

User Guide

Industrial IoT Gateway

Applies to: ZGW-10

EPI-233-03

© EpiSensor

Table of Contents

Safety Information **4**
- Installation 4
- NCC Warnings 5
- Intended Use 5
- Related Documents 5
- What's Included? 6

Getting Started **6**
- Connecting to the Gateway 6
- Changing the Default Password 11

Home **11**
- General 12
- Sensor Network 13
- Data Export 13
- Network 14

Settings → Add Nodes **14**

Nodes **15**

Nodes → Node Settings **19**
- Information 20
- Status 21
- Properties 21
- Sensors 22

Nodes → Node Settings → Sensor Settings **24**
- Sensor Information 24
- Sensor Properties 25

Data → Graph View **27**

Data → Data File Archive **29**

Settings → Data Export **29**
- Quality of Service 30
- Status 30
- Settings 30
- EpiSensor JSON 31
- Edge JSON 32
- CSV via FTP 33
- RKDAP 35

Layout **36**

Settings → Ethernet **37**

Settings → Cellular **39**

Settings → Time & Date 41
Settings → System 42
Settings → Password 44
Settings → Sensor Network 45
Logs → Log View 46
Logs → Log Settings 47
Logs → Log File Archive 49
About → Overview 49
Ordering Information 51
Region Specific Features 53
Troubleshooting & Support 53
Warranty 54
Glossary 54

Safety Information

Please read these instructions carefully before trying to install, operate, service or maintain the ZGW-10. The following special notes may appear throughout the user guide (or on the equipment labels) to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure for users.

Symbol	Description
	The addition of either symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.
	This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

Installation

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by EpiSensor for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Installation, wiring, testing and service must be performed in accordance with all local and national electrical codes.

Installation & Safety Notes
➔ EpiSensor equipment should be installed, operated, serviced and maintained only by qualified personnel. EpiSensor does not assume any responsibility for any consequences arising out of the use of this equipment.
➔ Clearly label the device’s disconnect circuit mechanism and install it within easy reach of the operator.
➔ The fuses / circuit breakers must be rated for the installation voltage and sized for the available fault current.

NCC Warnings

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者:此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策

Appropriate use is advised to minimise the impact of electromagnetic waves.

減少電磁波影響，請妥適使用

Radio wave power density MPE standard value: 1 mW/cm^2, measured value of the sent product: 0.142 mW/cm^2, it is recommended that the device antenna be at least 20 cm away from the human body when in use.

電波功率密度 MPE 標準值:1 mW/cm^2,送測產品實測值:0.142 mW/cm^2,建議使用時設備天線至少距離人體 20 公分

Intended Use

Do not use this device for critical control or protection applications where human or equipment safety relies on the operation of the control circuit. Failure to follow these instructions can result in death, serious injury, or equipment damage.

Related Documents

Related installation and configuration documents are listed in the following table:

Document	Reference No.
EpiSensor ZGW-10 Datasheet	EPI-213-01
EpiSensor ZGW-10 Install Sheet	EPI-215-01
Gateway API User Guide	ESE-009-08
Bootloading on a live Gateway	EPI-064-00
Use of Node Profiles on the EpiSensor Gateway	EPI-208-00

What's Included?

The items included with each EpiSensor Gateway are as follows:

ZGW-10		
	**Qty**	**Item**
	1	ZGW-10 IoT Gateway
	1	Primary Cellular Antenna
	1	Secondary Cellular Antenna

The ZGW-10 Gateway requires an external 12/24V power supply that is not included as standard. For information on the accessories available for each model, please contact support@episensor.com

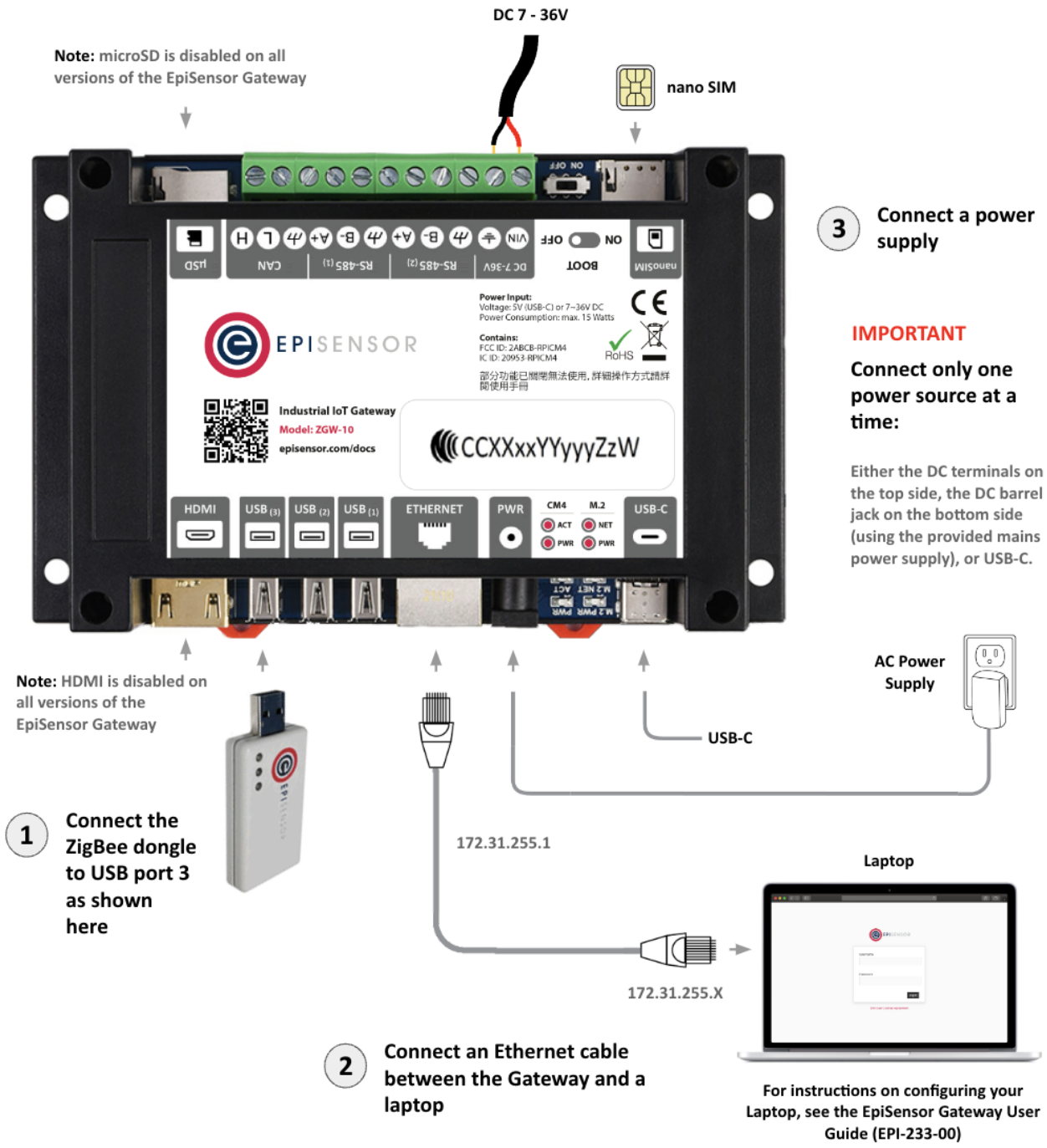
Getting Started

EpiSensor's IoT platform is easy to deploy, configure and scale and includes a range of sensor products that can monitor a variety of environmental and energy usage parameters in commercial and industrial environments.

This user guide contains technical information on configuring and maintaining the central component in the platform - the Gateway. For a minimum system, you will need a Gateway, a computer to access the web interface of the Gateway, an Ethernet cable (included) and at least one wireless node.

Connecting to the Gateway

Please confirm that all items listed above are present before proceeding. Also note the following guide relates to release V4 of the Gateway software.



Quick Setup for ZGW-10

1. Connect the ZigBee dongle to USB port 3 as shown above
2. Connect an Ethernet cable between your computer and the Ethernet Port on the ZGW-10 Gateway
3. If your version of the ZGW-10 has a cellular modem, Wi-Fi / Bluetooth or GPS, connect the antennas as shown on page 2 of the ZGW-10 install sheet (document ref. EPI-215-01).

4. Connect a 12V / 24V power supply to Gateway's DC input jack (marked "PWR" on the label), to the USB-C port, or to the green DC input terminals. Note: only connect one power source at a time.
5. Configure your computer's Ethernet settings with a static IP address of **172.31.255.123** and a subnet mask of **255.255.255.0**
6. Connect to http://172.31.255.1:8081/ with a modern browser
7. Login with Username: admin, Password: A1
8. Go to Settings → System. Select 'Form New Network' and Submit. Wait for 20 seconds.
9. Go to Settings → Add Nodes and enable 'allow join' mode for 1 hour.
10. Power on any mains-powered nodes. Press and hold 'mode button' until the Status LED flashes on battery-powered nodes.
11. If the nodes are in factory default condition, they will connect to the Gateway and appear in the nodes list.

Important Note

The factory default IP address for all Gateways is 172.31.255.1

It can take up to 5 minutes for the Gateway to initialise. After this time, go to http://172.31.255.1:8081/ in a modern browser and you should see the Gateway login interface below.

Important Note

You will need access to port 8081 to access the web interface of the Gateway and the API. Other ports used depending on what features are enabled and what data export type is selected.

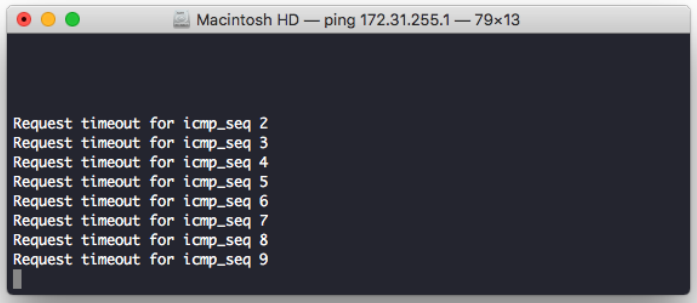
There are four LEDs on the ZGW-10. The M.2 PWR and M.2 NET LEDs indicate the cellular modem status and are described later in this document in the section on enabling the cellular modem. The PWR and ACT LEDs indicate the general state of the ZGW-10 as follows:

PWR LED STATUS	ACT LED STATUS	Meaning
OFF	*	Gateway is not powered.
ON	FLASHING	Gateway is powered and operating normal. Note that the ACT LED duty cycle is low when the gateway is operating normally. It will have a longer duty cycle during the boot sequence of the gateway.

ON	ON	During the boot sequence both LEDs may be ON for a duration of a few seconds. However if both LEDs remain ON the boot sequence has failed.

The Gateway supports all recent versions of Chrome, Firefox, Safari and Edge web browsers. On older browsers, some features may not display correctly.

If the login page fails to load, try pinging the Gateway's IP address from the command line on your computer:



If the ping request is timing out, verify that the physical network connection is OK, and check that the network settings have been applied correctly.

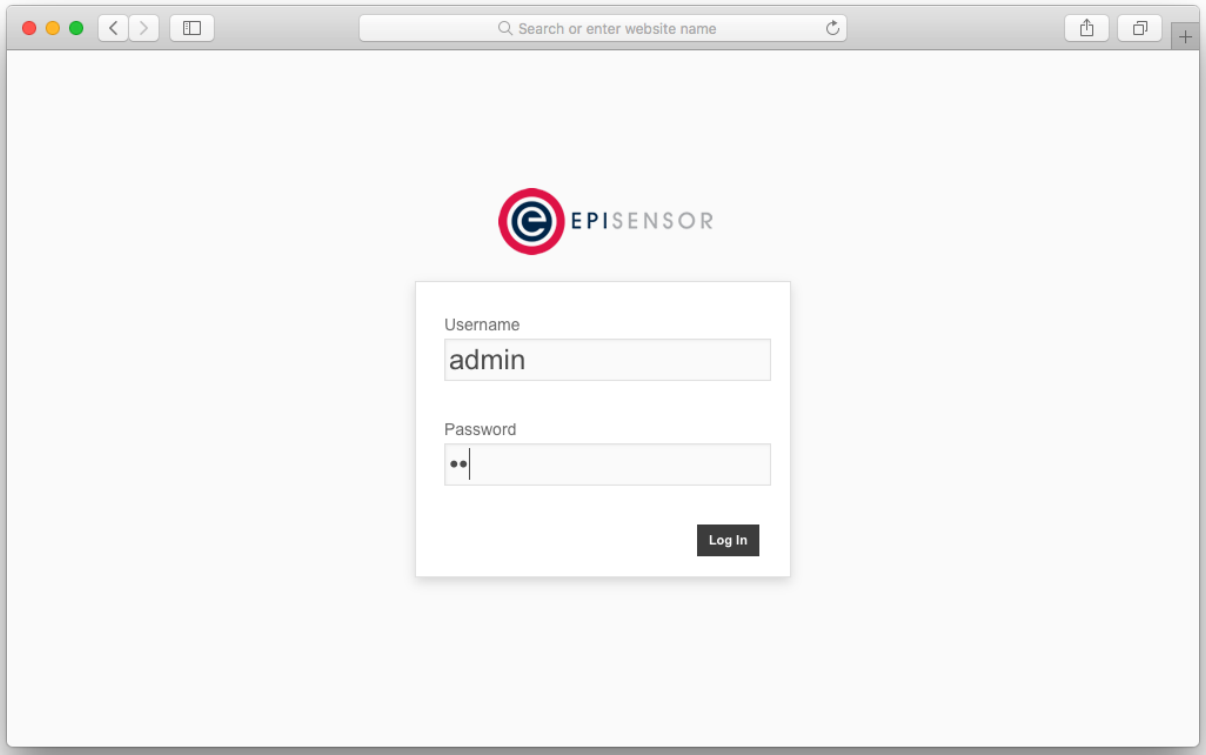


Figure 1 - Login Screen

Important Note
The default Gateway user account is Administrator; the default login details for this account are as follows: **Username:** Administrator **Password:** A1

On recent Gateway software releases, “admin” will also be accepted as the username for this account. If the incorrect password is entered, four more attempts are permitted before the user is locked out for five minutes. After five minutes has elapsed you can try again, up to another five attempts are allowed, and so on. In the event of the password being irretrievable, please contact support@episensor.com

After logging in, you will see a navigation bar at the top of the page. The sections in this document match the links in this top navigation.

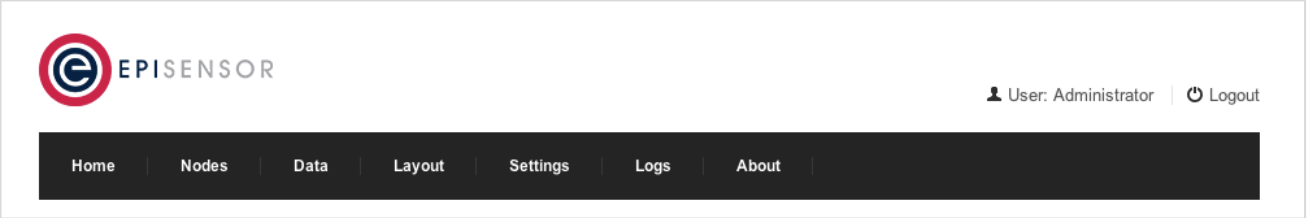


Figure 2 - Navigation

Changing the Default Password

It is strongly recommended to change the default account password after login by navigating to Settings → Password. Please note that passwords are case sensitive. The screenshot below shows the password change interface. Passwords can consist of letters [A-Z] and [a-z], numbers [0-9] and the following characters [. ! * ^ _ -]

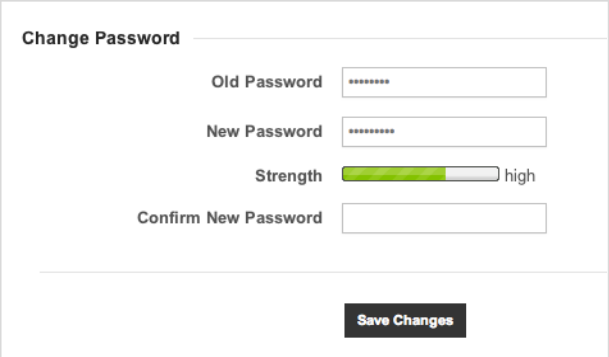


Figure 3 - Password Change Screen

After successful login, there is a session timeout on the web interface. After one hour of inactivity on the web-interface users will have to re-login to the web interface.

Home

The Home page is the first page encountered after log-in. The aim of the Home page is to provide an overview of the status of the Gateway.

