Omni

USER INSTRUCTIONS

Proprietary

Trademark

The term ‘Innotech’ used in this manual is a trademark of Mass Electronics Pty Ltd trading as Innotech Control Systems Australia.

'Microsoft' and 'Windows' are registered trademarks of Microsoft Corporation in the United States and other countries.

'Android' is a trademark of Google Inc. The Android robot can be used, reproduced and modified freely and is licensed under the terms of the Creative Commons 3.0 Attribution License.

'Apple' is a trademark of Apple Inc., registered in the U.S. and other countries. Third Party products which are compatible with Apple products or technology may use Apple related word marks such as but not restricted to 'Apple', 'Macintosh' and 'iMac'.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license by Apple Inc.

Disclaimer

While great efforts have been made to assure the accuracy and clarity of this document, Mass Electronics Pty Ltd assumes no liability resulting from any omissions in this document, or from misuse of the information obtained herein. The information in this document has been carefully checked and is believed to be entirely reliable with all of the necessary information included. Mass Electronics Pty Ltd reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and make changes from time to time in content hereof with no obligation to notify any persons of revisions or changes. Mass Electronics Pty Ltd does not assume any liability arising out of the application or any use of any product or circuit described herein; neither does it convey licence under its patent rights or the rights of others.

Document Management

Document Title: Omni User Instructions

Revision History

Version Number	Date	Summary of Changes
1.0	September 2017	Document first edition
1.1	August 2018	Add new settings (Modbus, ISS), update access level Permissions tables and web server screens, update Device Info screens.
1.2	February 2020	Updated Web server screens and information for new interface. Add custom access levels.

Contents

Contents (Continued)

HMI Menus

Contents (Continued)

Omni Web Server

Omni

USER INSTRUCTIONS

1 Preliminary Information

INNOTECH®

1-1 Overview

This manual is designed to provide the customer with complete and comprehensive documentation for the Omni Controller. This document contains detailed procedures for HMI (Human Machine Interface / Front Panel) and on-board web server operation of the BEMS (Building and Energy Management System) Controller.

1-1.1 About this Document

This manual is intended to provide the user with complete and easy-to-follow instructions for HMI operation of the Omni BEMS Controller from the front panel and web server. In preparing these instructions, Innotech assumed that the typical operator is not necessarily familiar with the operation of computer systems. For this reason, operating instructions and procedures are presented at a technically basic level and as clearly as possible.

Each Controller is designed to be set-up to its own application requirements and since each customer's application is different, no two units have identical step-by-step operating procedures. However, the Omni BEMS Controller is user-friendly and operation is simple once the necessary operational information has been explained. The operating procedures in this manual are based on typical operating scenarios.

References made throughout this manual to "Omni", "Controller" or "BEMS Controller" refer to all models of the Omni BEMS Controller except where specified.

1-1.2 Scope of this Document

This technical manual has multiple sections:

Table 1-1: Manual Scope

Chapter	Description
Chapter 1 - Preliminary Information	Chapter 1 provides related information of a general nature. This chapter also contains a brief description of the Omni Controllers.
Chapter 2 - Operation	Chapter 2 provides information for configuring an Omni Controller.
Chapter 3 - HMI Menus	Chapter 3 provides an overview of the various HMI screens.
Chapter 4 - Omni Web Server	Chapter 4 provides information about the Omni web server.

1-1.3 Information Icons

Throughout this manual, icons are used to illustrate important notes. Examples are shown below.

*These notices provide extra information. It is non-critical information but **should be read**.*

IMPORTANT

*These notices contain information about the software that **must be done** before proceeding further to ensure success.*

1-2 Description of the Omni BEMS Controller

The Innotech Omni BEMS Controller is the main component of the Omni System. Other components of the system, such as expansion devices are passive units with no front panel operation associated with them.

C40D Controller shown with parts labels. The C20 model is physically the same as the C40 but with less UIOs.

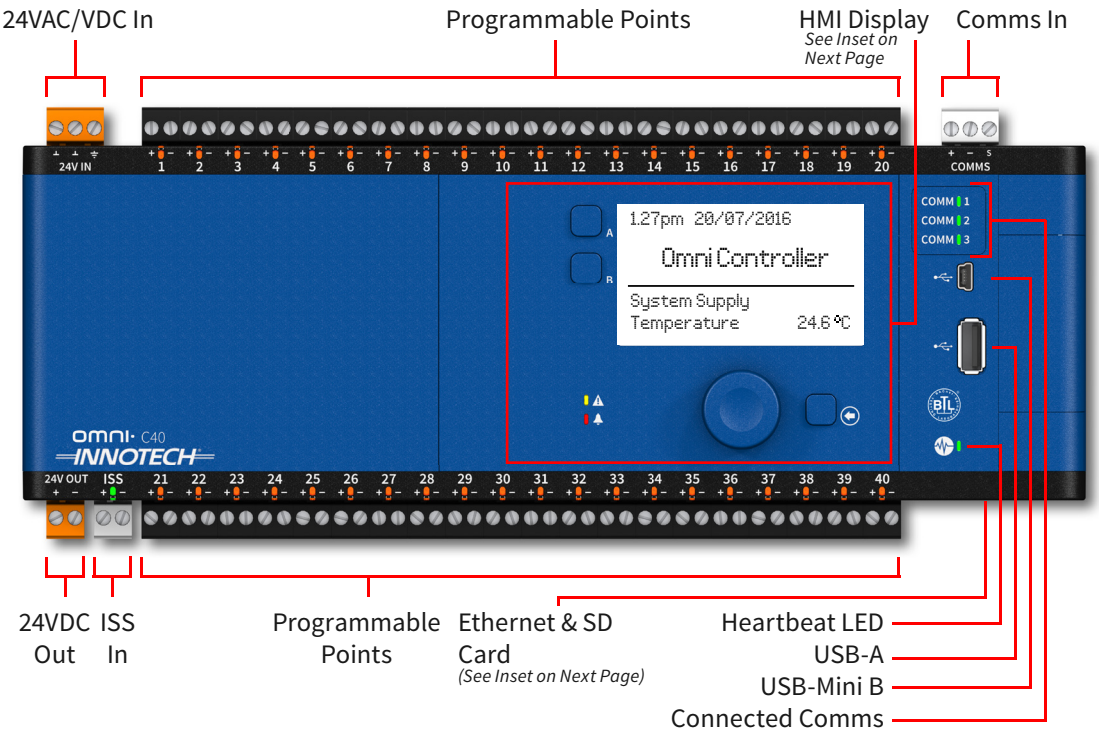


Figure 1-1: Omni C40D BEMS Controller

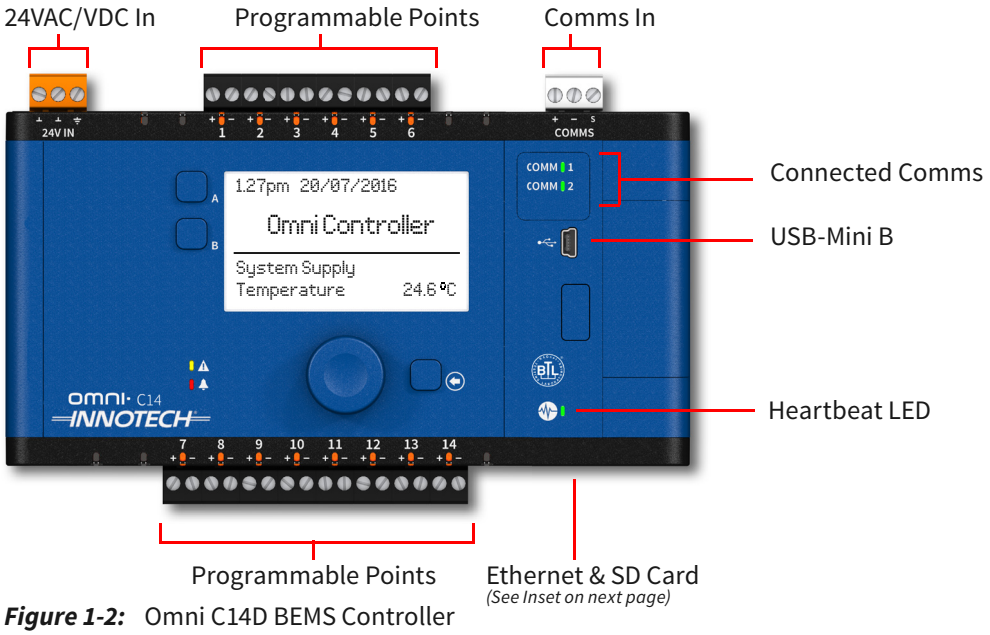


Figure 1-2: Omni C14D BEMS Controller

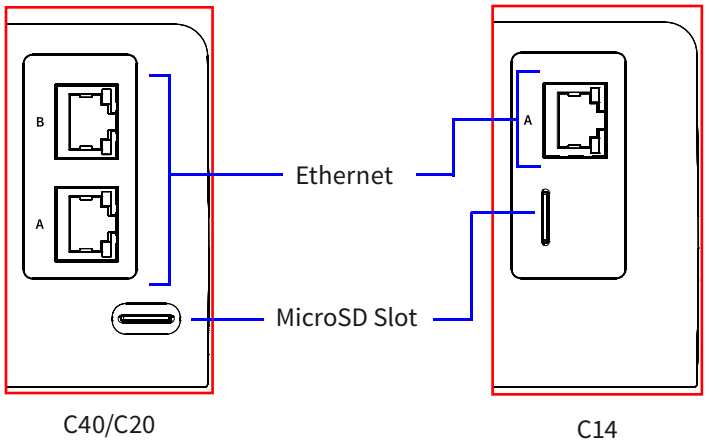


Figure 1-4: Inset: Omni Controller Ethernet and Micro SD Card slot (on underside)

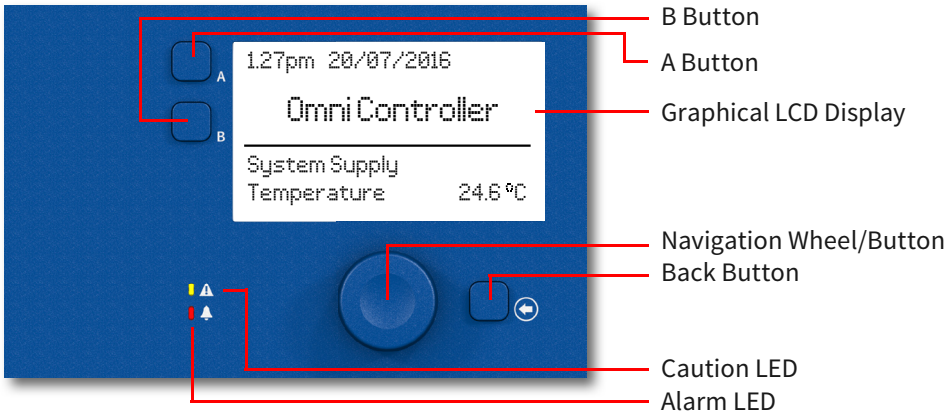


Figure 1-3: Inset: Omni OHM01 HMI Display (all models)

The retrofit display (OMH01) is the same for all Omni controllers. Omni models with a display have 'D' in the model name (C40D, C20D, C14D). Non-display models can be fitted with the retrofit display.

The Omni U10 Expansion Device, expands the input and output capabilities of the controller. The U10 expands the amount of programmable points (UI/O) by 10. Multiple U10 Expansion Devices can be used to expand the available UI/Os. Once configured, no operator action is required for the expansion device. The table below shows the expansion capabilities of each controller.

Table 1-2: Omni U10 Expander Limit

Omni Model	Expander Maximum
C40/C40D	5
C20/C20D	5
C14/C14D	Not Supported

When more than five U10 devices are connected, the maximum speed will drop by 50%.

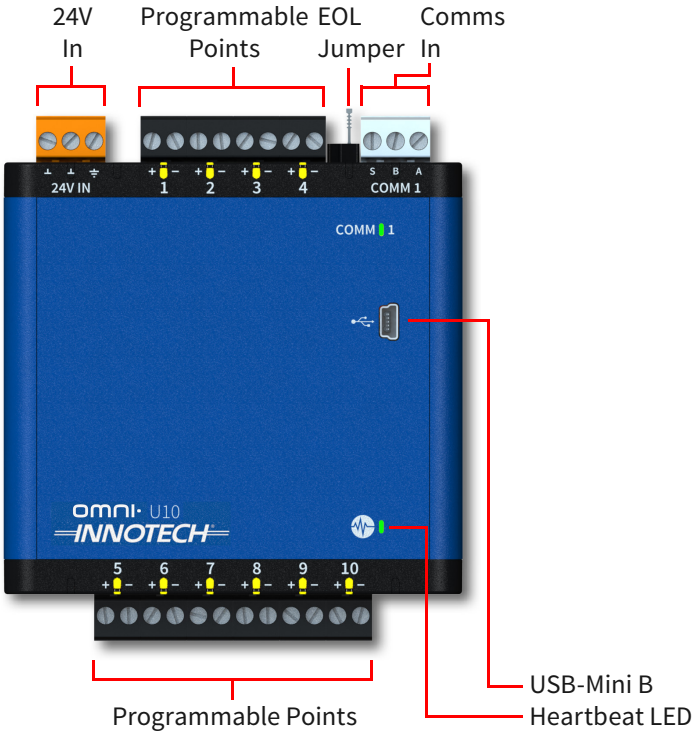


Figure 1-5: Omni U10 Expansion Device

1-2.1 What It Does

The Controller is designed mainly for automatic control of large-scale heating, ventilation and air conditioning (HVAC) systems; operator action is mainly limited to monitoring tasks. The Digital Controller replaces older systems in which multiple analogue controllers were used for control of large HVAC systems.

The Omni Controller can operate as a standalone device, while more complex installations can use multiple controllers sharing data between controllers and a computer. Communications among the Omni BEMS Controllers is a via an Ethernet backbone with the option of RS485 networks for Innotech backward compatibility and other protocols such as BACnet MS/TP.

Omni controllers and remote expansion modules have fully Programmable Points, which can all be used as either universal inputs or universal outputs (UI/O).

For the purposes of this manual, the terms "Programmable Points" and "Universal Inputs/Outputs (UI/O)" are interchangeable and are defined in the same way as "points which can be programmed as Inputs or Outputs".

1-2.2 Focus Configuration Software

Before being placed in service, the BEMS Controller is “tailored” to its intended application by the Innotech Focus Software. The user can design the Controller's operating program using the configuration software. The designer uses the software to develop a functional block diagram of the entire mechanical system interconnected with the Controller and containing all necessary operating values. When the design is completed, the software user loads the new configuration into the Controller’s ROM where it stays resident until such time as reprogramming may be necessary.

In addition to establishing the specific operating configuration of the system, the Focus Configuration Software also sets up specific functions which can be monitored, used and/or changed by the Digital Controller operator, such as:

- System Operating Schedules, daily, weekly and yearly
- Access Codes defining what functions/data are available to an operator
- Organisation of monitoring data into logical groups (pages) for presentation to an operator
- Organisation of System Pages containing data of interest to supervisory personnel
- Audible or visual alarms of system and processing faults
- Process values (setpoints)

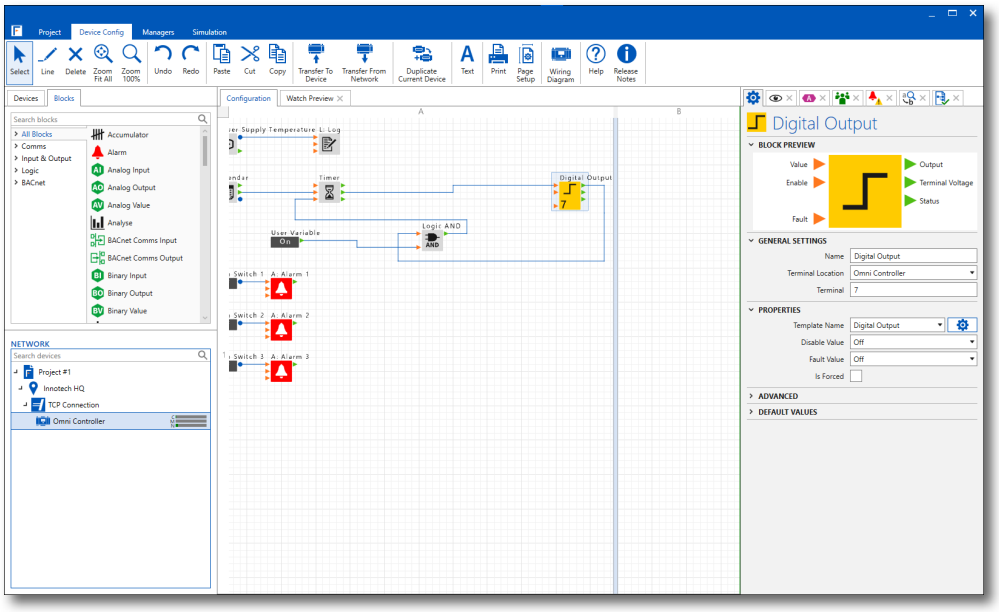


Figure 1-6: Focus Configuration Software

This page has been left intentionally blank.

Omni

USER INSTRUCTIONS

2 Operation

INNOTECH®

2-1 Overview

Omni BEMS Controllers feature a state of the art processor and are designed for versatility and ease of use. Using the Focus configuration software, these controllers can be easily configured for customer specific applications. The Omni operating procedure may vary for each controller depending on your configuration.

A user friendly interface and ease of operation is common among all Omni controllers. This section of the document provides the following information to help you with the operation of Omni BEMS Controller.

Please note the screen shots used throughout this document are taken from a typical Omni Controller. Any differences among the various controllers will be detailed accordingly.

Table 2-1: Operation Section Scope

Section	Title	Description
2-1	Overview	Description of the Omni BEMS Controller.
2-2	Omni Start-up	Description of the Omni start-up process.
2-3	Menu Structure	Description of the Omni menu structure.
2-4	Controls and Indicators	Description of the parts of the Omni.

2-2 Omni Start-up

The Omni BEMS Controller is normally powered at installation and then left powered indefinitely; therefore the operator would not normally perform start-up procedures. However, maintenance actions or a power failure could require the unit to be restarted.

After applying power to the Controller, the Omni logo will be displayed on the LCD and the Heartbeat LED will be orange. After the Omni has finished its boot sequence, the home screen will be displayed and the Heartbeat LED will change to green.

2-3 Menu Structure

2-3.1 Menu Overview

This section of the document provides information about the basic structure of the menu screens for the Omni Controllers. Information on general navigation through the various menu screens is also provided in this section. See the HMI Menus section for further details.

2-3.2 Structure of Menus

The LCD screen is the primary method by which the user interacts with the HMI (Human Machine Interface) on the controller.

This section is applicable only to Omni Controllers with an onboard HMI or Controllers using an external Omni HMI interface.

A representation of the structure of menus within an Omni controller is shown below. More detailed information on the menu structure and LED indicators is contained elsewhere in this section. A detailed description of the menus for the different models of Omni controllers follows in subsequent sections.

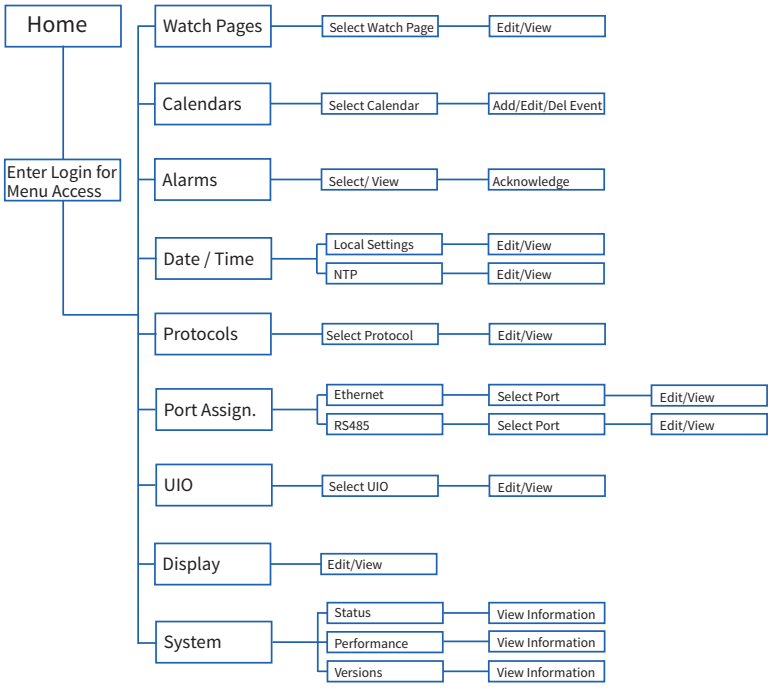
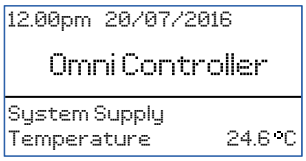


Figure 2-1: HMI Menu Flow Chart

2-4 Controls and Indicators

2-4.1 Liquid Crystal Display (LCD)



The LCD (where installed) is the main indicator component of the Digital Controller; it is a 128x64 pixel graphical display.

The LCD contains an automatic white backlight feature that enhances the visibility of the LCD presentation. The backlight turns on automatically whenever any button is pressed or navigation wheel is pressed or moved. The backlight will turn off without user interaction after the time specified in the Display Settings.

2-4.2 Navigation Wheel

The navigation wheel is used to move around the menu structure of the Omni controllers. Moving the wheel left or right will scroll up or down in a menu or change a selected value.

The navigation wheel can also be pressed to confirm settings or enter a menu.

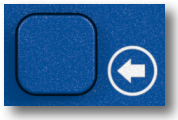
2-4.3 A Button

The 'A' button is used to show the Watch Pages menu (when at the Home screen). Login is required.

2-4.4 B Button

The 'B' button is used to show the Notifications (Alarms) screen (when at the Home screen). Login is required.

2-4.5 Back Button

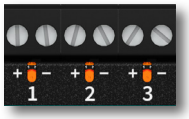


The back button is used for navigating back to the previous screen. Hold the button for 2 seconds at any screen to return to the home page (as shown above).

2-4.6 Heartbeat LED

The Heartbeat LED is located at the bottom right of the Controller below the USB port(s) and among other things indicates that primary operating power is applied to the Digital Controller when lit. A green LED will flash on and off (heartbeat) to indicate that the Controller is "alive".

2-4.7 Progammable Point (UI/O) LEDs

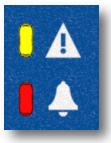


When used as a digital input or output, the LED will light orange. A flashing orange LED indicates that there is a problem.

2-4.8 Comms LEDs

When connected, the LED for the connected Comm will light. A flickering LED indicates that data is being sent or received.

2-4.9 Alarms & Warnings



Alarms on Omni Controllers can be programmed to notify the operator when a certain event occurs. These can be utilised to notify you of any critical events that are being monitored. Alarms can be configured in the Innotech Focus software.

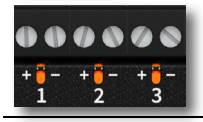
If an alarm or warning is active, the associated LED will light on the controller.

Alarms can either appear constantly on the controller LCD or scroll between alarms every 5 seconds if more than one alarm is triggered. How these are displayed will depend on how the alarms have been configured.

2-4.10 Omni Indicator Identification

The table below shows the different LED states that may be seen on your Omni device.

Table 2-2: Omni LED Indicators

LED		LED Indication	What It Means
	Heartbeat	Green Flash	Controller status OK
		Static Orange & Green	Controller shows orange and green during booting
		Red Flash	Controller fault
		Orange Flash	Shown when upgrading, during config transfer, initialising etc.
		Orange Slow Flash	Power fail - controller power is below limit for normal operation
	HMI - Alarm	Red	Alarm is active
	HMI - Warning	Orange	Warning is active
	Programmable Points	Orange	Connected as a digital input or output
		Orange Flash	Programmable point fault
	Comms	Red	Data transmit
		Green	Data receive
		Orange	The combination of the red and green LEDs can appear orange due to the processing speed
	ISS Input	Green	Connected device

This page has been left intentionally blank.

Omni

USER INSTRUCTIONS

3 HMI Menus

INNOTECH®

3-1 Overview

This section of the document provides detailed information about the structure and functionality of the HMI for the Omni BEMS Controllers. A brief description of each menu and information on configuring various parameters is also provided in this section.

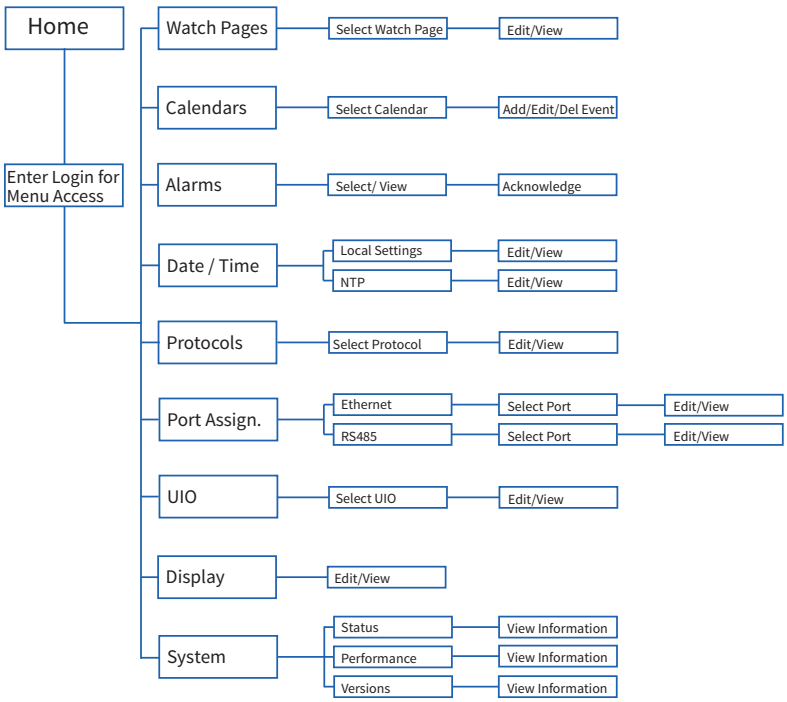


Figure 3-1: HMI Menu Flow Chart

Please note the screenshots used throughout this document are taken from a typical Omni BEMS Controller with HMI. Any differences among the various controllers will be detailed accordingly.

3-1.1 Icons used in this section

The table below shows lists the icons used in this manual and the related button on the Omni HMI.

Table 3-1: HMI Button Icons

Icon	HMI Button	Description
A	'A' Button	At the home screen, press to show the Watch page screen.
B	'B' Button	At the home screen, press to view the Notifications screen.
	Back Button	Press Back to cancel value editing and to go back to the previous screen. Hold the Back button for 2 seconds at any screen to return to the home screen.
	Wheel Scroll	Scroll the wheel left or right to navigate menus and screens. It is also used to change values.
	Wheel Press	Press the wheel button to enter a menu screen or change a value to edit mode.

3-1.2 HMI Access

The user's access level also determines which HMI menus are visible/accessible.

Table 3-2: HMI Access

Access Level	Menus								
	Watch Pages	Calendar	Alarms	Date/ Time	Protocols	Port Assign.	UIO	Display	System
Adjuster	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Administrator	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Commissioner	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Engineer	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Facility Manager	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Observer	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write
Key	Green - Menu Visible (Access Available) Red - Menu Visible (Access Unavailable) Grey - Menu Not Visible (Access Unavailable)								

3-2 Main Menu

3-2.1 Overview

This section of the document provides information on navigating the HMI on the Omni BEMS Controller.

Turn the navigation wheel left or right to move the selection up or down on the HMI. The menu navigation is not continuous and when the top or bottom is reached, it does not loop around. Eg: When on menu 9/9, continuing to scroll will not move to 1/9.

Press the centre of the navigation wheel to select the menu. The first screen seen will be the Login screen.

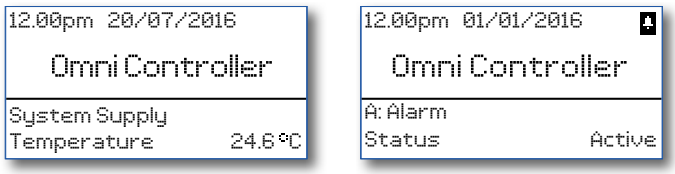
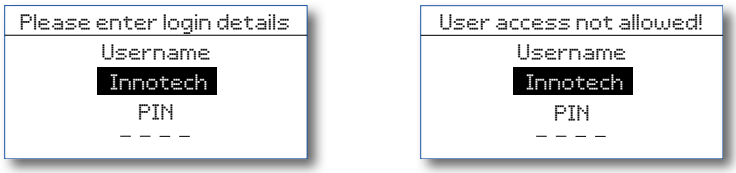


Figure 3-2: Examples of the LCD Home Screen

All screens in this section are indicative only.

3-2.2 Login Screen

Use the navigation wheel to select and enter your login to access the HMI menus.



If programmed, you will be required to login if you press the A or B button. If your access level does not allow viewing of these pages, access will be denied.

Figure 3-3: HMI Login Screen

3-2.3 Watch Pages

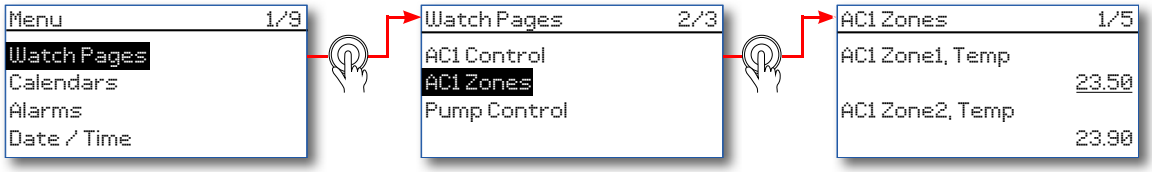


Figure 3-4: Watch Page Menu Item & Watches Menu

This section provides information about the use of Flash and Watch pages within the Omni controller.

Each page typically contains data to be monitored by the user (hence the term Watch Page) and process values, such as controller setpoints, which may be viewed and edited.

The content of each page is normally arranged in a logical manner; for example, all the data on Watch Page 6 might represent parameters for Heating and Cooling Zone 6. The arrangement and content of each Watch Page and level of access for individual users is programmed by the Focus Configuration Software.

3-2.3.1 Watches & Watch Pages

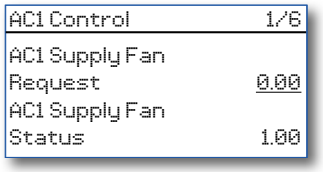


Figure 3-5: Watch Page View

When the device is first configured by the Focus Configuration software, it is possible to place the current value of a node of any block within the configuration on a Watch page. These Watch pages allow users to quickly view important I/O and block values on specified watch pages. If an item has an underline, this indicates the cursor position in the screen and signifies that the item is not editable.

3-2.3.2 Editable Watches

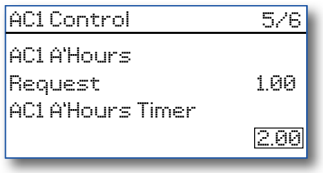


Figure 3-6: Editable Watch Value

Watch pages may also be configured with watches that are editable by the user. These may refer to temperature setpoints or other adjustable user variables. An adjustable watch parameter can be edited directly on the controller. If an item's value is in a box, this indicates the cursor position in the screen and that the item is editable.
To edit the item, press the Navigation wheel button, rotate the wheel to edit the value, press the button to save. To cancel, press the back button before saving the value.

3-2.4 Flash Pages

Omni controllers also contain a specific page known as a Flash page. Watches assigned to this page are displayed at the bottom of the Home Page at three second intervals. After start-up the first Flash Watch is displayed for three seconds, followed by the next Flash Watch for three seconds, and so on until the cycle is repeated. You can also rotate the navigation wheel to move through the watches.

Alarms that have the Display option marked in the block are sent to the display as a flash (if programmed). Alarm annunciation has priority and overrides the flash page until all alarms are cleared.

The Flash Watch feature is especially useful for applications containing many watches; it allows you to easily monitor a range of specified watches without having to access a Watch Page and manually scroll through it.

3-2.5 Calendars

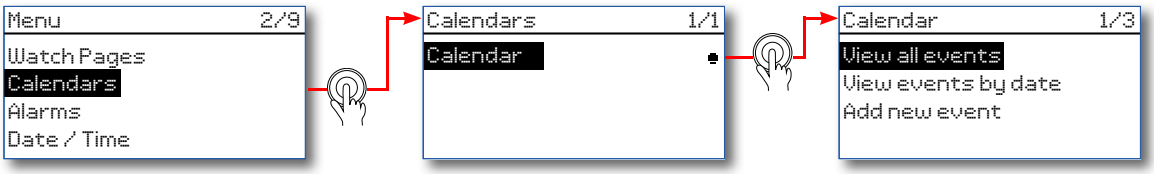


Figure 3-7: Calendar Menu Item

The Calendar menu is used for viewing and programming schedules on your Omni Controller. The circle next to the calendar indicates if events are currently active. Filled circle = active, unfilled circle = inactive.

3-2.5.1 Add a Calendar Event using the HMI

Select Add new event on the HMI to begin the creation of a new Calendar event. There are 9 menu options for creating a new event (the 10th option is Delete Event). Note: The event name cannot be changed on the HMI.

1. Recurrences - by default it is set to Repeat Never, selecting this line will open the recurring event options.
2. All Day - if you change this option to Yes, you cannot specify a start, stop time or duration.
3. Start Date - Select a start date for the event.
4. Start Time - Select a start time for the event.
5. Duration - The duration will be calulated automatically when a start and stop time is entered, you can also edit this option manually and the stop time will be recalculated accordingly.
6. Stop Date - Enter a stop date for the event.
7. Stop Time - Enter a stop time for the event.
8. Value - Select either ON or OFF to determine if the event should turn a configuration on or off when active.
9. Priority - Select the event priority. If events overlap, the priority will determine which event is active.
10. After you have finished editing, press the back button and select Yes to save the changes.

