



Sentry LANServer

USERS MANUAL

This manual will help the user set up the Sentry LANServer; browse to the various pages and provides basic troubleshooting guidelines. If the user is going beyond the standard web pages provided with the LANServer and needs to design and construct specific pages then please use the manual "Sentry LANServer – Developer's Manual".

APPLICABILITY & EFFECTIVITY

This manual provides instructions for the following Sierra Monitor products:

Model	Description
5391-01	Sentry LANServer, 1-4 Sentry Controllers
5391-02	Sentry LANServer, 5+ Sentry Controllers

The instructions are effective for the above models as of December 1, 1998

Instruction Manual Part Number: T12017
Rev.A1.

Table of Contents

1.	PRODUCT DESCRIPTION	4
1.1.	General	4
1.2.	Features.....	4
1.3.	Operation	4
1.4.	Sentry Firmware Version	5
1.5.	Connections	5
2.	QUICK START	8
2.1.	LANServer Terminology	8
2.2.	Quick Start	8
3.	BROWSER SECURITY SETTINGS	9
3.1.	ActiveX Controls and Security	9
3.2.	Setting Browser Security Settings for ActiveX controls	9
3.3.	Cookies and Browser Security.....	11
3.4.	Setting the Browser Privacy Settings for Cookies	11
4.	OTHER BROWSING COMPUTER SETTINGS	13
4.1.	Synchronizing/Setting LANServer Time.....	13
5.	BROWSING AND INTERPRETING SENTRY INFORMATION	14
5.1.	General Browsing - Navigating	14
5.2.	Interpreting Zone Buttons	14
5.3.	Interpreting Sentry-Sensor Controls	16
5.4.	Interpreting Sentry -Combo Controls	17
5.5.	Interpreting Sentry Alarms.....	18
5.6.	Understanding the Alarm Table Colors.....	19
5.7.	Acknowledging Alarms	19
5.8.	Interpreting Sentry Events	21
5.8.1.	<i>Event Report Types</i>	21
5.9.	Understanding the Events Page	23
5.9.1.	<i>Events Page and the Date / Time</i>	23
5.9.2.	<i>What happens if Event Logging is disabled?</i>	23
5.9.3.	<i>Potential Problems with Event Logging</i>	24
5.10.	Managing Sentry Events	25
5.10.1.	<i>Uploading</i>	25
5.10.2.	<i>How Event Time Stamps are reported</i>	26
5.10.3.	<i>Manual upload</i>	26
5.10.4.	<i>Potential Problems with an Upload</i>	26
5.11.	Interpreting the Sentry Face Plate	27
5.11.1.	<i>Troubleshooting the Sentry FacePlate Screen</i>	31
5.12.	Backing Up the Sentry Calibration Data	32
5.12.1.	<i>Calibration Backup Control</i>	32
5.13.	Interpreting Analog, Text and LED controls	34
5.13.1.	<i>Analog Controls</i>	35
5.13.2.	<i>Text Controls</i>	35
5.13.3.	<i>LED Controls</i>	36
5.14.	Using the LANServer to allow customers to upload files.....	37
APPENDIX 1.	TROUBLESHOOTING	38
Appendix 1.1.	Objects Report 'Offline'	38
Appendix 1.2.	Objects report 'Not Found'	38

Appendix 1.3.	Page login.htm not found	38
Appendix 1.4.	User ids and passwords are not available for validation. Try again.	38
Appendix 1.5.	Alarm Page doesn't auto refresh when there is a new alarm.....	38
Appendix 1.6.	Buttons Display in White	39
Appendix 1.7.	Cookie Length.....	39
Appendix 1.8.	Sentry Calibration Backup (SentryBK) produces a warning message on completion.	40
Appendix 1.9.	LANServer Configuration LED	40
APPENDIX 2.	LANSERVER ERROR MESSAGES	41
APPENDIX 3.	WINSOCK ERROR MESSAGES	46
APPENDIX 4.	FIELDSEVER ACTIVEX CONTROLS.....	56
Appendix 4.1.	Ana1	56
Appendix 4.2.	LED1.....	56
Appendix 4.3.	Char1.....	56
Appendix 4.4.	Limitations and Supported Environments.....	57
APPENDIX 5.	GENERAL	58
Appendix 5.1.	9.1 Browser Caching.....	58

1. Product Description

1.1. General

Sierra Monitor Corporation offers a wide range of choices for data output from Sentry Gas Monitoring systems. In some cases a simple printer output of gas conditions, calibration confirmations and alarms is satisfactory to meet due diligence requirements. In large plant-wide monitoring situations the Modbus serial communications output is used to interface to existing or new GUI programs that might include information from other safety and process systems in the plant. For most applications the solution lies between these two choices. The Sentry LANServer has been developed to combine the power and flexibility of the Sentry Gas Risk Management System with the interoperability strength of the FieldServer LANServer from FieldServer Technologies. The reliability of a proven gas detection system is combined with the modern technology of the web.

