

Greyhound Data Collector - Installers Guide

Greyhound Data Collector (GDC-001-02)

January 9, 2008

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Botech AB.

Document No. BOTECH041007-EN

Printed in Sweden

Copyright © 2003-2006 Botech AB
All Rights Reserved



Botech AB
Ledeburgatan 1
SE-211 55 Malmö
Sweden
<http://www.botech.se>
info@botech.se

Hubit® , Greyhound® and Botech® are registered trademarks of Botech AB.
Other names in this manual are only used in identifying purposes and can be the registered trademarks of their respective owner.

Contents

1	Contact information	6
2	Introduction	7
2.1	Hardware	8
3	Start page	9
4	Schematics	10
5	Alarms	11
5.1	Overview	11
5.2	Statistics	12
5.3	Events	13
5.4	Blocking	13
5.5	Configuration	14
6	Trends	15
6.1	Selection	15
6.2	Scaling	16
6.3	Zoom and Sampling	17
6.4	Export as XLS	18
7	Reports and documents	19
7.1	Value overview	19
7.2	Documents	21
7.2.1	Report templates	22
8	Server logs	25
9	Configuration	28
9.1	Network and system settings	30
9.1.1	eth0 - WAN Network	31
9.1.2	eth1 - LAN Network	32
9.1.3	DNS	32
9.2	POP3	32
9.3	MYSQL	32
9.3.1	Firewall and routing	34
9.3.2	Port forwarding	35
9.3.3	ADSL Login	36
9.3.4	DynDns	37
9.3.5	Modem	38
9.3.6	SSH Port	39
9.3.7	HTTP Port	39
9.3.8	Timezone and NTP	40
9.3.9	System clock	40
9.3.10	System name	41
9.3.11	System password	41
9.4	System info	42
9.5	Datapoints and drivers	43

9.5.1	Overview	43
9.5.2	Greyhound Data Collector address	43
9.5.3	Greyhound Data Collector address rules	43
9.5.4	Point configuration page	44
9.5.5	System	45
9.5.6	Connection	46
9.5.7	Add connection	48
9.5.8	Driver stack	49
9.5.9	Integrate connection	51
9.5.10	Device	53
9.5.11	Point	55
9.5.12	Point flags	57
9.5.13	Point overview page	58
9.5.14	Utility driver points and functions	60
9.5.15	Converter	63
9.5.16	Converter functions	63
9.5.17	Converter Parameters	65
9.5.18	Converter examples	66
9.6	Alarms	72
9.6.1	Overview	72
9.6.2	Alarm point configuration	73
9.6.3	Upgrade	73
9.7	Accounts	76
9.7.1	Overview	76
9.7.2	Security	77
9.7.3	Messaging	82
9.8	Programming	88
9.8.1	Overview	88
9.8.2	Translator	89
9.8.3	SoftPLC	90
9.9	Other: Start page	94
9.10	Other: Messaging	96
9.10.1	Services	96
9.10.2	Redirect delay	97
9.10.3	Status reports	97
9.11	Other: Enterprise	99
9.12	Other: Database tools	100
9.13	Other: Schematics	101
9.14	Reboot	102
10 Log out		103
11 Tips and Tricks		104
11.1	Encrypted communication	104
11.2	Performance	107
11.2.1	Browsing the unit	107
11.2.2	Settings/system	107
11.2.3	Optimize data reading	107
11.2.4	Optimize data logging	107
11.2.5	Software version	108

11.3 Securing Greyhound Data Collector	109
11.4 Passwords and user names	109
11.4.1 Bad passwords	109
11.4.2 Good passwords	109
11.5 Firewall	109
11.6 DOS attacks	110
11.7 Firmware and software versions	110
11.8 Limiting access for users	110
11.9 TPIPE	110

1 Contact information

Botech AB
Ledeburgatan 5
211 55 Malmö
Sweden

Phone +46 (0)40 - 30 77 51
Fax +46 (0)40 - 22 98 98
Email info@botech.se
Web <http://www.botech.se>

2 Introduction

This document is the main reference material for the Greyhound Data Collector (GDC-001-02).

This introduction briefly describes the layout of this document as well as providing an overview of server hardware and server software.

In chapter 2 through 10, the graphical user interface is explained in detail.

Chapter 11 and 12 provides useful information when presented with specific problems or questions.

Supported drivers are detailed in Appendix A through C.

2.1 Hardware



Figure 1: GDC-001-02

Art. Nr.	GDC-001-02
Processor	Intel Pentium 4
RAM	128+ Mb
FLASH	-
Serial ports	3x RS232
Ethernet (1000 MBit)	2
Power	220V AC
Power consumption	-
Operation environment	-
Mechanical	19" rackmount, 1U

Table 1: Hardware

3 Start page

The first page a user comes into contact with is the login page.



Figure 2: Login page

This is where the user name and password is entered to get access to the system. The user is also presented with the option to select language and skin.

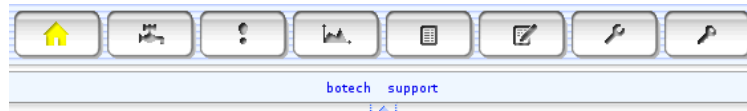


Figure 3: Default start page

On successful login, the user is directed to the default start page. By default, the start page only contains a product image and hyperlinks for mail support and website. To configure the start page to show more than this, please refer to section 9.9 on page 94.

4 Schematics

The Schematics page is (or can be configured to be) the main page for real time presentation. The Schematics page provide a list of active schematics and the current selected schematic as a Java Applet. Please refer to section 9.13 on page 101 for information on what options are available.

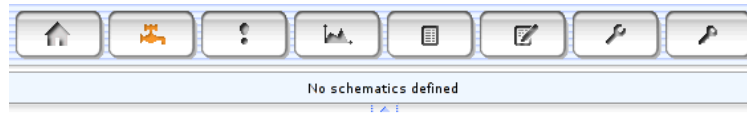


Figure 4: An empty schematics page

Below the main navigation buttons is a menu with links to all configured active schematics.

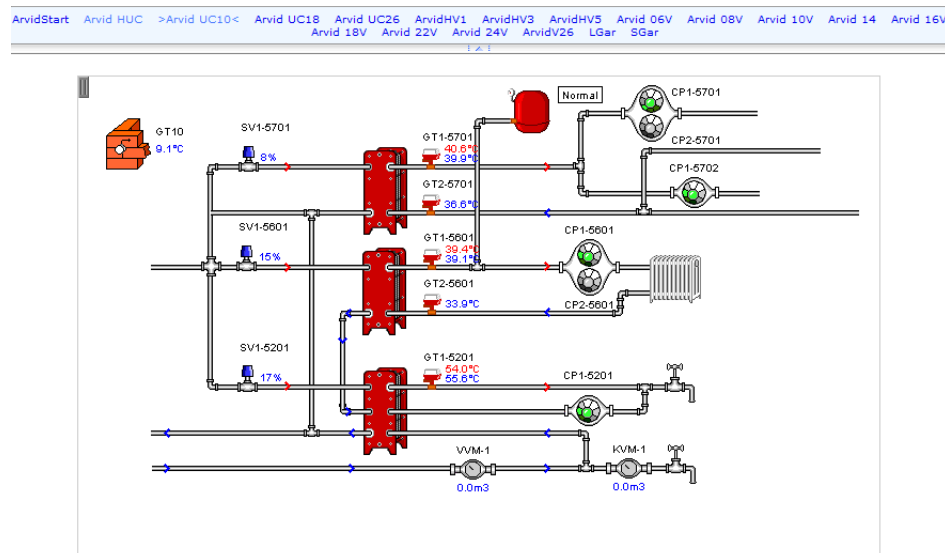


Figure 5: An example schematics page

5 Alarms

The alarm page provides both brief and detailed information on alarm points of interest in the system. Blocking can be set and configuration on user interface behaviour can be done. Please refer to section 9.6 on page 72 for information on detailed alarms configuration.

The alarm list has five functions. All alarms can be color-coded. Each alarm point can be clicked to a) go to schematic, b) execute command, c) read associated text, d) acknowledge alarm. More information is available for each alarm point (i.e. list events, time when alarm first occurred etc.)

The alarm list by default displays the status function. This function will display the alarms in the system that requires user interaction. That is alarms that are in one of the following states: active unacknowledged, active acknowledged, inactive unacknowledged or blocked.

5.1 Overview

Table 2 lists the possible states of an alarm point that makes it appear in the alarms list. Figure 6 shows an example of an active alarms list.

Alarm status	Default color	Optional
Active, not acknowledged	Red	
Active, acknowledged	Yellow	
Inactive, not acknowledged	Green	
Blocked	Magenta	Yes

Table 2: Shown alarms

status	priority	occurred at	alarm point	alarm text	acknowledged
Active	B	2007-08-30 12:08:14	LB04_VVX01_LA	A5404 LB04_VVX01_Spl.ans	-
Signal source LOCAL:JohannelundA5403.PLC43.LB04_VVX01_LA Current value 1.0 Documentation /manuals/LB04.PDF Source device LOCAL:JohannelundA5403.PLC43 Time active 00:31:10 Schematic LB04 Alarm point ID 315 Active read-cycles 0 Blocked No Acknowledge Value at alarm activation 1.0 Number of unacknowledged activations 276 First appeared 2007-08-31 16:46:34					
Active	B	2007-08-30 13:00:23	LB19_IP41_GP12_LA	A5401 LB19-GP12	-
Active	B	2007-08-30 18:05:07	CB02_IP01_LA	A5403 CB02-IP01 Driftfel	-
Inactive	B	2007-08-26 05:08:33	VAB1_GP41_LL	A5281 VAB1-GP41 L.Salam	-
Active	B	2007-08-12 11:07:05	LB07_PK01_OKOP_LA	A5402 LB07-PK01 Onsk.	-
Active	B	2007-08-31 10:55:21	CA09_LA	A5404 CA08 Driftfel	2007-08-31 16:20:53 Bravida
Active	B	2007-08-30 11:00:10	CA09_LA	A5404 CA09 Driftfel	2007-08-30 12:40:14 Bravida

Figure 6: Alarm list with detailed information

Field	Description
Status	Active, Inactive or Blocked
Priority	A,B,C or D
Occured at	Date and time
Alarm point	Name of alarm
Alarm text	Alarm description text.
Acknowledged	Date, time and user
Signal source	Path to data point that generated alarm
Source device	Path to device that generated alarm
Alarm point ID	ID of alarm point
Blocked	Shows if an alarm is currently blocked
Value at alarm activation	The value of 'Signal source' at activation
Current value	Current value of 'Signal source'
Time Active	Time in hours,minutes and seconds of active alarm
Active read cycles	Number of reads that alarm has been active
Number of unacknowledged activations	Number of cycles through active and normal without acknowledgment
Documentation	Link to documentation specific for alarm
Schematic	Link to schematic connected to alarm
Command	Command to execute, listed with user defined text
Acknowledge	Link to acknowledge alarm
First appeared	Date and time when alarm first went active

Table 3: Alarm list information fields

5.2 Statistics

The statistics function shows the number of active alarms (acknowledged/not acknowledged), the number of inactive alarms (acknowledged/not acknowledged).



```

alarms >statistics< events blocking configuration
┌───────────┴───────────┐
Alarm point count      417
Active, not acknowledged  4
Active, acknowledged   2
Inactive, not acknowledged 1
Blocked                 0

```

Figure 7: Alarm statistics

5.3 Events

The alarm event log shows changes in alarm point status, such as when an alarm goes active, inactive or is acknowledged. It also shows commands executed and which user has done what and when concerning alarms. Both alarm name and alarm text are shown to identify the alarm.

status	priority	alarm	occurred at	acknowledged	user
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 15:09:14	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 14:58:09	
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 13:35:59	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 13:25:17	
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 13:23:44	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 13:11:02	
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 13:10:39	Acknowledge
Active	B	LB13_FF01_GP12_LA	AS401 LB13-GP12	2007-09-26 13:00:23	Acknowledge
Acknowledged	-	LB04_VVX01_LA		2007-09-26 12:54:25	
Acknowledged	-	AS403_OKAS_LA		2007-09-26 12:54:13	
Inactive	-	LB13_FF01_GP12_LA	AS401 LB13-GP12	2007-09-26 12:52:49	
Acknowledged	-	LB13_FF01_GP12_LA		2007-09-26 12:52:20	
Inactive	-	AS403_OKAS_LA	AS403 Servicelucka Öppen	2007-09-26 10:34:19	
Active	B	AS403_OKAS_LA	AS403 Servicelucka Öppen	2007-09-26 10:33:05	2007-09-26 12:54:12 Vega
Active	B	KB02_PK01_LA	AS402 KB02-PK01 Driftfel	2007-09-26 10:25:37	Acknowledge
Inactive	-	KB02_PK01_LA	AS402 KB02-PK01 Driftfel	2007-09-26 10:24:38	
Active	B	LB13_FF01_GP12_LA	AS401 LB13-GP12	2007-09-26 10:24:36	2007-09-26 12:52:19 Vega
Inactive	-	LB13_FF01_GP12_LA	AS401 LB13-GP12	2007-09-26 10:17:39	
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 09:55:49	
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 09:25:45	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 09:14:34	
Inactive	-	VÅ01_GP41_LL	AS201 VÅ01-GP41 Låglarm	2007-09-26 09:14:24	
Active	B	VÅ01_GP41_LL	AS201 VÅ01-GP41 Låglarm	2007-09-26 09:09:33	Acknowledge
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 09:36:19	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 09:25:38	
Active	B	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 01:47:15	Acknowledge
Inactive	-	LB04_VVX01_LA	AS403 LB04-VVX01 S:Larm	2007-09-26 01:36:32	

Figure 8: Alarm event list

5.4 Blocking

The blocking function lets the privileged user block or unblock alarms. A blocked alarm will show up in the alarms list in a specific color, but it will not be treated as an active alarm in terms of messaging (such as SMS, email or printer services). An alarm can be blocked for a specified amount of time, or indefinitely. Filters are provided in case many alarm points exist, to make it easier for the user to find what alarm should be blocked. Both alarm name and signal source are shown in order to help identify the alarm. See figure 9 for an example.

alarm name	signal source	priority	blocked until	until	for (minutes)
VÅ01_GT11_LA	LOCALJohannelundAS201.PLC21.VÅ01_GT11_LA	B	-	block	
VÅ01_GT41_LA	LOCALJohannelundAS201.PLC21.VÅ01_GT41_LA	B	-	block	
AS403_OKAS_ILA	LOCALJohannelundAS403.PLC43.AS403_OKAS_ILA	B	-	block	
TF05_ST82_2025_LA	LOCALJohannelundAS201.PLC21.TF05_ST82_2025_LA	B	-	block	
PLC01_BATT_LL	LOCALJohannelundAS201.PLC21.PLC01_BATT_LL	B	-	block	
AS201_FBR1_LA	LOCALJohannelundAS201.PLC21.AS201_FBR1_LA	B	-	block	
AS201_SL_OVERSTR_LA	LOCALJohannelundAS201.PLC21.AS201_SL_OVERSTR_LA	B	-	block	
AS201_AUTSAK_LA	LOCALJohannelundAS201.PLC21.AS201_AUTSAK_LA	B	-	block	

Figure 9: Alarm block interface

5.5 Configuration

The configuration function lets the privileged user configure the alarmlist. Colors for different alarm status, both in brief and detailed view can be set here. Other configuration options are shown in table 4.

Figure 10: Alarm configuration

Name	Description
Show blocked alarms	Show blocked alarms in alarms list
Show alarm popup	Show popup for user when new alarm occurs
Show event source	Show signal source in event log and status page
Sort alarm list by time	Sort by time or priority
Refresh rate	Auto refresh rate for alarms list

Table 4: Alarm configuration options

6 Trends

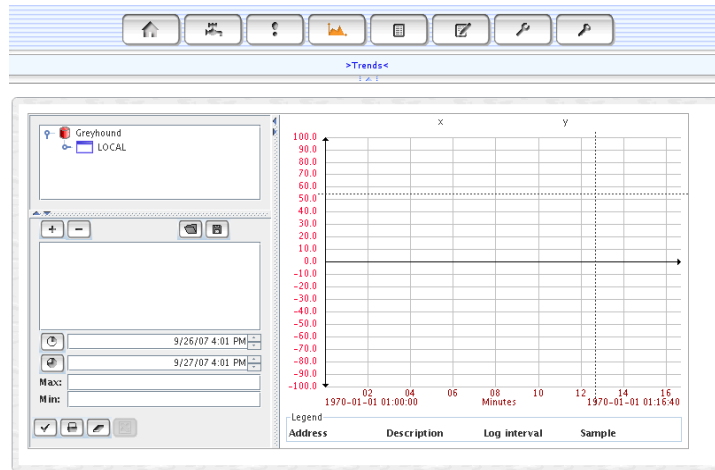


Figure 11: Trend interface

The Trend interface is used to examine and analyze historical data logs of the server. Multiple data points can be selected and be presented in a graph with different colors. Time interval, scales (common or individual) and colors can be configured on the fly. The graph is zoomable and all samples can be exported to Microsoft Office Excel format, XLS. Selected configuration can be saved for future use. The Trend interface is also directly reachable from the schematics where the selection of datapoints can be pre-configured. For further reference on which points and what data can be logged, intervals etc see subsection 9.5.11 on page 55.

6.1 Selection

The left side panel presents an interface based on the hierarcial data point design as described in subsection 9.5.11 on page 55. Only points which are logged are shown. To add a data point to the legend, select the point in the tree view and press the '+'-button - or use double click. Up to five points can be added this way. To change the color of data point representation, double click the point in the list view on the lower half as shown in figure 12. A selection (including time interval and scaling options) can be save for future use using the load and save buttins located between the panels. To remove a point from the legend, use the '-'-button.

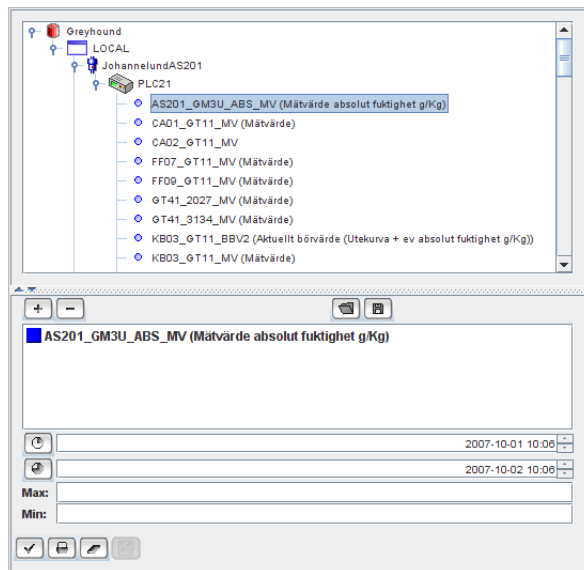


Figure 12: Trend datapoint selection

6.2 Scaling

When the legend contains more than one point, the 'single/multiple scale' switch will be shown as in figure 13. By default this switch is not selected and each point will be shown in its own vertical automatically selected scale. (Please not that this option is overridden by the manual scaling options as described below.) If selected, all trends will be shown in a single scale which is that of the first point in the list.

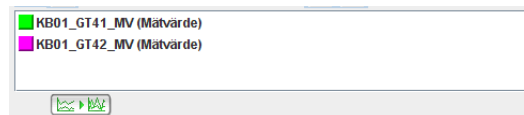


Figure 13: Trend scaling

The user can also set manual scaling options in regards of minimum and maximum vertical values to show on screen.

6.3 Zoom and Sampling

In order to zoom a specific area of the trend, click and drag in the area of interest. A dotted blue rectangle will appear showing which area will be zoomed. This operation can be repeated recursively to further zoom the graph. In order to zoom out, use right click in the zoomed area. See figure 14 for an example.

