



ACCESS CONTROLLER

FB-10 MK2

User Manual

Document Revision 4.1

DOCUMENT REVISION HISTORY					
DOCUMENT REVISION	REVISION DATE	DESCRIPTION	GUI Version	Release	Approve
1.0	01 Nov 2008	Initial Preliminary Release	1.0.0.0	TC	JA
1.1	01 Jan 2009	Final Release	1.1.0.0	TC	JA
1.2	01 Feb 2009	IEC/FCC Approvals Added	1.2.0.0	TC	JA
1.3	10 Mar 2009	Static Routing & DAC Control	1.3.1.4	TC	JA
2.0	14 Jul 2009	User level restrictions MAC Address reservations	2.0.0.5	FR	JA
2.1	13 Nov 2009	FB10-PRO RM version added Italian Language Added Default Firewall Group	2.0.0.7	TC	JA
3.0	06 May 2010	Spend Control Added Lock MAC to IP Added DNS Blocking Added	3.0.0.0	TC	JA
3.1	21 Sep 2010	Switch Back Added Overheat protection Added	3.0.1.1	RB	JA
4.0	22 Dec 2011	Advanced DHCP Services Automatic Failover Added Bandwidth Management Bandwidth Monitoring QoS	4.0.0.0	RB	TC
4.1	09 Sept 2013	New Chassis Layout Updates to QoS Updates to Overheat Temps DHCP Gateway add.	4.3.0.0	RB	

© Livewire Connections Ltd

Unit 41 • Barwell Business Park

Leatherhead Road, Chessington, Surrey KT9 2NY

United Kingdom

Tel +44 (0) 207 9740 900 • Fax +44 (0) 207 9740 949

ALL RIGHTS RESERVED

Information in this document is subject to change without notice and does not represent a commitment on the part of Livewire Connections Ltd.

It is recommended to download the latest revision of the User Manual from <http://www.livewire-connections.com/support> or request a copy from your distributor.

Published in the United Kingdom

INDEX

		Page
1	Safety Summary	5
2	Disclaimer	6
3	Introduction	7
4	What's in the Box	7
5	Installation Guide	
	5.1 - Hardware Mounting	8
	5.2 - Typical Installation Network Diagram	9
	5.3 - Connecting your devices	11
	5.4 - Communicating with the FB-10	11
	5.5 - Installing Software	11
	5.6 - Login Prompt	11
6	5.7 - Activating your hardware	12
	6.1 - Admin Login	13
	6.2 - System Configuration	14
	6.3 - Call Detail / Control	16
	6.3.1 - Set Service Costs	17
	6.3.2 - Spend Controls	18
	6.4 - Reserved IP Settings	20
	6.5 - Internet Connections	21
	6.6 - Advanced Configuration	23
	6.7 - Group Settings (Firewall Groups)	24
	6.8 - Firewall Settings	26
	6.8.1 - DNS Settings	28
	6.9 - Port Forwarding	29
	6.10 - Static Routes	30
	6.10.1 - QoS Settings	31
	6.10.2 - Bandwidth Monitoring	33
	6.11 - Remote Access	37
	6.12 - User Configuration	38
	6.13 - Default Users	39
	6.14 - Support Information	40
6.15 - Factory Default Reset	41	
6.15 - Switch Back Settings	42	
6.16 - Automatic Fail Over	43	

7 User GUI	7.1 - User Login	45
	7.2 - User GUI Screenshot	45
	7.3 - User GUI (Restricted) Screenshot	46
	7.4 - User GUI Controls	47
8 Appendix	8.1 - Troubleshooting	59
	8.2 - Connection States Colour Indicators	51
	8.3 - Internet Connections - Templates	52
	8.4 - Interface Drawing	54
	8.5 - Hardware Drawing FB-10	55
	8.6 - Hardware Drawing Rack Mount Kit	56
9 Technical Specification		57
10 Further Information		57

1. Safety Summary



THE FOLLOWING GENERAL SAFETY PRECAUTIONS MUST BE OBSERVED DURING ALL PHASES OF OPERATION, SERVICE AND REPAIR OF THIS EQUIPMENT. FAILURE TO COMPLY WITH THESE PRECAUTIONS OR WITH SPECIFIC WARNING ELSEWHERE IN THIS MANUAL VIOLATES SAFETY STANDARDS OF DESIGN, MANUFACTURE AND INTENDED USE OF THE EQUIPMENT. LIVEWIRE CONNECTIONS LTD ASSUMES NO LIABILITY FOR THE CUSTOMER'S FAILURE TO COMPLY WITH THESE REQUIREMENTS.

GROUND THE EQUIPMENT

To minimise shock hazard, the equipment must be connected to an electrical ground.

AVOID INTERFERENCE

To avoid interference, do not run cables parallel to AC wiring, or near fluorescent lights or other high magnetic or electrical fields. Interference from these types of sources causes equipment to be faulty and will automatically void warranty conditions.

AVOID LONG CABLE LENGTHS

Any cable longer than 5 meters must be shielded, and all peripheral equipment must be grounded.

DO NOT OPERATE IN AN EXPLOSIVE ATMOSPHERE

Do not operate the equipment in the presence of flammable gases or fumes. Operation of any electrical equipment in such an environment constitutes a definite safety hazard.

DO NOT SERVICE OR ADJUST ALONE

Do not attempt internal service or adjustments unless another person, capable of rendering first aid resuscitation, is present.

KEEP AWAY FROM LIVE CIRCUITS

Operating personnel must not remove equipment covers. Only qualified maintenance personnel must make component replacement and internal adjustment. Do not replace components with the power cable connected. Under certain conditions, dangerous voltage may exist even with the power cable removed. To avoid injuries, always disconnect power and discharge circuits before touching them.

DO NOT MODIFY CONFIGURATION OF SOFTWARE

This product is a self-contained system installed and configured by a qualified distributor. Modification of software configuration can result in loss of communications and increased airtime bills. Configuration can only be done by or on written instruction by a qualified distributor.

ALWAYS FOLLOW MANUFACTURERS ADVICE

Suppliers and manufacturers of communications equipment and peripherals provide a wide range of advice on the correct installation of their equipment. The customer should always aim to follow the guidance as provided by suppliers and manufacturers.

2. Disclaimer



The Access Controller FB-10 and FB-10 PRO are products designed to provide visibility and control to off-vessel data communications. The product has no least cost routing functionality and is designed to aid the operator in switching between different off-vessel data connections.

It is the operator's sole responsibility to ensure that the connection selected is appropriate for the operator's data requirement. It is also the operator's sole responsibility to ensure that the connection is manually terminated at the end of each session. Livewire Connections strongly recommends that the operator checks the connection device equipment (such as handset display or modem status lights) to ensure the connection has been terminated. Livewire Connections strongly recommends that for connections that are billed per data used or per time used that additional Service Provider level traffic monitoring and spending control is applied.

The use of the inbuilt Firewall is strongly recommended to restrict unwanted outbound traffic. It is the operator's responsibility to ensure the firewall settings are correctly configured. The use of the inbuilt Spend Control is highly recommended to restrict unwanted traffic. It is the operator's responsibility to ensure the Spend Control feature is correctly configured. The Automatic Failover feature should be used in conjunction with Switch Back to ensure the primary service is resumed as soon as possible. The Automatic Failover feature should be used in conjunction with Spend Control if the secondary service is charged per Mb or per Min.

Livewire Connections Ltd accepts no liability whatsoever for any airtime costs incurred during the use of the Access Controller FB-10, FB-10 PRO & FB-10 PRO RM regardless of howsoever or by whom they have been incurred

The Access Controller is based on Debian GNU/Linux which contains free software made available under several licenses like GPL/LGPL and BSD. For the exact distribution terms for each program, please see the description available in individual files at <http://192.168.5.1/gpl> (the IP address may vary depending on your Access Controller FB-10 configuration).

Debian GNU/Linux comes with no warranty from the original software developer, to the extent permitted by applicable law. For any warranty issues, please contact your local distributor from which your Access Controller FB-10 was purchased.

3. Introduction

Congratulations on the purchase of your new Livewire Connections Access Controller FB-10. This device will manage all of your off-vessel data requirements and allow visibility and control for all your data traffic. The Livewire Connections Access Controller FB-10 can be configured in minutes to manage all your existing connections as well as adding additional firewall user group management, port forwarding, remote WAN to WAN access, spend control, QoS, Bandwidth Monitoring and data statistics.

From a simple single page graphical interface it is possible to manage all of your off vessel communications including, but not limited to **VSAT, Inmarsat Fleet & Fleet Broadband, Iridium OpenPort, Thuraya DSL, ISDN, GPRS/3G, Off-Vessel WiFi and Shore ADSL.**

4. What's in the box

The Access Controller FB-10 is shipped with the following components:

- Access Controller FB-10
- Localized AC/DC Power Supply
- Mounting Brackets (shelf or Rack mount specified when ordering).
- Warranty activation form
- Hardware test certificate
- Quick Start Guide / Bridge Reference Card



5. Installation Guide

5.1. Mount the hardware in a suitable location using the supplied mounting brackets. The following should be considered when choosing a suitable location:

- **Ventilation** – The FB-10 requires good ventilation. A minimum separation distance of 200mm is required from the heat sink on the top of the hardware and around the side vents. If the hardware is to be mounted in a cupboard or enclosure it is necessary to ensure the enclosure has good ventilation or cooling available at all times. There is a fan venting from the left side. It is necessary to ensure the fan is kept free from dust and cleaned when required.
- **Power supply** – The FB-10 must be connected to Uninterruptible Power Supply (UPS) / Surge Protector to prevent any damage from inconsistent onboard power.
- **Cable Length** – If it is intended to connect Serial devices to the FB-10 it is necessary to consider the maximum cable length recommended by the device manufacturer.
- **Mounting** – The FB-10 can be supplied with a Wall Mount/Shelf Kit or 19" Rack mount kit please specify when ordering the brackets you require. If in doubt one of our members of staff can assist you in choosing or recommending mounting solutions.

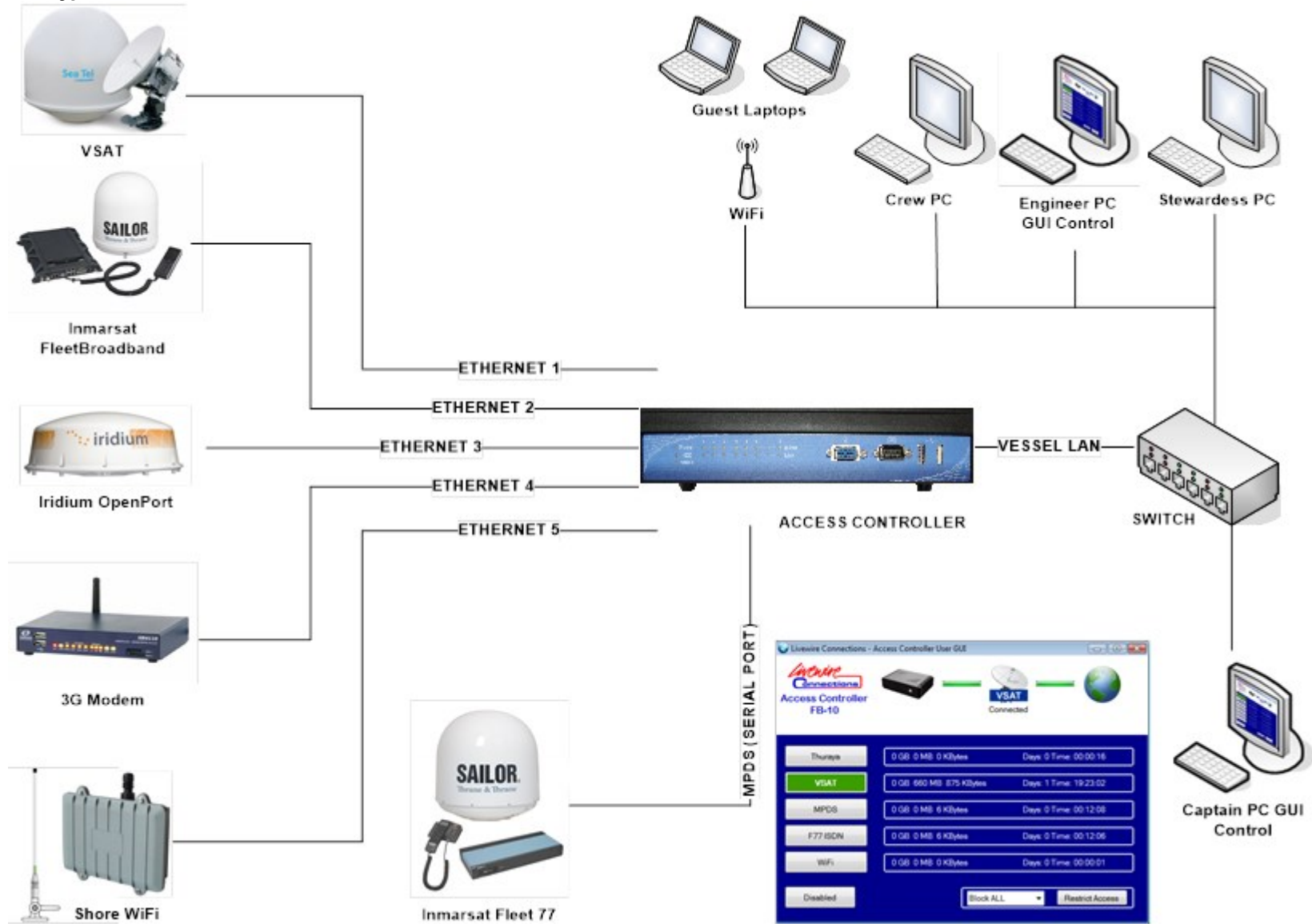
Rack Mounting Brackets



Wall/Shelf Mounting Brackets



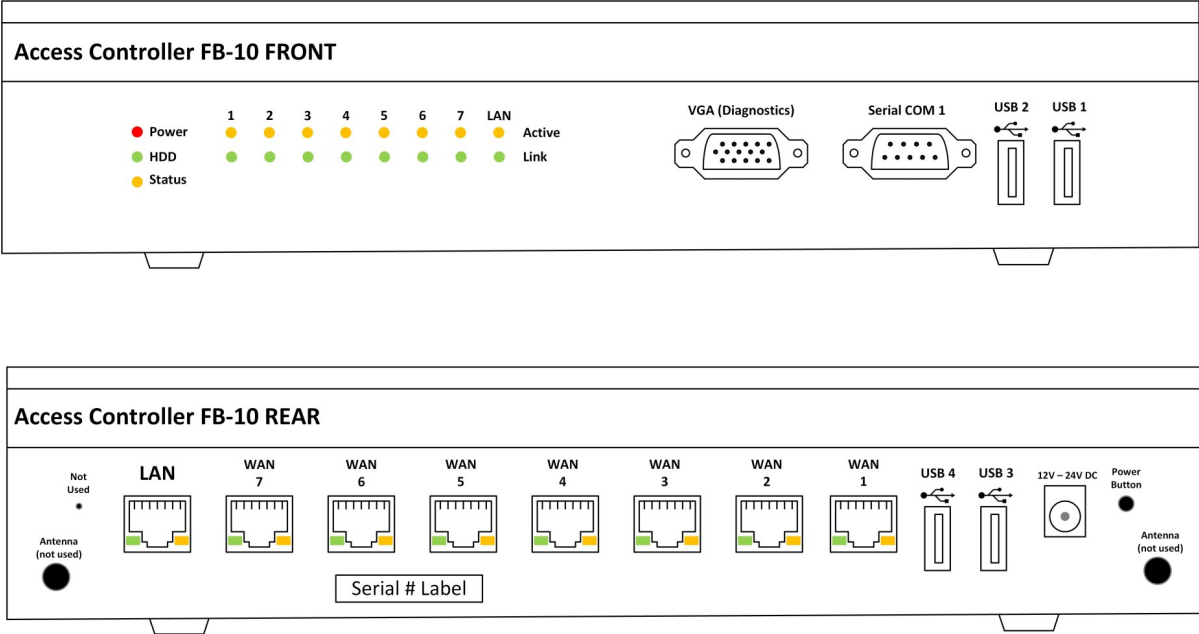
5.2. Typical Vessel Network Installation



5.3. Connect your off-vessel communication devices via either a Serial (DB-9 connector), Ethernet, or USB to Ethernet* connection.

Access Controller FB-10 Interface Diagram:

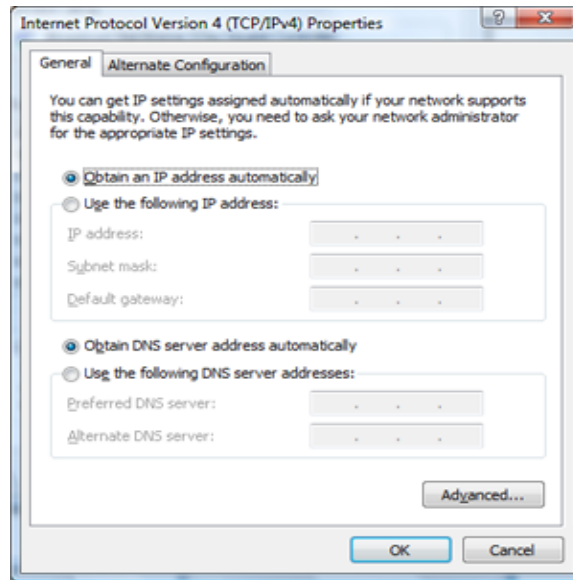
- 1 x Vessel LAN Ethernet RJ45 (Port 8)
- 7 x WAN Ethernet RJ45
- 1 x Serial
- 1 x VGA (For Livewire diagnostic use)
- 2 x USB Front (For approved USB to Ethernet convertor devices only)
- 2 x USB Rear (For approved USB to Ethernet convertor devices only)



**The support for approved USB devices is intended to increase the number of Serial or Ethernet ports by adding a USB to Serial/Ethernet convertor. For a full list of approved USB devices visit <http://www.livewire-connections.com/support> or contact your distributor.*

5.4. Connect 'Vessel LAN' port (LAN 8) to your onboard network switch or computer. (It may be necessary to use a crossover cable for direct connection to a computer). The default IP address of the FB-10 is **192.168.5.1**

5.5. As factory default the FB-10 has DHCP Server enabled. Ensure that your computer is configured to 'Obtain an IP address automatically' and 'Obtain DNS server address automatically' as per below and navigate to <http://192.168.5.1> in any web browser. If the page does not load see *Appendix 8.1 – Troubleshooting*



When the page loads click '**Click here for the Access Controller software**' button to download the software. Run the Setup file and follow the onscreen instructions.

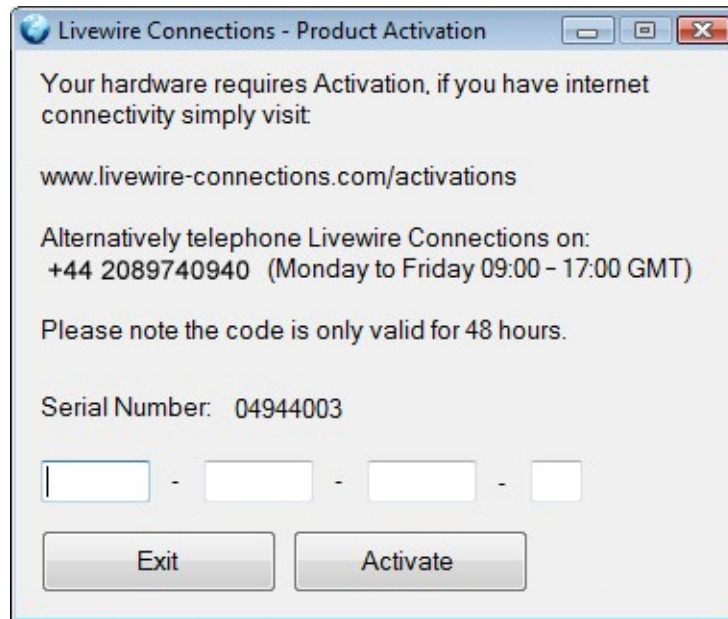
5.6. From the shortcut on the Desktop or from the Start Menu run the '**Access Controller**' shortcut.

