

CIRCUITWERKES
Makers of Innovative Electronics

**Operation &
Technical Manual**

**Silence Sentinel
Web Based Audio Monitor & Controller**

Hardware Version 1
Manual Rev 0.9
Firmware Version 1.9 / Software v1.3.26
Revised 09/22/2010

Table of Contents

| | |
|--|-----------|
| Contacting CircuitWerkes..... | 4 |
| Unpacking your Silence Sentinal..... | 4 |
| SAFETY INFORMATION | 4 |
| PRODUCT OVERVIEW | 5 |
| INTRODUCTION..... | 5 |
| Inputs and Outputs..... | 5 |
| <i>Back panel connections</i> | <i>6</i> |
| <i>Silence Sentinal Front panel indicators:</i> | <i>6</i> |
| CONNECTING YOUR SENTINAL TO OTHER EQUIPMENT | 7 |
| Audio Inputs | 7 |
| RELAY OUTPUTS:..... | 7 |
| EXTERNAL STATUS INPUTS | 7 |
| USING THE INTERNAL WEB SERVER..... | 8 |
| Networking basics: | 8 |
| Connecting to the Sentinal for the first time:..... | 9 |
| Using the Sentinal’s Web server: | 10 |
| Logging In: | 10 |
| Sentinal Configuration: | 12 |
| Event Types: | 13 |
| Installing & Running the Software: | 14 |
| Using the Software..... | 15 |
| Understanding the Grid Display | 15 |
| Configuration using the Software: | 16 |
| SPECIFICATIONS | 17 |
| WARRANTY | 18 |

NOTE: This technical manual & information presented within is subject to change.

Contacting CircuitWerkes

For help with setting up or operating the Silence Sentinal, please contact us at the following:

Phone: 352-335-6555

E-mail: info@circuitwerkes.com

Website: www.circuitwerkes.com

Unpacking your Silence Sentinal

Note: CircuitWerkes is not responsible for product damage during shipment. Inspect your shipment carefully for external signs of damage. CircuitWerkes suggests that you unpack your shipment as soon as possible after receipt to inspect it for signs of damage that might not be visible from the outside. If the shipment appears to be damaged, keep the original boxes and packing material for inspection by the carrier. All damage claims should be made directly to the carrier. Do not delay. Call the carrier as soon as damage is discovered.

You should have received the following items with each Silence Sentinal that you have purchased:

- [] (1) CircuitWerkes 15V Power Supply
- [] (1) Sentinal Software CD

If you have not received all of the items shown with your shipment, please carefully check inside the box or boxes because items occasionally get lost in the packing materials and can be hard to find. If your items are not found, please call CircuitWerkes at 352-335-6555 or e-mail us at support@circuitwerkes.com.

In case your product is in need of service our shipping information is as follows:

CircuitWerkes, Inc.

Attn: RMA #

2805 NW 6th Street

Gainesville, Florida, 32609, USA

Please obtain an RMA from us and verify the address before returning any products.



Safety Information

WARNING!

The Sentinal's relays are not intended to switch hazardous voltages. The exposed terminals make connecting such voltages to the Sentinal extremely dangerous and it should never be attempted. The terminal strips are not designed to shield humans from potentially dangerous Voltages. Contact with high Voltages can cause serious injury or death. The maximum recommended Voltage for the Sentinal is 30V. Switching of high voltages should only be done externally and in a manner that isolates the voltages from accidental contact with people.

Surge Protection

Although the Sentinal has built-in resistance to voltage changes, we recommend that you use a power surge protector or line conditioner on the incoming AC line. Lightning strikes and other high surges in voltage levels will damage your Sentinal and connected equipment if it is not properly protected.

UPS Standby Power System

We recommend that you connect your Sentinal to a battery backup system. While all operating and user parameters are stored in non-volatile RAM, brownout conditions and lightning induced spikes can disable or damage equipment. A UPS helps minimize the risk to the Sentinal and has the added benefit that it will then be able to notify you of the power outage by phone, pager, or data, depending on the configuration of your system.

Product Overview

Introduction

The CircuitWerkes Silence Sentinal is a Web enabled audio monitoring tool with integrated control capability. An internal Web server lets you monitor your audio from any Web browser, anywhere in the world. When silence is detected, the Silence Sentinal can perform user-programmed, automated, sequences of actions and can also respond to user control via the network or via external contact closure inputs. Three levels of user control are available ranging from reader up to administrator.

Up to two Silence Sentinals can be optionally rack mounted in a single sized rack shelf. Administrators can perform all setup through the Web server.

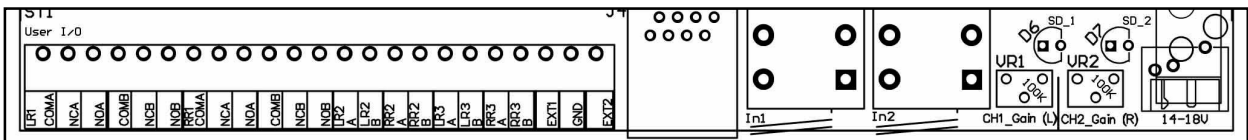
This manual is valid for firmware version 1.6 only. For firmware version 1.4 and earlier, please do not use this manual.

Inputs and Outputs

As seen in Figure 1 below, the Sentinal has a number of connectors on the back panel to interface with your equipment. The following table is a list giving the name of each connector, followed by a brief description of its function.

