SMARTSWARM 300 Series

SMARTSWARM 341

User Manual

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 No.:   SmartSwarm 341_R1_0717manual.docx

CONTENTS

LIST OF TABLES

1. INTRODUCTION

SmartSwarm 341 is an IoT Integration Gateway powered by B+B SmartWorx SmartSwarm technology. Whilst it is able to integrate data from a number of Advantech and non-Advantech sources, it is primarily intended for use in applications where users need to interface to B+B SmartWorx first generation WZZARD wireless sensor networks and pass data into an IoT platform or application. Other Advantech data source options supported include ADAM and WISE I/O modules and also the SmartSwarm 351 Modbus interface gateways.
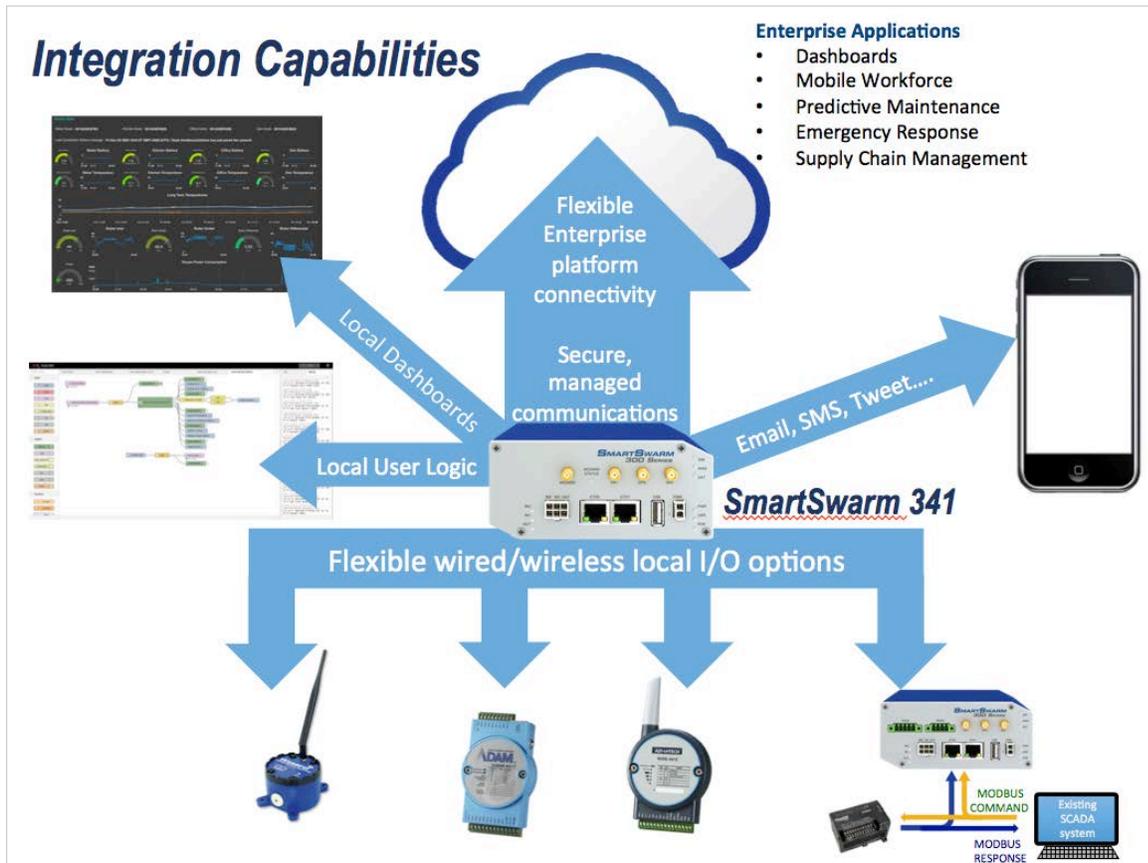
The gateway offers facilities for the manipulation of data prior to onward transmission via a Node-RED user programming environment and supports, via Node-RED, the direct export of data to a variety of platforms and in a variety of formats for applications where the sophistication of an enterprise level IoT approach is not required.

Standard data presentation capabilities include:
- The ability to serve dashboards via an embedded webserver.
- Direct interaction with users via email, SMS, tweet, etc.
- MQTT publish & subscribe (including an embedded broker for interaction with local MQTT devices).
- REST, web socket, UDP/TCP packets.

Payload encoding formats, including in JSON, XML, plain text, etc.

These standard facilities may be expanded by the download of additional function nodes from the Node-RED public library, offering a variety of connectors for different protocols, databases, web services platforms and systems.

Device management is available from the SmartWorx Hub platform, offering the ability to remotely manage configuration, firmware and application downloads.

Available in cellular or wired (Ethernet) uplink versions, the SmartSwarm 341 also acts as a simple router, routing traffic from the local LAN to the uplink, and providing firewall and VPN support.

2. EXAMPLE SYSTEM SETUP WORKFLOW

In this section, we will walk through an example workflow.
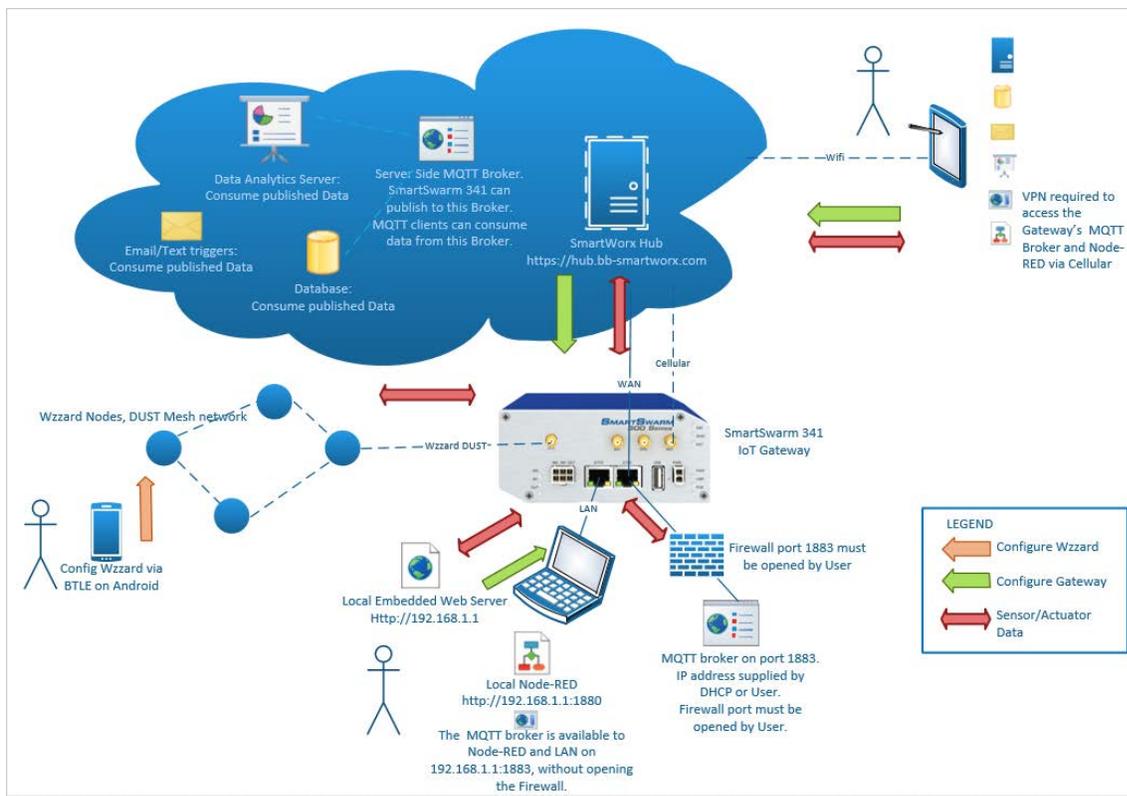
2.1 CONNECT YOUR SMARTSWARM IOT GATEWAY

First, ensure your hardware is physically connected.

If using cellular, connect your cellular antennae to the ANT and DIV connectors.

Insert a valid and data-provisioned SIM card into SIM 1: for the purposes of this example, we will assume your outbound WAN connection will be using a cellular connection. If this is not the case and your uplink is solely via Ethernet, then it is not necessary to connect antennae or install a SIM.

In this example, we will connect with a Wzzard wireless sensor node.

2.2 CONFIGURE YOUR SMARTSWARM IOT GATEWAY'S CONNECTIVITY TO SMARTWORK HUB

Use an Ethernet cable to connect your local laptop/desktop computer to your SmartSwarm Gateway's ETH0 port.

> ⚠️ *If you do not intend to use the cellular interface as your WAN connection, this step may not be necessary. ETH1 is configured to accept an IP address from a DHCP server. Providing that your environment permits it, the SmartSwarm gateway will then use ETH1 as the outbound WAN port.*
>
> *The USR LED will turn On (yellow) if the SmartSwarm gateway can automatically find a route, via ETH1, to **hub.bb-smartworx.com.***

The ETH0 port of the device has IP address **192.168.1.1**

The ETH0 port of the device is a DHCP server, so it will automatically serve an IP Address in the 192.168.1.x range to your laptop/desktop computer. Please ensure your laptop/desktop computer is configured to accept an IP address automatically from a DHCP server.

Open a web-browser, and browse to **192.168.1.1**

You will be prompted to sign in. The default password is "5mart5warm" (*uses figure 'five 'in place of 'S'*). We recommend that you change this default password after you login for the first time.
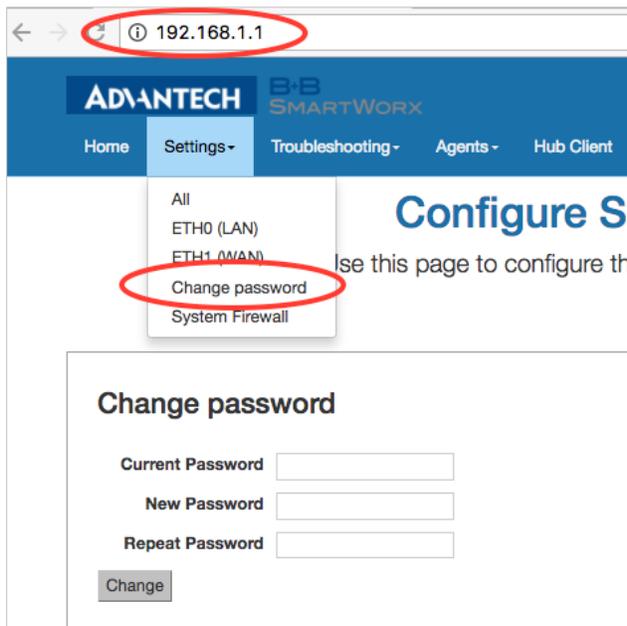
Select "Settings"->"Cellular (WAN)", and enter the appropriate APN and network authentication settings for your SIM card. In our example, we only need to enter an APN.

Enter the APN name and optional credentials, as required by your SIM card provider / network operator.

That's all you need to do.
The device will now attempt to:

(a) make a WAN connection using the cellular network, then:
(b) make a secure connection to SmartWorx Hub (on **hub.bb-smartworx.com**).

When (a) is successful, the WAN LED will turn on (yellow).
When (b) is successful, the USR LED will turn on (yellow).

The time it takes for (a) to be successful depends on your cellular network. But, you should expect it to be successful within minutes. If the WAN LED is not turning on, you may have entered invalid APN or network credential information for that SIM card.

Please verify that you are using a valid SIM card and valid cellular settings.

When the USR LED is On (yellow), your device has a secure connection to SmartWorx Hub.
The following graphic shows that the WAN and USR LEDs are both on (yellow).

⚠	*NOTE: If there is an internet connection both via cellular and Eth1, then the SmartSwarm 341 will use the Ethernet connection as the main route, and the cellular connection as the backup.*

Open a browser page, and login to SmartWorx Hub on *https://hub.bb-smartworx.com*

(NOTE: If you do not already have a user account on SmartWorx Hub, you may create one directly from *https://hub.bb-smartworx.com*, and use it immediately.)

In this example, we assume that (a) you have an account to login with SmartWorx Hub, and (b) you are using the cloud instance of SmartWorx Hub to manage your devices.
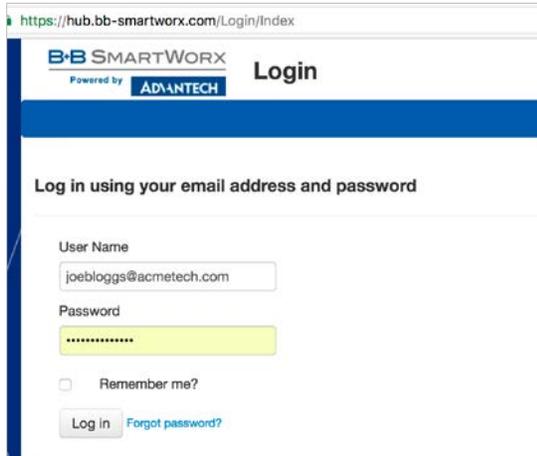
Go to the "Devices"->"Claim Device" screen to bring your new SmartSwarm Device into your Device Farm.

