



# **Platinum**

## **Firmware for CMG-EAM, DAS, NAM and DCM**

### **Operator's Guide**

Part No. MAN-EAM-0001

Designed and manufactured by  
Güralp Systems Limited  
3 Midas House, Calleva Park  
Aldermaston RG7 8EA  
England

**Proprietary Notice:** The information in this manual is proprietary to Güralp Systems Limited and may not be copied or distributed outside the approved recipient's organisation without the approval of Güralp Systems Limited. Güralp Systems Limited shall not be liable for technical or editorial errors or omissions made herein, nor for incidental or consequential damages resulting from the furnishing, performance, or usage of this material.

---

Issue C    2010-11-18

# Table of Contents

---

|   |           |
|---|-----------|
| <b>1 Introduction.....</b>                                    | <b>6</b>  |
| 1.1 A Note on Terminology.....                                | 8         |
| 1.1.1 Sensor.....   | 8         |
| 1.1.2 Digitiser.....  | 8         |
| 1.1.3 Digital Sensor or Digital Instrument.....               | 9         |
| 1.2 Hardware Overview.....                                    | 9         |
| 1.3 Software Overview.....                                    | 10        |
| 1.4 Typical Applications.....                                 | 11        |
| 1.4.1 Autonomous remote data-logger.....                      | 11        |
| 1.4.2 Protocol Converter.....                                 | 11        |
| 1.4.3 Array Concentrator.....                                 | 12        |
| 1.4.4 Resilient Networking.....                               | 13        |
| 1.4.5 CD1.1 Networking.....                                   | 14        |
| 1.5 Document Conventions.....                                 | 14        |
| <b>2 First Steps.....</b>                                     | <b>15</b> |
| 2.1 Connecting to the Serial Port.....                        | 15        |
| 2.2 Connecting to the network port.....                       | 17        |
| 2.2.1 DHCP-assigned addresses.....                            | 18        |
| 2.2.2 Assigning a static IP address.....                      | 19        |
| 2.2.3 Connecting to the web interface.....                    | 19        |
| 2.2.4 Connecting using SSH.....                               | 21        |
| 2.3 Changing the password.....                                | 24        |
| <b>3 Configuration System Overview.....</b>                   | <b>27</b> |
| 3.1 Using the configuration system via the web interface..... | 27        |
| 3.2 Using the command-line configuration system.....          | 30        |
| 3.2.1 Text entry fields.....                                  | 32        |
| 3.2.2 Check-boxes.....  | 33        |
| 3.2.3 Drop-down menus.....                                    | 33        |
| 3.2.4 Using forms.....  | 34        |
| 3.3 Configuration Management.....                             | 36        |
| 3.3.1 Saving a configuration.....                             | 37        |
| 3.3.2 Deleting a saved configuration.....                     | 37        |
| 3.3.3 Restoring a configuration.....                          | 38        |
| <b>4 Firmware Upgrades.....</b>                               | <b>40</b> |
| 4.1 Determining the current firmware level.....               | 40        |
| 4.2 Upgrade Methods.....                                      | 41        |
| 4.2.1 Upgrading via the internet.....                         | 41        |

|          |   |           |
|----------|---|-----------|
| 4.2.2    | Upgrading from a local mirror.....                  | 42        |
| 4.2.3    | Upgrading from a USB storage device.....            | 46        |
| 4.3      | Upgrade Types.....                                  | 49        |
| 4.3.1    | Standard upgrade.....                               | 49        |
| 4.3.2    | Upgrade and restore defaults.....                   | 50        |
| 4.3.3    | Upgrade and force factory defaults.....             | 51        |
| 4.4      | Upgrade logs.....                                   | 51        |
| <b>5</b> | <b>Data Handling Overview.....</b>                  | <b>52</b> |
| <b>6</b> | <b>Configuring Networking.....</b>                  | <b>55</b> |
| 6.1      | Configuring physical network interfaces.....        | 55        |
| 6.1.1    | Configurable parameters in standard mode.....       | 56        |
| 6.1.2    | Configurable parameters in expert mode.....         | 58        |
| 6.2      | Virtual network (VLAN) interfaces.....              | 61        |
| 6.2.1    | Configurable parameters in standard mode.....       | 63        |
| 6.2.2    | Configurable parameters in expert mode.....         | 64        |
| 6.3      | Network Time Protocol (NTP).....                    | 64        |
| 6.3.1    | Configurable parameters in standard mode.....       | 65        |
| 6.3.2    | Configurable parameters in expert mode.....         | 66        |
| 6.4      | Email configuration.....                            | 66        |
| 6.4.1    | Configurable parameters.....                        | 67        |
| 6.5      | Configuring the SSH Server.....                     | 67        |
| 6.5.1    | Configuring sshd via the web interface.....         | 68        |
| 6.5.2    | Configuring sshd from the command line.....         | 69        |
| 6.6      | Working with PPP.....                               | 69        |
| 6.6.1    | Setting up a PPP Connection.....                    | 69        |
| 6.6.2    | Monitoring a PPP connection.....                    | 72        |
| 6.7      | Configuring TCP to serial converters.....           | 74        |
| 6.7.1    | Simple server mode.....                             | 75        |
| 6.7.2    | Simple client mode.....                             | 77        |
| <b>7</b> | <b>Digitiser Configuration.....</b>                 | <b>78</b> |
| 7.1      | Configuring Digitisers using the web interface..... | 78        |
| 7.2      | Configuring digitisers from the command line.....   | 89        |
| <b>8</b> | <b>Digitiser Synchronisation.....</b>               | <b>90</b> |
| 8.1      | RTSTATUS packets.....                               | 90        |
| 8.2      | Using NTP with CMG-DAS units.....                   | 91        |
| 8.3      | Using GPS with Authenticated Digitisers.....        | 91        |
| 8.4      | Using NTP with Authenticated Digitisers.....        | 93        |
| 8.5      | Configuring NMEA as an NTP clock source.....        | 93        |
| 8.6      | Configuring NMEA output.....                        | 94        |

|  |                |
|--|----------------|
| <b>9 Receiving Data.....</b>                               | <b>97</b>      |
| 9.1 GCF from serial devices.....                           | 97             |
| 9.2 BRP - GCF From Network Devices.....                    | 101            |
| 9.2.1 Configurable parameters in standard mode.....        | 102            |
| 9.2.2 Configurable parameters in expert mode.....          | 103            |
| 9.3 Data from Scream! servers.....                         | 104            |
| <br><b>10 Recording and Retrieving Data.....</b>           | <br><b>107</b> |
| 10.1 Preparing removable drives.....                       | 107            |
| 10.2 Recording data.....                                   | 109            |
| 10.2.1 Configurable parameters in standard mode.....       | 110            |
| 10.2.2 Configurable parameters in expert mode.....         | 112            |
| 10.2.3 File name escape sequences.....                     | 115            |
| 10.3 Retrieving data.....                                  | 117            |
| 10.3.1 Retrieving data from the removable drive.....       | 117            |
| 10.3.2 Reading the removable drive on other computers..... | 127            |
| <br><b>11 Transmitting Data.....</b>                       | <br><b>128</b> |
| 11.1 GCF BRP Network Server.....                           | 128            |
| 11.1.1 Configurable parameters in standard mode.....       | 129            |
| 11.1.2 Configurable parameters in expert mode.....         | 131            |
| 11.2 GCF Scream Server.....                                | 133            |
| 11.2.1 Configurable parameters in standard mode.....       | 134            |
| 11.2.2 Configurable parameters in expert mode.....         | 137            |
| 11.3 SEEDlink.....   | 138            |
| 11.3.1 The GDI Mini-SEED compressor.....                   | 138            |
| 11.3.2 The SEEDlink server.....                            | 142            |
| 11.4 Güralp Seismic Monitoring System.....                 | 145            |
| 11.4.1 Configurable parameters in standard mode.....       | 145            |
| 11.4.2 Configurable parameters in expert mode.....         | 147            |
| 11.5 Quick Seismic Characteristic Data.....                | 148            |
| 11.5.1 Configurable parameters in standard mode.....       | 149            |
| 11.5.2 Configurable parameters in expert mode.....         | 150            |
| 11.6 WIN Sender.....                                       | 151            |
| 11.6.1 Configurable parameters in standard mode.....       | 152            |
| 11.6.2 Configurable parameters in expert mode.....         | 154            |
| <br><b>12 Building Networks.....</b>                       | <br><b>155</b> |
| 12.1 GDI-link.....   | 155            |
| 12.1.1 The GDI-link transmitter.....                       | 155            |
| 12.1.2 The GDI link receiver.....                          | 158            |
| 12.2 Güralp Secure TCP Multiplexer.....                    | 161            |
| 12.2.1 The GSTM Client.....                                | 161            |
| 12.2.2 The GSTM Server.....                                | 164            |

|  |                |
|--|----------------|
| <b>13 Monitoring Operations.....</b>                               | <b>168</b>     |
| 13.1 Diagnostics and the Summary menu.....                         | 168            |
| 13.1.1 System Status.....  | 168            |
| 13.1.2 System Log.....   | 169            |
| 13.1.3 Incoming Data.....  | 170            |
| 13.1.4 Version and Serial Numbers.....                             | 171            |
| 13.2 The Control Menu.....   | 171            |
| 13.2.1 Digital I/O (power control and anti-tamper monitoring)..... | 171            |
| 13.2.2 Digitiser/Sensor Control.....                               | 173            |
| 13.2.3 Rebooting.....  | 181            |
| 13.2.4 Services.....   | 181            |
| 13.2.5 RAID Array Services.....                                    | 182            |
| 13.3 Tools Menu.....   | 182            |
| 13.3.1 Passwords.....  | 182            |
| 13.3.2 GCF Audit Log Viewer.....                                   | 182            |
| 13.3.3 GDI Channels Display.....                                   | 185            |
| <br><b>14 Appendices.....</b>                                      | <br><b>189</b> |
| 14.1 Setting the System Identity (Hostname).....                   | 189            |
| 14.2 Authenticated Digitisers.....                                 | 190            |
| 14.2.1 Internal Connections.....                                   | 191            |
| 14.2.2 Variable Gain Inputs.....                                   | 193            |
| 14.2.3 USB operations.....   | 196            |
| 14.3 Connector pin-outs.....                                       | 198            |
| 14.3.1 Peli-case: PORTs A, B, C.....                               | 198            |
| 14.3.2 Peli-case: DATA OUT port.....                               | 199            |
| 14.3.3 Peli-case: USB.....   | 200            |
| 14.3.4 Peli-case: NETWORK.....                                     | 201            |
| 14.3.5 Peli-case: Console.....                                     | 202            |
| 14.3.6 Cylinder: GPIO.....   | 203            |
| 14.3.7 Cylinder: GPS.....  | 204            |
| 14.3.8 Cylinder: USB.....  | 205            |
| 14.3.9 Cylinder: Power.....  | 206            |
| 14.3.10 Cylinder: Ethernet.....                                    | 207            |
| 14.3.11 Cylinder: Data.....  | 208            |
| 14.3.12 Cylinder: SENSOR A & B.....                                | 209            |
| 14.3.13 Cylinder: Auxiliary Input.....                             | 210            |
| 14.4 Using Minicom.....  | 211            |
| <br><b>15 Revision history.....</b>                                | <br><b>214</b> |

# 1 Introduction

---

The CMG-EAM (Embedded Acquisition Module) is a versatile module intended to integrate one or more seismic sensors with various communications systems. It can also act as a stand-alone data recorder or as a communications hub in larger networks.



This document describes the configuration and operation of Platinum Firmware, which is the native firmware of CMG-EAMs, CMG-NAMs and CMG-DAS units. CMG-DCMs can be upgraded to run Platinum firmware: for such units, once upgraded, this manual should be used instead of MAN-DCM-0001.

The CMG-DCM is a stand-alone communications module equipped with a removable hard drive (located under the lid), three bi-directional serial ports and support for external USB storage devices and Ethernet networking. Some CMG-DCMs were embedded into CMG-DAS units such as the DM24S3DCM (see below).



The CMG-EAM is the next generation CMG-DCM and includes totally re-designed electronics. It provides all the above facilities along with an extra serial port (designated for console use), a battery-backed real-time clock, current, voltage and tamper-line monitoring plus an optional encryption/authentication module.



The CMG-EAM is available in a variety of packages including Peli-case (as shown above), borehole, ocean-bottom and metal tube (steel or aluminium) versions (top left).

CMG-EAMs are also supplied embedded into CMG-DAS units such as the DM24S6EAM.

The CMG-NAM (Network Appliance Module) is a rack-mountable device intended to complement data communications networks using CMG-EAMs, and contains more interfaces, processing power and storage. The CMG-NAM is intended for use in a data centre and consumes more power than the CMG-EAM, which was designed specifically to be a low power device.



The CMG-DAS range of products combine the flagship CMG-DM24 analogue-to-digital converter with the communications, storage and protocol flexibility of the CMG-EAM in a single package.

They are available in numerous packages, including Peli-case, steel or aluminium tubes and sensor-top versions.

All of these units are Linux-based devices but no Linux knowledge is required. The use of Linux provides a high degree of flexibility: additional functionality can often be added on request – contact Gralp Systems for further information.

## 1.1 A Note on Terminology

---

Güralp Systems Ltd are aware that various common technical terms have acquired subtly different meanings for different audiences. The following terms are used consistently within this document and are intended to have the meanings given below:

### 1.1.1 Sensor

---

By “sensor”, we mean a seismometer (accelerometer or velocimeter) or other transducing instrument (e.g. geophone or hydrophone) with analogue outputs - i.e. where a continuously varying voltage is used to represent the magnitude of the quantity being measured.

An example of a sensor is the CMG-3T true broadband seismometer, depicted on the right in standard configuration.



### 1.1.2 Digitiser

---



By “digitiser”, we mean an electronic device designed to accept analogue inputs from one or more sensors and, using sampling techniques, convert these analogue signals into streams of numerical data, which are then stored or transmitted digitally.

An example of a digitiser is the CMG-DM24 shown on the right in standard form and, on the left, packaged for borehole operation.





### 1.1.3 Digital Sensor or Digital Instrument

---

By “Digital Sensor” or “Digital Instrument”, we mean a single unit combining the functions of both sensor and digitiser - with the meanings defined above.



Within this document, the term digital sensor is used in the context of either digital inputs - which may usefully be connected to either digitisers or digital sensors - or configuration dialogues which can be used to configure both stand-alone digitisers or the digitiser modules embedded within digital sensors.

An example of a digital sensor is the CMG-3TD true broadband digital seismometer, shown on the left in standard configuration and, on the right, in bore-hole format.



## 1.2 Hardware Overview

---

Platinum firmware runs on CMG-EAMs, CMG-NAMs, CMG-DASs and CMG-DCMs. CMG-DCM units (Mk2x and above) shipped with earlier firmware can be field-upgraded to run Platinum firmware either over the internet, from a local computer or from a USB data storage device.

The CMG-EAM is based upon an Intel PXA270 32-bit processor running at 312MHz with 64Mb of RAM and 512Mb of on-board flash. The amount of flash memory can be increased with the use of Güralp plug-in flash modules. The CMG-EAM has 100Base-TX Ethernet, up to 8 serial ports for connecting to external devices and several USB ports.

The CMG-DCM uses an Intel SA1100 (StrongArm) 32-bit processor running at 220MHz with 64Mb of RAM and 192Mb of on-board flash. The CMG-DCM has up to 7 serial ports for external devices and 10Base-T Ethernet.

The CMG-NAM is a flexible platform but is generally based upon a VIA C7 processor with 512Mb of RAM and various options for local storage, including RAID arrays. It has 100Base-TX Ethernet.

## 1.3 Software Overview

---

The Platinum firmware is very flexible and can be configured to perform many tasks. An overview of its capabilities is presented here:

- Data acquisition:
  - Data can be acquired in various formats via Ethernet or serial ports.
- Recording:
  - Data can be recorded to removable disk in various formats. Recording initially occurs to internal flash, which is flushed to removable disk when full or on demand. This minimises power usage;
  - The removable disk can be removed at any time without data loss.
- Data forwarding:
  - GCF output via serial port or TCP stream;
  - GCF output via Scream Server (TCP/UDP);
  - Güralp Data Interconnect (GDI), used for interchanging data both between CMG-EAMs and between CMG-EAMs and CMG-NAMs;
  - CD1.1 output;
  - WIN output;
  - QSCD (Quick Seismic Characteristic Data; designed by KIGAM) output;
  - GSMS (Güralp Seismic Monitoring System) output.
- Network communication:
  - The CMG-EAM has a built-in wired Ethernet connection;
  - Modem support (Iridium, GPRS, etc.);

- Support for multiple redundant network links to increase resilience;
- Other connectivity options, such as wireless Ethernet (IEEE802.11) and Bluetooth can be added on request, please contact Güralp sales for more information.
- Processing:
  - Various types of data processing can be carried out by the CMG-EAM. Please contact Güralp sales for more information.

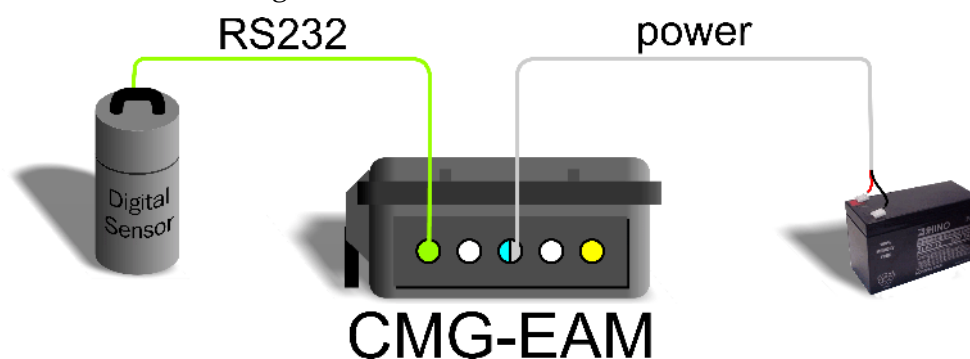
Section 5 gives a description of how data is handled within the CMG-EAM.

## 1.4 Typical Applications ---

### 1.4.1 Autonomous remote data-logger ---

In this application, depicted below, a CMG-EAM is used to collect data from a digital instrument (or analogue instrument and digitiser) and store it on its hard drive. The low power consumption and high storage capacity of the CMG-EAM makes it ideal for this purpose.

Where appropriate, the battery supply can be augmented with a solar panel and the CMG-EAM is capable of interfacing with and monitoring the associated charge controller.

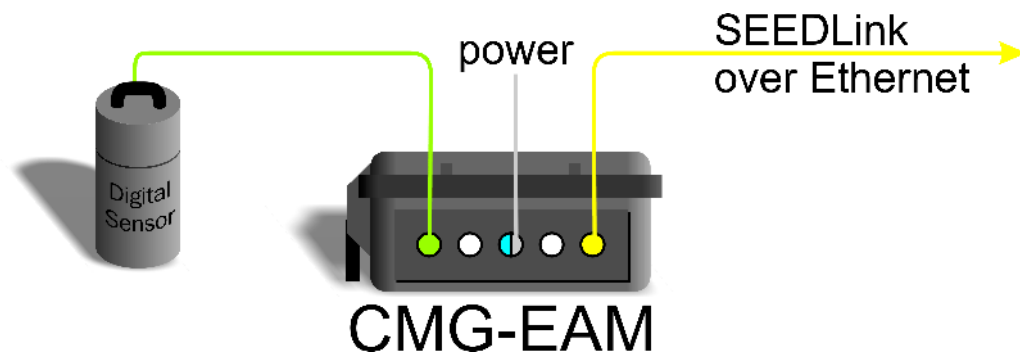


If it is desired to contact the CMG-EAM for monitoring or urgent data download purposes, the unit can be fitted with a GPRS or satellite modem, allowing remote connectivity.

### 1.4.2 Protocol Converter ---

The CMG-EAM can be deployed as a protocol converter: the wide variety of output formats and connectivity options make it ideal for

this application. In the illustration above, a digital instrument's GCF output is retransmitted as SEEDLink data over Ethernet.

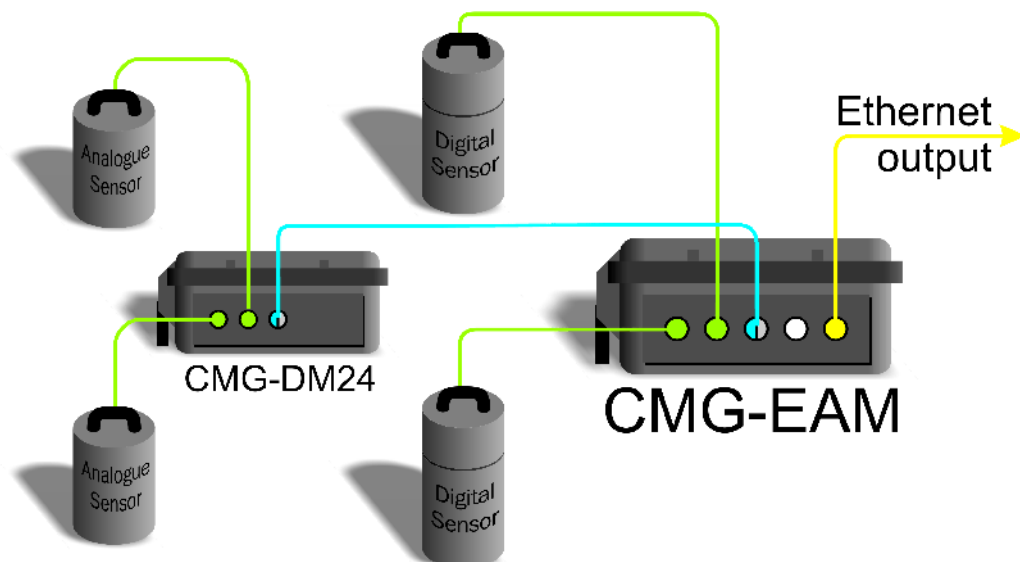


### 1.4.3 Array Concentrator

---

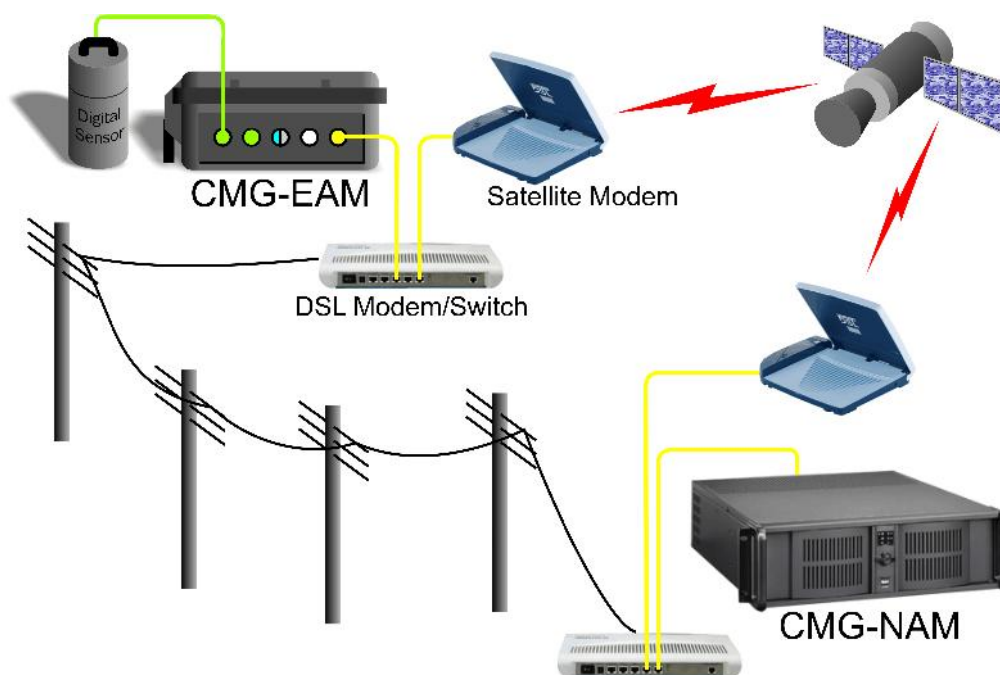
The CMG-EAM is well suited to combining the data from a number of instruments in an array and retransmitting them over a single link (serial or network).

If the output link is over a network, all three serial ports of a standard CMG-EAM (including the “DATA OUT” port) are available for connection to digitisers or digital instruments, allowing up to eighteen channels to be aggregated. An arbitrary number of CMG-EAMs may be chained together, allowing for even more extensive arrangements.



#### 1.4.4 Resilient Networking

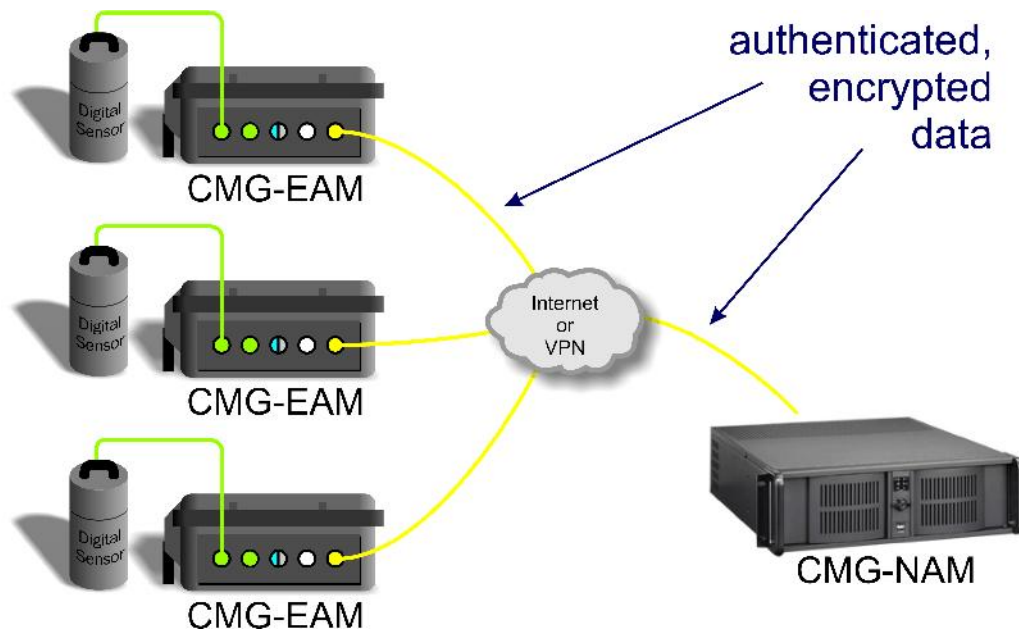
Platinum firmware includes a number of ways to implement network resilience. For example, the GSTM protocol (for communication between Platinum units) allows data to be routed over a low-cost but unreliable DSL network with automatic switch-over to a higher-cost satellite link only when the DSL network is unavailable. The failed link is regularly retried and, when communication is re-established, the data are re-routed back to the lower cost link.



It is also possible to use data filtering (by channel name and/or sample rate) in such a way that, should it become necessary to use the higher-cost link, only high priority data (e.g. samples resulting from an activated trigger) are sent across this link while lower priority data are enqueued until the low-cost link becomes available again.

### 1.4.5 CD1.1 Networking

---



Platinum firmware has support for CD1.1 frame generation and forwarding with strong encryption and authentication provided by an optional embedded Spyrys hardware encryption device, allowing CMG-EAMs and CMG-NAMs to form the basis of a secure CD1.1 network.

## 1.5 Document Conventions

---

Throughout this manual, examples are given of command-line interactions. In all such examples, a fixed-width typeface will be used:

Example of the fixed-width typeface used.

Commands that you are required to type will be shown in bold:

Example of the fixed-width, bold-face typeface.

Where data that you type may vary depending on your individual configuration, such as parameters to commands, these data are additionally shown in italics:

Example of the fixed-width, bold-faced, italic typeface.

Putting these together into a single example:

System prompt: **user input with variable parameters**

## 2 First Steps

---

The CMG-EAM can be configured and monitored either over an Ethernet network or via a serial (RS232) line. Network access is preferred. The configuration interface is accessible using a web browser or, in character mode, using ssh or over a serial connection from a terminal emulator.

All models are fitted with at least one network port which can be automatically configured using DHCP. If DHCP is not available, serial access is required in order to set up the network parameters.

The CMG-EAM has four serial ports, any of which can be configured for this purpose, although the 'D' connector located under the lid is a dedicated console port.

The CMG-DCM has three serial ports: the port labelled “DATA OUT” is normally used for console access and a combined serial and power cable is provided for this purpose.

The hardware fitted to CMG-NAMs varies but one serial port will usually be designated as the console port.

### 2.1 Connecting to the Serial Port

---

The CMG-EAM's console port is a 9-pin 'D' connector (with DCE wiring) located under its lid. It can be connected via a serial (RS232) modem cable (i.e. pins 2 (RxD), 3 (TxD) and 5 (ground) connected straight through) to a serial terminal or to a PC running either ScreaM! or terminal emulation software. The default settings for this port are as follows:

- 38,400 baud;
- 8 data bits, no parity, 1 stop bit (8N1); and
- No flow control.

These settings are not configurable, preventing accidental lock-out due to inadvertent changing of the port settings.

The CMG-DCM does not have a dedicated console port: the “DATA OUT” port is normally used for console access. A combined power and serial cable is provided with both CMG-EAMs and CMG-DCMs for connection to this port.

The “DATA OUT” port can be connected to a serial terminal or PC running either *Scream!* or terminal emulation software. The default settings for this port are as follows:

- 115,200 baud;
- 8 data bits, no parity, 1 stop bit (8N1); and
- No flow control.

**Note:** these settings can be changed and, indeed, the port re-configured for a different purpose, preventing console access.

Once you have connected the serial cable, you can run a terminal emulator to interact with the CMG-EAM. Under Windows you are advised to use the terminal emulator shipped with *Scream!* v4.5, although HyperTerminal can be used. Under Unix or Linux, Miquel van Smoorenburg's *minicom* terminal emulator (more details from <http://alioth.debian.org/projects/minicom>) is recommended, although most terminal emulators can be used. An extract from Minicom's user manual is reproduced in Section 14.4, on page 211.

Once connected, press the <Enter> key until you see the login prompt.

**Note:** If a terminal session has just been closed, it can take up to 10 seconds for a new session to start.

You should log in as *root*, which is the standard Unix “superuser”. The password is set to *rootme* when shipped from the factory. To log in, type *root* and press enter. When prompted for the password, type *rootme* (nothing will be echoed while you are typing) and press <enter>. You will then be presented with a shell prompt, which will accept commands:

```
eam999 login: root
Password: rootme
eam999 ~ #
```

The output may vary slightly due to the configuration of the unit. In particular, the hostname (*eam999* in this example) will be different.

Some applications on the CMG-EAM use a system called “ncurses”, which allows graphical interfaces to be implemented on text-only terminals. This requires the applications to know the type of terminal



from which they are being accessed. The terminal type is stored in an environment variable called **TERM**, which is queried with the command

```
eam999 ~ # echo $TERM
vt100
eam999 ~ #
```

(note the use of the \$ sign when accessing the value of this variable) and set with the command

```
eam999 ~ #: export TERM=vt100
```

No spaces should be used around the '=' sign.

The CMG-EAM is aware of around thirty different terminal types and uses the “terminfo” system to support them (so you can add your own types, if you need). Files describing each terminal type are stored under the directory (folder) `/usr/share/terminfo` in sub-directories named after the initial letter of the terminal name.

Some settings for specific applications are:

- **SSH** under Unix, or **puTTY** under Windows (running in SSH mode): no action required - the SSH protocol sets the **TERM** environment variable automatically.
- **Minicom** under Unix: no change. Minicom emulates a vt100-style terminal and automatically maps the keystrokes and display sequences for the actual terminal you are using, so the default **TERM** setting of **vt100** is correct.
- **HyperTerminal** under Windows: choose the File menu option “Settings”, and ensure that the terminal type is set to **VT100**. HyperTerminal will then emulate a vt100-style terminal, which will match the default **TERM** of **vt100** on the CMG-EAM.

These settings will provide the best results for the listed applications. Note that when connecting with **SSH** from, for example, an **xterm** window, use of the mouse for menu navigation is supported.

---

## 2.2 Connecting to the network port

To use the network port, you must first set up a network address. Some networks use the Dynamic Host Configuration Protocol (DHCP) to automatically assign network addresses; others need manual configuration (normally referred to as “static” addressing). Before you

can access the CMG-EAM over a network, you must set (for static addresses) or discover (if you use DHCP) its IP address.

### 2.2.1 DHCP-assigned addresses

---

If your network uses DHCP to assign addresses, connect the CMG-EAM to the network and reboot it by turning the power off and on again. Your network administrator may then be able to tell you the address that has been assigned to the CMG-EAM but, if not, you can connect via a serial port and issue the `ip` command:

```
eam999 ~ # ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
    link/ether 00:50:c2:40:54:75 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.101/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::250:c2ff:fe40:5475/64 scope link
        valid_lft forever preferred_lft forever
eam999 ~ #
```

The key things to look for here are the adapter status and the IP address. The first line of the output should contain the word `UP`, confirming that the adaptor has been enabled. The IP address that has been assigned is shown on the line beginning `inet` - in this case, it is `192.168.0.101` (with a netmask of 24-bits indicated by `/24`).

**Note:** With an IP version 6 network, the IP address will be on a line beginning `inet6`. In practice, most networks today are still IPv4, as in the above example.

When using DHCP, it is recommended that the DHCP administrator allocates a fixed IP address to the CMG-EAM's MAC address in order to avoid unexpected address changes.

**Note:** If you are setting up a unit in the laboratory for subsequent deployment in the field, you can set up the final network address using the web interface and over-ride it with a temporary, static network address using the command line. The web-configured address will take effect when the unit is next rebooted.

### 2.2.2 Assigning a static IP address

---

If the network you are connecting to does not use DHCP, you must first connect via a serial port in order to configure a static IP address. Connect the CMG-EAM to the network and power-cycle it before proceeding: its network interface will not be enabled unless it sees a network at boot.

Once logged in, issue the following command:

```
eam999 ~ # ip addr add 192.168.0.1/24 dev eth0
```

You can change the IP address to anything you wish. It must be specified in CIDR format where the actual address is followed by the number of bits of the network mask. The above example uses 192.168.0.1 with a netmask of 255.255.255.0 (24 bits of network address). A PC connected to this network could communicate with the CMG-EAM if it was configured to use an IP address of (for example) 192.168.0.2 with a matching netmask of 255.255.255.0.

If you wish to connect to the CMG-EAM from a PC, they must either both have the same network address (usually the first three numbers of the IP address) or be able to connect to each other via routers. In the latter case, you will need to tell the CMG-EAM the address of its default router. Issue the command:

```
eam999 ~ # ip route add default via 192.168.0.254
```

substituting the address of your network's default router in place of the address shown.

**Note:** Both the static IP address and any route configured in this way are temporary and will persist only until the CMG-EAM is rebooted or powered off. Refer to section 6.1 on page 55 for information about configuring permanent static IP addresses and routes.

### 2.2.3 Connecting to the web interface

---

The CMG-EAM provides a web (HTTP) interface which is intended to be used for most configuration and control tasks. This is the recommended way of controlling the CMG-EAM.

Once the IP address of the CMG-EAM has been set or determined, you can connect to its web-server. Simply type `http://` followed by the IP address of the unit into your web browser's address bar (e.g. `http://192.168.0.1` ). You should be prompted for a user-name and password. The user-name is `root` and the initial password, as shipped, is `rootme` (the same as on the command line).

If you are connecting to the CMG-EAM over a network that you consider insecure, it is recommended that you use the HTTPS (secure HTTP) protocol, which uses TLS to encrypt the link. Simply change the `http://` prefix to `https://` in the browser's address bar. Most browsers will complain that the certificate cannot be verified: This is not a problem: simply press the “accept” button to proceed. The link will then be encrypted and nobody will be able to “sniff the wire” in an attempt to discover passwords and other data.

Once connected and logged in, you will be presented with the main summary screen. This contains general information about the status and health of the CMG-EAM:

## Main menu

dcm105

**Summary**

[System events](#)

[System status](#)

[Version and serial numbers](#)

**Control**

[Port A sensor](#)

[GSLA-1566](#)

[Power](#)

[Services](#)

**Tools**

[CD1.1 log analyser](#)

[Firmware](#)

[GCF audit log viewer](#)

[GDI channels](#)

[diagnostics](#)

|  |   |  |
|--|---|--|
| <b>System uptime</b><br>Status: good —<br>2009-06-23T09:36:17Z<br>System has been up for approximately 3 days. | <b>GCF in: Port A</b><br>Status: good —<br>2009-06-23T09:37:30Z<br>Last 5 minutes:<br><ul style="list-style-type: none"> <li>• 112 blocks (0.4 per second).</li> <li>• 0 naks (0.0 per second).</li> </ul>                      | <b>GCF in: Port B</b><br>Status: unknown —<br>2009-06-23T09:37:30Z<br><b>No blocks seen.</b> |
| <b>GCF in: Port F</b><br>Status: unknown —<br>2009-06-23T09:37:31Z<br><b>No blocks seen.</b>                   | <b>NTP</b><br>Status: good —<br>2009-06-23T09:37:08Z<br><ul style="list-style-type: none"> <li>• NTP has locked the system clock.</li> <li>• Estimated error is 3444µs.</li> <li>• Clock source is Guralp digitiser.</li> </ul> |  |

Generated at 2009-06-23T09:37:35Z by `libstatus.cgi 1.2.6`. Portions of output copyright (c)2009, Guralp Systems Ltd.

The exact contents and layout of this screen will vary depending on the configuration of both the EAM and of any attached hardware.

If the browser fails to connect, the most likely explanation is that the machine running the browser does not have working network communications to and from the CMG-EAM. This can be verified by “pinging” the IP address of the browser from the command line of the CMG\_CMG-EAM:

```
eam999 ~ # ping -c3 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
64 bytes from 192.168.0.2: seq=0 ttl=63 time=2.284 ms
64 bytes from 192.168.0.2: seq=1 ttl=63 time=1.129 ms
64 bytes from 192.168.0.2: seq=2 ttl=63 time=1.944 ms
--- 192.168.42.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.129/1.785/2.284 ms
eam999 ~ #
```

To resolve this class of problem, ensure that the cables are functioning (which can be verified by checking the diagnostic lights on most switches/hubs) and double-check that the PC and CMG-EAM are on the same subnet (which means the netmasks must match and the first sections – as defined by the netmask - of the IP addresses must match). The website [http://en.wikipedia.org/wiki/IP\\_address](http://en.wikipedia.org/wiki/IP_address) has some useful information for those for whom sub-networking is unfamiliar.

---

## 2.2.4 Connecting using SSH

SSH (secure **shell**) is the most flexible way to control a CMG-EAM, but it is less friendly than using the web interface. It is possible to configure more advanced operations using SSH but the majority of control and configuration tasks can be achieved most easily through the web interface.

SSH is shipped as standard with most Linux distributions and is available for Windows as part of *PuTTY*, available for free from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

The next section will discuss the use of the `ssh` command-line utility; PuTTY-specific details are provided in the section after.

### 2.2.4.1 SSH connections using the `ssh` program

To use SSH, you must know or discover the IP address of the unit, as described in the previous section. Once you have the IP address, issue the `SSH` command on the PC you are using:

```
mypc$ ssh root@192.168.0.1
```

Replace `192.168.0.1` with the IP address of the CMG-EAM.

The first time you use SSH to connect to a host, you will be asked to verify the “host key”. This can be ignored the first time but, if you are ever asked this again, it means that either the host key of the CMG-EAM has changed – perhaps because of a firmware upgrade – or there is a network address conflict or, worse, a security problem on your network.

```
user@mypc:~$ ssh root@192.168.0.1
The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established.
RSA key fingerprint is 62:a6:70:29:d4:1a:db:5a:75:6e:96:13:54:f5:a9:d9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.1' (RSA) to the list of known hosts.
root@192.168.0.1's password:
eam999 ~ #
```

You will be prompted for a password; the default password is `rootme`. Note that no characters will be echoed to the screen as you type the password.

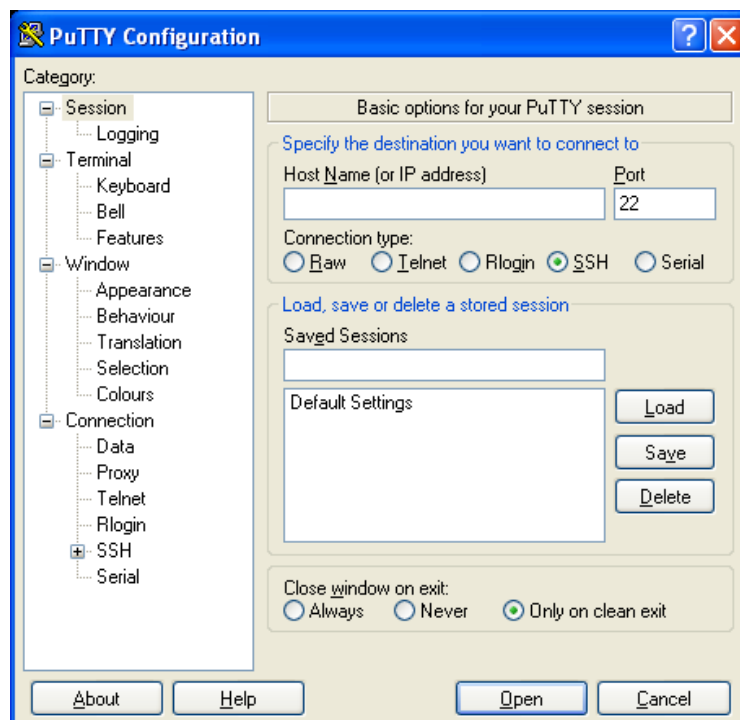
Once connected, you will be presented with a shell prompt which is ready to accept commands.

When you are finished with your SSH session and want to disconnect, enter “exit” at the command line, or type a <Ctrl>D character. There are a number of escape sequences for controlling the session, all of which begin with a tilde ('~') so, if you need to send a tilde character to the CMG-EAM, type two tildes consecutively. For more information, see the section on “Escape Characters” in the SSH manual page at <http://man-wiki.net/index.php/1:ssh>

**Note:** If you plan to use ssh regularly to communicate with a CMG-EAM, you can configure the system to bypass the password prompt from a list of pre-authorised computer/user combinations. This involves generating a unique key-pair (for the user and PC which will access the CMG-EAM) and then copying the public half of the key-pair to the CMG-EAM. This is documented at <http://suso.org/docs/shell/ssh.sdf>

### 2.2.4.2 SSH connections using PuTTY

To use PuTTY, you must know or discover the IP address of the unit, as described in the previous section. Once you have the IP address, start PuTTY by choosing it from the “Start” menu or double-clicking on its icon. You will be presented with the following screen:



Enter the IP address of the CMG-EAM into the “Host Name (or IP address)” box, check that “SSH” is selected as the “Connection type” and then click the **Open** button.

The first time you use SSH to connect to a host, you will be asked to verify the “host key”:





This can be ignored the first time (simply click **Yes** to dismiss the dialogue) but, if you are ever asked this again, it means that either the host key of the CMG-EAM has changed – perhaps because of a

firmware upgrade – or there is a network address conflict or, worse, a security problem on your network.

You will now be prompted for a login name: the default is **root**. - type this at the prompt and hit <enter>. You will next be prompted for a password; the default password is **rootme**. Note that no characters will be echoed to the screen as you type the password.



Once connected, you will be presented with a shell prompt which is ready to accept commands. The shell prompt contains the CMG-EAM's serial number.

When you are finished with your SSH session and want to disconnect, type “exit” at the command line, or  + .

**Note:** If you plan to use ssh regularly to communicate with a CMG-EAM, you can configure the system to bypass the password prompt from a list of pre-authorised computer/user combinations. This involves generating a unique key-pair (for the user and PC which will access the CMG-EAM) and then copying the public half of the key-pair to the CMG-EAM. This is implemented using the PuTTYgen and Pageant programs: see section 6.5 on page 67 and the help facility within PuTTY for more information.

