the same folder where is your application or in your system path.
If your Operating System is Windows 32 bits, just copy in System32 folder.
If your Operating System is Windows 64 bits, copy 64 bits version in System32 folder and 32 bits version in SysWow64 folder.

API 1.0

Requires the following libraries:

- libeay32.dll
- ssleay32.dll

You can download from: https://slproweb.com/products/Win32OpenSSL.html

API 1.1

Requires the following libraries:

- libcrypto-1_1.dll
- libssl-1_1.dll

You can download from: https://slproweb.com/products/Win32OpenSSL.html

OSX

Newer versions of OSX doesn't include openssl libraries or are too old, so you must deploy with your application. Deploy these libraries using following steps:

- Open Project/Deployment in your project.
- Add required libraries.
- Set RemotePath = 'Contents\Macos\'.
- Call this method IdOpenSSLSetLibPath(System.SysUtils.GetCurrentDir) in initialization section.

API 1.0

Requires the following libraries:

- libcrypto.dylib
- libssl.dylib

API 1.1

Requires the following libraries:

- libcrypto-1_1.dll
- libssl-1_1.dll

There is one version for 32 bits and another for 64 bits. You must copy these libraries in the same folder where is your application or in your system path.
If your Operating System is Windows 32 bits, just copy in System32 folder.
If your Operating System is Windows 64 bits, copy 64 bits version in System32 folder and 32 bits version in SysWow64 folder.

iOS

To install OpenSSL in a 32-bit or 64-bit iOS device, you must copy the libcrypto.a and libssl.a SSL library files to your system. Download the .zip iOS OpenSSL, extract it and find the .a files in the \lib directory. You must copy the libcrypto.a and libssl.a SSL library files to these directories:

- C:\Program Files (x86)\Embarcadero\Studio\20.0\lib\iosDevice<architecture>\debug
- C:\Program Files (x86)\Embarcadero\Studio\20.0\lib\iosDevice<architecture>\release

Modify **IdCompilerDefines.inc** and enable SGC_OPENSSL_API_1_1 in IOS section:

```
{$IFDEF IOS}
  {$DEFINE HAS_getifaddrs}
  {$DEFINE USE_OPENSSL}
  {$IFDEF CPUARM}
    // RLebeau: For iOS devices, OpenSSL cannot be used as an
external library,
    // it must be statically linked into the app.  For the iOS
simulator, this
    // is not true.  Users who want to use OpenSSL in iOS device
apps will need
    // to add the static OpenSSL library to the project and then
include the
    // IdSSLOpenSSLHeaders_static unit in their uses clause. It
hooks up the
    // statically linked functions for the IdSSLOpenSSLHeaders
unit to use...
    {$DEFINE STATICLOAD_OPENSSL}
// sgc--> enable for openssl API 1.1
{$DEFINE SGC_OPENSSL_API_1_1}
  {$ENDIF}
{$ENDIF}
```

Android

Newer versions of Android doesn't include openssl libraries or are too old, so you must deploy with your application. Deploy these libraries using following steps:

- Open Project/Deployment in your project.
- Add required libraries.
- Set RemotePath = '.\assets\internal'.
- Call this method IdOpenSSLSetLibPath(TPath.GetDocumentsPath) in initialization section.

API 1.0

Requires the following libraries:

- libcrypto.so
- libssl.so

API 1.1

Requires the following libraries:

- libcrypto.so
- libssl.so

Topics

General

WebSocket Events

WebSocket connections have the following events:

OnConnect
The event raised when a new connection is established.

OnDisconnect
The event raised when a connection is closed.

OnError
The event raised when a connection has any error.

OnMessage
The event raised when a new text message is received.

OnBinary
The event raised when a new binary message is received.

By default, sgcWebSockets uses an **asynchronous** mechanism to raise these events, when any of these events is raised internally, it queues this message and is dispatched by the operating system when is allowed. This behaviour can be modified using a property called **NotifyEvents**, by default **neAsynchronous** is selected, if **neNoSync** is checked then events will be raised without synchronizing with the main thread (if you need to update any VCL control or access to shared resources, then you will need to implement your own synchronizing method).

neNoSync is recommended when:

1. You need to handle a lot of messages on a very short period of time.
2. Your project is built for command line (if you don't set neNoSync, you won't get any event).
3. Your project is a library.

If no, then you can set default property to **neAsynchronous**.

WebSocket Parameters Connection

Supported by

TsgcWebSocketClient
Java script

Sometimes is useful to pass parameters from client to server when a new WebSocket the connection is established. If you need to pass some parameters to the server, you can use the following property:

Options / Parameters

By default, is set to '/', if you need to pass a parameter like id=1, you can set this property to '/?id=1'

On Server Side, you can handle client parameters using the following parameter:

```
procedure WSServerConnect(Connection: TsgcWSConnection);
begin
  if Connection.URL = '/?id=1' then
    HandleThisParameter;
end;
```

Using Javascript, you can pass parameters using connection url, example:

```
<script src="http://localhost/sgcWebSockets.js"
type="text/javascript"></script>
<script type="text/javascript">var socket = new
sgcWebSocket('ws://localhost/?id=1');</script>
```

Using inside a DLL

If you need to work with Dynamic Link Libraries (DLL) and sgcWebSockets (or console applications), **NotifyEvents** property needs to be set to **neNoSync**.

Features

Authentication

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

Java script (*only URL Authentication is supported)

WebSockets Specification doesn't have any authentication method and Web Browsers implementation don't allow to send custom headers on new WebSocket connections.

To enable this feature you need to access to the following property:

Authentication/ Enabled

sgcWebSockets implements 3 different types of WebSocket authentication:

Session: client needs to do an HTTP GET passing username and password, and if authenticated, server response a Session ID. With this Session ID, client open WebSocket connection passing as a parameter. You can use a normal HTTP request to get a session id using and passing user and password as parameters

```
http://host:port/sgc/req/auth/session/:user/:password
```

example: (user=admin, password=1234) -->
http://localhost/sgc/req/auth/session/admin/1234

This returns a token that is used to connect to server using WebSocket connections:

ws://localhost/sgc/auth/session/:token

URL: client open WebSocket connection passing username and password as a parameter.

```
ws://host:port/sgc/auth/url/username/password
```

example: (user=admin, password=1234) -->
http://localhost/sgc/auth/url/admin/1234

Basic: implements Basic Access Authentication, only applies to VCL Websockets (Server and Client) and HTTP Requests (client Web Browsers don't implement this type of authentication). When a client tries to connect, it sends a header using AUTH BASIC specification.

You can define a list of Authenticated users, using **Authentication/ AuthUsers** property. You need to define every item following this schema: user=password. Example:

admin=admin
user=1234

....

There is an event called **OnAuthentication** where you can handle authentication if the user is not in AuthUsers list, client doesn't send an authorization request... You can check User and Password params and if correct, then set Authenticated variable to True. example:

```
procedure WSServerAuthentication(Connection: TsgcWSConnection; aUser,
aPassword: string; var Authenticated: Boolean);
begin
  if (aUser = 'John') and (aPassword = '1234') then
    Authenticated := True;
end;
```

Secure Connections

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient
Web Browsers

SSL support is based on Indy implementation, so you need to deploy openssl libraries in order to use this feature.
TsgcWebSocketClient supports Microsoft SChannel, so there is no need to deploy openssl libraries for windows 32 and 64 bits if SChannel option is selected in WebSocket Client.

Server Side

To enable this feature, you need to enable the following property:

SSL/ Enable

There are other properties that you need to define:

SSLOptions/ CertFile/ KeyFile/ RootCertFile: you need a certificate in .PEM format in order to encrypt websocket communications.

SSLOptions/ Password: this is optional and only needed if the certificate has a password.

SSLOptions/ Port: port used on SSL connections.

Client Side

To enable this feature, you need to enable the following property:

TLS/ Enable

OpenSSL

By default, client and server components based on Indy make use of openSSL libraries when connect to secure websocket servers.
Indy only supports 1.0.2 openssl API so API 1.1 is not supported. If you compile sgcWebSockets with our custom Indy library you can make use of API 1.1 and select TLS 1.3 version. Just select in OpenSSL_Options properties which openSSL API would you use:

- oslAPI_1_0: it's default indy API, you can use standard Indy package with openssl 1.0.2 libraries.
- oslAPI_1_1: only select if you are compiling sgcWebSockets with our custom Indy library. Will use openssl 1.1.1 libraries.

Events

There are 2 events which can be used to customize your SSL settings:

OnSSLGetHandler

This event is raised before SSL handler is created, you can create here your own SSL Handler (needs to be inherited from TIdServerIOHandlerSSLBase or TIdIOHandlerSSLBase) and set the properties needed

```
procedure OnServerSSLGetHandler(Sender: TObject; aType: TwsSSLHandler;
var aSSLHandler:
TIdServerIOHandlerSSLBase);
begin
  aSSLHandler := TCustomSSLHandler.Create(nil);
  ...
end;
```

OnSSLAfterCreateHandler

If no custom SSL object has been created, it creates by default using OpenSSL handler. You can access to SSL Handler properties and modify if needed

```
procedure OnSSLAfterCreateHandler(Sender: TObject; aType:
TwsSSLHandler; aSSLHandler:
TIdServerIOHandlerSSLBase);
begin
  TIdServerIOHandlerSSLOpenSSL(aSSLHandler).SSLOptions.Method :=
sslvTLSv1_2;
end;
```

Microsoft SChannel

From sgcWebSockets 4.2.6 you can use SChannel instead of openssl (only for windows from Windows 7+). This means there is no need to deploy openssl libraries. TLS 1.0 is supported from windows 7 but if you need more modern implementations like TLS 1.2 in Windows 7 you must enable TLS 1.1 and TLS 1.2 in Windows Registry.

HeartBeat

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

On Server components, automatically sends a ping to all active WebSocket connections every x seconds.

On Client components, automatically sends a ping to the server every x seconds.

WatchDog

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

On Server components, automatically restart server after unexpected disconnection.

On Client components, automatically reconnect to server after unexpected disconnection.

Logs

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

This is a useful feature that allows debugging WebSocket connections, to enable this, you need to access to the following property:

LogFile/ Enabled

Once enabled, every time a new connection is established it will be logged in a text file. On Server component, if the file it's not created it will be created but with you can't access until the server is closed, if you want to open log file while the server is active, log file needs to be created before start server.

Example:

```
127.0.0.1:49854 Stat Connected.

127.0.0.1:49854 Recv 09/11/2013 11:17:03: GET / HTTP/1.1
Upgrade: websocket
Connection: Upgrade
Host: 127.0.0.1:5414
Origin: http://127.0.0.1:5414
Pragma: no-cache
Cache-Control: no-cache
Sec-WebSocket-Key: 1n598ldHs9SdRfxUK8u4Vw==
Sec-WebSocket-Version: 13
Sec-WebSocket-Extensions: x-webkit-deflate-frame

127.0.0.1:49854 Sent 09/11/2013 11:17:03: HTTP/1.1 101 Switching
Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: gDuzFRzwHBc18P1CfinlvKv1BJc=

127.0.0.1:49854 Stat Disconnected.
0.0.0.0:0 Stat Disconnected.
```

HTTP

Supported by

TsgcWebSocketHTTPServer

TsgcWebSocketHTTPServer is a component that allows handling WebSocket and HTTP connections using the SAME port. Is very useful when you need to set up a server where only HTTP port is enabled (usually 80 port). This component supports all TsgcWeBSocketServer features and allows to serve HTML pages.

You can **serve HTML pages statically**, using **DocumentRoot** property, example: if you save test.html in directory "C:\inetpub\wwwroot", and you set **DocumentRoot** to "C:\inetpub\wwwroot". If a client tries to access to test.html, it will be served automatically, example:

http://localhost/test.html

Or you can **serve HTML or other resources dynamically** by code, to do this, there is an event called **OnCommandGet** that is fired every time a client requests a new HTML page, image, javascript file... Basically, you need to check which document is requesting client (using ARequestInfo.Document) and send a response to client (using AResponseInfo.ContentText where you send response content, AResponse.ContentType which is the type of response and a AResponseInfo.ResponseNo with a number of response code, usually is 200), example:

```
procedure WSServerCommandGet(AContext: TIdContext; ARequestInfo:
TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
begin
  if ARequestInfo.Document = '/myfile.js' then
  begin
    AResponseInfo.ContentText := '<script
type="text/javascript">alert("Hello!");</script>';
    AResponseInfo.ContentType := 'text/javascript';
    AResponseInfo.ResponseNo := 200;
  end
end;
```

Broadcast and Channels

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer

Broadcast method by default send message to **all clients connected**, but you can use **channels** argument to filter and **only broadcast message to clients subscribed** to a channel.

Example: your server has 2 types of connected clients, desktop and mobile devices, so you can create 2 channels "desktop" and "mobile".

If you can identify in OnConnect event of server if a client is mobile, you can do something like following.

```
procedure OnServerConnect(Connection: TsgcWSConnection);
begin
  if desktop then
    TsgcWSConnectionServer(Connection).DoSubscribe('desktop');
end;
```

First cast Connection to TsgcWSConnectionServer to access subscription methods and if fits your filter, will be subscribed to desktop channel. Subscription to a channel can be done in any event, example, you can ask to client to tell you if it's mobile or not and send a message from client to server with info about client. Then you can only broadcast to desktop connections:

```
Server.Broadcast('Your text message', 'desktop');
```

If you have 100 connections and 30 are mobile, message will be only sent to other 70.

Bindings

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer

Usually, Servers have more than one IP, if you enable a WebSocket Server and set listening port to 80, when the server starts, tries to listen port 80 of ALL IP, so if you have 3 IP, it will block port 80 of each IP's.

Bindings allow defining which exact IP and Port are used by the Server. Example, if you need to listen on port 80 for IP 127.0.0.1 (internal address) and 80.254.21.11 (public address), you can do this before the server is activated:

```
With WSServer.Bindings.Add do
begin
  Port := 80;
  IP := '127.0.0.1';
end;
With WSServer.Bindings.Add do
begin
  Port := 80;
  IP := '80.254.21.11';
end;
```

Compression

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient
Web Browsers like Chrome

This is a feature that works very well when you need to send a lot of data, usually using a binary message, because it compresses WebSocket message using protocol "PerMessage_Deflate" which is supported by some browsers like Chrome.

To enable this feature, you need to activate the following property:

Extensions/ PerMessage_Deflate / Enabled

When a client tries to connect to a WebSocket Server and this property is enabled, it sends a header with this property enabled, if Server has activated this feature, it sends a response to the client with this protocol activated and all messages will be compressed, if Server doesn't have this feature, then all messages will be sent without compression.

On Web Browsers, you don't need to do anything, if this extension is supported it will be used automatically, if not, then messages will be sent without compression.

If WebSocket messages are small, is better don't enable this property because it consumes cpu cycle to compress/decompress messages, but if you are using a big amount of data, you will notify and increase on messages exchange speed.

Flash

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer

WebSockets are supported natively by a wide range of web browsers (please check http://caniuse.com/websockets), but there are some old versions that don't implement WebSockets (like Internet Explorer 6, 7, 8 or 9). You can enable **Flash Fallback** for all these browsers that don't implement WebSockets.

Almost all other or older browser support Flash installing Adobe Flash Player. To Support Flash connection, you need to **open port 843** on your server because Flash uses this port for security reasons to check for cross-domain-access. If port 843 is not reachable, waits 3 seconds and tries to connect to Server default port.

Flash is only applied if the Browser doesn't support WebSockets natively. So, if you enable Flash Fallback on the server side, and Web Browser supports WebSockets natively, it will still use WebSockets as transport.

To enable Flash Fallback, you need to access to **FallBack / Flash** property on the server and **enable** it. There are 2 properties more:

1. Domain: if you need to restrict flash connections to a single/multiple domains (by default all domains are allowed). Example: This will allow access to domain swf.example.com

```
swf.example.com
```

2. Ports: if you need to restrict flash connections to a single/multiple ports (by default all ports are allowed). Example: This will allow access to ports 123, 456, 457, and 458

```
123,456-458
```

Flash connections only support Text messages, binary messages are not supported.

Custom Objects

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient
TsgcWebSocketClient_SocketIO

Every time a new WebSocket connection is established, sgcWebSockets creates a TsgcWSConnection class where you can access to some properties like identifier, bytes received/sent, client IP... and there is a property called **Data** where you can store objects in memory like database access, session objects...

```
//You can create a new class called MyClass and create some
properties, example:
TMyClass = class
private
  FRegistered: Boolean;
  FUser: String;
public
  property Registered: Boolean read FRegistered write FRegistered;
  property User: String read FUser write FUser;
end;

// Then, when a new client connects, OnConnect Event, create a new
TMyClass and Assign to Data:
procedure WSServerConnect(Connection: TsgcWSConnection);
begin
  Connection.Data := TMyClass.Create;
end;

// Every time a new message is received by the server, you can access
your custom object using Connection.Data property.
procedure WSServerMessage(Connection: TsgcWSConnection; const Text:
string);
begin
  if TMyClass(Connection.Data).Registered then
    DoSomeStuff();
end;

// When a connection is closed, you may free your object:
procedure TfrmServerChat.WSServerDisconnect(Connection:
TsgcWSConnection; Code: Integer);
var
  oMyClass: TMyClass;
begin
  oMyClass := TMyClass(Connection.Data);
  if Assigned(oMyClass) then
  begin
    oMyClass.Free;
    Connection.Data := nil;
  end;
end;
```

IOCP

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer

***Requires custom Indy version.**

IOCP for Windows is an API which allows handles thousands of connections using a limited pool of threads instead of using a thread for connection like Indy by default does.
To enable IOCP for Indy Servers, Go to **IOHandlerOptions** property and select **iohIOCP** as IOHandler Type.

```
Server.IOHandlerOptions.IOHandlerType := iohIOCP;
Server.IOHandlerOptions.IOCP.IOCPThreads := 8;
Server.IOHandlerOptions.IOCP.WorkOpThreads := 32;
```

IOCPThreads are the threads used for IOCP asynchronous requests (overlapped operations) and WorkOpThreads are threads used to process these asynchronous requests (read and write bytes).
Maximum value of WorkOpThreads is 64, but you must adjust this value accordingly to your number of physical processors * 2, so if you have a cpu with 16 processors, set a WorkOpThreads value of 32.

Enabling IOCP for windows servers is recommended when you need handle thousands of connections, if your server is only handling 100 concurrent connections at maximum you can stay with default Indy Thread model.

OnDisconnect event not fired

IOCP works differently from default indy IOHandler. With default indy IOHandler, every connection runs in a thread and these thread are running all the time and checking if connection is active, so if there is a disconnection, it's notified in a short period of time.

IOCP works differently, there is a thread pool which handles all connections, instead of 1 thread = 1 connection like indy does by default. For IOCP, the only way to detect if a connection is still alive is trying to write in socket, if there is any error means that connection is closed. There are 2 options to detect disconnections:

1. If you use **TsgcWebSocketClient**, you can enable it in Options property, **CleanDisconnect := True** (by default is disabled). If it's enabled, before the client disconnects it sends a message informing the server about disconnection, so the server will receive this message and the OnDisconnect event will be raised.
2. You can enable **heartbeat** on the **server** side, for example every 60 seconds, so it will try to send a ping to all clients connected and if there is any client disconnected, OnDisconnect will be called.

ALPN

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

***Requires custom Indy version.**

Application-Layer Protocol Negotiation (ALPN) is a Transport Layer Security (TLS) extension for application-layer protocol negotiation. ALPN allows the application layer to negotiate which protocol should be performed over a secure connection in a manner that avoids additional round trips and which is independent of the application-layer protocols. It is needed by secure HTTP/2 connections, which improves the compresslion of web pages and reduces their latency compared to HTTP/1.x.

Client

You can configure in TLSOptions.ALPNProtocols, which protocols are supported by client. When client connects to server, these protocols are sent on the initial TLS handshake 'Client Hello', and it lists the protocols that the client supports, and server select which protocol will be used, if any.

You can get which protocol has been selected by server accessing to ALPNProtocol property of TsgcWSConnectionClient.

Server

```
When there is a new TLS connection, OnSSLALPNSelect event is called,
here you can access to a list of protocols which are supported by
client and server can select which of them is supported.


If there is no support for any protocol, aProtocol can be left empty.
```

```
// Client
procedure OnClientConnect(Connection: TsgcWSConnection);
var
  vProtocol: string;
begin
  vProtocol := TsgcWSConnectionClient(Connection).ALPNProtocol;
end;

// Server
procedure OnSSLALPNSelect(Sender: TObject; aProtocols: TStringList;
var aProtocol: string);
var
  i: integer;
begin
  for i := 0 to aProtocols.count - 1 do
  begin
    if aProtocols[i] = 'h2' then
    begin
```

```
      aProtocol := 'h2';
      break;
    end;
  end;
end;
```

Quality Of Service

Supported by

TsgcWSPServer_sgc
TsgcWSPClient_sgc
TsgcWSPClient_MQTT
Java script

SGC Default Protocol and MQTT implements a QoS (Quality of Service) for message delivery, there are 3 different types:

Level 0: "At most once", where messages are delivered according to the best efforts of the underlying TCP/IP network. Message loss or duplication can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after.

Level 1: "At least once", where messages are assured to arrive but duplicates may occur.

Level 2: "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied.

Level 0

The message is delivered according to the best efforts of the underlying TCP/IP network. A response is not expected and no retry semantics are defined in the protocol. The message arrives at the server either once or not at all.

The table below shows the QoS level 0 protocol flow.

Client	Message and direction	Server
QoS = 0	PUBLISH ---------->	**Action:** Publish a message to subscribers

Level 1

The receipt of a message by the server is acknowledged by a ACKNOWLEDGEMENT message. If there is an identified failure of either the communications link or the sending device or the acknowledgement message is not received after a specified period of time, the sender resends the message. The message arrives at the server at least once.

A message with QoS level 1 has a Message ID in the message.

The table below shows the QoS level 1 protocol flow.

Client	Message and direction	Server
QoS = 1	PUBLISH	**Actions:**

Message ID = x **Action:** Store message	---------->	• Store message • Publish a message to subscribers • Delete message
Action: Discard message	ACKNOWLEDGEMENT <----------	

If the client does not receive an ACKNOWLEDGMENT message (either within a time period defined in the application, or if a failure is detected and the communications session is restarted), the client may resend the PUBLISH message.

Level 2

Additional protocol flows above QoS level 1 ensure that duplicate messages are not delivered to the receiving application. This is the highest level of delivery, for use when duplicate messages are not acceptable. There is an increase in network traffic, but it is usually acceptable because of the importance of the message content.

A message with QoS level 2 has a Message ID in the message.

The table below shows the QoS level 2 protocol flow. There are two semantics available for how a PUBLISH flow should be handled by the recipient.

Client	Message and direction	Server
QoS = 2 Message ID = x **Action:** Store message	PUBLISH ---------->	**Action:** Store message
	PUBREC <----------	Message ID = x
Message ID = x	PUBREL ---------->	**Actions:** • Publish a message to subscribers • Delete message
Action: Discard message	ACKNOWLEDGEMENT <----------	Message ID = x

If a failure is detected, or after a defined time period, the protocol flow is retried from the last unacknowledged protocol message. The additional protocol flows to ensure that the message is delivered to subscribers once only.

Queues

Supported by

TsgcWSPServer_sgc
TsgcWSPClient_sgc
Java script

SGC Default Protocol implements Queues to add persistence to published messages (it's only available for **Published messages**)

Level 0: Messages are not queued on Server

Level 1: only last message is queued on Server, and is sent every time a client subscribes to a new channel or connects to the server.

Level 2: All messages are queued on Server, and are sent every time a client subscribes to a new channel or connects to the server.

Level 0

The message is not queued by Server

The table below shows the Queue level 0 protocol flow.

Client	Message and direction	Server
Queue = 0	PUBLISH ---------->	**Action:** Publish a message to subscribers

Level 1

A message with Queue level 1 is stored on the server and if there are other messages stored for this channel, are deleted.

The table below shows the Queue level 1 protocol flow.

Client	Message and direction	Server
Queue = 1	PUBLISH ---------->	**Actions:** • Deletes All messages of this channel • Store last message by Channel
Action: Process message	NOTIFY <----------	**Action:** Every time a new client subscribes to this channel, the last message is sent.

This is useful where publishers send messages on a "report by exception" basis, where it might be some time between messages. This allows new subscribers to instantly receive data with the retained, or Last Known Good, value.

Level 2

All messages with Queue level 2 are stored on the server.

The table below shows the Queue level 2 protocol flow.

Client	Message and direction	Server
Queue = 2	PUBLISH --------->	**Action:** Store message
Action: Process message	NOTIFY <---------	**Action:** Every time a new client subscribes to this channel, ALL Messages are sent.

Transactions

Supported by

TsgcWSPServer_sgc
TsgcWSPClient_sgc
Java script

sgcWebSockets SGC Protocol supports transactional messaging, when a client commits a transaction, all messages sent by the client are processed on the server side. There are 3 methods called by the client:

StartTransaction

Creates a New Transaction on the server side and all messages that are sent from the client to the server after this method, are queued on Server side, until the client calls to Commit or Rollback

Client	Message and direction	Server
Channel = X	STARTTRANSACTION ---------->	**Action:** Creates a new Queue to store all Messages of the specified channel
Channel = X	PUBLISH ---------->	**Action:** Message is stored on Server Side.
Action: Client get confirmation of message sent	ACKNOWLEDGEMENT <----------	**Action:** Server returns an Acknowledgement to the client because message is stored.
....	....	....

Commit

When a client calls to commit, all messages queued by the server are processed.

Client	Message and direction	Server
Channel = X	COMMIT ---------->	**Action:** Process all messages queued by Transaction

RollBack

When a client calls to RollBack, all messages queued by the server are deleted and not processed on the server side.

Client	Message and direction	Server
Channel =	ROLLBACK	**Action:** Delete all messages queued by

X	---------->	Transaction

TCP Connections

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketServer_HTTPAPI
TsgcWebSocketClient

By default, sgcWebSocket use WebSocket as protocol, but you can use plain TCP protocol in client and server components.

Client Component
Disable WebSocket protocol.

```
Client.Specifications.RFC6455 := False;
```

Server Component
Handle event OnUnknownProtocol and set Transport as trpTCP and Accept the connection.

```
procedure OnUnknownProtocol(Connection: TsgcWSConnection;  var Accept:
Boolean);
begin
  Connection.Transport := trpTCP;
  Accept := True;
end;
```

Then when a client connects to the server, this connection will be defined as TCP and will use plain TCP protocol instead of WebSockets. Plain TCP connections don't know if the message is text or binary, so all messages received are handle OnBinary event.

End of Message
If messages are big, sometimes can be received fragmented. There is a method to try to find end of message setting which bytes find. Example: STOMP protocol, all messages ends with byte 0 and 10

```
procedure OnWSClientConnect(Connection: TsgcWSConnection);
begin
  Connection.TCPEndOfFrameScanBuffer := eofScanAllBytes;
  Connection.AddTCPEndOfFrame(0);
  Connection.AddTCPEndOfFrame(10);
end;
```

SubProtocol

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

WebSocket provides a simple subprotocol negotiation, basically adds a header with protocols name supported by request, these protocols are received and if the receiver supports one of them, sends a response with subprotocol supported.

sgcWebSockets supports several SubProtocols: MQTT, WAMP... and more. You can implement your own subprotocols using a very easy method, just call RegisterProtocol and send SubProtocol Name as an argument.

Example: you need to connect to a server which implements subprotocol "Test 1.0"

```
Client := TsgcWebSocketClient.Create(nil);
Client.Host := 'server host';
Client.Port := server.port;
Client.RegisterProtocol('Test 1.0');
Client.Active := True;
```

Throttle

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

Bandwidth Throttling is supported by Server and Client components, if enabled, can limit the number of bits per second sent/received by the socket. Indy uses a blocking method, so if a client is limiting its reading, unread data will be inside the client socket and the server will be blocked from writing new data to the client. As much slower is client reading data, much slower is server writing new data.

Server-sent Events (Push Notifications)

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
Java script

SSE are not part of WebSockets, defines an API for opening an HTTP connection for receiving push notifications from a server.

SSEs are sent over traditional HTTP. That means they do not require a special protocol or server implementation to get working. In addition, Server-Sent Events have a variety of features that WebSockets lack by design such as automatic reconnection, event IDs, and the ability to send arbitrary events.

Events

- **Open:** when a new SSE connection is opened.
- **Message:** when the client receives a new message.
- **Error:** when there any connection error like a disconnection.

JavaScript API

To subscribe to an event stream, create an EventSource object and pass it the URL of your stream:

```
var sse = new EventSource('sse.html');

sse.addEventListener('message', function(e)
 {console.log(e.data);
}, false);

sse.addEventListener('open', function(e) {
  // Connection was opened.
}, false);

sse.addEventListener('error', function(e) {
  if (e.readyState == EventSource.CLOSED) {
    // Connection was closed.
  }
}, false);
```

When updates are pushed from the server, the onmessage handler fires and new data is available in its e.data property. If the connection is closed, the browser will automatically reconnect to the source after ~3 seconds (this is a default retry interval, you can change on the server side).

Fields

The following field names are defined by the specification:

event

The event's type. If this is specified, an event will be dispatched on the browser to the listener for the specified event name; the web site would use addEventListener() to listen for named events. the onmessage handler is called if no event name is specified for a message.

data

The data field for the message. When the EventSource receives multiple consecutive lines that begin with data:, it will concatenate them, inserting a newline character between each one. Trailing newlines are removed.

id

The event ID to set the EventSource object's last event ID value to.

retry

The reconnection time to use when attempting to send the event. This must be an integer, specifying the reconnection time in milliseconds. If a non-integer value is specified, the field is ignored.

All other field names are ignored.

For multi-line strings use #10 as line feed.

Examples of use:

If you need to send a message to a client, just use WriteData method.

```
// If you need to send a message to a client, just use WriteData
method.
Connection.WriteData('Notification from server');

// To send a message to all Clients, use Broadcast method.
Connection.Broadcast('Notification from server');

// To send a message to all Clients, use Broadcast method.
Connection.Broadcast('Notification from server');

// To send a message to all Clients using url 'sse.html', use
Broadcast method and Channel parameter:
Connection.Broadcast('Notification from server', '/sse.html');

// You can send a unique id with an stream event by including a line
starting with "id:":
Connection.WriteData('id: 1' + #10 + 'data: Notification from
server');

// If you need to specify an event name:
Connection.WriteData('event: notifications' + #10 + 'data:
Notification from server');
```

javascript code to listen "notifications" channel:

```
sse.addEventListener('notifications',      function(e) {
   console.log('notifications:'  + e.data);
},  false);
```

LoadBalancing

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketLoadBalancerServer

Load Balancing allows distributing work between several back-end servers, every time a new client requests a connection, it connects to a load balancer server (which is connected to back-end servers) and returns a connection string with information about the host, port... which is used by the client to connect to a server. If you have for example 4 servers, with this method all servers will have, more or less, the same number of connections, and workload will be similar.

If a client wants to send a message to all clients of all servers, just use broadcast method, and this message will be broadcast to all servers connected to Load Balancer Server.

To enable this feature:

1. Drop a TsgcWebSocketLoadBalancerServer component, set a listening port and set active to True.

2. Server and Client components, have a property called LoadBalancer, where you need to set host and port of Load Balancer Server, and enabled True.

Files

Supported by

TsgcWSPServer_sgc
TsgcWSPClient_sgc

This protocol allows sending files from client to server and from server to client in an easy way. You can send from really small files to big files using a low memory usage. You can set:

1. Packet size in bytes.
2. Use custom channels to send files to only subscribed clients.
3. The progress of file send and received.
4. Authorization of files received.
5. Acknowledgement of packets sent.

Proxy

Supported by

TsgcWebSocketClient

Client WebSocket components support WebSocket connections through HTTP proxies, to enable proxy connection you need to activate the following properties:

Proxy / Enabled

Once set to True, you can set up:

Host: Proxy server address
Port: Proxy server port
UserName/Password: Authentication to connect to proxy, only if required.

You can configure SOCKS proxies accessing to SOCKS property and set Enable to True.

Fragmented Messages

Supported by

TsgcWebSocketServer
TsgcWebSocketHTTPServer
TsgcWebSocketClient

By default, when a stream is sent using sgcWebSockets library, it sends all data in a single packet or buffers all packets and when the latest packet is received, OnBinary message event is called.
This behaviour can be customized by **Options.FragmentedMessages** property, which accepts following values:

1. frgOnlyBuffer: this is the default value, means that packet messages will be buffered and only when all stream is received, OnBinary message will be called.
2. frgOnlyFragmented: this means that OnFragmented event only will be called for every packet received.
3. frgAll: this means that OnFragmented event will be called for every packet received and when the full stream is received.

OnFragmented event is useful when you must send big streams and receiver must show progress of the transfer.

Example: the client must send a stream of size 1.000.000 bytes to server and server wants show progress for every 1000 bytes received

The client will send a stream using writedata method with a size for a packet of 1000

```
Client.WriteData(stream, 1000);
```

The server will set in Options.FragmentedMessages := frgAll and will handle OnFragmented event to receive progress of streams

```
procedure OnFragmented(Connection: TsgcWSConnection;  const Data:
TMemoryStream; const OpCode: TOpcode; const Continuation: Boolean);
begin
  ShowProgress(Data.Size);
  if not Continuation then
    SaveStream(Data);
end;
```

Components

TsgcWebSocketClient

TsgcWebSocketClient implements Client WebSocket Component and can connect to a WebSocket Server. Follow the next steps to configure this component:

1. Drop a **TsgcWebSocketClient** component onto the form

2. Set **Host** and **Port** (default is 80) to connect to an available WebSocket Server. You can set **URL** property and Host, Port, Parameters... will be updated from URL. **Example:** wss://127.0.0.1:8080/ws/ will result:

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := '127.0.0.1';
oClient.Port := 80;
oClient.TLS := True;
oClient.Options.Parameters := '/ws/';
```

3. You can select if you require **TLS** (secure connection) or not, by default is not Activated.

4. You can connect through an HTTP Proxy Server, you need to define proxy properties:

Host: hostname of the proxy server.
Port: port number of the proxy server.
Username: user to authenticate, blank if anonymous.
Password: password to authenticate, blank if anonymous.

5. If the server supports **compression**, you can enable compression to compress messages sent.

6. Set **Specifications** allowed, by default all specifications are allowed.

RFC6455: is standard and recommended WebSocket specification.

Hlxie76: always is false

7. If you want, you can handle events

OnConnect: when a WebSocket connection is established, this event is fired

OnDisconnect: when a WebSocket connection is dropped, this event is fired

OnError: every time there is a WebSocket error (like mal-formed handshake), this event is fired

OnMessage: every time the server sends a text message, this event is fired

OnBinary: every time the server sends a binary message, this event is fired

OnHandhake: this event is fired when handshake is evaluated on the client side.

OnException: every time an exception occurs, this event is fired.

OnSSLVerifyPeer: if verify certificate is enabled, in this event you can verify if server certificate is valid and accept or not.

8. Set property Active = true to start a new websocket connection

Most common uses

- **Connection**
  - How Connect WebSocket Server
  - Open a Client Connection
  - Close a Client Connection
  - Keep Connection active
  - Dropped Disconnections
  - Connect TCP Server

- **Secure Servers**
  - Connect Secure Server

- **Send Messages**
  - Send Text Message
  - Send Binary Message

- **Receive Messages**
  - Receive Text Messages
  - Receive Binary Messages

- **Authentication**
  - Client Authentication

- **Other**
  - Client Exceptions
  - Client WebSocket HandShake
  - Client Register Protocol
  - Client Proxies

Methods

WriteData: sends a message to a WebSocket Server. Could be a String or MemoryStream. If "size" is set, the packet will be split if the size of the message is greater of size.

Ping: sends a ping to a Server. If a time-out is specified, it waits for a response until a time-out is exceeded, if no response, then closes the connection.

Start: uses a secondary thread to connect to the server, this prevents your application freezes while trying to connect.

Stop: uses a secondary thread to disconnect from the server, this prevents your application freezes while trying to disconnect.

Connect: try to connect to the server and wait till the connection is successful or there is an error.

Disconnect: try to disconnect from the server and wait till disconnection is successful or there is an error.

Properties

Authentication: if enabled, WebSocket connection will try to authenticate passing a username and password.

Implements 4 types of WebSocket Authentication

Session: client needs to do a HTTP GET passing username and password, and if authenticated, server response a Session ID. With this Session ID, client open WebSocket connection passing as a parameter.

URL: client open WebSocket connection passing username and password as a parameter.

Basic: uses basic authentication where user and password as sent as HTTP Header.

Token: sends a token as HTTP Header. Usually used for bearer tokens where token must be set in AuthToken property.

- **OAuth:** if a OAuth2 component is attached, before client connects to server, it requests a new Access Token to Authorization server. OAuth2 Component.

Host: IP or DNS name of the server.

HeartBeat: if enabled try to keeps alive WebSocket connection sending a ping every x seconds.

Interval: number of seconds between each ping.

Timeout: max number of seconds between a ping and pong.

TCPKeepAlive: if enabled, uses keep-alive at TCP socket level, in Windows will enable SIO_KEEPALIVE_VALS if supported and if not will use keepalive. By default is disabled. Read about Dropped Disconnections.

Time: if after X time socket doesn't sends anything, it will send a packet to keep-alive connection (value in milliseconds).

Interval: after sends a keep-alive packet, if not received a response after interval, it will send another packet (value in milliseconds).

ConnectTimeout: max time in milliseconds before a connection is ready.

LoadBalancer: it's a client which connects to Load Balancer Server to broadcast messages and get information about servers.

Enabled: if enabled, it will connect to Load Balancer Server.

Host: Load Balancer Server Host.

Port: Load Balancer Server Port.

Servers: here you can set manual WebSocket Servers to connect (if you don't make use of Load Balancer Server get server connection methods), example:

```
http://127.0.0.1:80
http://127.0.0.2:8888
```

ReadTimeout: max time in milliseconds to read messages.

WriteTimeOut: max time in milliseconds sending data to other peer, 0 by default.

Port: Port used to connect to the host.

LogFile: if enabled save socket messages to a specified log file, useful for debugging.

Enabled: if enabled every time a message is received and sent by socket it will be saved on a file.

FileName: full path to the filename.

NotifyEvents: defines which mode to notify WebSocket events.

neAsynchronous: this is the default mode, notify threaded events on asynchronous mode, adds events to a queue that are synchronized with the main thread asynchronously.

neSynchronous: if this mode is selected, notify threaded events on synchronous mode, needs to synchronize with the main thread to notify these events.

neNoSync: there is no synchronization with the main thread, if you need to access to controls that are not thread-safe, you need to implement your own synchronization methods.

Options: allows customizing headers sent on the handshake.

FragmentedMessages: allows handling Fragmented Messages

frgOnlyBuffer: the message is buffered until all data is received, it raises OnBinary or OnMessage event (option by default)
frgOnlyFragmented: every time a new fragment is received, it raises OnFragmented Event.
frgAll: every time a new fragment is received, it raises OnFragmented Event with All data received from the first packet. When all data is received, it raises OnBinary or OnMessage event.

Parameters: define parameters used on GET.

Origin: customize connection origin.

RaiseDisconnectExceptions: enabled by default, raises an exception every time there is a disconnection by protocol error.

ValidateUTF8: if enabled, validates if the message contains UTF8 valid characters, by default is disabled.

CleanDisconnect: if enabled, every time client disconnects from server, first sends a message to inform server connection will be closed.

Extensions: you can enable compression on messages sent.

Protocol: if exists, shows the current protocol used

Proxy: here you can define if you want to connect through a HTTP Proxy Server. If you need to connect to SOCKS proxies, just enable SOCKS.Enable property too.

WatchDog: if enabled, when an unexpected disconnection is detected, tries to reconnect to the server automatically.

Interval: seconds before reconnects.

Attempts: max number of reconnects, if zero, then unlimited.

Throttle: used to limit the number of bits per second sent/received.

TLS: enables a secure connection.

TLSOptions: if TLS enabled, here you can customize some TLS properties.

RootCertFile: path to root certificate file.
CertFile: path to certificate file.
KeyFile: path to certificate key file.
Password: if certificate is secured with a password, set here.
VerifyCertificate: if certificate must be verified, enable this property.
Version: by default uses TLS 1.0, if server requires a higher TLS version, here can be selected.
IOHandler: select which library you will use to connection using TLS.
iohOpenSSL: uses OpenSSL library and is the default for Indy components. Requires to deploy openssl libraries for win32/win64.
iohSChannel: uses Secure Channel which is a security protocol implemented by Microsoft for Windows, doesn't require to deploy openssl libraries. Only works in Windows 32/64 bits.
OpenSSL_Options: allows to define which OpenSSL API will be used.
oslAPI_1_0: uses API 1.0 OpenSSL, it's latest supported by Indy
oslAPI_1_0: uses API 1.1 OpenSSL, requires our custom Indy library and allows to use OpenSSL 1.1.1 libraries (with TLS 1.3 support).

TsgcWebSocketClient

Connection

TsgcWebSocketClient | Connect WebSocket Server

URL Property

The most easy way to connect to a WebSocket server is use **URL** property and call **Active = true**.

Example: connect to echo.websocket.org using secure connection.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.URL := 'wss://echo.websocket.org';
oClient.Active := true;
```

Host, Port and Parameters

You can connect to a WebSocket server using Host and port properties.

Example: connect to echo.websocket.org using secure connections

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'echo.websocket.org';
oClient.Port := 443;
oClient.TLS := true;
oClient.Active := true;
```

TsgcWebSocketClient | Client Open Connection

Once your client is configured to connect to server, there are 3 different options to call Open a new connection.

Active Property

The most easy way to open a new connection is Set Active property to true. This will try to connect to server using component configuration.
If you set Active property to false, will close connection if active.
This method is executed in the same thread that caller. So if you call in the Main Thread, method will be executed in Main Thread of application.

Open Connection

```
oClient := TsgcWebSocketClient.Create(nil);
...
oClient.Active := true;
```

When you call Active = true, **you can't still send any data to server** because client maybe is still connecting, you must first wait to OnConnect event is fired and then you can start to send messages to server.

Close Connection

```
oClient.Active := false;
```

When you call Active = false, **you cannot be sure that connection is already closed** just after this code, so you must wait to OnDisconnect event is fired.

Start/Stop methods

When you call Start() or Stop() to connect/disconnect from server, is executed in a secondary thread, so it doesn't blocks the thread where is called. Use this method if you want connect to a server and let your code below continue.

Open Connection

```
oClient := TsgcWebSocketClient.Create(nil);
...
oClient.Start();
```

When you call Start(), **you can't still send any data to server** because client maybe is still connecting, you must first wait to OnConnect event is fired and then you can start to send messages to server.

Close Connection

```
oClient.Stop();
```

When you call Stop(), **you cannot be sure that connection is already closed** just after this code, so you must wait to OnDisconnect event is fired.

Connect/Disconnect methods

When you call Connect() or Disconnect() to open/close connection from server, this is executed in the same thread where is called, but it waits till process is finished. You must set a Timeout to set the maximum time to wait till process is finished (by default 10 seconds)

Example: connect to server and wait till 5 seconds

```
oClient := TsgcWebSocketClient.Create(nil);
...
if oClient.Connect(5000) then
  oClient.WriteData('Hello from client')
else
  Error();
```

If after calling Connect() method, the result is successful, you can already send a message to server because connection is alive.

Example: connect to server and wait till 10 seconds

```
if oClient.Disconnect(10000) then
  ShowMessage('Disconnected')
else
  ShowMessage('Not Disconnected');
```

If after calling Disconnect() event the result is successful, this means that connection is already closed.

TsgcWebSocketClient | Client Close Connection

Connection can be closed using Active property, Stop or Disconnect methods, read more from Client Open Connection.

CleanDisconnect

When connection is closed, you can notify other peer that connection is closed sending a message about close connection, to enable this feature, Set Options.CleanDisconnect property to true.
If this property is enabled, before connection is closed, a Close message will be sent to server to notify that client is closing connection.

Disconnect

TsgcWSConnection has a method called Disconnect(), that allows to disconnect connection at socket level. If you call this method, socket will be disconnected directly without waiting any response from server. You can send a Close Code with this method.

Close

TsgcWSConnection has a method called Close(), which allows to send a message to server requesting to close connection, if server receives this message, must close the connection and client will receive a notification that connection is closed. You can send a Close Code with this method.

TsgcWebSocketClient |Client Keep Connection Open

Once your client has connected to server, sometimes connection can be closed due to poor signal, connection errors... there are 2 properties which helps to keep connection active.

HeartBeat

HeartBeat property allows to **send a Ping** every X **seconds** to **maintain connection alive**. Some servers, close TCP connections if there is no data exchanged between peers. HeartBeat solves this problem, sending a ping every a specific interval. Usually this is enough to maintain a connection active, but you can set a TimeOut interval if you want to close connection if a response from server is not received after X seconds.

Example: send a ping every 30 seconds

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.HeartBeat.Interval := 30;
oClient.HeartBeat.Timeout := 0;
oClient.HeartBeat.Enabled := true;
oClient.Active := true;
```

WatchDog

If WatchDog is enabled, when client detects a disconnection, WatchDog try to reconnect again every X seconds until connection is active again.

Example: reconnect every 10 seconds after a disconnection with unlimited attempts.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.WatchDog.Interval := 10;
oClient.WatchDog.Attempts := 0;
oClient.WatchDog.Enabled := true;
oClient.Active := true;
```

TsgcWebSocketClient | Dropped Disconnections

Once the connection has been established, if no peer sends any data, then no packets are sent over the net. TCP is an idle protocol, so it assumes that the connection is active.

Disconnection reasons

- **Application closes:** when a process is finished, usually sends a FIN packet which acknowledges the other peer that connection has been closed. But if a process crashes there is no guarantee that this packet will be sent to other peer.
- **Device Closes:** if devices closes, most probably there won't be any notification about this.
- **Network cable unplugged:** if network cable is unplugged it's the same that a router closes, there is no data being transferred so connection is not closed.
- **Loss signal from router:** if application loses signal from router, connection will still be alive.

Detect Half-Open Disconnections

You can try to detect disconnections using the following methods
Second Connection
You can try to open a second connection and try to connect but this has some disadvantages, like you are consuming more resources, create new threads... and if other peer has rebooted, second connection will work but first won't.
Ping other peer
If you try to send a ping or whatever message with a half-open connection, you will see that you don't get any error.

Enable KeepAlive at TCP Socket level
A TCP keep-alive packet is simply an ACK with the sequence number set to one less than the current sequence number for the connection. A host receiving one of these ACKs responds with an ACK for the current sequence number. Keep-alives can be used to verify that the computer at the remote end of a connection is still available. TCP keep-alives can be sent once every TCPKeepAlive.Time (defaults to 7,200,000 milliseconds or two hours) if no other data or higher-level keep-alives have been carried over the TCP connection. If there is no response to a keep-alive, it is repeated once every TCPKeepAlive.Interval seconds. KeepAliveInterval defaults to 1000 milliseconds.

You can enable per-connection KeepAlive and allow that TCP protocol check if connection is active or not. This is the preferred method if you want to detect dropped disconnections (for example: when you unplug a network cable).

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.TCPKeepAlive.Enabled := True;
oClient.TCPKeepAlive.Time := 5000;
oClient.TCPKeepAlive.Interval := 1000;
```

TsgcWebSocketClient | Connect TCP Server

TsgcWebSocketClient can connect to WebSocket servers but can connect to plain TCP Servers too.

