

ComCap Data Capture Utility v4.20

Copyright Magenta Systems Ltd, 2019

ComCap User Manual

Table of Contents

Part I Installation and Use	8
1 Introduction	8
2 Upgrading from ComCap v3 to v4.....	11
3 Serial Port Tutorial.....	12
4 Networking Tutorial.....	14
5 SSL/TLS and Certificates.....	16
6 Installation	22
7 Getting Started.....	23
8 Main Capture Window.....	25
9 Telnet Terminal.....	33
10 ComCap Map.....	34
Part II Common Settings	38
1 Capture Logging.....	38
2 Common	41
3 Network	45
4 Serial Ports	50
5 Merging	53
6 LAN/Misc	54
7 Log Files	55
8 Alerts	58
9 Email	60
10 SMS	62
11 Data Loss	64
Part III Capture Settings	68
1 General	68
2 Records	71
3 Logging	75
4 Files	78
5 Email	83
6 Printing	86
7 Sounds/Data Loss.....	88
8 Database	90
9 Data Format.....	94

10	Network	98
11	Filters and Alerts.....	101
12	GPS	102
Part IV Databases		108
1	Introduction.....	108
2	Microsoft SQL Server.....	109
3	IBM DB2	111
4	Sun MySQL.....	114
5	Sample Databases.....	121
Part V Miscellaneous		126
1	ComGen Data Stream Generator.....	126
2	Test Serial Ports and Hardware Event.....	132
3	Concatenation Utility.....	132
4	Null Modem Emulator (com0com).....	133
5	Release Notes.....	135
6	Copyright Information and Support.....	159
Index		161

Part



1 Installation and Use

1.1 Introduction

ComCap is a Windows application designed to capture data received on PC serial communications ports or using network TCP and UDP streams and write it to text files. Captured data is shown in scrolling windows, and may be printed, written to SQL database tables or echoed to other PCs using network protocols or serial ports. Captured data can have text added such as date and time, a serial number and remote IP address. Data from up to 999 serial ports and network streams can be captured simultaneously, in separate files, with various file rotation schemes to start new files periodically. ComCap will capture to files on two separate disk drives for redundancy and will send email and SMS alerts if problems occur. ComCap is both a system tray and background service application that can be set to start automatically when windows starts, and remain unobtrusive. When using the background service, captured data may be still be viewed as it arrives.

ComCap features include:

- Capture from up to 999 serial COM ports, TCP/IP Server, TCP/IP Client and UDP/IP network protocols simultaneously, with suitable hardware. Many network appliances output log information, typically using the UDP/IP 'syslog' protocol, and as telephone switches become network aware they are offering network logging instead of the serial port.
- Serial COM ports are dynamically detected as they are installed and removed from Windows, so capture will automatically start if a USB serial device is plugged in, and stop if it's unplugged.
- Capture from serial ethernet device servers that 'convert' serial port data to network protocols, from Brainboxes, MRI, StarTek, Lantronix, [Lavalink](#), RE Smith and Tysso eCov for instance, easing data capture distances, Audon in the UK sells eNet converters.
- ComCap supports IPv4 and IPv6 network standards, and SSL/TLS network capture and echo, to provides encryption of data sent over the internet, and to confirm the identity of the other party with X509 SSL/TLS certificates. It includes support for the latest TLSv1.3 protocol.
- Email may be captured, such as the alert emails sent by internet aware appliances, such as firewalls, security monitors, power distribution units, uninterruptible power supplies, remote sensors, transponders, etc. The emails may be written to a SQL database or used to trigger alerts.
- GPS NMEA 0183 sentences and various vehicle tracker output can be parsed into simple comma separated records, allowing location information received from a serial or network connected GPS sensor to be easily saved to a SQL database. A map window shows a GPS track to ensure everything is working.
- GPS location data may be captured on Windows tablets and high end laptops that have a GPS location sensor built-in.
- Captured data is optionally shown in scrolling windows as it arrives, and earlier data can be viewed as well. Coloured tabs indicate which channels have started capturing data and which are stopped.
- Data from multiple serial or network capture channels may be merged or consolidating, allowing all data to be displayed in a single window, written to a single log file, and added to a database using a single connection.

- Capture files may be in separate directories for each capture port and new files may be created daily or multiple per day (at specified times), weekly (Monday), monthly, hourly, every few minutes, after an inactivity period, when a new page character is received, each new record, or a fixed file name may be used. Multiple channels may optionally capture data into a common file, to reduce the number of separate log files.
- When a capture file is closed and rotated for a new file, it may be moved to another directory for further processing or emailed to multiple recipients.
- Capture file names (and optionally paths) are automatically generated, with file name format customised with date and time in various ways, numeric or alphabetic.
- Capture data may be written to a database, such as Microsoft SQL Server or MySQL. Data formats may be created to identify fields within each line of data, as fixed width columns, character separated columns (CSV) or variable named columns. ComCap examines the SQL tables or stored procedures for column names and types, and allows mapping of which field of data is written to which SQL column. ComCap protects data that can not be immediately written to the database due to network problems, and will write it once the database becomes available again.
- ComCap can echo or proxy captured data directly to serial communications ports or parallel ports to drive printers, or echo to the network using UDP/IP (syslog), TCP/IP Server or TCP/IP Client protocols. Network echo can be used to allow capture of the same data to a maximum of five PCs simultaneously for redundancy or for remote capture with one PC near the data source echoing data to a centralised location.
- ComCap displays the status of the serial port CTS, DSR and DCD lines, and if a TCP/IP connection is established is connected, and flashes when data is received.
- ComCap has options to safeguard captured data, closing the log after each line to force it to write to disk, or after an inactivity period or periodically every few seconds or minutes.
- A separate information log file is maintained showing when capture starts and stops and other ComCap events, it will log capture status hourly with the number of lines received from each port or stream and to which logs it is being written. The information log may be sent to a remote PC using network protocols, perhaps to another copy of ComCap, to ease central monitoring of remote capture.
- A sound file may be played when each new line of data is captured (with a minimum gap between sounds, in case of frequent data).
- Raw data may be captured unchanged from the COM port or network stream, or the data may be cleaned up with non-printing characters removed and trailing spaces removed.
- When capture is started or stopped, command strings may be optionally transmitted and periodically repeated, perhaps to trigger a remote appliance to start or stop. Optionally, extra commands may be transmitted on demand, perhaps to configure a remote capture device.
- Captured lines may have text added at the start or end, that can include escape sequences to add a serial number (of specified length), date and time in various formats, PC name, local or remote IP address.
- A comment may be added manually to any capture channel, using a pop-up dialog, this is intended to assist in documenting batch captures, perhaps from laboratory instruments.
- Continuous data streams may be selectively captured to reduce the amount of data saved, for

instance from GPS locators or environmental sensors.

- Alerts for problems are presented in a pop-up window and may be sent by email, by SMS to mobile telephones, using either a GSM modem or SMS internet gateway or to a remote PC using network protocols, perhaps to another copy of ComCap, to ease central monitoring of remote capture. Alerts may also be triggered for phrases in captured data.
- Data loss checking, to detect if other windows applications caused ComCap to possibly lose data. An alert may be triggered if new data is not captured after a period, configurable by time and day of week, or if the PC appears to hang for a short period.
- For redundancy, ComCap will capture logs on two different disk drives at the same time, and continue logging if one of the disk drives is lost, the drives may be across a network with remote logon details specified. ComCap makes multiple attempts to open files, in case of conflict problems such as backup and protects data until it can be written to the capture file. If disk space runs low, ComCap will send an alert.
- Captured data may be filtered, so that lines containing unwanted content are ignored. Alerts may be sent according to filtered data.
- ComCap usually runs as a Windows service that starts immediately the PC starts without needing a user to log-on. There is also a system tray application which can configure, monitor and control the service displaying data currently being captured, but which will also capture data if the service is not used.
- ComCap is supported on Windows Vista, 7, 8, 10, 2008, 2012 and 2016, both 32-bit and 64-bit editions. Note Windows XP, 2003 and 2000 are no longer supported, but should still work. ComCap may be run with a higher priority than other windows applications to ensure stable data capture, although a dedicated PC is recommended for valuable information.
- There are two editions of ComCap version 4:
 - **ComCap v4 Standard** edition is limited to three simultaneous serial or network channels and does **not** support database or data filtering
 - **ComCap v4 Unlimited** edition has no channel restriction and adds database and data filtering support
- ComCap v5 is currently in development and beta testing, with many new new features. There will be an upgrade cost from v4, but v5 can be purchased now and the license key used for v4 or v5.

ComCap was originally designed to capture telephone call logging data from the serial port provided on most telephone switching systems (PABXs), typically called Call Data Records (CDR). The saved data may then be used as input to telephone call management applications that will cost calls and produce reports on telephone usage or for security audit purposes.

ComCap is application non-specific and will capture any data that arrives on a serial port or using network protocols. It has been used for a wide variety of purposes, such as logging output from test, alarm, GPS and monitoring equipment and serial printer data (but it can not process printer control characters).

Please note that ComCap is not designed to monitor data between modems and PC applications, it requires exclusive access to the serial port so no other application can use the port at the same time.

The ComCap distribution includes the 'ComGen Data Stream Generator' application which is designed to generate various types of test streams using any or all of the PC serial COM ports and potentially

dozens of network streams, UDP Client, TCP Client or TCP Server, and has been used extensively for testing ComCap capturing multiple channels. There is also a small 'Test Serial Ports and Hardware Events' utility that may be useful in testing communication port and cabling problems.

If the requirement is to capture serial data from another application on the same PC, ComCap includes a Null Modem Emulator (com0com) from <http://com0com.sourceforge.net/> that installs a linked pair of virtual serial ports, instead of needing to use a physical pair of COM ports and a null modem cable.

Web: <https://www.magsys.co.uk/comcap/>

Help File for ComCap Release 4.20, 22nd May 2019.

1.2 Upgrading from ComCap v3 to v4

The main benefits of upgrading from ComCap v3 to v4 are as follows:

- Capture of TCP/IP Client, TCP/IP Server and UDP/IP network protocols
- Increase from 30 to 999 maximum capture channels
- Transmit commands on start and stop capture
- Improved line ending and restart capture
- Redundancy writing to two different log disk drives
- Better error handling for log file errors
- Higher program priority to avoid data loss
- New multiple logs per day capture interval
- More flexible text addition to capture data
- Capture direct to a SQL database
- Better printing options, bypassing Windows print queue
- Echo captured data, using serial or network protocols
- View data captured by the service version
- Control service version from tray version
- Configuration data in files rather than the registry
- Alerts by email and SMS to mobile telephones
- Main window does not show unused serial ports
- View full and old logs in new larger window
- There are two editions of ComCap version 4:

- **ComCap v4 Standard** edition is limited to three simultaneous serial or network channels and does NOT support database or data filtering
- **ComCap v4 Unlimited** edition has no channel restriction and adds database and data filtering support

Please note that ComCap v4 is effectively a new application (COMCAP4.EXE), and may be installed in parallel with ComCap v3 (COMCAP.EXE), although only one version will be able to access the same serial ports at the time. ComCap v3 license keys will run for 24 hours in v4, for trial purposes. All settings need to be newly created for a first install of ComCap v4. Once ComCap v4 is installed and working correctly, ComCap v3 should be un-installed. On the Start menus, ComCap v4 is installed as ComCap4.

Also note that there is no longer a separate service version of ComCap, the service version is now effectively integrated into the tray application, and is now automatically installed or de-installed, and enabled, through Preferences, and controlled by the tray application. The ComCap v4 Background Service is installed as 'ComCap Service', rather than 'Magenta ComCap Service' for v3.

1.3 Serial Port Tutorial

Serial Ports Overview

When ComCap was originally designed all PCs had one or two fixed serial RS232 ports with a DB9 connector. Fixed serial ports with DB9 or DB25 connectors are now rare, although PCI expansion cards are often used, and removable USB, virtual and Bluetooth serial ports are common. Some of these serial ports can come and go as they are plugged and unplugged. Up to 999 installed serial COM ports will be displayed, not necessarily contiguously, but only three may be captured with ComCap Standard. Note that RS232 serial ports not recognised by the PC BIOS need special windows driver software installed, which is usually supplied with the hardware. Some virtual ports may have strange names like CNCA2, but these will work identically to those starting with COM.

The Serial Ports grid in Common Settings shows all ports installed on the PC including those currently removed and unusable, which are typically USB serial ports that are unplugged. This means capture can be set-up and started for ports that are currently removed, and will start immediately the USB device is plugged into and becomes available to Windows. Likewise capture will be paused if a serial port disappears, and restart if it re-appears.

If the port is unknown, the Test Serial Ports and Hardware utility supplied with ComCap may be used to find which port has active signal lines.

Virtual serial ports may also be installed by some applications to allow those applications to be accessed by software such as ComCap. If the requirement is to capture serial data from another application on the same PC, ComCap includes a Null Modem Emulator (com0com) from <http://com0com.sourceforge.net/> that installs a linked pair of virtual serial ports, CNCA0 and CNCB0e, instead of needing to use a physical pair of COM ports and a null modem cable.

When ComCap starts, the Info Log reports all installed serial ports, with various items of information that may be found in different places in Windows, for example:

```
COM1, Enabled=Y, Communications Port, (Standard port types), Serial0
COM3, Enabled=N, Prolific USB-to-Serial Comm Port, Prolific, , USB
\VID_067B&PID_2303&REV_0400, Port_#0001.Hub_#0003
COM4, Enabled=N, CyberSerial 950 16C950, SIIG, , OXPCIMF\*PNP0509
COM11, Enabled=Y, D-Link DU-562M External Modem, CXT, Winachsf0, USB
\VID_0572&PID_1300&REV_0100, Port_#0007.Hub_#0004
COM12, Enabled=Y, Enhanced Communication Port, Oxford Semiconductor, OXMF0, OXMF
\*PNP0501, oxmf bus, port 0
```

```
COM24, Enabled=N, Standard Serial over Bluetooth link, Microsoft, , BTHENUM\{\
_VID&0001000f_PID&1200,
COM26, Enabled=Y, USB Serial Port, FTDI, VCP0, FTDIBUS\COMPORT&VID_0403&PID_6001,
CNCA0, Enabled=Y, com0com - serial port emulator, Vyacheslav Frolov, com0com10, com0com\port,
CNCA0
```

where COM1 is a motherboard port, COM3 is a removed USB Prolific port, COM4 is a null modem, COM11 is a USB modem, COM12 (and COM13 to COM19) are an 8-way MRI PCI card, COM24 is a Bluetooth serial port, COM26 is a USB FTDI port. The VID_x strings may be used to Google search for unknown hardware device identification if looking for new drivers. Enabled=N means the port is removed, usually an unplugged USB device, but could be a removed PCI card. Port and hub may identify USB ports. Beware if a USB device is plugged into a different socket, it will often be installed as a new COM port.

Signed Device Drivers for Windows 64-bit

With the 64-bit editions of Windows 7, 8, 10, 2008 R2, 2012, 2016 and later, Windows will no longer accept unsigned drivers for serial port expansion products such as USB, PCI or PCI Express cards. For manufacturers, getting signed drivers from Microsoft is expensive and they are usually only available for products still being manufactured and supported. Some RS232 cards and dongles used for testing ComCap under Windows XP no longer work under Windows 7 64-bit and later, but new signed drivers are now available from Microsoft Update or manufacturers sites for other newer hardware. Specific hardware still working includes:

- MRI PCI8S/R PCI high-speed 8 port serial adapter using Oxford Semiconductor chips, <http://www.mri.co.uk/>, which are also available in 1, 2 and 4 RS232 ports, MRI also sells PCI Express and USB adapters with up to 8 ports.
- Lava Computer DSerial 2-port PCI card, Lava also sells 4 and 8 port serial cards, <http://www.lavalink.com/>.
- StarTek FTDI (Future Technology Devices International) USB serial cables, <http://www.startech.com/> and <http://www.ftdichip.com/>, widely available.
- StarTek Prolific USB serial cable (beware cheap imitations), <http://www.startech.com/> and <http://www.prolific.com.tw/> often included in other products such as GPS devices, also used by <http://plugable.com/> USB to RS232 Adapters..
- Winchiphead CH340 USB serial cable from <http://wch-ic.com/>

Serial to Network Converters or Ethernet Device Servers

To overcome the restricted length of RS232 serial port cables (about 30 metres), in recent years serial ethernet device servers have evolved which convert serial port data to network protocols, usually TCP/IP. Usually small modem sized units, but sometimes just large plugs, these converters usually have a small internal web server used to configure the IP address and port and serial port parameters, and support TCP Client and TCP Server protocols. Some support two or more serial ports.

Such converters are offered by Brainboxes, MRI, StarTek, Lantronix, [Lavalink](#), RE Smith and Tysson eCov for instance, easing data capture distances, Audon in the UK sells eNet converters.

Note ComCap can itself be used as serial to network converter, by capturing from one or more serial ports and echoing data using network protocols. There are also open source free software network converters, such as 'COM Port to TCP Redirector' from <http://com0com.sourceforge.net/>.

Most of these serial ethernet device servers come with Windows driver software that causes the remote serial ports to be presented as virtual serial ports in Windows. While convenient for supporting old software that only recognises serial ports, these drivers are usually unnecessary for ComCap

capture since the original TCP/IP stream can usually be captured directly. Bypassing these virtual serial ports removes a possible failure mode, and will usually result in better performance due to use of IP packets.

1.4 Networking Tutorial

IP Addressing and Ports

Internet Protocol (IPv4) use 32-bit addresses with 16-bit port numbers to uniquely a host process on computers, the address is usually shown as four sets of numbers, ie 192.168.0.1, while the port is a simple number from 1 to 65,536. Domain names such as www.magsys.co.uk are a higher level over IP addresses, but are not supported by ComCap, at present. Computers may have specific IP addresses allocated to them or temporary addresses from a DHCP server that may change each time the computer is booted. ComCap needs fixed IP addresses so don't use DHCP.

IP ports numbered below 1,204 are pre-allocated to specific internet protocols (sometimes different for TCP and UDP), 514 for syslog, 21 for telnet, etc, while higher port numbers are used automatically by the computer for specific connections or may be specified by users for unique connections.

IPv6 is a newer internet protocol that uses longer 128-bit addresses or 16-bytes (although only 64-bit are for public routing). IPv6 addresses are shown in hex pairs separated by colons, so 0123:4567:89ab:cdef:0123:4567:89ab:cdef could be a possible IPv6 address, but they are always shown in abbreviated form by removing leading zeros and most colons if there are four zeros. Magenta's IPv6 address is 2a00:1940:2:2:: which is a /64, Google is 2001:4860:: which is a massive /32 block. Public IPv6 addresses currently all start with 2, local IPv6 address usually start with fe80::. The last 64-bit of the IPv6 address may be allocated automatically by Windows based on the PC MAC address, so a PC might be fe80::306b:7ecb:1f6f:24ff internally, and 2a00:1940:2:2:306b:7ecb:1f6f:24ff publicly, or it may be specified specifically, so the Google DNS server is 2001:4860:4860::8888. One special IPv6 address is :: which is equal to 0:0:0:0:0:0:0:0, and means all IPv5 addresses, like 0.0.0.0 is all IPv4 addresses.

There is display convention for displaying and sometimes entering IPV6 addresses of using square brackets, to avoid confusion with the port at the end which historically was separated by a semicolon. Local IPv6 addresses also sometimes have a scope prefix following %, which should be used if seen. When ComCap starts, it will report allocated addresses, similarly to:

```
[fe80::306b:7ecb:1f6f:24ff%11], [fe80::136:4a6b:870b:e19%30], [2a01:348:6:68c::2],  
[fe80::6185:2151:a9a6:5fad%27]
```

In logs, ComCap will usually added the port, ie .'Connected OK to [fe80::35ac:4130:4438:5fcc]:514' .

If using a browser with IPv6 address, the square brackets are needed, ie [http://\[2a00:1450:4009:806::1012\]/](http://[2a00:1450:4009:806::1012]/) is the Google home page, but generally the square brackets are ignored when entered an IPv6 address in a settings field.

Host Names

Although all network connected devices have an IP address, at least for publicly available devices it is usual for them to also have a host name, with DNS (dynamic name server) being used to map names to IP addresses. Local area networks also support NETBIOS names, which are computer names. Host names are often hierarchical, being composed of a domain and sub domain, ie www.magsys.co.uk. While host names are often more convenient to use, the need to look-up an IP address using a DNS server adds an extra failure possibility and sometimes a security vulnerability if the DNS server is compromised.

ComCap allows host names to be specified for UDP Client and TCP Client (see below), but not for UDP Server or TCP Server. The latter may be available by means of a host name, but ComCap only

listens on specific IP addresses and is unaware if DNS is available. Host names are generally required when using TCP Client with SSL/TLS and certificate checking, since certificates are normally issued for host names, not IP addresses.

UDP

User Datagram Protocol (UDP) is a connectionless network protocol using IP that sends packets of data without any handshaking or acknowledgement, but very efficiently, with the hope that a server is listening for it. Each packet or datagram is generally self contained and variable length, usually the length of data being sent (often without any line ending). Because UDP is connectionless, applications may stop and start without any hindrance, albeit potentially with lost data. UDP should be loss free on local area networks, but is more problematic across wide area networks where the error correction of TCP is needed to cope with lost packets.

UDP is used for two common protocols, Syslog generally using port 514, and SNMP using port 162. UDP has one other benefit, two or more appliances or clients may send UDP data to the same server.

When ComCap is set-up for UDP Server, it will accept any UDP data on the specified port but can optionally filter packets from different remote IP addresses to different capture channels, keeping data from different sources separate. UDP Server can listen on one specified port, on addresses 0.0.0.0 or :: meaning all addresses on the PC, or on just one specific selected address.

While UDP is connectionless, ComCap Echo to Remote will optionally ping the remote host before sending UDP packets to establish it exists, although this does not mean a UDP server is listening on the remote computer, just that the computer is running.

TCP Overview

Transmission Control Protocol (TCP) is a connection oriented protocol using IP that has initial handshaking when making a connection that opens a two way reliable stream between two computers, with error correction and packet acknowledgements. If one computer disconnects or there is a network failure somewhere, the other computer will also disconnect (although this may be after a timeout). TCP packets are variable size with lines of data often split into two or more packets, or combined into a single packet, so it's essential each line is clearly terminated, usually with CR and LF. A TCP connection needs to be negotiated between two computers, the one that starts is called the client while the one waiting for connections is the server.

TCP Client

TCP Client originates a connection to a remote server and waits for a response, usually for about 40 seconds before failing. If the connection fails, the client therefore needs to keep retrying to establish the connection, with ComCap allowing a configurable wait between attempts and limiting the number of retries. TCP Client can connect to a specified port on a single specific remote IP address or host name.

ComCap can optionally ping the remote TCP Server first to establish the computer is accessible, waiting 10 seconds for a response (much shorter than the timeout for a TCP connection, but even if the ping works, there may be no server available so the connection may still fail. TCP Client is a one-one connection between two specific computers.

TCP Server

TCP Server listens for incoming connections from remote TCP Clients on a specified IP port. When a TCP Client connects, the two-way connection is established on a new IP port, allowing further clients to connect to the original IP port. TCP Server can listen on one specified port, on addresses 0.0.0.0 or :: meaning all addresses on the PC, or on just one specific selected address.

ComCap allows two or more TCP Servers to be set-up on the same port, allowing multiple clients to connect and send data. ComCap will optionally filter connections from different remote IP addresses to different capture channels, keeping data from different clients separate. Note this is different to UDP Server, because a ComCap channel must be set-up for each different client because only one connection is allowed per channel.

Ethernet and Packets

Ethernet is the physical hardware layer used by IP for cabled networks, also called IEEE 802.3, supported by ethernet network adaptors each with a unique 48-bit MAC address. Each ethernet packet comprises a header with the source and destination MAC addresses and protocol (usually IP, but also ARP, ICMP, IPX, IPV6). For IP protocol, the packet header adds the source and destination IP addresses, time to live, checksum and protocol (UDP, TCP, etc). For UDP and TCP protocols, the packet header also adds the source and destination ports, data length and checksum. TCP protocol also adds flags to open and close connections and sequence numbers used for error detection and correction. The header overhead (and minimum size) for a UDP packet is 42 characters, for TCP it's 54 characters. The Ethernet hardware level adds a frame preamble and frame check sequence, but these are removed before software sees the packet.

Serial to Network Converters or Ethernet Device Servers

To overcome the restricted length of RS232 serial port cables (about 30 metres), in recent years serial ethernet device servers have evolved which convert serial port data to network protocols, usually TCP/IP. Usually small modem sized units, but sometimes just large plugs, these converters usually have a small internal web server used to configure the IP address and port and serial port parameters, and support TCP Client and TCP Server protocols. Some support two or more serial ports.

Such converters are offered by Brainboxes, MRI, Lantronix, [Lavalink](#), RE Smith and Tysso eCov.

Note ComCap can itself be used as serial to network converter, by capturing from one or more serial ports and echoing data using network protocols. There are also open source free software network converters, such as 'COM Port to TCP Redirector' from <http://com0com.sourceforge.net/>.

1.5 SSL/TLS and Certificates

SSL/TLS Overview

SSL/TLS, secure socket layer and transport layer security, provides encryption of TCP/IP data being sent over the internet, and also allows client and server to confirm the identity of the other party with X509 SSL/TLS certificates.

SSL/TLS is not supported for UDP.

There is no automatic SSL/TLS negotiation, both ends of the connection need to support SSL/TLS (or not) for a connection to work, if one end does not support SSL/TLS, the connection will fail without any real error.

SSL/TLS TCP Client

TCP/IP Client is easy to set-up, really just a tick box, does not need a certificate, unless the server specifically want to check the identity of client which ComCap does not yet support. ComCap may optionally verify the remote server certificate to ensure it is talking to the correct server, but this increases the time for a connection to made while certificates are transmitted and checked, potentially causing the connection to fail. Also, ComCap needs the trusted root certificate used to sign the server's certificate, which is how the chain of trust is proved. ComCap can check certificates against an included PEM Bundle File with a few hundred:

```
C:\ProgramData\Magenta-Systems\ComCap4\Certificates\RootCaCertsBundle.pem
```

This file name is setup in Common Settings, Common where SSL security settings are also specified for all TCP Clients and TCP Servers, these settings may prevent connections to lower or higher security clients or servers.

Or certificates may be checked using the Windows Certificate Store is used by Internet Explorer and other applications. This is periodically updated through Windows Update, and there are Windows tools

to view and add certificates. For the store only, certificate revocation can be checked, beware this requires internet access and can take several seconds, or longer.

The checked SSL/TLS certificates may be logged similarly to:

```
telecom-tariffs: 3 SSL Certificates in the verify chain:
```

```
Depth #1 Verify Result: ok  
Issued to: www.telecom-tariffs.co.uk,  
Alt Domains: www.telecom-tariffs.co.uk, telecom-tariffs.co.uk  
Issuer: RapidSSL CA, GeoTrust, Inc.
```

```
Depth #2 Verify Result: ok  
Issued to: RapidSSL CA, GeoTrust, Inc.  
Issuer: GeoTrust Global CA, GeoTrust Inc.
```

```
Depth #3 Verify Result: ok  
Issued to: GeoTrust Global CA, GeoTrust Inc.  
Issuer: Trusted Root
```

which is public certificate signed by an intermediate certificate, signed by a root certificate in the Windows store and PEM file.

It is also possible the certificate may be self-issued and self signed, similarly to:

```
Echo Send: 1 SSL Certificates in the verify chain:  
Depth #1 Verify Result: self signed certificate  
Issued to: logs.comcap.co.uk, ComCap  
Issuer: Self Signed
```

This certificate was created by ComCap, see below.

SSL/TLS TCP Server

For TCP/IP Server SSL/TLS certificates are essential, since they control encryption as well as verification. Although an SSL certificate is generally issued to a domain host name, ComCap will be unaware of this host name, only the IP address can be specified. Two or three files need to be supplied to make SSL/TLS work correctly:

<p>SSL Server Private Key</p>	<p>The server private key is created on the server to be protected and controls the encryption. It is never transmitted anywhere and must remain private, otherwise the public certificate can be used by other parties to impersonate this server. ComCap includes the private key for the self signed test certificate in the file: <code>comcap-prvkey.pem</code> that internally looks like this:</p> <pre># X509 SSL Private Key # Subject Common Name: logs.comcap.co.uk # Subject Organisation: Magenta Systems Ltd # Subject Organisation Unit: ComCap Test Certificate # Issuer: Self Signed # Expires: 01/01/2031 -----BEGIN PRIVATE KEY----- MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBywggSiAgEAAoIBAQDpk13FCrP Tktrl cyZSJ6HSscgvm3VLn+GOFx3cECgBarjzylul0ie5DrVXeC3DgYvRjXpGHLj/ CAU44 PNrv7Bvoj +JVvNSIFxLI3uAb0y5R7xDkVWugjXZCHELTnY8gbM7rBvEkR52L5UIH 9OhJJ16GfOX7KGEO+BYy2o2fbqmW03Yb5aGrT2nOsRmiAvQDCgU+Nxc +UtlOh3G6 DTeFYI3DtWme3y2YhOuf1pmepuSVQ4P3f98HOwQqCYFA1eZF2XRrsRObGE EZU9D+T 4S4VH5COKDU19H7VZTGWa8zAFe3es8WC48aRIFW+5Q73 +COxUk6ZXdlc9DtDKCYT bG8g5O/ NAgMBAAECggEAWlvZFaX7RSj1nD/3niaY0nmulwSR0w1jKtisMRLRakMn bs1x+tM1Klc+9aRFaXi+el/n4nzAy4OHx/e61r/nWAN5kqN3O9p+ONkHp5v9ulKa nUv4R1cSXabjL0wvl2KgdYI89gUCbKEpxT14MvyY87wTmCLZ0vml9MxZp0i/ Mlom Qk0KRY2q4/toLC7FWn7gUnGER758WX5mETddmBkfONS +5i22z0g7YK5MtSv7DSJ8 3b+OplgtuOf3hL+tRn4N15GE4Nd8twIS0kiRomBU0fTHT0o0RDX/WuM2DLHV +zxh BfRrX3W1exl/Wn47wqaK2VwNQH1YZEmLg6/I95VuvQKBgQD9KslU6tMv1DrB +IJI P0sfVrquv9RE7IkYcnlJZ5jxkZFr9LE1F9Vn3ALDWxlvMhHusl3zwmBnbqt/wG1V s8IVcrCBfaObnHtNEAsCuyUJ0reLzcPeYDvdq5Qhg9otx8tqxfDPBumHrqdWdx 2R +JkNx+2uA5Lx4xpsG +zorQFfAwKBgQDsMHVxtmsynvJBpZSQfSHQdD7lwAJAQ6p7 FvRScySo5FcbVO5RETWpIKfUFpmagciPTqKMn/ mUFnBjIKwJFOuYZIcnRV8R841V 4KsaytFTqqbwT3ZQR6 +BLen3T2tvBDvOmjg2N0C4oPr2XN7oI0SP898MQaZsxThp BgOaxrsU7wKBgEg50bB5QgDOMmkuyhS0gfer5DaAocV8nkn8NB/9/0NDvVlo P/oe r5Ju0Rb8v2ZZiYYoNodJeAlqKGFm+6RMoV1PGA4JUWjNDtxAbHO +AmYYCKdl781c czW4G12rOS6AZocyq23U0gEUkcb4OqZvXvLwi91uRZjeqqYXHxKQEOkTAoG AftM6 jTft8f2lihiWYmVAd4WkLlxg6Q8soPHfedJ4UfRizbtaSM+b6BZ51AnaqzubbVBF OovAYYN3EBHKGwpPw8HfTPgUJ7iHISEF39oecvXEtG +G0W7cz9nOs0zDHJbCYpsv KfWbXEic2eNekrh/ SWkjURqDeg6gzsw67Q6HGKMCgYBkSLfnX66goLa1whUoF0zg TNEIaLwr4nhzMKvJYYk/2EQ59S30/nplzngvQj8H9ruxs8fZmDa9k702tqRIM1bi pPmAgw3wmdgFjfwvPVRrJULBBRN8rnGc5Hz98YjhHtmmt08s/8dqlvjAs6DvMQ 2I ejY86RYeGQPNwFjBeexgLA== -----END PRIVATE KEY-----</pre>
-------------------------------	---

SSL Certificate Authority	Sometimes the server certificate is not signed by a trusted root certificate, but by an intermediate certificate that is itself signed by the trusted root. In this case the file name of the PEM file containing any such intermediate certificates needs to be specified here. In the client example earlier on this page, the RapidSSL certificate is an intermediate certificate.
SSL Server DH Params	<p>DH Params are private and public keys used for SSL key exchange in DH, DHE, ECDH and ECDHE protocols. ComCap includes three pre-defined DH files: comcap-dhparams1024.pem, comcap-dhparams2048.pem, comcap-dhparams4096.pem, but for highest security the OpenSSL tools should be used to create your own DH Params.</p> <pre>-----BEGIN DH PARAMETERS----- MIGHAoGBAOuZatHzoGKWmGlpTDVhpXJhcyXqiBDVknRkXwEvG6uRCZdKIX MRlyxv TR4zgV+QCExZd74hN28D6VFi/ jrE6xUciJ41kSwf8DOXkWLaR81r1p8nBOJLAPBF ooQVBKZ4HxX29vXGnJjdAvrdhN0/h+9z/Dej4ZqE7PgyKw6nKg2LAgEC -----END DH PARAMETERS-----</pre>

Creating and Getting SSL/TLS Certificates

ComCap includes a Windows that allows either a self signed certificate to be created, or for a request to be created that allows a commercial certificate to be purchased. This window can be accessed by a button from either Common or Channel Settings, when specifying SSL/TLS file names.

Create SSL X509 Certificate or Request

Certificate Type

Self Signed Certificate

Request for CA Certificate

Certificate File Prefix: comcaptest2-

Common Name, usually Domain: logs.comcap.co.uk

Key Bits: 2048

Organisational Unit: xxxx

Organisation Name: Organisation

Locality: xxx

State/County: State

Country Code: GB

Email Address:

Expire Date: 31/12/2023

Is Certificate Authority

Replace Existing Certificate Files

Create Close

Certificate Type

For a self signed certificate, most of the certificate fields may be left as defaults since the certificate will not be used to identify identity. To order a commercial server certificate issued by a Certificate Authority, a request file and private key is created, the first only of which is sent to the authority who will use it to create a server certificate that is returned and used with the private key file.

Certificate File Prefix

ComCap creates three different files in the Certificates sub-directory, with the specified prefix, each is a small text file with the PEM extension.

```
C:\Users\All Users\Magenta-Systems\ComCap4\Certificates
```

Common Name, usually Domain

The Common Name is the host domain name to be secured.

Key Bits

2,048 key bits are recommended, but shorter may be used if 2,048 is not supported by the CA.

Organisation Unit, Name

These details are really cosmetic, and are only displayed when a raw certificate is viewed, but may be validated by a CA.

Locality, State/County, Country Code

These details are really cosmetic, and are only displayed when a raw certificate is viewed, but may be validated by a CA.

Email Address

The email address is usually ignored.

Expire Date

Certificates have a limited life, to ensure they are not used perpetually if stolen or misused. Only valid for a self signed certificate. Once a certificate expires, client may refuse to connect to the server.

Is Certificate Authority

Used for a self signed certificate.

Create/Replace Files

When 'Create' is clicking, two small text files will be created in the Certificates sub-directory, with the specified file prefix, and the fields on the Network tab updated for the new certificate files.

For a CA Request, the certificate request file ending with '`certrequest.pem`' should be opened in a text editor and the base64 block from '`--BEGIN CERTIFICATE REQUEST--`' copied to the certificate authority web site when requested. ComCap generates a second private key file ending with '`prvkey.pem`' with '`--BEGIN PRIVATE KEY--`' which should not be sent anywhere. Once approved, the CA will return a file with a block '`--BEGIN CERTIFICATE--`' which should be specified as the certificate file.

If a Self Signed Certificate is generated, ComCap creates a file with suffix '`cert.pem`' with '`--BEGIN CERTIFICATE--`' instead of the CA request, and the second private key file ending with '`prvkey.pem`'.

With a CA certificate, there may be one or more certificates for the authority itself that were used to sign the server certificate (a certificate chain or bundle) and the file containing one or more of these '`--BEGIN CERTIFICATE--`' blocks needs to be specified as 'SSL Certificate Authority' in ComCap..

1.6 Installation

ComCap is usually distributed as a ZIP file `COMCAP.ZIP`, which should first be unzipped into a temporary folder. The program `SETUP.EXE` should then be run to install ComCap. About 15 Mbytes of disk space is required for applications, help and supporting files. ComCap may be installed on Windows XP and later, but is only supported on Windows 2003 and later.

If you have received an executable with the name `COMCAPS.EXE`, this should be run to install the software.

Important: a user with administrative level privileges must install ComCap, and configure the service version.

ComCap is normally installed into the `C:\Program Files\Comcap` directory. On Windows 64-bit editions, the install directory will be `C:\Program Files (x86)\Comcap`. Note the Background Service version is not installed when running set-up, but from within ComCap itself, using Common Settings, Capture Logging. Note the installation directory can be changed, if you don't want non-Microsoft software buried under `Program Files` with its various security restrictions, so `c:\magenta` could be an alternative.

ComCap 4 may be accessed by users without administrator access to the PC, provided file permissions are set-up accordingly for the directories being used by ComCap. Note that only administrators may start and stop Windows services. If ComCap is configured to run as a service, non-administrators will be able to run the system tray application and monitor the service, but not start or stop it (the buttons are hidden). The PC name, user name and security level are logged on start-up, for the service it will say: User: SYSTEM (Administrator).

All ComCap settings are stored in files, rather than in the registry, to ease sharing between users and back-up. Actual configuration settings are stored in the Windows common application path:

```
C:\Users\All Users\Magenta-Systems\ComCap4
```

The actual files are `comcap.config` and `comcap.current`, so the complete file name is `C:\Users\All Users\Magenta-Systems\ComCap4\comcap.config`. The `comcap.config` file is only updated when configuration changes occur, the `comcap.current` file contains dynamic information updated ever few seconds, such as log names and serial numbers. A sub-directory `certificates` is used to save SSL/TLS certificates.

User specific information such as windows sizes and positions, fonts, etc, for the tray application is stored separately for each user in a single file:

```
C:\Users\(Administrator)\AppData\Roaming\Magenta-Systems\comcap.forms
```

 or

where `(Administrator)` is replaced by the user logon name. If access to directories is blocked, or they don't exist, then the configuration files are stored in the ComCap program directory.

Until registered, ComCap will only run for one hour before capture is automatically stopped. It will be necessary to restart ComCap to continue capture. ComCap may be registered using a secure order form at the web site <http://www.magsys.co.uk/comcap/>. Once the order has been processed, a small file `userreg.txt` is returned as an email attachment, which should be copied into the ComCap program directory. If ComCap is already running, it should be exited and restarted to see the new file. When started, ComCap will show the name of the individual or company that registered the software and will run continually. The registration status is shown in the information log on start-up and when capture starts.

ComCap is run from Start, Programs, Magenta Systems, then click ComCap4. The ComCap icon will

appear in the System Tray, which should be clicked to restore the main application window. ComCap may be set-up to auto start each time windows is booted through Common.

Although the ComCap Background Service may be used logged-on to the 'local system account', for SQL use or access to network drives it's necessary to specify a specific user account with a password. This also ensures that dates and times in ComCap will be formatted according to that user's preferences, rather than the American default, and allows access to network resources. Windows Echo printing is only possible when using the account of a user that has the required printer installed. Note that ComCap is dependent upon other Windows services running, specifically Remote Procedure Call (RPC) and Telephony, and will not start if these are disabled.

Note that the ComCap PC must be running continually for data to be captured. Any power saving features, such as the hard disk being powered down, should be disabled, and suspending the PC will also stop anything being captured.

For the ComCap tray application needs administrator rights in order to start and stop the ComCap Service. This can be done just when needed by right clicking on the ComCap icon and selecting 'Run as administrator', or permanently through Properties, Compatibility, tick 'Run this program as an administrator'.

See Null Modem Emulator (com0com) for details about installation of this extra.

Uninstalling

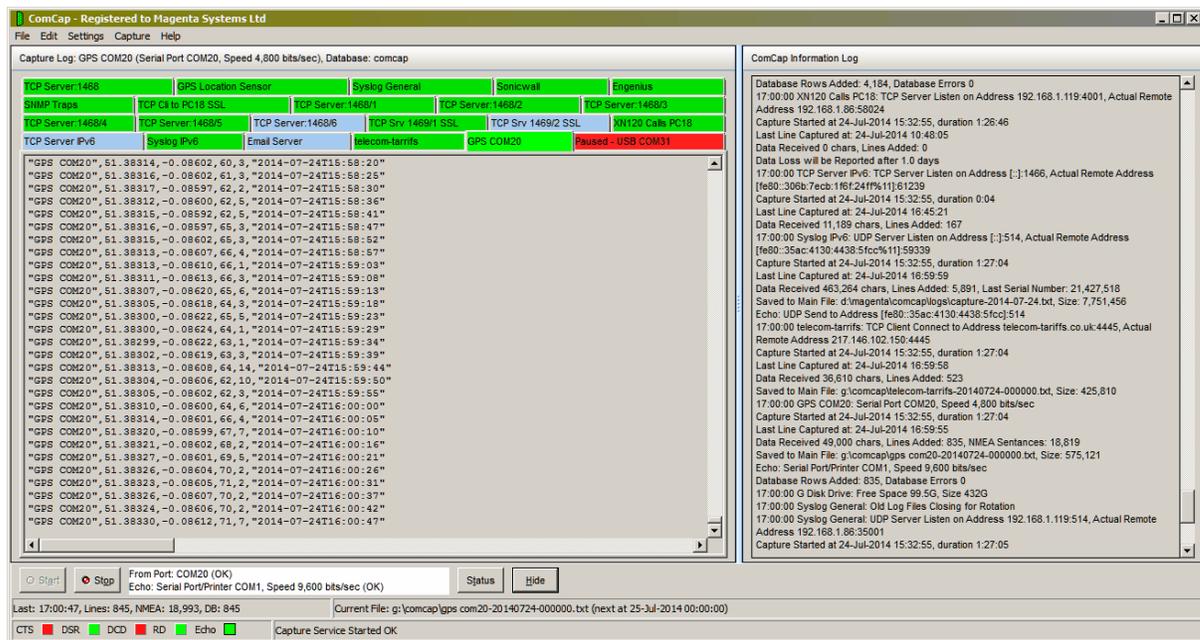
ComCap may be removed from the Control Panel, Add/Remove Programs, or by running the program `UNINSTAL4.EXE` in the installation directory. The uninstaller will remove all installed programs and files. It will not remove any capture or log files that ComCap has created.

1.7 Getting Started

When the ComCap Tray application is started, it immediately minimises itself to the system tray, usually in the bottom right of the screen.

If ComCap is currently capturing data, the system tray icon will show a green blob . If capture is stopped it changes to red .

Left or right clicking on the green ComCap icon will open the ComCap Main Capture Window, with a Capture Log window on the left and an Information Log window on the right.



Initial Set-Up

Before any capture may be done, various Common Settings must be specified, selected from the Settings.

If ComCap is to be run as a Background Service so it starts automatically when the PC boots before anyone logs in, it must be setup initially by a user with administrator privileges. When starting ComCap right click on the icon and click on 'Run as Administrator'. Alternatively, right click on the icon, click on Properties, then Compatibility, then tick 'Run this program as an administrator' so that ComCap always has admin privileges.

In Common Settings, Capture Logging the operating mode should be specified, whether capture is using the Tray or Background Service applications, whether they should auto start when Windows starts and whether the Background Service is to be monitored by the Tray application.

In Common Settings, Network, any network capture TCP Client, TCP Server or UDP Server channels should be created.

In Common Settings, Serial Ports, and serial RS232 port channels should be created.

In Common Settings, Log Files, the Default Log directory must be specified.

When saving Settings, it is possible an 'access denied' error may appear due to file security modify permissions not allowing the current user to update settings. This should not happen if the program is being run with administrator privileges. If the file access denied error occurs, use Windows Explorer to give modify permissions to the current to all files in the ComCap4 ProgramData directory shown in the info log window.

Once these Common Settings have been specified, the ComCap Main Capture Window will be updated to reflect the Network and Serial Port channels to be captured, and the Settings menu will allow additional Capture Settings to be specified for each capture channel, such as the format of data being captured, whether it should be saved to a database, printed or echoed to other computers, and the frequency of the Capture Log files saved.

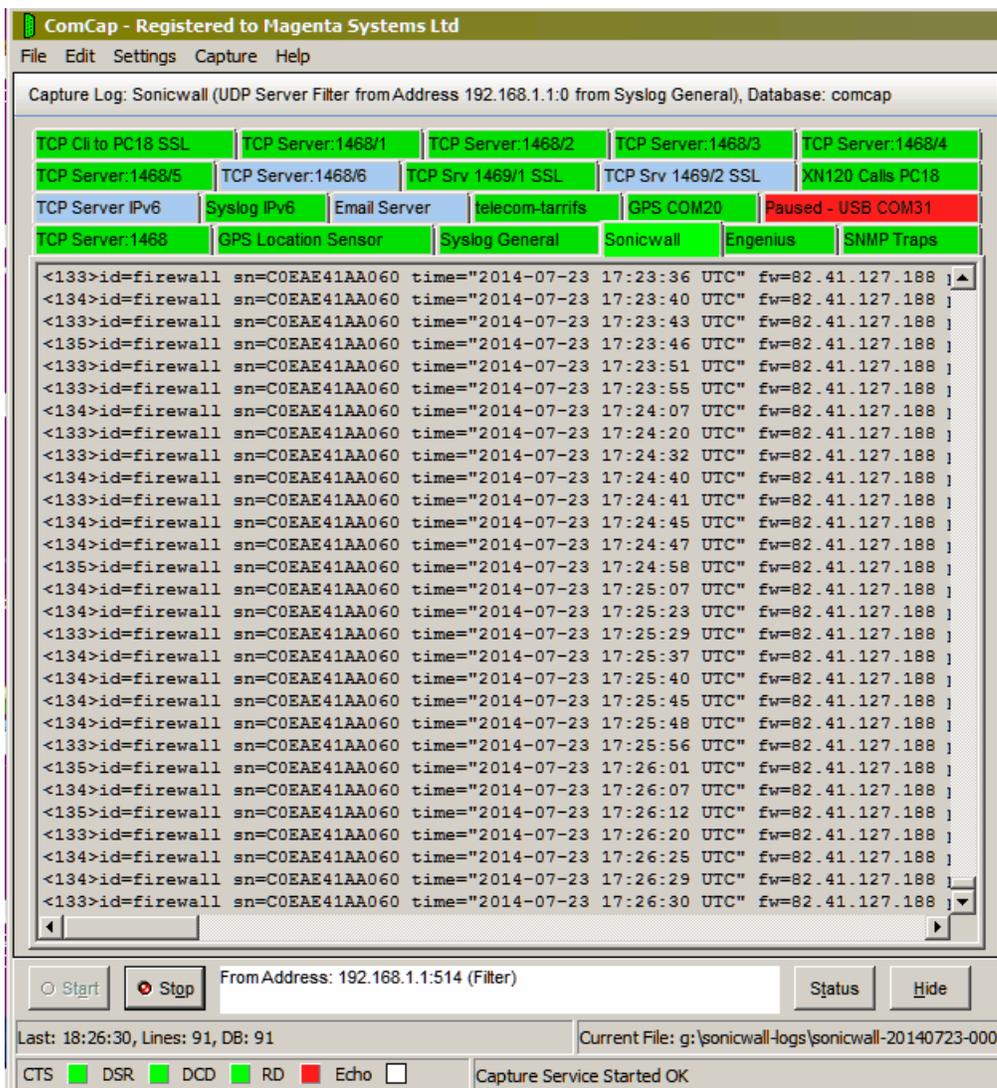
Common and Capture Settings may be changed while ComCap is capturing live data, but a prompt will

be provided after they are saved allowing capture to be restarted to make the new settings effective.

Finally, clicking the Start button in the main ComCap Main Capture Window will start capture.

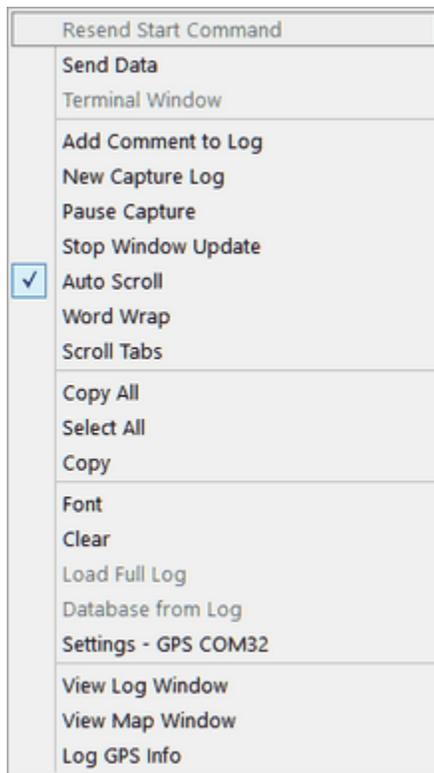
1.8 Main Capture Window

When the ComCap tray version is started, it immediately minimises itself to the system tray, usually in the bottom right of the screen. Left or right clicking on the ComCap icon will open the main ComCap window, with the Capture Log window on the left (first image below) and the Information Log window on the right (second image below). There is a narrow vertical splitter between the two windows that may be used to adjust the width of each, while the main window can be dragged by its edges or corners to increase or decrease its size.



(Main Window, Left, showing Capture Log Window)





(Main Window, Right, showing Information Log Window), Capture Log (Right Click Menu)

Capture Log Window

The Capture Log window is initially empty for a fresh ComCap install, the image above shows three serial COM and 19 network tabs that have been set-up through Common Settings, Network and Serial Ports.

The tabs are coloured to indicate capture state. Silver means all capture is stopped, Blue that the channel is ready to start capture (TCP Server only), Green that data capture has started and Red that capture for that channel has stopped. The brighter colour is the currently selected tab.

Clicking on a tab changes the Capture Log window to the new serial or network channel and loads and displays previously logged data for that channel, if any. This data may be initially several days old, since a new log is not opened until new data is captured. The intention is that any recently captured data can be viewed, even when stopping and restarting capture.

Any channel can also be displayed by selecting it from the main Capture menu, and may be configured from the main Settings menu. The title bar shows the configuration of the current channel:

```
Capture Log: CDRs COM3 (Serial Port COM3, Speed 9,600 bits/sec), Database: COMCAP
```

while the panel in the button bar show the current state of the channel:

```
From: COM3 (OK), Echo: UDP Send to IP 192.168.1.107:514 (OK)
```

The status bar below the button bar shows the time that the last line was captured, the number of lines captured since starting, optionally the number of rows written to the database, then the file name of the main current file to which this channel is being captured, and finally the date and time at which the capture file name will be rotated and a newly named file opened.

The status bar at the bottom of the window has five coloured indicators labelled CTS, DSR, DCD, RD and Echo which are made active for the current channel. For serial ports, the first three show the

status of the Clear To Send, Data Set Ready and Data Carrier Detect signal lines as green (low) or red (high), while for networks CTS indicates listening or attempting to connect, while DSR and DCD indicate an open connection. The fourth Receive Data indicator will flash green for one second as data is received (for data at a rate of one line per second or faster it will stay green), while the first Echo indicator shows white for no echo, green if echo is OK or red if echo has failed. Note the signal indicators are meaningless when capture is stopped.

Right clicking on the Capture Log window displays a pop-up menu that offers further options, depending on whether capture is stopped or started, which are detailed below. Most of these options are also available on the main menus.

Information Log Window

The Information Log window shows messages about which channels are being captured and their configuration such as to which log files and databases captured data is being written. Typically, the status information is updated hourly for all channels with cumulative totals, but may be reported at any time by clicking the Status button. Any capture errors are shown in this window. Right clicking on the Information Log window displays a pop-up menu that offers further options which are detailed below.

When the network configuration is loaded, and when capture is started, a warning is logged if a configured local IP no longer exists on the PC, due to networking being changed. Currently, capture will still attempt to start, since other channels may still work, but those channels trying to use a non-existent IP address will give network errors. This mainly affects TCP and UDP server channels set-up to listen on a single IP, rather than 0.0.0.0 for all IPs on the PC. On the other hand, if the PC IP address has changed perhaps due to DHCP being configured, data directed at the original IP address will not arrive anyway.

Start and Stop Capture buttons

The Start and Stop buttons allow capture to be started and stopped. The actual action depends on whether the capture is by the Background Service or Tray applications, which is indicated in the status bar at the bottom of the screen on start-up. If using the Background Service, the buttons will start and stop the service, if the logged-on user has the rights to do so (otherwise the buttons are disabled), and will also start the tray version monitoring the service, if so configured. If capturing using the Tray application, capture will immediately start.

When stopping capture, a dialog will appear to 'Confirm Stop All Captures?', in case the button is clicked by accident. The confirm stop dialog will also appear when exiting the ComCap Tray version if capture has been started, but not if Background Service is being used.

Status button and Capture Status menu

The Status button and Capture Status main menu option are used to log the status of all capture channels, including all the current log files names. This may be configured to occur every hour in Common Settings, Log Files.

Hide button and Hide Main Window menu

The Hide button and Hide Main Window file menu options both cause the main window to be minimised to the System Tray, while capture continues.

Stop Capture and Exit, and Exit menu option

The Exit file menu option and the X Close button in the top right Window cause the Tray version to terminate. If the Tray version is performing capture, the option will say Stop Capture and Exit and the confirm stop dialog will appear before ComCap is exited.

