

Infrastructure Monitoring

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.

19/05/2026 11:23:09

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

Table of Contents

1. System Overview	3
2. Configuring the Fortimus	4
2.1. Configuring Triggers on the Fortimus	4
2.2. Configuring CAP Messages – Sending	6
3. Configuring CAP Receiver in Discovery	7
4. Configuring Modbus Server in Discovery	11
5. Testing Utility Tool – Final Steps	14
5.1. Testing the CAP Receiver	14
5.2. Testing the Modbus Server	15
5.3. Testing Communication Between the CAP Receiver and Modbus Server	17
6. Further Options – Monitoring the Modbus Server	19

1. System Overview

After following this document you should have:

- A Güralp Data Centre ready to record and archive MiniSEED records
- A Discovery pre-configured to:
 - Start automatically (if closed, it 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. Additionally, 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 automatically set up and wait for the next event.



Caution: 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, as well as to confirm that the Modbus server is configured correctly.

2. Configuring the Fortimus

2.1. 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.

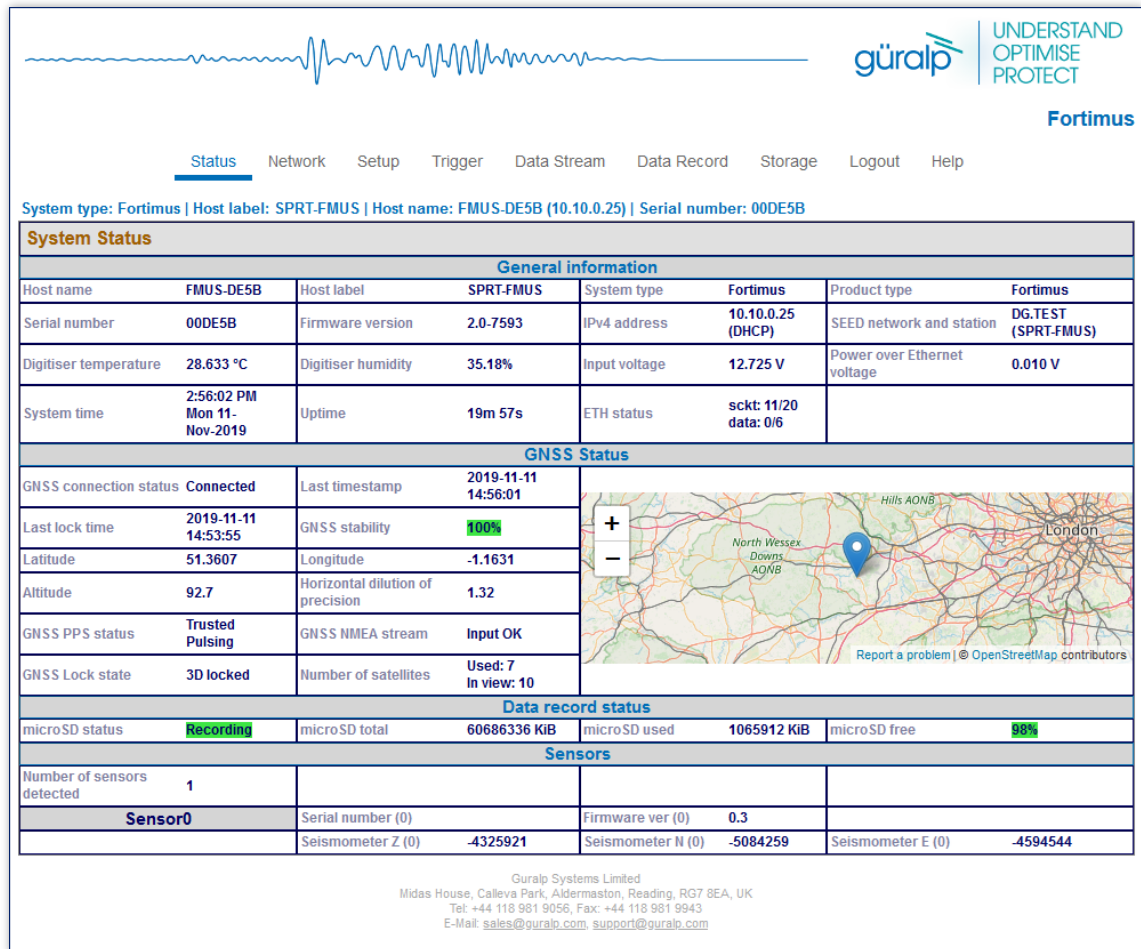


Figure 1. Fortimus webpage configuration

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, 0ACC0) 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	OK 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	OK MNN	RESP_file_12
0ACC0	200 Hz ▾	EEW CAP Parameters - Observer ▾	☐	DG.02169	0J HNE	RESP_file_15
0ACC2	5 Hz ▾	Transforms Disabled for this tap ▾	☐	DG.02169	OK MNE	RESP_file_16
0ACCC0	200 Hz ▾	Transforms Disabled for this tap ▾	☐	DG.02169	0J HCA	RESP_file_5

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 0ACC0)	6.7267114 m.s	50CalbA	Request Event Data
Mon Mar 9 16:08:49 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	4.9866849 m.s	First Seismo Triplet	Request Event Data