URL Property

The most easy way to connect to a WebSocket server is use **URL** property and call **Active = true**.

Example: connect to 127.0.0.1 port 5555

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.URL := 'tcp://127.0.0.1:5555';
oClient.Active := true;
```

Host, Port and Parameters

You can connect to a TCP server using Host and port properties.

Example: connect to 127.0.0.1 port 5555

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Specifications.RFC6455 := false;
oClient.Host := '127.0.0.1';
oClient.Port := 5555;
oClient.Active := true;
```

Secure Servers

TsgcWebSocketClient | Connect Secure Server

TsgcWebSocketClient can connect to WebSocket servers using secure and none-secure connections.

You can configure a secure connection, using URL property or Host / Port properties, see Connect to WebSocket Server.

TLSOptions

In **TLSOptions** property there are the properties to **customize a secure connection**. The most important property is **version**, which specifies the **version of TLS protocol**. Usually setting **TLS property to true** and **TLSOptions.Version to tls1_2** is enough for the wide majority of WebSocket Servers.

If you get an **error trying to connect to a server** about TLS protocol, **most probably** this server r**equires a TLS version newer** than you set. **Example:** if you set TLSOptions.Version = tls1_0 and you get an error about TLS protocol, try to set to tls1_2 and most probably will work.

If **TLSOptions.IOHandler** is set to **iohOpenSSL**, you need to **deploy OpenSSL libraries** (which are the libraries that handle all TLS stuff), check the following article about OpenSSL.
If **TLSOptions.IOHandler** is set to **iohSChannel**, then there is **no need to deploy** any library.

Send Messages

TsgcWebSocketClient | Client Send Text Message

Once client has connected to server, it can send Text Messages to server. To send a Text Message, just call WriteData() method and send your text message.

Send a Text Message

Call To **WriteData()** method and send a Text message. This method is executed on the **same thread** that is called.

```
TsgcWebSocketClient1.WriteData('My First sgcWebSockets Message!.');
```

If **QueueOptions.Text** has a **different value from qmNone**, instead of be processed on the same thread that is called, it will be processed on a secondary thread. By default this option is disabled.

TsgcWebSocketClient | Client Send Binary Message

Once client has connected to server, it can send Binary Messages to server. To send a Text Message, just call WriteData() method and send your binary message.

Send a Binary Message

Call To **WriteData()** method and send a Binary message. This method is executed on the **same thread** that is called.

```
oStream := TMemoryStream.Create(nil);
Try
  ...
  TsgcWebSocketClient1.WriteData(oStream);
Finally
  oStream.Free;
End;
```

If **QueueOptions.Binary** has a **different value from qmNone**, instead of be processed on the same thread that is called, it will be processed on a secondary thread. By default this option is disabled.

TsgcWebSocketClient | Client Send a Text and Binary Message

WebSocket protocol only allows to types of messages: Text or Binary. But you can't send a binary with text in the same message.
One way to solve this, is add a header to binary message before is sent and decode this binary message when is received.

There are 2 functions in sgcWebSocket_Helpers which can be used to set a short description of binary packet, basically adds a header to stream which is used to identify binary packet.

Before send a binary message, call method to encode stream.

```
sgcWSStreamWrite('00001', oStream);
TsgcWebSocketClient1.WriteData(oStream);
```

When binary message is received, call method to decode stream.

```
sgcWSStreamRead(oStream, vID);
```

The only limitation is that text used to identify binary message, has a maximum length of 10 characters (this can be modified if you have access to source code).

Receive Messages

TsgcWebSocketClient | Receive Text Messages

When client receives a Text Message, **OnMessage** event is fired, just read Text parameter to know the string of message received.

```
procedure OnMessage(Connection: TsgcWSConnection; const Text: string);
begin
  ShowMessage('Message Received from Server: ' + Text);
end;
```

By default, client uses **neAsynchronous** method to dispatch OnMessage event, this means that **this event is executed on the context of Main Thread**, so it's thread-safe to update any control of a form for example.

If your client receives lots of messages or you need to control the synchronization with other threads, set NotifyEvents property to **neNoSync**, this means that OnMessage event will be e**xecuted on the context of connection thread**, so if you require to update any control of a form or access shared objects, you must implement your own synchronization methods.

TsgcWebSocketClient | Receive Binary Messages

When client receives a Binary Message, **OnBinary** event is fired, just read Data parameter to know the binary message received.

```
procedure OnBinary(Connection: TsgcWSConnection; const Data:
TMemoryStream);
var
  oBitmap: TBitmap;
begin
  oBitmap := TBitmap.Create;
  Try
    oBitmap.LoadFromStream(Data);
    Image1.Picture.Assign(oBitmap);
    Log(
      '#image uncompressed size: ' + IntToStr(Data.Size) +
      '. Total received: ' + IntToStr(Connection.RecBytes));
  Finally
    FreeAndNil(oBitmap);
  End;
end;
```

By default, client uses **neAsynchronous** method to dispatch OnMessage event, this means that **this event is executed on the context of Main Thread**, so it's thread-safe to update any control of a form for example.

If your client receives lots of messages or you need to control the synchronization with other threads, set NotifyEvents property to **neNoSync**, this means that OnMessage event will be e**xecuted on the context of connection thread**, so if you require to update any control of a form or access shared objects, you must implement your own synchronization methods.

Authentication

TsgcWebSocketClient | Client Authentication

TsgcWebSocket client supports 4 types of Authentications:

- **Basic:** sends an HTTP Header during WebSocket HandShake with User and Password encoded as Basic Authorization.
- **Token:** sends a Token as HTTP Header during WebSocket HandShake, just set in Authentication.Token.AuthToken the required token by server.
- **Session:** first client request an HTTP session to server and if server returns a session this is passed in GET HTTP Header of WebSocket HandShake. (* own authorization method for sgcWebSockets library).
- **URL:** client request authorization using GET HTTP Header of WebSocket HandShake. (* own authorization method for sgcWebSockets library).

Authorization Basic

Is a simple authorization method where user and password are encoded and passes as an HTTP Header. Just set User and Password and enable only Basic Authorization type to use this method.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Authorization.Enabled := true;
oClient.Authorization.Basic.Enabled := true;
oClient.User := 'your user';
oClient.Password := 'your password';
oClient.Authorization.Token.Enabled := false;
oClient.Authorization.URL.Enabled := false;
oClient.Authorization.Session.Enabled := false;
oClient.Active := True;
```

Authorization Token

Allows to get Authorization using JWT, requires you obtain a Token using any external tool (example: using an HTTP connection, OAuth2...).
If you Attach an OAuth2 component, you can obtain this token automatically. Read more about OAuth2.
Basically you must set your AuthToken and enable Token Authentication.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Authorization.Enabled := true;
oClient.Authorization.Token.Enabled := true;
oClient.Authorization.Token.AuthToken := 'your token';
oClient.Authorization.Basic.Enabled := false;
oClient.Authorization.URL.Enabled := false;
oClient.Authorization.Session.Enabled := false;
oClient.Active := True;
```

Authorization Session

First client connects to server using an HTTP connection requesting a new Session, if successful, server returns a SessionId and client sends this SessionId in GET HTTP Header of WebSockets HandShake.
Requires to set UserName and Password and set Session Authentication to True.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Authorization.Enabled := true;
oClient.Authorization.Session.Enabled := true;
oClient.User := 'your user';
oClient.Password := 'your password';
oClient.Authorization.Basic.Enabled := false;
oClient.Authorization.URL.Enabled := false;
oClient.Authorization.Token.Enabled := false;
oClient.Active := True;
```

Authorization URL

This Authentication method, just passes username and password in GET HTTP Header of WebSockets HandShake.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Authorization.Enabled := true;
oClient.Authorization.URL.Enabled := true;
oClient.User := 'your user';
oClient.Password := 'your password';
oClient.Authorization.Basic.Enabled := false;
oClient.Authorization.Session.Enabled := false;
oClient.Authorization.Token.Enabled := false;
oClient.Active := True;
```

Other

TsgcWebSocketClient | Client Exceptions

Sometimes there are some errors in communications, server can disconnect a connection because it's not authorized or a message hasn't the correct format... there are 2 events where errors are captured
OnError
This event is fired every time there is an error in WebSocket protocol, like invalid message type, invalid utf8 string...

```
procedure OnError(Connection: TsgcWSConnection; const Error: string);
begin
  WriteLn('#error: ' + Error);
end;
```

OnException
This event is fired every time there is an exception like write a socket is not active, access to an object that not exists

```
procedure OnException(Connection: TsgcWSConnection; E: Exception);
begin
  WriteLn('#exception: ' + E.Message);
end;
```

By default, when **connection is closed by server**, an **exception will be fired**, if you don't want that these exceptions are fired, just disable in **Options.RaiseDisconnectExceptions**.

TsgcWebSocketClient | WebSocket HandShake

WebSocket protocol uses an HTTP HandShake to upgrade from HTTP Protocol to WebSocket protocol. This handshake is handled internally by TsgcWebSocket Client component, but you can add your custom HTTP headers if server requires some custom HTTP Headers info.

Example: if you need to add this HTTP Header "Client: sgcWebSockets"

```
procedure OnHandshake(Connection: TsgcWSConnection; var Headers:
TStringList);
begin
  Headers.Add('Client: sgcWebSockets');
end;
```

You can check HandShake string before is sent to server using OnHandShake event too.

TsgcWebSocketClient | Client Register Protocol

By default, TsgcWebSocketClient doesn't make use of any SubProtocol, basically websocket sub-protocol are built on top of websocket protocol and defines a custom message protocol, example of websocket sub-protocols can be MQTT, STOMP...

WebSocket SubProtocol name is sent as an HTTP Header in WebSocket HandShake, this header is processed by server and if server supports this subprotocol will accept connection, if is not supported, connection will be closed automatically

Example: connect to a websocket server with SubProtocol name 'myprotocol'

```
Client := TsgcWebSocketClient.Create(nil);
Client.Host := 'server host';
Client.Port := server.port;
Client.RegisterProtocol('myprotocol');
Client.Active := True;
```

TsgcWebSocketClient | Client Proxies

TsgcWebSocket client support connections through proxies, to configure a proxy connection, just fill the **Proxy** properties of TsgcWebSocket client.

```
Client := TsgcWebSocketClient.Create(nil);
Client.Proxy.Enabled := true;
Client.Proxy.Username := 'user';
Client.Proxy.Password := 'secret';
Client.Proxy.Host := '80.55.44.12';
Client.Proxy.Port := 8080;
Client.Active := True;
```

TsgcWebSocketServer

TsgcWebSocketServer implements Server WebSocket Component and can handle multiple threaded client connections. Follow the next steps to configure this component:

1. Drop a TsgcWebSocketServer component onto the form

2. Set Port (default is 80). If you are behind a firewall probably you will need to configure it.

3. Set Specifications allowed, by default all specifications are allowed.

RFC6455: is standard and recommended WebSocket specification.

Hixie76: it's a draft and it's only recommended to establish Hixie76 connections if you want to provide support to old browsers like Safari 4.2

4. If you want, you can handle events:

OnConnect: every time a WebSocket connection is established, this event is fired.

OnDisconnect: every time a WebSocket connection is dropped, this event is fired.

OnError: every time there is a WebSocket error (like mal-formed handshake), this event is fired.

OnMessage: every time a client sends a text message and it's received by server, this event is fired.

OnBinary: every time a client sends a binary message and it's received by server, this event is fired.

OnHandhake: this event is fired after the handshake is evaluated on the server side.

OnException: every time an exception occurs, this event is fired.

OnAuthentication: if authentication is enabled, this event is fired. You can check user and password passed by the client and enable/disable Authenticated Variable.

OnUnknownProtocol: if WebSocket protocol is not detected (because the client is using plain TCP protocol for example), in this event connection can be accepted or rejected.

OnStartup: raised after the server has started.

OnShutdown: raised after the server has stopped.

5. Create a procedure and set property Active = True.

Most common uses

- **Start**
  - Server Start
  - Server Bindings
  - Server Startup - Shutdown

- Server Keep Active

- **Connections**
  - Server Keep Connections Alive

- **Authentication**
  - Server Authentication

- **Send Messages**
  - Server Send Text Message
  - Server Send Binary Message

- **Receive Messages**
  - Server Receive Text Message
  - Server Receive Binary Message

Methods

Broadcast: sends a message to all connected clients.

Message / Stream: message or stream to send to all clients.

Channel: if you specify a channel, the message will be sent only to subscribers.

Protocol: if defined, the message will be sent only to a specific protocol.

Exclude: if defined, list of connection guid excluded (separated by comma).

Include: if defined, list of connection guid included (separated by comma).

WriteData: sends a message to a single or multiple clients. Every time a Client establishes a WebSocket connection, this connection is identified by a Guid, you can use this Guid to send a message to a client.

Ping: sends a ping to all connected clients. If a time-out is specified, it waits a response until a time-out is exceeded, if no response, then closes the connection.

DisconnectAll: disconnects all active connections.

Start: uses a secondary thread to connect to the server, this prevents your application freezes while trying to connect.

Stop: uses a secondary thread to disconnect from the server, this prevents your application freezes while trying to disconnect.

Properties

Authentication: if enabled, you can authenticate WebSocket connections against a username and password.

Authusers: is a list of authenticated users, following spec:

user=password

Implements 3 types of WebSocket Authentication

Session: client needs to do an HTTP GET passing username and password, and if authenticated, server response a Session ID. With this Session ID, client open WebSocket connection passing as a parameter.

URL: client open Websocket connection passing username and password as a parameter.

Basic: implements Basic Access Authentication, only applies to VCL Websockets (Server and Client) and HTTP Requests (client web browsers don't implement this type of authentication).

Bindings: used to manage IP and Ports.

Connections: contains a list of all clients connections.

Count: Connections number count.

Extensions: you can enable compression on messages sent (if client don't support compression, messages will be exchanged automatically without compression).

FallBack: if WebSockets protocol it's not supported natively by the browser, you can enable the following fallbacks:

Flash: if enabled, if the browser hasn't native WebSocket implementation and has flash enabled, it uses Flash as a Transport.

ServerSentEvents: if enabled, allows to send push notifications from the server to browser clients.

Retry: interval in seconds to try to reconnect to server (3 by default).

HeartBeat: if enabled try to keeps alive Websocket client connections sending a ping every x seconds.

Interval: number of seconds between each ping.

Timeout: max number of seconds between a ping and pong.

TCPKeepAlive: if enabled, uses keep-alive at TCP socket level, in Windows will enable SIO_KEEPALIVE_VALS if supported and if not will use keepalive. By default is disabled.

Interval: in milliseconds.

Timeout: in milliseconds.

LoadBalancer: it's a client which connects to Load Balancer Server to broadcast messages and send information about the server.

AutoRegisterBindings: if enabled, sends automatically server bindings to load balancer server.

AutoRestart: time to wait in seconds after a load balancer server connection has been dropped and tries to reconnect; zero means no restart (by default);

Bindings: here you can set manual bindings to be sent to Load Balancer Server, example:

```
WS://127.0.0.1:80
WSS://127.0.0.2:8888
```

Enabled: if enabled, it will connect to Load Balancer Server.

Guid: used to identify server on Load Balancer Server side.

Host: Load Balancer Server Host.

Port: Load Balancer Server Port.

MaxConnections: max connections allowed (if zero there is no limit).

NotifyEvents: defines which mode to notify WebSocket events.

neAsynchronous: this is the default mode, notify threaded events on asynchronous mode, adds events to a queue that are synchronized with the main thread asynchronously.

neSynchronous: if this mode is selected, notify threaded events on synchronous mode, needs to synchronize with the main thread to notify these events.

neNoSync: there is no synchronization with the main thread, if you need to access to controls that are not thread-safe, you need to implement your own synchronization methods.

Options:

FragmentedMessages: allows handling Fragmented Messages

frgOnlyBuffer: the message is buffered until all data is received, it raises OnBinary or OnMessage event (option by default)
frgOnlyFragmented: every time a new fragment is received, it raises OnFragmented Event.
frgAll: every time a new fragment is received, it raises OnFragmented Event with All data received from the first packet. When all data is received, it raises OnBinary or OnMessage event.

HTMLFiles: if enabled, allows to request Web Browser tests, enabled by default.

JavascriptFiles: if enabled, allows to request Javascript Built-in libraries, enabled by default.

RaiseDisconnectExceptions: enabled by default, raises an exception every time there is a disconnection by protocol error.

ReadTimeOut: time in milliseconds to check if there is data in socket connection, 10 by default.

WriteTimeOut: max time in milliseconds sending data to other peer, 0 by default.

ValidateUTF8: if enabled, validates if the message contains UTF8 valid characters, by default is disabled.

ReadEmptySource: max number of times an HTTP Connection is read and there is no data received, 0 by default (means no limit). If the limit is reached, the connection is closed.

SecurityOptions:

OriginsAllowed: define here which origins are allowed (by default accepts connections from all origins), if the origin is not in the list closes the connection.

SSL: enables secure connections.

SSLOptions: used to define SSL properties: certificates filenames, password...

ThreadPool: if enabled, when a thread is no longer needed this is put into a pool and marked as inactive (do not consume CPU cycles), it's useful if there are a lot of short-lived connections.

MaxThreads: max number of threads to be created, by default is 0 meaning no limit. If max number is reached then the connection is refused.

PoolSize: size of ThreadPool, by default is 32.

OpenSSL_Options:

APIVersion: allows to define which OpenSSL API will be used.
oslAPI_1_0: uses API 1.0 OpenSSL, it's latest supported by Indy
oslAPI_1_0: uses API 1.1 OpenSSL, requires our custom Indy library and allows to use OpenSSL 1.1.1 libraries (with TLS 1.3 support).
ECDHE: if enabled, uses ECDHE instead of RSA as key exchange. Recommended to enable ECDHE if you use OpenSSL 1.0.2.

WatchDog: if enabled, restart the server after unexpected disconnection.

Interval: seconds before reconnects.

Attempts: max number of reconnects, if zero, then unlimited.

Throttle: used to limit the number of bits per second sent/received.

TsgcWebSocketServer

Start

TsgcWebSocketServer | Start Server

The first you must set when you want start a Server is set a Listening Port, by default, this is set to port 80 but you can change for any port.
Once the port is set, there are 2 methods to start a server.

Active Property

If you set Active property to true, server will start to listening all incoming connection on port set.

```
oServer := TsgcWebSocketServer.Create(nil);
oServer.Port := 80;
oServer.Active := true;
```

If you set Active property to false, server will stop and close all active connections.

```
oServer.Active := false;
```

Start / Stop methods

While if you call Active property the process of start / stop server is done in the same thread, calling Start and Stop methods will be executed in a secondary thread.

```
oServer := TsgcWebSocketServer.Create(nil);
oServer.Port := 80;
oServer.Start();
```

If you call Stop() method, server will stop and close all active connections.

```
oServer.Stop();
```

TsgcWebSocketServer | Server Bindings

By default, if you only fill **Port property**, server **binds listening port of ALL IPs**, so if for example, you have 3 IP: 127.0.0.1, 80.5411.22 and 12.55.41.17. Your server will bind this port on 3 IPs.
Usually is recommended only binding to needed IPs, here is where you can user Bindings property.
Instead of use Port property, just use Binding property and fill with IP and Port required.

Example: bind Port 5555 to IP 127.0.0.1 and IP 80.58.25.40

```
oServer := TsgcWebSocketServer.Create(nil);
With oServer.Bindings.Add do
begin
  IP := '127.0.0.1';
  Port := 5555;
end;
With oServer.Bindings.Add do
begin
  IP := '80.58.25.40';
  Port := 5555;
end;
oServer.Active := true;
```

TsgcWebSocketServer | Server Startup Shutdown

Once you have set all required configurations of your server, there are 2 useful events to know when server has started and when has stopped.

OnStartup

This event is fired when server has started and can process new connections.

```
procedure OnStartup(Sender: TObject);
begin
  WriteLn('#server started');
end;
```

OnShutdown

This event is fired after server has stopped and no more connections are accepted.

```
procedure OnShutdown(Sender: TObject);
begin
  WriteLn('#server stopped');
end;
```

TsgcWebSocketServer | Server Keep Active

Once server is started and OnShutdown event is fired, sometimes server can stopped for any reason. If you want to restart server after an unexpected close, you can use WatchDog property

WatchDog

If WatchDog is enabled, when server detects a Shutdown, WatchDog try to restart again every X seconds until server is active again.

Example: restart every 10 seconds after an unexpected stop with unlimited attempts.

```
oServer := TsgcWebSocketServer.Create(nil);
oServer.WatchDog.Interval := 10;
oServer.WatchDog.Attempts := 0;
oServer.WatchDog.Enabled := true;
oServer.Active := true;
```

SSL

TsgcWebSocketServer | Server SSL

Server can be configured to use **SSL Certificates**, in order to get a Production Server with a server certificate, you must **purchase** a Certificate from a **well known provider**: Namecheap, godaddy, Thawte... For **testing purposes** you can use a **self-signed certificate** (check out in Demos/Chat which uses a self-signed certificate).

Certificate must be in **PEM format**, PEM (from Privacy Enhanced Mail) is defined in RFCs 1421 through 1424, this is a container format that may include just the public certificate (such as with Apache installs, and CA certificate files /etc/ssl/certs), or may include an entire certificate chain including public key, private key, and root certificates. To create a single pem certificate, just open your private key file, copy the contents and paste on certificate file.

Example:

certificate.crt

```
-----BEGIN CERTIFICATE-----
.....
-----END CERTIFICATE-----
```

certificate.key

```
-----BEGIN PRIVATE KEY-----
.....
-----END PRIVATE KEY-----
```

certificate.pem

```
-----BEGIN PRIVATE KEY-----
.....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
.....
-----END CERTIFICATE-----
```

To enable SSL, just **enable SSL property** and configure the paths to **CertFile**, **KeyFile** and **RootFile**. If certificate contains entire certificate (public key, private key...) just set all paths to the same certificate.

Another property you must set is **SSLOptions.Port**, this is the port used for secure connections.

Simple SSL Configuration

Example: configure SSL in IP 127.0.0.1 and Port 443

```
oServer := TsgcWebSocketServer.Create(nil);
oServer.SSL := true;
oServer.SSLOptions.CertFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.KeyFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.RootCertFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.Port := 443;
```

```
oServer.Port := 443;
oServer.Active := true;
```

SSL and None SSL

You can allow to server, to listening more than one IP and Port, check Binding article which explains how works. Server can be configured to allow SSL connections and None SSL connections at the same time (of course listening on different ports). You only need to bind to 2 different ports and configure port for ssl connections and port for none ssl connections.

Example: configure server in IP 127.0.0.1, port 80 (none encrypted) and 443 (SSL)

```
oServer := TsgcWebSocketServer.Create(nil);
With oServer.Bindings.Add do
begin
  IP := '127.0.0.1';
  Port := 80;
end;
With oServer.Bindings.Add do
begin
  IP := '127.0.0.1';
  Port := 443;
end;
oServer.Port := 80;
oServer.SSL := true;
oServer.SSLOptions.CertFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.KeyFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.RootCertFile := 'c:\certificates\mycert.pem';
oServer.SSLOptions.Port := 443;
oServer.Active := true;
```

Connections

TsgcWebSocketServer | Server Keep Connections Alive

Once your client has connected to server, sometimes connection can be closed due to poor signal, connection errors... use Heartbeat to keep connection alive.

HeartBeat

HeartBeat property allows to **send a Ping** every X **seconds** to **maintain connection alive**. Some servers, close TCP connections if there is no data exchanged between peers. HeartBeat solves this problem, sending a ping every a specific interval. Usually this is enough to maintain a connection active, but you can set a TimeOut interval if you want to close connection if a response from client is not received after X seconds.

Example: send a ping to all connected clients every 30 seconds

```
oServer := TsgcWebSocketServer.Create(nil);
oServer.HeartBeat.Interval := 30;
oServer.HeartBeat.Timeout := 0;
oServer.HeartBeat.Enabled := true;
oServer.Active := true;
```

Authentication

TsgcWebSocketServer | Server Authentication

TsgcWebSocket server supports 3 types of Authentications:

- **Basic:** read an HTTP Header during WebSocket HandShake with User and Password encoded as Basic Authorization.
- **Session:** first client request an HTTP session to server and if server returns a session this is passed in GET HTTP Header of WebSocket HandShake. (* own authorization method for sgcWebSockets library).
- **URL:** read request authorization using GET HTTP Header of WebSocket HandShake. (* own authorization method for sgcWebSockets library).

You can set a list of Authenticated users, using **AuthUsers** property, just set your users with the following format: user=password

OnAuthentication

Every time server receives an Authentication Request from a client, this event is called to return if user is authenticated or not.
Use Authenticated parameter to accept or not the connection.

```
procedure OnAuthentication(Connection: TsgcWSConnection; aUser,
aPassword: string; var Authenticated: Boolean);
begin
  if ((aUser = 'user') and (aPassword = 'secret')) then
    Authenticated := true
  else
    Authenticated := false;
end;
```

OnUnknownAuthentication

If Authentication is not supported by default, like JWT, still you can use this event to accept or not the connection. Just read the parameters and accept or not the connection.

```
procedure OnUnknownAuthentication(Connection: TsgcWSConnection;
AuthType, AuthData: string; var aUser, aPassword: string; var
Authenticated: Boolean);
begin
  if AuthType = 'Bearer' then
  begin
    if AuthData = 'jwt_token' then
      Authenticated := true
    else
      Authenticated := false;
  end
  else
```

```
    Authenticated := false;
end;
```

Send Messages

TsgcWebSocketServer | Server Send Text Message

Once client has connected to server, server can send text messages. To send a Text Message, just call WriteData() method to send a message to a single client or use Broadcast to send a message to all clients.

Send a Text Message

Call To **WriteData()** method and send a Text message.

```
TsgcWebSocketServer1.WriteData('guid', 'My First sgcWebSockets
Message!.');
```

If **QueueOptions.Text** has a **different value from qmNone**, instead of be processed on the same thread that is called, it will be processed on a secondary thread. By default this option is disabled.

You can call to WriteData() method from **TsgcWSConnection** too, **example:** send a message to client when connects to server.

```
procedure OnConnect(Connection: TsgcWSConnection);
begin
  Connection.WriteData('Hello From Server');
end;
```

Send a message to ALL connected clients

Call To **Broadcast()** method to send a Text message to all connected clients.

```
TsgcWebSocketServer1.Broadcast('Hello From Server');
```

TsgcWebSocketServer | Server Send Binary Message

Once client has connected to server, server can send binary messages. To send a Binary Message, just call WriteData() method to send a message to a single client or use Broadcast to send a message to all clients.

Send a Text Message

Call To **WriteData()** method and send a Binary message.

```
TsgcWebSocketServer1.WriteData('guid', TMemoryStream.Create);
```

If **QueueOptions.Binary** has a **different value from qmNone**, instead of be processed on the same thread that is called, it will be processed on a secondary thread. By default this option is disabled.

You can call to WriteData() method from **TsgcWSConnection** too, **example:** send a message to client when connects to server.

```
procedure OnConnect(Connection: TsgcWSConnection);
begin
  Connection.WriteData(TMemoryStream.Create);
end;
```

Send a message to ALL connected clients

Call To **Broadcast()** method to send a Binary message to all connected clients.

```
TsgcWebSocketServer1.Broadcast(TMemoryStream.Create);
```

Receive Messages

TsgcWebSocketServer | Server Receive Text Message

When server receives a Text Message, **OnMessage** event is fired, just read Text parameter to know the string of message received.

```
procedure OnMessage(Connection: TsgcWSConnection; const Text: string);
begin
  ShowMessage('Message Received from Client: ' + Text);
end;
```

By default, server uses **neAsynchronous** method to dispatch OnMessage event, this means that **this event is executed on the context of Main Thread**, so it's thread-safe to update any control of a form for example.

If your server receives lots of messages or you need to control the synchronization with other threads, set NotifyEvents property to **neNoSync**, this means that OnMessage event will be e**xecuted on the context of connection thread**, so if you require to update any control of a form or access shared objects, you must implement your own synchronization methods.

TsgcWebSocketServer | Server Receive Binary Message

When server receives a Binary Message, **OnBinary** event is fired, just read Data parameter to know the binary message received.

```
procedure OnBinary(Connection: TsgcWSConnection; const Data:
TMemoryStream);
var
  oBitmap: TBitmap;
begin
  oBitmap := TBitmap.Create;
  Try
    oBitmap.LoadFromStream(Data);
    Image1.Picture.Assign(oBitmap);
    Log(
      '#image uncompressed size: ' + IntToStr(Data.Size) +
      '. Total received: ' + IntToStr(Connection.RecBytes));
  Finally
    FreeAndNil(oBitmap);
  End;
end;
```

By default, server uses **neAsynchronous** method to dispatch OnMessage event, this means that **this event is executed on the context of Main Thread**, so it's thread-safe to update any control of a form for example.

If your server receives lots of messages or you need to control the synchronization with other threads, set NotifyEvents property to **neNoSync**, this means that OnMessage event will be e**xecuted on the context of connection thread**, so if you require to update any control of a form or access shared objects, you must implement your own synchronization methods.

TsgcWebSocketHTTPServer

TsgcWebSocketHTTPServer implements Server WebSocket Component and can handle multiple threaded client connections as TsgcWebSocketServer, and allows to server HTML pages using a built-in HTTP Server, sharing the same port for WebSocket connections and HTTP requests.

Follow the next steps to configure this component:

1. Drop a TsgcWebSocketHTTPServer component in the form

2. Set Port (default is 80). If you are behind a firewall probably you will need to configure it.

3. Set Specifications allowed, by default all specifications are allowed.

RFC6455: is standard and recommended WebSocket specification.

Hixie76: it's a draft and it's only recommended to establish Hixie76 connections if you want to provide support to old browsers like Safari 4.2

4. If you want, you can handle events:

OnConnect: every time a WebSocket connection is established, this event is fired.

OnDisconnect: every time a WebSocket connection is dropped, this event is fired.

OnError: every time there is a WebSocket error (like mal-formed handshake), this event is fired.

OnMessage: every time a client sends a text message and it's received by server, this event is fired.

OnBinary: every time a client sends a binary message and it's received by server, this event is fired.

OnHandhake: this event is fired after handshake is evaluated on the server side.

OnCommandGet: this event is fired when HTTP Server receives a GET command requesting a HTML page, an image... Example:

```
AResponseInfo.ContentText :=
'<HTML><HEADER>TEST</HEAD><BODY>Hello!</BODY></HTML>';
```

OnCommandOther: this event is fired when HTTP Server receives a command different of GET.

OnCreateSession: this event is fired when HTTP Server creates a new session.

OnInvalidSession: this event is fired when an HTTP request is using an invalid/expiring session.

OnSessionStart: this event is fired when HTTP Server starts a new session.

OnCommandOther: this event is fired when HTTP Server closes a session.

OnException: this event is fired when HTTP Server throws an exception.

OnAuthentication: if authentication is enabled, this event if fired. You can check user and password passed by the client and enable/disable Authenticated Variable.

OnUnknownProtocol: if WebSocket protocol is not detected (because the client is using plain TCP protocol for example), in this event connection can be accepted or rejected.

* In some cases, you may get a high consume of cpu due to unsolicited connections, in these cases, just return an error 500 if it's a HTTP request or close connection for Unknown Protocol requests.

5. Create a procedure and set property Active = true.

Most common uses

- **HTTP**
  - HTTP Server Requests
  - HTTP Dispatch Files
- **Other**
  - HTTP Server Sessions

Methods

Broadcast: sends a message to all connected clients.

Message / Stream: message or stream to send to all clients.

Channel: if you specify a channel, the message will be sent only to subscribers.

Protocol: if defined, the message will be sent only to a specific protocol.

Exclude: if defined, list of connection guid excluded (separated by comma).

Include: if defined, list of connection guid included (separated by comma).

WriteData: sends a message to a single or multiple clients. Every time a Client establishes a WebSocket connection, this connection is identified by a Guid, you can use this Guid to send a message to a client.

Ping: sends a ping to all connected clients.

DisconnectAll: disconnects all active connections.

Properties

Connections: contains a list of all clients connections.

Bindings: used to manage IP and Ports.

DocumentRoot: here you can define a directory where you can put all html files (javascript, HTML, CSS...) if a client sends a request, the server automatically will search this file on this directory, if it finds, it will be served.

Extensions: you can enable compression on messages sent (if client don't support compression, messages will be exchanged automatically without compression).

MaxConnections: max connections allowed (if zero there is no limit).

Count: Connections number count.

AutoStartSession: if SessionState is active, when the server gets a new HTTP request, creates a new session.

SessionState: if active, enables HTTP sessions.

KeepAlive: if enabled, connection will stay alive after the response has been sent.

ReadStartSSL: max. number of times an HTTPS connection tries to start.

SessionList: read-only property used as a container for TIdHTTPSession instances created for the HTTP server.

SessionTimeOut: timeout of sessions.

TsgcWebSocketHTTPServer

HTTP

TsgcWebSocketHTTPServer | HTTP Server Requests

Use OnCommandGet to handle HTTP client requests. Use the following parameters:

- **RequestInfo:** contains HTTP request information.

- **ResponseInfo:** is the HTTP response to HTTP Request.
  - **ContentText:** is the response in text format.
  - **ContentType:** is the type of Content-Type.
  - **ResponseNo:** number of HTTP response, example: 200.

```
procedure OnCommandGet(AContext: TIdContext; ARequestInfo:
TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
begin
  if ARequestInfo.Document = '/' then
  begin
    AResponseInfo.ContentText := '<html><head><title>Test
Page</title></head><body></body></html>';
    AResponseInfo.ContentType := 'text/html';
    AResponseInfo.ResponseNo := 200;
  end;
end;
```

TsgcWebSocketHTTPServer | HTTP Dispatch Files

When a client request a file, **OnCommandGet** event is fired, but you can use **DocumentRoot** property to dispatch automatically files.

Example: if you set **DocumentRoot** to **c:/www/files**. Every time a new file is requested, will search in this folder if file exists and if exists, will be dispatched automatically.

Other

TsgcWebSocketHTTPServer | Sessions

HTTP is state-less protocol (at least till HTTP 1.1), so client request a file, server sends a response to client and connection is closed (well, you can enable keep-alive and then connection is not closed immediately, but this is far beyond the purpose of this article). The use of the sessions, allows to store some information about client, this can be used during a client login for example. You can use whatever session unique ID, search in the list of sessions if already exists and if not exists, create a new session. Session can be destroyed after some time without using it or manually after client logout.

Configuration

There are some properties in TsgcWebSocketHTTPServer which enables/disables sessions in server component. Let's see the most important:

Property	Description
SessionState	This is the first property which has to be enabled in order to use Sessions. Without this property enabled, sessions won't work
SessionTimeout	Here you must set a value greater than zero (in milliseconds) for max time session will be active.
AutoStartSession	Sessions can be created automatically (AutoStartSession = true) or manually (AutoStartSession = false). If Sessions are created automatically, server will use RemoteIP as unique identifier to see if there is an active session stored.

```
TsgcWebSocketHTTPServer1.SessionState := True;
TsgcWebSocketHTTPServer1.SessionTimeout := 600000;
AutoStartSession := False;
```

Create Session

In order to create a new session, we must create a new **session id** which is **unique**, you can use whatever, **example:** if client is authenticating, you can use user + password + remoteip as session id.
Then, we search in Session list if already exists, if not exists, we create a new one.

When a new session is create **OnSessionStart** event is called and when session is closed, **OnSessionEnd** event is raised.

```
procedure OnCommandGet(AContext: TIdContext; ARequestInfo:
TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
var
  vID: String;
  oSession: TIdHTTPSession;
begin
  if ARequestInfo.Document = '/' then
    AResponseInfo.ServeFile(AContext, 'yourpathhere\index.html')
  else
  begin
    // check if user is valid
    if not ((ARequestInfo.AuthUsername = 'user') and
(ARequestInfo.AuthPassword = 'pass')) then
      AResponseInfo.AuthRealm := 'Authenticate'
    else
    begin
      // create a new session id with authentication data
      vID := ARequestInfo.AuthUsername + '_' +
ARequestInfo.AuthPassword + '_' + ARequestInfo.RemoteIP;

      // search session
      oSession := TsgcWebSocketHTTPServer1.SessionList.GetSession(vID,
ARequestInfo.RemoteIP);

      // create new session if not exists
      if not Assigned(oSession) then
        oSession :=
TsgcWebSocketHTTPServer1.SessionList.CreateSession(ARequestInfo.Remote
IP, vID);

      AResponseInfo.ContentText('<html><head></head><body>Authenticate
d</body></html>');
      AResponseInfo.ResponseNo := 200;
    end;
  end;
end;
```

TsgcWebSocketServer_HTTPAPI

The HTTP Server API enables applications to communicate over HTTP without using Microsoft Internet Information Server (IIS). Applications can register to receive HTTP requests for particular URLs, receive WebSocket requests, and send WebSocket responses. The HTTP Server API includes SSL support so that applications can exchange data over secure HTTP connections without IIS. It is also designed to work with I/O completion ports.

Follow the next steps to configure this component:

1. Drop a TsgcWebSocketServer_HTTPAPI component in the form

2. Add which URL/s you need register, example: if connections to port 8080 with "/ws/" parameter is WebSocket connection, register the following URL

```
WSServer.Bindings.NewBinding('127.0.0.1', 8080, '/ws/');
```

3. Set Specifications allowed, by default all specifications are allowed.

RFC6455: is standard and recommended WebSocket specification.

Hixie76: it's a draft and it's only recommended to establish Hixie76 connections if you want to provide support to old browsers like Safari 4.2

4. If you want, you can handle events:

OnConnect: every time a WebSocket connection is established, this event is fired.

OnDisconnect: every time a WebSocket connection is dropped, this event is fired.

OnError: every time there is a WebSocket error (like mal-formed handshake), this event is fired.

OnMessage: every time a client sends a text message and it's received by server, this event is fired.

OnBinary: every time a client sends a binary message and it's received by server, this event is fired.

OnHandhake: this event is fired after the handshake is evaluated on the server side.

OnException: this event is fired when HTTP Server throws an exception.

OnAuthentication: if authentication is enabled, this event is fired. You can check user and password passed by the client and enable/disable Authenticated Variable.

OnUnknownProtocol: if WebSocket protocol is not detected (because the client is using plain TCP protocol for example), in this event connection can be accepted or rejected.

OnAsynchronous: every time an asynchronous event has been completed, this event is called.

5. Create a procedure and set property Active = true

Properties

Timeouts: allows overriding default timeouts of HTTP API Server.

EntityBody: the time, in seconds, allowed for the request entity body to arrive.
DrainEntityBody: The time, in seconds, allowed for the HTTP Server API to drain the entity body on a Keep-Alive connection.
RequestQueue: The time, in seconds, allowed for the request to remain in the request queue before the application picks it up.
IdleConnection: The time, in seconds, allowed for an idle connection.
HeaderWait: The time, in seconds, allowed for the HTTP Server API to parse the request header.
MinSendRate: The minimum sends rate, in bytes-per-second, for the response. The default response sends rate is 150 bytes-per-second.

MaxConnections: maximum number of connections (zero means unlimited, value by default).

MaxBandwidth: maximum allowed bandwidth rate in bytes per second (zero means unlimited, value by default).

ThreadPoolSize: by default 32 (maximum allowed is 64), allows setting number of threads of HTTP API Server.

Asynchronous: by default is disabled, if enabled, messages sent don't wait till completed. You can check when asynchronous is completed **OnAsynchronous** event.

SSLOptions: here you can customize ssl properties.

CertStoreName: allows to set the name of certificate store where is certificate.
Hash: this is the hexadecimal thumbprint value of certificate and is required by server to retrieve certificate. You can find hash of certificate using powershell, running a "dir" comand on the certificates store, example: dir cert:\localmachine\my

Methods

Broadcast: sends a message to all connected clients.

Message / Stream: message or stream to send to all clients.

Channel: if you specify a channel, the message will be sent only to subscribers.

Protocol: if defined, the message will be sent only to a specific protocol.

Exclude: if defined, list of connection guid excluded (separated by comma).

Include: if defined, list of connection guid included (separated by comma).

WriteData: sends a message to a single or multiple clients. Every time a Client establishes a WebSocket connection, this connection is identified by a Guid, you can use this Guid to send a message to a client.

Ping: sends a ping to all connected clients.

DisconnectAll: disconnects all active connections.

TsgcWebSocketClient_SocketIO

This component is **deprecated**, use API SocketIO.

TsgcWebSocketClient_SocketIO inherits all properties and methods from TsgcWebSocketClient and allows connecting to a Socket.IO Server.

Methods

These messages are only supported by ioAPI0:

SendDisconnect: Signals disconnection. If no endpoint is specified, disconnects the entire socket.

Examples:

Disconnect a socket connected to the /test endpoint.

```
SendDisconnect('/test');
```

Disconnect the whole socket

```
SendDisconnect;
```

SendConnect: Only used for multiple sockets. Signals a connection to the endpoint. Once the server receives it, it's echoed back to the client.

Example, if the client is trying to connect to the endpoint /test, a message like this will be delivered:

```
SendConnect('[path] [query]');
```

Example:

```
SendConnect('/test?my=param');
```

To acknowledge the connection, the server echoes back the message. Otherwise, the server might want to respond with an error packet.

SendHeartBeat: Sends a heartbeat. Heartbeats must be sent within the interval negotiated with the server. It's up to the client to decide the padding (for example, if the heartbeat timeout negotiated with the server is 20s, the client might want to send a heartbeat every 15s).

Example:

```
SendHeartBeat;
```

SendTextMessage: A regular message.

Example: send a text message "Hi Folks", with id "fjghs121" to clients connected to EndPoint "/test"

```
SendTextMessage('Hi Folks', 'fjghs121', '/test');
```

SendJSONMessage: A JSON encoded message.

Example: send a JSON encoded message "{"a":"b"}"

```
SendJSONMessage('{"a":"b"}');
```

SendEvent: An event is like a JSON message, but has a mandatory name and args fields. The name is a string and args an array.

The event names: 'message', 'connect', 'disconnect', 'open', 'close', 'error', 'retry', 'reconnect' are reserved, and cannot be used by clients or servers with this message type.

Example: send event "test" with arguments "["1","2","3"]"

```
SendEvent('test', ["1","2","3"]);
```

SendACK: An acknowledgement contains the message id as the message data. If a + sign follows the message id, it's treated as an event message packet.

Example: simple acknowledgement of message id "2"

```
SendACK("2");
```

SendError: For example, if a connection to a sub-socket is unauthorized.

Example: send error "not authorized" with advise "connect with admin user"

```
SendError("not authorized", "connect with admin user");
```

SendNoop: No operation. Used for example to close a poll after the polling duration times out.

Example:

```
SendNoop;
```

Events

These events are only raised if "RawMessages" property is disabled and ioAPI0 is selected.

OnMessageDisconnect

OnMessageConnect

OnMessageHeartBeat

OnMessageText

OnMessageJSON

OnMessageEvent

OnMessageACK

OnMessageError

OnMessageNoop

Properties

RawMessages: if not enabled (which is default) socket.io messages are processed and specific socket.io messages events are raised, if enabled, then socket.io messages are not processed and OnMessage event is raised.

IO_API: specifies SocketIO version:

ioAPI0: supports socket.io 0.* servers (selected by default)

ioAPI1: supports socket.io 1.* servers

IO_CloseTimeout: close timeout received from Socket.io server.

IO_HandShakeTimestamp: only enable if you want to send timestamp as a parameter when a new session is requested (enable this property if you try to access a gevent-socketio python server).

IO_HeartBeatTimeout: HeartBeat timeout received from Socket.io server.

IO_SessionId: SessionId received from Socket.io server.

IO_Base64: if enabled, binary messages are received as base64.

IO_HandShakeCustomURL: allows customizing url to get socket.io session.

IO_Namespace: allows setting a namespace when connects to a server.

TsgcWSHTTPWebBrokerBridgeServer

TsgcWSHTTPWebBrokerBridgeServer use **TIdHttpWebBrokerBridge** as server base and is useful if you want to use a single server for DataSnap, HTTP and WebSocket connections.

TsgcWSHTTPWebBrokerBridgeServer inherits from **TsgcWebSocketHTTPServer**, so you can refer to this server.

Follow next steps to replace TIdHttpWebBrokerBridge for TsgcWSHTTPWebBrokerBridgeServer :

1. Create a new instance of TsgcWSHTTPWebBrokerBridgeServer.

2. Replace all calls to TIdHttpWebBrokerBridge for TsgcWSHTTPWebBrokerBridgeServer.

3. To Handle WebSocket connections just refer to TsgcWebSocketHTTPServer.

Events

```
//OnCommandRequest
// When server gets a new HTTP request, this event is called and here
you can customize http response.

FServer := TsgcWSHTTPWebBrokerBridgeServer.Create(Self);
FServer.OnCommandRequest := OnCommandRequestEvent;
FServer.OnCommandGet := OnCommandGetevent;

procedure OnCommandRequestEvent(AThread: TIdContext; ARequestInfo:
TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo; var aHandled:
Boolean);
begin
  if ARequestInfo.Document = '/test.html' then
    aHandled := True;
end;

procedure OnCommandGetevent(AContext: TIdContext; ARequestInfo:
TIdHTTPRequestInfo; AResponseInfo: TIdHTTPResponseInfo);
begin
  if ARequestInfo.Document = '/test.html' then
  begin
    AResponseInfo.ResponseNo := 200;
    AResponseInfo.ContentText := 'hello all';
  end;
end;
```

TsgcWebSocketClient_WinHTTP

TsgcWebSocketClient implements Client VCL WebSocket Component and can connect to a WebSocket Server, it's based on WinHTTP API and requires Windows 8 or higher. Follow the next steps to configure this component:

1. Drop a TsgcWebSocketClient_WinHTTP component in the form

2. Set Host and Port (default is 80) to connect to an available WebSocket Server. You can set URL property and Host, Port, Parameters... will be updated from URL. Example: wss://127.0.0.1:8080/ws/ will result:

```
oClient := TsgcWebSocketClient_WinHTTP.Create(nil);
oClient.Host := '127.0.0.1';
oClient.Port := 80;
oClient.TLS := True;
oClient.Options.Parameters := '/ws/';
```

3. You can select if you want TLS (secure connection) or not, by default is not Activated.

4. If you want, you can handle events

OnConnect: when a WebSocket connection is established, this event is fired

OnDisconnect: when a WebSocket connection is dropped, this event is fired

OnError: every time there is a WebSocket error (like mal-formed handshake), this event is fired

OnMessage: every time the server sends a text message, this event is fired

OnBinary: every time the server sends a binary message, this event is fired

OnException: every time an exception occurs, this event is fired.

