

## SYSLOG Introduction

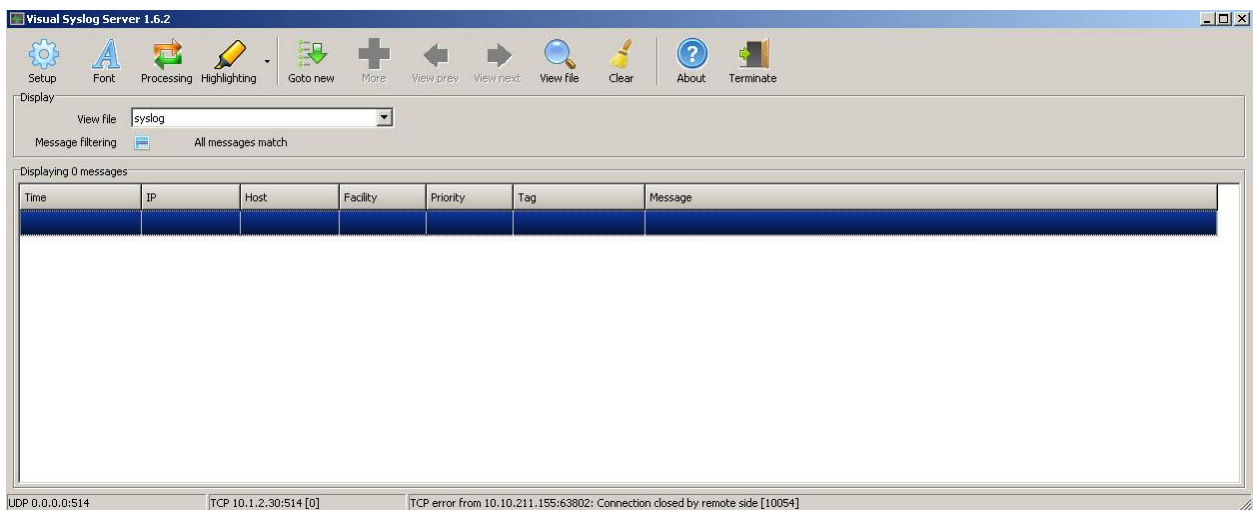
Syslog is a standard messaging service that can be used to monitor security and other events. It is available on the M580 using Unity Pro version 10.0 or greater. The following is a descriptive example of using syslog with Unity.

In a system using syslog the M580 acts as a client sending messages to a syslog server. Each message is time-stamped and an NTP or SNTP server must also be configured. This example uses a BME P58 1020 PAC. The NTP server is a TCSESM083F2CU0 Connexium switch. The syslog server is an open source server Visual Syslog. The configuration of each is described in the attachment.

