Sensonix Web Services

Instruction Manual

SENSONIX

178337

Contents

1 Sensonix Web Services

The website *https://data.sensonix.net* is the home page for Sensonix services. From the home page the user can learn more about the subscription service plans.

Activating a cellular data plan allow the data collection device to communicate using the cellular network. Click on the secure.sensonix.net link to subscribe to a cellular data plan.

A web services data plan provides cloud storage, data visualization, notifications, and data management for the data collection device. Click on the secure.sensonix.net link to subscribe to a web services plan.

Log into the Sensonix web site by clicking the Sensonix Web Services link or entering *https://data.sensonix.net/login.aspx*.

1.1 Web Services Subscriptions

Follow these steps to activate a web service account.
1. Understand the basic operation of the website.
2. Calculate the data storage requirements for an application.
3. Go to *secure.sensonix.net* to sign up for a subscription service.

The data plans for the web service vary with the number of users and the amount of register data to store, and custom plans are available. When requesting a web service plan please allow up to one business day to complete the implementation. To change a subscription service or discontinue a service, please contact Sensonix at *support.sensonix.net*.

The Web Service Packages are predefined subscription services. The variation within the tiers of subscription services are based on a few characteristics of the website:

Conglomerate / Company

A company contains one or more sites (DXM Controllers). A Conglomerate is a group of two or more companies.

Sites

A site is a storage location for a single DXM Controller. Many sites can be contained within a company

Users

Unique logins to the web site. Only one Username can be logged in at a time.

Data Point

A data point is a single website storage element organized by a timestamp and contains a register value. The value can represent a temperature, humidity, distance, or various other sensor readings. Purchasing a 50,000 point package, you get a total of 50,000 data points of storage in the web server. The number of data points is applied at the company level. With Web Service Packages with multiple companies, the number of data points is applied at the conglomerate level with the administrator defining the split for each company.

Alarms

Notifications created by the user to send E-mail or SMS messages based on conditions of the data.

1.1.1 Calculating the Data Storage Requirements

The amount of website data storage required is based on the setup parameters the user chooses for the DXM Controller.

The setup parameters are:

• The number of data points (Local Registers) to save
• How often the data points are sent to the website
• How many days of history (data retention) to save the data points.

Enter the setup parameters in the Data Point Estimator at *https://data.sensonix.net*. Click **More** to see the data calculator.

Data Point Estimator
13440 data points = 1 ▾ device(s), uploading 20 ▾ data points every 15 ▾ minutes, stored for 7 ▾ day(s).

In the example, a single DXM Controller is configured to send 20 registers of data every 15 minutes. The data storage required to save the data for 7 days would be 13,440 data points. The total data points are set by the Web Service Package. Change the Web Service Package to increase or decrease the total amount of data points.

Adjust the number of days of data retained to manage the total number of data points in the system under the **Settings > Companies**. Click on the edit button next to the company name. The webpage also shows the settings for the company and the limits defined by the service.

1.1.2 Website Data Storage

The tiers of Web Service Packages offer variations of data point storage. The data point storage defines the total amount of memory storage allocated for a company. As data comes in from DXM Controllers, it is saved using a portion of the data storage. When saved data becomes older than the data retention time, data is removed from data storage.

With simple planning, the limit of data point storage should not be reached. If the DXM Controllers are programmed to send more data than the web site is configured to accept in a given time period, a warning message is sent to the company administrator when the data point storage is at 100%. The company administrator must log in immediately to the account and change the number of days data is retained to reduce the amount of storage used at the web server (Under **Settings > Companies**).

New data is not saved if the Data Point Storage is full. Alternatively, more data points can be added by choosing a different Web Service Package.

1.1.3 Subscribe to the Web Services

To subscribe to a web service, follow these steps.

1. Go to *https://data.sensonix.net* and click on the **secure.sensonix.net** link.
2. If you have previously created an account click **Login** to continue. If you are creating a login for the first time, follow these steps.
   a) Select a subscription type and subscription plan.
   b) Create a username and password. Use a valid email address for the username.
   c) Enter the payment information and mailing address.
   d) Click to read the terms and conditions.
   A customer service representative will contact you within one business day to supply log in and password credentials.
3. Set up the website data retention for your application. See *Create a New Site* on page 7.
4. Configure a DXM Controller to push data to the website. See *Modify Local Registers Individually* on page 8.

1.2 Activating and Provisioning a Cellular Plan

Activating the device cellular capabilities requires two basic steps:
1. Activate a cellular plan.
2. Provision the cellular modem on the wireless network.

1.2.1 Activating a Cellular Plan

The Sensonix secure website for purchasing device cellular data plans can be accessed by going to *https://data.sensonix.net* and click on the *secure.sensonix.net* link. If you have previously created an account, click **Login** to continue.
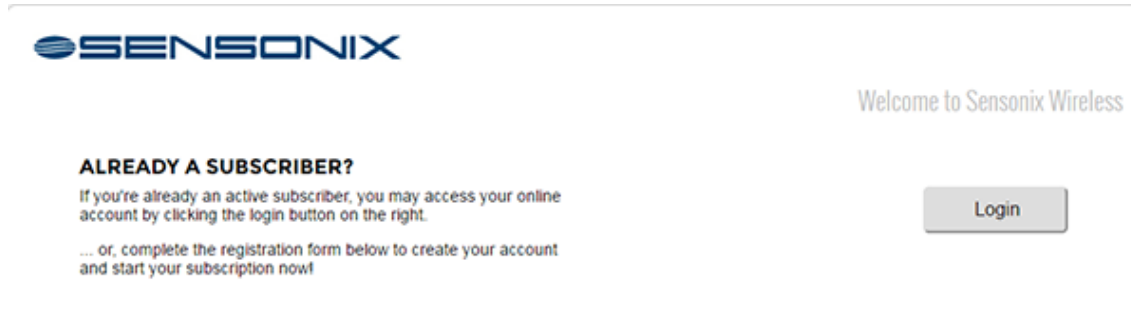
If you are creating a login for the first time:

1. Select the subscription type and subscription plan.
2. Create a Username/Password (E-mail address for Username).
3. Enter payment information, mailing address, and MEID.
4. Enter Cellular MEID (Mobile Equipment Identifier). See below.
5. Click to read the Terms and Conditions.

