Omega Enterprise Gateway 2.4

User's Manual

Omega Headquarters:

Omega Engineering, Inc.

800 Connecticut Ave. Suite 5N01, Norwalk, CT 06854

Toll-Free: 1-800-826-6342 (USA & Canada only)

Customer Service: 1-800-622-2378 (USA & Canada only)

Engineering Service: 1-800-872-9436 (USA & Canada only)

Tel: (203) 359-1660

Fax: (203) 359-7700

e-mail: info@omega.com

Website: omega.com

Omega Engineering, Limited:

1 Omega Drive, Northbank, Irlam Manchester M44 5BD United Kingdom

Omega Engineering, GmbH:

Daimlerstrasse 26 75392 Deckenpfronn Germany

M5666-1122

Table of Contents

1 Introduction

OMEGA Enterprise Gateway 2.4 (OEG 2.4) is replacement software for the OMEGA OPC Server, iCONNECT, iLOG HTTPGet, iPort, Mail Notifier, Virtual Coordinator, and OMEGA Dashboard. Users currently using the aforementioned software, are encouraged to install OEG. OEG supports the following OMEGA products:

- Legacy OMGEA Probes/Sensors
- Wireless Transmitters
- Smart Probes
- Smart Interfaces

The OEG 2.4 server can be installed on the following OS/Platforms: Windows 7, 8, 9, 10, & 11. Windows Server 2008, 2012, & 2016. All OS are 64-bit. OMEGA does not recommend operating OEG on 32-bit OS. The OEG web client is platform-independent. The minimum hardware requirements for server installation are: Dual Core: CPU 2.4 GHz or higher; Memory: 500 GB or higher.

Note **Disclaimer:** Functions described in this document are subject to the features outlined in the license tier the user has purchased.

1.1 Use Scenarios

OMEGA Enterprise Gateway 2.4 is a bridge between OMEGA sensing devices and industrial applications. It is a standalone IoT sensing software that delivers device provisioning, state and status monitoring, data logging, visualization, and analytics. A variety of OMEGA devices are supported by this Gateway software. Typical application deployment scenarios are shown below:

1.1.1 Integrated with Enterprise Applications

OMEGA Enterprise Gateway can feed sensing data to the OPC UA compliant applications such as SCADA, HMI, MES, etc. via the OPC UA server (licensed). Once the user adds OMEGA devices to the Gateway, the Gateway automatically exposes all sensing data as OPC UA nodes. The Enterprise application can then pull all OPC UA node values and display them on the screen.

1.1.2 Standalone Solution for Sensing, Archiving, and Analytics

In many environment sensing applications such as hotel room temperature monitoring a building temperature/humidity monitoring, OMEGA Enterprise Gateway can provide real-time monitoring, alarms, notifications, archiving, and analytics that are required in these applications.

2 Installation

The OEG 2.4 zip file contains the installer package for the software. Follow these steps to complete the installation process:

Step 1: Unzip and open the Omega Enterprise Gateway file downloaded from the Omega website.

Note: Included in the installer package are the OEG Application Files, .msi installer file, User's Manual, Release Notes, License, Copyright Notice, and End User License Agreement.

Step 2: Click the **OEGOneClickInstall.msi** file and proceed through the setup to launch Omega Enterprise Gateway for the first time.

Note: A desktop shortcut icon of Omega Enterprise Gateway is created after the installation. This shortcut will launch OEG after the initial installation.

Step 3: During the Omega Enterprise Gateway Setup process, the user will be prompted to complete the OPC UA Local Discovery installation wizard.

Figure 1: OPC UA Local Discovery Server installation

Step 4: Once the installation process is complete, OEG will launch automatically.

3 Logging In

3.1 First Time Log-In

When logging into OEG for the first time, click **Need Help?** to be presented with a one-time Username and Password.

Username: **admin**
Password: **Omega**

Users will be prompted to create a new password upon a successful first-time login. The Username can be changed by navigating to the **System Settings**.

If first-time login is not possible, the Omega Enterprise Gateway may need to be power cycled. To power cycle the OEG software, navigate to the **Windows OS Services** application on the computer, locate **Omega Enterprise Gateway** in the list of items, right-click Omega Enterprise Gateway, click **Stop,** and then click **Start** to complete the power cycle. Users may then attempt first-time login again.

4 Device Management

Once logged in, users will be directed to the **Devices** tab of OEG. From this interface, users will be able to manage the devices connected to OEG.

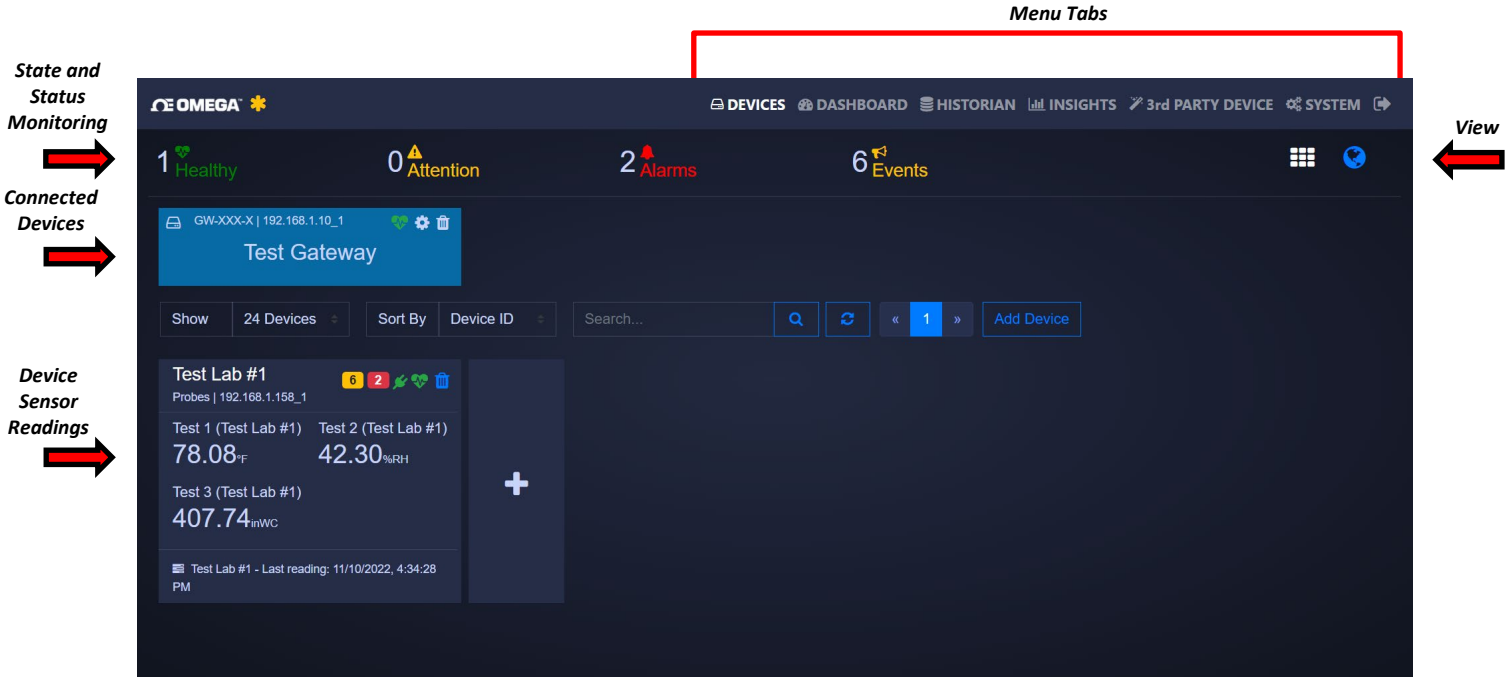

Figure 2: OEG home interface

Important: Devices connected directly to OEG through a USB, Serial, or TCP connection must be removed from OEG if they will be used with another application such as SYNC configuration software.

4.1 Add Device

To add a device, click the + icon to the right of the device readings or click the **Add Device** and fill out the product details, connection parameters, and reading interval of the device that will be added.

4.2 Delete Device

To delete a device, locate the icon located next to the **Connected Device** that will be deleted.

4.3 Rename Device

Clicking the icon allows users to rename the device.

4.4 Refresh

To refresh the list of devices, click the icon located near the device search bar.

4.5 View

The View tab offers options regarding how data will be displayed.

4.5.1 Tile View

Provides a standard tile view of the interface.

4.5.2 Map View

Provides a map view of the connected devices by displaying their location.

Note: Map View is only available on **OEG Pro**, **OEG Business,** and **OEG Business Pro**.

4.6 Device Settings

By clicking on the **Device Readings**, OEG will display live readings, alarms and events, and settings for that device.

4.6.1 Measurements

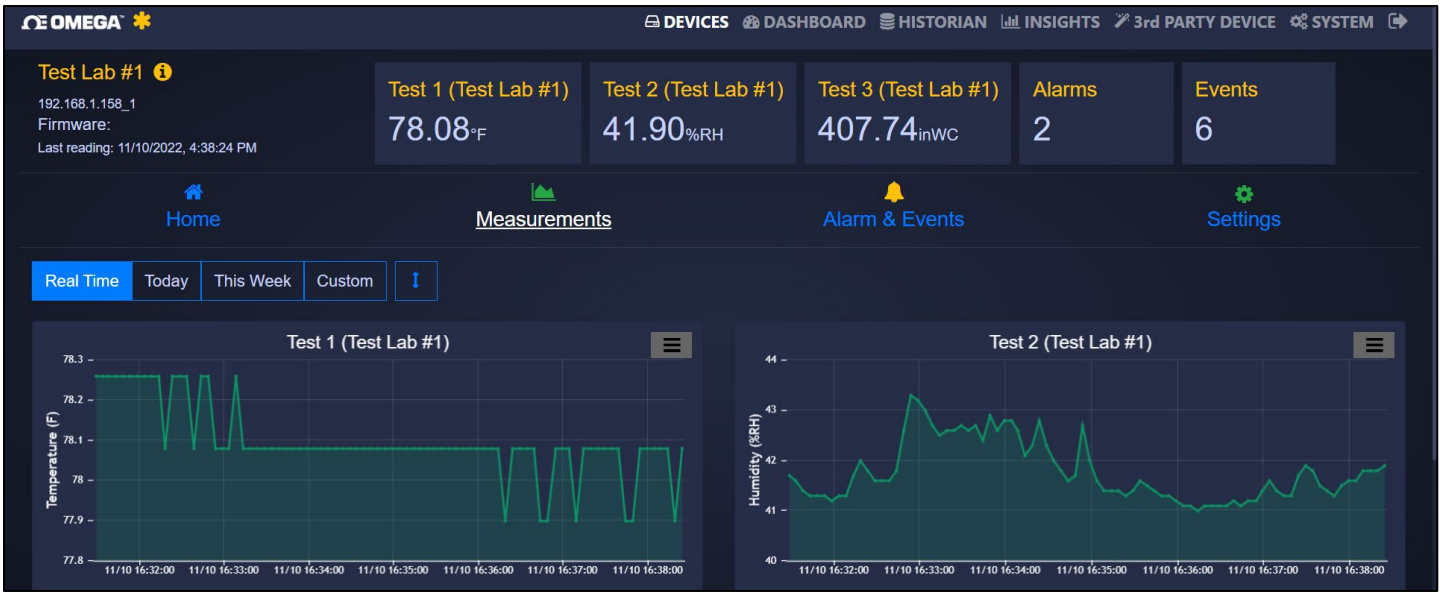

Figure 3: Device Readings and Measurements

The Measurements tab displays live readings for the device. It allows users to change from live readings to a specified range of time.

4.6.2 Historic Alarms and Events

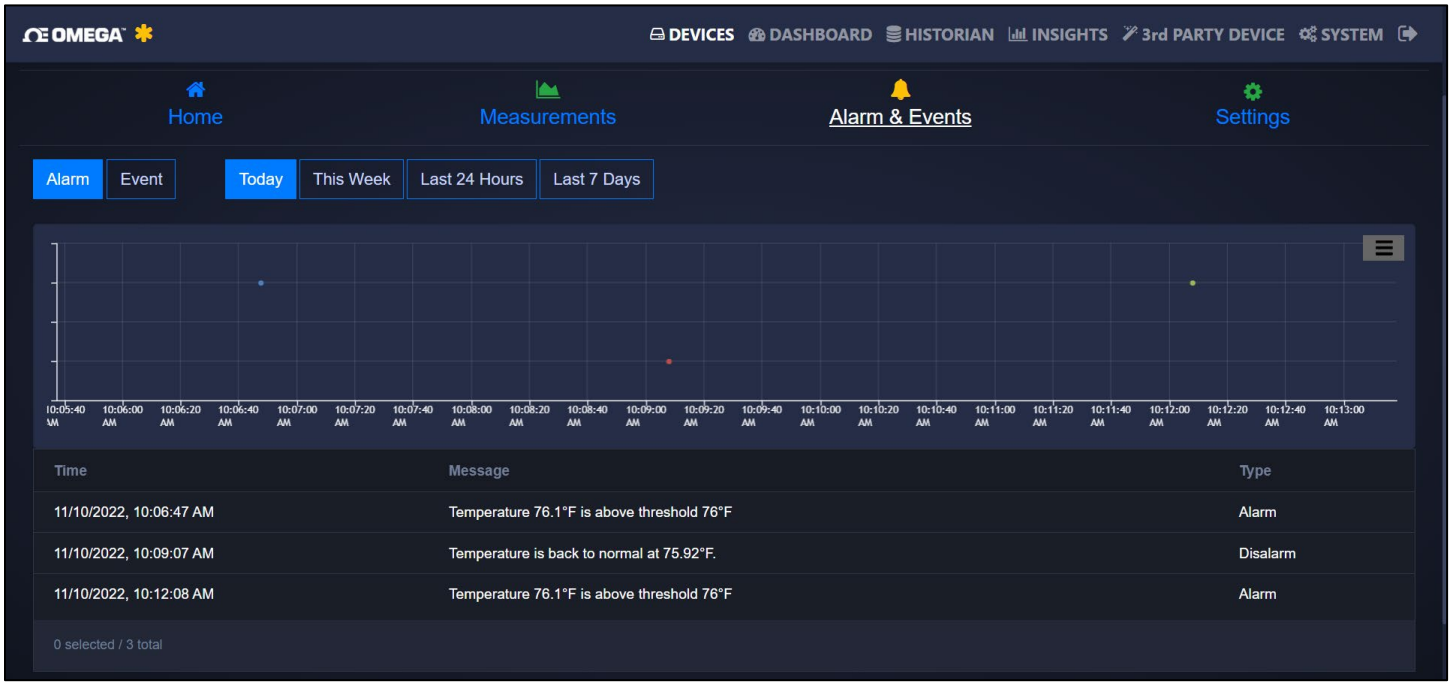

Figure 4: Historic Alarms and Events interface

The Alarms and Events tab displays all alarms and events that were triggered by this device. It includes a short message describing the nature of the alarm/event.

Note: Historic Alarms and Events are only available on **OEG Pro**, **OEG Business**, and **OEG Business Pro**.

4.6.3 General Settings

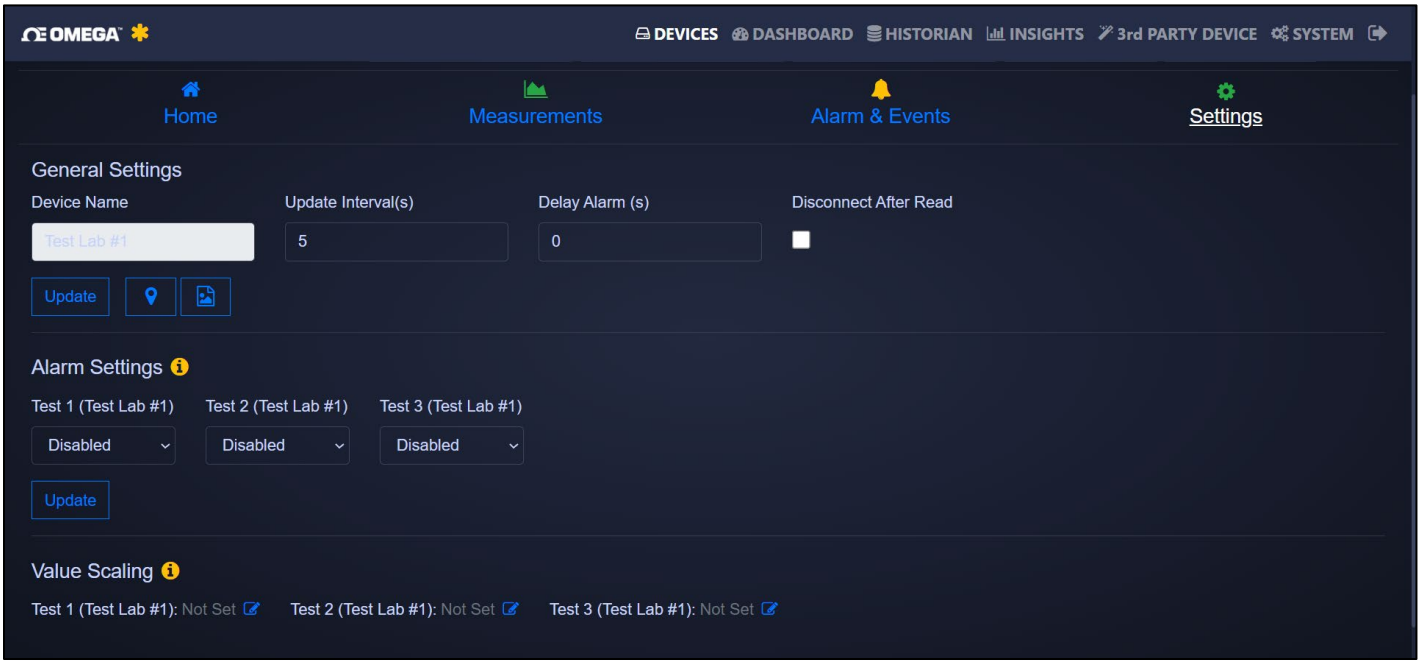

Figure 5: Device Settings (General, Alarm, and Value Scaling)

The **Settings** tab allows users to change all settings relevant to how the device interacts with OEG. Users can customize device name, device location, and all settings relevant to alarm and event thresholds.