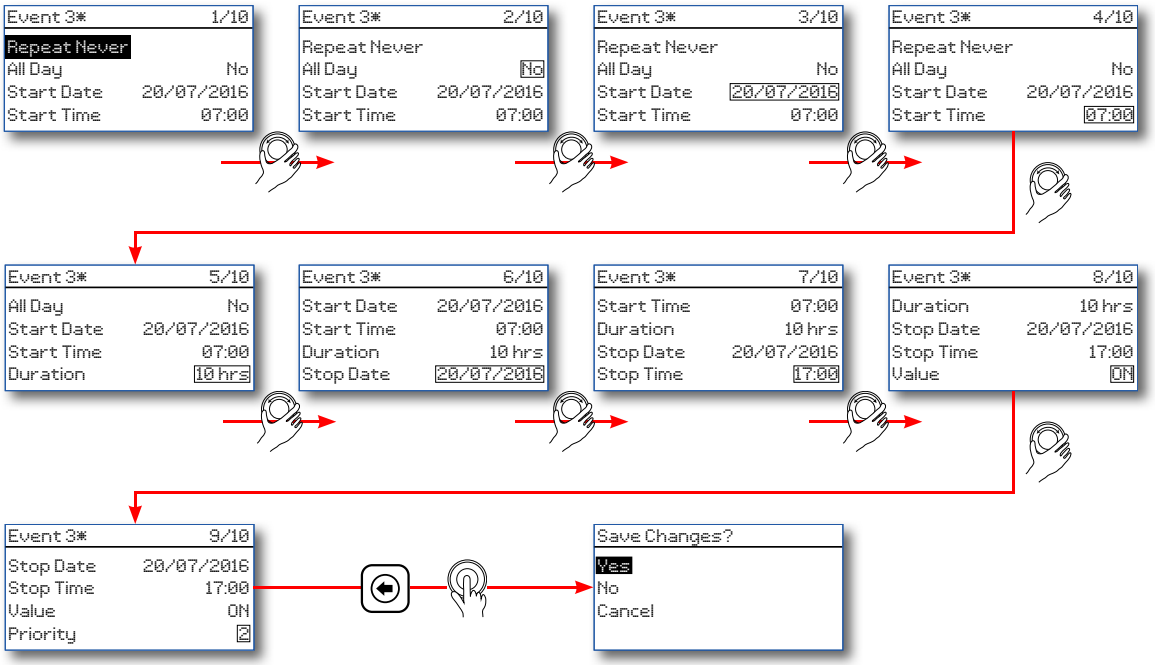


Figure 3-8: Calendar - Add Event

3-2.5.2 Add a Recurring Event

Recurrences by default are set to Repeat Never, select Repeat Never by pressing the navigation wheel to open the Recurrence Options.

1. Select using the navigation wheel and change between Never, Daily, Weekly, Monthly and Yearly.
2. Every - Select a frequency for the event.
3. End - Select a end option for the event. Select either By Date or After no. of events. Selecting one of these options will add an additional item to the menu to select a date or number of events.
4. After editing has been finished. Press the back button to return to the event. You will have to press the back button again and select Yes to save the changes to the event.

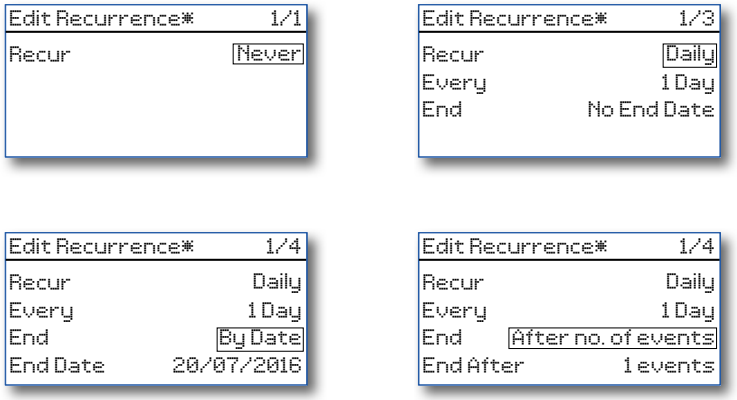


Figure 3-9: Calendar - Recurrence Options

3-2.5.3 Edit a Calendar Event on the HMI

Editing a calendar event is the same as creating an event. View an event to select and edit the event.

3-2.5.4 Delete a Calendar Event on the HMI

When editing an existing event, another option is added at the bottom for Delete Event.

1. Rotate the navigation wheel to Delete event and press the wheel.
2. Press the navigation wheel to delete the event.

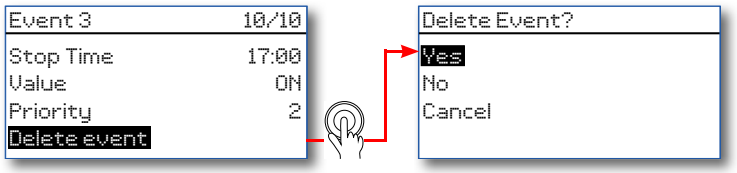


Figure 3-10: Calendar - Delete Event

3-2.5.5 View Calendar Events

Calendar events can be viewed by date or all can be viewed. In the event list a filled circle indicates that the event is active. Conversely, an unfilled circle indicate that the event is inactive. Recurrences are also visible in this view, [d] = daily, [w] = weekly etc.

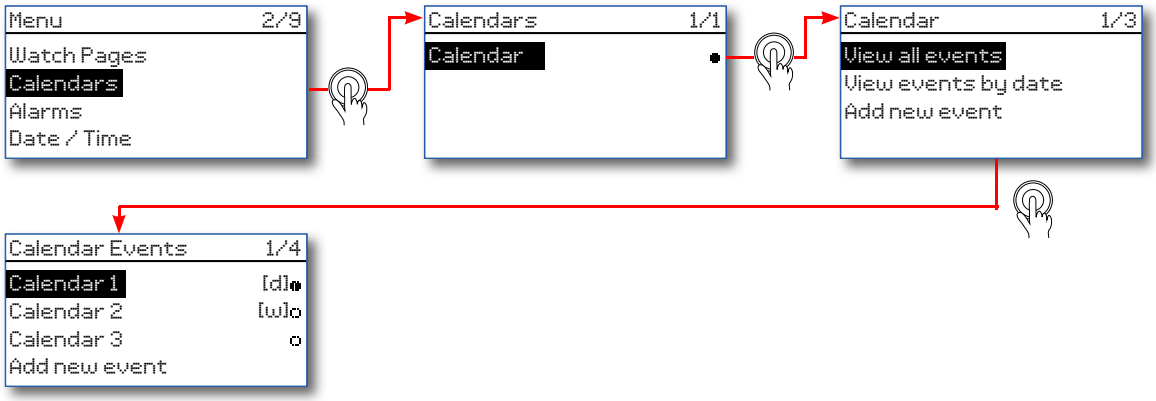


Figure 3-11: Calendar - View Events

3-2.6 Alarms

The Alarms screen shows the active alarms or warnings for your Omni system. Any active alarms will also show on the Omni home screen. Pressing the B Button at the home screen will show the Alarms screen after logging in (assuming you have access). Alarms can be reset from the HMI.

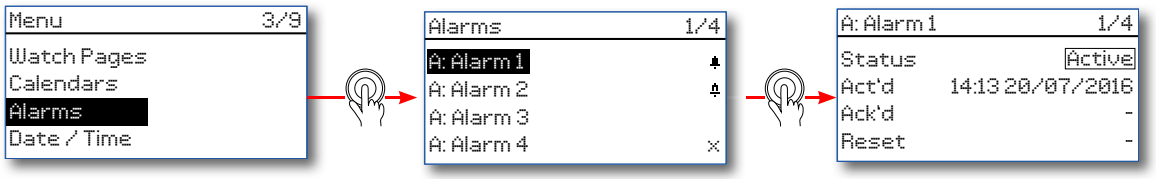


Figure 3-12: Alarms Page Menu Item & Example LCDs

There are four alarm states shown on the HMI. Filled in bell = active alarm, unfilled bell = alarm acknowledged, blank = alarm ok, x = alarm offline.

All alarms in the configuration will show on this screen. The list will be reordered automatically by priority: active, acknowledged, ok and offline.

3-2.6.1 Acknowledging Alarms

Use the wheel to select the alarm and press the navigation wheel button. Press the button when the Status is highlighted, press the wheel button when Yes is selected to acknowledge the alarm.

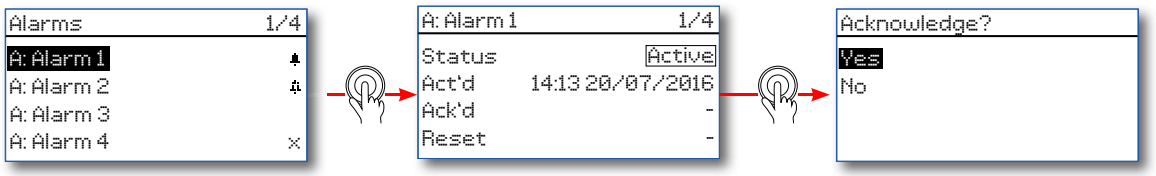


Figure 3-13: Alarm Acknowledgement

3-2.7 Date / Time

The Date/Time menu is for viewing and editing the Date and Time settings as well as the activating or deactivating the Network Time Protocol settings on your Omni device.

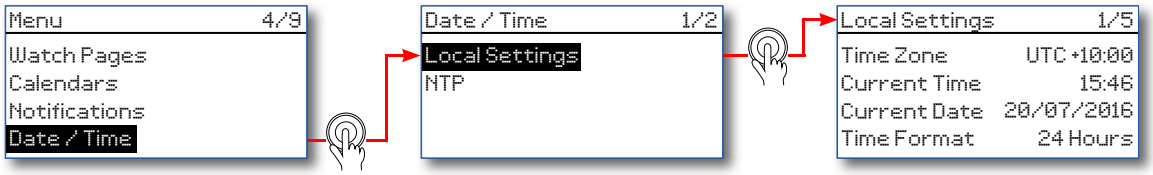


Figure 3-14: Date/Time Menu Item & Example LCDs

NTP can be enabled and disabled from the HMI, but the server settings cannot be modified. You must use the Omni Controller's on-board web server or Innotech Focus software.

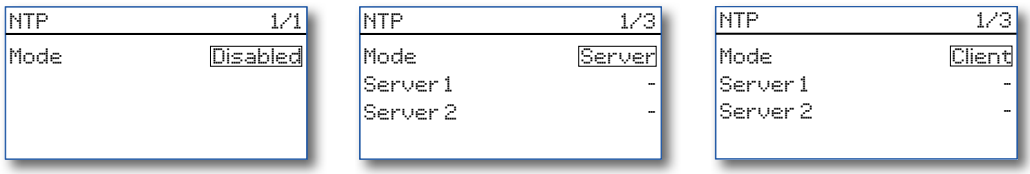


Figure 3-15: NTP Settings

3-2.8 Protocols

The Protocols menu is for viewing and editing the Protocol settings for the Omni Controller.

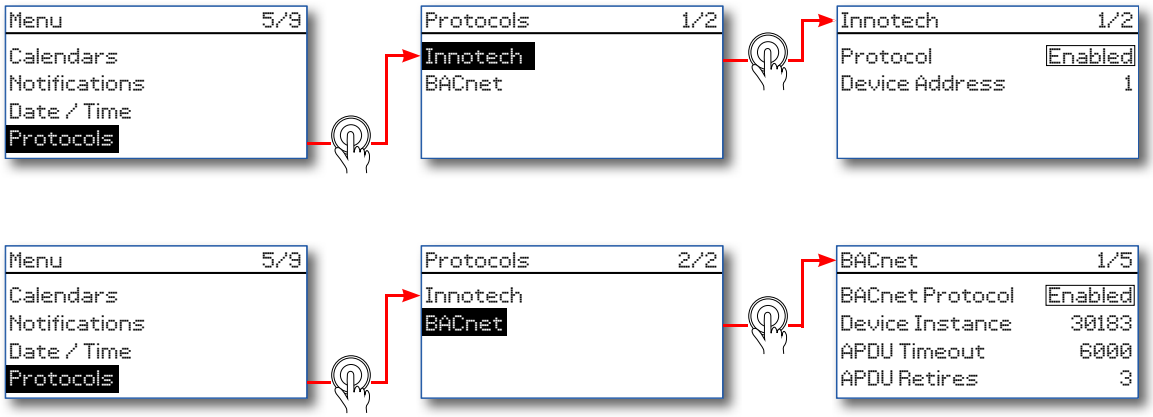


Figure 3-16: Protocols Menu Item & Example LCDs

3-2.9 Port Assignment

The Port Assignment menu is for viewing and editing the Port Assignment settings for the Omni Controller.

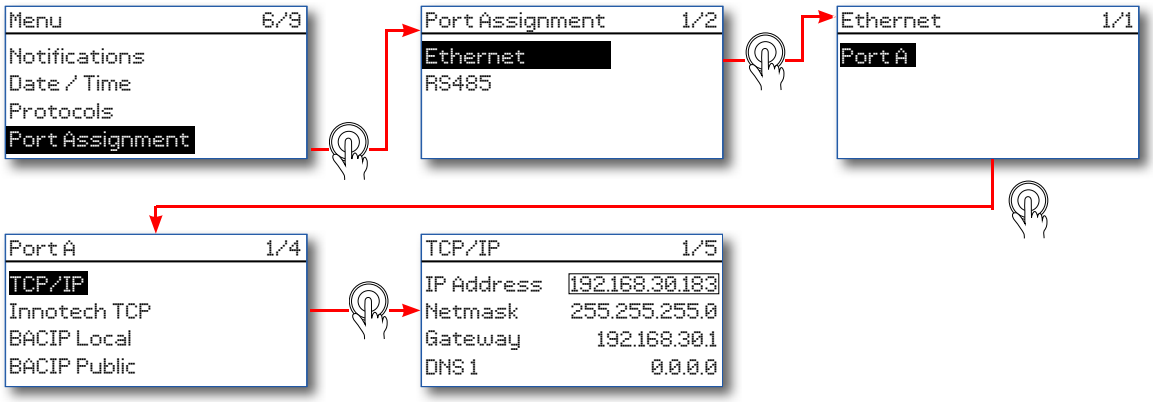


Figure 3-17: Port Assignment Menu Item & TCP/IP Example

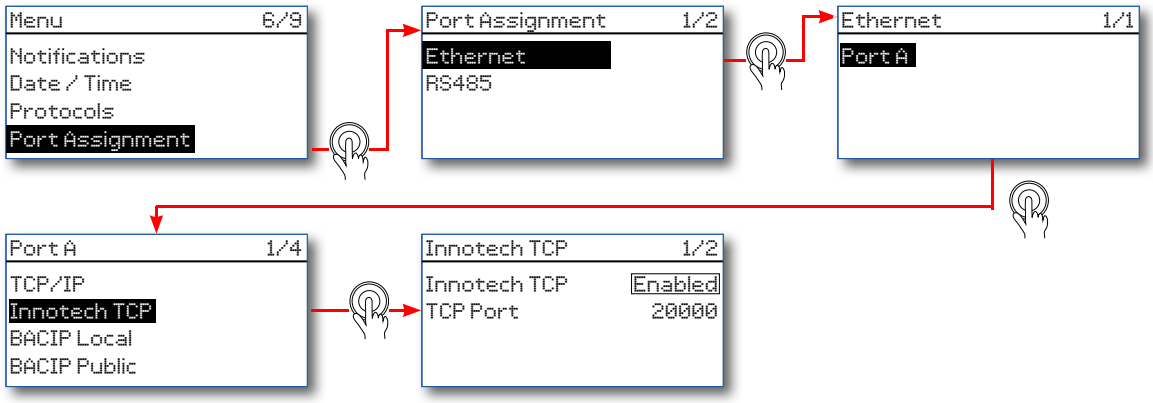


Figure 3-18: Port Assignment Menu Item & Innotech TCP Example

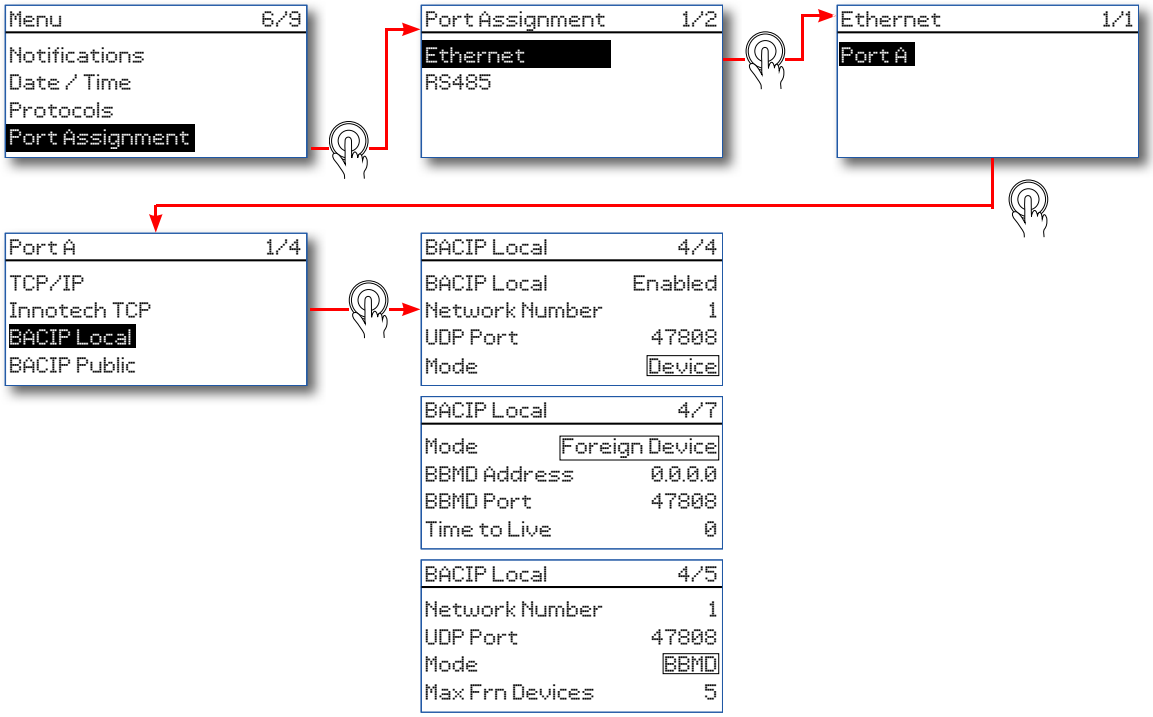


Figure 3-19: Port Assignment Menu Item & BACIP Local Modes

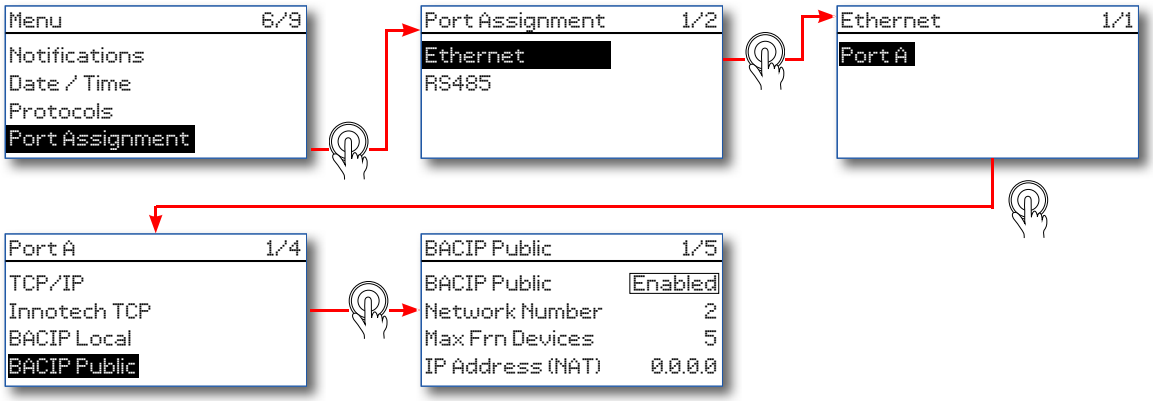


Figure 3-20: Port Assignment Menu Item & BACIP Public

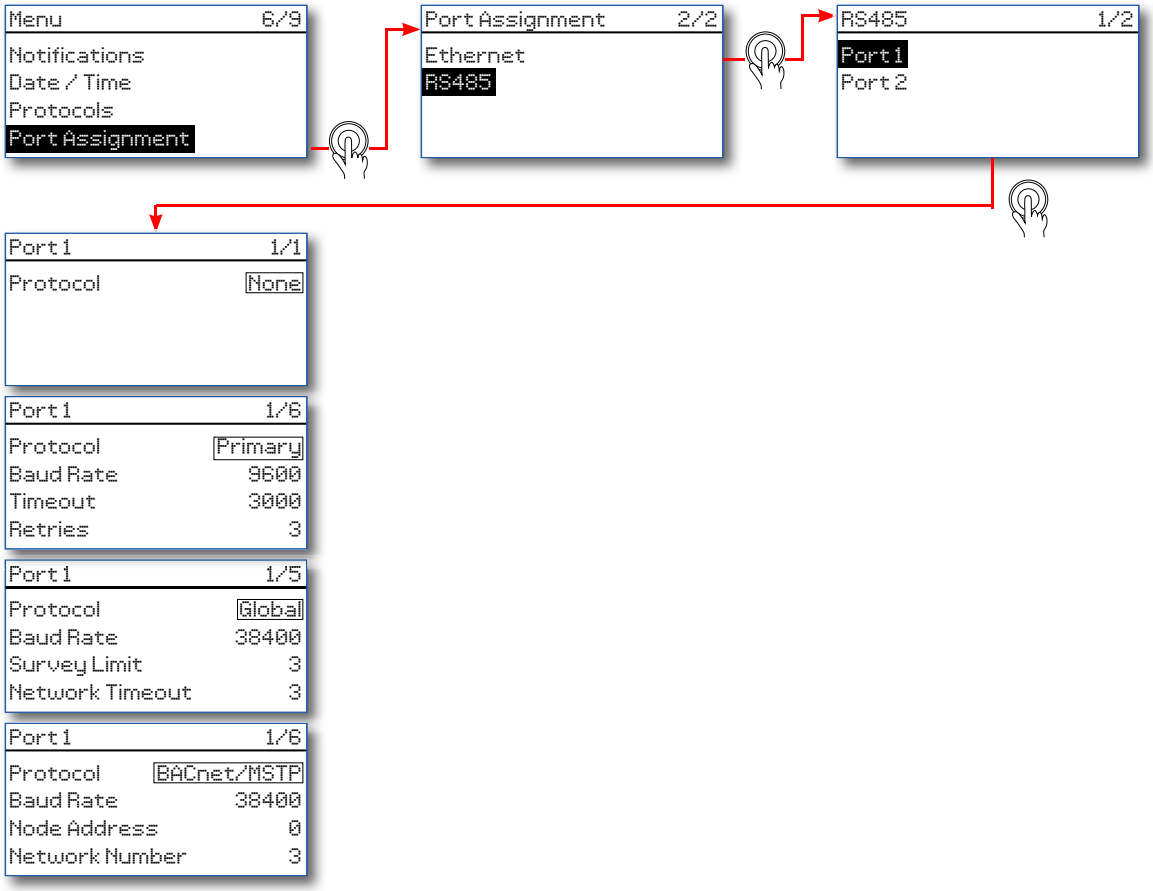


Figure 3-22: Port Assignment Menu Item & RS485 Options

3-2.10 UIO

The UIO menu is for viewing and editing UIO parameters. Only some parameters can be edited. Use the navigation wheel and wheel button to edit as required.

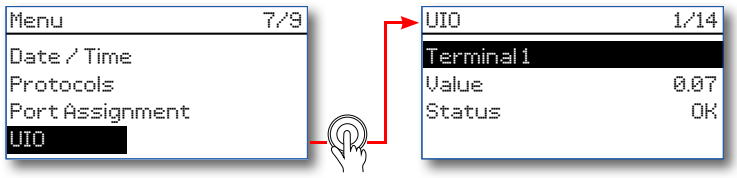


Figure 3-21: UIO Menu Item & Example LCD

3-2.11 Display

The Display menu is for editing the Session and Backlight Timeout settings for the HMI. The timeout can be set between 0 and 60 seconds.

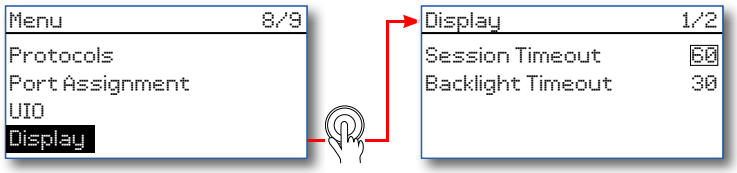


Figure 3-23: Display Menu Item & Example LCD

3-2.12 System

The System menu is for the viewing of the Omni controller's system voltages and temperatures. Rotate the wheel to view information about your Omni controller.

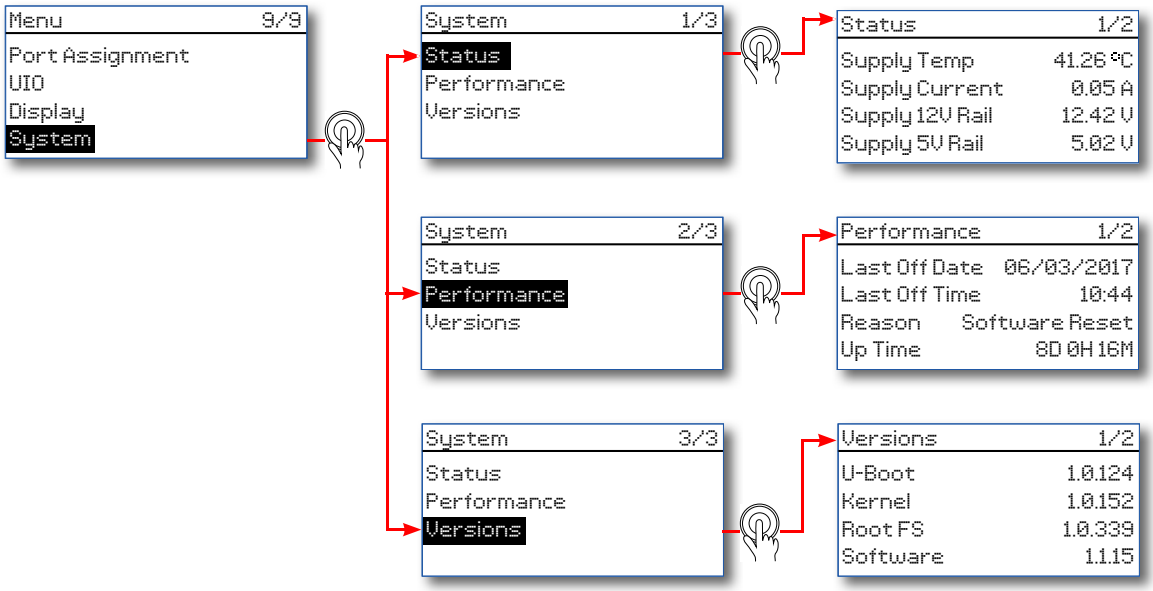


Figure 3-24: System Menu Item & Example LCDs

3-2.13 Editing Parameters using the HMI

Editing settings using the Omni HMI is a simple process. Follow the flow diagram for an overview of how to edit a parameter.

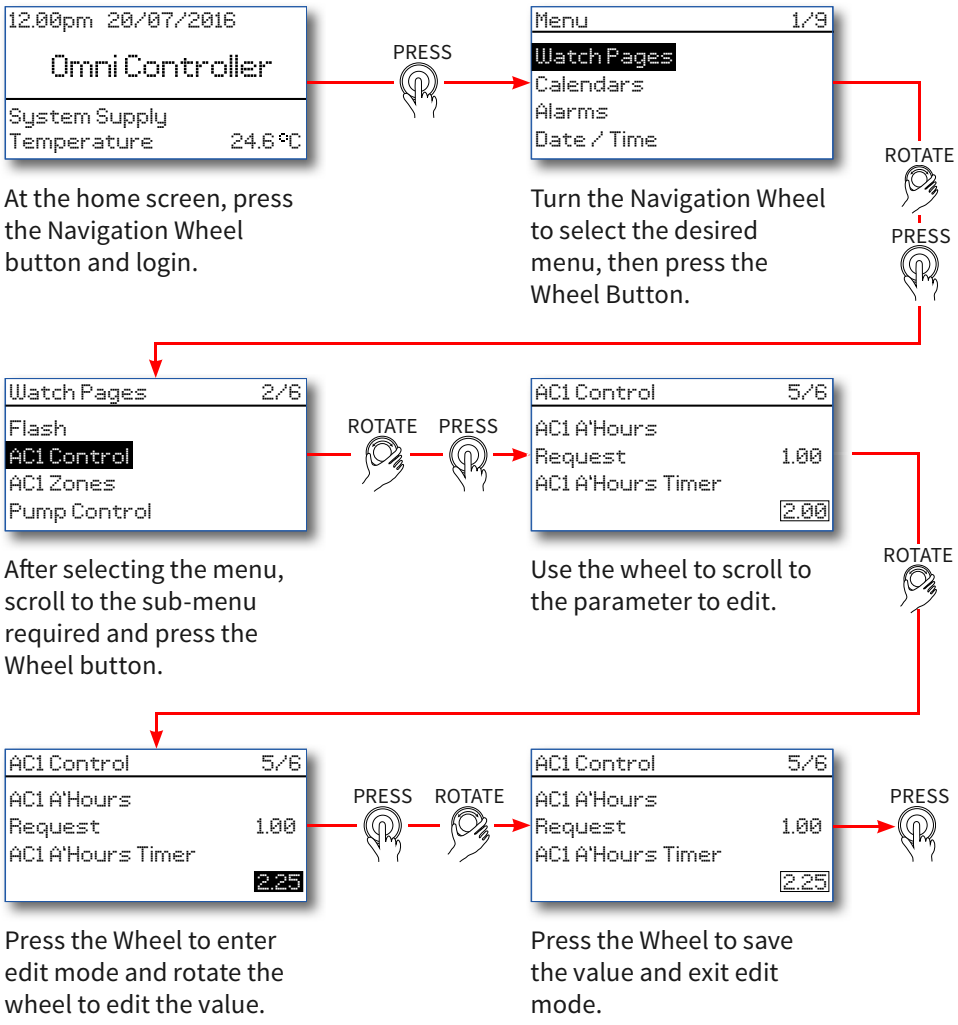
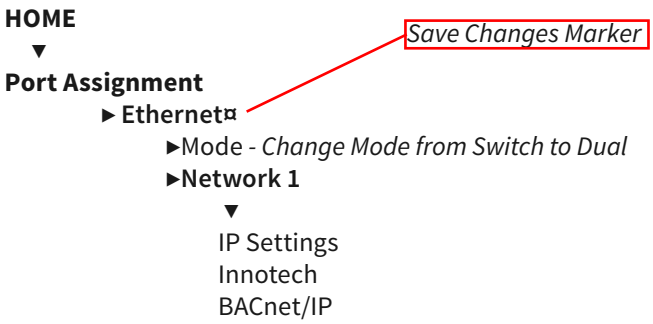


Figure 3-25: Parameter Setting Flow Chart

3-2.14 Saving Parameters

When changing parameters relating to the Omni Controller rather than the loaded configuration such as IP Address changes, you need to confirm the changes.

The display will remember the level of the menu that changes were made and the prompt will only appear when exiting from that level.



Changes will be saved at the level of menu they were made at.

In this instance, Mode was changed.

If you entered the Network 1 settings and made changes, the Save changes prompt will only appear when you back out of the Ethernet screen.

The prompt appears at the highest level that a change was made.

Figure 3-26: Save Prompt Level

A HMI screen that requires changes to be saved will have an asterix next to the HMI page name. When you leave the HMI page, a Save changes screen will appear. Select Yes, No or Cancel at this screen to continue.

Yes - Save changes
No - Exit screen without saving changes
Cancel - Return to previous screen without saving. Changes made will still be shown.

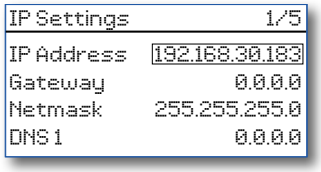


Figure 3-27: Settings Changed

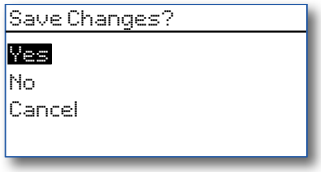


Figure 3-28: Save Changes?

This page has been left intentionally blank.

Omni

USER INSTRUCTIONS

4 Omni Web Server

INNOTECH®

4-1 Overview

This section of the document provides detailed information about accessing and using the on-board Web Server for configuring your Omni BEMS Controller.

Select the section from the menu at the side of the screen to enter a configuration screen. Most sections have sub menus for further configuration.

Omni Web Server is cross-platform and is accessed via your selected web browser. Use the IP Address of the Omni Controller to access the Omni Web Server and enter your username and password.

General terminology is used in this section based on using the Omni Web Server in a Microsoft Windows environment with mouse input. The Omni Web Server is also compatible with Android and iOS operating systems and notes will appear throughout where required for operation of the interface in different environments.

ANDROID

These notices indicate a piece of useful information which should be read for Android users.

iOS

These notices indicate a piece of useful information which should be read for iOS users.

4-2 Omni Web Server

4-2.1 Logging In

Type in the IP address of your controller into a web browser. After the page has loaded, enter your User Name & Password and then click Login to log in to the web server.

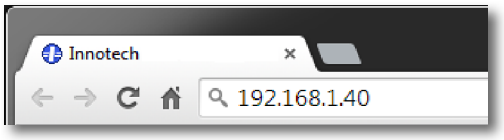


Figure 4-1: Enter IP Address in Browser

The IP used in the image above is an example only. Enter the IP specific to your controller. The default IP is 192.168.2.100.

IMPORTANT

The Username and Password fields are both case sensitive. 'Innotech' is not the same as 'innotech'.