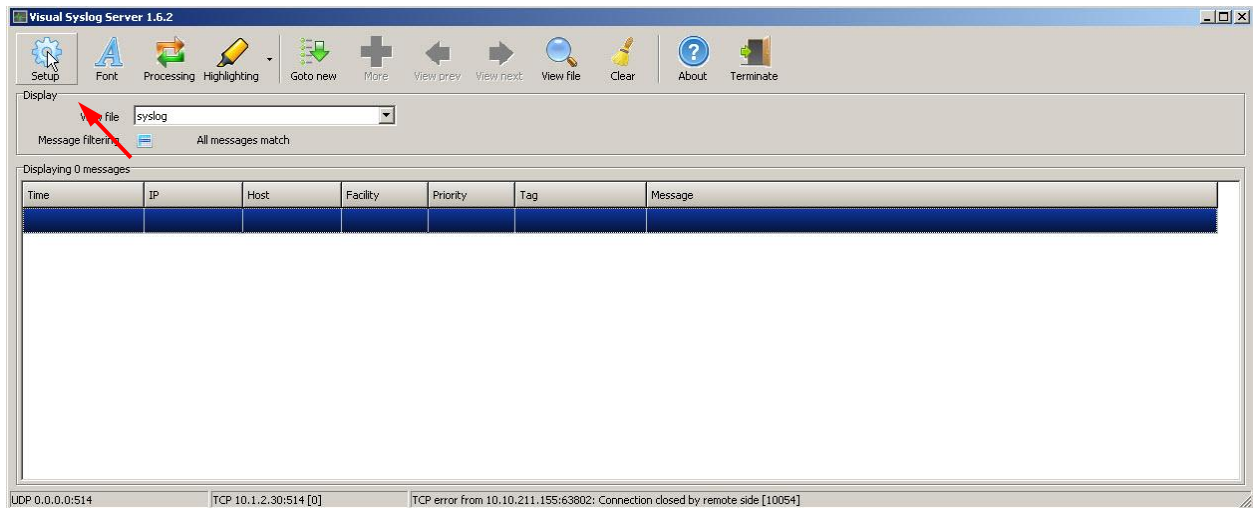
### Syslog server

Any syslog server may be used. Visual Syslog is a free open source server that can be downloaded at <http://maxbelkov.github.io/visualsyslog/>. It is available for Windows, simple to configure, and has a nice graphical interface.

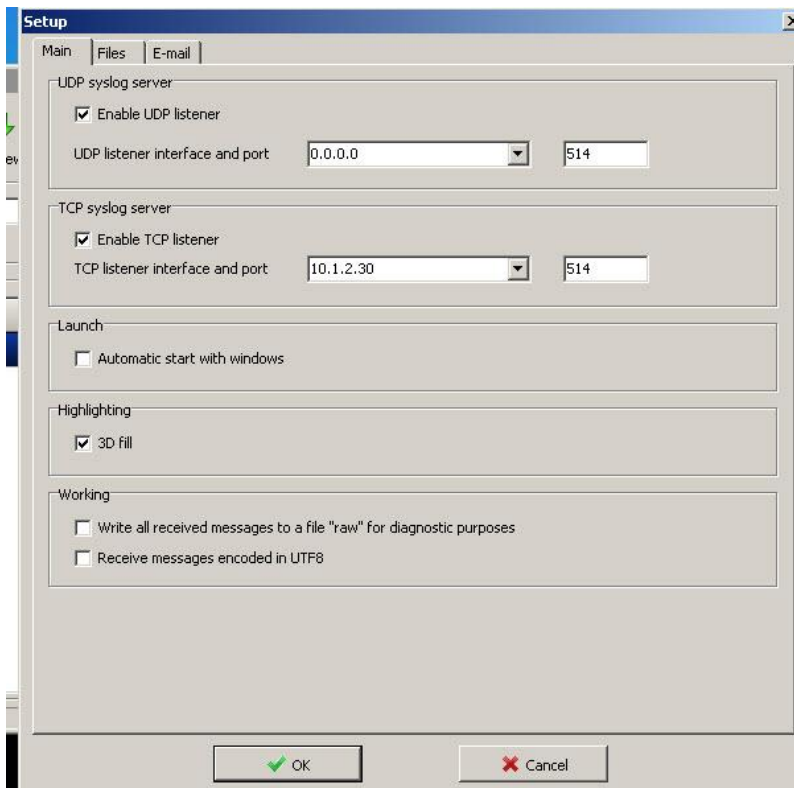
After installing and running visual syslog the initial screen appears



Click on Setup



We have to simply enter the IP address and the port that syslog will use. The M580 uses TCP so that is all we have to configure. The IP address of the PC that runs visual syslog has an address of 10.1.2.30. I have chosen port 514 although you can use any free port. This port must be the same as the one configured in UnityPro.