Note: Value Scaling is only available on **OEG Pro**, **OEG Business**, and **OEG Business Pro**.

4.6.4 Setting a Device Location

OEG allows users to assign a **Location** to any device connected to OEG. Device locations can be viewed by switching from the default **Tile View** to the **Map View** in the **Devices** menu tab. To set a device location, follow these steps:

Step 1: Click the **Device Tile** of the device that will have its location changed.

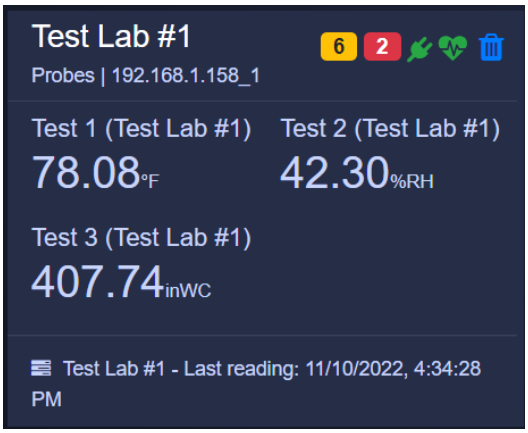

Figure 6: Device Tile as it appears in the OEG UI

Step 2: Click on the device **Settings** tab and click the **Location** icon. A **Set Device Location** pop-up will appear.

Step 3: The user can either drag-and-drop the blue pin to the desired location or click on the **Move to your location** button to use the current location associated with the PC. Using the Move to your location button requires permission to share the location of the PC. Click **Ok** when finished.

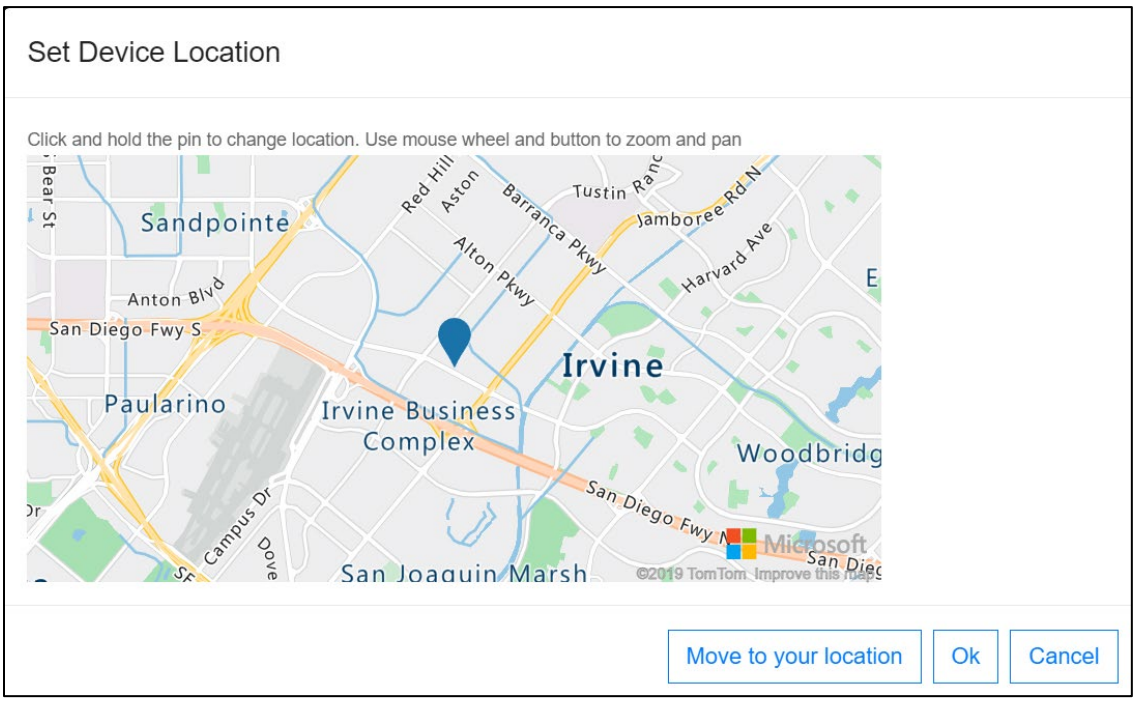

Figure 7: Set Device Location pop-up window

Step 4: Navigate to the **Map View** from the **Devices** main menu tab and the device will appear at the updated location.

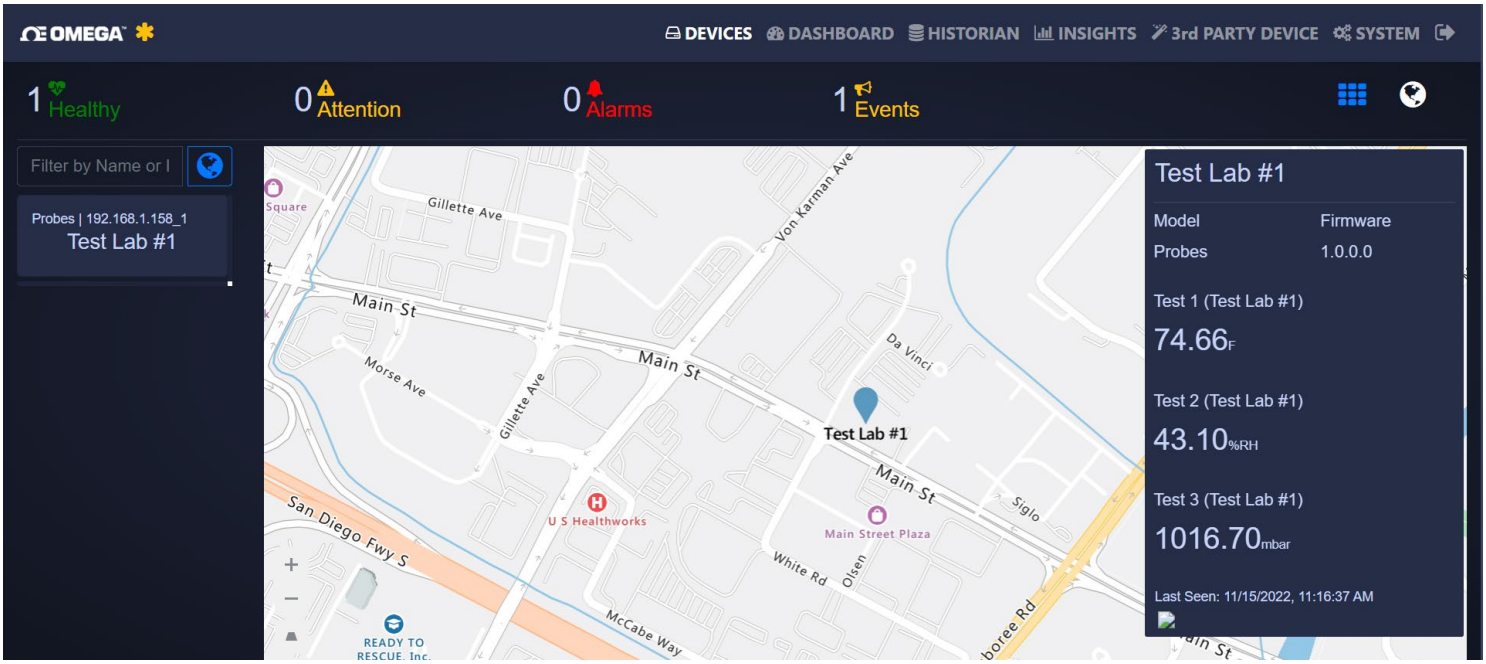

Figure 8: OEG Map View

5 Dashboard

Note: Dashboard features are only available on **OEG Pro**, **OEG Business**, and **OEG Business Pro**.

5.1 Creating a Monitoring Page

OEG offers a fully customizable Dashboard to monitor live device data.

Figure 9: OEG Dashboard interface

Click the + icon to create a new dashboard. Once users have named their dashboard, they can begin to add widget displays that will display their transmitted data as a meter, a graph, or as text. A device must be assigned to the widget so that it will begin to display readings from that device. Any combination of widgets and devices can be added and customized to create unique dashboards.

Step 1: Create and name the dashboard

Step 2: Choose the preferred widget to display device data.

Step 3: Assign a device to the widget.

6 Historian

The Historian creates a report of past readings within a range of time and presents them as a graph. Through the Historian tab, OEG allows users to export their chart data as a .csv file. To view past readings, start by clicking **Select Data Points**.

Figure 10: OEG Historian interface

Note: The Historian is only available on **OEG Pro**, **OEG Business**, and **OEG Business Pro**.

6.1 Select Data Points

The Select Data Points tab allows users to specify what device(s) will be displayed in the historian. The data will then be displayed in a graph.

6.2 Graph Types

OEG currently offers three standard graph views when displaying data. Of the three, only the graph style can predict future values. To utilize the **Predict Future Value** feature, enter the date and time of the value that will be predicted and click the **Predict Future Values** button to display the data.

7 Insights

The Insights interface provides analytics on the health and activity of the device ecosystem. Analytics include operation activities, measurement alarms, communication errors, battery history, and signal history.

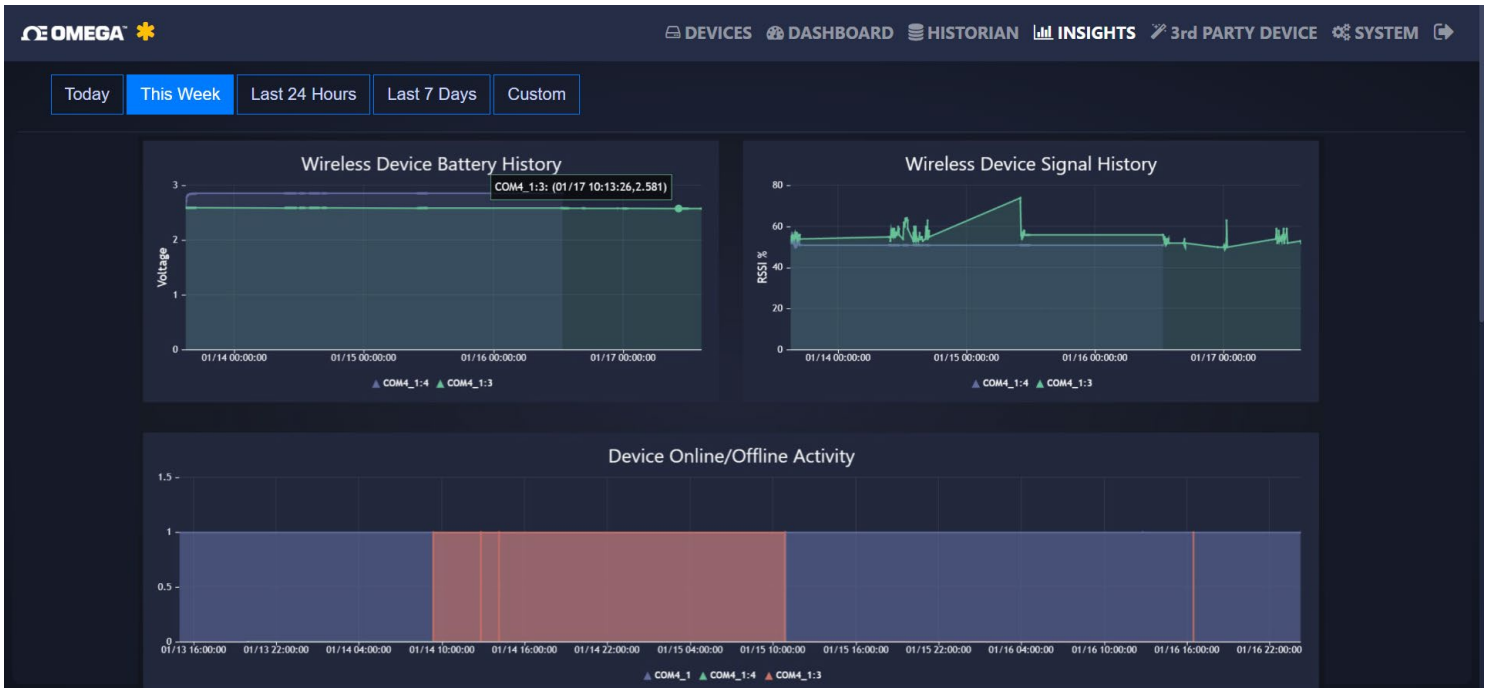

Figure 11: OEG Insights interface

Note: The Insights interface is available on **all versions** of OEG 2.4.

8 Third-Party Devices

Omega Enterprise Gateway allows for 3rd Party Device integration through MODBUS or ASCII. To add a 3rd party device, follow these steps:

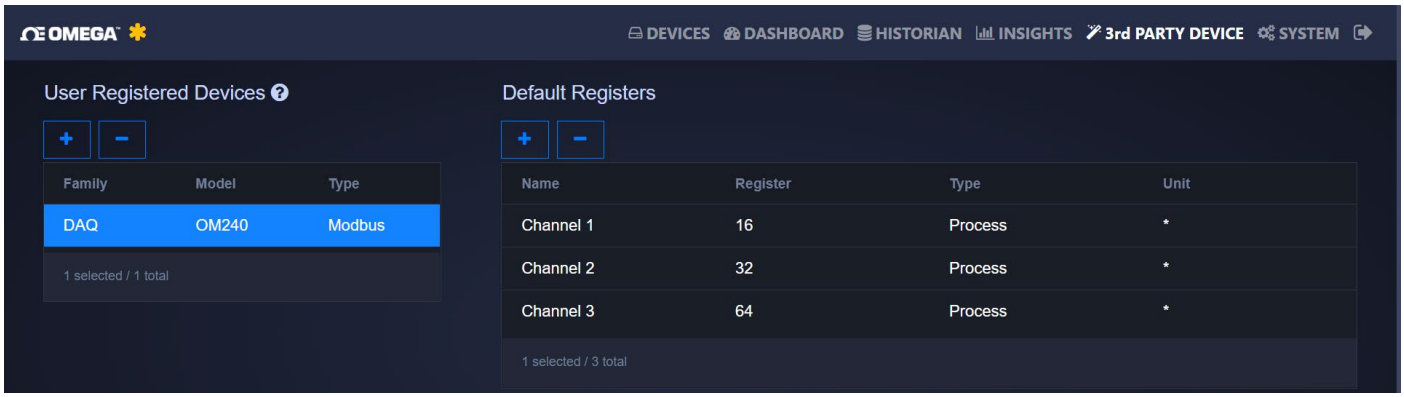

Figure 12: Third-Party Device interface

Step 1: Click the + icon under **User Registered Devices** and register the device.

Step 2: Click the + icon under **Default Registers** to create and define registers for the device.

To delete a 3rd party device or register from OEG, click the device or register to highlight it, and click the − icon under **User Registered Devices** to delete a device or click the − icon under Default Registers to delete a register.

Note: 3rd Party Device integration is only available on **OEG Business Pro**.

9 System Settings

The System Settings for OEG allow users to customize their profile, the units displayed, other users who can access and view the Dashboard, data update rate, license status, and firmware management.