Pause Capture and Resume Capture right click menu

These options are only available if capture has been started, and allow a single channel to have capture paused and then resumed. The tab description indicates any channels that are paused. While paused, the Capture Settings may be changed. This option may sometimes be used to reset a network channel that gets stalled.

Settings menu and right click menu

Allows Common Settings or channel specific Capture Settings to be changed. This may only be done while capture is running, but if the settings are changed a prompt will appear so capture can be restarted for all channels (after Common Settings) or just this channel to make the new settings effective.

Edit menu options

There are various option on the Edit and window right click menus, that allow captured data to be selected and copied to the clipboard, Select All, Copy, and Copy All. Clear may be used clear the current Capture Log window, but it will be refreshed if another channel tab is selected and then the current channel reselected.

Stop Window Update right click menu

On the Capture Log window right click menu, Stop Window Update is a toggle option (ticked when set) that temporarily stops display of captured data for the selected channel only.

Auto Scroll right click menu

On the Capture Log window right click menu, toggling Auto Scroll stops ComCap forcing scrolling to the end of the window before adding a new line of captured data. However, this behaviour depends upon the version of Windows, it does not seem to have any effect on W2K, but with Windows 98 the log window will flicker less. This applies to all channels.

Word Wrap right click menu

On the Capture Log window right click menu, toggling Word Wrap determines whether captured lines are word wrapped to the Capture Log window width, or displayed in a horizontally scrolled window. This applies to all channels.

Scroll Tabs right click menu

On the Capture Log window right click menu, toggling Scroll Tabs determines whether multiple Capture Log window tabs are displayed in two or more rows, or instead horizontally scrolled by the left and right arrows. This will only matter if about four or more channels are captured, where the number of lines of captured data that can be viewed will be reduced as the number of channels increases. But scrolling means the capture state of all channels can no longer be easily checked since many tabs will be hidden. This applies to all channels. This option is set automatically if more than 32 channels are configured, since otherwise there is unlikely to be sufficient screen space to display all the tabs in rows.

Log Font menu and right click menu

Allows the font used for the Capture Log and Information Log windows to be separately specified. The Capture Log font must be fixed width, Lucida Console being very readable or else Courier New, usually sized at 8 point. The Information Log window can be any font and defaults to Arial 8 point.

Load Full Log right click menu

Only available when capture is stopped, Load Full Log causes the full current log to be loaded for display. Normally ComCap only displays the last few thousand lines (set in Capture Logging while this option will display all lines in the log in the Capture Log window, which might take a few seconds to display.

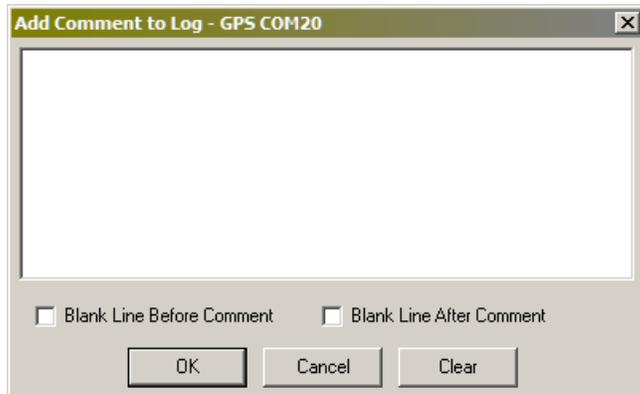
Database from Log right click menu

This option allows previously captured data to be added to the database, from the capture log. This is typically done in a recovery situation when a database problem meant data was only captured to a log and not the database. See Capture Settings, Database for more information.

Add Comment to Log right click menu

For some capture applications, it may be useful to add a comment into the capture log. The right click menu Add Comment to Log option causes a small dialog will appear, allowing one or more lines to text to be entered, with tick boxes specifying whether blanks lines should be added before or after the text lines. This feature is intended to assist in documenting batch captures, perhaps from laboratory

instruments. Note the added text is processed in the same way as any normal captured line, which might mean serial number or time stamps being added. Add Comment is only available when capturing using the Tray version.



New Capture Log, right click menu

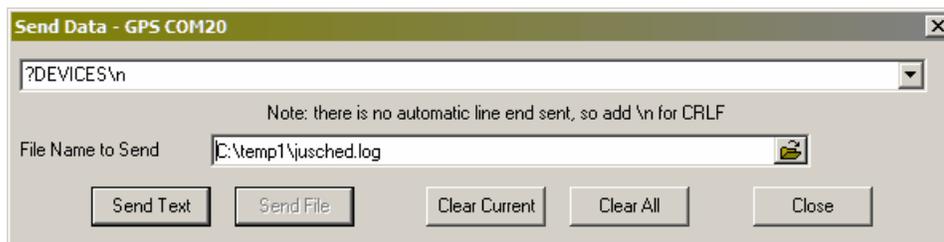
Allows a new Capture Log file to be created on demand, rather than according to the normal settings, perhaps so the old log may be checked without worrying about more captured data being added. The Information Log should report the capture log has been rotated and show the old and new log names. The new log will have the current time, which means the Log Name Format must include a time mask, ideally including seconds otherwise this can only be used once a minute.

Resent Start Command, right click menu

If a Start Command has been configured, it may be resent using the right click menu option. This may be needed to send data to 'wake-up' a capture device.

Send Data, right click menu

The right click menu Send Data option displays a new window allowing custom data to be sent on demand, with the last 50 command sent selectable from a drop down box. This may be needed to send data to 'wake-up' a capture device. The text entered may include the same escape sequences and pauses as the Start Command, see Capture Settings, General For TCP/UDP only, a file to be selected and sent, typically to configure remote capture device, or load new firmware. Note the file may not contain and escape sequences or pauses.



View Log Window menu and right click menu

For improved log viewing, there is also a resizable Log View window. This may be opened from View Log Window on the right click menu when the current capture log will be loaded and displayed, or from View Log Windows on the file menu which will initially display a Select ComCap Log file selection window, allowing any log to be selected and displayed. The View Log window includes an Update Current Log (F5) menu option to reload the current log, or another log may be specified and opened.

```

ComCap View Log - g:\comcap\gps com20-20140723-000000.txt (19.8K)
File Edit Help
"GPS COM20", 51.38290, -0.08629, 64, 0, "2014-07-23T02:26:26"
"GPS COM20", 51.38256, -0.08767, 64, 103, "2014-07-23T02:26:31"
"GPS COM20", 51.38225, -0.08755, 64, 35, "2014-07-23T02:26:45"
"GPS COM20", 51.38175, -0.08821, 64, 71, "2014-07-23T02:26:51"
"GPS COM20", 51.38199, -0.08840, 64, 29, "2014-07-23T02:26:57"
"GPS COM20", 51.38242, -0.08665, 64, 130, "2014-07-23T02:27:06"
"GPS COM20", 51.38294, -0.08660, 64, 57, "2014-07-23T02:27:11"
"GPS COM20", 51.38271, -0.08706, 64, 40, "2014-07-23T02:27:16"
"GPS COM20", 51.38238, -0.08745, 64, 45, "2014-07-23T02:27:21"
"GPS COM20", 51.38256, -0.08701, 64, 36, "2014-07-23T02:27:26"
"GPS COM20", 51.38259, -0.08692, 74, 7, "2014-07-23T02:27:32"
"GPS COM20", 51.38229, -0.08764, 64, 60, "2014-07-23T02:27:37"
"GPS COM20", 51.38238, -0.08674, 159, 63, "2014-07-23T02:27:43"
"GPS COM20", 51.38220, -0.08731, 132, 44, "2014-07-23T02:27:48"
"GPS COM20", 51.38189, -0.08803, 107, 60, "2014-07-23T02:27:54"
"GPS COM20", 51.38190, -0.08806, 94, 2, "2014-07-23T02:27:59"
"GPS COM20", 51.38205, -0.08800, 87, 17, "2014-07-23T02:28:04"
"GPS COM20", 51.38216, -0.08802, 82, 12, "2014-07-23T02:28:09"
"GPS COM20", 51.38220, -0.08804, 78, 4, "2014-07-23T02:28:15"
"GPS COM20", 51.38222, -0.08804, 76, 1, "2014-07-23T02:28:20"
"GPS COM20", 51.38218, -0.08821, 74, 12, "2014-07-23T02:28:26"
"GPS COM20", 51.38197, -0.08838, 74, 26, "2014-07-23T02:28:36"
"GPS COM20", 51.38183, -0.08864, 71, 24, "2014-07-23T02:28:51"
"GPS COM20", 51.38187, -0.08835, 69, 21, "2014-07-23T02:29:00"
"GPS COM20", 51.38227, -0.08703, 66, 107, "2014-07-23T02:29:05"

```

Telnet Terminal Window, menu and right click menu

If this option is taken from the right click menu, it will display the Telnet Terminal window with the IP address defaulted to that of the channel. The Telnet Terminal allows interaction with remote TCP/IP Servers, for testing and configuration. It is only possible to use the Telnet Terminal while capture is stopped.

View Map Window

If the channel is processing GPS data, clicking this option display the ComCap Map window.

Log GPS Info

If the channel is processing GPS data, clicking this option will add general GPS information to the info log, depending on the capabilities of the GPS source. For a full NEMA data stream, satellite information is listed:

```

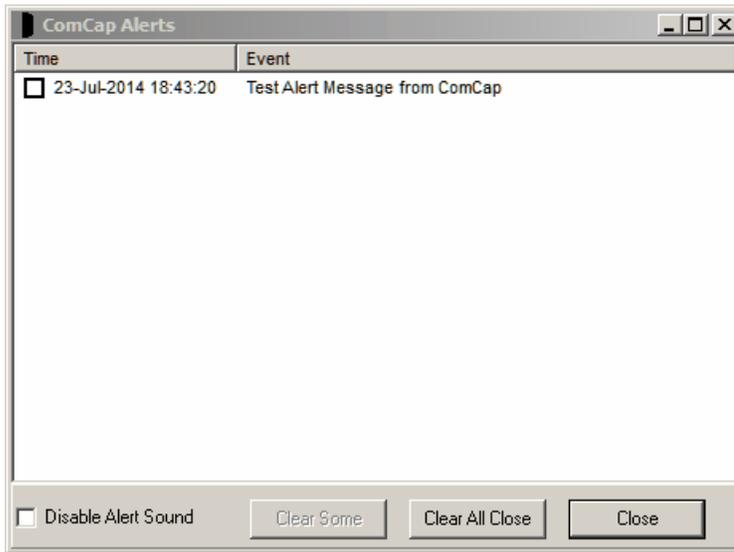
Satellites in View = 12
Satellites Used = 4
Speed (Knots) = 1.6
True Heading = 85.91
Error Radius = 3.4
Geoidal Separation = 47m
PDOP = 4.5
HDOP = 3.4
Satellite 25, Azimuth 267, Elevation 69, S/N 24, Fix
Satellite 12, Azimuth 61, Elevation 68, S/N 18, Fix
Satellite 14, Azimuth 263, Elevation 49, S/N 27, Fix
Satellite 2, Azimuth 97, Elevation 21, S/N 4
Satellite 6, Azimuth 60, Elevation 20, S/N 5
Satellite 29, Azimuth 193, Elevation 23, S/N 4
Satellite 24, Azimuth 129, Elevation 36, S/N 0
Satellite 31, Azimuth 301, Elevation 15, S/N 0
Satellite 4, Azimuth 26, Elevation 7, S/N 0

```

Alert Window menu

The Alert Window normally appears automatically when an alert is triggered, but may be opened from

the Alert Window file menu option.



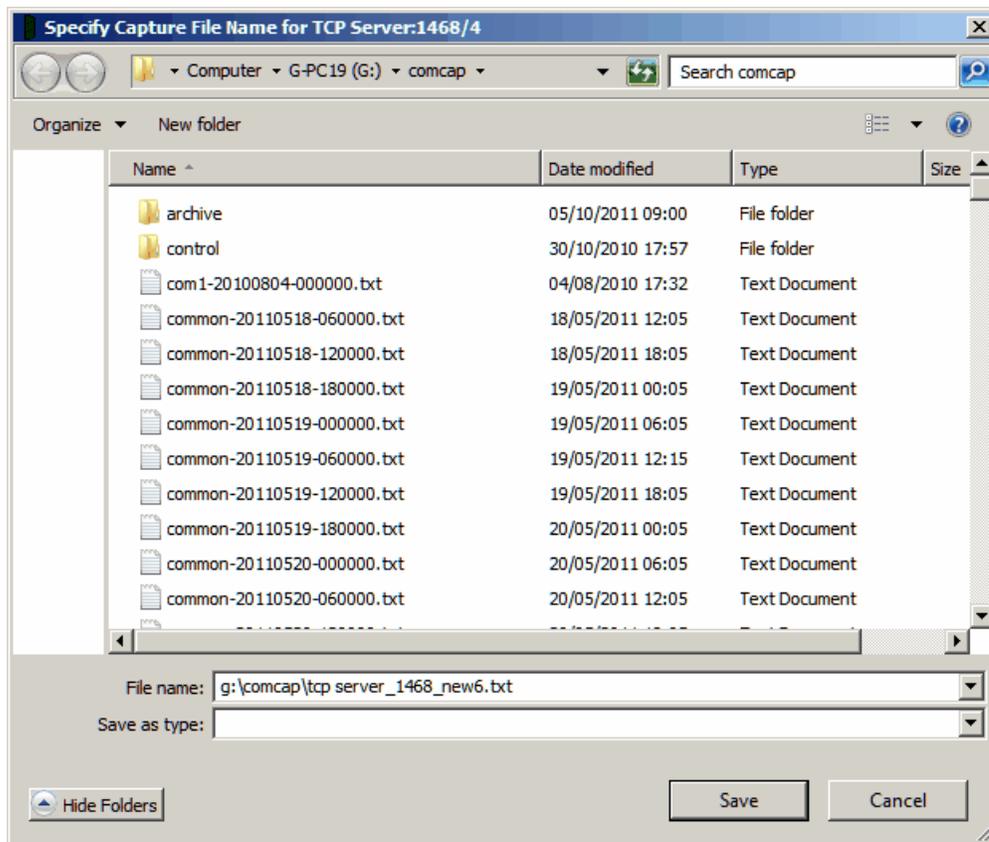
The Alert Window displays multiple alerts, which may be cleared individually, and will show alerts when the ComCap Background Service is running, provided the Tray application is also running. Buttons available are Clear Some (selected alerts), Clear All Close and Close. Ticking the Disable Alert Sound box will temporarily disable any further sounds until ComCap is restarted, useful when continual alerts are being generated.

Test Alert menu

To allow alerts to be tested, the Test Alert file menu options causes an immediate test alert, that may be displayed, sent as an email or an SMS to a mobile telephone, depending on which are set-up in Common Settings, Email/SMS.

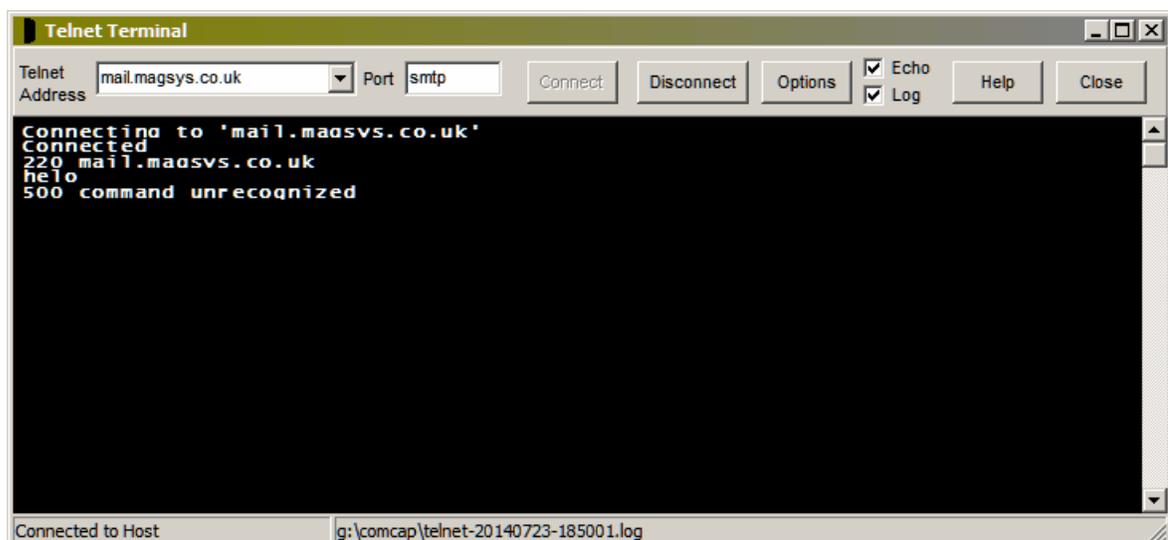
Prompt on Start for File Name

One or more capture channels may be specified in xCapture Settings, Files to prompt for a specific file name each time capture is started, in which case a dialog similar to the following will appear:



Note that capture will not start until the file name is specified. An existing file name may be used, with captured data added to the end of the file. This feature is intended for applications where data is being captured from a single device for a specific purpose, such as a laboratory test. The 'Add Comment to Log' right menu option might also be useful to add information to the capture log.

1.9 Telnet Terminal



This window provides ANSI terminal emulation using the TCP/IP Telnet protocol to interact with a remote terminal server or host computer. The window is resizable depending upon desired size and screen resolution. A number of terminal options are specified through a dialog box. A log of each Telnet session may be saved, written to the normal logging directory with a file name format telnet-yyyymmdd-hhnnss.

Telnet Address

Specify the host address for the remote computer. This will only connect if the host supports the Telnet protocol. The last 20 addresses specified will be saved for re-use in the drop down list box.

Port

The connection port for the remote computer, generally 'telnet'.

Connect

This button initiates a connection to the remote computer. This may fail if an invalid Telnet Address has been specified or if the remote computer does not support Telnet.

Disconnect

This button closes the connection.

Options

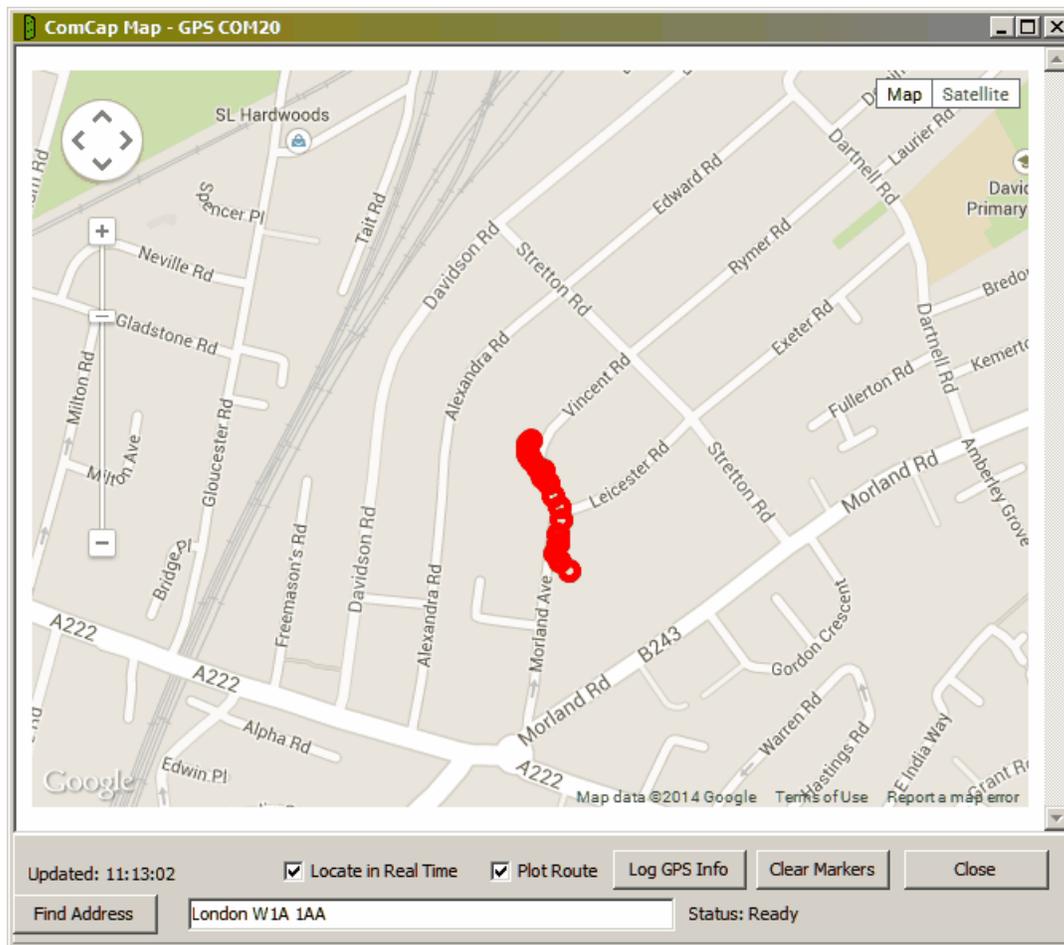
Display a dialog box with various terminal appearance options. These may be defaulted appropriately by clicking the A11, Labo, RDV or USUS buttons.

Note: Options are saved separately for each telnet host address specified, when the Options dialog is saved, and automatically restored when that host address is used again.

Rows	The number of screen rows for the terminal emulation window, normally 25 rows. The font size will be adjusted to fit the rows into the window.
Cols	The number of columns for the terminal emulation window, normally 80 columns.
Lheight	The Line Height in points, usually 12 point.
Font	Display a Font selection dialog allowing the desired fixed pitch screen font to be chosen.
AutoCR	If ticked, a carriage return is sent when the cursor key is used to move down a line.
AutoLF	If ticked, a line feed is sent when the carriage return is sent.
Local Echo	If ticked, any typing in the terminal will appear locally. This is used when the remote computer does not echo text back.
Monochrome	if ticked, disables colours.
OEM Charr Set	If ticked, use the OEM character set used by DOS.
Uppercase	If ticked, forces typing as upper case.
Function Keys	Defines the keyboard function keys are being compatible with SCO UNIX, VT100 or A11.

1.10 ComCap Map

If the channel is processing GPS data, right clicking in the main windows allows the ComCap Map window to be displayed. The map window is free floating and may remain open while ComCap is hidden. However, only a single channel may be mapped at a time:



Note this Windows uses Google maps, and requires internet access to download the latest maps, although earlier displayed maps may remain cached if offline. A red marker indicates a new GPS location.

Locate in Real Time

Tick box that determines whether new GPS location marker should be plotted on the map.

Plot Route

Tick box that determines whether old markers should remain on the map when a new one is plotted, thus creating a route.

Log GPS Info

Clicking this option will add general GPS information to the info log, depending on the capabilities of the GPS source.

For a NEMA data stream, detailed satellite information is listed:

Satellites in View = 12
Satellites Used = 4
Speed (Knots) = 1.6
True Heading = 85.91
Error Radius = 3.4
Geoidal Separation = 47m
PDOP = 4.5

HDOP = 3.4
Satellite 25, Azimuth 267, Elevation 69, S/N 24, Fix
Satellite 12, Azimuth 61, Elevation 68, S/N 18, Fix
Satellite 14, Azimuth 263, Elevation 49, S/N 27, Fix
Satellite 2, Azimuth 97, Elevation 21, S/N 4
Satellite 6, Azimuth 60, Elevation 20, S/N 5
Satellite 29, Azimuth 193, Elevation 23, S/N 4
Satellite 24, Azimuth 129, Elevation 36, S/N 0
Satellite 31, Azimuth 301, Elevation 15, S/N 0
Satellite 4, Azimuth 26, Elevation 7, S/N 0

For the Concox TR02 device GSM information is added but less satellite information:

Sensor ID: 358899053538305
GSM Signal Level: 4
Voltage Level: 5
Location Area Code: 0195
Mobile Network Code: 0
Mobile Cell Id: 0
Satellites in View = 13
Satellites Used = 13
True Heading = 88
Magnetic Heading = 88
Satellite 1, Azimuth 0, Elevation 0, S/N 27
Satellite 2, Azimuth 0, Elevation 0, S/N 36

Clear Markers

Clicking the button clears all markers on the map.

Find Address

Allows the map to be relocated to the result of an address search. Untick Locate in Real Time first, or the map will revert to plot a new location.

Part



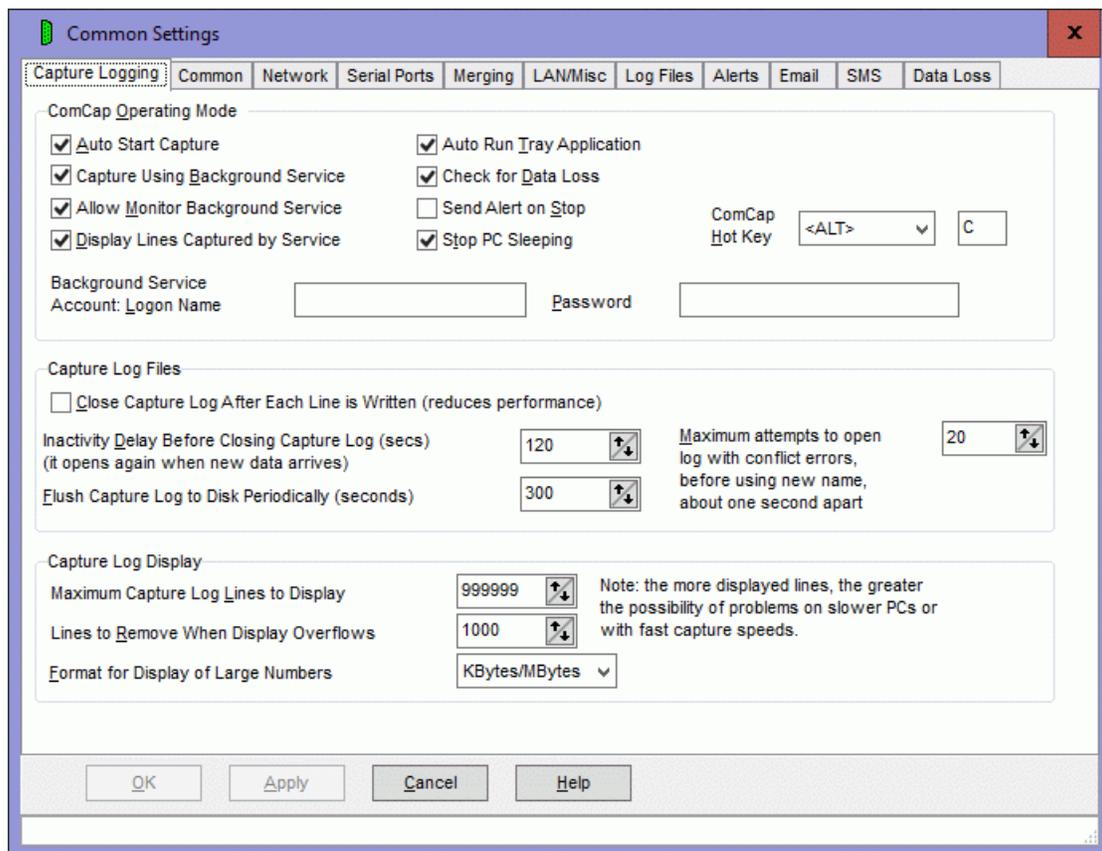
2 Common Settings

2.1 Capture Logging

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines the ComCap Operating Mode, Capture Log Files options that apply to allow capture channels, and Capture Log Display settings for monitoring capture in real time.

Important: a user with administrative level privileges must install ComCap, and configure the service version.

The ComCap tray version may be run as an administrator by right clicking on the ComCap desktop icon and clicking 'Run as administrator' or through Properties, Compatibility, 'Run this program as an administrator'. With Windows 10, if ComCap is given permanent administrator rights, it will not be possible to have it automatically start when Windows is booted. Workarounds for this are being investigated.



Auto Start Capture

This option specifies that capture should start immediately ComCap is run, without waiting for the Start Capture button to be clicked. Note that Background Service only auto starts when the PC boots, if it's newly configured (see below), it needs to be start manually.

Capture Using Background Service

If ComCap has been run by a logon without administrator privileges, the tick box is greyed out and a message 'Only an Administrator Can Change Background Service Details' will appear. To overcome this, when starting ComCap right click on the icon and click on 'Run as Administrator'. Alternatively,

right click on the icon, click on Properties, then Compatibility, then tick 'Run this program as an administrator' so that ComCap always has admin privileges.

This option specifies that ComCap will only capture using the background service, not the tray application. Should be used in conjunction with Auto Start Capture option so that capture starts as soon as the PC boots. Ticking this option causes 'ComCap Service' to be installed in the Windows Services database, or removed from the database if unticked. Changing this option will cause display a dialog confirming that ComCap needs to exit once Common Settings are saved and should then be restarted. The PC Event Log will contain entries for ComCap4, showing when it was started and stopped, and some errors.

Note it is not possible to run ComCap as a service if any capture channels have Log Name Format of 'Prompt on Start' specified, which causes a dialog to appear when capture starts requesting a file name.

The service properties will have Recovery set as 'Restart the Service' so that ComCap automatically restarts if for some reason it crashes. Note that ComCap is dependent upon other Windows services running, specifically Remote Procedure Call (RPC) and Telephony, and will not start if these are disabled.

Background Service Account

If the Background Service is configured, it will normally be set-up to use the local system account. Running in the local system account has some limitations. SQL can usually not be accessed, network shared drives might not be accessed (so the capture and log files must be on the local PC), no printing is available nor are regional settings available so some dates might be formatted in American style. A local PC account name and password may be specified here, to allow the Background Service to run in that account, with all functionality becoming available.

Note that mapped network drives (ie those accessed using a drive letter) are still not available even with a logon, unless set-up specifically for the Background Service through Local Area Network Logon and Drive Mapping.

The first time the Background Service is configured, it will may be necessary to update 'ComCap Service' Properties, Login, This Account, click OK and a dialog should ask if the account should be updated with 'Logon as Service Rights', and confirm this. Unless this is done, the service will give a login error on start-up. This may not be necessary if the account already has service rights, perhaps required for another application.

Allow Monitor Background Service

This option specifies that the ComCap background service and tray applications are linked together, so that the log windows and indicators are updated with what the service is doing, in the same way as when capturing using the tray application, and that clicking the various buttons and options cause those actions in the background service. For instance, clicking the main Start button will run the background service to start capture instead of the tray version doing it. Note the major difference here is that exiting the tray application will not stop capture if the background service is being used. The tray application continually monitors the service so if the service is found to have stopped an alert will be sent and it will be automatically restarted after 20 seconds, provided the Stop button is not pressed meanwhile. An alert is also sent on start-up if ComCap is found to have previously stopped without a clean close down.

Display Lines Captured by Background Service

This tick box is only applicable if the Background Service is used, and specifies that the ComCap Tray application is able to display captured text as it were capturing the text itself. Effectively it means that the Service echoes each captured line to the Tray application for display using a TCP/IP stream. If the volume of data expected to be captured is very high (hundreds of lines per second), or if live monitoring is not required, untick this option. Note captured data is only echoed while the Tray application window is open, not if it's hidden. The information log is always echoed, if the Tray application is running, so that progress and error messages may be seen.

Auto Run Tray Application

This option specifies that the ComCap Tray application should start as soon as the user logs-on. Should be used in conjunction with Auto Start Capture option so that capture starts as soon as the user logs-on on, if capturing using the tray application.

Check for Data Loss

If ticked, allows loss of data to be detected by checking how many minutes since the last data was received. This is only useful where the data flow is reasonably steady, but different warning times may be set for different times of the day and week, for instance with business telephone call logging where there may be no data at night or at the weekends. This setting also needs to be ticked in each separate channel before it is effective, but note the same data settings will apply to all channels. There are various Data Loss Recovery options that need to be configured.

Send Alert on Stop

If ticked, specifies that an alert should be sent when ComCap stops. Alert methods are defined at Alert Actions. Note an alert is automatically sent when ComCap starts, if the previous stop was unexpected.

Stop PC Sleeping

If ticked, Comcap tries to stop Windows placing tablets and laptops in sleep mode, but testing shows Windows may ignore this setting, unfortunately.

Close Capture Log after Each Line is Written

Normally the capture log file remains open to allow continuous data to be captured (but see the 'Inactivity Delay' and 'Flush Capture Log' options below). This tick box option causes the capture log file to be closed after each line has been written and is really designed for low speed data capture, since there is a system overhead to opening and closing the capture log file. But it will be useful for those users that have another application needing to access the capture log file. If enabled, the other two options for closing the log are disabled. If another application accesses the ComCap capture log file, ensure it's only ever opened without a write lock, otherwise ComCap will get errors attempting to reopen the file, and will eventually start using a new log file (see below).

Inactivity Delay before Closing Capture Log (seconds)

This option specifies how many seconds ComCap should wait after the last line of data was captured before the capture log file is closed. Closing the capture log file forces captured data to be flushed to disk. This inactivity delay may be set between one second and 999 seconds, defaulting to 120 seconds. The shorter the delay, the safer the data, but there's always an overhead opening and closing files so a figure between 30 and 180 seconds is a good compromise. Beware the capture log may not be closed for much longer periods if there is never a gap in captured data longer than this delay period. Data is normally written to disk whenever internal buffers fill, but this does not necessarily happen at the end of a line, so if the PC crashes, a partial record may be found at the end of the file. If data security is absolutely crucial, use the 'Close capture log after each line written' option above.

Flush Capture Log to Disk Periodically (seconds)

This option specifies that the capture log file should be closed regularly so that data is flushed to disk. This setting is effective only used when new data is being continually captured and the 'Inactivity delay' setting (see above) does not cause the file to close. If the PC subsequently locks up or crashes, less information will be lost than if the file remained open. This setting defaults to 120 seconds with a minimum of one second and a maximum of 999 seconds (note 'Close capture log after each line' is more effective, but with a higher system overhead).

Maximum Attempts to Open Log with Conflict Errors

This option specifies the number attempts that will be made to open a capture or information log when there are conflict problems, perhaps because the file is being backed-up or accessed by another application. The default number of attempts is 10, maximum 99, with file open attempts about one

second apart. Any data captured while the log is still closed is cached, and written as soon as the log is successfully opened. After the specified number of failed attempts, the log file name is changed to the current date and time with seconds, ie `name-yyyymmdd-hhmmss.txt`. After continued failure attempts of double that specified (that is new attempts each with a new file name), capture will stop for that channel.

Maximum log lines to display, and Lines to remove when display overflows

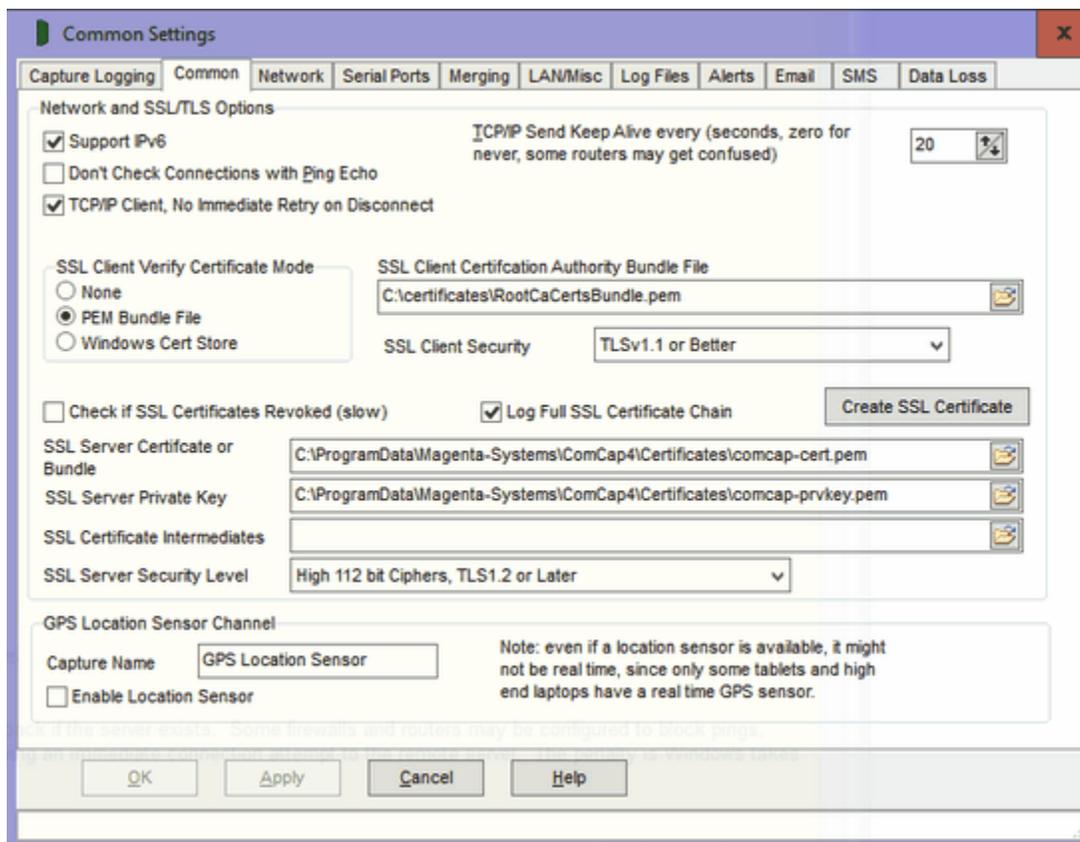
These settings relate to viewing captured data as it arrives on the screen. Memory restrictions mean that it's sensible to restrict the amount of old captured data available for viewing in the scrolling capture window. This is particularly important when multiple channels of data are being captured simultaneously, because when changing the channel being viewed the old logged data has to be reloaded from disk. For best performance, the fewer lines of captured data that are shown in the capture window, the better. The 'Maximum log lines to display' defaults to 5,000 lines, but may be set between 100 and 99,999 lines. If the number of lines in the capture window exceeds this figure, it is automatically reduced in size by 'Lines to remove when display overflows' (which must be fewer lines than the maximum) and defaults to 500 lines. These example settings means that at least the previously 4,500 lines captured will always be available for scroll back, with a maximum of 5,000 lines.

Format for Display of Large Numbers

Determines how ComCap displays long numbers, either as Bytes (ie 123,456,789 bytes) or KBytes/MBytes (ie 123.5MBytes). This causes file size, lines captured, data rows written, etc, to be displayed and logged in KBytes or MBytes once they exceed 99,999, for easier reading. .

2.2 Common

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines the common Network and SSL/TLS settings, and allows a GPS Location Sensor Channel to be set-up.



Support IPv6

Ticking this box enabled IPv6 support for ComCap, allowing IPv6 addresses to be specified in various Windows.

Don't Check Connections with Ping Echo

As detailed on Network configuration, TCP Client normally sends a ping to a remote server, which is echoed back if the server exists. Some firewalls and routers may be configured to block pings, causing ComCap to fail to receive the echo and be unable to connect. This tick box bypasses the ping, allowing an immediate connection attempt to the remote server. The penalty is Windows takes about 40 seconds to time out a failed connection attempt, compare to 10 seconds for ping.

TCP/IP Client, No Immediate Retry on Disconnect

TCP/IP is often not a reliable protocol due to routing issues, sessions may drop expectedly because a router somewhere has been rebooted, re-cabled or many other reasons. ComCap therefore attempts to re-establish any TCP/IP Client connections that are unexpectedly terminated. In existing releases, there are two immediate attempts to reconnect, after which the number of further attempts and delay between them is defined in the grid in Common Settings, Network (zero attempts means keep trying for ever). This option applies to all channels, capture and echo, and prevents those two immediate retries so the first retry is after 'Wait Seconds'. Some appliances may be unable to cope with an immediate reconnect.

TCP/IP Send Keep Alive

For TCP Client only, this option enables automatic keep alive messages to be transmitted every few seconds, defaulting to 20 seconds. Keep alive is only needed when there are long gaps during data capture, and a router or firewall may disconnect the TCP/IP connection due to inactivity (perhaps after 5 or 10 minutes). This option should not be needed on LANs. Setting seconds to zero disables Keep Alive, which may upset some routers.

SSL Client Verify Certificate Mode

When using TCP/IP Client, specifies whether the SSL certificate from the remote server to ensure it is talking to the correct server. Note this increases the time for a connection to be made while certificates are transmitted and checked, potentially causing the connection to fail. Also, ComCap needs the trusted root certificate used to sign the server's certificate, which is how the chain of trust is proved, from a PEM Bundle File or Windows Certificate Store which is used by Internet Explorer and other applications. The type of validation is common to all ComCap channels, but individual channels need to also be set to check the remote certificates.

SSL Client Certificate Authority Bundle File

The PEM Bundle File is a file supplied with ComCap with a few hundred root certificates:

C:\ProgramData\Magenta-Systems\ComCap4\Certificates\RootCaCertsBundle.pem

Extra PEM root certificates can be added to this file if needed, manually, or it can be replaced with a file containing only certificates that should be trusted, perhaps self signed certificates.

SSL Client Security

Specifies the SSL security level for all TCP/IP Clients (including email) to ensure that minimum SSL/TLS security standards are enforced. The options are:

None	All protocols and ciphers, any key lengths
SSLv3 Only	SSLv3 only, all ciphers, any key lengths, MD5 hash
TLSv1 Only	TLSv1 only, all ciphers, RSA/DH private keys => 2,048 bits
TLSv1.1 Only	TLSv1.1 only, all ciphers, RSA/DH private keys => 2,048 bits
TLSv1.2 Only	TLSv1.2 only, all ciphers, RSA/DH private keys => 2,048 bits
TLSv1.3 Only	TLSv1.3 only, all ciphers, RSA/DH private keys => 2,048 bits
TLSv1 or Better	TLSv1 or later, all ciphers, RSA/DH private keys => 1,024 bits
TLSv1.1 or Better	TLSv1.1 or later, all ciphers, RSA/DH private keys => 1,024 bits
TLSv1.2 or Better	TLSv1.2 or later, all ciphers, RSA/DH private keys => 2,048 bits
Backward Ciphers	TLSv1 or later, backward ciphers, RSA/DH private keys => 1,024 bits, ECC keys => 160 bits, no MD5, no SHA1 hash
Intermediate Ciphers	TLSv1.1 or later, intermediate ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash
High Ciphers, 2048 keys	TLSv1.2 or later, high ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash
High Ciphers, 3072 keys	TLSv1.2 or later, high ciphers, RSA private keys => 3,072 bits, ECC keys => 256 bits, Forward Security forced
High Ciphers, 7680 keys	TLSv1.2 or later, high ciphers, RSA private keys => 7,680 bits, ECC keys => 384 bits, Forward Security forced

The default security level is 'TLSv1.1 or Better' which PCI DSS council standards, but this is expected to become TLSv1.2 or better soon. Generally the only reason to support old protocols or low security standards is to access 10 year or older servers that only supported those old protocols. Likewise, all SSL certificates have used 2,048 bit minimum private keys for several years and any older ones should have long expired (except some root certificates). The SHA1 hash was used to sign old certificates now replaced by SHA2 (aka SHA-256). Some SSL ciphers are potentially open to attack, but may still be needed to access very old servers that don't support anything better. Private keys with RSA 3,072 bits are the minimum recommended by NIST for use after year 2030, larger RSA keys increase the size of SSL certificates and thus the handshaking for each SSL connection.

Note if the security level is set too high, an SSL/TLS connection may just fail without any sensible explanation.

Check if SSL Certificates Revoked (slow)

For the store only, certificate revocation can be checked, beware this requires internet access and can take several seconds, or longer, since not all certificate authorities support online checking.

Revocation is done when a certificate has been stolen or misused, and is no longer trusted.

Log Full SSL Certificate Chain

Ticking this option causes all SSL certificates in the verification chain to be logged, each time a connection is opened.

SSL Server Certificate

Allows a default SSL Server Certificate file to be specified, see SSL/TLS and Certificates. The certificate file may be PEM, DER, PFX/P12, P7 format, optionally a bundle including a private key and one or more intermediate certificates necessary. Only PEM, PFX/P12 can include private key and intermediates. If the private key is password protected (PFX.P12 usually are), 'password' is hard coded and can not be changed. Note each TCP/IP Server channel may have different certificates specified. The certificate, private key and intermediate chain will be checked during entry and before the channel starts capture against the Certificate Authority Bundle file specified above, to ensure any clients connecting do so without SSL errors.

SSL Server Private Key

If the SSL Server Certificate was not a bundle including a private key, allows a default SSL Server Private Key X509 PEM file to be specified, see SSL/TLS and Certificates. Note each TCP/IP Server channel may have different certificates specified.

SSL Certificate Intermediates

If the SSL Server Certificate was not a bundle including intermediates, allows a default SSL Certificate Intermediate X509 PEM file to be specified, see SSL/TLS and Certificates.

SSL Server Security Level

Specifies the SSL security level for all TCP/IP Servers to ensure that minimum SSL/TLS security standards are enforced. The options are:

None	All protocols and ciphers, any key lengths
SSLv3 Only	SSL3 only, all ciphers, any key lengths, MD5 hash
Backward Ciphers, TLS1 or Later	TLSv1 or later, backward ciphers, RSA/DH private keys => 1,024 bits, ECC keys => 160 bits, no MD5, no SHA1 hash
Intermediate Ciphers, TLS1.1 or Later	TLSv1.1 or later, intermediate ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash
Intermediate Ciphers FS, TLS1.1 or Later	TLSv1.1 or later, intermediate ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash, Forward Security forced
High 112 bit Ciphers, TLS1.2 or Later	TLSv1.2 or later, high ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash
High 128 bit Ciphers, TLS1.2 or Later	TLSv1.2 or later, high ciphers, RSA private keys => 3,072 bits, ECC keys => 256 bits, Forward Security forced
High 192 bit Ciphers, TLS1.2 or Later	TLSv1.2 or later, high ciphers, RSA private keys => 7,680 bits, ECC keys => 384 bits, Forward Security forced
TLSv1.2 or Earlier	TLSv1.2 or earlier, intermediate ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash, Forward Security forced
TLSv1.3 Only	TLSv1.3 only, intermediate ciphers, RSA private keys => 2,048 bits, ECC keys => 224 bits, no RC4 ciphers, no SHA1 hash, Forward Security forced

While using the highest level of security is always best, this may prevent older clients connecting to ComCap. If clients attempt to connect with the latest TLSv1.3 protocol but fail, try setting security to 'TLSv1.2 or Earlier', the latest is not always the best. Note that the server SSL certificate must have a key length of the minimum the security level requires, or capture will not start.

Create SSL Certificate

Clicking this button brings up a new window allowing either a certificate request for a certificate authority to be created, or a self signed certificate see SSL/TLS and Certificates.

GPS Location Sensor Channel

Some Windows tablets and high end laptops have a GPS location sensor built-in that supports the Windows Location Service allowing sharing location information between Windows applications.

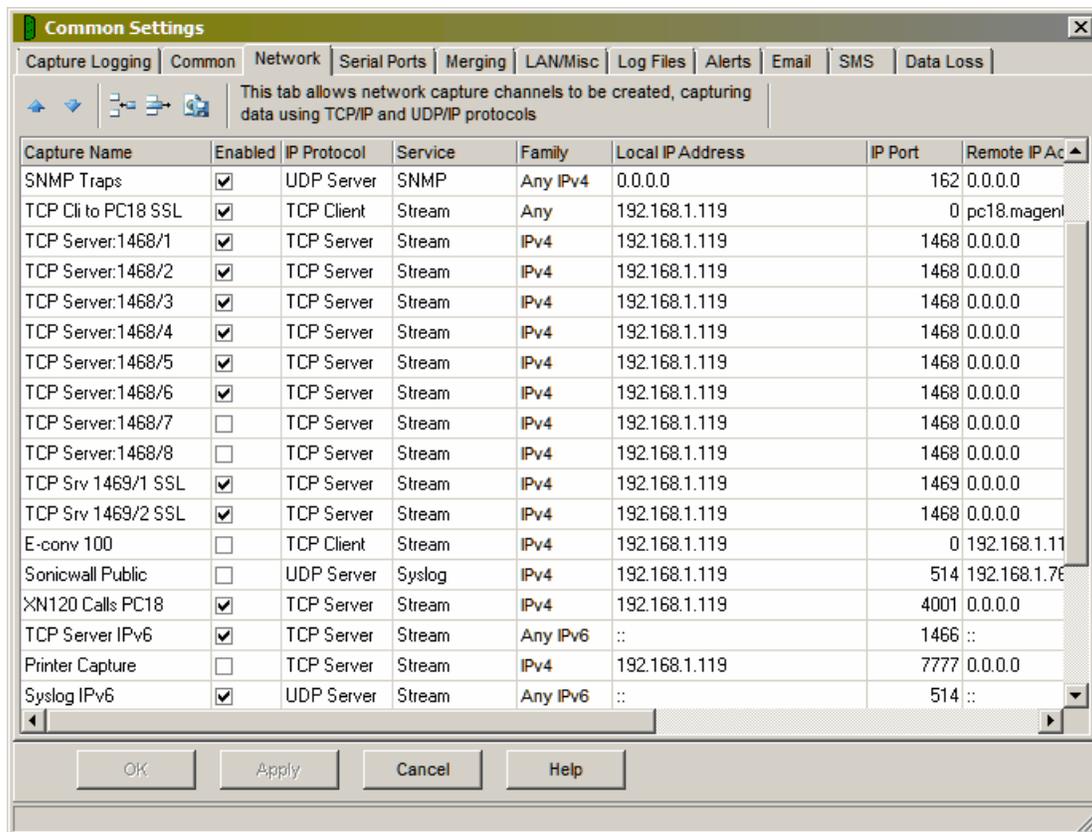
Ticking the 'Enable Location Sensor' box and entering a Capture Name causes a new channel to be created that will enable the Windows Location Service and capture GPS information it. More configuration is needed on the Channel Settings GPS Tab. When capture is started, Windows may pop-up a small window warning the Windows Location Service has been accessed, which is intended as a warning when applications access it without the user's knowledge.

Note these settings may not be available if the service is not installed, and may give an error when started if there is no GPS sensor. Also, PCs without a location sensor may still return a fixed location, which ComCap will capture, but with little purpose since it never changes.

Note that little diagnostic information may be available, the Asus VivoTab Note 8 tablet used for testing does not provide any satellite information.

2.3 Network

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines up to 999 network capture channels that are specified using a grid.



Merge Channels

When capturing data from multiple sources, one capture channel is needed for each separate source. For instance, if GPS data is being captured from 10 vehicles, at least 10 TCP/IP Server channels must be created.

To ease administration and set-up, one or more Merge Channels may be set-up combining or consolidating captured data from multiple channels, allowing all data to be displayed in a single window, written to a single log file, and added to a database using a single connection instead of one for each channel. One record at a time is merged, which may be one or more lines depending on the capture channel 'Line or Record End' setting (there is no record setting for merge channels). Merge Capture Name are a subset of the network or serial Capture Name, so in the screen capture above the channels named 'TCP Server 1468/1', 'TCP Server 1468/2', etc, are merged to a new channel named 'TCP Server 1468'.

Grid Control Buttons

There are five buttons used to manipulate the Network grid:

Move Row Up	Used to move the selected row higher up the grid.
Move Row Down	Used to move the selected row lower down the grid.
Add New Row	Causes a new blank row to be added at the bottom of the grid.
Delete Row	Causes the selected row to be permanently deleted.
Copy Row	Causes the selected row to be copied to a new row at the bottom of the grid.

For a refresh install, a new blank row is automatically created. Note that the Network grid scrolls horizontally to show more columns. To add or edit the grid, click on the required box and an edit control of some sort will appear, perhaps a drop down box arrow, an edit field or numeric up/down arrows. Once the edit is complete, click on another box to ensure the edit is saved, losing focus from the grid causes the last edit to be cancelled.

Capture Name

The Capture Name uniquely identifies this capture channel, and is displayed on the main window tabs and in the information logs. It may optionally be added to each captured line and may be used as part of the file name for capture logs. Generally, the name should be as short as possible, while meaningfully describing the purpose of the channel. Note Capture Names must be unique for Serial Ports as well.

Enabled

The Enabled tick box determines whether this channel will be captured. If unticked, the channel will not appear in the main window. It's typically used to temporarily disable a channel without deleting it.

IP Protocol

The IP Protocol is selected from a drop down box with the following options:

None	No protocol is specified, the same as not enabling the channel
------	--

UDP Server	Listens for incoming UDP datagrams (or packets) on the specified local IP address and port. Two or more remote computers may send UDP datagrams to the same UDP Server. Note there no handshaking or error correction with UDP, packets may be lost or become corrupted without ComCap being aware.
TCP Server	Listens for incoming TCP Clients on the specified local IP address and port and negotiates a connection. A single TCP Server can only accept one connection at a time. If the connection is broken, the TCP Server may take several minutes before accepting a new TCP Client. Two or more TCP Server channels (with different Capture Names) may be set-up on the same local IP address and port (use the Copy Row button) and ComCap will assign remote TCP Clients to these channels sequentially, in the order in which they appear in the grid, optionally filtering on Remote IP address, and finally refuse the connection if there are no free TCP Servers.
TCP Client	<p>Originates a TCP connection to a specified remote TCP Server IP address and port. Optionally, the connection may be from a specified local IP address and port, but normally it will be a random port which is safer because ports remain in use for a few minutes when closed preventing re-use. TCP Client is always a single connection to one remote computer. If the initial connection fails or it drops unexpectedly, it will attempt to connect again according to the Retry Attempts specified below.</p> <p>Windows TCP itself performs several attempts to make a connection, usually failing after about 40 seconds if the TCP Server does not respond. To reduce this period between attempts, ComCap by default first pings the remote computer with a timeout of only 10 seconds, before making the TCP connection attempt if the computer responds. The connection may still fail if there is no TCP Server listening, but this normally provided more rapid retry attempts. In rare cases, ping may be blocked by firewalls or routers, and may be disable in on the LAN/Misc Tab.</p>
Email Server	Listens for incoming email on the specified local IP address and port, usually 25 or 587, and negotiates a connection. A single Email Server can only multiple connections and will capture the emails in the order completely received. Needs more settings on the Capture Settings, Email tab. Internet appliances that will send email to ComCap should have their SMPT Mail Server changed to this local IP address, or set-up DNS for this address.

