Instruction Manual
Environment Monitor with Optional PoE

Watchdog 15
Firmware v3

Geist 1821 Yolande Ave., Lincoln, NE 68521
800.432.3219 | 402.474.3400 | geistglobal.com

Table of Contents

Specifications

Overview

The Watchdog 15 is a self-contained environment monitor with an onboard temperature/humidity sensor. Equipped with two digital sensor ports, the Watchdog 15 can support up to four external sensors using a splitter. The Watchdog 15 can be optionally configured at the factory to support Power-Over-Ethernet (PoE).

All onboard and external sensors are measured every 5 seconds. Sensor data collected by Watchdog 15 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.

Onboard Sensors

Watchdog 15 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.

Remote Sensors

Available 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.

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 15.

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.

Note: Sensors use Cat. 3 wire and RJ12 connectors. Wiring must be straight-through: reverse polarity will temporarily disable all sensors until corrected.

Note: 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.

Environmental

Temperature

Operating:	-25 °C (-4°F) min	80 °C (176 °F) max
Storage:	-40 °C (-40°F) min	80 °C (176 °F) max

Humidity

Operating:	5% min 95% max	(non-condensing)
Storage:	5% min 95% max	(non-condensing)

Elevation

Operating:	0 m (0 ft.) min	2000 m (6561 ft.) max
Storage:	0 m (0 ft.) min	15240 m (50000 ft.) max

Electrical

6-18 Volts DC, 2 Amps
Power-Over-Ethernet (PoE) Enabled (Class 0)

Networking

Protocols

HTTP, HTTPS (TLS v1.2), SMTP/POP3, ICMP, DHCP, TCP/IP, NTP, Syslog, SNMP (v1/2c/3)

Ethernet Link Speed

10/100 Mbps; full duplex

User Interfaces

HTML, SNMP, CSV/Plain Text, JSON API

EMC Verification

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.

Installation

Guidelines

- If the Watchdog 15 is installed in a cabinet the ambient temperature of the rack should be no greater than 80 °C.
- Install the Watchdog 15 such that the amount of airflow required for safe operation of equipment is not compromised.
- Mount the Watchdog 15 so that a hazardous condition is not achieved due to uneven mechanical loading.

Network Overview

This product comes preconfigured with a default IP address set. Simply connect to the Environmental Monitoring Unit and access the web page with your browser.

Default IP Address

The Watchdog 15 has a default IP address for initial setup and access to the unit if the assigned address is lost or forgotten. Once an IP address is assigned to a unit, the default IP address is no longer active. To restore the default IP address, press the reset button located beside the network connector and hold for approximately 20 seconds. Both the idle and activity lights near the network connector will both light up when the IP address has been reset.

Note: Pressing the reset button will restore the default IP address and will also clear all password settings.

The Configuration page allows you to assign the network properties or use DHCP to connect to your network. Access to the unit requires the IP address to be known, so use of a Static IP or reserved DHCP is recommended. The default address is shown on the front of the unit:

- **IP Address:** 192.168.123.123
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.123.1

Initial Setup

Connect the Watchdog 15 to your computer using an Ethernet cable. The Watchdog 15 support IPv6 address via NDP but it does not support static or DHCPv6 IPv6 addressing.

Windows

Navigate to the Local Area Network Adapter Connections Properties and change the Internet Protocol Version 4 (TCP/IPv4) Properties. Select “Use the following IP address”. Use these settings:

- **IP Address:** 192.168.123.1
- **Subnet Mask:** 255.255.255.0
- **Gateway:** Leave blank

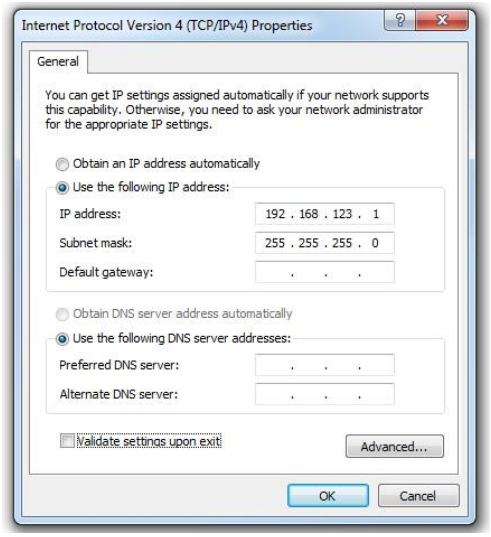

Figure 1: Network settings for initial setup. Images varies depending on Windows versions.

Save changes. The unit should now be accessible in a web browser via the unit's permanent IP address: http://192.168.123.123/.

OS X

Open System Preferences via the Dock or the Apple menu.

Select "Network" under "Internet and Network."

Select "Ethernet" from the list on the left side of the window and enter these settings on the right side of the window:

- **Configure:** Manually
- **IP Address:** 192.168.123.1
- **Subnet Mask:** 255.255.255.0
- **Router:** Leave blank

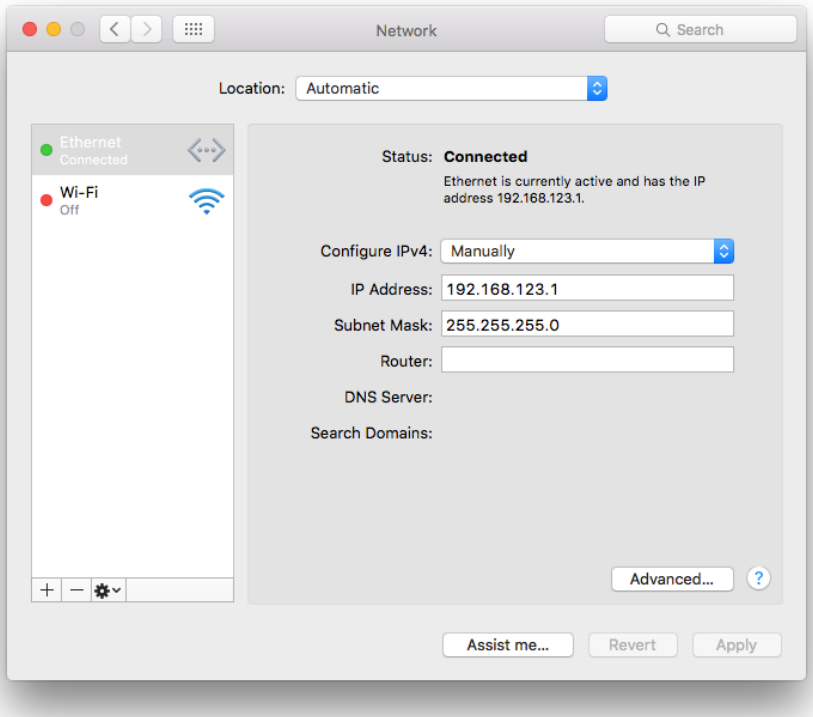

Figure 2: OS X network settings for initial setup. Image varies depending on OS X versions.

Apply changes.

The unit should now be accessible in a web browser via the unit's permanent IP address: http://192.168.123.123/.

Web Interface

General

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 Overview Page

The front page, *Overview*, gives a real time view 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.

The menu bar allows access to the rest of the Environment Monitor's functionality.

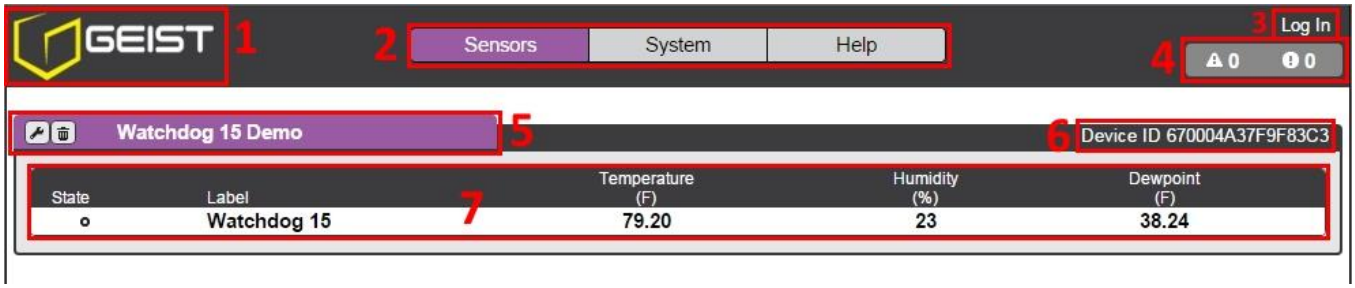

Figure 3: Overview Page – Sensor and I/O Data

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*", and "*Logging.*" (Refer to the appropriate section for more details).
  - **System:** Available options are "*Users*", "*Network", "Email", "SNMP", "Syslog", "Admin", "Time", "Locale", "Restore Defaults", and "Firmware Update."* (Refer to the appropriate section for more details).
  - Help: Available options are "*Info*" and "*Support Site*" (Refer to the appropriate section for more details).

