R9 Technology Online Portal User Guide

June 2020

Release 1.1

R9 Technology

17217 Waterview Parkway Suite 1.202Y

Dallas, TX 75252

www.r9technology.com

Document Revisions

Date	Version Number	Document Changes
06/10/2020	R1.1	First release of document

Table of Contents

1 Introduction

This manual describes R9 Technology's IoT web browser interface operation, and primary IoT hardware devices. The web interface, or "portal" is used by a customer to setup, monitor, and manage their system. The browser-based portal allows customers to interact with their collected data and modify the system operation including configuring alerts and customizing weekly or monthly reports. A web browser such as **Google "Chrome"** is recommended for use with the R9 portal system.

The two physical IoT devices that you will likely be using are:

1. G200 Gateway device (Picogate). This device is the main control element and acts as a bridge between your local sensor devices and the internet.
2. SN400 sensor node (Piconode). This device accumulates cabled sensor data, and forwards it to the gateway using a wireless connection. A monitored location should typically implement one gateway, and one or several nodes.

Various sensor types are available to connect to the SN400 sensor node (for example: temperature, humidity, door closure, light level, tank level, etc.). A typical system includes one G200 gateway and one or several SN400 node devices. The gateway establishes a wireless connection to a cellular carrier network (T-Mobile, AT&T). Therefore, no ethernet or WIFI connection is required. The SN400 nodes are the endpoints for the R9 system. These devices are distributed throughout the customer site, and placed near equipment that requires monitoring. The SN400 devices have four sensor inputs, therefore it is possible to have one SN400 monitor several pieces of equipment. Specific cabled sensor devices (for example, temperature, humidity) are then plugged into the SN400 node and routed into the equipment that is being monitored. The SN400 node communicates with the G200 gateway using a 915Mhz ISM frequency band wireless network.

Once powered and configured in the portal, the G200 and SN400 devices will communicate with each other and establish a local sensor network. No additional user input is required to establish the network. Both the G200 and SN400 sample data on a 15-minute collection interval (for the "Safezone" application). Therefore, data in the portal will always be displayed using a 15-minute interval.

Before your wireless monitoring system can be used, the following (setup) steps must be completed in the order indicated below. This manual will guide the user through the setup process.

1. User Account Setup and Registration
2. Adding G200 Gateway(s) to the web portal
3. Adding SN400 Node(s) to the web portal
4. Configuring ports for the SN400 node(s)
5. Configuring the web portal (alerts, reports, subscription)

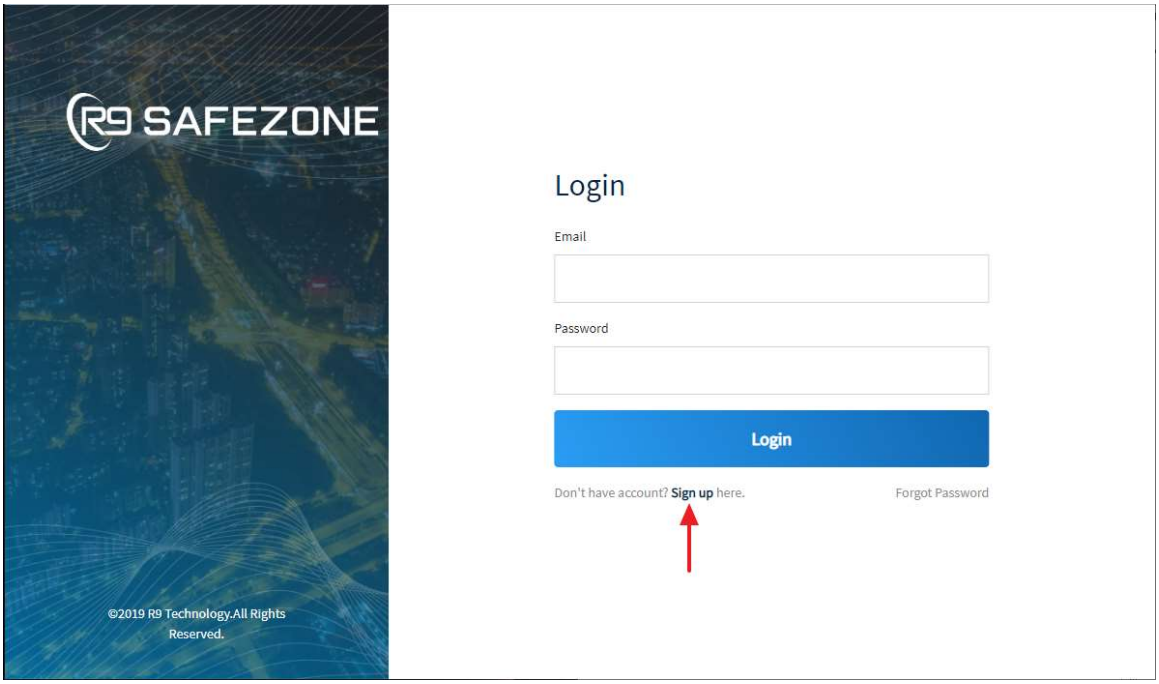
Note that only steps 1-3 have to be completed when you are setting up and testing the wireless performance of your hardware for the first time. Steps 4 and 5 can be completed at a later time after the hardware operation is verified.

2 R9 Technology User Account Setup

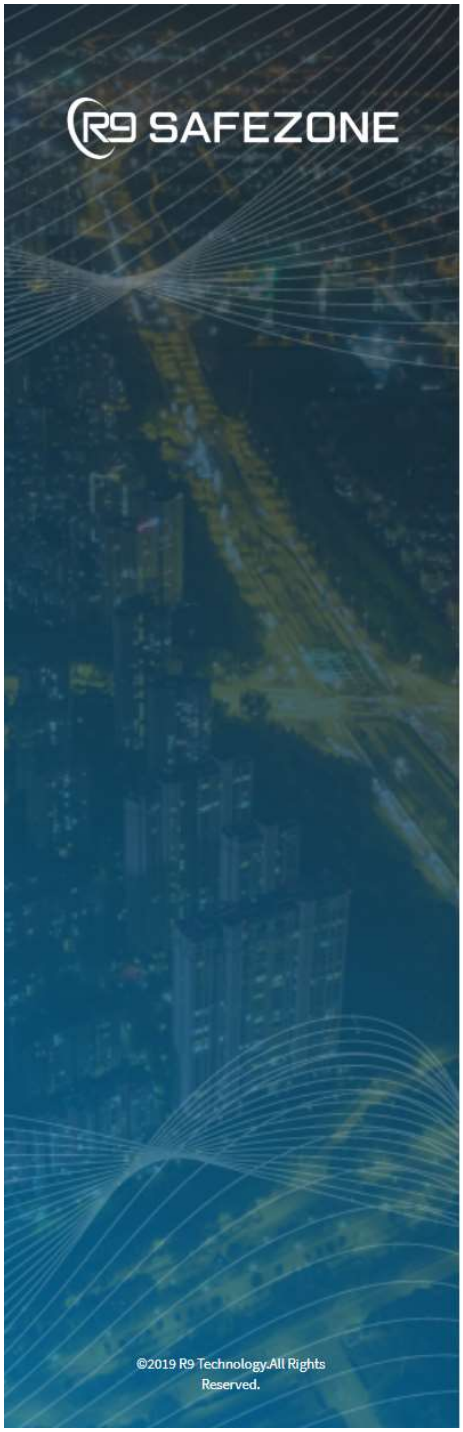
First time users are required to create a user account to configure their system. The R9 portal provides a "new user" option that streamlines the registration and setup process. The interface is designed to guide the user "step by step" to expedite gathering the required system information. New users should always use this option.

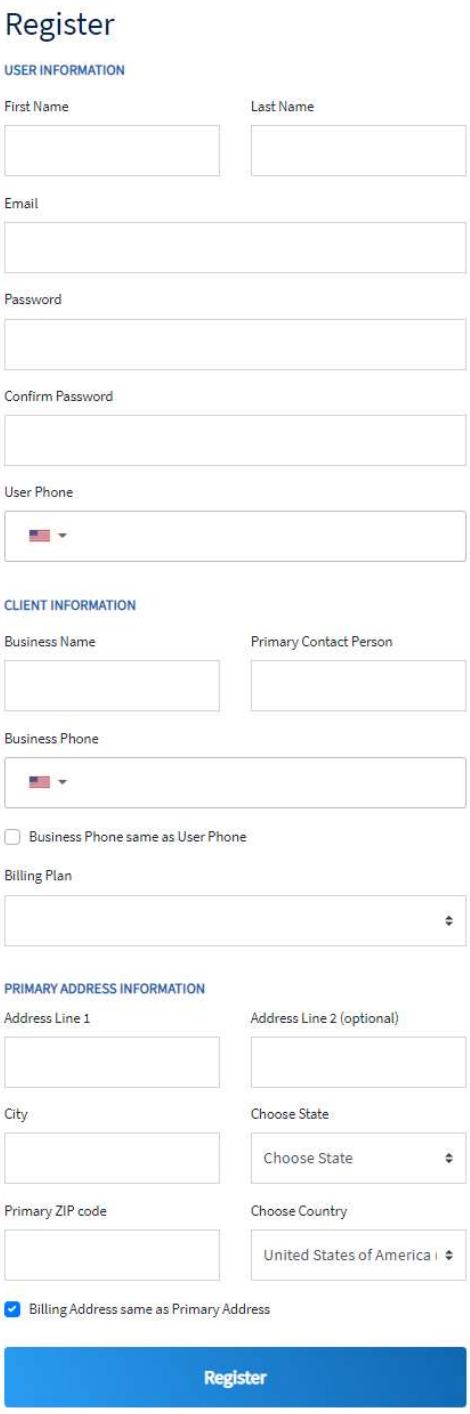
For ongoing system operation and modifications, users can manually edit their system information after logging into the R9 portal system.

Navigate to the customer login page located at https://portal.r9technology.com or select the "Portal" menu from R9 Technology's webpage at https://r9tech.com.



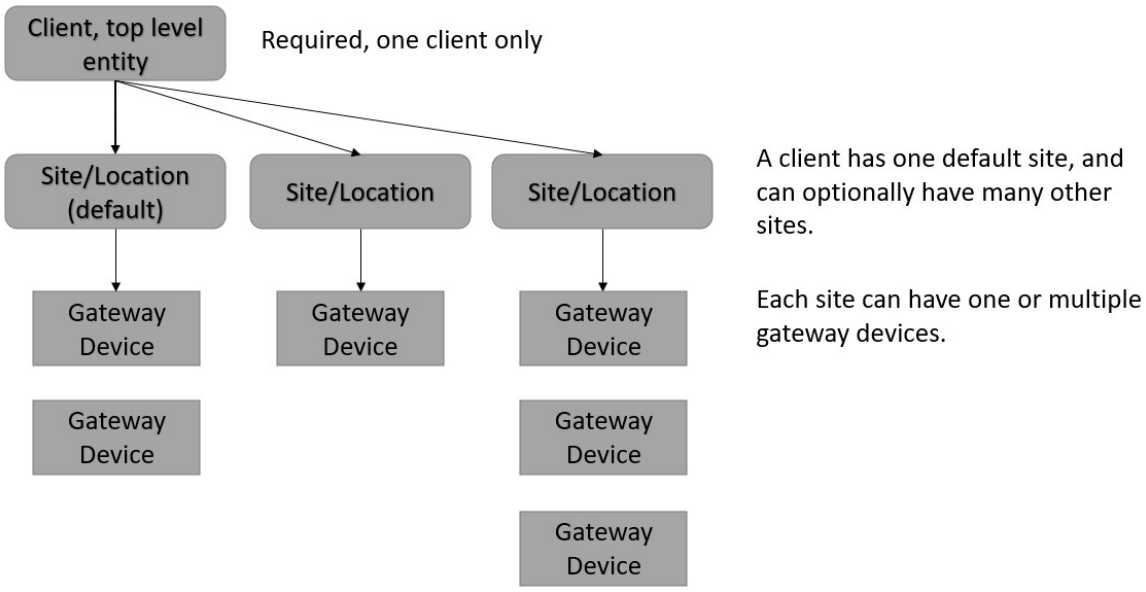
1. Click “Sign up” to start the user account setup. The information entry screen shown below will be displayed, and will be used to enter business name and address information.





2. Fill in the required “User” and “Client” information by following the instructions on the screen. For this menu, **user information,** refers to a person that is the owner,

manger, or owner's representative of the "top level" entity (business) that will be implementing the R9 system. For this menu, **client information,** refers to the business name and address of the "top level" entity that will be implementing the R9 system, possibly at multiple geographic locations and even for different business types or names. The diagram below gives some insight into the organization of user information in the R9 portal. Note that at this point, you are entering DEFAULT information for the business name and address of the "top level" client entity; additional business name and address information is not **required** for locations (these can be optionally entered later).



3. Click the "Register" button. The user registration activity is now completed.
4. An email will be sent to the email address provided. Please follow the link contained to validate your account.
5. By clicking the activation link, the browser will be redirected to the Login page. Login into the system to begin the hardware configuration activity.

It is recommended that the "User Phone" number (in the user information section) be for a smart phone that can receive SMS text messages. The "User Phone" will be used by default as the first phone number for SMS text messaging (alerts); this number can be changed or deleted at a later time in the "alerts" menu. Note that in the R9 system, *location* and *site* refer to a physical business address and are used interchangeably.

3 Adding Hardware to the web portal

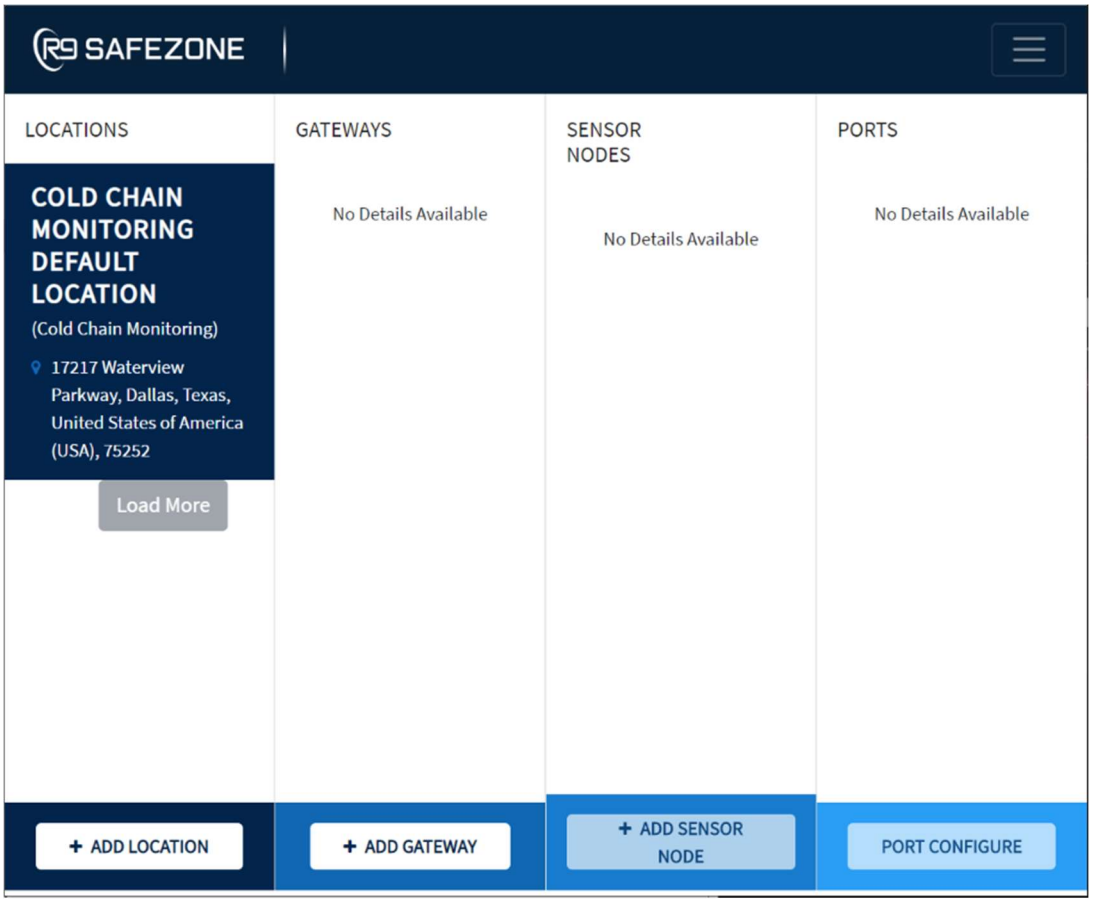
This section will describe how the gateway and node devices are associated with the user account. **The gateway must be configured first, before nodes can be added.**

The following steps show the sequence of steps required to add hardware to the R9 portal. Popup windows will guide the user through this activity. Access to the physical gateway and node devices is required for these steps:

1. Add Gateway
2. Add Sensor Nodes
3. Configure Sensor Node Ports

When a user accesses the portal for the first time, they will be automatically directed to the "Safezone" configuration page and led through the onboarding process. Note: the R9 portal always creates a default location using the information you entered during registration. This information can be changed later if necessary.

