Server User Manual

Document Number:	Cloudworks Server User Manual
Client:	User
Date:	January 2020
Issue:	V 1.0
Status:	Draft
Classification:	Confidential
S/W File Name	Cloudworks Server User Manual Ver.docx

Copyright Cape Digital Solutions.
This document contains information relating to the rights of Cape Digital Solutions. The confidentiality agreement provisions are applicable to this document. When no longer needed for authorised purposes, this document must be destroyed or returned to Cape Digital Solutions.

Cape Digital Solutions reserves the right to change the design or specifications of their products without prior notice.

The contents of this manual are the property of Cape Digital Solutions and may not be copied or modified without prior permission, in writing, from Cape Digital Solutions, Cape Town, South Africa.

Table of Contents

1 System Architecture ..... Error! Bookmark not defined.

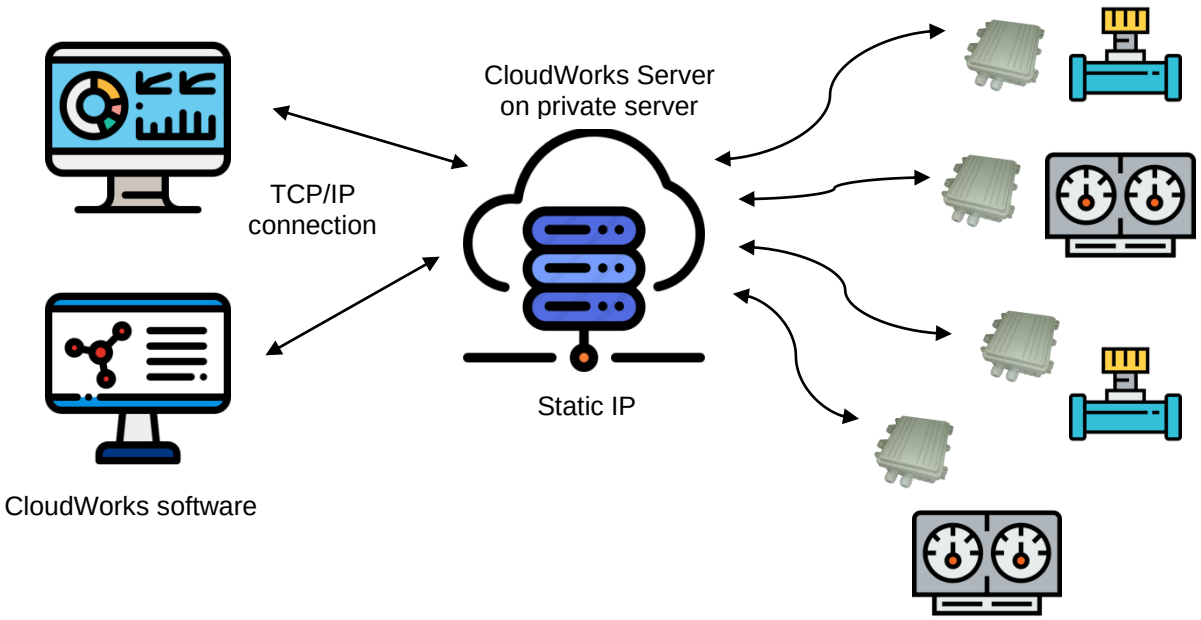
1.1 System Overview 3
1.2 MySQL Database Architecture 4
1.3 Logging in to Cloudworks Server 5
1.4 System Setup 7
1.5 Managing Vendors 10
1.6 Communications Status 12

1 CLOUDWORKS SERVER

1.1 System Overview

The main function of the **Cloudworks Server** software is to operate as a communications go between for the remote **Cloudworks** client software and the remote devices. This architecture allows the remote devices to operate on networks that only provide dynamic IP's such as most mobile operators. In order for them to communicate correctly to the user software, they need to connect via a server with a fixed IP. This can be on a private network or simply on an internet exposed server. Fully private networks can be established using VPN's etc.

It's secondary function is to extract the data from the remote devices and insert it into their respective databases, of which it can support multiples thereof. Each database has associated with it a 'Vendor Code' - this code is programmed onto each remote device so that when it connects to the server, **Cloudworks Server** will know into which database the data is to be inserted. The 'Vendor Code' also serves as a way of separating data communications between different remote systems.



VERY IMPORTANT:-

Cloudworks Server communicates with the outside world using two communications ports.

1. UDP Protocol on Port 13000 (connection to remote devices)
2. TCP Protocol on Port 13000 (connection to **Cloudworks** client/third party software)

