GEIST
MONITOR

Watchdog 100
Instruction Manual

Table of Contents

Chapter 4 - Final Checkout   61

Introduction

Welcome

Notice to Users

Geist, a division of PCE, Inc., reserves the right to make changes to this document without notice to any user or reseller of this product. Geist, a division of PCE, Inc., also reserves the right to substitute or terminate distribution of this document, with no obligation to notify any person or party of such substitutions or terminations.

Copyrights

© 2017 - Geist, a division of PCE, Inc.
All Rights Reserved

Trademarks

All Trademarks contained herein are registered to Geist, a division of PCE, Inc.

Use and Disclosure Restrictions

The software and documentation contained in this publication are copyrighted materials.

Recovery Act Buy American

Geist products adhere to the Buy American provisions of the American Recovery and Reinvestment Act of 2009 (Recovery Act). All Geist goods manufactured in our Lincoln, Nebraska, plant have undergone substantial transformation during production.

Trade Agreements Act (TAA)

Geist goods manufactured in our Lincoln, Nebraska, plant have undergone substantial transformation during production. These Geist products adhere to U.S. Trade Agreements Act and can be supplied for GSA Schedules and other government contracts.

Geist Policy on Conflict Minerals

This document details Geist's corporate policy regarding the use of conflict minerals. The policy expressed in this document should be considered to cover the Geist and Geist Europe divisions of PCE Inc.

Section 1502 of the Dodd-Frank Act which was passed by the US Congress in 2010 requires certain companies to annually disclose their use of conflict minerals. Conflict minerals covered under this act include tantalum, tin, tungsten, and gold.

Although Geist is not directly subjected to the requirements of the Dodd-Frank Act, Geist recognizes that all companies within the electronics manufacturing industry supply chain are impacted by this legislation. Geist supports the intent of the law, which is the reduction of violence within the Democratic Republic of the Congo and will take several actions to both advance the goals of the Dodd-Frank Act and to provide exceptional support to our customers.

· Geist will work with our direct suppliers to identify purchased components and materials that contain tin, tantalum, tungsten or gold.
· Geist will work with our direct suppliers to trace sources of any tin, tantalum, tungsten or gold used in our products back to the smelter.
· Geist will document our efforts to trace tin, tantalum, tungsten, and gold minerals back to the smelter and will accurately report the results to our customers.
· Geist will continue to monitor industry progress in identifying conflict-free smelters and will adjust corporate policy as the electronics supply chain becomes more fully documented.

Geist will not require that our direct suppliers source only conflict-free minerals until an adequate number of smelters has been reliably identified and audited by The Electronic Industry Citizenship Coalition (EICC) and the Global e-Sustainability Initiative (GeSI) to service the electronic industry supply chain. Mandating a conflict-free supply chain before an adequate number of smelters has been identified will prohibit the use of all tin, tantalum, tungsten, and gold originating in the Democratic Republic of the Congo and surrounding countries. This prohibition would cut off the sole income source for many artisanal miners within the region and may result in increased violence within the Democratic Republic of the Congo in direct opposition to the goals of the Dodd-Frank Act. Geist will work continuously with our direct suppliers in order to annually increase the percentage of documented conflict-free minerals that are used in our products until all products can be certified as conflict-free.

WEEE Declaration

Geist Europe is obligated to finance the cost of the collection, treatment, recovery and environmentally sound disposal of all products sold by Geist Europe into the UK market this includes:

· New WEEE (displaying 'the crossed out wheeled bin symbol') that Geist Europe has placed onto the market after the 13th August 2005; and

· Historic WEEE (not displaying 'the crossed out wheeled bin symbol'), when Geist Europe is supplying new WEEE that is intended to replace the historic WEEE and is of equivalent type or fulfills the same function even if the historic WEEE was manufactured by a third party.

Please contact Geist Europe on 01823 275100 for further details or to arrange collection. (UK Only)

Document Usage

All reasonable efforts have been made to assure the accuracy of this document from any technical or typographical errors or omissions. Geist, a division of PCE, Inc., and its affiliates disclaim responsibility for any labor, materials, or costs incurred as a result of usage of this document. Nor shall Geist, a division of PCE, Inc., and its affiliates be liable for any damages, inclusive of loss of profits or data, arising from the use of or in connection with this document.

Geist, a division of PCE, Inc., reserves the right to make changes to this document without notice to any user or reseller of this product. Geist, a division of PCE, Inc., also reserves the right to substitute or terminate distribution of this document, with no obligation to notify any person or party of such substitutions or terminations.

About this Manual

This document provides an overview of Geist product(s), the major topics covered include:

- Copyright, Trademarks, and Disclosure Restrictions.
- Instructions for installing, powering and using the equipment.
- Information that will aid in managing and maintaining the equipment.

Revision History

Revision	Date	Notes	Approved By
1.0	4/20/2017	Initial Version	SC

Organization of the Manual

This Geist document contains the following product information:

- Product Specifications - This chapter describes the major product characteristics and its functional role within the system. Where appropriate, reference to cabling among product components and to other Geist product(s) is provided.

- Installation - This chapter provides installation information for the preparation and use of Geist products as well as procedures required to adequately mechanically and electrically attach Geist product into supporting systems.

- Setup - This chapter provides instructions on power-up procedures after product installation and configuration of the software and features.

- Final Checkout - Technical Support guidelines and safety information are provided in this chapter.

Audience Profile

This document is intended for use by authorized technicians experienced with same of similar product types and for personnel requiring guidance for equipment installation, operation, maintenance, and support.

On-line Documentation

This document is available on-line and within the corresponding *Geist Product Manuals*. Additional Geist product supporting *Videos*, *Product Literature* and *Case Studies* can be found on the *Geist Resource* page.

Product firmware updates can be found and downloaded from the *Geist Support* site, under *Firmware Updates*.

Should this product fail within its warranty period and be in need of repair or replacement, a Return Material Authorization may be obtained on-line from the *RMA Form* link located within the *Geist Support* site.

Reporting Document Errors

Should you discover any error or identify a deficiency in this document, please take time to contact us at the following email address:

Geist-Documents@geistglobal.com

Please be sure to provide us with the document name, part number, and page number(s). Also, please provide us with description of the error or the deficiency for the document. If you would like for us to contact you, please provide us with your name and contact information.

Thank you for your time. We appreciate any comments and feedback you can provide.

Conventions

The information contained within this document is established around the framework of various conventions, which are defined as follows:

Software

- Release Management: Product name, Version control; (Watchdog 100, v3.3.0)
  - Product Name: Name of Hardware Platform
  - Version control: V(ersion) Platform #, Major #, Minor #

Hardware

Product Classification
  - Power Distribution Unit
    - Basic
    - Monitored only
    - Switched only
    - Monitored + Switched
  - Environmental Monitoring
  - Cooling
  - Data Center Infrastructure Management (DCIM)

Figure 1   Overlay Symbology Guide
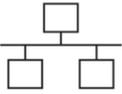
	Ethernet		Activity / Idle
	Power over Ethernet		Power
IOIOI	Serial	A~	Amps
	Remote Display		Reboot
	Remote Sensors		Silence
	Uplink		Scroll
	Temp		GU Right
	Sensor Configuration		GU Left
		GU Center	
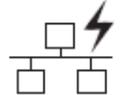
Figure 1 The chart above depicts the symbols used on Geist overlays.

Safety

This document contains varying levels of alerts pertaining to product and user safety. The alerts are visually presented with graphics and text per Geist equipment guidelines.

The representations are:

⚠	# DANGER INDICATES AN **IMMINENT** HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, WILL RESULT IN **DEATH OR SERIOUS INJURY**.

⚠	# WARNING INDICATES A **POTENTIAL** HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, COULD RESULT IN **DEATH OR SERIOUS INJURY**.

⚠	# CAUTION INDICATES A **POTENTIAL** HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, COULD RESULT IN **PRODUCT DAMAGE** AND **MINOR TO MODERATE INJURY**.

⚠	# NOTE Provides useful information that is beneficial for operation and usage of this product.

Figures

Figures presented in this document are identified and designated as follows:

'Figure:', Chapter # - Image #

Example:

Figure 1-1   Name and/or Title goes here

Tables

Tables presented in this document are identified and designated as follows:

'Table:', Chapter # - Image #

Example:

Table 1-1   Name and/or Title goes here

Column 1	Column 2	Column 3	Column 4	Column 5
Text	Text	Text	Text	Text
Text	Text	Text	Text	Text
Text	Text	Text	Text	Text
Text	Text	Text	Text	Text

Chapter 1 - Product Specifications

Product Specifications

Overview

The Watchdog 100 provides remote environmental monitoring and alarming capability needed to detect climate conditions in critical environments. The Watchdog 100 has a built-in sensor to monitor temperature, humidity and dew point, as well as one port for adding remote sensors. The Watchdog 100 also has four I/O ports for connecting additional external 5Vdc sensors such as Flood and Door Sensors. Additionally, the Watchdog 100 provides one output relay that can be operated remotely or set to automatically open or close based on alarm conditions. The Watchdog 100 can be optionally configured at the factory to support Power-Over-Ethernet (PoE).

All internal and external sensors are measured every 5 seconds. Sensor data collected by Watchdog 100 units provides useful trend analysis data. While all values are not absolute in relation to a known unit, trend analysis of the data allows users to view changes and draw useful conclusions about what is happening over time in the monitored environment.

Figure 1-1   Watchdog 100

Onboard Sensors

Watchdog 100 contains the following onboard sensors:

- **Temperature:** Measures temperature and can be displayed in °C or °F. The accuracy is ±0.5 °C from -20 °C to 80 °C. Note: This sensor may be heated by internal circuitry in the unit; a temperature offset is available to re-calibrate.
- **Humidity:** Measures the percent of water vapor in the air within ±2% from 20% to 80%.
- **Dew Point**: Calculated measurement of temperature at which moisture in the air will turn to liquid based on the humidity and temperature measurements.
- **AI1:** Scales 0 to 5 Vdc input to 0-99, dry contacts may be used.
- **AI2:** Scales 0 to 5 Vdc input to 0-99, dry contacts may be used.
- **AI3:** Scales 0 to 5 Vdc input to 0-99, dry contacts may be used.
- **AI4:** Scales 0 to 5 Vdc input to 0-99, dry contacts may be used.

Figure 1-2   Watchdog 100-P

Analog I/O Sensors

The Watchdog 100 units come equipped with four Analog I/O ports for connecting additional external sensors such as Flood and Door Sensors. The four ports are designed to accept a 0-5 Vdc analog input; alternatively, an internal 100K pull up resistor to 5 V allows for the use of dry contacts. The Analog I/O port input is converted to a digital number ranging from 0 to 99 and is displayed on the Sensors page. Unused I/O ports will display a value of 99. This range can be adjusted on the display page allowing the user to modify the value to make it more meaningful to the user.

Flood sensors act as conductivity bridges. Moisture across the contacts causes the value to drop. Door switches can be wired in a serial connection; if the chain is broken the entire group is classified as open. The limiting factor on the I/O ports is the length of the wire, found to be around 400 feet.

