INSTRUCTION MANUAL

MODEL CAPWATCH

(Common Alerting Protocol Weather Alert Total Coverage Hub)

Commercial Alerting Device

Document Rev. 1.02a

Document Date: 03.26.2019

GORMAN-REDLICH

GORMAN REDLICH
257 West Union St.
Athens, Ohio 45701

Ph: 740-593-3150 www.Gorman-Redlich.com

Contents

Product Information

WARRANTY

For a period of 1 year from date of shipment, Gorman-Redlich warrants the CAPWATCH to be free from defects in materials and workmanship and will repair or replace, at its option, any CAPWATCH unit that fails in normal service without a charge for parts or labor and with a flat $25 fee, prepaid by purchaser, to cover shipping and handling. Units can only be accepted for adjustment under Warranty following notification by letter, telephone or e-mail. Units showing evidence of modification or abuse, in the judgment of Gorman-Redlich, cannot be accepted for repair under Warranty, but will be repaired for a reasonable fee, with the consent of the purchaser.

LICENSE

With the purchase of the Gorman-Redlich CAPWATCH equipment, the original purchaser receives the hardware and license for use of the included CAPWATCH SENTRY software. Software license allows use of the CAPWATCH SENTRY software only on the original CAPWATCH hardware on which it was installed from the factory. Use of the CAPWATCH hardware and CAPWATCH SENTRY software is subject to the Gorman-Redlich Mfg. Co. CAPWATCH/CAPWATCH SENTRY End User License Agreement (EULA) and such use constitutes acceptance of the EULA. Software updates, as they become available, are provided to users at no charge for the duration of the support period specified at time of purchase. Further updates to provide enhanced functionality may be released subsequent to purchase and installation of CAPWATCH equipment, either before or after the termination of the support period. Upgrades to new software versions outside of the support period may incur additional costs.

COMMON ALERTING PROTOCOL

The Common Alerting Protocol (CAP) is an XML-based data format for exchanging public warnings and emergencies between alerting technologies. CAP allows warning messages to be distributed consistently and simultaneously across multiple warning systems. This protocol allows for the inclusion of large amounts of information about emergency situations which can range from general situational data to information intended for specific alerting platforms.

GENERAL DESCRIPTION OF CAPWATCH ALERTING DEVICE

The National Oceanic and Atmospheric Administration (NOAA) and its child agency, the National Weather Service (NWS) deliver timely weather alerts and information (*alert products*) in CAP format by means of internet alert feeds. Such alert products conform to the Common Alerting Protocol v1.2 specification and are further constrained by the Integrated Public Alert and Warning System (IPAWS) Profile v1.0 specification.

The Gorman-Redlich CAPWATCH system retrieves alerting products from NWS alert feeds in the form of XML files. These files are compared to a variety of standards and specifications to ensure message validity as well as being filtered by user-specified location and event type filters. Valid messages are then processed and relayed according to the user-configured outputs, which may include (but is not limited to) alert tones, text-to-speech rendered alert information, email notifications, serial data output, and relay contact closure.

NOTE: Gorman-Redlich Mfg. Co. strongly suggests operating the CAPWATCH device with an uninterruptible power supply (UPS) for both surge protection and battery back-up functionality.

Hardware Components

Front Panel

1. Intake ventilation grate
2. Universal Serial Bus (USB) port
3. Red power LED labeled “POWER”

Side Panel

1. Exhaust ventilation grate
2. RS232 serial data port labeled “SERIAL PORT”

Rear Panel

1. PS/2 mouse port labeled “MOUSE”
2. PS/2 keyboard port labeled “KEYBOARD”
3. RS232 serial data port labeled “SERIAL PORT”
4. VGA video-out port labeled “VGA PORT”
5. Four (4) Universal Serial Bus (USB) ports labeled “USB 1” “USB 2” “USB 3” and “USB 4”
6. 10/100/1000 RJ45 ethernet port labeled “LAN”
7. 1/8-inch TRS line audio input jack labeled “AUDIO IN”
8. 1/8-inch TRS audio output jack labeled “AUDIO OUT”
9. 1/8-inch TRS microphone input jack labeled “MIC IN”
10. Power reset button labeled “RESTART”
11. Barrel-type power jack labeled “12V 5A”
12. Audio loop-through and relay contact closure header
13. Audio output adjustment pot labeled “MODULATION ADJUST”

Hardware Connections

Connections for Setup

Prior to using the CAPWATCH unit, some minor initial setup must be performed to ensure proper operation. This setup requires your interaction with the unit via normal PC interface hardware (e.g. keyboard, mouse, monitor).

1. Attach a mouse using either a PS/2 connection to the MOUSE port or a USB connection to any of the available USB ports on the rear of the CAPWATCH unit.
2. Attach a keyboard using either a PS/2 connection to the KEYBOARD port or a USB connection to any of the available USB ports on the rear of the CAPWATCH unit.
3. Attach a monitor using a VGA cable to the VGA PORT on the rear of the CAPWATCH unit.
4. Attach a network-connected ethernet cable to the RJ45 LAN port on the rear of the CAPWATCH unit.
5. Power on the CAPWATCH unit by attaching the 12V 5A AC adapter (labeled CAP power supply) to the power jack (labeled 12V 5A) on the rear of the CAPWATCH unit and plug it in to the power source. Gorman-Redlich strongly suggests using an uninterruptible power supply (UPS) with the CAPWATCH unit. The unit should begin the boot process automatically. If it does not, press the red START button on the rear of the unit.
6. (optional) Additional connections may be required based on user output preferences. These connections may include RS232 serial data line for logging, alert text display or other functionality, audio cables via the 1/8" TRS connection or audio header, among others. It would not be practical to list all possible installation variations; please consult with your installation technician for the connections required to meet your needs. If audio output (via "AUDIO PROGRAM LINES") levels require adjustment, the "MODULATION ADJUST" potentiometer on the rear of the unit may be adjusted.

Unit Setup

Once the unit is powered up with the above connections, the CAPWATCH unit may be configured as desired to site-specific preferences including network setup, printer installation, monitoring and interface options (e.g. logging devices), USB peripherals (e.g. flash drives), etc. (*see Software Setup section below*).

Due to the varied nature of such setup from one site to another, it is impossible to cover all possible setup procedures. Manufacturer's instructions should be followed for installation and use of devices such as printers, USB drives, USB-to-RS232 adapters, digital signage, public address systems, warning lighting, logging devices or software, etc.

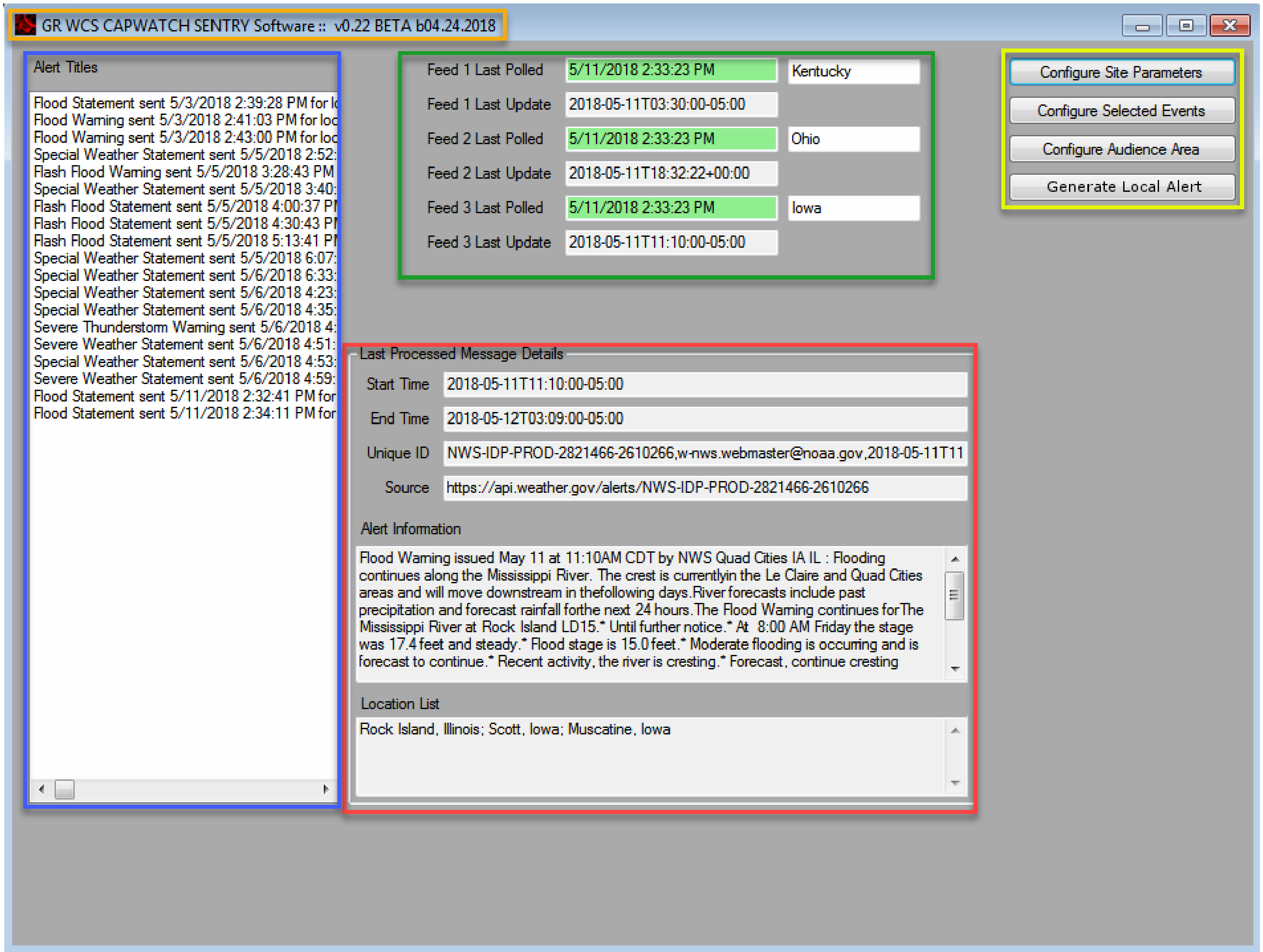
The CAPWATCH unit must be configured for connectivity with your station's specific network setup. Again, due to the varied nature of such systems, it is impossible to cover all possibilities here. The steps necessary to ensure CAPWATCH connectivity mirror those required for any PC on your network. This includes opening/unblocking ports for HTTP requests (default: 80) and SMTP activity if email functionality is desired (default: 25). The CAPWATCH SENTRY should be allowed access through station firewall and other network protection. If your station's network utilizes dynamic host control protocol (DHCP), simply attaching the CAPWATCH to the network should provide connectivity. If static IP addressing is required, such settings may be entered by navigating to START | Control Panel and searching for the View Network Connections option. Right-mouse-click the connection to be used and choose Properties. Contact your station's network technician for station-specific setup details.