Mon Mar 9 14:14:30 2026 < 1 second	Threshold Trigger (0ACCZ0)	1.8591215 m.s	0ACCZ0	Request Event Data
Mon Mar 9 14:14:30 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	0.5815286 m.s	0ACCZ2	Request Event Data
Mon Mar 9 10:26:05 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	3.9575861 m.s	First Seismo Triplet - Recording	Request Event Data
Fri Mar 6 16:03:13 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	5.0743128 m.s	S0SeisZA	Request Event Data
Fri Mar 6 16:02:39 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	6.7522682 m.s	0ACCN0	Request Event Data
Fri Mar 6 16:01:54 2026 < 1 second	Threshold Trigger (0ACCZ0)	1.9613129 m.s	0ACCN2	Request Event Data
Fri Mar 6 16:01:54 2026 < 1 second	Threshold Trigger (0ACCN0 0ACC0)	4.5329764 m.s	S0SeisNA	Request Event Data
Previous Events			0ACC0	Request Event Data
			0ACC2	Request Event Data
			S0SeisEA	Request Event Data
			MEMS Accelerometer Triplet	Request Event Data
			0AXLZ0	Request Event Data
Sources				
Local Tap Triggers				
Tap Trigger A	Sensor 0	Select Tap		
Tap Trigger B	No Trigger			

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. Only when multiple instruments are configured as part of a single trigger is this value used. Otherwise, it is ignored. For the 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)
Event Window (Seconds)	5	Initial Timeout (Seconds)	10	3D or Z & NE
Tap Trigger B		No Trigger		
Triggers configuration				
Source	Tap Trigger A [First Seismo Triplet]	Score	100	Destination
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.

2.2. 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 Guralp Discovery Software Manual.

Further information on each of the parameters can be found in section 2.10.2 of the Guralp Technical Manual available at <https://www.guralp.com/documents/FMUS.pdf>

3. 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**.

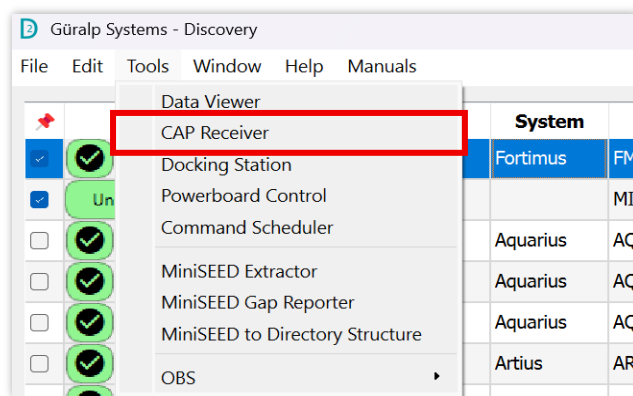


Figure 5 CAP receiver widget in Discovery is accessible through the Tools menu on the main page

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.