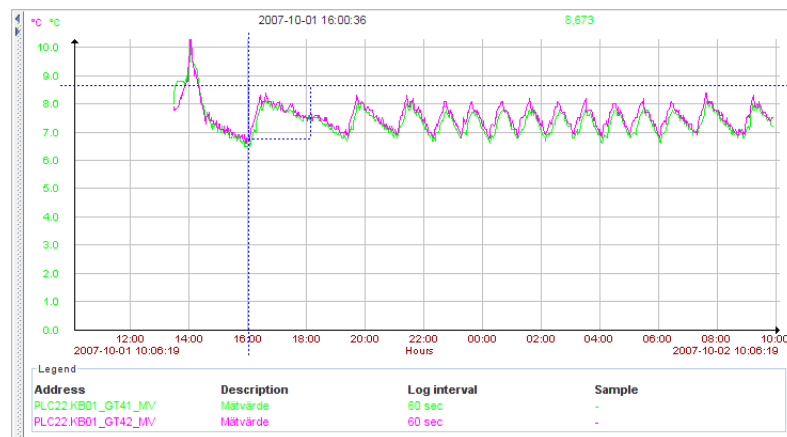


Figure 14: Trend area zoom

Besides the coordinates shown on the top of the trend area, exact coordinates for a specific sample can be shown by letting the mouse pointer hover over a sample for two seconds. The detailed coordinates will then be shown in the legend area on the lower half of the screen. See figure 15 for an example.

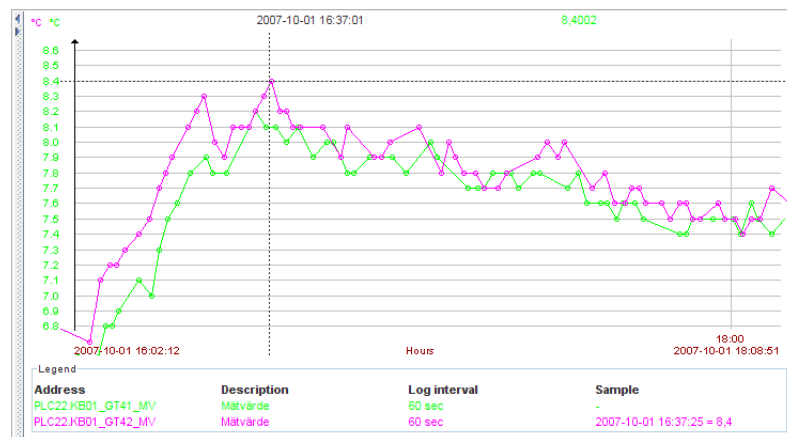


Figure 15: Trend sample detail

6.4 Export as XLS

Trend data can be saved locally in Microsoft Office Excel XLS format. This applies to both single datapoints and up to five simultaneous. This makes it possible to use Excel functions for graph drawings, integration in existing projects and snapshot backups.

7 Reports and documents

This section consists of two parts, "Value overview" and "Documents". Value overview is a "live" report where current values from all points can be viewed and it's also possible to write new values to writeable points. There are reports available in "documents" as well but these are static and generated by either the user or SoftPLC as files. These files are stored on the Greyhound Data Collector disk. Other files (various documents) such as manuals etc are also available here.

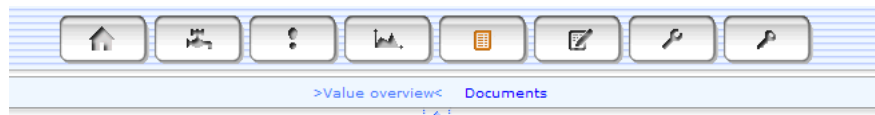


Figure 16: Reports and documents

7.1 Value overview

Value overview shows all point-values and the value-link presents the user with more options. Each device corresponds to a row which can be opened and closed with the +/- icons. The device description text is shown in bold followed by the Greyhound Data Collector address path (system.connection.device) and possibly a link to the main schematic for this device. If the description text isn't specified the device name is shown instead. See section 9.5.10 for information about how to configure device description and main schematic.

If the device is opened, all points to the device are shown. Point description is used but if this is not specified, name is used instead. In the value-link popup it is possible to write new value (if it is a writeable point), open trend (if the point is logged) and also with the settings-link, open the point overview page. See section 9.5.13 for more information about the point overview page. The settings-link is only available for administrator accounts (or for other generic accounts configured with "all configuration allowed"). See section 9.7.2 for information about account authorization. Administrators can also perform a multiple write command with the "write to all identical points" checkbox. This means that the write command is sent to all writeable points with identical names. The value (both the value link and the value in the popup) is also colour coded if the point has been configured with high and/or low limits. If the value is within the limits it is shown with default colour blue. If not, value is shown in red. See section 9.5.11 for information about how to configure point properties such as high/low limits.

It is possible to limit the points shown by using the various filters available. Point selection can with these filters for example be limited to only show writeable points with flag 'f' from a specific device. If all filters are empty or default, all points are included.

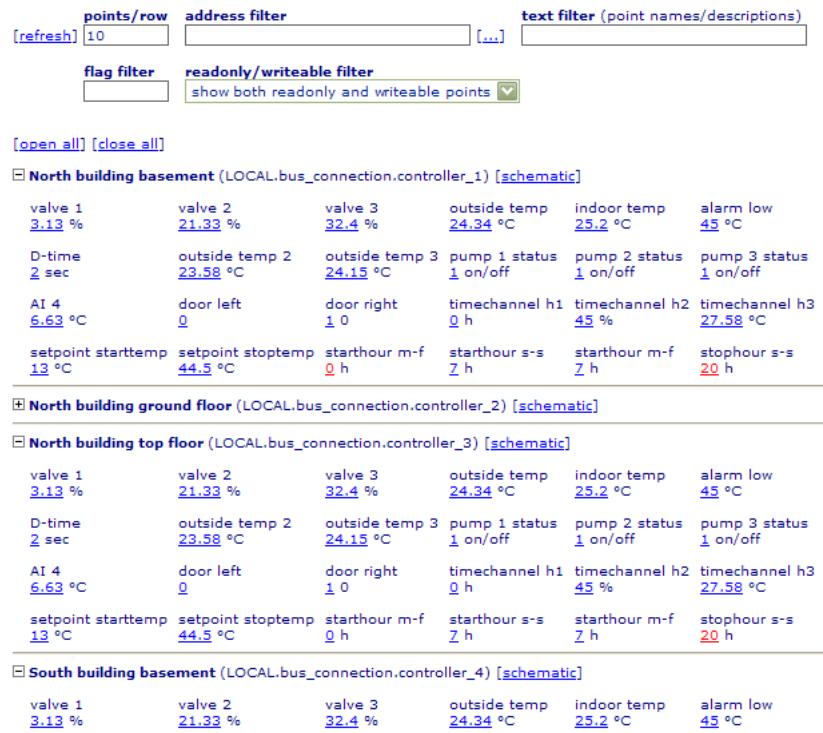


Figure 17: Value overview

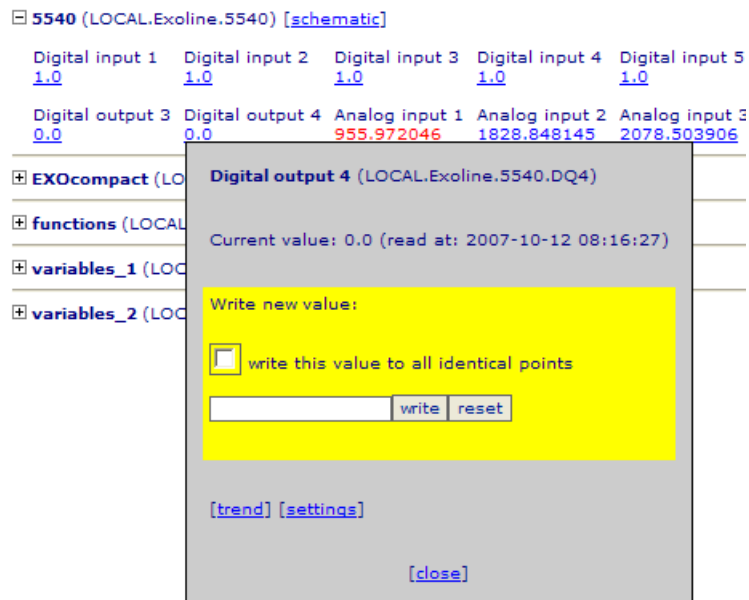


Figure 18: Point info popup

7.2 Documents

The documents section offers the possibility to store various files on the Greyhound Data Collector disk. These files are categorized in seven directories and each directory is meant for a particular type of files. The files uploaded or created, are used throughout the entire system in various ways as described in the table below. Each file is presented as a link with which the files can be either directly opened in a new browser window or downloaded. Binary files such as compressed archives are not viewable in the browser, these can only be downloaded.

The plc report directory is the only one stored in the temporary memory area and will be emptied at reboot. Files in anyone of the other directories are stored on disk and will not be removed at reboot. Files can be uploaded to all directories except "PLC reports". Furthermore, a create report wizard is available in the Reports directory.

Directory	Description
PLC reports	Reports created automatically by the PLC. Note: emptied at reboot. See section 9.8.3 for information about the SoftPLC and how to generate reports with it.
Reports	Reports created by the user. Use the 'create report' wizard
Manuals	Various files and documents which can be connected to for example alarms or schematic components.
Templates	Used by the 'create report' wizard. Templates decides the report appearance, see section 7.2.1 below for more information.
Address files	Text files which contains physical point addresses that are too long to fit into the normal database address column. Note: Only (possibly) required for Calculus and EIBNet points. See section 9.5.11 for information about physical point addresses.
Conversion files	Text files which contains point conversion functions that are too long to fit into the normal database convert column. See section 9.5.15 for information about the convert function.
Misc	Various files and documents which can be connected to for example alarms or schematic components.

Table 5: Documents directories

[refresh]

- PLC reports
- Reports
 - [create] [upload]

File	Size	Modified	Move
values.html	3.0 kb	2007-10-12 08:22:18	<input type="text"/>
logs.txt	2.74 kb	2007-08-21 16:00:44	<input type="text"/>
- Manuels
 - [upload]

File	Size	Modified	Move
Datasheet GHS-009-01.pdf	418.14 kb	2006-12-05 10:12:36	<input type="text"/>
Datasheet GHS-008-01.pdf	158.53 kb	2006-12-05 10:11:51	<input type="text"/>
BOT GHS-008-01 Manual.pdf	1.75 Mb	2007-09-11 12:17:21	<input type="text"/>
BOT GHS-007-02 Manual.pdf	1.82 Mb	2006-12-05 10:12:01	<input type="text"/>
- Templates
- Address files
 - [upload]

File	Size	Modified	Move
min.txt	118 bytes	2007-09-11 12:17:21	<input type="text"/>
max.txt	118 bytes	2007-09-11 12:17:21	<input type="text"/>
eib.txt	39 bytes	2007-06-14 12:41:45	<input type="text"/>
av.txt	116 bytes	2007-09-11 12:17:21	<input type="text"/>
- Conversion files
- Misc

Figure 19: Documents

7.2.1 Report templates

Templates decides the report appearance. Template files can be created as plain textfiles by the user and uploaded to the templates folder. A template is formatted with so called tags and free text (e.g. html). Furthermore, the template is divided into seven parts which each represents a specific part of the resulting report. "Parts" are separated with start and end identifiers, i.e. [part]...[/part]. The available parts are described in the table below.

Template part	Description
[FILETYPE]	Decides the resulting report file type. This affects how the report is shown in the browser when "view" is selected.
[SUBJECT]	If the report is created by the SoftPLC and connected to email recipients, this part decides the email message subject.
[HEADER]	Main header of the report which precedes all point specific information.
[DATAHEADER]	Header included directly before the data/value of each point.
[DATA]	Point data/value.
[DATAFOOTER]	Footer included directly after the data/value of each point.
[FOOTER]	Main footer of the report which ends the report.

Table 6: Report template parts

In all parts, except [FILETYPE], a number of tags as mentioned above can be used. Each tag corresponds to information/data and the tag is replaced with this information when the report is generated. Tags are used to include for example point values and names into the report. The available tags are described in the table below.

Template tag	Corresponds to
[SN]	System (server) name.
[ST]	System time.
[N]	Point name.
[D]	Point description.
[V]	Point value.
[T]	Point value timestamp.
[U]	Point unit.
[R]	Point readable.
[W]	Point writeable.
[L]	Point loginterval.
[I]	Point ID.
[A]	Point physical address.
[F]	Point flags.
[GA]	Point Greyhound Data Collector address, i.e. "system.connection.device.point".

Table 7: Report template tags

Not all tags are available in all part, i.e. point value ([V]) is only available in the [DATA] part. It also depends on the report type. More tags are available in the [DATA] part if it is a value report than if it is a log report. See table below for the available tags in respective part.

Template part	Available tags
[FILETYPE]	–
[SUBJECT]	[SN], [ST].
[HEADER]	[SN], [ST].
[DATAHEADER]	[N], [D], [U], [R], [W], [L], [I], [A], [F], [GA].
[DATA]	If log report: [V], [T]. If value report: [V], [T], [N], [D], [A], [F], [U], [GA].
[DATAFOOTER]	[N], [D], [U], [R], [W], [L], [I], [A], [F], [GA].
[FOOTER]	[SN], [ST].

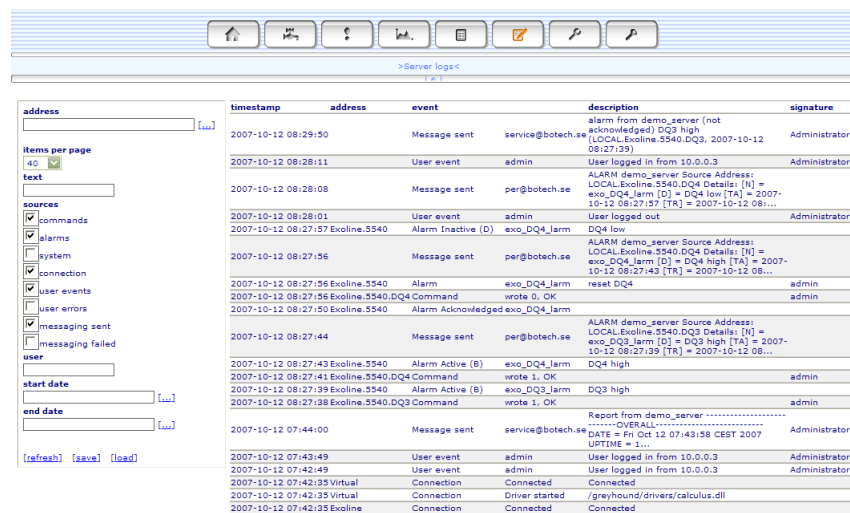
Table 8: Available tags in respective part

Example:

```
[FILETYPE].html[/FILETYPE]
[SUBJECT]report from [SN][/SUBJECT]
[HEADER]<html><body><table><tr><td colspan=2><
H2>Logreport: [SN]</H2></td></tr>[/HEADER]
[DATAHEADER]<tr><td colspan=2>Point: <I>[GA]</I>[D]
</td></tr><tr><td><b>Value</b></td>
<td><b>Read at</b></td></tr>[/DATAHEADER]
[DATA]<tr><td><b>[V]</b></td><td>[T]</td></tr>[/DATA]
[DATAFOOTER]<tr><td colspan=2><HR>
</td></tr>[/DATAFOOTER]
[FOOTER]<tr><td colspan=2>Generated at [ST]</td></tr></table>
</body></html>[/FOOTER]
```

8 Server logs

Eight different types of logs are available in the main server log. These are shown in chronological order with the most recent events at the top. Each log-type has a corresponding checkbox with which different log-types can be shown or hidden. Only the types (checkboxes) which the user has access to are enabled and therefore possible to view events from. See section 9.7.2 for information about account authorization. The event information is divided and shown in five fields: timestamp, address, event, description and signature. Depending on the log-type, different information is shown in these fields and not all fields are applicable on all log-types, e.g. account signature is empty for connection events. Address refers to the Greyhound Data Collector address, see section 9.5.2 for definition and information about Greyhound Data Collector addresses



timestamp	address	event	description	signature
2007-10-12 08:29:50		Message sent	alarm from demo_server (not acknowledged) DQ3 high (LOCAL:Exoline.5540.DQ3, 2007-10-12 08:27:59)	Administrator
2007-10-12 08:28:11		User event	User logged in from 10.0.0.3	Administrator
2007-10-12 08:28:08		Message sent	ALARM demo_server Source Address: LOCAL:Exoline.5540.DQ4 Details: [N] = exo_DQ4_larm [D] = DQ4 low [TA] = 2007-10-12 08:27:57 [TR] = 2007-10-12 08:27:57	Administrator
2007-10-12 08:28:01		User event	User logged out	Administrator
2007-10-12 08:27:57	Exoline.5540	Alarm Inactive (D)	exo_DQ4_larm DQ4 low	
2007-10-12 08:27:56		Message sent	ALARM demo_server Source Address: LOCAL:Exoline.5540.DQ4 Details: [N] = exo_DQ4_larm [D] = DQ4 high [TA] = 2007-10-12 08:27:43 [TR] = 2007-10-12 08:27:43	
2007-10-12 08:27:56	Exoline.5540	Alarm	exo_DQ4_larm reset DQ4	admin
2007-10-12 08:27:56	Exoline.5540.DQ4	Command	wrote 0, OK	admin
2007-10-12 08:27:50	Exoline.5540	Alarm Acknowledged	exo_DQ4_larm	
2007-10-12 08:27:44		Message sent	ALARM demo_server Source Address: LOCAL:Exoline.5540.DQ3 Details: [N] = exo_DQ3_larm [D] = DQ3 high [TA] = 2007-10-12 08:27:39 [TR] = 2007-10-12 08:27:39	
2007-10-12 08:27:43	Exoline.5540	Alarm Active (B)	exo_DQ4_larm DQ4 high	admin
2007-10-12 08:27:41	Exoline.5540.DQ4	Command	wrote 1, OK	admin
2007-10-12 08:27:39	Exoline.5540	Alarm Active (B)	exo_DQ3_larm DQ3 high	
2007-10-12 08:27:38	Exoline.5540.DQ3	Command	wrote 1, OK	admin
2007-10-12 07:44:00		Message sent	Report from demo_server -----OVERALL----- DATE = Fri Oct 12 07:43:58 CEST 2007 UPTIME = 1...	Administrator
2007-10-12 07:43:49		User event	User logged in from 10.0.0.3	Administrator
2007-10-12 07:42:49		User event	User logged in from 10.0.0.3	Administrator
2007-10-12 07:42:35	Virtual	Connection	Connected	Connected
2007-10-12 07:42:35	Virtual	Connection	Driver started /greyhound/drivers/calculus.dll	Connected
2007-10-12 07:42:35	Exoline	Connection	Connected	Connected

Figure 20: Server log view

The available log types are explained in the table below.

Log type	Description
Commands	Write commands sent by either users or the SoftPLC
Alarms	Alarm event log. A subset of the complete alarm events page. See section 5.3 for information about the alarm events page.
System	Various system level events and errors.
Connection	Various connection level events and errors.
User events	User account validation and security events, e.g. login, logout, forced logout, sms-command etc
User errors	User account validation and security errors, e.g. failed login attempts, account locked out, unathourized sms-commands etc.
Messaging sent	Messages (email, sms, printer) sent log (alarms, reports etc)
Messaging failed	Messages which couldn't be sent, e.g. invalid recipient address etc. See section 9.7.3 for information about Messaging.

Table 9: Log types

Since the log is chronological, users can follow a certain procedure directly on one page. For example: an alarm occurred, sms notification was sent to user, user logged in, acknowledged alarm and then wrote command to the alarm signal source. The alarm changed to inactive. User logged out.

