
# Stealth and Watchdog User's Guide

# Manitou Stealth and WatchDog ser's Guide

## © Copyright 2012 Bold Technologies LTD



Reference Number: SWD_UG_r2
Date of Issue: April 2012

---

***Bold Technologies Ltd***
***421 Windchime Place***
***Colorado Springs CO 80919***
***USA***

***Phone: +1-719-593-2829***
***Toll Free US 1-800-255-2653 (BOLD)***
***Fax: +1-719-599-3953***
***Email: sales@boldgroup.com***
***support@boldgroup.com***

### Acknowledgements

**Publisher**
*Bold Technologies, Ltd.*

**Author**
*Bold Technologies*
*Technical Writer*

# Stealth & WatchDog for Manitou

Bold offers additional modules to improve efficiency and allow for more control within the Manitou monitoring system, including the Stealth Logger and WatchDog.

- Stealth Logger and Viewer provide an easy way to take your central station paperless, saving money and the environment. Stealth Logger replaces your impact printers that capture receiver output and consume paper at an overwhelming rate. Stealth Logger also lets you monitor signal traffic, receiver and line usage in a convenient graphical display. Plus, Stealth Logger data is stored separately from the Manitou database, providing another protection against data loss.

- WatchDog monitors all of the system functions and resources and receives reports of any warnings, errors, or failures.

# Introduction

This document contains information and instructions on how to use Stealth Logger and Stealth Viewer with the Manitou Alarm Monitoring system and other automation systems, as well as configuring Manitou for use with WatchDog.

# How to Use this Guide

This guide has been created with the intent for one topic to flow in to the next and is meant to be viewed as a .pdf or in electronic form. Incorporated herein are overviews, key terms and definitions as well as numerical, step-by-step instructions on how to perform different tasks in Stealth and WatchDog as well as setup certain functions.

Occasionally, a bullet arrow will be used to designate when only one step is needed to perform an action. In addition, certain icons and standard formatting have been applied to help get the most out of the document's content.

## Formatting Key

| Formatting | Used for |
|---|---|
| ‹Bolded› | Bolded letters in brackets refer to actual keys on the keyboard. |
| *Italicized* | Italicized words indicate certain titles within the software such as window names, etc. as well as to provide emphasis on certain words. |
| **Bolded** | Bolded words are used to signify important data, action paths and software buttons such as **OK** or **Jump To** menu/**Workflow**. |

# Icon Key

| Icon | Used for | Description/Formatting example |
|---|---|---|
|  | Recommendation/Idea | *Suggestions to enhance usage of software functions and features.* |
|  | Valuable Information | *Any type of information deemed to be valuable such as subject notes and additional information pertaining to the subject matter.* |
|  | Warning/Caution | **Reminders of things NOT to do or to be careful and/or aware of.** |
| | ***Example*** | Provides examples to further explain topics or steps. |

# UL Compliance for Printerless Environments

A central-station is not prohibited from using computer equipment (event loggers) to record signals received on receivers, in lieu of printers that are connected to or are part of receiving equipment, when the following conditions are met:

- Computers used for this purpose shall be redundant;
- In the event of failure of either the primary or back-up computer, there shall be an audible or visual indication within 90 seconds of the failure. The signal shall be obvious to the operator/ responsible central-station staff. In addition, the central-station staff shall be capable of, and the back-up computer shall be ready for, switching over within 30 seconds so that the back-up computer is energized and connected to the affected receivers.
- The primary and back-up computers shall be isolated from the automation system computer/s (i.e., these computers shall not be configured in such a way that the signals from the receivers that are intended to be transmitted to the automation system computer/s have to first pass through the primary and back-up computers).
- The primary and back-up computers shall have transient protection as required in Electrical Transient Protection, Section 7 of the Standard for Central Station Automation Systems UL 1981.
- The communication lines between the computer and the receiver must be supervised so that, within 90 seconds, a distinct audible or visual trouble signal indicates the occurrence of a single break, a single ground-fault condition, or a short circuit that prevents the required operation of the computer.
- The captured signals must be retrievable upon demand in a maximum of 5 seconds.
- Signals must be presented, at a minimum, in the same manner as they would be by receiver printers.
- **All printer connections to Stealth Logger shall have the printer output enabled at all times to capture events and provide necessary electrical supervision for UL.**
- **WatchDog must not be disabled for UL applications.**

## Environmental Controls

Hardware shall be located in an environment where the temperature is maintained at a level within the temperature rating range of the equipment.

## HVAC Standby Power

The HVAC system shall have 24 hours of standby power. The standby power for the HVAC shall be provided by the central station's engine-driven generator(s). If the central station chooses to do so, it may provide the standby power for the HVAC system by an uninterruptible power supply (UPS), or the like.

Exception: When the hardware is rated for use in environments with temperatures between 32EF (0EC) and 120EF (49EC), 24 hours of standby power is not required for the HVAC system.

## Source of Power

- Hardware shall be powered by a UPS that complies with either the Standard for Uninterruptible Power Supply Equipment, UL 1778, or the Standard for Power Supplies for Fire-Protective Signaling Systems, UL 1481.
- In order to perform maintenance and repair service, a means for disconnecting the input to a UPS and output from a UPS while maintaining continuity of power supply to the automation system shall be provided.
- If a power conditioner is being used, it shall comply with the Standard for Power Units Other Than Class 2, UL 1012. In order to perform maintenance and repair service, a means for disconnecting the input to a power conditioner and output from a power conditioner while maintaining continuity of power to the automation system shall be provided.

## Supply Line Protection

The printerless environment hardware primary power source shall be protected by surge protective devices (SPD) that comply with the Standard for Surge/Protective Devices, UL 1449. The SPD shall have as Maximum Continuous Operating Voltage (MCOV) equal to or greater than the normal operating voltage of the system. The SPD Type Designation (Type 1, 2 or 3) must be suitable for the specific installation application.

## Signaling Line Protection

The communications circuits shall be protected by secondary protectors for communications circuits. These protectors shall comply with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B. The transient protectors shall have a marked rating of 50 volts or less.

## Minimum System Configuration

Each separate system (Active, Standby) must contain the following minimum requirements:

### Application/Database Servers

(1) Intel Pentium III 1GHz processor
(1) 1GB RAM
(1) 18GB IDE HD
(1) CDROM drive
(1) Floppy drive

### Workstations

(1) Intel Pentium III 500Mhz processor
(1) 256MB RAM
(1) 20GB IDE hard drive
(1) Soundcard and speakers
(1) CDROM drive

### Serial Concentrator

(1) Digi EtherLite or similar serial product

### Ethernet

10/100baseT Ethernet switches with enough ports for each server, workstation and serial concentrator plus room for growth
Cat 5 twisted pair wire to each server, workstation and serial concentrator

## Signal Event History

In accordance with UL 827 (The Standard for Central Station Services) and NFPA 72, all signal event history (known as records) shall be retained for one year and available upon demand. Manitou can provide these records which are kept on the local alarm monitoring servers or archived on medium. Since Stealth uses a similar database for storage of history files, these records need to be kept for a period of 1 (one) year. If the hard disk drives are not capable of handling records for this period, then routine backup of the database/event records may be required.

Stealth Logger only needs to comply with this requirement (signal event history records) when there is a failure with automation and signals are being handled from the printerless environment system, meaning Stealth Logger. Additionally, Bold Technologies, Ltd. requires or advocate database backups.

## Software Version

1. To display the software version, go to *C:\Program Files\Bold Technologies\Stealth Logger*.
2. Right click on the .exe file.
3. Click on **Properties**.
4. Click on the *Version* tab.

The File Version will list the version that is currently installed on the machine.

**UL certified Central Stations are required to employ BOLD WatchDog software or the SPE WatchDog timer hardware. When using the Bold WatchDog software, Alerting CPUs may not use a screen saver with this program.**

# Stealth

## About Stealth Logger

The Manitou Stealth Logger application is designed to monitor and log any activity provided via TCP, UDP, or Serial connections. Additionally, the Stealth Logger tracks signal activity trends and resource usage. It is a source for backup data in case the main automation system has a critical failure.

The WatchDog component of Stealth Logger monitors communication from Manitou, the Application Server, Signal Handler, Marshaller, FEP (Front End Processor) or other predefined system prompts in Manitou. If any component fails, the WatchDog will alert the Operator so alarms may be handled manually as necessary.

In turn, the Stealth Logger will monitor the state of the WatchDog, and is programmed to print out signal information in the event of a failure. This protects against data loss or signals being overlooked during any failure of the main automation system components.

All activity monitored by the Stealth Logger is stored in its own database, separate from other Manitou data. Instructions and details about implementing the Stealth Logger and its database appear in the sections below.

## Features Summary

The Stealth Logger contains several features for specific uses:

- Numerous views for observing data.
- Query tools in Stealth Viewer.
- Ability to set up several workstations and devices.
- WatchDog mode.
- Send manual events.