If you have forgotten your password, click the *I've Forgotten My Password* link. Enter your User Name and click Reset Password and follow the prompts. Once you receive a temporary password or if you remember your old password, login and reset your password.

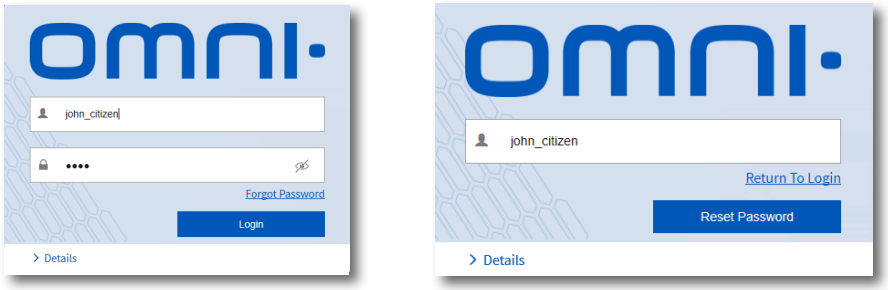


Figure 4-2: Login Dialog Box and Forgot Password Dialog Box

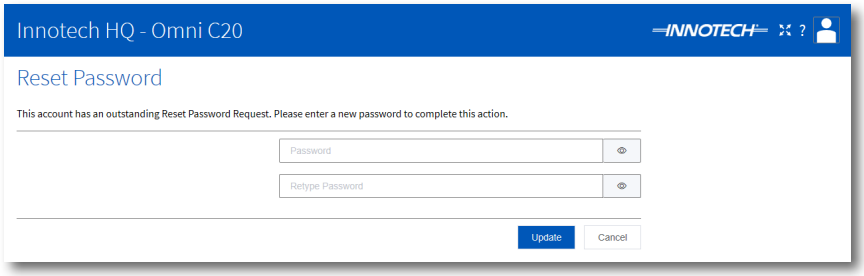


Figure 4-3: Reset Password Screen

Figure 4-4: Password Reset Window

4-2.2 Configuration Updates

When the browser cache is cleared or a new configuration is transferred to the controller, the browser will detect it and update the cache to provide faster loading of the web pages. During the process, the window will darken and updating will take place. No interaction is possible during the update. After completion, the web server is ready to use.

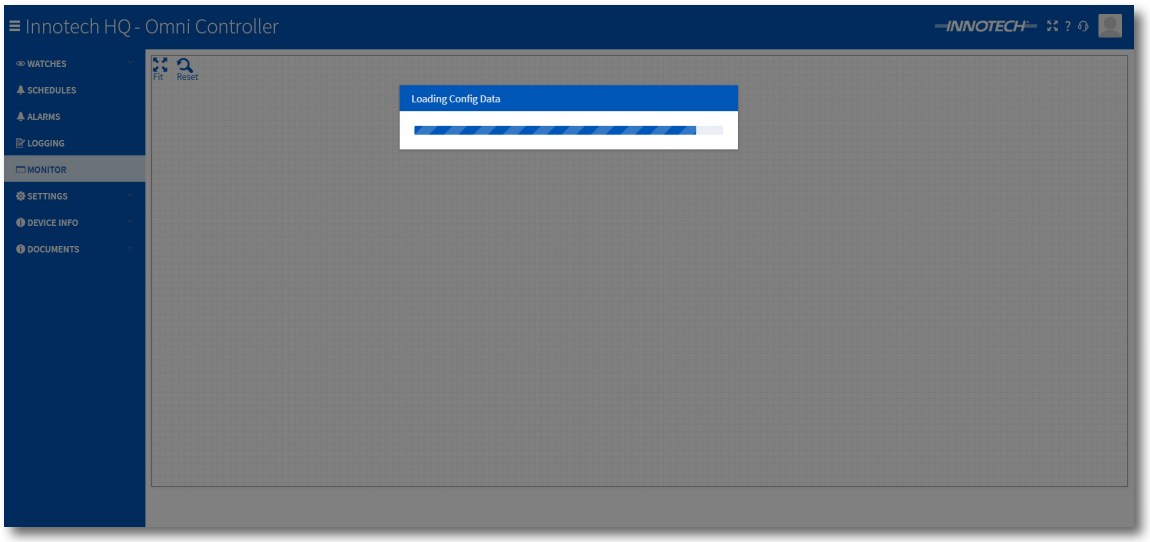


Figure 4-5: Updating Configuration Data

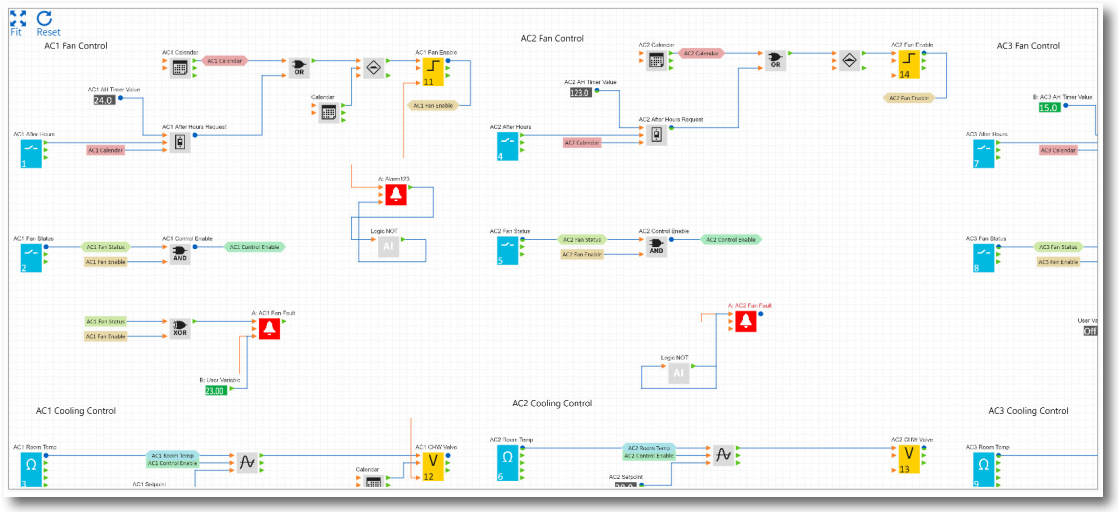


Figure 4-6: Configuration Updated/Transferred

4-2.3 Network

The Network item is only visible if Web Network Master is enabled in the Web Access settings. The Network screen displays the Omni devices on the network specified in the Web Access > Network settings. You can access another device from this screen.

When you click the current device, the Watches screen will show. If you click a device with a different IP, the login screen will show. Enter the login details to access the Web Server on the remote device.

The devices shown here can be sorted by Alarm Status, Omni Status, Alphabetically or by Default (as listed in the Web Access > Network settings.

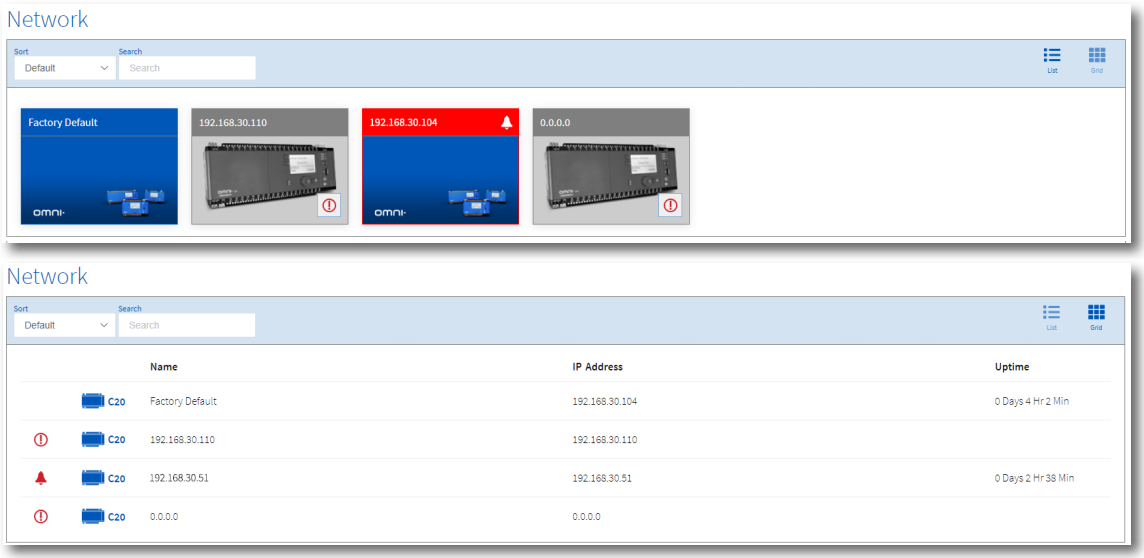


Figure 4-7: Network Screen - Icon and List Views

Cookies must be enabled on browsers used on Windows based computers for the Network screen to function correctly when HTTPS is used.

ANDROID

Cookies must be enabled for the Network screen to function correctly when HTTPS is used.
Enabling cookies in Chrome: Tap the menu icon and navigate to Settings > Content settings. Tap Accept cookies to enable.

iOS

Cookies must be enabled for the Network screen to function correctly when HTTPS is used.
Chrome for iPad: Cookies are enabled by default.
Safari for iPad: At the home screen go to Settings > Safari, set Block Cookies to Always Allow.

4-2.4 Watches

The Watches screen contains data to be monitored by the user (hence the term 'Watch') such as controller setpoints. The arrangement and content of each Watch Page and level of access for individual users is programmed by the Focus Configuration Software.

Click the graph button at the start of the line for each item to display a data graph for the selected item.

4-2.4.1 Other Pages

The other custom made pages are defined in the Focus configuration software and display watches, their live data and graphs. Use the horizontal navigation bar above the first graph to change how much of the graph is viewed. Click and drag a handle at the end to dynamically move the view.

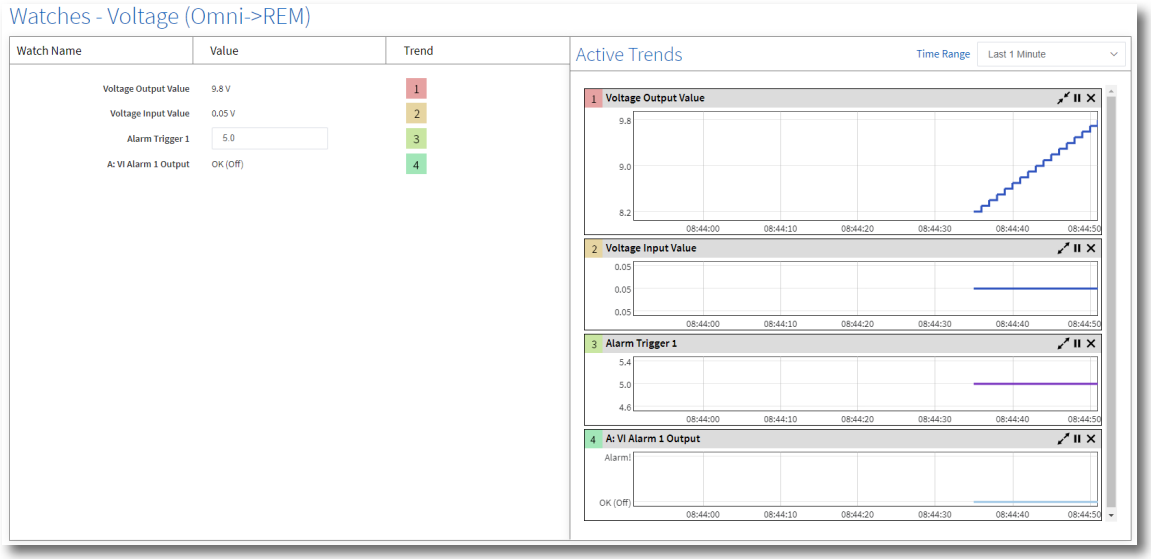


Figure 4-8: Watches Screen

4-2.5 Schedules

Schedules are programmed using the Schedules page, clicking a Calendar block on the Monitor tab or via the Calendar blocks in the Focus software. Click a Calendar to show the calendar details. This screen shows the status of the calendars.

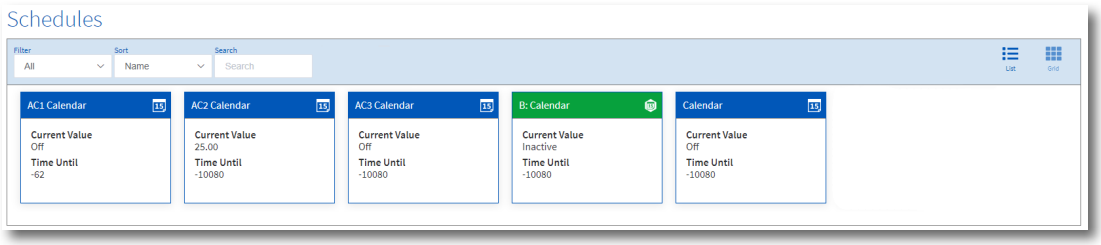


Figure 4-9: Schedules Screen - Calendar List

4-2.5.1 Calendars

The Schedules screen is used to view/edit schedules for your controller. You can change the calendar between Monthly, Weekly and Daily views.

Scheduled events can be made to repeat daily, weekly, monthly, yearly and can also can be created with custom repetitions. They can be made to repeat indefinitely or end on a certain date or after specified occurrences.

Events can be given a priority (number based, 1 is the highest priority) which will ensure that a higher priority event will trigger in the case of overlapping events.

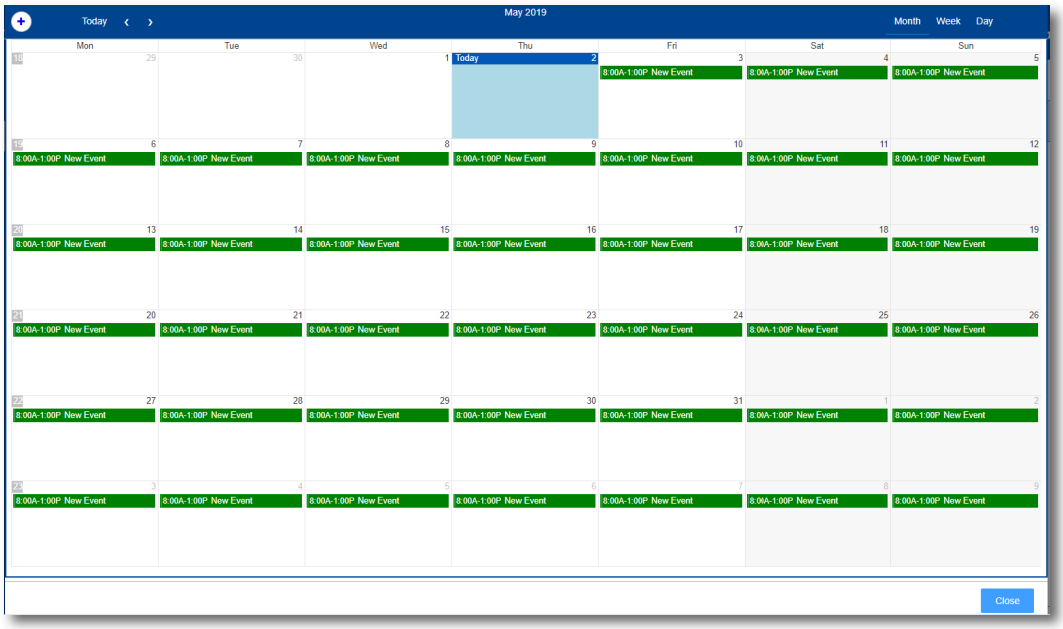


Figure 4-10: Schedules Screen - Calendar Month View

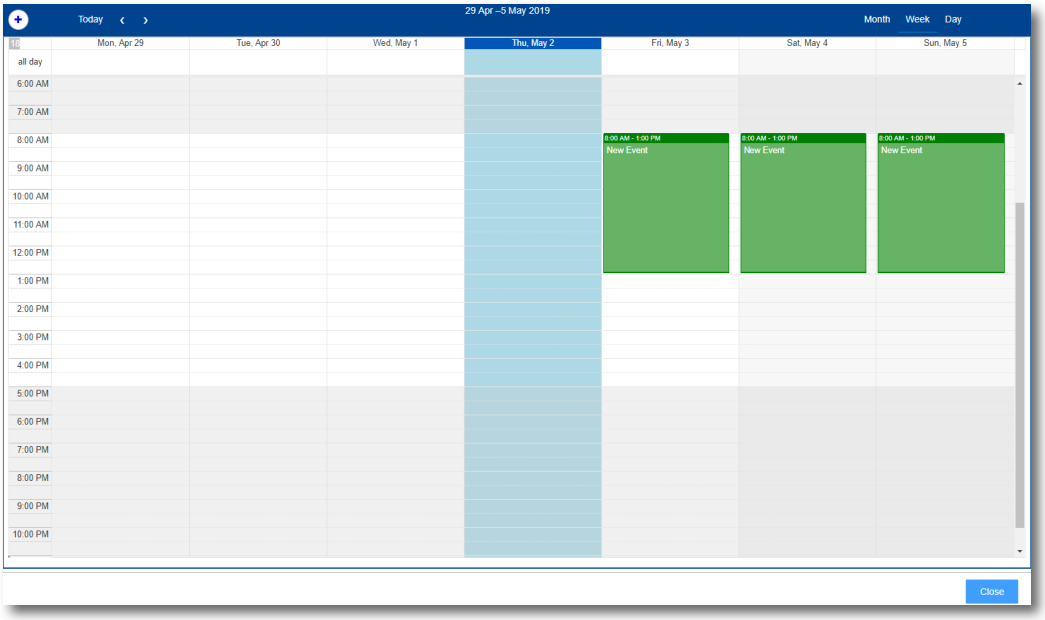


Figure 4-11: Schedules Screen - Calendar Weekly View

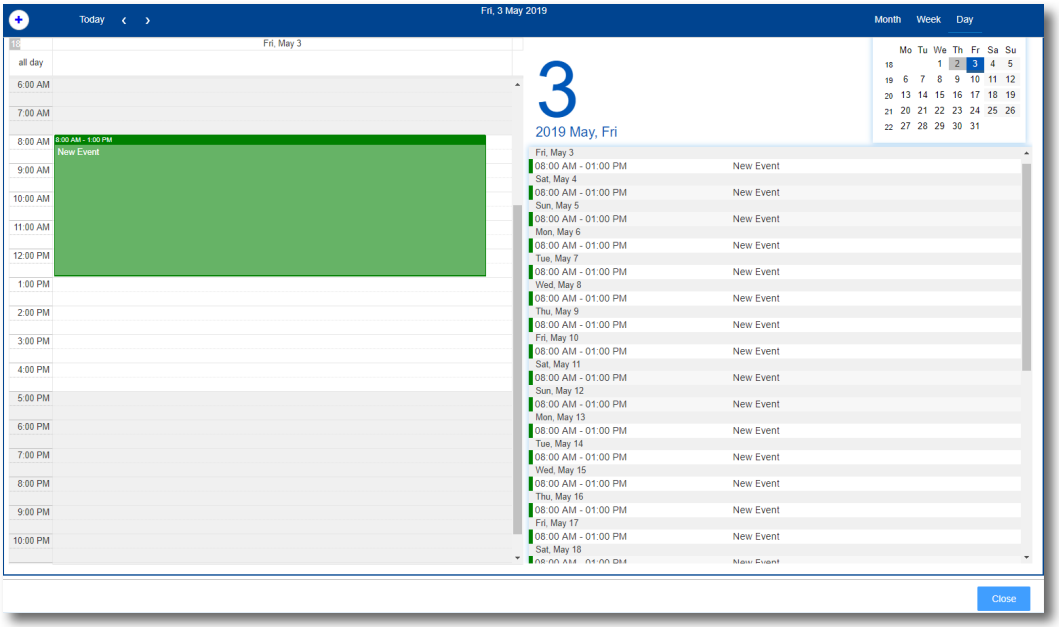


Figure 4-12: Schedules Screen - Calendar Daily View

Add New Calendar Event

Click the Add New Event button or double click the a day header (month view) or a time period to create a new calendar event.

Figure 4-13: Schedules Screen - Add New Event Button

Fill in the required details for the new calendar event and click save when done. Click Recurrence Details to edit the Repetition settings for the event.

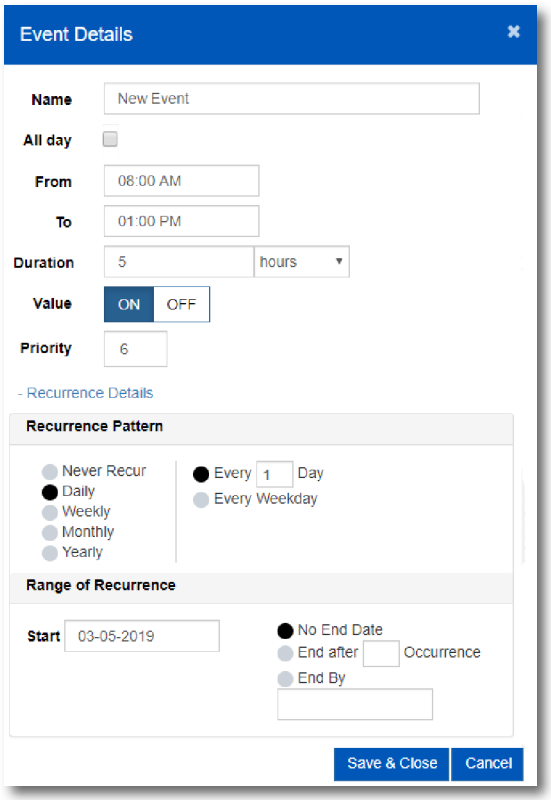


Figure 4-14: Schedules Screen - Add New Event Window

Table 4-1: Recurrence Options

Combo	Description
Repeat	No Repeat, Daily, Weekly, Monthly, Yearly. When a repeat is selected, you then need to select if or when the event will end.
Priority	A priority of 1 will override any events at a lower priority.

Edit Calendar Event

Click the event to open the event details window. If the event repeats, you will asked to select if you want to edit this instance or all instances.

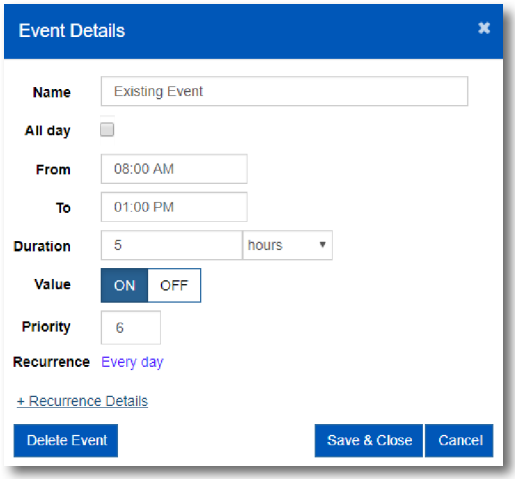


Figure 4-15: Schedules Screen - Event Details Window

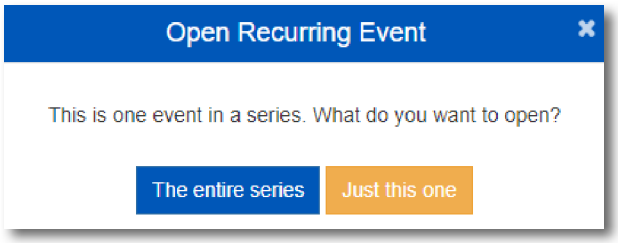


Figure 4-16: Schedules Screen - Recurrence Options

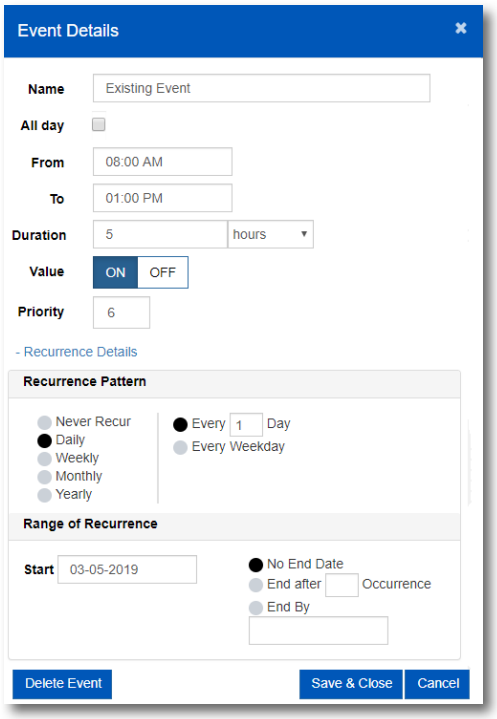


Figure 4-17: Schedules Screen - Edit Event Recurrence

Click Save to save your changes. Click Cancel to undo your edits and revert to the previously saved event.

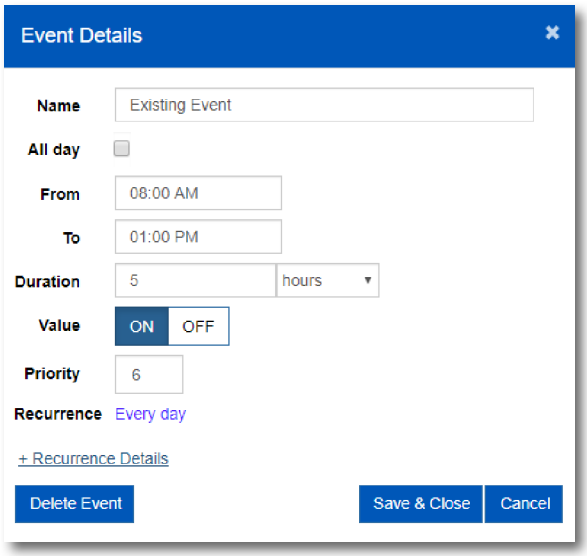


Figure 4-18: Schedules Screen - Edit Event Recurrence

Delete Calendar Event
Events can only be deleted from the edit window. After entering the event edit window, click Delete Event to delete the event.

4-2.5.2 Calendar States

Calendars on the Schedules tab are colour coded to show their current state at a glance.

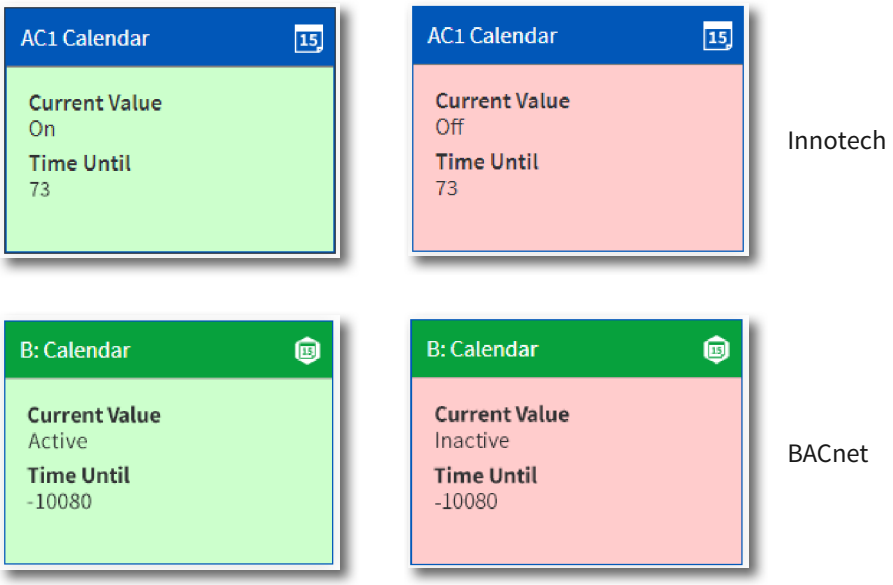


Figure 4-19: Schedules Screen - Calendar States

4-2.6 Alarms

The Alarms screen will show the details of any Alarms that have been activated in the system. Clicking any alarm will show the history of the alarm. An alert will flash red when the there are active alarms to alert the user.

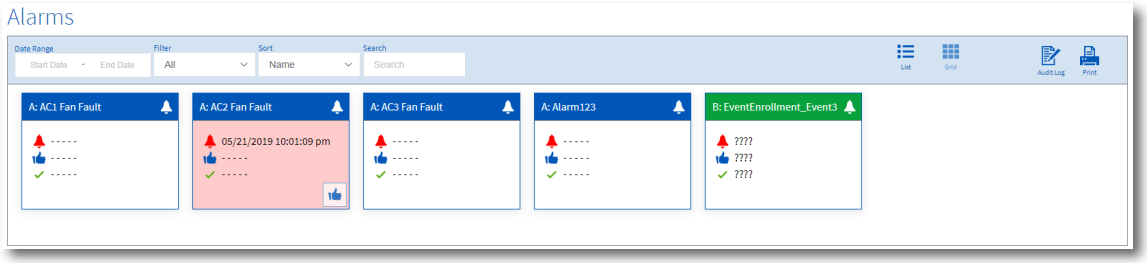


Figure 4-20: Alarms Overview

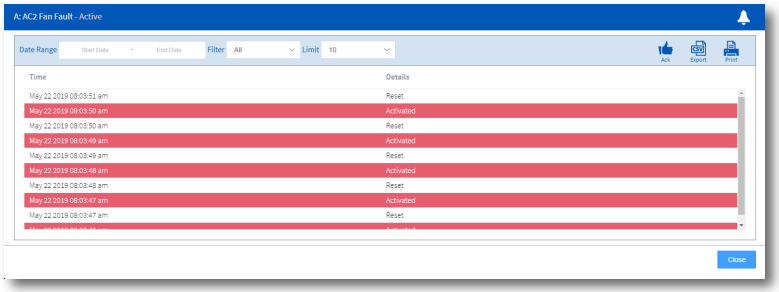


Figure 4-21: Alarms History

4-2.6.1 Acknowledging Alarms

Acknowledge the alarm by clicking the hand icon on the alarm.

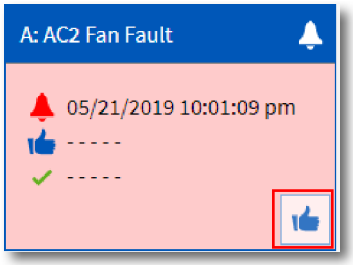


Figure 4-22: Acknowledgement Icon

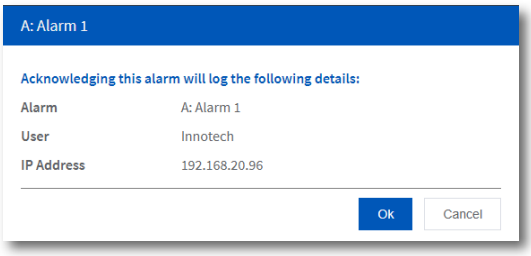


Figure 4-23: Acknowledge Alarm Browser Message

After clicking OK, the alarm icon will change to orange and the time of acknowledgement noted in the alarm history. When the alarm is acknowledged, it is still active. Remedy the problem and when the alarm is reset, the icon will change to green.

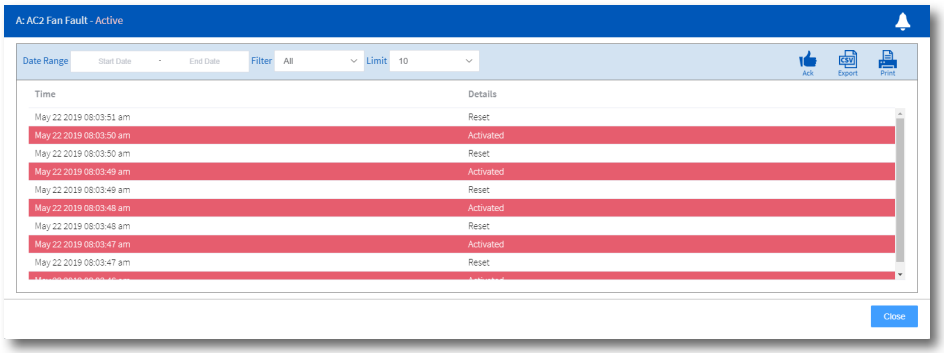


Figure 4-24: Acknowledged Alarm History

4-2.6.2 Alarm Filtering

Click in the Search field and start typing the name of the alarm. As you type the list of alarms will be filtered to show only those specified by the filter.

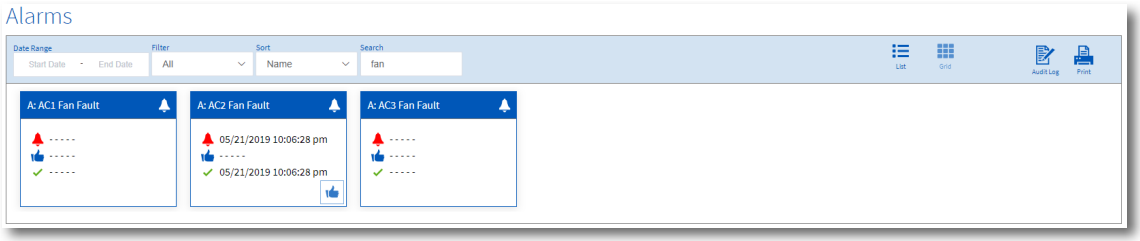


Figure 4-25: Alarm Filter

4-2.7 Logging

The Logging screen is used to view custom data logs of a selected item. Log and Alarm blocks can be viewed.