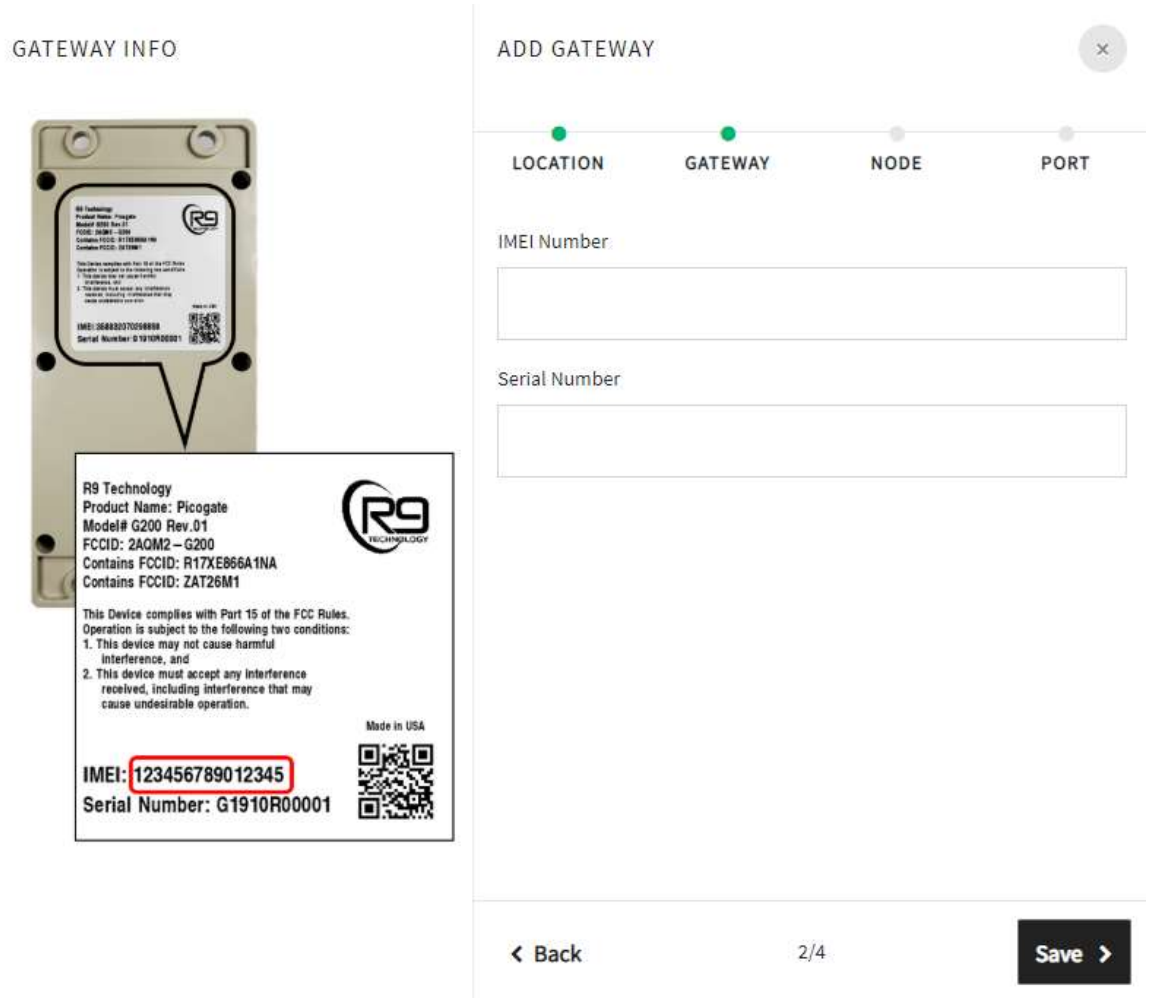
For current users expanding or updating their existing systems, please take care to assign the hardware to the appropriate Location, Gateway, Nodes, and ports (by selecting from the list).



3.1 Adding a Gateway to the web portal

Once a location/site has been selected the user can begin assigning their gateway and nodes. First time users will see only the top-level (default) client location. If an alternate location is desired for adding the first gateway, then start by selecting the "Add Location" button. The following steps can be used to add a gateway to the R9 portal.

1. Click the "ADD GATEWAY" button (after selecting the desired location from the list). A pop-up window will appear.
2. Locate the Gateway label on the back of the unit and enter the information in the appropriate fields. Once completed press the "Save" button; the Gateway has now been added.
3. Repeat the steps above for additional gateways requiring registration. To expedite the text entry process, the QR code on the label can be scanned into a text file, or a text file of gateway IMEI and serial numbers can be obtained from R9 Technology. The numbers can then be copied/pasted into the proper field.



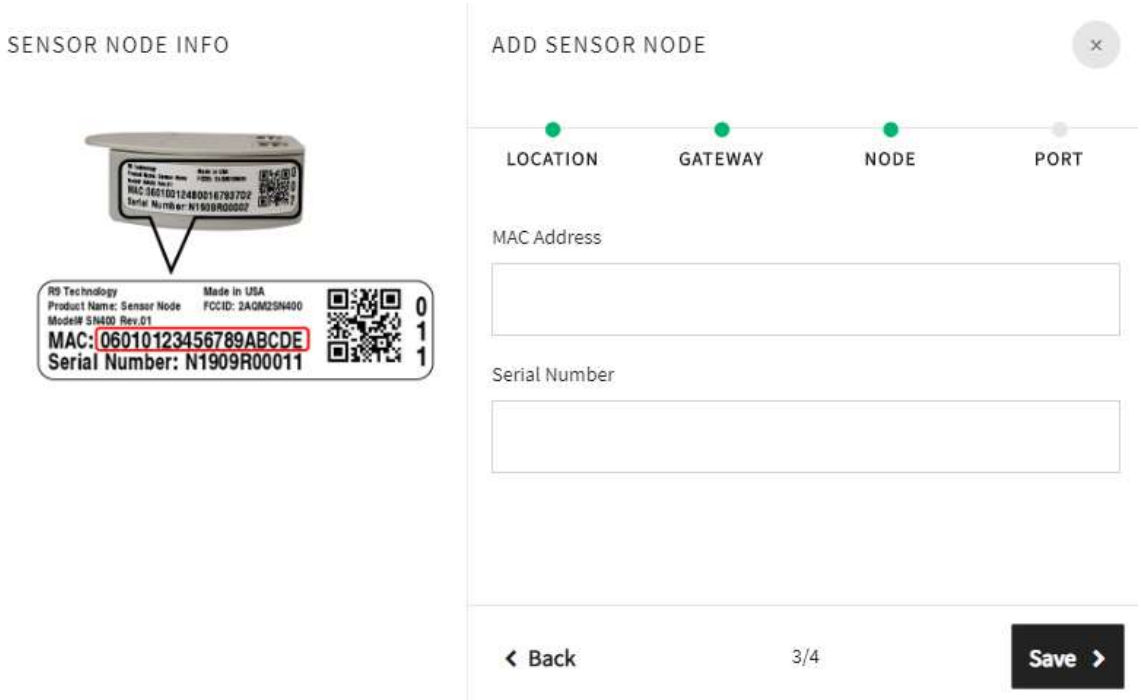
3.2 Adding a Sensor Node to the web portal

New users performing initial configuration, will automatically be directed to the "Add sensor node" window after their gateway has been added. Follow the instructions in the popup window.

Existing users can also additional sensor nodes by selecting the appropriate location and gateway in which the node is intended to be assigned.

1. Click the "Add sensor node" button (**after selecting the desired location and gateway from the list**). A pop-up window will appear.
2. Locate the node label on the side of the unit and enter the information in the appropriate fields. Once completed press the "Save" button; the node has now been added.
3. Repeat the steps above for additional nodes requiring registration. To expedite the text entry process, the QR code on the label can be scanned into a text file, or a text file of node MAC and serial numbers can be obtained from R9 Technology. The numbers can then be copied/pasted into the proper field.

Note that each gateway is limited to supporting 50 node devices.



3.3 Configuring ports on the Sensor Node

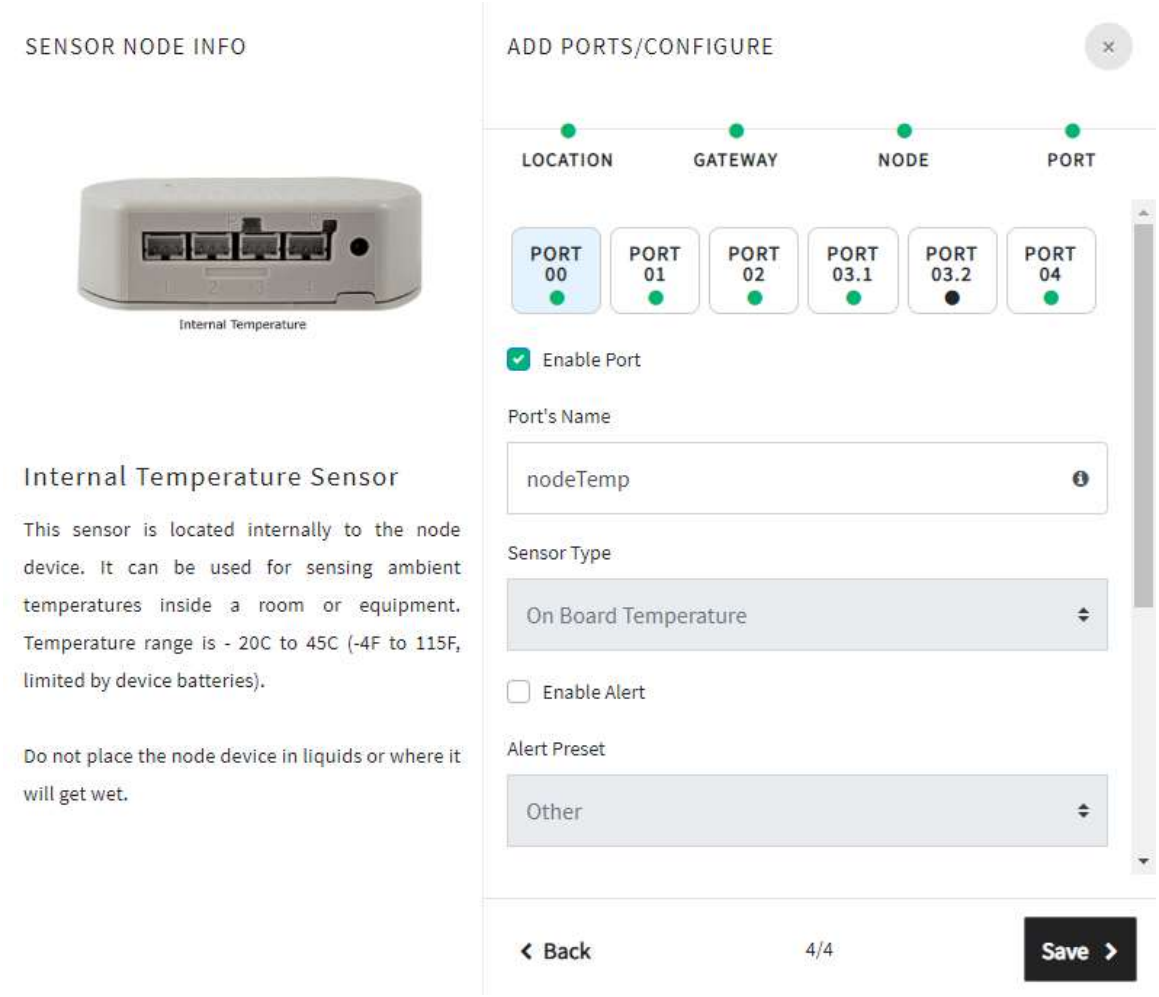
For first time configuration, new users will **automatically** be directed to the "PORT CONFIGURE" window after the node has been added. Follow the instructions in the popup window. It is not required configure that ports immediately for the dashboard to function, this can be done at a later time.

New or previously configured users can add or edit additional sensors by selecting the appropriate location, gateway, and node in which the sensor is intended to be added or changed. Click the "PORT CONFIGURE" button located on the configuration screen. This will launch the "PORT CONFIGURE" popup window. Follow the instructions provided.

R9 Technology currently offers one port configuration for the SN400 "Safezone" application. This configuration will support the following sensor types:

- Port 1: Temperature (digital pulse count)
- Port 2: Temperature (digital pulse count)
- Port 3: Humidity and Temperature (digital one wire)
- Port 4: Door Ajar (switch open/close)

Note: Port 00 is the Node's onboard temperature sensor. Because it is built-in to the node, it is always available, but must be enabled to be viewed in the dashboard. This port can be used to report the ambient temperature for the node's location.