When prompted enter the default admin username ('**admin**') and default admin password ('**password**'). Select '**Admin GUI**' and press **OK**



For further instructions please see either **Administrator GUI** or **User GUI** sections later in the manual.

5.7. Hardware Activation Code



When you login the first time you may be asked to enter the Hardware Activation Code. This Hardware Activation Code is available by either visiting <http://www.livewire-connections.com/activations> or by telephoning +44 (0) 208 9740 940 (Monday to Friday 09:00 – 17:00 GMT).

You will require the FB-10 Serial Number that is displayed on the Activation Prompt. When you receive the Hardware Activation Code, enter the code (without dashes) and click 'Activate'. Please note that the code is only valid for 48 hours and can only be generated a limited amount of times. Please also note that the code is case sensitive.

If you are not asked for the Hardware Activation Code the hardware may have been activated prior to dispatch by your distributor.

6. Administrator GUI (Graphical User Interface)

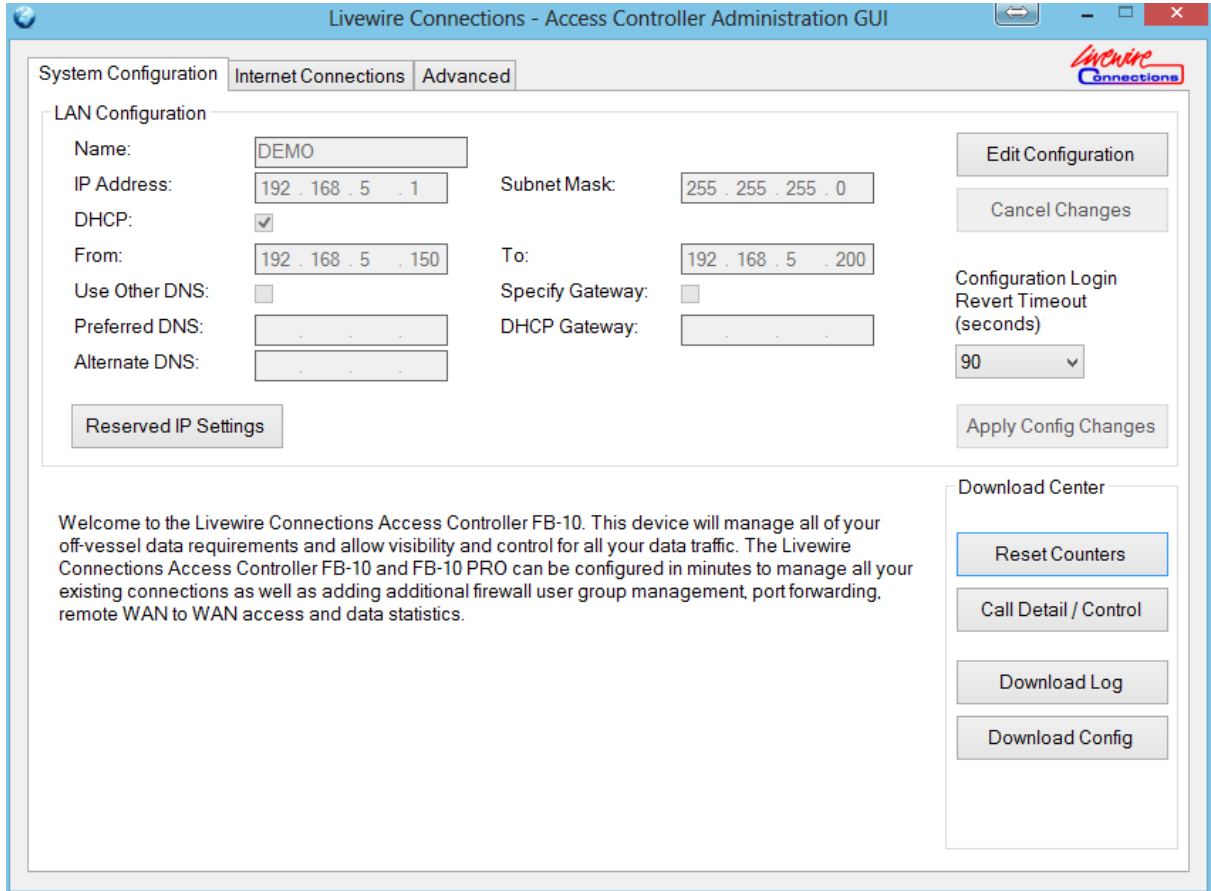
- 6.1. From either the shortcut on the Desktop or from the Start Menu open the '**Access Controller**'. When prompted enter the default admin username ('**admin**') and default admin password ('**password**'). Select '**Admin GUI**' and press OK. If the login is not successful see [Appendix 8.1 – Troubleshooting](#)



You will see the following tabs:

- [System Configuration](#) – Configure IP network settings for the Access Controller and Local Area Network (LAN). Managed DHCP Server settings if required. Download Call and System Logs and Configuration Files. Manage Call Spend Control.
- [Internet Connections](#) – Add, Edit and Delete Services (Internet Connections) to be controlled by the Access Controller.
- [Advanced](#) – Optional configuration of Firewall, QoS, DNS Blocking, Port Forwarding, Static Routing, WAN to WAN Remote Access, Sea Tel DAC Control, User configuration, Support and Firmware uploads.

6.2. System Configuration



The default IP Address for the FB-10 is **192.168.5.1** - by default the FB-10's inbuilt *DHCP* server is enabled with a default range of 192.168.5.100 – 192.168.5.200

To change the IP Address select '*Edit Configuration*' and enter the configuration as below:

LAN Configuration	
<i>Name</i>	Enter a name for the configuration (Eg Vessel Name). This name will appear on the User GUI.
<i>IP Address</i>	This is the IP address that will be assigned to the Vessel LAN port. Please note, this needs to be in the same IP range as your LAN or you will not be able to access the FB-10.
<i>Subnet Mask</i>	This is the Subnet Mask that will be assigned to the chosen port when selected. Typically this should be 255.255.255.0
<i>DHCP</i>	If selected the device will provide IP details to those devices set to automatically obtain network settings. This should be switched off if any other device on the network is configured to provide this functionality. WARNING – If you disable DHCP and forget the IP address range you might not be able to access the FB-10 without a Factory Reset
<i>From</i>	If DHCP is enabled this specifies the first IP Address issued from the FB-10 to devices on the network. This range should not be used by any other devices on the network otherwise IP Address conflicts may occur.
<i>To</i>	If DHCP is enabled this specifies the last IP Address issued from the FB-10 to devices on the network. This range should not be used by any other devices on the network otherwise IP Address conflicts may occur.

<i>Use other DNS IP Address</i>	If selected, the IP Address defined below will be provided as the primary DNS server, for instance if you have an internal Windows server or perhaps prefer to use public DNS such as 8.8.8.8. If not, then the IP of the Access Controller will be used. You also have the option to define a secondary DNS server should your primary be unreachable.
<i>Specify Gateway</i>	When checked this allows you to use the input box below and add a Gateway that will be provided via DHCP to client machines, this for instance could be a Router or Layer 3 switch on your internal network should you have a structured network with various VLAN's. If this option is left unchecked then the Access Controller will be specified as the network gateway for all clients.
<i>Configuration Login Revert Timeout</i>	Time limit (in seconds) within which a user must re-login to the Access Controller after changes have been committed before they are automatically undone. This is to prevent loss of connectivity due to errors in entering the IP configuration. The default setting is 90 seconds. This can be disabled by selecting 'Disabled' from the drop down.
<i>Reserved IP Settings</i>	Allows IP addresses to be reserved or locked to specific MAC addresses. See section 5 for details.
<i>Edit Configuration</i>	Edit the LAN Configuration settings
<i>Cancel Changes</i>	Cancel any unapplied changes to the IP configuration.
<i>Apply Configuration</i>	Commit changes to the Access Controller. It will be necessary to login again within the number of seconds defined in the <i>Configuration Login Revert Timeout</i> or the applied changes will be lost.
Download Center	
<i>Reset Counters</i>	Reset to zero the volume and time counters for all services. Note: This cannot be undone although the Call Logs will be unaffected.
<i>Call Detail / Control</i>	Enables the user to download a Call Log that can be exported into Excel or similar spreadsheet application via CSV file, for call analysis. Also enables users to set spending limits for each service. See section 6.3.2 for details.
<i>Download Log</i>	Enables the user to download a Technical Log for diagnostic testing & troubleshooting. (see Appendix 8.1 – Troubleshooting). The log will open in the users default web browser.
<i>Download Config</i>	Enables the user to download a Configuration file (.cfg) to enable the user to backup and transfer all configurable settings onto the FB-10.

6.3. Call Detail / Control

Livewire Connections - Access Controller Call Logs

All Records Start Date: 28 April 2010 - 15:38
 All Records Starting End Date: 28 April 2010 - 15:38
 All Records Between

	Date / Time	Action	Group	service	Data Vol (KBytes)	Duration (Sec)	Cost
▶	28 Apr 2010 11:18:09	VSAT call placed	All	VSAT	0	32	0.00
	28 Apr 2010 11:18:50	Thrane FB 250 call placed	All	Thrane FB 250	0	303	0.01
	28 Apr 2010 11:24:01	Thrane FB 250 call placed	All	Thrane FB 250	21	38	0.25
	28 Apr 2010 11:24:58	VSAT call placed	All	VSAT	300	471	0.00
	28 Apr 2010 11:33:03	3G call placed	Crew Restricted	3G	4736	549	18.50
	28 Apr 2010 11:42:49	VSAT call placed	Crew Restricted	VSAT	288769	1766	0.00
	28 Apr 2010 12:12:29	3G call placed	All	3G	47643	146	186.11
	28 Apr 2010 12:15:10	Shore WiFi call placed	All	Shore WiFi	266929	465	0.00
	28 Apr 2010 12:23:06	Thrane FB 250 call placed	All	Thrane FB 250	163410	328	1906.98
	28 Apr 2010 12:28:48	Shore ADSL call placed	All	Shore ADSL	13829	79	0.00
	28 Apr 2010 12:30:18	VSAT call placed	All	VSAT	0	2	0.00
	28 Apr 2010 12:30:31	VSAT call placed	All	VSAT	2235605	11262	0.00
	28 Apr 2010 15:38:27	3G call placed	All	3G	23620	73	92.27
	28 Apr 2010 15:39:51	Thrane FB 250 call placed	All	Thrane FB 250	5461	134	63.73

Call Logs	
<i>All Records</i>	Select all call records. Please note the call records older then 6 months will automatically be deleted.
<i>All Records Starting</i>	Select all call records from the <i>Start Date</i> .
<i>All Records Between</i>	Select all call records between the <i>Start Date</i> and the <i>End Date</i> .
<i>Start Date</i>	Select the start date. Please note the call records older then 6 months will automatically be deleted. It is possible to enter the Start Time as well as the start date by manually typing in the field in 24 hour format.
<i>End Date</i>	Select the end date.
<i>All Details</i>	Filter between successful calls and failed calls. A failed call is when a call failed to connect during the dialup procedure.
<i>Get Call Log</i>	Preview the results of your query in the table
<i>Save CSV</i>	Export the results of your query to a .CSV file. This can then be imported into Microsoft Excel or other spreadsheet applications for further analysis.
<i>Date/Time</i>	Logs the date and time that the call was initiated.
<i>Action</i>	Logs the user action to initiate or terminate a call.
<i>Group</i>	Logs the Firewall Group that was applied at the time of the call.
<i>Service</i>	Logs the type of service (Internet Connection) that was placed.
<i>Data Vol</i>	Logs the amount of Data that was both transmitted and received in the call.
<i>Duration</i>	Logs the amount of time that the call was active. (in Seconds)
<i>Cost</i>	Estimates the cost of the call based on the User Configured Service Costs (see below)

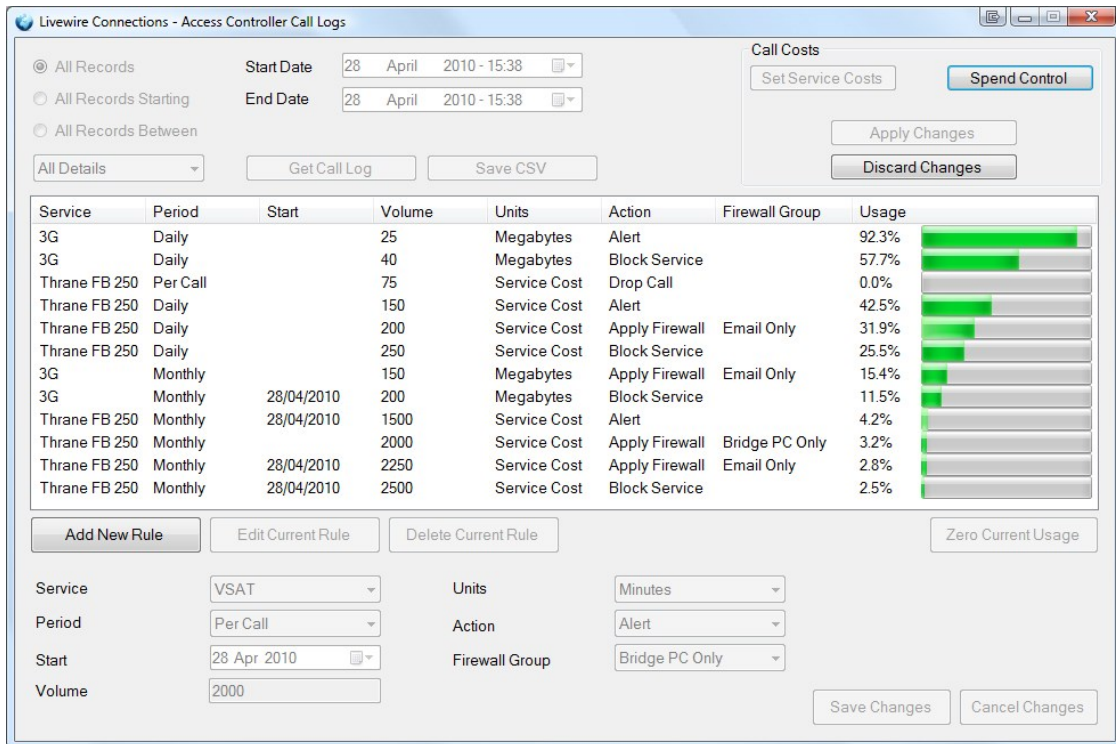
Call Costs	
<i>Set Service Costs</i>	Allows users to enter unit call costs based on either time or volume for each service. See section 6.3.1
<i>Spend Controls</i>	Allows users to configure spending limits and alert monitors. See section 6.3.2
<i>Zero Current Usage</i>	Resets selected Spend Control - See section 6.3.2
<i>Delete Control</i>	Deletes selected Spend Control - See section 6.3.2
<i>Apply Changes</i>	Apply Changes to Spend Controls and Service Costs - See section 6.3.2 and See section 6.3.1
<i>Cancel Changes</i>	Cancels Changes to Spend Controls and Service Costs - See section 6.3.2 and See section 6.3.1

6.3.1.Call Detail / Control - Set Service Costs

No.	Service	Charge on Time	Charge on Data	Cost	Units
1	VSAT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.00	Minutes
2	3G	<input type="checkbox"/>	<input checked="" type="checkbox"/>	4.00	Megabytes
3	Shore WiFi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.00	Minutes
4	Thrane FB 250	<input type="checkbox"/>	<input checked="" type="checkbox"/>	11.95	Megabytes
5	Shore ADSL	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0.00	Minutes

Set Service Costs	
<i>Set Service Costs</i>	Select to enter the Service Cost configuration.
<i>Apply Changes</i>	Apply changes made to the Service Costs entry form.
<i>Discard Changes</i>	Cancel changes made to the Service Costs entry form.
<i>No.</i>	This is a sequential number assigned to each service.
<i>Service</i>	This will list the services that are currently configured on the FB-10
<i>Charge on Time</i>	Check if the service selected is charged by time.
<i>Charge on Data</i>	Check if the service selected is charged by data used.
<i>Cost</i>	This is the cost of the service applied either per Minute, per Megabyte or per Megabit. If the service has a fixed monthly cost, enter the cost as zero. The monetary units of 'Cost' are notional and therefore could be \$, £, € etc. However it is necessary to convert each of the different Service Costs into the same currency so that the Spend Controls can calculate based on a monetary value. See section 6.3.2
<i>Units</i>	Use the drop down menu to define the units or either time or volume to estimate the call cost. Volume can be measured in Megabytes or Megabits. Time is only measured in Minutes.