## 2.3 Changing the password

---

Access to a Platinum system is password-protected. As shipped, the user name is **root** and the password is **rootme**. The same password is used for both login and web authorisation. In the majority of cases, there is no need to alter the password from the default setting.



Where security is a concern - for example, where systems may be left connected to the internet for any significant period - you may wish to change the password. In this case, you should also use secure HTTP to access the web interface rather than the more common http. To do this, prefix the URL to the device with the **https:** protocol specifier rather than **http:**. For example, if you can access your system as **http://192.168.0.1**, you can also use **https://192.168.0.1** and this will prevent your new password from being retrieved by eavesdroppers.

There is much information available on-line for choosing a strong password, for example: <http://tinyurl.com/strongpws>.

Selecting “Passwords” from the “Tools” menu takes you to a screen from which you can change the password used for both command-line access and for the web interface.

[Home](#) → [Tools](#) → [Passwords](#)

---

## Password change

Select user:

|                      |                  |
|----------------------|------------------|
| <input type="text"/> | Current password |
| <input type="text"/> | New password     |
| <input type="text"/> | Confirm          |

---

*Generated at 2010-02-04T13:55:35Z by passwd.cgi from Pt-users 1.0.4. Portions of output copyright (c)2010, Guralp Systems Ltd..*

Currently, the only user configured on a CMG-EAM is root. The password is changed immediately but the built-in web-server can continue to use the old password for some time after a change. If this is a problem, the web service can be restarted from the Services page (see section 13.2.4 on page 181) by clicking the “Restart” button for the “httpd” service.

To change the password from the command line, issue the command **passwd**: You will be prompted twice for the desired new password:

```
eam2010 ~ # passwd
New password:
Repeat:
Password changed.
eam2010 ~ #
```

**Note:** There is no way to recover a lost password and it is very awkward (although not impossible) to regain access to a system without a password. Despite much conventional wisdom, you may be safer writing the password down and storing it in a physically secure place rather than risk forgetting it.

If you do lose your password, please contact Gralp Systems' technical support team for advice.

## 3 Configuration System Overview

All key configuration tasks can be carried out either from the command line, using the `gconfig` tool, or via the web interface, using the “Configuration” → “All options” menu item. Both these methods invoke the same underlying software and present identical navigation and parameter options.

The web interface presents some additional options. Some of these are merely short-cuts into the main configuration system while others offer additional monitoring information. Configuration of attached digitisers can be carried out using the web interface but not from the CMG-EAM's command line (although access to the digitiser's command line is available).

The command-line interface also supports a number of advanced facilities which are not available via the main configuration system: these are mostly diagnostic tools which are not required for normal operation.

### 3.1 Using the configuration system via the web interface

The web interface to the configuration system is split into two frames.

|  |   |  |  |
|--|---|--|--|
| <b>Main menu</b><br><br><b>eam2243</b><br><br><b>Summary</b><br><a href="#">System status</a><br><a href="#">Version and serial numbers</a><br><br><b>Control</b><br><a href="#">Digital I/O</a><br><a href="#">Reboot</a><br><a href="#">Services</a> | <b>System uptime</b><br>Status: good —<br>2010-01-15T16:17:01Z<br>System has only just come up.   | <b>GCF in: Port A</b><br>Status: unknown —<br>2010-01-15T16:18:09Z<br><b>No blocks seen.</b> | <b>GCF in: Port C</b><br>Status: unknown —<br>2010-01-15T16:18:09Z<br><b>No blocks seen.</b> |
|  | <b>NTP</b><br>Status: unknown —<br>2010-01-15T16:17:58Z   |  |  |
|  | <ul style="list-style-type: none"> <li>• NTP has not locked the system clock as the estimated error is too large.</li> <li>• Estimated error is 1000000µs.</li> </ul> |  |  |
|  |   |  |  |

The left-hand frame contains the system ID above a menu while the right-hand frame displays sub-menus, input forms and display screens. When a sub-menu has been used, the top of the right-hand frame shows the menu options that have been selected in order to reach the current screen. These options are hyper-linked and can be used to return to previous screens.

In the example shown below, the operator has clicked on “All options” in the left-hand menu (in the “Configuration” section) and then chosen “Networking” from a right-hand pane sub-menu and then “eth0” from the resulting right-hand pane sub-menu.

|                     |      |
|---------------------|------|
| Device              | eth0 |
| Device name (Fixed) | eth0 |

The “All options” item from the “Configuration” section of the left-hand menu is referred to simply as “Configuration” and this is also the entry point for the command-line interface to the configuration system. This page can be reached from almost every point in the system by clicking on the [Home](#) button displayed at the bottom of most right-hand pane forms.

In some cases, the same screen can be reached by a variety of routes. For example, the screen above can be reached (with two fewer clicks) by selecting the “Interfaces” short-cut from the “Networking” section of the left-hand pane menu and then clicking through to “eth0”. The links at the top of the right-hand pane will not reflect the fact that a short-cut has been taken.

|                     |      |
|---------------------|------|
| Device              | eth0 |
| Device name (Fixed) | eth0 |

Most of the configuration forms have on-line help available. This can be turned on for the current page by clicking the [Help](#) button displayed at the bottom of the form. The help text will appear in blue, interleaved with the form itself.

Many of the configuration forms have two modes, “simple” and “expert”. They display, by default, only the parameters most likely to be used. For example, the network interface form mentioned above does not normally display IP aliasing parameters. When access is required to these additional features, they can be displayed by clicking

the **Expert** button displayed at the bottom of the form. They can be hidden again by clicking on the **Simple** button.

In all cases, any changes made to the contents of the forms only exist in the browser until they are sent to the CMG-EAM using the **Submit** button.

User input to the forms can often only be validated after submission. Where invalid parameters have been detected, this is signalled back to the operator by redrawing the same form with extra text, in red, added. The number of errors is displayed at the top of the form:

[Home](#) → [Configuration](#) → [Networking](#) → [eth0](#)

## Network Interface eth0

2 errors found

|             |   |
|-------------|---|
| Device      | <input type="text" value="eth0"/><br>Device name (Fixed)              |
| MAC address | <input type="text" value="00:01:c0:05:43:cb"/><br>MAC address (Fixed) |
| Description | <input type="text" value="Primary wired network interface"/>          |

The actual error messages are displayed next to the fields whose contents have offended:

The following parameters are used only in a static configuration.

|  |  |
|--|--|
| IP address   | <input type="text" value="192.168.0.1"/><br>Address in IPv4 or IPv6 format, with CIDR format netmask (see help)  |
| Missing CIDR label or netmask length. Add trailing /number of bits ? |  |
| Default route (gateway)  | <input type="text" value="192.268.0.254"/><br>The IP address of the gateway router, for access to other networks |
| Invalid address  |  |

Throughout the remainder of this manual, screen-shots of the configuration system's web interface will normally omit the left-hand pane, as in the two illustrations above.

## 3.2 Using the command-line configuration system

---

All of the configuration facilities available under the “All options” menu item (in the left-hand menu of the web interface) are also available from a text-based GUI tool called `gconfig` (Güralp Configurator). This can be accessed either by using a serial link or, over the network, by using `ssh`.

Connection via a serial link is discussed in section 2.1 on page 15 and connecting over Ethernet is described in section 2.2 on page 17. The use of `ssh` is covered in section 2.2.4 on page 21.

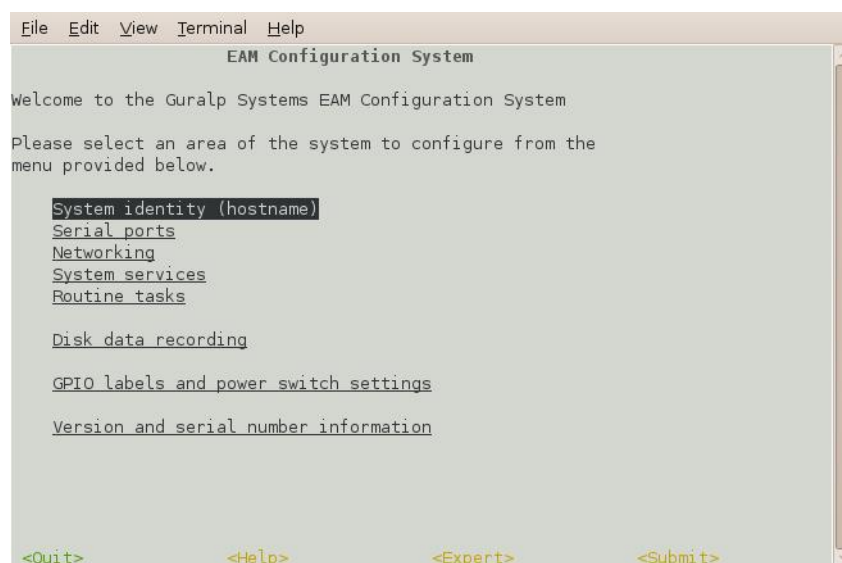
For optimal display, you must let the CMG\_EAM know what type of terminal or emulator you are using. This is done by setting the terminal type as an environment variable using the command:

```
eam999 ~ # export TERM=TERM_TYPE
```

The value of the `TERM` variable, **`TERM_TYPE`**, depends upon the terminal emulator you are using and should be chosen as follows:

| Emulator in use                                | TERM setting   |
|--|--|
| <code>ssh</code> under Unix                    | No action required - the <code>ssh</code> protocol sets the <code>TERM</code> environment variable automatically.  |
| PuTTY (in <code>ssh</code> mode) under Windows | No action required - the <code>ssh</code> protocol sets the <code>TERM</code> environment variable automatically.<br><br>PuTTY will default to <code>xterm</code> emulation, allowing the mouse to be used within <code>gconfig</code> .                       |
| Minicom under Unix                             | Minicom emulates a <code>vt100</code> -style terminal and automatically maps the keystrokes and display sequences for the actual terminal you are using, so the default <code>TERM</code> setting of <code>vt100</code> is correct.                            |
| HyperTerminal under Windows                    | Using the File menu option “Settings”, ensure that the terminal type is set to <code>VT100</code> . HyperTerminal will then emulate a <code>vt100</code> -style terminal, which will match the default <code>TERM</code> of <code>vt100</code> on the CMG-EAM. |
| Scream!  | Scream! versions before 4.5 do not support the required screen-drawing control codes so its use with <code>gconfig</code> is not recommended.  |

When you enter the `gconfig` command, the initial screen looks like this:




The `gconfig` interface can be navigated entirely using the keyboard but, if you use `xterm` (or your terminal emulator supports an “xterm” mode) you can use your mouse to select menu items, input fields and items from drop-down menus. The scroll-wheel is not currently supported, so you need to use the keyboard to access second and subsequent pages of multi-page forms.




`gconfig` displays menus and forms. The screen-shot above is an example of a menu. The following table shows the navigation keys that are available for use with menus:

| Keystroke     | Used for...   |
|---------------|---|
| →, ↓ or ⇨     | Cursor to next item   |
| ← or ↑        | Cursor to previous item   |
| ↵             | Select item under cursor  |
| Page Up or F6 | Move to the next page of a multi-page menu                            |
| Page Up or F5 | Move to the previous page of a multi-page menu                        |
| F1            | Go to the home menu or, if there already, exit <code>gconfig</code> . |

The four words enclosed in chevrons at the bottom of the above screen-shot,






act as push-buttons. They are always present at the bottom of each gconfig screen, although they change slightly according to the context. To invoke the action associated with any of them, move the cursor to it and press the  key.

In the example, all options other than  are disabled and this is indicated by the colour coding. If you select an item from a menu which leads to a sub-menu, the  option changes to  and invoking it will then take you back to the top-level menu.




Selecting a menu item will lead you either to another menu or to a form. Forms are composed of editable fields, which are either:

- Text-entry fields, into which the operator can type textual parameters. Text-entry fields are identified by surrounding braces: '[' and ']';
- Check-boxes, where the operator has a “yes/no” choice. Check-boxes are identified by surrounding guillemots: '{' and '}'; or
- Drop-down menus, where the operator must choose one option from a list. Drop-down menus are identified by surrounding chevrons: '<' and '>'.

To move between fields, use the ,  or  keys.






### 3.2.1 Text entry fields

---







To edit the contents of a text-entry field, place the cursor on the field, using the ,  or  keys, and start typing. Characters typed are always inserted at the current cursor position i.e. existing characters are never over-typed. The whole field is shown with a black background, as seen below, and the cursor is identifiable as a pale block.





The  and  keys move the cursor within the field and the  key deletes characters to the left of the cursor. When you are satisfied with the new value, the  and  keys allow you to move to the previous and next fields, respectively.

### 3.2.2 Check-boxes

To change the setting of a check-box, place the cursor on the field, using the ,  or  keys, and use the  key to toggle between selected and not selected. When you are satisfied with the new value, the  and  keys allow you to move to the previous and next fields, respectively.

When the value is “yes”, “enabled” or otherwise selected, the field is shown with an 'X' in it:

```

Description      [Primary wired network interface]
Enable interface [X]
Startup enable   {Y}

```

When the value is “no”, “disabled” or otherwise de-selected, the field is shown as blank:

```

Description      [Primary wired network interface]
Enable interface [ ]
Startup enable   {Y}





```

### 3.2.3 Drop-down menus

```

MTU               [ ]
Configuration method <-DHCP (Dynamic Host Configuration Protocol) >
DHCP options







```

To change the setting of a drop-down menu field, place the cursor on the field, using the ,  or  keys, and activate the menu by using the  key.

```



Startup enable    {Y}
Enact on submit
Media speed/type
MTU
Configuration     Unconfigured but powered up (possible VLAN trunk) ol) >
DHCP options       Static
                   DHCP (Dynamic Host Configuration Protocol)
                   Powered off
Extra dhcpd arguments [ ]




```

While the menu is active, you can move between options using the the , , ,  and  keys: the currently selected option is shown highlighted. When the desired option is selected, press the  key again to confirm the choice and de-activate the menu.

### 3.2.4 Using forms



---



Most of the configuration forms have on-line help available. This can be turned on for the current page by using the  button displayed at the bottom of the form. The help text will appear in blue, interleaved with the form itself. Help can also be activated using the  key.



Many of the configuration forms have two modes, “simple” and “expert”. They display, by default, only the parameters most likely to be used. For example, the network interface form does not normally display IP aliasing parameters. When access is required to these additional features, they can be displayed by using the  button displayed at the bottom of the form. They can be hidden again by using the  button. It is also possible to toggle between simple and expert mode using the  key.



Some forms are too large to fit in a single page. In this case, an indicator appears at the top right of the screen. For example, the network interface configuration form, in expert mode, takes three pages to display:



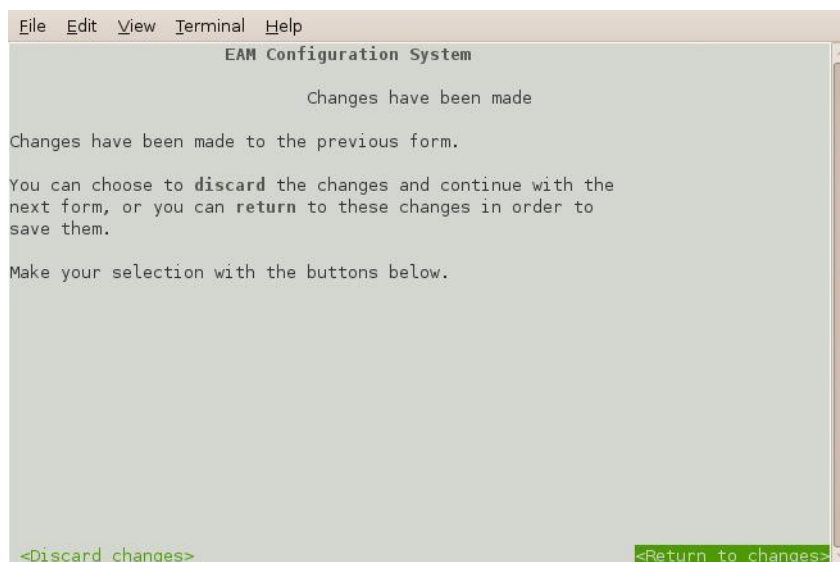
To move to subsequent pages, you can use either the  or the  key.


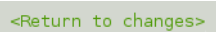
To return to previous pages, you can use  or .

When all required fields have been set to the desired values, the changes can be enacted by using the  button or the  key.






It is possible to leave any form by using the  button ( or the  key) but, if you have made changes to the contents of any fields, the system will warn you that you will lose your changes if you continue.











It offers an opportunity to return to the form:



Select  to ignore any parameters that you have altered and continue to the home menu or select  to review the form and, if desired, submit it before navigating away from it.

The following table provides a summary of all keystrokes that can be used when filling or navigating forms:

| Keystrokes used in forms   |  |
|--|--|
| Keystroke  | Used for...  |
|  or  | Cursor to next field or, if in activated drop-down menu field, next item in drop-down menu |
|   | Cursor to next field or, if in text field, move edit cursor rightwards                     |
|   | Cursor to previous field or, if in activated drop-down menu field, next item in drop-down  |
|   | Cursor to previous field or, if in text field, move edit cursor leftwards                  |

| Keystrokes used in forms   |   |
|--|---|
|   | Activate or deactivate list field or bottom-line button               |
|   | Toggle check-box  |
|   | Go to the home menu or, if there already, exit <code>gconfig</code> . |
|   | Display help text   |
|   | Show “expert mode” fields   |
|   | Submit the current form   |
|  or  | Move to the next page of a multi-page form                            |
|  or  | Move to the previous page of a multi-page form                        |

### 3.3 Configuration Management

---

The CMG-EAM has a comprehensive configuration management system that allows both complete configurations and individual classes of configuration information, such as data processing and networking, to be saved individually and merged during restoration.

This feature can be very useful when multiple CMG-EAMs are to be configured for a project. In a typical array with a central communications hub arrangement, only two data processing configurations need be created: one for the hub and one for an array element. The latter can then be copied from CMG-EAM to CMG-EAM to avoid having to configure each unit individually. Network configurations need be created for each element of the array and for the hub but these can all be created and stored on a single CMG-EAM. If the complete set of stored configurations is then copied to each machine and to any “hot spares”, then every CMG-EAM becomes rapidly interchangeable: all that is required to deploy a unit is to restore the correct data processing configuration (hub or element) and then restore the appropriate network configuration.

Configuration files can also be backed up and stored on different sites to provide a disaster management resource.

### 3.3.1 Saving a configuration

From the “Configuration” section of the main menu, select “Save/Restore”. The following screen appears:

#### Configuration management

Restore

| ID | Date       | Time  | Description     | Actions                 |
|----|------------|-------|-----------------|-------------------------|
| 1  | 2009/06/12 | 14:03 | standard config | Restore Download Delete |

Save

Checked modules will be saved:

| Module                                       | Description                                       |
|--|---|
| <input checked="" type="checkbox"/> platinum | Main instrument and data processing configuration |
| <input checked="" type="checkbox"/> network  | Networking and communications configuration       |
| <input checked="" type="checkbox"/> userid   | User names (ID) and passwords                     |
| <input checked="" type="checkbox"/> system   | Additional system core configuration              |

Description

Upload

Archive

Generated at 2009-07-13T15:35:59Z by *config-manage.cgi* 0.2.3. Portions of output copyright (c)2009, Guralp Systems Ltd.

To save a configuration, use the check-boxes to select which elements you wish to include, enter a descriptive name in the “Description” field and click on “Save configuration”. The configuration is saved onto the CMG-EAM and will appear in the list of saved configurations at the top of the page.

If you are using the web interface, you can download this configuration to the computer running the browser by clicking the “Download” button in the list of saved configurations at the top of the page.

### 3.3.2 Deleting a saved configuration

If a configuration has been saved in error or a saved configuration is no longer required, it can be deleted using the above screen. Each saved configuration in the “Restore” table has an associated “Delete” button in the “Actions” column. Clicking the button deletes the associated configuration.

### 3.3.3 Restoring a configuration

The same screen is used for restoring a configuration. Simply select the required saved configuration from the list at the top of the page and hit the restore button. The following screen appears:

#### Configuration management

2009/07/13 15:59 test

Restore modules

Checked modules will be restored:

|                                     | Module   | Description                                       |
|-------------------------------------|----------|---|
| <input checked="" type="checkbox"/> | platinum | Main instrument and data processing configuration |
| <input checked="" type="checkbox"/> | network  | Networking and communications configuration       |
| <input checked="" type="checkbox"/> | userid   | User names (ID) and passwords                     |
| <input checked="" type="checkbox"/> | system   | Additional system core configuration              |

Restore type

☒ User files restore  
☐ Full (core) restore  
☐ Full restore and purge all other modules

Action

[Return to Configuration management main form](#)

Generated at 2009-07-13T15:59:34Z by *config-manage.cgi* 0.2.3. Portions of output copyright (c)2009, Guralp Systems Ltd.

The date and time at which the configuration was saved is shown; in the example above, this is the 13<sup>th</sup> of July, 2009 at 15:59. The name of the configuration is also given; in the example above, this is “test”.

Even if a configuration was saved with all modules selected, it is possible to restore only a subset of configuration information. Select what you wish to restore by ticking or clearing the appropriate checkboxes.

Unless you are recovering from, say, a corrupted device, you should leave the “Restore type” set to “User files restore”.

Click the “Restore configuration” button to load the configuration values from the saved data into the CMG-EAM's files. Depending on the significance of the changes between the saved configuration and the previous, active configuration, you may need to stop and restart a number of services (see “Services” in section 13.2.4 on page 181) or reboot the unit completely (see section 13.2.3 on page 181) before all your changes will come into effect.

If you have a reasonable working knowledge of the service configuration files used internally by the CMG-EAM, you may find the

dry run facility useful. Clicking the “Dry run restoration” button produces a list of files that would be over-written - but without actually making any changes. This is also a useful tool for exploring the effects of different configuration classes.

## 4 Firmware Upgrades

Platinum firmware is regularly updated to provide extra features, improve performance and, occasionally, to correct errors. The upgrade process is fast, simple and can be carried out remotely using either the web or command-line interface.

**Note:** This procedure does not upgrade the firmware of connected or embedded digitisers, which should be upgraded using the `data-terminal` command as documented in section 13.2.2.2 on page 177.

The upgrade process makes use of the rsync protocol which uses an elegant and efficient algorithm to, effectively, transfer only the differences between revisions; even within individual files. This significantly reduces the time required, compared to traditional upgrade methods.

### 4.1 Determining the current firmware level

From the web interface, select “Version and serial numbers” from the “Summary” section of the left-hand-pane menu.

Home → Summary → [Versions](#)

### Main menu

eam2243

**Summary**

- [System status](#)
- [Version and serial numbers](#)

**Control**

- [Digital I/O](#)
- [Reboot](#)
- [Services](#)

**Tools**

- [CD1.1 log analyser](#)
- [Environment logs](#)
- [Firmware](#)
- [GCF audit log viewer](#)
- [GDI channels](#)
- [display](#)
- [Passwords](#)
- [Removable disk](#)

**Configuration**

- [All options](#)
- [Hostname](#)
- [Sys/Port](#)

### EAM Version information

Software repository label: platinum-stable  
Software build number: 3012

### Hardware versions

EAM serial: 2243  
EAM version: D  
CPU module serial: 00:01:c0:05:43:cb  
CPU module version: CM-X270L-D64-F4-C312-N512-E-R-TE  
CPLD version:

### Manufacturing log

Factory\_conf 2009-11-19 10:52

### CPU module manufacturing log

Manufacturing log  
15-Feb-2009  
L 64 4 312 0 512 0 1 - 1 0 0 0 1.5 0 0  
ETH MAC: 00:01:c0:05:43:cb  
NAND flash cylinder count: 0  
CPLD rev. 1.3

Home Help Expert Submit



The same information can be obtained at the command line by using `gconfig` and selecting “Version and serial number information”. If you just want quick access to the software build number, this is contained in the file `/etc/build.version`, which can be read with the command:

```
eam2243 ~ # cat /etc/build.version
# Overall build version
BUILD_LABEL="platinum-stable"
BUILD_VERSION="3012"
eam2243 ~ #
```

The version, in this case, can be seen to be 3012.

## 4.2 Upgrade Methods

---

In order to be upgraded, the unit needs access to the latest version of the firmware. If an internet connection is available, Gralp Systems Ltd's software repository can be used. This is described in section 4.2.1.

If a number of units share a common network but that network is not connected to the internet, you can make you own copy of the software repository on a PC or laptop, which can be connected the network either permanently or temporarily, and use that as the upgrade source. This is described in section 4.2.2.

If one or more units to be upgraded but internet access is not available, the new firmware can be copied to a USB storage device, such as a memory stick, and the upgrade performed from that. This is described in section 4.2.3.

### 4.2.1 Upgrading via the internet

---

In order to upgrade over the internet from Gralp Systems Ltd's software repository, the unit must have its networking properly configured. In particular, a DNS (Domain Name Service) server and a default gateway (or defined route) must both be configured. It is advisable to check these before proceeding.

To check for correct configuration of both of these items, issue the command:

```
ping -c3 rsync.guralp.com
```

This will send three “echo request” packets to the GSL upgrade server and listen for responses. If both the DNS server and the correct gateway (router) are configured, the output will look like this:

```
eam2010 ~ # ping -c3 rsync.guralp.com
PING rsync.guralp.com (80.68.92.160): 56 data bytes
64 bytes from 80.68.92.160: seq=0 ttl=55 time=58.280 ms
64 bytes from 80.68.92.160: seq=1 ttl=55 time=66.845 ms
64 bytes from 80.68.92.160: seq=2 ttl=55 time=56.413 ms

--- rsync.guralp.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 56.413/60.512/66.845 ms
eam2010 ~ #
```

If the DNS server is correctly configured but the gateway is not correctly configured, the output will look like this:

```
eam2010 ~ # ping -c3 rsync.guralp.com
PING rsync.guralp.com (80.68.92.160): 56 data bytes
ping: sendto: Network is unreachable
eam2010 ~ #
```

If you are using DHCP, it is advisable to correct this problem by reconfiguring the DHCP server to supply the correct route. If you are using static addressing, enter the address of the internet gateway router in the “Default route (gateway)” field of the network interface configuration form. See section 6.1.2 on page 58 for more details.

If the DNS server is not configured correctly (or at all), the output will look like this:

```
eam2010 ~ # ping -c3 rsync.guralp.com
ping: bad address 'rsync.guralp.com'
eam2010 ~ #
```

If you are using DHCP, it is advisable to correct this problem by reconfiguring the DHCP server to supply the correct name-server details. If you are using static addressing, enter the address of a suitable DNS server in the “Nameserver” field of the network interface configuration form (only available in expert mode). See section 6.1.2 on page 58 for more details.

Once the network has been checked, you can proceed to upgrade the unit by following the instructions in section 4.3 on page 49.

### 4.2.2 Upgrading from a local mirror

---

Setting up a mirror involves three steps:

Downloading the mirror content;

- Setting up a local rsync server; and
- Configuring the client EAMs to use the new server.

The procedure differs depending on the operating system of the local mirror server.

#### 4.2.2.1 Instructions for Linux/Unix computers

##### Downloading the mirror content

---

The mirror can occupy a significant amount of disk space, depending on the which architectures you need to support. See the sections for each architecture (below) for the current space requirements. You should pick a disk partition with ample space in which to store your own copy. In order to simplify the download, we recommend that you start with an empty directory each time. If you wish to make a fresh copy after a new firmware release, it is much easier to create this in an empty directory than to "update" an existing mirror. You can keep multiple, simultaneous versions of the firmware if you wish and tell each EAM which version to use when upgrading.

The server on which you create the mirror should have access to the internet during the download step but does not need internet access while it is acting as an upgrade server. It does, of course, need to be accessible by your networked EAMs. It is possible to create the mirror content on a removable disk attached to an internet-connected computer and then move the disk to a different computer when it is to be served.

Create the mirror directory and use the `cd` command to make it your current directory. As root, enter one or more of the following command sequences to download the mirror content. Each sequence downloads the files for a particular architecture. If you know, for example, that you will never want to upgrade a CMG-NAM64, you can omit the commands for this architecture.

**Note:** Be careful not to omit the final `'.'` or the space before it in the `rsync` commands below.

##### CMG-DCMs

---

This architecture currently requires around 50MB of disk space for the mirror.

```
GSLSRC=rsync.guralp.com/platinum-stable/CMG-DCM-mk2x  
rsync -EgHloprt看 --exclude resolv.conf rsync://$GSLSRC .
```

### CMG-EAMs

---

This architecture currently requires around 54MB of disk space for the mirror.

```
GSLSRC=rsync.guralp.com/platinum-stable/CMG-DCM-mk4  
rsync -EgHloptv --exclude resolv.conf rsync://$GSLSRC .
```

### CMG-NAMs

---

This architecture currently requires around 94MB of disk space for the mirror.

```
GSLSRC=rsync.guralp.com/platinum-stable/CMG-NAM  
rsync -EgHloptv --exclude resolv.conf rsync://$GSLSRC .
```

### CMG-NAM64s

---

This architecture currently requires around 125MB of disk space for the mirror.

```
GSLSRC=rsync.guralp.com/platinum-stable/CMG-NAM64  
rsync -EgHloptv --exclude resolv.conf rsync://$GSLSRC .
```

### Setting up a local rsync server

---

Your local rsync server is configured by creating the file `/etc/rsyncd.conf`. If the serving host already runs an rsync server, you should modify this file (basically, add an extra module) in order to allow access from the EAMs to the mirror directory: we assume that you have the knowledge to do this without further assistance. This section covers setting up a new, dedicated rsync server.

You will need to choose a TCP port number which will not conflict with another service on your network. The port number should be greater than 1024 in order to avoid additional complexity. Consult your network administrator for an available port or simply try 61616 and, if you get an error saying that the port is in use when you attempt to start the server, choose a different random number in the range 49152 - 65535. 61616 will be used in the following example and should be replaced with the port number you have chosen or been allocated. If there are firewalls between your server and the EAMs, you will need to open channels through them for this port.

You will also need to choose a module name for the server. This can be any descriptive string but, for simplicity, it is best to stick to numbers, lower-case letters and hyphens (-). The name `platinum-`

`local-mirror` has been used in the following example and should be replaced with the module name you have chosen.

Create the file `/etc/rsyncd.conf` with the following contents:

```
port = 61616
[platinum-local-mirror]
path = /path/to/your/local/mirror/directory
comment = GSL-EAM firmware
numeric ids = yes
log file = /path/to/writeable/log/file
timeout = 600
hosts allow = *
```

Consult the manual page for `rsyncd.conf(5)` for details of further options that you can use in this file, including security improvements that you may wish to put in place. This is available on-line at <http://man-wiki.net/index.php/5:rsyncd.conf>.

Once the `/etc/rsyncd.conf` file is ready, you can start the rsync server with the command

```
sudo rsync --daemon
```

If you want to run the rsync server permanently, it is possible to start it via `inetd`, `xinetd` or an `rc` script. Consult the manual page for `rsyncd.conf(5)` for further details.

### Configuring the upgrade system to use the new server

---

The standard upgrade source must be over-ridden: on each unit to be upgraded, create the file `/etc/conf.d/upgrade.local` with the following content:

```
RSYNC_HOST="address.of.my.server"
RSYNC_PORT="61616"
RSYNC_MODULE="platinum-local-mirror"
```

replacing:

- `address.of.my.server` with the DNS name or IP address of the mirror server;
- `61616` with the port number you chose earlier; and
- `platinum-local-mirror` with the module name you chose earlier;

The EAMs can now be updated from the mirror by following the instructions in section 4.3 on page 49. Note that the files `/etc/conf.d/upgrade.local` on each EAM will not be disturbed by the upgrade process and, so, only need to be created once.

### 4.2.2.2 Instructions for Windows computers

The procedure for building a mirror site on a windows computer is essentially the same as for Linux/Unix, although the rsync program (and the cygwin library needed to run it) typically need to be installed and additional steps are required to run rsync as a service (or daemon, in Linux terminology). Instructions for setting up rsync in daemon mode under Windows are available on-line from <http://www.samba.org/rsync/nt.html>.

Once rsync is running as a daemon, you can follow the Unix/Linux instructions for setting up the mirror and client EAMs. Remember to retain the lines

```
use chroot = false
strict modes = false
```

at the top of `/etc/rsyncd.conf` on the server.

If you use Windows Firewall, you may need to configure it to allow incoming access to the port number that you have chosen.

### 4.2.3 Upgrading from a USB storage device

---

For situations where it is either impossible or undesirable to upgrade over a network, G ralp Systems Ltd can supply the latest Platinum firmware on a USB memory stick, along with an appropriate adaptor cable, part number CAS-DCM-0038.

The adapter cable is required when upgrading the firmware of a CMG-DCM, a CMG-EAM and most CMG-DAS units but not when upgrading a CMG-NAM.



You will need both physical access and command-line access to the device being upgraded. Command-line access may be via ssh or a serial connection.

- If you are upgrading a CMG-DCM, CMG-DAS or CMG-EAM, connect the adapter cable to the USB socket of the unit and plug the firmware pod into the adapter cable;
- If you are upgrading a CMG-NAM, plug the firmware pod directly into a USB socket on the unit. Please note that, depending on the internal cable layout of your NAM, it may be necessary to connect the firmware pod to a USB port on the back of the device (near the network socket) rather than to one on its front panel.

The upgrade procedure consists of either three or four steps:

1. *CMG-EAM hardware only*: power up the USB ports;
2. Connect the firmware pod;
3. Mount the filesystem; then
4. Run the upgrade.

Each of these steps is now described in detail:

#### Power up the USB ports

---

This step only needs to be carried out on CMG-EAM hardware. The hardware for CMG-DCMs, CMG-NAMs and CMG-DAS units do not have control over the 5V USB supply and, on these units, power is always provided to the USB ports.

Depending on the revision of CMG-EAM firmware installed before the upgrade, there are three possible commands for powering up the USB ports.

**Note:** Using the wrong command is completely harmless and merely results in an error message, so it is easiest - and perfectly safe - to simply enter all three commands at the terminal

Ignoring any error messages, enter these commands at the terminal:

```
echo 1 > /sys/class/gpio/USBpowerB/level
ioline -L USBA_power -o 1
ioline -L USBB_power -o 1
```

### Connect the firmware pod

---

If you are upgrading a CMG-EAM, CMG-DAS or CMG-DCM, the supplied cable (CAS-DCM-0038) should be attached to the 6-pin mil-spec USB connector of the module. The firmware pod is then connected to the end of this cable.

A CMG-NAM unit has standard USB sockets and these can be used to directly connect the firmware pod. Please note that, depending on internal cable layout, it may be necessary to connect the firmware pod to a USB socket on the back of the device (near the network socket) rather than to one on its front panel.

Once connected, it will take a few seconds for the device to be scanned and registered by the operating system. You can confirm this by looking for USB mass storage registration entries in the system logfile, /var/log/messages.

### Mount the filesystem

---

Once the firmware pod is connected and registered, the filesystem should be mounted by entering the following command:

```
mount -t ext2 -o ro /dev/disk/by-label/Pt-firmware /mnt
```

### Run upgrade script

---

Once the filesystem is mounted, you can run the upgrade script. This is not the same script that is used for network upgrades but it takes the same optional arguments. These arguments are documented in section 4.3 on page 49, which should be read before proceeding.

Once you have decided which argument, if any, you wish to use, run the script with the command:

```
/mnt/upgrade optional_argument
```

**Note:** Some early Platinum releases only had ext3 filesystem support. If this is the case, the above command will result in an "Invalid argument" error message. If this occurs, simply change **ext2** in the above command to **ext3**.

Ensure there are no error messages and then reboot the device. Once the unit has rebooted, the upgrade process is then complete.



## 4.3 Upgrade Types

There are three different types of upgrade, each of which is described below. When upgrading via the web interface the desired type is selected by pressing the appropriate button. When upgrading directly from the command line or from a USB storage device, the required type is selected by the use or omission of command-line arguments.

### 4.3.1 Standard upgrade

The standard upgrade brings the firmware to the latest revision while respecting and preserving all configuration settings.

**Technical Note:** All files on the hard drive are left untouched, as are any files in the directories `/home`, `/root`, `/var` and `/usr/local`. In addition, any file with an extension of `.local` will be preserved: this is the mechanism by which most configuration settings are safeguarded.

To perform a standard upgrade using the web interface, select “Firmware” from the “Tools” menu. The following screen is displayed:

## Firmware update

### Upgrade from server

Upgrade this system's firmware over the network using the Guralp rsync server.

| Option  | Description  |
|---|--|
| <input type="button" value="Upgrade"/>          | Standard upgrade from rsync server.                      |
| <input type="button" value="Advanced options"/> | Display advanced upgrade options. Not normally required. |

*Generated at 2009-03-24T13:47:34Z by firmware.cgi 1.0.0. Portions of output copyright (c)2009, Guralp Systems Ltd..*

Press the “upgrade” button and watch the screen for any error messages.

To perform the same upgrade from the command line, simply enter the command

```
eam999 ~ # upgrade
```

with no arguments, watch the screen for any error messages and then reboot to complete the process.

### 4.3.2 Upgrade and restore defaults

---

The standard upgrade respects and preserves user configuration settings. In some circumstances it may be necessary to overwrite these settings and return all configuration settings to their factory defaults. The unit is not completely restored to factory condition: this allows for the possibility of implementing customisations and user-developed scripts which persist across upgrades.

**Technical Note:** All files on the hard drive are left untouched, as are any files in the directories `/home`, `/root`, `/var` and `/usr/local`. Files with the extension `.local` are deleted.

To restore defaults while upgrading using the web interface, select “Firmware” from the “Tools” menu as before but then press the “Advanced options” button. The following screen is displayed:

## Firmware update

---

### Upgrade from server

Upgrade this system's firmware over the network using the Guralp rsync server. You may also sync default configuration files, erasing your own settings and restoring the defaults.

| Option                           | Description   |
|----------------------------------|---|
| Upgrade                          | Standard upgrade from rsync server.   |
| Upgrade (restore defaults)       | Upgrade from rsync server and restore default settings for all programs. Erases user settings.  |
| Upgrade (force factory settings) | Upgrade from rsync server and force factory settings. Erases all changes made to files and settings. Erases data that is not on removable disk. |

*Generated at 2009-03-24T16:24:55Z by firmware.cgi 1.0.0. Portions of output copyright (c)2009, Guralp Systems Ltd..*

The first button, “Upgrade”, does exactly the same as the similar button on the previous screen. The “Upgrade (restore defaults)” button performs the action described in this section.

To perform this action from the command line, invoke the upgrade script with the argument `--restore-defaults`:

```
eam999 ~ # upgrade --restore-defaults
```

Watch the screen for any error messages and then reboot the unit to complete the process.

### 4.3.3 Upgrade and force factory defaults

---

The third upgrade option effectively wipes everything other than the hard drive while installing the new revision, leaving the unit as it would be delivered. Avoid using this option if you have made any customisations to your unit or installed any scripts. If in doubt, please consult Gralp Systems Ltd technical support for advice before proceeding. Conversely, if you have made changes which you believe have adversely affected the unit but are having trouble undoing them, this option lets you start with a clean slate.

To invoke this option from the web interface, select “Firmware” from the “Tools” menu but then press the “Advanced options” button. From the resulting screen, press the “Upgrade (force factory settings)” button. Watch the screen for any error messages and then reboot the unit to complete the process.

To perform this action from the command line, invoke the upgrade script with the argument `--force-factory-settings`:

```
eam999 ~ # upgrade --force-factory-settings
```






Watch the screen for any error messages and then reboot the unit to complete the process.


## 4.4 Upgrade logs

---

The upgrade process stores all progress and error messages in the file `/var/log/upgrade.log`. If you suspect that there has been a problem with an upgrade or you wish to have full details of what has changed, you can inspect this file by issuing the command

```
eam999 ~ # less /var/log/upgrade.log
```

You can scroll forward through the file simply by pressing the  key. For more control, you can move forward and backwards, line by line, with the  and  keys or, page by page, with the  and  keys.

The  key should be used to return to the command line.

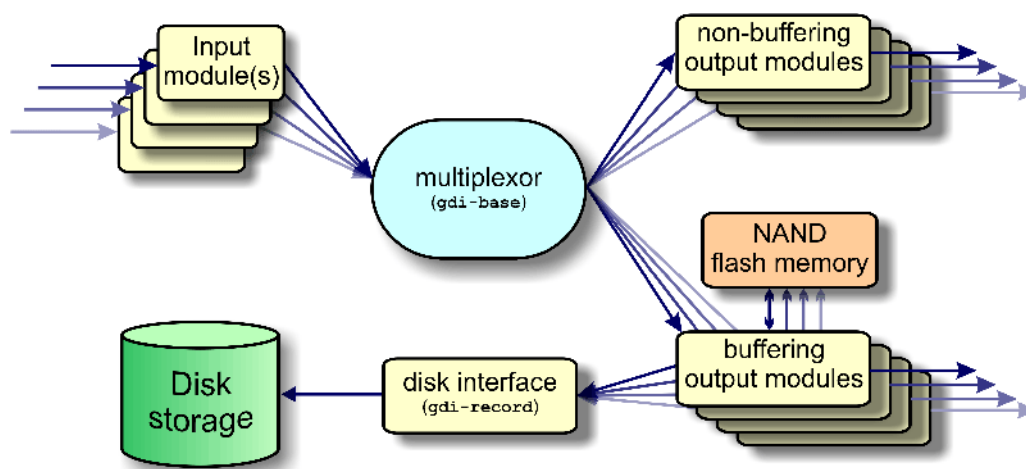
If you wish to obtain a copy of this log file, it can be copied from the system to an external computer either via the serial port (see section 10.3.1.3 on page 124) or over the network (see section 10.3.1.2 on page 120).

## 5 Data Handling Overview

The data handling system of the CMG-EAM is very flexible, due to its modular software architecture. All data flowing through the CMG-EAM is routed through a single multiplexor module called **gdi-base**. This communicates directly with all input modules, which handle the various incoming data streams, and all output modules, which convert the data into the required formats. All incoming data is stored and accessed internally in an intermediate format, regardless of the format in which it was originally received.

**Note:** The sole exception to this is incoming CD1.1 data which, for reasons related to frame signing (an authentication technology), do not pass through **gdi-base**. CD1.1 data-handling and the associated system configuration are covered in a separate manual, MAN-EAM-1100, which is available for download from [www.guralp.com](http://www.guralp.com).

The diagram below shows the basic internal organisation of the CMG-EAM, ignoring the CD1.1 subsystem.



The multiplexor makes incoming data available to the output modules. These come in two flavours: simple modules (such as those for WIN, GSMS and QSCD) simply convert the data streams and output them in the required format; other modules maintain a ring-buffer which is used to, for example, satisfy BRP back-fill requests. The ring-buffers use the NAND flash memory. These output modules also send data to **gdi-record**, which handles all hard disk writing requests, regardless of format.

The `gdi-base` and `gdi-record` programs are designed to be stateless, so that the data on the disk are always consistent. This means the system is tolerant of the power or disk being removed at any time.

