Airborne M2M™

USER MANUAL

ABDN-er/se-DP55x series

ABDN-er/se-IN5xxx series

_Revision 1.3

_September 2018

B+B SmartWorx

Powered by ADVANTECH

Advantech B+B SmartWorx - Americas
707 Dayton Road
Ottawa, IL 61350 USA
Phone (815) 433-5100
Fax (815) 433-5105

Advantech B+B SmartWorx - European Headquarters
Westlink Commercial Park
Oranmore, Co. Galway, Ireland
Phone +353 91-792444
Fax +353 91-792445

www.advantech-bb.com
support@advantech-bb.com

Documentation Number: ABDx-xx_ProductSeries_r3_3818um

TABLES OF CONTENTS

Figures

Tables

CONVENTIONS

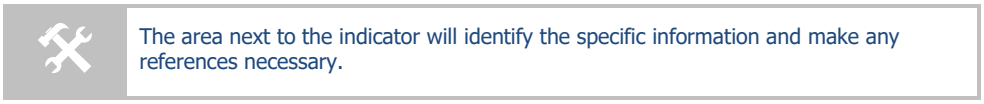
The following section outlines the conventions used within the document. Where convention is deviated from, the deviation takes precedence and should be followed. If you have any questions related to the conventions used or clarification of indicated deviation, please contact B+B SmartWorx Sales or Wireless Support.

TERMINOLOGY

Airborne Device Server and AirborneM2M Device Server terms are used to describe the devices in the opening section of this document. After this section, the term ***module*** will be used to describe the devices.

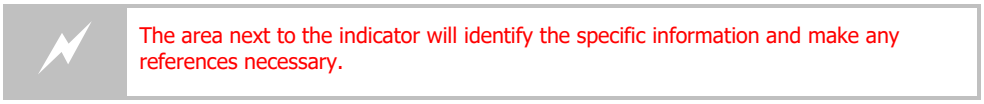
NOTES

A note contains information that requires special attention. The below convention will be used. The area next to the indicator will identify the specific information and make any references necessary.



CAUTION

A caution contains information that, if not followed, may cause damage to the product or injury to the user. The shaded area next to the indicator will identify the specific information and make any references necessary.



FILE FORMAT

These documents are provided as Portable Document Format (PDF) files. To read them, you need Adobe Acrobat Reader 4.0.5 or higher. For the latest version of Adobe Acrobat Reader, go to the Adobe website (www.adobe.com).

PRODUCT DESCRIPTION

This guide describes the AirborneM2M™ device servers and wireless adapters from B+B SmartWorx, Inc. AirborneM2M™ is a fully integrated, 802.11 wireless Local Area Network (LAN) connectivity device designed to provide wireless LAN and Internet connectivity in industrial, scientific, medical and transportation applications where an existing communications interface already exists. The AirborneM2M family of products supports Serial (RS-232/422/485), Ethernet and a combination these interfaces in a range of packaging options.

The AirborneM2M™ product family provides true plug-and-play wireless connectivity. By delivering convenient, easy-to-deploy wireless network connectivity, the device servers and adapters significantly reduce the complexities of wireless system deployment and network implementation. At the same time, users can move equipment without the cost and time associated with wired network drops and environment restrictions. This provides flexibility for seasonal demands, line and staffing changes, and more.

The AirborneM2M™ family includes models with dual band radios; the ABDNx supports 802.11a/b/g/n.

The AirborneM2M™ Serial Bridges and Device Servers provide a simple connection between the 802.11 wireless LAN and three leading serial interfaces: RS-232, RS-422, and RS-485.

The Bridge acts transparently between any device using these interfaces and a wireless LAN. Using the B+B SmartWorx virtual communications port Windows device driver, OEMs can communicate with their devices from any workstation on the same network as if the workstation and devices were directly attached through a serial port.

The AirborneM2M™ Ethernet Adapter provides a link between the 802.11 wireless LAN and any Ethernet-ready device with an RJ-45 connector. It acts transparently between the device and a wireless LAN. By integrating AirborneM2M™ into existing and legacy platforms, OEMs can significantly enhance their products by delivering increased value and functionality to their entire customer base.

The Airborne family includes the ability to simultaneously use the serial-to-wireless and Ethernet-to-wireless connectivity in the same unit. This capability provides for multiple connections to the same machine or consolidation of multiple wireless units into a single device.

The AirborneM2M™ products open the world of remote device monitoring and management, as well as wide-area data collection, to any device or machine or plant that has an external serial or Ethernet connection and a network infrastructure. A development kit provides quick and easy access to the bridge's configuration and functions, while providing OEMs with a platform to develop their branded solutions. The bridge also provides the capability to perform firmware upgrades that allow new features to be added quickly and easily, protecting your investment.

The Enterprise family includes the most advanced security support available for the device class in the industry, including WPA, WPA2 and full Enterprise support. The devices can be used with the most advanced WLAN networks being deployed today. Airborne products are based on the industry leading Airborne device server and wireless adapter technology from B+B SmartWorx, providing a fully compatible and familiar device interface across all product ranges. If you have used one of them, you have used them all.

FEATURES

- 802.11 WiFi Radio with 32-bit ARM9 CPU (128Mb SDRAM, 64Mb Flash)
  - ABDN series supports 802.11a/b/g/n
- Integrated Airborne Device Server and Wireless Adapter Technology.
- Supports WEP, WPA, WPA2 and 802.1x Supplicant, with Certificates.
- The wireless device server includes integrated:
  - 802.11 Radio Driver
  - TCP/IP stack, UDP, telnet, FTP server
  - Data bridging and buffering
  - Command Line Interface (CLI)
  - Web Interface
  - WPA Supplicant
  - DHCP Server (Ethernet Interface)
  - Firewall and Port Forwarding (Ethernet)
  - FTP Server
- Supports flexible antenna selection.
- Operating Temperature (-40 to +85 °C)
- Storage Temperature (-40 to +85 °C)
- Industry standard wired connections:
  - DB-9 Serial Connectors (RS-232/422/485)
  - RJ-45 (10/100 Ethernet)
- Multiple host interfaces supported:
  - Single and Dual Serial (RS-232/422/485) – up to 921K baud
  - 10/100 Ethernet
- Uses 5-36 VDC power source input
- Power connector options include 2.1mm Barrel Jack, Terminal Block and custom connectors.
- Power-over-Ethernet (PoE) using an 802.3af Class 1 PSE device (ABDx-ER-IN5xx8 models)
- Integrated Site Survey mode
- Advanced Low Power modes
- Rugged Mounting options
- Virtual COM Port driver (Win XP, Vista, 7)
- Worldwide Regulatory Support (FCC, IC, CE)

DEVICE TYPES

This manual covers all variations available in the AirborneM2M™ device family. The following section identifies the different types both functional and classification. In most cases, the functional types are available in the listed classifications. If you are not certain which type you have or would like clarify the available options, please contact B+B SmartWorx Sales or Technical Support.

SERIAL

This device supports a single or dual serial port and provides serial to 802.11 bridging. The serial devices can support one or more of the following serial interface types:

- RS-232
- RS-422
- RS-485

Default configuration on all models is RS-232. Conversion to RS-422/RS-485 requires software configuration and, in some models, jumper setting changes. These are covered in the following sections.

This device allows the connection of a serial port to an 802.11 network.

ETHERNET

The Ethernet adapter provides a wireless interface to an existing Ethernet port (RJ-45). Depending on the model of device, the connection to the Ethernet port of the host is made via an RJ-45 socket or pigtail with an RJ-45 plug.

The device supports a 10/100 Ethernet interface with auto-configuration. Manual control of the interface is possible through the web or CLI interface.

SERIAL + ETHERNET

This device allows simultaneous connection of Serial and Ethernet ports. Providing the same functionality on each port that is available on the individual devices, it is possible to maintain network based connections to both the Ethernet and Serial ports without compromise of functionality or performance.

Each interface can be configured and operated independently of the others. Connection to the serial port can be made via both the wireless and Ethernet ports supporting redundant network connectivity for high reliability applications.

ENTERPRISE CLASS

The Enterprise Class product provides the best cost vs. performance in the AirborneM2M™ product family. The packaging is compact and designed to fit with non-industrial applications and markets. This product class supports the full industrial operating temperature range and the complete set of functional capabilities of the Airborne™ Device Server and Wireless Adapter technology.

Figure 1 - Enterprise AirborneM2M™ Device

The Enterprise class product is ideal for the following application types:

- Medical equipment
- Point-of-Sale devices
- CNC/DNC equipment
- Time clocks
- Scales
- Data collection devices
- Vehicle diagnostics

Enterprise Class products include an Ethernet device and require a 5 VDC power source. See datasheet for more details, inclusions and accessories.

INDUSTRIAL CLASS

Developed to support the demands of the industrial and automotive environments, the features of the Industrial Class products offer a more flexible and rugged alternative to the enterprise class devices. This product class supports the full industrial operating temperature range and the complete set of functional capabilities of the Airborne Device Server and Wireless Adapter technology.

Figure 2 - Industrial AirborneM2M™ Device

The industrial family includes a metal enclosure and requires a 5-36V DC power source, capable of exceeding the SAE J1455 power requirements. See datasheet for more details, inclusions and accessories.

The Industrial class product is ideal for the following application types:

- CNC/DNC equipment
- Vehicle diagnostics
- Telematics
- Remote monitoring and management
- Industrial control

The Industrial Class of products includes Ethernet only, Serial only and dual (Serial+Ethernet) capability. Some models support Power-over-Ethernet (PoE) when connected to an 802.3af Class 1 PSE device.

BLOCK DIAGRAMS

The following outlines the block diagram for the devices:

Figure 3 - ABDN-ER-DP55x Block Diagram

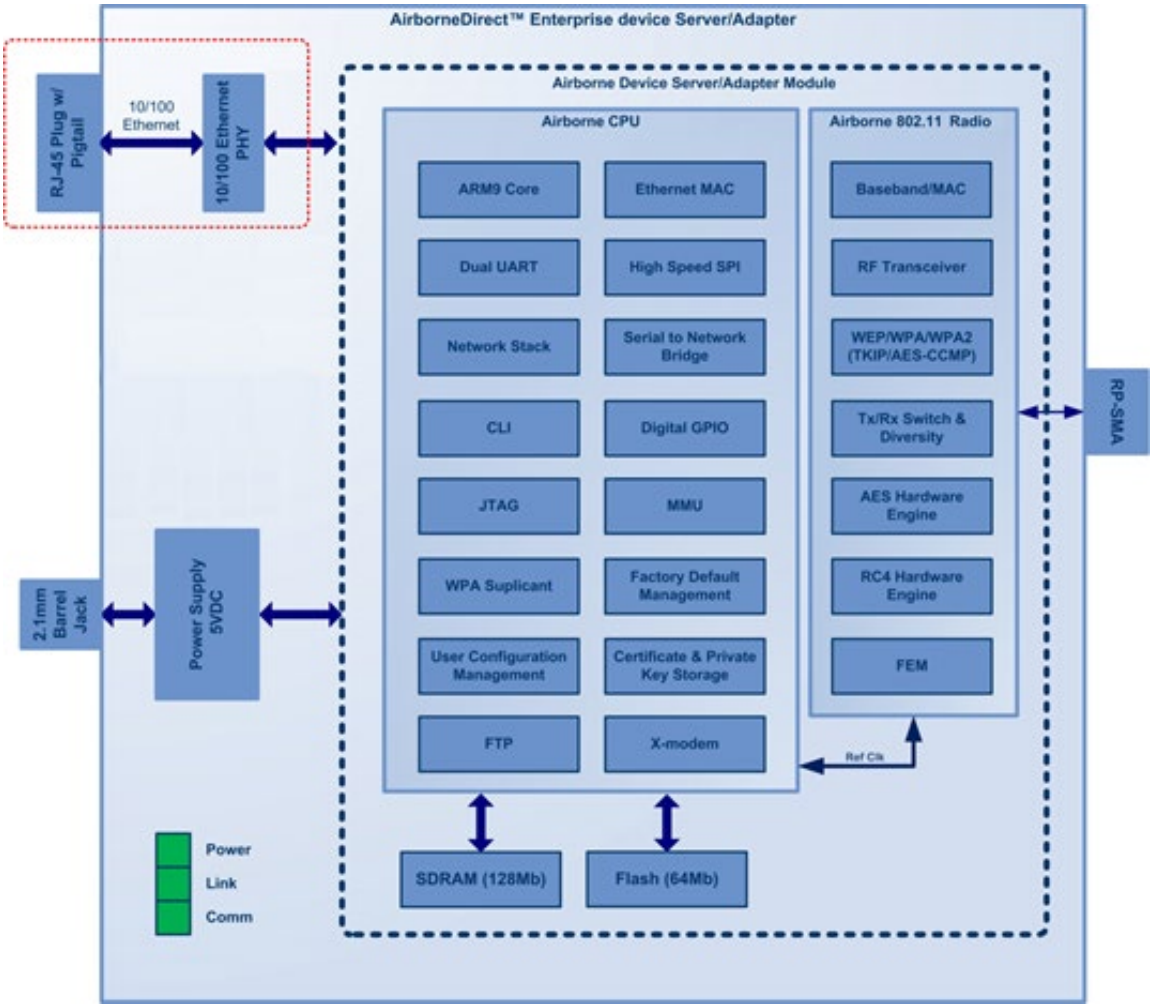
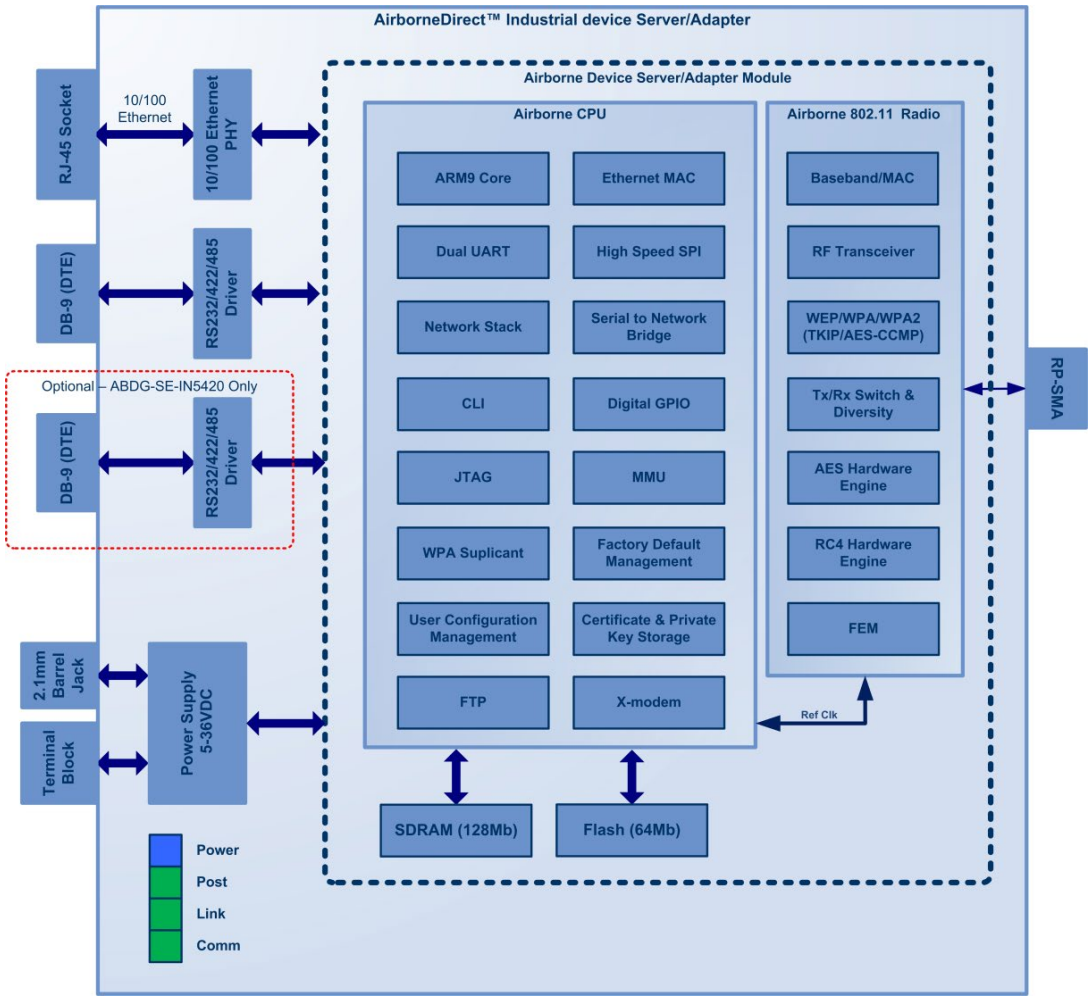


Figure 4 - ABDN-er/se-IN5xxx Block Diagram



PIN OUT AND CONNECTORS

Pin definition is dependent on the device type selected. The following defines the pin outs for the individual interfaces.

SERIAL PORTS

The AirborneM2M™ units support either a single or dual serial port configuration. The port pin out can change depending on the interface configuration chosen. Table 1 shows the pin out for the interface selected.

Figure 5 - DE-9 (DB-9) Connector Pin-out

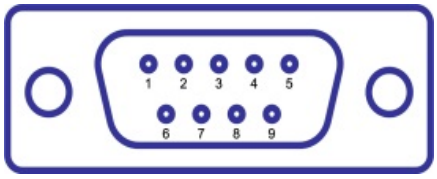


Table 1 – Serial Port Pin Definition

Pin	RS-232 (DTE)	RS-232 w/ Power on pin 9[2]	RS-422/RS485 4-wire	RS-485 2-wire
1	No Connect	No Connect	No Connect	No Connect
2	RxD	RxD	RxD+	Connect to pin 3[3]
3	TxD	TxD	TxD+	TxD+/RxD+
4	No Connect	No Connect	No Connect	No Connect
5	GND	GND	GND	GND
6	No Connect	No Connect	RxD-	Connect to pin 9[3]
7	RTS	RTS	No Connect	No Connect
8	CTS	CTS	No Connect	No Connect
9	No Connect	5VDC (Input)	TxD-	TxD-/RxD-

1. For 2-wire operation, the user must externally connect pin 3 to pin 2 and pin 6 to pin 9.
2. Power on pin 9 only available on Enterprise devices (ABDN-xx-DP551).
3. Only required on Industrial products (ABDN-xx-IN54xx)

Table 2 shows the availability of the serial ports and available interface types by product class.

Table 2 - Serial Ports by Product Class

Device Class	Port 1	Port 2
Enterprise	RS-232 RS-422 (4-wire) RS-485 (2-wire)	N/A
Industrial	RS-232 RS-422 (4-wire) RS-485(2-wire)	N/A
	RS-232 RS-422 (4-wire) RS-485(2-wire)	RS-232 RS-422 (4-wire)

The Port 1 and Port 2 interfaces support the following configurations:

- Baud: 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 115200, 230400, 460800, 921600
- Flow Control: None, Hardware (CTS/RTS), Software (XON/XOFF)
- Port 1 Default Settings: 9600, 8, N, 1, No Flow Control
- Port 2 Default Settings: 9600, 8, N, 1, No Flow Control

ETHERNET PORT

The AirborneM2M™ Ethernet devices support a single interface. This is a 10/100Mbps interface that supports auto-negotiation and cross-over cabling. The interface also supports both half and full duplex for 10Mbps and 100Mbps. Table 3 shows the interface pin out.

In some Industrial models, the Ethernet port supports Power-over-Ethernet (PoE) when connected to an 802.3af Class 1 PSE device. Both Mode A (MDI and MDI-X) and Mode B powering schemes are supported (Table 3a).

Figure 6 - Ethernet Jack Pin Out

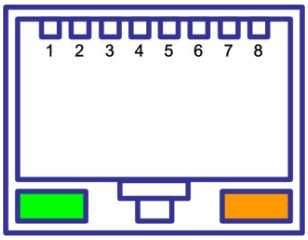


Table 3 - Ethernet Connector Pin Out

Pin	RJ45 Socket (Industrial)	RJ45 Plug (Enterprise)
1	TxD+	RxD+
2	TxD-	RxD-
3	RxD+	TxD+
4	NC	NC
5	NC	NC
6	RxD-	TxD-
7	NC	NC
8	NC	NC
Green LED	Valid TCP/IP connection made with Airborne Adapter: **Off** No TCP/IP connection **On** Valid TCP/IP Connection	N/A
Yellow LED	Power-on Self Test (POST): **Off** Not powered or has failed POST **On** Passed POST	N/A

Table 3a - PoE Pinout Alternatives

Pin	Alternate A (MDI-X)	Alternate A (MDI)	Alternate B (All)
1	Negative V_{PSE}	Positive V_{PSE}	
2	Negative V_{PSE}	Positive V_{PSE}	
3	Positive V_{PSE}	Negative V_{PSE}	
4			Positive V_{PSE}
5			Positive V_{PSE}
6	Positive V_{PSE}	Negative V_{PSE}	
7			Negative V_{PSE}
8			Negative V_{PSE}

CONNECTOR DEFINITION

There are a total of five connectors used by the AirborneM2M™ family. Which connectors are available on your product depend on the model you purchased. The definition for the connectors is common to all product classes. Table 4 provides definitions for the connectors.

Table 4 - Connector Description

Type	Description	Product Class
Serial	DE-9 Connector Male	Enterprise, Industrial
Ethernet	RJ45 Plug	Enterprise
Ethernet	RJ45 Socket	Industrial
Antenna	RP-SMA	Enterprise, Industrial
Power	2.1mm Barrel Jack	Enterprise, Industrial
Power	2 Position Terminal Block	Industrial

OEM RESET SWITCH (FACTORY RESET)

All AirborneM2M™ devices support the ability to reset the configuration back to OEM defaults. This is useful when a device has been incorrectly configured and has lost the ability to communicate on any of the available ports, preventing access to one of the configuration interfaces and blocking your ability to recover the device by correcting the configuration.

Table 5 describes the sequence for OEM resetting the AirborneM2M™ devices. All devices use the same process. However, the location of the OEM reset switch varies between product families.

Table 5 - OEM Reset Procedure

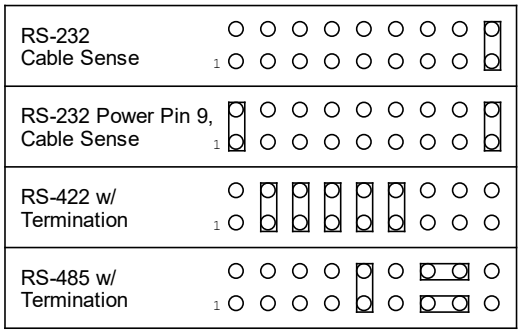
1	Disconnect or turn off the power supply.
2	Press the OEM reset (factory reset) button. This may require the use of a small narrow object, it is important that this object is not sharp as it may cause damage to the unit.
3	While holding the OEM button pressed reapply power to the unit.
4	Hold the OEM reset button for 5-6 seconds after power has been applied.
5	Release the OEM reset button.
6	The device will restart with the installed OEM defaults. If no OEM Configuration is applied the device will return to B+B SmartWorx factory defaults. See section 15.6 on use of OEM factory configurations.

The location of the OEM reset button for the Enterprise devices is on the back of the enclosure, underneath the label near the pigtail. The Industrial devices' OEM reset button is on the Ethernet/Power end of the box next to the 2.1mm barrel connector (See section 10.0.)

ENTERPRISE SERIAL INTERFACE JUMPERS

The Enterprise Serial Device Server supports RS-232/422/485 interface drivers, as well as power over pin 9. Selection of these options is made through both the web interface and hardware jumpers. Figure 7 shows the interface selection jumpers for the different interface types.

Figure 7- Interface Selection Jumpers



The jumper selections must be made while the device is unpowered and before being used in the final application.

The interface type selected by the interface jumpers in Figure 7 must match the selected configuration for the **Configuration | Serial Port Settings | Serial Interface Type** setting in the web interface.

INDICATOR LEDS

The devices provide indicator LEDs to provide feedback on the state of the device. These LEDs are a useful tool during installation and troubleshooting.

Table 6 - Enterprise LED Indicators

LED	Color	Airborne Device State
POWER	○	Adapter is not powered.
	●	Adapter failed Power On Self Test (POST) and is not configured for wireless communication.
	●	*Adapter passed POST but is not configured for wireless network communication.*
	●	Adapter passed POST and is configured for wireless communication.
LINK	○	Adapter is not powered.
	✳	(Periodic Blinking) Adapter is searching for a valid network (Access Point) that matches device's configuration.
	●	Adapter has successfully associated with an Access Point.

LED	Color	Airborne Device State
COMM	○	If Power LED is also Off, then Adapter is not powered. If Power LED is On, then either: • A physical connection detected on Serial/Ethernet cable. • No TCP session from wireless interface has been established.
	🔴	No physical Serial/Ethernet connection has been detected.
	☀🔴	(Blinking – OFF/Red) A physical Serial/Ethernet connection has been detected and there is traffic across the interface. No TCP connection to the adapter has been established on the wireless interface.
	🟠	A TCP connection to the adapter from the wireless interface has been established but no physical connection on the Serial/Ethernet interface has been detected.
	☀🟢	(Blinking – Green/Orange) A physical Serial/Ethernet connection has been detected and there is Serial/Ethernet traffic across the interface. A TCP connection to the adapter has been established (On WLAN or Ethernet interface).
	🟢	A physical Serial/Ethernet connection has been detected. A TCP connection to the adapter has been established from the WLAN or Ethernet interface but no traffic has been detected.

Table 7 - Industrial LED Indicators

LED	Color	Airborne Device State
POWER	○	Adapter is not powered.
	🔵	Adapter is powered.
POST	○	Adapter is not powered.
	🔴	Adapter failed Power On Self Test (POST) and is not configured for wireless communication.
	🟠	Adapter passed POST but is not configured for wireless network communication.
	🟢	Adapter passed POST and is configured for wireless communication.
LINK	○	Adapter is not powered.
	☀🔴	(Periodic Blinking) Adapter is searching for a valid network (Access Point) that matches device's configuration.
	🟢	Adapter has successfully associated with an Access Point.
COMM	○	If Power LED is also Off, then Adapter is not powered. If Power LED is On, then: • No TCP session from WLAN or Ethernet interface has been established.
	🟢	A TCP connection to the adapter has been established from the Wireless or Ethernet interfaces but no traffic has been detected.

ELECTRICAL & RF SPECIFICATION

Table 8- Absolute Maximum Values1

Parameter	Min.	Max.	Unit
Maximum Supply Voltage - Enterprise	4.5	5.5	VDC
Maximum Supply Voltage - Industrial	5.0	36	VDC
PoE 802.3af Class1 – Industrial (IN5xx8 models)	37	57	VDC
Power Dissipation		3.00	W
Operating Temperature Range	-40	85	ºC
Storage Temperature	-40	85	ºC

Note: 1. Values are absolute ratings, exceeding these values may cause permanent damage to the device.

Table 9 - RF Characteristics – 802.11a/b/g/n

Symbol	Parameter	Rate (Mb/s)	Min.	Average dBm / mW		Peak dBm / mW		Units
P_{OUTB}	Transmit Power Output 802.11b	11, 5.5, 2, 1		15.0	31.6			dBm
P_{OUTG}	Transmit Power Output 802.11g	6, 9, 12, 18, 24, 36, 48, 54		12.6	18.2			dBm
P_{OUTA}	Transmit Power Output 802.11a	6, 9, 12, 18, 24, 36, 48, 54		17.0	50.1			dBm
P_{RSENB}	Receive Sensitivity 802.11b	11		-86				dBm
		1		-92				
P_{RSENG}	Receive Sensitivity 802.11g	54		-72				dBm
		36		-78				
		18		-84				
		6		-89				
P_{RSENA}	Receive Sensitivity 802.11a	54		-74				dBm
		36		-80				
		18		-86				
		6		-90				
$F_{RANGEBG}$	Frequency Range		2412			2484		MHz
F_{RANGEA}	Frequency Range 802.11a		4910 5150 70			4990 5350 5825		MHz

The transmit power is automatically controlled by the device for minimum power consumption.
The transmit power at the antenna connector is listed in Table 9 above (±2dBm).

Table 10 - Supported Data Rates by Band

Band	Supported Data Rates (Mb/s)
802.11b	11, 5.5, 2, 1
802.11a/g	54, 48, 36, 24, 18, 12, 9, 6
802.11n	65, 58.5, 42, 39, 26, 19.5 13, 6.5

Table 11 - Operating Channels

Band	Region	Freq Range (GHz)	No. of Channels	Channels
802.11b[1,2]	US/Canada	2.401 - 2.473	11	1 – 11
	Europe	2.401 - 2.483	13	1 – 13
802.11g[1,2]	US/Canada	2.401 - 2.473	11	1 – 11
	Europe	2.401 - 2.483	13	1 – 13
802.11a[2]	US/Canada	5.15 - 5.35, 5.725 - 5.825	13	36,40,44,48,52,56,60,64,149,153,157, 161,165
	Europe	5.15 - 5.35, 5.47 - 5.725	19	36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140

1. Only channels 1, 6 and 11 are non-overlapping.
2. Channel count denotes number of non-overlapping channels. Channels shown represent non-overlapping channel numbers.

AC ELECTRICAL CHARACTERISTICS – TRANSMITTER

Transmit power is automatically managed by the device for minimum power consumption. The transmit power at the RF connector is listed in Table 9 for 802.11a/b/g Modes (all rates).

PERFORMANCE/RANGE

The following table illustrates the typical data rates, performance and range the device is capable of providing using an omni-directional antenna.

Table 12 - Radio Typical Performance Range

Data Rate	Typical Outdoor Distance (Unity gain antenna)	Typical Outdoor Distance (2dBi antenna gain on each end for B/G mode)
1.0 Mb/s	240m	380m
11.0 Mb/s	135m	215m
6Mb/s 802.11g	135m	215m
6Mb/s 802.11a	49m	155m
54Mb/s 802.11g	12m	19m
54Mb/s 802.11a	4.5m	14m

Ranges are affected by receiver sensitivity, transmit power, free-space path loss, antenna gain, and link margin. Actual range will vary from those stated. Non-line-of-site applications will result in typical values less than shown above.