Key Features

- *Internal Web Server lets you see your status from anywhere in the world*
- *Web server VU meters are fast responding*
- *Detects Stereo or Dual Mono Silence (independantly adjustable channels)*
- *User-programmed relays (DPDT) close automatically or via Web control*
- *Balanced or unbalanced audio inputs.*
- *12 User-definable alarm conditions can trigger up to 3 actions per alarm*
- *External trigger inputs can activate user-defined actions*
- *Relays can be momentary or latching.*
- *DHCP or Static IP capable*
- *Free GUI software to monitor your site*



| |
|-------------------------------------|
| Sentinal Rear connectors & controls |
|-------------------------------------|

Back panel connections

| Name | Type | Description |
|-------------|--------------|---|
| Power In | 2.1mm Barrel | Accepts 14-18 V AC or DC @ 200mA |
| Sil Det 2 | Red LED | Indicates when silence is detected on channel 2 (right) |
| Gain Right | Trimmer | Adjusts the input level to the #2 A/D converter |
| Sil Det 1 | Red LED | Indicates when silence is detected on channel 1 (left) |
| Gain Left | Trimmer | Adjusts the input level to the #1 A/D converter |
| Audio In 2 | ¼" TRS | Audio input to feed channel 2 (right) for audio monitoring. |
| Audio In 1 | ¼" TRS | Audio input to feed channel 1 (left) for audio monitoring. |
| Network | RJ-45 | Connects your LAN or Internet to the internal Web server. |
| Status LEDs | G & Y LEDs | Blinking yel = proper operation. Solid green = Net connected. |

Ext 1 & 2 Screw Terms External Status inputs. Can trigger actions/alarms.

Relay Outputs Screw Terminals The Sentinal has six relays that are divided in to "Left" and "Right" groups. Each group contains one DPDT & 2 SPST relays. Although the relays are named by group, any event on either channel can be used to operate any relay. Everything is completely user defined.

| |
|---|
| <p>Important Note: the DPDT relays are rated at 1Amp while the SPST relays are rated at 10va or 100mA (non inductive).</p> |
|---|

Silence Sentinal Front panel indicators:

| Name | Type | Description |
|--------|---------------|--|
| PWR | LED Indicator | Indicates that the main power supply is operating. |
| Link | LED Indicator | Lights up whenever the network is connected |
| Cust 1 | LED Indicator | Lights when a user defined event triggers this LED |
| Cust 2 | LED Indicator | Lights when a user defined event triggers this LED |

Connecting your Sentinal to other equipment

Audio Inputs

The Sentinal has two, balanced, audio inputs that it monitors. Gain control potentiometers are associated with each input to let you calibrate your audio level to the internal metering of the Sentinal.

Types of audio connectors

Figure 1a

1/4" TRS (phone) PLUG

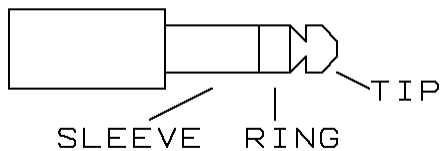
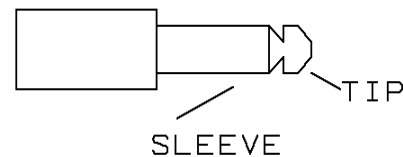


Figure 1b

1/4" TS (mono) Jack



1/4" jacks come in two varieties: Tip, Ring & Sleeve (TRS) or Tip & Sleeve (TS or Mono). TRS jacks are preferred for the input connections to the Sentinal, however TS jacks can be used for as well.

Relay Outputs:

The Sentinal is equipped with 6 relays organized in 2 channels to provide you with control over your external equipment or to switch balanced audio.

Relays 1L and 1R are DPDT relays which are ideal for use as a simple, stereo, audio switcher. These relays can also be operated in momentary mode, so they can be used as standard control outputs, as well. All six contacts of each relay are brought out on the back panel barrier strip, so any and all of their contacts may be utilized. Each of the remaining four relays are normally open SPST (form A) contacts that can be used for general control purposes. The SPST relays are rated at 10va, non-inductive. Higher loads may damage them. The DPDT relays are rated for 1A max., non-inductive.

External Status Inputs

The Sentinal's status inputs can be used to determine the status (on/off) of your equipment. The status input connectors are located immediately to the left of the network connector and are labelled Ext1 and Ext2. These inputs accept only contact closures to ground as inputs. Do not source voltages to these inputs. Status inputs can be used to trigger actions when closed or opened.

Using the Internal Web Server

Networking basics:

Before reading any further, we would like to mention that the following section is not intended to be a comprehensive guide to networks, nor does it necessarily describe your network. Indeed, we have found that networks vary quite a lot and yours will probably be different than is described here. We assume that you, or a network administrator, is familiar with your network and knows how to set it up to accommodate Web servers that exist within your network. The brief discussion provided below is only intended to be used as a very non-specific description of how a network might function.

In Internet land, devices on your network get unique IP addresses because each piece of hardware has a serial number embedded into it. Every device with a serial number, called a MAC address, has to get an IP address assigned to it in order to function using the networking protocol called TCP/IP, which is what is used for the Internet. The router in your network uses those IP addresses that it assigns to keep track of what data requests have been made and how to route responses to the devices that need data. In a way, the IP address is sort of like a nickname that computers use to talk to each other. A computer will only respond if it has been called by name. So, the IP addresses are what one computer uses to address or talk to another computer. The router also uses those IP addresses to manage the flow of communications between each computer so that they are not all talking at once like an old fashioned party-line.