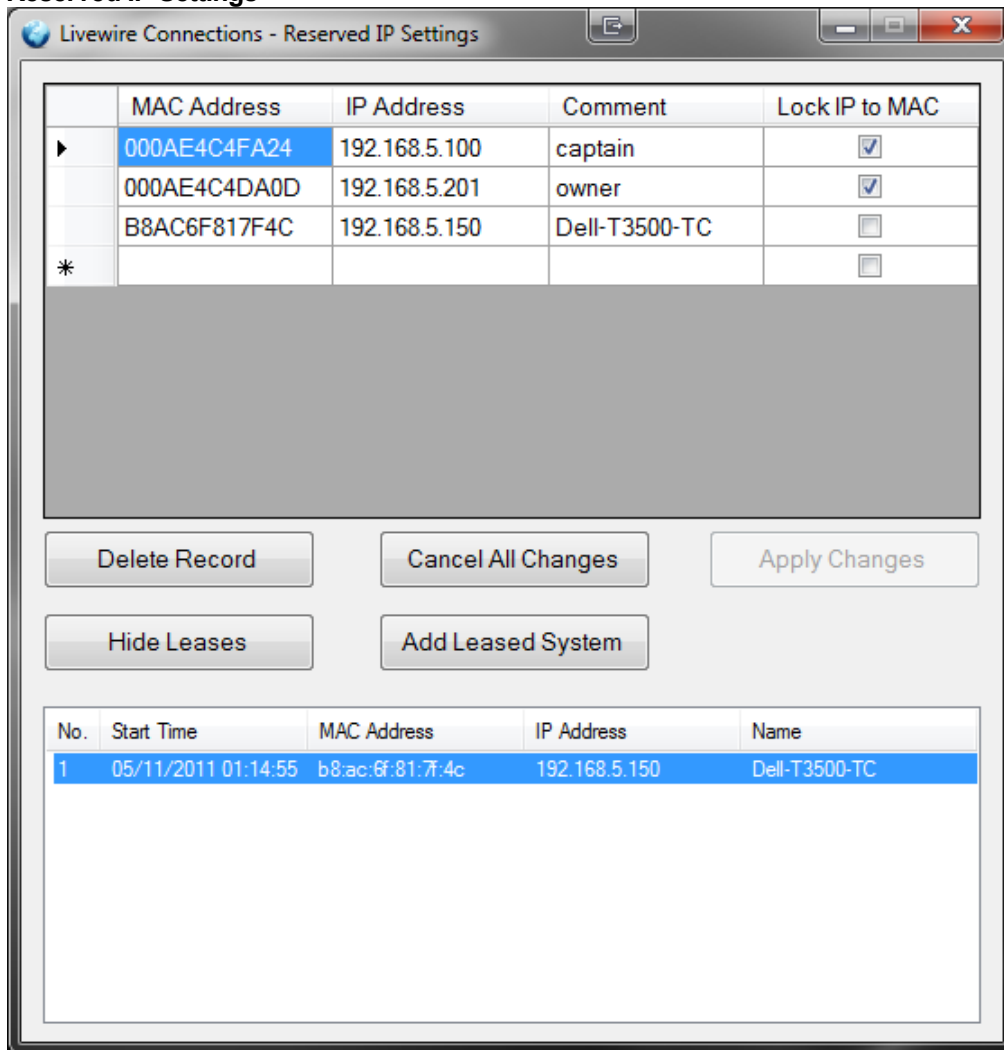
6.3.2. Call Detail / Control – Spend Controls



Spend Controls	
<i>Spend Controls</i>	Select to enter the Spend Control configuration.
<i>Zero Current Usage</i>	This resets the highlighted Spend Control usage to Zero. Example: A rule is configured that allows a Service to use 50Mb per month starting from 1 st Feb 2013 before the Service is Blocked. If on the 18 th Feb 2013 the rule is triggered, the operator can login to the Admin GUI and select ' <i>Zero Current Usage</i> '. This will reset the usage to zero allowing a further 50Mb to be used before 28 th Feb 2013. On the 1 st March 2013 the Usage counter will reset to zero to allow a further 50Mb in the next month. An alternative option for the operator would be to change the <i>Volume</i> for the rule to allow say 60Mb. However, in this case the <i>Volume</i> for all following months would also remain at 60Mb.
<i>Delete Control</i>	This deletes the selected Spend Control rule.
<i>Apply Changes</i>	Apply changes made to the Spend Controls entry form
<i>Cancel Changes</i>	Cancelled changes made to the Spend Controls entry form
<i>Service</i>	Select the service to which you want the Spend Control rule to apply. In addition you can select ALL SERVICES in which the rule will be applied across all the Internet Connections (usually with units of Service Cost).
<i>Period</i>	Use the drop down menu to select between: Per Call – Rule is applied to a single call. i.e. Time or Data is calculated between when the Service button is selected on the User GUI and when either the Disable button is selected or another (or the same) Service is selected. Daily – Rule is applied to calls placed on a single day from 00:00 to 23:59. The <i>Usage</i> is reset at 00:00 on the following day. (All times UTC) Weekly – Rule is applied to calls placed in a single 7 day week from 00:00 on the day specified in the <i>Start</i> calendar. The <i>Usage</i> is reset at 00:00 on the same day for the following week. (All times UTC) Monthly – Rule is applied to calls placed in a single calendar month from 00:00 on the date specified in the <i>Start</i> calendar. The <i>Usage</i> is reset at 00:00 on the same calendar date for the following month. (All times UTC)

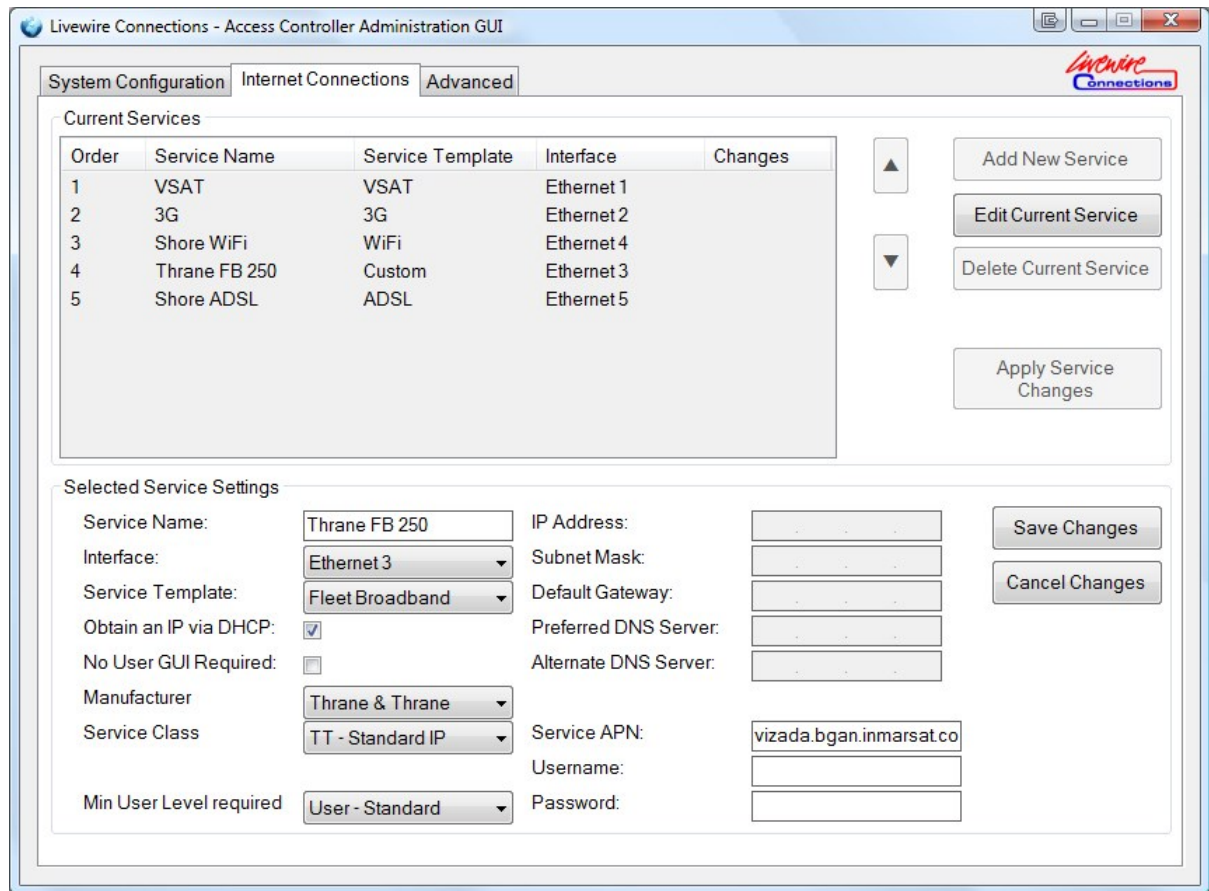
<i>Start</i>	Use the calendar to select the day (for Weekly Periods) or Date (for Monthly Periods) to which the rule applies. It is not necessary to set the <i>Start</i> date for <i>Per Call</i> or <i>Daily</i> rules.
<i>Volume</i>	This is the volume of data or time that must be reached for the Action to be applied. The units depend on the Unit selected in the Units cost column.
<i>Units</i>	Use the drop down menu to select between: Service Cost – Action is triggered when specified Volume of <i>Service Cost</i> is reached in the set <i>Period</i> as defined in ‘Set Service Costs’ – See section 4.1. The monetary units of ‘Cost’ are notional and therefore could be \$, £, € etc. However when using ALL SERVICES as the selected <i>Service</i> it is necessary to convert each of the different Service Costs into the same currency. Minutes – Action is triggered when specified Volume of Time (in Minutes) is reached in the set <i>Period</i> . Megabytes – Action is triggered when specified Volume of Data (in Megabytes) is reached in the set <i>Period</i> .
<i>Action</i>	Use the drop down menu to select between: Alert – When specified <i>Volume</i> is reached within the specified <i>Period</i> for the specified <i>Service</i> a Pop-Up message box is displayed on all open User GUIs. If no User GUIs are open (See Section 6.5 – No GUI Required) Alert is displayed when the next User GUI is opened. Data will continue to be allowed if no User GUI is open. If more than 1 User GUI is open then the Pop-Up message can be accepted by any user and will then disappear on all User GUIs. Drop Call – When specified <i>Volume</i> is reached within the specified <i>Period</i> the specified <i>Service</i> will be set to <i>Disabled</i> . This will occur even if no User GUIs are open. This Action is normally used in ‘ <i>Per Call</i> ’ <i>Periods</i> . Apply Firewall – When specified <i>Volume</i> is reached within the specified <i>Period</i> the <i>Firewall Group</i> chosen will be applied for the specified <i>Service</i> . This will occur even if no User GUIs are open. Block Service – When specified <i>Volume</i> is reached within the specified <i>Period</i> the specified <i>Service</i> will be set to <i>Disabled</i> . If there is an attempt to reconnect the <i>Service</i> a Pop-Up message box is displayed on all open User GUIs stating the <i>Service</i> (or ALL SERVICES) are barred. The Services will be barred even if no User GUIs are open, although the Pop-Up message will only be displayed when a User GUI is opened and a <i>Service</i> selected.
<i>Firewall Group</i>	Use the drop down menu to choose the <i>Firewall Group</i> to be applied when ‘ <i>Apply Firewall</i> ’ <i>Action</i> is triggered. For information on creating <i>Firewall Groups</i> and <i>Firewall rules</i> see Sections 6.7 and 6.8 .
<i>Usage</i>	This is a numerical and graphical display of current usage as a percentage of the allowed usage. When <i>Usage</i> reaches 100% the specified <i>Action</i> is triggered.

6.4. Reserved IP Settings





Reserved IP Settings	
<i>MAC Address</i>	This is the MAC address of the device for which you wish to reserve a IP address (Always give the same address). The formatting should be in the following syntax, example: AA12CC34EE56F (Without Colons)
<i>IP Address</i>	This is the IP address that you want to reserve for that MAC address. This should be a unique address not in used by any other device.
<i>Comments</i>	Optional comments to identify the device. Example: Fred's iPhone
<i>Lock IP to MAC</i>	The MAC Address is a physical address on a device that never changes. If checked the Lock feature prevents a user changing their IP address on their own PCs to circumnavigate Firewall settings. If the user does change their IP they will lose all connectivity to the internet.
<i>Delete Record</i>	Deletes the highlighted item.
<i>Cancel All Changes</i>	Undo any changes which have not been applied yet.
<i>Apply Changes</i>	Applies all the unsaved changes which have been made.
<i>Show/Hide Leases</i>	Display and hide the DHCP lease pane
<i>Add Leased System</i>	Selecting a row in the DHCP lease pane and selecting ' Add Leased System ' adds the machine to the reserved IP settings. Here you can add a custom name if you desire such as 'Captain' which would make more sense when monitoring your bandwidth.

6.5. Internet Connections



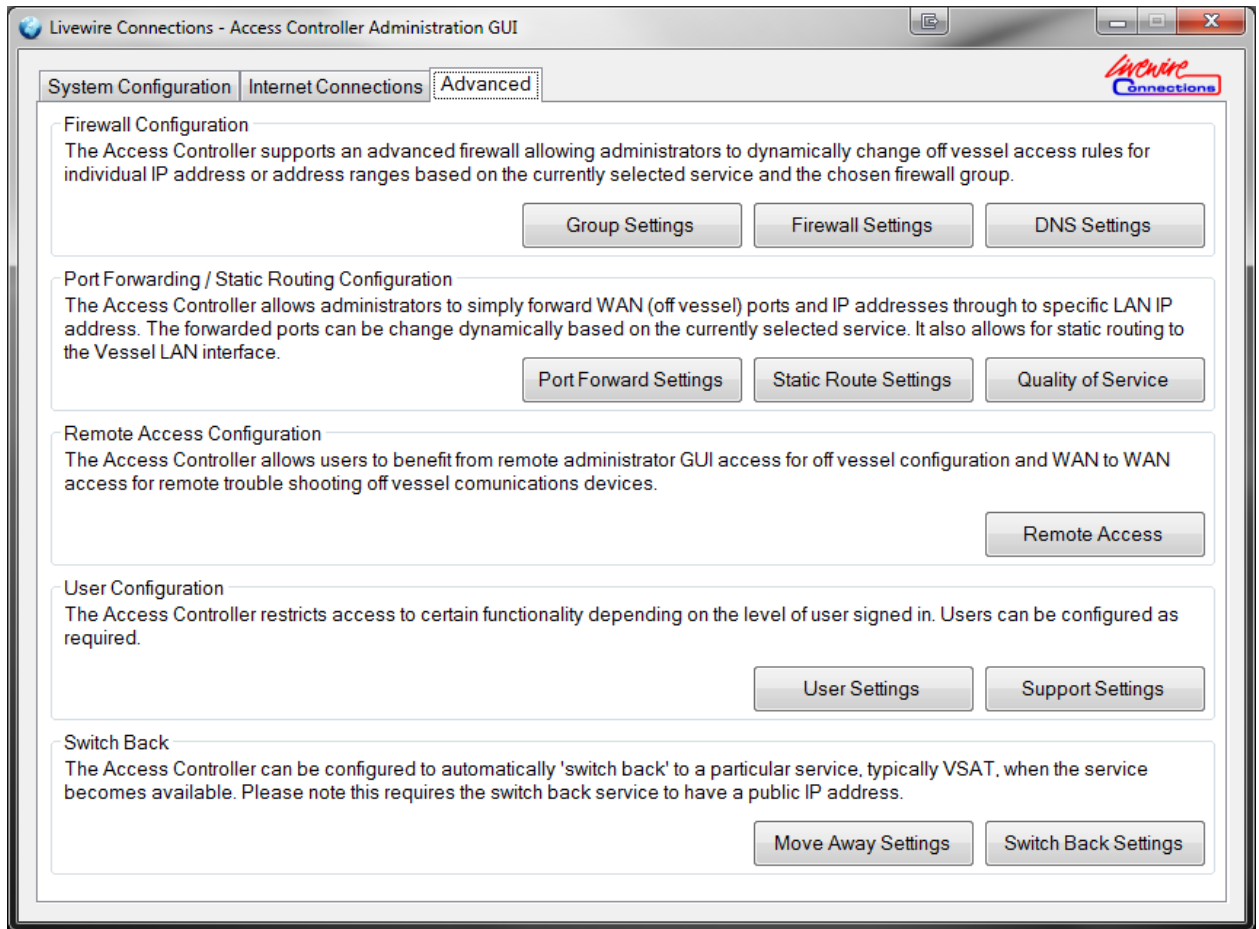
To add a new service (Internet Connection) select 'Add New Service' and enter the configuration as below:

The configuration options below will only be visible for the appropriate *Interface* and *Service Template* selection. To view all configurable options for each *Interface* choose *Custom* from the *Service Template*.

All Services	
<i>Add New Service</i>	Add a new service to be configured.
<i>Edit Current Service</i>	Edit an existing service to be reconfigured.
<i>Delete Current Service</i>	Deletes the selected existing service.
<i>Undelete Current Service</i>	Undelete the selected recently deleted service.
<i>Apply Service Changes</i>	Applies new or edited service configuration. Any current active connections will be disconnected.
<i>Save Changes</i>	Saves new or edited service configuration (Ready to be Applied).
<i>Cancel Changes</i>	Cancel a new or edited service configuration.
 <i>Up Arrow</i>	Re-order list of services in User GUI.
 <i>Down Arrow</i>	Re-order list of services in User GUI.
<i>Service Name</i>	This is the name to be displayed on the User GUI to represent the Service/Internet Connection (e.g. VSAT).
<i>Interface</i>	Select the Interface to which the service is connected corresponding to the Interface diagram in Appendix 8.4.
<i>Service Configuration</i>	Select hardware/connection type based on Service Template selected.

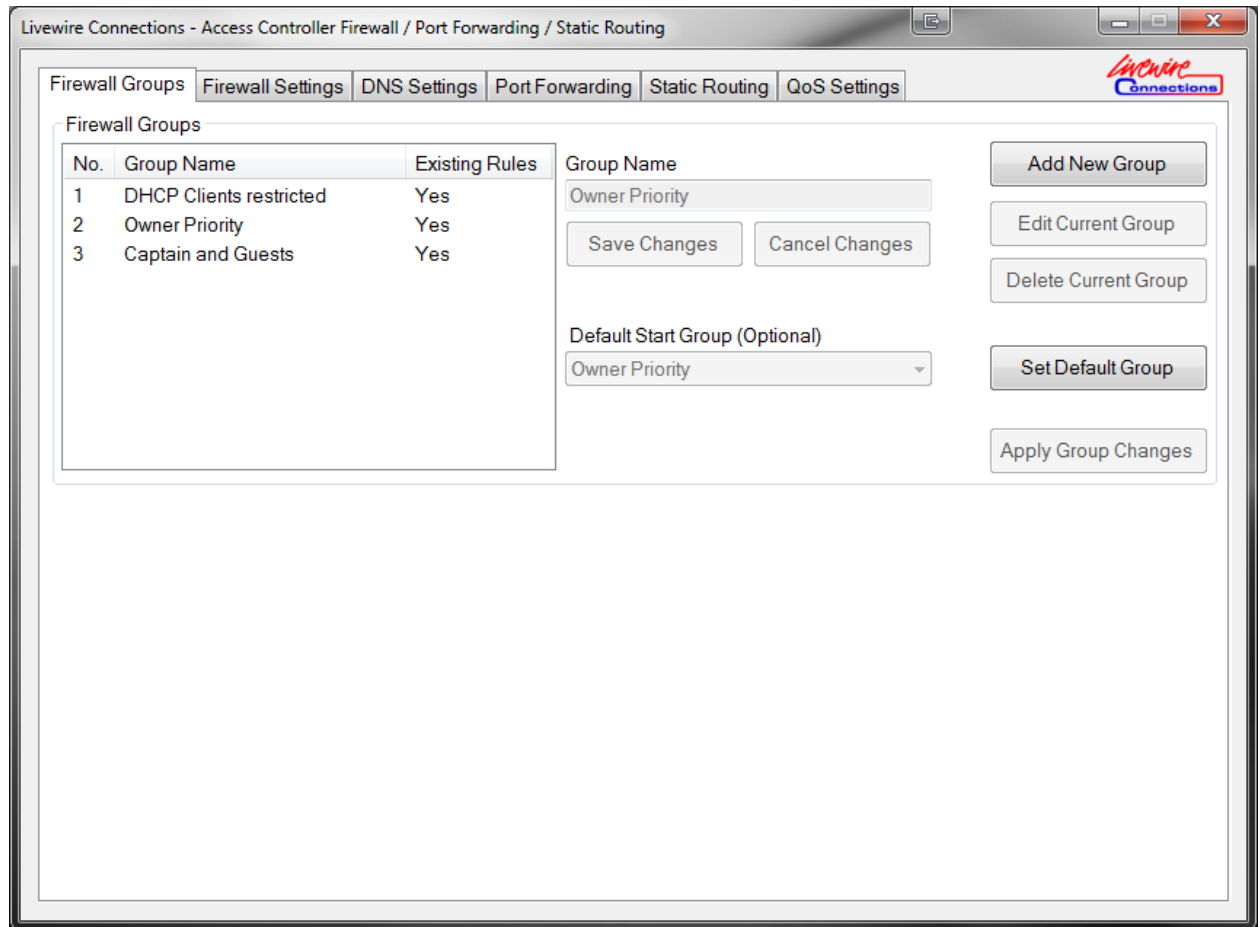
<i>No Traffic Timeout</i>	This is the period of inactivity (no data transfer), in seconds, after which the call will be dropped. Please note: having dropped a call the system will then place a further call if data transfer starts again.
<i>No GUI Required</i>	If the no GUI required box is checked the service will remain connected even if all user GUIs are closed. This should only be used with fixed cost services such as VSAT to avoid unexpected bills.
<i>Min User Level required</i>	Minimum User Level required to be able to select this service. If the logged in user has not got the required user level, then the service will not be available for selection. (Text will be shown in red).
Ethernet Services	
<i>IP Address</i>	This is the IP address that will be assigned to the selected port when the service is selected. Please note that this needs to be in the same IP range as the device to which you are trying to connect.
<i>Subnet Mask</i>	This is the Subnet Mask that will be assigned to the selected port when the service is selected. Typically this should be 255.255.255.0
<i>Default Gateway</i>	This is the Default Gateway that will be assigned to the selected port when the service is selected. Typically this should be the same IP address as your connection device. (e.g. VSAT Modem IP).
<i>Preferred DNS server</i>	Enter your Preferred DNS server. Typically this may be the same IP address as your connection device.
<i>Alternate DNS server</i>	Enter your Alternate DNS server. Typically this may be the same IP address as your connection device. (Optional)
<i>Obtain an IP via DHCP</i>	If you are connecting to another Ethernet device that will provide you with the appropriate IP address then you should check this option.
Dialup Services	
<i>Username</i>	This is the username required to authenticate a dialup connection.
<i>Password</i>	This is the password required to authenticate a dialup connection.
<i>Service APN</i>	The APN supplied to you by the ISP for the network to which you are connecting. (Typically for GPRS/3G and Fleet Broadband Networks).
<i>Number Dialed</i>	The number use in dialup connections to connect to the ISP. For some connections it may be required to add a hash symbol (#) after the number (eg Inmarsat MPDS). – <i>Only available on Custom serial connections.</i>
<i>Initialisation String 1</i>	This is used for entering a bespoke AT command used to initialise your connection, if required by your ISP. – <i>Only available on Custom serial connections.</i>
<i>Initialisation String 2</i>	This is used for entering a second bespoke AT command used to initialise your connection, if required by your ISP. – <i>Only available on Custom serial connections.</i>
<i>Port Speed</i>	This sets the serial port speed required to connect to your serial device. Typically this should be left at 115200. – <i>Only available on Custom serial connections.</i>

6.6. Advanced



The *Advanced Tab* allows access to some of the FB-10 features for advanced users. Factory defaults permit standard operation of the FB-10 without making any changes under the *Advanced Tab*.

