Post-GDB Setup – Triggers, CAP and Modbus

This document serves as a detailed summary of the key steps in configuring your devices, configuring Discovery, and testing the system all together.

Once the Güralp Data Box (GDB) has been connected to the network and the devices have been added to the GDC as well as the registry, we recommend taking additional steps to ensure that the Fortimus unit(s) have been correctly configured to trigger based on significant motion and send a CAP Message to the correct location.

0. System Overview

After following the Quick Start Guide for Güralp Data Box you should have:

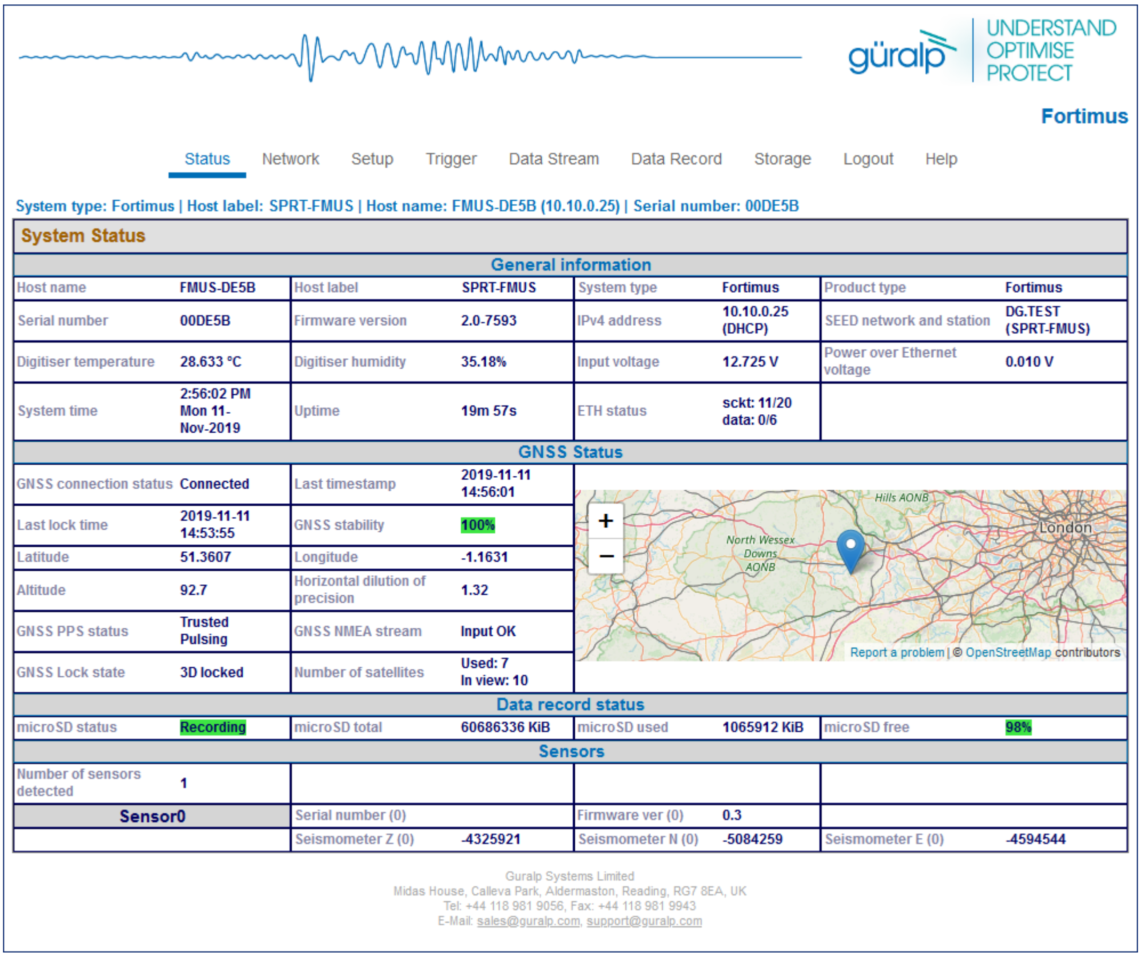
- A Güralp Data Centre ready to record and archive MiniSEED records
- A Discovery pre-configured to
  - Start automatically (if closed opens again after 20 seconds)
  - Start a Modbus server automatically (port **11502**)
  - Start a CAP Receiver automatically (port **11900**)
- Example Python scripts used to query the Modbus server
- Our Testing Utility Toolkit used for sending test CAP messages

This hands-free setup will allow you to find the best way to integrate your system with the various State of Health and critical alarm features we offer. When setup is complete the system can be queried by a Modbus client and as seismic events occur they will be recorded, downloads of event MiniSEED will happen automatically, the event will be reflected in the Modbus server, and Discovery will setup waiting for the next event.

1. Configuring the Fortimus

1.1 Configuring Triggers on the Fortimus

The Fortimus configuration page can be accessed through a web browser on any device on the local network, by typing in the IP address of the sensor. Alternatively, it can be accessed through Discovery on any device by right-clicking the name of the device -> View Web Page. The following page should now be visible.



System type: Fortimus | Host label: SPRT-FMUS | Host name: FMUS-DE5B (10.10.0.25) | Serial number: 00DE5B

System Status

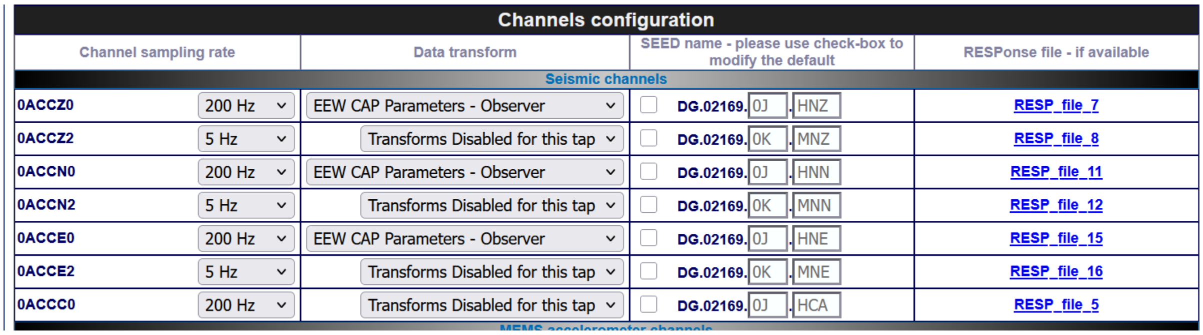
General information							
Host name	FMUS-DE5B	Host label	SPRT-FMUS	System type	Fortimus	Product type	Fortimus
Serial number	00DE5B	Firmware version	2.0-7593	IPv4 address	10.10.0.25 (DHCP)	SEED network and station	DG.TEST (SPRT-FMUS)
Digitiser temperature	28.633 °C	Digitiser humidity	35.18%	Input voltage	12.725 V	Power over Ethernet voltage	0.010 V
System time	2:56:02 PM Mon 11-Nov-2019	Uptime	19m 57s	ETH status	sckt: 11/20 data: 0/6		
GNSS Status							
GNSS connection status	Connected	Last timestamp	2019-11-11 14:56:01				
Last lock time	2019-11-11 14:53:55	GNSS stability	100%				
Latitude	51.3607	Longitude	-1.1631				
Altitude	92.7	Horizontal dilution of precision	1.32				
GNSS PPS status	Trusted Pulsing	GNSS NMEA stream	Input OK				
GNSS Lock state	3D locked	Number of satellites	Used: 7 In view: 10				
Data record status							
microSD status	Recording	microSD total	60686336 KiB	microSD used	1065912 KiB	microSD free	98%
Sensors							
Number of sensors detected	1						
Sensor0		Serial number (0)		Firmware ver (0)	0.3		
		Seismometer Z (0)	-4325921	Seismometer N (0)	-5084259	Seismometer E (0)	-4594544

Guralp Systems Limited
Midas House, Calleva Park, Aldermaston, Reading, RG7 8EA, UK
Tel: +44 118 981 9056, Fax: +44 118 981 9943
E-Mail: sales@guralp.com, support@guralp.com

Figure 1. Fortimus webpage configuration

To configure triggers for each sensor, first navigate to the Data Stream tab. Under the “Channels configuration” header, you will find a list of all channels which can be streamed via SeedLink or GDI, including seismic channels and state of health channels for diagnostic and/or monitoring purposes. Next to each of the channel names, there is a drop-down menu to enable different types of triggering on each of the channels. This is disabled by default. Select the option “EEW CAP Parameters – Observer”. This enables the calculation and sending of peak ground motion values (PGA, PGV, PGD) and has no influence on the seismic data being streamed or recorded.

Be sure to enable the transform for all 3 seismic components (default names 0ACCZ0, 0ACCN0, 0ACCE0) on the channel you wish to enable triggering for. This is compatible with all seismic channels. Once you have done this, the device will need to be rebooted for configuration to apply.