Type in the last 7 digits from your Device's Device-ID (this is written both on the Device itself and on the box that you took your Device out of).

Enter the last 6 digits of your Device's MAC Address (this is written both on the Device itself, and on the box that you took your Device out of), then select 'Check Device ID' to check that your device is available to be claimed by you: Assuming it is, then select "Claim Device".

If the check process fails, carefully re-enter the information indicated above. Be very careful not to confuse '8' & 'B' or '0' & 'D'/'C'. If the process still fails, please contact B+B SmartWorx technical support.
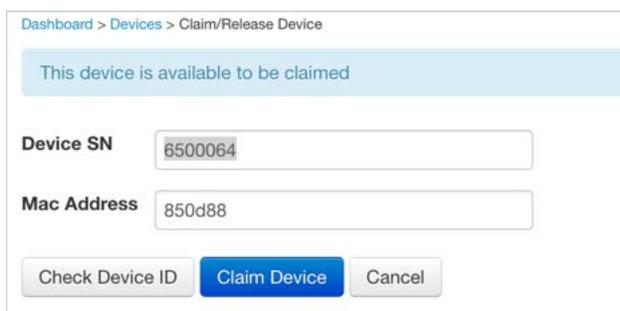
Your Device is now available for you to manage.

By selecting the 'Devices/View Devices' screen we can see that the device is available, and that it is currently On-line.

2.3 CONFIGURE THE GATEWAY'S MESH INTERFACE

Select your SmartSwarm Gateway by clicking on the Device ID.

Now, select the Wzzard App.

The default value for Network ID is: **1981**

The default value for Join Key is: **default**

The MQTT Broker will be enabled by default.

You should change the default settings only if you have configured, or if you intend to configure, your Wzzard wireless sensor node(s) to something other than the default values.

⚠	*We recommend that for each of your Deployed Wzzard Mesh Networks, you change only the Network ID. The Network ID and Join Key on all of your Wzzard wireless sensor nodes in your Wzzard Mesh Network must be the same, and it must match the Network ID that you configure for your SmartSwarm Gateway.*

Apply your changes.

2.4 CONNECT THE WZZARD WIRELESS SENSOR NODE TO THE SMARTSWARM IOT GATEWAY

By default, the mesh Network ID is set to 1981, and the Join Key is left blank (or use the text: **default**).

This corresponds to the default settings used in the WZZARD wireless sensor nodes. If everything is left in default configuration, then a new Wzzard node simply needs to be powered up in order for it to find and join the mesh network.

To configure your Wzzard to use a non-default Network ID and/or Join Key, please consult your Wzzard documentation.

When the Wzzard node is powered on, and the LED stops blinking, then it has successfully connected with a SmartSwarm gateway.

> ⚠ *If multiple gateways are used in the same geographic area, configured with the same Network ID and Join Key, then new Wzzard nodes will connect to the first gateway they find. If you have more than one Gateway, please* **ensure all your Gateways are using different Network IDs, and configure your WZZARD sensor nodes accordingly.**

2.5 EXPLORE THE NODE-RED ENVIRONMENT

Select the Node-RED App.

The SmartSwarm 341 runs a Node-RED programming environment by default but, the firewall port on the SmartSwarm gateway must be opened in order to access this service.

In order to access the Node-RED environment from your web-browser, you will need to open TCP port 1880 within the Node-RED containerized-application firewall.

Remember to Apply Changes to force your changes to take effect.

This will open port 1880, which enables access to the Node-RED Service on all physical interfaces.

You may access Node-RED via ETH1, using the WAN IP Address that has been assigned to ETH1 of your Device.

Remember to append ":1880" to the ETH1 IP Address. e.g. **10.8.0.198:1880**
(assuming the ETH1 WAN IP address that has been assigned is 10.8.0.198)

Alternatively, you may access the Node-RED programming environment by connecting your laptop/desktop via Ethernet cable to ETH0 of your device, and pointing your browser at: **192.168.1.1:1880**

> ⚠️ *Another alternative is to create an OpenVPN tunnel for your device, then remotely connect to your devices' Node-RED programming environment over the secure tunnel.*

2.6 GET DATA FROM A WZZARD NODE INTO THE GATEWAY USING NODE-RED

From the Node-RED Palette, select the "Wzzard" Input Node, and drag it onto the editor canvas.

Double-click on it to configure it.

By default, the Port will be 1883. Do not change this.

In the Topic field, enter: "BB/+/data", then click DONE.

This will subscribe to all data that is being published by all of the Wzzard wireless sensor nodes that are available on the current Wzzard Mesh Network.

From the Node-RED Palette, select the "debug" output node, and drag it onto the editor canvas. Join up the "Wzzard" node to the "debug" node.

Deploy this Node-RED Flow.

You should see that the "Wzzard" node is now "connected".

Turn on Debug output.

Now, you can verify that you are receiving Data from your Wzzard sensor nodes in the "debug" panel in the side-bar.
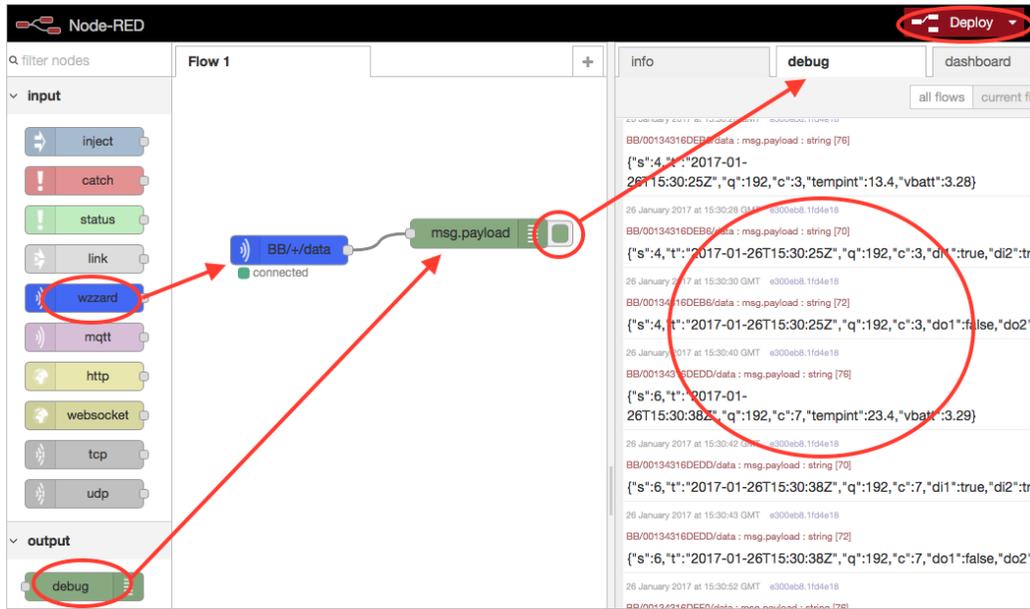
2.7 VERIFY YOUR SETUP

The checkpoints for your setup are:

- A secure connection has been established between your SmartSwarm gateway and SmartWorx Hub.

  o The USR LED on the SmartSwarm gateway is on (yellow).

  o You have an account on SmartWorx Hub. You have claimed your Device. You can manage your Device, and you can see that it is Online.

- There is a Wireless-Mesh connection between the SmartSwarm gateway and your wireless Wzzard mesh network.

  o The Gateway has been configured with a Network ID and Join Key.

  o The Wzzard Status LED on the IoT Gateway is on or blinking.

  o The Wzzards have been configured with the same Network ID and Join Key as the Gateway.

  o The Wzzards have been turned on and the LED has stopped blinking (it is off).

  o There is only one Gateway in the geographic vicinity with the same Network ID and Join Key.

- You have successfully opened a Node-RED session on the SmartSwarm gateway.

  o On the Node-RED session, you have a successful connection to the Wzzard Mesh network.

  o You can verify Sensor Data is being received from each of the Wzzard nodes on the Mesh, using the Debug Node-RED node and the Debug Tab on the Node-RED Editor.

NOTE: It is also possible to configure the mesh network and firewall from the local webserver within the gateway. Refer to the relevant sections in this manual for further information.

3. HARDWARE INSTALLATION

3.1 MOUNTING THE DEVICE

The unit may be mounted in any orientation. It can simply be placed on a flat surface or it can be DIN rail mounted using the supplied CKD2 holder.
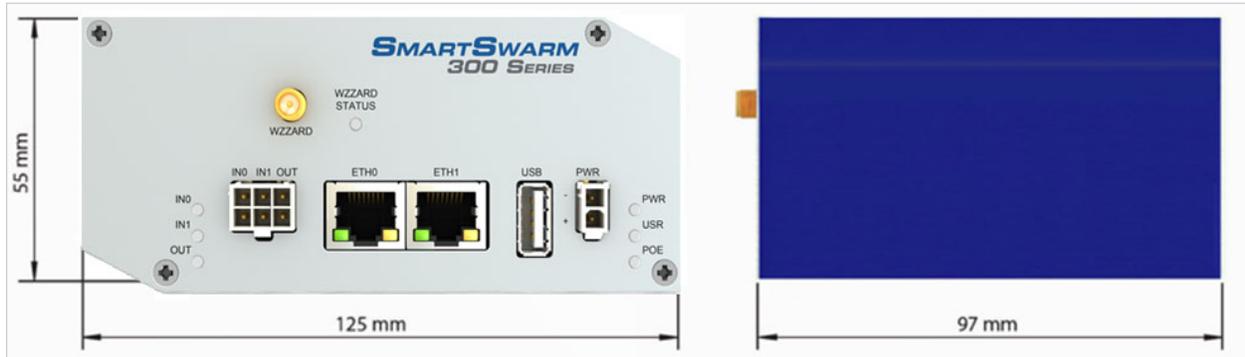
3.1.1 INSTALLING/REMOVING FROM A DIN RAIL

The CKD2 holder, which is used for mounting the gateway on a DIN rail, should be mounted such that the smaller flange on the holder is at the top when the unit is mounted on a DIN rail.

Default Orientation of the CKD2 Holder

To insert into a DIN rail, hook the lower (longer) flange into the DIN rail then rotate the top of the unit towards the DIN rail until it clicks into place. To remove from the DIN rail, lightly push the IoT gateway upwards until the top part of the CKD2 holder clears the top of the DIN rail. The top of the gateway can then be pulled away from the DIN rail, which will in turn release the lower DIN connection point.
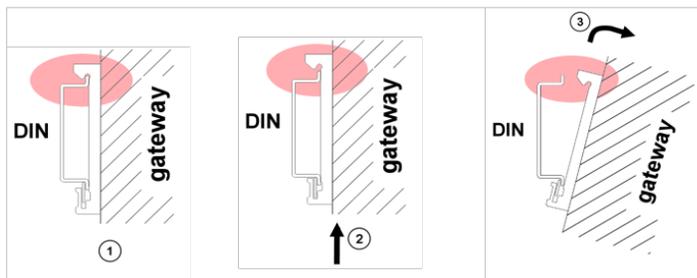
3.2 POWER CONNECTOR "PWR"
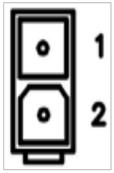
Panel Socket 2-pin

Pin	Identification	Description
1	GND(-)	Negative pole of DC supply voltage
2	VCC(+)	Positive pole of DC supply voltage (+10 to +60 V DC)

Table 1. Power Connector

The unit accepts the connection of power supplies in the range +10 V to +60 V DC. Protection against reverse polarity connection is built into the device.
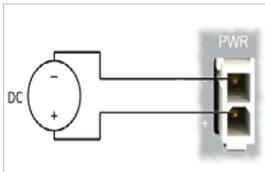
Circuit Example

3.3 ETHERNET PORT (ETH0 AND ETH1)
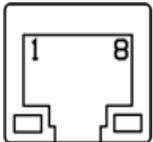
Panel Socket – RJ45

PIN	Signal Mark	Description	Data Flow Direction
1	TXD+	Transmit Data – positive pole	Input/Output
2	TXD-	Transmit Data – negative pole	Input/Output
3	RXD+	Receive Data – positive pole	Input/Output
4	—	—	—
5	—	—	—
6	RXD-	Receive Data – negative pole	Input/Output
7	—	—	—
8	—	—	—

Table 2. Ethernet Ports

Ethernet cables plug directly into the sockets. Always use a cable with an operational locking tab to avoid intermittent communications problems.

⚠	*The insulation strength is up to 1.5 kV.*
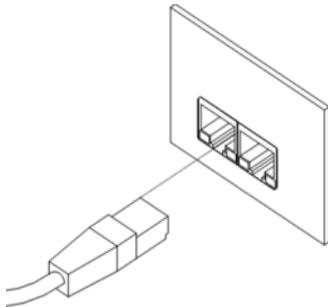
By default, ETH0 is set up as a DHCP server and is intended for the connection of diagnostic devices. ETH1 is set up as a DHCP client and may be used as an uplink for MQTT data being sent from the device.