9.1 Profile

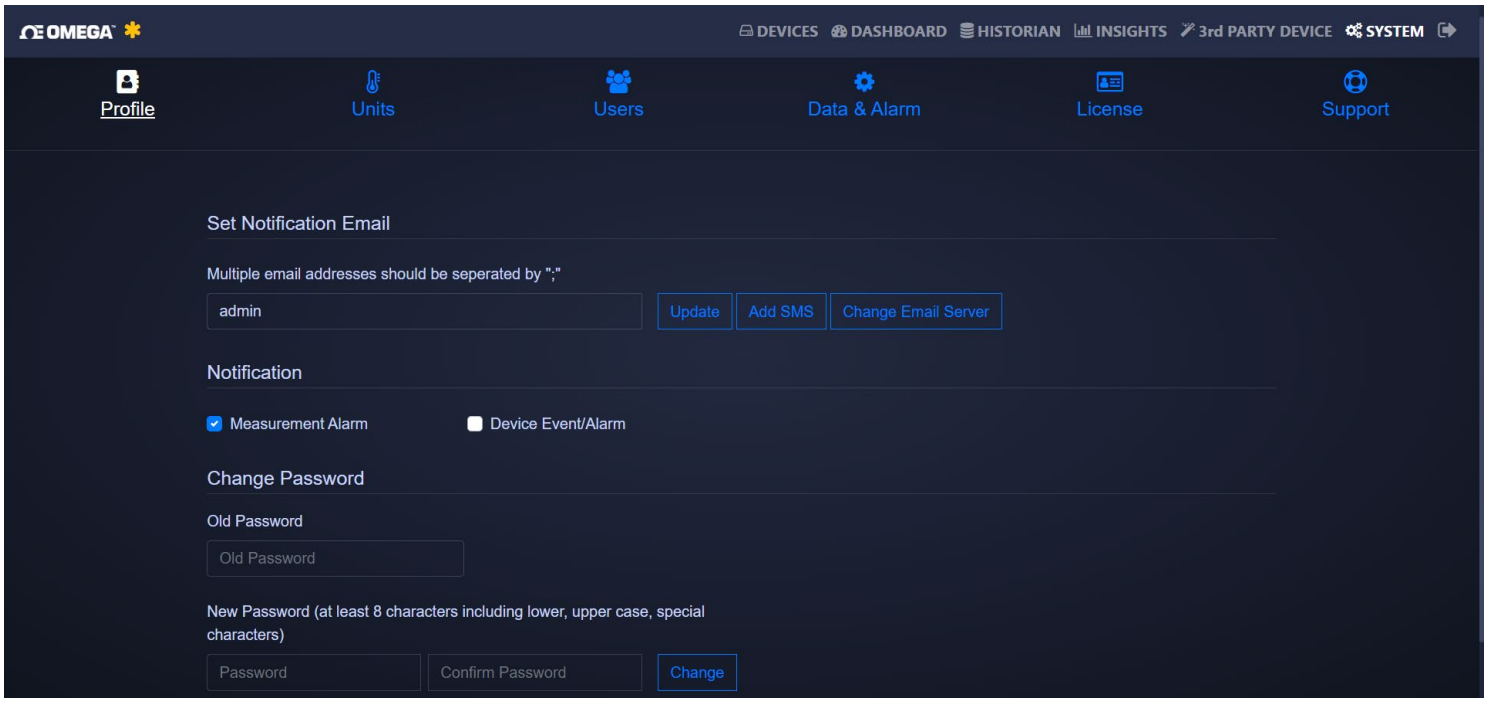

Figure 13: OEG System Profile settings

From the Profile tab, users can create a list of email addresses that will receive notifications when alarms or events are triggered and change their password.

9.1.1 Change Email Server

Users can change the default email server to their preferred service by clicking **Change Email Server**.

Important: Administrator access is required. OEG must be run as an administrator when using an alternative email server. It is recommended that users seek troubleshooting solutions for email notifications from the alternative email service provider being used.

Figure 14: Change Email Server configuration

9.2 Units

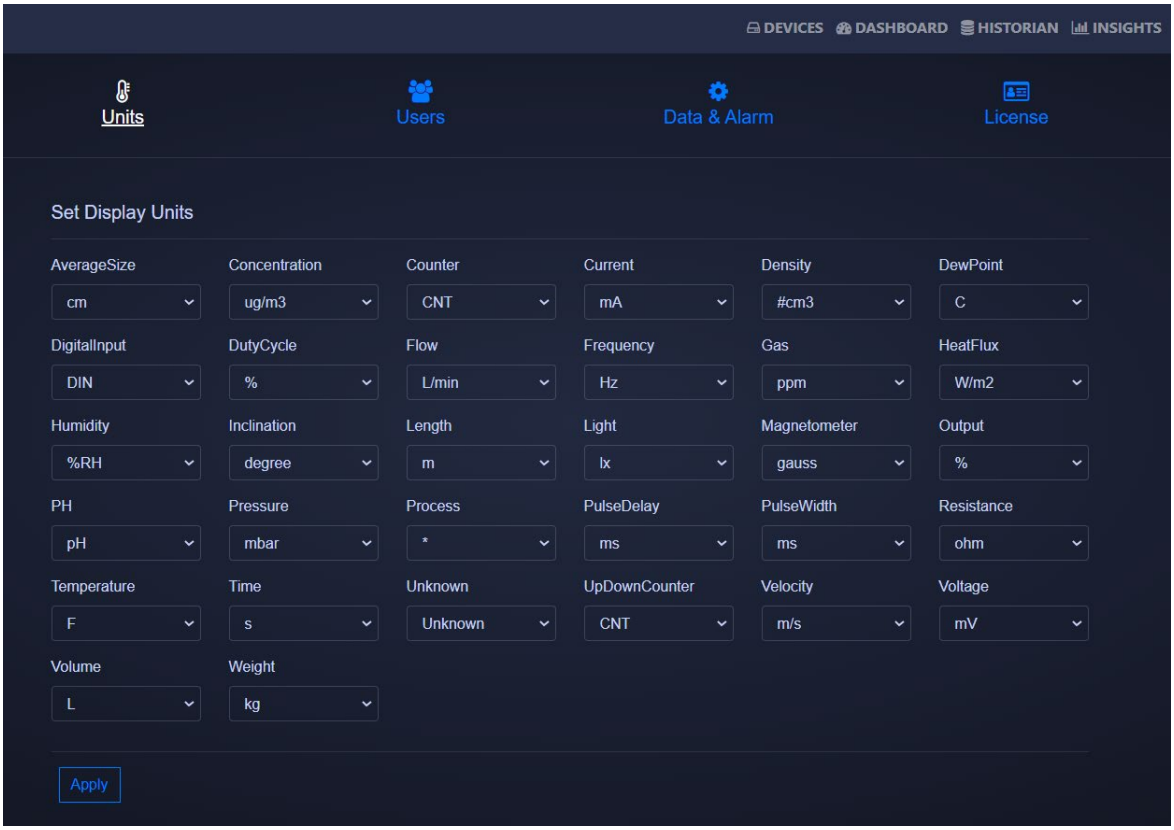

Figure 15: OEG System Units settings

The Units tab allows users to change the units of measurement that are displayed on OEG.

Note: Changing the units of measurement only affects the readings displayed on Omega Enterprise Gateway. Smart Sensors interpret data in SI.

9.3 Users

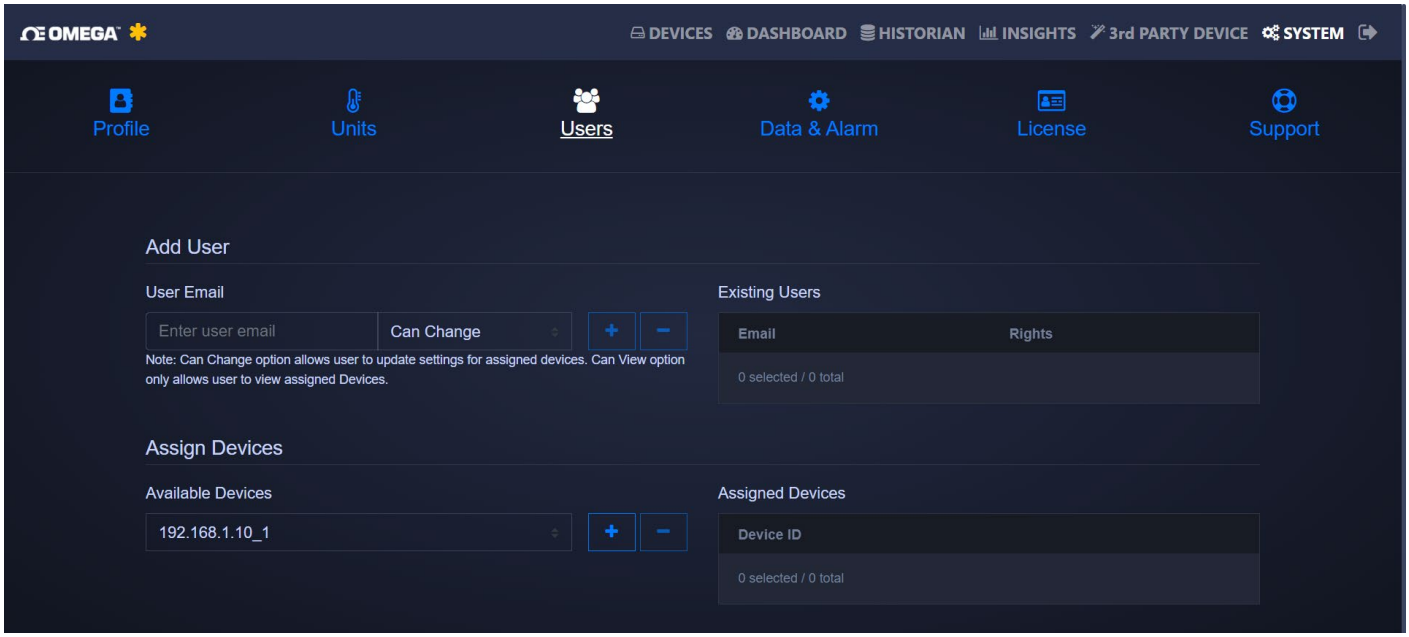

Figure 16: OEG System Users settings

User access to the OEG account can be managed by typing the email address of the users who will have access to either change, or view, the readings of the devices connected to the account. Users who are added here will only have access to devices that have been added in the **Assigned Devices** section. Additionally, they can restrict access to **View Only** or **Can Change**.

Note: Multi-Level Access is only available on **OEG Business Pro**. Additional user access is only possible when the admin OEG account is still actively running. If the admin OEG account is not actively running, additional users may not have access to the account.

9.3.1 Add a User

To add a user, type the email address in the **User Email** textbox, then determine whether the user should have access to change or only view the assigned devices. Click the + icon to send an invitation link to the provided email address. The email will come with a URL associated with the OEG account along with a one-time, temporary password. Once the new user has logged in for the first time, they will be prompted to enter a new password and will be able to access the same data as the admin of the OEG account.

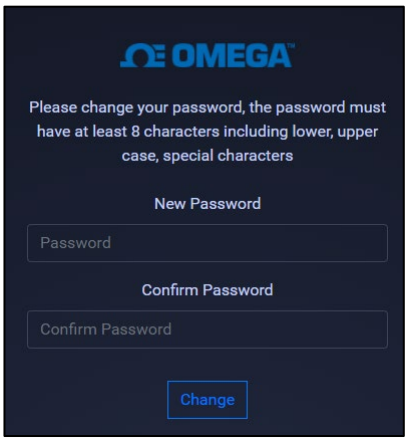

Figure 17: OEG additional user new

9.3.2 Remove a User

To remove a user, simply highlight the email address of the user and click the − icon.

9.4 Data & Alarm

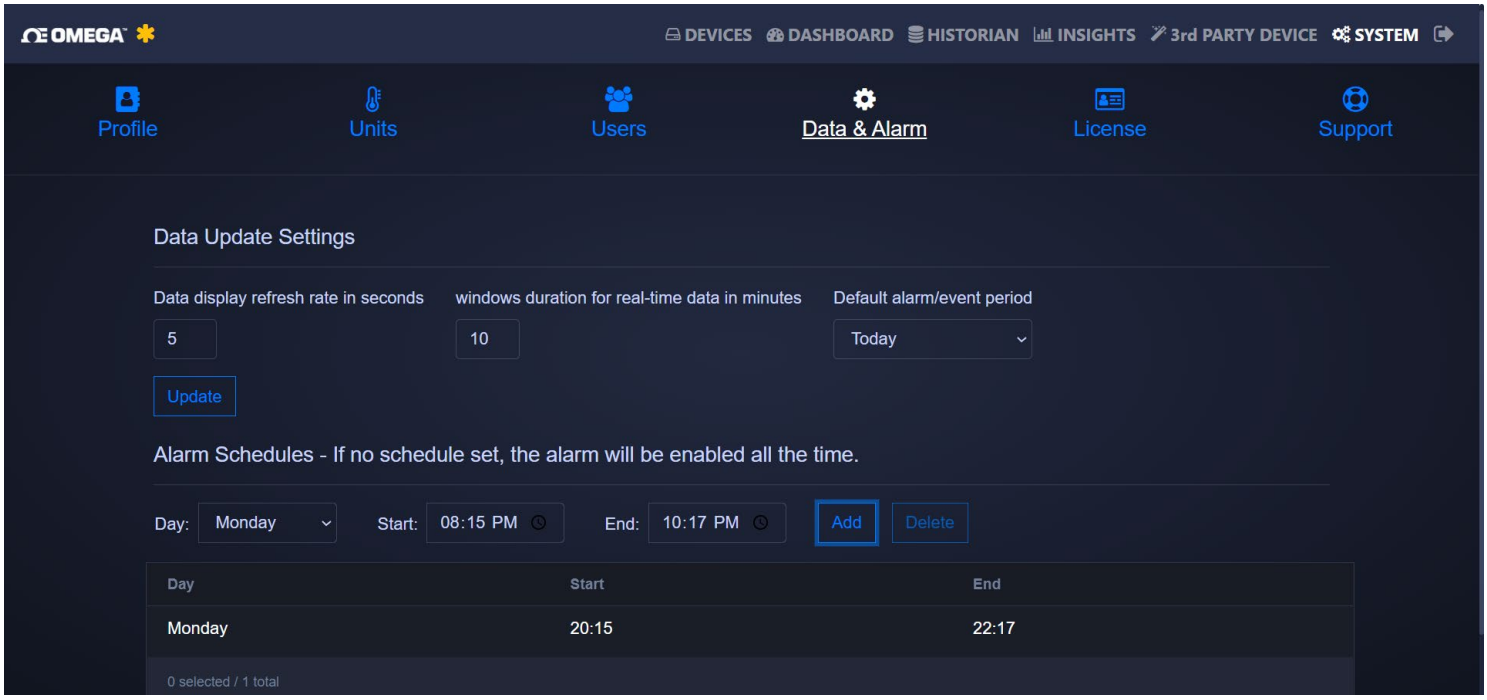

Figure 18: OEG System Data settings

The Data Tab allows users to configure the frequency at which data is updated within the OEG interface.

9.5 License

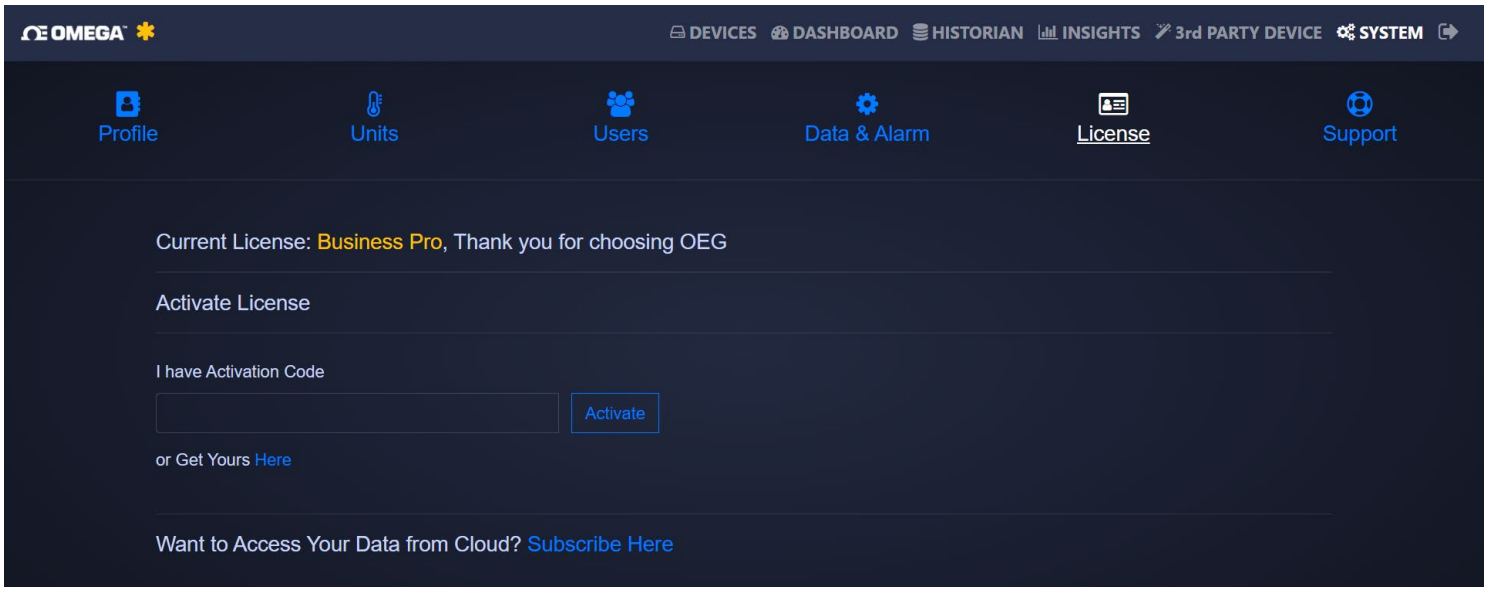

Figure 19: OEG System License settings

The License tab displays information regarding the user's current OEG license. From this section, an activation code can be entered to activate a license. Users may also subscribe to Layer N Cloud from this section to have access to their data anywhere.