Connections for Operation

Once the unit has been configured for operation, interface devices such as a keyboard, mouse and monitor are not required for operation although they may be left attached for monitoring, testing, or further setup. The network cable must remain attached so that the unit is able to receive alerts and the power cable must remain attached.

Software Setup and Use

The CAPWATCH SENTRY software begins automatically once the unit has completed the boot-up process. Upon starting, the software dialog will appear on screen after a short initialization period (up to 20 seconds). The software consists of several interfaces: the main software screen, a Site Configuration screen, an Event Configuration screen, an Audience Configuration screen, and a Local Alert Generation screen. Upon starting, the user will be presented with the main CAPWATCH SENTRY screen with the current version number and build date listed at the top (orange box in figure); four additional interfaces are accessible through the buttons on the main screen.



GR WCS CAPWATCH SENTRY Software :: v0.22 BETA b04.24.2018

Alert Titles

Flood Statement sent 5/3/2018 2:39:28 PM for l
Flood Warning sent 5/3/2018 2:41:03 PM for loc
Flood Warning sent 5/3/2018 2:43:00 PM for loc
Special Weather Statement sent 5/5/2018 2:52:
Flash Flood Warning sent 5/5/2018 3:28:43 PM
Special Weather Statement sent 5/5/2018 3:40:
Flash Flood Statement sent 5/5/2018 4:00:37 P
Flash Flood Statement sent 5/5/2018 4:30:43 P
Flash Flood Statement sent 5/5/2018 5:13:41 P
Special Weather Statement sent 5/5/2018 6:07:
Special Weather Statement sent 5/6/2018 6:33:
Special Weather Statement sent 5/6/2018 4:23:
Special Weather Statement sent 5/6/2018 4:35:
Severe Thunderstorm Warning sent 5/6/2018 4:
Severe Weather Statement sent 5/6/2018 4:51:
Special Weather Statement sent 5/6/2018 4:53:
Severe Weather Statement sent 5/6/2018 4:59:
Flood Statement sent 5/11/2018 2:32:41 PM for
Flood Statement sent 5/11/2018 2:34:11 PM for

Feed 1 Last Polled 5/11/2018 2:33:23 PM Kentucky
Feed 1 Last Update 2018-05-11T03:30:00-05:00
Feed 2 Last Polled 5/11/2018 2:33:23 PM Ohio
Feed 2 Last Update 2018-05-11T18:32:22+00:00
Feed 3 Last Polled 5/11/2018 2:33:23 PM Iowa
Feed 3 Last Update 2018-05-11T11:10:00-05:00

Last Processed Message Details

Start Time 2018-05-11T11:10:00-05:00
End Time 2018-05-12T03:09:00-05:00
Unique ID NWS-IDP-PROD-2821466-2610266,w-nws.webmaster@noaa.gov,2018-05-11T11
Source https://api.weather.gov/alerts/NWS-IDP-PROD-2821466-2610266

Alert Information

Flood Warning issued May 11 at 11:10AM CDT by NWS Quad Cities IA IL : Flooding continues along the Mississippi River. The crest is currentlyin the Le Claire and Quad Cities areas and will move downstream in thefollowing days.River forecasts include past precipitation and forecast rainfall forthe next 24 hours.The Flood Warning continues forThe Mississippi River at Rock Island LD15.* Until further notice.* At 8:00 AM Friday the stage was 17.4 feet and steady.* Flood stage is 15.0 feet.* Moderate flooding is occuring and is forecast to continue.* Recent activity, the river is cresting.* Forecast, continue cresting

Location List

Rock Island, Illinois; Scott, Iowa; Muscatine, Iowa

CAPWATCH Main Software Interface

The main software screen contains information about and results from message processing as well as buttons to access configuration interfaces. Note that alert processing information will only be shown as above *after* an alert has been successfully processed. Upon startup, all boxes will be blank until alert polling and processing begins.

Main Interface Components

The main interface window consists of four main components: polling information, last message processed information, previously processed message alert titles, and configuration/alert generation buttons.

Polling Information

Information about enabled alert feeds, the last time that the feed was successfully polled, and the last time that the feed was updated is displayed in the top-center of the window, highlighted above by the green box. Three pieces of information are shown for each of the three available feeds:

1. **Last Polled timestamp** indicates the last time that the feed was successfully polled (checked for the presence of new alerts). This timestamp is displayed in local time. If the feed is enabled, this timestamp should update at the start of each polling cycle (typically 30 seconds). If the unit is successfully polling the feed, this timestamp will be highlighted in GREEN. If the unit cannot communicate with the alert feed, the timestamp will stop updating and will turn YELLOW if below the missed-poll threshold and then RED if the number of failed polling attempts surpasses the missed-poll threshold. If the unit is unable to communicate with the alert feeds, check your network connectivity.
2. **Last Update timestamp** indicates the last time that the feed was updated by the alert originator. This timestamp is shown as UTC time with time-zone offset. This value only update if and when alert originators update the feed to add, remove, or update alerts and may not update often if no alert events are occurring.
3. **Feed State** indicates the state that is being polled for each of the enabled feeds. If the Geo-Filtering function is enabled, this control will display the LAT/LONG coordinates configured for the unit.

Last Message Processed Details

The lower-center portion, as highlighted in the red box above, of the main software interface shows details of the last message processed, including the start and end time of the event, the unique identifier of the alert, the source of the alert, and the alert text associated with the alert.

This portion of the interface will not be populated with information unless and until the first alert has been processed

Alert Titles (Previously Processed Messages)

The left side of the main CAPWATCH SENTRY interface, as highlighted in the blue box above, displays an overview list of the most recently processed messages. This overview includes the type of alert, the time of the alert, and the locations impacted by the alert. Due to the narrow width of this component, it may be necessary to use the horizontal scroll bar at the bottom of the display to view all of the details for a given alert.

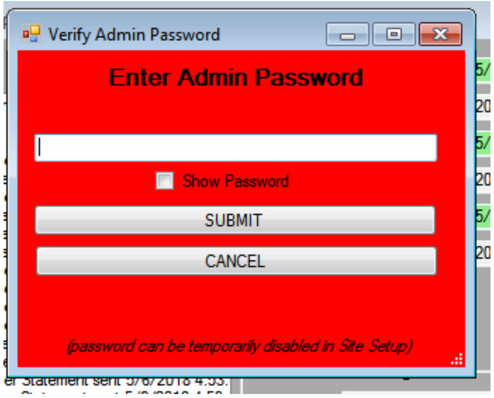
Again, this display will not be populated with data unless and until the first alert has been processed.

Additional Interface Access Buttons

At the top-right of the main interface window, as highlighted in the yellow box above, are the buttons to access additional interfaces. Additional information about these interfaces are included in separate sections below. These include:

1. **Configure Site Parameters**, where the user can adjust settings related to which feeds are polled, output options, password options, email configuration, and more.
2. **Configure Selected Events**, where the user can select which event codes for which they want to filter.
3. **Configure Audience Area**, where the user can select which FIPS-based locations they want to activate or configure lat/long coordinates.
4. **Generate Local Alert**, where the user can locally generate an alert message that is distributed through the configured output channels.

Password Entry



(password can be temporarily disabled in Site Setup)

Unless the option has been disabled, when accessing the additional configuration and alert generation interfaces, the user will be presented with a password entry box as shown here.