More information on protocols may be found in the Networking Tutorial.

Note that SSL/TLS is not specified on this tab, it is set on the Capture Settings Network tab.

If high speed data is being captured, the TCP/UDP buffer size may be increased, see Network Performance on the Capture Settings Network tab.

Service

The Service is selected from a drop down box with the following options:

Stream	Captured data is considered a continuous stream, not containing any specific service protocol. It may use any ports.
Syslog	System logging is a service protocol typically used by networking appliances such as routers and firewalls, but also printers and software applications to remotely log data. Syslog is characterised by lines starting with a number in angle brackets, ie <99> sometimes followed by the data and computer name, the number is decoded by ComCap into facility and severity types that may be used to ignore routine data. Syslog normally uses UDP Server listening on port 514, but for improved reliability sometimes uses TCP Server on port 1468.
Reliable Syslog	Reliable System Logging is an improved version of Syslog. It is not currently supported by ComCap and we've not seen any internet appliances using it yet, but it will be supported when a means of testing it is found. .
SNMP	System Network Management Protocol Trap is a binary protocol used by internet appliances, mostly to signal errors and problems. It uses UDP Server on port 162. ComCap does not currently decode the binary packets, but this will be added in a forthcoming release.
Avaya RSP	Avaya RSP is a protocol used for telephone logging by Avaya telephone switches which is not supported by ComCap, but will when a means of testing it is found.

Family

Specifies the IP address family, IPv6 will only be available if enabled on the Common tab.

Any	Allows either an IPv4 or IPv6 address to be entered, or an host name. Local address must be selected from a list of any configured addresses on the PC (if more than one).
IPv4	Requires IPv4 address only. Local address must be selected from a list of configured IPv4 address on the PC (if more than one).
IPv6	Requires IPv6 address only. Local address must be selected from a list of configured IPv6 address on the PC (if more than one).
Any IPv4	Will set the address to 0.0.0.0
Any IPv6	Will set the address to ::.

Local IP Address

The Local IP Address is selected from a drop down box that will be filled with all the IP addresses allocated to the computer (at least one, often more on servers) and also 0.0.0.0 and :: which means all IP addresses, depending on the Family specified above. Local IP Address should generally be left as 0.0.0.0 or :: for TCP and UDP Server, for TCP Client it only need to set specifically if the remote TCP Server is expecting connections from a specific IP.

Local IP Port

The Local IP Port must always be specified as non-zero for TCP and UDP Server, as a number between 1 and 65,536. Typically it will be 514 for Syslog, 162 for SNMP. Only one server can listen

on the same port on the same PC, if a port is chosen that's already being used by another application, the TCP or UDP server will fail to open. For TCP Client, the port is generally left as zero so Windows chooses a random port, but may need to set specifically if the remote TCP Server is expected connections from a specific port. If defining your own Local IP Port, use a high number between 10,000 and 65,000 to avoid conflicts with other applications.

Remote IP Address

For TCP and UDP Server, the Remote IP Address is generally left as 0.0.0.0 or ::, meaning any, so connections are accepted from any remote computer. If multiple server channels are set-up listening on the same local IP address and port, the Remote IP Address may be used as a filter, so specific channels will only accept connections from specific remote IP addresses. If the multiple server channels are set-up, the first channel must have a 0.0.0.0 Remote IP Address so it can accept connections from anywhere.

For TCP Client, the Remote IP Address must be set to that of the remote computer to which a connection should be opened.

Remote IP Port

For TCP and UDP Server, the Remote IP Port is generally left as 0. If a Remote IP Address is specified to filter remote connections to this channel, the Remote IP Port may be specified as non-zero as well to further reduce the filtering to connections from that port.

For TCP Client, the Remote IP Port must be set to that of the TCP Server on the remote computer to which a connection should be opened.

Filter Information

Filter Information is currently used.

Retry Attempts

For TCP Client only, Retry Attempts specifies the number of connection attempts that should be made to the remote computer before failing. Zero attempts means never stop, but keep retrying for ever, other the maximum attempts is 99.

Wait Seconds

For TCP Client only, Wait Seconds specifies the gap between a failed connection and the next retry attempt, with a minimum of 10 seconds and maximum of 300 seconds (five minutes). Note a connection attempt takes a minimum of 10 seconds, but about 40 seconds if ping is disabled. The more frequent the connection attempts, the more potential network traffic that is carried, but the lesser probability of lost data.

Channel Id

The Channel Id is fixed data and can not be edited. Ids are allocated sequentially as new network channels are defined, but remain fixed if channels are re-ordered or renamed in the grid. The Channel Id is used to identify settings in the configuration files `comcap.config` and `comcap.current`, ie [NET1], [NET2], etc.

Errors

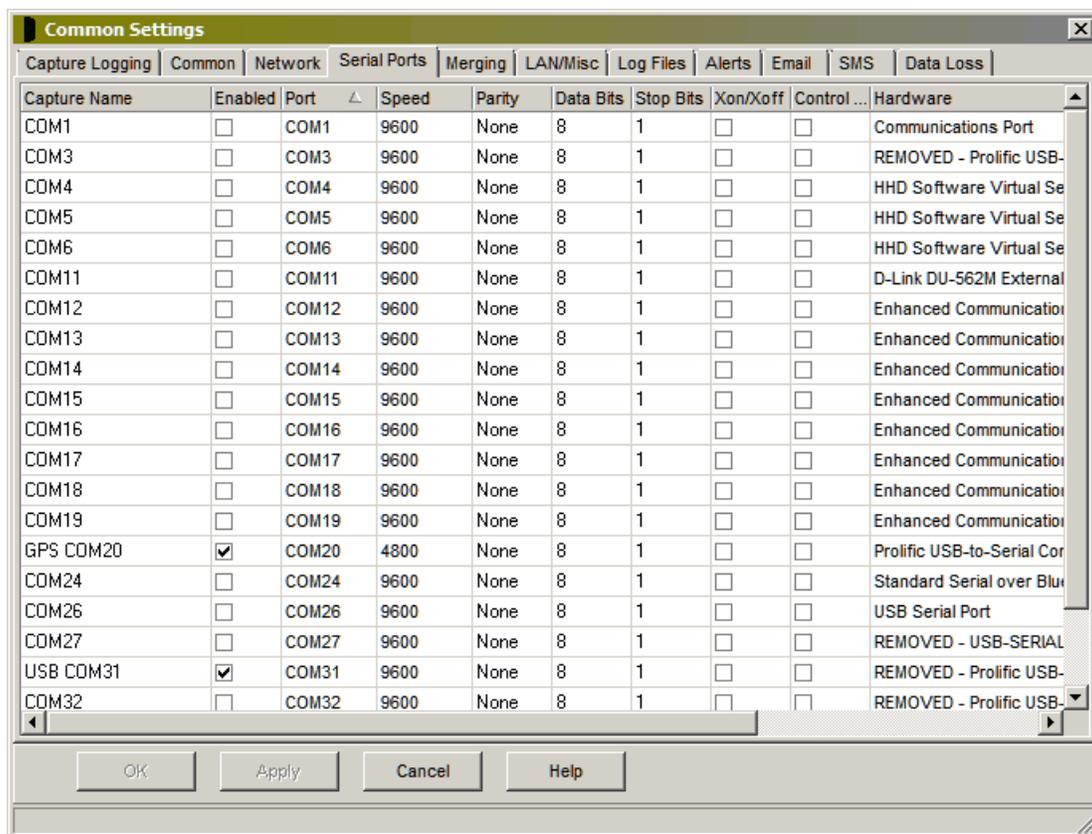
When the OK and Apply buttons are clicked, the Network channels are checked and validated, and may result in the following errors:

Config Error: Too Many Channels	A maximum of three network and serial channels is allowed in ComCap Standard Edition, and 999 in the Unlimited Edition. Disable one or more channels.
---------------------------------	---

Config Error: Local Port Must Not Be Zero	For TCP and UDP Server, the local port may not be zero.
Config Error: Listen must have blank Remote IP and Filter	For multiple TCP and UDP Server channels on the same local IP and port, the first channel must have a 0.0.0.0 remote IP address.
Config Error: Remote IP Address and Port Must Be Specified	For TCP Client, the remote IP address and port must be specified.
Must Specify Network IP Protocol	If the channel is enabled, the IP Protocol can not be none.
Must Specify Network Capture Name	The Capture Name can not be left blank.
Duplicate Capture Name – xxx	The Capture Name must be unique between Network and Serial Port channels.
Network Local IP Port Must Not Be Zero for Server	For TCP and UDP Server, the local port may not be zero.
Network Remote IP Port Must Not Be Zero for Client	For TCP Client, the remote IP port may not be zero.
Network Remote IP Address Must Be Specified	For TCP Client, the remote IP address may not be blank.

2.4 Serial Ports

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines up to 999 Serial Port capture channels (hardware permitting) that are specified using a grid.



Serial Ports Overview

This grid allows different settings to be specified for each different serial RS232 communications port, see Serial Port Tutorial for more information. It's important to understand the grid shows all ports installed on the PC including those currently removed and unusable, which are typically USB serial ports that are unplugged. So capture can be set-up and started for ports that are currently removed, and will start immediately the USB device is plugged into and becomes available to Windows. Likewise capture will be paused if a serial port disappears, and restart if it re-appears. The word REMOVED appears in the Hardware column for ports currently not-installed.

To edit the grid, click on the required box and an edit control of some sort will appear, perhaps a drop down box arrow, an edit field or numeric up/down arrows. Once the edit is complete, click on another box to ensure the edit is saved, losing focus from the grid causes the last edit to be cancelled.

Merge Channels

When capturing data from multiple sources, one capture channel is needed for each separate source. To ease administration and set-up, one or more Merge Channels may be set-up combining or consolidating captured data from multiple channels, allowing all data to be displayed in a single window, written to a single log file, and added to a database using a single connection instead of one for each channel. One record at a time is merged, which may be one or more lines depending on the capture channel 'Line or Record End' setting (there is no record setting for merge channels). Merge Capture Name are a subset of the network or serial Capture Name, so in the screen capture above the channels named 'COM1', 'COM2', etc, are merged to a new channel named 'COM'.

Capture Name

The Capture Name uniquely identifies this capture channel, and is displayed on the main window tabs and in the information logs. It may optionally be added to each captured line and may be used as part of the file name for capture logs. Generally, the name should be as short as possible, while meaningfully describing the purpose of the channel. The Capture Name defaults to the serial port

name. Note Capture Names must be unique for Network channels as well.

Enabled

The Enabled tick box determines whether this channel will be captured. If unticked, the channel will not appear in the main window. It's typically used to temporarily disable a channel without deleting it.

Port

Displays the port name, from COM1 to COM200, may not be changed. The COM port is used to identify settings in the configuration files `comcap.config` and `comcap.current`, ie [COM1], [COM2], etc.

Speed

Speed is a drop down list of possible communication speeds for the RS232 data source, ranging from 300 to 256,000 bits per second. Older PCs may only reliably support speeds up to 9,600 bits/sec. Actual communication speed is bits per second divided by the bits per character which is typically 10 (1 start bit, 8 data bits, 1 stop bit), so 9,600 bits/sec equals 960 characters per second (about 12 lines). If random data is being captured, try adjusting the Speed higher or lower. If there are problems capturing data, sometimes slowing the speed will help, but must be done at the data source as well.

Parity

Parity is a drop down list of possible parity types used by the RS232 data source being captured. For 8-bit data, parity is usually set to None. For 7-bit data, there are odd, even, mark and space options (which then total 8 bits). Rarely, parity is used with 8-bit data. If the parity is incorrect, some characters may appear incorrectly, typically as foreign characters.

Data Bits

Data Bits is a drop down list of data bits in the RS232 data source, ranging from 5 to 8 bits per second. 5 and 6 bits are used by telegraph and telex type sources (only upper case letters), 7-bit is ASCII upper and lower, 8-bit also includes foreign characters and special symbols. 7-bit usually has odd or even parity selected as well, 8-bit is normally no parity.

Stop Bits

Stop Bits is a drop down list of the number of stop bits in the RS232 data source, normally 1 bit, but perhaps 2 bits for very slow data.

Xon/Off Flow Control

ComCap normally uses hardware flow control, by setting the RTS and DTR lines high when capture is started and then dropping RTS if no more data can be buffered. Selecting Xon/Xoff flow control causes xon and xoff symbols to be transmitted when data can be accepted or needs to be stopped. The size of the download data buffer for each COM port is about 62,000 bytes which is about one minute of data at 9,600 bits/sec, after which flow control should stop new data being received in the rare case that ComCap can not process incoming data in real time.

Control Lines

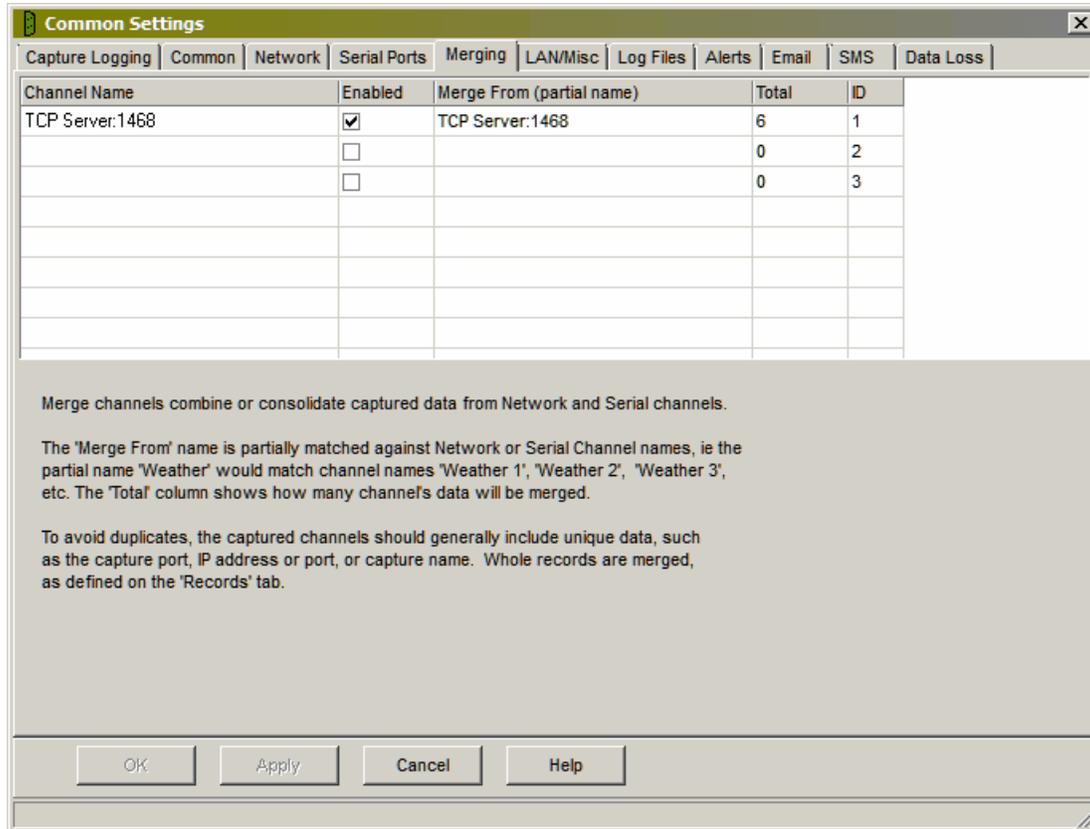
This option determines whether the three serial control lines CTS, DTS and DCD should be checked during capture, to make detection of connection or hardware problems easier since an alert can be sent if capture stops. If ticked, capture will only start when at least one of the three control lines goes high, and will stop if they all drop. Note this is really cosmetic only (with the tab colour changing red to green) and start/stop logging, and data will be still be captured even if all the control line are low. But unless the channel is seen to 'start', some functionality may not work correctly such as capture file name roll over.

Hardware

Description of the serial COM port hardware. May be preceded by REMOVED if the port is not currently available in Windows, perhaps because a USB serial port is unplugged. It is still possible to enable a removed port for capture, but capture will not start until the port is re-installed by Windows.

2.5 Merging

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines merge capture channels that are specified using a grid.



Merging Overview

Merge Channels combine or consolidating captured data from multiple Network and Serial channels. It is effectively an alternate form of capture data Echo. This benefit applications capturing data from multiple sources, allowing all data to be displayed in a single window, written to a single log file, and added to a database using a single connection instead of one for each channel. One record at a time is merged, which may be one or more lines depending on the capture channel 'Line or Record End' setting (there is no record setting for merge channels).

Most channel settings apply equally to capture and merge channels, but generally should not be duplicated. Some effort may be needed to avoid duplicate data being merged from different channels. With 'Add Custom Text to Captured Lines', the network or serial channel setting should be used to add a channel name, remote IP address, or device id, while the merge channel could add date and time and serial number so they are unique for the channel.

Note that currently if a merge channel is paused, the capture channels continue but data is not merged.

Capture Name

The Capture Name uniquely identifies this capture channel, and is displayed on the main window tabs and in the information logs. It may optionally be added to each captured line and may be used as part of the file name for capture logs. Generally, the name should be as short as possible, while meaningfully describing the purpose of the channel. Note Capture Names must be unique for Network and Serial channels.

Enabled

The Enabled tick box determines whether this channel will be captured. If unticked, the channel will not appear in the main window. It's typically used to temporarily disable a channel without deleting it.

Merge From (partial name)

Specifies the partial name of the network or serial channels whose captured data should be merged to this channel. The Merge From name that is partially matched against Network or Serial Channel names, ie the partial name 'Weather' would match channel names 'Weather 1', 'Weather 2', 'Weather 3', etc, and in the screen capture above the channel 'TCP Server 1468' will be merged from those network channels named 'TCP Server 1468/1', 'TCP Server 1468/2', etc.

Total

This' column shows how many channel's data will be merged, based on the Merge From partial name matching.

2.6 LAN/Misc

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines Local Area Network Logon and Drive Mapping, Windows Freeze Recovery, Network Options and displays ComCap license key details.

Local Area Network Logon and Drive Mapping

These options are primarily used when the ComCap Background Service needs to save files on shared network drives. Shared drives mapped for the current user are not available for the service,

and login credential may not be available for UNC shares.

Local Drive to Map may be set to UNC Path or a specific drive letter that should have a network share mapped to a Remote PC Name and Share, with a specific User Id and Password. If a specific drive is mapped, it is done as soon as ComCap starts, and unmapped when it closes. It must not duplicate an existing mapped drive letter or share. If UNC Path is specified, then log file name must be full UNC paths without drive letters, ie `\\pc\share\file.txt`.

The Test Mapping button will test the mapping details, it should connect and then disconnect to the shared drive, with any errors appearing in the Information Log.

Windows Freezing

ComCap provides an automatic workaround for a serious potential problem if Windows temporarily freezes due to the misbehaviour of other applications or hardware. Freezing is normally seen by the mouse being non-responsive and the system tray clock stopping. If a Windows application hogs all the CPU, it may stop Windows and ComCap correctly capturing data.

If ComCap seemingly freezes for more five seconds, a warning message is logged an Alert optionally generated. It is recommended the cause of such freezing is determined and the other application stopped. The Application Priority on the Capture Logging tab may be set to High or Real Time to reduce the likelihood of other applications blocking ComCap. If a freeze exceeds a specified number of seconds, capture may be optionally restarted, but data may still have been lost during the freeze.

Sometimes the freezing can be much longer, in particular if there are disk drive problems or if an EIDE tape drive is being used. A Hewlett-Packard 20 GB Trevan drive used under Windows XP SP1 causes a test PC to freeze for over two minutes while the tape is being positioned at the start and end of backup, and this is devastating for data capture. The long freeze not only causes data to be lost, but confuses various internal timers so no more data is captured.

Application Priority

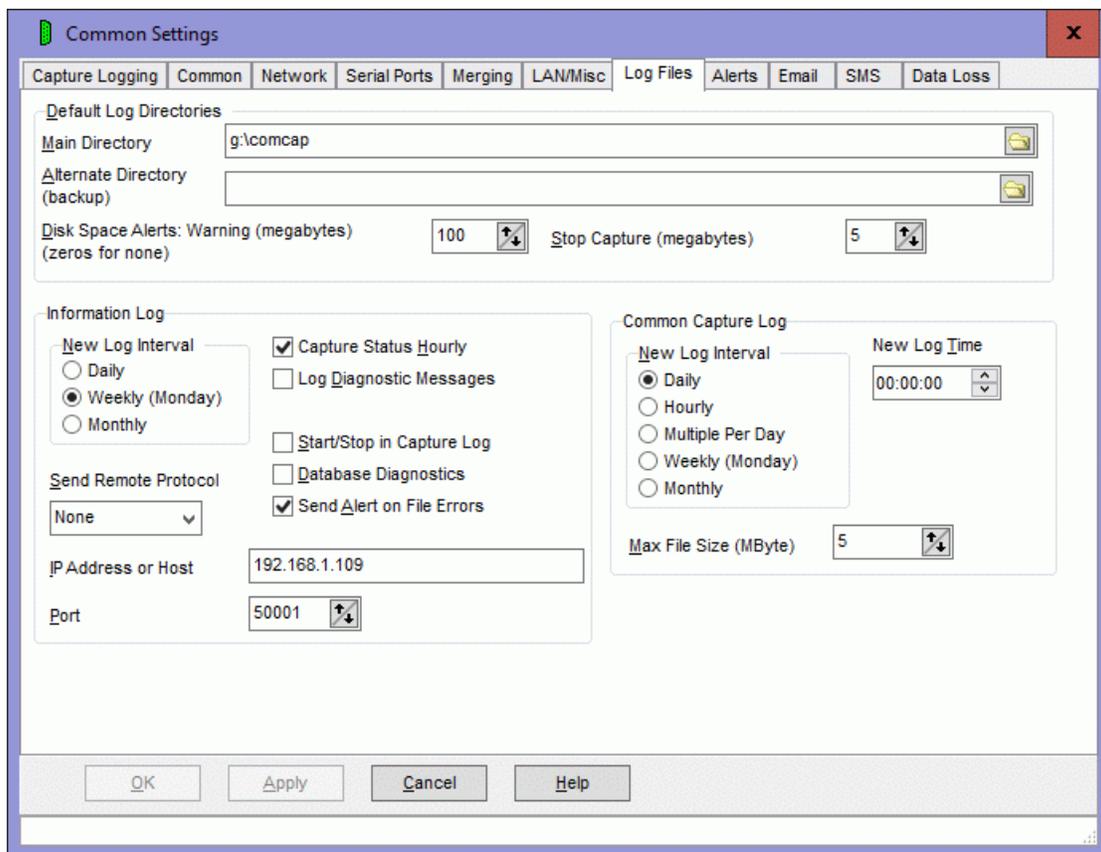
This option specifies the priority at which the ComCap application will run, in comparison with other Windows applications. Windows is multi-tasking with often dozens of applications are running at the same time (including many background services). Each application gets a few milliseconds CPU time, each second, to allow it to keep running. If one application starts using excessive CPU, others slow down and sometimes appear to hang with the worst case being when the mouse becomes frozen. Windows has four main priority levels, Low, Normal, High and Real Time, which most applications run with Normal priority. The Application Priority menu defaults ComCap to High priority, making loss of data due to other application using too much CPU less likely. ComCap can be set to run as Real Time which means it has higher priority than most Windows functions such as mouse movement, flushing files, etc, but may mean the PC locks up completely if ComCap were to severely misbehave (which is, we hope, unlikely).

License Key

Several fields display the ComCap license key details, if found, and may show an expiry date for a limited duration demonstration key.

2.7 Log Files

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines the Default Log Directories, Information Log settings and Common Capture Log settings.



Default Log Directories

Allows Main and Alternate Log Directories to be specified, in which Information Log files and Common Log files will be created. The default directories may be overridden for Capture Logs for each channel. The Alternate Log Directory may be left blank if backup logs on a second disk drive or network share are not required. Clicking the icon at the end of directory edit box displays a Browse for Folder dialog allowing a drive and directory to be selected. It is not possible to save Common Settings unless a test file can be created and written to the Main Log Directory, and to the Alternate if specified. If network shares are used, a LAN Logon may need to be set-up on the LAN/Misc tab.

Note that ComCap will exceptionally save Capture Logs and Information Logs in the program directory, if the default directories are unavailable or are not specified during start-up.

Disk Space Alerts

These options allow for disk space checking, so ComCap does not use all available disk space and then just die. Warning free megabytes may be specified, below which an Alert will be triggered. If space continues to reduce, ComCap capture can stop when a lower free megabytes is reached, to prevent the drive filling completely. If this functionality is not required, set the megabytes to zero. Note one gigabyte is 1,000 megabytes. These settings relate to the drives on which the Main and Alternate Log Directories are located. If different drives are used for specific capture channels, these will not be monitored.

Information Log Interval

The Information Log file contains information about capture configuration, when capture starts and stops, the capture log file names and capture status. It is generally a low volume file, unless a lot of errors occur.

The New Log Interval may be set to Daily, Weekly (Monday) or Monthly.

The log name formats are `info-yyyy-mm.txt`, ie `info-2006-09.txt` for September 2006 or are `info-yyyy-mm-dd.txt`, ie `info-2006-09.29.txt` for daily or weekly. Note that if there are problem opening old Information Log files, a time may be added to file name, but logging will revert to the normal log at midnight.

Capture Status Hourly

This tick box causes ComCap to log the Capture Status at the top of each hour, including the names of all the log files.

Log Diagnostic Messages

This tick box specifies that extra diagnostic messages should be written to the information log file, generally more information about file opening and closing (which happens all the time). These messages may increase the size of the logs somewhat, and are not needed unless there are capture file problems.

Start/Stop in Capture Log

This tick box specifies that the date and time capture starts and stops should be added to the Capture Log, which can be very useful to diagnose capture problems. However this extra information may cause problems if the Capture Log is further processed by other applications.

Database Diagnostics

This tick box specifies that extra database diagnostic messages should be written to the information log file, generally not needed unless there are database problems.

Send Alert on File Errors

This tick box specifies that an alert should be triggered for any file errors, such access conflicts or hardware problems.

Send Remote

These options allow the Information Log to be sent to a remote computer using network protocols, quite likely to be captured by another copy of ComCap for remote monitoring. The Send Remote Protocol may be None, UDP, TCP Client or TCP Server, with the remote IP Address and Port also needing to be specified. This option is strongly recommended, if possible, since it means any disk problems can be logged on a different PC where local logging may fail.

Common Capture Log

The Common Capture Log allows two or more capture channels to save data into the same file. This is set-up in Capture Settings, Files. The Common Capture Log has a fixed name format, always `common-yyyymmdd-hhnnss.txt`.

New Log Interval

The New Log Interval specifies how often a new Common Capture Log file should be opened.

Daily	A new capture log is opened once a day, at the New Log Time, see below.
Hourly	A new capture log is opened each hour, on the hour.
Multiple Per Day	Multiple new capture logs are opened each day, according to Logs Per Day, starting at the New Log Time, see below.
Weekly (Monday)	A new capture log is opened once a week, at midnight on Sunday.
Monthly	A new capture log is opened once a month, at midnight on the first day of the month.

New Log Time

For 'New Log: Daily', specifies at what time of day the new log is created, defaulting to 00:00:00 for midnight.

Logs Per Day

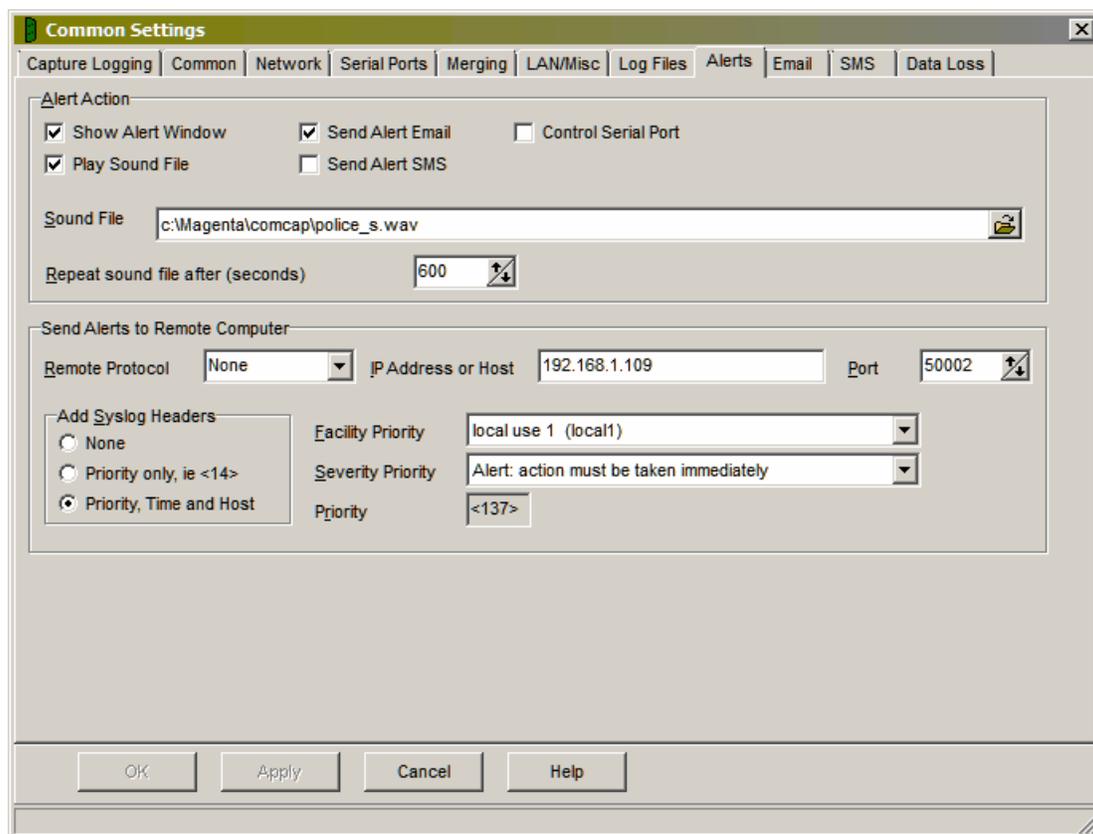
For 'Multiple Per Day', specifies how many new log file should be opened each day, starting at the New Log Time. Four logs per day with a new time of 00:00 would create new logs every six hours at 00:00, 06:00, 12:00 and 18:00; three logs starting at 06:00 would create new logs every eight hours at 06:00, 14:00 and 22:00; seven logs per day from 00:00 would create new logs every 206 minutes, at 03:26, 06:52, 10:18, etc. The minimum Logs Per Day is two, maximum is 12, for lower or higher use the Hourly or Daily settings.

Max File Size (MBytes)

This option allows the maximum common capture file size to be limited, with a new file being created once a specified size is reached, in megabytes. The default is 2,000 (which is 2 gigabytes). Some care is needed with log name format, specifically if it does not contain sufficient granularity to create a unique file name, so if more than than one file per day is needed, the name mask must include at least hours. If a new file name can not created, a default name with date and time in seconds will be created.

2.8 Alerts

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines Alert Actions.



Alert Overview

Alerts are actions triggered by ComCap in response to events to which the user's attention needs to be drawn, usually for error conditions. The various alerts are configured on different Common Settings and Capture Settings tabs:

ComCap Stop	Common Settings, Capture Logging
Disk Space Running Low Disk Space Below Minimum Required WARNING - Disk No Longer Available File Errors	Common Settings, Log Files
PC Temporary Freeze Detected	Common Settings, LAN/Misc
No Data Received	Common Settings, Data Loss
Database Error, Failed to Start Capture, Database Not Opened Database Error, Capture Being Paused until Database is Available	Capture Settings, Database
Alert for Lines with Phrases	Capture Settings, Filters and Alerts

Show Alert Window

Ticking this option causes the Alert Window to be shown, listing recent alerts. The Tray version of ComCap must be running for the Alert Window to be shown, but capture may be by the Background Service. Alerts remain displayed until cleared manually, or until ComCap exits. They are always put in the Information Log.

Play Sound File

If Show Alert Window is enabled, ticking this option causes the specified Sound File to be played when the window is first opened, and repeated after a specified period in seconds until the Alert Window is closed, minimum 10 seconds, maximum 300 seconds (5 minutes).

Send Alert Email

Ticking this option causes Alerts to be sent by email, using Common Settings, Email/SMS.

Send Alert SMS

Ticking this option causes Alerts to be sent by SMS to a mobile telephone, using using Common Settings, Email/SMS.

Control Serial Port

Ticking this option causes Alerts to be sent by raising the RTS and DTR control lines on a specified RS232 serial port for one or more seconds. If the serial port is wired to a low current relay, this output may be used to sound a bell or alarm to draw attention to ComCap.

Send Alerts to Remote Computer

These options allow Alerts to be sent to a remote computer using network protocols, quite likely to be captured by another copy of ComCap for remote monitoring. The Send Remote Protocol may be None, UDP, TCP Client or TCP Server, with the remote IP Address and Port also needing to be specified. The IP address or Host entered may be IPv4 or IPv6, or a host name, and will be detected automatically.

Add Syslog Headers

Specifies that syslog headers should be added to Alerts send to a Remote Computer:

Priority Only	<14> is a Priority value where the first 7 bits of the number are a facility code and the last 3 bits are severity, selected from the drop down Facility Priority and Severity Priority lists. The Actual Priority text that will be added is show,
Priority, Time and Host	Also add the time and host and program name, similar in format to: <14>Mar 25 17:03:04 PC09 ComCap

Note that Syslog headers are normally only used with UDP.

Alert Control Serial Port

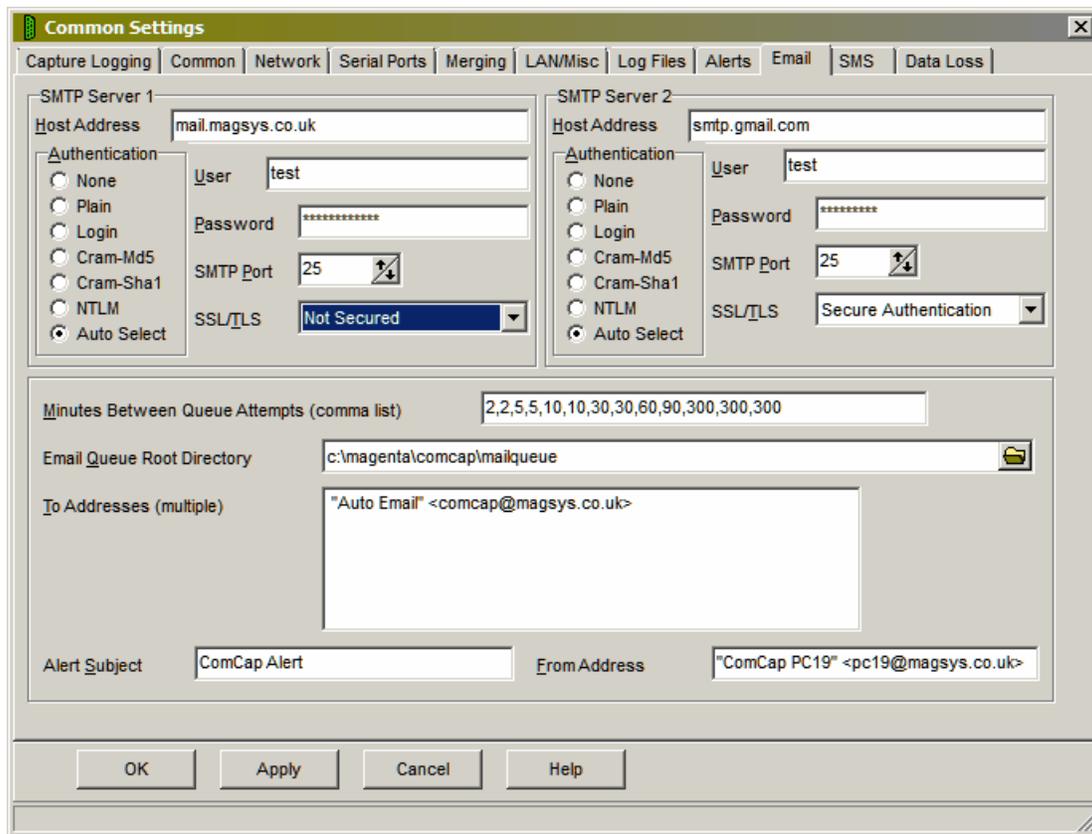
Specifies the serial RS232 communications port that will have the control lines RTS and DTR raised for the specified number of seconds. Note that only serial ports that are not already being used for capture, echo or printing may be selected.

Test Alert

Clicking this button causes an immediate test alert to be sent, according to the various settings above and on the Email/SMS tab.

2.9 Email

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines how alerts and logs are sent by email.



Email Overview

These settings define how Alerts and logs will be sent by email. Note email will require a network connection to either a local LAN with an email SMTP server, or to the internet. ComCap may send two or more alerts in each email. Sending emails is free of charge.

Email Queue

A mail queue is used by ComCap, so email alerts will not be lost if there are network problems or if ComCap stops for any reason. If there are problems sending email immediately, it will be retried potentially over 24 hours or more. Note the email queue is only running while ComCap is running, but if ComCap is stopped it will make one attempt to send any pending emails (such as logs emailed on close) within 30 seconds (but not for longer since Windows might be closing ComCap to reboot).

SMTP Servers, Host Address, Authentication, User/Password, and SMTP Port

One or two SMTP server details need to be specified, if the first is unavailable, the second will be attempted. For each SMTP server, the host names or IP addresses need to be specified, to which emails will be relayed. The Authentication should be Auto Select for the best choice available on the server with the User name and Password specified, or a particular authentication method may be chosen: Plain, Login, Cram-Md5, Cram-Sha1 or NTLM (the last three encrypt the password). If the SMTP Server is running on an SMTP Port other than the standard 25, this may be specified.

Secure Email, SSL/TLS

Secure email using SSL/TLS may be specified, which is required by services such as Gogglemail and Windows Live Hotmail. 'SSL/TLS Connection' should be used with SMTP Port 465 and forces an implicit TLS connection to this port. 'SSL/TLS Authentication' normally uses port 25, but will check if the server returns a STARTTLS response to indicate it supports SSL/TLS authentication at which point a secure connection is established instead. Note that the SMTP server SSL certificate is not currently checked. To support SSL/TLS, two files are included with ComCap, libeay32.dll and ssleay32.dll.

Minutes Between Queue Attempts

This option specified the period in minutes between attempts to send email from the queue, with one attempt for each of the two SMTP Servers, if both specified. For instance, 2,3,5,5,10 would cause retry attempts after 2, 5, 10, 15 and 25 minutes from when the email was queued, Note that some email servers support grey listing and reject the first email attempt from a new sender but allow a retry 10 or 15 minutes later, something that is very effective in blocking spam emails (since they don't usually retry).

Email Queue Root Directory

ComCap uses temporary files to hold queued email, the root directory for which needs to be specified here. A control sub-directory contains some small files listed queue details and retries, and the badmail sub-directory contains mail that could not be sent after all retries were exhausted. To stop emails being sent, simply delete any files with the EML extension.

Default Subject and From Address

The Default Subject is used for alert emails sent by ComCap, and might be `ComCap Alert`. Likewise, the From Address should be specified with a descriptive name in double quotes, followed by the actual email address in angle quotes, ie `"ComCap Alert" <comcap@magsys.co.uk>`.

To Addresses

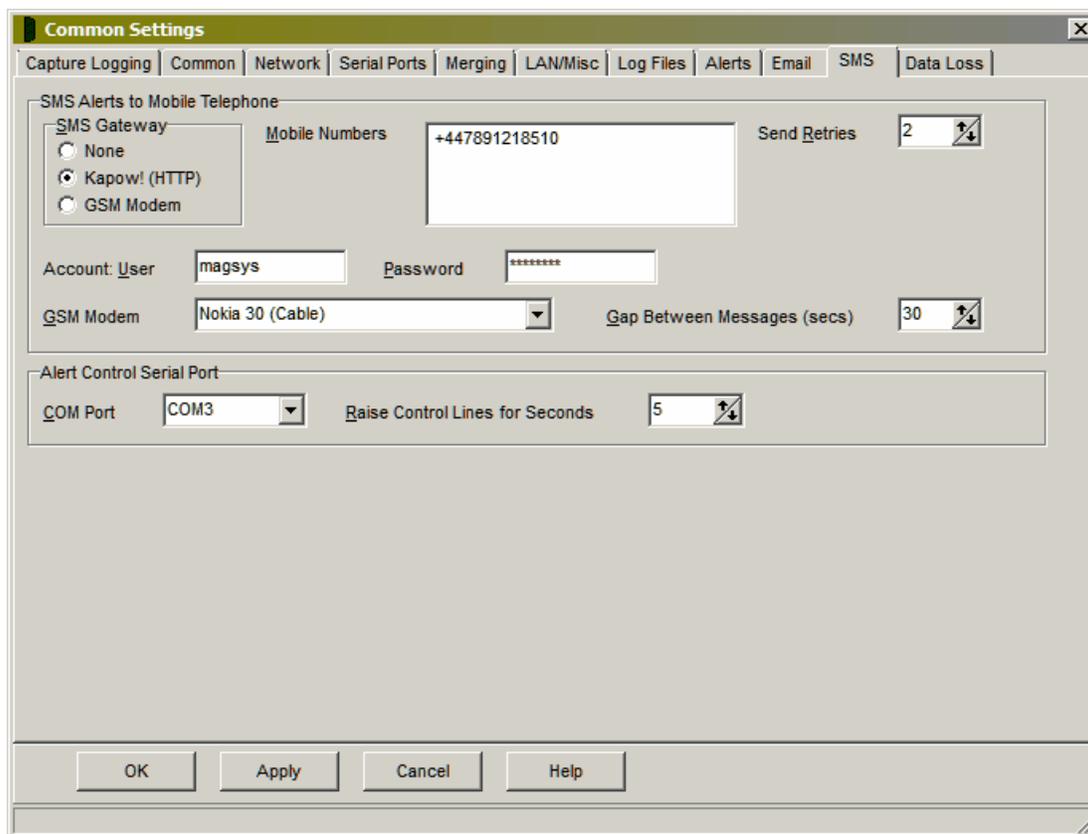
One or more addresses may be specified to which the alert will be sent, each address should be on a separate line, with a descriptive name in double quotes, followed by the actual email address in angle quotes, ie `"Angus Robertson" <angus@magsys.co.uk>`.

Authentication, User and Password

If the SMTP server needs authentication, this may be selected from Plain, Login or CRAM-MD5 and specified.

2.10 SMS

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines how alerts are sent by SMS to mobile telephones.



SMS Overview

SMS (Short Message Service), but commonly called 'texts', are short messages sent to mobile telephones (and more rarely special landline telephones), with a maximum payload length of 140 8-bit characters or 160 7-bit ASCII characters. Note SMS delivery is by its nature unreliable, the mobile telephone may not be switched on or be out of area, and SMS can get queued in the delivery centres for hours or days, if traffic is busy.

ComCap currently supports two different methods of sending SMS, known as the SMS Gateway, an internet gateway and a GSM modem cabled to a PC serial port. Currently only a single internet gateway is supported by ComCap, others will be added on request provided they offer at least the same level of service. We are unlikely to add 'free' SMS gateways since the economics of sending SMS mean the cost has to be covered by advertising or sponsorship web pages, which ComCap can not use.

SMS Gateway – Kapow! (HTTP)

The Kapow! SMS gateway at <http://www.kapow.co.uk/> is a bureau that allows SMS messages to be sent over the internet using various methods, including email. Our experience of the Kapow! service is excellent, with SMS normally being sent within 30 seconds. A permanent internet connection is required to use the Kapow! SMS gateway.

The Kapow! SMS gateway requires an account to be set-up and message credits to be purchased before any SMS can be sent. Cost starts at £8.50 for 100 messages, reducing for larger purchases. By default, messages will be sent with From-Id of `www.kapow.co.uk`, but a personalised address or telephone may be purchased for a one-off £50 if preferred.

ComCap uses an HTTP POST request to send SMS via Kapow!, and also provides message progress information by HTTP, so ComCap can report the SMS has actually been delivered to a mobile telephone. The Information Log below shows an SMS being sent by Kapow!, the account has 129

message credits left, and the message was confirmed as delivered in less than 20 seconds, sometimes it's only five seconds. SMS sent to mobile telephones outside the UK may take longer.

```
11:03:05 Starting to Send Alert SMS to +447891218xxx
11:03:05 Text Message Accepted by Kapow for +447891218xxx with reference 11599561857812153
11:03:05 Kapow Messages Credits Remaining: 129
11:03:05 Finished Sending SMS Alerts
11:03:11 Text Message Not Yet Sent by Kapow for +447891218xxx - Message Buffered Awaiting
Delivery
11:03:17 Text Message Not Yet Sent by Kapow for +447891218xxx - Message Buffered Awaiting
Delivery
11:03:23 Text Message Sent OK by Kapow for +447891218xxx
```

ComCap checks SMS progress every five seconds, but stops if the message has still not been delivered after 30 minutes.

SMS Gateway – GSM Modem

A GSM modem allows sending of SMS without needing internet access. ComCap has been tested with two dedicated GSM Modems, a Nokia 30 and Siemens MC35 (the TC35 is similar but for the USA), but should work with other GSM modems or mobile phones (with a serial COM port or USB lead) that support the ETSI 07.05 specification. Note however that our testing was problematic, with both available GSM modems being less reliable than one would expect. Also note that GSM Modems may get a poor signal if used in computer rooms with lots of shielding.

GSM Modems can also receive SMS, and before sending SMS ComCap will download any waiting SMS into the Alert window, so that the waiting indicator on the GSM modem stops flashing. But ComCap does not check for incoming SMS unless an alert is being sent.

Mobile Numbers

One or more mobile telephone numbers may be specified to which SMS will be sent, one per line, in full international format, always stating with + including the country code, ie +447891234567 and without any spaces. SMS are charged separately for each mobile number used.

Send Retries

The number of retry attempts to send SMS may be specified, there is a five second delay between each attempt.

Account User and Password

For the Kapow! SMS gateway only, these fields specify the account and password.

GSM Modem

A drop down box here displays any installed modems, including GSM modems. Don't attempt to send SMS with normal modems.

Gap Between Messages

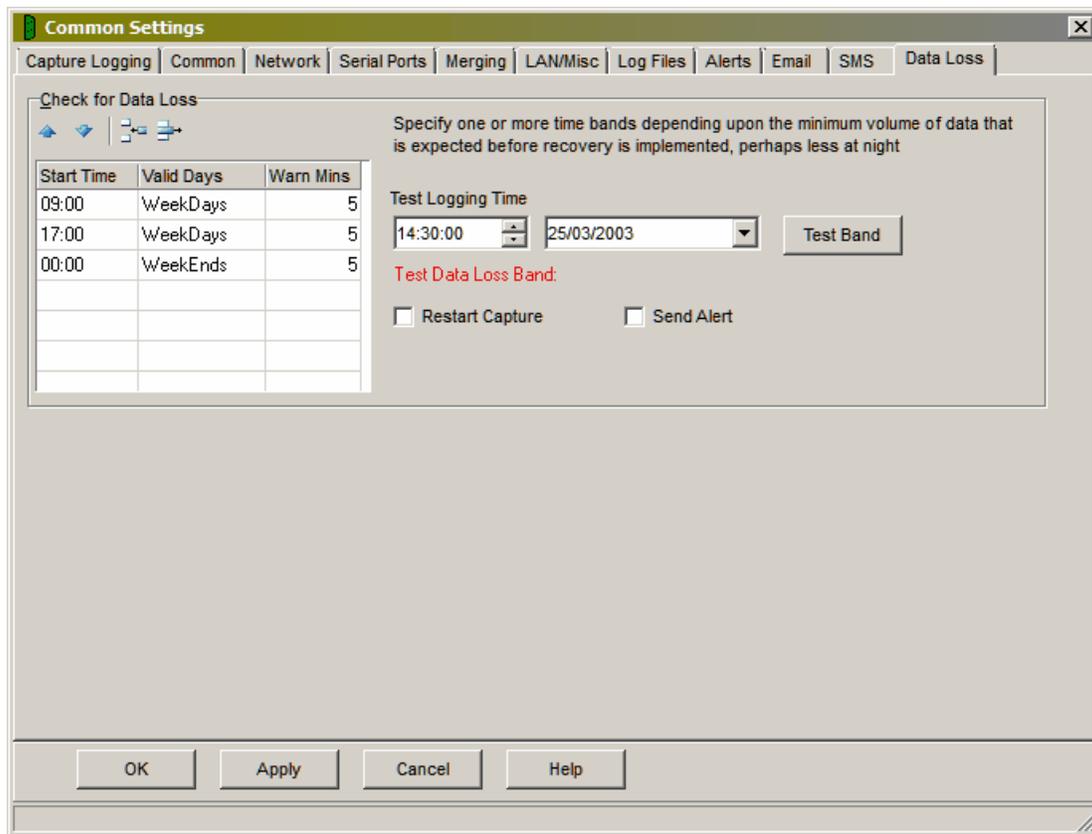
This option is not yet used. It's intended to restrict the frequency of SMS being sent, but during testing alerts are rare.

Test SMS

Clicking the Test SMS button causes an SMS to be sent immediately. If there are any problem, please email the appropriate lines from the Information Log to comcap@magsys.co.uk.

2.11 Data Loss

The Common Settings apply to all capture channels. Once these settings have been specified, OK or Apply should be clicked. This tab defines Alert Actions and Check for Data Loss.



Check for Data Loss Overview

ComCap provides a means to check that data is being continually captured, in case a problem stops capture. This is only useful where the data flow is reasonably steady, but different warning times may be set for different times of the day and week, for instance with business telephone call logging where there may be no data at night or at the weekends.

'Check for Data Loss' also needs to be ticked in Capture Settings, General for each separate channel before it is effective, and these common settings may be overridden by settings on Capture Settings, Sounds/Data Loss if different values are needed for different capture channels.

A multi-line grid allows several time periods to be specified, each with a different warning period, set in minutes (where zero is no warning).

Grid Control Buttons

There are four buttons used to manipulate the Data Loss grid:

Move Row Up	Used to move the selected row higher up the grid.
Move Row Down	Used to move the selected row lower down the grid.
Add New Row	Causes a new blank row to be added at the bottom of the grid.
Delete Row	Causes the selected row to be permanently deleted.

Data Loss Time Bands

It is common to need different warning settings at varying times of the day or week, perhaps depending on the volume of telephone calls. An unlimited number of time bands may be specified, one on each row of the grid.

Band Start Time

Specifies the start time for the band, where 00:00 is midnight. The start times should be arranged in increasing order by day. ComCap has default start times of 09:00 and 17:00 for weekdays, and 00:00 for weekends.

Valid Days

Specifies the day of the week on which this time band is valid, or weekdays, weekends or every day. Clicking or typing in the Valid Day column will cause a drop down arrow to appear, allowing a list to be dropped down with the days of the week, weekdays and weekend options. Please be careful not to allow multiple choices, such as Monday and Weekdays, this is not validated and the first found will be used. Any other day setting overrides every day, so you can not mix it with specific days.

Warn Minutes

Specifies the warning time in minutes after which the specified action will occur if no data is received by the channel. This period will be dependent entirely on the frequency of the type of data being received, and needs to be set sufficiently high to avoid unnecessary warnings, up to a maximum of 9,999 minutes (almost one week).

Default Periods

The default periods are 09:00 Weekdays with a warning after 5 minutes, 17:00 Weekdays 0 minutes (no checking) and 00:00 Weekends 0 minutes (no checking), which means that the data loss warning is only enabled 9am to 5pm Monday to Friday.

Test Button

A test button is provided that allows testing of periods for any specific date and time, to ensure there are no conflicts.

Restart Capture

Ticking this option will cause capture to be restarted in case Windows has failed in some way. Beware this may cause loss of data from other active channels since all are restarted together.

Send Alert

Ticking this option causes a data loss alert to be triggered.

Part



3 Capture Settings

3.1 General

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies General capture information.

Save to Database

If ticked, specifies that captured data should be written to a database. A Database tab will appear, also the Data Format on this tab needs to be specified.

Filters and Alerts

If ticked, specifies that captured data may be filtered by ignoring certain captured text, and trigger alerts from other captured text. A Filters and Alerts tab will appear allowing these settings to be specified.

Pause Capture if Echo Stops

Not yet supported, but Pause Capture if Echo Stops will do as it suggests.

No Log Display

If ticked, specifies that captured data should not be displayed in the main windows as it arrives. This reduces the overhead on the PC, and might be useful for very slow PCs.

Check for Data Loss

If ticked, data loss checking becomes effective for this channel, triggering actions and alerts if data is

not captured for a specified period. By default, the data loss settings are taken from Common Settings, Data Loss but they may be overridden by settings on the Sounds/Data Loss tab if different values are needed for different capture channels.

Alert on Unexpected Stop

If ticked, triggers an alert if the channel is stopped due to a network connection dropping.

GPS Data Processing

If ticked, specifies that captured data should be processed according to more settings on the GPS tab.