Connector	Purpose	Default Setting
ETH0	**LAN port (default)** Connect your laptop or PC to this port to get a local web-server for device configuration and diagnostics.	**DHCP Server** IP Address: 192.168.1.1 NetMask: 255.255.255.0
ETH1	**WAN port (default)** Connect this port to your WAN to allow the device to obtain access to the remote device management service, SmartWorx Hub, over Ethernet.	**DHCP Client** The device will automatically obtain an IP address from your DHCP server, if you have a DHCP server provisioned to supply one.

Table 3. Ethernet Port Usage

If a connection exists via ETH1, it will take priority over a cellular connection for northbound data.

3.4 CELLULAR CONNECTION

If your device is cellular-enabled, you will need to attach the relevant antennae and install a data-enabled SIM card before you can use cellular connections.

3.4.1 ANTENNA CONNECTORS ANT, DIV AND GPS

If cellular communications are required, main and diversity antennas must be connected to the IoT Gateway via SMA connectors on the front panel. The *ANT* connector is used to connect the main antenna of the device. A second, diversity antenna, should be connected to the second cellular antenna connector (DIV) in order to improve the gateway radio performance at low signal strength, or in areas where the RF environment is constantly changing. (For example, near a road.) The third connector (*GPS*) is intended for GPS antenna connection and is not currently used by the SmartSwarm 341.

⚠	*The device cannot connect reliably to an LTE cellular network without an appropriate antenna connected to ANT and DIV.*

Antennae are connected by screwing to the SMA connector on the front panel of the IoT Gateway.
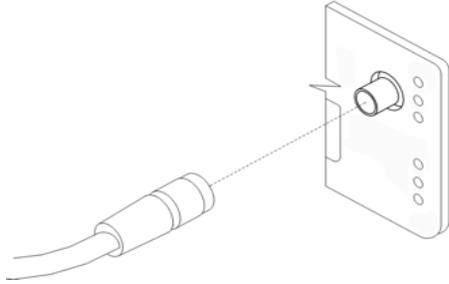
3.4.2 SIM CARD READER

Two SIM card readers for 3 V and 1.8 V SIM cards are placed on the rear panel of the device. Only the first of these (SIM1) is currently supported by SmartSwarm 341. In order to operate on a cellular network it is necessary to insert an activated, data enabled SIM card with an unblocked PIN code.

3.4.2.1 INSERTING/REPLACING A SIM CARD

⚠	*Before inserting or removing the SIM card disconnect the device from the power supply.*

Using a plastic opening tool, or your fingernail, press the SIM card into its slot until you hear a click.

To remove a SIM card press the SIM into the unit until you hear a click. After the click, release the card and it will pop out of its slot.

Remove the SIM card and push any other SIM card into the slot until it clicks in place.

⚠	*Only SIM1 is supported in the initial release of SmartSwarm 341.*

3.5 WZZARD WIRELESS SENSOR NETWORK

Please attach the supplied DUST Mesh Antenna to the Wzzard port.

The Wzzard LED will be ON (yellow) when the Wzzard application is up and running inside the gateway.

The Wzzard LED will blink briefly when there is data being transmitted or received on the Wzzard interface.

3.6 MICROSD CARD READER

The MicroSD card socket, located on the rear panel of the unit, may be used to store or read files. This feature is useful in the context of any Node-RED flows that you may write, which need to store large amounts of data.

If the Gateway is powered on with SD card inserted, then it will be mounted on **/mnt/sd**

The SD Card will only be available if you have the Node-RED application installed (this is installed by default on your SmartSwarm 341 Gateway).

3.7 USB PORT

The USB port, located on the front panel of the unit, may be used to store or read files. This feature is useful in the context of any Node-RED flows that you may write, which need to store large amounts of data.

If the Gateway is powered on with a USB storage device inserted, then it will be mounted on **/mnt/usb**

The USB storage device will only be available if you have the Node-RED application installed (this is installed by default on your SmartSwarm 341 Gateway).

3.8 I/O PORT

The I/O port, located on the front panel, is currently unused by SmartSwarm 341.

3.9 LEDS

The following table describes the LED operation on the SmartSwarm device:

LED	Color	State	Description
PWR	Green	Off	No power
		On	Device is booting
		Blinking	Device is in normal operating mode
		Fast Blinking	Device is updating firmware. Do not power off
USR	Yellow	Off	The device does not have a working session established with SmartWorx Hub
		On	The device has a working secure session established with SmartWorx Hub
PoE	Not Used	Not Used	Not used
DAT	Red	Off	There is no communication on the cellular interface at this moment
		Blinking	There is communication in progress on the cellular interface
SIM	Green	Off	Reset button pressed or the device is booting
		On	Ready for operation. SIM 1 is enabled
WAN	Yellow	Off	There is no cellular connection between the SmartSwarm device and the cellular service provider
		On	A cellular connection has been successfully established between the SmartSwarm device and the cellular service provider
WZZARD STATUS	Yellow	Off	The Wzzard App on the Gateway is either not installed or not running
		On	The Wzzard App is installed and running
		Blinking	There is communication in progress on the Dust SmartMesh IP network
IN0	Green	Off	The default state
		On	Binary input No. 0 is active (user defined)
IN1	Green	Off	The default state
		On	Binary input No. 1 is active (user defined)
Out	Yellow	Off	The default state
		On	Binary output is active (user defined)
ETH0 ETH1	Green	On	10 Mb/s
		Off	100 Mb/s
ETH0 ETH1	Yellow	On	The network cable is connected
		Off	Network cable is not connected
		Blinking	Data transmission in progress

Table 4. LED Indicators

4. CONFIGURE CONNECTIVITY TO SMARTWORX HUB

All configuration of the SmartSwarm 341 IoT Gateway can be performed using the SmartWorx Hub cloud based management platform.

⚠️	*SmartWorx Hub is accessed via the primary uplink port on the SmartSwarm 341. This is ETH1 if it is connected to a local LAN providing outbound (internet) access or the cellular connection if no outbound LAN connection exists via ETH1.*
	The connection status to SmartWorx Hub is indicated by the LEDs on the front panel of the SmartSwarm Gateway. The USR LED will be solid ON (yellow) if a secure connection to SmartWorx Hub has been achieved.

If the internet connection is to be via cellular connection, then ensure that appropriate antennas are connected, and SIM card inserted, before moving on to the first step below.

4.1 STEP #1: CONNECT TO LOCAL WEBSERVER

Connect a local laptop or desktop PC to ETH0. Open a browser and navigate to 192.168.1.1. Note that if you have another LAN connection (e.g. via Wi-Fi) you may need to disconnect this second session, depending upon your network settings and the domain of the LAN.

4.2 STEP #2: CONFIGURE THE CELLULAR APN DETAILS

Enter the APN name and optional credentials as required by your SIM card provider / network operator. Apply it. The WAN LED will turn ON (yellow) when the cellular connection has been successfully established.

4.3 STEP #3: VERIFY THE SECURE CONNECTION WITH SMARTWORX HUB

The USR LED will turn on (yellow) when the device successfully makes a secure connection with SmartWorx Hub (*https://hub.bb-smartworx.com*).

There is no specific setup step for this, This will happen automatically as soon as the Device has a valid WAN route through which it can make a secure connection to SmartWorx Hub.

4.4 STEP #4: VERIFY THAT YOUR DEVICE IS AVAILABLE ON SMARTWORX HUB

The device verification will be complete when you can see that your device is shown as "Online" in SmartWorx Hub.

4.4.1 CREATE AN ACCOUNT ON SMARTWORX HUB

If you do not already have a user account on SmartWorx Hub, you may create one directly from *https://hub.bb-smartworx.com*, and use it immediately.

From the Login page, select "Create Account".
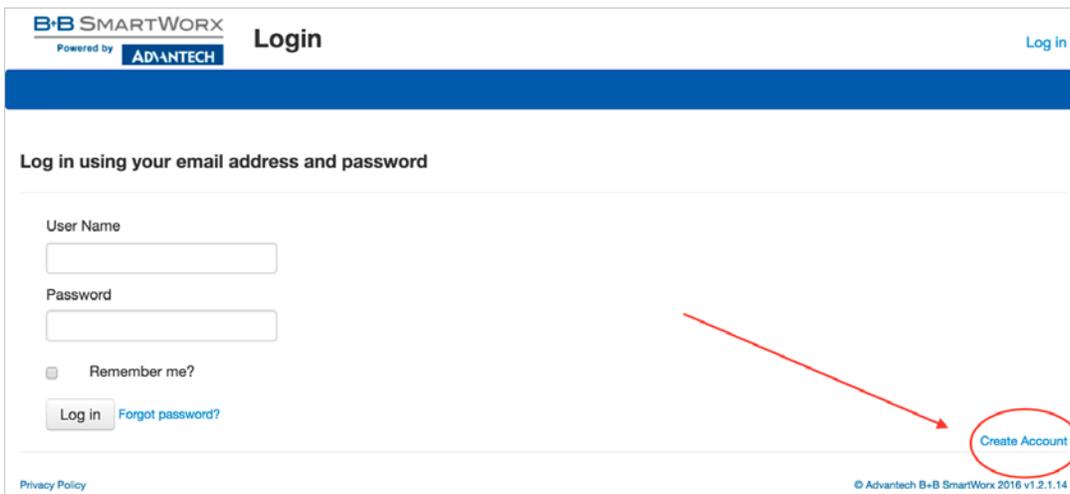
You will be presented with a Form to fill out.

When you have completed the Form, your account will be created automatically.

SmartWorx Hub will send you an auto-generated email, which will verify your email address, and which will give you a link back to SmartWorx Hub from which you will be prompted to create your password.

Once you have successfully created login credentials for yourself, you will be able to login to SmartWorx Hub.

Once you have accepted the terms of the EULA, you will be granted access to SmartWorx Hub.

> ⚠️ *By default, you will be granted a Trial License to SmartWorx Hub.*
>
> *SmartWorx Hub is free to use for your first 50 connected SmartSwarm devices. Note that this total does not include other B+B SmartWorx devices such as SmartFlex, SmartMotion and SmartStart routers. Only 2 such devices may be connected to a free account of SmartWorx Hub.*
>
> *If you wish to extend the terms of this automatically allocated License, please contact your local Advantech B+B SmartWorx Sales representative.*

Now that you have created login credentials for yourself, you may login.
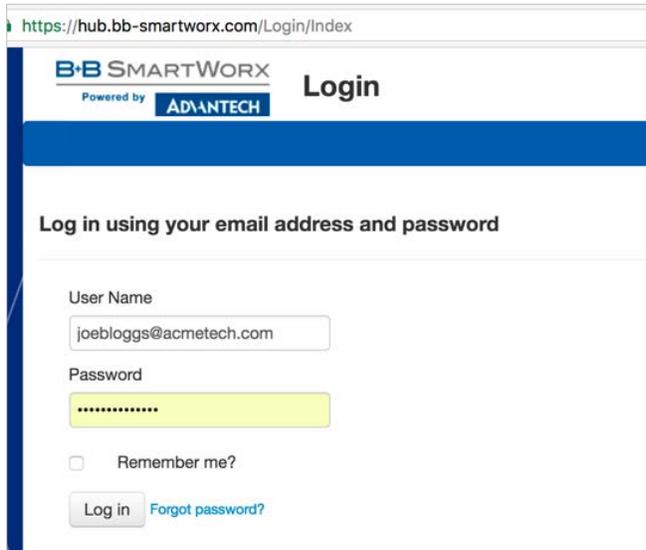
4.4.2 CLAIM YOUR DEVICES ON SMARTWORX HUB

Go to the "Devices"->"Claim Device" screen to bring your new SmartSwarm Device into your Device farm.

To Claim a Device, you must be able to verify that you physically have that Device in your possession.

We use a 2-factor verification process: You will be asked to enter both the Device ID and the MAC Address for each Device that you wish to Claim.

For each Device that you wish to Claim:

Type in the last 7 digits from your Device's **Device-ID** (this is written both on the Device itself and on the box that you took your Device out of). Enter the last 6 digits of your Device's **MAC Address** (this is written both on the Device itself and on the box that you took your Device out of), then select 'Check Device ID' to check that your device is available to be claimed by you: Assuming it is, select "Claim Device".

If the check process fails, carefully re-enter the information indicated above. Be very careful not to confuse '8' & 'B' or '0' & 'D'/'C'. If the process still fails, please contact B+B SmartWorx technical support.

Your Device is now available for you to manage.

By selecting the 'Devices/View Devices' screen we can see that the device is available, and that it is currently Online.

!	*You will need to refresh this page to see the current status of your devices.*

4.5 FACTORY DEFAULTS

If the unit is not connecting as expected, it may be reset to Factory Defaults at any time by pressing and holding the Reset button on the back-panel of the device for more than 10 seconds.

NOTE: Resetting a device to factory defaults will have the following effects:

Configuration Settings: All settings are reset to their default values.

Apps: App settings are reset to default. Any App downloaded from SmartWorx Hub is not deleted.

Node-RED flows and additional palette nodes: Not affected.

Node-RED created files: Not affected.

