

Wzzard™ Condition Based Monitoring Kit Setup Guide



ADVANTECH

B+B
SMARTWORX



USA

Advantech B+B SmartWorx
707 Dayton Road
Ottawa, IL 61350 USA

Phone (815) 433-5100 -- **General Fax** (815) 433-5105

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

Europe

Advantech B+B SmartWorx
Westlink Commercial Park
Oranmore, Co. Galway, Ireland

Phone +353 91-792444 -- **Fax** +353 91-792445

Document: 710-10505-00_WSMKIT3Bx-CBM_R2_SetupGuide_1316

CONDITION BASED MONITORING KIT

The Wzzard™ Condition Based Application Bundle makes it simple to see the real time and historical temperature, current and vibration of any individual machine. Data can be exported for further analysis. Email or text message alerts can be sent when user-configured high or low limits are exceeded in critical applications. Installation costs are kept low using the Wzzard wireless sensing platform. The platform creates a self-forming, self-healing wireless mesh network that eliminates the need for wires and requires no special skills to install. Each Wzzard sensor node is powered by long life batteries.

After you install the monitoring software on your Windows PC, you can monitor the Condition based dashboard on that machine, or configure it to serve web pages that you can monitor from any web browser on your network.



WSKIT3BE-CBM/ WSKIT3BC-CBM

The contents of the kit include:

- | | | |
|---------|--------------------|--|
| - Qty 3 | WSD2CJA | Wzzard Nodes ANALOG/THERMO 2-AIN, 2-J TYPE, 1-DO |
| - Qty 1 | ERT351 or RT3G-350 | Ethernet or Cellular Gateway with SmartMesh IP Network board |
| - Qty 6 | WTJ-10-60 | J Type Thermocouples |
| - Qty 3 | JC10F50-V | 50A Clamp On Current Sensors |
| - Qty 1 | APP-BCBM | USB flash drive (2GB) with B-Scada dashboard and Documentation |



WSKIT3BE-CBM-V/WSKIT3BC-CBM-V

The contents of the vibration kit include:

- Contents of the CBM kit (listed above)
- Qty 3 LP252-2R2-1D Vibration 4-20 ma sensors
- Qty 3 CB111-A2R-010-Z Vibration cables
- Qty 3 MDR-20-24 DIN rail mount power supply 24VDC
- Qty 3 210-10497-00 RES 250 OHM 1/2W .1% AXIAL

SMARTMESH IP SET UP GUIDELINES

While a Wzzard network is self-forming, self-managing and self-optimizing, there are a few simple, but critical, pieces that you must include at the planning stage before deploying a Wzzard network.

The key to planning a quality Wzzard network is to provide the Wzzard Network Gateway with the building blocks it needs to build a robust network. For maximum reliability, each Wzzard node should have more than one path back to the gateway. Each Wzzard node is also a repeater node so arrange your network so every node has more than one neighbor. Placing Nodes within range of only one other device along a maximally spaced string will result in a fragile network that is prone to Node resets and data loss.

The first hop Nodes are the devices that will be placed within range of the Network Gateway Node, and within range of each other. As you add nodes to your network, you should ensure that you have multiple nodes in range of the gateway.

Device placement can change the effective range by orders of magnitude. At one end of the spectrum, devices placed on elevated poles or towers with clear line of sight to other Nodes in the network may have a range of 1000m or more. At the other end, devices placed on the ground or next to large metal objects may have an effective range of 10m or less. The most accurate way to estimate range is to evaluate range in a real environment using the same placement methods that will be used in the final installation. That being said, it is convenient to use as a starting point. To begin with, we recommend that customers plan on their devices working at a spacing of 50m

for Nodes with internal antennas or 100m for Nodes with external antenna for a typical indoor application. In a typical outdoor installation these numbers can be doubled to 100m for internal antennas and 200m for external antennas. Analysis of the first of several 'typical' deployments can guide the typical range number up or down.