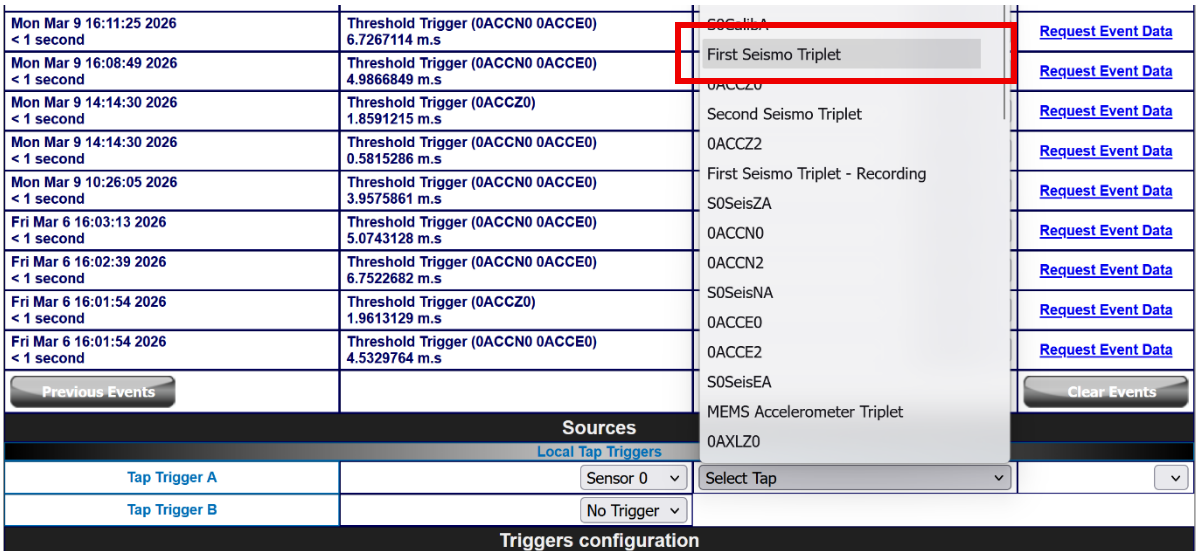
Channels configuration

Channel sampling rate		Data transform	SEED name - please use check-box to modify the default	RESPonse file - if available
Seismic channels				
0ACCZ0	200 Hz	EEW CAP Parameters - Observer	□ DG.02169.0J.HNZ	RESP_file_7
0ACCZ2	5 Hz	Transforms Disabled for this tap	□ DG.02169.0K.MNZ	RESP_file_8
0ACCN0	200 Hz	EEW CAP Parameters - Observer	□ DG.02169.0J.HNN	RESP_file_11
0ACCN2	5 Hz	Transforms Disabled for this tap	□ DG.02169.0K.MNN	RESP_file_12
0ACCE0	200 Hz	EEW CAP Parameters - Observer	□ DG.02169.0J.HNE	RESP_file_15
0ACCE2	5 Hz	Transforms Disabled for this tap	□ DG.02169.0K.MNE	RESP_file_16
0ACCC0	200 Hz	Transforms Disabled for this tap	□ DG.02169.0J.HCA	RESP_file_5

MEMS accelerometer channels

Figure 2. Transforms can be enabled via the drop-down menu for all channels under the Data Stream tab

Once the device has finished rebooting, navigate to the Trigger tab. Below the seismic event table is the heading titled Sources. Using the drop down menu, change "No Trigger" to "Sensor 0" and additional options will become available. Under "Select Tap", there will be an option for "First Seismo Triplet".



Mon Mar 9 16:11:25 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 6.7267114 m.s	Request Event Data
Mon Mar 9 16:08:49 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 4.9866849 m.s	Request Event Data
Mon Mar 9 14:14:30 2026 < 1 second	Threshold Trigger (0ACCZ0) 1.8591215 m.s	Request Event Data
Mon Mar 9 14:14:30 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 0.5815286 m.s	Request Event Data
Mon Mar 9 10:26:05 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 3.9575861 m.s	Request Event Data
Fri Mar 6 16:03:13 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 5.0743128 m.s	Request Event Data
Fri Mar 6 16:02:39 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 6.7522682 m.s	Request Event Data
Fri Mar 6 16:01:54 2026 < 1 second	Threshold Trigger (0ACCZ0) 1.9613129 m.s	Request Event Data
Fri Mar 6 16:01:54 2026 < 1 second	Threshold Trigger (0ACCN0 0ACCE0) 4.5329764 m.s	Request Event Data
Previous Events		Clear Events

Sources

Local Tap Triggers

Tap Trigger A	Sensor 0	Select Tap	
Tap Trigger B	No Trigger		

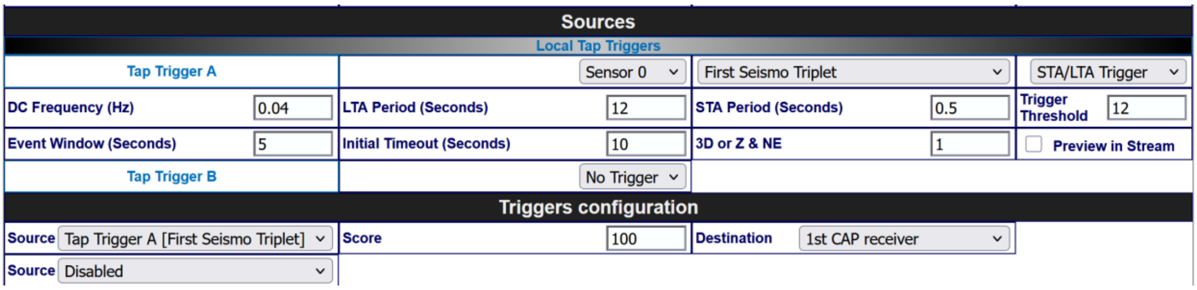
Triggers configuration

Figure 3 Enable First Seismo Triplet as a trigger source

Once done, change "No Trigger" to either "STA/LTA Trigger" or "Threshold Trigger", depending on the triggering algorithm desired, then enter the trigger parameters in the following fields. The triggering threshold (in case of threshold triggering) or the STA/LTA trigger ratio (in the case of STA/LTA triggering) should be configured to the **lowest magnitude desired** to be treated as an event. In other words, this value should be set below or equal to the value which would constitute the lowest level of alarm.

NOTE: When using a seismic triplet as a trigger source, the sensor can be configured to trigger based on the 3D resultant of all 3 seismic components (Z, N & E) or to separate the vertical and horizontal components, and trigger based on the Z component and the 2D resultant of the N and E components separately. Please ensure that the field “3D or Z & NE” has the correct value for your application. (1 for 3D resultant, 0 for separate Z and NE components).

Once the trigger source has been configured, head to the next section down titled Triggers configuration. Select “Tap Trigger A [First Seismo Triplet]”, which is the source created in the previous step. The Score field assigns a ‘weight’ to this trigger, which is used when assessing multiple-source triggers. When multiple instruments are configured under a single trigger, this value is used. Otherwise, it is ignored. For destination select “1st CAP receiver” assuming the case of a single-source trigger.



Sources

Local Tap Triggers

Tap Trigger A			Sensor 0	First Seismo Triplet		STA/LTA Trigger	
DC Frequency (Hz)	0.04	LTA Period (Seconds)	12	STA Period (Seconds)	0.5	Trigger Threshold	12
Event Window (Seconds)	5	Initial Timeout (Seconds)	10	3D or Z & NE	1	□ Preview in Stream	
Tap Trigger B			No Trigger				

Triggers configuration

Source	Tap Trigger A [First Seismo Triplet]	Score	100	Destination	1st CAP receiver		
Source	Disabled						

Figure 4 Example configuration parameters for an STA/LTA trigger on the separated Z and NE components, with a CAP receiver set as the destination

The instrument is now fully configured to trigger based on the selected parameters, and when conditions are met, an event will be recorded in the Seismic Events Table above, containing a timestamp, event duration, the maximum signal difference, and an option to request miniSEED data for the source tap.

1.2 Configuring CAP Messages – Sending

The Fortimus can be configured to send messages using the Common Alerting Protocol (CAP) when the device triggers on a seismic event. Various parameters control how the cap message is generated. Enter the destination IP address for the CAP message (i.e.: the address of the machine hosting the CAP receiver) and the port on which the CAP receiver is listening.

NOTE: In the case where a GDB is hosting the CAP receiver, the default port number used is **11900**. This is not the same as the default port number listed in the Güralp Discovery Software Manual.

Further information on each of the parameters can be found in section 7.17.2 of the Güralp Fortimus Technical Manual available at https://www.guralp.com/documents/MAN-FOR-0002.pdf

2. Configuring CAP Receiver in Discovery

The GDB comes preinstalled with Güralp Discovery, which includes a CAP (Common Alerting Protocol) receiver. It listens on a specified UDP port for incoming CAP messages. When one arrives, it is displayed and plotted on a map. In addition, the receiver can open a TCP connection to the cloud-based registry server and display CAP messages that have been sent to the registry server. All CAP messages can be stored in a log-file. The full message is recorded so that it can be re-loaded later, if required.