Although it will only take 20 to 30 minutes to activate a cellular plan, it may take up to 24 hours for the cellular plan to become active on the wireless network.

The **MEID** (Mobile Equipment Identifier) is located on the top of the cellular modem. If the cellular modem is already installed, remove the top cover to view the MEID. The MEID number consists of the numbers 0 through 9 and the letters A through F.

Double check the MEID when entered into the website, an incorrect MEID entry causes delays in processing the cellular plan.

1.2.2 Install the Cellular Modem and Antenna Cable

1. Orient the cellular modem as shown and verify the pins are properly aligned.

2. Firmly press the modem into the 24-pin socket.
3. Attach the antenna cable as shown, starting by connecting one end of the cable to the device base board.

1.2.3 Provision the Cellular Modem

Verify the cellular antenna, antenna cable, and cellular modem are properly installed before provisioning the cellular modem. After a qualified cellular plan is in place and the cellular modem is installed in the device, provision the cellular modem.

1. From the device's LCD top menu, select **System** > **Provision Cell**.
2. Follow the onscreen instructions.
3. After provisioning is complete, cycle power to the device.

2 Logging into the Sensonix Web Services

The web server captures data from the device and allows users to collect and view the data or update and manage the device using a web browser. The data is sent to the web site using either a cellular connection or an Ethernet connection.

A company login will be created with a login and password. Use both the web site and the DXM Configuration Tool to set up and configure your data collection. Use Internet Explorer or Google Chrome as your Internet browser and enter the URL: *https://data.sensonix.net/login*. The login page appears.

2.1 Create a New Site

After you log into the site, go to **Settings** > **Sites**.

1. Click on **+New Site**.

   Create a new site for each DXM that will be sending data to the web server.
2. Enter a site name.
3. Copy the **Site ID** number shown on the dashboard.

   The **Site ID** number created by the web server is used by the DXM Configuration Tool when you create the configuration XML file for the device. The **Site ID** is the address the webserver uses to store the data pushed from the device.

2.2 Modifying the XML Configuration File

Use the DXM Configuration Tool to configure the operation of the device. For more help on all the capabilities of the configuration platform, refer to the DXM Configuration Tool manual.

Launch the DXM Configuration Tool software. You can use one of these three screens to modify registers:

- **Local Registers**—Edits individual registers
- **Modify Multiple Registers**—Edits multiple registers at the same time
- **Local Registers in Use**—Edits individual registers

Refer to the *DXM Configuration Tool Instruction Manual* for more details.

2.2.1 Modify Local Registers Individually

This example configuration sets the device to push registers values to the web server.
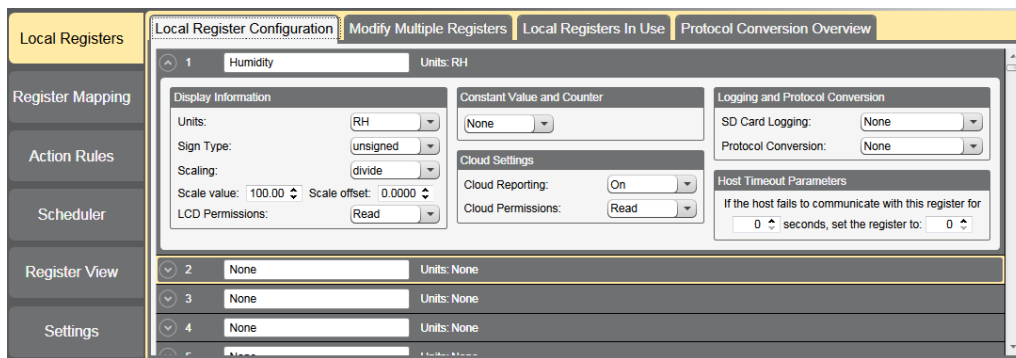
1. Go to the **Local Registers** > **Local Register Configuration** screen.

   The local registers are a pool of integer and floating point registers that can be used by the controller to save data that was created, store data from external devices, or store basic constants. The local registers are where the user defines the data sent to the web server.

   This screen shows how each local register is defined.
2. Click on the down arrow next to the first line for Local Register 1.
   The parameters for Local Register 1 display.
3. To push the register values to the web server, set **Cloud Reporting** to ON.
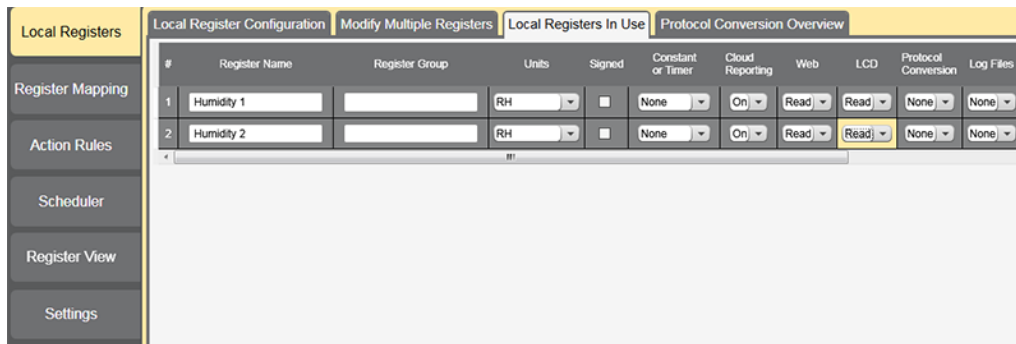4. Set the **Cloud Permissions** to read.