IP addresses are usually doled out within a fixed range, so it's also easier for humans to remember a device's location via its IP address than to try to remember every item's MAC number. For instance an internal network might use the IP range of 192.168.1.### where ### can be 001 through 254. Once the network administrator has set up the address range, he or she only has to keep track of what's assigned to the last three digits of the address range.

Generally, simple networks are divided into two sets of addresses. There are the addresses that exist inside the network (called the private or LAN side) and then there are addresses that exist on the Internet (public or WAN) side of the network. We've already described the private side above, but getting stuff on the private side to talk to the public side can be tricky.

When you have one device that is connecting your internal network to the Internet, like a cable modem or DSL modem, it also has a unique serial number, so it gets assigned an IP address from your ISP. But the ISP only sees the modem, not other equipment on the inside of your network, so they cannot assign multiple IP addresses (actually they can, but that's another story). Although you probably only have one IP address, you will have a whole range of port numbers that you can use for each IP address that exists on the private side of your network. Usually, different types of communications use standardized ports to talk to devices. For instance http (Web browsing) is mostly done on port 80. FTP is usually port 21. E-mail might use port 25. Often, we want to set our network connection up to pass port 80 to some device on our network, like the Sentinal, that serves up web pages. We do that by telling the router/firewall to pass port 80 requests to the IP address that we know we have previously assigned to the Sentinal. To do that, we have to tell our firewall that it's okay to send port 80 requests to the Sentinal, otherwise it'll just block those requests if they come from the public side of the firewall. As described earlier, each device on the private side needs a static IP address that is set by the network administrator. So, each item on the inside of a network that will be communicating with the outside world has to have an IP address within the local network **AND** it must also have the appropriate port opened on the firewall. On the Internet side of the firewall, there is usually only the main IP address and the port number.

When you put it all together it might look like this:

Public IP address 67.234.98.135, port 630 could be mapped to internal IP address 192.168.1.250, port 80. So a browser request made to 67.234.98.135:630 would serve up a web page because you would really be talking to 192.168.1.250:80. Once you have that properly configured, your Sentinal can serve up Web pages from inside of your network to the Internet.

Connecting to the Sentinal for the first time:

Most networks use a router as their central hardware. When a device is plugged into a router, the device normally obtains an IP address from the router using a process called DHCP. By default, the Silence Sentinal obtains a DHCP address from your network's DHCP server. In order to connect to the Sentinal, you have to know what its network IP address is. An IP address inside a network will usually look like XXX.XXX.X.XXX, for example 192.168.1.100. Your router knows this information and you can usually find out what the address is by logging into the setup page of your router. Most routers have a page that shows the attached devices. This can be shown as part of the router's DHCP page, or it may be shown in a separate LAN discovery page. Once you know the IP address of your device, you will be able to connect to it by entering the address into your browser's address bar. **The sentinal's status LED (Yellow next to the RJ-45 connector) blinks out the last address octet a few seconds after the Sentinal has been powered up.** You can use these numbers to identify the position of the Sentinal on your network's router. Alternately, you can use the CircuitWerkes Netscanner utility, found on our website or on the CD that came with your Sentinal to locate the device on your network.

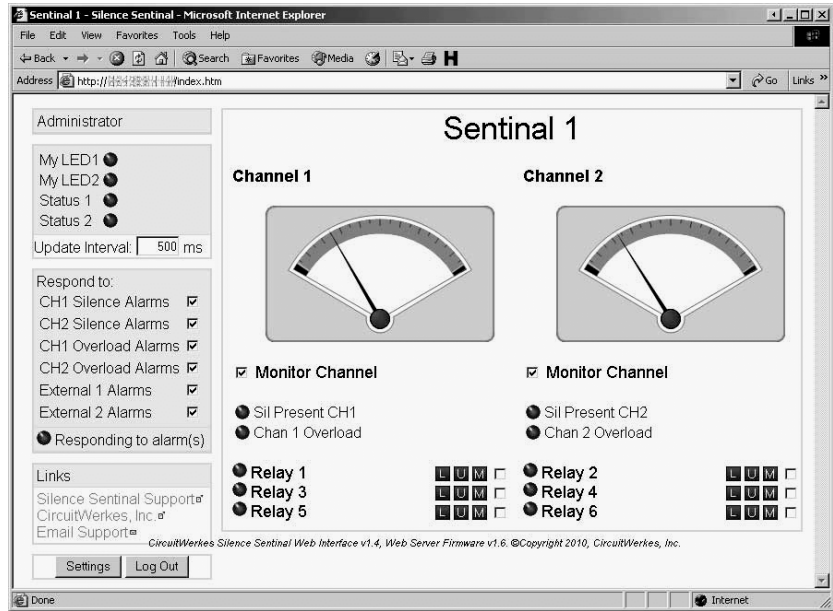
If you do not use a router in your network or if you want to configure your Sentinal via a direct connection, the default IP address for this device is 192.168.1.250. If making a direct connection, you must set your computer's network settings to match the Sentinal's settings. Your PC's TCP/IP properties must be set to 192.168.1.xxx with a netmask of 255.255.255.0. Once you have connected to the Sentinal, you can set its IP address to whatever you wish from the configuration page.