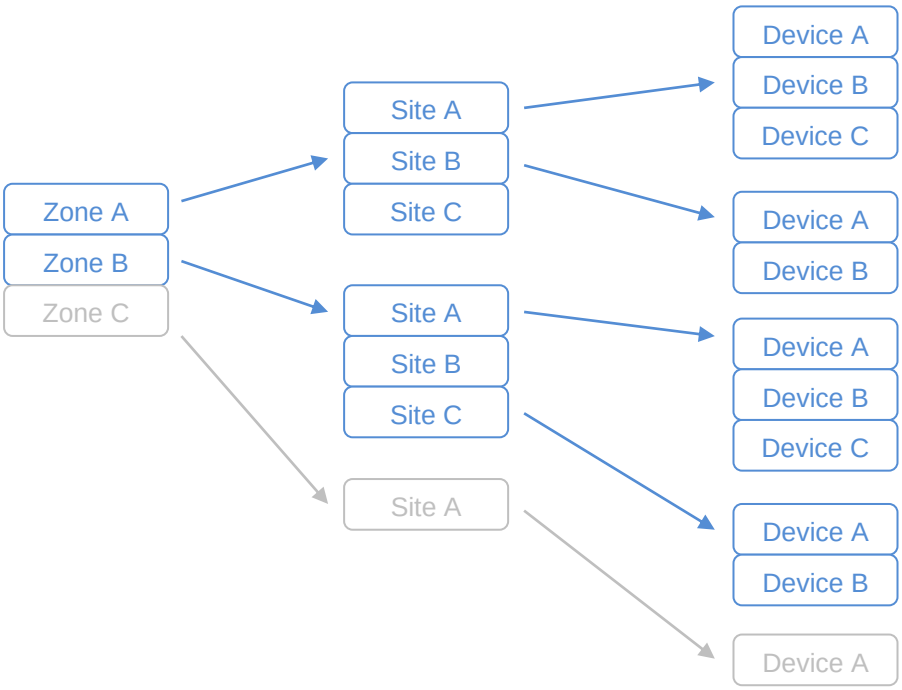
Both these ports need to be allowed by the firewall for communications. This can normally be done by your IT department. These are the default port numbers but they can be changed in the 'System Setup' screen.

A further requirement is for MySQL Server to be installed on the server hosting the database. This can be installed from MySQL Server install.

Please remember to write down the selected root access password when setting up the database manager. Losing this password may make it impossible to get access to your database in the future.

1.2 MySQL Database Architecture

Before logging into the system it would be best to discuss the architecture of the database. In order for it to be easier to navigate the devices in the field, the database has been divided in 3 groups at different levels. At the top most level are the zones. Zones could be geographical areas such as cities/countries or non-geographical entities such as clients etc. Within a zone there are sites. A site would be an installation within a zone, such as a building or basically a sub section of a zone. Contained in a site are all the devices associated with that site. For example a remote pump station with three loggers would have those three loggers listed within that site.



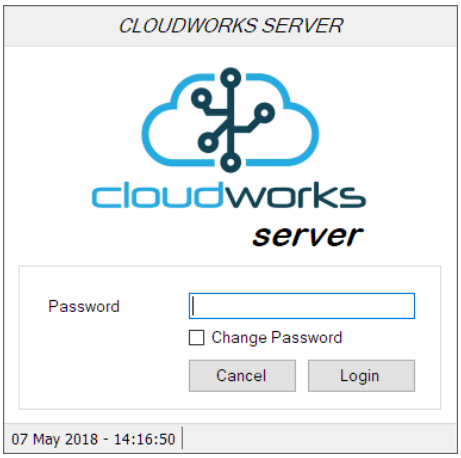
MySQL Database Architecture

Important Note:

The Cloudworks Server software supports multiple databases. What this means is that the server will automatically populate the database that is associated with a specific device. Each database and device has a Vendor Code assigned to it. Data is matched between these systems using that code. This code is also used to separate communications between different vendors, preventing the cross accessing of devices by unauthorised users.

1.3 Logging in to Cloudworks Server

Once Cloudworks Server has been installed (Cloudworks Server install), it can be run and the user can log in. Each time the software is run, it will automatically access the Cloudworks server and check if there is not perhaps a newer version available. Should a newer version be found, you will be prompted to install. Cloudworks Server is being continuously upgraded with new functions etc, so it would be advisable to always accept the newer version.



For a new system, there is no Password and you can simply log in directly. The purpose of the password is to simply try and restrict user access where possible. The server itself, should however, already be a user restricted system.

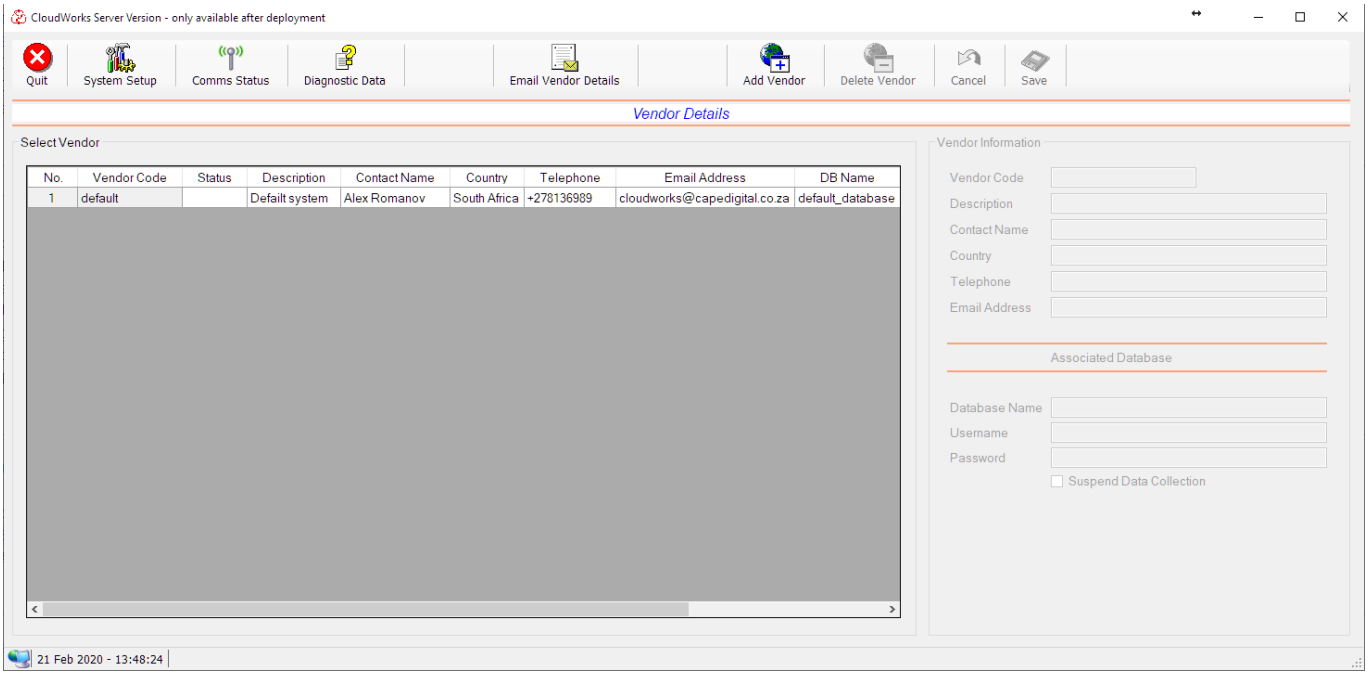
This password can be changed by ticking the 'Change Password' box on the Login screen. When this block is ticked, further entry fields will pop up that need your new password entered twice. The Login button will only be available if the two newly entered passwords are the same and not blank.