   If the **Cloud Permissions** are set to Read, the web server only views data from the device and cannot write data to the device. If the permissions are set to Write, the web server only writes to the device and cannot read the data. If the permissions are set to Read/Write, the web server can read the data from the device and write to the device from the web.

   This tells the website to display the register and sets this register to read only at the website. The register's contents displays under the **Registers** menu.

Modify Local Registers Individually

2.2.2 Modify Registers Using the Local Registers in Use Screen

Use this screen to modify the parameters of any local registers being used.

1. Go to the **Local Registers** > **Local Registers in Use** screen.
   A list of the local registers being used displays.
2. Using the drop-down lists, change the desired parameters.
3. To push register values to the web server, set **Cloud Reporting** to on and **Web** to read.

   If **Web** is set to Read, the web server only views data from the device and cannot write data to the device. If the permissions are set to Write, the web server only writes to the device and cannot read the data. If the permissions are set to Read/Write, the web server can read the data from the device and write to the device from the web.

   This tells the website to set this register to read only at the website. The register's contents displays under the **Registers** menu.

2.2.3 Modify Multiple Registers

Modify a range of registers from the **Local Registers** > **Modify Multiple Registers** screen.
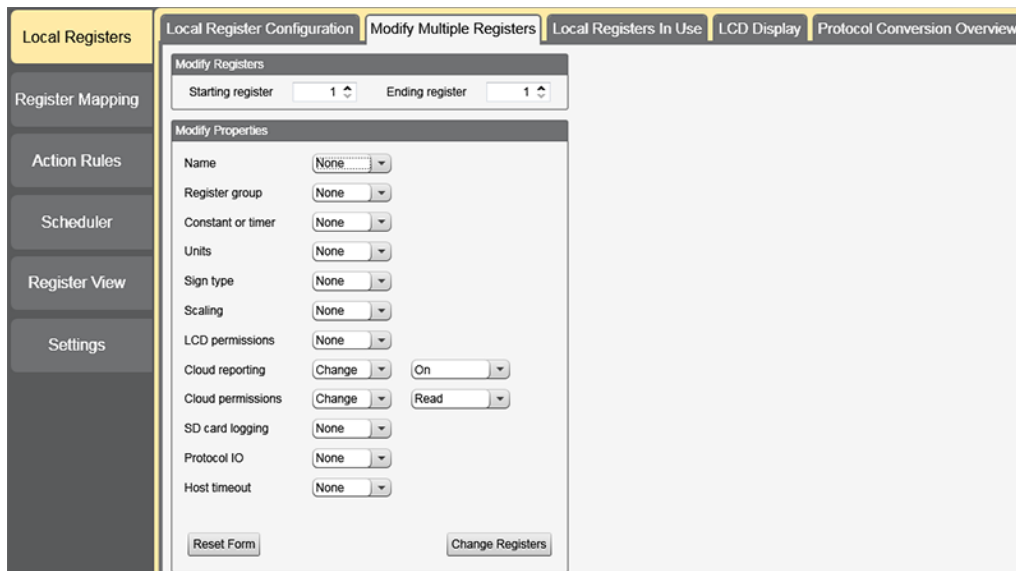
1. Enter the **Starting register** and **Ending register**.
2. Select the value to change using the drop-down list next to each value.
3. Enter the new value in the field provided.
4. To push register values to the web server, set **Cloud Reporting** to on and **Cloud Permissions** to read.

   If the **Cloud Permissions** are set to Read, the web server only views data from the device and cannot write data to the device. If the permissions are set to Write, the web server only writes to the device and cannot read the data. If the permissions are set to Read/Write, the web server can read the data from the device and write to the device from the web.

   This tells the website to set this register to read only at the website. The register's contents displays under the **Registers** menu.
5. Click **Change Registers**.

2.2.4 Configure the Cloud Settings

1. To configure the connection to the web server, go to the **Settings** > **Cloud Services** screen.
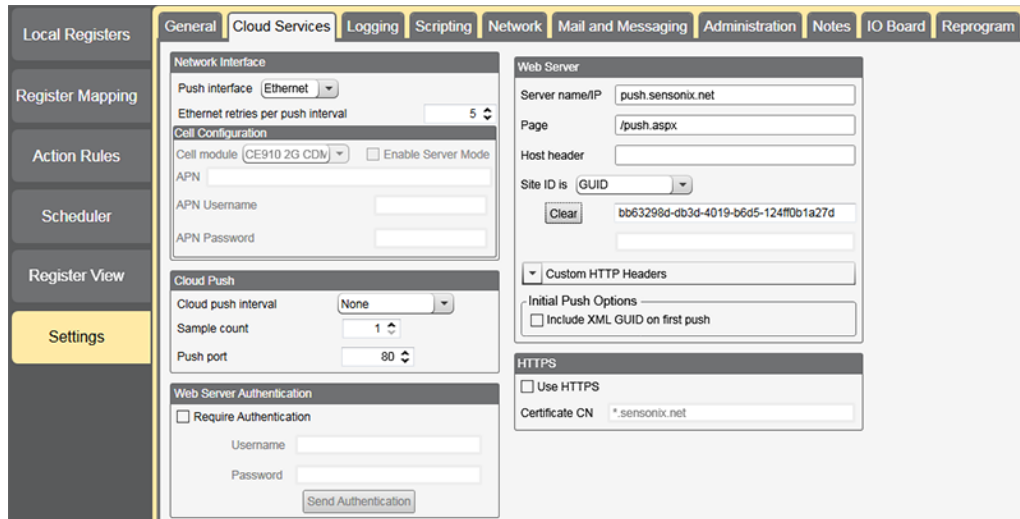
2. Copy and paste the **Site ID**.