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. Mouse over to read description.

5. Device Label

- Displays the user-assigned label of this unit (see "*Device Labeling and Temperature Offset"*).

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 device.

Overview Page Configuration

Note that you must log in before making any changes. Only users with Control or Admin level have access to these settings.

Device Labeling and Temperature Offset

The device label and temperature offset can be change on the "*Overview*" page.

1. Click the Configuration icon and change the device's temperature offset and ***Label*** as needed. (***Name*** is the factory name or model, and cannot be changed.)
2. Once done, click ***Save***.

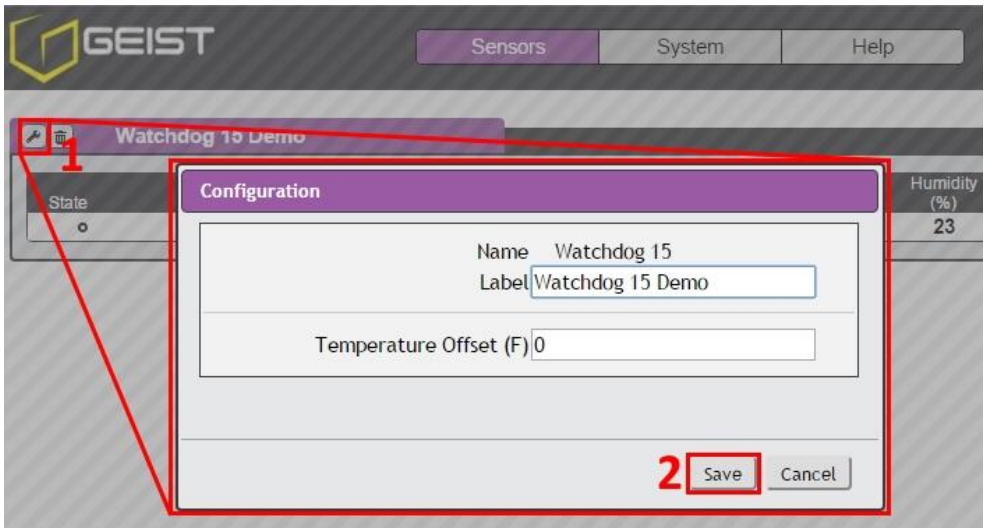

Figure 4: Device Label Configuration Dialog

Deleting

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.

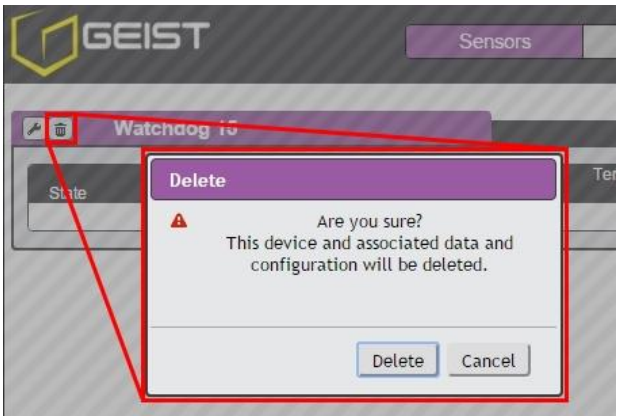

Figure 5: Device Data Delete Dialog

Alarms and Warning Page

The *Alarms and Warnings Page* allows the user to establish alarm conditions for each sensor reading. Alarm conditions can be established with either high or low trip thresholds. The alarms are displayed in different sections based on the sensor the alarm is associated with. Alarm options include relays, Email and SNMP traps.

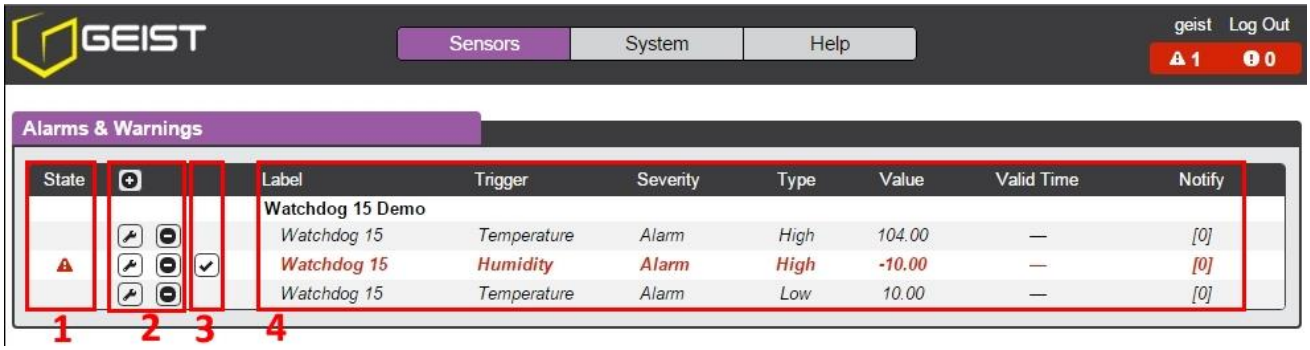

Figure 6: Alarms and Warnings Page

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 will indicate 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 and Warnings.**
   - ⊕ - Add new Alarms and Warnings.
   - 🔧 - Modify existing Alarms and Warnings.
   - ⊖ - Delete Existing Alarms and 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 that clicking this symbol does not clear the Warning or Alarm Event, it just stops the notifications from repeating.)

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

Add/Modify Alarms and Warnings

To add a new Alarm or Warning Event:

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

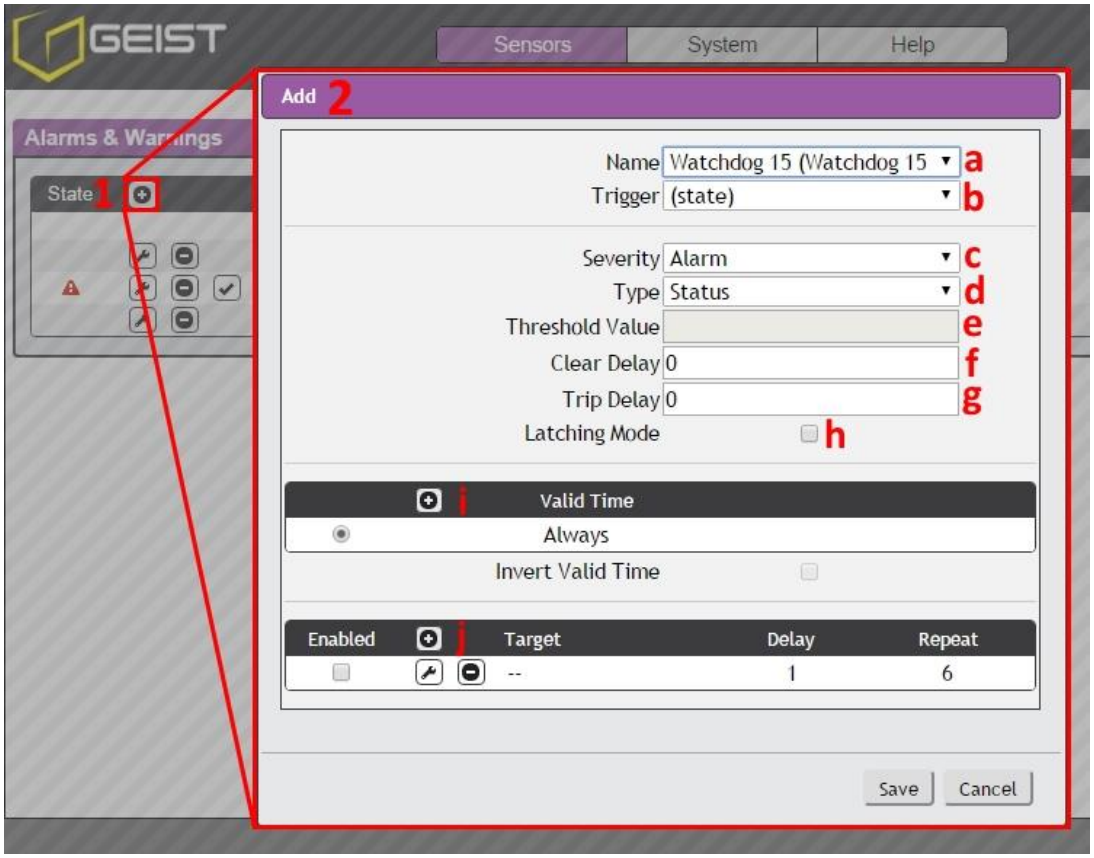

Figure 7: Add Alarm Dialog

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, or Dew point) 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 remain active until the event is acknowledged, even if the measurement subsequently returns to normal.

i. To set ***Valid Time*** for the alarms or warnings condition, click the Add icon. Select the desired days and time ranges.