Figure 1-3   Flood Sensor Wiring
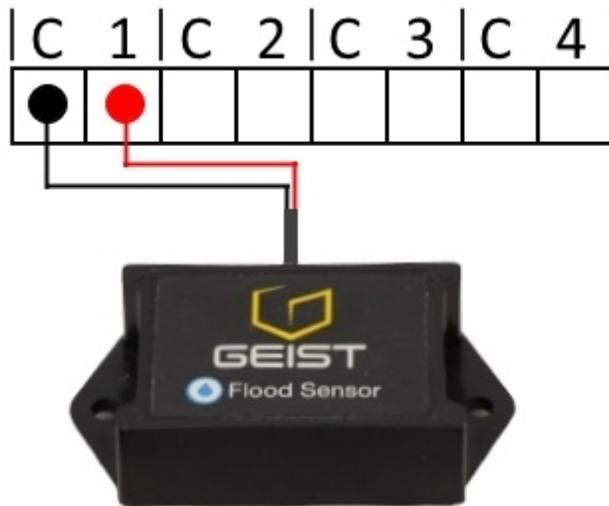
Figure 1-4   Door Sensor Wiring
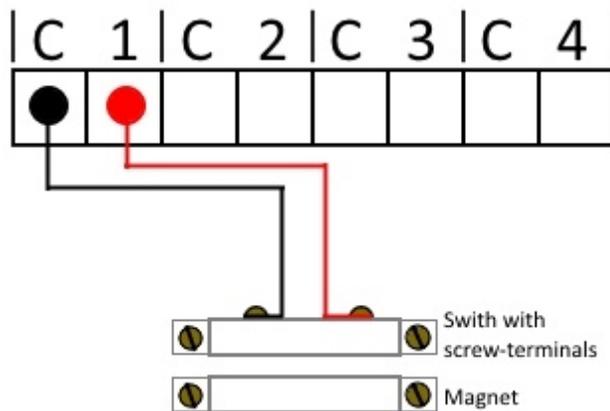
Available Analog I/O Sensors

- **FS:** Flood Sensor
- **RDPS:** Door Sensor
- **SA-1:** Smoke Alarm
- **RCP-2:** 125 V City Power Monitor
- **WSK-10:** 10' Water Sensing Cable Kit
- **WSK-40:** 40' Water Sensing Cable Kit

- **-48 IVS-DC:** Isolate Voltage Sensor, -48Vdc
- **30 VDCM:** Power Monitor

Remote Sensors

Available Remote Sensors
- **SRT:** Stainless Remote Temperature
- **GTHD:** Temperature / Humidity / Dew Point
- **GT3HD:** Temperature / Humidity / Dew Point with ability to add two RT sensors
- **RTAFHD3:** Temperature / Air Flow / Humidity / Dew Point
- **A2D:** Converts analog I/O Sensors to Remote Digital Sensors

RTAFHD3 Compatibility
The (G)RTAFHD3 sensor cannot be utilized in combination with the discontinued (G)RTAF and (G)RTAFH sensors or (G)RTHD sensors built prior to 2010. If you desire to add (G)RTAFHD3 sensors to an existing installation currently utilizing incompatible sensors, please contact Customer Service for installation options. (G) indicates Global Sensor variants that may be used outside of the US.

Connecting Remote Sensors
Plug-and-play remote sensors may be attached to the unit at any time via the RJ-12 ⓒ connectors on the face of the unit. In some cases splitters may be required to add additional sensors. Each sensor has a unique serial number and is automatically discovered and added to the web page. Up to four sensors may be connected to the Watchdog 100.

The display order of the sensors on the web page is determined by the serial number of each sensor. Friendly names for each sensor can be customized on the Sensors Overview page.

<table>
<tr><td>

⚠ (triangle with exclamation mark)

</td><td>

NOTE

Sensors use Cat. 3 wire and RJ12 connectors. Wiring must be straight-through: reverse polarity will temporarily disable all sensors until corrected. Sensors use a serial communication protocol and are subject to network signaling constraints dependent on shielding, environmental noise, and length of wire. Typical installations allow runs of up to 600 feet of sensor wire.

</td></tr>
</table>

Environmental

The operational environmental limits pertaining to Temperature, Humidity and Elevation are as defined below.

Temperature

Table 1-1   Temperature Limits

	Minimum	Maximum
Operating	-10°C (50°F)	45°C (104°F)
Storage	-25°C (-13°F)	65°C (149°F)

Humidity

Table 1-2   Humidity Limits

	Minimun	Maximum
Operating	5%	95% (non-condensing)
Storage	5%	95% (non-condensing)

Elevation

Table 1-3   Elevation Limits

	Minimun	Maximum
Operating	0 m (0 ft)	2000 m (6561 ft)
Storage	0 m (0 ft)	15,240 m (50,000 ft)

Electrical

6-12 Volts DC, 2 Amps
Power-Over-Ethernet (PoE) Enabled (Class 0)

Output Relay Contact Ratings
The output relay contacts are intended to carry low voltage signals only. Do not exceed the following ratings on the output relay contacts:

DC: 60V, 30W
AC: 30Vrms, 1A

WARNING
The Watchdog 100 unit has not been evaluated for and should not be used in any application in which the failure of the hardware could lead to death, personal injury or severe physical or property damage or environmental damage (collectively, "High-Risk Applications"), including but not limited to the operation of nuclear facilities, mass transit systems, aircraft navigation or aircraft communication systems, air traffic control, weapon systems and direct life support machines. Geist expressly disclaims any express or implied warranty or condition of fitness for High-Risk Applications.

CAUTION
Consideration should be given to lockout-tagout and other procedures required for servicing external devices controlled by the Watchdog 100 output relays. Appropriate safety precautions must always be taken when operating or maintaining equipment connected to the Watchdog 100. Geist assumes no responsibility or liability for any injury or damage to any persons or property resulting from improper operation or maintenance of a device connected to the Watchdog 100.

Networking

The product communications requirements are identified below.

Ethernet

The Ethernet link speed for this product is: 10/100 Mb; full duplex.

Protocols

The communications protocols supported by this product include:
HTTP, HTTPS (TLS v1.2), SMTP/POP3, ICMP, DHCP, TCP/IP, NTP, Syslog,
SNMP (v1/2c/3 and GDP.

User Interfaces

This product supports the following user interfaces:
SNMP, Web GUI, and JSON API.

Regulatory Compliance

Geist products are regulated for Safety, Emissions, and Environment Impact per the below agencies and policies.

Underwriters Laboratories (UL)

UL Standards are used to assess products; test components, materials, systems and performance; and evaluate environmentally sustainable products, renewable energies, food and water products, recycling systems and other innovative technologies.

The UL standards specific to this equipment are as noted on the device nameplate.

Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications laws, regulation and technological innovation.

The FCC standards specific to this equipment are:

This Class A device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

	WARNING
⚠	Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

RoHS/WEEE

WEEE stands for Waste from Electrical and Electronic Equipment. WEEE Directive 2002/96/EC mandates the treatment, recovery and recycling of electric and electronic equipment (90% ends up in landfills). All applicable products in the EU market must pass WEEE compliance and carry the "Wheelie Bin" sticker.

RoHS, also known as Lead-Free, stands for Restriction of Hazardous Substances. RoHS, also known as Directive 2002/95/EC, originated in the European Union and restricts the use of six hazardous materials found in electrical and electronic products. All applicable products in the EU market after July 1, 2006 must pass RoHS compliance. RoHS impacts the entire electronics industry and many electrical products as well.

RoHS specifies maximum levels for the following six restricted materials:

- Lead (Pb): < 1000 ppm
- Mercury (Hg): < 100 ppm
- Cadmium (Cd): < 100 ppm
- Hexavalent Chromium: (Cr VI) < 1000 ppm
- Polybrominated Biphenyls (PBB): < 1000 ppm
- Polybrominated Diphenyl Ethers (PBDE): < 1000 ppm
- Bis(2-Ethylhexyl) phthalate (DEHP): < 1000 ppm
- Benzyl butyl phthalate (BBP): < 1000 ppm
- Dibutyl phthalate (DBP): < 1000 ppm
- Diisobutyl phthalate (DIBP): < 1000 ppm

See product label for RoHS/WEEE compliance marks.

Chapter 2 - Installation

Pre-Installation

Guidelines
- If the Watchdog 100 is installed in a cabinet, the ambient temperature of the rack should be no greater than 80 °C.
- Install the Watchdog 100 such that the amount of airflow required for safe operation of equipment is not compromised.
- Mount the Watchdog 100 so that a hazardous condition is not achieved due to uneven mechanical loading.

Installation

1. Using appropriate hardware, mount unit at desired location. See next section for examples.

2. Connect AC power supply to appropriate source, or if using PoE, connect Ethernet cable to PoE enabled switch port.

3. Connect any external plug and play sensors into the devices RJ-12 ports ⓒ .

Network Setup

The Watchdog 100 has a default IP address for initial setup and access. Once you have assigned an IP address, the default IP address will no longer be active. To restore the default IP address and reset all user-account information, if the user-assigned address or passwords are lost or forgotten, press and hold the network-reset button located below the Ethernet port for 15 seconds.

To completely erase ALL of the user settings and restore the unit back to its factory-default state, disconnect power from the Watchdog 100, then press and hold the network-reset button while powering up the unit.

The Network page (located under the System Tab) allows you to assign the network properties manually, or use DHCP to connect to your network. Access to the unit requires the IP address to be known. Use of a static IP or a reserved DHCP is recommended. The default address is shown on the front of the unit:

Table 2-1   Default IP Address

IP Address:	192.168.123.123
Subnet Mask:	255.255.255.0
Gateway:	192.168.123.1

To access the unit for the first time, you will need to temporarily change your computer's network settings to match the 192.168.123. xxx subnet. To set up the unit, connect it to your computer's Ethernet port, then follow the appropriate instructions for your computer's operating system.

Windows

· **Windows 2000 / XP / Server 2003:**
Click the **Start** button, choose **Settings**, then **Network Connections.**

· **Windows 7 / Server 2008:**
Click the **Start** button, then choose **Control Panel** >> **Adjust Your Computer's Settings** >> **View Network Status and Tasks** >> **Change Adapter Settings**. (Alternatively, on some Windows 7 machines, this may be **Start**, then **Settings** >> **Control Panel** >> **Network and Sharing Center** >> **Change Adapter Settings**.)

· **Windows 8 / Server 2012:**
Move the mouse cursor to the bottom or top right corner of the screen, click the **Settings** icon, then select **Control Panel**. Change the view type from **Category** to **Large** or **Small Icons** if necessary, then select **Network and Sharing Center**, then **Change Adapter Settings**.

· **Windows 10:**
Click the **Start** button, then choose **Network & Internet**, then click **Change adapter options.**

Locate the entry under **LAN or High-Speed Internet** or **Local Area Connection** which corresponds to the network card (NIC).

|	**NOTE**
⚠	Most computers will have a single Ethernet NIC installed, but a WiFi or 3G adapter will also show as a NIC in this list, so be sure to choose the correct entry.

Double-click on the network adapter's entry in the **Network Connections** list to open its status dialog box, then click the **Properties** button to open the **Local Properties** window.

Figure 2-2 Local Area Connection Properties
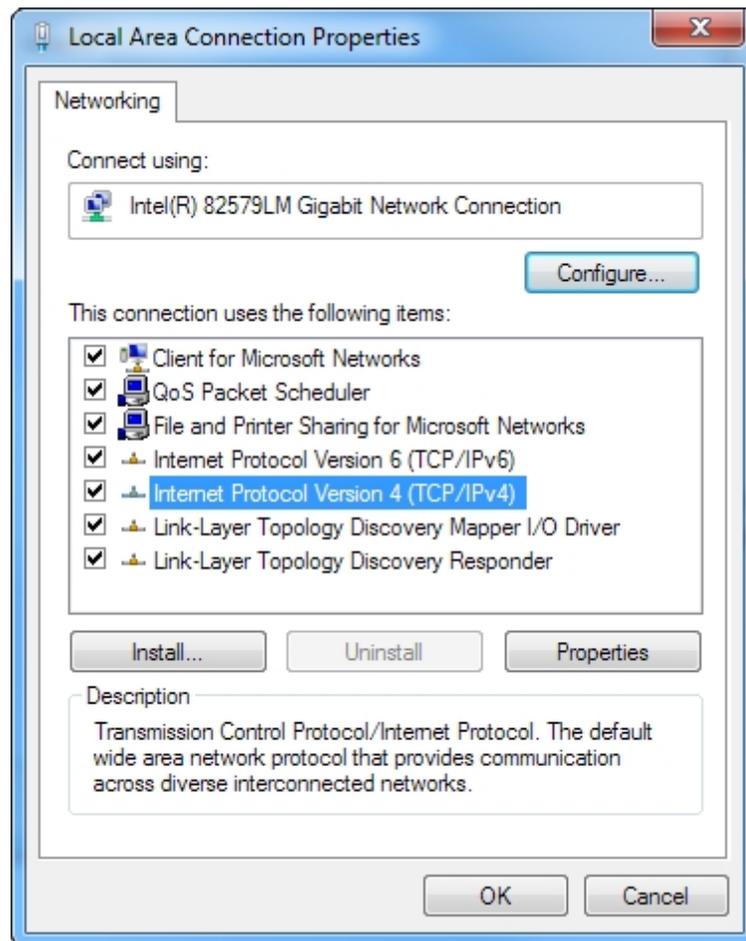
Find the entry titled "**Internet Protocol Version 4 (TCP/IPv4)**" in the list, then click the **Properties** button to open the **Internet Protocol Properties** window. If you see more than one TCP/IP entry, as in the example above, the computer may be configured for IPv6 support as well as IPv4; make sure to select the entry for the IPv4 protocol. Write down the current NIC card settings so you can restore them to normal after you have completed the setup procedure.