# Overview

## Configuration

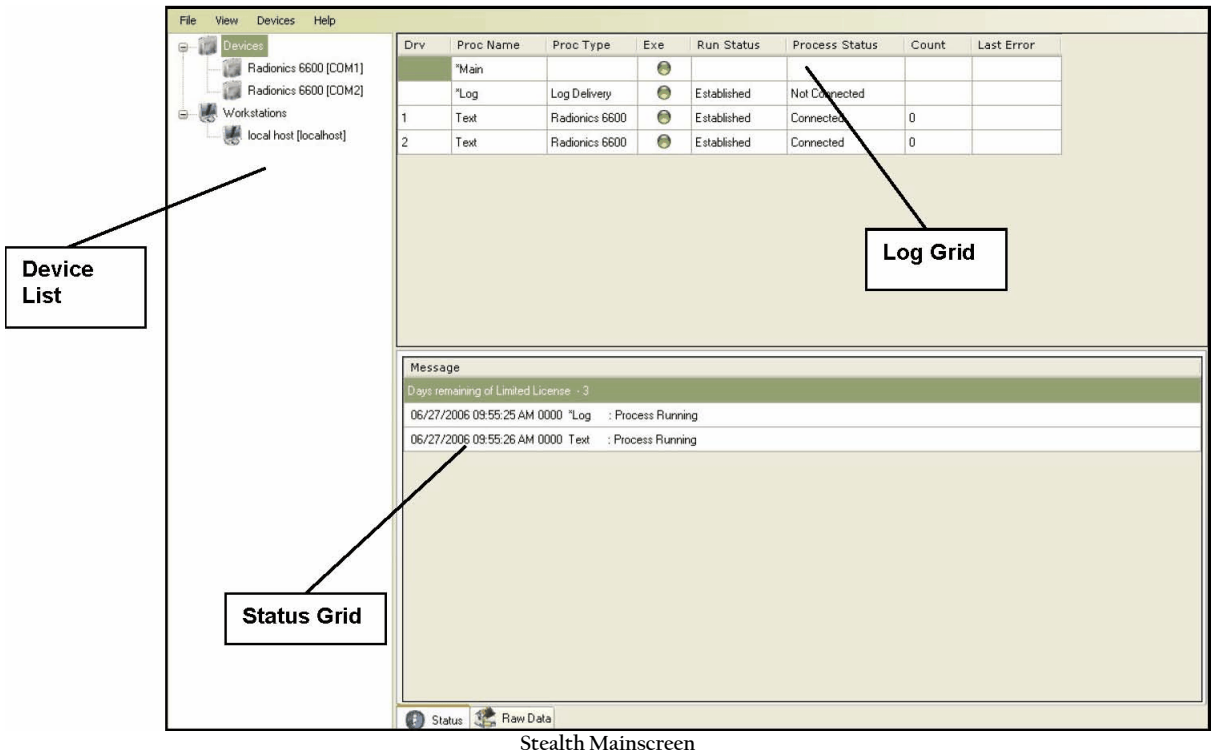
The Stealth Logger monitors the output of all configured Devices. That activity is stored in its own database and made available for searches and printed output. The configuration of the Stealth Logger includes connectivity to the receivers, WatchDog, and a printer. Additional configuration is done through the Stealth Logger interface, so that the software recognizes all monitored Devices. System configuration details appear below.

The Stealth Viewer is a separate program used in conjunction with the Stealth Logger. Users can view receiver activity in several graphs, search for specific data, and monitor activity, as well as print reports.

**UL certified Central Stations are required to employ a workstation for audible and visual notification. This workstation may not use a screen saver with this program. Server failure is displayed in the Stealth Viewer Software.**

## Screen Description Overview

When Stealth Logger is running, several grids, lists and other options are displayed.




Stealth Mainscreen

**Device List** – The Device Lists displays all Devices and Workstations added and monitored by Stealth Logger. Log Grid- Displays information on the monitored Devices Log code

**Status Grid** – Displays messages received (e.g. processes starting or WatchDog alerts).

# Devices

Rather than being connected to a line printer, each receiver's printer output is sent to the Stealth Logger. Serial printer output can be connected directly to the Stealth Logger server. Parallel printer output requires the use of a parallel to serial converter. Each connected Device is also added and configured through the Stealth Logger interface on the Device Setup Tab based on settings required by the individual Device. The Stealth Logger may then be connected to a printer in case the need for physical printed output arises.

When the Stealth Logger runs, it will create the required tables and begin inserting data into the database. Every line of output from monitored devices will be logged into this database and will be available for searching through the *History* tab in the application.

# Add a Device

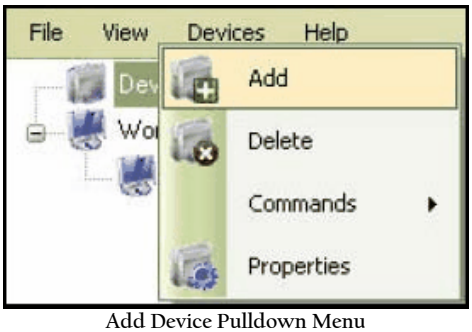
To begin logging receiver activity, a Device must first be added to the program. The Device list is found in the far left column of the screen. This information enables each device and informs the application about what the settings are for each device.

Devices can be added in two ways:

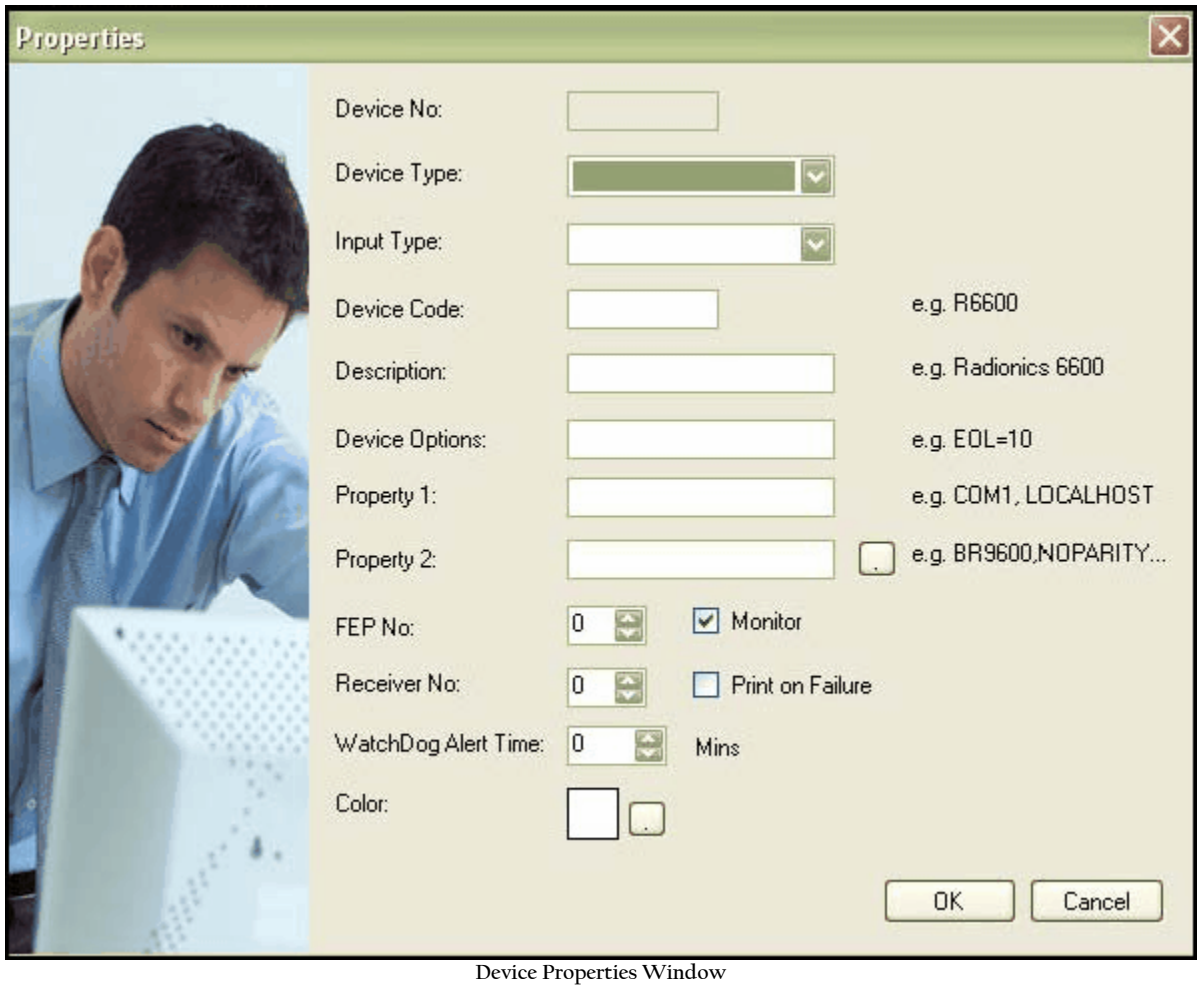
1. From the *File* menu, select **Add a Device.**


Add a Device

2. Right-click on the Device icon. Once a Device is added, a Properties window is displayed.




Add Device Pulldown Menu




Device Properties Window

The Properties screen contains several required fields for adding a Device, including, but not limited to:

- Device Type
- Input Type
- Device Code
- Description
- Device Options
- WatchDog Alert Time
- Print on Failure
- Color

## Device Type

The Device Type field indicates the type of document the logger will read (ex: a text document).

- Select **Text** from the drop-down menu. Once the Input Type is selected, several fields on the *Properties* window will change.
- Once the *Device Type* field is selected, several fields in the *Properties* window will change.