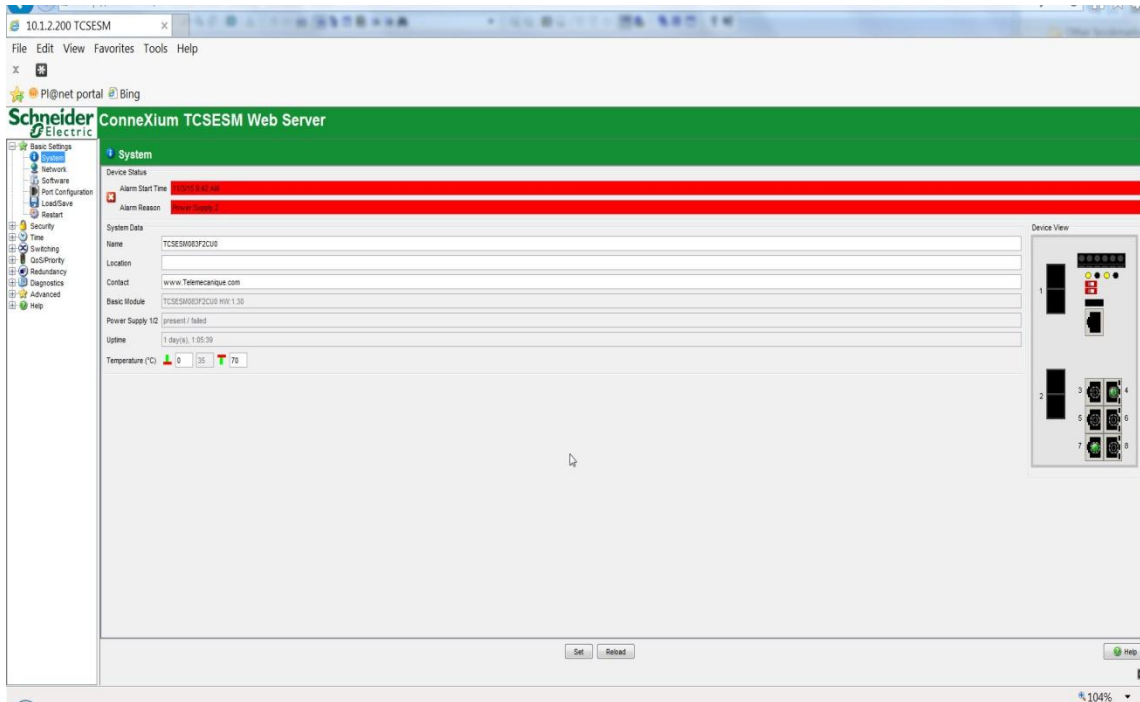


Click OK and leave the application running.

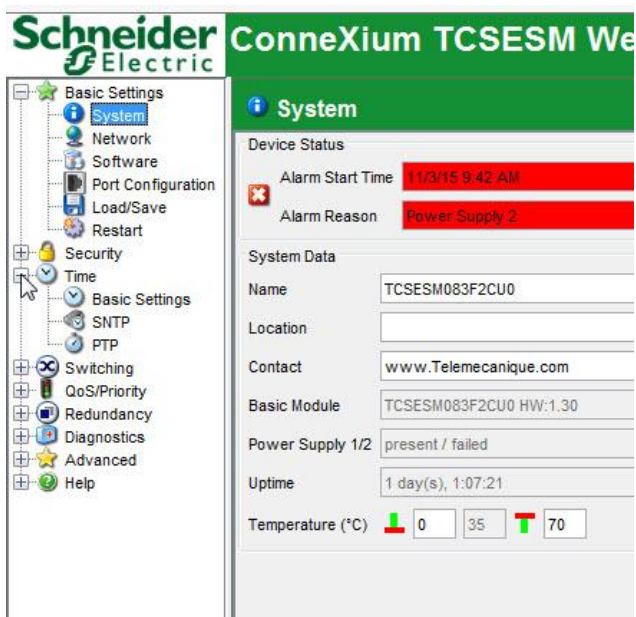
## NTP Server

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are exactly the same in their messages so we can use an SNTP server. Schneider Electric's Connexium switches can be configured as SNTP servers as follows.

Using a Web Browser that allows Java enter the IP address of the switch in the URL. The homepage of the switch will appear after logging in as admin the following screen appears



Click on the “+” next to Time in the left column.



Click on SNTP and the following appears. We are configuring an SNTP Server. All that has to be done is click the Server Status to On.

ConneXium TCESM Web Server

SNTP

Operation  
 On  Off

Configuration SNTP Client

Client Status  On  Off

External Server Address

Redundant Server Address

Server Request Interval [s]

Accept SNTP Broadcasts

Threshold for obtaining the UTC [ms]

Disable Client after successful Synchronization

Configuration SNTP Server

Server Status  On  Off

Anycast Destination Address

VLAN ID

Anycast Send Interval [s]

Disable Server at local Time Source

Set Reload

Then click Set.