8. Create a procedure and set property Active = True.

Methods

WriteData: sends a message to a WebSocket Server. Could be a String or TStream.

Properties

Authentication: if enabled, WebSocket connection will try to authenticate passing a username and password.

Implements 1 type of WebSocket Authentication

Basic: client open WebSocket connection passing username and password inside the header.

Asynchronous: by default, requests are synchronous, execution of your application stops when you make new requests and resumes when you get a response. If you don't want that requests stop your application, enable this property.

Host: IP or DNS name of the server.

HeartBeat: if enabled try to keeps alive a WebSocket connection sending a ping every x seconds.

Interval: number of seconds between each ping.

Timeout: max number of seconds between a ping and pong.

ReadTimeout: max time in milliseconds to read messages.

Port: Port used to connect to the host.

NotifyEvents: defines which mode to notify websocket events.

neAsynchronous: this is the default mode, notify threaded events on asynchronous mode, adds events to a queue that are synchronized with the main thread asynchronously.

neSynchronous: if this mode is selected, notify threaded events on synchronous mode, needs to synchronize with the main thread to notify these events.

neNoSync: there is no synchronization with the main thread, if you need to access to controls that are not thread-safe, you need to implement your own synchronization methods.

Options: allows customizing headers sent on the handshake.

Parameters: define parameters used on GET.

Origin: customize connection origin.

Protocol: if exists, shows the current protocol used

Proxy: here you can define if you want to connect through an HTTP Proxy Server.

WatchDog: if enabled, when an unexpected disconnection is detected, tries to reconnect to the server automatically.

Interval: seconds before reconnects.

Attempts: max number of reconnects, if zero, then unlimited.

TLS: enables a secure connection.

TsgcWebSocketLoadBalancerServer

TsgcWebSocketLoadBalancerServer allows distributing messages across a group of servers and distributes clients connections using a random sequence or fewer connections algorithm.

Load Balancer Server, inherits all methods and properties from TsgcWebSocketServer.

Follow the next steps to configure this component:

1. Drop a TsgcWebSocketLoadBalancerServer component in the form

2. Set Port (default is 80). If you are behind a firewall probably you will need to configure it.

3. Configure LoadBalancer properties:

> **3.1** lbRandom: every time a new client request a new connection, it will return a random server.
>
> **3.1** lbConnections: every time a new client request a new connection, it will return server with fewer clients connected.

4. There are serveral events which are specific of LoadBalancerServer:

OnBeforeSendServerBinding: raised before binding is sent to a new client connection.

OnClientConnect: every time a client connection is stablished, this event is fired.

OnClientDisconnect: every time a client connection is dropped, this event is fired.

OnClientMessage: raised when a new text message is received from the server.

OnClientBinary: raised when a new binary message is received from the server.

OnClientFragmented: raised when a new fragmented message is received from the server.

OnServerConnect: raised when a new server connects to LoadBalancerServer.

OnServerDisconnect: raised when a server disconnects from LoadBalancerServer.

OnServerReady: raised when a server is ready to accept messages.

5. Configure "LoadBalancer" property of back-up servers, to connect to LoadBalancer Server.

6. Create a procedure and set property Active = true

TsgcWebSocketProxyServer

TsgcWebSocketProxyServer implements a WebSocket Server Component which listens to client WebSocket connections and forwards data connections to a normal TCP/IP server. This is especially useful for browser connections because allows a browser to virtually connect to any server.

TsgcIWWebSocketClient

TsgcIWWebSocketClient implements Intraweb WebSocket Component and can connect to a WebSocket Server. Follow the next steps to configure this component:

1. Drop a TsgcIWWebSocketClient component in the form

2. Set Host and Port (default is 80) to connect to an available WebSocket Server. You can set URL property and Host, Port, Parameters... will be updated from URL. Example: wss://127.0.0.1:8080/ws/ will result:

```
oClient := TsgcIWWebSocketClient.Create(nil);
oClient.Host := '127.0.0.1';
oClient.Port := 80;
oClient.TLS := True;
oClient.Options.Parameters := '/ws/';
```

3. You can select if you want TLS (secure connection) or not, by default is not Activated.

4. Set Transports allowed.

WebSockets: it will use standard WebSocket implementation

Emulation: if browser doesn't support WebSockets, then it will use a loop AJAX callback connection

5. If you want, you can handle events

OnAsyncConnect: when a WebSocket connection is established, this event is fired

OnAsyncDisconnect: when a WebSocket connection is dropped, this event is fired

OnAsyncError: every time there is a WebSocket error (like mal-formed handshake), this event is fired

OnAsyncMessage: every time the server sends a message, this event is fired

OnAsyncEmulation: this event is fired on every loop of emulated connection

6. Create an Async Procedure and set property Active := True

Methods

Open: Opens a WebSocket Connection.

Close: Closes a WebSocket Connection.

WriteData: sends a message to WebSocket Server.

Properties

Connected: is a read-only variable and returns True if the connection is Active, otherwise returns False.

JSOpen: here you can include JavaScript Code on the client side when a connection is opened.

JSClose: here you can include JavaScript Code on the client side when a connection is closed.

JSMessage: here you can include JavaScript Code on the client side when clients receive a message from the server. You can get Message String, using Javascript variable "text".

JSError: here you can include JavaScript Code on the client side when an error is raised. You can get Message Error, using Javascript variable "text".

Connections

TsgcWSConnection

TsgcWSConnection is a wrapper of client WebSocket connections, you can access to this object on Server or Client Events.

Methods

WriteData: sends a message to the client.

Close: sends a close message to other peer. A "CloseCode" can be specified optinally.

Disconnect: close client connection from the server side. A "CloseCode" can be specified optionally.

Ping: sends a ping to the client.

AddTCPEndOfFrame: if connection is plain TCP, allows to set which byte/s define the end of message. Message is buffered till is received completely.

Subscribed: returns if the connection is subscribed to a custom channel.

Subscribe: subscribe this connection to a channel. Later you can Broadcast a message from server component to all connections subscribed to this channel.

UnSubscribe: unsubscribe this from connection from a channel.

Properties

Protocol: returns sub-protocol used on this connection.

IP: returns Peer IP Address.

Port: returns Peer Port.

LocalIP: returns Host IP Address.

LocalPort: returns Host Port.

URL: returns URL requested by the client.

Guid: returns connection ID.

HeadersRequest: returns a list of Headers received on Request.

HeadersResponse: returns a list of Headers sent as Response.

RecBytes: number of bytes received.

SendBytes: number of bytes sent.

Transport: returns the transport type of connection:

trpRFC6455: a normal WebSocket connection.

trpHixie76: a WebSocket connection using draft WebSocket spec.

trpFlash: a WebSocket connection using Flash as FallBack.

trpSSE: a Server-Sent Events connection.

trpTCP: plain TCP connection.

TCPEndOfFrameScanBuffer: allows to define which method use to find end of message (if using trpTCP as tansport).

eofScanNone: every time a new packet arrive, OnBinary event is called.

eofScanLatestBytes: if latest bytes are equal to bytes added with AddTCPEndOfFrame method, OnBinary message is called, otherwise this packet is buffered

eofScanAllBytes: search in all packet if find bytes equal to bytes added with AddTCPEndOfFrame method. If true, OnBinary message is called, otherwise this packet is buffered

Data: user session data object, here you can pass an object and access this every time you need, for example: you can pass a connection to a database, user session properties...

Protocols

Protocols

With WebSockets, you can implement Sub-protocols allowing to create customized communications, **for example** you can implement a sub-protocol over WebSocket protocol to communicate a customized application using JSON messages, and you can implement another sub-protocol using XML messages.

When a connection is open on the Server side, it will validate if sub-protocol sent by the client is supported by the server, if not, then it will close the connection. A server can implement several sub-protocols, but only one can be used on a single connection.

Sub-protocols are very useful to create customized applications and be sure that all clients support the same communication interface.

Although the protocol name is arbitrary, it's recommended to use unique names like "dataset.esegece.com"

With sgcWebSockets package, you can build your own protocols and you can use built-in sub-protocols provided:

1. Protocol SGC: implemented using JSON-RPC 2.0 messages, provides the following patterns: RPC, PubSub, Transactional Messages, Messages Acknowledgment and more.

2. Protocol Dataset: inherits from Default Protocol, can send dataset changes (new record, save record or delete a record) from the server to clients.

3. Protocol Files: implemented using binary messages, provides support for send files: packet size, authorization, QoS, message acknowledgement and more.

4. Protocol Presence: allows to know who is subscribed to a channel, example: chat rooms, collaborators on a document, people viewing the same web page, competitors in a game...

5. Protocol AppRTC: is a webrtc demo application developed by Google and Mozilla, it enables both browsers to “talk” to each other using the WebRTC API.

6. Protocol WebRTC: open source project aiming to enable the web with Real-Time Communication (RTC) capabilities.

7. Protocol WAMP 1.0: open WebSocket subprotocol that provides two asynchronous messaging patterns: RPC and PubSub.

8. Protocol WAMP 2.0: open WebSocket subprotocol that provides two asynchronous messaging patterns: RPC and PubSub.

9. Protocol MQTT: MQTT is a Client Server publish/subscribe messaging transport protocol. It is lightweight, open, simple, and designed so as to be easy to implement.

10. Protocol STOMP: STOMP is the Simple (or Streaming) Text Orientated Messaging Protocol. STOMP provides an interoperable wire format so that STOMP clients can communicate with any STOMP message broker to provide easy and widespread messaging interoperability among many languages, platforms and brokers.

10.1 STOMP for RabbitMQ: client for RabbitMQ Broker.

10.2 STOMP for ActiveMQ: client for ActiveMQ Broker.

If you need to use **more than one protocol using a single connection** (example: you may need to use **default protocol** to handle Remote Procedure Calls and **Dataset protocol** to handle database connections) you can assign a "Broker" to each protocol component and all messages will be exchanged using this intermediary protocol (you can check "Tickets Demo" to get a simple example of this).

Protocols can be registered at **runtime**, just call Method **RegisterProtocol** and pass protocol component as a parameter.

Javascript Reference

Here you can get more information about common javascript library used on sgcWebSockets.

Protocols Javascript

Default Javascript sgcWebSockets uses **sgcWebSocket.js** file.

Here you can find available methods, you need to replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure your access to sgcWebSocket.js file as:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
```

Open Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
</script>
```

sgcWebSocket has 3 parameters, only first is required:

```
sgcWebSocket(url, protocol, transport)
```

- **URL:** WebSocket server location, you can use "ws:" for normal WebSocket connections and "wss:" for secured WebSocket connections.

  ```
  sgcWebSocket('ws://127.0.0.1')

  sgcWebSocket('wss://127.0.0.1')
  ```

- **Protocol:** if the server accepts one or more protocol, you can define which is the protocol you want to use.

  ```
  sgcWebSocket('ws://127.0.0.1', 'esegece.com')
  ```

- **Transport:** by default, first tries to connect using WebSocket connection and if not implemented by Browser, then tries Server Sent Events as Transport.

  Use WebSocket if implemented, if not, then use Server Sent Events:

  ```
  sgcWebSocket('ws://127.0.0.1')
  ```

  Only use WebSocket as transport:

  ```
  sgcWebSocket('ws://127.0.0.1', '', ['websocket'])
  ```

  Only use Server Sent as transport:

  ```
  sgcWebSocket('ws://127.0.0.1', '', ['sse'])
  ```

Open Connection With Authentication

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
```

```
<script>
  var socket = new
sgcWebSocket({"host":"ws://{%host%}:{%port%}","user":"admin","password
":"1234"});
</script>
```

Send Message

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
  socket.send('Hello sgcWebSockets!');
</script>
```

Show Alert with Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
  socket.on('message', function(event)
  {
    alert(event.message);
  }
</script>
```

Binary Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
  socket.on('stream', function(event)
  {
    document.getElementById('image').src =
URL.createObjectURL(event.stream);
    event.stream = "";
  }
</script>
```

Binary (Header + Image) Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
  socket.on('stream', function(event)
  {
```

```
    sgcWSStreamRead(evt.stream, function(header, stream) {
      document.getElementById('text').innerHTML = header;
      document.getElementById('image').src =
URL.createObjectURL(event.stream);
      event.stream = "";
    }
  }
</script>
```

Show Alert OnConnect, OnDisconnect and OnError Events

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  var socket = new sgcWebSocket('ws://{%host%}:{%port%}');
  socket.on('open', function(event)
  {
    alert('sgcWebSocket Open!');
  };
  socket.on('close', function(event)
  {
    alert('sgcWebSocket Closed!');
  };
  socket.on('error', function(event)
  {
    alert('sgcWebSocket Error: ' + event.message);
  };
</script>
```

Close Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  socket.close();
</script>
```

Get Connection Status

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script>
  socket.state();
</script>
```

Subprotocols

Default

Protocol Default

This is default sub-protocol implemented using "JSONRPC 2.0" messages, every time you send a message using this protocol, a JSON object is created with the following properties:

jsonrpc: A String specifying the version of the JSON-RPC protocol. MUST be exactly "2.0".

method: A String containing the name of the method to be invoked. Method names that begin with the word rpc followed by a period character (U+002E or ASCII 46) are reserved for rpc-internal methods and extensions and MUST NOT be used for anything else.

params: A Structured value that holds the parameter values to be used during the invocation of the method. This member MAY be omitted.

id: An identifier established by the Client that MUST contain a String, Number, or NULL value if included. If it is not included it is assumed to be a notification. The value SHOULD normally not be Null [1] and Numbers SHOULD NOT contain fractional parts [2]

JSON object example:

```
{"jsonrpc": "2.0", "method": "subtract", "params": [42, 23], "id": 1}
```

Features

- **Publish/subscribe** message pattern to provide one-to-many message distribution and decoupling of applications. Supports Wildcard characters, so you can subscribe to a hierarchy of channels. Example: if you want to subscribe to all channels which start with 'news', then call Subscribe('news*').
- A messaging transport that is **agnostic** to the content of the payload
- **Acknowledgment** of messages sent.
- Supports **transactional messages** through server local transactions. When the client commits the transaction, the server processes all messages queued. If client rollback the transaction, then all messages are deleted.
- Implements **QoS** (Quality of Service) for message delivery.

Components

TsgcWSPClient_sgc: Server Protocol Default VCL Component.

TsgcWSPClient_sgc: Client Protocol Default VCL Component.

Javascript Component: Client Javascript Reference.

Browser Test

If you want to test this protocol with your favourite Web Browser, please type this URL (you need to define your custom host and port)

```
http://host:port/esegece.com.html
```

TsgcWSPServer_sgc

This is Server Protocol Default Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

Methods

Subscribe / UnSubscribe: subscribe/unsubscribe to a channel. Supports wildcard characters, so you can subscribe to a hierarchy of channels. Example: if you want to subscribe to all channels which start with 'news', then call Subscribe('news*').

Publish: sends a message to all subscribed clients. Supports wildcard characters, so you can publish to a hierarchy of channels. Example: if you want to send a message to all subscribers to channels which start with 'news', then call Publish('news*').

RPCResult: if a call RPC from the client is successful, the server will respond with this method.

RPCError: if a call RPC from the client it has an error, the server will respond with this method.

Broadcast: sends a message to all connected clients, if you need to broadcast a message to selected channels, use Channel argument.

WriteData: sends a message to single or multiple selected clients.

Properties

RPCAuthentication: if enabled, every time a client requests an RPC, method name needs to be authenticated against a username and password.

Methods: is a list of allowed methods. Every time a client sends an RPC first it will search if this method is defined on this list, if it's not in this list, OnRPCAuthentication event will be fired.

Subscriptions: returns a list of active subscriptions.

UseMatchesMasks: if enabled, subscriptions and publish methods accepts wildcards, question marks... check MatchesMask Delphi function to see all supported masks.

Events

OnRPCAuthentication: if RPC Authentication is enabled, this event is fired to define if a client can call this method or not.

OnRPC: fired when the server receives an RPC from a client.

OnNotification: fired every server receive a Notification from a client.

OnBeforeSubscription: fired every time before a client subscribes to a custom channel. Allows denying a subscription.

OnSubscription: fired every time a client subscribes to a custom channel.

OnUnSubscription: fired every time a client unsubscribes from a custom channel.

OnRawMessage: this event is fired before a message is processed by component.

TsgcWSPClient_sgc

This is Client Protocol Default Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Methods

Publish: sends a message to all subscribed clients.

RPC: Remote Procedure Call, client request a method and response will be handled OnRPCResult or OnRPCError events.

Notify: the client sends a notification to a server, this notification doesn't need a response.

Broadcast: sends a message to all connected clients, if you need to broadcast a message to selected channels, use Channel argument.

WriteData: sends a message to a server. If you need to send a message to a custom TsgcWSProtocol_Server_sgc, use "Guid" Argument. If you need to send a message to a single channel, use "Channel" Argument.

Subscribe: subscribe client to a custom channel. If the client is subscribed, OnSubscription event will be fired.

Unsubscribe: unsubscribe client to a custom channel. If the client is unsubscribed, OnUnsubscription event will be fired.

UnsubscribeAll: unsubscribe client from all subscribed channel. If the client is unsubscribed, OnUnsubscription event will be fired for every channel.

GetSession: requests to server session id, data session is received OnSession Event.

StartTransaction: begins a new transaction.

Commit: server processes all messages queued in a transaction.

RollBack: server deletes all messages queued in a transaction.

Events

OnEvent: this event is fired every time a client receives a message from a custom channel.

OnRPCResult: this event is fired when the client receives a successful response from the server after a RPC is sent.

OnRPCError: this event is fired when the client receives a error response from the server after an RPC is sent.

OnAcknowledgment: this event is fired when the client receives error an acknowledgment from the server that message has been received.

OnRawMessage: this event is fired before a message is processed by the component.

OnSession: this event is fired after a successful connection or after a GetSession request.

Properties

Queue: disabled by default, if True all text/binary messages are not processed and queued until queue is disabled.

QoS: Three "Quality of Service" provided:

Level 0: "At most once", the message is delivered according to the best efforts of the underlying TCP/IP network. A response is not expected and no retry semantics are defined in the protocol. The message arrives at the server either once or not at all.

Level 1: "At least once", the receipt of a message by the server is acknowledged by an ACKNOWLEDGMENT message. If there is an identified failure of either the communications link or the sending device, or the acknowledgement message is not received after a specified period of time, the sender resends the message. The message arrives at the server at least once. A message with QoS level 1 has an ID param in the message.

Level 2: "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied. If there is an identified failure of either the communications link or the sending device, or the acknowledgement message is not received after a specified period of time, the sender resends the message.

Subscriptions: returns a list of active subscriptions.

TsgcIWWSPClient_sgc

This is Intraweb Client Protocol Default Component, you need to drop this component in the form and select a TsgcIWWebSocketClient Component using Client Property.

Methods

WriteData: sends a message to a server. If you need to send a message to a custom TsgcWSProtocol_Server_sgc, use "Guid" Argument. If you need to send a message to a single channel, use "Channel" Argument.

Subscribe: subscribe client to a custom channel. If the client is subscribed, OnSubscription event will be fired.

Unsubscribe: unsubscribe client to a custom channel. If client is unsubscribed, OnUnsubscription event will be fired.

Protocol Default Javascript

Default Protocol Javascript sgcWebSockets uses **sgcWebSocket.js and esegece.com.js** files.

Here you can find available methods, you need to replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
<script src="http://www.example.com:80/esegece.com.js"></script>
```

Open Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
</script>
```

Send Message

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.send('Hello sgcWebSockets!');
</script>
```

Show Alert with Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcmessage', function(event)
  {
    alert(event.message);
  }
</script>
```

Publish Message to test channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.publish('Hello sgcWebSockets!', 'test');
</script>
```

Show Alert with Event Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
```

```
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcevent', function(event)
  {
    alert('channel:' + event.channel + '. message: ' + event.message);
  }
</script>
```

Call RPC

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  var params = {param:10};
  socket.rpc(GUID(), 'test', JSON.stringify(params));
</script>
```

Handle RPC Response

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcrpcresult', function(event)
  {
    alert('result:' + event.result);
  }
  socket.on('sgcrpcerror', function(event)
  {
    alert('error:' + event.code + ' ' + event.message);
  }
</script>
```

Call Notify

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  var params = {param:10};
  socket.notify('test', JSON.stringify(params));
</script>
```

Send Messages in a Transaction

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');

  socket.starttransaction('sgc:test');
  socket.publish('Message1', 'sgc:test');
  socket.publish('Message2', 'sgc:test');
  socket.publish('Message3', 'sgc:test');
  socket.commit('sgc:test');
```

```
</script>
```

Show Alert OnSubscribe or OnUnSubscribe to a channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcsubscribe', function(event)
  {
    alert('subscribed: ' + event.channel);
  }
  socket.on('sgcunsubscribe', function(event)
  {
    alert('unsubscribed: ' + event.channel);
  }
</script>
```

Show Alert OnConnect, OnDisconnect and OnError Events

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('open', function(event)
  {
    alert('sgcWebSocket Open!');
  };
  socket.on('close', function(event)
  {
    alert('sgcWebSocket Closed!');
  };
  socket.on('error', function(event)
  {
    alert('sgcWebSocket Error: ' + event.message);
  };
</script>
```

Get Session

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcsession', function(event)
  {
    alert(event.guid);
  };
  socket.getsession();
</script>
```

Close Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  socket.close();
```

```
</script>
```

Get Connection Status

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');

  socket.state();
</script>
```

Set QoS

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');

  socket.qoslevel1();
  socket.publish('message', 'channel');
</script>
```

Set Queue Level

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');

  socket.queuelevel2();
  socket.publish('message1', 'channel1');
  socket.publish('message2', 'channel1');
</script>
```

Dataset

Protocol Dataset

This protocol inherits from Protocol Default and it's useful if you want to broadcast dataset changes over clients connected to this protocol.

It uses "JSON-RPC 2.0" Object, and every time there is a dataset change, it sends all field values (* only fields supported) using Dataset Object.

To allow the component to search records on the dataset, you need to specify which fields are the Key, example: if in your dataset, ID field is the key you will need to write a code like this

```
procedure OnAfterOpenDataSet(DataSet: TDataSet);
begin
  DataSet.FieldByName('ID').ProviderFlags :=
    Dataset.FieldByName('ID').ProviderFlags + [pfInKey];
end;
```

Components
TsgcWSPServer_Dataset: Server Protocol Dataset VCL Component.

TsgcWSPClient_Dataset: Client Protocol Dataset VCL Component.

Javascript Component: Client Javascript Reference.

Browser Test
If you want to test this protocol with your favourite Web Browser, please type this URL (you need to define your custom host and port)

```
http://host:port/dataset.esegece.com.html
```

TsgcWSPServer_Dataset

This is Server Protocol Dataset Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property and select a Dataset Component using Dataset Property.

This component inherits from TsgcWSProtocol_Server_sgc all methods and properties.
Properties
ApplyUpdates: if enabled, every time the server receives a dataset update from client, it will be saved on the server side.

NotifyUpdates: if enabled, every time dataset server changes, server broadcasts this change to all connected clients.

NotifyDeletes: if enabled, every time a record is deleted, server broadcasts this to all connected clients.

AutoEscapeText: if enabled (disabled by default), automatically escape/unescape characters inside field values like "{", "["...

AutoSynchronize: if enabled, every time a client connects to the server, the server will sent metadata and all dataset records to client.

UpdateMode: if umWhereAll (by default) all fields are broadcasted to clients, if umWhereChanged only Fields that have changed will be broadcasted to connected clients.

Methods
BroadcastRecord: sends dataset record values to all connected clients.

MetaData: sends metadata info to a client.

Synchronize: sends all dataset records to a client.

Events
These events are specific on the dataset protocol.

OnAfterDeleteRecord: event fired after a record is deleted from Dataset.

OnAfterNewRecord: event fired after a record is created on Dataset.

OnAfterUpdateRecord: event fired after a record is updated on Dataset.

OnBeforeDeleteRecord: event fired before a record is deleted from Dataset. If Argument "Handled" is True, means that the user handles this event and if won't be deleted (by default this argument is False)

OnBeforeNewRecord: event fired before a record is created on Dataset. If Argument "Handled" is True, means that the user handles this event and if won't be inserted (by default this argument is False)

OnBeforeUpdateRecord: event fired before a record is updated on Dataset. If Argument "Handled" is True, means that the user handles this event and if won't be updated (by default this argument is False)

OnBeforeDatasetUpdate: event fired before a dataset record is updated.

TsgcWSPClient_Dataset

This is Client Protocol Dataset Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property and select a Dataset Component using Dataset Property.

This component inherits from TsgcWSProtocol_Client_sgc all methods and properties.

Methods
Subscribe_all: subscribe to all available channels

new: fired on new dataset record.
update: fired on post dataset record.
delete: fired on delete dataset record.

Synchronize: requests all dataset records from the server

GetMetaData: requests all dataset fields from server

Events
These events are specific on the dataset protocol.

OnAfterDeleteRecord: event fired after a record is deleted from Dataset.

OnAfterNewRecord: event fired after a record is created on Dataset.

OnAfterUpdateRecord: event fired after a record is updated on Dataset.

OnAfterSynchronize: event fired after synchronization has ended.

OnBeforeDeleteRecord: event fired before a record is deleted from Dataset. If Argument "Handled" is True, means that the user handles this event and if won't be deleted (by default this argument is False)

OnBeforeNewRecord: event fired before a record is created on Dataset. If Argument "Handled" is True, means that user the handles this event and if won't be inserted (by default this argument is False)

OnBeforeUpdateRecord: event fired before a record is updated on Dataset. If Argument "Handled" is True, means that user the handles this event and if won't be updated (by default this argument is False)

OnBeforeSynchronization: event fired before a synchronization starts.

OnMetaData: event fired after a GetMetaData request. Example:

```
procedure OnMetaData(Connection: TsgcWSConnection; const JSON:
TsgcObjectJSON);
var
  i: integer;
  vFieldName, vDataType: string;
  vDataSize: Integer;
  vKeyField: Boolean;
begin
  for i:= 0 to JSON.Count -1 do
```

```
  begin
    vFieldName := JSON.Item[i].Node['fieldname'].Value;
    vDataType := JSON.Item[i].Node['datatype'].Value;
    vDataSize := JSON.Item[i].Node['datasize'].Value;
    vKeyField := JSON.Item[i].Node['keyfield'].Value;
  end;
end;
```

Properties

AutoSubscribe: enabled by default, if True, client subscribes to all available channels after successful connection.

ApplyUpdates: if enabled, every time the client receives a dataset update from server, it will be saved on the client side.

AutoEscapeText: if enabled (disabled by default), automatically escape/unescape characters inside field values like "{", "["...

NotifyUpdates: if enabled, every time dataset client changes, it sends a message to server notifying this change.

UpdateMode: if umWhereAll (by default) all fields are transmitted to the server, if umWhereChanged only Fields that have changed will be transmitted to the server.

TsgcIWWSPClient_Dataset

This is Intraweb Client Protocol Dataset Component, you need to drop this component in the form and select a TsgcIWWebSocketClient Component using Client Property and select a Dataset Component using Dataset Property.

This component inherits from TsgcIWWSPClient_sgc all methods and properties.

Methods
Subscribe_New: fired on new dataset record
Subscribe_Update: fired on post dataset record
Subscribe_Delete: fired on delete dataset record

Protocol Dataset Javascript

Dataset Protocol Javascript sgcWebSockets uses **sgcWebSocket.js and dataset.esegece.com.js** files.

Here you can find available methods, you need to replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
<script
src="http://www.example.com:80/dataset.esegece.com.js"></script>
```

Open Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws_dataset('ws://{%host%}:{%port%}');
</script>
```

Send Message

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws_dataset('ws://{%host%}:{%port%}');
  socket.send('Hello sgcWebSockets!');
</script>
```

Show Alert with Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcdataset', function(event)
  {
    alert(event.dataset);
  }
</script>
```

Show Alert with Dataset Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws_dataset('ws://{%host%}:{%port%}');
  socket.on('sgcmessage', function(event)
```

```
  {
    alert(event.message);
  }
</script>
```

Show Alert OnSubscribe or OnUnSubscribe to a channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws_dataset('ws://{%host%}:{%port%}');
  socket.on('sgcsubscribe', function(event)
  {
    alert('subscribed: ' + event.channel);
  }
  socket.on('sgcunsubscribe', function(event)
  {
    alert('unsubscribed: ' + event.channel);
  }
</script>
```

Show Alert OnConnect, OnDisconnect and OnError Events

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  var socket = new sgcws_dataset('ws://{%host%}:{%port%}');
  socket.on('open', function(event)
  {
    alert('sgcWebSocket Open!');
  };
  socket.on('close', function(event)
  {
    alert('sgcWebSocket Closed!');
  };
  socket.on('error', function(event)
  {
    alert('sgcWebSocket Error: ' + event.message);
  };
</script>
```

Subscribe All Dataset Changes

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  socket.subscribe_all();
</script>
```

UnSubscribe All Dataset Changes

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
```

```
<script>
  socket.unsubscribe_all();
</script>
```

Handle Dataset Changes

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
var socket = new sgcws_dataset('ws://{%host%}:{%port%}');

socket.on('sgcdataset', function(evt){

if ((evt.channel == "sgc@dataset@new") || (evt.channel ==
"sgc@dataset@update")) {

... here you need to implement your own code insert/update records ...
}
else if (evt.channel == "sgc@dataset@delete") {

... here you need to implement your own code to delete records ...

}
});
</script>
```

Close Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  socket.close();
</script>
```

Get Connection Status

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/dataset.esegece.com.js"></script>
<script>
  socket.state();
</script>
```

Files

Protocol Files

This protocol allows sending files using binary WebSocket transport. It can handle big files with a low memory usage.

Features

- **Publish/subscribe** message pattern to provide one-to-many message distribution and decoupling of applications.
- **Acknowledgment** of messages sent.
- Implements **QoS** (Quality of Service) for file delivery.
- Optionally can request **Authorization** for files received.
- **Low memory** usage.

Components

TsgcWSPServer_Files: Server Protocol Files VCL Component.

TsgcWSPClient_Files: Client Protocol Files VCL Component.

Classes

TsgcWSMessageFile: the object which encapsulates file packet information.

TsgcWSPServer_Files

This is the Server Files Protocol Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

Methods

SendFile: sends a file to a client, you can set the following parameters

aSize: size of every packet in bytes.
aData: user custom data, here you can write any text you think is useful for client.
aChannel: if you only want to send data to all clients subscribed to this channel.
aQoS: type of quality of service.
aFileId: if empty, will be set automatically.

BroadcastFile: sends a file to all connected clients. You can set several parameters:

aSize: size of every packet in bytes.
aData: user custom data, here you can write any text you think is useful for client.
aChannel: if you only want to send data to all clients subscribed to this channel.
aExclude: connection guids separated by a comma, which you don't want to send this file.
aInclude: connection guids separated by a comma, which you want to send this file.
aQoS: type of quality of service.
aFileId: if empty, will be set automatically.

Properties

Files: files properties.

BufferSize: default size of every packet sent, in bytes.

SaveDirectory: the directory where all files will be stored.

QoS: quality of service

Interval: interval to check if a qosLevel2 message has been sent.

Level: level of quality of service.

qosLevel0: the message is sent.

qosLevel1: the message is sent and you get an acknowledgment if the message has been processed.

qosLevel2: the message is sent, you get an acknowledgment if the message has been processed and packets are requested by the receiver.

Timeout: maximum wait time.

ClearReceivedStreamsOnDisconnect: if disabled, when reconnects, try to resume file download for qosLevel2, by default is enabled.

ClearSentStreamsOnDisconnect: tif disabled, when reconnects, try to resume file upload for qosLevel2, by default is enabled.

Events

OnFileBeforeSent: fired before a file is sent. You can use this event to check file data before is sent.

OnFileReceived: fired when a file is successfully received.

OnFileReceivedAuthorization: fired to check if a file can be received.

OnFileReceivedError: fired when an error occurs receiving a file.

OnFileReceivedFragment: fired when a fragment file is received. Useful to show progress.

OnFileSent: fired when a file is successfully sent.

OnFileSentAcknowledgment: fired when a fragment is sent and the receiver has processed.

OnFileSentError: fired when an error occurs sending a file.

OnFileSentFragment: fired when a fragment file is sent. Useful to show progress.

TsgcWSPClient_Files

This is the Server Files Protocol Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Methods

SendFile: sends a file to the server, you can set the following parameters

aSize: size of every packet in bytes.
aData: user custom data, here you can write any text you think is useful for the server.
aQoS: type of quality of service.
aFileId: if empty, will be set automatically.

Properties

Files: files properties

BufferSize: default size of every packet sent, in bytes.

SaveDirectory: the directory where all files will be stored.

QoS: quality of service

Interval: interval to check if a qosLevel2 message has been sent.

Level: level of quality of service.

qosLevel0: the message is sent.

qosLevel1: the message is sent and you get an acknowledgment if the message has been processed.

qosLevel2: the message is sent, you get an acknowledgment if the message has been processed and packets are requested by the receiver.

Timeout: maximum wait time.

ClearReceivedStreamsOnDisconnect: if disabled, when reconnects, try to resume file download for qosLevel2, by default is enabled.

ClearSentStreamsOnDisconnect: tif disabled, when reconnects, try to resume file upload for qosLevel2, by default is enabled.

Events

OnFileBeforeSent: fired before a file is sent. You can use this event to check file data before is sent.

OnFileReceived: fired when a file is successfully received.

OnFileReceivedAuthorization: fired to check if a file can be received.

OnFileReceivedError: fired when an error occurs receiving a file.

OnFileReceivedFragment: fired when a fragment file is received. Useful to show progress.

OnFileSent: fired when a file is successfully sent.

OnFileSentAcknowledgment: fired when a fragment is sent and the receiver has processed.

OnFileSentError: fired when an error occurs sending a file.

OnFileSentFragment: fired when a fragment file is sent. Useful to show progress.

TsgcWSMessageFile

This object is passed as a parameter every time a file protocol event is raised.

Properties

- BufferSize: default size of the packet.
- Channel: if specified, this file only will be sent to clients subscribed to specific channel.
- Method: internal method.
- FileId: identifier of a file, is unique for all files received/sent.
- Data: user custom data. Here the user can set whatever text.
- FileName: name of the file.
- FilePosition: file position in bytes.
- FileSize: Total file size in bytes.
- Id: identifier of a packet, is unique for every packet.
- QoS: quality of service of the message.
- Streaming: for internal use.
- Text: for internal use.

Presence

Protocol Presence

Presence protocol allows to know who is subscribed to a channel, this makes more easy to create chat applications and know who is online, example: game users, chat rooms, users viewing the same document...
Features

- By default user is **identified by a name**, but this can be **customized** passing more data: email, company, twitter...
- Events to **Authorize** if a **Channel** can be created, if a **member** is allowed...
- Every time a new **member joins** a channel, all members are **notified**.
- **Publish messages** to all channel subscribers.
- **Low memory** usage.

Components
TsgcWSPServer_Presence: Server Protocol Presence VCL Component.

TsgcWSPClient_Presence: Client Protocol Presence VCL Component.

Classes
TsgcWSPresenceMessage: the object which encapsulates presence packet information.

TsgcWSPServer_Presence

This is Server Presence Protocol Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

Methods
: All methods are handled internally by the server in response to client requests.

Properties
: You must link this component to a **Server** or to a **Broker** if you are using more than one protocol.

  Acknowledgment: if enabled, every time a server sends a message to client assign an ID to this message and queues in a list. When the client receives a message, if detect it has an ID, it sends an Acknowledgment to the server, which means the client has processed message and server can delete from the queue.

  - **Interval:** interval in seconds where server checks if there are messages not processed by client.
  - **Timeout:** maximum wait time before the server sends the message again.

Events
: There are several events to handle actions like: a new member request to join a channel, a new channel is created by a member, a member unsubscribes from a channel...

New Member

```
// When a new client connects to a server, first sends member data to
the server to request a new member. Following events can be called:

// OnBeforeNewMember:
// Server receives a request from the client to join and the server
accepts or not this member. Use Accept parameter to allow or not this
member.
// By default all members are accepted.

procedure OnBeforeNewMember(aConnection:  TsgcWSConnection; const
aMember: TsgcWSPresenceMember; var Accept: Boolean);
begin
  if aMember.Name = 'Spam' then
    Accept := False;
end;

// OnNewMember:
// After a new member is accepted, then this event is called and means
this member has join member list. You can use aMember.
// Data property to store objects in memory like database access,
session objects...

procedure OnNewMember(aConnection: TsgcWSConnection; const aMember:
TsgcWSPresenceMember);
begin

end;
```

Subscriptions

```
// When a client has joined as a member, can subscribe to new
channels, if a channel not exists, the following events can be called:

// OnBeforeNewChannel:
// Server receives a subscription request from the client to join this
channel but the channel doesn't exist, the server can accept or not
// to create this channel. Use Accept parameter to allow or not this
channel. By default, all channels are accepted.

procedure OnBeforeNewChannelBeforeNewChannel(Connection:
TsgcWSConnection; const aChannel: TsgcWSPresenceChannel;
  const aMember: TsgcWSPresenceMember; var Accept: Boolean)
begin
  if aChannel.Name = 'Spam' then
    Accept := False;
end;

// OnNewChannel: After a new channel is accepted, then this event is
called and means a new channel has been created.
// Channel properties can be customized in this event.

procedure OnNewChannel(Connection: TsgcWSConnection; var aChannel:
TsgcWSPresenceChannel);
begin

end;

// If the channel already exists or has been created, the server can
accept or no new subscriptions.

// OnBeforeNewChannelMembers:
// Server receives a subscription request from a client to join this
channel, the server can accept or not a member join.
// Use Accept parameter to allow or not this member. By default, all
members are accepted.

procedure OnBeforeNewChannelMember(Connection: TsgcWSConnection; const
aChannel: TsgcWSPresenceChannel; const aMember: TsgcWSPresenceMember;
  var Accept: Boolean)
begin
  if aMember.Name = 'John' then
    Accept := True
  else if aMember.Name = 'Spam' then
    Accept := False;
end;

// OnNewChannelMember:
// After a new member is accepted,  then this event is called and
means a new member has joined the channel.
// All subscribers to this channel, will be notified about new
members.

procedure OnNewChannelMember(Connection: TsgcWSConnection; const
aChannel: TsgcWSPresenceChannel; const aMember: TsgcWSPresenceMember);
begin
```

UnSubscriptions

```
// Every time a member unjoin a channel or disconnects, the server is
notified by following events:

// OnRemoveChannelMember:
// Server receives a subscription request from a client to join this
channel but the channel doesn't exist,
// the server can accept or not to create this channel. Use Accept
parameter to allow or not this channel. By default all channels are
accepted.

procedure OnRemoveChannelMember(Connection: TsgcWSConnection; const
aChannel: TsgcWSPresenceChannel; const aMember: TsgcWSPresenceMember);
begin
  Log('Member: ' + aMember.Name + ' unjoin channel: ' +
aChannel.Name);
end;

// When a member disconnects, automatically server is notified:

// OnRemoveMember: when the client disconnects from protocol, this
event is called and server is notified of which never has
disconnected.

procedure OnRemoveMember(aConnection: TsgcWSConnection; aMember:
TsgcWSPresenceMember);
begin
  Log('Member: ' + aMember.Name);
end;
```

Errors

```
// Every time there is an error, these events are called, example:
server has denied a member to subscribe to a channel, a member try to
subscribe to
// an already subscribed channel...

//OnErrorMemberChannel: this event is called every time there is an
error trying to create a new channel, join a new member, subscribe to
a channel...

procedure OnErrorMemberChannel(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aChannel: TsgcWSPresenceChannel;
  const aMember: TsgcWSPresenceMember);
begin
  Log('#Error: ' + aError.Text);
end;

// When a member disconnects, automatically server is notified:

// OnErrorPublishMsg: when a client publish a message and this is
denied by the server, this event is raised.

procedure OnErrorPublishMsg(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aMsg: TsgcWSPresenceMsg;
  const aChannel: TsgcWSPresenceChannel; const aMember:
TsgcWSPresenceMember);
begin
```

```
  Log('#Error: ' + aError.Text);
end;
```

TsgcWSPresenceMessage

This object encapsulates all internal messages exchange by server and client presence protocol.

TsgcWSPresenceMember

ID: internal identifier
Name: member name, provided by the client.
Info: member additional info, provided by the client.
Data: TObject which can be used for server purposes.

TsgcWSPresenceMemberList

Member[i]: member of a list by index
Count: number of members of the list

TsgcWSPresenceChannel

Name: channel name, provided by the client.

TsgcWSPresenceMsg

Text: text message, provided by the client when call Publish method

TsgcWSPresenceError

Code: integer value identifying the error
Text: error description.

TsgcWSPClient_Presence

This is Server Presence Protocol Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Properties
Presence: member data

- **Name:** member name.
- **Info:** any additional info related to member (example: email, twitter, company...)

Acknowledgment: if enabled, every time a client sends a message to server assign an ID to this message and queues in a list. When the server receives the message, if detect it has an ID, it sends an Acknowledgment to the client, which means the server has processed message and the client can delete from the queue.

- **Interval:** interval in seconds where the client checks if there are messages not processed by server.
- **Timeout:** maximum wait time before the client sends the message again.

Methods
There are several methods to subscribe to a channel, get a list of members...

Connect

```
// When a client connects, the first event called is OnSession, the
server sends a session ID to the client, which identifies this client
in the server connection list.
// After OnSession event is called, automatically client sends a
request to the server to join as a member, if successful, OnNewMember
event is raised

procedure OnNewMember(aConnection: TsgcWSConnection; const aMember:
TsgcWSPresenceMember);
begin

end;
```

Subscriptions

```
// When a client wants subscribe to a channel, use method "Subscribe"
and pass channel name as argument

Client.Subscribe('MyChannel');
```

```
// If the client is successfully subscribed, OnNewChannelMember event
is called. All members of this channel will be notified using the same
event.

procedure OnNewChannelMember(Connection: TsgcWSConnection; const
aChannel: TsgcWSPresenceChannel; const aMember: TsgcWSPresenceMember);
begin
  Log('Subscribed: ' + aChannel.Name);
end;

// if server denies access to a member, OnErrorMemberChannel event is
raised.

procedure OnErrorMemberChannel(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aChannel: TsgcWSPresenceChannel;
  const aMember: TsgcWSPresenceMember)
begin
  Log('Error: ' + aError.Text);
end;
```

UnSubscriptions

```
// When a client unsubscribe from a channel, use method "Unsubscribe"
and pass channel name as argument

Client.Unsubscribe('MyChannel');

// If a client is successfully unsubscribed, OnRemoveChannelMember
event is called. All members of this channel will be notified using
the same event.
// All members of this channel will be notified using the same event.

procedure OnNewChannelMember(Connection: TsgcWSConnection; const
aChannel: TsgcWSPresenceChannel; const aMember: TsgcWSPresenceMember);
begin
  Log('Unsubscribed: ' + aChannel.Name);
end;

// if a client can't unsubscribe from a channel, example: because is
not subscribed, OnErrorMemberChannel event is raised.

procedure OnErrorMemberChannel(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aChannel: TsgcWSPresenceChannel;
  const aMember: TsgcWSPresenceMember)
begin
  Log('Error: ' + aError.Text);
end;

// When a client disconnects from the server, OnRemoveEvent is called.

procedure OnRemoveMember(aConnection: TsgcWSConnection; aMember:
TsgcWSPresenceMember);
begin
  Log('#RemoveMember: ' + aMember.Name);
end;
```

Publish

```
// When a client wants to send a message to all members or all
subscribers of a channel, use "Publish" method

Client.Publish('Hello All Members');

Client.Publish('Hello All Members of this channel', 'MyChannel');

// If a message is successfully published, OnPublishMsg event is
called. All members of this channel will be notified using the same
event.

procedure OnPublishMsg(Connection: TsgcWSConnection; const aMsg:
TsgcWSPresenceMsg; const aChannel: TsgcWSPresenceChannel;
  const aMember: TsgcWSPresenceMember);
begin
  Log('#PublishMsg: ' + aMsg.Text + ' ' + aMember.Name);
end;

// if a message can't be published, OnErrorPublishMsg event is raised.

procedure OnErrorPublishMsg(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aMsg: TsgcWSPresenceMsg;
  const aChannel: TsgcWSPresenceChannel; const aMember:
TsgcWSPresenceMember);
begin
  Log('#Error: ' + aError.Text);
end;
```

GetMembers

```
// A client can request to the server a list of all members or all
members subscribed to a channel. Use "GetMembers" method

Client.GetMembers;

Client.GetMembers('MyChannel');

// If a message is successfully processed by the server, OnGetMembers
event is called

procedure OnGetMembers(Connection: TsgcWSConnection; const aMembers:
TsgcWSPresenceMemberList; const aChannel: TsgcWSPresenceChannel);
var
  i: Integer;
begin
  for i := 0 to aMembers.Count - 1 do
    Log('#GetMembers: ' + aMembers.Member[i].ID + ' ' +
aMembers.Member[i].Name);
end;

// If there is an error because the member is not allowed or is not
subscribed to channel, OnErrorMemberChannel event is raised

procedure OnErrorMemberChannel(Connection: TsgcWSConnection; const
aError: TsgcWSPresenceError; const aChannel: TsgcWSPresenceChannel;
```

```
  const aMember: TsgcWSPresenceMember);
begin
  Log('Error: ' + aError.Text);
end;
```

Invite

```
// A client can invite to other member to subscribe to a channel.