    The Site ID is that long string of numbers and letters from the Sensonix Web Services site.

3. Verify the **Server Name/IP** is set to `push.sensonix.net` and the **Page** is set to `/push.aspx` for sending to the Sensonix Web Services site.

4. Set the **Cloud Push Interval** to a value appropriate for your application.

    The **Cloud Push Interval** determines how often the device pushes the data to the web. The faster the push interval, the more data is sent to the site. Cellular plans can only push at an interval of 10 minutes or longer, while Ethernet connections can push at an interval of 1 minute or longer. The **Logging Interval** specifies how often data is gathered by the device.

    For example, if the **Cloud Push Interval** was set to 15 minutes and the **Logging Interval** was set to 5 minutes, then during each data push (every 15 minutes) three sets of data would be pushed to the web.

5. Save the configuration file by going to **File** > **Save**.

    No spaces or special characters are permitted in file names.

6. With a USB cable connected to the device, go to the **Device** > **Connection Settings** menu.

7. Select the appropriate COMM port and click **Connect**.
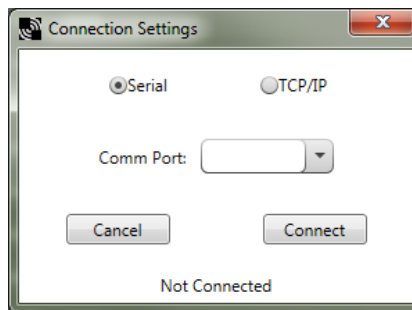
    If multiple COMM ports are visible, try each one until the software is able to connect to the device.

8. Go to **Device** > **Send Configuration to the Device** to upload the new XML file.

2.3 Upload the XML Configuration File to the Website

To upload an XML configuration file to the website, follow these instructions.

1. At the webserver, select **Settings** > **Sites**.
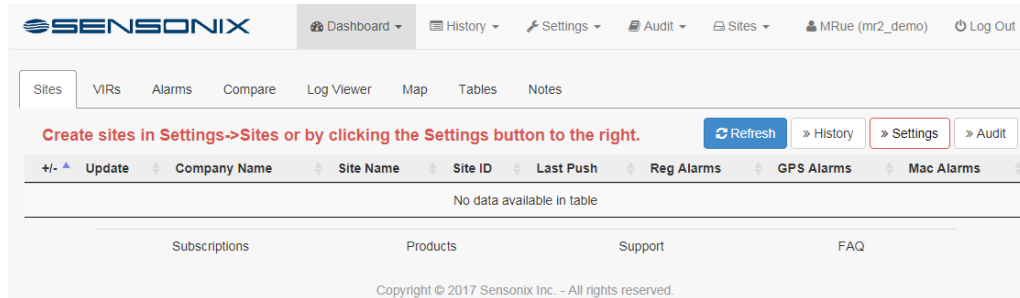
2. Click **Send XML to Web**.
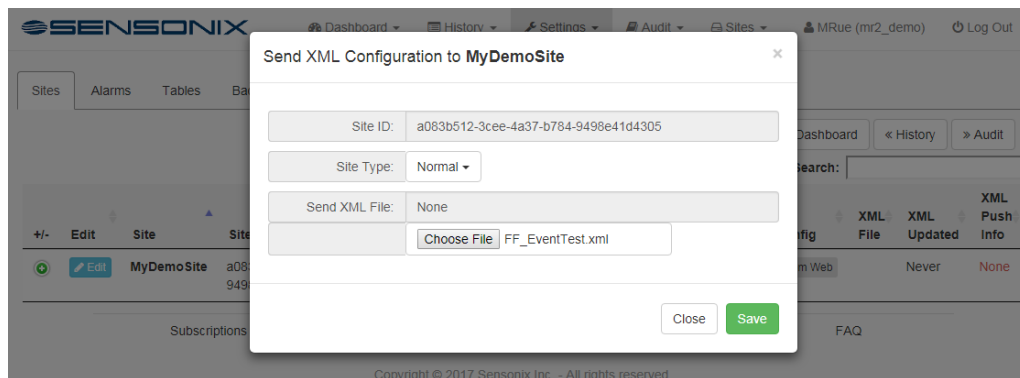
3. Click **Choose File**. Select the file that was just updated to the DXM and click **Save**.
   After the XML file is loaded into the webserver, the webserver uses the register names and configurations defined in the configuration file.
4. Click on the **Site Name** link to go to the configured registers to see the values uploaded by the device.

3 Main Menu Reference

3.1 Dashboard Menu System

The Dashboard page is the page for viewing data collection device data. Use this page to view waveforms, compare waveforms, organize data sets, view alarm conditions, and view GPS coordinates.

Access the following pages from the Dashboard:
- Alarms—Displays your alarms and status rules
- Compare—Compares register data
- Log Viewer—Displays log files sent via email
- Map—Displays the location of the wireless device according to the GPS coordinates defined in the DXM Configuration Tool
- Notes—Captures a history of configuration changes entered by the user
- Sites—Lists all wireless devices pushing data to the website
- Tables—Allows the user to customize their data
- VIRs—Very Important Registers

3.1.1 Alarms

The **Alarm** page displays the alarms and status rules defined by the user.

Define the necessary alarms from the **Settings** > **Alarms** webpage, accessed from either the **Settings** > **Alarms** menu or the white **Settings** button in the upper right.

Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens. For more information, see *Alarm Settings* on page 17.

3.1.2 Compare

Use **Compare** to graphically compare registers collected by the website.