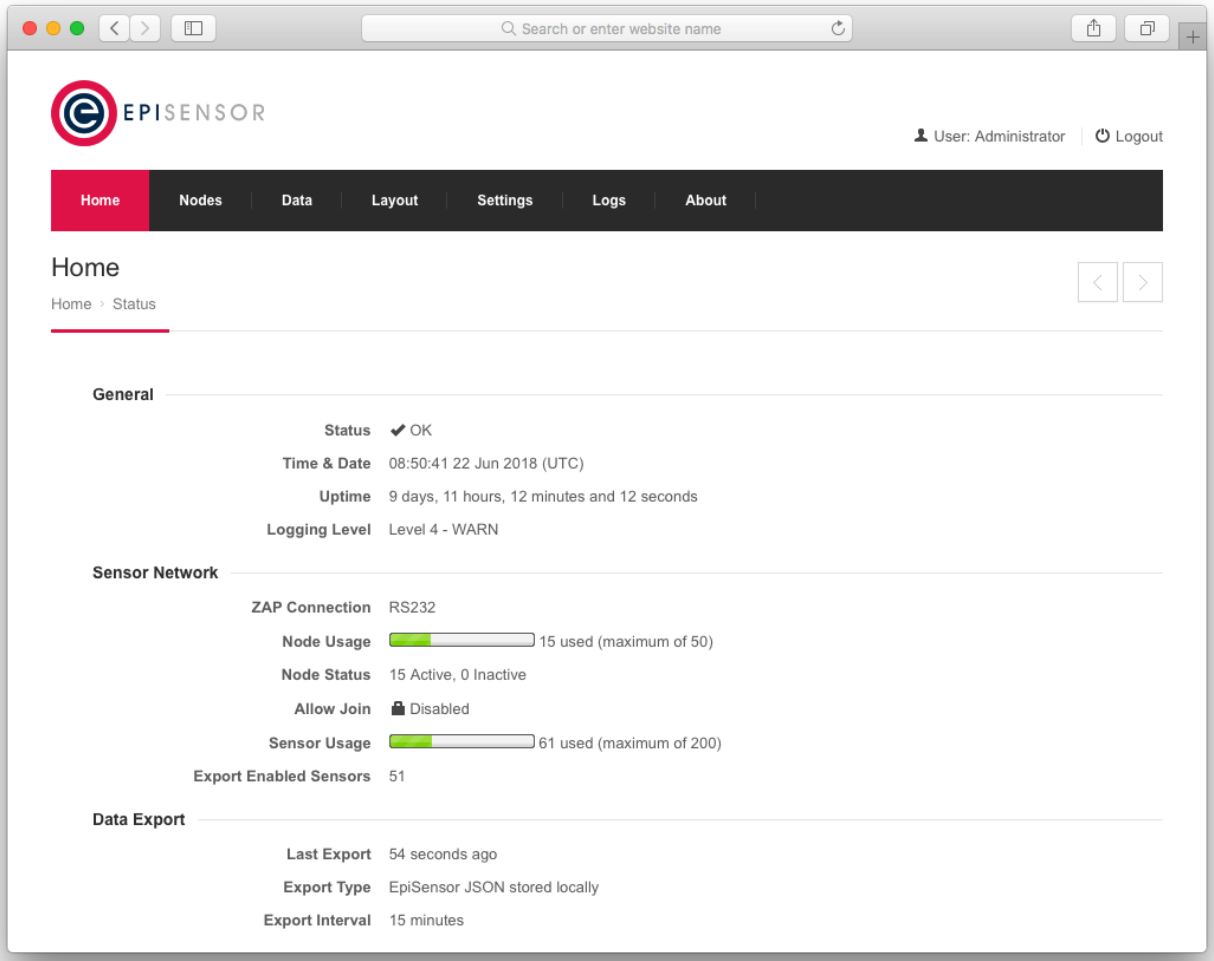


Figure 4 - Dashboard View

General

Status: The status of the Gateway system. This indicates whether or not the gateway software is up and running. It does not indicate the status of the wireless sensor network. If this parameter is not showing “OK” please contact EpiSensor support.

Time & Date: The current time and date in terms of Coordinated Universal Time (UTC).

Uptime: How long the Gateway application has been running for in days, hours, minutes and seconds.

Logging Level: The currently configured Log Level (See Logs → Log Settings for more information).

Sensor Network

This subsection provides information about the wireless sensor network that this Gateway is controlling. The term “Node” refers to all EpiSensor wireless monitoring products. A node may have zero or more “Sensors”.

Example
 An EpiSensor TES-11 temperature sensor node has two sensors: a temperature sensor and a battery level sensor.

ZAP Connection: This indicates how the NGR is configured to connect to the ZAP. The connection will be either via RS232 or via Socket.

Node Usage: This represents the number of nodes currently joined to the wireless sensor network. There is a progress bar which shows the current usage level and the maximum allowed. The maximum number of nodes that may be joined to the ZGW-10 Gateway network is 100.

Node Status: The node status in terms of inactive and active nodes. Active nodes are nodes that are operating as expected, inactive nodes are nodes that have not reported data as expected.

Allow Join: The allow join status indicates whether or not the Gateway has opened the network for new nodes to join. (See Settings → Add Nodes for more information).

Sensor Usage: This represents the number of sensors in the wireless sensor network that are reporting data. This value is shown on a progress bar. The maximum number of reporting sensors in the ZGW-10 Gateway network is 1000.

Export Enabled Sensors: The number of sensors that have been enabled for ‘data export’ on this Gateway. This parameter is useful when licensing 3rd party software products.

Data Export

This subsection displays information relating to the data export features on the Gateway.

Last Export: Displays the amount of time that has passed since the Gateway last exported data.

Export Type: The active data export ‘driver’.

Export Interval: How often the Gateway is configured to export data.

Network

This section provides an overview of how the Gateway is connected to a LAN or the Internet.

Connection: Shows the active network interface – this could be Ethernet or Cellular modem.

Internal IP: The IP that the Gateway has been configured with or assigned by a DHCP server.

External IP: If the Gateway has Internet access, this is the Gateway's IP address on the internet. This is determined by polling an external server on the Internet.

Settings → Add Nodes

To add a node to the Gateway first navigate to the Settings → Add Nodes page of the Gateway web interface.

By default the wireless sensor network is 'closed' and does not allow new nodes to join. From this page, the network may be 'opened', thus allowing new nodes to join. Similarly from this page, an 'open' network may be 'closed' which re-enables the wireless sensor network and prevents new nodes from joining.

If a network is currently 'closed', it may be opened by selecting the Allow Join 'Enable' radio button and selecting the time period for which Allow Join should be enabled for, then clicking 'Submit'.

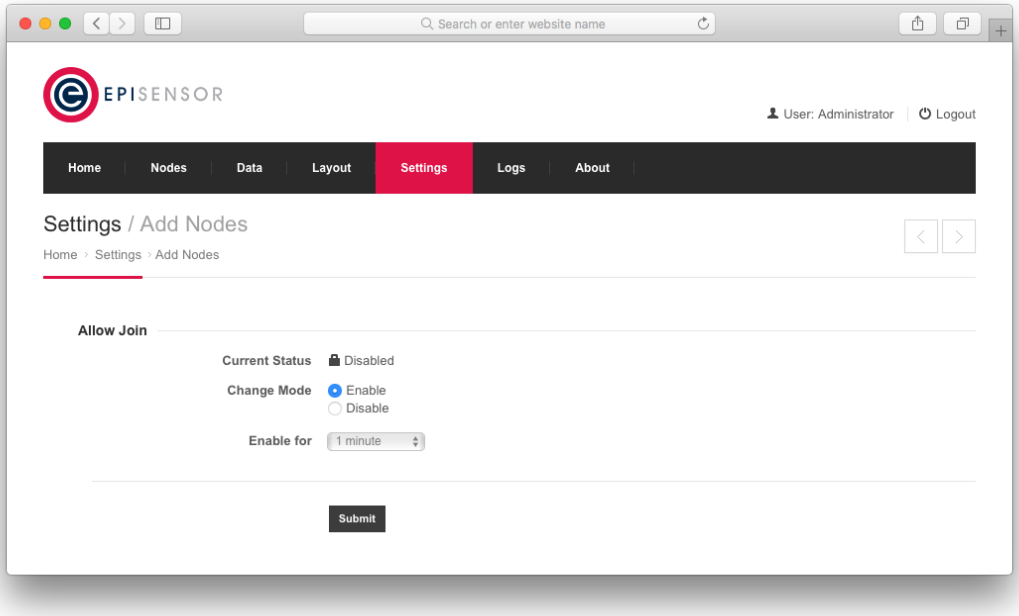


Figure 5 - Allow Join

If a network is currently 'open', it may be closed by selecting the Allow Join 'Disable' radio button, and submitting the form.

Example	
	If a network is currently ‘open’ and allow join mode is enabled for X amount of time, this will override the previously selected time period.

For adding nodes to a network when the ZAP (Zigbee Access Point) firmware version is lower than 1.60, please contact support@episensor.com. The firmware version of the ZAP can be checked on the Settings → Sensor Network page.

When “allow join” mode has been enabled on the Gateway, mains powered nodes that are in a factory default state should detect the open network and join the Gateway. They will appear in the Nodes → List View page. To add battery powered nodes to the Gateway, press and hold the button until the LED flickers and then turns on constantly, and then release the button. This will wake the battery powered node up from a low power state and force it to scan for open networks, (assuming the node is in a factory default state). For the location of the button and LED see the relevant section of the user guide relating to that product.

To join nodes that have already been associated with another Gateway, a ‘factory reset’ will be required. For instructions on resetting a node to the factory default state, see the “Button and LED Interface” section of this document.

Nodes

This Nodes page shows the list of nodes that have been added to the Gateway. This list may be empty if there is no ZAP connected or if the ZAP is connected but no nodes have been added to the Gateway.

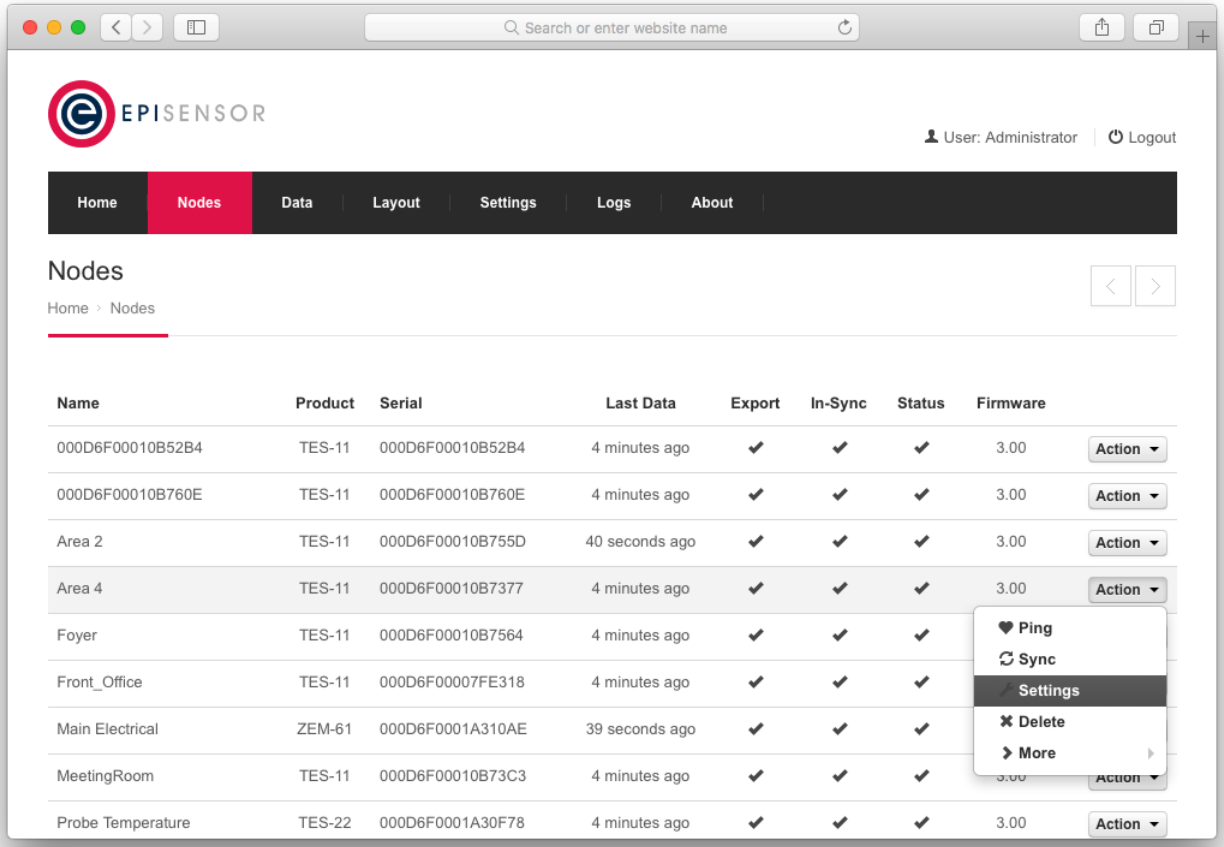


Figure 6 - Nodes List View

Note the hierarchy of settings for Nodes and Sensors. The nodes list (above) lists each node connected to the Gateway, with status information and links to take action or view node settings.

The node settings page provides status and communications information specific to that node, allowing users to change node level settings and list the sensors associated with that node. Navigate to the node settings page using the drop-down ‘action’ menu. The user can then go a level deeper into a settings page for each sensor.

Note

Some “batch commands” are available from the nodes list page that can save time when configuring data export. A batch command is a command that changes settings for all of the sensors on a node.

For each node in the network the following information is shown:

Name: The node name, by default is the node serial number but may be assigned on the Nodes → Settings page (use the 'action' drop-down menu to access this page).

Product Code: The EpiSensor specific product code. Details on product codes can be found in the products section of this user guide or at https://episensor.com/products

Serial: The unique serial number of the node (also referred to as the "long address" of the node).

Last Data: The amount of time since the last data point was received from any sensor of this node. This will show "None" if no data has been received.

Note	
	This value is approximated to the nearest second, minute, hour or day. For example "5 hours" could be 5 hours plus any number of minutes and seconds past the hour. The exact time of the last data point can be found on the Node Settings page.

Export: If at least one sensor of this node is enabled for data export then a tick will be shown ✔. Otherwise it is set to the following icon: ❗

In Sync: A warning icon will be shown if there are over-the-air commands pending for this node: ❗ Over-the-air commands are issued as a result of the selection of an "Action" from the drop down list for each node. If the node is 'in-sync' with the information on the Gateway, the following icon will be shown: ✔

Status: If no communications have been received (data or heartbeats) from a node in the last 30 minutes, the status column will show the following icon: ❗ Otherwise the column will show the following icon: ✔ The purpose of this field is to highlight nodes that are no longer connected to the wireless network. "Heartbeats" are messages received regularly from all nodes on the network that inform the Gateway that they are active on the network.

Firmware: This field lists the version of firmware that each node is running. For optimal performance the node firmware version should be 2.60 or higher.

'Legacy mode' will automatically be enabled for nodes with a firmware version of 2.6 or lower. There are no additional settings to be configured for this mode. Data from these nodes will be interpolated to a 15 minute reporting interval. Cumulative sensors such as kWh or pulse sensors will report in kWh/15min period. The Export ID and other parameters for these sensors can be configured in the normal way. For more information on Legacy Mode please contact support@episensor.com

For each node in the network the actions shown below are available from the drop down list:

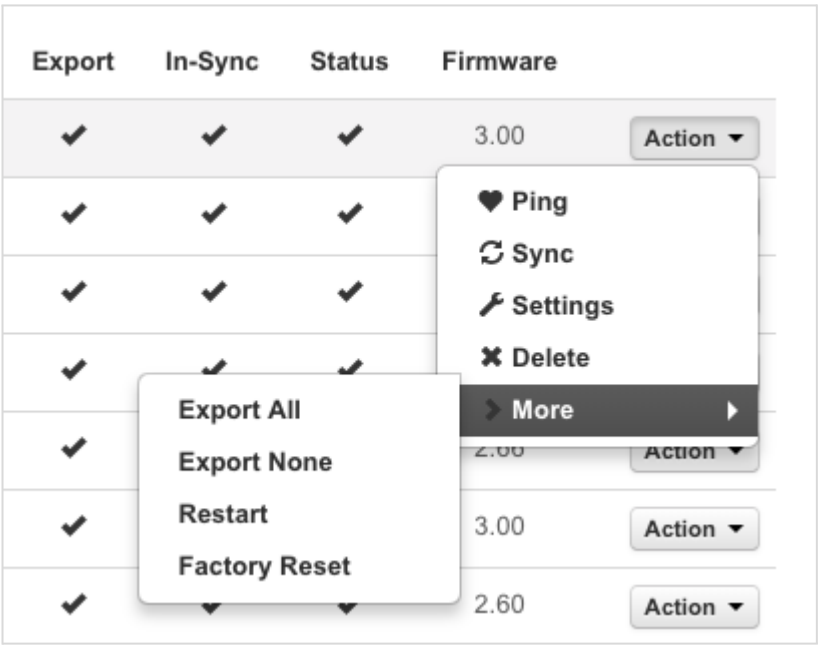


Figure 7 - Nodes List Action Drop-Down

Each of the actions above is described in more detail as follows:

Ping: Send a "Ping" over-the-air command to the node. The purpose of sending a Ping command to a node is to check if it is alive.