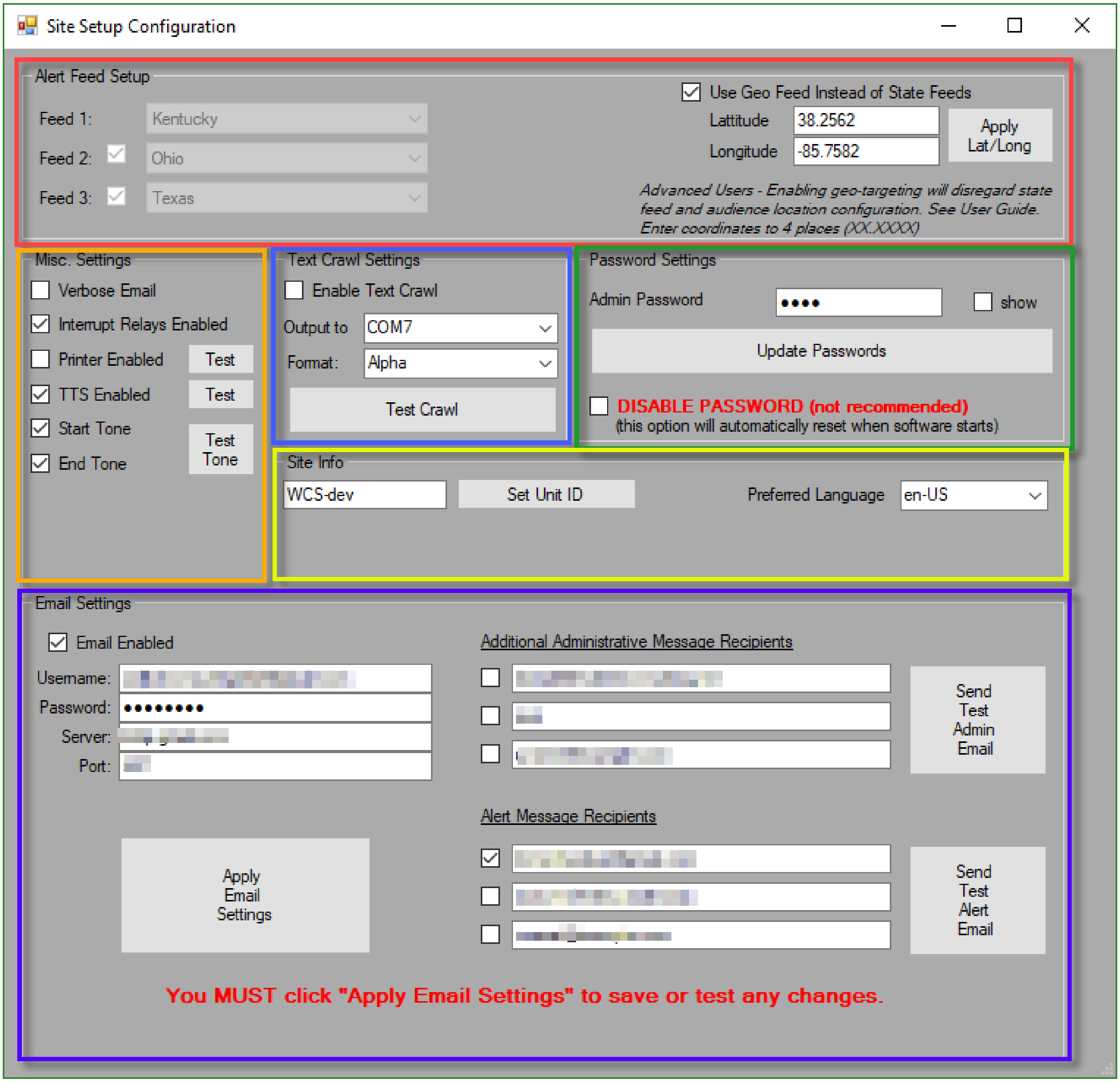
Enter your CAPWATCH administrator password in the text box and either press the [enter] key or click the SUBMIT button. The password will be obscured on-screen for security purposes, although the *Show Password* checkbox can be marked to show the password on-screen to ensure correct entry.

If the user changes their mind and decides not to proceed to the configuration or alert generation interface, the CANCEL button will exit this window.

The password requirement for entering additional configuration and alert generation interfaces can be disabled in the Site Configuration dialog, although *this is not recommended* for security purposes. If enabled, this option will remain enabled until manually disabled or until the CAPWATCH SENTRY software is restarted.

Configuring Site Parameters

The Site Parameter configuration interface is accessed by clicking the “Configure Site Parameters” button on the main interface window. This interface is where the user may configure various settings pertaining to which states’ alert feeds are polled, alert text output options, relay functionality, alert tone output, text-to-speech (TTS) output, passwords, email notification options, primary language, unit ID, and more.



Site Setup Configuration

Alert Feed Setup

Feed 1: Kentucky

Feed 2: ☑ Ohio

Feed 3: ☑ Texas

☑ Use Geo Feed Instead of State Feeds

Latitude: 38.2562

Longitude: -85.7582

Advanced Users - Enabling geo-targeting will disregard state feed and audience location configuration. See User Guide. Enter coordinates to 4 places (XX.XXXX)

Misc. Settings

- ☐ Verbose Email
- ☑ Interrupt Relays Enabled
- ☐ Printer Enabled
- ☑ TTS Enabled
- ☑ Start Tone
- ☑ End Tone

Text Crawl Settings

☐ Enable Text Crawl

Output to: COM7

Format: Alpha

Password Settings

Admin Password: ●●●● ☐ show

☐ DISABLE PASSWORD (not recommended)
(this option will automatically reset when software starts)

Site Info

WCS-dev

Preferred Language: en-US

Email Settings

☑ Email Enabled

Username: [redacted]

Password: ●●●●●●●●

Server: [redacted]

Port: [redacted]

Additional Administrative Message Recipients

☐ [redacted]

☐ [redacted]

☐ [redacted]

Alert Message Recipients

☑ [redacted]

☐ [redacted]

☐ [redacted]

You MUST click "Apply Email Settings" to save or test any changes.

CAPWATCH SENTRY Site Configuration Interface

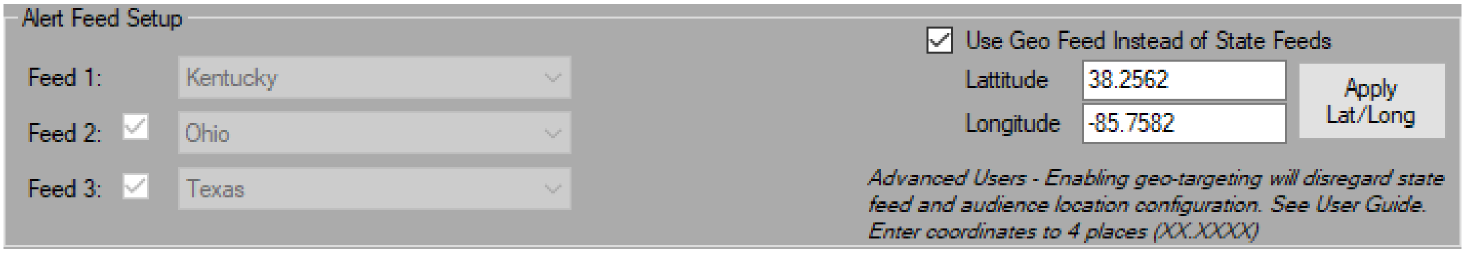
There are six main components to the Site Configuration interface: Alert Feed Setup (highlighted by the red box above), Text Crawl Settings (blue box), Password Settings (green box), Site Info settings (yellow box), Email Settings (purple box), and Miscellaneous Settings (orange box). Each of these components are described in greater detail below.

Alert Feed Setup

The Alert Feed Setup controls allow the user to select between one and three state feeds for the CAPWATCH to poll for alerts. Typical installations will likely only have one state feed enabled, although installations near state borders or master control centers responsible for multiple locations may wish to enable additional feeds.

Alternatively to selecting state-specific alert feeds, advanced users may enable geo-filtering of alerts by entering the latitude and longitude of the location they wish to monitor. When this option is enabled, state feed selection will be disabled, although the configuration options entered here will remain saved in the unit configuration files.

Latitude values (between -90 and 90) and longitude values (between -180 and 180) should be entered in *decimal format only (no Hours-Minutes-Seconds format)* and should be entered to four decimal places. Once the lat/long values have been entered, the user **must press the "Apply Lat/Long" button** to store these values. If invalid values are entered, the user will receive a warning and the value will be reset to 00.0000,00.0000.



Alert Feed Setup

Feed 1: Kentucky

Feed 2: ☑ Ohio

Feed 3: ☑ Texas

☑ Use Geo Feed Instead of State Feeds

Lattitude 38.2562

Longitude -85.7582

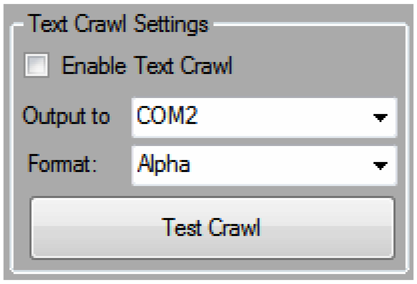
Advanced Users - Enabling geo-targeting will disregard state feed and audience location configuration. See User Guide. Enter coordinates to 4 places (XX.XXXX)

Feed 1 is enabled by default and cannot be disabled, as a minimum of one feed is required to be monitored for operation. Feed 2 and Feed 3 are enabled or disabled by marking the checkbox next to them. When geo-filtering is enabled, Feed 2 and Feed 3 are disabled, as the geo-coordinates query will return all alerts that effect the specified location.

For standard alert feed polling, un-check the Geo Feed checkbox to enable State Feed setup controls and use the dropdown box(es) to select which state you wish to monitor for any enabled feeds. The new settings will be reflected on the main screen upon exiting the Site Setup configuration interface.

NOTE 1: *This selection only causes the CAPWATCH to check the selected feeds for the presence of alerts; to process alerts, specific locations must be selected in the Audience Area configuration interface, described below.* **NOTE 2:** *When geo-filtering is enabled, Audience Area configuration values are disregarded as the results are pre-filtered to the configured location. However, configured Audience Area values are still retained in the unit configuration files.*

Text Crawl Setup



Text Crawl Settings

□ Enable Text Crawl

Output to COM2

Format: Alpha

CAPWATCH allows for output of detailed alert information, including the event Headline, Description, and Instructions, via serial RS232 data in a variety of formats. To enable this feature, mark the checkbox in this portion of the interface. It is recommended to have already set up the selected output COM port and output format before enabling the feature.

Selecting a COM Port

If use of this feature is desired, select a serial RS232 COM port from the dropdown box. COM1 and COM2 are physical DB-9 serial ports on the CAPWATCH unit. If a USB-to-RS232 adapter is used to create a virtual COM port, it will have a different number. Follow manufacturer instructions for attaching and determining the virtual COM port number.

Selecting Output Format

This dropdown allows selection of the serial data output format. A number of formatting options are available; the format should be selected based on the equipment that is attached to the CAPWATCH.