10 Remote Access

Note: Remote Access is available on **all versions** of OEG 2.4.

OEG allows users to access their data from any device connected to the same local network with web browser access. To access data remotely, click on the automatically generated URL at the bottom of the OEG interface. The URL will begin with HTTP:// and will be based on the local network settings. By navigating to the URL on a separate device that is connected to the same local network, data can be access remotely.

Note: Only devices with web browsers on the same network as the one hosting the OEG data will be able to access the data remotely. OEG data cannot be accessed if the web browser is on a different network.

Alternatively, parameters for **Remote Access** can be accessed by closing the OEG software application, right-clicking the desktop shortcut for OEG, and clicking **Run as Administrator**. Two parameters can be set for web server access at the bottom of the screen:

1. The web server port number. The default HTTP port for OMEGA Enterprise Gateway is 8080. Users can change it to any port.

2. The option to turn on/off the HTTPS connection.

Note: A server has multiple usages, therefore the default HTTP port 80 might be occupied.

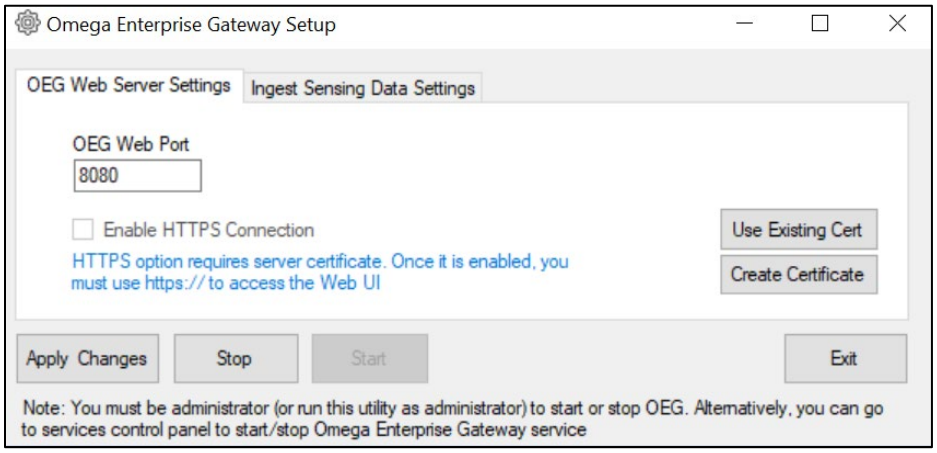

Figure 20: OEG Remote Access setup

If users want to use a secure connection for web browsing or calling APIs, they can turn on the HTTPS connection by selecting the checkbox **Enable HTTPS Connection**. To secure the connection, a certificate must be provided. The default self-signed certificate can be used by clicking **Create Certificate** or users can select an existing certificate. When users select an existing certificate, ensure that the certificate can be used for remote machine authentication. Users who will create a certificate on their own must be aware that they will need to use the correct IP address to access the Gateway web page.

Note: If the utility detects a user-created certificate on a local machine, the **Create Certificate** button will be grayed out to prevent duplicated creation.

11 Connecting to Layer N Cloud

Note: The following section will outline how to connect Omega Enterprise Gateway to Layer N Cloud. An active, registered Layer N Cloud account is necessary to connect the two accounts. Although OEG does not require Internet connection to operate, if the account is added to the Layer N Cloud as a gateway, an Internet connection will be required.

To connect an OEG account to a Layer N Cloud account, follow these steps:

Step 1: Click the icon at the top right of the OEG interface.

Step 2: Take note of the unique **ID** and the **Secure Code for Cloud Registration** that appears in the pop-up.

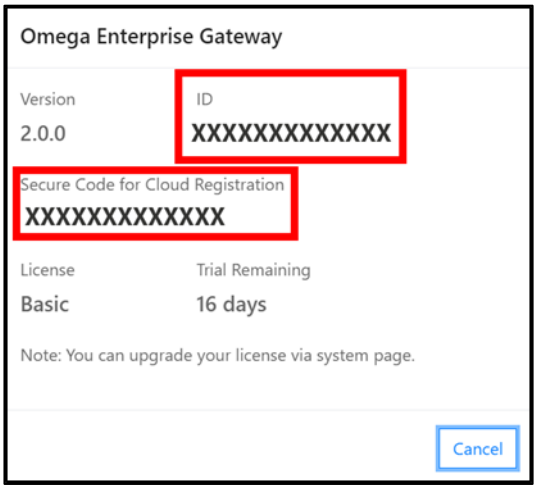

Figure 21: OEG Unique ID and Secure Code for Cloud Registration

Step 3: Open a web browser and navigate to **cloud.omega.com**.

Step 4: Sign in to the Layer N Cloud account.

Note: Users who don't have an account can create one by clicking **Sign Up**.

Step 5: After signing in, click **Add Gateway**.

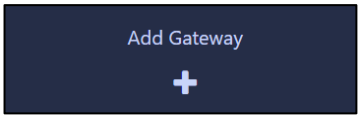

Figure 22: Layer N Cloud Add Gateway button

Step 6: Enter the **ID** and **Secure Code for Cloud Registration** that from the OEG account (Gateway) and assign a name to the new Gateway.

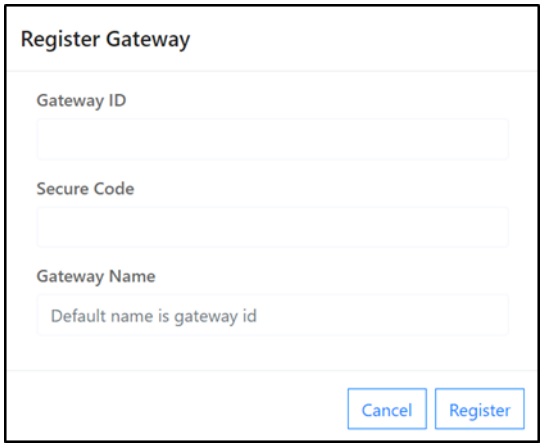

Figure 23: Layer N Cloud Gateway Registration

Important: Once users have registered their OEG ID to their Layer N Cloud account, they must power cycle the OEG software. To power cycle the OEG Software, navigate to the Windows OS Services application on the computer, locate Omega Enterprise Gateway in the list of items, right-click Omega Enterprise Gateway, and click Restart.

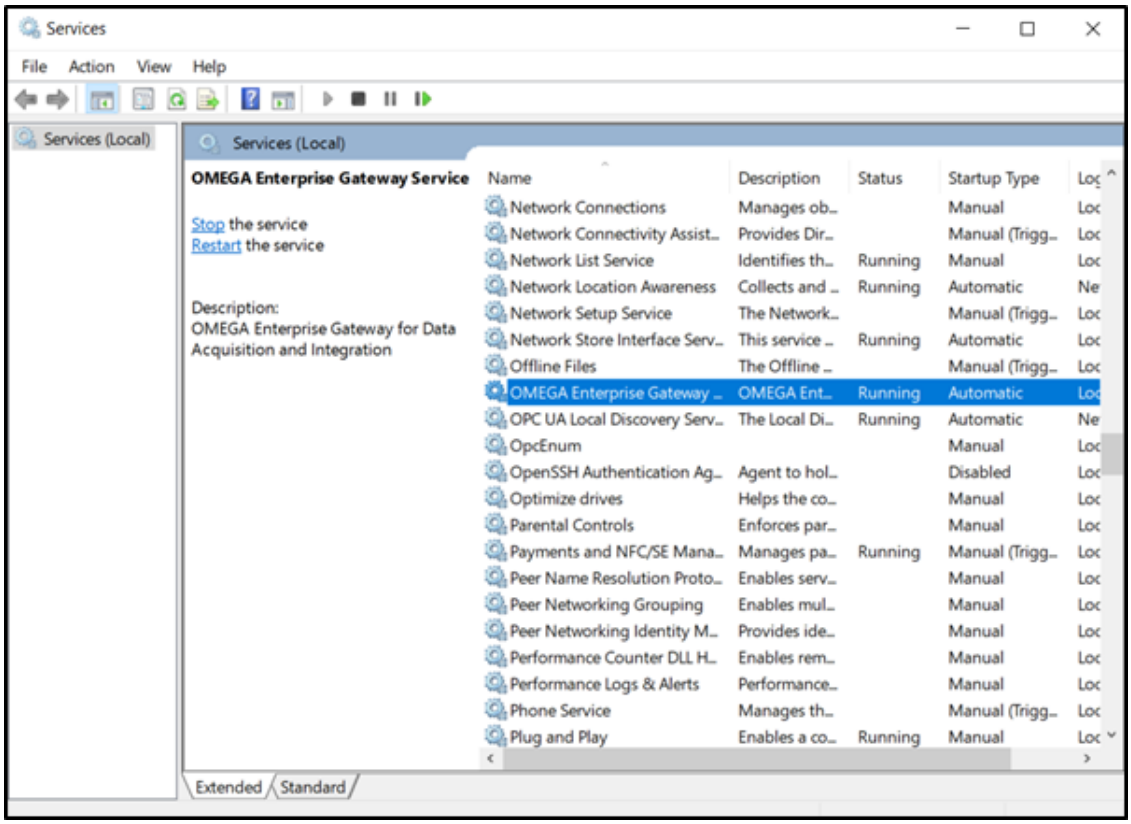

Figure 24: Windows OS Services menu

Once these steps are complete, the user will have successfully connected their Omega Enterprise Gateway to Layer N Cloud.

11.1 Limitations

When an OEG account is added to the Layer N Cloud, some devices connected to OEG may not be displayed properly on the Layer N Cloud user interface. Omega Engineering is constantly working on bringing its extensive catalogue of devices to the Layer N Cloud.

12 Adding a Layer N Gateway to OEG (Enterprise Mode)

Omega Enterprise Gateway 2.4 software (OEG) supports Layer N GW-001 models in local-area network environments with the addition of the Enterprise Mode feature in Layer N GW-001 models with firmware version 1.10 or higher. The Enterprise Mode feature provides a local-area solution to sensing and data logging by bringing the advanced sensing suite of Layer N Smart devices to the following paid tiers of OEG 2.4:

- Omega Enterprise Gateway Pro
- Omega Enterprise Gateway Business
- Omega Enterprise Gateway Business Pro

12.1 Configuring Sensing Devices after Pairing with OEG

If a sensing device paired wirelessly or wired directly to the Layer N Gateway has been configured or modified after the Layer N Gateway has been added to OEG, the user must reboot the Layer N Gateway and restart the OEG software to sync with the configuration made to the connected device.

12.2 What is Needed?

The following materials are required to download OEG, upgrade the GW-001 firmware, and to add the Gateway to OEG.

- **A Windows 7, 8, 9, 10, or 11 OS PC** to purchase, download, and run OEG. The PC will also be used check for the latest GW-001 firmware and will provide access to the internal Gateway UI to upgrade the firmware and enable Enterprise Mode.

- **A DHCP-enabled router with Internet access** and an open RJ45 Ethernet port to upgrade the firmware of the GW-001 for first time setup; also needed if the GW-001 firmware version is outdated.

- **One RJ45 Ethernet cable** to connect the Gateway to the DHCP-enabled router and to connect to the local area network PC or router after the Enterprise Mode process is complete.

- **An assembled GW-001 device**

Important: If the OEG License being used has not been activated, an internet connection will be needed for a one-time license activation before proceeding. Adding a Layer N Gateway as a Device to OEG is only available on non-trial licenses of OEG.

12.3 Download a Qualifying OEG license Tier

A qualifying OEG 2.4 license tier can be purchased and downloaded from the OMEGA Engineering website at the following URL:

https://www.omega.com/en-us/oeg

Note: Omega Link compatibility is only available for **OEG Pro**, **OEG Business**, and **OEG Business Pro** license tiers.

Once a qualifying license tier has been purchased and downloaded on a Windows PC, users may proceed by installing the software on the PC that will run OEG 2.4. Exit the software once the download process is complete.

12.4 Navigate to the GW-001 User Interface

A successful connection between a GW-001 and OEG requires the GW-001 to run on **firmware version 1.10 or higher**. Users can check for the latest firmware by navigating to the **GW-001 User Interface (UI)** on a PC with a web browser.

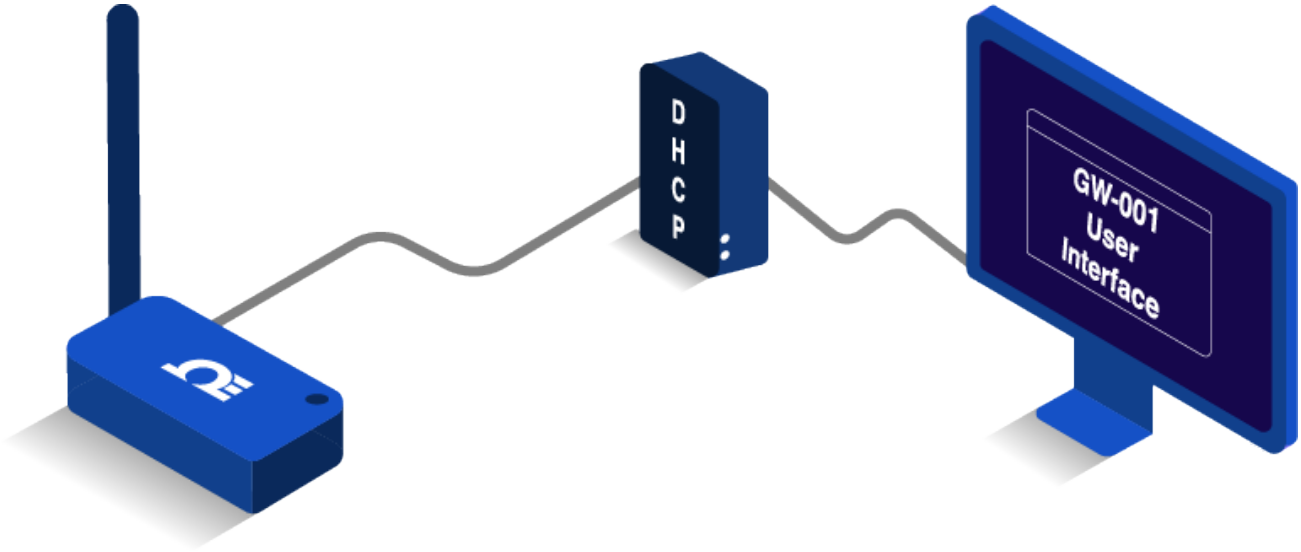

Figure 25: GW-001 First-Time UI access setup

To access the GW-001 UI for the first time, use an **RJ45 Ethernet Cable** to plug the GW-001 device to a **DHCP-enabled router with Internet access** and follow the steps below:

Step 1: Using a Windows PC on the same network as the connected GW-001, type the following URL:

http://omegaiotgatewayXXXX.local

(**XXXX** should be replaced with the last 4 digits of the GW-001 **MAC address** printed on the label located on the underside of the GW-001 device).

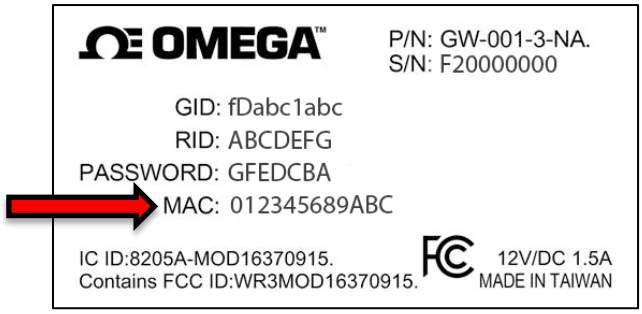

Figure 26: GW-001 Underside Label with Mac Address

Step 2: From the GW-001 UI login screen, enter the password for the GW-001 (if this is a first-time login, enter the password located on the underside label of the GW-001 device.) When entered successfully, the user will be granted access to the GW-001 UI.

Important: If the user is unable to access the GW-001 UI using the DHCP-enabled router method, the Bonjour service may need to be installed on the PC. The service can be downloaded from the following URL:

http://omegaupdates.azurewebsites.net/software/bonjour

12.5 Download and Install the Latest GW-001 Firmware

From the main page of the GW-001 UI, click the **Settings** tab then click the **System** tab.