To populate the **Compare** page, follow these steps:
1. Below the graph, select the data collection device from the drop-down list.
2. Select the first data point to graph from the next drop-down list.
3. Click **+Add to Graph**.
4. Continue to select inputs from this or other data collection device(s) and add the data points to the graph.

In the example shown, three data points are graphed from one data collection device. You may select to view the data over the last day, 3 days, 7 days, or a custom date range. Adjust the Y axis range as needed to view the data.

Saving Compare Templates—After the comparison signals are defined, save the template by entering a template name and then clicking **Save**. Reload the template by selecting the template from the template down-down list. Templates can be used by any user within the defined company group.

Multiple Axes—Compare registers of different scales by selecting the appropriate graph axis when adding the signal to the graph.

3.1.3 Log Viewer

Use **Log Viewer** to display the log files sent via email from a DXM Controller.
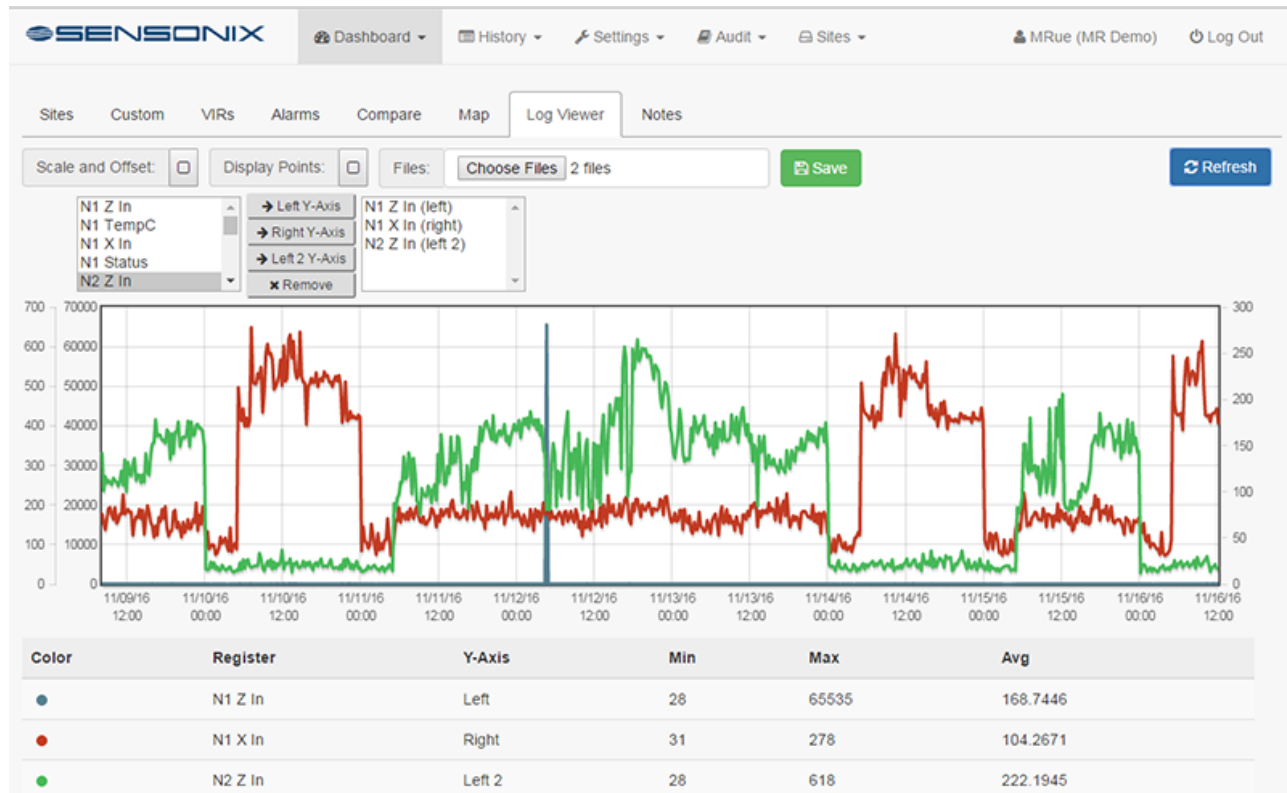
To view a log file:

1. Click **Choose Files**.

2. Select the log file you wish to view and click **Open**.
3. From the panel on the left, select the signals to display and click Left, Right, or Left 2.
   - Left—Sets the selected data to use the y-axis on the left.
   - Right—Sets the selected data to use the y-axis on the right.
   - Left 2—Sets the selected data to use a second y-axis on the left.
4. Select any appropriate options (scale and offset, display points).
5. Click **Refresh** to update the displayed data. Click **Save**.
6.

The data key displays at the bottom of the webpage, along with the left and right axis fields. To change the axis minimum and maximum, enter view values and click **Refresh**.

3.1.4 Map

Use **Map** to view the position of the wireless device on a map scaled to the device positions.