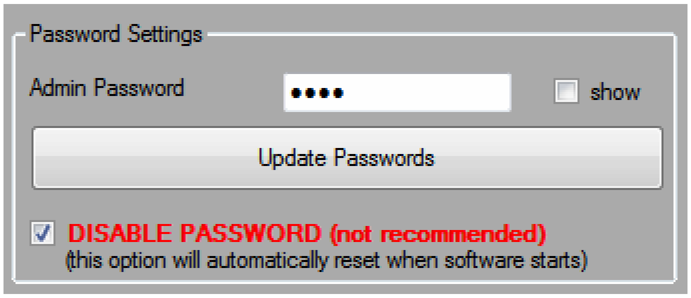
1) **XBOB** – This option formats the alert text for the Decade Engineering XBOB character generator, which can be used to display text crawls overlaid on analog video.
2) **Evertz** – This options formats the alert text to be compatible with Evertz keyers for digital signage or video displays.
3) **VDS** – This option formats the alert text for Video Data Systems character generators for video displays.
4) **CODI** – This option formats the alert text for the Chyron CODI text and graphics generator for video displays.
5) **Alpha** – This option formats the alert text to the Alpha Protocol for Adaptive Micro Systems Alpha-compatible digital LED signage.

Password Settings

This portion of the Site Configuration interface provides options for changing the administrator password for the CAPWATCH SENTRY software and disabling the password requirement for accessing the additional interfaces.

Viewing and Setting the Administrator Password

Choose a good, secure password that you will remember. Passwords are never stored in plain-text; they are stored as AES128 encrypted data. As such, lost passwords cannot be recovered. Gorman-Redlich may, however, be able to reset the password to a known value for the user.



Password Settings

Admin Password •••• □ show

☑ DISABLE PASSWORD (not recommended)
(this option will automatically reset when software starts)

NOTE: ***to prevent unauthorized access, modification of settings, or generation of alert messages, user <u>must</u> change the password to one of their own choosing upon receipt of the unit unless a custom administrator password was configured from the factory.***

Marking the *Show Password* checkbox will display the current password on-screen to verify the current password or to ensure correct entry when updating the password. If the user wishes to update the administrator password, the new password should be typed into the textbox and must then click the *Update Password* button.

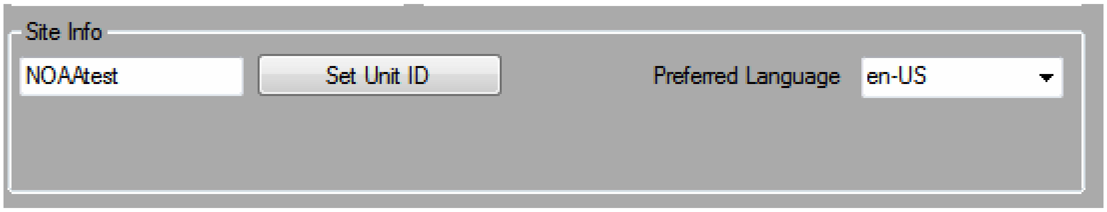
Disabling Password Requirement

Marking the DISABLE PASSWORD checkbox will disable the requirement to enter the password to access additional configuration and alert generation interfaces from the main interface window. <u>Enabling this option is not recommended for security purposes</u>.

Entering the administrator password will still be required to send locally-generated alert messages.

If enabled, this option will remain enabled until manually disabled or until the CAPWATCH SENTRY software is restarted.

Site Info Setup



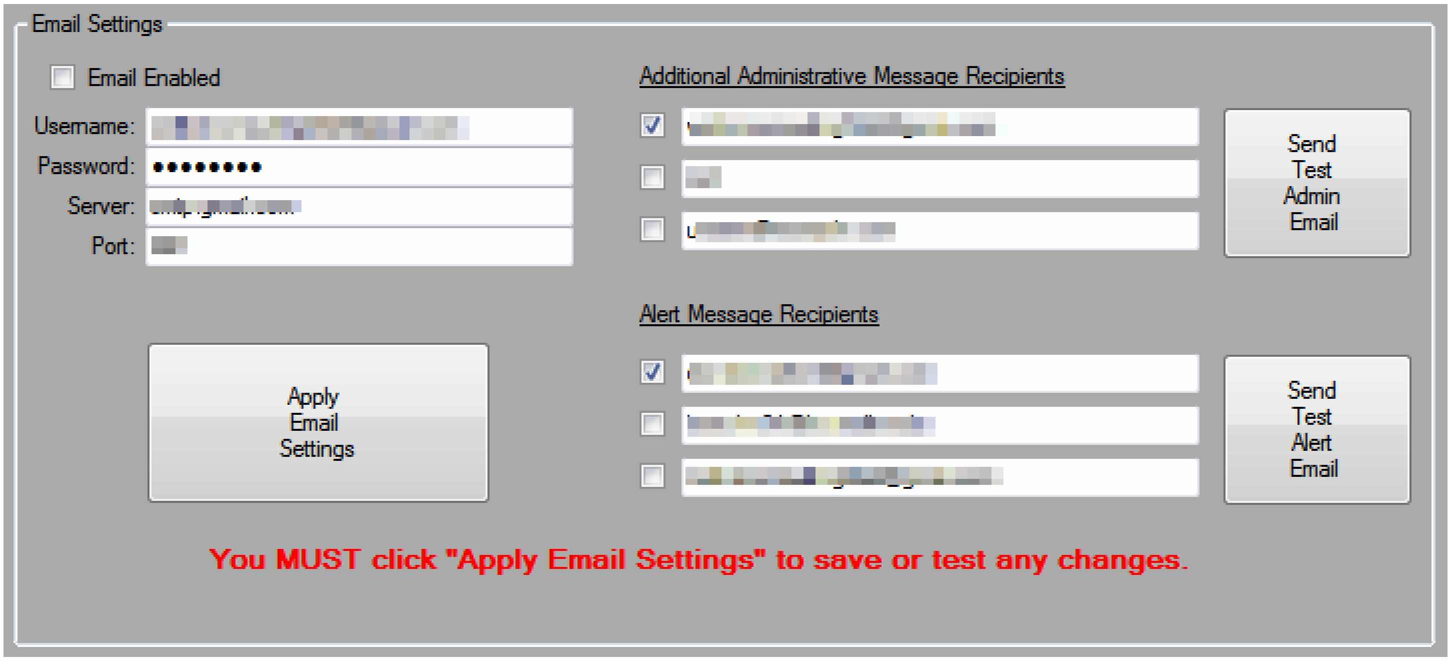
Site Info

NOAAtest

Preferred Language: en-US

These controls allow for setting the Unit ID (used for identifying the CAPWATCH unit in logging, reporting, and email notifications) and selecting the primary language for alert processing.

Email Settings



Email Settings

□ Email Enabled

Username: [redacted]

Password: ••••••••

Server: [redacted]

Port: [redacted]

Additional Administrative Message Recipients

☑ [redacted]

□ [redacted]

□ [redacted]

Alert Message Recipients

☑ [redacted]

□ [redacted]

□ [redacted]

You MUST click "Apply Email Settings" to save or test any changes.

This portion of the Site Setup interface controls CAPWATCH email preferences. Whenever any changes are made to the email server settings or message recipient lists, the *Apply Email Settings* button MUST be clicked after entering new settings to apply the changes.

Enabling and Disabling Email Functionality

To enable CAPWATCH SENTRY email functionality for administrative messages and processed alert notifications, mark the *Email Enabled* checkbox at the top of this section of the interface.

Email Server Settings

The CAPWATCH SENTRY software sends email notifications using the user's own external email service. Setup is similar to any other email client and is accomplished the email username, password, SMTP server, and port number. Please consult your email provider's instructions or your IT personnel to find these settings for your email service. **NOTE:** *passwords are not stored in plain-text on the CAPWATCH unit; they are stored as AES128 encrypted data.*

Once email settings have been entered, click the *Apply Email Settings* button to save the changes

Email settings can be tested to ensure correct configuration by using the test buttons described below once recipient addresses have been entered.

Due to the varied nature of each email provider's settings, we cannot provide support for third-party email services.

Known good server settings include:

Gmail: [full email address][smtp.gmail.com][587][password] (must request app-specific password if 2-factor authentication is enabled)

Yahoo!: [full email address][smtp.mail.yahoo.com][587][password]

MS Live Mail: [full email address][smtp-mail.outlook.com][587][password]

GoDaddy Hosted Mail: [full email address][smtpout.secureserver.net][465][password]

1and1 Hosted Mail: [full email address][smtp.1and1.com][587][password]

We have received reports of issues configuring email functionality with Microsoft Exchange/Outlook365 servers.

Administrative Message Recipients

Addresses entered as administrative message recipients will receive email notifications pertaining to the operation of the CAPWATCH SENTRY software, such as connectivity issues with the NOAA/NWS alert feeds. Only enter email recipients from whom you have permission to send emails.

To add an administrative message recipient, enter their email address in the text box, mark the checkbox next to the address to enable it, and click the *Apply Email Settings* button to save the changes. If the checkbox is unmarked, the email address will remain in the text box but emails will not be sent to this address. Up to three recipients can be added. If additional recipients are desired, it is recommended to set up a third-party email distribution list and add the list's address as a recipient.

To test email configuration, a test administrative message can be sent by clicking the *Send Test Admin Email* button. If the email is successfully sent, a message box will appear after a few seconds indicating that the message was sent. If a message box appears indicating that the message was not sent, check your email server setup configuration.

Alert Message Recipients

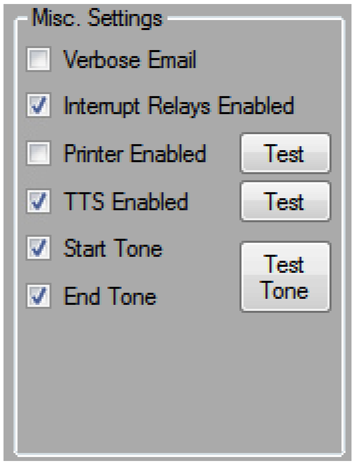
Addresses entered as alert message recipients will receive email notifications when an alert is processed. These messages will contain information about the alert message including start and end times, message type, event description, and instructions. Only enter email recipients from whom you have permission to send emails.