Echo Type

Echo Type specified if captured data should be echoed or proxied to another computer or printer, in one of the following ways:

Windows Printer	Captured data will be echoed to any installed Windows local or network printer. A new tab will appear where more Printing settings can be made.
Serial Port/Printer	Captured data will be echoed to a serial port, which may be cabled to a printer or another computer. A new tab will appear where more Printing settings can be made.
Parallel Port Printer	Captured data will be echoed to the LPT1 parallel port, which may be cabled to a printer. A new tab will appear where more Printing settings can be made.
UDP (Syslog)	Captured data will be echoed to a remote computer using the UDP network IP protocol, optionally with Syslog headers. A new tab will appear where more Network settings can be made.
TCP Server	Captured data will be echoed to a maximum of five remote computers using the TCP Server IP protocol. A new tab will appear where more Network settings can be made.
TCP Client	Captured data will be echoed to a remote computer using the TCP Client IP protocol. A new tab will appear where more Network settings can be made. This option may be used for 'IP Printing' using port 9100.

The serial and parallel port printer options may be preferred over using a normal Windows printer because the Windows printer drivers often prevent data being printed while it's still being captured. Driving the printers directly avoids any Windows queues or buffering, giving immediate print on impact printers, or full pages when 66 to 72 lines have arrived at a page printer (like a laser). The downside of direct printer access is that codes may need to be set to the printer to set margins, paper length, font size, etc.

Data Format

This option is used to define the Data Format for captured data, where separate columns need to be identified to be saved to database columns or for filtering and alerts.

Fixed Width Columns	Fixed width columns is the most common data capture format where each line is the same length with columns separated by a variable number of spaces so each has a fixed starting position and length. Sometimes trailing space at the line end are skipped so the lines are variable length.
Character Separated Columns (CSV)	Character Separated Columns (sometimes called Character Separated Variables) data is where variable length columns have a separator character usually a comma. To allow the columns to contain the separating character, they may optionally, or always, have double quotes, ie "ComGen Test", "192.168.1.109", "PC09" ComCap allows the separating character to be specified, and then counts columns to identify them.
Variable Named Columns (=)	Variable named columns data is where space separated columns are named, so the column name is followed by the data, with double quotes being used if the data contains a space, ie msg="Connection Opened" n=6258475 src=192.168.1.109:3008:LAN dst=216.22.212.19:80:WAN proto=tcp/http. This format is used by the Sonicwall firewall appliance for it's Syslog.

The selection of Data Format here defines the appearance of the grid on the Data Format tab.

Idle TCP Server Close Session Timeout, Zero None (secs)

This option is only available for TCP Server capture or Echo to TCP Server, and allows a TCP Server session to be closed if no data has been received for a specified period of seconds. Generally a remote TCP Client will reconnect when it has more data to send. This timeout is primarily for error conditions where a session remotely fails without a clean close down happening, so TCP Server waits for ever for new data, unless Data Loss checking is used to restart capture which is more complex. The timeout should vary depending on how frequently data is expected, and may be up to 99,999 seconds (69 days).

Note that 'Check for Data Loss' provides similar functionality, but is more extreme in it's handling since it will cause the channel to restart, closing files, database, etc, perhaps sending an alert, whereas the session timeout is gently within only minimum disconnection logging while waiting for a new session to connect.

Capture Restart Attempts

If capture fails to start, Capture Restart Attempts are specified as seconds before another attempt is made to start capture. This duration is also used for restarts caused by database problems.

Commands to Send upon Start and Stop Capture

Command strings may optionally be sent when capture is started and stopped, perhaps to trigger a remote appliance to start or stop. The strings may include escape sequences to specify non-printing characters:

\n	New line (CRLF)
\f	Form Feed (FF)
\c	Carriage Return (CR)
\l	Line Feed (LF)

\\	Backslash (\)
\e	Escape (ESC)
\xnn	Any hex code where nn is 01 to FF
\P	50ms pause in the data being sent, with multiples allowing a longer delay. Note the pause may not necessarily be effective with TCP/IP, because packets may get combined at transport level, nor may the pause be exactly 50ms due to other activity within ComCap

Note that no line end is normally sent, so \n will commonly be used. A delay in seconds may be specified before the data is sent, to allow the connection to settle and perhaps for start-up data to be received. Zero means no delay.

Repeat Start Command

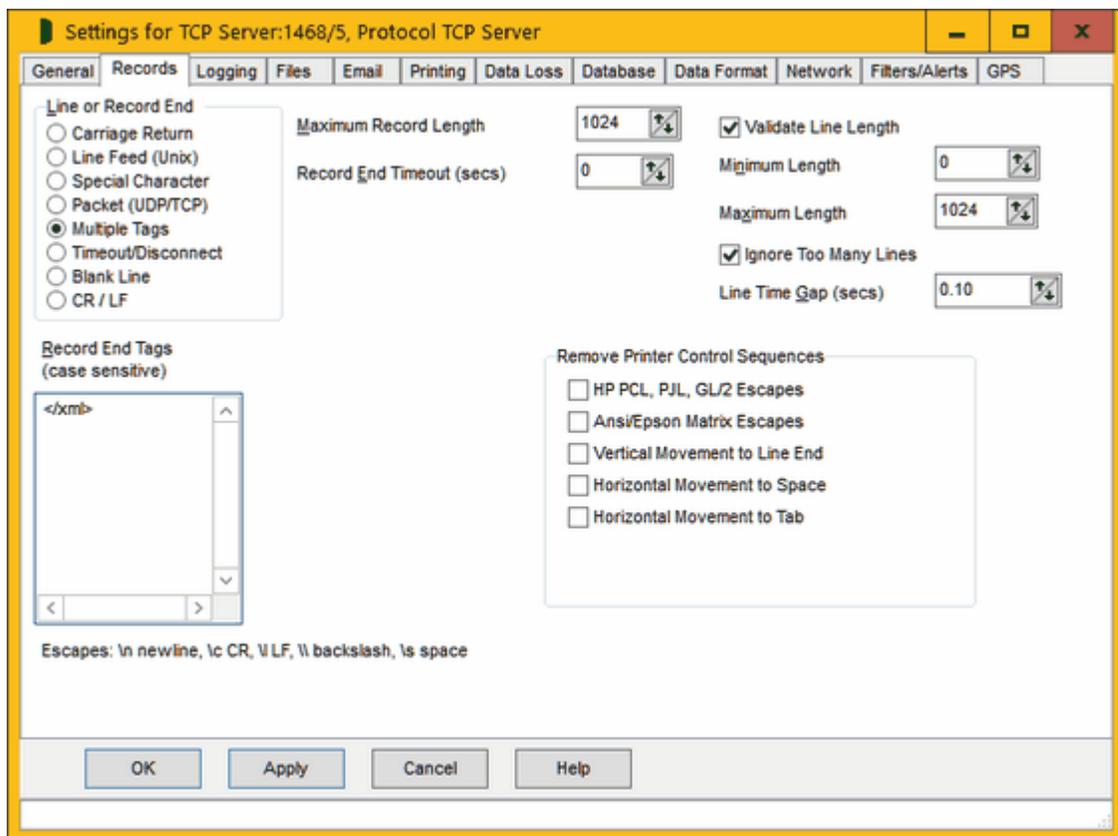
Setting 'Repeat Start Command' to a non-zero value of seconds causes the Start command text to be repeatedly sent at the specified interval. The maximum interval is 999,999 seconds (277 hours), with zero meaning don't repeat the command. This is a fail safe for appliances that only return data when triggered, in case they are reset or repowered while capture is running.

Log Only First Command Sent

Ticking this option prevents repeated logging when the Start Command is repeated sent, filling up the info log.

3.2 Records

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies General capture information



Line or Record End

This option specified how ComCap checks for the end off each captured line or record, so it can be displayed and captured. Identifying records is important for database capture, since one line is assumed to contain only one record.

Carriage Return	This is the normal line ending for PC ASCII files which normally have both CR and LF at the end of a line and CR and FF (form feed) at the end of a page. Note that LF and FF are ignored.
Line Feed (Unix)	This option should be used for files created by UNIX systems, which typically only have LF characters. FF (form feed) at the end of a page is ignored.
Special Character	Allows any line ending character to be specified in hex, may be used for special protocols
Packet (UDP/TCP)	This is the default for the UDP protocol where one line is sent per datagram or packet usually without any CR or LF. Note that CR or LF in the packet will be ignored using this option. Beware that the TCP protocol allows packets to be split or combined by routers and firewalls, so received packets may not always be identical content to those sent.

Multiple Tags	Allows the end of a line or record to be determined by one or more short words or tags, instead of by CR or LF. This is primarily designed to ease parsing for database capture, so that multi line data can be processed, and also for multiple records to be sent without line endings.
Timeout/Disconnect	Allows end of line or record by Line End Timeout (see below) or disconnection. The same effect can be achieved by specifying a special character that is never expected. This is intended for capturing multiple line data such as remote alarm reports, which arrive as a burst of data, separated by a gap from the next report or by serial lines dropping or TCP channel disconnecting
Blank Line	Allows end of line or record by a blank line. Multiple line non-blank records to be captured as a single long line when a blank line is reached. Specifically, Nortel telephone switches generate call data records (CDRs) comprising three lines of call data following by a blank line, and this option allows such records to be captured as a single long line making subsequent processing such as adding to SQL much easier. Note a blank line is considered as CRLF CRLF.
CR / LF	Allows end of line for PC ASCII files with both CR and LF at the end of a line. FF (form feed) at the end of a page is ignored. CR/LF is safer than CR alone when capturing packet type data containing non-ASCII values.

Note that a line also has a maximum length, as defined below, and will be 'broken' when it's reached if no line end character is found first. If the display shows lines combined together, this usually means the wrong Line End is selected. A line is also 'ended' when a TCP session closes or capture is stopped, which may result in a partial record or line.

Max Line Length

The Maximum Line Length may be specified up to 20,000 characters, with a default length of 256 characters. If the maximum is reached, the captured line is broken and wrapped to the next line. Validate Line Length below may be used to ignore captured lines that are shorter or longer than specified limits without wrapping them.

Line End Timeout

A Line End Timeout may now be specified in seconds, where zero means no timeout, up to 300 seconds. When the timeout expires, an incomplete captured line will be processed, saved and displayed. This is usually only necessary when non-ASCII data is being captured where there are no carriage returns or line feeds, but may also be useful when setting up ComCap to capture from a serial port with unknown speed, since it can be used to cause display of the 'corrupted' data caused by speed mismatch which will be missing line ends.

Special Line Ending (hex)

If Line or Record Ending is specified as Special Character, this field specifies that character in hexadecimal notation.

Validate Line Length

If ticked, a minimum and maximum line lengths may be specified in characters, allowing shorter or longer lines to be ignored. This check is done after leading and/or trailing space is removed, but

before escaped text is added. It may be useful where data or transmission becomes corrupted combining two or more lines, or truncating a line, and specifically for database capture where a records of a certain length are expected.

Ignore Too Many Lines, Line Time Gap

This option may be used to reduce the amount of data captured from devices sending continuous streams, such as GPS locators or environmental sensors. A 'Line Time Gap' in fractions of a second (two decimal places) may be specified during which any new data will be ignored. If the gap is set to 0.50 second, then only a maximum of two lines per second will be captured, or it may be one line every few seconds. The number of lines ignored are still counted and reported. This feature may be used to slow down database updates by ignoring data arriving too fast. Note that due to Windows multi-tasking, the intervals may not be precise.

Record End Tags

If Line or Record Ending is specified as Multiple Tags, one or more short words or tags may be specified in a list, one line per tag. If these records have unwanted preceding or following tags, these may also be set as record endings and then filtered by phrases or minimum line length. For instance, the following data was sent by ComGen without any line endings:

```
<TEST>
<xml XML Packet from ComGen Id 8 on PC09 at 2009/10/14-00:15:54:334 />
<xml XML Packet from ComGen Id 8 on PC09 at 2009/10/14-00:16:24:334 />
<xml XML Packet from ComGen Id 8 on PC09 at 2009/10/14-00:16:54:334 />
```

so setting the Record End Tags as <TEST> and /> causes ComCap to break the records so they may be filtered or captured to a database sensibly, in this case with the minimum line length validated to remove the device id on the first line.

Record End Tags may include escaped characters similarly to 'Add Escaped Text', specifically \n new line, \c CR, \l LF, \ backslash and \s space, so text only at the end of a line can be specified as a tag.

Remove Printer Control Sequences

This option offers various means of cleaning up data captured from older computer printer output. If possible, the old computer printer driver should be configured for something as basic as possible, to avoid additional print formatting escape commands being added. If this is not possible, ComCap will attempt to remove these escape commands.

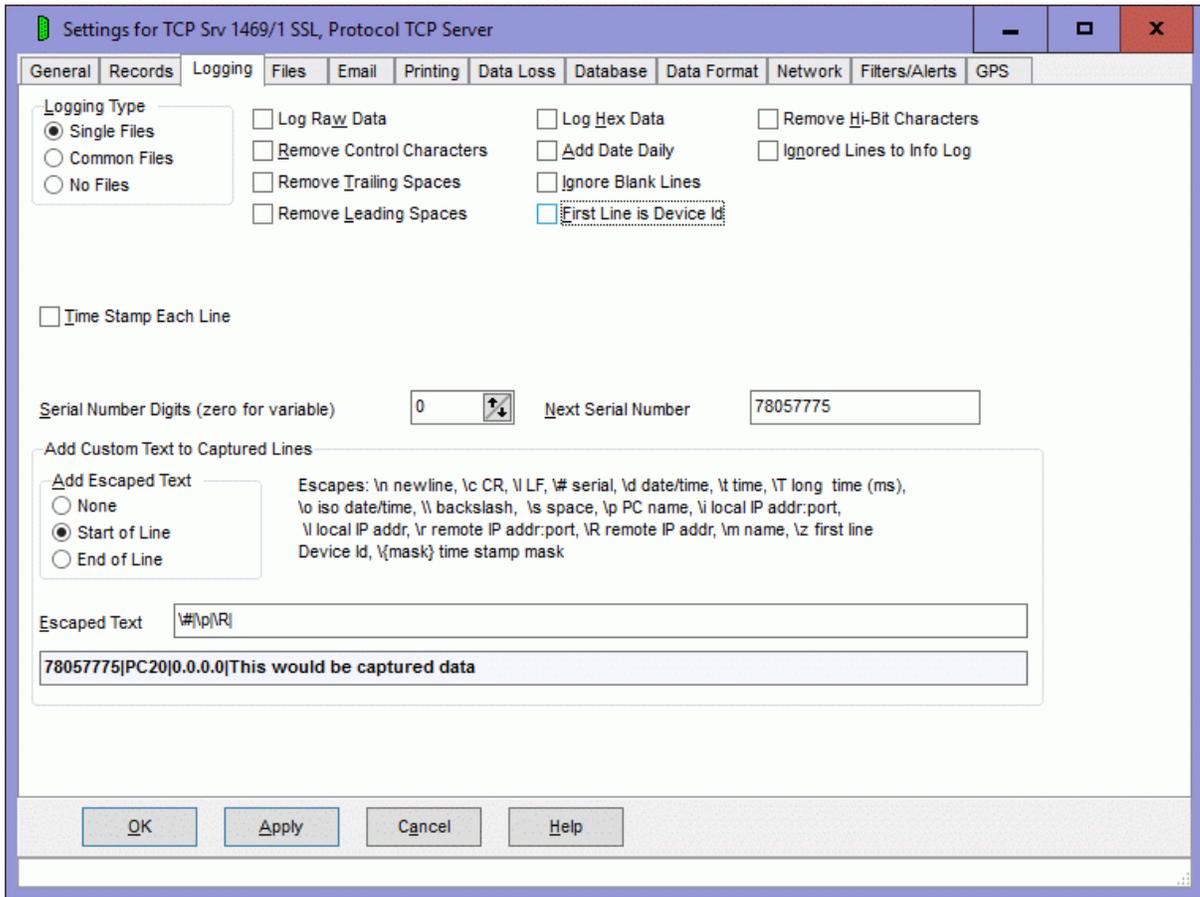
HP PCL, P JL, GL/2 Escapes	Removes the PCL3, PCL4 and PCL5 codes used by most Hewlett-Packard printers and many others emulating them, including fonts and raster graphics. PCL6 codes are ignored.
Ansi/Epson Matrix Escapes	Removes codes mostly used by old impact printers, note there are many permutations of these codes defined by different manufacturers, and only the most common codes are handled.
Vertical Movement to Line End	Converts PCL cursor movement to a line end.
Horizontal Movement to Space	Converts PCL cursor movement to a space.
'Horizontal Movement to Tab	Converts PCL cursor movement to a tab.

Beware printer drivers can use massive amounts of cursor movement, even placing each word or character individually on a page, so captured data may not be as expected. For instance, some Windows applications printing using PCL5 send each word on a separate line preceded by several PCL cursor movement escapes, and followed by CRLF, so even after removing the escapes, ComCap will end up with one word per line.

For debugging purposes, ticking 'Ignored Lines to Info Log' on the Logging tab causes any removed printer controls (except binary and graphics) to be logged to check that no real content is being removed.

3.3 Logging

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies how captured data should be logged and manipulated.



Logging Type

The Logging Type menu specifies how capture data is written to files.

Single Files	Each channel captures to it's own single file
Common Files	Two or more capture channels save data into the same common file as specified in Common Settings, Log Files. Note that old data for individual channels can not be viewed when changing tabs, since it has not been written to separate files.

No Files	Captured data is not written to any file, usually where it is just being echoed or saved to a database. This option is really not recommended.
----------	--

Log Raw Data

ComCap normally processes any received data to remove or translate non-printing characters that may cause problems in capture log files. Ticking this option causes data to be captured exactly as received. The data display on the screen will still be processed to remove non-printing characters.

Remove Control Characters

ComCap normally translates superfluous control characters captured into spaces; this includes null, tabs, form feeds, etc. If this setting is ticked, such control characters are removed completely. Which option is preferred will depend upon the data being received. Some data may include tabs to separate columns of information, so conversion to a space is better; other data may include padding nulls which cause formatting problems if converted to spaces so are best removed. If control characters are needed in the capture log, use the Log Raw Data option, see above. This is not allowed if Log Raw Data is ticked.

Remove Trailing Spaces

If ticked, specifies that trailing spaces or control characters at the end of each line should be removed. This is not allowed if Log Raw Data is ticked.

Remove Leading Spaces

If ticked, specifies that leading spaces or control characters at the beginning of each line should be removed. This is not allowed if Log Raw Data is ticked.

Log Hex Data

If ticked, causes all captured data to be converted into hexadecimal (doubling the size). This is primarily intended for capturing binary data, but may be used a debugging tool to find the exact format of data being captured, for instance the type of line endings. Normal line ending rules are applied when capturing in hex, so lines may be broken on linefeed, etc (also saved in hex).

Add Date Daily

If ticked, causes the date and time to be added before the first data is captured each day, or when logging starts.

Ignore Blank Lines

If ticked, causes lines without any printable characters to be ignored. This will reduce the size of logs that contain far too many blank lines. This option should generally be used with 'Remove Control Characters'.

First Line is Device Id

If ticked, causes the first captured line to be saved and not logged. The first line may then be added to subsequent captured lines using 'Add Escaped Text' with the \z command. A number of remote TCP devices may be configured to identify themselves when a TCP session connects, by sending a device id as the first line of data. For instance, Tyso eCov serial to TCP/IP converter sends a five digit configurable number as the first line, while some GSM/3G modems send a device type and IMEI number. So effectively the Device Id is added to each captured line to identify it, specifically with TCP Server where lots of different remote devices may be calling home. For instance, the raw output from Tyso eCov 100 when starting a session is:

```
02345A
```

```
Text test line from ComGen Id 2 on MAGSERVER at 19:15:37 serial 009688
```

```
Text test line from ComGen Id 2 on MAGSERVER at 19:15:38 serial 009689
```

```
Text test line from ComGen Id 2 on MAGSERVER at 19:15:39 serial 009690
```

so this option suppresses the device Id on the first line, and adds it the each following line instead.

02345A Text test line from ComGen Id 2 on MAGSERVER at 19:15:37 serial 009688
 02345A Text test line from ComGen Id 2 on MAGSERVER at 19:15:38 serial 009689
 02345A Text test line from ComGen Id 2 on MAGSERVER at 19:15:39 serial 009690

Remove Hi-Bit Characters

If ticked, filters out any characters with the hi-bit set, above ASCII 127. This complements 'Remove Control Characters' and may help clean up corrupted modem data.

Ignored Lines to Info Log

If ticked, causes line ignored by 'Validate Line Length' or 'Ignore Lines with Phrases' to be logged to the information log instead. Note this is really for debugging, the info log might get large if a lot of lines are ignored. Lines ignored for 'too many' are not logged since this defeats the purpose. This option also logs printer control sequences removed.

Time Stamp Each Line, Time Stamp Mask

If ticked, adds a time stamp and optional text at the start of each logged line. This may be useful when logging periodic data such as alarms that don't include the time within the captured data, or where the time may be inaccurate. The Time Stamp Mask should be specified, this defaults to `hh:nn:ss:zzz|` which would cause something like `12:41:05:107|` to precede each captured line. The `:zzz` can be removed if millisecond accuracy is not needed. This option is not available if logging 'Raw Data'. The mask characters and format are identical to those used for Custom Log Names, see Files. Note that Escaped Text at the start of the line is added after Time Stamp Each Line, if both are used together.

Next Serial Number, Serial Number Digits

ComCap allocates a Serial Number for each line that is captured (unique to each channel). Next Serial Number specifies the next serial number to be used, and may be changed if necessary. The serial number increments for each captured line will wrap back to one when it reaches the specified Serial Number Digits length, or zero if it should increment indefinitely. The Serial Number may be added to each captured line using the Add Escaped Text option below, or used in a database column. This is primarily for the benefit of other applications that process the data in real time, so they don't process duplicate data. It may also be used to confirm that lines have not been lost from the capture logs. Note it will not help if data is lost before being written to the logs.

Add Escaped Text

To assist in identifying and optionally further processing captured text, extra text may be added to the start or end of each captured line. The extra text may include escape sequences to added

<code>\#</code>	Serial Number, unique to channel incremented for each line, with leading zeros according to Serial Number Digits above
<code>\d</code>	Date and time, ie 21-Jun-2006 20:10:12. Note this is a fixed date format, if more flexible formatting is needed use the Time Stamp Each Line option above.
<code>\t</code>	Time, ie 20:10:12
<code>\o</code>	ISO date and time, ie 2006-06-21T20:12:11, recommended for database capture
<code>\T</code>	Long time with milliseconds to three decimal places, ie 10:22:56:586 (but Windows is not millisecond accurate)
<code>\s</code>	Space, used as a separator at the start or end of the escaped text, not necessary within the text
<code>\p</code>	PC Name (NETBIOS),ie MYCOMPUTER
<code>\i</code>	Local IP address and port, ie 192.168.44.55:514

\l	Local IP address, ie 192.168.44.55
\r	Remote IP address and port, ie 192.168.44.55:514
\R	Remote IP address, ie 192.168.44.55
\m	Capture Name, note spaces may cause problems
\n	New Line (CRLF), not generally recommended
\f	Form Feed (FF)), not generally recommended
\c	Carriage Return (CR)), not generally recommended
\l	Line Feed (LF), not generally recommended)
\\	Backslash (\)
\e	Escape (ESC)), not generally recommended
\xnn	Any hex code where nn is 01 to FF
\z	Device Id, saved from first line captured
\{ }	Adds freely format dates and times, similarly to 'Time Stamp Each Line' using mask characters placed between the two curly brackets. The mask characters and format are identical to those used for Custom Log Names, see Files and the example below.

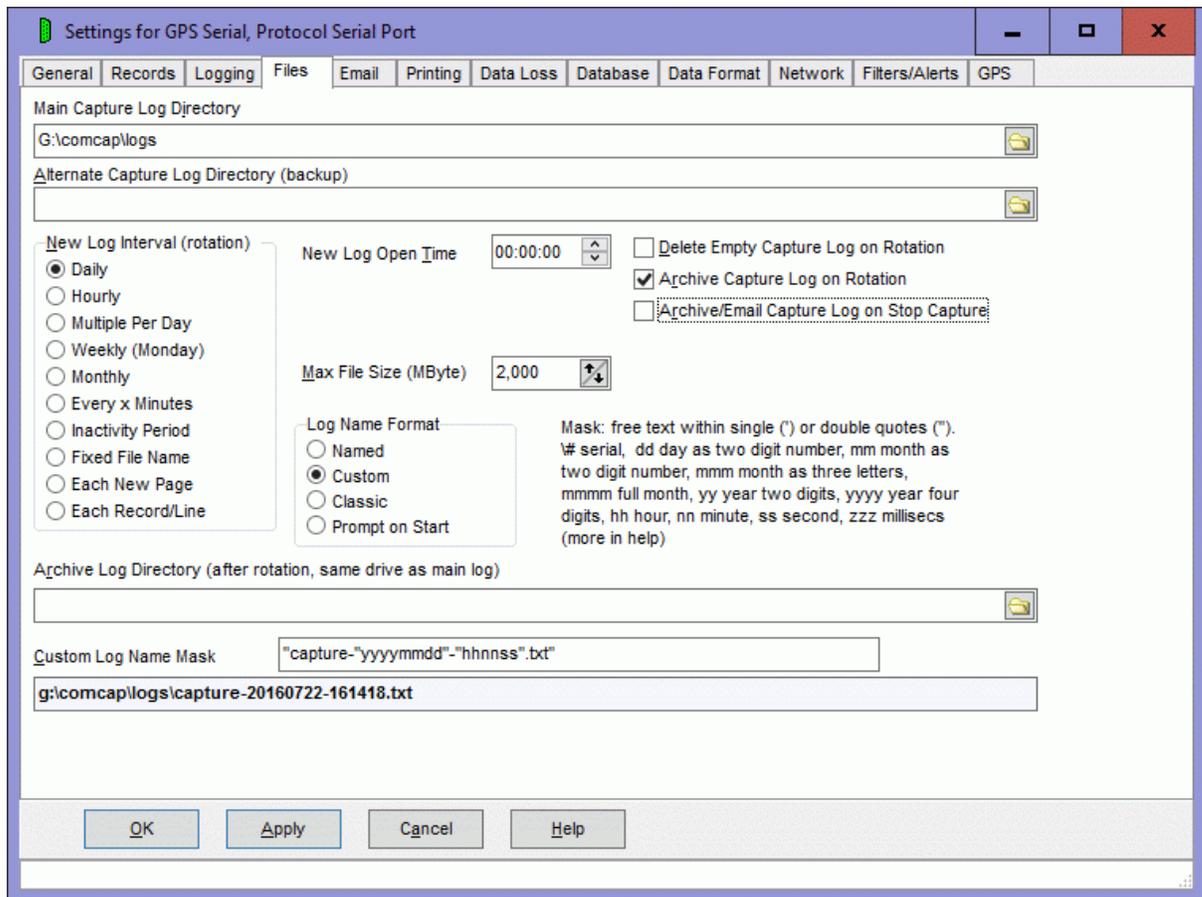
For Serial Number Digits set to eight, examples of adding escaped text are as follows:

Escaped Text	Resulting Text
\# \ols	0123567 2006-06-21T20:12:11
#\#	0124567
,"#\#"	,"0123567"
\p,\r,	MYCOMPUTER, 192.168.44.55:514,
\{hh:nn:ss.zzz}	12:59:06.720
\{yyyymmdd"-"hhnnss}	20121101-124906

Note that Escaped Text at the start of the line is added after Time Stamp Each Line, if both are used together. Escaped Text is not allowed if Log Raw Data is ticked.

3.4 Files

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies Capture Log file names.



x

Capture Log Directories

Allows Main and Alternate Capture Log Directories to be specified, in which capture log files be created. The Alternate Directory may be left blank if backup logs on a second disk drive or network share are not required. Clicking the icon at the end of directory edit box displays a Browse for Folder dialog allowing a drive and directory to be selected. If a new directory should be created, just enter it and it will be done automatically. It is not possible to save Capture Settings unless a test file can be created and written to the Main Capture Log Directory, and to the Alternate if specified. If network shares are used, a LAN Logon may need to be set-up in Common Settings, LAN/Misc. UNC network paths may be used.

Note that ComCap will exceptionally save Capture Logs and Information Logs in the program directory, if the normal directories are unavailable or are not specified during start-up.

New Log Interval

Specifies how often a new Capture Log file should be opened. Note that each separate channel uses separate files (unless Common Logs are specified), and may have different settings.

Daily	A new capture log is opened once a day, which is at the New Log Time, see below. If the log is opened at midnight, the file name need only contain a date mask otherwise it needs the time of day as well.
Hourly	A new capture log is opened each hour, on the hour. This could be used with a custom name mask of "capture-\"yyyyymmdd-hh\".txt" so the file name contains hours only, and no minutes.

Multiple Per Day	Multiple new capture logs are opened each day, according to Logs Per Day, starting at the New Log Time, see below.
Weekly (Monday)	A new capture log is opened once a week, on Monday, starting at the New Log Time, see below.
Monthly	A new capture log is opened once a month, at midnight on the first day of the month.
Every x Minutes	A new capture log is opened after the time period specified in New Log Every (see below), perhaps every 30 minutes. Typically used for high traffic situations. The difference from Multiple Per Day is that a new log is opened each time capture starts, and then periodically.
Inactivity Period	A new capture log is opened each time the old log is closed due to the 'Inactivity delay before closing capture log' specified in Capture Logging expires. This setting is typically used for capturing batch information, such as printed reports.
Fixed File Name	Always used the same fixed file name for the capture log, beware the log may be get very large unless purged by another application.
Each New Page	A new capture log is opened at the end of each page, when a form feed control character is received. This setting is typically used for capturing batch information, such as printed reports.
Each Record/Line	A new capture log is opened for each record, which is usually one line, which will create lots of short log files. This is really intended for capturing multiple line data such as remote alarm reports where the record end is specified as a timeout or (end) or something, rather than high speed tabular type data.

Note that the Log Interval has an effect on how much old data can be viewed interactively. When changing capture tabs to view data from other channels, only data from the current capture file is restored, if any. To look at older data, the specific capture log must be opened by file name. This also applies to Common Files logging, where data from more than one channel is written to the same common log file, so can not be restored to different tabs.

New Log Open Time

For the New Log Interval Daily, specifies at what time of day the new log is created, defaulting to 00:00:00 for midnight. If the time is set to anything other than midnight, the 'Log Name Format' must include provision for the time of day in the file name.

New Log Every

For New Log Interval: Every x Minutes, specifies how often a new log file should be opened, defaulting to every 60 minutes. Note that new log files are only created when new capture data arrives, so there will not be any empty files during quiet periods. Logs are always opened on the exact minute.

Logs Per Day

For New Log Interval Multiple Per Day, specifies how many new log file should be opened each day, starting at the New Log Time. Four logs per day with a new time of 00:00 would create new logs every six hours at 00:00, 06:00, 12:00 and 18:00; three logs starting at 06:00 would create new logs at 06:00, 14:00 and 22:00; seven logs per day from 00:00 would create new logs every 206 minutes, at 03:26, 06:52, 10:18, etc. The minimum Logs Per Day is two, maximum is 12, for lower or higher use the Hourly or Daily settings.

Max File Size (MBytes)

This option allows the maximum capture file size to be limited, with a new file being created once a specified size is reached, in megabytes. The default is 2,000 (which is 2 gigabytes). Some care is needed with log name format, specifically if it does not contain sufficient granularity to create a unique

file name, so if more than than one file per day is needed, the name mask must include at least hours. If a new file name can not created, a default name with date and time in seconds will be created.

Delete Empty Capture Log on Rotation

Ticking this option avoids empty capture logs remaining on disk, after they are closed and a new log opened. Note this only applies to the main capture log, not the alternate.

Archive Capture Log on Rotation

Ticking this option causes a log file closed for rotation for a new file name to be moved to an archive directory on the same disk drive. Many ComCap users further process capture logs, sometimes with difficulty due to the files being continually updated, so this options means that scanning the archive directory and will only find completed capture logs, and not those still open in the main capture directory. To FTP an archived capture log, use our DUN Manager application which offers various Scheduled Tasks including FTP Upload which will automatically FTP any files it finds in a specified directory (use the new 'Archive Capture Log on Rotation' feature, see above) and then move them elsewhere so they are not sent again.

Archive Log Directory

Specifies the directory to which the capture log should be moved when closed on rotation for a new log file. This directory must be on the same disk as tge capture directory, since the capture log is renamed to new directory, rather than being copied which is potentially much slower.

Archive/Email Capture Log on Stop Capture

Ticking this option causes the log to be archived even if the rotation time has not yet arrived when ComCap is stopped. If ComCap is restarted before the next rotation time, a new log with the previous name will be created, but when it is finally archived it will be renamed by the addition of -1, -2, etc, to the file name to avoid a conflict with previously archived log file names, if any.

Log Name Format

Specifies whether the file name format used for log file is standard or is customised by the user.

Named	This format uses the channel name, then the date and time, ie the mask is <code>name-yyyyymmdd-hhmmss.txt</code> , so for Channel Name <code>Cdrs com3</code> , the log name format would be: <code>d:\logs\cdrs com3-20061005-152014.txt</code>
Custom	For a Custom log Name Mask of " <code>phonelogs-\"yyyy-mm\".txt</code> ", the log name format would be: <code>d:\logs\phonelogs-2006-oct.txt</code>
Classic	This is the format used by ComCap v3, for serial port channels it's capture followed by the port number, then the date and time, ie the mask is <code>captureX-yyyyymmdd-hhmmss.txt</code> , for network channels it's network following by the Channel Id: <code>d:\logs\capture3-20061005-152059.txt</code>
Prompt on Start	Allows a specific file name to be specified each time capture is started. Setting this option automatically sets 'Fixed File Name', and can only be done if ComCap is not specified for Auto Start or to run as a Background Service, since ComCap would never actually start. The initial file name can be specified here, but ComCap always saves the last name specified in the Open File dialog that appears when capture starts. This feature is intended for applications where data is being captured from a single device for a specific purpose, such as a laboratory test. The 'Add Comment to Log' right menu option might also be useful to add information to the capture log.

Custom Log Name Mask

The Custom Name Format allows a Custom Log Name Mask may be created. This is done using mask characters that specify how the log date and optional time are formatted in the file name.

The Custom Log Name Mask may optionally include a sub-directory typically using a partial date, so a new sub-directory is created monthly or daily, to avoid large numbers of files in the same directory, in the format: subdir/filename.txt.

Be very careful creating the file mask, it must include sufficient date and time masks to ensure a unique file name is created to match how often new logs are opened, so a daily log must have the day, an hourly log the time, and new record/line a serial number, seconds or milliseconds depending on how often new data will arrive.

\#	Add the current serial number to the mask, which may be used instead of date and time for unique sequential file names.
----	---

Date and time elements are creating using characters strings from the following table:

c	Date and time using the Windows default settings.
d	Day as a number without a leading zero (1-31).
dd	Day as a number with a leading zero (01-31).
ddd	Day as an abbreviation (Sun-Sat).
dddd	Day as a full name (Sunday-Saturday).
dddddd	Date using the short Windows default setting.
ddddddd	Date using the long Windows default setting.
m	Month as a number without a leading zero (1-12).
mm	Month as a number with a leading zero (01-12).
mmm	Month as an abbreviation (Jan-Dec).
mmmm	Month as a full name (January-December).
yy	Year as a two-digit number (00-99).
yyyy	Year as a four-digit number (0000-9999).
h	Hour without a leading zero (0-23).
hh	Hour with a leading zero (00-23).
n	Minute without a leading zero (0-59).
nn	Minute with a leading zero (00-59).
s	Second without a leading zero (0-59).
ss	Second with a leading zero (00-59).
zzz	Milliseconds with leading zeroes (000 to 999)
t	Time using the short Windows default setting.
tt	Time using the long Windows default setting
am/pm	The am/pm specifier can use lower, upper, or mixed case.
a/p	The a/p specifier can use lower, upper, or mixed case.

/	Date separator character.
:	Time separator character.
\	Path separator character, not at front or end.

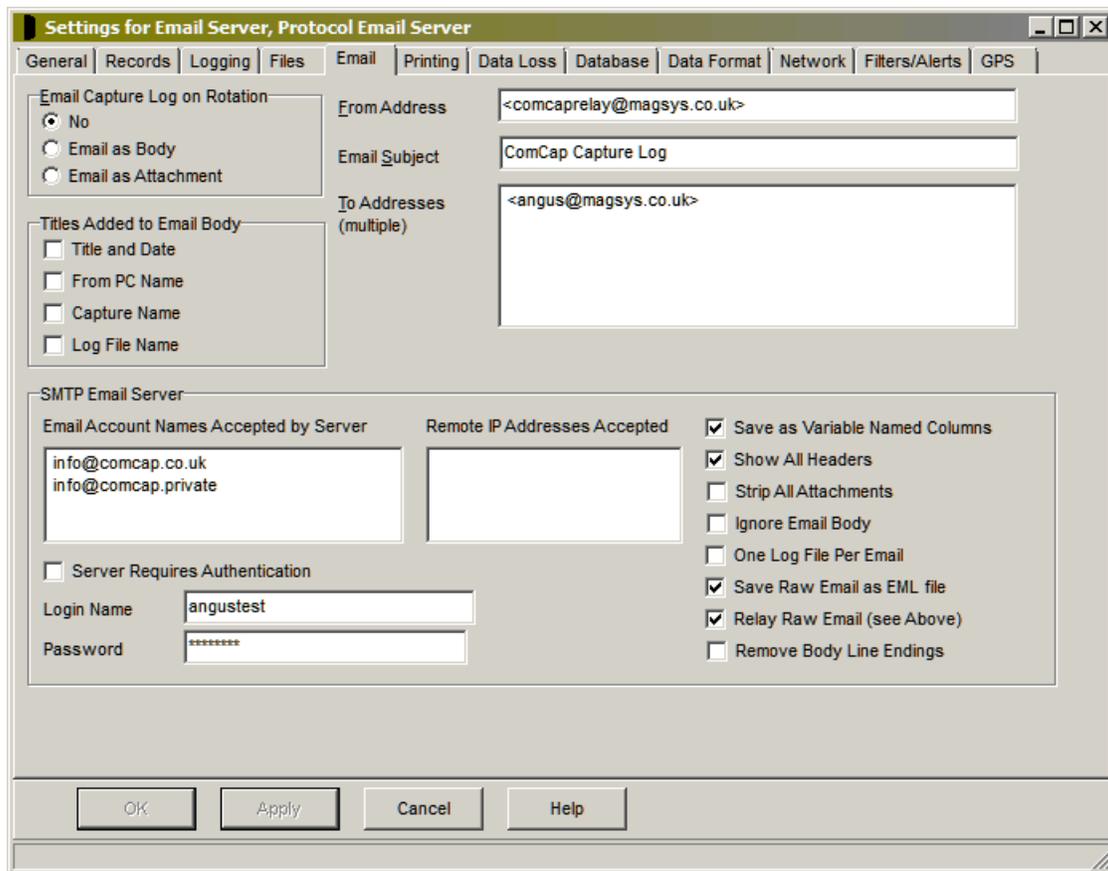
Any text to appear in the file name should be within single (') or double quotes ("). Note that a directory path may be included within the mask, so new directories are created each day or month. The mask must not include the leading back slash. The following table shows several mask examples.

Mask – quotes are needed	Resulting File Name
"capture-"yyyymmdd".txt"	capture-20060828.txt
"capture2-"yyyymmdd"- "hnnss".txt"	capture2-20060828-145404.txt
yyyy"- "mmm"- "dd".log"	2006-Aug-28.log
ddd" "d" "mmmm".txt"	Wednesday 28 August.txt
"cdr-"dd/mm/yy".log"	cdr-28/08/06.log
"month-"mm"info1-"yyyymmdd".txt"	month-09\info1-20060929.txt
"info1-"yyyymm"\ "dd".txt"	info1-200609\29.txt
"info1-"yyyymm"\ "yyyymmdd".txt"	info1-200609\20060929.txt
"info1-\#.txt"	info1-123456.txt (serial number)
'yyyy-mm"capture-"yyyymmdd".txt"'	\2006-09\capture-20060828.txt

As the Custom Log Name Mask is typed, the resulting file name appears dynamically. When capturing data from multiple channels, note the file names must be unique if the capture logs are saved in the same directory. It is not possible to add the channel number or name using mask characters so it must be added as text, ie 1 or 2, etc.

3.5 Email

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies how captured data may be emailed, and how email itself can be captured.



Email Capture Log on Rotation

This option allows capture logs to be automatically emailed when closed and rotated. There are options to 'Email as Body' where the log will be copied into the body of the message, or 'Email as Attachment' where the capture file will be attached to a short body. On the Files tab, 'Archive/Email Capture Log on Stop Capture' causes the log to be emailed even if the rotation time has not yet arrived when ComCap is stopped. For email to function, at least one SMTP Server must be specified in Common Settings, Email.

Note that emails are placed in a queue, as detailed in Common Settings, Email. There is a maximum size of 10 Mbytes for the capture log to be emailed, although some email servers may not accept email of that size.

Email Subject, From Address

The Email Subject should be specified, then the From Address with a descriptive name in double quotes, followed by the actual email address in angle quotes, ie "Works PC19" <pc19@magsys.co.uk>.

To Addresses

One or more addresses may be specified to which the log will be sent, each address should be on a separate line, with a descriptive name in double quotes, followed by the actual email address in angle quotes, ie "ComCap" <comcap@magsys.co.uk>.

Titles Added to Email Body

Each email created has up to four title lines added in the body, above the log, to provide identification. Which of these four titles is added depends on four tick boxes: Title and Date, From PC Name, Capture Name and Log File Name. Unticking a box removes that title.

SMTP Email Server

ComCap can capture alert emails sent by internet aware appliances, such as firewalls, security monitors, power distribution units, uninterruptible power supplies, remote sensors, transponders, etc. The emails may be written to a SQL database or used to trigger alerts. An Email Server channel must first be set-up in Common Settings, Network with a single local address, usually with port 25 or 587. Internet appliances that will send email to ComCap should have their SMPT Mail Server changed to this local IP address, or set-up DNS for this address.

Email Account Names Accepted by Server

Specified a list of email addresses for which the server will accept email, these don't need real domains so info@comcap.private is acceptable, or *@comcap.private would allow email from any address with that domain, ie xxx@comcap.private. Email sent to addresses not on this list will be rejected by the server and not captured.

Remote IP Addresses Accepted

Specified a list of IP addresses from which email will be accepted, if left blank email will be accepted from any IP addresses.

Server Requires Authentication

Specifies the email server should only accept email if first authenticated with a single login name and password. Authentication methods supported are AUTH PLAIN, LOGIN, CRAM-MD5 and CRAM-SHA1.

Save as Variable Named Columns

Accepted emails can be captured as multiple lines of plain text, or by ticking this box as a single record. Each line of the email is formatted similarly to Subject="ComCap email testing" so ComCap Data Format parsing can separate the headers to be added to a SQL database. Three extra headers are always added, X-Envelope-From, X-Envelope-To and X-Originating-IP all from the SMTP envelope, in case the normal To: or From: headers are inadequate, and Date is converted to ISO format. The entire body becomes Body='xxx' with line endings replaced by \n. Unfortunately ComCap can not currently process CRLF in a record, it breaks too many things, but \n can translated back to CRLF in a SQL stored procedure if necessary.

Show All Headers

Ticking this option' will capture all the email headers, otherwise only From, To, Subject and Date are kept.

Strip All Attachments

MIME encoded emails are automatically decoded, but only text-plain and text-html sections processed. This option causes all but the main body to be ignored.

Ignore Email Body

Ticking this option only saves the email headers and might be sufficient where the subject contains the alert information.

One Log File Per Email

Ticking this option' causes capture log rotation for each new email provided the file name format is suitable.

Save Raw Email as EML File

Ticking this option causes each complete email to be saved separately to the capture file but in the same folder, with a unique file name, where it could be processed by another application.

Relay Raw Email

Ticking this option causes the complete email to be forwarded to one or more email addresses specified as 'To Addresses' (same as emailing logs).

Remove Body Line Endings

If ticked, line ending in the email body are replaced by spaces instead of \n, although this may

seriously mess up formatting.

SQL Email Capture

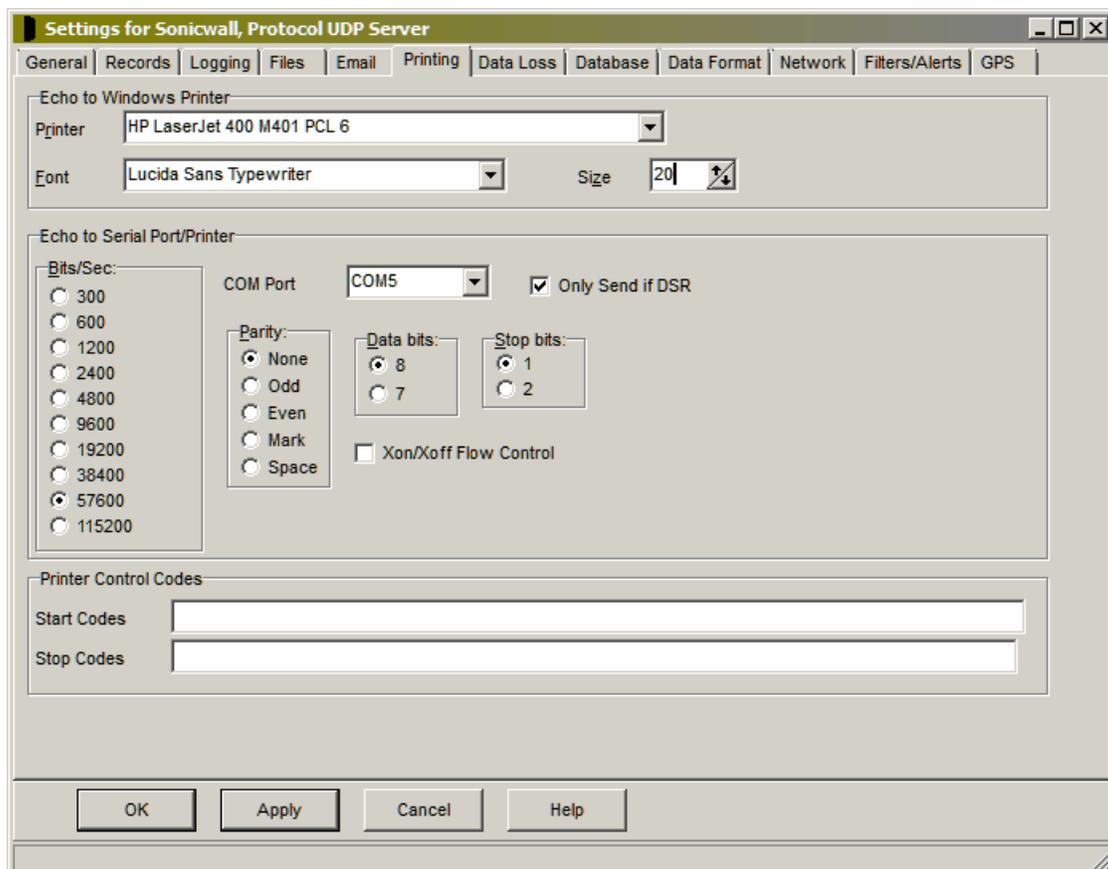
Since email formats vary so wildly, conceptually saving them with ComCap can cause many issues. Hopefully the 'Variable Named Columns' format and other options described are a good start, but ComCap users are welcome to offer feedback on alternatives from the real life emails generated by various appliances.

To demonstrate saving emails to a SQL database, a new Microsoft SQL Server table capture_email has been added to 'newdb-mssql.sql' and matching stored procedures to 'storedproc-mssql.sql'.

The maximum email size that is accepted is 32,000 characters, and SQL will usually only handle a field 8,000 characters long so that is really the maximum body size.

3.6 Printing

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies how captured data is echoed to printers or a serial port.



Echo to Windows Printer Overview

Allows captured data to be echoed to any installed Windows local or network printer. Only one channel can be printed at a time. Page printers may be used subject to the printer perhaps timing out waiting for new data and printing partial pages, but this feature is really designed for impact printers. To print using the ComCap Background Service, the service must be set-up with the account of a user

that has the required printer installed.

Note that some page printers may not start printing at all until capture is stopped and will instead spool the entire capture session. Magenta Systems has tested printing primarily with Hewlett-Packard LaserJet printers, III and 4000 series, and the Windows drivers for these have options 'Print Directly to Printer' and 'Spool print documents, Start Printing Immediately', on the Advanced properties tab. Either of these options causes pages to be printed as they are complete.

As an alternate to this option, 'Echo to TCP/IP Client' may be used for 'IP Printing' using port 9100. Many network printing will accept print data on TCP/IP port 9100.

Windows Printer

This option specifies the Windows printer to which captured data should be echoed. Clicking the arrow causes a drop down box to appear with a list of installed printers. If the selected printer is subsequently uninstalled, printing from ComCap will fail.

Font

This option specifies the font that will be used for printing which is selectable from the drop down list. Usually select a fixed pitch font such as Courier New.

Size

This option specifies the font point size for the printer.

Echo to Serial Port/Printer Overview

ComCap can echo captured data directly to a serial communications port to drive printers with a serial port directly, bypassing the Windows drivers and giving immediate print on impact printers, or full pages when 66 to 72 lines have arrived at a page printer (like a laser). This option can also be used to echo captured data to another computer using a serial cable. If multiple printers are available with sufficient serial ports, multiple channels can be printed.

COM Port

The Serial COM Port may be chosen from a drop list which excludes any already configured for capture. Note that if this COM Port is subsequently selected for capture, printing will fail.

Communication Port Parameters

The various serial parameters such as speed in Bits/Sec, Parity, Data Bits and Stop Bit need to be specified from the appropriate menus.

Only Send if DSR

To avoid overflowing buffers, ticking the Only Send if DSR box will disable serial port output unless a DSR signal is received from the printer or computer.

Echo to Parallel Port Printer Overview

ComCap can echo captured data directly to the parallel print port LPT1, but without any control. If the printer is not connected there is no warning. Testing has shown that windows will cache data if the printer becomes temporarily unavailable. Only one channel can print at a time.

Printer Control Codes – Start and Stop

For both serial and parallel printers, start and stop codes may be sent when a channel starts capture and stops, in order to initialise the printer, select paper, margins and font (Windows printer drivers take care of all this).

The Start and Stop codes may include escape sequences to specify non-printing characters:

\n	New line (CRLF)
\f	Form Feed (FF)

\c	Carriage Return (CR)
\l	Line Feed (LF)
\\	Backslash (\)
\e	Escape (ESC)
\xnn	Any hex code where nn is 01 to FF

For example, the start and stop code for a Hewlett-Packard LaserJet 4100 could be:

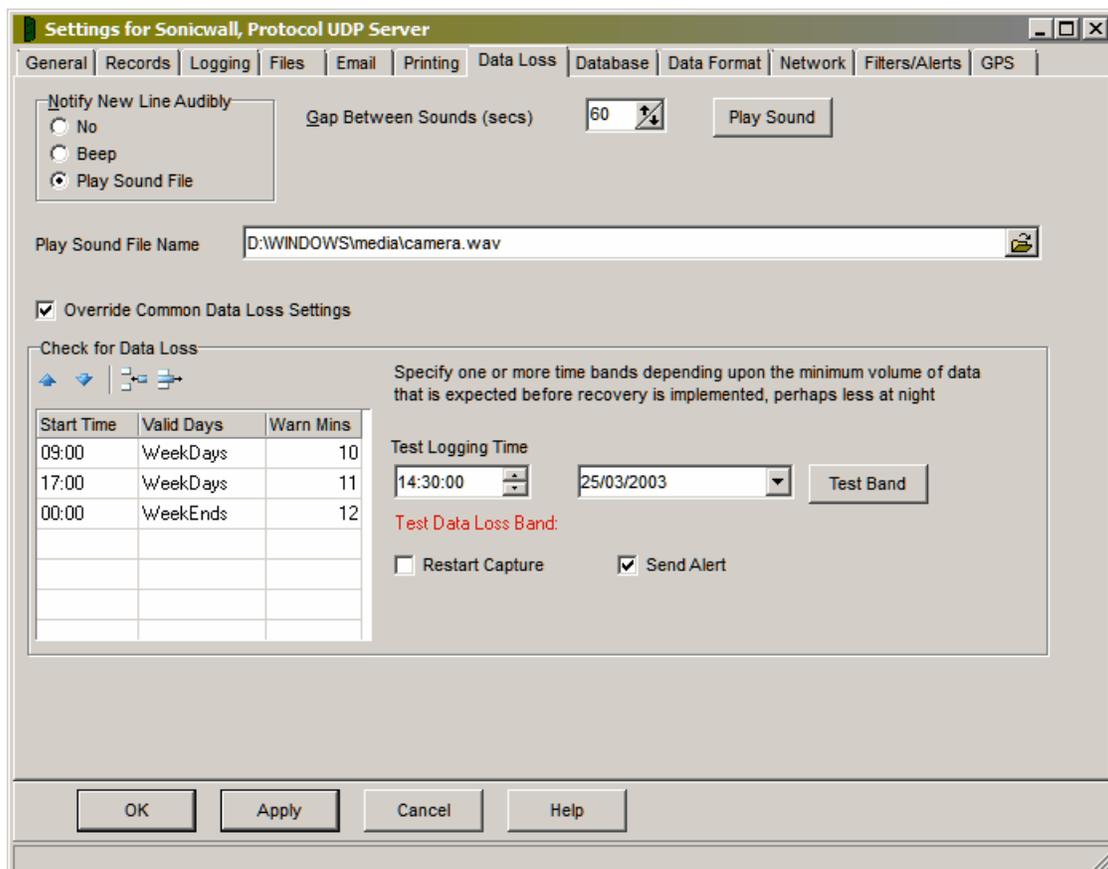
Start Codes: \e%-12345X\eE\&a5L\e&166F\&e(s15H

Stop Codes: \eE\&e%-12345X

which will set a left margin of 5, 66 lines per page, and 15 pitch Courier. The printer must be able to accept data with CRLF as line endings.