To view the location of your wireless devices, define the GPS coordinates in the DXM Configuration Tool. GPS coordinates can be a live feed from a GPS sensor or can be a fixed location. Save your XML file before uploading it to the data collection device.
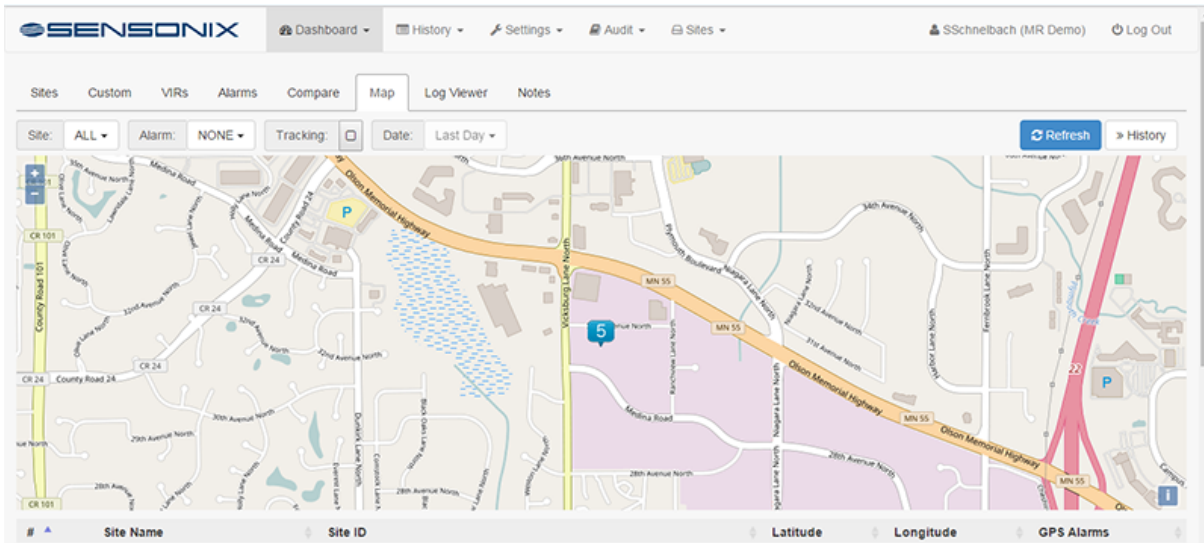
Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens.

3.1.5 Notes

Use **Notes** to capture the history of configuration changes or application changes for your wireless device.

Users can add notes to the DXM configuration file using the DXM Configuration Tool or enter notes from the website. To add a new note from the website:

1. Click **+Add New Note**.
2. In the **Create New Note** dialogue box, select the **Site** from the drop-down list of available sites.
3. Enter a subject line.
4. Type your note.
5. Click **Add Note**.

Click **Refresh** to update the displayed data.

3.1.6 Sites

The **Dashboard** > **Sites** webpage displays a glimpse of the data collection device pushing data to the website. There is a unique site ID for each controller pushing to the website. To create a new site, go to **Settings** > **Sites**.
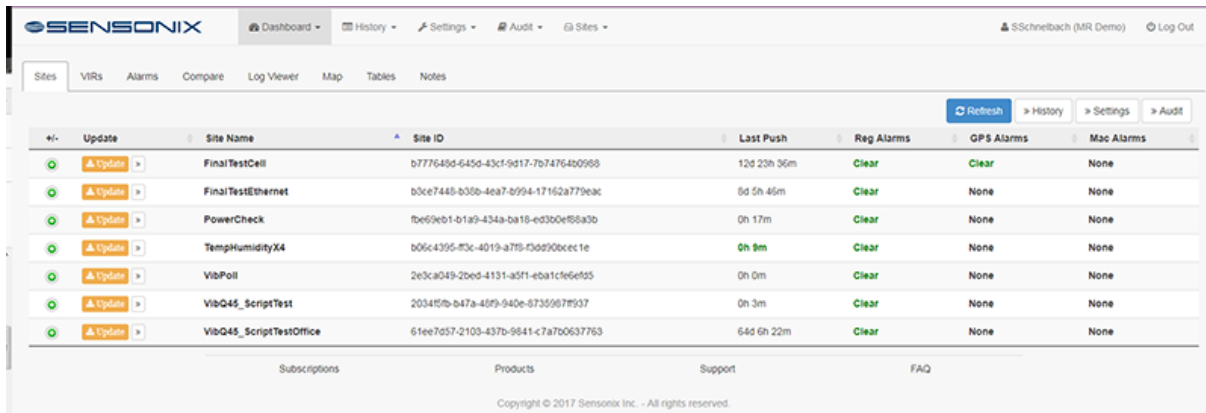
Click the green + to the left of the site listing to display the basic information about the connection with that wireless device. Click on the site name to view the registers associated with that device. From this webpage, you may compare the register values or select them as Very Important Registers (VIRs) to display on the VIR webpage.

Click **Update Device** to send data to the device at the next push interval.

The Communications Type defines the method to communicate with the data collection device. Typically, ethernet or cellular connected devices wait until the next push interval; cellular connected devices have the option to send SMS(text) messages to immediately update the data collection device.

The data destined for the data collection device is queued for the next push interval. Data includes:
- Local Register data—Update Local Register data on the data collection device
- Configuration File—XML file from DXM Configuration Tool
- Script File—ScriptBasic programming file; *.sb
- Generic File—ScriptBasic support file and data files for the root directory of the SD card
- Update time—Adjust the real time clock on the data collection device
- Clear HTTP Logs—Clear history files of uploaded data to the webserver
- Set Root Password—Set the root password for the device, restricts configuration tool changes
- Set LCD password—LCD password locks the LCD display for the data collection device
- Reboot—restarts the data collection device processor, but does not effect the I/O board, ISM radio, or display board.
- Firmware File—Updates the data collection device firmware with a *.hex file.

After a message is queued for the device, the message count is shown under the **Pending** column. Click on the **Pending** count for the device to get more detailed data.

SMS messages are sent immediately and do not show up as pending events. SMS messages are not guaranteed to be delivered.

Click **Settings** to display the **Settings** webpage. From here, you can adjust the settings of the website or device configuration files.

Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens.

3.1.7 Tables

Use the **Tables** webpage to view a customized organization of your data as it is defined under **Settings** > **Tables**.

To compare selected data points:

1. Select the checkbox next to the **Compare** button.
2. Select the individual data points to compare.
3. Click **Compare**.

The selected data points are graphically displayed on the **Compare** webpage.

Click **Refresh** to update the displayed data.