5. SMARTSWARM 341 ON SMARTWORX HUB

!	*Once you have Claimed your Device on SmartWorx Hub (see previous chapter) you may edit and configure it.* *If your device is currently offline, all changes you make are queued. All of your changes will be immediately applied as soon as the device comes online.*

5.1 DEVICE MANAGEMENT

Please refer to the SmartWorx Hub user manual for more detailed information on general device management.

With large device populations, use the search textbox to restrict the display to those units with matching information.

Find the device that you wish to manage in the "**View Devices**" screen, and click on it to open the "**Manage Device**" screen.

For the SmartSwarm 341 IoT Gateway, there are two applications that you may select in order to configure them: Wzzard, and Node-RED.

Refer to the chapters on configuring Wzzard, Node-RED and gateway connectivity to get data on the significance of the configurable parameters available.

6. CONFIGURE THE WZZARD INTERFACE AND LOCAL MQTT BROKER

When you click on the Wzzard App, you will be presented with the configuration screen that enables you to configure the IoT Gateway's Dust SmartMesh IP wireless sensor network interface; the IoT Gateway's MQTT Broker; and the IoT Gateway's MQTT Bridge.

To join the SmartMesh IP wireless sensor network, each Wzzard Node must be configured with the correct Network ID and Join Key. The Network ID and Join Key together must form a unique combination for every wireless sensor network.

It is the Network ID and Join Key that bind the IoT Gateway to the SmartMesh IP wireless sensor network. These parameters are persistent and should be set up once prior to, or during, installation.

The Network ID of the IoT Gateway must match the Network ID of the Wzzard nodes on the intended wireless sensor network. If multiple networks are operating on the site, additional care should be taken to ensure that the Nodes' Network IDs are set correctly.

Wzzard Wireless Sensor Nodes use a Join Key to encrypt the initial join request when joining a network. If the Join Key used by the Node does not match the Join Key configured on the Gateway, the Gateway will not be able to decrypt the join message and will not allow the Node to join the network.

All of these settings can be configured in the gateway via SmartWorx Hub, or via the Local Embedded Web Server that resides on the Gateway.

!	*The External MQTT Broker (enabled via the "MQTT Bridge" setting) is a 3rd party service: Advantech B+B SmartWorx does not provide this service. Any MQTT 3.1.1 compliant broker may be used.*

!	*For information on deploying MQTT in a secure manner we recommend that you refer to "MQTT and the NIST Cybersecurity Framework" which is available on the OASIS website (http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity).*

6.1 VIA SMARTWORX HUB

Navigate to the "Manage Devices" screen, then select your SmartSwarm-341 device.
From the "Manage Apps" section, select the "Wzzard" application.

6.2 VIA LOCAL WEBSERVER

Access the local webserver (e.g. via ETH0, 192.168.1.1) and navigate to the "Wzzard" tab using the top menu bar.

!	*The Default Password to access the local webserver is "5mart5warm". We recommend you change this on first use of the local webserver.*

SmartMesh IP

Network ID 1959

Join Key

MQTT Broker

☑ Broker Enable

Broker Port 1883

MQTT Bridge

☐ Bridge Enable

Bridge Port 1883

Bridge Address

User

Password

Client Identifier

Apply

6.3 CONFIGURATION PARAMETERS

The same configuration options are available from SmartWorx Hub as from the local webserver.

SmartMesh IP		
Configure parameters associated with the local WZZARD wireless sensor network		
Setting	**Valid Settings**	**Description**
Network ID	Integer value between 1 and 65534. Default Value: 1981	The Network ID of the SmartMesh IP Wzzard wireless sensor network. Only Wzzard nodes configured with this ID will be able to join the gateway's wireless sensor network. The default value is consistent with factory default value of the Network ID set for all Wzzard nodes. Multiple Wzzard networks may co-exist as long as they have different Network IDs, and each has a dedicated gateway.
Join Key	32 digit hexadecimal value (0-9, A-F) For security purposes, this value is not visible on-screen. To reset this value to it's factory default, type the word "default" into this	An optional additional security parameter. The Join Key is used to encrypt the initial join request issued by WZZARD nodes. If configured, then all WZZARD nodes connecting to the gateway must also be configured with the same Join Key. The default value is consistent with the factory default value of the Join Key set for all Wzzard nodes.

	field. Default Value: This is set in-factory to a secret value.	If left blank, the Gateway will use the Default Join key.

MQTT Broker
Configure access to the internal MQTT broker on the SmartSwarm gateway.

Setting	Valid Settings	Description
Broker Enable	Enable / Disable Default Value: Enabled	When enabled, the data received by the Gateway from the SmartMesh IP wireless sensor network will be available internally for consumption by the Node-RED MQTT node and the Node-RED Wzzard node. When disabled, this data will not be available to the Node-RED application on the Gateway. If the broker is enabled, it may be accessed via ETH0, using address: 192.168.1.1:1883 (assuming the default configuration) *Note that the broker may be accessed via the WAN interfaces also, but only if there's an available intranet connection on ETH1, or if there's a VPN tunnel running over the Cellular interface. In either case it is necessary to open the relevant firewall port in order to allow the inbound connection.*
Broker Port	Integer value between 1 and 65534. This is a Network Port number: some Network Ports are reserved for system use. Default Value: 1883	The local MQTT broker TCP port number. There is usually no reason to change this from the default value.

MQTT Bridge
Configure access to an external broker for data from WZZARD nodes.
NOTE: This option allows data received by the internal broker, such as that published by WZZARD nodes, to automatically be directed to an external broker, via the SmartSwarm Gateway.
A subscription is also set up to the 'set' topic to allow configuration of Wzzard nodes via the external broker.
This is an independent process from any broker access configured from within Node-RED

Setting	Valid Settings	Description
Bridge Enable	Enable / Disable Default Value: Disabled	If you wish to automatically re-publish the available data from the Wzzard wireless sensor network from this IoT Gateway to a remote (e.g. Cloud Based) MQTT broker, enable this feature. NOTE: This feature does not apply to MQTT data from other sources.
Bridge	Integer value between 1	The Port Number of the Remote MQTT Broker that you wish to publish

Port	and 65534. Default Value: 1883	the IoT Gateway's data to. MQTT Brokers use port 1883 by default. MQTT Brokers with TLS security use port 8883. Please set this value to the Port used by your Remote MQTT Broker.
Bridge Address	An IP Address or URL Default Value: NULL	This is the IP Address or URL of your Remote MQTT Broker. NOTE: A DNS server must be setup for URL entries to work.
User	Alphanumeric character string Default Value: NULL	This is the username you need to use as your access-credentials on your Remote MQTT Broker. This field is optional: if your remote MQTT broker requires this, it is required here also.
Password	Alphanumeric character string Default Value: NULL	This is the password you need to use as your access-credentials on your Remote MQTT Broker. This field is optional: if your remote MQTT broker requires this, it is required here also.
Client Identifier	Alphanumeric character string Default Value: NULL	Unique identifier, used by the Remote Broker, to uniquely identify each client. This field is optional and may be left blank. We recommend that you use a random number.

Table 4. WZZARD Interface and Broker Settings

!	*After the Gateway has successfully registered with SmartWorx Hub, any changes made on the local webserver on the Gateway will be automatically replicated and synchronized with SmartWorx Hub (and visa versa).*

6.4 THE SMARTMESH IP COMMAND LINE INTERFACE (CLI)

For diagnostics and troubleshooting purposes, there is a command-line interface available to the SmartMesh IP wireless sensor network.

This CLI interface provides access to the Gateway's Dust SmartMesh IP hardware interface.

The CLI may only be accessed via the Local Webserver: it is not accessable via SmartWorx Hub.

Open the local webserver (e.g. 192.168.1.1 on ETH0).

!	*In order to access the CLI, you must have the system firewall TCP port 8000 open on the physical interface that you're using.* *e.g. if you're using ETH0, with IP address 192.168.1.1, then navigate to Settings -> Firewall, and add TCP Port 8000 on ETH0 as an open port.*

Navigate to the Wzzard application tab.

You can access the CLI by clicking on the link-text that says "Click here to open Dust CLI".

The DUST CLI interface will present itself in another Browser Tab.

Click through to that Browser Tab.

```
Welcome to SmartSwarm6300189.
This is Dust CLI and you are connecting from 192.168.1.212

DustCLI ONLINE @ 26 January 2017 at 11:13:42 GMT

Baudrate= 9600

 $ help


 help
 help
 Commands:
    mlog
    mhwlog
    login
    logout
 >

$
```

There is a built-in help menu.

Type "help" at the command prompt (the $) to see the list of available options.

To access the CLI, type in "login viewer" at the command prompt.

6.4.1 BASIC FEATURES OF THE CLI

Some of the Basic Features that Advantech B+B SmartWorx may ask you to use, for diagnostics purposes, are:

CLI Function	Usage	Description
sm	sm	Show Motes. This function will list all of the currently connecting wireless sensor motes (i.e. Wzzards). The list will show the MAC addresses of the motes (Wzzards).
show	show <subcommand> e.g.	Show some more detailed information.
	show stat	Show network stats, including reliability, stability, latency.
	show mote 2	Show stats specific to mote 2 (Wzzard 2).
	show ver	Show version information for the SmartMesh IP Manager.
	show config	Show configuration information for current Mesh network.

7. NODE-RED APPLICATIONS

Node-RED is a tool for wiring together hardware devices, APIs and online services, based on a simple to learn, graphical UI. There are many free external resources explaining how to program using Node-RED and this document will therefore not go into this detail. Some useful external resources can be found at:

http://Node-RED.org/docs/getting-started/ (ignore the sections on installing, upgrading and running Node-RED as these elements are already taken care of by the SmartSwarm system).

http://Node-REDguide.com/

The 'function' node within Node-RED allows users to create their own node functionality by embedding JavaScript code within the function. A general description of the various JavaScript methods can be found at

https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Methods_Index

NOTE: Due to the resource constrained nature of the SmartSwarm gateway (see later in this section), not all of the methods described in the above document exist in the gateway.

This document does however provide information about specific B+B SmartWorx nodes added to the standard palette, and also about how to access Node-RED on a SmartSwarm device, both via a local connection, and remotely via SmartWorx Hub.

The following acronyms are used:

> LEWS = Local Embedded Webserver, accessed by entering the gateways IP address into a connected browser. (eg 192.168.1.1 on the LAN port (ETH0) if system defaults have not been changed.)

> SWH - = SmartWorx Hub, the remote configuration and management platform for SmartSwarm devices and Routers

7.1 B+B SMARTWORX IMPLEMENTATION

There are a number of things to be aware of and keep in mind regarding the Node-RED implementation on the SmartSwarm 341:

7.1.1 RESOURCE CONSTRAINTS

Node-RED runs in a container within the SmartSwarm 341. This means that it does not interact directly with the SmartSwarm 341 system hardware and firmware, but instead operates within the container and via API links within it. This offers significant protection for the user against user applications being able to disable the core gateway operation, either accidentally or maliciously. It must be understood, however, that the SmartSwarm 341 is resource constrained in terms of available RAM and flash storage, and care should be taken with any functions which will use this up, for example logging data to files without a mechanism to limit their size.

7.1.2 B+B SMARTWORX CUSTOM NODES AND NECESSARY CONVENTIONS

7.1.2.1 WZZARD NODE

Two custom Node-RED Wzzard nodes are provided on the default palette. The first of these passes messages received from the Wzzard nodes through to the flow (in msg.payload), whilst the second allows flows to write data to Wzzard devices. On first use, the node needs to be configured with the port number that the local Wzzard data is interfaced via. The default value for this is 1883, and there should be no need to change this.

If you need to subscribe to Wzzard information from an external broker, for example if coming from a different site, then you should use the standard Node-RED MQTT input and output nodes, and not the custom Node-RED Wzzard nodes.

⚠️	For details of the Wzzard topic space and payload conventions, please refer to the 'MQTT Topics and JSON Data Format' document, available from our website at: http://advantech-bb.com/wp-content/uploads/2016/03/MQTT_Topics_and_JSON_Data_Format_R3_User_Manual_0316.pdf

7.1.2.2 FILE NODES

Due to the containerization of the Node-RED application, any filename used should be preceded by '/' if it is to be stored in flash, or /tmp/ if it is to be stored in RAM. Files stored in RAM will not persist over a power fail, but will be quicker in operation, and will not take space that could otherwise be used for flows.
Further nesting of directories is possible, for example /myDirectory/myFile will create a directory (myDirectory) on flash and store the file (myFile) in that directory.