3.7 Sounds/Data Loss

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies Sounds and allows the common data loss settings to be overridden if required and specific separately for each channel.



Notify New Line Audibly

This option allows newly captured lines of data should be notified audibly, either by a PC beep or by

playing a specified sound file.

This feature is really designed for low volume data capture, such as swipe card logging. This feature works with the service version, and may be useful as a gentle confirmation that data is being captured.

Gap Between Sounds

A gap in seconds may be specified between audible notifications, to prevent continual noise when receiving frequent data. This gap is common to all capture ports, so there any further sounds are suppressed until the specified gap for the latest capture port has expired.

Play Sound File Name

A sound file `camera.wav` is supplied, as an example of what may be played.

Override Common Data Loss Settings

Unless this box is ticked, data loss settings are taken from Common Settings, Data Loss and the remainder of the data loss options on this tab will not appear.

Check for Data Loss Overview

ComCap provides a means to check that data is being continually captured, in case a problem stops capture. This is only useful where the data flow is reasonably steady, but different warning times may be set for different times of the day and week, for instance with business telephone call logging where there may be no data at night or at the weekends.

'Check for Data Loss' also needs to be ticked on the General tab before it is effective.

A multi-line grid allows several time periods to be specified, each with a different warning period, set in minutes (where zero is no warning).

Grid Control Buttons

There are four buttons used to manipulate the Data Loss grid:

Move Row Up	Used to move the selected row higher up the grid.
Move Row Down	Used to move the selected row lower down the grid.
Add New Row	Causes a new blank row to be added at the bottom of the grid.
Delete Row	Causes the selected row to be permanently deleted.

Data Loss Time Bands

It is common to need different warning settings at varying times of the day or week, perhaps depending on the volume of telephone calls. An unlimited number of time bands may be specified, one on each row of the grid.

Band Start Time

Specifies the start time for the band, where 00:00 is midnight. The start times should be arranged in increasing order by day. ComCap has default start times of 09:00 and 17:00 for weekdays, and 00:00 for weekends.

Valid Days

Specifies the day of the week on which this time band is valid, or weekdays, weekends or every day. Clicking or typing in the Valid Day column will cause a drop down arrow to appear, allowing a list to be dropped down with the days of the week, weekdays and weekend options. Please be careful not to allow multiple choices, such as Monday and Weekdays, this is not validated and the first found will be used. Any other day setting overrides every day, so you can not mix it with specific days.

Warn Minutes

Specifies the warning time in minutes after which the specified action will occur if no data is received by the channel. This period will be dependent entirely on the frequency of the type of data being received, and needs to be set sufficiently high to avoid unnecessary warnings, up to a maximum of 9,999 minutes (almost one week).

Default Periods

The default periods are 09:00 Weekdays with a warning after 5 minutes, 17:00 Weekdays 0 minutes (no checking) and 00:00 Weekends 0 minutes (no checking), which means that the data loss warning is only enabled 9am to 5pm Monday to Friday.

Test Button

A test button is provided that allows testing of periods for any specific date and time, to ensure there are no conflicts.

Restart Capture

Ticking this option will cause capture to be restarted in case Windows has failed in some way. Beware this may cause loss of data from other active channels since all are restarted together.

Send Alert

Ticking this option causes a data loss alert to be triggered.

3.8 Database

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies Database settings.

The screenshot shows the 'Settings for Sonicwall, Protocol UDP Server' dialog box with the 'Database' tab selected. The 'Database Type' is set to 'ADO (OLE DB/ODBC)'. The 'Specify Database' button is visible. The 'Stored Procedure' is set to 'capture_sonicwall_put2'. The 'Database' field shows 'comcap using SQLOLEDB.1 from Server PC18\MSSQL2008'. Under 'How to Add Records', 'Stored Procedure' is selected. Under 'Extra Columns', 'Update serial_nr Column' and 'Update event_time Column' are checked. The 'Connection Timeout (secs)' is set to 10, 'Database Inactivity (secs, zero leave open)' is set to 0, and 'Maximum Rows to Buffer before Pausing Capture' is set to 500. Several checkboxes are present: 'Alert for Database Problems' (checked), 'Immediate Pause for Database Problems' (unchecked), 'Escape Backslash (MySQL)' (checked), 'No Pause for Full Buffer (Ignore Data)' (checked), 'Ignore Records That Cause Error' (unchecked), and 'Save/Restore Buffered Rows to Disk' (checked). The 'OK', 'Apply', 'Cancel', and 'Help' buttons are at the bottom.

Database Support and Requirements

ComCap allows captured data to be saved in a database table. Currently only databases supported by Microsoft Data Access Components (MDAC or ADO) may be used, with testing using Microsoft SQL Servers 2000, 2005 and 2008, Sun MySQL 5.1 and IBM DB2 v9.7. In theory Access (Jet) could be used, but since SQL Server 2005 and 2008 Express are free (database limited to 4 gigs), there seems little point. MDAC may be used with any database with an ODBC or OLE DB Provider driver, however not all drivers provide the same level of support and may not be usable with ComCap. Please check the help page for the specific databases for recommended drivers and data link set-up:

- Microsoft SQL Server
- Sun MySQL
- IBM DB2

For Windows 2000, MDAC 2.8 SP1 (free download from Microsoft [MDAC Downloads](#)) should be installed before attempting to configure database support in ComCap. Windows XP SP2, Windows 2003, Vista, 2008 and 7 include MDAC as part of the core operating system.

ComCap also includes Sample Database SQL scripts to create empty tables and stored procedures, to illustrate database capture.

Background Service

If ComCap is configured to capture to a database using the Background Service, the service must be set-up with a local PC account name and password, see Capture Logging.

Database Type

This option selects the technology that ComCap uses for database access, currently only ADO using Microsoft Data Access Components (MDAC) with OLE DB or ODBC drivers. Future ComCap releases may support more efficient database access technology.

Specify Database

The Specify Database Button displays the MDAC Data Link Properties dialog. From there, first select the OLE DB provider, usually SQL Server but perhaps ODBC or Jet. On the Connection tab, select or enter a SQL server name (it may be available in the drop down box, but may need a UNC name entered), then specify authentication to logon to the database, and finally the actual database to be used. Click Test Connection to make sure SQL is working, then OK. ComCap will then open the database and the details will be displayed to confirm it's all working OK. More than one channel may capture data to the same database table, but each channel will use a separate link, to allow saving in parallel. More details for specific databases may be found at:

- Microsoft SQL Server
- Sun MySQL
- IBM DB2

Note the database and optionally stored procedure to add records must already exist before ComCap can be configured.

How to Add Records

This option determines how records will be added to the database:

Insert into Table	A Database Table selection field will appear, with a drop down box listing all the tables in the database, from which one should be selected. ComCap will use the SQL INSERT statement to add records directly into this table, using the columns specified in the Data Format.
-------------------	---

Stored Procedure	A Stored Procedure selection field will appear, with a drop down box listing all the stored procedure in the database, from which one the one created for this channel should be selected. Note that not all databases support stored procedures.
------------------	---

Extra Columns

ComCap supports two special database columns, `serial_nr` and `event_time` which may be completed automatically by ComCap. This option has two tick boxes to specify the database table has one or both of these columns as columns. In the case of stored procedure, these columns must be the first one or two parameters, in that order. If these extra columns are used, don't attempt to put data into them using the Data Format. More details about these extra columns may be found at Sample Database SQL scripts.

Connection Timeout

This option specifies the database connection timeout in seconds, defaulting to 30 seconds, with a minimum of 10 seconds. Generally keep a low timeout since this also restricts the frequency when repeat attempts may be made to reconnect to the database. The maximum timeout is 120 seconds.

Database Inactivity

This option allows the database connection to be closed after an idle period in seconds with no new data captured, up to a maximum of 600 seconds. The database will be automatically re-opened when new data arrives. Setting zero seconds will leave the database connection open continually, which is normally perfectly OK.

Maximum Rows to Buffer Before Pausing Capture

When a data row can not be written to the database immediately, it is automatically buffered so it can be written later. This can happen because capture is happening faster than data can be written to the database, which may be limited to only 50 to 150 rows maximum per second, or due to other database problems or errors. The maximum number of rows that may be buffered can be configured from 50 to 99,999. When this maximum number of rows is exceeded, capture may be automatically paused until the buffered rows are written successfully, or subsequent rows are ignored (but still written to the capture log file) depending on the option 'No Pause for Full Buffer (Ignore Data)' see below. Note that rows are buffered in memory, so this must be sufficient for the data expected to be buffered. If ComCap is exited before the buffered rows are written, the rows are lost, unless 'Save/Restore Buffered Rows to Disk' is enabled, see below. Another way to reduce the load on the database is 'Ignore Too Many Lines' option on the Records tab, which allows a gap in fractions of a second to be specified between lines, which may be useful to reduce the amount of data captured from devices sending continuous streams, such as GPS locators or environmental sensors.

Alert for Database Problems

Ticking this option will cause an alert to be triggered for database problems, specifically if the database can not be opened.

Immediate Pause for Database Problems

Temporary database problems are almost inevitable, perhaps due to communication problems or the database server being rebooted, so ComCap has various means of coping with them. ComCap is able to temporarily buffer data that can not be written to the database, according to the Maximum Rows to Buffer Before Pausing Capture option above. Sometimes, the remote data source may be able to buffer data more safely, so ticking this option will immediately pause capture if the database becomes unavailable due to an error. Attempts are made to restart capture and re-open the database according to Delay Before Restart seconds on the General tab and when successful any buffered rows are written. This setting also effects how capture is started, normally data capture starts immediately while the database is still being opened with data temporarily cached and written once the database is available, unless this option is ticked. Beware this may cause some confusion when initially testing database capture, unless the errors in the information log are seen.

Escape Backslash (MySQL)

Ticking this option avoids a problem with old versions of MySQL that treat the backslash character as the first of an escape sequence (ie \f is form feed). This option sends \ as \\ so MySQL saves it as \ instead of reporting a syntax error. Newer versions of MySQL have a configuration option to disable escape sequences.

No Pause for Full Buffer (Ignore Data)

Ticking this option allows capture to log files to continue even if a database is unavailable, or if the capture rate is so fast that a database can not keep up. This works in conjunction with 'Maximum Rows to Buffer before Pausing Capture' so that once the limit is reached subsequent rows are ignored instead of being buffered, but are still written to the capture log file. This feature is primarily designed to support capture applications that regularly update the same information, such as global positioning satellite data where a vehicle position need not be recorded every second. The number of rows not written to the database is logged similarly to the following:

```
Database Rows Added: 3,990, Database Errors 16, Skipped 113
```

and also reported in the tray application in brackets after the number of DB rows. Note the minimum number of rows that may be buffered is 50, which is required for normal operation where 10 or more rows may be captured as a burst which may be faster than they can be written to SQL.

Ignore Records That Cause Error

Ticking this option prevents a row being buffered when a SQL error occurs and the database is closed and re-opened to try and clear the error. This is primarily intended to overcome syntax and duplicate key errors where the database can not write a specific row of data and will get stuck in a repeating loop trying to write the same row again and again. Unfortunately, due to the widely varying error responses from different SQL databases, this feature might cause a row to be lost if the network is lost or the SQL server simply stopped while a row is being written.

Save/Restore Buffered Rows to Disk

ComCap always buffers rows in memory that can not be written to a database due to network errors, and updates the database as soon as it becomes available again. If this option is not used, buffered rows are lost forever if ComCap is exited before the database connection has been successfully restored. With this option, the buffered rows are saved to a file (in the same directory as the config files) when capture is stopped (but not paused) and restored to the buffer when capture is started again. The actual file name is reported in the info log file. Beware this may cause a problem if the database format is changed so the buffered rows are no longer valid, so just delete the file.

Recovery Functionality for Old Data

Database problems are unfortunately inevitable. The database server might get rebooted by Windows Update (despite all settings saying don't reboot), network issues could break the connection, and many other reasons may cause captured data to fail to be written to the database. ComCap therefore provides a recovery feature Database from Log, accessed from the right click menu in the main window, which allows previously captured data to be added to the database, from an old Capture Log.

When clicked, a File Open dialog allows the capture log to be selected. A dialog then warns 'Confirm Read Capture Log and Add X Rows to Database for (channel)?' If OK is clicked, all lines in the Capture Log will be added to the database, using the settings for that channel. If the extra serial_nr column is used this will have a normal increment Serial Number, but the event_time column will reflect the time the row was added, not when it was captured. This is one reason why it's better to add these extra columns to the capture log, so they can be imported accurately later. To avoid duplicate rows, it may be necessary to manually edit a copy of the capture log to remove any lines successfully added to the database.

This recovery feature can also be used for testing database Data Format settings, without needing to wait for new data to be captured.

3.9 Data Format

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies the Data Format for captured data, where separate columns need to be identified to be saved to database columns or for filtering and alerts. The appearance of the grid depends upon the Data Format on the General tab.

Grid Control Buttons

There are seven buttons used to manipulate the Data Format grid, left to right:

Move Row Up	Used to move the selected row higher up the grid.
Move Row Down	Used to move the selected row lower down the grid.
New Columns from Database Table	Used to read the selected database table definitions or stored procedure parameters, and fill the grid with Column Name, Column Type, Column Length and if it's Nullable. Note that clicking the New Columns button clears any user data entered in the grid
Open Sample Log	Display a file open dialog allowing a Capture Log with sample data to be opened
Sample Log Up	Displays and parses the previous Capture Log line.
Sample Log Down	Displays and parses the next Capture Log line
Reparse Sample Data	Parses the current Capture Log line, usually after the location of the data columns has been changed

If the grid is empty, or if the database table or stored procedure have been changed, click the New Columns from Table button to fill the grid.

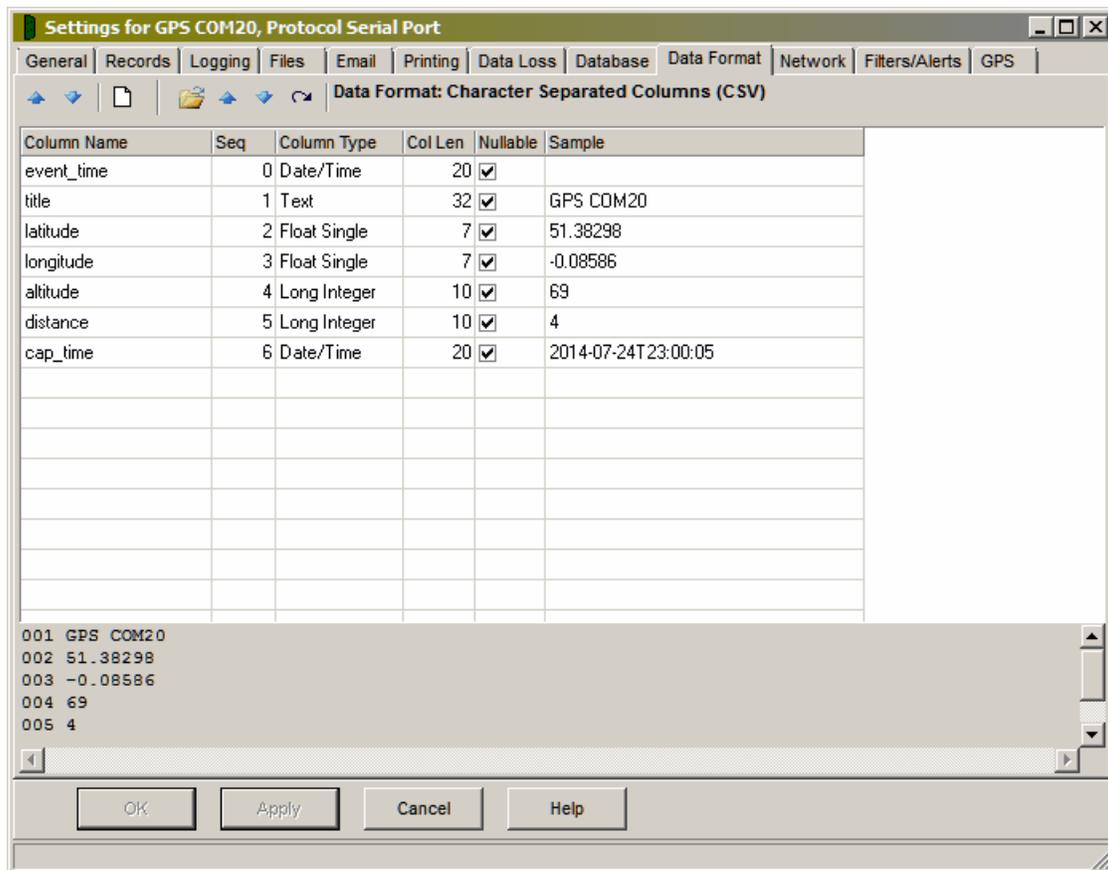
To ease creation of the Data Format, captured data is dynamically parsed in exactly the way it would be when been added to a database table, so you can easily check how the format you specify will identify data columns for the database. The sample data is taken from anything showing in the main capture window, or a specific Sample Log may be opened. The current sample data row is shown both in the grid, and below the grid in different formats.

To edit the columns in the Data Format grid, click on the required box and an edit control of some sort will appear, perhaps a drop down box arrow, an edit field or numeric up/down arrows. Once the edit is complete, click on another box to ensure the edit is saved, losing focus from the grid causes the last edit to be cancelled.

Data Format: Fixed Width Columns

displayed in the grid Sample column, according to the current Data Positions and Lengths. If a Data Position is changed, the Reparse button should be clicked to refresh the Sample column. The Sample columns show Invalid Column if the data can not be parsed.

Data Format: Character Separated Columns (CSV)



For Data Format: Character Separated Columns (CSV), the grid shows four fixed columns, and one user editable column.

Column Name, Column Type, Column Length and Nullable

These columns are pre-filled from the table definition or stored procedure parameters and can not be changed. If the table or SP is changed, click the New Columns from Database button to refresh them, but beware Sequence will be cleared. The Column Type column shows the definition of that column, any attempt to write alphanumeric data to a numeric column will cause a SQL error. Currently, ComCap lets the ADO or the stored procedure raise errors for data type incompatibilities and captured data is not actually validated (except for blanks, see below).

Sequence Number

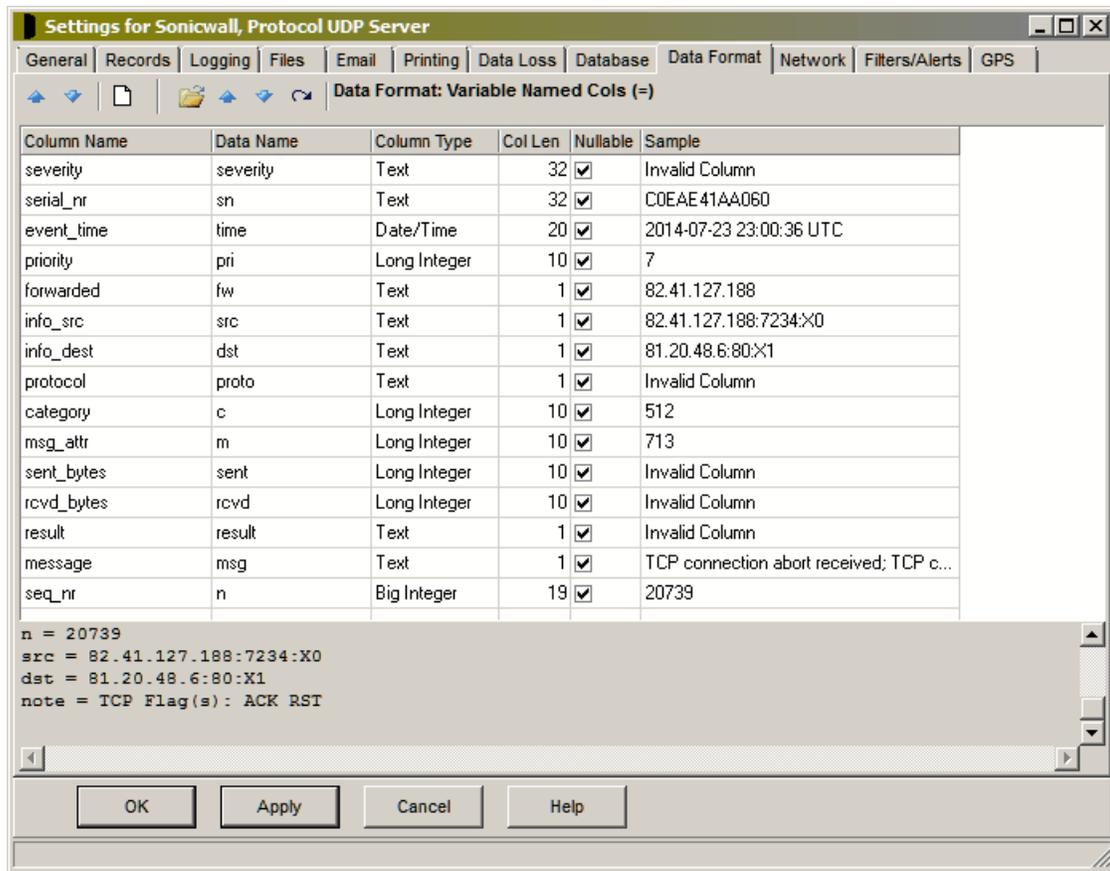
Character separated columns are identified by simply counting the separators. The Sequence Number column is editable, and is used to define the number for each database column. The first Sequence Number is one. If a database column or parameter is to be left blank, set the Sequence Number to 0. If the column data length is longer than the Column Length, it will be truncated. All data is trimmed to remove leading and trailing spaces.

Blank data often causes trouble. If a column contains all spaces, it is converted to a NULL for Date/Time Column Types or if the table allows nulls in the column. Because all stored procedure parameters are Nullable, numeric values are passed as 0 and text as blank.

Sample Data

The panel below the grid shows the current Sample Data line displayed as one row per column, preceded by the Sequence Number. The Sample Log Up and Down buttons may be used to select different lines of Sample Data. The Sample Data line is automatically parsed and the identified columns displayed in the grid Sample column, according to the current Sequence Numbers. If a Sequence Number is changed, the Reparse button should be clicked to refresh the Sample column. The Sample columns show Invalid Column if the data can not be parsed.

Data Format: Variable Named Columns (=)



Specifying the data format 'variable named columns' is similar, except the data column name is specified instead of the sequence. The sample data is parsed to separate the data names from the data values. Note spaces are not allowed in the data names. Any named columns not found are treated as blank or null.

For Data Format: Variable Named Columns (=), the grid shows four fixed columns, and one user editable column.

Column Name, Column Type, Column Length and Nullable

These columns are pre-filled from the table definition or stored procedure parameters and can not be changed. If the table or SP is changed, click the New Columns from Database button to refresh them, but beware Sequence will be cleared. The Column Type column shows the definition of that column, any attempt to write alphanumeric data to a numeric column will cause a SQL error. Currently, ComCap lets the ADO or the stored procedure raise errors for data type incompatibilities and captured

data is not actually validated (except for blanks, see below).

Data Name

Variable Named Columns are identified by their names, which may or may not be the same as the database Column Names. The Data Name column is editable, and is used to define the name for each database column. If a database column or parameter is to be left blank, leave Data Name blank. If the column data length is longer than the Column Length, it will be truncated. All data is trimmed to remove leading and trailing spaces.

Blank data often causes trouble. If a column contains all spaces, it is converted to a NULL for Date/Time Column Types or if the table allows nulls in the column. Because all stored procedure parameters are Nullable, numeric values are passed as 0 and text as blank.

Sample Data

The panel below the grid shows the current Sample Data line displayed as one row per column, preceded by the Data Name. The Sample Log Up and Down buttons may be used to select different lines of Sample Data. The Sample Data line is automatically parsed and the identified columns displayed in the grid Sample column, according to the current Data Names. If a Data Name is changed, the Reparse button should be clicked to refresh the Sample column. The Sample columns show Invalid Column if the data can not be parsed. This is quite likely with Variable Named Data where only the columns actually used are presented.

3.10 Network

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies Echo UDP (Syslog), TCP Server and TCP Client settings.

Settings for TCP Srv 1469/1 SSL, Protocol TCP Server

General Records Logging Files Email Printing Data Loss Database Data Format Network Filters/Alerts GPS

Echo to Network

Add Syslog Headers

None

Priority only, ie <14>

Priority, Time and Host

Add CRLF End of Line (UDP only)

Actual Priority <14>

Facility Priority user-level messages

Severity Priority Informational: informational messages

Echo to Remote - Remote Address

Remote IP Address or Host 0.0.0.0

Remote IP Port 514

Wait Seconds 5

Retry Attempts 20

Echo to Remote - Local Address

Local IP Address 0.0.0.0

Local IP Port 1468 Port 0 is Random

Network Performance

Capture TCP/UDP Buffer Size (KB) 8

Echo TCP/UDP Buffer Size (KB) 8

SSL/TLS - Transport Layer Security

SSL/TLS for Capture SSL/TLS for Echo

SSL Server Certificate C:\ProgramData\Magenta-Systems\ComCap4\Certificates\c

SSL Server Private Key C:\ProgramData\Magenta-Systems\ComCap4\Certificates\c

SSL Certificate Intermediates

Client Validate Server Certificate

Create SSL Certificate

OK Apply Cancel Help

SSL Security

In addition to SSL settings on this tab, see Common Settings, Common where SSL security settings are specified for all TCP Clients and TCP Servers, these settings may prevent connections to lower or higher security clients or servers.

Echo to Network Overview

ComCap can echo or proxy any captured data to the network, using UDP (syslog), TCP Server or TCP Client protocols, which are detailed in the Networking Tutorial. Effectively, this allows ComCap to convert serial data to network protocols, to be captured on remote PCs for viewing or redundancy.

Using TCP Server, data may be echoed to a maximum of five remote PCs (using TCP Client) that connect to the Local IP Address and Port. Connections are refused for connections in excess of five. TCP Client and UDP need a remote IP address to be specified, and are thus limited to a single remote PC.

TCP/IP Client may also be used for 'IP Printing' using port 9100. Many network printing will accept print data on TCP/IP port 9100.

Add Syslog Headers, Priority (Facility/Severity) Text

Specifies that syslog headers should be added to echoed lines:

Priority Only	<14> is a Priority value where the first 7 bits of the number are a facility code and the last 3 bits are severity, selected from the drop down Facility Priority and Severity Priority lists. The Actual Priority text that will be added is show,
Priority, Time and Host	Also add the time and host and program name, similar in format to: <14>Mar 25 17:03:04 PC09 ComCap

Note that Syslog headers are normally only used with UDP.

Add CRLF End of Line (UDP only)

This tick box specifies whether echoed UDP lines should have CRLF added to the end of each captured line. The TCP protocols always have CRLF added for end of line.

Echo to Remote - Remote IP Address and Port, Retry Attempts, Wait Seconds

For UDP and TCP Client, these fields allow the Remote IP Address and Remote IP Port to be specified, to which captured data will be echoed. They may not left blank or zeros. For UDP Syslog, the port is usually 514, for TCP Client it should be above 1,024, the same as that of the remote TCP Server which is listening.

UDP is an unreliable protocol where data is sent blind with no confirmation it has been received by the remote computer, which might not even exist.

TCP Client is reliable, and also needs Retry Attempts and Wait Seconds to be specified, so that connection attempts are repeated if they fail. Setting Retry Attempts to zero causes indefinite attempts to be performed.

Echo to Remote - Local IP Address and Port

For TCP Server, this is the Local IP Address for server, selected from a drop down box, usually 0.0.0.0 and the IP Port on which the server will listen for remote TCP clients, usually higher than 1,024. For UDP and TCP Client, the IP address should usually be 0.0.0.0 and the port set to zero so that Windows selects port randomly. A fixed port may be used to identify multiple UDP or TCP sessions

from the same PC, but when a connection is lost there may be delay of several minutes before the port can be re-used.

SSL/TLS for Capture

If ticked, SSL/TLS will be enabled for capture with TCP Client or TCP Server.

SSL/TLS for Echo

If ticked, SSL/TLS will be enabled for echo using TCP Client or TCP Server.

SSL Server Certificate

For TCP Server for capture or echo, a SSL Server Certificate X509 PEM file must be specified, see SSL/TLS and Certificates. Will default to the certificate specified in Common Settings, Common. If SSL is enabled for both capture and echo, both with TCP Server, the same certificate will be used for both.

SSL Server Private Key

For TCP Server for capture or echo, a SSL Server Private Key X509 PEM file must be specified, see SSL/TLS and Certificates. Will default to the certificate specified in Common Settings, Common.

Client Validate Server Certificate

For TCP Client for capture or echo, specifies the remote SSL server certificate should be checked according to the settings in Common Settings, Common. This is optional and does

Client Validate Server Certificate

For TCP Client for capture or echo, specifies the remote SSL server certificate should be checked according to the settings in Common Settings, Common. This is optional and does not prevent SSL being used, it may slow down connection set-up and potentially cause errors that prevent capture.

Create SSL Certificate

Clicking this button brings up a new window allowing either a certificate request for a certificate authority to be created, or a self signed certificate see SSL/TLS and Certificates.

Network Performance Overview

Added a new setting to improve performance when capturing high speed TCP and UDP traffic. TCP/UDP uses memory buffers to temporarily save received or sent data before ComCap is able to process it, which default to 8 Kbytes. With TCP, if data is not extracted from the buffer, the speed at which data is received will slow down, but with UDP received data is simply lost since there are no handshaking packets to confirm data needs to be delayed or resent. It should only be necessary to increase the capture buffer size if a lot of data is being received each second, maybe 16K/sec or more, or if the PC is very slow or has other CPU intensive applications so that ComCap can not get the CPU it needs. Note these new settings only appear for channels actually listening or sending data, not filter or merge channels.

Capture TCP/UDP Buffer Size (KB)

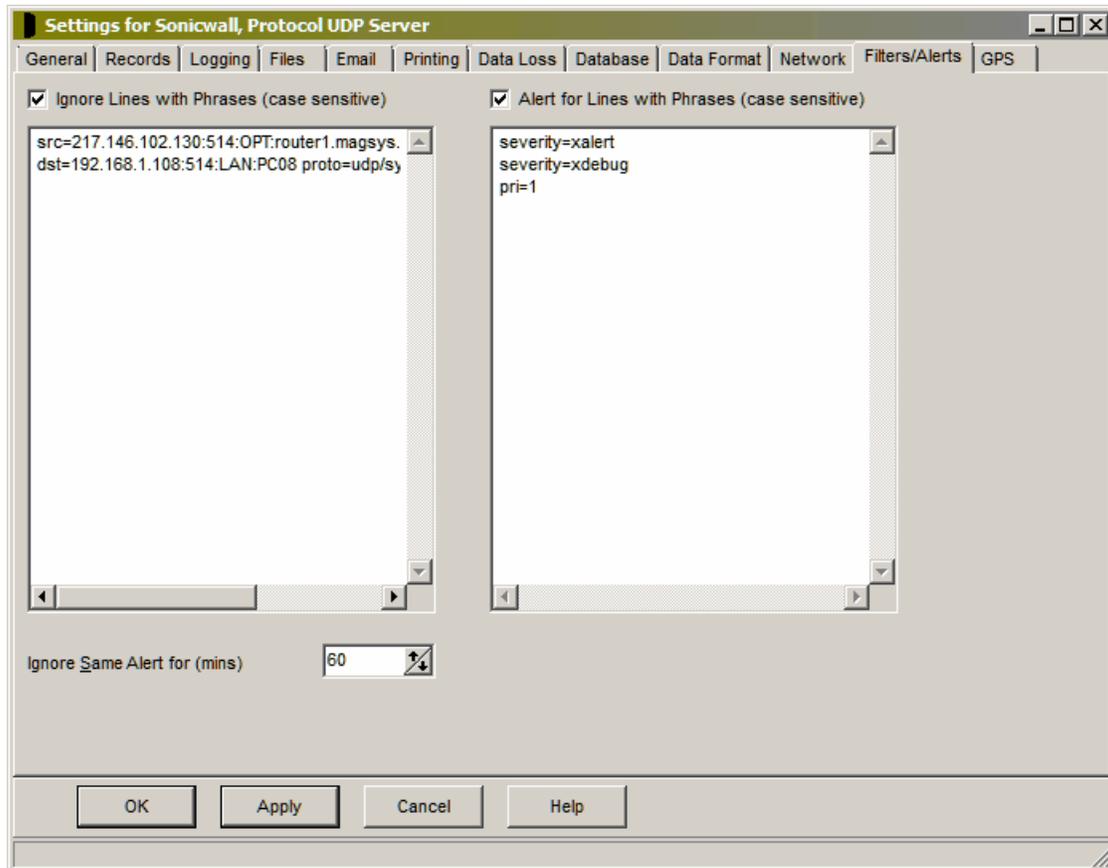
Allows the size of the TCP/UDP buffer uses to capture data to be increased from the default of 8 which means 8KB (8,192 bytes). Typically 32 or 64 should be sufficient for the large buffer. This field only appears for listening channels, not those filtered or merged from other channels.

Echo TCP/UDP Buffer Size (KB)

Allows the size of the TCP/UDP buffer uses to echo data to be increased from the default of 8 which means 8KB (8,192 bytes). Typically 32 or 64 should be sufficient for the large buffer. This field only appears if Echo has been specified for this channel.

3.11 Filters and Alerts

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies Filter and Alert information.



Options on this tab search captured data, perform filtering and trigger alerts. Note that searching is on a single line, a phrase that is split between two lines will not be found. Also searches are case sensitive, so multiple phrases will need to be entered to test for case permutations.

Ignore Lines with Phrases (case sensitive)

Ticking this option causes each captured line to be checked against one or more phrases (entered one line at a time), and ignored if any are found. The ignored line is not saved or shown in the log window, but ComCap counts how many lines are ignored due to these various filters and checks and shows the total in the status bar and hourly in the Information Log.

Alert for Lines with Phrases (case sensitive)

Ticking this option causes each captured line to be checked against one or more phrases (entered one line at a time), with an alert being triggered if any are matched. The alert may be a pop-up window, email or SMS message, as configured in Common Settings, Alerts, and will include the channel name and the captured line.

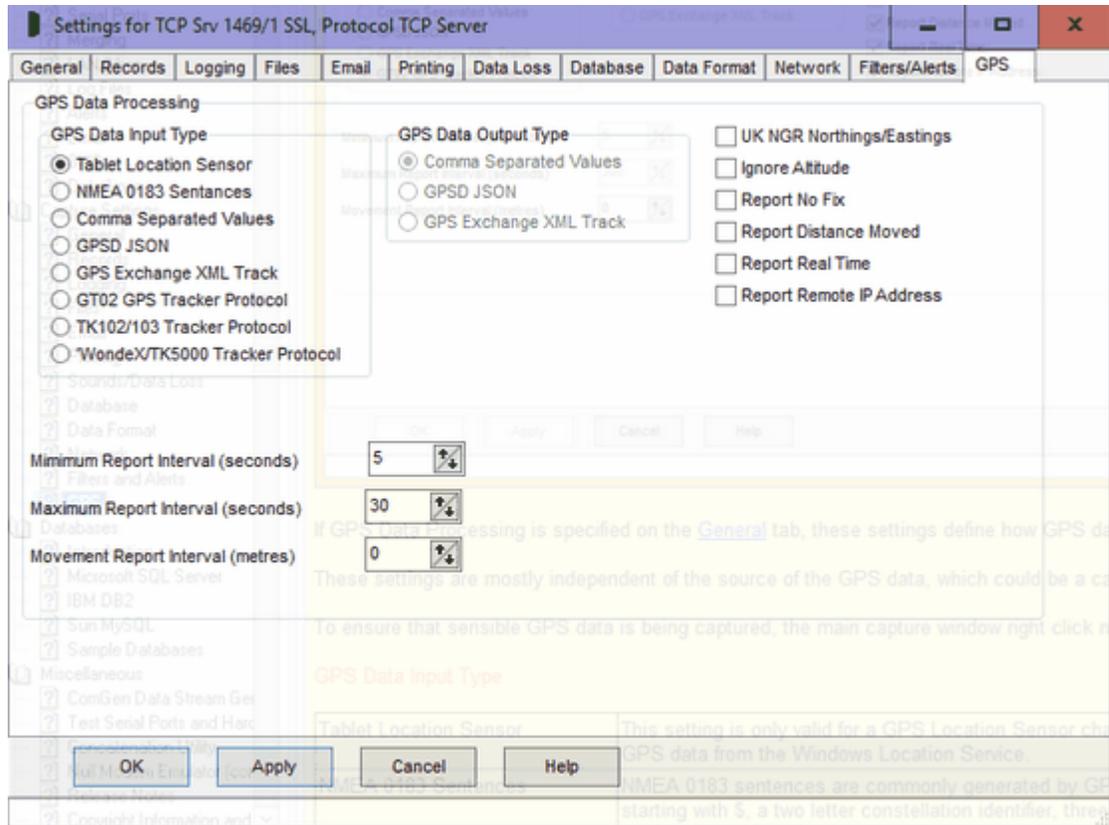
Ignore Same Alert for (mins)

This option works in conjunction with 'Alert for Lines with Phrases' preventing the same alert being sent again until the specified period in minutes is reached. If more than one alert filter is specified, each filter will still trigger an alert the first time it is detected. This will avoid too many emails or SMS

messages being sent when the same alert is continually repeated.

3.12 GPS

Capture Settings are set-up separately for each capture channel. Once these settings have been specified, OK or Apply should be clicked. This tab specifies GPS Data Processing information. .



If GPS Data Processing is specified on the General tab, these settings define how GPS data should be processed.

These settings are mostly independent of the source of the GPS data, which could be a captured serial port of a network protocol.

To ensure that sensible GPS data is being captured, the main capture window right click menu has an option View Map Window that displays the ComCap Map window and shows a location track.

GPS Data Input Type

Tablet Location Sensor	This setting is only valid for a GPS Location Sensor channel, that automatically processes GPS data from the Windows Location Service.
------------------------	--

NMEA 0183 Sentences	<p>NMEA 0183 sentences are commonly generated by GPS receivers, these are text lines starting with \$, a two letter constellation identifier, three letter command, several arguments and ending with a checksum to allow corrupted sentences to be skipped, ie:</p> <pre>\$GPRMC,112500.044,A,5122.9867,N,00005.1107,W,12.77,100.45,290714,,A*47 \$GPGGA,112501.044,5122.9900,N,00005.1017,W,1,03,2.6,49.5,M,47.0,M,,0000*72 \$GPGSA,A,2,25,31,14,,,,,,,,,4.1,2.6,3.2*33 \$GPGSV,2,1,08,14,20,221,12,25,67,080,18,31,53,296,29,29,68,192,*7D \$GPGSV,2,2,08,12,29,088,,02,28,056,,09,20,147,,06,06,026,*7F</pre> <p>NMEA 0183 sentences processed are: GGA, GSA, GSV, RMC, GLL and VTG, others are ignored.</p>
Comma Separated Values	Allows capture of the ComCap GPS CSV format described below, perhaps echoed from another copy of ComCap. Main advantage is access to the ComCap Map Window.
GPSD JSON	GPSD is a Linux application that accepts input from numerous GPS devices and produced a consistent output stream using JSON formatting. Not yet supported, unable to test.
GPS Exchange XML Track	GPS Exchange XML Track is an XML format describing a GPS track. Not yet supported, unable to test.
GT02 GPS Tracker Protocol	<p>GPS Tracker Communications Protocol GT02 is used by Concox TR02 vehicle trackers that combine GPS, GPRS and GSM is a small 12V driven package designed for mounting in vehicles. This device is programmed by SMS messages and returns location and movement information to a TCP/IP Server. To keep mobile data cost low, it only sends location during movement, although does return periodic handshakes while connected. ComCap needs one TCP/IP Server channel configured for each simultaneous device that will connect, all with the same local IP and port, then Channel Settings should have 'GPS Data Processing' ticked with input type of 'GTO2 GPS Tracker Protocol' selected, tick 'No Altitude', 'Report No Fix' and 'Report Distance Moved'. On the Records tab, set Line or Record End to CR/LF, on the Logging tab tick 'Log Raw Data'. Note the GT02 reports the time a fix was taken, not when it was transmitted. New fixes may be cached by the tracker if not online and sent together when an internet connection is re-established, or an old fix may be sent when a new connection is made.</p>
TK102/103 Tracker Protocol	The Xenun TK102/103 format is essentially the NMEA RMC sentence, preceded by date/time and mobile number, followed by useful stuff from other NMEA sentences like satellite count, mobile IMEI and cell station stuff. This data format is TCP/IP server only.
WondeX/TK5000 Tracker Protocol	The WondeX/TK5000 format used by VT-10, VT300 and other devices is a simple format with IMEI, time, co-ordinates, speed and direction. This data format is TCP/IP server only.

The TK102/103 and /TK5000 are also used by an Android application MyLiveTracker by Michael Skerwiderski available free from Google Store: <https://play.google.com/store/apps/details?id=de.msk.mylivetracker.client.android> which allows a mobile devices to be tracked. Once the app is installed, go to Settings, Tracking, Server, and enter the public server address or domain name and port of the ComCap TCP/IP capture channel. In Protocol, set TK102 Emulator, Buffer 10 positions, Time Trigger will send location that often even if stationary, Distance Trigger sends location after so many metres movement, Close Connection after upload is safer, Finish Upload with Linefeed is good. No account is needed for simple protocols without HTTP. The click the large Tracking box and the runtime. location

and uploader boxes turn green, and ComCap should start showing GPS rows.

GPS Data Output Type

Comma Separated Values	Saves GPS data in ComCap GPS CSV format described below.
GPSD JSON	Saves GPS data in GPSD JSON format. Not yet supported, unable to test.
GPS Exchange XML Track	Saved GPS data in GPS Exchange XML Track format. Not yet supported, unable to test.

UK NGR Northings/Eastings

For the UK only, degrees may be replaced by UK NGR Northings/Eastings in simple metres, which allows easier calculations.

Ignore Altitude

If ticked, the Altitude column is ignored.

Report No Fix

If ticked, will periodically log that no fix is available, to distinguish from a missing GPS sensor.

Report Distance Moved

If ticked, distance moved between each fix in metres will be reported.

Report Real Time

If ticked, adds a real time stamp in local time when the record was captured, may be later than fix time

Report Remote IP Address

If ticked, adds the Remote TCP/IP address of the modem.

Minimum Report Interval

Specifies the minimum interval in seconds between reports. This is designed to reduce the volume of GPS data captured, where a report once a second is not necessary.

Maximum Report Interval

Specifies the maximum interval in seconds before an old report will be repeated if no reports have been made. This is designed so something is logged periodically if stationary.

Movement Report Interval

Specifies a movement distance in metres before a report will be made. This is designed to avoid logging while stationary.

ComCap GPS CSV Format

A typical captured line may look like:

```
"GPS Concox UK",533312,166660,0,0,8,8,"358899053800739",363, "2015-05-07T19:26:09", "2015-05-08T12:30:12", "212.183.128.151"
```

1	Channel Name	ComCap channel name
2	Latitude	Latitude in decimal degrees, positive or negative, or UK NGR Northings
3	Longitude	Longitude in decimal degrees, positive or negative, or UK NGR Eastings
4	Altitude	Altitude in metres - optional

5	Distance	Distance in metres since last report - optional
6	Speed	Speed in metres per second - only for GT02
7	Course/Direction	Course or direction in degrees
8	IMEI ID	Unique IMEI ID of the GSM modem - only for GT02
9	Packet sequence number	Packet sequence number, to allow check if records have been lost, note sequence numbers may wrap around - only for GT02
10	Fix time stamp	Fix time stamp of report from device, in ISO date and time format, note this may be UTC/GMT time, not local time and may be days old if the device has not moved.
11	Real time stamp	Real time stamp in local time when the record was captured, may be later than fix time - optional
12	Remote IP address	Remote TCP/IP address of modem - optional

GPS Testing

Most testing was with a GlobalSat BU-353-S4 USB GPS Receiver, a two inch diameter device with a roof magnet that presents as a Prolific serial port (a version with a real serial connector is also available), and the Concox TR02 vehicle tracker. Also tested were a battery operated GlobalSat BT-359 Bluetooth CoPilot GPS device (but Bluetooth serial ports are not always very reliable) and NMEA 0183 streaming from a Nexus 7 Android tablet.

GPS SQL Database Capture

To demonstrate saving GPS data to a SQL database, a Microsoft SQL Server table `capture_gps` will be found in `'newdb-mssql.sql'` and matching stored procedures to `'storedproc-mssql.sql'`. Data Format should be specified as Character Separated Columns (CSV), the database set-up with table `capture_gps` and stored procedure `capture_gps_put` which requires six of the columns listed above, and `event_time` to be ticked.

Part



4 Databases

4.1 Introduction

ComCap allows captured data to be saved in a database table.

Currently only databases supported by Microsoft Data Access Components (MDAC or ADO) may be used, with testing using Microsoft SQL Servers 2000, 2005 and 2008, Sun MySQL 5.1 and IBM DB2 v9.7.

In theory Access (Jet) could be used, but since SQL Server 2005 and 2008 Express are free (database limited to 4 gigs), there seems little point.

MDAC may be used with any database with an ODBC or OLE DB Provider driver, however not all drivers provide the same level of support and may not be usable with ComCap. Please check the help page for the specific databases for recommended drivers and data link set-up:

- Microsoft SQL Server
- Sun MySQL
- IBM DB2

For Windows 2000, MDAC 2.8 SP1 (free download from Microsoft [MDAC Downloads](#)) should be installed before attempting to configure database support in ComCap. Windows XP SP2, Windows 2003, Vista, 2008 and 7 include MDAC as part of the core operating system.

ComCap also includes Sample Database SQL scripts to create empty tables and stored procedures, to illustrate database capture.

A database needs to be specified separately for each capture channel, on the Capture Settings, Database tab. The columns to save and how to extract them from the captured data are defined on the Capture Settings, Data Format tab. For problem solving, Common Settings, Log Files has an Database Diagnostics tick box that specifies that extra database diagnostic messages should be written to the information log file.

ComCap can write to different databases for different channels.

Database Performance

ComCap has been successfully tested with one network channel capturing and writing 50 records per second to a database table using SQL Server 2005 (running on a separate computer), while 20 other channels were capturing more slowly and writing to different tables. Record are buffered in memory before being written, so if capture rate is briefly higher no records should be lost.

Serious SQL database issue with Windows 7 SP1 and Windows 2008 R2 SP1

Microsoft released service pack 1 for Windows 7 32-bit and 64-bit and Windows 2008 R2 during February 2011, and has introduced a serious SQL database issue in the Microsoft Data Access Components with all versions of ComCap prior to Release 4.9. If captured data is being saved to a database, for each written line three internal handles and some memory are no longer correctly released by a Microsoft database component, which causes a memory leak in ComCap. As more lines are written, more memory is leaked, causing a PC slow down and eventually ComCap, and perhaps the PC, will crash having run out of memory, probably once about 100,000 lines have been captured depending on PC resources.

Note this database problem does not happen on the original versions of Windows 7 or Windows 2008 R2, or any other earlier versions of Windows, but was probably introduced by Microsoft hotfix KB983246 which fixed a different deadlock issue that could cause ComCap to hang, and which is

available for Windows XP and later. So if this hotfix is installed, the same memory leak may be introduced.

The issue may be seen in SP1 with ComCap running by opening Task Manager, on the Processes tab Select Columns, Memory Working Set and Handles, and for process comcap4.exe these will be seen to be increasing each time a line is written to the database. ComCap will normally be using a few hundred handles depending on configuration, anything more than 1,000 is unexpected. Also note that ComCap will be very slow to stop when handles are being leaked, during testing it became non-responsive for 10 minutes as 180,000 handles were released. This Microsoft database component has been widely used by other Windows applications for 10 years, which may also be effected after SP1 is installed if they use the same ExecuteComplete database event as ComCap.

This database issue was reported in March 2011 to Microsoft at <http://social.msdn.microsoft.com/Forums/en-PH/sqldataaccess/thread/68e23681-f6b5-4ed5-b963-e63e34eeac2f> where it has been reproduced by Microsoft and other developers, the cause determined and a fix discussed in October 2011 at <http://blogs.msdn.com/b/psssql/archive/2011/10/03/yes-we-made-a-mistake-and-are-finally-going-to-fix-it.aspx>.

The bug was been fixed in the first beta of Windows 8, and for Windows 7 and 2008 R2 at <http://support.microsoft.com/kb/2640696> with a hotfix in February 2012, which should also be included in service pack 2 in 2012 or 2013. If the hotfix is installed, when ComCap starts it will report 'Msado15.dll version 6.1.7601.17761 (win7sp1_gdr.120112-1636)' in the info log, the fault version says 'version 6.1.7601.17514'.

ComCap Release 4.9 and later fix this problem by no longer using the faulty event and should also resolve possible longer term rare reports of ComCap locking up during database updates in Windows XP and 2003. Any ComCap database users with 4.8 or earlier are strongly recommended to upgrade to 4.9 or later or install the KB2640696 fix.

4.2 Microsoft SQL Server

ComCap has been tested with Microsoft SQL Server version 2005, 2008, 2008 R2 and 2012, both standard and express editions. There are no differences between set-up and data capture for these various versions. While SQL Server may be installed on the same PC as ComCap, for important applications a dedicated server is better.

Microsoft Data Access Components (MDAC or ADO) must be installed, which are standard with Windows 2003 and later.

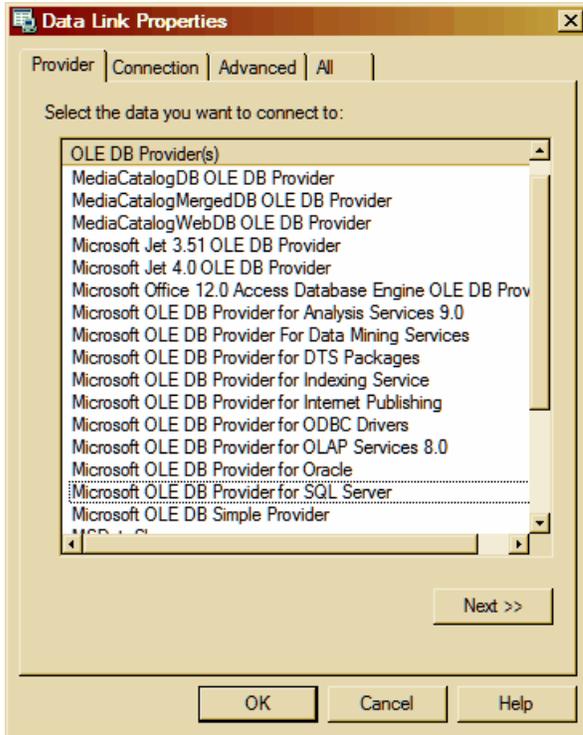
Sample Database Tables

The database table to which ComCap data will be written must be created before ComCap can be configured, and the database must be running.

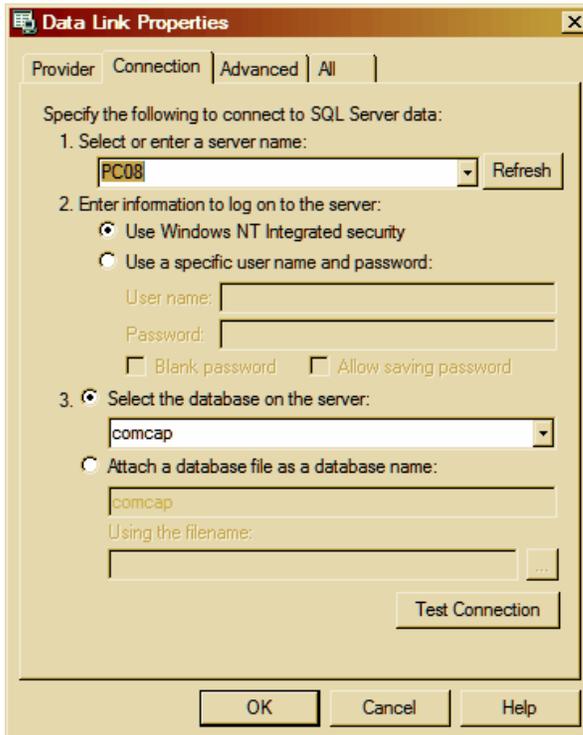
ComCap includes Sample Database SQL scripts to create empty tables and stored procedures, for Microsoft SQL Server these are in the two files `newdb-mssql.sql` and `storedproc-mssql.sql`. One of the Microsoft tools may be used to run the scripts into SQL server, such as SQL Server Management Studio or Universal SQL Editor is recommended. Then open the `newdb-mssql.sql` file and change the `FILENAME` statements with disk paths for the database data and log files to those for the SQL server, then Run all statements into SQL. Assuming there are no errors, open `storedproc-mssql.sql` and Run that in to add the stored procedures. Beware that running in `newdb-mssql.sql` more than once will delete any data already captured by first dropping the old tables, before it creates fresh empty tables.