Client.Invite('MyChannel', 'E54541D0F0E5R40F1E00FEEA');

// When the other member receives the invitation, OnChannelInvitation
event is called and member can Accept or not the invitation.

procedure OnChannelInvitation(Connection: TsgcWSConnection; const
aMember: TsgcWSPresenceMember; const aChannel: TsgcWSPresenceChannel;
  var Accept: Boolean);
begin
  if aChannel = 'MyChannel' then
    Accept := True
  else
    Accept := False;
end;
```

Protocol Presence Javascript

Presence Protocol Javascript sgcWebSockets uses **sgcWebSocket.js and presence.esegece.com.js** files.

Here you can find available methods, you must replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
<script
src="http://www.example.com:80/presence.esegece.com.js"></script>
```

Open Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
</script>
```

New Member after connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.on('sgcsession', function(event)
  {
    socket.newmember(event.id, 'John', 'Additional Info');
  });
</script>
```

Subscribe to Topic 1 channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.subscribe('Topic 1');
</script>
```

Unsubscribe from Topic 1 channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.unsubscribe('Topic 1');
```

```
</script>
```

Publish Message to Topic 1 channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.publish('Hello sgcWebSockets!', 'Topic 1');
</script>
```

Receive Message

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.on('sgcpublishmsg', function(event)
  {
    console.log('#publishmsg: ' + event.message.text);
  });
</script>
```

Get All Members Connected

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.on('sgcgetmembers', function(event)
  {
    for (var i  in event.members) {
     console.log(event.members[i].id + ' ' + event.members[i].name);
    }
  });
  socket.getmembers();
</script>
```

Show Alert when Members subscribe/unsubscribe

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.on('sgcnewmember', function(event)
  {
    alert('#new member: ' + event.member.name);
  }
  );
  socket.on('sgcremovemember', function(event)
  {
    alert('#removed member: ' + event.member.name);
  }
```

```
  );
  socket.on('sgcnewchannelmember', function(event)
  {
    alert('#new member: ' + event.member.name + ' in channel: ' +
event.channel.name);
  }
  );
  socket.on('sgcremovechannelmember', function(event)
  {
    alert('#remove member: ' + event.member.name + ' from channel: ' +
event.channel.name);
  }
  );
</script>
```

Show Alert OnConnect, OnDisconnect and OnError Events

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  var socket = new sgcws_presence('ws://{%host%}:{%port%}');
  socket.on('open', function(event)
  {
    alert('sgcWebSocket Open!');
  };
  socket.on('close', function(event)
  {
    alert('sgcWebSocket Closed!');
  };
  socket.on('sgcerrormemberchannel', function(event)
  {
    alert('#error member channel: ' + event.error.text);
  }
  );
  socket.on('sgcerrorpublishmsg', function(event)
  {
    alert('#error publish: ' + event.error.text);
  }
  );
</script>
```

Close Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script
src="http://{%host%}:{%port%}/presence.esegece.com.js"></script>
<script>
  socket.close();
</script>
```

MQTT

Protocol MQTT

MQTT is a Client-Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and the Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.

The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include:

· Use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications.

· A messaging transport that is agnostic to the content of the payload.

· Three qualities of service for message delivery:
  · "At most once", where messages are delivered according to the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after.
  · "At least once", where messages are assured to arrive but duplicates can occur.
  · "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied.

· A small transport overhead and protocol exchanges minimized to reduce network traffic.

· A mechanism to notify interested parties when an abnormal disconnection occurs.

Features

- Supports **3.1.1** and **5.0** MQTT versions.
- **Publish/subscribe** message pattern to provide one-to-many message distribution and decoupling of applications.
- **Acknowledgment** of messages sent.
- Implements **QoS** (Quality of Service) for message delivery (all levels: At most once, At least once and Exactly once)
- **Last Will Testament**.
- **Secure** connections.
- **HeartBeat** and **Watchdog**.
- **Authentication** to server.

Components
TsgcWSPClient_MQTT: MQTT Client Component.

Most common uses

- **Connection**
  - Client MQTT Connect
  - Connect Mosquitto MQTT Servers
  - Client MQTT Sessions
  - Client MQTT Version

- **Publish & Subscribe**
  - MQTT Publish Subscribe
  - MQTT Topics
  - MQTT Subscribe
  - MQTT Publish Message
  - MQTT Receive Messages

- **Other**
  - MQTT Clear Retained Messages

TsgcWSPClient_MQTT

The MQTT component provides a lightweight, fully-featured MQTT client implementation with support for versions 3.1.1 and 5.0. The component supports plaintext and secure connections over both standard TCP and WebSockets.

Connection to a MQTT server is simple, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property. Set host and port in TsgcWebSocketClient and set Active := True to connect.

MQTT v5.0 is not backward compatible (like v3.1.1). Obviously too many new things are introduced so existing implementations have to be revisited.

According to the specification, MQTT v5.0 adds a significant number of new features to MQTT while keeping much of the core in place.

- The Clean Session flag functionality is divided into 2 properties to allow for finer control over session state data: the CleanStart parameter and the new SessionExpInterval.
- Server disconnect: Allow DISCONNECT to be sent by the Server to indicate the reason the connection is closed.
- All response packets (CONNACK, PUBACK, PUBREC, PUBREL, PUBCOMP, SUBACK, UNSUBACK, DISCONNECT) now contain a reason code and reason string describing why operations succeeded or failed.
- Enhanced authentication: Provide a mechanism to enable challenge/response style authentication including mutual authentication. This allows SASL style authentication to be used if supported by both Client and Server, and includes the ability for a Client to re-authenticate within a connection.
- The Request / Response pattern is formalized by the addition of the ResponseTopic.
- Shared Subscriptions: Add shared subscription support allowing for load balanced consumers of a subscription.
- Topic Aliases can be sent by both client and server to refer to topic filters by shorter numerical identifiers in order to save bandwidth.
- Servers can communicate what features it supports in ConnectionProperties.
- Server reference: Allow the Server to specify an alternate Server to use on CONNACK or DISCONNECT. This can be used as a redirect or to do provisioning.
- More: message expiration, Receive Maximums and Maximum Packet Sizes, and a Will Delay interval are all supported.

Methods

Connect: this method is called automatically after a successful WebSocket connection.

Ping: Sends a ping to the server, usually to keep the connection alive. If you enable HeartBeat property, ping will be sent automatically by a defined interval.

Subscribe: subscribe client to a custom channel. If the client is subscribed, OnMQTTSubscribe event will be fired.

SubscribeProperties: (New in MQTT 5.0)

- **SubscriptionIdentifier:** MQTT 5 allows clients to specify a numeric subscription identifier which will be returned with messages delivered for that subscription. To verify that a server supports subscription identifiers, check the "SubscriptionIdentifiersAvailable"
- **UserProperties:** This property is intended to provide a means of transferring application layer name-value tags whose meaning and interpretation are known only by the application programs responsible for sending and receiving them.

Example:

```
Delphi
oProperties := TsgcWSMQTTSubscribe_Properties.Create;
Try
  oProperties.SubscriptionIdentifier := 16385;
  MQTT.Subscribe('myChannel', mtqsAtMostOnce, oProperties);
Finally
  FreeAndNil(oProperties);
End;
```

Unsubscribe: unsubscribe client to a custom channel. If the client is unsubscribed, OnMQTTUnsubscribe event will be fired.

UnsubscribeProperties: (New in MQTT 5.0)

- **UserProperties:** This property is intended to provide a means of transferring application layer name-value tags whose meaning and interpretation are known only by the application programs responsible for sending and receiving them.

Example:

```
Delphi
oProperties := TsgcWSMQTTUnsubscribe_Properties.Create;
Try
  oProperties.UserProperties.Add('Temp=21');
  oProperties.UserProperties.Add('Humidity=55');
  MQTT.UnSubscribe('myChannel', mtqsAtMostOnce, oProperties);
Finally
  FreeAndNil(oProperties);
End;
```

Publish: sends a message to all subscribed clients. There are the following parameters:

Topic: is the channel where the message will be published.

Text: is the text of the message.

QoS: is the Quality Of Service of published message. There are 3 possibilities:

mtqsAtMostOnce: (by default) the message is delivered according to the best efforts of the underlying TCP/IP network. A response is not expected and no retry semantics are defined in the protocol. The message arrives at the server either once or not at all.

mtqsAtLeastOnce: the receipt of a message by the server is acknowledged by an ACKNOWLEDGMENT message. If there is an identified failure of either the communications link or the sending device or the acknowledgement message is not received after a specified period of time, the sender resends the message. The message arrives at the server at least once. A message with QoS level 1 has an ID param in the message.

mtqsExactlyOnce: where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied. If there is an identified failure of either the communications link or the sending device, or the acknowledgement message is not received after a specified period of time, the sender resends the message.

Retain: if True, Server MUST store the Application Message and its QoS, so that it can be delivered to future subscribers whose subscriptions match its topic name. By default is False.

PublishProperties: (New in MQTT 5.0)

- **PayloadFormat:** select payload format from: mqpfUnspecified (which is equivalent to not sending a Payload Format Indicator) or mqpfUTF8 (Message s UTF-8 Encoded Character Data).
- **MessageExpiryInterval:** Length of time after which the server must stop delivery of the publish message to a subscriber if not yet processed.
- **TopicAlias:** is an integer value that is used to identify the Topic instead of using the Topic Name. This reduces the size of the PUBLISH packet, and is useful when the Topic Names are long and the same Topic Names are used repetitively within a Network Connection.
- **ResponseTopic:** is used as the Topic Name for a response message.
- **CorrelationData:** The Correlation Data is used by the sender of the Request Message to identify which request the Response Message is for when it is received.
- **UserProperties:** This property is intended to provide a means of transferring application layer name-value tags whose meaning and interpretation are known only by the application programs responsible for sending and receiving them.
- **SubscriptionIdentifier:** A numeric subscription identifier included in SUBSCRIBE packet which will be returned with messages delivered for that subscription.
- **ContentType:** String describing content of message to be sent to all subscribers receiving the message.

Disconnect: disconnects from MQTT server.

ReasonCode: code identifies reason why disconnects.(New in MQTT 5.0)

DisconnectProperties (New in MQTT 5.0)

- **SessionExpiryInterval:** Session Expiry Interval in seconds.
- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.
- **ServerReference:** can be used by the Client to identify another Server to use.

Auth: is sent from Client to Server or Server to Client as part of an extended authentication exchange, such as challenge / response authentication. (New in MQTT 5.0)

ReAuthenticate: if True Initiate a re-authentication, otherwise continue the authentication with another step.

AuthProperties

- **AuthenticationMethod:** contains the name of the authentication method.
- **AuthenticationData:** contains authentication data.
- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.

Events

OnMQTTBeforeConnect: this event is fired before a new connection is established. There are 2 parameters:

CleanSession: if True (by default), the server must discard any previous session and start a new session. If false, the server must resume communication.

ClientIdentifier: every new connection needs a client identifier, this is set automatically by component, but can be modified if needed.

OnMQTTConnect: this event is fired when the client is connected to MQTT server. There are 2 parameters:

Session:

1. If client sends a connection with CleanSession = True, then Server Must respond with Session = False.
2. If client sends a connection with CleanSession = False:

- If the Server has stored Session state, Session = True.
- If the Server does not have stored Session state, Session = False

ReasonCode: returns code with the result of connection.(New in MQTT 5.0)
ReasonName: text description of ReturnCode.(New in MQTT 5.0)
ConnectProperties: (New in MQTT 5.0)

- **SessionExpiryInterval:** Session Expiry Interval in seconds.
- **ReceiveMaximum:** number of QoS 1 and QoS 2 publish messages, the server will process concurrently for the client.
- **MaximumQoS:** maximum accepted QoS of PUBLISH messages to be received by the server.
- **RetainAvailable:** indicates whether the client may send PUBLISH packets with Retain set to True.
- **MaximumPacketSize:** maximum packet size in bytes the server is willing to accept.
- **AssignedClientIdentifier:** the Client Identifier which was assigned by the Server when client didn't send any.
- **TopicAliasMaximum:** indicates the hishest value that the server will accept as a Topic Alias sent by the client.
- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.
- **WildcardSubscriptionAvailable:** indicates whether the server supports wildcard subscriptions.
- **SubscriptionIdentifiersAvailable:** indicates whether the server supports subscription identifiers.
- **SharedSubscriptionAvailable:** indicates whether the server supports shared subscriptions.
- **ResponseInformation:** used as the basis for creating a Response Topic.
- **ServerReference:** can be used by the Client to identify another Server to use.
- **AuthenticationMethod:** identifier of the Authentication Method.
- **AuthenticationData:** string containing authentication data.

OnQTTDisconnect: this event is fired when the client is disconnected from MQTT server. Parameters:

ReasonCode: returns code with the result of connection.(New in MQTT 5.0)
ReasonName: text description of ReturnCode.(New in MQTT 5.0)
DisconnectProperties: (New in MQTT 5.0)

- **SessionExpiryInterval:** Session Expiry Interval in seconds.
- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.
- **ServerReference:** can be used by the Client to identify another Server to use.

OnMQTTPing: this event is fired when the client receives an acknowledgment from a ping previously sent.

OnMQTTPubAck: this event is fired when receives the response to a Publish Packet with QoS level 1. There is one parameter:

PacketIdentifier: is packet identifier sent initially.
ReasonCode: returns code with the result of connection.(New in MQTT 5.0)
ReasonName: text description of ReturnCode.(New in MQTT 5.0)
PubAckProperties: (New in MQTT 5.0)

- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.

OnMQTTPubComp: this event is fired when receives the response to a PubRel Packet. It is the fourth and final packet of the QoS 2 protocol exchange. There are the following parameters:
PacketIdentifier: is packet identifier sent initially.
ReasonCode: returns code with the result of connection.(New in MQTT 5.0)
ReasonName: text description of ReturnCode.(New in MQTT 5.0)
PubCompProperties: (New in MQTT 5.0)

- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
- **UserProperties:** provide additional information to the Client including diagnostic information.

OnMQTTPublish: this event is fired when the client receives a message from the server. There are 2 parameters:
Topic: is the topic name of the published message.
Text: is the text of the published message.
PublishProperties: (New in MQTT 5.0)

- **PayloadFormat:** select payload format from: mqpfUnspecified (which is equivalent to not sending a Payload Format Indicator) or mqpfUTF8 (Message s UTF-8 Encoded Character Data).
- **MessageExpiryInterval:** Length of time after which the server must stop delivery of the publish message to a subscriber if not yet processed.
- **TopicAlias:** is an integer value that is used to identify the Topic instead of using the Topic Name. This reduces the size of the PUBLISH packet, and is useful when the Topic Names are long and the same Topic Names are used repetitively within a Network Connection.
- **ResponseTopic:** is used as the Topic Name for a response message.
- **CorrelationData:** The Correlation Data is used by the sender of the Request Message to identify which request the Response Message is for when it is received.
- **UserProperties:** This property is intended to provide a means of transferring application layer name-value tags whose meaning and interpretation are known only by the application programs responsible for sending and receiving them.
- **SubscriptionIdentifier:** A numeric subscription identifier included in SUBSCRIBE packet which will be returned with messages delivered for that subscription.
- **ContentType:** String describing content of message to be sent to all subscribers receiving the message.

OnMQTTPubRec: this event is fired when receives the response to a Publish Packet with QoS 2. It is the second packet of the QoS 2 protocol exchange. There are the following parameters:
PacketIdentifier: is packet identifier sent initially.
ReasonCode: returns code with the result of connection.(New in MQTT 5.0)
ReasonName: text description of ReturnCode.(New in MQTT 5.0)
PubRecProperties: (New in MQTT 5.0)

- **ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.

•**UserProperties:** provide additional information to the Client including diagnostic information.

OnMQTTSubscribe: this event is fired as a response to subscribe method. There are the following parameters:

PacketIdentifier: is packet identifier sent initially.
Codes: codes with the result of a subscription.
SubscribeProperties: (New in MQTT 5.0)

•**ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
•**UserProperties:** provide additional information to the Client about subscription.

OnMQTTUnSubscribe: this event is fired as a response to subscribe method. There are the following parameters:

PacketIdentifier: is packet identifier sent initially.
Codes: codes with the result of a subscription.
UnsubscribeProperties: (New in MQTT 5.0)

•**UserProperties:** provide additional information to the Client about subscription.

OnMQTTAuth: this event is fired as a response to Äuth method. There is one parameter: (New in MQTT 5.0)

ReasonCode: returns code with the result of connection.
ReasonName: text description of ReturnCode.
AuthProperties:

•**AuthenticationMethod:** contains the name of the authentication method used for extended authentication.
•**AuthenticationData:** data associated to authentication.
•**ReasonString:** represents the reason associated with this response. This Reason String is a human readable string designed for diagnostic.
•**UserProperties:** provide additional information to the Client including diagnostic information.

Enhanced Authentication (New in MQTT 5.0)

To begin an enhanced authentication, the Client includes an Authentication Method in the ConnectProperties. This specifies the authentication method to use. If the Server does not support the Authentication Method supplied by the Client, it may send a Reason Code "Bad authentication method" or Not Authorized.

Example:

- Client to Server: CONNECT Authentication Method="SCRAM-SHA-1" Authentication Data=client-first-data
- Server to Client: AUTH ReasonCode="Continue authentication" Authentication Method="SCRAM-SHA-1" Authentication Data=server-first-data
- Client to Server AUTH ReasonCode="Continue authentication" Authentication Method="SCRAM-SHA-1" Authentication Data=client-final-data
- Server to Client CONNACK ReasonCode=0 Authentication Method="SCRAM-SHA-1" Authentication Data=server-final-data

Properties
MQTTVersion: select which MQTT version (3.1.1 or 5.0) will use to connect to server.

Authentication: disabled by default, if True a UserName and Password are sent to the server to try user authentication.

HeartBeat: enabled by default, if True, send a ping every X seconds (set by Interval property) to keep alive connection.

LastWillTestament: if there is a disconnection and is enabled, a message is sent to all connected clients to inform that connection has been closed.

- **Enabled:** enable if you want activate last will testament.
- **Text:** is the message that the server will publish in the event of an ungraceful disconnection.
- **Topic:** is the topic that the server will publish the message to in the event of an ungraceful disconnection. **Is mandatory if LastWillTestament is enabled.**
- **Retain:** enable if server must retain message after publish it.
- **WillProperties:** (New in MQTT 5.0)
    - **WillDelayInterval:** The Server delays publishing the Client's Will Message until the Will Delay Interval has passed or the Session ends, whichever happens firs
    - **PayloadFormat:** select payload format from: mqpfUnspecified (which is equivalent to not sending a Payload Format Indicator) or mqpfUTF8 (Message s UTF-8 Encoded Character Data).
    - **MessageExpiryInterval:** Length of time after which the server must stop delivery of the will message to a subscriber if not yet processed.
    - **ContentType:** string describing content of will message.
    - **ResponseTopic:** Used as a topic name for a response message.
    - **CorrelationData:** binary string used by client to identify which request the response message is for when received.
    - **UserProperties:** can be used to send will related properties from the Client to the Server. The meaning of these properties is not defined by MQTT specification.

ConnectProperties: (New in MQTT 5.0) are connection properties sent with packet connect.

- **Enabled:** if True, connect properties will be sent to server.
- **SessionExpiryInterval:** if value is zero, session will end when network connection is closed.
- **ReceiveMaximum:** the Client uses this value to limit the number of QoS 1 and QoS 2 publications that it is willing to process concurrently.
- **MaximumPacketSize:** the Client uses the Maximum Packet Size to inform the Server that it will not process packets exceeding this limit.
- **TopicAliasMaximum:** the Client uses this value to limit the number of Topic Aliases that it is willing to hold on this Connection.
- **RequestResponseInformation:** the Client uses this value to request the Server to return Response Information in the CONNACK. If False indicates that the Server MUST NOT return Response Information, If True the Server MAY return Response Information in the CONNACK packet.
- **RequestProblemInformation:** the Client uses this value to indicate whether the Reason String or User Properties are sent in the case of failures. If the value of Request Problem Information is False, the Server MAY return a Reason String or User Properties on a CONNACK or DISCONNECT packet but MUST NOT send a Reason String or User Properties on any packet other than PUBLISH, CONNACK, or DISCONNECT.
- **UserProperties:** can be used to send connection related properties from the Client to the Server. The meaning of these properties is not defined by MQTT specification.

- **AuthenticationMethod:** containins the name of the authentication method used for extended authentication.

Connection

TsgcWSPClient_MQTT | Client MQTT Connect

In order to connect to a MQTT Client, you must create first a TsgcWebSocketClient and a TsgcWSPClient_MQTT. Then you must attach MQTT Component to WebSocket Client.

Basic Usage
Connect to Mosquitto MQTT server using websocket protocol. Subscribe to topic: "topic1" after connect.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8080;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const ReasonCode: Integer; const ReasonName: string; const
ConnectProperties: TsgcWSMQTTCONNACKProperties);
begin
  oMQTT.Subscribe('topic1');
end;
```

Client Identifier
MQTT requires a **Client Identifier** to identify client connection. Component sets a **random value** automatically but you can set your own Client Identifier if required, to do this, just handle **OnBeforeConnect** event and set your value on aClientIdentifier parameter.

```
procedure OnMQTTBeforeConnect(Connection: TsgcWSConnection; var
aCleanSession: Boolean; var aClientIdentifier: string);
begin
  aClientIdentifier := 'your client id';
end;
```

Authentication
Somes servers require an user and password to a**uthorize MQTT connections**. Use **Authentication** property to set the value for username and password before connect to server.

```
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Authentication.Enabled := True;
oMQTT.Authentication.UserName := 'your user';
oMQTT.Authentication.Password := 'your password';
```

TsgcWSPClient_MQTT | Connect MQTT Mosquitto

Use the following sample configurations to connect to a Mosquitto MQTT Server.
MOSQUITTO MQTT WebSockets

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8080;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;
```

MOSQUITTO MQTT WebSockets TLS

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8081;
oClient.TLS := True;
oClient.TLSOptions.Version := tls1_2;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;
```

MOSQUITTO MQTT Plain TCP

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 1883;
oClient.Specifications.RFC6455 := False;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;
```

MOSQUITTO MQTT Plain TCP TLS

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8083;
oClient.Specifications.RFC6455 := False;
oClient.TLS := True;
oClient.TLSOptions.Version := tls1_2;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;
```

TsgcWSPClient_MQTT | Client MQTT Sessions

Clean Start
OnMQTTBeforeConnect event, there is a parameter called **aCleanSession**. If the value of this parameter is **True**, means that client **want start a new session**, so if server has any session stored, it must discard it. So, when OnMQTTConnect event is fired, aSession parameter will be false. If the value of this parameter is **False** and there is a session associated to this client identifier, the server must resume communications with the client on state with the existing session.

So, if client has an **unexpected disconnection**, and you want to **recover the session** where was disconnected, in OnMQTTBeforeConnect set **aCleanSession = True** and **aClientIdentifier = Client ID of Session**.

Session
Once successful connection, check **OnMQTTConnect** event, the value of Session parameter.

Session = true, means session has been resumed.
Session = false, means it's a new session.

```
procedure TfrmWebSocketClient.MQTTMQTTBeforeConnect(Connection:
TsgcWSConnection; var aCleanSession: Boolean; var aClientIdentifier:
string);
begin
  aCleanSession := false;
  aClientIdentifier := 'previous client id';
end;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const ReasonCode: Integer; const ReasonName: string; const
ConnectProperties: TsgcWSMQTTCONNACKProperties);
begin
  if Session then
    WriteLn('Session resumed')
  else
    WriteLn('New Session');
end;
```

TsgcWSPClient_MQTT | Client MQTT Version

Currently, MQTT Client supports the following specifications:

- **MQTT 3.1.1:** http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html
- **MQTT 5.0:** https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

You can select which is the version which will use the MQTT Client component using MQTTVersion property.

MQTT 3.1.1: TsgcWSPClient_MQTT.Version = mqtt311
MQTT 5.0: sgcWSPClient_MQTT.Version = mqtt5

PubSub

TsgcWSPClient_MQTT | MQTT Publish Subscribe

The publish/subscribe pattern (also known as pub/sub) provides an alternative to traditional client-server architecture. In the client-sever model, a client communicates directly with an endpoint.The pub/sub model **decouples the client that sends a message (the publisher) from the client or clients that receive the messages (the subscribers)**. The publishers and subscribers never contact each other directly. In fact, they are not even aware that the other exists. **The connection between them is handled by a third component (the broker)**. The job of the broker is to filter all incoming messages and distribute them correctly to subscribers.

With **TsgcWSPClient_MQTT** you can **Publish messages** and **Subscribe to Topics**.

Subscribe Topic
Subscribe to Topic "topic1" after a successful connection.

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8080;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const ReasonCode: Integer; const ReasonName: string; const
ConnectProperties: TsgcWSMQTTCONNACKProperties);
begin
  oMQTT.Subscribe('topic1');
end;
```

Publish Message
Publish a message to all subscribers of "topic1"

```
oClient := TsgcWebSocketClient.Create(nil);
oClient.Host := 'test.mosquitto.org';
oClient.Port := 8080;
oMQTT := TsgcWSPClient_MQTT.Create(nil);
oMQTT.Client := oClient;
oClient.Active := True;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const ReasonCode: Integer; const ReasonName: string; const
ConnectProperties: TsgcWSMQTTCONNACKProperties);
begin
  oMQTT.Publish('topic1', 'Hello Subscribers topic1');
end;
```

TsgcWSPClient_MQTT | MQTT Topics

Topics
In MQTT, the word topic refers to an UTF-8 string that the broker uses to filter messages for each connected client. The topic consists of one or more topic levels. Each topic level is separated by a forward slash (topic level separator)

myHome / groundfloor / livingroom / temperature

In comparison to a message queue, MQTT topics are very lightweight. The client does not need to create the desired topic before they publish or subscribe to it. The broker accepts each valid topic without any prior initialization. Note that each topic must contain at least 1 character and that the topic string permits empty spaces. Topics are case-sensitive.

WildCards
When a client subscribes to a topic, it can subscribe to the exact topic of a published message or it can use wildcards to subscribe to multiple topics simultaneously. A wildcard can only be used to subscribe to topics, not to publish a message. There are two different kinds of wildcards: _single-level and _multi-level.

Single Level: +
As the name suggests, a single-level wildcard replaces one topic level. The plus symbol represents a single-level wildcard in a topic.

myHome / groundfloor / + / temperature

Any topic matches a topic with single-level wildcard if it contains an arbitrary string instead of the wildcard. For example a subscription to _myhome/groundfloor/+/temperature can produce the following results:

YES => myHome / groundfloor / livingroom / temperature
YES => myHome / groundfloor / kitchen / temperature
NO => myHome / groundfloor / livingroom / brightness
NO => myHome / firstfloor / livingroom / temperature
NO => myHome / groundfloor / kitchen / fridge / temperature

Multi Level: #
The multi-level wildcard covers many topic levels. The hash symbol represents the multi-level wild card in the topic. For the broker to determine which topics match, the multi-level wildcard must be placed as the last character in the topic and preceded by a forward slash.

myHome / groundfloor / #

YES => myHome / groundfloor / livingroom / temperature
YES => myHome / groundfloor / kitchen / temperature
YES => myHome / groundfloor / kitchen / brightness
NO => myHome / firstfloor / kitchen / temperature

When a client subscribes to a topic with a multi-level wildcard, it receives all messages of a topic that begins with the pattern before the wildcard character, no matter how long or deep the topic is. If you specify only the multi-level wildcard as a topic (_#), you receive all messages that are sent to the MQTT broker.

TsgcWSPClient_MQTT | MQTT Subscribe

You can Subscribe to a Topic using method Subscribe from TsgcWSPClient_MQTT. This method has the following parameters:

Topic: is the name of the topic to be subscribed.
QoS: one of the 3 QoS levels (not all brokers support all 3 levels). If not specificed uses mtqsAtMostOnce. Read more about QoS Levels.
SubscribeProperties: if MQTT 5.0, are additional properties about subscriptions.

Subscribe QoS = At Least Once

```
MQTT.Subscribe('topic1', mtqsAtLeastOnce);
```

Subscribe MQTT 5.0

```
oProperties := TsgcWSMQTTSubscribe_Properties.Create;
oProperties.SubscriptionIdentifier := 1234;
oProperties.UserProperties.Add('name=value');

MQTT.Subscribe('topic1', mtqsAtMostOnce, oProperties);
```

TsgcWSPClient_MQTT | MQTT Publish Message

You can publish messages to all subscribers of a Topic using **Publish** method, which has the following parameters:

Topic: is the name of the topic where the message will be published.
Text: is the text of the message.
QoS: one of the 3 QoS levels (not all brokers support all 3 levels). If not specificed uses mtqsAtMostOnce. Read more about QoS Levels.
Retain: if true, this message will be retained. And every time a new client subscribes to this topic, this message will be sent to this client.
PublishProperties: if MQTT 5.0, these are the properties of the message.

Publish a simple message

```
MQTT.Publish('topic1', 'Hello Subscribers topic1');
```

Publish QoS = At Least Once

```
MQTT.Publish('topic1', 'Hello Subscribers topic1', mtqsAtLeastOnce);
```

Publish Retained message

```
MQTT.Publish('topic1', 'Hello Subscribers topic1', mtqsAtMostOnce,
true);
```

TsgcWSPClient_MQTT | MQTT Receive Messages

Messages sent by server, are received **OnMQTTPublish** event. This event has the following parameters:

Topic: is the name of the topic associated to this message.
Text: is the text of the message.
PublishProperties: if MQTT 5.0, these are the properties of the published message.

Read published Messages

```
procedure OnMQTTPublish(Connection: TsgcWSConnection; aTopic, aText:
string; PublishProperties: TsgcWSMQTTPublishProperties);
begin
  WriteLn('Topic: ' + aTopic + '. Message: ' + aText);
end;
```

Other

TsgcWSPClient_MQTT | MQTT Clear Retained Messages

By default, every MQTT topic can have a retained message. The standard MQTT mechanism to clean up retained messages is sending a retained message with an empty payload to a topic. This will remove the retained message.

```
MQTT.Publish('topic1', '', mtqsAtMostOnce, true);
```

STOMP

Protocol STOMP

STOMP is the Simple (or Streaming) Text Orientated Messaging Protocol. STOMP provides an interoperable wire format so that STOMP clients can communicate with any STOMP message broker to provide easy and widespread messaging interoperability among many languages, platforms and brokers.

Our STOMP client components support following STOMP versions: 1.0, 1.1 and 1.2.

Components

TsgcWSPClient_STOMP: generic STOMP Protocol client, allows to connect to any STOMP Server.

TsgcWSPClient_STOMP_RabbitMQ: STOMP client for RabbitMQ Broker.

TsgcWSPClient_STOMP_ActiveMQ: STOMP client for ActiveMQ Broker.

TsgcWSPClient_STOMP

This is Client Protocol STOMP Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Methods

Send: The SEND frame sends a message to a destination in the messaging system.

Subscribe: The SUBSCRIBE frame is used to register to listen to a given destination.

UnSubscribe: The UNSUBSCRIBE frame is used to remove an existing subscription.

ACK: ACK is used to acknowledge the consumption of a message from a subscription.

NACK: NACK is the opposite of ACK. It is used to tell the server that the client did not consume the message.

BeginTransaction: is used to start a transaction. Transactions in this case apply to sending and acknowledging - any messages sent or acknowledged during a transaction will be processed atomically based on the transaction.

CommitTransaction: is used to commit a transaction in progress.

AbortTransaction: is used to roll back a transaction in progress.

Disconnect: use to graceful shutdown connection, where the client is assured that all previous frames have been received by the server.

Events

OnSTOMPConnected: this event is fired after a new connection is established.

version : The version of the STOMP protocol the session will be using. See Protocol Negotiation for more details.

STOMP 1.2 servers MAY set the following headers:

heart-beat : The Heart-beating settings.

session : A session identifier that uniquely identifies the session.

server : A field that contains information about the STOMP server. The field MUST contain a server-name field and MAY be followed by optional comment fields delimited by a space character.

OnSTOMPMessage: this event is fired when the client receives a message.

The MESSAGE frame MUST include a destination header indicating the destination the message was sent to. If the message has been sent using STOMP, this destination header SHOULD be identical to the one used in the corresponding SEND frame.

The MESSAGE frame MUST also contain a message-id header with a unique identifier for that message and a subscription header matching the identifier of the subscription that is receiving the message.

If the message is received from a subscription that requires explicit acknowledgment (either client or client-individual mode) then the MESSAGE frame MUST also contain an ack header with an arbitrary value. This header will be used to relate the message to a subsequent ACK or NACK frame.

MESSAGE frames SHOULD include a content-length header and a content-type header if a body is present.

MESSAGE frames will also include all user-defined headers that were present when the message was sent to the destination in addition to the server-specific headers that MAY get added to the frame.

OnSTOMPReceipt: this event is fired once a server has successfully processed a client frame that requests a receipt.

A RECEIPT frame is an acknowledgment that the corresponding client frame has been processed by the server. Since STOMP is stream based, the receipt is also a cumulative acknowledgment that all the previous frames have been received by the server. However, these previous frames may not yet be fully processed. If the client disconnects, previously received frames SHOULD continue to get processed by the server.

OnSTOMPError: this event is fired if something goes wrong.
The ERROR frame SHOULD contain a message header with a short description of the error, and the body MAY contain more detailed information (or MAY be empty).
If the error is related to a specific frame sent from the client, the server SHOULD add additional headers to help identify the original frame that caused the error. For example, if the frame included a receipt header, the ERROR frame SHOULD set the receipt-id header to match the value of the receipt header of the frame which the error is related to.
ERROR frames SHOULD include a content-length header and a content-type header if a body is present.

Properties

Authentication: disabled by default, if True a UserName and Password are sent to the server to try user authentication.

HeartBeat: Heart-beating can optionally be used to test the healthiness of the underlying TCP connection and to make sure that the remote end is alive and kicking. In order to enable heart-beating, each party has to declare what it can do and what it would like the other party to do. 0 means it cannot send/receive heart-beats, otherwise it is the desired number of milliseconds between heart-beats.

Options: The name of a virtual host that the client wishes to connect to. It is recommended clients set this to the host name that the socket was established against, or to any name of their choosing. If this header does not match a known virtual host, servers supporting virtual hosting MAY select a default virtual host or reject the connection.

Versions: Set which STOMP versions are supported.

Brokers

TsgcWSPClient_STOMP_RabbitMQ

This is Client Protocol STOMP Component for RabbitMQ Broker, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Destinations
The STOMP specification does not prescribe what kinds of destinations a broker must support, instead the value of the destination header in SEND and MESSAGE frames is broker-specific. The RabbitMQ STOMP adapter supports a number of different destination types:

- **Topic:** SEND and SUBSCRIBE to transient and durable topics.
- **Queue:** SEND and SUBSCRIBE to queues managed by the STOMP gateway.
- **QueueOutside:** SEND and SUBSCRIBE to queues created outside the STOMP gateway.
- **TemporaryQueue:** create temporary queues (in reply-to headers only).
- **Exchange:** SEND to arbitrary routing keys and SUBSCRIBE to arbitrary binding patterns.

Methods
Publish: The SEND frame sends a message to a destination in the messaging system.
PublishTopic
PublishQueue
PublishQueueOutside
PublishTemporaryQueue
PublishExchange

Subscribe: The SUBSCRIBE frame is used to register to listen to a given destination.
Supports following subscriptions
SubscribeTopic
SubscribeQueue
SubscribeQueueOutside
SubscribeTemporaryQueue
SubscribeExchange

UnSubscribe: The UNSUBSCRIBE frame is used to remove an existing subscription.
Supports following UnSubscriptions
UnSubscribeTopic
UnSubscribeQueue
UnSubscribeQueueOutside
UnSubscribeTemporaryQueue
UnSubscribeExchange

ACK: ACK is used to acknowledge the consumption of a message from a subscription.

NACK: NACK is the opposite of ACK. It is used to tell the server that the client did not consume the message.

BeginTransaction: is used to start a transaction. Transactions in this case apply to sending and acknowledging - any messages sent or acknowledged during a transaction will be processed atomically based on the transaction.

CommitTransaction: is used to commit a transaction in progress.

AbortTransaction: is used to roll back a transaction in progress.

Disconnect: use to graceful shutdown connection, where the client is assured that all previous frames have been received by the server.

Events

OnRabbitMQConnected: this event is fired after a new connection is established.

version : The version of the STOMP protocol the session will be using. See Protocol Negotiation for more details.

STOMP 1.2 servers MAY set the following headers:

heart-beat : The Heart-beating settings.

session : A session identifier that uniquely identifies the session.

server : A field that contains information about the STOMP server. The field MUST contain a server-name field and MAY be followed by optional comment fields delimited by a space character.

OnRabbitMQMessage: this event is fired when the client receives a message.

The MESSAGE frame MUST include a destination header indicating the destination the message was sent to. If the message has been sent using STOMP, this destination header SHOULD be identical to the one used in the corresponding SEND frame.

The MESSAGE frame MUST also contain a message-id header with a unique identifier for that message and a subscription header matching the identifier of the subscription that is receiving the message.

If the message is received from a subscription that requires explicit acknowledgment (either client or client-individual mode) then the MESSAGE frame MUST also contain an ack header with an arbitrary value. This header will be used to relate the message to a subsequent ACK or NACK frame.

MESSAGE frames SHOULD include a content-length header and a content-type header if a body is present.

MESSAGE frames will also include all user-defined headers that were present when the message was sent to the destination in addition to the server-specific headers that MAY get added to the frame.

OnRabbitMQReceipt: this event is fired once a server has successfully processed a client frame that requests a receipt.

A RECEIPT frame is an acknowledgment that the corresponding client frame has been processed by the server. Since STOMP is stream based, the receipt is also a cumulative acknowledgment that all the previous frames have been received by the server.

However, these previous frames may not yet be fully processed. If the client disconnects, previously received frames SHOULD continue to get processed by the server.

OnRabbitMQError: this event is fired if something goes wrong.

The ERROR frame SHOULD contain a message header with a short description of the error, and the body MAY contain more detailed information (or MAY be empty).

If the error is related to a specific frame sent from the client, the server SHOULD add additional headers to help identify the original frame that caused the error. For example, if the frame included a receipt header, the ERROR frame SHOULD set the receipt-id header to match the value of the receipt header of the frame which the error is related to.

ERROR frames SHOULD include a content-length header and a content-type header if a body is present.

Properties

Authentication: disabled by default, if True a UserName and Password are sent to the server to try user authentication.

HeartBeat: Heart-beating can optionally be used to test the healthiness of the underlying TCP connection and to make sure that the remote end is alive and kicking. In order to enable heart-beating, each party has to declare what it can do and what it would like the other party to do. 0

means it cannot send/receive heart-beats, otherwise it is the desired number of milliseconds between heart-beats.

Options: The name of a virtual host that the client wishes to connect to. It is recommended clients set this to the host name that the socket was established against, or to any name of their choosing. If this header does not match a known virtual host, servers supporting virtual hosting MAY select a default virtual host or reject the connection.

Versions: Set which STOMP versions are supported.

TsgcWSPClient_STOMP_ActiveMQ

This is Client Protocol STOMP Component for ActiveMQ Broker, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Destinations
The STOMP specification does not prescribe what kinds of destinations a broker must support, instead the value of the destination header in SEND and MESSAGE frames is broker-specific. The Active STOMP adapter supports a number of different destination types:

- **Topic:** SEND and SUBSCRIBE to transient and durable topics.
- **Queue:** SEND and SUBSCRIBE to queues managed by the STOMP gateway.

Publish Options
Note that STOMP is designed to be as simple as possible - so any scripting language/platform can message any other with minimal effort. STOMP allows pluggable headers on each request such as sending & receiving messages. ActiveMQ has several extensions to the Stomp protocol, so that JMS semantics can be supported by Stomp clients. An OpenWire JMS producer can send messages to a Stomp consumer, and a Stomp producer can send messages to an OpenWire JMS consumer. And Stomp to Stomp configurations, can use the richer JMS message control.

STOMP supports the following standard JMS properties on SENT messages:

- **CorrelationId:** Good consumers will add this header to any responses they send.
- **Expires:** Expiration time of the message.
- **JMSXGroupID:** Specifies the Message Groups.
- **JMSXGroupSeq:** Optional header that specifies the sequence number in the Message Groups.
- **Persistent:** Whether or not the message is persistent.
- **Priority:** Priority on the message.
- **ReplyTo:** Destination you should send replies to.
- **MsgType:** Type of the message.

Methods
Publish: The SEND frame sends a message to a destination in the messaging system.
PublishTopic
PublishQueue

Subscribe: The SUBSCRIBE frame is used to register to listen to a given destination.
Supports following subscriptions
SubscribeTopic
SubscribeQueue

UnSubscribe: The UNSUBSCRIBE frame is used to remove an existing subscription.
Supports following UnSubscriptions
UnSubscribeTopic
UnSubscribeQueue

ACK: ACK is used to acknowledge the consumption of a message from a subscription.

NACK: NACK is the opposite of ACK. It is used to tell the server that the client did not consume the message.

BeginTransaction: is used to start a transaction. Transactions in this case apply to sending and acknowledging - any messages sent or acknowledged during a transaction will be processed atomically based on the transaction.

CommitTransaction: is used to commit a transaction in progress.

AbortTransaction: is used to roll back a transaction in progress.

Disconnect: use to graceful shutdown connection, where the client is assured that all previous frames have been received by the server.

Events

OnActiveMQConnected: this event is fired after a new connection is established.

version : The version of the STOMP protocol the session will be using. See Protocol Negotiation for more details.

STOMP 1.2 servers MAY set the following headers:

heart-beat : The Heart-beating settings.

session : A session identifier that uniquely identifies the session.

server : A field that contains information about the STOMP server. The field MUST contain a server-name field and MAY be followed by optional comment fields delimited by a space character.

OnActiveMQMessage: this event is fired when the client receives a message.

The MESSAGE frame MUST include a destination header indicating the destination the message was sent to. If the message has been sent using STOMP, this destination header SHOULD be identical to the one used in the corresponding SEND frame.

The MESSAGE frame MUST also contain a message-id header with a unique identifier for that message and a subscription header matching the identifier of the subscription that is receiving the message.

If the message is received from a subscription that requires explicit acknowledgment (either client or client-individual mode) then the MESSAGE frame MUST also contain an ack header with an arbitrary value. This header will be used to relate the message to a subsequent ACK or NACK frame.

MESSAGE frames SHOULD include a content-length header and a content-type header if a body is present.

MESSAGE frames will also include all user-defined headers that were present when the message was sent to the destination in addition to the server-specific headers that MAY get added to the frame.

OnActiveMQReceipt: this event is fired once a server has successfully processed a client frame that requests a receipt.

A RECEIPT frame is an acknowledgment that the corresponding client frame has been processed by the server. Since STOMP is stream based, the receipt is also a cumulative acknowledgment that all the previous frames have been received by the server. However, these previous frames may not yet be fully processed. If the client disconnects, previously received frames SHOULD continue to get processed by the server.

OnActiveMQError: this event is fired if something goes wrong.

The ERROR frame SHOULD contain a message header with a short description of the error, and the body MAY contain more detailed information (or MAY be empty).

If the error is related to a specific frame sent from the client, the server SHOULD add additional headers to help identify the original frame that caused the error. For example, if the frame included a receipt header, the ERROR frame SHOULD set the receipt-id header to match the value of the receipt header of the frame which the error is related to.

ERROR frames SHOULD include a content-length header and a content-type header if a body is present.

Properties

Authentication: disabled by default, if True a UserName and Password are sent to the server to try user authentication.

HeartBeat: Heart-beating can optionally be used to test the healthiness of the underlying TCP connection and to make sure that the remote end is alive and kicking. In order to enable heart-beating, each party has to declare what it can do and what it would like the other party to do. 0 means it cannot send/receive heart-beats, otherwise it is the desired number of milliseconds between heart-beats.

Options: The name of a virtual host that the client wishes to connect to. It is recommended clients set this to the host name that the socket was established against, or to any name of their choosing. If this header does not match a known virtual host, servers supporting virtual hosting MAY select a default virtual host or reject the connection.

Versions: Set which STOMP versions are supported.

AppRTC

Protocol AppRTC

WebRTC (Web Real-Time Communication) is an API definition being drafted by the World Wide Web Consortium (W3C) to enable browser to browser applications for voice calling, video chat and P2P file sharing without plugins. The RTC in WebRTC stands for Real-Time Communications, a technology that enables audio/video streaming and data sharing between browser clients (peers). As a set of standards, WebRTC provides any browser with the ability to share application data and perform teleconferencing peer to peer, without the need to install plug-ins or third-party software.

WebRTC components are accessed with JavaScript APIs. Currently, in development are the Network Stream API, which represents an audio or video data stream, and the PeerConnection API, which allows two or more users to communicate browser-to-browser. Also under development is a DataChannel API that enables communication of other types of data for real-time gaming, text chat, file transfer, and so forth.

appr.tc is a WebRTC demo application developed by Google and Mozilla, it enables both browsers to “talk” to each other using the WebRTC API.
Components
TsgcWSPServer_AppRTC: Server Protocol AppRTC VCL Component.

TsgcWSPServer_AppRTC

This is Server Protocol AppRTC Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

Parameters

- **IceServers:** here you can configure turn/stun servers for WebRTC connections.
- **RoomLink:** URL base to access room. Example: https://mydemo.com/r/
- **WebSocketURL:** URL to WebSocket server. Example: wss://mydemo.com

*WebRTC Protocol requires STUN/TURN server, demos use public STUN/TURN servers for testing purposes. In order to put in a production system, a dedicated STUN/TURN server is required (not provided with sgcWebsockets library).

WebRTC

Protocol WebRTC

WebRTC (Web Real-Time Communication) is an API definition being drafted by the World Wide Web Consortium (W3C) to enable the browser to browser applications for voice calling, video chat and P2P file sharing without plugins. The RTC in WebRTC stands for Real-Time Communications, a technology that enables audio/video streaming and data sharing between browser clients (peers). As a set of standards, WebRTC provides any browser with the ability to share application data and perform teleconferencing peer to peer, without the need to install plug-ins or third-party software.

WebRTC components are accessed with JavaScript APIs. Currently, in development are the Network Stream API, which represents an audio or video data stream, and the PeerConnection API, which allows two or more users to communicate browser-to-browser. Also under development is a DataChannel API that enables communication of other types of data for real-time gaming, text chat, file transfer, and so forth.

Components
TsgcWSPServer_WebRTC: Server Protocol WebRTC VCL Component.

Browser Test
If you want to test this protocol with your favourite Web Browser, please type this url (you need to define your custom host and port)

```
http://host:port/webrtc.esegece.com.html
```

TsgcWSPServer_WebRTC

This is Server Protocol WebRTC Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

*WebRTC Protocol requires STUN/TURN server, demos use public STUN/TURN servers for testing purposes. In order to put in a production system, a dedicated STUN/TURN server is required (not provided with sgcWebsockets library).

Protocol WebRTC Javascript

Here you can find available methods, you need to replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
<script
src="http://www.example.com:80/webrtc.esegece.com.js"></script>
```

Open Connection
When a WebSocket connection is opened, browser request access to local camera and microphone, you need to allow access.

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/webrtc.esegece.com.js"></script>
<script>
  var socket = new sgcws_webrtc('ws://{%host%}:{%port%}');
</script>
```

Open WebRTC Channel
When a browser has access to local camera and microphone, 'sgcmediastart' event is fired and then you can try to connect to another client using webrtc_connect procedure

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/webrtc.esegece.com.js"></script>
<script>
  var socket = new sgcws_webrtc('ws://{%host%}:{%port%}');
  socket.on('sgcmediastart', function(event)
  {
    socket.webrtc_connect('custom channel');
  }
</script>
```

Close WebRTC channel

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/webrtc.esegece.com.js"></script>
<script>
  socket.webrtc_disconnect('custom channel');
</script>
```

WAMP

Protocol WAMP

WAMP is an open WebSocket subprotocol that provides two asynchronous messaging patterns: RPC and PubSub.