Figure 2-3   Internet Protocol Version 4
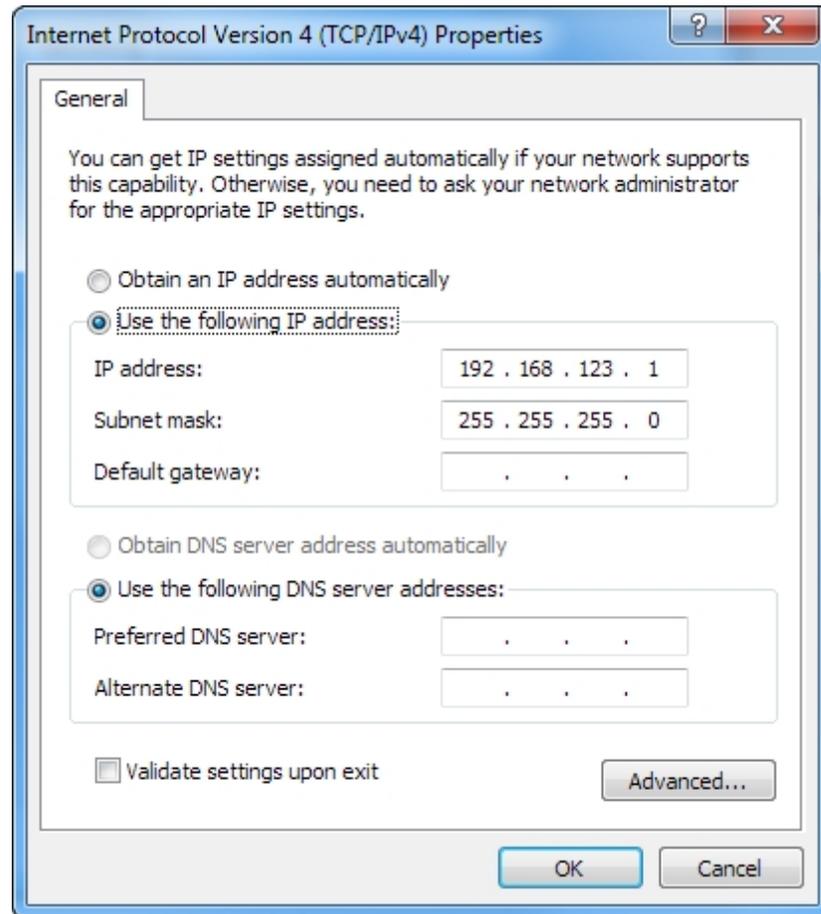
Choose the **Use the following IP address** option, then set **IP address** to 192.168.123.1 and **Subnet Mask** to 255.255.255.0. For this initial setup, **Default Gateway** and the **DNS Server** entries can be left blank. Select **OK**, then **OK** again to close both the **Internet Protocol Properties** and **Local Properties** windows.

Once the NIC settings are configured properly, you should be able to access the unit by typing **http://192.168.123.123** into the address bar of your web browser. If you are setting up the unit for the first time, or if the unit has been reset back to factory defaults via the network-reset button, the unit will require you to create an Admin account and password before you can proceed.

Once you have created an Admin account and have logged into it, the unit's default **Sensors** page should come up by default. Navigate to the **System** tab, then the **Network** page to configure the device's network properties. The unit's IP Address, Subnet Mask, Gateway, and DNS settings can either be assigned manually, or acquired via DHCP.

Note that the new settings will take effect when the **Save** button is clicked. The browser will no longer be able to reload the web page from the 192.168.123.123 address and will probably display a "page not found" or "host unavailable" message. This behavior is normal. Once you have finished configuring the unit's IP address, simply repeat the steps above, and change the computer's Ethernet NIC card settings back to the ones you wrote down prior to changing them, to restore its normal network and internet settings.

Mac

Click the **System Preferences** icon on the Dock, and choose **Network**.

Figure 2-4   Mac System Preferences
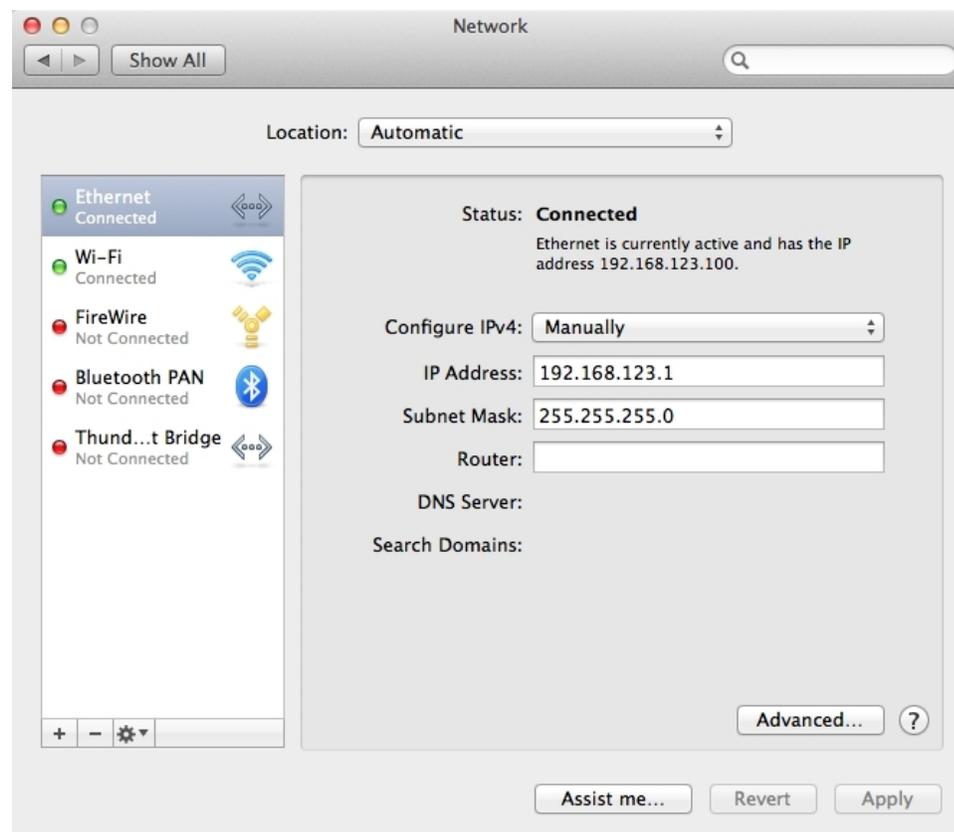
Be sure **Ethernet** is highlighted on the left side of the NIC window. In most cases, there will be one Ethernet entry on a Mac. Write down the current settings so you can restore them to normal after you have completed the setup procedure.

Select **Manually** from the **Configure IPv4** drop-down list, then set **IP Address** to 192.168.123.1 and **Subnet Mask** to 255.255.255.0. The **Router** and **DNS Server** settings can be left blank for this initial setup. Click **Apply** when finished.

Once the NIC settings are configured properly, you should be able to access the unit by typing http://192.168.123.123 into the address bar of your web browser. If you are setting up the unit for the first time, or if the unit has been reset back to factory defaults via the network-reset button, the unit will require you to create an Admin account and password before you can proceed.

Once you have created the Admin account and logged into it, the unit's default **Sensors** page should come up by default. Navigate to the **System** tab, then the **Network** page to configure the device's network properties. The unit's IP Address, Subnet Mask, Gateway, and DNS settings can either be assigned manually, or acquired via DHCP.

The new settings will take effect when the **Save** button is clicked, so the browser will no longer be able to reload the web page from the 192.168.123.123 address and will probably display a "page not found" or "host unavailable" message. This behavior is normal. Once you have finished configuring the unit's IP address, simply repeat the steps above, and change the computer's Ethernet NIC card settings back to the ones you wrote down prior to changing them, to restore its normal network and internet settings.

Chapter 3 - Setup

Web Interface

The unit is accessible via a standard, unencrypted HTTP connection as well as an encrypted HTTPS (SSL) connection. The following web pages are available:

Sensors Page

Overview

The front page, Sensors Overview, gives both current and historical views of the unit's data. Readings for the internal temperature, humidity and dew point sensors along with all external sensors, such as the A2D converter, will be shown. Plug-and-play external sensors appear below the internal sensors when attached.

Figure 3-1   Sensors Overview Page

1. Geist Logo
   - Clicking on this logo from any page will reload the Sensors Overview page.

2. Sensors, System, and Help Tab
   - Mouse over to show sub-menus:
     - Sensors: Available options are "**Overview**" (this page), "**Alarms and Warnings**", "**Cameras**", "**Logging**", and "**Data Graphing**".
     - System: available options are "**Users**", "**Network**", "**Web Server**", "**Time**", "**Email**", "**SNMP**", "**Syslog**", "**Admin**", "**Locale**", and "**Utilities**". Refer to the appropriate section under "**System**".
     - Help: available options are "**Info**" and "**Support Site**" Refer to the appropriate section under "**Help**".

3. Log In / Log Out
   - Click to log in or log out of the unit. Note that both username and password are case sensitive and no spaces are allow. Prohibited characters for username only are: $&`:<>[ ] { }"+%@/ ; =?\^|~',

4. Alarms and Warnings
   - Indicates the number of Alarms and Warnings currently occurring, if any.

5. Device Label
   - Displays the user-assigned label of this unit.

6. Device ID
   - Unique product identification and cannot be changed. May be required for technical support.

7. Connected Sensors
   - Displays State, Temperature, Humidity and Dew Point of connected sensors.

8. Relay
   - Displays and configure relay state (Energize/De-energize). The Watchdog 100 has one relay that can be operated remotely or set automatically opened or closed based on alarm conditions. Friendly names for the relay give the option of changing the state name from "Energized/De-energized" to something more meaningful to user.

Figure 3-2   Icons

 Configuration Icon   **Operation Icon**

<table>
<tr><td>⚠️</td><td>

NOTE
You must log in before making any changes. Only users with Control-level authorizations have access to these settings.
</td></tr>
</table>

Device Labeling and Temperature Offset

1. Click the desired Configuration icon, and change the device's **Label** and **Temperature Offset** as needed. **Name** is the device's factory name or model, and cannot be changed.