Click **Settings** to display the **Settings** webpage. From here, you can edit, delete, or arrange the register data that displays on the **Dashboard** > **Tables** webpage. For more information, see *Tables Settings* on page 18.

3.1.8 Very Important Registers (VIRs)

The **VIRs** webpage allows users to view a subset of the total push data for a device site.

To add registers to the VIRs list:

1. Go to the **Dashboard** > **Sites** webpage.
2. Click on the link to the site name that you'd like to add to the VIR page.
3. Click on the **VIR+** button next to the desired register.

These selected registers now appear on the VIRs webpage.

Click **Refresh** to update the displayed data.

3.2 History

History maintains logs of information about the device and its operation.

Access the following pages from the **History** page:
- **Alarms**—Displays the history log for the alarms defined in the website
- **Backups**—Logs the back-up time and status if an FTP site is set up to back up the webserver data
- **GPS**—Displays the history log for Geo fencing alarms
- **Updates**—Tracks the data sent from the website to the data collection device
- **Uploads**—Contains a day history of raw data feeds from the data collection device

3.2.1 Alarms

The **Alarm** page displays the history log for the alarms defined in the website.

This page does not display alarm conditions set at the DXM Controller level.

3.2.2 Backups

The **Backups** page logs the backup time and status if an FTP site is set up to backup the webserver data.

Click **Refresh** to update the displayed data. Click **Download** to download the site data from a specific date. Clicking the white buttons takes you to those screens.

3.2.3 GPS

The **GPS** page displays the history log for Geo fencing alarms.

Geo fencing alarms are defined under the **Settings** > **Alarms** webpage.

Click **Refresh** to update the displayed data. Click **Download** to download the site data from a specific date. Clicking the white buttons takes you to those screens.

3.2.4 Updates

The Updates page tracks the data sent from the website to the DXM Controller.

Register updates, time updates, configuration file updates, or ScriptBasic program updates are saved in this log.

Click **Refresh** to update the displayed data. Click **Download** to download the site data from a specific date. Clicking the white buttons takes you to those screens.

3.2.5 Uploads

Contains a history of raw data feeds from the DXM Controller.

The first push data from the DXM Controller after powering up is an initialization packet that contains extra metadata about the controller. Each log is assigned an id number, and the list of logs is date and time stamped to indicate when the file was transferred from the wireless device to the website.

By default, only the last day's log file history is displayed, but you may select to see three or seven days of log file activity.

Click **Refresh** to update the displayed data. Click **Download** to download the site data from a specific date. Clicking the white buttons takes you to those screens.

3.3 Settings

Use the **Settings** page to manage parameter settings for various website functions.

Access the following pages from **Settings**:
- **Alarms**—Adds new alarm conditions using the New Alarm button
- **Backups**—Schedules a website backup of various data logs to a FTP server
- **Companies**—Add a new company or adjust company-level parameters
- **Custom**—Creates custom views of register data in a spreadsheet format
- **Sites**—Contains the various settings for individual DXM Controllers
- **Users**—Add new users and maintain existing users for the website

3.3.1 Alarm Settings

Use the **Alarm** page to add new alarm conditions.

Select the alarm type and enter the parameter data. Alarm types include the following.

Connectivity—Detects if the DXM Controller is no longer sending data to the website. If the DXM Controller is programmed to push data every 30 minutes, set the connectivity alarm to 2× to 3× that time plus some guard band, approximately 70–100 minutes. If network connectivity is expected to be poor, extend the alarm time to prevent false alarms.

Register Limit—Detects if the website register limit is reached. The register limit is based on the amount of storage the website subscription has purchased. For more information, see *Create or Edit an Alarm* on page 20.

Cross Site—Each DXM Controller is expected to have a unique Site ID string. If more than one DXM Controller has the same Site ID string, the push data may be corrupted. Set this alarm to catch multiple DXM Controllers pushing to the same Site ID.

Register—Set based on the data sent to the website. A data comparison is made with the incoming data to create an email.

Geofence—Create a fence based on a rectangular set of GPS coordinates. Any push data marked with GPS coordinates outside the Geofence creates an alarm condition.

Click **Edit** to change any alarm setting, including selecting the alarm type, site name, warning timeout, error timeout, and the email address to send email alerts to.

Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens.

3.3.2 Backup Settings

Use the **Backup** page to schedule a website backup of data logs to an FTP server.

From **Settings** > **Backups**, define the data to dump, site name, backup schedule, and FTP parameters. For instructions, see *Create an FTP Backup* on page 20.

Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens.

3.3.3 Company Settings

Use **Companies** to add a new company or adjust company-level parameters.

Most parameters on the **Settings** > **Companies** page require an administrator or higher level of website permissions.

3.3.4 Site Settings

The **Sites** page contains the settings for individual data collection devices.

Click on the **+** at the left of the site row to display information about the site configuration.

Edit—Allows the user to:
- Change the site name
- Move the site to another conglomerate or company (permissions required)
- Set up authentication for any username or password that must be sent by the data collection device to gain access to the website; the authentication username and password must be set up on the data collection device
- Select **Auto-Configure**
- Select a ScriptBasic file

Enable **Auto-Configure** to have the data collection device download a new XML configuration file and ScriptBasic file from the website. Enter the data collection device's serial number into the field. When the data collection device pushes to the webserver, a new XML file and optionally a ScriptBasic file downloads to the device. Use Auto-Configure when deploying of a large number of data collection devices.

Send XML to Web and **Get XML from Web**—Upload or download the configuration file to allow the website to be automatically populated with configuration parameters. XML configuration files created from the DXM Configuration Tool are used for the data collection device and for the website.

New Site—Creates a new site location for the DXM Controller to push data.

Click **Refresh** to update the displayed data. Clicking the white buttons takes you to those screens.