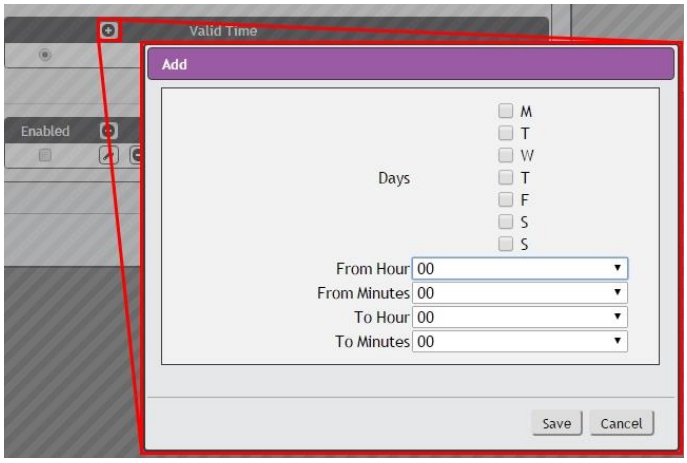

Figure 8: Add Valid Time Dialog

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:

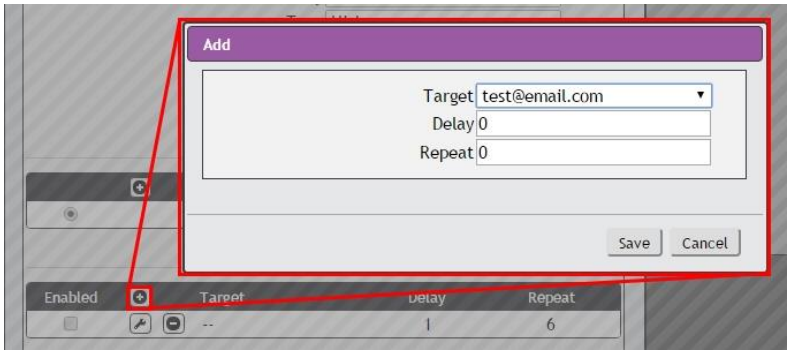

Figure 9: Add Target Dialog

- ***Target*** is the Email address or SNMP manager to which notifications should be sent when the event is tripped.
  Note: that **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 screenshot below for example.

Figure 10: Multiple Target Delays and Repeats

- ***Delay*** determines how long this Event must remain tripped for before this Action's first notification is sent. (Note that this is different from the *Trip Delay* above. *Trip Delay* determines how long the threshold value has to be exceeded before the event itself is tripped; this delay determines how long the Event must remain 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.

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.

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 change an existing notification action, click the Modify icon next to the action you wish to change, then modify its settings as above.

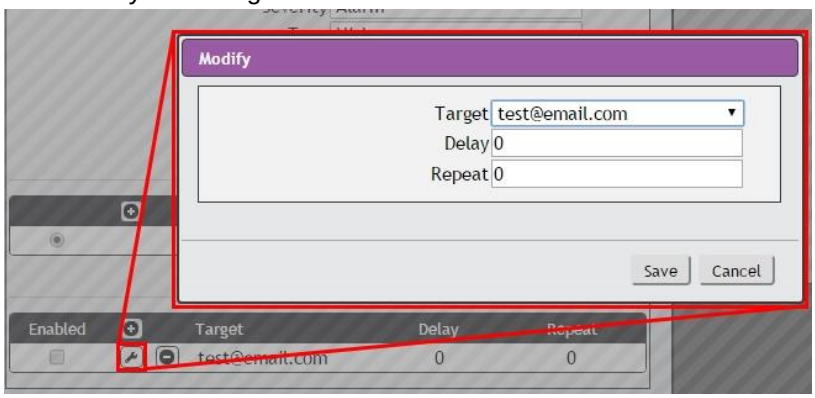

Figure 11: Modify Target Dialog

To remove a notification Action entirely, click the Delete icon to remove the action from the list, then click ***Delete*** to confirm.

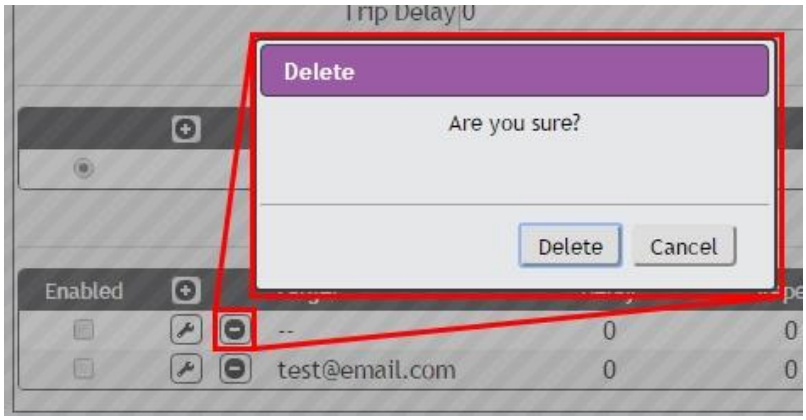

Figure 12: Delete Target Dialog

When finished, click ***Save*** to save this Alarm or Warning event.

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 its settings as above.

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.

Cameras Page

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:** 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. **Note:** Some cameras require additional software downloads to display live video in a web browser.