4-2.7.1 Downloading a Log Graph

1. Specify the time period for the downloaded logs from the Date Range combo.

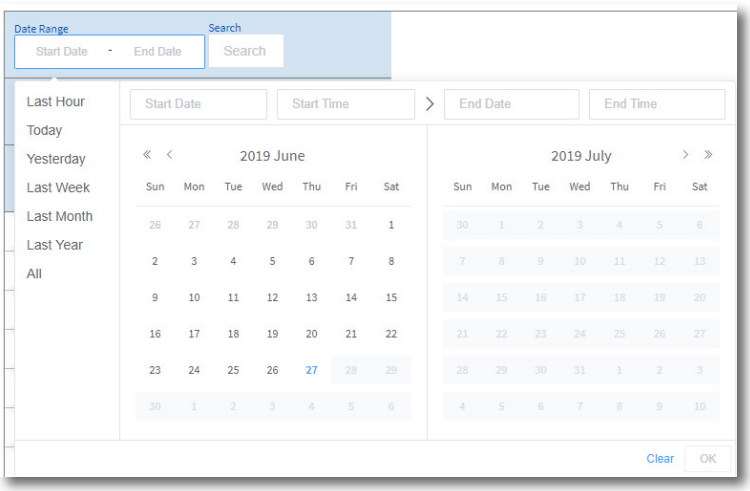


Figure 4-26: Logging - Log Extraction Duration

2. Click one or more Log or Alarm block rows to mark for download.
3. Click Extract to download the logs. You can stop downloading a log graph at any time by clicking the Stop button. After download, moving the cursor on the graph shows the logged value. You can zoom the graph by using the mouse wheel and CTRL and SHIFT keys in combination with the wheel. Hovering over an item on the left, will highlight the line on the graph.
4. The line under the graph can be adjusted using the handles on either end to show a different time period.

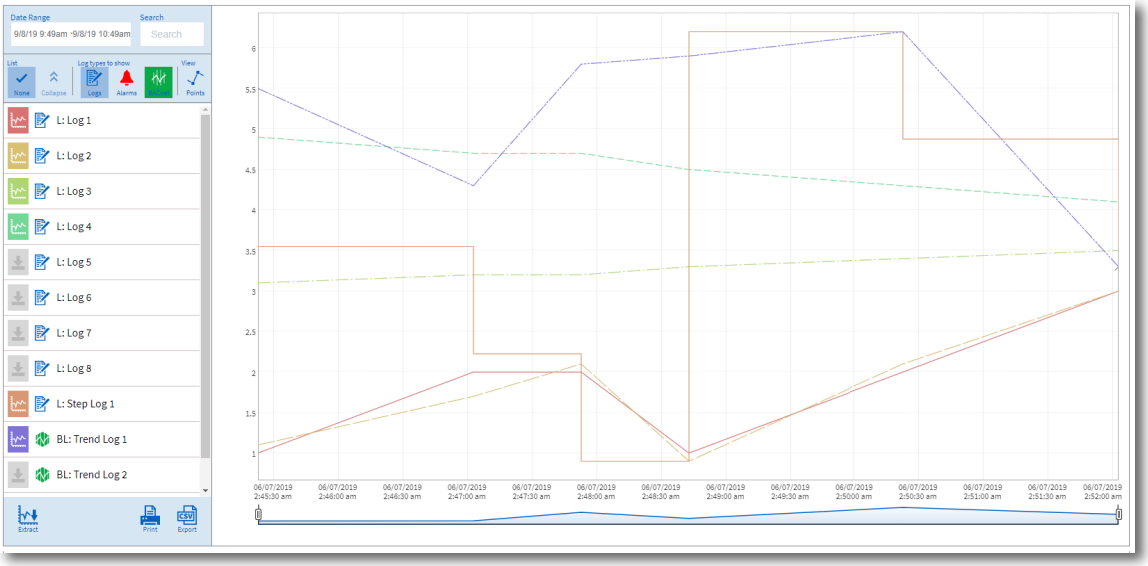


Figure 4-27: Logging - Graph Downloaded

4-2.7.2 Viewing a Section of the Downloaded Data

1. Click and drag the handles at each end of the graph overview at the bottom to change the viewed range.
2. The graph will dynamically change as the handles are moved.

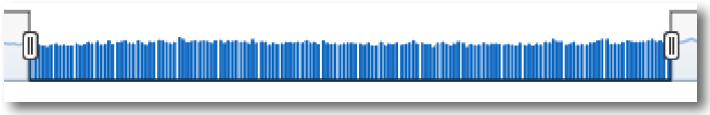


Figure 4-28: Logging - Viewing Range

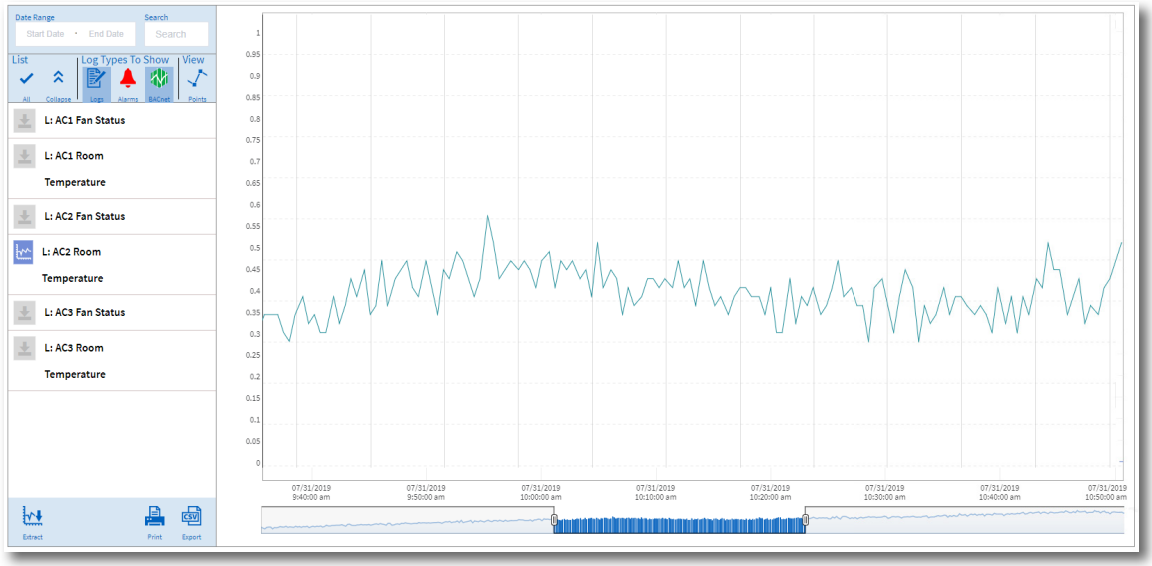


Figure 4-29: Logging - Graph Range

4-2.7.3 Printing a Log Graph

1. Use the print shortcut CTRL+P to print the current log view.
2. A Print dialog window will open for specifying your printer.
3. Click OK to print the graph.

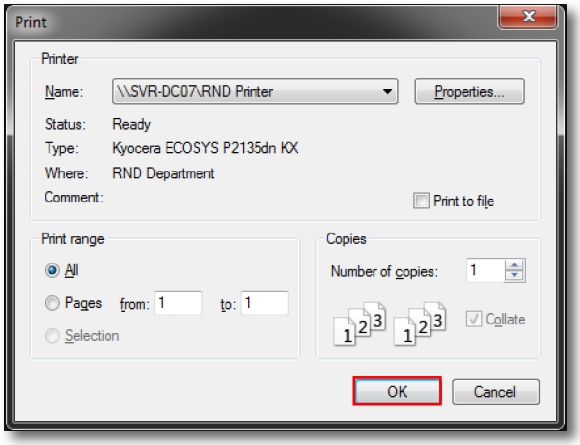


Figure 4-30: Logging - Print Dialog

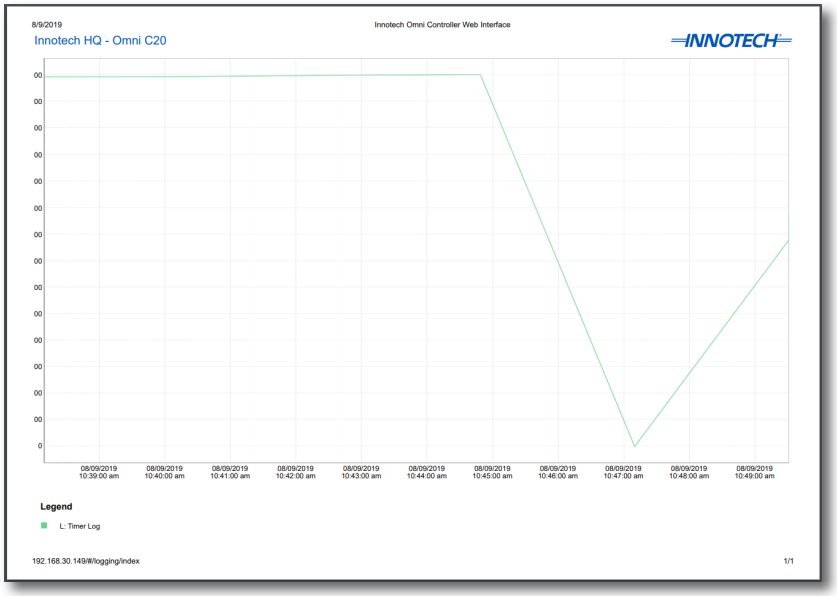


Figure 4-31: Logging - Print Preview

ANDROID

Chrome: Press on the Menu and select 'Print...'. Press and select 'Save as PDF' or 'All Printers...' to select a printer. Change the page size and copies if required.

iOS

Chrome for iPad: At the top right tap More Share, select Print, select printer options and settings, tap Print.
Safari for iPad: Tap the settings icon, tap Print, tap Select Printer..., tap Print.

4-2.7.4 Exporting to CSV

1. After downloading your log, click the Export to CSV button.
2. You will be promted by your browser to save the file. Save the file to your device, taking note of the save location.
3. Open the CSV file using a spreadsheet program to view the results.

Figure 4-32: Logging - Save CSV Export?

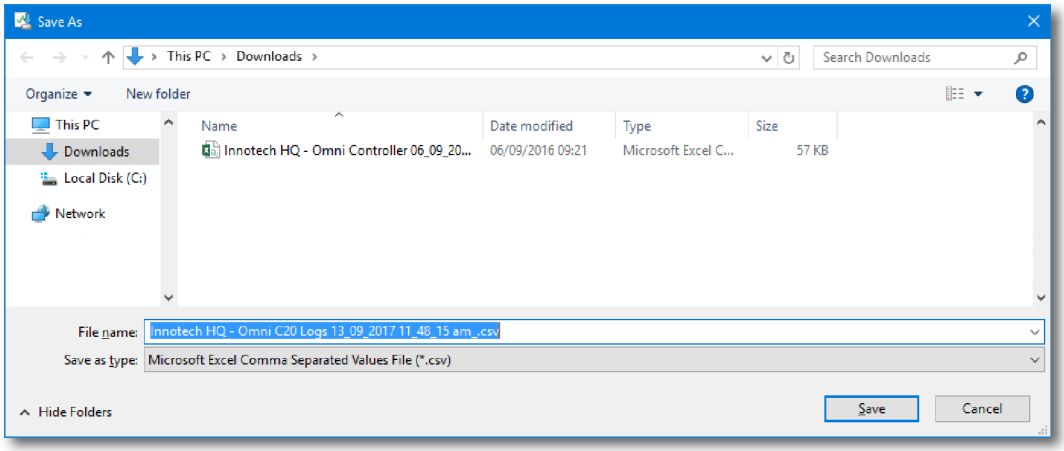


Figure 4-33: Logging - Select File Location

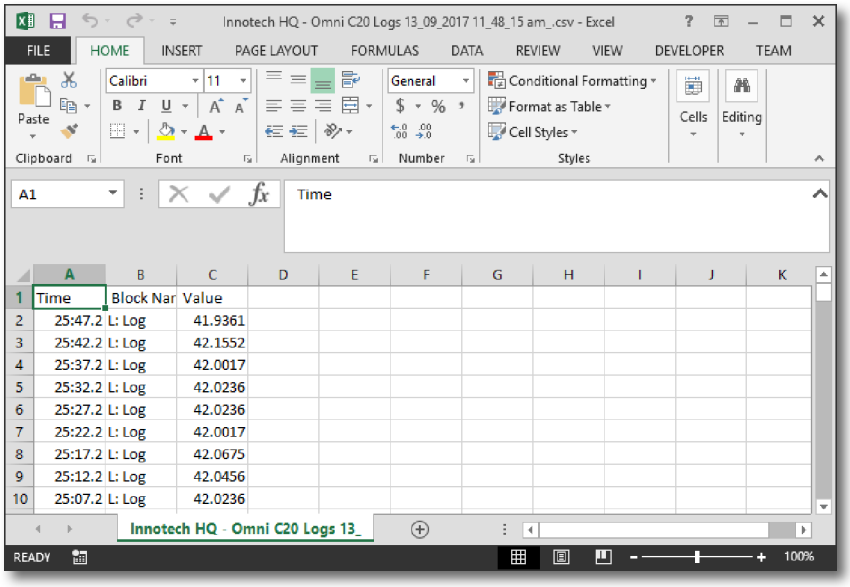


Figure 4-34: Logging - Exported CSV File

ANDROID

Chrome: Press on Export to CSV, follow the onscreen prompts.

iOS

Chrome for iPad: Press on Export to CSV, follow the onscreen prompts.
Safari for iPad: Press on Export to CSV, follow the onscreen prompts.

4-2.7.5 Formatting the Time Field

If you are viewing your CSV file in Microsoft Excel, the Time field will not initially be formatting correctly. Follow these steps to reformat your Time field.

1. Click the Row Header to select the column.

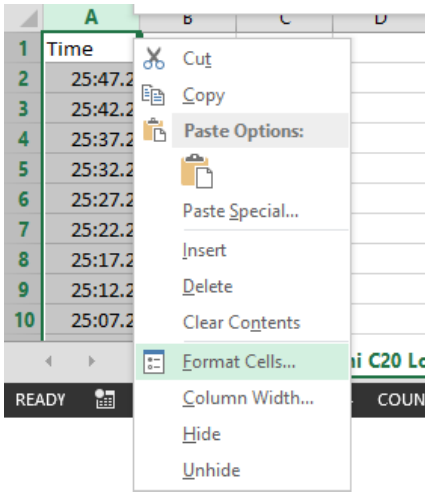


Figure 4-35: Cell Context Menu

2. Right click a cell and select Format Cells

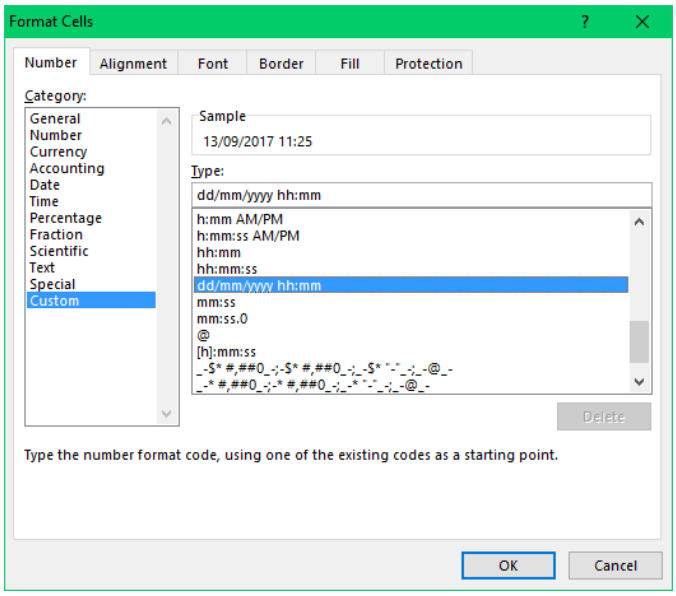


Figure 4-36: Format Cells Window

3. Choose an appropriate cell format and click ok.

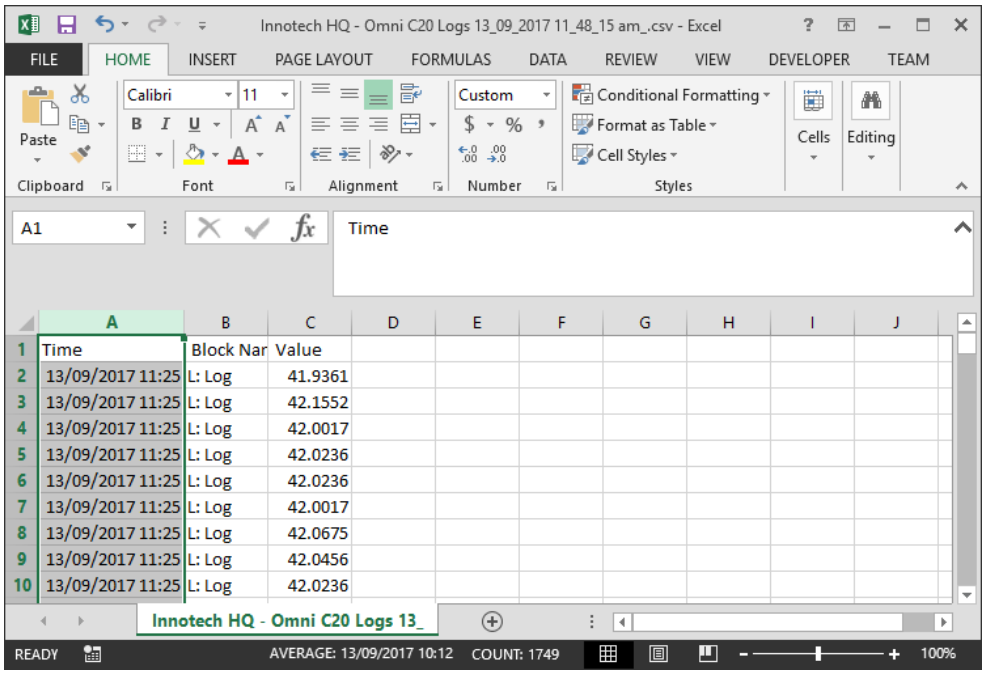


Figure 4-37: Column Reformatted

4-2.8 Monitor

The Monitor screen displays the current configuration saved on the Omni Controller you are accessing. Most blocks can be clicked to display more information about that block and click any output node to view live data from the controller. Some block settings can be edited after clicking.

Only one block's information window can be opened at once. Click the Fit button to fit the entire configuration in the viewable area or 100% to see the configuration at 100% view.

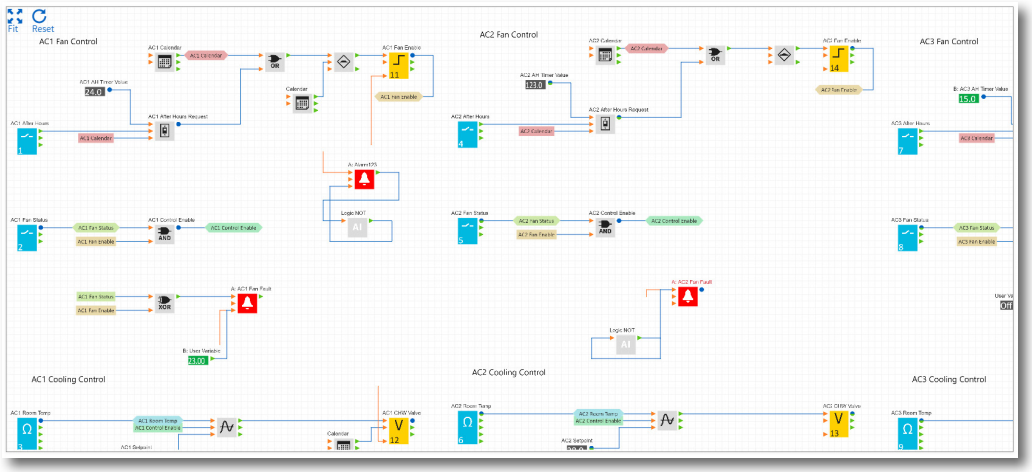


Figure 4-38: Monitor Screen Overview

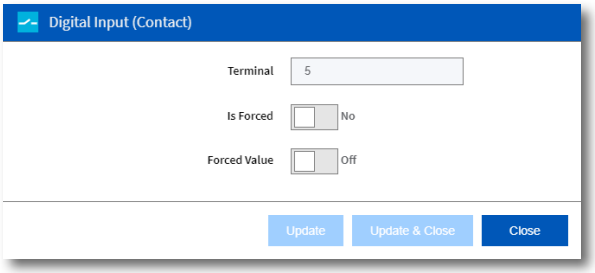


Figure 4-39: Block Details

- Some block values can be edited while the controller is being accessed with the web server.
- Click a node to see an inspector.
- Double click anywhere in the inspector to view a live graph.
- Many live data inspectors can be opened simultaneously.

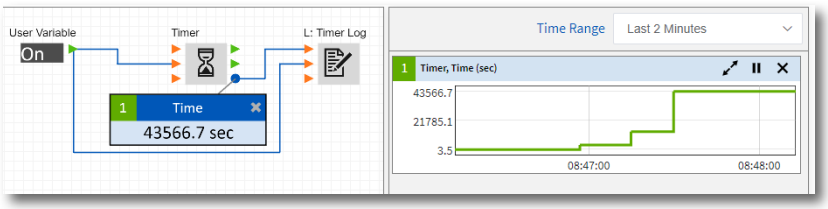


Figure 4-40: Omni Live Data Inspector with Graph

4-2.9 Settings

The Settings Screen has multiple categories for configuring your Omni Controller. Settings shown will be applicable to the model and settings of the controller.

The Settings section has many sub-sections for configuring your Omni Controller. Use these links to quickly move to the section you require.

Table 4-2: Settings Section Index

4-2.9.1 Device

The Device Settings are simply for naming and describing your Omni Controller. Naming it something meaningful will assist with identification on larger systems. The name specified here will show on the controller's HMI if it is fitted.

1. Enter a Name, Description, Location and Site Details for the Omni Controller.
2. Click Update.

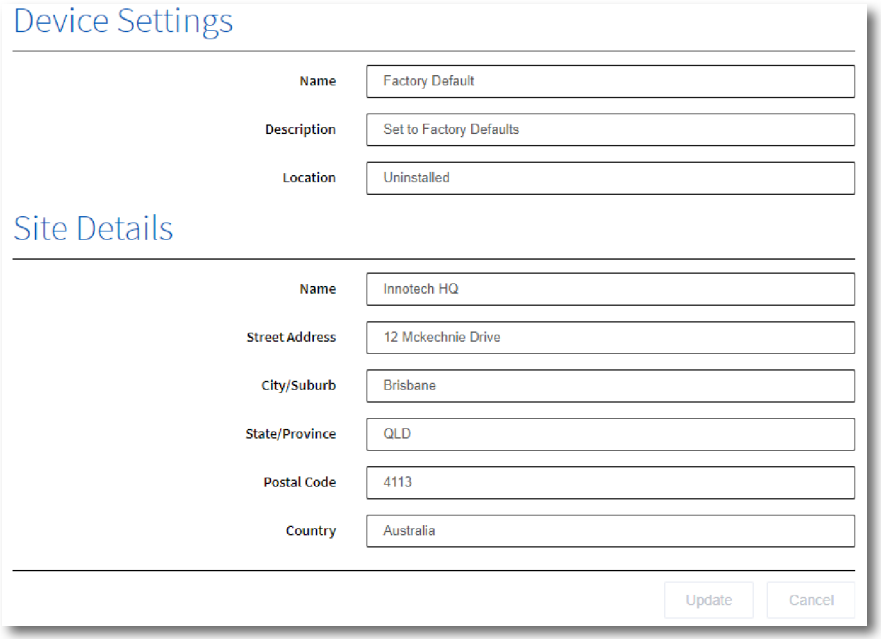


Figure 4-41: Settings - Device

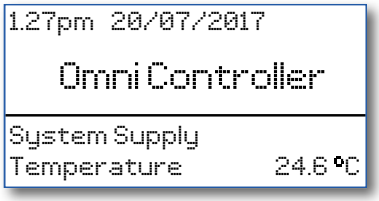


Figure 4-42: HMI Showing Device Name

4-2.9.2 Protocols

Select a protocol from the list in the menu at the left. Follow the steps below to change the Protocol Settings for the Omni Controller.

BACnet Settings

Click BACnet at the left to select the BACnet settings. Enable the protocol to modify the settings.

Device Settings

1. Enable the BACnet protocol.
2. Enter settings as required.
3. Click Update to update your Omni Controller.

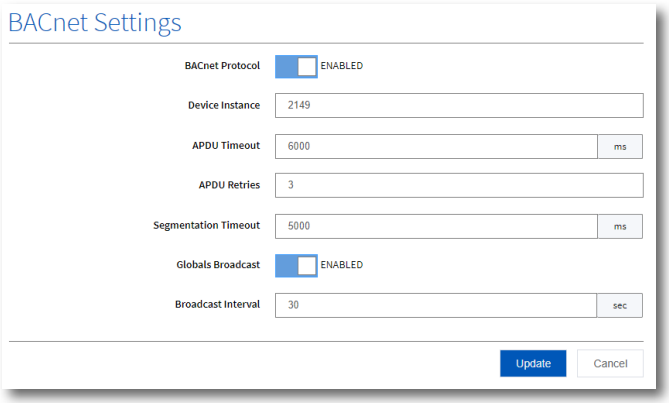


Figure 4-43: Settings - Protocols (BACnet Device Instance Settings)

Innotech Protocol

1. Click the slider to enable or disable the protocol.
2. Enter a number in the Device Address text box.
3. Click Update to update the Omni Controller.

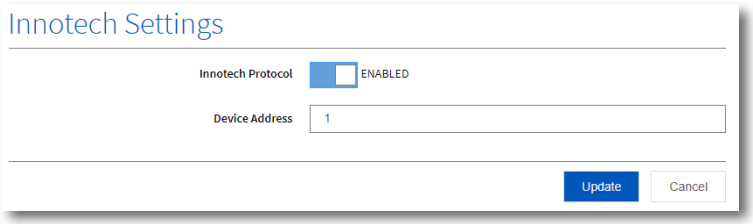


Figure 4-44: Settings - Protocols (Innotech Protocol)

Modbus Protocol

1. Click the slider to Enable or Disable.
2. Click Update to update the Omni Controller.

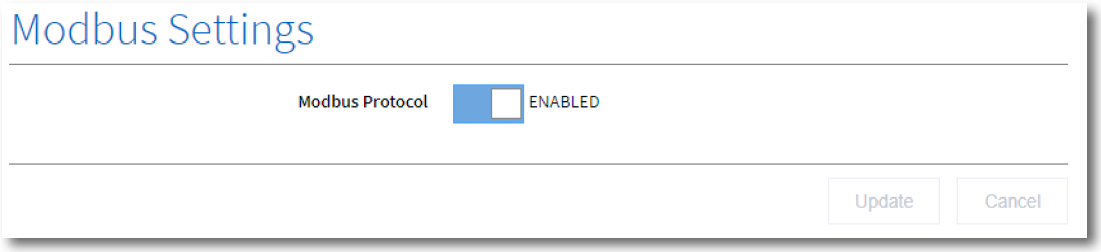


Figure 4-45: Settings - Protocols (Modbus Protocol)

The Omni Controller must have a Modbus feature licence installed to utilise the Modbus protocol.

ISS Protocol

1. Click the slider to Enable or Disable.
2. Click Update to update the Omni Controller.

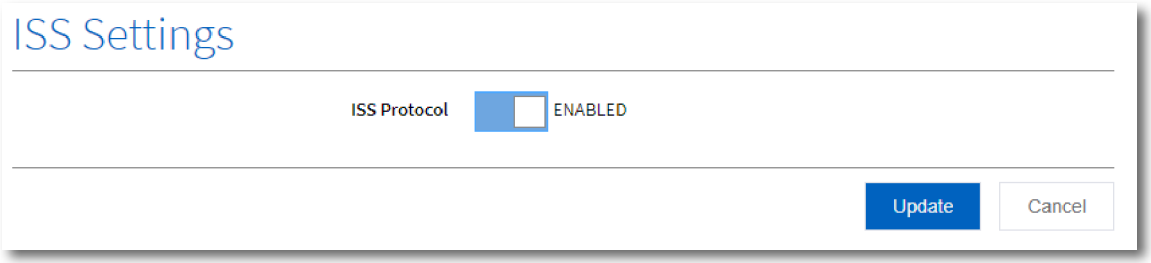


Figure 4-46: Settings - Protocols (ISS Protocol)

4-2.9.3 Port Assignment

Clicking Port Assignment will select the first item (Ethernet) by default. Follow the steps below to change the Port Assignment for the Omni Controller.

Ethernet

Select Switch or Dual from the Mode combo box to change the settings (Switch/Dual selection not available for C14 Models).

1. Select Switch or Dual Mode.
2. If Dual is selected, select either Port A or Port B.
3. If not already selected, click Configuration under the TCP/IP heading.
4. Edit the Configuration settings at the right as required for your network. The MAC Address is also shown in the TCP/IP Ethernet settings and cannot be edited.
5. When complete, click Update to update your Omni controller.

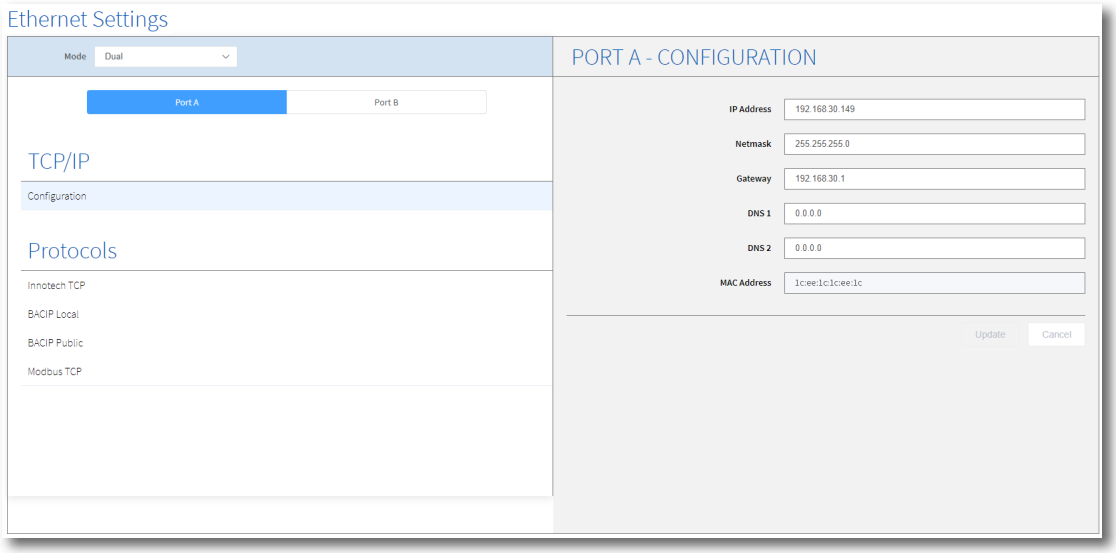


Figure 4-47: Settings - Port Assignment (Ethernet)

Innotech TCP

1. Click the switch to enable Innotech TCP.
2. Specify a TCP Port Number (or accept the default settings).
3. Click Update to update the controller.

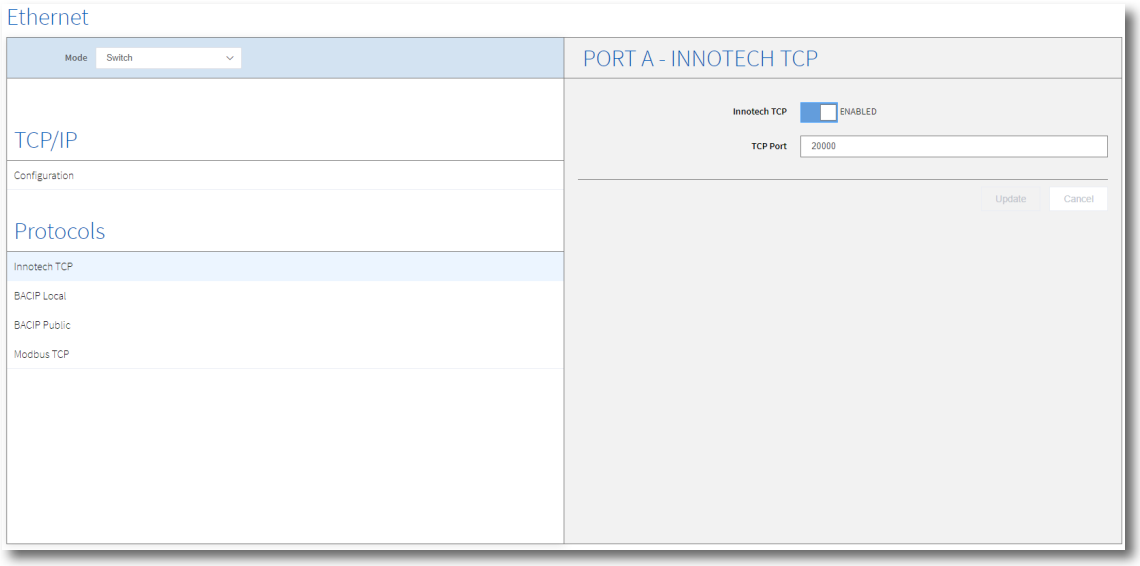


Figure 4-48: Settings - Port Assignment (Innotech TCP)

BACnet IP

BACnet IP Local Settings - Device Mode

1. Click the switch to enable BACIP Local.
2. Change the Mode to Device.
3. Enter the Network Number and UDP Port (or accept the default settings).
4. Click Update to update your Omni Controller.

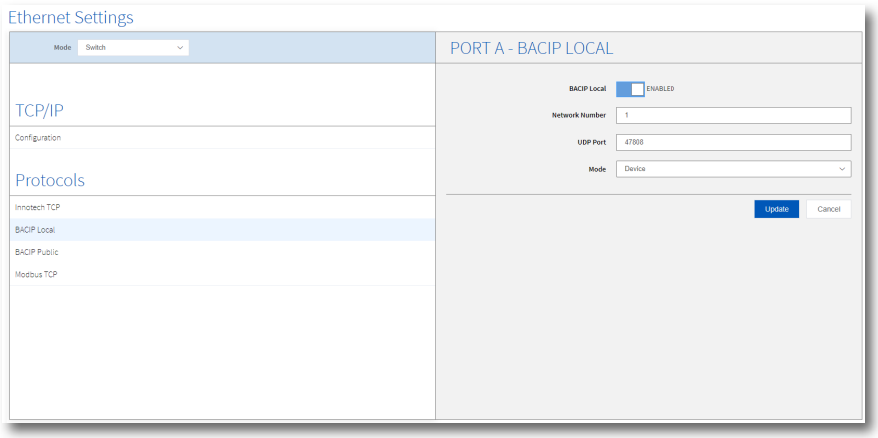


Figure 4-49: Settings - Port Assignment (BACnet IP Local Device Mode Settings)

BACnet IP Local Settings - Foreign Device Mode

1. Click the switch to enable BACIP Local.
2. Change the mode to Foreign Device.
3. Enter the Network Number and UDP Port (or accept the default settings).
4. Enter the BBMD Port and Address.
5. Specify a Time to Live value in seconds.
6. Click Update to update your Omni Controller.