Very important to note is that although the user may not have logged in past this point, the Cloudworks Server software is already fully functional. Logging in is really just to allow access to the system to make changes etc.

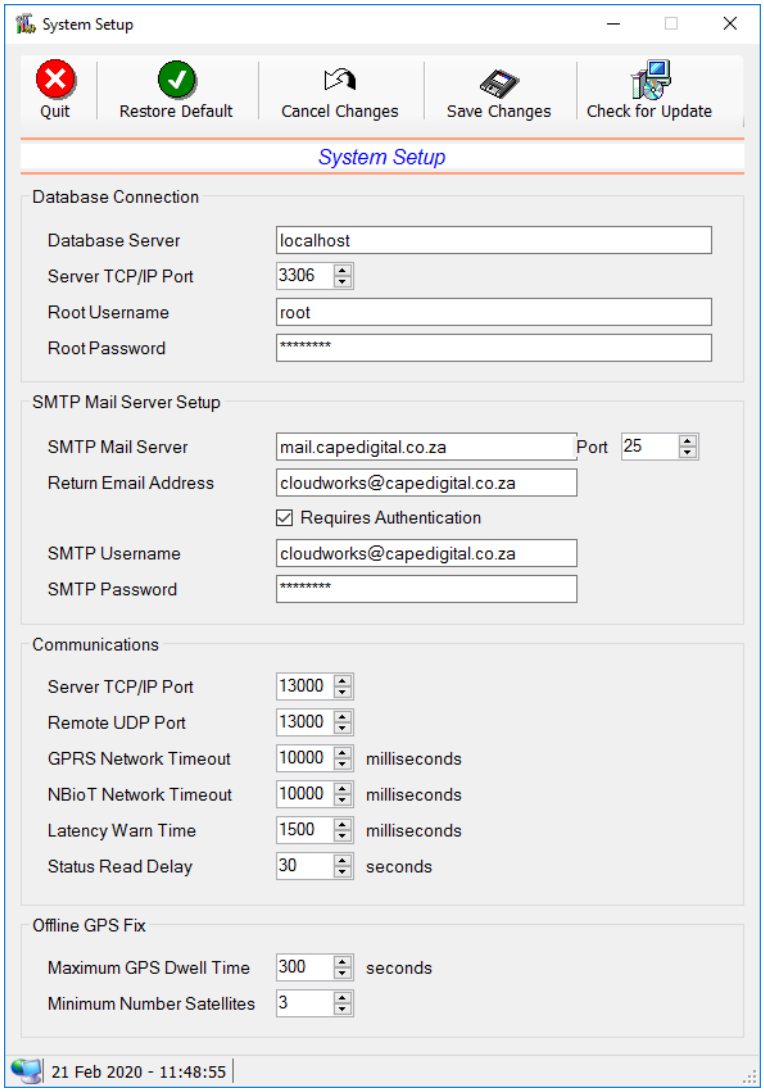
Once you have entered these details, you can press the 'Login' button to enter the system.

Operating of the Cloudworks Server software is fairly straight forward. It simply is maintenance of the different vendors and their associated databases. The main screen ('Vendor Details') screen opens to list all the registered vendors on the server.



1.4 System Setup

Before starting to use the **Cloudworks Server** software, it will be necessary to check the system setup parameters to ensure that the rest of the software will function correctly. The System Setup screen is accessed by pressing the 'System Setup' button in the tool bar. There are a few parameters that need to be setup under this section for the **Cloudworks Server** software to operate correctly.



Although the **Cloudworks Server** software goes and checks the server for updates every time it is run, it is also possible to do a direct check by pressing the 'Check for Update' button in the toolbar. First thing to do would be to check that your software is fully up to date. If a new update is available, you will be prompted through the whole update process.

The database connection details can be entered under the 'Database Connection' heading. If the database server is the same server which is running **Cloudworks Server**, then the 'Database Server' should be set to 'localhost'. It is possible to run **Cloudworks Server** on one server and populate a database on a completely different server. The 'Database Server' field should then be set to this other server.