⚠	*Note that it is possible for you to store files to an inserted SD Card (by writing to **/mnt/sd/***<filename>*), or to an inserted USB storage device (by writing to to **/mnt/usb/***<filename>*).* *The USB storage device, or SD Card, must be inserted before the Gateway is powered up.*

7.1.3 ADDING NODES TO THE DEFAULT PALETTE

The default palette of nodes is installed, curated and supported by B+B SmartWorx. It is, however, still possible for users to add further nodes from the public library at http://flows.Node-RED.org either via the Local Embedded Webserver (LEWS) or remotely from SmartWorx Hub (SWH), subject to the following:

- The gateway must have an open internet connection in order to fetch the required nodes.
- Additional nodes are added at the user's risk. B+B SmartWorx does not warrant that any third party nodes will install or work correctly within the Node-RED implementation on the gateway.
- Due to the nature of the NPM packet installer used to manage nodes, a number of code libraries are required to fully support the various calls that NPM might make, and it is impractical to include all of these libraries within the core SmartSwarm 341 image due to the resource constrained nature of the device highlighted above. Some third party nodes will therefore simply fail to load as their underlying dependencies will not be supported.
- B+B SmartWorx has no control over third party node implementations, and it is possible that these may be updated at any time. An updated node may operate differently to one previously installed and may not be backwards compatible. It is therefore strongly recommended that users keep details of the specific version numbers of any nodes they install, so that these same versions can be used in future deployments. To specify a particular version of the node, use the format node_name@x.y.z, where node_name is the name of the node given in the public flows library, and x.y.z represents the version number of the version you wish to download. Note that, when loading previous versions of nodes, it may be necessary to perform a gateway reset before they will appear in the palette.
- B+B SmartWorx tests and releases known stable versions of the Node-RED core system. As such, it is possible, even likely, that at any point in time, the version of Node-RED installed in a SmartSwarm gateway may be some iterations behind the publicly released version.

7.1.3.1 ADDING NODES VIA LEWS

Navigate to the Node-RED tab on the menu bar. Enter the full name of the node you wish to install from the public library (http://flows.Node-RED.org). Select the 'install' action and click on the Execute button. To uninstall nodes, repeat the above process, but select the 'uninstall' action. Note the comments in 'Adding Nodes to the Default Palette' above.
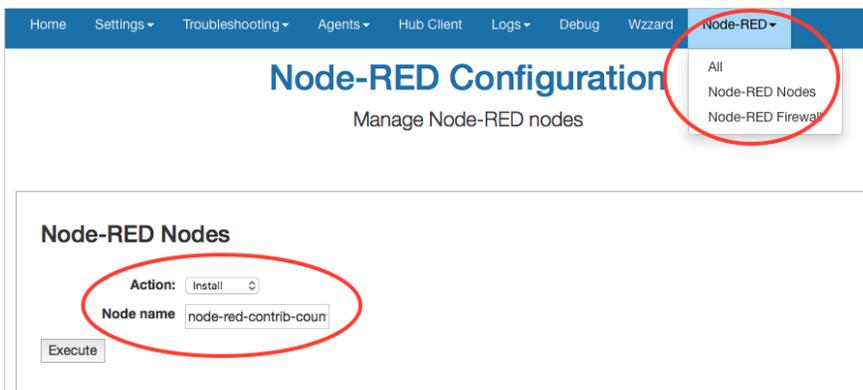
7.1.3.2 ADDING NODES VIA SWH

Navigate to the manage device window for the device in question and click on the Node-RED application. Enter the name of the desired node in the node field of the Add or Remove nodes pane, and click on 'Apply Changes'. To uninstall, repeat the above process but tick the "Uninstall" check box. Note the comments in 'Adding Nodes to the Default Palette' above.

7.2 ACCESS TO NODE-RED

For security purposes, access to the Node-RED editor and dashboards is disabled by default, and users must open the Node-RED firewall port 1880 via either LEWS or SWH before they can gain access to Node-RED. Once the firewall port has been opened, the Node-RED editor can be accessed from a connected browser using the URL <device IP address>:1880, and any dashboards created can be found at <device IP address>:1880/ui. For example, assuming no changes have been made to the default settings of ETH0, then connecting a PC directly to ETH0 via an Ethernet cable and browsing to '192.168.1.1:1880' will access the Node-RED main screen.

Similarly, any local dashboards created using Node-RED can be accessed by adding the /ui extension to this address, so in the previous example, would appear at '192.168.1.1:1880/ui'.

7.2.1 CHANGING THE FIREWALL SETTINGS VIA LEWS

Select the Node-RED dropdown in the menu bar and choose the Node-RED Firewall option. Click on the '+ Port' link and set the protocol to TCP and the Port to 1880. Click on 'Save' and the port should appear in the table of enabled ports.
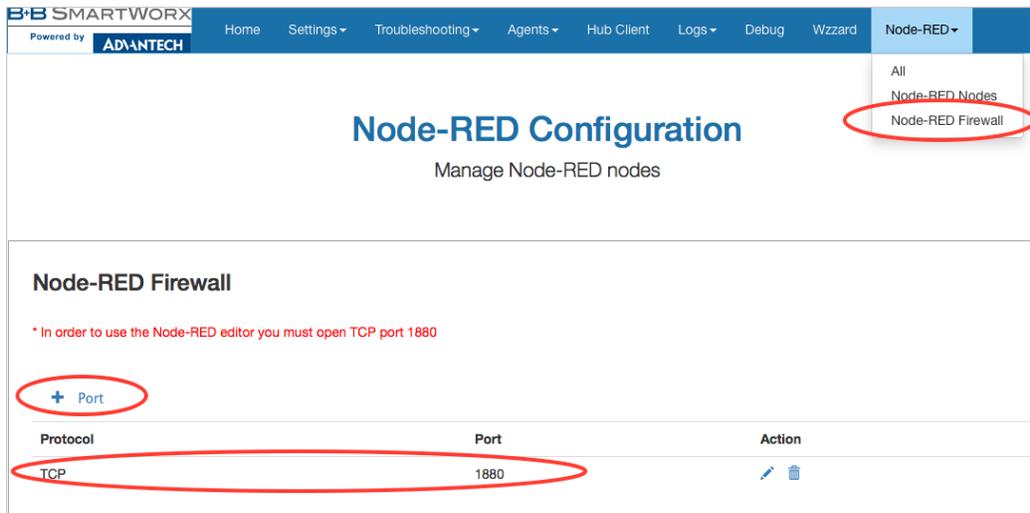
7.2.2 CHANGING THE FIREWALL SETTINGS VIA SWH

Navigate to the main management screen for the gateway in question, and click on the Node-RED link in the list of installed Apps. Select the 'Firewall' option from the menu in the top left of the resulting page. Click on the 'Add Rule' link and set the port to 1880. Finally, click on the 'Apply changes' button to deploy to the remote gateway.

Note in either case, it is only necessary to open the port in the Node-RED firewall. The corresponding entry in the system firewall will be automatically made.
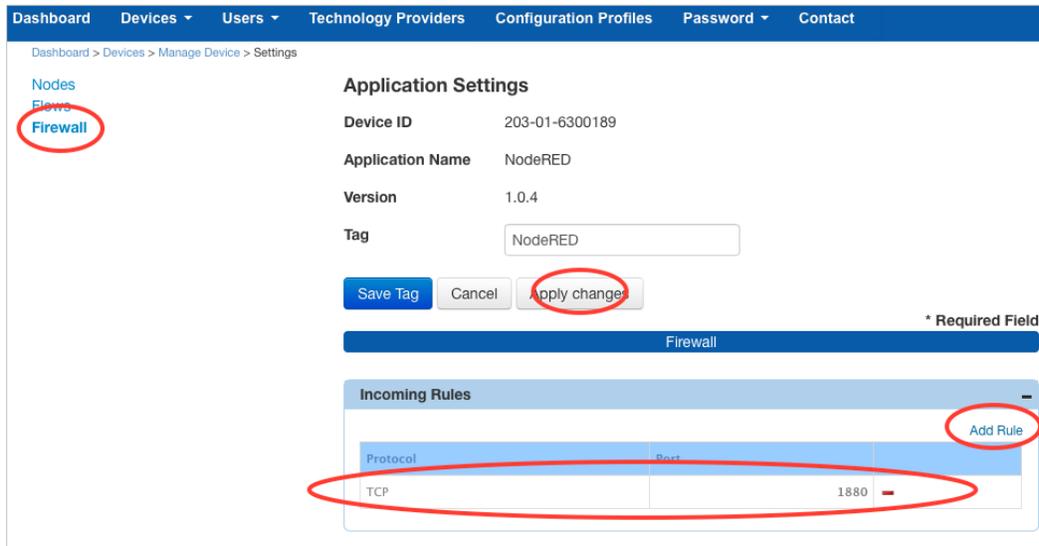
7.2.3 OPENING OTHER FIREWALL PORTS

Depending upon the nature of the user Node-RED flows developed, it may be necessary for other firewall ports to be open in order to establish correct operation. Where the connection is outbound (which is normally the case) then the system will open the necessary ports automatically. Should any nodes be deployed which require the ability for external devices and services to connect via an inbound connection, it will be necessary to explicitly open the appropriate ports in the Node-RED firewall. Again, opening a port via the Node-RED firewall inherently creates a corresponding port to be opened on all external interfaces in the system firewall. If more restricted access is required (for example, a user may be happy for an inbound connection from a device on the local LAN, but not want the same connection to be possible via the WAN), then the system firewall entry can be modified accordingly afterwards.

7.3 NODE-RED HINTS & TIPS

7.3.1 DEVELOP ON THE GATEWAY

Because of the implementation features outlined above, it is strongly advised that Node-RED flows are developed on a target gateway, rather than developing offline on a PC and then transferring the flows. A Node-RED environment downloaded to a PC is likely to differ from the version loaded on the gateway, both in terms of the version of the core Node-RED implementation and node versions, but also potentially in the underlying node-js dependencies.

7.3.2 GLOBAL VARIABLES

When writing flows, it is often useful for an event in one part of the flow to affect, or to be combined with other parts. This can often be achieved by using global variables. A global variable is created by prefixing the variable name with 'context.global.', so for example 'context.global.variableName'. This variable can be referenced anywhere in the flow.

7.3.3 INITIALIZATION

Often, as a flow develops, it is important to be able to set initial values of parameters, or to create other setup conditions. It is a good idea for the first element entered during the creation of any new flow is an 'inject' node, set to run at startup and not repeat, connected to a function node in which any initialization is performed.
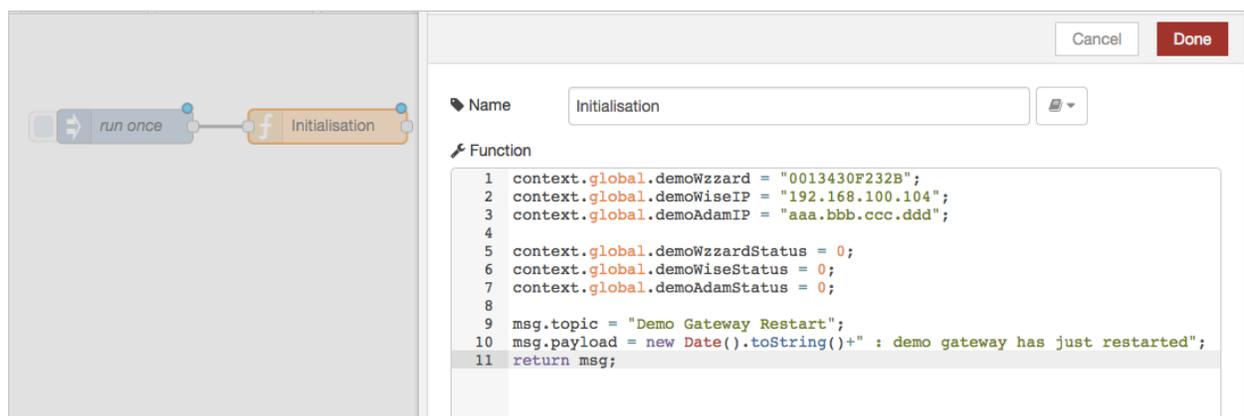
For example, the above code initializes some global variables for use elsewhere within the flows and creates a message topic and string indicating a gateway restart which can be connected to downstream messaging nodes, eg. to send an email on restart.

7.3.4 ALIASING WZZARD ID

Messages coming from Wzzard nodes include the MAC ID of the node within the topic space so that there is a unique identifier for the node. It is useful to alias this immediately upon receipt by the gateway into something more meaningful, for example 'conference room', or 'shutdown valve 1'. This means that downstream code can use the alias and, should the physical node need replacing in the future, only the alias needs to be changed for the code to continue working. There are a number of ways this could be achieved. As one example, in the above initialization code, the variable context.global.demoWzzard is set to the MAC ID of a particular node – "0013430F232B".
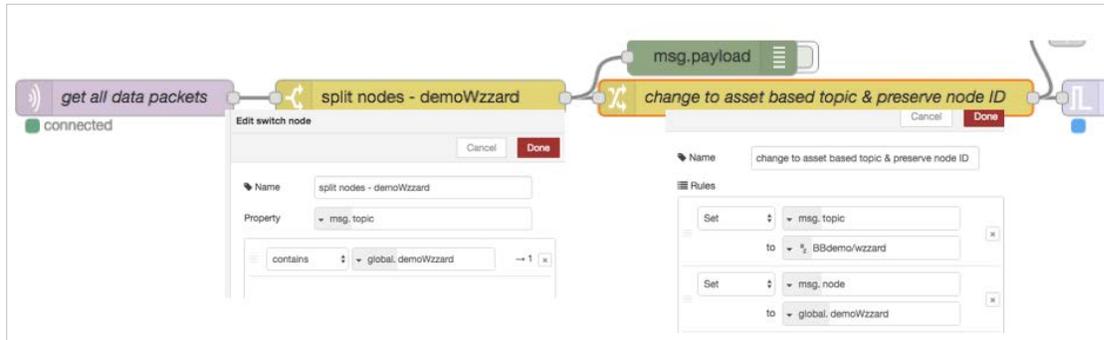
In another part of the flow, once the raw data is recovered, a 'switch' function is used to look for an incoming MAC ID equal to the value in context.global.demoWzzard, and to pass the packet on to output one if a match is found. This output is wired to a 'change' node, which changes the topic associated with the message to BBdemo/Wzzard, and adds a new field into the payload called 'node' which is set to the MAC ID of the physical node. Further elements in the flow can now use the topic identifier 'BBdemo/Wzzard', and should the physical node be changed in the future, then all that needs to happen is the initial declaration in the initialization section needs to have the new MAC ID substituted.