Any number of input modules can be configured to acquire data in any supported format from any source, simultaneously. These modules convert their data and pass it to the multiplexor. Data can be acquired in any of the following formats, from multiple sources:

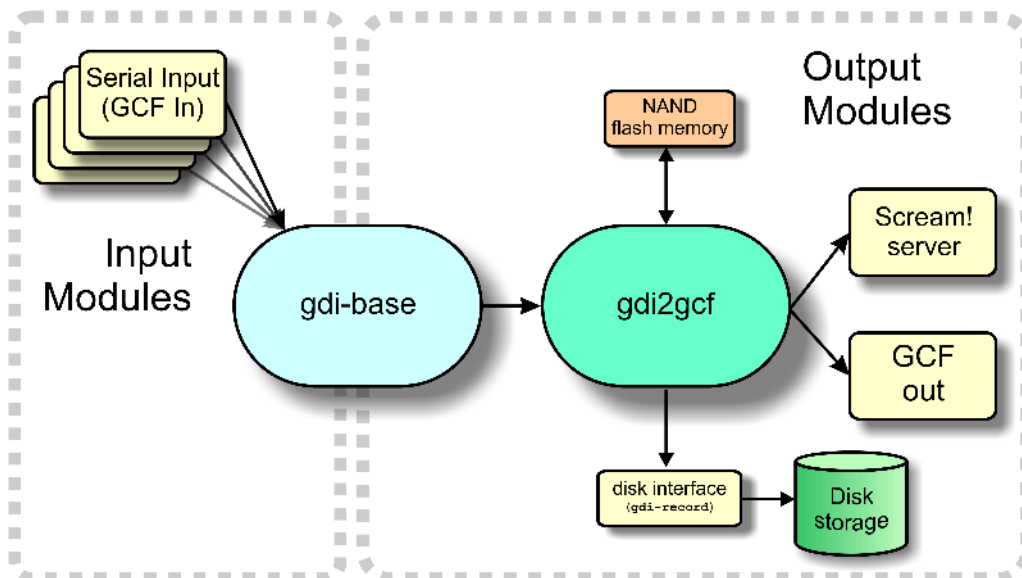
- BRP via serial lines;
- Scream via 100BaseTX Ethernet or ppp;
- GDI-link via 100BaseTX Ethernet or ppp; and
- CD1.1

The architecture has been designed to support the addition of extra formats simply by adding input modules. Please contact Güralp Systems if you have requirements which are currently unsupported.

Any number of output modules can be configured to send data in any supported format to any destination. The following data formats are supported:

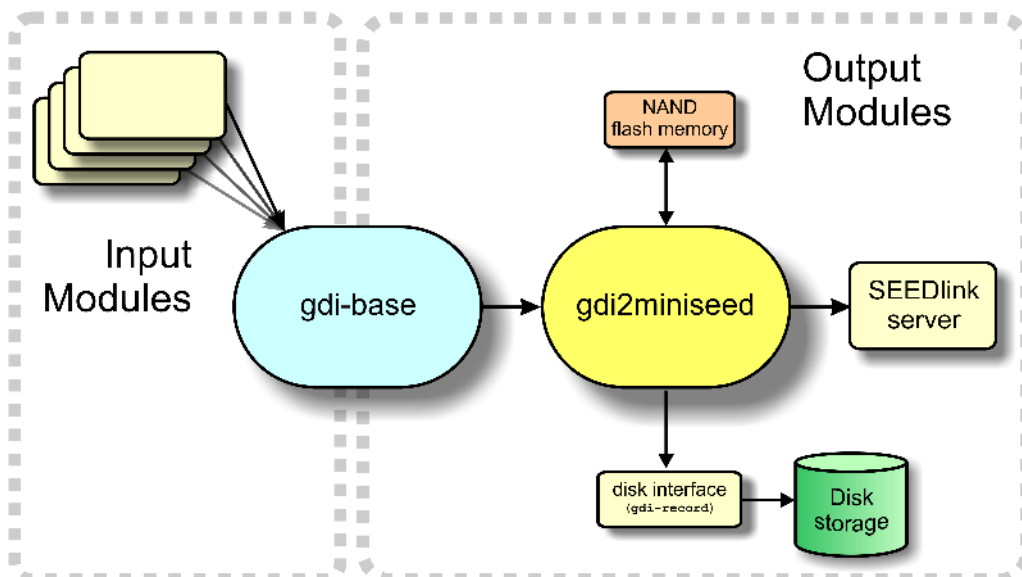
- GCF output via serial port or TCP stream;
- GCF output via Scream (TCP or UDP);
- GDI (Güralp Data Interconnect);
- GDI-link;
- CD1.1;
- WIN format output;
- QSCD - Quick Seismic Characteristic Data (designed by KIGAM) output; and
- GSMS (Güralp Seismic Monitoring System) output.

In the default, factory configuration, the CMG-EAM is configured to receive serial GCF input on all of its serial ports except Data Out. There is a single chain of data through the multiplexor to a Scream server. Data are also recorded to disk in GCF format. This is shown in the following diagram:



The `gdi2gcf` module, known as the GCF compressor, is responsible for re-blocking GDI samples into GCF blocks. It provides data to all GCF output modules as well as to the `gdi-record` module, which writes GCF files to disk. It has a number of configuration options, which are described in section 10.2 on page 109.

A similar arrangement applies to miniSEED data: the `gdi2miniseed` module provides data to the SEEDlink server and to `gdi-record`.



## 6 Configuring Networking

---

Platinum firmware includes comprehensive support for Ethernet networking. Features include VLAN (virtual network) support, an `iptables` firewall and IPV6 support

Minimal network configuration is described in section 2.2 on page 17. and those steps will allow you to communicate with your device over a network. The configuration changes made in that way will not, however, survive a reboot: to make the configuration permanent, follow the procedures in this section.

### 6.1 Configuring physical network interfaces

---

The hardware of a CMG-DCM, CMG-EAM or CMG-DAS has a single physical network interface while CMG-NAMs may be equipped with multiple physical network interfaces. Platinum firmware follows the standard Linux convention of naming the first physical network interface present on a system `eth0` and subsequent interfaces `eth1`, `eth2`, etc.

To configure a physical network interface from the web interface, select “Networking” from the “Configuration” → “All options” menu **or** select the “Interfaces” short-cut from the “Networking” menu. To configure a physical network interface from the command line, start `gconfig` and select “Networking” from the top level menu.

The following screen is displayed (only the web version is shown here: the character version is laid out and behaves identically):

[Home](#) → [Configuration](#) → [Networking](#)

---

### Networking configuration

Select a network interface to configure:

- [eth0 - Primary wired network interface](#)
- [Create a new VLAN interface](#)

or a network service:

- [Network Time Protocol \(NTP\) daemon](#)
- [Mail Transfer Agent \(e-mail service\)](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 2010-01-22T17:38:30Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

The first link on this screen takes you to the configuration page for the first physical network interface. If your hardware has multiple physical interfaces, you may need to create configurations for them using the “Create a new interface” button. Once created, they can be configured in an identical manner to `eth0`, as described below.

### 6.1.1 Configurable parameters in standard mode

---

The configuration form is large and is shown here in parts.

[Home](#) → [Configuration](#) → [Networking](#) → [eth0](#)

---

## Network Interface `eth0`

|                      |   |
|----------------------|---|
| Device               | <div>eth0</div> <div>Device name (Fixed)</div>  |
| MAC address          | <div>00:01:c0:05:43:cb</div> <div>MAC address (Fixed)</div>   |
| Description          | <div>Primary wired network interface</div> <div>User description of the interface</div>   |
| Enable interface     | <div><input checked="" type="checkbox"/></div> <div>Allow the interface to be used</div>  |
| Startup enable       | <div><input checked="" type="checkbox"/></div> <div>Start the interface at system startup</div>                                   |
| Enact on submit      | <div><input type="checkbox"/></div> <div>Check to enact changes when page is submitted. Uncheck to enact on reboot.</div>         |
| Configuration method | <div>DHCP (Dynamic Host Configuration Protocol) ▼</div> <div>Determines how the interface parameters are discovered and set</div> |

The first field, **Device**, is not editable. It displays the name of the network interface being configured.

The **MAC address** field is also not editable. It shows the *Media Access Control* address of the adapter's hardware. It is often useful to know this when configuring DHCP servers: by binding an IP address to a particular MAC address, the DHCP administrator can ensure that the device retains the same IP address across reboots.

The **Description** field allows the operator to modify the description of this interface in configuration dialogues and error messages. This is of limited value when there is only a single interface but, for example, when a CMG-NAM has multiple interfaces, it may be useful to rename them in order to reflect their logical function rather than their physical position.



The **Enable interface** check-box can be ticked in order to enable the interface or cleared in order to disable it. No other configuration settings are changed when the interface is disabled, allowing use of the interface to be suspended without deleting the configuration.

The **Startup enable** check-box controls whether the interface is enabled automatically when the unit boots.

The **Enact on submit** check-box controls whether changes made using the rest of this form take effect immediately or are only written to the configuration files. When this box is cleared, changes will only take effect the next time the unit is booted or the interface is reconfigured with this box ticked.

The **Configuration method** drop-down menu offers the following choices:

- **Static** - The interface will take its address and routing parameters from values entered by the operator.
- **DHCP (Dynamic Host Configuration Protocol)** - The interface will attempt to obtain its address and routing parameters from a DHCP server.
- **Unconfigured but powered up (possible VLAN trunk)** - The interface will not be used directly but is available for carrying virtual network (VLAN) traffic.
- **Powered off** - The interface will not be used and the interface chip is disabled, reducing the total power consumption by around 200mW.

The remainder of the screen looks like this:

## Static IP address

The following parameters are used only in a static configuration.

|   |   |
|---|---|
| IP address  | <input type="text"/><br>Address in IPv4 or IPv6 format, with CIDR format netmask (see help) |
| Default route (gateway)   | <input type="text"/><br>The IP address of the gateway router, for access to other networks  |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/> |   |

*Generated at 2010-01-21T15:19:37Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

The **IP address** field is only used if the **Configuration method** drop-down menu is set to “Static”. The address should be entered in CIDR format, where the address is followed by a slash and then the number of bits defining the netmask, e.g. **192.168.0.1/24** for IPV4 or **2001:db8::/32** for IPV6.

For more information about CIDR, please refer to [http://en.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing).

The **Default route (gateway)** field should be populated with the IP address of the default router. If more complicated routing configurations are required, these can be entered in expert mode.

### 6.1.2 Configurable parameters in expert mode

---

The following additional parameters are available when in expert mode.

**Media type/speed** - This is a drop-down menu offering the following options for controlling the communication speed and duplex mode of the network link:

- Automatically detected and set
- Restrict speed to 10Mbps. Recommended to save power
- Fixed 100baseTx, full duplex
- Fixed 100baseTx, half duplex
- Fixed 10baseTx, full duplex
- Fixed 10baseTx, half duplex

**MTU** - This text field allows the Maximum Transfer Unit to be set for the network link. This parameter controls the maximum packet size used for outgoing network packets. If any segment of a link between two systems has a restriction on packet size, larger packets flowing across the link must be fragmented - broken into smaller parts - and then re-assembled on arrival. This is inefficient and can badly affect the throughput of a link. In such situations, it makes sense to restrict the maximum packet size at the sender (to match the limitation) so that all packets can pass unimpeded.

There is no method to empirically determine the optimum MTU for a given link from the CMG-EAM itself but, if the link is to a PC (or, in the case of, say, a link between two CMG-EAMs, one end can

temporarily be replaced by a PC) the PC can be used to investigate the link properties and the correct value can be obtained.

For more information, please see <http://www.dslreports.com/faq/695>. Note that, if testing from a PC running Windows, the MTU of the Windows PC should be set to 1500 before starting the test.

The **Extra dhcpcd arguments** field can be used to change the operation of the DHCP client. Please see <http://man-wiki.net/index.php/8:dhcpcd> for information about what options can be added here.

The **Extra ip addr arguments** field can be used to tune the operation of the network interface. A non-standard broadcast address can be specified by entering `broadcast broadcast_address`. For other settings that can be used here, please see <http://linux.die.net/man/8/ip>.

The **Nameserver** field should be used to specify the IP address of the DNS server for your network. This field must be set correctly before internet firmware upgrades can be used. A secondary DNS server's address can be added in the **Backup nameserver** field.

The **Default route (gateway)** field should be populated with the IP address of the gateway router, for access to other networks or to the Internet. This field must be set correctly before internet firmware upgrades can be used.

The **ip route arguments** field can be used to modify the invocation of the `ip route add` command in order to, e.g., set the *route metric*. The options that can be set here are mostly highly technical and should rarely be required. Please see <http://linux.die.net/man/8/ip> for more information.

Two tables appear at the the bottom of the form when in expert mode: the IP aliasing table and the Extra routes table. These are shown in the screen-shot below.

The **IP aliasing** table is used to add extra addresses to this interface, a practice known as multi-homing. By default, the table displays three blank rows but, should you need more, complete the first three and submit the form: it will be redrawn with extra blank rows. The columns in the table are:

- **IP and CIDR:** The address should be entered in CIDR format, where the address is followed by a slash and then the number of bits defining the netmask, e.g. `192.168.0.1/24` for IPV4 or `2001:db8::/32` for IPV6.

- **Broadcast:** Enter the broadcast address to be associated with this address on the interface.
- **ip addr arguments:** This field can be used to tune the operation of the network interface. For settings that can be used here, please see <http://linux.die.net/man/8/ip>.
- **Delete:** For populated table rows, a check-box appears in this column. To delete the associated alias, tick the check-box and submit the form.

## IP aliasing

IP aliasing or multihoming can be configured by supplying additional IP addresses in this table.

| IP and CIDR          | Broadcast            | ip addr arguments    | Delete                   |
|----------------------|----------------------|----------------------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

## Extra routes

The following routes are added to the interface after it has come up. This is in addition to the default route added above.

| Type (see help)                          | Destination          | Gateway              | ip route args        | Delete                   |
|--|----------------------|----------------------|----------------------|--------------------------|
| unicast <input type="button" value="v"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| unicast <input type="button" value="v"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| unicast <input type="button" value="v"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

---

*Generated at 2010-01-22T11:04:45Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

The second table, **Extra routes**, is used to add extra network and host routes to allow access to networks other than those connected via the default router specified earlier, or to force packets to traverse a particular route despite the default router setting. By default, the table displays three blank rows but, should you need more, complete the first three and submit the form: it will be redrawn with extra blank rows. The columns in the table are:

- **Type:** This drop-down menu offers the following choices:
  - **unicast** - This is the normal setting for a host or network route. The route entry describes real paths to the destinations specified in the **Destination** column.

- **unreachable** - these destinations are unreachable. Packets are discarded and the ICMP message *host unreachable* is generated. An *EHOSTUNREACH* error may appear in `/var/log/messages`.
  - **blackhole** - these destinations are unreachable. Packets are discarded silently. An *EINVAL* error may appear in `/var/log/messages`.
  - **prohibit** - these destinations are unreachable. Packets are discarded and the ICMP message *communication administratively prohibited* is generated. An *EACCES* error may appear in `/var/log/messages`.
  - **local** - the destinations are assigned to this host. The packets are looped back and delivered locally.
  - **broadcast** - the destinations are broadcast addresses. The packets are sent as link broadcasts.
- **Destination:** The host or network to which this route offers access should be entered here in CIDR format, where the address is followed by a slash and then the number of bits defining the netmask, e.g. `192.168.0.1/24` for IPV4 or `2001:db8::/32` for IPV6.
  - **Gateway:** Enter the IP address of the host which serves as the gateway to the specified destination.
  - **ip route args:** This field can be used to modify the invocation of the associated `ip route add` command in order to, e.g., set the *route metric*. The options that can be set here are mostly highly technical and should rarely be required. Please see <http://linux.die.net/man/8/ip> for more information.
  - **Delete:** For populated table rows, a check-box appears in this column. To delete the associated alias, tick the check-box and submit the form.

## 6.2 Virtual network (VLAN) interfaces

---

Platinum firmware supports the use of Virtual Local Area Networks (VLANs) to partition network traffic on the same physical subnet. Virtual interfaces can be created and assigned to a particular VLAN tag

(ID) and a particular physical interface. A full discussion of VLANs is beyond the scope of this document.

To configure a virtual network interface from the web interface, select “Networking” from the “Configuration” → “All options” menu *or* select the “Interfaces” short-cut from the “Networking” menu. To configure a physical virtual interface from the command line, start `gconfig` and select “Networking” from the top level menu.

The following screen is displayed (only the web version is shown here: the character version is laid out and behaves identically):

[Home](#) → [Configuration](#) → [Networking](#)

---

## Networking configuration

Select a network interface to configure:

- [eth0 - Primary wired network interface](#)
- [Create a new VLAN interface](#)

or a network service:

- [Network Time Protocol \(NTP\) daemon](#)
- [Mail Transfer Agent \(e-mail service\)](#)

[Home](#)

[Help](#)

[Expert](#)

[Submit](#)

---

*Generated at 2010-01-22T17:38:30Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

The second option, “Create a new VLAN interface” takes you to the following screen (shown here in parts):

[Home](#) → [Configuration](#) → [Networking](#) → [New VLAN](#)

---

## VLAN Interface Creation

|                      |   |
|----------------------|---|
| Hosting Interface    | <div>eth0 - Primary wired network interface ▾</div> <div>The interface that will be used for the VLAN</div>                       |
| VLAN tag             | <div><input type="text"/></div> <div>The tag to use for the VLAN (four digit decimal number)</div>                                |
| Description          | <div><input type="text" value="Newly created VLAN interface"/></div> <div>User description of the interface</div>                 |
| Enable interface     | <div><input checked="" type="checkbox"/></div> <div>Allow the interface to be used</div>  |
| Startup enable       | <div><input checked="" type="checkbox"/></div> <div>Start the interface at system startup</div>                                   |
| Configuration method | <div>DHCP (Dynamic Host Configuration Protocol) ▾</div> <div>Determines how the interface parameters are discovered and set</div> |

### 6.2.1 Configurable parameters in standard mode

---

The **Hosting Interface** drop-down menu is populated with a list of the physical interfaces present on the system. Select the physical interface over which you wish this virtual interface's traffic to flow.

The **VLAN tag** text field should be populated with the required VLAN tag. This identifies packets sent over this interface as belonging to the specified VLAN.

The **Description** text field can be edited to provide a more useful name for the interface.

The **Enable interface** check-box can be ticked in order to enable the interface or cleared in order to disable it. No other configuration settings are changed when the interface is disabled, allowing use of the interface to be suspended without deleting the configuration.

The **Startup enable** check-box controls whether the interface is enabled automatically when the unit boots.

The **Configuration method** drop-down menu offers the following choices:

- **Static** - The interface will take its address and routing parameters from values entered by the operator.
- **DHCP (Dynamic Host Configuration Protocol)** - The interface will attempt to obtain its address and routing parameters from a DHCP server with a matching VLAN tag.
- **Powered off** - The interface will not be used and the interface chip is disabled, reducing the total power consumption by around 200mW.

The remainder of the screen looks like this:

### Static IP address

The following parameters are used only in a static configuration.

|   |   |
|---|---|
| IP address  | <input type="text"/><br>Address in IPv4 or IPv6 format, with CIDR format netmask (see help) |
| Default route (gateway)   | <input type="text"/><br>The IP address of the gateway router, for access to other networks  |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/> |   |

---

If DHCP is not being used, the **IP address** text field should be populated with the required address in CIDR format, where the address is followed by a slash and then the number of bits defining the netmask, e.g. `192.168.0.1/24` for IPV4 or `2001:db8::/32` for IPV6.

For more information about CIDR, please refer to [http://en.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing).

The **Default route (gateway)** field should be populated with the IP address of the default router for this VLAN. If more complicated routing configurations are required, these can be entered in expert mode.

### 6.2.2 Configurable parameters in expert mode

---

A set of additional parameters are available when in expert mode. These are identical to the additional parameters on the physical interface configuration screen, as described in section 6.1.2 on page 58 and are not discussed further here.

## 6.3 Network Time Protocol (NTP)

---

The Network Time Protocol (NTP) is a method of synchronising the clocks of computer systems over networks, including those with variable latency, such as packet-switched networks. Platinum firmware include a fully-featured NTP implementation, which can be used to keep the system clock synchronised to external time sources, such as Internet NTP servers, connected digitisers and connected GPS receivers.

CMG-EAM hardware includes a battery-backed real-time clock (RTC) module which can retain system time with tolerable accuracy during periods of power loss. This is also true of CMG-NAMs and CMG-DAS units incorporating CMG-EAM modules but not of CMG-DCMs and earlier CMG-DAS units with internal CMG-DCM modules - their system time will revert to January the 1<sup>st</sup>, 1970 after each power-cycle.

The system clock is used to provide time-stamps for log-file messages and can also be used to generate NMEA and PPS signals, emulating a GPS receiver, in order to synchronise external equipment, such as a CMG\_DM24 digitiser module. This technique is described in section 8.5 on page 93.

The NTP subsystem displays its status in a panel of the “System status” display of the web interface. This panel includes the current system date and time, the lock status, estimated error and current clock source.



To configure NTP from the web interface, select “Networking” from the “Configuration” → “All options” menu and then click on the link for “Network Time Protocol (NTP) daemon” **or** select the “NTP” short-cut from the “Networking” menu. To configure NTP from the command line, start `gconfig`, select “Networking” from the top level menu and then select “ Network Time Protocol (NTP) daemon”.

The following screen is displayed:

[Home](#) → [Configuration](#) → [Networking](#) → [NTP](#)

## Network Time Protocol

| Acquire time from connected GPS   | <input type="checkbox"/>            | Allows NTP to acquire the time from connected GPS receivers. |
|---|-------------------------------------|--|
| Acquire time from connected digitisers  | <input checked="" type="checkbox"/> | Allows NTP to acquire the time from suitable digitisers.     |
| The following servers will be queried for the time. You can specify a server by hostname or by IP address.  |                                     |  |
| Server address  | Delete                              |  |
| <input type="text"/>  | <input type="checkbox"/>            |  |
| <input type="text"/>  | <input type="checkbox"/>            |  |
| <input type="text"/>  | <input type="checkbox"/>            |  |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/> |                                     |  |

Generated at 2010-01-25T11:44:16Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

### 6.3.1 Configurable parameters in standard mode

The **Acquire time from connected GPS** check-box tells the system that a GPS receiver has been attached to one of the serial ports and is to be used as a clock source. The serial port used must be configured with a “Port function” of “NMEA in. Receive GPS data for NTP” and, when used with Guralp supplied GPS receivers, must be set to 4,800 baud operation, as described in 8.5 on page 93. No further configuration is required.

The **Acquire time from connected digitisers** check-box tells the system that one or more attached digitisers are to be considered as accurate clock sources. For this to work, the digitiser must produce “RTSTATUS” packets. CMG-CD24 digitisers and digital sensors incorporating them, such as the CMG-6TD, will do this unconditionally when running firmware version 279 or later. CMG\_DM24 digitisers can have these packets enabled or disabled via

software. They are automatically enabled if the digitiser is ever configured via the interface in Platinum.

The **Server address** table allows a number of Internet or network-accessible NTP servers to be listed for use as clock sources. You can specify these servers by either IP address or hostname. If names are used, they must either be listed in the local hosts file (/etc/hosts) or resolvable via the Domain Name Service (DNS). Entries in this table can be deleted by ticking the associated check-box and submitting the form.

### 6.3.2 Configurable parameters in expert mode

---

The only difference between standard and expert mode on this screen is the addition of a **Server options** column to the NTP servers table.

| Server address       | Server options       | Delete                   |
|----------------------|----------------------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

This text field can be used to provide additional control over how the NTP daemon uses the server. The options are described in the standard `ntp.conf` manual page, available on-line at <http://linux.die.net/man/5/ntp.conf>.

## 6.4 Email configuration

---

Platinum firmware is capable of sending system alerts via email over the Internet or over a local area network.

This feature is currently unused but is provided for future expansion.

To configure email from the web interface, select “Networking” from the “Configuration” → “All options” menu and then click on the link for “Mail Transfer Agent (e-mail service)” **or** select the “Mail” short-cut from the “Networking” menu. To configure NTP from the command line, start `gconfig`, select “Networking” from the top level menu and then select “Mail Transfer Agent (e-mail service)”.

The following screen is displayed:

[Home](#) → [Configuration](#) → [Networking](#) → [Mail](#)

## Mail Transfer Agent

These parameters control the Mail Transfer Agent (MTA) used to relay e-mail between machines.

|                    |   |
|--------------------|---|
| Enable MTA         | <input checked="" type="checkbox"/><br>Start the MTA at system startup                |
| Smart host         | <input type="text"/><br>Smart delivery host (leave blank to attempt direct delivery)  |
| Mail host identity | <input type="text"/><br>Our identifying name (leave blank to use the global hostname) |
| Postmaster alias   | <input type="text"/><br>The mail address all "system" mail should be directed to      |

[Home](#)
[Help](#)
[Expert](#)
[Submit](#)

Generated at 2010-01-25T14:45:17Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

### 6.4.1 Configurable parameters

The **Enable MTA** check-box is used to control whether the mail transfer agent is started automatically at boot time. If this check-box is left clear, the MTA can still be started manually from the services menu (see section 13.2.4 on page 181).

Most email configurations use a “smart host” to route mail. This can greatly simplify the administration: only one node on a network, the smart host, needs to be configured to know about any intricacies of the system and all other machines need only know the location of the smart host. If the **Smart host** text field is populated with the name or address of such a host, all mail is sent directly to that host for further routing. If this field is left blank, the MTA will attempt to use DNS to discover the mail host(s) for any given address and then deliver mail directly.

The optional **Mail host identity** text field specifies the hostname from which outgoing emails should appear to originate. If this field is left blank, the real hostname is used.

The **Postmaster alias** text field allows you to specify the address to which all internally generated mail should be sent: This should be set to the email address of the CMG-EAM's administrator.

## 6.5 Configuring the SSH Server

The CMG-EAM has an ssh server running on its Ethernet port which allows remote terminal access.

The ssh server, `sshd`, can not currently be configured using `gconfig` although it can be configured via the web interface. If web access is unavailable, it is possible to configure `sshd` from the command line by directly editing the configuration files.

### 6.5.1 Configuring `sshd` via the web interface

---

From the main screen of the web interface, under Configuration, Networking, select “SSH server”. The screen is not reproduced in this document as it is particularly large, due to the amount of explanatory text. Each option is, however, discussed below.

The version of `sshd` installed (openSSH) supports both version 1 and version 2 of the ssh protocol. Version 1 has some well-known weaknesses and should be avoided if at all possible, but some commercially available systems still do not support v2, so v1 is supported here for compatibility. The **Enable SSH Protocol v1** check-box should be cleared unless your ssh client cannot support v2 or cannot be upgraded to support it. Click the **Change server options** button to commit this change.

If you want to download the ssh server's public key to allow the connecting host to check and verify the CMG-EAM's identity, use the relevant **Download server public key** button – there is one each for protocol versions 1 and 2. There is also the capability to command the CMG-EAM to create a new private/public key pair from this screen.

To configure password-less login to the CMG-EAM, you can upload the public key of the connecting machine to the CMG-EAM using the **New client key** section. Browse the connecting host's file system for the key file (usually named `id_dsa.pub`) and upload it here. This will allow password-less root access to the system from that machine.

Client keys which have been uploaded are displayed in the **Authorised client keys** section. Any existing authorised keys can be removed: Select the check-box next to the key you wish to remove and click **Remove selected keys**.

**Note:** password-less login via ssh v2 is, perhaps counter-intuitively, the most secure way to access your CMG-EAM. There is a useful discussion of the ssh protocol and full details of its usage at the site <http://tinyurl.com/whyssh>

**Note:** Systems are shipped with a pre-authorised client key to which Gralp Systems' support staff have the matching key. This allows us to access you unit and reset the root password should you forget it. You are free to delete this key if you wish.

There is a second (and significantly more complicated) way of resetting the root password if you have physical access to the system. Please contact support if you find yourself in this situation.

---

### 6.5.2 Configuring sshd from the command line

This is a complex issue and use of the web interface is strongly encouraged unless you are familiar with Linux text editors, configuration files and sshd itself. The configuration file is located at `/etc/ssh/sshd_config` and its syntax and semantics are described at [http://man-wiki.net/index.php/5:sshd\\_config](http://man-wiki.net/index.php/5:sshd_config). More detailed discussion is beyond the scope of this document.

---

## 6.6 Working with PPP

PPP, or Point-to-Point Protocol, is a data link protocol that can carry IP packets over a serial link between two networking nodes. It can provide connection authentication, transmission encryption privacy, and compression. Platinum firmware includes an implementation of PPP which can be used to provide network links between sites or to connect to an Internet Service Provider (ISP). A number of “chat scripts” are provided, allowing connection negotiation and establishment over PSTN, GPRS and satellite modems.

---

### 6.6.1 Setting up a PPP Connection

To configure a PPP connection, you will need a user ID and authentication code (the PAP secret) as required by the remote server. In addition, a dial up (chat) script specific to the service you are using must be created. If one does not already exist for your service, please contact Gralp support.

To set up this connection, connect to the CMG-EAM configuration system via either the web interface or by using gconfig from the command line interface. From the main screen select “Serial ports” and select the port to which the modem is connected. Change the function of the port to “PPP. PPP network connection”, with the correct baud rate for the modem. Click “Submit” to save these changes. Go back to the configuration of the serial port and click on “PPP network configuration”.

You will see this screen (shown in parts):

[Home](#) → [Configuration](#) → [Serial](#) → [PortA](#) → [PPP](#)

---

## Port A PPP Settings

|   |  |
|---|--|
| Connection type                                     | <div>Local serial link (active/client mode) ▼</div> <div>The connection style to use</div> |
| Number of seconds to power down modem between calls | <div>0</div>   |

### IP addresses and routing

This section can be left empty if the remote end of the link performs all the configuration. Otherwise, some or all options may be supplied. If the remote link is also the router, you should use the "Default route" option.

|                          |   |
|--------------------------|---|
| Local IP address         | <div></div> <div>Sets the local IP address. Omit if remote end assigns one</div>              |
| Remote IP address        | <div></div> <div>Sets the remote IP address. Generally omitted</div>                          |
| Local IP address (IPv6)  | <div></div> <div>Sets the local IP address. Omit if remote end assigns one</div>              |
| Remote IP address (IPv6) | <div></div> <div>Sets the remote IP address. Generally omitted</div>                          |
| Default route            | <div><input type="checkbox"/></div> <div>Causes PPP daemon to provide the default route</div> |

Choose the required **Connection type** from the following list:

- Local serial link (active/client mode)
- Local serial link (passive/server mode)
- GPRS connection via Vodafone
- GPRS connection via T-Mobile

The choices available from this menu reflect the chat scripts installed on your system. If you wish to use a satellite modem or GPRS with an ISP other than those listed, please contact Güralp Systems Ltd technical support.

In the **Number of seconds to power down modem between calls** text field, set the desired time-out for the modem, if required.

The “IP addresses and routing” section of this page handles the network configuration. In active/client mode or when connecting to an ISP, the remote PPP daemon will set these parameters, in which case this section can be left blank.

If you are using PPP between, say, two CMG-EAMs, one should be designated the client and the other the server. The “IP addresses and routing” parameters for the client should be left blank and those for the server completed as follows:

If using IPv4 networking, the **Local IP address** field should be populated with an IP address from an otherwise unused reserved class C network address range, such as 192.168.123.1 (with no CIDR postfix) and the **Remote IP address** field should be populated with an IP address from the same network, such as 192.168.123.2 - this address is provided to the client at connection initiation.

If using IPv6 networking, the **Local IP address IPv6** and **Remote IP address IPv6** fields should be used instead.

If the **Default route** check-box is ticked, the PPP daemon will modify the routing table on successful connection, setting the remote end of the PPP link as the default gateway.

The final section of this page handles PPP security:

### Authentication

If you are using authentication, you may fill out this section. Otherwise, it can be left untouched.

|                             |   |
|-----------------------------|---|
| User ID                     | <input type="text"/><br>User identity to supply if requested  |
| PAP secret                  | <input type="text"/><br>Optional secret that matches the user ID                                      |
| Require peer authentication | <input type="checkbox"/><br>Requires that the remote peer authenticate itself to the local PPP daemon |

[Home](#) [Help](#) [Expert](#) [Submit](#)

Enter the **User ID** and **PAP secret** given to you by your service provider in the appropriate fields. Click “Submit” to save the changes.

The standard Linux commands `ppp-on`, `ppp-off`, `ip`, `ping`, and `traceroute` are available from the command line for use in controlling and testing PPP connections but it is also possible to configure a “watchdog” service to monitor a PPP connection and automatically restart it should it fail. This is described in the next section.

## 6.6.2 Monitoring a PPP connection

---

PPP connections can be monitored and, should they fail for any reason, automatically restarted. To configure this facility, connect to the CMG-EAM configuration system via either the web interface or by using `gconfig` from the command line interface. From the “All options” menu, select “System services” and then, under Network Utilities, select “`pppd-watchdog -- PPP link watchdog`”.

You can create a number of watchdogs if you are running PPP on several ports. This screen allows you to select any of the existing watchdog services for re-configuration or to create a new watchdog service.

[Home](#) → [Configuration](#) → [Services](#) → [pppd-watchdog](#)

---

### PPP link watchdog instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 2010-01-26T11:06:57Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

In this instance, no services are configured, so the only option is to create a new service.

When “Create a new service instance” is selected, the following screen is displayed:



[Home](#) → [Configuration](#) → [Services](#) → [pppd-watchdog](#) → 0

## PPP daemon watchdog

|   |  |
|---|--|
| User description  | <input type="text" value="PPP link watchdog (instance 1)"/><br>User label for the service instance       |
| Enable  | <input type="checkbox"/><br>Enable the service at system startup   |
| Delete  | <input type="checkbox"/><br>Delete this service instance   |
| Daemon startup delay  | <input type="text" value="30"/> s<br>Length of time, in seconds, for the PPP daemon to start             |
| Test command  | <input type="text" value="/bin/ping -c 5 gstm.guralp.com"/><br>Command to run to test the link is active |
| Time between tests  | <input type="text" value="30"/> s<br>Length of time, in seconds, between test runs                       |
| Reboot fail count   | <input type="text" value="30"/><br>Number of failures before system is rebooted                          |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/> |  |

Generated at 2010-01-26T11:08:34Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

If you are configuring a number of watchdogs, you can use the **User description** field to give each of them memorable names.

The **Enable** check-box should normally be ticked but can be left clear if you only want to use the associated PPP connection occasionally.

An existing watchdog service can be stopped and its configuration deleted by selected the **Delete** check-box and then clicking the “Submit” button.

If the PPP connection relies on a modem link for its transport, there may be a significant delay between instructing the PPP link to start and the connection being established. So that the watchdog does not falsely detect a failed link during this period, it can be instructed to sit idle for a number of seconds before it begins to test the link. The length of the required delay should be entered into the **Daemon startup delay** field.

Once the start-up delay time has elapsed, the watchdog periodically tests the connection. To ensure that there is a valid end-to-end connection where, for example, a multi-hop link is in use, the exact method of testing is user-configurable: any valid command can be entered into the **Test command** field and its exit status is taken to represent the link status (zero for link up, non-zero for down). The most common method used is to use the `ping` command to verify ICMP connectivity to the ultimate remote host, but you are free to use

the command or script of your choice here, so long as it returns a non-zero exit status on link failure.

**Note:** When using `ping`, you should always use the `-c count` option or the command will never return.

The contents of the **Time between tests** field determines how often the configured test is applied. It can be set high to conserve bandwidth or set low to improve failure response times. It can also be used to keep a sparsely-used link alive where a “disconnect-on-inactivity” feature would otherwise interrupt it.

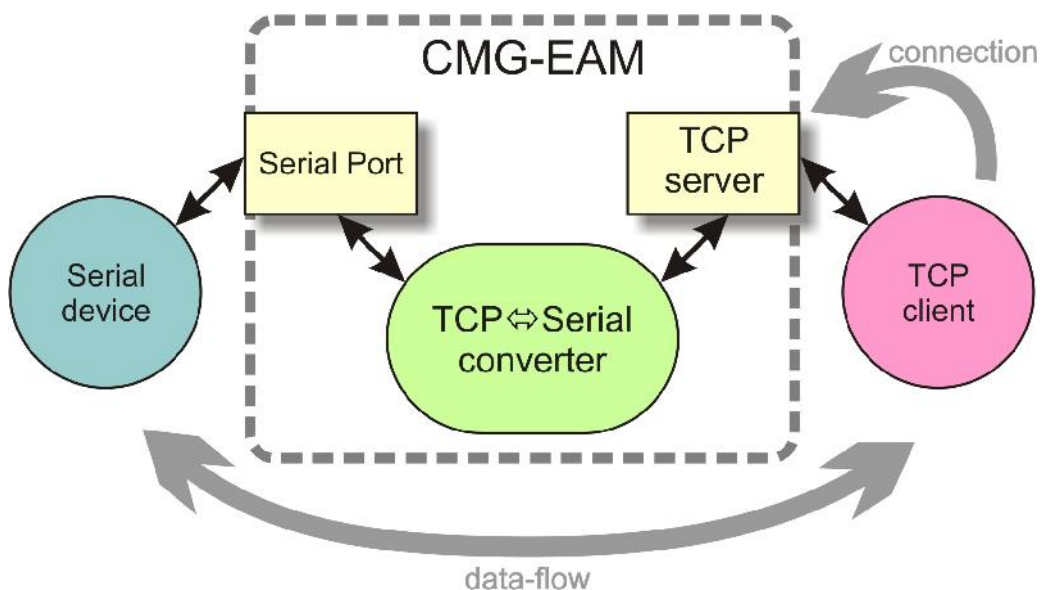
If the link test fails repeatedly, the CMG-EAM is rebooted. The number of failed tests before this happens is controlled by the “Reboot fail count” field.

The ppp watchdog service can be started, stopped and restarted using the “Services” page under the “Control” menu. See section 13.2.4 on page 181.

## 6.7 Configuring TCP to serial converters

---

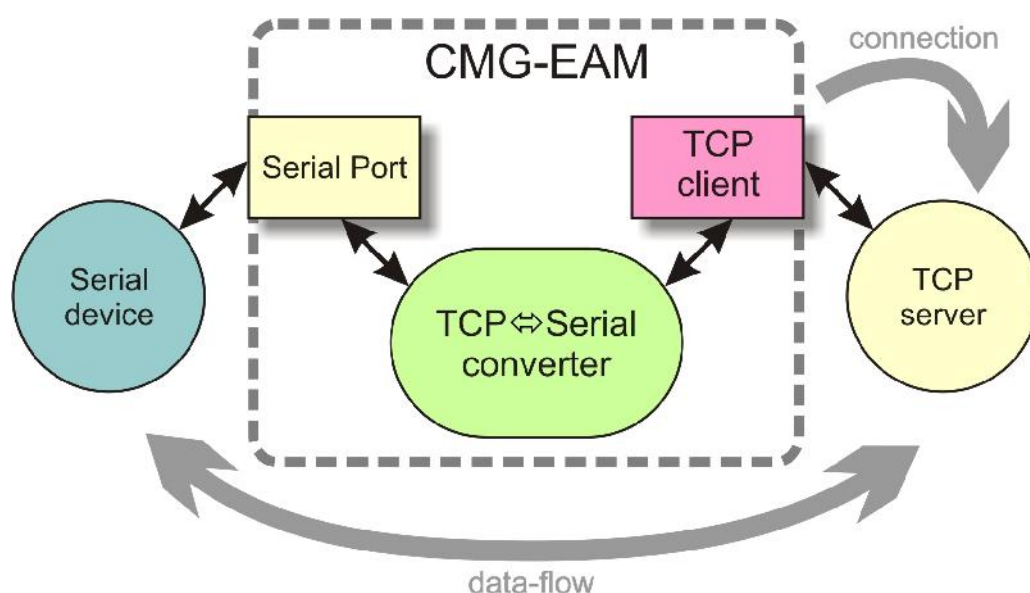
The CMG-EAM can act as a TCP to serial converter, effectively transporting data between one (or more) of its serial ports and a TCP connection. There are two different modes of operation, as detailed below. Any number of serial ports can be configured as TCP converters, as long as the TCP port numbers do not clash.



In “Simple server” mode, the CMG-EAM listens for incoming TCP connections and, should it receive one that matches its configured rules, accepts the connection and begins copying data between the serial port and the TCP connection.

The CMG-EAM can be configured to only listen on particular addresses and ports, to only accept connections from certain addresses or blocks of addresses and to reject connections from certain addresses or blocks of addresses.

In “Simple client mode”, the CMG-EAM will connect to an external TCP server on a particular address and port and then copy data bidirectionally between the serial port and the network port.



To configure the converter, select “Serial Ports” in the configuration menu, then choose the required port. Set the function to “tcp serial converter”, select the baud rate, and save the settings. You can then use the “TCP serial converter settings” button at the bottom of the page to configure the converter.

The converter's configuration page allows you to choose the mode at the top (“Operation mode”). The other options on the page are only required in certain modes; see below for which modes require which options.

### 6.7.1 Simple server mode

In Simple server mode, the converter opens the serial port and creates a TCP server socket. Whenever a client connects to the socket, the converter reads raw data from the serial port and writes it to the client, and reads raw data from the client and writes it to the serial port. The

serial port hardware control lines cannot be read or altered in this mode.

Simple server mode has two relevant options: the list of addresses to listen to, and an optional list of addresses to filter. The server can listen on multiple simultaneous local ports and addresses (although only one client can be active at a time).

The “Bind host” option is usually left blank. If specified, it is the name or IP address on which this server socket will listen. For example, if you specify “localhost” here, then this socket will only listen for incoming connections on the loopback address, and not on the external Ethernet port. Leave it blank to listen to all addresses.

The “Bind service” option must be specified. It is the TCP port number (1-65535) or service name (such as “tcpserial”) for the socket. This can be anything you choose, although we recommend that you use the names `tcpserial`, `tcpserial1`, `tcpserial2` and so on through to `tcpserial15`, which are pre-defined to correspond to port numbers 10002, 10003, through to 10017.

The mapping from port names to port numbers is configured by the conventional Linux file `/etc/services` which can be edited from the command line if required.

If desired, you can configure a list of addresses from which to accept connections. If no addresses are configured, then all incoming addresses will be accepted. Otherwise, connections will only be accepted if they match an entry in the table with its Reject box unticked. Entries are matched in order; as soon as a match is made, the connection is accepted or rejected, and no further processing is done.

The “IP addresses” fields can each specify a host name, an IP address or an IP address range (given in CIDR format). For example, to accept connections from LAN addresses, you can add the addresses:

- **10.0.0.0/8**  
(anything from 10.0.0.0 to 10.255.255.255);
- **172.16.0.0/12**  
(anything from 172.16.0.0 to 172.31.255.255);
- **192.168.0.0/16**  
(anything from 192.168.0.0 to 192.168.255.255); and

- **127.0.0.1**  
(loopback address).

### **6.7.2 Simple client mode**

---

This mode of operation is similar to simple server, except that the CMG-EAM establishes an outgoing TCP client connection rather than listening on a socket. It writes raw data from the serial port to the remote server, and writes raw data from the remote server to the serial port. It does not support the querying or setting of the serial port hardware control lines.

In this mode, only a single option needs to be provided: the contact details for the remote server (IP address and port). The format of this option is “host,service”. The host may be a hostname or an IP address. The service may be a TCP port number or a service name from `/etc/services`.

## 7 Digitiser Configuration

### 7.1 Configuring Digitisers using the web interface

---

The configuration interface can be used to configure the digitiser module in a CMG-DAS or any serially attached Güralp digitiser, such as CMG-DM24 or CMG-CD24. The internal digitiser module in a CMG-DAS is, effectively, serially connected so both internal and external digitisers are handled identically.

The “System Setup” sub-menu of the “Configuration” menu alters dynamically to reflect the system's embedded and attached devices. For every digitiser detected, an entry appears which allows you to configure the digitiser.

**Note:** To control (as opposed to configure) the digitiser and its attached instrument (sensor locking, mass centring, etc.) see section 13.2.2 on page 173.

The information shown on this screen is often retrieved from the digitiser using a sequence of background commands over a serial communications line and, so, may take a few seconds to display. A progress indicator is displayed during this process. It is possible to display this sequence of commands (together with the responses received from the digitiser) and this may be useful both for learning the command-line interface of the digitiser and for debugging any unexpected behaviour. To do this, select “Show full digitiser dialogue in future form submissions” from the miscellaneous section near the bottom of the configuration screen.