6.7. Group Settings (Firewall Groups)

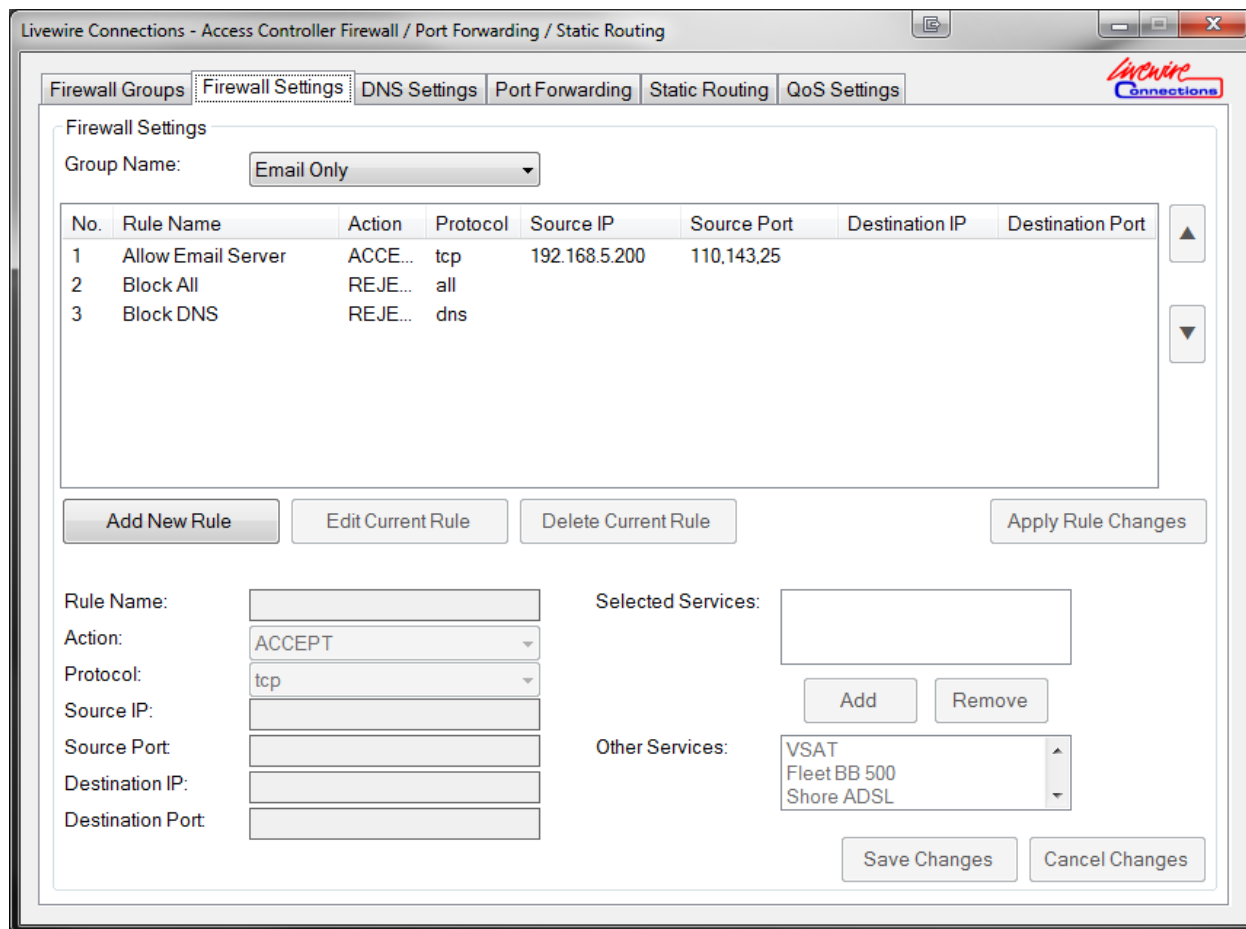


Firewall Groups	
<i>Add New Group</i>	Add a new Group to which Firewall Rules can be applied.
<i>Edit Current Group</i>	Edit an existing Group to which Firewall Rules are applied. Note all rules applied to this group under <i>Firewall Settings</i> will be retained.
<i>Delete Current Group</i>	Delete an existing Group to which Firewall Rules are applied. Note all rules applied to this group under <i>Firewall Settings</i> will be removed.
<i>Apply Group Changes</i>	Commit any changes to the Access Controller.
<i>Set Default Group</i>	Change the default firewall group (Activates 'Default Start Group' drop down menu).
<i>Default Start Group</i>	Drop down list of firewall groups. The select group will be used after a restart or loss of power.
<i>Save Default Group</i>	Exits out of the Default Group option
<i>Group Name</i>	Enter name of the Firewall Group (eg 'Crew Access', 'Email Only' etc). This is the name that will appear in the dropdown on the User GUI.
<i>Cancel Changes</i>	Cancel the current changes to the Group Name.
<i>Save Changes</i>	Saves the current changes to the Group Name.
<i>Existing Rules</i>	Yes/No – Shows if the group has any Firewall Rules are applied under <i>Firewall Settings</i> . Note: If you delete a group all existing rules applied to that group under <i>Firewall Settings</i> , <i>DNS settings</i> & <i>QoS</i> will be removed.

Example use of internet access control using Firewall Groups

Group Name	Users based on IP Address	VSAT	Shore WiFi	Fleet Broadband	3G Roaming
Full Access	Owner Laptop	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
	Captain Desktop	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
	Crew WiFi	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
Email Only	Owner Laptop	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
	Captain Desktop	EMAIL ONLY	EMAIL ONLY	EMAIL ONLY	EMAIL ONLY
	Crew WiFi	EMAIL ONLY	EMAIL ONLY	EMAIL ONLY	EMAIL ONLY
Restricted Crew	Owner Laptop	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
	Captain Desktop	FULL ACCESS	FULL ACCESS	EMAIL ONLY	NONE
	Crew WiFi	FULL ACCESS	FULL ACCESS	NONE	NONE
Owner Onboard	Owner Laptop	FULL ACCESS	FULL ACCESS	FULL ACCESS	FULL ACCESS
	Captain Desktop	FULL ACCESS	FULL ACCESS	EMAIL ONLY	EMAIL ONLY
	Crew WiFi	NONE	NONE	NONE	NONE

6.8. Firewall Settings (Traffic filtering)



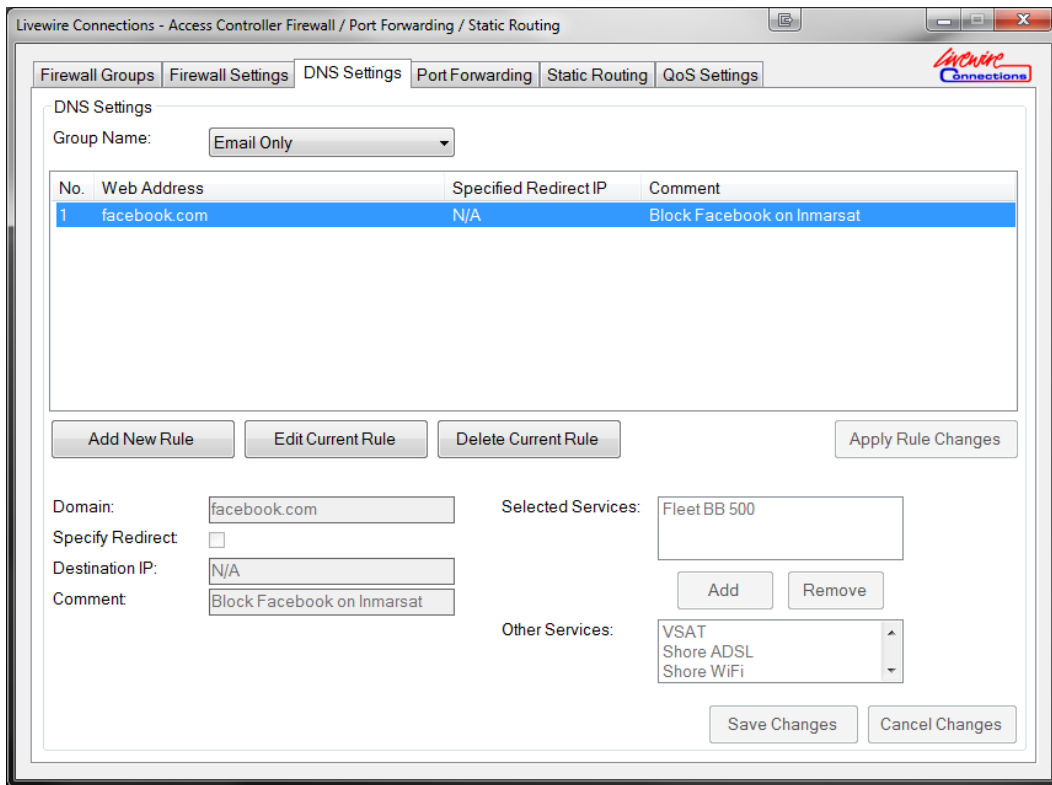
Firewall Settings	
<i>Group Name</i>	Select Group Name you wish to View/Configure as defined in <i>Firewall Groups</i> .
<i>Add New Rule</i>	Add a new rule to be configured.
<i>Edit Current Rule</i>	Edit configuration of an existing rule.
<i>Delete Current Rule</i>	Delete the configuration of an existing rule.
<i>Apply Rule Changes</i>	Applies saved rule changes to the FB-10.
<i>No.</i>	This is the number that is automatically assigned to the rule. The Firewall Rules are applied in this order (i.e. Top to Bottom).
<i>Up Arrow</i>	Select a rule then change the order in which the rules are applied (Applies rules from Top to bottom).
<i>Down Arrow</i>	Select a rule then change the order in which the rules are applied (Applies rules from Top to Bottom)
Entering a Rule	
<i>Rule Name</i>	This is the name given to the current rule (E.g. Email Server Only).
<i>Action</i>	Select required Action for rule. ACCEPT (Accept the packet), DROP (Silently drop the packet without sending an ICMP reject message), REJECT (Reject the packet and send an ICMP reject message).
<i>Protocol</i>	Select protocol for the rule to be applied (TCP, UDP, ICMP, ALL, DNS) NOTE: The ALL option does not cover DNS queries as they are relayed via the Access Controller and therefore require a separate rule to allow/block. NOTE: The DNS protocol only blocks DNS requests for clients using

	the Access Controller as their only DNS server. Public DNS servers won't be blocked, use a normal TCP/UDP port 53 block for this.
<i>Source IP</i>	IP address of the packet data source. Leaving blank will assume all source IP addresses. IP addresses can be entered as singles (192.168.5.50) or using ranges (192.168.5.55-192.168.5.60). Multiple ranges and/or IPs can be entered using commas (192.168.5.50,192.168.5.55-192.168.5.60). The IP used here can be an internal LAN IP or external internet IP.
<i>Source Port</i>	Port of the packet data source. Leaving blank will assume all ports. Ports can be added in the format 110 or 110,143
<i>Destination IP</i>	IP address of the packet data destination. Leaving blank will assume all destination IP addresses. IP addresses can be entered as singles (192.168.5.50) or using ranges (192.168.5.55-192.168.5.60). Multiple ranges and/or IPs can be entered using commas (192.168.5.50,192.168.5.55-192.168.5.60). The IP used here can be an internal LAN IP or external internet IP.
<i>Destination Port</i>	Port of the packet data destination. Leaving blank will assume all ports. Ports can be entered as singles (110) or using ranges (1024-2024). Multiple ranges and/or ports can be entered using commas (110,1024-2024).
<i>Selected Services</i>	Services (Internet Connections) for which the rule will be applied.
<i>Other Services</i>	Services (Internet Connections) configured on the FB-10 for which the rule will not be applied.
<i>Add</i>	Add Service for which the rule will be applied.
<i>Remove</i>	Remove Service for which the rule will be applied.
<i>Save Changes</i>	Save changes for the current rule.
<i>Cancel Changes</i>	Cancel changes for the current rule.



Important Note: The default action is to allow all traffic. Most common setup scenarios usually therefore have a 'Block All' REJECT/DROP rule at the bottom. If there is not a single REJECT/DROP rule in the list then this is very likely to be incorrectly setup. Livewire Connections recommends that the firewall is setup by an experienced network administrator as incorrect usage/setup will allow unwanted data to leave the vessel.

6.8.1. DNS Settings



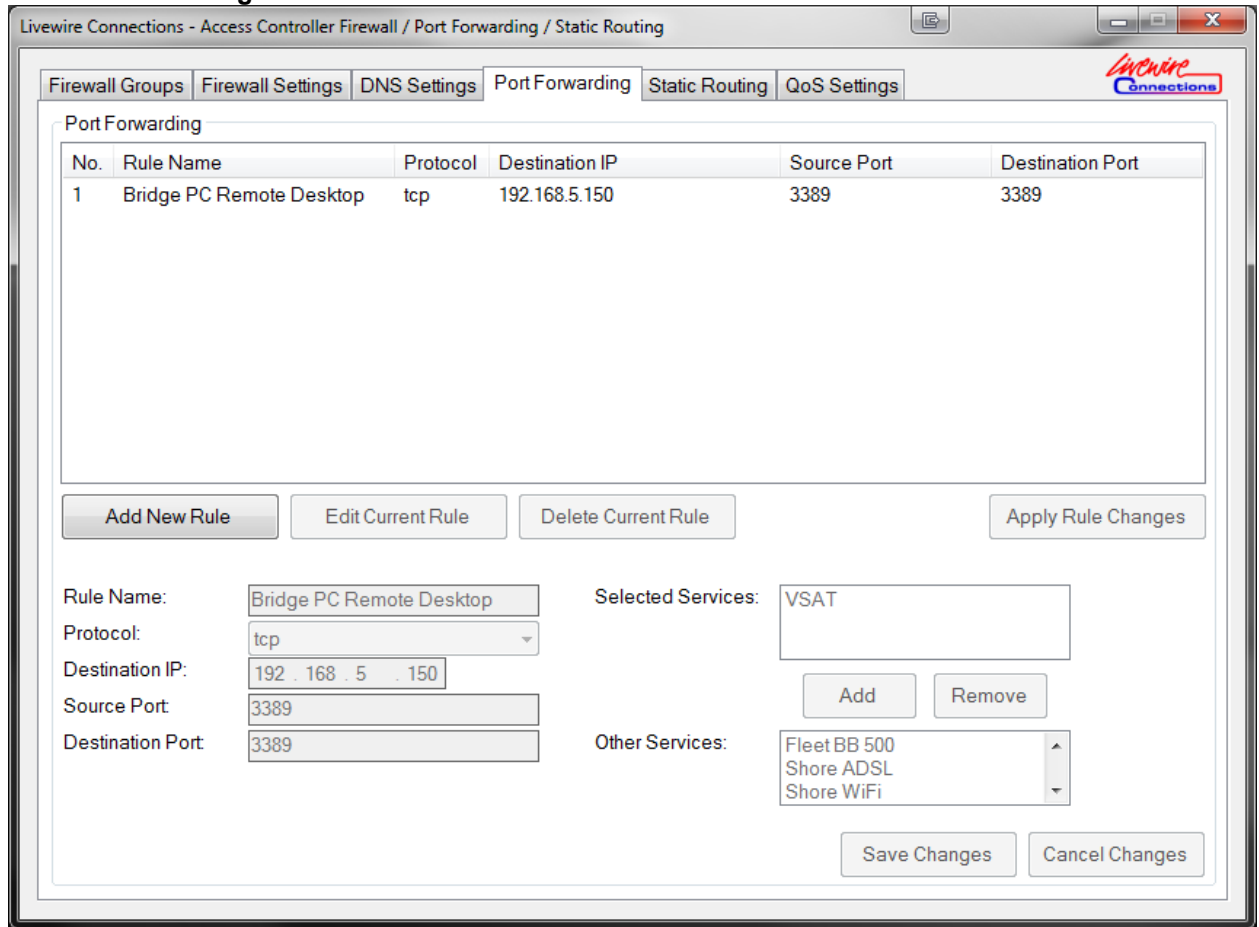
DNS Settings	
<i>Group Name</i>	Select Firewall Group to which the DNS rules will apply.
<i>Add New Rule</i>	Add a new rule to be configured.
<i>Edit Current Rule</i>	Edit configuration of an existing rule.
<i>Delete Current Rule</i>	Delete the configuration of an existing rule.
<i>Apply Rule Changes</i>	Applies saved rule changes to the FB-10.
<i>Domain</i>	Enter the domain that you want to restrict (E.g. facebook.com it is best to enter all variants such as facebook.co.uk).
<i>Specify Redirect</i>	Select to redirect users to the 'Destination IP' (below) address if the user attempts to access a domain that is blocked. If this is not selected the user is presented with a default 'DNS blocked' message
<i>Destination IP</i>	This is the IP address of a website to which users will be redirected if 'Specify Redirect' is selected.
<i>Comment</i>	This is a description for the rule that is only visible in the Admin GUI
<i>Selected</i>	Services (Internet Connections) for which the rule will be applied.
<i>Other Services</i>	Services (Internet Connections) configured on the FB-10 for which the rule will not be applied.
<i>Add</i>	Add Service for which the rule will be applied.
<i>Remove</i>	Remove Service for which the rule will be applied.
<i>Save Changes</i>	Save changes for the current rule.
<i>Cancel Changes</i>	Cancel changes for the current rule.