Here are some best practices for deploying Edge Nodes:

- It is better to place a device at its final location and then have it join the network than to form your network ahead of time and subsequently scatter Nodes around the site
- Guarantee that the device hardware is working before it is installed. This can be done by pushing the configuration button and checking the status LED. A single blink will occur if the Node is active
- Install the Gateway first and then devices at the 1st hop and so on.
- If you have pre-planned for each Node to have multiple neighbors, it is not necessary to wait for a Node to join before proceeding to the installation of the next Node. It is more important to verify that each device is on, and then to verify that all devices have joined at the Gateway by checking the status LED. The status LED will stop blinking when the Node has successfully joined the network.
- It is better not to install devices very close to ground. It is preferable to install them at least 1m above ground.
- It is better to place devices away from any flat metal objects. (At least 12cm away if possible)

To join the network, the Node must be configured with the correct Network ID and Join Key that bind the device to the network. These parameters are persistent and should be set up once prior to installation. Refer to quick start guide for programming information.

A Node's Network ID must match the Network ID of the Gateway of the intended network. If multiple networks are operating on the site, additional care should be taken to ensure that the Nodes' Network IDs are set correctly. Similarly, if a Node moves from one location to another in the deployment space, it may leave its current Network ID and may not be able to rejoin. 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 Node's 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. For ease of use, we recommend using a single, deployment-specific Join Key shared by all Nodes but unique to the customer. This will prevent malicious devices from joining the network. This means that a Node need only be configured with the secure common Join Key to join the network.

A Node's Network ID must match the Network ID of the Gateway of the intended network. If multiple networks are operating on the site, additional care should be taken to ensure that the Nodes' Network IDs are set correctly. Similarly, if a Node moves from one location to another in the deployment space, it may leave its current Network ID and may not be able to rejoin. 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 Node's 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. For ease of use, we recommend using a single, deployment-specific Join Key shared by all Nodes but unique to the customer. This will prevent malicious devices from joining the network. This means that a Node need only be configured with the secure common Join Key to join the network.

SPECTRE GATEWAY SETUP

1. Attach the antenna to the AUX port.
2. Attach the Ethernet cable to the ETH port on the gateway and the other end to your PC
You will use an Ethernet connection to configure the router and to communicate with it.
3. Attach Power
Apply +10 to +30 V DC. The router has built-in protection against reverse polarity.
4. Configure the router
The default router IP address is: 192.168.1.1

Default Username = root

Default Password = root

Important! Please change your password. To do this select **Change Password** item under **Administration** section of the main menu.

5. Connect to the web client
6. Select the **User Modules** item under the **Customization** section of the main menu to view and configure the **IoT Gateway** user module.

Note: If you are having trouble connecting to the gateway, be sure that the PC is setup to use DHCP or has a static 192.168.1.x IP address.

Status	General Status
General	Primary LAN
Network	IP Address : 192.168.1.1 / 255.255.255.0
DHCP	MAC Address : 00:0A:14:83:A7:8C
IPsec	Rx Data : 16.4 KB
DynDNS	Tx Data : 6.9 KB
System Log	> More Information <
Configuration	Secondary LAN
LAN	IP Address : Unassigned
VRRP	MAC Address : 00:0A:14:83:A7:8D
PPPoE	> More Information <
Backup Routes	Peripheral Ports
Firewall	Expansion Port 1 : Ethernet
NAT	Expansion Port 2 : Dust
OpenVPN	Binary Input : Off
IPsec	Binary Output : Off
GRE	System Information
L2TP	Firmware Version : 5.1.3 (2015-04-24)
PPTP	Serial Number : 6000471
DynDNS	Profile : Standard
NTP	Supply Voltage : 12.3 V
SNMP	Temperature : 29 °C
SMTP	Time : 2015-11-03 20:44:24
Expansion Port 1	Uptime : 0 days, 0 hours, 2 minutes
Expansion Port 2	
USB Port	
Startup Script	
Up/Down Script	
Automatic Update	
Customization	
User Modules	
Administration	
Change Profile	

7. This web page shows the user modules that have been loaded into the router and the version number of each module. Click on the **IoT Gateway** User Module to bring up the configuration screen.