The digitiser configuration screen is large and is shown here in sections. The first section displays the digitiser's identification string and serial number and allows these to be set. It also displays the digitiser's software version:

#### C914-3K55

| Identity              |                                      |
|-----------------------|--------------------------------------|
| System identification | <input type="text" value="C914"/>    |
| Serial number         | <input type="text" value="3K55,00"/> |
| Software version      | v.103 build 70                       |

The system identification string and serial number can be changed by altering these fields and then clicking the “Submit changes” button at the bottom of the screen. If the digitiser is running in dual serial mode, both serial numbers are displayed on this screen in separate rows.

The next section configures the digitiser for its attached devices:

| Connected devices   |                     |
|---------------------|---------------------|
| Sensor type         | CMG-3T / ESPC ▾     |
| Timing source       | NMEA protocol GPS ▾ |
| GPS power cycling   | Disabled ▾          |
| Mass auto centering | At 60% excursion ▾  |

Device info blocks

Info block 1 is set.

Display device info blocks

The sensor type can be set although this has no effect on the CMG-EAM's operation and acts as a memo field.

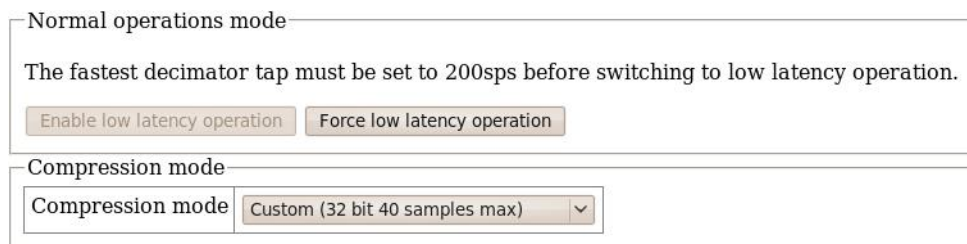
The timing source for the digitiser should be set to “NMEA protocol GPS” (which should be used for all GPS devices) or “None”, for situations where there is no timing source.

GPS units can be turned off to save power in battery-powered environments. In order to keep the internal clock synchronised, the GPS unit is regularly turned on for long enough to obtain an accurate time and then turned off. The “GPS power-cycling” drop-down allows you to select the intervals at which this happens (1, 2, 3, 4, 6, 8, 21 or 24 hours) or whether to leave the GPS constantly powered up.

“Info blocks” are areas of storage within the digitiser which can hold arbitrary data. In some applications, such as when generating strong motion packets, they should hold structured information about the attached sensors. Refer to the strong motion set-up guide for more information about this topic. If you do not need them to hold structured data, you can use them to store any information you wish, such as sensor details. There are one or two info blocks per digitiser and the display will recognise this fact. The “Display device info blocks” button shows the contents of the infoblocks and allows you to upload new data to them, should you wish.

The next section of the screen controls the latency mode and compression mode of the digitiser. Low latency mode is intended for use with strong motion calculations. The digital filtering is changed from finite impulse response (FIR) to infinite impulse response (IIR) and packets are output each second at twenty samples per second in order to achieve very near real time data.

Low latency mode cannot be selected unless certain preconditions are met: for example, the first decimator output must be set to two hundred samples per second. If all preconditions are satisfied, the **Enable low latency operation** button is enabled. As an alternative, the **Force low latency operation** button can be used to make all necessary changes before enabling low latency mode.



Normal operations mode

The fastest decimator tap must be set to 200sps before switching to low latency operation.

Enable low latency operation Force low latency operation

Compression mode

Compression mode Custom (32 bit 40 samples max) ▼

The **Compression mode** drop-down menu controls how samples are packed, affecting both data latency and line utilisation. GCF packets contain a 32-bit starting value and then a series of differences between consecutive samples. When the input signal is relatively quiet, these differences can often be expressed as 8-bit quantities. When the input signal includes large transients, the differences are transmitted as 32-bit quantities. For intermediate level signals, 16-bit values can be used. This is known as compression as it can “compress” four samples into the space otherwise occupied by a single value. The digitiser can be configured to limit the amount of compression used.

The difference values are stored in records, which are four bytes long and, so, may contain four 8-bit differences, two 16-bit differences or one 32-bit difference. A GCF packet can contain up to 250 records so the maximum number of samples in a packet is between 250 (when 32-bit differences are used) and 1000 (for eight-bit differences).

Packets must start on whole-second boundaries, so they are not always filled. In addition, it is possible to configure the digitiser to further restrict the number of records in a packet in order to decrease latency.

The drop-down menu controls both of these settings and usually offers the following choices:



- “Recommended (8-bit 20 records max)” - this setting represents the best compromise for throughput: allowing 8-bit compression potentially increases the number of samples per packet and limiting packets to twenty records guarantees reasonably low latency.
- “On (8-bit 250 records max)” - this setting optimises line utilisation, allowing maximum compression and minimising the number of packet headers transmitted.
- “Off (32-bit 20 samples max)” - this setting disables compression, forcing samples to be transmitted as 32-bit differences. Latency is reduced by limiting the number of records to twenty per packet.

If the system is connected to a digitiser that is using a different combination of compression control and sample limits, it will appear as an extra item in the drop-down menu, labelled “Custom”. For example:

- “Custom (16-bit 40 samples max)”

would appear if these settings had been manually configured from, say, the digitiser's command line.

The “Decimator outputs” section of the screen shows and controls which digitiser taps have been configured to output data, both in continuous and triggered states.

Decimator outputs

|       | Sample Rate                            |            | Output                              |                                     |                                     |                          |        |
|-------|--|------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------|
|       |  |            | Z                                   | N                                   | E                                   | X                        |        |
| Tap 0 | 500sps                                 | continuous | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Delete |
|       |  | triggered  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |        |
| Tap 1 | 250sps                                 | continuous | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Delete |
|       |  | triggered  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |        |
| Tap 3 | 25sps <input type="button" value="v"/> | continuous | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Delete |
|       |  | triggered  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> |        |

The output column is extended when using 7-channel digitisers. Extra taps can be added with the “Add new output” button. The rates available at each tap are dependant on the rate selected at the previous tap: the base sampling rate is 2000 samples per second and each tap can be configured to divide this by either 2, 4 or 5. The available rates

are shown in the table below, along with a way to configure each, although there are sometimes very many different ways to configure any given rate.

| Desired<br>output rate | Intermediate<br>steps |
|------------------------|-----------------------|
| 4                      | 400, 100, 20          |
| 5                      | 400, 100, 20          |
| 8                      | 400, 200, 40          |
| 10                     | 400, 100, 50          |
| 16                     | 400, 80               |
| 20                     | 400, 100              |
| 25                     | 400, 100              |
| 40                     | 400, 200              |
| 50                     | 400, 250              |
| 80                     | 400                   |
| 100                    | 400                   |
| 125                    | 500                   |
| 200                    | 400                   |
| 250                    | 500                   |
| 400                    | <i>tap 1</i>          |
| 500                    | <i>tap 1</i>          |
| 1000                   | <i>tap 1</i>          |

The triggering settings are normally hidden but can be revealed by clicking the “View trigger settings” button. The following extra dialogues are displayed:

Output triggering

STA/LTA trigger

Trigger input Tap 0, 500sps : 25Hz to 225Hz

| Enable channel                 | Short Term Average (secs)      | Long Term Average (secs)        | Triggering ratio               |
|--------------------------------|--------------------------------|---------------------------------|--------------------------------|
| <input type="checkbox"/> Z (0) | <input type="text" value="1"/> | <input type="text" value="10"/> | <input type="text" value="4"/> |
| <input type="checkbox"/> N (1) | <input type="text" value="1"/> | <input type="text" value="10"/> | <input type="text" value="4"/> |
| <input type="checkbox"/> E (2) | <input type="text" value="1"/> | <input type="text" value="10"/> | <input type="text" value="4"/> |
| <input type="checkbox"/> X (3) | <input type="text" value="1"/> | <input type="text" value="10"/> | <input type="text" value="4"/> |

Level trigger

Trigger input Tap 0, 500sps

STA/LTA triggers activate when the ratio of the short-term average to the long-term average (of the input signal) exceeds a configured value. The **trigger input** drop-down menu allows the selection of the input signal to be used for these calculations, along with one of three filter settings. The available filters have lower corner frequencies based on fixed fractions of the sample frequency: specifically, 5%, 15% and 25% of the sample rate. The upper corner is the Nyquist frequency (half the sample rate). For example, if a tap configured for 25 samples per second, the three filters offered will have pass-bands of 1.25Hz to 11.25Hz, 2.5Hz to 11.25Hz and 6.125Hz to 11.25Hz.

The periods over which the short term and long term averages are computed, along with the triggering ratio itself, can be altered by changing values in the table. The check-boxes next to each component are used to enable or disable the use of that component's output in the STA/LTA triggering algorithm.

Level triggering is controlled by the following dialogue:

Level trigger

Trigger input Tap 0, 500sps

Trigger highpass filter Disabled

| Enable channel                 | Triggering level                       |
|--------------------------------|--|
| <input type="checkbox"/> Z (0) | <input type="text" value="214748364"/> |
| <input type="checkbox"/> N (1) | <input type="text" value="214748364"/> |
| <input type="checkbox"/> E (2) | <input type="text" value="214748364"/> |
| <input type="checkbox"/> X (3) | <input type="text" value="214748364"/> |

External trigger

The tap to be used as input should be selected from the **Trigger input** drop-down menu. All configured taps are available, regardless of whether they have been selected for continuous output or not. An optional highpass filter can be applied to eliminate the effect of any DC offset in the sensor's output. The available corner frequencies are 100, 300 and 1000 seconds.

The check-boxes labelled with component designators are used to include or exclude the associated component from the triggering algorithm. If one is ticked, a trigger will be activated if that component's instantaneous output exceeds the value entered into the **Triggering level** field in the same row.

The final section of the triggering configuration screen concerns external triggering and pre- and post-trigger times.

☐ X (3)

External trigger

Enable external trigger input ☐

Enable external trigger output ☐

Triggered output timings

Pre-trigger time 10 seconds ▼

Post-trigger time 20 seconds ▼

Return to main settings Add new trigger tap

Help Refresh display Submit changes Submit & Reboot digitiser

*Generated at 2010-02-03T16:54:22Z by digitiser-config.cgi 0.3.0. Portions of output copyright (c)2010, Guralp Systems Limited.*

Full coverage of external triggering is beyond the scope of this manual and the interested reader is referred to the relevant digitiser manual.

The **pre-trigger time** and **post-trigger time** drop-down menus control the amount of data transmitted around each trigger period. The options offered range from 5 seconds to 4 minutes. The “0 seconds” setting disables the feature.

The “Add new trigger tap” button inserts an extra row in the decimator output table and returns the display to the main digitiser configuration settings screen.

The next section of the main display shows and controls the transmission of data from the auxiliary and state-of-health channels of the digitiser:

Multiplexor channels

| Auxiliary inputs                                   | System SOH  |
|--|---|
| <input type="checkbox"/> M0 - channel 0            | <input checked="" type="checkbox"/> M8 - Z mass postition   |
| <input type="checkbox"/> M1 - channel 1            | <input checked="" type="checkbox"/> M9 - N/S mass postition |
| <input type="checkbox"/> M2 - channel 2            | <input checked="" type="checkbox"/> MA - E/W mass postition |
| <input checked="" type="checkbox"/> M3 - channel 3 | <input type="checkbox"/> MB                                 |
| <input checked="" type="checkbox"/> M4 - channel 4 | <input type="checkbox"/> MC                                 |
| <input type="checkbox"/> M5 - channel 5            | <input type="checkbox"/> MD                                 |
| <input type="checkbox"/> M6 - channel 6            | <input checked="" type="checkbox"/> ME                      |
| <input type="checkbox"/> M7 - channel 7            | <input checked="" type="checkbox"/> MF                      |

Inputs M3 through M7 and MB through MF are typically derived by digitising (at 16-bit resolution) the analogue inputs on the “Auxiliary” connector of the digitiser although, in some configurations, they may be connected to internal sensors. M8, M9 and MA provide mass position data from the first sensor and, for seven-channel digitisers, M0, M1 and M2 perform the same function for the second instrument. Output from each displayed channel can be enabled by ticking the associated check-box or disabled by clearing it.

This is followed by the Transmission Mode selection dialogue (not reproduced here). One mode can be selected from the following list:

- Direct mode - Data are transmitted in real-time, without being copied to local storage. Only a small transmit buffer is used.
- Filing mode - Data are stored in local flash storage. A periodic status heartbeat is transmitted to inform listeners that data are available from storage.
- Adaptive mode - Data are transmitted in real-time whenever possible. Any unacknowledged transmission is stored, and retransmitted oldest first when the line is not being used for real-time traffic.
- FIFO mode - Data are stored locally and transmitted in strict FIFO order. If the link is lost for a period, real-time data will be delayed while the stored data are transmitted.
- Dual mode - Continuous data are transmitted as in "direct" mode and Triggered data is stored in flash as in "filing" mode.

- Duplicate mode - Data are transmitted as if in "direct" mode and also stored in flash as in "filing" mode although without the "heartbeat" operation.

The next section of the web page allows the selection of one of two storage modes, which affect how data are stored in the digitiser's local flash storage:

| Storage mode                     |   |
|----------------------------------|---|
| <input checked="" type="radio"/> | Enable storage re-use.<br>When local storage is full, new data arriving will over-write the oldest data in the buffer.  |
| <input type="radio"/>            | Enable write once storage.<br>When local storage is full, new data arriving will be transmitted as if in "direct" mode and will not over-write the already stored data. |
| <input type="checkbox"/>         | Reset flash buffers on next digitiser update.   |

Selecting the **Reset flash buffers on next digitiser update** check-box will cause all data in the flash storage to be erased and the read pointers to be reset. Use with caution: data will be erased.

The next section controls two settings associated with data transmission:

| Transmission parameters |   |
|-------------------------|---|
| Heartbeat interval      | <input type="text" value="9"/> seconds<br>The periodic status heartbeat is only used with "filing" and "dual" data modes. |
| Acknowledgement delay   | <input type="text" value="150"/> milliseconds<br>How long to wait before a transmission is assumed to have failed.        |

When the digitiser is in the "filing" or "dual" transmission modes, regular heart-beat messages are sent. This allows software such as Scream! to be aware of the devices even though they are not sending sampled waveform data. The frequency of these messages can be set to an integer number of seconds using the **Heartbeat interval** text field.

When the digitiser is in the "adaptive" or "FIFO" transmission modes, special action is taken if data cannot be transmitted. The **acknowledgement delay** field controls how long the digitiser waits for an acknowledgement packet before assuming that the link has failed. This should be set to an integer number of milliseconds.

The “Ports” section of the web page allows control of the baud rates of the digitiser's serial ports:

| Ports       |   |
|-------------|---|
| Serial port | Baud rate   |
| Data out    | <div>115200 ▾</div> Changing the data out rate will require the same change to be made in your communications software.   |
| GPS         | <div>38400 ▾</div> This setting is only used for non-GPS operations. If a GPS device is enabled the port will be set to the GPS rate of 4800 baud regardless of this setting. |
| Data in     | <div>38400 ▾</div>  |

For a stand-alone digitiser or digital instrument, the “GPS” and “Data in” ports are exposed on external connectors. The “Data out” port is assumed to be connected to the CMG-EAM, CMG-DCM or CMG\_NAM and the rate set here must match that set for the appropriate serial port (see section 9.1 on page 97 for details of reconfiguring serial ports).

If a stand-alone digitiser or digital instrument is fitted with a Lantronix Ethernet or WiFi option, it uses the “Data out” port settings for its internal communications with the digitiser. Changing the associated baud rate requires making a network connection to the Lantronix unit's web interface and selecting the matching baud rate from its control page.

**Note:** For CMG-DAS systems, the digitiser's “Data out” port is connected internally to the CMG\_EAM module's “Port A” and both ports must use the same Baud rate. The digitiser's “Data in” port is used to provide a console for the digitiser (without interrupting seismic data transmission) and is connected internally to the CMG\_EAM module's “Port B”. Again, both ports must use the same Baud rate. The digitiser's “GPS” port is connected to the CMG\_EAM module's “Port C”. This connection can be used in two ways: the CMG-EAM module can share with the digitiser the data from the physical GPS receiver and use it as an NTP clock source (see section 6.3 on page 64); or, alternatively, the CMG-EAM module can be synchronised to another time source (such as Internet NTP) and provide NMEA signals to the digitiser module. In either case, The digitiser module's “GPS” port and the CMG-EAM module's “Port C” must use the same Baud rate.

The final section of the digitiser control web page is entitled “Miscellaneous features”. This section displays a warning in red if a discrepancy is detected between the EAM's time and the digitiser's own clock. If the two clocks have reasonable synchronisation, this message is suppressed. A typical warning looks like this:

Digitiser clock is displaced by more than 5 minutes from the system clock.  
(Plus 7 minutes.)

This section of the page is shown here without the warning:

Miscellaneous features

☐ Transmit Unified Status Packets. (Recommended)  
☐ Set the digitiser clock from the system clock on next form submission.  
☐ Show full digitiser dialog in future form submissions.

Help

Refresh display

Submit changes

Submit & Reboot digitiser

Generated at 2010-02-04T09:20:08Z by digitiser-config.cgi 0.3.0. Portions of output copyright (c)2010, Guralp Systems Limited.

The first check-box enables the transmission of Unified Status Packets. Unified Status Packets are a machine-readable representation of the data carried in the normal, human-readable status streams and allow programs such as Scream! to access complete and consistent state-of-health information regardless of any status stream customisations.

The second check-box allows the one-time re-synchronisation of the digitiser to the EAM's system clock. The third toggles display of the underlying dialogue with the digitiser, as described at the beginning of this section.

Note that, as with all web interfaces, options selected on this screen will not take effect until the page is submitted.

Extra buttons at the bottom of this page allow the refreshing of the web page display with up-to-date information and offer the opportunity to reboot the digitiser.

**Note:** Some digitiser configuration changes require the digitiser to be rebooted before they will take effect. Please consult the digitiser manual for more information.



## 7.2 Configuring digitisers from the command line.

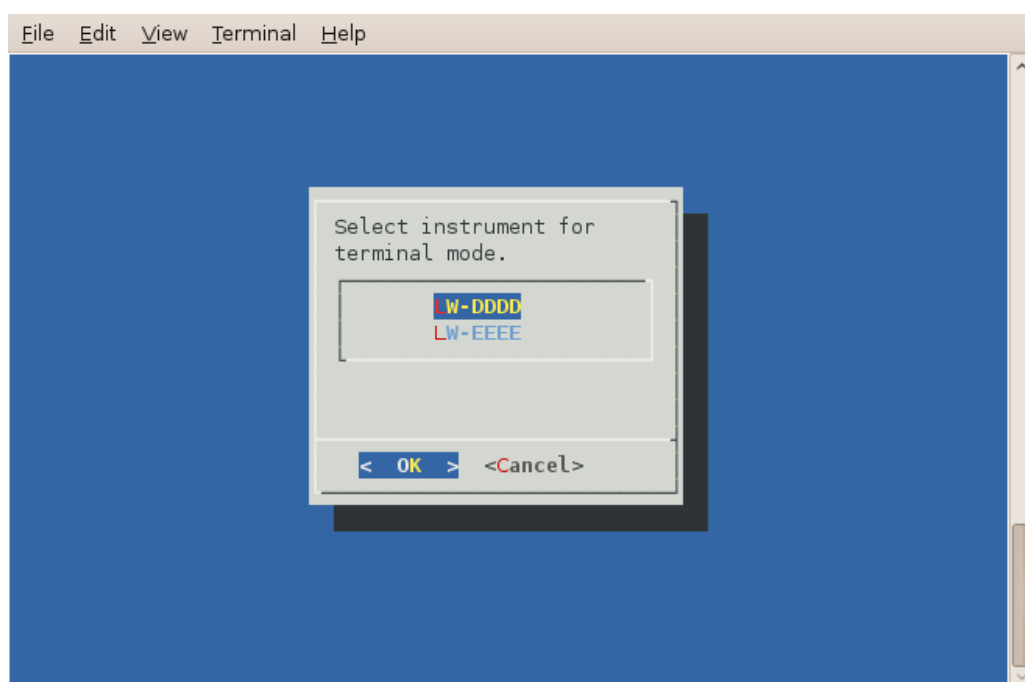
Platinum provides a tool, data-terminal, which allows direct access to the command-line of any serially attached digitiser. This gives the greatest level of control but also involves the most complexity.

Interactions with the digitiser's command-line are beyond the scope of this document: please consult the relevant digitiser manual for information on this topic. This section discusses use of the data-terminal tool only.

To invoke the tool, enter the command

```
data-terminal
```

You will be presented with a menu listing all digitisers to which a connection can be made:



Select the required digitiser from the menu. The data-terminal program will suspend any service running on the associated port and start a minicom session with the correct communications parameters already set.

The use of minicom is described in section 14.4 on page 211. When you have finished configuring the digitiser, key **Ctrl** + **A** then **Q** to exit. Any previously running service will be restarted.

## 8 Digitiser Synchronisation

---

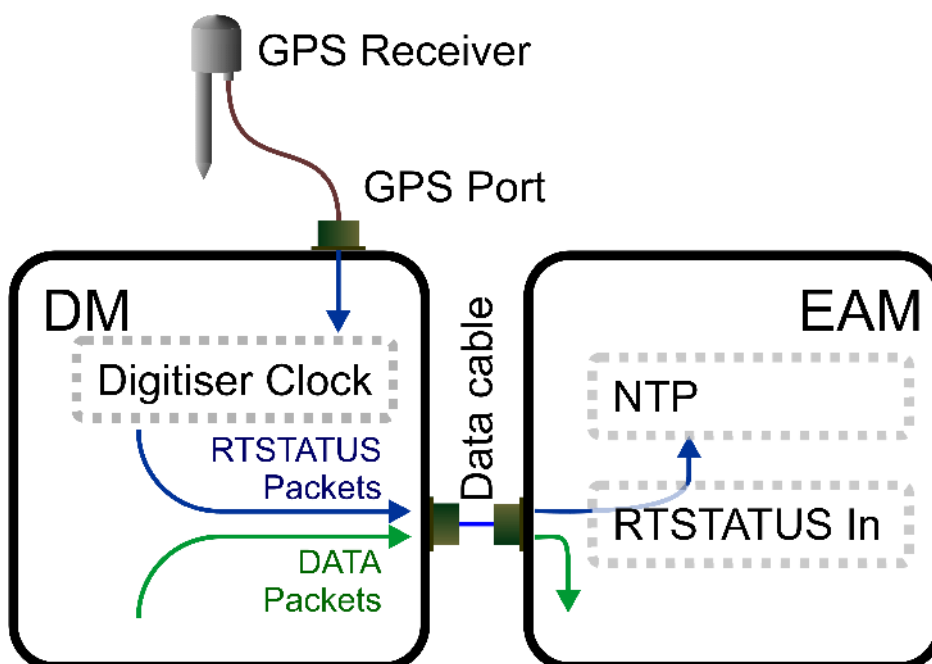
Accurate time-stamping of samples is essential to seismology. Güralp Systems Ltd recommend the use of GPS receivers for generating clock signals wherever possible: they are the most accurate time sources available for all practical purposes. Where GPS receivers cannot be used but an internet connection is available, Network Time Protocol (NTP) can produce acceptable results. Platinum firmware can produce NTP-synchronised NMEA output for use with GPS-capable devices.

CMG-EAMs, CMG-DCMs and CMG-NAMs have an internal clock which is used to time-stamp log-file entries (but not data samples). This lock is managed by the NTP subsystem. CMG-DAS units and Authenticated Digitisers have two clocks: the digitiser clock and the EAM/DCM clock: the former is used to time-stamp data samples and the latter to time-stamp log-file entries. The EAM/DCM clock is also managed by NTP. The two clocks can be synchronised in a number of ways.

### 8.1 RTSTATUS packets

---

Where a CMG-EAM or CMG-DCM is used with an external GPS-synchronised GSL digitiser, the digitiser can emit special synchronisation packets called RTSTATUS packets. These are transmitted along the same link as the data packets. Platinum units can use these as a time source for NTP: see section 6.3 on page 64 for more details.



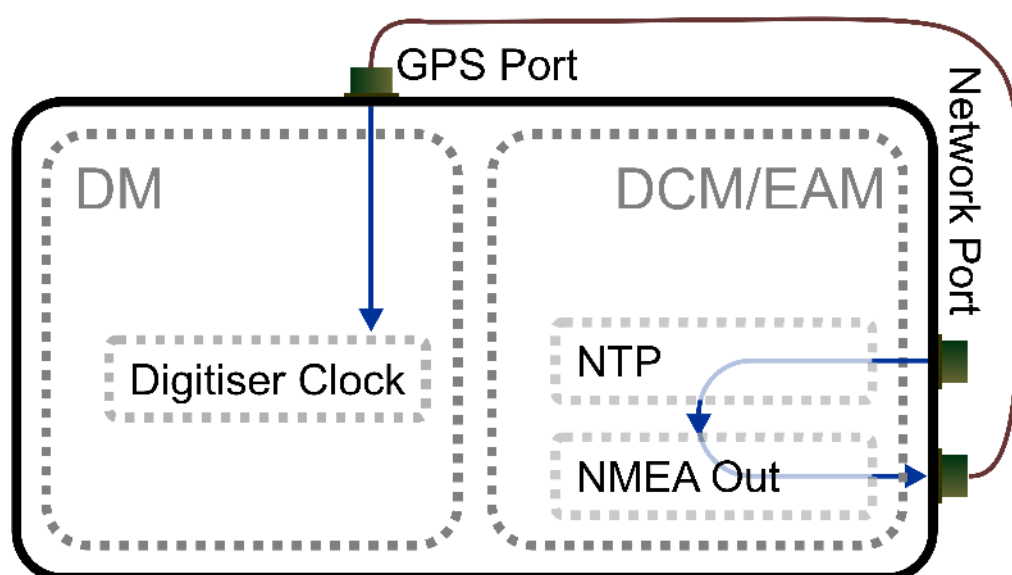
**Note:** RTSTATUS packets are available with MkIII DM24 units. Earlier units, such as MkIIs, are not capable of generating these packets.

**Note:** RTSTATUS packets are available with CD24 units running firmware revision 279 and above.

This is also the recommended configuration for CMG-DAS units, where GPS reception is available.

## 8.2 Using NTP with CMG-DAS units

Where GPS reception is not practical but an internet connection is available, NTP can be used to synchronise the Platinum clock, which can then generate NMEA output. This NMEA data-stream can be fed to the GPS input of the digitiser module using an external cable from a serial port.



To configure the NTP subsystem, see section 6.3 on page 64.

To configure NMEA output, see section 8.6 on page 94.

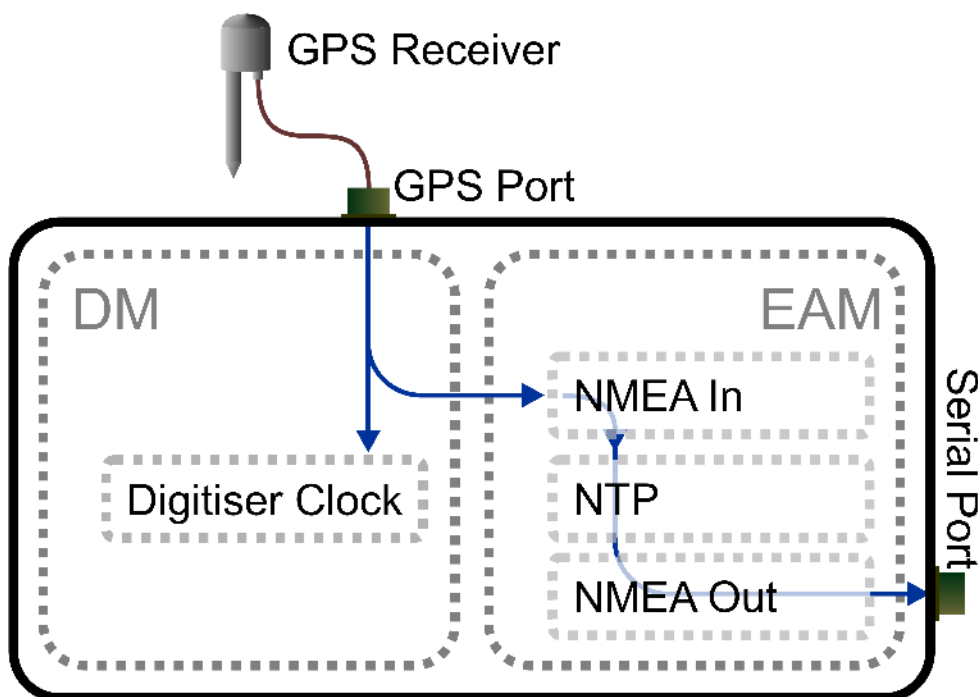
## 8.3 Using GPS with Authenticated Digitisers

Güralp Systems Ltd's authenticated digitisers provide a CMG-DM24 and a CMG-EAM in a single package. An internal, bi-directional

connection is made between Port C of the EAM and the digitiser module. This connection can operate in one of two modes:

- An external GPS receiver can provide input to both the digitiser module's clock circuitry and the EAM's NTP subsystem; or
- The EAM's NTP subsystem can provide NMEA to the digitiser module's clock circuitry. In this case, the external GPS socket is automatically disconnected.

The data flow when a GPS receiver is used is illustrated below:



If required, the NTP subsystem can provide NMEA output via a serial port which can then be used to synchronise an additional digitiser. This, however, is optional and no serial port is dedicated to this use.

To configure the NTP subsystem, see section 6.3 on page 64.

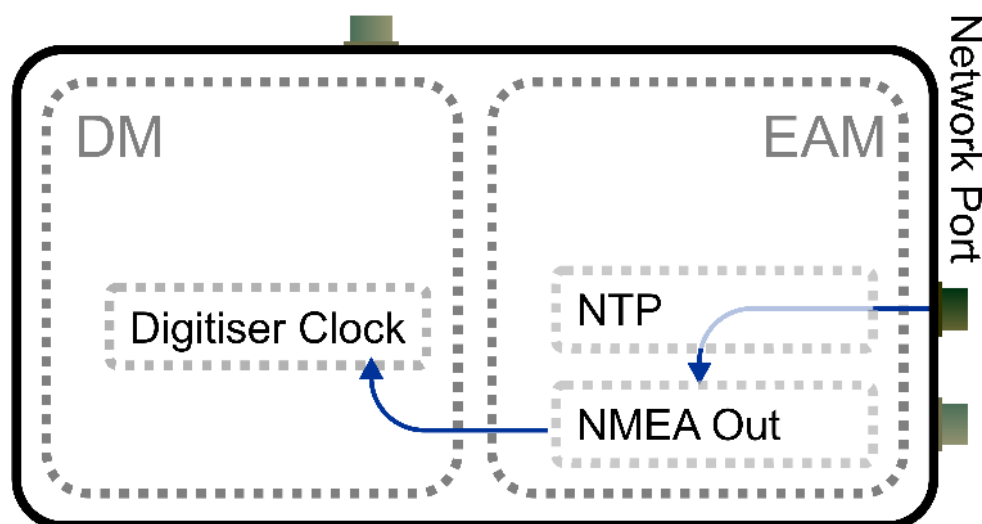
To configure NMEA as an NTP clock source, see section 8.5 on page 93.

To configure NMEA output, see section 8.6 on page 94.

## 8.4 Using NTP with Authenticated Digitisers

Please see the discussion of synchronisation options available with Authenticated Digitisers in the previous section.

The data flow when NTP is used as the primary clock source is illustrated below:



**Note:** The external GPS connector is disconnected when Port C of the EAM is set to “NMEA Out” and connected to the digitiser's GPS input in all other cases.

To configure the NTP subsystem, see section 6.3 on page 64.

To configure NMEA output, see section 8.6 on page 94.

## 8.5 Configuring NMEA as an NTP clock source

To configure NTP to use NMEA as a clock source, two steps are required. First, tick the **Acquire time from connected GPS** check-box in the NTP configuration page as described in section 6.3 on page 64.

Secondly, configure the relevant serial port as an NMEA input.

To do this, using the web interface, select “Serial ports” from the “Configuration” → “All options” menu **or** select the “Serial ports” short-cut from the “Configuration” → “Data transfer/recording options” menu. To configure an NMEA input from the command line, start `gconfig` and select “Serial ports” from the top level menu.

Next, select the serial port from which you want to input NMEA.

**Note:** For authenticated digitisers, this will be Port C. For more details of Authenticated Digitisers, please see section 14.2 on page 190.

Set the **Port function** to “NMEA out. NMEA (time + fixed position) output” and the **Port speed** to 4800. Click “Submit” to save the changes.

[Home](#) → [Configuration](#) → [Serial](#) → [PortC](#)

---

## Port C serial configuration

|               |  |
|---------------|--|
| Name          | <input type="text" value="Port C"/><br>Port name (Fixed)   |
| Port function | <input type="text" value="NMEA in. Receive GPS data for NTP"/><br>Function the port currently supports |
| Port speed    | <input type="text" value="4800"/><br>Baudrate at which the port operates                               |

- [NMEA output settings](#)
- [GCF input settings](#)
- [GCF output settings](#)

---

## 8.6 Configuring NMEA output

Platinum can generate simulated GPS data (NMEA-0183) to synchronise a connected digitiser's clock. In this case, the internal clock of the CMG-EAM is used as a reference for the digitiser. In order to provide a sufficiently accurate time-stamp, the clock must be controlled using NTP (See section 6.3 on page 64).

To configure NMEA Output using the web interface, select “Serial ports” from the “Configuration” → “All options” menu **or** select the “Serial ports” short-cut from the “Configuration” → “Data transfer/recording options” menu. To configure NMEA Output from the command line, start `gconfig`, select “Serial ports” from the top level menu.

Next, select the serial port from which you want to output NMEA. Only one port can be used for NMEA output at any time: the timing constraints are such that a single processor cannot produce the pulse-per-second (PPS) signal on two ports simultaneously with sufficient accuracy.

**Note:** For Authenticated Digitisers, Port C should be used in order to provide NMEA output to the internal digitiser module. If a GPS receiver is used, the “Data Out” Port (exposed as the DATA connector) can be used to provide timing to additional, external digitisers.

Set the **Port function** to “NMEA out. NMEA (time + fixed position) output” and the **Port speed** to 4800. Click “Submit” to save these changes.

[Home](#) → [Configuration](#) → [Serial](#) → [PortC](#)

## Port C serial configuration

|               |   |
|---------------|---|
| Name          | Port C<br>Port name (Fixed)   |
| Port function | NMEA out. NMEA (time + fixed position) output<br>Function the port currently supports |
| Port speed    | 4800<br>Baudrate at which the port operates   |

- [NMEA output settings](#)
- [GCF input settings](#)
- [GCF output settings](#)

Go back the configuration of the serial port and click on “NMEA output settings”. You will see this screen:

[Home](#) → [Configuration](#) → [Serial](#) → [PortC](#) → [NMEA output](#)

## Port C NMEA Settings

|            |  |
|------------|--|
| Latitude   | 0000.0000,N<br>Device latitude. Format 0000.0000,N                                 |
| Longitude  | 00000.0000,E<br>Device longitude. Format 00000.0000,E                              |
| Height     | 00000<br>The device height in meters, 5 digits                                     |
| Geoid      | 000<br>The difference between sea level and geoid height                           |
| Invert PPS | <input type="checkbox"/><br>Whether the pulse per second signal should be inverted |

[Home](#)
[Help](#)
[Expert](#)
[Submit](#)

Generated at 1970-01-02T01:14:00Z by gcs 2.0.2. Portions of output copyright (c)1970, Guralp Systems Limited.

Here, you can configure the NMEA sentences that will be sent to the digitiser. You can specify the location (latitude, longitude, elevation), the geoid (the offset of the location from the theoretical earth surface) and whether to invert the Pulse-Per-Second signal (if unchecked, the PPS line will be briefly asserted each second, on the second, and held to ground at other times). It is not essential that the position string sent matches the physical location of the digitiser, as only the GPS time signal is used by the digitiser. Click “Submit” to save the changes.

The following additional parameters are available in expert mode:

|  |                          |  |
|--|--------------------------|--|
| Invert PPS                               | <input type="checkbox"/> | Whether the pulse per second signal should be inverted     |
| Log file                                 | <input type="text"/>     | Path to log file. Leave blank to use syslog.               |
| Log level                                | Important notices ▼      | Minimum severity level of messages to record in log.       |
| Max NTP error                            | <input type="text"/>     | Maximum clock drift (in microseconds) to accept as locked. |
| <div>Home   Help   Simple   Submit</div> |                          |  |

---

*Generated at 1970-01-02T01:16:27Z by gcs 2.0.2. Portions of output copyright (c)1970, Guralp Systems Limited.*

It may sometimes be desirable, for debugging purposes, to separate log messages for this input from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

The **Max NTP error** text field controls the accuracy of synchronisation which must be achieved by NTP before the resulting NMEA sentences will indicate that the “GPS” is locked.



## 9 Receiving Data

---

The modular architecture of Platinum software allows seismic data to be received simultaneously from a number of sources and using a number of protocols, as discussed in section 1.3 on page 10. Extra protocols can be implemented by request: please contact Guralp Systems Ltd for more details.

At the time of writing, Platinum firmware is shipped with support for CD1.1, Guralp Compressed Format (GCF) data received over serial ports, GCF data received over a network using the Block Recovery Protocol (BRP) and GCF data forwarded from a copy of Scream!

The use of CD1.1 is covered in a separate manual, MAN-EAM-1100. The use of the other receivers is described in this section.

### 9.1 GCF from serial devices

---

Any or all of the serial ports may be configured to receive GCF data from a serially attached digitiser or digital instrument.

To configure a port for this purpose, select “Serial ports” from the “Configuration” → “All options” menu *or* select the “Serial ports” short-cut from the Configuration” → “Data transfer/recording” menu. To configure a physical network interface from the command line, start `gconfig` and select “Serial ports” from the top level menu.

The following screen appears:

[Home](#) → [Configuration](#) → [Serial](#)

---

### Serial ports configuration

Select a port to configure:

- [Data Out - GCF out \(115200 baud\)](#)
- [Port A - GCF in \(38400 baud\)](#)
- [Port B - GCF out \(38400 baud\)](#)
- [Port C - GCF in \(38400 baud\)](#)
- [Port D - GCF in \(38400 baud\)](#)
- [Port E - GCF in \(38400 baud\)](#)
- [Port F - GCF in \(38400 baud\)](#)
- [Port G - GCF in \(38400 baud\)](#)
- [Console - Terminal \(38400 baud\)](#)
- [Aux port 1 - Terminal \(38400 baud\)](#)
- [Aux port 2 - Terminal \(38400 baud\)](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 2010-01-26T13:26:56Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

Each port on the system is listed along with its function and line speed. Any port can be used for any function with the exception of the console port, which is dedicated to the terminal function, and the internal ports used for inter-module communications in CMG-DAS units.

**Note:** When configuring units without a dedicated console port, such as the CMG-DCM, take care not to “lock yourself out” of the system by, eg, configuring all serial ports for non-terminal functions before completing network access configuration.

Select the link for the serial port you wish to configure for GCF input. The following screen will appear:

[Home](#) → [Configuration](#) → [Serial](#) → [PortA](#)

---

### Port A serial configuration

|               |   |
|---------------|---|
| Name          | <div>Port A</div> <div>Port name (Fixed)</div>  |
| Port function | <div>GCF in. Inbound GCF data gathering</div> <div>Function the port currently supports</div> |
| Port speed    | <div>38400</div> <div>Baudrate at which the port operates</div>                               |

- [NMEA output settings](#)
- [GCF input settings](#)
- [GCF output settings](#)
- [PPP network configuration](#)
- [TCP serial converter settings](#)
- [Modbus device settings](#)

Home

Help

Expert

Submit

Generated at 2010-01-26T14:22:33Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

Select “GCF in. Inbound GCF data gathering” from the **Port function** drop-down menu, set the appropriate Baud rate using the **Port speed** drop-down menu and then click on the GCF input settings link.

[Home](#) → [Configuration](#) → [Serial](#) → [PortA](#) → [GCF input](#)

---

### Port A block recovery protocol settings

Disable rewind

☐

Disable BRP rewinding, for DM24s in adaptive mode etc.

Home

Help

Expert

Submit

Generated at 2010-01-26T14:27:58Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

In standard mode, the only option available is to disable BRP rewinding. In some modes, some digitisers will not allow BRP to rewind to earlier blocks. In these modes, missed packets will, instead, be sent at a later time. However, the log-file will accumulate many entries about sending NAKs and giving up. These may be avoided by telling the receiver that its digitiser is using one of these modes and that rewinding will not work. The log messages are harmless, so leave this check-box clear if unsure.

The following additional options appear in expert mode:

[Home](#) → [Configuration](#) → [Serial](#) → [PortA](#) → [GCF input](#)

## Port A block recovery protocol settings

|                    |   |
|--------------------|---|
| Disable rewind     | <input type="checkbox"/><br>Disable BRP rewinding, for DM24s in adaptive mode etc.        |
| Transmission delay | <input type="text"/> s<br>Transmission delay in fractional seconds, used for NTP.         |
| Log file           | <input type="text"/><br>Path to log file. Leave blank to use syslog.                      |
| Log level          | Important notices ▾<br>Minimum severity level of messages to record in log.               |
| Audit log size     | 256KiB (medium) ▾   |
| Debug port         | <input type="text"/><br>TCP port number or service name to which a copy of input is sent. |
| GDI multiplexor    | Default data transport daemon ▾<br>Select which GDI multiplexor instance to send data to. |

[Home](#)
[Help](#)
[Simple](#)
[Submit](#)

Generated at 2010-01-26T14:40:24Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

The **Transmission delay** text field allows the operator to specify the total delay incurred during packet transmission from the attached digitiser. Digitisers can produce special “RTSTATUS” packets which can be used to synchronise the NTP subsystem and, hence, the system clock, with the digitiser's own GPS-synchronised clock (see section 6.3 on page 64). Unlike normal NTP peer dialogues, there is no transmission delay discovery mechanism so, for optimal accuracy, it is important to specify the value here. The ordinary delay associated with packet transmission down a “short” serial cable is already calculated and used, so this field only needs populating if additional delays generated by, say, line drivers or modems, are encountered.

It may sometimes be desirable, for debugging purposes, to separate log messages for this input from the standard system log. The **Log file** text field can be populated with a path name which will then be used for

dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

The GCF input subsystem keeps its own audit log, independent from the system log. The contents of this log are available using the “GCF Audit Log viewer” facility as described in section 13.3.2 on page 182. The amount of data retained is controlled by the **Audit log size** drop-down menu, whose choices are:

- 64Kib (small);
- 256Kib (medium);
- 2MiB (large); and
- 16MiB (huge).

It is possible to copy all incoming data, verbatim, to a network port, which can be specified in the **Debug port** text field. This is an advanced debugging technique which is beyond the scope of this manual.

In most configurations, all data from all inputs is sent to a single multiplexor which then feeds all outputs, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this receiver. The menu offers a list of currently configured multiplexers.

## 9.2 BRP - GCF From Network Devices

---

The CMG-EAM can receive data from network enabled instruments such as the CMG-6TD and networked digitisers such as the CMG-DM24. Data can be received from any number of sources, by creating multiple GCF BRP receiver instances.

To set up a GCF BRP receiver on the CMG-EAM, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Configuration” → “Data transfer/recording” menu. To configure a receiver from the command line, start `gconfig` and select “System services” from the top level menu.