Important Note: DNS settings limitation

DNS Blocking will only be applied if the users are using the FB-10 to manage DNS and it is their only DNS server. If users have either external DNS servers specified (can be blocked through the firewall) or pages have been DNS cached while on other external networks (E.g. Internet Café) then it may be still possible to access restricted domains. Web browsers also tend to cache DNS lookups for a longer time. This feature is mainly designed to be used to block other applications like Anti-Virus/Windows Updates or to block certain websites all the time.

6.9. Port Forwarding



Port Forwarding	
<i>Add New Rule</i>	Add a new rule to be configured.
<i>Edit Current Rule</i>	Edit configuration of an existing rule.
<i>Delete Current Rule</i>	Delete the configuration of an existing rule.
<i>Apply Rule Changes</i>	Applies saved rule changes to the FB-10.
Entering a Rule	
<i>Rule Name</i>	This is the name given to the current rule (Eg Video Conferencing).
<i>Protocol</i>	Select protocol for the rule to be applied (TCP, UDP, ICMP, GRE).
<i>Destination IP</i>	IP address of the device on the LAN to which traffic on the specified port will be forwarded.
<i>Source Port</i>	Incoming Port number. Enter the port number which will be used for the external incoming connection. Ports can be entered as singles (110) or using ranges (1024-2024).
<i>Destination Port</i>	Destination Port number. Enter the port number that the device on the LAN is expecting an incoming connection. Ports can be entered as singles (110) or using ranges (1024-2024).
<i>Selected Services</i>	Services (Internet Connections) for which the rule will be applied.
<i>Other Services</i>	Services (Internet Connections) configured on the FB-10 for which the rule will not be applied.
<i>Add</i>	Add Service for which the rule will be applied.
<i>Remove</i>	Remove Service for which the rule will be applied.
<i>Save Changes</i>	Save changes for the current rule.
<i>Cancel Changes</i>	Cancel changes for the current rule.

Note for port forwarding to work correctly you will need a Public IP on your internet connection, this will then be used from the outside of the vessel to contact the Access Controller on board.

6.10. Static Routing

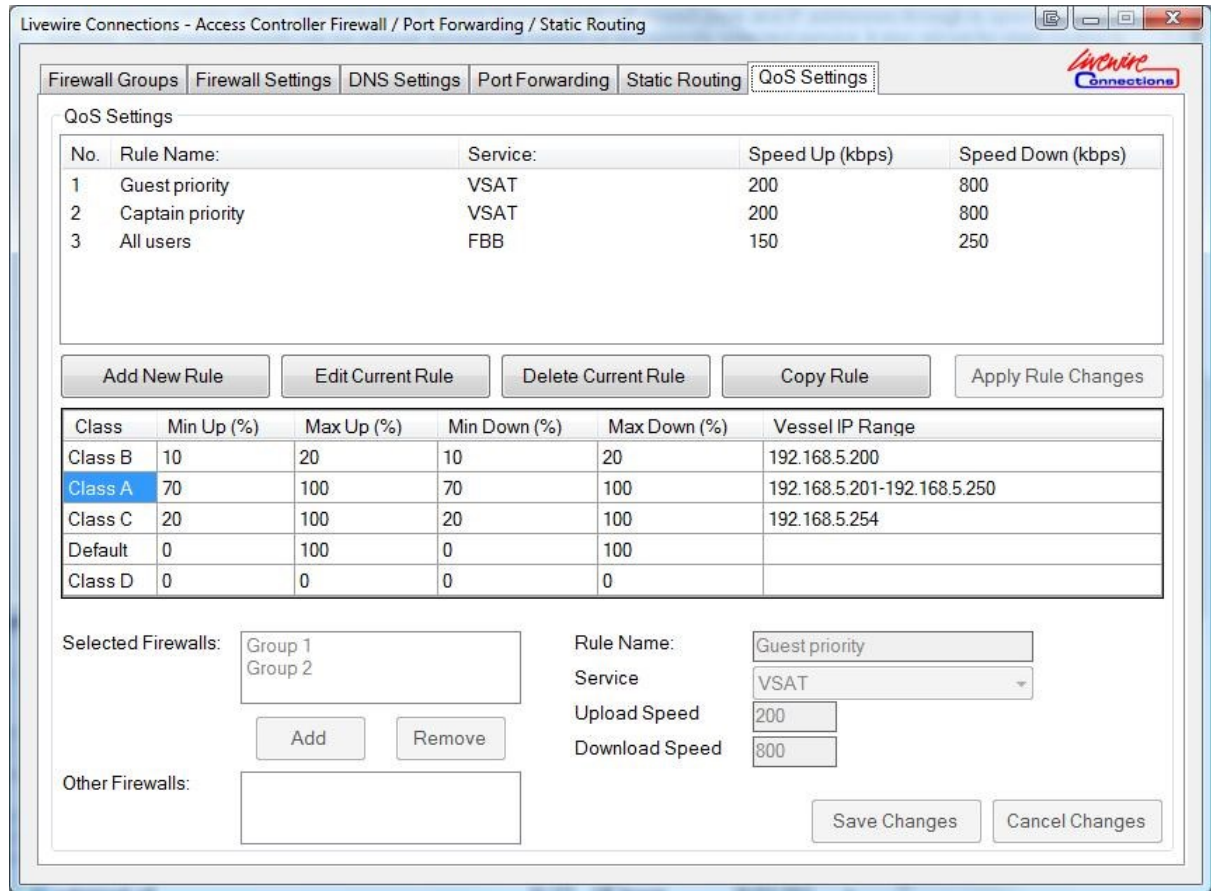
Static Routing

No.	Rule Name	Type	Destination IP	Netmask	Gateway	Gateway IP
1	Entertainment VLAN	NET	192.168.4.0	255.255.255.0	True	192.168.5.254

Rule Name:
 Rule Type:
 Destination IP:
 Netmask:
 Via Gateway:
 Gateway IP:

Static Routing	
<i>Add New Rule</i>	Add a new rule to be configured.
<i>Edit Current Rule</i>	Edit configuration of an existing rule.
<i>Delete Current Rule</i>	Delete the configuration of an existing rule.
<i>Apply Rule Changes</i>	Applies saved rule changes to the FB-10.
Entering a Rule	
<i>Rule Name</i>	This is the name given to the current rule (Eg AV VLAN).
<i>Rule Type</i>	Static Routes allow for NET rules (Routing to a Network Range) or HOST rule (Routing to an individual IP address)
<i>Destination IP</i>	Define the IP address to which the Static Rule will route. If host type is a NET rule, then enter the IP address of the start of the range (192.168.4.0).
<i>Netmask:</i>	Define the Net to which the Static Rule will route. (255.255.255.0 for entire subnet).
<i>Via Gateway:</i>	Check to define if you want the Static Route to route via a Gateway.
<i>Gateway IP:</i>	Define the IP address of the gateway to which the Static Rule will route (Usually an internal LAN router or Layer 3 Switch, this should be on the same subnet as the FB10 LAN).
<i>Save Changes</i>	Save changes for the current rule.
<i>Cancel Changes</i>	Cancel changes for the current rule.

6.10.1.QoS Settings



QoS Settings	
<i>Add New Rule</i>	Add a new rule to be configured.
<i>Edit Current Rule</i>	Edit configuration of an existing rule.
<i>Delete Current Rule</i>	Delete the configuration of an existing rule.
<i>Copy Rule</i>	Copies 'Classes' percentage values and IP range(s) from a previous rule for you to use in a new rule.
<i>Apply Rule Changes</i>	Applies saved rule changes to the FB-10.
Entering a Rule	
<i>Rule Name</i>	This is the name given to the current rule (E.g. Crew Restriction).
<i>Service</i>	The internet connection that you wish the rule to apply to, this is carried over from your internet connections page. (I.e. VSAT, Fleet Broadband).
<i>Upload Speed</i>	Estimated Uplink Speed of your selected service. This should be a realistically achievable speed for the service and not simply the maximum stated value, we recommend you perform several speed tests to verify your true speed achievable.
<i>Download Speed</i>	Estimated Downlink Speed of your selected service. This should be a realistically achievable speed for the service and not simply the maximum stated value, we recommend you perform several speed tests to verify your true speed achievable.
<i>Selected Firewalls</i>	These are the Firewall Groups to which the QoS settings will be applied when enabled and using the specified service. NB. It is not necessary to have any other firewall rules associated with these firewall groups if you only require QoS settings.
<i>Other Firewalls</i>	These are the other Firewalls Groups configured on the FB-10 that do not currently have any QoS settings configured for the selected service.

<i>Class</i>	Top down list, allows you to differentiate bandwidth percentages between IP addresses/Ranges.
<i>Min Up (%)</i>	The minimum upload speed that will be made available for a particular class expressed as a percentage of the overall upload speed. Any cell left blank will be set to a value of 0%. Please note, for correct operation the sum of all Min Up percentages should not add up to more than 100%.
<i>Max Up (%)</i>	The maximum upload speed that will be made available for a particular class expressed as a percentage of the overall upload speed. This can be configured to cap a classes maximum speed or to allow it to utilise unused bandwidth assigned to other classes. To cap a class simply enter a maximum value greater than or equal to your Min Up (%) but less than 100. The higher the maximum value is above the Min Up (%) the more available bandwidth the class will be able to utilise. For full free bandwidth utilisation across all classes the Max Up (%) for all classes should be set to 100.
<i>Min Down (%)</i>	The minimum download speed that will be made available for a particular class expressed as a percentage of the overall download speed. Any cell left blank will be set to a value of 0%. Please note, for correct operation the sum of all Min Down percentages should not add up to more than 100%.
<i>Max Down (%)</i>	The maximum download speed that will be made available for a particular class expressed as a percentage of the overall upload speed. This can be configured to cap a classes maximum speed or to allow it to utilise unused bandwidth assigned to other classes. To cap a class simply enter a maximum value greater than or equal to your Min Down (%) but less than 100. The higher the maximum value is above the Min Down (%) the more available bandwidth the class will be able to utilise. For full free bandwidth utilisation across all classes the Max Down (%) for all classes should be set to 100.
<i>Vessels IP Range</i>	The IP range / individual IPs included within each class. This can be from different subnet ranges and across VLANs. IP addresses can be entered as singles (192.168.5.50) or using ranges (192.168.5.55-192.168.5.60). Multiple ranges and/or IPs can be entered using commas (192.168.5.50,192.168.5.55-192.168.5.60). Please note, any IP not specified here will be handled by the Default Class.
<i>Save Changes</i>	Save changes for the current rule.
<i>Cancel Changes</i>	Cancel changes for the current rule.



Important Note: QoS Limitations.

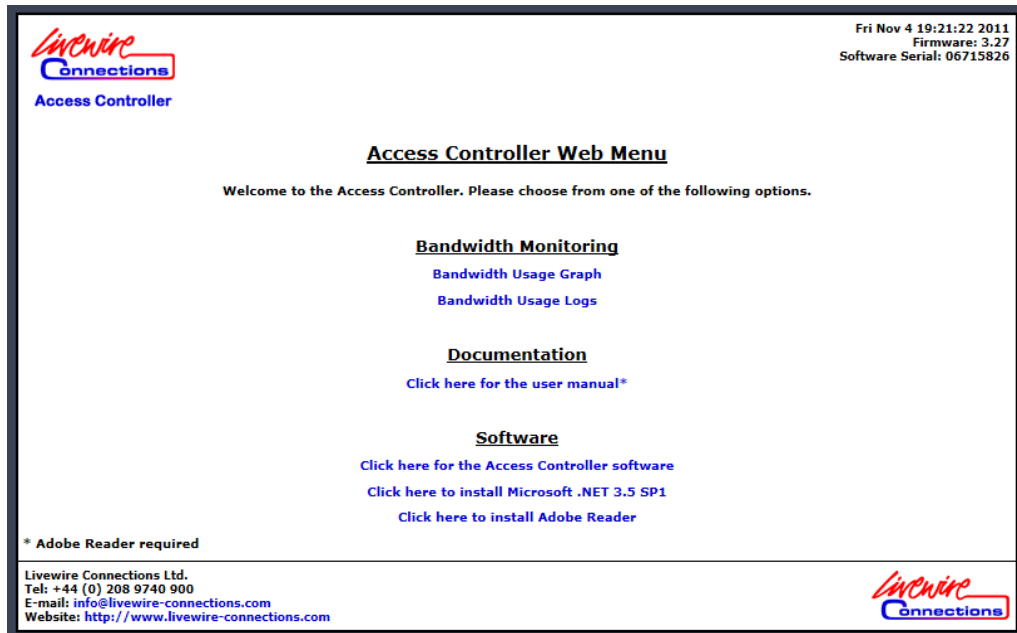
Please note, for the QoS feature to work as specified when using services with highly volatile bandwidths you must configure the upload speed to be a realistically achievable level or cap non-essential classes. In reality if you have a contended 1024kbps maximum downlink speed you are unlikely to always get the full 1024kbps, be this due to network traffic, bad weather or poor installation of RF Equipment. We recommend that you perform speed tests to ascertain your average download and upload speeds.

6.10.2. Bandwidth Monitoring.

Live and historical monitoring of the current bandwidth (speed) and data volume usage can now be accessed from the Access Controller web interface. The web interface can now be easily accessed from within the User GUI by Clicking on the picture of the FB10 Access Controller unit circled below:



After the webpage has opened you will find the links to the Bandwidth logs and graphs in the middle of the web page. To view your entire networks usage of your internet connection; use the '**Bandwidth Usage Graph**' hyperlink. To view usage on an individual level (Per; IP address/User) then use the '**Bandwidth Usage Logs**' hyperlink.



Bandwidth Usage Logs:

On the following page you can organise and select how you want to display the Internet connections usage. You can go to individual PC's and see who or what is taking up your bandwidth.

Access Controller Bandwidth Monitor

Welcome to the Access Controller Bandwidth Monitor Logs.
From here you will be able to see the bandwidth logs of your network by IP address.

Period: Order By:

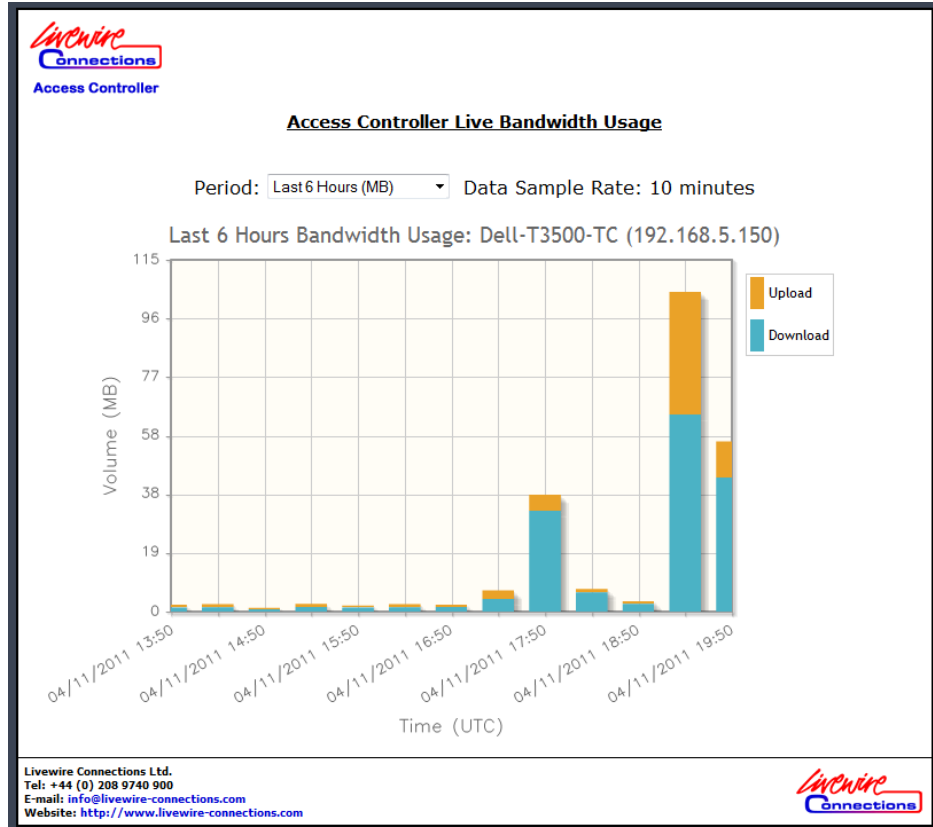
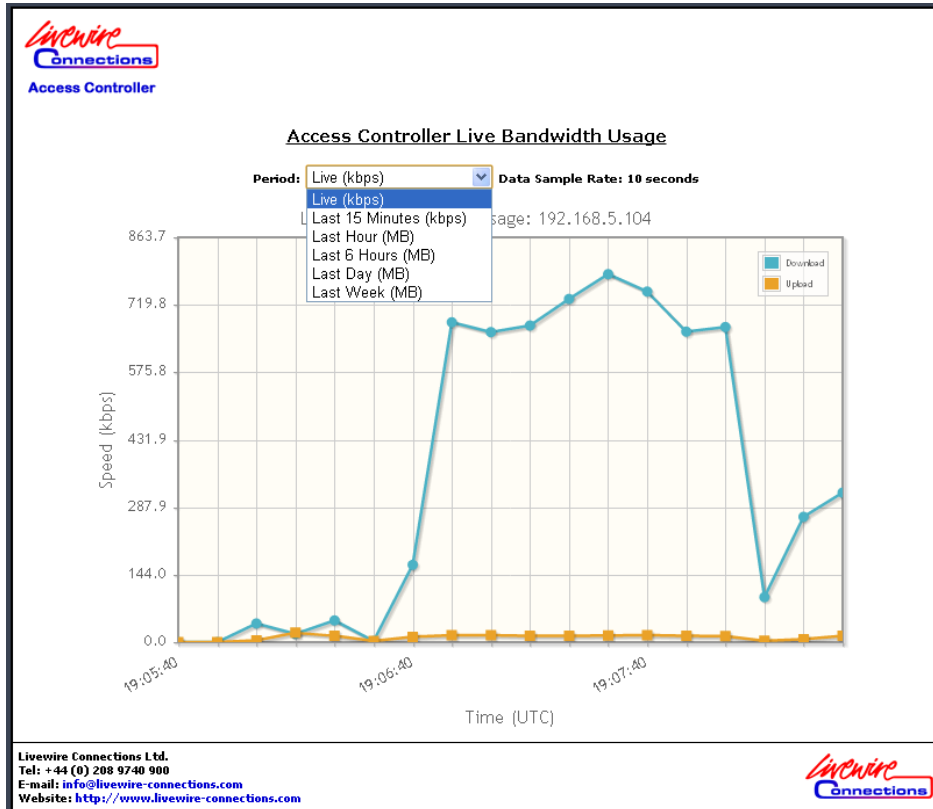
Computer (Click to view)	Total Data - high to low	Total Data - low to high	IP Address	Upload (MB)	Combined (MB)
ALL	Last 6 Hours	26.4906		0.7982	27.2888
192.168.5.91	Last Day	8.6065		0.2800	8.8865
192.168.5.104	Last Week	17.8841		0.5182	18.4024

Livewire Connections Ltd.
Tel: +44 (0) 208 9740 900
E-mail: info@livewire-connections.com
Website: <http://www.livewire-connections.com>

Access Controller Bandwidth Monitor	
<i>Period</i>	Historic time period that you want to see the data usage over.
<i>Order By</i>	Allows you to sort the table view by IP or Data Usage.
<i>Reload Data</i>	Refreshes the webpage to show changes in data usage since webpage was opened.
<i>Computer</i>	Select from ALL to see total activity or click on an individual PC/IP (i.e: 192.168.5.91) to see that devices usage of the internet bandwidth.
<i>Download (MB)</i>	Total data downloaded by device in selected time. Displayed in Megabytes as this is a volume of data rather than speed measurement and will show how much data has been downloaded from the internet.
<i>Upload (MB)</i>	Total data uploaded by device in selected time. Displayed in Megabytes as this is a volume of data rather than speed measurement and will show how much data has been uploaded to the internet.
<i>Combined (MB)</i>	Total data usage by device(s) expressed as a volumetric figure in Megabytes. Combines the downloaded and uploaded data via the Access Controller to/from the internet.