The Web server always uses port 80. Often, sites have multiple devices that want to use port 80, including some routers. In most cases, your router can simply redirect a different outside (WAN) port to the individual Web servers' inside IP addresses. For instance, the Sentinal and an audio IP device each have Web servers using port 80. The Sentinal has an internal IP address of 192.168.1.250 and suppose that the audio device has an IP of 192.168.1.200. If you are on the inside (LAN) of the network everything looks great. You can browse to either device and everything works. To access the site from the outside, you must open a "pinhole" that allow data to pass from browsers to your Sentinal. You can encounter a problem if you try to route WAN port 80 to LAN port 80 for both Web servers. Only one will be assigned. You will not gain access to the second one. Instead, redirect LAN port 80 for each device to a different outside port, such as 800 and 801. In practice, you would access your site by entering its IP address followed by a colon and the port number (xxx.xxx.xxx.xxx:800), or by its URL name followed by the port (www.mysite.com:800). Note that some routers, such as those made by Netgear cannot redirect ports.

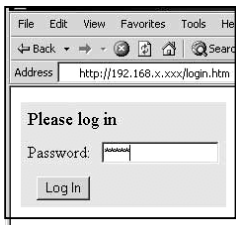
NOTE: Most, if not all, Linksys routers have a serious defect in pinholes that will prevent you from outside accessing all Web servers that require port 80. Linksys uses port 80 for their router's own Web server that is used for configuration. Further, they do not provide any option for redirecting port numbers from the LAN side of the router to the LAN side of the router. The result is that you cannot use port 80 to access an LAN side Web server, nor can you change the port number to access that device. As far as we know, Linksys is the only company that has this defect, but there could be others. **If you use a Linksys router, you will not be able to access the Sentinal, nor any other device with a Web server on port 80 from the public side of the network.**

Using the Sentinal's Web server:

Your Sentinal contains an onboard Web server which is the heart of its monitoring capability. This Web server has proved to be very stable & supports multiple, simultaneous users and many different browsers. Although the interface looks simple, the real power of the Web server lies "under the hood", in its speed. Readings are continually updated, at a user defined speed, which is much faster than many competing products. Your actual speed depends upon the network and upon your PC's horsepower. Your PC reads the raw data from the Sentinal and "draws" the meter movements. Your computer's ability to draw quickly has a direct effect upon how frequently the meters move. The default update speed is 500ms which updates the meter position 2x each second. Speeds of 50ms can be achieved on fast networks, however, if you request data too fast, your network or your PC may not be able to handle it and you can get a periodic message saying that the Sentinal is not responding. If that happens frequently, slow the updating down by using a bigger number in the "Update Interval" box.



Logging In:



By browsing to whatever IP address your Sentinal has, you will be presented with a login screen. **The default administrator's login is 12345678**, unless you have previously set this differently from the configuration menu. There are three access levels to the Sentinal, reader, controller and administrator. Only administrators can configure the Sentinal. Controllers can operate relays while reader level has no control. The default administrator's password is simply 12345678. Passwords are a maximum of 5 characters.

If you are using Internet Explorer and you incorrectly enter the password one time, you may have to close your browser and reload it because IE cache's the passwords and will try to use them even if they don't work and you have tried to enter a different password. To avoid that problem change your IE settings for temporary files so that Explorer checks for new versions of stored pages on every visit. Other browsers such as Firefox, Opera and Chrome do not, generally, have this problem, however, we still recommend IE be used for changing configuration of the Sentinal. Any browser can be used for monitoring.

Once you have entered the correct password, it will take a few seconds to load the Sentinal's page. Once done, you will have access to the metering and controls of the Sentinal. If you are an administrator, you will also be able to manage the Sentinal's settings.

Monitoring and control using the Web server:

Displays Current Access Level

Event Indicators: Cust 1 & 2 light when user-defined events occur. Ext 1 & 2 show when either of the two external status inputs are closed. Update interval defines how often your meters move.

Administrators can select which kinds of alarms to respond to. Unchecking a box prevents responding to that type of alarm.

When "responding to Alarms" is "ON", the Sentinel may not respond to user input while it is processing action steps.

Settings button opens the configuration menu in a new window.

Relay LEDs. On when relays are energized.

Relay controls: U is unlatch, L = Latch and the "M" button is momentary for duration of mouse-down. The "checkbox" has been added next to each relay function. When checked, this box disables changes to that relay, be it automated or by Web control. If a relay is latched and an automated script would have unlatched it, the relay will remain on. Uncheck the box for normal function.

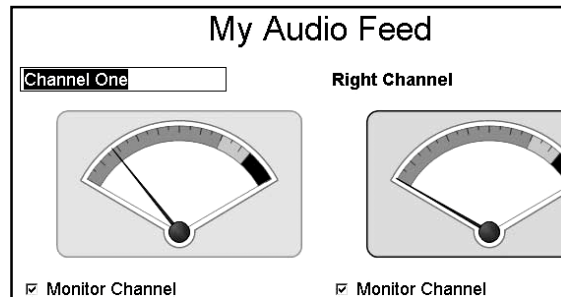
Metering for Chan 1 and Chan 2. Green background indicates normal operation. Red indicates silence or overload. Grey means that channel is not being monitored.

The Sentinel's Web server display gives you the ability to monitor audio on two channels and to control six relays. Four of the relays are SPST while two are DPDT, suitable for either controlling external equipment or for switching audio. Relays can be latched or momentary.