From the “System Services” menu, select “GCF BRP network client”. The next screen shows a list of all GCF BRP receiver instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [gcf-in-brp](#)

---

### GCF BRP network client instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 2010-01-26T13:11:45Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

To configure a new GCF BRP receiver instance, select “Create new service instance”. The following screen allows you to configure the parameters of the service:

## Network BRP client settings

|                   |  |
|-------------------|--|
| User description  | <input type="text" value="GCF BRP network client (instance 1)"/><br>User label for the receiver instance |
| User label        | <input type="text" value="Network BRP in 0"/><br>Application label used for identification in logs       |
| Enable            | <input type="checkbox"/><br>Enable this BRP receiver at system startup                                   |
| Delete            | <input type="checkbox"/><br>Delete this BRP receiver instance  |
| Remote server     | <input type="text"/><br>The remote server to connect to for data   |
| Remote service    | <input type="text" value="10002"/><br>The remote service or port number to connect to                    |
| Allow disconnects | <input checked="" type="checkbox"/><br>Attempt to reconnect broken TCP connections                       |
| Disable rewind    | <input type="checkbox"/><br>Disable BRP rewinding, for DM24s in adaptive mode etc.                       |

Generated at 2010-01-26T13:17:27Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

### 9.2.1 Configurable parameters in standard mode

The **User description** text-field sets the name of the service; this should be set to a meaningful name for the data that it will be receiving, such as the IP or hostname of the network digitiser.

The **User label** is another optional text-field. If set, this label is used to identify the particular client instance in log-files.

The service can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely using the **Delete** check-box.

Specify the hostname or IP address of the network digitiser in the **Remote Server** text-field and the port (name or number) that the digitiser is transmitting on in the **Remote service** box.

If the **Allow disconnects** check-box is ticked, the instance will attempt to automatically recover from lost connections by trying to reconnect to the server.

If the **Disable rewind** check-box is ticked, no attempts will be made to request missing data blocks. This should only be selected if the server is unable to fulfil such requests.

## 9.2.2 Configurable parameters in expert mode

Additional options appear on this screen when in expert mode:

|                    |  |
|--------------------|--|
| Disable rewind     | <input type="checkbox"/> Disable BRP rewinding, for DM24s in adaptive mode etc.  |
| Log file           | <input type="text"/><br>Path to log file. Leave blank to use syslog.   |
| Log level          | Important notices <input type="button" value="v"/><br>Minimum severity level of messages to record in log.               |
| Audit log size     | 256KiB (medium) <input type="button" value="v"/>   |
| Debug port         | <input type="text"/><br>TCP port number or service name to which a copy of input is sent.                                |
| Port name override | <input type="text"/><br>Replacement port name to display for terminal access.  |
| GDI multiplexor    | Default data transport daemon <input type="button" value="v"/><br>Select which GDI multiplexor instance to send data to. |

Generated at 2010-01-27T15:12:12Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

It may sometimes be desirable, for debugging purposes, to separate log messages for this input from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

The GCF input subsystem keeps its own audit log, independent from the system log. The contents of this log are available using the “GCF Audit Log viewer” facility as described in 13.3.2 on page 182. The amount of data retained is controlled by the **Audit log size** drop-down menu, whose choices are:

- 64Kib (small);



- 256Kib (medium);
- 2MiB (large); and
- 16MiB (huge).

It is possible to copy all incoming data, verbatim, to a network port, which can be specified in the **Debug port** text field. This is an advanced debugging technique which is beyond the scope of this manual.

The **Port name override** text field allows the operator to specify a descriptive name for this data source. If left blank, it will be labelled with the IP address and service number of the source device, and this label will appear in, for example, the GDI channels display and the network tree in Scream!.

In most configurations, all data from all inputs is sent to a single multiplexor which then feeds all outputs, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this receiver. The menu offers a list of currently configured multiplexers.

## 9.3 Data from Scream! servers

---

The CMG-EAM has the ability to receive data over the network from Scream! servers. Data can be received from a number of Scream! servers using a single Scream! client.

To set up a Scream! client on the CMG-EAM, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Configuration” → “Data transfer/recording” menu. To configure a Scream! client from the command line, start `gconfig` and select “System services” from the top level menu. From the “System Services” menu, select “gcf-in-scream -- GCF Scream network client”. The next screen shows a list of all Scream network client instances that have been configured:

### GCF Scream network client instance selection

- [Create new service instance](#)

---

Generated at 2009-07-10T14:20:01Z by `ecs 1.1.5`. Portions of output copyright (c)2009, Guralp Systems Limited.



To configure a Scream receiver, select “Create new service instance”. The resulting screen allows you to configure the parameters of the service.

[Home](#) → [Configuration](#) → [Services](#) → [gcf-in-scream](#) → 0

## Scream network client

|   |  |
|---|--|
| User description  | <input type="text" value="GCF Scream network client (instance 1)"/><br>User label for the convertor instance |
| Enable  | <input type="checkbox"/><br>Enable the convertor at system startup   |
| Delete  | <input type="checkbox"/><br>Delete this convertor instance   |
| Please note this page has additional descriptions for the sections below; press the Help button to view them. |  |

## Network options

|               |   |
|---------------|---|
| Local address | <input type="text"/><br>Local interface address or hostname. Leave blank for all. |
| Local service | <input type="text" value="scream1"/><br>Local port number or service name.        |

## Servers

Each server requires a unique name. This is used for configuration and logging only.

| Name                 | Hostname             | Service              | Type  | Delete                   |
|----------------------|----------------------|----------------------|-------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | UDP ▾ | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | UDP ▾ | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | UDP ▾ | <input type="checkbox"/> |

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 2010-01-27T16:04:54Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.

The **User description** field sets the name of the service; this should be set to a meaningful name for the data that it will be receiving, such as the IP or hostname of the Scream! server.

The service can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely using the **Delete** check-box.

If the CMG-EAM has multiple IP addresses, you can optionally restrict the client so that all connection attempts are made via only one address by putting it in the **Local address** field. You can also specify that requests should be made from a specific port number by entering

it in the **Local service** field. These two fields can normally be left blank.

In the “Servers” section, you specify the details of the Scream! servers from which you want to pull data. The **Name** field should contain a descriptive name for identification purposes. The **Hostname** field must contain the DNS name or IP address of the desired server. The **Service** field should contain the UDP/TCP port number on which the server is listening for data requests. Port numbers can be mapped to names using the standard Linux `/etc/services` file, which can be edited from the command line.

In the **Type** column, choose whether you wish to use UDP packets or TCP connections. With UDP packets, the GCF protocol keeps track of which packets have been received and automatically requests retransmission of any missing data. TCP, on the other hand, is a connection-orientated protocol which handles packet sequencing and retransmission itself (at the cost of a little extra network overhead).

## 10 Recording and Retrieving Data

Data can be recorded to internal and external storage, in raw GCF format or in miniSEED format. Data can be browsed via the web interface or copied to external computers for further processing.

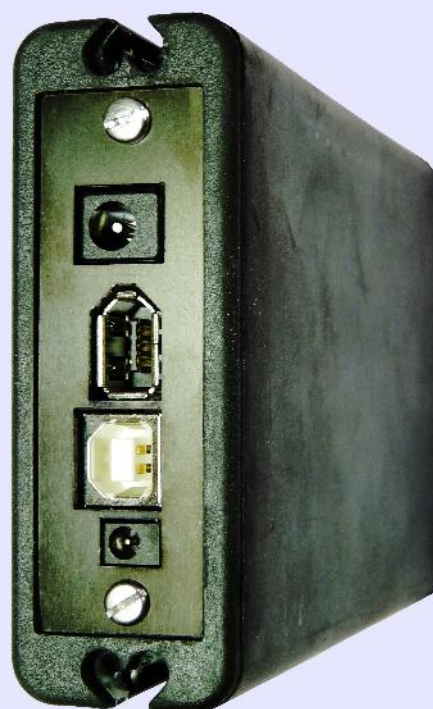
### 10.1 Preparing removable drives

When a new removable disk is to be used with a CMG-EAM, it must first be formatted for use. The disk can be formatted by any computer, but the CMG-EAM also has the capability of formatting the disk itself. The CMG-EAM accepts disks formatted in either ext3 format (which is faster and more reliable, but can only be read under Linux systems) or VFAT format (slower and arguably less reliable, but can be read under all operating systems). To prepare the disk on a PC, simply format it with a single partition containing either of the above file-systems; it can then be inserted directly into a CMG-EAM.

**Note:** When using removable disks from CMG-EAMs and CMG-DCMs with PCs, you may need to provide a power supply for the disk.

When using a six-circuit (powered) IEEE1394 FireWire interface, the disk can draw its power from the host PC. When connected to a four-circuit (unpowered) FireWire interface, such as Sony i.Link, external power needs to be applied as described below. Power also needs to be supplied when using the USB interface.

A power supply of between 4.5V and 30V DC should be connected to the 2.1mm barrel connector (lowermost in the picture). The central pin of the connector should be connected to the positive supply line.



**IMPORTANT:** Do not connect anything to the larger barrel connector, which is used for the heater and temperature sensor.

To prepare the disk on the CMG-EAM using the web interface, select the “Removable disk” item from the “Tools” menu and then click on the “Format disk” button. After a delay, while the disk powers up, the following screen will appear:

[Home](#) → [Tools](#) → [Removable disk](#) → [Format](#)

---

## Removable disk

---

### Format and partition disks

If you have accessed the disk within the last minute or so, or if it is in use by another program, then formatting will fail. In this case, simply wait and try again in some minutes.

Usually, you will want to select a disk under the *partitioning* option below. This partitions and formats the disk. If you know that you have other partitions on the device that you want to keep, you can use the more advanced *format* option.

Select disk for partitioning

The following disks are attached. Pressing the Partition button will cause the selected disk to be repartitioned and then formatted. This will erase any other partitions and filesystems on the disk.

Select partition for formatting

The following disks have valid partition tables. The partitions they contain may be formatted. Select a partition and press the Format button.

*Generated at 2010-01-28T16:25:31Z by `rdisk.cgi`. Portions of output copyright (c)2010, Guralp Systems Ltd.*

The drop-down menus for device selection use the Linux device naming convention, where `/dev/sda` is the first device, `/dev/sdb` is the second and so on. Individual partitions on devices are identified by an appended number, so `/dev/sda1` is the first partition on the first device and `/dev/sdb3` is the third partition on the second device.

The “Partition” button causes the selected device to be repartitioned with a single partition which is then reformatted. If you are using a device with existing partitions that you wish to preserve, you should use the “Format” button instead.

Successful completion of the format is signalled by a short, on-screen message. The disk is then ready for use.

Disks can also be formatted from the command line with the command

```
eam999 ~ # rdisk format
```

## 10.2 Recording data

All data recording is performed by the `gdi-record` module. Data are recorded first to a buffer held in flash memory. When the buffer utilisation exceeds a configurable percentage, a process is triggered to flush the data to the hard drive. In low power applications, the hard drive will normally be powered down and, so, must be powered up, and mounted before use. It is then dismounted and powered down once the flush is complete.

The disk is equipped with a temperature sensor and heating element. In low temperature applications, the disk will automatically be warmed to a safe operating temperature before power is applied.

The options that control this process are all on one page but, given its size, it is shown here in sections.

To configure data storage, select “Disk data recording” from the “Configuration” → “All options” menu *or* select the “Disk recording” short-cut from the Configuration” → “Data transfer/recording” menu. To configure recording from the command line, start `gconfig` and select “Disk data recording” from the top level menu.

The first part of the configuration screen for `gdi-record` looks like this:

[Home](#) → [Configuration](#) → [Disk recording](#)

### Disk recording configuration

These parameters control global disk recording operation and the removable disk support daemon (`rdisk`).

|  |  |  |
|--|--|--|
| Disable all recording  | <input type="checkbox"/>               | Disable all data recording to disk                     |
| Recycle files  | <input type="checkbox"/>               | Remove old files from the hard disk when low on space. |
| Check output flush   | Every 5 minutes ▾                      | How often to check whether output needs flushing       |
| Recording destination  | Removable USB disk in internal tray. ▾ | The destination device for recording to                |
| Using the removable disk support daemon. Use expert mode if you wish to disable. |  |  |

The default settings for this service will work in most installations but, if you wish to fine-tune the behaviour of `gdi-record`, there are a number of configurable options.

### 10.2.1 Configurable parameters in standard mode

---

The following configuration options are available from the “simple” dialogue:

- **Disable all recording.** This check-box, when ticked, unconditionally disables all recording.
- **Recycle files** – If this check-box is ticked, `gdi-record` will remove the oldest files from external storage to make room for new data when the external storage becomes full. If this option is cleared then, when the storage becomes full, the module will check periodically for free space and start writing again when it can.
- In order to reduce power consumption, `gdi-record` does not write continuously to the hard drive. Data are buffered in flash memory and, at a configurable interval, these data are checked to see which complete files can be written to disk. The **Check output flush** option controls how often this happens. The options are every minute, every five, fifteen or thirty minutes and every hour.
- The **Recording destination** drop-down menu controls where data are stored. The options may include one or more of:
  - “Removable USB disk in internal tray” - this is the default setting for CMG\_EAMs and CMG-DCMs. Data are written to the removable USB/FireWire disk and can be read via the web interface, the command line or by removing the disk and attaching it to an external USB or FireWire host, such as a laptop.;
  - “External USB drive on mil-spec connector” - data will be stored on external media, which should be attached to the USB connector. The `rdisk` daemon handles the required operations for mounting and un-mounting the file-system;
  - “Internal USB storage” - for authenticated digitisers only, data can be stored on internal USB-accessible flash memory. It can be retrieved by a USB host (such as a laptop) connected via the GPIO connector. See section 14.2.3.1 on page 196 for more details;
  - “Ring buffer on flash module” - some systems are equipped with an external flash module to extend the

storage capacity beyond that available on the normal file-system. Data written here are accessible via the web interface or, from the command line, under the path `/media/flash_module`;

- “Record files under `/var/spool/recdata`” - this is the only option on CMG-NAMs and CMG-NAM64s and it is not available on other platforms. Data are written directly to the internal hard drive and are accessible via the web interface or, from the command line, under the path `/var/spool/recdata`.

### 10.2.1.1 GCFFraw Options

GCFFraw is the native recording format of Platinum firmware. It can be read directly by **Scream!** and other GSL software packages are available for converting it into other formats.

### GCFFraw recording

These parameters control the recording of raw GCF packets.

|                       |   |
|-----------------------|---|
| Disable GCF recording | <input type="checkbox"/><br>Disable the recording of raw GCF data.    |
| File period           | <div>30 minutes ▾</div> <div>Time span held in each output file</div> |

GCFFraw recording is enabled by default. To disable it, select the **Disable GCF recording** check-box.

GCF files contain data from all streams and can grow quite large. The data are split into manageable chunks on the basis of sample times. By default, every thirty minutes the current file is closed and recording recommences to a new file. This interval can be changed using the **File period** drop-down. The options are 15 or 30 minutes and 1, 2, 3, 4, 6 or 12 hours.

Extra options are introduced to this screen by pressing the “Expert” button. These include file name format control for GCF and miniSEED. See the following section for details.

### 10.2.1.2 Mini-SEED Options

For some applications, it is more convenient to store the data directly in mini-SEED format. The third section of the “Disk data recording” page controls options related to recording in this format. If recording in mini-SEED format is enabled, a GDI Mini-SEED compressor

(converter) is started automatically. See section 11.3 on page 138 for more details.

### mini-SEED recording

These parameters control the recording of data as mini-SEED packets.

|                             |   |
|-----------------------------|---|
| Disable mini-SEED recording | <input checked="" type="checkbox"/> Disable recording data as mini-SEED packets.  |
| File period                 | 30 minutes <input type="button" value="v"/><br>Time span held in each output file |

---

*Generated at 2010-01-27T17:26:55Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

Mini-SEED recording is disabled by default. To enable it, clear the **Disable mini-SEED recording** check-box.

By default, every three hours the current mini-SEED file is closed and recording recommences to a new file. This interval can be changed using the **File period** drop-down menu. The options are 15 or 30 minutes and 1, 2, 3, 4, 6 or 12 hours.

### 10.2.2 Configurable parameters in expert mode

---

|                  | How often to check whether output needs flushing   |
|------------------|--|
| Use rdisk        | <input checked="" type="checkbox"/> Use the removable disk support daemon to mount the output tree |
| Output directory | <input type="text"/><br>Root of the output tree  |
| Check file       | <input type="text"/><br>Optional marker file required before flush is allowed.                     |
| Mount command    | <input type="text"/><br>Optional command to prepare the output tree for writing.                   |
| Unmount command  | <input type="text"/><br>Optional command to release the output tree after writing.                 |

The first set of extra options, shown above, apply to all recording.

The **rdisk** daemon controls the disk's power and heater and is designed to simplify the process of mounting and dismounting the removable disk pack. Its user interface is described in detail in section 10.3.1.2 on page 120. Where there are no removable drives (as, for example, in a typical CMG\_NAM configuration), the use of **rdisk** is unnecessary. It may be turned off by clearing the **Use rdisk** check-box.



If `rdisk` is not used, the **Output directory** text field must be populated with a pathname to the desired storage directory. If a directory name is given here and `rdisk` is used, the directory named must be the same as or a subdirectory of the directory managed by `rdisk`.

It is sometimes desirable to synchronise the flushing of memory to disk with an external application. This can be achieved with the use of a semaphore file: the external application writes the file when it is ready to receive data and can remove it in order to inhibit flushing. To activate this feature, enter the desired semaphore file into the **Check file** text field. The same technique can be used to detect the mount status of removable hardware.

An arbitrary command can be run immediately prior to flushing the memory to disk. This is typically used for mounting external storage devices on, say, a CMG-NAM but could also be used for synchronising operations with an external application. If you require to use such a command, specify it in the **Mount command** text field.

The **Unmount command** text field fulfils a similar function but is run immediately after flushing.

|                  |   |
|------------------|---|
|                  | Time span held in each output file  |
| Fill threshold   | <input type="text" value="50"/> %<br>Percentage buffer fill that triggers an output flush   |
| Directory format | <input type="text" value="%Y%-j-gcfraw"/><br>Format for creating the output parent directory                                      |
| File name format | <input type="text" value="%Y%jT%H%MZ.gcf"/><br>File name format for creating the output files                                     |
| GCF compressor   | <input type="text" value="GCF compressor. Default instance"/><br>Select which GCF compressor/ringbuffer instance to get data from |

The second set of expert options, shown above apply only to GCF recording.

The **Fill threshold** text field allows control over the percentage utilisation of the buffer memory which triggers a flush to disk. The default is fifty percent.

The **Directory format** text field can be used to control the base directory under which all GCF files are stored. It can be populated with a constant path name component or it can include escape sequences to include variable data such as the stream name: these are described in section 10.2.3 on page 115.

The **File name format** text field allows files to be given descriptive names to help identify the data within. Escape sequences can be used to include variable data such as the stream name: the available escape sequences are described in section 10.2.3 on page 115. A hierarchical directory structure can be created by incorporating forward-slash characters, '/', into the name: these act as directory separators.

The **GCF compressor** drop-down menu allows the operator to select which instance of `gdi2gcf` is used as the data source. The menu will offer all configured instances.

|   |  |
|---|--|
|   | Time span held in each output file   |
| Fill threshold  | <input type="text" value="50"/> %<br>Percentage buffer fill that triggers an output flush  |
| Directory format  | <input type="text" value="%Y%j-mseed"/><br>Format for creating the output parent directory   |
| File name format  | <input type="text" value="%Y%jT%H%MZ-%s-%c-%n-%l.mseed"/><br>File name format for creating the output files                          |
| Mini-SEED compressor  | <input type="text" value="Mini-SEED compressor. Default instance"/><br>Select which Mini-SEED compressor/ringbuffer to get data from |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Simple"/> <input type="button" value="Submit"/> |  |

*Generated at 2010-01-28T14:15:59Z by gcs 1.1.8. Portions of output copyright (c)2010, Guralp Systems Limited.*

The third set of expert-mode options, shown above, apply only to miniSEED recording.

The **Fill threshold** text field allows control over the percentage utilisation of the buffer memory which triggers a flush to disk. The default is fifty percent.

The **Directory format** text field can be used to control the base directory under which all miniSEED files are stored. It can be populated with a constant path name component or it can include escape sequences to include variable data such as the stream name: these are described in section 10.2.3 on page 115.

The **File name format** text field allows files to be given descriptive names to help identify the data within. Escape sequences can be used to include variable data such as the stream name: the available escape sequences are described in section 10.2.3 on page 115. A hierarchical directory structure can be created by incorporating forward-slash characters, '/', into the name: these act as directory separators.

The **mini-SEED compressor** drop-down menu allows the operator to select which instance of `gdi2miniseed` is used as the data source. The menu will offer all configured instances.

### 10.2.3 File name escape sequences

---

Escape sequences are used in the file and directory name fields in the disk recording configuration page. They all begin with a '%' character and are used to insert variable data such as the data or stream name into the file or directory name; each escape sequence is replaced with the relevant value. Any non-escape sequence characters are copied verbatim into the name. All numbers are decimal and will have leading zeroes added to fill the number of digits.

The available escape sequences are:

- **%d** 2 digit day of month (01-31)
- **%H** 2 digit hour in 24 hour clock (00-23)
- **%j** 3 digit Julian day
- **%m** 2 digit month (01-12)
- **%M** 2 digit minute (00-59)
- **%y** 2 digit year i.e. without century digits (00-99)
- **%Y** 4 digit year
- **%s** 5 char SEED station identifier (spaces are removed from all SEED Ids)
- **%c** 3 char SEED channel identifier
- **%n** 2 char SEED network identifier
- **%l** 2 char SEED location identifier

If the format string ends in a `.extension` (without any escape sequences in the extension) then this extension will be noted and used in some other locations – e.g. for the top level date directory.

The default format string is `%Y%j-%H%M-%s-%c-%n-%l.mseed`

Slashes “/” will cause subdirectories to be created. Using them as date separators will have unintended and, usually, undesirable consequences.

#### 10.2.3.1 Some examples

The default `%Y%jT%H%MZ-%s-%c-%n-%l.mseed` includes every piece of information possible. The date format matches that used by the GCF recorder. This will produce file-names like:

```
2008315T1442Z-TEST1-BHE-NN-LL.mseed
```

To combine all the channels from a given station simply omit the channel marker from the file name format string:

```
%Y%jT%H%MZ-%s--%n-%l.mseed
```

It is recommended that the “--” is left in place to highlight the omitted channel id. This will produce file-names like:

```
2008315T1442Z-TEST1--NN-LL.mseed
```

If you specifically want to include a marker to identify that it contains all channels, the use of a lower case string will differentiate it from a regular channel name, which is always presented in upper case.

```
%Y%jT%H%MZ-%s-all-%n-%l.mseed
```

yields file-names like:

```
2008315T1442Z-TEST1-all-NN-LL.mseed
```

If you prefer human readable dates, rather than using the Julian date

```
%Y_%m_%d-%H:%M-%s-%c-%n-%l.mseed
```

yields file-names like:

```
2008_08_14-14:42-TEST1-BHE-NN-LL.mseed
```

**Note:** don't use / as a date separator as this will split the data into sub-directories which is probably not the desired result.

It is often required to separate the data into sub directories by network and station prefix. In this case, it is recommended that the network and station id are still included in the file-name so that the contents of the file are still recognisable even if it is moved to a different location.

```
%n_%s/%Y%jT%H%MZ-%s-%c-%n-%l.mseed
```

will store the data like this:

```
NN_TEST1      2008315T1442Z-TEST1-BHE-NN-LL.mseed
                2008315T1452Z-TEST1-BHE-NN-LL.mseed
                2008315T1502Z-TEST1-BHE-NN-LL.mseed
                ...
NN_TEST2      2008315T1442Z-TEST2-BHE-NN-LL.mseed
                2008315T1452Z-TEST2-BHE-NN-LL.mseed
                2008315T1502Z-TEST2-BHE-NN-LL.mseed
                ...
```

## 10.3 Retrieving data

---

Data are recorded first to a buffer held in flash memory. When the buffer utilisation exceeds a configurable percentage, a process is triggered to flush the data to the hard drive. In low power applications, the hard drive will normally be powered down and, so, must be powered up and mounted before use. It is then dismounted and powered down once the flush is complete.

If you wish to work with data on the removable drive, it must first be powered up. This is done automatically when using the web interface but must be done manually when working from the command line. If you wish to work with recent data, a manual flush should first be performed in order to move the data from the buffer memory to the drive.

### 10.3.1 Retrieving data from the removable drive

---

#### 10.3.1.1 Downloading over a network, using the web interface

**Note:** It can take several seconds to pre-heat and power up the drive. Be prepared for short delays when using some of the following commands.

To retrieve data from the removable drive using the web interface, select “Removable disk” from the “Tools” menu. The following screen appears:

[Home](#) → [Tools](#) → [Removable disk](#)

## Removable disk

Connect removable disk and select action.

| Description   | Action                           |
|---|----------------------------------|
| View filesystems on attached disks. Use this to check for valid disks, to find how much space is available, to see whether the disk is in use, and to view files on the disk. | <a href="#">View filesystems</a> |
| Write whatever is currently buffered in flash to disk.  | <a href="#">Flush to disk</a>    |
| Partition and format attached disks. This will erase <i>ALL</i> data on the disk.   | <a href="#">Format disk</a>      |

*Note:* actions may take some time to complete if the disks are not powered up. The web page will not load until after this has occurred. Please be patient.

*Generated at 2010-01-28T17:23:23Z by rdisk.cgi. Portions of output copyright (c)2010, Guralp Systems Ltd.*

If you wish to retrieve recent data, click the “Flush to disk” button to copy all pending data from the buffer memory to the hard drive. A progress screen will display messages as the various stages of the process complete.

[Home](#) → [Tools](#) → [Removable disk](#) → [Flush](#)

## Removable disk

### Flush files to disk

```
Data flush has been signalled to daemon.
This may take some time to complete.
User triggered flush started
Contacting rdisk daemon
Rdisk daemon mount complete
Flushing GCF buffers
Committing output tree
Tree commit completed
Releasing storage
Flush complete
```

Child exited with status 0. **Normally interpreted as success.**

*Generated at 2010-01-28T17:26:48Z by rdisk.cgi. Portions of output copyright (c)2010, Guralp Systems Ltd.*

Once the flush process has completed, as shown above, return to the main disk menu by clicking on “Removable disk” on the “Tools” menu.

You can now click the “View filesystems” button. This will power up any connected disks and, after a short delay, present a list of attached disks and their details (filesystem, free space, etc).

[Home](#) → [Tools](#) → [Removable disk](#) → [Filesystems](#)

## Removable disk

### View filesystem details

Filesystem details.

| UUID      | Type | Size    | Free space      | Earliest entry | Used by | Index of files             |
|-----------|------|---------|-----------------|----------------|---------|----------------------------|
| 50AD-F5D8 | vfat | 37.2GiB | 34.0GiB (91.4%) | 2009336-gcfraw |         | <a href="#">View files</a> |

Generated at 1970-01-03T15:34:16Z by *rdisk.cgi*. Portions of output copyright (c)1970, Guralp Systems Ltd.

Clicking on the “View Files” buttons takes you to the “Removable disk file index” screen, which displays folders and files. Sub-directories (folders) have a “Follow” button next to them and files have a “Download” button.

The first screen typically looks like this:

[Home](#) → [Tools](#) → [Removable disk](#) → [Filesystems](#) → [50AD-F5D8](#)

### Removable disk file index

Filesystem UUID: 50AD-F5D8

Path: /

Choose a subdirectory to follow, or a file to download.

| File or directory name | File size | Follow or download     |
|------------------------|-----------|------------------------|
| 2009336-gcfraw         |           | <a href="#">Follow</a> |
| 2009337-gcfraw         |           | <a href="#">Follow</a> |
| 2009338-gcfraw         |           | <a href="#">Follow</a> |
| 2009339-gcfraw         |           | <a href="#">Follow</a> |
| 2009340-gcfraw         |           | <a href="#">Follow</a> |
| 2009341-gcfraw         |           | <a href="#">Follow</a> |
| 2009342-gcfraw         |           | <a href="#">Follow</a> |
| 2009343-gcfraw         |           | <a href="#">Follow</a> |
| 2009344-gcfraw         |           | <a href="#">Follow</a> |
| 2009345-gcfraw         |           | <a href="#">Follow</a> |
| 2009346-gcfraw         |           | <a href="#">Follow</a> |

Descending into one of these directories (using the follow button) produces this:

[Home](#) → [Tools](#) → [Removable disk](#) → [Filesystems](#) → [50AD-F5D8](#) → [/2009336-gcfraw](#)

### Removable disk file index

Filesystem UUID: 50AD-F5D8  
Path: /2009336-gcfraw

Choose a subdirectory to follow, or a file to download.

| File or directory name      | File size | Follow or download                      |
|-----------------------------|-----------|---|
| .. (up to parent directory) |           | <input type="button" value="Follow"/>   |
| 2009336T0930Z.gcf           | 0.9MiB    | <input type="button" value="Download"/> |
| 2009336T1000Z.gcf           | 2.2MiB    | <input type="button" value="Download"/> |
| 2009336T1030Z.gcf           | 1.8MiB    | <input type="button" value="Download"/> |
| 2009336T1100Z.gcf           | 1.7MiB    | <input type="button" value="Download"/> |
| 2009336T1130Z.gcf           | 1.9MiB    | <input type="button" value="Download"/> |
| 2009336T1200Z.gcf           | 1.9MiB    | <input type="button" value="Download"/> |
| 2009336T1230Z.gcf           | 1.9MiB    | <input type="button" value="Download"/> |

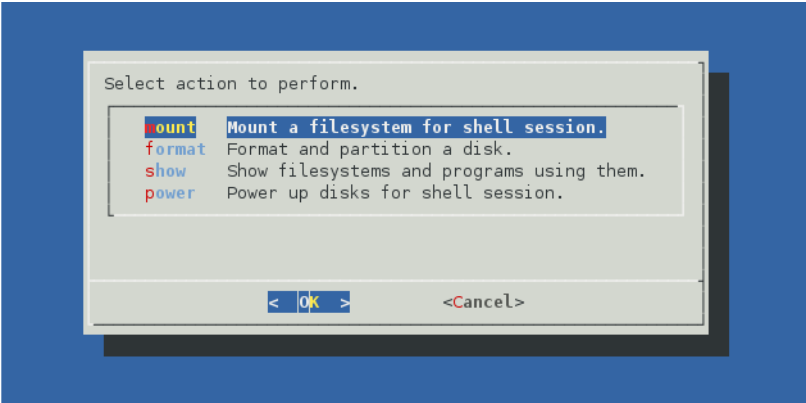
If the displayed directory contained subdirectories, you could continue to navigate down them using the “Follow” buttons. When files are present, as in the above screen-shot, they each have an associated “Download” button which invokes your web browser's standard download facility to copy the data to your computer.

#### 10.3.1.2 Downloading over a network, using the command line

**Note:** It can take several seconds to pre-heat and power up the drive. Be prepared for short delays when using some of the following commands.

Before data can be retrieved from the removable drive, it must first be brought to operating temperature, powered up and the relevant file-systems mounted. A utility, `rdisk`, is provided to accomplish this.

When invoked without arguments, `rdisk` displays a menu:





The “mount” option, which can be selected with the **M** key, displays a menu of available file-systems on removable media. When you choose your desired file-system, it is mounted under `/media` and you will be told the exact mount point and then presented with a command prompt. This is a sub-shell: the file-system will remain mounted and the disk will remain powered up until you exist the shell (with the `exit` command or by keying **Ctrl** + **D**).

The “format” option, which can be selected with the **F** key, prepares a drive for use, as described in section 10.1 on page 107.

The “show” option, which can be selected with the **S** key, lists all available removable drives, together with their file-system type, size, free space and date of earliest entry.

When using shell scripts, all of these menu functions can be accessed by passing the function name as an argument to `rdisk`. For example:

```
eam999 ~ # rdisk show
```

performs the same function as selecting “show” from the `rdisk` menu.

Once the disk is powered up and the relevant file-system mounted, the recorded files can be browsed with standard Linux shell commands such as `cd` and `ls`. They can be copied to a remote PC using the network or over the serial port (as described in section 10.3.1.3 on page 124).

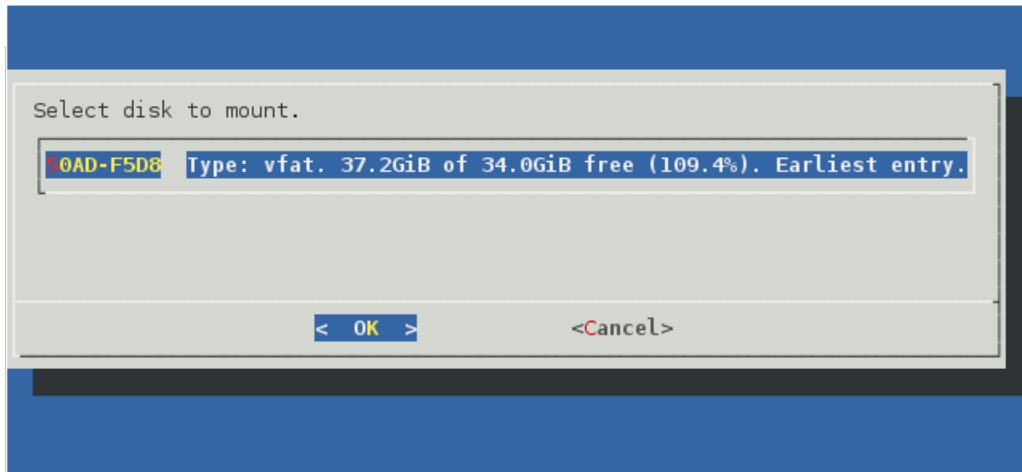
To copy files over the network, the use of `scp` or `rsync` is recommended. The `scp` program is most convenient to use and can copy single files or recursively copy directories. The `rsync` program is more complicated but is ideal when a remote copy of the data is to be updated regularly, since it minimises the traffic over the network by only copying new or changed files.

For Linux users, `scp` is installed by default or available as an optional package in most distributions. Consult your operating system documentation for more details. For Windows users, the WinSCP package is recommended: this has the additional benefit of providing a graphical, explorer-like interface for browsing files on the CMG-EAM. WinSCP can be downloaded for free from <http://winscp.net>.

The screen-grab below shows a complete session recorded from a Linux PC. The operator connects to a CMG-EAM, powers up the disks,

downloads all recorded files, powers down the disks and then disconnects.

```
fish@fish-desktop:~/tmp$ ssh root@51.187.130.165
dcm105 ~ # rdisk mount
Connected to server. Powering up disks and requesting details...
```



```
Requesting disk with UUID `50AD-F5D8'...
The disk is mounted at: /media/50AD-F5D8
A new bash session has been created.
```

When you exit from this bash session (which you can do with `exit' or Ctrl-D), the disk will be unmounted. It will remain mounted (and thus powered up) until you exit. Then you will be returned to your original shell.

```
dcm105 ~ # ^Z [suspend ssh]
```

```
[1]+  Stopped                  ssh root@51.187.130.165
fish@fish-desktop:~/tmp$ scp -r root@51.187.130.165:/media/50AD-F5D8 .
2009336T1030Z.gcf                100% 1886KB 314.3KB/s   00:06
2009336T1100Z.gcf                100% 1781KB 356.2KB/s   00:05
2009336T1130Z.gcf                100% 1910KB 382.0KB/s   00:05
2009336T1200Z.gcf                100% 1928KB 385.6KB/s   00:05
2009336T1230Z.gcf                100% 1957KB 326.2KB/s   00:06
2009336T1300Z.gcf                100% 1889KB 377.8KB/s   00:05
fish@fish-desktop:~/tmp$ fg
ssh root@51.187.130.165
```

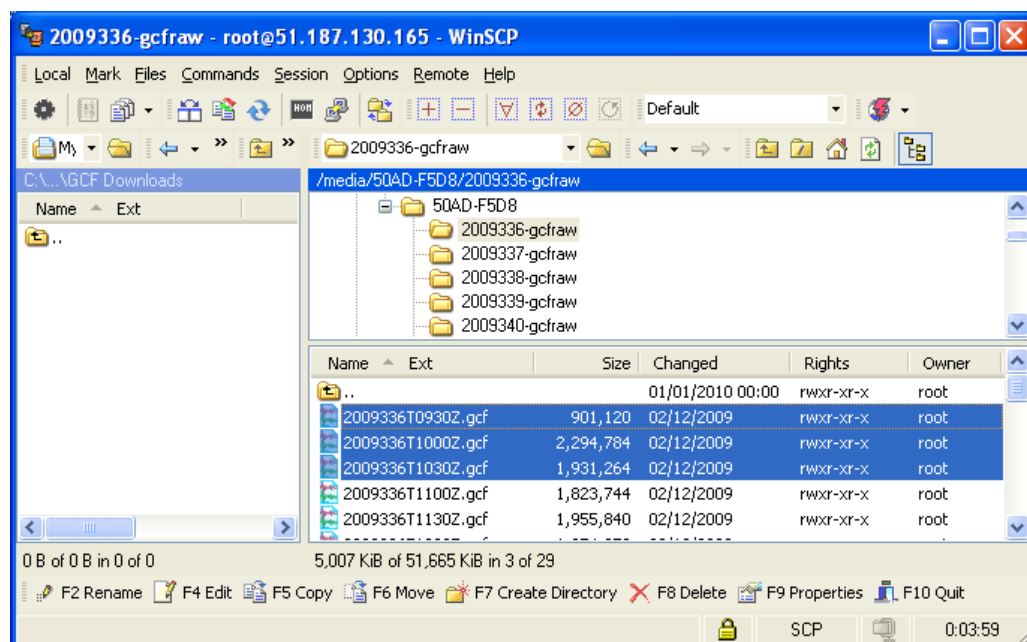
```
dcm105 ~ # exit
```

Disk no longer required by this shell session.

```
dcm105 ~ # logout
Connection to 51.187.130.165 closed.
fish@fish-desktop:~/tmp$ fg
```

Note the use of ssh's tilde ('~') escape followed by **Ctrl** + **Z** to suspend the ssh session and return to the calling PC, in order to run the scp command with the disk still mounted. The **fg** command (foreground) returns control to the ssh session.

Windows users should follow the same procedure to log in, power up and mount the file system. At this point, rather than suspending the ssh shell, they can connect with WinSCP and navigate to the `/media` directory. The recorded files will then be displayed and can be dragged and dropped to appropriate locations on the PC:



When the transfer is complete, return to the ssh session and power down the disks (with the `exit` command or by keying **Ctrl** + **D**).

Using `rsync` is very similar: simply replace the invocation of `scp` in the above instructions with an appropriate `rsync` command.

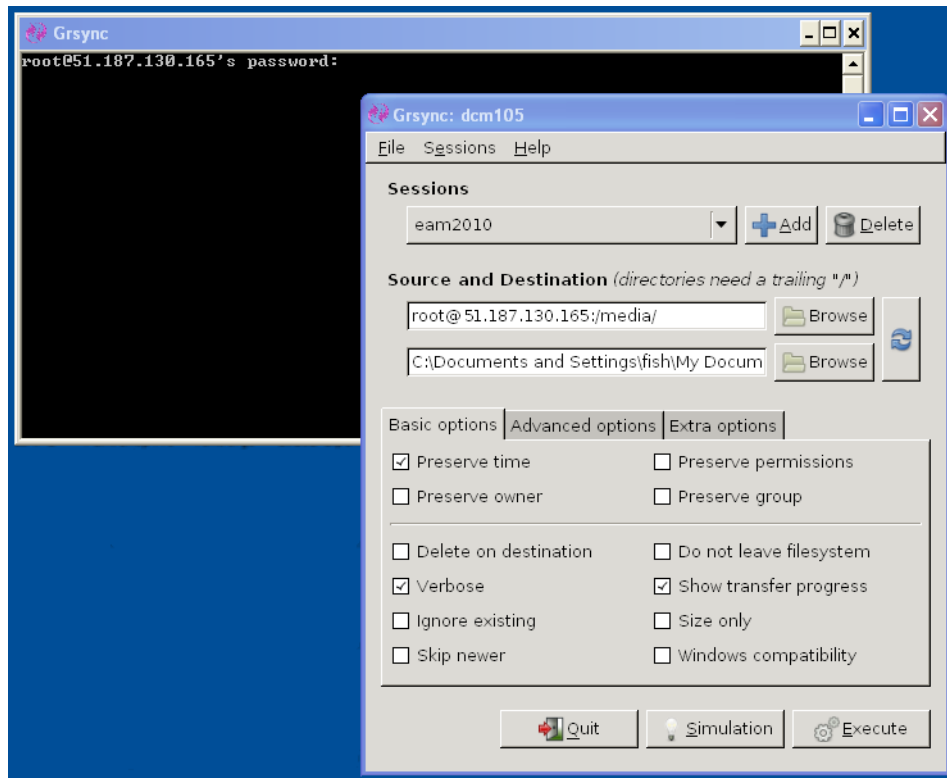
For Linux users, the simplest usage is

```
me@mypc:~/dl $ rsync -avz root@51.187.130.165:/media/*/ .
```

This will copy all files from all removable drives to the current directory on the invoking computer. Only the differences are transferred, making this particularly efficient when used regularly. For more advanced usage, please see the `rsync` manual, available on-line at <http://man-wiki.net/index.php/1:rsync-2006.11.06>

Windows users can download a free port of `rsync` using the `cygwin` library (see <http://www.cygwin.com/> for more information) or use one of several free, graphical interfaces, such as `grsync`, available from <http://sourceforge.net/projects/grsync-win/files>

The following screen-shot shows grsync about to download all data from a removable drive. Note the password prompt appearing in the separate console window.



#### 10.3.1.3 Downloading over a serial port, using the command line

In situations where it is not convenient to use the network interface, files can be downloaded from the removable disk using one of three file-transfer protocols, X-modem, Y-modem or Z-modem. None of these protocols were ever rigidly standardised so, if you are not using one of the terminal emulators discussed in this section, you may need to experiment a little: this is reflected in the huge range of optional arguments that the transfer program accepts.

The X-modem transmitter is invoked as **sx**, the Y-modem transmitter as **sy** and the Z-modem transmitter as **sz**. They are, in fact, all implemented by the same program so the detailed help message (displayed with the **--help** option) describes options relevant to all three protocols.

Linux users are advised to use the minicom terminal emulator. This includes X-modem support and its use is described below. For Windows users, we describe the use of HyperTerminal, which is supplied with many Windows systems.

For minicom users, the X-modem protocol should first be configured: start minicom and type **Ctrl** + **A** (minicom's escape sequence) and then **O** to display the options menu:

```
Welcome to minicom 2.3

OPTIONS: I18n
Compiled on Sep 25 2009, 23:40:20.
Port /dev/ttyS0

Press CTRL-A Z for help on special keys

+-----[configuration]-----+
eam2243 logi| Filenames and paths |
Password:   | File transfer protocols |
eam2243 ~ # | Serial port setup      |
            | Modem and dialling     |
            | Screen and keyboard    |
            | Save setup as dfl     |
            | Save setup as..   |
            | Exit              |
+-----+-----+

```

Select “File transfer protocols” and ensure that the command used for X-modem transfers is set to `/usr/bin/sx -vv`

To download a file, mount the disk if required, enter the command

```
eam2010 ~ # sx path-to-file
```

and then immediately type **Ctrl** + **A** followed by **R** to activate minicom's receive file function. Select “xmodem” from the resulting menu and then enter a name for the downloaded file. The transfer should start immediately:

```
The disk is mounted at: /media/50AD-F5D8
A new bash session has been created.

When you exit from this bash session (which you can do with
`exit'+-----[xmodem download - Press CTRL-C to quit]-----+
remain|
you wi|rx: ready to receive 2009336T1030Z.gcf |
      |Bytes received: 154112 BPS:5978        |
eam201|
      |Transfer complete                      |
      |                                     |
      | READY: press any key to continue...  |
+-----+-----+

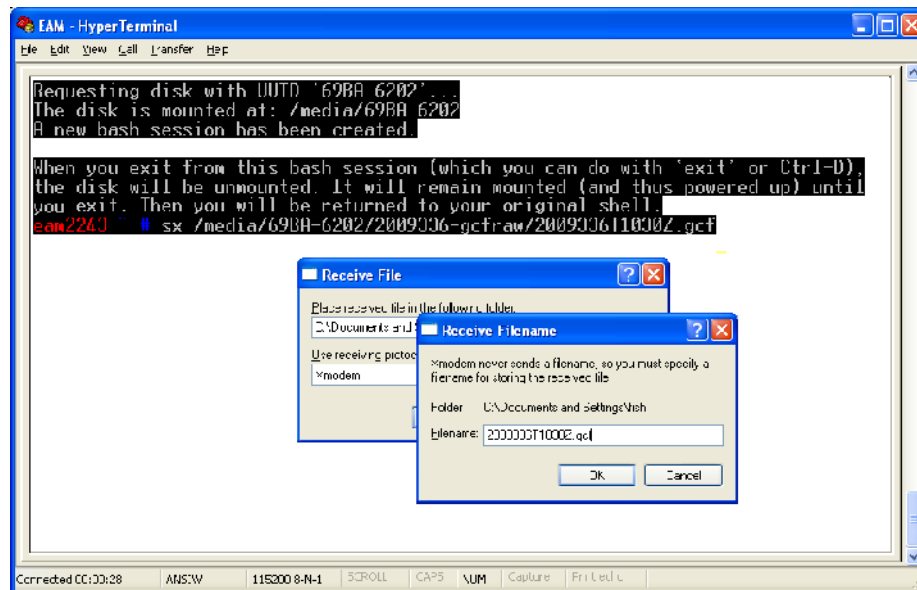
```

A display counter indicates the progress and eventual completion of the transfer.