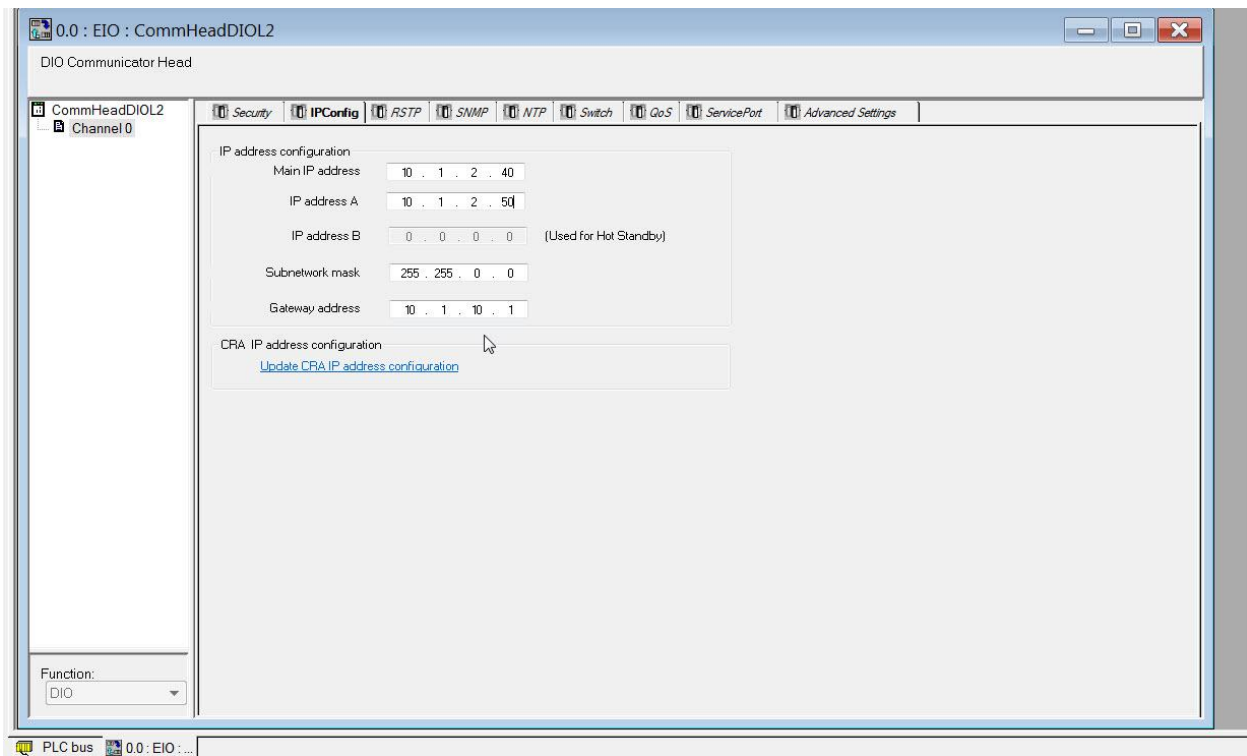
The SNTP Server will then be running.

