WebWayOne Command Centre

User Guide

Issue Level	Author	Date	Comments
1.0	Tom Davies	03.12.2015	First Issue

Table of Contents

1.0 Command Centre.....How It Works....What It Does 3
1.1 Login 5
1.2 Operator Levels 7
Observers 7
Operators 7
Administrators 7
Super Users 7
1.3 Loading Estates 8
1.4 Loading Sites 9
1.5 Control / Status Screen Breakdown 10
1.5.1 Link Status and Site States 11
1.5.2 Ethernet Status 13
1.5.3 Cellular Status 14
1.5.4 Poll Status 15
1.5.5 Hardware Status 16
1.5.6 Site History 17
2.0 Availability 18
3.0 Alarms 19
4.0 Commissioning - Take On / Take Off 21
5.0 Configuration Updates / Modifying Sites 21
5.1 Updating Configuration Immediately 22
5.2 Updating Configuration on Next Poll 22
6.0 Reboot Site Function 22
Reboot Immediately 22
Reboot on Next Poll 23
Reboot via SMS 23
7.0 Firmware 23
8.0 Managing Users 23
9.0 Software Updates 24

1.0 Command Centre.....How It Works....What It Does

The WebWayOne Command Centre is a Microsoft Windows based PC application which provides a means of controlling and monitoring the status of any Estate of WebWayOne Communicators through network connections to the WebWayOne Gateways.

Using a sophisticated but intuitive menu system, the Estate Manger shows live monitoring of Estates and of the Sites within an Estate. Its status screens highlight large-scale communication problems within Estates and also on Site communication problems with individual Communicators. Tools within the Command Centre allow operators to diagnose on-Site hardware and configuration problems and to remotely fix any configuration problems found.

Command Centre was originally designed by the WebWay Development team as a internal tool to provide a user interface for the management of WebWay SPTs in the field. Over time it has been developed and rolled out to customers so they also can pro-actively monitor SPTs in the field.

A number of things need to happen before a user can log into Command Centre.

Firstly a Command Centre connection will need to be configured. After the installation of Command Centre from the installation binary; the party completing the installation will need to configure Command Centre to talk to the intended MCT cluster.

If the end-user is only connecting to one MCT cluster then this configuration can be completed using the 'Command Centre' icon which is installed on the desktop as the 'gdf' (gateway definition file) otherwise additional ‘gdf’ files can be generated (typically one for each MCT cluster.)

When configuring the 'gdf' file the party completing the installation will need to log in with the WWO Manager credentials to fill connection credentials and define the destination addresses of the MCTs which the Command Centre will connect to.

Command Centre can be configured to connect to either external IP addresses of MCTs (on port 22 or the defined SSH port) or when Command Centre is on the same network as the MCTs it can connect via internal addressing. When connected via internal addresses on port 50575 Command Centre does not need to have Public/Private SSH key pair credentials defined (the fields are left blank in the WWO Manager configuration.)

For an external connection the SSH User and associated public/private key pair will need to be selected and filled in correct field in the second column and the file path to the associated key file will also need to be defined. The private key will be in a different format to the Remote Manager key but share the same public key partner on the MCT.

A valid Login Username and Password are also required. This can be any user of any level of user access as in this part it is only used by Command Centre for the initial log in to read the allowed user list from the MCT. Please be aware that any change to this user will render this install of Command Centre non-functional until a valid user/password combination is entered. The Login Username and Password are value defined in a table on the MCT and are not the same as the Public/Private SSH key pair. They can be configured to match if required.

With this configuration method WebWay maintains the security of the solution by restricting individual user access whilst at the same time providing a consistent level of user access for the individual. For example user 'tomd' has the same access to sites and Operator level on any Command Centre instance regardless of the permission level of the SSH key used for the connection.

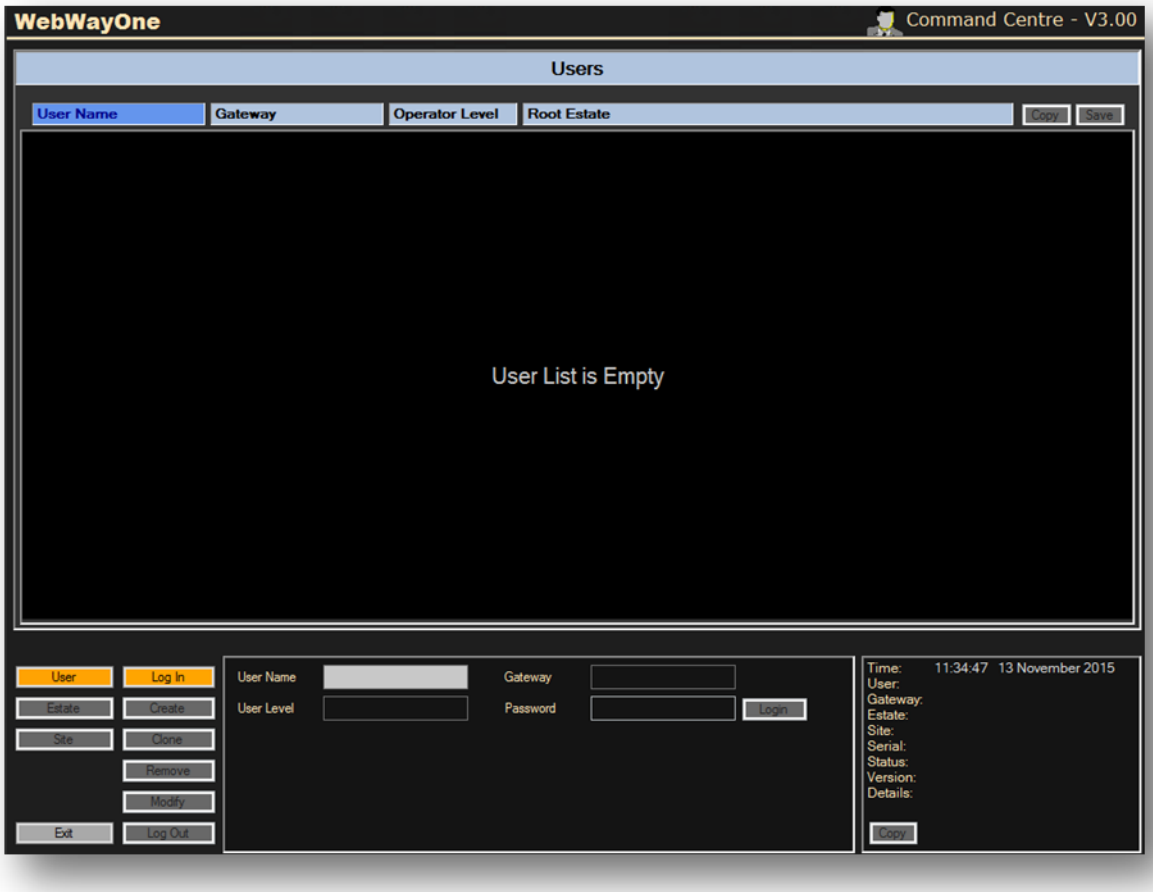
Prior to installation the customer could have a Command Centre User and Password created on any instance of Command Centre logged into the MCT cluster by a user of the appropriate Operator level.