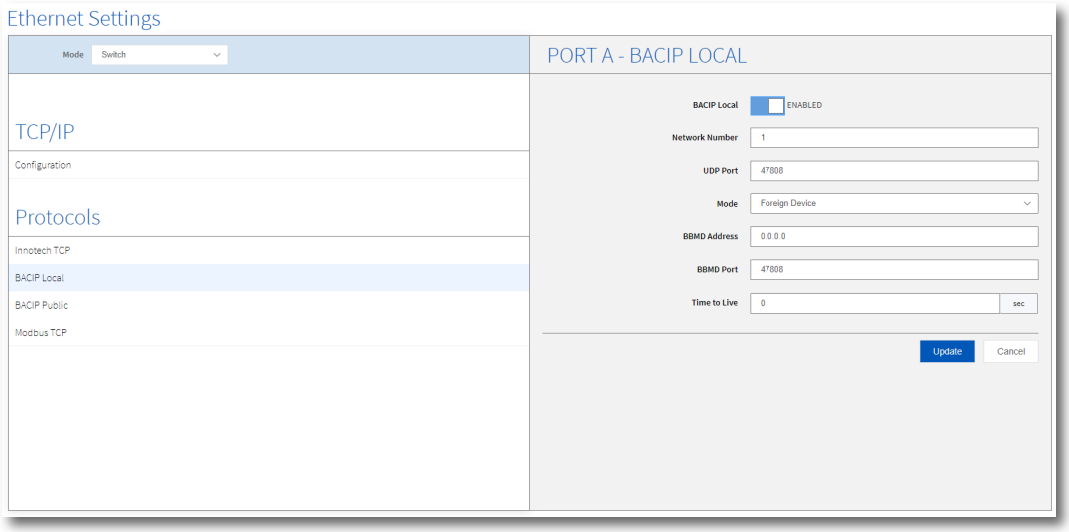


Figure 4-50: Settings - Port Assignment (BACnet IP Local Foreign Device Mode Settings)

BACnet IP Local Settings - BBMD Mode

1. Click the switch to enable BACIP Local.
2. Change the mode to BBMD.
3. Enter the Network Number and UDP Port (or accept the default settings).
4. Edit a BBMD Maximum Foreign Device value.
5. In the Distribution Table, enter an IP and Port and click add to the item to the table.
6. Click Update to update your Omni Controller.

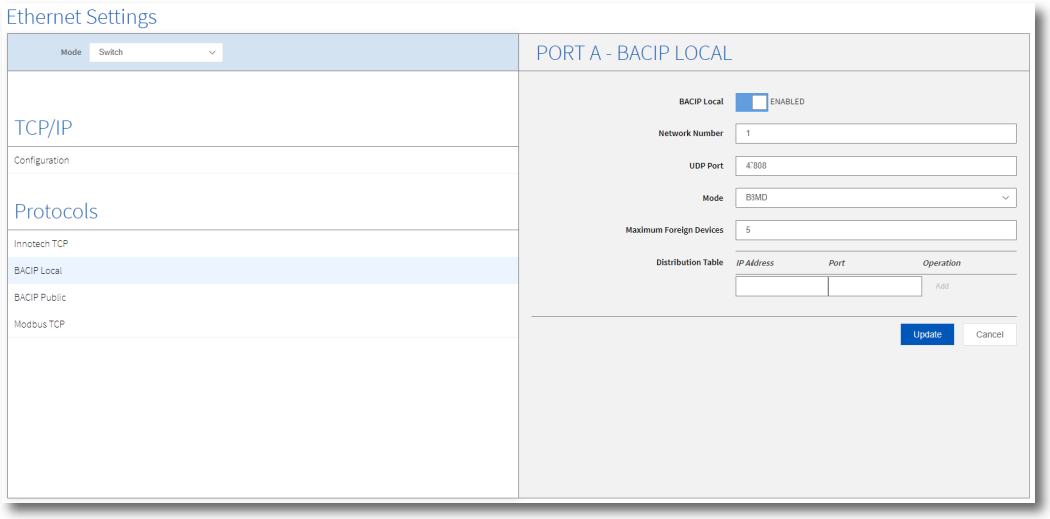


Figure 4-51: Settings - Port Assignment (BACnet IP Local BBMD Mode Settings)

BACnet IP Public Settings

1. Click the switch to enable BACnet IP Public.
2. Enter a Network number, maximum foreign devices, UDP port and Public IP Address.
3. In the Distribution Table, enter an IP and Port and click add to the item to the table.
4. Click Update to update your Omni Controller.

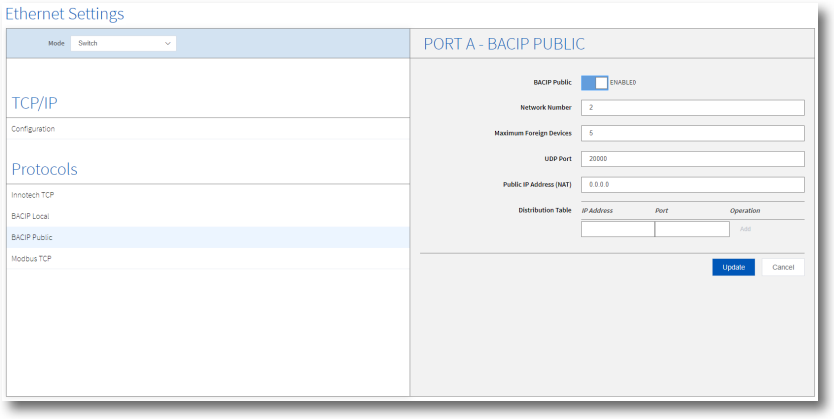


Figure 4-52: Settings - Port Assignment (BACnet IP Public Settings)

Modbus TCP

1. Click the switch to enable Modbus TCP.
2. Enter the Response Timeout (or accept the default settings).
3. Click Update to update the controller.

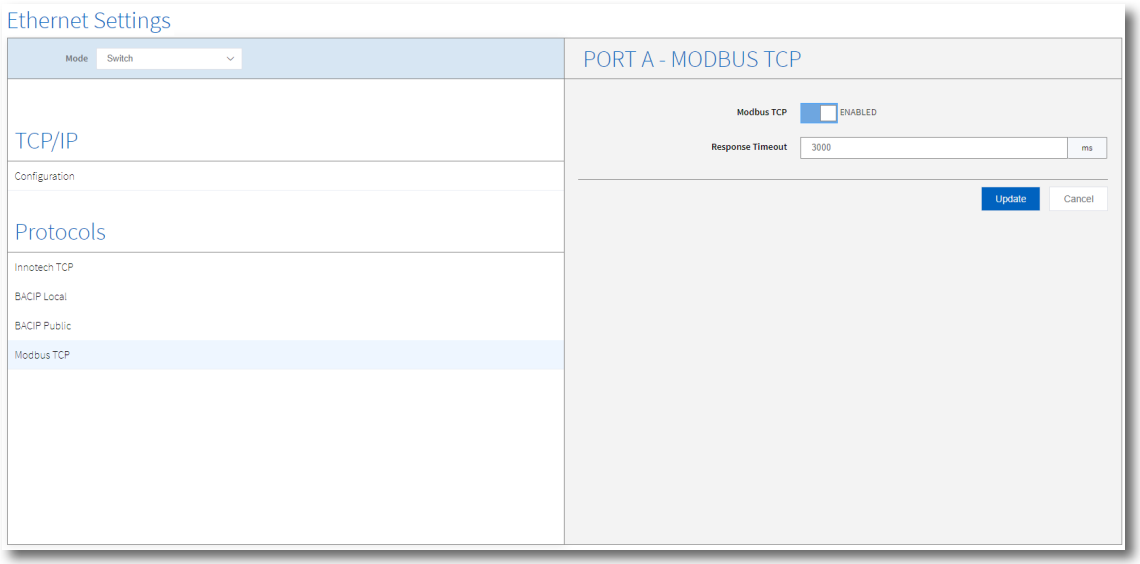


Figure 4-53: Settings - Port Assignment (Modbus TCP Settings)

The Omni Controller must have a Modbus feature licence installed to utilise the Modbus protocol.

RS-485

Click an RS-485 port at the left to configure the settings. Select a protocol to show the settings.

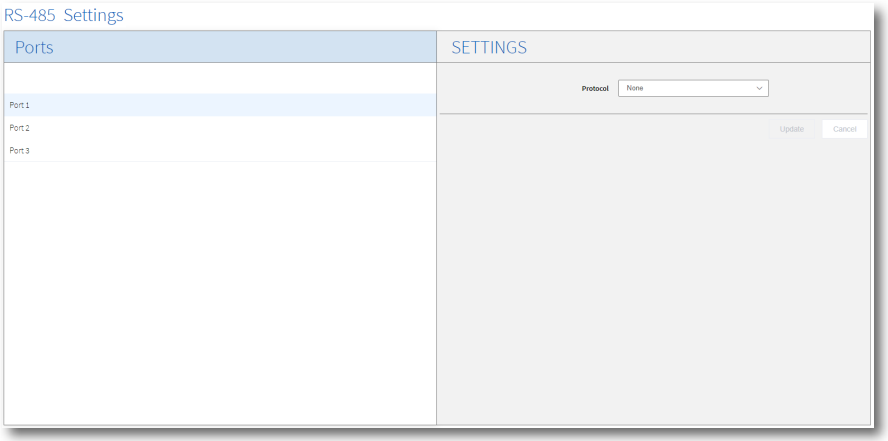


Figure 4-54: Settings - Port Assignment (RS-485 - Select Protocol)

Omni REM is only available on Port 3.

Innotech Net

1. Enter/Select details as required.
2. Click Update to update your Omni Controller.

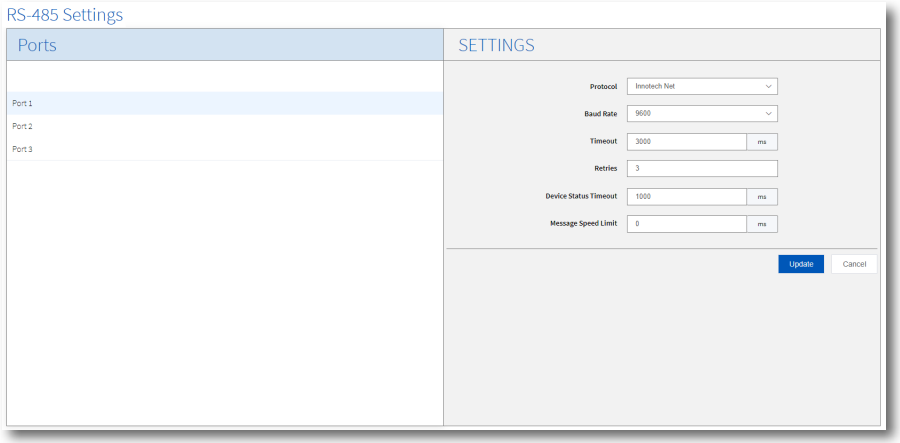


Figure 4-55: Settings - Port Assignment (RS-485 - Innotech Net Protocol)

Innotech Global

1. Enter/Select the details required.
2. Click Update to update your Omni Controller.

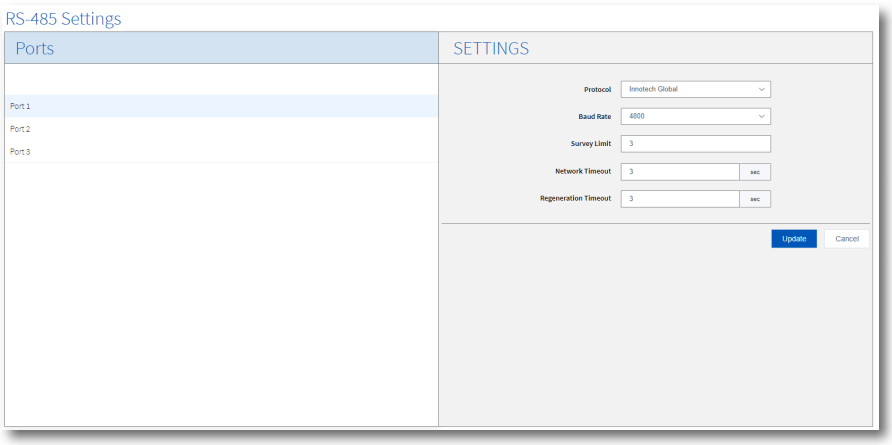


Figure 4-56: Settings - Port Assignment (RS-485 - Innotech Global Protocol)

BACnet MS/TP

1. Enter/Select details as required.
2. Click Update to update your Omni Controller.

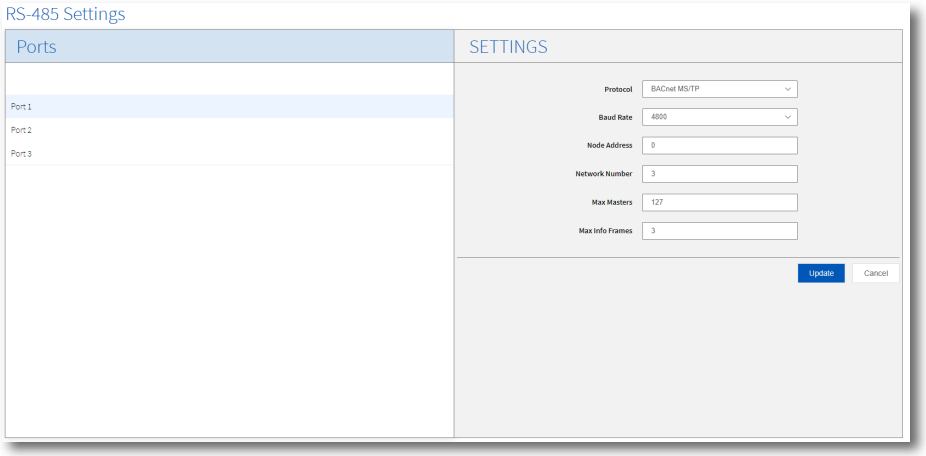


Figure 4-57: Settings - Port Assignment (RS-485 - BACnet MS/TP)

Modbus RTU

1. Enter/Select details as required.
2. Click Update to update your Omni Controller.

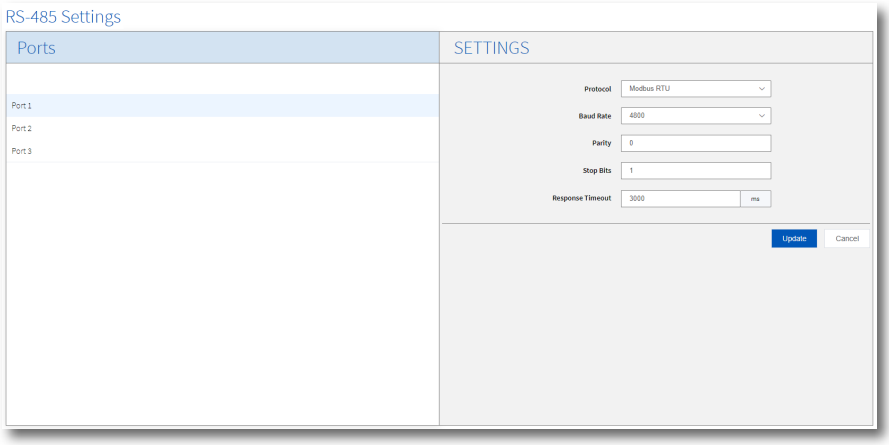


Figure 4-58: Settings - Port Assignment (RS-485 - Modbus RTU)

Omni REM

1. Select Omni REM if you have an Omni U10 REM connected to your RS-485 port.
2. Click Update to update your Omni Controller.

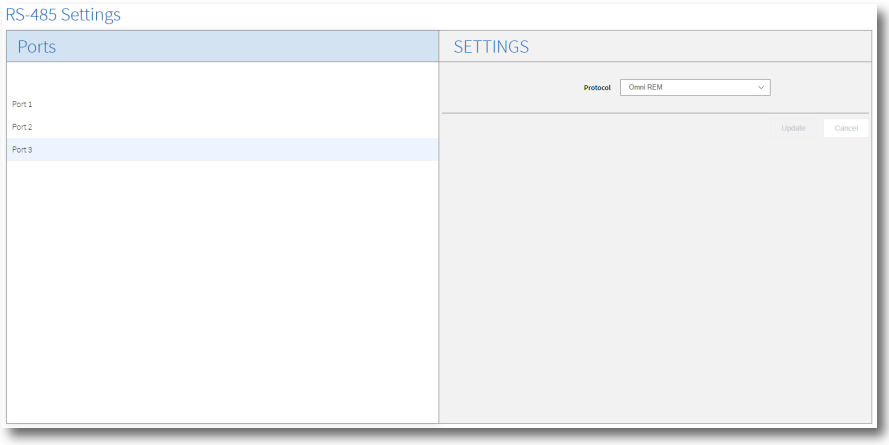


Figure 4-59: Settings - Port Assignment (RS-485 - Omni REM)

RS-485 Port 2 & 3 Port Assignment is configured in the same way as detailed for Port 1. C14 only has two RS-485 ports. This is reflected in the settings.

You can only have one Innotech Net and one Innotech Global port configured on the Omni to connect to an Innotech RS-485 network of devices. All three ports can be set to BACnet MS/TP if required.

4-2.9.4 Date & Time

Local Settings

Click Date & Time and then Local Settings.

1. Specify the time, date, time zone and display format for the Omni Controller.
2. Select your country and time zone from the Country and Time Zone combo boxes or select your time zone on the map.
3. Click Update to update the controller when done.

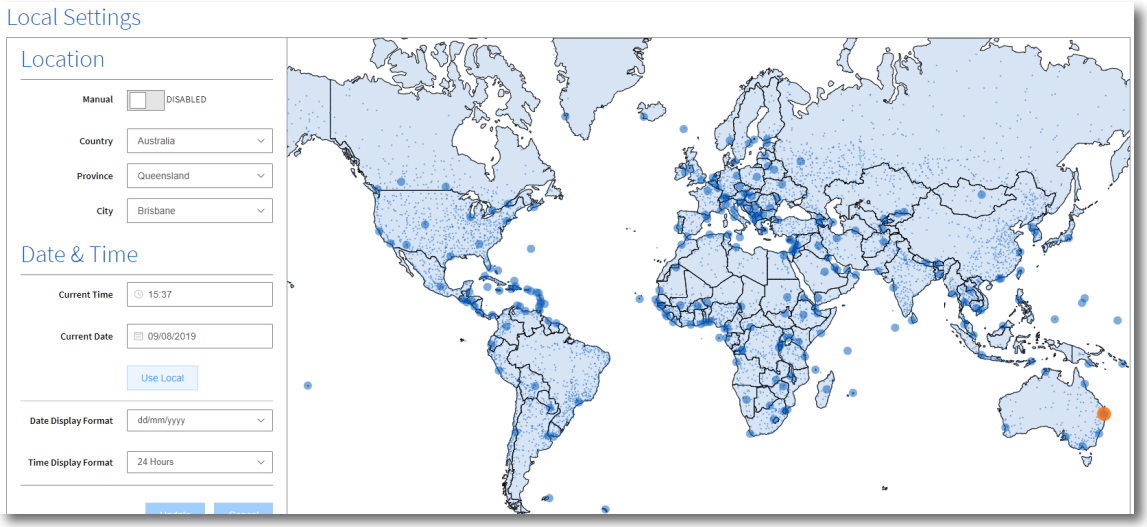


Figure 4-60: Settings - Date and Time Local Settings

When an Omni device is configured at Innotech address one (default), it is the Innotech time master and will time sync all attached Innotech devices connected to the Net and Global comms port.

Map and Manual Modes

1. To set the local time zone using Map mode, select the Country, Province (State) and City. Click Update to update the controller.
2. To set the local time zone using Manual mode, specify the Latitude, Longitude and select the Time Zone. Click Update to update the controller.

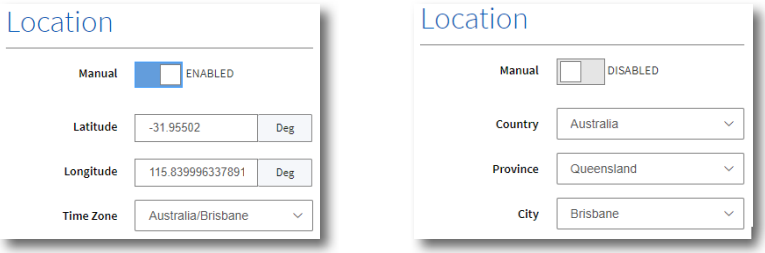


Figure 4-61: Settings - Date and Time Location Modes

IMPORTANT

- *Northern Latitudes are specified with a positive number, southern Latitudes should be specified with a negative number as in the right-side image above.*
- *Eastern Longitudes are specified with a positive number as in the right-side image above, western Longitudes should be specified with a negative number.*
- *Example: 27.45503S / 153.0351E is equal to -27.45503 / 153.0351.*

Daylight Savings

Click Daylight Saving to view Daylight Savings details for your selected timezone. If the selected Timezone does not have Daylight Savings, no information will be available.

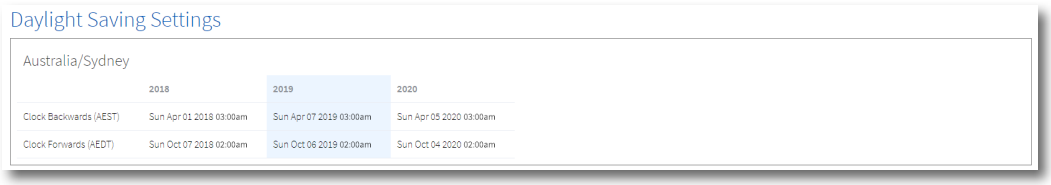


Figure 4-62: Settings - Date and Time Daylight Savings

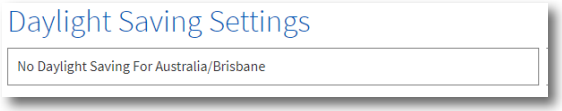


Figure 4-63: Settings - Date and Time Daylight Savings Unavailable

Network Time Protocol
Click NTP to set the Network Time Protocol (NTP) settings for the Omni controller.

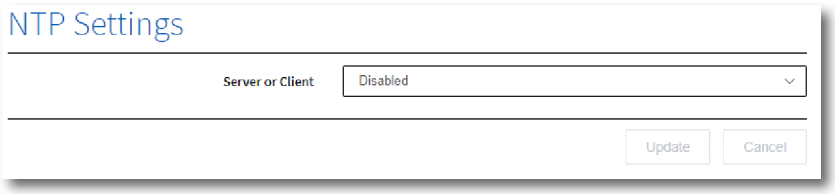


Figure 4-65: Settings - Date and Time NTP Settings

Server
Select Server from the combo box to set the Omni controller as the server for other devices on the network.

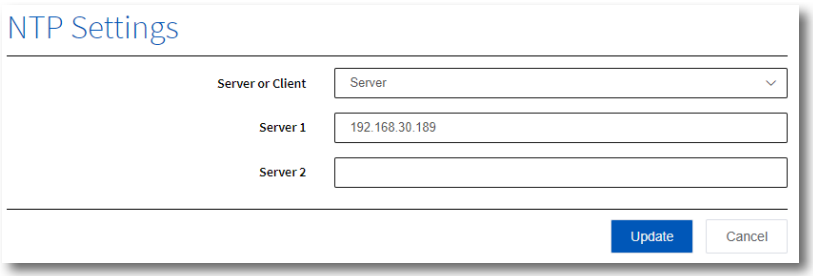


Figure 4-66: Settings - Date and Time NTP Server Settings

The Network Time Protocol is used to set this Omni's Time and Date via a NTP server. The configured Omni can then time sync any locally connected Innotech devices and BACnet devices, as described elsewhere, if required via the configurable options.

Client
Select Client from the combo box to enable the Omni controller to sync its time settings from a specified server. The server specified is an IP address. Two servers can be specified for a backup. The IP can be a Server specified Omni Controller or other time server available on your network.

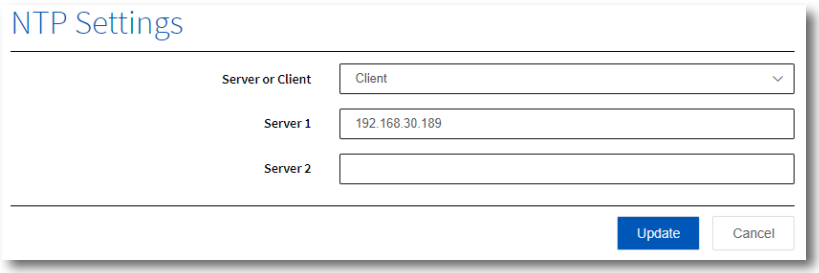


Figure 4-64: Settings - Date and Time NTP Client Settings

BACnet Time Sync
Select a Time Sync Accepted item from the combo and then click the Transmit Time Sync Enabled button to show further settings. The interval settings specifies the interval at which Time sync messages are transmitted.

After editing your settings, click Update to update your controller.

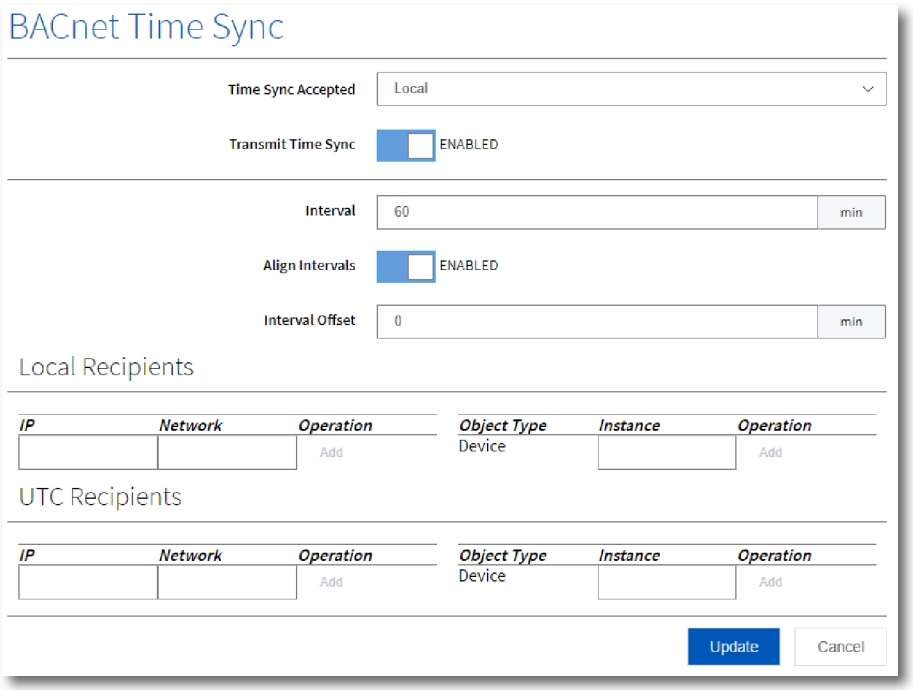


Figure 4-67: Settings - Date and Time BACnet Time Sync Settings

BACnet time sync is used to synchronise the date and time across a BACnet network. When the Transmit Time Sync is enabled the device is responsible for synchronising the recipient's date and time to match its own. The Recipient must be configured to accept Time Sync messages. For Omni devices this is done via the Time Sync settings, for other BACnet devices this would have to be configured as per their own settings.

Once configured the Omni device will transmit Time Sync messages based on the Interval and other settings selected. Both Local Time sync messages or UTC Time sync messages can be transmitted. Local Time syncs will set the Recipients date and time to exactly match the Master device. This is useful in situations where BACnet devices do not support Timezones. UTC Time syncs will cause the Recipients date and time to synchronise to the Masters but it will apply it's own timezone offset. This is useful in situations where the BACnet device support timezones and the BACnet network may be connected across multiple zones.

Best practice for Omni devices is to use UTC time syncs and have the Timezone set correctly.

Table 4-3: BACnet Time Sync Settings

Setting	Description
Time Sync Accepted	Can be set to None, Local, UTC or Both. This setting means that the device will accept Time Sync requests from other BACnet devices on the network. *Local* - The Local Time is uses to synchronise the recipient's date and time. This is best used when the recipient does not support timezones. *UTC* - The Global UTC Time is used to synchronise the recipient's date and time. This is best used when the recipient supports timezones. **Note**: The timezone needs to be correctly set on all devices.
Transit Time Sync	Enable this device as a Time Sync Master - this option will send time sync messages to the network.
Interval	Interval at which the time sync occurs.
Align Intervals	When enabled and the Interval is a factor of (divides without remainder) an hour or day, then the beginning of the period specified for time synchronisation shall be aligned to the hour or day, respectively.
Interval Offset	Allows the time sync to be offset by a number of minutes from the alignment with the hour or day. The offset used shall be the value of [Interval Offset] modulo [the value of Interval]. For example if Interval_Offset has the value 31 and Interval is 30, the offset used shall be 1 minute.
Recipient Lists	This table lists the Local and UTC recipients to be time synced with this device. You can enter information for Network devices, BACnet objects or both. All items listed will be synced.

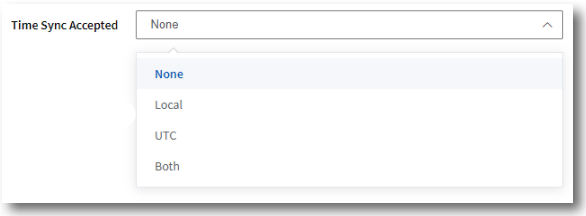


Figure 4-68: Settings - Date and Time BACnet Time Sync Accepted

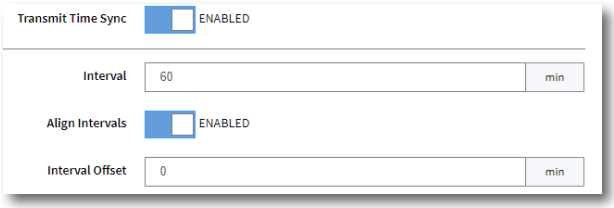


Figure 4-69: Settings - Date and Time BACnet Transmit Time Sync

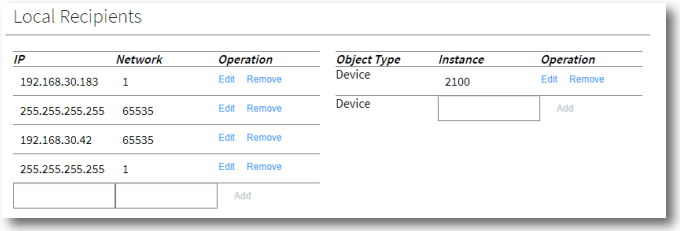


Figure 4-70: Settings - Date and Time BACnet Time Sync Recipients

Table 4-4: Recipient Settings via BACnet Address

Network	Address	Network			Address		
	Node/IP	Specific	Local	Global	IP	MS/TP Node	Broadcast
1	192.168.x.x	✓	×	×	✓	×	×
1	255.255.255.255	✓	×	×	×	×	✓
1	110	✓	×	×	×	✓	×
0	192.168.x.x	×	✓	×	✓	×	×
0	255.255.255.255	×	✓	×	×	×	✓
0	110	×	✓	×	×	✓	×
65535	192.168.x.x	×	×	✓	✓	×	×
65535	255.255.255.255	×	×	✓	×	×	✓
65535	110	×	×	✓	×	✓	×

Network Number values in the table relate to the following: 1-65534 (a specific Network on the BACnet Internetwork), 0 (Local Broadcast), 65535 (Global Broadcast).

To send a Time sync to a specific BACnet MS/TP device then specify the MSTP Node Addresses of the device (0-255). To broadcast to all MSTP devices then use the Broadcast Address of 255.255.255.255.

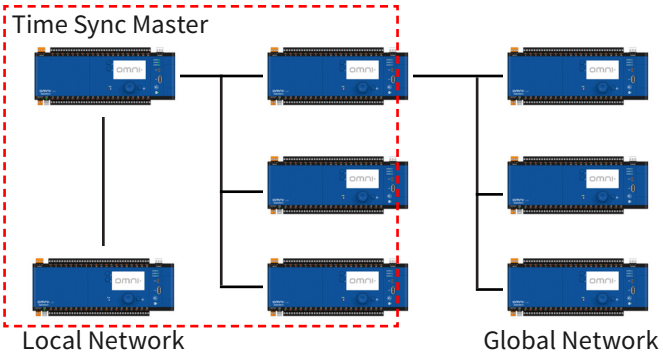


Figure 4-71: Settings - Date and Time Indicative Network Layout

Local BACnet Network devices are connected to the Time Sync Master. Global BACnet network devices are connected via devices connected to the Time Sync Master.

4-2.9.5 Web Access

General

The General Settings page is for changing the web access settings for the controller. After changing the settings, click Update to update the Omni Controller.