Setting Up a Database Connection

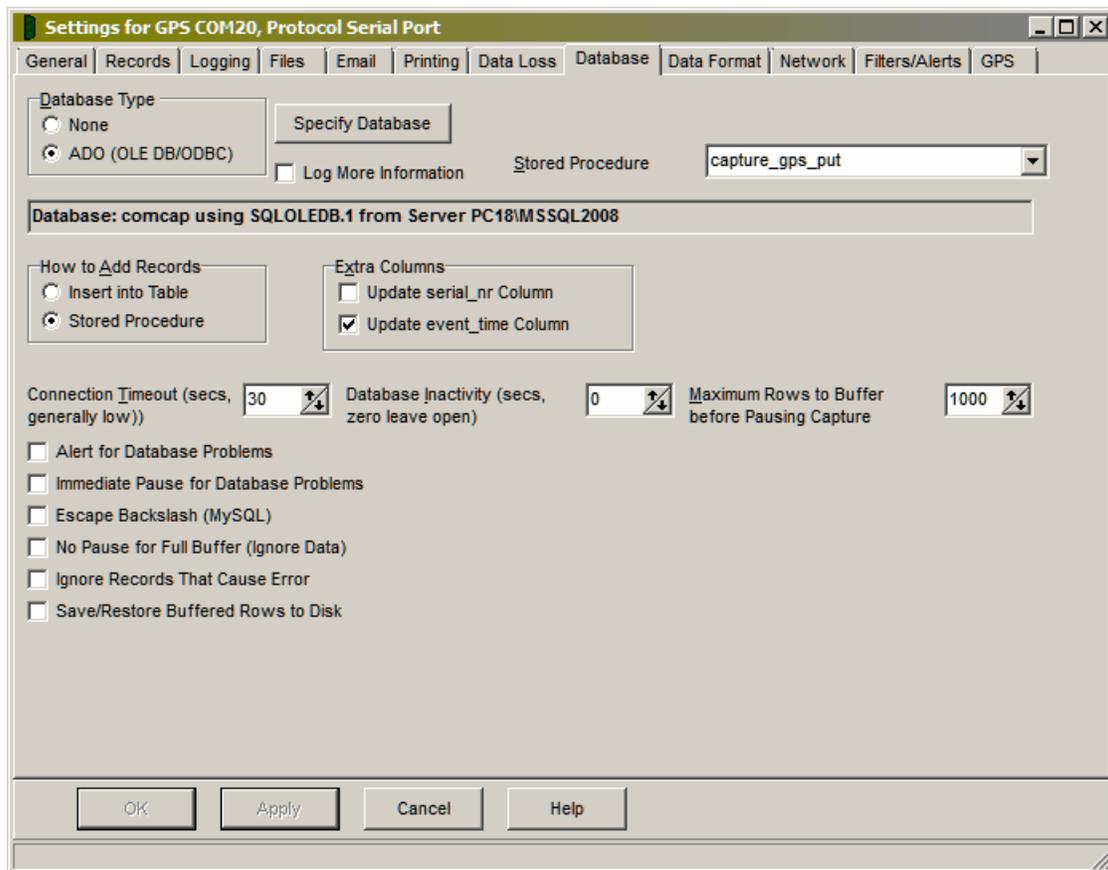
On the Capture Settings, Database tab, choose Database Type as ADO, then click the Specify Database button displays the MDAC Data Link Properties dialog, showing a list of installed data providers:



From the provider list, select Microsoft OLE DB Provider for SQL Server, and click Next>>:.



On the Connection tab, select or enter a SQL server name (it may be available in the drop down box, but may need a UNC path or IP address entered), then specify authentication to logon to the database, and finally the actual database to be used. Click Test Connection to make sure SQL is working, then OK.



ComCap will then open the database and the details will be displayed to confirm it's all working OK. ComCap can either insert data directly into a table, or pass data to a stored procedure that may manipulate the data and insert it into one or more tables. When you choose 'How to Add Records', a list of either SQL Tables or Stored Procedures will appear, from which one should be chosen. The list of stored procedures will include lots beginning sp_ but these should be ignored. How the data is chosen for the database is specified on the Data Format tab. Other settings on this tab are detailed at Database tab.

4.3 IBM DB2

ComCap has been tested against IBM DB2 Express-C v9.7 for Windows, using the 'IBM OLE DB Provider for DB2' that is part of the client package that may be downloaded from: <http://www-01.ibm.com/software/data/db2/express/> During install, you get an option to install just the client rather than the server, but beware it installs several windows services anyway.

Microsoft Data Access Components (MDAC or ADO) must first be installed. Windows XP SP2, Windows 2003, Vista, 2008 and 7 include MDAC as part of the core operating system, for Windows 2000, MDAC 2.8 SP1 (free download from Microsoft [MDAC Downloads](#)) should be installed before attempting to configure database support in ComCap.

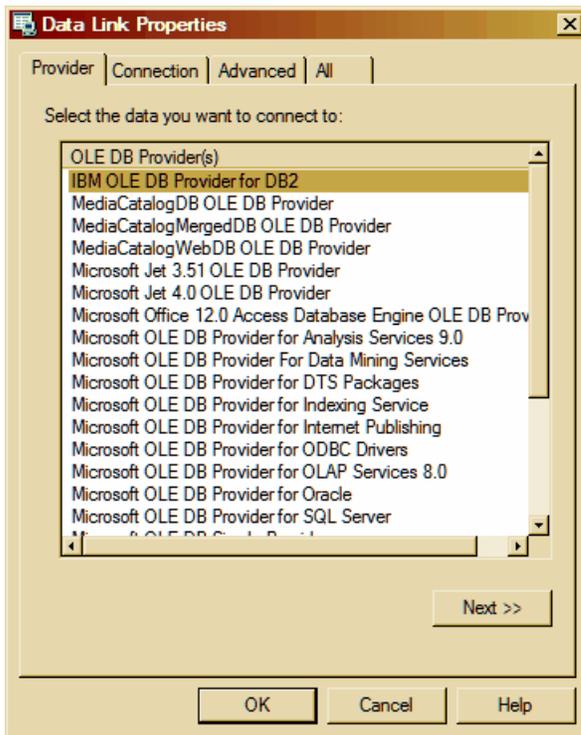
Sample Database Tables

The database table to which ComCap data will be written must be created before ComCap can be configured, and the database must be running.

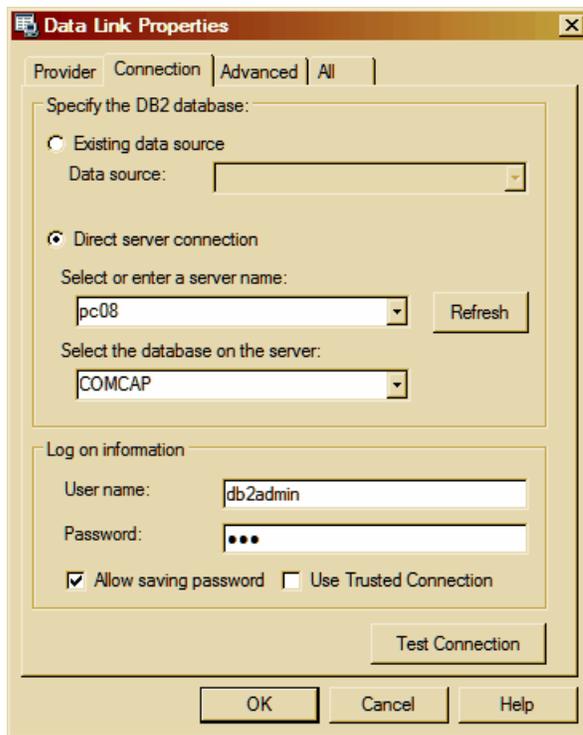
ComCap includes Sample Database SQL scripts to create empty tables and stored procedures, for IBM DB2 this is the file newdb-ibmdb2.sql. One of the IBM tools may be used to run the script into DB2, or Universal SQL Editor is recommended. Note that writing using stored procedures has not been tested.

Setting Up a Database Connection

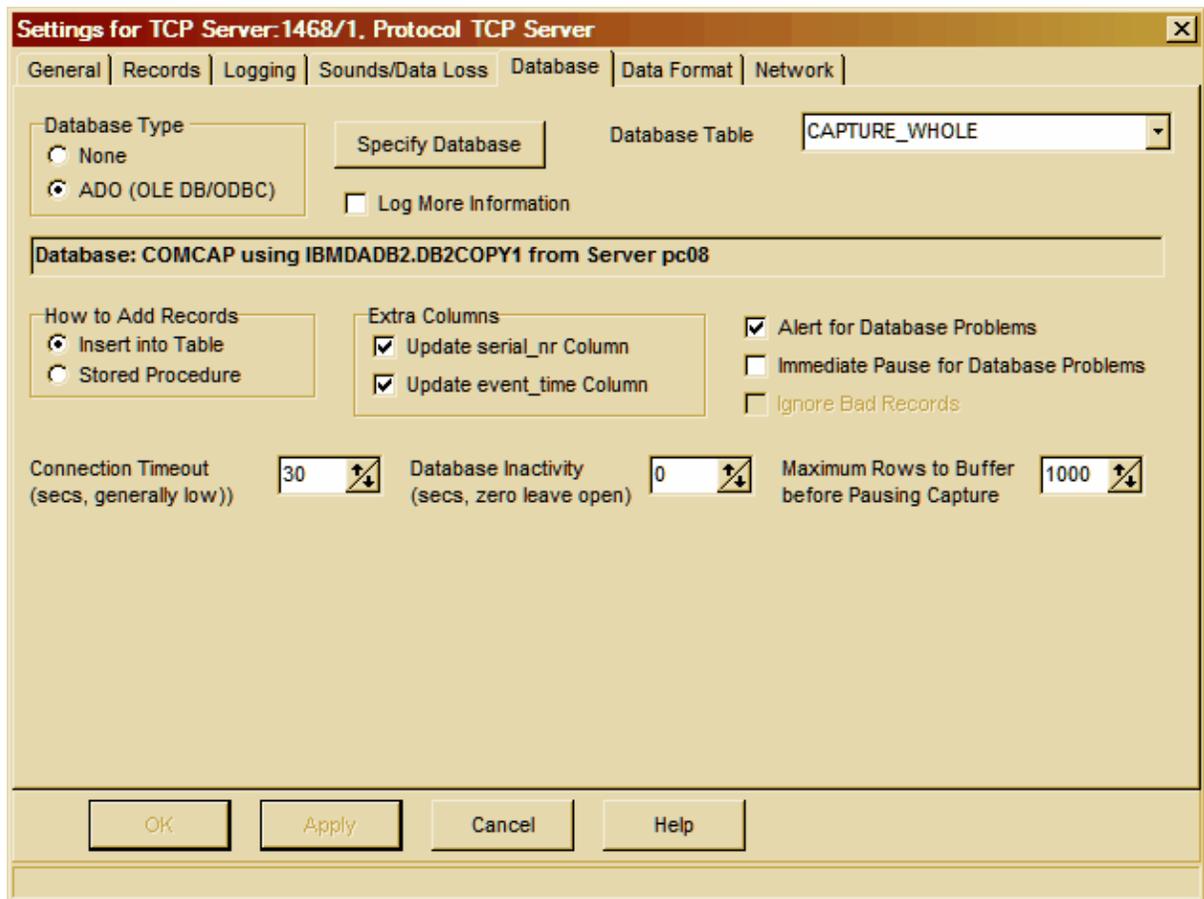
On the Capture Settings, Database tab, choose Database Type as ADO, then click the Specify Database button displays the MDAC Data Link Properties dialog, showing a list of installed data providers:



From the provider list, select IBM OLE DB Provider for DB2, and click Next>>:.



On the Connection tab, choose 'Direct Server Connection' with the server name as an IP address or host, it should then allow a database to be selected once a logon has been entered and 'Allow Saving Password' ticked. Click Test Connection to make sure SQL is working, then OK.



ComCap will then open the database and the details will be displayed to confirm it's all working OK. ComCap can either insert data directly into a table, or pass data to a stored procedure that may manipulate the data and insert it into one or more tables. When you choose 'How to Add Records', a list of either SQL Tables or Stored Procedures will appear, from which one should be chosen. The list of tables and stored procedures will include lots of system functions but these should be ignored. How the data is chosen for the database is specified on the Data Format tab. Other settings on this tab are detailed at Database tab.

4.4 Sun MySQL

ComCap has been tested against Sun MySQL v5.1 community edition, using the 'Connector/OBBC 3.51 driver' from <http://dev.mysql.com/downloads/>
Note the 'ODBC 5.1' driver does not seem to work with ComCap, nor does the 'MySQL OLEDB Provider'.

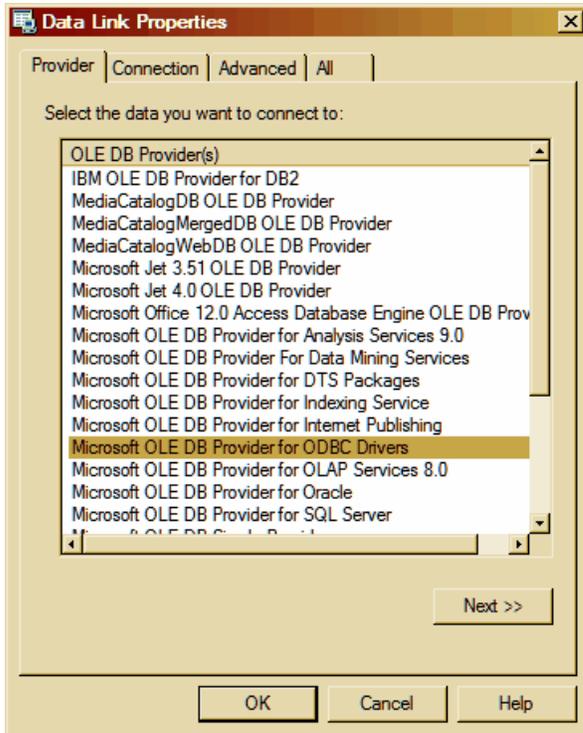
Sample Database Tables

The database table to which ComCap data will be written must be created before ComCap can be configured, and the database must be running.

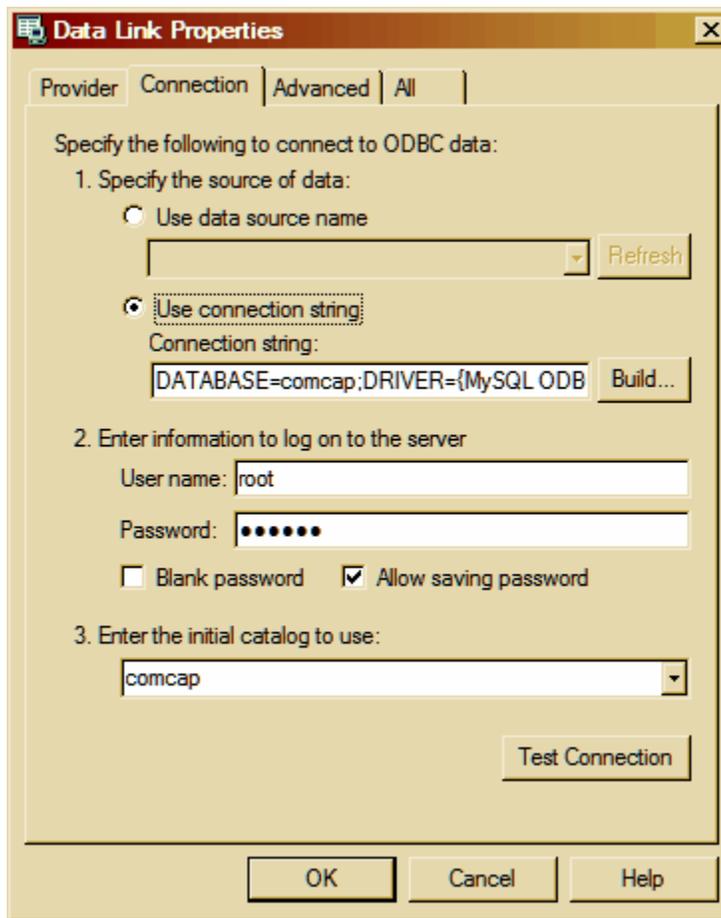
ComCap includes Sample Database SQL scripts to create empty tables and stored procedures, for IBM DB2 this is the file `newdb-ibmdb2.sql`. One of the IBM tools may be used to run the script into DB2, or Universal SQL Editor is recommended. Note that writing using stored procedures has not been tested.

Setting Up a Database Connection

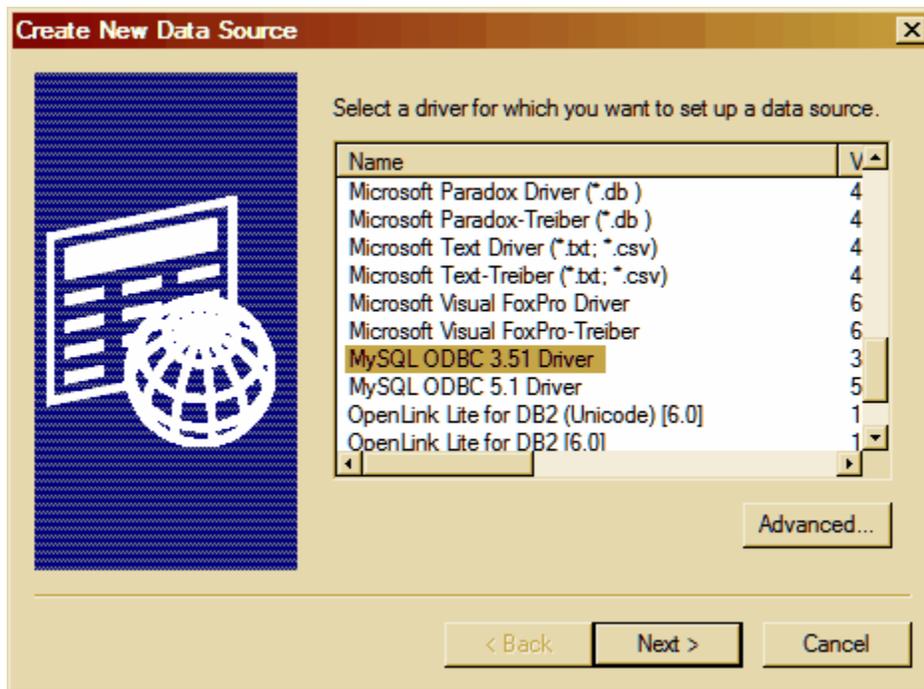
On the Capture Settings, Database tab, choose Database Type as ADO, then click the Specify Database button displays the MDAC Data Link Properties dialog, showing a list of installed data providers:



From the provider list, select Microsoft OLE DB Provider for ODBC Drivers, and click Next>>:.



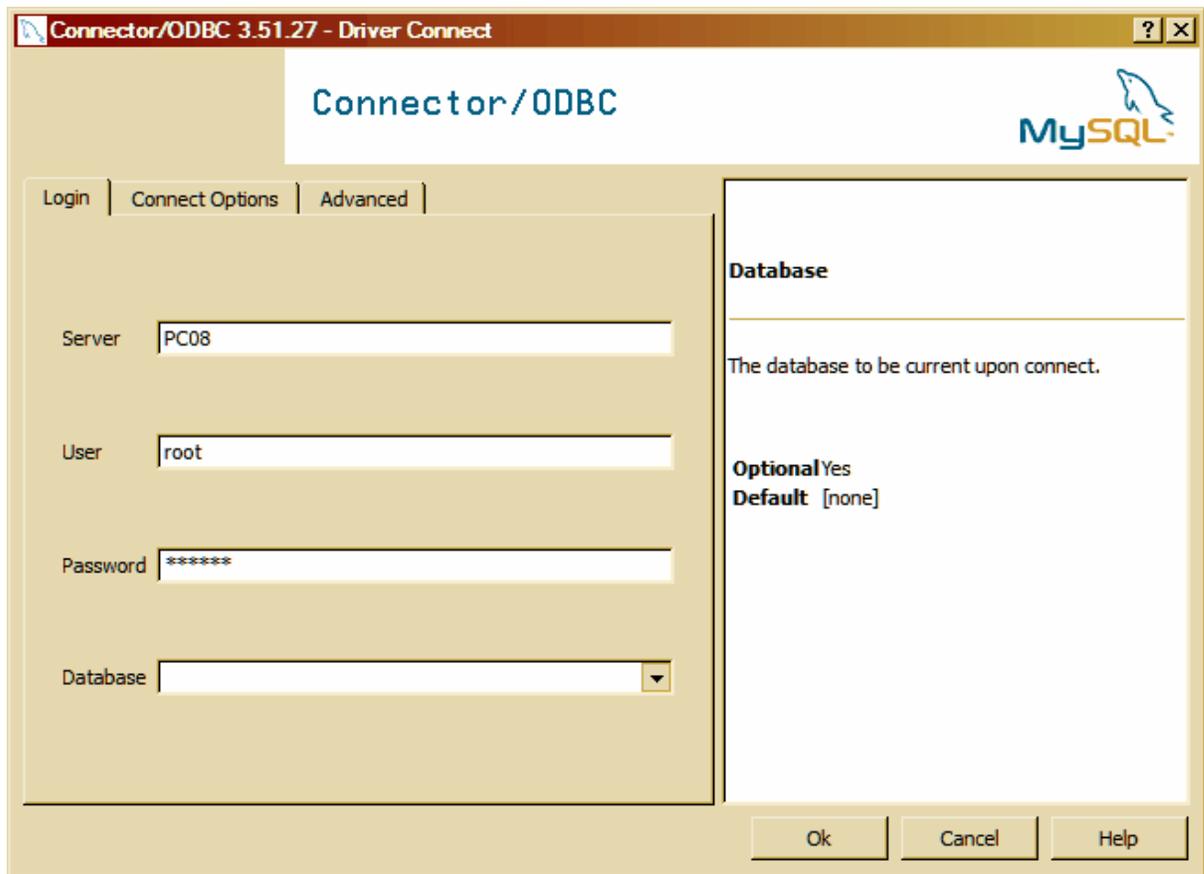
On the Connection tab, choose Use Connection String and click the Build button. A Select Data Source dialog will appear (shown below) from which an existing ODBC connection for MySQL may be chosen, or the New button clicked to create a new data source:



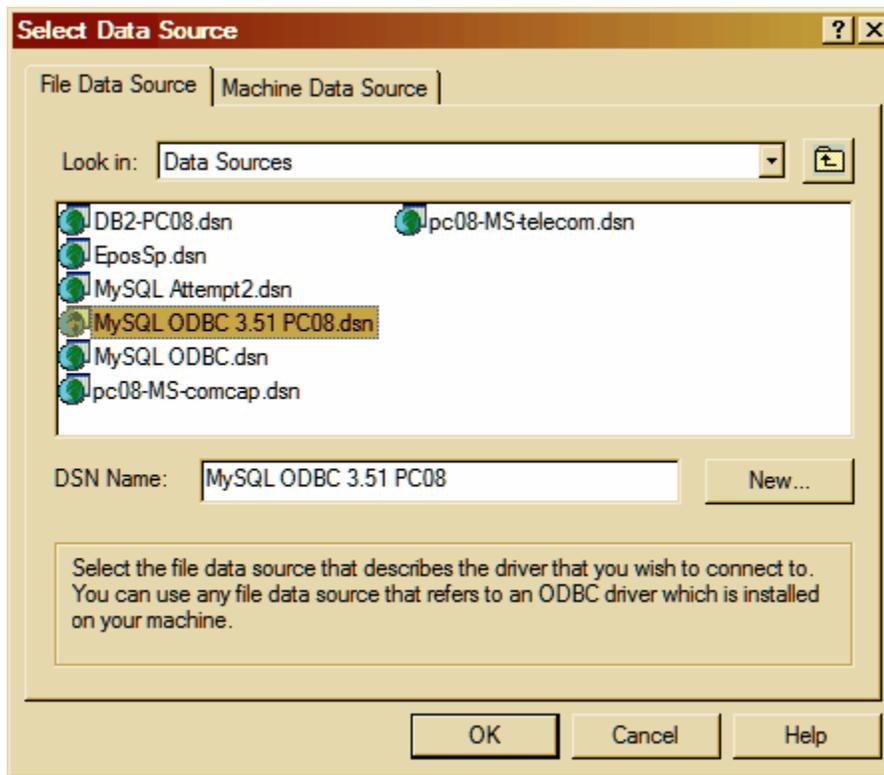
The Create New Data Source window will appear with a list of data sources, select MySQL ODBC 3.51 Driver (not 5.1 Driver) and click Next>.



The next window asks for the directory location and name with which to save the ODBC connection, click Next> again will display a summary page, from which OK should be clicked, which will then display a further Connector/ODBC dialog:



This driver connector dialog should have the server and logon details supplied, then click OK.



You are then back on the Select Data Source dialog with your new Data Source Name (DSN) being shown, click OK and you are back on the Data Link Properties dialog.

Data Link Properties

Provider | **Connection** | Advanced | All

Specify the following to connect to ODBC data:

1. Specify the source of data:

Use data source name

Use connection string

Connection string:
DATABASE=comcap;DRIVER={MySQL ODB} Build...

2. Enter information to log on to the server

User name: root

Password: ●●●●●●

Blank password Allow saving password

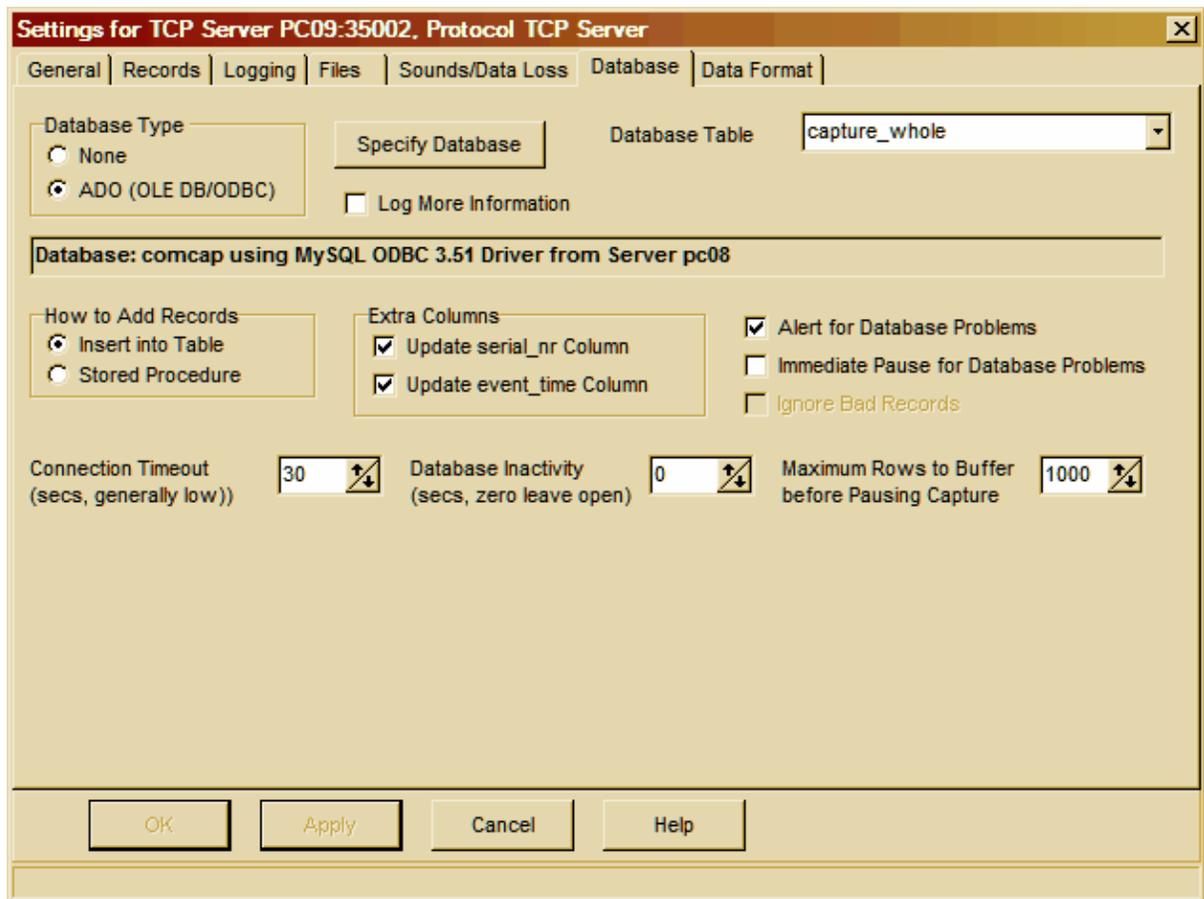
3. Enter the initial catalog to use:

comcap

Test Connection

OK Cancel Help

Specify authentication to logon to the database, and then the actual database to be used. Click Test Connection to make sure SQL is working, then OK



ComCap will then open the database and the details will be displayed to confirm it's all working OK. ComCap can either insert data directly into a table, or pass data to a stored procedure that may manipulate the data and insert it into one or more tables. When you choose 'How to Add Records', a list of either SQL Tables or Stored Procedures will appear, from which one should be chosen. The list of stored procedures will include lots beginning sp_ but these should be ignored. How the data is chosen for the database is specified on the Data Format tab. Other settings on this tab are detailed at Database tab.

Backslash Issue

There is a potential problem with old versions of MySQL that treat the backslash character as the first of an escape sequence (ie \f is form feed). The Database tab has an Escape Backslash option sends \ as \\ so MySQL saves it as \ instead of reporting a syntax error. Newer versions of MySQL have a configuration option to disable escape sequences.

4.5 Sample Databases

ComCap includes various SQL script files, `newdb-xx.sql` and `storedproc-xx.sql` where `xxx` is a database type, containing SQL statements to create a COMCAP SQL database with four example tables, and stored procedures (for some databases only) to add records to those tables and provide limited reporting.

The help pages for the specific databases explain how to use the SQL script files.

Microsoft SQL Server

Sun MySQL
IBM DB2

Sample Tables

There are four sample tables in the COMCAP database:

capture_whole	Three columns: <code>serial_nr</code> , <code>event_time</code> and <code>info</code> , where the whole record is stored. Another application or SQL stored procedures could be used to further analyse the captured data. <code>serial_nr</code> and <code>event_time</code> provide the primary key, see below.
capture_fixed	16 columns for telephone call data record logging: <code>serial_nr</code> , <code>event_time</code> , and various call fields. <code>serial_nr</code> and <code>event_time</code> provide the primary key.
capture_csv	Six columns designed to match the comma separated fields created by the ComGen test data generator, using two columns as the key.
capture_sonicwall	24 columns designed to match the Sonicwall firewall syslog variable named columns. Note the SQL column names are longer than the syslog names. Because there is no obvious unique key, a SQL identity column is used the key.
capture_email	Seven columns designed to capture emails, with the four main headers, originating IP address and a single 8000 long field for the email body. Because there is no obvious unique key, a SQL identity column is used the key. MS SQL Server only at present.
capture_gps	Seven columns designed to capture GPS location information using the ComCap GPS CSV format. There is an <code>event_time</code> column which is used as the key with the title or channel name. MS SQL Server only at present.

While ComCap can be used to write directly to these, or any other, SQL tables, it is generally recommended that stored procedures are used instead since these allow data validation and manipulation to be performed using SQL functions and commands. For instance, dates and times may be manipulated using SQL string functions into unambiguous formats that SQL will accept, ideally ISO format (`yyyy-mm-ddThh:mm:ss.zzz`). All stored procedures called by ComCap must return a single row resultset with two columns, `retcode` and `retmess`, with `retcode` set to 100 for success, anything else results in ComCap reporting an error with the `retmess` (this is illustrated in `storedproc-mssql.sql`).

ComCap handles two columns specially, `serial_nr` and `event_time`, if used. Note these column names must not be used for other purposes if ComCap is told to use them. These extra columns are updated with the channel Serial Number and the time that the event was added to the database, if specified, and are usually the unique key for the table. The Serial Number is the same as used for adding escaped text to the captured data and the starting number and length may be specified on the Logging tab. While these two special columns will provide a unique database key where there is nothing guaranteed unique in the captured data, it is generally recommended that the Serial Number and event time are added as escaped text to the captured line, and then selected in the data format as columns for the database, this has the advantage of keeping the logged files the same as the database.

Sample Stored Procedures

There are six sample stored procedure supplied to put data into the various sample tables:

capture_whole_put	This stored procedure simply saves three columns without any further processing.
capture_fixed_put1	This stored procedure is designed to process CDRs in the sample-bts7#2.txt file where call_time is passed as HH:MM to which the current date is added and call_len as HH:SS, both of which are stored in DATETIME columns.
capture_fixed_put2	This stored procedure is designed to process CDRs in the erikkson.txt file where call_time is either YYMMDD HHMM or MMDDHHMM both of which are converted into DATETIME with the years, and call_len which seconds and also converted to DATETIME.
capture_csv_put	This stored procedure simply saves six columns without any further processing.
capture_sonicwall_put	This stored procedure simply saves 15 columns without any further processing.
capture_sonicwall_put2	Similar to above, but parses IP address and port and source into separate columns, ie 192.168.1.109:3743:LAN is saved to three separate columns to ease selection.
capture_email_put	This stored procedure simply saves seven columns without any further processing
capture_gps_put	This stored procedure simply saves seven columns without any further processing

The storedproc-mssql.sql file also has several xx_lst sample stored procedures to list rows in each of the four sample tables by date range, and some SQL statements that can be used to find out how many rows have been saved to each table, and to truncate the tables to remove all rows.

To set-up ComCap to save captured data to a database, the SQL table and ideally stored procedure must be created first, to allow ComCap to read the column and parameter definitions. It is also recommended that some data is first captured, which will considerably ease setting the Data Format that defines how columns will be taken from captured data.

Part

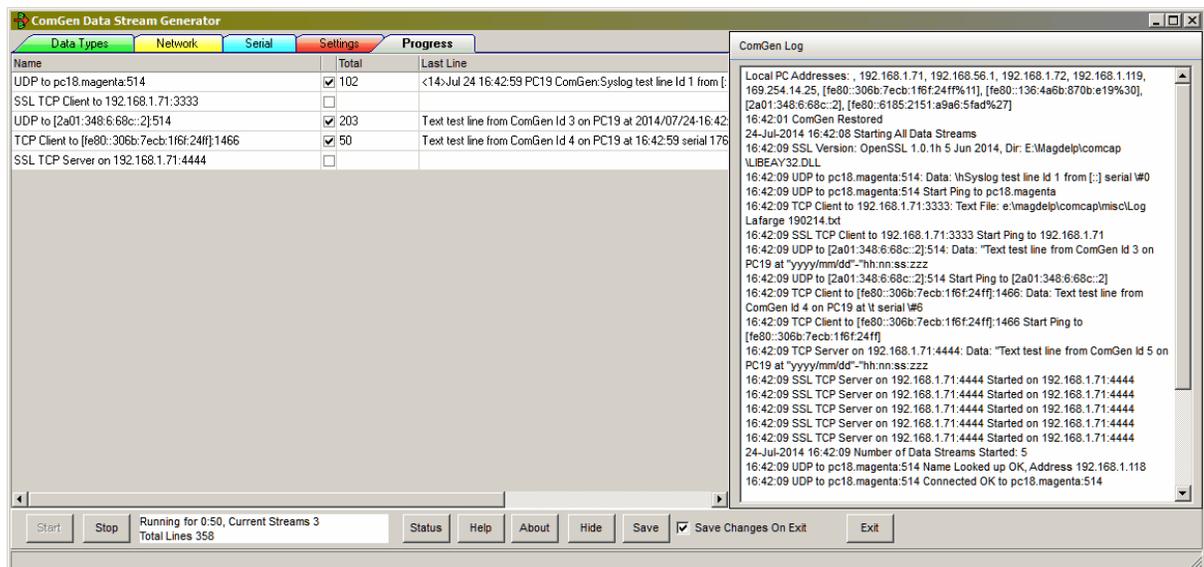


5 Miscellaneous

5.1 ComGen Data Stream Generator

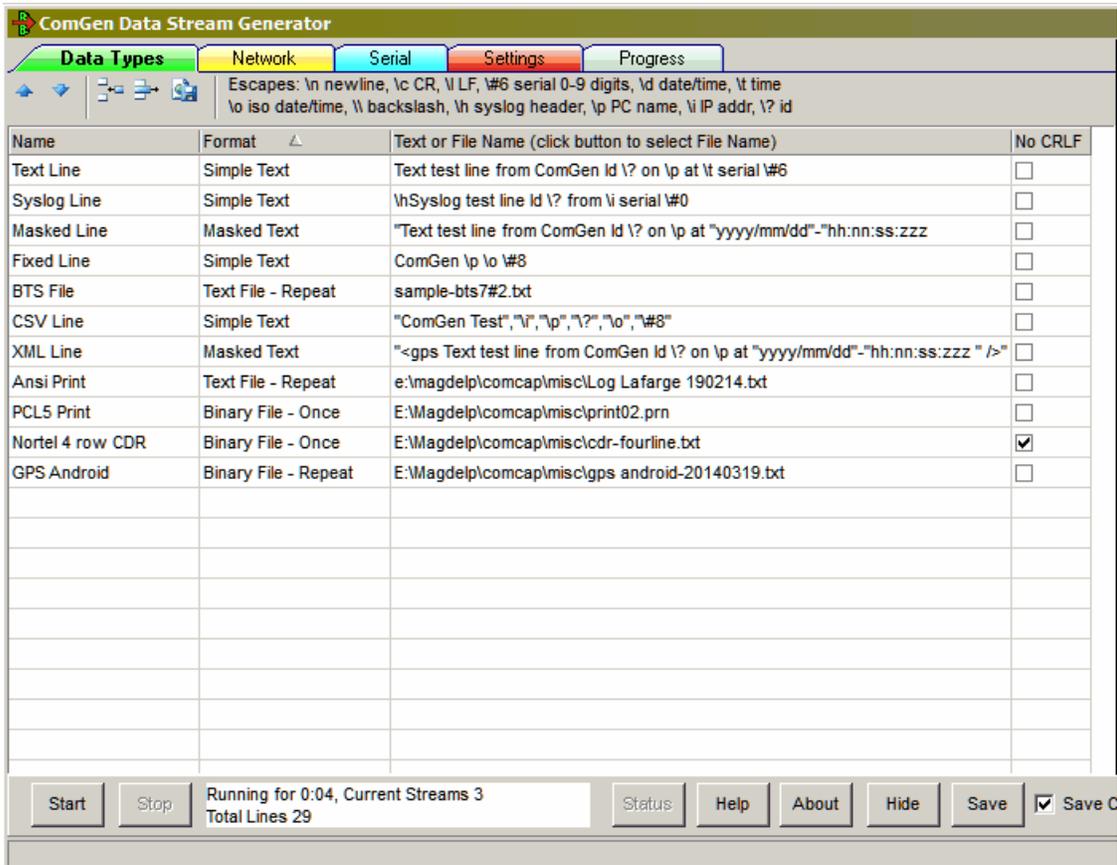
ComGen is an application delivered free with ComCap 4, designed for testing ComCap. It generate various types of test streams using any or all of the PC serial COM ports and potentially dozens of network streams, UDP Client, TCP Client or TCP Server, using SSL/TLS if needed, with both IPv4 and IPv6 protocols.

ComGen is a low overhead application, and will run for hundreds of hours, generating millions of lines of test data, to thoroughly test ComCap. It may be installed on the same PC as ComCap, or copied onto remote PCs and run there.



ComGen only has a single window, with five tabs: Data Types, Network, Serial, Settings and Progress, and a right hand log window. Note ComGen does not write any log files.

Data Types



Data Types defines the actual lines of data that will be streamed, which may be the common between two or more channels. Each different type should be given a name, and a format selected:

Simple Text	Simple text including escape sequences as listed below.
Masked Text	Masked Text including escape sequences and also time and data mask characters formatted in the same way as ComCap capture Files. Note all text is treated as a mask unless surrounded by quotes.
Text File - Once	Text data from a file, sent one line at a time when CRLF is found. Sent once, then stops.
Text File - Repeat	Similar, but repeats on reaching the end.
Binary File - Once	Binary data from a file, sent 100 bytes at a time ignoring CRLF. Sent once, then stops. Sending 10 lines per second will send 1Kbyte of data per second.
Binary File - Repeat	Similar, but repeats on reaching the end.

Both text formats may include one or more escape sequences:

\#6	Serial Number, where the digit is the number of digits to use, with leading zeros.
-----	--

\d	Date and time, ie 21-Jun-2006 20:10:12. Note this is a fixed date format, if more flexible formatting is needed use the Time Stamp Each Line option above.
\t	Time, ie 20:10:12
\o	ISO date and time, ie 2006-06-21T20:12:11, recommended for database capture
\s	Space, used as a separator at the start or end of the escaped text, not necessary within the text
\p	PC Name (NETBIOS),ie MYCOMPUTER
\i	Local IP address, ie 192.168.44.55
\m	Channel Name, note spaces may cause problems
\n	New line (CRLF), not generally recommended
\f	Form Feed (FF)), not generally recommended
\c	Carriage Return (CR)), not generally recommended
\l	Line Feed (LF), not generally recommended
\\	Backslash (\)
\e	Escape (ESC)), not generally recommended
\xnn	Any hex code where nn is 01 to FF
\?	ComGen channel ID
\h	Syslog header

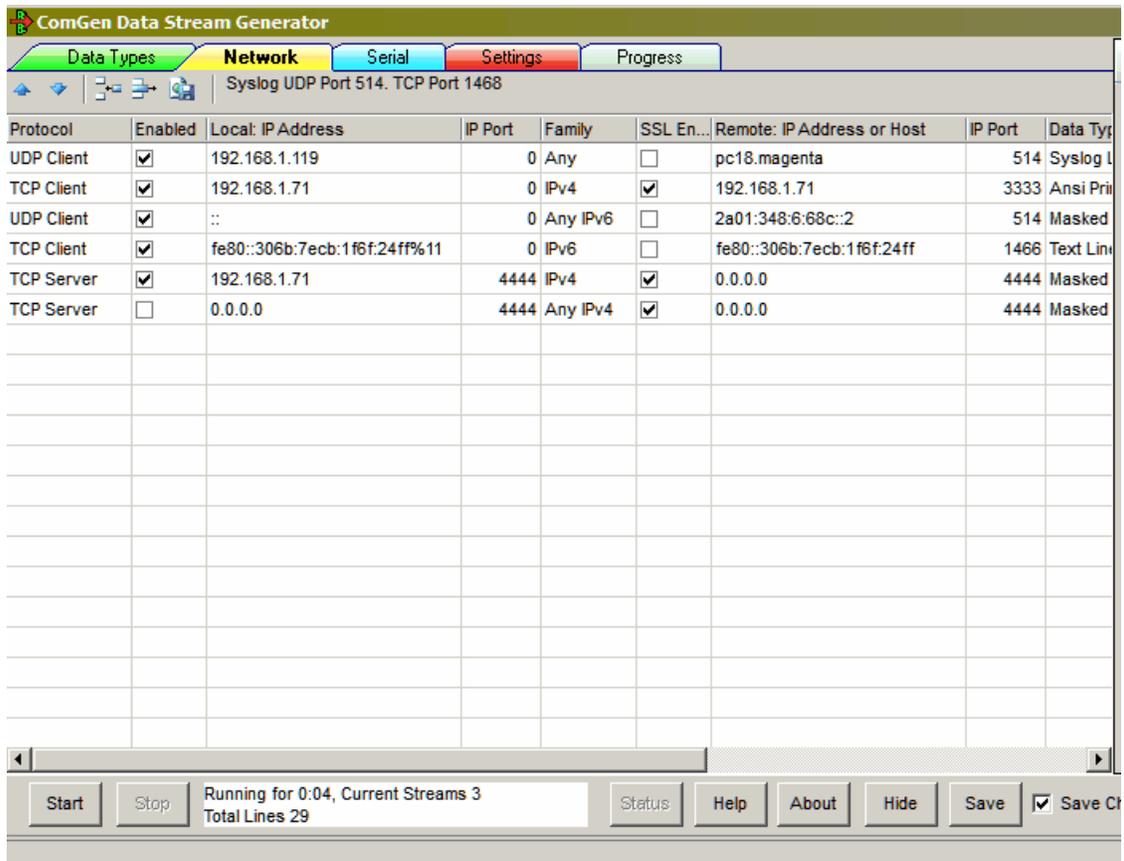
When using Text or Binary File formats, the button at the end of the row may be clicked to select a file to stream. The file may be actual data captured by ComCap such as CDRs (two small sample files are supplied) or any other data, optionally including the escape sequences above.

A sample Simple Text format might be:

```
Text test line from ComGen Id \? on \p at \t serial \#8
```

No CRLF ticked means no line ending is sent for Simple Text or Masked Text, which is usually how UDP data is sent.

Network Data Configuration



Network configuration is very similar to Common Settings, Network, specifying UDP Client, TCP Server or TCP Client parameters. Note that SSL is set-up in the grid, unlike in ComCap itself. A remote host name can only be specified if Family is set to Any. To simplify this grid, retry attempts have been made common to all channels and are specified on the Settings tab, see below.

Data Type

Clicking Data Type will drop down a list of all the Data Types specified on the previous tab, from which one should be selected.

How Often, Often By

How Often is used to specify the frequency with which data is generated for this channel, selected from the drop down menu as Each Second, Each Minute, Each Hour and Random (between one and 10 seconds) with the Often By multiplier. So 5 by Each Second is five lines of text each second, 30 by Each Minute is one line every two seconds. ComGen has been tested with up to 50 lines per second, and is limited to 60 lines per second. Note that all lines are sent at the start of the second, rather than being spread out evenly.

Next Serial

This column specifies the Next Serial Number that will be used for the data, if it includes the \# mask.

Lines/Session

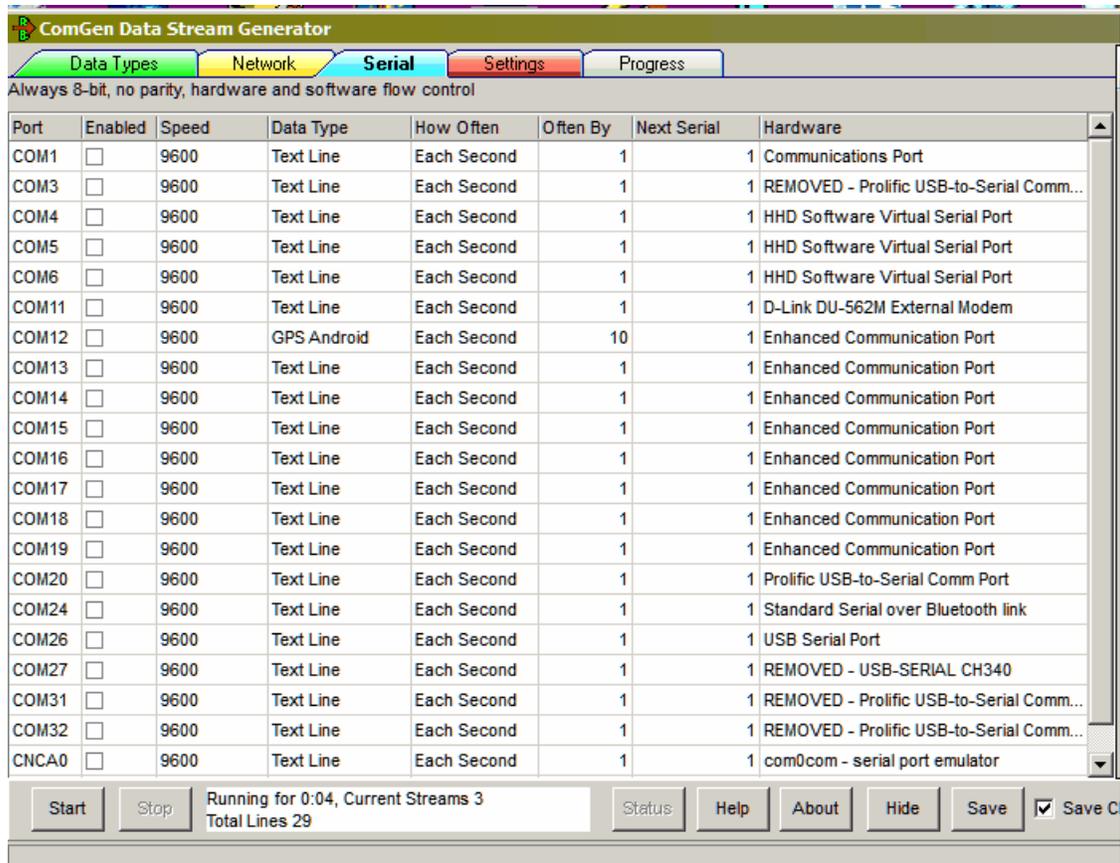
Specifying a non-zero number for TCP Client causes the TCP session to be disconnected after that many lines of data have been sent, to simulate remote data capture devices that continually connect, send some data and then disconnect.

Device Id (first line)

Specifying non-blank text causes this text to send at the start of the session before any other data is

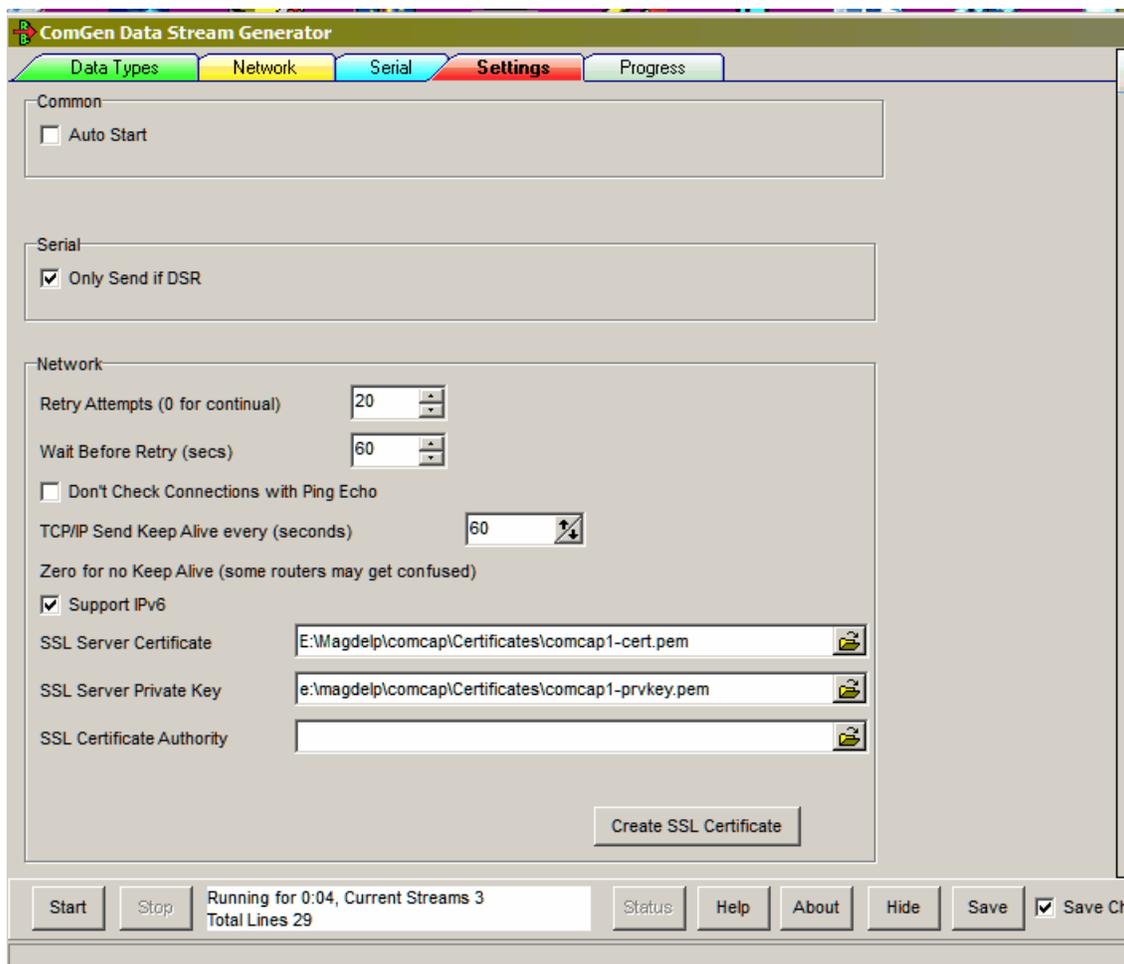
sent, to simulate remote data capture devices that identify themselves in some way (like the Ecov). If this data should be sent as a separate line, use a /n escape to send CRLF, ie <TEST>\n

Serial Data Configuration



Serial configuration is very similar to that in Common Settings, Serial Ports. Note that ComGen only support 8 bit's for data with 1 stop bit and no parity. There are additional columns allowing the data frequency, type and serial numbers to be specified, see above. Some virtual ports may have strange names like CNCA2, but these will work identically to those starting with COM.

Settings



The Settings tab has some more options:

Common

The Auto Start tick box specifies that streaming starts as soon as ComGen is run. If ComGen is to run when Windows starts, a shortcut should be placed in the Windows Startup folder.

Serial Configuration

The Only Send if DSR tick box specifies that serial data should only be sent if the remote computer has raised Data Terminal Ready.

Network Configuration

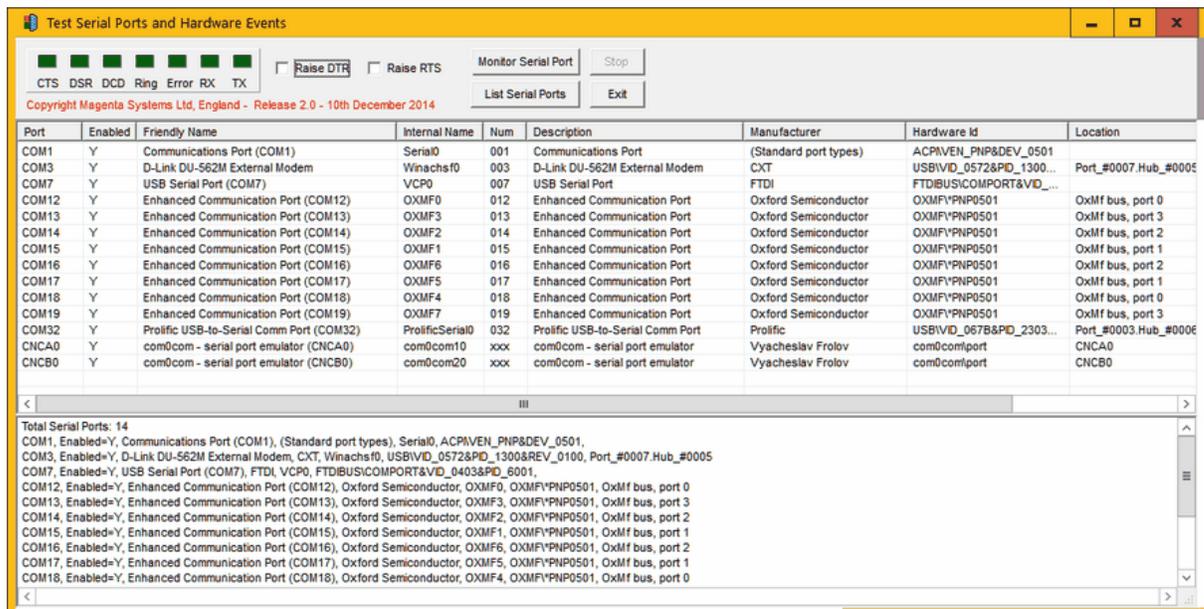
These network settings are common to all network channels, Retry Attempts (zero for continual attempt), Wait Before Retry is the delay between attempts, Don't Check Connections with Ping Echo is a tick box, TCP/IP Send Keep Alive specifies how often in seconds a keep alive should be sent to stop a router or firewall dropping an idle connection. IPv6 needs to be enabled here. The same SSL certificate will be used for all TCP/IP Server streams. There is no remote server certificate checking for TCP/IP client.