### Configuring Syslog in Unity.

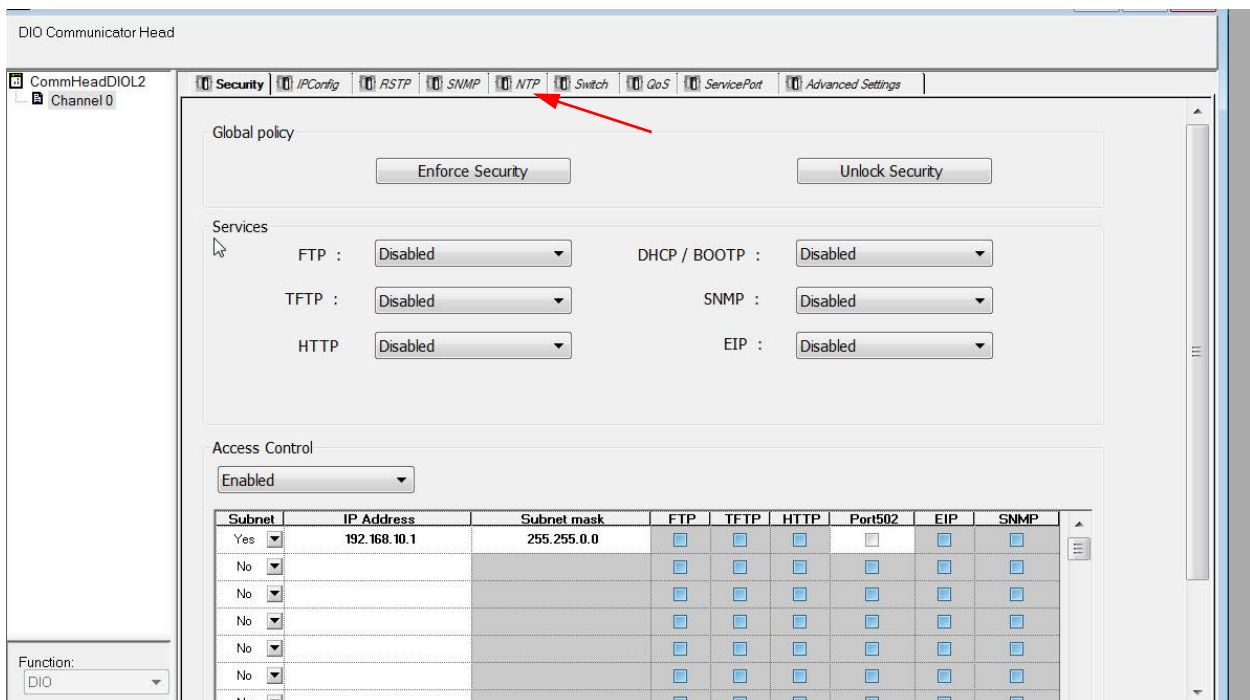
Open a new project in Unity choosing the M580 you are using. We are using a BMEP581030



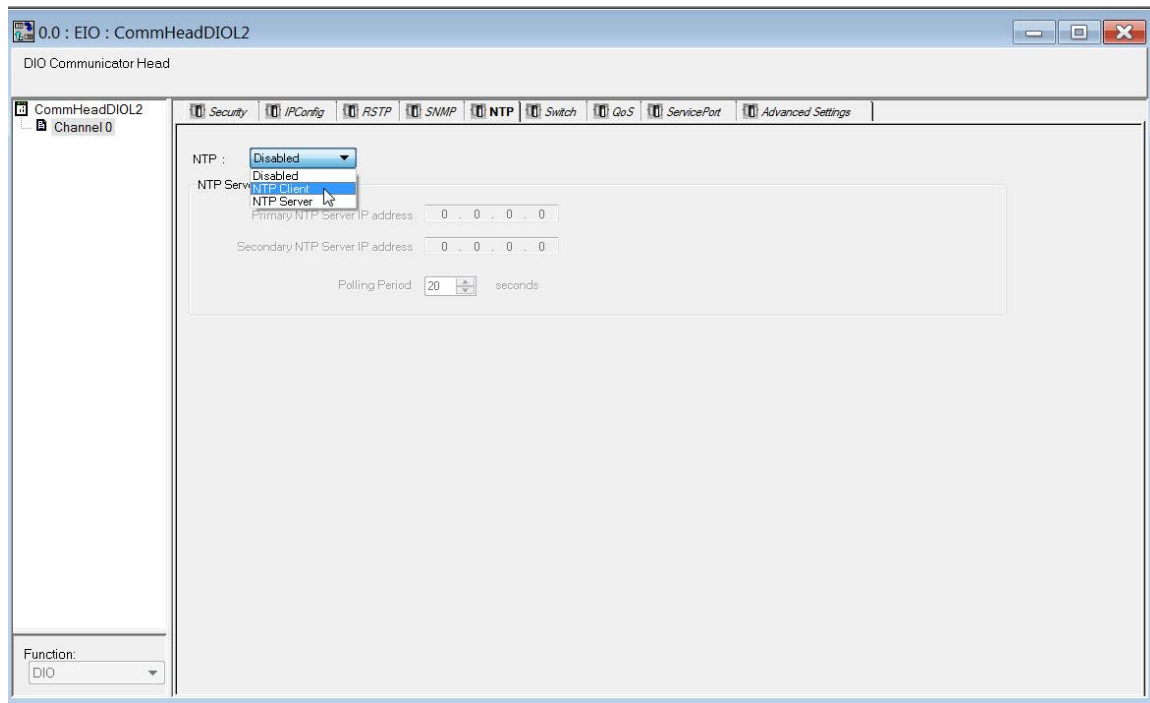
We will use the Main port to log the messages (IP 10.1.2.40).