Technically, WAMP is an officially registered WebSocket subprotocol (runs on top of WebSocket) that uses JSON as message serialization format.

What is RPC?

Remote Procedure Call (RPC) is a messaging pattern involving peers to two roles: client and server.
A server provides methods or procedure to call under well-known endpoints.
A client calls remote methods or procedures by providing the method or procedure endpoint and any arguments for the call.
The server will execute the method or procedure using the supplied arguments to the call and return the result of the call to the client.

What is PubSub?

Publish & Subscribe (PubSub) is a messaging pattern involving peers of three roles: publisher, subscriber and broker.
A publisher sends (publishes) an event by providing a topic (aka channel) as the abstract address, not a specific peer.
A subscriber receives events by first providing topics (aka channels) he is interested. Subsequently, the subscriber will receive any events publishes to that topic.
The broker sits between publishers and subscribers and mediates messages publishes to subscribers. A broker will maintain lists of subscribers per topic so it can dispatch new published events to the appropriate subscribers.
A broker may also dispatch events on its own, for example when the broker also acts as an RPC server and a method executed on the server should trigger a PubSub event.
In summary, PubSub decouples publishers and receivers via an intermediary, the broker.

Components
TsgcWSPServer_WAMP: Server Protocol WAMP VCL Component.

TsgcWSPClient_WAMP: Client Protocol WAMP VCL Component.

Javascript Component: Client Javascript Reference.

Browser Test
If you want to test this protocol with your favourite Web Browser, please type this URL(you need to define your custom host and port)

```
http://host:port/wamp.esegece.com.html
```

TsgcWSPServer_WAMP

This is Server Protocol WAMP Component, you need to drop this component in the form and select a TsgcWebSocketServer Component using Server Property.

Methods

CallResult: When the execution of the remote procedure finishes successfully, the server responds by sending a message with the result.

- **CallId:** this is the ID generated by client when request a call to a procedure
- **Result:** is the result, can be a number, a JSON object...

CallError: When the remote procedure call could not be executed, an error or exception occurred during the execution or the execution of the remote procedure finishes unsuccessfully for any other reason, the server responds by sending a message with error details.

- **CallId:** this is the ID generated by the client when requesting a call to a procedure
- **ErrorURI:** identifies the error.
- **ErrorDesc:** error description.
- **ErrorDetails:** application error details, is optional.

Event: Subscribers receive PubSub events published by subscribers via the EVENT message.

- **TopicURI:** channel name where is subscribed.
- **Event:** message text.

Events

OnCall: event fired when the server receives RPC called by the client

- **CallId:** this is the ID generated by the client when requesting a call to a procedure
- **ProcUri:** procedure identifier...
- **Arguments:** procedure params, can be a integer, a JSON object, a list...

OnPrefix: Procedures and Errors are identified using URIs or CURIEs, this event is fired when a client sends a new prefix

- **Prefix:** compact URI expression.
- **URI:** full URI.

TsgcWSPClient_WAMP

This is Client Protocol WAMP Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Methods

Prefix: Procedures and Errors are identified using URIs or CURIEs, the client uses this method to send a new prefix.

- **aPrefix:** compact URI expression.
- **aURI:** full URI.

Subscribe: A client requests access to a valid topicURI (or CURIE from Prefix) to receive events published to the given topicURI. The request is asynchronous, the server will not return an acknowledgement of the subscription.

- **aTopicURI:** channel name.

UnSubscribe: Calling unsubscribe on a topicURI informs the server to stop delivering messages to the client previously subscribed to that topicURI.

- **aTopicURI:** channel name.

Call: sent by the client when requests a Remote Procedure Call (RPC)

- **aCallId:** this is the UUID generated by client
- **aProcURI:** procedure identifier.
- **aArguments:** procedure params, can be a integer, a JSON object, a list...

Publish: The client will send an event to all clients connected to the server who have subscribed to the topicURI.

- **TopicURI:** channel name.
- **Event:** message text.

Events

OnWelcome: is the first server-to-client message sent by a WAMP server

- **SessionId:** is a string that is randomly generated by the server and unique to the specific WAMP session. The sessionId can be used for at least two situations: 1) specifying lists of excluded or eligible clients when publishing event and 2) in the context of performing authentication or authorization.
- **ProtocolVersion:** is an integer that gives the WAMP protocol version the server speaks, currently it MUST be 1.
- **ServerIdent:** is a string the server may use to disclose it's version, software, platform or identity.

OnCallError: event fired when the remote procedure call could not be executed, an error or exception occurred during the execution or the execution of the remote procedure finishes unsuccessfully for any other reason, the server responds by sending a message with error details

- **CallId:** this is the ID generated by the client when requesting a call to a procedure
- **ErrorURI:** identifies the error.
- **ErrorDesc:** error description.
- **ErrorDetails:** application error details, is optional.

OnCallResult: event fired when the execution of the remote procedure finishes successfully, the server responds by sending a message with the result.

- **CallId:** this is the ID generated by client when request a call to a procedure
- **Result:** is the result, can be a number, a JSON object...

OnEvent: event fired when the client receives PubSub events published by subscribers via the EVENT message.

- **TopicURI:** channel name where is subscribed.
- **Event:** message text.

Protocol WAMP Javascript

Here you can find available methods, you need to replace {%host%} and {%port%} variables as needed, example: if you have configured your sgcWebSocket server to listen port 80 on www.example.com website you need to configure:

```
<script src="http://www.example.com:80/sgcWebSockets.js"></script>
<script src="http://www.example.com:80/wamp.esegece.com.js"></script>
```

Open Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
</script>
```

Send New Prefix

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.prefix('sgc', 'http://www.esegece.com');
</script>
```

Request RPC (Remote Procedure Call)

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.call('', 'sgc:CallTest', '20')
</script>
```

Subscribe to a TopicURI

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.subscribe('sgc:test)
</script>
```

UnSubscribe to a TopicURI

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
```

```
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.unsubscribe('sgc:test)
</script>
```

Publish message

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.publish('sgc:channel', 'Test Message', [], []);
</script>
```

Show Alert with Message Received

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws('ws://{%host%}:{%port%}');
  socket.on('sgcmessage', function(event)
  {
    alert(event.message);
  }
</script>
```

Show Alert OnCallResult or OnCallError

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.on('wampcallresult', function(event)
  {
    alert('call result: ' + event.CallId + ' - ' + event.CallResult);
  }
  socket.on('wampcallerror', function(event)
  {
    alert('call error: ' + event.CallId + ' - ' + event.ErrorURI + ' -
' + event.ErrorDesc + ' - ' + event.ErrorDetails);
  }
</script>
```

Show Alert OnEvent

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.on('wampevent', function(event)
  {
    alert('call result: ' + event.TopicURI + ' - ' + event.Event);
  }
</script>
```

Show Alert OnConnect, OnDisconnect and OnError Events

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  var socket = new sgcws_wamp('ws://{%host%}:{%port%}');
  socket.on('open', function(event)
  {
    alert('sgcWebSocket Open!');
  };
  socket.on('close', function(event)
  {
    alert('sgcWebSocket Closed!');
  };
  socket.on('error', function(event)
  {
    alert('sgcWebSocket Error: ' + event.message);
  };
</script>
```

Close Connection

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  socket.close();
</script>
```

Get Connection Status

```
<script src="http://{%host%}:{%port%}/sgcWebSockets.js"></script>
<script src="http://{%host%}:{%port%}/wamp.esegece.com.js"></script>
<script>
  socket.state();
</script>
```

WAMP 2.0

Protocol WAMP 2

WAMP provides Unified Application Routing in an open WebSocket protocol that works with different languages.

Using WAMP you can build distributed systems out of application components which are loosely coupled and communicate in (soft) real-time.

At its core, WAMP offers two communication patterns for application components to talk to each other:

- Publish & Subscribe (PubSub)

- Remote Procedure Calls (RPC)

WAMP is easy to use, simple to implement and based on modern Web standards: WebSocket, JSON and URIs.

Components
TsgcWSPClient_WAMP2: Client Protocol WAMP2 VCL Component.

TsgcWSPClient_WAMP2

This is Client Protocol WAMP Component, you need to drop this component in the form and select a TsgcWebSocketClient Component using Client Property.

Session Methods

- **ABORT:** Both the Router and the Client may abort the opening of a WAMP session by sending an ABORT message.

  Reason MUST be an URI.
  Details MUST be a dictionary that allows to provide additional, optional closing information (see below).

No response to an ABORT message is expected.

- **GOODBYE:** A WAMP session starts its lifetime with the Router sending a WELCOME message to the Client and ends when the underlying transport disappears or when the WAMP session is closed explicitly by a GOODBYE message sent by one Peer and a GOODBYE message sent from the other Peer in response.

  Reason MUST be a URI.
  Details MUST be a dictionary that allows providing additional, optional closing information.

Publish/Subscribe Methods

- **PUBLISH:** When a Publisher requests to publish an event to some topic, it sends a PUBLISH message to a Broker:

  Request is a random, ephemeral ID chosen by the Publisher and used to correlate the Broker's response with the request.
  Options is a dictionary that allows to provide additional publication request details in an extensible way. This is described further below.
  Topic is the topic published to.
  Arguments is a list of application-level event payload elements. The list may be of zero length.
  ArgumentsKw is an optional dictionary containing application-level event payload, provided as keyword arguments. The dictionary may be empty.

If the Broker is able to fulfil and allowing the publication, the Broker will send the event to all current Subscribers of the topic of the published event.
By default, publications are unacknowledged, and the Broker will not respond, whether the publication was successful indeed or not.

- **SUBSCRIBE:** A Subscriber communicates its interest in a topic to a Broker by sending a SUBSCRIBE message:

  Request MUST be a random, ephemeral ID chosen by the Subscriber and used to correlate the Broker's response with the request.
  Options MUST be a dictionary that allows providing additional subscription request details in an extensible way.
  Topic is the topic the Subscriber wants to subscribe to and MUST be a URI.

- **UNSUBSCRIBE:** When a Subscriber is no longer interested in receiving events for a subscription it sends an UNSUBSCRIBE message

Request MUST be a random, ephemeral ID chosen by the Subscriber and used to correlate the Broker's response with the request.
SUBSCRIBED.Subscription MUST be the ID for the subscription to unsubscribe from, originally handed out by the Broker to the Subscriber.

RPC Methods

•**CALL:** When a Caller wishes to call a remote procedure, it sends a CALL message to a Dealer:

Request is a random, ephemeral ID chosen by the Caller and used to correlate the Dealer's response with the request.
Options is a dictionary that allows to provide additional call request details in an extensible way. This is described further below.
Procedure is the URI of the procedure to be called.
Arguments is a list of positional call arguments (each of arbitrary type). The list may be of zero length.
ArgumentsKw is a dictionary of keyword call arguments (each of arbitrary type). The dictionary may be empty.

•**REGISTERCALL:** A Callee announces the availability of an endpoint implementing a procedure with a Dealer by sending a REGISTER message:

Request is a random, ephemeral ID chosen by the Callee and used to correlate the Dealer's response with the request.
Options is a dictionary that allows providing additional registration request details in a extensible way. This is described further below.
Procedure is the procedure the Callee wants to register

•**UNREGISTERCALL:** When a Callee is no longer willing to provide an implementation of the registered procedure, it sends an UNREGISTER message to the Dealer:

Request is a random, ephemeral ID chosen by the Callee and used to correlate the Dealer's response with the request.
REGISTERED.Registration is the ID for the registration to revoke, originally handed out by the Dealer to the Callee.

•**INVOCATION:** If the Dealer is able to fulfil (mediate) the call and it allows the call, it sends a INVOCATION message to the respective Callee implementing the procedure:

Request is a random, ephemeral ID chosen by the Dealer and used to correlate the Callee's response with the request.
REGISTERED.Registration is the registration ID under which the procedure was registered at the Dealer.
Details is a dictionary that allows to provide additional invocation request details in an extensible way. This is described further below.
CALL.Arguments is the original list of positional call arguments as provided by the Caller.
CALL.ArgumentsKw is the original dictionary of keyword call arguments as provided by the Caller.

•**YIELD:** If the Callee is able to successfully process and finish the execution of the call, it answers by sending a YIELD message to the Dealer:

INVOCATION.Request is the ID from the original invocation request.
Options is a dictionary that allows providing additional options.
Arguments is a list of positional result elements (each of arbitrary type). The list may be of zero length.

ArgumentsKw is a dictionary of keyword result elements (each of arbitrary type). The dictionary may be empty.

Events

OnWAMPSession: After the underlying transport has been established, the opening of a WAMP session is initiated by the Client sending a `HELLO` message to the Router

- **Realm:** is a string identifying the realm this session should attach to
- **Details:** is a dictionary that allows to provide additional opening information

OnWAMPWelcome: A Router completes the opening of a WAMP session by sending a WELCOME reply message to the Client.

- **Session:** MUST be a randomly generated ID specific to the WAMP session. This applies for the lifetime of the session.
- **Details:** is a dictionary that allows to provide additional information regarding the open session.

OnWAMPChallenge: this event is raised when server requires client authenticate against server.

- **Authmethod:** this is the authentication method requested by server, example: ticket.
- **Details:** optional
- **Secret:** here client can set secret key which will be used to authenticate.

Example: Authentication using ticket method.

```
// First OnWAMPSession event will be called asking details about new
session, set realm and authentication id which will be sent to serve

procedure OnWAMPSession(Connection: TsgcWSConnection;
    var aRealm, aDetails: string);
begin
  aRealm := 'realm1';
  aDetails := '{"authmethods": ["ticket"], "authid": "joe"}';
end;

// If AuthId parameter is accepted by server, it will request an
authentication through Challenge message, here you can set "secret
key" of "authid" param.

procedure OnWAMPChallenge(Connection:
    TsgcWSConnection; AuthMethod, Details: string; var Secret:
string);
begin
  Secret := 'your secret key';
end;
```

```
// If Authentication is successful, server will send a Welcome message

procedure OnWAMPWelcome(Connection: TsgcWSConnection;
    SessionId: Int64; Details: string);
begin
  ShowMessage('authenticated');
end;
```

OnWAMPAbort: Both the Router and the Client may abort the opening of a WAMP session by sending an ABORT message.

- **Reason:** MUST be an URI.
- **Details:** MUST be a dictionary that allows providing additional, optional closing information.

OnWAMPGoodBye: A WAMP session starts its lifetime with the Router sending a `WELCOME` message to the Client and ends when the underlying transport disappears or when the WAMP session is closed explicitly by a GOODBYE message sent by one Peer and a `GOODBYE` message sent from the other Peer in response.

- **Reason:** MUST be an URI.
- **Details:** MUST be a dictionary that allows to provide additional, optional closing information.

OnWAMPSubscribed: If the Broker is able to fulfill and allow the subscription, it answers by sending a SUBSCRIBED message to the Subscriber

- **SUBSCRIBE.Request:** MUST be the ID from the original request.
- **Subscription:** MUST be an ID chosen by the Broker for the subscription.

OnWAMPUnSubscribed: Upon successful unsubscription, the Broker sends an UNSUBSCRIBED message to the Subscriber

- **UNSUBSCRIBE.Request:** MUST be the ID from the original request.

OnWAMPPublished: If the Broker is able to fulfill and allowing the publication, and PUBLISH.Options.acknowledge == true, the Broker replies by sending a PUBLISHED message to the Publisher:

- **PUBLISH.Request:** is the ID from the original publication request.
- **Publication:** is a ID chosen by the Broker for the publication.

OnWAMPEvent: When a publication is successful and a Broker dispatches the event, it determines a list of receivers for the event based on Subscribers for the topic published to and, possibly, other information in the event. Note that the Publisher of an event will never receive the published event even if the Publisher is also a Subscriber of the topic published to. The Advanced Profile provides options for more detailed control over publication. When a Subscriber is deemed to be a receiver, the Broker sends the Subscriber an EVENT message.

- **SUBSCRIBED.Subscription:** is the ID for the subscription under which the Subscriber receives the event - the ID for the subscription originally handed out by the Broker to the Subscribe*.
- **PUBLISHED.Publication:** is the ID of the publication of the published event.
- **DETAILS:** is a dictionary that allows the Broker to provide additional event details in a extensible way.
- **PUBLISH.Arguments:** is the application-level event payload that was provided with the original publication request.
- **PUBLISH.ArgumentKw:** is the application-level event payload that was provided with the original publication request.

OnWAMPError: When the request fails, the Broker sends an ERROR

- **METHOD:** is the ID of the Method.
- **REQUEST.ID:** is the ID of the Request.
- **DETAILS:** is a dictionary that allows the Broker to provide additional event details in a extensible way.
- **ERROR:** describes the message error.
- **PUBLISH.Arguments:** is the application-level event payload that was provided with the original publication request.
- **PUBLISH.ArgumentKw:** is the application-level event payload that was provided with the original publication request.

OnWAMPResult: The Dealer will then send a RESULT message to the original Caller:

- **CALL.Request:** is the ID from the original call request.
- **DETAILS:** is a dictionary of additional details.
- **YIELD.Arguments:** is the original list of positional result elements as returned by the Callee.
- **YIELD.ArgumentsKw:** is the original dictionary of keyword result elements as returned by the Callee.

OnWAMPRegistered: If the Dealer is able to fulfill and allowing the registration, it answers by sending a REGISTERED message to the Callee:

- **REGISTER.Request:** is the ID from the original request.
- **Registration:** is an ID chosen by the Dealer for the registration.

OnWAMPUnRegistered: When a Callee is no longer willing to provide an implementation of the registered procedure, it sends an UNREGISTER message to the Dealer:

- **Request:** is a random, ephemeral ID chosen by the Callee and used to correlate the Dealer's response with the request.
- **REGISTERED.Registration:** is the ID for the registration to revoke, originally handed out by the Dealer to the Callee.

APIs

WebSocket APIs

There are several implementations based on WebSockets: finance, message publishing, queues... sgcWebSockets implements the most important APIs based on WebSocket protocol. In order to use an API, just attach API component to the client and all messages will be handled by API component (only one API component can be attached to a client).

List of WebSocket APIs:

1. SocketIO: is a JavaScript library for real-time web applications. It enables real-time, bi-directional communication between web clients and servers.

2. Blockchain: Blockchain WebSocket API allows developers to receive Real-Time notifications about new transactions and blocks.

3. Bitfinex: Bitfinex is one of the world's largest and most advanced cryptocurrency trading platform. Users can exchange Bitcoin, Ethereum, Ripple, EOS, Bitcoin Cash, Iota, NEO, Litecoin, Ethereum Classic...

4. Pusher: Pusher is an easy and reliable platform with flexible pub/sub messaging, live user lists, authentication...

5. SignalR: is a library for ASP.NET developers that makes developing real-time web functionality using WebSockets as transport.

6. Bittrex: is a US-based cryptocurrency exchange.

7. Binance: is an international multi-language cryptocurrency exchange.

8. Bitstamp: Bitstamp is one of the world's longest standing crypto exchange, supporting the blockchain ecosystem since 2011.

9. Huobi: is an international multi-language cryptocurrency exchange.

10. Cex: is a cryptocurrency exchange and former Bitcoin cloud mining provider.

11. Bitmex: is a cryptocurrency exchange and derivative trading platform.

12. SignalRCore: ASP.NET Core SignalR is an open-source library that simplifies adding real-time web functionality to apps.

13. FXCM: also known as Forex Capital Markets, is a retail broker for trading on the foreign exchange market.

14. Kraken: is a US-based cryptocurrency exchange.

15. Discord: is one of the most popular communication tools for online gaming and streaming.

WebSocket APIs can be registered at **runtime**, just call Method **RegisterAPI** and pass API component as a parameter.

Other APIs:

1. **Telegram:** is a cloud-based instant messaging and voice over IP service. Users can send messages and exchange photos, videos, stickers, audio and files of any type.

APIs

API SocketIO

SocketIO

Socket.IO is a JavaScript library for real-time web applications. It enables real-time, bi-directional communication between web clients and servers. It has two parts: a client-side library that runs in the browser, and a server-side library for Node.js. Both components have a nearly identical API. Like Node.js, it is event-driven.

Messages Types

0: open (Sent from the server when a new transport is opened (recheck))

1: close (Request the close of this transport but does not shut down the connection itself.)

2: ping (Sent by the client. The server should answer with a pong packet containing the same data)
example
client sends: 2probe
server sends: 3probe

3: pong (Sent by the server to respond to ping packets.)

4: string message (actual message, client and server should call their callbacks with the data.)
example:
42/chat,[“join”,”{room:1}"]
4 is the message packet type in the engine.io protocol
2 is the EVENT type in the socket.io protocol
/chat is the data which is processed by socket.io
socket.io will fire the “join” event
will pass "room: 1" data. It is possible to omit namespace only when it is /.

5: upgrade (Before engine.io switches a transport, it tests, if server and client can communicate over this transport. If this test succeeds, the client sends an upgrade packets which requests the server to flush its cache on the old transport and switch to the new transport.)

6: noop (A noop packet. Used primarily to force a poll cycle when an incoming WebSocket connection is received.)

Properties

API: specifies SocketIO version:

ioAPI0: supports socket.io 0.* servers (selected by default)

ioAPI1: supports socket.io 1.* servers

ioAPI2: supports socket.io 2.* servers

Base64: if enabled, binary messages are received as base64.

HandShakeCustomURL: allows customizing URLl to get socket.io session.

HandShakeTimestamp: only enable if you want to send timestamp as a parameter when a new session is requested (enable this property if you try to access a gevent-socketio python server).

Namespace: allows setting a namespace when connects to the server.

Polling: disabling this property, client will connect directly to server using websocket as transport.

Parameters: allows to set connection parameters.

EncodeParameters: if enabled, parameters are encoded.

Methods

```
// Use WriteData method to send messages to socket.io server
(following Message Types sections)

// 1. call method add user and one parameter with John as user name

TsgcWSAPI_SocketIO.WriteData('42["add user", "John"]');

// 2. call method join of channel /chat

TsgcWSAPI_SocketIO.WriteData('42/chat,["join","{room:1}"]');
```

Events

OnHTTPConnectionSSL

```
// When a WebSocket server requires secure connections, you can get an
error message like this when a client tries to connect to server:

//   Error connecting with SSL. error:XXXXXXXX:SSL
routines:ssl3_read_bytes:tlsv1 alert protocol version

// This error means that your client is trying to connect using a TLS
version which is not supported by the server.
// To resolve this error you must handle OnSSLAfterCreateHandler of
WebSocket client component and set a newer TLS version.
// For example: here we are setting TLS 1.2 as a protocol version.

procedure TfrmWebSocketClient.SOCKETIOHTTPConnectionSSL(Sender:
TObject;
    aSSLHandler: TIdSSLIOHandlerSocketBase);
begin
  TIdSSLIOHandlerSocketOpenSSL(aSSLHandler).SSLOptions.Method :=
sslvTLSv1_2;
end;
```

OnHTTPRequest

```
// Before a new websocket connection is established, socket.io server
requires client open a new HTTP connection to get a new session id.
// In some cases, socket.io server requires authentication using HTTP
headers, you can use this event to add custom HTTP headers,
// like Basic authorization or Bearer token authentication


procedure TfrmWebSocketClient.SOCKETIOHTTPRequest(Sender: TObject;
aRequest: TsgcWSSocketIOHTTPRequest);
begin
  aRequest.Headers.Add('Authorization: Bearer
ajdlfkjsdklfjsadlje3wwe34994ashfadfzkjsdlkjf');
end;
```

OnAfterConnect

```
// This event is called after socket.io connection is successful and
client can send messages to server.
// Here you can subscribe to namespaces for example.
```

API Blockchain

Blockchain

Blockchain WebSocket API allows developers to receive Real-Time notifications about new transactions and blocks.

Once WebSocket is open you can subscribe to a channel:

- **SubscribeTransactions:** Subscribe to notifications for all new bitcoin transactions.
- **UnsubscribeTransactions:** UnSubscribe to notifications for all new bitcoin transactions.

- **SubscribeAddress:** Receive new transactions for a specific bitcoin address.
- **UnSubscribeAddress:** Stop receiving new transactions for a specific bitcoin address.

Transactions are received **OnNewTransaction** Event:


```
{
    "op": "utx",
    "x": {
        "lock_time": 0,
        "ver": 1,
        "size": 192,
        "inputs": [
            {
                "sequence": 4294967295,
                "prev_out": {
                    "spent": true,
                    "tx_index": 99005468,
                    "type": 0,
                    "addr": "1BwGf3z7n2fHk6NoVJNkV32qwyAYsMhkWf",
                    "value": 65574000,
                    "n": 0,
                    "script":
"76a91477f4c9ee75e449a74c21a4decfb50519cbc245b388ac"
                },
                "script":
"483045022100e4ff962c292705f051c2c2fc519fa775a4d8955bce1a3e29884b27852
77999ed02200b537ebd22a9f25fbbbcc9113c69c1389400703ef2017d80959ef0f1d68
5756c012102618e08e0c8fd4c5fe539184a30fe35a2f5fccf7ad62054cad29360d871f
8187d"
            }
        ],
        "time": 1440086763,
        "tx_index": 99006637,
        "vin_sz": 1,
        "hash":
"0857b9de1884eec314ecf67c040a2657b8e083e1f95e31d0b5ba3d328841fc7f",
        "vout_sz": 1,
        "relayed_by": "127.0.0.1",
        "out": [
            {
                "spent": false,
                "tx_index": 99006637,
```

```
                "type": 0,
                "addr": "1A828tTnkVFJfSvLCqF42ohZ51ksS3jJgX",
                "value": 65564000,
                "n": 0,
                "script":
"76a914640cfdf7b79d94d1c980133e3587bd6053f091f388ac"
            }
        ]
    }
}
```


- **SubscribeBlocks:** Receive notifications when a new block is found. Note: if the chain splits you will receive more than one notification for a specific block height.
- **UnSubscribeBlocks:** Stop receiving notifications when a new block is found. Note: if the chain splits you will receive more than one notification for a specific block height.

Blocks are received **OnNewBlock** event:


```
{
    "op": "block",
    "x": {
        "txIndexes": [
            3187871,
            3187868
        ],
        "nTx": 0,
        "totalBTCSent": 0,
        "estimatedBTCSent": 0,
        "reward": 0,
        "size": 0,
        "blockIndex": 190460,
        "prevBlockIndex": 190457,
        "height": 170359,
        "hash":
"000000000000006436073c07dfa188a8fa54fefadf571fd774863cda1b884b90f",
        "mrklRoot":
"94e51495e0e8a0c3b78dac1220b2f35ceda8799b0a20cfa68601ed28126cfcc2",
        "version": 1,
        "time": 1331301261,
        "bits": 436942092,
        "nonce": 758889471
    }
}
```

API Bitfinex

Bitfinex

Bitfinex is one of the world's largest and most advanced cryptocurrency trading platform. Users can exchange Bitcoin, Ethereum, Ripple, EOS, Bitcoin Cash, Iota, NEO, Litecoin, Ethereum Classic...

Bitfinex WebSocket API version is 2.0

Each message sent and received via the Bitfinex's WebSocket channel is encoded in JSON format

A symbol can be a trading pair or a margin currency:

- Trading pairs symbols are formed prepending a "t" before the pair (i.e tBTCUSD, tETHUSD).
- Margin currencies symbols are formed prepending an "f" before the currency (i.e fUSD, fBTC, ...)

After a successful connection, **OnBitfinexConnect** event is raised and you get Bitfinex API Version number as a parameter.

You can call **Ping** method to test connection to the server.

If the server sends any information, this can be handle using **OnBitfinexInfoMessage** event, where a Code and a Message are parameters with information about the message sent by the server. Example codes:

20051 : Stop/Restart WebSocket Server (please reconnect)
20060 : Entering in Maintenance mode. Please pause any activity and resume after receiving the info message 20061 (it should take 120 seconds at most).
20061 : Maintenance ended. You can resume normal activity. It is advised to unsubscribe/subscribe again all channels.

In case of error, **OnBitfinexError** will be raised, and information about error provided. Example error codes:

10000 : Unknown event
10001 : Unknown pair

In order to change the configuration, call **Configuration** method and pass as a parameter one of the following flags:

CS_DEC_S = 8; // Enable all decimal as strings.
CS_TIME_S = 32; // Enable all times as date strings.
CS_SEQ_ALL = 65536; // Enable sequencing BETA FEATURE
CHECKSUM = 131072; // Enable checksum for every book iteration. Checks the top 25 entries for each side of the book. The checksum is a signed int.

Subscribe Public Channels

There are channels which are public and there is no need to authenticate against the server. All messages are raised **OnBitfinexUpdate** event.

SubscribeTicker

The ticker is a high level overview of the state of the market. It shows you the current best bid and ask, as well as the last trade price. It also includes information such as daily volume and how much the price has moved over the last day.

```
// Trading pairs
[
  CHANNEL_ID,
  [
    BID,
    BID_SIZE,
    ASK,
    ASK_SIZE,
    DAILY_CHANGE,
    DAILY_CHANGE_PERC,
    LAST_PRICE,
    VOLUME,
    HIGH,
    LOW
  ]
]
// Funding pairs
[
  CHANNEL_ID,
  [
    FRR,
    BID,
    BID_PERIOD,
    BID_SIZE,
    ASK,
    ASK_PERIOD,
    ASK_SIZE,
    DAILY_CHANGE,
    DAILY_CHANGE_PERC,
    LAST_PRICE,
    VOLUME,
    HIGH,
    LOW
  ]
]
```

SubscribeTrades

This channel sends a trade message whenever a trade occurs at Bitfinex. It includes all the pertinent details of the trade, such as price, size and time.

```
// on trading pairs (ex. tBTCUSD)
[
  CHANNEL_ID,
  [
    [
      ID,
      MTS,
      AMOUNT,
      PRICE
    ],
```

```
    ...
  ]
]
// on funding currencies (ex. fUSD)
[
  CHANNEL_ID,
  [
    [
      ID,
      MTS,
      AMOUNT,
      RATE,
      PERIOD
    ],
    ...
  ]
]
```

SubscribeOrderBook

The Order Books channel allows you to keep track of the state of the Bitfinex order book. It is provided on a price aggregated basis, with customizable precision. After receiving the response, you will receive a snapshot of the book, followed by updates upon any changes to the book.

```
// on trading pairs (ex. tBTCUSD)
[
  CHANNEL_ID,
  [
    [
      PRICE,
      COUNT,
      AMOUNT
    ],
    ...
  ]
]

// on funding currencies (ex. fUSD)
[
  CHANNEL_ID,
  [
    [
      RATE,
      PERIOD,
      COUNT,
      AMOUNT
    ],
    ...
  ]
]
```

SubscribeRawOrderBook

These are the most granular books.

```
// on trading pairs (ex. tBTCUSD)
[
  CHANNEL_ID,
  [
    [
      ORDER_ID,
      PRICE,
      AMOUNT
    ],
    ...
  ]
]

// on funding currencies (ex. fUSD)
[
  CHANNEL_ID,
  [
    [
      OFFER_ID,
      PERIOD,
      RATE,
      AMOUNT
    ],
    ...
  ]
]
```

SubscribeCandles

Provides a way to access charting candle info. Time Frames:

1m: one minute
5m : five minutes
15m : 15 minutes
30m : 30 minutes
1h : one hour
3h : 3 hours
6h : 6 hours
12h : 12 hours
1D : one day
7D : one week
14D : two weeks
1M : one month

```
[
  CHANNEL_ID,
  [
    [
      MTS,
      OPEN,
      CLOSE,
      HIGH,
      LOW,
      VOLUME
    ],
    ...
  ]
]
```

Subscribe Authenticated Channels

This channel allows you to keep up to date with the status of your account. You can receive updates on your positions, your balances, your orders and your trades.

Use **Authenticate** method in order to Authenticate against the server and set required parameters.

Once authenticated, you will receive updates of: Orders, positions, trades, funding offers, funding credits, funding loans, wallets, balance info, margin info, funding info, funding trades...

You can request **UnAuthenticate** method if you want to log off from the server.

API Pusher

Pusher

Pusher it's an easy and reliable platform with nice features based on WebSocket protocol: flexible pub/sub messaging, live user lists (presence), authentication...

Pusher WebSocket API is 7.

Data is sent bi-directionally over a WebSocket as text data containing UTF8 encoded JSON (Binary WebSocket frames are not supported).

You can call **Ping** method to test connection to the server. Essentially any messages received from the other party are considered to mean that the connection is alive. In the absence of any messages, either party may check that the other side is responding by sending a ping message, to which the other party should respond with a pong.

Before you connect, you must complete the following fields:

```
Pusher.Cluster := 'eu'; // cluster where is located your pusher
account
Pusher.Key := '9c3b7ef25qe97a00116c'; // your pusher api key
Pusher.Name := 'js'; // optional, name of your application
Pusher.Version := '4.1';  // optional, version of your application
Pusher.TLS := True; // if encrypted, set to True
Pusher.Secret := '2dc792e1916ac49e6b3f'; // pusher secret string
(needed for private and absence channels)
```

After a successful connection, **OnPusherConnect** event is raised and you get following fields:

- Socket ID: A unique identifier for the connected client.
- Timeout: The number of seconds of server inactivity after which the client should initiate a ping message (this is handled automatically by component).

In case of error, **OnPusherError** will be raised, and information about error provided. An error may be sent from Pusher in response to invalid authentication, an invalid command, etc.

4000-4099

Indicates an error resulting in the connection being closed by Pusher, and that attempting to reconnect using the same parameters will not succeed.

4000: Application only accepts SSL connections, reconnect using wss://
4001: Application does not exist
4003: Application disabled
4004: Application is over connection quota
4005: Path not found
4006: Invalid version string format
4007: Unsupported protocol version
4008: No protocol version supplied

4100-4199

Indicates an error resulting in the connection being closed by Pusher, and that the client may reconnect after 1s or more.

4100: Over capacity

4200-4299

Indicates an error resulting in the connection being closed by Pusher, and that the client may reconnect immediately.

4200: Generic reconnect immediately
4201: Pong reply not received: ping was sent to the client, but no reply was received - see ping and pong messages
4202: Closed after inactivity: The client has been inactive for a long time (currently 24 hours) and client does not support ping. Please upgrade to a newer WebSocket draft or implement version 5 or above of this protocol.

4300-4399

Any other type of error.

4301: Client event rejected due to rate limit

Channels

Channels are a fundamental concept in Pusher. Each application has a number of channels, and each client can choose which channels it subscribes to.

Channels provide:

- A way of filtering data. For example, in a chat application, there may be a channel for people who want to discuss ‘dogs’
- A way of controlling access to different streams of information. For example, a project management application would want to authorise people to get updates about ‘projectX’

It's strongly recommended that channels are used to filter your data and that it is not achieved using events. This is because all events published to a channel are sent to all subscribers, regardless of their event binding.

Channels don’t need to be explicitly created and are instantiated on client demand. This means that creating a channel is easy. Just tell a client to subscribe to it.

There are 3 types of channels:

- **Public channels** can be subscribed to by anyone who knows their name
- **Private channels** introduce a mechanism which lets your server control access to the data you are broadcasting
- **Presence channels** are an extension of private channels. They let you ‘register’ user information on subscription, and let other members of the channel know who’s online

Public Channels
Public channels should be used for publicly accessible data as they do not require any form authorisation in order to be subscribed to.

You can subscribe and unsubscribe from channels at any time. There’s no need to wait for the Pusher to finish connecting first.

Example: subscribe to channel "my-channel".

Delphi
```
APIPusher.Subscribe('my-channel');
```

If you are subscribed successfully **OnPusherSubscribe** event will be raised, if there is an error you will get a message in **OnPusherError** event.

All messages from the subscribed channel will be received **OnPusherEvent** event.

Private Channels
Requires Indy 10.5.7 or later

Private channels should be used when access to the channel needs to be restricted in some way. In order for a user to subscribe to a private channel permission must be authorised.

Example: subscribe to channel "my-private-channel".

Delphi
```
APIPusher.Subscribe('my-private-channel', pscPrivateChannel);
```

If you are subscribed successfully **OnPusherSubscribe** event will be raised, if there is an error you will get a message in **OnPusherError** event.

All messages from the subscribed channel will be received **OnPusherEvent** event.

Presence Channels
Requires Indy 10.5.7 or later

Presence channels build on the security of Private channels and expose the additional feature of an awareness of who is subscribed to that channel. This makes it extremely easy to build chat room and “who’s online” type functionality to your application. Think chat rooms, collaborators on a document, people viewing the same web page, competitors in a game, that kind of thing.

Presence channels are subscribed to from the client API in the same way as private channels but the channel name must be prefixed with presence-. As with private channels an HTTP Request is made to a configurable authentication URL to determine if the current user has permissions to access the channel.

Information on users subscribing to, and unsubscribing from a channel can then be accessed by binding to events on the presence channel and the current state of users subscribed to the channel is available via the channel.members property.

Example: subscribe to channel "my-presence-channel".

Delphi
```
APIPusher.Subscribe('my-presence-channel', pscPresenceChannel,
'{"user_id":"John_Smith","user_info":{"name":"John Smith"}}');
```

If you are subscribed successfully **OnPusherSubscribe** event will be raised, if there is an error you will get a message in **OnPusherError** event.

All messages from the subscribed channel will be received **OnPusherEvent** event.

Publish Messages

Not only you can receive messages from subscribed channels, but you can also send messages to other subscribed users.
Call method **Publish** to send a message to all subscribed users of channel.

Example: send an event to all subscribed users of "my-channel'

Delphi

```
APIPusher.Publish('my-event', 'my-channel');
```

Publish no more than 10 messages per second per client (connection). Any events triggered above this rate limit will be rejected by Pusher API. This is not a system issue, it is a client issue. 100 clients in a channel sending messages at this rate would each also have to be processing 1,000 messages per second! Whilst some modern browsers might be able to handle this it’s most probably not a good idea.

API SignalR

SignalR

SignalR component uses WebSocket as transport to connect to a SignalR server, if this transport is not supported, an error will be raised.
SignalR client component has a property called SignalR where you can set following data:

- **Hubs:** contains a list of hubs the client is subscribing to.
- **ProtocolVersion:** the version of the protocol used by the client, supports protocol versions from 1.2 to 1.5
- **UserAgent:** user agent used to connect to SignalR server.

Hubs Messages

Hubs API makes it possible to invoke server methods from the client and client methods from the server. The protocol used for persistent connection is not rich enough to allow expressing RPC (remote procedure call) semantics. It does not mean however that the protocol used for hub connections is completely different from the protocol used for persistent connections. Rather, the protocol used for hub connections is mostly an extension of the protocol for persistent connections.

When a client invokes a server method it no longer sends a free-flow string as it was for persistent connections. Instead, it sends a JSON string containing all necessary information needed to invoke the method. Here is a sample message a client would send to invoke a server method:

```
WriteData('{"H":"chathub","M":"Send","A":["Delphi Client","Test
message"],"I":0}');
```

The payload has the following properties:
I – invocation identifier – allows to match up responses with requests
H – the name of the hub
M – the name of the method
A – arguments (an array, can be empty if the method does not have any parameters)

The component has the following events:

OnSignalRConnect

When the client connects successfully to the server, this event is raised.

OnSignalRDisconnect

When the client is disconnected from the server, this event is raised.

OnSignalRError

When there is an error in WebSocket connection.

OnSignalRMessage

The protocol used for persistent connection is quite simple. Messages sent to the server are just raw strings. There isn't any specific format they have to be in. Messages sent to the client are more structured. The properties you can find in the message are as follows:

C – message id, present for all non-KeepAlive messages
M – an array containing actual data.

```
{"C":"d-9B7A6976-B,2|C,2","M":["Welcome!"]}
```

OnSignalRResult

When a server method is invoked the server returns a confirmation that the invocation has completed by sending the invocation id to the client and – if the method returned a value – the return value, or – if invoking the method failed – the error.
Here are sample results of a server method call:

```
{"I":"0"}
```

A server void method whose invocation identifier was "0" completed successfully.

```
{"I":"0", "R":42}
```

A server method returning a number whose invocation identifier was "0" completed successfully and returned the value 42.

```
{"I":"0", "E":"Error occurred"}
```

OnSignalRKeepAlive

This event is raised when a KeepAlive message is received from the server.

API Bittrex

Bittrex

The Bittrex WebSocket API is implemented using **SignalR**.
Bittrex component has a property called Bittrex where you can fill API Keys provided by Bittrex to get access to your account data.

Authenticate

Verifies a user's identity to the server and begins receiving account-level notifications. Needs an ApiKey and ApiSecret, which can be obtained in Bittrex user page.
Updates are received OnBittrexMessage event, where Callback is "OrderDelta" or "BalanceDelta".
JSON Order Response

```
{
    AccountUuid : Guid,
    Nonce       : int,
    Type        : int,
    Order:
    {
        Uuid              : guid,
        Id                : long,
        OrderUuid         : guid,
        Exchange          : string,
        OrderType         : string,
        Quantity          : decimal,
        QuantityRemaining : decimal,
        Limit             : decimal,
        CommissionPaid    : decimal,
        Price             : decimal,
        PricePerUnit      : decimal,
        Opened            : date,
        Closed            : date,
        IsOpen            : bool,
        CancelInitiated   : bool,
        ImmediateOrCancel : bool,
        IsConditional     : bool,
        Condition         : string,
        ConditionTarget   : decimal,
        Updated           : date
    }
}
```

QuerySummaryState

```
: '{' '    Nonce' ':' int '    Delta' ':' '    {' '        Uuid'
'         :' guid '        AccountId' '    :' int '        Currency'
'     :' string '        Balance' '      :' decimal
'        Available' '    :' decimal '        Pending' '      :'
decimal '        CryptoAddress' ':' string '        Requested' '    :'
bool '        Updated' '      :' date '        AutoSell' '     :' bool
'    ';">Allows
```

```
 the caller to retrieve the full order book for a specific market.
There
 is only one Parameter called MarketName, e.g. BTC-ETH
```

Updates are received **OnBittrexMessage** event, where Callback is "QueryExchangeState"

JSON Response

```
{
    MarketName : string,
    Nonce      : int,
    Buys:
    [
        {
            Quantity : decimal,
            Rate     : decimal
        }
    ],
    Sells:
    [
        {
            Quantity : decimal,
            Rate     : decimal
        }
    ],
    Fills:
    [
        {
            Id        : int,
            TimeStamp : date,
            Quantity  : decimal,
            Price     : decimal,
            Total     : decimal,
            FillType  : string,
            OrderType : string
        }
    ]
}
```

QuerySummaryState

Allows the caller to retrieve the full state for all markets.

Updates are received **OnBittrexMessage** event, where Callback is "QuerySummaryState"

JSON Response

```
{
    Nonce     : int,
```

```
    Summaries :
    [
        {
            MarketName     : string,
            High           : decimal,
            Low            : decimal,
            Volume         : decimal,
            Last           : decimal,
            BaseVolume     : decimal,
            TimeStamp      : date,
            Bid            : decimal,
            Ask            : decimal,
            OpenBuyOrders  : int,
            OpenSellOrders : int,
            PrevDay        : decimal,
            Created        : date
        }
    ]
}
```

SubscribeToExchangeDeltas

Allows the caller to receive real-time updates to the state of a single market. There is only one Parameter called MarketName, e.g. BTC-ETH

If user is subscribed to the feed, **OnBittrexSubscribed** event will be raised.

Updates are received **OnBittrexMessage** event, where Callback is "MarketDelta"

JSON Response

```
{
    MarketName : string,
    Nonce      : int,
    Buys:
    [
        {
            Type     : int,
            Rate     : decimal,
            Quantity : decimal
        }
    ],
    Sells:
    [
        {
            Type     : int,
            Rate     : decimal,
            Quantity : decimal
        }
    ],
    Fills:
```

```
    [
        {
            FillId    : int,
            OrderType : string,
            Rate      : decimal,
            Quantity  : decimal,
            TimeStamp : date
        }
    ]
}
```

SubscribeToSummaryDeltas

Allows the caller to receive real-time updates of the state of all markets.

If the user is subscribed to the feed, **OnBittrexSubscribed** event will be raised.

Updates are received **OnBittrexMessage** event, where Callback is "SummaryDelta"

JSON Response

```
{
    Nonce : int,
    Deltas :
    [
        {
            MarketName     : string,
            High           : decimal,
            Low            : decimal,
            Volume         : decimal,
            Last           : decimal,
            BaseVolume     : decimal,
            TimeStamp      : date,
            Bid            : decimal,
            Ask            : decimal,
            OpenBuyOrders  : int,
            OpenSellOrders : int,
            PrevDay        : decimal,
            Created        : date
        }
    ]
}
```

SubscribeToSummaryLiteDeltas

Allows the caller to receive real-time updates of the state of all markets but only *market name, the last price, and the base currency*

If user is subscribed to the feed, **OnBittrexSubscribed** event will be raised.

Updates are received **OnBittrexMessage** event, where Callback is "LiteSummaryDelta"

JSON Response

```
{
    Deltas :
    [
        {
            MarketName : string,
            Last       : decimal,
            BaseVolume : decimal
        }
    ]
}
```

API Binance

Binance

Binance is an international multi-language cryptocurrency exchange. It offers some APIs to access Binance data. The following APIs are supported:

1. **WebSocket**
2. **streams:** allows to subscribe to some methods and get data in
3. real-time. Events are pushed to clients by server to subscribers.
4. Uses WebSocket as protocol.

5. **UserData**
6. **stream:** subscribed clients get account details. Requires an
7. API key to authenticate and uses WebSocket as protocol.

8. **REST**
9. **API:** clients can request to server market and account data.
10. Requires an API Key and Secret to authenticate and uses HTTPs as protocol.

Properties

Binance API has 2 types of methods: public and private. Public methods can be accessed without authentication, example: get ticker prices. Only are only private and related to user data, those methods requires the use of Binance API keys.

- **ApiKey:**
- you can request a new api key in your binance account, just copy the
- value to this property.

- **ApiSecret:**
- API secret is only required for REST_API, websocket api only requires
- ApiKey for some methods.

- **HTTPLogOptions:**
- stores in a text file a log of HTTP requests

- **Enabled:**
- if enabled, will store all HTTP requests of WebSocket API.

- **FileName:**
- full path of filename where logs will be stored

- **REST:**
- stores in a text file a log of REST API requests

- **Enabled:**
- if enabled, will store all HTTP Requests of REST API.

- **FileName:**
- full path of filename where logs will be stored.

WebSocket Stream API

Base endpoint is wss://stream.binance.com:9443, client can subscribe / unsubscribe from events after a successful connection.

The following Subscription / Unsubscription methods are supported.

Method	Parameters	Description
AggregateTrades	Symbol	push trade information that is aggregated for a single taker order
Trades	Symbol	push raw trade information; each trade has a unique buyer and seller
KLine	Symbol, Interval	push updates to the current klines/candlestick every second, minute, hour...
MiniTicker	Symbol	24hr rolling window mini-ticker statistics. These are NOT the statistics of the UTC day, but a 24hr rolling window for the previous 24hrs.
AllMiniTickers		24hr rolling window mini-ticker statistics for all symbols that changed in an array. These are NOT the statistics of the UTC day, but a 24hr rolling window for the previous 24hrs. Note that only tickers that have changed will be present in the array.
Ticker	Symbol	24hr rolling window

		ticker statistics for a single symbol. These are NOT the statistics of the UTC day, but a 24hr rolling window for the previous 24hrs.
AllMarketTickers		24hr rolling window ticker statistics for all symbols that changed in an array. These are NOT the statistics of the UTC day, but a 24hr rolling window for the previous 24hrs. Note that only tickers that have changed will be present in the array.
BookTicker	Symbol	Pushes any update to the best bid or ask's price or quantity in real-time for a specified symbol.
AllBookTickers		Pushes any update to the best bid or ask's price or quantity in real-time for all symbols.
PartialBookDepth	Symbol, Depth	Top <levels> bids and asks, pushed every second. Valid <levels> are 5, 10, or 20.
DiffDepth	Symbol	Order book price and quantity depth updates used to locally manage an order book.

After a successful subcription / unsubscription, client receives a message about it, where id is the result of Subscribed / Unsubscribed method.