User Modules	
IoT Gateway 1.1 (20150608T160912Z)	Delete
New Module	Browse... Add or Update

8. The IoT Gateway Settings screen contains sections for configuring the sensor network, the internal MQTT broker, and the MQTT Bridge to an external cloud partner. At a minimum, enable the **MQTT Broker Enable** and click on the **Save** button to store the settings in the gateway.

IoT Gateway Settings	
SmartMesh IP	
Network ID	
<input type="text" value="1981"/>	The SmartMesh IP network identifier (1 - 65534).
Join Key	
<input type="text"/>	Enter a value only if the SmartMesh IP common join key (32 hexadecimal digits) is to be changed; otherwise, leave this blank to keep the current common join key.
MQTT Broker	
MQTT Broker Enable	
<input type="checkbox"/> On	Enable the local MQTT broker.
MQTT Broker Port	
<input type="text" value="1883"/>	The local MQTT broker TCP port number (1 - 65535).
MQTT Bridge	
MQTT Bridge Enable	
<input type="checkbox"/> Off	Enable bridging to a remote MQTT broker.
MQTT Bridge Port	
<input type="text" value="1883"/>	The remote MQTT broker TCP port number (1 - 65535).
MQTT Bridge Address	
<input type="text"/>	The remote MQTT broker address.
MQTT Bridge User	
<input type="text"/>	The user name for the remote MQTT broker.
MQTT Bridge Password	
<input type="text"/>	The password for the remote MQTT broker.
MQTT Bridge Client Identifier	
<input type="text"/>	The client identifier for the remote MQTT broker.
Dust Link	
Dust Link Enable	
<input type="checkbox"/> Off	Enable Dust Link installation tool for initial site survey. During the site survey, no SmartMesh IP data will be sent to the MQTT Broker or MQTT Bridge.
Dust Link Port	
<input type="text" value="8001"/>	The TCP port number used to listen for Dust Link (1 - 65535).
<input type="button" value="Save"/>	<input type="button" value="Restore"/> <input type="button" value="Return"/>

DOWNLOAD B+B SMARTWORX WZZARD SENSOR BLE APP

Wzzard nodes are configured using Bluetooth from a supported Android device. The application can be found on the Google Play Store with the name “B+B SmartWorx Wzzard Sensor”. Your Android device must support Bluetooth low energy or “Bluetooth LE”.

1. Go to the Google Play Store and search for “B+B SmartWorx Wzzard Sensor”.
2. Install the app

POWER UP WZZARD EDGE NODE

1. Remove the (4) black screws that hold the top of the node in place
2. Install your batteries
Use (2) 3.6V 2400 mAh Lithium Thionyl Chloride AA batteries.
3. Install the battery clip
4. Replace the cover and tighten the (4) screws. Screws must be tightened to 5 in-lb torque in order to maintain IP66 rating. (This can be accomplished via hand tightening.)
5. Check LED

After you have installed the batteries the LED will begin to blink. This indicates that the Node is attempting to establish a network connection. The LED will cease blinking when a connection is made.

Status LED		
Data	Solid On	Module startup initialization, approx. 10 sec.
	Slow Blink (1 per sec)	Attempting to establish connection with SmartMesh IP network
	Fast Blink (10 per sec)	Firmware Update in progress
	OFF	Unit is connected to wireless network

6. Attach the External Antenna



Note: The best way to remove the clip is to insert a small flathead screwdriver between the batteries and the clip, parallel to the batteries, and give the screwdriver a gentle twist. This will remove the clip without damage.