The Data Rate is the supported connection rate for the wireless link; the actual data throughput for the link will be less than the stated data rates.

ANTENNA

The unit supports antenna connection through a single Hirose U.FL connector, located on the top surface of the radio next to the RF shielding.

Any antenna used with the system must be designed for operation within the 2.4GHz ISM band and specifically must support the 2.412GHz to 2.482GHz. For 802.11b/g, the 5GHz ISM band and must specifically support 5.1GHz to 5.9GHz for 802.11a operation. They are required to have a VSWR of 2:1 maximum referenced to a 50Ω system impedance.

ANTENNA SELECTION

The Airborne radio supports a number of antenna options, all of which require connection to the U.FL connectors on the radio. Ultimately the antenna option selected will be determined by a number of factors, including consideration of the application, mechanical construction and desired performance. Since the number of possible combinations is endless, we will review some of the more common solutions in this section. If your application is not covered during this discussion, please contact B+B SmartWorx Technical Support for more specific answers.

The available antenna connections include:

- Host board mounted antenna
- Host chassis mounted antenna
- Embedded antenna

In addition to the above options, location and performance need to be considered. The following sections discuss these items.

HOST BOARD MOUNTED ANTENNA

Host board mounted requires that an antenna connection is physically mounted to the host system board. It also requires that the host board include a U.FL connector to allow a U.FL-to-U.FL coaxial lead to connect from the radio to the host board. It will then require 50Ω matched PCB traces to be routed from the U.FL connector to the antenna mount.

There are several sources for the U.FL-to-U.FL coaxial cable. These include Hirose, Sunridge and IPEX. Please contact B+B SmartWorx for further part numbers and supply assistance.

This approach can simplify assembly but does require that the host system configuration can accommodate an antenna location that is determined by the host PCB. There are also limitations on the ability to seal the enclosure when using this approach.

This approach also restricts the selection of available antennas. When using this approach, antennas that screw or press fit to the PCB mount connector must be used. There are many options for the antenna connector type. However, if you want to utilize the FCC/IC modular approval, the connector choice must comply with FCC regulations. These state that a non-standard connector, e.g. RP-TNC/RP-SMA, is required. TNC/SMA connectors are not allowed.

HOST CHASSIS MOUNTED ANTENNA

Host Chassis mounted antennas require no work on the host PCB. They utilize an antenna type called 'flying lead'. There are two types of flying leads: one that provides a bulkhead mounted antenna connector and one that provides a bulkhead mounted antenna. The type you choose will be determined by the application.

A flying lead system connects a U.FL coaxial lead to the radio's U.FL connector. The other end of the coax is attached to either a bulkhead mounted antenna connector or directly to an antenna that has an integrated bulkhead mount.

In either of the two cases, using this approach significantly reduces antenna system development effort and provides greater flexibility in the available antenna types and placement in the host system chassis.

When using the flying lead antenna (integrated bulkhead mounting), there are no connector choice restrictions for use with the FCC/IC modular certification. However, if the flying lead connector is used, the same restrictions apply as identified for the Host Mounted Antenna.

There are many suppliers of flying lead antenna and connectors. B+B SmartWorx' Airborne antenna product line offers a range of antenna solutions.

EMBEDDED ANTENNA

Use of embedded antennas can be the most interesting approach for M2M industrial and medical applications. Their small form factor and absence of any external mounting provides a very compelling argument. There is a downside to this antenna type and it comes with performance. Antenna performance for all of the embedded options will, in most cases, be less than that achievable with external antenna. This does not make them unusable but, it will impact choice of antenna type and requires more focus on placement.

The three main embedded antenna types are PCB embedded, chip (PCB mounted) and flying lead. Each has its advantages and disadvantages (See Table 13).

Table 13 - Embedded Antenna Options

Antenna Type	Features			
	Cost	Size	Availability	Performance
PCB Embedded	Lowest	Largest	Custom	Poor
Chip	Low	Small	Standard	Poor
Flying Lead	Low	Small	Standard	Fair

PCB Embedded – This approach embeds an antenna design into the host PCB. This is very common with add-in Wi-Fi cards (CF, PCMCIA, SDIO, etc.) as it requires no external connections and is the cheapest production approach. The lower production cost requires significant development cost and lack of performance and flexibility.

Chip – The integration of a chip antenna is simple and requires a relatively small footprint on the host system. However, it does suffer from the same limitations of flexibility and performance as the PCB embedded approach. There are relatively large numbers of suppliers of this type of antenna and a range of configuration and performance options as well.

Flying Lead – This approach is similar to the flying lead solution for external antennas. The difference is the form factors are smaller and provide a range of chassis and board mounting options, all for internal use. This approach suffers less from the performance and flexibility limitations of the other approaches, since the location of the antenna is not determined by the host PCB design. The assembly of a system using this approach maybe slightly more complex since the antenna is not necessarily mounted on the host PCBA.

ANTENNA LOCATION

The importance of this design choice cannot be over-stressed. In fact, it can be the determining factor between success and failure of Wi-Fi implementation.

There are several factors that must to be considered when determining location:

- Distance of antenna from radio
- Location of host system:
  - Proximity to RF blocking or absorbing materials
  - Proximity to potential noise or interference
  - Position relative to infrastructure (access points or laptops)
- Orientation of host system relative to infrastructure:
  - Is it known
  - Is it static

To minimize the impact of the factors above, the following things need to be considered during the development process:

- Minimize the distance between the radio and the location of the antenna. The coaxial cable between the two impacts Transmit Power and Receive Sensitivity negatively. B+B SmartWorx recommends using 1.32-1.37mm outer diameter U.FL coaxial cables.
- Minimize the locations where metal surfaces come into contact or are close to the location of the antenna.
- Avoid locations where RF noise, close to or overlapping ISM bands, may occur. This includes microwave ovens and wireless telephone systems in the 2.4GHz and 5.0GHz frequency range.
- Mount the antenna as high on the equipment as possible.
- Locate the antenna where there is a minimum obstruction between the antenna and the location of the access points. Typically, access points are located in the ceiling or high on walls.
- Keep the main antenna's polarization vertical, or in-line with the antenna of the access points. 802.11 systems utilize vertical polarization and aligning both Transmit and Receive antenna maximizes the link quality.

Even addressing all of the above factors does not guarantee a perfect connection. However, with experimentation, an understanding of the best combination will help identify a preferred.

PERFORMANCE

Performance is difficult to define as the appropriate metric changes with each application or may indeed be a combination of parameters and application requirements. The underlying characteristic that, in most cases, needs to be observed is the link quality. This can be defined as the bandwidth available over which communication between the two devices can be performed. The lower the link quality, the less likely the devices can communicate.

Measurement of link quality can be made in several ways: Bit Error Rate (BER), Signal to Noise (SNR) ratio, Signal Strength (SS), and may also include the addition of distortion. The link quality is used by the radio to determine the link rate. Generally, as the link quality for a given link rate drops below a predefined limit, the radio will drop to the next lowest link rate and try to communicate using it.

The reciprocal is also true. If the radio observes good link quality at one rate, it will try to move up to the next rate to see if communication can be sustained using it. It is important to note that, for a given position, the link quality improves as the link rate is reduced. This is because, as the link rate drops, the radio's Transmit Power and Receive Sensitivity improve.

From this it can be seen that looking at the link rate is an indirect way of assessing the quality of the link between the device and an access point. You should strive to make the communication quality as good as possible in order to support the best link rate. However, be careful not to *over specify* the link rate. Consider your application's bandwidth requirements and tailor your link rate to optimize the link quality. For example, the link quality for a location at 6Mb/s is better than it would be for 54Mb/s. If the application only needs 2Mb/s of data throughput, the 6Mb/s rate would provide a better link quality.

Aside from the radio performance, there are a number of other things that contribute to the link quality. These include items discussed earlier and choices made when looking at the overall antenna gain. The antenna gain contributes to the Equivalent Isotropically Radiated Power (EIRP) of the system. This is part of an overall measurement of the link quality called "link margin".

Link Margin provides a measure of all the parts of the RF path that impact the ability of two systems to communicate. The basic equation looks like this:

EIRP (dB) = TxP + TxA – TxC

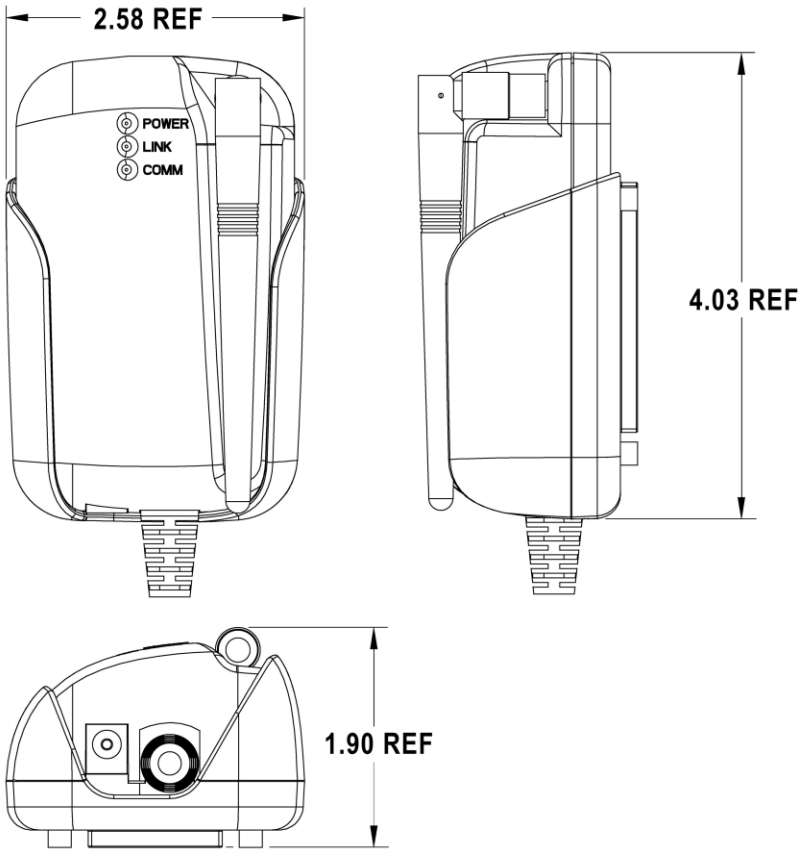
Link Margin (dB) = EIRP – FPL + (RxS + RxA – RxC)

Where:
TxP = Transmitter output power (dBm)
TxA = Transmitter antenna gain (dBi)
TxC = Transmitter to Antenna coax cable loss (dB)
FPL = Free Path Loss (dB)
RxS = Receiver receive sensitivity (dBm)
RxA = Receiver antenna gain (dBi)
RxC = Receiver to Antenna coax cable loss (dB)

This is a complex subject and requires more information than is presented here. B+B SmartWorx recommends reviewing the subject and evaluating any system at a basic level.

It is then possible, with a combination of the above items and an understanding of the application demands, to achieve a link quality optimized for the application and host design. It is important to note that this is established with a combination of hardware selection, design choices, and configuration of the radio.

MECHANICAL OUTLINE – ENTERPRISE CLASS



Antenna Connector: **RP-SMA (Reverse Polarity – SMA)**

Requires 2.4GHz/5GHz ISM band antenna, 50 input impedance, RP-SMA connector

Serial Connector: **DB-9M (Male)**

Requires DB-9 (female)

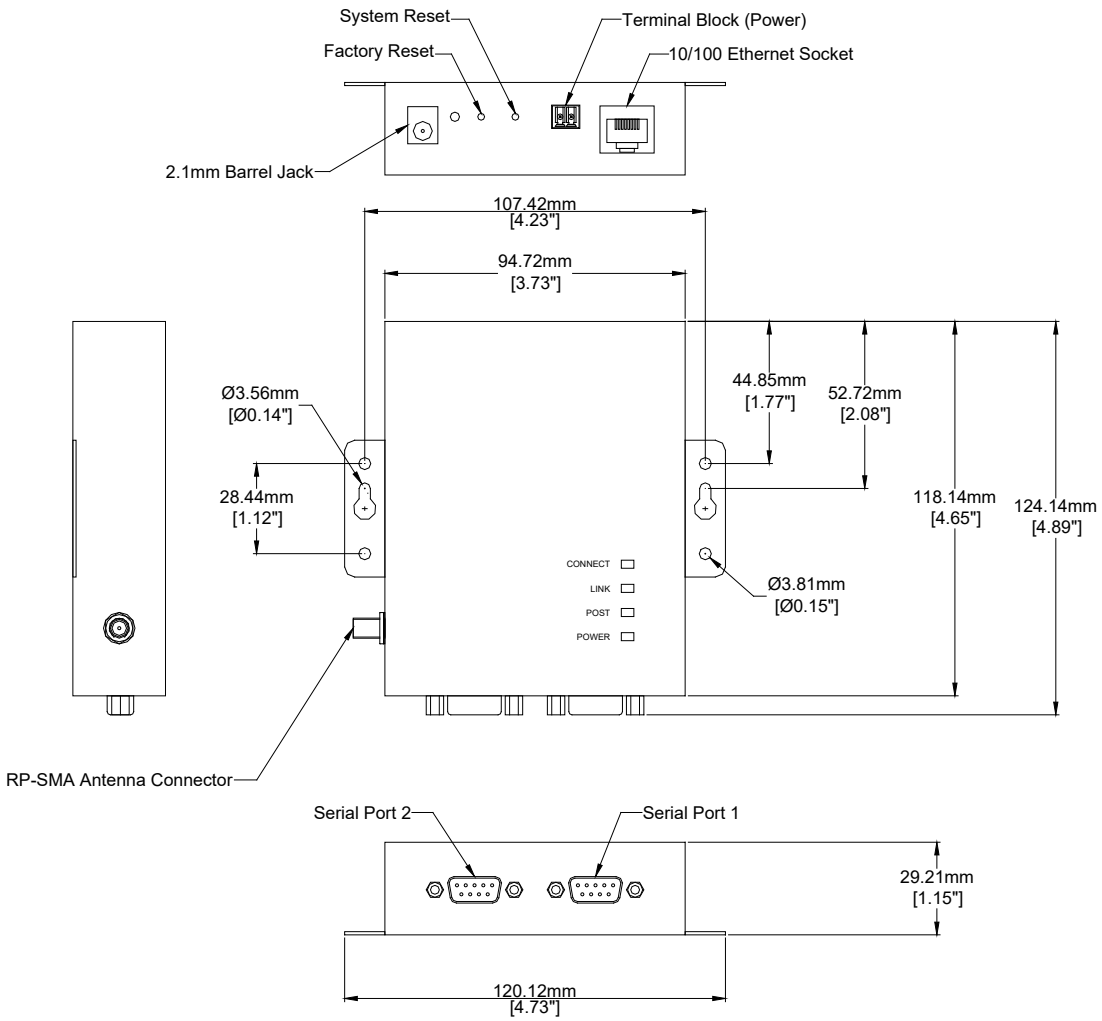
Ethernet Connector: **RJ-45 Plug**

Requires RJ-45 socket, 10/100 Ethernet interface

Power Connector: **2.1mm Barrel Jack**

Requires 2.1mm ID, 5.5mm OD, +5VDC center pin

MECHANICAL OUTLINE – INDUSTRIAL CLASS



Antenna Connector:	**RP-SMA (Reverse Polarity – SMA)** Requires 2.4GHz/5GHz ISM band antenna, 50 input impedance, RP-SMA connector
Serial Connector:	**DB-9M (Male)** Requires DB-9F (female)
Ethernet Connector:	**RJ-45 Socket** Requires RJ-45 plug, 10/100 Ethernet interface
Power Connector:	**2.1mm Barrel Jack** Requires 2.1mm ID, 5.5mm OD, +5VDC center pin
Power Connector:	**Terminal Block (2 connector)** Requires 16-30 AWG gauge wire.

GETTING STARTED

UNPACK THE AIRBORNEM2M™ DEVICE

Unpack the AirborneM2M™ device and compare the package contents with the items listed on the front of the included Quick Start Guide. If any item is missing or damaged, contact B+B SmartWorx immediately.

CONNECT AIRBORNEM2M™ TO HOST

Connect the Airborne Direct unit to a system capable of configuring it. The preferred initial connection depends on the class and type of product:

Serial – Enterprise: Connect to a serial port on the host or through a serial to USB adapter.

Serial – Industrial: Connect the RJ-45 socket to an RJ-45 socket using a CAT 5 Ethernet cable.

Ethernet – Enterprise: Connect to an RJ-45 socket on the host.

Ethernet – Industrial: Connect the RJ-45 socket to an RJ-45 socket using a CAT 5 Ethernet cable.

ATTACH ANTENNA AND POWER-UP THE AIRBORNEM2M™

Attach the supplied antenna to the RP-SMA connector on the AirborneM2M™ unit. Connect the supplied AC adapter to the power connector.

- If using your own power supply, ensure the correct power connector type and polarity are being used.
- Verify the appropriate voltage to be applied by checking Table 8 for the correct product class.
- Confirm the device is receiving power by verifying that the POST LED is lit when the supply is applied.

CONFIGURING DEVICE – INDUSTRIAL SERIAL (ABDX-SE-IN5XXX)

The following describes initial connection to an AirborneM2M™ Serial Device Server (ABDN-SE-IN54xx). If you have an Ethernet device (ABDN-ER-DP55x/IN50xx), please go to section 14.0. If you have purchased an ABDN-SE-DP55x device, please go to section 13.0 for the set-up instructions.

Table 14 provides step-by-step instructions for configuration of the ABDN-SE-IN54xx product family.

Table 14 – ABDN-SE-IN54xx Accessing the Web Interface

1	Open the AirborneM2M™ packaging and locate the Install CD.
2	Place the CD in the CD/DVD drive of the laptop or desktop you will be using to configure the AirborneM2M™ device. Follow the on screen directions for installation of the appropriate device software and documentation.
3	Connect the Ethernet cable on ABDx to an Ethernet port on the laptop or desktop system.
4	Apply power to the ABDN-SE-IN54xx.

5

The unit will boot and display one of the following LED patterns:

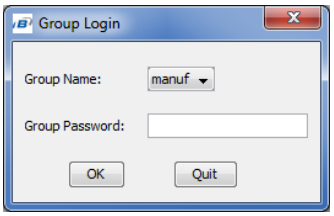
ABDx-SE-IN5xxx

COMM:	● Off
LINK :	● Red
POST:	● Orange
POWER:	● Blue

6

Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system.

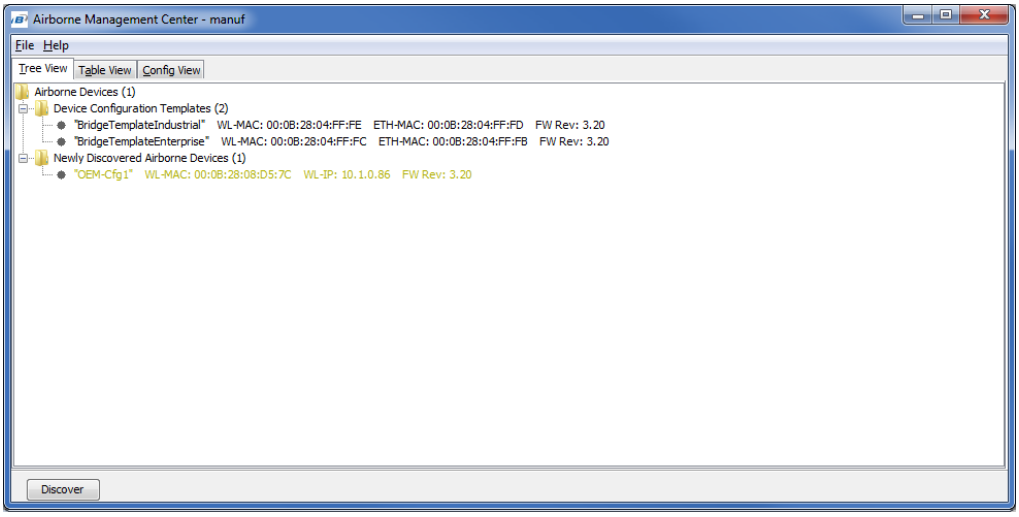
When the application opens, the following dialog will be displayed:



Select Group Name: **manuf** and enter Group Password: **dpac**

7

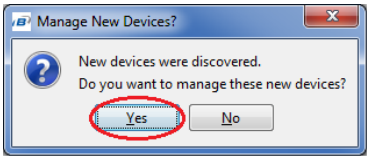
The AMC will load and discover the attached device.

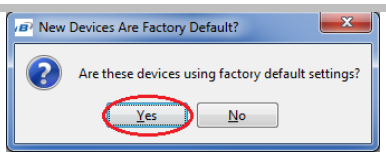


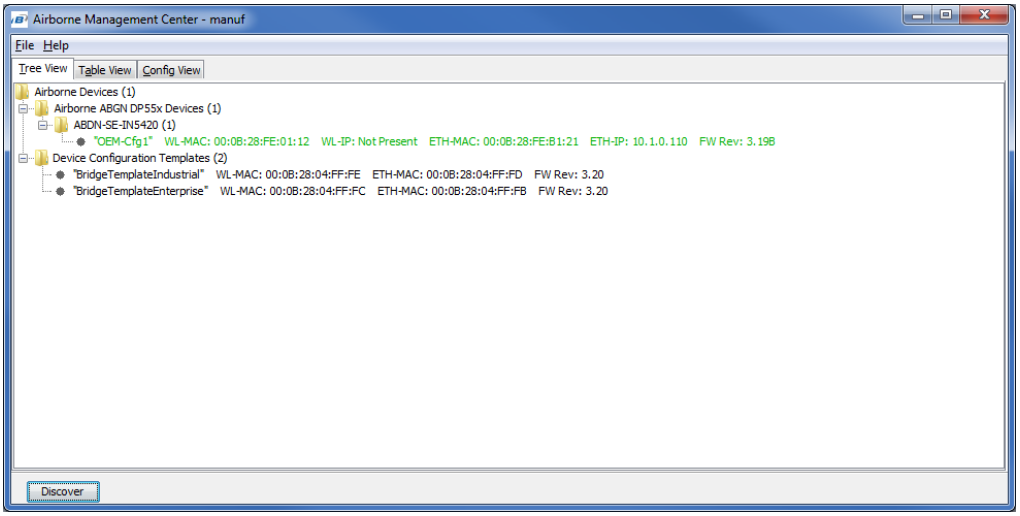
If the unit is not detected, please verify that your firewall is disabled. Run a "Discover". If the unit is still not being detected, close down AMC and restart it by doing a Right-click on the AMC icon and select "Run as administrator".

8

Manage Your Device



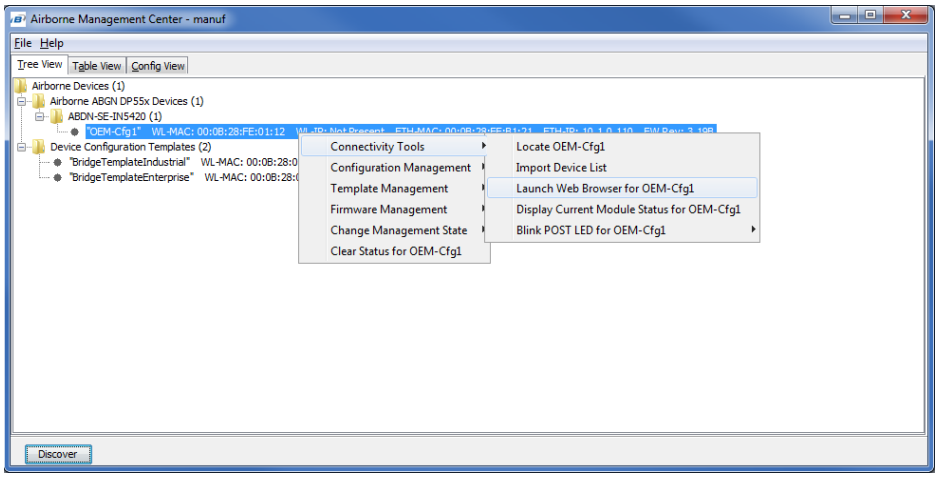




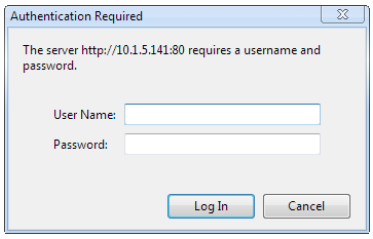
9

The devices status will move to managed and the device will be displayed under the device type/group it belongs to. Right-click the device and then:

1. Select **Connectivity Tools**
2. Select **Launch Web Browser for OEM-Cfg1**



Username= “dpac”
Password = “dpac”

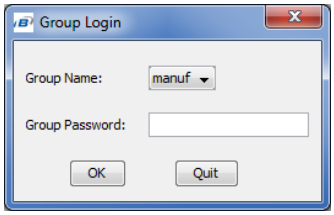


10	Opening web page shows adapter status. Links to the available configuration options are identified in the left hand menu. The top menu bar provides access to different operations that can be performed by the AirborneM2M™ device. See section 15.0 for a full description of how to use the web interface.
11	Using Express Setup: If this is the first time you have configured the device, the Express Setup page will be displayed. Please refer to section 16.0 to continue set-up of the device. If this is not the first time, proceed to section to update configuration.
12	When the **Reboot** button is pressed, the unit will restart and install new settings. This may take 15-20 seconds. Please refresh the web interface after the boot cycle has completed.
13	When configured correctly, the LED pattern should match the following: **ABDx-SE-IN5xxx** — *No TCP Connection* — *TCP Connection* COMM: ● Off — ● Green LINK : ● Green — ● Green POST: ● Green — ● Green POWER: ● Blue — ● Blue
14	To use the adapter on the wireless network, address all traffic to the IP address of the wireless interface of the ABDN-SE- IN54xx. This address is listed in the home page of the web interface.

CONFIGURING DEVICE – ENTERPRISE/INDUSTRIAL ETHERNET (ABDN-ER-DP55X/-XX-IN5XXX)

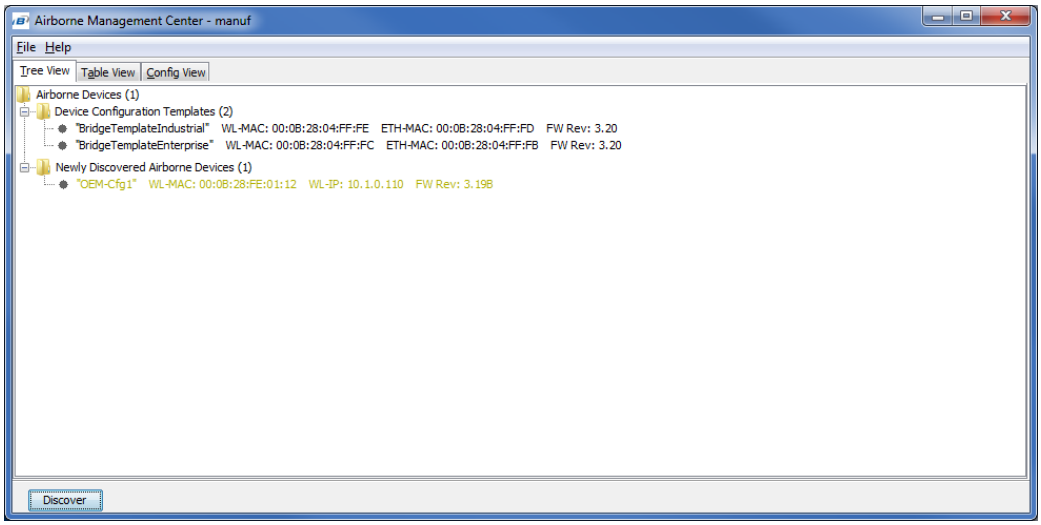
The following instructions describe how access the AirborneM2M™ Ethernet device and web interface for initial configuration of the unit.

Table 15 – ABDN-ER-DP55x / ABDN-xx-IN5xxx Accessing the Web Interface

1	Open the AirborneM2M™ packaging and locate the Install CD.
2	Place the CD in the CD/DVD drive of the laptop or desktop that you will be using to configure the AirborneM2M™ device. Follow the onscreen directions for installation of the appropriate device software and documentation.
3	Connect the Ethernet cable on ABDx to an Ethernet port on the laptop or desktop system.
4	Apply power to the ABDx-ER-DP5xx/IN5xxx.
5	The unit will boot and display one of the following LED patterns: **ABDx-ER-DP5xx** — *Associated (Open Network)* — *Not Associated* POWER: Green — Green LINK : Green — Red (Periodic Blinking) COMM: Red — Red **ABDx-ER-IN5xxx** COMM: Off LINK : Off POST: Orange POWER: Blue
6	Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system. When the application opens. the following dialog will be displayed:  Select Group Name: **manuf** and enter Group Password: **dpac**

7

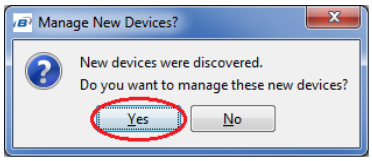
The AMC will load and discover the attached device.