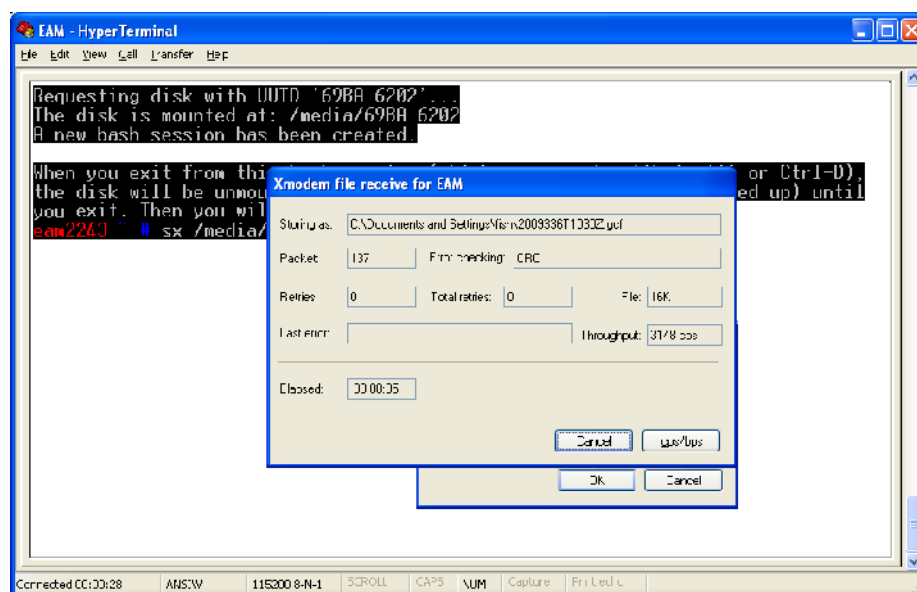
HyperTerminal users should mount the disk, type the command

```
eam2010 ~ # sx path-to-file
```

and then immediately select “Receive File...” from the “Transfer” menu. A dialogue asking for the destination directory name is followed by another asking for the destination file name:



When you click the “OK” button, a progress indicator appears:



You will be returned to the prompt when the transfer is complete.

### **10.3.2 Reading the removable drive on other computers**

---

The removable drive may be disconnected from the system at any time without risk of data loss. In practice, users will normally manually flush the memory contents to disk (using either the `rdisk flush` command or the “Flush to disk” button on the “Removable disk” page of the web interface) and allow that process to complete before removing the drive.

The drive can then be connected to any computer that supports external USB or FireWire storage devices. In some circumstances, you may need to provide a power connection to the drive: see section 10.1 on page 107 for more details.

The disk may have been formatted as either a VFAT or ext3 volume. Windows computers cannot read ext3 volumes without additional software such as “Explore2fs” or “DiskInternals Linux Reader”. See <http://www.howtoforge.com/access-linux-partitions-from-windows> for more details about these two packages.

## 11 Transmitting Data

---

Received data may be retransmitted in near real time in one or more of a number of different formats. By default, a GCF Scream server is configured to forward all received data. Any other desired transmitters must be configured and enabled before use.

The following transmission services are currently available:

- GCF BRP network server - see section 11.1
- GCF Scream network server - see section 11.2
- GSMS: Guralp Seismic Monitoring System - see section 11.4
- QSCD: Quick Seismic Characteristic Data - see section 11.5
- WIN sender - see section 11.6

These servers are all described in the following sections.

### 11.1 GCF BRP Network Server

---

The GCF BRP network server transmits Guralp Compressed Format (GCF) data using the Block Recovery Protocol (BRP) over an Ethernet network.

To configure a GCF BRP network server from the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a GCF BRP network server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “gcf-out-brp” from the System Services menu. The next screen shows a list of all GCF BRP server instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [gcf-out-brp](#)

---

#### GCF BRP network server instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-07T15:29:11Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*



You can reconfigure any existing service by clicking on its menu entry. To configure a new GCF BRP server instance, select “Create new service instance”. The following screen allows you to configure the parameters of the service. It is a large form and is shown here in parts.

[Home](#) → [Configuration](#) → [Services](#) → [gcf-out-brp](#) → [0](#)

## Network BRP server settings

|                  |  |
|------------------|--|
| User description | <input type="text" value="GCF BRP network server (instance 1)"/><br>User label for the server instance |
| User label       | <input type="text" value="Network BRP out 0"/><br>Application label used for identification in logs    |
| Enable           | <input type="checkbox"/><br>Enable this BRP receiver at system startup                                 |
| Delete           | <input type="checkbox"/><br>Delete this BRP receiver instance  |

## Network parameters

|                            |  |
|----------------------------|--|
| Server hostname/IP address | <input type="text"/><br>The hostname or IP address the server will bind to. Leave empty for all. |
| Server port/service name   | <input type="text" value="10002"/><br>The TCP and UDP port number or service name to listen on.  |

### 11.1.1 Configurable parameters in standard mode

The **User description** text field can be used to rename the service in configuration menus to something more indicative of its function. Likewise, the **User label** text field can be used to provide a shorter but still potentially more useful name for use in log files.

The **Enable** check-box, when ticked, causes this service to start automatically when the system is re-booted. If this check-box is cleared, the service will need to be started manually (from the “Control” → “Services” menu)

The **Delete** check-box, if ticked, causes the configuration for this instance to be removed from the system when the form is submitted.

The **Server hostname/IP address** text field can be used to restrict the server to listen for incoming connection requests only via particular network interfaces. If multiple interfaces or addresses are configured for this system, entering the IP address or associated hostname of one

of them prevents connection attempts made to all other addresses. If left blank, connection requests will be considered from all interfaces.

The **Server port/service name** field must be populated with the service name or port number on which it will listen for incoming connections. This must not be used by any other service on this system.

The next section of the form looks like this:

### Protocol parameters

|                 |   |
|-----------------|---|
| ACK/NAK timeout | <input type="text" value="150"/> ms<br>Time to wait for ACK/NAK before transmitting next block (milliseconds).          |
| Mode            | <div>Direct - simple transmission with link error correction but no backfill ▾</div> <div>Block transmission mode</div> |

### Output filtering

This section allows you to choose whether to transmit all GCF blocks as they are received from the GCF convertor, or only a subset.

|   |  |
|---|--|
| Output type   | <div>All blocks ▾</div> <div>Select which types of block to transmit</div>   |
| Max sample rate   | <div><input type="text"/> samples per second</div> <div>If filtering by sample rate, the maximum sample rate to send</div> |
| If filtering by channel name, the channels to be transmitted should be entered below. The exact name of the channel must be given, in the format SYSID-STRID. |  |

The **ACK/NAK timeout** text field should be populated with an integer value which specifies the number of milliseconds the server should wait for an acknowledgement packet before transmitting the next block.

The **Mode** drop-down menu controls the BRP transmission mode of the server. At present, the only available choice is “Direct - simple transmission with link error correction but no backfill”. Future implementations will offer additional options.

The “Output filtering” section allows the operator to control which data are transmitted, selecting by block type, sample rate or channel name.

The **Output type** drop-down menu offers a choice of:

- “All blocks” - filtering by block type is disabled;
- “Only status blocks” - no data blocks are transmitted;

- “Only blocks below a certain sample rate” - the threshold sample rate is specified in the following text field; and
- “Only blocks matching a list of channel names” - offering the highest granularity of control.

If the previous field is set to “Only blocks below a certain sample rate”, the **Max sample rate** text field is used to specify the threshold, above which data are not transmitted.

If the **Output type** field is set to “Only blocks matching a list of channel names”, the channel names must be specified in the following table:

| Channel name         | Delete                   |
|----------------------|--------------------------|
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |

---

*Generated at 1970-01-07T15:33:37Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

Channel should be specified by giving their system ID and their stream ID, separated by a hyphen ('-'). Existing entries may be deleted by ticking the associated check-box and submitting the form. If the form is submitted when the table is full, extra blank lines are appended.

### **11.1.2 Configurable parameters in expert mode**

---

The following additional configuration parameters are available by clicking the “Expert” button at the bottom of the form.

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

### Expert options

|   |  |
|---|--|
| Log file  | <input type="text"/><br>Path to log file. Leave blank to use syslog.                         |
| Log level   | Important notices ▼<br>Minimum severity level of messages to record in log.                  |
| Audit log size  | 256KiB (medium) ▼  |
| GCF convertor   | GCF compressor. Default instance ▼<br>Select which GCF convertor instance to send data from. |
| State directory   | /var/lib/gcf-out-brp.0<br>Directory in which application state is stored.                    |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Simple"/> <input type="button" value="Submit"/> |  |

*Generated at 1970-01-07T15:37:50Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

The GCF BRP sender keeps its own audit log, independent from the system log. The contents of this log are available using the “GCF Audit Log viewer” facility as described in section 13.3.2 on page 182. The amount of data retained is controlled by the **Audit log size** drop-down menu, whose choices are:

- 64Kib (small);
- 256Kib (medium);
- 2MiB (large); and
- 16MiB (huge).

It is possible to copy all incoming data, verbatim, to a network port, which can be specified in the **Debug port** text field. This is an advanced debugging technique which is beyond the scope of this manual.

In most configurations, all data for all transmitters is taken from a single multiplexor, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to

select a multiplexer instance with which to associate this transmitter. The menu offers a list of currently configured multiplexers.

The GCF BRP protocol requires the transmitter to store some state information. By default, this is held in the directory `/var/lib/gcf-out-brp.n` where *n* is the instance number (counting from zero for the first instance). The **State directory** text field can be used to cause this information to be stored elsewhere: typically on another device. This may be useful for managing storage utilisation in complex configurations.

## 11.2 GCF Scream Server

---

The GCF Scream network server transmits Guralp Compressed Format (GCF) data in the native Scream! protocol over an Ethernet network.

To configure a GCF Scream network server from the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a GCF Scream network server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “gcf-out-scream” from the System Services menu. The next screen shows a list of all GCF Scream server instances that have been configured:

[Home](#) – [Configuration](#) – [Services](#) → [gcf-out-scream](#)

---

### GCF Scream network server instance selection

Select the GCF Scream network server instance you wish to configure:

- [Scream server \(GCF network sender\) - starts automatically](#)
- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-07T15:41:05Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

You can reconfigure any existing service by clicking on its menu entry. To configure a new GCF Scream server instance, select “Create new service instance”. The following screen allows you to configure the parameters of the service. It is a large form and is shown here in parts.

### 11.2.1 Configurable parameters in standard mode

[Home](#) → [Configuration](#) → [Services](#) → [gcf-out-scream](#) → [default](#)

#### Scream server configuration

|                            |   |
|----------------------------|---|
| User description           | <input type="text" value="Scream server (GCF network sender)"/><br>User label for this Scream server instance |
| Server hostname/IP address | <input type="text"/><br>The hostname or IP address the server socket will bind to. Leave empty for all.       |
| Server port/service name   | <input type="text" value="scream"/><br>The TCP and UDP port number or service name to listen on.              |

#### Terminal mode

| Disable terminal access  | <input type="checkbox"/><br>Check this to disable terminal access through Scream clients. |                          |
|--|---|--------------------------|
| Use the table below to limit terminal access to certain hosts. See help. |   |                          |
| IP address and mask  | Reject  | Delete                   |
| <input type="text"/>   | <input type="checkbox"/>  | <input type="checkbox"/> |
| <input type="text"/>   | <input type="checkbox"/>  | <input type="checkbox"/> |
| <input type="text"/>   | <input type="checkbox"/>  | <input type="checkbox"/> |

The **User description** text field can be used to rename the service in configuration menus and log files to something more indicative of its function.

The first instance can neither be disabled nor deleted but, if subsequent instances are created, two additional check-boxes appear on their associated configuration menu:

The **Enable** check-box, when ticked, causes this service to start automatically when the system is re-booted. If this check-box is cleared, the service will need to be started manually (from the “Control” → “Services” menu)

The **Delete** check-box, if ticked, causes the configuration for this instance to be removed from the system when the form is submitted.

The **Server hostname/IP address** text field can be used to restrict the server to listen for incoming connection requests only via particular network interfaces. If multiple interfaces or addresses are configured for this system, entering the IP address or associated hostname of one

of them prevents connection attempts made to all other addresses. If left blank, connection requests will be considered from all interfaces.

The **Server port/service name** field must be populated with the service name or port number on which it will listen for incoming connections. This must not be used by any other service on this system.

The next section of the form looks like this:

### Push destinations

It is possible to push Scream packets over UDP to several destinations without needing a client to send a GCFSEND request. Additionally, it is possible to broadcast to a network, although the broadcast option is turned off by default to avoid misconfiguration.

| Host                 | Port                 | Delete                   |
|----------------------|----------------------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

Enable broadcast

☐  
Check this to enable pushing Scream packets to network broadcast addresses.

The scream server is capable of both responding to data requests from clients (PULL mode) and of sending data uninvited to remote destinations (PUSH mode). The table above is used to list any PUSH mode clients. For each, a **Host** must be specified as either an IP address or hostname and a **Port** must be given as either a service number or name. Existing entries can be deleted by ticking the associated **Delete** check-box and submitting the form.

By default, the server will not send to network broadcast addresses. This behaviour can be enabled by ticking the **Enable broadcast** check-box.

The “Output filtering” section allows the operator to control which data are transmitted, selecting by block type, sample rate or channel name.

### Output filtering

This section allows you to choose whether to transmit all GCF blocks as they are received from the GCF convertor, or only a subset.

|  |  |
|--|--|
| Output type  | <div>All blocks</div> <div>Select which types of block to transmit</div>                       |
| Max sample rate  | <div></div> samples per second<br>If filtering by sample rate, the maximum sample rate to send |
| If filtering by channel name, the channels to be transmitted should be entered into the table below. The exact name of the channel must be given, in the format SYSID-STRID. |  |

The **Output type** drop-down menu offers a choice of:

- “All blocks” - filtering by block type is disabled;
- “Only status blocks” - no data blocks are transmitted;
- “Only blocks below a certain sample rate” - the threshold sample rate is specified in the following text field; and
- “Only blocks matching a list of channel names” - offering the highest granularity of control.

If the previous field is set to “Only blocks below a certain sample rate”, the **Max sample rate** text field is used to specify the threshold, above which data are not transmitted.

If the **Output type** field is set to “Only blocks matching a list of channel names”, the channel names must be specified in the following table:

| Channel name | Delete |
|--------------|--------|
| <div></div>  |        |
| <div></div>  |        |
| <div></div>  |        |
| <div></div>  |        |
| <div></div>  |        |
| <div></div>  |        |

Home

Help

Expert

Submit

---

*Generated at 1970-01-07T15:42:27Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*



## 11.2.2 Configurable parameters in expert mode

The following additional configuration parameters are available by clicking the “Expert” button at the bottom of the form.

### Advanced options

|                |   |
|----------------|---|
| V4.0 COM names | <input checked="" type="checkbox"/><br>Check this to use old V4.0 COMxx port names. Uncheck for meaningful names. |
| Node name      | <input type="text"/><br>The node name used in the block description field. Leave blank for hostname               |
| Log file       | <input type="text"/><br>Path to log file. Leave blank to use syslog.  |
| Log level      | Important notices ▾<br>Minimum severity level of messages to record in log.                                       |
| Audit log size | 256KiB (medium) ▾   |
| GCF convertor  | GCF compressor. Default instance ▾<br>Select which GCF convertor instance to send data from.                      |

[Home](#)
[Help](#)
[Simple](#)
[Submit](#)

Generated at 1970-01-07T15:53:18Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

Early versions of the Scream protocol expected all data to originate from COM ports and the port number was used to identify data sources. Version 5 and above of the protocol allow for a much more flexible naming scheme. The **V4.0 COM names** check-box can be cleared to enable advanced naming or ticked to retain compatibility with earlier versions of the protocol.

The protocol includes a description field identifying the source of each block. By default, this is set to the host name of the originating machine but it can be over-ridden by entering a value in the **Node name** text field.

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;

- Informational messages;
- Important notices; or
- Warnings

The GCF Scream sender keeps its own audit log, independent from the system log. The contents of this log are available using the “GCF Audit Log viewer” facility as described in section 13.3.2 on page 182. The amount of data retained is controlled by the **Audit log size** drop-down menu, whose choices are:

- 64Kib (small);
- 256Kib (medium);
- 2MiB (large); and
- 16MiB (huge).

In most configurations, all data for all transmitters is taken from a single multiplexor, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this transmitter. The menu offers a list of currently configured multiplexers.

## 11.3 SEEDlink

---

The Standard for the Exchange of Earthquake Data (SEED) is an international standard format for the exchange of digital seismological data developed by the USGS and adopted as a standard by the Federation of Digital Broad-Band Seismograph Networks (FDSN). MiniSEED data is a stripped-down version of SEED data which only contains waveform data, without the station and channel metadata that are included in full SEED.

Incoming data in any format other than CD1.1 is converted first into GDI format. In order to transmit SEEDlink data or record it to disk, it must be converted into miniSEED format and this is done by the `gdi2miniseed` module, known as the GDI Mini-SEED compressor.

### 11.3.1 The GDI Mini-SEED compressor

---

A default instance of the GDI Mini-SEED compressor is provided. Further instances can be created if required for complex implementations. Although the default instance is not set to start automatically, it is a necessary prerequisite for both SEEDlink transmission and recording, so it will be started as a dependant service when required.

To configure a GDI Mini-SEED compressor from the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a GDI Mini-SEED compressor from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “gdi2miniseed -- Mini-SEED compressor” from the System Services menu. The next screen shows a list of all Mini-SEED compressor instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [gdi2miniseed](#)

## Mini-SEED compressor instance selection

Select the Mini-SEED compressor instance you wish to configure:

- [Mini-SEED compressor. Default instance - does not start automatically](#)
- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 1970-01-06T02:36:01Z by gcs 2.0.3. Portions of output copyright (c)1970, Guralp Systems Limited.

Although the default instance is marked as “does not start automatically”, it will be started if a dependant service is started.

You can reconfigure any existing compressor by clicking on its menu entry. To configure a new Mini-SEED compressor instance, select “Create new service instance”. The following screen allows you to configure the parameters of the compressor. The first part of the screen looks like this:

[Home](#) → [Configuration](#) → [Services](#) → [gdi2miniseed](#) → [default](#)

## GDI Mini-SEED compressor

`gdi2miniseed` converts samples acquired through the system into Mini-SEED (Data only SEED) blocks suitable for use with other 3rd party software. Compressed blocks are written into a ring buffer for recording, transmission and backfill.

|                  |   |
|------------------|---|
| User description | Mini-SEED compressor. Default instance<br>User label for this Mini-SEED compressor instance |
| Enable           | <input type="checkbox"/><br>Enable the compressor at system startup                         |
| Buffer size      | <input type="text" value="64"/> MiB<br>Ring buffer size in MiB                              |
| Block size       | <input type="text" value="512 bytes"/><br>Size of the mini-SEED data block recorded         |

The name of the compressor can be set to a meaningful name for the data that it will handle by populating the **User description** text field. The server can be enabled or disabled at boot-up using the **Enable** check-box.

Data converted by the compressor are written to a ring-buffer which is read by both the miniSeed recorder and the SEEDlink transmitter. The size of this buffer can be set using the **Buffer size** text entry field, which accepts an integer number of mebibytes.

The SEED block size is set in the compressor and can not be changed by subsequent software modules. This has the important implication that, if data are to be transmitted using the SEEDlink server, this parameter *must* be set to 512 bytes. The size is controlled by the **Block size** drop-down menu and the possible choices range from 256 bytes to 8K bytes, doubling at each step. The default value is 4K bytes: this is chosen as the optimal for disk recording.

The rest of the compressor configuration screen concerns channel name mapping.

## Channels

Select which channels to compress. See help for more details.

| Naming mode   |                   |                          |
|---|-------------------|--------------------------|
| Automatic - all channels are compressed and named automatically |                   |                          |
| Select how channels are selected for compression and named      |                   |                          |
| System name   | SEED channel name | Delete                   |
| LW-DDDD00   | DDDD.SOH.LW.00    | <input type="checkbox"/> |
| LW-DDDD1B   | DDDD.AIB.LW.0B    | <input type="checkbox"/> |
| LW-EEEE1B   | EEEE.AIB.LW.0B    | <input type="checkbox"/> |
| LW-DDDDE4   | DDDD.HHE.LW.04    | <input type="checkbox"/> |

The **Naming mode** drop-down menu offers three choices:

- “Automatic - all channels are compressed and named automatically”. This mode offers no filtering and provides system-generated names for each channel forwarded by **gdi-base**.
- “Semi-automatic - all channels are compressed, names may be mapped below”. In this mode, one or more of the channels may be renamed by adding entries to the mapping table. If you wish to use this mode, it may be useful first to run the system in automatic mode for a short while: this will populate the mapping table with an entry for each currently

known channel, which can serve as the basis for your own mapping table.

- “Manual - only channels named below are compressed”. This mode offers both channel filtering and name mapping. If you wish to use this mode, it may be useful first to run the system in automatic mode for a short while: this will populate the mapping table with an entry for each currently known channel, which can serve as the basis for your own mapping table.

Entries from the mapping table can be deleted by ticking their associated check-box and submitting the form.

Additional configuration parameters are available in expert mode:

|                    |  |
|--------------------|--|
| Database directory | <input type="text" value="/var/lib/gdi2miniseed.default"/><br>Path in which database and control files are placed. Must be unique                            |
| Log file           | <input type="text"/><br>Path to log file. Leave blank to use syslog.   |
| Log level          | <input type="button" value="Important notices"/> <input type="button" value="v"/><br>Minimum severity level of messages to record in log.                    |
| GDI multiplexor    | <input type="button" value="Default data transport daemon"/> <input type="button" value="v"/><br>Select which GDI multiplexor instance to compress data from |

*Generated at 1970-01-06T03:02:02Z by gcs 2.0.3. Portions of output copyright (c)1970, Guralp Systems Limited.*

The **Database directory** field can be used to control the location of the ring-buffer and associated files. In most configurations, the default location is adequate but if, for example, a very large ring-buffer is desired and the optional extra flash memory module is fitted, it may be desirable to use the extra memory for this purpose. To do this, enter into this field the path to a unique directory under `/media/flash_module`.

It may sometimes be desirable, for debugging purposes, to separate log messages for this compressor from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

In most configurations, all data for all compressors are taken from a single multiplexer, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this compressor. The menu offers a list of currently configured multiplexers.

### 11.3.2 The SEEDlink server

---

The SEEDlink server transmits data in miniSEED format (data only, no station and channel metadata) over the network to remote data consumers. The data are generated by a GDI Mini-SEED compressor instance.

**Note:** The SEEDlink server requires data in 512 byte blocks - the compressor must be reconfigured from its default setting (4 Kbytes) if the SEEDlink server is to be used: see the previous section for details.

A single SEEDlink server instance takes data from a single compressor instance and can serve multiple, simultaneous clients. If it is required to serve different channels to different clients, multiple server instances should be configured, each receiving data from a different compressor instance (the channel selection is controlled by the compressor, not the server). A server has a configured “Organization” name: if data are to appear to come from multiple organizations, multiple server instances should be configured: they can share a compressor instance if they will be serving the same channels or a number of compressor instances can be used.

To configure a SEEDlink server from the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a SEEDlink server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “seedlink-out -- SEEDlink network server” from the System Services menu. The next screen shows a list of all SEEDlink server instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [seedlink-out](#)

## SEEDlink network server instance selection

Select the SEEDlink network server instance you wish to configure:

- [SEEDlink network server \(instance 1\) - starts automatically](#)
- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 1970-01-06T03:28:38Z by gcs 2.0.3. Portions of output copyright (c)1970, Guralp Systems Limited.

You can reconfigure any existing service by clicking on its menu entry. To configure a new SEEDlink server, select “Create service instance”. The following screen allows you to configure the parameters of the server.

[Home](#) → [Configuration](#) → [Services](#) → [seedlink-out](#) → [0](#)

## SEEDlink server configuration

|                            |   |
|----------------------------|---|
| User description           | <input type="text" value="SEEDlink network server (instance 1)"/><br>User label for this SEEDlink server instance |
| Enable                     | <input checked="" type="checkbox"/><br>Enable this SEEDlink server at system startup                              |
| Delete                     | <input type="checkbox"/><br>Delete this SEEDlink server instance  |
| Server hostname/IP address | <input type="text"/><br>The hostname or IP address to listen on. Leave empty for all.                             |
| Server port/service name   | <input type="text" value="seedlink"/><br>The TCP port number or service name to listen on.                        |
| Organization               | <input type="text"/><br>Name of organization (if blank Guralp Systems Ltd will be used)                           |

[Home](#) [Help](#) [Expert](#) [Submit](#)

Generated at 1970-01-06T03:30:33Z by gcs 2.0.3. Portions of output copyright (c)1970, Guralp Systems Limited.

The name of the server should be set to a meaningful name for the data that it will serve by populating the **User description** text field.

The server can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely by selecting the **Delete** check-box.

To configure the server to listen for incoming data requests only on a specific IP address, set this (or the associated host name) in the **Bind host** text field. By default it will listen on all configured interfaces.

Set the port (port number or service name) that you want the server to listen on in the **Service Port** text field.

The server identifies itself to clients with an organization name: this should be entered into the **Organization** text-field. If left blank, the value will default to “Guralp Systems Ltd”.

Additional configuration parameters are available in expert mode:

### Advanced options

|                                    |   |
|------------------------------------|---|
| Log file                           | <input type="text"/><br>Path to log file. Leave blank to use syslog.  |
| Log level                          | <div>Important notices ▾</div><br>Minimum severity level of messages to record in log.                              |
| Mini-SEED convertor                | <div>Mini-SEED compressor. Default instance ▾</div><br>Select which Mini-SEED convertor instance to send data from. |
| <div>Home Help Simple Submit</div> |   |

*Generated at 1970-01-06T03:34:05Z by gcs 2.0.3. Portions of output copyright (c)1970, Guralp Systems Limited.*

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

In the default configuration, all data for all servers is taken from a single compressor, as described at the beginning of this section. For more complex configurations, it is possible to configure multiple compressors, each with their own multiplexor input and set of output servers. In these situations, the **Mini-SEED convertor** drop-down menu can be used to select a compressor instance with which to associate this server. The menu offers a list of currently configured compressors.



## 11.4 Guralp Seismic Monitoring System

GSMS is a protocol designed by Guralp Systems to send real time, low latency strong motion data.

To configure a GSMS server from the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a GSMS server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “gsms-out -- GSMS sender” from the System Services menu. The next screen shows a list of all GCF Scream server instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [gsms-out](#)

### GSMS sender instance selection

- [Create new service instance](#)

Home Help Expert Submit

*Generated at 1970-01-07T18:02:13Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

You can reconfigure any existing service by clicking on its menu entry. To configure a new GSMS server, select “Create service instance”. The following screen allows you to configure the parameters of the server.

#### 11.4.1 Configurable parameters in standard mode

The name of the server should be set to a meaningful name for the data that it will serve by populating the **User description** text field. The optional **User Label** text field can be filled in with a name which will then be used to identify this instance in log files.

The server can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely by selecting the **Delete** check-box.

To configure the server to listen for incoming data requests only on a specific IP address, set this (or the associated host name) in the **Bind host** text field. By default it will listen on all configured interfaces.

Set the port (port number or service name) that you want the server to listen on in the **Service Port** text field.

# GSMS sender configuration

|                  |  |
|------------------|--|
| User description | <input type="text" value="GSMS sender (instance 1)"/><br>User label for the transmitter instance |
| User label       | <input type="text"/><br>Application label used for identification in logs                        |
| Enable           | <input type="checkbox"/><br>Enable the transmitter at system startup                             |
| Delete           | <input type="checkbox"/><br>Delete this transmitter instance                                     |

## Network parameters

|              |  |
|--------------|--|
| Bind host    | <input type="text"/><br>The hostname or IP address the server will bind to. Leave empty for all. |
| Service port | <input type="text" value="9001"/><br>The TCP and UDP port number or service name to listen on.   |

If you want the server to pro-actively send data to remote GSMS receivers, enter their IP addresses (or host names) in the **Push host** column and port numbers (or service names) in the **Service** column of the “Push hosts” table. For each, select TCP or UDP from the **Protocol** drop-down menu - this must match the receiver's setting.

## Push hosts

| Protocol | Push host            | Service              | Delete |
|----------|----------------------|----------------------|--------|
| UDP ▾    | <input type="text"/> | <input type="text"/> |        |
| UDP ▾    | <input type="text"/> | <input type="text"/> |        |
| UDP ▾    | <input type="text"/> | <input type="text"/> |        |


The GSMS server need not send all data from all channels to its clients: it is possible to select which channels are transmitted. Select one of the three different transmission modes:

- Automatic: all channels are transmitted and named automatically
- Semi-automatic: all channels are transmitted and names can be mapped using a configuration table
- Manual: only channels named in the configuration table are transmitted.

The relevant part of the screen (shown truncated) looks like this:

## Channels

Select which channels to transmit. See help for more details.

| Naming mode <span>Automatic - all channels are transmitted and named automatically</span> <br>Select how channels are selected for transmission and named |   |                          |
|--|---|--------------------------|
| System name  | Output channel name (SEED)                  | Delete                   |
| <input type="text" value="LW-DDDDE4"/>   | <input type="text" value="DDDD.HHE.LW.04"/> | <input type="checkbox"/> |
| <input type="text" value="LW-EEEEZ4"/>   | <input type="text" value="EEEE.HHZ.LW.04"/> | <input type="checkbox"/> |
| <input type="text" value="LW-EEEEE4"/>   | <input type="text" value="EEEE.HHN.LW.04"/> | <input type="checkbox"/> |
| <input type="text"/>   | <input type="text"/>                        |                          |
| <span>Home</span> <span>Help</span> <span>Expert</span> <span>Submit</span>  |   |                          |



Generated at 1970-01-07T18:04:33Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

The software will attempt to populate the table based on incoming data streams so it is a good idea to configure all input sources and run the system for a few minutes before completing this table.

### 11.4.2 Configurable parameters in expert mode

The following additional configuration parameters are available by clicking the “Expert” button at the bottom of the form.

#### Expert options

|   |  |
|---|--|
| Log file  | <input type="text"/><br>Path to log file. Leave blank to use syslog.   |
| Log level   | <span>Important notices</span> <br>Minimum severity level of messages to record in log.         |
| GDI multiplexor   | <span>Default data transport daemon</span> <br>Select which GDI multiplexor to gather data from |
| <span>Home</span> <span>Help</span> <span>Simple</span> <span>Submit</span> |  |

Generated at 1970-01-07T18:29:57Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

In most configurations, all data for all transmitters is taken from a single multiplexor, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this transmitter. The menu offers a list of currently configured multiplexers.

## 11.5 Quick Seismic Characteristic Data

---

QSCD is a protocol developed by KIGAM (<http://www.kigam.re.kr/eng>) to send strong motion results, which are computed every second.

To set up a QSCD server on the CMG-EAM, first configure the relevant strong motion data sources as described in section 7 on page 78, then, from the web interface, select “System services” from the “Configuration” → “All options” menu *or* select the “Services” shortcut from the “Data transfer/recording” menu. To configure a QSCD server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “qscd-out -- KIGAM QSCD (Quick Seismic Characteristic Data) sender ” from the System Services menu. The next screen shows a list of all QSCD server instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [qscd-out](#)

---

### KIGAM QSCD (Quick Seismic Characteristic Data) sender instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-07T20:20:48Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

You can reconfigure any existing service by clicking on its menu entry. To configure a new QSCD server, select “Create service instance”. The following screen allows you to configure the parameters of the server. As it is a large screen, it is shown here in pieces.

### 11.5.1 Configurable parameters in standard mode

[Home](#) → [Configuration](#) → [Services](#) → [qscd-out](#) → [0](#)

#### QSCD sender configuration

|                  |  |
|------------------|--|
| User description | KIGAM QSCD (Quick Seismic Characteristic Data) sender (instar<br>User label for the transmitter instance |
| Enable           | <input type="checkbox"/><br>Enable the transmitter at system startup                                     |
| Delete           | <input type="checkbox"/><br>Delete this transmitter instance   |

The **User description** of the server should be set to a meaningful name for the data that it will serve.

The server can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely by selecting the **Delete** check-box.

#### Network parameters

| Station name         | DCM10<br>5 letter SEED like station name to identify transmission |                          |
|----------------------|---|--------------------------|
| Push host            | Service   | Delete                   |
| <input type="text"/> | <input type="text"/>  | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/>  | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/>  | <input type="checkbox"/> |

Like SEED, QSCD links require a unique name to identify the source of the data. This should be entered into the **Station name** field, under “Network parameters”.

To send QSCD data to remote hosts, enter their DNS names or IP addresses in the table, with the associated service name or port number for each. Port names and numbers are associated with each other in the standard Linux `/etc/services` file.

## Strong motion data channels

Select the instrument being used for QSCD packets here. The instrument must be a CMG-DM24mk3 set up for strong motion mode (including SI output).

Instruments which seem to be configured for strong motion:

GSL-2010  
GSL-2011  
GSL-2012

|   |                      |        |        |
|---|----------------------|--------|--------|
| Instrument  | <input type="text"/> |        |        |
| Enter instrument name (SYSID-SER) here. Omit last two digits from channel name. |                      |        |        |
| Home  | Help                 | Expert | Submit |

---

*Generated at 1970-01-07T20:22:04Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

The CMG-EAM scans all incoming data and prepares a list, in the correct format, of the names of instruments which are sending strong motion results. Enter one of these names in the **Instrument** field.

The QSCD protocol only supports a single instrument. If you need to transmit results from multiple instruments, you should configure multiple QSCD sender instances, one for each instrument.

### 11.5.2 Configurable parameters in expert mode

---

The following additional configuration parameters are available by clicking the “Expert” button at the bottom of the form.

#### Expert options

|  |                                 |        |        |
|--|---------------------------------|--------|--------|
| Log file   | <input type="text"/>            |        |        |
| Path to log file. Leave blank to use syslog.         |                                 |        |        |
| Log level  | Important notices ▼             |        |        |
| Minimum severity level of messages to record in log. |                                 |        |        |
| GDI multiplexor                                      | Default data transport daemon ▼ |        |        |
| Select which GDI multiplexor to gather data from     |                                 |        |        |
| Home   | Help                            | Simple | Submit |

---

*Generated at 1970-01-07T20:33:32Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the

standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

In most configurations, all data for all transmitters is taken from a single multiplexor, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexer** drop-down menu can be used to select a multiplexer instance with which to associate this transmitter. The menu offers a list of currently configured multiplexers.

## 11.6 WIN Sender

---

WIN is a Japanese seismic data format.

To set up a WIN server on the CMG-EAM using the web interface, select “System services” from the “Configuration” → “All options” menu **or** select the “Services” short-cut from the “Data transfer/recording” menu. To configure a WIN server from the command line, start `gconfig` and select “System services” from the top level menu.

Now select “win-out -- WIN sender ” from the System Services menu. The next screen shows a list of all WIN server instances that have been configured:

[Home](#) → [Configuration](#) → [Services](#) → [win-out](#)

---

### WIN sender instance selection

- [Create new service instance](#)

---

*Generated at 1970-01-07T20:37:03Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

You can reconfigure any existing service by clicking on its menu entry. To configure a new WIN sender, select “Create service instance”. The following screen allows you to configure the parameters of the sender. It is shown here in parts.



### 11.6.1 Configurable parameters in standard mode

[Home](#) → [Configuration](#) → [Services](#) → [win-out](#) → 0

#### WIN format transmitter configuration

|                  |   |
|------------------|---|
| User description | <input type="text" value="WIN sender (instance 1)"/><br>User label for the service instance |
| User label       | <input type="text"/><br>Application label used for identification in logs                   |
| Enable           | <input type="checkbox"/><br>Enable the transmitter at system startup                        |
| Delete           | <input type="checkbox"/><br>Delete this transmitter instance                                |

The **User description** of the service should be set to a meaningful name for the data that it will send. The **User label** can be set to distinguish this instance from others in the log files. The sender can be enabled or disabled at boot-up using the **Enable** check-box or deleted entirely by selecting the **Delete** check-box.

The WIN transmitter can be configured to be either a TCP server to multiple clients, or a UDP sender to a single address. If you want to sent the data to multiple clients, set up the CMG-EAM as a TCP server and the remote machines as clients that connect to it.

#### Network parameters

|                     |  |
|---------------------|--|
| Protocol            | <input type="text" value="TCP server accepting multiple clients"/><br>Set the protocol used for transmission |
| Hostname            | <input type="text"/><br>Hostname or IP address to use  |
| Service             | <input type="text" value="9999"/><br>Service or port number to use   |
| Max delay           | <input type="text" value="5"/><br>Maximum delay before data is transmitted (seconds)                         |
| Early transmit size | <input type="text" value="450"/><br>Packets exceeding this size may be transmitted early                     |
| UTC offset          | <input type="text" value="+9 hours (JST)"/><br>Hour offset from UTC to apply to timestamps                   |

To configure the sender as a TCP server, select “TCP server accepting multiple clients” from the **Protocol** drop-down list. To use a specific IP address to listen for requests from clients, set this in the **Hostname** box. By default it will listen on all interfaces. Set the port that you want the server to listen on in the **Service** box.



If you only want to send the data to a single UDP server, select “UDP datagrams sent to specified address” from the **Protocol** drop-down list. Configure the remote machine's hostname or IP address in the **Hostname** box and set the port number that the remote machine will listen on in the **Service** box.

The WIN sender will buffer up data before it is sent so that outgoing packets have a second's worth of data from all channels. If no data is received from some channels within a certain time limit, the data from other channels will be transmitted anyway. This limit is specified by the value in the **Max delay** field and defaults to five seconds. If a packet in construction exceeds the size specified by **Early transmit size** this packet will also be sent early.

The WIN Format uses the local time in order to time-stamp packets. The offset of the local time-zone from UTC used in the GCF data is specified in the **UTC Offset** box.

The final table specifies the mapping from GDI channel names to WIN channel numbers.

**Note:** Previous versions of the firmware required this mapping to be entered in SEED notation but this is no longer the case.

## Channels

| GDI channel name                       | WIN channel number   | Delete                   |
|--|----------------------|--------------------------|
| <input type="text" value="LW-DDDD00"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text" value="LW-DDDDE4"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text" value="LW-DDDDM8"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/>                   | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/>                   | <input type="text"/> | <input type="checkbox"/> |

*Generated at 1970-01-07T20:38:16Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

If the form is submitted when the table is full, extra blank rows will be added when the form is redrawn. Existing entries in this table can be deleted by ticking the **Delete** check-box and submitting the form.

### 11.6.2 Configurable parameters in expert mode

The following additional configuration parameters are available by clicking the “Expert” button at the bottom of the form.

#### Expert options

|  |  |
|--|--|
| Log file                                 | <input type="text"/><br>Path to log file. Leave blank to use syslog.                                   |
| Log level                                | <div>Important notices ▾</div> <div>Minimum severity level of messages to record in log.</div>         |
| GDI multiplexor                          | <div>Default data transport daemon ▾</div> <div>Select which GDI multiplexor to gather data from</div> |
| <div>Home   Help   Simple   Submit</div> |  |

---

*Generated at 1970-01-07T20:43:43Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

It may sometimes be desirable, for debugging purposes, to separate log messages for this transmitter from the standard system log. The **Log file** text field can be populated with a path name which will then be used for dedicated logging. If left blank, logging occurs (via the standard Linux syslog facility) to `/var/log/messages`.

The **Log level** drop-down menu controls the level of detail present in log messages, whether to syslog or to a dedicated log file. Not all of the standard syslog logging levels are available. The menu offers a choice (in order of decreasing detail) of:

- Debugging information;
- Informational messages;
- Important notices; or
- Warnings

In most configurations, all data for all transmitters is taken from a single multiplexor, as described in section 1.3 on page 10. For more complex configurations, it is possible to configure multiple multiplexers, each with their own set of input and output services. In these situations, the **GDI multiplexor** drop-down menu can be used to select a multiplexer instance with which to associate this transmitter. The menu offers a list of currently configured multiplexers.

## 12 Building Networks

### 12.1 GDI-link

The GDI-link protocol provides the most efficient means of exchanging data between two systems running Platinum firmware. GDI is the native data format of the central data multiplexer, the `gdi-base` module, and GDI-link allows highly efficient, low latency data exchange between two such multiplexers without the overhead of any additional protocol conversion. State of health information is attached to samples before transmission.

GDI links have transmitters, which send data, and receivers which receive it. These terms do not refer to the direction of initiation of the network connection: a receiver can initiate a connection to a transmitter and vice versa.

A single GDI-link receiver can accept data from multiple transmitters and a single transmitter can send data to multiple receivers, allowing maximum flexibility in configuring seismic networks.

#### 12.1.1 The GDI-link transmitter

To configure a GDI-link transmitter, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using `gconfig` from the command line interface. From the main screen select “services”, then “GDI link transmitter”. The next screen shows a list of all GDI link transmitter instances that have been configured on the CMG-EAM.

[Home](#) → [Configuration](#) → [Services](#) → [gdi-link-tx](#)

### GDI link transmitter instance selection

Select the GDI link transmitter instance you wish to configure:

- [System gdi-link transmitter - starts automatically](#)
- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

*Generated at 1970-01-06T20:04:37Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

In most circumstances you will only need a single GDI link transmitter but this screen allows you to create more if desired.

To configure the transmitter, click on the link corresponding to the required instance. You will see the following screen (only the top part of which is shown here):

[Home](#) → [Configuration](#) → [Services](#) → [gdi-link-tx](#) → [default](#)

---

## GDI Link Transmitter

gdi-link-tx transmits samples in the native protocol of the Platinum software suite, called Guralp Data Interconnect. This is a low-latency real-time transmission protocol which sends encoded state of health with samples.

|                  |  |
|------------------|--|
| User description | <div>System gdi-link transmitter</div> <div>User label for this transmitter module</div> |
|------------------|--|

### Network settings

|                    |   |
|--------------------|---|
| Client name        | <div></div> <div>Used to identify this transmitter to other receivers. Leave empty for default.</div> |
| Local IP address   | <div></div> <div>IP address or host name to listen on. Leave empty for default.</div>                 |
| Local port/service | <div></div> <div>Service name or TCP port number to listen on. Leave empty for default.</div>         |

The description of the instance can be changed if desired. This may be useful if you have multiple instances. This description is seen when viewing running services or configuring instances. It is not seen by the clients.

Subsequent instances can be enabled or disabled with a check-box but this is absent from the page for the default instance because the default instance is always enabled.

The instance name, as seen by the client, can be set in the first field under “Network settings”. A suitable default is used if this field is left blank.