Discovery software should automatically start when the GDB receives power. When the main interface has loaded, the CAP receiver function can be accessed using the menu bar under Tools.

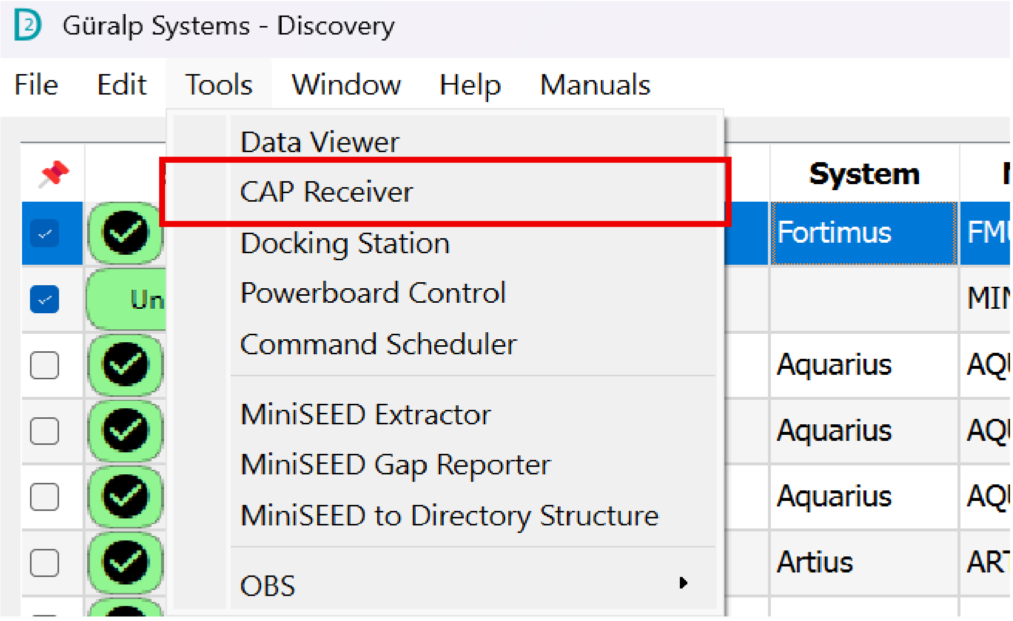
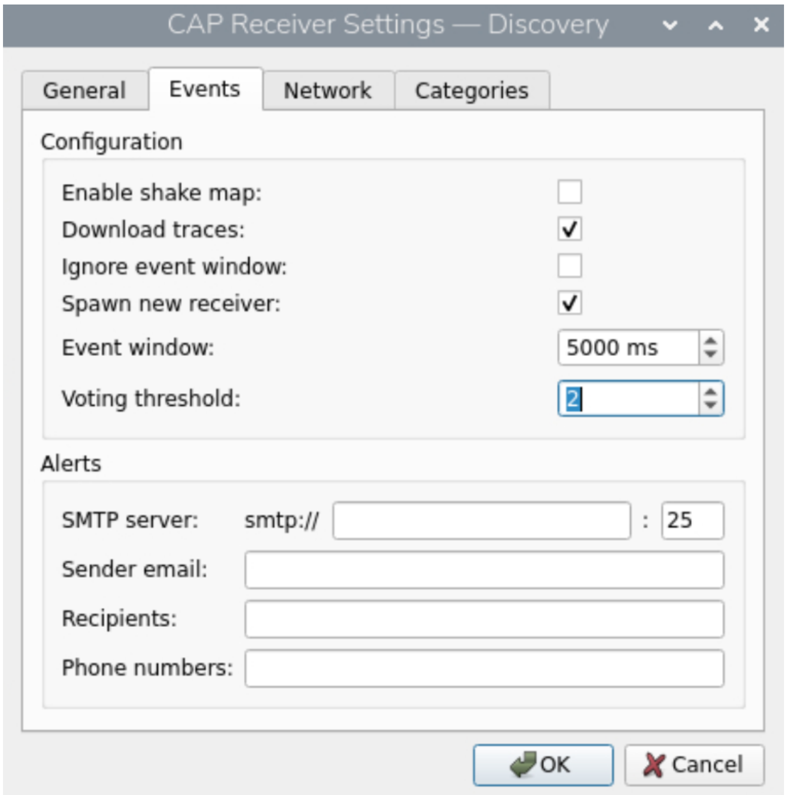


Figure 5 CAP receiver widget in Discovery is accessible through the Tools menu on the main page

When the CAP receiver window opens, navigate to the settings menu. Under the Network tab, ensure that the CAP receiver port number is identical to the destination port number configured on the Fortimus. When hosting a CAP receiver in Discovery on a GDB, the default port number should be **11900**. To start listening for CAP messages on the specified UDP port, click Start. The client is now listening for CAP messages to be sent by the configured devices.

Within the Settings menu, the voting threshold determines the amount of CAP messages that need to be received within the defined event window, before they are deemed "real" and an event is declared. Increasing this number to 2 means that 2 different sensors must trigger simultaneously.



Configuration

Enable shake map: □

Download traces: ☑

Ignore event window: □

Spawn new receiver: ☑

Event window: 5000 ms

Voting threshold: 2

Alerts

SMTP server: smtp:// : 25

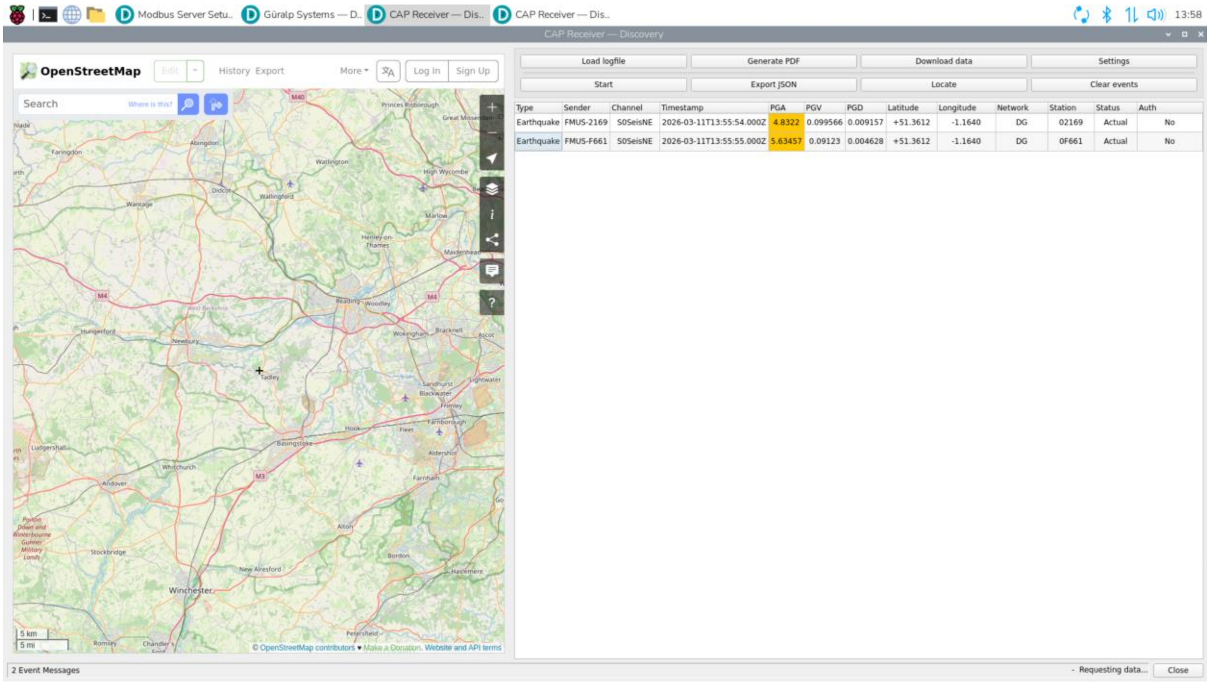
Sender email:

Recipients:

Phone numbers:

Figure 6 The CAP receiver can be configured to require a certain number of messages to be received within a period of time before an event is declared

When a sensor configured to send CAP messages to an address identifies a seismic event according to the selected parameters, the message will be sent to the CAP receiver and immediately be displayed in the main display window.