1.1 Login

Before Command Centre can perform any operation or display any information about Sites, Estates, Users or Gateways, a user has to log in to obtain:

- Authentication – to prove the operator is known to the Gateway, has a valid password and therefore has the access rights to the Command Centre controls on that Gateway
- Authorization – to let the Gateway know which of Command Centres features are accessible by the user, by means of their Operator Level.

When the Command Centre application is loaded; it will attempt to contact the MCTs which it has been configured to talk to. This will be displayed on the splash screen. Once a connection has been made to each of the MCT in turn Command Centre will read the user-list from the MCT provided that it has been configured correctly.



The user will be presented with blank login space. At this point the user will need to enter their username and press enter (whilst the cursor is still in the white box).

The user will then be presented with a choice of MCTs (if they have been configured and if there are available slots for login).

User Name	Gateway	Operator Level	Root Estate
tomd	WWO Development (1)	SuperUser	gateway
tomd	WWO Development (2)	SuperUser	gateway

The user then enters their password and is given access. The workspace then displays the user list consisting of all the users who have the same level of access or less.

This screen also displays in Column Four the highest estate within the estate tree each user has access to.

User Name	Gateway	Operator Level	Root Estate
TestUser1	WWO Development (1)	SuperUser	gateway
TestUser10	WWO Development (1)	Operator	gateway
TestUser11	WWO Development (1)	Operator	gateway
TestUser12	WWO Development (1)	Operator	gateway
TestUser13	WWO Development (1)	Operator	gateway
TestUser14	WWO Development (1)	Operator	gateway
TestUser15	WWO Development (1)	Operator	gateway

The access level is shared across each of the MCTs of the cluster. It also maintains the security of the solution by restricting individual user access whilst at the same time providing a consistent level of user access for the individual. For example user 'tomd' has the same access to sites and Operator level on any Command Centre instance regardless of the permission level of the SSH key used for the connection.

1.2 Operator Levels

Command Centre has four "Operator Levels". When a new user is created, their user Account is assigned an Operator level which tells Command Centre which features and facilities are to be made available to that user when they log in. The user's Operator Levels are shown in the third column of the User Workspace.

The operator levels are: Observers, Operators, Administrators and Super Users.

Observers

Observers can only:

- View the status of Estates
- View the status of Sites
- View alarms from Sites

Operators

Operators can do everything Observers can do and in addition:

- Commission and Decommission Sites
- Update configuration on Sites
- Upgrade Firmware on Sites
- Reset Sites
- Reboot Sites
- Reset the 'Flooded' status of Individual Sites
- Control output relays on the Communicators on Sites
- Generate, edit and view support tickets for Sites
- Perform Interface and Path diagnostics
- Perform Board-level diagnostics

Administrators

Administrators can do everything Operators can do and in addition:

- Create and Clone Sites
- Modify Sites details
- Remove Sites
- Create and Clone Users
- Modify User details
- Remove Users
- Change and view board configuration parameters
- Create Estates
- Modify Estates (rename and move to new parent Estate)
- Remove Estates
- View Gateway Status (Flood Status, Unknown Sites, Unknown Numbers)
- Clear Gateway flood state

Super Users

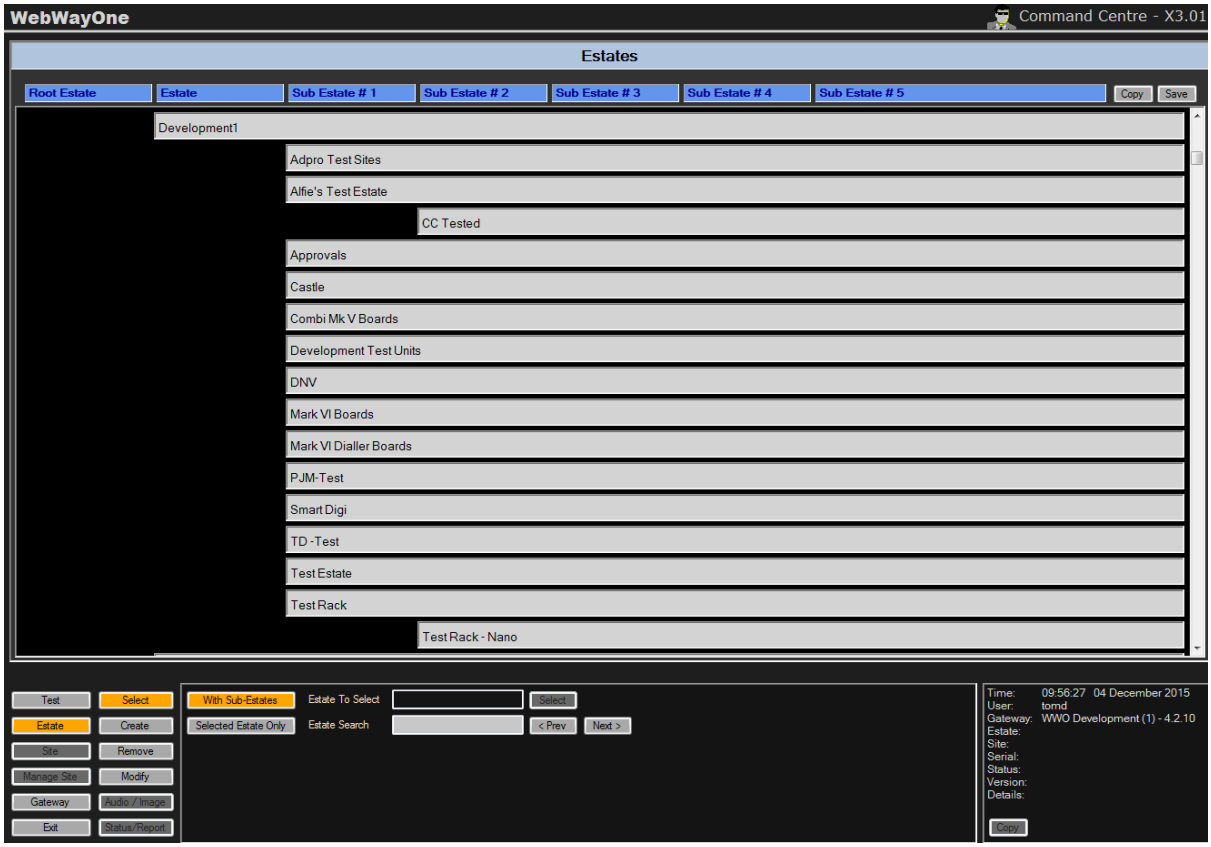
Super Users can do everything Administrators can do and in addition:

- Set Gateway flood state.
- Add Gateways to the Command Centre
- Remove Gateways from Command Centre
- Modify details of Gateways
- Perform Advanced Communicator diagnostics on Sites.