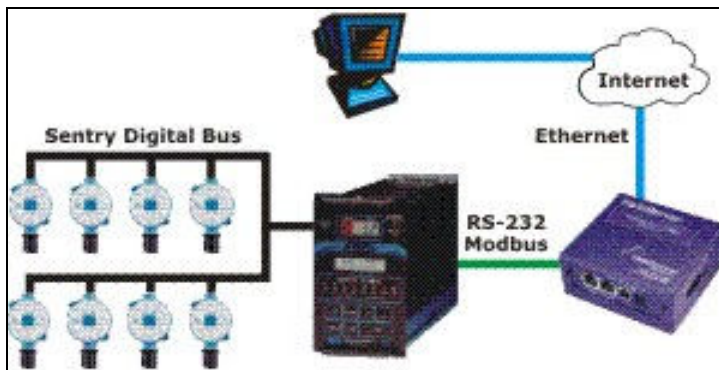
1.2. Features

The LANServer provides a cost-effective, easy-to-use graphical display of hazardous gas conditions using the Microsoft™ Explorer web-browser

- Safety data presented visually on a PC located in the plant or remotely
- Interaction with the hazardous gas detection system through a familiar web browser - no requirement to learn a new GUI program
- Ability to web-browse to system data using LAN, WAN or over the Internet
- Easy to configure graphical color changes are displayed as events
- All current alarms dynamically displayed and updated on a single web page
- An event log provides easy access to history for due diligence
- Cost-effective system includes ActiveX tools to configure using Microsoft FrontPage.
- The full system available from a single supplier with an outstanding reputation for before and after sales technical support

1.3. Operation

All of the data available from the Sentry Modbus serial communications link interfaces to the LANServer via an RS-232 link. The LANServer converts the information into a graphical display package that can be viewed using Microsoft Internet Explorer. Standard introductory screens enable the user to start operating immediately. Configuration software and the ActiveX tools supplied enable the user to modify the provided display to individual specifications using Microsoft FrontPage. Sierra Monitor can provide graphical design and development service if desired.



The standard LANServer package includes a “home” screen, a **graphical “zone”** screen, a **tabular “zone”** screen, an **alarms** screen, an **event log** screen and the **Sentry display** screen. The Alarms page contains all active alarms and notes whether or not they have been acknowledged. The Event Log page notes all events (alarms and change of states) that have occurred over a recent period of time.

1.4. Sentry Firmware Version

The LANServer is designed to work with Sentry controllers containing Sentry Firmware of version 6.10bF or newer. If the Sentry controller in question has an older firmware version please contact Sierra Monitor or a local SMC representative to obtain the necessary upgrade.

1.5. Connections

The standard Sentry LANServer Model 5391-01 includes the FieldServer Technologies LANServer plus the necessary cables and connectors to interface the LANServer to the Sentry controller and to the Ethernet. In a typical application the LANServer will be mounted in a NEMA 4X enclosure with the Sentry controller (Figure 1.1). If ordered with a Sentry NEMA 4X package the LANServer will already be installed in the enclosure with the serial connection from the LANServer to the Sentry controller(s). The LANServer will also be connected to an RJ45 connection mounted on the outside of the enclosure to which the user can connect to the LANServer via the web, WAN or Internet.