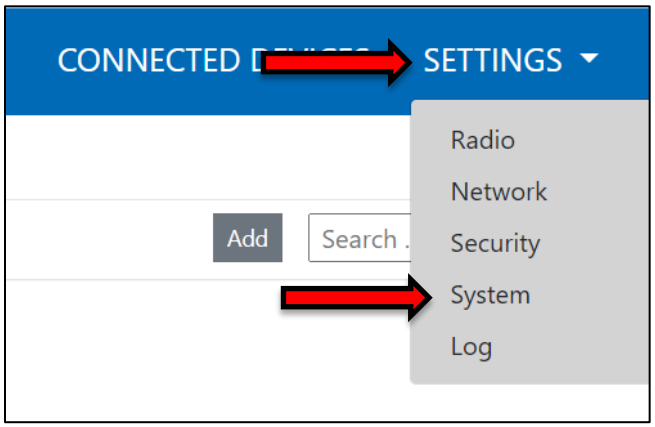

Figure 27: GW-001 UI System Settings Tab

When presented with the System Settings menu, users may click the Check Online button to check for the latest GW-001 firmware version available.

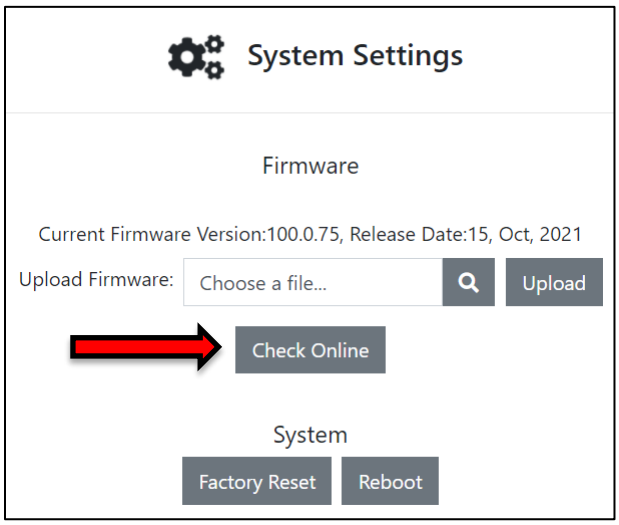

Figure 28: GW-001 UI System Settings menu

The user may then download the latest version and upload it to the GW-001 device by clicking the **Upload Firmware** search bar and selecting the firmware file from the **File Explorer**. A **red** LED will appear on the GW-001 indicating the upgrade is in progress.

Once the update process is complete, the LED on the GW-001 will blink **green**. The GW-001 will reboot and the user will need to log back into the GW-001 UI. The new firmware version will appear on the main page of the GW-001 UI once logged back in.

12.6 Enable Enterprise Mode

When the GW-001 has been upgraded to the latest firmware version, Enterprise Mode will be made available in the **Security Settings**. Click the **Settings** tab in the upper right corner of the screen and clicking **Security** from the dropdown.

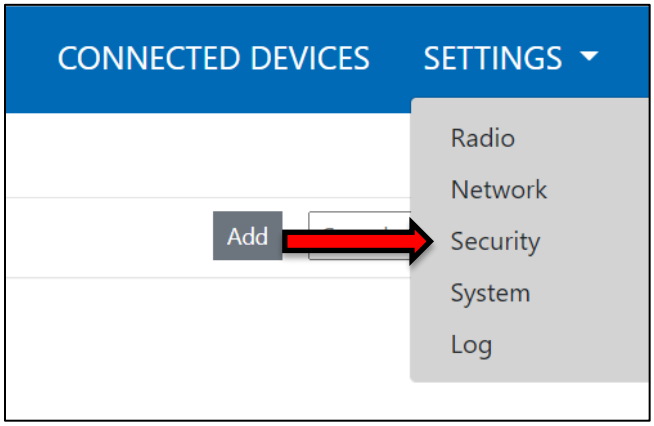

Figure 29: GW-001 UI Security Settings Tab

From the **Security Settings** menu, users will be able to disable the cloud registration requirement thus enabling Enterprise Mode. Click the **Turn Off Cloud Registration** checkbox to disable the feature and to set the GW-001 to Enterprise Mode. Click the **Update** button to save the change. The GW-001 LED will repeatedly blink **amber/orange** to indicate the device is in **Enterprise Mode**.

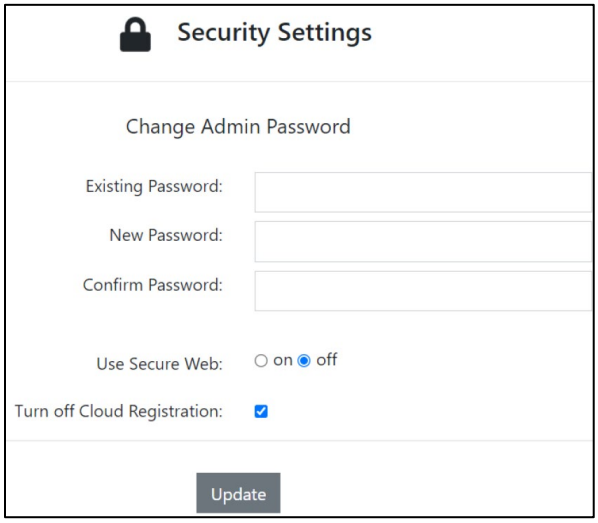

Figure 30: GW-001 UI Security Settings Menu

12.7 Add the GW-001 to OEG as a Device

If the GW-001 will be moved and connected to a local area network, it should be moved at this point and connected directly to a DHCP-enabled, local-area network router or directly to the local-area network Windows PC that has OEG 2.4 installed. Both methods require a connection via RJ45 Ethernet cable.

Local-Area Network DHCP Router Setup

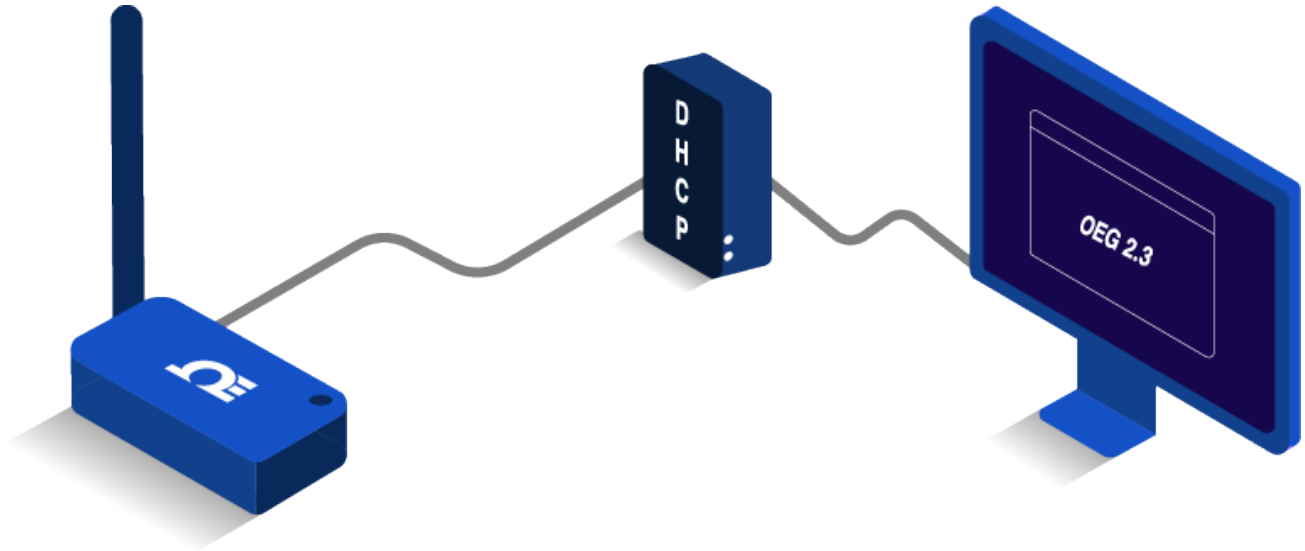

Figure 31: Local-Area-Network DHCP-Router Setup Overview

Local-Area Network Direct-to-PC Setup

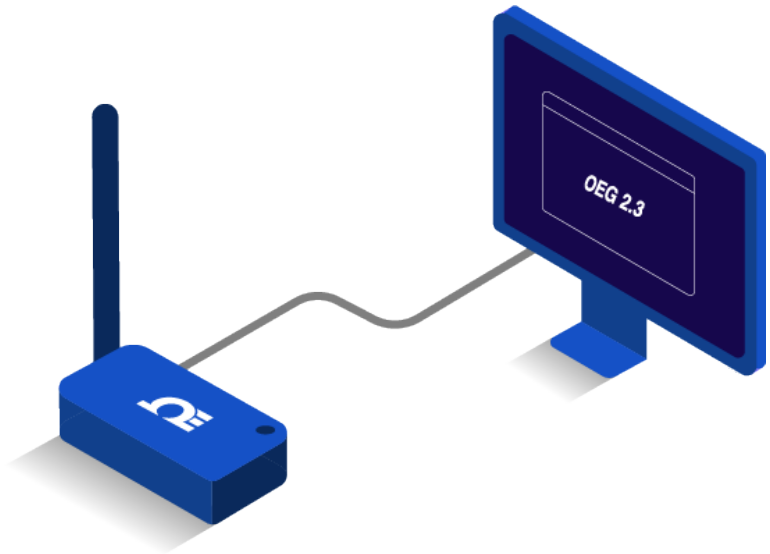

Figure 32: Local-Area Network Direct-to-PC Setup Overview

Once the GW-001 has been connected to a local-area network router or local-area network PC, launch OEG 2.4 and log in to the OEG account. Follow the steps below to add a GW-001 to OEG as a device:

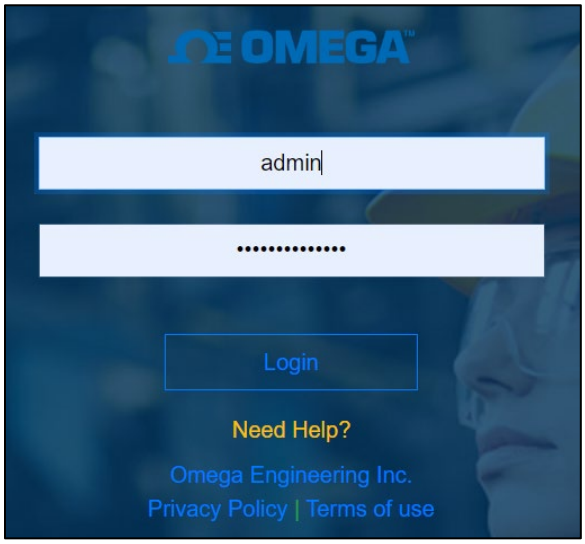

Figure 33: OEG Login Page

Step 1: After logging in to the OEG account, from the homepage, click the + icon or the **Add Devices** button. Then select **GW-001-Series Gateway** from the **Product Family** dropdown and **GW-XXX-X** from the **Product Model** dropdown.

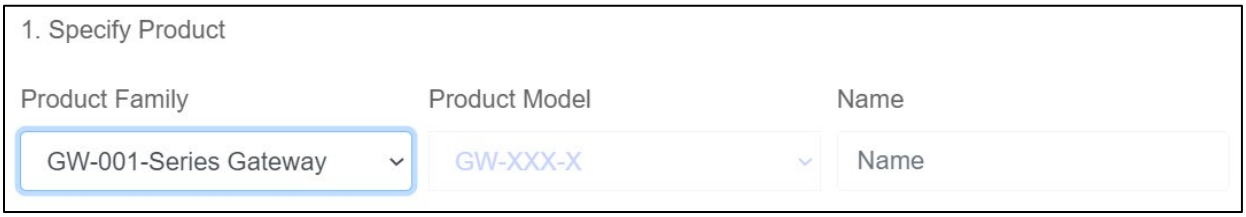

Figure 34: OEG interface Add Device menu – Layer N GW-XXX-X

Step 2: Input the **IP Address** of the connected GW-001 ***as it appears in the local-area network***.

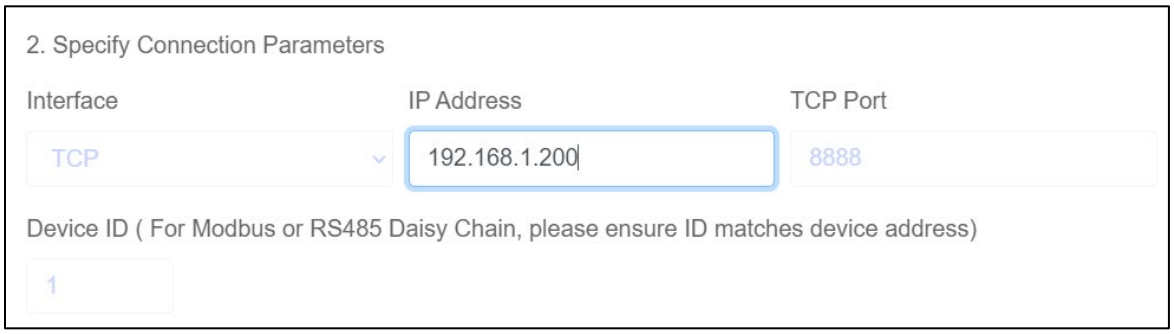

Figure 35: OEG interface Add Device menu – Connection Parameters

Important: If the GW-001 unit has been disconnected and moved to a separate DHCP-enabled local-area network router or PC, the user must log back into the gateway internal UI to identify the **new IP Address** that the device has been assigned under new the local-area network.

Step 3: Click **Advanced** to reveal the text field for **Username** and **Password**. The Username will automatically populate to "admin". Input the password required to access the gateway internal UI in the Password textbox.

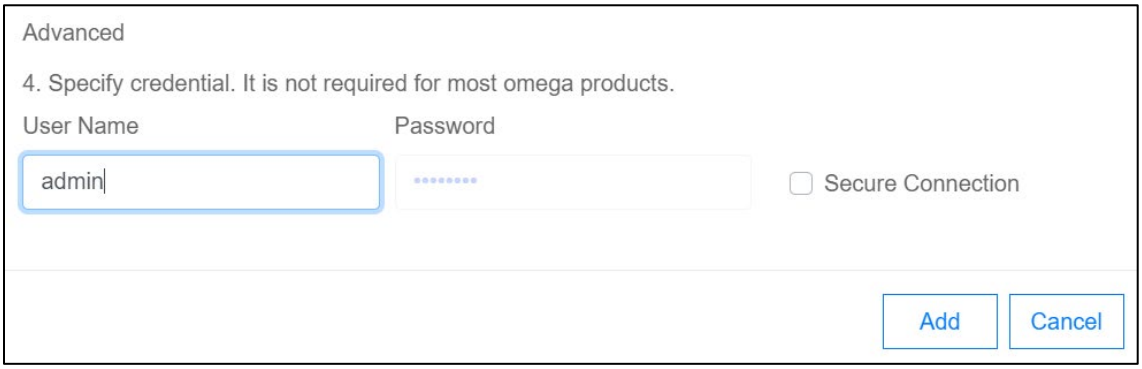

Figure 36: OEG Interface Add Device menu – Gateway Username and Password input

Step 4: Click **Add** to finalize your configuration.

All devices connected to the GW-001 will appear, including those that are offline. The readings from offline units will display as NaN.

Note: The maximum reading interval is 120 seconds for Layer N Gateway. After switching to **Enterprise Mode** from **Cloud Mode**, the Layer N Gateway device should be manually powered off and on again. Omega Enterprise Gateway should also be restarted from the Windows OS Services application. In the future, if users will be using the Layer N Cloud service, they must navigate to the Gateway web UI again to uncheck the **Turn off Cloud Registration** box.

13 Adding an iServer 2 to Omega Enterprise Gateway (OEG)

iServer 2 devices can be added to Omega Enterprise Gateway 2.4 (OEG) in a non-internet environment by adding the iServer 2 to OEG as a device. There are two methods to connect the iServer 2 to OEG:

- The first method requires the iServer 2 to be set to the default DHCP network setting and requires access to a DHCP-enabled router with an open port and an RJ45 Ethernet cable.

- The second method requires Administrator access to the Windows OS PC running OEG and requires the iServer 2 to be set to the Static IP network setting and the iServer 2 unit to be plugged in directly to the Windows PC.

13.1 Method 1: DHCP Router Method

To add an iServer 2 to OEG using the DHCP router method, begin by ensuring the iServer 2 is set to the default DHCP network settings and follow the steps below.

Step 1: Connect the iServer 2 unit to a DHCP-enabled router using an RJ45 Ethernet cable.

Step 2: Ensure the Windows PC that will run OEG is on the same network as the connected iServer 2.

Step 3: Launch and log in to your OEG account.

Step 4: Click the + icon or **Add Devices**. Then select **iServer 2** from the **Product Family** dropdown and click **TC** or **Probe** from the **Product Model** dropdown, depending on the model of iServer 2 being connected.