Infrastructure monitoring

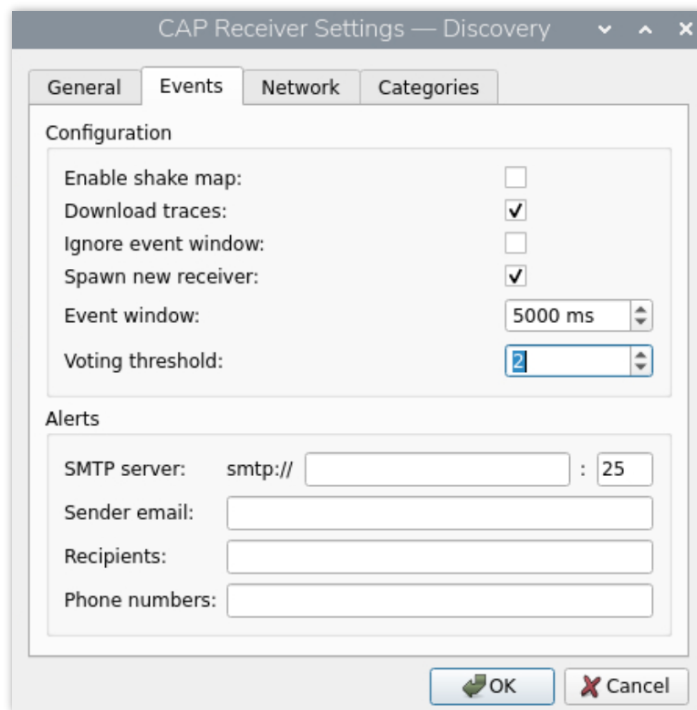


Figure 6 The CAP receiver can be configured to require a certain number of messages to be received within a period of time before an event is declared

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.

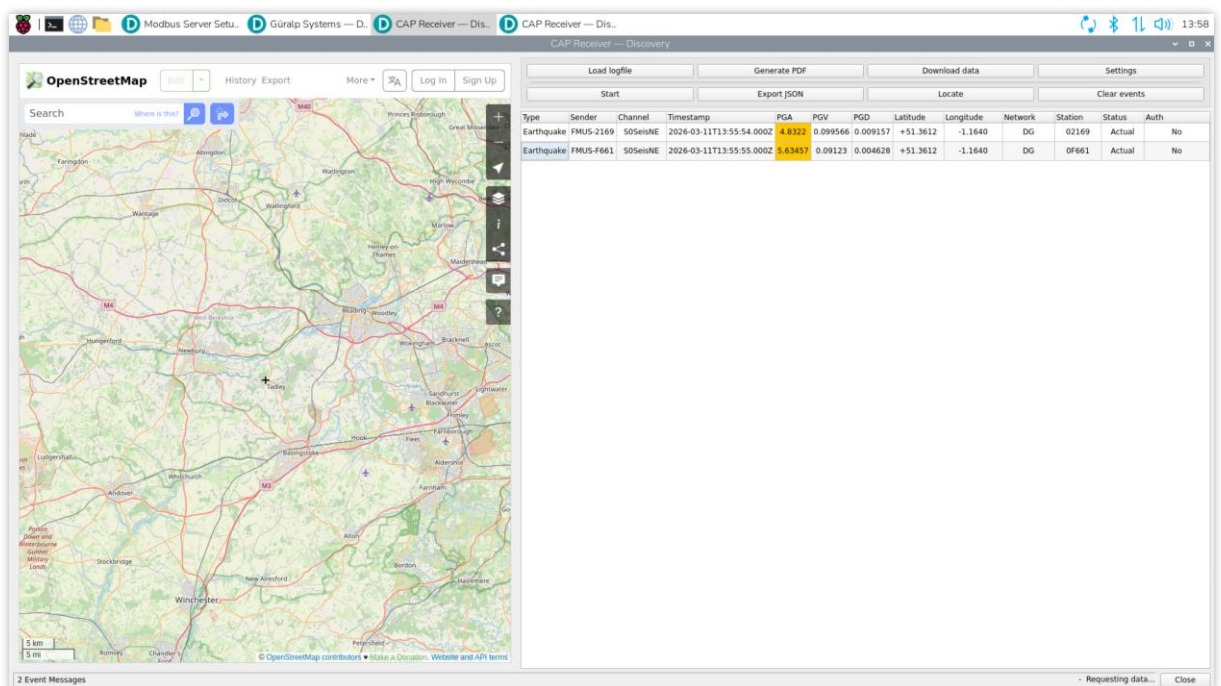
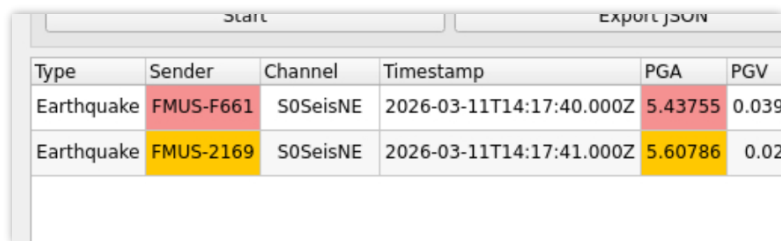


Figure 7 CAP receiver after receiving 2 CAP messages from 2 Fortimus, featuring system and seismic information in the table on the right

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.