Because this software operates globally on this database system, the Username and Password should have root access. With this level of access, it will be able to create or remove databases and/or users, one of its primary functions.

There are three other major parameters that need to be configured. One of them is the SMTP Mail Server Setup. The **Cloudworks Server** software uses a direct connection to your mail server for the sending of access data to newly captured vendors via email. SMTP protocols are used to send these mails and settings can be obtained from either your internet service provider or IT department. Please note that emails can normally only be sent through an SMTP server when you are connected to the particular network associated with that service provider. Sending an email from an external network is called 'relaying' and is blocked by most SMTP servers. This is to prevent SPAM mails being sent from an unknown user. If your mails are not being delivered, it will probably be for this reason.

The second set of parameters are important for the communications between the **Cloudworks Server** and the outside world. The 'Server TCP/IP Port' is the port to which the **Cloudworks** client software will connect to the server as well as all the remotes devices. This defaults to 13000 but can be changed to another port if there is a clash. Please remember though, each remote **Cloudworks** client program and all the remote device needs to be adjusted to this value as well.

The remaining parameters are used for advanced tweaking of the communications and should probably be left at their default values.

Once all these parameters have been set, press 'Save Changes' and restart the program when prompted.

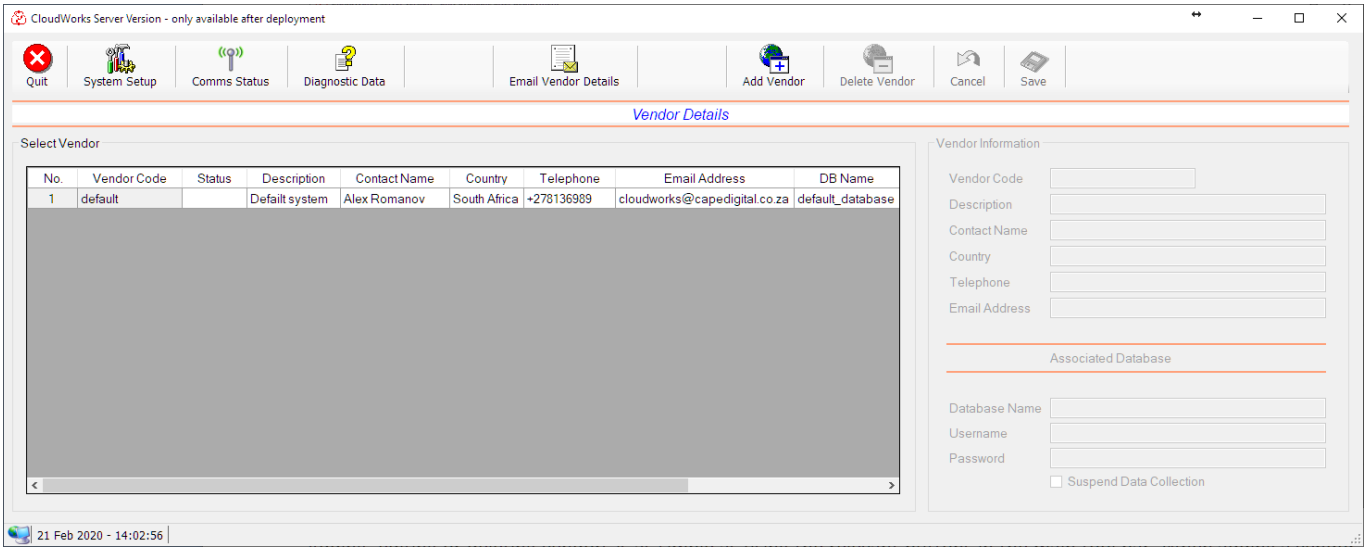
Parameter definitions:-

Parameter	Notes
Database Server	The Server Name or IP address of the server that is hosting your database.
Server TCP/IP Port	Computers make a connection to the MySQL Database Manager software on the server through a TCP/IP communications port. MySQL uses the port number 3306 as a default. This can be changed to another port in case of a clash or for enhanced security reasons. Please note that both the server and **Cloudworks** client software need to be operating on the same port for the connection to function.
Root Username	MySql Server root Username. Normally is just 'root'.
Root Password	Password for the root Username.
SMTP Mail Server	The Name or IP address of the server that is hosting your SMTP Mail server.
Return Email Address	When mails are sent out to an SMTP mail server, one of its prerequisites to sending is to also have a return email address (sender address) to which it can report if a mail has not been sent. The mail server also uses this to determine if this is a valid mail and not a SPAM mailer.
Requires Authentication	Tick this box if your mail server requires authentication when sending mails. Many SMTP servers do not require this as you are sending from their own networks and you would already be familiar to them.
SMTP Username	Your Username for the SMTP Server.
SMTP Password	Your Password for the SMTP Server.
Server TCP/IP Port	Communications port through which a TCP/UDP connection for comms to the outside world is initiated. This port number is by default 13000 but can be changed if it clashes with other systems.
GPRS Network Timeout	Time allowed for a command to propagate the whole system before it is considered to have failed. GPRS Network. Parameter is in milliseconds.