1.3 Loading Estates

Once a user has logged into the Command Centre platform they will want to be able to view estates and sites.

The user will need to select ‘Estate’; this will load the user’s visible estate tree into the work area. (Users will only be able to see and access what they have been given permission to see and access.)

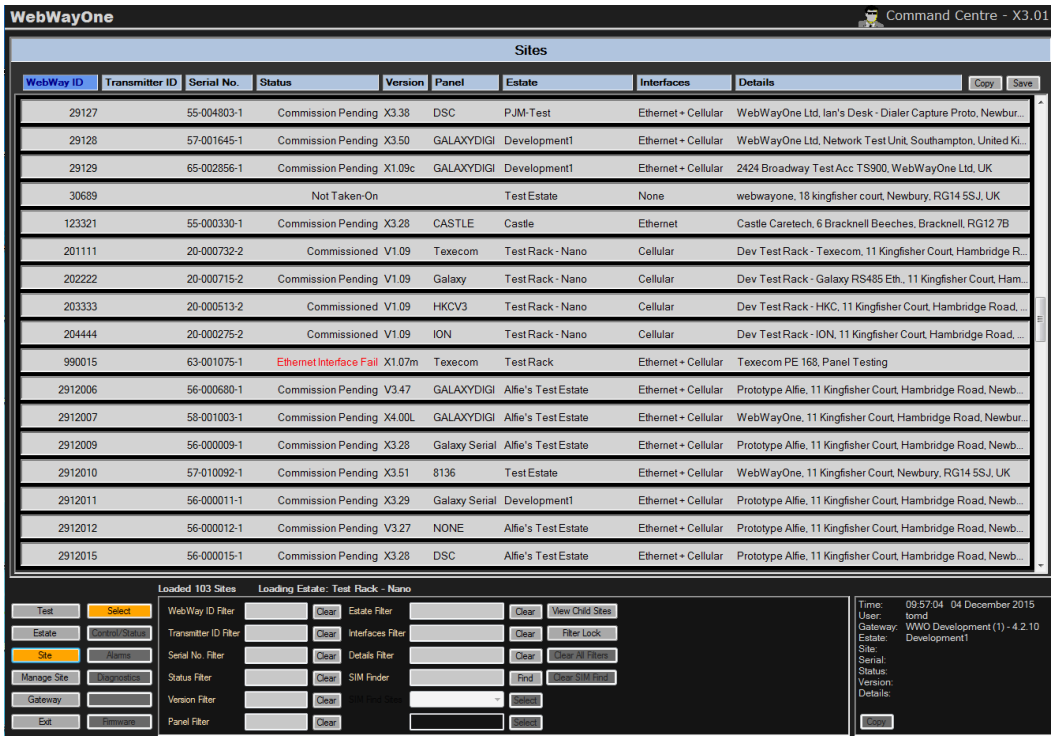


Estates can then be loaded by double-clicking on the appropriate estate in the workspace. Command Centre will then load all the sites within the estate which can then be viewed. Loading an estate will load all the sites within sub-estates of the estate loaded unless the ‘Selected Estate Only’ option is activated.

The ‘Estate Search’ option can be used to search of the full name or part name of the estate. Where the estate of a site is not known it is possible to load the entire gateway (provided the user has the access level) and then search for the site at the site level with the site details (address, postcode etc.)

1.4 Loading Sites

Once an 'Estate' is selected the user can then move down to the site level to load and view individual sites.



The workspace will now show a list of all the sites within the loaded estate. The workspace will show the current state of the site as well as some of the site information.

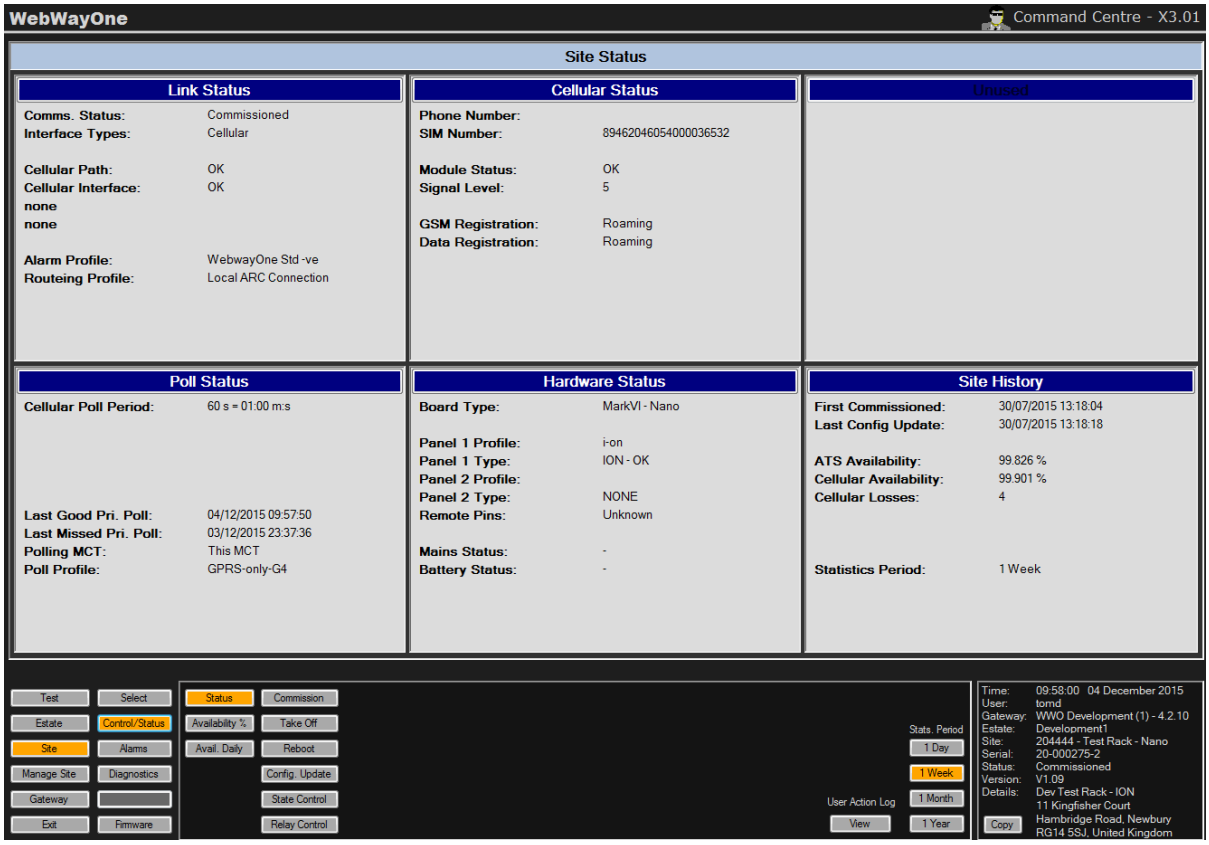
Filling in values into the fields in the Control Menu will filter the results in the workspace above.