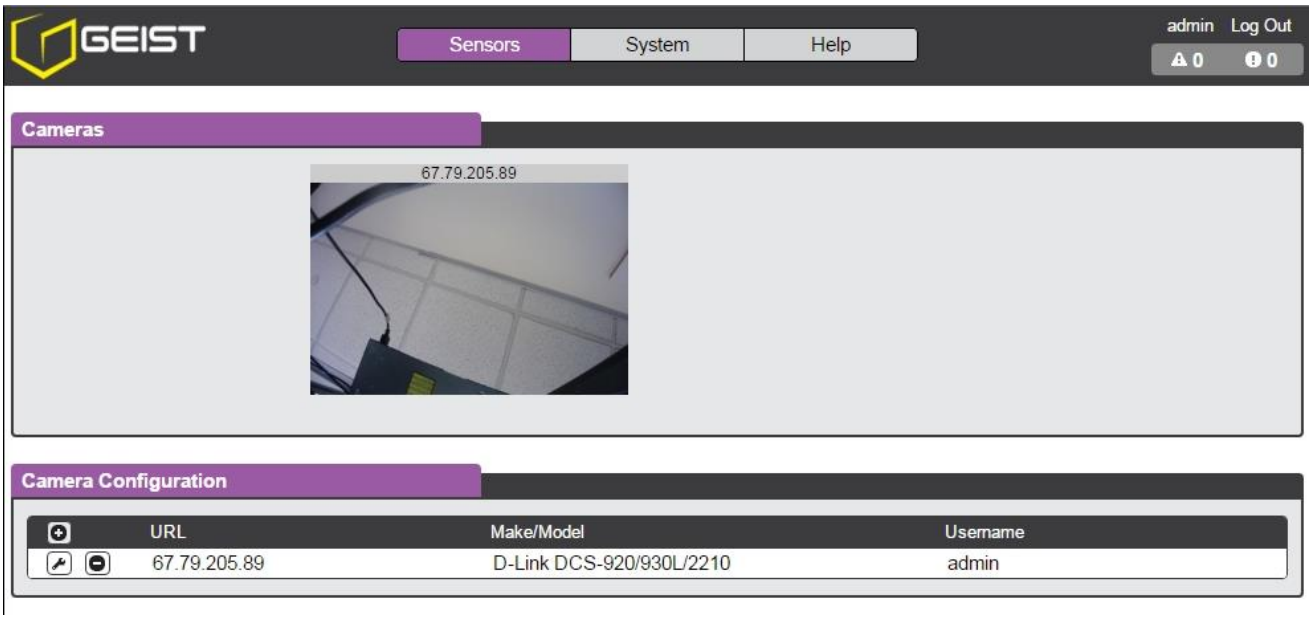

Figure 13: Cameras Page

Camera Page Configuration

Adding a Camera

1. Click the Add icon.
2. Enter in the requested information.
3. Click Save when finished.

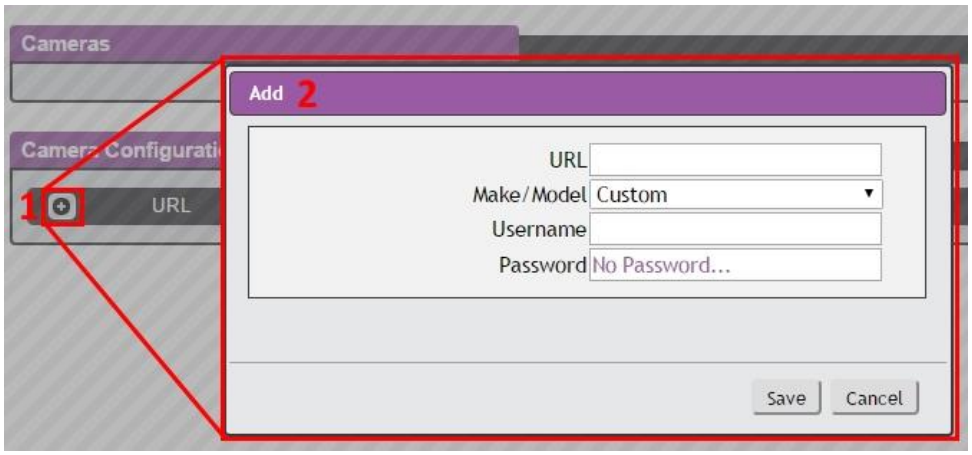

Figure 14: Add Camera Dialog

Modifying a Camera

1. Click the Modify icon.
2. Make the changes.
3. Click ***Save*** when finished.

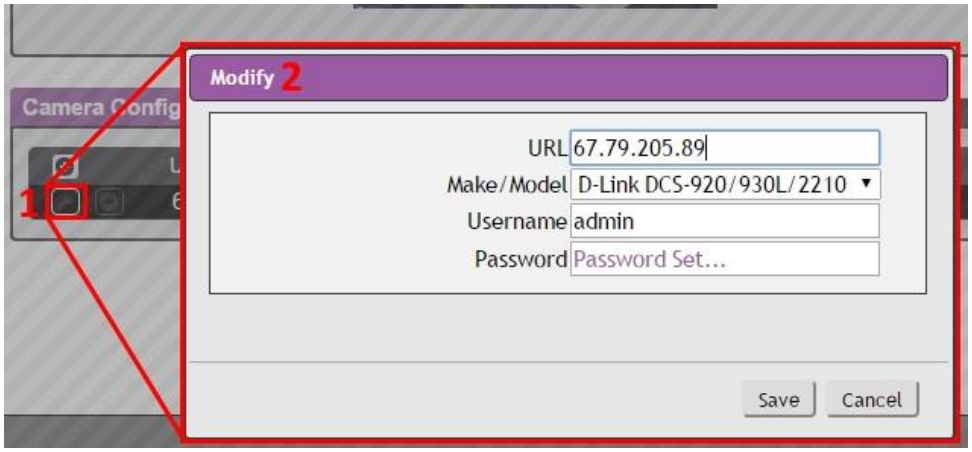

Figure 15: Modify Camera Dialog

Deleting a Camera

1. Click the Delete icon.
2. Confirm the prompt.

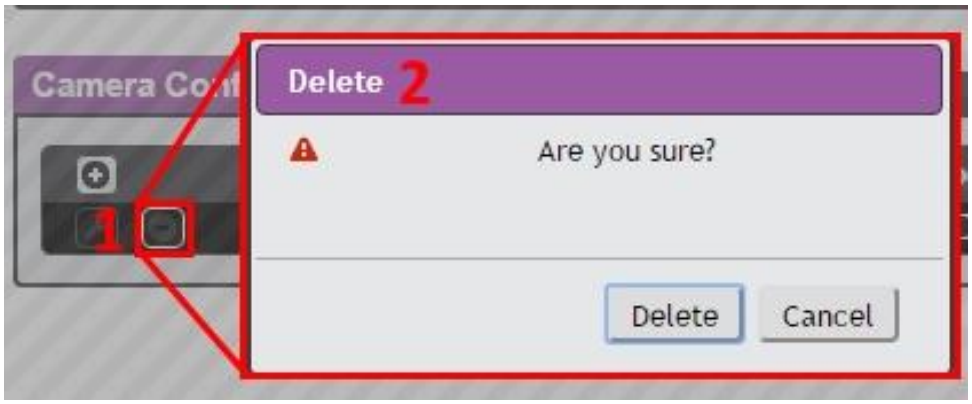

Figure 16: Delete Camera Dialog

Logging Page

The *Logging Page* allows the user to access the historical data recorded by the unit. Selected sensor values are logged into the data file at a rate of one point per minute. Please note that although data is logged once per minute, all sensor data used in the real time display and alarm functions is read at least once every 5 seconds for internal and external sensors. The graphed data is color coded for quicker identification. Recorded data is available for download in Comma-Separated Values (CSV) or JavaScript Object Notation (JSON) file types.