SETTING UP WZZARD EDGE NODES

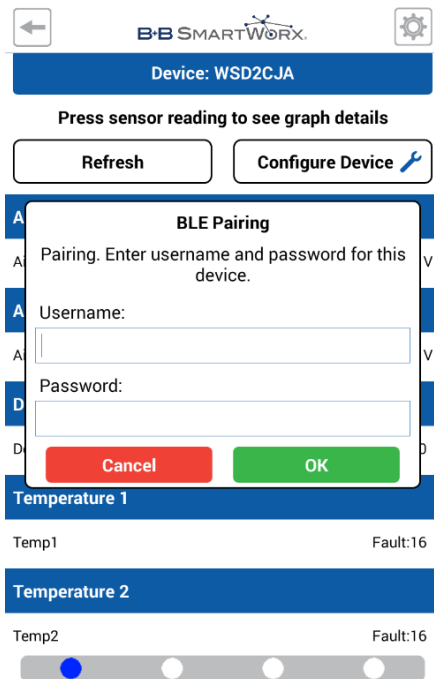
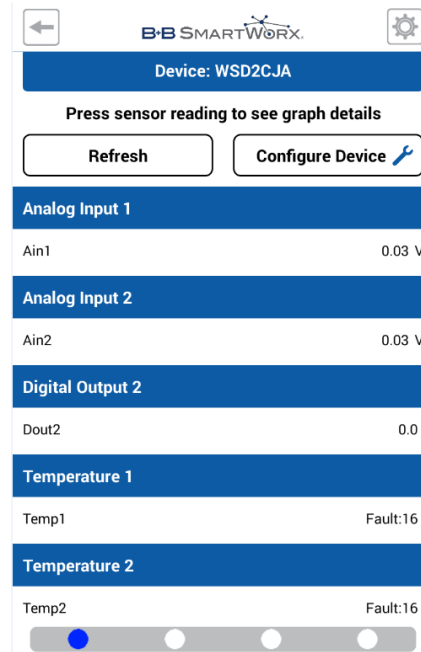
1. Run the Wzzard Sensor app on your Android device
2. Press the Configuration Button on the node.
3. Select the Node you desire to configure.

The advertise screen appears. The data comes from BLE advertisements, provided that advertisements are enabled. The advertisement data will not update when you are paired with the unit.

TIP: The node automatically disables Bluetooth after 3 minutes if no connection is made. To restart Bluetooth, press the Configuration button on the Wzzard node.

4. Press the "Configure Device" button on the App. This will pop up a window that allows you to pair with the device and enter configuration parameters.
5. Login to the node:
The default username and password are:
Username = "admin"
Password = "admin"

Note: When you enter the login information the Wzzard Intelligent Edge Node will pair with your handheld device. A popup screen will appear during the pairing process.



When the pairing process is complete you will be taken to a menu screen that allows you to begin configuring your Wzzard Intelligent Edge Node.

There are four main areas:

Radio Setup

Configure Network Bluetooth LE Settings

Sensor Setup

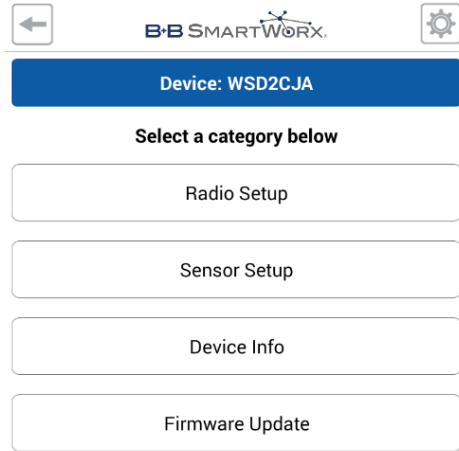
Configure internal and external sensors

Device Info

Wzzard Intelligent Edge Node information

Firmware Update

Update the firmware over the air using Bluetooth.

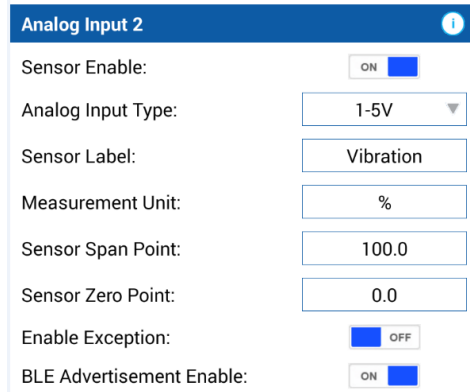
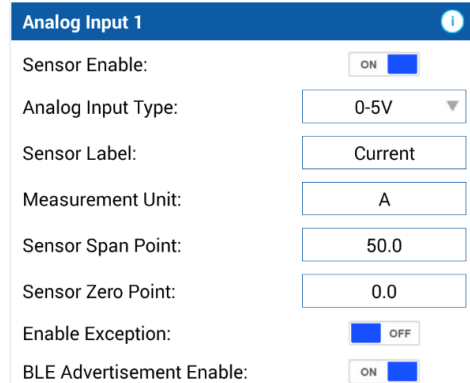


6. Click the **Sensor Setup** button
7. Set the **Publish interval** for the Wzzard node. The default is 1 minute. Shorter intervals will reduce battery life.
8. Set the **Sensor Span Point** and **Sensor Zero Point** for each sensor. This range should match the sensor range stated in the table below.