It is possible to filter the search by using the available filters which are:

Filter	Description
Address	Only show events from a specific Greyhound Data Collector address, e.g. events from a certain connection.
text	Free text filter. Specified string must be found either in the event or description fields.
User	Events connected to a specific user or all users with the entered user filter string somewhere in the name.
Start	Only show events which occurred after 'start'.
Stop	Only show events which occurred before 'stop'.

Table 10: Log filters

Note: not all filters affect all log-types, e.g. address filter doesn't affect user events.

With the "Save" and "load" links it is possible to save and load a specific filter and log-types configuration for quicker access.

9 Configuration

The configuration section of the Greyhound Data Collector consists of eight subsections where all the required settings and parameters are configured by the user. Most of these pages are though restricted to administrator level and only administrators or users with corresponding security authorization are allowed to access the complete configuration interface. See section 9.7.2 for more information about security and account validation.

A couple of the pages described here are also used as configuration interfaces in Craft sites, which means that this part of the manual is also applicable as documentation when working with Craft sites. In fact, most often the configuration is performed in Craft and then published as a 'site' to the Greyhound Data Collector.

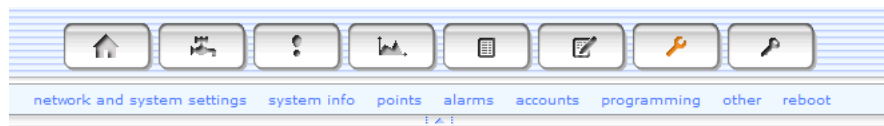


Figure 21: Configuration section

Section	Description
Network and system settings	Configure various network and main system settings (see 9.1).
System info	Informative page only, shows current settings of (for example) network and main system parameters as well as overall system performance (see 9.4).
Points	Configure data points and drivers for the connected external devices such as outstations and PLCs (see 9.5).
Alarms	Configure alarm points (see 5).
Accounts	Configure user accounts including both account security authorizations and messaging receivers (see 9.7).
Programming	Configure SoftPLC and translator rules (see 9.8).
Other	Various configuration, divided into five sections in this manual: start page, messaging, enterprise, database tools and schematics.
Reboot	Reboot page (see 9.14).

Table 11: Configuration sections

9.1 Network and system settings

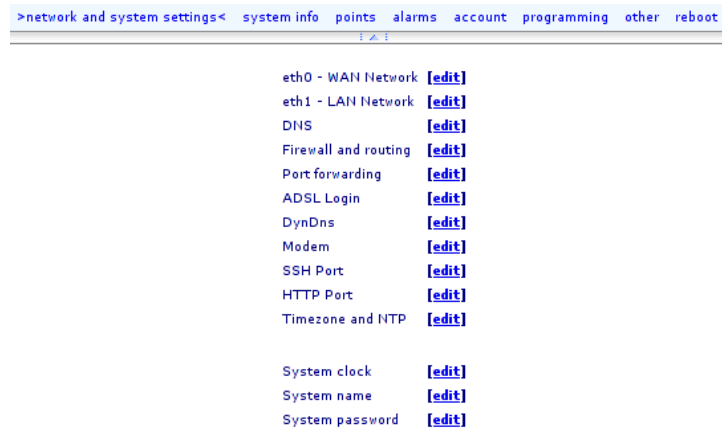


Figure 22: Network and system settings

9.1.1 eth0 - WAN Network

eth0 - WAN Network

Boot protocol	dhcp			
IP Address	192	168	0	2
Netmask	255	255	255	0
Gateway	192	168	0	1
	Save		Cancel	

Figure 23: WAN configuration

The "eth0 - WAN Network" page configures Eth0. This network interface is used to connect Greyhound Data Collector to Internet or a local network.

Note that "eth0" as referred to in this document in some cases are marked LAN1 on the physical box of the Greyhound Data Collector.

You can either use DHCP, which means that the Greyhound Data Collector gets a dynamically assigned IP address, or you can set a static IP address. For DHCP to work, there must be an available DHCP server on the network (Eth0). There are a couple of ways to find out the new address of Greyhound Data Collector if DHCP is chosen.

- The IP addresses of the available ethernet interfaces are displayed in the system applet (available on the Settings page).
- Greyhound Data Collector sends statusmail, a heartbeat, containing its current IP address. To use this alternative you must configure a mail service and accounts. Instructions on how to do this is available in the section [9.7.3](#) on page [82](#).
- The network administrator can possibly assign a DNS-name to the MAC address of the Greyhound Data Collector.
- Greyhound Data Collector can use DynDNS, see section [9.3.4](#) on page [37](#).

DHCP:

- Set 'Boot protocol' to 'dhcp'
- Save

Static IP-address:

- Set 'Boot protocol' to 'none'
- Fill in the fields for IP, netmask and gateway.
- Save

9.1.2 eth1 - LAN Network

eth1 - LAN Network

Boot protocol	none			
IP Address	192	.168	.1	.2
Netmask	255	.255	.255	.0
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

Figure 24: LAN configuration

The 'Network interface 2' configures Eth1 in the same way as Eth0, with the exception of gateway. The default settings for Eth1 is IP address: 192.168.1.2 and Netmask: 255.255.255.0.

IMPORTANT NOTE: The Greyhound Data Collector firewall does not affect this interface. Always use Network interface 1 (Eth0) when connecting the Greyhound Data Collector to public networks such as the Internet.

9.1.3 DNS

Domain Name Server

DNS1	195	.54	.122	.200
DNS2	195	.54	.122	.204
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

Figure 25: Domain Name Server

Configure the DNS that Greyhound Data Collector will use. The DNS is used to translate IP notation (like 192.168.0.1) to name notation (like www.google.com).

9.2 POP3

The POP3 page configures the POP3 account settings that makes it possible for the Greyhound Data Collector to collect e-mails. The parameters needed is available from the ISP or e-mail operator. Enter the name or IP-address of the POP3 server in POP3.HOST. Enter account username and password in the following two entries. POP3.INTERVAL specifies the time in minutes between mailbox reading and emptying attempts.

9.3 MYSQL

The settings for the MYSQL database included in the Greyhound Data Collector should be left as is unless an external database server is used. Enter the name or IP-address of the MYSQL server in MYSQL.HOST. Enter account username and

password in the following two entries. `MYSQL_DB` is the name of the MYSQL database and `MYSQL_PORT` is the TCP port of the MYSQL server.

9.3.1 Firewall and routing

Firewall and routing

Enable routing	yes
Enable firewall	yes
Open web server port in firewall	yes
Open FTP server port in firewall	no
Open SSH/Telnet server port in firewall	no
Open database server port in firewall	no
Open user define port A in firewall	0
Open user define port B in firewall	0
Open user define port C in firewall	0

Save Cancel

Figure 26: Firewall configuration

In 'Firewall and routing' the user configure the Greyhound Data Collector built-in firewall. The firewall factory default filters everything except HTTP.

Field	Description
Enable routing	Use the Greyhound Data Collector as a gateway between Eth0 and Eth1.
Enable firewall	Use the Greyhound Data Collector as a firewall to filter certain services.
Open web server port	Opens HTTP for traffic (default TCP port 80).
Open FTP server port	Opens FTP for traffic (TCP port 21).
Open SSH server port	Opens SSH (secure shell) for traffic (TCP port 22).
Open database server port	Opens DBS should for traffic. (TCP port 5000)
Open user defined port A	Opens a user defined port for traffic.
Open user defined port B	Opens a user defined port for traffic.
Open user defined port C	Opens a user defined port for traffic.

Table 12: Firewall

The user defined ports opens both the TCP and UDP ports. Both TCP and UDP are forwarded when the port forwarding is enabled. For further explanation about the firewall configuration, see example in the port forwarding section (see section [9.3.2](#) on page [35](#)).

9.3.2 Port forwarding

Port forwarding

Figure 27: Port forwarding

In 'Port forwarding', the user configure forwarding of IP services from Eth1 to Eth0. For example a web camera can be connected to the subnet on Eth1 and the picture become available from the IP address used by Eth0.

Field	Description
Enable user defined port X forwarding Port X	Enables or disables the portforward The port where you access the service from on Eth0.
Server IP X	The IP address of the device on Eth1.
Server port X	The TCP or UDP port of the subnet de- vice.

Table 13: Port forwarding

Example We want to add a web-camera and a secondary Greyhound Data Collector to an existing Greyhound Data Collector (primary). We only have one IP-address on the public network (Eth0).

1. The IP address of the primary Greyhound Data Collector in this example is 10.220.221.121 (eth0, public network) and 192.168.1.2 (eth1, subnet).
2. Connect the web camera to the subnet and configure it using the following network settings:

IP address: 192.168.1.4
 Netmask:255.255.255.0
 Default gateway: 192.168.1.2.

3. Connect the secondary Greyhound Data Collector to the subnet and configure it using the following network settings:

IP address: 192.168.1.5
 Netmask:255.255.255.0
 Default gateway: 192.168.1.2.

4. Login to the primary Greyhound Data Collector and select the settings menu. Choose 'Network settings', and step forward to Firewall settings.
5. Configure the firewall settings, and open the user ports 81 and 82. make sure both ROUTER and FIREWALL are enabled (yes). We will add the web-camera on port 81, and the secondary Greyhound Data Collector on port 82.
6. Configure the port forwarding settings. Enable two portforwarders. Enter the IP addresses of the two devices, and set the ports.
7. Reboot the primary Greyhound Data Collector.
8. The web-camera is now available on 10.220.221.121:81 and the secondary Greyhound Data Collector on 10.220.221.121:82.

9.3.3 ADSL Login

ADSL Login

The screenshot shows a configuration window titled "ADSL Login". It contains the following fields and values:

- Enable automatic ADSL login:** A dropdown menu with "no" selected.
- ADSL login server IP:** A dotted IP address field containing "10.0.0.1".
- ADSL user name:** A text input field containing "uid".
- ADSL user password:** A text input field containing "pwd".
- At the bottom, there are two buttons: "Save" and "Cancel".

Figure 28: ADSL configuration

If the Greyhound Data Collector is connected to the Internet through ADSL, it is possible to configure the Greyhound Data Collector to automatically login to the Swedish ISP Telia.

Field	Description
Enable automatic ADSL login	Enables/Disables the use of ADSL login.
ADSL login server IP	The ISP login-server address
ADSL user name	ADSL account username
ADSL user password	ADSL account password

Table 14: ADSL automatic login

9.3.4 DynDns

DynDns

Enable dynamic DNS registration	no
Name of the host	
Service type	dyndns
User name	
User password	
Interface to register	eth0
	Save Cancel

Figure 29: Dynamic DNS

Greyhound Data Collector supports DynDNS. This enables a dynamically assigned public IP address to be associated with a DNS name, for example “http://myserver.dyndns.org”. If you want to use DynDNS, you must first register at <http://www.dyndns.org> to obtain a DNS name. When registering the DNS name, a username and a password are also specified. This is then entered into Greyhound Data Collector.

Field	Description
Enable dynamic DNS registration	Enable/disable DynDNS.
Name of the host	The registered DNS name ex. myserver.dyndns.org.
Service type	dyndns. Do not change.
User name	Registered username.
User password	Registered password.
Interface to register	Select which IP address to report (eth0 or eth1).

Table 15: DynDNS

NOTE: Enable DynDNS as late in the configuration procedure as possible. Every time the Greyhound Data Collector is rebooted it will send a request to a DynDNS server with the current IP address and if this is done too often the DNS name will be blocked by DynDNS.

9.3.5 Modem

The 'Modem' page provides settings for Point-to-Point-Protocol used for dialup networking.

Modem configuration
(Uses serial device 0 if enabled)

Enable dialin	no
Enable dialout	no
Modem type	Analogue/Analogue
Modem init string	ATZ
ISP phonenumber	
ISP username	
ISP Password	
Dialin username	root
Dialin password	pass
Dialin server IP	192 .168 0 .2
Dialin client IP	192 .168 0 .3
Dialin ring count	1
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 30: Modem configuration

Field	Description
Enable dialin	Enables the dial in function. The Greyhound Data Collector will act as an ISP.
Enable dialout	Enables the dial-out function. The Greyhound Data Collector will connect to an ISP to send alarms.
Modem type	The first type is used when acting as an ISP (dial-in), and the second type is used when connecting to an ISP to send alarms (dial-out). Ex. GSM/GPRS means that GSM will be used when client is dialing in to the Greyhound Data Collector and GPRS when the Greyhound Data Collector is dialing out.
Modem init string	Init to the modem.
ISP phone number	The phone number to the ISP to use.
ISP username	The user name to use when logging in to the ISP.
ISP password	The password to use when logging in to the ISP.
Dialin username	The user name that the remote client use.
Dialin password	The password that the remote client use.
Dialin server IP	The IP address of the Greyhound Data Collector (for the dial-up link)
Dialin client IP	The IP address that the client (the caller) will get when connected.
Dialin ring count	Select the number of RING signals that shall be received before answering the incoming call.

Table 16: PPP

If 'Enable dialin' and/or 'Enable dialout' is enabled, the PPP service will occupy serial device 0 (COM1). Make sure you disable any driver-connection using serial device 0.

The PPP service is tested using the following modems/configurations:

GSM/GPRS: 'Fargo Maestro 100' and 'Siemens M35iT GSM/GPRS terminal'.

GSM/GSM: 'Fargo Maestro 100' and 'Siemens M35iT GSM/GPRS terminal'.

Analogue/Analogue: 'USRrobotics analogue modem'.

WARNING! Be careful when connecting the Greyhound Data Collector to a local area network (LAN) when using the dialup possibilities, since it might be possible to access the LAN from the dialup computer.

9.3.6 SSH Port



Figure 31: SSH port configuration

SSH port is the TCP port used for SSH tunnels as described in section 11.1 on page 104

9.3.7 HTTP Port



Figure 32: HTTP port configuration

Configure the TCP port that the Greyhound Data Collector web server should use.

9.3.8 Timezone and NTP

Figure 33: Time zone configuration

Configure the use of a timeserver (NTP) and which timezone you want to use. If NTP is enabled the Greyhound Data Collector will synchronize the system time with a timeserver on the Internet. The time from the NTP server is requested at startup (boot-time). If there is no NTP server available, or if the network is down, the system time will be used. If a city is chosen in the timezone dropdown menu, the Greyhound Data Collector will automatically adjust the system time for daylight savings.

Field	Description
Timezone	The timezone your Greyhound Data Collector system is placed in.
Enable NTP	Enables/Disables the use of NTP.
NTP Server	IP-address or host name of the NTP server.

Table 17: NTP

9.3.9 System clock

Figure 34: System time

Set the local time of the Greyhound Data Collector.

9.3.10 System name

System name

Set name

Figure 35: System name

Set an identifying string for the Greyhound Data Collector. Used in report sending as described in section 9.7.3 on page 82

9.3.11 System password

System password

Password

Figure 36: System password

Set system password of the Greyhound Data Collector, used for SSH tunnels as described in section 11.1 on page 104

9.4 System info

System info page displays various important system configuration parameters, for example system name, version and performance. It also shows the current addresses (both IP and MAC) of the available network interfaces.



Figure 37: System info

The "more" link offers more parameters such as point count, internal application status and also comments/warnings to parameters which possibly needs to be noticed. The "more" page is very useful to send (e.g. screen-dump) to a support technician if something isn't working properly.

9.5 Datapoints and drivers

9.5.1 Overview

The external devices (field busses, outstations, PLCs etc) with which the Greyhound Data Collector communicates, are organized in 4 levels in the internal Greyhound Data Collector database. System is the top level and it represents "this" server. Every system has one or more connections. A connection corresponds to a physical connection to an external field bus. Every connection is configured with one or more drivers which handles the actual communication with the connected equipment. Furthermore, connections has one or more devices connected to it and a device corresponds to an outstation, PLC or similar, available on the external field bus. The devices contains the different objects, called points, that are to be read/written. A point is thus a single value in an outstation or PLC.

9.5.2 Greyhound Data Collector address

A Greyhound Data Collector address is defined as the four levels described above separated with '.' hence "system.connection.device.point". This represents the internal address, search path, for each defined point or any other level in the Greyhound Data Collector. **Note:** This has nothing to do with the external device specific physical addresses which has to be configured for the devices and points in order for the drivers to address and read/write a value in a connected external device. The Greyhound Data Collector address is only used internally, for example to connect a point to a schematic or to a SoftPLC rule.

9.5.3 Greyhound Data Collector address rules

There are two important rules regarding the Greyhound Data Collector address format:

- 1. Only A-Z, a-z, 0-9, - and _ are allowed characters in the system, connection, device and point names. Note: space is consequently not allowed.**

- 2. The name must be unique on each level.**

There cannot exist two points with identical names in the same device or two devices in the same connection with identical names etc. It is however allowed to have identical names if the, for example, identical points belong to different devices.

9.5.4 Point configuration page

The 'points' section in the configuration menu is where all points and the address levels above points (i.e. systems, connections, devices) are configured. Drivers are configured here as well. The different levels are organized and accessible in a tree-view where 'system' is the top (root) tree-node and 'point' is the bottom node. With the top menu filters, address and text, users can decide which connections, devices and points to show. The text filter only applies to the point names and descriptions, for example: text filter = 'set' means that only points with 'set' somewhere in either the name or description will be shown. The system, connection and device levels are configured individually by clicking the respective names. More than one point can however be configured at once with the available 'edit selected', 'delete selected' and 'copy selected' links in the top menu. These are also available (as well as save/cancel) in a popup if the right mouse button is clicked.



Figure 38: Points configuration page

9.5.5 System

The top address level 'system' corresponds to the server on which the Greyhound Data Collector software is run. Greyhound Data Collector is preconfigured with the system 'LOCAL' and this is the recommended setting for the Greyhound Data Collector systems which this manual covers. Do not change this name if you are not absolutely sure of what you are doing. The system popup contains the following parameters and functions:

Parameter/function	Description
Name	System name.
Description	System description.
Add connection	Opens the "add connection" page. See section 9.5.7 for more information.
Apply changes	Reloads all connections to this system. If anything is changed in the tree, apply changes is required in order to submit the changes to the Greyhound Data Collector. Note: It is not required to 'apply changes' for each change individually. When all configuration is done, select 'apply changes'.

Table 18: System



Figure 39: System parameters and functions

9.5.6 Connection

A 'connection' is the interface that exists between the Greyhound Data Collector software and a field bus system. The connection popup contains the following parameters and functions:

Parameter/function	Description
Name	Connection name.
Enabled	Enable/disable the connection.
Connected	Shows if the connection currently connected (running) or not.
Always connected	If 'yes' the Greyhound Data Collector will always start and 'connect' the connection.
Manual connect request active	If 'Always connected' is disabled, users can manually start ('connect') the connection. This is also automatically performed when a user loads a schematic which requests values from points in this connection. This can for example be useful if the connection connects to the external devices through a modem connection.
Established last connection at	Timestamp when the connection was last connected.
Store values when rebooting server	If 'yes', point values are stored and reloaded at system reboot.
Edit	Opens the edit connection page.
Delete	Deletes the entire connection and all devices and points belonging to it.
Add a device to this connection	Adds a new device to the connection.
Show driver stack and driver properties	Opens the view/edit driver stack/properties window. See section 9.5.8 for more information.
Integrate this connection with another server	Opens the 'Integrate server' window. See section 9.5.9 for more information.
Export connection to import file	Export connection to a Craft Designer import file. See Craft Designer manual for more information about import files.

Table 19: Connection

If the connection is either disabled or 'Always connected' is disabled, it will be colour-coded in red in the tree-view.