If a Device Type is not selected, an error will occur.


Device Type Error

➢ Click **OK** to return to the *Properties* menu, and select an **Input Type** from the drop-down menu.

## Input Type

There are several forms of Input Types:

- Serial Port: An input/output connection on the computer that allows it to communicate with other Devices in a serial fashion-data bits flowing on a single pair of wires.
- TCP/IP In/Out: Transmission Control Protocol/Internet Protocol. Communication protocol suite and standard for all Internet-connected machines.
- UDP: User Datagram Protocol. Transports data as a connectionless protocol, using packet switching.

*Select the Input Type (Serial Port, TCP/IP In, TCP/IP Out, or UDP). The Input Type in Stealth Logger must match the Input Type of the Device that will be monitored. The Input Type of the Device can be found in the documentation that accompanies the Device.*

If using a TCP/IP connection:

➢ If the Device is acting as a TCP/IP In server, the Stealth Logger Device Input Type should be set up as TCP/IP Out. If the Device is using TCP/IP Out, the Stealth Logger Device Input Type should be set up as TCP/IP In.

*Some fields in the Properties window will change based on the Input Type.*

## Device Code

The Device Code designates the name of the Device that will be identified both by the Stealth Logger and the Stealth Viewer when viewing logs.

- Enter the desired name of the Device Code into the field (ex: LOG3; RR600). This field is limited to six (6) characters.


*No special characters may be used in this field.*

## Description

The Description field is used as a general description of the log.

- Type the desired name of the Description into the field (ex: Security log 1; Radionics 6000).


*No special characters may be used in this field.*

## Device Options

The Device Options indicates the End of Line (EOL) decimal character in each Device. Note that the EOL character in each Device may differ.

**Example:** A particular Device may use EOL=10. This is the ASCII decimal character for new line feed or carriage return.


*In order to utilize the All Events Logger (AEL), the Device Options field must be set to EOL=NULL allows Stealth Logger to utilize the All Events Logger (AEL) with Manitou.*

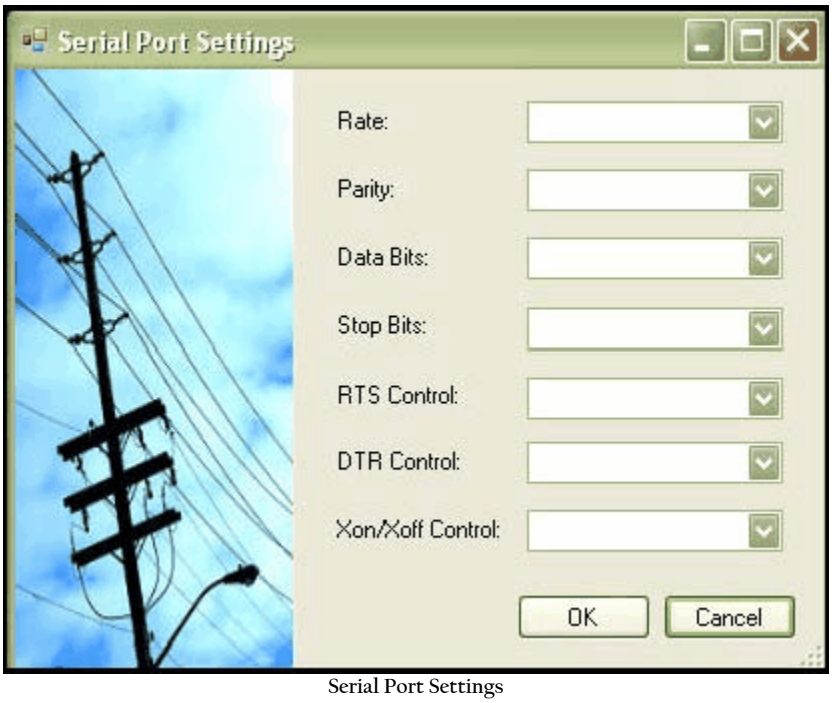
The EOL character has not been set correctly if (a) no data is fed and therefore is not displayed in the Stealth Logger and/or Stealth Viewer, or (b) a significantly large line of data is read by the Stealth Logger. This line of data has been buffered by a maximum character length, and the EOL character must be set in order for the data to be read properly.

## Additional Fields

Depending on the type of **Input Type** selected, several fields may or may not be displayed.

If a Serial Port is used:

1. Enter the Port Name (ex: COM1)
2. Enter the Port Settings. Click on the box next to the Port Settings field to open the Serial Port Settings window.




Serial Port Settings

The Serial Port Settings must match the Device settings. If not already known, the Serial Device settings can be found in the documentation that accompanies the Device.

If TCP/IP Out is used:

- Enter the host name (ex: localhost)

If UDP is used:

- No additional fields are used.

Port No:

- Enter the port number from which the log will read from (ex: 7002).

If using a UDP port:

- The port number will automatically default to the UDP port number.

## FEP No. and Receiver No.

Use the up/down arrows to select the FEP number and Receiver number associated with this Device.

## Monitoring

If the Stealth Logger should monitor activity on this device, check the Monitor checkbox. If, for example, this is a backup device, leave the Monitor checkbox unchecked until this device is in use within the automation system. A Central Station may want to include this type of update to the

Device Details screen as part of the documented backup procedures.

## Print on Failure

Check the "Print on System Failure" checkbox if raw signal data should be sent to a printer and handled by Operators manually in case of system failure. This allows signals to be addressed as they arrive even if a particular receiver is not communicating with Manitou. The Central Station Operator(s) would simply handle those manually.

## WatchDog Alert Time

The WatchDog Alert Time setting can be used to specify periods of time for older receivers to send a signal to WatchDog. In the event that WatchDog does not receive a signal for a specific amount of time, a warning signal will occur from WatchDog to alert Operators.

Users with newer receivers do not need to utilize the WatchDog Alert Time, as signals, or "heartbeats," are automatically sent from the receiver to the WatchDog in regular intervals.

## Color

The Color Picker allows users to associate each Device with a distinct color, so that it is easily discernable in the bar and line graphs on the Graphs Tab in the Stealth Viewer.

- Select the desired color for the current Device and click **OK**.


Color Picker

When finished with the Properties screen, click OK to finish adding the Device entry.

- A pop-up info box will appear, stating the driver needs to be started. Click OK.

The new Device will now appear in the Device list located in the left column of the screen.

### Starting, Stopping, and Re-starting a Device

To quickly start, stop, or re-start the newly added Device, highlight the Device by right-clicking on it, and select the appropriate action.


Device Commands Menu

## Edit a Device

1. Highlight the Device in the Device lists, and left-click on the Device.
2. Click **Properties**.
3. Make changes to fields as necessary.
4. Click **OK** at the bottom of the window to save the new information about the Device.

## Delete a Device

1. Stop the Device if it is running by highlighting the Device, right-click, and select "Stop" from the menu.
2. Right-click on the Device.
3. Click **Delete**.
4. Click **Yes** or **No**.

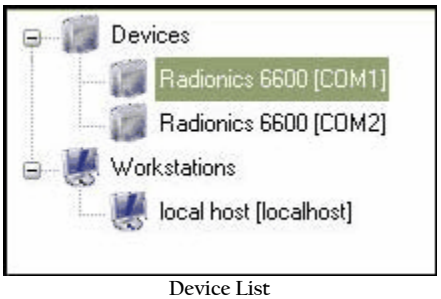
The Device has been deleted. If a Device is removed in error, it will need to be re-added using the Add a Device instructions above.

# Receivers

Logging activity can be turned on or off on any receiver listed within the network.

## Start Logging

Begin logging receiver activity by highlighting the appropriate Device in the Device list.




Device List

1. Click on the *Devices* menu.
2. Select **Start**.
3. Repeat for all Devices that need to begin logging activity.

The Device now logs receiver activity. A successful log is indicated by the lighted green button.

## Stop Logging

1. Stop logging receiver activity by highlighting the appropriate Device in the Device list.
2. Click on the Devices menu.
3. Select Stop.
4. Repeat for all Devices that need to be stopped.