Once the user has found the site they wish to view then they will need to double-click the site in the workspace and it will load it as the 'active' site.

The bottom-right information panel will now display the site information of the current 'loaded/active' site.

1.5 Control / Status Screen Breakdown

Once the user has select an individual site they will need to click on the 'Control/Status' button to view the current information of the selected site.



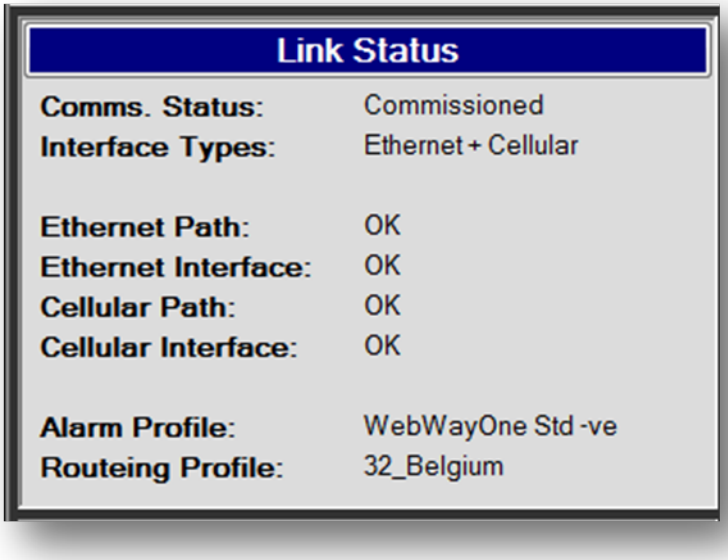
From this screen the user is presented with additional information on current state of the configured paths of the SPT. This information is a reflection of the last state the SPT reported into the receiver so the Command Centre platform is not logged directly into the SPT.

From this screen a trained user can distinguish the manner in which a site is signalling; the current status of the transmission paths; where the signals are being delivered; how frequently the site is polling in and an overall picture of site performance over a short period.

This guide will break down each of the 'panels' within the workspace in further detail.

1.5.1 Link Status and Site States

The first panel of the Control/Status screen is the '*Link Status'*; this defines which communication path the sites and by extension the SPT in the field is configured to communicate over.



The '*Comms Status'* displays the current status of the site. The various states users are likely to encounter are listed below;

Not Taken-On = No SPT has been installed on this site to signal to this site ID.

Commission Pending = this means that a site has an SPT associated to it but the site is pending communication from the SPT. If this does not change within 10 minutes then the site is not communicating.

Commissioned = this means that all configured paths are functioning. Column 8 in this screen shows which Interfaces are configured for this site.

Comms Fail = this indicates the site was functioning and has lost communications with the MCT so the MCT has declared a communications failure.

GPRS Interface Fail = this indicates the SPT has lost signal to the local mobile cell. Either the cell has an issue or the aerial equipment is not good enough/placed well enough to pick up a signal. This state means that the other communications path is still working.

GPRS Path Fail = this indicates the SPT is picking up the local cell but cannot communicate through the mobile network. Either there is a networking issue or a configuration issue. This state means that the other communications path is still working.

Ethernet Interface Fail = this indicates the Ethernet cable is not connected into a live network. This state means that the other communications path is still working.

Ethernet Path Fail = this indicates the Ethernet is physically connected on site but there is a configuration or network access problem. This state means that the other communications path is still working.

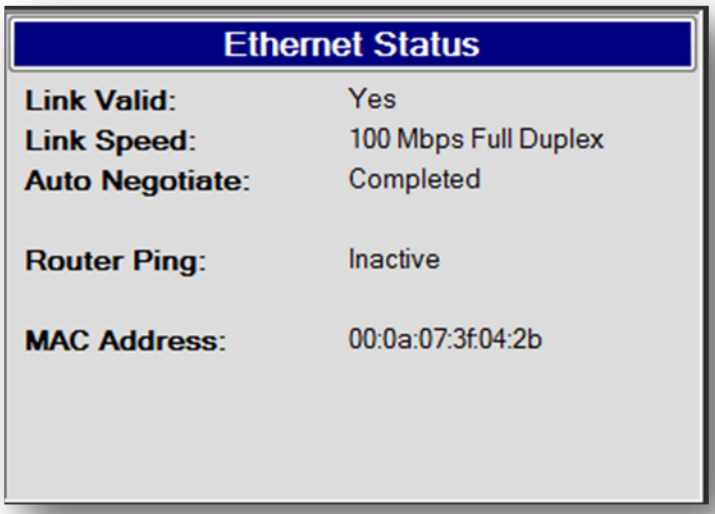
The '*Alarm Profile'* details which hardwire pin profile has been selected and applied to the site. New hardwire pin profiles should only be configured by WebWay Technical staff; details on amending which of the pre-configured profiles is used for the site will be covered further in this document.

The '*Routeing Profile'* details the configuration of where the alarms are being delivered. New destinations should only be configured by WebWay Technical . Details on amending this field will be covered further on in this document.

Which of the following panel are displayed to the user will change dependant on the interfaces configured for a particular site. For example a site configured for Ethernet only (as the only communications interface) will not have a 'Cellular Status' panel and will not include reference to the availability of a cellular path in the 'Site History' panel.

1.5.2 Ethernet Status

The '*Ethernet Status'* panel displays information relevant to the Ethernet connection where Ethernet is defined as a path in the configuration of the site.