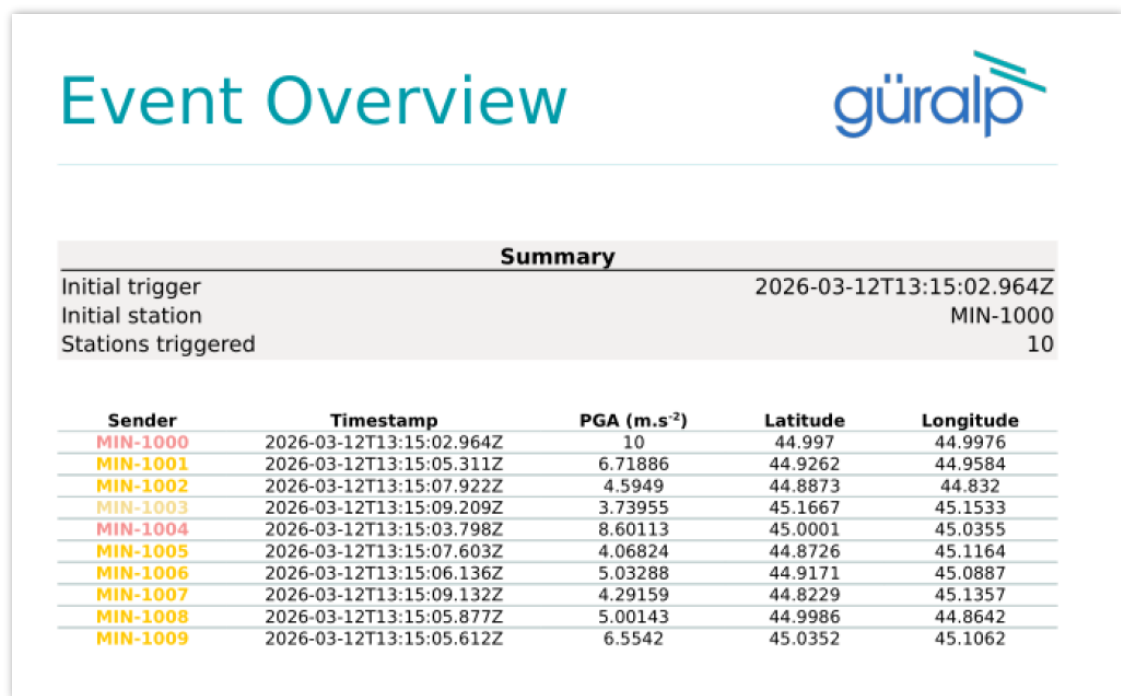


Figure 10 Results of an event declared by the CAP receiver can be exported as a PDF for easier analysis

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.

4. 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.

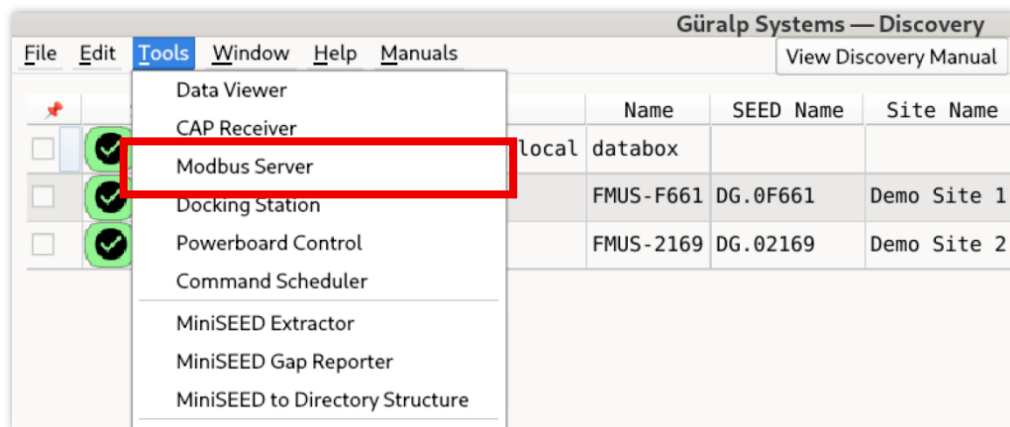


Figure 11 Discovery features a Modbus Server widget which enables communication of information to an outside client