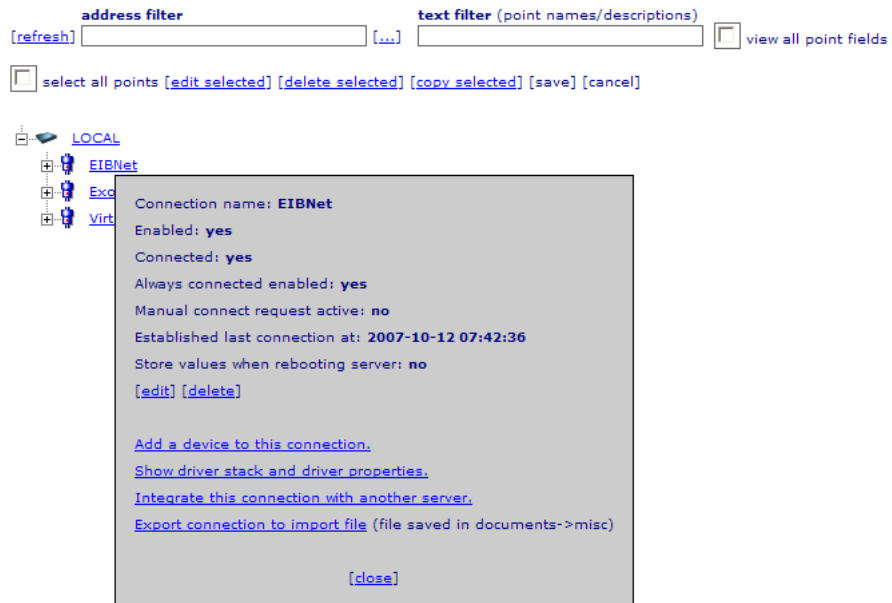


Figure 40: Connection parameters and functions



Figure 41: Edit connection page

9.5.7 Add connection

On this page, a new connection is created and configured. For description of the connection parameters, see table 19 above. Besides these connection parameters, a driver stack needs to be specified. In most cases a connection is handled by two stacked drivers. The first driver (stack-order 1) is a protocol driver and the second (stack-order 2) is a transport driver (serial, ip etc). In some cases only one driver is used, for example 'Calculus driver' or drivers with a built in transport layer.

After the connection has been created, the driver properties most often needs to be configured (e.g. timeouts, serial-paramaters etc). The driver stack and properties are available from the connection popup, 'Show driver stack and driver properties', after the connection has been created. See section 9.5.8 for more information the driver configuration.

Connection properties:

Connection name:

Enable connection:

Enable 'Always connected':

Store values when rebooting:

Specify the driver-stack:
 In most cases a connection is handled by two stacked drivers. The first driver (stack-order 1) is a protocol driver and the second (stack-order 2) is a transport driver (serial, ip etc). In some cases only one driver is used, for example 'Calculus driver' or drivers with a built in transport layer.
 NOTE: After the connection has been created, the driver properties most often needs to be specified (e.g. timeouts, serial-paramaters etc). The driver properties are available in the connection pop-up after the connection has been created. Please refer to the driver manuals for more information about drivers and driver properties.

Stack-order 1:

Stack-order 2:

Stack-order 3:

Stack-order 4:

Stack-order 5:

[\[save\]](#) [\[close\]](#)

Figure 42: Add connection

9.5.8 Driver stack

This page shows the driver stack and driver properties in a tree view format ordered by ascending driver stack order. To view and edit the respective properties available for each driver, click the open tree node icon (+ image) in front of the driver. When opened, all driver properties to the driver are shown. Each driver has a property list which vary depending on the driver. For example, a serial port driver needs a valid serial port configured (as a property) whilst the ip driver needs a target ip address.

Both the driver stack and the driver properties can be configured on this page. Drivers and properties can also be added with the respective 'add' links and deleted by clicking on the delete icon (red minus image) in front of each driver and property. With 'edit stack' drivers can both be replaced, e.g. replace the serial port driver with a ip driver, and moved to another stack placement (change stack order).

[refresh] [edit_stack] [edit_properties] [save] [cancel] [close]

Driver-stack for connection **Exoline**

[add_driver]

- [-] EXoline (stack-order: 1)
 - [add_property]

Property	Description	Data type	Value
Packettimeout		INTEGER	5
Sleeptime		INTEGER	300
Alarmscaninterval		INTEGER	120
Readblocks		INTEGER	1
- [+] TPIPE (stack-order: 2)
- [+] RS232 (stack-order: 3)

Figure 43: Driver tree-view

Example: an existing driver stack uses a protocol driver at stack order 1 and a transport driver at stack order 2. To insert the utility driver 'T-pipe' in between these, first select 'add driver' then 'edit stack'. When edit has been selected, it is possible to specify a driver (in this example 'T-pipe') in the drop-down menu. Also configure this new driver with stack order 2 and finally move the ip driver to stack order 3.

”Edit properties” works in a similar way. When selected, it is possible to edit all visible properties. Depending on driver-property, different property-values and formats are expected. Please refer to the respective driver manuals for information about the driver properties.

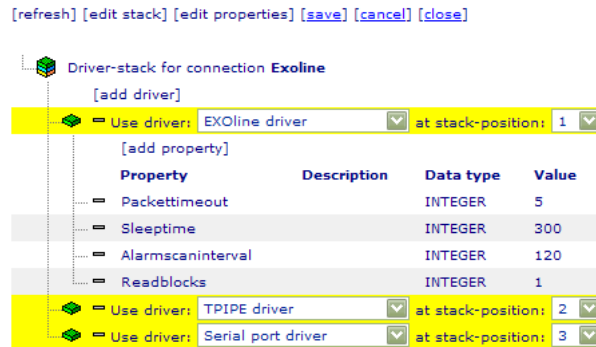


Figure 44: Edit driver stack

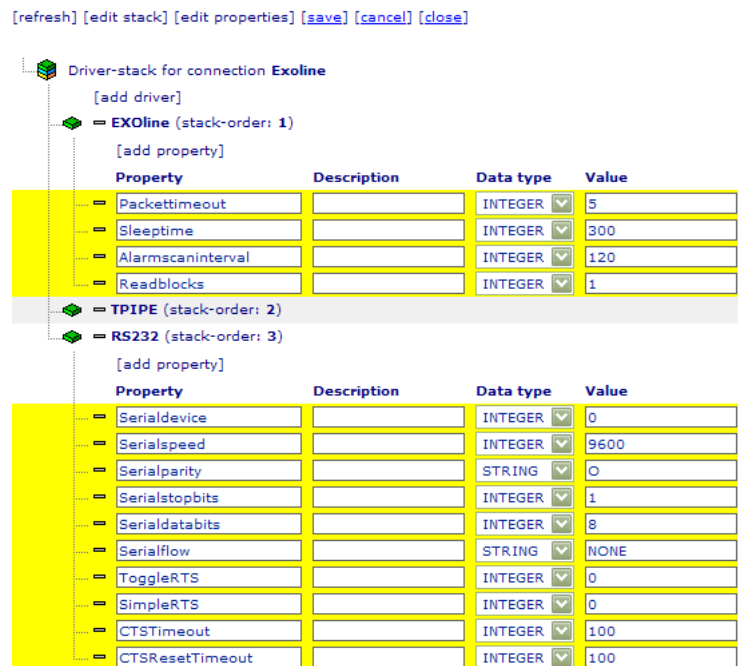


Figure 45: Edit driver properties

9.5.9 Integrate connection

A connection on a Greyhound Data Collector can be 'integrated' and used as a gateway by another Greyhound Data Collector. In the following text, 'gateway connection' refers to a 'normal' connection which communicates with external devices (outstations, PLCs etc) through for example a serial cable. 'Remote connection' refers to the connection on the remote server with which the 'gateway connection' will be integrated.

The gateway connection must have a corresponding remote connection on the remote Greyhound Data Collector. The remote connection communicates with the external devices through the gateway connection and it is possible to both read data from and write data to the external devices through the gateway connection. All communication between the connections is initiated by the gateway connection. This means that it doesn't matter if the Greyhound Data Collector running the gateway connection is located on a closed net and with a private ip-address as long as it can connect to the remote server. This is very useful if a number of installations located on private nets or perhaps connected through a GPRS modem, needs to be monitored. Simply integrate these servers with one public server and all installations will be monitored from the public, 'remote' Greyhound Data Collector. The gateway communicates with the remote server through standard http request which ensures a reliable connection.

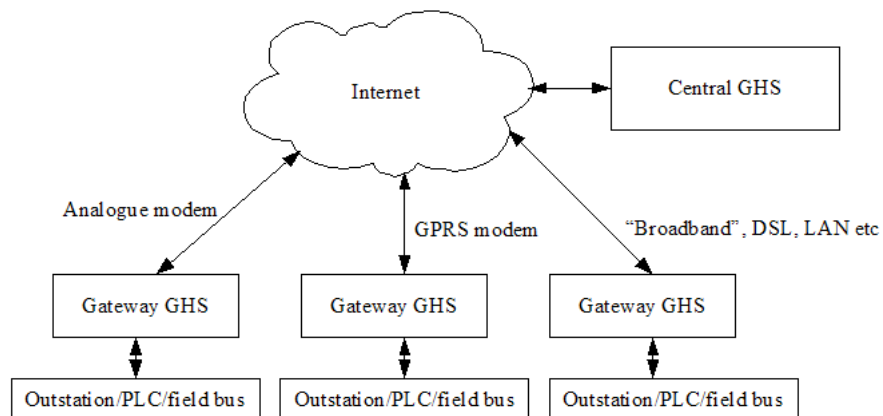


Figure 46: Integrate connection overview

The data is sent in files which are uploaded to the remote server and the remote connection must therefore be configured with the generic file driver. **Note:** the names of the corresponding devices and points must be identical in both connections. The connection names can however be different since a driver property to the remote generic driver specifies which gateway system and connection to read/write data to/from.

Which data to send (values, logs, alarms) and how often, are configured by the user as well as if write commands that are executed on the remote server should be automatically collected and executed. Furthermore, the gateway connection can be configured to search for update-patches on the remote server. See table 20 for information about all available configuration parameters.

(bold = required parameter)

Enable:

Address and login parameters for receiving server:

Server IP:

Server http-port:

Server user name:

Server password:

Communication settings:

Always maintain established session:

Use dial-out connection:

Modem reboot AT-command:

Data communication settings: (at least one needs to be enabled, 0 = disabled)

Send values every: seconds

Send alarms every: seconds

Fetch write-commands every: seconds

Send logs every: seconds

Send logs from points with flag:

Filter the logs sent to a: seconds interval

Check for patches every: seconds

Group settings:

Group name:

[\[save\]](#) [\[close\]](#)

Figure 47: Integrate connection

9.5.10 Device

A 'device' is an outstation, PLC, I/O-card or similar which can be addressed on a connected fieldbus. Sometimes there is no physical correspondence, but a 'virtual' device must still always be configured in order to maintain the Greyhound Data Collector address structure. For example, the utility drivers watcher and calculus (see 9.5.14) uses virtual devices, as well as a couple of field bus drivers (e.g. EIB) where the only addressing available is on point level. In most cases though, drivers address a point within a device and hence requires both a device and point address. The device popup contains the following parameters and functions:

If the device is disabled, it will be colour-coded in red in the tree-view.

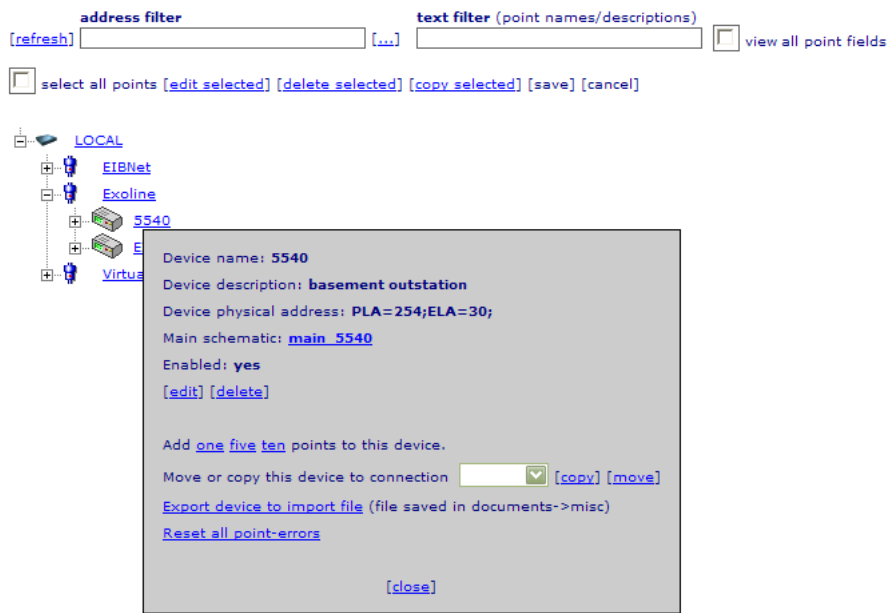


Figure 48: Device parameters and functions

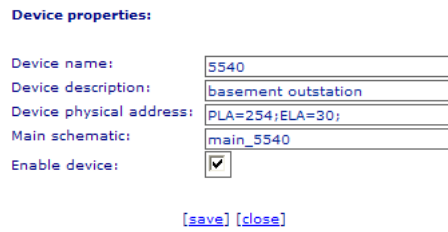


Figure 49: Edit device page

9.5.11 Point

A 'point' is an object in a device. This object can be a set point, a parameter, part of a time channel or similar (just about anything actually). More than one point can be edited, copied or deleted at once by using the top menu links. Points are selected with the checkbox available in front of every point in the tree-view. 'Edit selected', 'delete selected' and 'copy selected' affects all selected points. Hence, these links only affect points and are also available in a popup if the right mouse button is clicked. Systems, connections and devices are edited and deleted within respective popup as described previously. By default, the most important point parameters are shown. All parameters can however be shown by ticking the 'view all point fields' checkbox in the top menu. Furthermore, each point name is a link which opens the point overview page described in 9.5.13. Besides the point parameters described in this section, the point overview also shows the various internal relations between a point and for example an alarm point or a SoftPLC rule.

The screenshot shows a software interface for viewing points. At the top, there are filters for 'address filter' and 'text filter (point names/descriptions)', along with a 'view all point fields' checkbox. Below the filters are action buttons: 'select all points', 'edit selected', 'delete selected', 'copy selected', 'save', and 'cancel'. The main area is divided into a tree view on the left and a table on the right. The tree view shows a hierarchy starting with 'LOCAL', followed by 'EIBNet', 'Exelline', and '5540'. The table lists various digital and analog points with their physical addresses, current values, and control flags.

Name	Description	Physical address	Value	Log interval (sec)	Readable	Writeable
DI1	Digital input 1	LN=200;VAP=13;TYPE=LV;	1.0	60	X	
DI2	Digital input 2	LN=200;VAP=14;TYPE=LV;	1.0	60	X	
DI3	Digital input 3	LN=200;VAP=15;TYPE=LV;	1.0	60	X	
DI4	Digital input 4	LN=200;VAP=16;TYPE=LV;	1.0	60	X	
DI5	Digital input 5	LN=200;VAP=17;TYPE=LV;	1.0	60	X	
DI6	Digital input 6	LN=200;VAP=18;TYPE=LV;	1.0	60	X	
DI7	Digital input 7	LN=200;VAP=19;TYPE=LV;	1.0	60	X	
DI8	Digital input 8	LN=200;VAP=20;TYPE=LV;	1.0	60	X	
DO1	Digital output 1	LN=200;VAP=47;TYPE=LV;	0.0	60	X	X
DO2	Digital output 2	LN=200;VAP=48;TYPE=LV;	0.0	60	X	X
DO3	Digital output 3	LN=200;VAP=49;TYPE=LV;	1.0	60	X	X
DO4	Digital output 4	LN=200;VAP=50;TYPE=LV;	0.0	60	X	X
AI1	Analog input 1	LN=201;VAP=18;TYPE=RV;	955.972046	60	X	
AI2	Analog input 2	LN=201;VAP=21;TYPE=RV;	1828.112671	60	X	

Figure 50: Point view

A point has the following parameters:

Note: The log table size, is always a multiple of 8 kB due to the filesystem. This means that 8 kB is the smallest filesize available. If 'Max Logsize' is not specified, the default value 32 will be used (about 4000 samples). When, or if, a log file gets full the oldest samples starts to be overwritten.

'Edit selected' reloads the page with the selected points colour coded in yellow and editable.

If more than one point are to be edited at once, a global edit form is shown just above the tree-view. To enable this form, tick the 'global config' checkbox. When a parameter is specified in the global form, all selected points will be updated but will not be permanently saved until "save" is selected.

address filter text filter (point names/descriptions) view all point fields

select all points [edit selected] [delete selected] [copy selected] [save] [cancel]

global config

LOCAL

- EIBNet
- Exoline
- 5540

Name	Description	Physical address	Value	Log interval (sec)	Readable	Writeable
<input type="checkbox"/> DI1	Digital input 1	LN=200;VAP=13;TYPE=Lv;	1.0	60	<input type="checkbox"/>	X
<input checked="" type="checkbox"/> DI2	Digital input 2	LN=200;VAP=14;TYPE=Lv;	1.0	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DI3	Digital input 3	LN=200;VAP=15;TYPE=Lv;	1.0	60	<input type="checkbox"/>	X
<input checked="" type="checkbox"/> DI4	Digital input 4	LN=200;VAP=16;TYPE=Lv;	1.0	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DI5	Digital input 5	LN=200;VAP=17;TYPE=Lv;	1.0	60	<input type="checkbox"/>	X
<input checked="" type="checkbox"/> DI6	Digital input 6	LN=200;VAP=18;TYPE=Lv;	1.0	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> DI7	Digital input 7	LN=200;VAP=19;TYPE=Lv;	1.0	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> DI8	Digital input 8	LN=200;VAP=20;TYPE=Lv;	1.0	60	<input type="checkbox"/>	X
<input type="checkbox"/> DQ1	Digital output 1	LN=200;VAP=47;TYPE=Lv;	0.0	60	X	X

Figure 51: Edit point view

9.5.12 Point flags

Point flags are used either for enable a specific point behaviour or to group points. The point groups are used as selection filters (flag filters) on various pages and for point-selection in reports, e.g. include all points with flag 'k' into a report. See section 7.2 for manual report generation in 'Documents' and section 9.8.3 for automatic 'SoftPLC' report generation.

The point flags in the table below are reserved and generates a specific point behaviour. They can still be used for grouping and selection but the functionality as described below will always be enabled when using a reserved flag.

9.5.13 Point overview page

The point overview page can be accessed and opened from various parts of the Greyhound Data Collector. There are links to this page from the point tree view, programming page, value overview etc. In most cases where a Greyhound Data Collector address is shown, the address is in fact shown as a link to the point overview page for the respective point. The point overview page can also link to the point overview page for a another point which is connected to the first point through a calculus relation.

Besides the possibility to view and edit the various point parameters as described above (see table 22), the point overview also offers to:

- Write new value to the point (if writeable)
- Delete the point log file
- Show point relations, i.e. connected alarm-points, SoftPLC/translator rules and calculus points.

LOCAL.Exoline.5540.DQ1

Value	<input type="text" value="0.0"/>	<input type="button" value="Write"/>	<input type="button" value="Reset"/>
Last read	2007-10-12 09:52:40		
Point name	<input type="text" value="DQ1"/>		
Description	<input type="text" value="Digital output 1"/>		
Physical address	<input type="text" value="LN=200;VAP=47;TYPE=LV;"/>		
Unit	<input type="text"/>		
Flags	<input type="text" value="f"/>		
Log-interval	<input type="text" value="60"/>	<input type="button" value="[delete log file]"/>	
Log max size	<input type="text" value="0"/>		
Converter	<input type="text"/>		
Priority	<input type="text" value="0"/>		
Readable	<input checked="" type="checkbox"/>		
Writeable	<input checked="" type="checkbox"/>		
Low limit	<input type="text" value="0.0"/>		
High limit	<input type="text" value="0.0"/>		

[\[save\]](#) [\[refresh\]](#) [\[close\]](#)

Last error --
Last error at --

The point is connected to the following alarm points:

Alarm point
[exo_DQ1_alarm](#)

No PLC rules are connected to this point

The point is connected to the following translator rules:

Point 1	Data direction	Point 2
[view] LOCAL.EIBNet.IPRouter.button	==>	LOCAL.Exoline.5540.DQ1

No Calculus points are connected to this point

[\[close\]](#)

Figure 52: Point overview page

Write value

Simply enter the new value and click the write button. The result will be shown in a new window but for actual driver result, the command log described in the 'Server logs' section must be consulted, see section 8.