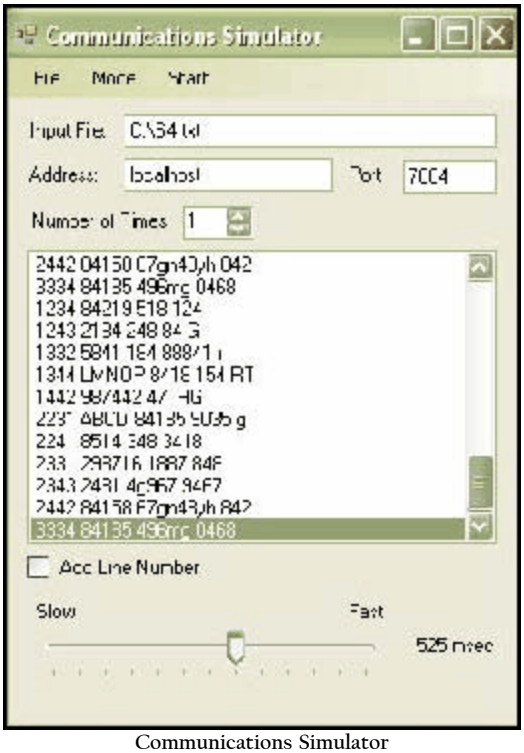
The Device no longer logs receiver activity. A successful stop is indicated by the lighted red button.

| Drv | Proc Name | Proc Type | Exe | Run Status | Process Status | Count | Last Error |
|---|---|---|---|---|---|---|---|
| | *Main | | | | | | |
| | *Log | Log Delivery | | Established | LDP Connected | | |
| 1 | Text | Radionics 6600 | | Normal Closedown | Unknown | 71 | |

Receiver Activity Log

# Testing a Device

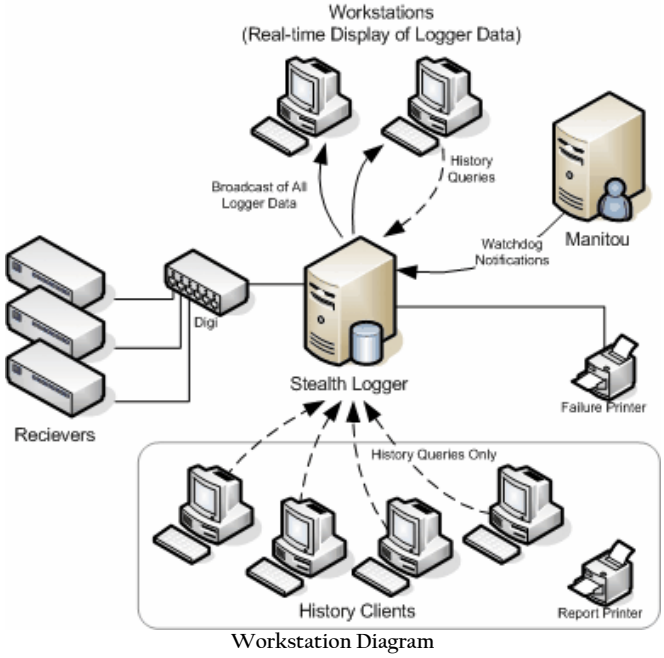
Users may choose to test a Device to ensure that it is set up and logging properly using a Communications Simulator.




Communications Simulator

1. Add a new Device (See page 7 for instructions on adding a new Device).
2. In Stealth Logger, select the test Device from the Device list, and click on the *Devices* menu, and click **Start**.
3. Locate the Communications Simulator and open the program.
4. Select UDP or Serial Port from the *Mode* menu on the Communications Simulator.
5. In the *Input File* field, add a text file to test. This test text file may include any variation of letters or numbers.
6. If using a UDP, add the port number that matches the test Device port number.
7. Indicate the number of times the log should run.
8. Adjust the speed of the test log at the bottom of the Communications Simulator.
9. Click **Start**.

# Workstations




Workstation Diagram

Adding a workstation allows users to utilize the Graphs View in the Stealth Viewer. Several different workstations can be added to Stealth Logger to monitor activity from a different computer than the Stealth Logger server.

*Adding multiple (4+) workstations may cause Stealth Logger and Stealth Viewer to run slower. For example, four workstations will send the same data four times to Stealth Logger.*

## Add a Workstation


Adding a Workstation

1. Go to the *File Menu* › *Workstations*
2. Enter the Station IP address or name.
3. Enter the Station description.
4. Check the "Monitor Watchdog" box if the workstation is going to monitor WatchDog.
5. Check the "Print on Failure" to print to a printer in the event of a WatchDog failure.
6. Click **OK**.

# Add a Manual Event

Adding a manual event allows users to manually send signals to Stealth Logger.

To add a Manual Event:

1. Start the Device.
2. Go to the *File* menu and click on *Manual Signal*.
3. Enter a Manual Signal (ex: 18543 54FR4 8468)
4. Click the **Send** button.

The manual signal has been sent. Both the *Status* tab and the *Raw Data* tab will show the manual signal.

# Login Database

The Login Database allows users to login to the SQL Sever. Stealth Logger will use the SQL Server authentication or the Windows authentication as the login.


SQL Server Login

Enter the *User name* and *Password* to log in to the Stealth Logger database. Click **OK**.

*Checking the Windows Authentication box enables the Server Login to attempt to use the current Windows User name and Password. If the server is located on the machine running Stealth Logger, check this box to use this login.*

If the server is not located on the machine, an error will occur:


Login Error

1. Click **OK** and uncheck the *Windows Authentication* box.
2. Enter the *SQL Sever User name* and *Password*.
3. Click **OK**.

# Startup Options

Users can utilize the Startup Options to start Stealth Logger in normal or Watchdog Mode. To use Watchdog Mode, see Using Stealth Logger in WatchDog Mode .

*Any time a user wishes to switch modes, Stealth Logger must be closed and re-started.*

# Stealth Logger Views

## Raw Data View

The Raw Data View shows the list of incoming signals, during the period that the Stealth Logger is running, as signals are received and logged in the Stealth database. This log shows the Device number, the date and time, and the signal description - raw signal data coming directly from a receiver.

All of the entries appearing in this pane are logged into the database used by the Stealth Logger and are searchable on the *History* tab in the Stealth Viewer.

| No | Date | Signal |
|---|---|---|
| 1 | 6/27/2006 2:12 PM | 5011 181234R15101001 |
| 1 | 6/27/2006 2:12 PM | 5011 181234E15101001 |
| 1 | 6/27/2006 2:12 PM | 5011 181234R13001001 |
| 1 | 6/27/2006 2:12 PM | 5011 181234E13001001 |
| 1 | 6/27/2006 2:12 PM | 1011 0000 A 15 |
| 1 | 6/27/2006 2:12 PM | 1011 0000 A 13 |
| 1 | 6/27/2006 2:12 PM | 1011 0000 A 11 |
| 1 | 6/27/2006 2:12 PM | 1011 0000 A 07 |
| 1 | 6/27/2006 2:12 PM | 1011 1234 9 001 |
| 1 | 6/27/2006 2:12 PM | 1011 1234 8 001 |
| 1 | 6/27/2006 2:12 PM | 1011 1234 7 001 |
| 1 | 6/27/2006 2:12 PM | 1011 1234 6 001 |
| 1 | 6/27/2006 2:12 PM | 1011 1234 5 001 |

Raw Data

## Status View

The Status View displays messages received during logs. All activity that is logged is marked in the messages area.

# Stealth Viewer

When Stealth Viewer is running, several graphs, lists and other options are displayed.

## Graphs Tab

Stealth Viewer has two tabs to view receiver data. The *Graphs* tab displays in different formats all of the current system information within a number of different areas.

### Graphs Displays

**Receiver Data** - The receiver data displays the raw data received by Stealth Logger.

**Bar Graph** – Provides a visual display of the number of signals received on each Device.

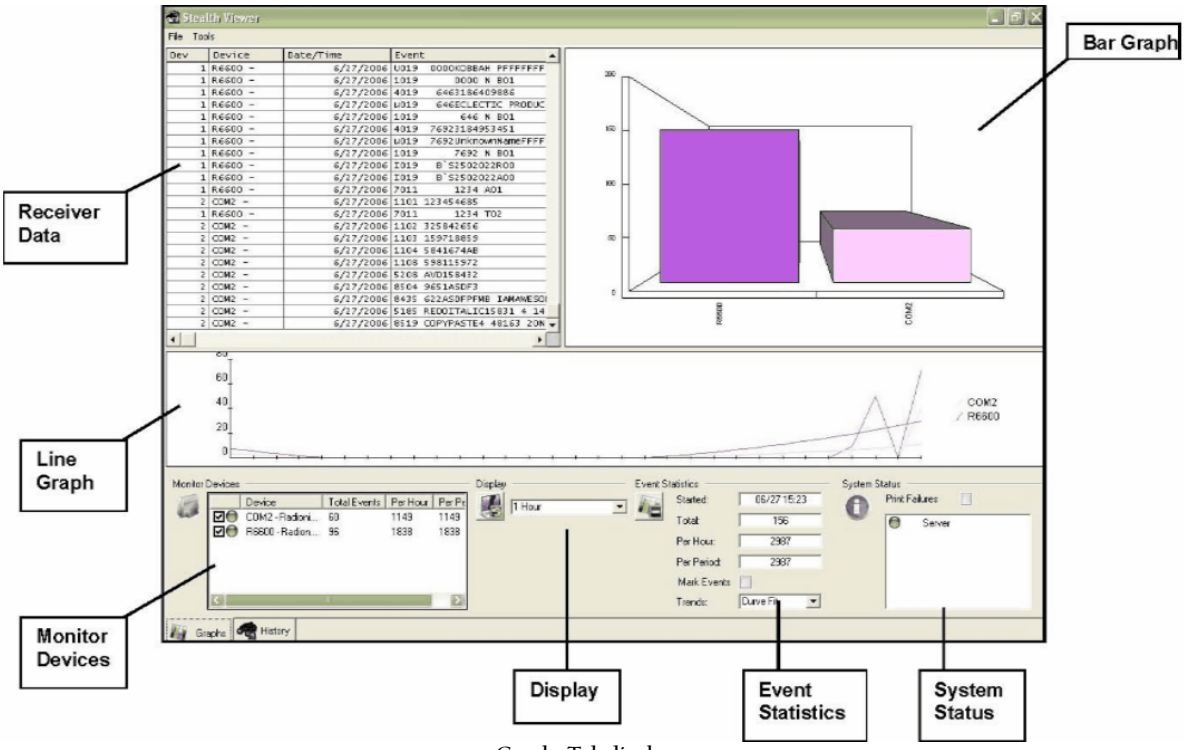
**Line Graph** - Displays a line graph of number of signals over time.