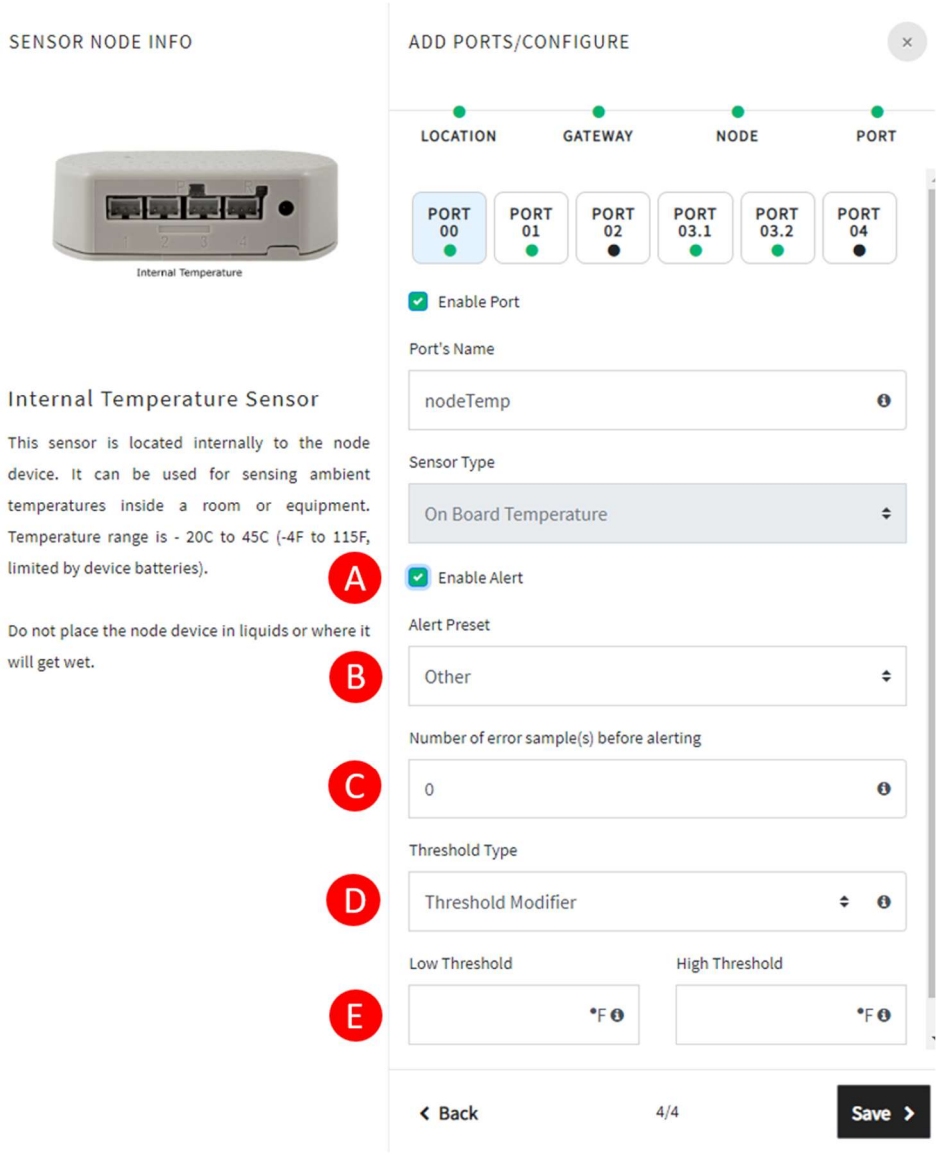


Each sensor node has 4 physical ports and one internal port. Click the appropriate port button for each sensor you have installed to begin the configuration process. The "Enable Port" box must be selected if you want to use a given port. Each node port can also generate alerts. The "Enable Alert" box must be selected if you would like to receive alerts for events relating to a specific port on a sensor.

The information icon shown here, is available throughout the portal to provide additional information about the required configuration fields. Hover over the icon with your mouser pointer to display more information.

It is recommended to enter a descriptive name for the port (Port's Name in diagram above). This is so you can easily identify your port data in the web dashboard. For example, "Walk in Freezer", "Front Dairy Refrigerator", "Ice Cream Counter", etc.

The Alert configuration requires several user inputs in order to operate properly. The following diagram provides some additional information about the required fields.

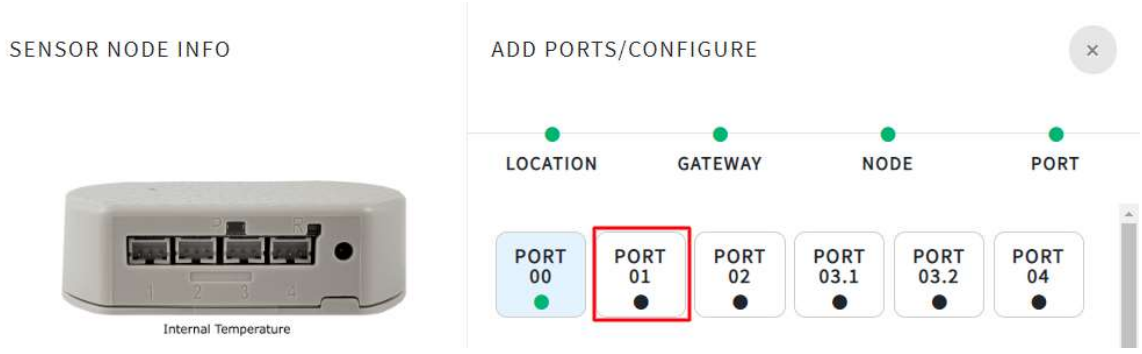


A. Enable Alert: This box must be checked to receive a SMS alert for this port.
B. Alert Preset: These selections auto fill the remaining fields for specific equipment types. The "Other" selection allows the user to customize the remaining fields.
C. Number of "out of range" error sample(s) before alerting: This field allows the system to ignore a user defined number of out of range samples before sending a SMS alert. This is useful to ensure alert conditions are real and

require alerting. For example, freezers which normally cycle through defrost "warming cycles" can cause false alerts, if the alerts are triggered too soon. If a defrost cycle lasts for one hour, you could set the error samples to 5 before alerting (5 x 15 minutes = 1.5 hour of bad samples before alerting).

D. Threshold Modifier: This field allows the user to define the type of alert to be configured for a port. Options include: "Outside a Range" a SMS will be sent if a sample is above or below the defined thresholds. "Above Threshold" a SMS will be sent if the sample is above the defined threshold and "Below Threshold" a SMS will be sent if the sample is below the defined threshold.
E. Thresholds: These fields allow the user to define the sample values that will generate a SMS alert. The received sample value must be either "greater than" or "less than" the value set in the "High Threshold" and/or "Low Threshold" fields.

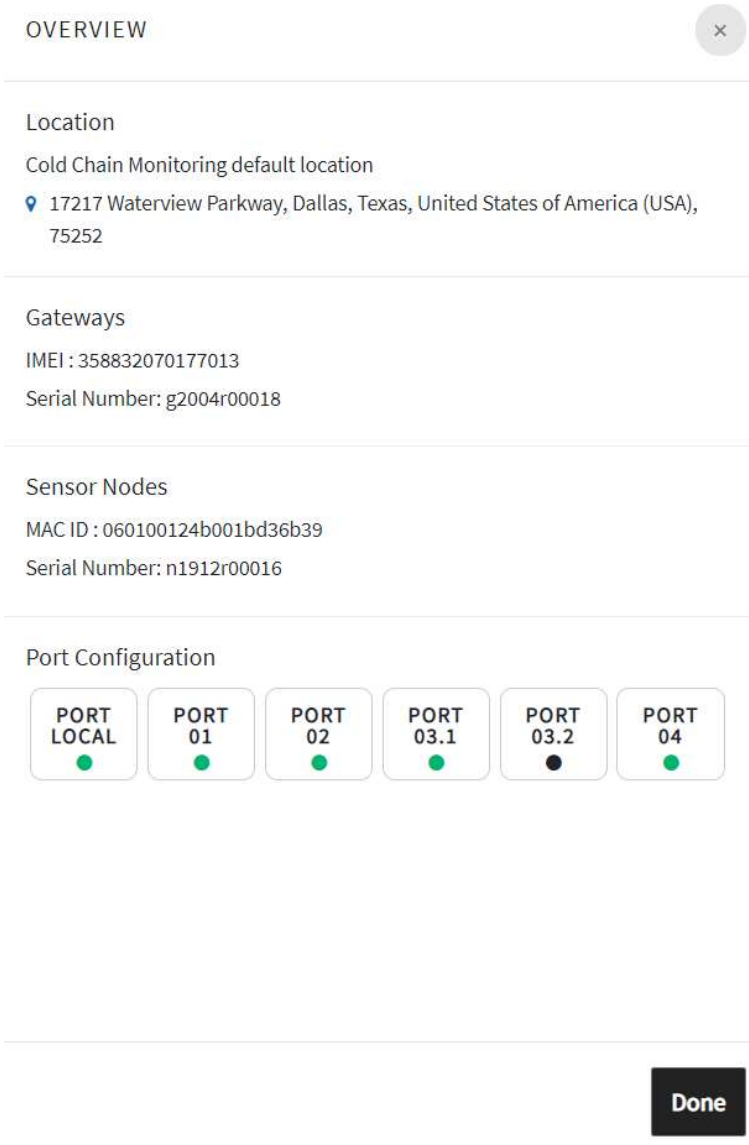
Once the alert fields for the selected port have been configured click the next port button you would like to enable for your system. Continue adding and configuring the remaining ports. Only enable ports that have a sensor plugged into them. The only port not requiring an attached sensor is Port00 (onboard node temperature sensor). You can quickly identify the enabled ports by identifying a "Green" dot on each port button. A "Black" dot represents a port that is not enabled. Do not click the "Save" button until you have configured all the ports you wish to enable for the node. Your Port configuration is saved each time you click to a different port.



Alert Quantity and Alert Condition Reset: Alerts can be enabled and generated for each port. Whenever an alert threshold is exceeded (for example temperature range), you will receive a maximum of three SMS text alerts (on 15-minute intervals) to indicate the alert condition. After receiving three alerts, you will not receive any more alerts even if the alert condition still exists. If the temperature sampling goes back into the normal range on its own, then the alert condition is reset, and you can now receive another three alerts if the

range is exceeded again later. Every time you change the thresholds on a port, for example, the high and low temperature thresholds, the alert condition is automatically reset, and will now activate and send alert SMS text again if the thresholds are exceeded. If you set an alert threshold that is outside the current sample point (current temperature out of range for this example), you will immediately receive an alert on the next sample (15 minutes) assuming the number of samples before alerting is set to 0. This could be done if you want to test the alerting on a specific port.

Once you have completed configuring all your enabled ports click the "Save" button. This will store all the port configuration data to the portal for the selected node. The sensor node overview window will now open.



The “Overview” page is a short summary that identifies the Location, Gateway and Sensor Node that just completed configuration. Additionally, a port summary is shown at the bottom. This identifies which ports are enabled and those that are disabled. If you wish to change this configuration click “Done”, select the Sensor Node to be modified and click the “Port Configure” button. Repeat the process above. Modifications can be made any time using the web portal interface. Continue onboarding your remaining Sensor Nodes.

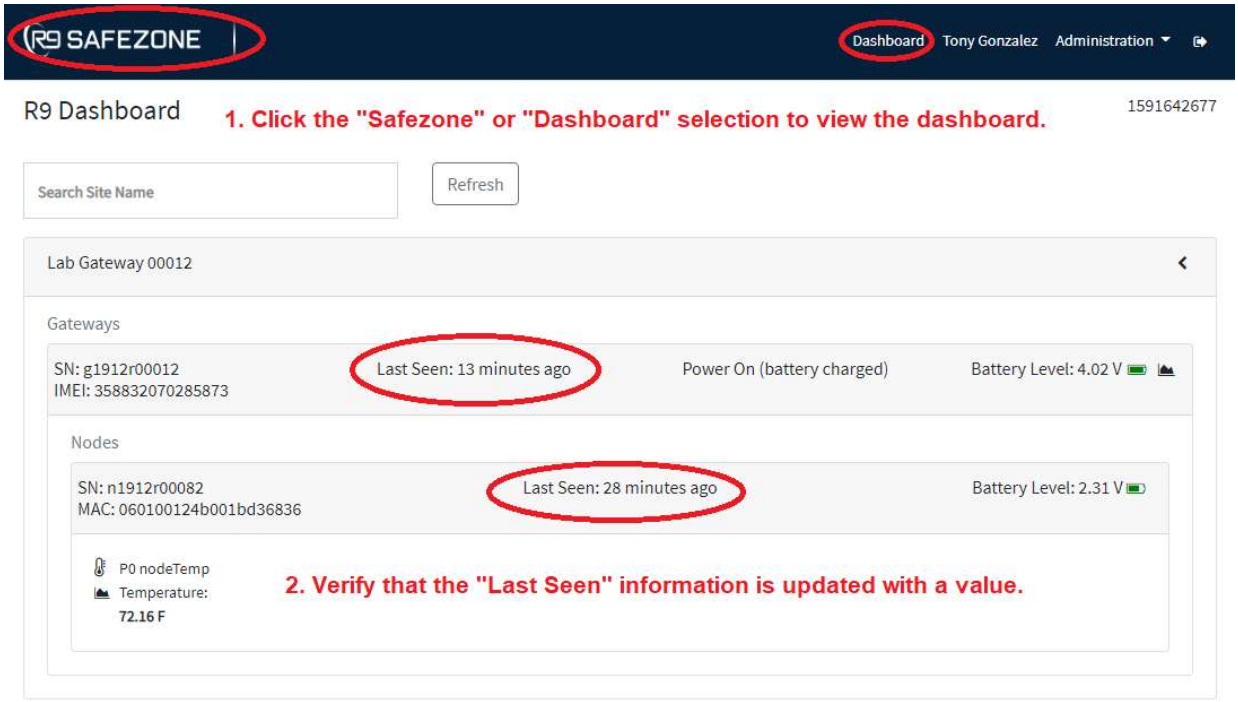
Once you complete configuring your system, you can now move on to the dashboard screen view. Click the “Dashboard” menu button located in the top right corner of the banner or the “Safezone” logo on the upper left of the screen to view the dashboard. This concludes system configuration. The next section gives information on how to verify your equipment is working properly in the R9 portal dashboard.

3.4 Verifying Gateway and Node Operation

If you are entering a new system in the portal for the first time, you should check the portal dashboard to view your gateway and node devices, and insure they are functioning properly. Note that you **do not** have to configure node ports before the gateway and node devices can be checked. Both devices will function without ports enabled. To check the operation of the gateway and nodes in the dashboard, complete the following steps.

1. Locate the black banner on the top of the screen and click on either the "Safezone" logo or the "Dashboard" text label. This will load the main dashboard screen in your web browser. This dashboard is always used to monitor the hardware and data in your system.
2. Locate the "Last Seen" fields for both the gateway and the node(s) that were just added. These fields will transition from "Onboarding" to "Last Seen" for both devices when they are configured and communicating properly in the system.

The gateway device should update to "Last Seen" in less than 15 minutes. The node devices might indicate "Onboarding" status for 15-30 minutes before they update with current information. Note that there is other information that will update for both the gateway and node, including the "Battery Level". The Battery Level will read 0V while onboarding is displayed, but will update to actual battery voltage after a good wireless connection is established. You can click on the small chart icon to view chart information, although it will take time for significant chart data to accumulate. Chart operation is covered in more detail in later sections of this document. Note that sensor ports will have to be configured (next section) to accumulate sensor port data, but voltage and wireless signal strength data will accumulate over time, even when sensor ports are not yet configured.



3.5 Deleting Gateways or Nodes from the web portal

Adding equipment for a new installation is implemented using the "Configuration" menu selection. Deleting of equipment is NOT implemented using this menu. If you need to delete a gateway or node device:

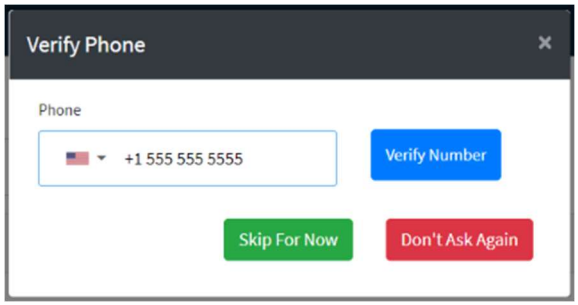
1. Select the "Sites" tab from the main pulldown menu.
2. Select the "View/Add Gateway" tab for the specific gateway system you want to edit.
3. Now you can delete a specific gateway or select "View/Add Node" for node list editing.
4. If you selected "View/Add Node", you are presented with a list of your nodes, and you can select specific nodes to delete.

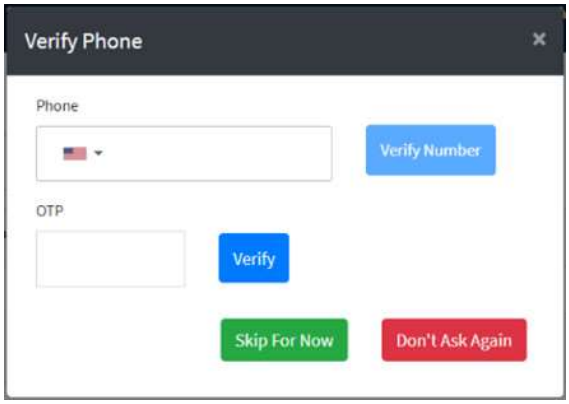
Be careful when deleting your equipment, as this process cannot be undone. You can always add the equipment again in the "Configuration" menu if you delete equipment by accident. If you delete a gateway, all the associated nodes for that specific gateway will also be deleted. Deleting a site/location (with multiple gateways) will also delete all gateways and nodes associated with that site/location.