The *'Link Valid'* indicates if the SPT has been able to establish a physical connection onto networking equipment (router/switch). This will either be Yes/No dependant on whether the Ethernet interface can see Layer 1 connection to a switch or router.

The '*Link Speed'* displays the currently configured (normally through Auto-Negotiation) speed of a valid Ethernet connection.

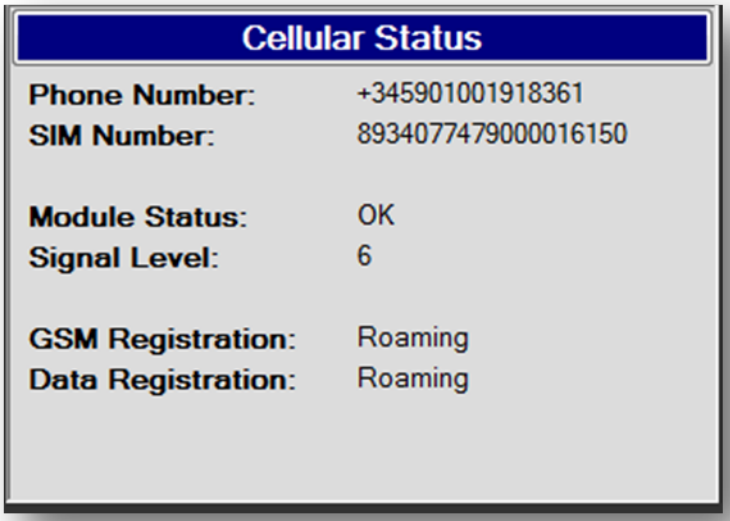
'*Auto Negotiate'* indicates that the SPT has been able to auto-negotiate a successful connection onto the local Ethernet network.

'*Router Ping'* shows the current ping status of a router when the mechanism is configured correctly. (This is not typically used on a standard site.)

'MAC Address' displays the MAC Address of the SPT which can be used by end-user IT Technicians to find the SPT on their networks. This field is set in the SPT on Production and is calculated from the serial number. This field will display even without a valid Ethernet connection working as Command Centre is able to calculate it from the serial number allocated to the site.

1.5.3 Cellular Status

The '*Cellular Status'* panel displays the information relevant to the Cellular connection if where 'Cellular' is configured as a communications path in the site configuration.



The '*Phone Number'* field displays the phone number allocated to the SIM which is installed in the SPT.

The '*SIM Number'* is the SIM number of the SIM which is installed in the SPT.

'Module Status' is a reflection of a period check by the SPT that the ISM module on the SPT is present and functional.

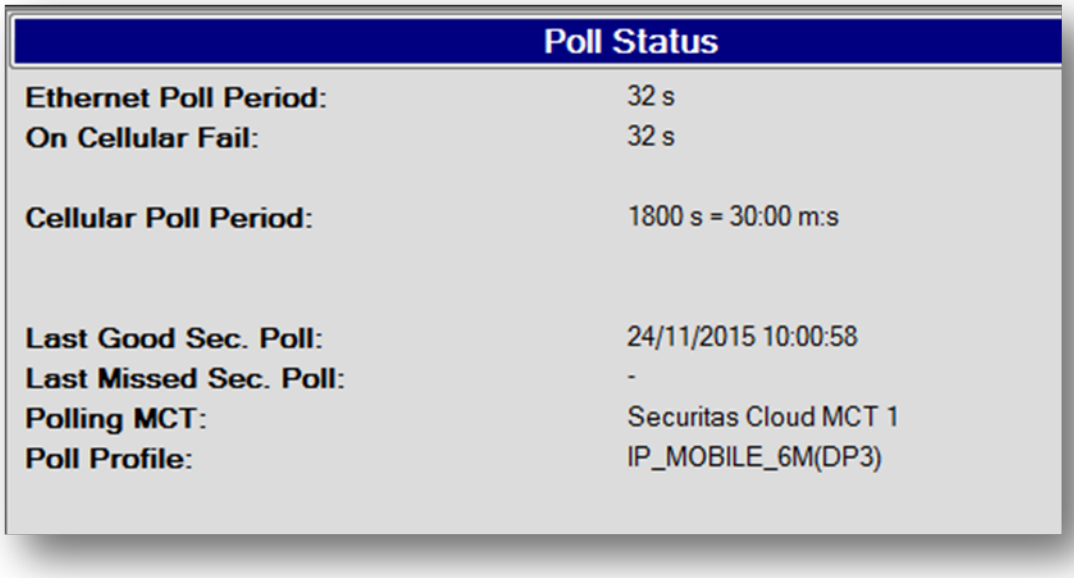
'*Signal Level'* is a measure of the strength of signal the SPT is able to see using a scale of 0-10 (with 10 being displayed on the SPT as A.) This measure is taken from the SPT each time it polls in. (A value may be in this field if the unit is in a 'Comms Fail' state and it is a reflection of the last signal strength seen before a communications loss.)

The '*GSM Registration'* and '*Data Registration'* are indicators of the state of the SPT's SIM on the mobile network at the point of the last successful poll from the SPT.

Additional diagnostics can display which network a unit has connected onto and whether a unit is using 3G or has fallen back to 2G.

1.5.4 Poll Status

The '*Poll Status'* panel displays information relevant to the polling configuration and status relevant to the site.



The '*Ethernet Poll Period'* denotes the time the MCT expects between sequential polls over the Ethernet interface when the interface and path are in a good working state.

'*On Cellular Fail'* denotes the time the MCT will expect between sequential polls over the Ethernet interface when the cellular interface is in a failed state.

'*Cellular Poll Period'* denotes the time the MCT expects between sequential polls over the cellular interface when the SPT/site is in a good working state.

'*Last Good Sec. Poll'* denotes the last time that the SPT polled in successfully over the Secondary Interface.