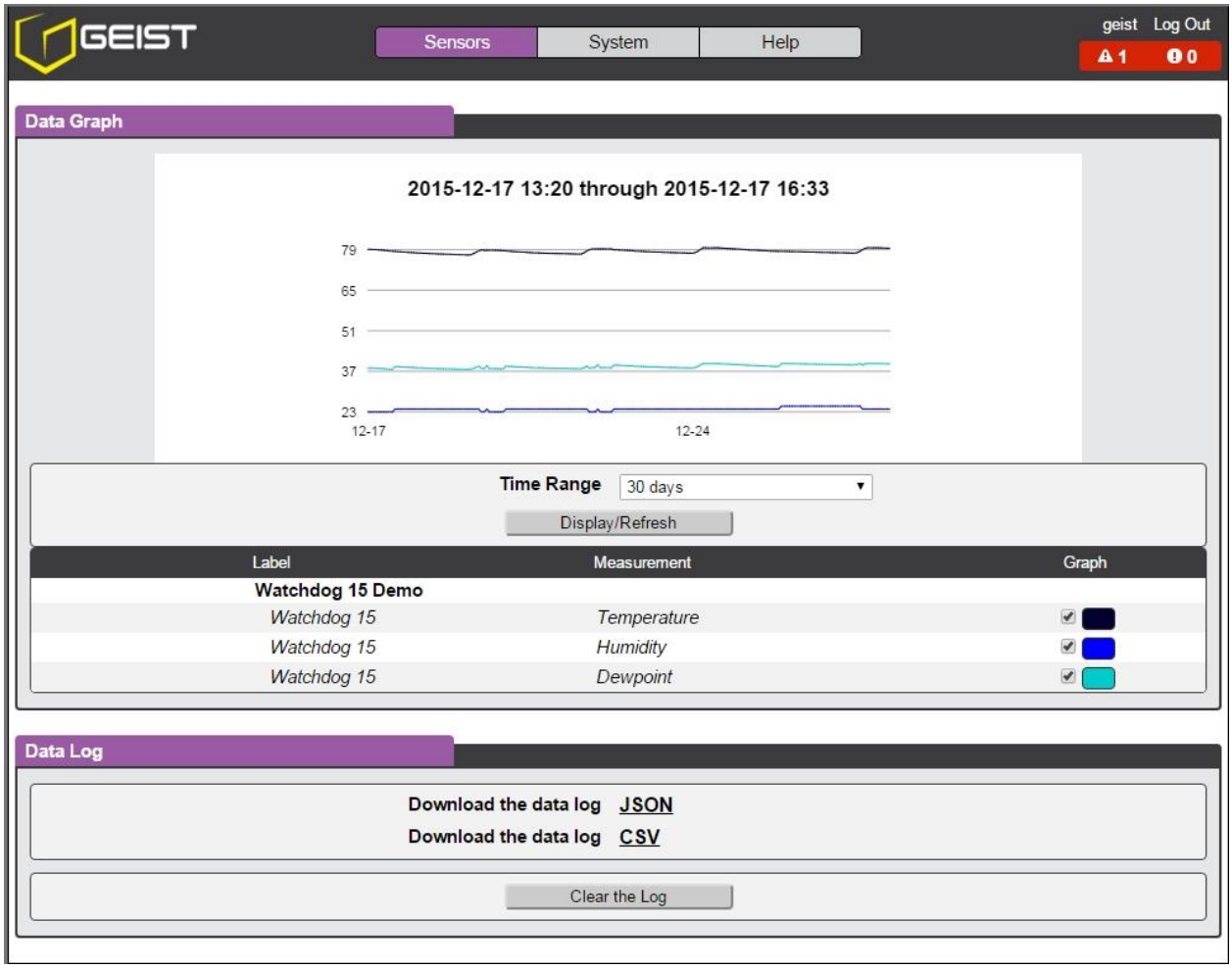

Figure 17: Logging Page

Logging Page Configuration

Adding Graph

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

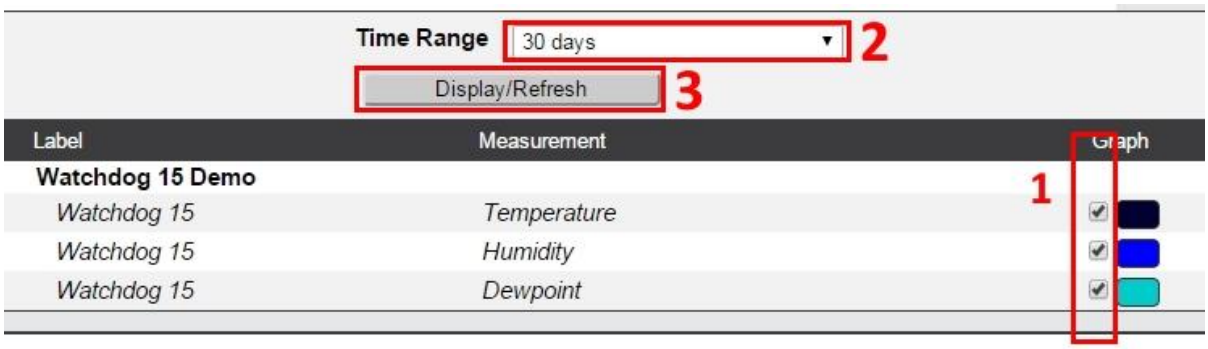

Figure 18: Add Data Graph

Download Data Log

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

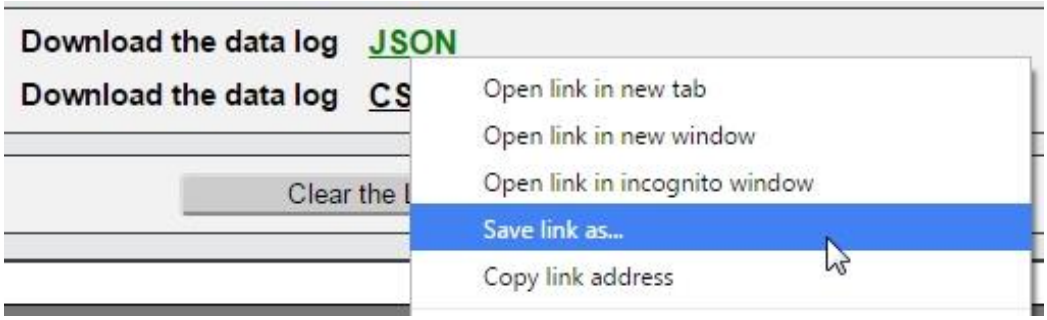

Figure 19: Download Data

Clear Data Log

1. Click Clear the Log button. Note: all previously recorded data will be deleted.
2. Confirm deletion.

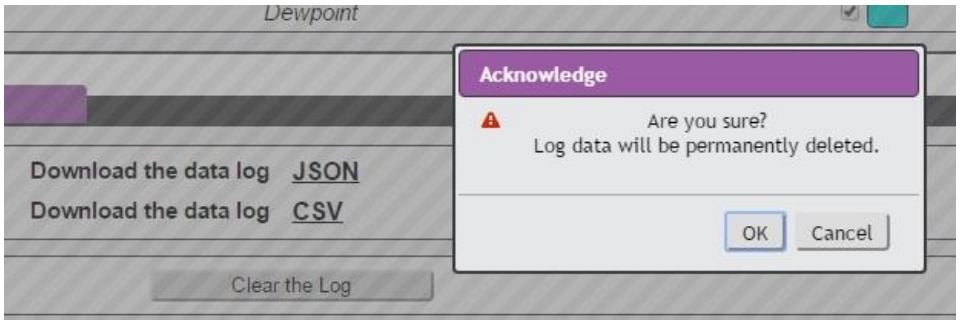

Figure 20: Clear Data

System User Accounts Page

The *User Accounts Page* allows you to manage or restrict access to the unit's features by creating accounts for different users.

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

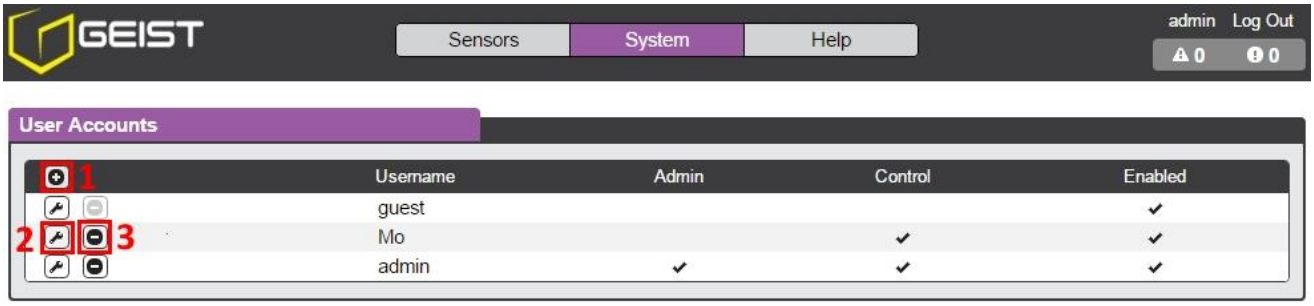

Figure 21: System User Accounts Page

Note that 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, Delete, or Modify other accounts. The Guest account cannot Add, Delete, or Modify any account, not even itself.

To Add or Modify a User's Account

1. Click the Add or Modify User icon.

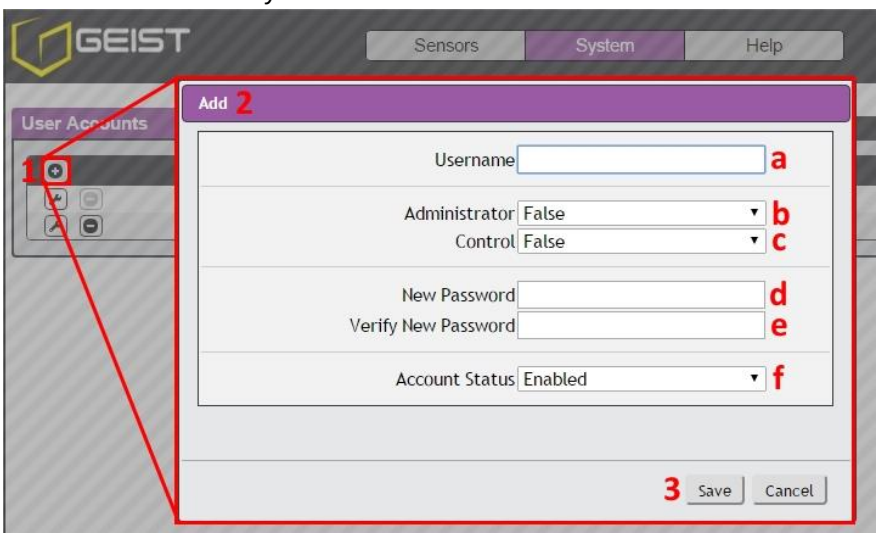

Figure 22: Add User Accounts Dialog

2. Create or modify the account information as follows:
   a. **Username:** The name of this account. Usernames may be up to 24 characters long, are case-sensitive, and may not contain spaces or any of these prohibited characters:
   $ & ' : < > [ ] { } " + % @ / ; = ? \ ^ | ~ ' ,
   Note that 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. **Verify New Password:** retype the account password from (d), above. Both fields must match for the password to be accepted.
f. **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 and 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.

Note: 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:

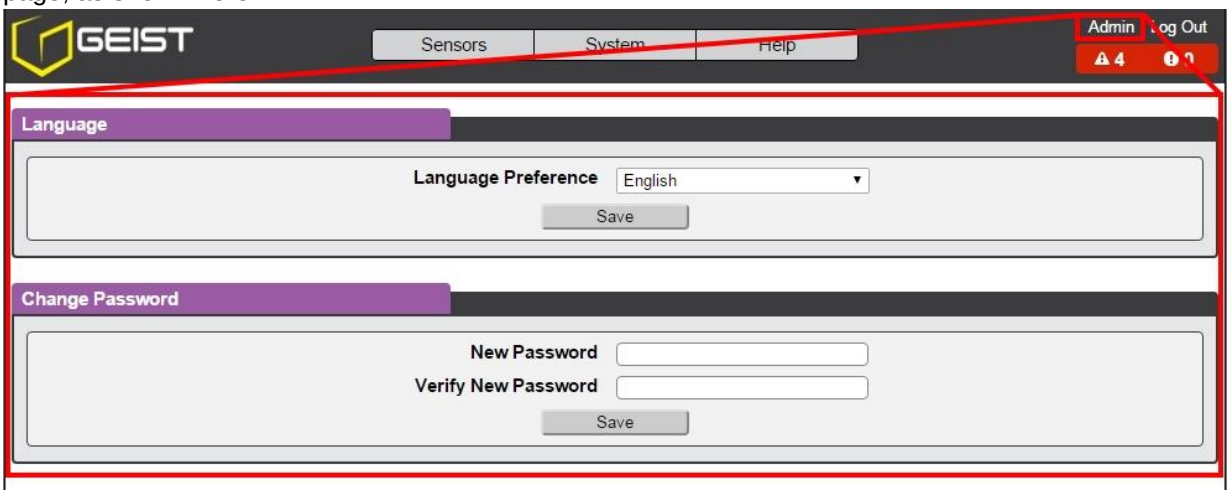

Figure 23: Language and Password Update Page

Network Page

The unit's network configuration is set here. Settings pertaining to the unit's network connection are:

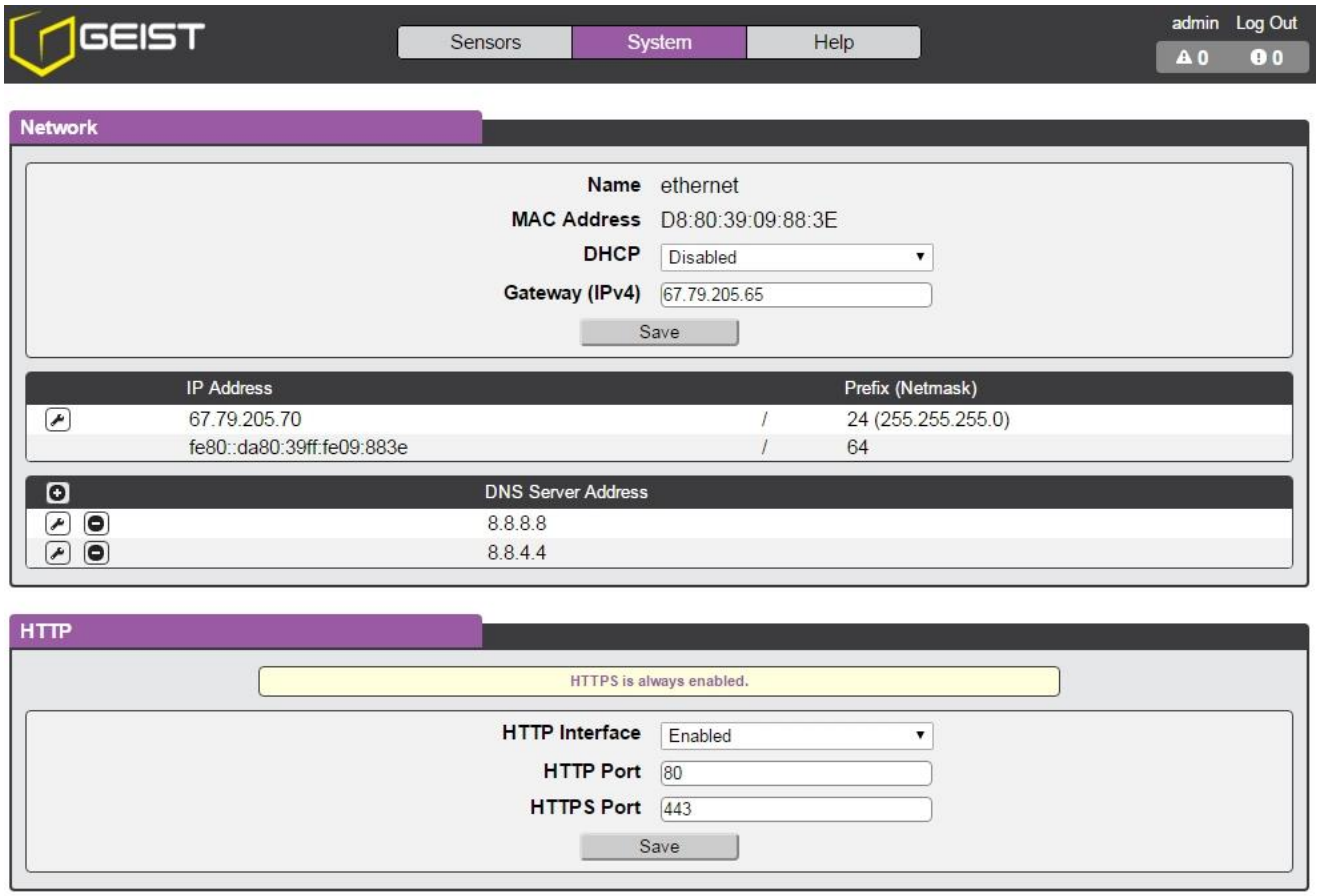

Figure 24: Network Page

- ***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 that 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.
- **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. Note that any changes you make to the Network settings will take effect instantly 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.

Email Page

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

Figure 25: Email Page

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 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.
- ***"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.)

Configure Target Email

Target Email addresses can be configured as follows:

Figure 26: Configuration Target Email Info

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 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 Page

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 up to two IP addresses.

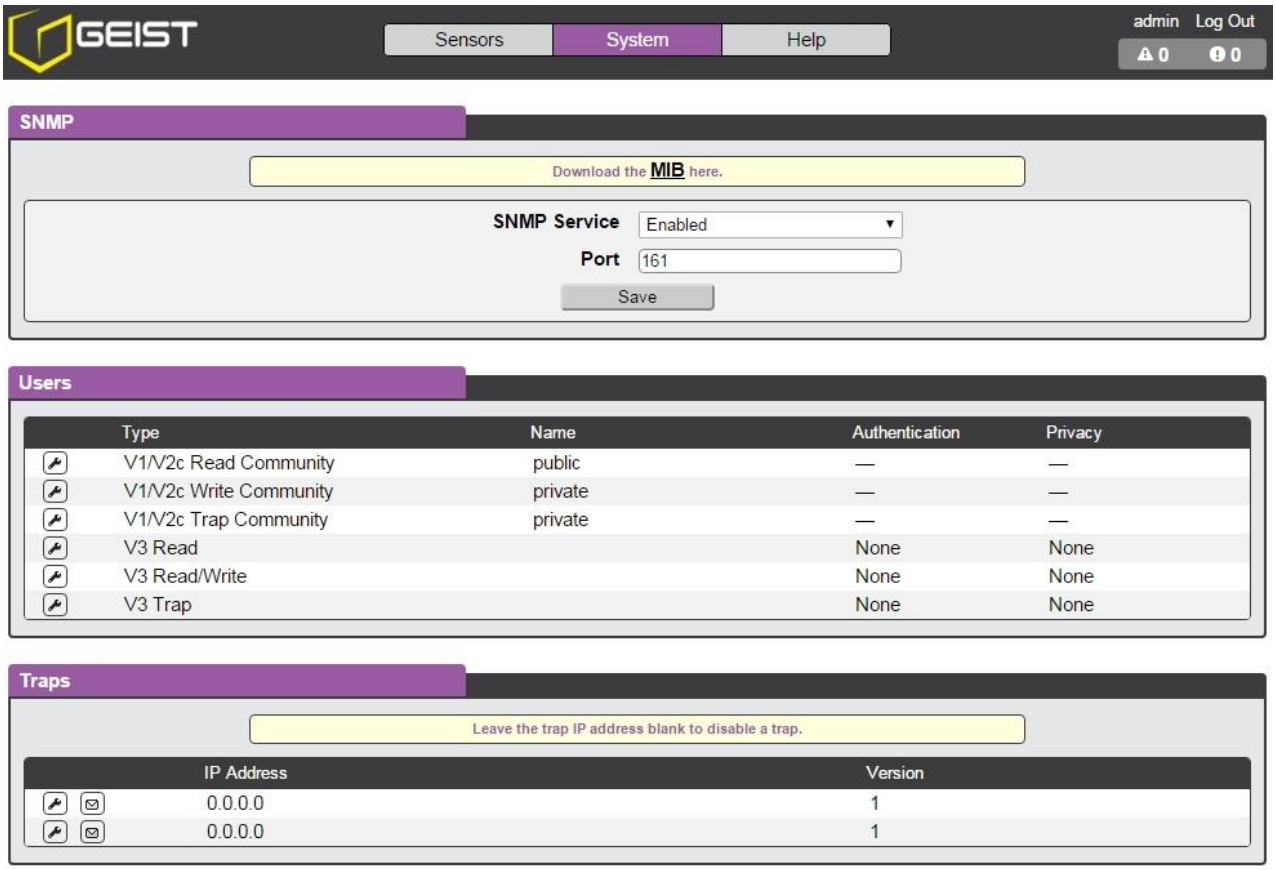

Figure 27: SNMP Page

SNMP Configuration

The ***SNMP Service*** can be enabled or disabled 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 The MIB can be downloaded use with SNMP monitoring tools. Clicking the **MIB** 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 28: SNMP Configuration Section

SNMP Users Configuration

The ***Users*** section allows you to configure the various V1/V2c Read, Write, and Trap communities' name (no spaces allow) for SNMP services by clicking on the Configuration icon . You can also configure the authentication types and encryption methods used for the SNMP v3 if desired.