To add an alert message recipient, enter their email address in the text box, mark the checkbox next to the address to enable it, and click the *Apply Email Settings* button to save the changes. If the checkbox is unmarked, the email address will remain in the text box but emails will not be sent to this address. Up to three recipients can be added. If additional recipients are desired, it is recommended to set up a third-party email distribution list and add the list's address as a recipient.

To test email configuration, a test alert message can be sent by clicking the *Send Test Alert Email* button. If the email is successfully sent, a message box will appear after a few seconds indicating that the message was sent. If a message box appears indicating that the message was not sent, check your email server setup configuration.

Miscellaneous Settings

This section contains additional settings for the operation of the CAPWATCH unit.



Misc. Settings

☐ Verbose Email

☑ Interrupt Relays Enabled

☐ Printer Enabled

☑ TTS Enabled

☑ Start Tone

☑ End Tone

Verbose Emails

Enabling this option, if email functionality is enabled and properly configured, will send alert processing emails any time the unit finds an alert, whether it is fully processed or not (i.e. if it does not match all user-specified filters). Most users will not wish to enable this option, but it may be useful for CAPWATCH administrators who want notification of all events affecting their area even if it does not set off additional message triggers.

Interrupt Relays

Enabling this option will cause the primary interrupt relays to energize at the start of a processed message and release once message processing is finished. These relays may be used to trigger external equipment such as Public Address (PA) systems, emergency lighting, sirens, and more.

Your unit may be equipped with an optional second set of interrupt relays for “Very Important Events” (VIE). The custom behavior of these optional VIE relays is controlled by a separate configuration file that should not be modified by the user. For units with this feature enabled, events that are configured as VIE will be processed as usual with the exception that an additional set of relays will close during the processing of such messages.

Printer

Enabling this option will cause the CAPWATCH SENTRY software to print the details of processed alerts to the system’s default printer. Consult your printer’s documentation for installation and setup instructions. **WARNING:** *if no physical USB or networked printer is installed and configured on the CAPWATCH unit, the default printer may be a software file “printer” that requires user input to complete file creation (such as entering a filename). If this is the case, the software may stop processing further messages until it receives the user input.*

To test the print functionality, the *Test* button next to the *Printer Enabled* line will attempt to print a test page.

Text to Speech

Enabling this option will cause the CAPWATCH SENTRY software to use Text-to-Speech (TTS) technology to read the details of the alert aloud. Audio output will be from the 3.5mm audio output jack and/or the audio out headers on the rear of the unit, depending on the installation.

The TTS functionality can be tested by clicking the *Test* button next to this option, which will cause the TTS voice to speak a short test phrase.

Start and End Tones

Enabling these options will cause a short tone to play at the start and end, respectively, of message processing. These tones are typically used as attention tones before and after the TTS audio of the alert message over PA systems to let users know that an alert message will follow and that the alert TTS has completed.

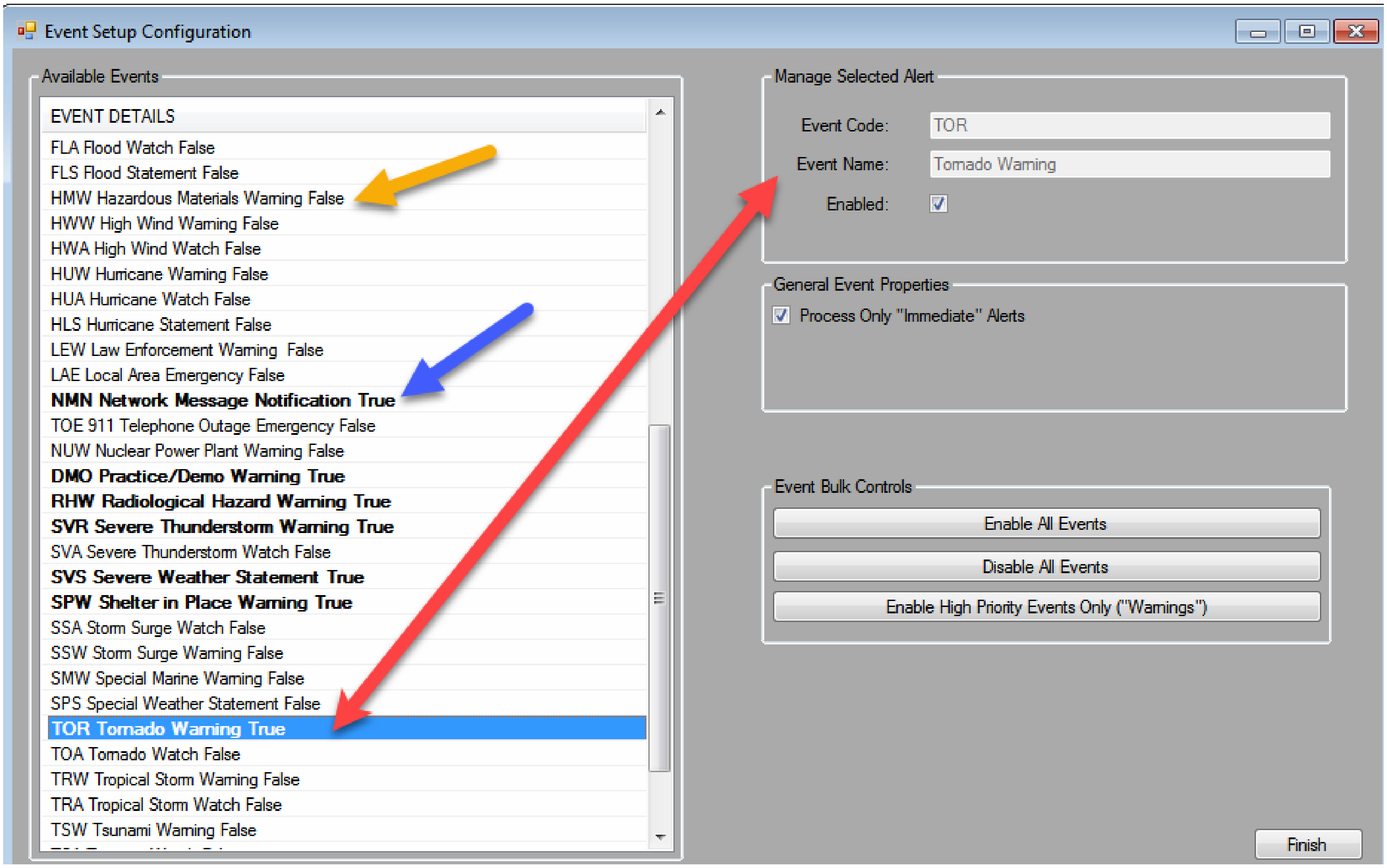
The *Test Tone* button will attempt to play the tone to allow checking the audio output.

Testing Configuration Settings

A full test of the CAPATCH SENTRY configuration can be performed by using the System Configuration Test Message feature. For more information on this feature, see the *Generating Alerts Locally* section below.

Event Setup Configuration

The Event Setup interface is accessed by clicking the “Configure Selected Events” button on the main interface window. This interface is where the user may select which events they want the CAPWATCH SENTRY software to process.



FLA Flood Watch False
FLS Flood Statement False
HMW Hazardous Materials Warning False
HWW High Wind Warning False
HWA High Wind Watch False
HUW Hurricane Warning False
HUA Hurricane Watch False
HLS Hurricane Statement False
LEW Law Enforcement Warning False
LAE Local Area Emergency False
NMN Network Message Notification True
TOE 911 Telephone Outage Emergency False
NUW Nuclear Power Plant Warning False
DMO Practice/Demo Warning True
RHW Radiological Hazard Warning True
SVR Severe Thunderstorm Warning True
SVA Severe Thunderstorm Watch False
SVS Severe Weather Statement True
SPW Shelter in Place Warning True
SSA Storm Surge Watch False
SSW Storm Surge Warning False
SMW Special Marine Warning False
SPS Special Weather Statement False
TOR Tornado Warning True
TOA Tornado Watch False
TRW Tropical Storm Warning False
TRA Tropical Storm Watch False
TSW Tsunami Warning False

Event Code: TOR
Event Name: Tornado Warning
Enabled: ☑

☑ Process Only "Immediate" Alerts

Selecting and Managing Events

The *Available Events* list on the left side of the interface displays the three-letter event code, event name, and status of each of the possible event codes that may be delivered through the NOAA/NWS alert feed. Clicking on an event from the list will populate that event’s information into the *Manage Selected Alert* controls at the top-right of the window, as shown by the red arrow above. To enable processing of the selected event, mark the “Enabled” checkbox. To disable the alert type, uncheck the box.

In the *Available Events* list, in addition to the *True/False* status information, enabled events will be displayed in **BOLD** text, as shown by the blue arrow above. Events that are not enabled will be shown in regular text, as shown by the orange arrow above.