2. Once done, click **Save**.

Figure 3-3   Device Labeling and Temperature Offset
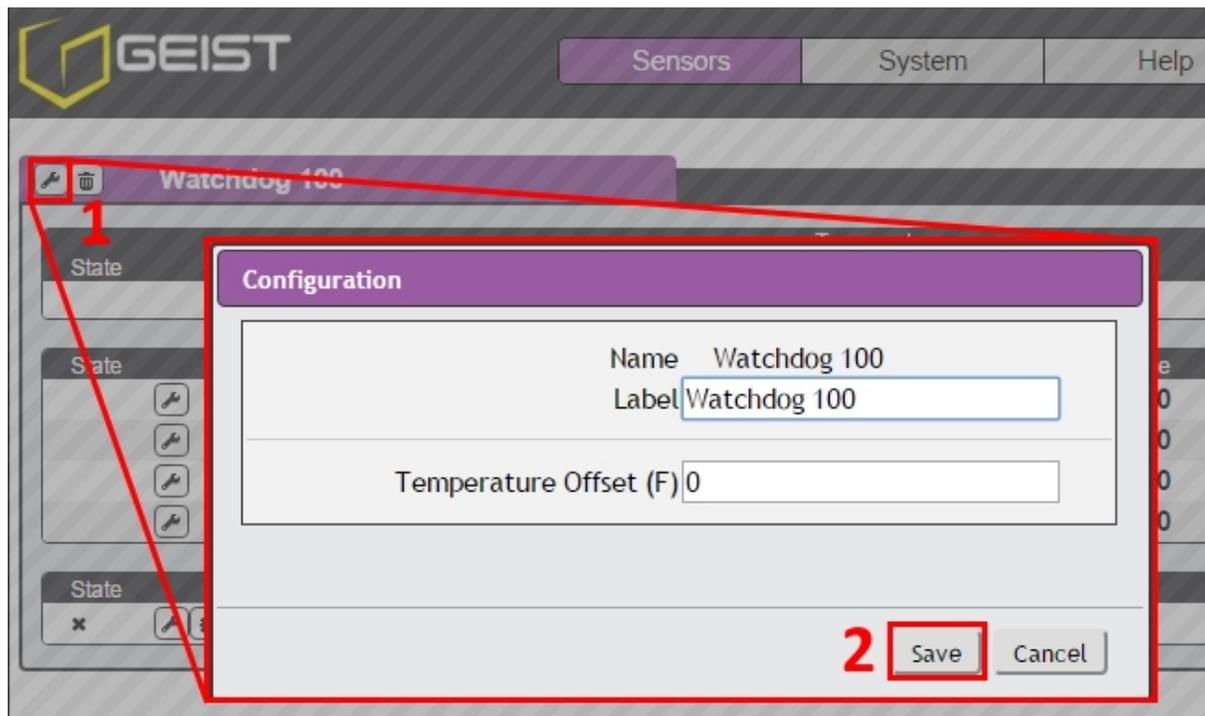
Deleting a Sensor

This device and associated data and configuration can be deleted by clicking the delete icon 🗑 and following the confirmation prompt. The deleted device must be removed, otherwise, it will be re-detected and shown on the page.

Figure 3-4   Deleting a Sensor
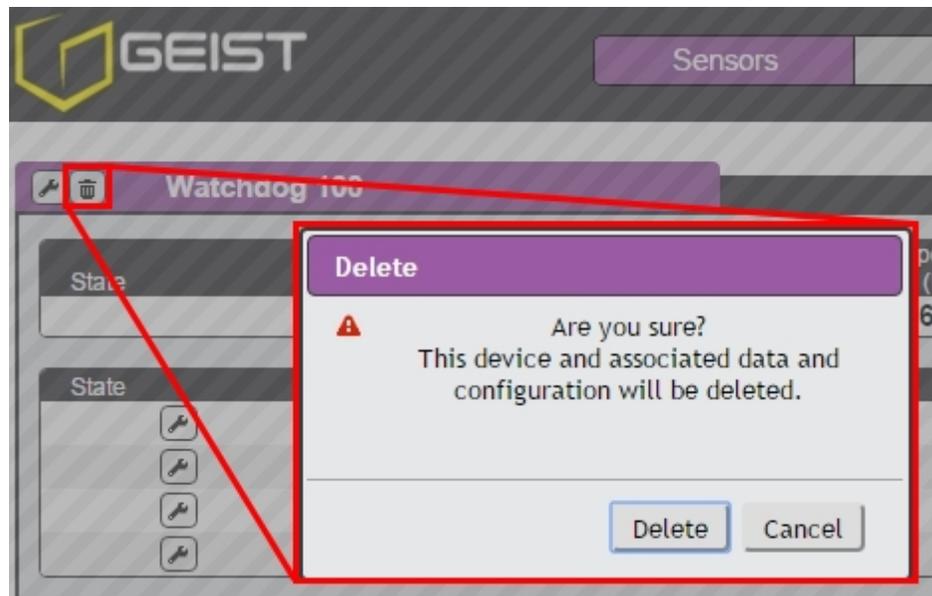
Relay Control

Relay Contact Ratings

The output relay contacts are intended to carry low voltage signals only. Do not exceed the following ratings on the output relay contacts:

DC: 60V, 30W
AC: 30Vrms, 1 A

Relay Configuration

The Watchdog 100 units provide one output relay that can be operated remotely or set to automatically open or closed based on alarm conditions. A relay in non-latching mode will automatically energize and de-energize as its associated alarms trip and clear. A relay in latching mode will similarly energize on an alarm trip, but will only de-energize when acknowledged by the user on the *Alarms and Warning* page. See *Add/Modify Alarms and Warnings* for additional information on associating an alarm condition with the output relay.

Relay Labeling and Mode Select

The relay label and manual override or alarm mode can be changed on the "Configuration" page.

Figure 3-5   Relay Labeling and Mode Select
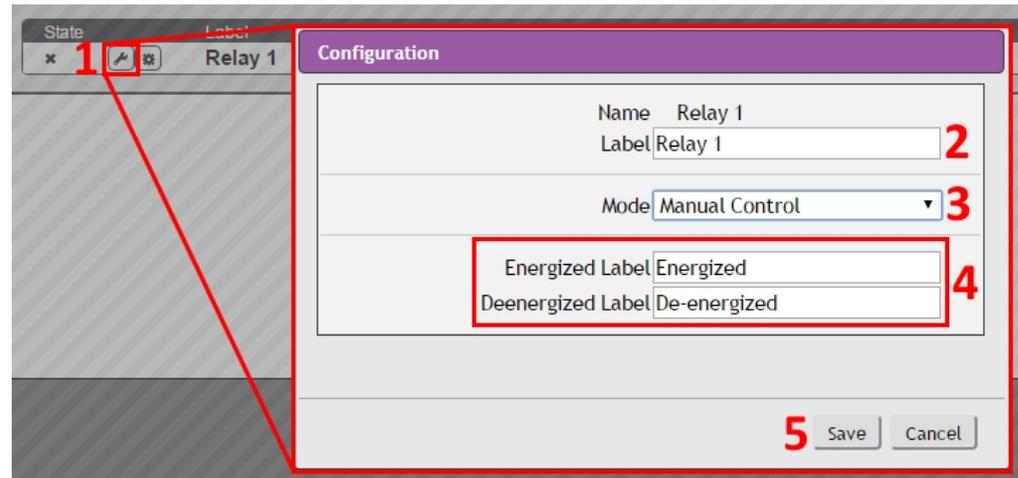
1. Click on the **Configuration** icon 🔧.

2. Change label to desired name.

3. Select desired mode:
    a. **Alarm Control:** Act according to Alarms and Warning settings.
    b. **Manual Control:** Enable user to force the relay to energize or de-energize. See **Relay Manual Control Setting** below.

4. Change label of Energize/De-energize to desired name.

5. Click **Save** when done.

Relay Manual Control Setting

Figure 3-6   Relay Control Setting
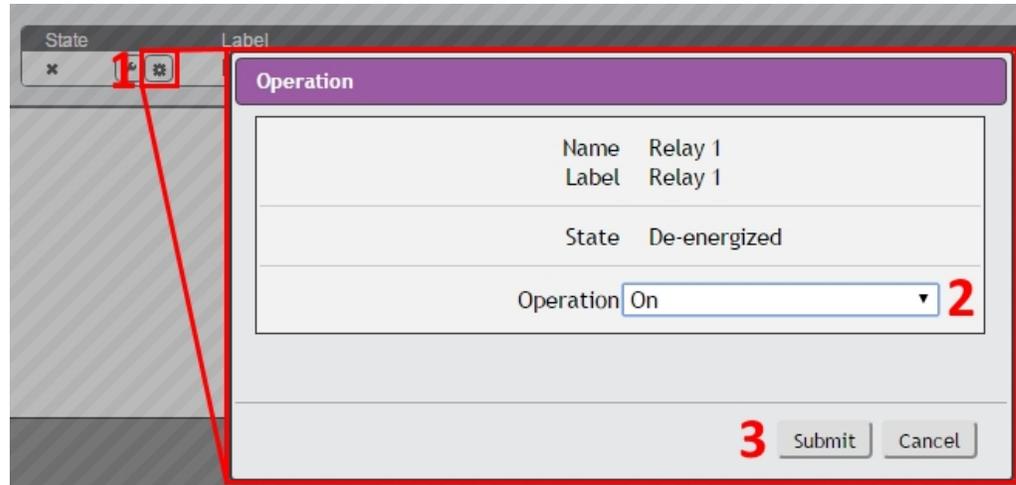
1. Click on the **Setting** icon.

2. Change **Operation** to desired relay condition: On (Energized); Off (De-energized). Notice the **State** label. This describes the current state of the relay.

3. Click **Submit** to commit the change.

Alarms & Warnings

The Alarms & Warnings Page allows the user to establish alarm or warning conditions (hereafter referred to as "Events") for each sensor reading. Events are triggered when a measurement exceeds a user-defined threshold, either going above the threshold ("high-trip") or below it ("low-trip"). Events are displayed in different sections, based on the device or measurement the Event is associated with. Each Event can have one or more actions to be taken when the Event occurs.

Figure 3-7   Alarms and Warnings Page

1. **State:** Shows the status of each Event.
   - Empty: No alert condition.
   - ！ : This symbol indicates that this particular "Warning" Event has been tripped. A tripped Warning Event displays in orange.
   - ▲ : This symbol indicates that this particular "Alarm" Event has been tripped. A tripped Alarm Event displays in red.
   - ✔ : This symbol indicates that this Event has been acknowledged by user after being tripped. It will remain this way until the condition being measured by this Event returns to normal (i.e., ceases to exceed the trigger threshold for this Event).

2. **Configuration:** Add/Delete/Modify Alarms & Warnings.
   - ⊕ : Add new Alarms & Warnings.
   - 🔧 : Modify existing Alarms & Warnings.
   - ⊖ : Delete Existing Alarms & Warnings.

3. **Notification:** Notify user of tripped Events, and request acknowledgment.
   - Empty: No alert condition.
   - ☑ : Acknowledge button. When a Warning or Alarm Event has occurred; the user can click on this symbol to acknowledge the Event and stop the unit from sending any more notifications about it. Note: Clicking this symbol does not <u>clear</u> the Warning or Alarm Event, it just stops the notifications from repeating.