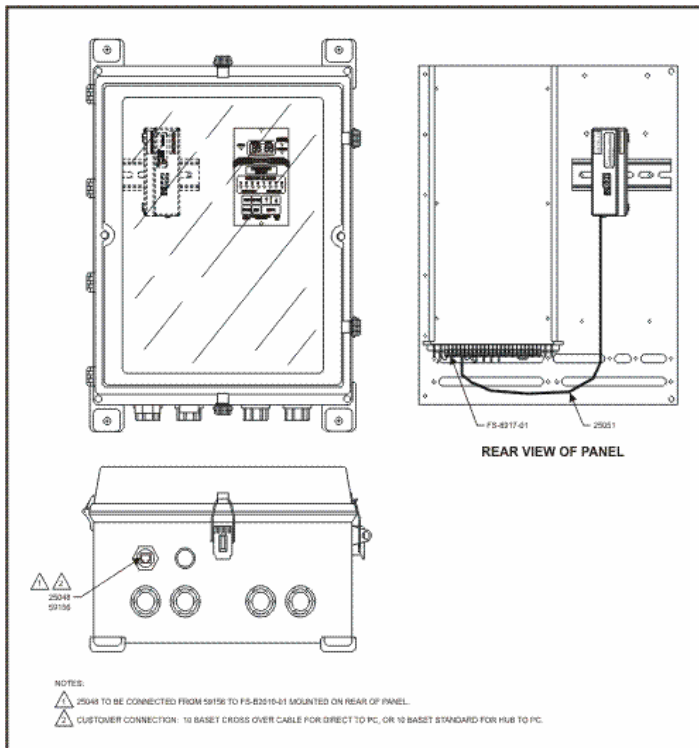


Fig 1.1: Model 5391-01 LANServer in NEMA 4X Enclosure

In applications where only one Sentry controller is involved (1 to 8 sensors) the LANServer will connect to the Sentry controller via RS-232 and to the PC with the LAN browser via a crossover Cat5 cable (or via a hub with a standard cat5 cable). (Figure 1.2)

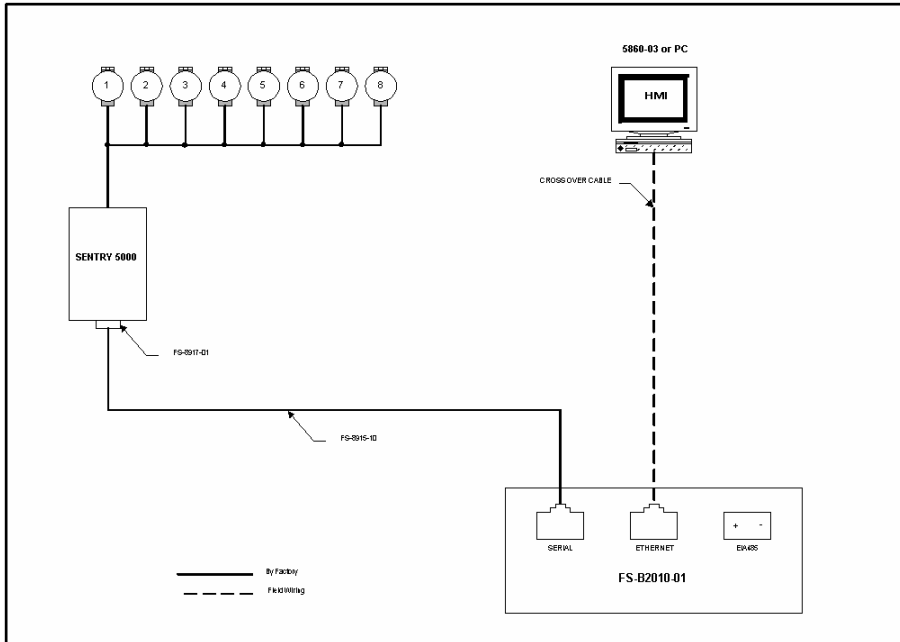


Fig 1.2: Model 5391-01 LANServer with single Sentry Controller

For applications requiring the use of 2 to 4 Sentry controllers it is necessary to utilize RS-485 communication from the controllers to the LANServer. Each Sentry will have a 4301-10 RS-232/RS-485 converter to provide the necessary RS-485 communication from the Sentry. This RS-485 link will interface to the RS-485 port on the LANServer. The Ethernet output from the LANServer can then interface directly to a computer (via a crossover cable) or to the LAN, WAN, Internet or PC via a hub. (Figure 1.3)