	Sensor	Analog Input Type	Span Point	Zero Point
Analog Input 1	JC10F50-V	0-5V	50	0
Analog Input 2	LP252-2R2-1D	1-5V	100	0

Optionally the user can set the **Sensor Label** and **Measurement Unit**.

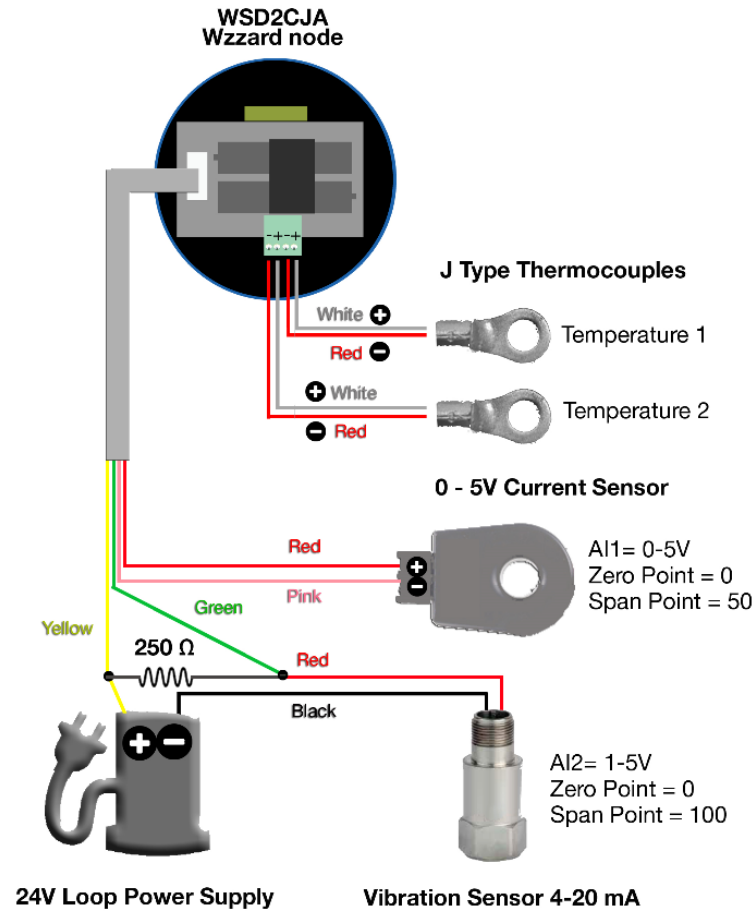
Note: The user should set **Sensor Enable** to off if they do not plan to monitor the data. For example, if the user has the WSKIT3Bx-CBM, then they should disable Analog Input 2.