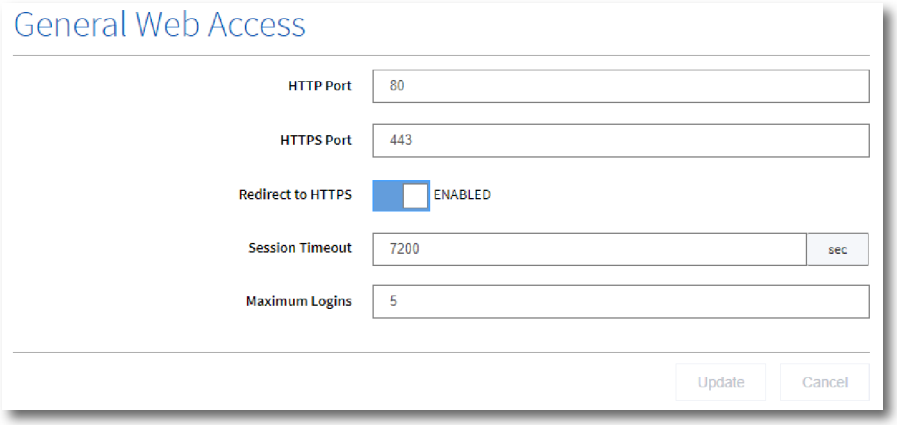


Figure 4-72: Settings - Web Access - General

HTTPS Information

Introduction

HTTPS connection is a protocol for secure communication over a computer network which is widely used on the Internet.

HTTPS provides two main benefits to the user.

1. Trust
   It provides authentication that the webserver you want to communicate to is actually the one you think it is. This protects against man-in-the-middle attacks.
2. Encryption
   It provides bi-directional encryption of communications between a client and server, which protects against eavesdropping and tampering with or forging the contents of the communication.

From the page (shown on the previous page) you have the ability to specify a secure HTTPS port. Enabling Redirect to HTTPS will ensure that if the IP is entered in the browser without HTTPS, it will automatically redirect the browser to the secure page.

On sites that the Omni is port forwarded to an external IP and you want to use https, you will also need to port forward the HTTPS port as well as the HTTP port.

By default HTTPS is always available it you want to use it. To use HTTPS, simply enter in a browser *https://IPAddress* like below.

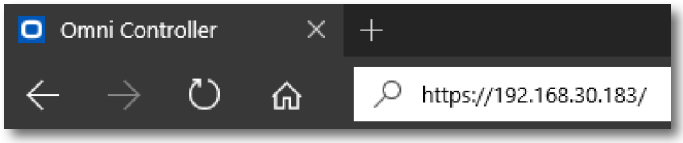


Figure 4-73: Settings - Web Access - HTTPS Address In Browser

Certificate Information & Installation
By installing a certificate on your computer or tablet, your Omni connection will become a trusted connection. Browsers can give you information about the https connection. Normally by the colour of the https lock will let you know if the connection is secure. For example: in Chrome (computer) you can get more information by clicking on the https lock and get access to the following information by clicking on the Details link.

If a certificate is not installed, you may see a screen like below.

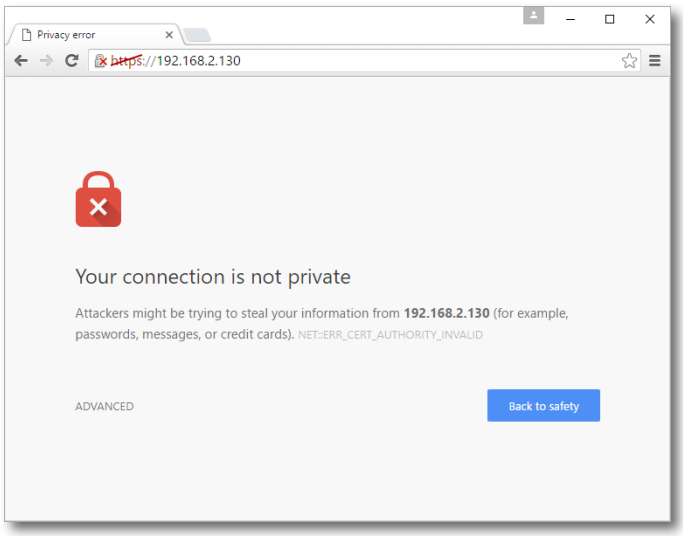


Figure 4-74: Settings - Web Access - Untrusted Connection (Chrome)

This error means that the browser cannot verify the trust component of HTTPS. If the user continues the connection is still secure, but the Omni certificate is unknown to the browser. The browser doesn't know if the certificate is really who it says it is and therefore tells the user that there might be an issue.

You can continue on from this error by clicking advanced and the connection will still be secure, however it will always have a red line through https whenever you go to this device.

Browsers base trust on if the certificate is chained or derived from a "Trusted Root Certificate Authority" certificate that is installed into the browser's certificate store by default. There are many places you can get or purchase certificates from. The free certificates expire after about 60 days, and the longest one you can purchase works for about 3 years.

As such we are unable to install a trusted certificate into the Omni by default as eventually they will expire and also you have to purchase them for a particular domain the site will be using.

We have made and Innotech "Trusted Root Certificate Authority" certificate which the user can import to their computer or device and when they access any Omni controller anywhere, the browser will trust it and you will not get any warnings or red locks symbols etc.

For a business with a managed IT network, the IT department would be able to include our certificate to be automatically installed into the machines they manage. However, you can also manually do it various ways. The certificate must be installed into the "Trusted Root Certificate Authorities" certificate store on your computer.

Certification Installation - Computer

1. Double click the certificate file and click Install Certificate.

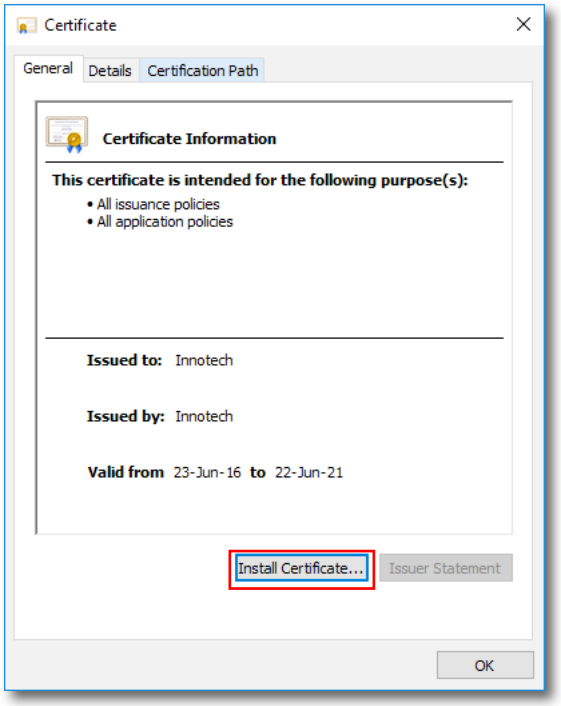


Figure 4-75: Settings - Install Certificate Window

The Innotech Certificate is available for free by contacting your Innotech representative.

2. Select Current User or Local Machine (depending on your preference) and click Next.

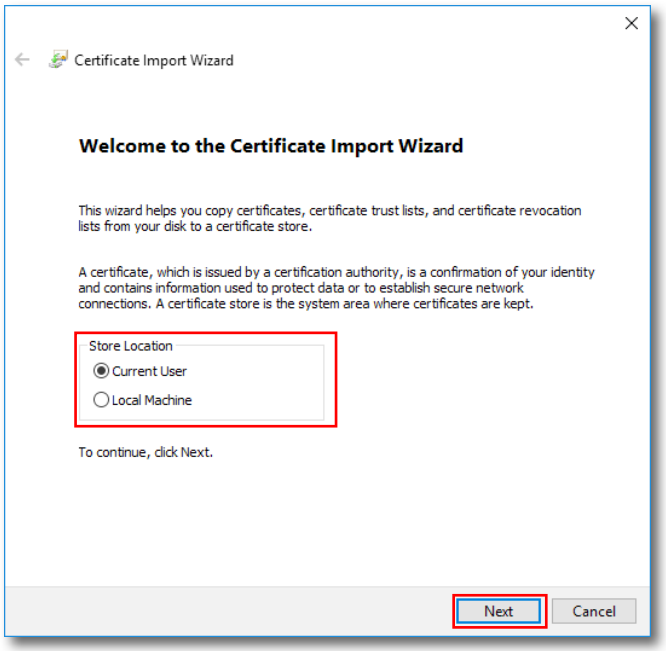


Figure 4-76: Settings - Certificate Import Wizard

3. Select "Place all certificates in the following store" and click Browse. In the window, select "Trusted Root Certification Authorities" and click OK. Click Next and OK to finish installing the certificate.

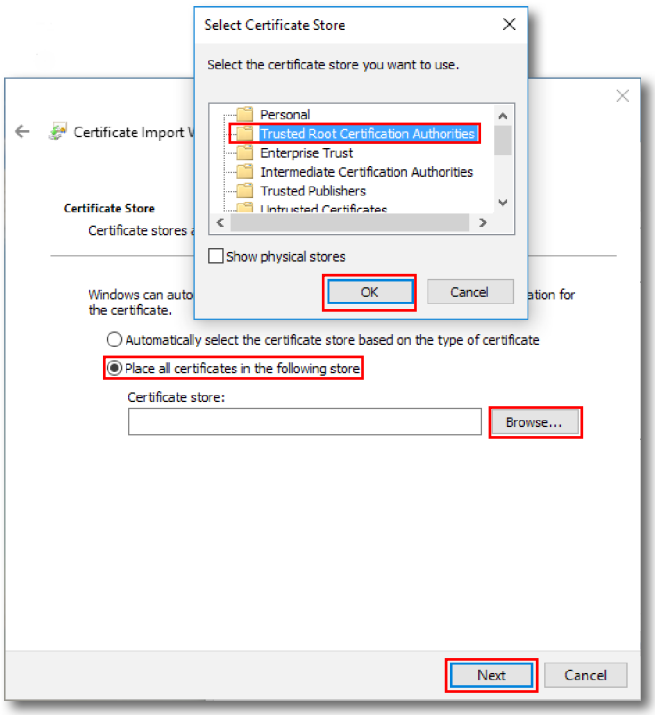


Figure 4-77: Settings - Select Certificate Store

Certification Installation - Android
This procedure provides details on installing HTTPS Certificates on the most common Android tablet types.

Installation of the security certificate on an Android device requires that a secure pin, password or security pattern be set on the device.

1. Connect your Android tablet to your computer via a USB cable. You may be asked if you wish to allow access via USB, if so select Yes.

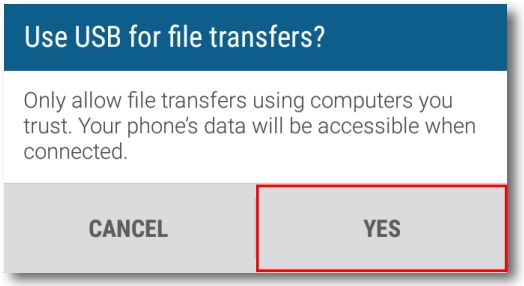


Figure 4-78: Settings - Android Certificates (USB Confirmation)

2. Copy the innotech-omni-CA.crt file to your Android device.
3. Find the file on your Android device and press on the .crt file to open.
4. Press OK.
   If you do not have security setup on your device, a popup appears which says "To use credential storage, set the screen lock type pattern, PIN or password". Set a code or pattern.

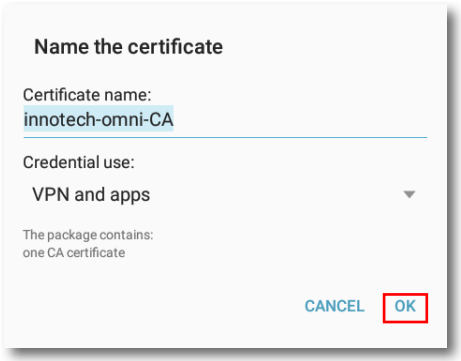


Figure 4-79: Settings - Android Certificates (Name the Certificate)

5. After installation, "Innotech Omni CA installed" will appear on the screen.

Figure 4-80: Settings - Android Certificates (Install Confirmation)

To view the certificate:
Samsung Tab A (v6.0.1): Go to Settings > Lock Screen and Security > Other Security Settings > View Security Certificates. Tap on Users. Tap Innotech Pty Ltd to view the details of the security certificate.

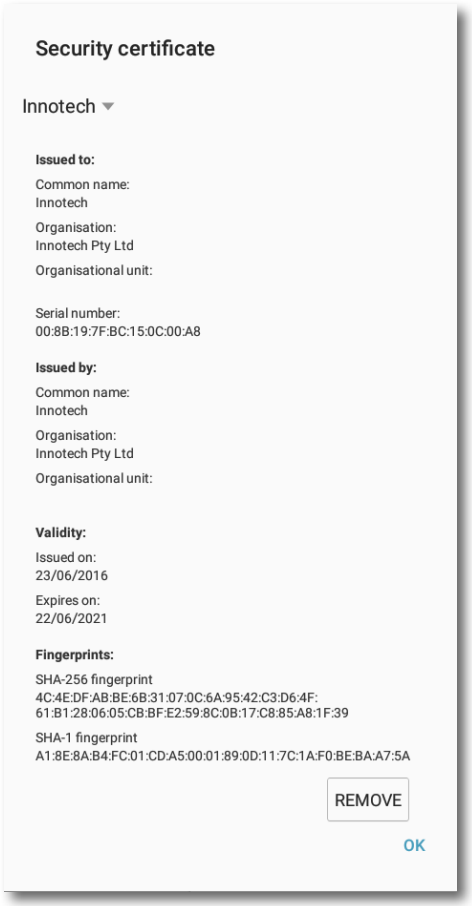


Figure 4-81: Settings - Android Certificates (View Certificate)

The Android procedure was tested with Android v6.0.1 using a Samsung Galaxy Tab A.

Android is a registered trademark of Google Inc.

Certification Installation - iPad

This procedure provides details on installing HTTPS Certificates on the iPad tablets.

The easiest way to install a HTTPS Certificate on an iPad is by sending the certificate to the iPad via email.

1. Once the file is downloaded, press on the file.
2. After pressing on the file, the iPad will show some notices about being a trusted file and the verified Innotech security certificate is ready for use.
3. The certificate can be found in:
   Settings > General > Profile > Innotech > Certificate

After installation a secure connection should be seen when connecting to your device.

If email is unavailable on your device, you can copy the certificate to your device using iTunes.

Viewing the Certificate

1. In the settings select General and press Profile.

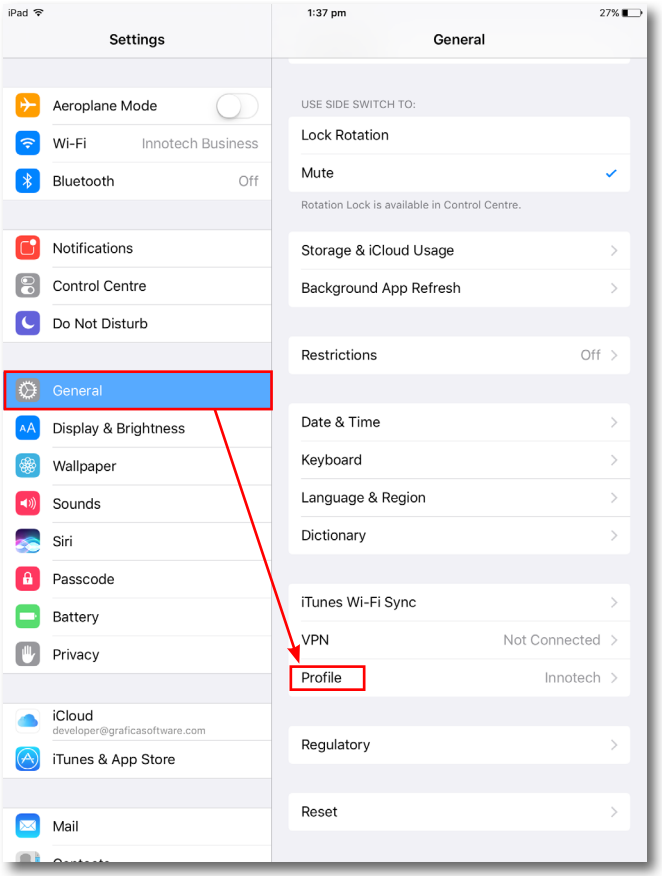


Figure 4-82: Settings - iPad Certificates (General Settings)

2. Press the Innotech Profile.

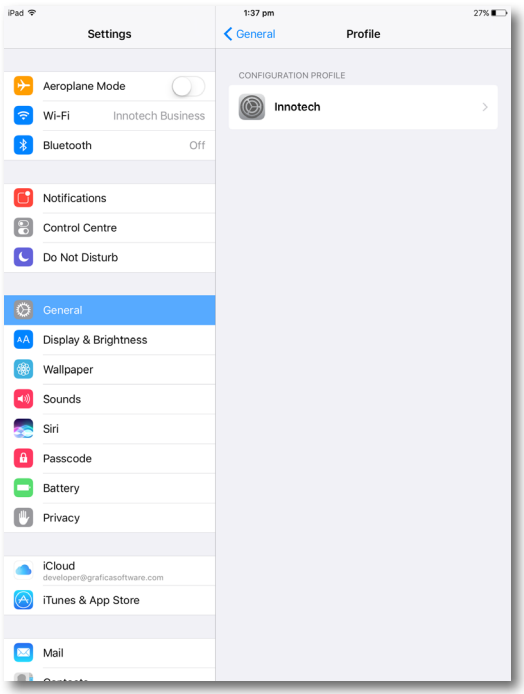


Figure 4-83: Settings - iPad Certificates (Available Profiles)

3. The certificate will be shown.

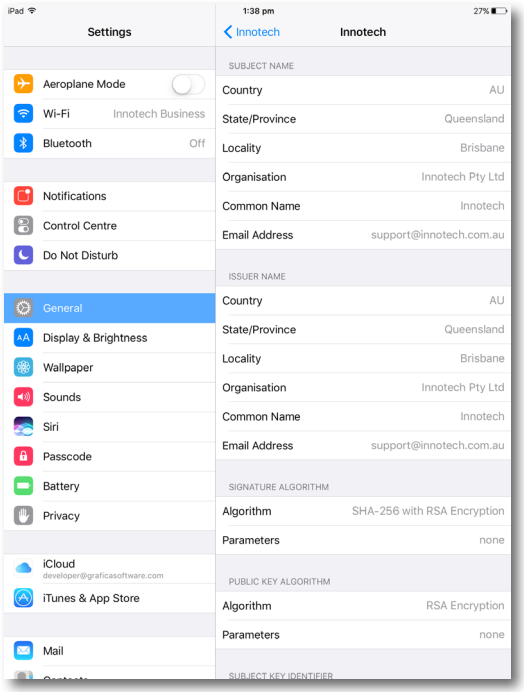


Figure 4-84: Settings - iPad Certificates (Profile Details)

iOS *The iPad procedure was tested with an iPad Mini 2 using iOS® 10.*
IOS® is a registered trademark of Cisco Inc., licensed to Apple Inc.

Images

The Images Settings page is for changing the Site Logo and Wallpaper for the Log In screen. Click Select File and a dialog box will open for selecting your desired image file. Click Update to update the Omni controller after selection. Image types include and are not limited to .bmp, .gif, .jpg & .png. Files should be limited to 2MB.

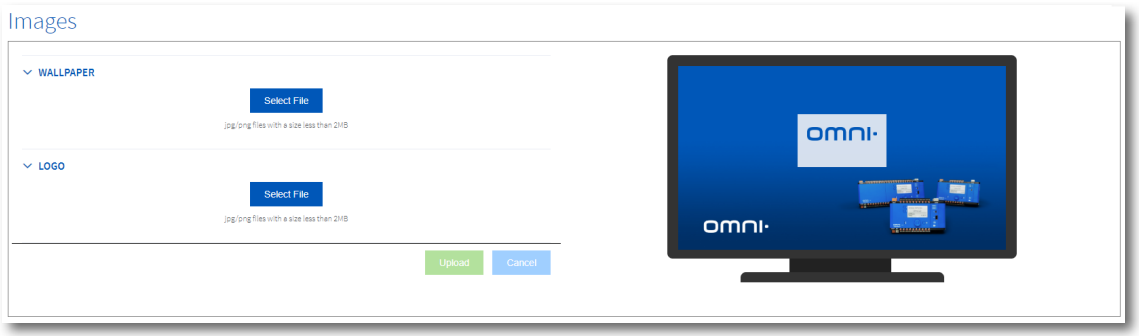


Figure 4-85: Settings - Web Access - Images

Network

The Network Settings page is for setting access to the Omni network. Select the Access Type (Internal Access or External Access) from the combo box.

Enter an IP Address and click the green add button to add Omni controllers to the Web Server network. The order that devices are added in this screen is the order devices are shown on the Network tab when sorting by default. Device names will be determined from the Device settings.

Devices listed here can be accessed (after login) from the Network screen.

Click Update to update the Omni controller after making changes (restart required).

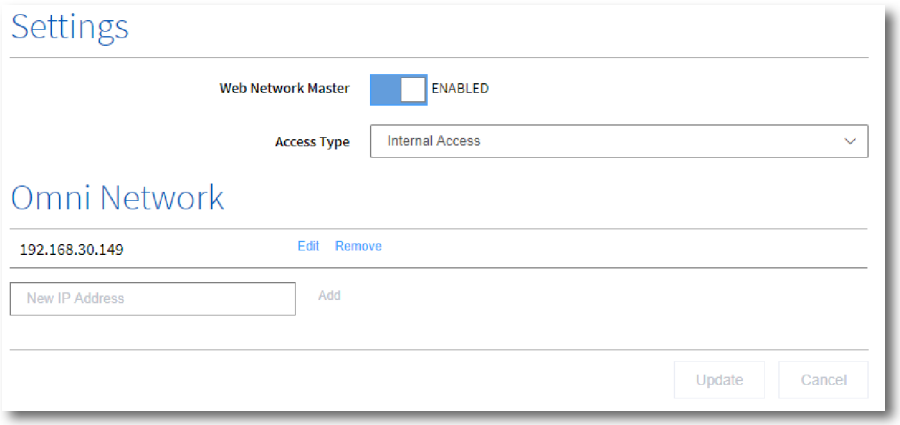


Figure 4-86: Settings - Web Access - Network

4-2.9.6 Security

SSL Certificate

All Omni controllers can generate security certificates for connecting to your controller using https. In this section, choose to either use the Omni generated security certificate or a 3rd party certificate. Add an Alternative Name (DNS) if required and click Update, then click Regenerate Certificate to create a new Security Certificate.

IMPORTANT

Regenerating a new certificate will erase the existing certificate.

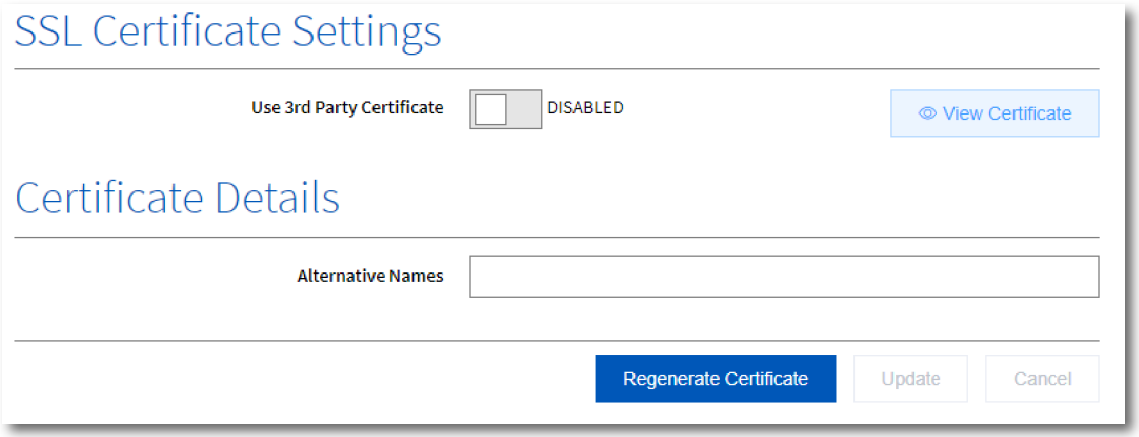


Figure 4-87: Settings - Security - Use Omni Certificate

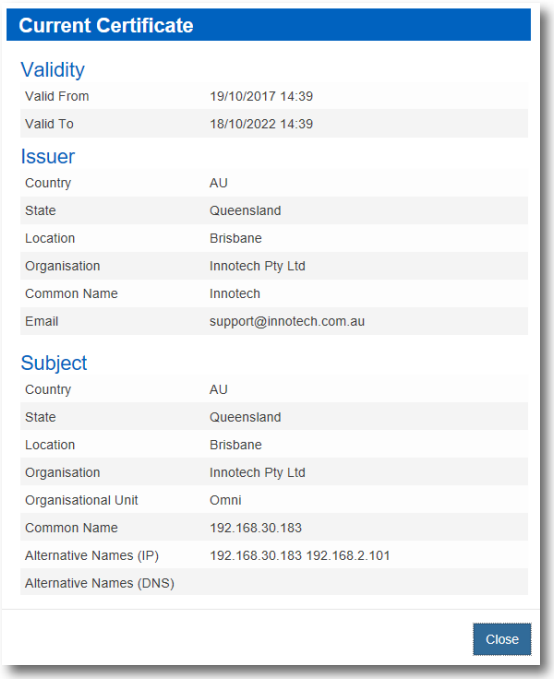


Figure 4-88: Settings - Security - View Current Certificate

3rd Party Certificates
Click the button use 3rd Party Certificates to prepare a Certificate Signing Request for your 3rd party certificate provider or to upload your certificate.

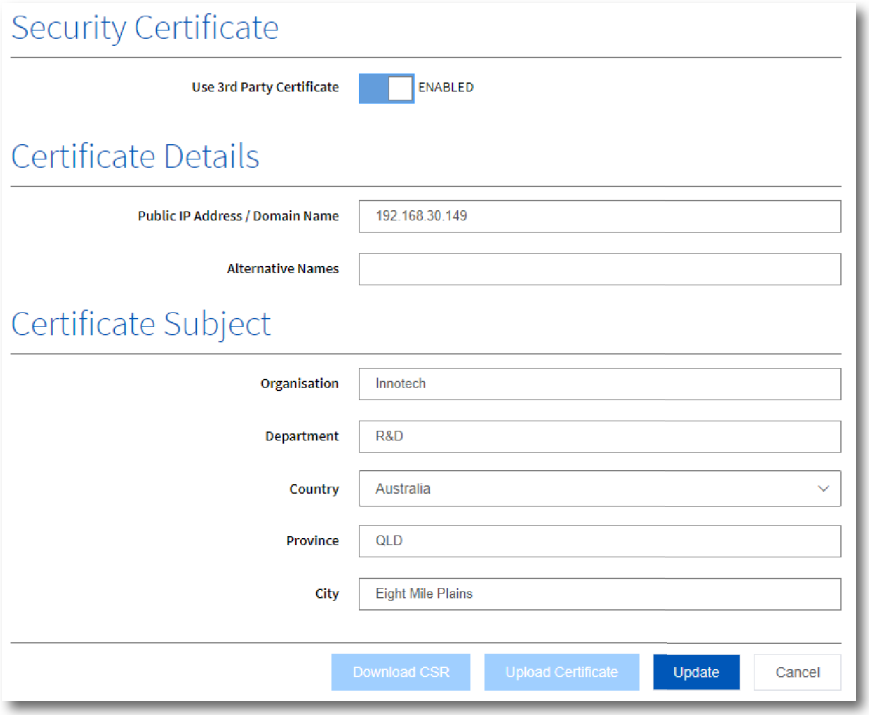


Figure 4-89: Settings - Security - Enable 3rd Party Certificates

IMPORTANT
Use with caution, downloading a new CSR will invalidate any previous CSR's that you have not uploaded certificates for.

Before uploading a 3rd party certificate you need to send your CSR (Certificate Sigining Request) file to the 3rd party certificate supplier.

1. Fill in the Certificate Details and Certificate Subject section.
2. Click Update.
3. Click Download CSR, read the warning, click Continue and save the file to your computer.
4. The CSR needs to be provided to the certificate supplier. Once approved, they may send you back a .crt file or they will the security certificate code to be pasted into a text file, which should be saved with a .crt extension.

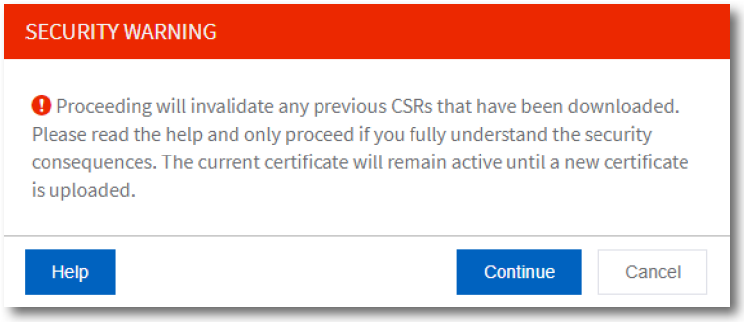


Figure 4-90: Settings - Security - Download CSR Warning

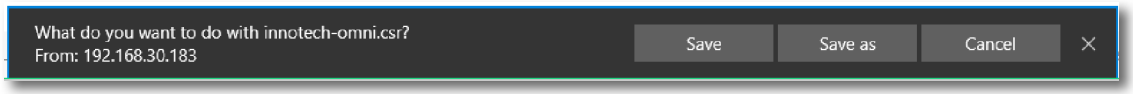


Figure 4-91: Settings - Security - CSR Save Dialogue

5. Click Upload Certificate, read the security warning and click Continue.
6. Use the dialog to select your certificate file to upload to the controller.

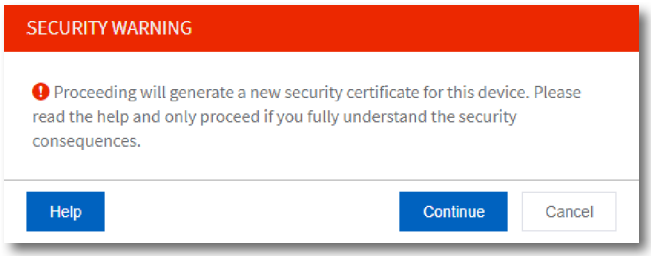


Figure 4-92: Settings - Security - Security Warning

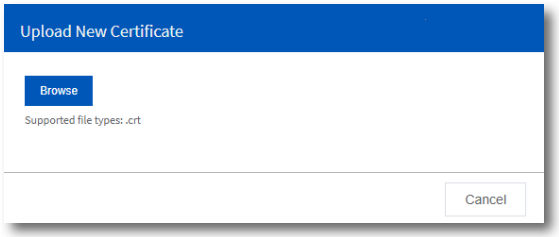


Figure 4-93: Settings - Security - Upload New Certificate Dialogue

Data Sharing
When linking your calendar software such as Outlook to your Omni controller, use the IP address listed here.

The URL's and Username is not editable, only the Password can be changed. After entering a new password, click Update to save your changes.

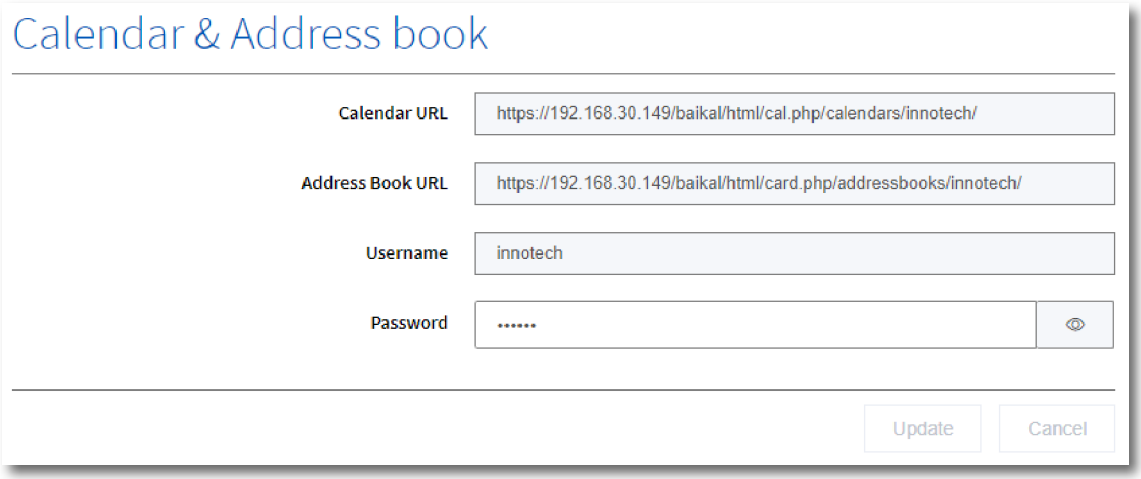


Figure 4-94: Settings - Security - Data Sharing

Config Protection
Click Enable or Disable to configure the Configuration Security loaded onto the device.
Click Update to save your changes.

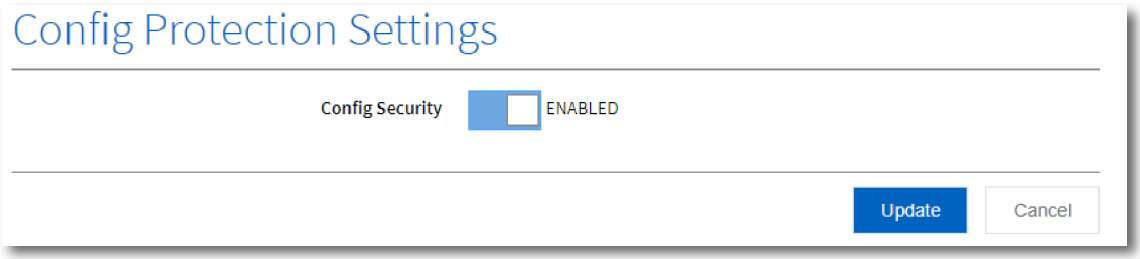


Figure 4-95: Settings - Security - Config Security

4-2.9.7 Display Access

The Display Access Settings page is for setting access control and session timeout for the controller HMI (if fitted).

Click Update to update the Omni controller after making changes.