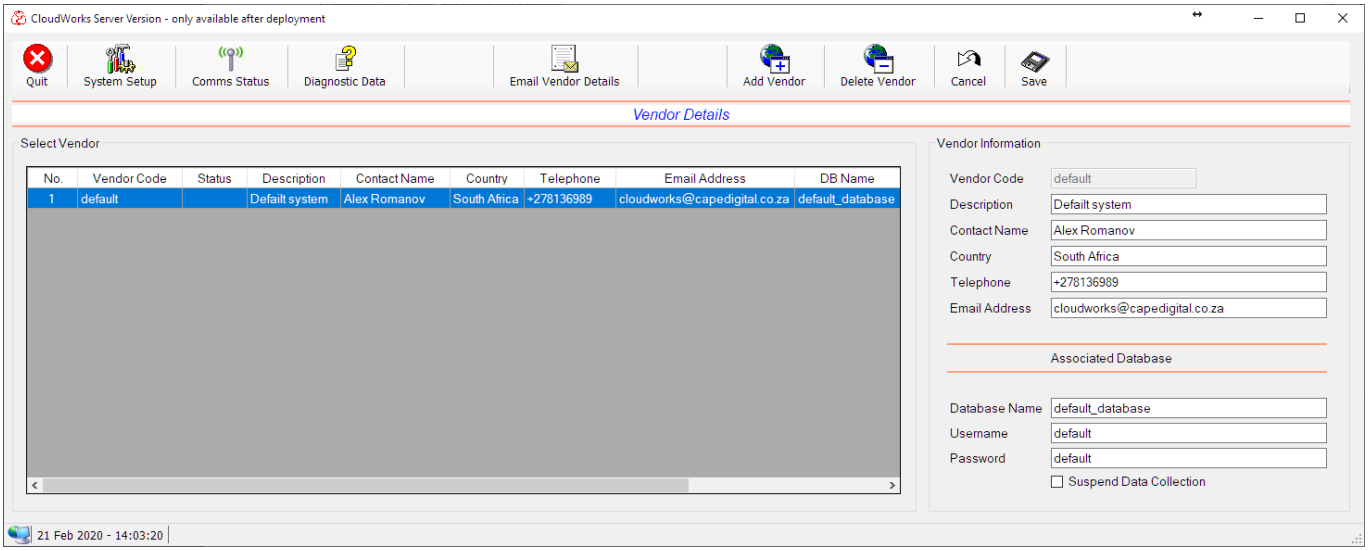
NBIoT Network Timeout	Time allowed for a command to propagate the whole system before it is considered to have failed. NBIoT Network. Parameter is in milliseconds.
Latency Warn Time	The latency time is the delay between the server sending a command to a remote device on the GSM network and the time it takes for a response to be received. This gives a good indicator to the level of congestion on the GSM network. When displaying the comms status any latency time greater than the Latency Warn Time will be displayed in red. Setting in milliseconds.
Status Read Delay	The number of seconds the server must wait before accessing online devices and requesting their current status information for insertion into their respective databases.
Diagnostic Port	There is a local TCP/IP diagnostic port available to monitor data traffic etc. This port number is defined in this parameter. Used for advanced features only.

Lastly are the two GPS parameters. When selecting an Offline 'Trigger GPS Read' in **Cloudworks** client, these two parameters come into effect. The first, 'Maximum GPS Dwell Time' is the maximum number of minutes the server must wait for the remote device to get a GPS lock before forcing a shutdown. The second parameter refers to how many satellites need to be observed before the lock is accepted. Fewer satellites result in a faster fix but will compromise the accuracy.

1.5 Managing Vendors



Adding, editing or deleting vendors is as simple as using the relevant buttons in the main tool bar. When adding a vendor, the 'Vendor Information' box on the right of the screen will become active allowing for the relevant data to be populated. The most important thing here, is to choose a unique Vendor Code which would best describe that vendor. The other vendor data is supplementary but should be populated as far as possible. Importantly however, is 'Associated Database' information. As discussed earlier, each vendor has an associated database, the details for which are captured here.



Once you are happy with the vendor information press the 'Save' button.

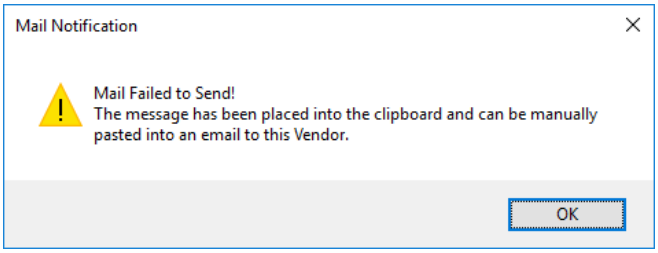
When a new vendor is created, a new database with its Username and Password will also be created. This information is needed by each user to access the database from **Cloudworks** client. Should the database not exist, or the user access details change, you will be prompted to confirm it as such.

To edit a vendor, simply click on the vendor in the table and their data will be populated in the right hand side of the screen. Edit and press 'Save' to apply the changes. Pressing 'Cancel' will ignore any editing you have done and revert to the original data.

Deleting is also achieved by selecting the vendor in the table and pressing the 'Delete Vendor' button. After some prompts, the vendor and its associated data will be removed from the database. Care should be taken to not accidently delete a live vendor as there is no recovering from this operation.

New vendors, or vendors that have lost their passwords, can have their database, username and password details sent to them via email by pressing the 'Email Vendor Details' button in the main toolbar.

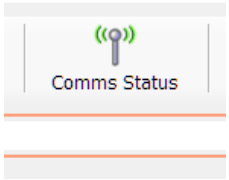
The email system is reliant on the SMTP server settings in the 'System Setup' being correct. Should an email fail to send, a warning will be flashed onto the screen showing the failure message.