The Sentinel also has two status inputs that are monitored. Their status is shown in the upper left side of the screen as "Ext 1" and "Ext 2". When their inputs are connected to ground, the associated indicator turns from gray to green. External status inputs can also be used as events to initiate alarm actions.

Sentinel Configuration:

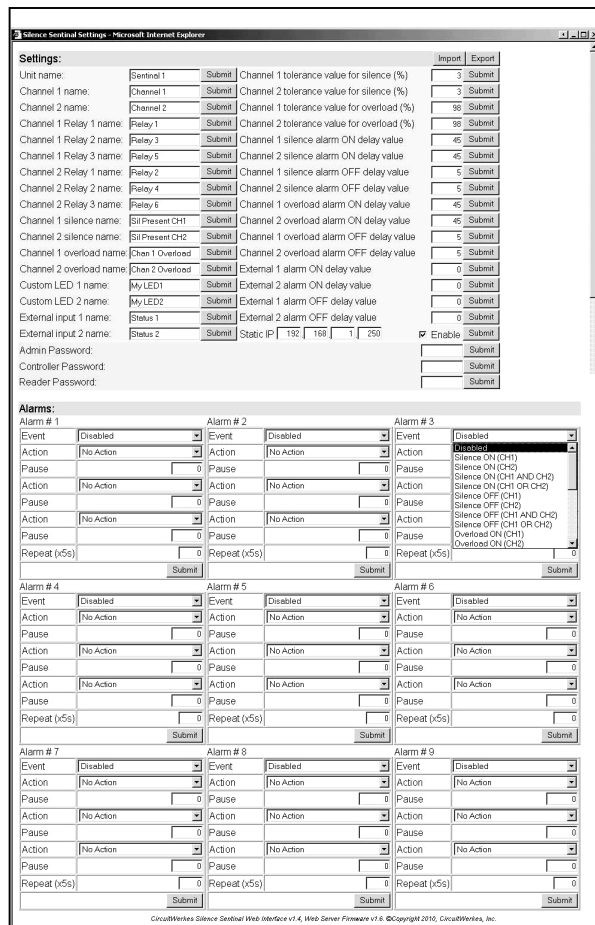
Administrators and controllers can operate relays and view the meters. Readers can login to see the meters, but cannot control anything. Administrators can read meters, operate relays and perform configuration setup tasks, including editing labels by just clicking on them from the main page.



Above: Quick-changing a Label (Admin Only)
Below: The main settings Form

In addition to quick changing the labels, administrators can click on the “settings” button to open up the main configuration form in a new window.

The configuration form lets you setup a static IP address, setup passwords for the various access levels, lets you change label names, define silence and overload levels for each channel and specify the delay before an event is registered as an alarm and starts an action step.



The action steps are user-defined functions that the Sentinel will perform whenever an event is triggered. These events are usually called alarms, but they can also be simple responses to any particular input as defined by you.

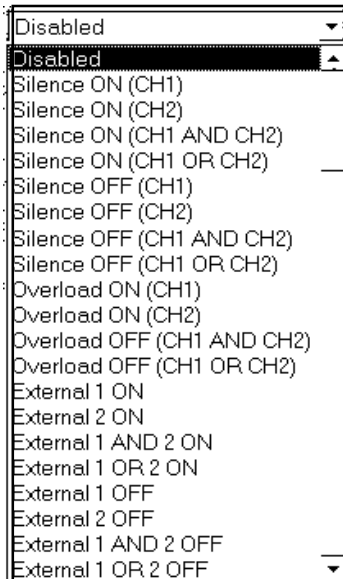
The “alarms” are defined by two parameters:

1. The triggering event
2. The step, or steps that you want to take when an event occurs.

A sequence may be repeated by entering a value in the “repeat x5s” box. This is a delay before repeat measured in 5 second intervals. For instance, entering a 2 = 10 seconds. The maximum delay is 300 secs. (max value = 60). Repeat should not be used for summed channels (and / or conditions). Infinite repeats can occur, particularly when “off” conditions are set to repeat. Use two alarms when repeat functions are desired.

Important Note: Do not use any quote marks (either single or double) in any labels. These will interfere with the java and your Web server may stop working properly. You might still be able to use the software to change the problem labels if that happens

Event Types:



There are 24 events that can trigger actions.

The first eight are permutations of silence detection. You can react to silence on one or both, or either channel, or you can react to the return of audio on those same channels.

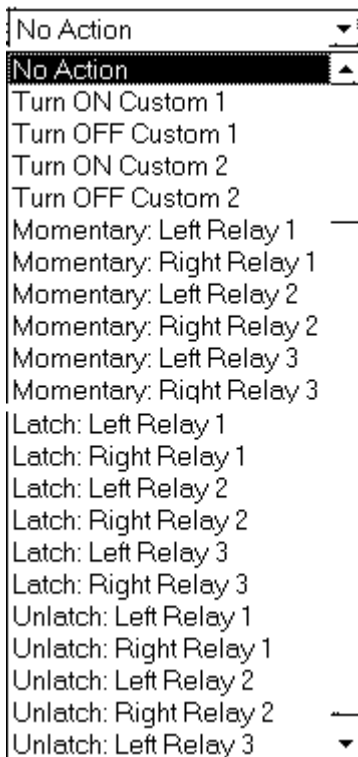
Similar to silence detection, overload detection indicates when too much audio is present on a channel.