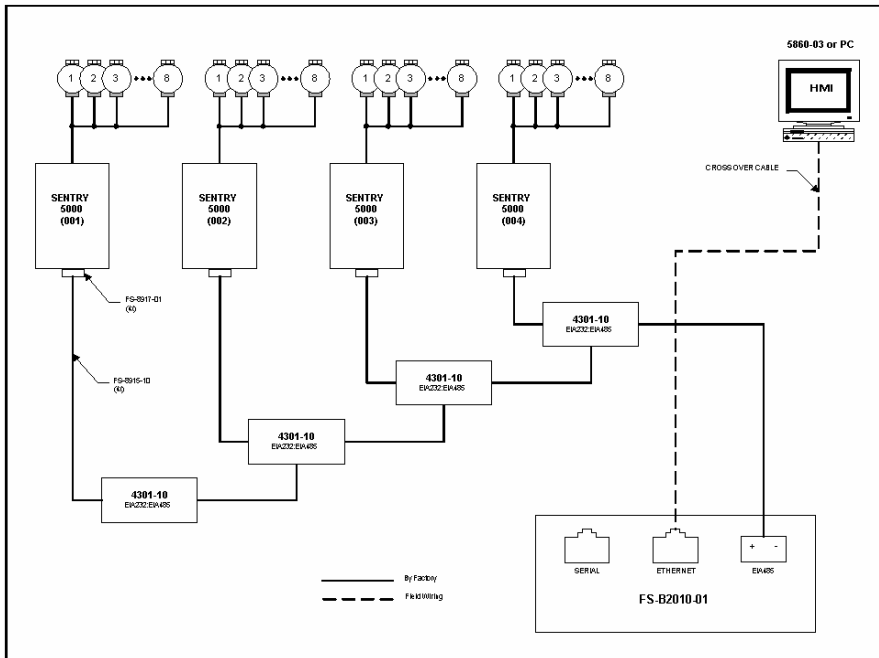


Fig. 1.3: Model 5391-01 LANServer with 2-4 Sentry Controllers

In applications calling for greater than 4 Sentry controllers it will be necessary to use the Model 5391-02 LANServer which consist of the larger multiport LANServer from FieldServer Technologies. In such applications multiple Sentry controllers can interface to the LANServer via either RS-232 or RS-485 interface and the LANServer will interface to the PC, LAN, WAN or Internet via the Ethernet port. (Figure 1.4)

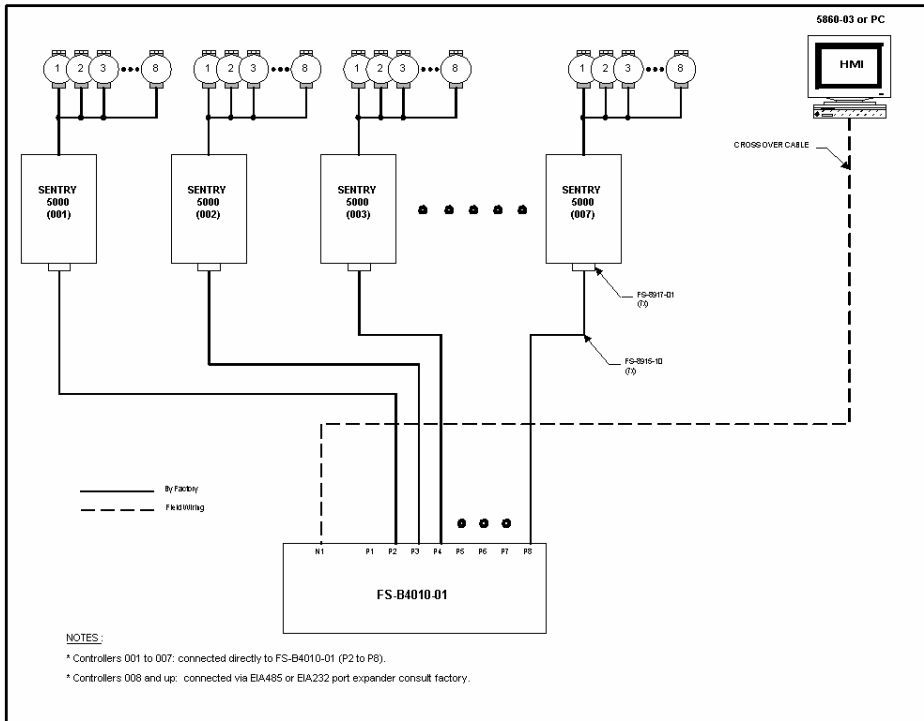


Fig 1.4: Model 5391-02 LANServer with greater than 4 Sentry Controllers

2. Quick Start

2.1. LANServer Terminology

Browsing PC	The PC being used to view the web pages.
LANServer	A LANServer is a program that, using the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to browsing PC. As an example, every computer on the Internet that contains a Web site must have a Web server program.
Web Browser	The software application used to connect to and view pages on the Internet. The Sentry LANServer is designed to be view on Internet Explorer. If using another Web Browser check with Sierra Monitor for compatibility.