ATTACHING THE SENSORS ON THE INTELLIGENT EDGE NODES

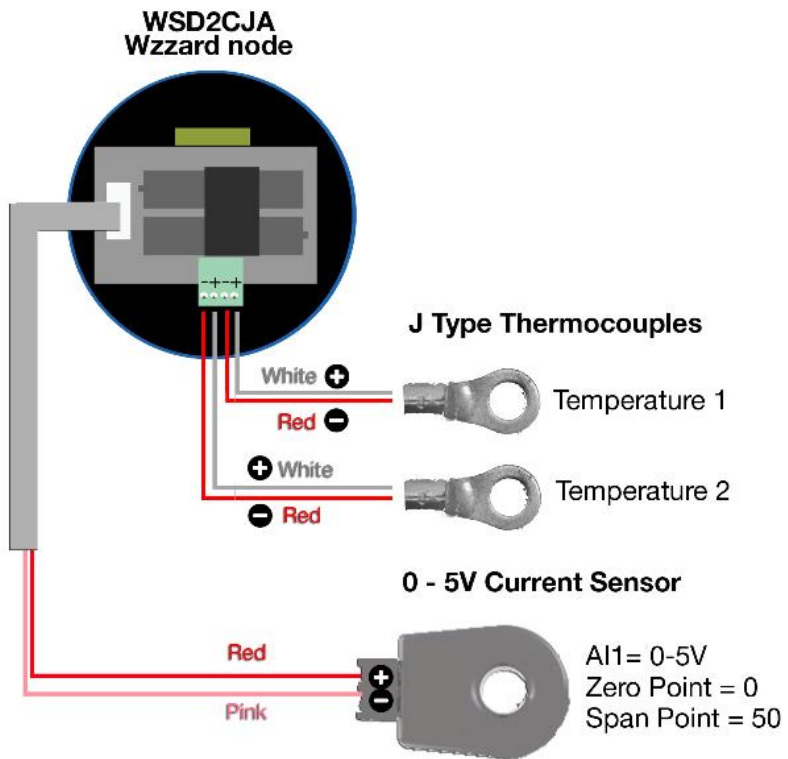
1. Wire Your Sensors

Model Number: WSKIT3Bx-CBM-V



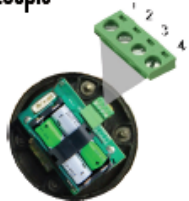
Note The vibration sensor has a current loop output so it requires a loop power supply. The resistor converts the current in the loop to a voltage that can be read by the node.

Model Number: WSKIT3Bx-CBM



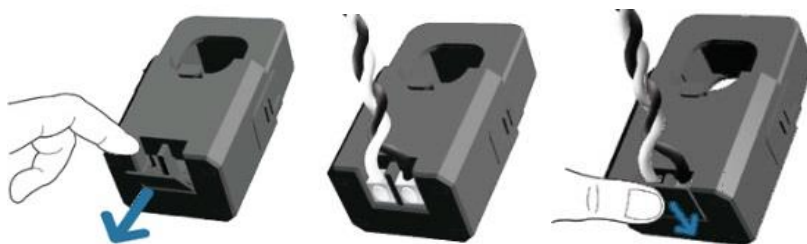
Terminal Block Connections: Thermocouple

Thread the thermocouple wires through the conduit and attach them to the terminal block.



Clamp on Current Sensor

Open the wire protector clamp by pushing it away from the sensor body. Attach your wires. Close the wire protector clamp.



2. Mount your Sensors

The sensor can be mounted in any position.

Open the clamp release by pushing it away from the sensor body. Run the wire you are monitoring through the opening in the sensor.



Close the sensor firmly around your wire and ensure that the clamp release has snapped back into place.

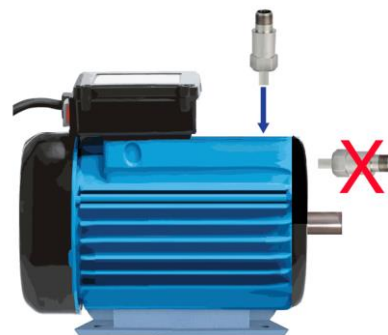
Thermocouple Sensor

Attach each thermocouple to the surface you wish to monitor.



Vibration Sensor

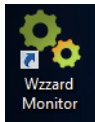
1. Mount only in thick housing wall.
2. Ensure that the signal direction is correct
3. Drill and tap $\frac{1}{4}$ " 28 UNF hole at the mounting location, $\frac{3}{8}$ " mm depth
4. Tighten the sensor to 70 in lbs of torque