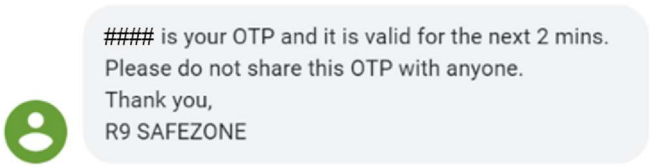
3.6 Alert phone number configuration

After completing initial registration, the system will prompt the user to verify the phone number that was entered. This is usually required before any alerts can be sent, although only the client_owner level phone number can ignore this process.

Note: Once the "Verify Number" button is selected, the user will receive a text message containing a one-time passcode (OTP) which is valid for 2 minutes. Enter the OTP into the appropriate field. This verifies that the phone number is valid and can receive SMS text messages. The user is now directed to the dashboard.



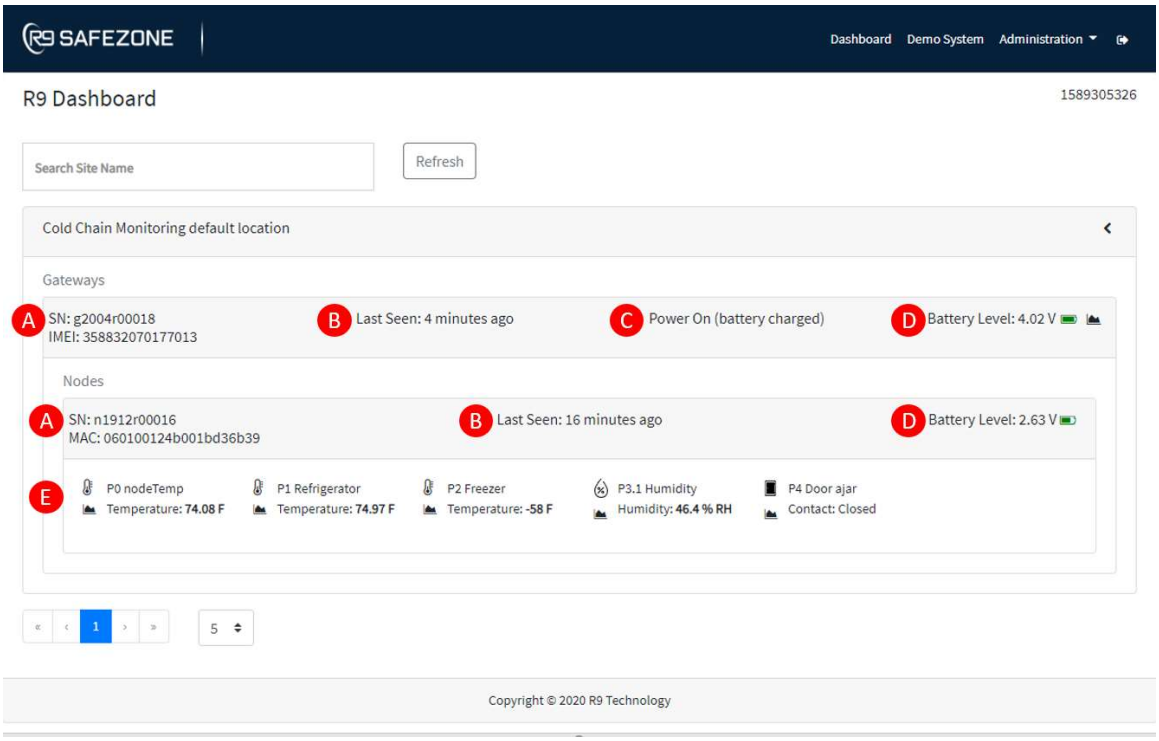




4 Navigating the web portal

The web interface or "portal" is used by a customer to view and manage their IoT data, configure alerts, add users, and set report intervals. Currently this is done with a web browser. Google "Chrome" is recommended for use with the R9 portal system.

The image below depicts the R9 portal **dashboard**, which includes one gateway and one node. The dashboard screen is the primary window from which you can view equipment status and sensor port data in the R9 system. Depending on user permissions, the dashboard you see may show one site or many sites (in list format). Each site may have one or more gateways. Charting information is always displayed on a per gateway or per node basis. A brief description of the dashboard fields is shown below.



A. Gateway (serial number and IMEI ID) and Node (serial number and MAC ID). These numbers identify specific devices in your system.
B. Last Seen, Indicates the most recent check-in time for both the gateway and nodes.
C. Current power state of the gateway. This field will indicate if the gateway is operating on AC power or operating on battery power (AC power is out).
D. Current battery level. This field is available for both the gateway and nodes. The battery icon will turn "Yellow" when the batteries are in a low state. Node batteries

will need to be replaced when this condition is observed. The gateway battery will automatically recharge when AC power returns.

E. Sensor information with selectable chart icon. This field displays all "enabled" sensors and their last recorded value for the assigned node.

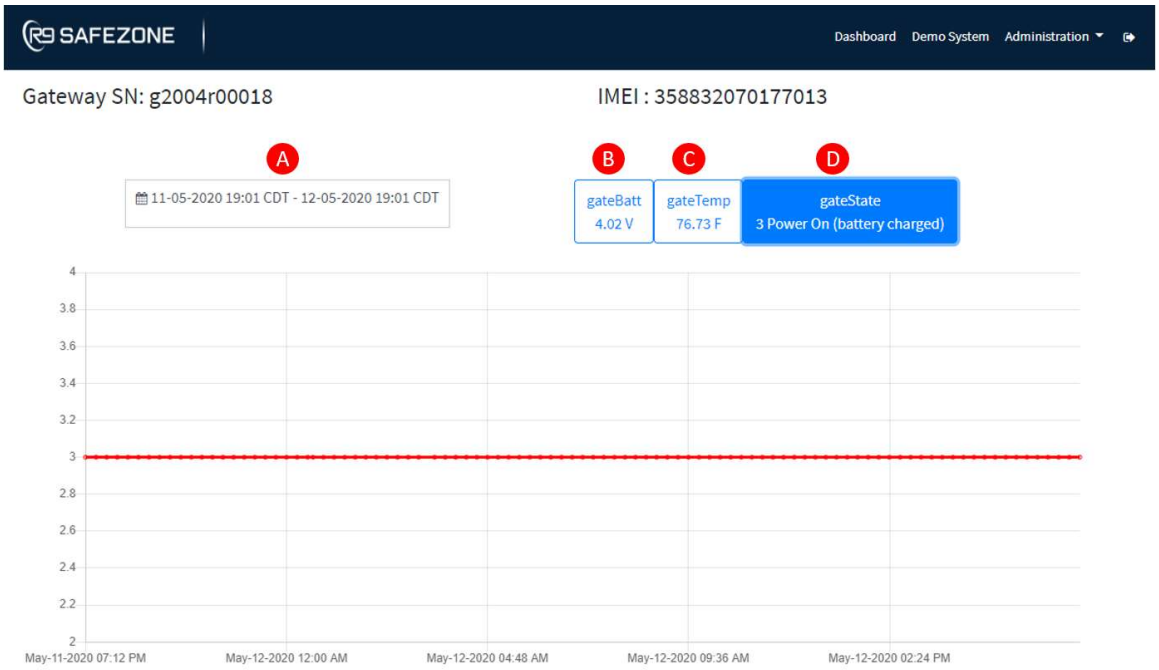
The chart icon shown here, allows the user to access historical data in a graphical format. Chart data can be accessed for the gateway by using the chart icon next to the gateway's battery level icon. Additionally, node port data and battery level data can be accessed by using any of the chart icons shown next to the node ports.

4.1 Chart selection

The dashboard allows the client to select the charting information for both the gateway and node. When charting information is available the chart icon will appear next to the appropriate field as seen in the above image.

4.1.1 Gateway Chart

The image below depicts a standard gateway charting screen. A brief description of the fields follows.



A. Selectable calendar button can be used to identify a specific date range to be displayed. Select specific start and end days from the calendar with the mouse, or select a duration range (24hr, 3day, last week). Note that start and end time can be

changed (at the bottom of the menu), as well as the months that are currently displayed. The default display is the last 6 hours of data.

B. gateBatt: indicates the current battery level. A full battery charge will display approximately 4V.
C. gateTemp: indicates the internal temperature of the gateway
D. gateState: indicates the power state of the gateway. The gateway is powered by an AC power source or the onboard battery backup. The gateway has 3 gateState levels which are defined as:
    1. **AC Power Off, Battery On**
       This state indicates the gateway has lost AC power and is running on the backup battery. This state is invoked when the unit has been unplugged, a breaker opened, or loss of facility power. Your gateway should run for approximately 8 to 20 hours using battery power if AC power is lost.
    2. **AC Power On, Battery Charging**
       This state indicates the gateway is receiving power and charging the backup battery.
    3. **AC Power On, Battery Fully Charged**
       This state indicates the gateway is receiving power and the backup battery is fully charged.

4.1.2 Node Chart

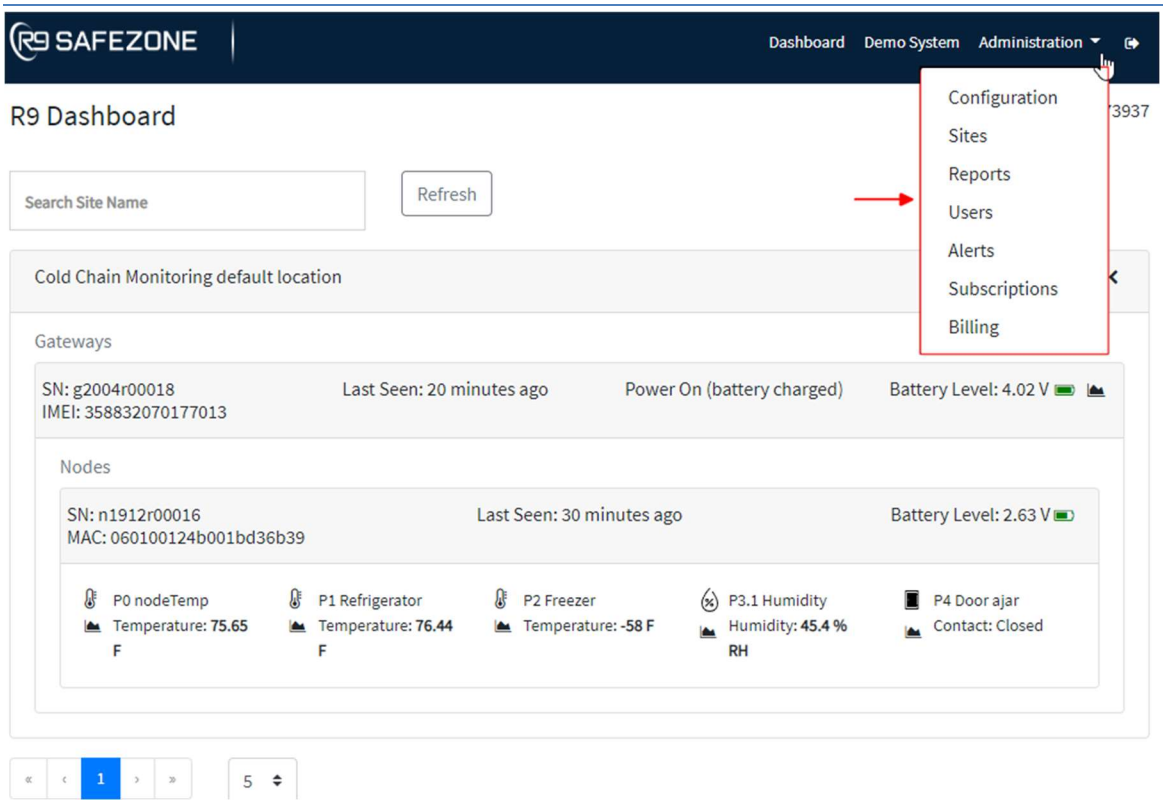
The image below shows a typical node charting screen. Each point shown on the graph represents a sample collected from the sensor node. Samples are collected every 15 minutes from the sensor node for the "Safezone" application. The chart feature is very important, as it allows a user to view measurement trends over time, of the equipment that is being monitored. To assist with interpreting equipment alerts, the chart for corresponding equipment can be used to more easily view and visualize conditions that are generating the alert. A brief description of each field is listed below.

A. Selectable calendar button can used to identify a specific date range to be displayed.
B. This is the collection of enabled ports on the selected node. Each port will display the assigned name, last recorded value and the samples unit type. Click each port button to enable or disable it's chart data.
C. gateRssi: indicates the node signal strength, as received by the gateway. Click this button to display this data in chart form.
D. nodeBatt: indicates the current battery level for the node. Click this button to display this data in chart form.
E. nodeRssi: indicates the gateway signal strength, as received by the node. Click this button to display this data chart.

4.2 Web portal Administration

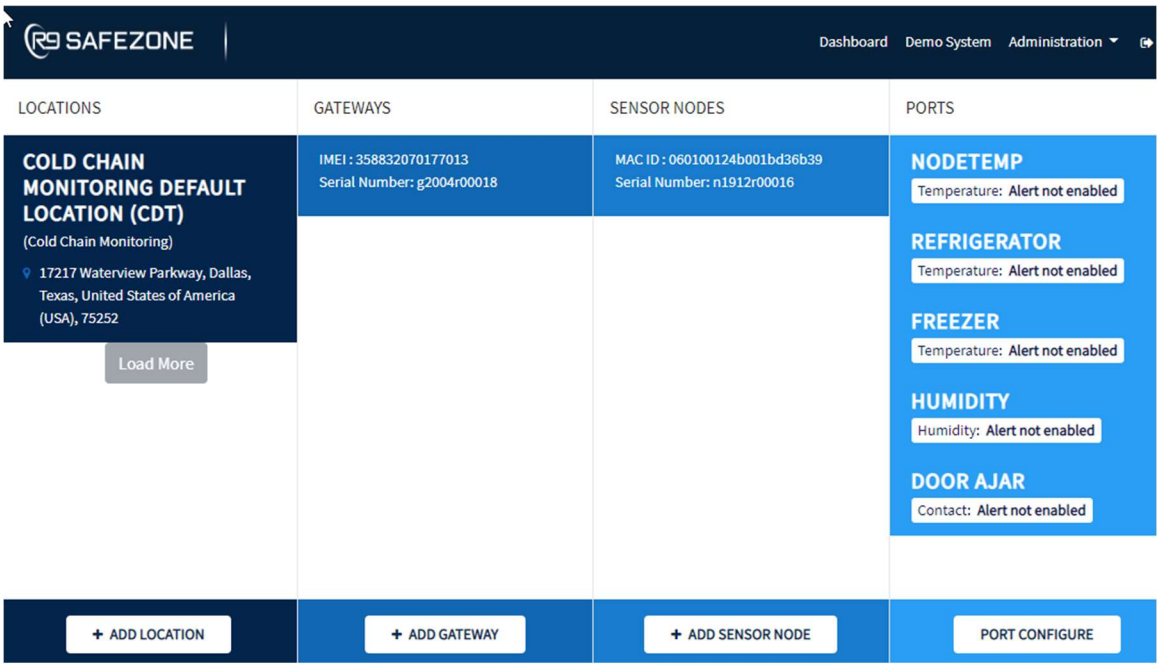
The Safezone system is configured and managed through the web portal. The web portals main control menu is accessed from the dashboard. Select the "Administration" button located in the top right corner of the banner as shown in the image below. Note that the administration drop-down menu is only visible for users with the proper permissions, and may not show all selections for site_admin and site_user roles.