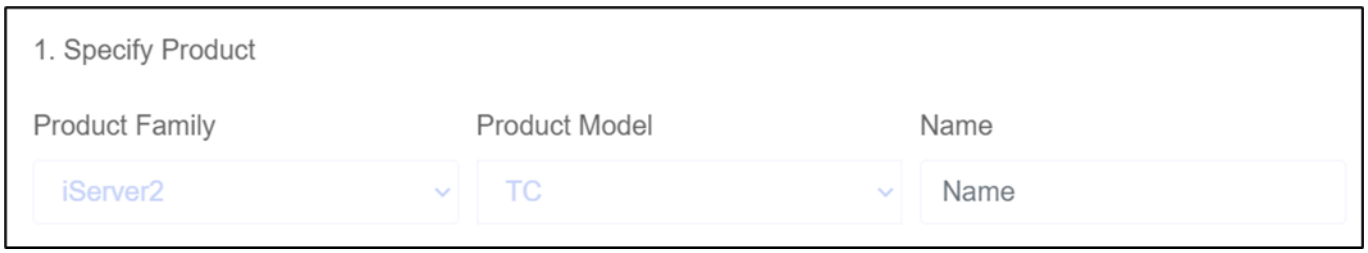

Figure 37: OEG Add Devices menu – iServer 2 Model

Step 5: Input the IP Address of the connected iServer 2 **as it appears in your local-area network**.

Figure 38: OEG Add Devices menu – Connection Parameters

Important: If the DHCP-enabled iServer 2 unit has been disconnected and moved to a separate DHCP-enabled, local-area network router or PC, the user must identify the new IP Address that the unit has been assigned under the local-area network. For models with a display, the new IP Address will appear on the unit display. For models without a display, users can access the iServer 2 web UI to check the new IP Address.

Step 6: Click **Add** to finalize your configuration.

All sensing devices connected to the iServer 2 will appear on OEG after the pairing is successful. The readings from offline units will display NaN. For more information on how to navigate OEG, refer to the OEG Software User's Manual.

13.2 Method 2: Static IP (Direct to PC) Method

To add an iServer 2 to OEG using the Static IP (direct to PC) method, begin by ensuring the iServer 2 is set to the Static IP network settings and confirm the Static IP address is set to the preferred address. The Windows PC network settings will need to be configured to properly pair the iServer 2 and OEG. Follow the steps below:

Important: Administrator access to the Windows PC is required to configure the Network settings of the PC.

Step 1: Navigate to the iServer 2 web UI and assign a Static IP address to the iServer 2 unit. Then exit the web UI.

Step 2: Connect the iServer 2 unit directly to the Windows PC with OEG using an RJ45 Ethernet cable.

Step 3: Navigate to the **Windows Control Panel** and click **Network and Sharing Center**.

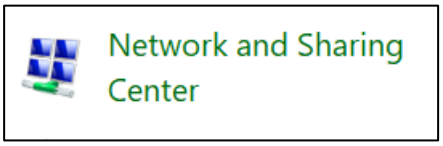

Figure 39: Windows Network and Sharing Center

Step 4: Click the **Unidentified Network Connection.**

Figure 40: Network and Sharing Center – Unidentified Network

Step 5: Click **Properties**.

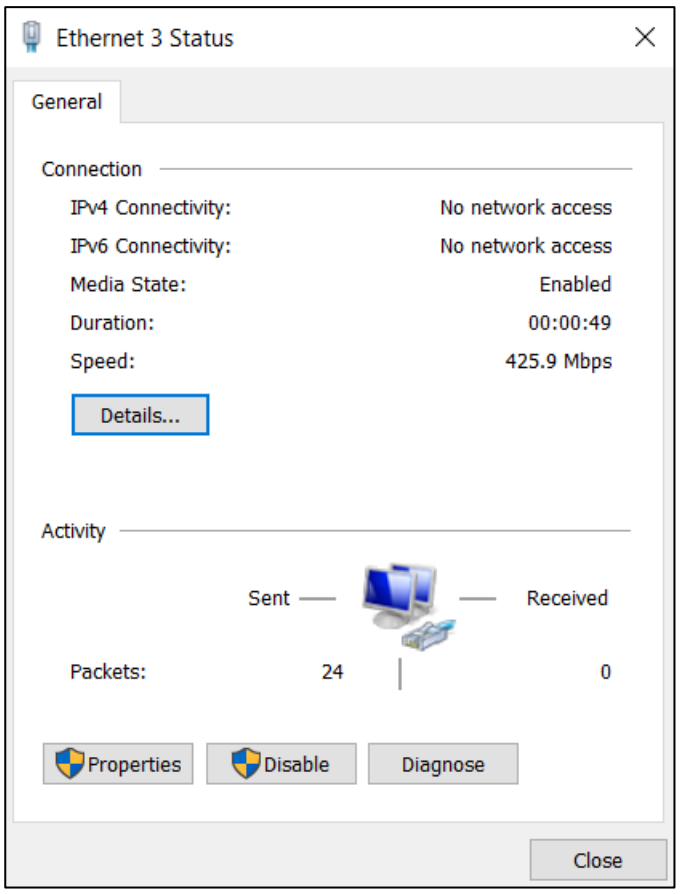

Figure 41: Unidentified Network Status

Step 6: Click **Internet Protocol Version 4 (TCP/IPv4)** to highlight the selection and then click **Properties.**

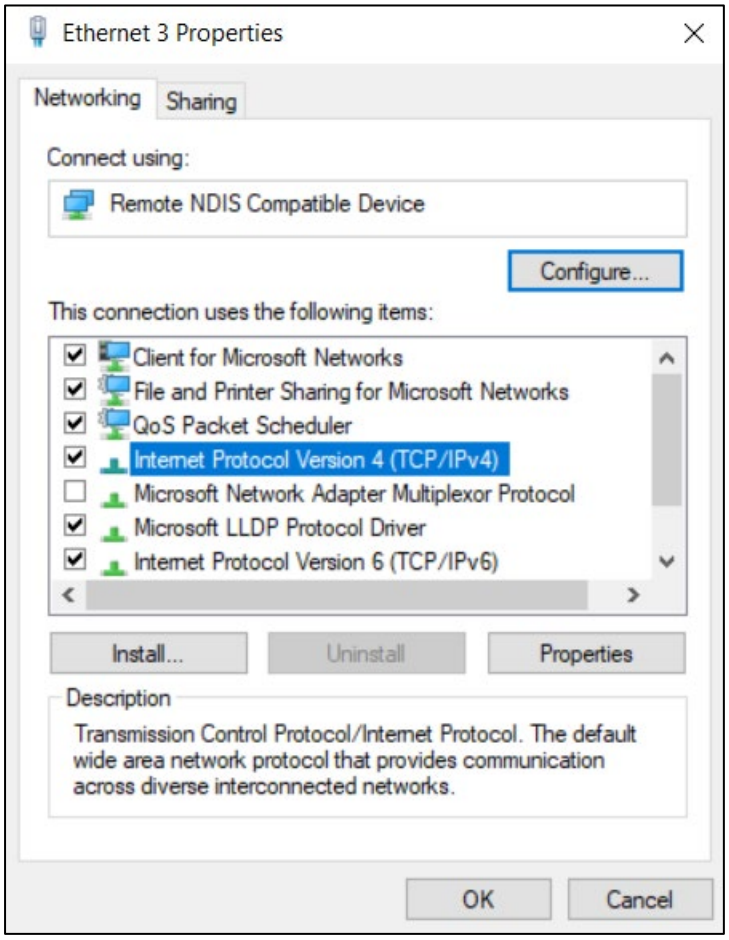

Figure 42: Unidentified Network Properties

Step 7: Click **Use the following IP address** and enter an IP address that uses the same network part (the first nine digits of the IP address) but with a unique host part (the last three digits of the IP address) as the static IP Address assigned to the iServer 2 in Step 1.

*For example, if the Static IP assigned to the iServer 2 is: **192.168.3.200,** then the IP address entered in the text box should be: **192.168.3.XXX** (the XXX should be any value that is **NOT** 200)*

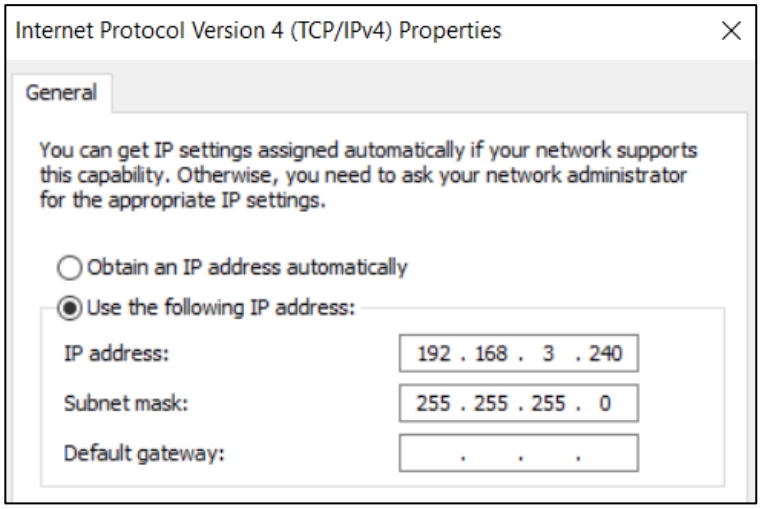

Figure 43: TCP/IPv4 and subnet mask properties for micro-USB 2.0 connection

Step 8: Click **OK** to finalize

Step 9: Launch and log in to your OEG account.

Step 10: Click the + icon or **Add Devices**. Then select **iServer 2** from the **Product Family** dropdown and click **TC** or **Probe** from the **Product Model** dropdown, depending on the model of iServer 2 being connected.

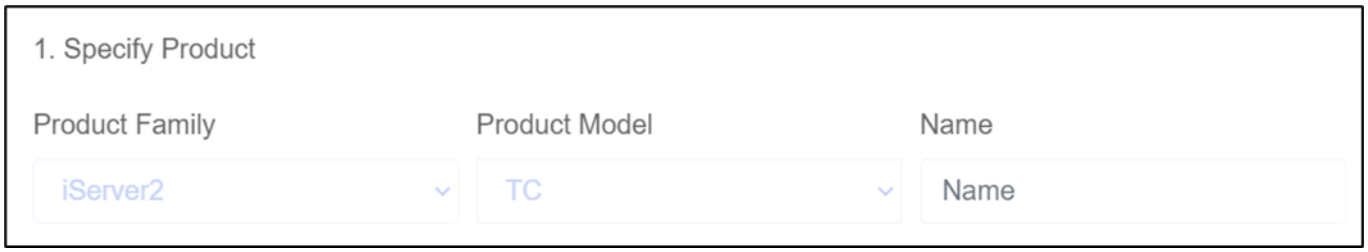

Figure 44: OEG Add Devices menu – iServer 2 Model

Step 11: Input the static IP Address of the connected iServer 2.

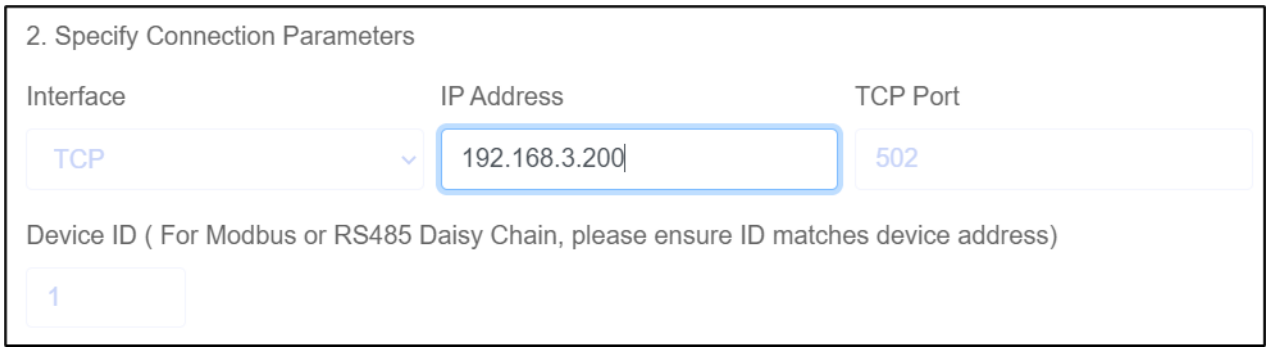

Figure 45: OEG Add Devices menu – Connection Parameters

Step 12: Click **Add** to finalize your configuration.

All sensing devices connected to the iServer 2 will appear on OEG after the pairing is successful. The readings from offline units will display NaN.

13.3 Configuring Sensing Devices after Pairing with OEG

If the device name, sensor name, meta data, or sensor units of the iServer 2 are modified or configured after the device has been paired to OEG, it may take up to 5 minutes for the changes to be reflected correctly in the OEG user interface. It is highly recommended that users reboot OEG or delete and re-add the iServer 2 device to OEG if the user has made changes to the iServer 2 sensor units after the device has been paired to OEG to ensure the collected sensor data remains consistent.

14 Integrating to Another Enterprise Software

Note: OPC UA/DA integration is only available on **OEG Business** and **OEG Business Pro**.

Omega Enterprise Gateway provides two ways to integrate sensing data into other enterprise applications.

1. OPC UA Server (requires license)
2. OPC DA Server (requires license)

14.1 OPC UA Server

Omega Enterprise Gateway comes with an embedded OPC UA server. This OPC UA server allows the OPC UA compliant enterprise application to connect to OEG and retrieve sensing data. Once OEG is running, the OPC UA server will also run and become exposed through the following URL:

opc.tcp://hostname:51210/OMEGA/OPCServer

Note: The hostname will either be the DNS name or IP Address of the machine that the Gateway is installed on.

For example, using OPC UA Foundation's sample client tool, users may browse supported protocols in the server configuration dialog and select one to connect to. Click **OK** and use an anonymous login.

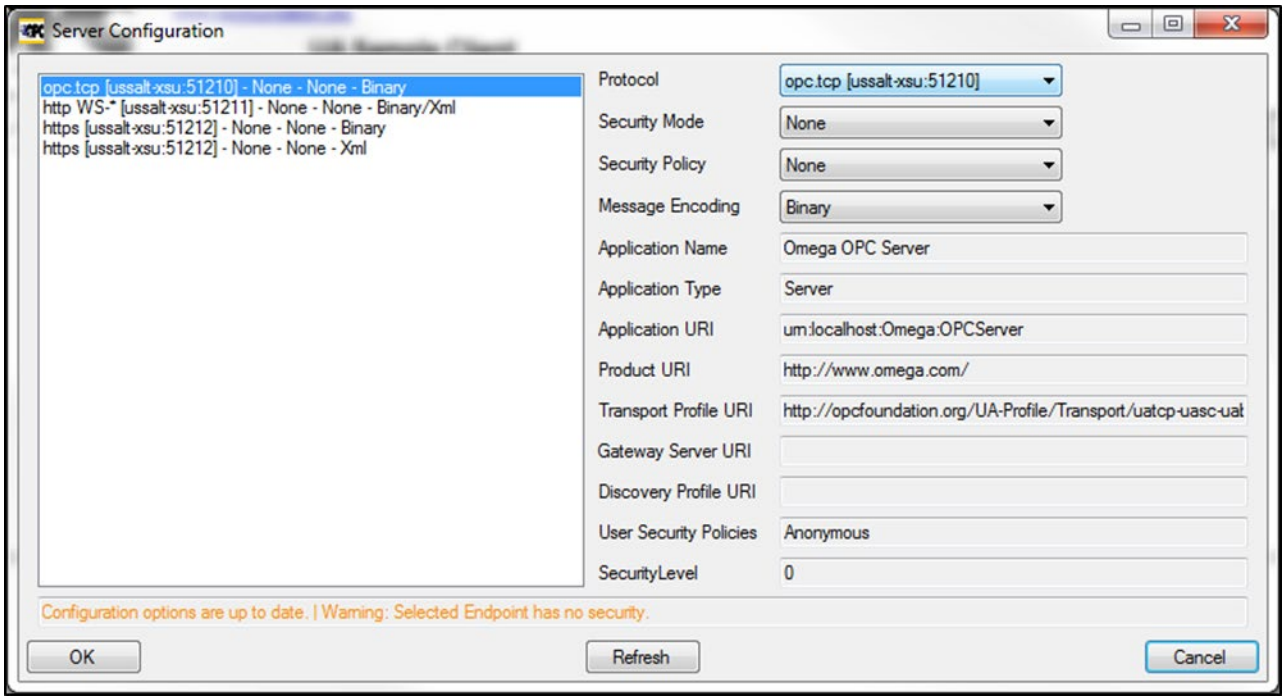

Figure 46: OPC UA Server Configuration

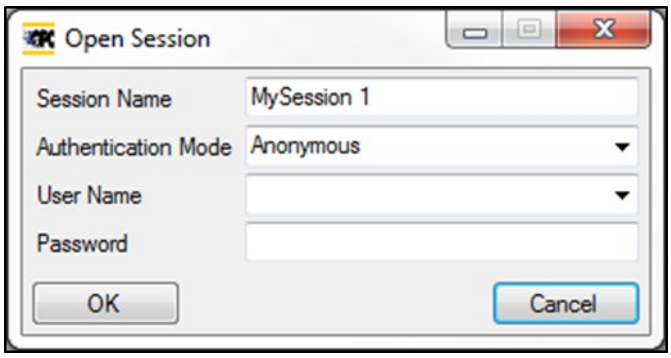

Figure 47: OPC UA Server Session Login

Once signed in, users can browse the measurements in the tree structure.