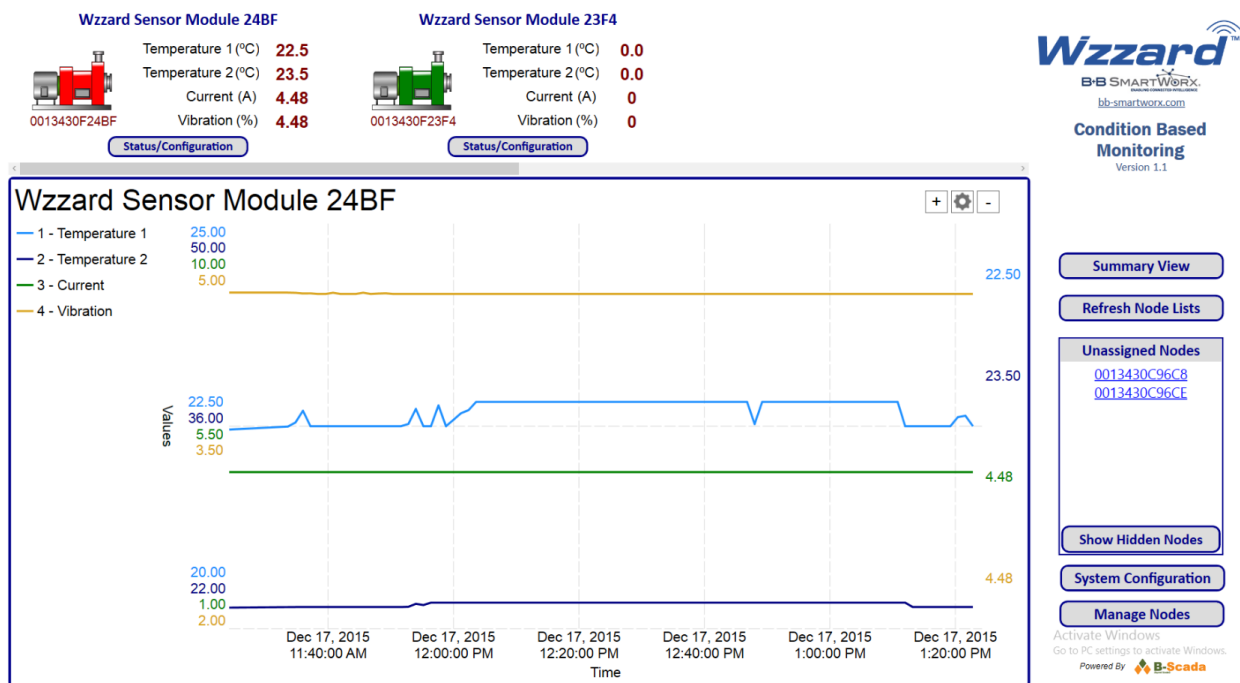
SETTING UP YOUR DASHBOARD

Note: If there are plans to use the Web client of the Energy Monitor Dashboard (e.g. for remote access from another device), see Appendix A in the User Guide before going any further.

1. Insert the USB flash drive, into your PC. Open the Removable Drive via Windows Explorer.
2. Select the **install.cmd** file. Right click and select **Run as administrator**.
3. Click **Yes** on the User Account Control Dialog.
4. Follow the instructions within the install script.
5. When the installation is complete, this new shortcut will be on your Desktop.



To start the Dashboard, double click the shortcut. The Dashboard will appear.



6. Click the **System Configuration** button to set the Gateway/Broker IP address if your gateway was setup on a network, or if it is not using the default IP Address of **192.168.1.1**. Click **Save**.
7. The MAC addresses of the nodes that are connected to the Gateway will appear on the **Unassigned Nodes** list. To add a node to the main page of the Dashboard for monitoring, click the node's MAC Address and click the **Assign Node** button. Do this for each of the nodes that you want to monitor. If you have nodes on the network that are for network purposes only, or are not supplying data to be monitored, you can click the node and select **Hide Node** to move the node to the **Hidden** list. This prevents unnecessary clutter, and makes it easier to identify new nodes that appear on the network.



NOTE: Depending upon the number of nodes connected to the network, it may take a few minutes for the nodes to appear. You may need to click the **Refresh Node Lists** button to see new nodes if they don't appear automatically.

For more information refer to the *Wzzard Condition Based Monitoring Dashboard User Manual*.

ADVANTECH B+B SMARTWORX TECHNICAL SUPPORT

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

Fax: 815-433-5109

Email: support@advantech-bb.com

Web: www.advantech-bb.com