Type	Sender	Channel	Timestamp	PGA	PGV	PGD	Latitude	Longitude	Network	Station	Status	Auth
Earthquake	FMUS-2169	S0SeisNE	2026-03-11T13:55:54.000Z	4.8322	0.099566	0.009157	+51.3612	-1.1640	DG	02169	Actual	No
Earthquake	FMUS-F661	S0SeisNE	2026-03-11T13:55:55.000Z	5.63457	0.09123	0.004628	+51.3612	-1.1640	DG	0F661	Actual	No

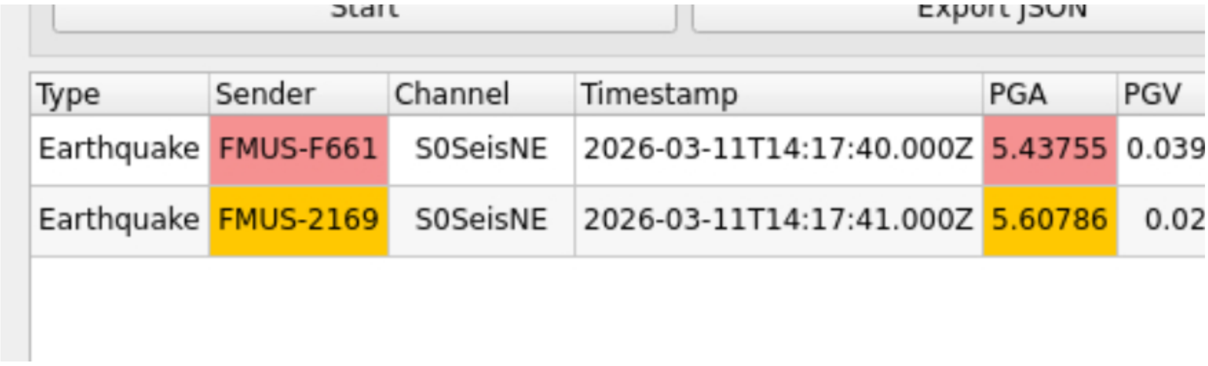
2 Event Messages

Figure 7 CAP receiver after receiving 2 CAP messages from 2 Fortimus, featuring system and seimic information in the table on the right

The column headers in the table are configurable in Settings, giving a range of useful information from the CAP messages. Colour coding schemes are used for the peak ground movement columns and optionally for the Sender column if Site Fragility is enabled. If Site Fragility is enabled, colour coding and categorisation of events into different severities is customisable on a sensor-by-sensor basis.

Site Fragility Threshold	**Colour**	**Corresponding Modbus Alarm**
Safe	Green	None
Warning	Yellow	System Alarm High
Warning-High	Orange	System Alarm High
Danger	Red	System Alarm High-High

Figure 8 table of different configurable site fragility thresholds, with corresponding CAP receiver colour codes and Modbus System Alarm



Type	Sender	Channel	Timestamp	PGA	PGV
Earthquake	FMUS-F661	S0SeisNE	2026-03-11T14:17:40.000Z	5.43755	0.039
Earthquake	FMUS-2169	S0SeisNE	2026-03-11T14:17:41.000Z	5.60786	0.02

Figure 9 Custom site fragility file allows for customised colour coding of PGA severity

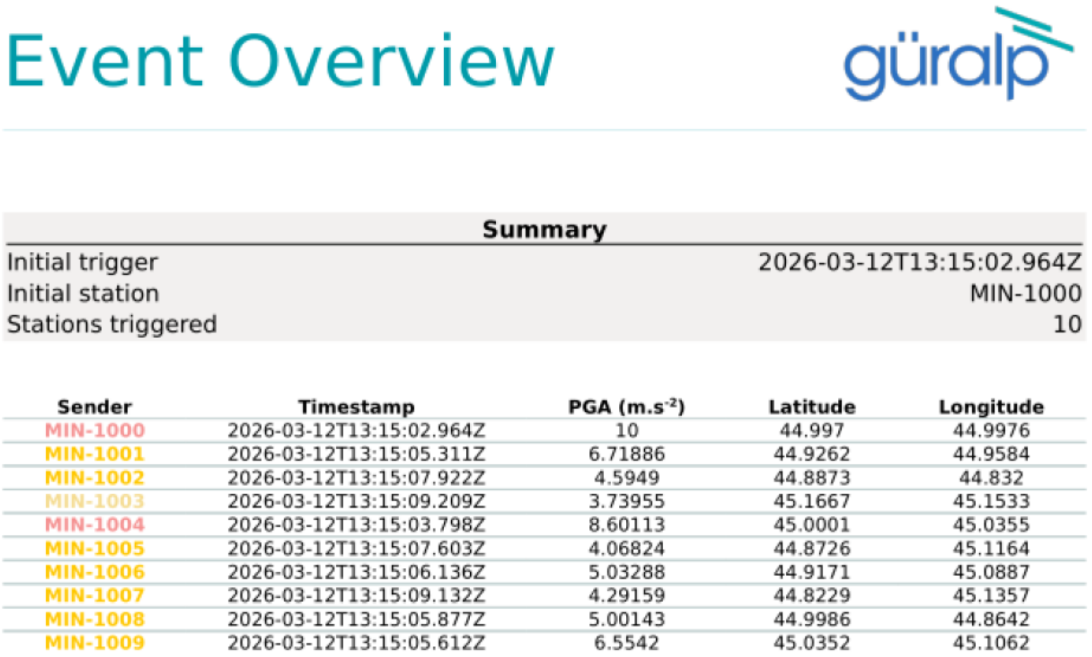
For further information about Site Fragility and configuration, please see section 5.1.3 of the Discovery Software Manual.

As visible in the above example, the event detected at FMUS-F661 is classified as a high "Danger" event (red) despite recording a lower PGA than the recording at FMUS-2169 (5.43755 < 5.60786) which is classified as a "Warning-High" event. This configuration allows the user to monitor sensors individually according to their relative significance. For example, an event detected by sensor contained within a steel enclosure at a construction site may hold more significance than a sensor far from the site at an office building and can thus be configured with more sensitive severity thresholds.

Once an event has occurred, the resulting information can be exported as a PDF by clicking the Generate PDF button. The file will be stored in the folder:

/home/guralp/.config/Guralp Systems/Discovery/CAPReceiver/

In a folder timestamped at the time of the event. The file storage path can be configured in the Settings menu of the CAP receiver. Within this folder you will find the generated PDF, alongside a log of the raw CAP messages received, as well as a JSON file for exporting the data to other software.



Event Overview

Summary	
Initial trigger	2026-03-12T13:15:02.964Z
Initial station	MIN-1000
Stations triggered	10

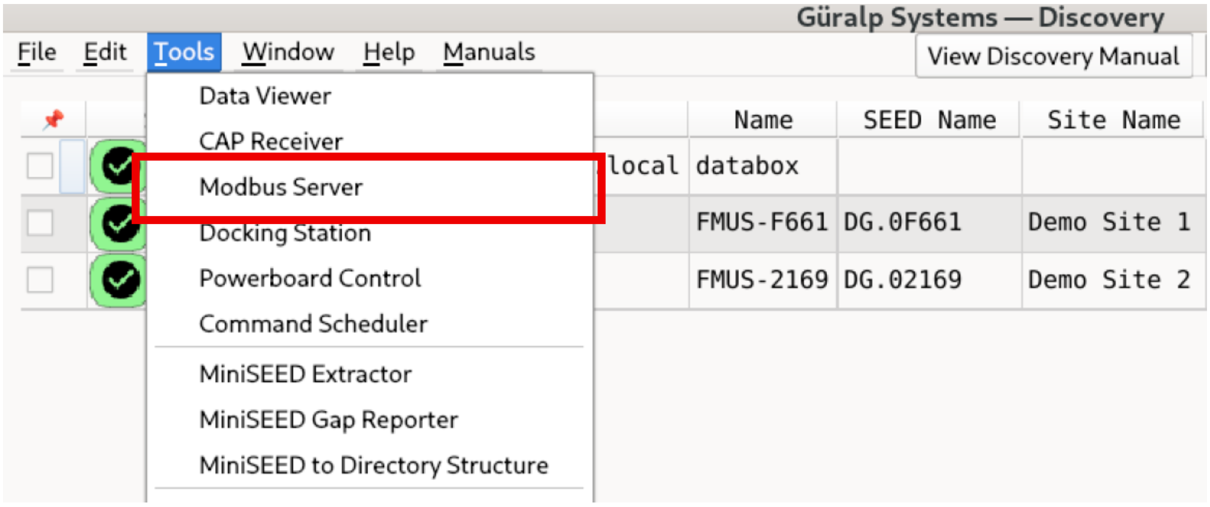
Sender	Timestamp	PGA (m.s^{-2})	Latitude	Longitude
MIN-1000	2026-03-12T13:15:02.964Z	10	44.997	44.9976
MIN-1001	2026-03-12T13:15:05.311Z	6.71886	44.9262	44.9584
MIN-1002	2026-03-12T13:15:07.922Z	4.5949	44.8873	44.832
MIN-1003	2026-03-12T13:15:09.209Z	3.73955	45.1667	45.1533
MIN-1004	2026-03-12T13:15:03.798Z	8.60113	45.0001	45.0355
MIN-1005	2026-03-12T13:15:07.603Z	4.06824	44.8726	45.1164
MIN-1006	2026-03-12T13:15:06.136Z	5.03288	44.9171	45.0887
MIN-1007	2026-03-12T13:15:09.132Z	4.29159	44.8229	45.1357
MIN-1008	2026-03-12T13:15:05.877Z	5.00143	44.9986	44.8642
MIN-1009	2026-03-12T13:15:05.612Z	6.5542	45.0352	45.1062

Figure 10 Results of an event declared by the CAP receiver can be exported as a PDF for easier analysis

The event data will automatically be downloaded in miniSEED format to the same event folder. The data will be separated by individual seismic channels for further inspection using Discovery's built-in Data Viewer, or other tools such as ObsPy. The time window for which data is recorded before and after an event occurs can be configured in the Settings menu under the Network heading -> Download request range.