The four External "ON" events occur whenever one or both of the external status inputs are grounded, while the four External "OFF" events happen whenever the external status inputs are ungrounded.

Each of these trigger events can be used to perform a different action. For instance, one alarm event (and action) might be if silence detection on channel 1 causes relay #1 to latch "ON". A second event might then be used to unlatch relay #1 when silence "OFF" is detected on channel one. By using two alarm events, you can create an automatic switchover system that will operate whenever silence occurs and will automatically reverse itself whenever audio returns.

Each type of alarm is governed by its own set of timers, so you can choose how quickly the Silence Sentinal will respond to a particular condition. For instance, the channel 1 silence detection might be set to occur after 30 seconds of silence, but you might want to know that audio has returned after only 5 seconds, so that you can restore main programming. Setting a timer to zero is an instant response.

Actions:



Any action can perform any of the tasks on the list, regardless of if the action is a so called "left" or "right" event. Actions can be used to operate relays, either momentarily or latching. When a latching action is performed, often a matching "unlatch" or "release" event is used to undo the action when the triggering event is over.

In addition to operating relays, the custom LEDs can be operated. The Custom LEDs are represented graphically on the Web server as gray (off) or green (on) lights. There are also two real LEDs on the front panel of the Sentinal that are operated by the same actions.

Each alarm (action) can have up to three steps. There are programmable pauses available between steps as well. Using these, it is possible to have one event, close a relay, turn on one of the LEDs and then pause for a few seconds, then close, or open, another relay.

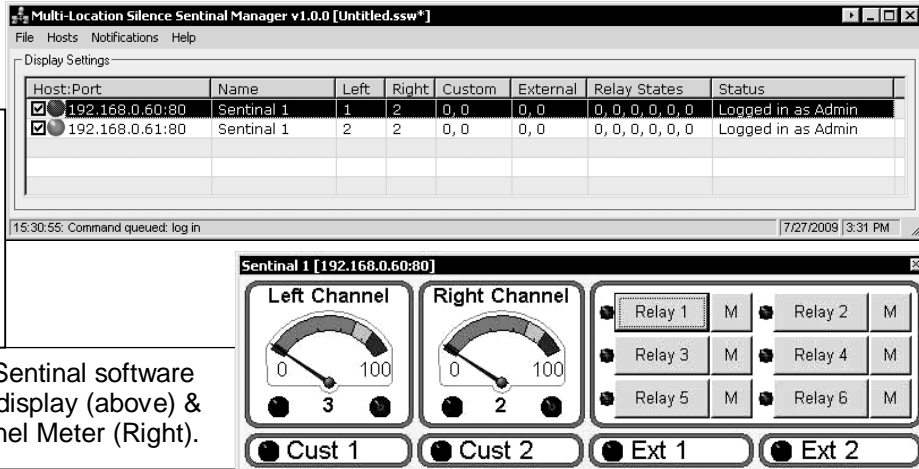
Whenever actions are occurring, the Sentinal will not respond to outside commands or to other events until the action has completed. If a pause is set to 60 seconds, then the Sentinal will not be responsive to outside control, nor will it update its meters, until that time, plus whatever amount of time to run the action steps has passed.

Note that the configuration page lets you export and import settings from your browser. On some computers, the import/export function may only work properly with Internet Explorer.

Sentinal Software

NOTE: The Sentinal software is an experimental release. It may do unpredictable or annoying stuff. If you experience problems, we'd like to know about them so that we can fix the software. Please e-mail us at support@circuitwerkes.com.

The Sentinal software main display (above) & Channel Meter (Right).



The Sentinal includes a Windows-based, Multi-Site, setup and control software client. You can download a free copy from our website at <http://www.broadcastboxes.com/support.html>. The software is not required in order to use the Sentinal, but is handy, especially when working with multiple units. The Software is divided into two main function groups, control and setup.

The setup mode lets you program your Sentinal and duplicates the setup options available via Web browser. Setup is menu-driven and is designed to make programming as easy as possible. All Sentinal parameters are available via the menus and, once set-up, the programming parameters can be saved to local files. The local files can then be used to program other Sentinals or as a backup in case it ever becomes necessary to reset your Sentinal to factory defaults. You may save as many Sentinal configurations as you want. By modifying one configuration file and then saving it as another name, you can create an infinite number of files for setting up different Sentinals.

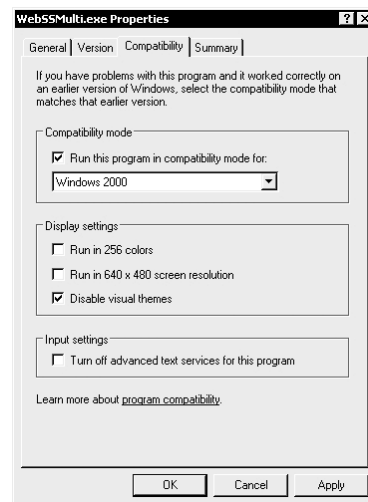
The control mode lets you operate the Sentinal without opening a Web browser for each unit.

The software interface lets you hide any, or all, of the meter and control panels, letting you display only the ones that you want to see.

A very useful feature is the e-mail alert. When an fault condition is detected, e-mail can be automatically generated notifying you of the condition.