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.
- **System Fault Alarm:** this indicates that a communication, timing, or storage issue has been identified with one or more of the devices from which data is being put in the server. It is tied to the state of health information for each device, displayed in the status column of the Discovery main window.

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

Infrastructure monitoring

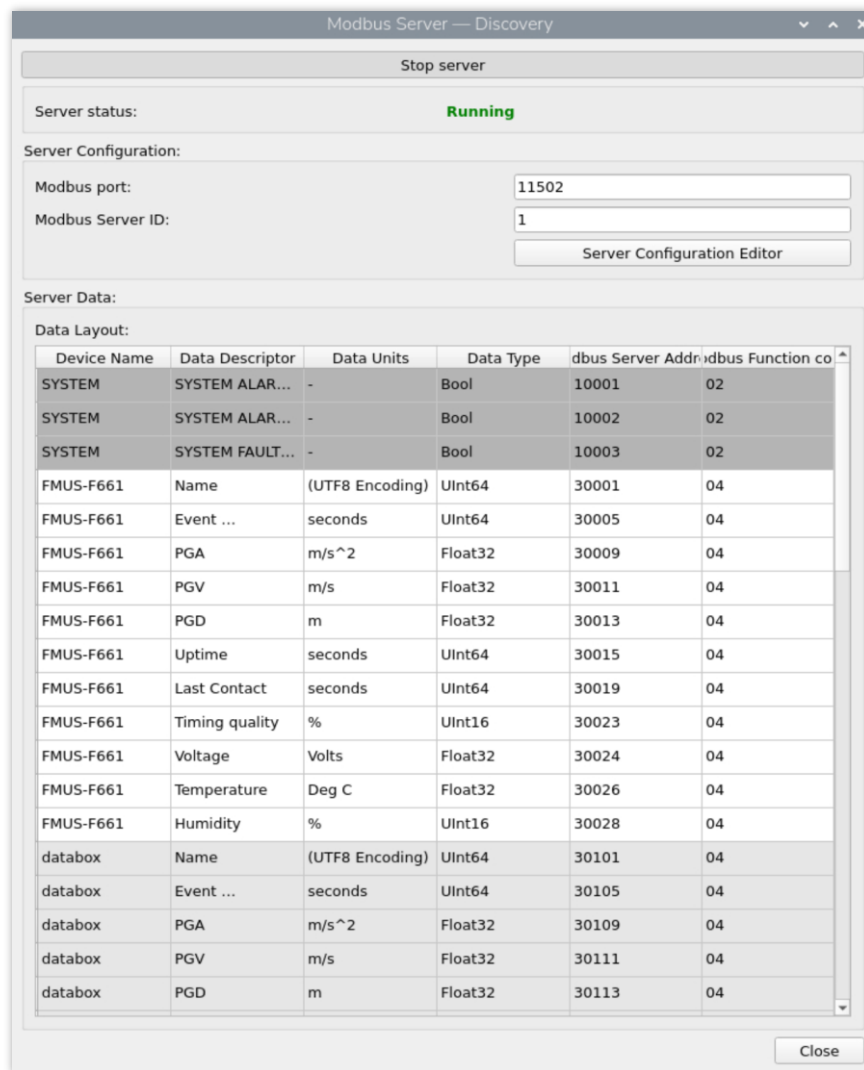


Figure 12 Modbus Server widget in Discovery, featuring a Data Layout Table to aid navigation of the registers in which system alarms and sensor information are stored

Infrastructure monitoring

The image shows a 'Modbus Server Configuration — Discovery' window. It has three main sections: General Settings, System Alarm Settings, and Device Settings. The General Settings section includes fields for Modbus Port (11502), Modbus Server ID (1), and Server Update Timer (10000 ms). The System Alarm Settings section has a checkbox for 'Include System Alarms' (checked) and radio buttons for 'Alarm Reset' (selected: 'On Register Query', unselected: 'On Timeout'), with a 'Set Timeout (ms)' field (10000). The Device Settings section has buttons for 'Reset Device List' and 'Include All Devices', and a table of discovered 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.