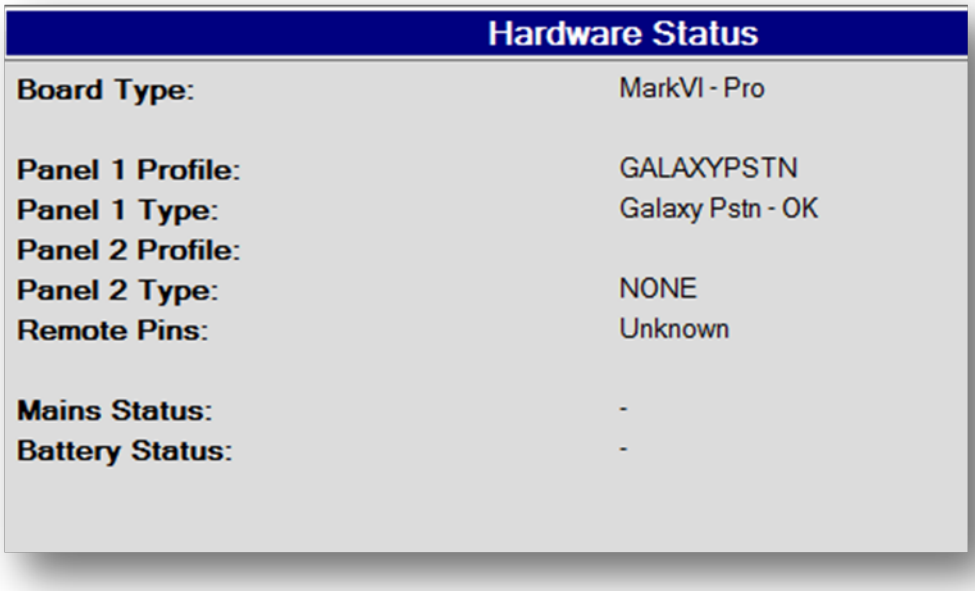
'Last Missed Sec Poll' denotes the last time at which the SPT was expected to poll into the MCT over the secondary interface but failed to do so successfully.

'*Polling MCT'* denoted which of the MCT cluster is the 'active' polling MCT. This is the MCT that the SPT is primarily talking to over (when in a good state) its primary interface. If the user is logged into Command Centre on the MCT which is the 'Polling MCT' then the 'Last Good...Poll' and 'Last Missed...Poll' will be displayed for the Primary interface. If the user is logged into the 'Non-Polling MCT' then the Polling information will be for the secondary interface (where one is configured).

'*Poll Profile'* displays the currently configured poll profile for with which the site has been configured.

1.5.5 Hardware Status

The *Hardware Status* panel displays information relevant to the status of the board in terms of physical hardware and the state of the interface(s) which have been configured.



'*Board Type'* denotes the hardware variant of the SPT which is allocated to the site.

'*Panel 1 Profile'* denotes the name of a panel hardware profile which has been selected/configured in the site configuration.

'*Panel 1 Type'* denotes the state of the interface to a configured panel. Where connected via RS485 or RS232 this reflects the state of a 'heartbeat' between the SPT and the panel.

'*Panel 2 Profile'* denotes a second configured panel hardware profile which has been selected / configured in the site configuration.

'*Panel 2 Type'* denotes the state of the interface to an additional configured panel. Where connected via RS485 or RS232 this reflects the state of a 'heartbeat' between the SPT and the panel.

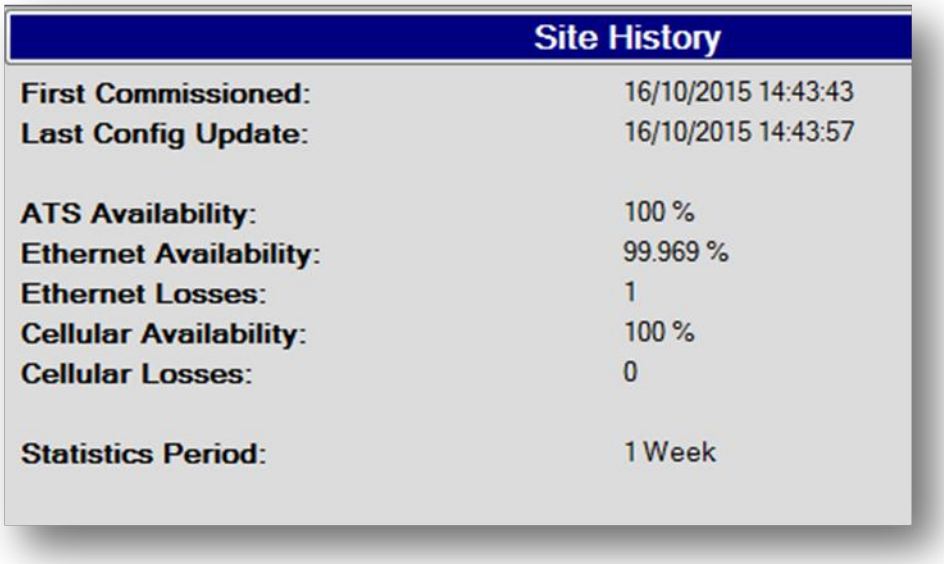
'*Remote Pins'* denotes the current state of a 'Remote Pins' board in relation to a 'heartbeat' which exists between the SPT and the Remote Pins board where a Remote Pins Board is configured.

'Mains Status' denotes the current state of the Mains where it is configured to signal the state via the direct onboard connection of the SPT rather than a hardwire pin.

'Battery Status' denotes the current state of the Battery where it is configured to signal the state via the direct onboard connection of the SPT rather than a hardwire pin.

1.5.6 Site History

The *'Site History'* panel details key information about availability and specific site actions in a 'quick view' information panel to allow for easier site management.



'*First Commissioned'* shows the date and time of the first Commission of this Site

'Last Config. Update' shows the date and time of the last known configuration update for the Site

'ATS Availability' shows the availability of the ATS as a whole over the period shown in the "Statistics Period" field. This is the percentage time that either the Primary (in this example Ethernet) and or the Secondary (in this example Cellular) paths have been available for alarm transmission

'*Ethernet Availability'* shows the availability of the Ethernet Paths as a whole over the period shown in the "Statistics Period" field. This is the percentage time in the period for which at least one Ethernet path was healthy and available for alarm transmission.

'*Cellular Availability'* shows the availability of the Cellular Paths as a whole over the period shown in the "Statistics Period" field. This is the percentage time in the period for which at least one Cellular path was healthy and available for alarm transmission.

'*Ethernet Losses'* this shows the number of times the Ethernet Interface or all Ethernet Paths have gone from a working state to a non-working state in the period shown in the "Statistics Period" field.

'Cellular Losses' this shows the number of times the Cellular Interface or all Cellular Paths have gone from a working state to a non-working state in the period shown in the "Statistics Period" field.