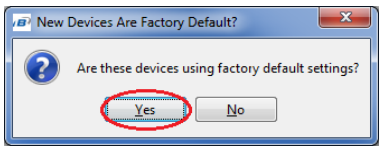


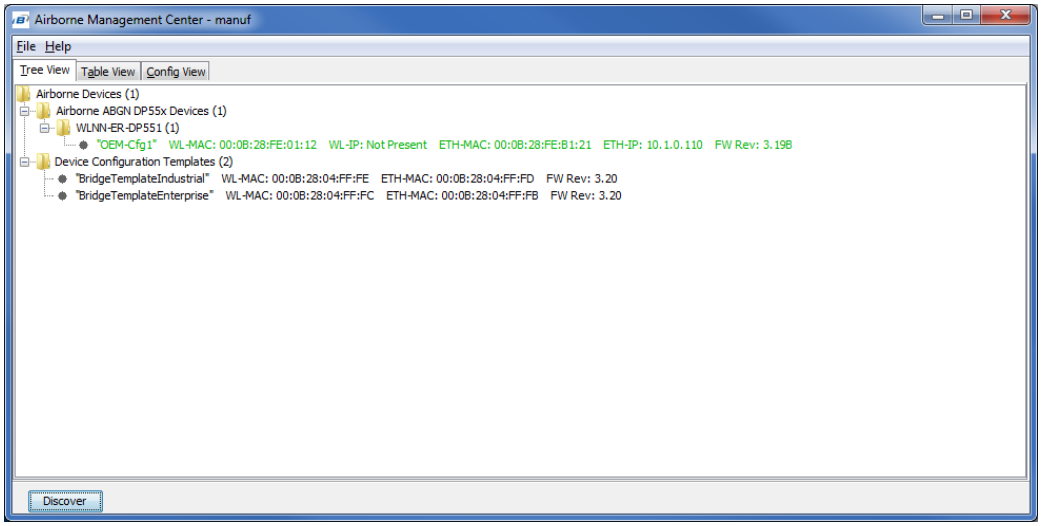
If the unit is not detected. please verify that your firewall is disabled. Run a "Discover". If the unit is still not being detected, close down AMC and restart it by doing a Right-click on the AMC icon and select "Run as administrator".

8

Manage Your Device

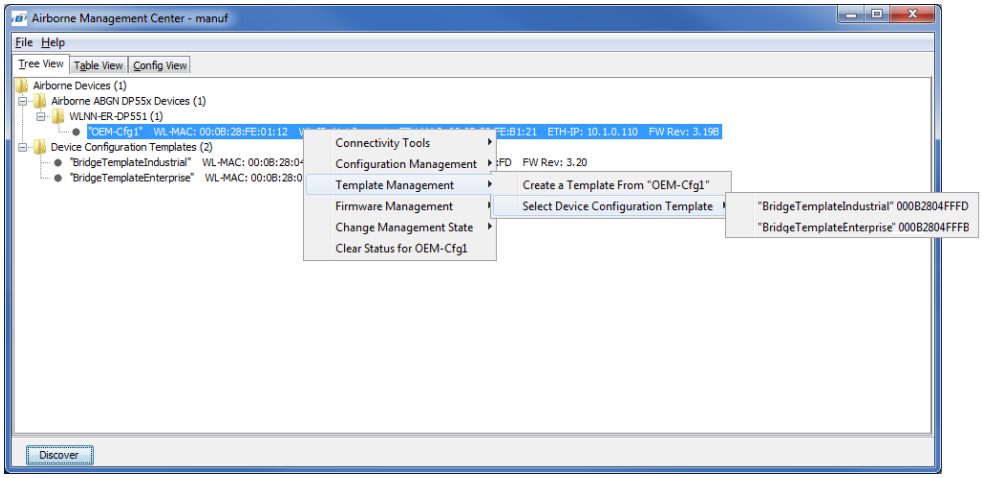






The device's status will move to managed and the device will be displayed under the device type/group it belongs too.
To convert the Ethernet device to Bridge mode, follow these steps:

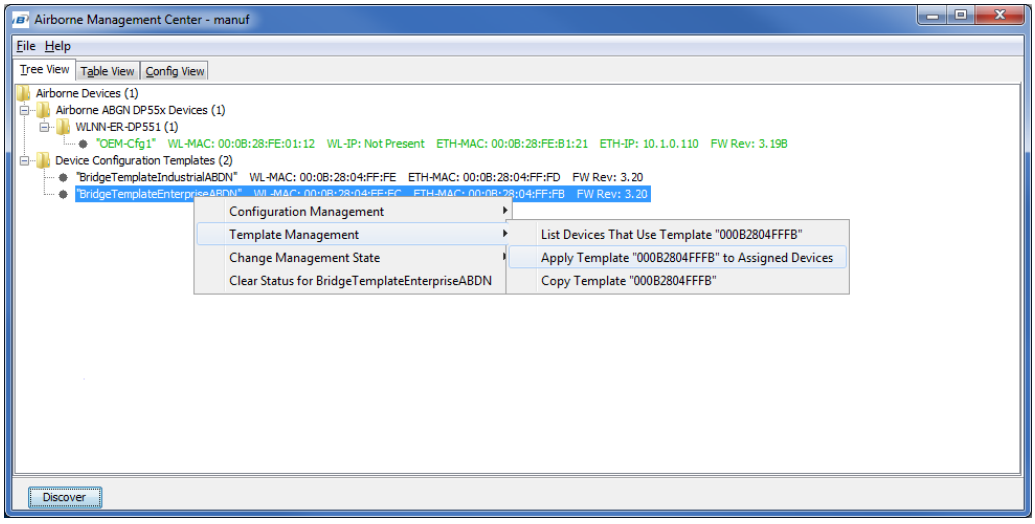
1. Right-click the device (or select multiple devices first, then right-click a device)
2. Select **Template Management**
3. Select **Select Device Configuration Template**
4. Select the correct bridge template



9

Once you have assigned the template to the devices, you can then apply the template using these steps:

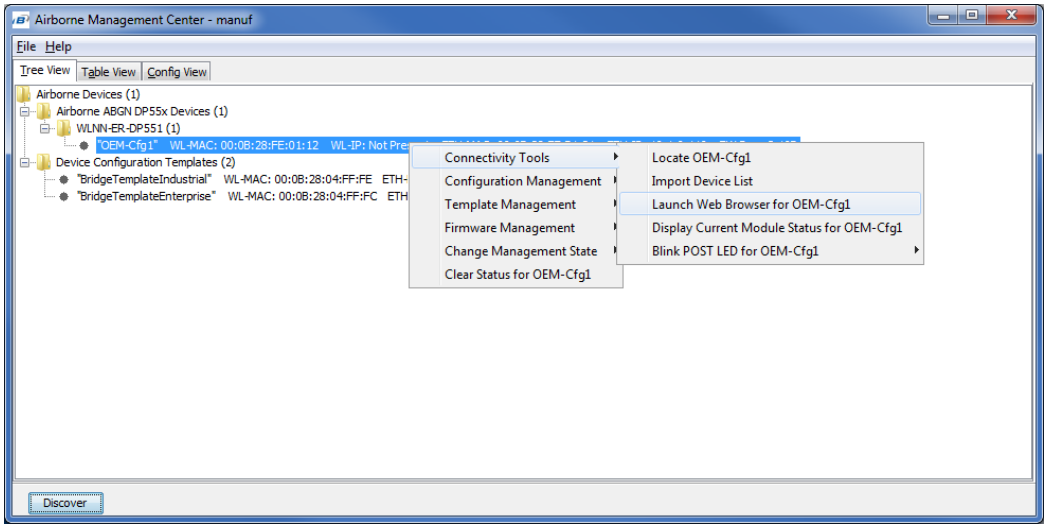
1. Right-click the **Template**
2. Select **Template Management**
3. Select **Apply Template "*template id*" to Assigned Devices**



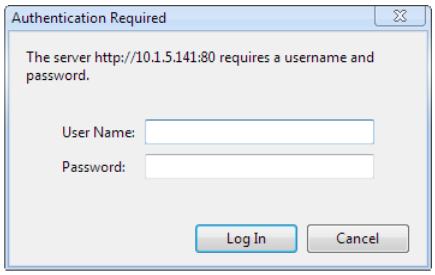
10

Now launch the Web Browser and configure the device. Right-click the device and then:

1. Select **Connectivity Tools**
2. Select **Launch Web Browser for OEM-Cfg1**



Username= “dpac”
Password = “dpac”



11

Opening web page shows adapter status.
Links to the available configuration options are identified in the left hand menu.
The top menu bar provides access to different operations that can be performed by the AirborneM2M™ device.
See section 15.0 for a full description of how to use the web interface.

12

Using Express Setup:
If this is the first time you have configured the device, the Express Setup page will be displayed, please refer to section 16.0 to continue set-up of the device.
If this is not the first time, proceed to section to update configuration.

13

When the **Reboot** button is pressed, the unit will restart and install new settings. This may take 15-20 seconds. Please refresh the web interface after the boot cycle has completed.

14	When configured correctly the LED pattern should match the following: **ABDN-ER-DP5%x** POWER: Green LINK : Green COMM: Red **ABDN-ER-IN5xxx** — *No TCP Connection* — *TCP Connection* COMM: Off — Green LINK : Green — Green POST: Green — Green POWER: Blue — Blue
15	To use the adapter on the wireless network, address all traffic to the IP address of the wireless interface of the ABDx-ER-DP5xx/IN5xxx. This address is listed in the home page of the web interface.

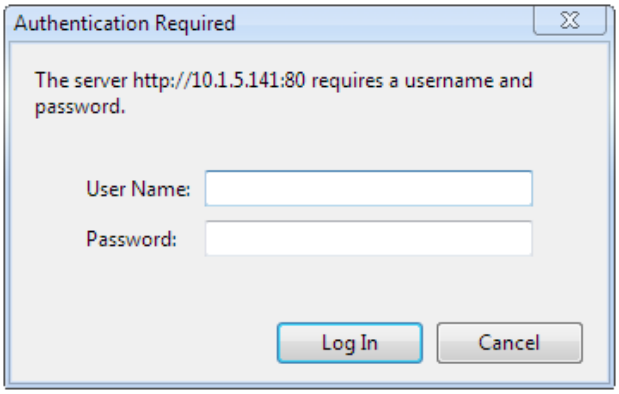
USING THE WEB INTERFACE

AirborneM2M™ Device Servers and Wireless Adapters include a web interface that provides access to module status, parameter modification, certificate and configuration file management. To use the web interface, follow the steps outlined in section 14.0 to establish the IP address of the module. Once the IP address is known, open a web browser and enter the IP address of the module in the URL window.

The web interface currently supports Internet Explorer v6.0 thru 9.0, Firefox v3.x+, Opera v9.6+, Chrome v4.0+ and Safari v5.0.5+.

When the authentication request is returned enter:

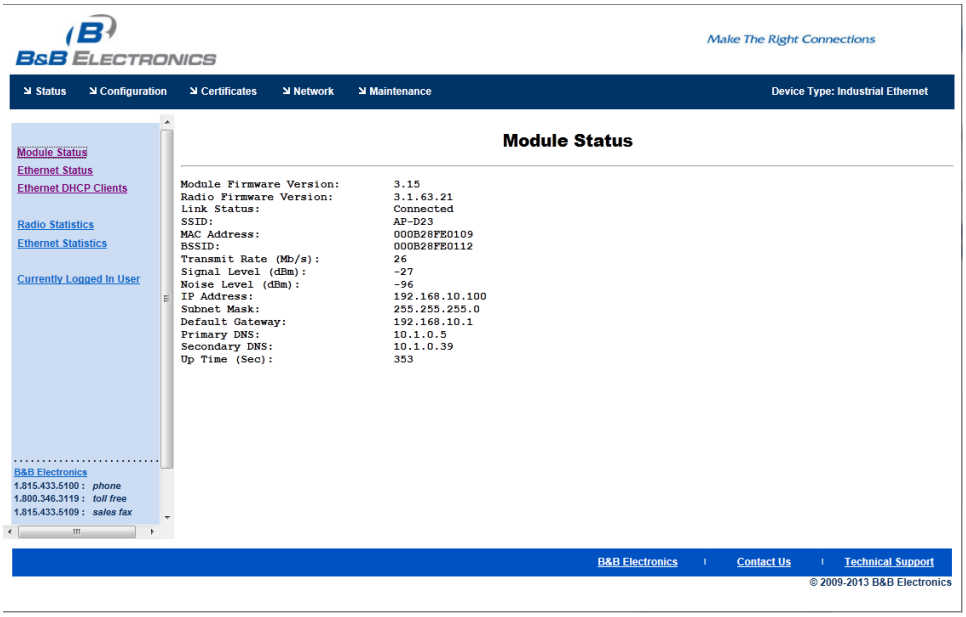
Figure 8 - Website Login



Username: dpac
Password: dpac

After successfully authenticating with the module, you will be logged into the web server. If this is the first time you have accessed the device the Express Setup page will be displayed see section 16.0 for configuration of the device using this page. If you have previously configured the device the default home page will be displayed (see Figure 9). From here you can update device settings if required. A quick overview of the web interface follows.

Figure 9 - Default Home Page



NAVIGATION BAR

Figure 10 - Website Navigation Bar

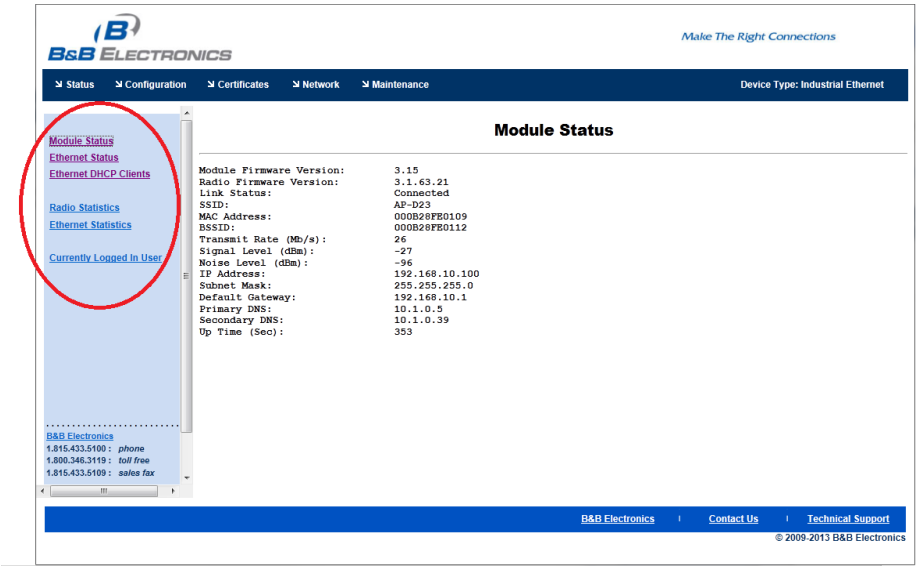
Table 16 - Navigation Bar Items

Title	Description
Status	Provides status and performance characteristics for the network interfaces available. Includes connection status, radio and Ethernet statistics.
Configuration	Allows viewing and configuration of all the interface settings including wireless LAN, network connectivity, security, FTP client, serial port and web server. Includes the interface for delivery of OEM and user configuration files, as well as management and viewing of current configurations.
Certificates	This menu item provides the interface for certificate delivery and management. Included in this section are the abilities to view resident certificates, upload and delete certificates.
Network	With this section, it is possible to locate other Airborne Device Server modules on the current network. It is also possible to scan for available Access Points.
Maintenance	This section allows the updating of the module's firmware. You can also revert the device settings to OEM defaults and restart the module remotely. The module locate function is also enabled in this section.

FEATURE LINKS

Each Navigation Bar link has a set of Features/Fields that it allows access to. These are different for each Navigation option and change for different device selections. The Feature Links are located in the left hand panel of the web page (see Figure 11).

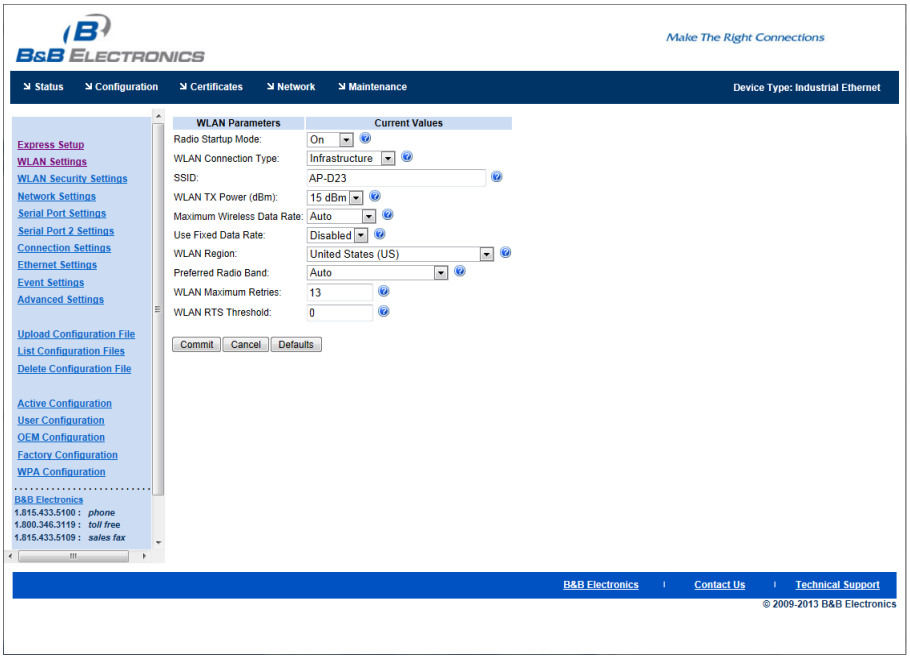
Figure 11- Feature Links



NAVIGATING THE WEBSITE

A standard web page looks like Figure 12. The navigation bar runs along the top of the page; page specific feature links are list in the left hand pane of the page; and specific parameters are shown in the main display panel.

Figure 12 - Airborne Web Page



To select any of the items, move your cursor over the item and press the Left-hand mouse button. The items in the Navigation bar and the Feature Links are hyperlinks and will cause the mouse cursor to change form an arrow pointer to a finger pointer when placed over them.

To find out what a specific field does, move the cursor over the field and hover for about a second. A help balloon will appear and will provide details on the function of the field and its valid range of values.

UPDATING A FIELD

To update a field, select the field by pressing the Left-hand mouse button. Then, either type in the appropriate content or select from the pull-down menu.

Once you have finished modifying parameters, scroll to the bottom of the page and press the **Commit** button. The page will then indicate that changes have been completed successfully. You can then return to the configuration page by pressing the **Reload** button or restart the module by pressing the **Reboot** button.

Note that the changes to the parameters will not be applied until a module restart (reboot) has been completed.

Before the **Commit** button has been pressed, all modified fields can be returned to their original state by pressing the **Cancel** button.

UPLOADING CERTIFICATES

Adding certificates to the Airborne Device Server module is easy when using the web interface.

Figure 13 - Upload Certificate Web page

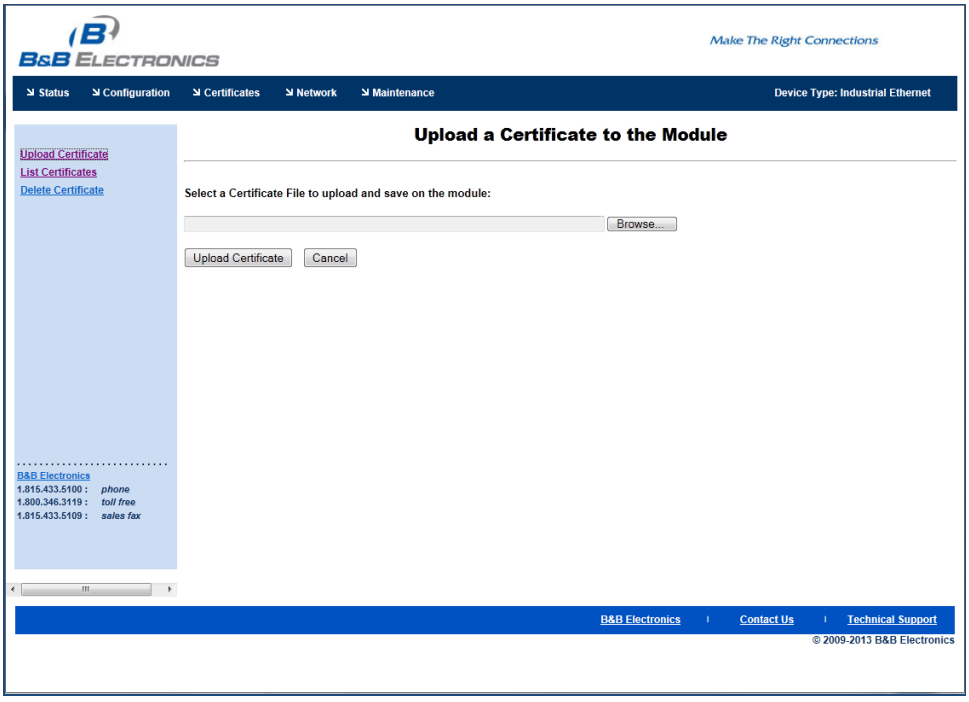


Table 17 - Uploading Certificates

Step	Description
Navigation Bar Select **Certificates**	You will see a list of certificates currently resident on the module when you enter the Certificate File List window.
Feature Link Select **Upload Certificates**	You will see a window open with a field to enter the location of the certificate you want to upload.
Press **Browse...** Button	This will open a dialog box in which you can locate the certificate that you want to upload to the module. Select the Certificate file and press **Open**. This will return you to the Certificate Upload window and will have entered the location and file name of the certificate you want to upload in the field next to the **Browse...** button.
Press **Upload Certificate**	You will then see a notice that the certificate has been successfully uploaded to the module.
Press **List certificates Files**	This will show the current certificates resident on the module and will include the file just uploaded.

UPLOAD CONFIGURATION FILES

The Airborne Device Server module supports User, Encrypted and OEM configuration files for provisioning the module. Delivery of these configuration files can be performed through the web interface. A full description of these files can be found in the Airborne CLI manual.

To upload configuration files, follow the steps in Table 14.

Figure 14 - Upload Configuration Web Page

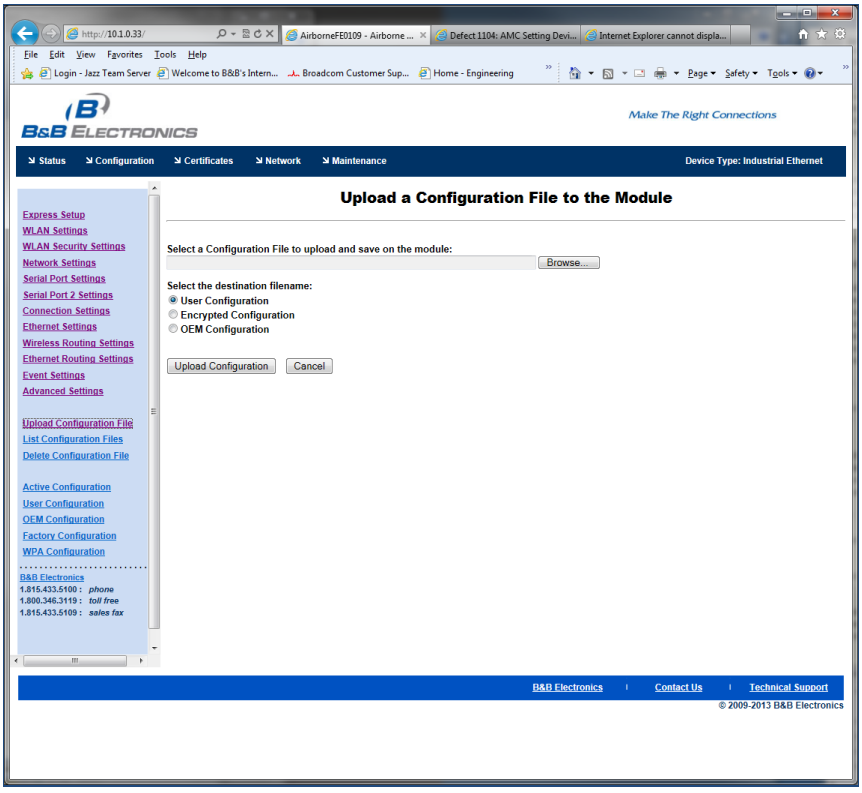


Table 18 - Uploading Configurations

Step	Description
Navigation Bar Select **Configuration**	You will see major WLAN parameters displayed.
Feature Link Select **Upload Configuration File**	You will see a window open with a field to enter the location of the configuration you want to upload, along with a choice of User, Encrypted or OEM Configuration.
Press **Browse...** Button	This will open a dialog box in which you can locate the file that you want to upload to the module. Select the configuration file and press **Open**. This will return you to the Configuration Upload window and will have entered the location and name of the file that you want to upload in the field next to the **Browse...** button.
Select **User, Encrypted** or **OEM Configuration**	This defines the configuration you are installing. Only the OEM Configurations will survive a factory reset.
Press **Upload Configuration**	You will then see a notice that the configuration has been successfully uploaded to the module.
Press **List Configuration Files**	This will show the current configuration files resident on the module and will include the file just uploaded.

Uploading a configuration file will overwrite any configuration file already stored on the module. This will cause a change in configuration when a module restart is performed.

IMPORTANT: Confirm that the OEM or USER settings in the configuration files will allow the user to communicate with the module after the upload and a restart has been completed.

UPDATING FIRMWARE

The module's firmware may be updated using the web interface. Please refer to Table 22 for the procedure to do this.

Updating the firmware will not alter any existing configuration files or certificates loaded on the module.

You will first need to obtain the version of firmware you want to install from the B+B SmartWorx website or B+B SmartWorx Technical Support. The firmware will be a binary image file (.img) and indicate the version of the firmware within the file name.

Once you have obtained the firmware, save the firmware image to a location on the system you are browsing the module from, or a location accessible to the system you are browsing the module from.

Figure 15 - Firmware Update Page

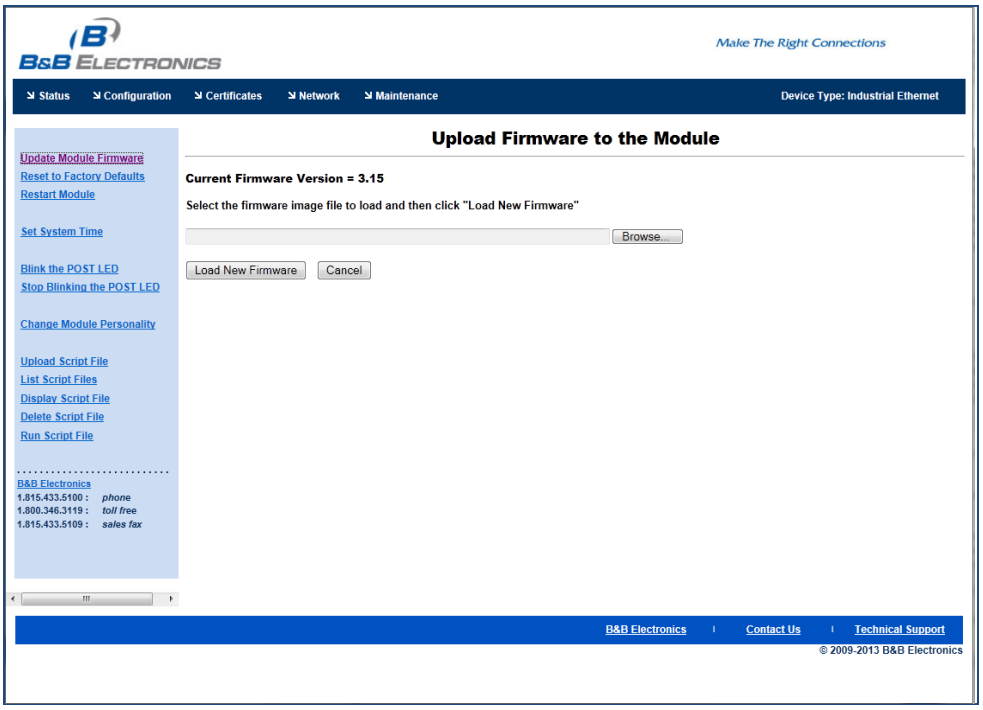


Figure 16 - Firmware Update in Progress

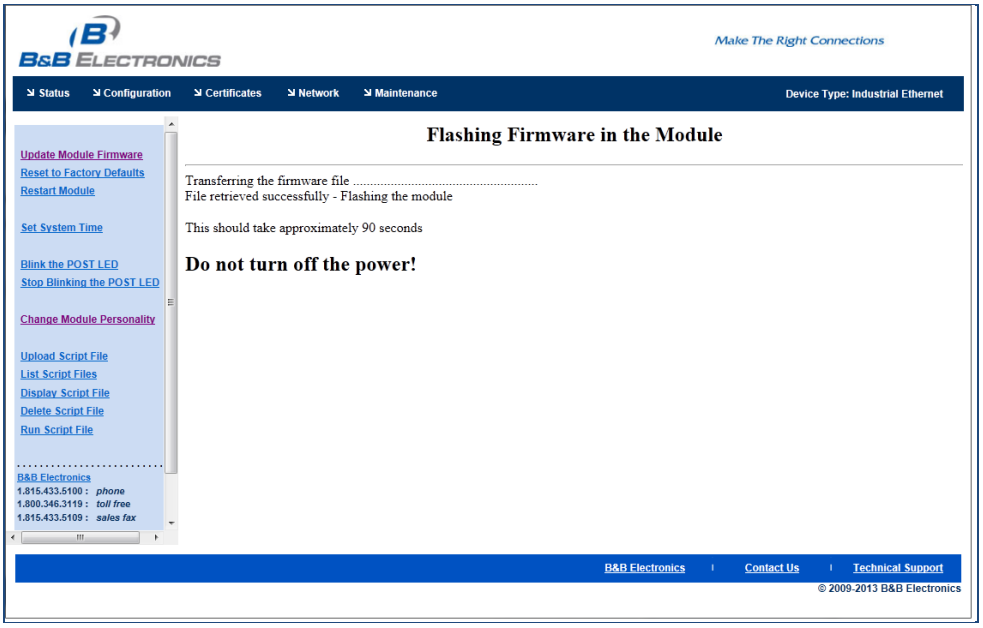


Figure 17 - Firmware Update Complete

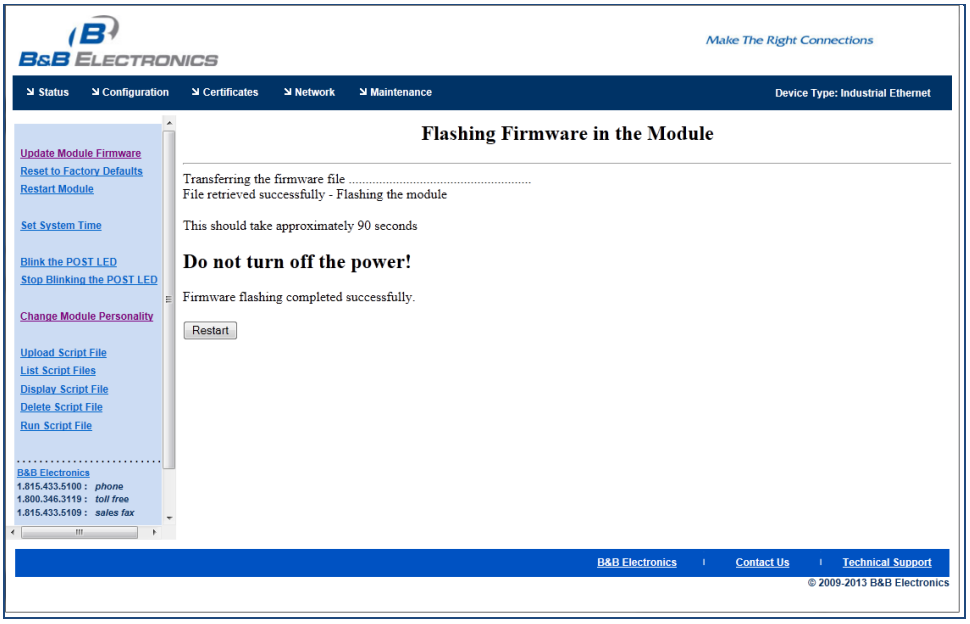


Table 19 - Updating Firmware

Step	Description
Navigation Bar Select **Maintenance**	This will open a window showing the current module status.
Feature Link Select **Update Module Firmware**	You will see a window open with a field to enter the location of the module firmware that you want to upload. The current firmware version number is displayed at the top of the page.
Press **Browse...** Button	This will open a dialog box in which you can locate the firmware image you want to upload to the module. Select the firmware image file and press **Open**. This will return you to the Upload Firmware window and will have entered the location and file name of the firmware image that you want to upload in the field next to the **Browse...** button.
Press **Load New Firmware**	You will then see a notice that the firmware upload has begun (**Error! Reference source not found.**). When the upload has been completed successfully and the firmware updated, a window indicating this will be shown (Figure 17).
Press **Reboot**	This will restart the module and the new firmware will be loaded.