3. Configuring Modbus Server in Discovery

The Modbus Server tool within Güralp Discovery allows for a Modbus TCP Server to be hosted from a device running the Discovery software. This enables the communication of information from a Discovery program to an outside client via the Modbus Protocol. When run at startup, Discovery automatically begins hosting a Modbus server on the default port **11502**. To access configuration, the Modbus Server widget is accessible from the Tools menu in the main interface.



	Name	SEED Name	Site Name
local	databox		
	FMUS-F661	DG.0F661	Demo Site 1
	FMUS-2169	DG.02169	Demo Site 2

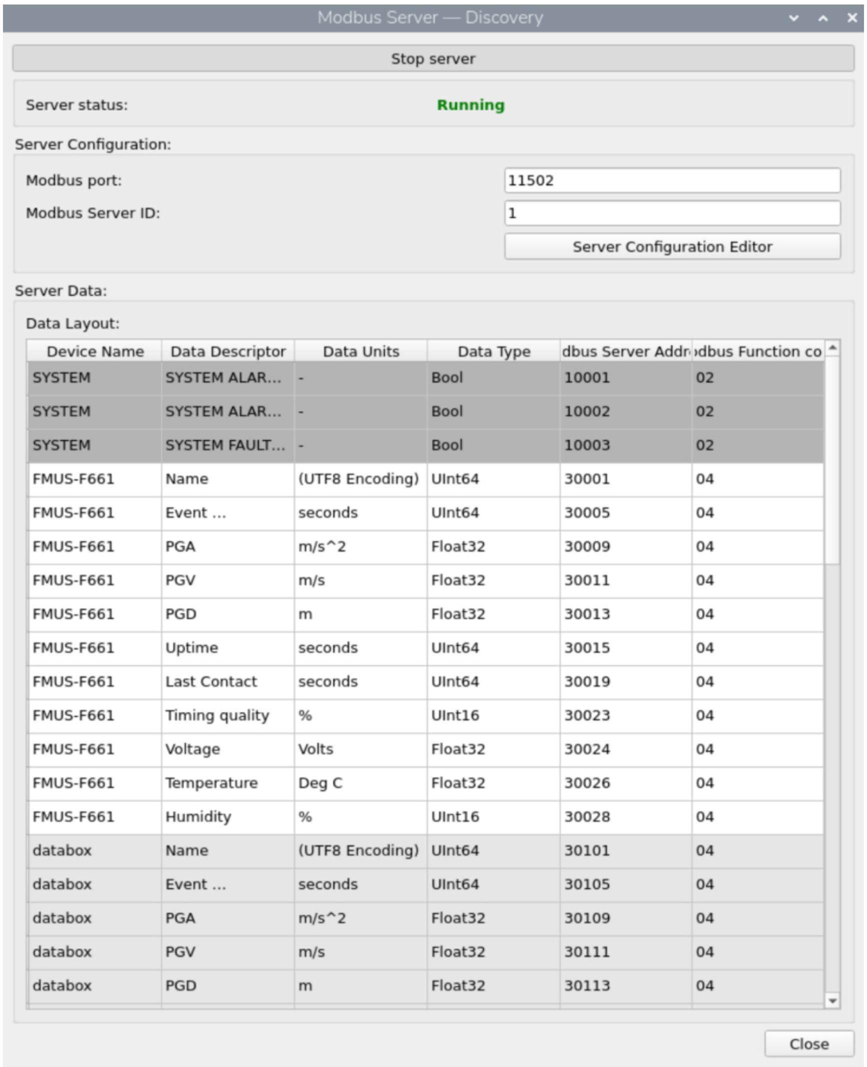
Figure 11 Discovery features a Modbus Server widget which enables communication of information to an outside client

Within the Modbus Server widget, Discovery displays a Data Layout Table which displays key information about the contents being hosted on the server. Further configuration options in the Server Configuration menu allow the user to select which devices should be included on the Modbus server, as well as whether the system alarms should be reset upon register query or be held for a set timeout.

Under the default configuration, the Modbus Server will set up three different alarms, which will alert the user to a change in circumstances that demand the user’s attention. These alarms are as follows:

- System Alarm High: this indicates that ground movement has been detected, with PGA exceeding the user-defined “Safe” threshold but below the “Danger” threshold.
- System Alarm High-High: this indicates that ground movement has been detected with PGA exceeding the user-defined “Danger” threshold.

Further information about the contents of the server can be found in Section 5.2 of the Discovery Software Manual.



Modbus Server — Discovery

Stop server

Server status: **Running**

Server Configuration:

Modbus port: 11502

Modbus Server ID: 1

Server Configuration Editor

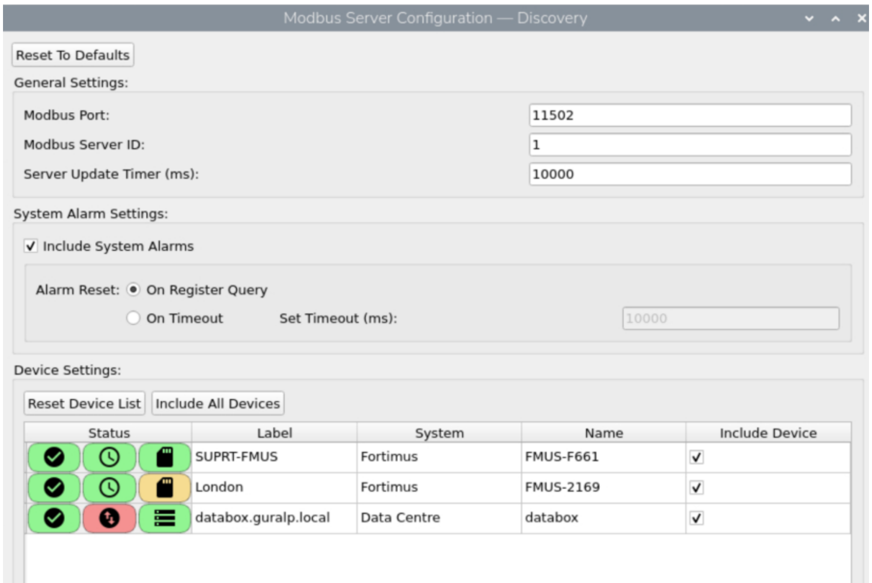
Server Data:

Data Layout:

Device Name	Data Descriptor	Data Units	Data Type	dbus Server Addr	›dbus Function co
SYSTEM	SYSTEM ALAR...	-	Bool	10001	02
SYSTEM	SYSTEM ALAR...	-	Bool	10002	02
SYSTEM	SYSTEM FAULT...	-	Bool	10003	02
FMUS-F661	Name	(UTF8 Encoding)	UInt64	30001	04
FMUS-F661	Event ...	seconds	UInt64	30005	04
FMUS-F661	PGA	m/s^2	Float32	30009	04
FMUS-F661	PGV	m/s	Float32	30011	04
FMUS-F661	PGD	m	Float32	30013	04
FMUS-F661	Uptime	seconds	UInt64	30015	04
FMUS-F661	Last Contact	seconds	UInt64	30019	04
FMUS-F661	Timing quality	%	UInt16	30023	04
FMUS-F661	Voltage	Volts	Float32	30024	04
FMUS-F661	Temperature	Deg C	Float32	30026	04
FMUS-F661	Humidity	%	UInt16	30028	04
databox	Name	(UTF8 Encoding)	UInt64	30101	04
databox	Event ...	seconds	UInt64	30105	04
databox	PGA	m/s^2	Float32	30109	04
databox	PGV	m/s	Float32	30111	04
databox	PGD	m	Float32	30113	04

Close

Figure 12 Modbus Server widget in Discovery, featuring a Data Layout Table to aid navigation of the registers in which system alarms and sensor information are stored



Modbus Server Configuration — Discovery

Reset To Defaults

General Settings:

Modbus Port: 11502

Modbus Server ID: 1

Server Update Timer (ms): 10000

System Alarm Settings:

☑ Include System Alarms

Alarm Reset: ● On Register Query

○ On Timeout Set Timeout (ms): 10000

Device Settings:

Reset Device List | Include All Devices

Status			Label	System	Name	Include Device
✓	🕒	▮	SUPRT-FMUS	Fortimus	FMUS-F661	☑
✓	🕒	▮	London	Fortimus	FMUS-2169	☑
✓	❗	☰	databox.guralp.local	Data Centre	databox	☑

Figure 13 Modbus Server configuration editor allows you to edit the Modbus port and Server ID number, as well as configure system alarms to update based on a set timeout, or be held until queried.