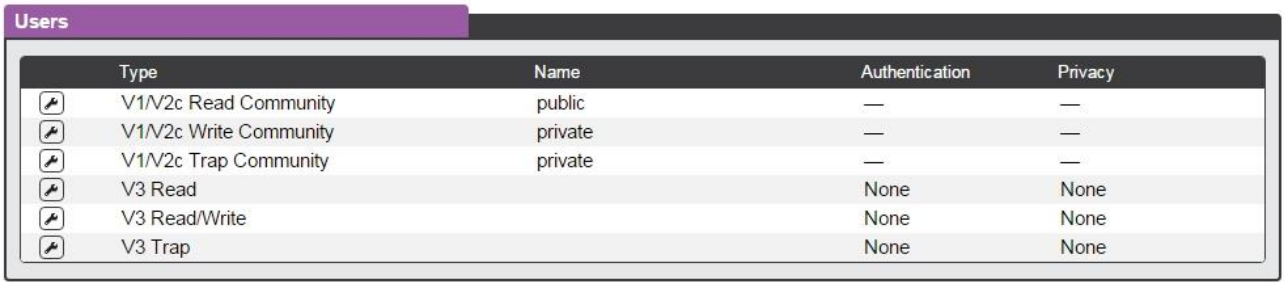

Figure 29: Users SNMP Configuration Section

SNMP Traps Configuration

Traps allows you to define the IP addresses and SNMP types that you wish the traps to be sent to.
To configure a trap destination:

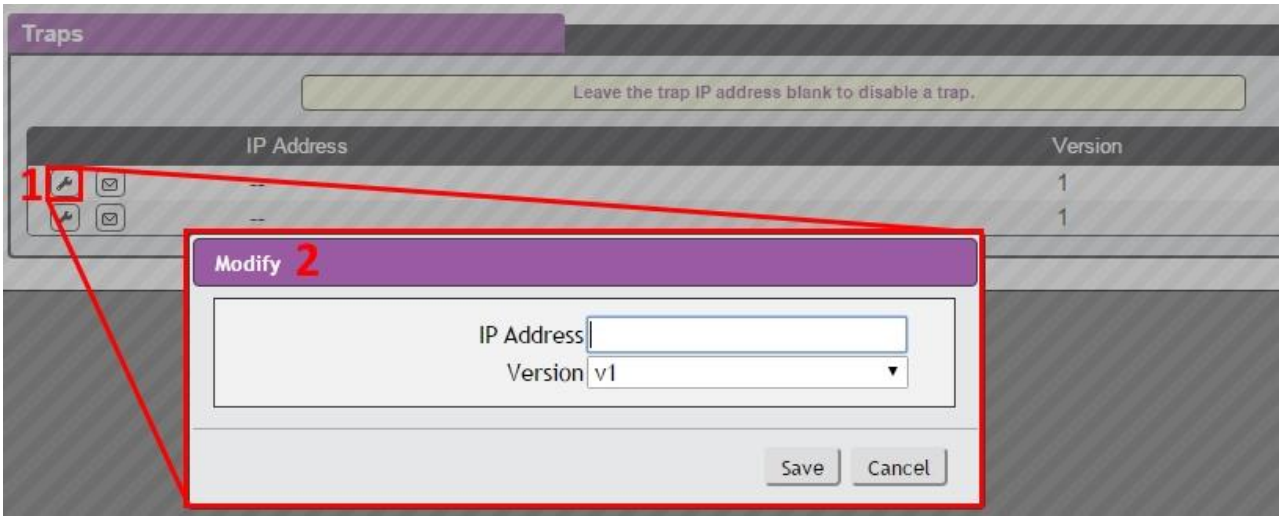

Figure 30: Modify Traps

1. Locate the ***Traps*** section of the SNMP page, and click on the Modify icon.
2. Enter the ***IP Address*** which the trap should be sent to, select the trap ***Version*** to be used (v1, v2c, or v3), and click ***Save***. Once completed, a test trap may be sent by clicking on the envelop icon (Send Test Trap).

Syslog Page

Syslog data can be captured remotely but must first be setup and enabled via the *Syslog Page*. Note that this function is primarily useful for diagnostic purposes, and **should normally be left Disabled** unless advised to enable it by Geist technical support for troubleshooting a specific issue.

Figure 31: Syslog Page

Admin Page

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 that 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.

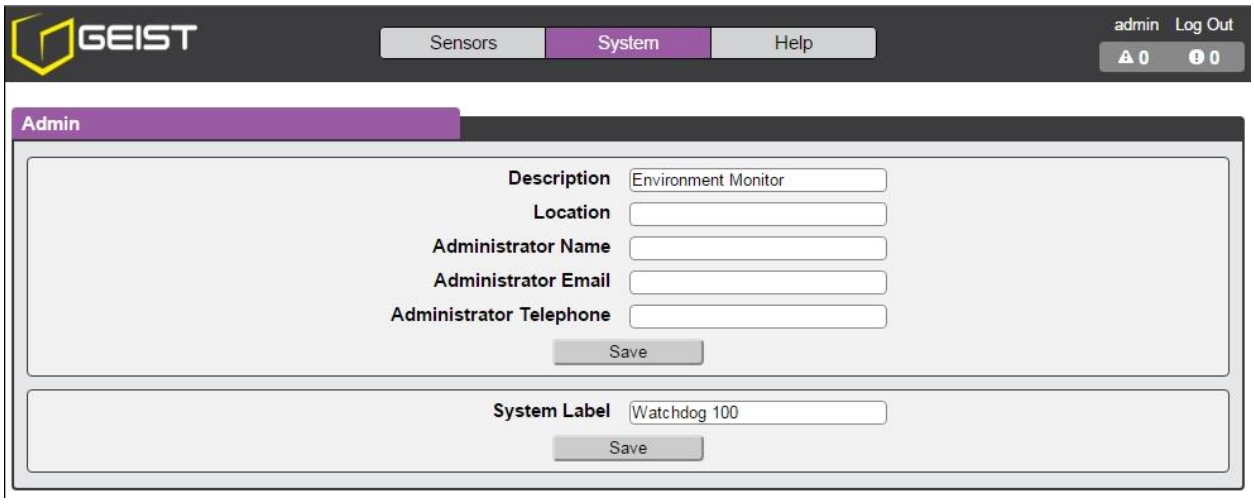

Figure 32: Admin Page

Time Page

The system clock is set here. The unit comes preconfigured with the Primary NTC Server *pool.ntc.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.

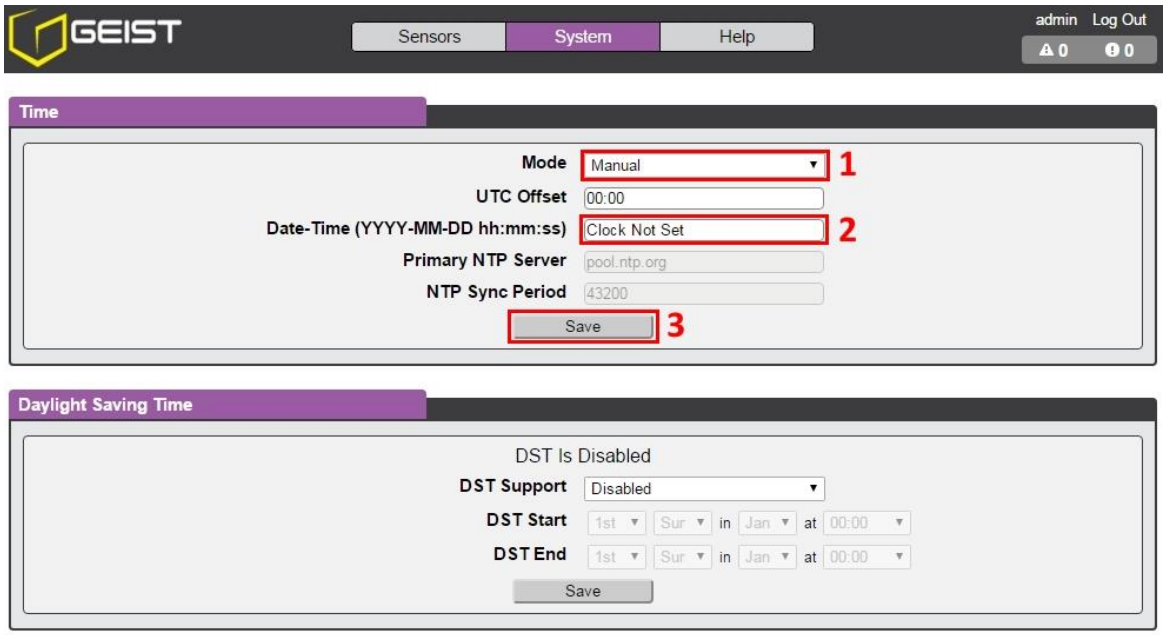

Figure 33: Time Page

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.