A separate section for each selection in the drop-down menu is provided in this section of the document: **Configuration, Sites, Reports, Users, Alerts, Subscriptions, Billing.**



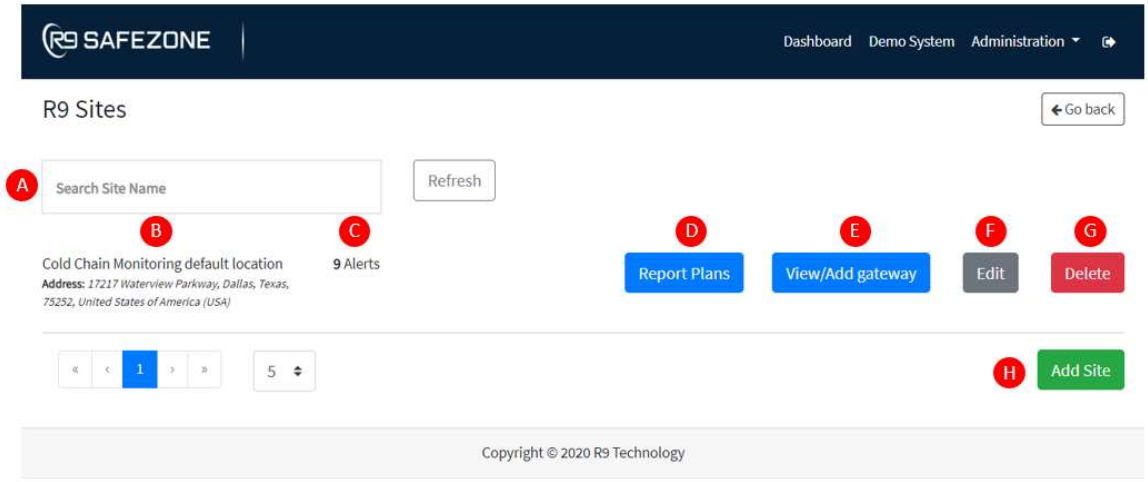
4.2.1 Configuration

The "Configuration" screen allows the user to add Locations (sites), Gateways, Sensor Nodes and Ports to their Safezone system. This window is the same as was accessed during the initial onboarding process. This menu is designed be self-descriptive and provide text and pictures to streamline the process of adding new sites and hardware.



4.2.2 Sites

The "Sites" screen allows users to view and manage the different locations/sites in which their systems are deployed. It also provides an interface to allow the customer to view, add, or delete hardware along with editing or creating report plans. The following image provides an overview of the Site window.



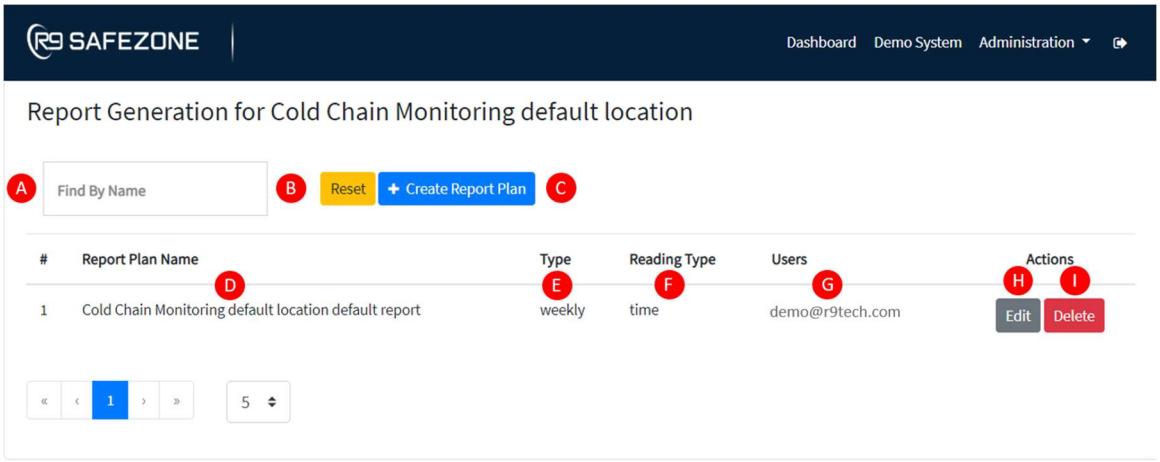
A. Search Site/Location Name field can be used for customers having multiple sites. This is a convenient method for sorting sites.
B. Site/Location Name filed provides the user with the name and physical address of each of the customer's sites.
C. Monthly Alert Count. This field provides users with the current number of alerts a site has received. This count value is reset at the beginning of each month.
D. Report Plan Button, this button opens the report plan generation window. Users can add or modify the time intervals for the generated weekly and monthly reports.
E. View/Add Gateway button, this button allows users to view or delete a location's assigned gateways. Once accessing the View/Add gateway page, users can then subsequently select to View/Add/Delete a gateway's assigned nodes.
F. Edit button, this button opens a window which allows the user to edit the sites name, address, and group phone number. This is not the alert phone number
G. Delete button, this button will remove the **entire site** from the user's system. This action cannot be undone. Additionally, all gateways, sensor nodes and configured ports will be deleted from the system. Caution should be exercised when using this feature.

H. Add Site button, this button will forward the user to the configuration window. From the configuration window users can add additional sites, gateways, or sensor nodes

4.2.2.1 Report Plans

The Report Plans button activates the user interface for modifying or creating a site's report generation procedure. When a user clicks the "Report Plans" button (shown above) for the selected site, the report plan screen is displayed. This screen is used to view and edit existing report plans or to add a new report plan. Note that report plans are always associated with a single location/site. There can be one or more gateways associated with a site/location. Each, and every gateway at a site will have its node/port information (if the port is enabled) included in the report. Because report plans can be customized, a single site can have more than one report plan.

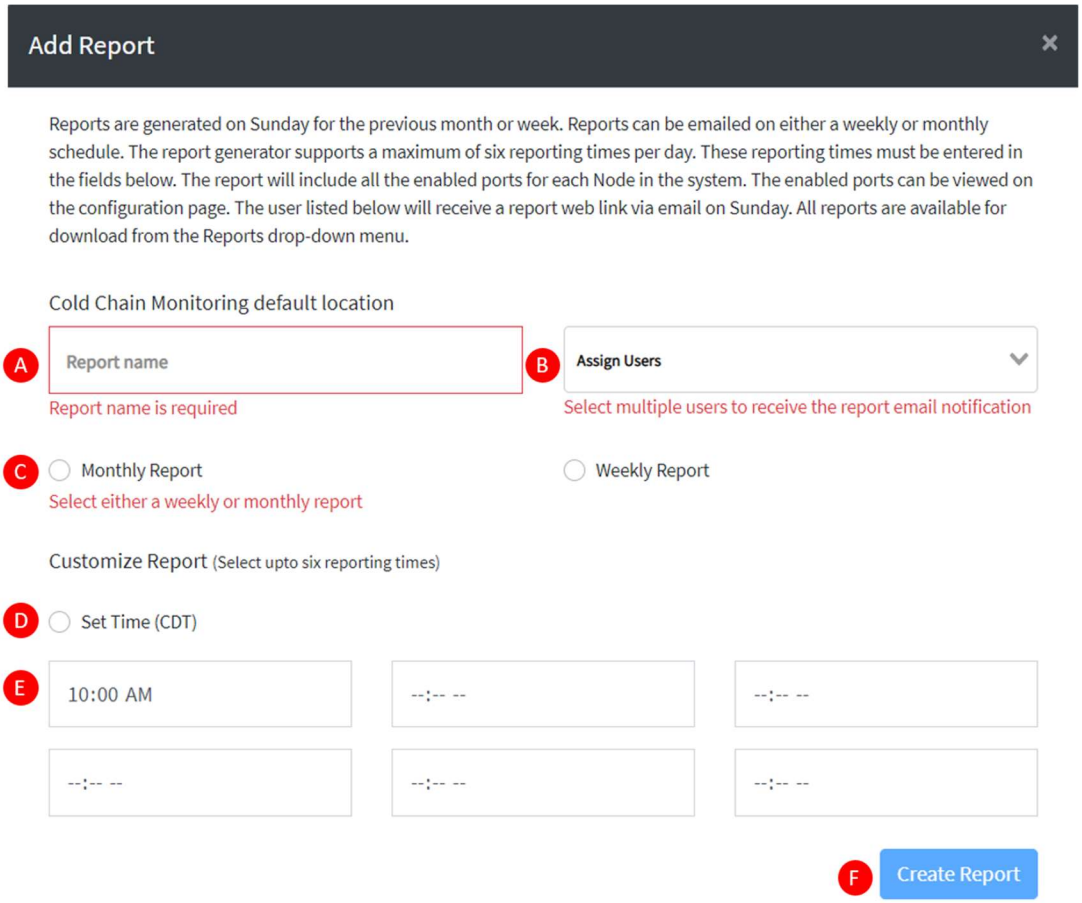
Reports contain port readings for temperature, humidity, and door ajar status for specific dates and times in excel .csv format. Reports can be stored by a business or restaurant in electronic or paper form as part of their quality records. **Note that reports should be permanently stored by a customer** on their local system, as all report information is purged from the R9 system after 3 months.



A. Find By Name field can be used for customers having multiple report plans. This is a convenient method for sorting plans.
B. Reset Button, this button resets the Find By Name field to empty.
C. Create Report Plan button, this button will open the create new report plan window
D. Report Plan Name, each report will be given a unique report plan name by the user. The only exception to this is the default report plan that is created when a user first registers with the R9 portal system. In this case the system creates the default report plan. The default plan can be edited by the user.

E. Type field, this field indicates when the report will be provided. Supported options and weekly or monthly.
F. Reading Type field, this field indicates the unit for the report. The only supported type is Time.
G. User field, this field indicates the users that will receive an emailed copy of the generated report.
H. Edit button, this button allows the user to modify the report plan.
I. Delete button, this button allows the user to delete the alert plan. This action cannot be undone. Caution should be exercised when using this feature.

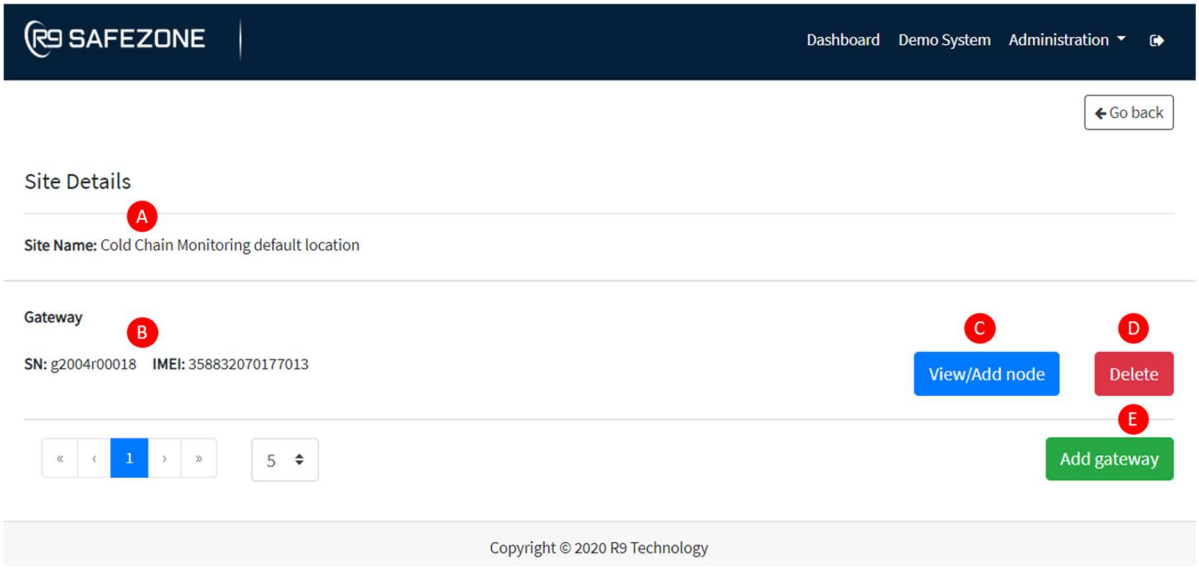
Creating a report plan is accomplished by clicking the "Create Report Plan" button shown above. The screen below will then display. The systems default reporting times are 10 am and 4 pm. The data at these times will be captured and included in the user's report for each port that is enabled. The report will be in an excel file format. Reports are created and emailed on Sunday for the previous month or week. All reports are stored for a period of 3 months on the R9 servers. Reports older than 3 months are purged automatically from the R9 system. Download and save any reports you want to keep on your local storage device.



A. Report Name field is used by the user to provide the report plan with a unique name.
B. Assign Users field allows the users to add up to 3 users to receive the created weekly or monthly reports. Users must exist in the R9 portal system prior to being available for addition to the assign user selection
C. Monthly or Weekly report bubble. The report will be generated and emailed on either a weekly or monthly basis. User's must select one. Additional plans can be created to accommodate users wanting both a weekly and monthly reports.
D. Set time, the set time bubble must be selected to change the reporting times.
E. Reporting times field. Users can select up to six reporting times for the report.
F. Create Report button, clicking this button will finish and create the report plan as described above. It will not create a report, an actual report will be created per the report plan. Reports are always generated on Sunday for the previous week or month.

4.2.2.2 View/Add Gateway

Each site/location can have more than one gateway installed. The View/Add gateway button is also used for deleting a gateway from the system. When a user clicks the view/add gateway button for the selected site, the following window will open.

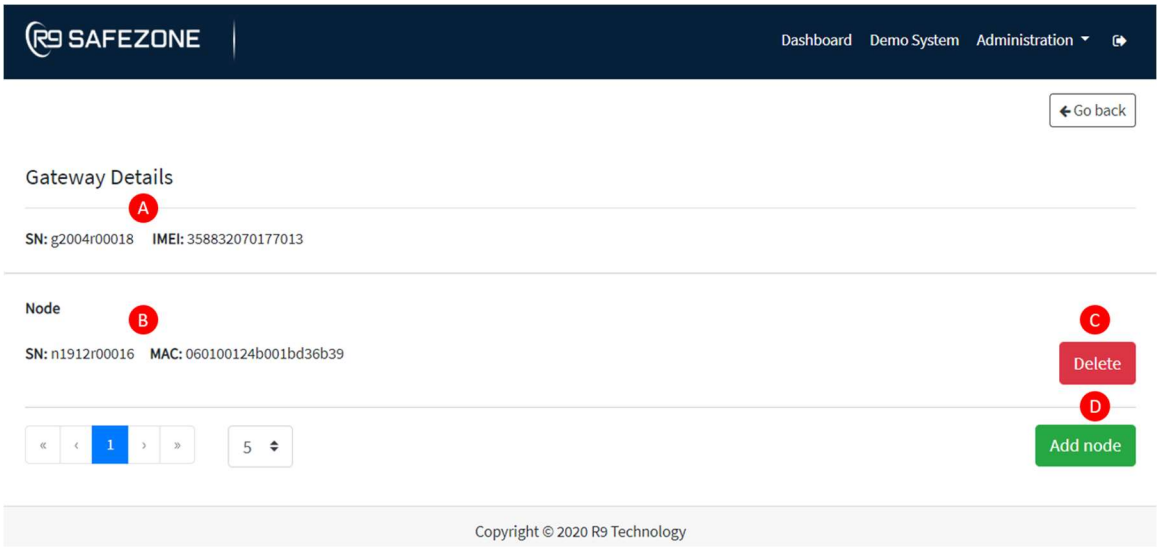


A. Site/Location Name filed provides the user with the name of the selected customer site.

B. Gateway Information, this field provides the user with the serial number and IMEI number for the gateway assigned to the specified site. For sites having more than one gateway a list of gateways will be provided.
C. View/Add node button, this button allows the user to see all the nodes assigned to this gateway and also delete individual nodes by proceeding with this button.
D. Delete button, this button will remove the gateway from the user's system. This action cannot be undone. Additionally, all sensor nodes and configured ports assigned to this gateway will be deleted from the system. Caution should be exercised when using this feature.
E. Add gateway button, this button will forward the user to the configuration window. From the configuration portal window, users can add additional locations, gateways, or sensor nodes.