DO NOT REMOVE POWER FROM THE MODULE DURING THE FIRMWARE UPDATE.

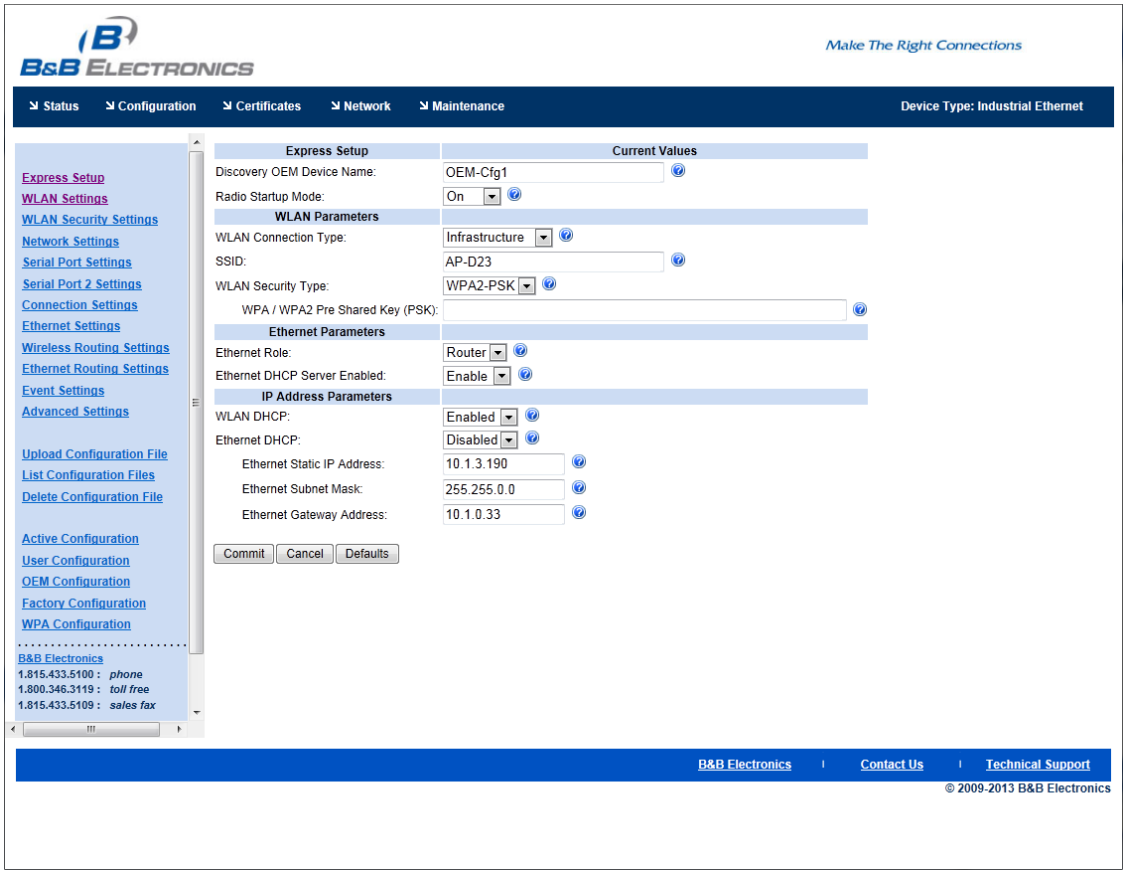
This may cause the device to become non-operational. If this happens, contact B+B SmartWorx Technical Support.

EXPRESS SETUP CONFIGURATION PAGE

When the device's web interface is accessed for the first time an Express Setup page will be shown. This page is designed to allow a quick device set-up by presenting the most popular device configuration options in a single location. For more advanced configurations the full set of options are available in the feature links (left-hand column).

The Express Setup web page will display the necessary fields based on the selections made during configuration. The Express Setup page looks like (Figure 18):

Figure 18 - Express Setup Page



To configure the device for operation, each field must be configured correctly. The following steps should be taken to configure the device (Note: not all fields will be visible):

Table 20 - Express Page Setup

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN parameters.
Feature Link Select **Express Setup**	This step is optional. If this is the first time the device has been configured, this page will automatically be displayed.
Select **Discovery OEM Device Name**	This parameter allows you to name the device uniquely or group into a functional set. When device discovery is used, this name identifies the found device. If you wanted to uniquely identify the device, you could mark it with a label e.g. Dev1, and then enter Dev1 in this field. When the device is found, it will identify itself as Dev1. Alternately, you could indicate the type of equipment the device is attached to e.g. Haas TL-2 (CNC Turning Center), by giving the unit a name like Haas_TL_2. When discovered, you can then identify the device you are accessing. Enter the text string is you want to change the default value. This field is optional.
Select **Radio Startup Mode**	Select **On** from the drop down menu for the radio to operate.
Select **Wireless LAN Connection Type**	If you are using Access Points, make sure this is set to **Infrastructure** from the drop down menu. If you want to use **AdHoc,** set this accordingly. Additional settings may be required to fully configure for AdHoc mode. These are covered if section 17.2.
Select **SSID**	Enter the name of the wireless network you want to access. This field is case sensitive.
Select **Wireless LAN Security Type**	Select the security type the wireless network you want to access is using. Depending on the option you choose, you may have to enter additional information. Once you have selected the security type, the required inputs will be displayed. All displayed fields must be completed. If the security type is not in the available selections, more are available in the *WLAN Security Settings* page. If you choose to use this page, make sure you commit the change before selecting the *WLAN Security Settings* page.
Select **WLAN DHCP**	If your WLAN network uses DHCP to assign IP addresses to the wireless clients, select **Enabled** from the drop down menu. If you are using static IP addresses, select **disabled** from the drop down menu. **WLAN Static IP** and **WLAN Subnet Mask** will need to be entered.
Select **Ethernet DHCP**	If the Ethernet network connected to the Ethernet port uses DHCP to assign IP addresses to the wired clients, you should select **Enabled** from the drop down menu. If you are using static IP addresses, you should select **Disabled** from the drop down menu. **Ethernet Static IP** and **Ethernet Subnet Mask** will need to be entered. **Important:** This field is only used if the Ethernet interface is set as a client (default for serial devices). If set as a router, the field is ignored. See section 21.0 for a full description of configuring the unit as an Ethernet router.
Select **WLAN Static IP**	This field defines the static IP address for the wireless interface. This address is only used if the **WLAN DHCP** is disabled or DHCP failed. Default: **192.168.10.1**

Step	Description
Select **WLAN Subnet Mask**	This field defines the subnet mask used by the wireless interface. This mask is only used if the **WLAN DHCP** is disabled or DHCP failed. Default: **255.255.255.0**
Select **Ethernet Static IP**	This field defines the static IP address for the Ethernet interface. When configured as a serial device server (Ethernet interface is in **client** mode) this address is only used if the **Ethernet DHCP** is disabled or DHCP failed. Default: **192.168.2.100**
Select **Ethernet Subnet Mask**	This field defines the subnet mask used by the Ethernet interface. When configured as a serial device server (Ethernet interface is in client mode) this mask is only used if the **Ethernet DHCP** is disabled or DHCP failed. Default: **255.255.255.0**
Select **Ethernet Gateway Address**	This field defines the gateway IP address used by the Ethernet interface. When configured as a serial device server (Ethernet interface is in client mode) this mask is only used if the **Ethernet DHCP** is disabled or DHCP failed. Default: **192.168.2.1**
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Express Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses it will be necessary to configure the network interface, see the next step.

The web interface supports advanced configuration of the device through the additional pages available. The following sections provide guidance on how to use these pages for specific configurations.

CONFIGURING THE WIRELESS INTERFACE

The following section will outline how to configure the wireless interface for both infrastructure and AdHoc networks.

CONFIGURING FOR INFRASTRUCTURE NETWORKS

Infrastructure networks use Access Point and/or Wireless Routers to provide wireless access to a network. Each wireless network is identified by a name referred to as the SSID (**S**ervice **S**et **ID**entifier). To configure the device with the necessary parameters to operate with an infrastructure network, use the following steps.

Table 21 - Configuring Wireless Interface - Infrastructure

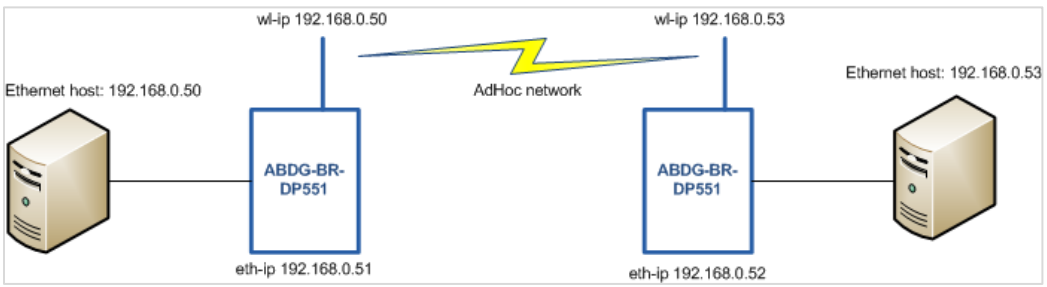
Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Settings**	This step is optional. The default home page for the **Configuration** link in the **Navigation Bar** is **WLAN Settings**.
Select **Radio Startup Mode**	Select **On** from the drop down list.
Select **Wireless LAN Connection Type**	Select the **Infrastructure** form the drop down list.
Select **SSID**	Enter the name of the wireless network that you want the device to use. This cannot include spaces.
Select **Wireless LAN Region**	Select the most appropriate region for the deployment location of the device.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **WLAN Settings** page.
Feature Link Select **WLAN Security Settings**	The wireless interface is now configured. However, most wireless networks use security to protect the network and users from unauthorized use. Selecting **WLAN Security Settings** will allow configuration of the device's security settings for the network. This is covered in section 18.0.

CONFIGURING FOR ADHOC NETWORKS

AdHoc networks use peer-to-peer connection to create a local wireless network. These can be useful when no infrastructure (AP) is available. Each wireless network is identified by a name referred to as the ESSID (**E**xtended **S**ervice **S**et **ID**entifier). To configure the device with the necessary parameters to operate with an AdHoc, use the following steps.

Table 22 - Configuring Wireless Interface - AdHoc

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Settings**	This step is optional. The default home page for the **Configuration** link in the **Navigation Bar** is **WLAN Settings**.
Select **Radio Startup Mode**	Select **On** from the drop down list.
Select **Wireless LAN Connection Type**	Select the **AdHoc** from the drop down list.
Select **Wireless LAN Channel**	This determines the 802.11 channel that the device will use when it establishes a connection with another device in the AdHoc network. Select a channel that is clear, i.e. one which has no other 802.11 network using it. It is not necessary for all devices in a single AdHoc network to have the same channel number selected.
Select **SSID**	Enter the name of the wireless network that you want the device to use. This cannot include spaces.
Select **Wireless LAN Region**	Select the most appropriate region for the deployment location of the device.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **WLAN Settings** page.
Feature Link Select **WLAN Security Settings**	The wireless interface is now configured. However, most wireless networks use security to protect the network and users from unauthorized use. Selecting **WLAN Security Settings** will allow us to configure the devices security settings for the network. This is covered in section 18.
Feature Link Select **Network Settings**	The wireless interface is now configured. However, most AdHoc networks do not have a DHCP server available to provide IP address to the devices in the network. Therefore, it is necessary to assign a static IP address to the wireless interface. Selecting **Network Settings** will allow configuration of the device with a static IP address. This is covered in section 19.0. A bridge unit will require static IP addresses.



CONFIGURING THE SECURITY SETTINGS

Almost all 802.11 networks use some sort of security to protect the network from unauthorized use. There are many types of security options available. The following section will cover how to configure the device for the most popular options. If your security configuration is not covered, further details can be found in the Airborne Enterprise CLI Reference Manual.

CONFIGURING FOR WEP SECURITY

Although an old protocol WEP is still used by many networks, the Airborne device supports many variations of WEP. However, only the most popular ones are covered in the following table. If the basic 64 or 128 bit WEP configuration does not work, please refer to the Airborne Enterprise CLI Reference Manual for the other available options.

Table 23 - Configuring for WEP Security

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Security Settings**	The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed.
Select **Wireless LAN Security**	Select **WEP64** or **WEP128** from the drop down list. The options identify the length of the key that will be used with the security protocol.
Select **Authentication Type**	Select **Auto** from the drop down list. This field should not need to be changed. Only modify if you have been specifically told to by the network administrator.
Select **Default WEP Key**	Select the key number that matches the selection used by the AP's in the wireless network. This must match for authentication to be successful. There must be a valid key in the selected key number field.
Select **WEP Key 1 - 4**	Select the key field that matches the one selected in Default WEP Key field. Enter the key exactly as it is entered into the AP. If **WEP64** is selected the key length is 10 digits. If **WEP128** is selected the key length is 26 digits. More than one key field can be completed.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **WLAN Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range the wireless interface will connect. If the network is using DHCP, then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses, it will be necessary to configure the network interface. See the next step.
Feature Link Select **Network Settings**	The wireless interface is now configured. However, if the WLAN network does not have a DHCP server available to provide IP address to the device, it is necessary to assign a static IP address to the wireless interface. Selecting **Network Settings** will allow us to configure the device with a static IP address. This is covered in section 19.0.

CONFIGURING FOR WPA-PSK SECURITY

This security type is a very popular type and is easy to configure. Most often used in SOHO and home environments, some enterprise networks do use it.

Table 24 - Configuring for WPA Security

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Security Settings**	The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed.
Select **Wireless LAN Security**	Select **WPA-PSK** from the drop down list.
Select **WPA Protocol Version**	Select **Auto** from the drop down list. This field should not need to be changed. Only modify if you have specifically been told to by the network administrator.
Select **WPA/WPA2 Pre Shared Key (PSK)**	Enter the PreShared Key used by the AP. The PSK is case sensitive and must be entered exactly as it is in the AP. The PSK cannot include spaces.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **WLAN Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device is rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. If the network is using DHCP, then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses, it will be necessary to configure the network interface. See the next step.
Feature Link Select **Network Settings**	The wireless interface is now configured. However, if the WLAN network does not have a DHCP server available to provide IP address to the device, it necessary to assign a static IP address to the wireless interface. Selecting **Network Settings** will configuration of the device with a static IP address. This is covered in section 19.0.

CONFIGURING FOR WPA2-PSK SECURITY

This security type is a very popular type and is easy to configure. Most often used in SOHO and home environments, WPA2-PSK is starting to be widely used by enterprise networks.

Table 25 - Configuring for WPA2 Security

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Security Settings**	The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed.
Select **Wireless LAN Security**	Select **WPA2-PSK** from the drop down list.
Select **WPA/WPA2 Pre Shared Key (PSK)**	Enter the PreShared Key used by the AP. The PSK is case sensitive and must be entered exactly as it is in the AP. The PSK cannot include spaces.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **WLAN Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. If the network is using DHCP, then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses, it will be necessary to configure the network interface. See the next step.
Feature Link Select **Network Settings**	The wireless interface is now configured. However, if the WLAN network does not have a DHCP server available to provide IP address to the device, it is necessary to assign a static IP address to the wireless interface. Selecting **Network Settings** will allow configuration of the device with a static IP address. This is covered in section 19.0.

CONFIGURING FOR PEAP SECURITY

This security type is a very popular type for enterprise networks. Actual use of the security protocol requires that the network is using a RADIUS server for device authentication. Depending on the security policies of the network, this protocol supports authentication with and without a CA (Certification Authority) certificate.

The Airborne device supports PEAPv0 using both WPA (TKIP) and WPA2 (AES-CCMP) encryption. The device will automatically use the most appropriate encryption type to obtain authentication to the WLAN.

Table 26 - Configuring for PEAP Security

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **WLAN Security Settings**	The wireless interface must be configured before configuring the security for the network. A page showing the range of security options and fields is displayed.
Select **Wireless LAN Security**	Select **PEAP** from the drop down list.
Select **EAP Identity**	Enter the RADIUS server account name provided by the network administrator. If a Windows domain server is being used for authentication, the server domain must be included in the **EAP Ident** field
Select **EAP Password**	Enter the RADIUS server account password for the **EAP Ident**.
Select **EAP Phase 1 String**	Enter `peaplabel=0`
Select **EAP Phase 1 String**	Enter `auth=MSCHAPV2`
Select **CA Certificate Filename**	Enter the name of the Certificate Authority (CA) certificate stored on the device. Storing Certificates on the device is cover in section 15.5. If the network security does not require the use of a CA certificate, this field should be left blank.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **WLAN Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device is rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. If the network is using DHCP, then an IP address will be assigned to the WLAN interface and IP connectivity is possible over the WLAN network. If the network is using static IP addresses, it will be necessary to configure the network interface. See the next step.
Feature Link Select **Network Settings**	The wireless interface is now configured. However, if the WLAN network does not have a DHCP server available to provide IP address, to the device, it necessary to assign a static IP address to the wireless interface. Selecting **Network Settings** will allow configuration of the device with a static IP address. This is covered in section 19.0.

CONFIGURING NETWORK SETTINGS

Once the device is authenticated to a wireless network, communication is possible. However, before TCP/IP connectivity can be achieved, the device must obtain a valid IP address on the WLAN and/or Ethernet interface.

The Airborne device supports both DHCP and Static IP addressing for both the WLAN and Ethernet interfaces. The following sections cover the correct configuration for both DHCP and Static IP addressing on the interfaces.

When the Ethernet interface is in client mode, DHCP can be used on either the WLAN or Ethernet interface but, not on both interfaces at the same time.

The Ethernet interface configuration only applies when the interface is in client mode and is being used by a serial device server. The configuration of the Ethernet interface,e when being used with the Ethernet adapter (ABDx-ER) products, is covered in section 21.0.

The Ethernet configuration sections do not apply to devices that do not have an available Ethernet port; these include but are not limited to the ABDx-SE-DP5xx product families.

CONFIGURING DHCP ON WLAN INTERFACE

DHCP enabled on the WLAN interface is the default configuration for the Ethernet devices. For serial devices the default is DHCP disabled on the WLAN interface. It requires that there is a DHCP server on the WLAN network that the device has authenticated to and that the necessary network policies will allow the server to lease an address to the Airborne™ device.

Table 27 - Configuring DHCP - WLAN

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **WLAN DHCP**	Select **Enabled** from the dropdown menu.
Optional Select **WLAN DHCP Name**	Provides a method of uniquely identifying the device in the DHCP lease table on the DHCP server. The default name is **AirborneXXXXXX**, where **XXXXXX** matches the last 6 octets of the WLAN interface MAC address.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated, the network should lease an IP address to the WLAN interface and IP connectivity is possible over the WLAN network.

CONFIGURING DHCP ON ETHERNET INTERFACE

DHCP, enabled on the Ethernet interface, is the default configuration for the serial devices. The Ethernet interface must be in client mode for this setting to be used.

The Airborne Device does not support the ability to enable DHCP on the WLAN and Ethernet interfaces simultaneously (when in client mode). Only one may have DHCP enabled at a time. The other interface must be configured to use a static IP address.

Table 28 - Configuring DHCP – Ethernet

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Ethernet Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is covered in this page.
Select **Ethernet Role**	Select **Client** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Ethernet Settings** page.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **Ethernet DHCP**	Select **Enabled** from the drop down menu.
Optional Select **WLAN DHCP Name**	Provides a method of uniquely identifying the device in the DHCP lease table on the DHCP server. The default name is **AirborneXXXXXX**, where **XXXXXX** matches the last 6 hexadecimal digits of the Ethernet interface MAC address.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated, the network should lease an IP address to the WLAN interface and IP connectivity is possible over the WLAN network.

CONFIGURING A STATIC IP ADDRESS ON WLAN INTERFACE

Static IP addresses on the WLAN interface is the default configuration for serial devices. It is important to verify that the address being entered is unique to the device when on the network.

Table 29 - Configuring Static IP – WLAN

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **WLAN DHCP**	Select **Disable** from the drop down menu.
Select **WLAN Static IP Address**	Enter the assigned static IP address. The address must be in the format: **XXX.XXX.XXX.XXX**
Select **Subnet Mask**	Enter the subnet mask for the network. The mask must be in the format: **XXX.XXX.XXX.XXX**
Select **Gateway IP Address**	Enter the assigned Gateway IP address. The address must be in the format: **XXX.XXX.XXX.XXX**
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device is rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated, the network will use the assigned static IP address on the WLAN interface making IP connectivity possible over the WLAN network.

CONFIGURING A STATIC IP ADDRESS ON ETHERNET INTERFACE

This is not the default configuration for the Ethernet interface. It is important to verify that the address being entered is unique to the device when on the network.

The Airborne Device does not support the ability to enable DHCP on the WLAN and Ethernet interfaces simultaneously (when in client mode). Only one may have DHCP enabled at a time. The other interface must be configured to use a static IP address.

Table 30 - Configuring Static IP – Ethernet

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Ethernet Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields, setting the mode of operation for the Ethernet interface is done in this page.
Select **Ethernet Role**	Select **Client** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Ethernet Settings** page.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **Ethernet DHCP**	Select **Disable** from the drop down menu.
Select **Ethernet Static IP Address**	Enter the assigned static IP address. The address must be in the format: **XXX.XXX.XXX.XXX**
Select **Ethernet Subnet Mask**	Enter the subnet mask for the network. The mask must be in the format: **XXX.XXX.XXX.XXX**
Select **Ethernet Gateway IP Address**	Enter the assigned Gateway IP address. The address must be in the format: **XXX.XXX.XXX.XXX**
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device is rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated, the network will use the assigned static IP address on the Ethernet interface making IP connectivity possible over the Ethernet network.

CONFIGURING SERIAL DEVICE SERVER

ABDx-SE-DP5xx/IN5xxx devices are shipped preconfigured for use as Serial Device Servers. All that is required is configuration of the WLAN parameters and security protocols. However, the following section covers the full configuration of a Serial Device Server to aid in installation and deployment of the units.

If the Windows Virtual COM port driver is being used with the device, configure only the WLAN network parameters and security protocols through the web interface. All other parameters will be controlled by the VCOM driver. Installation and configuration of the VCOM driver is covered in section 21.0.

The following section shows how to manually configure the unit to accept TCP/IP connections and automatically set-up a data tunnel with one of the serial ports. The configuration is independent of the source of the request, as the tunnel ports are available to both the WLAN and Ethernet interfaces.

The Airborne devices support conditional tunnel binding based on rules included in the configuration. The major options will be included.

CONFIGURING SERIAL PORT FOR ACCESS ON TELNET PORT

A data tunnel can be made using the device's telnet port as the network connection port. This does require authenticating with the device and manually initiating the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 31 – Configure Data Tunnel on Telnet Port

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Connection Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **Telnet Port**	Enter the port number that you want to use for a telnet (TCP/IP) connection to the device. The default **23** should only be changed if your application requires access to port 23 for another purpose.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Connection Settings** page.
Feature Link Select **Serial Port 1 Settings/Serial Port 2 Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration. Setting the default mode of operation for the serial interface is done in this page.
Select **Serial CLI Default Mode**	Select **Listen** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Serial Port X Settings** page. Select this if you have further configuration options to change.

Step	Description
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated, the network it is possible for a TCP/IP connection to be made on the Telnet port.

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface, follow the steps in Table 32.

Table 32 - Data Tunnel using Telnet Port

Step	Description
Open TCP socket to device	Using the WLAN IP Address and configured telnet port number.
Authenticate with device	`auth dpac dpac` Any user level above L5 can authenticate with the unit. Device responds `OK`
Open data tunnel to serial port	`pass-x` Where `x` can be `p1`, `p2` or `any`. `p1` or `p2` binds to the indicated serial port, as long as the serial port is in listen mode and does not already have a data tunnel open. `any` binds to the first serial port which is in listen mode and does not already have a data tunnel open.

CONFIGURING SERIAL PORT 1 FOR ACCESS ON TUNNEL PORT

A data tunnel can be made using the device's tunnel port as the network connection port. This does not require authenticating with the device and automatically initiates the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 33 – Configure Data Tunnel on Serial Port 1 Tunnel Port (TCP)

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Connection Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **Tunnel Enabled**	Select **Enabled**.
Select **Tunnel Port**	Enter the port to be used for the tunnel. Default is **8023**. This should only be changed if a port is already defined for the application server or it is already being used by another service.
Select **Tunnel Mode**	Select **TCP** from drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Connection Settings** page.
Feature Link Select **Serial Port Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration. Setting the default mode of operation for the serial interface is done in this page.
Select **Serial CLI Default Mode**	Select **Listen** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Serial Port Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated to the network, it is possible for a TCP/IP connection to be made on the Telnet port.

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface, follow the steps in Table 34.

Table 34 - Data Tunnel using Tunnel Port on Serial Port 1

Step	Description
Open TCP socket to device	Using the WLAN IP Address and configured tunnel port number for Serial Port 1 (Default 8023).

CONFIGURING SERIAL PORT 2 FOR ACCESS ON TUNNEL PORT

A data tunnel can be made using the device's tunnel port as the network connection port. This does not require authenticating with the device and automatically initiates the tunnel connection. Configuring the device to support this approach to establishing a data tunnel is covered in the following table.

Table 35 – Configure Data Tunnel on Serial Port 2 Tunnel Port (TCP)

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Connection Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **Tunnel Enabled – Serial Port 2**	Select **Enabled**.
Select **Tunnel Port – Serial Port 2**	Enter the port to be used for the tunnel. Default is **8024**. This should only be changed if a port is already defined for the application server or it is already being used by another service.
Select **Tunnel Mode – Serial Port 2**	Select **TCP** from drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Connection Settings** page.
Feature Link Select **Serial Port 2 Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration. Setting the default mode of operation for the serial interface is done in this page.
Select **Serial CLI Default Mode**	Select **Listen** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Serial Port 2 Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated to the network, it is possible for a TCP/IP connection to be made on the Telnet port.

To establish a data tunnel and gain access to the serial data from the WLAN or Ethernet interface, follow the steps in Table 36.

Table 36 - Data Tunnel using Tunnel Port on Serial Port 2

Step	Description
Open TCP socket to device	Using the WLAN IP Address and configured tunnel port number for Serial Port 2 (Default 8024).

CONFIGURING SERIAL PORT 1 AS TCP CLIENT

In this mode, the device will attempt to initiate a TCP connection to a network-based server and establish a data tunnel with Serial Port 1 on a successful network connection.

Table 37 - Configure Serial Port 1 as TCP Client

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Connection Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **TCP Port**	Enter the port on which the target server is listening for TCP connections.
Select **TCP Timeout**	Enter the inactivity timeout in seconds, after which the device will close the open data tunnel on Serial Port 1. The default **0** disables the timeout.
Select **TCP Retry Time**	Enter the period (in seconds) the device should use to retry establishing the TCP connection to the target server.
Select **Primary TCP Target Server IP Address**	Enter the IP address of the primary target server. The address must be in the format: **XXX.XXX.XXX.XXX**
Optional Select **Secondary TCP Target Server IP Address**	Enter the IP address of the secondary target server. The address must be in the format: **XXX.XXX.XXX.XXX** This address will be used if the initial attempts to connect to the primary server fail. This field is optional.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Connection Settings** page.
Feature Link Select **Serial Port 1 Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration. Setting the default mode of operation for the serial interface is done in this page.
Select **Serial CLI Default Mode**	Select **Pass** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Serial Port 1 Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated to the network, the device will attempt to make a TCP connection with primary target server, using the configured port number.

CONFIGURING SERIAL PORT 2 AS TCP CLIENT

In this mode the device will attempt to initiate a TCP connection to a network based server and establish a data tunnel with Serial Port 2 on a successful network connection.