Locale Page

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.

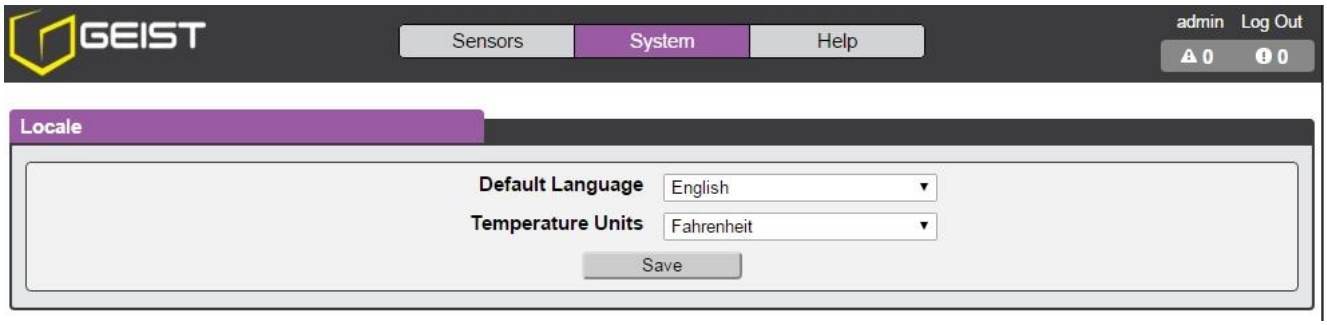

Figure 34: Locale Page

Restore Defaults Page

The *Restore Defaults Page* 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 Settings, Except Network and Users: Erases all settings except the Network and User Accounts.

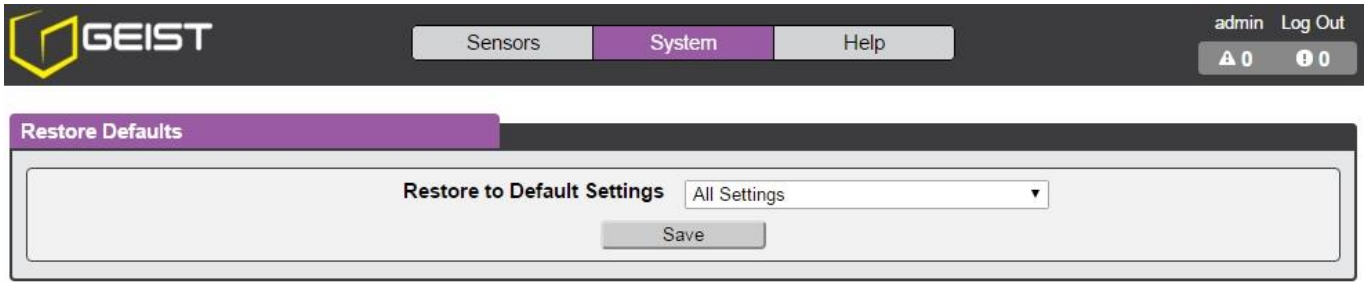

Figure 35: Restore Defaults Page

Firmware Update Page

Use the *Firmware Update Page* 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.

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.

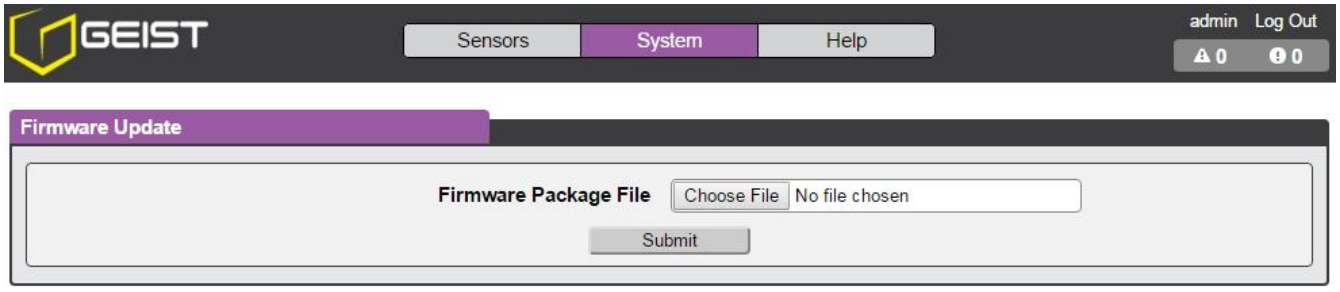

Figure 36: Firmware Update Page

Upgrading Firmware

1. Click the "*Choose File*" button.
2. Search for the downloaded firmware file and click Open.
3. Click "*Submit*" button to update.

Help Info Page

The Info Page displays the unit's current configuration information, including the Device Name, ID, and type installed. The unit's current firmware versions, network information, and manufacturer support information is also here.

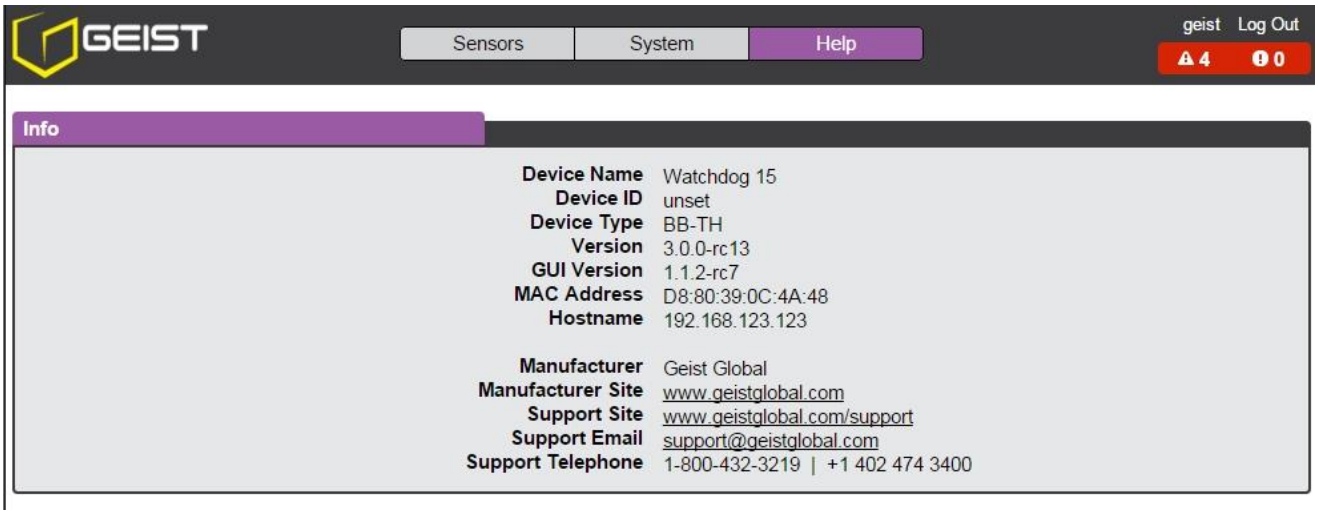

Figure 37: Help Info Page

Help Support Site

Technical support and documentation can be found at *http://www.geistglobal.com/support/manuals*

Technical Support

Resetting the Unit

Should the Watchdog 15 loose communication; the processor may be manually rebooted by removing power momentarily from the unit. To restore the default IP address, press the reset button located beside the network connector and hold for approximately 20 seconds. Both the idle and activity lights near the network connector will both light up when the IP address has been reset.

Service and Maintenance

No service or maintenance is required. Do not attempt to open the unit or you may void the warranty. No serviceable parts inside.

More Technical Support

http://www.geistglobal.com
(800) 432-3219
Email: support@geistglobal.com
Or contact your distributor.

Using Microsoft Exchange as an SMTP server

If your facility uses a Microsoft Exchange Email server, it can be used by the WATCHDOG 15 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 15 to send Emails through your Exchange server, the following notes may be helpful in resolving the problem.

Note that these suggestions only apply if you are using your own, physical Exchange server! Microsoft's hosted "Office365" service is not compatible with the WATCHDOG 15 using firmware versions prior to v3.0.0, as Office365 requires a Start-TLS connection. Firmware versions 3.0.0 and beyond have support for Start-TLS and are compatible with Office365.

First, since the WATCHDOG 15 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 15'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 15 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 15 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 15 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 plugins 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 15 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.

Table of Figures

Revision History

Revision	Date	Notes	Approved By
1.0	8/9/2012	Initial Version	CG
2.0	2/13/2015	Change Product Name and Update Interface.	QN
3.0	12/30/15	BB3.0 Upgrade Changes and A2D support	QN