4.2.2.3 View/Add Node

Each gateway can have one, or up to fifty nodes. The view/add node button provides for viewing and deleting sensor nodes in the system. When a user clicks the view/add node button for the selected gateway, the following window will open.

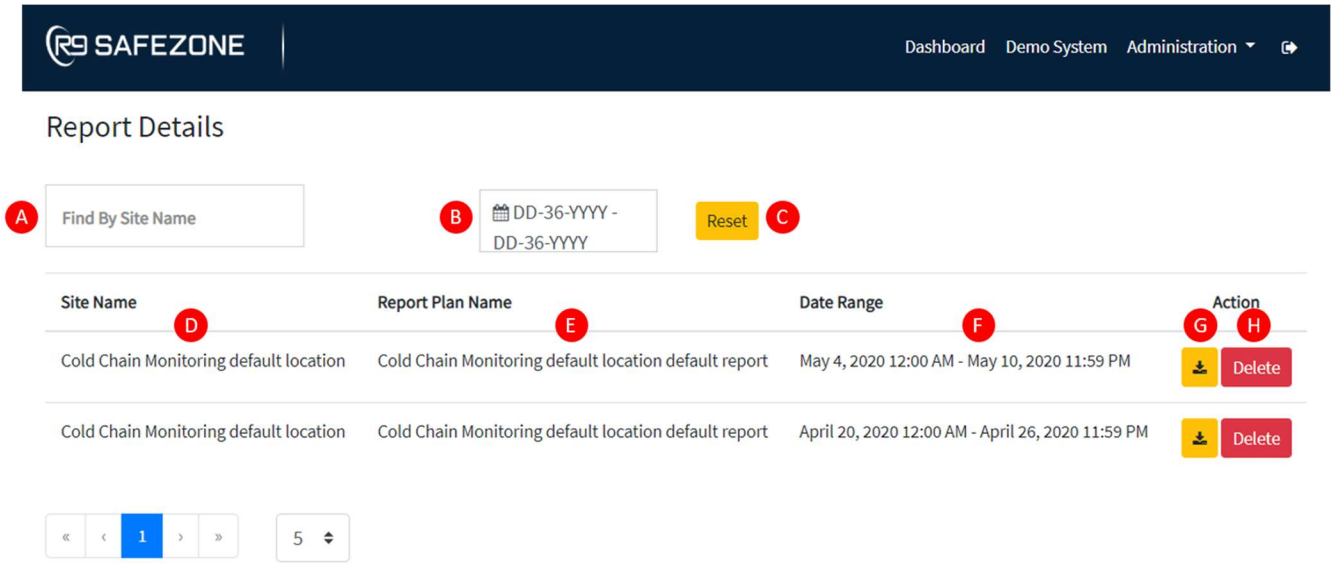


A. Gateway Information, this field provides the user with the serial number and IMEI number for the gateway currently being edited.
B. Sensor node Information, this field provides the user with the serial number and MAC ID number for the sensor node(s) assigned to the selected gateway. For sites having more than one sensor node a list of sensor nodes will be provided.

C. Delete button, this button will remove the node from the user's system. This action cannot be undone. Additionally, all configured ports assigned to this sensor node will be deleted from the system. Caution should be exercised when using this feature.
D. Add node button, this button will forward the user to the main configuration window. From the configuration window users can add additional locations, gateways, or sensor nodes.

4.2.3 Reports

Previously generated reports can be viewed, downloaded, and deleted using the "Reports" main pull-down menu selection. Reports are always associated with a single location/site and report plan. Each site can have multiple report plans if desired (due to flexibility in report configuration). Each site may contain more than one gateway. Each gateway/node set at each site has data included in the report (if the node port is enabled at the time of the report run). Reports are always generated on Sunday for the previous week or month. All reports are stored for a period of 3 months. Reports older than 3 months are purged automatically from the system.



A. Find By Site Name field can be used for customers having multiple sites and multiple report plans. This is a convenient method for sorting reports.
B. Date Sort field can be used to display reports for a given date range. This is important for users needing to pull reports for all sites relating to a specific date range.

C. Reset button, this button will reset the Date Sort field.
D. Site Name, this column displays the name of the site for the report.
E. Report Plan Name, this column displays the report plan used to generate the report.
F. Date Range, this column displays the date range for the generated report. The date range will reflect either a weekly or monthly period.
G. Download button, click this button to download the report to your computer. All reports are provided .CSV (Microsoft Excel) format.
H. Delete button, click this button to delete the report from the R9 system. This action cannot be undone.

The image below is a sample of the excel format report data. If a port sample is missing in the database for any reason (for example a node was removed or powered off for a period of time) then the missing sample(s) will display as "-".

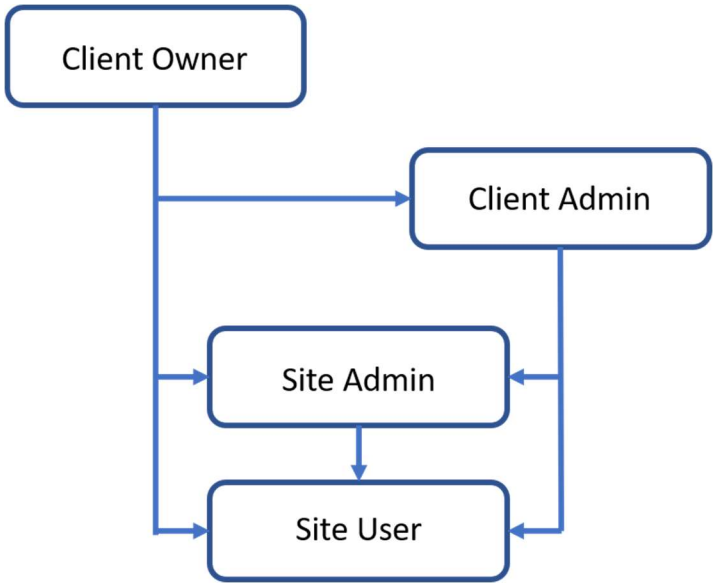
Site	Greenville Store												
Weekly Report	20200210 - 20200216												
Type	Time (08:00 AM, 10:00 AM, 12:00 AM, 02:00 PM, 04:00 PM, 06:00 PM) Central Standard Time (CST)												
Gateway	SN: g1912r00022, IMEI: 358832070203181												
Node	SN: n1912r00004, MAC: 060100124b001bd37861												
Date	Port Name	Time 1	Value 1	Time 2	Value 2	Time 3	Value 3	Time 4	Value 4	Time 5	Value 5	Time 6	Value 6
2/10/2020	unit_top_temp	8:00 AM	66.2	10:00 AM	67.21	12:00 AM	68.45	2:00 PM	67.55	4:00 PM	66.43	6:00 PM	67.66
2/11/2020	unit_top_temp	8:00 AM	67.44	10:00 AM	68.11	12:00 AM	66.76	2:00 PM	65.97	4:00 PM	67.89	6:00 PM	67.66
2/12/2020	unit_top_temp	8:00 AM	69.24	10:00 AM	66.54	12:00 AM	68	2:00 PM	67.78	4:00 PM	66.76	6:00 PM	65.97
2/13/2020	unit_top_temp	8:00 AM	69.69	10:00 AM	69.46	12:00 AM	69.69	2:00 PM	68.56	4:00 PM	69.35	6:00 PM	65.75
2/14/2020	unit_top_temp	8:00 AM	66.76	10:00 AM	-	12:00 AM	68.34	2:00 PM	-	4:00 PM	-	6:00 PM	68.9
2/15/2020	unit_top_temp	8:00 AM	66.88	10:00 AM	70.59	12:00 AM	68.68	2:00 PM	69.91	4:00 PM	68.34	6:00 PM	-
2/16/2020	unit_top_temp	8:00 AM	66.43	10:00 AM	68	12:00 AM	69.01	2:00 PM	69.13	4:00 PM	69.91	6:00 PM	68.9
2/10/2020	fridge_temp	8:00 AM	42.58	10:00 AM	42.35	12:00 AM	44.26	2:00 PM	42.24	4:00 PM	42.35	6:00 PM	42.35
2/11/2020	fridge_temp	8:00 AM	42.35	10:00 AM	42.24	12:00 AM	42.24	2:00 PM	42.46	4:00 PM	42.35	6:00 PM	42.13
2/12/2020	fridge_temp	8:00 AM	42.46	10:00 AM	42.46	12:00 AM	42.01	2:00 PM	42.8	4:00 PM	42.8	6:00 PM	42.46
2/13/2020	fridge_temp	8:00 AM	43.59	10:00 AM	44.04	12:00 AM	43.25	2:00 PM	43.81	4:00 PM	43.59	6:00 PM	42.69
2/14/2020	fridge_temp	8:00 AM	43.25	10:00 AM	-	12:00 AM	43.36	2:00 PM	-	4:00 PM	-	6:00 PM	43.25
2/15/2020	fridge_temp	8:00 AM	43.48	10:00 AM	43.14	12:00 AM	43.59	2:00 PM	43.59	4:00 PM	43.59	6:00 PM	-
2/16/2020	fridge_temp	8:00 AM	43.7	10:00 AM	43.48	12:00 AM	43.93	2:00 PM	43.36	4:00 PM	43.59	6:00 PM	44.71
2/10/2020	freezer_humidity	8:00 AM	83.9	10:00 AM	60.6	12:00 AM	60	2:00 PM	57.6	4:00 PM	80.9	6:00 PM	58.6
2/11/2020	freezer_humidity	8:00 AM	57.9	10:00 AM	58.9	12:00 AM	75.2	2:00 PM	82.4	4:00 PM	60	6:00 PM	80.1
2/12/2020	freezer_humidity	8:00 AM	84.8	10:00 AM	85	12:00 AM	58.9	2:00 PM	92	4:00 PM	56.8	6:00 PM	86.9
2/13/2020	freezer_humidity	8:00 AM	57.6	10:00 AM	65.6	12:00 AM	65.5	2:00 PM	74.2	4:00 PM	58.2	6:00 PM	90.9
2/14/2020	freezer_humidity	8:00 AM	58.1	10:00 AM	-	12:00 AM	60.4	2:00 PM	-	4:00 PM	-	6:00 PM	68
2/15/2020	freezer_humidity	8:00 AM	57.5	10:00 AM	66.7	12:00 AM	58.4	2:00 PM	58.4	4:00 PM	93	6:00 PM	-
2/16/2020	freezer_humidity	8:00 AM	66.8	10:00 AM	60.4	12:00 AM	73.6	2:00 PM	62.3	4:00 PM	63.5	6:00 PM	61.7
2/10/2020	freezer_temp	8:00 AM	-0.76	10:00 AM	0.14	12:00 AM	-1.84	2:00 PM	-2.02	4:00 PM	4.64	6:00 PM	0.14
2/11/2020	freezer_temp	8:00 AM	0.32	10:00 AM	-2.56	12:00 AM	4.64	2:00 PM	-0.94	4:00 PM	1.4	6:00 PM	-1.84
2/12/2020	freezer_temp	8:00 AM	-0.4	10:00 AM	5	12:00 AM	-0.04	2:00 PM	4.28	4:00 PM	-2.56	6:00 PM	0.68
2/13/2020	freezer_temp	8:00 AM	0.5	10:00 AM	-1.3	12:00 AM	-1.84	2:00 PM	-2.2	4:00 PM	-0.22	6:00 PM	4.82
2/14/2020	freezer_temp	8:00 AM	-0.58	10:00 AM	-	12:00 AM	1.04	2:00 PM	-	4:00 PM	-	6:00 PM	3.74
2/15/2020	freezer_temp	8:00 AM	-1.3	10:00 AM	3.56	12:00 AM	-0.94	2:00 PM	-0.4	4:00 PM	4.28	6:00 PM	-
2/16/2020	freezer_temp	8:00 AM	-2.02	10:00 AM	1.4	12:00 AM	4.1	2:00 PM	1.22	4:00 PM	-2.56	6:00 PM	0.5

4.2.4 Users

The "Users" main menu selection is where new system users can be added, and user roles or permissions can be set or changed. The "Safezone" system uses on a hierarchical user permissions structure. The structure is comprised of four user roles with each subsequent role having a reduced permission level. Client_owners or client_admins will need to determine the appropriate permission level when adding new users to their system. The following provides an overview of the Safezone user structure, and their abilities to change system parameters such as alerting, hardware configuration, and new user roles.

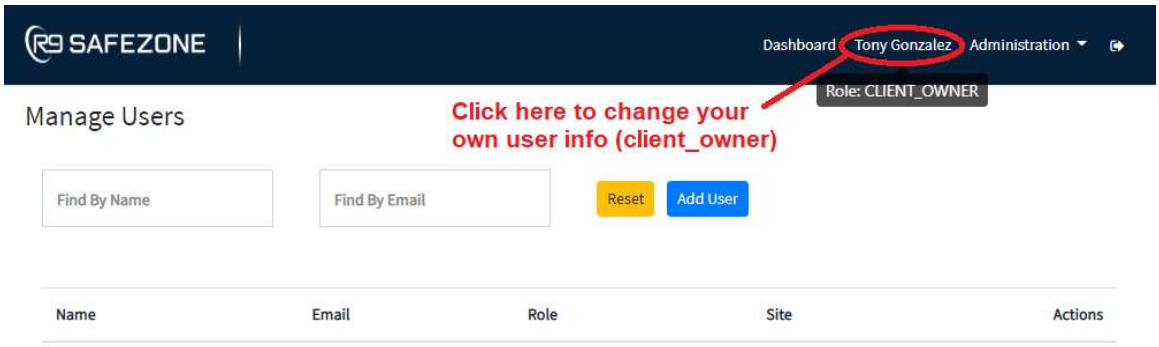
1. **CLIENT_OWNER** – The client_owner is the highest permission level for the R9 portal system. There can only be **one** client_owner permission assigned per customer system. The client_owner permission extends to all sites existing on the system. The client_owner role is assigned to the first user during the initial onboarding activity. Client_owner status provides the user full access to *view* or *modify* all information located in the system**. The client_owner is likely a business owner, business executive, or manager of an IT department.**
2. **CLIENT_ADMIN** – none or many client_admins can exist in a system. The client_admin has the same permission levels as the client_owner, except, the client_admin cannot access or remove the client_owner's information. The client_owner or client_admin can remove and assign new client_admins. **The client_admin is likely the client_owner's administrative assistant, direct report, or business representative.**
3. **SITE_ADMIN** – none or many site_admins can exist in a system. This level of user permission allows *viewing* and *modification* of the dashboard for a specific location/site only. It is possible for the same user to have multiple site_admin (or site_user) permission levels at different sites. **The site_admin is likely the manager of a specific restaurant or business location.**
4. **SITE_USER** – none or many site_users can exist in a system. This level of user permission allows *viewing* of the dashboard and receiving alerts for the specific location/site. This user does not have permissions to change the system configuration. It is possible for the same user to have multiple site_user (or site_admin) permission levels at different sites. **The site_user is likely an employee of a specific restaurant or business location.**

Permissions hierarchy flow chart:

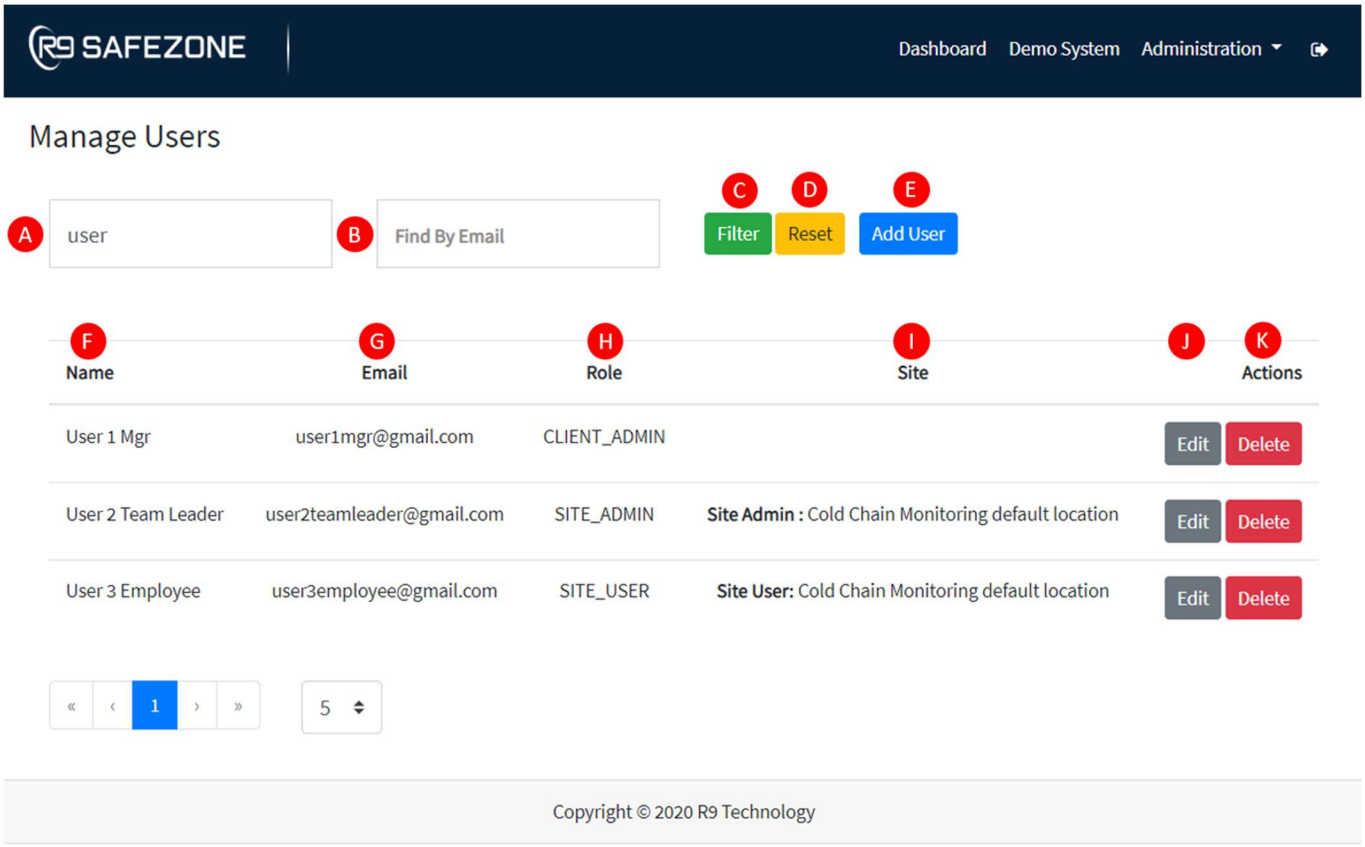


4.2.4.1 Managing Users

The "Manage Users" window (select Users under main drop down menu) allows a client_owner or client_admin to view, add, or modify users for their Safezone system. New users are assigned a "user role" which determines the level of access they are permitted to use. The manage users screen only allows selection and editing of lists of users that have lower permission, than the current permission level of the active user. To edit your own user information (for example a client_owner), click your name, as shown in the upper right of the screen image below.



For managing lower permission users in list format, the Manage Users screen should be used. A description of its operation is shown below.

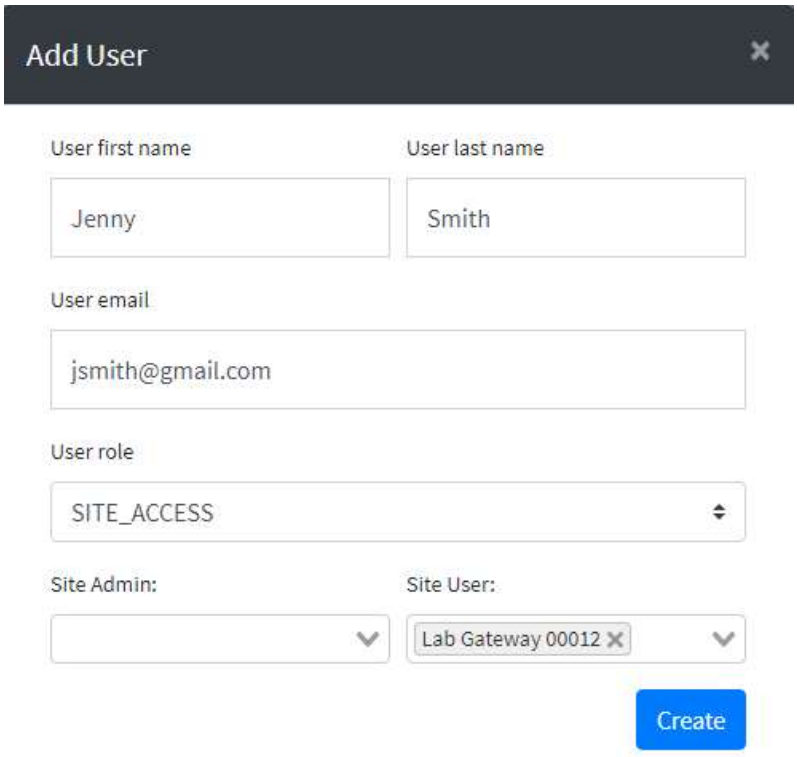


A. User field can be used to find a specific user using their name. Partial name searches are allowed. All users including the partial search will be displayed. Click the "Filter" button to initiate the search.
B. Find By Email field can be used to find a specific user using their email address. Partial email address searches are allowed. All users including the partial search will be displayed. Click the "Filter" button to initiate the search.
C. Filter button, this button initiates both the name and email address search feature.
D. Reset button, this button will reset both the name and email address filter fields.
E. Add User button, this button will open the Add New User window. Refer to the next section for more details.
F. User Name field, this column displays the users name.
G. User Email field, this column displays the user email address.
H. User Role field, this column displays the user's assigned system role.

I. Site field, this column displays the user's assigned sites and the specific role they have been assigned for each site. Example: A user could be a Site_admin at one location and a Site_user at another location.
J. Edit button, this button allows a user's information to be modified. Refer to the next section for more details.
K. Delete button, this button allows a user to be removed from the system. This action cannot be undone.

4.2.4.2 Adding or Editing Users

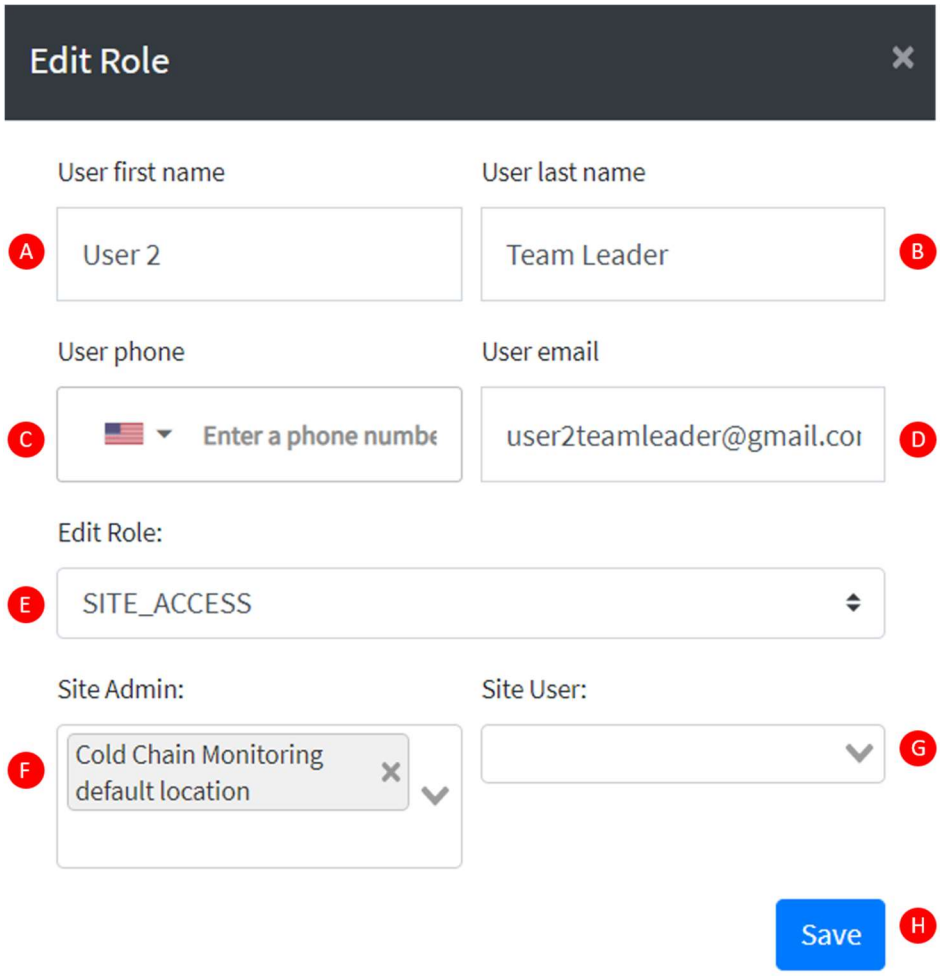
When a new user is added to the system by pressing the ADD USER button, their personal contact information is entered. Enter the first and last name, and the user email. In the top "User role" field, only one of two user roles can be selected: **client_admin and site_access**. If client_admin is selected, then the new user definition is complete. Client_admins have privileges similar to the client_owner, and access to all sites. If site_access is selected, the user can then, subsequently be given site_admin or site_user privileges for one or all sites/locations that are currently in the system (using the lower assignment fields). Note that there can only be only one client_owner in a system, and this role is always assigned during initial system onboarding.



The contact email entered for a new user allows the user to receive an invite via email, and then log onto the R9 system for the first time. When a new user first logs on, they will

create a user password, enter their alert phone number (SMS text message enabled), and initiate OTP validation of the alert phone number. Email can also be used by a new user to receive site reports.

Existing users can be edited by pressing the EDIT button and activating the Edit Users role window which is shown below. This menu is similar to the ADD USER button described above.



A. User first name field.
B. User last name field.
C. User phone number field. This is only required if the user will be added to an alert plan for a site. If a phone number is provided the user will be required to validate their phone number prior to being added to an alert plan.
D. User email field. This is only required if the user will be added to a report plan for a site.

E. Edit Role field. The Edit role field has two available options, client_admin and site_access (similar to add new user screen). Client_admin will provide the new user with permissions equal to the client_owner, thus no site will need to be selected. This user will have access to all sites. The site_access selection should be used if the new user will be restricted to a specific site or sites. **Note:** If client_admin is selected then fields F and G will no longer be displayed.
F. Site_admin field, this field allows the Administrator to assign the new user as site_admin for a specific site(s). Administrators must select all the appropriate sites that the new user will be considered a site_admin. If the user is only considered a site_user, then leave the Site_admin field empty.
G. Site_user field, this field allows the Administrator to assign the new user as site_user for a specific site(s). Administrators must select all the appropriate sites that the new user will be considered a site_user. If the user is only considered a site_admin, then leave the Site_user field empty.
H. Save button, click this button to save the new user configuration to your system.

4.2.5 Alerts

Each customer location/site can have one alert plan with three alert recipients. The "Alerts" screen allows the customer to view and add users to be notified when an alert condition is generated by the system. Note that each location/site may be assigned multiple gateways, and all of these gateways and their respective nodes will drive alerts into the single alert plan for the site.

Anytime a new location/site is created, a default alert plan is created for the site. By default, the user that creates the site (client_owner or client_admin) will be added as the first user in the alert plan. This user can be changed at a later time. Each alert plan must have a minimum of 1 user and a maximum of 3 users. Only users with validated phone numbers can be added to an alert plan. Users will be prompted with a reminder to validate their phone number each time they log into the system. The reminder will continue until a user either opts out of the reminder or until they validate their phone number.

Alert Plan Overview :
The Alert plan defines a list of individuals to be contacted, using SMS text, when your Safezone system experiences an alert condition.
Alert conditions include:
- Gateways or nodes that have not reported recently
- Loss of AC power (gateway only)
- Low battery condition on gateway or node
- Ports that are outside of their configured safe range

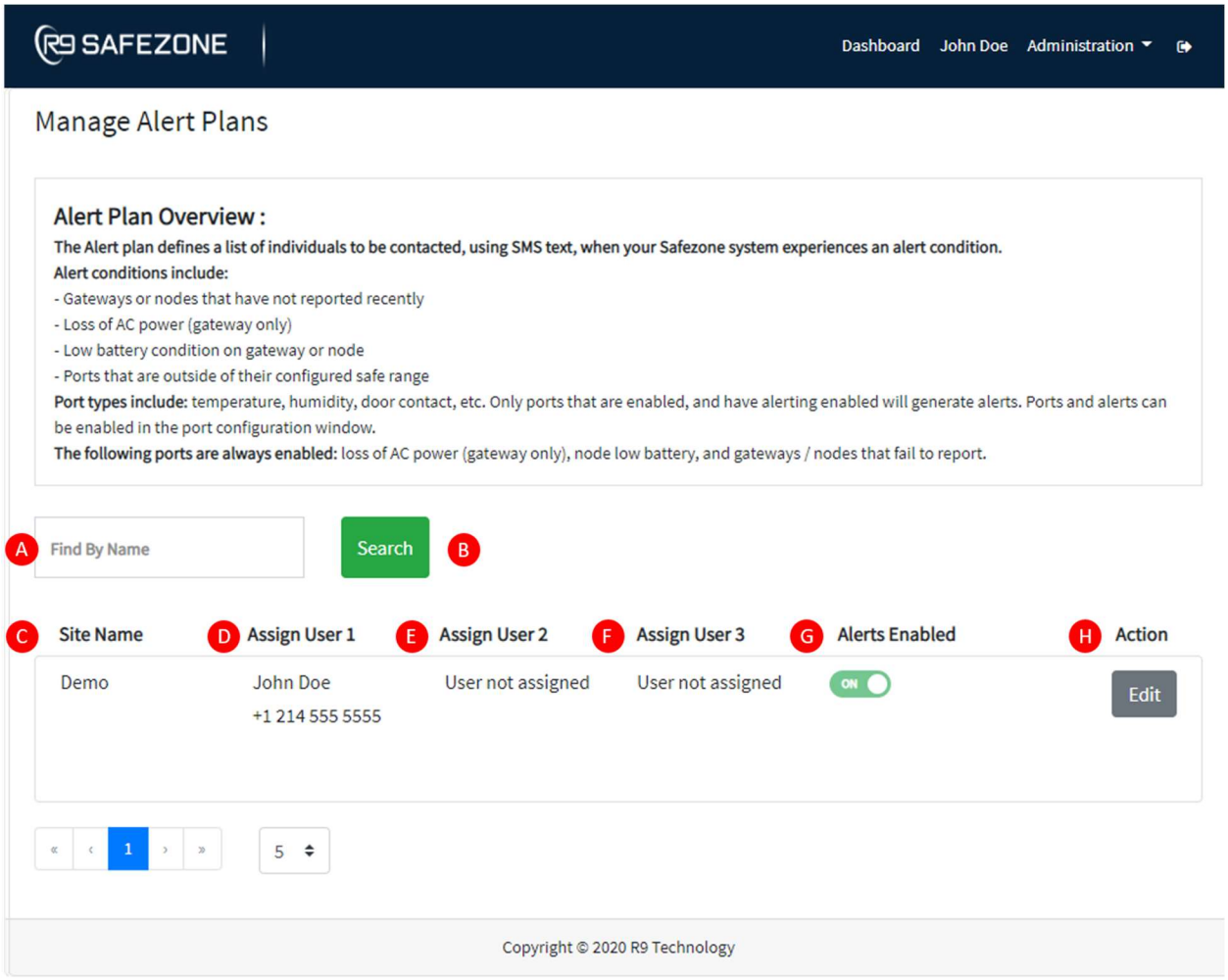
Port types include: temperature, humidity, door contact, etc. Only ports that are enabled and have alerting enabled will generate alerts. Ports and alerts can be enabled in the port

configuration window.
The following port alerts are always enabled: loss of AC power service (gateway only), gateway low battery, node low battery, and gateways or nodes that fail to report.