Progress

When all the settings are completed, click Start to commence data streaming. The Progress tab shows one row for each stream of data being generated, a tick box indicates if that channel is currently streaming data, the total number of lines generated can be seen and the actual text of the last line (which may help getting the Data Type escapes correct).

5.2 Test Serial Ports and Hardware Event

A 'Test Serial Ports and Hardware Events' (previously Test RS232 Signals) utility is supplied with ComCap, which may be useful for simple communications port testing. It allows any installed windows serial communications port to be open, shows the status of the five RS232 signal lines and whether any data is being received, and allows the DTR and RTS control lines to be raised or lowered.



If a modem is connected to the serial port and it has front panel indicators, toggling DTR will cause TR to flash, confirming that the modem is cabled correctly to the PC. If a null modem cable is used to connect two PCs each running the utility, the opposing DSR and CTS indicators will appear as DTR and RTS are toggled on each PC.

Some virtual ports may have strange names like CNCA2, but these will work identically to those starting with COM.

This utility does not show or send any data, it's just designed to ease resolving cabling problems, or even identifying which PC back panel connector is which communications port.

Note this utility only shows serial ports that are exist and enabled, while the ComCap Serial Ports grid in Common Settings shows all ports installed on the PC including those currently removed and unusable, which are typically USB serial ports that are unplugged.

5.3 Concatenation Utility

The ComCap distribution includes a Concatenation Utility, written by a ComCap user. It allows multiple text file captured by ComCap to be combined into a single larger text file that may be easier to import into a telephone call management application.

When accessed, one panel shows possible source files which may be selected for concatenation by clicking the '>>' or 'Add All' buttons. Once all the correct files appear in the right hand window, click 'Sort by Name and Remove Duplicates', and then the 'Concatenate' button. A Save File dialog will then

appear, allowing the output file to be specified. Progress during concatenation is shown in the output window. Only text files are supported.

5.4 Null Modem Emulator (com0com)

If there is a requirement to capture serial data from another application on the same PC, the Null Modem Emulator (com0com) from <http://com0com.sourceforge.net/> may be installed. This provides linked pairs of virtual serial ports, ie COM21 is linked to COM22, so any data sent to COM21 arrives at COM22. This avoids needing to use a pair of physical ports and a null modem cable. It might be used for capturing serial printer data.

The information that follows is from the com0com readme file that may be found in the files com0com-i386.zip (for Windows 32-bit) and com0com-x64-signed.zip (for Windows 64-bit) in the ComCap install directory. Note com0com is an open source project and has not been tested by Microsoft WHQL, so skip the security alerts that appear during 64-bit installation.

Introduction

The Null-modem emulator is an open source kernel-mode virtual serial port driver for Windows, available freely under GPL license. You can create an unlimited number of virtual COM port pairs and use any pair to connect one application to another. Each COM port pair provides two COM ports with default names starting at CNCA0 and CNCB0. The output to one port is the input from other port and vice versa.

Usually one port of the pair is used by Windows application that requires a COM port to communicate with a device and other port is used by device emulation program.

For example, to send/receive faxes over IP you can connect Windows Fax application to CNCA0 port and t38modem (part of the OpenH323 project) to CNCB0 port. In this case the t38modem is a fax modem emulation program.

The homepage for com0com project is <http://com0com.sourceforge.net/>.

Installing

Simply run the installer (setup.exe). An installation wizard will guide you through the required steps. If the Found New Hardware Wizard will pop up then

- select "No, not this time" and click Next;
- select "Install the software automatically (Recommended)" and click Next.

The one COM port pair with names CNCA0 and CNCB0 will be available on your system after the installation.

You can add more pairs with the Setup Command Prompt:

1. Launch the Setup Command Prompt shortcut.
2. Enter the install command, for example:

```
command> install - -
```

The system will create 3 new virtual devices. One of the devices has name "com0com - bus for serial port pair emulator" and other two of them have name "com0com - serial port emulator" and located on CNCA_n and CNCB_n ports.

To get more info enter the help command, for example:

```
command> help
```

Testing

1. Start the Hyper Terminal on CNCA0 port.
2. Start the Hyper Terminal on CNCB0 port.
3. The output to CNCA0 port should be the input from CNCB0 port and vice versa.

Uninstalling

Simply launch the com0com's Uninstall shortcut in the Start Menu or remove the "Null-modem emulator (com0com)" entry from the "Add/Remove Programs" section in the Control Panel. An uninstallation wizard will guide you through the required steps.

HINT: To uninstall the old version of com0com (distributed w/o installer) install the new one and then uninstall it.

FAQ & HOWTO

Q. Is it possible to change the names CNCA0 and CNCB0 to COM2 and COM3?

A. Yes, it's possible. To change the names:

1. Launch the Setup Command Prompt shortcut.
2. Enter the change commands, for example:

```
command> change CNCA0 PortName=COM2
command> change CNCB0 PortName=COM3
```

Q. The baud rate setting does not seem to make a difference: data is always transferred at the same speed. How to enable the baud rate emulation?

A. To enable baud rate emulation for transferring data from CNCA0 to CNCB0:

1. Launch the Setup Command Prompt shortcut.
2. Enter the change command, for example:

```
command> change CNCA0 EmuBR=yes
```

Q. The HyperTerminal test succeeds, but I get a failure when trying to open the port with CreateFile ("CNCA0", ...). GetLastError() returns ERROR_FILE_NOT_FOUND.

A. You must prefix the port name with the special characters "\\.\". Try to open the port with CreateFile ("\\\\.\CNCA0", ...).

Q. My application hangs during its startup when it sends anything to one paired COM port. The only way to unhang it is to start HyperTerminal, which is connected to the other paired COM port. I didn't have this problem with physical serial ports.

A. Your application can hang because receive buffer overrun is disabled by default. You can fix the problem by enabling receive buffer overrun for the receiving port. Also, to prevent some flow control issues you need to enable baud rate emulation for the sending port. So, if your application use port CNCA0 and other paired port is CNCB0, then:

1. Launch the Setup Command Prompt shortcut.
2. Enter the change commands, for example:

```
command> change CNCB0 EmuOverrun=yes
command> change CNCA0 EmuBR=yes
```

Q. I have to write an application connected to one side of the com0com port pair, and I don't want users to 'see' all the virtual ports created by com0com, but only the really available ones.

A. If your application use port CNCB0 and other (used by users) paired port is CNCA0, then CNCB0 can be 'hidden' and CNCA0 can be 'shown' on opening CNCB0 by your application. To enable it:

1. Launch the Setup Command Prompt shortcut.
2. Enter the change commands:

```
command> change CNCB0 ExclusiveMode=yes  
command> change CNCA0 PlugInMode=yes
```

5.5 Release Notes

ComCap Release 4.20 - May 2019

1 - Support has been added for TLSv1.3, the first improvement in SSL for about 10 years, using OpenSSL 1.1.1b.

2 - In Common Settings, Common, 'SSL Client Security' now specifies the SSL security level for all TCP/IP Client (including email) to ensure that minimum security standards are enforced. The options are:

- SSLv3 Only
- TLSv1 Only
- TLSv1.1 Only
- TLSv1.2 Only
- TLSv1.3 Only
- TLSv1 or Better
- TLSv1.1 or Better
- TLSv1.2 or Better
- Backward Ciphers
- Intermediate Ciphers
- High Ciphers, 2048 keys
- High Ciphers, 3072 keys
- High Ciphers, 7680 keys

If there are problems accessing servers using earlier beta versions of TLSv1.3, set the Security Level to TLSv1.2 Only. Updated SSL root certificates with more of those commonly used.

3 - In Common Settings, Common, 'SSL Server Security Level' now specifies the SSL security level for all TCP/IP Servers to ensure that minimum security standards are enforced. The options are:

- SSLv3 Only
- Backward Ciphers, TLS1 or Later
- Intermediate Ciphers, TLS1.1 or Later
- Intermediate Ciphers FS, TLS1.1 or Later
- High 112 bit Ciphers, TLS1.2 or Later
- High 128 bit Ciphers, TLS1.2 or Later
- High 192 bit Ciphers, TLS1.2 or Later
- TLSv1.2 or Earlier
- TLSv1.3 Only

Ideally use TLSv1.1 minimum since TLSv1 has been deprecated by the PCI DSS council. It's no longer necessary to specify DHParams, SSL Server ECDH Key or SSL Allowed Host Names.

4 - Added support for two more GPS vehicle and personal trackers data formats: Xenun TK102/103 and WondeX/TK5000. The Xenun TK102/103 format is essentially the NMEA RMC sentence, preceded by date/time and mobile number, followed by useful stuff from other NMEA sentences like satellite count, mobile IMEI and cell station stuff. The WondeX/TK5000 format used by VT-10, VT300

and other devices is a simple format with IMEI, time, co-ordinates, speed and direction. Both these data formats are TCP/IP server only. They are also used by a Android application MyLiveTracker by Michael Skerwiderski available free from Google Store:
<https://play.google.com/store/apps/details?id=de.msk.mylivetracker.client.android>.

5 - ComCap4 now includes ComGen5 instead of ComGen4, which has been rewritten to support more functionality creating test data streams to exercise ComCap4. There is a new ComGen5 Settings window with the same four tab that were previously in the main window. The Network Channels tab has a new protocol 'Multi TCP Client' which will generate the number of clients as specified in the new 'Clients' column, up to 2,000 at present. Each client session will terminate after 'Lines/Session' have been sent. To avoid starting all these sessions at once (which most servers will be unable to handle), the General tab has a new setting 'Maximum New TCP Client Sessions Per Second' to restrict that number, typically 100 per second, or less for slower servers. The tab also has 'Random Gap Between Sessions (secs)' with 'Minimum' and 'Maximum' being specified, defaulting to 5 and 60 seconds, so that repeat sessions are staggered. Any sessions that fail to connect first time will retry after 'Wait Before Retry (secs)' for 'TCP Client Retry Attempts'.

6 - ComGen5 will now create HTTP requests to test web servers. There are three new Data Type Formats, HTTP GET URL, HTTP POST URL, HTTP PUR URL which should be used with TCP Client or Multi TCP Client. The Remote Host and Port are set in the Network grid, with the page and parameters specified as the Data Type Text, ie: HTTP GET URL and '/index.html' will get that URL, multiple URLs can be accessed by separating them with |, ie: '/page1.html|/page2.html|/page3.html'. For both POST and PUT, parameters follow the URL and ?, ie: /upload.html?Text test line from ComGen Id \? on \p at \t session \S serial \#6 with the escape dynamically processed identically to Simple Text format. ComGen5 does not support pipelining but waits for a response to each request, which is reported in the result column of the main progress grid. In Setting, General, the 'HTTP User Agent' for the requests may be specified. The request and first response will always be logged, but generally subsequent requests are not logged, see below, just counted.

7 - ComGen5 now include optional log files. The Settings, General tab has a tick box 'Write Log File' and 'Directory' which if completed cause daily log files to be created. 'Log All Connection Attempts' defaults to unticked to reduce the amount of logging with repeated connections and disconnections, so only the first and last are generally logged, but may be ticked for full logging of all attempts.

8 - ComGen5 includes the same 'SSL Client Security' and 'SSL Server Security Level' options as ComCap4 on the Network Options tab where the SSL server certificate is specified.

ComCap Release 4.18 - July 2017

1 - Fixed a long term nasty logging bug when there was a problem writing to the information log, that caused ComCap to exhaust memory and crash. This would happen if Main and Alternate logging directories were the same, so the second log files could not be opened and the usual solution of using a different file name would fail since the name is the same in both directories. The original bug is now fixed, and checks made to ensure Main and Alternate logging directories are different. This issue did not effect error handling Capture Logging.

2 - ComCap and ComGen now use the latest OpenSSL 1.1.0f version with the latest security fixes..

ComCap Release 4.17 - March 2017

1 - Fixed a bug that meant email being sent that failed all retries was not deleted from mail queue, but caused logging to go wild with errors.

2 - When starting an SSL server channel, the SSL server certificate, private key and optional intermediate chain are now validated to ensure the SSL server will start correctly, for instance the private key matches the certificate, the certificate is issued by an intermediate and/or by a root CA

authority, and that certificates have not expired. Previously, only PEM certificates were supported, ComCap now also supports DER, PFX, P12, P7B, CER and CRT file formats. PFX/P12 (PKC12) is convenient because it can contain certificate, private key and intermediates so only a single file needs to be used.

3 - Fixed a validation issue introduced in ComCap 4.13 that prevented an IP address being specified to sent the Information Log remotely using UDP or TCP Client.

4 - Fixed two problems with Email channels, they no longer always listen on port 587 and listening now correctly ceases when a channel is stopped.

5 - ComCap4 and ComGen now use the new OpenSSL 1.1.0 version with the latest security fixes. The OpenSSL DLLs are now digitally signed and checked when being loaded, for improved security.

6 - If an unexpected error happens during capture, an alert is now sent and capture restarted.

ComCap Release 4.16 - October 2016

1 - Fixed a problem introduced in the last release that meant some lines of rapid data capture may have not appeared on the screen when being captured by the service version. No data was lost and it was still logged, this was purely a display issue. ComCap5, currently in beta, improves the way data is displayed so is able to display data being captured at the rate of thousands of lines per second, whereas ComCap4 is limited to hundreds of lines. Viewing data at such rates is not really practical since the scrolling windows only show the last 5,000 lines (configurable), but ComCap5 will not become non-responsive under heavy traffic.

2 - ComCap4 and ComGen now use the new OpenSSL 1.1.0b version with the latest security fixes and features, including ChaCha20-Poly1305 encryption cipher suites, X25519 elliptic curve for ECDH ciphers and OCB and CCM mode ciphers.

3 - Improved error messages when setting up Network channels so that trying to use a target host name instead of an IP address says this only works if Family is set to 'Any'

ComCap Release 4.15 - July 2016

1 - ComCap now supports capture files larger than 2 gigabytes in size. Previously errors were reported once this size was reached and a new file safely created without loss of data.

2 - In Channel Settings, Files, a new option has been added 'Max File Size (MBytes)' defaulting to 2,000 (which is 2 gigabytes) that restricts the size of capture files to a larger or smaller size, after which they will be rotated with a new file name. A similar new option in Common Settings, Log Files, specifies the maximum size for Common Capture Logs.

3 - In Common Settings, Capture Logging, a new option 'Format for Display of Large Numbers' has been added, which may be set to Bytes or KBytes/MBytes. This causes file size, lines captured, data rows written, etc, to be displayed and logged in KBytes or MBytes once they exceed 99,999, for easier reading. Fixed a problem displaying the size of captured data once it exceeded 2 gigabytes.

4 - In Channel Settings, General, a new option has been added 'Idle TCP Server Close Session Timeout, Zero None (secs)' which allows a TCP Server session to be closed if no data is received. Generally a remote TCP Client will reconnect when it has more data to send. This timeout is primarily for error conditions where a session remotely fails without a clean close down happening, so TCP Server waits for ever for new data, unless Data Loss checking is used to restart capture which is more complex. The timeout should vary depending on how frequently data is expected, and may be up to 99,999 seconds (69 days). This new setting also applies to Echo to TCP Server.

5 - Fixed a bug that prevented the tray version of ComCap automatically running when Windows 10 was booted, if ComCap had been given elevated access rights (run as administrator) in order to configure or control the ComCap Background Service. It will be necessary to untick 'Auto Run Tray Application', restart ComCap, then retick it to ensure the registry is updated correctly. Also, ComCap will now automatically restart if the ComCap Background Service setting is changed, rather than needing to be restarted manually.

6 - Fixed a bug introduced in the last release that prevented serial capture channels automatically restarting if a disconnected USB serial ports became available again.

7 - In Common Settings, Network, error messages relating to invalid IP address entry now show the Capture Name, to ease finding the failing row.

8 - When sending alert and capture file emails, the SSL server certificate is now checked, if so specified in Common Settings, Common.

9 - When starting TCP Server channels with SSL support, details of the SSL certificate specified are now logged and an alert sent if the certificate has expired or is about to expire.

10 - Fixed a problem that prevented ComCap being used after the year 2030.

11 - In Capture Settings, Logging, 'Add Escaped Text' is documented as \r adding a Remote IP Address but this accidentally got changed to address and port in Release 4.13 when IPv6 was added. So this release adds \R which adds the remote IP Address alone while the documentation has been corrected to show \r adds address:port. Likewise \l now adds Local IP Address only and \i adds address:port.

12 - Cleaned up some SSL issues with missing certificates. The OpenSSL DLLs will now only be loaded from the ComCap main directory to avoid conflict with older OpenSSL versions installed elsewhere. Updated OpenSSL libraries to the latest versions with all the latest security fixes.

ComCap Release 4.14 - September 2015

1 - This is a minor release of ComCap, with a few new features and bug fixes, including better GPS support. ComCap has been tested on Windows 10 for several months, with no unexpected issues, except that only this release will correctly report that it is running on Windows 10. Earlier versions will almost certainly work on Windows 10, but will report they are running Windows 8, so an upgrade for Windows 10 is not essential.

2 - In Windows 10, it is not possible to have desktop start-up programs with administrator rights, they simply don't run when you logon on (presumably a new anti-malware measure). But the ComCap tray application needs administrator rights in order to start and stop the ComCap Service. Normally, the ComCap Service will start automatically when Windows boots, and the ComCap Tray application can still monitor the service, change settings and pause/resume single channels, but it can not stop the ComCap Service or Start it again without being given administrator rights through Properties, Compatibility, 'Run this program as an administrator'. So the ComCap Service will need to be controlled by the Services Windows Administrator Tool, if you want the ComCap Tray to start automatically. Workarounds for this are still being investigated. Note that some Common Settings changes require the ComCap service to be restarted, for instance adding or removing channels, and unless this is done separately using the Services tool the ComCap tray may get very confused and show the wrong data for some channels (only a cosmetic issue).

3 - Added a feature to allow a new Capture Log file to be created on demand, rather than according to the normal settings. In the Capture Log window, select the channel, right click and click 'New Capture Log'. The Information Log should report the capture log has been rotated and show the old and new log names. The new log will have the current time, which means the Log Name Format must include a

time mask, ideally including seconds otherwise this can only be used once a minute.

4 - In Capture Settings, Records, added a new 'Line or Record End' of 'CR / LF' as an alternative to CR or LF. Because ComCap normally strips non-ASCII characters one or other is normally fine, but CRLF is safer when capturing packet type data containing non-ASCII values. Also, a form feed character is no longer treated as a line end unless 'Carriage Return' is specified.

5 - Added support for the GPS Tracker Communications Protocol GT02, that is used by Concox TR02 vehicle trackers that combine GPS, GPRS and GSM in a small 12V driven package designed for mounting in vehicles. This device is programmed by SMS messages and returns location and movement information to a TCP/IP Server. To keep mobile data cost low, it only sends location during movement, although it does return periodic handshakes while connected. ComCap needs one TCP/IP Server channel configured for each simultaneous device that will connect, all with the same local IP and port, then Channel Settings should have 'GPS Data Processing' ticked with input type of 'GT02 GPS Tracker Protocol' selected, tick 'No Altitude', 'Report No Fix' and 'Report Distance Moved'. On the Records tab, set Line or Record End to CR/LF, on the Logging tab tick 'Log Raw Data'. Two new tick boxes 'Report Real Time' and 'Report Remote IP address' have been added to add two more columns to GPS capture.

For GT02 GPS Tracker Protocol, the last fix is repeated every three minutes for each heartbeat packet, to indicate the tracker is stationary but still communicating. The packet sequence number is reported to ease checking for lost packets. Note the GT02 reports the time a fix was taken, not when it was transmitted. New fixes may be cached by the tracker if not online and sent together when an internet connection is re-established, or an old fix may be sent when a new connection is made. Fixed a problem that meant the GPS Map was not updated for a merge channel. For the GT02 protocol, the captured columns are:

- 1 - Channel Name
- 2 - Latitude
- 3 - Longitude
- 4 - Altitude - optional
- 5 - Distance - optional
- 6 - Speed
- 7 - Course/Direction
- 8 - IMEI ID
- 9 - Packet sequence number
- 10 - Fix time stamp
- 11 - Real time stamp - optional
- 12 - Remote IP address - optional

```
"GPS Concox UK",533312,166660,0,0,8,8,"358899053800739",363,
"2015-05-07T19:26:09","2015-05-08T12:30:12","212.183.128.151"
```

where optional columns are determined by tick boxes. Note the TR02 does not provide altitude information so this field is missing. Also the test unit in the UK is returning time at GMT+5 and the documentation does not offer any SMS commands to set the time zone. Once, the tracker also lost the ComCap server IP address and had to be reprogrammed via SMS.

The right click menu option 'Log GPS info' will put general information from the TR02 device into the Information Log, as follows, with satellite info cut:

```
Sensor ID: 358899053538305
GSM Signal Level: 4
Voltage Level: 5
Location Area Code: 0195
Mobile Network Code: 0
Mobile Cell Id: 0
Satellites in View = 13
```

Satellites Used = 13
True Heading = 88
Magnetic Heading = 88
Satellite 1, Azimuth 0, Elevation 0, S/N 27
Satellite 2, Azimuth 0, Elevation 0, S/N 36

6 - Fixed some cosmetic issues when running ComCap without administrator rights. The hidden Start/Stop buttons now have a caption explaining this, and ComCap Tray will no longer try to restart the service if it stops.

7 - TCP/IP is often not a reliable protocol due to routing issues, sessions may drop expectedly because a router somewhere has been rebooted, re-cabled or many other reasons. ComCap therefore attempts to re-establish any TCP/IP Client connections that are unexpectedly terminated. In existing releases, there are two immediate attempts to reconnect, after which the number of further attempts and delay between them is defined in the grid in Common Settings, Network (zero attempts means keep trying for ever). This release adds a new tick box on the Common tab, 'TCP/IP Client, No Immediate Retry on Disconnect' which applies to all channels, capture and echo, and prevents those two immediate retries so the first retry is after 'Wait Seconds'. Some appliances may be unable to cope with an immediate reconnect.

8 - Fixed a problem with echo and SSL TCP/IP Client, that meant SSL certificate checking was still done even if specified to be ignored, which prevented a connection with a self signed certificate.

9 - Improved SSL support for DH and ECDH key exchange, which allows Forward Secrecy ciphers to be implemented. In Common Settings, Common, a new 'SSL Server DH Params' file name is specified, defaulting to comcap-dhparams1024.pem which is supplied with ComCap. In Channel Settings, Network, 'SSL Server DH Params' is also specified, with 'SSL Server ECDH Key' which should generally be set to Automatic. Note both client and server need to support these key exchanges for negotiation to work. Similar improvements are in ComGen. Updated OpenSSL libraries to the latest 1.0.2d versions with all the latest security fixes. If Forward Secrecy is important, you should create your own DH Params file using the OpenSSL tools.

10 - When SSL is configured for capture or echo, the channel descriptions now mention SSL, in case the channel name does not.

11 - When starting, ComCap now reports more information about the PC local IP addresses, including the network adaptor names. ComCap also now reports any changes to IP address configuration on the PC, such as IP addresses being added or removed, but does not yet stop any channels that will fail due to an IP address being removed.

12 - The 'Test RS232 Signals' is now called 'Test Serial Ports and Hardware Events' and has been redesigned with a list view detailing all the properties of the installed serial RS232 ports, with greater detail about each port. Clicking on a port will attempt to start monitoring of that port. Hardware changes as USB ports are connected or removed will be shown.

13 - ComGen now uses the correct local IP address for added masked text, when there is more than one.

ComCap Release 4.13 - July 2014

1 - This is a major release of ComCap, with several new important features: dynamic serial RS232 port detection, SSL/TLS encryption and certificates, IPv6 support, SMTP email capture, GPS NMEA 0183 parsing, GPS Location Sensor channel, new map window, and better support for tablets and touch screens.

2 - When ComCap was originally designed all PCs had fixed serial RS232 ports and these were

detected only when ComCap started. Fixed serial ports with DB9 or DB25 connectors are now rare, with removable USB, virtual and Bluetooth serial ports common, so ComCap now dynamically detects serial ports as they come and go. The Serial Ports grid in Common Settings now shows all ports installed on the PC including those currently removed and unusable, which are typically USB serial ports that are unplugged. So capture can now be set-up and started for ports that are currently removed, and will start immediately the USB device is plugged into and becomes available to Windows. Likewise capture will be paused if a serial port disappears, and restart if it re-appears. This change also fixes a problem they caused some Bluetooth serial ports to be ignored.

3 - In Common Settings, Serial Ports, the grid now shows an extra column Hardware that displays the port Friendly Name as seen in Device Manager. If the serial port is not currently usable, 'REMOVED' precedes the name, but the port may still be configured. The Info Log reporting of serial ports has also been improved with more details about the ports, which may help identification, ie:

```
COM1, Enabled=Y, Communications Port, (Standard port types), Serial0
COM3, Enabled=N, Prolific USB-to-Serial Comm Port, Prolific, ,
USB\VID_067B&PID_2303&REV_0400,Port_#0001.Hub_#0003
COM4, Enabled=N, CyberSerial 950 16C950, SIIG, , OXPCIMF\*PNP0509
COM11, Enabled=Y, D-Link DU-562M External Modem, CXT, Winachs0,
USB\VID_0572&PID_1300&REV_0100,Port_#0007.Hub_#0004
COM12, Enabled=Y, Enhanced Communication Port, Oxford Semiconductor, OXMF0,
OXMF\*PNP0501, oxmf bus, port 0
COM24, Enabled=N, Standard Serial over Bluetooth link, Microsoft, ,
BTHENUM\{}_VID&0001000f_PID&1200,
COM26, Enabled=Y, USB Serial Port, FTDI, VCP0, FTDIBUS\COMPORT&VID_0403&PID_6001,
CNCA0, Enabled=Y, com0com - serial port emulator, Vyacheslav Frolov, com0com10, com0com\port,
CNCA0
```

where COM1 is a motherboard port, COM3 is a removed USB Prolific port, COM11 is a USB modem, COM12 (and COM13 to COM19) are an 8-way MRI PCI card, COM4 to COM10 are the same card with older non-signed drivers so disabled. COM24 is a Bluetooth serial port, COM26 is a USB FTDI port. The VID_x strings may be used to Google search for unknown hardware device identification if looking for new drivers. Enabled=N means the port is removed, usually an unplugged USB device, but could be a removed PCI card. Port and hub may identify USB ports. Beware if a USB device is plugged into a different socket, it will often be installed as a new COM port.

4 - With the 64-bit editions of Windows 7, 8, 2008 R2, 2012, and later, Windows will no longer accept unsigned drivers for serial port expansion products such as USB, PCI or PCI Express cards. For manufacturers, getting signed drivers from Microsoft is expensive and they are usually only available for products still being manufactured and supported. Some RS232 cards and dongles used for testing ComCap under Windows XP no longer work under Windows 7 64-bit and later, but new signed drivers are now available from Microsoft Update or manufacturers sites for other newer hardware. Specific hardware still working includes:

- MRI 8 way RS232 PCI card using Oxford Semiconductor chips
- Lava 2 way DSerial PCI card
- FTDI USB serial cable
- Prolific USB serial cable (beware cheap imitations)
- Winchiphead USB serial cable

5 - Added SSL/TLS support for ComCap network capture and echo. SSL/TLS provides encryption of data being sent over the internet, and also client and server to confirm the identity of the other party with X509 SSL/TLS certificates. Previously, ComCap only allowed IP addresses to be specified, but SSL/TLS certificates are mostly for domain host names, so a remote host name may now be specified for TCP/IP Client, instead of a remote IP address, provided family is set to 'Any'. Beware specifying a host name means a DNS look-up needs to happen before capture can start, which potentially can fail. Note that SSL/TLS is not supported for UDP, and that a certificate is required for TCP/IP Server to provide the private and public encryption keys. TCP/IP Client does not need a certificate, unless the

server specifically want to check the identity of client, which ComCap does not yet support.

6 - In Common Settings, a new Common tab has various default SSL/TLS settings, some of which can be overridden in specific Channel Settings. Common Settings allows default SSL Server file names for X509 'SSL Server Certificate', 'SSL Server Private Key' and optionally 'SSL Certificate Authority' to be specified. 'SSL Client Verify Certificate Mode' may be set to None, PEM Bundle File or Windows Cert Store. The PEM Bundle File is a file supplied with ComCap with a few hundred root certificates:

```
C:\ProgramData\Magenta-Systems\ComCap4\Certificates\RootCaCertsBundle.pem
```

while Windows Certificate Store is a similar Microsoft store used by Internet Explorer and other applications. For the store only, certificate revocation can be checked, beware this requires internet access and can take several seconds, or longer. The checked certificates may be logged similarly to:

```
telecom-tariffs: 3 SSL Certificates in the verify chain:
```

```
Depth #1 Verify Result: ok
Issued to: www.telecom-tariffs.co.uk,
Alt Domains: www.telecom-tariffs.co.uk, telecom-tariffs.co.uk
Issuer: RapidSSL CA, GeoTrust, Inc.
```

```
Depth #2 Verify Result: ok
Issued to: RapidSSL CA, GeoTrust, Inc.
Issuer: GeoTrust Global CA, GeoTrust Inc.
```

```
Depth #3 Verify Result: ok
Issued to: GeoTrust Global CA, GeoTrust Inc.
Issuer: Trusted Root
```

```
Echo Send: 1 SSL Certificates in the verify chain:
Depth #1 Verify Result: self signed certificate
Issued to: logs.comcap.co.uk, ComCap
Issuer: Self Signed
```

The first example is public certificate, the second is a test certificate supplied with ComCap. Note the Common Settings determine if and how remote server certificates are checked, each channel has an extra option 'Client Validate Server Certificate' which must also be ticked.

7 - In Channel Settings, Network, a new box 'SSL/TLS - Transport Layer Security' has been added. There are two tick boxes, 'SSL/TLS for Capture' and 'SSL/TLS for Echo' which specify when SSL/TLS should be used. For TCP/IP Server, the three default certificates from Common Settings will appear, but may be changed for individual certificates if necessary. For TCP/IP Client, 'Client Validate Server Certificate' should be ticked if this feature is needed, provided that 'SSL Client Verify Certificate Mode' is also specified in Common Settings. For TCP/IP Server only, SSL certificates are essential, since they control encryption as well as verification. Note that if capture and echo are both configured as TCP/IP Server, the same certificate is used for both, so the host name should be the same for both. Although an SSL certificate is generally issued to a domain host name, ComCap will be unaware of this host name, only the IP address can be specified. Note there is no automatic SSL/TLS negotiation, both ends of the connection need to support SSL/TLS (or not) for a connection to work, if one end does not support SSL/TLS, the connection will fail without any real error. ComCap now uses the latest 1.0.1h OpenSSL libraries with all the latest security fixes, it was never distributed with the earlier flawed 1.0.1 libraries.

8 - The SSL certificate files are X509 PEM files, that can be purchased from certificate authorities for a domain name that point to the IP address for the TCP/IP Server, alternatively, ComCap will create free self signed certificates. Clicking the 'Create SSL Certificate' button brings up a new window allowing either a certificate request for a certificate authority to be created, or a self signed certificate. For the latter, most of the certificate fields may be left as defaults since the certificate will not be used to

identify identity, but is ordering creating a CA Request the details should be carefully entered, particularly the Common Name which is the host domain name to be secured. When 'Create' is clicking, two small text files will be created in the Certificates sub-directory, with the specified file prefix, and the fields on the Network tab updated for the new certificate files. For a CA Request, the file ending with 'certrequest.pem' should be opened in a text editor and the base64 block from '--BEGIN CERTIFICATE REQUEST--' copied to the certificate authority web site when requested. Once approved, the CA will return a file with a block '--BEGIN CERTIFICATE--' which should be specified as the certificate file. ComCap generates a second file ending with 'prvkey.pem' with '--BEGIN PRIVATE KEY--' which should not be sent anywhere. If a Self Signed Certificate is generated, ComCap creates a file with suffix 'cert.pem' with '--BEGIN CERTIFICATE--' instead of the CA request. With a CA certificate, there will be one or more certificates for the authority itself, that were used to sign the server certificate (a certificate chain or bundle) and the file containing one or more '--BEGIN CERTIFICATE--' blocks needs to be specified as 'SSL Certificate Authority' in ComCap. For an SSL connection, the information log will report 'Starting SSL Handshake' when the connection is made but won't start accepting data until 'SSL Connected OK with TLSv1, cipher AES256-SHA, 256 secret bits' is reported. If handshaking fails, the connection attempt will retry.

9 - Added IPv6 support for ComCap network capture and echo. IPv6 is the next generation of IP addresses that will increasingly become used as the present IPv4 ranges are depleted. Windows XP and later all support IPv6, and it's usually enabled as standard on recent PCs with Windows 7 and 8. In Common Settings, Common, there is a new tick box 'Support IPv6' must be set before any IPv6 addresses may be entered in the Network tab grid. A new network column 'Family' allows Any, IPv4, IPv6, Any IPv4 or Any IPv6. Any IPv4 will set the address to 0.0.0.0 while Any IPv6 sets the address to ::. Local IP Address offers a list of configured IPv4 and IPv6 addresses. If a remote host name is specified instead of an IP address, set Any and the family will be detected once the IP address has been looked up from a DNS server, if both IPv4 and IPv6 addresses are offered, the first is used. In Channel Settings, Network, the Local and Remote Echo IP Addresses or Host Name may be specified as IPv6 or IPv4, and the family will be set automatically.

10 - IPv6 addresses starting with fe80:: are LAN addresses usually automatically generated for each PC on the LAN, while addresses starting with 2 are public routable IPv6 addresses. Sometimes the fe80 addresses are shown with %xx at the end, which should be removed when entering them. For display and reporting, ComCap follows the convention of enclosing IPv6 addresses in square brackets, ie [fe80::136:4a6b:870b:e19] to distinguish them from dotted IPv4 addresses, but the brackets are never entered in fields. Each time ComCap starts, all the IPv4 and IPv6 addresses configured for the PC are reported in the information log.

11 - Added SMTP email capture, intended to capture alert emails sent by internet aware appliances, such as firewalls, security monitors, power distribution units, uninterruptible power supplies, remote sensors, transponders, etc. The emails may be written to a SQL database or used to trigger alerts.

12 - In Common Settings, Network, there is a new 'IP Protocol' of 'Email Server' for which a single local address should be selected, usually with port 25 or 587, with remote IP address left as 0.0.0.0. Internet appliances that will send email to ComCap should have their SMPT Mail Server changed to this local IP address, or set-up DNS for this address.

13 - In Channel Settings, Email, a new 'SMTP Email Server' box adds several more configuration options. 'Email Account Names Accepted by Server' is a list of email addresses for which the server will accept email, these don't need real domains so info@comcap.private is acceptable, or *@comcap.private would allow email from any address with that domain, ie xxx@comcap.private. 'Remote IP Addresses Accepted' allows restriction from which IP addresses email will be accepted. 'Server Requires Authentication' allows a single login name and password to be specified that will be required before email can be accepted, support AUTH PLAIN, LOGIN, CRAM-MD5 and CRAM-SHA1 methods.

14 - Accepted emails can be captured as multiple lines of plain text, or by ticking 'Save as Variable Named Columns' as a single record, ie each line of the email is formatted similarly to Subject="ComCap email testing" so ComCap Data Format parsing can separate the headers to be

added to a SQL database. Three extra headers are always added, X-Envelope-From, X-Envelope-To and X-Originating-IP all from the SMTP envelope, in case the normal To: or From: headers are inadequate, and Date is converted to ISO format. The entire body becomes Body='xxx' with line endings replaced by \n or if 'Remove Body Line Endings' is ticked by spaces. Unfortunately ComCap can not currently process CRLF in a record, it breaks too many things, but \n can translated back to CRLF in a SQL stored procedure if necessary. Note that MIME encoded emails are automatically decoded, and only text-plain and text-html sections processed. The maximum email size that is accepted is 32,000 characters, and SQL will usually only handle a field 8,000 characters long so that is really the maximum body size. Ticking 'Show All Headers' will capture all the email headers, otherwise only From, To, Subject and Date are shown. 'Ignore Email Body' only saves the email headers and might be sufficient where the subject contains the alert information. 'One Log File Per Email' causes capture log rotation for each new email provided the file name format is suitable. 'Save Raw Email as EML File' causes each complete email to be saved separately to the capture file but in the same folder, with a unique file name, where it could be processed by another application. 'Relay Raw Email' causes the complete email to be forwarded to one or more email addresses specified as 'To Addresses' (same as emailing logs). Since email formats vary so wildly, conceptually saving them with ComCap can cause many issues. Hopefully the 'Variable Named Columns' format and other options described are a good start, but ComCap users are welcome to offer feedback on alternatives from the real life emails generated by various appliances. To demonstrate saving emails to a SQL database, a new Microsoft SQL Server table capture_email has been added to 'newdb-mssql.sql' and matching stored procedures to 'storedproc-mssql.sql'.

15 - Added GPS (global positioning satellite) support by parsing the NMEA 0183 sentences commonly generated by GPS receivers into simple comma separated records, allowing location information received from a serial or network connected GPS sensor to be easily saved to a database. For diagnostics, satellite information may also be saved to the information log on request. NMEA 0183 sentences processed are: GGA, GSA, GSV, RMC, GLL and VTG, others are ignored. In Channel Settings, General, a new box 'GPS Data Processing' should be ticked, on the new GPS tab the input and output types may be specified, also the minimum interval in seconds between reports, and the maximum interval before an old report will be repeated if nothing new, or a minimum movement in metres before a report will be made (all designed to reduce repeat data captured). A typical captured line may look like:

```
"GPS COM20",51.38325,-0.08605,76,2,"2014-06-23T17:44:16"
```

with the channel name, latitude and longitude in decimal degrees, altitude, distance in metres since last report, time stamp report captured as sent by remote device (might be UTC). For the UK only, degrees may be replaced by UK NGR Northings/Eastings in simple metres. Future releases may add support for parsing other data formats, including GPSD JSON and GPS Exchange XML tracks, and saving data in these formats. Most testing was with a GlobalSat BU-353-S4 USB GPS Receiver, a two inch diameter device with a roof magnet that presents as a Prolific serial port (a version with a real serial connector is also available). Also tested were a battery operated GlobalSat BT-359 Bluetooth CoPilot GPS device (but Bluetooth serial ports are not always very reliable) and NMEA 0183 streaming from a Nexus 7 Android tablet. To demonstrate saving GPS data to a SQL database, a new Microsoft SQL Server table capture_gps has been added to 'newdb-mssql.sql' and matching stored procedures to 'storedproc-mssql.sql'.

16 - Added a new GPS Location Sensor Channel to support Windows tablets and high end laptops that have a GPS location sensor built-in that supports the Windows Location Service allowing sharing location information between applications. In Common Settings, Common, tick Enable Location Sensor and enter a Capture Name. Note these settings may not be available if the service is not installed, and may give an error when started if there is no GPS sensor. Otherwise configuration is similar to GPS support detailed above, except that little diagnostic information may be available, the Asus VivoTab Note 8 tablet used for testing does not provide any satellite information.

17 - A new GPS Map window has been added for channels with GPS Data Processing enabled, that uses Google Maps to display the track taken as new GPS locations are processed, provided an internet connection is available to download the maps. This window is accessed from the right click

menu for a channel and requires internet access to download the Google maps.

18 - Fixed a nasty bug when capturing to a database where, in some circumstance, capture got stuck in a loop trying to open the database and closing it again, introduced in 4.11.

19 - When the user clicks buttons and menu options to stop or pause Capture, these are now logged to make diagnostics easier.

20 - In Common Settings, a new option 'Stop PC Sleeping' may be ticked to try and stop Windows placing tablets and laptops in sleep mode, but testing shows Windows may ignore this setting, unfortunately.

21 - Fixed an initial set-up bug that meant sometimes there was no live display of successfully captured data. This happened if ComCap was initially accessed and exited without setting up any capture channels, and then only a single channel was set-up. The problem did not happen if two or more channels were configured.

22 - ComCap has been successfully tested on an Asus VivoTab Note 8in tablet running Windows 8.1. Using a stylus instead of mouse or fingers provides the precision to click all menus and buttons.

23 - ComCap now correctly displays Windows 8.1 as that version, rather than Window 8, likewise Windows 2012 R2 instead of Windows 2012.

24 - The Common and Channel Settings windows are now both resizable, both larger and smaller, larger to get more channels on the screen, if smaller scroll bars now appear to allow settings to be made on screen with small dimensions. All Windows have now been testing with 125% fonts and repositioning done where text was unreadable. When first accessed, particularly when using font sizing larger than 100%, it may be necessary to drag the bottom right corner of Windows down so all the items in the window become visible.

25 - To ease access, ComCap now supports an optional global hot key to display or hide the ComCap window, as an alternate to clicking the ComCap icon in the system tray. The exact key combination is configured in Common Settings, Capture Logging. If the PC has a touch screen, the hot key will default to ALT-C. Within ComCap, the F1 and F2 keys will now start and stop capture, as an alternate to the normal buttons.

26 - When setting up a new UDP Server channel, Line or Record End now defaults to 'Packet' which is common for that protocol.

27 - in Common Settings, after configuring serial ports, the serial mouse driver is now automatically disabled. This prevents a stream of serial data (such as GPS) being detected as a mouse during the boot process, and stopping it being captured.

28 - With TCP/IP Client channels, if the remote server is not available and ComCap is set-up to periodically attempt to reconnect, ComCap now correctly shows the channel as paused, and allows immediate resume to trigger another connect attempt, rather than waiting until for the next scheduled attempt.

29 - Fixed various bugs relating to the display and network echo of captured lines longer than about 800 characters, the data itself was always written to files safely.

30 - In Channel Settings, Records, there is a new 'Line or Record End' option 'Blank Line'. This is designed to allow multiple line non-blank records to be captured as a single long line when a blank line is reached. Specifically, Nortel telephone switches generate call data records (CDRs) comprising three lines of call data following by a blank line, and this new option allows such records to be captured as a single long line making subsequent processing such as adding to SQL much easier. Note a blank line is considered as CRLF CRLF.

31- In Channel Settings, Records, the 'Line or Record End' option 'Multiple Tags' now correctly supports escaped controls \n, \c and \l for new lines, CR and LF, previously these were removed before tags were checked. So a tag of '\n\n' would have the same effect as the new 'Blank Line' record end, '\n\n\n' would need two blank lines, etc.

32 - Fixed some problems correctly reloading settings when these were changed while capture was running. The service version no longer restarts capture if settings are changed while capture is paused. The Settings menu no longer disables entries unnecessarily.

33 - Fixed a problem introduced in 4.5 that stopped Send Data being able to Send a File from the interactive desktop version of ComCap only, this continued to work when using the service version. Note that Send File is only currently supported for TCP Client and TCP Server, not UDP or Serial.

34 - Fixed a long term problem with Echo to Windows Printer. If this option was somehow configured but Windows no Longer had any installed printers, it was not possible to access Settings to change Echo back to none. If a specific printer is removed, ComCap should revert to the default printer.

35 - When selecting a new table or stored procedure, the data format fields are now automatically reloaded, rather than needing the 'New Columns' button to be clicked.

36 -- In Capture and Common Settings, more fields which are disabled due to being unavailable or not configured are now shown greyed to make it more obvious they can not be accessed.

37 - The Test RS232 Signals and ComGen tools have been updated for the same new serial port detection capabilities as ComCap.

38 - ComGen has been updated to support IPv6 and SSL/TLS, with similar features to ComCap for which it is the main testing platform. On the Settings tab, a new tick box 'Enable IPv6' has been added. On the Network tab has two new columns for 'Family' and 'SSL Enable'. If SSL is enabled for TCP Server, the certificate files should be specified on the Options tab, and a self signed certificate can be created if needed. Note the same certificate will be used for all ComGen TCP/Server channels. A remote host name may now be specified for instead of a remote IP address, provided family is set to 'Any'. Note that TCP/IP Client certificate is not support by ComGen, which is only a test tool.

ComCap Release 4.12 - April 2013

1 - Improved Capture Settings, Logging, 'Add Escaped Text' to be able to freely format dates and times, similarly to 'Time Stamp Each Line'. There is a new escape sequence \{} which allows the same time and date mask characters as supported by time stamps and capture file names to be placed between the two curly bracket. So \{hh:nn:ss.zzz} will add a time stamp as 12:59:06.720 and \{yyyymmdd}-"hhnnss} would give 20121101-124906.

2 - In Channel Settings, Logging, a new tick box 'Ignored Lines to Info Log' causes line ignored by 'Validate Line Length' or 'Ignore Lines with Phrases' to be logged to the information log instead. Note this is really for debugging, the info log might get large if a lot of lines are ignored. Lines ignored for 'too many' are not logged since this defeats the purpose. This option also logs printer control sequences removed.

3 - In Channel Settings, Records, 'Remove Printer Control Sequences' offers various means of cleaning up data captured from older computer printer output. 'HP PCL, PJJ, GL/2 Escapes' removes the codes used by most Hewlett-Packard printers and many others emulating them, including fonts and raster graphics. 'Ansi/Epson Matrix Escapes' removes codes mostly used by old impact printers, note there are many permutations of these codes and only the most common codes are handled. 'Vertical Movement to Line End' converts PCL cursor movement to a line end, 'Horizontal Movement to Space' converts PCL cursor movement to a space, 'Horizontal Movement to Tab' converts PCL cursor movement to a tab. Ticking 'Ignored Lines to Info Log' causes any removed printer controls (except

binary and graphics) to be logged for debugging purposes. Beware printer drivers can use massive amounts of cursor movement, even placing each word or character individually on a page, so captured data may not be as expected.

4 - In Channel Settings, Logging, a new tick box 'Remove Hi-Bit Characters' filters out any characters with the hi-bit set, above ASCII 127. This complements 'Remove Control Characters' and may help clean up corrupted modem data.

5 - In Channel Settings for Merge channels, more settings are now disabled since they are only effective on the original capture channel, before merge occurs.

6 - In Common and Channel Settings, any errors updating the ComCap configuration files are now correctly reported. Usually this will be 'access denied' due to file security modify permissions not allowing the current user to update settings. It is now also possible to cancel from this error. All settings errors now also appear in the Information Log for clarity. If the file access denied error occurs, use Windows Explorer to give modify permissions to the current to all files in the ComCap4 ProgramData directory shown in the info log window.

7 - In Common Settings, Capture Logging, if ComCap is being used by a logon without administrator privileges it is not possible to enable or disable the Background Service so the tick box is greyed out and a caption has been added to explain this.

8 - The Windows minimise button in the title bar now reliably hides ComCap, previously it worked only the first time it was used.

9 - The ComGen data generator tool is now able to send binary files as well as text files, specifically printer files containing fonts and raster graphics. It sends blocks of 100 bytes as a line. Also fixed a problem selecting file names.

ComCap Release 4.11 - January 2012

1 - Fixed a bug introduced in release 4.10 that prevented Remote Address details being specified or changed for 'Echo Types' of TCP Client, TCP Server and UDP (Syslog). If previously set-up, these features still functioned correctly.

2 - Fixed a bug introduced in release 4.10 that stopped ComCap starting on some PCs with older operating systems that did not have recent Thawte root security certificates installed through Windows Update.

3 - Fixed a bug introduced in release 4.6 that prevented more than a single remote connection to Echo TCP/Server, when it should have allowed five remote connections. Also improved the error messages to provide a banner to the remote client when a connection is refused and log it locally as well. Fixed a bug with multiple remote connections, that caused echo to stop for all connections when just one connection dropped.

ComCap Release 4.10 - October 2011

1 - Fixed a bug introduced in release 4.8 that meant the date and time added to a captured line with the 'Time Stamp Each Line' setting was the time the previous line was captured, or blank for the first line. This bug did not effect the date and time added by the more versatile option 'Add Custom Text to Captured Lines'. This bug unfortunately also effected database time stamps.

2 - Fixed a bug introduced in release 4.8 when changing Common Settings while capture is still running, such that disabling Background Service mode did not always stop the ComCap service first. If Channel Settings are changed while a channel is paused with the service version, the new settings

are correctly used. This previously only worked if the channel was stopped or running, not paused.

3 - Fixed a database bug introduced in release 4.9 that sometimes caused an error to appear after successfully adding a database row using the 'Insert into Table' option, which then caused a second attempt to add the same row, causing further duplicate key errors.

4 - Fixed a possible database issue introduced in release 4.9 that may have caused excessive CPU use and/or large log files when repeatedly trying and failing to add bad records to a database. Retries are now slowed down with a maximum of about 1,000 attempts before a record is abandoned. Note the 'Ignore Records That Cause Error' always stopped these retries.

5 - Fixed a long term issue with the service version putting two meaningless entries in the Windows Event Log each time ComCap started.

6 - Fixed a bug with TCP Client that meant retry attempts could stop after certain unexpected socket connection errors, so capture stopped.

7 - In Capture Settings, Files, a new Log Name Format of 'Prompt on Start' has been added which allows a specific file name to be specified each time capture is started. Setting this option automatically sets 'Fixed File Name', and can only be done if ComCap is not specified for Auto Start or to run as a Background Service, since ComCap would never actually start. This feature is intended for applications where data is being captured from a single device for a specific purpose, such as a laboratory test. The 'Add Comment to Log' right menu option might also be useful to add information to the capture log.

8 - Added a new setting to improve performance when capturing high speed TCP and UDP traffic. In Capture Settings, Network, a new Network Performance box has 'Capture TCP/UDP Buffer Size (KB)' and 'Echo TCP/UDP Buffer Size (KB)', both which default to 8 which means 8KB (8,192 bytes). These buffers are where TCP/UDP temporarily saves received or sent data before ComCap is able to process it. With TCP, if data is not extracted from the buffer, the speed at which data is received will slow down, but with UDP received data is simply lost since there are no handshaking packets to confirm data needs to be delayed or resent. It should only be necessary to increase the capture buffer size if a lot of data is being received each second, maybe 16K/sec or more, or if the PC is very slow or has other CPU intensive applications so that ComCap can not get the CPU it needs. Note these new settings only appear for channels actually listening or sending data, not filter or merge channels.

9 - If using the 'Email Capture Log on Rotation' feature, there are now four new tick boxes to specify which title lines are added to the email body, to potentially keep the email simple. These four titles are 'Title and Date', 'From PC Name', 'Capture Name' and 'Log File Name'.

10 - Increased the maximum data loss checking period from 999 to 9,999 minutes, to allow for data arriving once a day (1,440 minutes), such as a new date in a telephone log. The logs now show the data loss period in hours or days, after one hour. Note that the period starts from when ComCap capture was last started, if later than the actual last line.

11 - When ComCap starts, it now checks the program's digital signing certificate to ensure the program file has not become corrupted in such a way that it might behave unpredictably, and instead gives a warning and refuses to start. If this happens, please inform Magenta Systems Ltd so the corruption cause can be identified. The Windows and ADO versions are now logged when ComCap starts, to ease problem finding.

12 - In the main Window, the 'Scroll Tabs' feature is now only automatically enabled if there are more than 100 capture channels, rather than 32 at present. This allows simpler single click tab channel selection for more channels, if the capture window is sufficiently large to display all the desired tabs.

13 - Fixed a possible issue with Windows 7 where dates may have been formatted in default USA format, when a different locale was specified during initial Windows installation and not changed subsequently.

14 - It is no longer possible to email capture logs larger than 10 megs in size. If the SMTP mail server gives an error with the email being too large, retry attempts are now skipped to avoid continual failures. Restored mail queue logging, lost in release 4.8.

ComCap Release 4.9 - May 2011

1 - The unlimited version of ComCap now supports a maximum of 999 capture channels. This resolves an issue with PCs with more than 500 serial COM ports. For those wondering how any one PC can support so many COM ports when most how have just one, the answer is a rack of ethernet Serial Device Servers and hundreds of virtual COM ports.

2 - Merge Channels have been added as a way of combining or consolidating captured data from multiple Network and Serial channels. It is effectively a new form of capture data Echo. This will benefit applications capturing data from multiple sources, allowing all data to be displayed in a single window, written to a single log file, and added to a database using a single connection instead of one for each channel. One record at a time is merged, which may be one or more lines depending on the capture channel 'Line or Record End' setting (there is no record setting for merge channels).

Most channel settings apply equally to capture and merge channels, but generally should not be duplicated. Some effort may be needed to avoid duplicate data being merged from different channels. With 'Add Custom Text to Captured Lines', the network or serial channel setting should be used to add a channel name, remote IP address, or device id, while the merge channel could add date and time and serial number so they are unique for the channel. Note that currently if a merge channel is paused, the capture channels continue but data is not merged.