```
{
  "result": null,
  "id": 1
}
```

User Data Stream API

Requires a valid ApiKey obtained from your binance account, and ApiKey must be set in Binance.ApiKey property of component.

The following data is pushed to client every time there is a change. There is no need to subscribe to any method, this is done automatically if you set a valid ApiKey.

Method	Description
Account Update	Account state is updated with the outboundAccountInfo event.
Balance Update	Balance Update occurs during the following: • Deposits or withdrawals from the account • Transfer of funds between accounts (e.g. Spot to Margin)
Order Update	Orders are updated with the executionReport event.

REST API

The base endpoint is: https://api.binance.com. All endpoints return either a JSON object or array. Data is returned in ascending order. Oldest first, newest last.

Public API EndPoints

These endpoints can be accessed without any authorization.

General EndPoints

Method	Parameters	Description
Ping		Test connectivity to the Rest API.
GetServerTime		Test connectivity to the Rest API and get the current server time.
GetExchangeInformation		Current exchange trading rules and symbol information

Market Data EndPoints

Method	Parameters	Description
GetOrderBook	Symbol	Get Order Book.
GetTrades	Symbol	Get recent trades
GetHistoricalTrades	Symbol	Get older trades.
GetAggregateTrades	Symbol	Get compressed, aggregate trades. Trades that fill at the time, from the same order, with the same price will have the quantity aggregated.
GetKLines	Symbol, Interval	Kline/candlestick bars for a symbol. Klines are uniquely identified by their open time.
GetAveragePrice	Symbol	Current average price for a symbol.
Get24hrTicker	Symbol	24 hour rolling window price change statistics. Careful when

		accessing this with no symbol.
GetPriceTicker	Symbol	Latest price for a symbol or symbols.
GetBookTicker	Symbol	Best price/qty on the order book for a symbol or symbols.

Private API EndPoints

Requires an APIKey and APISecret to get authorized by server.

Account Data EndPoints

Method	Parameters	Description
NewOrder	Symbol, Side, Type	Send in a new order.
TestNewOrder	Symbol, Side, Type	Test new order creation and signature/recvWindow long. Creates and validates a new order but does not send it into the matching engine.
QueryOrder	Symbol	Check an order's status.
CancelOrder	Symbol	Cancel an active order.
GetOpenOrders		Get all open orders on a symbol. Careful when accessing this with no symbol.
GetAllOrders	Symbol	Get all account orders; active, canceled, or filled.
NewOCO	Symbol, Side, Quantity, Price, StopPrice	Send in a new OCO
CancelOCO	Symbol	Cancel an entire

		Order List
QueryOCO	Symbol	Retrieves a specific OCO based on provided optional parameters
GetAllOCO		Retrieves all OCO based on provided optional parameters
GetOpenOCO		Get All Open OCO.
GetAccountInformation		Get current account information.
GetAccountTradeList	Symbol	Get trades for a specific account and symbol.

Events

Binance Messages are received in TsgcWebSocketClient component, you can use the following events:

OnConnect

After a successful connection to Binance server.

OnDisconnect

After a disconnection from Binance server

OnMessage

Messages sent by server to client are handled in this event.

OnError

If there is any error in protocol, this event will be called.

OnException

If there is an unhandled exception, this event will be called.

Additionally, there is a specific event in Binance API Component, called **OnBinanceHTTPException**, which is raised every time there is an error calling an HTTP Request (REST API or WebSocket User Stream).

API Bitstamp

Bitstamp

Bitstamp is a bitcoin exchange based in Luxembourg. It allows trading between USD currency and bitcoin cryptocurrency. It allows USD, EUR, bitcoin, litecoin, ethereum, ripple or bitcoin cash deposits and withdrawals.
Supports latest WebSocket API V2.

Methods

- **SubscribeLiveTicker:** get live trades from currency selected. JSON data:

id	Trade unique ID.
amount	Trade amount.
amount_str	Trade amount represented in string format.
price	Trade price.
price_str	Trade price represented in string format.
type	Trade type (0 - buy; 1 - sell).
timestamp	Trade timestamp.
microtimestamp	Trade microtimestamp.
buy_order_id	Trade buy order ID.
sell_order_id	Trade sell order ID.

- **SubscribeLiveOrders:** get live orders from currency selected. JSON data:

id	Order ID.
amount	Order amount.
amount_str	Order amount represented in string format.

price	Order price.
price_str	Order price represented in string format.
order_type	Order type (0 - buy; 1 - sell).
datetime	Order datetime.
microtimestamp	Order action timestamp represented in microseconds.

- **SubscribeLiveOrderBook:** get live order book from currency selected. JSON data:

bids	List of top 100 bids.
asks	List of top 100 asks.
timestamp	Order book timestamp.
microtimestamp	Order book microtimestamp.

- **SubscribeLiveDetailOrderBook:** get live detail order book from currency selected. JSON data:

bids	List of top 100 bids [price, amount, order id].
asks	List of top 100 asks [price, amount, order id].
timestamp	Order book timestamp.
microtimestamp	Order book microtimestamp.

- **SubscribeLiveFullOrderBook:** get live full order book from currency selected. JSON data:

bids	List of changed bids since last broadcast.

asks	List of changed asks since last broadcast.
timestamp	Order book timestamp.
microtimestamp	Order book microtimestamp.

API Huobi

Huobi

Huobi is an international multi-language cryptocurrency exchange.

Methods

SubscribeKLine

K line data, including the opening price, closing price, highest price, lowest price, volume, turnover, number of transactions, etc. per unit time interval $period Optional values: { 1min, 5min, 15min, 30min, 60min, 4hour ,1day, 1mon, 1week, 1year }

```
     {


{
  "status": "ok",
  "rep": "market.btcusdt.kline.1min",
  "tick": [
    {
      "amount": 1.6206,
      "count":  3,
      "id":     1494465840,
      "open":   9887.00,
      "close":  9885.00,
      "low":    9885.00,
      "high":   9887.00,
      "vol":    16021.632026
    },
    {
      "amount": 2.2124,
      "count":  6,
      "id":     1494465900,
      "open":   9885.00,
      "close":  9880.00,
      "low":    9880.00,
      "high":   9885.00,
      "vol":    21859.023500
    }
  ]
}
```

SubscribeMarketDepth

Handbook depth, according to different step aggregation, buy one, buy two, buy three, and sell one, sell two, sell three, etc. type Optional value: { step0, step1, step2, step3, step4, step5, percent10 } (combination depth 0-5); when step0, no depth is merged

```
{
  "ch": "market.btcusdt.depth.step0",
  "ts": 1489474082831,
  "tick": {
```

```
    "bids": [
    [9999.3900,0.0098], // [price, amount]
    [9992.5947,0.0560],
    // more Market Depth data here
    ]
    "asks": [
    [10010.9800,0.0099]
    [10011.3900,2.0000]
    //more data here
    ]
  }
}
```

SubscribeTradeDetail

Transaction record, including transaction price, volume, direction of transaction, etc.

```
{
  "ch": "market.btcusdt.trade.detail",
  "ts": 1489474082831,
  "tick": {
        "id": 14650745135,
        "ts": 1533265950234,
        "data": [
            {
                "amount": 0.0099,
                "ts": 1533265950234,
                "id": 146507451359183894799,
                "price": 401.74,
                "direction": "buy"
            },
            // more Trade Detail data here
        ]
    }

  ]
  }
}
```

SubscribeMarketDetail

Last 24 hours of volume, turnover, opening price, closing price, highest price, lowest price, number of transactions, etc.

```
{
  "rep": "market.btcusdt.detail",
  "status": "ok",
  "id": "id12",
  "tick": {
    "amount": 12224.2922,
    "open":   9790.52,
    "close":  10195.00,
    "high":   10300.00,
    "ts":     1494496390000,
    "id":     1494496390,
```

```
    "count":  15195,
    "low":    9657.00,
    "vol":    121906001.754751
  }
}
```

SubscribeMarketTickers

Information on the daily K line, the last 24 hours of trading, etc.

Events

OnHuobiSubscribed: event called after a successful subscription.

OnHuobiUnSubscribed: event called after a successful unsubscription.

OnHuobiUpdate: every time there is an update in data (kline, market depth...) this event is called.

OnHuobiError: if there is an error in Huobi API, this event will provide information about error.

API Cex

Cex

WebSocket API allows getting real-time notifications without sending extra requests, making it a faster way to obtain data from the exchange
Cex component has a property called Cex where you can fill API Keys provided by Cex to get access to your account data.

Message encoding

- All messages are encoded in JSON format.
- Prices are presented as strings to avoid rounding errors at JSON parsing on client side
- Compression of WebSocket frames is not supported by the server.
- Time is presented as integer UNIX timestamp in seconds.

Authentication

To get access to CEX.IO WebSocket data, you should be authorized.

- Log in to CEX.IO account.
- Go to https://cex.io/trade/profile#/api page.
- Select the type of required permissions.
- Click "Generate Key" button and save your secret key, as it will become inaccessible after activation.
- Activate your key.

Connectivity

- If a connected Socket is inactive for 15 seconds, CEX.IO server will send a PING message.
- Only server can be an Initiator of PING request.
- The server sends ping only to the authenticated user.
- The user has to respond with a PONG message. Otherwise, the WebSocket will be DISCONNECTED. This is handled automatically by the library.
- For the authenticated user, in case there is no notification or ping from the server within 15 seconds, it would be safer to send a request like 'ticker' or 'get-balance' and receive a response, in order to ensure connectivity and authentication.

Public Channels

These channels don't require to Authenticate before. Responses from the server are received by OnCexMessage event.

- **SubscribeTickers:** Ticker feed with only price of transaction made on all pairs (deprecated)

```
{
    "e": "tick",
    "data": {
        "symbol1": "BTC",
        "symbol2": "USD",
        "price": "428.0123"
    }
}
```

- **SubscribeChart:** OHLCV chart feeds with Open, High, Low, Close, Volume numbers (deprecated)

```
{
    'e': 'ohlcv24',
    'pair': 'BTC:USD',
    'data': [
        '418.2936',
        '420.277',
        '412.09',
        '416.9778',
        '201451078368'
    ]
}
```

- **Subscribe Pair:** Market Depth feed (deprecated)

```
{
    'e': 'md_groupped',
    'data': {
        'pair': 'BTC:USD',
        'id': 11296131,
        'sell': {
            '427.5000': 1000000,
            '480.0000': 263544334,
            ...
        },
        'buy': {
            '385.0000': 3630000,
            '390.0000': 1452458642,
            ... 400+ pairs togather with 'sell' pairs
        }
    }
}
```

- **Subscribe Pair:** Order Book feed (deprecated)

```
{
    'e': 'md',
    'data': {
        'pair': 'BTC:USD',
        'buy_total': 63221099,
        'sell_total': 112430315118,
        'id': 11296131,
        'sell': [
            [426.45, 10000000],
            [426.5, 66088429300],
            [427, 1000000],
            ... 50 pairs overaall
        ],
        'buy': [
            [423.3, 4130702],
            [423.2701, 10641168],
            [423.2671, 1000000],
            ... 50 pairs overaall
        ]
    }
}
```

Private Channels

To access these channels, first call Authenticate method. Responses from the server are received OnCexMessage event.

GetTicker

```
{
    "e": "ticker",
    "data": {
        "timestamp": "1471427037",
        "low": "290",
        "high": "290",
        "last": "290",
        "volume": "0.02062068",
        "volume30d": "14.38062068",
        "bid": 240,
        "ask": 290,
        "pair": [
            "BTC",
            "USD"
        ]
    },
    "oid": "1471427036908_1_ticker",
    "ok": "ok"
}
```

GetBalance

```
{
    "e": "get-balance",
```

```
    "data": {
           "balance": {
            'LTC': '10.00000000',
            'USD': '1024.00',
            'RUB': '35087.98',
            'EUR': '217.53',
            'GHS': '10.00000000',
            'BTC': '9.00000000'
        },
           "obalance": {
              'BTC': '0.12000000',
              'USD': "512.00",
           },
       },
       "time": 1435927928597
    "oid": "1435927928274_2_get-balance",
    "ok": "ok"
}
```

SubscribeOrderBook

```
{
"e": "order-book-subscibe",
"data": {
   "timestamp": 1435927929,
   "bids": [
      [
         241.947,
         155.91626
      ],
      [
         241,
         981.1255
      ],
   ],
   "asks": [
      [
         241.95,
         15.4613
      ],
      [
         241.99,
         17.3303
      ],
   ],
   "pair": "BTC:USD",
   "id": 67809
},
"oid": "1435927928274_5_order-book-subscribe",
"ok": "ok"
}
```

UnSubscribeOrderBook

```
{
"e": "order-book-unsubscribe",
"data": {
```

```
   "pair": "BTC:USD"
},
"oid": "1435927928274_4_order-book-unsubscribe",
"ok": "ok"
}
```

GetOpenOrders

```
{
"e": "open-orders",
"data": [
   {
      "id": "2477098",
      "time": "1435927928618",
      "type": "buy",
      "price": "241.9477",
      "amount": "0.02000000",
      "pending": "0.02000000"
   },
   {
      "id": "2477101",
      "time": "1435927928634",
      "type": "sell",
      "price": "241.9493",
      "amount": "0.02000000",
      "pending": "0.02000000"
   }
],
"oid": "1435927928274_9_open-orders",
"ok": "ok"
}
```

PlaceOrder

```
{
"e": "place-order",
"data": {
   "complete": false,
   "id": "2477098",
   "time": 1435927928618,
   "pending": "0.02000000",
   "amount": "0.02000000",
   "type": "buy",
   "price": "241.9477"
},
"oid": "1435927928274_7_place-order",
"ok": "ok"
}
```

CancelReplaceOrder

```
{
```

```
"e": "cancel-replace-order",
"data": {
   "complete": false,
   "id": "2689009",
   "time": 1443464955904,
   "pending": "0.04000000",
   "amount": "0.04000000",
   "type": "buy",
   "price": "243.25"
},
"oid": "1443464955209_16_cancel-replace-order",
"ok": "ok"
}
```


GetOrderRequest

In CEX.IO system, orders can be present in the trade engine or in an archive database. There can be time periods (~2 seconds or more), when the order is done/cancelled, but still not moved to the archive database. That means you cannot see it using calls: archived-orders/open-orders. This call allows getting order information in any case. Responses can have different format depending on orders location.


```
{
"e": "get-order",
"data": {
   "user": "XXX",
   "type": "buy",
   "symbol1": "BTC",
   "symbol2": "USD",
   "amount": "0.02000000",
   "remains": "0.02000000",
   "price": "50.75",
   "time": 1450214742160,
   "tradingFeeStrategy": "fixedFee",
   "tradingFeeBuy": "5",
   "tradingFeeSell": "5",
   "tradingFeeUserVolumeAmount": "nil",
   "a:USD:c": "1.08",
   "a:USD:s": "1.08",
   "a:USD:d": "0.00",
   "status": "a",
   "orderId": "5582060"
},
"oid": "1450214742135_10_get-order",
"ok": "ok"
}
```


CancelOrderRequest


```
{
"e": "cancel-order",
"data": {
   "order_id": "2477098"
   "time": 1443468122895
},
"oid": "1435927928274_12_cancel-order",
"ok": "ok"
```

```
}
```

GetArchivedOrders

```
{
"e": "archived-orders",
"data": [
   {
       "type": "buy",
       "symbol1": "BTC",
       "symbol2": "USD",
       "amount": 0,
       "amount2": 5000,
       "remains": 0,
       "time": "2015-04-17T10:46:27.971Z",
       "tradingFeeBuy": "2",
       "tradingFeeSell": "2",
       "ta:USD": "49.00",
       "fa:USD": "0.98",
       "orderId": "2340298",
       "status": "d",
       "a:BTC:cds": "0.18151851",
       "a:USD:cds": "50.00",
       "f:USD:cds": "0.98"
   },
   {
       "type": "buy",
       "symbol1": "BTC",
       "symbol2": "USD",
       "amount": 0,
       "amount2": 10000,
       "remains": 0,
       "time": "2015-04-08T15:46:04.651Z",
       "tradingFeeBuy": "2.99",
       "tradingFeeSell": "2.99",
       "ta:USD": "97.08",
       "fa:USD": "2.91",
       "orderId": "2265315",
       "status": "d",
       "a:BTC:cds": "0.39869578",
       "a:USD:cds": "100.00",
       "f:USD:cds": "2.91"
    }
],
"oid": "1435927928274    15_archived-orders",
"ok": "ok"
}
```

OpenPosition

```
{
    "e": "open-position",
    "oid": "1435927928274_7_open-position",
    "data": {
        'amount': '1',
        'symbol': 'BTC',
        "pair": [
```

```
            "BTC",
            "USD"
        ],
        'leverage': '2',
        'ptype': 'long',
        'anySlippage': 'true',
        'eoprice': '650.3232',
        'stopLossPrice': '600.3232'
    }
}
```

GetPosition

```
{
  "e": "get_position",
  "ok": "ok",
  "data": {
    "user": "ud100036721",
    "pair": "BTC:USD",
    "amount": "1.00000000",
    "symbol": "BTC",
    "msymbol": "USD",
    "omamount": "1528.77",
    "lsymbol": "USD",
    "lamount": "3057.53",
    "slamount": "3380.11",
    "leverage": "3",
    "stopLossPrice": "3380.1031",
    "dfl": "3380.10310000",
    "flPrice": "3057.53333333",
    "otime": 1513002370342,
    "psymbol": "BTC",
    "ptype": "long",
    "ofee": "10",
    "pfee": "10",
    "cfee": "10",
    "tfeeAmount": "152.88",
    "rinterval": "14400000",
    "okind": "Manual",
    "a:BTC:c": "1.00000000",
    "a:BTC:s": "1.00000000",
    "oorder": "89101551",
    "pamount": "1.00000000",
    "lremains": "3057.53",
    "slremains": "3380.11",
    "oprice": "4586.3000",
    "status": "a",
    "id": "125531",
    "a:USD:cds": "4739.18"
  }
}
```

GetOpenPositions

```
{
    'e': 'open_positions',
    "oid": "1435927928256_7_open-positions",
```

```
    'ok': 'ok',
    'data': [
        {
            'user': 'ud100036721',
            'id': '104102',
            'otime': 1475602208467,
            'symbol': 'BTC',
            'amount': '1.00000000',
            'leverage': '2',
            'ptype': 'long',
            'psymbol': 'BTC',
            'msymbol': 'USD',
            'lsymbol': 'USD',
            'pair': 'BTC:USD',
            'oprice': '607.5000'
            'stopLossPrice': '520.3232',
            'ofee': '1',
            'pfee': '3',
            'cfee': '4',
            'tfeeAmount': '3.04',
            'pamount': '1.00000000',
            'omamount': '303.75',
            'lamount': '303.75',
            'oorder': '34106774',
            'rinterval': '14400000',
            'dfl': '520.32320000',
            'slamount': '520.33',
            'slremains': '520.33',
            'lremains': '303.75',
            'flPrice': '303.75000000',
            'a:BTC:c': '1.00000000',
            'a:BTC:s': '1.00000000',
            'a:USD:cds': '610.54',
        },
        ...
    ]
}
```

ClosePosition

```
{
    'e': 'close_position',
    "oid": "1435927928364_7_close-position",
    'ok': 'ok',
    'data': {
        'id': 104034,
        'ctime': 1475484981063,
        'ptype': 'long',
        'msymbol': 'USD'
        'pair': {
            'symbol1': 'BTC',
            'symbol2': 'USD'
        }
        'price': '607.1700',
        'profit': '-12.48',
    }
}
```

API Bitmex

Bitmex

Is a cryptocurrency exchange and derivative trading platform.

Methods

Subscribe / Unsubscribe

BitMEX allows subscribing to real-time data. This access is not rate-limited once connected and is the best way to get the most up-to-date data to your programs. In some topics, you can pass a Symbol to filter events by symbol, example: trades, quotes...

The following subscription topics are available without authentication:

- **btmAnnouncement**: Site Announcements
- **btmChat**: Trollbox chat
- **btmConnected**: Statistics of connected users/bots
- **btmFunding**: Updates of swap funding rates. Sent every funding interval (usually 8hrs)
- **btmInstrument**: Instrument updates including turnover and bid/ask
- **btmInsurance**: Daily Insurance Fund updates
- **btmLiquidation**: Liquidation orders as they're entered into the book
- **btmOrderBookL2_25**: Top 25 levels of level 2 order book
- **btmOrderBookL2**: Full level 2 order book
- **btmOrderBook10**: Top 10 levels using traditional full book push
- **btmPublicNotifications**: System-wide notifications (used for short-lived messages)
- **btmQuote**: Top level of the book
- **btmQuoteBin1m**: 1-minute quote bins
- **btmQuoteBin5m**: 5-minute quote bins
- **btmQuoteBin1h**: 1-hour quote bins
- **btmQuoteBin1d**: 1-day quote bins
- **btmSettlement**: Settlements
- **btmTrade**: Live trades
- **btmTradeBin1m**: 1-minute trade bins
- **btmTradeBin5m**: 5-minute trade bins
- **btmTradeBin1h**:1-hour trade bins
- **btmTradeBin1d**: 1-day trade bins

The following subjects require authentication:

- **btmAffiliate**: Affiliate status, such as total referred users & payout %
- **btmExecution**: Individual executions; can be multiple per order
- **btmOrder**: Live updates on your orders
- **btmMargin**: Updates on your current account balance and margin requirements
- **btmPosition**: Updates on your positions
- **btmPrivateNotifications**: Individual notifications - currently not used
- **btmTransact**: Deposit/Withdrawal updates
- **btmWallet**: Bitcoin address balance data, including total deposits & withdrawals

Example of messages received:


```
{
      "table":"orderBookL2_25",
      "keys":["symbol","id","side"],
      "types":{"id":"long","price":"float","side":"symbol","size":"lon
g","symbol":"symbol"}
      "foreignKeys":{"side":"side","symbol":"instrument"},
      "attributes":{"id":"sorted","symbol":"grouped"},
      "action":"partial",
      "data":[
        {"symbol":"XBTUSD","id":17999992000,"side":"Sell","size":100,"
price":80},
        {"symbol":"XBTUSD","id":17999993000,"side":"Sell","size":20,"p
rice":70},
        {"symbol":"XBTUSD","id":17999994000,"side":"Sell","size":10,"p
rice":60},
        {"symbol":"XBTUSD","id":17999995000,"side":"Buy","size":10,"pr
ice":50},
        {"symbol":"XBTUSD","id":17999996000,"side":"Buy","size":20,"pr
ice":40},
        {"symbol":"XBTUSD","id":17999997000,"side":"Buy","size":100,"p
rice":30}
      ]
}

{
      "table":"orderBookL2_25",
      "action":"update",
      "data":[
        {"symbol":"XBTUSD","id":17999995000,"side":"Buy","size":5}
      ]
    }
{
      "table":"orderBookL2_25",
      "action":"delete",
      "data":[
        {"symbol":"XBTUSD","id":17999995000,"side":"Buy"}
      ]
}
{
      "table":"orderBookL2_25",
      "action":"insert",
      "data":[
        {"symbol":"XBTUSD","id":17999995500,"side":"Buy","size":10,"pr
ice":45},
      ]
}
```


Authentication

If you wish to subscribe to user-locked streams, you must authenticate first. Note that invalid authentication will close the connection.

BitMEX API usage requires an API Key.

Permanent API Keys can be locked to IP address ranges and revoked at will without compromising your main credentials. They also do not require renewal.

To use API Key auth, you must generate an API Key in your account.

Cal method **Authenticate** before subscribe to any Authenticated Topic.

Events

```
// OnBitmexConnect
// after client successfully connects to the server, server sends to
client a message to confirm connection to the server.

procedure OnBitmexConnect(Sender: TObject; const aMessage: string);
begin
  Log('#Bitmex Connected: ' + aMessage);
end;

// OnBitmexSubscribed
// event called after a successful subscription.

procedure OnBitmexSubscribed(Sender: TObject; const aChannel: string);
begin
  Log('Bitmex Subscribed: ' + aChannel);
end;

// OnBitmexUnsubscribed
// event called after a successful unsubscription.

procedure OnBitmexUnsubscribed(Sender: TObject; const aChannel:
string);
begin
  Log('Bitmex Subscribed: ' + aChannel);
end;

// OnBitmexAuthenticated
// after the client has authenticated against the server using ApiKey
and ApiSecret, the client receives a message which confirms
authentication.

procedure OnBitmexAuthenticated(Sender: TObject);
begin
  Log('#Bitmex Authenticated');
end;

// OnBitmexMessage
// all updates from subscribed topics, will be notified using this
event. You can know which Topic is, accessing to aTopic parameter.

procedure OnBitmexMessage(Sender: TObject; const aTopic:
TwsBitmexTopics; const aMessage: string);
begin
  Log('Bitmex Message: ' + aMessage);
end;

// OnBitmexError
// if there is an error in Bitmex API, this event will provide
information about error.
```

```
procedure OnBitmexError(Sender: TObject; const aMessage: string);
begin
  Log('Bitmex Error: ' + aMessage);
end;
```

API SignalRCore

SignalRCore

ASP.NET Core SignalR is an open-source library that simplifies adding real-time web functionality to apps. Real-time web functionality enables server-side code to push content to clients instantly.

Good candidates for SignalR:

- Apps that require high-frequency updates from the server. Examples are gaming, social networks, voting, auction, maps, and GPS apps.
- Dashboards and monitoring apps. Examples include company dashboards, instant sales updates, or travel alerts.
- Collaborative apps. Whiteboard apps and team meeting software are examples of collaborative apps.
- Apps that require notifications. Social networks, email, chat, games, travel alerts, and many other apps use notifications.

SignalRCore sgcWebSockets component uses WebSocket as transport to connect to a SignalRCore server, if this transport is not supported, an error will be raised.

Hubs

SignalRCore uses hubs to communicate between clients and servers. SignalRCore provides 2 hub protocols: text protocol based on JSON and binary protocol based on MessagePack. The sgcWebSockets component only implements JSON text protocol to communicate with SignalRCore servers.
To configure which Hub client will use, just set in **SignalRCore/Hub** property the name of the Hub before the client connects to the server.

Connection

When a client opens a new connection to the server, sends a request message which contains format protocol and version. sgcWebSockets always sends format protocol as JSON. The server will reply with an error if the protocol is not supported by the server, this error can be handled using **OnSignalRCoreError** event, and if the connection is successful, **OnSignalRCoreConnect** event will be called.

When a client connects to a SignalRCore server, it can send a ConnectionId which identifies client between sessions, so if you get a disconnection client can reconnect to server passing same prior connection id. In order to get a new connection id, just connect normally to the server and you can know ConnectionId using **OnBeforeConnectEvent**. If you want to reconnect to the server and pass a prior connection id, use **ReConnect** method and pass **ConnectionId** as a parameter.

SignalRCore Protocol

The SignalR Protocol is a protocol for two-way RPC over any Message-based transport. Either party in the connection may invoke procedures on the other party, and procedures can return zero or more results or an error. Example: the client can request a method from the server and

server can request a method to the client. There are the following messages exchanged between server and clients:

- **HandshakeRequest:** the client sends to the server to agree on the message format.
- **HandshakeResponse:** server replies to the client an acknowledgement of the previous HandshakeRequest message. Contains an error if the handshake failed.
- **Close:** called by client or server when a connection is closed. Contains an error if the connection was closed because of an error.
- **Invocation:** client or server sends a message to another peer to invoke a method with arguments or not.
- **StreamInvocation:** client or server sends a message to another peer to invoke a streaming method with arguments or not. The Response will be split into different items.
- **StreamItem:** is a response from a previous StreamInvocation.
- **Completion:** means a previous invocation or StreamInvocation has been completed. Can contain a result if the process has been successful or an error if there is some error.
- **CancelInvocation:** cancel a previous StreamInvocation request.
- **Ping:** is a message to check if the connection is still alive.

Authorization

Authentication can be enabled to associate a user with each connection and filter which users can access to resources. Authentication is implemented using Bearer Tokens, client provide an access token and server validates this token and uses it to identify then user.
In standard Web APIs, bearer tokens are sent in an HTTP Header, but when using websockets, token is transmitted as a query string parameter.
The following methods are supported:

srcaRequestToken

If Authentication is enabled, the flow is:

1. First tries to get a valid token from server. Opens an HTTP connection against Authentication.RequestToken.URL and do a POST using User and Password data.
2. If previous is successful, a token is returned. If not, an error is returned.
3. If token is returned, then opens a new HTTP connection to negotiate a new connection. Here, token is passed as an HTTP Header.
4. If previous is successful, opens a websocket connection and pass token as query string parameter.

- **Authentication.Enabled:** if active, authorization will be used before a websocket connection is established.
- **Authentication.Username:** the username provided to server to authenticate.
- **Authentication.Password:** the secret word provided to server to authenticate.
- **Authentication.RequestToken.PostFieldUsername:** name of field to transmit username (depends of configuration, check http javascript page to see which name is used).
- **Authentication.RequestToken.PostFieldPassword:** name of field to transmit password (depends of configuration, check http javascript page to see which name is used).
- **Authentication.RequestToken.URL:** url where token is requested.
- **Authentication.RequestToken.QueryFieldToken:** name of query string parameter using in websocket connection.

srcaSetToken

Here, you pass token directly to SignalRCore server (because token has been obtained from another server).

- **Authentication.Enabled:** if active, authorization will be used before a websocket connection is established.
- **Authentication.SetToken.Token:** token value obtained.

Communication between Client and Server

```
// There are three kinds of interactions between server and clients:

// Invocations: the Caller sends a message to the Callee and expects a
message indicating that the invocation
// has been completed and optionally a result of the invocation

// Example: client invokes SendMessage method and passes as parameters
user name and text message. Sends an Invocation Id to
// get a result message from the server.

SignalRCore.Invoke('SendMessage', ['John', 'Hello All.'], 'id-
000001');

procedure OnSignalRCoreCompletion(Sender: TObject; Completion:
TSignalRCore_Completion);
begin
  if Completion.Error  '' then
    ShowMessage('Something goes wrong.')
  else
    ShowMessage('Invocation Successful!');
end;

//Non-Blocking Invocations: the Caller sends a message to the Callee
and does not expect any further messages for this invocation.
// Invocations can be sent without an Invocation ID value. This
indicates that the invocation is "non-blocking".

// Example: client invokes SendMessage method and passes as parameters
user name and text message.
// The client doesn't expect any response from the server about the
result of the invocation.

SignalRCore.Invoke('SendMessage', ['John', 'Hello All.']);

// Streaming Invocations: the Caller sends a message to the Callee and
expects one or more results returned by the Callee followed
// by a message indicating the end of invocation.
```

```
// Example: client invokes Counter method and requests 10 numbers with
an interval of 500 milliseconds.

SignalRCore.InvokeStream('Counter', [10, 500], 'id-000002');

procedure OnSignalRCoreStreamItem(Sender: TObject; StreamItem:
TSignalRCore_StreamItem; var Cancel: Boolean);
begin
  DoLog('#stream item: ' + StreamItem.Item);
end;

procedure OnSignalRCoreCompletion(Sender: TObject; Completion:
TSignalRCore_Completion);
begin
  if Completion.Error  '' then
    ShowMessage('Something goes wrong.')
  else
    ShowMessage('Invocation Successful!');
end;
```

Invocations

```
// In order to perform a single invocation, the Caller follows the
following basic flow:

procedure Invoke(const aTarget: String; const aArguments: Array of
Const; const aInvocationId: String = '');
procedure InvokeStream(const aTarget: String; const aArguments: Array
of Const; const aInvocationId: String);

// Allocate a unique Invocation ID value (arbitrary string, chosen by
the Caller) to represent the invocation.
// Call Invoke or InvokeStream method containing the Target being
invoked, Arguments and InvocationId (if you don't send InvocationId,
you won't get completion result).
// If the Invocation is marked as non-blocking (see "Non-Blocking
Invocations" below), stop here and immediately yield back to the
application.
// Handle StreamItem or Completion message with a matching Invocation
ID.

SignalRCore.InvokeStream('Counter', [10, 500], 'id-000002');

procedure OnSignalRCoreStreamItem(Sender: TObject; StreamItem:
TSignalRCore_StreamItem; var Cancel: Boolean);
begin
  if StreamItem.InvocationId = 'id-000002' then
    DoLog('#stream item: ' + StreamItem.Item);
end;

procedure OnSignalRCoreCompletion(Sender: TObject; Completion:
TSignalRCore_Completion);
begin
  if StreamItem.InvocationId = 'id-000002' then
  begin
    if Completion.Error  '' then
      ShowMessage('Something goes wrong.')
    else
      ShowMessage('Invocation Successful!');
```

```
  end;
end;


//You can call a single invocation and wait for completion.

function InvokeAndWait(const aTarget: String; aArguments: Array of
Const; aInvocationId: String; out Completion: TSignalRCore_Completion;
  const aTimeout: Integer = 10000): Boolean;
function InvokeStreamAndWait(const aTarget: String; const aArguments:
Array of Const; const aInvocationId: String;
  out Completion: TSignalRCore_Completion; const aTimeout: Integer =
10000): Boolean;

// Allocate a unique Invocation ID value (arbitrary string, chosen by
the Caller) to represent the invocation.
// Call InvokeAndWait or InvokeStreamAndWait method containing the
Target being invoked, Arguments and InvocationId
// The program will wait till completion event is called or Time out
has been exceeded.

var
  oCompletion: TSignalRCore_Completion;
begin
  if SignalRCore.InvokeStreamAndWait('Counter', [10, 500], 'id-
000002', oCompletion) then
    DoLog('#invoke stream ok: ' + oCompletion.Result)
  else
    DoLog('#invocke stream error: ' + oCompletion.Error);


procedure OnSignalRCoreStreamItem(Sender: TObject; StreamItem:
TSignalRCore_StreamItem; var Cancel: Boolean);
begin
  if StreamItem.InvocationId = 'id-000002' then
    DoLog('#stream item: ' + StreamItem.Item);
end;
```

Cancel Invocation

```
// If the client wants to stop receiving StreamItem messages before
the Server sends a Completion message, the client can send a
CancelInvocation message
// with the same InvocationId used for the StreamInvocation message
that started the stream.


procedure OnSignalRCoreStreamItem(Sender: TObject; StreamItem:
SignalRCore_StreamItem; var Cancel: Boolean);
begin
  if StreamItem.InvocationId = 'id-000002' then
    Cancel := True;
end;
```

Completion and Results

```
// An Invocation is only considered completed when the Completion
message is received. If the client receives an Invocation from the
server,
// OnSignalRCoreInvocation event will be called.

procedure OnSignalRCoreInvocation(Sender: TObject; Invocation:
TSignalRCore_Invocation);
begin
  if Invocation.Target = 'SendMessage' then
    ... your code here ...
end;

// Once invocation is completed, call Completion method to inform
server invocation is finished.

// If result is successful, then call CompletionResult method:

SignalRCore.CompletionResult('id-000002', 'ok');

// If not, then call CompletionError method:

SignalRCore.CompletionError('id-000002', 'Error processing
invocation.');
```

Close Connection

```
// Sent by the client when a connection is closed. Contains an error
reason if the connection was closed because of an error.

SignalRCore.Close('Unexpected message').

// If the server close connection by any reason, OnSignalRCoreClose
event will be called.

procedure OnSignalRCoreClose(Sender: TObject; Close:
TSignalRCore_Close);
begin
  DoLog('#closed: ' + Close.Error);
end;
```

Ping

```
// The SignalR Hub protocol supports "Keep Alive" messages used to
ensure that the underlying transport connection remains active. These
messages help ensure:

// Proxies don't close the underlying connection during idle times
(when few messages are being sent)
// If the underlying connection is dropped without being terminated
gracefully, the application is informed as quickly as possible.
```

```
// Keep alive behaviour is achieved calling Ping method or enabling
HeartBeat on WebSocket client.
// If the server sends a ping to the client, the client will send
automatically a response and OnSignalRCoreKeepAlive event will be
called.

procedure OnSignalRCoreKeepAlive(Sender: TObject);
begin
  DoLog('#keepalive');
end;
```

API Kraken

Kraken

Overview

WebSockets API offers real-time market data updates. WebSockets is a bidirectional protocol offering fastest real-time data, helping you build real-time applications. The public message types presented below do not require authentication. Private-data messages messages can be subscribed on a separate authenticated endpoint.

Kraken offers a REST API too with Public market data and Private user data (which requires an authentication).

Configuration

Private API requires to get create an API from your Kraken account.
Kraken allows Test environment on WebSocket protocol, enable Beta property from Kraken Property to use this beta feature.

APIs supported

- WebSockets Public API: connects to a public WebSocket server.
- WebSockets Private API: connects to a private WebSocket server and requires an API Key and API Secret to Authenticate against server.
- REST Public API: connects to a public REST server.
- REST Private API: connects to a public REST server and requires an API Key and API Secret to Authenticate against server.

Kraken Examples

How Connect to Public WebSocket Server

```
oClient := TsgcWebSocketClient.Create(nil);
oKraken := TsgcWSAPI_Kraken.Create(nil);
oKraken.Client := oClient;
oClient.Active := True;
```

How Connect to Private WebSocket Server

```
oClient := TsgcWebSocketClient.Create(nil);
oKraken := TsgcWSAPI_Kraken.Create(nil);
oKraken.Kraken.ApiKey := 'your api key';
oKraken.Kraken.ApiSecret := 'your api secret';
oKraken.Client := oClient;
oClient.Active := True;
```

How Get Ticker from REST API

```
oClient := TsgcWebSocketClient.Create(nil);
oKraken := TsgcWSAPI_Kraken.Create(nil);
oKraken.Client := oClient;
ShowMessage(oKraken.GetTicker(['XBTUSD']));
```

How Get Account Balance from REST API

```
oClient := TsgcWebSocketClient.Create(nil);
oKraken := TsgcWSAPI_Kraken.Create(nil);
oKraken.Kraken.ApiKey := 'your api key';
oKraken.Kraken.ApiSecret := 'your api secret';
oKraken.Client := oClient;
ShowMessage(oKraken.GetAccountBalance());
```

Kraken

API Kraken | WebSockets Public API

Connection
URL: wss://ws.kraken.com

Once the socket is open you can subscribe to a public channel by sending a subscribe request message.

General Considerations

- All messages sent and received via WebSockets are encoded in JSON format
- All floating point fields (including timestamps) are quoted to preserve precision.
- Format of each tradeable pair is A/B, where A and B are ISO 4217-A3 for standardized assets and popular unique symbol if not standardized.
- Timestamps should not be considered unique and not be considered as aliases for transaction ids. Also, the granularity of timestamps is not representative of transaction rates.

Supported Pairs
ADA/CAD, ADA/ETH, ADA/EUR, ADA/USD, ADA/XBT, ATOM/CAD, ATOM/ETH, ATOM/EUR, ATOM/USD, ATOM/XBT, BCH/EUR, BCH/USD, BCH/XBT, DASH/EUR, DASH/USD, DASH/XBT, EOS/ETH, EOS/EUR, EOS/USD, EOS/XBT, GNO/ETH, GNO/EUR, GNO/USD, GNO/XBT, QTUM/CAD, QTUM/ETH, QTUM/EUR, QTUM/USD, QTUM/XBT, USDT/USD, ETC/ETH, ETC/XBT, ETC/EUR, ETC/USD, ETH/XBT, ETH/CAD, ETH/EUR, ETH/GBP, ETH/JPY, ETH/USD, LTC/XBT, LTC/EUR, LTC/USD, MLN/ETH, MLN/XBT, REP/ETH, REP/XBT, REP/EUR, REP/USD, STR/EUR, STR/USD, XBT/CAD, XBT/EUR, XBT/GBP, XBT/JPY, XBT/USD, BTC/CAD, BTC/EUR, BTC/GBP, BTC/JPY, BTC/USD, XDG/XBT, XLM/XBT, DOGE/XBT, STR/XBT, XLM/EUR, XLM/USD, XMR/XBT, XMR/EUR, XMR/USD, XRP/XBT, XRP/CAD, XRP/EUR, XRP/JPY, XRP/USD, ZEC/XBT, ZEC/EUR, ZEC/JPY, ZEC/USD, XTZ/CAD, XTZ/ETH, XTZ/EUR, XTZ/USD, XTZ/XBT

Methods
Ping
Client can ping server to determine whether connection is alive, server responds with pong. This is an application level ping as opposed to default ping in WebSockets standard which is server initiated
Ticker
Ticker information includes best ask and best bid prices, 24hr volume, last trade price, volume weighted average price, etc for a given currency pair. A ticker message is published every time a trade or a group of trade happens.
Subscribe to a ticker calling SubscribeTicker method:

```
SubscribeTicker(['XBT/USD']);
```

If subscription is successful, **OnKrakenSubscribed** event will be called:

```
procedure OnKrakenSubscribed(Sender: TObject;ChannelId: Integer; Pair,
Subscription, ChannelName: string; ReqID:Integer);
begin
  DoLog('#subscribed: ' + Subscription + ' ' + Pair + ' ' +
ChannelName);
end;
```

UnSubscribe calling UnSubscribeTicker method:

```
UnSubscribeTicker(['XBT/USD']);
```
If unsubscription is successful, OnKrakenUnSubscribed event will be called:

```
procedure OnKrakenUnSubscribed(Sender: TObject; ChannelId: Integer;
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#unsubscribed: ' + Subscription + ' ' + Pair);
end;
```
If there is an error while trying to subscribe / unsubscribe, OnKrakenSubscriptionError event will be called.

```
procedure OnKrakenSubscriptionError(Sender: TObject; ErrorMessage,
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#subscription error: ' + ErrorMessage);
end;
```
Ticker updates will be notified in OnKrakenData event.

```
[
  0,
  {
    "a": [
      "5525.40000",
      1,
      "1.000"
    ],
    "b": [
      "5525.10000",
      1,
      "1.000"
    ],
    "c": [
      "5525.10000",
      "0.00398963"
    ],
    "v": [
      "2634.11501494",
      "3591.17907851"
    ],
    "p": [
      "5631.44067",
      "5653.78939"
    ],
    "t": [
      11493,
      16267
    ],
    "l": [
      "5505.00000",
      "5505.00000"
    ],
    "h": [
      "5783.00000",
      "5783.00000"
    ],
    "o": [
      "5760.70000",
```

```
      "5763.40000"
    ]
  },
  "ticker",
  "XBT/USD"
]
```

OHLC

When subscribed for OHLC, a snapshot of the last valid candle (irrespective of the endtime) will be sent, followed by updates to the running candle. For example, if a subscription is made to 1 min candle and there have been no trades for 5 mins, a snapshot of the last 1 min candle from 5 mins ago will be published. The endtime can be used to determine that it is an old candle. Subscribe to a OHLC calling SubscribeOHLC method, you must pass pair and interval.

```
SubscribeOHLC(['XBT/USD'], kin1min);
```

If subscription is successful, OnKrakenSubscribed event will be called:

```
procedure OnKrakenSubscribed(Sender: TObject;ChannelId: Integer; Pair,
Subscription, ChannelName: string; ReqID:Integer);
begin
  DoLog('#subscribed: ' + Subscription + ' ' + Pair + ' ' +
ChannelName);
end;
```

UnSubscribe calling UnSubscribeOHLC method:

```
UnSubscribeOHLC(['XBT/USD'], kin1min);
```

If unsubscription is successful, OnKrakenUnSubscribed event will be called:

```
procedure OnKrakenUnSubscribed(Sender: TObject; ChannelId: Integer;
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#unsubscribed: ' + Subscription + ' ' + Pair);
end;
```

If there is an error while trying to subscribe / unsubscribe, OnKrakenSubscriptionError event will be called.

```
procedure OnKrakenSubscriptionError(Sender: TObject; ErrorMessage,
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#subscription error: ' + ErrorMessage);
end;
```

OHLC updates will be notified in OnKrakenData event.

```
[
  42,
  [
    "1542057314.748456",
    "1542057360.435743",
    "3586.70000",
    "3586.70000",
    "3586.60000",
    "3586.60000",
    "3586.68894",
    "0.03373000",
    2
  ],
```

```
  "ohlc-5",
  "XBT/USD"
]
```

Trade
Trade feed for a currency pair.
Subscribe to Trade feed calling SubscribeTrade method.

```
SubscribeTrade(['XBT/USD']);
```

If subscription is successful, OnKrakenSubscribed event will be called:

```
procedure OnKrakenSubscribed(Sender: TObject;ChannelId: Integer; Pair,
Subscription, ChannelName: string; ReqID:Integer);
begin
  DoLog('#subscribed: ' + Subscription + ' ' + Pair + ' ' +
ChannelName);
end;
```

UnSubscribe calling UnSubscribeTrade method:

```
UnSubscribeTrade(['XBT/USD']);
```

If unsubscription is successful, OnKrakenUnSubscribed event will be called:

```
procedure OnrakenUnSubscribed(Sender: TObject; ChannelId: Integer;
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#unsubscribed: ' + Subscription + ' ' + Pair);
end;
```

If there is an error while trying to subscribe / unsubscribe, OnKrakenSubscriptionError event will be called.

```
procedure OnKrakenSubscriptionError(Sender: TObject; ErrorMessage,
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#subscription error: ' + ErrorMessage);
end;
```

Trade updates will be notified in OnKrakenData event.

```
[
  0,
  [
    [
      "5541.20000",
      "0.15850568",
      "1534614057.321597",
      "s",
      "l",
      ""
    ],
    [
      "6060.00000",
      "0.02455000",
      "1534614057.324998",
      "b",
      "l",
      ""
    ]
```

```
  ],
  "trade",
  "XBT/USD"
]
```

Book

Order book levels. On subscription, a snapshot will be published at the specified depth, following the snapshot, level updates will be published.

Subscribe to a Book calling SubscribeBook method, you must pass pair and depth.