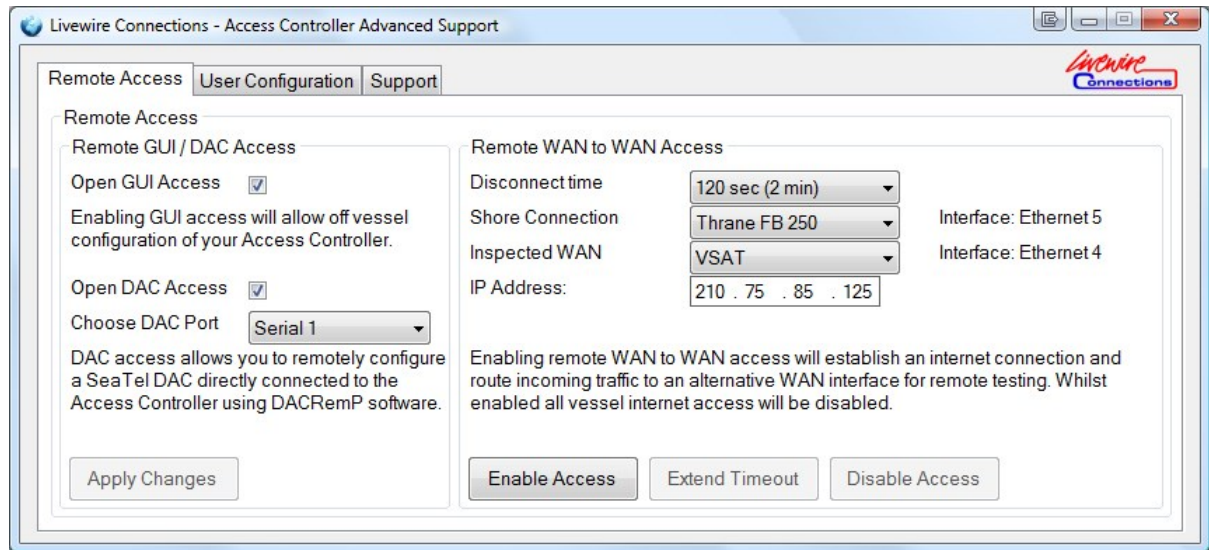
Bandwidth Usage Graph:

This page shows you the 'Live' overall usage of your internet service.



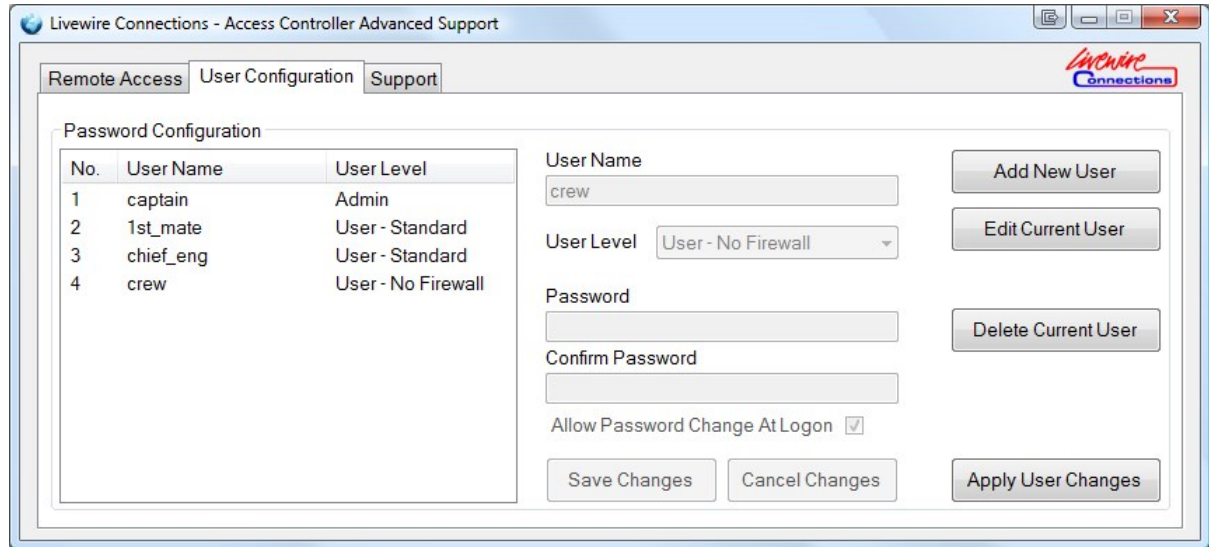
Access Controller Live Bandwidth Usage (Graphs)	
<i>Period</i>	Historic time period that you want to see the data usage over. For Live and Last 15 Minutes the graph shows speed in kilobits per second (kbps) whilst for periods over 15 minutes the chart shows total data volumes in Megabytes (MB) measured during that time period
<i>Data Sample Rate</i>	This is the rate at which data was sampled in order to create the graph / chart. At the highest rate the data is sampled once every 10 seconds and an average speed is calculated based on the volume of data transferred during that time. NB. As speeds are averaged over the 10 seconds they will not capture the maximum data speed at a single point in time but will provide a smoothed representation of speeds attained.
<i>Speed (kbps)</i>	Displays the bandwidth usage for Live or Last 15 minutes in kilobits per second (kbps).
<i>Volume (MB)</i>	Once a historic value over 15 minutes has been selected in the Period drop down box then the vertical axis will show volume in Megabytes (MB) rather than speed.
<i>Time (UTC)</i>	The horizontal axis will change dependant on Period selected to reflect a suitable time interval (This time is synchronised with the Bios clock on the FB10 motherboard and not the local time).

6.11. Remote Access



Remote Access	
<i>Open GUI Access</i>	Tick check box to enable remote GUI access. Enabling GUI Access will allow off vessel configuration of your Access Controller via a public IP.
<i>Open DAC Access</i>	DAC access allows you to remotely configure a Sea Tel DAC Antenna Control Unit directly connected to the FB-10 using DACRemP IP Software (Port 8889) supplied by Sea Tel. This feature can be used remotely if the Open GUI Access is enabled. On higher latency connections the Timeout and Pacing values in DACRemP need to be changed.
<i>Choose DAC Port</i>	Choose the Serial Port that is used to connect the FB-10 to the DAC M&C Port. Please note: Enabling Remote DAC Support on a selected port will delete any service currently assigned to that port. To ensure no further services are configured on that port it will not appear in the port list under services again until this function is disabled. Your Admin GUI will be restarted automatically and any changes that have not been applied will be lost.
<i>Apply Changes</i>	Applies changes to the <i>Open DAC Access</i> and <i>Open GUI Access</i> check box.
Remote WAN to WAN Access	
<i>Disconnect Time</i>	This is the time (in seconds/minutes) after which the remote user will be disconnected from the FB-10 after no further user intervention.
<i>Shore Connection</i>	This is the connection used to establish your shore link.
<i>Inspected WAN Service</i>	This is the device you are looking to query, for diagnostic/configuration remotely.
<i>IP Address</i>	This is the IP address that will be assigned to your shore connection when forwarded to the other WAN port. Please note, this needs to be in the same range as the device you are trying to connect to but must not be the same as your WAN interface.
<i>Enable Access Button</i>	Enables WAN to WAN access. Enabling will establish an internet connection and will route incoming traffic to an alternative WAN interface. (E.g. Your VSAT will route to the Shore WiFi, so a technician can come in on the VSAT and repair or configure the Shore WiFi,).
<i>Extend Timeout</i>	This will reset the disconnect time to the original setting, allowing more time for the remote user to use WAN to WAN inspection.
<i>Disable Access</i>	This terminates the WAN to WAN session.

6.12. User Configuration



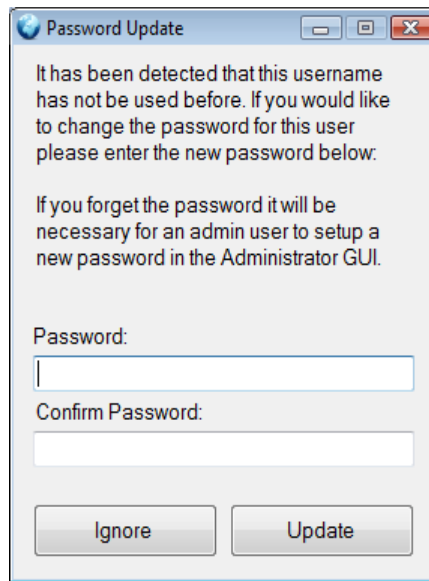
Password Configuration	
<i>Add New User</i>	Add a new user to be configured.
<i>Edit Current User</i>	Edit configuration of an existing user.
<i>Delete Current User</i>	Delete the configuration of an existing user.
<i>Apply User Changes</i>	Commit changes to the Access Controller.
Adding a User	
<i>User Name</i>	This is the user name given to the current user to login (E.g. Captain)
<i>User Level</i>	Apply access level to user account. The following levels are available, ADMIN - Allows access to Admin & User GUI USER - Allows access only to the User GUI USER RESTRICTED - Allows access only to the User GUI. USER FIREWALL GROUP - Allows access only to the User GUI (Firewall cannot be disabled/enabled. However it can be changed) USER NO FIREWALL – Allows access only to the User GUI (Firewall cannot be changed, disabled or enabled) Further restrictions can be applied on individual services. See the “Min User Level required” option in Section 6.5.
<i>Password</i>	This is the password associated with the user name. The password is case sensitive.
<i>Confirm Password</i>	The chosen password has to be entered again to be verified
<i>Allow Password Change At Logon</i>	If selected this allows a new user to change the login password after the new user’s initial login. The password change prompt will only appear when the user logs in for the first time. This is to allow an administrator to setup a user account and then for a user to select their own password.
<i>Save Changes</i>	Save changes made to the selected user.
<i>Cancel Changes</i>	Cancel changes made to the selected user.

6.13. Default Users

The follow user accounts are setup by default on the FB-10:

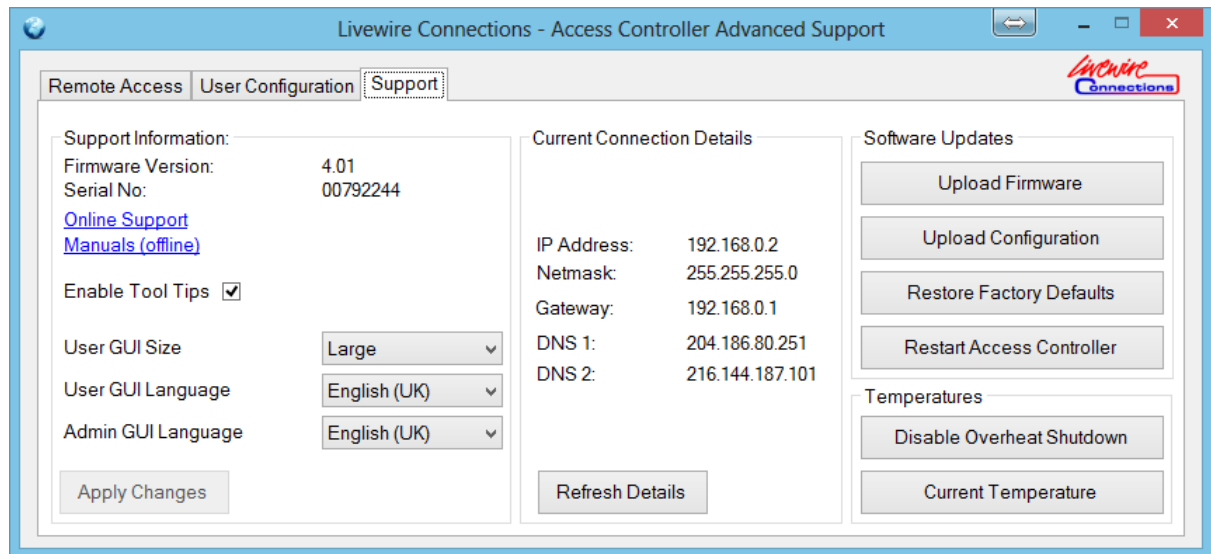
Username: admin
Password: password
User Level: ADMIN

Username: user
Password: password
User Level: USER



When you create a new user and have the '*Allow Password Change at Logon*' ticked, you will see the above password change prompt. This is to allow an administrator to setup a user account and then a user to select their own password.

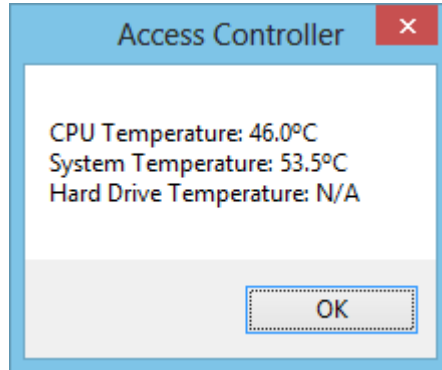
6.14. Support Information



Support Information	
<i>Firmware Version</i>	This is the current firmware version on the unit.
<i>Serial Number</i>	This is the software serial number of the Access Controller.
<i>Online Support</i>	This is a link to the support area of the Livewire Connections website. (Internet access required).
<i>Manuals (Offline)</i>	This is a link to the user manual (stored on the FB10).
<i>Enable Tool Tips</i>	Enables helpful tool tips in the Admin GUI.
<i>User GUI Size</i>	Change the size of the User GUI for different resolution screens.
<i>User GUI Language</i>	Change the language of the User GUI. (More languages to be released soon).
<i>Admin GUI Language</i>	Change the language of the Admin GUI. (More languages to be released soon).
<i>Apply Changes</i>	Applies changes made to the GUI Settings above.
Current Connections Details	
<i>IP Address:</i>	This states the IP address received by the current connection in use. If it says N/A then the values can not be retrieved, most likely cause is that no service is selected in the User GUI.
<i>Netmask:</i>	This states the Netmask being applied to the current connection.
<i>Gateway:</i>	This states the Gateway being used by the current connection.
<i>DNS 1:</i>	This states the Primary DNS being used by the current connection.
<i>DNS 2:</i>	This states the Secondary DNS being used by the current connection.
<i>Refresh Details</i>	Use this button to refresh the current connection details page.
Software Updates	
<i>Upload Firmware</i>	Enables the FB-10's Firmware to be upgraded. Firmware uploads and installation instructions are released at http://www.livewire-connections.com/support
<i>Upload Configuration</i>	This allows users to upload previously downloaded configuration. Please note that you download configuration on the System Configuration page.
<i>Restore Factory Defaults</i>	This restores all configuration changes back to the default factory settings. The default factory IP address is 192.168.5.1
<i>Restart Access Controller</i>	This restarts the Access Controller.
<i>Disable/Enable Overheat Shutdown</i>	This allows you to turn off/on the overheat protection which is built into the Access Controller. It is highly recommended that you keep the Overheat Shutdown enabled. (If overheat shutdown is disabled you may void your product warranty, please contact Livewire for further

	information).
<i>Current Temperature</i>	This will display the current temperature of the Hard Drive, Processor and System board (Note that if you have a Solid State Hard Drive installed then the Hard Drive temperature will not be displayed).

Current Temperature Screen:



6.15. Overheat Protection

A built in feature of the Access Controller is the Overheat Shutdown. This feature detects when the internal temperature of the Access Controller gets excessively high, and then shuts down the system in a controlled manner before any hardware damage occurs. If you are experiencing these *Overheat shutdowns* and the ambient temperature is not in excess of 35 degrees Celsius, then your Access Controller is situated incorrectly where is insufficient airflow?

Livewire Connections strongly recommends you keep the feature enabled. You may invalidate your warranty by disabling this feature; it is there only for diagnostic purposes or in emergencies.

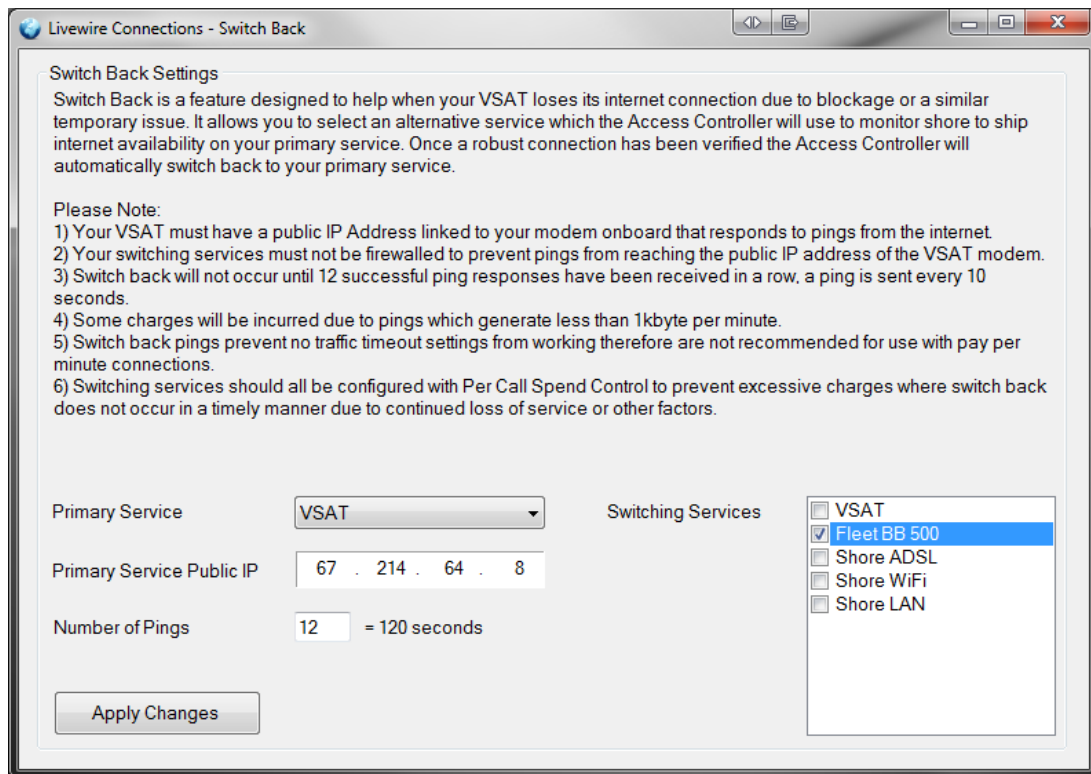
6.16. Hardware Factory Default Reset

It is possible to reset the FB-10 to factory defaults by pressing the Power Button on the front of the FB-10 5 times within 5 seconds. If successful the FB-10 will beep several times before resetting. The factory reset can be cancelled by pressing the button a further 5 times before the beep sequence ends.

6.17. Access Controller Switch Back

You need to have a public IP for your Primary Service, typically a VSAT. When the Primary service is out of range or in blockage, using your User GUI, you would manually connect to the internet using an alternative service. Assuming you have setup the switch back for the service, the Access Controller will continually check to see when your Primary Service is back online, it does this in the form of a 'Ping'. Once the Access Controller receives 12 successive ping responses in a row, which are sent 10 seconds apart, it will revert the internet connection back to the Primary Service.