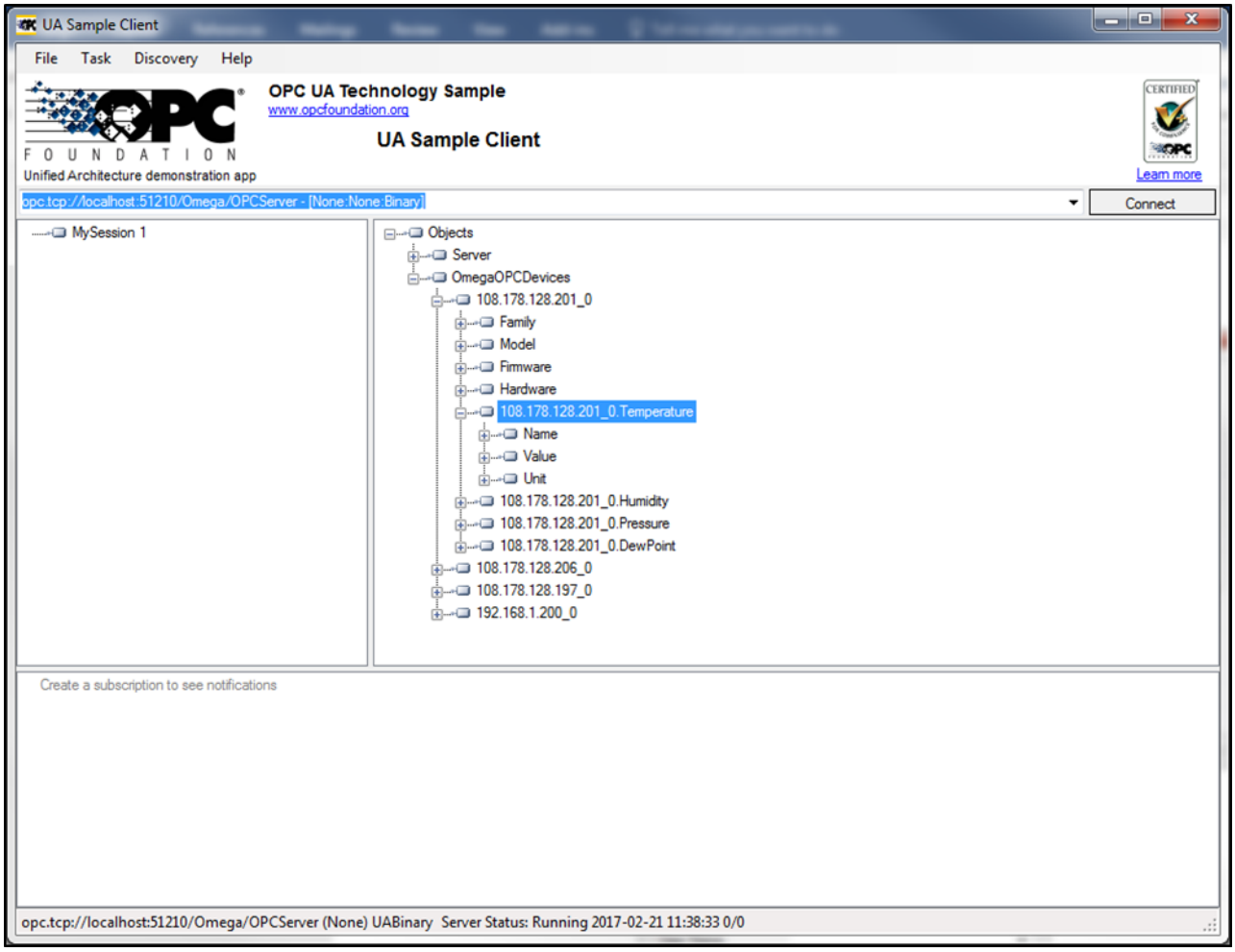

Figure 48: OPC UA Sample Client tree structure

Each measurement is presented as a tree node and has three attributes: Name, Value, and Unit. To display the most current readings, right-click the measurement node and click Browse in the pop-up menu.

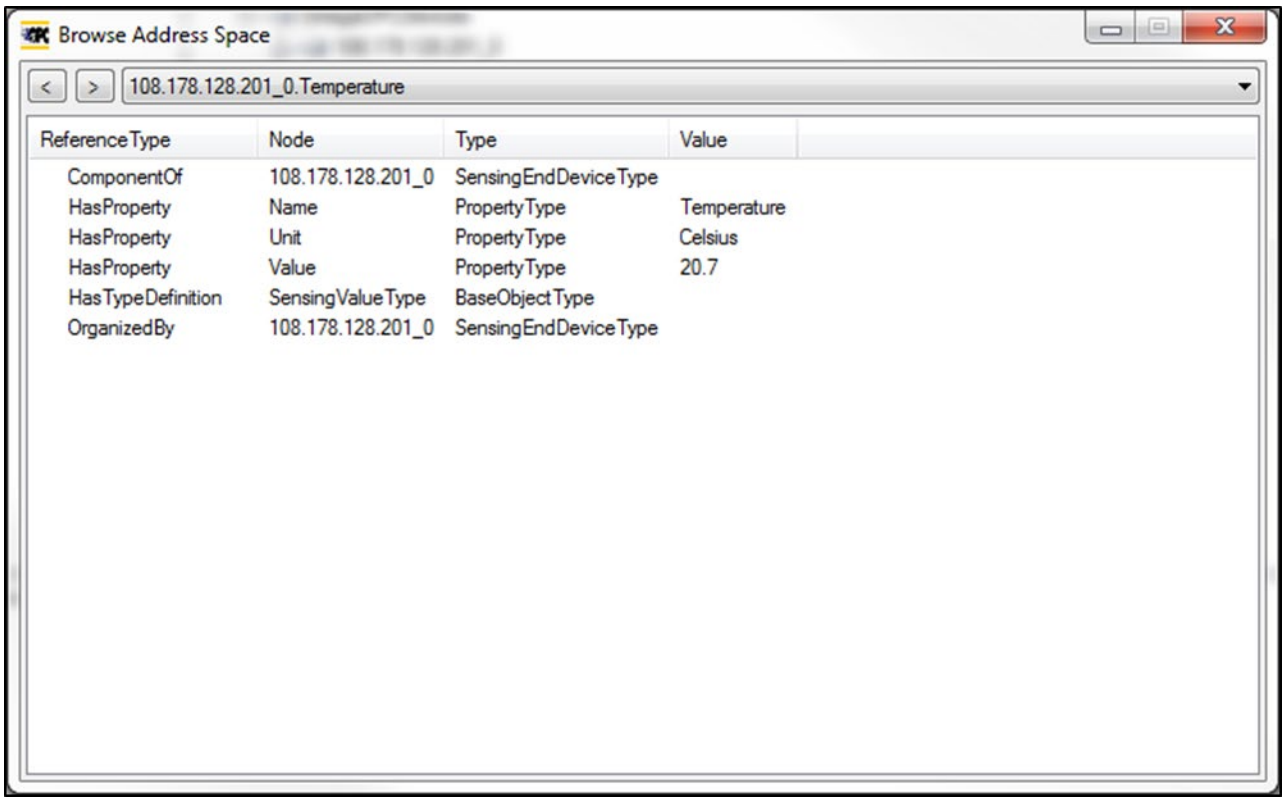

Figure 49: OPC UA Server Address Space Browser

Different OPC client applications, such as Enterprise application, have a different UI to access the OPC server. Please refer to the user manual of the software you are using.

14.2 OPC DA Server

Omega Enterprise Gateway exposes the OPC DA 2.0 and 3.0 compatible server that allows the OPC DA client to connect. Below is an example of using Matrikon's free OPC DA Explorer to test the OPC Server. You can download the OPC Explorer here:

https://www.matrikonopc.com/downloads/176/software/index.aspx

Once the software is started, you can navigate to OMEGA Enterprise Gateway DA OPC Server and click the **Connect** button to connect to the OPC server.

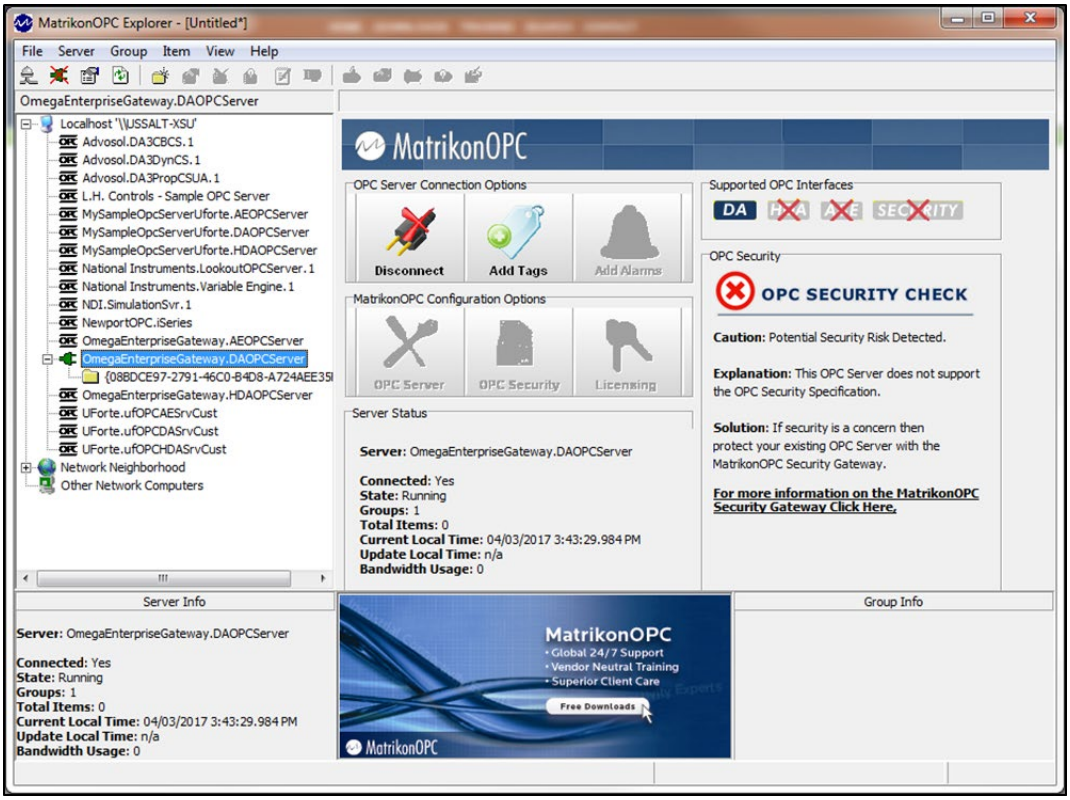

Figure 50: Matrikon OPC DA Explorer

Once the server is connected, you can browse the items from the available items list box. Items are automatically populated once you have added a device to the Omega Enterprise Gateway.

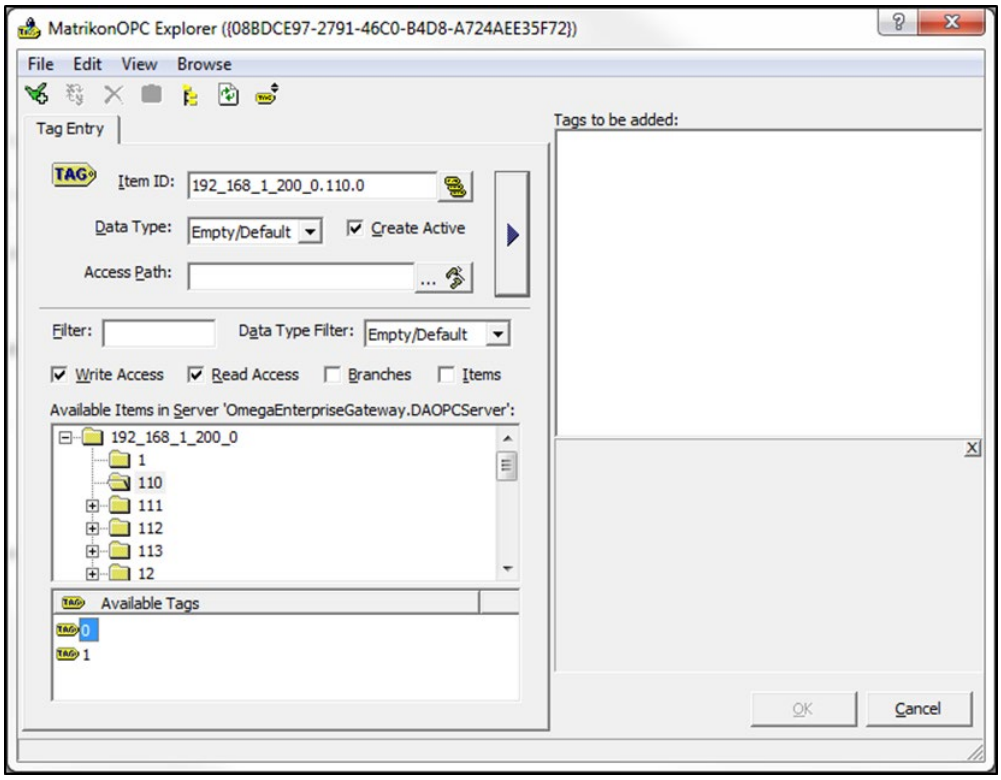

Figure 51: Matrikon OPC DA Explorer available items list

15 Exporting Data with the OEG Data Tool

The Omega Enterprise Gateway (OEG) Data Tool allows users to backup, restore, clean, and export OEG data. The OEG Data Tool can be utilized to accomplish the following tasks:

- **Backup Data** – The *Backup Data* function provides an efficient way to back up critical OEG user data collections. This feature is a critical step when migrating OEG from one computer to another computer.

- **Restore Data** – The *Restore Data* function allows users to restore all previously backed up OEG data collections. When coupled with the *Backup Data* function, users can migrate OEG from one computer to another.

- **Clean Data** – The *Clean Data* function provides users with a tool to clean abnormal data by removing collections that have 0 data points due to misconfiguration. Some devices may occasionally read abnormal data due to environmental electromagnetic interference or other factors.

- **Export Data** – The *Export Data* function exports each sensor channel into a single *.csv* file. Users can utilize the OEG Data Tool to combine all selected measurements into a single *.csv* file.

Note: Omega Engineering is not responsible for data lost due to user error. The Data Tool is only available for users with **Pro**, **Business**, or **Business Pro** OEG license tiers.

15.1 Launching the OEG Data Tool

After downloading and installing OEG, navigate to the Windows OS search bar and type **OEG Data Tool** to find and open the OEG Data Tool application.

Important: When connecting to the OEG Database, users must enter the **OEG URL** and the **Admin Password**. The OEG URL is the same URL used to access the user's OEG web UI. The Admin Password is same as the OEG admin password.

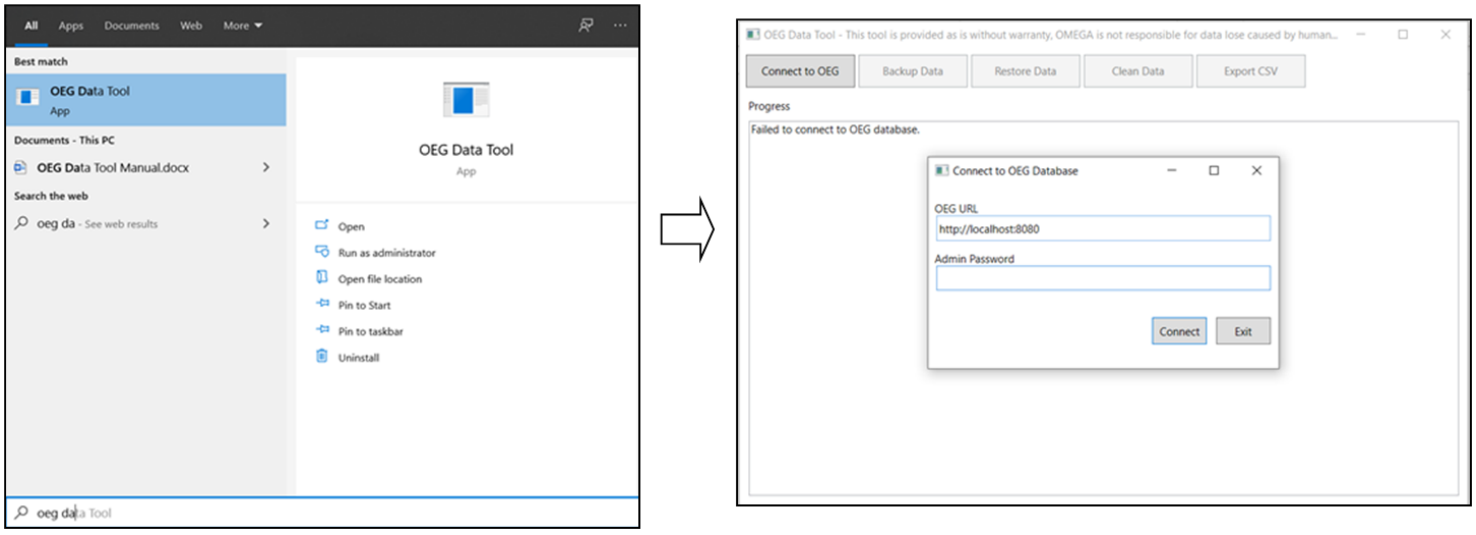

Figure 52: Launching the OEG Data Tool

15.2 Backup Data

Upon successful login, all function buttons are enabled. To begin the **Backup Data** process, follow these instructions:

Step 1: Click on the **Backup Data** button.