```
SubscribeBook(['XBT/USD'], kde10);
```

If subscription is successful, OnKrakenSubscribed event will be called:

```
procedure OnKrakenSubscribed(Sender: TObject;ChannelId: Integer; Pair,
Subscription, ChannelName: string; ReqID:Integer);
begin
  DoLog('#subscribed: ' + Subscription + ' ' + Pair + ' ' +
ChannelName);
end;
```

UnSubscribe calling UnSubscribeBook method:

```
UnSubscribeBook(['XBT/USD'], kde10);
```

If unsubscription is successful, OnKrakenUnSubscribed event will be called:

```
procedure OnKrakenUnSubscribed(Sender: TObject; ChannelId: Integer;
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#unsubscribed: ' + Subscription + ' ' + Pair);
end;
```

If there is an error while trying to subscribe / unsubscribe, OnKrakenSubscriptionError event will be called.

```
procedure OnKrakenSubscriptionError(Sender: TObject; ErrorMessage,
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#subscription error: ' + ErrorMessage);
end;
```

Book updates will be notified in OnKrakenData event.

```
[
  0,
  {
    "as": [
      [
          "5541.30000",
          "2.50700000",
          "1534614248.123678"
      ],
      [
          "5541.80000",
          "0.33000000",
          "1534614098.345543"
      ],
      [
          "5542.70000",
          "0.64700000",
```

```
            "1534614244.654432"
        ]
      ],
      "bs": [
        [
            "5541.20000",
            "1.52900000",
            "1534614248.765567"
        ],
        [
            "5539.90000",
            "0.30000000",
            "1534614241.769870"
        ],
        [
            "5539.50000",
            "5.00000000",
            "1534613831.243486"
        ]
      ]
    },
    "book-100",
    "XBT/USD"
]
```

Spread

Spread feed to show best bid and ask price for subscribed asset pair. Bid volume and ask volume is part of the message too.

Subscribe to Spread feed calling SubscribeSpread method.

```
SubscribeSpread(['XBT/USD']);
```

If subscription is successful, OnKrakenSubscribed event will be called:

```
procedure OnKrakenSubscribed(Sender: TObject;ChannelId: Integer; Pair,
Subscription, ChannelName: string; ReqID:Integer);
begin
  DoLog('#subscribed: ' + Subscription + ' ' + Pair + ' ' +
ChannelName);
end;
```

UnSubscribe calling UnSubscribeSpread method:

```
UnSubscribeSpread(['XBT/USD']);
```

If unsubscription is successful, OnKrakenUnSubscribed event will be called:

```
procedure OnrakenUnSubscribed(Sender: TObject; ChannelId: Integer;
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#unsubscribed: ' + Subscription + ' ' + Pair);
end;
```

If there is an error while trying to subscribe / unsubscribe, OnKrakenSubscriptionError event will be called.

```
procedure OnKrakenSubscriptionError(Sender: TObject; ErrorMessage,
Pair, Subscription: string; ReqID: Integer);
begin
  DoLog('#subscription error: ' + ErrorMessage);
end;
```

Spread updates will be notified in OnKrakenData event.

```
[
  0,
  [
    "5698.40000",
    "5700.00000",
    "1542057299.545897",
    "1.01234567",
    "0.98765432"
  ],
  "spread",
  "XBT/USD"
]
```

Other Methods
You can subscribe / unsubscribe to all channels with one method:

```
SubscribeAll(['XBT/USD']);

UnSubscribeAll(['XBT/USD']);
```

OHLC interval value is 1 if all channels subscribed.

Events
OnConnect: when websocket client is connected to client.
OnKrakenConnect: called after successful websocket connection and when server send system status.
OnKrakenSystemStatus: called when system status changes.
OnKrakenSubscribed: called after a successful subscription to a channel.
OnKrakenUnSubscribed: called after a successful unsubscription from a channel.
OnKranSubscriptionError: called if there is an error trying to subscribe / unsubscribe.
OnKrakenData: called every time a channel subscription has an update.

API Kraken | WebSockets Private API

Connection
URL: wss://ws-auth.kraken.com

Once the socket is open you can subscribe to private-data channels by sending an authenticated subscribe request message.

Authentication
The API client must request an authentication "token" via the following REST API endpoint "GetWebSocketsToken" to connect to WebSockets Private endpoints. The token should be used within 15 minutes of creation. The token does not expire once a connection to a WebSockets API private message (openOrders or ownTrades) is maintained.
In order to get a Websockets Token, an API Key and API Secret must be set in Kraken Options Component, the api key provided by Kraken in your account

```
Kraken.ApiKey := 'api key';
Kraken.ApiSecret := 'api secret';
```

Methods
OwnTrades
Get a list of own trades, on first subscription, you get a list of latest 50 trades

```
SubscribeOwnTrades();
```

Later, you can unsubscribe from OwnTrades, calling UnSubscribeOwnTrades method

```
UnSubscribeOwnTrades();
```

Response example from server

```
[
  [
    {
      "TDLH43-DVQXD-2KHVYY": {
        "cost": "1000000.00000",
        "fee": "600.00000",
        "margin": "0.00000",
        "ordertxid": "TDLH43-DVQXD-2KHVYY",
        "ordertype": "limit",
        "pair": "XBT/EUR",
        "postxid": "OGTT3Y-C6I3P-XRI6HX",
        "price": "100000.00000",
        "time": "1560520332.914664",
        "type": "buy",
        "vol": "1000000000.00000000"
      }
    }
  ],
  "ownTrades"
]
```

Open Orders
Feed to show all the open orders belonging to the user authenticated API key. Initial snapshot will provide list of all open orders and then any updates to the open orders list will be sent. For status change updates, such as 'closed', the fields orderid and status will be present in the payload

```
SubscribeOpenOrders();
```
Later, you can unsubscribe from OpenOrders, calling UnSubscribeOpenOrders method

```
UnSubscribeOpenOrders();
```
Response example from server


```
[
  [
    {
      "OGTT3Y-C6I3P-XRI6HX": {
        "cost": "0.00000",
        "descr": {
          "close": "",
          "leverage": "0:1",
          "order": "sell 0.00001000 XBT/EUR @ limit 9.00000 with 0:1
leverage",
          "ordertype": "limit",
          "pair": "XBT/EUR",
          "price": "9.00000",
          "price2": "0.00000",
          "type": "sell"
        },
        "expiretm": "0.000000",
        "fee": "0.00000",
        "limitprice": "9.00000",
        "misc": "",
        "oflags": "fcib",
        "opentm": "0.000000",
        "price": "9.00000",
        "refid": "OKIVMP-5GVZN-Z2D2UA",
        "starttm": "0.000000",
        "status": "open",
        "stopprice": "0.000000",
        "userref": 0,
        "vol": "0.00001000",
        "vol_exec": "0.00000000"
      }
    }
  ],
  "openOrders"
]
```


Add Order
Send a new Order to Kraken

```
oKrakenOrder := TsgcWSKrakenOrder.Create;
oKrakenOrder.Pair := 'XBT/USD';
oKrakenOrder._Type := kosBuy;
oKrakenOrder.OrderType := kotMarket;
oKrakenOrder.Volume := 1;
AddOrder(oKrakenOrder);
```
List of Order parameters

```
pair = asset pair
type = type of order (buy/sell)
ordertype = order type:
    market
    limit (price = limit price)
```

```
    stop-loss (price = stop loss price)
    take-profit (price = take profit price)
    stop-loss-profit (price = stop loss price, price2 = take profit
price)
    stop-loss-profit-limit (price = stop loss price, price2 = take
profit price)
    stop-loss-limit (price = stop loss trigger price, price2 =
triggered limit price)
    take-profit-limit (price = take profit trigger price, price2 =
triggered limit price)
    trailing-stop (price = trailing stop offset)
    trailing-stop-limit (price = trailing stop offset, price2 =
triggered limit offset)
    stop-loss-and-limit (price = stop loss price, price2 = limit
price)
    settle-position
price = price (optional.  dependent upon ordertype)
price2 = secondary price (optional.  dependent upon ordertype)
volume = order volume in lots
leverage = amount of leverage desired (optional.  default = none)
oflags = comma delimited list of order flags (optional):
    viqc = volume in quote currency (not available for leveraged
orders)
    fcib = prefer fee in base currency
    fciq = prefer fee in quote currency
    nompp = no market price protection
    post = post only order (available when ordertype = limit)
starttm = scheduled start time (optional):
    0 = now (default)
    +<n> = schedule start time <n> seconds from now
    <n> = unix timestamp of start time
expiretm = expiration time (optional):
    0 = no expiration (default)
    +<n> = expire <n> seconds from now
    <n> = unix timestamp of expiration time
userref = user reference id.  32-bit signed number.  (optional)
validate = validate inputs only.  do not submit order (optional)
optional closing order to add to system when order gets filled:
    close[ordertype] = order type
    close[price] = price
    close[price2] = secondary price
```

Response example from server

```
{
  "descr": "buy 0.01770000 XBTUSD @ limit 4000",
  "event": "addOrderStatus",
  "status": "ok",
  "txid": "ONPNXH-KMKMU-F4MR5V"
}
```

Cancel Order

Cancel order

```
CancelOrder('Order Id');
```

Response example from server

```
{
  "event": "cancelOrderStatus",
  "status": "ok"
```

```
}
```

API Kraken | REST Public API

Connection
URL: https://api.kraken.com

Kraken Public API doesn't require any authentication.

Configuration
The only configuration is enable or not a log for REST HTTP requests. Enable HTTPLogOptions if you want to save in a text file log all HTTP Requests/Responses

Events
OnKrakenHTTPException: this event is called if there is any exception doing an HTTP Request from REST Api.

Methods
GetServerTime
This method is to aid in approximating the skew time between the server and client. Returns Time in Unix format.

```
{"error":[],"result":{"unixtime":1586705546,"rfc1123":"Sun, 12 Apr 20
15:32:26 +0000"}}
```

GetAssets
Returns information about Assets

```
{"error":[],"result":{"ADA":{"aclass":"currency","altname":"ADA","deci
mals":8,"display_decimals":6}}}
```

GetAssetPairs
Returns information about a pair of assets

```
Kraken.REST_API.GetAssetPairs(['XBTUSD']);
```

GetTicker
Returns ticker information

```
Kraken.REST_API.GetTicker(['XBTUSD']);
```

GetOHLC
Returns Open-High-Low-Close data.

```
Kraken.REST_API.GetOHLC('XBTUSD');
```

GetOrderBook
Returns Array pair name and market depth.

```
Kraken.REST_API.GetOrderBook('XBTUSD');
```

GetTrades
Returns recent trade data of a pair.

```
Kraken.REST_API.GetTrades('XBTUSD');
```

GetSpread
Returns recent spread data of a pair.

```
Kraken.REST_API.GetSpread('XBTUSD');
```

API Kraken | REST Private API

Connection
URL: https://api.kraken.com

Authentication
REST Private API requires an API Key and API Secret, these values are provided by Kraken in your account.

```
Kraken.ApiKey := 'api key';
Kraken.ApiSecret := 'api secret';
```

Methods
GetAccountBalance
Returns your account balance.

```
Kraken.REST_API.GetAccountBalance();
```

GetTradeBalance
Returns information about your trades.

```
Kraken.REST_API.GetTradeBalance();
```

GetOpenOrders
Returns a list of open orders.

```
Kraken.REST_API.GetOpenOrders();
```

GetClosedOrders
Returns a list of closed orders.

```
Kraken.REST_API.GetClosedOrders();
```

QueryOrders
Query information about an order.

```
Kraken.REST_API.QueryOrders('1234');
```

GetTradesHistory
Returns an array of trade info.

```
Kraken.REST_API.GetTradesHistory();
```

QueryTrades
Query information about a trade.

```
Kraken.REST_API.QueryTrades('1234');
```

GetOpenPositions
Returns position info.

```
Kraken.REST_API.GetOpenPositions('1234');
```

GetLedgers
Returns associative array of ledgers info.

```
Kraken.REST_API.GetLedgers();
```
QueryLedgers
Returns associative array of ledgers info.

```
Kraken.REST_API.QueryLedgers('1234');
```
GetTradeVolume
Returns trade volume info.

```
Kraken.REST_API.GetTradeVolume();
```
AddExport
Adds a new report export.

```
Kraken.REST_API.AddExport('Report All Trades');
```
ExportStatus
Get Status of reports

```
Kraken.REST_API.ExportStatus();
```
RetrieveExport
Get Report by report id.

```
Kraken.REST_API.RetrieveExport('GOCO');
```
RemoveExport
Remove Report by report id.

```
Kraken.REST_API.RemoveExport('GOCO');
```
Add Order
Adds a new order

```
pair = asset pair
type = type of order (buy/sell)
ordertype = order type:
    market
    limit (price = limit price)
    stop-loss (price = stop loss price)
    take-profit (price = take profit price)
    stop-loss-profit (price = stop loss price, price2 = take profit
price)
    stop-loss-profit-limit (price = stop loss price, price2 = take
profit price)
    stop-loss-limit (price = stop loss trigger price, price2 =
triggered limit price)
    take-profit-limit (price = take profit trigger price, price2 =
triggered limit price)
    trailing-stop (price = trailing stop offset)
    trailing-stop-limit (price = trailing stop offset, price2 =
triggered limit offset)
    stop-loss-and-limit (price = stop loss price, price2 = limit
price)
    settle-position
price = price (optional.  dependent upon ordertype)
price2 = secondary price (optional.  dependent upon ordertype)
volume = order volume in lots
leverage = amount of leverage desired (optional.  default = none)
```

```
oflags = comma delimited list of order flags (optional):
    viqc = volume in quote currency (not available for leveraged
orders)
    fcib = prefer fee in base currency
    fciq = prefer fee in quote currency
    nompp = no market price protection
    post = post only order (available when ordertype = limit)
starttm = scheduled start time (optional):
    0 = now (default)
    +n = schedule start time n seconds from now
    n = unix timestamp of start time
expiretm = expiration time (optional):
    0 = no expiration (default)
    +n = expire n seconds from now
    n = unix timestamp of expiration time
userref = user reference id.  32-bit signed number.  (optional)
validate = validate inputs only.  do not submit order (optional)
optional closing order to add to system when order gets filled:
    close[ordertype] = order type
    close[price] = price
    close[price2] = secondary price


oKrakenOrder := TsgcWSKrakenOrder.Create;
oKrakenOrder.Pair := 'XBT/USD';
oKrakenOrder._Type := kosBuy;
oKrakenOrder.OrderType := kotMarket;
oKrakenOrder.Volume := 1;
Kraken.REST_API.AddOrder(oKrakenOrder);
```

CancelOrder

Cancels an open order by id

```
Kraken.REST_API.CancelOrder('1234');
```

API FXCM

FXCM

FXCM, also known as Forex Capital Markets, is a retail broker for trading on the foreign exchange market. FXCM allows people to speculate on the foreign exchange market and provides trading in contract for difference (CFDs) on major indices and commodities such as gold and crude oil. It is based in London.

FXCM offers a web-based REST API which can be used to establish secure connectivity with FXCM's trading systems for the purpose of receiving market data and trading.

FXCM sgcWebSockets component uses WebSocket (socket.io) and HTTP as transports to connect to a FXCM Servers.

Connection

To use the REST API, you will need:

- **Access Token** generated with Trading Station Web https://tradingstation.fxcm.com/.
- Select which API do you want connect: api-demo.fxcm.com or api.fxcm.com.

```
// ... create components
oClient := TsgcWebSocketClient.Create(nil);
oFXCM := TsgcWSAPI_FXCM.Create(nil);
oFXCM.Client := oClient;

// ... set properties FXCM
oFXCM.FXCM.AccessToken := 'here your access token';
oFXCM.FXCM.Host := 'api.fxcm.com';
oFXCM.FXCM.Port := 443;
oFXCM.FXCM.TLS := True;

// ... connect to server
oClient.Active := True;
```

Messages

Once authenticated against server, FXCM uses websocket to receive unsolicited messages like price updates and you can request data from server using HTTP methods.

Delphi

```
oClient.OnMessage(Connection: TsgcWSConnection; const Text: string);
begin
  // ... here we receive all messages from server
end;
```

Methods

- **GetSymbols:** Request a list of all available symbols.

- **SubscribeMarketData:** After subscribing, market price updates will be pushed to the client via the socket.
- **SubscribeTradingTables:** Subscribes to the updates of the data models. Update will be pushed to client via the socket. Type of update can be determined by "Model" Parameter.
- **SnapshotTradingTables:** In case continuous updates of the trading tables is not needed, it is possible to request a one-time snapshot. Gets current content snapshot of the specified data models.
    - Model choices:
        - Offer
        - OpenPosition
        - ClosedPosition
        - Order
        - Summary
        - LeverageProfile
        - Account
        - Properties
- **UpdateSubscriptions:** Offers table will show only symbols that we have subscribed to using update_subscriptions.
- **TradingOrder:** allows to send open orders, modify, close...
- **GetHistoricalData:** Allow user to retrieve candles for a given instrument at a given time frame. If time range is specified, number of candles parameter is ignored, but still required. There is a limit on the number of candles that can be returned in one request.

API Discord

Discord

Gateways are Discord's form of real-time communication over secure WebSockets. Clients will receive events and data over the gateway they are connected to and send data over the REST API.

Authorization

First you must generate a new Bot, and copy Bot Token which will be used to authenticate through API. Then set this token in API Component.

Delphi
```
TsgcWSAPI_Discord.DiscordOptions.BotOptions.Token := '... bot token here ...';
```

Intents

Maintaining a stateful application can be difficult when it comes to the amount of data you're expected to process, especially at scale. Gateway Intents are a system to help you lower that computational burden.
When identifying to the gateway, you can specify an intents parameter which allows you to conditionally subscribe to pre-defined "intents", groups of events defined by Discord. If you do not specify a certain intent, you will not receive any of the gateway events that are batched into that group. The valid intents are (zero value means all events are received):

GUILDS (1 << 0) = Integer (1)
 - GUILD_CREATE
 - GUILD_DELETE
 - GUILD_ROLE_CREATE
 - GUILD_ROLE_UPDATE
 - GUILD_ROLE_DELETE
 - CHANNEL_CREATE
 - CHANNEL_UPDATE
 - CHANNEL_DELETE
 - CHANNEL_PINS_UPDATE
GUILD_MEMBERS (1 << 1) = Integer (2)
 - GUILD_MEMBER_ADD
 - GUILD_MEMBER_UPDATE
 - GUILD_MEMBER_REMOVE
GUILD_BANS (1 << 2) = Integer (4)
 - GUILD_BAN_ADD
 - GUILD_BAN_REMOVE
GUILD_EMOJIS (1 << 3) = Integer (8)
 - GUILD_EMOJIS_UPDATE
GUILD_INTEGRATIONS (1 << 4) = Integer (16)
 - GUILD_INTEGRATIONS_UPDATE
GUILD_WEBHOOKS (1 << 5) = Integer (32)
 - WEBHOOKS_UPDATE
GUILD_INVITES (1 << 6) = Integer (64)
 - INVITE_CREATE
 - INVITE_DELETE
GUILD_VOICE_STATES (1 << 7) = Integer (128)

- VOICE_STATE_UPDATE
GUILD_PRESENCES (1 << 8) = Integer (256)
- PRESENCE_UPDATE
GUILD_MESSAGES (1 << 9) = Integer (512)
- MESSAGE_CREATE
- MESSAGE_UPDATE
- MESSAGE_DELETE
GUILD_MESSAGE_REACTIONS (1 << 10) = Integer (1024)
- MESSAGE_REACTION_ADD
- MESSAGE_REACTION_REMOVE
- MESSAGE_REACTION_REMOVE_ALL
- MESSAGE_REACTION_REMOVE_EMOJI
GUILD_MESSAGE_TYPING (1 << 11) = Integer (2048)
- TYPING_START
DIRECT_MESSAGES (1 << 12) = Integer (4096)
- CHANNEL_CREATE
- MESSAGE_CREATE
- MESSAGE_UPDATE
- MESSAGE_DELETE
- CHANNEL_PINS_UPDATE
DIRECT_MESSAGE_REACTIONS (1 << 13) = Integer (8192)
- MESSAGE_REACTION_ADD
- MESSAGE_REACTION_REMOVE
- MESSAGE_REACTION_REMOVE_ALL
- MESSAGE_REACTION_REMOVE_EMOJI
DIRECT_MESSAGE_TYPING (1 << 14) = Integer (16384)
- TYPING_START

HeartBeat

HeartBeats are automatically handle by component so you don't need to worry about it. When client connects to server, server sends a HELLO response with heartbeat interval, component reads response and adjust automatically heartbeat so send a ping every x seconds. Sometimes server can send a ping to client, this is handled automatically by client too.

Connection Ready

When connection is ready, after a successful login and authorization by server, **OnDiscordReady** event is raised and then you can start to receive updates from server.

Connection Resume

If connection closes unexpectedly, when client tries to reconnect, it calls **OnDiscordBeforeReconnect** event, component automatically saves all data needed to make a successful resume, but parameters can be changed if needed. If you don't want to reconnect and start a new clean session, just set Reconnect to False.

If session is resumed, **OnDiscordResumed** event is fired. If it's a new session, **OnDiscordReady** fill be fired.

Dispatch Events

Events are dispatched **OnDiscordDispatch**, so here you can read events sent by server to client.

Delphi
```
procedure OnDiscordDispatch(Sender: TObject; const aEvent, RawData:
string);
begin
  DoLog('#discord dispatch: ' + aEvent + ' ' + RawData);
end;
```

aEvent parameter contains parameter name.
RawData contains full JSON message.

HTTP Requests
In order to request info about guild, users, udpate data... instead of use gateway websocket messages, Discord requires to use HTTP requests, so find bellow all methods available to do an HTTP request:

```
function GET_Request(const aPath: String): string;
function POST_Request(const aPath, aMessage:  String): string;
function PUT_Request(const aPath, aMessage:  String): string;
function PATCH_Request(const aPath, aMessage:  String): string;
function DELETE_Request(const aPath: String):  string;
```

Example: get current user info

Delphi
```
result := GET_Request('/users/@me');
```

sample response from server:

```
{
"id": "637423922035480852",
"username": "test",
"avatar": null,
"discriminator": "5125",
"bot": true,
"email": null,
"verified": true,
"locale": "en-US",
"mfa_enabled": false,
"flags": 0
}
```

Other APIs

Telegram

API Telegram

Telegram

Telegram offers two kinds of APIs, one is **Bot API** which allows to create programs that use Bots and HTTPs as protocol. **Telegram API and TDLib** allows to build customized Telegram clients and is much more powerful than Bot API.

sgcWebSockets **supports TDLib through tdjson** library, which means that you can build your own telegram client. TDLib takes care of all network implementation details, encryption and local data storage. TDLib supports all Telegram features.

TDLib (Telegram Database Library) Advantages

- **Cross-platform:** can be used on Windows, Android, iOS, MacOS, Linux... currently only Windows (win32 an win64) is supported by sgcWebSockets.
- **Easy to use:** uses json messages to communicate between application and telegram.
- **High-performance:** In the Telegram Bot API, each TDLib instance handles more than 24000 bots.
- **Consistent:** TDLib guarantees that all updates will be delivered in the right order.
- **Reliable:** TDLib remains stable on slow and unreliable internet connections.
- **Secure:** All local data is encrypted using a user-provided encryption key.
- **Fully Asynchronous:** Requests to TDLib don't block each other. Responses will be sent when they are available.

Dependencies
TDLib requires other third-parties libraries: OpenSSL and ZLib. These libraries must be deployed with tdjson library.

* Windows versions requires VCRuntime which can be download from microsoft:
https://www.microsoft.com/en-us/download/details.aspx?id=52685

Creating your Telegram Application
In order to obtain an API id and develop your own application using the Telegram API you need to do the following:

- Sign up for Telegram using any application.
- Log in to your Telegram core: https://my.telegram.org.
- Go to **API development tools** and fill out the form.
- You will get basic addresses as well as the **api_id** and **api_hash** parameters required for user authorization.
- For the moment each number can only have one **api_id** connected to it.

These values must be set in **Telegram.API** property of Telegram component. In order to authenticate, you can authenticate as an user or as a bot, there are 2 properties which you can set to login to Telegram:

- **PhoneNumber:** if you login as an user, you must set your **phone number** (with international code), example: +34699123456
- **BotToken:** if you logi8n as a bot, set your token in this property (as provided by telegram).

The following parameters can be configured:

- **ApplicationVersion:** application version, example: 1.0

- **DeviceModel:** device model, example: desktop
- **LanguageCode:** user language code, example: en.
- **SystemVersion:** verison of operating system, example: windows.

Once you have configured Telegram Component, you can set Active property to true and program will try to connect to Telegram.

Sample Code

```
oTelegram := TsgcTDLib_Telegram.Create(nil);
oTelegram.Telegram.API.ApiHash := 'your api hash';
oTelegram.Telegram.API.ApiId := 'your api id';
oTelegram.PhoneNumber := 'your phone number';
oTelegram.ApplicationVersion := '1.0';
oTelegram.DeviceModel := 'Desktop';
oTelegram.LanguageCode := 'en';
oTelegram.SystemVersion := 'Windows';
oTelegram.Active := true;
```

Authorization
There are two events which can be called by library in order to get an Authentication Code (delivered in Telegram Application, not SMS) or to provide a password.

OnAuthenticationCode

This event is called when Telegram sends an Authorization Code to Telegram Application and user must copy this code and set in Code argument of this event.

```
procedure OnAuthenticationCode(Sender: TObject; var Code: string);
begin
  Code := InputBox('Telegram Code', 'Introduce code', '');
end;
```

OnAuthenticationPassword

This event is called when Telegram requires that user set a password.

Authorization Status
Once authorization has started, you can check the status of authorization **OnAuthorizationStatus** event, this event is called every time there is a change in status of authorization. Some values of Status are:

- authorizationStateWaitTdlibParameters
- authorizationStateWaitEncryptionKey
- authorizationStateWaitPhoneNumber
- authorizationStateWaitCode
- authorizationStateLoggingOut
- authorizationStateClosed
- authorizationStateReady

Connection Status
Once connection has started, you can check the status of connection **OnConnectionStatus** event, this event is called every time there is a change in status of connection. Some values of Status are:

- connectionStateConnecting
- connectionStateUpdating
- connectionStateReady

Methods
TsgcTDLib_Telegram API Component support the most following methods.

Method	Parameters	Description
SendTextMessage	**aChatId:** Id of Chat which message will be sent **aText:** Text of Message.	Sends a Text Message to a Chat
SendDocumentMessage	**aChatId:** Id of Chat which message will be sent **aFilePath:** full file path of document	Sends a Document to a Chat.
SendPhotoMessage	**aChatId:** Id of Chat which message will be sent **aFilePath:** full file path of photo **aWidth:** witdh of photo. **aHeight:** width of photo.	Sends a Photo to a Chat.
SendVideoMessage	**aChatId:** Id of Chat which message will be sent **aFilePath:** full file path of video **aWidth:** witdh of video. **aHeight:** width of video. **aDuration:** duration of video in seconds.	Sends a Video to a Chat.
AddChatMember	**aChatId:** Id of Chat which message will be sent	Adds a new member to a chat. Members

	aUserId: Identifier of the user. **aForwardLimit:** The number of earlier messages from the chat to be forwarded to the new member; up to 100. Ignored for supergroups and channels.	can't be added to private or secret chats. Members will not be added until the chat state has been synchronized with the server.
AddChatMembers	**aChatId:** Id of Chat which message will be sent **aUserIds:** Identifiers of the users to be added to the chat.	Adds multiple new members to a chat. Currently this option is only available for supergroups and channels. This option can't be used to join a chat. Members can't be added to a channel if it has more than 200 members. Members will not be added until the chat state has been synchronized with the server.
JoinChatByInviteLink	**aLink:** Invite link to import;	Uses an invite link to add the current user to the chat if possible. The new member will not be added until the chat state has been synchronized

		with the server.
CreateNewSecretChat	**aUserId:** Identifier of the user.	Creates a new secret chat.
CreateNewBasicGroupChat	**aUserIds:** Identifiers of the users to be added to the chat. **aTitle:** Title of the new basic group	Creates a new basic group
CreateNewSupergroupChat	**aTitle:** Title of the new SuperGroup **aIsChannel:** True, if a channel chat should be created. **aDescription:** Chat Description.	Creates a new supergroup or channel.
CreatePrivateChat	**aUserId:** Identifier of the user. **aForce:** If true, the chat will be created without network request. In this case all information about the chat except its type, title and photo can be incorrect	Returns an existing chat corresponding to a given user
GetChats	**aOffsetOrder:** Chat order to return chats from **aOffsetChatId:** Chat identifier to return chats from **aLimit:** The maximum number of chats to be returned.	Returns an ordered list of chats. Chats are sorted by the pair (order, chat_id) in decreasing order.
GetChatHistory	**aChatId:** Chat identifier **aFromMessageId:** Identifier of the message starting from which history must be fetched; use 0 to get results from the last	Returns messages in a chat. The messages are returned in a reverse chronological order

	message. **aOffset:** Specify 0 to get results from exactly the from_message_id or a negative offset up to 99 to get additionally some newer messages. **aLimit:**The maximum number of messages to be returned	
GetUser	**aUserId:** User Identifier	Returns information about a user by their identifier.
Logout		Logouts from Telegram.
TDLibSend	**aRequest:** JSON Request.	Send any Request in JSON protocol.

Example How to send a Text Message

```
oTelegram := TsgcTDLib_Telegram.Create(nil);
oTelegram.Telegram.API.ApiHash := 'your api hash';
oTelegram.Telegram.API.ApiId := 'your api id';
oTelegram.PhoneNumber := 'your phone number';
oTelegram.Active := true;
...
oTelegram.SendTextMessage('1234', 'My First Message from
sgcWebSockets');
```

Example How to send a method not implemented

You can Send Any JSON message using TDLibSend method, example: join a telegram chat.

```
oTelegram := TsgcTDLib_Telegram.Create(nil);
oTelegram.Telegram.API.ApiHash := 'your api hash';
oTelegram.Telegram.API.ApiId := 'your api id';
oTelegram.PhoneNumber := 'your phone number';
oTelegram.Active := true;
...
oTelegram.TDLibSend('{"@type": "joinChat", "chat_id": "1234"}');
```

Check the following url to know all JSON methods: Telegram JSON API.

Events

OnBeforeReadEvent

This event is called when JSON message is received by Telegram API component and is still not processed. Set Handled property to True if you process this event manually or don't want that event is processed by component. You can use this event to log all messages too.

OnMessageText
This event is called when a New Message Text has been received, read MessageText parameter to access to message text properties.

- **ChatId:** Chat Identifier.
- **MessageId:** Message Identifier.
- **SenderUserId:** Sender Identifier.
- **Text:** Text of message.

OnMessageDocument
This event is called when a New Document Message is received. Access to MessageDocument to get access to Document properties.

- **ChatId:** Chat Identifier.
- **MessageId:** Message Identifier.
- **SenderUserId:** Sender Identifier.
- **FileName:** Name of Document.
- **DocumentId:** Document Identifier.
- **LocalPath:** full path to local file if exists.
- **MimeType:** Mime-type of document.
- **Size:** Size of Document.
- **RemoteDocumentId:** Remote Document Identifier.

OnMessagePhoto
This event is called when a New Photo Message is received. Access to MessagePhoto to get access to Photo properties.

- **ChatId:** Chat Identifier.
- **MessageId:** Message Identifier.
- **SenderUserId:** Sender Identifier.
- **PhotoId:** Photo Identifier.
- **LocalPath:** full path to local file if exists.
- **Size:** Size of Photo.
- **RemotePhotoId:** Remote Photo Identifier.

OnVideoPhoto
This event is called when a New Video Message is received. Access to MessageVideo to get access to Video properties.

- **ChatId:** Chat Identifier.
- **MessageId:** Message Identifier.
- **SenderUserId:** Sender Identifier.
- **VideoId:** Photo Identifier.
- **LocalPath:** full path to local file if exists.
- **Width:** width of video.
- **Height:** height of video.

- **Duration:** duration in seconds of video.
- **Size:** Size of Video.
- **RemoteVideoId:** Remote Photo Identifier.

OnNewChat
This event is called when a new chat is received.

- **ChatId:** Chat Identifier.
- **ChatType:** Chat Type (chatTypeSupergroup, chatTypePrivate...)
- **Title:** Chat name.
- **SuperGroupId:** Group Id if is a SuperGroup.
- **IsChannel:** returns if is channel or not.

OnEvent
This event is called when a new Event is received by API Component. Can be used to process some events not implemented by API Component.

- **Event:** Event name (events like: updateOption, updateUser...)
- **Text:** full JSON message

OnException
This event is called if there is any exception when processing Telegram API Data.

Properties
MyId: returns the User Identifier of current user.

Full Code Sample
Check the following code sample which shows how connect to Telegram API, ask user to introduce a Code (if required by Telegram API), send a message when connection is ready and Log Text Messages received.

```
oTelegram := TsgcTDLib_Telegram.Create(nil);
oTelegram.Telegram.API.ApiHash := 'your api hash';
oTelegram.Telegram.API.ApiId := 'your api id';
oTelegram.PhoneNumber := 'your phone number';
oTelegram.ApplicationVersion := '1.0';
oTelegram.DeviceModel := 'Desktop';
oTelegram.LanguageCode := 'en';
oTelegram.SystemVersion := 'Windows';
oTelegram.Active := true;
procedure OnAuthenticationCode(Sender: TObject; var Code: string);
begin
  Code := InputBox('Telegram Code', 'Introduce code', '');
end;
procedure OnMessageText(Sender: TObject; MessageText:
TsgcTelegramMessageText);
begin
  Log('Message Received: ' + MessageText.Text);
end;
procedure OnConnectionStatus(Sender: TObject; const Status: string);
begin
  if Status = 'connectionStateReady' then
    oTelegram.SendTextMessage('1234', 'Hello Telegram!');
```

```
end;
```

Extensions

Extensions

WebSocket protocol is designed to be extended. WebSocket Clients may request extensions and WebSocket Servers may accept some or all extensions requested by clients.

Extensions supported:

1. Deflate-Frame: compress WebSocket frames.

2. PerMessage-Deflate: compress WebSocket messages.

Extensions | PerMessage-Deflate

PerMessage is a WebSocket protocol extension, if the extension is supported by Server and Client, both can compress transmitted messages:

- Uses Deflate as the compression method.
- Compression only applies to Application data (control frames and headers are not affected).
- Server and client can select which messages will be compressed.

Max Window Bits

This extension allows customizing Server and Client size of the sliding window used by LZ77 algorithm (between 8 - 15). As greater is this value, more probably will find and eliminate duplicates but consumes more memory and CPU cycles. 15 is the default value.

No Context Take Over

By default, previous messages are used to compression and decompression, if messages are similar, this improves the compression ratio. If Enabled, then each message is compressed using only its message data. By default is disabled.

MemLevel

This value is not negotiated between Server and Client. when set to 1, it uses the least memory, but slows down the compression algorithm and reduces the compression ratio; when set to 9, it uses the most memory and delivers the best performance. By default is set to 1.

** Indy version provided with Rad Studio XE2 raises an exception because of zlib version mismatch with initialization functions, to fix this, just update your Indy version to latest.*

Extensions | Deflate-Frame

Is a WebSocket protocol extension which allows the compression of frames sent using WebSocket protocol, supported by WebKit browsers like chrome or safari. This extension is supported on Server and Client Components.

This extension has been deprecated.

** Indy version provided with Rad Studio XE2 raises an exception because or zlib version mismatch with initialization functions, to fix this, just update your Indy version to latest.*

IoT

IoT

The Internet of things (IoT) refers to the concept of extending Internet connectivity beyond conventional computing platforms such as personal computers and mobile devices, and into any range of traditionally "dumb" or non-internet-enabled physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled.

sgcWebSockets package implements the following IoT clients:

1. Amazon AWS IoT: AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers, or smart appliances and the AWS Cloud. This enables you to collect telemetry data from multiple devices, and store and analyze the data. You can also create applications that enable your users to control these devices from their phones or tablets.

2. Azure IoT Hub: IoT Hub is a managed service, hosted in the cloud, that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages. You can use Azure IoT Hub to build IoT solutions with reliable and secure communications between millions of IoT devices and a cloud-hosted solution backend.

Amazon

IoT Amazon MQTT Client

What Is AWS IoT?

AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers, or smart appliances and the AWS Cloud. This enables you to collect telemetry data from multiple devices, and store and analyze the data. You can also create applications that enable your users to control these devices from their phones or tablets.

Message broker

Provides a secure mechanism for devices and AWS IoT applications to publish and receive messages from each other. You can use either the MQTT protocol directly or MQTT over WebSocket to publish and subscribe.

The AWS IoT message broker is a publish/subscribe broker service that enables the sending and receiving of messages to and from AWS IoT. When communicating with AWS IoT, a client sends a message addressed to a topic like Sensor/temp/room1.

The message broker, in turn, sends the message to all clients that have registered to receive messages for that topic. The act of sending the message is referred to as publishing. The act of registering to receive messages for a topic filter is referred to as subscribing.

The topic namespace is isolated for each AWS account and region pair. For example, the Sensor/temp/room1 topic for an AWS account is independent from the Sensor/temp/room1 topic for another AWS account. This is true of regions, too. The Sensor/temp/room1 topic in the same AWS account in us-east-1 is independent from the same topic in us-east-2. AWS IoT does not support sending and receiving messages across AWS accounts and regions.

The message broker maintains a list of all client sessions and the subscriptions for each session. When a message is published on a topic, the broker checks for sessions with subscriptions that map to the topic. The broker then forwards the publish message to all sessions that have a currently connected client.

MQTT Client

TsgcIoTAmazon_MQTT_Client is the component used for connect to AWS IoT, one client can connect to only one device. Client connects using plain MQTT protocol and authenticates using a X.509 Client Certificate.

In order to connect to AWS IoT, client needs the following properties:

> **Amazon.ClientId:** identification of client, optional.
> **Amazon.Endpoint:** server name where MQTT client will connect.
> **Amazon.Port:** by default uses port 8883. If port is 443, uses ALPN automatically to connect. Requires custom Indy version.
> **Certificate.CertFile:** path to X.509 client certificate.
> **Certificate.KeyFile:** path to X.509 client key file.

Client can send optionally a ClientId to identifiy client connection, then others clients can subscribe to receive a notification every time this client has connected, subscribed, disconnected...

Amazon MQTT implementation is based on MQTT version 3.1.1 but it deviates from the specification as follows:

- In AWS IoT, subscribing to a topic with Quality of Service (QoS) 0 means a message is delivered zero or more times. A message might be delivered more than once. Messages delivered more than once might be sent with a different packet ID. In these cases, the DUP flag is not set.
- AWS IoT does not support publishing and subscribing with QoS 2. The AWS IoT message broker does not send a PUBACK or SUBACK when QoS 2 is requested.
- When responding to a connection request, the message broker sends a CONNACK message. This message contains a flag to indicate if the connection is resuming a previous session. The value of this flag might be incorrect if two MQTT clients connect with the same client ID simultaneously.
- When a client subscribes to a topic, there might be a delay between the time the message broker sends a SUBACK and the time the client starts receiving new matching messages.
- The MQTT specification provides a provision for the publisher to request that the broker retain the last message sent to a topic and send it to all future topic subscribers. AWS IoT does not support retained messages. If a request is made to retain messages, the connection is disconnected.
- The message broker uses the client ID to identify each client. The client ID is passed in from the client to the message broker as part of the MQTT payload. Two clients with the same client ID are not allowed to be connected concurrently to the message broker. When a client connects to the message broker using a client ID that another client is using, a CONNACK message is sent to both clients and the currently connected client is disconnected.
- On rare occasions, the message broker might resend the same logical PUBLISH message with a different packet ID.
- The message broker does not guarantee the order in which messages and ACK are received.

Connect to AWS IoT

```
// First, you must sign in your AWS console, register a new device and
create a X.509 certificate for this device.
// Once is done, you can create create a new TsgcIoTAmazon_MQTT_Client
and connect to AWS IoT Server.
// For example:

oClient := TsgcIoTAmazon_MQTT_Client.Create(nil);
oClient.Amazon.Endpoint := 'a2ohgdjqitsmij-ats.iot.us-west-
2.amazonaws.com';
oClient.Amazon.ClientId := 'sgcWebSockets';
oClient.Certificate.CertFile := 'amazon-certificate.pem.crt';
oClient.Certificate.KeyFile := 'amazon-private.pem.key';
oClient.OnMQTTConnect := OnMQTTConnectEvent;
oClient.Active := True;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const ReturnCode: TmqttConnReturnCode);
begin
  ShowMessage('Connected to AWS');
end;
```

Topics

```
// The message broker uses topics to route messages from publishing
clients to subscribing clients. The forward slash (/) is used to
separate topic hierarchy.
// The following table lists the wildcards that can be used in the
topic filter when you subscribe.
// # Must be the last character in the topic to which you are
subscribing. Works as a wildcard by matching the current tree and all
subtrees.
//    For example, a subscription to Sensor/# receives messages
published to Sensor/, Sensor/temp, Sensor/temp/room1, but not the
messages published to Sensor.
// + Matches exactly one item in the topic hierarchy. For example, a
subscription to Sensor/+/room1 receives messages published to
Sensor/temp/room1, Sensor/moisture/room1, and so on.
oClient := TsgcIoTAmazon_MQTT_Client.Create(nil);
...
oClient.OnSubscribe := OnSubscribeEvent;

vPacketIdentifier := oClient.Subscribe('Sensor/moisture/room1');

procedure OnMQTTSubscribe(Connection: TsgcWSConnection;
aPacketIdentifier: Word; aCodes: TsgcWSSUBACKS);
begin
  if vPacketIdentifier = aPacketIdentifier then
    ShowMessage('Subscribed to topic Sensor/moisture/room1');
end;

// Client, can send a message using Publish method.
oClient.Publish('Sensor/moisture/room1', '{"temp"=10}');

// Messages received from server, are dispatched OnMQTTPublishEvent.

procedure OnMQTTPublish(Connection: TsgcWSConnection; aTopic, aText:
string);
begin
  DoLog('Received Message: ' + aTopic + ' ' + aText);
end;
```

Reserved Topics

Following methods are used to subscribe / publish to reserved topics.

Subscribe_ClientConnected(const aClientId: String): AWS IoT publishes to this topic when an MQTT client with the specified client ID connects to AWS IoT
Subscribe_ClientDisconnected(const aClientId: String): AWS IoT publishes to this topic when an MQTT client with the specified client ID disconnects to AWS IoT
Subscribe_ClientSubscribed(const aClientId: String): AWS IoT publishes to this topic when an MQTT client with the specified client ID subscribes to an MQTT topic
Subscribe_ClientUnSubscribed(const aClientId: String): AWS IoT publishes to this topic when an MQTT client with the specified client ID unsubscribes to an MQTT topic

Publish_Rule(const aRuleName, aText: String): A device or an application publishes to this topic to trigger rules directly

Publish_DeleteShadow(const aThingName, aText: String): A device or an application publishes to this topic to delete a shadow

Subscribe_DeleteShadow(const aThingName: String): A device or an application subscribe to this topic to delete a shadow
Subscribe_ShadowDeleted(const aThingName: String): The Device Shadow service sends messages to this topic when a shadow is deleted
Subscribe_ShadowRejected(const aThingName: String): The Device Shadow service sends messages to this topic when a request to delete a shadow is rejected
Publish_ShadowGet(const aThingName, aText: String): An application or a thing publishes an empty message to this topic to get a shadow
Subscribe_ShadowGet(const aThingName: String): An application or a thing subscribe to this topic to get a shadow
Subscribe_ShadowGetAccepted(const aThingName: String): The Device Shadow service sends messages to this topic when a request for a shadow is made successfully
Subscribe_ShadowGetRejected(const aThingName: String): The Device Shadow service sends messages to this topic when a request for a shadow is rejected
Publish_ShadowUpdate(const aThingName, aText: String): A thing or application publishes to this topic to update a shadow
Subscribe_ShadowUpdateAccepted(const aThingName: String): The Device Shadow service sends messages to this topic when an update is successfully made to a shadow
Subscribe_ShadowUpdateRejected(const aThingName: String): The Device Shadow service sends messages to this topic when an update to a shadow is rejected
Subscribe_ShadowUpdateDelta(const aThingName: String): The Device Shadow service sends messages to this topic when a difference is detected between the reported and desired sections of a shadow
Subscribe_ShadowUpdateDocuments(const aThingName: String): AWS IoT publishes a state document to this topic whenever an update to the shadow is successfully performed

Persistent Sessions

A persistent session represents an ongoing connection to an MQTT message broker. When a client connects to the AWS IoT message broker using a persistent session, the message broker saves all subscriptions the client makes during the connection. When the client disconnects, the message broker stores unacknowledged QoS 1 messages and new QoS 1 messages published to topics to which the client is subscribed. When the client reconnects to the persistent session, all subscriptions are reinstated and all stored messages are sent to the client at a maximum rate of 10 messages per second.

You create an MQTT persistent session setting the **cleanSession** parameter to False **OnMQTTBeforeConnect** event. If no session exists for the client, a new persistent session is created. If a session already exists for the client, it is resumed.

Devices need to look at the **Session** attribute in the **OnMQTTConnect** event to determine if a persistent session is present. If **Session is True**, a persistent session is present and stored messages are delivered to the client. If **Session is False**, no persistent session is present and the client must re-subscribe to its topic filters.

Persistent sessions have a default expiry period of 1 hour. The expiry period begins when the message broker detects that a client disconnects (MQTT disconnect or timeout). The persistent session expiry period can be increased through the standard limit increase process. If a client has not resumed its session within the expiry period, the session is terminated and any associated stored messages are discarded. The expiry period is approximate, sessions might be persisted for up to 30 minutes longer (but not less) than the configured duration.

Azure

IoT Azure MQTT Client

What is Azure IoT Hub?

IoT Hub is a managed service, hosted in the cloud, that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages. You can use Azure IoT Hub to build IoT solutions with reliable and secure communications between millions of IoT devices and a cloud-hosted solution backend. You can connect virtually any device to IoT Hub.

IoT Hub supports communications both from the device to the cloud and from the cloud to the device. IoT Hub supports multiple messaging patterns such as device-to-cloud telemetry, file upload from devices, and request-reply methods to control your devices from the cloud. IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

IoT Hub's capabilities help you build scalable, full-featured IoT solutions such as managing industrial equipment used in manufacturing, tracking valuable assets in healthcare, and monitoring office building usage.

Message broker

IoT Hub gives you a secure communication channel for your devices to send data. IoT Hub and the device SDKs support the following protocols for connecting devices:

- **MQTT**
- **MQTT** over **WebSockets**

Multiple authentication types support a variety of device capabilities:

- **SAS** token-based authentication to quickly get started with your IoT solution.
- Individual **X.509 certificate** authentication for secure, standards-based authentication.

MQTT Client

TsgcIoTAzure_MQTT_Client is the component used for connect to Azure IoT, one client can connect to only one device. Client connects using plain MQTT protocol and authenticates using SAS / X.509 Client Certificate.

In order to connect to Azure IoT Hub, client needs the following properties:

Azure.IoTHub: server name where MQTT client will connect.
Azure.DeviceId: name of device in azure IoT Hub.

Azure allows multiple authentication types, by default uses SAS tokens.

SAS Authentication

SAS.Enabled: enable if authentication uses SAS.
SAS.SecretKey: here SAS Token from your Azure IoT Account.

X509 Certificates

Certificate.Enabled: enable if authentication uses certificates.
Certificate.CertFile: path to X.509 client certificate.
Certificate.KeyFile: path to X.509 client key file.
Certificate.Password: if certificate has a password set here.
Version: TLS version, by default uses TLS 1.0

Azure MQTT implementation is based on MQTT version 3.1.1 but it deviates from the specification as follows:

- IoT Hub does not support QoS 2 messages. If a device app publishes a message with QoS 2, IoT Hub closes the network connection.
- IoT Hub does not persist Retain messages. If a device sends a message with the RETAIN flag set to 1, IoT Hub adds the x-opt-retain application property to the message. In this case, instead of persisting the retain message, IoT Hub passes it to the backend app.
- IoT Hub only supports one active MQTT connection per device. Any new MQTT connection on behalf of the same device ID causes IoT Hub to drop the existing connection.

Connect to Azure IoT Hub

```
// First, you must sign in your Azure account, register a new device
and create an authentication
// method for this device. Once is done, you can create create a new
TsgcIoTAzure_MQTT_Client
// and connect to Azure IoT Hub.