3.3.5 Tables Settings

Use the **Tables** page to create custom views of register data in a spreadsheet format.

> Select minimum or maximum values to highlight in yellow or red on the graph.
> -- OKAY, I'm not sure how to do this. I tried with the demo configuration. I'll try again, but so far nothing is happening.

1. Define the descriptions for up to five column headers of data.
2. Add rows by clicking **Add Row** on the upper right of the page.
3. Select the registers to display in each column.
4. Click **Save**.

This custom view appears on the **Dashboard** page.

Click **Refresh** to update the displayed data.

3.3.6 User Settings

Use **Users** to add new users and maintain existing users for the website.

Changing user settings requires manager or higher permissions.

The following permission levels may view these screens.

Permissions	Dashboard	History	Settings	Audit
Multi-Admin	x	x	x	x
Administrator	x	x	x	x
Manager	x	x	x	
View Only	x	x		

The following permission levels may create, edit, or delete within these screens.

Permissions	Company	User	Site	Alarm	Backups
Multi-Admin	x	x	x	x	x
Administrator		x	x	x	x
Manager			x	x	
View Only					

3.4 Audit

Use the **Audit** page to maintain logs of changes for this company, including changes to the XML configuration, alarms, backups, users and companies.

The **Audit** page requires a manager or higher permissions access the audit log data. Access the following pages from **Audit**:

- **Sites**—View the log file of adjustments made to the XML configuration file by site name
- **Alarms**—View the creation of or changes to alarm conditions
- **Backups**—View the creation of or changes to backups conditions
- **Users**—View the log that tracks changes made to user profiles
- **Companies**—View all company changes

3.5 Sites

The upper level **Sites** menu displays the list of Sites from **Dashboard** > **Sites**.

4 Configuration Instructions

4.1 Create or Edit an Alarm

Alarms create email or SMS notifications that alert users when user-defined conditions exist. The user must have Administrator or Manager permissions to create or edit website alarms. After an alarm is defined, edit the alarm by clicking **Edit**.

1. At the Sensonix Web Services website, select **Settings** > **Alarms**.
2. Click **+ New Alarm** to define a new alarm condition.

A pop-up window appears.

3. From the drop-down list, select the Alarm Type.
   - **Connectivity**—Detects if the DXM Controller is no longer sending data to the website. If the DXM Controller is programmed to push data every 30 minutes, set the connectivity alarm to 2× to 3× that time plus some guard band, approximately 70–100 minutes. If network connectivity is expected to be poor, extend the alarm time to prevent false alarms.
   - **Register Limit**—Detects if the website register limit is reached. The register limit is based on the amount of storage the website subscription has purchased. For more information, see *Create or Edit an Alarm* on page 20.
   - **Cross Site**—Each DXM Controller is expected to have a unique Site ID string. If more than one DXM Controller has the same Site ID string, the push data may be corrupted. Set this alarm to catch multiple DXM Controllers pushing to the same Site ID.
   - **Register**—Set based on the data sent to the website. A data comparison is made with the incoming data to create an email. The Duration parameter defines a trigger based on multiple register values over a period of time. The Count parameter defines a trigger based on the last X number of reports coming to the website.
   - **Geofence**—Create a fence based on a rectangular set of GPS coordinates. Any push data marked with GPS coordinates outside the Geofence creates an alarm condition.
4. Define the alarm name.
5. Select the site name.
6. Select the local register, comparison operator, and the comparison value for the alarm testing.
7. To send an email based on the alarm conditions, select Enable Email Alerts and enter a valid email address.
8. Click **Save**.

4.2 Create an FTP Backup

1. On the Sensonix Data Services website, go to **Settings** > **Backups**.

2. In the upper right corner of the screen, click **+ New Report**.

A pop-up window appears to enter parameters for the FTP backup.

3. Select the type of backup report to create.

    •   Registers—All Local Register data defined in the site
    •   Logs—Data sent from the DXM Controller to the web server; data is only recorded for 24 hours
    •   Alarms—Alarm data
    •   Updates—Data transactions sent from the web server to the DXM controller.
    •   Audit Sites—Change log for site data
    •   Audit Alarms—Change log for alarm data
    •   Audit Users— Change log for users

4. Select the Site name to create the backup, then define the schedule of the FTP backup.

    •   Daily
    •   Weekly
    •   Monthly

5. Define the FTP address, username, and password of the site to send the report data.
6. Select the maximum number of retries for the backup to be sent.
7. Set the desired time zone/time off of UTC for the backup to operate under.
8. Click **Save**.

4.3 Setting the DXM Controller to use Authentication

The device can be configured to send login and password credentials for every HTTP packet sent to the webserver. This provides another layer of security for the webserver data.

Setup requires both the webserver and the device to be given the same credentials for the login and password. The webserver authentication username and password are not stored in the XML configuration file and must be stored in the device.

1. From within the DXM Configuration Tool, go to **Settings** > **Cloud Services**.

2. Define the username and password in the **Webserver Authentication** section of the screen.

The first time you select **Require Authentication**, a pop-up box appears with additional instructions. Since the data is not stored in the XML configuration file, it is hidden from view of the DXM Configuration Tool.

3. Click on **Send Authentication**.

The controller must be connected to the PC for this operation to succeed.

The data transmits directly to the device's non-volatile memory. If successful, a pop-up window appears, asking to reboot the device.

4. Select **Yes** to reboot the device.

4.3.1 Setting the Web Services to Use Authentication

1. At the Sensonix Web Services site, go to **Settings** > **Sites**.
2. To edit the site settings, click **Edit** on the line of the site name.

At the bottom of the pop-up window is a checkbox to enable authentication/validation.

3. Enter the same username and password as used in the DXM Configuration Tool. The username and password do not need to be a defined user within the Sensonix Web Services website.