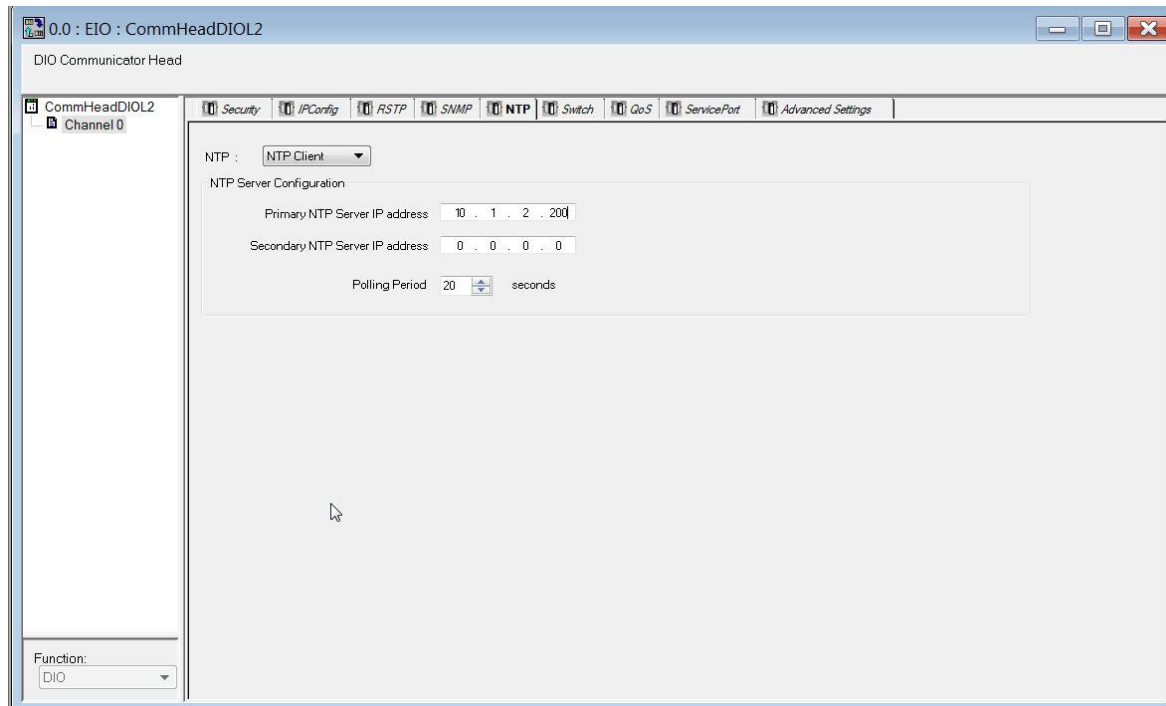
Now we will configure NTP. Click on the NTP Tab.