4. The actual conditions for the various Alarms & Warnings settings are shown here.

To add a new Alarm or Warning Event:

1. Click the Add/Modify Alarms & Warnings button:

Figure 3-8   Adding Alarms and Warnings

2. Set the desired conditions for this Event as follows:
   a. Select the **Name** of the device you wish to set an Event on.

   b. Select the measurement (temperature, humidity, etc.) you want to **Trigger** the Event.

   c. Set the **Severity** level ("Warning", or "Alarm") for this Event.

   d. Select the threshold **Type**, "high" (trips if the measurement goes above the threshold) or "low" (trips if the measurement goes below the threshold).

   e. Type in the desired **Threshold Value** (any number between -999.0 ~ 999.0 is valid).

f. Type in the desired **Clear Delay** time in seconds. Any value other than "0" means once this Event is tripped, the measurement must return to normal for this many seconds before the Event will clear and reset. Clear Delay can be up to 14400 seconds (4 hours).

g. Type in the desired **Trip Delay** time in seconds. Any value other than "0" means that the measurement must exceed the threshold for this many seconds before the Event will be tripped. Trip Delay can be up to 14400 seconds (4 hours).

h. **Latching Mode**: If enabled, this Event and its associated Actions (see below) remain active until the Event is acknowledged, even if the measurement subsequently returns to normal.

i. **Valid Time:** Allows user to set specific times an Event will trigger a notification. Multiple **Valid Time** entries can be set allowing users to set alerts to notify different **Targets** based on time of day or day of week.

j. To determine where the alert notifications will be sent to when this particular Alarm or Warning Event occurs, click the **Add** icon to create a new Action, then select the desired options from the drop-down menu:

Figure 3-9   Add Page
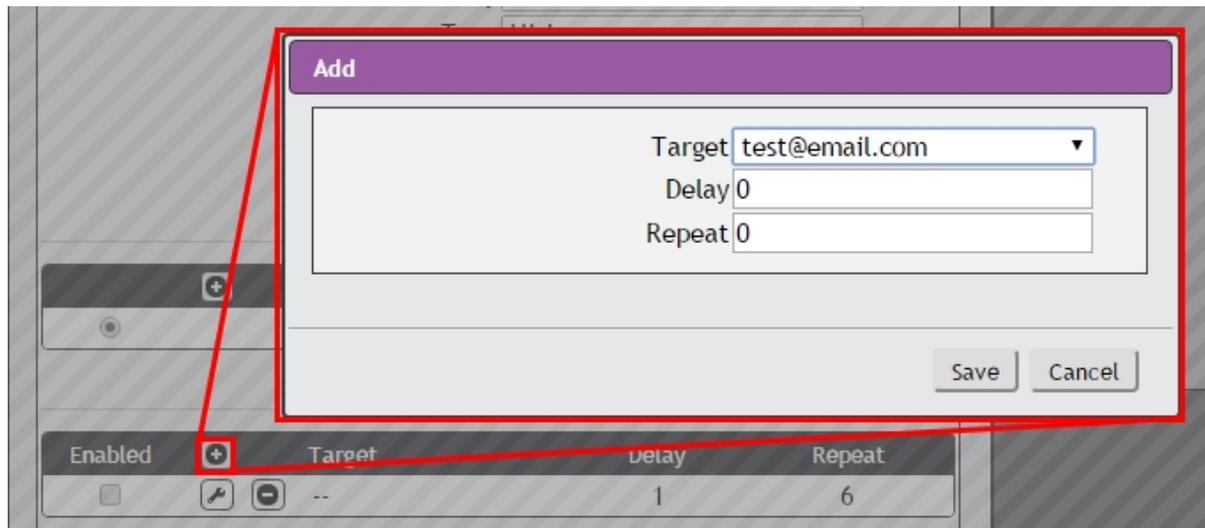
• **Target:** is the email address or SNMP manager to which notifications should be sent when the Event is tripped.

> ⚠️ **NOTE**
> Target Delays and Repeats are shared across all alarms. If multiple Delay and/or Repeat values are needed for specific Targets, each one must be added to the Target list and then the appropriate 'Enabled' box checked on each alarm. See screen-shot below for example.

Figure 3-10 Target Page

Enabled	⊕		Target	Delay	Repeat
☐	🔧	⊖	target@email.com	90	0
☑	🔧	⊖	target@email.com	60	0

- **Delay:** determines how long this Event must remain tripped for before this Action's first notification is sent. This is different from the Trip Delay above. Trip Delay determines how long the threshold value has to be exceeded <u>before</u> the Event itself is tripped. This delay determines how long the Event must <u>remain</u> tripped before this Action occurs. Delay can be up to 14400 seconds (4 hours). A Delay of 0 will send the notification immediately.

- **Repeat:** determines whether multiple notifications will be sent for this Event Action. Repeat notifications are sent at the specified intervals until the Event is acknowledged, or until the Event is cleared and reset. The Repeat interval can be up to 14400 seconds (4 hours). A Repeat of 0 disables this feature, and only one notification will be sent.

Then, click **Save** to save this notification Action.

More than one Action can be set for an Alarm or Warning; to add multiple Actions, just click the Add icon again and set each one as desired. Each alert can have up to 32 Actions associated with it.

To change an existing Alarm or Warning Event:
Click the **Modify** icon next to the Alarm or Warning Event you wish to change, then modify the specific settings as shown.

Figure 3-11 Modify Action Page
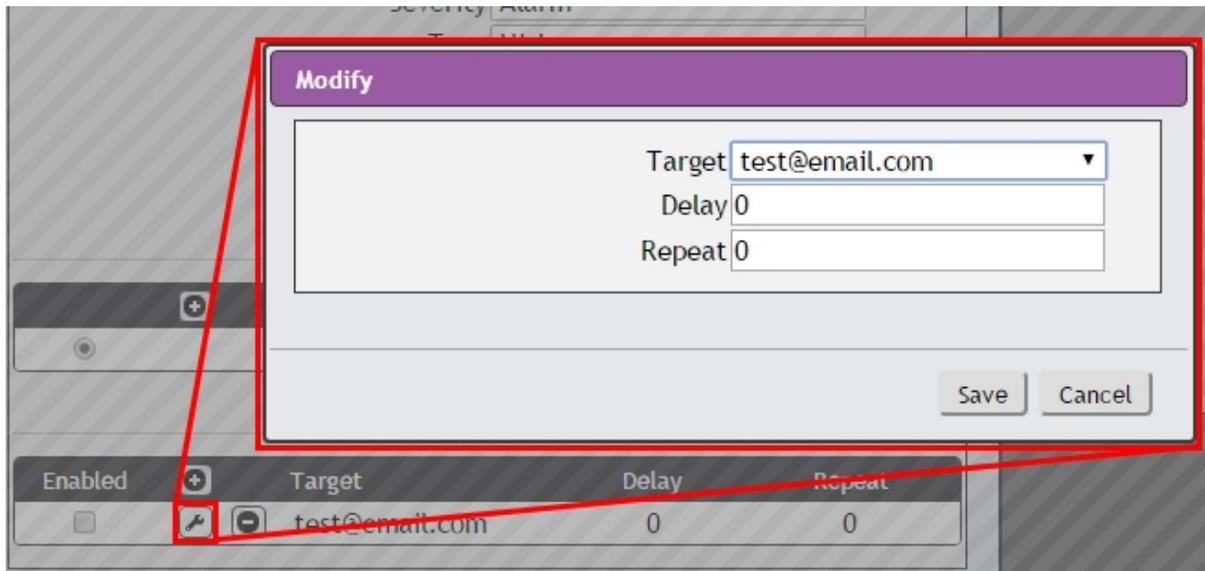
Once an Action has been added, each Action has its own checkbox in the "enabled" column at the far left. The default is unchecked (disabled) when you first add each Action; set the checkbox to enable it. This allows you to selectively turn different Actions on and off for testing.

To delete an existing Alarm or Warning Event:
Click the Delete icon next to the Alarm or Warning Event you wish to change, then click **Delete** to confirm.

Figure 3-12 Delete Action Page
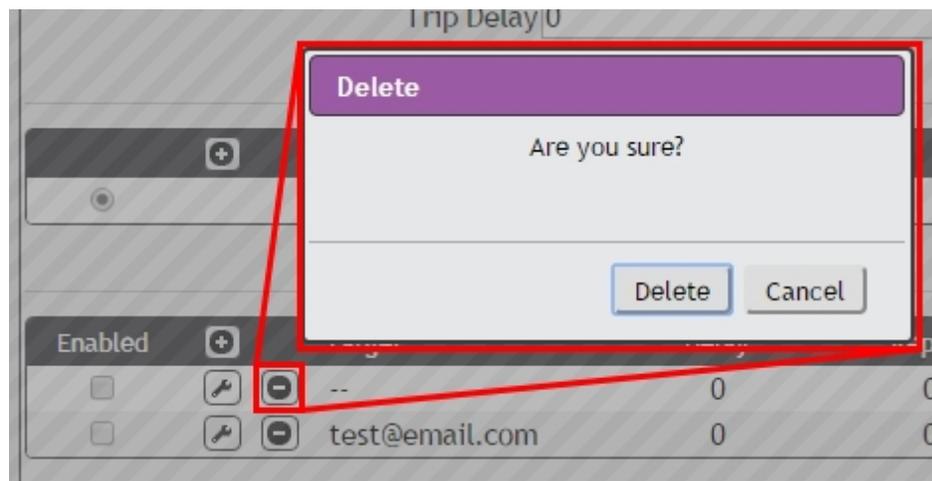
3. When finished, click **Save** to save this Alarm or Warning event.

Cameras

The Cameras Page allows the user to add IP-addressable network cameras for remote monitoring. Up to four IP-addressable network cameras can be added.

> ⚠ **NOTE**
>
> Some cameras require additional software downloads to display live video in a web browser. Each camera must be set to allow anonymous access to enable this feature. Clicking on the camera image opens the camera's website in a new browser window.

Figure 3-13 Cameras Page

To add a new camera:

1. Click the Add/Modify Camera button:

Figure 3-14 Add a Camera
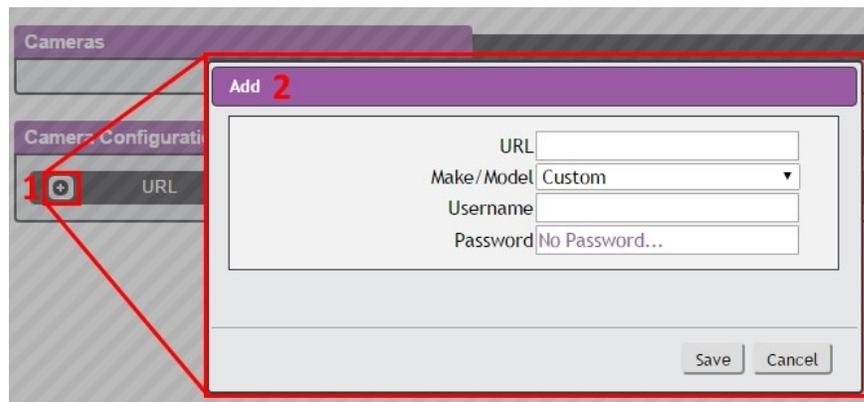
2. Set the desired conditions for this Event as follows:
   a. Enter the URL of the online camera.
   b. Select the Make/Model of camera you are connecting to.
   c. Enter the Username if necessary.
   d. Enter the Password if necessary.
3. Click **Save**.

Modifying a camera:

1. Click the Modify icon.

Figure 3-15 Modify a Camera
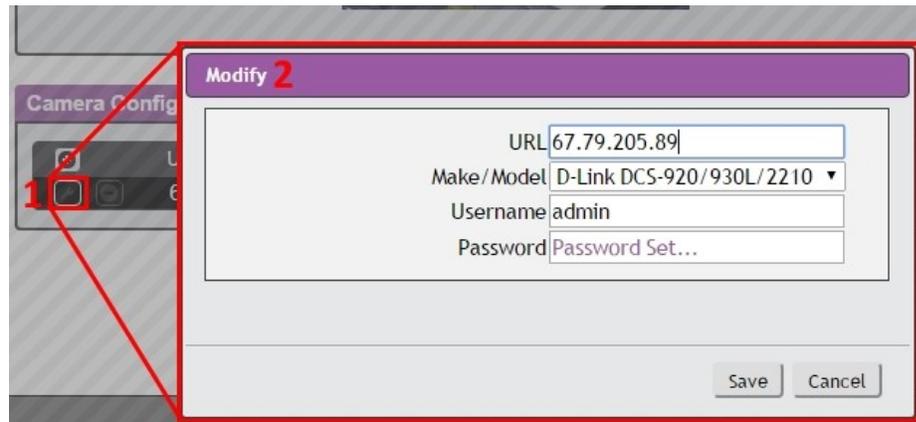
2. Make the changes.
3. Click **Save** when finished.