**Monitor Devices** - Displays a list of all Devices added to the Device List and whether or not certain aspects of the Manitou System are running.

**Display** - Allows the user to indicate how many hours or days of activity to display in the graphs.

**Event Statistics** - Displays information about the activity shown on the *Graphs* tab.

**System Status** - Displays whether or not certain aspects of the Manitou System are running.




Graphs Tab display

# Graphs View

The *Graphs View* tab displays an overall summary with both bar and line graphs, the Logger display, system status, statistics, and other various data displays.

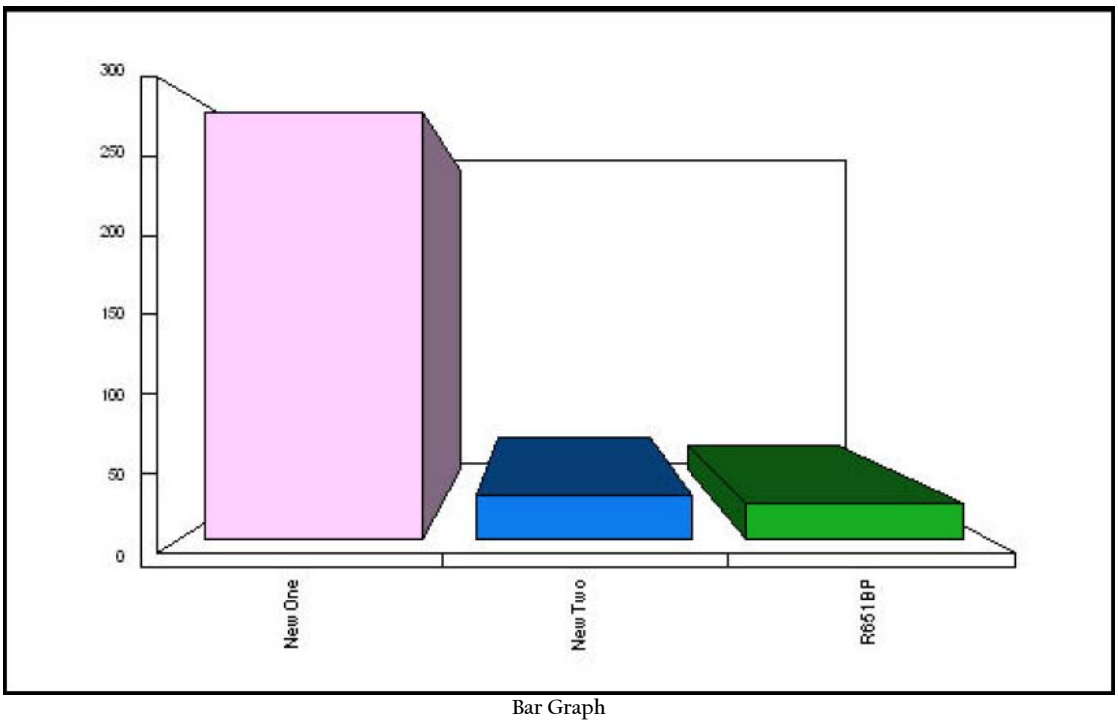
The Logger display in the upper left corner is the list of incoming signals, during the period that the Stealth Logger is running, as signals are received and logged in the Stealth database. This log shows the Device number, the Description for each device, the Date/Time of each signal, and the Event information - raw signal data coming directly from a receiver. All of the entries appearing in this pane are logged into the database used by the Stealth Logger and are searchable on the *History* tab.

## Bar Graph

The Bar Graph pane in the upper right corner of the Stealth Viewer gives a visual display of the number of signals received on each Device since the last time the information on the *Graphs* tab was refreshed. The COM Ports are indicated along the lower edge of this display. When Devices are added and removed, there will appear more or fewer bars in this graph.

Since each of the bars in the graph above corresponds to the activity on a single Device, clicking on any one of the bars in the bar graph limits the line graph and the Raw Data view to display only the activity on that selected Device; i.e. clicking on the blue bar causes the line graph to refresh and show only the activity on that particular Device.

*Clicking again on the same bar/Device refreshes the line graph display to show all Devices.*




Bar Graph

## Line Graph

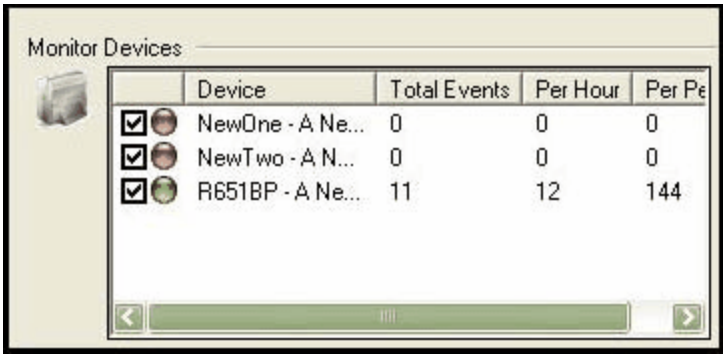
The middle pane of the *Graphs* tab displays a line graph of number of signals over time. This area can be configured to show a period of fewer or more hours or days, depending on preferences. The lines displayed are color-coded to correspond with the Devices being monitored.

Users can view a single device's activity by doing one of the following:

- Click on that device in the bar graph display and wait for the refresh. The bar representing the device will appear selected and the line graph will refresh to show only that device's activity.
- To view all device activity in the line graph, click again on the device in the bar graph. The screen will refresh to show all activity.
- In the Monitor Devices area, uncheck the boxes for devices other than the one to be viewed, and click the **Display Data** button to refresh the screen.
- Check the boxes again to enable the display of other devices, and click **Display Data** to refresh the screen.

## Monitor Devices

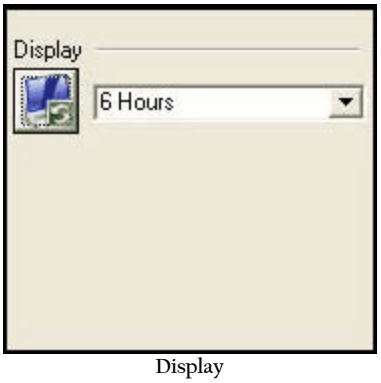
In the lower left corner of the *Graphs* tab is the Monitor Devices list. This area displays a list of all Devices added to the Device List and whether or not certain aspects of the Manitou System are running. Checking and unchecking the boxes in this display affect the information shown in the other areas of this tab - e.g.: Logger, Bar Graph, or Line Graph.




Monitor Devices

## Display

The Display area on the bottom of the *Graphs* tab allows the user to indicate how many hours or days of activity to display in the Bar Graph and Line Graph on this tab. Regardless of the time period indicated, the history remains stored in the Stealth database, and is searchable on the *History* tab. The time period selected here affects the display within the graphs only.



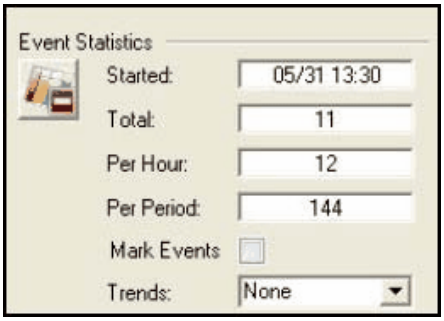

Display

To display a specific time period:

1. Select the desired time.
2. Click on the **Refresh Data** button.

## Event Statistics

The Event Statistics area of the *Graphs* tab displays information about the activity shown on this tab. The Started field shows when the graphs on this screen were last reset to show recent data. The other fields show how many Total signals are currently displayed, how many signals Per Hour are estimated or averaged, and how many signals Per Period are estimated.




Event Statistics


Clicking on the **Reset Data** button will reset the Event Statistics back to zero.