Processing Only “Immediate” Alerts

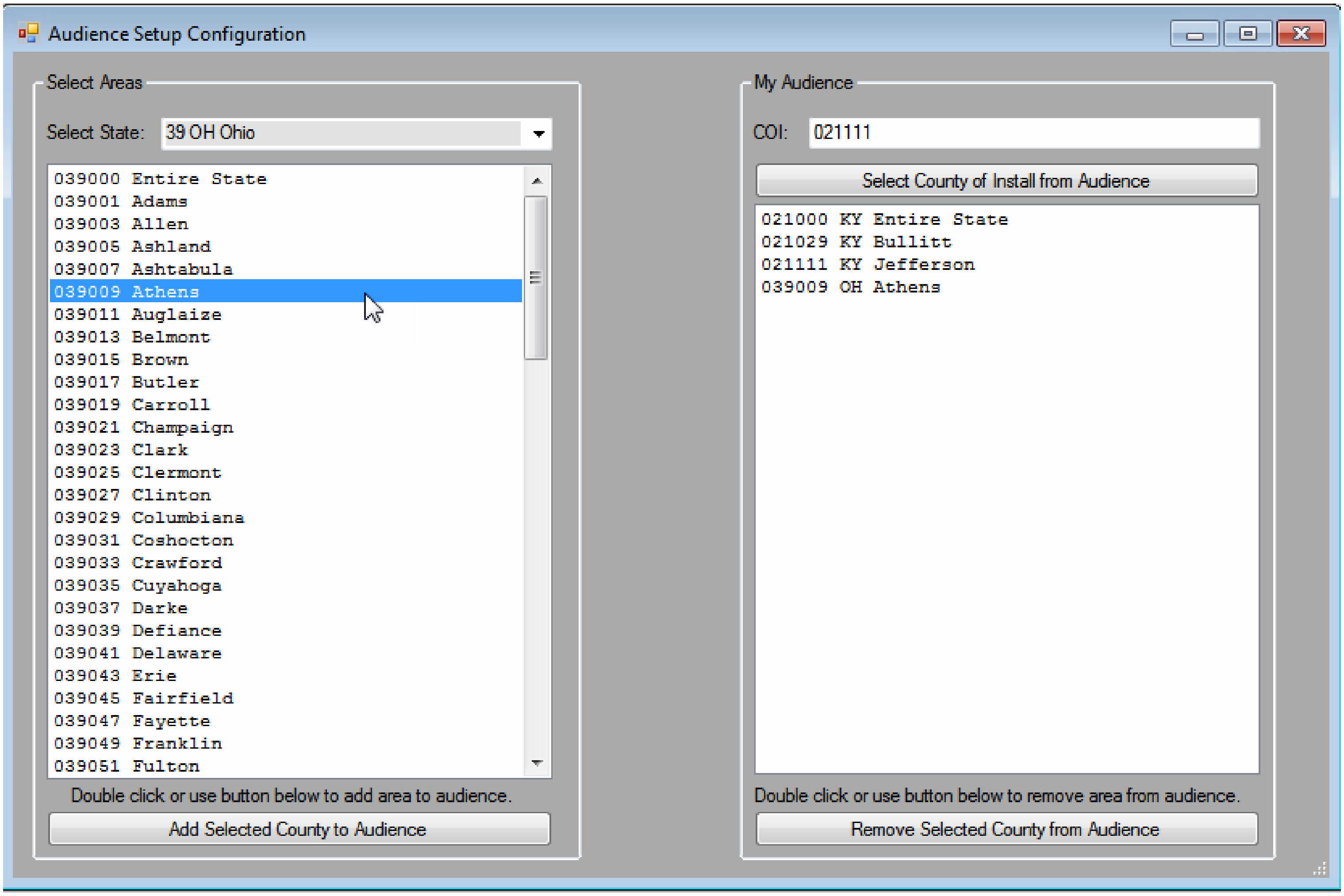
The NOAA/NWS includes alert meta-data, including whether the event poses an immediate threat or not. If the processing of only messages marked as “immediate” is desired, check this box. If processing of ALL messages sent with enabled event codes is desired, uncheck this box.

Event Bulk Controls

Event bulk controls allow the user to quickly reset all event codes to an enabled or disabled status. This is useful if a total reconfiguration of selected events is desired.

Controls are also available to enable only all “high priority” messages.

Audience Area Configuration


Audience Setup Configuration
Select Areas
My Audience
Select County of Install from Audience
Double click or use button below to add area to audience.
Add Selected County to Audience
Double click or use button below to remove area from audience.
Remove Selected County from Audience

Select State: 39 OH Ohio

```
039000 Entire State
039001 Adams
039003 Allen
039005 Ashland
039007 Ashtabula
039009 Athens
039011 Auglaize
039013 Belmont
039015 Brown
039017 Butler
039019 Carroll
039021 Champaign
039023 Clark
039025 Clermont
039027 Clinton
039029 Columbiana
039031 Coshocton
039033 Crawford
039035 Cuyahoga
039037 Darke
039039 Defiance
039041 Delaware
039043 Erie
039045 Fairfield
039047 Fayette
039049 Franklin
039051 Fulton
```

COI: 021111

```
021000 KY Entire State
021029 KY Bullitt
021111 KY Jefferson
039009 OH Athens
```

The Audience Configuration interface is accessed from the main interface window by clicking the *Configure Audience Area* button. From this window, the area filters can be configured. When a location is added to the audience area in this interface, the CAPWATCH will respond to alerts that affect that location, provided that they match other filters (such as enabled event codes).

NOTE: *While any FIPS-based Audience Area configuration values selected in the screen are always stored in the system configuration files, if the Geo-Filtering option is enabled in Site Setup, this Audience Area selection will be disregarded as alert query results will be pre-filtered to the specified geographic location based on the configured LAT/LONG values.*

Adding Areas to the Audience

First, select a state from the *Select State* dropdown box. States are listed with their FIPS code number, state abbreviation, and name. When a state is selected, the box below the dropdown menu will be populated with the FIPS code subdivisions of the state, which are typically equivalent to counties.

To add a location to the audience, either click on the location to highlight its line in the list and then click *Add Selected County to Audience* or simply double-click the location.

By default, when the first location from a new state is added to the audience area, the code for messages affecting the entire state will also be added. Additionally, the first location added will be selected as the County of Installation. If you wish to change the county of installation, simply select the correct location from the *My Audience* list and click *Select County of Install from Audience*.

Removing Areas from the Audience

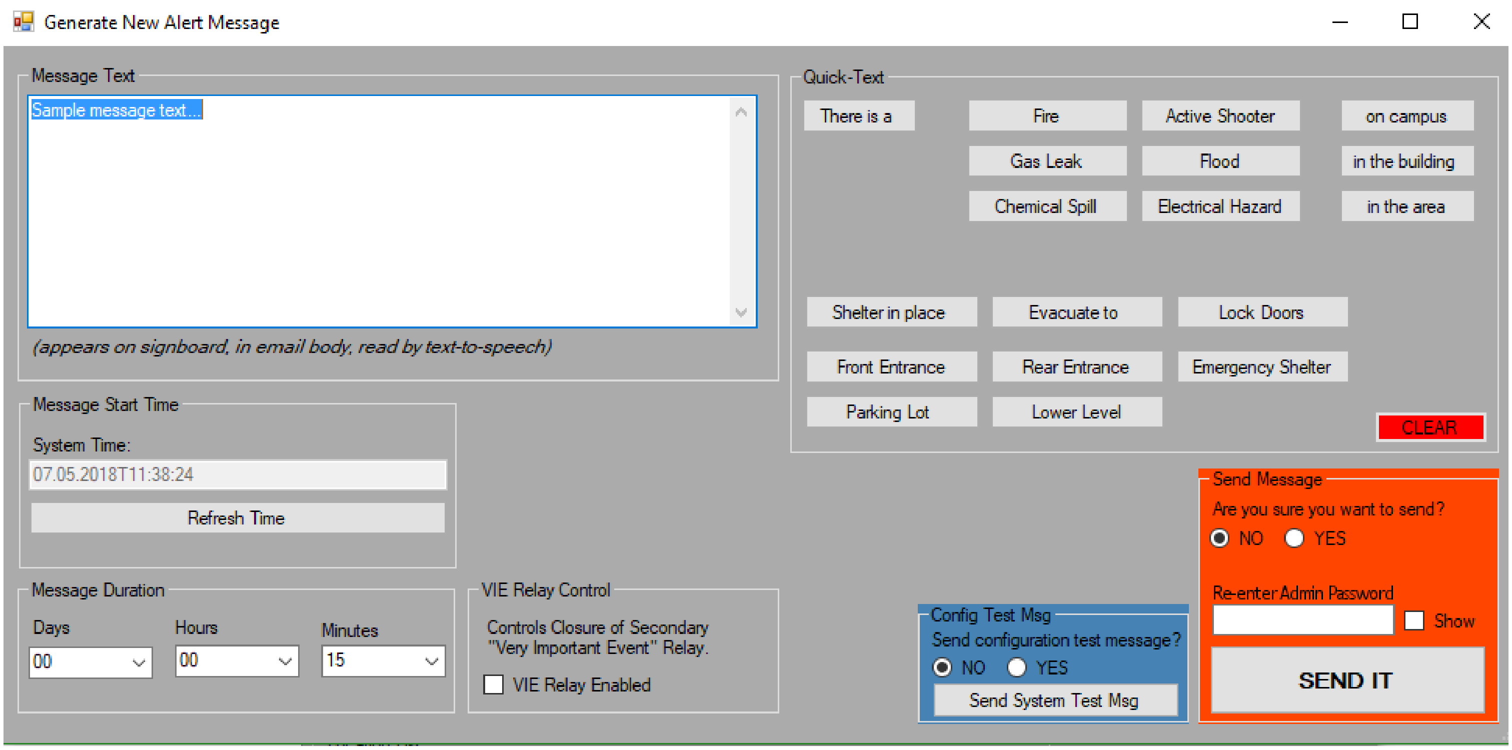
If you accidentally add a location that you do not want, or if you simply wish to stop receiving messages for a location in your audience area, you can remove that location from your list.

To do so, click the location in the *My Audience* list to highlight its line and then click *Remove Selected County from Audience*, or double-click the location line in the list.

Generating Alerts Locally

Typically, messages processed by the CAPWATCH unit will be those generated by and received from NOAA/NWS via their CAP alert feeds. However, users may wish to locally generate their own messages to be processed – either to notify building occupants of a local emergency that the NOAA/NWS may not cover (such as fire, chemical spill, attack, or other situation) or simply to test their system or perform a drill.