7.3.5 REMOVING LINES FROM FILES TO MAINTAIN LENGTH

As indicated above, due to the limited resources available within the gateway, care must be taken when creating files that their length will not grow indefinitely. One method to achieve this would be to turn the file into a circular buffer, such that for every new line added to the bottom of the file, an old line from the top of the file is removed. Adding the new line is easy, as the 'file' function allows you to simply append data to an existing file. Removing the first line can be achieved by reading a file into a function block, modifying the contents then writing back to the file.
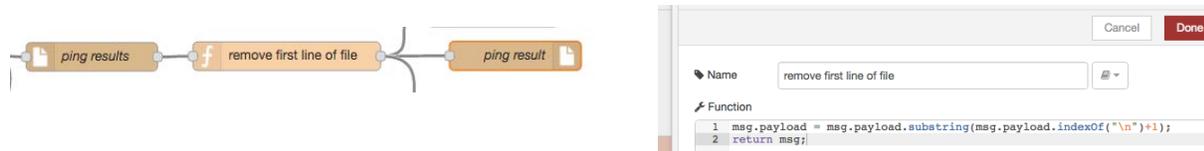
The code needed within the function is shown in the example above.

NOTE: It is also possible to use the output of a UI chart node to create a ring buffer of values with timestamps.

7.3.6 CALCULATING THE LNGTH OF FILES (NUMBER OF LINES)

Of course, you will need to be able to determine the number of lines in a file to decide when to start truncating the top. This can be achieved using an 'exec' node as follows:
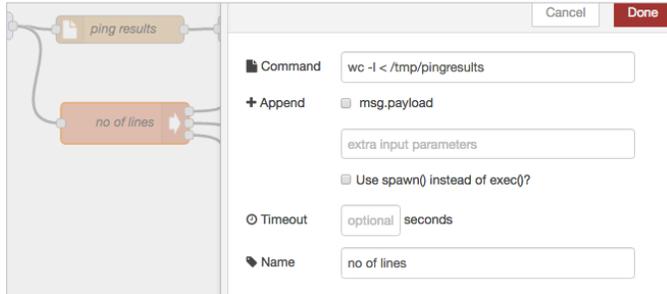
Note that the '-I' element uses a lower case L.

7.3.7 SUBSRIBE ONCE AND FILTER IN NODE-RED

When using input nodes such as Wzzard, MQTT, etc., it should be remembered that each node essentially creates an IP connection in the background. Whilst it would be possible to use multiple input nodes, each subscribing to very specific data topics in order to trigger the downstream flows, this is wasteful of resources and can slow down the gateway operation considerably. It is better to use fewer subscriptions with wildcards and to filter out the specific items of interest within a flow.

7.3.8 NODE_RED DOESN'T "SCAN"

The order of execution of Node-RED nodes does not have any relationship with their order on the page (ie all things being equal, Node-RED flows do NOT execute left to right, top to bottom). In flows where race conditions can exist therefore, it is recommended that delay nodes are introduced to ensure the desired precedence of execution is achieved.

7.4 GETTING DATA FROM WZZARD, ADAM, AND WISE UNITS USING NODE-RED

7.4.1 WZZARD

1. Navigate to the Node-RED home screen and drag a Wzzard input node onto the canvas. Drag a debug node onto the canvas and connect the two together.

2. Double click on the Wzzard input node. Click on the pencil button in the resulting screen to configure the local interface. You will only need to do this once.
3. In the resulting screen, unless you have been advised differently by B+B SmartWorx, simply click the 'Add' button to create the required connection on port 1883.
4. Select the topic to which you want to subscribe. Wzzard nodes publish sensor data on the topic 'BB/<mac_id>/data', where <mac_id> is the 12 digit number printed on the Wzzard node label beginning with 001343.
5. To get all sensor data from all connected nodes, subscribe using the '+' wildcard in place of <mac_id> - ('BB/+/data').

6. To get all data from all nodes subscribe using the '#' wildcard in place of everything after the 'BB' ('BB/#')
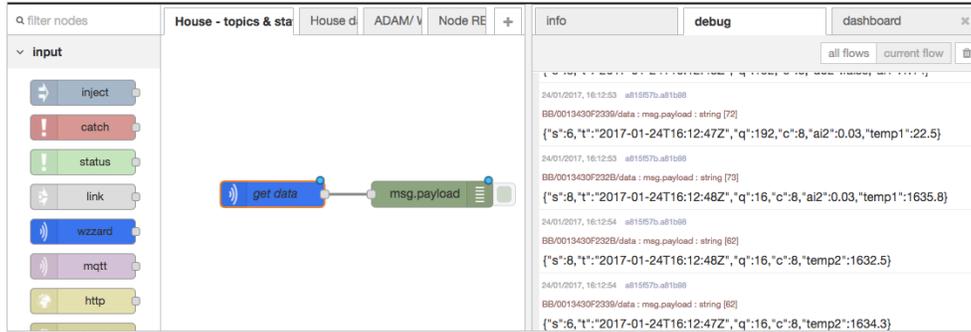
7. You should now see the data being published by the selected, connected nodes appearing in the 'debug' tab on the right hand side of the screen. Note that these appear as TEXT in the resulting output from the MQTT input node and therefore may need to be passed through a JSON node before further processing in Node-RED.

8. Details of the available topics and payloads from a WZZARD node can be found in the document at: http://advantech-bb.com/wp-content/uploads/2016/03/MQTT_Topics_and_JSON_Data_Format_R3_User_Manual_0316.pdf

7.4.2 ADAM AND WISE

There are two options for the recovery of data from Advantech ADAM & WISE units, the selection between them basically being governed by what protocols the particular ADAM/WISE unit supports. If the device supports REST, then the recommended method is to use the 'http request' node, and perform a REST query:

7.4.2.1 VIA REST
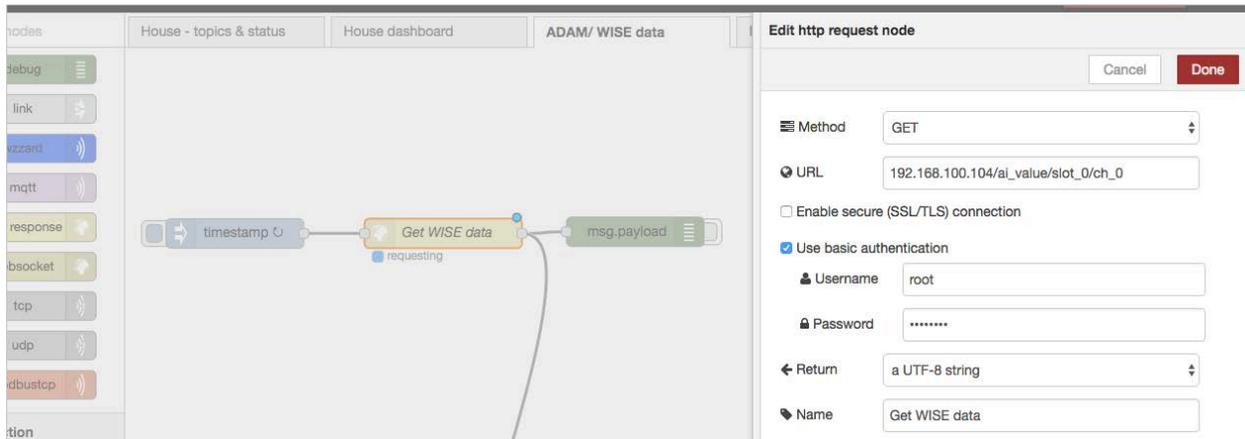
Note that the above example is given for recovering analogue input data from a WISE4000 device. The IP address specified in the URL is the IP address of the WISE unit from which the data is to be recovered. The URL required for an ADAM differs slightly in format. Refer to the appropriate device user manual for detail of the URL format for that device, and the alternative URLs to recover other data types. Note that it is necessary to trigger the read operation and, in the above example, this is achieved using an 'inject' node and setting it to repeat at the desired interval.

It is also possible to write data to WISE and ADAM units using the http request node and changing the method to 'POST'.

7.4.2.2 VIA MODBUS TCP

If the target device does not support REST, then it is possible to extract data using Modbus TCP.

In order to do this, it is first necessary to download a Modbus TCP node and install it into the system palette. See the section on 'Adding nodes to the default palette' above. B+B SmartWorx has tested and verified operation of the 'Node-RED-contrib-modbustcp' node for this operation.

> ⚠️ *Note that the latest version of this node has dependencies not yet supported on the SmartSwarm 341, and it is therefore necessary to download an earlier version 0.1.0. To do this, specify the node name as 'Node-RED-contrib-modbustcp@0.1.0' when installing the node.*

Again, the IP address used in the 'server' entry is that of the target device (in the above example an ADAM). The FC field should be adjusted to match the type of data you wish to recover, and the address field counts from zero starting at the base address for that number type. In the above example, therefore, the operation will result in a read of coils 00,001 to 00,016, once every 5 seconds.

7.4.3 SMARTSWARM 351

SmartSwarm 351 is natively MQTT compatible. In the SmartSwarm 351 unit, set the target broker to match the local network address of the SmartSwarm 341 device. For example, assuming the default configuration in the SmartSwarm 341, and a connection via ETH0, then the broker address in the SmartSwarm 351 should be set to 192.168.1.1.

In Node-RED, an MQTT input node can be used in a similar fashion to that detailed in Section 6.4.1 above to access the information published by the SmartSwarm 351. The 'topic' definition in the Node-RED MQTT input block will need to be set to match the topic schema configured within the SmartSwarm 351, and may use the standard wildcards ('+' to accept any value in an individual field within the topic space; '#' to accept any value in a field and all lower order fields). Note that the settings for broker bridging set in the SmartSwarm 341 will also apply to data received from the SmartSwarm 351, so if bridging is enabled, all data from the SmartSwarm 351 will also be passed to the external bridged broker.

The SmartSwarm 341 also automatically routes non-local addresses to the active WAN/cellular uplink, and so if the 351 is configured to publish data to an external broker (rather than to the broker in the 341), this traffic will simply be routed transparently through the 341, and the data will not be available to Node-RED unless an MQTT node is used to subscribe to the same external broker.