To delete a camera:

To remove a camera entirely, click the **Delete** icon to remove the camera from the list, then click Delete to confirm:

Figure 3-16 Delete a Camera
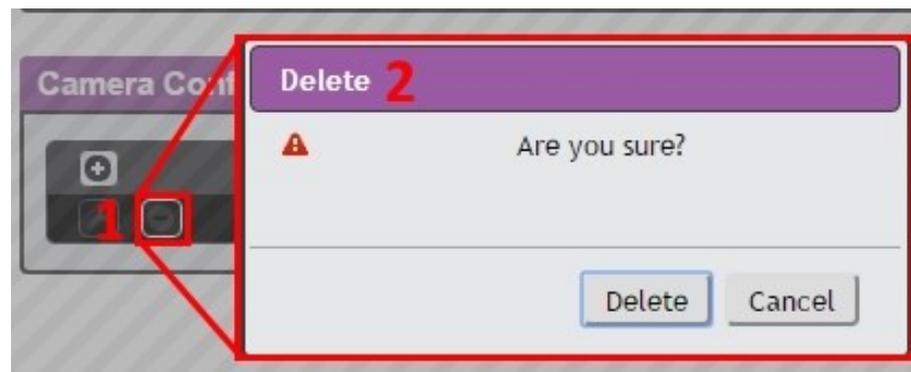
Logging

The Logging Page allows the user to download the historical data recorded by the unit. Recorded data is available for download in Comma-Separated Values (CSV) or JavaScript Object Notation (JSON) file types. Data is written to the log every 60 seconds, however, all sensor data used in by the real-time display and alarm functions is read at least once every 5 seconds.

Figure 3-17 Logging Page
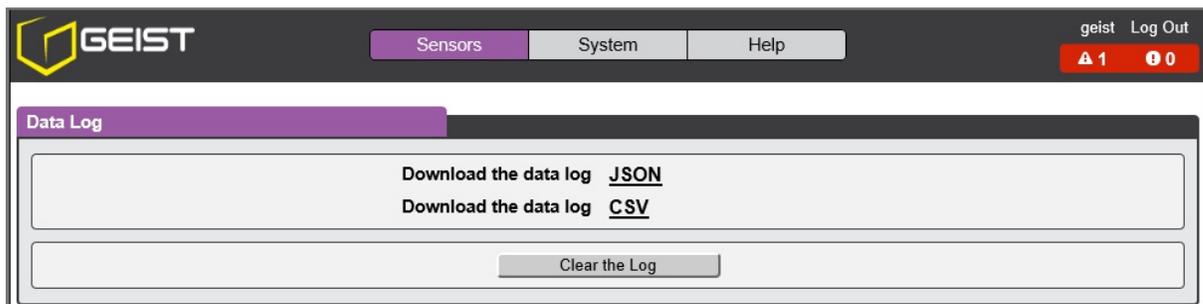
Download Data Log:

1. Right click on the desired data type.
2. Choose **Save** link as…
3. Follow save link prompt.

Figure 3-18 Download Data Log
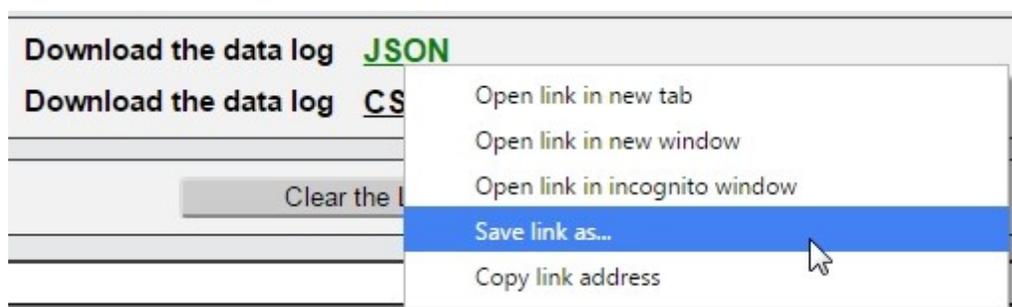
Clear Data Log:

1. Click **Clear the Log** button.

Figure 3-19 Clear Data Log
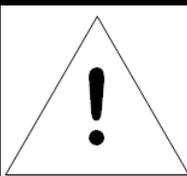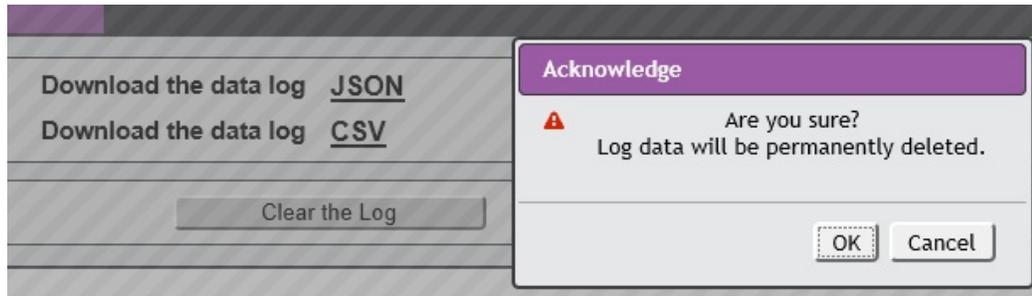

	NOTE
⚠	All previously recorded data will be deleted.

2. Confirm deletion.

Data Graph

The **Data Graph** page allows a user to display the historical data from the data log in graph format.

Figure 3-20 Data Graph


Configuring Graph:

1. Click the desired measurement to highlight it.
2. Choose the Time Range (15 minutes to 30 days).
3. Click **Display/Refresh** button to display changes.

System

Users

The Users page in the System menu allows you to manage or restrict access to the unit's features by creating accounts for different users.

Figure 3-21 User Account Page
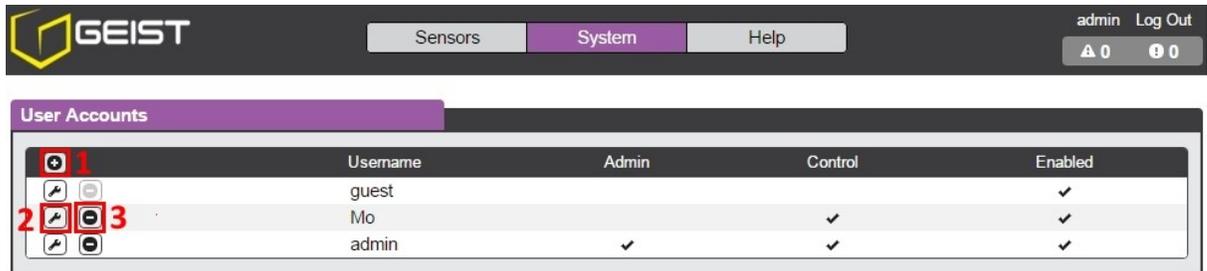
There are three buttons available on the User Accounts page:
1. Add New User Account
2. Modify User's Account
3. Delete User's Account

⚠	**NOTE**
	Only an Administrator-level account can Add, Modify, or Delete users. Control-level and View-Only accounts can change their own passwords via the Modify button, but cannot Add or Delete accounts, or Modify other accounts. The Guest account cannot Add, Delete, or Modify any account, not even itself.

To Add or Modify a user Account:

1. Click the **Add** or **Modify** User icon.

Figure 3-22 Add or Modify User Account Page
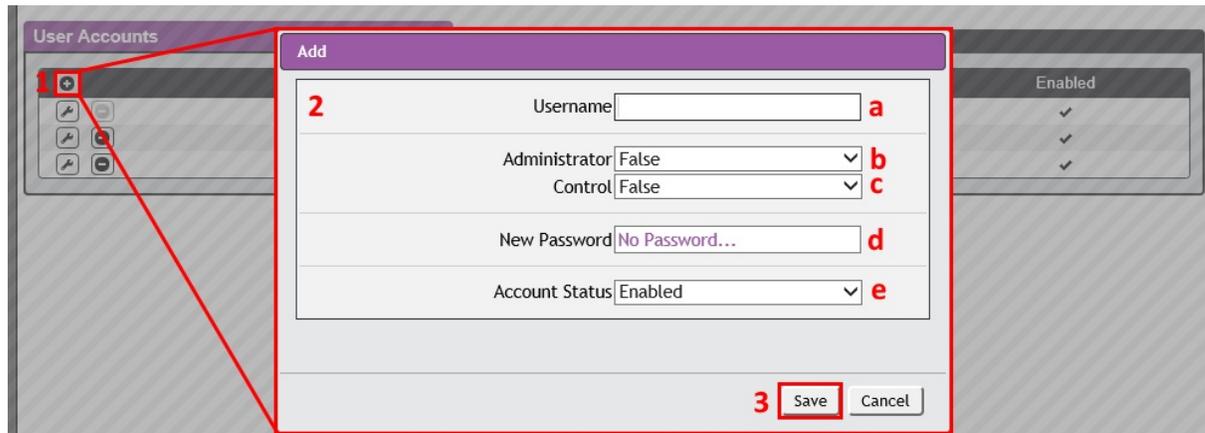
2. Create or modify the account information as follows:
   a. **Username:** the name of this account. User names may be up to 24 characters long, are case-sensitive, and may not contain spaces or any of these prohibited characters: $&`:<>[] {}"+%@/ ; =?\^|~', Note that an account's username cannot be changed after the account is created.

   b. **Administrator:** if set to True, this account has Administrator-level access to the unit, and can change any setting.

   c. **Control:** if set to True, this account has Control-level access. Setting Administrator to True will automatically set Control to True as well. Setting this to False makes the account a View-Only account.

   d. **New Password:** account passwords may be up to 24 characters long, are case-sensitive, and may not contain spaces.

   e. **Account Status:** set the account to Enabled or Disabled. Disabling an account prevents it from being used to log in, but does not delete it from the account list.

3. Click the **Save** button when finished.

Account Types:

- **Administrator**: Administrator accounts (accounts with both Administrator and Control authority set to True, as above) have full control over all available functions and settings on the device, including the ability to modify System settings and add, modify, or delete other users' accounts.

- **Control**: Control accounts (accounts with only Control set to True) have control over all settings pertaining to the device's sensors. They can add, modify, or delete Alarms & Warning Events and notification Actions, and can change the names or labels of the device and its sensors. Control accounts cannot, however, modify System settings or make changes to other users' accounts.

- **View**: If both Administrator and Control are set to False, the account is a View-Only account. The only changes a View-Only account is permitted to make are changing their own account's password, and changing the preferred language for their own account. View-Only accounts cannot change any device or system settings.

- **Guest**: Anyone who brings up the unit's web page without logging in will automatically be viewing the unit as Guest. By default, the Guest account is a View-Only account, and cannot make changes to any settings, although the Administrator can elevate the Guest account to Control-level access if desired, allowing anyone to make changes to names, labels, alarm events, and notifications without logging in. The Guest account cannot be deleted but can be disabled to require login for viewing system status.

Figure 3-23 Change User Password Page

- **Edit User**: Once a user has logged in to their account, they can change their password or language preference by clicking their username, shown next to the Log Out hyperlink at the top right-hand corner of the web page, as shown here.

Network

The unit's network configuration is set on the Network tab of the System menu. Settings pertaining to the unit's network connection are:

Figure 3-24 Network Configuration Page

- **DHCP**: Allows the unit to request a dynamic IP address from a server on the network when Enabled. The default is Disabled, or static IP addressing.