2.2. Quick Start

Step 1: Find the IP address of the Sentry LANServer
This should be provided. Otherwise use the utility "RUIPING" on the Utility CD -ROM to locate and identify the IP address of the LANServer in question.

Step 2: Start the browser

Step 3: Browse to the Sentry LANServer



The Sentry LANServer "home" page will appear

Step 4: Continue Browsing.

Use the buttons and links included on the Web Pages as well as the 'back' button to navigate from page to page.

3. Browser Security Settings

Security Settings must be set to enable the use of ActiveX controls and Cookies. Unless specifically informed which settings to adjust **assume that both groups of settings must be configured correctly.**

3.1. ActiveX Controls and Security

ActiveX controls can have access to the resources of the computer on which they are running. For this reason they may be considered a security risk. The ActiveX controls provided by Sierra Monitor only use the network connection resource of the computer. They never access the disk or file storage system or any personal or private information on the computer and they never send Sierra Monitor any information other than that documented for each control. Neither Sierra Monitor nor anyone else can use these ActiveX controls (as distributed) to compromise the system security

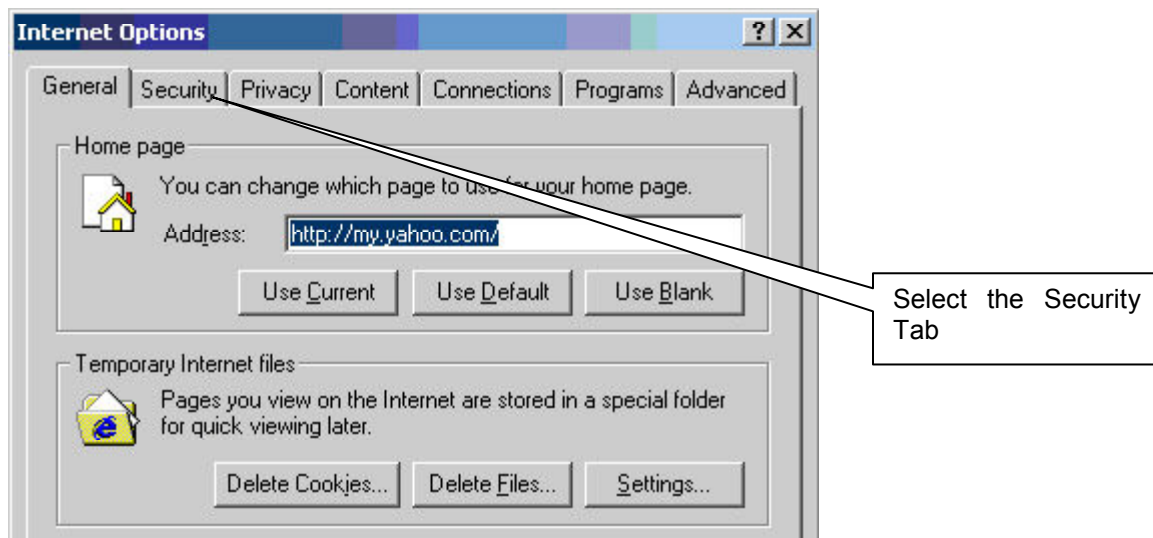
As there is a theoretical security risk, most browser's have default security settings which do not allow ActiveX controls to be run on a computer. The following information outlines how to change the default security settings to allow the ActiveX controls to run on the computer.