8. OTHER DOCUMENTATION

Document Title	Where?
Wzzard MQTT Topics and JSON Data Format	http://advantech-bb.com/wp-content/uploads/2016/03/MQTT_Topics_and_JSON_Data_Format_R3_User_Manual_0316.pdf
Wzzard Sensing Platform Network Planning & Installation	http://advantech-bb.com/wp-content/uploads/2016/03/Wzzard_Network_Planning_and_Installation_Application_Note_R2_2515.pdf
Wzzard Sensing Platform Bluetooth Application Manual	http://advantech-bb.com/wp-content/uploads/2016/03/Wzzard_Bluetooth_App_R2_User_Manual_2515.pdf
Node-RED Community Pages	http://Node-RED.org
Node-RED Node and Flow Library	http://flows.Node-RED.org/
Node-RED Programming Guide	http://Node-REDguide.com/
MQTT and the NIST Cybersecurity Framework"	http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html
JavaScript Methods Index	https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Methods_Index
SmartWorx Hub User Manual	https://hub.bb-smartworx.com/Login/Help?HelpFile=bbdms_help.pdf
OpenVPN Documentation	https://openvpn.net/index.php/open-source/documentation/howto.html#client

Table 6. Other Documentation

9. APPENDIX 1 - HARDWARE RATINGS

9.1 ENVIRONMENTAL

IoT Gateway SmartSwarm 300 series		
Temperature Range	Operating Storage	-40 to +75 deg.C -40 to +85 deg.C
Cold Start	-35 deg. C -40 deg. C	Data transfers via mobile network are available immediately Data transfers via mobile network are available approximately in five minutes after the start of the device. Everything else is functional immediately.
Humidity	Operating Storage	0 to 95 % relative humidity, non-condensing. 0 to 95 % relative humidity, non-condensing.
Altitude	Operating	2000 m / 70 kPa
Degree of Protection		IP42
Supply Voltage		10 to 60 V DC
Consumption	Idle Average Peak	2,5 W 4W 11 W
Dimensions		55x97x125 mm (DIN 35 mm)
Weight		Approximately 400 g (depends on interface)
Antenna Connectors		3 x SMA – 50 Ohm (cellular version) 1 x SMA – 50 Ohm (wired version)
User Interface	2x ETH USB I/O Wzzard Radio	Ethernet (10/100 Mbit/s) USB 2.0 (not currently supported) 6-pin panel socket (not currently supported) via SMA

Table 7. Environmental Specifications

9.2 TYPE TESTS

Phenomena	Test	Description	Test Levels
ESD	EN 61000-4-2	Enclosure contact Enclosure air	± 6 kV (crit. A) ± 8 kV (crit. A)
RF Field AM Modulated	IEC 61000-4-3	Enclosure	20 V/m (crit. A) (80 – 2700 MHz)
Fast Transient	EN 61000-4-4	Signal ports Power ports Ethernet ports	± 2 kV (crit. A) ± 2 kV (crit. A) ± 2 kV (crit. A)
Surge	EN 61000-4-5	Ethernet ports Power ports I/O ports	± 2 kV (crit. B), shielded cable ± 0,5 kV (crit. B) ±1kV.LtoL(crit. A) ±2kV,LtoGND(crit. A)
RF Conducted	EN 61000-4-6	All ports	10 V/m (crit. A) (0,15 – 80 MHz)
Radiated Emission	EN 55022	Enclosure	Class B
Conducted Emission	EN 55022	DC power ports Ethernet ports	Class B Class B
Power Frequency Magnetic Field	EN 61000-4-8	Enclosure	160 A/m (crit. A)
Dry Heat	EN 60068-2-2	+75 ∘C, 40 % rel. humidity	
Cold	EN 60068-2-1	-40 ∘C	
Dump Heat	EN 60068-2-78	95 % rel. humidity (+40 ∘C)	

Table 8. Type Tests

9.3 CELLULAR MODULE

LTE Module for EMEA	
LTE Parameters	Bit rate 100 Mbps (DL) / 50 Mbps (UL) 3GPP rel. 8 standard Supported bandwidths: 5 MHz, 10 MHz, 20 MHz Supported frequencies: 800 / 900 / 1800 / 2100 / 2600 MHz
HSPA+ Parameters	Bit rate 21,1 Mbps (DL) / 5,76 Mbps (UL) 3GPP rel. 7 standard UE CAT. 1 to 6, 8, 10, 12, 14 3GPP data compression Supported frequencies: 900 / 2100 MHz
UMTS Parameters	PS bit rate 384 kbps (DL) / 384 kbps (UL) CS bit rate 64 kbps (DL) / 64 kbps (UL) W-CDMA FDD standard Supported frequencies: 900 / 2100 MHz
GPRS/EDGE Parameters	Bit rate 237 kbps (DL) / 59,2 kbps (UL) GPRS multislot class 10, CS 1 to 4 EDGE multislot class 12, CS 1 to 4, MCS 1 to 9 Supported frequencies: 900 / 1800 / 1900 MHz
Supported GPRS/EDGE Power Classes	EGSM 900: Class 4 (33 dBm) GSM 1800/1900: Class 1 (30 dBm) EDGE 900: Class E2 (27 dBm) EDGE 1800/1900: Class E2 (26 dBm)

Table 9. Cellular Module

9.4 WZZARD RADIO MODULE

SMARTMESH IP RADIO -- 802.15.4E -- 2.4 GHZ		
Number of Channels	15	
Channel Separation	5 MHz	
Channel Clear Frequency	2405 + 5*(k-11) MHz	
Modulation	IEEE 802.15.4 Direct Sequence Spread Spectrum (DSSS)	
Raw Data Rate	250 kbps	
Range	Indoor	100 m
25 °C, 50% RH, +2dBi Omni-Directional	Outdoor	300 m
Antenna, Antenna 2 m	Free Space	1200 m
Receiver Sensitivity	Packet Data Error Rate (PER) = 1%	-93 dBm
Receiver Sensitivity	PER = 50%	-95 dBm
Output Power -Delivered to a 50 Ω load	High Calibration Setting	8 dBm
	Low Calibration Setting	0 dBm

Table 10. Wzzard Radio Module

9.5 OTHER TECHNICAL PARAMETERS

Other Technical Parameters	
CPU Power	2 DMIPS per MHz
Flash Memory	256 MB
RAM	512 MB
M-RAM	128 kB

Table 11. Other Technical Parameters

10. APPENDIX 2 – GENERAL SETTINGS

For every SmartSwarm device, there are some general settings and options that are available to you.

10.1 NETWORK

The Network settings enable you to configure operation of the ETH ports and the Cellular interface of your device.

By default, ETH0 has a static IP address of 192.168.1.1.

By default, ETH0 runs a DHCP server, which serves a DHCP address to a connecting device. This means that you should configure your desktop/laptop to take an IP address automatically when you connect it to ETH0 of the SmartSwarm device.

There is a local web-server, for local configuration purposes, served on ETH0 (http://192.168.1.1).

We recommend that you do not change the ETH0 default settings.

By default, ETH1 runs as a DHCP client.

By default, the cellular interface is not configured. But Note that you may have previously configured the Cellular Interface locally on your device.

!	*Changing network settings from SmartWorx Hub can result in breaking the working secure connection your device has to SmartWorx Hub.* *Please ensure you are applying appropriate network settings to your device, or that you have a contingency plan (e.g. local device access is available) in the event that you unintentionally cause the secure connection to drop.*

10.2 DHCP

The DHCP settings apply only to the DHCP server that runs on ETH0.

⚠	*At the time of writing, it is not possible to turn off the DHCP server that runs on ETH0. Please be careful not to connect ETH0 of the device into a LAN port that is also serving DHCP addresses.*

10.3 OPENVPN

You may configure up to two OpenVPN tunnels to run on your device.

This may be useful if you need the ability to reach the local-web-server on the device -- remotely, for example.

The user interface enables you to configure an OpenVPN tunnel to an OpenVPN server.

Before you begin to use an OpenVPN service, we recommend that you are familiar with the OpenVPN documentation, which is available here:

https://openvpn.net/index.php/open-source/documentation/howto.html#client

OpenVPN	
Enable Tunnel	Enable or Disable this tunnel interface. Disabled by default.
Protocol	UDP or TCP (TCP is default)
VPN Server (IP Port)	The IP Address of the OpenVPN Server, and the port the Server is listening on. This must be entered as a single string, like in this example: `148.251.6.41 1194` NOTE the separator between the IP address and port number is a <space> and not the more usual ':'.
Local Port	The local Port the device will (optionally) use to bind to the OpenVPN service on the server
Verbosity	Enable the debug-message level you want on your Device. The bigger the number, the more debug messages are written into the OpenVPN message log. We recommend that you use 0 here.
LZO Compression	Enable or Disable compression on the OpenVPN client-server connection. If compression is enabled on the server it must also be enabled on the device. Enabled by default.
Client Mode	Enabled or Disabled. Enabled by default. Must be enabled if the Tunnel is enabled.
...ate	The Certification Authority's certificate, which is used to generate the Client Certificate from the Certification Request generated by the Private Key. This must be the same CA certificate (or be in the chain-of-trust) that is used by the Server. The CA Certificate is the Server's Public Key.
Client Certificate	The Client Certificate is the certificate created by the CA for the Client (Device), from the Certificate Request that was sent to the CA. The Client Certificate is the Device's Public Key.
Key	The Private Key (for the Device) that is used to generate the Certification Request. The Certification Request is what you send to the Certification Authority.

Table 12. OpenVPN Fields

When OpenVPN feature is enabled, the Client Key, the Client Certificate, and the CA Certificate will be sent to the Device.

When the OpenVPN feature is disabled, all of these items will be removed from the Device.

So how do you create your Key, how do you get your Client Certificate, and how do you know what the CA certificate is?

You can generate your own private key (intended to be the Private Key of the Device).

Please consult "openssl" documentation, and please refer to your OpenVPN server's documentation.

Here's an example of how to create a private key. (There are many options that you can apply here; we're using one option for illustration purposes only):

```
$ openssl genrsa –out MyDevicePrivate.key 2048
```

You now have the "Key" required.

Next, you need to generate a Certificate Signing Request. Here's an example (again, this is only one of many possible examples):

```
$ openssl req –new –sha256 –key MyDevicePrivate.key –out
CertificateRequest.csr

Country Name: <your 2 letter country code>
State or Province Name: <your province name>
Locality Name: <your location name>
Organization Name: <your organization name>
Organizational Unit Name: <your team name>
Common Name: <your domain name> (e.g. "devid6500003")
email: <your email>
Challenge password: <blank, press enter>
Optional company name: <blank, press enter>
```

The output from this sequence is a file named "CertificateRequest.csr".
Now, you must send this Certificate Signing Request to your Certificate Authority for signing.

The CA that signs this certificate must be the same CA, or in the chain-of-trust of the CA, that has signed the Server's Certificate.

You will receive back your signed certificate (this is the Client Certificate that you require), along with the server's CA certificate (this is the CA Certificate that you require).

10.4 NTP CLIENT

You may specify up to 4 network time protocol servers for this Device.

10.5 FIREWALL

By default, all incoming ports on the SmartSwarm 341 are blocked except for the following:

Interface	DHCP server	ICMP (ping)	HTTP	SSH	Forward to Internet
ETH0	✔	✔	✔	✔	
ETH1		✔	✔	✔	✔
Cellular					✔
Tunnel*		✔	✔	✔	

Table 5. Firewall Rules

Additional inbound ports must normally be explicitly enabled by the user via the firewall configuration.

To enable an inbound port, click on the 'add rule' link and enter the desired port number in the new line which appears in the table. Select other fields as required from the drop down options. When you have completed the configuration, click on 'Apply changes' to send the configuration to the gateway.

To disable an inbound port, click on the red '-' symbol on the right hand side of the table entry. Click on 'Apply changes' to send to the gateway.

Note that some Firewall exception rules will be applied automatically, depending upon whether you have configured OpenVPN. For example, the *Tunnel interface will only exist when you have enabled an OpenVPN tunnel.

⚠	*Firewall Scope is indicated by the "Scope" Column.* *Because the Node-RED Application runs within a secure container, firewall ports that are required by the Node-RED run-time environment MUST BE OPENED FROM WITHIN THE NODE-RED APPLICATION.* *Firewall ports that have been opened by the Node-RED Application will be indicated as "Node-RED" in the Scope column.*

11. APPENDIX 3 – DIAGNOSTICS AND TROUBLESHOOTING

There is a local web-server interface on ETH0 of the SmartSwarm device.

This interface is intended to be used for two purposes:
   a) Configure the device's outbound (WAN) connectivity (using either the Cellular interface, or ETH1).
   b) Diagnosing and Troubleshooting problems, in collaboration with the Advantech B+B SmartWorx technical support team.

11.1 THE LOCAL WEB INTERFACE

There is an embedded web-server which provides a local interface on ETH0.

By default, ETH0 of the device is configured with IP address 192.168.1.1, subnet 255.255.255.0.

ETH0 is configured as a DHCP server: This means that if you physically connect ETH0 to your laptop/desktop the device will automatically serve an IP address of 192.168.1.x to your laptop/desktop.

The local web interface looks like this:
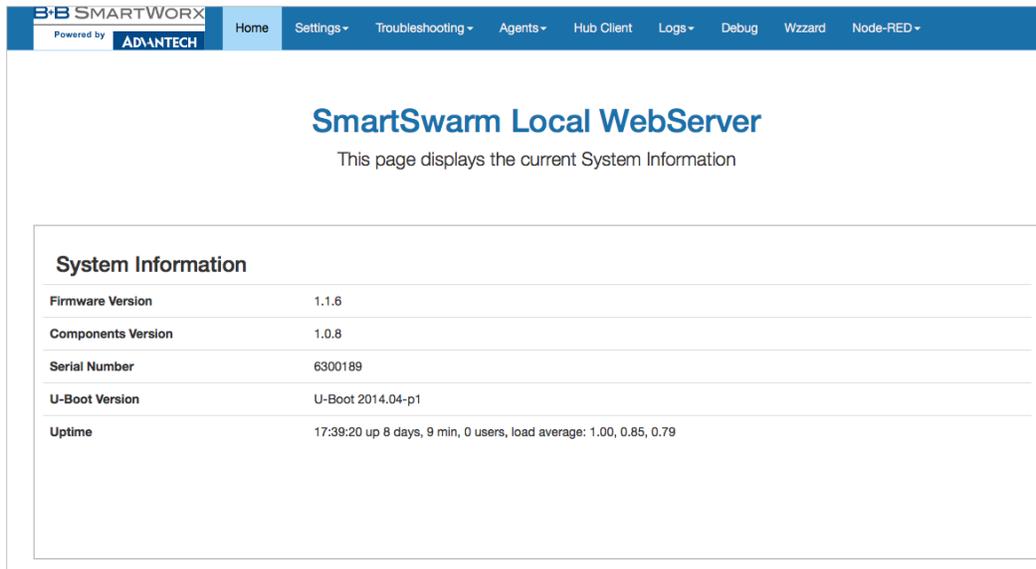
The following tabs are available: Home; Settings; Troubleshooting; Agents; Hub Client; Cellular (if this is a cellular device); Logs; Debug; Wzzard and Node-RED.