Sync: A "node property" can be a read-only or configurable parameter relating to a node or sensor. Selecting this action will issue a command to request that all node properties be refreshed. This action will result in numerous over-the-air commands being issued. It can be used if the settings pages for a node or sensor have not been fully populated (i.e. that some fields are displaying a dash "-" symbol). This could be caused by the Gateway being powered down while a new node is being added.

Export All: Enable data export from all sensors of this node. Export can be enabled or disabled for individual sensors from the Nodes → Settings (via "Action" drop-down list) → Sensor Settings (via "Action" drop-down list).

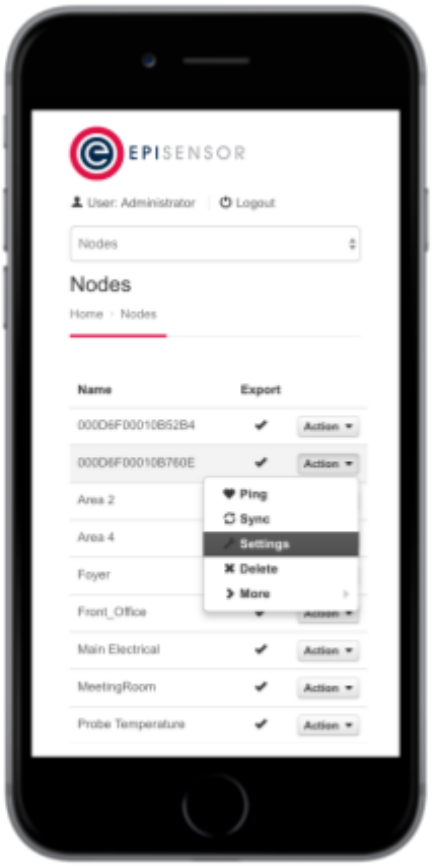
Export None: Disable data export for all sensors of this node. Export can be enabled or disabled for individual sensors of this node from the Nodes → Settings (via "Action" drop-down list) → Sensor Settings (via "Action" drop-down list).

Reset Node: Send an over-the-air command to reset the node. This is equivalent to power cycling the node (i.e. switching the nodes off and then on). No settings on the node will be lost.

Factory Reset Node: Send an over-the-air "factory reset" command to the node. In this case all node settings will be lost; the node will disconnect from the Gateway and will be returned to a factory default state.

Settings: Navigate to the Settings page for this node.

Delete: Remove this node from the Gateway. This does not remove the node from the wireless sensor network; it merely removes the node from the Gateway's records. This typically would be used to remove unresponsive nodes from the list. If a responsive node is removed from the list, it will automatically be added the next time it sends a heartbeat or a data point to the Gateway. To permanently delete a live node from the Gateway, first issue a “Factory Reset Node” command to the node, then delete the node from the Gateway.



After an action has been selected, a response message will be displayed at the top of the page. In the case of actions which result in over-the-air commands being issued, the response message can only confirm that the command was sent. The log file (accessed through Logs → Log View) will provide information regarding the response received from the node, assuming the Log Level is set to a high enough level (see ‘Log Settings’ section for more information). When the command has completed (successfully or not) the In-Sync flag will show the tick symbol. However, to confirm that the command has been implemented users must either check the log file, or the relevant settings page.

The Gateway’s web interface is designed to work on a variety of mobile phone and tablet web browsers. If the Gateway is accessed from these devices, the screen size will adapt. For mobile phone browsers in portrait mode, the top navigation bar will be replaced with a drop down list. In addition, on pages that include a table of data, some columns will be hidden to improve the user experience:

Figure 8 – Gateway web Interface on Mobile Web Browser

Nodes → Node Settings

The node settings page provides more detail on a specific node, and allows users to change node level settings. Changes to the node settings may be submitted by clicking the 'Save Changes' button and the bottom of the page.

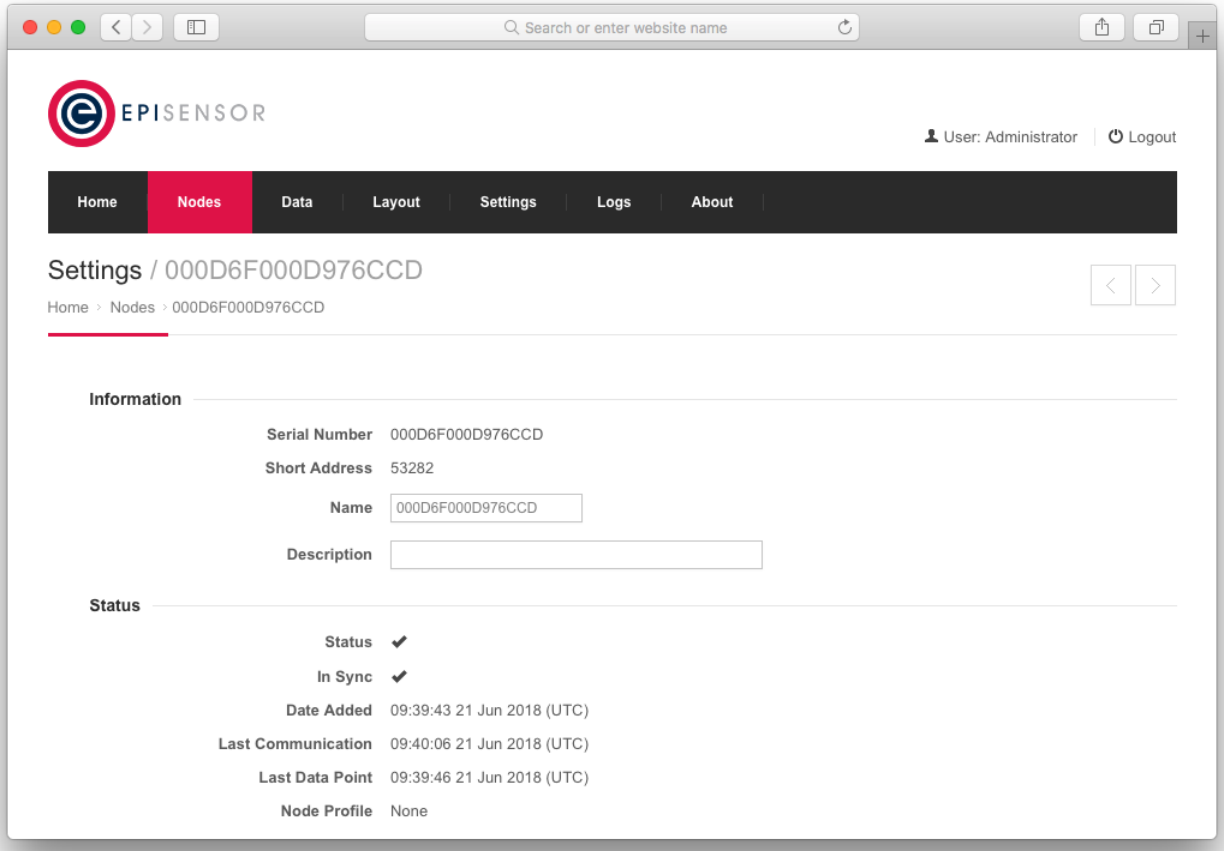


Figure 9 - Node Settings

Information

Serial Number: The unique serial number of this node.

Short Address: The short address of this node.

Name: The name of this node. This value defaults to the node serial number, however a non-default name may also be assigned. This name will be used then in the Nodes → List View and Data pages.

Note
Assigned node names may contain alphanumeric characters (A-Z, a-z, 0-9) as well as full stop (.), underscore (_), dash (-) and a space.

Description: A description of this node. This field is optional and could be used to describe a node location,

record an asset tag or to note when maintenance is due.

Note
Assigned node descriptions may contain alphanumeric characters (A-Z, a-z, 0-9) as well as full stop (.), underscore (_), dash (-) and a space.

Status

Status: If no communications have been received (data or heartbeats) from a node in the last 30 minutes, the status column will show the following icon: ❗ Otherwise the column will show the following icon: ✔ The purpose of this field is to highlight nodes that are unresponsive.

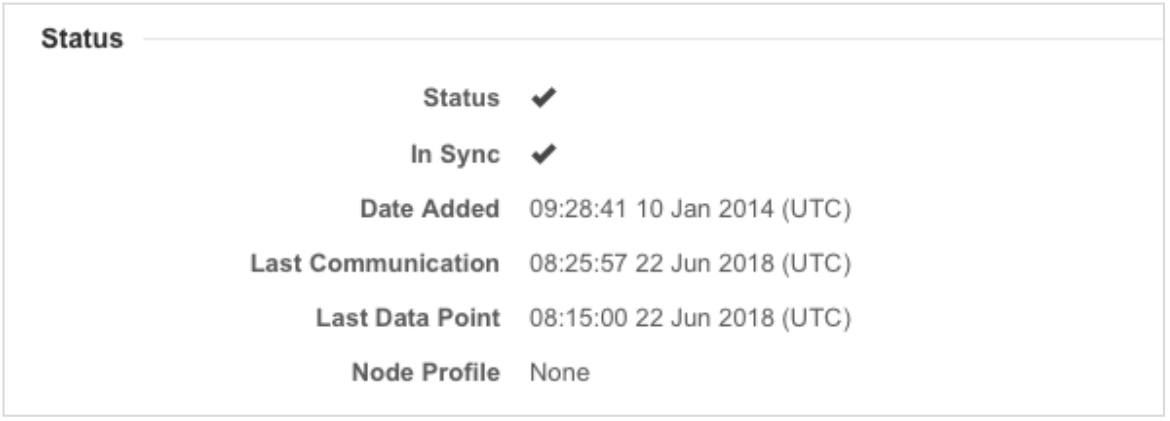


Figure 10 - Status Screen

In Sync: This flag indicates if there are over-the-air commands pending for this node. Over-the-air commands are issued as a result of the selection of an "Action" from the drop down list for each node. If there is a command pending, the following icon will be shown: ❗

Date Added: This is the date (in UTC) that the Gateway became aware of this node on the network.

Last Communications: This is the date (in UTC) of the last communication of any type received by the Gateway from this node.

Last Data Point: This is the date (in UTC) of the last data point received by the Gateway from this node.

Properties

This section will be populated dynamically based on the properties that the node reports. As a minimum set the "Product Code" property and the "Firmware Version" will always be present. If the property is writable, a text box or a drop-down selection list will be available to facilitate modifying the property value.

Product Code: The EpiSensor specific product code. Details on product codes can be found in the products section of this user guide.

Firmware Version: This field lists the version of firmware that each node is running. For optimal performance the node firmware version should be 2.60 or higher. For more information on 'Legacy Mode' for nodes with firmware version 2.6 or lower, see the Gateway / Nodes section above.

If the property values in this section are not completed or there is an absence of properties that would be expected for this product, try issuing a "Refresh all properties" command. This can be done from the Nodes → List View drop down "Action" list. It will take a number of seconds for the node level properties to be refreshed.

Sensors

This section will be populated based on the sensors that each node reports are present, as shown in the screenshot below.

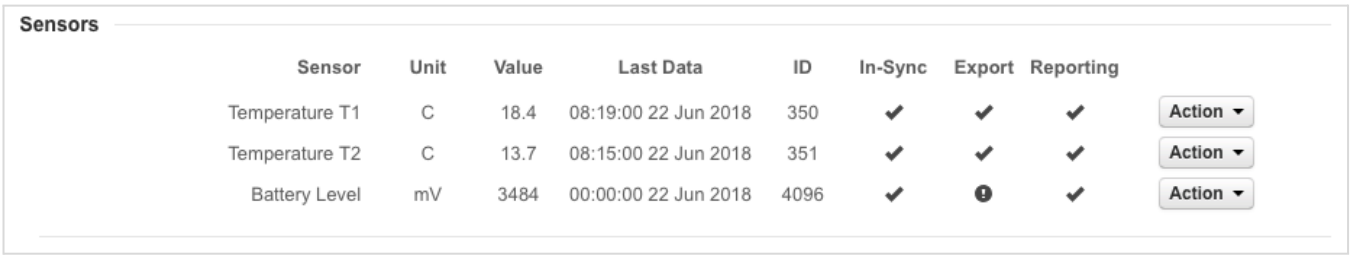


Figure 11 - Sensors Screen

For each sensor the following information is provided:

Sensor: The sensor name. For an explanation of each sensor name, see the relevant product section in this user guide.

Unit: The units of the sensor reports data in.

Value: The value of the last data point received from this sensor. A Dash (-) will be shown if no data points have been received from this sensor.

Last Data Point: The timestamp of the last data point received from this sensor or a dash (-) if no data points have been received from this sensor.

ID: The sensor ID number. Each sensor type has a unique ID.

In Sync: This flag indicates over-the-air commands are pending for this sensor. Over-the-air commands are issued as a result of the selection of an "Action" from the drop down list on the Nodes → Settings page or from a setting being changed on the Nodes → Settings → Sensor Settings page. If there is a command pending, the following icon will be shown:

Export: This icon indicates whether data export has been enabled or disabled for this sensor. The Export ID for a sensor can be configured on the Nodes → Settings → Sensor Setting page. If export is disabled for a sensor, the following icon will be shown:

Reporting: Indicates whether data reporting is enabled for this particular sensor. Reporting modes can be set from the Nodes → Settings → Sensor Setting page. If reporting is disabled for a sensor, the following icon will be shown:

For each sensor of the node the following actions are available from the drop down list:

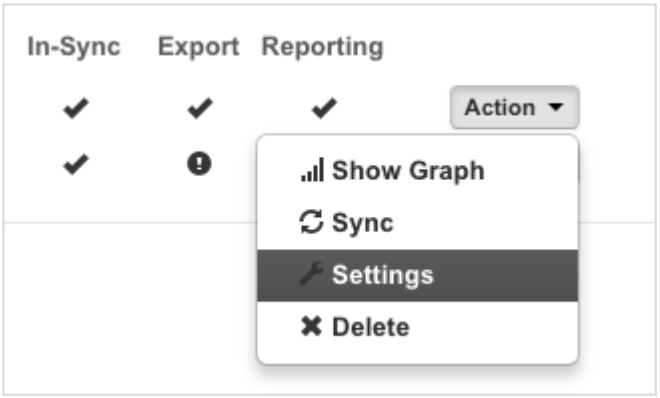


Figure 12 - Sensor Settings Action Drop-Down

Sync: Refresh all properties of this sensor of this node. The sensor properties are displayed on the Nodes → Settings → Sensor Settings page for each sensor. This action will result in numerous over-the-air commands being issued.

View Data Graph: This is a shortcut to display a data graph for this sensor as described in the Data → Graph View section of this guide. Default settings will be used when displaying a graph from this menu.

Settings: Navigate to the Sensor Settings page for this sensor.

Delete: Delete this sensor from the list. This does not remove the sensor from the wireless sensor network; it merely removes the sensor from the Gateway's records.

Note
If the sensor list in this section is not completed or there is an absence of sensors that would be expected for this product try issuing a “Sync” command. This can be done from the Nodes → List View drop down “Action” list. It will take a number of minutes for the node level properties to be refreshed. When this is complete, all items in the settings pages for that node should be populated.

Nodes → Node Settings → Sensor Settings

This page provides more details on a specific sensor. Changes to the sensor settings may be submitted by clicking the “Save Changes” button at the bottom of the page.