## Mark Events

The Mark Events checkbox highlights each line in the Logger area with the color selected on the *Devices* tab for each device. The resulting multi-color display color codes each line of activity.

| Dev | Device | Date/Time | Event |
|---|---|---|---|
| 1 | R6600 - | 6/27/2006 | I019 BpS309D0106A88 |
| 1 | R6600 - | 6/27/2006 | 1013 1410 30 |
| 2 | COM2 - | 6/27/2006 | 1101 123454685 |
| 2 | COM2 - | 6/27/2006 | 1102 325842656 |
| 1 | R6600 - | 6/27/2006 | 1014 1121 01 |
| 2 | COM2 - | 6/27/2006 | 1103 159718859 |
| 1 | R6600 - | 6/27/2006 | 1014 2817 99 |
| 2 | COM2 - | 6/27/2006 | 1104 5841674AB |
| 1 | R6600 - | 6/27/2006 | 1013 2817 99 |
| 2 | COM2 - | 6/27/2006 | 1108 598115972 |
| 1 | R6600 - | 6/27/2006 | 1014 1357 99 |
| 2 | COM2 - | 6/27/2006 | 5208 AVD158432 |
| 1 | R6600 - | 6/27/2006 | 4019 73063189326878 |
| 2 | COM2 - | 6/27/2006 | 8504 9651ASDF3 |
| 2 | COM2 - | 6/27/2006 | 8435 622ASDFPFMB IAMAWESOI |
| 1 | R6600 - | 6/27/2006 | u019 7306HARDY JIMMYFFFF |
| 2 | COM2 - | 6/27/2006 | 5185 REDOITALIC15831 4 14 |
| 1 | R6600 - | 6/27/2006 | u019 7306HARDY JIMMYFFFF |
| 2 | COM2 - | 6/27/2006 | 8519 COPYPASTE4 48163 20N |
| 1 | R6600 - | 6/27/2006 | 1019 7306 N B01 |
| 1 | R6600 - | 6/27/2006 | 4019 00003183578029 |
| 1 | R6600 - | 6/27/2006 | U019 0000KOBBAH PFFFFFFF |

Mark Events

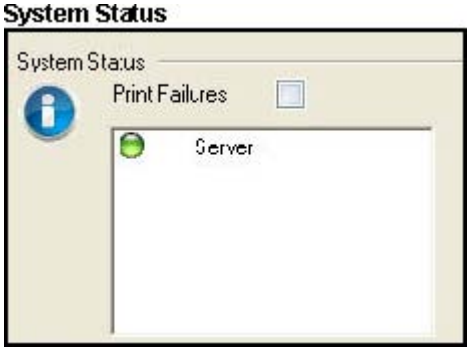
## Trends


Users have the option to view data trends in Stealth Viewer using the Trends drop-down menu in the Event Statistics area: Mean, Minimum/Maximum, Standard Deviation, Best Fit, and Curve Fit.

## System Status

The System Status area in the lower right corner of the *Graphs* tab displays whether or not certain aspects of the Manitou System are running. Red lights indicate that an application is not running or that the Stealth Logger is not connecting to that application.

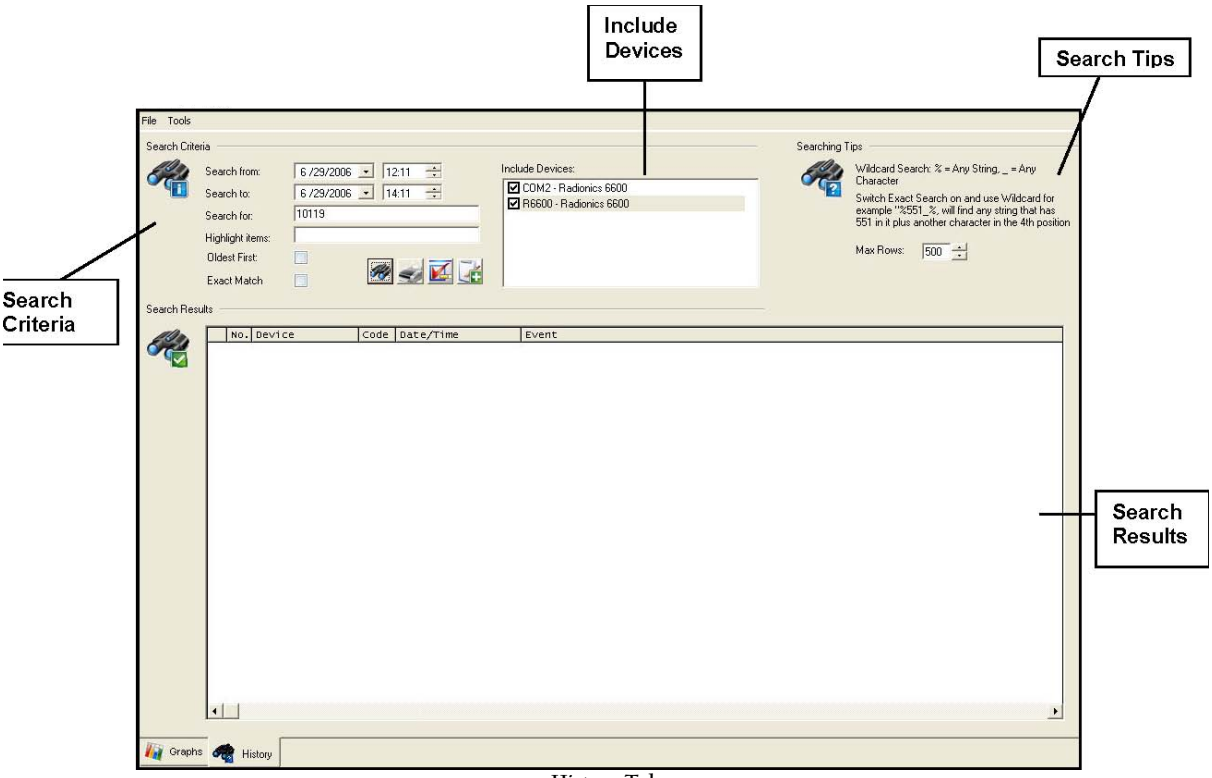
**System Status**




Check the Print Failures checkbox if the raw data from a failed Device (receiver data) should be sent to a selected printer. This allows signals to be addressed as they arrive even if a particular receiver is not communicating with Manitou. The Central Station Operator(s) will simply handle these manually.

# History Tab

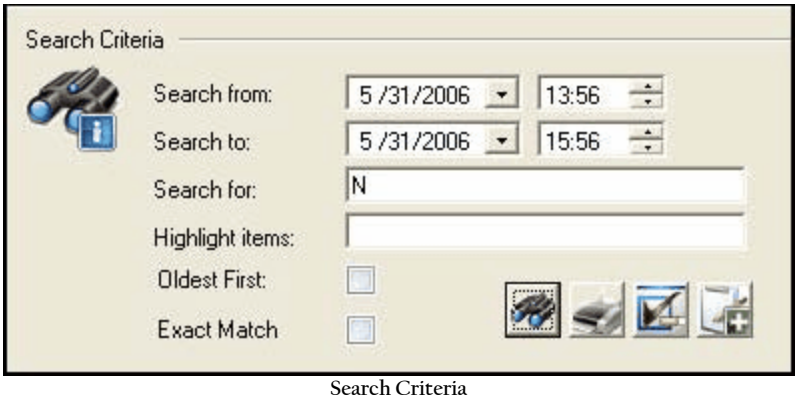
The *History* tab in the Stealth Viewer provides a Search interface for all entries based on date/time, keyword and Device parameters. The Search Results area in the lower portion of this tab displays the signals and activity that match the parameters set in the Search Criteria fields. The following sections provide details and instructions on the *History* tab options.




History Tab

## Search Criteria

The Search Criteria fields allow a user to enter parameters within which to search the data in the Stealth database. Results are displayed below in the Search Criteria window.

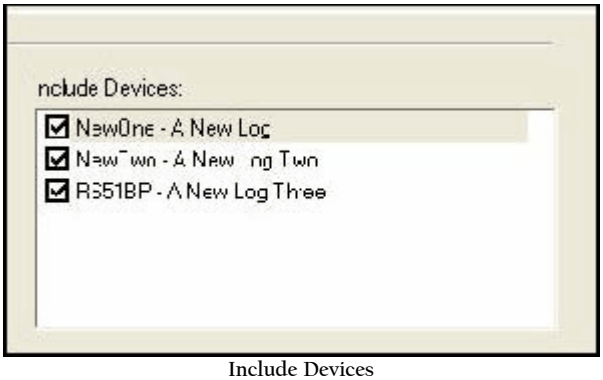



Search Criteria

- Use the drop-down arrows to select dates from the calendar interface.
- Use the roll up/down arrows to indicate specific hours (in 24-hour time) within which to search.
- For a more specific search, use text such as an IP address, area, zone or alarm code in the

"Search for" field.

- To search for data received on specific Devices, check or uncheck the checkboxes in the Include Devices window.




Include Devices

- Use the "Highlight items containing" field to further distinguish particular data in the results window.

## Search Icons

 Click the **Search** button to retrieve data that matches the search parameters set.

 Click the **Print Results** button to print the search results.

 Click the **Select All** button to select the search results entirely.

 Click the **Copy to Clipboard** button to copy the results to the clipboard.

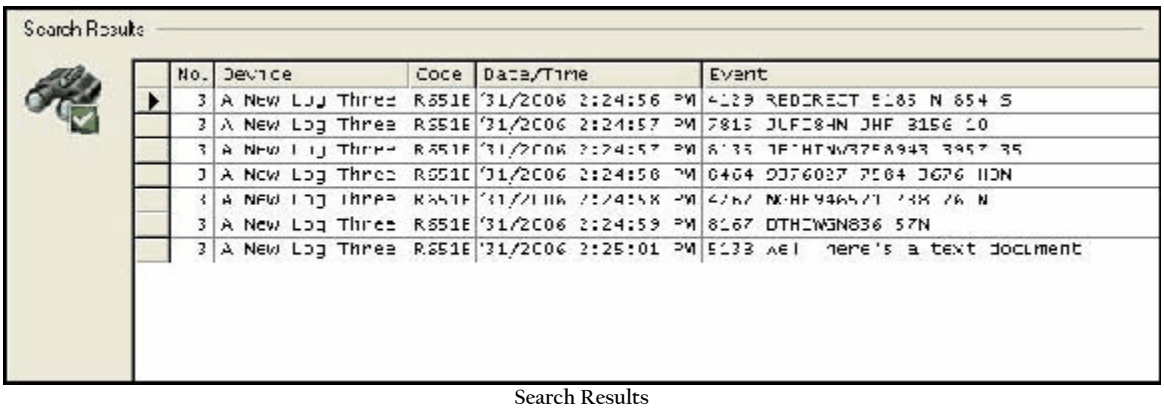
## Wildcard Search

Use the percent sign (%) in the "Search for" field to search any string; use an underscore ( _ ) to search for any character.