- **Gateway (IPv4)**: The IP address of the network gateway bridging your private network (LAN) to the public internet network. This is required if the unit needs to reach any services on the internet, such as a public email or NTP server. If DHCP is Enabled, this field will automatically be filled in when the DHCP service assigns the unit an IP address.

- **IP Address**: Displays the IPv4 and IPv6 addresses currently being used by the unit. Clicking on the Modify icon will allow you to change the unit's IPv4 address and Netmask. Note: If DHCP is enabled, then there will be no Modify icon, indicating that this address can't be changed by the user. The IPv6 address is a "Link Local" address inherent to the unit, and cannot be changed.

- **DNS:** Allows the unit to resolve host names for email, NTP, and SNMP servers as well as cameras.

<table>
<tr><td>

!
</td><td>

NOTE
Any changes you make to the Network settings will take effect once the Save button is clicked! If you have changed the IP address or HTTP/HTTPS ports, it will appear as if the unit is no longer responding because the browser will not be able to reload the web page. Just stop or close the browser window, then type in the new IP address into the browser's address bar, and the unit will be accessible.
</td></tr>
</table>

Web Server

The unit's Web Server configuration can be updated on the Web Server tab of the System menu.

Figure 3-25 HTTP Configuration Page

- **HTTP Interface**: Enables/disables access via HTTP. HTTPS interface will always be enabled. Available options are: Enabled or Disabled. It is not possible to disable the web interface completely.

- **HTTP/HTTPS Server Port:** Allows you to change the TCP ports which the HTTP and HTTPS services listen to for incoming connections. The defaults are port 80 for HTTP and 443 for HTTPS.

Time

The system clock is set here. The unit comes preconfigured with the Primary NTP Server pool.ntp.org time servers and is set to the Western Europe Time Zone (00:00 UTC). Should a local time server be preferred, enter its UTC offset or a local time server into the "UTC Offset" box and click the "Save" button. The unit attempts to contact the time servers during boot up and periodically while running. All log time stamps will present time as the number of seconds since the unit was powered up until a time server is contacted or the system clock is manually set.

Figure 3-26 HTTP Clock Setting

Manually Setting System Clock

1. From the **Mode**, click the drop down text box and select **Manual**.
2. Enter the **Date** and **Time** in the following format YYYY-MM-DD hh:mm:ss with time being in 2400 hours (military time).
3. Click **Save** when done.

Daylight Saving Time (DST) is supported and can be change in the Daylight Saving Time box.

Email

The unit is capable of sending email notifications to up to five email addresses when an Alarm or Warning Event occurs.

Figure 3-27 Email Configuration Page

Target email addresses can be configured as follows:

Legend of icons/buttons:
1. Add new target email address.
2. Modify existing target email address.
3. Delete existing target email address.
4. Send test email.

To send emails, the unit must be configured to access the mail server, as follows:

- **SMTP Server:** The name or IP address of a suitable SMTP or ESMTP server.

- **Port:** The TCP port which the SMTP Server uses to provide mail services. Typical values would be port 25 for an unencrypted connection, or 465 and 587 for a TLS/SSL-encrypted connection, but these may vary depending on the mail server's configuration.

- **Enable SSL:** If Enabled, the unit will attempt to connect to the server using a fully-encrypted TLS/SSL connection. Note that when this setting is enabled only fully-

encrypted sessions are supported; the "StartTLS" method, where the session starts out as unencrypted and then switches to encrypted partway through the session, is not supported. If using a service that utilizes StartTLS, such as Office365, please leave this option Disabled.

- **"From" Email Address:** The address which the unit's emails should appear to come from. Note that many hosted email services, such as Gmail, will require this to be the email account of a valid user.

- **Username** and **Password:** The login credentials for the email server. If your server does not require authentication (open relay), these can be left blank.

Microsoft Exchange servers will have to be set to allow SMTP relay from the IP address of the unit. In addition, the Exchange server will need to be set to allow "Basic Authentication", so that the unit will be able to log in with the AUTH LOGIN method of sending its login credentials. Other methods, such as AUTH PLAIN, AUTH MD5, etc. are not supported.

Figure 3-28 Email Target Configuration Page
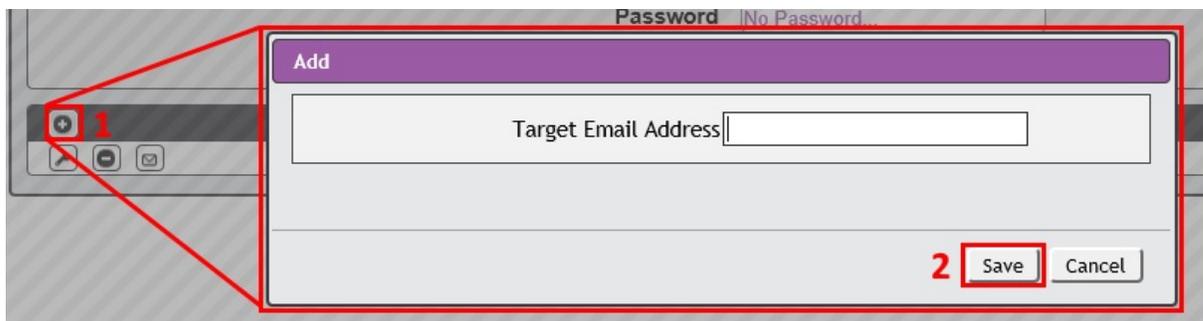
To Add or Modify a Target Email address:
1. Click on the **Add** or **Modify** icon.
2. Type email address and then click **Save**.

To Delete a Target Email address:
1. Click on the **Delete** icon next to the address you wish to delete.
2. Click the **Delete** button on the pop-up window to confirm.

To send a test email:
1. Click on the **Test Email** icon next to the address you wish to test.
2. A pop-up window will indicate that the test email is being sent. Click **OK** to dismiss the pop-up.

SNMP

Simple Network Management Protocol (SNMP) can be used to monitor the unit's measurements and status, if desired. SNMP v1, v2c and v3 are supported. In addition, alarm traps can be sent to up to two IP addresses.

Figure 3-29 SNMP Configuration Page
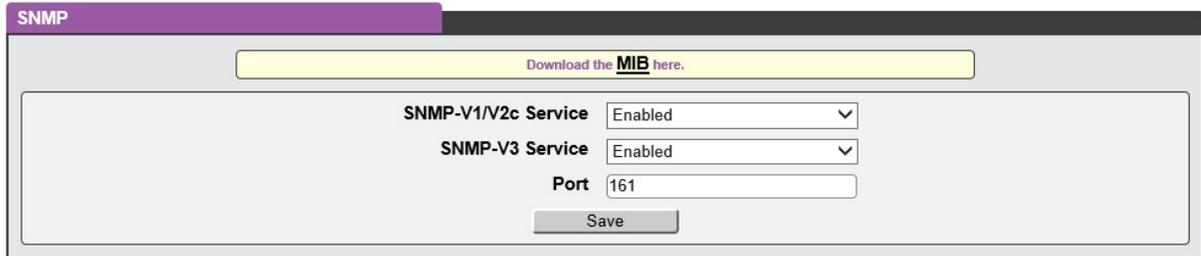
The **SNMP-V1/V2c and SNMP-V3 Service** can be enabled or disabled independently as desired. The service will normally listen for data-read requests (a.k.a. "GET requests") on **Port** 161, which is the usual default for SNMP services; this can also be changed if desired.

The Management Information Base (MIB) can be downloaded from the unit, if needed, via the MIB link at the top of the web page. Clicking this link will download a .ZIP archive containing both the MIB file itself, and a CSV-formatted spreadsheet describing the available OIDs in a human-readable form to assist you in setting up your SNMP manager to read data from the unit.

Figure 3-30 SNMP Users Configuration Page

The **Users** section allows you to configure the various Read, Write, and Trap communities for SNMP services. You can also configure the authentication types and encryption methods used for the SNMP v3 if desired. Click the Modify icon to change settings.

Figure 3-35 SNMP Traps Configuration Page

Traps allows you to define the IP addresses and SNMP types that you wish the traps to be sent to.

Figure 3-36 SNMP Traps/Types IP Configuration Page
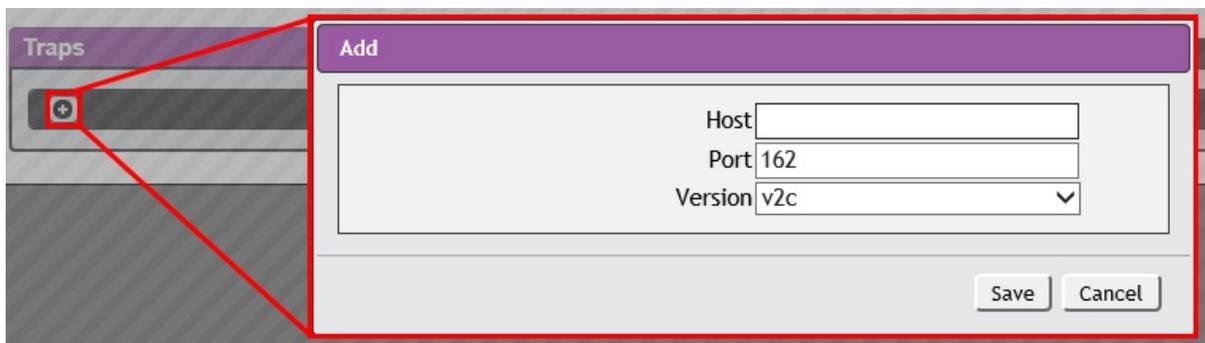
To configure a trap destination:
1. Locate the **Traps** section of the SNMP page, and click on the Add icon.
2. Enter the IP Address which the trap should be sent to in the **Host** field, change the **Port** number if required, select the trap **Version** to be used (v1, v2c, or v3), and click **Save**.

A test trap may be sent by clicking on the Test icon next to the Host IP address. Trap settings can also be updated/changed by clicking the Modify icon next to the Host IP address.

Syslog

Syslog data can be captured remotely but must first be setup and enabled via the Syslog page.

> ⚠️ **NOTE**
> This function is primarily used for diagnostic purposes, and should normally be left Disabled unless advised to enable it by Geist technical support for troubleshooting a specific issue.

Figure 3-37 Syslog Configuration Page
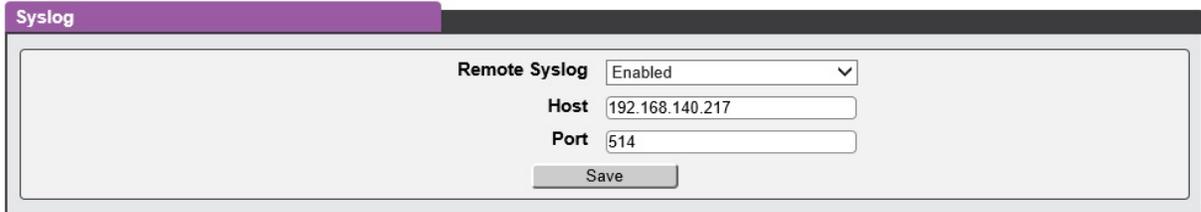
Admin

The Admin page allows the administrator of the device to save their contact information along with the device description and location. Once the info is saved by an administrator, other (non-administrator) users can view the information. Also, the System Label can be modified on this page. This label is typically shown in the title bar of the web browser's window, and/or on the browser tab(s) currently viewing the device.

> **⚠ NOTE**
>
> This information is strictly for the users' and administrator's convenience. The unit will not attempt to send emails to the "Administrator Email" address and this address cannot be chosen as the Target of an Event Action when configuring an Alarm or Warning Event.

Figure 3-38 Admin Configuration Page

Locale

The Locale page sets the default Language and Temperature Units for the device. These settings will become the default viewing options for the device, although individual users can change these options for their own accounts. The Guest account will only be able to view the device with the options set here.