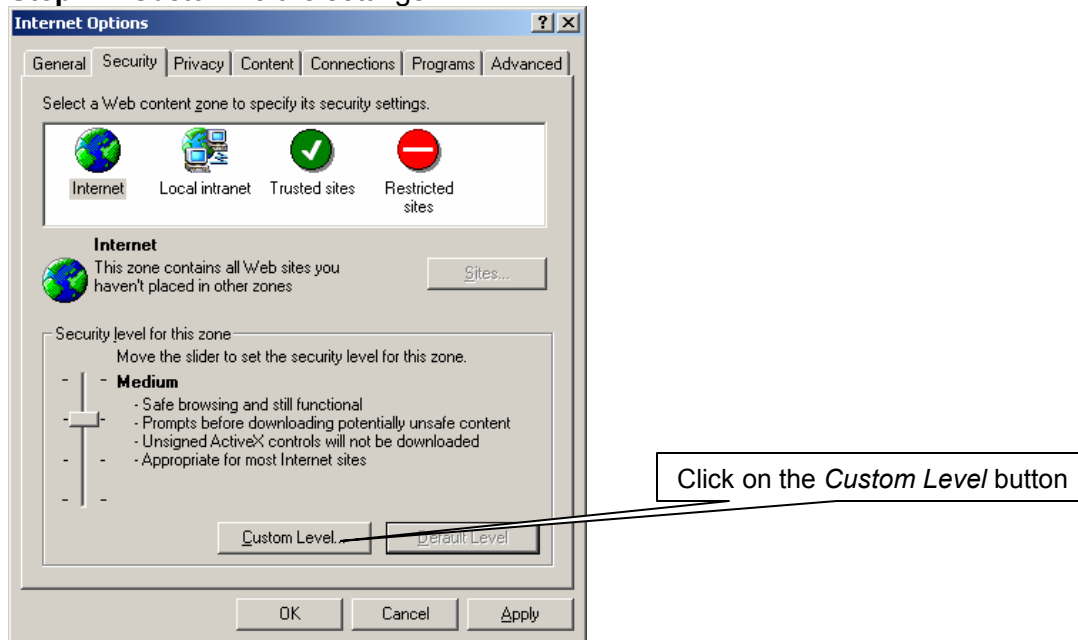
Note that some controls provided by Sierra Monitor may access the computer's resources in a way that conflicts with these statements. In this case the "Constructing a Sentry LANServer Project" manual will specify which other resources the ActiveX control uses.

3.2. Setting Browser Security Settings for ActiveX controls

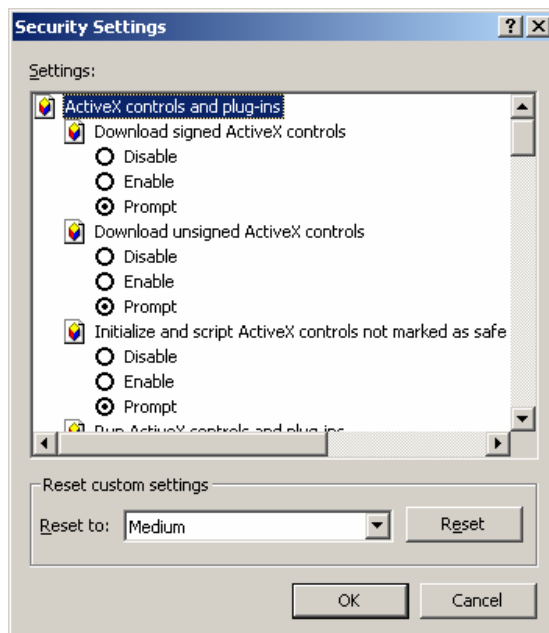
The following notes and examples apply to Internet Explorer 6. Other browsers have similar features and which are set in a similar way. Use the documentation of the browser to determine how to adjust the settings.

Step 1 – From the browser's pull down menu, select **Tools|Internet Options**.



Step 2 – Customize the settings.**Step 3 - Change the following settings**

- Download signed ActiveX Controls: Enable or Prompt
- Download unsigned ActiveX Controls: Enable or Prompt
- Initialize and Script ActiveX Controls not marked as safe: Enable or Prompt
- Run Active X Controls and plug-ins: Enable or Prompt
- Initialize and Script ActiveX Controls marked as safe: Enable or Prompt

**Step 4 – Review**

If in doubt about the meaning or effect of any of the settings then Sierra Monitor recommends that the user consult their system administrator before changing settings.