If the CMG-EAM has multiple network addresses, it can be restricted to listen for incoming connections on only one of them by entering its address here. If left blank, the transmitter will listen on all available instances.

The default service (port) for the transmitter is 1565 but an alternative port can be entered here if required.

Backfill is the process whereby missing data is recovered. It can be

## Backfill

By default, backfill is disabled. Be sure to enable it if required, and to set up an associated directory cleaner task to manage buffer space.

|                 |   |
|-----------------|---|
| Enable backfill | <input type="checkbox"/>  |
| Directory       | <input type="text" value="/var/lib/gdi-link-tx.default"/><br>Directory under which backfill files are stored. |

disabled if desired but, in most cases, you should leave this enabled.

The remainder of the screen contains a table within which you can configure the GDI link clients to which this transmitter should send data.

## Push destinations

| Peer name            | Remote host          | Remote service/port  | Enable at startup        | Delete |
|----------------------|----------------------|----------------------|--------------------------|--------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |        |

Generated at 1970-01-06T20:06:12Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

For each client, you should set:

- the **Peer name**: this should match the server name configured on the
- the **Remote host**: this is the DNS name or IP address of the GDI link client
- the **Remote service/port**: the default is 1566 but, if you have configured a different port on the GDI link client, you should enter the same port here.
- **Enable at startup** - this check-box controls whether

### 12.1.1.1 Additional options available in expert mode

The following additional options appear when in Expert mode:

### Advanced options

|                                    |   |
|------------------------------------|---|
| Log file                           | <input type="text"/>  |
|                                    | Path to log file. Leave blank to use syslog.                |
| Log level                          | <div>Important notices ▾</div>                              |
|                                    | Minimum severity level of messages to record in log.        |
| GDI multiplexor                    | <div>Default data transport daemon ▾</div>                  |
|                                    | Select which GDI multiplexor instance to compress data from |
| <div>Home Help Simple Submit</div> |   |

Generated at 1970-01-06T20:12:46Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

When you have entered all the required information, press Submit.

### 12.1.2 The GDI link receiver

---

To configure a GDI link receiver, connect to the CMG-EAM configuration system via either the web interface (select “All options”) or by using gconfig from the command line interface. From the main screen select “services”, then “GDI link receiver”. The next screen shows a list of all GDI link receiver instances that have been configured on the CMG-EAM.

[Home](#) → [Configuration](#) → [Services](#) → [gdi-link-rx](#)

---

### GDI link receiver instance selection

Select the GDI link receiver instance you wish to configure:

- [System gdi-link receiver - does not start automatically](#)
- [Create new service instance](#)

Home Help Expert Submit

Generated at 1970-01-06T20:17:01Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

In most cases, you will only need a single instance and you can enable and reconfigure the Default Instance for your requirements.

Clicking on the Default Instance link brings up the screen shown overleaf.

You can enter a descriptive name for the instance: this is useful if you are configuring multiple instances but, in most cases, this can be set to the hostname of the CMG-EAM.

The Network Settings section allows you to set an optional “client name” which will be visible from the GDI link server.

If the GSL-EAM has multiple network addresses, you can limit the GDI link receiver to use only one of them by entering it in the “Local IP address” field. If left blank, the receiver will listen on all configured addresses.

The default GDI link port is 1566 but this can be over-ridden if desired - you would want to do this if you had multiple instances running on the same address - by entering a port name or number in the “Local port/service” field.

[Home](#) → [Configuration](#) → [Services](#) → [gdi-link-rx](#) → [default](#)

## GDI Link Receiver

gdi-link-rx receives samples in the native protocol of the Platinum software suite, called Guralp Data Interconnect. This is a low-latency real-time transmission protocol which sends encoded state of health with samples.

|                  |   |
|------------------|---|
| User description | System gdi-link receiver<br>User label for this receiver module   |
| Enable           | <input type="checkbox"/><br>Enable the receiver at system startup |

## Network settings

|                    |  |
|--------------------|--|
| Client name        | <input type="text"/><br>Used to identify this receiver to other transmitters. Leave empty for default. |
| Local IP address   | <input type="text"/><br>IP address or host name to listen on. Leave empty for default.                 |
| Local port/service | <input type="text"/><br>Service name or TCP port number to listen on. Leave empty for default.         |

Backfill is the process whereby missing data is recovered. It can be disabled if desired but, in most cases, you should leave this enabled.

## Backfill

|                 |   |
|-----------------|---|
| Enable backfill | <input checked="" type="checkbox"/>   |
| Directory       | <input type="text" value="/var/lib/gdi-link-rx.default"/><br>Directory under which backfill state files are stored. |

The remainder of the screen contains a table within which you can configure the GDI link servers to which this receiver should listen.

## Servers

| Peer name | Remote host | Remote service/port | Enable at startup        | Channel filter                 |
|-----------|-------------|---------------------|--------------------------|--------------------------------|
| test      | 10.99.1.6   | gdi_link_tx         | <input type="checkbox"/> | No filter (receive everything) |
|           |             |                     | <input type="checkbox"/> | No filter (receive everything) |
|           |             |                     | <input type="checkbox"/> | No filter (receive everything) |
|           |             |                     | <input type="checkbox"/> | No filter (receive everything) |
|           |             |                     | <input type="checkbox"/> | No filter (receive everything) |
|           |             |                     | <input type="checkbox"/> | No filter (receive everything) |

[Home](#)
[Help](#)
[Expert](#)
[Submit](#)

Generated at 1970-01-06T20:18:15Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.

| Enable at startup        | Channel filter                   | Max sample rate | Channel names | Delete                   |
|--------------------------|----------------------------------|-----------------|---------------|--------------------------|
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 | D071-13292P   | <input type="checkbox"/> |
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 |               | <input type="checkbox"/> |
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 |               | <input type="checkbox"/> |
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 |               | <input type="checkbox"/> |
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 |               | <input type="checkbox"/> |
| <input type="checkbox"/> | No filter (receive everything) ▼ |                 |               | <input type="checkbox"/> |

Copyright (c)1970, Guralp Systems Limited.

For each server, you should set:

- the peer name: this should match the server name configured on the
- the remote host: this is the DNS name or IP address of the GDI link server
- the remote service/port: the default is 1565 but, if you have configured a different port on the GDI link server, you should enter the same port here.
- enable at start-up
- filtering: you can filter by sample rate or channel names



When you have entered all the required information, press Submit.

## 12.2 Guralp Secure TCP Multiplexer

---

The Guralp Secure TCP Multiplexer (GSTM) is a method by which TCP and UDP connections can be tunnelled in both directions over a single TCP connection. It is an essential tool in situations where local network service providers cannot provide fixed (static) IP addresses.

For example, in an installation involving a single, central data collection point and multiple, remote sensor sites it is sometimes impractical for the sensor sites to be allocated static IP addresses. Using GSTM allows the remote sites to initiate a single GSTM TCP connection to the central site. Once established, further TCP and UDP connections can be initiated in either direction: their packets are tunnelled over the GSTM link.

If no sites in an array can be assigned fixed IPs, including the central data collection point, a GSL-EAM or GSL-NAM can be installed anywhere that has a fixed IP address and used as a communications hub. All sites initiate GSTM connections to the hub, which can then act as a communications router, forwarding individual connections as required.

The initial link is established from a GSTM client to a GSTM server.

### 12.2.1 The GSTM Client

---

To set up a GSTM client on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “Guralp secure TCP multiplexor client”. The next screen shows a list of all GSTM client instances that have been configured on the CMG-EAM.

[Home](#) → [Configuration](#) → [Services](#) → [gstm-client](#)

---

### Guralp secure TCP multiplexor client instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-06T19:39:39Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

To configure a GSTM client, click “Create new service instance”. The resulting screen allows you to configure the parameters of the new instance.

[Home](#) → [Configuration](#) → [Services](#) → [gstm-client](#) → [0](#)

---

## Guralp secure TCP multiplexor client configuration

|                  |  |
|------------------|--|
| User description | <div>Guralp secure TCP multiplexor client (instance 1)</div> <div>User label for this GSTM client instance</div> |
| Enable           | <div><input type="checkbox"/></div> <div>Enable the GSTM client at system startup</div>                          |
| Delete           | <div><input type="checkbox"/></div> <div>Delete this GSTM client instance</div>                                  |

The “User description” field allows you to enter a mnemonic description of this instance, which may be useful if you intend to run multiple instances. The client can be set to start automatically when the CMG-EAM boots by clicking the “Enable” check-box, or deleted from the system entirely by clicking the “Delete” check-box.

## Server settings

|                |  |
|----------------|--|
| Server         | <div></div> <div>Hostname or IP address to connect to.</div>                             |
| Port/service   | <div>gstm</div> <div>TCP port number or service name to connect to.</div>                |
| Username       | <div>dcm105</div> <div>Name used to identify client to server.</div>                     |
| Encryption key | <div></div> <div>Pre-shared key used to encrypt communications. Must match server.</div> |

The client will automatically connect to a GSTM server who's DNS name or IP address is specified in the “Server” field, using a port who's service name or number is specified in the “Port/service” field. The client identifies itself to the server using a username: this can usefully be set to the hostname of the CMG-EAM.

**Note:** The username is the means by which the server refers to this client.

GSTM communication is encrypted using TLS. Each end of any GSTM link needs to be configured with the same pre-shared key. If the server has already been configured, the server administrator will

give you a value for the “Encryption Key” field; Otherwise, enter a random string into this field and let the person administering the server know what you have used.

## Link settings

|                          |   |
|--------------------------|---|
| Exit delay               | <input type="text" value="30"/><br>Number of seconds to wait on exit before restarting. |
| Watchdog interval        | <input type="text" value="30"/><br>Number of seconds between sending watchdog probes.   |
| Failover services        | <input type="text"/><br>Services to start when link fails.                              |
| Link established command | <input type="text"/><br>Command to issue when a good link is established.               |

*Generated at 1970-01-06T19:41:50Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

If the GSTM link fails for any reason, it is automatically restarted. There may be situations where the link cannot be restarted so, to prevent almost continuous restart attempts and consequent processor thrashing, a time delay is implemented between a link failure and a restart attempt. This defaults to thirty seconds but a different value can be configured if desired by entering it in the “Exit delay” field.

If a configured link carries no traffic for an extended period, the client will send “watchdog” packets to the server. This serves two functions: it reassures the client that the link is still usable and it defeats any “automatic disconnect on idle” mechanisms which may be active on some links. The time, in seconds, between such watchdog probes can be configured by entering a value in the “Watchdog interval” field.

If the watchdog packets do not elicit a response from the server, the link is assumed to have failed and, optionally, an additional service can be started in response. This will typically be another GSTM client in order to establish a back-up link. The GSTM client to be started should be identified here by its service descriptor, which takes the form `gstm-client.n` where *n* is an integer: 0 denotes the first configured client instance, 1 the second and so on.

When the GSTM link is established or re-established, it is possible to run an arbitrary command. Any text entered in the “Link established command” field is passed to the Linux shell for execution, so this can be a single command or the path to a shell script to execute multiple commands. Please contact Guralp support if you need assistance with this feature.

### 12.2.2 The GSTM Server

---

GSTM clients initiate connections to GSTM servers. To configure a GSTM server on the CMG-EAM, connect to the CMG-EAM configuration system via web or terminal. From the main screen select “Services”, then “Guralp secure TCP multiplexor server”. The next screen shows a list of all GSTM client instances that have been configured on the CMG-EAM.

[Home](#) → [Configuration](#) → [Services](#) → [gstm-server](#)

---

## Guralp secure TCP multiplexor server instance selection

- [Create new service instance](#)

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-06T19:46:12Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

This screen lists all currently configured server instances. Click on any server in the list to reconfigure it or, to create a new instance, click on “Create new service instance”.

The following screen appears (shown here in parts):

[Home](#) → [Configuration](#) → [Services](#) → [gstm-server](#) → [0](#)

---

## Guralp secure TCP multiplexor server configuration

|                  |  |
|------------------|--|
| User description | <input type="text" value="Guralp secure TCP multiplexor server (instance 1)"/><br>User label for this GSTM server instance |
| Enable           | <input type="checkbox"/><br>Enable the GSTM server at system startup   |
| Delete           | <input type="checkbox"/><br>Delete this GSTM server instance   |

The “User description” field is useful if several instances are to be created. Enter meaningful names here to help distinguish between them.

An instance can be set to start automatically when the CMG-EAM boots by ticking the “Enabled” check-box and deleted entirely by ticking the “Delete” check-box.

## Server settings

|                   |                                   |  |
|-------------------|-----------------------------------|--|
| Bind host         | <input type="text"/>              | The hostname or IP address the server will bind to. Leave empty for all. |
| Service port      | <input type="text" value="1599"/> | The TCP port number or service name to listen on.                        |
| TCP keepalive     | <input type="checkbox"/>          | Enable sending TCP keepalives (enabling the watchdog is preferred)       |
| Watchdog interval | <input type="text" value="30"/>   | Period in seconds between watchdog messages                              |

If the CMG-EAM has multiple IP addresses, the GSTM server can be constrained to listen on only one of them by entering its address in the “Bind host” field. If this field is left empty, the server will listen on all available IP addresses.

In the “Service port” field, enter the service name or port number on which you want the server instance to listen. If you are configuring multiple server instances, each needs a unique service/port. The service name to port number mapping is stored in the standard Linux file `/etc/services`, which can be edited from the command line.

The server is capable of generating TCP keep-alive packets in order to defeat any automatic “disconnect on idle” mechanisms which may be present on the link. Tick the “TCP keepalive” check-box to enable this feature.

Like the GSTM client, the GSTM server also generates watchdog packets to monitor for link failure. These may also be more effective at maintaining a link than TCP keep-alives because some network devices automatically block and/or spoof keep-alive packets. Watchdog packets are sent after a certain amount of time when the link appears to be idle and at regular intervals thereafter until traffic is detected. This time interval can be configured by entering an integer value, in seconds, in the “Watchdog interval” field.

## Client setting

| Client name          | Encryption key       | Startup command      | Delete                   |
|----------------------|----------------------|----------------------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

A single GSTM server instance can accept simultaneous connections from multiple clients. For each client, a row in the “Client setting” table needs to be filled in.

The “Client name” column should contain the username, as configured in the GSTM client. The encryption key should match that configured in the client (see the notes in the client configuration section on page 161 for more information).

The GSTM server can run an arbitrary command when a client successfully initiates communication. Any text entered into the “Startup command” column is passed to the Linux shell for execution. The path to a shell script can be entered here if it is required to run multiple commands. Contact Guralp support if you need assistance with this feature.

### Port forwards

| Listen address       | Listen service/port  | Target client        | Target service/port  | Delete |
|----------------------|----------------------|----------------------|----------------------|--------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |        |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |        |

[Home](#) [Help](#) [Expert](#) [Submit](#)

---

*Generated at 1970-01-06T19:47:39Z by gcs 2.0.0. Portions of output copyright (c)1970, Guralp Systems Limited.*

An active GSTM link can forward arbitrary TCP connections to the clients from any host that can access the server. The system is very flexible but complex configurations can become confusing. We suggest you adopt the following strategy:

1. Pick a private sub-network, not used elsewhere, to map to the clients. Nominate an address in this subnet to represent each client. For example, if you have seven clients, you could use addresses 10.99.0.1 through to 10.99.0.7 inclusive.
2. Configure all of these addresses as additional IP addresses on the sever. To do this, click on “Interfaces” under “Networking” in the “Configuration” section of the left-hand-side menu in the web interface or, if using the command line, choose “Networking” from the main menu in gconfig. Select the appropriate interface (typically eth0) and, on the resultant page, scroll to the bottom and click the “Expert” button.

Scroll down to the “IP aliasing” table and enter all of these addresses in CIDR format, one per line, into the table. CIDR format requires that the number of “network bits” be entered after the IP address, separated by a slash (eg 10.99.0.1/24). Unless you have more than 256 clients, you should use 24 network bits. When the table is full, press the submit button to add extra entries if necessary.

3. Return to the GSTM server configuration page. For each combination of client and service/port that you wish to access, fill in a row of the table:
  - “Listen address” should contain the address of the client on the private subnet that you have just allocated.
  - “Listen service/port” should contain the service name or port number of the service to which you wish to connect. For example, to access a web server at a client, you would enter `http` or `80`.
  - “Target client” should contain the username entered when configuring the GSTM client on the target CMG-EAM.
  - “Target service/port” should contain the same number as the second column: “Listen service/port”.

When the table is full, press the submit button to add extra entries if necessary.

Remote machines wishing to access services on clients via the GSTM server then need only configure a route to the appropriate new address. Default port numbers can then be used in applications such as browsers and *Scream!*, reducing the amount of configuration required.

Another strategy would use a single address and port-number mapping to achieve the same goals. This is equally effective but requires that remote machines wishing to access services on clients via the GSTM server use non-standard ports for those services. Many people find address mapping with direct port correspondence, as described above, easier to work with.

## 13 Monitoring Operations

This chapter details how to monitor and control the CMG-EAM. Some functionality is only available from the command line (when connected via a serial cable or via SSH over the network - see section 2 for details on how to do this) and other features are only available via the web interface. This chapter will describe both.

### 13.1 Diagnostics and the Summary menu

#### 13.1.1 System Status

To view the overall system status, simply go to the front page of the web interface (or choose the “System status” link in the left-hand frame within the “Summary” box).

One box is displayed per port or major subsystem. Boxes are colour-coded and may be displayed in red (bad), green (good) or white (no information).

**Main menu**

**eam2243**

**Summary**

[System status](#)

[Version and serial numbers](#)

**Control**

[Digital I/O](#)

[Reboot](#)

[Services](#)

**Tools**

[CD1.1 log analyser](#)

[Environment logs](#)

[Firmware](#)

[GCF audit log viewer](#)

[GDI channels display](#)

[Passwords](#)

|   |  |  |
|---|--|--|
| <b>System uptime</b><br>Status: good —<br>2010-02-04T10:34:29Z<br>System has been up for approximately 24 hours.  | <b>GCF in: Port A</b><br>Status: good —<br>2010-02-04T10:35:01Z<br>Last 5 minutes:<br><ul style="list-style-type: none"> <li>715 blocks (2.4 per second).</li> <li>0 naks (0.0 per second).</li> </ul>   | <b>GCF in: Port C</b><br>Status: unknown —<br>2010-02-04T10:34:43Z<br><b>No blocks seen.</b> |
| <b>NTP</b><br>Status: unknown —<br>2010-02-04T10:34:53Z<br><ul style="list-style-type: none"> <li>NTP has not locked the system clock as the estimated error is too large.</li> <li>Estimated error is 1000000µs.</li> <li>Clock source is <i>unspecified</i>.</li> </ul> | <b>Removable disk 69BA-6202</b><br>Status: good —<br>2010-02-04T08:21:49Z<br><ul style="list-style-type: none"> <li>Filesystem type: vfat.</li> <li>Size: 74.5GiB.</li> <li>Free: 74.4GiB (99.9%).</li> <li>Earliest entry: 2010034-gcfraw.</li> </ul> |  |

*Generated at 2010-02-04T10:35:14Z by libstatus.cgi 1.2.6. Portions of output copyright (c)2010, Guralp Systems Ltd.*

Red boxes indicate that some part of the system is malfunctioning, and require further investigation. Malfunctions could occur due to hardware failure but the most likely explanation is an incorrect configuration setting.



From the command line interface, you can view the same information by running **libstatus-query**:

```
eam999 ~ # libstatus-query
=====
2008-05-01T13:57:52Z: Good : System uptime
-----
System has been up for approximately 4 days.

=====
2008-05-01T13:59:16Z: Unknown : GCF in: Port A
-----
No blocks seen.

=====
2008-05-01T13:59:17Z: Good : GCF in: Port F
-----
Last 5 minutes:
* 1532 blocks (5.1 per second).
* 0 naks (0.0 naks per second).

=====
2008-05-01T13:59:14Z: Good : NTP
-----
NTP has locked the system clock.
Clock source is UDP/NTP.

=====
2008-05-01T13:44:11Z: Good : Removable disk 0000-0401
-----
Filesystem type: vfat.
Size: 37.2GiB.
Free: 24.9GiB (66.9%).
Earliest entry: 2008091-gcfraw.
```

---



### 13.1.2 System Log






The most important source of diagnostic and debugging information is the system log facility (“syslog”). This logs all messages from programs and from the Linux kernel. At present, this can only be viewed from the command line.

To view the system logs, you can use the **tail**, **less**, **grep** or **vi** commands to inspect the file `/var/log/messages` - older files are available as `/var/log/messages.1`, `/var/log/messages.2` etc.

Use the following syntax to view the files:

- **tail /var/log/messages**  
Views the last few entries.
- **tail -f /var/log/messages**  
As above but, after printing the last ten lines of the file,

continues to run, printing each new line as it is added to the log. Type  +  to stop the output and return to the command line.

- **less /var/log/messages**  
Views the whole log file; use the , ,  and  keys to navigate and the  key to exit.
- **vi /var/log/messages**  
Those users familiar with the **vi** text editor may wish to use it as the most powerful way to view log entries.
- **grep -i 'string' /var/log/messages**  
Searches for a string or pattern in the log file. This search is case insensitive (-i flag).



**grep** is a very powerful tool for searching for patterns. For more information, see the section on Regular Expressions in the **grep** manual page at <http://man-wiki.net/index.php/1:grep>

### 13.1.3 Incoming Data

---

The status web-page has one box for each GCF acquisition process. This box will be updated every minute to reflect the number of packets that have been acquired.

To view details of incoming GCF format data using the command line, use one of the following commands:

- **gdi-dump -l**  
Displays a list of channels and segments. For more information, see “GDI Channels Display” in section 13.3.3 on page 185;
- **gdi-dump -lm**  
Displays the the same data, along with meta-data added by the relevant input module; or
- **gdi-dump**  
Displays real-time information about each packet arriving, until interrupted by the operator typing  + .

### 13.1.4 Version and Serial Numbers

The “Version and serial numbers” item on the “Summary” menu displays information which may be useful for your own records or when requesting technical support. See section 4.1 on page 40 for more details.

## 13.2 The Control Menu

The “Control” menu of the web interface is a dynamic menu with content that changes depending on the attached devices. Two items on this menu are always present: “Reboot” and “Services”. CMG-NAM units fitted with RAID arrays will also have a “RAID array services” menu item. Other items will appear as required, depending on both the underlying hardware and attached devices.

### 13.2.1 Digital I/O (power control and anti-tamper monitoring)

The CMG-EAM mk4 hardware can be fitted with optional sensors to monitor the voltages and currents being supplied to the CMG-EAM and also to devices connected to the CMG-EAM ports, such as digitisers. A program on the CMG-EAM runs constantly in the background and monitors the sensors if they are fitted. The same program can monitor the anti-tampering lines, where fitted.

The “Digital I/O” item on the “Control” menu brings up the following screen, (the contents of which may vary with your hardware configuration):

[Home](#) → [Control](#) → [Digital I/O](#)

### I/O line status

| I/O line status and control. |   |       |  |
|------------------------------|---|-------|--|
| Line                         | Status  |       | Operations   |
| Data Out<br>Data Out power   | Output, Output, high(on)<br>Last changed: never |       | <div>View details/settings</div> <div>Set to input</div> <div>Set output low (switch off)</div> <div>Set output high (switch on)</div> |
|                              | voltage   | 11.87 |  |
|                              | Bus Voltage (V)                                 |       |  |
|                              | current   | 0.248 |  |
|                              | Current (A)                                     |       |  |
|                              | power   | 2.94  |  |
| Power (W)                    |   |       |  |
| Port A                       | Output, Output, high(on)<br>Last changed: never |       | <div>View details/settings</div> <div>Set to input</div>   |
|                              | voltage   | 11.87 |  |
|                              | Bus Voltage (V)                                 |       |  |
|                              | current   |       |  |
|                              | Current (A)                                     |       |  |
|                              | power   |       |  |
| Power (W)                    |   |       |  |

The top of this table on this page shows the real-time voltage, current and power for each monitored line, including each sensor-equipped

port of the system. There are also buttons to turn the power to the port on and off.

Clicking the “View details/settings” button produces the following screen (shown here in parts):

[Home](#) → [Control](#) → [Digital I/O](#) → [Details Data\\_Out](#)

---

## Line details

### Data Out power

Line ID: Data\_Out

#### I/O control

|                        |                  |
|------------------------|------------------|
| <b>Driver type</b>     | Output only      |
| <b>Impedance</b>       | Low (output)     |
| <b>Pin level</b>       | Output, high(on) |
| <b>Last transition</b> | Never            |

[Set to input](#)

[Set output low \(switch off\)](#)

[Set output high \(switch on\)](#)

The first part of the page duplicates the information shown on the main screen. The remainder of the page provides a more detailed report:

#### Properties

| Property   | Type       | Current value | Change  |
|--|------------|---------------|---|
| voltage<br>Bus Voltage (V)                                 | Read only  | 12.91         |   |
| current<br>Current (A)                                     | Read only  | 0.255         |   |
| power<br>Power (W)   | Read only  | 3.29          |   |
| low_voltage_threshold<br>Low voltage cut-off threshold (V) | Read/write | 0.000         | <input type="text" value="0.000"/><br><a href="#">Set</a> |
| cutoff_hysteresis<br>Cut-off hysteresis (V)                | Read/write | 0.000         | <input type="text" value="0.000"/><br><a href="#">Set</a> |
| system<br>True if this line is internal to the system      | Read only  | false         |   |
| Property   | Type       | Current value | Change  |

[Refresh](#)

[Return to front page](#)

---

Generated at 2010-02-04T11:19:52Z by *ioline.cgi* 1.0.6. Portions of output copyright (c)2010, Guralp Systems Ltd..

It is possible to protect attached devices from under-voltages by setting a **Low voltage cut-off threshold** value. If the monitored voltage falls below this value, it is automatically turned off. To prevent rapid, repeated power-cycling of attached devices, a hysteresis value should be set. The monitored voltage must rise above the sum of the threshold voltage and the hysteresis voltage before the supply will be re-enabled.

Click the “Return to front page” button to display the main Digital I/O summary again.

Below the port power monitors, the summary screen displays the anti-tamper lines (when these are fitted):

|                                     |  | Set output high (switch on) |
|-------------------------------------|--|-----------------------------|
|                                     |  | View details/settings       |
|                                     |  | Set to input                |
|                                     |  | Set output low (switch off) |
|                                     |  | Set output high (switch on) |
| tamper_5<br>External tamper 5       | Input, Input, high(on)<br>Last changed: 2010-01-27T17:36:34Z | View details/settings       |
|                                     |  | Set to input                |
|                                     |  | Set output low (switch off) |
|                                     |  | Set output high (switch on) |
| tamper_int<br>Chassis tamper detect | Input, Input, low(off)<br>Last changed: never                | View details/settings       |
|                                     |  | Set to input                |
|                                     |  | Set output low (switch off) |
|                                     |  | Set output high (switch on) |
| Line                                | Status   | Operations                  |
| Refresh                             |  |                             |

Generated at 2010-02-04T11:28:57Z by ioline.cgi 1.0.6. Portions of output copyright (c)2010,

The detail screen for the tamper detection items display no useful information beyond that displayed on the summary screen.

### 13.2.2 Digitiser/Sensor Control

The CMG-EAM allows *control* of attached digitisers and sensors via the web interface or the command line. To *configure* digitisers, see section 7 on page 78.

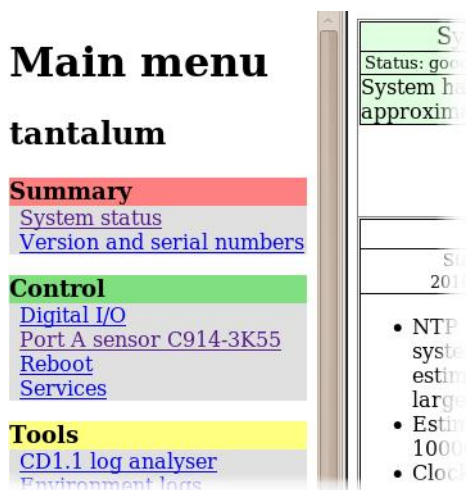
The web interface is simpler and requires no detailed knowledge of the attached devices. The command line interface is more powerful but requires detailed knowledge of the digitiser's command line interface and the manual for the digitiser in question should be referred to for further details.

#### 13.2.2.1 Digitiser/Sensor Control - Web interface

The main menu of the web interface adapts to include additional options when the system detects attached digitisers and/or digital sensors.

Extra items in the “Control” menu are associated with digitiser serial numbers. If a digitiser has two sensors attached to it, it is recommended that an extra serial number be added to the digitiser. See the relevant digitiser manual for information on how to configure this.

The menu items look like this:



In this illustration, the entry

Port A sensor C914-3K55

indicates the physical connection (Port A) to the attached device, the device type (sensor) and its serial number (C194-3K55). If the instrument is connected via TCP, the EAM connection is shown as host:port.

Selecting one of these menu items takes you to the “Digitiser Control” page. From here, one can query mass positions, lock, unlock and centre the sensor masses and perform calibration functions.

Where the attached device supports additional functions, such as bowl-levelling in an ocean-bottom system, additional controls will appear on this screen to support these features.

The screen is shown here in sections. The first deals with the sensor masses. Buttons are provided to query the mass positions, to lock the masses for transport and unlock and centre them for deployment. The verbatim output from the attached device is displayed in each case. Where a specific device does not support a specific function, the command is safely ignored.

## Digitiser Control

### C914-3K55

#### Mass positions

|  |   |  |
|--|---|--|
| <b>Query Masses</b><br>Display the current mass positions of the instrument.<br><input type="button" value="Run"/> | <b>Lock</b><br>Lock the masses for transport.<br><input type="button" value="Run"/> | <b>Unlock</b><br>Unlock the masses after installation.<br><input type="button" value="Run"/> |
| <b>Centre Masses</b><br>Centre the instrument's masses.<br><input type="button" value="Run"/>                      |   |  |

The second section of this web page deals with calibration. Note that all entered values must be integers so, for example, if you wish to calibrate with a 0.5Hz sine-wave, this should be entered as a 2 second period. Please refer to the relevant manuals for your digitiser and sensor for more details of these options.

The screen looks like this (shown in sections):

#### Calibration

|  |                                      |
|--|--------------------------------------|
| <b>Sine wave Calibration</b>             |                                      |
| Perform a calibration using a sine wave. |                                      |
| Component                                | All <input type="button" value="v"/> |
| Duration in minutes                      | <input type="text" value="2"/>       |
| Amplitude (percentage)                   | <input type="text" value="100"/>     |
| Frequency (Hz) or period (seconds)       | <input type="text" value="1"/>       |
| Units                                    | Hz <input type="button" value="v"/>  |
| <input type="button" value="Run"/>       |                                      |

The **Amplitude** value refers to an arbitrary full-scale output from the calibration circuitry. It can be left at 100% unless clipping is observed, in which case it should be reduced until an undistorted output is observed.

The square wave (step) and random calibration dialogues are similar:

**Square wave Calibration**

Perform a calibration using a square wave. The signal consists of a positive step of the given duration, followed by a negative step of the same duration.

|                        |     |
|------------------------|-----|
| Component              | All |
| Duration in minutes    | 2   |
| Amplitude (percentage) | 100 |

Run

**Random Calibration**

Perform a calibration using white noise.

|                        |     |
|------------------------|-----|
| Component              | All |
| Duration in minutes    | 2   |
| Amplitude (percentage) | 100 |

Run

The final section of the screen deals with the gimbal-mounted sensors deployed in ocean-bottom systems, which need control of their levelling and orientation functions. Where triaxial systems are mounted in a single bowl, the **Bowl** drop-down-menu should be left at "Single bowl". Where separate bowls are used for each component, the relevant component should first be selected from the menu.

## Ocean Bottom Systems

|   |   |   |
|---|---|---|
| <p><b>Deploy</b></p> <p>Deploy OBS system (levels the bowl, unlocks and centres the masses).</p> <p>Run</p> | <p><b>Level</b></p> <p>Level OBS bowl</p> <p>Bowl: Single bowl</p> <p>Run</p>                                     | <p><b>Return to Datum</b></p> <p>Returns bowl leveller to datum position.</p> <p>Bowl: Single bowl</p> <p>Run</p> |
| <p><b>Unlock OBS Components</b></p> <p>Unlock each of the OBS components.</p> <p>Run</p>                    | <p><b>Lock OBS Components</b></p> <p>Lock each of the OBS components.</p> <p>Run</p>                              | <p><b>Centre OBS Components</b></p> <p>Centre each of the OBS components.</p> <p>Run</p>                          |
| <p><b>Align bowl</b></p> <p>Align OBS bowl.</p> <p>Bowl: Single bowl</p> <p>Run</p>                         | <p><b>Recover</b></p> <p>Recover OBS system (locks the masses and returns bowl leveller to datum).</p> <p>Run</p> |   |

Generated at 2010-02-04T11:48:43Z by digitiser-control.cgi 2.2.0. Portions of output copyright (c)2010, Guralp Systems Ltd..



### 13.2.2.2 Digitiser/Sensor Control - Command line

Platinum provides both a high-level and a low-level interface to connected digitisers. The low-level interface involves interacting directly with the command-line of the digitiser and is described at the end of this section.

The high-level interface is provided by the `adc-command` command, which takes a number of sub-commands as described below. Each command must be directed to a specific sensor and this must be specified as the first argument. When invoked with no arguments, or with the `--help` argument, a list of available targets (referred to as “modules”) is displayed:

```
eam2010 ~ # adc-command --help
usage: adc-command <module> <command> [options...]

===== Available ADC modules =====
C914-3K55
C914-3K56
```

This is followed by a list of available sub-commands. In the descriptions below, ***module*** should be replaced by a name from the list provided by invoking `adc-command --help`.

- **`adc-command module mass-centre`**

Perform a centring operation on the sensor's masses. This sub-command takes no options.

- **`adc-command module mass-query`**

Display the current mass positions of the sensor. This sub-command takes no options. The masses are displayed in counts, every second for six seconds.

- **`adc-command module mass-lock`**

Lock the masses for transportation. This sub-command takes no options.

- **`adc-command module mass-unlock`**

Unlock the masses for deployment. This sub-command takes no options.

- **`adc-command module calib-sine arguments`**

Perform a sine-wave calibration according to the specified **arguments**, which are given as a space-separated list of key=value pairs:

- **component**=[ ALL | Z | N/S | E/W ] - specify the component(s) to be calibrated
  - **duration**=*m* - specify the duration, in minutes, where *m* is an integer value. For accurate results, the duration should be significantly longer than the response time of the instrument.
  - **amplitude**=*a* - specify the amplitude, where *a* is the integer percentage of the full output of the calibration signal generator. This can normally be given as 100 but should be reduced if clipping is noticed.
  - **freq**=*n* - specify the frequency (in integer Hertz) or period (in integer seconds) of the calibration signal, according to the setting of...
  - **freq\_or\_period**=[ Hz | sec ] - specifies whether the value associated with **freq** is interpreted as Hertz or seconds.
- **adc-command module calib-step arguments**

Perform a step calibration according to the specified **arguments**, which are given as a space-separated list of key=value pairs:

- **component**=[ ALL | Z | N/S | E/W ] - specify the component(s) to be calibrated
- **duration**=*m* - specify the duration, in minutes, where *m* is an integer value. The calibration signal will first go negative for this duration, then back to zero for the same duration, then go positive for this duration, then return to zero again for the same duration. For accurate results, the duration should be significantly longer than the response time of the instrument.
- **amplitude**=*a* - specify the amplitude, where *a* is the integer percentage of the full output of the calibration signal generator. This can normally be given as 100 but should be reduced if clipping is noticed.

- **adc-command module calib-noise arguments**

Perform a broad-band noise calibration according to the specified **arguments**, which are given as a space-separated list of key=value pairs:

- **component**=[ ALL | Z | N/S | E/W ] - specify the component(s) to be calibrated
- **duration**=*m* - specify the duration, in minutes, where *m* is an integer value. For accurate results, the duration should be significantly longer than the response time of the instrument.
- **amplitude**=*a* - specify the amplitude, where *a* is the integer percentage of the full output of the calibration signal generator. This can normally be given as 100 but should be reduced if clipping is noticed.

- **adc-command module obs-deploy**

Deploy an OBS system by levelling the bowl, then unlocking and centring each mass in turn. This sub-command takes no options.

- **adc-command module obs-level bowl=which**

Level the bowl or bowls of an OBS system. The parameter **which** should be one of 1BOWL (for single-bowl units), Z, N/S or E/W.

- **adc-command module obs-datum bowl=which**

Return the levelling bowl of an OBS system to the datum position. The parameter **which** should be one of 1BOWL (for single-bowl units), Z, N/S or E/W.

- **adc-command module obs-unlock**

Unlock each of the masses for deployment of an OBS system. This sub-command takes no options.

- **adc-command module obs-lock**

Lock each of the masses for deployment of an OBS system. This sub-command takes no options.

- **adc-command module obs-centre**

Centre each of the masses for deployment of an OBS system. This sub-command takes no options.

- **adc-command module obs-align bowl=which**

Align the levelling bowl of an OBS system. The parameter **which** should be one of 1BOWL (for single-bowl units), Z, N/S or E/W.

- **adc-command module obs-recover**

Prepare an OBS system for recovery by locking the masses and returning the bowl leveller to its datum position. This sub-command takes no options.

The CMG-EAM also provides the ability to connect to the terminal of any connected Guralp digitisers in order to configure their operation and control the attached sensors. To do this, connect to the CMG-EAM terminal as in section 2.1 or 2.2 and run the “data-terminal” command.

```
eam999 ~ # data-terminal
```

Select the desired digitiser (using the up/down arrow keys and Enter to select) from the list that is presented:

This will launch a minicom session (see section 14.4), allowing you to communicate with the digitiser terminal. For example:

```
Welcome to minicom 2.3-rc1

OPTIONS:
Compiled on Feb  9 2008, 16:59:26.
Port /dev/tts/0

          Press CTRL-A Z for help on special keys

LW B68000 CMG-5TD Command Mode
0 blocks in buffer | 256 blocks free
Guralp Systems Ltd - DM+FW v.103 mgs 13/02/08 (Build 65)

CTRL-A Z for help |115200 8N1 | NOR | Minicom 2.3-rc | VT102 | Offline
```

If the session closes due to a time-out (or you close it manually by issuing the `GO` command) then you will see the message `Killed by signal 15` and minicom will exit shortly thereafter.

If you wish to upload new digitiser firmware, please follow the digitiser manual to prepare it to accept firmware, then use the standard minicom “Send files” (`Ctrl` + `A`, `S`) command to initiate an X-Modem upload. Refer to section 14.4 for instructions on using Minicom. Digitiser firmware files may be found under the directory `/usr/share/firmware` on the CMG-EAM. Once downloaded, please follow the instructions given in the digitiser's manual to complete the process.

### 13.2.3 Rebooting

---

The “Reboot” item on the “Control” menu allows CMG-EAMs and CMG-DCMs to be rebooted. CMG-NAMs can be both rebooted and powered off. To reboot from the command line prompt, use the reboot command.

```
eam999 ~ # reboot
```

### 13.2.4 Services

---

The “Services” item from the “Control” menu takes you to the Services Control screen. This screen gives a list of all configured services: services are the background programs that read, convert and write data and carry out the individual functions of the CMG-EAM.

The services are presented in three columns. In the first is given the name of the service and, in italics, its description. The second column shows the word “Stopped” in red for any services which are not running and, for those which are running, the PID (process ID, a unique number which the operating system uses to keep track of running programs) and the date and time that this instance of the service was started. The third column has buttons allowing you to stop, start or re-start each service.

It is possible to monitor and control services from the command line using the `ps` command and various scripts in `/etc/init.local` and `/etc/init.d`. This should be familiar to Linux users but full details are beyond the scope of this manual.

## Service Control

|  |   |   |
|--|---|---|
| DataOut<br><i>Serial Data Out Port</i> | <b>Running</b><br>PID: 710<br>Started: Thu Jan 1<br>00:00:49 UTC 1970 | <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/> |
| PortA<br><i>Serial Port A</i>          | <b>Running</b><br>PID: 716<br>Started: Thu Jan 1<br>00:00:49 UTC 1970 | <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/> |
| PortB<br><i>Serial Port B</i>          | <b>Running</b><br>PID: 722<br>Started: Thu Jan 1<br>00:00:50 UTC 1970 | <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/> |
| PortC<br><i>Serial Port C</i>          | <b>Running</b><br>PID: 728<br>Started: Thu Jan 1<br>00:00:50 UTC 1970 | <input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Restart"/> |

### 13.2.5 RAID Array Services

---

RAID arrays provide increased data security at the cost of extra storage devices. They can prevent the loss of data in the event of a single drive failure. The “RAID Array Services” item on the “Control” menu will only be displayed on CMG-NAMs with RAID fitted. It displays a page which reports the status of and allows simple control of the fitted RAID array. The status of swap partitions are also reported on this page.

## 13.3 Tools Menu

---

### 13.3.1 Passwords

---

The password-change facility is described in section 2.3 on page 24.

### 13.3.2 GCF Audit Log Viewer

---

Detailed information about every GCF packet sent or received are stored on the GSL-EAM and can be viewed with the GCF Audit Log Viewer. To access the GCF Audit Log Viewer from the web interface, click on “GCF audit log viewer” on the “Tools” menu. To access the same information from the command line, enter the command

```
gcflogview
```

The initial screen displays all GCF data sources and sinks in a table, together with some summary information. In the example given, it can be seen that Ports B and F are inactive, Port A was receiving GCF data until 16:36 and the default instance of the Scream network server was sending GCF data until the same time.

## GCF audit log viewer

GCF audit logs. Select 'View' to view a log in more detail.

| Program                                       | Latest entry         | Size   | View                 |
|---|----------------------|--------|----------------------|
| Port A  | 2009-07-13T16:36:37Z | 256KiB | <a href="#">View</a> |
| Port B  | No entries           | 256KiB | <a href="#">View</a> |
| Port F  | No entries           | 256KiB | <a href="#">View</a> |
| Scream (GCF) network server, instance default | 2009-07-13T16:36:33Z | 128KiB | <a href="#">View</a> |
| Program                                       | Latest entry         | Size   | View                 |

Generated at 2009-07-13T16:36:37Z by *gcflogview.cgi* 1.0.5. Portions of output copyright (c)2009, Guralp Systems Ltd.

The “Size” column shows the size of the log buffer allocated to each data source or sink. The log buffer size can be changed from the relevant service or port configuration screens in expert mode.

For example, to allocate a larger log buffer to the GCF receiver running on Port A, click on “Serial ports” from the main menu, then on “Port A - GCF in”, “GCF input settings” and then click the “Expert” button. You will see a drop-down selection list labelled “Audit log size” from which you can select 64Kib, 256Kib, 2MiB or 16MiB.

To change the GCF audit log buffer size for the Scream network server, select “Services” from the “Data transfer/recording” section of the “Configuration” menu then click on “GCF Scream network server”. Click on the entry for the instance you wish to change and then click the “Expert” button at the bottom of the page. You will see a drop-down selection list labelled “Audit log size” from which you can select 64Kib, 256Kib, 2MiB or 16MiB.