5. Testing Utility Tool – Final Steps

5.1. 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
```

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:

Load logfile

Generate PDF

Download data

Settings

Start

Export JSON

Locate

Clear events

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.

Site fragility can be tested using an example file included with the GDB file by enabling site fragility from within the settings widget and uploading the fragility test file. The file is configured with arbitrary safe, warning and danger PGA thresholds for up to 5 test devices added via the Testing Utility Toolkit. (MIN-1000, MIN-1001, MIN-1002, MIN-1003, MIN-1004). The file is found at

```
/home/guralp/fragility_test.csv
```

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

5.2. 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, the default localhost address **127.0.0.1** should be applicable for this testing procedure. The script takes additional arguments in the form of:

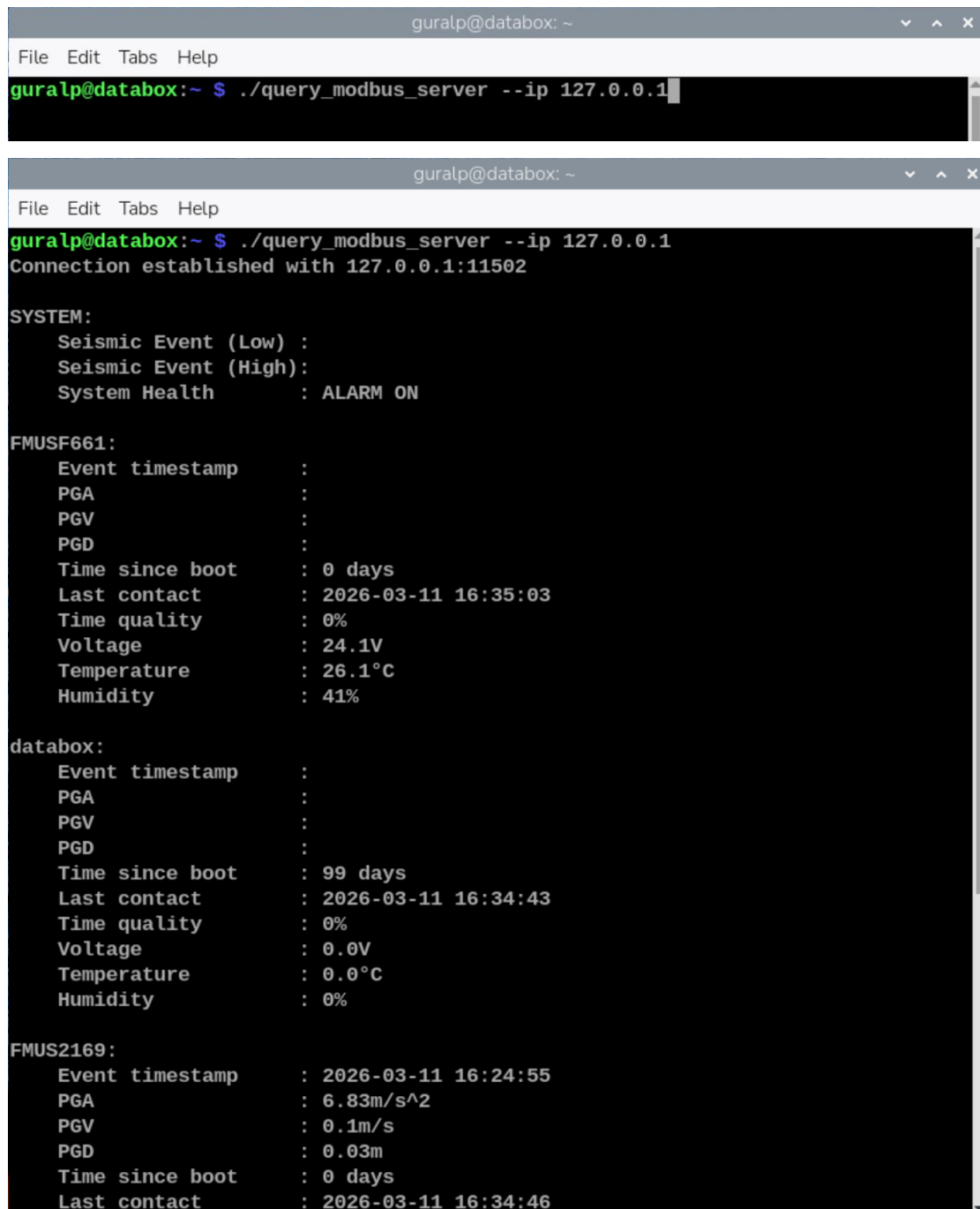
```
./query_modbus_server --ip [IP] --port [PORT] --slave [SLAVE]
```

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: ~  
File Edit Tabs Help  
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
```