3.3. Cookies and Browser Security

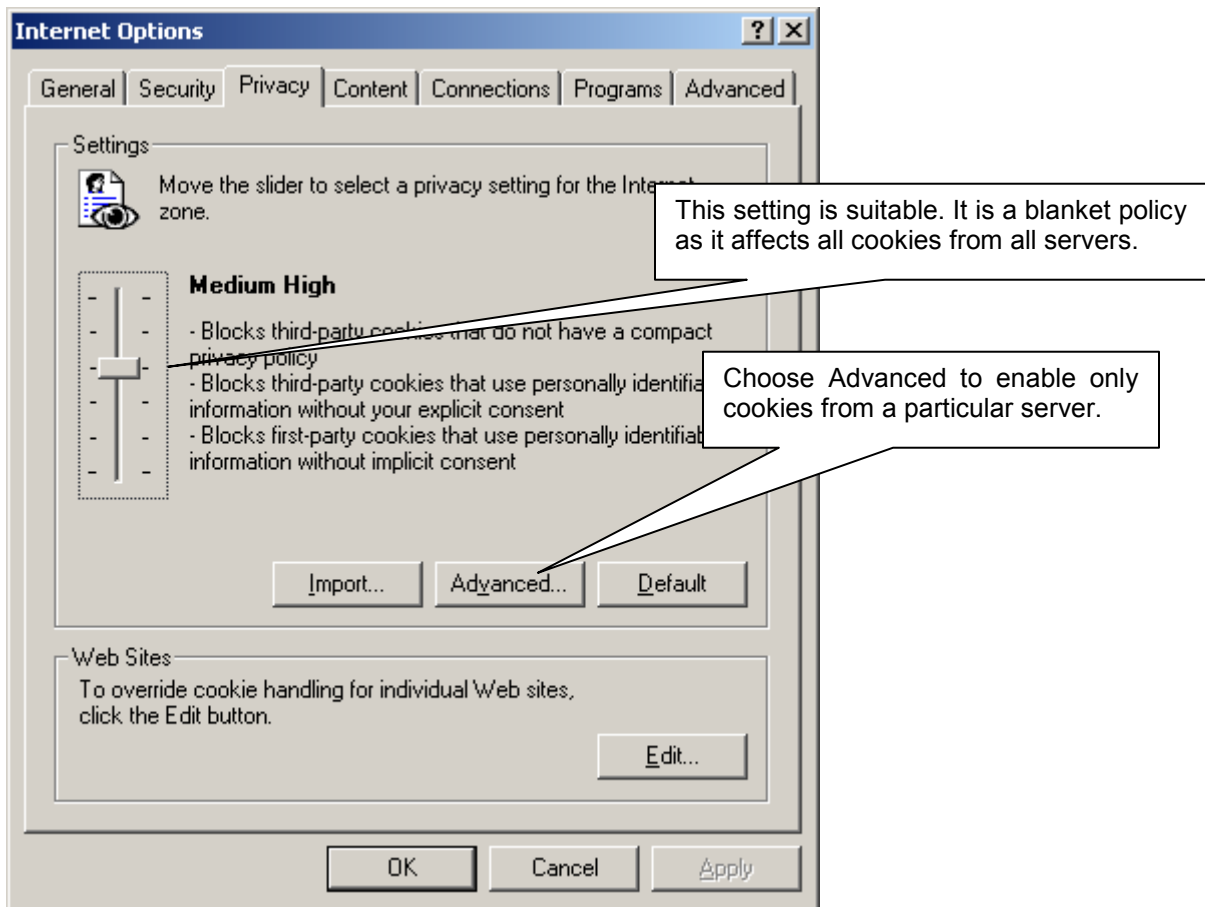
Cookies are a technology used by browsers to transfer information between a server and a browser. The transfer is bidirectional.