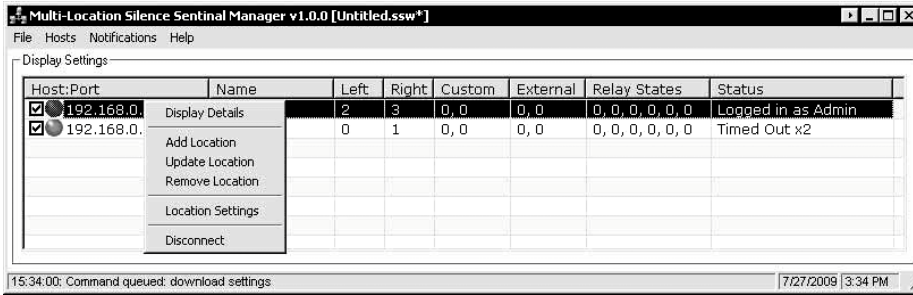
Installing & Running the Software:

The Sentinal software has an installer, so all you have to do is double click on the installer file and follow the prompts. Once you have the software installed, some users of Windows XP and Vista system have reported that the Sentinal software will not run properly unless compatibility mode is selected. To enable compatibility mode, find the installed .exe file which will usually be in your "C:\Program Files\CircuitWerkes\WebSSMulti\" folder. The file is called "WebSSMulti.exe". Right click on the file and choose properties from the menu. Once you have opened the properties box, select the "compatibility" tab and check the "Run this program in compatibility mode for" box and select "Windows 2000" from the drop down box. You might also have to check the box that turns off visual themes as well.



HINT: Before installing the software, ALWAYS check for updates on our Website.

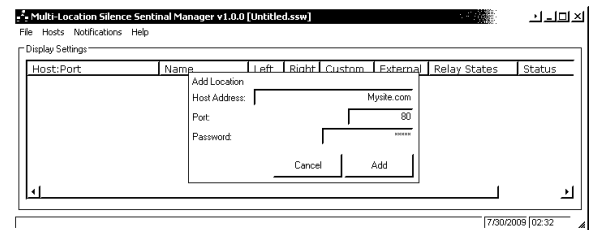
Using the Software



Left: Sentinel main form with two locations already added.

When you first start the software, you will see a small, unpopulated grid view that resembles a spreadsheet. This is the default multi-site viewer. To add a Silence Sentinel, right click on one of the grids and select "Add location" from the menu.

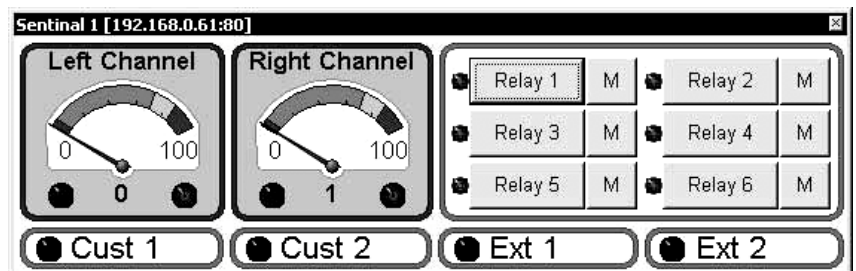
Adding a location is how you set up the software to begin monitoring your selected location. Fill in the IP address or the URL of the site, followed by the active port number and the access code. Then press the ADD button to place the site on the grid. Once a connection has been established, the LED indicator will turn green and the basic parameters from the site will be downloaded and be visible on the grid.



Understanding the Grid Display

Double clicking on a Site's line brings up the site monitoring applet.

The individual Site monitor gives you the same level of detail as the Web browser, but without having to run a browser. The individual site monitors are slaves to the main form, so when it is closed, they will also be, however, sites can be closed one by one, by clicking the X in the upper right corner.



Configuration using the Software:

The Sentinel software lets you perform the same setup tasks as those available using a Web browser. In addition, there are some local configuration parameters that can be setup such as which sites are loaded at startup and how e-mail notifications will be configured.

Display Details

Add Location

Update Location

Remove Location

Location Settings

Disconnect

This menu can be accessed from the "Hosts" button of the main display, or you can right click on the grid. The menu is context sensitive when you right click on the grid, meaning that it will enable the configuration for the specific site that you click on.

The "Location Settings" is where you access the configuration setup for each of your Sentinals.

The basic site configuration parameters are exactly the same as those found using your Web browser, but they are broken into six sections for easy management. Each of the sections is represented by a tab in the configuration menu.

The image shows five screenshots of the configuration software, each representing a different tab in the configuration menu. The tabs are: Tolerance, Communication, Alarms, Labels, and Administrative. Each screenshot shows various configuration options and checkboxes for that specific section.

The Hardware based configuration setup forms are the first five tabs. Note that configurations can be exported to (saved), or imported from, local files. The configuration check-boxes at the bottom of the form are global switches.

Settings for 192.168.0.61:80

Notifications

| Wait | Email Address | Time | Event |
|------|---------------|--------|-------|
| 0 | test@###.org | Always | All |

Add/Update Remove test@###.org [Always] Test2@*****.org [Always]

Alarm validation: 60 seconds Edit Master List

Channel Enables

Enable left channel monitoring Import Close

Enable right channel monitoring Export

Master Email List

| Mem # | Email Address | Name | Time |
|-------|-----------------|------|--------|
| 1 | test@###.org | | Always |
| 2 | Test2@*****.org | | Always |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |

Click on a line to add an address or edit one.