Table 38 - Configure Serial Port 2 as TCP Client

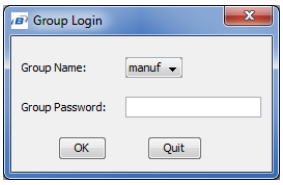
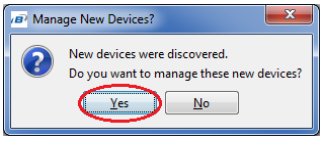
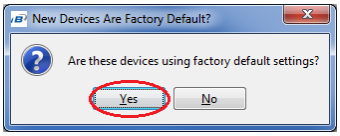
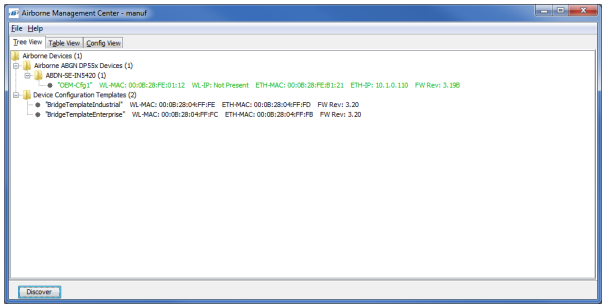
Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Connection Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **TCP Port – Serial Port 2**	Enter the port on which the target server is listening for TCP connections.
Select **TCP Timeout – Serial Port 2**	Enter the inactivity timeout in seconds, after which the device will close the open data tunnel on Serial Port 1. The default **0** disables the timeout.
Select **TCP Retry Time – Serial Port 2**	Enter the period (in seconds) the device should use to retry establishing the TCP connection to the target server.
Select **Primary TCP Target Server IP Address – Serial Port 2**	Enter the IP address of the primary target server. The address must be in the format: **XXX.XXX.XXX.XXX**
Optional Select **Secondary TCP Target Server IP Address – Serial Port 2**	Enter the IP address of the secondary target server. The address must be in the format: **XXX.XXX.XXX.XXX** This address will be used if the initial attempts to connect to the primary server fail. This field is optional.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Connection Settings** page.
Feature Link Select **Serial Port 2 Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. Displays a page showing the serial port configuration, setting the default mode of operation for the serial interface is done in this page.
Select **Serial CLI Default Mode**	Select **Pass** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Serial Port 2 Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Once authenticated to the network, the device will attempt to make a TCP connection with the primary target server using the configured port number.

INSTALLING AND USING THE AIRBORNE VIRTUALCOM DRIVER

B+B SmartWorx includes a virtual COM port device driver for the Microsoft Windows operating system with its serial devices. This driver acts as a Virtual COM port for applications requiring the use of a COM port for data communication. The driver redirects serial data to a TCP/IP connection between the host computer and target Airborne™ device.

Installation of the VCOM driver is done using the Airborne Management Center™ (AMC). The following table identifies the steps to install the VCOM driver for a specific device. Once installed, the host system will have additional COM ports by which the system may communicate with the device attached to the serial port on the Airborne™ device.

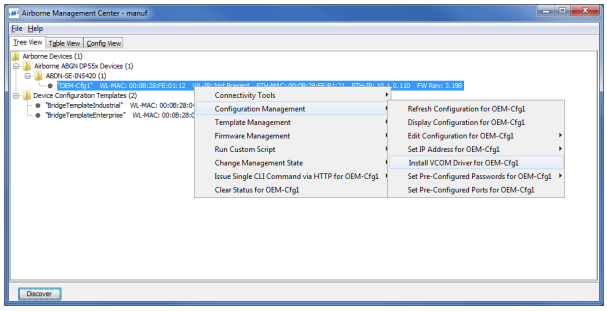
Table 39 - Install VCOM

1	Run the Airborne Management System application. This was installed during the CD installation and a menu item will be found in the Airborne folder located in the programs directory of your system. When the application opens the following dialog will be displayed:  Select Group Name: **manuf** and enter Group Password: **dpac**
2	The AMC will load and discover the attached devices. Manage your device.  
3	Managed devices will show up under the device type heading that they belong to. To install a VCOM driver, the device MUST have a serial port. 

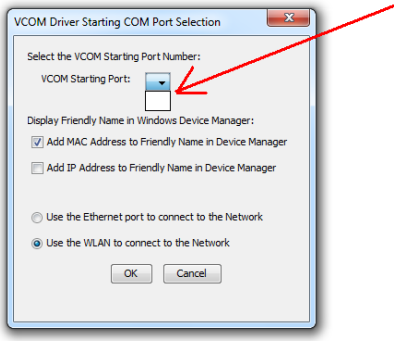
4

The status of the device will move to managed and it will be displayed under the device type/group it belongs too. To install the VCOM driver, right-click the target device:

1. Select **Configuration Management**
2. Select **Install VCOM Driver for OEM-Cfg1**

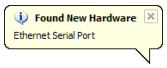


Note: if the port selection box does not have any ports listed, cancel the install, close AMC, then restart AMC by right-clicking the icon and clicking “Run as administrator”.



5

The VCOM driver will then be installed. When completed, the following message will be seen in the lower right-hand corner.



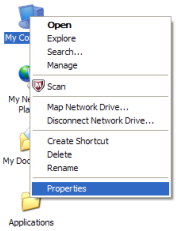
6

The installed VCOM ports are now available for use.

7

To identify the VCOM ports, right-click **My Computer**.

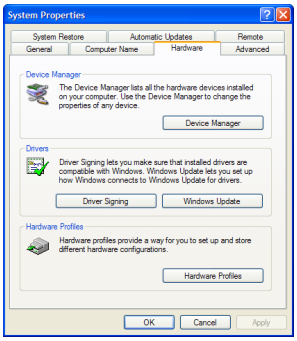
Select **Properties**.



8

Select the **Hardware** tab.

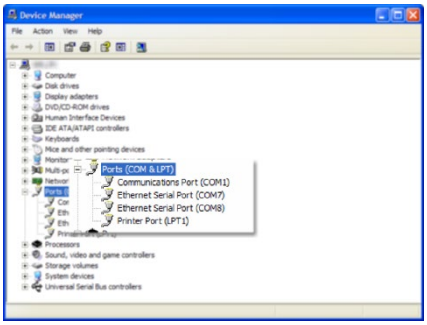
Select the **Device Manager** button.



9

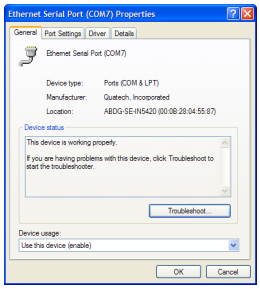
Select the **Ports (COM & LPT)** group; the list of available COM ports will be shown. The VCOM ports will be identified as **Ethernet Serial Port (COMx)**, where **x** will be an integer. This **COMx** reference identifies the VCOM to be used.

Note that, if your unit is a dual serial port device, two VCOM ports will have been created.



10

To identify which VCOM port is assigned to which device, right-click the **Ethernet Serial Port** and select **Properties**.



The **Location** label identifies the MAC address of the associated Airborne device.

Do not change the WLAN IP address settings for the Airborne device which is using the VCOM driver. Changing the IP address of the device will cause the VCOM driver not to function. It will need to be reinstalled if this occurs.

REPLACING A SERIAL CABLE

The serial device servers can be configured to act as a cable replacement using either an AdHoc or infrastructure network. In this application, you will need two (2) B+B SmartWorx Serial Device Servers. Once configured, the two devices will automatically connect and make a virtual serial connection between the two serial ports across the 802.11 network.

To establish the cable replacement, one device will be the Master and one the Slave. It does not matter which end of the serial connection is which. The master initiates the network connection and the slave waits for the master to connect. The following Table 40 and Table41 identify the required configurations for the master and slave. The configuration is for a single serial port; the same configuration can be used with those devices that support two serial connections.

The configurations in Table 40 and Table 41 use an AdHoc network. An infrastructure network can be used as long as static IP configuration is used for the slave device.

Table 40 - Cable Replacement - Slave Configuration

Step	Description
Configure the device to use an AdHoc network	See section 17.2 After the **Commit** at the end of the configuration, press the **Reload** Button.
Configure the device to use a static IP address on the WLAN interface	See section 19.3 After the **Commit** at the end of the configuration, press the **Reload** Button.
Configure the device to listen for a connection on the tunnel port	See section 20.2 After the **Commit** at the end of the configuration, press the **Reload** Button.
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of Interface and Network Parameters.
Feature Link Select **Serial Port Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the configuration options for TCP/IP and UDP connections to the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **Serial Port Bit Rate**	Select the appropriate bit rate to match the serial port that the device will be connected to.
Select **Parity**	Select the parity setting to match the serial port that the device will be connected to from the drop down list.
Select **Data Bits**	Select the number of data bits to match the serial port that the device will be connected to from the drop down list.
Select **Stop Bits**	Select the number of stop bits to match the serial port that the device will be connected to from the drop down list.
Select **Flow Control**	Select the flow control option to match the serial port that the device will be connected to from the drop down list.
Optional Select **Serial Assert**	Select the option to match the serial port that the device will be connected to from the drop down list. This is only required if software flow control has been selected.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **WLAN Settings** page.
Optional Press **Reload** [Button]	Reloads the **Serial Port Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will create an AdHoc network with the name you gave the SSID. As long as the network is in range, the wireless interface will connect.

Table 41 - Cable Replacement - Master Configuration

Step	Description
Configure the device to use an AdHoc network	See section 17.2 After the **Commit** at the end of the configuration, press the **Reload** Button.
Configure the device to use a static IP address on the WLAN interface	See section 19.3 After the **Commit** at the end of the configuration, press the **Reload** Button.
Configure the device to listen for a connection on the tunnel port	See section 20.2 After the **Commit** at the end of the configuration, press the **Reload** Button.
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of Interface and Network Parameters.
Feature Link Select **Serial Port Settings**	The serial port must be configured to work with the target device. This is a page showing the configuration options for the serial port.
Select **Serial Port Bit Rate**	Select the appropriate bit rate to match the serial port that the device will be connected to.
Select **Parity**	Select the parity setting to match the serial port that the device will be connected to from the drop down list.
Select **Data Bits**	Select the number of data bits to match the serial port that the device will be connected to from the drop down list.
Select **Stop Bits**	Select the number of stop bits to match the serial port that the device will be connected to from the drop down list.
Select **Flow Control**	Select the flow control option to match the serial port that the device will be connected to from the drop down list.
Optional Select **Serial Assert**	Select the option to match the serial port that the device will be connected to from the drop down list. This is only required if software flow control has been selected.
Select **Serial CLI Default Mode**	Select **Pass** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **WLAN Settings** page.
Feature Link Select **Connection Settings**	The target device configuration must be configured to make sure that the master device connects to the correct slave. A page showing the configuration options for TCP/IP and UDP connections to and from the device. Configuration of Telnet, HTTP and SSH ports is possible through this page.
Select **TCP Port**	This is the target port for the TCP connection on the slave device. This should be set to the listen port assigned during the configuration of the slave. The default for the listen port is **8023**.
Select **TCP Timeout**	This parameter allows the device to close the TCP socket to the slave should the connection be lost. The default of **0** disables the timeout. The timeout setting should be based on the period of time that a connection would not be used. It should at least exceed the worst case of the data period.
Select **Primary TCP Target Server IP Address**	Enter the static IP address that was given to the slave device during configuration.
Select **Outbound Transmit Type**	This is the outbound transmission protocol. Set this to **TCP** from the drop down list.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **WLAN Settings** page.
Optional Press **Reload** [Button]	Reloads the **Serial Port Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will create an AdHoc network with the name you gave the SSID. As long as the network is in range, the wireless interface will connect.

CONFIGURING ETHERNET ADAPTER

ABDx-ER-DP5xx/IN5xxx devices are shipped preconfigured for use as an Ethernet adapter. All that is required is to configure the WLAN parameters and security protocols. However, the following section will cover the full configuration of an Ethernet Device to aid installation and deployment of the units.

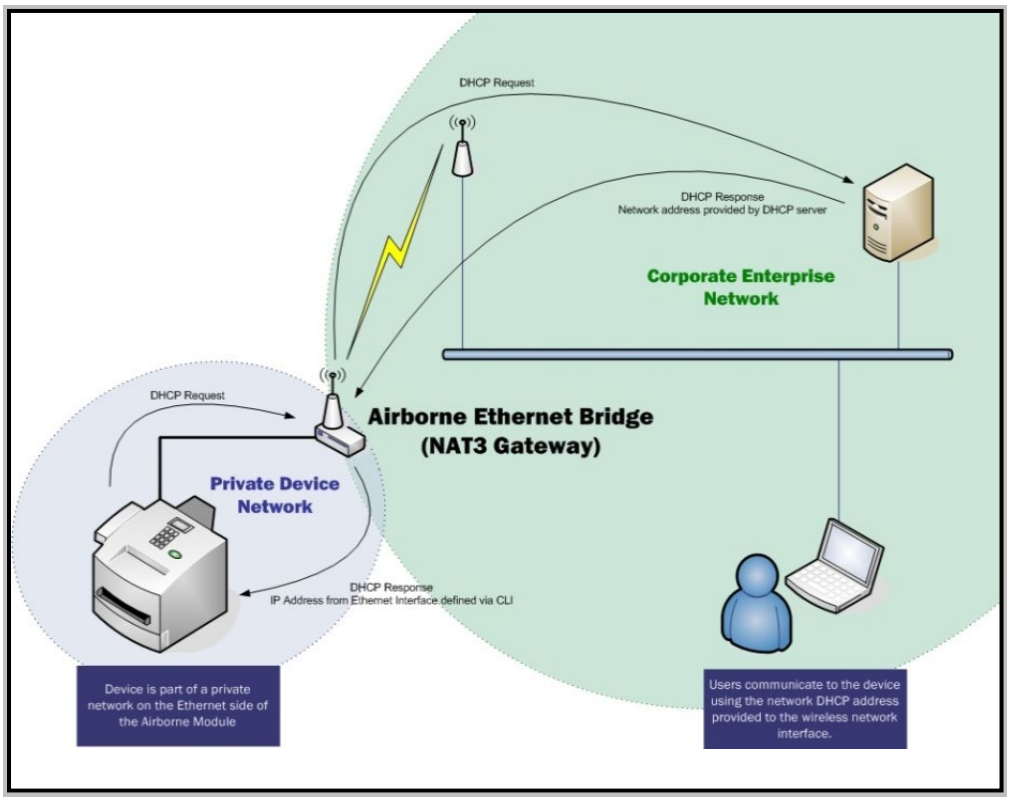
The Airborne Ethernet Adapter (-ER-) is a fully functional NAT Level 3 router, supporting a public IP address for the WLAN interface and a private network for the attached devices on the Ethernet interface. When configured as a Bridge Adapter, it disables routing and bridges all packets between the Ethernet and wireless interfaces.

ROUTER FUNCTIONALITY

Network Address Translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. In the case of a NAT Level 3 device, the modification of the packet headers provides for a translation between a single public IP address (that of the WLAN interface) and the IP address of the devices on the private network (Ethernet interface).

The Airborne Adapter WLAN interface is considered the public address and will be the point of contact on the target network (see Figure 19). This interface supports all the wireless and network authentication requirements including support for WPA2-Enterpise. It can acquire an IP address through both DHCP or user configured static IP. Configuration, association and authentication are handled entirely by the Airborne Bridge and require no interaction from the wired host on the private network.

Figure 19 - Ethernet Bridge Functionality



The private network is the wired interface provided by the bridge. This interface includes a DHCP server and supports dynamic and static IP address assignment. This means any Ethernet client supporting DHCP can be connected to the wired interface without any configuration changes. The private network host can communicate with the Airborne Adapter using the bridge's Ethernet IP address on the private network.

The Airborne Ethernet Adapter supports NAT Level 3 and, as such, provides the following advantages over the more traditional bridge functionality:

- A single network IP address on the public network. This simplifies management of the devices on the network.
- A single point of authentication. The Airborne device handles authentication for the public network. This means a single point of contact for all security interaction, simplifying deployment for the network.
- Zero security footprint on the private network host.
- Support for DHCP and static IP on the private network. This capability allows the host to be shipped without any configuration changes.
- Port forwarding. Allows you to decide if web page, telnet or FTP access should be forwarded to the private network or handled by the Airborne Bridge.
- Plug-n-Play. In most cases, all that is required for full functionality is configuration of the wireless interface for the target network. This can be done before deployment to minimize deployment time and complexity.

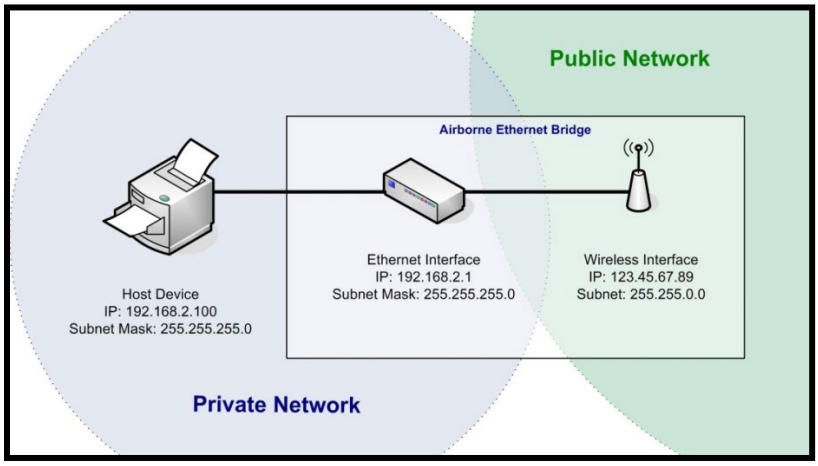
PUBLIC NETWORK INTERFACE

The public network interface is the Airborne Adapter WLAN port. This interface must be configured to associate and authenticate with the target network. Configuration of this interface is covered in section 17.0.

The public address becomes the target address for all accesses to the host device connected to the private network. In the example shown in Figure 20, any device on the public network wanting to communicate with the Host device (IP: 192.168.2.100), would use the IP address 123.45.67.89, the Airborne Ethernet Adapter will forward all traffic to the private address 192.168.2.100.

The network infrastructure will show the MAC and IP address of the Airborne Adapter WLAN interface as the network presence, as a consequence of this all traffic will be identified as being from or to this address.

Figure 20 - Airborne Ethernet Bridge IP Configuration



The public network interface supports the Airborne™ discovery protocol and will respond to discovery requests issued on the public network.

PRIVATE NETWORK INTERFACE

The private network interface is on the Ethernet port of the Airborne Adapter. The interface supports multiple Ethernet clients with either a static or DHCP sourced IP addresses. The configuration of this interface is covered in Table 42 and Table 43.

Table 42 - Ethernet Adapter interface Configuration – DHCP

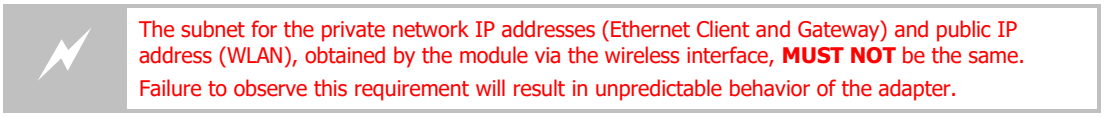
Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Ethernet Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields. Aetting the mode of operation for the Ethernet interface is done in this page.
Select **DHCP Server Enabled**	Select **Enable** from drop down menu.
Select **Ethernet Role**	Select **Router** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Ethernet Settings** page.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **Ethernet Static IP Address**	Enter a valid IP address. This address will be the first IP address leased. If more than one is leased, they will increment from this address. The subnet of the address must be different than the WLAN interface subnet. The address must be in the format: **XXX.XXX.XXX.XXX** This is also the default address all incoming traffic on the WLAN interface is routed to.
Select **Ethernet Subnet Mask**	Enter the subnet mask for the private network. The mask must be in the format: **XXX.XXX.XXX.XXX**
Select **Ethernet Gateway IP Address**	Enter a valid Gateway IP address. This is the Static IP address of the Ethernet interface on the private network. This must be in the same subnet as the **Ethernet Static IP Address**. The address must be in the format: **XXX.XXX.XXX.XXX**
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this if you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as reboote,d it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. The Ethernet interface will have leased IP addresses to the Ethernet clients and the Ethernet interface would have taken the **Ethernet Gateway IP Address**. Access to the public network from the private network is now possible.

Unless your public network is using the default 192.168.2.XX subnet, you should not change the Ethernet parameters.

Table 43 - Ethernet Adapter interface Configuration - Static IP

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Ethernet Settings**	The wireless interface and security must be configured before configuring the Ethernet settings. A page showing the range of Ethernet options and fields. Setting the mode of operation for the Ethernet interface is done in this page.
Select **DHCP Server Enabled**	Select **Disable** from drop down menu.
Select **Ethernet Role**	Select **Router** from the drop down menu.
Press **Commit** [Button]	Saves changes to the device.
Press **Reload** [Button]	Reloads the **Ethernet Settings** page.
Feature Link Select **Network Settings**	The wireless interface and security must be configured before configuring the network settings. A page showing the range of network options and fields, for both the WLAN and Ethernet interfaces, is displayed.
Select **Ethernet Static IP Address**	Enter the static IP address of the Ethernet client attached to the device's Ethernet port. The subnet of the address must be different than the WLAN interface subnet. The address must be in the format: **XXX.XXX.XXX.XXX** This is also the default address that all incoming traffic on the WLAN interface is routed to.
Select **Ethernet Subnet Mask**	Enter the subnet mask for the private network that matches the subnet mask on the Ethernet client. The mask must be in the format: **XXX.XXX.XXX.XXX**
Select **Ethernet Gateway IP Address**	Enter a valid Gateway IP address. This is the Static IP address of the Ethernet interface on the private network. This must be in the same subnet as the **Ethernet Static IP Address**, but a different address. The address must be in the format: **XXX.XXX.XXX.XXX** This address should be entered into the Gateway parameter for the Ethernet clients on the private network.
Press **Commit** [Button]	Saves changes to the device.
Optional Press **Reload** [Button]	Reloads the **Network Settings** page. Select this is you have further configuration options to change.
Optional Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured network. As long as the network is in range, the wireless interface will connect. Access to the public network from the private network is now possible.

The private network supports Airborne™ discovery protocol (UDAP) and will respond to discovery requests.



When attempting to make an out-bound connection to a device on the public network, the public network IP address of the device should be used. Figure 20, e.g.: the client with address 192.168.2.100, wants to connect to an FTP server with the address of 123.45.67.99, on the public network to perform a firmware download. The FTP address that would be used in the **Configuration/Advanced Settings** FTP Server Address or Name would be `123.45.67.99`. Note that this is not within the subnet of the Ethernet client. However, the NAT router will do the necessary address translations and packet header manipulations to ensure that out-bound and in-bound connections are maintained.

Any traffic between the Airborne Ethernet Adapter's Ethernet interface and Ethernet client on the private network will not be broadcast on the public network unless it is directed at the public network.

For most users, there will be no modification of the private network settings needed and, if the target Ethernet client uses DHCP to obtain an IP address, no change in configuration will be required.

BRIDGE FUNCTIONALITY

When the Adapter is a bridge, the Ethernet and 802.11 interfaces will be bridged together. All packets received on either interface will be forwarded to the other interface. Both interfaces reside on the same network, there are no Private and Public networks. The Ethernet IP configuration is used and the 802.11 IP configuration is ignored. The 802.11 interface will assume the IP address of the first Ethernet network client that has traffic sent across the bridge.

When acting as a bridge, the Adapter is still listening on the configured ports for remote access to the Adapter. If traffic to any of the configured ports (http, telnet, ftp, ssh, etc.) need to pass through the module, then the ports need to be reconfigured to use non-default settings.

Table 44 - Ethernet Adapter interface Configuration

Step	Description
Navigation Bar Select **Configuration**	You will see a group of fields under the banner of WLAN Parameters.
Feature Link Select **Express Setup**	A page showing the range of basic Wireless and Ethernet options and fields.
Select **Ethernet Role**	Select **Router** from the drop down menu.
Select **Ethernet Static IP Address**	Enter the static IP address for the Ethernet network. The IP address should be on the same subnet as the other network clients. The address must be in the format: XXX.XXX.XXX.XXX
Select **Ethernet Subnet Mask**	Enter the subnet mask for the private network that matches the subnet mask of the Ethernet client and network. The mask must be in the format: XXX.XXX.XXX.XXX
Optional Select **Web Server Port**	Enter a different value for this port if you want normal Web Server traffic that uses port 80 to pass through the adapter.
Optional Select **Telnet Port**	Enter a different value for this port if you want normal telnet traffic that uses port 23 to pass through the adapter.
Optional Select **Internal FTP Server Listen Port**	Enter a different value for this port if you want normal FTP traffic that uses port 21 to pass through the adapter.
Optional Select **Secure Shell Server (SSH) Port**	Enter a different value for this port if you want normal SSH traffic that uses port 22 to pass through the adapter.
Press **Commit** [Button]	Saves changes to the device.
Press **Restart** [Button]	Restarts the device. After the device as rebooted, it will attempt to authenticate to the configured wireless network. As long as the network is in range, the wireless interface will connect.

MAC CLONING

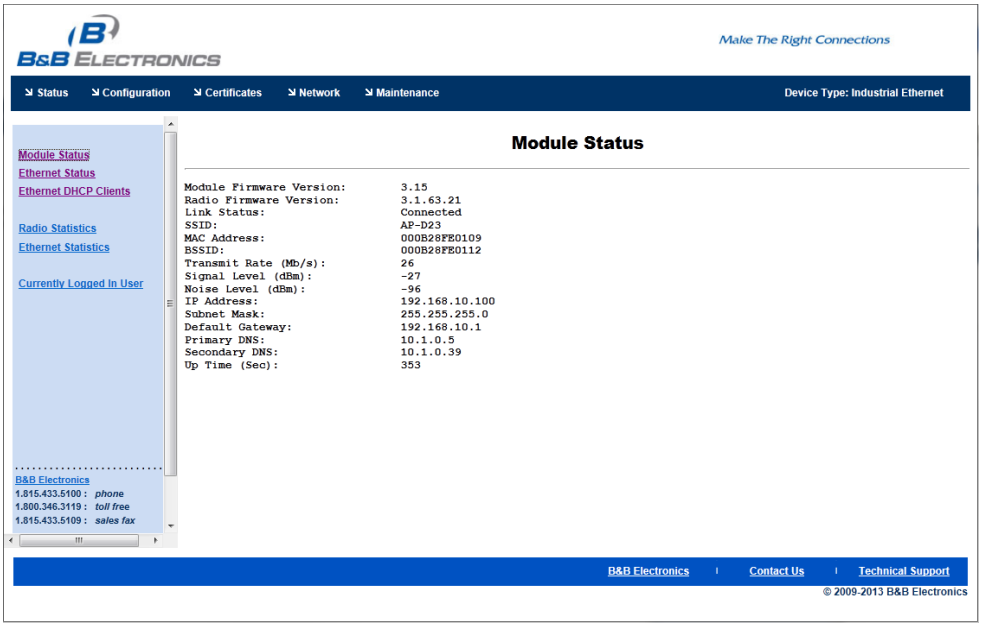
If the network is configured to not allow multiple MAC address for the same IP address, MAC address cloning should be enabled. MAC address cloning will cause the WLAN module to adopt the MAC address of the first Ethernet client that it sees traffic from. If the Ethernet client uses DHCP, the module will sniff the DHCP transactions and learn the MAC and IP that the client will use, and adopts them as its own. When in bridge-mode, this makes the module look like a “cable replacement” and should be transparent to the network.

WEB PAGE OVERVIEW

The following section highlights the contents of each web page and provides a reference to the associated CLI command. For further explanation of each of the fields, please refer to the referenced command in the table (see also Airborne Enterprise Command Line Reference Manual). When using a CLI command, typing a command followed by a space and a '?' will display help for the command (e.g. "wl-type ?").

MODULE STATUS

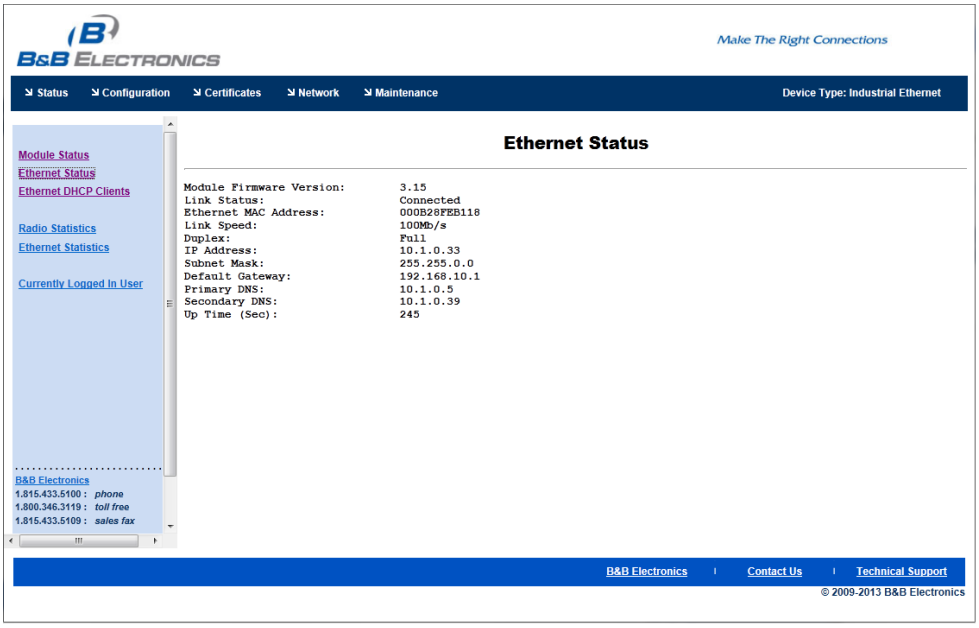
URL	/Status/Module Status
Description	The home page when authenticated to the Airborne device; this page provides important information about the device's firmware version, wireless connection status and wireless interface network configuration.