***Example:*** Searching for %1019_% will bring up search results that contain 1019 in the string and any other character in the fourth position.

## Search Results

Once parameters are set in the Search Criteria interface and a search is performed, the results appear in the *Search Results* window.




Search Results

## Highlight Items

Use the *Highlight items containing* field to further distinguish particular data in the results window.

***Example:*** In the search results below, typing the text "N" would highlight all items pertaining to that receiver data, without eliminating the other data in the window. The *Highlight items containing* field only searches data in the Event column.

**Highlighted items**

| No. | Device | Code | Date/Time | Event |
|---|---|---|---|---|
| 1 | Radionics 6500 | R665C | 27/2006 3:18:55 PM | 1319 0000 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:19:57 PM | 1319 646 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:19:58 PM | 1319 7692 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:20:50 PM | 1319 655 T FE |
| 1 | Radionics 6500 | R665C | 27/2006 3:20:56 PM | 1319 7306 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:20:58 PM | 1319 0000 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:24:00 PM | 1319 646 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:24:02 PM | 1319 7692 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:25:48 PM | 1319 655 T FE |
| 1 | Radionics 6500 | R665C | 27/2006 3:25:54 PM | 1319 7306 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:25:56 PM | 1319 0000 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:25:58 PM | 1319 646 N 3C1 |
| 1 | Radionics 6500 | R665C | 27/2006 3:26:00 PM | 1319 7692 N 3C1 |

# Switching from Main to Backup Computer

In the event that a Central Station needs to switch from an Active Server to a Backup or Tertiary Server, the following procedures must take place.

*To switch from System 2 to System 1, the user must reverse MANITOU1 and MANITOU2 in all instructions.*

## Summary

1. Stop the active system
2. Switch database replication
3. Start the new system
4. Switch the FEPs to the new system.

## Stop the Active System

1. Open the MSM on the active server (MANITOU1).
2. Right-click on the Broker and select **Stop**.
3. Wait for all lights to turn red.
4. Close any open windows (MSM, Logger, LogMonitor.exe)

## Switch Database Replication

1. Open the Replication Switchover application on MANFEP2.
2. Select the active system from the server list.
3. Click on **Switch**.
4. Wait for the Switch Complete message and click **OK**.
5. Click **Who** to verify that no replication services are down. The command prompt window should show the underlined header information, but no additional information should appear under that.
6. Use any key to close the command prompt window.

## Start the New System

1. Open the MSM on the standby server (MANITOU2).
2. Make sure that (System 2) is selected in the dropdown menu at the top of the window.
3. Right-click on the Broker and select **Start All**.
4. Right-click on the Stealth Logger and select **Start All**.
5. Double click the **Logger** icon on the desktop.

## Switch the FEPs

1. In the MSM right-click on FEP1 and select **Restart**.
2. Repeat above step for FEP 2.

## Verify the System

1. Confirm that operators can log in from the workstations.
2. Verify that the system is receiving and processing signals. The switchover is now complete.

# Troubleshooting

## Stealth Logger

### General

- **Device Type Error**

  Select a Device Type from the drop-down menu in the Device Properties window.

### Receiving activity

- **No activity is received or showing in the Stealth Logger.**

  Make sure the Input Type in the Device Properties window matches the Device Type that is being monitored.

- **Too much activity is showing in the Stealth Logger/Stealth Viewer.**

  Check the Device Options in the Device Properties Window. Make sure the End of Line (EOL) character is correct.

## Stealth Viewer

- **Graphs View is not showing in the Stealth Viewer.**

  Add a workstation in Stealth Logger

- **Stealth Viewer is running slowly.**

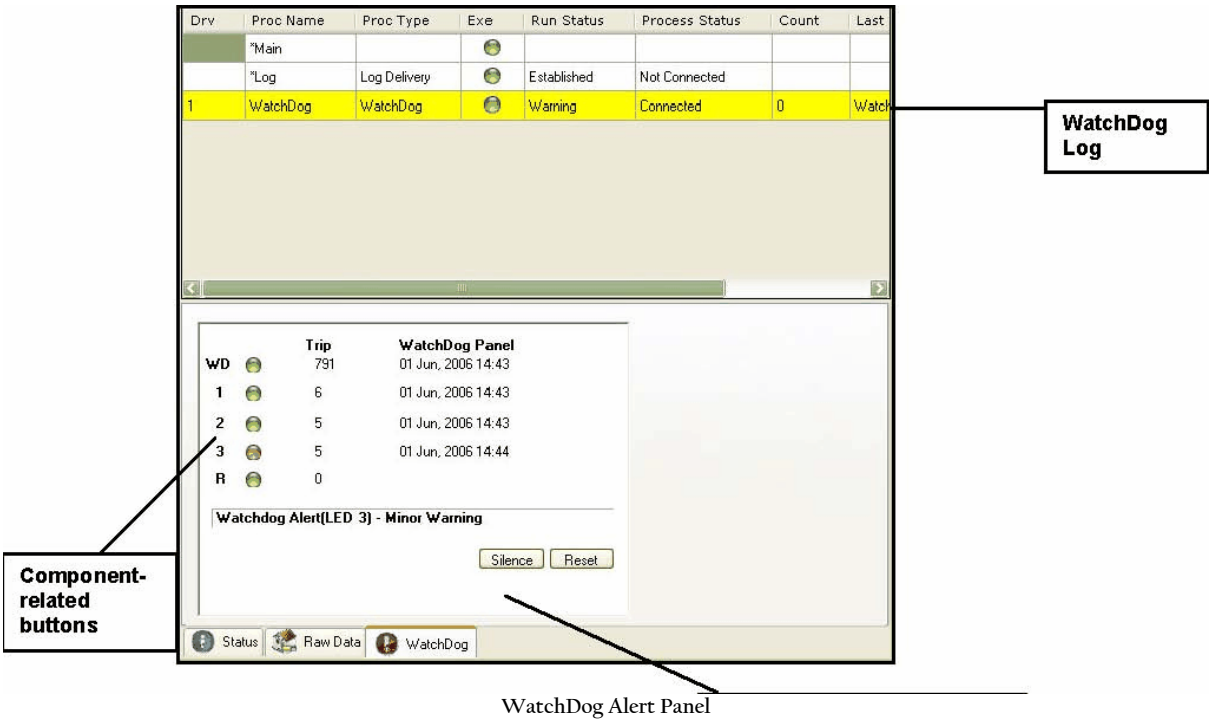
  1) Too many Devices may have been added. Run Stealth Viewer in the History Tab.

  2) The video card may be outdated. Contact Bold Technologies to find out the correct video card.

# Watchdog

Users have the option to run Stealth Logger in WatchDog, which provides both audio and visual alerts corresponding with hardware or software failures, or other predefined system prompts in Manitou.

Failure of any system-critical component will trigger WatchDog to emit a sound and light one of the three component-related buttons, labeled 1, 2, and 3 on the WatchDog Alert Panel. The lighted WatchDog ("WD") button monitors constant communication between Manitou and WatchDog. If communication is not received within the expected interval, WatchDog will emit a sound and the top, WD, button will light up.




Central Stations with UL certification must folow the subsequent protocol:

1. The Central Station must not disable the WatchDog feature
2. The WatchDog must be set for 90 seconds or less
3. The WatchDog screen in the Central Station must be in close proximity to the Operator
4. The WatchDog audible feature must be enabled
5. Disabling the WatchDog is not applicable to UL Central Stations

**UL certified Central Stations are required to employ Bold WatchDog software or the SPE timer hardware. When using the Bold WatchDog software, altering CPUs may not use a screensaver with this program.**

# Starting Stealth Logger in Watchdog

1. Open Stealth Logger.
2. Select **Startup options** from the File menu.
3. Check the WatchDog box.
4. Click **Yes** to restart Stealth Logger.
5. Click **OK**.
6. After Stealth Logger exits, open the program again.

The Stealth Logger will now operate in WatchDog Mode. Clicking on the *WatchDog* tab will show the WatchDog Panel where activity is monitored. Any system warnings will show in the WatchDog Panel.

# Adding a Device

Adding a Device while Stealth Logger is operating in WatchDog is similar to adding a Device while Stealth Logger is operating in normal mode.

1. Click on *File>Add Device*.
2. Select *WatchDog* from the *Device Type* drop-down menu.
3. Choose the desired Port.
4. Enter a description.
5. If using a Serial Port, enter the Port Name. If using TCP/IP, enter the Host Name.
6. Enter the Port Number.
7. Use the up/down arrows to select the FEP number and Receiver number associated with this Device.
8. If the Stealth Logger should monitor activity on this device, check the Monitor checkbox. If, for example, this is a backup device, leave the Monitor checkbox unchecked until this device is in use within the Manitou system. A Central Station may want to include this type of update to the Device Details screen as part of the documented backup procedures.
9. Check the *Print on System Failure* checkbox if raw signal data should be sent to a printer and handled by Operators manually in case of system failure.
10. Choose a color associated with this Device.
11. When finished with the *Properties* screen, click **OK** to finish adding the Device entry.
12. A pop-up info box will appear, stating the driver needs to be started. Click **OK**.