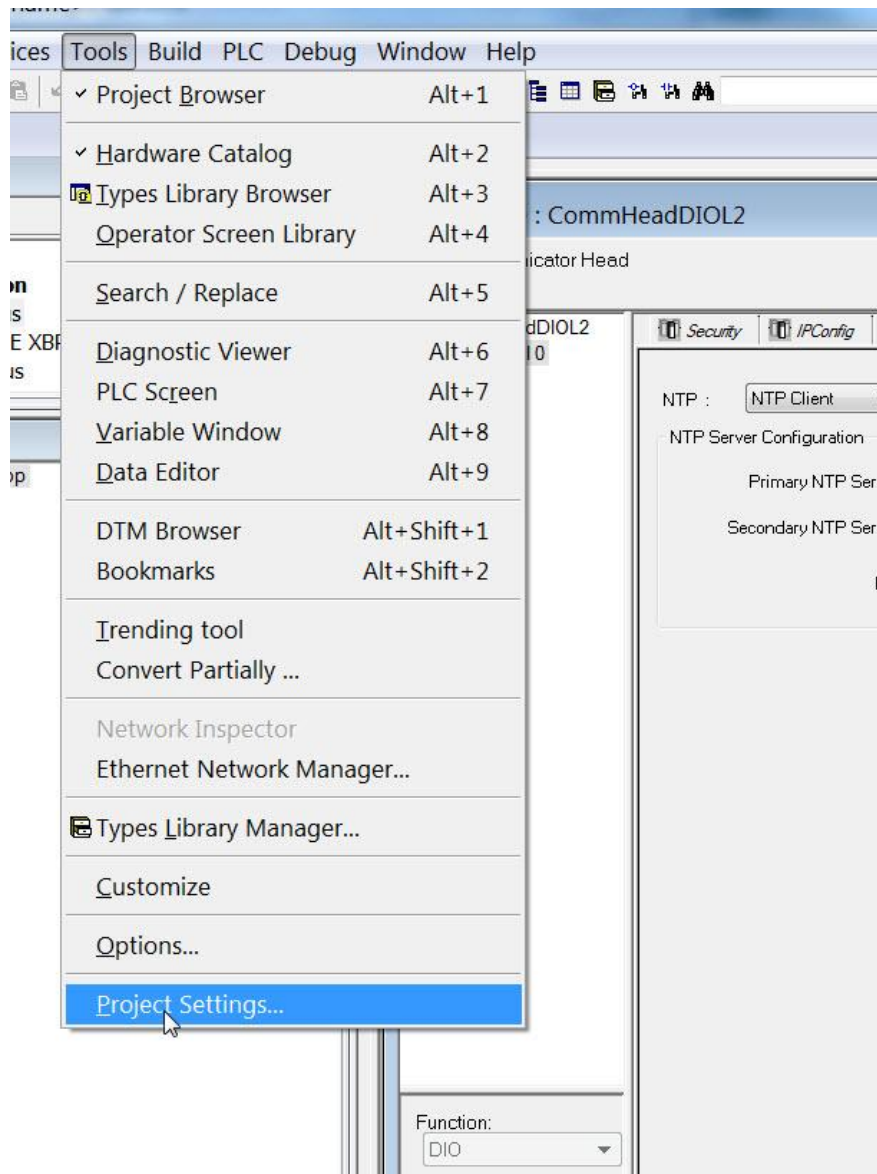
The following appears. Enable NTP client



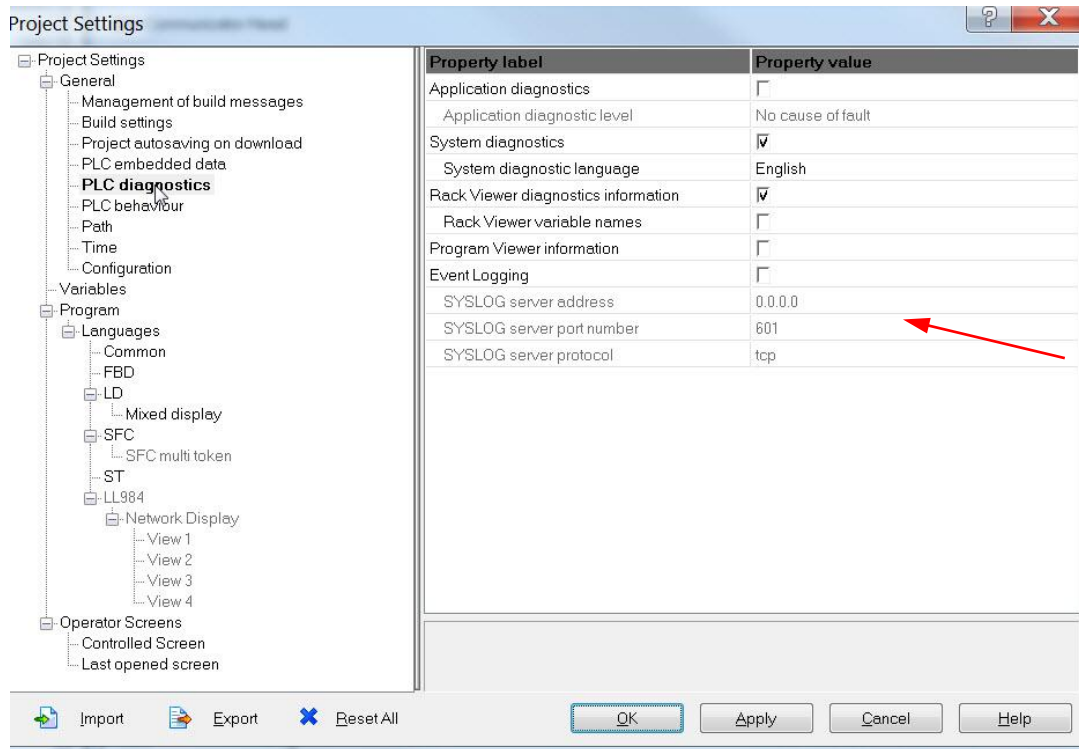
Enter the address of the NTP Server (the Connexium switch)