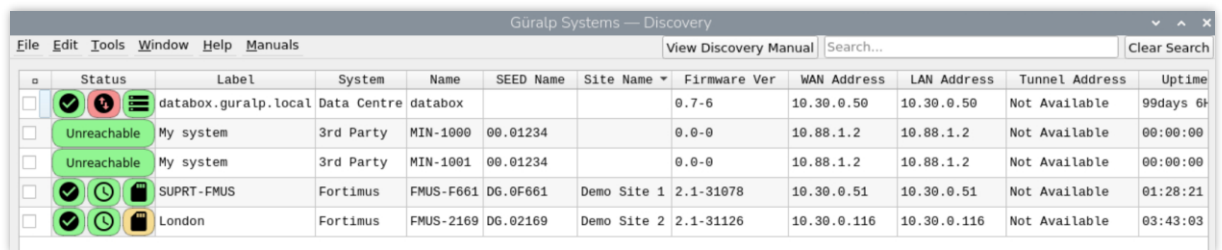
Figure 16 example output of the Python script used to query the Modbus server being hosted by a local Discovery client

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

5.3. 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.).



	Status	Label	System	Name	SEED Name	Site Name	Firmware Ver	WAN Address	LAN Address	Tunnel Address	Uptime
☐		databox.guraip.local	Data Centre	databox			0.7-6	10.30.0.50	10.30.0.50	Not Available	99days 6h
☐		My system	3rd Party	MIN-1000	00.01234		0.0-0	10.88.1.2	10.88.1.2	Not Available	00:00:00
☐		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	D6.0F661	Demo Site 1	2.1-31078	10.30.0.51	10.30.0.51	Not Available	01:28:21
☐		London	Fortimus	FMUS-2169	D6.02169	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.