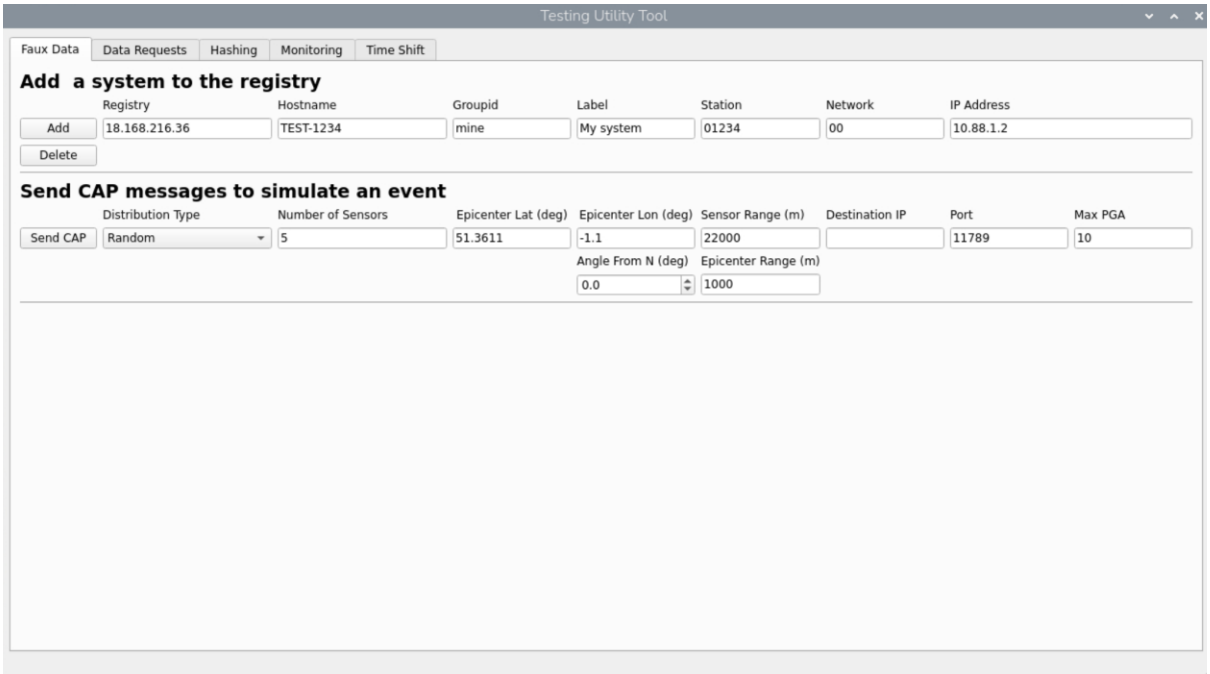
4. Testing Utility Tool – Final Steps

4.1 Testing the CAP Receiver

To test the CAP Receiver's ability to log events without the need for a real event to occur, Güralp provides a testing tool which simulates "triggers" which will send a CAP message to a specified address. This can be used to simulate any sensor deployment configuration, with parameters such as number of sensors, latitude, longitude and maximum PGA all being configurable.

The test tool is installed in /home/guralp/testing_utility_tool and can be opened manually from the file explorer as an executable, or by running the following in a terminal on the GDB:

```
./testing_utility_tool
```



Add a system to the registry

Registry	Hostname	Groupid	Label	Station	Network	IP Address
18.168.216.36	TEST-1234	mine	My system	01234	00	10.88.1.2

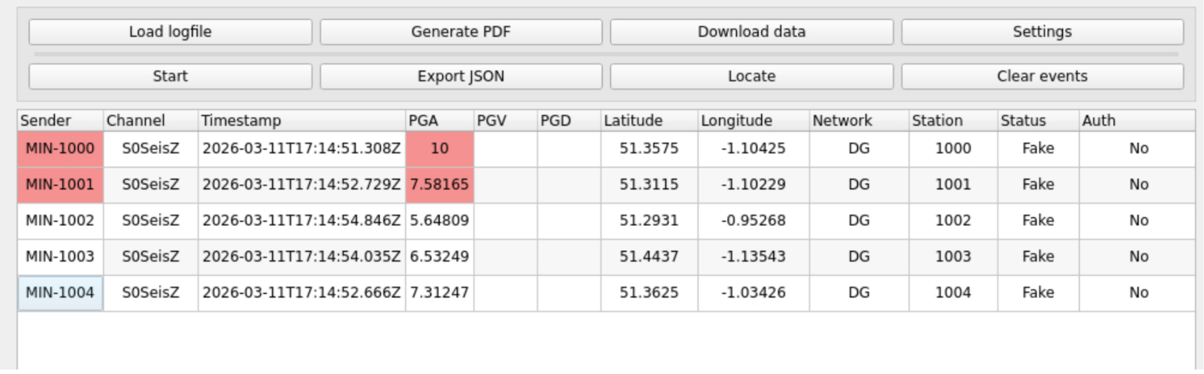
Send CAP messages to simulate an event

Distribution Type	Number of Sensors	Epicenter Lat (deg)	Epicenter Lon (deg)	Sensor Range (m)	Destination IP	Port	Max PGA
Random	5	51.3611	-1.1	22000		11789	10
			Angle From N (deg)	Epicenter Range (m)			
			0.0	1000			

Figure 14 Testing Utility Tool can simulate events from "fake" sensors, which can be used to test that the CAP receiver functions correctly

In the section "Send CAP messages to simulate an event", enter the number of sensors which should be simulated. In the Destination IP field, enter the address of the device hosting the CAP receiver. As the Testing Utility Tool is being run on the same device as the server is being hosted, default localhost address **127.0.0.1** should be applicable for this testing procedure. Ensure the port number also matches the one configured in the CAP receiver (default **11900**). Location and Max PGA values are optional and may be left as default but may be configured to more realistically simulate an event being detected by multiple sensors at a particular site.

Ensure that the Discovery CAP receiver is running and actively listening for CAP messages. Within the Testing Utility Tool, click Start. You should see a similar result to the following in the CAP receiver:



Sender	Channel	Timestamp	PGA	PGV	PGD	Latitude	Longitude	Network	Station	Status	Auth
MIN-1000	S0SeisZ	2026-03-11T17:14:51.308Z	10			51.3575	-1.10425	DG	1000	Fake	No
MIN-1001	S0SeisZ	2026-03-11T17:14:52.729Z	7.58165			51.3115	-1.10229	DG	1001	Fake	No
MIN-1002	S0SeisZ	2026-03-11T17:14:54.846Z	5.64809			51.2931	-0.95268	DG	1002	Fake	No
MIN-1003	S0SeisZ	2026-03-11T17:14:54.035Z	6.53249			51.4437	-1.13543	DG	1003	Fake	No
MIN-1004	S0SeisZ	2026-03-11T17:14:52.666Z	7.31247			51.3625	-1.03426	DG	1004	Fake	No

Figure 15 Fake events can be sent as CAP messages to the CAP receiver in Discovery

Depending on the number of sensors configured, fake CAP messages will be received from devices following the naming convention MIN-1000, MIN-1001, and so on. The PGA will be randomised between 0 and the maximum configured in the Testing Utility Tool, based on a random distance from the epicentre within the configured sensor range.

If the test is successful, you should find a list of fake events in the CAP receiver. this means the CAP receiver is correctly configured and will now be able to display event information when configured sensors trigger.