You will see your user GUI change automatically:

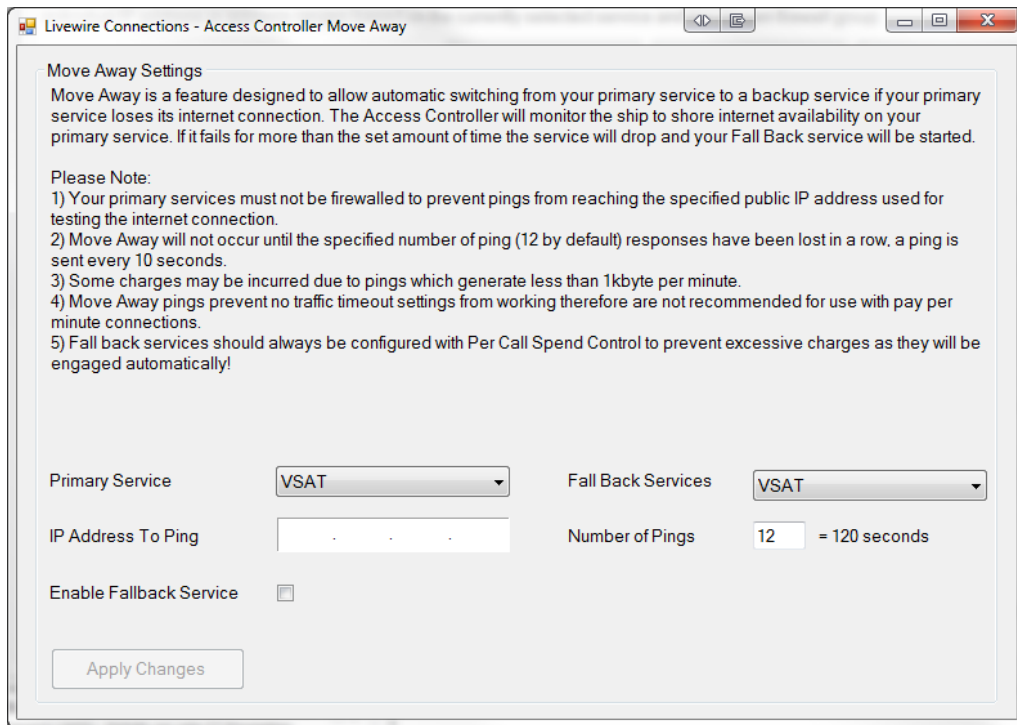


Switch Back Settings	
<i>Primary Service</i>	This is the service you want to automatically switch to when available.
<i>Primary Service Public IP</i>	This is the Public IP address of the Primary Service, (Normally public IP address of VSAT Modem). It is essential this IP address responds to pings from the internet. The primary service must not be firewalled to prevent pings from reaching the specified IP address for testing the internet connectivity.
<i>Switching Services</i>	Here you can select which of your other internet and communication services you wish to automatically revert back to your Primary Service, when the primary service becomes available.
<i>Number of Pings</i>	This is the number of consecutive pings that need to succeed before the service is automatically switched back to the primary service. The active Switching Service will ping the IP of the Primary Service constantly and switch after the specified number of consecutive pings have been successful.
<i>Apply Changes</i>	Applies changes made Automatic Failover settings to the Access Controller.

6.18. Access Controller Automatic Failover

Automatic Failover is a feature that if enabled allows the Access Controller to automatically switch to a secondary WAN connection in the event the primary connection suffers a loss of services.

This operated by constantly pinging a shore side IP address (normally the ISP's DNS server or similar). The ping is constantly sent from the Access Controller every 10 seconds. After a pre-determined number of unsuccessful pings (configurable as 'Number of Pings') the Access Controller will disconnect the Primary service and activate the Failover service. If service to the primary connection is restored Automatic Failover settings alone will not revert to the primary service unless in conjunction with [Switch Back](#).



Automatic Failover	
<i>Primary Service</i>	This is the service you wish to use as the primary service (eg VSAT)
<i>Failover Service</i>	This is the service you wish to use when the primary service does not have an internet connection. (eg Fleet Broadband)
<i>IP Address to Ping</i>	This is the IP address of a shore based server you wish to constantly ping to test internet connectivity.
<i>Number of Pings</i>	This is the number of consecutive pings that need to fail before the service is automatically switched. The Access Controller will ping the specified server once every 10 seconds.
<i>Enable Automatic Failover</i>	When check the Automatic Failover feature is enabled. Any loss in internet connectivity with the primary service will result in the automatic switching to the Failover Service. IMPORTANT NOTES: <ul style="list-style-type: none"> • The Automatic Failover feature should be used in conjunction with Switch Back to ensure the primary service is resumed as soon as possible. • The Automatic Failover feature should be used in conjunction with Spend Control if the secondary service is charged per Mb or per Min.
<i>Apply Changes</i>	Applies changes made Automatic Failover settings to the Access Controller.

Automatic Failover must be used with extreme care to avoid excessive airtime bills.

- The Automatic Failover service should be used in conjunction with [Switch Back](#) to ensure the primary service is resumed as soon as possible.
- The Automatic Failover service should be used in conjunction with [Spend Control](#) if the secondary service is charged per Mb or per Min. SIM provider level spend controls should always be used in addition to any onboard spend control.
- The primary service must not be firewalled to prevent pings from reaching the specified IP address for testing the internet connectivity.
- If the primary service is charged per Mb small data charges will apply for the monitoring of the primary service (approx 1kbyte/min).
- Automatic Failover will prevent '[No Traffic Timeout](#)' feature triggering and therefore it is not recommended when the primary connection is pay per minute.
- If the shoreside IP address used becomes unavailable the service will switch even if there is an good internet connection on the primary connection.

7. User GUI (Graphical User Interface)

7.1. User Login

From the shortcut on the Desktop or from the Start Menu run **'Access Controller'**.

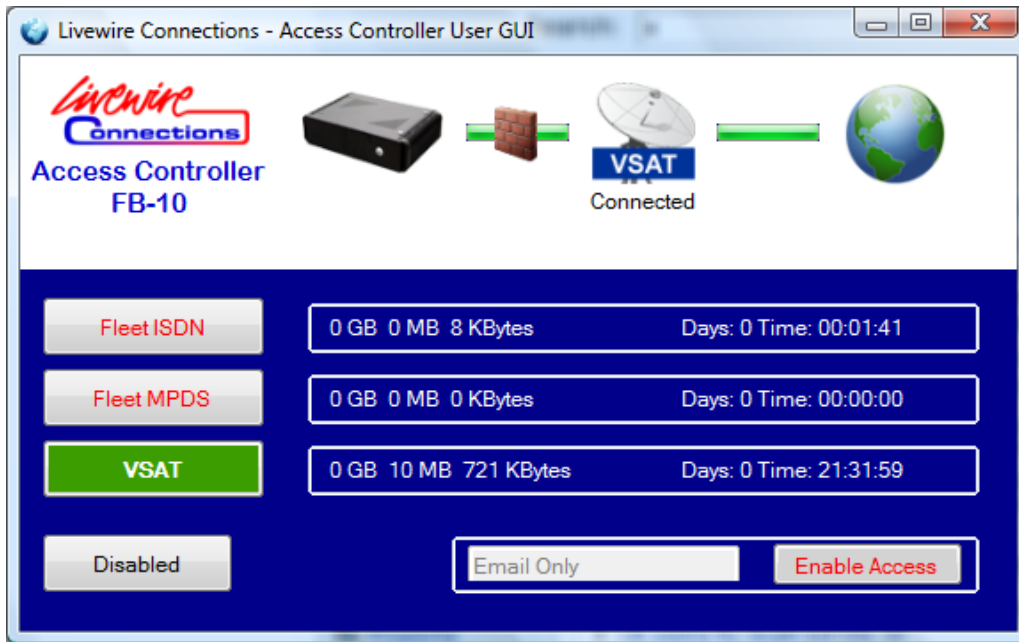
When prompted login using the default username (**'user'**) and default user password (**'password'**). Select **'User GUI'** and press **OK**. If the login is not successful see *Appendix 8.1 – [Troubleshooting](#)*



7.2. User GUI

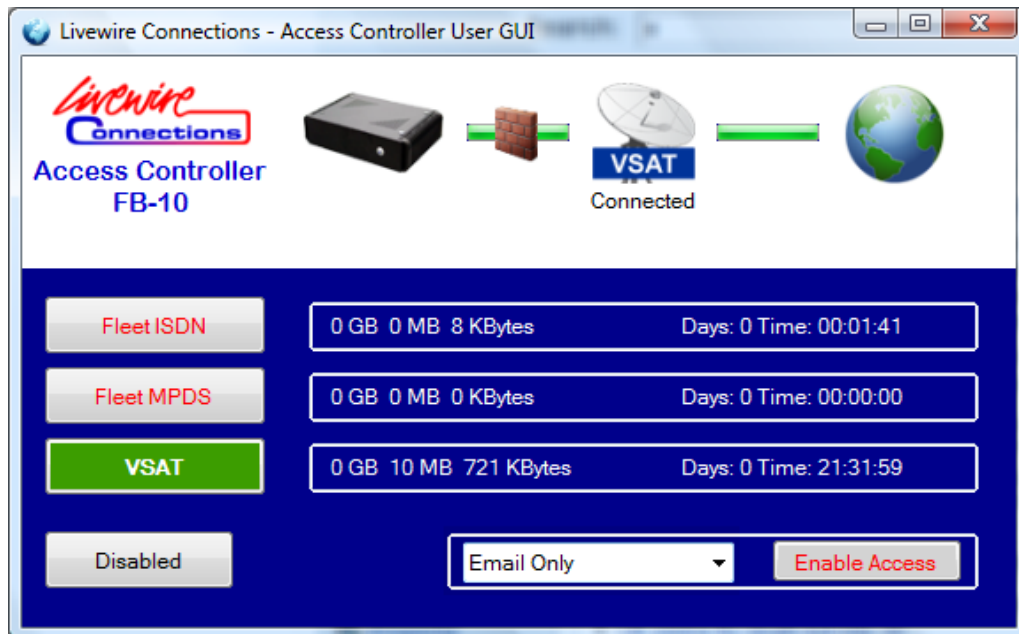


7.3. User GUI (Restricted Access)



Example:

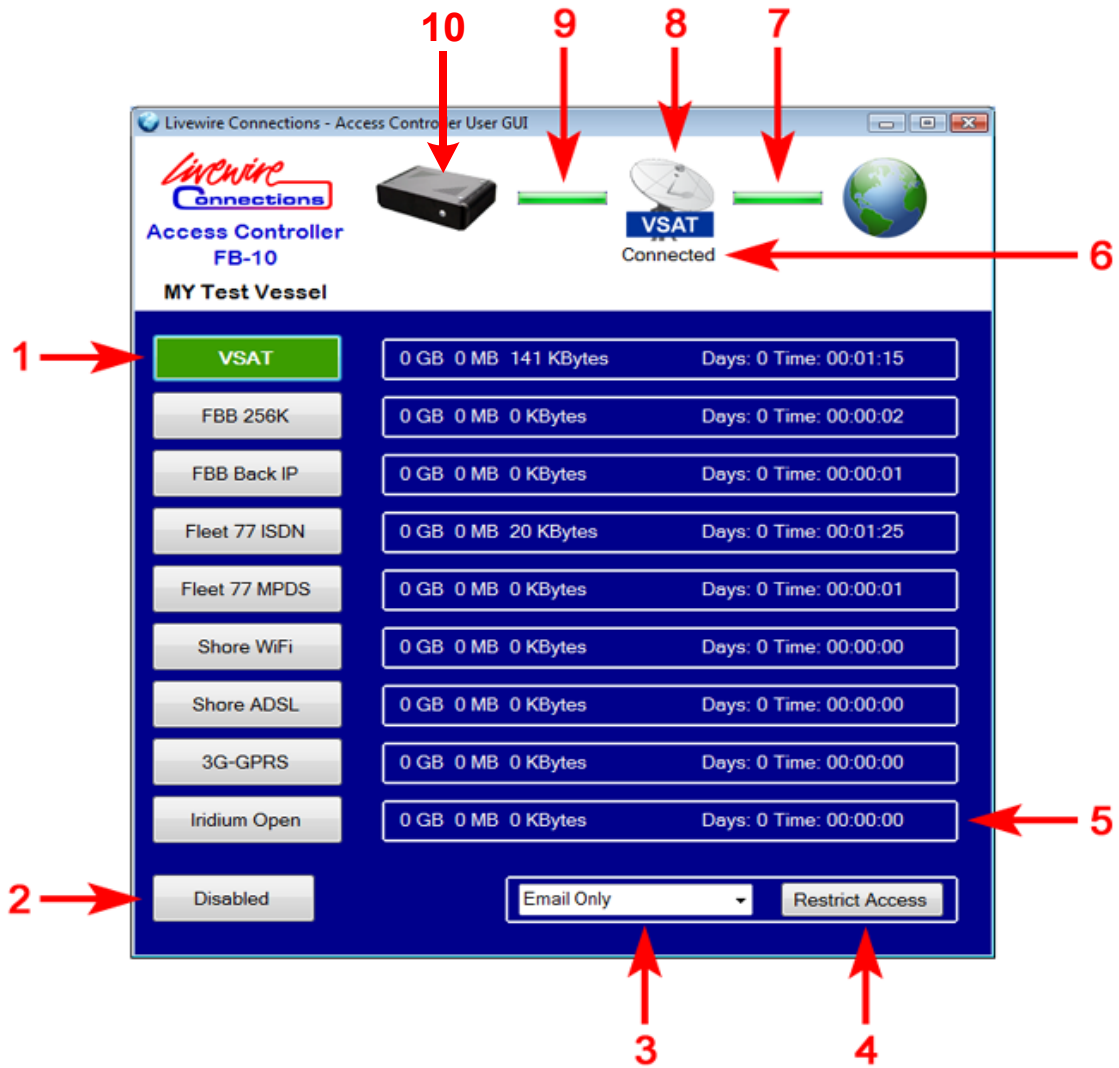
The logged in user above has too low permissions to select the Fleet ISDN and Fleet MPDS service. The user is also a “No Firewall” user so they cannot disable the Firewall, but they can change it.



Example:

The logged in user above has the same permissions as the previous Example. But here the user's firewall permission is set to “Firewall Group” so that the user can change it, but not disable/enable it.

7.4. User GUI Controls



#1	Service Activation Button	Select to activate named service. The box colour will change as follows: See Connection State Colour Indicators
#2	Disabled Button	Select to disconnect all services. Select a Service Activation Button (#1) to reconnect a service.
#3	Firewall Group Select	Use the drop down to select which Firewall Group will be applied.
#4	Restrict Access Button	Select to apply preconfigured Firewall Settings for the selected Firewall Group (#3). A 'wall' icon will appear across the LAN Status Indicator (#9)
#5	Volume & Time Counter	Counter displays the volume (measured in Gigabytes, Megabytes & Kilobytes) and time (measured in Days, Hours, Minutes and Seconds) of data measured at the WAN interface. (Note this will include local data between the Access Controller and the Modem device).
#6	Current State Status	Displays information regarding the current connection status. Error message will also be displayed here. See Troubleshooting
#7	WAN Status Indicator	Displays the status of the connection between the Modem Device and the Internet. (GREY: Disconnected GREEN: Connecting/Connected)
#8	Connection Icon	An icon representing the current connection. The icon used is dependent on the Service Template selected.

#9	LAN Status Indicator	Displays the status of the connection between the Access Controller and the Modem Device. (GREY: Disconnected GREEN: Connecting/Connected)
#10	FB10 Image	Click on the image to link through to the Access Controller web interface.

8. Appendix

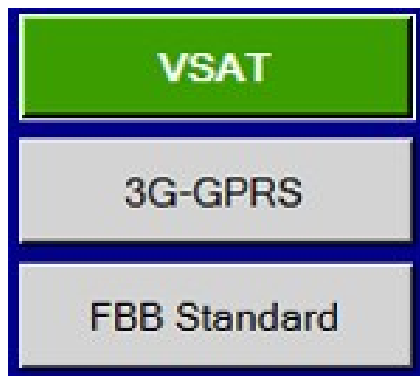
8.1. Troubleshooting

Issue/Error Message	Resolution
<p>Unable to Login to FB-10 (Message: Unable to connect in Title Bar)</p>	<ul style="list-style-type: none"> • Ensure that your PC is on the same IP range and subnet (default 255.255.255.0) as the FB-10. The default range is 192.168.5.X • Click 'Find' button on login page to try to automatically locate the FB-10. • Ensure that the FB-10 is switched on and power LED is illuminated. • If DHCP Server is enabled in the FB-10 (default) ensure that you have 'Automatically obtain IP address' selected in your Windows PC network configuration. • Ensure that you have connected an Ethernet patch cable securely to the LAN 8 interface of the FB-10. • If you are unable to access the FB-10 through the onboard vessel network as a test try to connect directly to the FB-10 with a Cross Over Ethernet cable between your PC and the LAN 8 port. • If you have recently changed the IP address of the FB-10 wait up to 600 seconds (Max Re Login Time) and try to connect on the original IP address. • Try to ping the FB-10 using Windows Command Prompt with the command for the default IP ping 192.168.5.1 and monitor the response. • Ensure that you have no Firewall rules on the PC or network that may be preventing access to the FB-10. • Power cycle the FB-10 by pressing the power button located on the front of the chassis and restart your PC.
<p>NO CARRIER</p>	<ul style="list-style-type: none"> • Check that the modem device is ready to make a call. • Check the device has registered successfully on the network. • Check the device has a valid GPS position (If relevant). • Check the device has good signal strength and is not blocked. • Check that the SIM card has not got a PIN number configured (if relevant)

BUSY	<ul style="list-style-type: none"> • The FB-10 cannot dial a connection as the line is busy. • Ensure that the device does not have a current call up and that is ready for a call.
ERROR	<ul style="list-style-type: none"> • Unspecified error received from the device. • Something is wrong with the terminal, check settings, signal strength or reboot terminal if error persists.
No response from terminal	<ul style="list-style-type: none"> • The access controller cannot communicate with the terminal. • Check that the device is connected to the correct interface port of the FB-10. • Check cable connection between the device and the FB-10.
Unknown CME Error received. Check system log for more details.	<ul style="list-style-type: none"> • Non standard error message received from terminal. • Unknown cause. Try rebooting the device.
Call failed during critical stage! Check handset to avoid rogue call!	<ul style="list-style-type: none"> • Connection lost to Fleet Broadband terminal, could not verify that call was dropped/initialised. • Check status of device.
Unexpected message received from terminal.	<ul style="list-style-type: none"> • A command or message was received from the FB terminal which was not expected. • Non-supported terminal manufacture or firmware version. • Check device has latest Firmware version available.
Could not connect to terminal. Check terminals status.	<ul style="list-style-type: none"> • The access controller cannot communicate with the terminal. • Check that the device is connected to the correct interface port of the FB-10. • Check cables connection to the device from the FB-10.
No cable/device attached	<ul style="list-style-type: none"> • No Ethernet cable was detected, • Ensure the correct cable type is used (Straight/Cross over) and that the device is properly connected.
Failed to get DHCP	<ul style="list-style-type: none"> • No DHCP server was detected. • Reconfiguring service as a static IP address or make sure the DHCP server is switched on in the device's setup • Reboot the device.

Failed to initialise IP configuration	<ul style="list-style-type: none"> The statically configured IP address settings could not be used, verify that they are correct and that they are not already in use by any other device.
Other Errors	<ul style="list-style-type: none"> Standard +CME Errors may be displayed in the FB-10. Please refer to your device documentation to resolve.