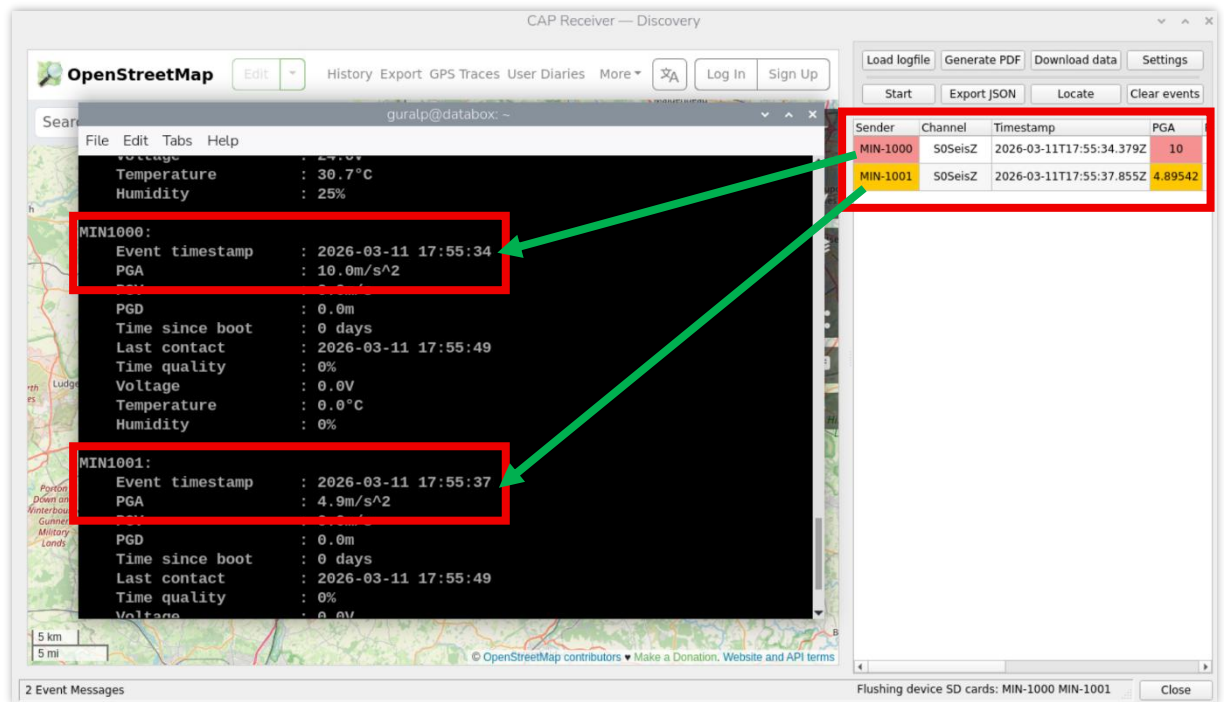


Figure 18 Testing Utility Tool can be used to add fake devices to a registry, which can then be queried via the Modbus server in Discovery when an event has occurred

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.

6. 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 (in seconds).

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

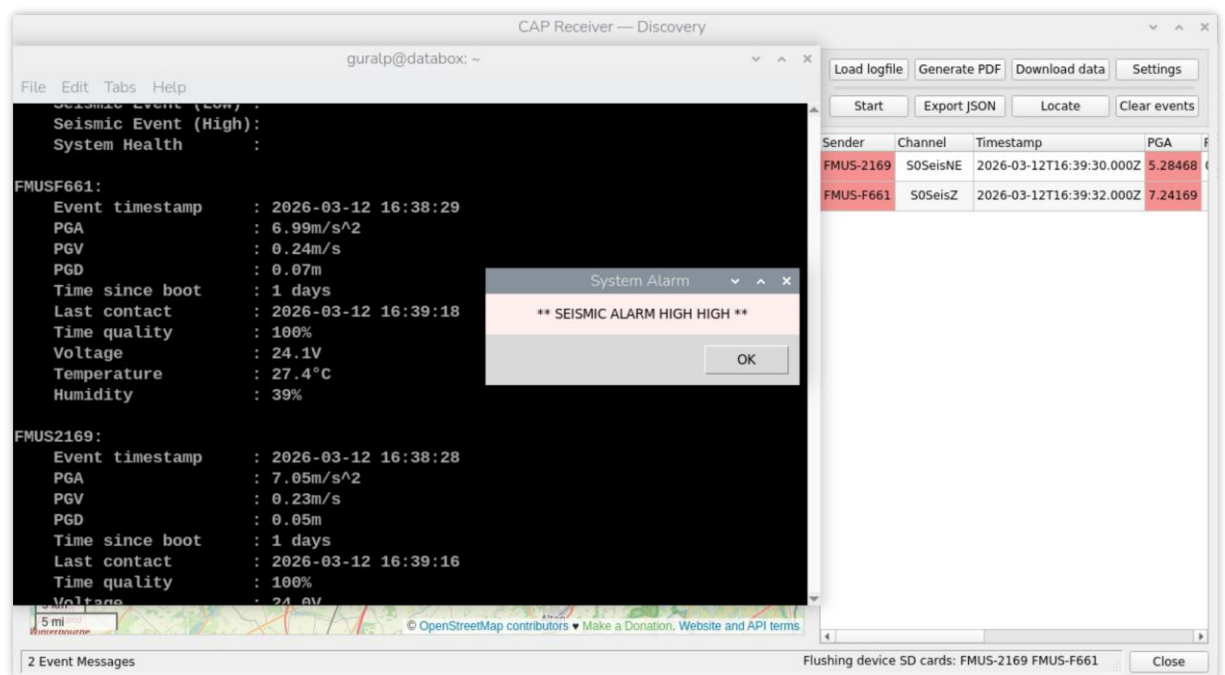


Figure 19 The GDB contains a Python script which can be used to continuously monitor the Modbus server hosted by Discovery. The script will listen for system alarms declared by the CAP receiver and generate a pop-up window warning the user when an alarm occurs