// For example:
oClient := TsgcIoTAzure_MQTT_Client.Create(nil);
oClient.Azure.IoTHub := 'youriothub.azure-devices.net';
oClient.Azure.DeviceId := 'YourDeviceId';
oClient.SAS.Enabled := True;
oClient.SAS.SecretKey := 'YourSecretKey';
oClient.OnMQTTConnect := OnMQTTConnectEvent;
oClient.Active := True;

procedure OnMQTTConnect(Connection: TsgcWSConnection; const Session:
Boolean; const
ReturnCode: TmqttConnReturnCode);
begin
  ShowMessage('Connected to Azure IoT Hub');
end;
```

Device To Cloud

```
// When sending information from the device app to the solution back
end, IoT Hub exposes following options:
```

```
// 1. Device-to-cloud messages for time series telemetry and alerts.

   oClient.Send_DeviceToCloud('{"temp"=10}', azuIoTQoS1);

// 2. Device twin's reported properties for reporting device state
information such as available capabilities,
// conditions, or the state of long-running workflows. For example,
configuration and software updates.

   oClient.Set_DeviceTwinsProperties('1', '{"sgc":1}');
```

Cloud To Device

```
// IoT Hub provides three options for device apps to expose
functionality to a back-end app:

// 1. Direct methods for communications that require immediate
confirmation of the result.
// Direct methods are often used for interactive control of devices
such as turning on a fan.

   oClient.Subscribe_DirectMethod;

// You can respond to public methods, using following method.

   oClient.RespondPublicMethod(RequestId, Status, 'Your Response',
azuIoTQoS1);

// 2. Twin's desired properties for long-running commands intended to
put the device into a certain desired state.
// For example, set the telemetry send interval to 30 minutes. You can
get Properties using following method.

   oClient.Get_DeviceTwinsProperties('1');

// 3. Cloud-to-device messages for one-way notifications to the device
app. To get messages, first you must subscribe.

   oClient.Subscribe_CloudToDevice;


// Messages are received OnMQTTPublish event.

procedure TFRMSGCClientIoT.AzureIoTMQTTPublish(Connection:
TsgcWSConnection; aTopic, aText: string);
begin
  DoLog('Received Message: ' + aTopic + ' ' + aText);
end;
```

HTTP

HTTP

HTTP protocol allows to fetch resources from servers like images, html documents...it's a slicent-server protocol which means that client request to server which resources need.

When a client wants connect to a server, follows next steps:

1. Open a new TCP connection
2. Sends a message to server with data requested

```
GET / HTTP/1.1
Host: server.com
Accept-Language: en-us
```

3. Read response sent by server

```
HTTP/1.1 200 OK
Server: Apache
Content-Length: 120
Content-Type: text/html

...
```

Components

- **OAuth2:** OAuth2 allows third-party applications to receive a limited access to an HTTP service
- **Amazon SQS:** is a fully managed message queues for microservices, distributed systems, and serverless applications.
- **Google Cloud Pub/Sub:** provides messaging between applications and is designed to provide reliable, many-to-many, asynchronous messaging between applications.

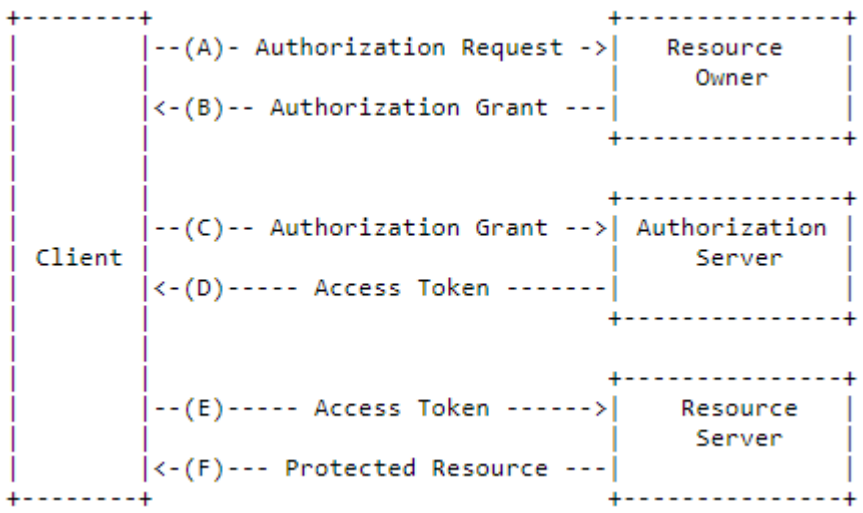
Authorization

HTTP | OAuth2

OAuth2 allows third-party applications to receive a limited access to an HTTP service which is either on behalf of a resource owner or by allowing a third-party application obtain access on its own behalf. Thanks to OAuth2, service providers and consumer applications can interact with each other in a secury way.

In OAuth2, there are 4 roles:

- **Resource Owner:** the user.
  - **Resource Server:** the server that hosts the protected resources and provides access to it based on the access token.
- **Client:** the external application that seeks permission.
- **Authorization Server:** issues the access token after having authenticated the user.



TsgcHTTP_OAuth2

This component allows to handle flow between client and the other roles, basically, when you set Active := True, opens a new Web Browser and requests user grant authorization, if successful, authorization server sends a token to application which is processed and with this token, client can connect to resource server. This component, starts a simple HTTP server which handles authorization server responses and uses an HTTP client to request Access Tokens.

LocalServerOptions

When a client needs a new Access Token, automatically starts an HTTP server to process response from Authorization server. This server is transparent for user and usually works in localhost. By default uses port 8080 but you can change if needed.

- **IP:** IP server listening, example: 127.0.0.1

- **Port:** by default 8080
- **RedirectURL:** (optional) allows to customized redirect url, example: http://localhost:8080/oauth/.

AuthorizationServerOptions

Here you must set URL for Authorization and Acces Token, usually these are provided in API specification. Scope is a list of all scopes requested by client.

- **AuthURL:** https://accounts.google.com/o/oauth2/auth
- **TokenURL:** https://accounts.google.com/o/oauth2/token
- **Scope:** https://mail.google.com/

OAuth2Options

ClientId is a mandatory field which informs server which is the identification of client. Check your API specification to know how get a ClientId. The same applies for client secret.
Sometimes, server requires a user and password to connect using Basic Authentication, if this is the case, you can setup this in Username/Password fields.

- **ClientId:** 180803918307-eqjtm20gqfhcs6gjklbbrreng022mqqc.apps.googleusercontent.com
- **ClientSecret:** _by1iYYrvVHxC2Z8TbtNEYJN
- **Username:**
- **Password:**

There are the following events to control the flow of OAuth2 process.

OnBeforeAuthorizeCode

```
// This is the first event, it's called before client opens a new Web
Browser session. URL parameter can be modified if needed (usually not
necessary).
procedure OnOAuth2BeforeAuthorizeCode(Sender: TObject; var URL:
string; var Handled: Boolean);
begin
  DoLog('BeforeAuthorizeCode: ' + URL);
end;
```

OnAfterAuthorizeCode

```
// After a successful Authorization, server redirects the response to
internal HTTP server, this response informs to client
// about Authorization code (which will be use later to get Access
Token), state, scope...
procedure OnOAuth2AfterAuthorizeCode(Sender: TObject; const Code,
State, Scope, RawParams: string; var Handled: Boolean);
begin
  DoLog('AfterAuthorizeCode: ' + Code);
end;
```

OnErrorAuthorizeCode

```
// If there is an error, this event will be raised with information
about error.
procedure OnOAuth2ErrorAuthorizeCode(Sender: TObject; const Error,
Error_Description, Error_URI, State, RawParams: string);
begin
  DoLog('ErrorAuthorizeCode: ' + Error + ' ' + Error_Description);
end;
```

OnBeforeAccessToken

```
// After get an Authorization Code, client connects to Authorization
Server to request a new Access Token. Before client connects,
// this event is called where you can modify URL and parameters
(usually not needed).
procedure OnOAuth2BeforeAccessToken(Sender: TObject; var URL,
Parameters: string; var Handled: Boolean);
begin
  DoLog('BeforeAccesToken: ' + URL + ' ' + Parameters);
end;
```

OnAfterAccessToken

```
// If server accepts client requests, it releases a new Access Token
which will be used by client to get access to resources server.
procedure OnOAuth2AfterAccessToken(Sender: TObject; const
Access_Token, Token_Type, Expires_In, Refresh_Token, Scope, RawParams:
    string; var Handled: Boolean);
begin
  DoLog('AfterAccessToken: ' + Access_Token + ' ' + Refresh_Token + '
' + Expires_In);
end;
```

OnErrorAccessToken

```
// If there is an error, this event will be raised with information
about error.
procedure OnOAuth2ErrorAccessToken(Sender: TObject; const Error,
Error_Description, Error_URI, RawParams: string);
begin
  DoLog('ErrorAccessToken: ' + Error + ' ' + Error_Description);
end;
```

OnBeforeRefreshToken

```
// Access token expire after some certain time. If Authorization
server releases a refresh token plus access token,
// client can connect after token has expires with a refresh token to
request a new access token without the need of user Authenticates
again
// with own credentials. This event is called before client requests a
new access token.
procedure ONOAuth2BeforeRefreshToken(Sender: TObject; var URL,
Parameters: string; var Handled: Boolean);
begin
  DoLog('BeforeRefreshToken: ' + URL + ' ' + Parameters);
end;
```

OnAfterRefreshToken

```
// If server accepts client requests, it releases a new Access Token
which will be used by client to get access to resources server.
procedure OnOAuth2AfterRefreshToken(Sender: TObject; const
Access_Token, Token_Type, Expires_In, Refresh_Token, Scope, RawParams:
    string; var Handled: Boolean);
begin
  DoLog('AfterRefreshToken: ' + Access_Token + ' ' + Refresh_Token + '
' + Expires_In);
end;
```

OnErrorRefreshToken

```
// If there is an error, this event will be raised with information
about error.
procedure OnOAuth2ErrorRefreshToken(Sender: TObject; const Error,
Error_Description, Error_URI, RawParams: string);
begin
  DoLog('ErrorRefreshToken: ' + Error + ' ' + Error_Description);
end;
```

OnHTTPResponse

```
// This event is called before HTTP response is sent after a
successful Access Token.
procedure OnOAuth2HTTPResponse(Sender: TObject; var Code: Integer; var
Text: string; Response: TObject; var Handled: Boolean);
begin
  Code := 200;
  Text := 'Successful Authorization';
end;
```

OAuth2 Code Example

```
// Example of use to connect to Google Gmail API using OAuth2.
oAuth2 := TsgcHTTP2_OAuth2.Create(nil);
oAuth2.LocalServerOptions.Host := '127.0.0.1';
oAuth2.LocalServerOptions.Port := 8080;
oAuth2.AuthorizationServerOptions.AuthURL :=
'https://accounts.google.com/o/oauth2/auth';
oAuth2.AuthorizationServerOptions.Scope.Add('https://mail.google.com/'
);
oAuth2.AuthorizationServerOptions.TokenURL :=
'https://accounts.google.com/o/oauth2/token';
oAuth2.OAuth2Options.ClientId := '180803918357-
eqjtn20gqfhcs6gjkebbrrenh022mqqc.apps.googleusercontent.com';
oAuth2.OAuth2Options.ClientSecret := '_by0iYYrvVHxC2Z8TbtNEYQN';

procedure OnOAuth2AfterAccessToken(Sender: TObject; const
Access_Token, Token_Type, Expires_In, Refresh_Token, Scope, RawParams:
    string; var Handled: Boolean);
begin



end;

oAuth2.OnAfterAccessToken := OnOAuth2AfterAccessToken;
oAuth2.Start;
```

AWS

Amazon AWS | SQS

What is Amazon SQS?

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS eliminates the complexity and overhead associated with managing and operating message oriented middleware, and empowers developers to focus on differentiating work. Using SQS, you can send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be available.

Benefits

Eliminate administrative overhead

> With SQS, there is no upfront cost, no need to acquire, install, and configure messaging software, and no time-consuming build-out and maintenance of supporting infrastructure.

Reliably deliver messages

> SQS lets you decouple application components so that they run and fail independently, increasing the overall fault tolerance of the system.

Keep sensitive data secure

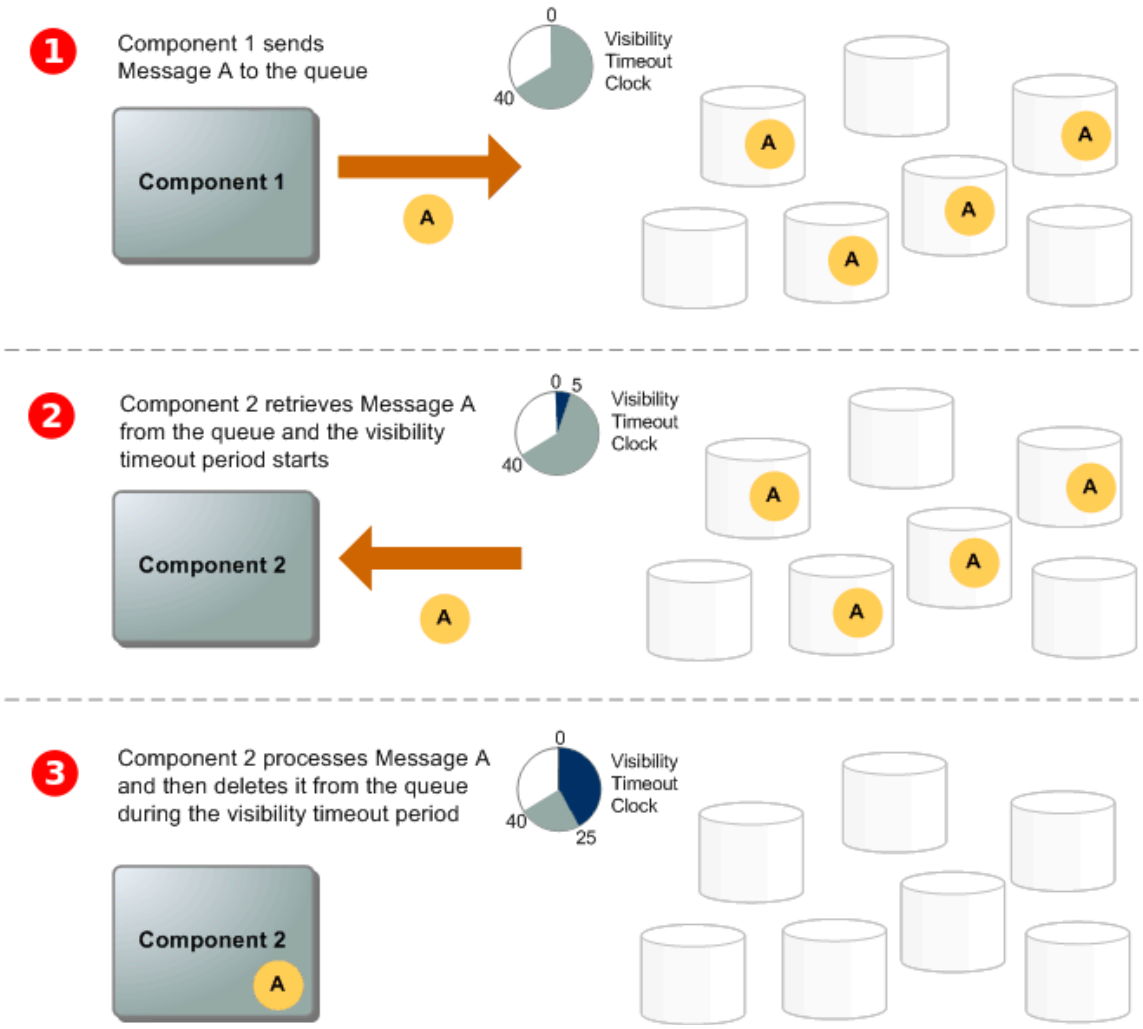
> You can use Amazon SQS to exchange sensitive data between applications using server-side encryption (SSE) to encrypt each message body.

Scale elastically and cost-effectively

> SQS scales elastically with your application so you don’t have to worry about capacity planning and pre-provisioning.

WorkFlow

The following scenario describes the lifecycle of an Amazon SQS message in a queue, from creation to deletion.



Getting Started with Amazon SQS

Before you begin, complete the steps in Setting Up Amazon SQS.

Step 1: Create a Queue

1. Sign in to the Amazon SQS console.
2. Choose Create New Queue.
3. On the Create New Queue page, ensure that you're in the correct region and then type the Queue Name.
4. Standard is selected by default. Choose FIFO.
5. To create your queue with the default parameters, choose Quick-Create Queue.

Your new queue is created and selected in the queue list.

Step 2: Send a Message

After you create your queue, you can send a message to it. The following example shows sending a message to an existing queue.

1. From the queue list, select the queue that you've created.
2. From Queue Actions, select Send a Message.
3. Your message is sent and the Send a Message to QueueName dialog box is displayed, showing the attributes of the sent message.

Step 3: Receive and Delete Your Message

After you send a message into a queue, you can consume it (retrieve it from the queue). When you request a message from a queue, you can't specify which message to get. Instead, you specify the maximum number of messages (up to 10) that you want to get.

Step 4: Delete Your Queue

If you don't use an Amazon SQS queue (and don't foresee using it in the near future), it is a best practice to delete it from Amazon SQS.

SQS Client

```
// TsgcHTTPAWS_SQS_Client is the component used for connect to Amazon
SQS.
// Client connects using HTTPs protocol and authenticates using Access
Key provided by Amazon.

// Before you try to connect to SQS service, you must set some data in
AWSOptions property.

// Region: your endpoint region, example: us-east-1.
// AccessKey: access key provided by Amazon.
// SecretKey: secret key provided by Amazon.

// The following methods are supported by SQS client:

// AddPermission
// Adds a permission to a queue for a specific principal. This allows
sharing access to the queue.

// ChangeMessageVisibility
// Changes the visibility timeout of a specified message in a queue to
a new value. The default visibility timeout for a message is 30
seconds.
// The minimum is 0 seconds. The maximum is 12 hours.

// ChangeMessageVisibilityBatch

// Changes the visibility timeout of multiple messages. This is a
batch version of ChangeMessageVisibility.
// The result of the action on each message is reported individually
in the response. You can send up to 10 ChangeMessageVisibility
requests.

// CreateQueue
// Creates a new standard or FIFO queue. You can pass one or more
attributes in the request.

  vURL := SQS.CreateQueue('sqs_queue');
  if vURL  '' then
    DoLog('#CreateQueue: ' + vURL);

// DeleteMessage
```

```
// Deletes the specified message from the specified queue. To select
the message to delete, use the ReceiptHandle of the message.

  if SQS.DeleteMessage('sqs_queue', '...receipt handle goes here...')
then
    DoLog('#DeleteMessage: ok');
  else
    DoLog('#DeleteMessage: error');

// DeleteMessageBatch
// Deletes up to ten messages from the specified queue. This is a
batch version of DeleteMessage. The result of the action on each
message is reported individually in the response.

// DeleteQueue
// Deletes the queue specified by the queue name, regardless of the
queue's contents.

  if SQS.DeleteQueue(txtQueueName.Text) then
    DoLog('#Delete Queue: ok')
  else
    DoLog('#Delete Queue: error');

// GetQueueAttributes
// Gets attributes for the specified queue.

  oAttributes := TsgcSQSAttributes.Create;
  Try
    if SQS.GetQueueAttributes('sqs_queue', oAttributes) then
    begin
      for i := 0 to oAttributes.Count - 1 do
        DoLog('#Attribute: ' + TsgcSQSAttribute(oAttributes.Item[i])
          .AttributeName + ' ' + TsgcSQSAttribute(oAttributes.Item[i])
          .AttributeValue);
    end
    else
      DoLog('#GetQueueAttributes: error');
  Finally
    FreeAndNil(oAttributes);
  End;

// GetQueueUrl
// Returns the URL of an existing Amazon SQS queue.

// ListDeadLetterSourceQueues
// Returns a list of your queues that have the RedrivePolicy queue
attribute configured with a dead-letter queue.

// ListQueueTags
// List all cost allocation tags added to the specified Amazon SQS
queue.

// PurgeQueue
// Deletes the messages in a queue specified by the QueueName
parameter.

  if SQS.PurgueQueue('sqs_queue') then
    DoLog('#PurgueQueue: ok')
  else
    DoLog('#PurgueQueue: error');
```

```
// ReceiveMessage
// Retrieves one or more messages (up to 10), from the specified
queue.

  oResponses := TsgcSQSReceiveMessageResponses.Create;
  Try
    if SQS.ReceiveMessage('sqs_test', oResponses) then
    begin
      for i := 0 to oResponses.Count - 1 do
      begin
        DoLog('#ReceiveMessage: ' +
TsgcSQSReceiveMessageResponse(oResponses.Item[i]).Body);
        FReceiptHandle :=
TsgcSQSReceiveMessageResponse(oResponses.Item[i]).ReceiptHandle;
      end;
    end;
  Finally
    FreeAndNil(oResponses);
  End;

// RemovePermission
// Revokes any permissions in the queue policy that matches the
specified Label parameter.

// SendMessage
// Delivers a message to the specified queue.

  if SQS.SendMessage('sqs_queue', 'My First Message') then
    DoLog('#SendMessage: ok')
  else
    DoLog('#SendMessage: error');

// SendMessageBatch
// Delivers up to ten messages to the specified queue. This is a batch
version of SendMessage.

// SetQueueAttributes
// Sets the value of one or more queue attributes. When you change a
queue's attributes, the change can take up to 60 seconds
// for most of the attributes to propagate throughout the Amazon SQS
system.

  oAttributes := TsgcSQSAttributes.Create;
  Try
    oAttributes.AddSQSAttribute(sqsatVisibilityTimeout, '45');
    if SQS.SetQueueAttributes('sqs_queue', oAttributes) then
      DoLog('#SetQueueAttributes: ok')
    else
      DoLog('#SetQueueAttributes: error');
  Finally
    FreeAndNil(oAttributes);
  End;

// TagQueue
// Add cost allocation tags to the specified Amazon SQS queue.

// UntagQueue
// Remove cost allocation tags from the specified Amazon SQS queue.
```

Events

OnSQSBeforeRequest

This event is called before sqs component does an HTTP request. You can get access to URL parameter and if Handled parameter is set to True, means component won't do an HTTP request.

OnSQSError

If there is any error when component do a request, this event will be called with Error Code and Error Description.

OnSQSResponse

This event is called after an HTTP request with raw response from server.

Google

Google Cloud | Pub/Sub

What is Google Cloud Pub/Sub?

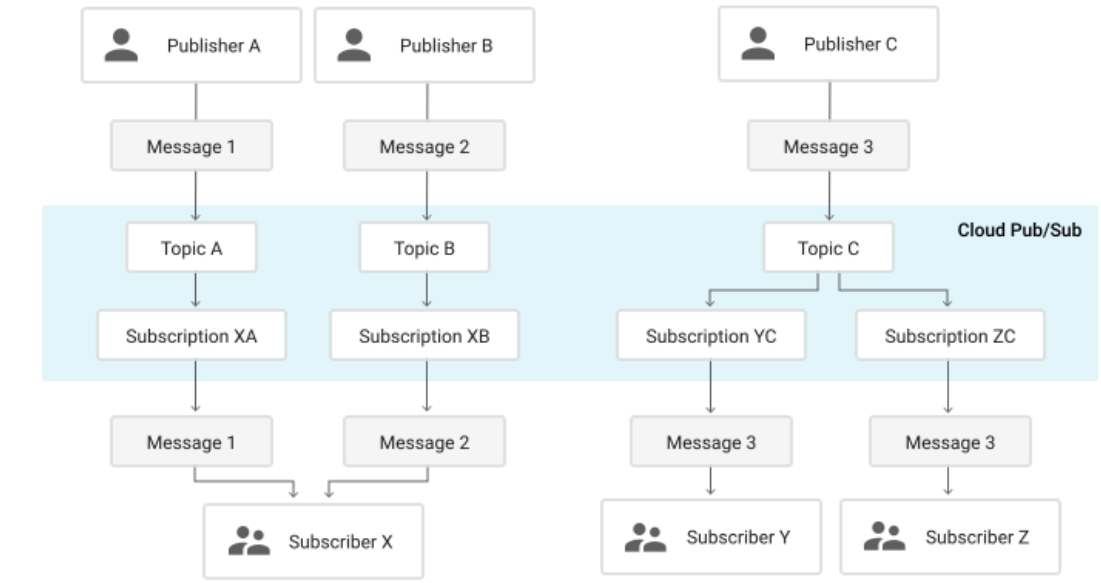
Pub/Sub brings the flexibility and reliability of enterprise message-oriented middleware to the cloud. At the same time, Pub/Sub is a scalable, durable event ingestion and delivery system that serves as a foundation for modern stream analytics pipelines. By providing many-to-many, asynchronous messaging that decouples senders and receivers, it allows for secure and highly available communication among independently written applications. Pub/Sub delivers low-latency, durable messaging that helps developers quickly integrate systems hosted on the Google Cloud Platform and externally.

Features

At-least-once delivery Synchronous, cross-zone message replication and per-message receipt tracking ensures at-least-once delivery at any scale.	**Open** Open APIs and client libraries in seven languages support cross-cloud and hybrid deployments.	**Exactly-once processing** Cloud Dataflow supports reliable, expressive, exactly-once processing of Cloud Pub/Sub streams.
Global by default Publish from anywhere in the world and consume from anywhere, with consistent latency. No replication necessary.	**No provisioning, auto-everything** Cloud Pub/Sub does not have shards or partitions. Just set your quota, publish, and consume.	**Compliance and security** Cloud Pub/Sub is a HIPAA-compliant service, offering fine-grained access controls and end-to-end encryption.
Integrated Take advantage of integrations with multiple services, such as Cloud Storage and Gmail update events and Cloud Functions for serverless event-driven computing.	**Seek and replay** Rewind your backlog to any point in time or a snapshot, giving the ability to reprocess the messages. Fast forward to discard outdated data.	

Publisher-subscriber relationships

A publisher application creates and sends messages to a topic. Subscriber applications create a subscription to a topic to receive messages from it. Communication can be one-to-many (fan-out), many-to-one (fan-in), and many-to-many.



Common use cases

- **Balancing workloads in network clusters.** For example, a large queue of tasks can be efficiently distributed among multiple workers, such as Google Compute Engine instances.
- **Implementing asynchronous workflows.** For example, an order processing application can place an order on a topic, from which it can be processed by one or more workers.
- **Distributing event notifications.** For example, a service that accepts user signups can send notifications whenever a new user registers, and downstream services can subscribe to receive notifications of the event.
- **Refreshing distributed caches.** For example, an application can publish invalidation events to update the IDs of objects that have changed.
- **Logging to multiple systems.** For example, a Google Compute Engine instance can write logs to the monitoring system, to a database for later querying, and so on.
- **Data streaming from various processes or devices.** For example, a residential sensor can stream data to backend servers hosted in the cloud.
- **Reliability improvement.** For example, a single-zone Compute Engine service can operate in additional zones by subscribing to a common topic, to recover from failures in a zone or region.

Configuration

Google Pub/Sub component client has the following properties:

- **GoogleCloudOptions.OAuth2.ClientId:** is the ClientID provided by Google to Authenticate through OAuth2 protocol.
- **GoogleCloudOptions.OAuth2.ClientSecret:** is the Client Secret string provided by Google to Authenticate through OAuth2 protocol.
- **GoogleCloudOptions.OAuth2.Scope:** is the scope of OAuth2, usually there is no need to modify the default value unless you need to get more access than default.
- **GoogleCloudOptions.OAuth2.LocalIP:** OAuth2 protocol requires a server listening answer from Authentication server, this is the IP or DNS. By default is 127.0.0.1.
- **GoogleCloudOptions.OAuth2.LocalPort:** Local server listening port.
- **GoogleCloudOptions.OAuth2.RedirectURL:** if you need to set a redirect url different from LocalPort + LocalIP, you can set in this property (example: http://127.0.0.1:8080/oauth2).

Google Pub/Sub Client

In order to work with Google Pub/Sub API, sgcWebSockets Pub/Sub component uses OAuth2 as default authentication, so first you must set your **ClientId** and **ClientSecret** from your google account.

```
oPubSub := TsgcHTTPGoogleCloud_PubSub_Client.Create(nil);
oPubSub.GoogleCloudOptions.OAuth2.ClientId := '... your google client
id...';
oPubSub.GoogleCloudOptions.OAuth2.ClientSecret := '... your google
client secret...';
```

This is required in order to get an Authorization Token Key from Google which will be used for all Rest API calls.

All methods return a response, which may be successful or return an error.

Projects.Snapshots

Method	Parameters	Description	Example
CreateSnapshot	project, snapshot, subscription	Creates a snapshot from the requested subscription. Snapshots are used in subscriptions.seek operations, which allow you to manage message acknowledgments in bulk. That is, you can set the acknowledgment state of messages in an existing subscription to the state captured by	`CreateSnapshot('pubsub-270909', 'snapshot-1', 'subscription-1')`

		a snapshot.	
DeleteSnapshot	project, snapshot	Removes an existing snapshot	`DeleteSnapshot('pubsub-270909', 'snapshot-1')`
ListSnapshots	project	Lists the existing snapshots	`ListSnapshots('pubsub-270909')`

Projects.Subscriptions

Method	Parameters	Description	Example
AcknowledgeSubscription			
CreateSubscription	project, subscription, topic	Creates a subscription to a given topic. If the subscription already exists, returns ALREADY_EXISTS. If the corresponding topic doesn't exist, returns NOT_FOUND.	`CreateSubscription('pubsub-270909', 'subscription-1', 'topic-1')`
DeleteSubscripton	project, subscription	Deletes an existing subscription. All messages retained in the subscription are immediately dropped.	`DeleteSubscription('pubsub-270909', 'subscription-1')`
GetSubscription	project, subscription	Gets the configuration details of a subscription.	`GetSubscription('pubsub-270909', 'subscription-1')`
ListSubscriptions	project	Lists matching subscriptions.	`ListSubscriptions('pubsub-270909', 'subscription-1')`
ModifyAckDeadlineSubscription	project, subscription, AckIds	Modifies the ack deadline for a specific message. This method is useful to indicate that more time is needed to process a message by the subscriber, or to make the message available for redelivery if the processing was interrupted. Note that this does not modify the subscription-level ackDeadlineSeconds used for subsequent messages.	
ModifyPushConfigSubscription	project, subscription	Modifies the PushConfig for a specified subscription.This may be used to change a push	

		subscription to a pull one (signified by an empty PushConfig) or vice versa, or change the endpoint URL and other attributes of a push subscription. Messages will accumulate for delivery continuously through the call regardless of changes to the PushConfig.	
Pull	project, subscription	Pulls messages from the server. The server may return UNAVAILABLE if there are too many concurrent pull requests pending for the given subscription.	`pull('pubsub-270909', 'subscription-1')`
Seek	project, subscription, timeUTC, snapshot	Seeks an existing subscription to a point in time or to a given snapshot, whichever is provided in the request. Snapshots are used in subscriptions.seek operations, which allow you to manage message acknowledgments in bulk. That is, you can set the acknowledgment state of messages in an existing subscription to the state captured by a snapshot. Note that both the subscription and the snapshot must be on the same topic.	

Projects.Topics

Method	Parameters	Description	Example
CreateTopic	project, topic	Creates the given topic with the given name	`CreateTopic('pubsub-270909', 'topic-1')`
DeleteTopic	project, topic	Deletes the	`DeleteTopic('pubsub-`

		topic with the given name. Returns NOT_FOUND if the topic does not exist. After a topic is deleted, a new topic may be created with the same name; this is an entirely new topic with none of the old configuration or subscriptions.	`270909', 'topic-1')`
GetTopic	project, topic	Gets the configuration of a topic.	`GetTopic('pubsub-270909', 'topic-1')`
ListTopics	project	Lists matching topics.	`ListTopics('pubsub-270909')`
Publish	project, topic, message	Adds one or more messages to the topic. Returns NOT_FOUND if the topic does not exist.	`Publish('pubsub-270909', 'topic-1', 'My First PubSub Message.')`

Projects.Topics.Subscriptions

Method	Parameters	Description	Example
ListTopicSubscriptions	project, topic	Lists the names of the subscriptions on this topic.	`ListTopicSubscriptions('pubsub-270909', 'topic-1')`

Most common methods

Find below the most common methods used with Google Cloud Pub/Sub API

How create a new Topic

Create a new topic for project with id: pubsub-270909 and topic name topic-1.

```
oPubSub := TsgcHTTPGoogleCloud_PubSub_Client.Create(nil);
oPubSub.GoogleCloudOptions.OAuth2.ClientId := '... your google client
id...';
oPubSub.GoogleCloudOptions.OAuth2.ClientSecret := '... your google
client secret...';
oPubSub.CreateTopic('pubsub-270909', 'topic-1');
```

Response from Server

```
{
  "name": "projects/pubsub-270909/topics/topic-1"
}
```

Publish a message

Publish a new message in new topic created

```
oPubSub := TsgcHTTPGoogleCloud_PubSub_Client.Create(nil);
oPubSub.GoogleCloudOptions.OAuth2.ClientId := '... your google client
id...';
oPubSub.GoogleCloudOptions.OAuth2.ClientSecret := '... your google
client secret...';
oPubSub.Publish('pubsub-270909', 'topic-1', 'My First Message from
sgcWebSockets.'));
```

Response from Server

```
{
  "messageIds": [
    "1050732082561505"
  ]
}
```

How Create a new Subscription

Create a new subscription for project with id: pubsub-270909, with subscription name subscription-1 and topic-1

```
oPubSub := TsgcHTTPGoogleCloud_PubSub_Client.Create(nil);
oPubSub.GoogleCloudOptions.OAuth2.ClientId := '... your google client
id...';
oPubSub.GoogleCloudOptions.OAuth2.ClientSecret := '... your google
client secret...';
oPubSub.CreateSubscription('pubsub-270909', 'subscription-1', 'topic-
1');
```

Response from Server

```
{
  "name": "projects/pubsub-270909/subscriptions/subscription-1",
  "topic": "projects/pubsub-270909/topics/topic-1",
  "pushConfig": {},
  "ackDeadlineSeconds": 10,
  "messageRetentionDuration": "604800s",
  "expirationPolicy": {
    "ttl": "2678400s"
  }
```

```
}
```

How Read messages from Subscription

Read messages from previous subscription created.

```
oPubSub := TsgcHTTPGoogleCloud_PubSub_Client.Create(nil);
oPubSub.GoogleCloudOptions.OAuth2.ClientId := '... your google client
id...';
oPubSub.GoogleCloudOptions.OAuth2.ClientSecret := '... your google
client secret...';
oPubSub.pubsub.Pull('pubsub-270909', 'subscription-1');
```

Response from Server

```
{
  "receivedMessages": [
    {
      "ackId": "PjA-
RVNEUAYWLF1GSFE3GQhoUQ5PXiM_NSAoRREFC08CKF15MEorQVh0Dj4N",
      "message": {
        "data": "TXkgRmlyc3QgTWVzc2FnZSBmcm9tIHNnY1dlYlNvY2tldHMu",
        "messageId": "1050732082561505",
        "publishTime": "2020-03-14T15:25:31.505Z"
      }
    }
  ]
}
```

Message is received Encode in Base64, so you must decode first to read contents.

```
sgcBase_Helpers.DecodeBase64('TXkgRmlyc3QgTWVzc2FnZSBmcm9tIHNnY1dlYlNv
Y2tldHMu=');
```

Reference

WebSockets

WebSocket is a web technology providing for bi-directional, full-duplex communications channels, over a single Transmission Control Protocol (TCP) socket.

The WebSocket API is being standardized by the W3C, and the WebSocket protocol has been standardized by the IETF as RFC 6455.
WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. The WebSocket protocol makes possible more interaction between a browser and a web site, facilitating live content and the creation of real-time games. This is made possible by providing a standardized way for the server to send content to the browser without being solicited by the client, and allowing for messages to be passed back and forth while keeping the connection open. In this way a two-way (bi-direction) ongoing conversation can take place between a browser and the server. A similar effect has been done in non-standardized ways using stop-gap technologies such as comet.

In addition, the communications are done over the regular TCP port number 80, which is of benefit for those environments which block non-standard Internet connections using a firewall. WebSocket protocol is currently supported in several browsers including Firefox, Google Chrome, Internet Explorer and Safari. WebSocket also requires web applications on the server to be able to support it.

More Information
Browser Support

JSON

JSON or **JavaScript Object Notation**, is a text-based open standard designed for human-readable data interchange. It is derived from the JavaScript scripting language for representing simple data structures and associative arrays, called objects. Despite its relationship to JavaScript, it is language-independent, with parsers available for many languages.

The JSON format is often used for serializing and transmitting structured data over a network connection. It is used primarily to transmit data between a server and web application, serving as an alternative to XML.

More Information

JSON-RPC 2.0

JSON-RPC is a stateless, light-weight remote procedure call (RPC) protocol. Primarily this specification defines several data structures and the rules around their processing. It is transport agnostic in that the concepts can be used within the same process, over sockets, over http, or in many various message passing environments. It uses JSON (RFC 4627) as data format.

Example: client call method subtract with 2 params (42 and 23). Server sends a result of 19.

Client To Server --> `{"jsonrpc": "2.0", "method": "subtract", "params": [42, 23], "id": 1}`

Server To Client<-- `{"jsonrpc": "2.0", "result": 19, "id": 1}`

Parsers

sgcWebSockets provides a built-in JSON component, but you can use your own JSON parser. Just implement following interfaces located at sgcJSON.pas:

IsgcJSON
IsgcObjectJSON

There are 3 implementations of theses interfaces

- **sgcJSON.pas:** default JSON parser provided.
- **sgcJSON_System.pas:** uses JSON parser provided with latest versions of delphi.
- **sgcJSON_XSuperObject.pas:** uses JSON library written by Onur YILDIZ, you can download sources from: https://github.com/onryldz/x-superobject

To use your own JSON parser or use some of the JSON parsers provided, just call **SetJSONClass** in your initialization method. For example: if you want use XSuperObject JSON parser, just call:

```
SetJSONClass(TsgcXSOJSON)
```

If you don't call this method, sgcJSON will be used by default.

More information

WAMP

The WebSocket Application Messaging Protocol (WAMP) is an open WebSocket subprotocol that provides two asynchronous messaging patterns: RPC and PubSub.

The WebSocket Protocol is already built into modern browsers and provides bidirectional, low-latency message-based communication. However, as such, WebSocket it is quite low-level and only provides raw messaging.

Modern Web applications often have a need for higher level messaging patterns such as Publish & Subscribe and Remote Procedure Calls.

This is where The WebSocket Application Messaging Protocol (WAMP) enters. WAMP adds the higher level messaging patterns of RPC and PubSub to WebSocket - within one protocol.

Technically, WAMP is an officially registered WebSocket subprotocol (runs on top of WebSocket) that uses JSON as message serialization format.

More Information

WebRTC

WebRTC is a free, open project that enables web browsers with Real-Time Communications (RTC) capabilities via simple Javascript APIs. The WebRTC components have been optimized to best serve this purpose. The WebRTC initiative is a project supported by Google, Mozilla and Opera.

WebRTC offers web application developers the ability to write rich, real-time multimedia applications (think video chat) on the web, without requiring plugins, downloads or installs. Its purpose is to help build a strong RTC platform that works across multiple web browsers, across multiple platforms.

More Information

MQTT

MQTT (MQ Telemetry Transport or Message Queue Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based "lightweight" messaging protocol for use on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited. The publish-subscribe messaging pattern requires a message broker. The broker is responsible for distributing messages to interested clients based on the topic of a message. Andy Stanford-Clark and Arlen Nipper of Cirrus Link Solutions authored the first version of the protocol in 1999.

The specification does not specify the meaning of "small code footprint" or the meaning of "limited network bandwidth". Thus, the protocol's availability for use depends on the context. In 2013, IBM submitted MQTT v3.1 to the OASIS specification body with a charter that ensured only minor changes to the specification could be accepted.MQTT-SN is a variation of the main protocol aimed at embedded devices on non-TCP/IP networks, such as ZigBee.
Historically, the "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. However, queuing itself is not required to be supported as a standard feature in all situations.

Specification
More Info

Server-Sent Events

Server-sent events (SSE) is a technology for where a browser gets automatic updates from a server via HTTP connection. The Server-Sent Events EventSource API is standardized as part of HTML5 by the W3C.

A server-sent event is when a web page automatically gets updates from a server. This was also possible before, but the web page would have to ask if any updates were available. With server-sent events, the updates come automatically.

Examples: Facebook/Twitter updates, stock price updates, news feeds, sport results, etc.

More information
Browser Support

OAuth2

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, and GitHub. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices.

Read more
Specification

License

License

eSeGeCe Components End-User License Agreement
eSeGeCe Components ("eSeGeCe") End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the Author of eSeGeCe for all the eSeGeCe components which may include associated software components, media, printed materials, and "online" or electronic documentation ("eSeGeCe components"). By installing, copying, or otherwise using the eSeGeCe components, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the program between you and the Author of eSeGeCe, (referred to as "LICENSER"), and it supersedes any prior proposal, representation, or understanding between the parties. If you do not agree to the terms of this EULA, do not install or use the eSeGeCe components.
The eSeGeCe components are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The eSeGeCe components are licensed, not sold.
If you want SOURCE CODE you need to pay the registration fee. You must NOT give the license keys and/or the full editions of eSeGeCe (including the DCU editions and Source editions) to any third individuals and/or entities. And you also must NOT use the license keys and/or the full editions of eSeGeCe from any third individuals' and/or entities'.
1. GRANT OF LICENSE
The eSeGeCe components are licensed as follows:
(a) Installation and Use.
LICENSER grants you the right to install and use copies of the eSeGeCe components on your computer running a validly licensed copy of the operating system for which the eSeGeCe components were designed [e.g., Windows 2000, Windows 2003, Windows XP, Windows ME, Windows Vista, Windows 7, Windows 8, Windows 10].
(b) Royalty Free.
You may create commercial applications based on the eSeGeCe components and distribute them with your executables, no royalties required.
(c) Modifications (Source editions only).
You may make modifications, enhancements, derivative works and/or extensions to the licensed SOURCE CODE provided to you under the terms set forth in this license agreement.
(d) Backup Copies.
You may also make copies of the eSeGeCe components as may be necessary for backup and archival purposes.
2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS
(a) Maintenance of Copyright Notices.
You must not remove or alter any copyright notices on any and all copies of the eSeGeCe components.
(b) Distribution.
You may not distribute registered copies of the eSeGeCe components to third parties. Evaluation editions available for download from the eSeGeCe official websites may be freely distributed.
You may create components/ActiveX controls/libraries which include the eSeGeCe components for your applications but you must NOT distribute or publish them to third parties.
(c) Prohibition on Distribution of SOURCE CODE (Source editions only).
You must NOT distribute or publish the SOURCE CODE, or any modification, enhancement, derivative works and/or extensions, in SOURCE CODE form to third parties.
You must NOT make any part of the SOURCE CODE be distributed, published, disclosed or otherwise made available to third parties.
(d) Prohibition on Reverse Engineering, Decompilation, and Disassembly.
You may not reverse engineer, decompile, or disassemble the eSeGeCe components, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

(e) Rental.
You may not rent, lease, or lend the eSeGeCe components.
(f) Support Services.
LICENSER may provide you with support services related to the eSeGeCe components ("Support Services"). Any supplemental software code provided to you as part of the Support Services shall be considered part of the eSeGeCe components and subject to the terms and conditions of this EULA.
eSeGeCe is licensed to be used by only one developer at a time. And the technical support will be provided to only one certain developer.
(g) Compliance with Applicable Laws.
You must comply with all applicable laws regarding use of the eSeGeCe components.
3. TERMINATION
Without prejudice to any other rights, LICENSER may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the eSeGeCe components in your possession.
4. COPYRIGHT
All title, including but not limited to copyrights, in and to the eSeGeCe components and any copies thereof are owned by LICENSER or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the eSeGeCe components are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by LICENSER.
5. NO WARRANTIES
LICENSER expressly disclaims any warranty for the eSeGeCe components. The eSeGeCe components are provided "As Is" without any express or implied warranty of any kind, including but not limited to any warranties of merchantability, non-infringement, or fitness of a particular purpose. LICENSER does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the eSeGeCe components. LICENSER makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb, or other such computer program. LICENSER further expressly disclaims any warranty or representation to Authorized Users or to any third party.
6. LIMITATION OF LIABILITY
In no event shall LICENSER be liable for any damages (including, without limitation, lost profits, business interruption, or lost information) rising out of "Authorized Users" use of or inability to use the eSeGeCe components, even if LICENSER has been advised of the possibility of such damages. In no event will LICENSER be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise. LICENSER shall have no liability with respect to the content of the eSeGeCe components or any part thereof, including but not limited to errors or omissions contained therein, libel, infringements of rights of publicity, privacy, trademark rights, business interruption, personal injury, and loss of privacy, moral rights or the disclosure of confidential information.

Index