Field	CLI Command
Displayed Page	`wl-info`

ETHERNET STATUS

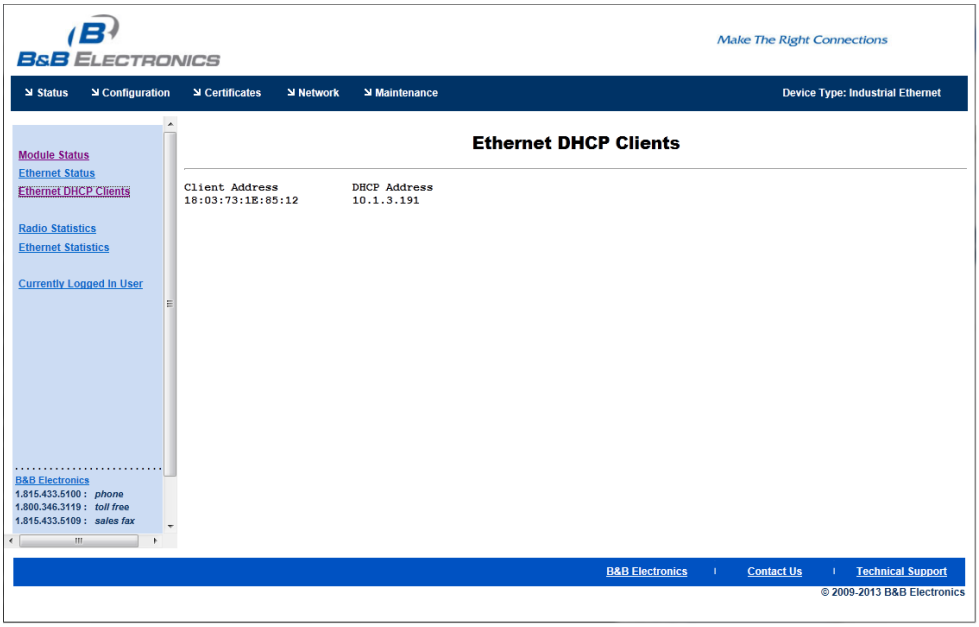
URL	/Status/Ethernet Status
Description	Provides important information about the device's firmware version, Ethernet connection status and Ethernet interface network configuration.



Field	CLI Command
Displayed Page	`eth-info`

ETHERNET DHCP CLIENTS

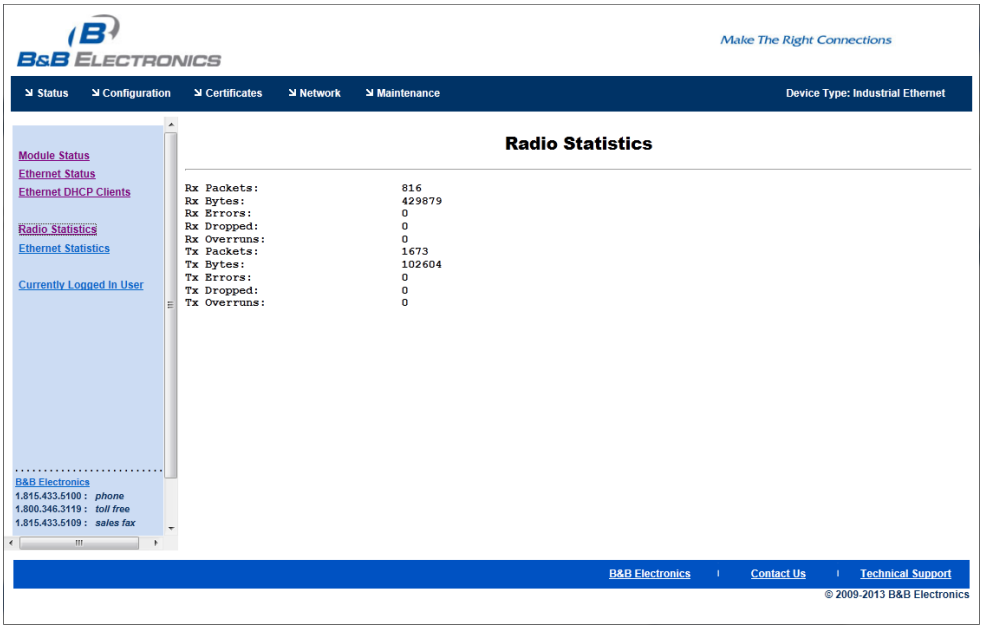
URL	/Status/Ethernet DHCP Clients
Description	Displays the IP address issued by the DHCP server to specific MAC addresses.



Field	CLI Command
Displayed Page	`eth-dhcp-clients`

RADIO STATISTICS

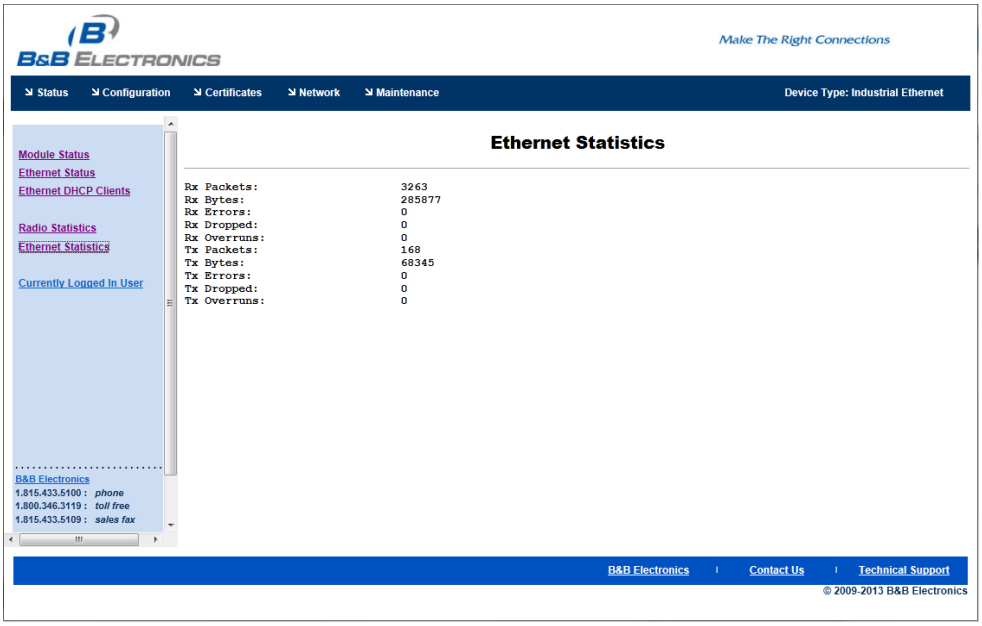
URL	/Status/Radio Statistics
Description	Provides information about the packet transmit and receive performance of the wireless interface.



Field	CLI Command
Displayed Page	`stats <blank> or radio`

ETHERNET STATISTICS

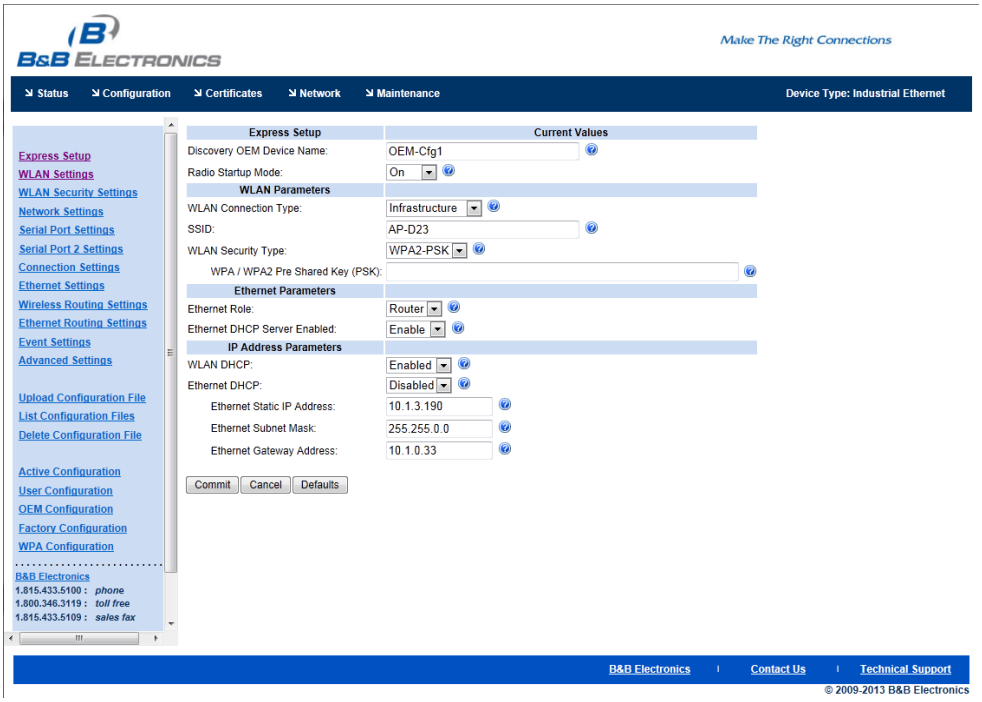
URL	/Status/Ethernet Statistics
Description	Provides information about the packet transmit and receive performance of the Ethernet interface.



Field	CLI Command
Displayed Page	`stats ethernet`

EXPRESS SETUP

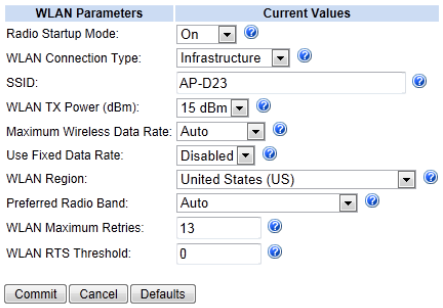
URL	/Configuration/Express Setup
Description	Provides a simplified configuration option set in a single page; this is the default home page when configuring the device for the first time or after a factory reset has been performed.



Field	CLI Command
Discovery OEM Device Name	`name-oem`
Radio Startup Mode	`radio-on, radio-off`
Wireless LAN Connection Type	`wl-type`
SSID	`wl-ssid`
Wireless LAN Security Type	`wl-security`
WEP Key 1	`wl-key-1`
WPA/WPA2Pre Shared Key (PSK)	`pw-wpa-psk`
LEAP User Name	`user-leap`
LEAP Password	`pw-leap`
PEAP Identity	`eap-ident`
PEAP Password	`eap-password`
Ethernet Role	`eth-role`
Ethernet DHCP Server	`eth-dhcp-server`
WLAN DHCP	`wl-dhcp`
Ethernet DHCP	`eth-dhcp`
WLAN Static IP Address	`wl-ip`
WLAN Subnet Mask	`wl-subnet`
Ethernet Static IP Address	`eth-ip`
Ethernet Subnet Mask	`eth-subnet`
Ethernet Gateway	`eth-gateway`

WLAN SETTINGS

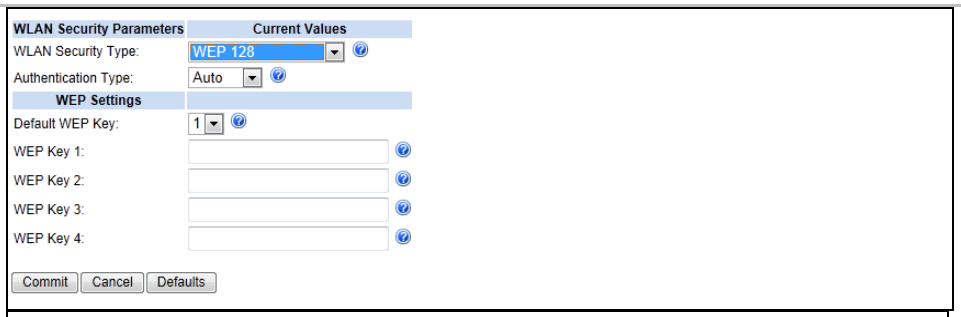
URL	/Configuration/WLAN Settings
Description	Configures the wireless interface settings including network name and type.

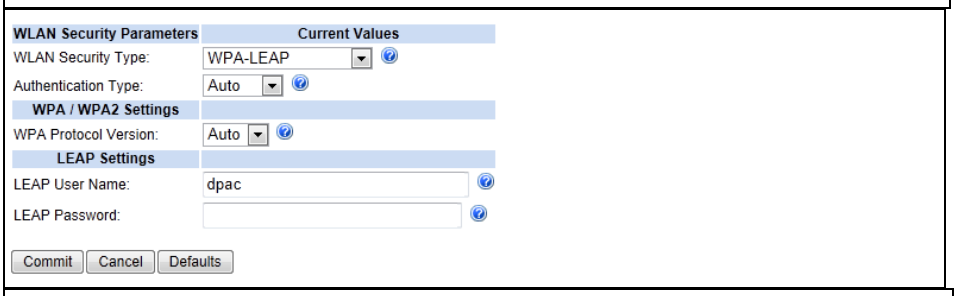


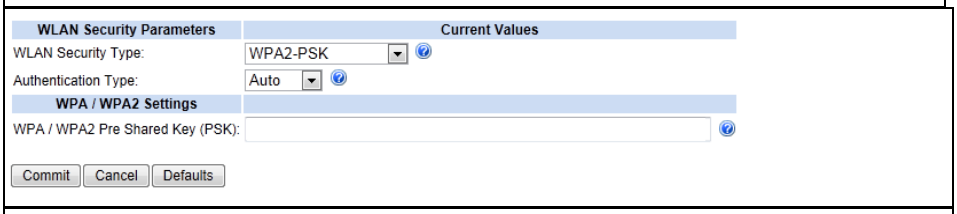
Field	CLI Command
Radio Startup Mode	`radio-on, radio-off`
Wireless LAN Connection Type	`wl-type`
SSID	`wl-ssid`
Wireless Transmit Power	`wl-tx-power`
Maximum Wireless Data Rate	`wl-rate`
Use Fixed Data Rate	`wl-fixed-rate`
Wireless LAN Region	`wl-region`
802.11 Band	`wl-band-pref`
Wireless Max Retries on TX	`wl-max-retries`
Wireless RTS Threshold	`wl-rts-threshold`

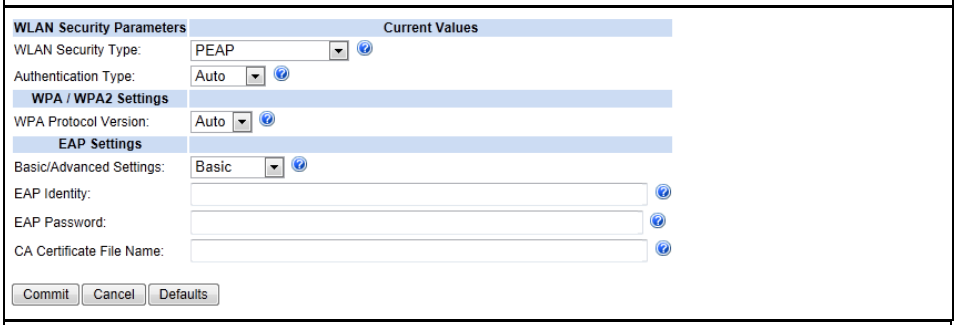
WLAN SECURITY SETTINGS

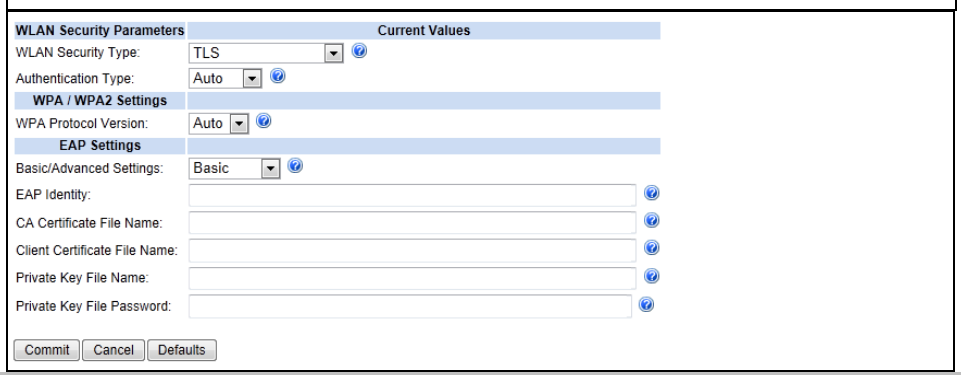
URL	/Configuration/WLAN Security Settings
Description	Configures the security settings for the target network.

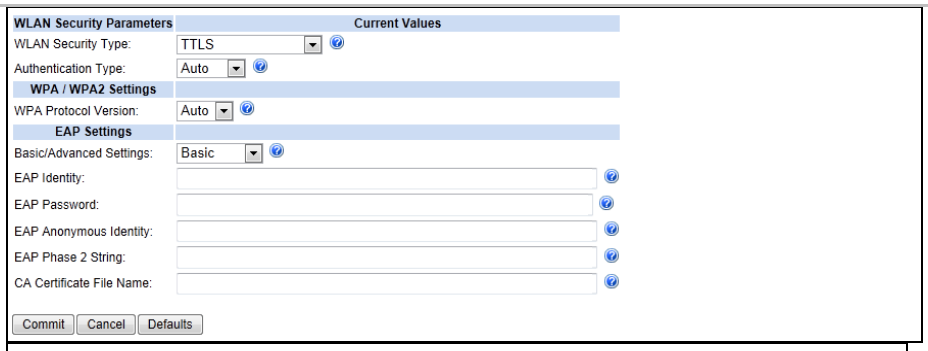


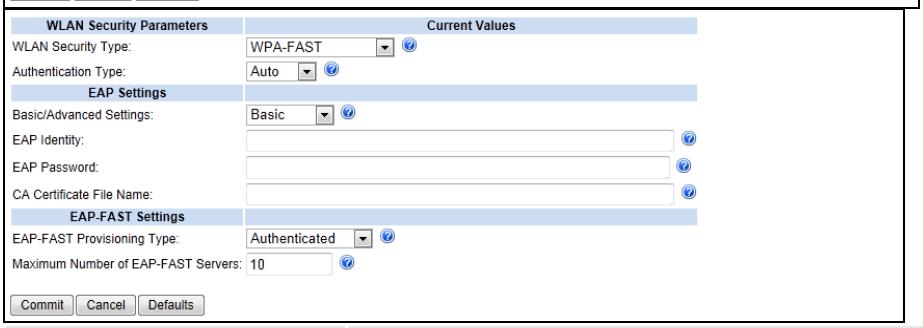








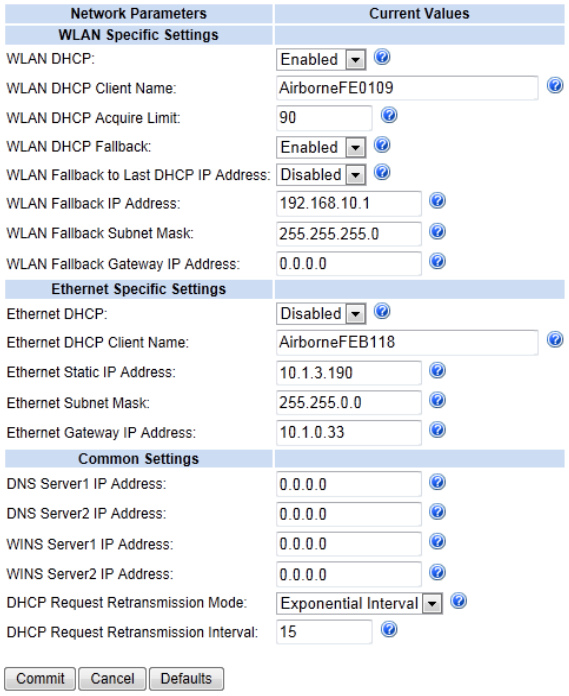




Field	CLI Command
Wireless LAN Security Type	`wl-security`
Authentication Type	`wl-auth`
Default WEP Key	`wl-def-key`
WEP Key 1 - 4	`wl-key-1, wl-key-2, wl-key-3, wl-key-4`
WPA Protocol Version	`wl-wpa-format`
LEAP User Name	`user-leap`
LEAP Password	`pw-leap`
WPA/WPA2 Pre Shared Key (PSK)	`pw-wpa-psk`
EAP Identity	`eap-ident`
EAP Password	`eap-password`
EAP Anonymous Identity	`eap-anon-ident`
EAP Phase String 1	`eap-phase1`
EAP Phase String 2	`eap-phase2`
EAP Subject Match String	`subject-match`
EAP Subject Match 2 String	`subject-match2`
EAP Alternate Subject Match String	`alt-subject-match`
EAP Alternate Subject Match 2 String	`alt-subject-match2`
CA Certificate File Name	`ca-cert-filename`
CA Certificate 2 File Name	`ca-cert2-filename`
Client Certificate File Name	`client-cert-filename`
Client Certificate 2 File Name	`client-cert2-filename`
Private Key File Name	`priv-key-filename`
Private Key File Password	`priv-key-password`
Private Key 2 File Name	`priv-key2-filename`
Private Key File 2 Password	`priv-key2-password`
DH Parameter File Name	`dh-parm-filename`
DH Parameter 2 File Name	`dh-parm2-filename`
EAP-FAST Provisioning Type	`eap-fast-provisioning`
Maximum Number of EAP-FAST Servers	`eap-fast-max-pac-list`

NETWORK SETTINGS

URL	/Configuration/Network Settings
Description	Configures wireless and Ethernet interface network settings including DHCP, static IP and fall back configurations.

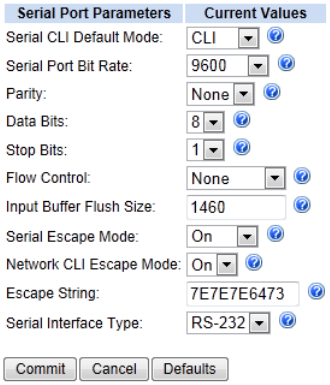


Field	CLI Command
WLAN DHCP	`wl-dhcp`
WLAN DHCP Client Name	`wl-dhcp-client`
WLAN Static IP Address	`wl-ip`
WLAN Subnet Mask	`wl-subnet`
WLAN Gateway IP Address	`wl-gateway`
WLAN DHCP Acquire Limit	`wl-dhcp-acqlimit`
WLAN DHCP Fallback	`wl-dhcp-fb`
WLAN Fallback to Last DHCP IP Address	`wl-dhcp-fbauto`
WLAN Fallback IP Address	`wl-dhcp-fbip`
WLAN Fallback Subnet Mask	`wl-dhcp-fbsubnet`
WLAN Fallback Gateway IP Address	`wl-dhcp-fbgateway`
Save Last WLAN DHCP IP Address as Fallback IP Addresses	`wl-dhcp-fbper`
Ethernet DHCP	`eth-dhcp`
Ethernet DHCP Client Name	`eth-dhcp-client`
Ethernet DHCP Acquire Limit	`eth-dhcp-acqlimit`
Ethernet Static IP Address	`eth-ip`

Ethernet Subnet Mask	`eth-subnet`
Ethernet Gateway IP Address	`eth-gateway`
Ethernet DHCP Fallback	`eth-dhcp-fb`
Ethernet Fallback to Last DHCP IP Address	`eth-dhcp-fbauto`
Ethernet Fallback IP Address	`eth-dhcp-fbip`
Ethernet Fallback Subnet Mask	`eth-dhcp-fbsubnet`
Ethernet Fallback Gateway IP Address	`eth-dhcp-fbgateway`
Save Last Ethernet DHCP IP Address as Fallback IP Addresses	`eth-dhcp-fbper`
DNS Server1/2 IP Address	`dns-server1, dns-server2`
WINS Server1/2 IP Address	`wins-server1, wins-server2`
WLAN DHCP Request Retransmission Mode	`wl-dhcp-mode`
WLAN DHCP Request Retransmission Interval	`wl-dhcp-interval`
Ethernet DHCP Request Retransmission Mode	`eth-dhcp-mode`
Ethernet DHCP Request Retransmission Interval	`eth-dhcp-interval`

SERIAL PORT SETTINGS

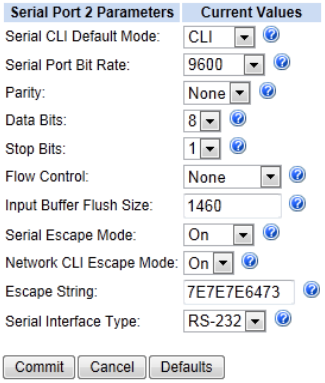
URL	/Configuration/Serial Port Settings
Description	Configures serial port settings on the primary serial port.



Field	CLI Command
Serial CLI Default Mode	`serial-default, serial-default-p1`
Serial Port Bit Rate	`bit-rate, parity-p1`
Parity	`parity, parity-p1`
Data Bits	`data-bits, data-bits-p1`
Stop Bits	`stop-bit, stop-bit-p1`
Flow Control	`flow, flow-p1`
Input Buffer Flush Size	`input-size, input-size-p1`
Serial Escape Mode	`esc-mode-serial, esc-mode-serial-p1`
Network CLI Escape Mode	`esc-mode-lan, esc-mode-lan-p1`
Escape String	`esc-str, esc-str-p1`
Serial Interface Type	`intf-type`

SERIAL PORT 2 SETTINGS

URL	/Configuration/Serial Port 2 Settings
Description	Configures serial port settings on the secondary serial port.

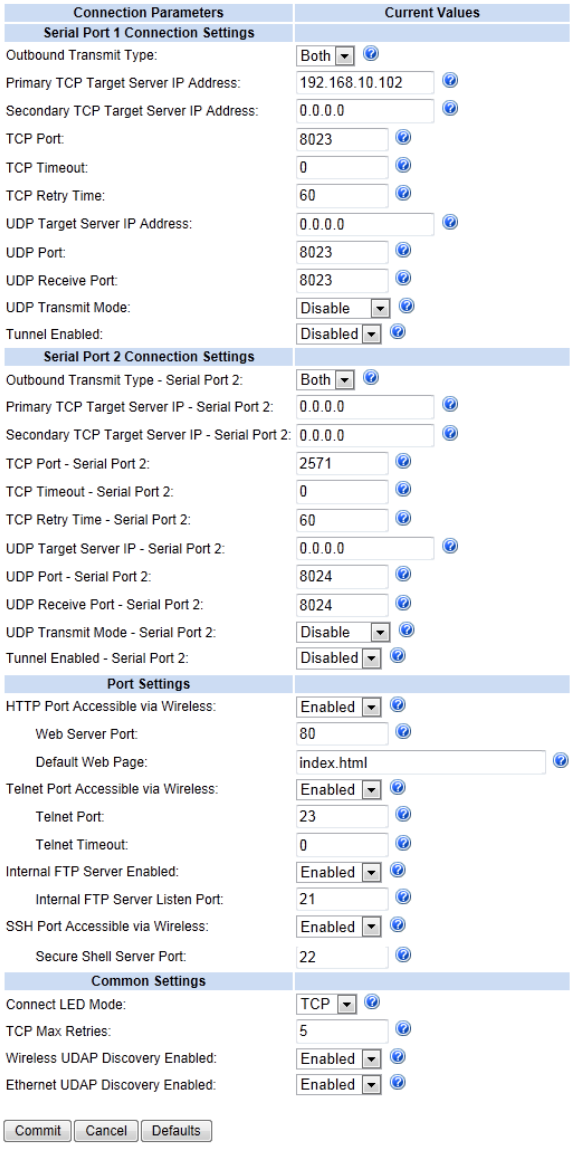


Field	CLI Command
Serial CLI Default Mode	`serial-default-p2`
Serial Port Bit Rate	`parity-p2`
Parity	`parity-p2`
Data Bits	`data-bits-p2`
Stop Bits	`stop-bit-p2`
Flow Control	`flow-p2`
Serial Assert	`serial-assert-p2`
Input Buffer Flush Size	`input-size-p2`
Serial Escape Mode	`esc-mode-serial-p2`
Network CLI Escape Mode	`esc-mode-lan-p2`
Escape String	`esc-str-p2`
Serial Interface Type	`intf-type`

Serial port 2 cannot run in RS-485 mode and will assume RS-422 mode even if it is set to RS-485 mode. Serial port 2 cannot run half-duplex and must have a 4-wire connection.

CONNECTION SETTINGS

URL	/Configuration/Connection Settings
Description	Configures the data tunnel and network port settings for both serial ports. Includes management of port access and service availability.

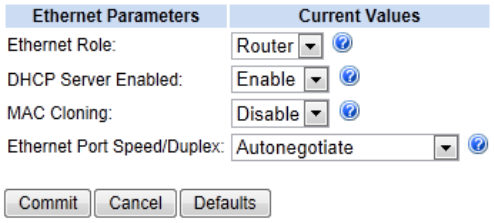


Field	CLI Command
Outbound Transmit Type	`wl-xmit-type, wl-xmit-type-p1`
Primary TCP Target Server IP Address	`wl-tcp-ip, wl-tcp-ip-p1`
Secondary TCP Target Server IP Address	`wl-tcp-ip2, wl-tcp-ip2-p1`
TCP Port	`wl-tcp-port, wl-tcp-port-p1`
TCP Timeout	`wl-tcp-timeout, wl-tcp-timeout-p1`

TCP Retry Time	wl-retry-time, wl-retry-time-p1
Tunnel Enabled	wl-tunnel, wl-tunnel-p1
Tunnel Port	wl-tunnel-port, wl-tunnel-port-p1
Tunnel Mode	wl-tunnel-mode, wl-tunnel-mode-p1
UDP Target Server IP Address	wl-udp-ip, wl-udp-ip-p1
UDP Port	wl-udp-port, wl-udp-port-p1
UDP Receive Port	wl-udp-rxport, wl-udp-rxport-p1
UDP Transmit Mode	wl-udp-xmit, wl-udp-xmit-p1
Outbound Transmit Type – Serial Port 2	wl-xmit-type-p2
Primary TCP Target Server IP Address – Serial Port 2	wl-tcp-ip-p2
Secondary TCP Target Server IP Address – Serial Port 2	wl-tcp-ip2-p2
TCP Port – Serial Port 2	wl-tcp-port-p2
TCP Timeout – Serial Port 2	wl-tcp-timeout-p2
TCP Retry Time – Serial Port 2	wl-retry-time-p2
UDP Target Server IP Address – Serial Port 2	wl-udp-ip-p2
UDP Port – Serial Port 2	wl-udp-port-p2
UDP Receive Port – Serial Port 2	wl-udp-rxport-p2
UDP Transmit Mode – Serial Port 2	wl-udp-xmit-p2
Tunnel Enabled – Serial Port 2	wl-tunnel-p2
Tunnel Port – Serial Port 2	wl-tunnel-port-p2
Tunnel Mode – Serial Port 2	wl-tunnel-mode-p2
HTTP Port Accessible via Wireless	http-port
Web Server Port	wl-http-port
Telnet Port Accessible via Wireless	telnet-port
Telnet Port	wl-telnet-port
Telnet Timeout	wl-telnet-timeout
Internal FTP Server Enabled	ftp-server
Internal FTP Server Listen Port	ftp-server-listen-port
SSH Port Accessible via Wireless	ssh-port
Secure Shell Server Port	wl-ssh-port
Connect LED Mode	wl-con-led
TCP Max Retries	tcp-retries
Wireless UDAP Discovery Enabled	wl-udap
Ethernet UDAP Discovery Enabled	eth-udap

ETHERNET SETTINGS

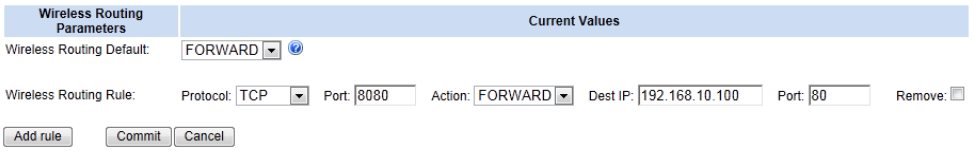
URL	/Configuration/Ethernet Settings
Description	Configures the Ethernet interface for AirborneM2M™ Ethernet devices.