Delete point log

There are three common scenarios when the point logs are deleted. Please follow the respective instructions below:

1. If the point should still be logged with the same file size: simply select "delete log file". A new log file will be created automatically.
2. If the point shouldn't be logged anymore: First change point parameter 'Log interval' (see table 22) to zero (i.e. disable logging). Then select system 'Apply changes' (see table 18) wait for 30 seconds and finally select 'delete log file'.
3. If the point should use a log file with another file size: First change point parameter 'Log max size' (see table 22) to the new value. Then select system 'Apply changes' (see table 18) wait for 30 seconds and finally select 'delete log file'.

Point relations

A point can be used as signal source (input) to alarm points (see 9.6), in SoftPLC- and translator rules (see 9.8) as well as input to a Calculus point (see 9.5.14). All these relations are shown on the point overview page as links which leads directly to the connected item.

9.5.14 Utility driver points and functions

A couple of special utility drivers are available in the Greyhound Data Collector. These drivers have no physical connection to external field busses and are worth a bit of explanation to avoid confusion. The most important and used of these are, Calculus, Watcher and T-pipe. T-pipe is used as a communication channel driver and do not use points whilst the other two are used for various functions defined as points. Connections running either the Calculus or the Watcher driver therefor needs a number of points defined in order to do something useful. Each point corresponds to a function and the point parameter 'physical address' is used to specify which function the respective point will have (see 22).

Although these 'virtual' points differs from normal points and often are used to extend the functionality of other 'real' points, they are still handled and processed as any other point in the Greyhound Data Collector. This means that they can be logged, used in schematics and for alarming etc.

Calculus

The Caluclus driver is a utility driver which can perform a number of various functions, e.g. calculate sum and avarage of other point values, save system time and name as point values, count how many times a point changes values or for how long another point has had a specific value. Mathematical operations such as sine, cosine, tangent and logarithms are also available.

Points and devices used in a Calculus connection are hence virtual in that sence that they have no direct connection to external devices (outstations, PLCs etc). Instead they use other points as value input, perform various calculations and uses the result as its value. Note: A Calculus point can also use another Calculus point as value input. The Calculus functions (sums, sine, count, time etc) are specified in the Calculus point physical address field .

Three examples:

- a Calculus point, named `sum_p1_p2`, with physical address (function) `'SUM(LOCAL.con1.dev1.p1,LOCAL.con1.dev1.p2)'` returns the sum of the values from 'p1' and 'p2' points.
- A Calculus point, named `'time_p1_on'`, with the physical address (function) `'TIME(LOCAL.con1.dev1.p1=1)'` returns the number of seconds the point 'p1' has had value 1.
- A Calculus point, named `'cosine_of_p2'`, with the physical address (function) `'COS(LOCAL.con1.dev1.p2)'` returns the cosine of the value of point 'p2'.

These relations between points through Calculus functions are shown in the point overview page (see 9.5.13), e.g. the point overview page for 'LOCAL.con1.dev1.p1' in the examples above would show relations to both the Calculus points `'sum_p1_p2'` and `'time_p1_on'`.

Furthermore, Calculus points can be used to store values from other points with for example the SoftPLC. For example, a writeable Calculus point, named `'last_time'`, with the physical point address `'VALUE(0)'` can be written with the system time by the SoftPLC every time another point, named 'p1', has value 10. This example

would result in that the user easily could see when the 'p1' point last had value 10, since this timestamp is stored by the SoftPLC to the 'last_time' Calculus point. System time is, as mentioned above, available as a Calculus point as well, physical address = 'CURRENTTIME(hh:mm:dd)'. VALUE(x) is a calculus physical address (function) which result in a point with the initial value x. See 9.8.3 for more information about the SoftPLC.

If the function string is too long (e.g. sum function for 30 points) for the point physical address database field (50 characters limit), the function can be entered into a text file and uploaded to the 'Address files' directory on the 'Documents' page. If a file is used, enter the file name in the database point field 'Physical address' in the format FILE=x where x is the file containing the actual address (function), e.g. FILE=sumfunction.txt. See 7.2 for more information about 'Documents'.

For more information about Calculus and the functions available, see the Calculus driver appendix.

The screenshot shows a software interface for managing Calculus points. At the top, there are two filter boxes: 'address filter' and 'text filter (point names/descriptions)'. Below these are several action buttons: '[refresh]', '[...]', and a checkbox for 'view all point fields'. A second set of buttons includes 'select all points', '[edit selected]', '[delete selected]', '[copy selected]', '[save]', and '[cancel]'. On the left, a tree view shows a hierarchy: LOCAL > EIBNet > Exoline > Virtual > functions. The main area displays a table of 12 points:

Name	Description	Physical address	Value	Log interval (sec)	Readable	Writeable
System_name	system name	SYSTEMNAME()	demo_server	0	X	X
System_time	system time	CURRENTTIME(hh:mm:ss)	10:02:56	0	X	
exo_ai_average	average of ais	FILE=av.txt	2233.05	60	X	
exo_ai_max	maximum value of ais	FILE=max.txt	2904.316650	60	X	
exo_ai_min	minimum value of ais	FILE=min.txt	956.339722	60	X	
yta		VALUE(110)	110	0	X	X
button_count	button changes	CHANGED(L.EIBNet.IPRouter.button)	1.0	300	X	
button_active	seconds	TIME(L.EIBNet.IPRouter.button=1)	0	0	X	X
button_active_h	hours	Q(L.Virtual.functions.button_active,3600)	0.0	0	X	X
cosine_bah	of button_active_hours	COS(L.Virtual.functions.button_active_h)	1.0	20	X	
sine_bah	of button_active_hours	SIN(L.Virtual.functions.button_active_h)	0.0	20	X	
loge_bah	of button_active_hours	LOG(L.Virtual.functions.button_active_h)	-inf	20	X	

At the bottom of the table, it says '12 points fetched'. Below the table, there are two more items in the tree view: 'variables_1' and 'variables_2'.

Figure 53: Calculus point examples page

Watcher

Unlike the Calculus points/functions, Watcher points doesn't use other points as value input and are consequently not connected to other points. Depending on the Watcher point function specified in 'physical address', various system parameters and values are available as the respective point values. Some of the available functions are: system load, time, uptime, serial port status and memory usage. Watcher points can thus be used to (for example) generate alarms when the system seems overloaded (high load) or for trending the amount of data going through the serial ports.

For more information about Watcher and the functions available, see the Watcher driver appendix.

T-pipe

T-pipe is used inside an existing 'normal' driver stack as a gateway to the connected external device. T-pipe listens a specific user define TCP port for incoming connection request. When a user remotely connects to this port, T-pipe takes control of the transport driver in the driver stack and thus lets the remote user communicate with the external device with for example third party programming tools etc.

Example:

A Greyhound Data Collector connection uses the protocol driver 'Exoline' at stack order 1, T-pipe at stack order 2 and the transport driver 'serial' at stack order 3 to read/write data from the connected (exoline compatible) external device. When the remote user connects to the T-pipe TCP-port, the user takes control over the 'serial' driver and can hence through this directly communicate with the external device. When the user disconnects, normal driver functionality is restored.

For more information about T-pipe, see the T-pipe driver appendix.

9.5.15 Converter

The converter is a layer for converting texts and numbers when sent and received from the drivers. It can for example round and scale floatingpoint values, bitmask integers and find and replace texts within strings. The commands is entered into the point field 'Convert', and consist of a semicolon separated list of commands with parameters. This way a number can be first bitmasked, shifted right, scaled and then finally rounded. When a value is written the commands are executed in the opposite order using the inverse functions.

If the Convert function string is too long for the database field (50 characters limit), the function can be entered into a text file and uploaded to the 'Conversion files' directory on the 'Documents' page. If a file is used, enter the file name in the database point field 'Convert' in the format FILE=x where x is the file containing the actual converter function(s), e.g. FILE=replacefunction.txt. See 7.2 for more information about 'Documents'.

9.5.16 Converter functions

R- The "R-" command disables the conversion when reading values.

W- The "W-" command disables the conversion when writing values.

C- The "C-" command disables the conversion of read values that goes to the cachefile. These values are the ones used for the schematics and actual values in reports etc.

L- The "L-" command disables the conversion of read values that goes to the logging subsystem. These values are the ones used for logging to files, and for generating alarms.

BCD8 *BCD8()*

The "BCD8" command, treats the value as a 2-digit BCD value and converts it to a normal integer.

BCD16 *BCD16()*

The "BCD16" command, treats the value as a 4-digit BCD value and converts it to a normal integer. T

BCD32 *BCD32()*

The "BCD32" command, treats the value as a 8-digit BCD value and converts it to a normal integer.

BITMASK8 *BITMASK8(int iMask) or BM8(int iMask)*

The "BITMASK8" or "BM8" command, converts the value to a 8-bit integer and then masks (AND operator) the value using iMask. The parameter iMask can be entered using binary, octal, decimal or hexadecimal representation (see section 9.5.17 below). There is no inverse function for this command, but the BITMASK8 command is executed as it is for writes also.

Example:

BITMASK8(00001111b) on the value 255 equals 15
BM8(F0h) on the value 255 equals 240

BITMASK16 *BITMASK16(int iMask) or BM16(int iMask)*

The "BITMASK16" or "BM16" command, converts the value to a 16-bit integer and then masks (AND operator) the value using iMask. The parameter iMask can be entered using binary, octal, decimal or hexadecimal representation (see section 9.5.17 below). There is no inverse function for this command, but the BITMASK16 command is executed as it is for writes also.

BITMASK32 *BITMASK32(int iMask) or BM32(int iMask)*

The "BITMASK32" or "BM32" command, converts the value to a 32-bit integer and then masks (AND operator) the value using iMask. The parameter iMask can be entered using binary, octal, decimal or hexadecimal representation (see section 9.5.17 below). There is no inverse function for this command, but the BITMASK32 command is executed as it is for writes also.

REPLACE *REPLACE(string find, string replacewith) or RE(string find, string replacewith)*

The "REPLACE" or "RE" command finds a string and replaces it with another string.

REPLACEALL *REPLACEALL(string find, string replacewith)*

The "REPLACEALL" command finds a string and replaces it with another string. Unlike the REPLACE function, the string searched must be identical to the 'find' string specified. REPLACEALL(1,alarm) has no effect on value '15', whilst REPLACE(1,alarm) would convert '15' to 'alarm5'.

ROUND *ROUND(int iDecimals) or R(int iDecimals)*

The "ROUND" or "R" command, converts the value to an IEEE double precision floatingpoint number, rounds it to the correct number of decimals and removes the trailing zeros. There is no inverse function.

SCALE *SCALE(double dSlope, double dOffset)* or *S(double dSlope, double dOffset)*

The "SCALE" or "S" command, converts the value to an IEEE double precision floatingpoint number and calculates the value(V) using the raw value(R) according to the following formula:

$$V = dSlope * R + dOffset$$

The inverse formula is (where V is the value that is written from the user interface, and R is the value sent to the driver):

if dSlope is 0.0

$$R = V$$

else

$$R = (V - dOffset) / dSlope$$

SHIFLEFT *SHIFLEFT(int iSHL)* or *SHL(int iSHL)*

The "SHIFLEFT" or "SHL" command, converts the value to a 32-bit integer and shifts the bits left iSHL steps. The parameter iSHL can be entered using binary, octal, decimal or hexadecimal representation (see section 9.5.17 below).

SHIFTRIGHT *SHIFTRIGHT(int iSHR)* or *SHR(int iSHR)*

The "SHIFTRIGHT" or "SHR" command, converts the value to a 32-bit integer and shifts the bits right iSHR steps. The parameter iSHR can be entered using binary, octal, decimal or hexadecimal representation (see section 9.5.17 below).

SWAP16 *SWAP16()*

The "SWAP16" command swaps the high and low octets in a 16-bit word.

9.5.17 Converter Parameters

Integer parameters Integer parameters are entered using the figures 0-9, A-F (hexadecimal) and the minus sign "-" for decimal numbers. Integer parameters can be entered using either binary, octal, decimal or hexadecimal representation. To use binary representation, just add the letter "b" at the end of the number: 11001000b. To use octal, add "o" and for hexadecimal use "h". To use decimal representation add "d" or add no letter.

Example:

BM16(FF00h)

```
BM8(4o)
BM8(255)
BM16(111100000000b)
```

Floatingpoint parameters Floatingpoint numbers are entered using figures 0-9, "-", the exponent "e" and the decimal separator ".".

Example:

```
SCALE(-0.34e1,2.4)
```

String parameters String parameters is entered using any character except for the reserved characters ';', ',', '(' and ')'.

Example:

```
REPLACE(On,Alarm)
REPLACE(Off,0)
```

9.5.18 Converter examples

Alarm bit Extract an alarm bit in a register value

```
"W-;BITMASK16(1000b);SHR(3)"
```

"W-" disables the function when writing. In this case because there are other flags in the register, and we don't know the value of these, and can therefore not set the register value.

"BITMASK16(1000b)" masks unwanted information from the register. Now the value will be either 0 or 8. The reason for using BITMASK16 instead of BITMASK8 in this case is only cosmetic. The source register is a 16-bit register.

"SHR(3)" shifts the value right 3 bits so the value will be either 0 or 1.

Alarm bit to text Extract an alarm bit in a register value and convert to text.

```
"W-;L-;BITMASK16(1000b);SHR(3);REPLACE(0,No alarm);REPLACE(1,Alarm)"
```

See the description for "W-", "BITMASK16(1000b)" and "SHR(3)" in section [9.5.18](#) above.

"L-" is used to disable the conversion for logging and alarms. To log the value 0 or 1 for the flag, use the example in section [9.5.18](#) above instead.

"REPLACE" is used to set the text "No alarm" when the register flag is 0, and

the text "Alarm" when the register flag is 1.

Text registers Replace text values read from a controller and converts them into numerical values, so it is possible to log the values and to create alarm events.

"REPLACE(ON,1);REPLACE(OFF,0)"

"REPLACE(ON,1)" replaces all occurrences of "ON" to 1.

"REPLACE(OFF,0)" replaces all occurrences of "OFF" to 0.

Parameter	Description
Enable	Enable/disable integration of the connection.
Server IP	Remote Greyhound Data Collector ip address.
Server http-port	Remote Greyhound Data Collector http port (default 80).
Server user name	Remote Greyhound Data Collector user name (login account).
Server password	Remote Greyhound Data Collector password.
Always maintain established session	Dont disconnect from the remote Greyhound Data Collector in between requests.
Use dial out connection	Select this if the server connects to the network (Internet) through a modem connection.
Modem AT reboot command	If a modem connection is used, an AT command can be specified which is executed automatically when the system encounters communication problems. Any command can be specified but a modem reboot command is recommended.
Send values every	Decides how often in seconds current values of all points are sent to the remote Greyhound Data Collector.
Send alarms every	Decides how often in seconds to check for, and possibly copy new alarms to the remote Greyhound Data Collector.
Fetch write commands every	Decides how often in seconds to check for, and possibly collect new write commands from the remote Greyhound Data Collector.
Send logs every	Decides how often in seconds point log data of selected points are sent to the remote Greyhound Data Collector.
Send logs from points with flag	Selects which points to include when sending logs, e.g. all points with flag 'k'.
Filter logs sent	Decides the minimum seconds in between two sequential log samples.
Check for patches every	Decides how often in seconds to check for, and possibly download and apply new patches from the remote Greyhound Data Collector. Patches are identified with the local system-name, configured in network and system settings 9.3.10, or with the group name described below.
Group name	All gateway servers with the same group name checks for the same patch on the remote Greyhound Data Collector (patch name = group name).

Table 20: Integrate connection

Parameter/function	Description
Name	Device name.
Description	Device description.
Physical Address	The device physical address. Used by the drivers to address the external device. Depending on which driver is used, different address parameters and formats are expected. See respective driver appendix for more information.
Main schematic	Optional, used by the Value overview report, see 7.1 .
Enabled	Enable/disable the device.
Edit	Opens the edit device page.
Delete	Deletes the device and all points belonging to it.
Add points	Adds 1, 5 or 10 new points to the device.
Move/copy	Move or copy the device and all points belonging to it, to the same (copy only) or another connection.
Export device to import file	Export device to a Craft Designer import file. See Craft Designer manual for more information about import files.
Reset all point errors	Resets the point error fields. See section 9.5.11 for more information about point fields/parameters.

Table 21: Device

Parameter	Description
Name	Point name.
Description	Point description.
Physical Address	The point physical address. Used by the drivers to address the a single value/register in an external device. Depending on which driver is used, different address parameters and formats are expected. See respective driver appendix for more information.
Convert	Convert function such as scaling or bitmasking. See section 9.5.15 for more information.
Value	Current value of the point.
Unit	Unit, such as m, kWh, Hz or similar. If "%" is wanted, specify "%%" .
Flags	Different flags can be specified in order to enable specific point behaviour or for point grouping. See section 9.5.12 for more information.
Log interval	Decides how often in seconds the read value should be stored for trend analysis. (0=don't store).
Log table size (kb)	Decides how much historical data to store in kB (1 sample = 8 bytes).
Priority	0 or 1 means that the point is read every read cycle. Higher values means that the point is read more seldom. Not all drivers support this, se respective driver appendix.
Readable	Decides if the point should be read.
Writeable	Decides if the point can be written.
Low limit	Used by the value overview report for value colour coding, see section 7.1. If the point is configured with the flag 'l' (enable low limit check flag) and the point value is below 'Low limit', the value is shown in red.
High limit	Used by the value overview report for value colour coding, see section 7.1. If the point is configured with the flag 'h' (enable high limit check flag) and the point value is over 'High limit', the value is shown in red.
Last error	Description of last error.
Last error at	Time when last error occurred.

Table 22: Point

Flag	Description
c	Clock log point. Log the point exactly at minute change. Note: 'Log interval' must be more than zero, for example log interval 900 (every 15:th minute) and c-flag, will result in a stored log sample at 00:00, 00:15, 00:30, 00:45, 01:00, 00:15 etc.
C	Only log when value changes. Each value is compared to last read value, not last stored, so equal values can be stored anyway. If 'Log interval' is zero, every change is stored. If 'Log interval' is greater than zero, the point will not be logged more often than this interval.
F	Force log even on errors (such as wrong checksum etc).
R	Store every reading, regardless of other parameters.
h	Enable high limit check in value overview report (See 7.1). h-flag is used together with the point parameter 'high limit'.
l	Enable low limit check in value overview report (See 7.1). l-flag is used together with the point parameter 'low limit'.
A, I, H, L	Previously used for alarm generation. Reserved for backward compatibility reasons.

Table 23: Point flags

9.6 Alarms

9.6.1 Overview

Alarms are either read directly from the external devices (e.g. alarm stack scanning) or generated by the Greyhound Data Collector. Not all drivers support direct reading of alarm stacks but generated alarms can be configured for all points defined in the Greyhound Data Collector. Furthermore, the main alarm list (which shows active and unacknowledged alarms) only displays generated alarms. Alarms read from external alarm stacks etc are only available in the historical alarm event list. This section describes how to configure alarms handled and generated by the Greyhound Data Collector and the following text refers exclusively to configuration of generated alarms, from now on referred to as "alarm" or "alarm point". For information about how the the resulting alarms are shown in the different Greyhound Data Collector alarm lists, see section 5.