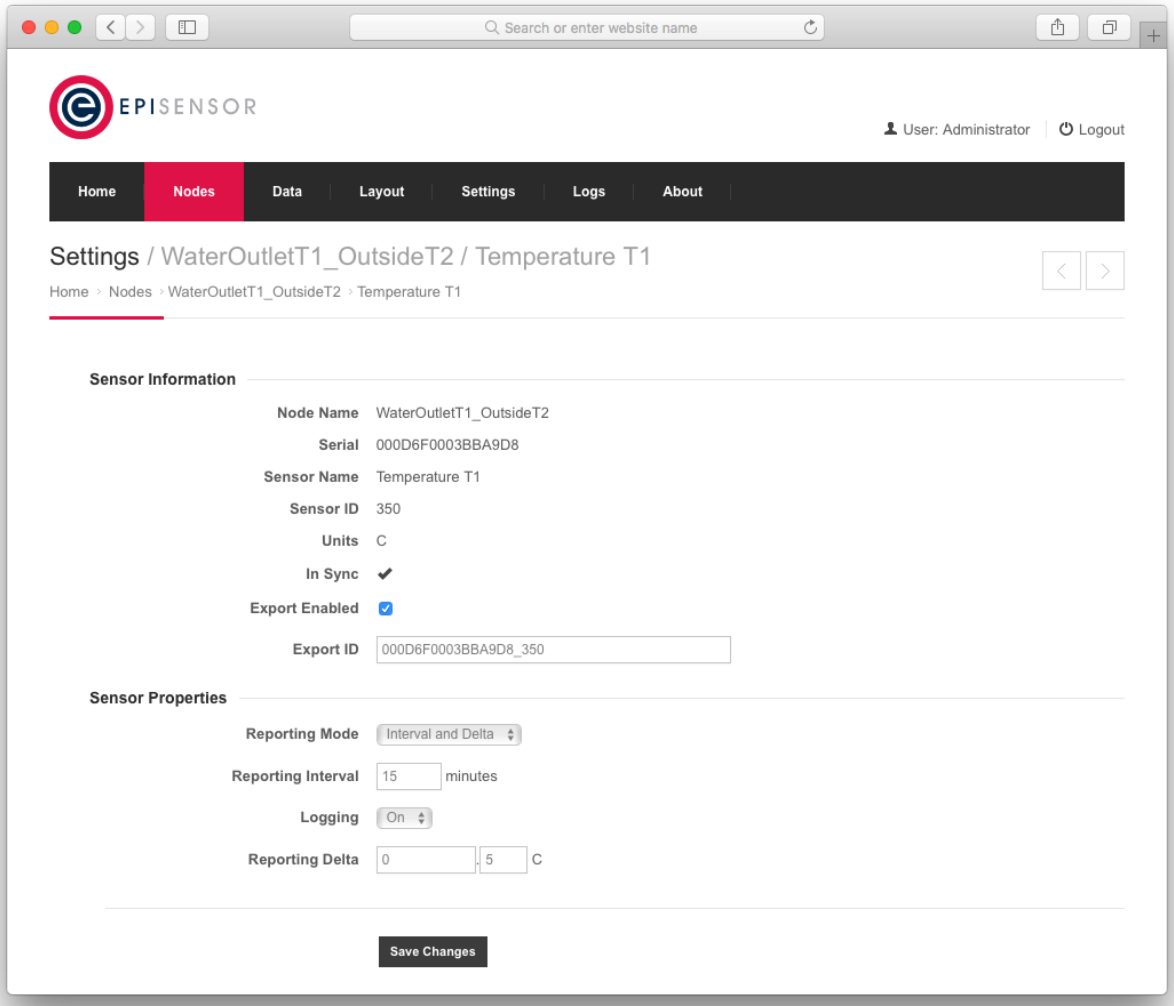


Figure 13 - Sensor Settings Page

Sensor Information

Node Name: The name of the node that this sensor belongs to (as assigned by the user on the Nodes → Settings page or by default the serial number of the node).

Serial: The serial number of the node that this sensor belongs to.

Sensor Name: The human readable name associated with this sensor.

ID: The sensor ID number. Each sensor type has a unique ID.

Units: The units of data the sensor reports data in.

In Sync: This flag indicates if there are over-the-air commands pending for this sensor. Over-the-air commands are issued as a result of an "Action" command being sent using the drop down list on the Nodes → Settings page, or from this page, or by changing a setting. If there is a command pending, the following icon will be shown:

Export Enabled: Shows whether or not this sensor is enabled for data export. If this check-box is ticked, export is enabled for this sensor. If this check box is not ticked, export is disabled for this sensor. If export is enabled, data received from this sensor will be exported from the Gateway, for example to 3rd party software systems. Export is disabled by default for all sensors.

Export ID: The export ID is a unique identifier that is exported with each data point to identify the source of that data. It can be used in 3rd party systems to define where a particular data feed is coming from. It is only relevant if data export is enabled for a sensor. The Export ID defaults to the node serial number combined with the sensor ID, separated by an underscore (_).

Example	
	The default export ID for the Total kWh sensor (Sensor ID = 333) on the ZEM-61 three phase electricity meter with serial number 000D6F0001A303D4 will be: 000D6F0001A303D4_333

This unique identifier can be used in 3rd party systems to identify this data feed as coming from the Total kWh sensor on the three phase meter with serial number 000D6F0001A303D4. This export ID can be changed from the default value, but must be unique on the Gateway.

Sensor Properties

This section will be populated dynamically based on the properties that the node reports for this sensor. As a minimum set the Reporting Mode, Reporting Interval, Logging and Reporting Delta properties will always be present. If the property is editable, a text box or a drop-down list will be available to facilitate modifying the property value.

If the reporting mode is set to **"Off"**, this sensor will not report data. The available reporting options are shown below. **"Interval only"** reporting will report data points periodically based on the reporting interval. Interval data will not be time-stamped exactly on the minute. "**Snap to clock**" mode forces the sensor to send a data point on the minute.

When using a relatively low-bandwidth wireless sensor network, and especially with large networks of sensors, it is generally better to minimise the amount of data being produced. However, it may also be a requirement to

capture events by reporting data as frequently as possible. To deal with these conflicting requirements, various 'Delta Reporting Modes' are available on all sensors.

"Delta only" mode reports a data point when a change is detected that exceeds the value defined in "Reporting Delta".

Example

If Reporting Delta is set to 5 volts for the RMS voltage sensor on a ZEM-61 three phase electricity meter and a change greater than or equal to 5 volts is detected, the sensor will report a data point. If the voltage continues to change, another data point will be reported 2 seconds later. Reporting at a 2 second interval will continue provided the value continues to change.

This feature allows the system to capture rapid and large changes as if the system had a reporting interval of 2 seconds, while not reporting very large volumes of data while the measured parameter is stable within the delta limits defined.

This facility is useful for monitoring unusual temperature rises, for example when a freezer door is opened, for capturing the inrush starting current of a large motor or for capturing the in-rush current for large incandescent lighting loads.

"Interval and Delta" is a hybrid of Interval and Delta reporting, where data will be reported on the interval, but also if a change is detected.

"Interval or Delta" mode is similar to the above mode, but the interval counter will be reset if a change is detected.

"Live Stream" mode will stream data to the Gateway every second. This mode will ignore the configured reporting interval.

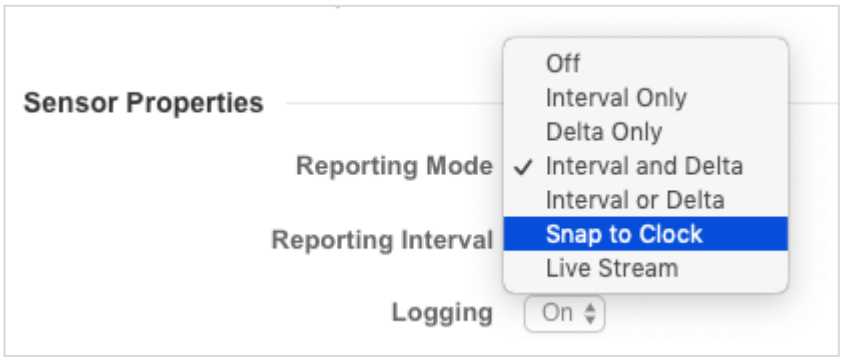


Figure 14 - Reporting Modes

If logging is enabled the sensor will log data when the Gateway is not available and then report the data as soon as the Gateway comes on-line again. Most nodes have a logging capacity of 10,000 data points. To calculate the

amount of time a particular node can log data for, first calculate how many data points will be produced per day for that node, and then divide the 10,000 point buffer by that number to get the number of days the node can log data for.

Example	
	A temperature monitoring node has two sensors: temperature and battery level. The temperature sensor is reporting data every 15 minutes, and the battery level sensor reports once per day. This node will produce 97 data points per day. Dividing the logging capacity (10,000 data points) by the number of data points produced per day = approximately 103 days.

If a node's logging buffer has recorded a large amount of data, it may take some time for this data to be uploaded from the node when the wireless sensor network is available again. All logged data will be uploaded in sequence, starting with the oldest data points. When a data message has been acknowledged, the next data point will be sent. Logged data can be cleared by issuing a "Factory Reset" command from the "Action" menu on the Nodes List page and enabling 'allow join' mode to allow the node to re-join the network after it has been reset.

If a sensor value is editable, this will be facilitated in this section by means of a "Set Sensor Value" text box. For example, this feature can be used to reset cumulative sensors such as kWh, or initialise them to a particular value.

If the property values in this section are incomplete or there is an absence of properties that would be expected for this product (i.e. that the fields are showing a dash "-" symbol), try refreshing all properties for this node using the "Action" drop down list for this sensor on the Node Settings page. It may take a number of minutes for all sensor properties to be refreshed.

Data → Graph View

The Gateway maintains a finite store of sensor data during runtime. The Data view functionality is not intended as an analysis tool but rather as an installation, debug and engineering tool. The stored data may be viewed as a graph. This data store is not persistent through restarts of the Gateway. Restarting the Gateway will mean that the data store is cleared. However, data that is queued for export is not lost (See Settings → Data Export page for more information).

To get started, navigate to the Date → Graph View page. By default, data from the first sensor in the list will be shown on the graph. To view data from another sensor, simply select it from the drop-down list and click 'Build Graph'

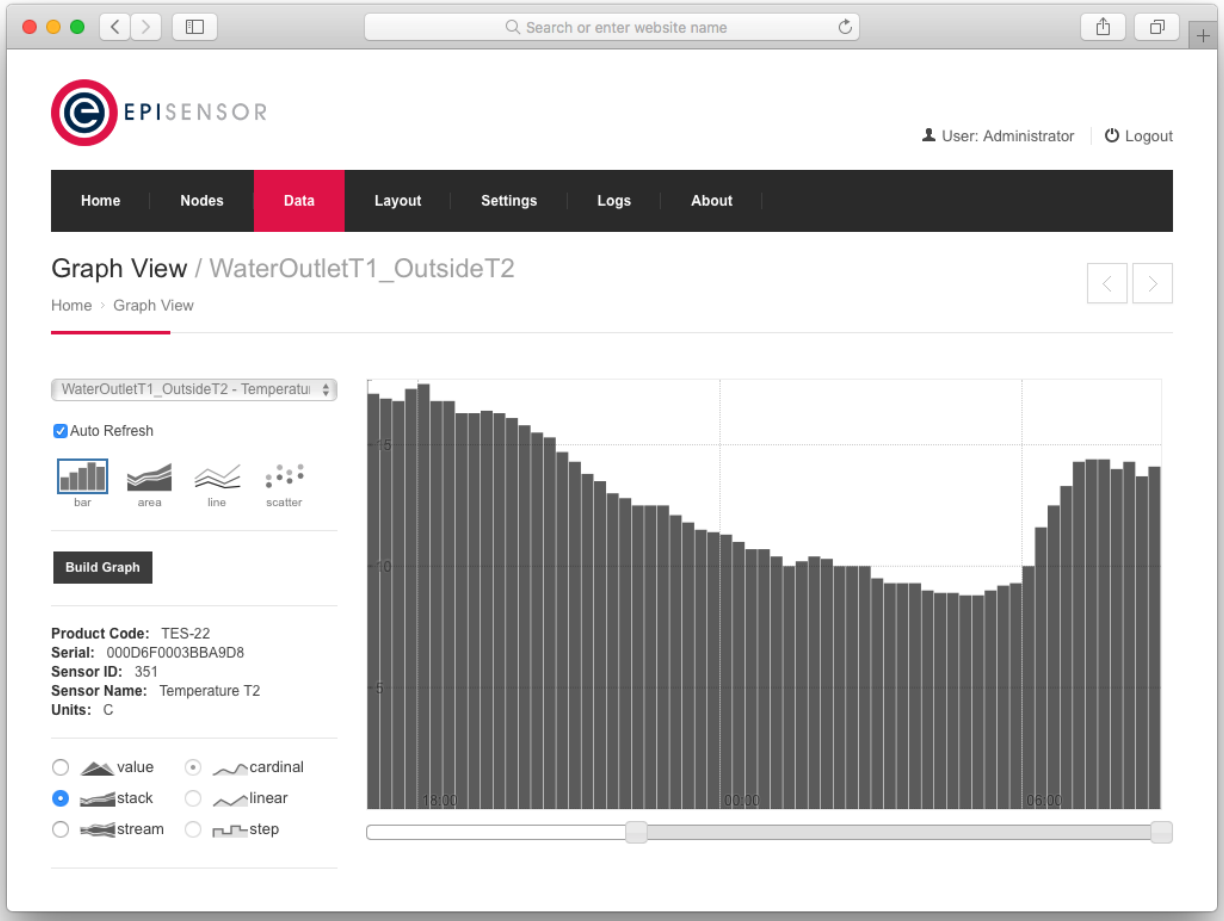


Figure 15 - Graph View Screen

From here the parameters of the data graph may be selected and the graph will be displayed by clicking the "Build Graph" button.

Auto Refresh: Whether or not the graph should be automatically refreshed while the graph page is loaded. If selected, the page will reload every minute.

A node and sensor summary is shown on the left hand side of the page. The graph can be zoomed using the slider control on the bottom of the graph (this feature requires modern browsers). The data point values and timestamps can be displayed by moving the mouse over the graph body.

The type of the graph (choice of bar, area, line, scatter) and the interpolation mode can be selected from the menu on the left of the page, below the node and sensor summary. The default graph type is 'Bar'. These values will be persisted through reloads of the page.

The Data View Graph may also be reached from a link in the drop down menu on each Node → Settings page. In this case the default graph building options are used (default graph type with auto-refresh disabled).

Data → Data File Archive

When data files are not exported (e.g. via HTTP(S) or FTP) and instead stored locally (see Settings → Data Export for more information) the locally stored files are listed on this page. These files can be downloaded from this location. The files are listed in date order with the most recent at the top of the page.

The ZGW-10 Gateway has a minimum of 8GB of on-board flash storage available, approximately 6GB of which is available for data storage.

However, it is not recommended to store large amounts of historic data on the Gateway in this way. This feature is intended to be a temporary store for data that may need to be archived in advance of an energy management software application or server being available. When the Gateway's flash memory is full, data from the wireless sensor network will be lost.

Settings → Data Export

Data received from sensors may be exported outside of the Gateway. Received data points from sensors are stored to the Gateway's file system and then exported to a server. The Gateway is a 'client push' system – this reduces problems associated with Firewall and NAT configuration. The Settings → Data Export Page allows the export of data to be configured.

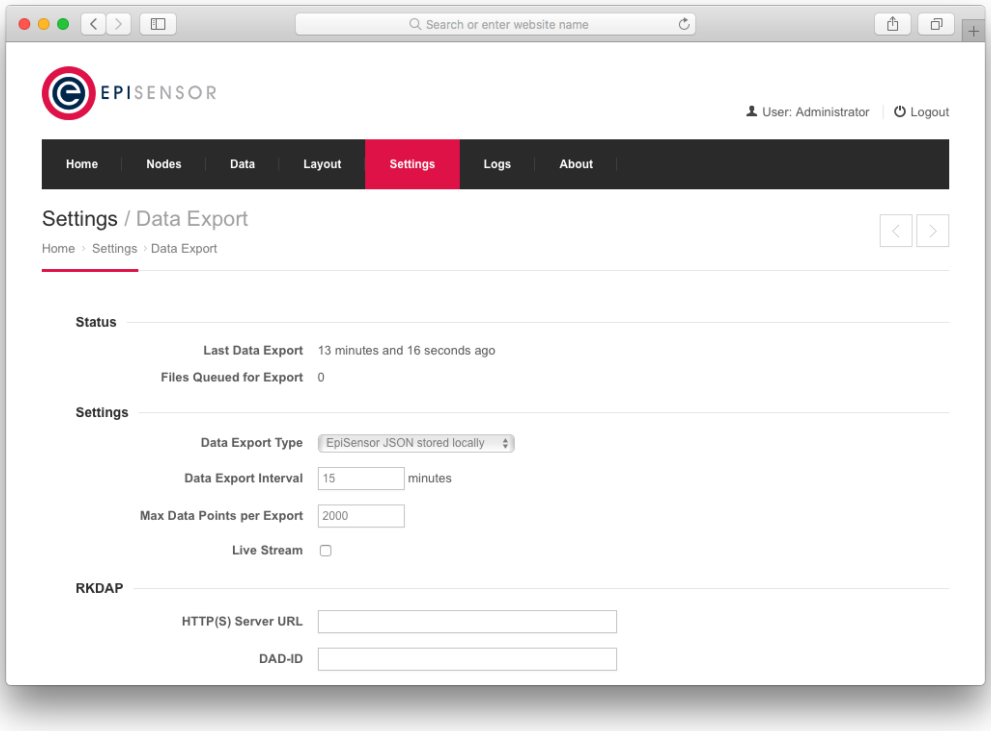


Figure 16 - Data Export Page

Quality of Service

Data in the EpiSensor platform is 'pushed' from each node to the Gateway via a ZigBee wireless mesh network. Nodes take a cautious approach to delivering data - if an acknowledgement is not received by the node in time, a data message will be retried. This usually results in sequential duplicate data messages, i.e. messages originating from the same sensor on the same node, with the same timestamp, one after another.