Now we will enable the syslog client. At the top of the screen click Tools, Project Settings.



Then choose PLC Diagnostics. Check the Event Logging box



Enter the IP address of the syslog server (10.1.2.30) and the same port number as the syslog server (514).

Property label	Property value
Application diagnostics	<input type="checkbox"/>
Application diagnostic level	No cause of fault
System diagnostics	<input checked="" type="checkbox"/>
System diagnostic language	English
Rack Viewer diagnostics information	<input checked="" type="checkbox"/>
Rack Viewer variable names	<input type="checkbox"/>
Program Viewer information	<input type="checkbox"/>
Event Logging	<input checked="" type="checkbox"/>
SYSLOG server address	10.1.2.30
SYSLOG server port number	514
SYSLOG server protocol	tcp

When the project has been built and runs the messages will appear in visual syslog.

The screenshot shows the Visual Syslog Server 1.6.2 application window. The interface includes a menu bar with options like Setup, Font, Processing, Highlighting, Goto new, More, View prev, View next, View file, Clear, About, and Terminate. Below the menu bar is a 'Display' section with a 'View file' dropdown set to 'syslog' and a 'Message filtering' section set to 'All messages match'. The main area displays a table of 23 messages. The table has columns for Time, IP, Host, Facility, Priority, Tag, and Message. The messages are color-coded: blue for notice/info, yellow for warning, and red for emergency. The status bar at the bottom shows 'UDP 0.0.0.0:514', 'TCP 10.1.2.30:514 [0]', and 'TCP error from 10.10.211.155:63802: Connection closed by remote side [10054]'.

Time	IP	Host	Facility	Priority	Tag	Message
Nov 02 14:59:35	10.1.2.40	1	logaudit	notice		1980-01-01T00:55:53.000Z 192.168.11.1 BMEP581020 NILVALUE DEVICE MANAGER @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:35	10.1.2.40	1	kern	info		1980-01-01T00:55:54.000Z 192.168.11.1 BMEP581020 NILVALUE Configuration @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:36	10.1.2.40	1	kern	info		1980-01-01T00:55:55.000Z 192.168.11.1 BMEP581020 NILVALUE Configuration @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:36	10.1.2.40	1	authpriv	warning		1980-01-01T00:56:08.000Z 192.168.11.1 BMEP581020 NILVALUE ETH @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:37	10.1.2.40	1	authpriv	emerg		1980-01-01T00:56:08.000Z 192.168.11.1 BMEP581020 NILVALUE RSTP @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:37	10.1.2.40	1	authpriv	emerg		1980-01-01T00:56:08.000Z 192.168.11.1 BMEP581020 NILVALUE RSTP @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:38	10.1.2.40	1	authpriv	emerg		1980-01-01T00:56:09.000Z 192.168.11.1 BMEP581020 NILVALUE RSTP @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:38	10.1.2.40	1	logaudit	notice		1980-01-01T00:58:25.000Z 192.168.11.1 BMEP581020 NILVALUE DEVICE MANAGER @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:39	10.1.2.40	1	authpriv	emerg		1980-01-01T00:58:32.000Z 192.168.11.1 BMEP581020 NILVALUE Modbus @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }
Nov 02 14:59:39	10.1.2.40	1	authpriv	emerg		1980-01-01T00:58:36.000Z 192.168.11.1 BMEP581020 NILVALUE Modbus @cee: { "issuerAddr": "192.168.11.1", "peerId": "192.168.11.1" }