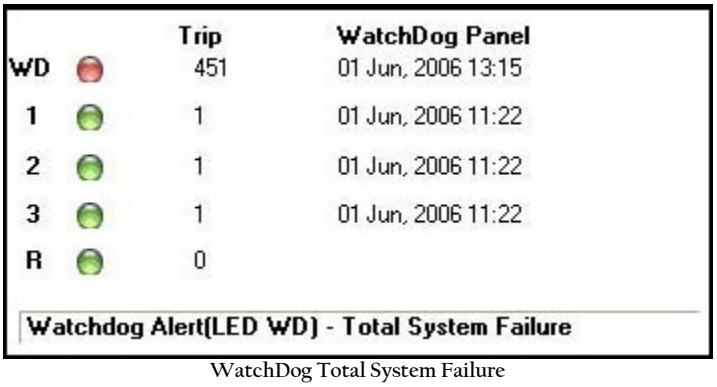
The new Device will now appear in the Device list located in the left column of the screen.

# System Warnings

System warnings occur when a failure or warning is sent from Manitou to the WatchDog.

## Total System Failure

WatchDog displays a total system failure warning when Manitou has failed to communicate (send a signal) to WatchDog within the expected time interval.

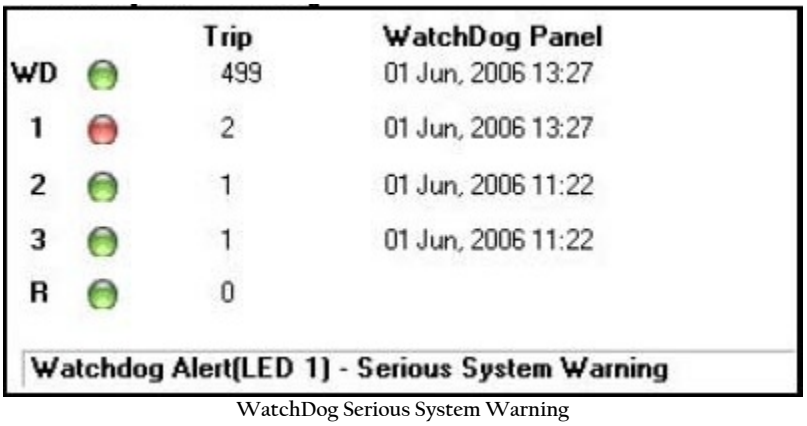



WatchDog Total System Failure

## Other System Warnings

Users can configure certain applications in Manitou to send system warnings to WatchDog to alert Operators of various warnings. For example, an Operator may configure Manitou to send a Serious System Warning to WatchDog if the Signal Handler stops running.

Manitou will send this alert to WatchDog, and WatchDog will emit a sound and the first (1) button will turn red: A System Warning, indicated by the second (2) lighted button, and a Minor Warning, indicated by the third (3) lighted button, can also be configured in Manitou, depending on the seriousness of the warning, such as an alarm process issue.




WatchDog Serious System Warning

# Sounds

When a warning occurs, WatchDog emits a sound to alert Operators. Users can silence the sound by clicking on the "silence" button on the WatchDog Alert Panel in Stealth Logger.

Users have the option to change the sound file to their preference. This sound file must be in .wav format.

1. Open the Windows Directory
2. Open the Media folder
3. Copy the preferred .wav file to the Media folder
4. Rename the file to watchdog.wav
5. Close the folder. The WatchDog will now play the preferred .wav file

# Disabling Watchdog

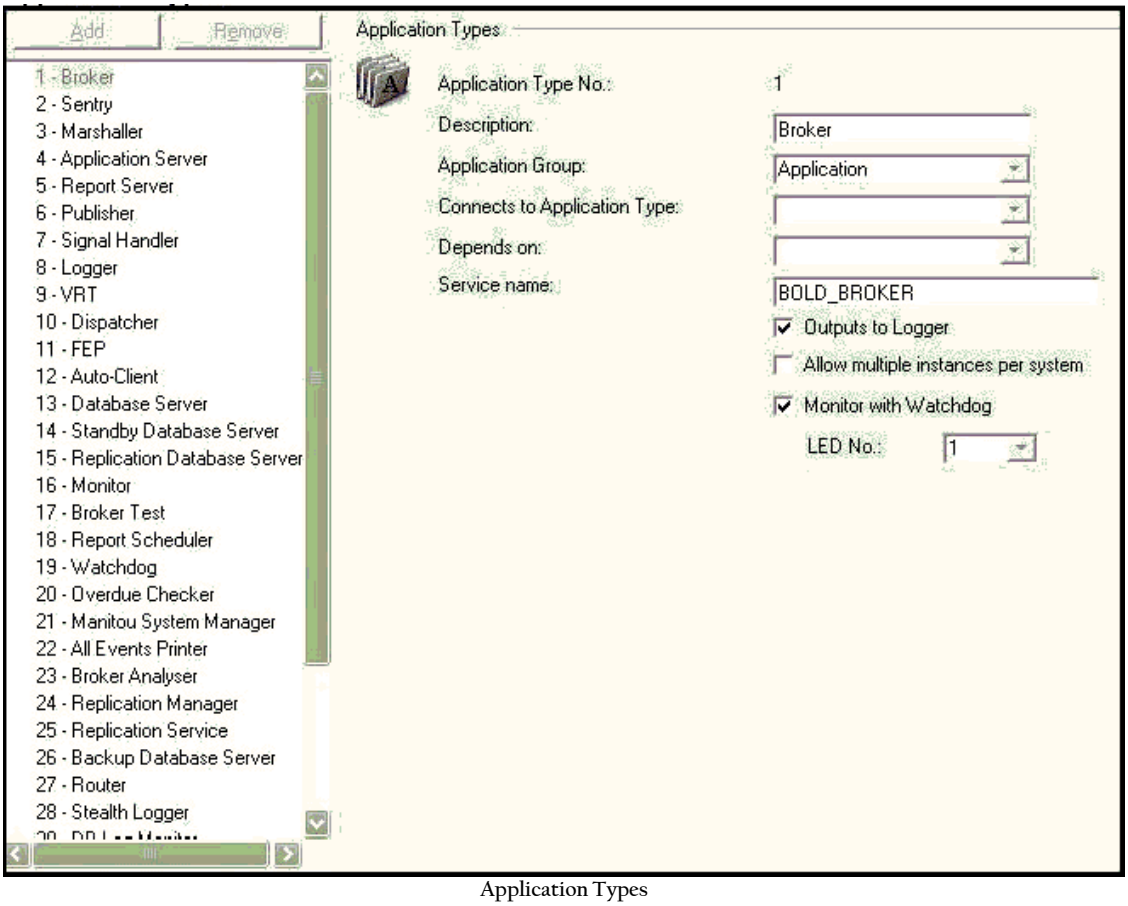
1. Go to *Startup Options* in the *File* menu
2. Uncheck the WatchDog box
3. Click **Yes** to restart Stealth Logger
4. Click **OK**
5. After Stealth Logger exits open the program again

Stealth Logger will now operate without WatchDog (Stealth Logger will now open in normal mode).

# Configuring Manitou Apps with Watchdog

Users can configure Manitou applications to be monitored by WatchDog (as a Stand-Alone Environment).

***Example:*** A Central Station may wish to monitor Signal Handler in the event that the service stops running (that no signals have been received for a certain period of time which may indicate that the Signal Handler is not receiving signals properly).




Application Types

To configure Manitou applications:

1. Open the Manitou Supervisor Workstation
2. Open the *Maintenance* menu
3. Click on **Setup**
4. Click on **Application Types**
5. Select the application to be monitored by WatchDog (ex: Broker or Signal Handler)
6. Click on the **Edit** button in *Application Types* window
7. Check the *Monitor with WatchDog* box
8. Use the drop-down menu to indicate to WatchDog the importance of this alarm (ex: 1= Serious System Warning, 2=System Warning, 3=Minor Warning)
9. When finished, click **Save**. WatchDog will now monitor this application

# Event Code Warnings

Users can configure Manitou to utilize WatchDog to alert Operators when an alarm or even has not been handled in adequate time.

To monitor events:

1. Open the Manitou Supervisor Workstation
2. Open the *Maintenance* menu
3. Click on **Setup**
4. Click on **Application Types**
5. Select the Event Center application from the applications list
6. Click on the **Edit** button in *Application Types* window
7. Check the *Monitor with WatchDog* box
8. Uncheck the *Outputs to Logger* box
9. Use the drop-down menu to indicate to WatchDog the importance of this alarm
10. When finished, click **Save**

**Central Stations with UL certification must follow the subsequent protocol:**

- The Central Station must not disable the WatchDog feature
- The WatchDog must be set for 90 seconds or less
- The WatchDog screen in the Central Station must be in close proximity to the Operator
- The WatchDog audible feature must be enabled