These sequential duplicate messages are filtered at the Gateway, so only one data point will be exported, however in certain circumstances, depending on the size, layout and traffic on the mesh network, duplicate data messages may not arrive in sequence and will not be filtered at the Gateway level.

This is sometimes referred to as the quality of service, and there are typically 3 levels defined as follows, where messages are delivered:

- At most once
- At least once
- Exactly once

EpiSensor's Gateway is configured to deliver data to the server "at least once". If there are issues with duplicate messages, we recommend running a simple deduplication process, to delete or quarantine data that has the same Export ID, the same timestamp and the same value.

Status

Last Data Export: Show the elapsed time since the last export of data or 'None' if no data has been exported.

Files Queued for Export: Shows how many files are awaiting export. Completed files would be awaiting export if the first attempt to export the file had failed.

Settings

Data Export Type: The format the data will be exported in and the transport mechanism. Currently there are five data formats available:

- RKDAP (JSON)
- EpiSensor JSON
- Edge JSON
- CSV
- JSON

And there are five transport protocols available:

- HTTP(S)
- FTP
- FTPS

- SFTP
- MQTT(S)
- Store data locally

Data Export Type	Description
EpiSensor JSON	Data will be exported in an efficient JSON format with an array of data points. A unique identifier (which defaults to the Gateway's serial number) can be configured. Data can be pushed to a HTTP(S) web service or stored locally.
Edge JSON	Data will be exported in an efficient JSON format, similar to EpiSensor JSON, with an array of data points. A unique identifier (which defaults to the Gateway's serial number) can be configured. Data can be pushed to a HTTP(S) web service or stored locally.
RKDAP	Export data file will be in the proprietary ResourceKraft format and will be exported using HTTP(S) as a transport mechanism, or stored locally.
CSV	Export data file will be in a CSV format with a single data point per row, and will be exported using FTP, FTPS, or SFTP as a transport mechanism, or stored locally.
Multi Column CSV	Export data file will be in a multi column CSV format and will be exported using FTP, FTPS, or SFTP as a transport mechanism, or stored locally.
Extended CSV	Export data file will be in an extended CSV format and will be exported using FTP, FTPS, or SFTP as a transport mechanism, or stored locally.

Figure 17 - Data Export Types Table

Data Export Interval: How often the data will be exported. Default is 30 minutes. Data can be exported as frequently as every minute.

Max Data Points per Export: The maximum number of data points per exported file. If the number of data points accumulated in a file reaches this number the file will be closed and exported even if the 'Data Export Interval' has not elapsed. This is a useful parameter to set if a low bandwidth GPRS internet connection is being used, and it will limit the size of file that will be exported so the export has a better chance of succeeding.

Live Stream: If this checkbox is ticked, the gateway will export as many data points as possible as soon as they have been processed by the gateway. This will, in effect, override the data export interval and maximum data points per export settings above.

EpiSensor JSON

HTTP(s) Character Encoding: The character encoding that will be used for the payloads of JSON data that will be exported. The options are UTF-8 and ISO-8859-1.

HTTP(S) Server URL: URL to use for HTTP or HTTPS. This field is validated as a URI with the following set of acceptable characters: [A-Za-z0-9.:/_-]

Gateway ID: This field is a unique identifier for the Gateway, which defaults to the serial number of the Gateway, but is configurable. Note that the Gateway ID field must also be completed in the case where EpiSensor JSON is stored locally. The Gateway ID field is validated with the following set of acceptable characters: [A-Za-z0-9.' '_-]

EpiSensor JSON Format:


```
{
  "method": "epi_data",
  "ver": "1.0",
  "gateway": "000D6F000DA7FC45",
  "data": [
    {
      "id": "000D6F001113AFCA_462",
      "period": "2018-07-02T21:45:00",
      "value": 22.2
    },
    {
      "id": "000D6F001113AFCA_464",
      "period": "2018-07-02T21:45:00",
      "value": 13.4
    }
  ]
}
```


In this example the Gateway ID is “000D6F000DA7FC45”. There are two data points in this file. The first data point has a timestamp of "2018-07-02T21:45:00" and a value of “22.2”. The time stamp is encoded according to a subset of RFC 3339 and is in terms of UTC. The sensor data value is a floating point value.

This data point originates from a data source with Export ID 000D6F001113AFCA_462. The default Export ID is the node serial number combined with the sensor ID (see Sensor Settings section for more information).

Edge JSON

HTTP(s) Character Encoding: The character encoding that will be used for the payloads of JSON data that will be exported. The options are UTF-8 and ISO-8859-1.

HTTP(S) Server URL: URL to use for HTTP or HTTPS. This field is validated as a URI with the following set of acceptable characters: [A-Za-z0-9.:/_-]

Gateway ID: This field is a unique identifier for the Gateway, which defaults to the serial number of the Gateway, but is configurable. Note that the Gateway ID field must also be completed in the case where Edge JSON is stored locally. The Gateway ID field is validated with the following set of acceptable characters: [A-Za-z0-9.' '_-]

Edge JSON Format:


```
{
   "method":"epi_edge_data",
   "ver":"1.0",
   "gateway":"000D6F00010B768E",
   "nodes":[
      {
         "serial_number":"000D6F000FF14359",
         "data":[
            {
               "id":"24",
               "export_id":"000D6F000FF14359_24",
               "timestamp":"1549018805",
               "value":12
            },
            {
               "id":"25",
               "export_id":"000D6F000FF14359_25",
               "timestamp":"1549018805",
               "value":1.142
            }
         ]
      }
   ]
}
```


In this example the Gateway ID is “000D6F00010B768E”. Data is originating from one node with serial “000D6F000FF14359” and there are two data points from that node in the payload. The first data point has a Unix / Epoch timestamp of "1549018805" and a value of “12”. The type of the sensor data value will depend on the sensor ID that’s producing it.

This data point has a unique key associated with it, called the Export ID, which is “000D6F000FF14359_24” in this case. The default Export ID is a concatenation of the node serial number and the sensor ID (see Sensor Settings section for more information).

CSV via FTP

Host: The FTP site host name or IP address.

Username: The FTP account user name.

Password: The FTP account password. The password can consist of letters [A-Z] and [a-z], numbers [0-9] and the following characters [. ! * ^ _ -]

Remote Directory: The remote directory to store files in. This is an optional field. Leading and trailing backslashes (\ ) are also optional and will be ignored.

FTP Timeout: The timeout to use for all FTP transactions. Default value is 300000 milliseconds.

Note



The FTP server must be configured to accept PASSIVE mode connections to avoid problems with Firewalls on the client side.

An example of a file in CSV format is shown here:

CSV Format:

```
ExportID, Date, Value
000D6F00010B528D_350,2012-10-02T17:29:00,23.8
000D6F00010B755D_462,2012-10-02T17:15:00,0.0
000D6F00010B528D_350,2012-10-02T17:32:00,23.9
000D6F00010B528D_350,2012-10-02T17:35:00,24.1
000D6F00010B528D_350,2012-10-02T17:36:00,23.9
000D6F00010B528D_350,2012-10-02T17:37:00,23.5
```

In this example there are 6 data points. The first data point has a timestamp of "2012-10-02T17:29:00" and a value of “23.8”. The timestamps is encoded according to a subset of RFC 3339 and is in terms of UTC, with an offset as configured in the time and date page of the settings section. The sensor data value is a floating point value. This data point originates from a data source with Export ID: 000D6F00010B528D_350. The default Export ID is the node serial number combined with the sensor ID (see the ‘Sensor Settings’ section for more information). Export ID’s should be noted when configuring data feeds in any other software system.

An example of a file in MultiColumn CSV format is shown here:

Multi Column CSV Format:

```
000D6F00010B74DD_333;12.04.2016 22:00:00;5498.2;12.04.2016 22:15:00;5498.4;
000D6F00010B74DD_333;13.04.2016 04:30:00;5508.9;
000D6F00010B74DD_333;13.04.2016 05:30:00;5511.6;
```

In this example there are 4 data points. The first data point has a timestamp of "12.04.2016 22:00:00" and a value of “5498.2”. The sensor data value is a floating point value. This data point originates from a data source

with Export ID: 000D6F00010B74DD_333. The default Export ID is the node serial number combined with the sensor ID (see the 'Sensor Settings' section for more information). Export ID's should be noted when configuring data feeds in any other software system.

For more information regarding the export protocol definitions contact: support@episensor.com

Note



The file name of the CSV file will be DAT_XXXXXX_YYYYYY.csv where XXXXXX is the Gateway's unique serial number and YYYYYY is a date/time stamp.

RKDAP

HTTP(S) Server URL: URL to use for HTTP or HTTPS as advised by ResourceKraft. This field is validated as a URI with the following set of acceptable characters: [A-Za-z0-9.:/_-]

DAD-ID: Data Acquisition Device Identifier as assigned by ResourceKraft. Please note that the DAD-ID field must also be completed in the case of RKDAP stored locally export type. The DAD-ID field is validated with the following set of acceptable characters: [A-Za-z0-9.' '_-]

RKDAP JSON Format:

```
{
    "method":"dad_data",
    "ver":"1.1",
    "dad_id":"TEST_00055",
    "data":[
        {"id":"000D6F00010B528D_350","period":"2012-09-27T16:26:00","value":22.2},
        {"id":"000D6F00010B7566_520","period":"2012-09-27T16:28:00","value":1.0}
    ]
}
```

In this example the DAD-ID is "TEST_00055". There are two data points in this file. The first data point has a time stamp of "2012-09-27T16:26:00" and a value of "22.2". The time stamp is encoded according to a subset of RFC 3339 and is in terms of UTC. The sensor data value is a floating point value.

This data point originates from a data source with Export ID 000D6F00010B528D_350. The default Export ID is the node serial number combined with the sensor ID (see Sensor Settings section for more information). ResourceKraft needs to be advised of the Export ID's (a.k.a data source ID's) so data feeds can be associated within ResourceKraft Advisor software.

If a data export via FTP or HTTP(S) fails, the export file will be stored on the local file system. The number of files queued for export in this way will be reflected in the “Status” section of this page. Export of these files will be retried periodically, based on the data export interval.

Note	
	Export files saved when a connection to the server is unavailable will not be available for download via the web interface.

If communications fail during a data export, an error will be returned and the data export file will be queued in the local file system to be exported when communications have been restored.

Layout

This module allows users to visualise the last communication path of the mesh network. A network diagram maps the connection path of each node on the wireless sensor network. Together with knowledge of the environment where the system is being installed, the Layout view can be a very useful tool for building strong mesh networks and identifying single points of failure.

End-nodes are coloured pink, while nodes that are routing data are coloured dark grey. Routing nodes can be collapsed by clicking on them. If a routing node has been collapsed it will turn light grey.

The nodes can be dragged and arranged so the labels can be read, but the diagram will default to a natural steady state when the nodes are released. The name of each node will be shown in a label aligned to the top-right corner of each node.

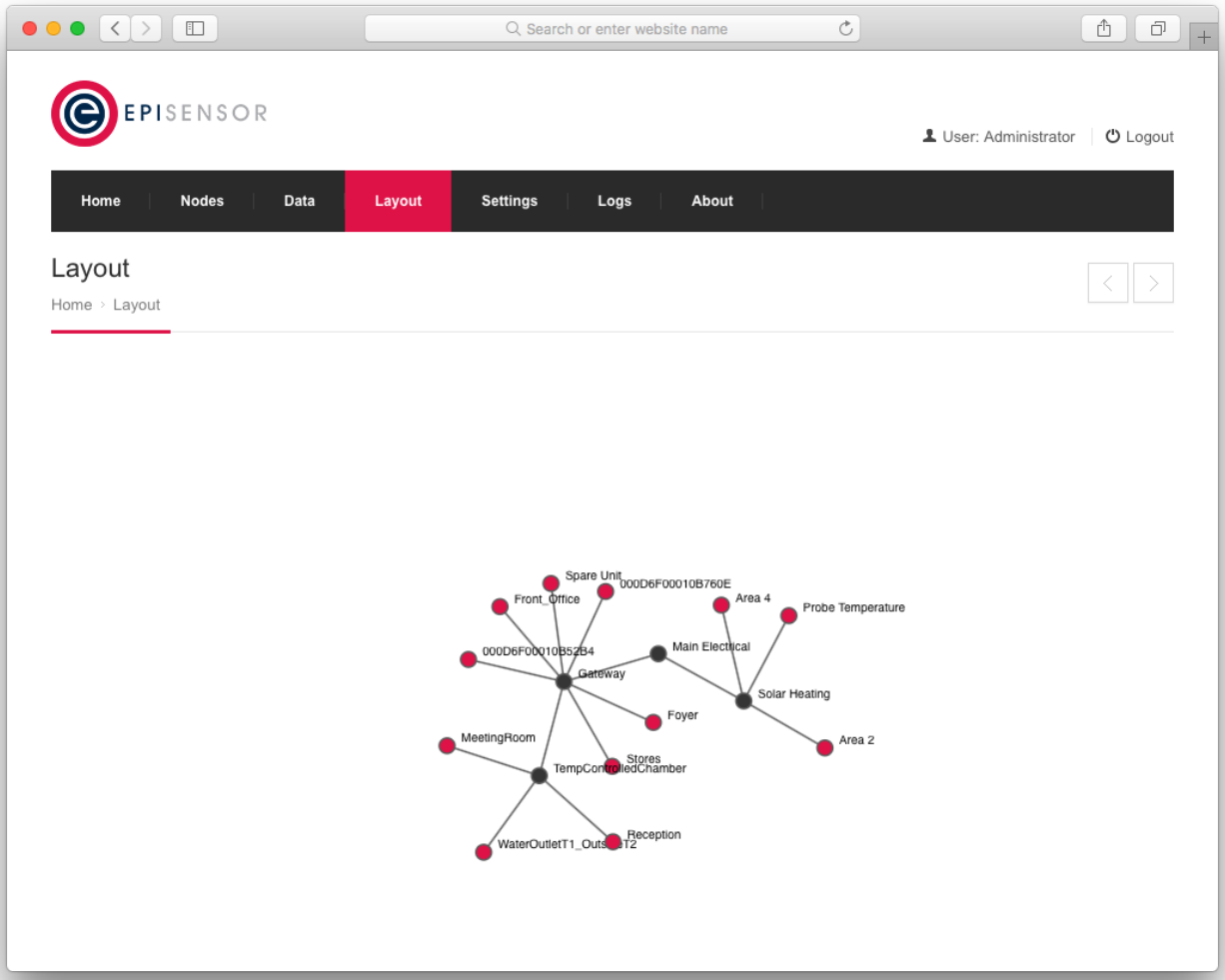


Figure 19 – Layout View Screenshot

Settings → Ethernet

The Settings → Ethernet page shows the status of the Ethernet interface on the Gateway and also allows users to configure the way the Gateway is assigned an IP address.