Figure 3-39 Locale Configuration Page
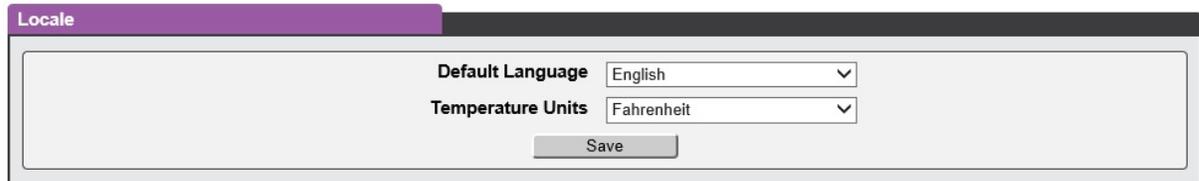
Locale	
Default Language	English
Temperature Units	Fahrenheit
	Save

Utilities

The Utilities page in the System menu provides the ability to restore defaults, reboot the communication system and perform firmware updates.

The Restore Defaults section allows the user to restore the unit's settings to the factory defaults. There are two options:

All Settings: erases all of the unit's settings, including all Network and User Accounts settings, effectively reverting the entire unit back to its original out-of-the-box state.

All Non-Network Settings: erases all settings except the Network and User Accounts.

Figure 3-40 Restore Default Page
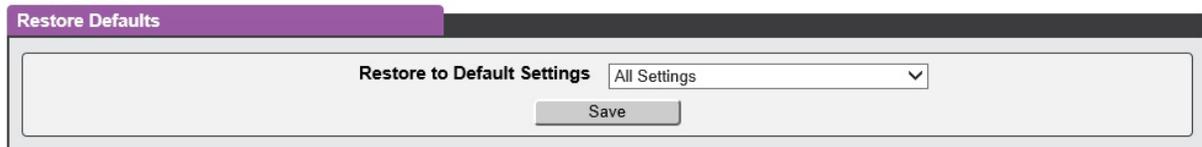
Restore Defaults	
Restore to Default Settings	All Settings
	Save

The Reboot section allows the user to perform a system reboot. This function will not affect power delivery to connected equipment.

Figure 3-41 Reboot Page
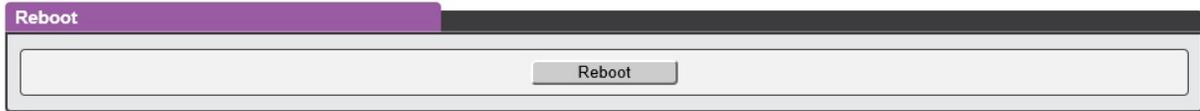
Use the Firmware Update section to load firmware updates into the unit. Firmware updates, when available, can be found on the Geist website: http://www.geistglobal.com/support/firmware.

You can also subscribe to a mailing list, to be notified of when firmware updates become available.

Figure 3-42 Firmware Update Page
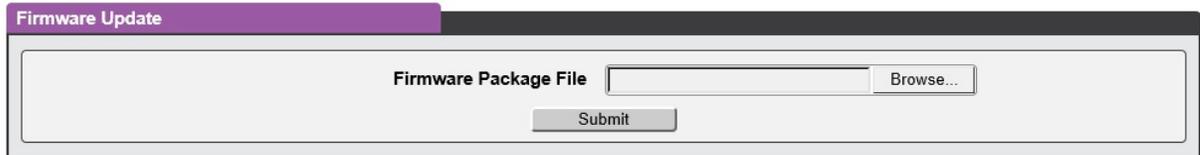
Firmware updates will typically come in a .ZIP archive file containing several files including the firmware package itself, a copy of the SNMP MIB, a "readme" text file explaining how to install the firmware, and various other support files as needed. Be sure to un-ZIP the archive and follow the included instructions.

Help

Info

The Info Page displays the unit's current configuration information, including the device name and ID, the unit's current firmware versions, and network information. Manufacturer support information is also here.

Figure 3-43 Info Page

Info	
Device Name	Watchdog 100
Serial Number	TB16091041
Model Number	WATCHDOG 100-NPS (GBB100)
Part Number	G1609
Device Type	BB-REL-THA4
Version	3.3.2
GUI Version	1.3.0
MAC Address	D8:80:39:82:94:05
Hostname	BBD88039829405
Manufacturer	Geist
Manufacturer Site	www.geistglobal.com
Support Site	www.geistglobal.com/support
Support Email	support@geistglobal.com
Support Telephone	1-800-432-3219 | +1 402 474 3400

Support Site

Technical support can be found at http://www.geistglobal.com/support

Americas
- 1 888 630 4445

Europe and Middle East
- From within the UK 0845 026 3853
- From abroad +44 845 026 3853

Asia
- English +1 888 630 4445 (US number)
- Chinese +86 755 8663 9505

Chapter 4 - Final Checkout

Final Checkout

Technical Support

Service and Maintenance

No service or maintenance is required. Do not attempt to open the Watchdog 100 or you may void the warranty. There are no serviceable parts inside the Watchdog 100.

More Technical Support

http://geistglobal.com

Americas

- 1 888 630 4445

Europe and Middle East

- From within the UK 0845 026 3853
- From abroad +44 845 026 3853

Asia

- English +1 888 630 4445 (US number)
- Chinese +86 755 8663 9505

Email: support@geistglobal.com or contact your distributor
Technical Support Form: http://www.geistglobal.com/Tech-Support

Using Microsoft Exchange as an SMTP server

If your facility uses a Microsoft Exchange email server, it can be used by the Watchdog 100 to send Alarm and Warning notification emails if desired. However, the Exchange server may need to be configured to allow SMTP connections from the unit first, as later version of Exchange often have SMTP services or basic authentication disabled by default. If you encounter difficulties in getting your Watchdog 100 to send emails through your Exchange server, the following notes may be helpful in resolving the problem.

⚠️ **NOTE**
These suggestions only apply if you are using your own, physical Exchange server! Microsoft's hosted "Office365" service is not compatible with the Watchdog 100 using firmware versions prior to v3.0.0, as Office365 requires a StartTLS connection. Firmware versions 3.0.0 and beyond have support for StartTLS and are compatible with Office365.

First, since the Watchdog 100 cannot use IMAP or Microsoft's proprietary MAPI/RPC Exchange/Outlook protocols to send messages, you will need to enable SMTP by setting up an "SMTP Send Connector" in the Exchange server. More information on setting up an SMTP Send Connector in Exchange can be found at this Microsoft TechNet article: **http://technet.microsoft.com/en-us/library/aa997285.aspx**

Next: Your Exchange server may also need to be configured to allow messages to be "relayed" from the monitoring unit. Typically, this will involve turning on the "**Reroute incoming SMTP mail**" option in the Exchange server's **Routing** properties, then adding the Watchdog 100's IP address as a domain which is permitted to relay mail through the Exchange server. More information about enabling and configuring SMTP relaying in Exchange can be found at this Microsoft TechNet article: **http://technet.microsoft.com/en-us/library/dd277329.aspx**

The SMTP "AUTH PLAIN" and "AUTH LOGIN" authentication methods (also known as "Basic Authentication) for logging in to the server are often no longer enabled by default in Exchange; only Microsoft's proprietary NTLM authentication method is enabled. The AUTH LOGIN method which the Watchdog 100 requires can be re-enabled as follows:
1. In the Exchange console under **server configuration**, select **hub transport**.
2. Right-click the client server, and select *properties* .
3. Select the **authentication** tab.
4. Check the **Basic Authentication** checkbox.
5. Uncheck the **Offer Basic only after TLS** checkbox
6. Apply or save these changes, and exit. Note that you may need to restart the Exchange service after making these changes.

Finally, once you have enabled SMTP, relaying, and the AUTH LOGIN Basic Authentication method, you may also need to create a user account specifically for the Watchdog 100 to log into. If you have already created an account prior to enabling the SMTP Send Connector, or you are trying to use an already-existing account created for another user, and the Watchdog 100 still cannot seem to connect to the Exchange server, the account probably did not properly inherit the new permissions when you enabled them as above. This tends to happen more often on Exchange servers that have been upgraded since the account(s) you are trying to use were first created, but can sometimes happen with accounts when new connectors and plug-ins are added regardless of the Exchange version. Delete the

user account, then create a new one for the monitoring unit to use, and the new account should inherit the SMTP authentication and mail-relaying permissions correctly.

If none of the above suggestions succeed in allowing your Geist Watchdog 100 to send mail through your Exchange server, then you may need to contact Microsoft's technical support for further assistance in configuring your Exchange server to allow SMTP emails to be sent from a 3rd-party, non-Windows device through your network.

Product-Specific Safety Notices

The specific procedural safety precautions relating to this product are stated below.

General Safety

Safety is a serious matter and all precautions should to taken to guarantee a safe work and operational environment. General safety precautions must be observed during all aspects of operation, service, and repair of equipment described in this document. Failure to comply with the safety warnings, procedures and guidelines as presented in this document is in violation of the safety standards of design, manufacture, and intended use of this equipment.

You are responsible for following the safety guidelines and warnings presented in this document for this equipment. Individuals using or maintaining Geist product(s) are expected to follow all the noted warnings and safety precautions necessary for safe operation of the equipment in your environment. Geist assumes no liability for failure to comply with these requirements.

Live Circuits Safety

> ⚠️ **DANGER**
>
> HAZARDOUS VOLTAGE, CURRENT, AND ENERGY LEVELS ARE PRESENT IN THIS PRODUCT. POWER SWITCHED CIRCUITS CAN HAVE HAZARDOUS VOLTAGES PRESENT EVEN WHEN THE SWITCH IS IN THE OFF POSITION. DO NOT OPERATE THE PRODUCT WITH ANY COVER PLATE REMOVED. ALWAYS MAKE SURE THAT PRODUCT IS FULLY ENCLOSED PRIOR TO USE.

Operating personnel must:

- Not remove equipment covers. Only Geist Authorized Service Personnel or other qualified maintenance personnel may remove equipment covers for internal sub-assembly, or component replacement, or any internal adjustment.
- Not replace any equipment component with power applied to the line cord. Under certain conditions, dangerous voltages may exist even with the input power cable disconnected. Any exceptions for 'Hot-Swap' modules will be specifically noted in this product document.
- Always disconnect input power and discharge circuits before touching any sub-assembly of circuit component.

Equipment Grounding

To minimize shock hazard, the equipment chassis and enclosure must be connected to an electrical earth ground. The input power cable must be either plugged into an industry electrical code compatible receptacle or wired directly into an electrical code compatible interface. The equipment earth ground wire (typically green) must be firmly connected to the facility electrical safety ground. The mating electrical interface to this equipment must comply with International Electromechanical Commission (IEC) standards.

Electrostatic Discharge

Geist strongly recommends that an anti-static precautions be taken when installing, removing, or working on and around static sensitivity equipment. Industry approved anti-static devices such as wrist and heel straps, in conjunction with conductive foam pads, should be available and implemented only after verifying that they are in good working condition.

Electronic components such as memory modules, circuit boards, and LED displays, are sensitivity to Electro-Static Discharge (ESD). Handling of such components should be done only after proper anti-static workspace conditions have been established. Any static producing packing materials such as plastic, Styrofoam, and some cardboards, should be removed and discarded in a timely manner.

Explosive Environment

Do not operate this equipment in the presence of flammable gases or fumes. Operation of any electrical equipment in such an environment constitutes a definite safety hazard.

Servicing and Adjustments

Do not attempt to service this equipment, there are no field serviceable parts or sub-assemblies. Any adjustments should be made by authorized service personnel only.

Repairs and Modifications

Because of the danger of electrocution and/or severe health hazard, do not install substitute parts or preform any unauthorized modifications of this equipment. It is best to contact Geist for Warranty and Repair Service to ensure that safety features are maintained.

GEIST MONITOR

Thank You For Purchasing Geist