4.2 Testing the Modbus Server

The GDB contains a Python script which can be used to test communication with the Modbus server. This can be used via the terminal on the GDB. Open a terminal window and enter:

```
./query_modbus_server --ip [IP]
```

Where [IP] is the address of the server host. As the script is being run on the same device as the server is being hosted, default localhost address **127.0.0.1** should be applicable for this testing procedure. The script takes additional arguments in the form of:

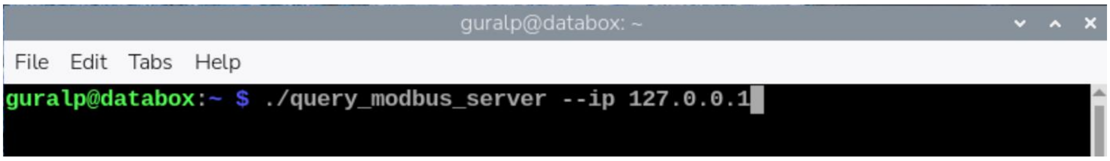
```
./query_modbus_server --ip [IP] --port [PORT] --slave [SLAVE]
```

Where [PORT] is the same port configured in the Modbus Server widget (default **11502**) and slave refers to the register being queried (default 1). The script can be found in

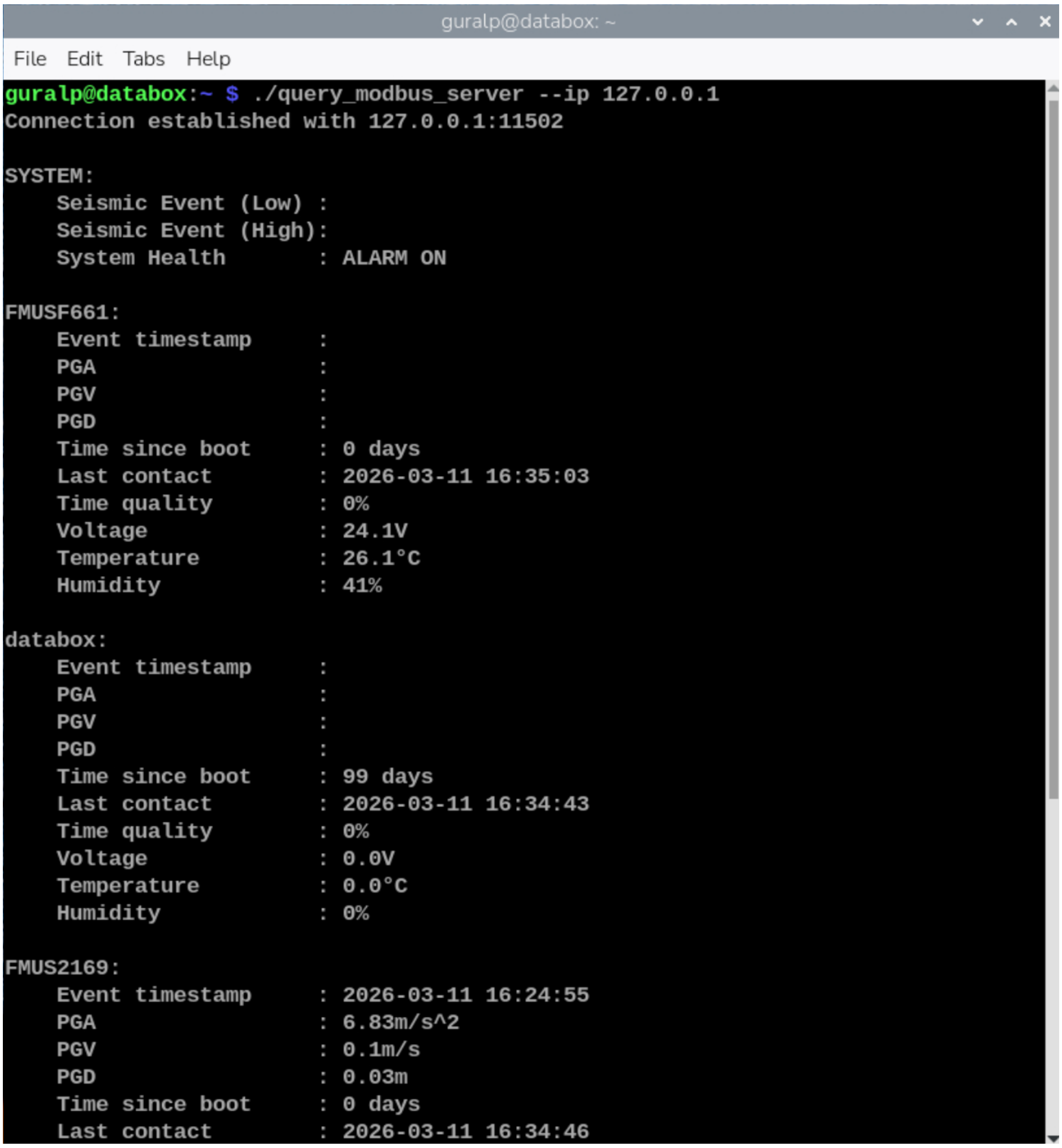
```
/home/guralp/query_modbus_server
```

on the GDB for inspection.

As an example, the script with default arguments and IP address **127.0.0.1** will return all the information hosted on the server. If the server has been correctly configured, the terminal output should look like the following.



```
guralp@databox:~ $ ./query_modbus_server --ip 127.0.0.1
```



```
guralp@databox:~ $ ./query_modbus_server --ip 127.0.0.1
Connection established with 127.0.0.1:11502

SYSTEM:
    Seismic Event (Low) :
    Seismic Event (High):
    System Health       : ALARM ON

FMUSF661:
    Event timestamp     :
    PGA                 :
    PGV                 :
    PGD                 :
    Time since boot     : 0 days
    Last contact        : 2026-03-11 16:35:03
    Time quality        : 0%
    Voltage             : 24.1V
    Temperature         : 26.1°C
    Humidity            : 41%

databox:
    Event timestamp     :
    PGA                 :
    PGV                 :
    PGD                 :
    Time since boot     : 99 days
    Last contact        : 2026-03-11 16:34:43
    Time quality        : 0%
    Voltage             : 0.0V
    Temperature         : 0.0°C
    Humidity            : 0%

FMUS2169:
    Event timestamp     : 2026-03-11 16:24:55
    PGA                 : 6.83m/s^2
    PGV                 : 0.1m/s
    PGD                 : 0.03m
    Time since boot     : 0 days
    Last contact        : 2026-03-11 16:34:46
```

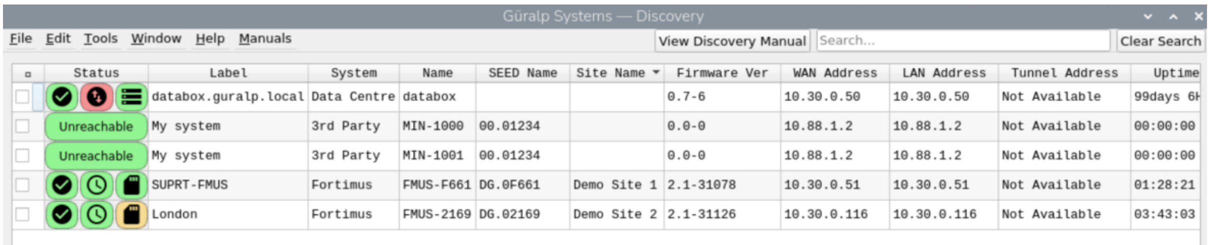
Figure 16 example output of the Python script used to query the Modbus server being hosted by a local Discovery client

You should see a similar output to the one above. If so, then the Modbus server has been correctly configured.

4.3 Testing Communication Between the CAP Receiver and Modbus Server

With both the CAP receiver and Modbus server configured, the last step is to test the link between the two. This can be done by adding the fake sensors used to generate the CAP messages to the GDB registry, simulating an event, and then querying the Modbus server to see if the information is being correctly communicated.

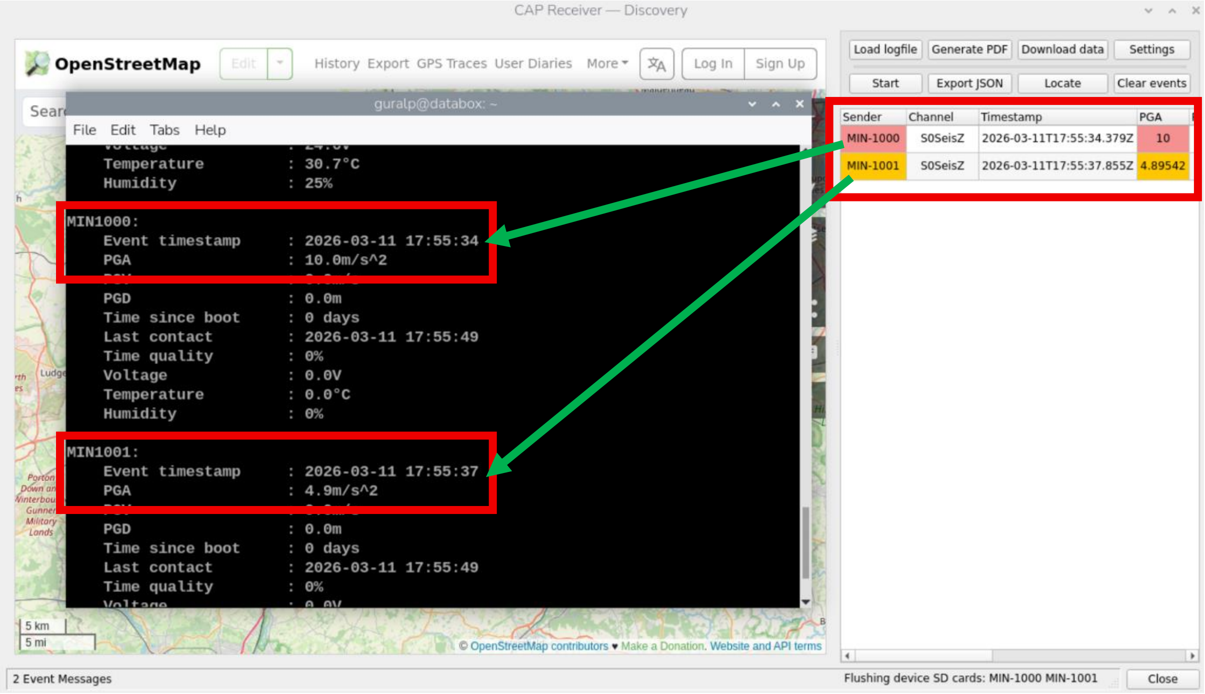
Within the Testing Utility Tool, navigate to the section titled “Add a system to the registry”. Enter the registry address (the IP address of the GDB) and change the Hostname field to MIN-1000. Groupid, Label, Station, Network and IP Address can be left as default. Click Add, and ensure that the fake sensor is now visible in the Registry view of the main Discovery window. Repeat this process as many times as desired, incrementing the Hostname by 1 each time (i.e.: MIN-1001, MIN-1002… etc.).