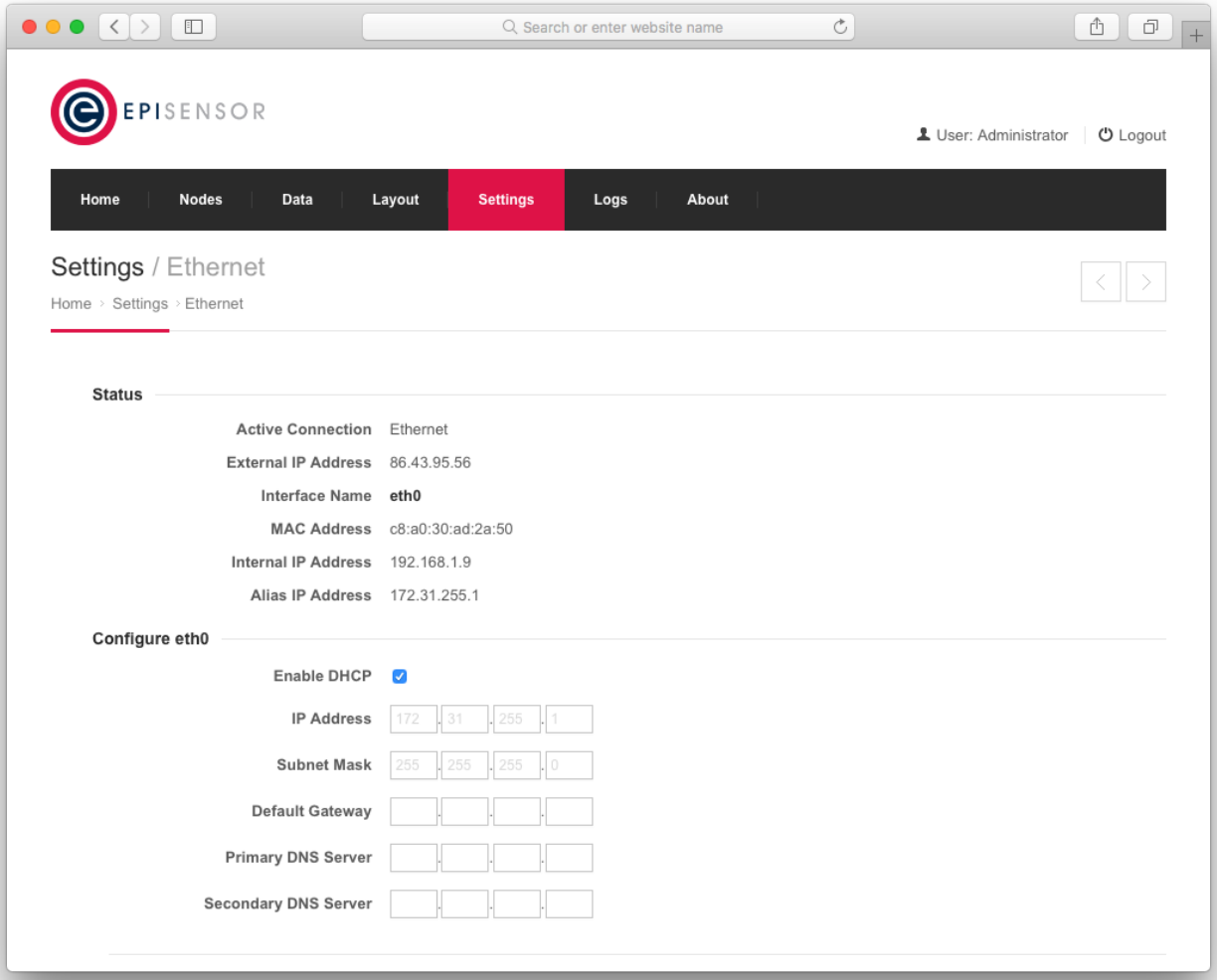


Figure 20 - Gateway Ethernet Settings

The following information is provided as part of the status of the Ethernet interface:

Name: The name of the Ethernet interface, typically eth0, or in the case of the Cellular modem being enabled, br0, because in this mode the Gateway can act as a network bridge.

MAC Address: The hardware address of the Gateway's Ethernet interface. This is a unique way of identifying the gateway hardware.

Internal IP Address: The internal IP address assigned to the named Ethernet interface.

External IP Address: The external IP address assigned to the named Ethernet interface as it appears on the Internet.

Status: This will indicate how the gateway is configured to connect to the Internet, i.e. via Ethernet or via Cellular modem. Please note that if the cellular modem is enabled, it should be disabled (see Settings → Cellular) before attempting to re-configure the Ethernet connection.

The configuration section of this page will be disabled if there is no Ethernet interface found or if the 3G modem is enabled. It is not possible to configure the Ethernet interface in these scenarios.

The following fields are used to configure the Ethernet interface:

Enable DHCP: If this checkbox is ticked, dynamic IP addressing will be enabled for the Ethernet interface. If this checkbox is ticked, the other input fields will be disabled because they are not required. If this check-box is un-ticked, a static IP address will be assigned to the Ethernet interface as defined below.

IP Address: The static IP address to assign. Default factory setting for the gateway is 172.31.255.1

Subnet Mask: The subnet mask to use. Default factory setting for the gateway is 255.255.255.0

Default Gateway: Optional field. If left blank, the default gateway will be derived from the IP Address.

Preferred DNS Server: Optional field. If left blank, no DNS server will be assigned.

Alternate DNS Server: Optional field. If left blank, no DNS server will be assigned.

Settings → Cellular

The Settings → Cellular section shows the status of the embedded Cellular modem (in the case where this is present – this is an optional Gateway component).

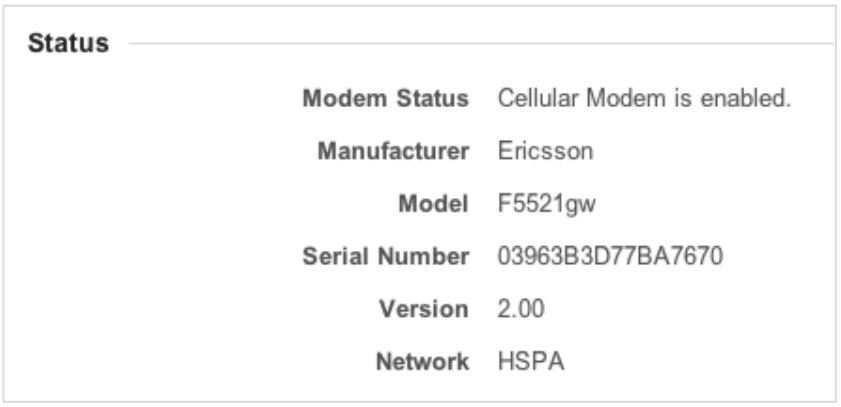


Figure 21 - Cellular Network Status

The following information is provided as part of the status of the Cellular Modem:

Status: Whether or not the modem hardware is detected / enabled.

Manufacturer: Modem manufacturer, as reported by the modem.

Model: Modem model, as reported by the modem.

Serial Number: Modem electronic serial number, as reported by the modem.

Version: The version of the modem installed, as reported by the modem.

Network: The network type supported by this modem.

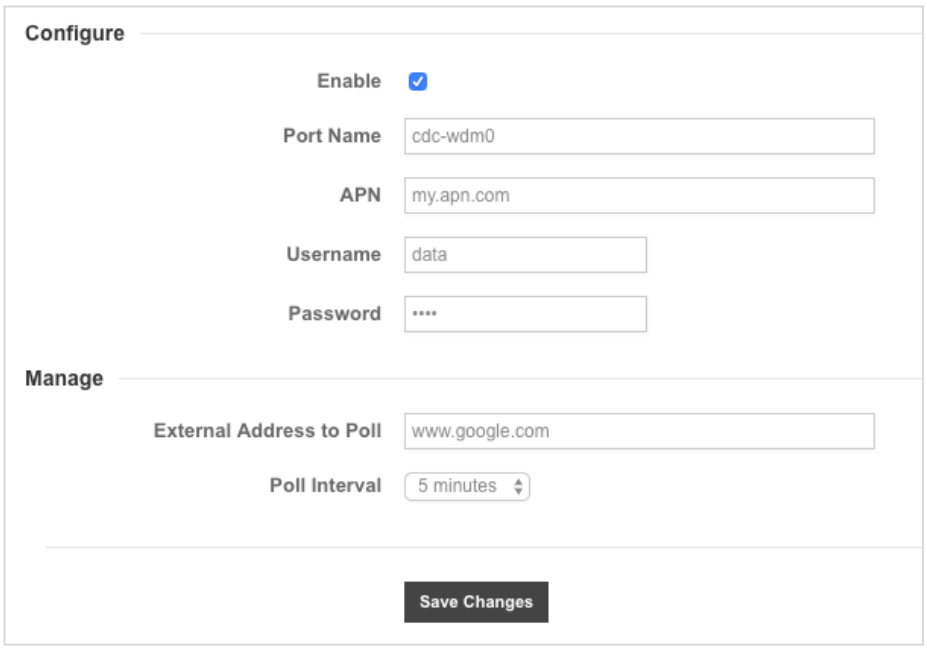


Figure 22 - Cellular Network Settings

The following information is used to configure the 3G cellular network connection:

Enable Cellular Modem: Whether or not to enable the cellular modem. This does not indicate whether or not the Gateway has successfully connected to the cellular network using the modem.

Port Name: Defaults to the USB location of an internal or external USB modem.

APN: The Access Point Name of the cellular provider's data connection. This field is mandatory and may be obtained from the cellular provider. The username is validated with the following set of acceptable characters: [A-Za-z0-9.' '_-].

Username: If the authentication type is 'PAP' or 'CHAP', the username to use for authentication should be entered here. The username is validated with the following set of acceptable characters: [A-Za-z0-9._-].

Password: If the authentication type is 'PAP' or 'CHAP', the password to use for authentication should be entered here. The password is validated with the following set of acceptable characters: [A-Za-z0-9.!*^_-].

When the modem settings are changed, a restart of the Gateway is required. In the case that the modem was disabled by the user, the Gateway will revert back to the factory default of a static IP address of 172.31.255.1 after restart. Thereafter, dynamic IP addressing or an alternative static IP address may be assigned using the Settings → Ethernet interface.

In the case where the modem was enabled by the user and connection to the cellular network was successful, after restart the Gateway will also be accessible via the Ethernet interface at 172.31.255.1. The Gateway will also be accessible via its external IP address (available on the Settings → Ethernet page) assuming this is permitted by the cellular operator.

In the case where the modem was enabled by the user, but connection to the cellular network was not successful, the Gateway will revert back to the factory default of a static IP address of 172.31.255.1 after restart. In this case the external IP address on the Settings → Ethernet page will be shown as “Unknown”.

External Address to Poll: By default, when the cellular connection is active, the Gateway will attempt to open a TCP connection to www.google.com at regular intervals to check that the connection is active and available. If this check fails, the Gateway will attempt to de-dial the connection.

Poll Interval: The rate at which the Gateway will attempt to open a TCP connection to the host configured above.

There are two LEDs on the ZGW-10 which indicate the modem status. The M.2 PWR LED will indicate when the modem is powered. The M.2 NET LED will indicate the modem status as follows:

M.2 PWR LED STATUS	M.2 NET LED STATUS	Meaning
OFF	OFF	Modem is not powered
ON	OFF	Modem is powered but not enabled.
ON	SLOW FLASHING (800ms on / 800 ms off)	Registered on the network but not connected.
ON	FAST FLASHING (200ms on / 200 ms off)	Connection established.
ON	ON	Connection Failed

Settings → Time & Date

The system time may be set from the Settings → Time page. The current system time is shown in terms of Universal Coordinated Time (UTC). The system time is composed of three elements:

Time Zone: Select the required time zone from the drop-down list. The default is UTC.

Date: Select the day, month and year from the drop down lists.

Time: Select the hour minute and second from the drop down lists.

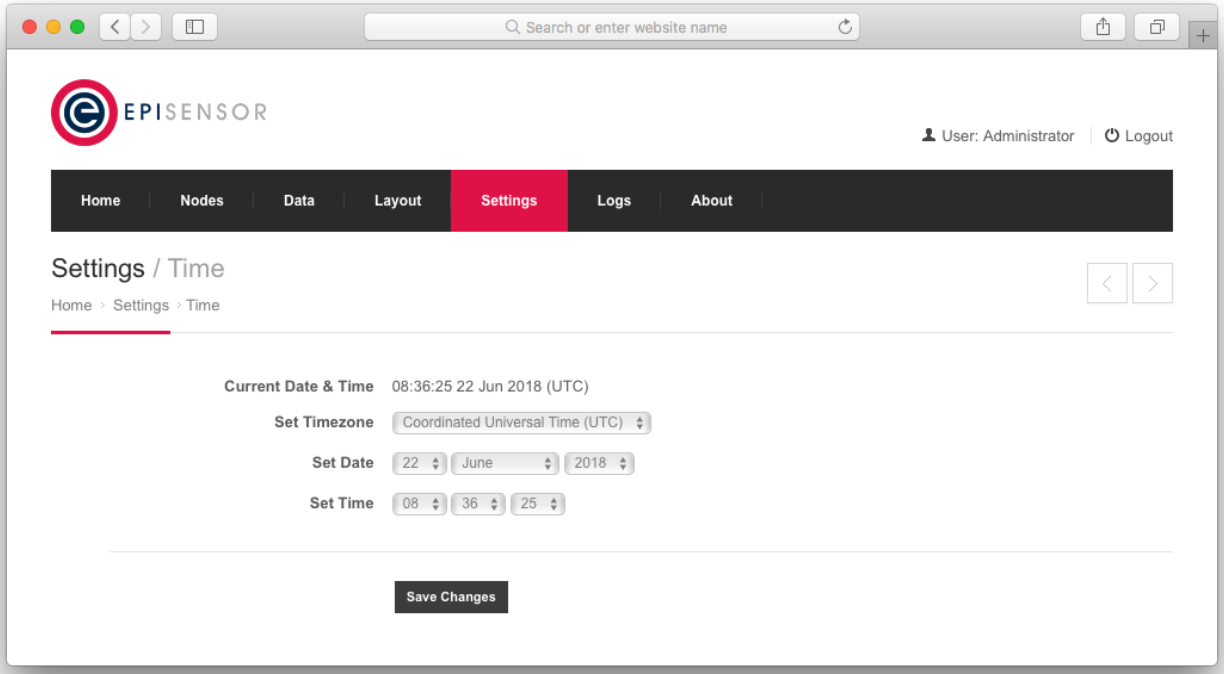


Figure 24 - Time and Date Settings Page

After selecting the time zone, date and time, click 'Save Changes' for the changes to take effect. Changing the system time will result in the Uptime field on the Dashboard page being reset. Changing the system time will also invalidate the "Time Since Last Data Export" field on the Settings → Data Export page and the "Time Since Last Data Point" on the Nodes → List View Page. These values will be corrected when the next data point is receive, or when the next data export succeeds.

Settings → System

The Settings → System page provides access to various system level commands.

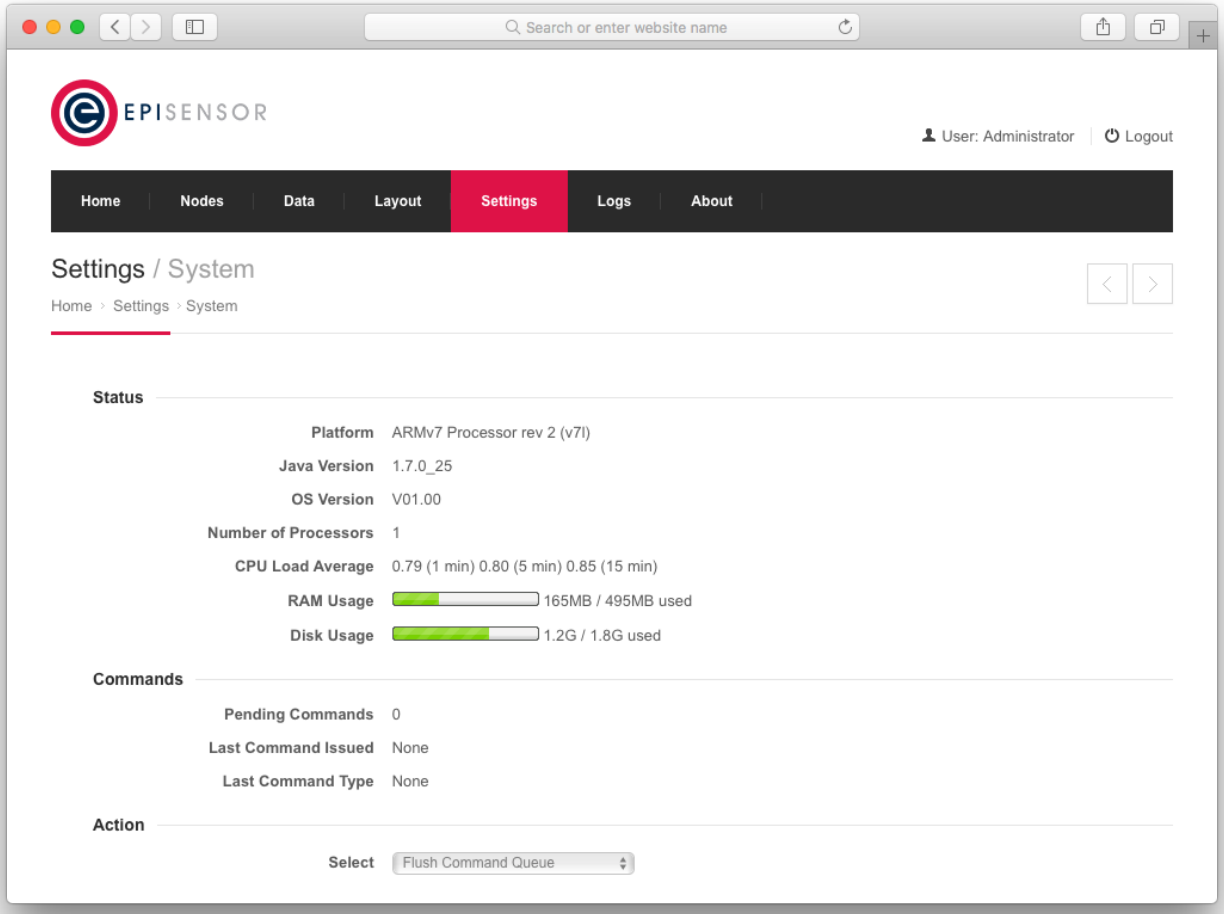


Figure 25 - System Settings Page

Flush Command Queue: Flush the queue of outgoing Gateway commands.