Merge Channels are set-up on the new 'Merging' tab in Common Settings, with a unique channel name, then a 'Merge From' name that is partially matched against Network or Serial Channel names, ie the partial name 'Weather' would match channel names 'Weather 1', 'Weather 2', 'Weather 3', etc. The 'Total' column shows how many channel's data will be merged.

3 - A 'New Log Interval' of Each Record/Line has been added, which will create lots of short log files each with a single line or record. This is really intended for capturing multiple line data such as remote alarm reports rather than high speed tabular type data. One disadvantage of this option is that when changing capture tabs to view previously captured data, only the data from the last file will be restored, which means just one record.

4 - A new 'Custom Log Name Mask' of \# will add the current serial number to the mask, which may be used instead of date and time for unique sequential file names. Previously custom masks had to include yy or yyyy for year, but this check has now been removed to allow more flexible file naming. Beware that sensible masks should still be used, to avoid duplicate file names.

5 - A new 'Line or Record End' of Timeout/Disconnect has been added. Previously the same effect could be achieved by specifying a special character that was never expected. This is intended for capturing multiple line data such as remote alarm reports, which arrive as a burst of data, separated by a gap from the next report or by serial lines dropping or TCP channel disconnecting.

6 - The main File menu has a new option 'Disable Alert Sound'. with a similar tick box in the Alert Window, which may be used to temporarily stop audible alerts driving you mad with repeated errors being reported. Fixed a long term problem that meant audible alerts from the service version of ComCap did not automatically repeat (if so specified).

7 - Totally rewrote the database code to avoid a serious SQL database memory leak issue introduced with Windows 7 SP1 and Windows 2008 R2 SP1, and not yet fixed by Microsoft. ComCap now performs all database processing in a new thread, to avoid using the Microsoft event that leaks memory. This has other performance benefits, since the Microsoft event started and stopped a thread

for each row written, now there is one thread running continually. Separating the database code into a thread also avoids lock-up problems that have rarely been reported, since the thread is monitored and can be restarted if it stops responding after two minutes. Also, the maximum number of database rows that can be written each second will be increased, typically at least 50 rows per second (ie 20ms per row), but less if the stored procedure does a lot of processing or if ComCap is updated the database with more than a few thousand buffered rows when buffer processing slows down updates.

8 - When capturing to a database, there is a new 'Save/Restore Buffered Rows to Disk' tick box. Previously, ComCap only buffered rows that could not be written to a database due to network errors in memory, and they were lost forever if ComCap was stopped before the database connection was successfully restored. With this new option, the buffered rows are saved to a file (in the same directory as the config files) when capture is stopped (but not paused) and restored to the buffer when capture is started again. The actual file name is reported in the info log file. Beware this may cause a problem if the database format is changed so the buffered rows are no longer valid, so just delete the file.

9 - The com0com serial port null modem emulation included with ComCap has been updated to version 2.2.2.0, and there is now a second signed version that may be installed on 64-bit versions of Windows. Note com0com is an open source project and has not been tested by Microsoft WHQL, so skip the security alerts that appear during 64-bit installation. Previously com0com could not be used on Windows 7 and 2008 R2 64-bit due to not having its driver signed.

ComCap Release 4.8 - January 2011

1 - It is now possible to change ComCap settings without first stopping capture. If settings are actually changed, the user is prompted to restart capture for a single channel or all channels, depending on what was changed, but this may be skipped and capture restarted later. Previously, settings tabs without any active settings were hidden until their features were enabled by various tick boxes (such as Save to Database, Check for Data Loss, etc). To make these settings more obvious, the tabs always appear but instead the options on them are disabled until needed.

2 - Email support has been improved to better ensure that alert emails are not lost due to internet problems or ComCap being stopped. A mail queue has been introduced, with extended retries potentially over 24 hours or more, so email alerts will not be lost if ComCap stops for any reason. The implication of the new mail queue is the use of temporary files to hold queued email, the root directory for which needs to be specified in Common Settings, Email. The previous simple retry attempts setting has been replaced by a comma list of 'Minutes Between Queue Attempts', ie 2,3,5,5,10,etc, which means retry attempts will take place 2, 5, 10, 15 and 25 minutes from when the email was queued, with one attempt for each of the two SMTP Servers, if both specified. Note that some email servers support grey listing and reject the first email attempt from a new sender but allow a retry 10 or 15 minutes later, something that is very effective in blocking spam emails (since they don't usually retry). Also note the email queue is only running while ComCap is running, but if ComCap is stopped it will make one attempt to send any pending emails (such as logs emailed on close, see below) within 30 seconds (but not for longer since Windows might be closing ComCap to reboot).

3 - Email support has further been improved by allowing separate authentication details to be specified for the two SMTP servers, which might be different ISPs, with new Authentication options such as NTLM, and by supporting secure email using SSL/TLS which is required by services such as Gogglemail. 'SSL/TLS Connection' should be used with SMTP Port 465 and forces an implicit TLS connection to this port. 'SSL/TLS Authentication' normally uses port 25, but will check if the server returns a STARTTLS response to indicate it supports SSL/TLS authentication at which point a secure connection is established instead. Note that the SMTP server SSL certificate is not currently checked. To support SSL/TLS, two new files are included with ComCap, libeay32.dll and ssleay32.dll.

4 - Many ComCap users further process capture logs, sometimes with difficulty due to the files being continually updated, so set short new log interval or rotations so new files are created regularly. To

assist this, ComCap now has a new Capture Setting on the Files tab, 'Archive Capture Log on Rotation' which causes a closed log file to be moved to a specified archive directory on the same disk drive. This will potentially avoid conflicts since the other processing application will only find completed capture logs, and not those still open. A further option 'Archive/Email Capture Log on Stop Capture' causes the log to be archived even if the rotation time has not yet arrived when ComCap is stopped. If ComCap is restarted before the next rotation time, a new log with the previous name will be created, but when it is finally archived it will be renamed by the addition of -1, -2, etc, to the file name to avoid a conflict with previously archived log file names, if any. To FTP a capture log, use our DUN Manager application which offers various Scheduled Tasks including FTP Upload which will automatically FTP any files it finds in a specified directory and then move them elsewhere so they are not sent again.

5 - Capture logs may now be automatically emailed when closed and rotated. There is a new tab Capture Setting, Email, with 'Email Capture Log on Rotation' as 'Email as Body' or 'Email as Attachment, depending on the requirement. An 'Email Subject', 'From:' and multiple 'To:' addresses may be specified. On the Files tab, 'Archive/Email Capture Log on Stop Capture' causes the log to be emailed even if the rotation time has not yet arrived when ComCap is stopped.

6 - The maximum captured line length has been increased from 2,048 to 20,000 characters, while the default length has been reduced to 256 characters. The Maximum Line Length is that beyond which a line is forcibly wrapped to the next line. There is also a Maximum Validated Line Length, which is used to ignore line which are too long, but without wrapping them.

7 - A new feature 'Ignore Too Many Lines' has been added, which may be used to reduce the amount of data captured from devices sending continuous streams, such as GPS locators or environmental sensors. A 'Line Time Gap' in fractions of a second may be specified during which any new data will be ignored. If the gap is set to 0.50 second, then only a maximum of two lines per second will be captured, or it may be one line every few seconds. The number of lines ignored are still counted and reported. This feature may be used to slow down database updates by ignoring data arriving too fast.

8 - When adding custom text to captured lines, a new escape \T has been added which gives a long time with milliseconds to three decimal places, ie 10:22:56:586. Beware Windows is not millisecond accurate, due to multi-tasking.

9 - The 'Info Messages in Capture Log' preference has been removed, due to recent testing showing potential sharing and reentrancy problems where an attempt is made to log error messages about capture logs to the capture log itself.

10 - In Capture Settings, Filters and Alerts, leading and trailing spaces are now removed from the filter phrases.

ComCap Release 4.7 - August 2010

1 - Made some improvements to automatically restart the ComCap service if it stops unexpectedly due to an error or is manually stopped for some reason. When the service version is enabled through Settings, Common, the service properties now have Recovery set as 'Restart the Service' to avoid needing to set this manually. Note this change only happens if the existing service is disabled through Settings, Common, and then re-enabled. Also, provided the user is logged-on and the tray version of ComCap is monitoring the service, if the service is found to have stopped an alert will be sent and it will be automatically restarted after 20 seconds, provided the Stop button is not pressed meanwhile. An alert is now sent on start-up if ComCap is found to have previously stopped without a clean close down. Further ComCap monitoring is planned for a future release to ensure ComCap never stops.

2 - In Common Settings, Alerts, a new option 'Control Serial Port' has been added, which causes the RTS and DTR control lines to be raised on a specified RS232 serial port for one or more seconds, whenever an alert is triggered. If the serial port is wired to a low current relay, this output may be used to sound a bell or alarm to draw attention to ComCap.

3 - In Capture Settings, Filters and Alerts, there is a new option 'Ignore Same Alert for (mins)' which works in conjunction with 'Alert for Lines with Phrases' preventing the same alert being sent again until the specified period in minutes is reached. If more than one alert filter is specified, each filter will still trigger an alert the first time it is detected. This will avoid too many emails or SMS messages being sent when the same alert is continually repeated.

4 - In Capture Settings, Files, a new option 'Delete Empty Capture Log on Rotation' has been added, to avoid empty capture logs remaining on disk. Note this only applies to the main capture log, not the alternate.

5 - In Capture Settings General, there is a new tick box 'Log Only First Command Sent' that prevents repeated logging when the Start Command is sent every few seconds or minutes, filling up the info log.

6 - In Capture Settings, Database, a new option 'Escape Backslash (MySQL)' has been added to avoid a problem with old versions of MySQL that treat the backslash character as the first of an escape sequence (ie \f is form feed). This option sends \ as \\ so MySQL saves it as \ instead of reporting a syntax error.

7 - In Capture Settings, Database, a new option 'No Pause for Full Buffer (Ignore Data)' has been added so that capture to log files will always continue even if a database is unavailable, or if the capture rate is so fast that a database can not keep up. This works in conjunction with 'Maximum Rows to Buffer before Pausing Capture' so that once the limit is reached subsequent rows are ignored instead of being buffered, but are still written to the capture log file. This feature is primarily designed to support capture applications that regularly update the same information, such as global positioning satellite data where a vehicle position need not be recorded every second. The number of rows not written to the database is logged similarly to the following:

```
Database Rows Added: 3,990, Database Errors 16, Skipped 113
```

and also reported in the tray application in brackets after the number of DB rows. Note the minimum number of rows that may be buffered is 50, which is required for normal operation where 10 or more rows may be captured as a burst which may be faster than they can be written to SQL.

8 - In Capture Settings, Database, a new option 'Ignore Records That Cause Error' has been added which prevents a row being buffered when a SQL error occurs and the database is closed and re-opened to try and clear the error. This is primarily intended to overcome syntax and duplicate key errors where the database can not write a specific row of data and will get stuck in a repeating loop trying to write the same row again and again. Unfortunately, due to the widely varying error responses from different SQL databases, this feature might cause a row to be lost if the network is lost or the SQL server simply stopped while a row is being written.

9 - Fixed a bug introduced in Release 4.6 for serial capture only that meant a Start Command was only send once and not repeated, instead giving an error each time.

10 - When ComCap starts, the PC local IP addresses are now listed in the info log. When the network configuration is loaded, and capture started, a warning is now given if a configured local IP no longer exists on the PC, due to networking having being changed. Currently, capture will still attempt to start, since other channels may still work, but those channels trying to use a non-existent IP address will give network errors. This mainly effects TCP and UDP server channels set-up to listen on a single IP, rather than 0.0.0.0 for all IP addresses on the PC. On the other hand, if the PC IP has changed perhaps due to DHCP being configured, data directed at the original IP address will not arrive anyway.

ComCap Release 4.6 - November 2009

1 - Fixed a long term problem with TCP Server where multiple channels are being captured from the same IP and port, which caused a problem restarting capture after it was paused (usually for database problems). This was caused by only one channel being paused instead of all related channels, but a

workaround has been found so capture now resumes correctly without an 'Address already in use' error.

2 - Channels configured for TCP Server now have tabs coloured blue rather than red when listening for incoming connections, changing to green when a connection is made. This also fixes a problem with the service version that meant the channel pop-up menu assumed the channel was stopped and allowed settings to be changed and capture resumed, rather than being paused.

3 - Tested ComCap support for IBM DB2 and Sun MySQL databases, fixing some minor issues. The IBM data link was previously unable to list table columns due to a slight difference in the schema arguments from Microsoft data links, it also returns all column names as upper case and sorted, which stopped the special database columns serial_nr and event_time being recognised. The error reporting listed database tables and columns has been improved so that data link errors are reported, rather than the lists just being left blank. Note that for a database to be supported by ComCap, the data link provider needs to support the ADO OpenSchema method, and this seems far from universal in third party providers or drivers. There is a new tick box 'Log More Information' on the Database tab that logs connection string and schema details, in case of problems in the future.

4 - If capture is to a database, previously when capture was started the database was opened before any data was accepted or logged. The default has now changed so that data capture starts immediately while the database is still being opened with data temporarily cached and written once the database is available, similarly to when database problem occur during capture. The old behaviour is retained if 'Immediate Pause for Database Problems' is ticked. Beware this may cause some confusion when initially testing database capture, unless the errors in the information log are seen. Reversed a database error handling change in 4.5 so that the first attempt to resume capture after it's been paused is again after 'Delay Before Restart', rather than immediately. This potentially avoids two or more restart attempts a second if restart immediately fails due to a database issue.

5 - Increased the number of database errors recognised as meaning the database server connection has been lost, each manufacturer returns it's own concept of errors, ie 'link failure', 'timeout', 'gone away', 'terminate', etc. The database is now closed after any error, since error reporting in usually better opening the database, however the last row is only saved if ComCap believes the error to be connectivity rather than a data format issue to avoid an endless loop of open and close. It is better to try and filter the data to avoid invalid data being written in the first place.

6 - ComCap was tested against IBM DB2 Express-C v9.7 for Windows, using the 'IBM OLE DB Provider for DB2' that is part of the client package that may be downloaded from: <http://www-01.ibm.com/software/data/db2/express/> During install, you get an option to install just the client rather than the server, but beware it installs several windows services anyway. When setting up Data Link Properties, choose the IBM provider, then 'Direct Server Connection' with the server name as an IP or host, it should then allow a database to be selected once a logon has been entered and 'Allow Saving Password' ticked. A SQL script to create four ComCap tables may be found in newdb-ibmdb2.sql. Note that writing to stored procedures has not been tested.

7 - ComCap was tested against Sun MySQL v5.1 community edition, using the 'Connector/OBBC 3.51 driver' from <http://dev.mysql.com/downloads/> When setting up Data Link Properties, choose the Microsoft OLE DB Provider for ODBC Drivers, 'Use Connection String', click Build, from the File Data Source tab click New, select 'MySQL ODBC 3.51 Driver;', click Next and specify a name for the link, a Driver Connect dialog will appear where the server IP or host, login and password, and database may be specified, after which the link appears in the list of DSNs and may be selected. Finally repeat the login and database selections on the Connection tab and tick 'Allow Saving Password'. Note the ODBC 5.1 driver does not seem to work with ComCap, nor does the 'MySQL OLEDB Provider'. A SQL script to create four ComCap tables may be found in newdb-mysql.sql. Note that writing to stored procedures has not been tested.

8 - Added a new 'Line or Record End' of 'Multiple Tags' which allows the end of a record to be determined by one or more short words or tags, instead of by CR or LF. This is primarily designed to ease parsing for database capture, so that multi line data can be processed, and also for multiple

records sent without line endings. If these records have unwanted preceding or following tags, these may also be set as record endings and then filtered by phrases or minimum line length. All the line end settings have been moved from the General and Logging tabs, to a new Records tab. Record End Tags may include escaped characters similarly to 'Add Escaped Text', specifically \n new line, \c CR, \ LF, \ backslash and \s space, so text only at the end of a line can be specified as a tag.

9 - Increased the maximum capture line length from 1,024 to 2,048.

10 - Made three improvements to the ComGen data generator, used to create data to test ComCap. Data Types now includes a column with a 'No CRLF' tick box to prevent CRLF being automatically added to each line. Network includes two new columns. 'Lines/Session' causes the TCP connection to be disconnected after that many lines of data have been sent, to simulate devices that periodically call home, send some data and then disconnect. Setting six lines per minute with one line/session will cause 10 sessions per minute. 'Device Id (first line)' causes some text to be sent once when a session connects, to simulate devices such as the Ecov that identify themselves when connected, note that CRLF is not added automatically so escapes should be used if a line ending is needed, ie \n for CRLF.

11 - Fixed a long term problem when running ComCap on Windows 2008 (and maybe Vista and 7) that meant, in some circumstances, the capture tabs in the main window were blank and not coloured.

12 - Fixed a problem introduced in the last release when Sending Data from the dialog using the interactive version only, where escape control sequences were ignored.

13 - Fixed a long term problem re-opening the info log that sometimes resulted in multiple 'file sharing violation' error messages and alerts. Also changed the mechanism for flushing the info log to disk, to reduce disk activity particularly with a lot of capture channels, which will be noticed when stopping capture.

ComCap Release 4.5 - September 2009

1 - Fixed a long term problem with the ComCap Service where interactive tray monitoring and remote alerts and logging were lost if capture was restarted automatically due to a temporary PC freeze or more than 15 seconds. Also added a periodic handshake to ensure tray monitoring has not stopped.

2 - It is now possible to set Data Loss checking separately for each capture channel, rather than all channels sharing the same settings, thus allowing for differing data flows and time zones for remote capture. In Capture Settings, on the General Tab if 'Check for Data Loss' is checked then new fields will appear on the Sounds/Data Loss tab. If 'Override Common Data Loss Settings' is checked, a grid identical to that in Common Settings appears, allowing different settings for each channel. These new settings are backward compatible, so no changes are needed if Data Loss is already set-up. Note that disabling Data Loss checking in Common Settings still disables it for all capture channels.

3 - Temporary database problems are almost inevitable, perhaps due to communication problems or the database server being rebooted, so ComCap has various means of coping with them. When a row can not be written to the database it is automatically buffered so it can be written later. This can happen because capture is happening faster than data can be written to the database, which may be limited to only 50 to 150 rows maximum per second. In previous versions, ComCap only buffered a maximum of 1,000 rows before automatically pausing capture, but this figure is now configurable from 50 to 99,999 rows on the Database tab. Note that rows are buffered in memory, so this must be sufficient for the data expected to be buffered. If ComCap is exited before the buffered rows are written, the rows are lost. Due to this, the 'Immediate Pause for Database Problems' will cause capture to be temporarily stopped so the source can continue to buffer data (is so capable). Attempts are made to re-open the database according to 'Delay Before Restart' seconds, and when successful any buffered rows are written.

4 - If 'Immediate Pause for Database Problems' is not specified, an alert is now sent when the database connection fails and another when it restarts. Improved error messages and alerts due to database problems, to avoid repeating the same alerts, and also added a new alert when capture restarts after being paused.

5 - Fixed a problem when attempts to reopen the database may have been skipped. Improved the error handling when there is a timeout writing to the database, usually due to communication problems. Fixed a problem when writing to databases using an ODBC connection when connection failure was not always detected correctly, thus stopping database re-open attempts

6 - The Information Log now has the date and time added when newly created, to avoid empty logs when there is nothing else to note. Fixed a problem with the ComCap service that meant small or empty log files may have been created in the program directory each time the services was started or stopped.

7 - The maximum captured line length may now be set to four characters (previously 64) before the line is broken.

8 - Fixed a bug sending data with UDP Server. Currently, UDP Send is only allowed if the channel is listening, not filtered from another channel.

9 - If echo captured data is configured, data received from the echo destination is now reverse echoed to the original capture source, with ComCap effectively behaving as a proxy. Currently, reverse echo data is handled a line at a time and echoed when each complete line is received, so can not be used for binary data. It is designed to send commands to remote capture devices. Reverse echo data is reported in the Information Log, not the capture logs.

10 - Fixed a validation problem on the Filters and Alerts tab, it's now possible to save settings with one of the filter lists blank.

11 - There is now no limit on the number of seconds that may be specified for the 'Repeat Start Command' allowing it to sent once a day, if required.

ComCap Release 4.4 - January 2009

1 - In order to assist with waking up and configuring remote capture servers, the right click menu has three new options: Resend Start Command, Send Data, and Terminal Window. The first two are only available when capture has been started, the Terminal Window only when it's stopped or paused. Resend Start Command simply resends the same data sent when capture starts, but on demand. Send Data displays a new window allowing custom data to be sent on demand, with the last 50 command sent selectable from a drop down box, or allowing a file to be selected and sent (TCP/UDP only), typically to configure remote capture device, or load new firmware.

2 - A Telnet Terminal window has been added, to allow interaction with remote TCP/IP Servers. It may be selected from the File menu in the Main Window, or the right click menu when the remote address and port will be set according to the channel settings. Terminal window options may be specified such as font and size, function key behaviour, echo, auto LF and CR, etc. If Log is ticked, anything typed or received in the window is written to a session log with the file name telnet-(date)-(time).log.

3 - Added the ability to trigger alerts from captured text. The new Filters and Alerts tab includes a tick box 'Alert for Lines with Phrases (case sensitive)' which causes a captured lines to be checked against one or more phrases (entered one line at a time), with an alert being triggered if any are matched. The alert may be a pop-up window, email or SMS message, as configured in Settings, Common, and will include the channel name and the captured line.

4 - A number of remote TCP devices may be configured to identify themselves when a TCP session connects, by sending a device id as the first line of data. For instance, Tysso eCov serial to TCP/IP

converter sends a five digit configurable number as the first line, while some GSM/3G modems send a device type and IMEI number. In Settings, Logging, 'First Line is Device Id' will cause the first captured line to be saved and not logged, and it may be added to subsequent captured lines using 'Add Escaped Text' with the \z command. So effectively the Device Id is added to each captured line to identify it, specifically with TCP Server where lots of different remote devices may be calling home.

5 - Added some more data validation and processing options, to clean up and reject unwanted captured data. In Settings, Logging, 'Remove Leading Spaces' ensures any control characters or blanks before real data are removed. 'Validate Line Length' allows lines shorter or longer than specified limits to be ignored. This check is done after space at the start and/or end of the line is removed, but before escaped text is added. On the Settings, General tab, ticking 'Filter and Alerts' will cause a new tab Filters and Alerts to appear, on which ticking 'Ignore Lines with Phrases (case sensitive)' causes a captured lines to be checked against one or more phrases (entered one line at a time), and ignored if any are found. ComCap now counts how many lines are ignored due to these various filters and checks, and shows the total in the status bar and hourly in the Information Log.

6 - It is now possible to add a pause into the Commands to Send Upon Start and Stop Capture, and the new Send Data command. \P (capital only) will cause a 50ms pause in the data being sent, with multiples allowing a longer delay. Note the pause may not necessarily be effective with TCP/IP, because packets may get combined at transport level, nor may the pause be exactly 50ms due to other activity within ComCap.

7 - Fixed a bug that meant the Log Files option Start/Stop in Capture Log did not always write the stop command, specifically if the capture file had closed due to inactivity.

8 - The Add Comment right click menu option is now effective when the ComCap service version is being used. Also, the Command window position is now restored correctly if moved.

9 - In Settings, Files, if Log Name Format is specified as Custom, the Custom Log Name Mask is now validated to ensure that it includes yy or yyyy mask characters for year. The custom mask has always been ignored unless yy was found, but without warning.

10 - If the Capture Log New Log Interval is set to Weekly, it's now also possible to set the New Log Open Time, so the log could rotate at 6am on Monday morning instead of midnight.

11 - When ComCap starts, the main window is only automatically minimised if Auto Start is specified.

12 - It's now possible to change channel settings during paused capture for both service and interactive versions, not just the latter.

13 - Fixed a bug introduced in Release 4.3 that meant the remote IP address and port could change line by line for TCP Client or Server, if data was being captured from other sessions at the same time.

14 - Fixed a possible bug that meant extra data might appear at the start of TCP session, if the connection was dropped and reconnected without capture being stopped and restarted.

15 - Fixed a bug that meant test email and SMS alerts could not be sent if ComCap was configured to use the service version and it was stopped. Also, the validation of Email To: addresses has been improved to stop a blank address preventing email being sent.

ComCap Release 4.3 - July 2008

1 - The Unlimited version now supports capture from up to 500 serial COM ports, TCP/IP Server, TCP/IP Client and UDP/IP network protocols simultaneously, with suitable hardware. It has been tested on Windows XP with 260 TCP/IP sessions created by ComGen (which never had a limit), writing capture logs one line per second, with only 2-6% CPU usage on a old Pentium 4 and 12 megs

memory usage.

2 - ComCap, ComGen and Signals now all support serial COM ports with names other than COM followed by a number, ie CNCA2. Virtual COM ports are sometimes installed with such strange names.

3 - When capturing data on the same channel from multiple UDP clients using different IP addresses, the correct IP of the last packet is now displayed and added to the capture log if the Remote IP Address is added as escaped text (\r), rather than the IP of the first packet only.

4 - It's now possible to use keyboard short cuts to copy text from the capture log windows, as well as the right click menu options.

5 - Improved the logging for license key failures, particularly when old version 3 keys are used by accident with ComCap version 4 (which needs newer keys).

ComCap Release 4.2 - November 2007

1 - In order to support capture from appliances that only return data when triggered, in Capture Settings, General a new option 'Repeat Start Command Every X Seconds' has been added. This causes the Start command text to be repeatedly sent at the specified interval. The maximum interval is 999 seconds, with zero meaning don't repeat the command.

2 - In Capture Settings, General, a 'Line End Timeout' may now be specified in seconds, where zero means no timeout, up to 300 seconds. When the timeout expires, an incomplete captured line will be processed, saved and displayed. This is usually only necessary when non-ASCII data is being captured where there are no carriage returns or line feeds, but may also be useful when setting up ComCap to capture from a serial port with unknown speed, since it can be used to cause display of the 'corrupted' data caused by speed mismatch which will be missing line ends.

3 - In Capture Settings, Logging, 'Ignore Blank Lines' causes lines without any printable characters to be ignored. This will reduce the size of logs that contain far too many blank lines. This option should generally be used with 'Remove Control Characters'.

4 - In Capture Settings, Logging, 'Log Hex Data' causes all captured data to be converted into hexadecimal (doubling the size). This is primarily intended for capturing binary data, but may be used a debugging tool to find the exact format of data being captured, for instance the type of line endings. Normal line ending rules are applied when capturing in hex, so lines may be broken on linefeed, etc (also saved in hex).

5 - The actual information log file names are now logged hourly. This may be useful where an emergency log is opened due to an access conflict on the original file.

6 - When configuring ComCap to 'Capture Using Background Service', a warning is now displayed if any channels are configured as 'Save to Database' and a service account has not been specified, since database access needs logon credentials.

7 - It's now again possible to specify UNC network paths in Log Directories with 'Capture Using Background Service'.

8 - When starting the ComCap background service from the ComCap tray version, the channel currently selected now starts to update immediately all channels have started, rather than the next time it's clicked.

9 - When using the TCP Server protocol to Echo captured Data, or Send Remote the Information Log or Alerts, up to five remote TCP Clients can now access the TCP Server simultaneously (previously just one). This allows ComCap to be used to distribute captured data to five other PCs, perhaps also

running ComCap.

10 - The highest numbered COM port recognised by ComCap has been increased from COM60 to COM200 to allow for virtual COM ports being installed with high numbers. Also, the Standard version now lists all installed COM ports, not just the first three, but still only allows capture from a maximum of three ports.

11 - If the requirement is to capture serial data from another application on the same PC, ComCap now includes a Null Modem Emulator (com0com) from <http://com0com.sourceforge.net/> that installs a linked pair of virtual serial ports, instead of needing to use a physical pair of COM ports and a null modem cable.

ComCap Release 4.1 - February 2007

1 - The ComCap system tray icon now shows a small red or green square to indicate whether capture is stopped or started.

2 - If ComCap is unregistered, an alert is now sent when capture starts and when it stops after one hour (24 hours with a v3 license). This will serve as a warning if the license key is lost or corrupted.

3 - Both the Information Log and Alerts may now be sent to a remote PC using UDP, TCP Client or TCP Server protocols, perhaps to another copy of ComCap. This will ease central monitoring of remote capture.

4 - The Alert window will now appear without also showing the tray capture window, which avoids unnecessary log scrolling on unattended PCs.

5 - Echo to Remote using UDP now pings the remote host before sending any data to establish it exists, and continues to ping at the 'Wait Seconds' interval during the capture session to ensure it's still available. Note this does not mean a UDP server is listening on the remote computer, just that the computer is running. This is disabled if Common Preferences 'Don't Check Connections with Ping Echo' is ticked.

6 - When using Echo to Remote with Syslog, the Severity and Facility Priorities are now selected from drop down lists, rather than needing to enter a numeric value (ie <14>).

7 - The ComCap application and set-up program are now both digitally signed as being from Magenta Systems Ltd. This will reduce the severity of the warnings that Windows Vista generates when programs are run.

8 - Fixed a bug with capture using TCP Server where an optional Start Command was only sent for the server remote connection, and not subsequent connections.

9 - Fixed a bug that meant the service version did not always log version and registration information on start-up.

10 - Fixed a bug that meant an unnecessary 'emergency' information log file might have been created in the program directory on start-up or close down. Such logs are generally only created when the correct log volume is not available or the log file can not be opened due to an error.

11 - In Common Settings, Serial Ports, a new column 'Control Lines' has been added. This option determines whether the three serial control lines CTS, DTS and DCD should be checked during capture, to make detection of connection or hardware problems easier since an alert can be sent if capture stops. If ticked, capture will only start when at least one of the three control lines goes high, and will stop if they all drop. Note this is really cosmetic only (with the tab colour changing red to green) and start/stop logging, and data will be still be captured even if all the control line are low. But unless the channel is seen to 'start', some functionality may not work correctly such as capture file

name roll over.

12 - In Common Settings, Log Files, a new tick box 'Send Alert on File Errors' has been added. If ticked, any major errors opening or writing the information or capture logs will generate an alert. Currently there may be repeated alerts, since such errors often happen rapidly in multiple channels, but this should be fixed shortly.

13 - In Common Settings, Capture Logging, a new tick box 'Send Alert on Stop' has been added. If ticked, an alert is sent every time ComCap is stopped. This is intended for where ComCap should be running 24/7, and where alerts are sent via email, SMS or remotely to warn of accidental stops. Note this will only work for a 'clean' close down, if ComCap is crashed from Task Manager or by Windows close down, the alert may not be sent.

14 - Attempted to handle a situation with the service version where a serious problem that causes hundreds or thousands of error lines in the information log could potentially overflow the 'echo to tray' communication channel and lock-up ComCap.

15 - Made a few improvements in ComGen. It will now close down faster when Windows itself closes down. UDP Client now pings the remote host before sending any data to establish it exists, and continues to ping during the session to ensure it's still available. Corrected the default Data Types that still had \s8 for a serial number (from an earlier beta) instead of \#8 used in the final release.

ComCap Release 4.0 - October 2006

New Release - Added TCP/IP and UDP.

ComCap Release 3.0 - April 2003

New Release

ComCap Release 2.0 - January 2001

New Release

ComCap Release 1.0 - February 2000

First Release

5.6 Copyright Information and Support

ComCap is copyright Magenta Systems Ltd, England, 1999 to 2019.

Magenta Systems Ltd
9 Vincent Road
Croydon
CR0 6ED
United Kingdom

Phone 020 8656 3636, International Phone +44 20 8656 3636

Email: comcap@magsys.co.uk
Web: <https://www.magsys.co.uk/comcap/>

Index

- 9 -

9100 Printing 98

- A -

Access (Jet) 90, 108, 109
Account, Background Service 38
Add Comment to Log 25
Add CRLF End of Line 98
Add Date Daily 75
Add Escaped Text 75
Administrative Privileges 22, 23, 38
ADO 90, 108, 109, 111, 114
Alert Email 60
Alert for (mins), Ignore Same 101
Alert for Data Loss 64, 88
Alert for Database Problems 90
Alert for Lines with Phrases 101
Alert for Low Disk Space 55
Alert for No Disk Space 55
Alert for Windows Freeze 54
Alert on Stop 38
Alert on Unexpected Stop 68
Alert Window 25
Alert Window, Show 58
Alerts 58
Alerts, Send Alert 58
Alerts, Test 25
Allow Monitor Background Service 38
Alternate Log Directory 55, 78
Android GPS App 102
ANSI Terminal 33
Ansi/Epson Matrix Escapes 71
Application Priority 38, 54
Archive Capture Log on Rotation 78
Archive Log Directory 78
Archive/Email Capture Log on Stop Capture 78
ARP 14
Attempts to Open Log 38
Auto Run Tray Application 38
Auto Scroll 25
Auto Start 78

Auto Start Capture 38
Auto Start ComGen 126
Avaya RSP 45

- B -

Background Service 11, 22, 38, 86
Backslash Issue, MySQL 114
Backup 22
Bands, Data Loss 64, 88
Binary File - Repeat 126
Binary File - Simple 126
Bits Per Second 50
Blank Data 94
Booting, PC 38
Brainboxes 14
Browse for Folder 55, 78
Buffer Size, TCP/UDP 98
Button Bar 25

- C -

CA Request 16
Capture Log 55
Capture Log Directories 78
Capture Log Names 38
Capture Log on Rotation, Email 83
Capture Log Window 25
Capture Logging 38
Capture Name 41, 45, 50, 53
Capture Restart Attempts 68
Capture Settings 25
Capture Settings, Data Format 94
Capture Settings, Database 90, 108, 109, 111, 114
Capture Settings, Files 78
Capture Settings, Filters and Alerts 101
Capture Settings, General 68
Capture Settings, Logging 75
Capture Settings, Network 98
Capture Settings, Printing 86
Capture Settings, Sounds 88
Capture State 25
Capture Status Hourly 55
Capture TCP/UDP Buffer Size 98
Capture Using Background Service 38
Capture, Merging 53
Capture, Pause/Resume 25

- Capture, Start/Stop 25
 - Carriage Return / Line Feed Line End 71
 - Carriage Return Line End 71
 - Character Separated Columns (CSV) Data Format 68, 94
 - Check for Data Loss 38, 68
 - Check if SSL Certificates Revoked (slow) 41
 - Checksum 14
 - Classic Log Name Format 78
 - Clear Alerts 25
 - Client Validate Server Certificate 98
 - Client, TCP 14, 45
 - Close Capture Log after Each Line is Written 38
 - Column Definitions, Database 90
 - Column Length, Database 94
 - Column Name, Database 94
 - Column Nullable, Database 94
 - Column Type, Database 94
 - Columns, Database Table 90, 108, 109, 111, 114, 121
 - COM Port, Printer 86
 - COM1 50
 - Combining multiple capture files 132
 - ComCap Background Service 38
 - ComCap GPS CSV format 102
 - ComCap Tray Application 38
 - ComCap v3 11
 - ComCap v4 Standard 11
 - ComCap v4 Unlimited 11
 - comcap.config 22, 45
 - comcap.current 22, 45
 - ComGen Data Stream Generator 126
 - Comma Separated Values 102
 - Command to Send upon Start and Stop 68
 - Common Capture Log 55
 - Common Files Logging, No Logging Files 75
 - Common Settings 25, 38, 45, 50, 54, 55, 58, 60, 62, 64
 - Communications Parameters, Serial Printer 86
 - Communications Port 50
 - Concatenation Utility 132
 - Concox TR02 vehicle tracker 102
 - Configuration Files 22, 45
 - Conflict Errors 38
 - Connection Timeout, Database 90
 - Connection, Database 90
 - Connections, TCP/IP 14
 - Connections, TCP/IP Ping Echo 45
 - Control Chars, Remove 75
 - Control Serial Port, Alert 58
 - Copyright Information 159
 - CPU Time 38, 54
 - CR / LF Line End 71
 - Create SSL Certificate 41, 98
 - Creating and Getting SSL/TLS Certificates 16
 - CSV Data Format 68, 94
 - Custom Log Name Format 78
 - Custom Log Name Mask 78
 - Custom Sub-Directory 78
 - Cyclades 50
- D -**
- Daily Logs 55, 78
 - Data Bits, Serial 50
 - Data Format 68, 90
 - Data Frequency 126
 - Data Length, Data Format 94
 - Data Link Properties, Database 90
 - Data Loss 64, 88
 - Data Loss Recovery 64, 88
 - Data Loss Settings, Override Common 88
 - Data Loss, Check for 68
 - Data Name, Data Format 94
 - Data Position, Data Format 94
 - Data Source Name 114
 - Data Stream Generator 126
 - Data Types 126
 - Database 11, 90, 94, 108, 109, 111, 114
 - Database Columns 94
 - Database Diagnostics 55
 - Database Errors 90
 - Database from Log 25, 90
 - Database Inactivity 90
 - Database Performance 108
 - Database, Save to 68
 - Date and Time Mask Characters 78
 - Date and Time, Add 75
 - Days, Valid 64, 88
 - DB2, IBM 90, 108, 111
 - DB25 connector 12
 - DB9 connector 12
 - Default Log Directories 55, 78
 - Delete Empty Capture Log on Rotation 78
 - Device Id, First Line is 75
 - Device Servers 14
 - DHCP 14

Diagnostic, Log 55
Directories, Capture Log 78
Disk Space Alerts 55
Display Lines Captured by Background Service 38
DNS 14
Domain Names 14
Don't Check Connections with Ping Echo 41
Drives, Shared Network 54, 55
DSN 114
DSR, Only Send if 86
Dynamic Name Server 14

- E -

Each New Page 78
Each Record/Line 78
Echo 98
Echo TCP/UDP Buffer Size 98
Echo to Network Overview 98
Echo to Printer Overview, Echo to 86
Echo Type 68
Edgeport 50
Email 60
Email Queue 60
Email Capture Log on Rotation 83
Email Overview 60
Email Queue Root Directory 60
Email Server 45
Email Servers 60
Email Subject 83
Email Titles 83
Email To Addresses 83
Email, Send Alert 58, 60
Empty Capture Log on Rotation, Delete 78
Enable Location Sensor 41
End Tags, Record 71
Error Correction 14, 45
Error, Network 45
Escape Backslash (MySQL) 90
Escape Sequences, Add Text 75
Escape Sequences, Printer 86
Escape Sequences, Start and Stop Commands 68
Escaped Text 90, 126
Ethernet 14
Ethernet Device Servers 12, 14
ETSI 07.05 Specification 62
Example Database Tables 90, 108, 109, 111, 114, 121

Exit Menu 25
Extra Database Columns 90

- F -

Family 45
File Name, Fixed 78
File Name, Prompt on Start for 25
File Names 78
File Names, Prompt on Start 78
File Size, Max 55, 78
Filter Information 45
Filter Lines with Phrases 101
Filters and Alerts 68
Find Address 34
First Line is Device Id 75
Fixed File Name 78
Fixed Width Columns Data Format 68, 94
Flow Control 50
Flush Capture Log to Disk Periodically 38
Font Size, Printer 86
Font, Log 25
Font, Printer 86
Format for Display of Large Numbers 38
Freezing, Windows 54
From Address 83
From Address, Email 60
FTP Capture Log on Rotation 78
Full Buffer (Ignore Data), No Pause for 90

- G -

Gap Between SMS Messages 62
Gap Between Sounds 88
Getting Started 23
GlobalSat 102
Google maps 34
GPRS 102
GPS data 34
GPS Data Input Type 102
GPS Data Output Type 102
GPS Data Processing 68, 102
GPS Exchange XML Track 102
GPS location marker 34
GPS Location Sensor 102
GPS Location Sensor Channel 41
GPS receivers 102

GPS SQL Database Capture 102
 GPS Testing 102
 GPS Tracker Communications Protocol GT02 102
 GPSD JSON 102
 Grid, Data Format 90, 94
 Grid, Data Loss 64, 88
 Grid, Network 45
 Grid, Serial 50
 GSM Modem 62, 102
 GT02, GPS Tracker Communications Protocol 102

- H -

Handshaking 14, 45
 Hardware Flow Control 50
 Hide Button 25
 High Priority 38, 54
 Host name 14
 Hourly Logs 78
 HP PCL, PJI, GL/2 Escapes 71

- I -

IBM DB2 90, 108, 111
 IBM OLE DB Provider for DB2' 111
 ICMP 14
 Idle TCP Server Close Session Timeout 68
 Ignore Altitude 102
 Ignore Blank Lines 75
 Ignore Lines with Phrases 101
 Ignore Records That Cause Error 90
 Ignore Same Alert for (mins) 101
 Ignore Too Many Lines 71
 Ignored Lines to Info Log 71, 75
 IMEI 102
 Immediate Pause for Database Problems 90
 Inactivity Delay before Closing Capture Log 38
 Inactivity Period 78
 Information Log 55
 Information Log Window 25
 Initial Set-Up 23
 Insert Into Tables 90
 Inside Out Networks 50
 Installation 22
 Interval, New Capture Log 78
 Interval, New Common Log 55
 Interval, New Information Log 55

IP Address 14, 45
 IP address family 45
 IP Addressing and Ports 14, 45
 IP Port 14, 45
 IP Printing 98
 IP Protocol 14, 45
 IPv4 14
 IPv6 14, 41
 IPv6 address 45
 IPX 14
 ISA Expansion Cards 50
 ISO Date and Time 90
 ISO Date and Time, Add 75

- K -

Kapow! SMS Gateway 62
 KBytes 38

- L -

LAN 14, 45, 54
 LAN/Misc 54
 Lantronix 14
 Lava Computer 50
 Lavalink 14
 License Key 54
 License Keys 11, 22
 Line End 71
 Line End Timeout 68
 Line Feed Line End 71
 Line Length, Maximum 71
 Line Length, Minimum and Maximum 71
 Line or Record End 71
 Line Time Gap 71
 Lines Per Minute 126
 Lines Per Second 126
 Lines to Remove When Display Overflow 38
 Load Full Log 25
 Local Area Network 54
 Local Area Networks 14, 45
 Local IP Address 45, 98
 Local IP Address, Add 75
 Local IP Port 45, 98
 Locate in Real Time 34
 Log Diagnostic Messages 55
 Log Directories, Capture 78

Log Directories, Default 55
Log Display, No 68
Log Errors 38
Log Files 55
Log Full SSL Certificate Chain 41
Log GPS Info 25, 34
Log Hex Data 75
Log Internal, Common Log 55
Log Interval, Capture Log 78
Log Interval, Information 55
Log Name Format 78
Log Only First Command Sent 68
Log Raw Data 75
Log, Telnet 33
Logging Type, Capture 75
Logon, LAN 54, 55, 78
Logs Per Day 55, 78
Low Disk Space 55
lueetooth serial ports 12

- M -

MAC Addresses 14
Magenta Systems Ltd 159
Main Capture Window 25
Main Capture Window, Main Capture 23
Mapped Drives 38, 54, 55
Mask Characters, Date and Time 78
Mask, Custom Log Name 78
Mask, Time Stamp 75
Masked Text 126
Max File Size 55, 78
Maximum Attempts to Open Log with Conflict Error 38
Maximum Length, Line 71
Maximum Line Length 71
Maximum Log Lines to Display 38
Maximum Report Interval 102
Maximum Rows to Buffer Before Pausing Capture 90
MBytes 38
MDAC 90, 108, 109, 111, 114
MDAC Data Link Properties 109, 111, 114
Merge Channels 45, 50, 53
Merge From (partial name) 53
Merging Captured Data 45, 50, 53
Merging Overview 53

Microsoft Data Access Components 90, 108, 109, 111, 114
Microsoft OLE DB Provider for SQL Server 109
Microsoft SQL Server 90, 108, 109
Minimum Disk Space 55
Minimum Length, Line 71
Minimum Report Interval 102
Minutes Between Queue Attempts 60
Mobile Numbers 62
Mobile Telephones 62
Monthly Logs 55, 78
Movement Report Interval 102
Moxa 50
Multiple Per Day 78
MyLiveTracker 102
MySQL ODBC 3.51 Driver 114
MySQL, Escape Backslash 90
MySQL, Sun 90, 108, 111, 114

- N -

Name Format, Logs 78
Named Log Name Format 78
Network 45
Network Adaptors 14
Network and SSL/TLS settings 41
Network Drives, Shared 54, 55
Network Packets 14, 45
Network Performance Overview 98
Network, Echo to 68
Networking Tutorial 14
New Log 78
New Log Every 78
New Log Interval, Capture Log 78
New Log Interval, Common Log 55
New Log Interval, Information Log 55
New Log Time 55, 78
Next Serial 126
Next Serial Number 75
NMEA 0183 Sentences 102
No Log Display 68
No Pause for Full Buffer (Ignore Data) 90
Nokia 30 Modem 62
Notify New Line Audibly 88
Null Columns, Database 94
Null Modem Emulator (com0com) 50, 133
Numbers, Format for Display of Large 38

- O -

ODBC connection for MySQL 114
 ODBC Drivers 90, 108, 114
 Only Send if DSR 126
 Override Common Data Loss Settings 88

- P -

Packet Line End 71
 Parallel Port Printer, Echo to 68, 86
 Parity, Serial 50
 Parsing Test Data 94
 Pause Capture 25
 Pause Capture if Echo Stops 68
 Pause for Database Problems 90
 Pause Send Data 68
 Pausing Capture, Maximum Rows to Buffer Before 90
 PC Event Log 38
 PC Name, Add 75
 PCI Expansion Cards 12, 50
 PEM Bundle File 16, 41
 Permissions 22
 Phrases, Filter or Alert 101
 Physical Hardware Layer 14
 Ping Echo 14
 Play Sound File 58
 Plot Route 34
 Port, IP 14, 45
 Port, Serial 50
 Print Spooling 86
 Printer 86
 Printer Control Code 86
 Printer Control Sequences, Remove 71
 Printer, Echo to 68
 Priority, Application 38, 54
 Program Directories 22
 Progress, ComGen 126
 Prompt on Start for File Name 25
 Prompt on Start Name Format 78
 Proxy Echo 68

- R -

RE Smith 14

Real Time Priority 38, 54
 Record End 71
 Record End Tags 71
 Recovery Functionality, Database 90
 Recovery, Data Loss 64, 88
 Release Notes 135
 Reliable Syslog 45
 Remote IP Address 45, 98
 Remote IP Address, Add 75
 Remote IP Port 45, 98
 Remote, Send Alert 58
 Remove Control Chars 75
 Remove Hi-Bit Characters 75
 Remove Leading Spaces 75
 Remove Printer Control Sequences 71
 Remove Trailing Spaces 75
 Reparse Sample Log 94
 Repeat Sound File 58
 Repeat Start Command 68
 Report Distance Moved 102
 Report No Fix 102
 Report Real Time 102
 Report Remote IP Address 102
 Resend Start Data 25
 Restart Attempts, Capture 68
 Restart Capture 64, 88
 Resume Capture 25
 Retries, Email Send 60
 Retries, SMS Send 62
 Retry Attempts, TCP Client 14, 45
 Root Certificate 16
 RS232 Communications Port 50
 RS232 communications port, Alert 58
 RS232 ports 12
 RS232 serial port 14
 RTS/DTR Flow Control 50

- S -

Sample Database 90, 108, 109, 111, 114, 121
 Sample Log Data 94
 Sample Stored Procedures 90
 Satellite 41
 Satellites 25, 34
 Save to Database 68
 Save/Restore Buffered Rows to Disk 90
 Scroll Tabs 25
 Search for Captured Data 101

- Secure Email 60
- Self Signed Certificate 16
- Send Alert 60, 62
- Send Alerts to Remote Computer 58
- Send Data 25
- Send File 25
- Send Remote Protocol 58
- Separating Character, Character Separated Columns 68
- Sequence Number, Data Format 94
- Sequential File Names 78
- Serial Com Ports 50
- Serial Number 75, 78, 90
- Serial Number Digits 75
- Serial Port, Alert Control 58
- Serial Ports 50, 126
- Serial Ports grid in Common Settings 12
- Serial Ports Overview 12
- Serial Printer 86
- Serial Printer, Echo to 86
- Serial Status Indicators 25
- Serial to Network Converters 12, 14
- Servers, TCP/UDP 14, 45
- Service, ComCap Background 38
- Session Timeout, Idle TCP Server Close 68
- Settings 22, 23
- Settings Menu 25
- Setup 22
- Set-Up, Initial 23
- Shared Drives 38, 54, 55
- Short Message Service 62
- Siemens MC35/TC35 Modem 62
- Signal Indicators 25
- Signal Lines 132
- Signed Device Drivers 12
- Single Files Logging 75
- Size, Printer Font 86
- SMS Delivery Progress 62
- SMS Gateway 62
- SMS Overview 62
- SMTP Authentication 60
- SMTP Email Server 83
- SMTP Email, Account Names Accepted by Server 83
- SMTP Email, Ignore Email Body 83
- SMTP Email, One Log File Per Email 83
- SMTP Email, Relay Raw Email 83
- SMTP Email, Remote IP Addresses Accepted 83
- SMTP Email, Remove Body Line Endings 83
- SMTP Email, Save as Variable Named Columns 83
- SMTP Email, Save Raw Email as EML File 83
- SMTP Email, Server Requires Authentication 83
- SMTP Email, Show All Headers 83
- SMTP Email, SQL Email Capture 83
- SMTP Email, Strip All Attachments 83
- SMTP Port 60
- SMTP Servers 60
- SMTP SSL/TLS 60
- SNMP 14, 45
- Sound File Name, Play 88
- Sound File, Play Alert 58
- Sound, Notify New Line 88
- Spaces, Remove Leading or Trailing 75
- Special Character Line End 71
- Special Line Ending (hex) 71
- Specify Database 90
- Speed 102
- Speed, Serial 50
- SQL Database 90, 108, 109, 111, 114
- SQL Email Capture 83
- SQL Errors 94
- SQL INSERT Statement 90
- SQL Query Analyser 90, 108, 109
- SQL Server Management Studio 90, 108, 109
- SQL Server, Microsoft 90, 108, 109
- SSL Allowed Host Names 41
- SSL Certificate Authority 16, 41, 98
- SSL Client Certificate Authority Bundle File 41
- SSL Client Verify Certificate Mode 41
- SSL Server Certificate 16, 41, 98
- SSL Server DH Params 16, 41, 98
- SSL Server ECDH Key 98
- SSL Server Private Key 16, 41, 98
- SSL/TLS for Capture 98
- SSL/TLS for Echo 98
- SSL/TLS Overview 16
- SSL/TLS, SMTP 60
- Start and Stop Commands 68
- Start Capture 25
- Start/Stop in Capture Log 55
- Status Bar 25
- Status Button 25
- Status Hourly, Capture 55
- Status Indicators 25
- Stop Bits, Serial 50

Stop Capture 25
 Stop Capture, Archive/Email Capture Log on 78
 Stop PC Sleeping 38
 Stop Window Update 25
 Stored Procedures 94
 Stream Data 45
 Streamed Text 126
 Sub-Directory, Custom 78
 Subject 60
 Sun MySQL 90, 108, 111, 114
 Support 159
 Support IPv6 41
 Syslog 14, 45
 Syslog Facility Priority 58
 Syslog Headers 98, 126
 Syslog Headers, Add 58
 Syslog Severity Priority 58
 Syslog, Echo 98, 126
 System Network Management Protocol 45

- T -

Tab Colours, Tabs 25
 Tab Scrolling 25
 Table Definitions 94
 Tables, Database 90, 94, 108, 109, 111, 114, 121
 Tablet Location Sensor 102
 TCP 14, 45
 TCP Client 14, 45, 126
 TCP Client, Echo to 68
 TCP Client, Network 45
 TCP Server 14, 45, 126
 TCP Server and TCP Client 98
 TCP Server, Echo to 68
 TCP/IP 14, 45
 TCP/IP Client, No Immediate Retry on Disconnect 41
 TCP/IP Send Keep Alive 41
 TCP/UDP Buffer Size 98
 Telnet Terminal 25, 33
 Terminal, Telnet 33
 Test Alert 58
 Test Alerts 25
 Test Data Loss Band 64, 88
 Test Mapping 54, 55
 Test RS232 12
 Test RS232 Signals 50, 132
 Test Serial Ports and Hardware Events 132

Text File - Repeat 126
 Text File - Simple 126
 Texts 62
 Time Stamp Each Line 75
 Time Stamp Mask 75
 Timeout, Idle TCP Server Close Session 68
 Timeout, TCP/IP 14, 45
 Titles Added to Email Body 83
 TK102/103 Tracker Protocol 102
 TK5000 Tracker Protocol, WondeX 102
 To Address, Email 60
 TR02 vehicle tracker, Concox 102
 Transmission Control Protocol 14, 45
 Tray Application, ComCap 38
 Tysso 14

- U -

UDP 14, 45
 UDP (Syslog), 98
 UDP (Syslog), Echo to 68
 UDP Client 126
 UDP/IP 14, 45
 UK NGR Northings/Eastings 102
 UNC Paths 54, 55, 78
 Uninstalling 22
 Upgrading from ComCap v3 to v4 11
 USB device 50
 USB Serial Ports 12, 50
 User Datagram Protocol 14, 45

- V -

Variable Named Columns (=) Data Format 68, 94
 View Log Window 25
 View Map Window 25
 View Old Data 78
 Virtual serial ports 12, 50, 133
 VT-10, VT300 GPS Devices 102

- W -

Warning Period 64, 88
 Weekly Log 55, 78
 Window, Main Capture 25
 Windows 2008 R2 SP1, SQL database issue with 108

Windows 7 SP1, SQL database issue with 108
Windows Certificate Store 16, 41
Windows Freezing 54
Windows Location Service 41
Windows Printer 86
Windows Printer, Echo to 68, 86
Windows Service 38
WondeX/TK5000 Tracker Protocol 102
Word Wrap 25

- X -

X509 SSL/TLS certificates 16
Xon/Xoff Flow Control 50