Messages can be generated in the CAPWATCH SENTRY software from the interface accessed by clicking the *Generate Local Alert* button from the main interface window.



Generate New Alert Message

Message Text: Sample message text...

(appears on signboard, in email body, read by text-to-speech)

Message Start Time

System Time: 07.05.2018T11:38:24

Message Duration

Days: 00 Hours: 00 Minutes: 15

VIE Relay Control

Controls Closure of Secondary "Very Important Event" Relay.

☐ VIE Relay Enabled

Config Test Msg

Send configuration test message? ● NO ○ YES

Send Message

Are you sure you want to send? ● NO ○ YES

Re-enter Admin Password

☐ Show

Message Text

From this window, the user can enter the text of their alert in the *Message Text* box. The text entered here will appear on text crawls and signboards, in the body of notification emails, and read by TTS if these options are enabled.

Quick-Text

To facilitate faster entry of message text, a number of Quick-Text buttons are available. Clicking these buttons will add the indicated word(s) to the Message Text at the cursor position.

Clicking the CLEAR button will delete all of the Message Text.

Message Start Time

The message start time is initially set to the time that the *Generate Local Alert* window opened. If you would like to update the start time before sending the message (such as if it took a long time to enter the rest of the message properties), you can click the *Refresh Time* button.

Message start times in the future may not be entered.

Message Duration

Duration of the event addressed by the message may be entered as number of days, hours, and minutes from the message start time.

VIE Relay Control

The Very Important Event relay control option indicates whether or not this locally-generated message should be treated as a VIE, thereby closing the secondary VIE relays during message processing.

Secondary VIE relays are an optional feature of the CAPWATCH and may not be installed or enabled on all CAPWATCH units.

Sending the Message

Activating the CAPWATCH system to send out an alert message is no small mater and should be taken seriously. To ensure that messages are not accidentally or maliciously sent out over the configured notification channels, several security measures are in place.

Are You Sure You Want to Send this Message?

To enable sending of the generated message, the user must first switch the selected radio button from NO to YES. Unless the YES selection has been made, the message will not be sent. If a user attempts to click the SEND button without indicating that they are sure they want to send it, they will receive a warning to that effect.

Re-Enter Administrator Password

The CAPWATCH administrator password must be entered before sending any locally generated message, even if the option to disable the password requirement for accessing additional interfaces has been selected.

Note that if the option to disable the password requirement for accessing additional interfaces has been selected, a user may be able to access the site setup interface and view or change the administrator password, thus allowing them to send a message. For that reason, it is not recommended to enable this option and, if it is enabled for convenience of configuring the unit, to then disable it once configuration is complete.

Configuration Test Messages

Proper configuration of the CAPWATCH SENTRY software may be tested and verified by sending a configuration test message using the controls highlighted in blue in the Generate Message dialog.

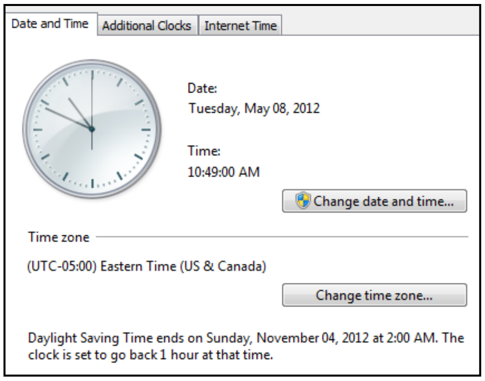
Before a configuration test message can be sent, the safety radio button for “*Send configuration test message?*” must be changed from NO to YES to ensure that you are intentionally sending the test message.

Clicking the “*Send System Test Msg*” button will enqueue a test message for distribution through the configured channels, which may include relay audio interrupt, alert tone audio output, text-to-speech (TTS) audio output, digital signage display, email notification, printed notifications, and others. The alert message will consist of verbiage indicating that the message is for configuration testing only and the test will <u>not</u> activate the VIE relays.

Ensuring Correct Clock Settings

To ensure correct calculation of alert expiration dates and valid time periods, it must be ensured that the unit is properly configured with the correct date, time and time zone settings.

To do this, left mouse click on the clock in the lower right of the CAPWATCH display and choose “Change date and time settings…” From within the resulting display (shown at right), ensure that the correct date, time and time zone are set. After the initial setting, the unit will automatically sync via the internet to ensure that the clock stays accurate.



Date:
Tuesday, May 08, 2012

Time:
10:49:00 AM

Time zone
(UTC-05:00) Eastern Time (US & Canada)

Daylight Saving Time ends on Sunday, November 04, 2012 at 2:00 AM. The clock is set to go back 1 hour at that time.

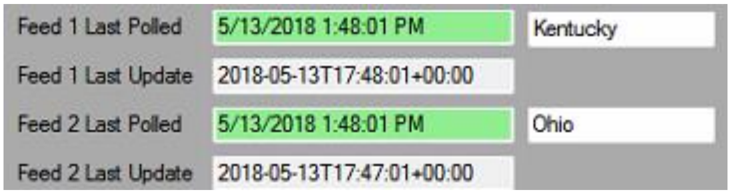
CAPWATCH Operation

Once the unit is properly configured as described above, the keyboard, video monitor and mouse used for configuration is no longer required. These items, however, may remain connected for monitoring, future configuration and local log access. Monitoring and configuration may also be achieved by use of an optional KVM switch, VNC technology or other remote access tools (may require additional setup and/or hardware). Operation begins automatically upon unit power-on, boot up and initialization delay.

The CAPWATCH will poll the specified CAP alert feeds and attempt to process new alerts as described below at a periodic interval. Alert summary logs, original XML CAP alert files and attached resource files are stored locally in the AlertNOAA directory at the root of the storage device

Alert Feed Polling

The CAPWATCH software will periodically poll the specified alert feeds to check for new messages. Information about the polling status will be displayed on the main software dialog as shown below.



Feed 1 Last Polled	5/13/2018 1:48:01 PM	Kentucky
Feed 1 Last Update	2018-05-13T17:48:01+00:00	
Feed 2 Last Polled	5/13/2018 1:48:01 PM	Ohio
Feed 2 Last Update	2018-05-13T17:47:01+00:00	

For each feed, the display will indicate which state the feed addresses, the last time that the CAPWATCH successfully polled that feed, and the last time that the feed was updated.

If you notice that last poll time is more than several minutes old, is highlighted in RED or YELLOW, or if you receive email notification of connectivity issues, please check your internet connection.

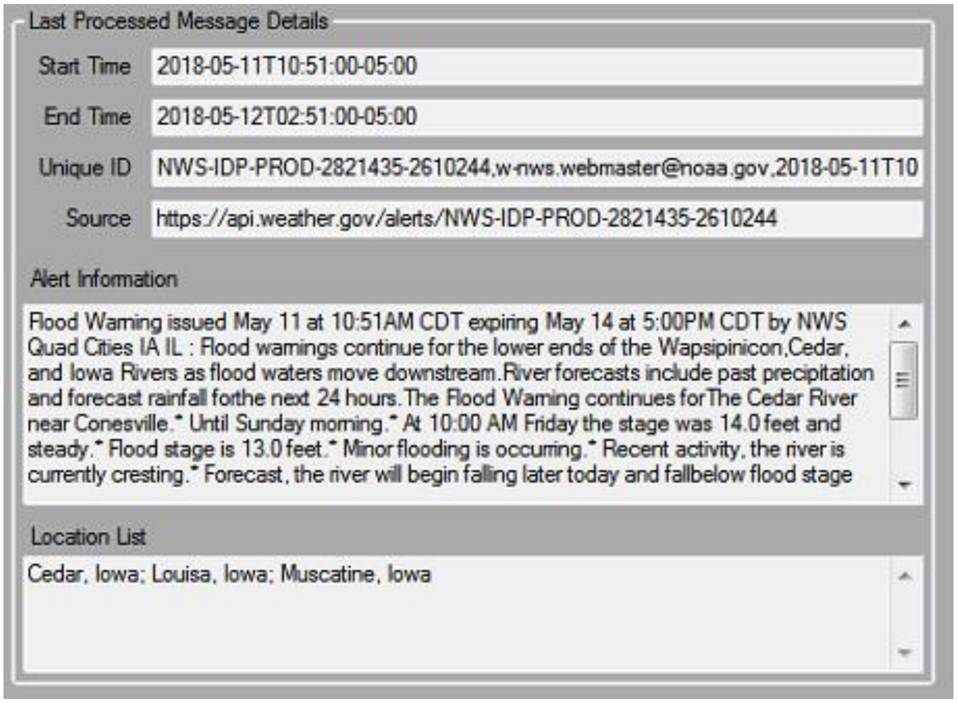
Note that the last feed update time may not change frequently if there is not much weather activity in the area.

Alert Message Processing

Once an alert has been received, the CAPWATCH will verify the alert's validity. First, the unit will verify that the message conforms to Common Alerting Protocol v1.2 specifications and the Integrated Public Alert and Warning System (IPAWS) Profile specifications. If the alert message passes this verification step, the message expiration time is checked to ensure that the alert is current. Finally, the received message is checked against the user-configured filters to ensure that it is within the targeted area and is a selected event type. If the message passes all of these checks, processing continues.

On-Screen Message Detail Display

When a message is successfully processed, details of the associated event are displayed on the main interface window in the *Last Processed Message Details* section. These details include the message start time, message end time, the unique identifier of the message, the source of the message, alert information (comprised of the CAP message's Headline, Description, and Instruction fields), and the list of locations impacted by the message.