The number of pending commands, the issue date and type of the last issued command are summarised in the Commands section at the start of the page shown above (Settings → System).

Form New Network: This command forms a new wireless sensor network. This will result in all nodes on the existing network being disconnected. After forming a new network, "Allow Join" mode should be enabled to allow nodes to join the new network. Forming a new network should only be done after consultation with EpiSensor support.

Note
Nodes must leave their current network before they will attempt to join a new network.

Restart Gateway Application: Restarts the Gateway software.

Shutdown Gateway Application: Shuts down the Gateway software.

Restart Gateway Hardware: Restarts the Gateway hardware (the Gateway software will be restarted as a result).

Shutdown Gateway Hardware: Shut down the Gateway hardware (the Gateway software will be shut down as a result). If it is necessary to power down the system, if possible this should be done using this command as opposed to unplugging the Gateway.

Factory Reset Gateway: This will return the Gateway to a factory default state. All settings will be lost and passwords will be reset. Use this feature with caution.

Factory Reset ZAP: Reset the Zigbee Access Point to a factory default state. All settings will be lost and all nodes will leave the Zigbee network. Allow join mode will be disabled.

Reset ZAP: Soft-reset the Zigbee Access Point. Allow join mode will be re-enabled after the restart if it was in this state prior to the restart.

Settings → Password

The password for the user that is currently logged in may be changed on this page. New passwords may contain alphanumeric characters (A-Z, a-z, 0-9) as well as full stop (.), underscore (_), dash (-), characters (! ^ *) and a space.

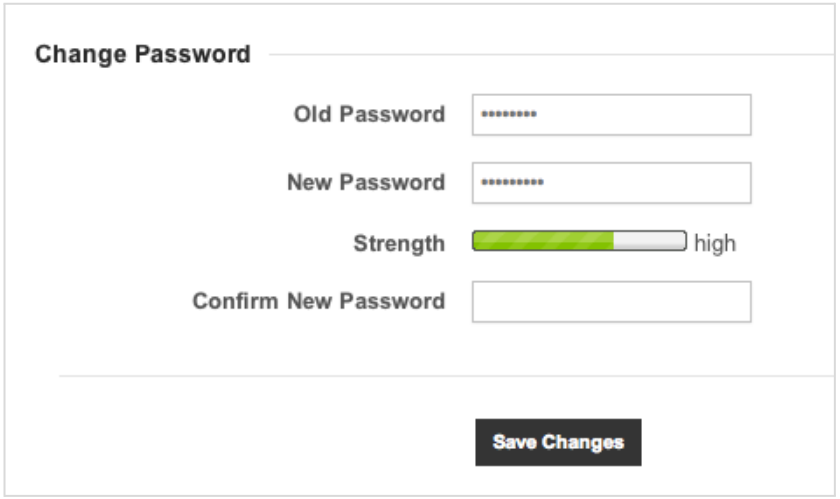


Figure 26 – Password Change Screen

If an invalid password is entered an error response message will be returned. If an incorrect old password, or the new password is incorrectly confirmed an error response message will be returned. If the new password is accepted, a successful response message is returned.

Settings → Sensor Network

This page gives an overview of the wireless sensor network that the Gateway is controlling.

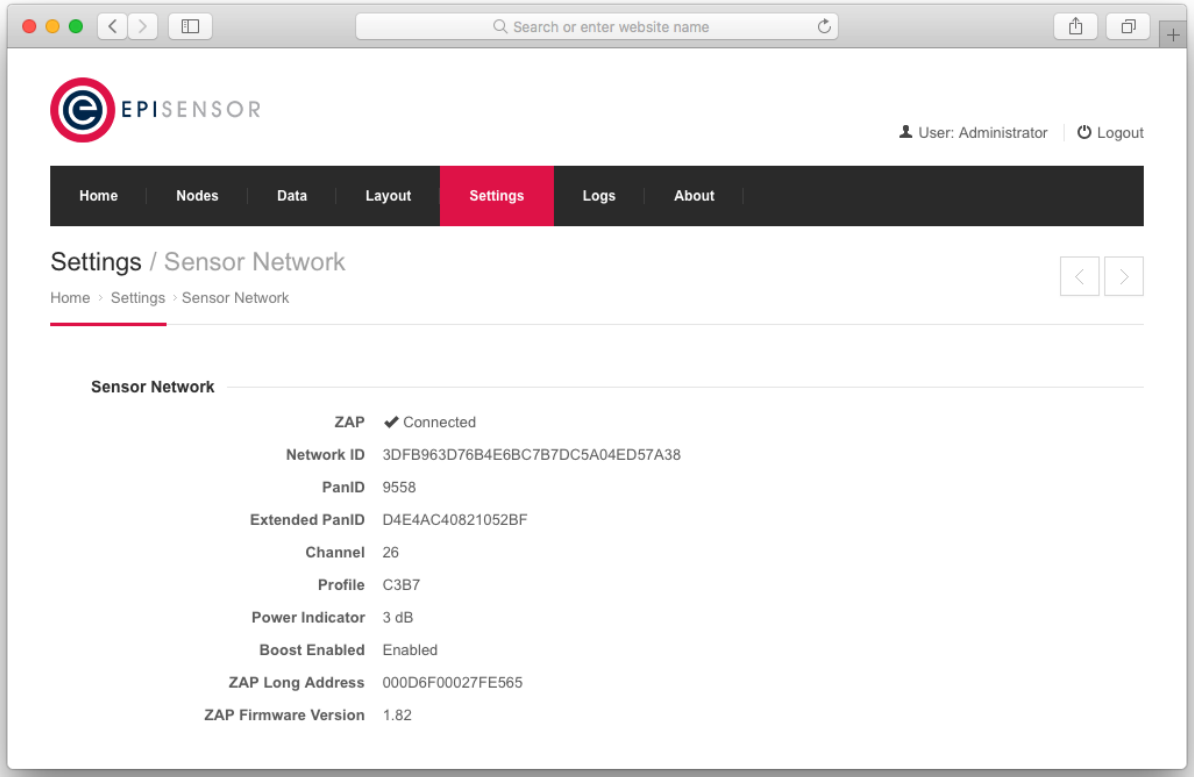


Figure 27 - Sensor Network Screen

ZAP: Whether or not a ZAP (Zigbee Access Point) is connected to the Gateway. If the status is 'Not Connected' and the Gateway is using an external USB Zigbee Access Point, confirm that the USB device is indeed plugged in.

Network ID: The Zigbee Network identifier. If this is showing all zeros, the Zigbee network has not been formed. A new network can be formed by issuing a 'Form New Network' command from the Settings → System page.

Pan ID: Zigbee Personal Area Network identifier.

Extended Pan ID: Zigbee Personal Area Network Extended identifier.

Channel: The channel number (11 - 26) within the 2.4GHz radio band in use by this Zigbee network.

Profile: A unique identifier assigned to EpiSensor by the Zigbee Alliance. It defines the EpiSensor Zigbee network Profile.

Power Indicator: An indicator of the Zigbee radio signal power.

Boost Enabled: Whether or not signal power boost is enabled. If this is enabled, the Zigbee radio signal power will be boosted by 2dB.

ZAP Long Address: The unique serial number of the ZAP. This is also defines the serial number of the gateway (see About → Overview page for more information).

ZAP Firmware: The firmware version of the ZAP. For optimal performance the firmware version of the ZAP should be 1.60 or higher. If the ZAP Firmware version is lower than 1.60 the following alert symbol is shown: For more information on 'Legacy Mode' see the Gateway / Nodes section.

Logs → Log View

The Gateway writes log messages to file. The currently active log file is called "gateway.log"

The logging mechanism may be configured via the Logs → Log Settings page and archived log files may be downloaded via the Logs → Log File Archive page. The Log View Page displays the contents of the most recent log file. The contents are displayed with the most recent log messages at the top of the page.

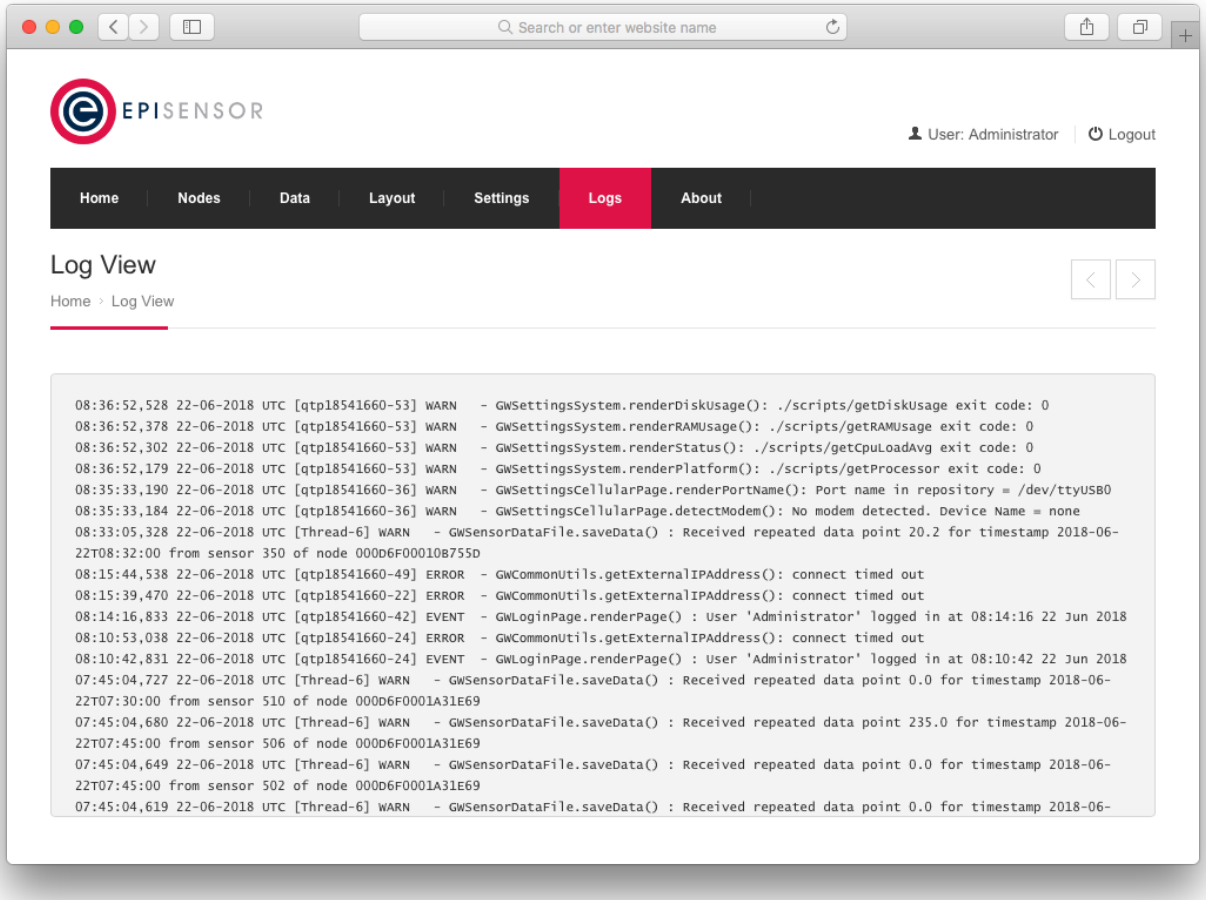


Figure 28 - Log View Page

Each log message will include the following information:

- Time that the log message was generated at.
- Execution thread that generated the message.
- The logging level of this message (e.g. INFO).
- The method that generated the message.
- The actual details of the log message.

Example Log Message
08:14:16,833 22-03-2018 UTC [qtp18541660-42] EVENT - GWLoginPage.renderPage() : User 'Administrator' logged in at 08:14:16 22 Jun 2018

Logs → Log Settings

The logging mechanism may be configured using this page. The current value of each parameter is displayed and the value of each parameter may be reconfigured from this page. To modify the value of one or more parameters enter the new parameter value(s) in the corresponding text box and click 'Save Changes'.

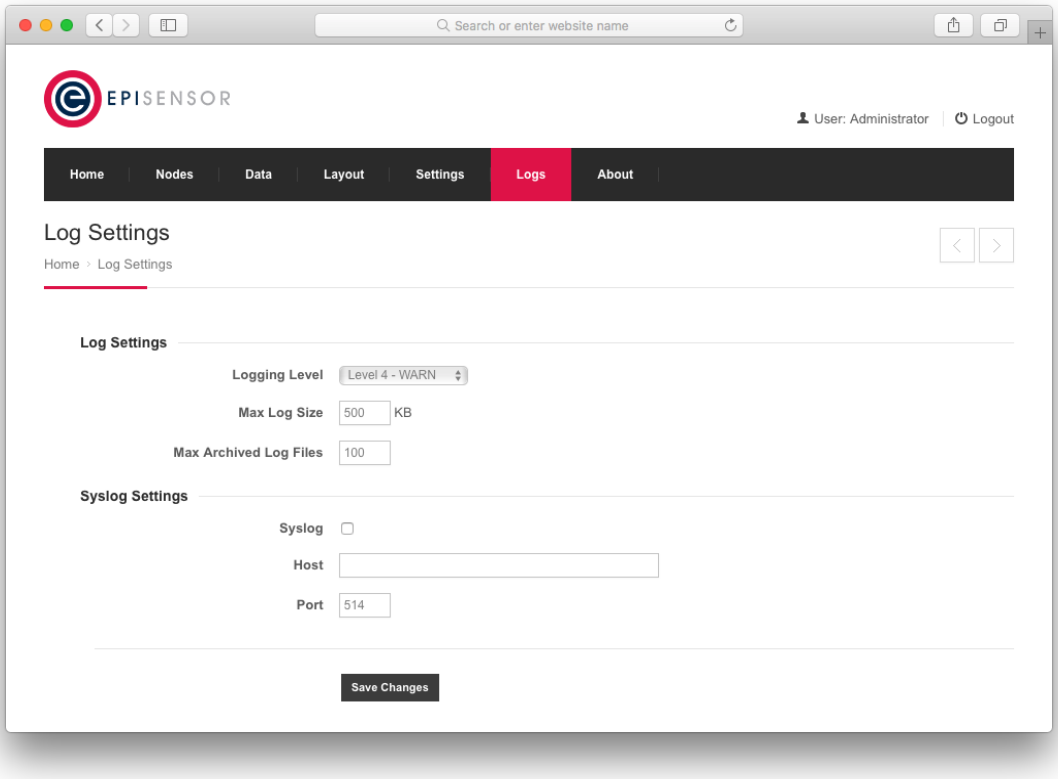


Figure 29 - Log Settings Page

Logging Level: This parameter controls the severity of log messages that will be recorded. There are 7 log severity levels as follows, with Level 1 being the lowest level which records most data, Level 7 being the highest level which records least data:

Log Level	Description
Level 1 - DEBUG	This is the lowest level and is used for debugging of the software. This log level is only available to “Engineer” level users.
Level 2 - INFO	This is the level used for non-error messages regarding the execution of the software processes.
Level 3 - SERIAL	This level is used to isolate just the incoming and outgoing serial communication traffic (between the Gateway and the ZAP).
Level 4 - WARN	This level is used for warning messages from the gateway application.
Level 5 - ERROR	This level is used for error messages from the gateway application.
Level 6 - FATAL	This level is used for fatal errors and software exception messages from the Gateway application.
Level 7 - EVENT	This level is used for significant events occurring in the gateway e.g. start-up, shutdown, nodes joining the network.

Figure 30 - Table of Logging Levels

If Level 1 - DEBUG is selected, the log file will contain log messages of severity DEBUG and higher. If Level 2 - INFO is selected, the log file will contain log messages of severity INFO and higher. If Level 7 - EVENT is selected the log file will contain log messages of severity EVENT only.

Max Log Size: The maximum size in Kilobytes that the log file can grow to. When the log file reaches the size defined here, it will roll-over. The default value is 900 KB. See also Max Archive Log Files.

Max Archived Log Files: The maximum number of log files that will be archived. The default value is 100. When the currently active log file reaches the configured Max Log Size, it will rollover and start a new “gateway.log”. If the Max Archived Log Files → 0, the old “gateway.log” will be renamed to “gateway.log.1” and so on. The next time the currently active log file reaches the configured Max Log Size, it will rollover again and start a new “gateway.log” file.

The maximum amount of disk space used by log files on the gateway will be equal to (Max Archive Log Files + 1)*(Max Log Size) in kilobytes. Setting the log level at a level higher than Level 3 - SERIAL is recommended to conserve disk space and avoid a large amount of data being written to the file system.

Logging to a Syslog server may also be enabled and configured with the following fields:

Syslog: If this is enabled, the Gateway will send log data to a syslog server. If this box is not checked, export of logs to a syslog server will be disabled.