Field	CLI Command
Ethernet Role	`eth-role`
DHCP Server Enabled	`eth-dhcp-server`
MAC Cloning	`wl-mac-clone`
Ethernet Port Speed/Duplex	`eth-mode`

WIRELESS ROUTING SETTINGS

URL	/Configuration/Wireless Routing Settings
Description	Configures the port forwarding routing rules for the wireless interface.



Field	CLI Command
Wireless Routing Default	`wl-route-default`
Add rule [Button]	`wl-route`

Additional details on using the wl-route command:

Usage: wl-route [tcp|udp|icmp|bcast|all] [port xxx] forward|drop|relay [xxx.xxx.xxx.xxx:xxx]

Sets up a specific rule for incoming wireless traffic.

The tcp|udp|icmp|bcast|all option selects the protocol for this rule.

The port option defines the port number for this rule. You cannot set the port option if the protocol is icmp or all.

The drop option will cause traffic matching the protocol and port specifications to be dropped. In this case, any parameters following the drop option will be ignored. The forward option will cause traffic to be forwarded to the Ethernet interface and requires another parameter to define the destination IP address and port. The other parameter is formatted as xxx.xxx.xxx.xxx:port.

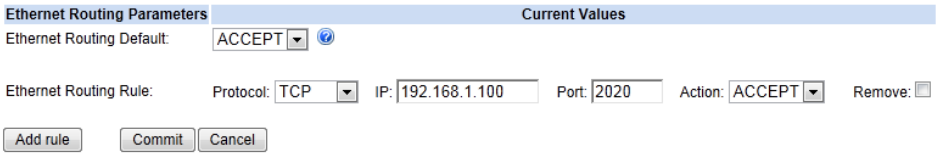
The relay option can only be used if the protocol is bcast and will cause UDP traffic with destination address 255.255.255.255 received on the specified port to be relayed to the Ethernet interface.

For example, the command wl-route tcp port 80 forward 192.168.2.101:8080 will cause all tcp port 80 traffic received on the wireless interface to be forwarded to IP address 192.168.2.101, port 8080 on the Ethernet interface.

wl-route with no parameters will display the current set of wireless routing rules in the order that they will be applied to incoming traffic.

ETHERNET ROUTING SETTINGS

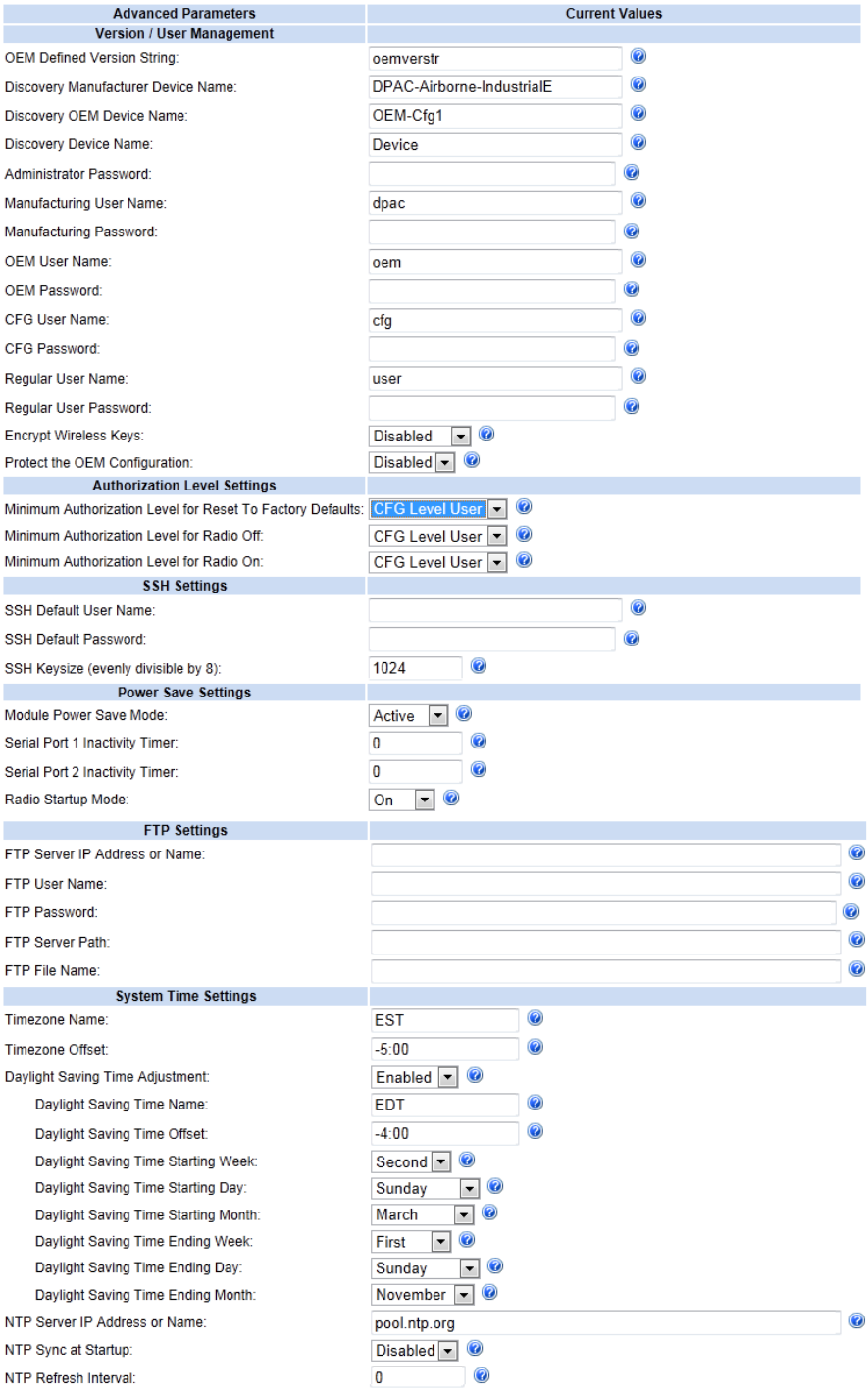
URL	/Configuration/Ethernet Routing Settings
Description	Configures the firewall routing rules for the Ethernet interface.



Field	CLI Command
Ethernet Routing Default	`eth-route-default`
Add rule [Button]	`eth-route`

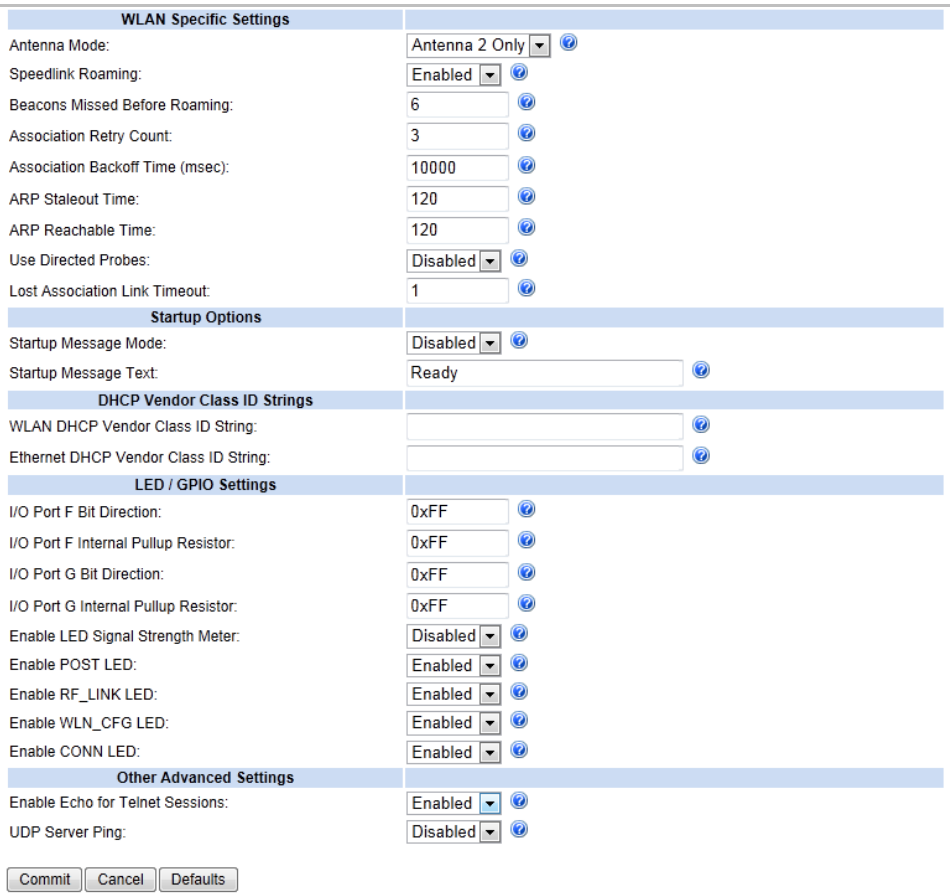
ADVANCED SETTINGS

URL	/Configuration/Advanced Settings
Description	Configures the advanced configuration settings for the unit, including authentication usernames and passwords, configuration of SSH, power save setup, GPIO, indicator LED and FTP settings.



Advanced Parameters	Current Values
Version / User Management	
OEM Defined Version String:	oemverstr
Discovery Manufacturer Device Name:	DPAC-Airborne-IndustrialE
Discovery OEM Device Name:	OEM-Cfg1
Discovery Device Name:	Device
Administrator Password:	
Manufacturing User Name:	dpac
Manufacturing Password:	
OEM User Name:	oem
OEM Password:	
CFG User Name:	cfg
CFG Password:	
Regular User Name:	user
Regular User Password:	
Encrypt Wireless Keys:	Disabled
Protect the OEM Configuration:	Disabled
Authorization Level Settings	
Minimum Authorization Level for Reset To Factory Defaults:	CFG Level User
Minimum Authorization Level for Radio Off:	CFG Level User
Minimum Authorization Level for Radio On:	CFG Level User
SSH Settings	
SSH Default User Name:	
SSH Default Password:	
SSH Keysize (evenly divisible by 8):	1024
Power Save Settings	
Module Power Save Mode:	Active
Serial Port 1 Inactivity Timer:	0
Serial Port 2 Inactivity Timer:	0
Radio Startup Mode:	On
FTP Settings	
FTP Server IP Address or Name:	
FTP User Name:	
FTP Password:	
FTP Server Path:	
FTP File Name:	
System Time Settings	
Timezone Name:	EST
Timezone Offset:	-5:00
Daylight Saving Time Adjustment:	Enabled
Daylight Saving Time Name:	EDT
Daylight Saving Time Offset:	-4:00
Daylight Saving Time Starting Week:	Second
Daylight Saving Time Starting Day:	Sunday
Daylight Saving Time Starting Month:	March
Daylight Saving Time Ending Week:	First
Daylight Saving Time Ending Day:	Sunday
Daylight Saving Time Ending Month:	November
NTP Server IP Address or Name:	pool.ntp.org
NTP Sync at Startup:	Disabled
NTP Refresh Interval:	0

cont.

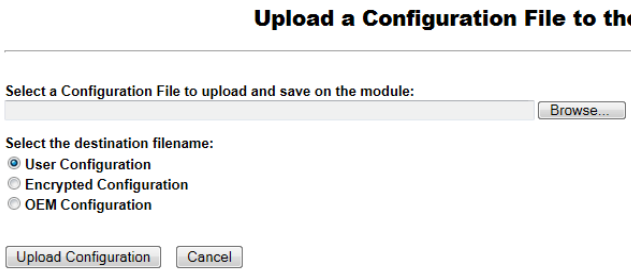


Field	CLI Command
OEM Defined Version String	
Discovery Manufacturer Device Name	`name-manuf`
Discovery OEM Device Name	`name-oem`
Discovery Device Name	`name-device`
Administrator Password	`pw-root`
Manufacturing User Name	`user-manuf`
Manufacturing Password	`pw-manuf`
OEM User Name	`user-oem`
OEM Password	`pw-oem`
CFG User Name	`user-cfg`
CFG Password	`pw-cfg`
Regular User Name	`user`
Regular User Password	`pw`
Encrypt Wireless Keys	`cfg-encrypt`
OEM Configuration Protect	`cfg-oem-protect`
Minimum Authorization Level for Reset	`auth-level reset`
Minimum Authorization Level for Radio off	`auth-level radio-off`
Minimum Authorization Level for Radio on	`auth-level radio-on`
SSH Default User	`ssh-default-user`
SSH Default Password	`ssh-default-password`
SSH Keysize (evenly divisible by 8)	`ssh-keysize`

Module Power Save Mode	pm-mode
Serial Port 1 Inactivity Timer	wl-sleep-timer, wl-sleep-timer-p1
Serial Port 2 Inactivity Timer	wl-sleep-timer-p2
Radio Startup Mode	radio-startup
FTP Server IP Address or Name	ftp-server-address
FTP User Name	ftp-user
FTP Password	ftp-password
FTP Server Path	ftp-server-path
FTP Filename	ftp-filename
Timezone Name	timezone-name
Timezone Offset	timezone-offset
Daylight Saving Time Adjustment	daylight-saving-time
Daylight Saving Time Name	daylight-saving-name
Daylight Saving Time Offset	daylight-saving-offset
Daylight Saving Time Starting Week	daylight-saving-startweek
Daylight Saving Time Starting Day	daylight-saving-startday
Daylight Saving Time Starting Month	daylight-saving-startmonth
Daylight Saving Time Ending Week	daylight-saving-stopweek
Daylight Saving Time Ending Day	daylight-saving-stopday
Daylight Saving Time Ending Month	daylight-saving-stopmonth
NTP Server IP Address or Name	ntp-server-address
NTP Sync at Startup	ntp-startup-sync
NTP Refresh Interval	ntp-refresh-interval
Antenna Mode	wl-ant
Speedlink Roaming	speedlink
Beacons Missed Before Roaming	wl-beacons-missed
Association Retry Count	wl-assoc-retries
Association Backoff Time (msec)	wl-assoc-backoff
ARP Staleout Time	arp-staleout-time
ARP Reachable Time	arp-reachable-time
Use Directed Probes	wl-specific-scan
Lost Association Link Timeout	wl-link-timeout
Startup Message Mode	startup-msg
Startup Message Text	startup-text
WLAN DHCP Vendor Class ID String	wl-dhcp-vendorid
Ethernet DHCP Vendor Class ID String	eth-dhcp-vendorid
I/O Port F Bit Direction	io-dir-f
I/O Port F Internal Pullup Resistor	io-pullup-f
I/O Port G Direction	io-dir-g
I/O Port G Internal Pullup Resistor	io-pullup-g
Enable LED Signal Strength Meter	led-mode
Enable POST LED	post-led
Enable RF_LINK LED	rf-link-led
Enable WLN_CFG LED	wln-cfg-led
Enable CONN LED	conn-led
Enable Echo for Telnet Sessions	telnet-echo
UDP Server Ping	wl-udp-ping

UPLOAD CONFIGURATION FILE

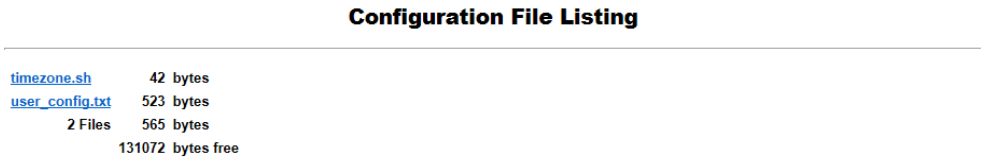
URL	/Configuration/Upload Configuration File
Description	Allows user, OEM or encrypted configuration files to be uploaded to the device.



Field	CLI Command
Upload Configuration [button]	`put-cfg`
User Config	`put-cfg user_config.txt`
Encrypted Configuration	`put-cfg user_enc_config.uue`
OEM Configuration	`put-cfg oem_config.txt`

LIST CONFIGURATION FILE

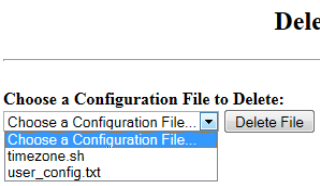
URL	/Configuration/List Configuration File
Description	Displays a list of the configuration files saved to the device.



Field	CLI Command
Displayed Page	`list-cfg`

DELETE CONFIGURATION FILE

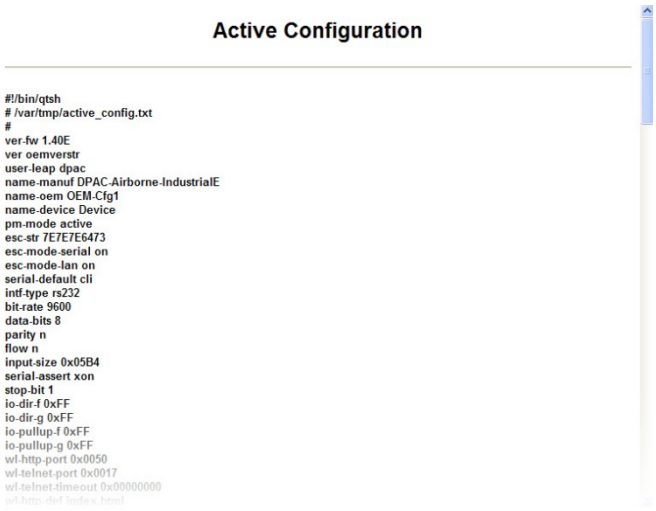
URL	/Configuration/Delete Configuration File
Description	Allows configuration files saved to the device to be deleted.



Field	CLI Command
Delete File [Button]	`del-cfg`

ACTIVE CONFIGURATION

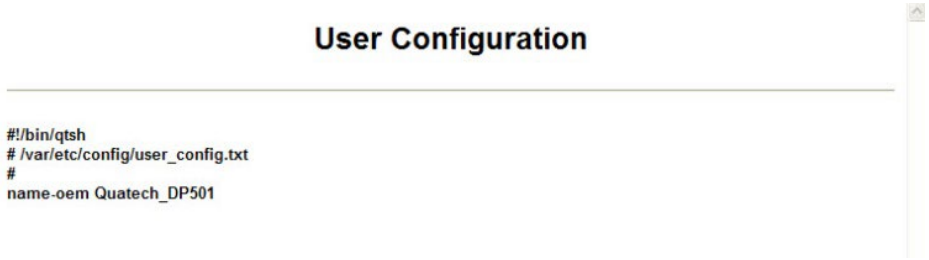
URL	/Configuration/Active Configuration
Description	Displays the current configuration settings being used by the device.



Field	CLI Command
Displayed Page	`cfg-dump active`

USER CONFIGURATION

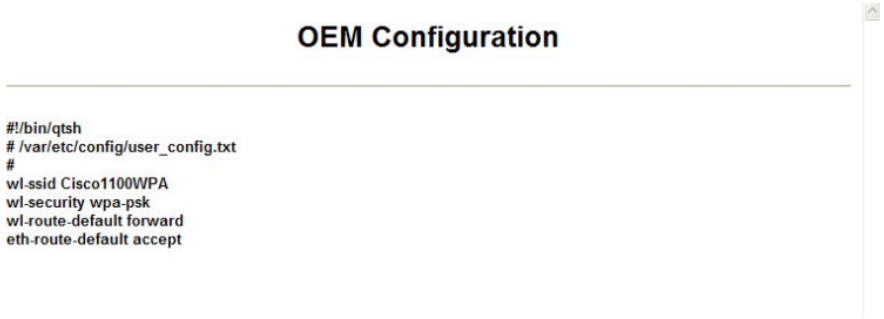
URL	/Configuration/User Configuration
Description	Displays the contents of the user_config.txt configuration file.



Field	CLI Command
Displayed Page	`cfg-dump user`

OEM CONFIGURATION

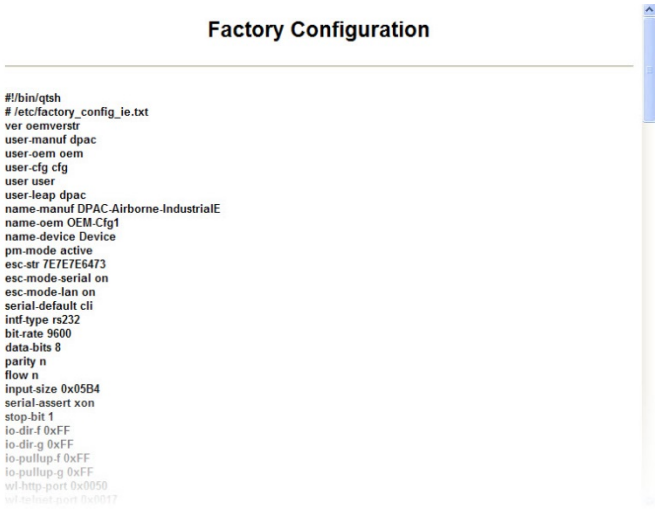
URL	/Configuration/OEM Configuration
Description	Displays the contents of the oem_config.txt configuration file.



Field	CLI Command
Displayed Page	`cfg-dump oem`

FACTORY CONFIGURATION

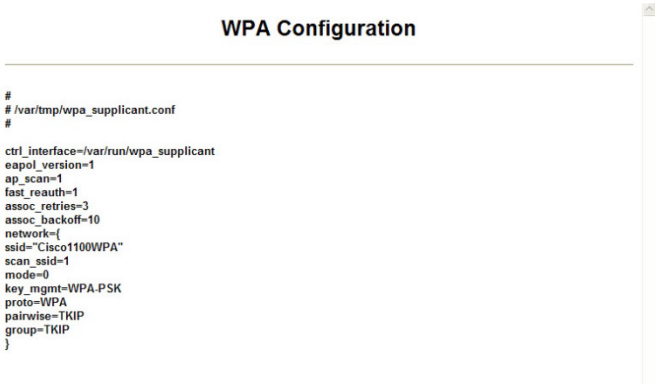
URL	/Configuration/Factory Configuration
Description	Displays the factory configuration settings. These are the default settings delivered from the B+B SmartWorx factory.



Field	CLI Command
Displayed Page	`cfg-dump factory`

WPA CONFIGURATION

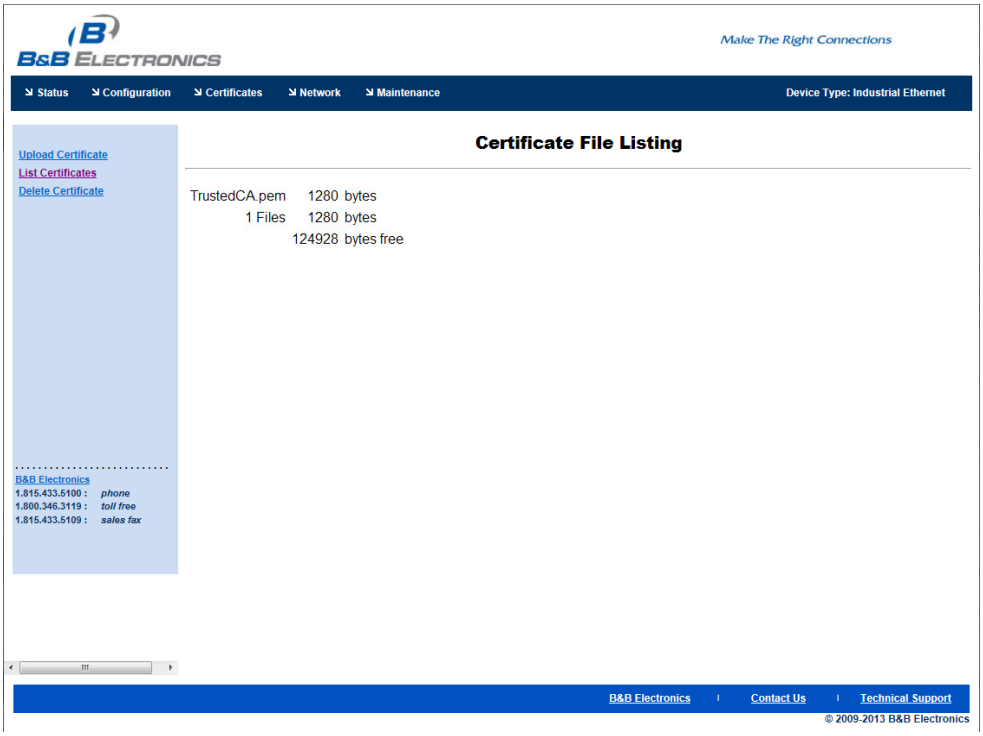
URL	/Configuration/WPA Configuration
Description	Displays the current security configuration settings being used by the device.



Field	CLI Command
Displayed Page	`cfg-dump wpa`

LIST CERTIFICATES

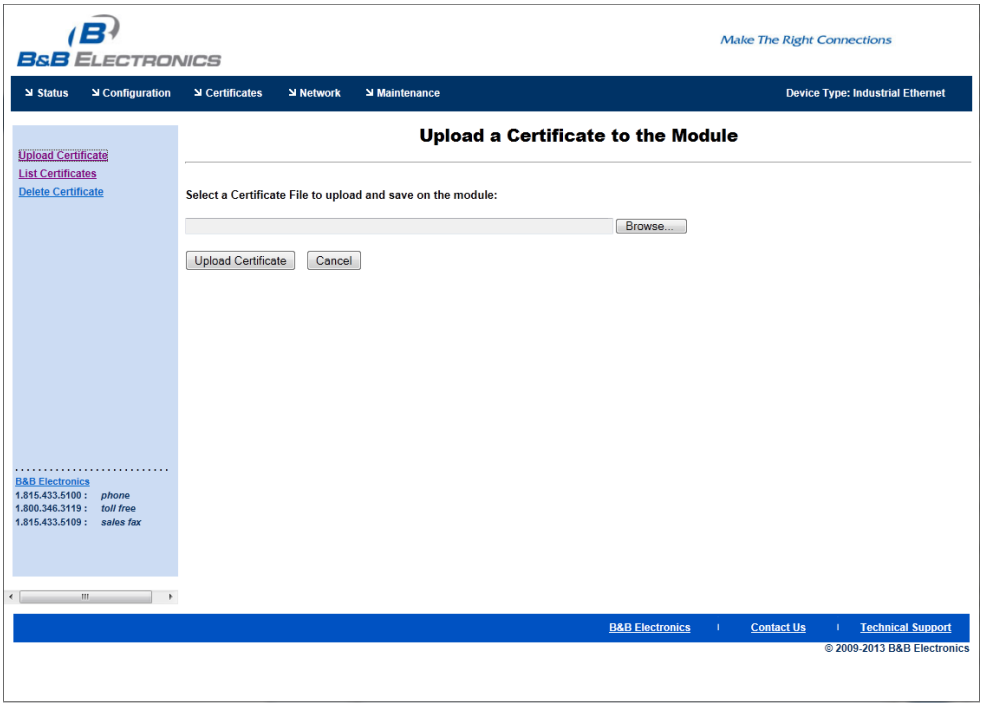
URL	/Certificates/List Certificates
Description	Displays a list of the certificates saved to the device. This is the home page for the certificates link.



Field	CLI Command
Displayed Page	`list-cert`

UPLOAD CERTIFICATE

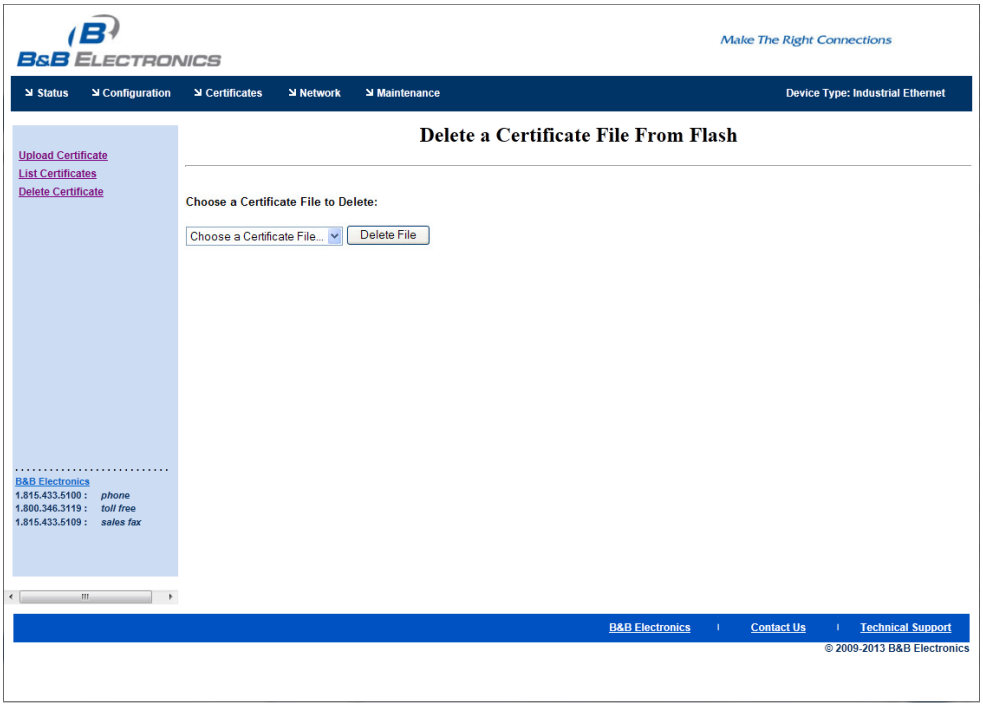
URL	/Certificates/Upload Certificate
Description	Enables certificates and private keys to be uploaded to the device.