11.1.1 HOME
From the Home tab, you can see some important information about your SmartSwarm device:
   ● Firmware Version
   ● Components Version
   ● Serial Number
   ● U-Boot Version
   ● Device Uptime, Connected Users, Load Average

11.1.2 SETTINGS

The Settings tab enables you to configure your connectivity ports:
- Cellular
- ETH0
- ETH1
- Change Password
- System Firewall

If you intend to use the Cellular interface for your outbound connection, you must enter your APN and network credentials here.

By default, ETH0 will operate as a LAN interface only and ETH1 will expect to be served an address from a DHCP server.

We assume that the DHCP server that serves this address will also provide a route to the internet. If this is not the case, you may need to re-configure your ETH1 interface.

You can change your default embedded-web-server authentication password here.

The System Firewall that is available from this interface works in the same way as the System Firewall that is offered from SmartWorx Hub (please refer to the SmartWorx Hub chapter).

11.1.3 TROUBLESHOOTING

The Troubleshooting tab gives you the ability to see the actual internal device status of a number of key interfaces, processes and settings.

This interface gives you a drop-down list of commands that you can trigger, so that you can gather some potentially valuable run-time information. In the case your device is not performing as you think it should.

When you're working with the Advantech B+B SmartWorx technical support engineer, he may ask you for some of the details that are available from this Tab.

In most cases, you must select the command from the drop-down list, then hit the '**Execute**' button.

This will execute the command on the device, and feedback the results to the browser window.
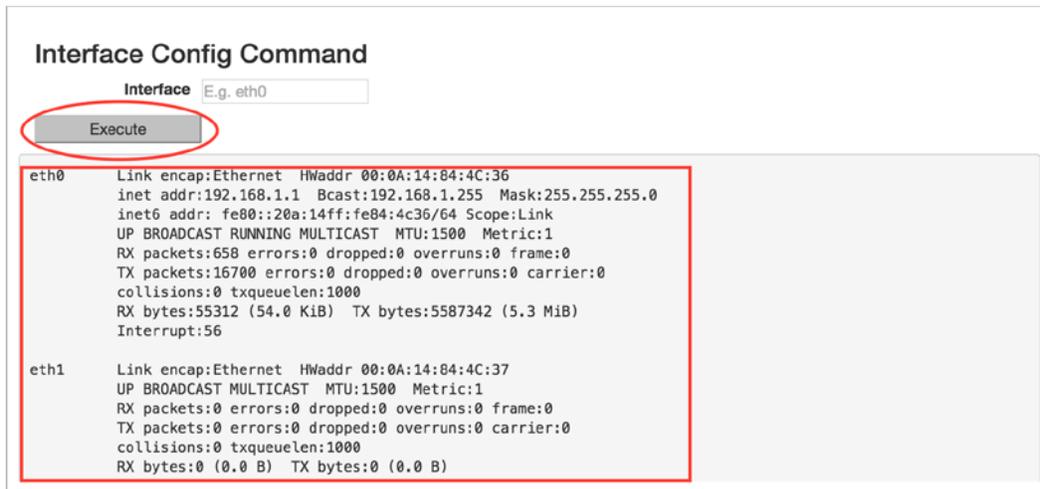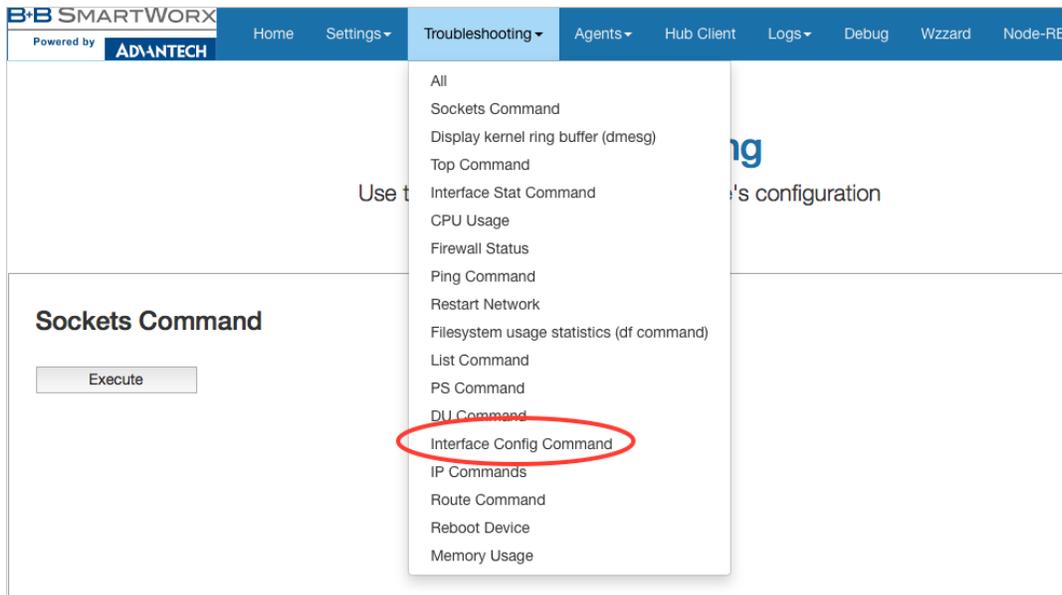
11.1.4 HUB CLIENT

Using this tab, you can change the default SmartWorx Hub Server instance that your device connects.
By default, your device will connect to hub.bb-smartworx.com using https on port 443.

If, for example, you have a hosted instance of SmartWorx Hub, you can change your devices' settings to connect to your hosted instance instead.

11.1.5 CELLULAR

Use the Cellular tab to get some cellular integrity diagnostics from your device.

Using this tab you can get:
- Signal Strength
- System Information
- Signal Information
- Card Status
- Cellular Module
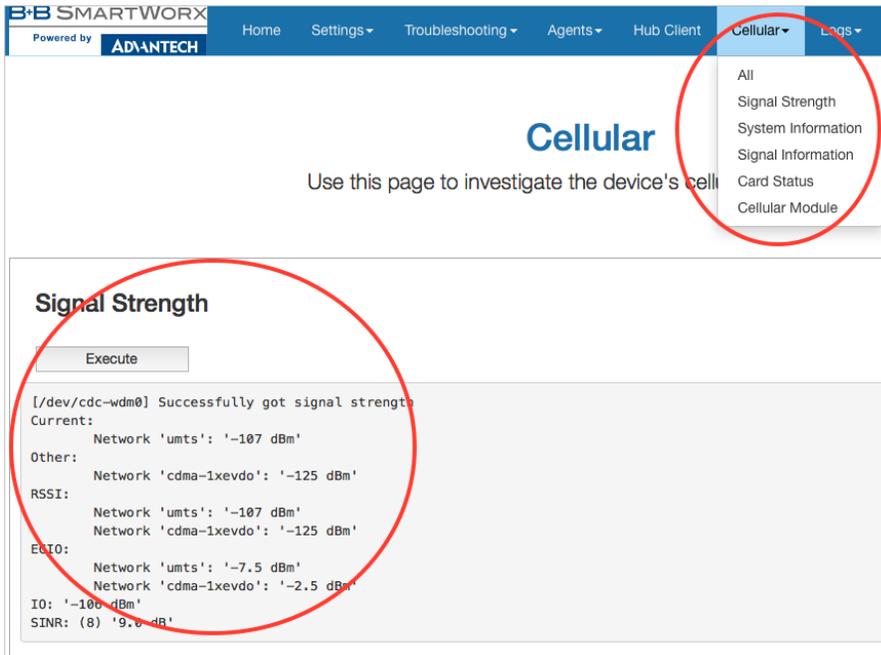
11.1.6 LOGS

The SmartSwarm device will keep debug message logs internally.

During the troubleshooting session, it may be important to open the Logs tab, and to take a copy of the messages from one of the debug-logs available.

To see live logs, you must turn on "Follow" mode and Execute.

Alternatively, you may take a current snapshot of the full log (since last reboot) by clicking on "See Full Log". This will open another browser window, in which the full system log will be shown.
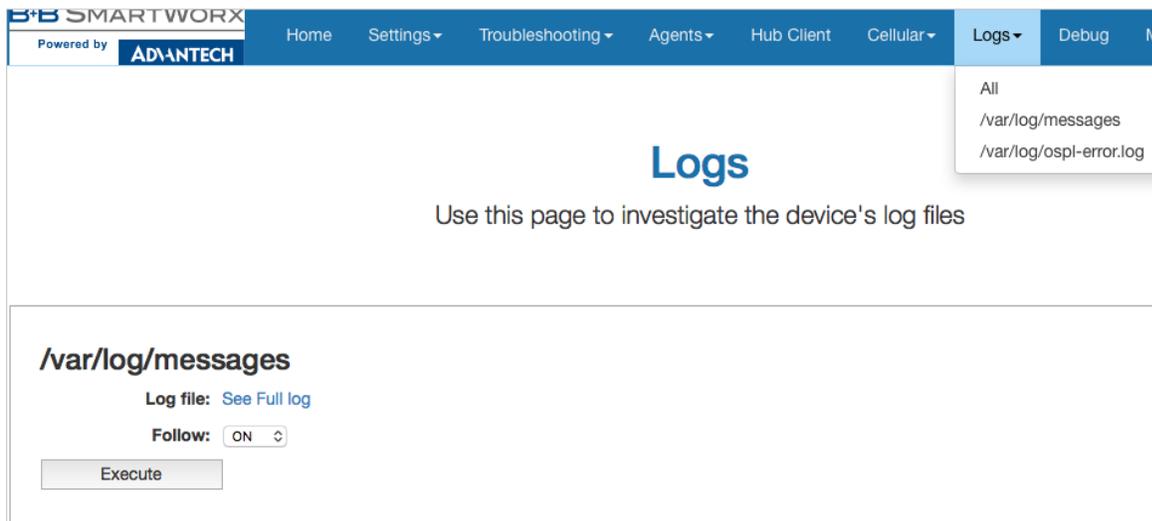
11.1.7 DEBUG AND AGENTS

It is best to use the Debug and Agents Tabs in conjunction with each other.

In the Debug tab, you can see some static debug information and you can select which Agent(s) you wish to see run-time information from.

In the Agents tab you can see run-time information (output) from the enabled Application Agents.

⚠	*In the SmartSwarm 341 Gateway, there aren't any Application Agents, so this view will not contain any information.*

12. NODE-RED LICENSE

Copyright JS
Foundation and other
contributors,
http://js.foundation

                         Apache License
                   Version 2.0, January 2004
                  http://www.apache.org/licenses/

        TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

        1. Definitions.

           "License" shall mean the terms and conditions for use, reproduction,
           and distribution as defined by Sections 1 through 9 of this document.

           "Licensor" shall mean the copyright owner or entity authorized by
           the copyright owner that is granting the License.

           "Legal Entity" shall mean the union of the acting entity and all
           other entities that control, are controlled by, or are under common
           control with that entity. For the purposes of this definition,
           "control" means (i) the power, direct or indirect, to cause the
           direction or management of such entity, whether by contract or
           otherwise, or (ii) ownership of fifty percent (50%) or more of the
           outstanding shares, or (iii) beneficial ownership of such entity.

           "You" (or "Your") shall mean an individual or Legal Entity
           exercising permissions granted by this License.

           "Source" form shall mean the preferred form for making modifications,
           including but not limited to software source code, documentation
           source, and configuration files.

           "Object" form shall mean any form resulting from mechanical
           transformation or translation of a Source form, including but
           not limited to compiled object code, generated documentation,
           and conversions to other media types.

           "Work" shall mean the work of authorship, whether in Source or
           Object form, made available under the License, as indicated by a
           copyright notice that is included in or attached to the work
           (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other
modifications
represent, as a whole, an original work of authorship. For the
purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces
of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright
owner
or by an individual or Legal Entity authorized to submit on behalf of
the copyright owner. For the purposes of this definition, "submitted"
means any form of electronic, verbal, or written communication sent
to the Licensor or its representatives, including but not limited to
communication on electronic mailing lists, source code control
systems,
and issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
excluding communication that is conspicuously marked or otherwise
designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity
on behalf of whom a Contribution has been received by Licensor and
subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   copyright license to reproduce, prepare Derivative Works of,
   publicly display, publicly perform, sublicense, and distribute the
   Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade

60

names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this
License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

ADVANTECH B+B SMARTWORX TECHNICAL SUPPORT

Phone: **+353 91 792444 (Oranmore, Co. Galway, IRELAND)**
(Monday - Friday, 8 a.m. to 5:30 p.m. UCT)

1 (800) 346-3119 (Ottawa, IL USA)
(Monday - Friday, 7 a.m. to 5:30 p.m. CST)

Email: support@advantech-bb.com
Web: www.advantech-bb.com