Last Processed Message Details

Start Time 2018-05-11T10:51:00-05:00

End Time 2018-05-12T02:51:00-05:00

Unique ID NWS-IDP-PROD-2821435-2610244,w-nws.webmaster@noaa.gov,2018-05-11T10

Source https://api.weather.gov/alerts/NWS-IDP-PROD-2821435-2610244

Alert Information

Flood Warning issued May 11 at 10:51AM CDT expiring May 14 at 5:00PM CDT by NWS Quad Cities IA IL : Flood warnings continue for the lower ends of the Wapsipinicon,Cedar, and Iowa Rivers as flood waters move downstream.River forecasts include past precipitation and forecast rainfall forthe next 24 hours.The Flood Warning continues forThe Cedar River near Conesville.* Until Sunday morning.* At 10:00 AM Friday the stage was 14.0 feet and steady.* Flood stage is 13.0 feet.* Minor flooding is occurring.* Recent activity, the river is currently cresting.* Forecast, the river will begin falling later today and fallbelow flood stage

Location List

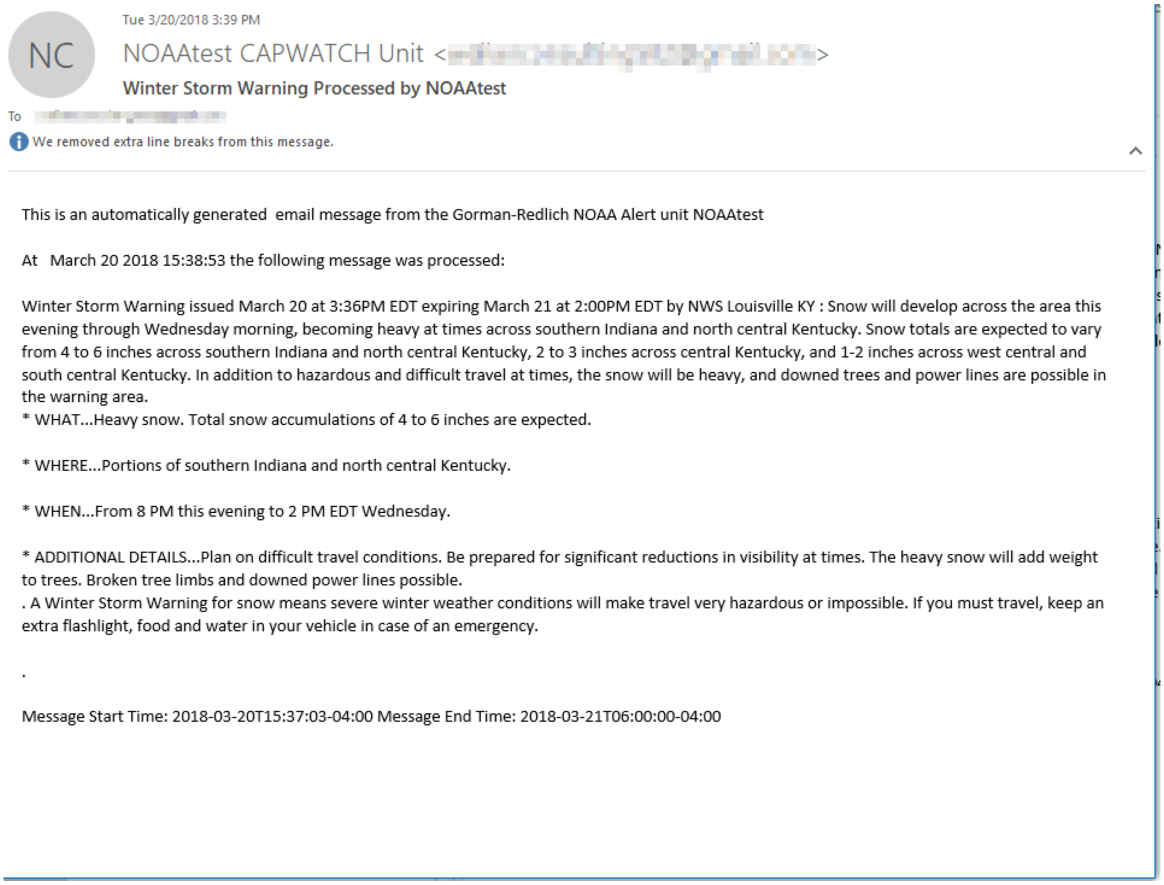
Cedar, Iowa; Louisa, Iowa; Muscatine, Iowa

Processed Message List

In addition to the alert detail display as described above, an overview of the most recently processed messages will be displayed on the left side of the main CAPWATCH SENTRY window. Due to the narrow width of the list window, it will likely be necessary to use the horizontal scroll bar at the bottom of the list to view the entire message entry.

Email Notifications

If enabled, the CAPWATCH will send email notifications to the configured alert notification recipient(s).



Tue 3/20/2018 3:39 PM

NOAAtest CAPWATCH Unit <[redacted]>

Winter Storm Warning Processed by NOAAtest

To [redacted]

We removed extra line breaks from this message.

This is an automatically generated email message from the Gorman-Redlich NOAA Alert unit NOAAtest

At   March 20 2018 15:38:53 the following message was processed:

Winter Storm Warning issued March 20 at 3:36PM EDT expiring March 21 at 2:00PM EDT by NWS Louisville KY : Snow will develop across the area this evening through Wednesday morning, becoming heavy at times across southern Indiana and north central Kentucky. Snow totals are expected to vary from 4 to 6 inches across southern Indiana and north central Kentucky, 2 to 3 inches across central Kentucky, and 1-2 inches across west central and south central Kentucky. In addition to hazardous and difficult travel at times, the snow will be heavy, and downed trees and power lines are possible in the warning area.
* WHAT...Heavy snow. Total snow accumulations of 4 to 6 inches are expected.

* WHERE...Portions of southern Indiana and north central Kentucky.

* WHEN...From 8 PM this evening to 2 PM EDT Wednesday.

* ADDITIONAL DETAILS...Plan on difficult travel conditions. Be prepared for significant reductions in visibility at times. The heavy snow will add weight to trees. Broken tree limbs and downed power lines possible.
. A Winter Storm Warning for snow means severe winter weather conditions will make travel very hazardous or impossible. If you must travel, keep an extra flashlight, food and water in your vehicle in case of an emergency.

.

Message Start Time: 2018-03-20T15:37:03-04:00 Message End Time: 2018-03-21T06:00:00-04:00

The configured Unit ID will appear as the recipient name, as well as in the email subject line and message body. This is useful for users who manage multiple CAPWATCH units to distinguish between which unit has processed alerts.

The message sender address will be the one configured in the Site Setup interface. To avoid having notification messages end up in a "junk" or "spam" folder, it is recommended to add this address to your email whitelist.

The email body will contain details such as when the message was processed, the Headline, Description, and any Instructions associated with the alert, the message start time, and the message end time.

Audio Output

Depending on the installation and setup of the CAPWATCH, there are multiple audio output options. Audio may be available from the 3.5mm stereo plug or the audio/relay header on the rear of the unit.

If Alert Start Tones are enabled, a brief attention tone will play at the start of message processing to signal that an alert is incoming.

Then, if Text-to-Speech (TTS) is enabled, the alert details will be spoken by TTS.

Finally, if Alert End Tones are enabled, a brief tone will play to indicate the end of the message.

Relay Contact Closure and Audio Interrupt

If *Interrupt Relays* are enabled in the Site Configuration, the primary relays will close during message processing. The relays will close before the start tones (if enabled) and remain closed until after the end tones (if enabled). This functionality occurs for all successfully processed alerts.

The primary relays can be used to provide a contact closure to external equipment, such as warning sirens, emergency lighting, or PA systems, or to interrupt audio that is looped through the header plug on the rear panel of the unit.

An optional secondary relay may be available on your unit. This relay, if installed and enabled, will provide a contact closure (opening and closing at the same time as described above) only for messages configured as Very Important Events (VIE). Enabling and configuration of the secondary relay feature is done only at the factory.

Message Text Output for Digital Signage and Video Crawls

As messages are successfully processed, if the *Text Crawl* option is enabled and correctly configured, the CAPWATCH unit will output the alert detail text over RS232 serial data from the configured COM port in the configured output format. See the Site Setup section on Text Crawl for details of those formats.

The message text that is output consists of the message Headline, Description, and Instruction as provided from NOAA/NWS for received alerts and for the entered message text for locally generated alerts.

The text included in the body of email notifications, RS232 output, and that read aloud by TTS will all be identical in order to be consistent and avoid confusion.

Printing

If the print option is enabled and a USB or networked printer is correctly installed and configured for the CAPWATCH unit, a print log containing message details will be sent to the unit's default printer. Please refer to your printer's documentation for installation and configuration instructions.

NOTE: *If no physical printer is installed or configured on the unit, the default printer may be a "software printer" that prints documents to a file. These types of printers may require user interaction to complete the "print" job (such as providing a filename) which may cause the software to be unresponsive until such user input is received. <u>DO NOT enable the print option unless you have correctly configured a printer.</u>*

Logging

In addition to the email and print logging capabilities described above, the CAPWATCH maintains local logs of its activity, including software boot, message processing, connectivity issues, and more. Logs are stored in the root of the unit's main storage device in the *AlertNOAA* directory.

Backing Up and Clearing Log Files

From time to time, it may be desirable to back up log files for long term storage or to clear log files to save space on the local storage device. *Please note that it is the user's responsibility to be aware of any record keeping and message log requirements and ensure compliance with them.*

Users may find the log files as described above by navigating to the *C:\AlertNOAA\logs\* directory on the unit's local storage. Log filenames indicate the month and year that they represent

To backup log files, select the desired log file and the *log* directory and copy/paste them to your desired storage device, such as a USB jump-drive, external hard drive or network location. Log files that are no longer needed may be deleted by right-clicking on the file and selecting "delete."

GORMAN REDLICH

257 West Union St.

Athens, Ohio 45701

Ph: 740-593-3150

www.gorman-redlich.com