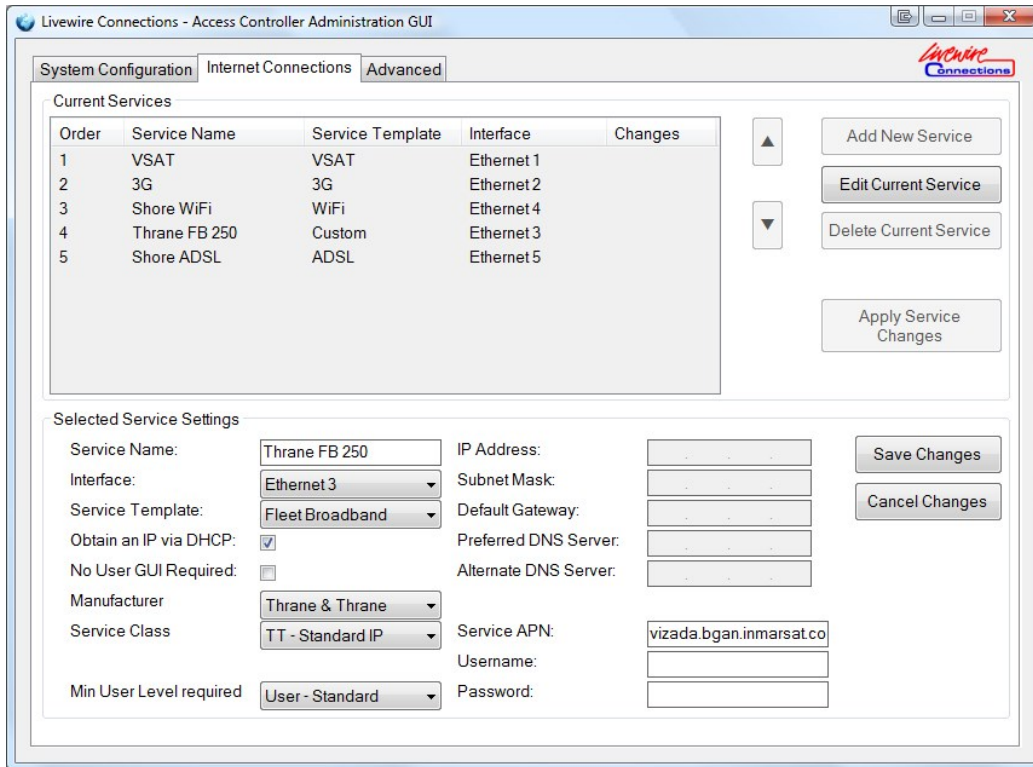
8.2. Connection State Colour Indicators:



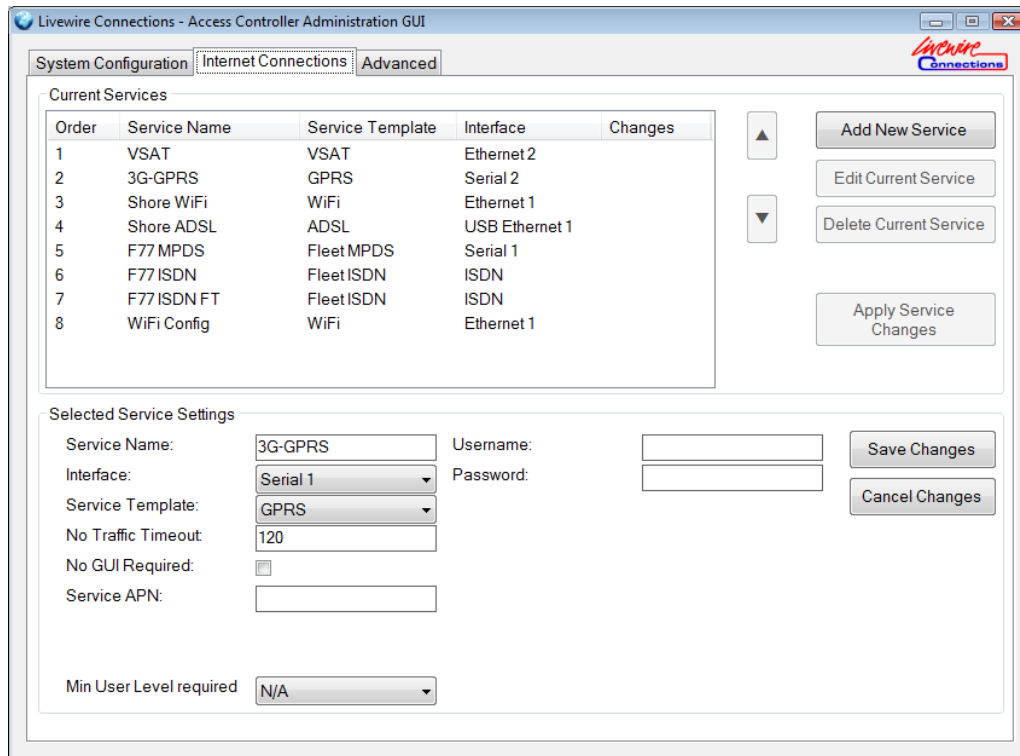
Example connection state colour indicator

Colour Indicator	Connection State
	Activating
	Idle
	Connecting
	Local Device Connect
	Authenticating
	Connected
	Disabled
	Error

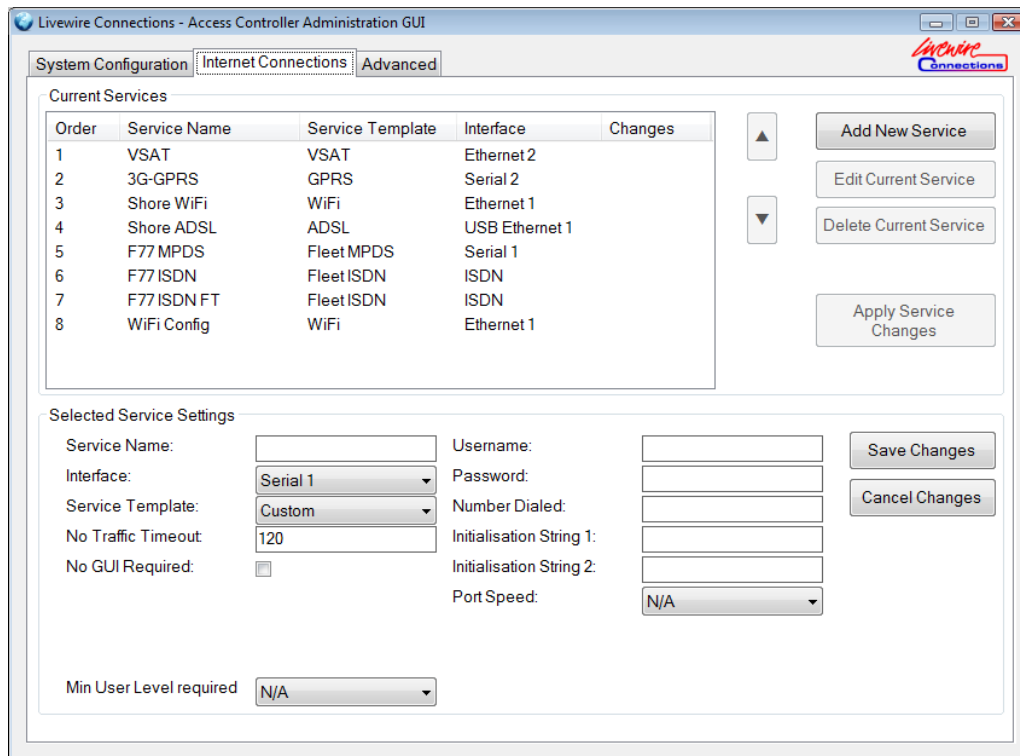
8.3. Internet Connections – Templates



Above is an Ethernet based service using the Thrane Fleet Broadband – Background Class template.

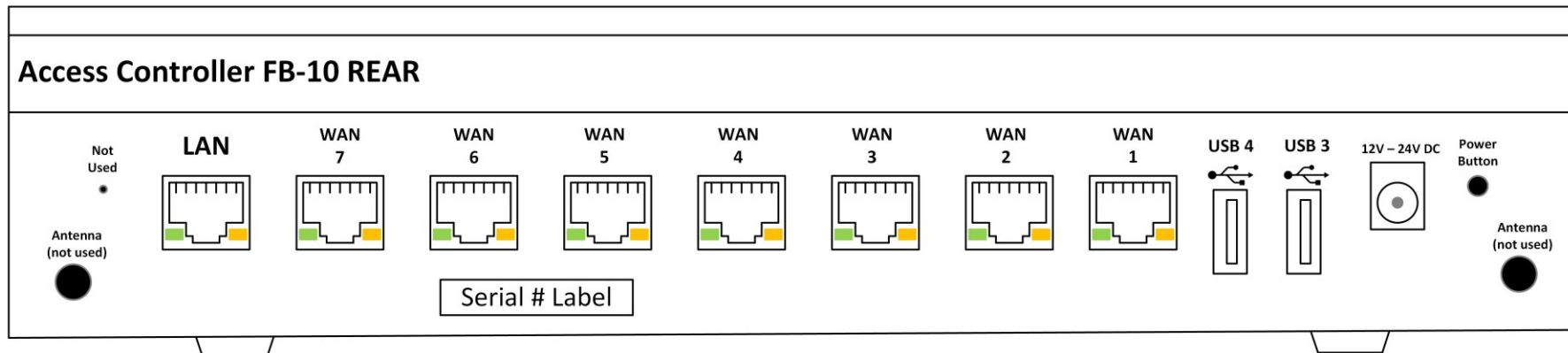
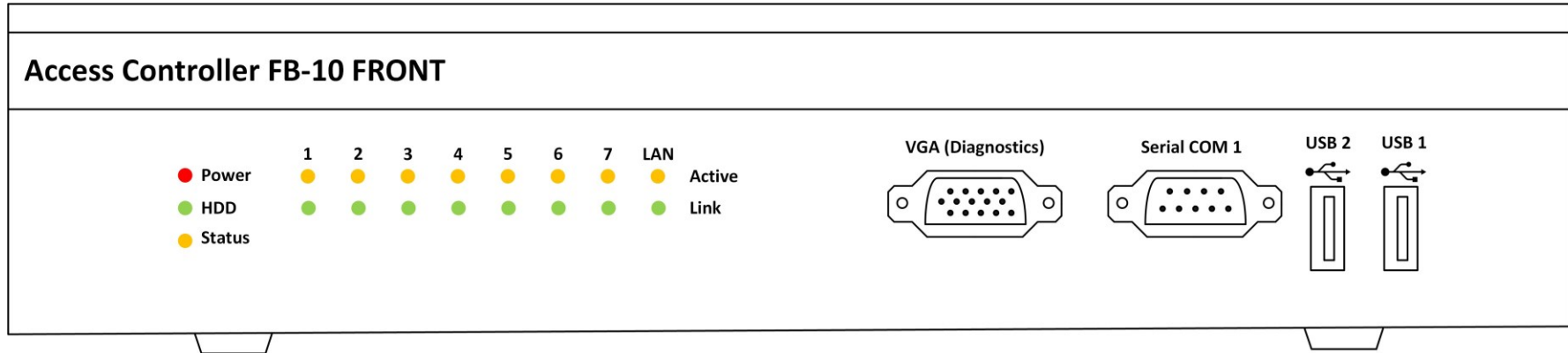


Above is a Serial based service using the GPRS template which provides only the necessary options for GPRS over serial connections.



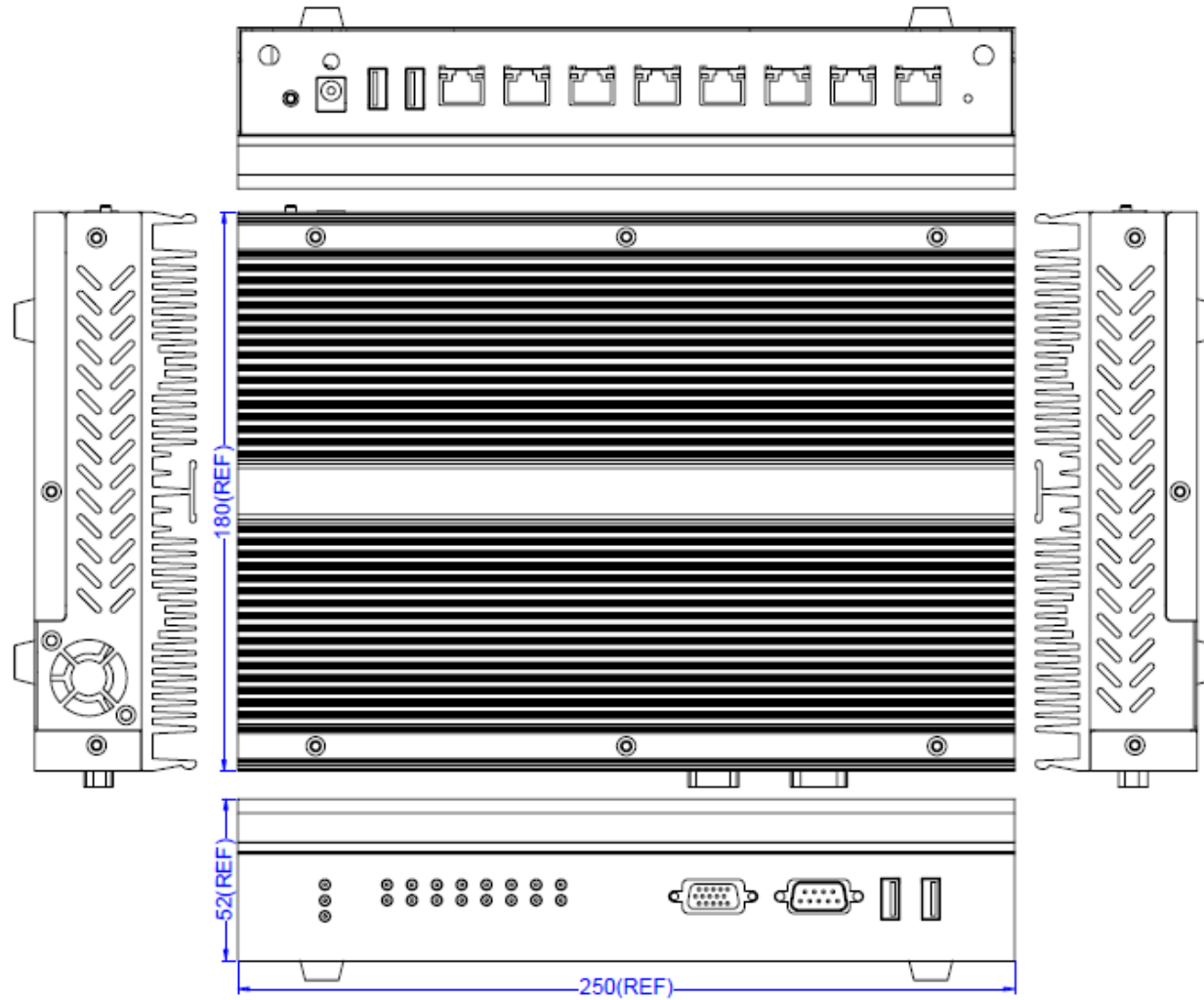
Above is a Serial based service using the Custom template which provides all the configurable options for serial connectivity.

8.4. Interface Drawing

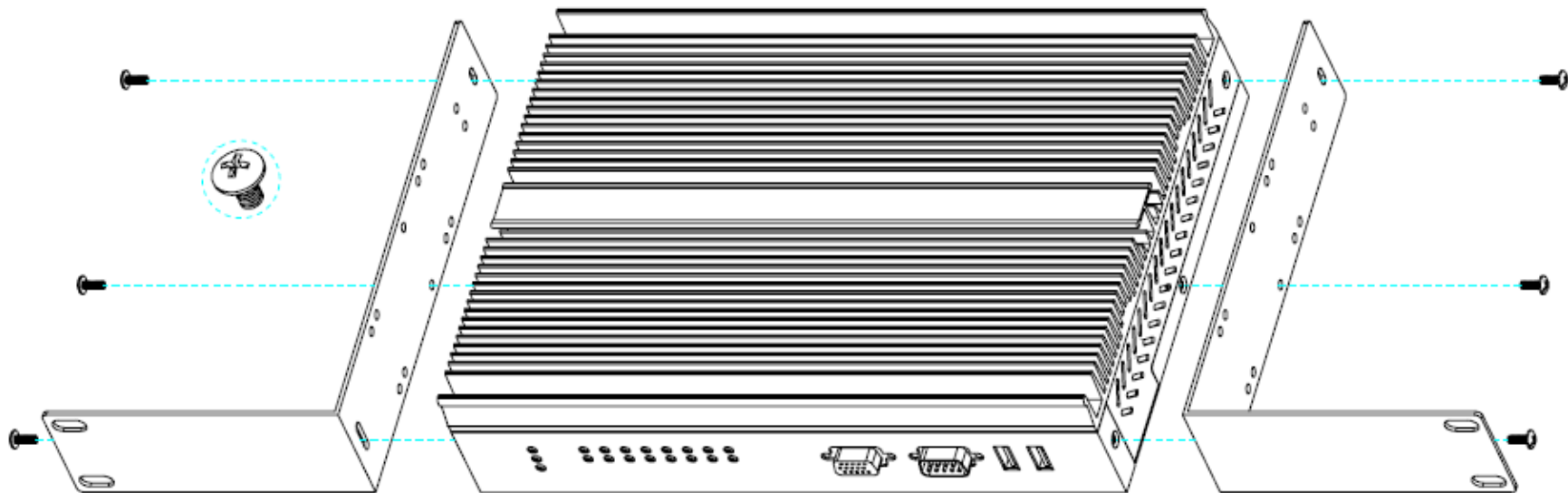


8.5. Hardware Drawing – FB 10 without brackets.

All dimensions are in mm



8.6. Hardware Drawing – FB 10 Rack mounted (19" Rack).



9. Technical Specifications

Model	FB-10
Dimensions (mm)	250(W) x 180(D) x 52(H) – Without rubber feet.
Weight	2.95 Kgs (Packaged Weight)
Chassis Material/Colour	Aluminium/Black/Blue
Ambient Operating Temperature	0 to 40°C
Operating Humidity	5~95% @ 60°C, non-condensing
Power Supply	12-24V DC input; 19V DC 100–240V AC. 1.5A 50-60Hz power adapter supplied
Interfaces	1 x Vessel LAN (Port 8) 7 x WAN (Ports 1-7) 4 x USB (For Approved devices only) 1 x Serial (RS232) 1 x VGA
Approvals	EN 55022:2006 +A1:2007, Class B EN 61000-3-2:2006 +A1:2009 +A2:2009 (Class D) EN 6100-3-3:2008 EN 55024:1998+A1:2001+A2:2003 IEC 61000-4-2: 2008 IEC 61000-4-3:2006+A1:2007 IEC 61000-4-4:2004 IEC 61000-4-5:2005 IEC 61000-4-6:2008 IEC 61000-4-8:2009 IEC 61000-4-11:2004 FCC 47 CFR PART 15 SUBPART B (Class B) IC ICES-003 Issue 4

10. Further Information

1. Updates

For Software, Firmware, User Manual, Demo and FAQ updates visit

<http://www.livewire-connections.com/support>

<http://www.accesscontroller.co.uk>

For more information about the *Livewire Access Controller FB-10* please contact your local distributor. Product brochures, software demos and pricing can be found at

<http://www.accesscontroller.co.uk>