For each alarm handled by the system, an alarm-point needs to be configured. An alarm-point is **not** the same thing as a point (data point) as described in section 9.5.11. An alarm point defines how an alarm should be generated and various functions such as connected documentation and/or schematics. Data points are however used as "signal source" to the alarm-points and therefore ultimately decides when an alarm is generated.

network and system settings > system info > points > alarms <

address filter text filter

[refresh] [clear] [su]

select all [new] [edit] [delete] [duplicate] [save] [cancel]

[apply changes] (note: restarts all drivers)

ID	Alarm name	Alarm type	Priority	Signal source	Limit	Alarm text (active)	Alarm text (inactive)
1	exo_DQ1_alarm	Digital alarm (positive slope)	B	LOCAL.Exoline.5540.DQ1		DQ1 high	DQ1 low
2	exo_DQ2_alarm	Digital alarm (positive slope)	B	LOCAL.Exoline.5540.DQ2		DQ2 high	DQ2 low
3	exo_DQ3_alarm	Digital alarm (positive slope)	B	LOCAL.Exoline.5540.DQ3		DQ3 high	DQ3 low
4	exo_DQ4_alarm	Digital alarm (positive slope)	B	LOCAL.Exoline.5540.DQ4		DQ4 high	DQ4 low
5	button_active_alarm	High limit alarm	A	LOCAL.Virtual.functions.button_active	100.0	button active more than 100 s	button active normal

5 items, 5 in total
Page [1]

Figure 54: Alarm configuration page

9.6.2 Alarm point configuration

Add alarm points with the "new" link. The "edit", "delete" and "duplicate" links affects all alarm points which are selected in the respective checkbox. The available filters in the top menu enables the user to limit the alarm points shown. With "Address filter", only alarm points with signal source from a specific Greyhound Data Collector address can be selected, e.g. only show alarm points with signal sources (data points) from a specific device. "Text filter" affects the alarm point name, e.g. only show alarm points with the string "out" somewhere in the name. When "edit" is selected, all available parameters of the alarm points selected are shown.

The following parameters can be configured for alarm points (required parameters in bold):

Note: After having added or changed any alarm configuration "apply changes" is required. See table 18 for more information about "apply changes".

The screenshot shows a web interface for configuring alarm points. At the top, there are filter fields for "address filter" and "text filter", along with a "refresh" button and a "clear" button. Below the filters, there are action buttons: "select all", "new", "edit", "delete", "duplicate", "save", and "cancel". A note indicates that clicking "apply changes" will restart all drivers. The main part of the interface is a table with columns for "ID", "Generation", "Alarm type", "Signal source", "Priority", "Texts", "Sending", and "Alarmlist functions". The table contains one row for a digital alarm with a positive slope, signal source LOCAL-Exoline.5540.DQ3, priority 0 (active), alarm name "exc_DQ3_alarm", alarm format "/manuals/BOT_GHS-007-02", and schematic "text". Below the table, there are configuration fields for "Delay read cycles" (0), "Delay seconds" (0), "Discard inactive events" (checkbox), "Priority (inactive)" (0), "Alarm text (active)" (DQ3 high), "Limit" (0.0), "Alarm text (inactive)" (DQ3 low), "Command" (LOCAL-Exoline.5540.DQ3=0), and "Command text" (reset DQ3).

ID	Generation	Alarm type	Signal source	Priority	Texts	Sending	Alarmlist functions
1		Digital alarm (positive slope)	LOCAL-Exoline.5540.DQ3	0 (active)	exc_DQ3_alarm	/manuals/BOT_GHS-007-02	text

Delay read cycles: 0
 Delay seconds: 0
 Discard inactive events:
 Priority (inactive): 0
 Alarm text (active): DQ3 high
 Limit: 0.0
 Alarm text (inactive): DQ3 low
 Command: LOCAL-Exoline.5540.DQ3=0
 Command text: reset DQ3

Figure 55: Alarm configuration, edit

9.6.3 Upgrade

Alarms were previously configured directly at data-point level. If the Greyhound Data Collector finds alarms defined in this way, it will present the user with an upgrade option. When upgrade is selected, new alarm points are automatically created and the parameters: alarm type, limit, name, alarm text active and alarm text inactive are imported.

Parameter	Description
Alarm type	Determines the alarm type, see table 25 below.
Alarm name	Name of the alarm-point.
Alarm text (active)	Description text for active alarm event.
Alarm text (inactive)	Description text for inactive alarm event.
Priority active	Priority (A-D) for active alarm event.
Priority inactive	Priority (A-D) for inactive alarm event.
Signal source	Data point used as input value.
Limit	High or low limit value for high/low limit alarm types.
Delay read cycles	The signal source value must fulfill the alarm criteria (e.g. over limit) for this number of consecutive reads before the alarm is generated.
Delay seconds	The signal source value must fulfill the alarm criteria (e.g. over limit) for this number of seconds before the alarm is generated.
Discard inactive events	Dont generate inactive events.
Document	Link a document to the alarm. See section 7.2 for more information about document handling.
Schematic	Link a schematic to the alarm.
Command	Configure a command which the user can execute directly from the alarm list (see section 5 for more information about the alarm list). Commands are entered in the format: "data point address=value", e.g. "LO-CAL.con.controller1.alarm_state=0".
Command text	Text used as execute command link, e.g. "reset this alarm". When the user clicks this link in the alarm list, the corresponding command configured is executed.
Alarm format	Specific message format used for this alarm-point. See section 9.7.3 for more information about messaging formats.

Table 24: Alarm point paramters

Alarm type	Description
Digital alarm (positive slope)	Generate active alarm when signal source value is 1 (limit parameter not used).
Digital alarm (negative slope)	Generate active alarm when signal source value is 0 (limit parameter not used).
High limit alarm	Generate active alarm when signal source value is over the "Limit" specified.
Low limit alarm	Generate active alarm when signal source value is below the "Limit" specified.

Table 25: Alarm types

9.7 Accounts

9.7.1 Overview

The accounts page is where all the user specific settings are configured. Each account corresponds to a user and is divided in two parts: security and messaging. The security part handles all Greyhound Data Collector user validation and authorization such as login and specific page access. The messaging part is where the users recipient addresses such as e-mail and sms addresses are configured. The accounts are categorized in different user groups. Each user groups corresponds to a specific security/access level but doesn't have any meaning or affect on the messaging settings.

The accounts page top menu offers the following function links:

Function	Description
Add user group	Add a new (generic) user group.
User login status	Shows the users currently logged in.
Clear outgoing message queue	Deletes all currently queued messages. Tooltip shows the number of messages queued.
Send message	Send messages to one or all configured recipient addresses.
Apply security changes	Required after having changed any security setting such as page access, login names, passwords, new/deleted or moved user.

Table 26: Top menu function links

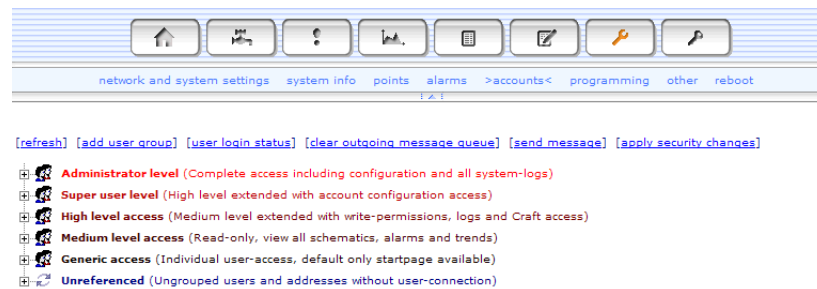


Figure 56: Account configuration, overview

9.7.2 Security

User security settings are divided in two parts: user parameters such as name, password etc, and page/function access. User parameters are viewed and configured by clicking the user name. See table 9.7.2 below for information about all available user parameters. The page and function access is found if both the user and the security tree-nodes are opened (with the '+' icons). The security tree-node is divided in four parts: read-, write-, schematic- and system components access. The read and write parts defines from/to which Greyhound Data Collector addresses read and write is possible. A user can hence for example be configured to have read access from the entire system but only write access to a specific connection or device, e.g. "LOCAL.con1.controller_basement". See section 9.5.2 for more information about Greyhound Data Collector addresses.

In the schematics part, users can be granted access to all or any other possible subset of the available schematics on the Greyhound Data Collector. If a user has access to a schematic where data point values from a non-authorized Greyhound Data Collector address are included, these particular values will not be displayed on the schematic. The "Value overview" page (see section 7.1) will however completely exclude devices to which the user hasn't got read access.

The "system components" represents the various pages and functions on the Greyhound Data Collector to which the user can be granted access. See table 9.7.2 for information about all available system component access objects.

The easiest way to grant a user access to the Greyhound Data Collector is to use the pre-defined medium-, high-, super user- or administrator level user groups. The user account will inherit the group authorization level and the only thing required to manually configure is the user security parameters, e.g. login name and password. Specific access settings found below the security tree-node (read/write/schematic/system) for users in these groups are readonly and can not be changed. Access authorization for users in the generic user group (or any user created group) can however be individually configured for each user account. Read, write and schematic access is then added by clicking the corresponding '+' icons which opens the respective select windows. To remove a read/write/schematic access, simply click the '-' icon in front of the access object. System component access is configured by clicking the "edit system access" link and then ticking the checkboxes of the respective objects. **Note:** Dont forget to apply the security changes after having changed the security settings.

Access-specification for the default user groups are found in table 9.7.2. **Note:** The unreferenced and Generic groups are not shown in this table. All unreferenced accounts (including connected messaging settings) are completely disabled and generic accounts has by default only login access.



Figure 57: User security parameters

Parameter	Description
User name	Name of the user.
Login name	Login name (UID)
Password	User login password (PWD).
Locked out	Account disabled (locked out). Note: Accounts are automatically locked out after 10 consecutive failed login attempts.
Valid from	Account is valid from this date and time.
Valid until	Account is valid until this date and time.
Inactivity timeout	Forced automatic logout after this number of seconds of user inactivity.
Allow login from	Possible to specify a specific ip or net address from where the corresponding user is allowed to login, e.g. 123.23.45.75 or 243.24.*.*
Startpage	User startpage after a successful login.

Table 27: User security parameters

The "edit" link opens an edit window where all the parameters can be configured. Users can also be moved to another user group from this window. The "delete" link moves the user account to the "unreferenced" group or completely deletes the account if "delete" is selected for accounts already in the "unreferenced" group. **Note:** Default administrator account can neither be moved to another group or deleted.



Figure 58: Security configuration tree view, pre-defined user group

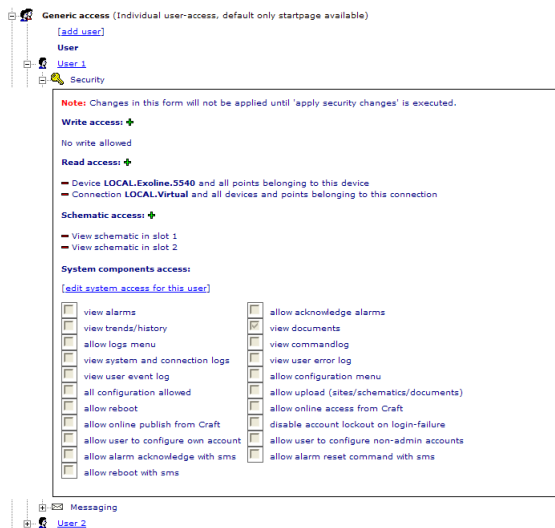


Figure 59: Security configuration tree view, generic group

Component	Description
View alarms	View alarm status end events (see 5).
View trends	Access the trend/graph page (see 6).
Documents and reports	Access to documents and value overview report (see 7). Note: "Value overview" requires read access in order to display values.
Logs menu	Access server logs menu (see 8).
Command log	View command events in the server log (see 8).
Configuration menu	Access configuration menu (required in order to "configure own account").
Configure own account	Configure the basic security parameters such as name and password as well as messaging recipient addresses for its own account. Note: User cannot change authorization/security level.
Acknowledge alarms	Acknowledge alarms in the alarm lists (see 5).
System/connection logs	View system and connection events in the server log (see 8).
Upload	Allow upload of Craft sites, documents and schematics.
Craft online access	Online access to data points etc from Craft.
Craft online publish	Online publish from Craft.
Alarm acknowledge with SMS	Allow acknowledge commands from the users messaging SMS address (see table 32).
Alarm reset command with SMS	Allow reset commands from the users messaging SMS address (see table 32).
Configure non-admin accounts	Full configuration access for all non-admin accounts.
User error log	View user error events (failed login etc) in the server log (see 8).
User event log	View user events (login etc) in the server log (see 8).
All configuration allowed	Complete configuration access.
Reboot	Allow user to reboot the Greyhound Data Collector (see 9.14).
Dont lockout on failed login	Disable the automatic account lockout on 10 consecutive failed login attempts.
Allow reboot with SMS	Allow reboot command (sms with text = 'reboot') from the users messaging SMS address.

Table 28: System components access objects

Component	Medium	High	Super user	Administrator
Value read access	X	X	X	X
All schematics	X	X	X	X
View alarms	X	X	X	X
View trends	X	X	X	X
Documents and reports	X	X	X	X
Logs menu	X	X	X	X
Command log	X	X	X	X
Configuration menu	X	X	X	X
Configure own account	X	X	X	X
Write value access		X	X	X
Acknowledge alarms		X	X	X
System/connection logs		X	X	X
Upload		X	X	X
Craft online access		X	X	X
Craft online publish		X	X	X
Alarm acknowledge with SMS		X	X	X
Alarm reset command with SMS		X	X	X
Configure non-admin accounts			X	X
User error log				X
User event log				X
All configuration allowed				X
Reboot				X
Dont lockout on failed login				X
Allow reboot with SMS				X

Table 29: Default user groups component access

9.7.3 Messaging

The Greyhound Data Collector messaging system handles all messages sent by the Greyhound Data Collector to recipient addresses. Messages can be sent in three different ways: as e-mails, sms:s through a GSM modem or as messages printed directly on a Greyhound Data Collector serial port. A corresponding "service" must be configured and used for the respective messages. A SMTP service is used for e-mail recipients, a GSM modem service for sms and a serial port service for printer messages. The services defines for example which SMTP server to use or the serial port parameters (e.g. baudrate, parity etc) the connected GSM modem uses. Services are not account specific, i.e. a single SMTP service can be used for all e-mail recipients, and the services are therefore not configured on the accounts page. See section 9.10.1 for more information about messaging services.

The Greyhound Data Collector messaging system handles seven types of messages: alarms, status reports, data reports, system events, connection events, security events and command events. All types except data reports are configured for each recipient address in the messaging tree-node. "Data reports" are generated by the SoftPLC and the recipient addresses used for the respective reports are configured directly in the SoftPLC rule which creates the report. See section 9.8.3 for more information about the SoftPLC. The other message types are described in table 30 below.

Message type	Description
Alarms	All alarms read and generated by the Greyhound Data Collector can be sent in various formats.
Status reports	Status reports are generated internally and contains overall system performance. See section 9.10.3 for information about how status reports are generated.
System events	Various system level events (also displayed in the server log, see section 8).
Connection events	Various connection level events (also displayed in the server log, see section 8).
Security events	Various security and user validation (login etc) events (also displayed in the server log, see section 8).
Command events	Write commands executed by the users (also displayed in the server log, see section 8).

Table 30: Message types

Add/edit/delete recipient addresses, parameteres and funtions

Each account can be configured with one (or more) recipient address(es). To add a new recipient address, click the "add address" link. This creates a new recipient address entry which then must be configured. All configurable parameters and functions have an edit ('pencil') and a delete ('minus') icon directly to the left. The green 'plus' icon to the right of "Receive alarms from" and time/text filters adds a new entry for the respective function. After having added for example a new text filter, the new filter entry must be edited and saved. Table 31 below describes the various parameteres and functions which can be configured for a recipient address. The parameters in bold are required and must be configured by the user whilst the others are optional. **Note:** By default a new recipient address is pre-defined to receive all alarm messages.

[refresh] [add_user_group] [user_login_status] [clear_outgoing_message_queue] [send_message] [apply_security_changes]

- [-] **Administrator level** (Complete access including configuration and all system-logs)
 - [add_user]
 - User
 - [-] Administrator
- [-] **Super user level** (High level extended with account configuration access)
 - [add_user]
 - User
 - [-] Mike Johnson
 - [-] Security
 - [-] Messaging

[add_address]

Address	Type	Service	Format subject	Format body
- mike@mail.com	normal	SMTP	alarm from [SN]	[D]([ADR],[TR])

Receive alarms from +

- System LOCAL and all connections, devices and points belonging to this system

No time filters defined +

No text filters defined +

Other message types

- Send status reports
- Send system events
- Send connection events
- Send security events
- Send command/write events

- [-] **Medium level access** (Read-only, view all schematics, alarms and trends)
- [-] **Generic access** (Individual user-access, default only startpage available)
- [-] **Unreferenced** (Ungrouped users and addresses without user-connection)

Figure 60: Recipient addresses

Parameter/function	Description
Address	The recipient address, e.g. an e-mail address or a phone number.
Type	"Normal" or "Delayed". Normal means that all alarms are sent immediately to the recipient address. Delayed means that only alarms that hasn't been acknowledged during the delay are sent. The delay time is by default 15 minutes but can be configured, see section 9.10.2.
Service	Select which messaging service to use, i.e. SMTP, SMS or PRINT (see section 9.10.1).
Format subject/body	Alarm messages are formatted with 'tags' and free text. A tag corresponds to a specific field in the alarm, e.g. description, priority etc, and the tag is replaced with actual alarm information before being sent. "Format subject" is used in the email subject field and "Format body" in the email body field if it is an e-mail recipient address. If it is a sms or printer recipient both these fields are used together as one. See table 32 for all available tags.
Receive alarms from	Each recipient address must be connected to at least one Greyhound Data Collector address (see section 9.5.2) in order to receive alarms. Alarms which originates from the Greyhound Data Collector address level configured, and the levels below, will be sent. For example: "LOCAL.MyConnection" will result in that alarms from the connection "LOCAL.MyConnection" and devices/points belonging to this connection will be sent. Note: More than one entry can be configured. By default "LOCAL" (system level) is created which means that all alarms are sent.
Alarm time filters	With the time filters, users can decide not to receive alarms to the recipient address at certain dates, weekdays and times. More than one time filter can be used and combined to the same recipient address.
Alarm text filters	With the text filters, users can both decide not to receive alarms or to only receive alarms that contains a specific string. Specific alarm fields can be used in the filter if "tag=string" is specified, e.g. "[P]=A" means dont send (or only send) if the alarm has priority A. More than one text filter can be used and combined to the same recipient address.
Other message types	Tick the checkboxes to receive the corresponding message types. See table 30 for information about the available message types.

Table 31: Recipient address parameters and functions

Note: "Type" (normal or delayed), "format" (body and subject), "Receive

alarms from” and time/text filters only affects alarm messages. The other message types (reports and system/connection/security/command-events) is hence not affected by these parameters and functions.