Güralp Systems — Discovery
File Edit Tools Window Help Manuals
View Discovery Manual
Search...
Clear Search

▫	Status	Label	System	Name	SEED Name	Site Name	Firmware Ver	WAN Address	LAN Address	Tunnel Address	Uptime
□	✓ ● ☰	databox.guralp.local	Data Centre	databox			0.7-6	10.30.0.50	10.30.0.50	Not Available	99days 6H
□	Unreachable	My system	3rd Party	MIN-1000	00.01234		0.0-0	10.88.1.2	10.88.1.2	Not Available	00:00:00
□	Unreachable	My system	3rd Party	MIN-1001	00.01234		0.0-0	10.88.1.2	10.88.1.2	Not Available	00:00:00
□	✓ 🕓 ▮	SUPRT-FMUS	Fortimus	FMUS-F661	DG.0F661	Demo Site 1	2.1-31078	10.30.0.51	10.30.0.51	Not Available	01:28:21
□	✓ 🕓 ▮	London	Fortimus	FMUS-2169	DG.02169	Demo Site 2	2.1-31126	10.30.0.116	10.30.0.116	Not Available	03:43:03

Figure 17 Testing Utility Tool allows the user to add fake devices to a registry

Once the device(s) are visible such as in the image above, ensure that the CAP receiver and Modbus Server are both running and actively listening. Return to the Testing Utility Tool and repeat the steps to send a fake CAP message from the fake sensors. Wait 1-2 seconds to ensure that Discovery has more than enough time to update the Modbus server. Then, re-run the query_modbus_server script from a terminal as done in the Configuring Modbus Server in Discovery section of this document.



```
    Temperature          : 30.7°C
    Humidity             : 25%

MIN1000:
    Event timestamp      : 2026-03-11 17:55:34
    PGA                  : 10.0m/s^2
    PGD                  : 0.0m
    Time since boot      : 0 days
    Last contact         : 2026-03-11 17:55:49
    Time quality         : 0%
    Voltage              : 0.0V
    Temperature          : 0.0°C
    Humidity             : 0%

MIN1001:
    Event timestamp      : 2026-03-11 17:55:37
    PGA                  : 4.9m/s^2
    PGD                  : 0.0m
    Time since boot      : 0 days
    Last contact         : 2026-03-11 17:55:49
    Time quality         : 0%
    Voltage              : 0.0V
```

Sender	Channel	Timestamp	PGA
MIN-1000	S0SeisZ	2026-03-11T17:55:34.379Z	10
MIN-1001	S0SeisZ	2026-03-11T17:55:37.855Z	4.89542

Flushing device SD cards: MIN-1000 MIN-1001

Figure 18 Testing Utility Tool can be used to add fake devices to a registry, which can then be queried via the Modbus server in Discovery when an event has occurred

Verify that the Sender name, Timestamp and PGA obtained from the query match the values configured in the Testing Utility Tool. If these values match, then the CAP receiver and Modbus server are correctly communicating between each other. This means that everything has been correctly configured, and the GDB is prepared to record, monitor and communicate information from seismic sensors on the network. At this point the fake devices may be removed from the GDB registry by repeating the same steps and instead clicking Remove.

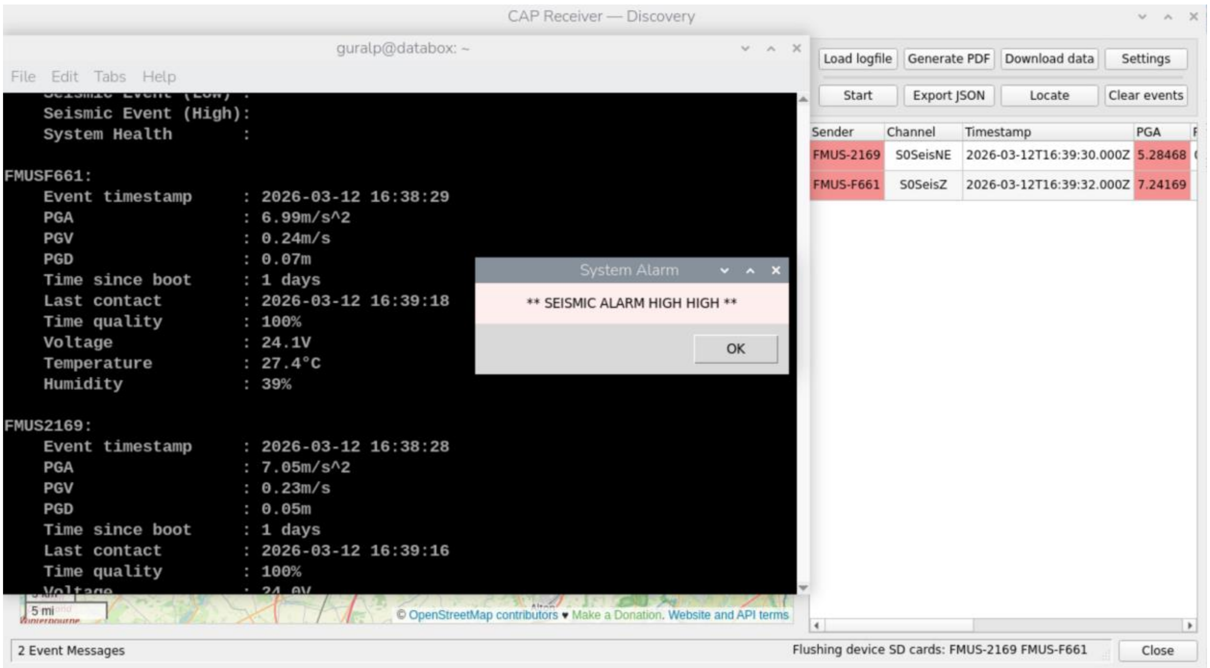
Further Options – Monitoring the Modbus Server

In addition to query_modbus_server the GDB contains a Python script named monitor_modbus_server which automatically queries the Modbus server at a fixed time interval. This program will run in the background and do nothing until there a system alarm is raised, caused either by a system fault or by an event PGA exceeding the user-defined warning threshold using the site fragility function. When this happens, a pop-up window will display the relevant information. The script can be stopped at any time by clicking Quit. The script is stored at

```
/home/guralp/monitor_modbus_server
```

Usage of the script is identical to query_modbus_server, with one additional argument for query interval.

```
./monitor_modbus_server --ip [IP] --port [PORT] --slave [SLAVE] --interval [interval]
```



```
    Seismic Event (Low) :
    Seismic Event (High):
    System Health       :

FMUSF661:
    Event timestamp     : 2026-03-12 16:38:29
    PGA                 : 6.99m/s^2
    PGV                 : 0.24m/s
    PGD                 : 0.07m
    Time since boot     : 1 days
    Last contact        : 2026-03-12 16:39:18
    Time quality        : 100%
    Voltage             : 24.1V
    Temperature         : 27.4°C
    Humidity            : 39%

FMUS2169:
    Event timestamp     : 2026-03-12 16:38:28
    PGA                 : 7.05m/s^2
    PGV                 : 0.23m/s
    PGD                 : 0.05m
    Time since boot     : 1 days
    Last contact        : 2026-03-12 16:39:16
    Time quality        : 100%
    Voltage             : 24.0V
```

** SEISMIC ALARM HIGH HIGH **

Sender	Channel	Timestamp	PGA
FMUS-2169	S0SeisNE	2026-03-12T16:39:30.000Z	5.28468
FMUS-F661	S0SeisZ	2026-03-12T16:39:32.000Z	7.24169

2 Event Messages

Flushing device SD cards: FMUS-2169 FMUS-F661

Figure 19 The GDB contains a Python script which can be used to continuously monitor the Modbus server hosted by Discovery. The script will listen for system alarms declared by the CAP receiver and generate a pop-up window warning the user when an alarm occurs