Email Options Send SMS Save Emails Close

Master Email List

SMTP Server: smtp.abcddefg.com Sender's Email: jess@mymail.com

Send via Outlook Express Port: 25 Send Test Email

Requires Authentication

Username: Acc't name here Additional Options

Password: Password Done

Email Options Send SMS Save Emails Close

Win-7 Note: Windows 7 has a mail merge bug that can prevent Outlook Express from properly handling external e-mail. A hotfix is available from Microsoft.

Email options (right) is where you setup your account information, etc. If you have Outlook Express installed on your PC and configured, the software can send e-mails via OE instead of directly. This is very useful where encryption is required. The software can also send SMS messages to most services (text rates of your carrier may apply).

The Outlook Express mailer option assumes that OE is your default mailer. If another program is your default mailer, then the default mailer will be used. If your software has a security option to "notify me when someone sends mail as me", this option must be disabled. In OE, this is in the "options/security tab. Security settings in the full version of MS Outlook prevent it from being used. This could be true of other mail clients, too, so be sure to check first. If you want to send multiple e-mails using OE, you can put all e-mails on one line (send all at once) with a comma separator between recipients (no spaces) or you can leave them as separate entries in the master list. If separate entries are used, allow 1 to 2 minutes minimum between each mailing.

Specifications

| | |
|-------------------|---|
| Dimensions | 1.75" H x 8.5" W x 6" D 1RU rack-shelf-mountable |
| Weight | approx. 3 lbs. |
| Power | 15Vdc supplied by included 117VAC @ 60 Hz wall adaptor |
| Relays | 6 SPDT relays rated at 10va @ 15 VDC. 4 DPDT relays rated at 1 A @ 30 VDC, 0.3 A @ 125 VAC for 5×10^5 cycles. |



CAUTION: While the Sentinal's DPDT relays can handle 120 VAC, this practice is very dangerous and is strongly discouraged by CircuitWerkes. Switching of high voltages should only be done in a manner which isolates the voltages from accidental contact with people. Don't do it!

| | |
|------------------------|---|
| Metering Inputs | 2 AC audio inputs ¼" TRS jacks capable of accepting -20 to +10dBm with reference to ground. |
| Status Inputs | 2 contact-closure inputs. Pull to ground to activate. |
| Ethernet | Internal Web server with DHCP or static IP capability. Browser must have Javascript. |
| Alarms | 9 onboard alarms can respond to 32 possible conditions, each. Responses can consist of single or up to 3 actions, performed in sequence, with user defined pauses. A list of 23 available actions lets the user define which actions can be taken for a given alarm. |
| Notifications | The included free software can monitor one, or multiple sites and send e-mails or SMS messages when alarm conditions are present. For secured mail servers, there is an option to use the default mailer program, such as Outlook Express, to send the notifications. |

Warranty

CircuitWerkes, Inc. (Manufacturer) warrants that this product is free of defects in both materials and workmanship. Should any part of this equipment be defective, Manufacturer agrees, at its option, to:

- A. Repair or replace any defective part free of charge (except transportation charges) for a period of two years from the date of the original purchase, provided the owner returns the equipment to the Manufacturer at the address set forth below or stated at time of RMA issue from Manufacturer. No charge will be made for parts or labor during this period:
- B. Furnish replacement for any defective parts in the equipment for a period of two years from the date of original purchase. Replacement parts shall be furnished without charge, except labor and transportation.

This warranty excludes assembled products not manufactured by Manufacturer whether or not they are incorporated in a Manufacturer product or sold under a Manufacturer part or model number.

THIS WARRANTY IS VOID IF:

- A. The equipment has been damaged by negligence, accident, act-of-God or mishandling, or has not been operated in accordance with the procedures described in the operating and technical instructions; or,
- B. The equipment has been altered or repaired by other than Manufacturer or authorized service representative of Manufacturer; or,
- C. Adaptations or accessories other than those manufactured or provided by Manufacturer have been made or attached to the equipment which, in the determination of Manufacturer, shall have affected the performance, safety or reliability of the equipment; or,
- D. The equipment's original serial number (if applicable) has been modified or removed.

NO OTHER WARRANTY, EXPRESS OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR USE, APPLIES TO THE EQUIPMENT, nor is any person or company authorized to assume any warranty for Manufacturer or any other liability in connection with the sale of Manufacturer's products.

Manufacturer does not assume any responsibility for consequential damages, expenses or loss of revenue or property, inconvenience or interruption in operation experienced by the customer due to malfunction in the purchased equipment. No warranty service performed on any product shall extend the applicable warranty period.

In case of unsatisfactory operation, the purchaser shall promptly notify Manufacturer at the address set forth below in writing, giving full particulars as to the defects or unsatisfactory operation. Upon receipt of such notice, manufacturer will give instructions respecting the shipment of the equipment, or such other matters as it elects to honor this warranty as above provided. This warranty does not cover damage to the equipment during shipping and Manufacturer assumes no responsibility for such damage. All shipping costs shall be paid by the customer.

Repair or Service Information

In the event of the need for service or repair, call CircuitWerkes at (352) 335-6555 for a Return Merchandise Authorization number (RMA). Then carefully package the unit along with a note of the problem and send it to the address below. Be sure to include your contact information (address - not PO Box - telephone numbers) and best time to call.

This warranty extends only to the original purchaser and is not assign-able or transferable.

CircuitWerkes • 2805 NW 6th Street • Gainesville, FL 32609
Voice 352.335.6555 • Fax 352.380.0230 • info@circuitwerkes.com • www.circuitwerkes.com