Host: The Syslog server host name or IP address.

Port: The Syslog server port number. The default is port 514.

Logs → Log File Archive

The currently active log file (gateway.log) and all archived log files are listed on this page. The files can be downloaded from this page. The files are listed in date order with the most recent at the top of the page.

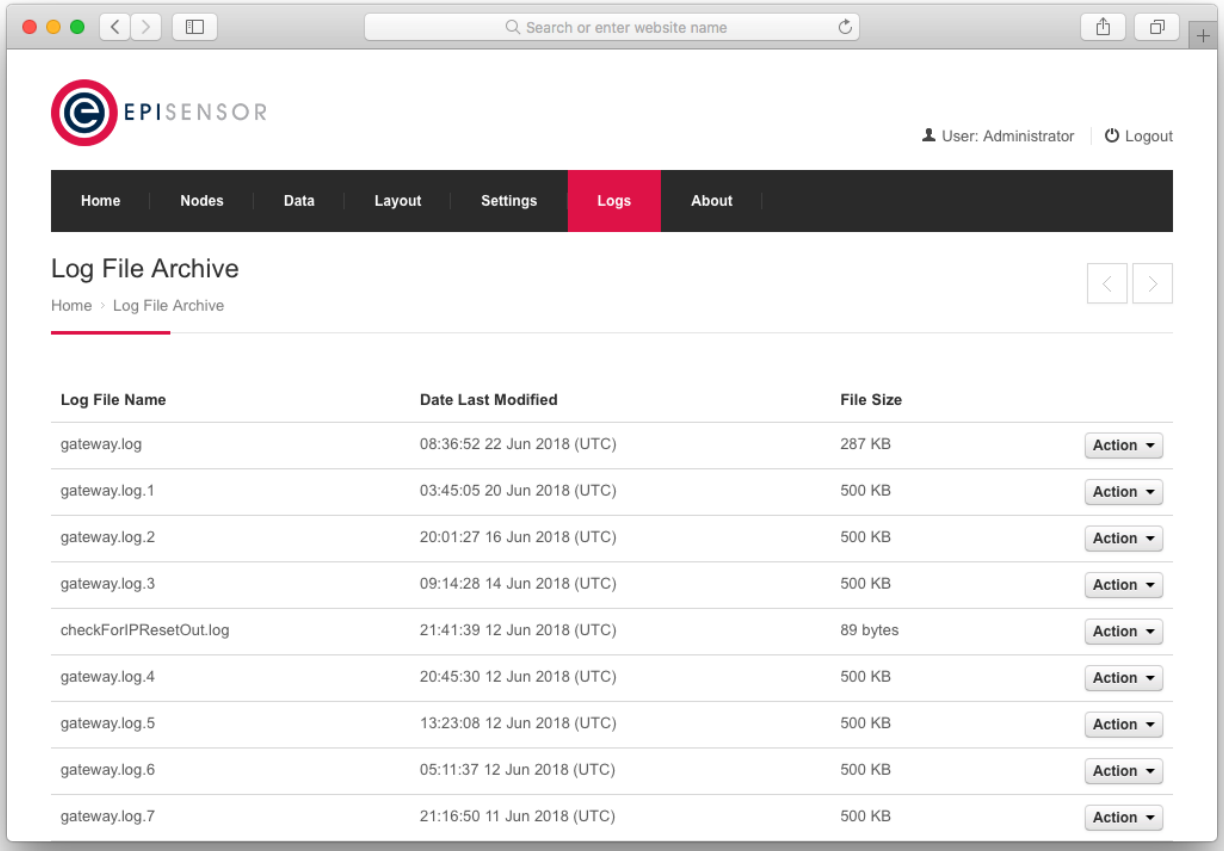


Figure 31 - Log File Archive Page

About → Overview

The Overview page in this section presents general information regarding the Gateway.

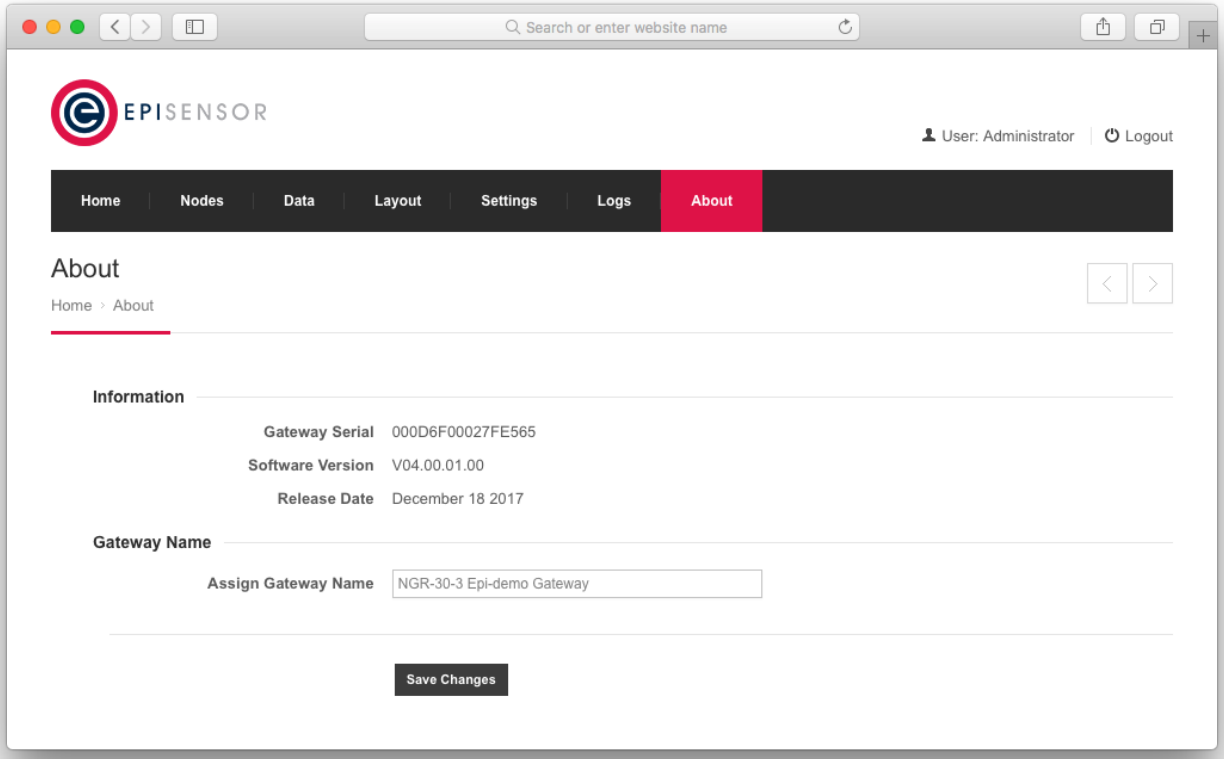


Figure 32 - About Page

Gateway Serial: This is the serial number of the Gateway. It is derived from the serial number of the ZAP that is connected to the Gateway. The Gateway serial number is used as a unique identifier in each data export file name. See the 'Data Export' section of this document for more information.

Example
DAT_XXX_YYY.zzz (where XXX is the gateway serial number, YYY is the file time stamp and zzz is the file type specific extension)

Software Version: This is the Gateway software version currently installed.

Release Date: This is the release date of the Gateway software version currently installed.

Assign Gateway Name: The name assigned to this instance of the Gateway. The default name is "Gateway". The user may assign another name as required by entering the name in the text box and clicking the 'Save Changes' button at the bottom of the page.

Alphanumeric characters (A-Z, a-z and 0-9) are allowed as well as spaces, dashes (-) and underscores (_). If an invalid Gateway name is entered in the text box, an error response message will be displayed and the Gateway name will not be changed. Otherwise, a successful response message will be displayed. The Gateway name assigned will appear in the footer of each page, except the Login page.

Ordering Information

EpiSensor products are available to order directly or via EpiSensor's distribution partners. The following table lists the available ZGW-10 options.

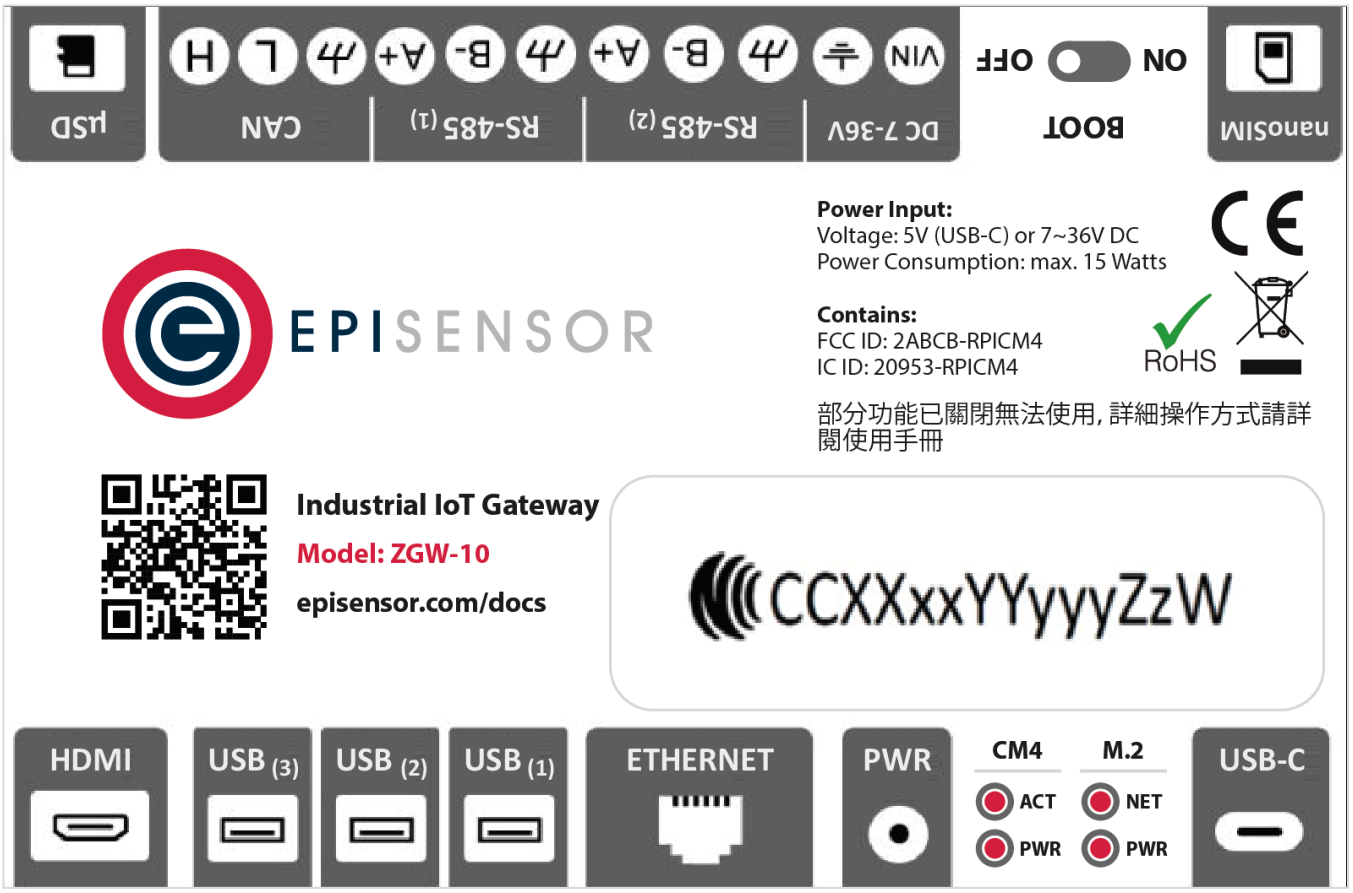
Product Code Example:		ZGW -	10 -	DZ -	4G -	WB -	NU -	EU
Product Line	**ZGW:** IoT Gateway							
Version	**10:** first generation ZGW **20:** second generation ZGW							
ZigBee	**DZ:** external (USB dongle) ZigBee Radio **UZ:** on-board (UART connected) ZigBee Radio							
Cellular / GPS	**4G:** on-board (M.2 connected) 4G modem based on Simcom SIM7600G **NC:** no cellular							
Wi-Fi / Bluetooth	**WB:** on-board Wi-Fi / Bluetooth **NW:** no on-board Wi-Fi / Bluetooth							
Hardware UI	**WU:** hardware user interface (eInk) **NU:** no hardware user interface							
Power Supply	**EU:** power adapter suitable for use in the EU (Europlug type C) **UK:** power adapter suitable for use in the UK **NA:** power adapter suitable for use in North America and Canada							

SKU	Description
ZGW-10-DZ-4G-WB-NU-UK	Ethernet, ZigBee USB dongle, 4G cellular, Wi-Fi / Bluetooth, no display, UK power supply
ZGW-10-DZ-4G-NW-NU-UK	Ethernet, ZigBee USB dongle, 4G cellular, no Wi-Fi / Bluetooth, no display, UK power supply
ZGW-10-DZ-NC-NW-NU-UK	Ethernet, ZigBee USB dongle, no cellular, no Wi-Fi / Bluetooth, no display, UK power supply
ZGW-10-DZ-NC-WB-NU-UK	Ethernet, ZigBee USB dongle, no cellular, Wi-Fi / Bluetooth, no display, UK power supply
ZGW-10-DZ-4G-WB-NU-EU	Ethernet, ZigBee USB dongle, 4G cellular, Wi-Fi / Bluetooth, no display, EU power supply

ZGW-10-DZ-4G-NW-NU-EU	Ethernet, ZigBee USB dongle, 4G cellular, no Wi-Fi / Bluetooth, no display, EU power supply
ZGW-10-DZ-NC-NW-NU-EU	Ethernet, ZigBee USB dongle, no cellular, no Wi-Fi / Bluetooth, no display, EU power supply
ZGW-10-DZ-NC-WB-NU-EU	Ethernet, ZigBee USB dongle, no cellular, Wi-Fi / Bluetooth, no display, EU power supply

Compliance Label

There is a compliance label on the front of the ZGW-10 with important compliance and regulatory information.



The label material is white PVC with permanent adhesive and matte overlaminate. The following table lists the certification and safety symbols that appear on the certification labels of the EpiSensor ZGW-10. Please refer to it for a definition of each symbol.

Symbol	Name	Description
CE	**CE Mark**	This marking certifies that a product has met EU consumer safety, health or environmental requirements.

	**WEEE Symbol**	The directive imposes the responsibility for the disposal of waste electrical and electronic equipment on the manufacturers of such equipment.
	**RoHS Directive**	Restriction of Hazardous Substances Directive restricts (with exceptions) the use of six hazardous materials in the manufacture of various types of electronic and electrical equipment.
	**NCC**	This symbol notes that the product has been approved for use in Taiwan by the NCC.

EpiSensor products are not suitable or specifically designed, manufactured or licensed for use in military, aviation, powerplant, medical or in other inherently dangerous or safety critical applications.

Region Specific Features

Some features of the ZGW-10 are not available in all regions worldwide. The following tables list features that are not available / disabled in each region:

Taiwan
• Micro SD Card slot • FAN header • Partial GPIO • CSI Camera Port • HDMI Port

Troubleshooting & Support

If you are experiencing problems with your Gateway or any other part of your EpiSensor system, or you notice something unusual - please contact EpiSensor support at the following email address, phone number or via live chat on our website.

- Email: support@episensor.com
- Tel: +353 61 512 500
- Website: http://episensor.com

For customers and partners who are deploying systems in business-critical environments, there are a number of support packages available that offer a higher level of service and response time. For more information on EpiSensor Premium Support, visit: http://episensor.com/premium-support/

Warranty

All EpiSensor products and provided with a 365 day limited warranty effective from the shipping/invoice date of an order. During the warranty period, under the conditions of normal use, EpiSensor will repair or replace any product that has a manufacturing defect.

Warranty can be extended by up to 4 years within 30 days of a purchase. For more information on warranty, visit: http://episensor.com/warranty/

Glossary

Definitions for terms and abbreviations used in this document are listed in the following table:

Term	Description
Sensor	Describes a feed of data within the EpiSensor system
Node	Used to describe a physical EpiSensor product
Gateway	The central computer that managed the EpiSensor system
ZigBee	IEEE 802.15.4 Wireless communications standard that EpiSensor nodes use
WSN	Wireless Sensor Network
Reporting Mode	Defines how an EpiSensor node should report data to the Gateway
Reporting Interval	The length of time between each data point produced by a node
Snap to Clock	Reporting mode where data is 'snapped' to the nearest 1 minute / 5 minute / 15 minute interval etc.
Interval and Delta	Reporting mode where data is produced when the reporting interval has elapsed, unless a change is detected
Allow join mode	A mode that can be enabled on the Gateway that allows new wireless nodes to join