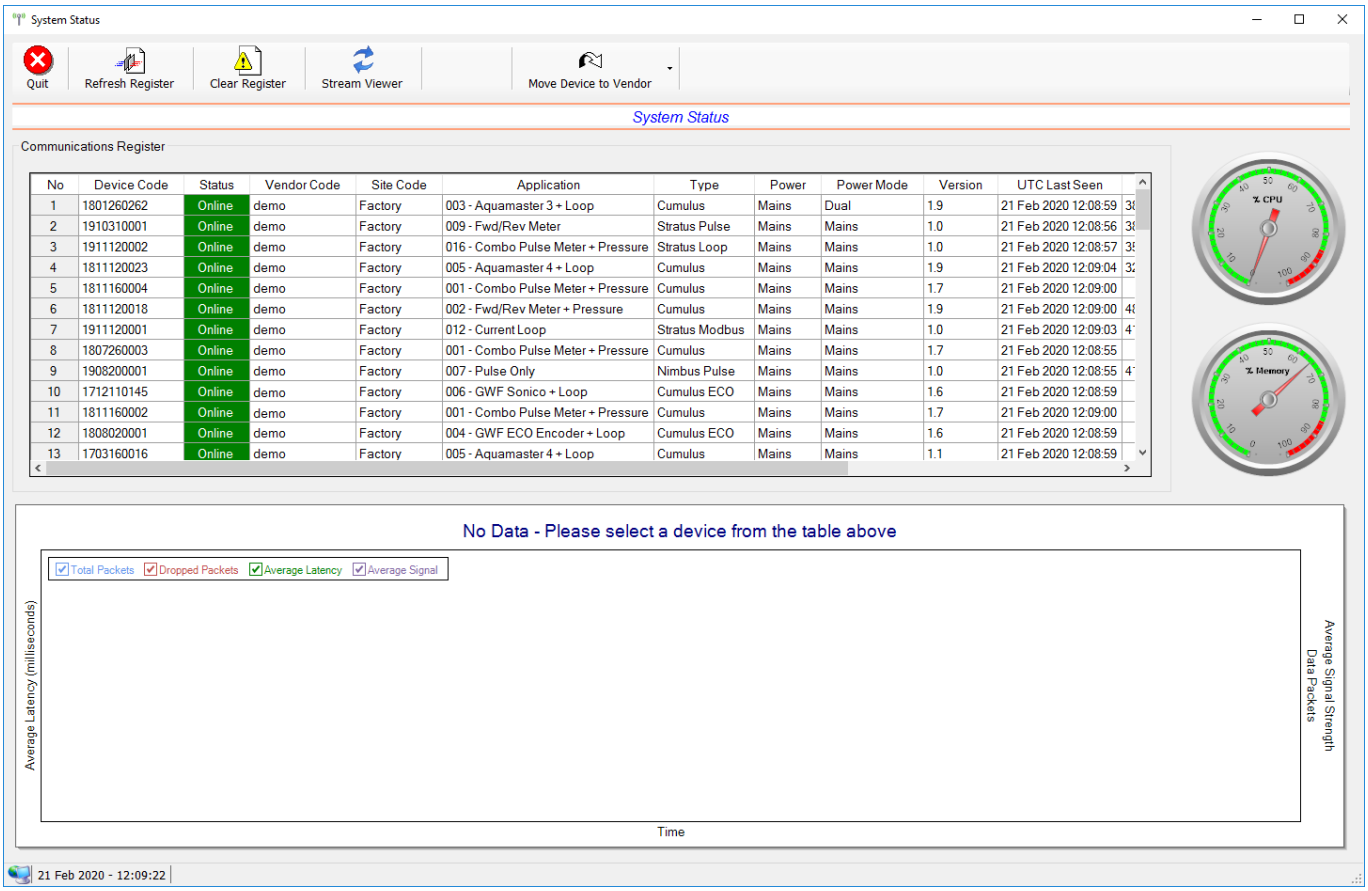
The body of the mail that was to be sent will be populated into the clipboard. This can be pasted into a mail using an external mail program and sent from there.

1.6 Communications Status

The 'Communications Status' module is a software tool that provides valuable information regarding the communications of devices on the Cloudworks system. This module is accessible from the 'Vendor Details' screen by pressing the 'Comms Status' button.



Pressing this will launch the 'System Status' Screen.



In order for the server to keep track of the various dynamic IP's and communications statuses of the remote devices, it keeps a register containing this information. On launching this screen the Communications Register is displayed in the main table. The register can be requested at any time by pressing the 'Refresh Register' button. To clear and restart this register, simply press the 'Clear Register' button.