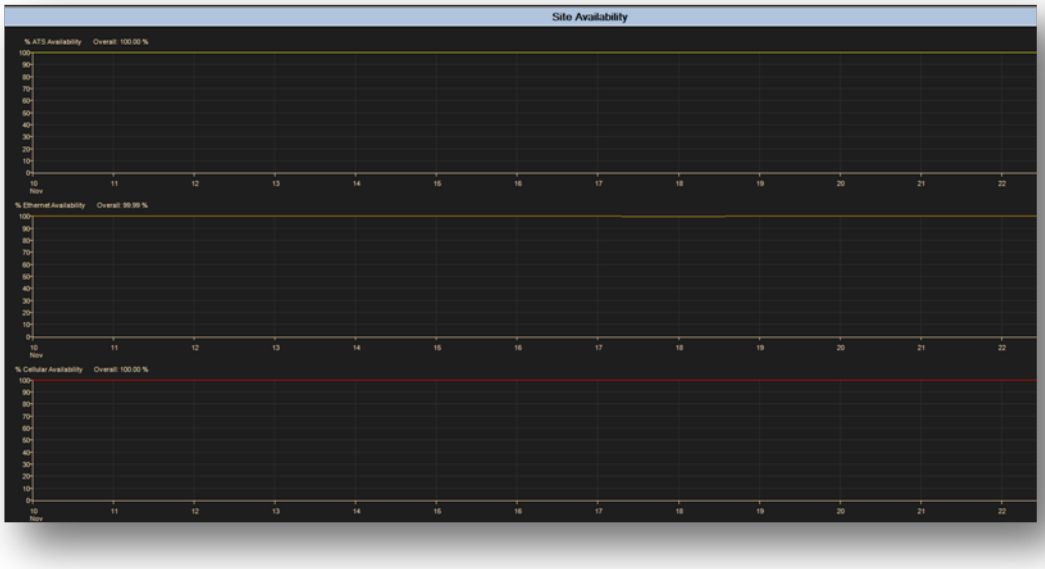
Statistics Period shows the period over which the Availability and Interface/Path Loss figures are calculated.

2.0 Availability

Users are able to view the times and dates of failures in a graphical format through the availability options of Command Centre.

Users can either availbility of a particular site either as '*Availability %*' or '*Availability Daily'*

'Availability %' displays a cumulative graph of the availability of the ATS as a whole and each of the configured paths individually.

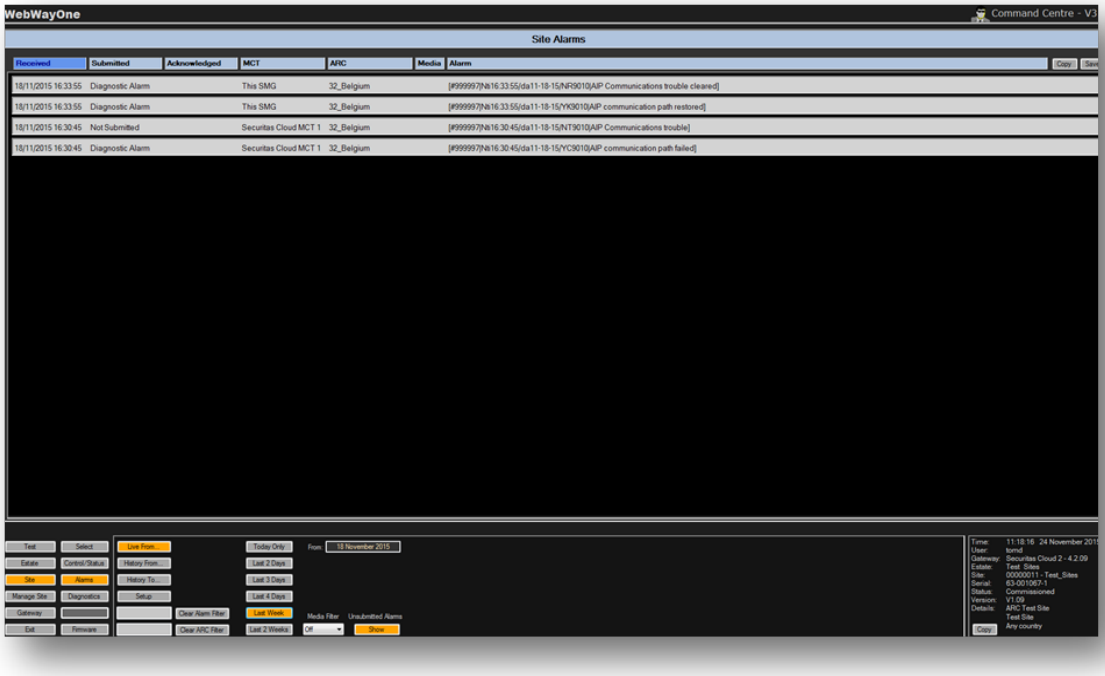


'*Avail. Daily'* provides a user friendly line graph with failures / recovery displayed more prominently as paths are recorded as either in an 'OK' (working) state or a 'fail' state. Hovering the mouse over a particular fail / restore (change of state) will display the time and date at which the path changed state.

3.0 Alarms

Command Centre can show the live alarms for the Current Site, displaying new alarms (by default) at the top of the screen as they occur. The latest alarm is shown at the top (although as usual, the column headers can be selected to change the sort column and order of the display).

To view live alarms from the Current Site the [Live From…] button in the [Site][Alarms] menu must be enabled.



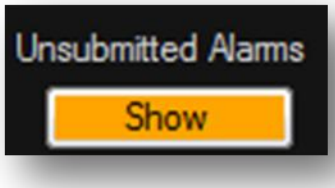
The live alarm list shows the alarms from today only by default. To view live alarms for up to two weeks ago, simply select the appropriate button.

As well as showing live alarms, Command Centre can also show Alarm history from the Current Site. Live alarms will not be shown in the Alarm History menus. However, if alarms arrive and either Alarm Clearing or Alarm Sound is enabled, the Live Alarm Menu will be automatically selected.

There are two ways of viewing alarm history:

- From a given date for a given period
- For a given period up to a given date

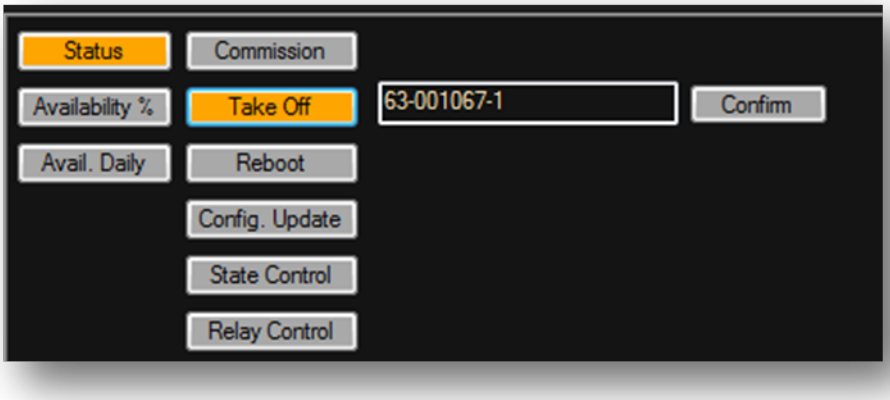
Some alarms which are delivered to the MCT are not passed the to the ARC. To view all alarm events (including diagnostic alarms and alarms held by Smart Reporting) click the [Show] button of Unsubmitted Alarms.