Whenever an alert threshold is exceeded (for example temperature range), you will receive a maximum of three SMS text alerts (on 15-minute intervals) to indicate the alert condition. After receiving three alerts, you will not receive any more alerts even if the alert condition still exists. If the temperature sampling goes back into the normal range on its own, then the alert condition is reset, and you can now receive another three alerts if the range is exceeded again later. Every time you change the thresholds on a port, for example, the high and low temperature thresholds, the alert condition is automatically reset, and will now activate and send alert SMS text again if the thresholds are exceeded. If you set an alert threshold that is outside the current sample point (current temperature out of range for this example), you will immediately receive an alert on the next sample (15 minutes) assuming the number of samples before alerting is set to 0. This could be done if you want to test the alerting on a specific port.

Alerts can be cancelled at any time by responding with the alert code shown in the SMS text message.

For items like gateway or nodes that fail to report, or node battery alerts, there is typically a delay of 1.5 hours before you will receive an alert. This time frequently allows alerts to clear themselves without user intervention. For gateway power loss (AC power interrupted), you will be notified if the power is out for more than a few minutes on the next reporting interval (15 minutes).



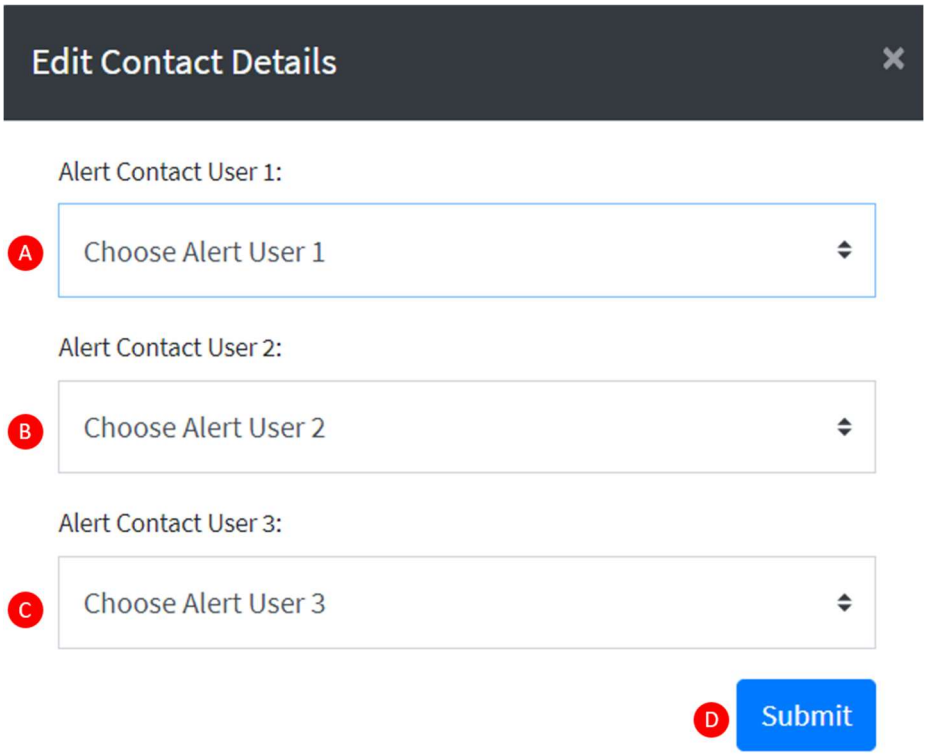
A. Find By Name field can be used for customers having multiple sites and multiple Alert plans. This is a convenient method for sorting plans.
B. Search button, this button initiates search feature.
C. Site Name field, this column displays the name of a site. Each location/site may implement multiple gateways.
D. Assign User 1 field, this column displays the first of three users that will be notified in the case of a site alert. This field defaults to the client_owner, but can be changed.
E. Assign User 2 field, this column displays the second of three users that will be notified in the case of a site alert.
F. Assign User 3 field, this column displays the third of three users that will be notified in the case of a site alert.
G. Alerts enabled button, this toggle button allows alerts to be turned on or off for an entire location/site. Note that a site may have more than one gateway. If, for example, a site is getting a new gateway added, or

experiencing issues which are generating alerts, the alerts can be disabled using this button.

H. Edit button, this button allows the alert plan to be modified.

4.2.5.1 Alert Edit Contact Details

Editing an Alert Plan is achieved using the EDIT button on the Manage Alert Plan window. The image below shows the "Edit Contact Details" window that opens when the EDIT button is clicked. The Edit Contact Details window is used to add and remove users for the specified alert plan. Only client_owners, client_admins and site_admins have permission to modify an alert plan.



A. Choose User 1 field, when clicked, this field will present the user with a drop-down menu of all the validated users which can be added to the sites alert plan.

B. Choose User 2 field, when clicked, this field will present the user with a drop-down menu of all the validated users which can be added to the sites alert plan.

C. Choose User 3 field, when clicked, this field will present the user with a drop-down menu of all the validated users which can be added to the sites alert plan.

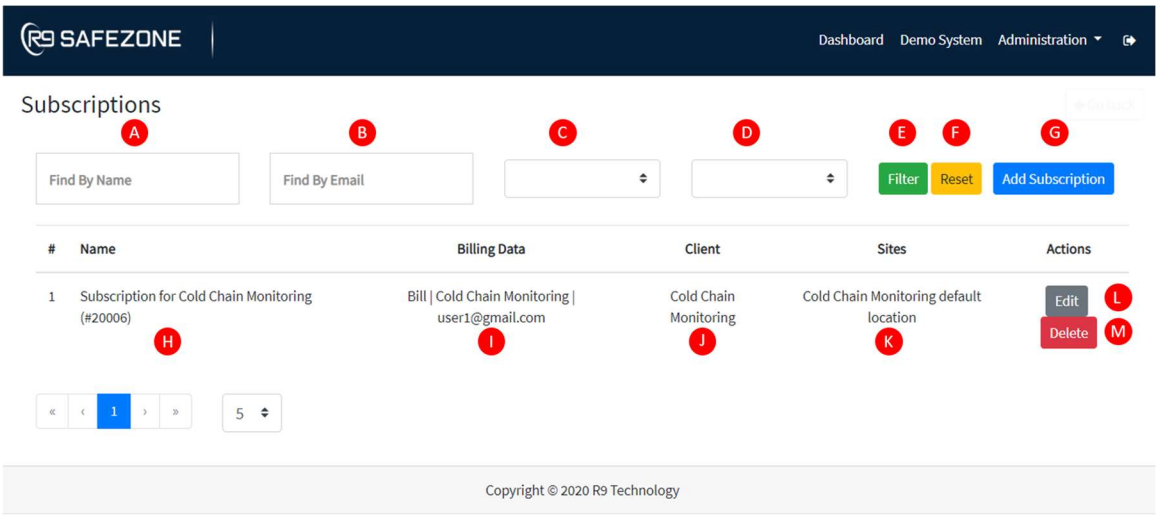
D. Submit button, this button submits the updated contact list for the sites alert plan.

4.2.6 Subscriptions

The “Subscriptions” window allows a user (client_owner or client_admin) to create and manage subscriptions, which are groups of sites that are assigned to a billed entity. A billed entity can contain a billing address that is different from location/site address. The billed entity does not have to contain R9 hardware or systems. The main information which compose the subscription details are: Contact information, annual or monthly billing, site equipment (site or multiple sites). Subscriptions are always accumulations of physical locations or sites.

A client_owner can have multiple subscriptions that are billed separately to different entities. This is useful when separate entities or business need to be billed for their respective portion of the overall monitoring costs.

R9 Technology offers a month to month and annual billing plan which is selected by the client when a site subscription is created.

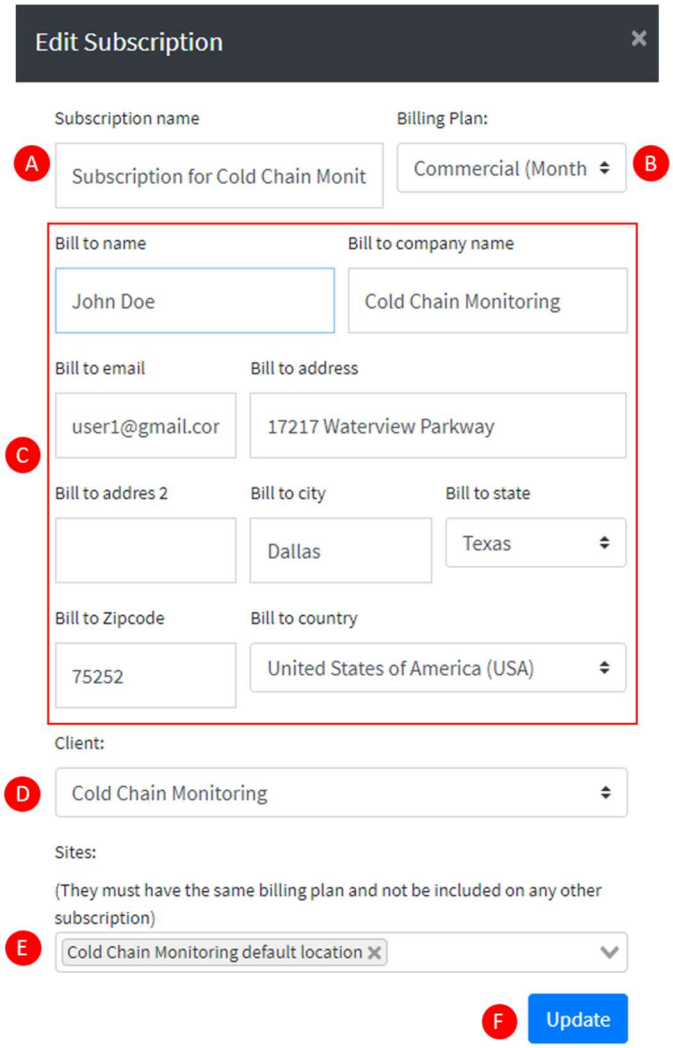


A. Find By Name field can be used for customers having multiple sites. This is a convenient method for sorting site subscription.
B. Find By Email field can be used for customers having multiple sites. This is a convenient method for sorting site subscription.
C. Client search field can be used for customers having multiple sites. This is a convenient method for sorting site subscription.
D. Site search field can be used for customers having multiple sites. This is a convenient method for sorting site subscription.

E. Filter button, this button initiates both the name, email address, client, and site search feature.
F. Reset button, this button will reset all four search fields.
G. Add Subscription button, this button allows the user to create a new subscription.
H. Name column, this column displays the subscription name.
I. Billing Data column, this column displays the billing information associated with the subscription.
J. Client column, this column displays the client name associated with the subscription.
K. Sites column, this column displays the site name associated with the subscription.
L. Edit button, this button allows the user to edit the subscription. Each individual subscription is assigned to a unique billing address that is entered in this screen. While in this screen, all sites/locations are available for assignment to this unique billing entity and address.
M. Delete button, this button allows the subscription to be removed from the system. This action cannot be undone. Note that if a subscription is removed, the associated equipment will quit functioning at the end of the billing period (month or year). This action will not remove the physical equipment from the portal system, but the data transfer will no longer take place at billing period end.

4.2.6.1 Edit Subscription

The edit subscription button allows a user to make modifications to their subscription groups. The following image and information provide an overview of the edit subscription window.



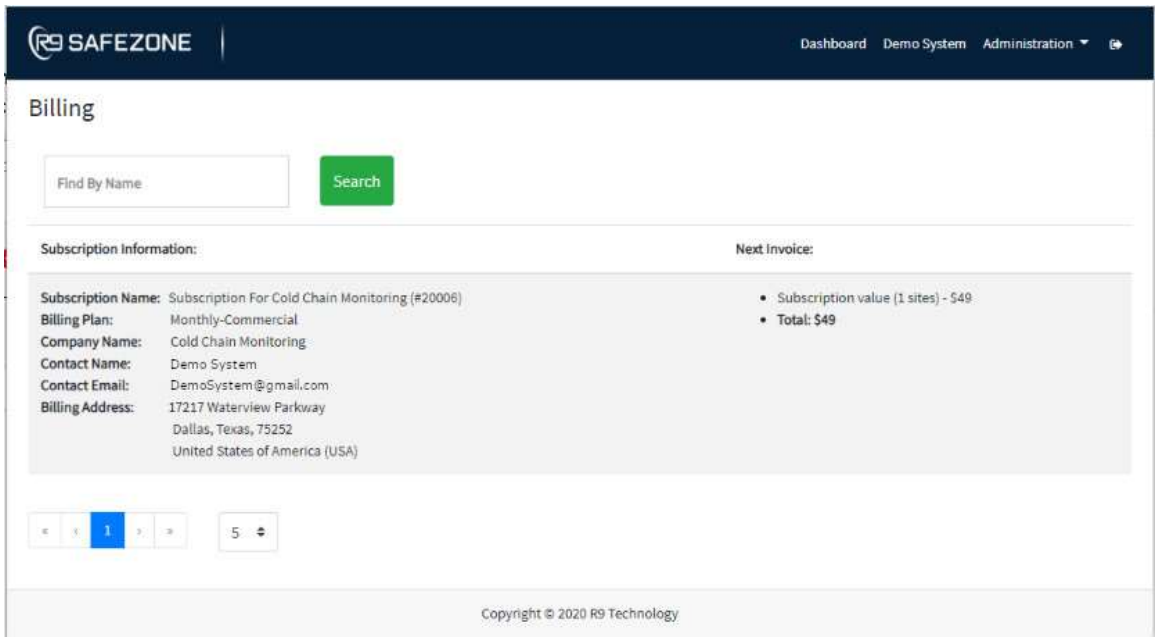
A. Subscription name field allows the user to name the site subscription.
B. Billing plan field allows the customer to select either month-to-month or an annual billing plan. Pricing varies depending on subscription type. Please check with your R9 Sales representative before changing your subscription.
C. Client information fields should be filled out with the customers billing contact information. This information can be unique and not associated with sites where equipment is located.
D. Client selection field. This drop-down menu allows the customer to select the client. There is only one client in the current system.

E. Client site field. This drop-down menu allows the customer to select the site(s) to be added to this portion of the subscription. One or many sites may be added.
F. Update button, this button will submit the subscription form to the R9 system.

4.2.7 Billing

The "Billing" main menu screen provides the user (client) with a summary of their subscriptions. It can be considered as viewing the result of the way subscriptions are currently configured using the subscription menu. The next invoice amounts per subscription are displayed.

Note that the billing system aggregates the currently configured hardware (input in configuration menu) at each site, and calculates the invoice cost by summing all the sites assigned to this particular subscription. The billing address shown can be unique and does not have to be associated with sites that contain R9 hardware. The subscription address, as displayed, is only used for billing and is assigned in the subscription menu.



—

For questions and support, please contact

R9 Technology

17217 Waterview Parkway Suite 1.202Y

Dallas, TX, 75252, USA

Product information

www.r9tech.com

Support e-mail address

requests@r9tech.com