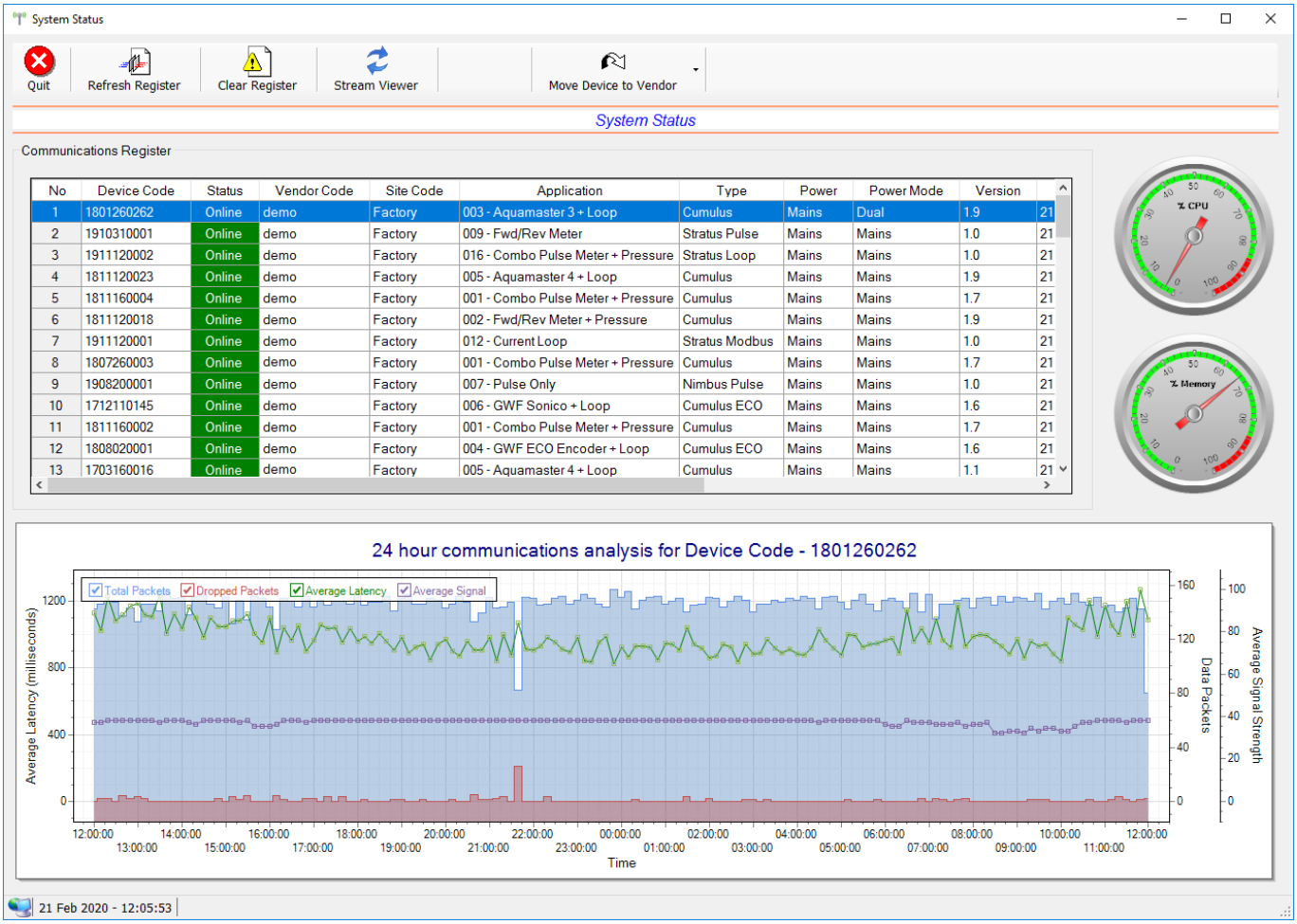
This register is continually updated by the remote heartbeat system or each time a battery device connects to the server. In order for a device to be present in the register, it will have needed to connect at some stage to the server. Pressing the 'Clear Register' button, will clear this register and restart the recording.

The data stored in the register is as follows:-

Parameter	Notes
Device Code	Device Code for the respective devices within the register
Status	Current communications status Offline/Online or Sleep. Note, when battery powered devices go offline, they are assumed to be asleep.
Vendor Code	Communications/Database Vendor Code assigned to the device.
Site Code	The Site Code is an independent coding system that is not currently used in the Cloudworks system.
Application	Application type assigned to device. Application types are explained in detail earlier in this document.
Type	Type of device. E.g. Cumulus logger CDS538 etc
Power	Current power status for the device. This is normally the same as the Power Mode except for Dual power devices that switch between mains and battery. This would be Mains or Battery.
Power Mode	Power Mode for the device. Mains/Battery/Dual.
Version	Onboard firmware version of device.
Port	Current connection Port number.
Signal	GSM signal strength at the remote device.
IP Address	Local GSM network IP address. For devices on a VPN with a static IP would show that static IP.
UTC Last Seen	Date and time the device was last seen by the server. UTC time.
Latency	When a data packet is sent from the server to a remote device and a response is received, there is a delay that is called the latency time in milliseconds). This time varies for different GSM networks and may alter during different periods of the day. By displaying the time here, it gives the user a fair indicator of how busy the GSM network is currently and possibly an explanation for communications that may be failing. These values are highlighted in red for readings greater than the value setup in the 'System Setup, screen.