Each entry in the table has a “View” button, which shows detail from the relevant log at block (packet) level). The view for Port A is shown here:

# GCF audit log viewer

## Port A

Search within this log

Recent entries

| Time         | Type               | Details  | Hex  |
|--------------|--------------------|--|--|
| 2009-07-13   |                    |  |  |
| 16:36:37.554 | GCF block received | ID: <b>A830-55TPNE</b><br>Timestamp: 2009-07-13T16:36:36.000000000Z<br>Digitiser: CMG-DM24-mk3<br>Block type: data<br>Sample rate: 20 samples/second<br>Compression: 32-bit<br>Number of samples: 20 | 80 07 47 6C<br>12 9A 80 1A<br>38 14 E9 94<br>1F 14 01 14 |
| 16:36:37.634 | GCF block received | ID: <b>A830-55TPSM</b><br>Timestamp: 2009-07-13T16:36:36.000000000Z<br>Digitiser: unknown, probably CMG-DM24-mk2<br>Block type: strong motion<br>Number of words: 50                                 | 80 07 47 6C<br>12 9A 80 06<br>38 14 E9 94<br>00 00 04 32 |
| 16:36:37.694 | GCF block received | ID: <b>A830-55TPEE</b><br>Timestamp: 2009-07-13T16:36:36.000000000Z<br>Digitiser: CMG-DM24-mk3<br>Block type: data<br>Sample rate: 20 samples/second<br>Compression: 32-bit<br>Number of samples: 20 | 80 07 47 6C<br>12 9A 7E 06<br>38 14 E9 94<br>1F 14 01 14 |

The first column shows the time-that the block was received (not the time-stamp on the block itself) and the second column shows the event type - “GCF block received” in most cases.

The “Details” column shows the stream ID from the received data block and the block time-stamp. The digitiser ID is shown if it is encoded in the block; otherwise, a best guess is displayed. The rest of the entry shows the block type, sample rate, compression level and the number of samples in the data block.

A hexadecimal display of the block header is shown in the final column.

An example of an audit log display for an out-going data-stream is shown below. This data is for the Scream network server:. The first column now shows the time that the block was transmitted; other details are the same as in the previous example.



## GCF audit log viewer

Scream (GCF) network server, instance default

Search within this log

### Recent entries

| Time         | Type           | Details  | Hex  |
|--------------|----------------|--|--|
| 2009-07-13   |                |  |  |
| 16:27:05.228 | GCF block sent | ID: <b>A830-55TP3O</b><br>Timestamp: 2009-07-13T16:18:44.000000000Z<br>Digitiser: unknown, probably CMG-DM24-mk2<br>Block type: data<br>Sample rate: 1 samples/second<br>Compression: 16-bit<br>Number of samples: 500 | 00 07 47 6C<br>12 9A 7D 54<br>38 14 E5 64<br>00 01 02 FA |
| 16:27:05.228 | GCF block sent | ID: <b>A830-55TP3Q</b><br>Timestamp: 2009-07-13T16:18:44.000000000Z<br>Digitiser: unknown, probably CMG-DM24-mk2<br>Block type: data<br>Sample rate: 1 samples/second<br>Compression: 16-bit<br>Number of samples: 500 | 00 07 47 6C<br>12 9A 7D 56<br>38 14 E5 64<br>00 01 02 FA |
| 16:27:05.228 | GCF block sent | ID: <b>A830-55TPZP</b><br>Timestamp: 2009-07-13T16:18:44.000000000Z<br>Digitiser: unknown, probably CMG-DM24-mk2<br>Block type: data<br>Sample rate: 1 samples/second<br>Compression: 16-bit<br>Number of samples: 500 | 00 07 47 6C<br>12 9A 81 05<br>38 14 E5 64<br>00 01 02 FA |

### 13.3.3 GDI Channels Display

It is often useful, particularly when configuring a CMG-EAM for a complex array, to see a list of the Stream IDs, or channel names, which the CMG\_EAM is receiving. The GDI Channels Display feature allows you to view a list of all active channels, together with some additional detail about each.

To access the GDI Channels Display from the web interface, click on “GDI Channels Display” on the “Tools” menu.

Similar information is available from the command line via the command `gdi-dump` with the `--list-only` option but the format is optimised for automated processing rather than human consumption. Giving the `--help` option provides usage details. Use of the web interface, however, is recommended.

The following summary screen is displayed:

## GDI Status

List of channels.

| Name        | Format   | Active segments              | Actions                      |                           |
|-------------|--|------------------------------|------------------------------|---------------------------|
| A830-55TPC2 | Signed 32-bit integer samples<br>40 samples/second | 1 (backfill only)            | <a href="#">View details</a> | <a href="#">Dump data</a> |
| A830-55TPE4 | Signed 32-bit integer samples<br>40 samples/second | 1 (backfill only)            | <a href="#">View details</a> | <a href="#">Dump data</a> |
| A830-55TPN4 | Signed 32-bit integer samples<br>40 samples/second | 1 (backfill only)            | <a href="#">View details</a> | <a href="#">Dump data</a> |
| A830-55TPZ4 | Signed 32-bit integer samples<br>40 samples/second | 1 (backfill only)            | <a href="#">View details</a> | <a href="#">Dump data</a> |
| A830-55TP2O | 32-bit floating point samples<br>1 samples/second  | 1 (realtime)<br>2 (backfill) | <a href="#">View details</a> | <a href="#">Dump data</a> |
| A830-55TP2P | 32-bit floating point samples<br>1 samples/second  | 1 (realtime)<br>2 (backfill) | <a href="#">View details</a> | <a href="#">Dump data</a> |

The first two columns show the names of the channels, together with information about the data format. The Active segments column shows details of data currently being received. A segment is a contiguous sequence of blocks so any data being back-filled always requires separate segments.

For each channel, you have the option of viewing detailed information about the data or the data itself, by use of the “View details” and “Dump data” buttons.

The “View details” button displays the following screen, shown here in parts:

### Channel A830-55TP2O details

#### Channel information

|                  |                               |
|------------------|-------------------------------|
| GDI channel name | A830-55TP2O                   |
| Sample format    | 32-bit floating point samples |
| Sample rate      | 1 samples/second              |

The first section of the screen, above, shows the channel name, sample format and sample rate, as seen on the previous screen.

#### Segments

Segments are continuous runs of time-series sampled data. Segments never contain gaps. A segment is considered *Realtime* if it has the most recent timestamp of all segments and if the last data for it was received less than 5 minutes ago according to the system clock. Otherwise, the segment is considered to be *Backfill*.

List of active segments.

| Segment time  | 2009-07-14T08:13:00Z   | 2009-07-10T12:04:21Z   | 2009-07-10T11:59:20Z  |
|---------------|--|--|---|
| Realtime?     | Realtime   | Backfill   | Backfill  |
| Clock status  | <b>Locked.</b> Differential 1 $\mu$ s.<br>Last update at 2009-07-14T08:13:00Z.                             | <b>Locked.</b> Differential 400 $\mu$ s.<br>Last update at 2009-07-10T12:04:21Z.                           | <b>Unlocked.</b> Clock never locked; unable to estimate differential.<br>Last update at 2009-07-10T11:59:20Z. |
| GPS status    | Fix: 3D. Location: 51.361208°N -51.361208°W<br>elevation 106.000m.<br>Last update at 2009-07-14T08:13:00Z. | Fix: 3D. Location: 51.361181°N -51.361181°W<br>elevation 114.000m.<br>Last update at 2009-07-10T12:04:21Z. | Fix: 3D. Location: 51.361180°N -51.361180°W<br>elevation 115.000m.<br>Last update at 2009-07-10T11:59:20Z.    |
| Channel flags | No SOH info from digitiser.<br>Are unified status packets enabled?   | No SOH info from digitiser.<br>Are unified status packets enabled?   | No SOH info from digitiser.<br>Are unified status packets enabled?  |

The next section of this screen, above, shows, for each active segment, detailed information decoded from the packet header.

The final section, below, shows the metadata associated with the stream, which is derived from the configuration parameters of the relevant input module:

### Metadata

Metadata is provided by the acquisition software module. Any metadata field may be overridden in the configuration of the *gdi\_base* module.

List of channel metadata.

| Name               | Value             |
|--------------------|-------------------|
| acquisition-device | Port A            |
| instrument-id      | A830-55TP         |
| terminal           | A830-55TP         |
| sample-units       | cms <sup>-2</sup> |
| instrument-type    | accelerometer     |
| component          | 2D                |
| Name               | Value             |

Return to index

Refresh display

The “Dump Data” buttons associated with each channel on the GDI Status display screens like the following:

## GDI Status

### Channel dump for A830-55TP20.

*Please note if this is a status channel there may be little or no data shown here.*

☒ Show meta data ☒ Show samples

New channel: ID 00000010, 32-bit floating point samples, 1 sps: A830-55TP20

```

acquisition-device = Port A
instrument-id = A830-55TP
terminal = A830-55TP
sample-units = cms-2
instrument-type = accelerometer
component = 2D

```

New segment: ID 00000010:00000000 2009-07-10T11:59:20Z

New segment: ID 00000010:00000001 2009-07-10T12:04:21Z

New segment: ID 00000010:00000002 2009-07-14T11:32:39Z

Initial subscription list complete

```

2009-07-14T11:32:39Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.230499
2009-07-14T11:32:40Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.038962
2009-07-14T11:32:41Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.003381
2009-07-14T11:32:42Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.078720
2009-07-14T11:32:43Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.449163
2009-07-14T11:32:44Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.468655
2009-07-14T11:32:45Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.135324
2009-07-14T11:32:46Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.133336
2009-07-14T11:32:47Z 00000010:00000002 (A830-55TP20) 1 32-bit floating point samples @ 1 sps
0.128433

```

Check-boxes are available to toggle the display of both metadata and sample data. These can be changed at any time and the “Restart dump” button used to refresh the display.

For sample data, each line displays the sample's time-stamp, the segment ID, the channel name in parentheses, the sample type and the actual sample value.

A button at the bottom of the screen allows the display to be refreshed with current data. There is also a button which, when clicked, returns the user to the main GDI Channels Display index page, so that another channel can be inspected.

## 14 Appendices

### 14.1 Setting the System Identity (Hostname)

The system identity is pre-set at the factory to contain a device-type identifier and the system's serial number, such as “EAM2010”. It should not be necessary to change this but, should you desire to, the following procedure can be used.

To set the system identity using the web interface, select “System identity (hostname)” from the “Configuration” → “All options” menu. To set the system identity from the command line, start `gconfig` and select “System identity (hostname)” from the top level menu.

The following screen is displayed:

[Home](#) → [Configuration](#) → [Hostname](#)

#### System identity (host name)

This is the name used to identify the system internally and to other systems in the local network.

|   |   |
|---|---|
| System ID   | <input type="text" value="dcm105"/> local.net |
|   | Host name (one word)                          |
| Allow DHCP override   | <input checked="" type="checkbox"/>           |
| <input type="button" value="Home"/> <input type="button" value="Help"/> <input type="button" value="Expert"/> <input type="button" value="Submit"/> |   |

*Generated at 1970-01-02T02:07:19Z by gcs 2.0.2. Portions of output copyright (c)1970, Guralp Systems Limited.*

Use this screen to set the hostname of the CMG-EAM. If the **Allow DHCP Override** check-box is ticked then, when the system requests an IP address from a DHCP server, the server response will override the hostname set on this screen.

## 14.2 Authenticated Digitisers.

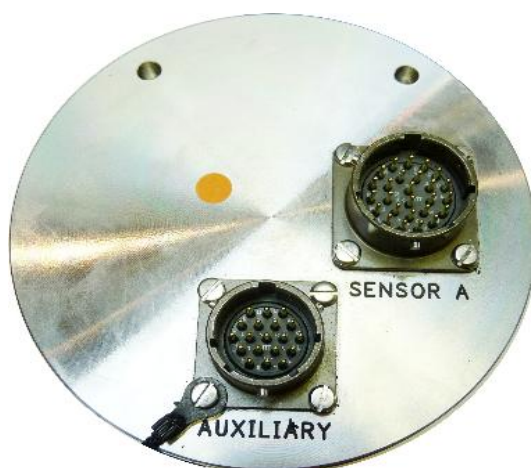
---

Güralp Systems Ltd's authenticated digitisers provide a CMG-DM24 and a CMG-EAM in a single package: a stainless steel or aluminium cylinder with an optional carrying/mounting bracket. An internal Spyrus PC card provides authentication and digital signing of CD1.1 frames and subframes.



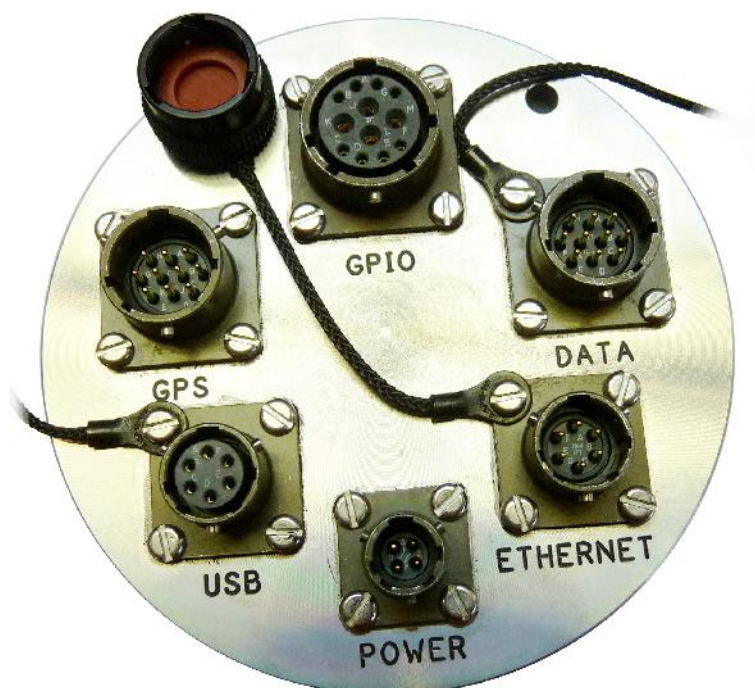
The system is fitted with variable gain analogue inputs, tamper-detection lines on all key connectors and an internal USB storage device, which is available to external USB host devices such as laptop computers.

The connectors are significantly different from other packages. The analogue connectors are grouped at one end of the cylinder:



and correspond to similarly labelled connectors on a standard CMG-DM24. The illustration shows a four-channel unit; the seven-channel unit has an additional connector for sensor B.

The digital connectors are arranged at the other end of the cylinder:



The pin-outs for each of these connectors are given in sections 14.3.6 through to 14.3.10.

### **14.2.1 Internal Connections**

---

Internally, the digitiser module and acquisition module are connected using three serial lines. The exact connections depend on the synchronisation mode, determined by the service running on Port C of the acquisition module.

In all cases, the GCF data output from the digitiser module is connected to Port A of the acquisition module, which should be set to “GCF in” at 38,400 Baud. It is currently possible to set the Baud rate of the digitiser's data output port and of the EAM's Port A independently, leading to a loss of data communication between the two modules if the two do not match. If you wish to have a higher transfer rate between the two modules, both ends must have their Baud rates increased separately.

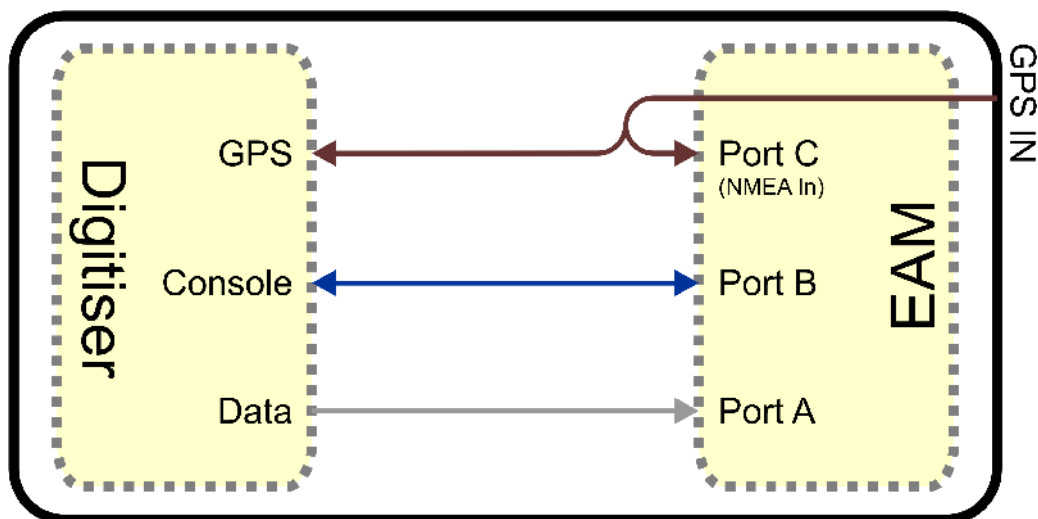


The digitiser module also exposes a dedicated console connection, which is internally attached to Port B of the acquisition module. This can be accessed from the command line of the acquisition module or, if desired, made accessible over the network. If you wish to disallow network access, set the service on the EAM's Port B to “none”. To enable access over the network, set the service on the EAM's Port B to “TCP serial converter. Serial data to TCP link converter” and configure the converter according to the instructions in section 6.7 on page 74.

It is currently possible to set the Baud rate of the digitiser's console port and of the EAM's Port B independently, leading to a loss of data communication between the two modules if the two do not match. If you wish to have a higher transfer rate between the two modules, both ends must have their Baud rates increased separately. The digitiser module's Baud rate must be changed first.

Port C of the acquisition module is used for synchronisation and can either provide NMEA to the digitiser module or share incoming GPS data from an external receiver. Different internal connections are used in each case: an analogue switch is controlled by the service selected for the EAM's Port C.

When the Port C service is set to “NMEA In”, the connections are as follows:

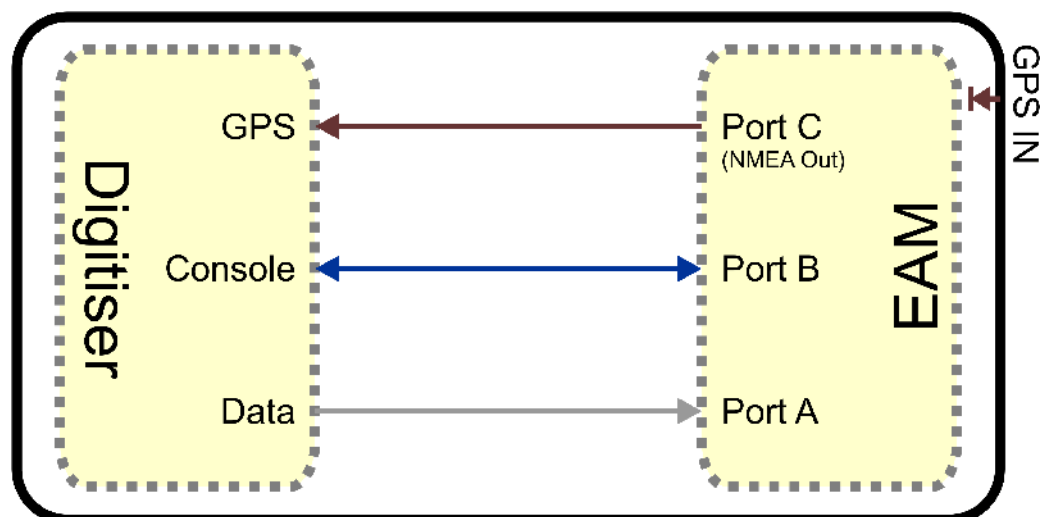


Incoming data from an external GPS receiver is available to both the digitiser and acquisition modules. Both the digitiser's GPS input and Port C of the acquisition module must run at 4,800 Baud. This should never be changed.



If an external GPS receiver is used but it is not required to use its data in the EAM, the service on Port C can be set to “none”.

If use of a GPS receiver is impractical but internet-derived NTP synchronisation is available, this can be used as the clock source for both the digitiser module and the acquisition module. By setting the service on Port C to “NMEA out”, the following connections are enabled:



Both the digitiser's GPS input and Port C of the acquisition module must run at 4,800 Baud. This should never be changed. Note that, in this mode, the external GPS socket is disconnected: it cannot be used as an output for additional digitisers.

### 14.2.2 Variable Gain Inputs

The authenticated digitiser is fitted with a programmable gain differential input amplifier which can be set to  $\times 1$ ,  $\times 2$ ,  $\times 4$ ,  $\times 8$ ,  $\times 16$ ,  $\times 32$  or  $\times 64$  gain operation.

The gain can be set individually for each input channel, either using the Platinum web configuration interface or directly from the digitiser's command line. In either case, the digitiser module must be re-booted before the new value will take effect.

The gain settings are reported in the status stream at boot time:

```

ADC #1 Version 760303
ADC o/s nulls 0 0 0 0
4 channel system
Gain Control : E8
Gain settings : Ch#0 *1 Ch#1 *1 Ch#2 *1 Ch#3 *1
  
```

In the example above, all channels are set to unity gain (channel 0 is the vertical component and 1, 2 and 3 are the North/South, East/West and auxiliary/calibration channels, respectively). On a seven-channel digitiser, channels 4, 5 and 6 are the vertical, North/South and East/West components for the second instrument). If variable-gain-aware firmware (v106b42 and above) is loaded on a digitiser without variable-gain hardware, the text “No gain stage” will appear in this position in the boot status stream.

The selected gain setting is encoded into the GCF headers by appropriating bits from the System ID which must, therefore, be chosen to be five (or fewer) characters long. See the note at the end of this section for more information. The InfoBlocks (see section 7 on page78) should be changed to reflect the amended System ID but the gain figure taken from the calibration document should be used unchanged, regardless of the variable gain setting chosen. Similarly the “calvals” file in Scream! should not be changed, other than to reflect the System ID; Scream! can deduce the variable gain settings in use from the GCF block headers and automatically take account of these during calibration operations.

To change the gain using the web interface, select the digitiser from the list in the “System setup” section of the “Configuration” menu and scroll down to the “Connected devices” section. The following additional sub-section appears:

The screenshot shows a web interface with a 'Mass auto centering' dropdown set to 'Disabled'. Below it is a section titled 'Input gain settings' containing four rows of input gain settings: 'Z input gain', 'N input gain', 'E input gain', and 'X input gain'. Each row has a dropdown menu currently set to 'x1 (unity)'. Below this section is a 'Device info blocks' section which contains the text 'Info block 1 is empty.'

(This table is extended to show three additional components when a seven-channel digitiser is detected.)

From here, the gain can be set individually for each component. If the “Submit” button is clicked, the changes will be stored in the digitiser module's configuration but will not take effect until the module is rebooted. If an immediate change is required, the “Submit & Reboot digitiser” button should be used instead.

To change the gain using the command line, use the **data-terminal** command to connect to the digitiser, as described in section 13.2.2.2 on page 177 and issue one of the following two commands.

To simultaneously set all channels to the same gain, enter the command:

**gain \*gains**

where **gain** is one of 1, 2, 4, 8, 16, 32 or 64. For example, to select  $\times 8$  gain on all channels, enter the command

**8 \*gains**

The digitiser must be rebooted before the change will take effect.

To set the gain for an individual channel, enter the command:

**channel gain \*gain**

where **channel** is one of 0 (vertical), 1 (North/South), 2 (East/West) or 3 (auxiliary/calibration). On seven channel digitisers, this parameter can also be one of 4 (vertical), 5 (North/South) or 6 (East/West), referring to the components from the second instrument. **gain** is one of 1, 2, 4, 8, 16, 32 or 64. For example, to select  $\times 16$  gain on just the vertical channel, enter the command

**0 16 \*gains**

The digitiser must be rebooted before the change will take effect.

**Note:** Software developers working with GCF packets can decode the selected gain setting from the GCF header as follows:

If the most significant bit of the System ID is zero, variable gain is not used. If the most significant two bits of the System ID are 10 or 11, the next three bits encode the gain, using this code:

| Bits 2, 3 & 4 | Gain        |
|---------------|-------------|
| 000           | not fitted  |
| 001           | $\times 1$  |
| 010           | $\times 2$  |
| 011           | $\times 4$  |
| 100           | $\times 8$  |
| 101           | $\times 16$ |
| 110           | $\times 32$ |
| 111           | $\times 64$ |

---

### 14.2.3 USB operations

The Authenticated Digitiser can behave as a USB storage device (via the GPIO connector) or as a USB host (via the USB connector).

#### 14.2.3.1 USB device mode

The Authenticated Digitiser is fitted with an internal Flash memory device which is accessible via USB. It can be written to by selecting “Internal USB storage” from the “Recording destination” drop-down menu on the “Disk recording” menu (see section 10.2 on page 109).

When a USB host, such as a laptop or PC, is connected to the GPIO port (who's pin-out is given in section 14.3.6 on page 203) internal circuitry detects the USB power and automatically connects the Flash memory to the USB socket, causing it to behave identically to a standard USB memory stick.

When no power is detected at the USB port, the Flash memory is available to the system as if it were a standard removable disk. All of the disk recording options described in section 10.2 (on page 109) will apply to this device.

#### **14.2.3.2 USB host mode**

If a USB storage device is connected to the USB port (who's pin-out is given in section 14.3.8 on page 205), it will be mounted under `/media`. It can be used to store seismic data by selecting “External USB drive on mil-spec connector” from the “Recording destination” drop-down menu on the “Disk recording” menu (see section 10.2 on page 109).<sup>109</sup>

# 14.3 Connector pin-outs

---

## 14.3.1 Peli-case: PORTs A, B, C....

---

These are standard 10-pin “mil-spec” sockets, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-12-10P and are available from Amphenol, ITT Cannon and other manufacturers.



The pin-out is such that the port can be connected to the serial output of a DM24 digitizer using a straight-through cable.

---

| Pin | Function           |
|-----|--------------------|
| A   | Power 0 V          |
| B   | Power +10 to +35 V |
| C   | RS232 RTS          |
| D   | RS232 CTS          |
| E   | RS232 DTR          |
| F   | RS232 DSR          |
| G   | RS232 ground       |
| H   | RS232 CD           |
| J   | RS232 transmit     |
| K   | RS232 receive      |

---

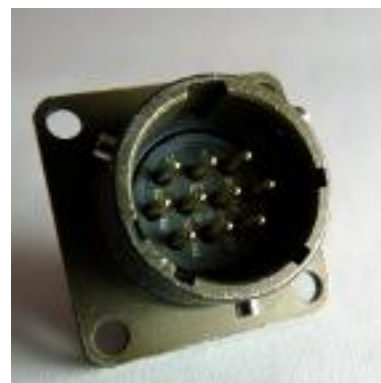


Wiring details for the compatible plug, \*\*\*-12-10P, as seen from the cable end (i.e. during assembly).

### 14.3.2 Peli-case: DATA OUT port

This is a standard 10-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-12-10S and are available from Amphenol, ITT Cannon and other manufacturers.



The pin-out is the same as the serial output of a DM24 digitizer, allowing you to insert a CMG-EAM into a pre-existing installation and maintain connectivity.

| Pin | Function                  |
|-----|---------------------------|
| A   | Power input, 0 V          |
| B   | Power input, +10 to +35 V |
| C   | RS232 CTS                 |
| D   | RS232 RTS                 |
| E   | RS232 DTR                 |
| F   | RS232 DSR                 |
| G   | RS232 ground              |
| H   | RS232 CD                  |
| J   | RS232 receive             |
| K   | RS232 transmit            |

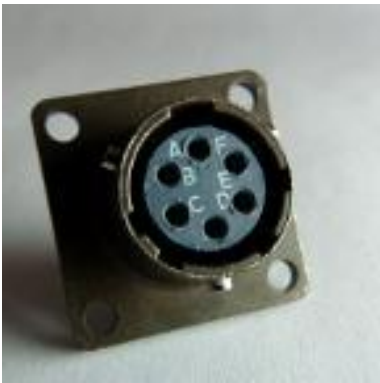


Wiring details for the compatible socket, \*\*\*-12-10S, as seen from the cable end (i.e. during assembly).

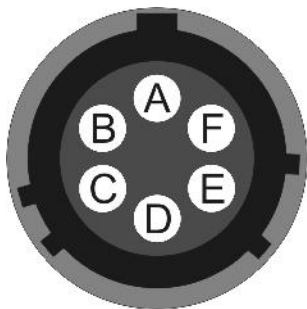
**14.3.3 Peli-case: USB**

This is a standard 6-pin “mil-spec” socket, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-10-06P and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function                    |
|-----|-----------------------------|
| A   | +5 V DC (USB Type A pin 1)  |
| B   | Data –ve (USB Type A pin 2) |
| C   | Data +ve (USB Type A pin 3) |
| D   | 0 V (USB Type A pin 4)      |
| E   | Shielding                   |
| F   | Switched power +10 to +35 V |



Wiring details for the compatible plug, \*\*\*-10-06P, as seen from the cable end (i.e. during assembly).



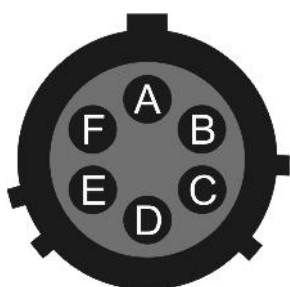
### 14.3.4 Peli-case: NETWORK

This is a standard 6-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-10-06S and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function                       |
|-----|--------------------------------|
| B   | Data transmit +ve (RJ45 pin 1) |
| C   | Data receive +ve (RJ45 pin 3)  |
| E   | Data receive –ve (RJ45 pin 6)  |
| F   | Data transmit –ve (RJ45 pin 2) |



Wiring details for the compatible socket, \*\*\*-10-06S, as seen from the cable end (i.e. during assembly).

**14.3.5 Peli-case: Console**

---

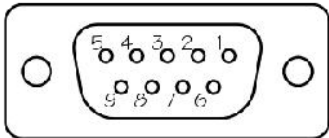
This is a standard DE9F (TIA-574) sub-miniature (D-sub) line socket, conforming to DIN 41652 and MIL-DTL-24308. They are very widely available, as are suitable mating connectors.



---

| Pin | Function               |
|-----|------------------------|
| 1   | <i>not connected</i>   |
| 2   | RS232 transmitted data |
| 3   | RS232 received data    |
| 4   | <i>not connected</i>   |
| 5   | Ground                 |
| 6   | <i>not connected</i>   |
| 7   | <i>not connected</i>   |
| 8   | <i>not connected</i>   |
| 9   | <i>not connected</i>   |

---



Wiring details for the compatible plug, DE9M, as seen from the cable end (i.e. during assembly).

### 14.3.6 Cylinder: GPIO

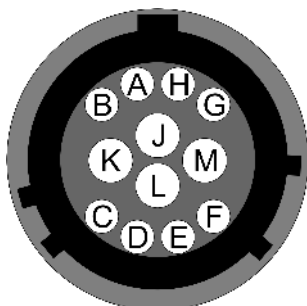
These are standard 12-pin “mil-spec” sockets, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-14-12S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-14-12P and are available from Amphenol, ITT Cannon and other manufacturers.



The USB lines provide external host access to the internal USB memory device. When power is sensed on pin J, an internal switch disconnects the memory device from the internal circuitry and connects it to this socket.

| Pin | Function   |
|-----|--|
| A   | USB Data -ve (USB Type A pin 1) - see text above.    |
| B   | USB Data +ve (USB Type A pin 3) - see text above.    |
| C   | Anti-tamper line 4                                   |
| D   | Anti-tamper line 3                                   |
| E   | Anti-tamper line 2                                   |
| F   | Anti-tamper line 1                                   |
| G   | Console transmit (RS232 TXD)                         |
| H   | Console receive (RS232 RXD)                          |
| J   | USB Power input (USB Type A pin 1) - see text above. |
| K   | Ground (USB Type A pin 4)                            |
| L   | Anti-tamper line 0                                   |
| M   | Ground   |

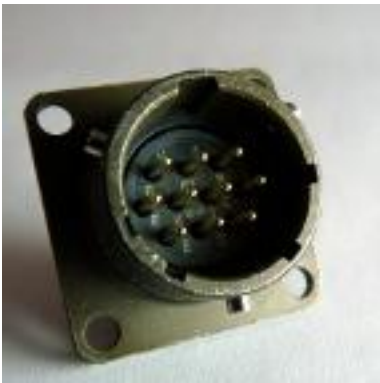


Wiring details for the compatible plug, \*\*\*-14-12P, as seen from the cable end (i.e. during assembly).

### 14.3.7 Cylinder: GPS

This is a standard 10-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-12-10S and are available from Amphenol, ITT Cannon and other manufacturers.



The pin-out is the same as the GPS input of a DM24 digitizer.

| Pin | Function                   |
|-----|----------------------------|
| A   | Power 0 V                  |
| B   | Power +12 V                |
| C   | 1pps signal                |
| D   | <i>not connected</i>       |
| E   | Digitizer console transmit |
| F   | Digitizer console receive  |
| G   | RS232 ground               |
| H   | Digitizer console ground   |
| J   | RS232 transmit to GPS      |
| K   | RS232 receive from GPS     |



Wiring details for the compatible socket, \*\*\*-12-10S, as seen from the cable end (i.e. during assembly).

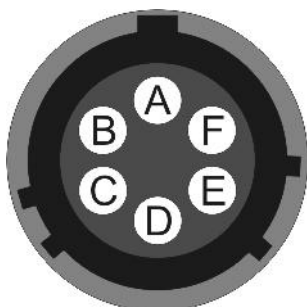
### 14.3.8 Cylinder: USB

This is a standard 6-pin “mil-spec” socket, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06S although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-10-06P and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function                    |
|-----|-----------------------------|
| A   | +5 V DC (USB Type A pin 1)  |
| B   | Data –ve (USB Type A pin 2) |
| C   | Data +ve (USB Type A pin 3) |
| D   | 0 V (USB Type A pin 4)      |
| E   | Shielding                   |
| F   | <i>not connected</i>        |



Wiring details for the compatible plug, \*\*\*-10-06P, as seen from the cable end (i.e. during assembly).

### 14.3.9 Cylinder: Power

---

This is a standard 4-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-08-04P although the initial “02E” varies with manufacturer.

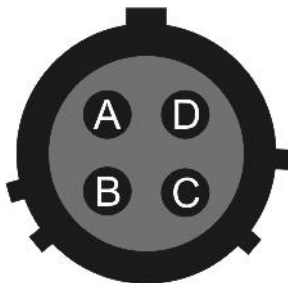
Suitable mating connectors have part-numbers like \*\*\*-08-04S and are available from Amphenol, ITT Cannon and other manufacturers.



---

| Pin | Function                          |
|-----|-----------------------------------|
| A   | Ground                            |
| B   | +ve supply input                  |
| C   | Anti-tamper line 5                |
| D   | External switched power output #1 |

---



Wiring details for the compatible socket, \*\*\*-08-04S, as seen from the cable end (i.e. during assembly).

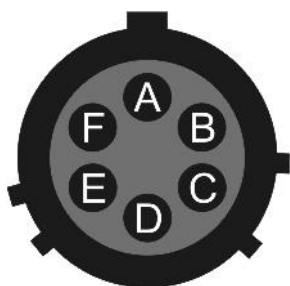
### 14.3.10 Cylinder: Ethernet

This is a standard 6-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-10-06P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-10-06S and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function                          |
|-----|-----------------------------------|
| A   | Ground                            |
| B   | Data transmit +ve (RJ45 pin 1)    |
| C   | Data receive +ve (RJ45 pin 3)     |
| D   | External switched power output #0 |
| E   | Data receive -ve (RJ45 pin 6)     |
| F   | Data transmit -ve (RJ45 pin 2)    |



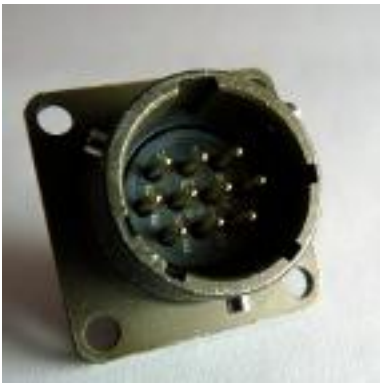
Wiring details for the compatible socket, \*\*\*-10-06S, as seen from the cable end (i.e. during assembly).

**14.3.11 Cylinder: Data**

---

This is a standard 10-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-12-10P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-12-10S and are available from Amphenol, ITT Cannon and other manufacturers.



---

| Pin | Function                  |
|-----|---------------------------|
| A   | Power input, 0 V          |
| B   | Power input, +10 to +36 V |
| C   | RS232 CTS                 |
| D   | RS232 RTS                 |
| E   | External trigger output   |
| F   | External trigger output   |
| G   | RS232 ground              |
| H   | External trigger input    |
| J   | RS232 receive             |
| K   | RS232 transmit            |

---



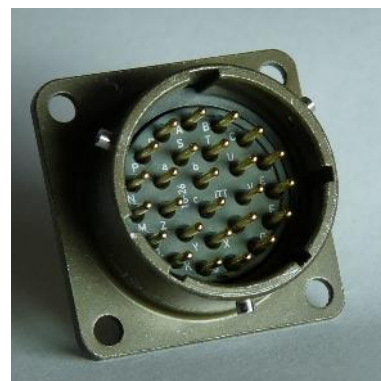
Wiring details for the compatible socket, \*\*\*-12-10S, as seen from the cable end (i.e. during assembly).



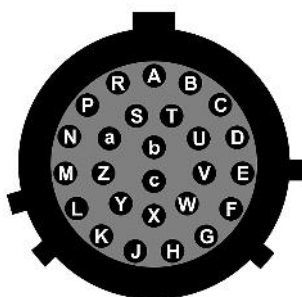
### 14.3.12 Cylinder: SENSOR A & B

This is a standard 26-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-16-26P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-16-26S and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function               | Pin | Function                    |
|-----|------------------------|-----|-----------------------------|
| A   | Vertical velocity +ve  | P   | Calibration signal          |
| B   | Vertical velocity -ve  | R   | Vertical calibration enable |
| C   | N/S velocity +ve       | S   | N/S calibration enable      |
| D   | N/S velocity -ve       | T   | E/W calibration enable      |
| E   | E/W velocity +ve       | U   | Centre                      |
| F   | E/W velocity -ve       | V   | <i>not connected</i>        |
| G   | Vertical mass position | W   | Unlock                      |
| H   | <i>not connected</i>   | X   | Lock                        |
| J   | N/S mass position      | Y   | Logic signal ground         |
| K   | Busy indicator LED     | Z   | <i>not connected</i>        |
| L   | E/W mass position      | a   | <i>not connected</i>        |
| M   | <i>not connected</i>   | b   | Power 0 V                   |
| N   | Signal ground          | c   | Power +10 to +24 V          |



Wiring details for the compatible socket, \*\*\*-16-26S, as seen from the cable end (i.e. during assembly).

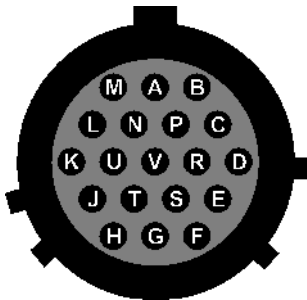
14.3.13 Cylinder: Auxiliary Input

This is a standard 19-pin “mil-spec” plug, conforming to MIL-DTL-26482 (formerly MIL-C-26482). A typical part-number is 02E-14-19P although the initial “02E” varies with manufacturer.

Suitable mating connectors have part-numbers like \*\*\*-14-19S and are available from Amphenol, ITT Cannon and other manufacturers.



| Pin | Function   | Pin | Function                                |
|-----|--|-----|---|
| A   | Optional <i>SENSOR B</i> auxiliary / calibration channel +ve | L   | <i>SENSOR A</i> signal ground           |
| B   | Optional <i>SENSOR B</i> auxiliary / calibration channel –ve | M   | Optional <i>SENSOR B</i> Mux channel M6 |
| C   | Optional <i>SENSOR B</i> signal ground                       | N   | Digital ground                          |
| D   | Optional <i>SENSOR B</i> Mux channel M3                      | P   | <i>not connected</i>                    |
| E   | Optional <i>SENSOR B</i> Mux channel M4                      | R   | <i>SENSOR A</i> Mux channel MB          |
| F   | Optional <i>SENSOR B</i> Mux channel M7                      | S   | <i>SENSOR A</i> Mux channel MC          |
| G   | <i>not connected</i>   | T   | <i>SENSOR A</i> Mux channel MF          |
| H   | Optional <i>SENSOR B</i> Mux channel M5                      | U   | <i>SENSOR A</i> Mux channel MD          |
| J   | <i>SENSOR A</i> auxiliary / calibration channel +ve          | V   | <i>SENSOR A</i> Mux channel ME          |
| K   | <i>SENSOR A</i> auxiliary / calibration channel –ve          |     |   |













Wiring details for the compatible socket, \*\*\*-14-19S, as seen from the cable end (i.e. during assembly).

## 14.4 Using Minicom



The CMG-EAM includes the Linux program minicom as a terminal emulator for use with serial devices, including Güralp digitisers. The following is part of the minicom man page.

Minicom is window based. To pop up a window with the function you want, hold the **Ctrl** key while typing **A** (from now on, we will use **Ctrl** + **A** to denote this), and then the function key (a-z or A-Z). By pressing **Ctrl** + **A** first and then **Z**, a help screen comes up with a short summary of all commands.

For every menu the following keys can be used:

- UP  or 
- DOWN  or 
- LEFT  or 
- RIGHT  or 
- CHOOSE 
- CANCEL 

The screen is divided into two portions: the upper 24 lines are the terminal-emulator screen. In this window, ANSI or VT100 escape sequences are interpreted. If there is a line left at the bottom, a status line is placed there. If this is not possible the status line will be showed every time you press **Ctrl** + **A**. On terminals that have a special status line, it will be used if the termcap information is complete and the -k flag has been given. Possible commands are listed next, in alphabetical order.

-  Pressing **Ctrl** + **A** a second time will just send a **Ctrl** + **A** to the remote system. If you have changed your "escape character" to something other than **Ctrl** + **A**, this works analogously for that character.
-  Toggle 'Add Linefeed' on/off. If it is on, a linefeed is added before every carriage return displayed on the screen.

- B** Gives you a scroll back buffer. You can scroll up with **U**, down with **D**, a page up with **B**, a page down with **F** and, if you have them, the **←** **→** **↑** **↓** and **Page Up** **Page Down** keys can also be used. You can search for text in the buffer with **S** (case-sensitive) or **↑** + **S** (case-insensitive). **N** will find the next occurrence of the string. **C** will enter citation mode. A text cursor appears and you specify the start line by hitting **↵** key. Then scroll back mode will finish and the contents with prefix '>' will be sent.
- C** Clears the screen.
- E** Toggle local echo on and off.
- F** A break signal is sent.
- I** Toggle the type of escape sequence that the cursor keys send between normal and applications mode. (See also the comment about the status line below).
- J** Jump to a shell. On return, the whole screen will be redrawn.
- K** Clears the screen, runs kermit and redraws the screen upon return.
- L** Turn Capture file on off. If turned on, all output sent to the screen will be captured in the file too.
- O** Configure minicom. Puts you in the configuration menu.
- P** Communication Parameters. Allows you to change the bps rate, parity and number of bits.
- Q** Exit minicom without resetting the modem. If macros changed and were not saved, you will have a chance to do so.
- R** Receive files. Choose from various protocols (external). If you have the filename selection window and the prompt for download directory enabled, you'll get a selection window for choosing the directory for downloading. Otherwise the download directory defined in the Filenames and paths menu will be used.

- S** Send files. Choose the protocol like you do with the receive command. If you don't have the filename selection window enabled (in the File transfer protocols menu), you'll just have to write the filename(s) in a dialog window. If you have the selection window enabled, a window will pop up showing the filenames in your upload directory. You can tag and untag filenames by pressing spacebar, and move the cursor up and down with the cursor keys or j/k. The selected filenames are shown highlighted. Directory names are shown [within brackets] and you can move up or down in the directory tree by pressing the spacebar twice. Finally, send the files by pressing ENTER or quit by pressing ESC.
- T** Choose Terminal emulation: Ansi(color) or vt100. You can also change the backspace key here, turn the status line on or off, and define delay (in milliseconds) after each newline if you need that.
- W** Toggle line-wrap on/off.
- X** Exit minicom, reset modem. If macros changed and were not saved, you will have a chance to do so.
- Y** Paste a file. Reads a file and sends its contents just as if it would be typed in.
- Z** Pop up the help screen.

## 15 Revision history

---

|            |   |   |
|------------|---|---|
| 2008-03-16 | A | New document  |
| 2009-06-16 | B | Major re-write for GDI. First official release.                                     |
| 2010-02-10 | C | Complete re-ordering and re-write. Additional material for authenticated digitisers |