4.0 Commissioning - Take On / Take Off

A Site may created before the serial number of the board is known. When the board is on Site and is installed, it must be associated with the Site details on the Gateway before it can be Commissioned. This process is known as 'Taking-On' the Site. To take on the Site, from the Site Modify Menu:

- Select [Status] submenu
- Select [Take On/Take Off] menu. If serial number is already allocated then users will be unable to 'Take On' an additional serial number before 'Take Off' of the existing serial number.
- Enter the Serial Number and press the [Take On / Take Off] button
- The success or failure of the process will be confirmed.



Possible failures might be:

- Incorrect format of serial number.
- Serial number is already taken on. Each serial number can only be associated with one site on the gateway.
- Serial number is not known by the Gateway.

'Take Off' is the same process in reverse. This removes the board /site allocation and allows for a different board to be associated with the site.

5.0 Configuration Updates / Modifying Sites

If a working, communicating Site has had a change in configuration or has only been partially configured on Site, it will require a full configuration update. There are two mechanisms available to send out a configuration update as shown in the menu.

5.1 Updating Configuration Immediately

To make the Gateway send configuration to the Communicator immediately press the [Now] button.

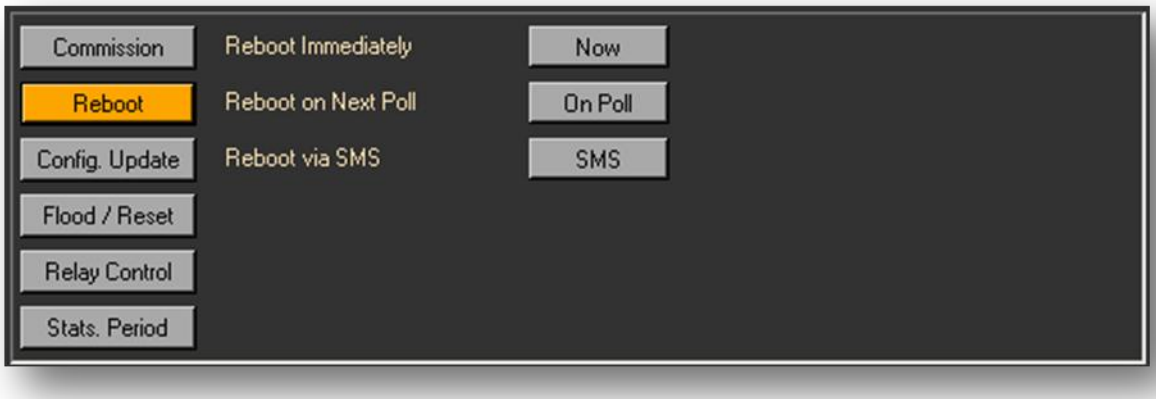
5.2 Updating Configuration on Next Poll

To make the Gateway send configuration to the Communicator the next time it polls in press the [On Poll] button.

Once the SPT has successfully been updated then the 'Last Config Update' value of the 'Site History' panel will update. In most cases the site will need a reboot to apply any configuration changes to the SPT into its working state.

6.0 Reboot Site Function

If the Communicator on a Site is to be rebooted (effectively restarting the software as if its power had been cycled off and on again), there are three choices available depending on the current state of the unit. Selecting the [Reboot] submenu shows the three choices.



Reboot Immediately

This makes MCT attempt to contact the SPT immediately with a command to make it restart. For units with an operating Ethernet interface, this is the fastest way to reboot it. Simply press the [Now] button.

For units which have GPRS as the Primary interface (or Ethernet units who's Ethernet interface is not working or configured properly) this will result in the Gateway attempting to force the unit to call back in on GPRS by sending it an encrypted SMS message. This mechanism normally works well but may take some time – if the unit is polling correctly it may be better to use the "Reboot on Next Poll" mechanism.

Reboot on Next Poll
This mechanism makes the MCT queue the reboot request for the Site until the Site next calls in with an active poll. To do this press the [On Poll] button.

This mechanism works on any interface but is aimed specifically at the units which have GPRS as their Primary interface. The reason for this is that GPRS is not normally treated as a permanently-on-line interface (like Ethernet is) and normally requires the Communicator to initiate all communications.

Reboot via SMS
This rebooting mechanism can be considered as a last resort if the two message-oriented mechanisms do not work. On receipt of the request to reboot a Site, the Gateway will send an SMS message to the unit directly. If the SMS is received the unit will immediately reboot. To do this press the [SMS] button

7.0 Firmware

The WebWayOne Development will periodically release new firmware for the WebWayOne SPT. This firmware can be applied remotely to the device via the WebWayOne infrastructure provided the device has a functional path and is connected onto the WebWayOne platform.

'V' versions of firmware are full release versions of firmware upgrades which have been tested and released for application to WebWayOne SPTs in the field. 'X' versions of firmware are test-versions of firmware which should not be uploaded to any units in the field without consultation with WebWayOne technical personnel.

Firmware can be upgraded and can also be downgraded. Any 'upload' of firmware from the MCT to an SPT will remain in the WebWayOne SPT until it takes a forced reboot from the Command Centre platform. If the SPT reboots for any other reason after the download of firmware then the software is deleted from the SPTs flash memory and is not applied. The download process will need to be restarted.

8.0 Managing Users

It is the responsibility of the ARC to manage User access to their MCT through the Command Centre platform. The addition of new users should be carried out by a nominated person at the ARC. WebWayOne will maintain a number of 'superuser' User accounts on the MCT in the Command Centre to allow for WebWay Technical to be able to access and assist. WebWay Technical will remove users at the request of the ARC.

For easier user management it is recommended that all user logins should be the email address of the user.

Further information on User Account Management can be obtained either through WebWay Technical Support or through your WebWay Sales Representative.

9.0 Software Updates

WebWayOne will periodically release updates to this software package. Legacy versions of this software should continue to work however Support for Legacy versions is discontinued upon release of a more current version. Where practical the first step in troubleshooting issues with Command Centre should involve upgrading the software to the latest release version.

More information can be obtained at WebWayWorld.com or through your WebWay Sales Representative.