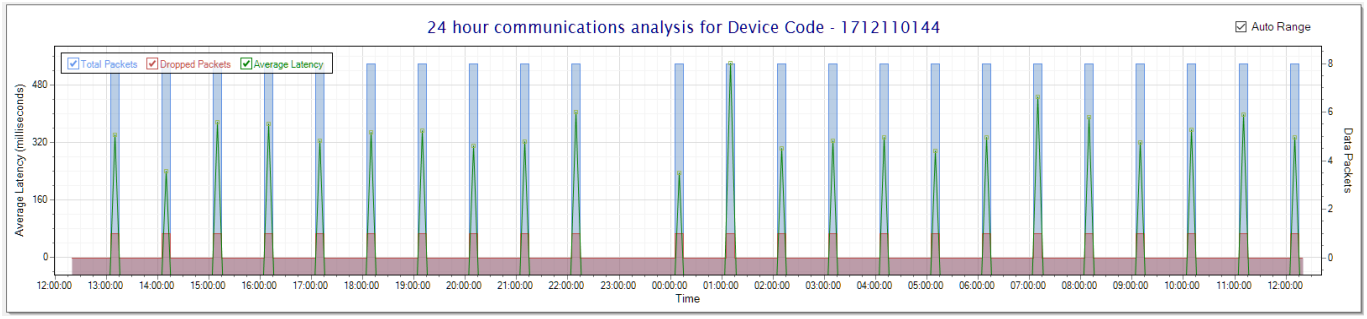
Included in the register is record of the data packet communications statuses for the previous 24 hours. Again, restarted if the server software is restarted or the register cleared. This record is divided into 10 minute intervals and holds the Total Number of Packets sent, the number of dropped packets (no response packets) and the average Latency time over that 10 minute period.

Selecting a device in the table will result in that record being plotted on the graph below.

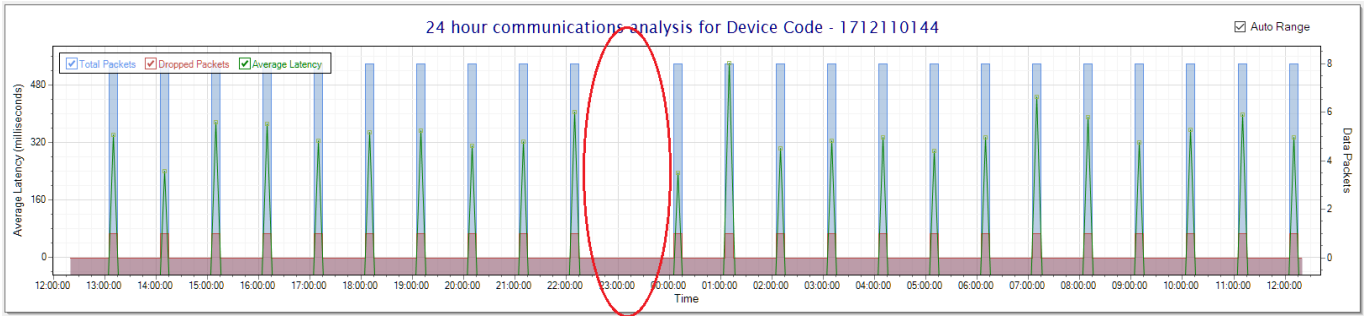


The example here is of a powered logger that is continually communicating with the server. As per the previous graphing options, individual series in the graph can be switched off/on by clicking the tick option on the top left of the graph. This information can be useful to ascertain how well the communications have been performing over the last 24 hours.

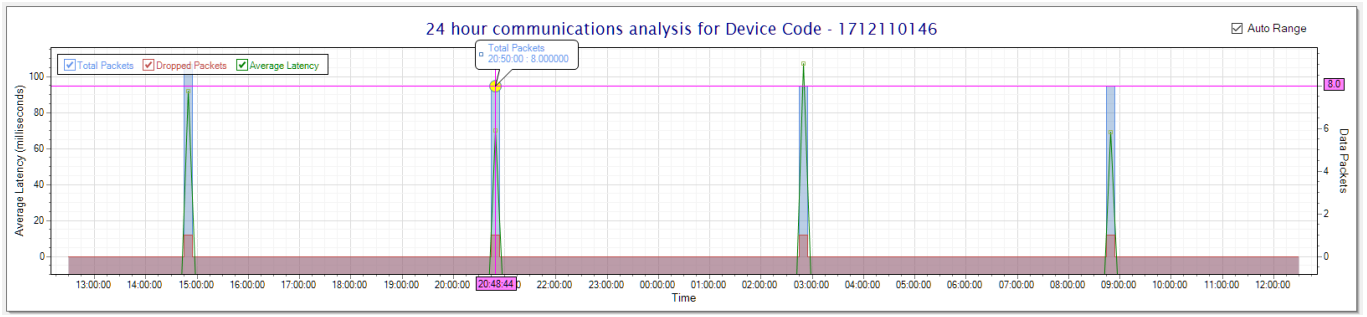
Especially useful is the graphing of a battery powered device. As seen below, it will indicate the times at which this device has successfully accessed the server.



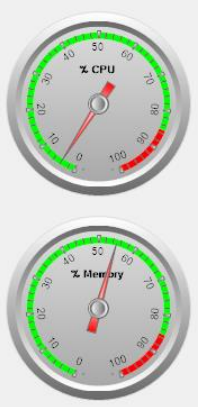
An interesting thing to note with this battery logger is that it was unable to connect at 23h00 (scheduled every hour), hence the missing comms block.



Battery loggers are normally set to wake up every 6 hours so their comms graphs would look like this.



Communications to and from remote devices are time sensitive in so much as a device that takes too long to reply will be considered non-responsive. To have a quick visual as to whether this is the remote device or simply the server that is currently overloaded with other tasks there are two needle dials representing the CPU and memory usage.



Often devices are deployed into the field where the user has forgotten to program the correct 'Vendor Code'. These devices will appear on the list of devices of the server, but the vendor will not be able to see it because of this error. This device can be easily moved by pressing the 'Move Device to Vendor' button. First select the device in the list (device must be online) and then select the new vendor from the dropdown button 'Move Device to Vendor' option list. This will automatically send the reset vendor command to that remote device and force it to restart, reconnecting it to the correct vendor.