High level access (Medium level extended with write-permissions, logs and Craft access)

[add user]

User

Mike Johnson

Security

Messaging

[add address]

Address	Type	Service	Format subject	Format body
mike@mail.com	normal	SMTP	alarm from [SN]	[D] ([ADR], [TR])

Receive alarms from \oplus
System LOCAL and all connections, devices and points belonging to this system

Alarm time filters \oplus
Do not send between (hh:mm): 00:00 and 23:59

Use this filter if it is:

monday tuesday wednesday thursday friday saturday sunday

Use this filter between dates (MM-DD): 06-01 and 07-31 (e.g. 11-01 = november first)

No text filters defined \oplus

Other message types

Send status reports

Send system events

Send connection events

Send security events

Send command/write events

Figure 61: Edit time filter

High level access (Medium level extended with write-permissions, logs and Craft access)

[add user]

User

Mike Johnson

Security

Messaging

[add address]

Address	Type	Service	Format subject	Format body
mike@mail.com	normal	SMTP	alarm from [SN]	[D] ([ADR], [TR])

Receive alarms from \oplus
System LOCAL and all connections, devices and points belonging to this system

Alarm time filters \oplus
Dont send between 00:00 and 23:59 on tue, wed, thu between dates 06-01 and 07-31

Alarm text-filters \oplus
Dont send if alarm contains: water

Other message types

Send status reports

Send system events

Send connection events

Send security events

Send command/write events

Figure 62: Edit text filter

Format tag	Description
'[SN]'	Server name configured in system and network settings.
'[N]'	Alarm (alarm point) name.
'[D]'	Alarm description (alarm point active/inactive texts).
'[TR]'	Timestamp read.
'[TA]'	Timestamp of alarm (might be different from "timestamp read" if it is a scanned (not generated) alarm).
'[F]'	All alarm flags.
'[S]'	Alarm status (alarm or normal).
'[P]'	Alarm priority (A, B, C or D).
'[ADR]'	Alarm Greyhound Data Collector address/signal source.
'[AC]'	SMS Acknowledge alarm command. If this tag is used instructions on how to acknowledge the alarm remotely with an SMS is included in the message. Note: The acknowledge sms must be sent from a phone number configured as a recipient address to a user account which is authorized to send the SMS acknowledge command, see section 9.7.2 for more information about security and user account authorization.
'[RC]'	SMS reset alarm command. If this tag is used instructions on how to execute the configured alarm point command remotely with an SMS is included in the message. Note: The reset command sms must be sent from a phone number configured as a recipient address to a user account which is authorized to send the SMS reset command, see section 9.7.2 for more information about security and user account authorization and section 9.6 for information about alarm commands.
' '	Adds a linefeed to the message.

Table 32: Message format tags

Alarm format can also be configured specifically on alarm point level (see section 9.6) and if so, it overwrites the recipient address specific format specified. Since there is only one format field available to each alarm point, two additional tags can be used for alarm point specific formats: '[SUBJECT]' and '[BODY]'. Everything after '[SUBJECT]' but before '[BODY]' is used as "Format subject" and the part after '[BODY]' is used as "Format body".

Example: "[SUBJECT]Alarm [N] from [ADR][BODY][D]Occurred at [TR]".

Example

In the following example user Administrator has two recipient addresses. The email address ("admin@mail.com") receives all alarms immediately. Security events and status reports are also sent to this address.

The sms address ("0707123456789") only receives unacknowledged (delayed) alarms from either the "5540" or "IPRouter" devices, outside office hours at week-days and if the string "high water level" is found somewhere in the alarm.

The screenshot shows the configuration for the Administrator account, divided into two sections for different recipient addresses.

Administrator

- Security
- Messaging

[add_address]

Address	Type	Service	Format subject	Format body
admin@mail.com	normal	SMTP	alarm from [SN]	[D] ([ADR], [TR])

Receive alarms from +

- System LOCAL and all connections, devices and points belonging to this system

No time filters defined +

No text filters defined +

Other message types

- Send status reports
- Send system events
- Send connection events
- Send security events
- Send command/write events

Address	Type	Service	Format subject	Format body
0707123456789	delayed	SMS	alarm [D] from [SN] (not acknowledged)	

Receive alarms from +

- Device LOCAL.Exoline.5540 and all points belonging to this device
- Device LOCAL.EIBNet.IPRouter and all points belonging to this device

Alarm time filters +

- Dont send between 08:00 and 16:00 on mon, tue, wed, thu, fri between dates 01-01 and 12-31

Alarm text-filters +

- Send if alarm contains: 'high water level'

Other message types

- Send status reports
- Send system events
- Send connection events
- Send security events
- Send command/write events

Figure 63: Example

9.8 Programming

9.8.1 Overview

The Greyhound Data Collector can be programmed to process various logical "rules". The programming rules are of two types: Translator or SoftPLC. Translator rules are always created in the default translator group whilst SoftPLC rules can be created in either the default SoftPLC group or in SoftPLC groups created by the user.

The top menu edit and delete links affects all rules which have been selected with the respective checkbox in front of every rule. If the top menu checkbox "Point links" is checked all Greyhound Data Collector point addresses included in the various rules are displayed as links. Left click on this link opens the point overview page (see 9.5.13) whilst right click opens a popup where current point value can be viewed and possibly written (if point is writeable).

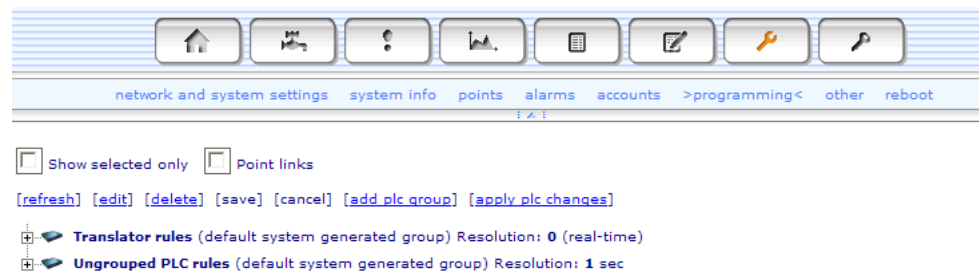


Figure 64: Programming overview

9.8.2 Translator

Translator rules are specialized for one purpose only, to transfer data point values to other data points. Each rule is configured with two points where at least one has to be writeable. The rule constantly checks the point values and if one has changed it is immediately written to the other point if the other point is writeable. Translator rules can therefore be used to move values from one connection (i.e. field bus) to another connection and hence translate values from one external device to another one. Values read from a Konnex field bus can for example be translated and used on a BACnet field bus.

Note: the server must be rebooted after having changed or added/deleted translator rules.

Show selected only Point links

[refresh] [edit] [delete] [save] [cancel] [add plc group] [apply plc changes]

Translator rules (default system generated group) Resolution: 0 (real-time)

[add translator-rule]

Point 1	Data direction	Point 2	Enabled
<input type="checkbox"/> LOCAL.EIBNet.IPRouter.button	==>	LOCAL.Exoline.5540.DQ1	yes
<input type="checkbox"/> LOCAL.EIBNet.IPRouter.temperature	==>	LOCAL.Exoline.5540.AQ1	yes
<input type="checkbox"/> LOCAL.Virtual.variables_1.var_1	<==>	LOCAL.Virtual.variables_2.var_1	yes

Ungrouped PLC rules (default system generated group) Resolution: 1 sec

Figure 65: Translator rules

9.8.3 SoftPLC

SoftPLC rules can be divided in different SoftPLC groups. The Greyhound Data Collector has a pre-defined ("Ungrouped") group and rules in this group are processed once every second. Other SoftPLC groups can be created with the "add plc group" link. User created groups can be configured with group name/description and resolution with the edit ('pencil') icon. Resolution decides how often rules in the corresponding group are processed. For overall system performance reasons, it is recommended to divide SoftPLC rules into different groups depending on the time-requirements of the rules. It is for example not necessary to process rules which handles slow processes, e.g. turn of the light once per day, every second.

A SoftPLC rule is configured with a number of criterias and actions. Criterias decides when to execute the configured actions. When the criteria(s) are fulfilled the rule goes active and executes the corresponding "positive slope" actions. Actions can also be configured to be executed on the "negative slope", i.e. when the rule goes inactive (hence criterias not fulfilled).

Criterias and actions are added to a rule be using the respective '+' icons in the rule overview box which is displayed if the rule is expanded. After having added the number of criterias and actions required, tick the rule checkbox and select "edit" in the top menu to configure the rule, criterias and actions.

Note: "Apply plc changes" (top menu link) is required after having changed or added/deleted SoftPLC rules.

See tables below for information about rule parameters and for descriptions of the various criteria and action types available.

Rule parameter	Description
Name	Rule name.
Description	Rule description.
Criteria logic	'AND' means that all criterias must be fulfilled in order for the rule to go active. As soon as at least one criteria isn't fulfilled, the rule goes inactive. If 'OR' is selected, the rule goes active as soon as (at least) one of the criterias is fulfilled and thus requires that none of the criterias are fulfilled for the rule to become inactive.
Enabled	Enable the rule.
Group	If rule is being edited, the rule can be moved to another group.
Current status	Displays if rule is currently active or inactive.
Actions executed	Displays the total number of actions executed since last system startup.

Table 33: SoftPLC rule parameters

Show selected only Point links
[\[refresh\]](#) [\[edit\]](#) [\[delete\]](#) [\[save\]](#) [\[cancel\]](#) [\[add_plc_group\]](#) [\[apply_plc_changes\]](#)

Translator rules (default system generated group) Resolution: 0 (real-time)
Reports (Sent to users) Resolution: 600 sec

Name	Description	Criteria logic	Enabled	Current status	Actions executed
value report values by email	AND	yes	1	5	
log report	logs by email	AND	yes	0	2

Force values (Check and force) Resolution: 1 sec

Name	Description	Criteria logic	Enabled	Current status	Actions executed
force locks	Weekend nights	AND	yes	0	0

Ungrouped PLC rules (default system generated group) Resolution: 1 sec

Figure 66: SoftPLC rules overview

Criteria type	Description
Value	Checks and compares a specific point value with the configured value.
Clock	Checks and compares the current time with the configured time.
Weekday	Checks and compares the current weekday with the configured weekday.
Day of month	Checks and compares the current day of month with the configured day of month.
Date	Checks and compares the current date with the configured date.
Compare	Checks the configured function. A function is specified with values, Greyhound Data Collector point addresses and the following mathematical expressions: +, -, *, /, >, < and =. Example: the compare criteria with function: "LOCAL.con.dev1.p1 + LOCAL.con.dev1.p2 > 5" is fulfilled when the sum of the values of points "p1" and "p2" is more than 5.
Number of alarms	Counts the number of alarms which originates from a specified Greyhound Data Collector address for a specific time and compares it to the specified limit.
Changed value	Checks is a specific point value changes.
Interval	Criteria is fulfilled every configured interval seconds.
PLC rule	Checks the status of another PLC rule.

Table 34: Criteria types

Action type	Description
Copy	Writes the current value of one point to another point.
Write	Writes a configured value to a point.
Alarm	Adds a alarm to the alarm event list. Note: These events are automatically connected to a virtual SoftPLC connection and device which are automatically created.
Log report	Creates a log report. Report can be viewed in the "documents" PLC reports directory (see 7.2) and also automatically sent to messaging recipient addresses (see section 9.7.3).
Value report	Creates a value report. Report can be viewed in the "documents" PLC reports directory (see 7.2) and also automatically sent to messaging recipient addresses (see section 9.7.3).

Table 35: Action types

Show selected only Point links
[\[refresh\]](#) [\[edit\]](#) [\[delete\]](#) [\[save\]](#) [\[cancel\]](#) [\[add plc group\]](#) [\[apply plc changes\]](#)

Translator rules (default system generated group) Resolution: 0 (real-time)
Reports (Sent to users) Resolution: 600 sec

Name	Description	Criteria logic	Enabled	Current status	Actions executed
value report	values by email	AND	yes	1	5
log report	logs by email	AND	yes	0	2

Force values (Check and force) Resolution: 1 sec

Name	Description	Criteria logic	Enabled	Current status	Actions executed
force locks	Weekend nights	AND	yes	0	0

Rule status overview:
 Rule hasn't executed any actions yet.
 Actions executed since last system startup:
 positive slope (criteria(s) fulfilled) : 0 (0 failed)
 negative slope (criteria(s) not fulfilled) : 0 (0 failed)
[Last state-changes](#)

Criteria:

- Type** **Criteria fulfilled when...**
- Weekday Weekday is in between saturday and sunday. Current weekday is friday.
- Clock Time is less than 08:00. Current time is 11:15.
- Value Point LOCAL.door_control.basement.main_lock is equal to 0 for at least 60 seconds.

Actions on positive slope:

- Type** **Description**
- Write 1 is written to LOCAL.door_control.basement.main_lock
- Alarm An alarm with text: 'Locked all basement doors' is generated

Actions on negative slope:

- Type** **Description**
- Alarm An alarm with text: 'Doors confirmed locked' is generated

Ungrouped PLC rules (default system generated group) Resolution: 1 sec

Figure 67: SoftPLC rules

Show selected only Point links
[\[refresh\]](#) [\[edit\]](#) [\[delete\]](#) [\[save\]](#) [\[cancel\]](#) [\[add plc group\]](#) [\[apply plc changes\]](#)

Translator rules (default system generated group) Resolution: 0 (real-time)
Reports (Sent to users) Resolution: 600 sec

Name	Description	Criteria logic	Enabled	Group	Current status	Actions executed
value report	values by email	AND	yes	Reports	1	5
log report	logs by email	AND	yes	Reports	0	2

Force values (Check and force) Resolution: 1 sec

Name	Description	Criteria logic	Enabled	Group	Current status	Actions executed
<input checked="" type="checkbox"/> force locks	Weekend nights	AND	<input checked="" type="checkbox"/>	Force values	0	0

Rule status overview:
 Rule hasn't executed any actions yet.
 Actions executed since last system startup:
 positive slope (criteria(s) fulfilled) : 0 (0 failed)
 negative slope (criteria(s) not fulfilled) : 0 (0 failed)
[Last state-changes](#)

Criteria:

- Type** **Criteria fulfilled when...**
- Weekday Weekday is in between 6-7 (1 = monday...7 = sunday)
- Clock Time is less than 08:00
- Value The value of point: LOCAL.door_control.basement.main_lock is equal to 0 for

Actions on positive slope:

- Type** **Description**
- Write 1 to point LOCAL.door_control.basement.main_lock
- Alarm Generate an alarm with text Locked all basement doors

Actions on negative slope:

- Type** **Description**
- Alarm Generate an alarm with text Doors confirmed locked

Ungrouped PLC rules (default system generated group) Resolution: 1 sec

Figure 68: Edit SoftPLC rules

9.9 Other: Start page

The first page when the user has logged in is by default a simple logotype or similar. It is however possible to configure the system to show information on the first page, and even to publish a schematic. Start page configuration is found if the "start page" tree node on the "Other" page is opened.

The different functions of the custom start page are described below.

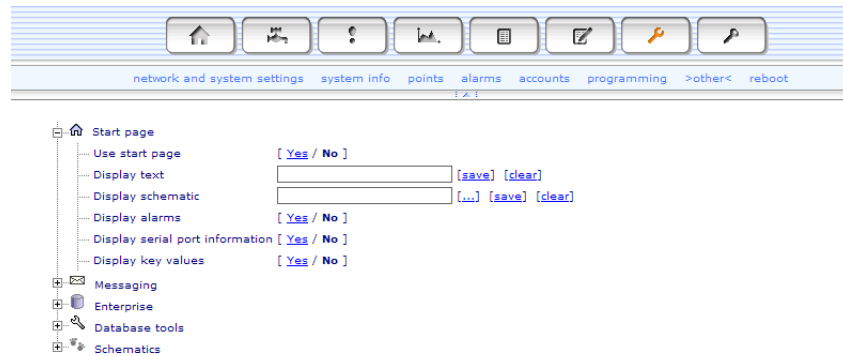


Figure 69: Start page configuration

Use start page: Select 'Yes' to enable the various functions described below.

Display text: The user can add text such as for example a link of choice to be shown on the first page.

Display schematic: The user can select a schematic to be shown on the first page.

Display alarms: The 'Alarms' section of the custom start page displays an overview of the current alarm status. It lists four types of statistics:

- Number of alarms currently active and not acknowledged.
- Number of alarms currently active and acknowledged.
- Number of alarms currently inactive and not acknowledged.
- Number of alarms currently blocked.

There is also a link which leads directly to the alarms list (click 'more...'). See section 5 for more information about alarms.

Display key values: The 'Values' section displays a selection of points and their current values. A maximum of three points can be chosen. Choose a point by adding 'V' into the flag-field in the database-editor. It also displays the current error rate, calculated by: $\text{error rate} = \text{Number of points with errors} / \text{Number of readable points}$.

Display serial port information: Provides a brief summary of the serial port status for port one and two. There is also a link which leads directly to the system settings page (click 'more...').

9.10 Other: Messaging

The messaging settings described in this section are not account specific and are used by all messaging recipients. For information about the account specific messaging settings (recipients etc), see section [9.7.3](#).

9.10.1 Services

Messaging services are used by the Greyhound Data Collector to send messages to messaging recipients. They define for example which smtp server or serial port to use and each recipient address configured in 'accounts' is connected to a specific service. Three types of services are supported by the Greyhound Data Collector: 'SMTP', 'SMS' and 'PRINT'. The Greyhound Data Collector has by default one of each service type pre-defined but these must be configured before being used. Services can be added with the respective "add" links and more than one service of the same type can be added, configured and used. To configure a service, click the edit icon ('pencil') just to the left of the respective service. The delete icon ('red minus') deletes the service but please note that all recipient addresses which are connected to the deleted service then must be configured to use another service. See table below for more information about the available service types.

Service type	Description
SMTP	Used by e-mail recipient addresses. It is required to configure the smtp server address. Sender address as well as smtp server login name and password might be required as well. These parameters should all be supplied by the network (and e-mail) service provider. If the Greyhound Data Collector operates through a dial out connection the 'Use dial out connection' checkbox must be checked. See section 9.3.5 for information about how to configure a modem dial out connection.
SMS	Used by sms recipient addresses. The Greyhound Data Collector sends sms:s through a GSM modem which is connected to a serial port on the Greyhound Data Collector. Which port to use as well as the various serial communication parameters (baudrate, parity etc) used by the GSM modem must be configured. The 'additional AT command' is not required but can be used to for example GSM operator login command if this is not stored in the connected GSM modem.
PRINT	Used to print messages directly to a printer connected to a serial port on the Greyhound Data Collector. Which port to use as well as the various serial communication parameters (baudrate, parity etc) used by the printer must be configured.

Table 36: Service types

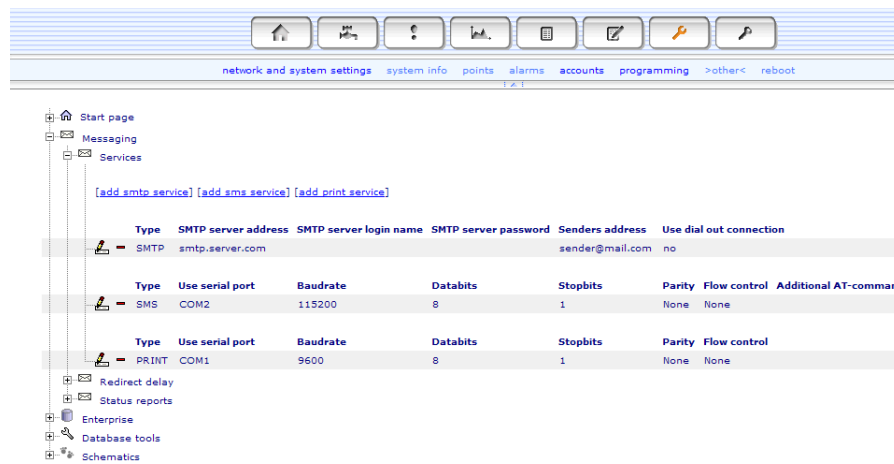


Figure 70: Messaging services

9.10.2 Redirect delay

Messaging recipient addresses can be configured to only receive alarm that has remained unacknowledged for a certain amount of time ('delayed' recipient type). Unacknowledged alarms are redirected to these recipients after this delay (if they are still unacknowledged). The delay is specified in seconds and are by default 900 (= 15 minutes). To edit the delay, click the edit icon ('pencil'). See section 9.7.3 for more information about 'delayed' messaging recipients.