Step 2: Select a backup folder and specify time range, click **Ok** to start the backup process.

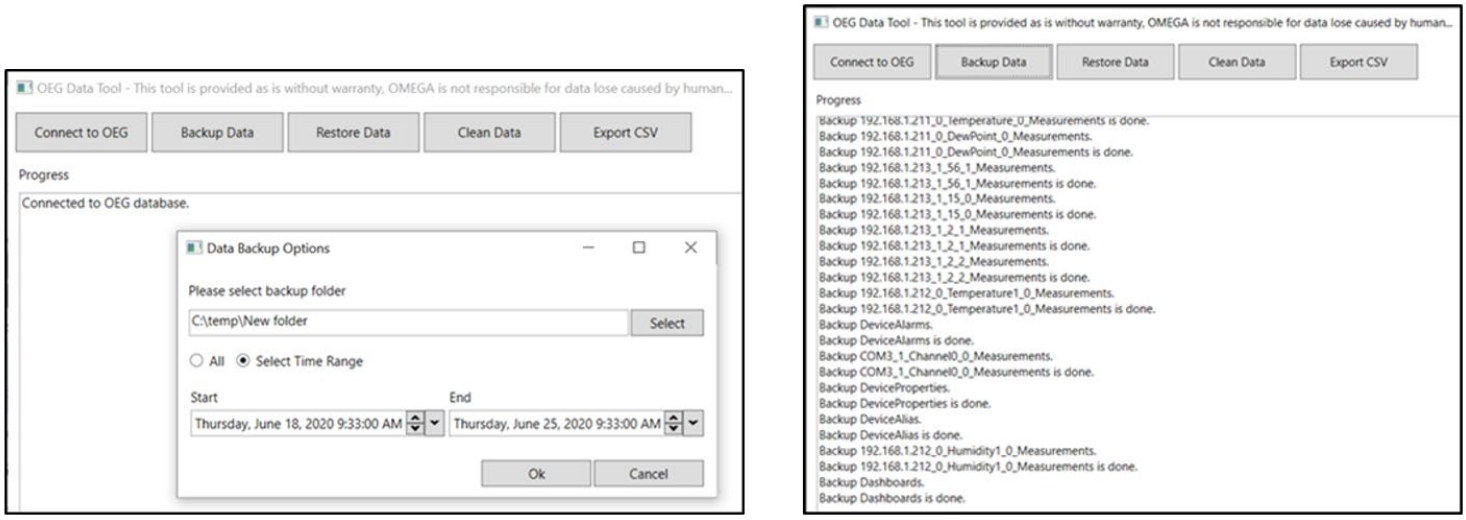

Figure 53: Data Backup Options interface

The backup progress will be displayed in the Data Tool textbox.

15.3 Restore Data

To restore data from previously backed up data, click on the **Restore Data** button. Clicking Restore Data will open the file folder and allow users to select one or more backup files. After selecting the backup file, click **Open** to start the restoration process. Progress will be displayed in the Data Tool textbox. Depending on the number of files selected, the Data Tool may need time to complete the restoration process.

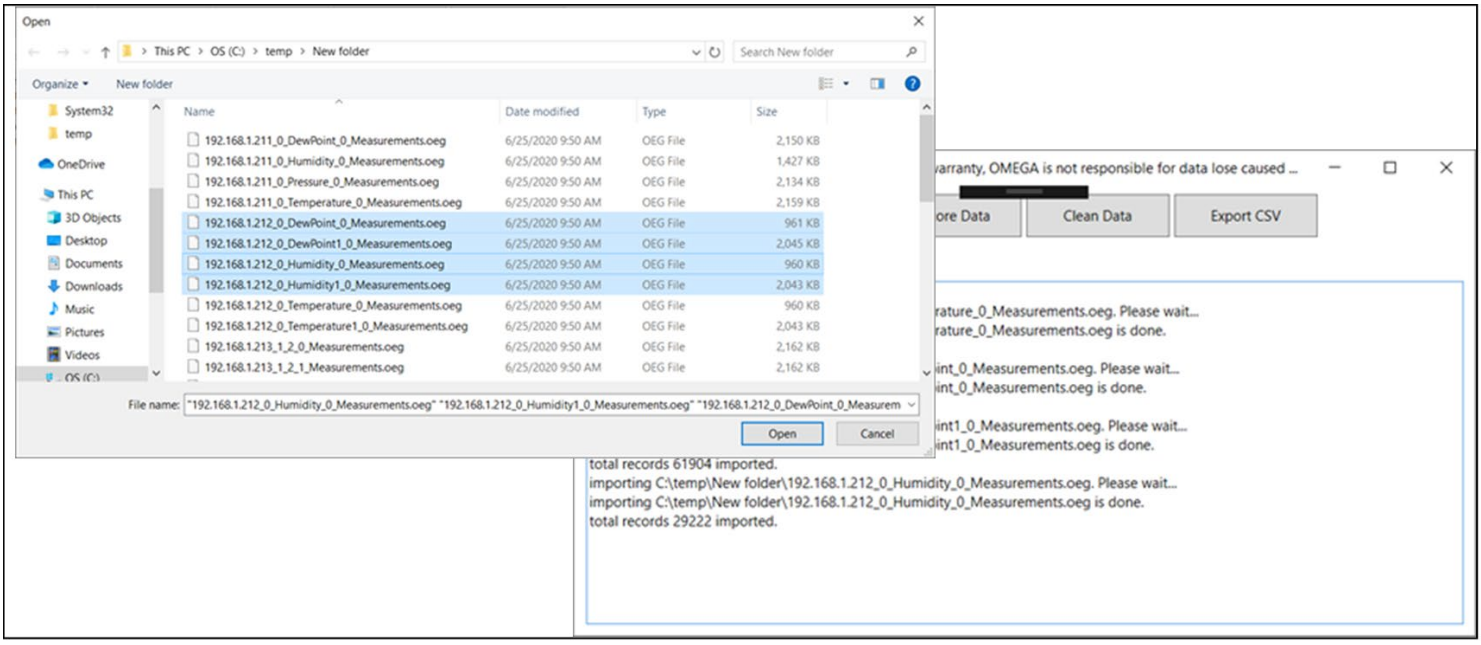

Figure 54: The user selects the backup data files that will be restored

15.4 Cleaning Data

Caution: Once data has been cleaned or deleted, it cannot be recovered.

OEG can capture abnormal readings from devices due to environmental electromagnetic interference and/or other unknown factors. Users can utilize the **Cleaning Data** function to remove abnormal readings. To delete data points, simply click the data points to highlight them and click the **Delete** button.

The data cleaning dialog will display all available data points. Users can apply filters to quickly identify points of interest. To start the cleaning process, follow the instructions below:

Step 1: Click on the **Clean Data** button to bring up the data cleaning dialog box and select data points and a date range to load the data in the chart.

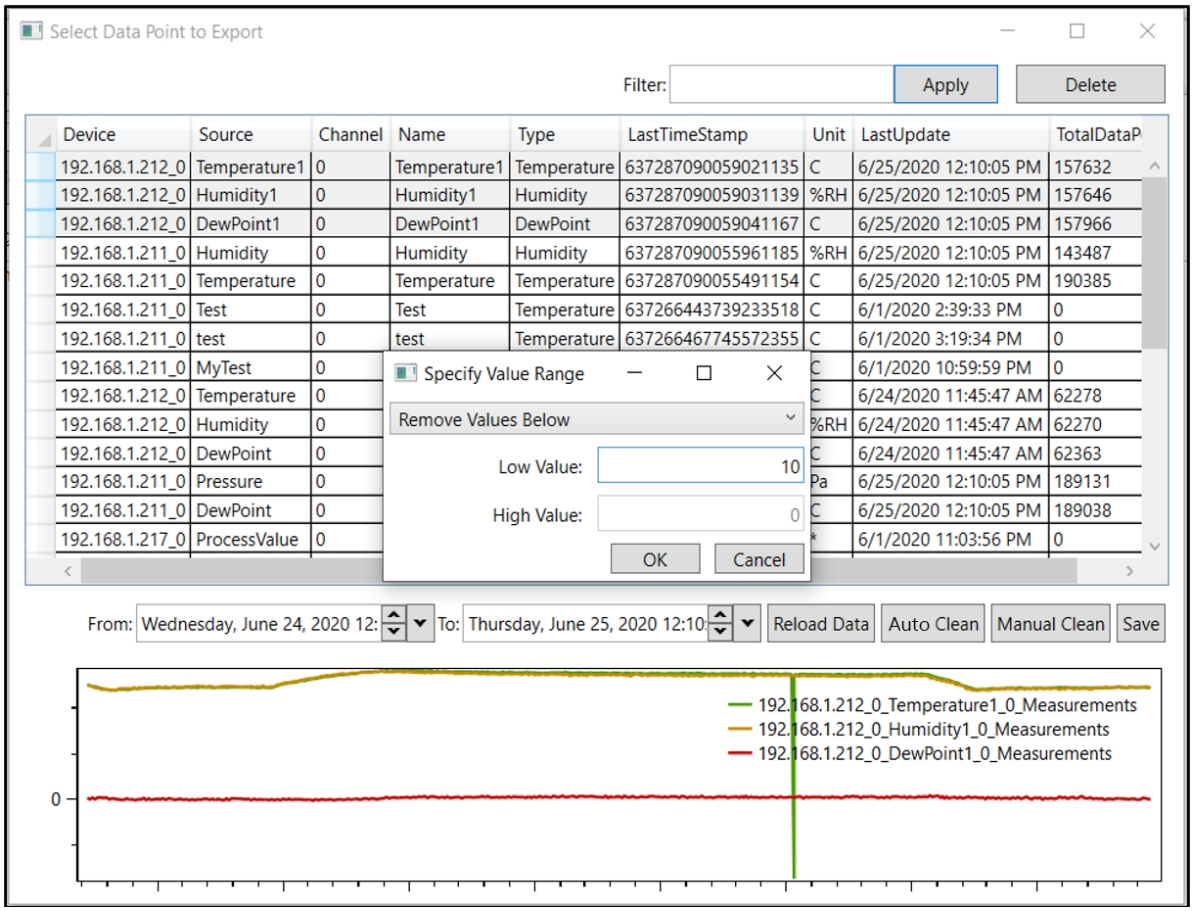

Figure 55: Users will select a range of data points to be cleaned

There are two methods to complete the data cleaning process. The **Auto Clean** function will try to detect abnormal data using running standard deviation check. The **Manual Clean** function allows users to specify outlier value ranges to remove the outliers.

Step 2: Choose **Auto Clean** or **Manual Clean** depending on your preference.

Step 3: After the data cleaning process is complete, click **Save** to save the cleaned data.

15.5 Export Data

The Export Data function allows users to combine multiple data points into a single .csv file. To utilize the Export Data function, follow these instructions:

Step 1: Click **Export CSV** and select the desired data, time range and file to export.

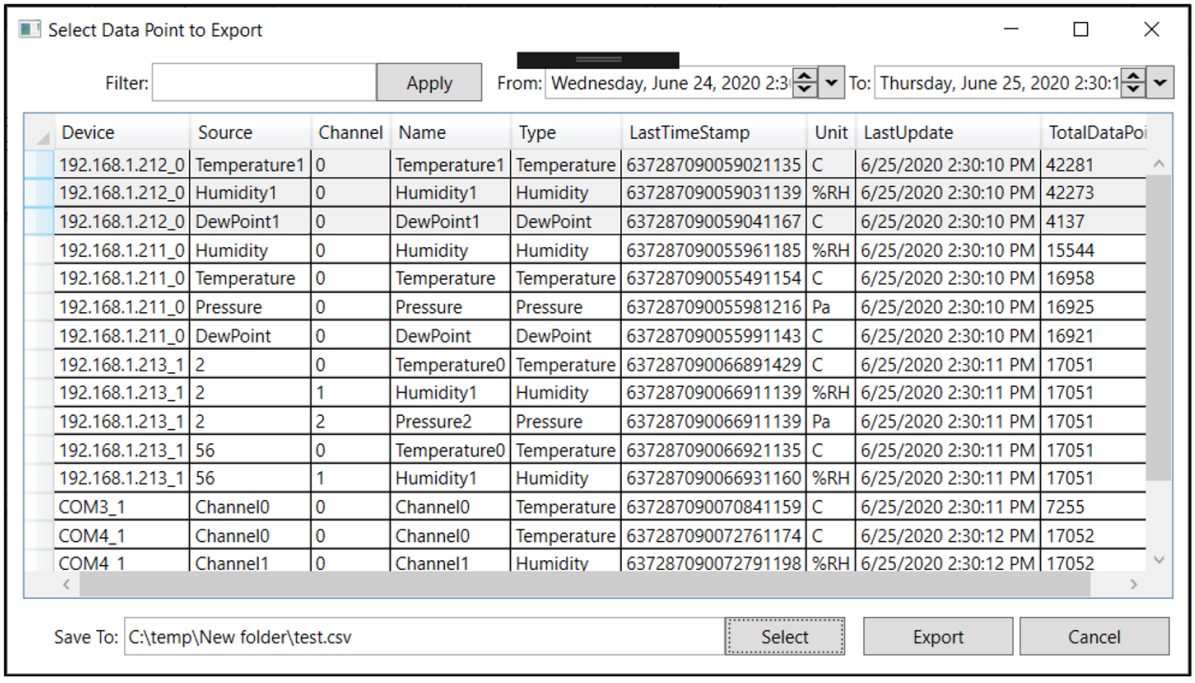

Figure 56: Users must define a range before exporting data

Step 2: Click the **Export** button to export the data.

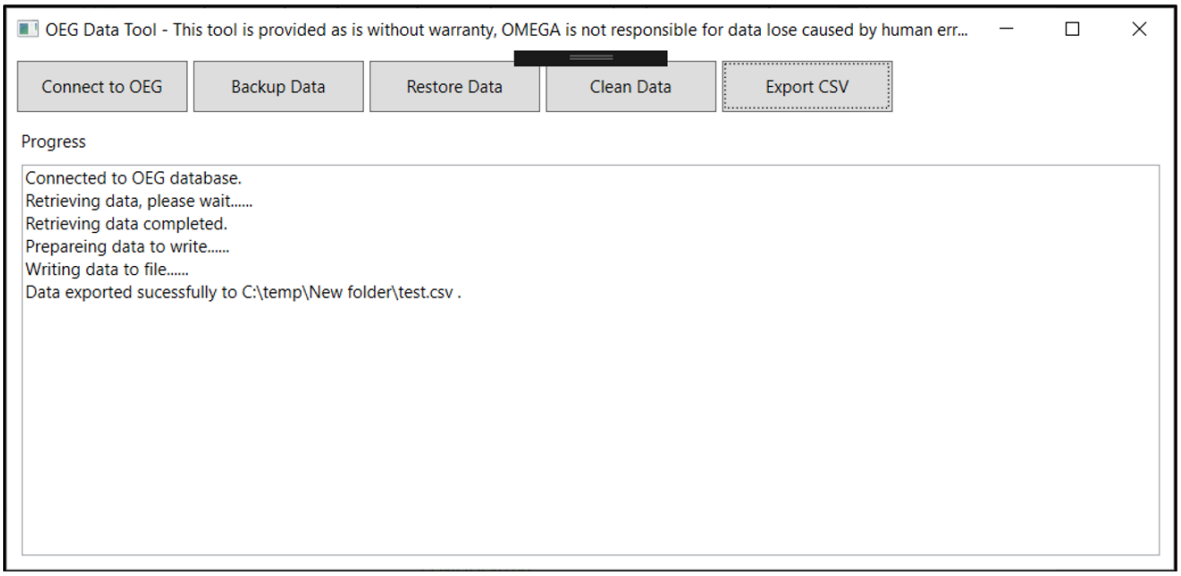

Figure 57: A successful export will be displayed in the Data Tool textbox.

This process will take time depending on how many data to be exported. The exportation progress will be displayed in the Data Tool textbox.