Field	CLI Command
Upload Certificate [Button]	`put-cert`

DELETE CERTIFICATE

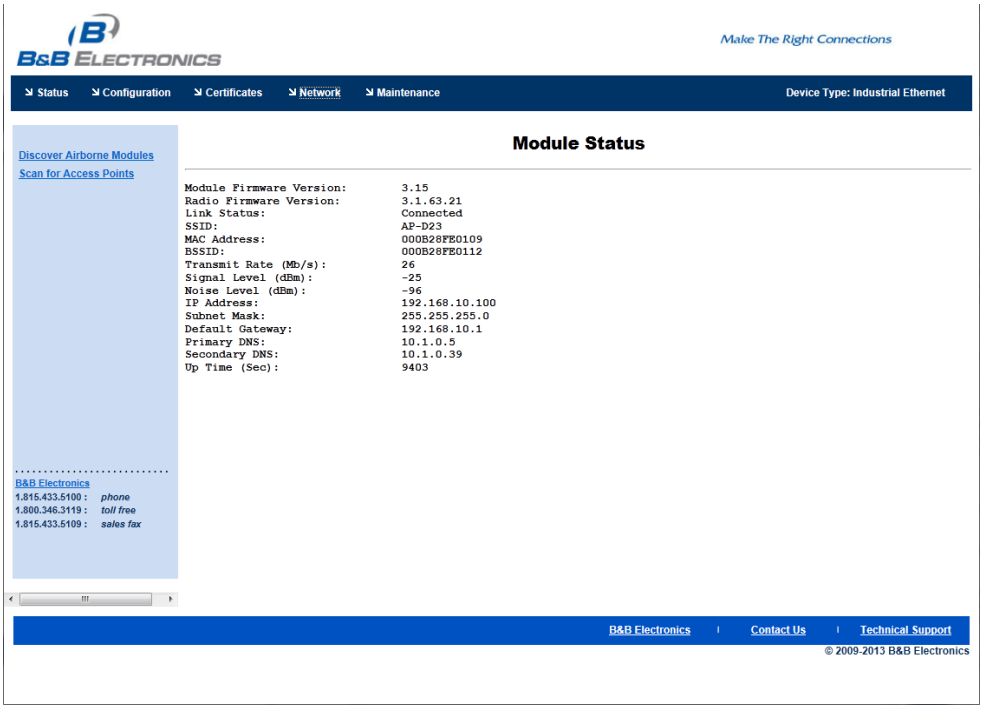
URL	/Certificates/Delete Certificate
Description	Allows certificates stored on the device to be deleted.



Field	CLI Command
Delete Certificate [Button]	`del-cert`

NETWORK (HOME PAGE)

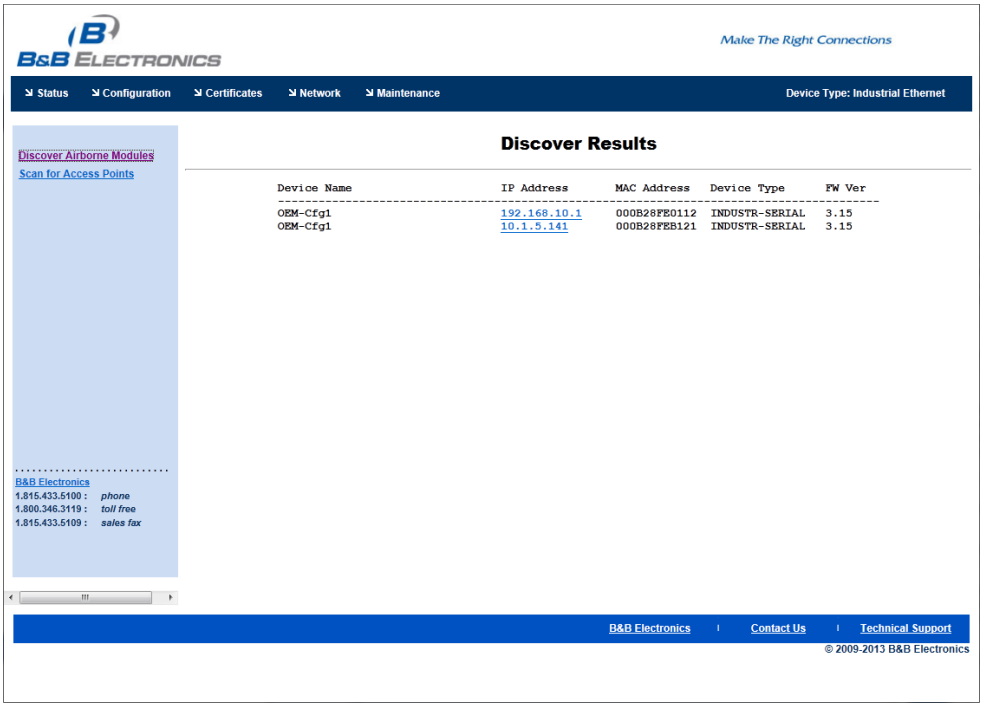
URL	/Network
Description	Home page for the network related pages.



Field	CLI Command
Displayed Page	`wl-info`

DISCOVER AIRBORNE MODULES

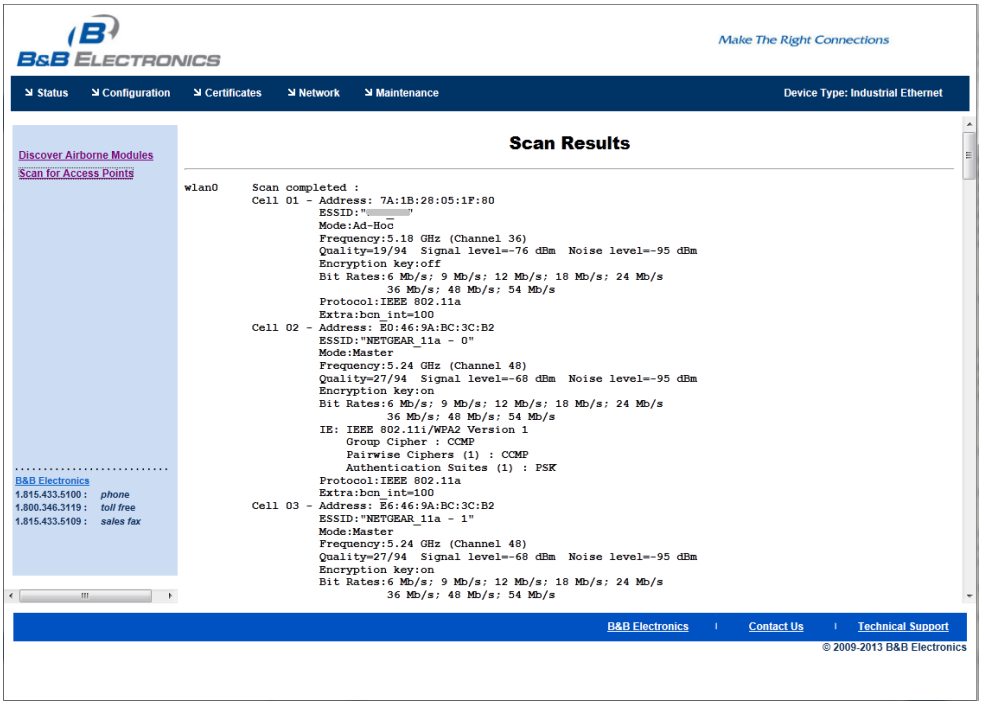
URL	/Network/Discover Airborne Modules
Description	Displays a list of Airborne devices, with IP address, device type and Wireless or Ethernet MAC address, visible to the device on the current network.



Field	CLI Command
Displayed Page	`discover`

SCAN FOR ACCESS POINTS

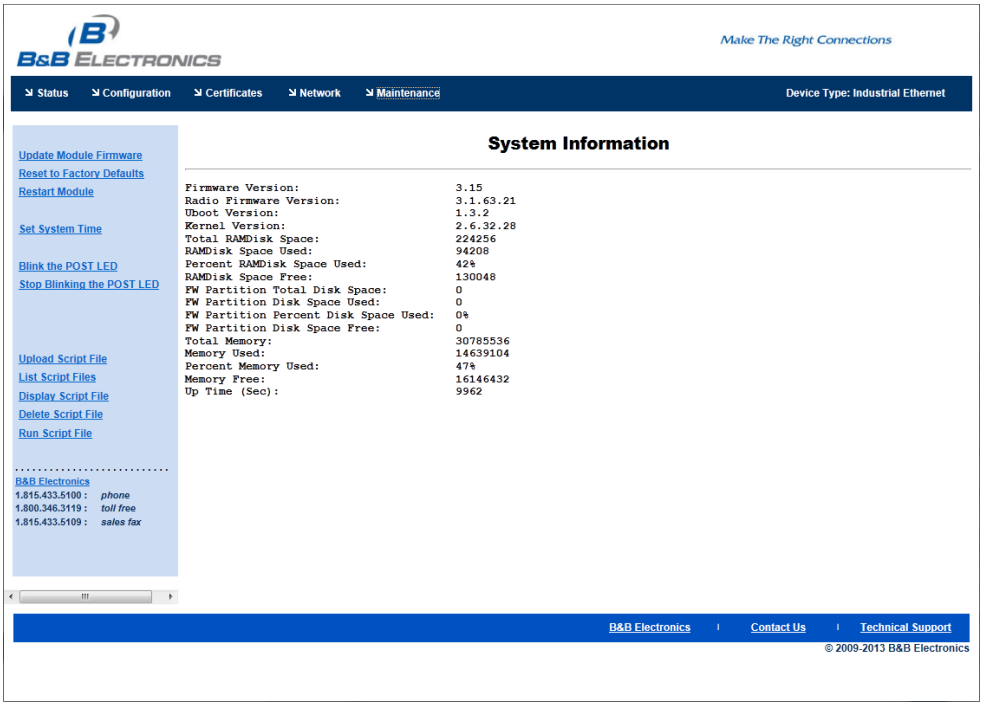
URL	/Network/Scan for Access Points
Description	Displays a list of wireless networks within range of the device



Field	CLI Command
Displayed Page	`wl-scan`

MAINTENANCE (HOME PAGE)

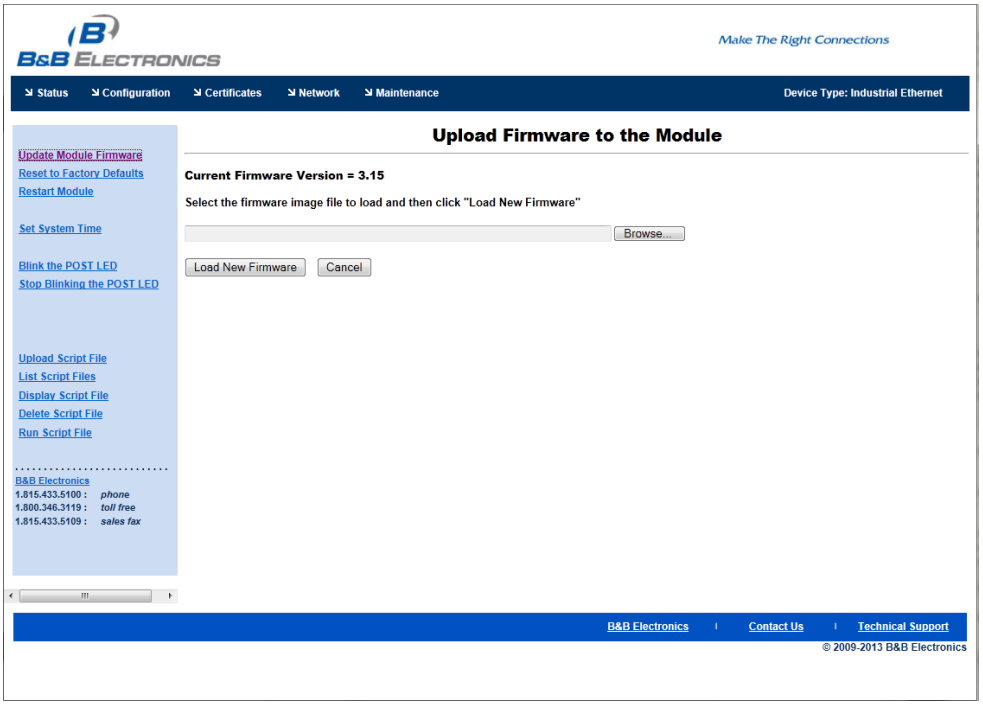
URL	/Maintenance
Description	Home page for the maintenance related pages.



Field	CLI Command
Displayed Page	`sys-info`

UPDATE MODULE FIRMWARE

URL	/Maintenance/Update Module Firmware
Description	Enables module firmware to be updated.



Field	CLI Command
Load New Firmware [Button]	`update`

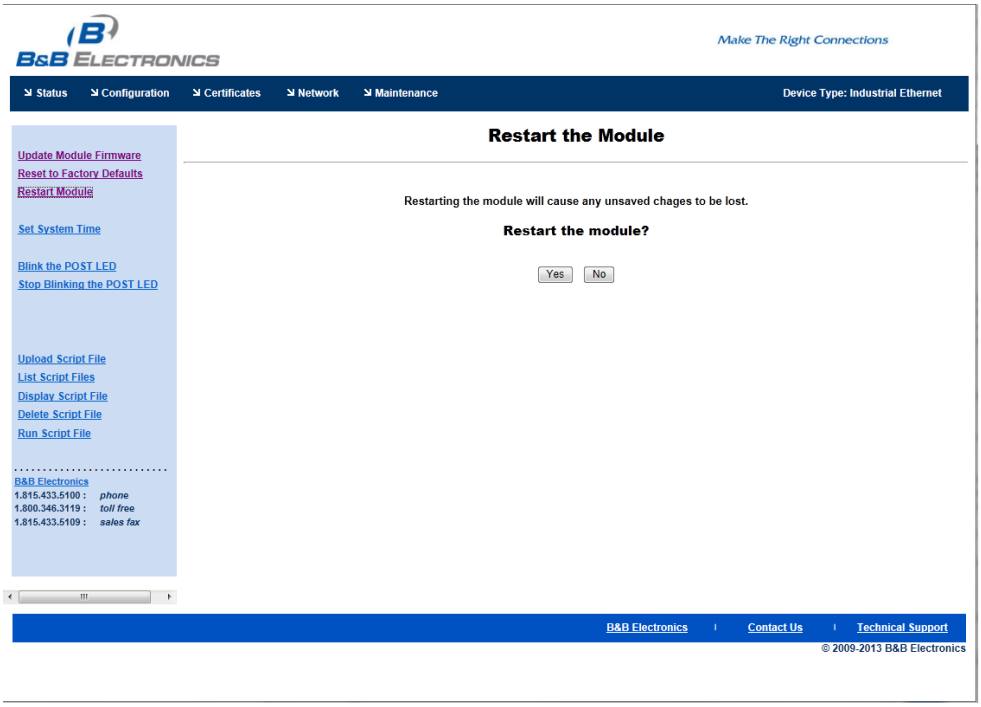
RESET FACTORY DEFAULTS

URL	/Maintenance/Reset Factory Defaults
Description	Returns device to factory defaults. If oem_config.txt is present, this will take precedence over the factory configuration.

Field	CLI Command
Yes [Button]	`reset`

RESTART MODULE

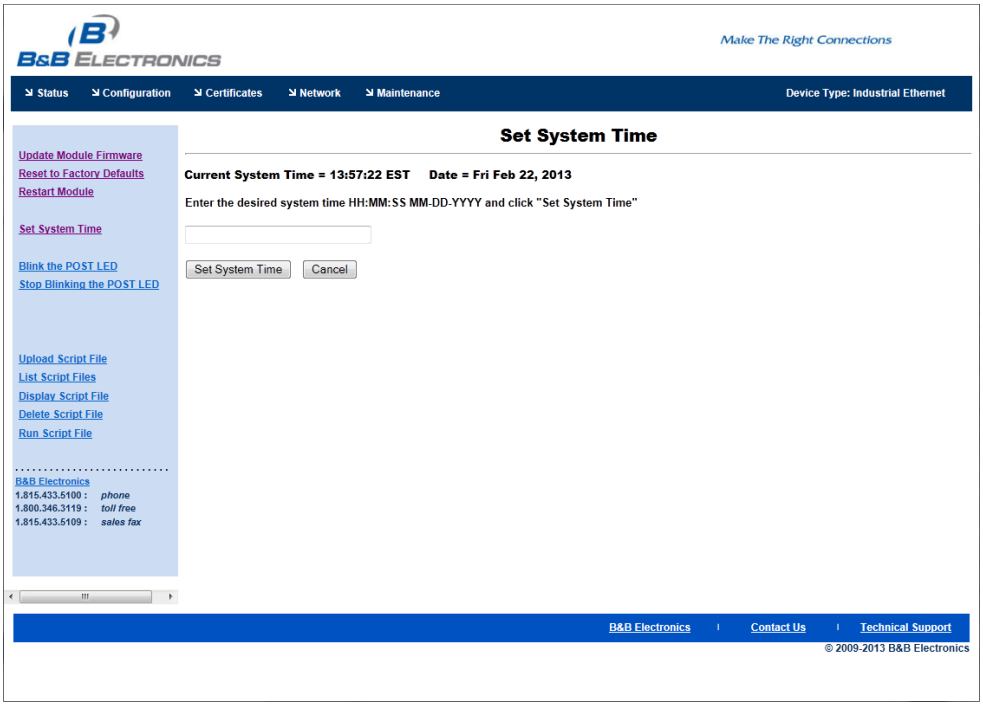
URL	/Maintenance/Restart Module
Description	Restarts device.



Field	CLI Command
Yes [Button]	`restart`

SET SYSTEM TIME

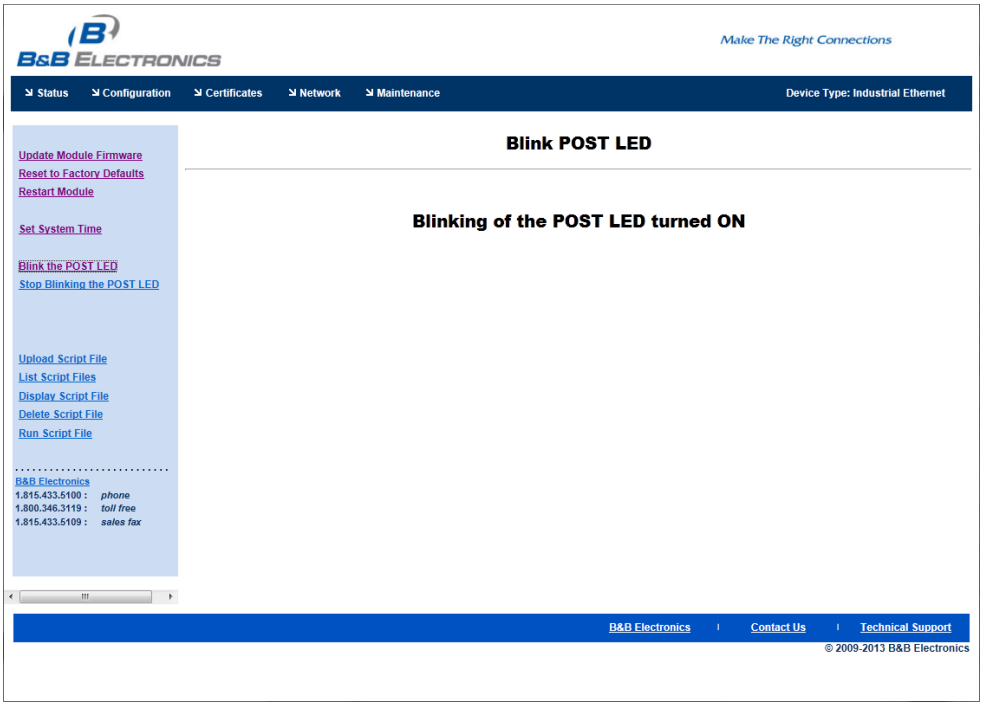
URL	/Maintenance/Set System Time
Description	Sets the current system time.



Field	CLI Command
Set System Time [Button]	`sys-time`

BLINK THE POST LED

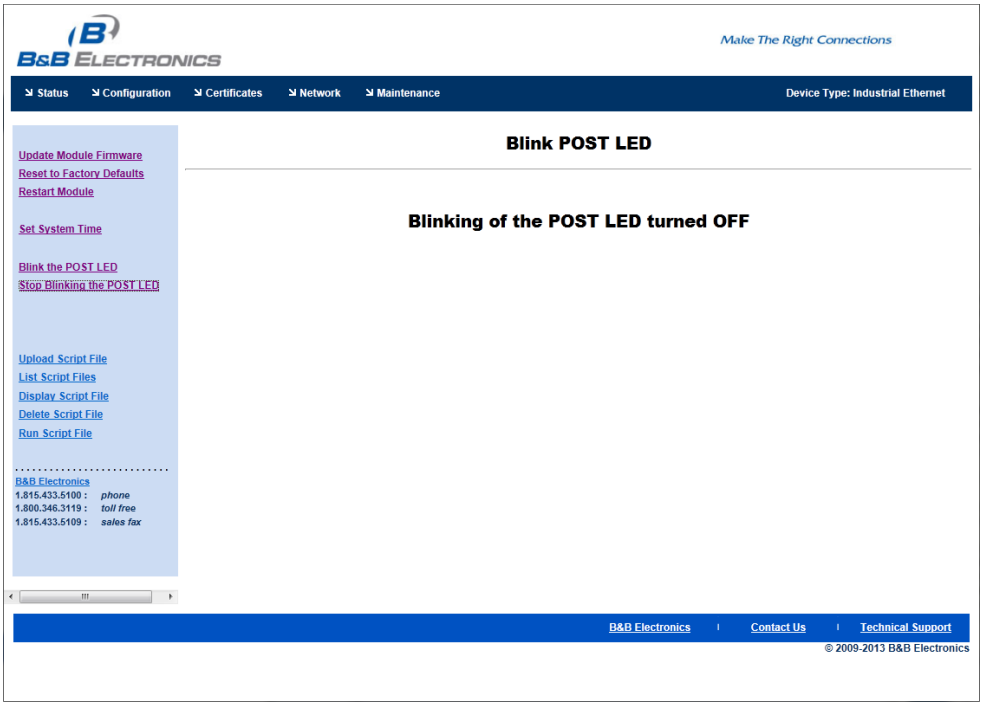
URL	/Maintenance/Blink the POST LED
Description	Starts the POST LED blinking. This identifies the specific device being communicated with.



Field	CLI Command
Displayed Page	`blink-post-led on`

STOP BLINKING THE POST LED

URL	/Maintenance/Stop Blinking the POST LED
Description	Stops the POST LED blinking.



Field	CLI Command
Displayed Page	`blink-post-led off`

CERTIFICATION & REGULATORY APPROVALS

IMPORTANT!

It is required that the following section be read and understood before use of the B+B Airborne™ device is permitted.

Use of approved antenna is required for compliance to FCC and IC regulations.

The unit complies with the following agency approvals:

Table 45 - Regulatory Approvals

Country	Standard	Status
North America (USA & Canada)	FCC Part 15 Sec. 15.107, 15.109, 15.207, 15.209, 15.247 Modular Approval	Complete
Europe	CISPR 16-1 :2014 ETSI EN 300 328 v2.1.1 2017 ETSI EN 301 893 v2.1.1 2017	Complete

FCC STATEMENT

This equipment has been tested and found to comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for assistance.
- Operations in the 5.15-5.25GHz and channel 5260MHz are restricted to indoor usage only.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC RF EXPOSURE STATEMENT

To comply with FCC/IC RF exposure compliance requirements, this device and its antenna must operate with a separation distance of a least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

INFORMATION FOR CANADIAN USERS (IC NOTICE)

This device has been designed to operate with an antenna having a maximum gain of 5.5dBi in the 5GHz band and 4.1 in the 2.4GHz band. An antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50Ω. Only an approved antenna may be used with this equipment.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Equivalent Isotropically Radiated Power (EIRP) is not more than required for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter (3913A-WLNN551) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device. Operations in the 5.15-5.25GHz and channel 5260MHz are restricted to indoor usage only.

Cet émetteur radio (3913A-WLNN551) a été approuvé par Industrie Canada pour fonctionner avec les types d'antennes énumérés ci-dessous avec le gain maximal admissible et l'impédance d'antenne requise pour chaque type d'antenne indiqué. Types d'antennes ne figurent pas dans cette liste, ayant un gain supérieur au gain maximum indiqué pour ce type, sont strictement interdites pour une utilisation avec cet appareil. Les opérations dans l'5,15 à 5,25 GHz et 5260MHz canaux sont limités à une utilisation en intérieur uniquement.

The following is a list of antennas approved to work with this transmitter. Please contact your B&B SmartWorx representative if you have any questions.

MFG	P/N	Max. Gain 2.4G (dBi)	Max. Gain 5G (dBi)	Impedance (Ω)
Laird	CAF 94505	2.0	4.0	50
Nearson	T131AH-2.4/4.9/5.X-S	2.0	2.0	50
Taoglas	GW.71.5153	3.8	5.5	50
Taoglas	PC.11.07.0100A	3.0	4.5	50
Taoglas	WS.01.B.305151	4.1	4.7	50
Taoglas	FXP.810.07.0100C	2.4	5.1	50
Taoglas	FXP.830.07.0100C	2.6	5.0	50

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population. Consult Safety Code 6, obtainable from Health Canada's website www.hc-sc.gc.ca.

This Device complies with Industry Canada license-exempt RSS standard(s).Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

FCC/IC MODULAR APPROVAL

This document describes the Airborne WLN FCC modular approval and the guidelines for use as outlined in FCC Public Notice (DA-00-1407).

The ABDx-XX-DP5xx is covered by the following modular grants:

Table 46 - Modular Approval Grant Numbers

Country	Standard	Grant
North America (USA)	FCC Part 15 Sec. 15.107, 15.109, 15.207, 15.209, 15.247 Modular Approval	F4AWLNN551
Canada	RSS 210 Modular Approval	3913A-WLNN551

By providing FCC modular approval on the Airborne WLN modules, the customers are relieved of any need to perform FCC Part15 Subpart C Intentional Radiator testing and certification, except where they want to use an antenna that is not already certified.

B+B SmartWorx supports a group of pre-approved antennas. Use of one of these antennas eliminates the need to do any further Subpart C testing or certification. If an antenna is not on the list, it is a simple process to add it to the pre-approved list without having to complete a full set of emissions testing. Please contact B+B SmartWorx Technical support for details of the company's qualification processes.

Please note that, as part of the FCC requirements for the use of the modular approval, the installation of any antenna must require a professional installer. This is to prevent any non-authorized antenna from being used with the radio. There are ways to support this requirement but, the most popular is to utilize a non-standard antenna connector; this designation includes the reverse polarity versions of the most popular RF antenna types (SMA, TNC, etc.). For more details please contact B+B SmartWorx.

The following documents are associated with this application note:

- FCC Part 15 – Radio Frequency Devices
- FCC Public Notice – DA-00-1407A1 (June 26, 2000)

B+B SmartWorx recommends that, during the integration of the radio into the customer's system, any design guidelines be followed. Please contact B+B SmartWorx Technical Support if you have any concerns regarding the hardware integration.

Contact B+B SmartWorx Technical Support for copies of FCC and IC grant certificates, test reports, Declarations of Conformity and Compliance, and updated approved antenna list.

REGULATORY TEST MODE SUPPORT

The Airborne Device Server includes support for all FCC, IC and ETSI test modes required to perform regulatory compliance testing on the module. Please contact B+B SmartWorx Technical Support for details on enabling and using these modes.

PHYSICAL & ENVIRONMENTAL APPROVALS

The device has passed the following primary physical and environmental tests. The test methods referenced are defined in SAE J1455, August1994.

Table 47 - Mechanical Approvals

Test	Reference	Conditions
Temperature Range (Operational)	Table 1B, Type 2b	-40 to +85 °C
Temperature Range (Non-Operational)		-40 to +125 °C
Humidity	Sect 4.2.3	0-95% RH @ 38 °C condensing Fig 4a – 8 hours active humidity cycle
Altitude	Sect 4.8	Operational: 0-12,000ft (62 KPa absolute pressure) Non-operational: 0-40,000ft (18.6 KPa absolute pressure)
Vibration*	Sect 4.9	Operational: 2.4 Grms, 10-1K Hz, 1hr per axis Non-operational: 5.2 Grms, 10-1K Hz, 1hr per axis
Shock*	Sect 4.10	Operational: 20Gs Max, 11ms half-sine pulse
Product Drop*	Sect 4.10.3.1	1m onto concrete, any face or corner, 1 drop
Packaging Drop*	Sect 4.10.2.1	32 inches onto concrete on each face and corner. Packaged in 'for transit' configuration.

* These tests were conducted with the module mounted in a suitable enclosure. See product datasheets for additional approvals. Test reports are available from B+B SmartWorx. Contact Technical Support for latest test documentation.