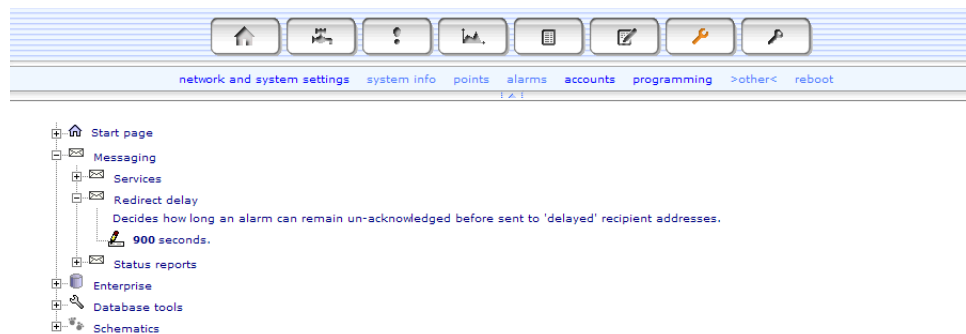


Figure 71: Messaging redirect delay

9.10.3 Status reports

A messaging recipient can be configured to receive internal status reports which are generated automatically by the Greyhound Data Collector at a certain interval. These reports contains overall system status and performance. Users can decide how often these reports should be generated (default once every hour) as well as the report format. The 'LONG' format contains all available information but it is

not reasonable to send this report to for example a sms recipient. The 'SHORT' format only contains ip information and system load and is therefore possible to send to a sms recipient as well.

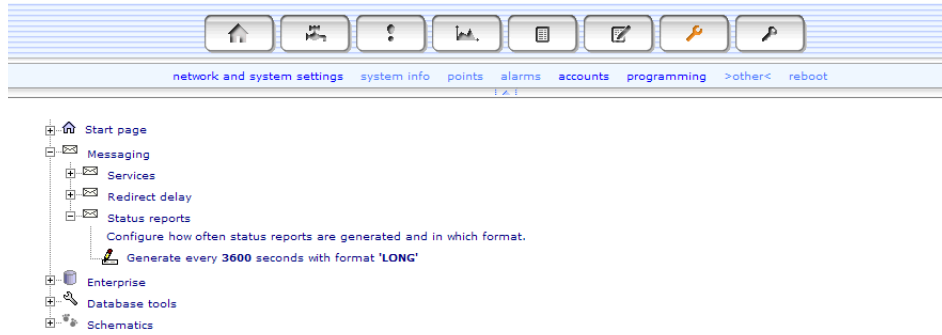


Figure 72: Messaging status reports

9.11 Other: Enterprise

A Greyhound Data Collector can be configured to send logs, values and alarms to a Enterprise server. This is sent in e-mails and the Enterprise e-mail address must hence be configured. Use the "add" link to add a new Enterprise address entry and the edit icon ('pencil') to configure the e-mail address as well as which messaging SMTP service to use. All alarms will be automatically copied to the Enterprise server through this address but values and logs are sent with SoftPLC data reports and the Enterprise recipient address must therefore be manually connected to these SoftPLC rules. See section 9.8.3 for information about the SoftPLC.

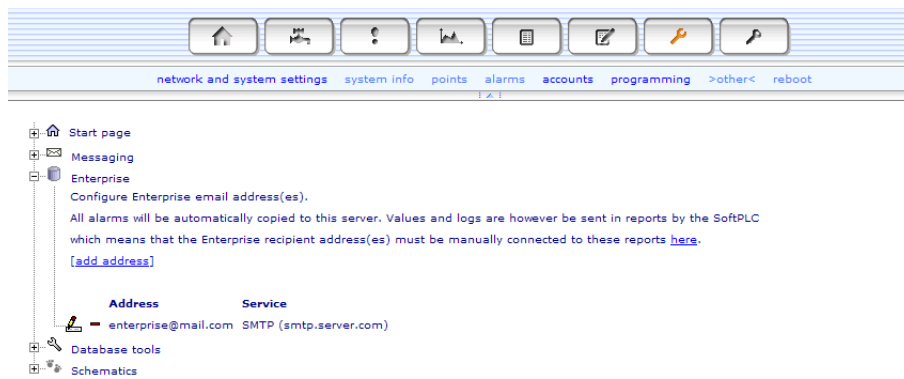


Figure 73: Enterprise configuration

9.12 Other: Database tools

Database tool	Description
Purge alarm events	Empties the alarm events log.
Purge system log	Empties the system events log.
Purge connection log	Empties the connection events log.
Purge messages sent log	Empties the 'messages sent' log.
Purge messages failed log	Empties the 'messages failed' log.
Purge command log	Empties the commands log.
Purge security events	Empties security events log.
Purge security error events	Empties security error events log.
Backup database	Copy and backup the entire database to the permanent storage disk. This is also performed automatically once every other hour and when the Greyhound Data Collector is rebooted.
Optimize database	Cleans and optimizes the database files.

Table 37: Database tools

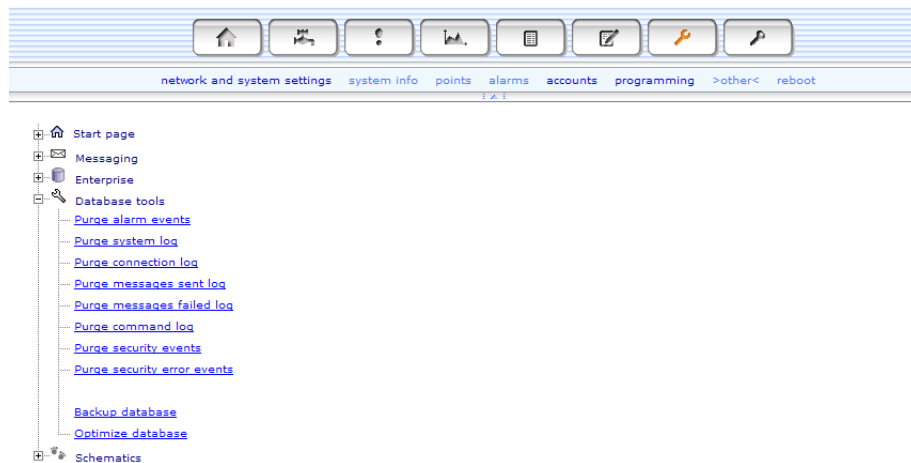


Figure 74: Database tools

9.13 Other: Schematics

The basic parameters of the schematics published to the Greyhound Data Collector can be viewed in the 'Schematics' section. Users can also decide to show or hide the respective schematic sub-menu link in the main schematics section (see section 4) with the Active "Yes/No" links.

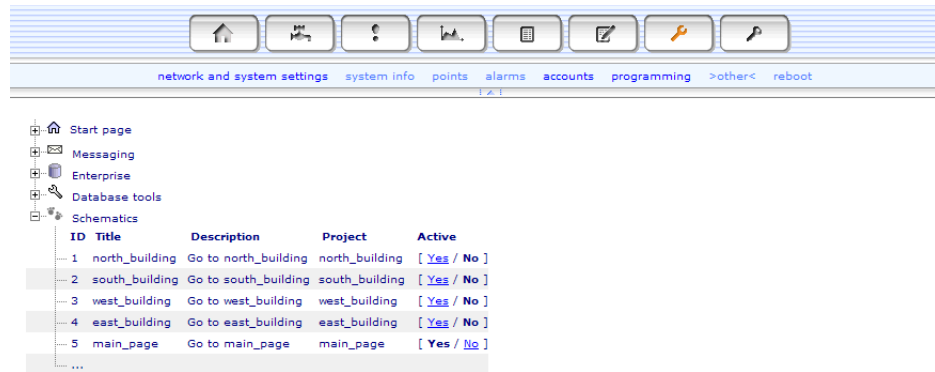


Figure 75: Schematics list

9.14 Reboot

Reboot the Greyhound Data Collector by clicking the reboot button. A complete backup of the internal database is performed prior to the actual reboot and the backup progress is displayed directly on the page. When the backup has finished, the Greyhound Data Collector is rebooted and when it has restarted the browser is automatically redirected the login page. **Note:** If the ip address and/or the http-port has been changed, the new address must be manually entered in the browser address bar after the reboot. Furthermore, a Greyhound Data Collector can not be rebooted again within the first 2 minutes after a reboot.



Figure 76: Reboot page

10 Log out

To log out from the Greyhound Data Collector, click the last main menu icon. If a user doesn't manually logout, a forced automatic logout is performed once the "Inactivity timeout" expires.

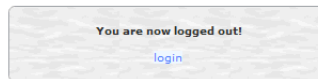


Figure 77: Log out

11 Tips and Tricks

11.1 Encrypted communication

The Greyhound Data Collector support the secure shell (SSH) protocol. SSH communication is encrypted and a SSH-tunnel can be used for accessing a Greyhound Data Collector. This requires that a SSH client program is located on the computer from where you want to access the Greyhound Data Collector. In the following example the SSH client 'Putty' is used.

1. Choose 'Tunnels' in the left view and enter a local port and the destination. The destination is entered in the form: ip address:port. If we want to access the web on the Greyhound Data Collector the destination port should be the webserver port 80 (if not changed). In this example the local port is 4500 which means that the Greyhound Data Collectorweb will be available through the local port 4500.

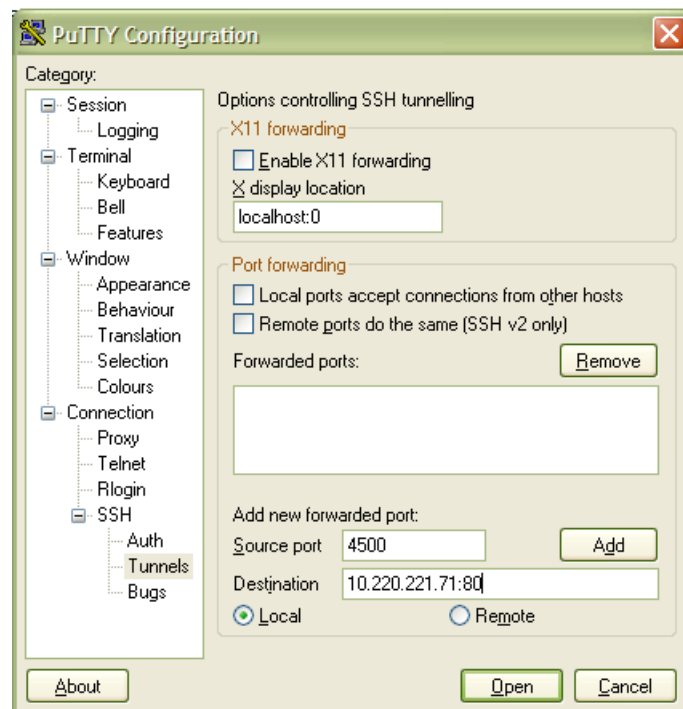


Figure 78: SSH tunnel

2. Select 'Session' in the left view and type in the destination IP address.
3. Select the SSH radio box and click 'Open'.

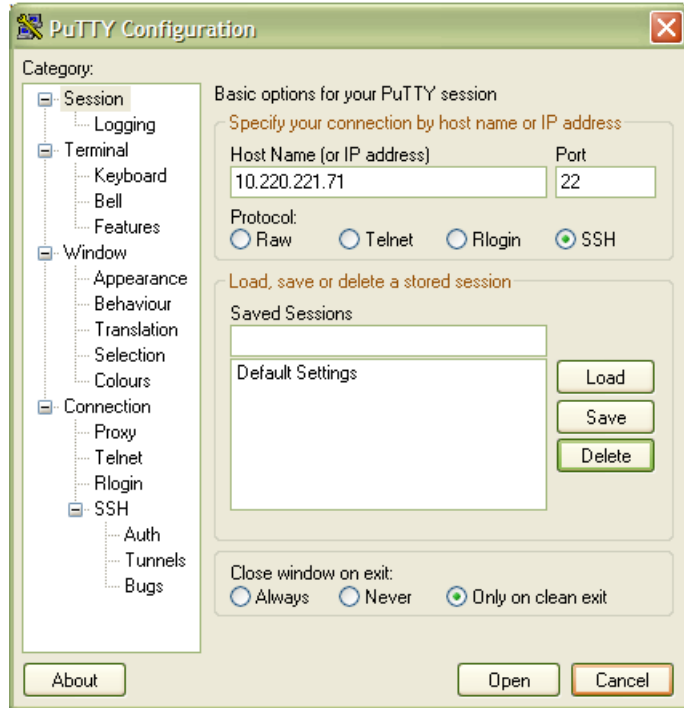
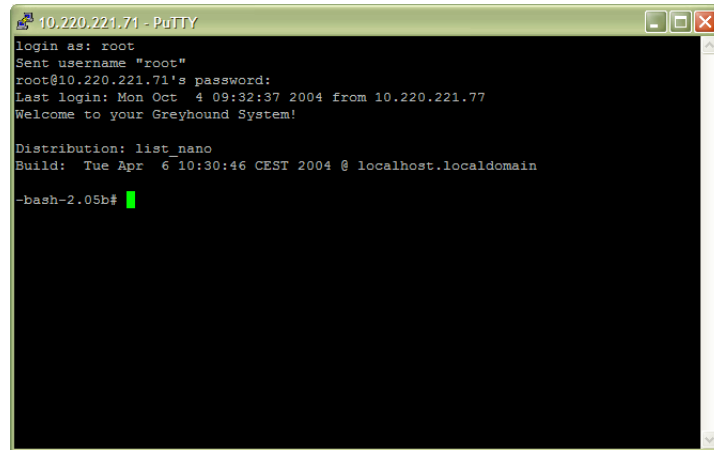


Figure 79: SSH tunnel

4. Log in on the destination Greyhound Data Collector. Default username: 'root' and password: '_ChangeRootPass'.



```
10.220.221.71 - PuTTY
login as: root
Sent username "root"
root@10.220.221.71's password:
Last login: Mon Oct  4 09:32:37 2004 from 10.220.221.77
Welcome to your Greyhound System!

Distribution: list_nano
Build: Tue Apr  6 10:30:46 CEST 2004 @ localhost.localdomain

-bash-2.05b#
```

Figure 80: SSH tunnel

5. To surf the Greyhound Data Collector through the ssh tunnel enter 'http://localhost:4500' in a webbrowser.

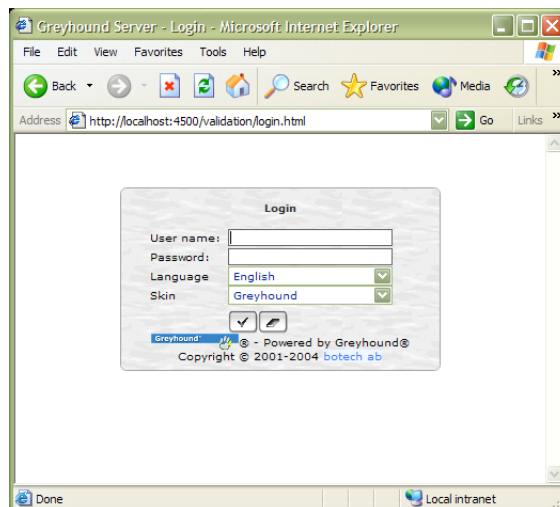


Figure 81: SSH tunnel

The local SSH program is connected to the Greyhound Data Collector on the TCP port 22 (ssh) which means that all services, except SSH, can be blocked on the Greyhound Data Collector.

11.2 Performance

Sometimes with an overloaded system, browsing the system is quite slow. Also timeouts when reading and writing data can occur. The system in itself limits the number of points, logs etc. that the user can configure but since the different protocol drivers can deliver data ranging from 1 read per second up to over a hundred reads per second for each connection, it is up to the user to tune the system to perform optimally.

11.2.1 Browsing the unit

The best measure of the system performance is how the system respond when browsing it. The system should not be much slower when it is running the drivers and reading data, compared to when it is delivered and empty.

11.2.2 Settings/system

On the 'System information' page, available from the settings page (see 9.4 on page 42), there is a system monitor that displays current system status. The "Load average" is of special interest. A load average below 1.0 is very good. A load average between 1.0 and 2.0 is acceptable, but above that you should consider optimize the system (see below).

11.2.3 Optimize data reading

For each data read a number of operations is executed. Depending on the point configuration this can be alarm checking, log interval, cache update etc. It is quite natural to try to read all data as fast as possible, but this are often not required. To optimize the performance it can be required to slow down the update interval for the points. Most drivers have a sleeptime or similar that is used to reduce the number of reads per second. Some drivers have priority possibilities that makes it possible to get high update speed for the most interesting points. Block reads that reads many points in one request are also common.

EXOline (see ?? on page ??) example:

By setting the properties `Sleeptime=0`, `Blockread=1` a read speed of over 200 points per second can be achieved. For many sites this is unnecessary high. Depending on how the EXOline units are configured and what data types that is read, "`Sleeptime=100`, `Blockread=0`" or "`Sleeptime=1000`, `Blockread=1`" will give a speed of about 5-20 reads per second. Note! Sleeptime is measured in milliseconds.

11.2.4 Optimize data logging

Always try to log only data that is useful. The best way to do this is by selecting a loginterval that is meaningful for the process monitored. For example when logging the outdoor temperature a loginterval of 60 seconds will only fill the database with

useless values. A loginterval of 900 seconds (15 minutes) or 3600 (1 hour) is better. To optimize the log set the flag to "C" that only logs changes. To optimize even further, the Converter function Round(1) can be used to only log changes of 0.1 degrees or more. Also remember that real-time trends can be used to show faster processes (see the Craft Designer documentation).

11.2.5 Software version

Speed optimizations is often included in newer versions of the Greyhound Data Collector software and firmware. Always look for and consider updating the system.

11.3 Securing Greyhound Data Collector

Securing Greyhound Data Collector involves preventing

- Easy guessing of passwords and user names
- Use of services not intended for external use.
- Denial Of Service attacks (DOS-attacks)
- The use of backdoors or design flaws to gain control to the system
- Unlimited access for users

To support the prevention the Greyhound Data Collector has a built in firewall, a validation system that can limit access to all parts of the system and the possibility to encrypt network traffic. It is up to the installer to enable these features and to configure them correctly. To help in this work the following information is useful.

11.4 Passwords and user names

The factory default passwords should always be changed. Change both the administrator and root account passwords. Good passwords mix upper/lowercase characters, figures and other ASCII characters like "!?_". This way dictionary password guessing tools cannot find the password. They shall also be of a certain length to make it hard to guess it by using brute force guessing. The password quality is equally important when settings user passwords. Also use usernames other than "admin", "guest" or any other easy to guess usernames since they will be locked out by too many login attempts.

11.4.1 Bad passwords

Name of children, pet etc. Single words.

11.4.2 Good passwords

"S3r!es?", "9D_allas!"

11.5 Firewall

Always enable the firewall, and close all ports not necessary. It should be sufficient to only have the http port opened. It is also possible to close the http port and use an encrypted ssh tunnel for access (see section 11.1 on page 104). When having the firewall enabled with only http access, it is impossible to access any other system services like ftp or the database server. The built-in firewall shall not act as a replacement for a real Internet firewall. The built in firewall has no functionality to for example recognize certain patterns in the communication that is typical for hacking attacks, sense port scans etc. that even basic modern firewalls do. The build-in firewall can be compared with the level of security a good personal firewall.

NOTE! Always use an external good Internet firewall when connecting the Greyhound Data Collectorto the Internet.

11.6 DOS attacks

Denial Of Service (DOS-attacks) is difficult to be protected from if no external firewall is used. Use an external firewall! By moving the web-port or by allowing ssh only you can make it more complicated for hackers to perform a DOS-attack.

11.7 Firmware and software versions

Always monitor the changelog for the Greyhound Data Collector (the changelog is found on the ftp server). Sometimes security enhancements or firmware upgrades is performed, and it might be a good idea to upgrade the system.

11.8 Limiting access for users

Always only give users the access they really need to perform their tasks. It is generally not a good idea to let all users be administrator. Also let each user have their own user account because then you are able to monitor their usage of the system in the different logs (logins, changing of values etc.).

11.9 TPipe

The TPipe driver is a very powerful tool that lets you for example reprogram devices from a distance. When connected to the Internet, the use of TPipe is only acceptable if using a ssh tunnel, or a very well defined rule in the external firewall.