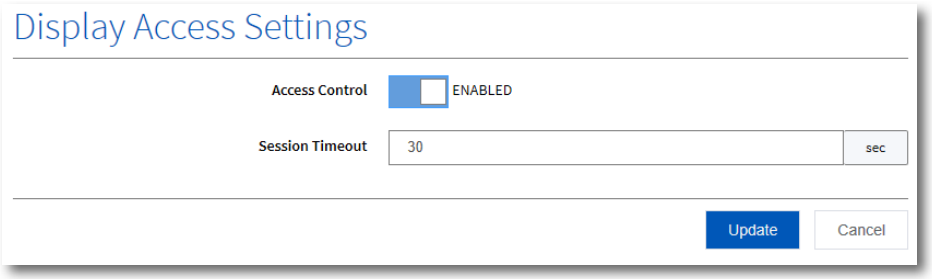


Figure 4-96: Settings - Display Access

4-2.9.8 Logging

The Logging settings are for specifying the default diagnostic log interval and the system log level.

1. Change the settings as required.
2. Click Update to update the Omni Controller.

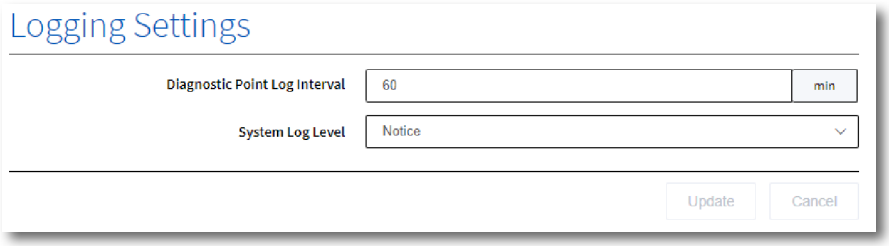


Figure 4-97: Settings - Data Logging

System Log Level

The System Log Level combo specifies what data is logged.

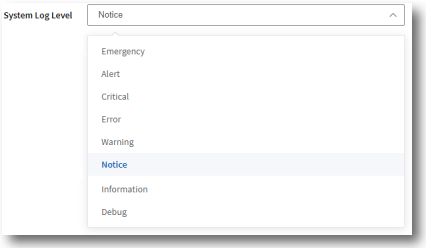


Figure 4-98: Settings - System Log Levels

Table 4-5: System Log Levels

Log Level	Description
Emergency	Severe error events, system unusable.
Alert	Severe error events that would require immediate action.
Critical	Severe error events, critical condition.
Error	Error event that might still allow the system to continue running.
Warning	Message about potentially harmful situations.
Notice	Messages that highlight the progress of the system at the highest level.
Information	Messages that highlight the progress of the system at a course-grained level.
Debug	Events that are most useful to debug an application, contains detailed info per operation.

4-2.9.9 System Units

This section is used for setting the system units for the Omni controller. By default this setting will be set to Auto Detection Enabled. When this setting is set to Auto Detection, the time zone will determine if the system units will be Metric or Imperial.

If you wish to manually choose the system units, click the slider to disable the Auto Detection and select Metric or Imperial from the Units combo box.

This setting can only be set using the Web Server and cannot be changed using the HMI.

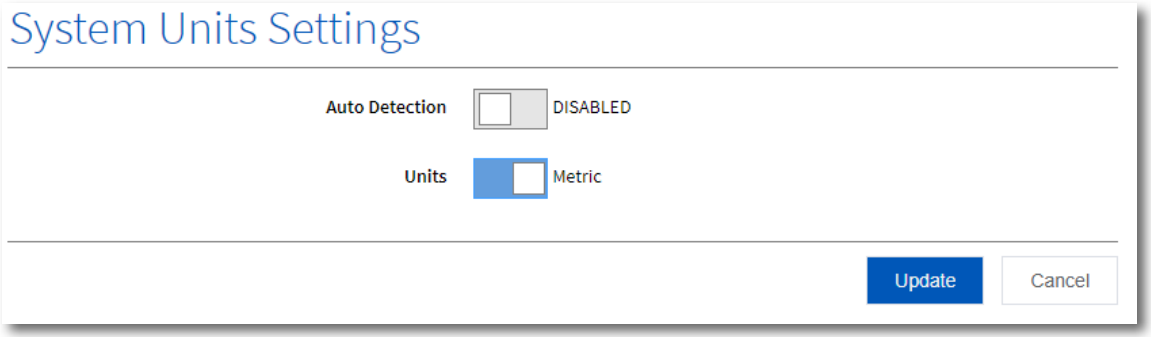


Figure 4-99: Settings - System Units - Auto Detection Enabled

4-2.9.10 Access Levels

This section is used to view access level groups. There are 6 preset access levels: Commissioner, Engineer, Facility Manager, Adjuster, Observer and Administrator as well as No Access. Each level has different access allowed to the web server. These access levels cannot be edited. You can, however, enable or disable contact hours for a group.

The Omni web server also has 3 fully customisable access levels.

After editing a custom item, click Update to update your Omni Controller.

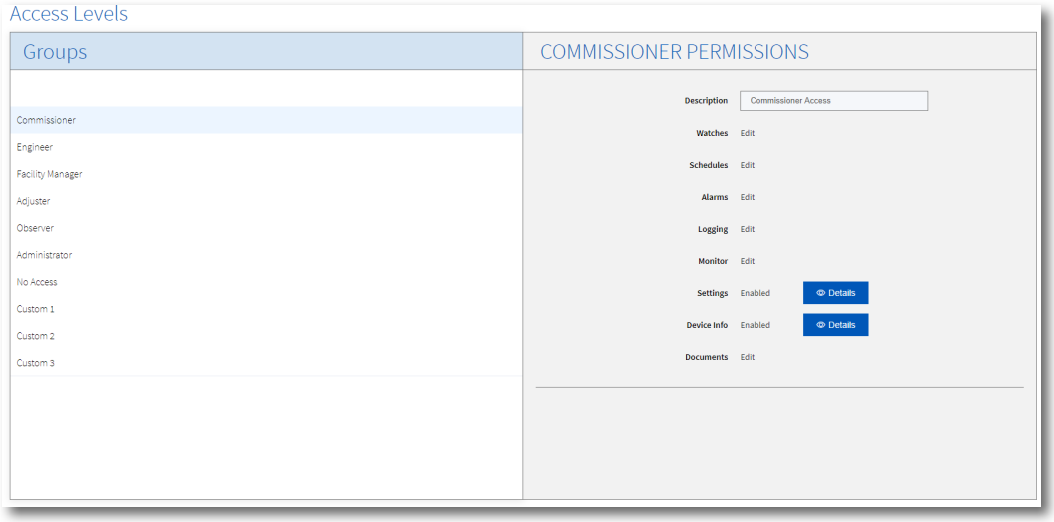


Figure 4-100: Settings - Access Levels

Table 4-6: Access Levels

Access Level	Permissions							
	①	②	③	④	⑤	⑥	⑦	⑧
Commissioner	Edit	Edit	Edit	Edit	Edit	Enabled	Enabled	Edit
Engineer	Edit	Edit	Edit	Edit	Edit	Enabled	Enabled	Edit
Facility Manager	Edit	Edit	Edit	Edit	View	Enabled	Enabled	Edit
Adjuster	Edit	Edit	Edit	Edit	None	Enabled	Enabled	View
Observer	View	View	View	View	None	Disabled	Enabled	View
Administrator	None	None	None	None	None	Enabled	Enabled	None
No Access	None	None	None	None	None	Disabled	Disabled	None

1. Watches
2. Schedules
3. Alarms
4. Logs
5. Monitor
6. Settings
7. Device Info
8. Documents

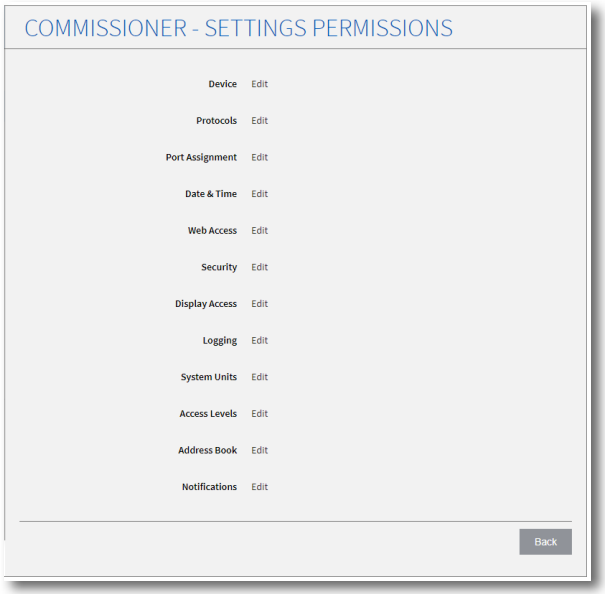


Figure 4-101: Settings - Access Levels Settings Permissions

Table 4-7: Access Levels - Settings Permissions

Access Level	Permissions										
	1	2	3	4	5	6	7	8	9	10	11
Commissioner	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit
Engineer	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit	Edit
Facility Manager	None	None	None	Edit	None	None	None	None	None	None	None
Adjuster	None	None	None	Edit	None	None	None	None	None	None	None
Observer	-	-	-	-	-	-	-	-	-	-	-
Administrator	None	None	Edit	Edit	None	None	None	None	Edit	Edit	Edit
No Access	-	-	-	-	-	-	-	-	-	-	-

1. Device
2. Protocols
3. Port Assignment
4. Date & Time
5. Web Access
6. Display Access
7. Logging
8. System Units
9. Access Levels
10. Address Book
11. Notifications

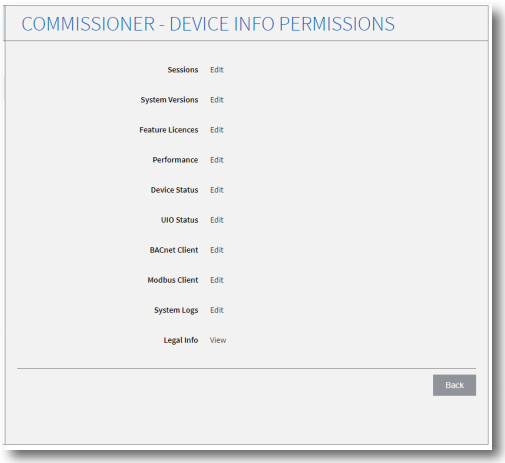


Figure 4-102: Settings - Access Levels Device Info Permissions

Table 4-8: Access Levels - Device Info Permissions

Access Level	Permissions								
	1	2	3	4	5	6	7	8	9
Commissioner	Edit	Edit	Edit	Edit	Edit	Edit	Edit	View	Edit
Engineer	Edit	Edit	Edit	Edit	Edit	None	Edit	View	None
Facility Manager	Edit	View	View	View	View	None	View	View	None
Adjuster	View	View	View	View	View	None	View	View	None
Observer	-	-	-	-	-	-	-	-	-
Administrator	Edit	View	View	View	View	None	View	View	None
No Access	-	-	-	-	-	-	-	-	-

1. Sessions
2. System Versions
3. Performance
4. Device Status
5. UIO Status
6. BACnet Client
7. System Logs
8. Legal Info
9. PHP Info

Creating a Custom Access Level

1. Name your custom access level.
2. Click an option for each item in the list.
3. If enabling Settings or Device Info permissions, click the Details button to customise each section. Click Update when done.
4. After you have completed the changes, click Update to update the controller.

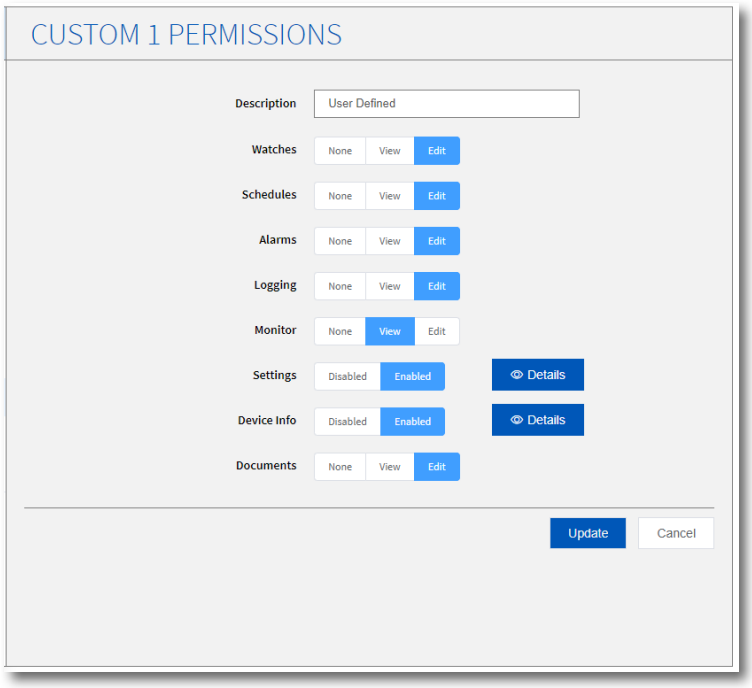


Figure 4-103: Settings - Custom Access Levels

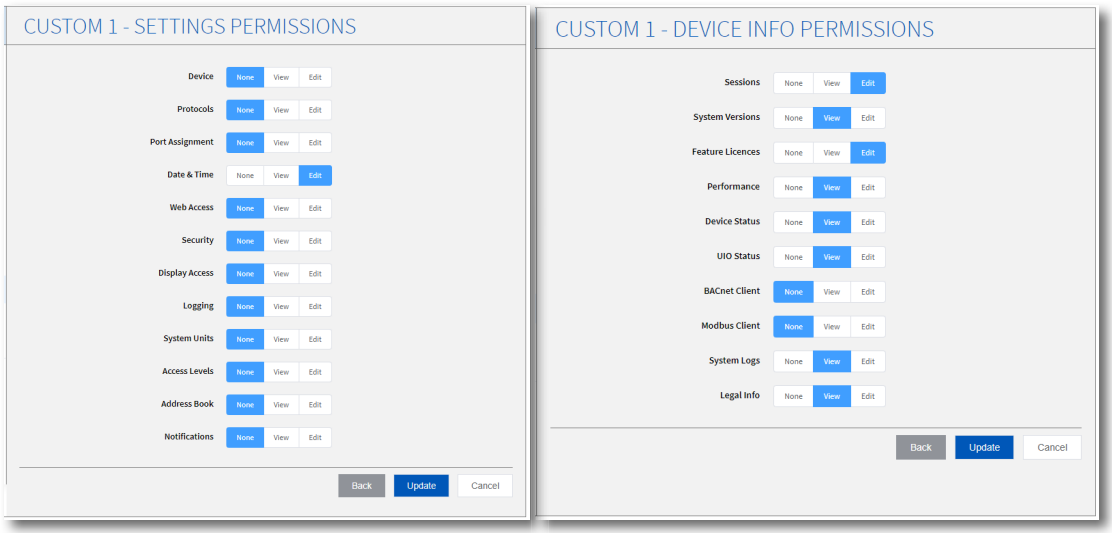


Figure 4-104: Settings - Custom Settings/Device Info

4-2.9.11 Address Book

Use the Address Book to add new user access to the controller. You must have sufficient access to be able to add new users. Only Commissioner, Engineer and Administrator level users can access the Address Book to add a user.

Add a new User

1. Add a new user by clicking the Add button
2. Fill in the fields and click Update to add the user.

Figure 4-105: Settings - Add User Button

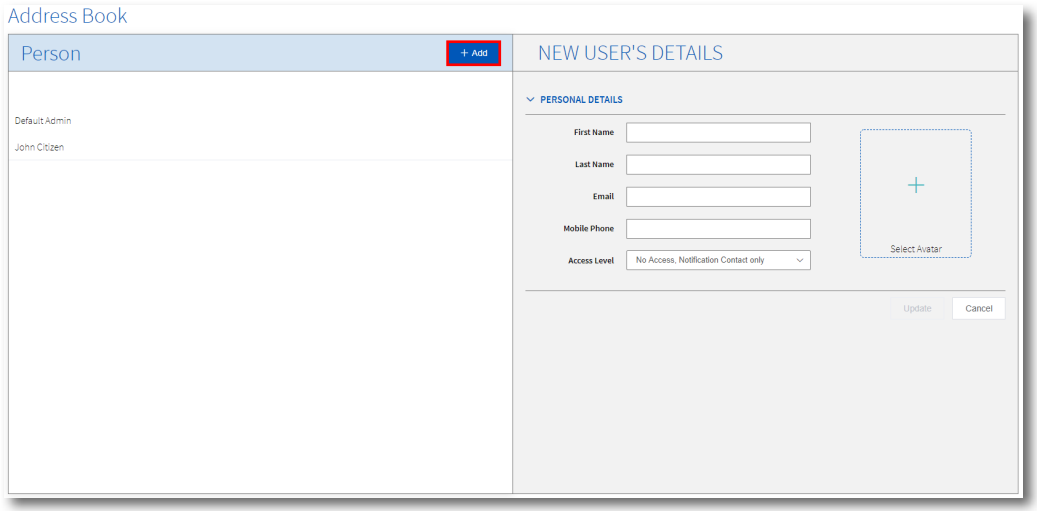


Figure 4-106: Settings - Add User Details

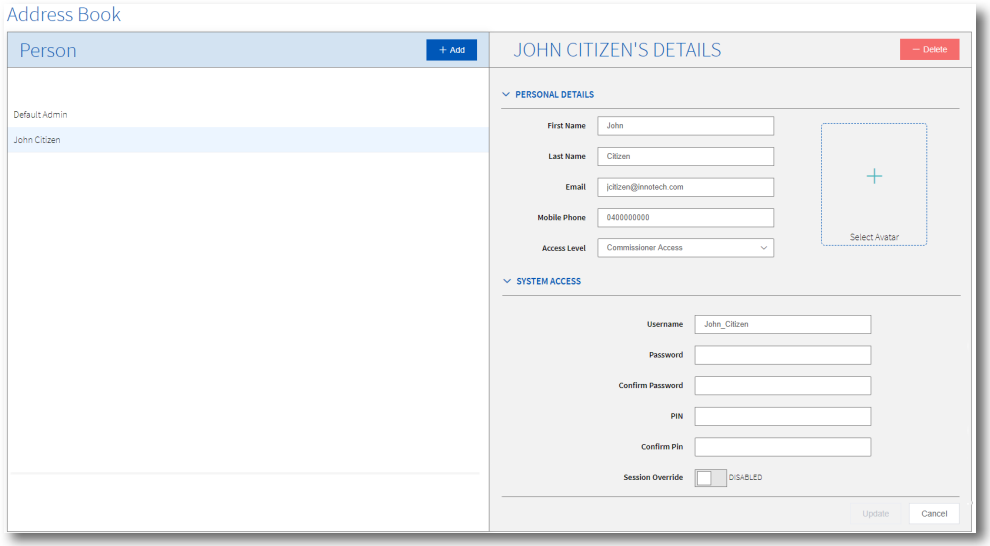


Figure 4-107: Settings - New User Details

Select an Avatar

1. Select a Person.
2. Click the Plus button to open the file browser.
3. Select a file and click Open.
4. Click Update to save the Avatar for the selected Person.

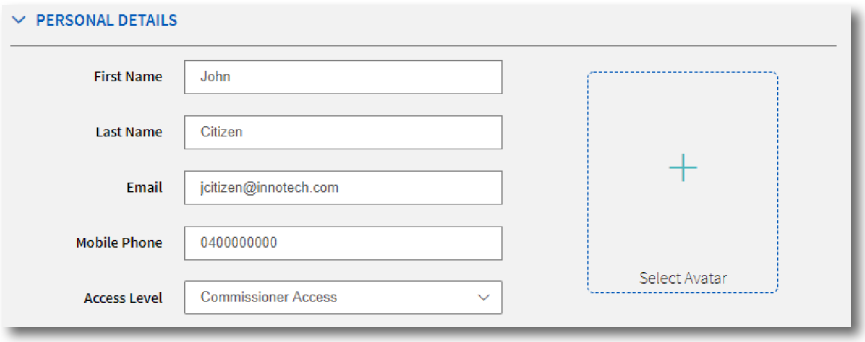


Figure 4-108: Settings - Add User Details

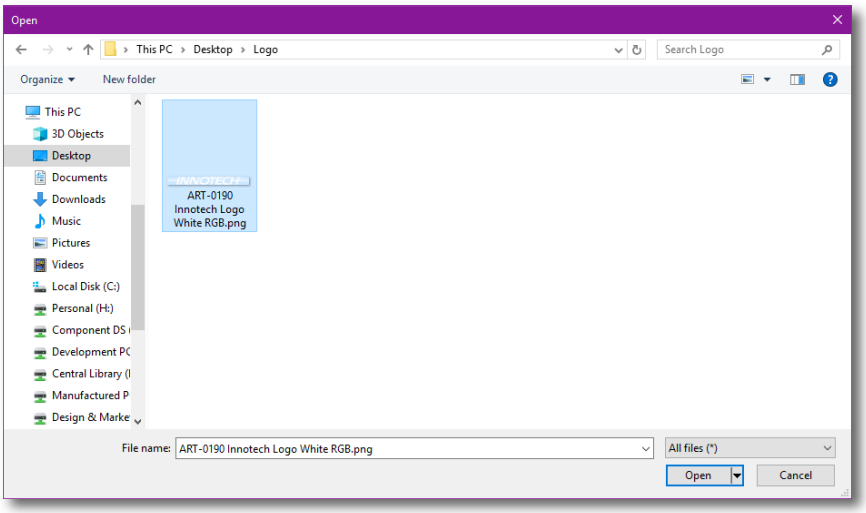


Figure 4-109: Settings - Add User Details

Delete a User

1. Select the user from the list.
2. Click the Delete button.

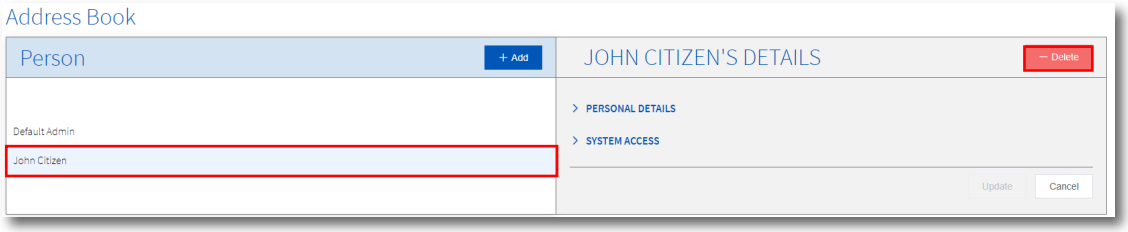


Figure 4-110: Settings - Select User for Deletion

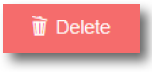


Figure 4-111: Settings - Delete Button

4-2.9.12 Notifications Type

The Notifications screen is for setting up Email and or Text Message alerts.

Email Notifications

1. Click Enabled to enable Email alerts.
2. Fill in the required details.
3. Click Update to update the Omni Controller when done.

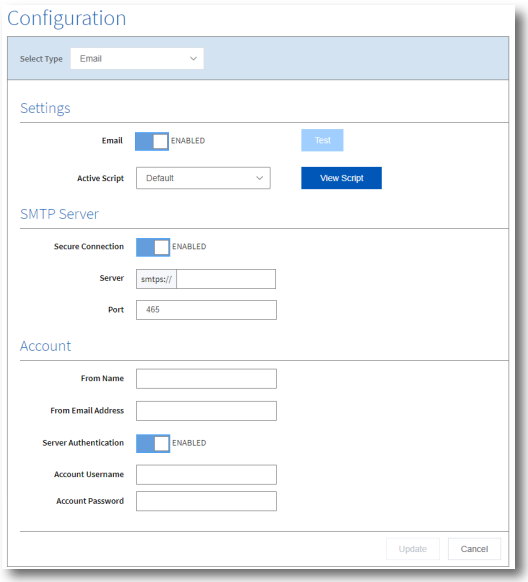


Figure 4-112: Settings - Notifications (Email)

Email Script

- Select the active email script - Default or Custom.
- When Custom is selected, you can click the copy button to copy a script for editing.

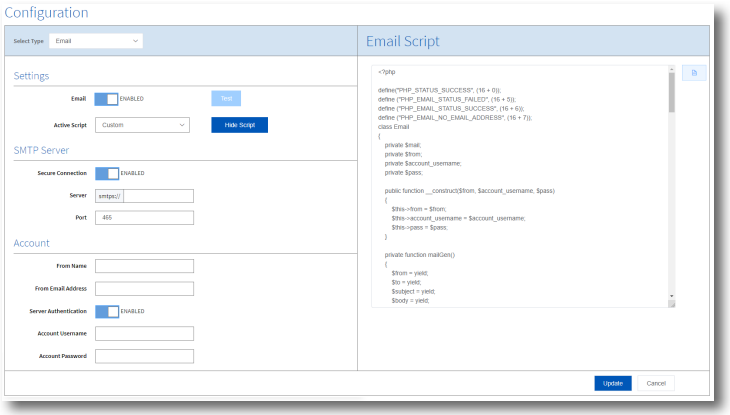


Figure 4-113: Settings - Notifications (Email Script Settings)

Text Message Notifications

1. Click Enabled to enable Text Message alerts.
2. Fill in the Server Phone Number details.
3. Click Update to update the Omni Controller when done.

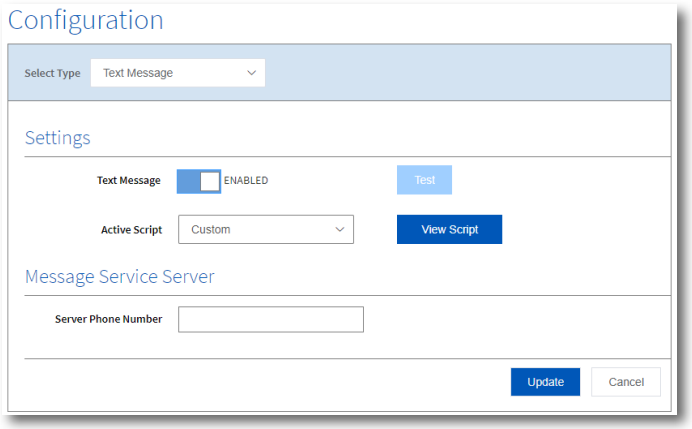


Figure 4-114: Settings - Notifications (Text Message)

Text Message Script

- Select the active script - Text-SAM2W, Text-SAM3GQ-USB or Custom.
- When Custom is selected, you can click the copy button to copy a script for editing.

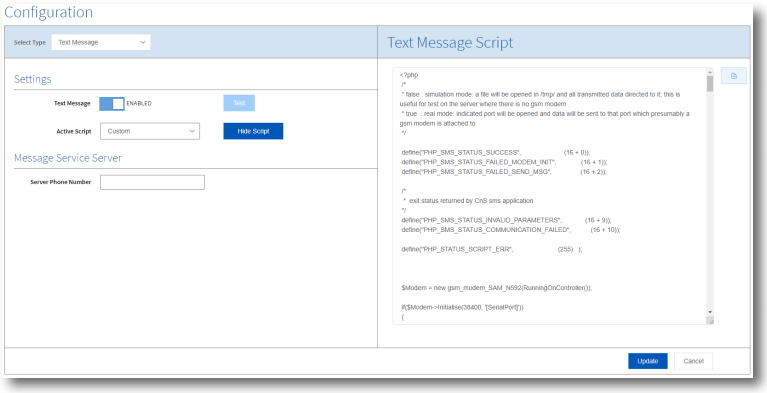


Figure 4-115: Settings - Notifications (Text Message Script)

4-2.9.13 Notifications Messages

The Notifications Messages screen is for setting up Email and or Text Message messages. You can create custom email and text messages. System Email and Text messages are provided by default for Omni System Alert messages.

IMPORTANT

Text Messages are suited to smaller alert messages.
Text messages may be truncated at 160 characters due to the limitations of the text messaging system.
If you require a message with multiple alarms, email would be more suitable.

Creating a new Message

1. Click the Add Button to create a new message.
2. Fill in a Name for the message and select Message Type from the combo.

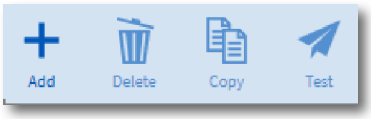


Figure 4-116: Settings - Notifications (Action Buttons)

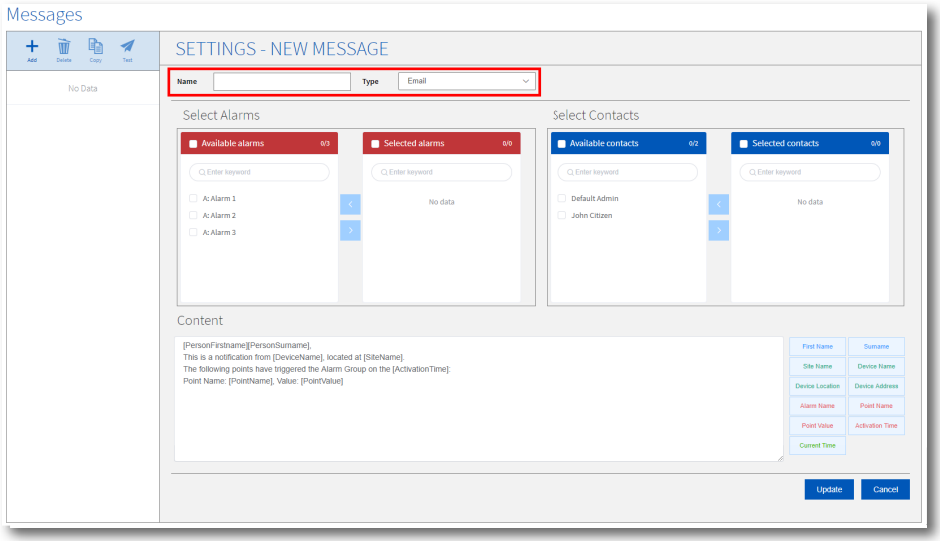


Figure 4-117: Settings - Notifications (Message Settings)

3. Select the Alarms for the message by clicking one or more alarms on the left.
4. Click the move button (highlighted in the blue rectangle) to move alarms from Available to Selected.

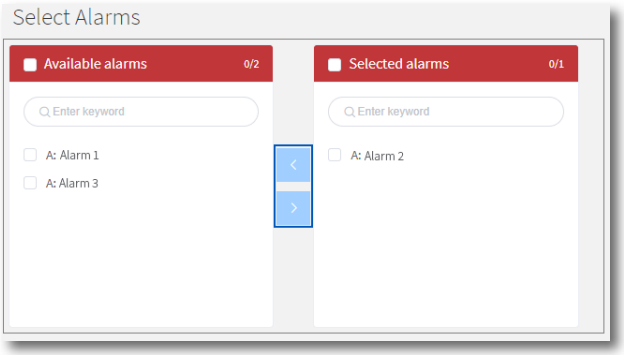


Figure 4-118: Settings - Notifications (Select Alarms)

5. Select the Contacts for the message by clicking one or more contacts on the left.
6. Click the move button (highlighted in the blue rectangle) to move contacts from Available to Selected.

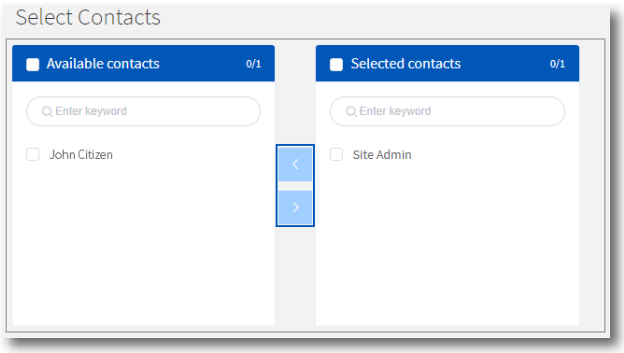


Figure 4-119: Settings - Notifications (Select Contacts)

7. Type custom text and use keywords to build your message.

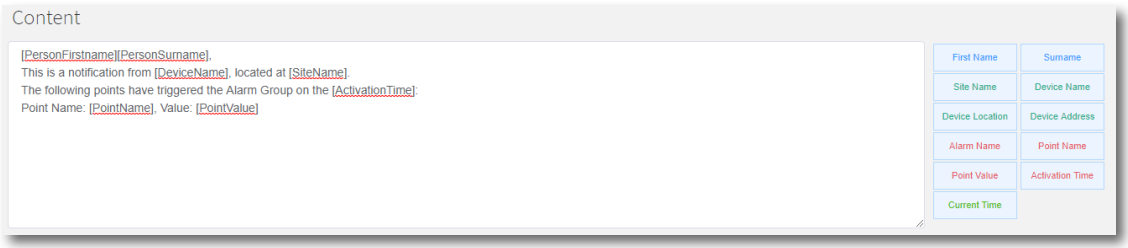


Figure 4-120: Settings - Notifications (Message Content)

8. Click Update to complete the message.

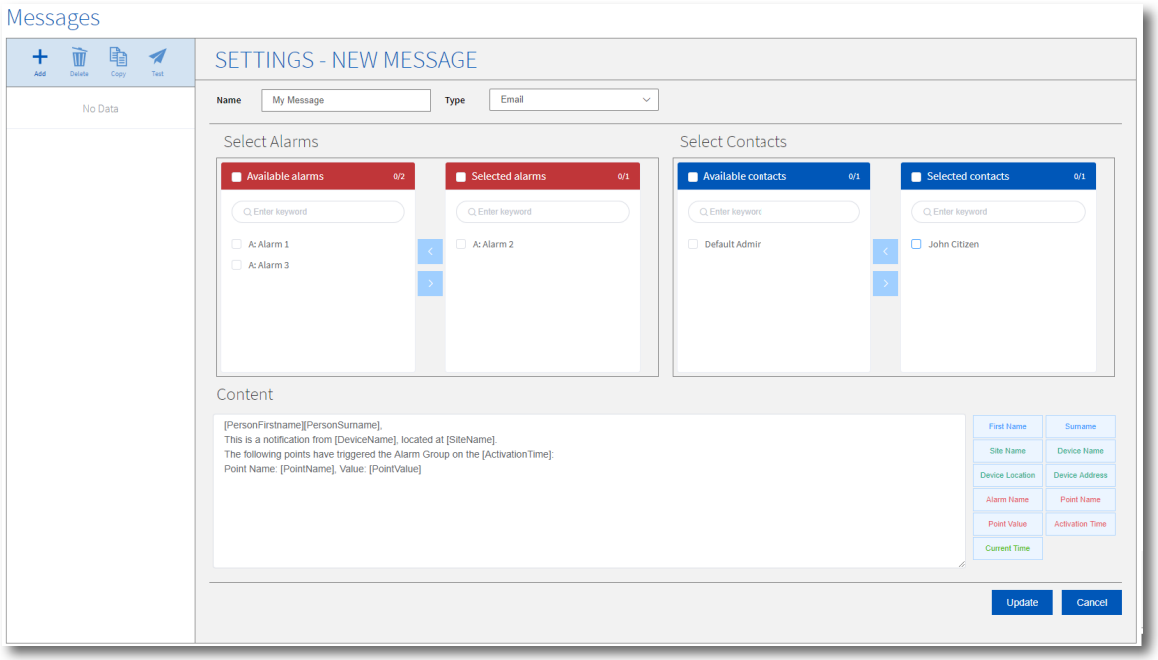


Figure 4-121: Settings - Notifications (Completed Message)

4-2.10 Device Info

The Device Info screen shows information about the connected Omni controller.
The Sessions page shows the currently connected session and a historical list of past sessions.

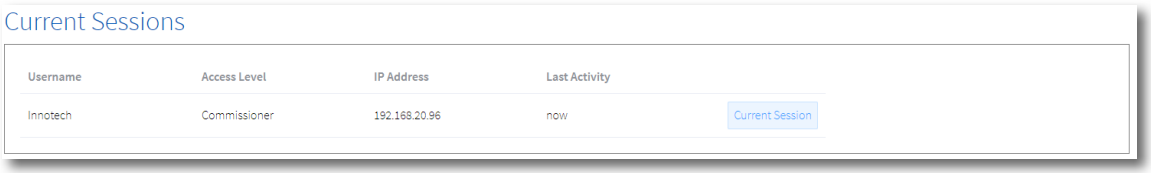


Figure 4-122: Device Info - Session Information

The System Versions page shows version numbers for the firmware and software on the connected controller.

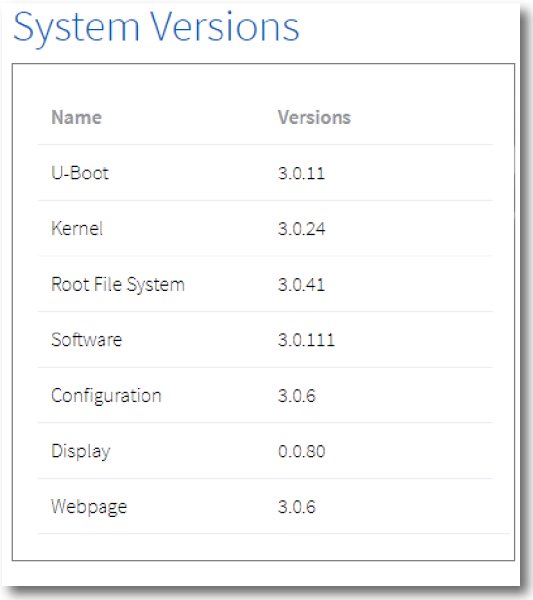


Figure 4-123: Device Info - System Versions

The Feature Licence page shows information about the current licences on the controller and provides the facility to upload new licences.

Figure 4-124: Device Info - Feature Licence

Feature Licences Upload
Licences for new features can be obtained from Innotech and uploaded to the controller from this screen.
Only .xml licence files can be uploaded to the controller

Click Upload New Licence to upload a Feature Licence file to the controller.

Click OK at the Warning screen if you wish to proceed.

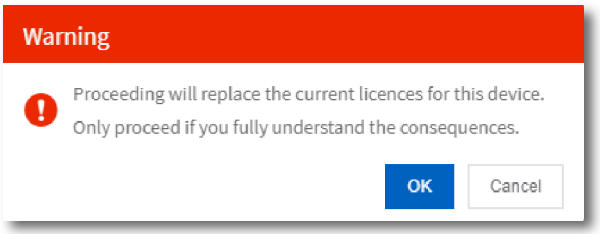


Figure 4-125: Device Info - Feature Licence Upload Warning

In the Open File dialogue, select your .xml licence file. Once the licence file selected, click Open.

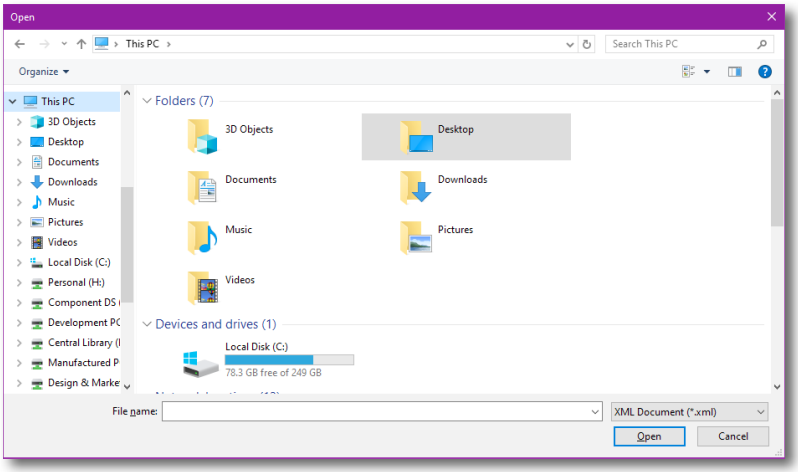


Figure 4-126: Device Info - Feature Licence Upload

The Performance page shows graphical statistics for the controller's usage.

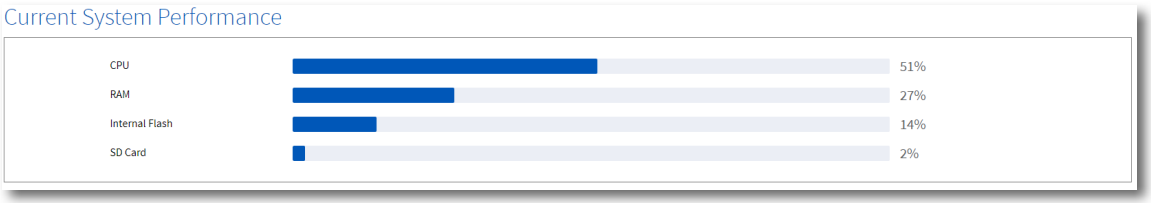


Figure 4-127: Device Info - Performance

The Device Status page shows details about the controller and any connected REMs. Click a heading to open the section and view more details about the controller. This page is also used for upgrading your Omni U10 REM.

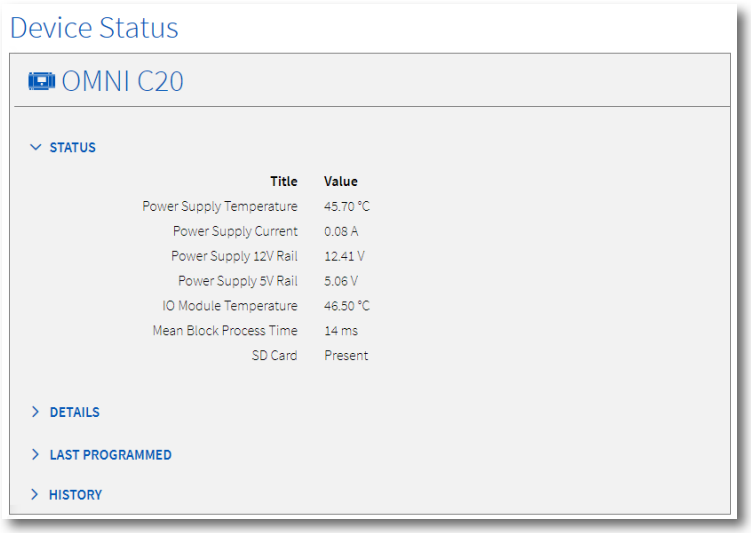


Figure 4-128: Device Info - Device Status

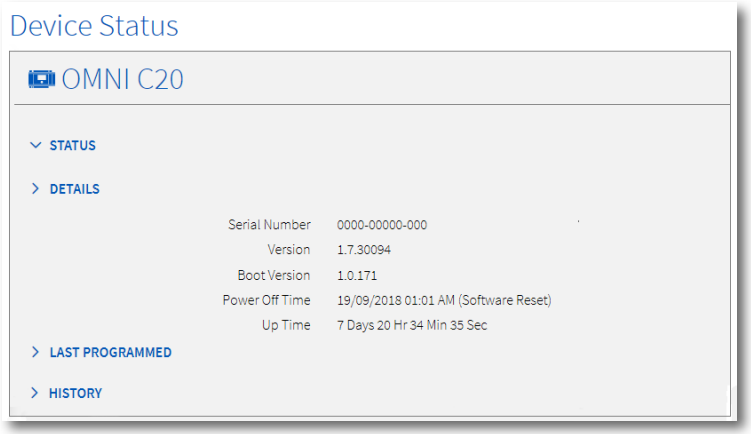


Figure 4-129: Device Info - Device Status (Details)

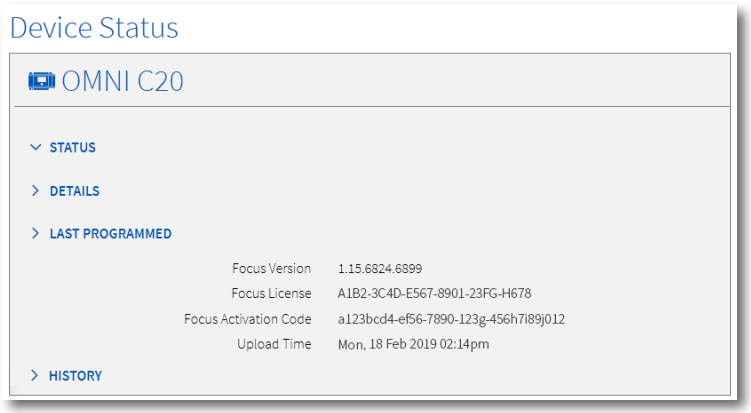


Figure 4-131: Device Info - Device Status (Last Programmed)

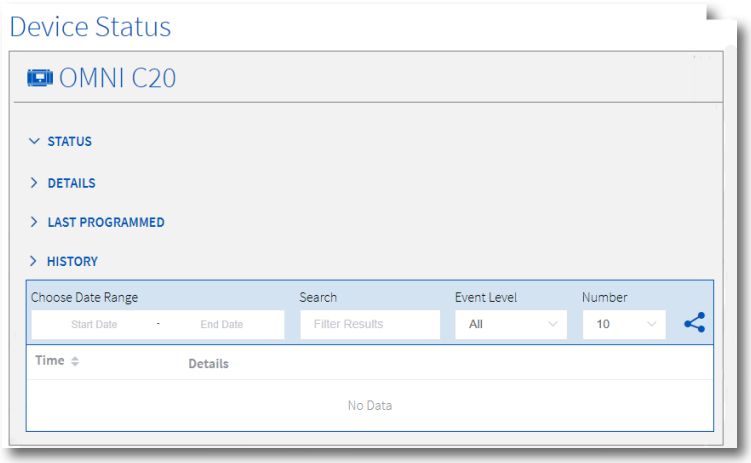


Figure 4-132: Device Info - Device Status (History)

The IO Status page shows details about the controller's Universal Inputs and Outputs (UIOs). On the left side you get an overview of each UIO. The right side shows details about any UIO you click on. You may be able to alter settings for the selected UIO depending on it's type. Only one subsection can be open at a time.

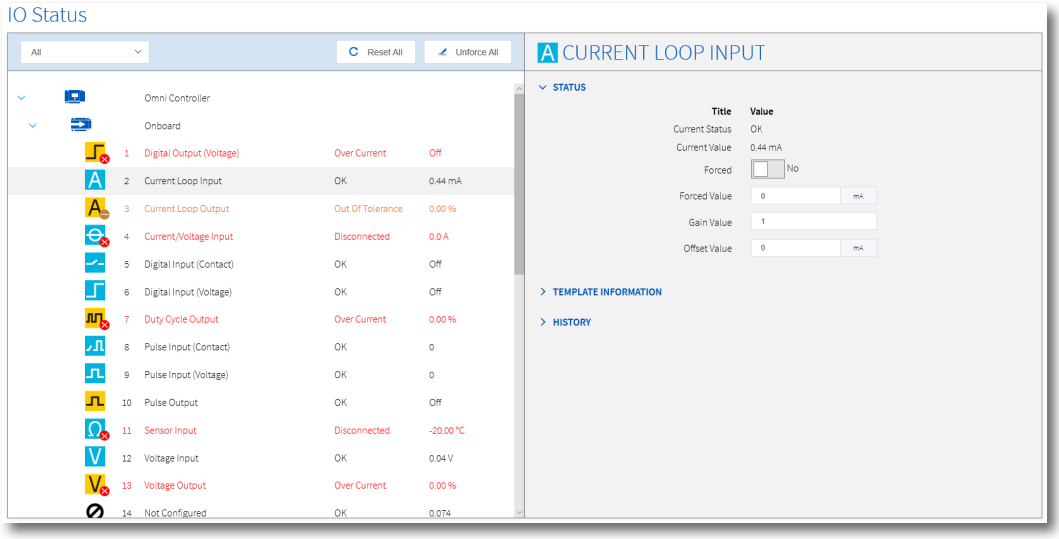


Figure 4-130: Device Info - IO Status

The Template Information section shows details (if applicable) about the template being used with the currently selected UIO. The content displayed will be different based on your selection.

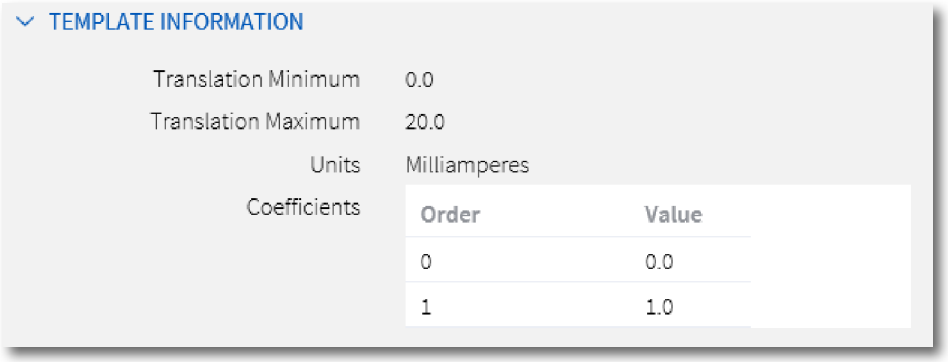


Figure 4-133: Device Info - Device Status (Last Programmed)

The History section shows the history of the currently selected UIO based on the search parameters. Click the share button at the right to save the history to a CSV file or print to PDF or a printer.

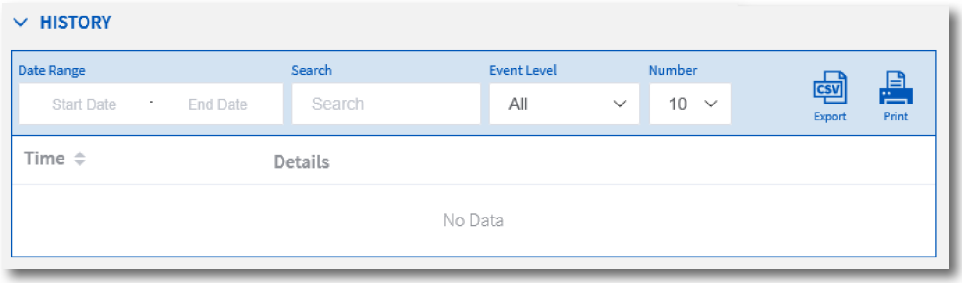


Figure 4-134: Device Info - Device Status (Last Programmed)

The BACnet client page shows information and settings for the controller's BACnet client. Changing the Select Service combo changes the screen fields.

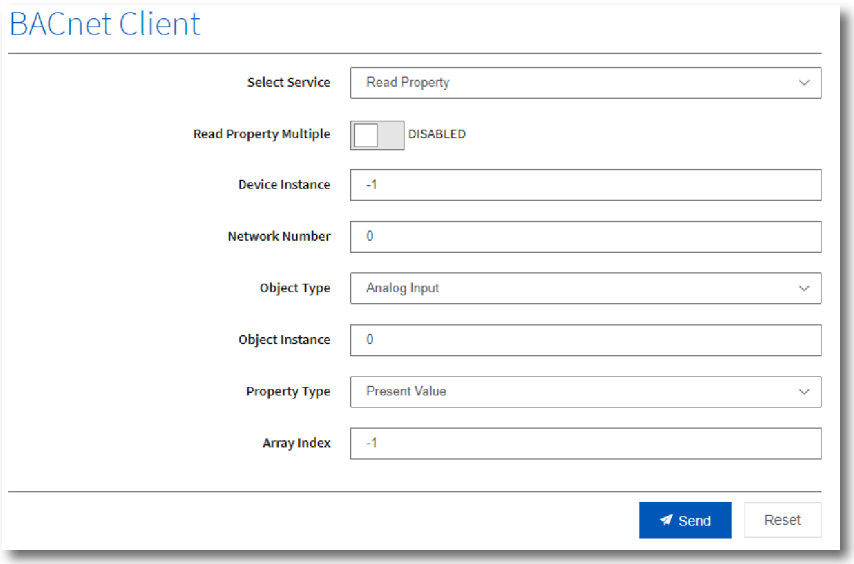


Figure 4-135: Device Info - BACnet Client

The Modbus Client page shows configuration settings for the Modbus Client on the connected controller.

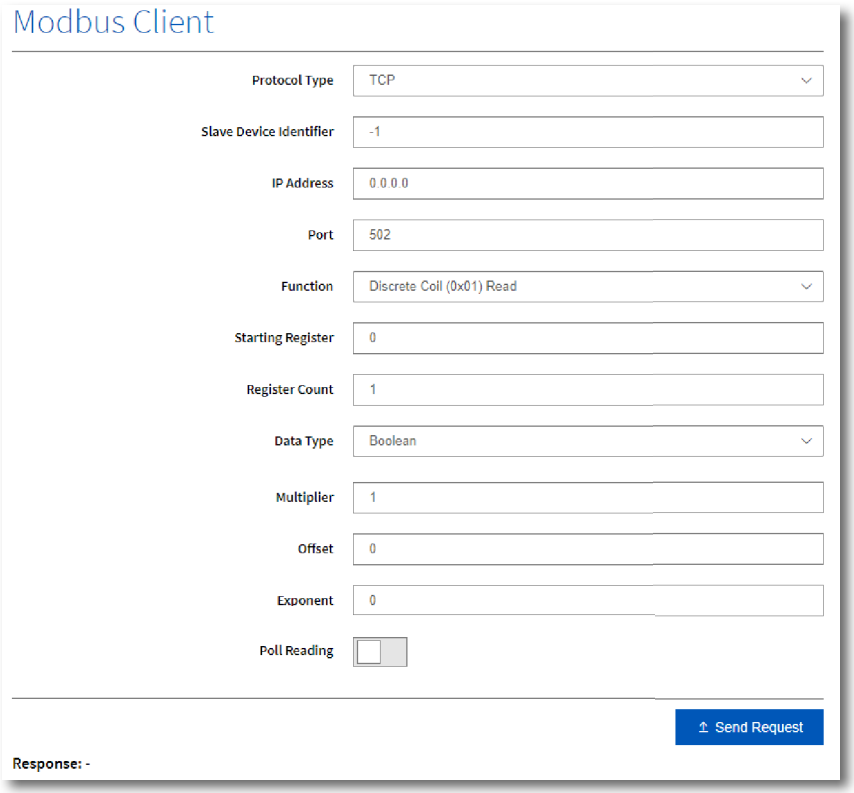


Figure 4-136: Device Info - Modbus Client

The System Logs page provides details on all the system messages that are provided from your Omni device. You can filter the logs results as required.

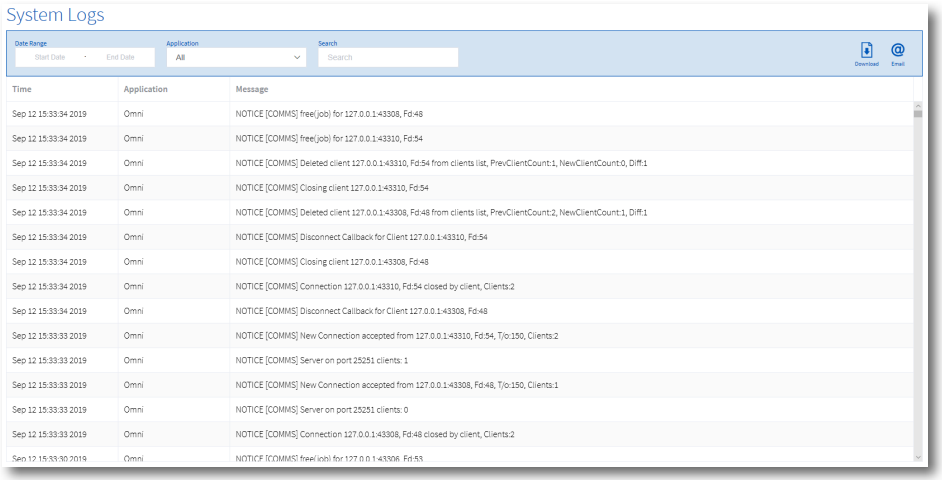


Figure 4-137: Device Info - System Logs

The Legal Info page displays the Software Licence Statement as well as information about the Open Source Licences used on the Omni Controller. You can contact Innotech to request a copy of a licence.

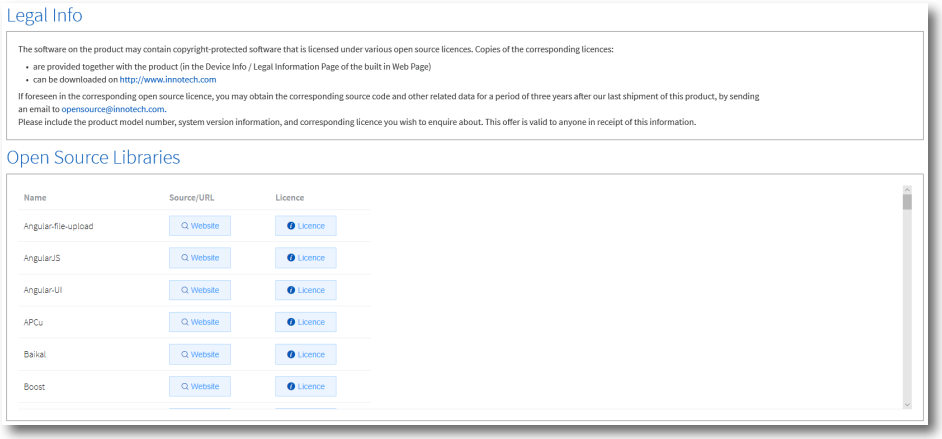


Figure 4-138: Device Info - Legal Info

4-2.10.1 Device Info - Upgrade Omni U10 REM

Omni U10 firmware should be automatically updated when the connected Omni controller firmware is updated. If you need to manually update the U10 firmware, follow this procedure in this section.

If an upgrade is required, REM Error will likely be shown at the bottom right of the window.

1. Click the Upgrade REMS title to open the upgrade section. You can force an upgrade even if one is not available.

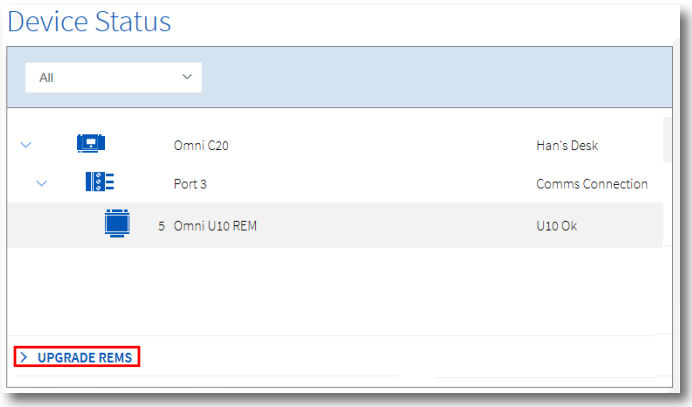


Figure 4-139: Device Info - Upgrade REMS

2. If required, change the Port and/or check the Force Upgrade checkbox.
3. Click the Upgrade Available button to start the upgrade process. During the upgrade, the Heartbeat LED will flash red and green.

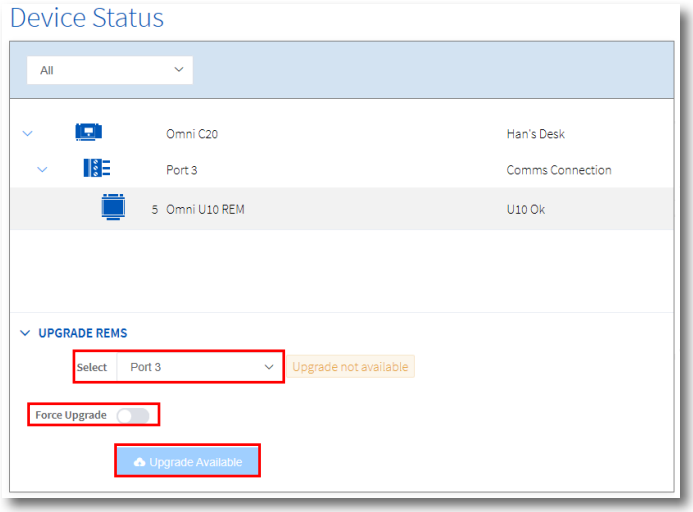


Figure 4-140: Device Info - Upgrade Options

The upgrade is complete when the log shows Upgrade Complete.

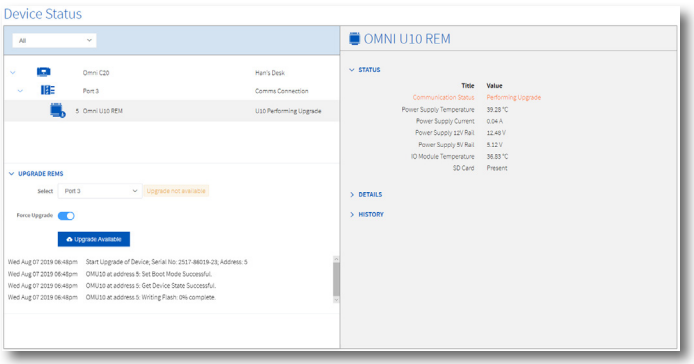


Figure 4-141: Device Info - Upgrade In Progress

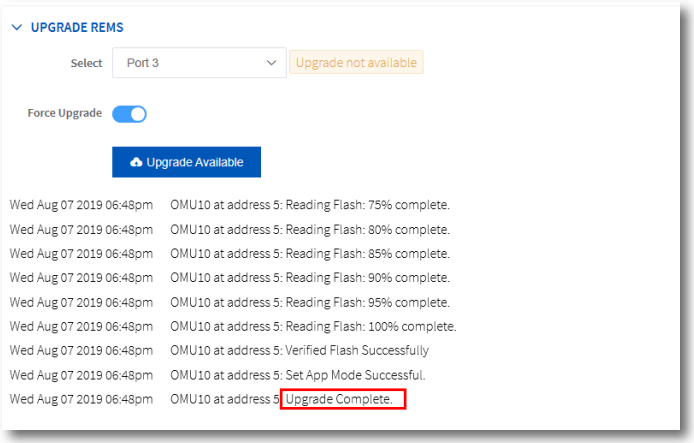


Figure 4-142: Device Info - Upgrade Complete

4-2.11 Documents

The Documents tab of the web server contains factory supplied Product Documents and a section for saving your own documents. The Product Documents may be updated when the controller firmware is updated.

In the Product Documents section, click a file to view. You can also save your own documents to the controller in the Saved Documents section.

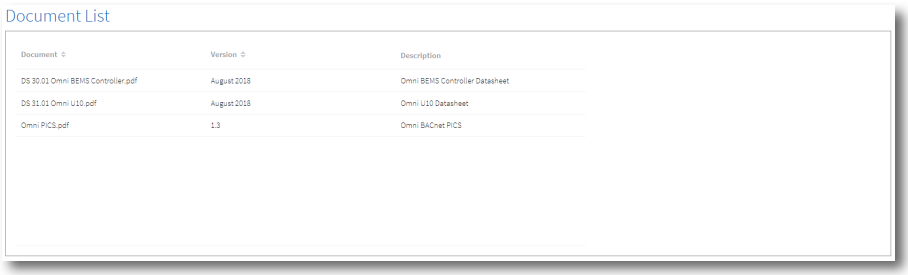


Figure 4-143: Documents - Product Documents

Saved Documents

1. Click Upload New to open the dialogue.
2. Click Browse to select a file and click Open.
3. Enter an Author and Description.
4. Click Save to save the document to the Omni controller.

- Existing files are deleted by pressing the red delete button.
- Only .gif, .jpg, .gif, .svg, .docx, .xlsx, .txt and .pdf can be uploaded to the controller and the file size is limited.
- Click a row to download and view the file.

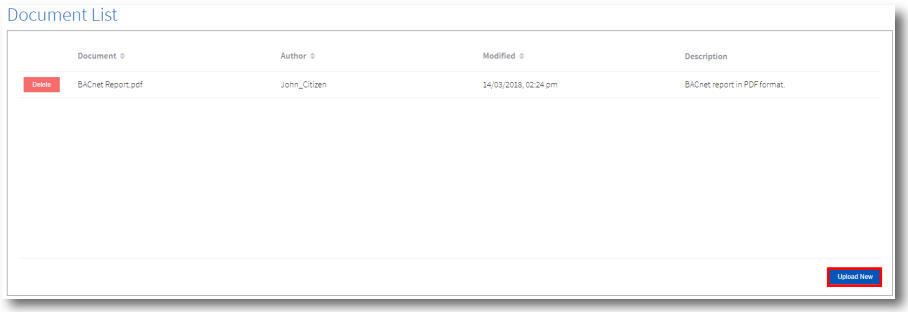


Figure 4-144: Documents - Saved Documents List

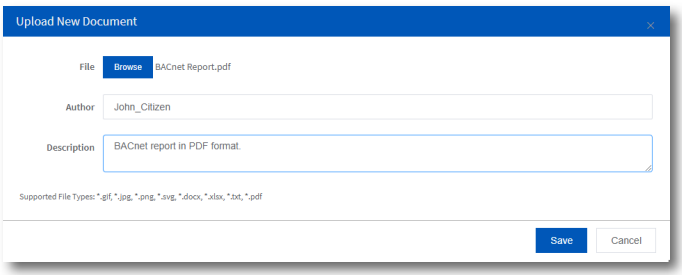


Figure 4-145: Documents - Upload Document Window

4-2.12 Logging Out

Log out from the Omni Web Server by clicking the Logout link at the top of the screen at any time. After clicking Logout, the Web Server will return to the Log In screen.

4-2.13 Omni Web Help

Click the Help link at the top of the screen to access the help information for Omni. The help will provide basic information about the Omni web server and HMI.

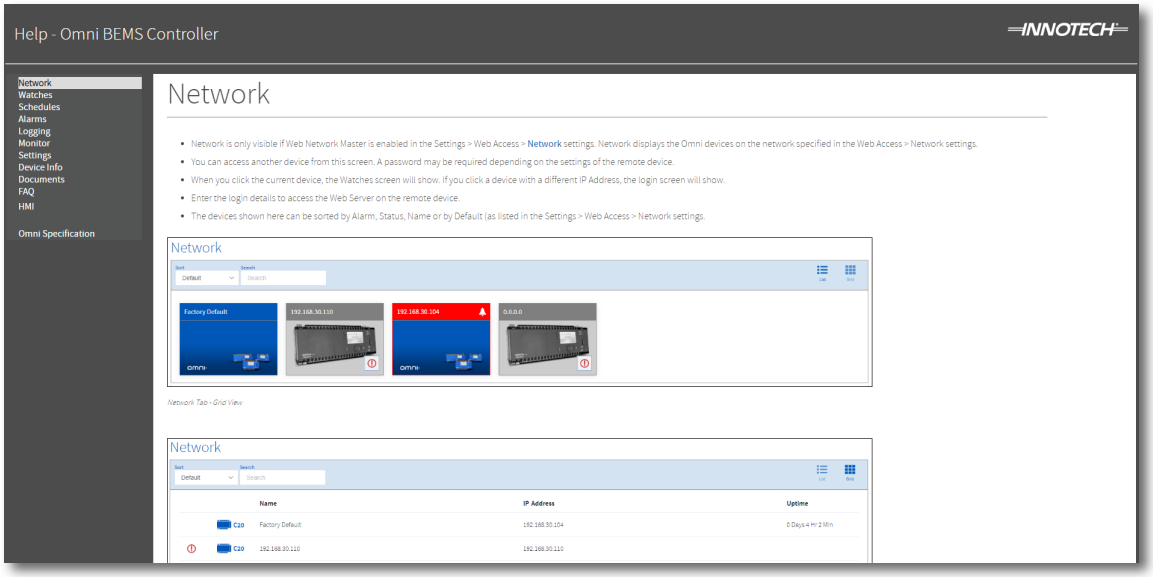


Figure 4-146: Omni Web Server Help Window

Innotech Support

Innotech provides technical information on the Web to assist you with using its products.
At www.innotech.com, you can find technical manuals, user instructions, and data sheets for all our products.

For direct product support or product information, contact your local distributor, or an Innotech representative.

You can contact us via email, phone, or postal mail:

Website: www.innotech.com
Email: sales@innotech.com
Phone: +61 7 3421 9100
Mail: Innotech Control Systems
P.O. Box 292
Sunnybank QLD 4109
Australia