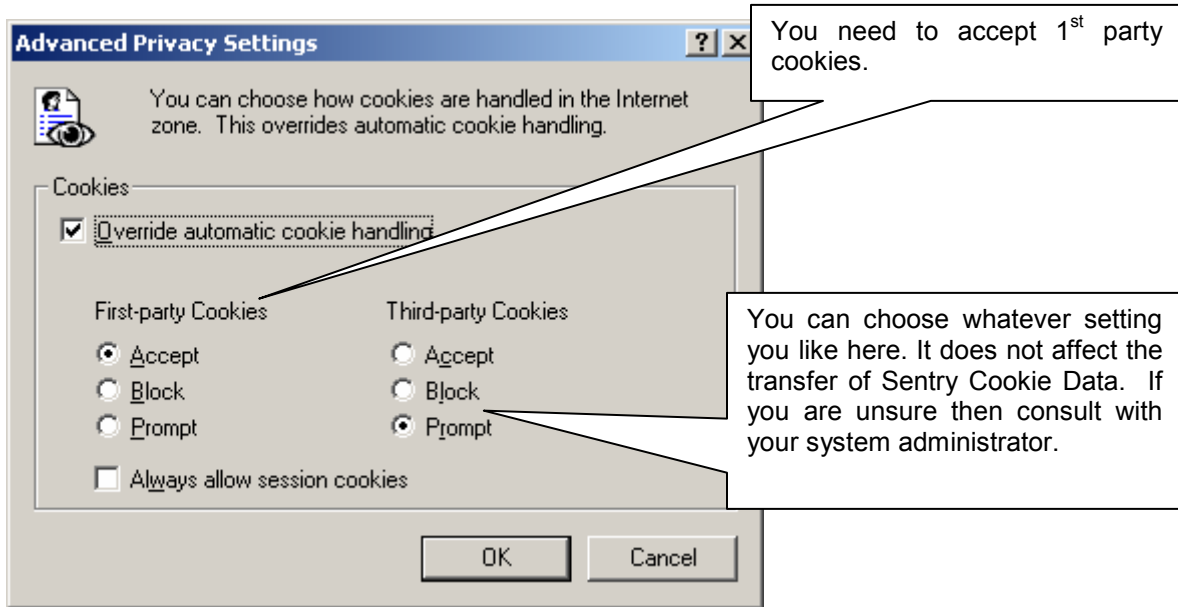
The cookies used by Sentry LANServer do not transfer any data about the user, the user's computer or preferences. Consider the use of Sierra Monitor cookies as safe.

It is necessary set the browser privacy settings to enable cookies. This can be applied as a blanket policy or the user can enable cookies from a particular server (in this case from a particular LANServer.)

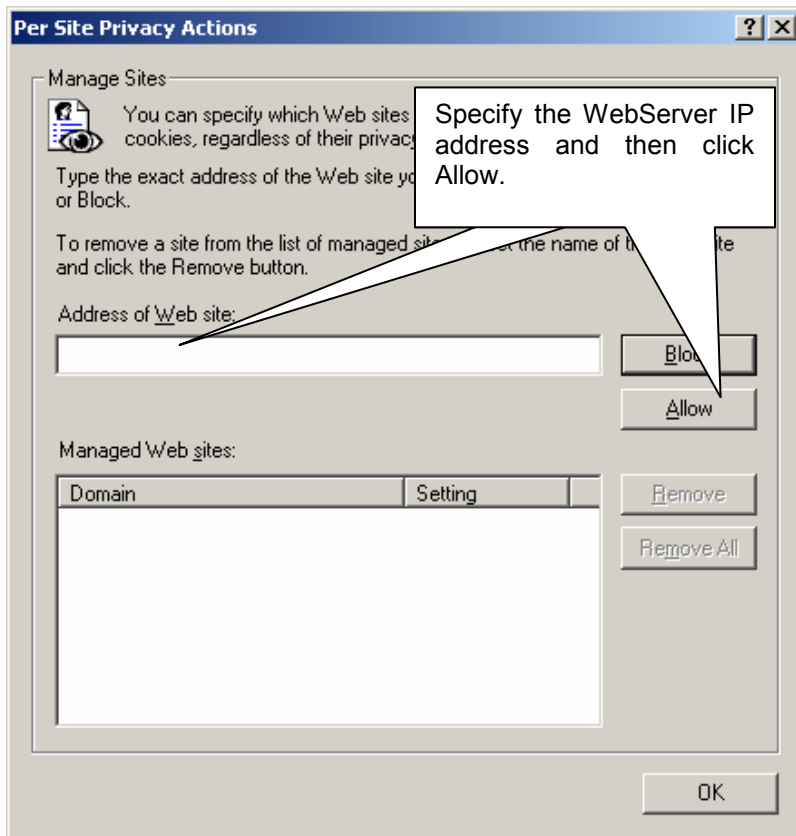
3.4. Setting the Browser Privacy Settings for Cookies

The following notes and dialogs apply to Internet Explorer Version 6.





Allowing cookies from a particular server is done by adding the server's name or IP Address.



4. Other Browsing Computer Settings

4.1. Synchronizing/Setting LANServer Time

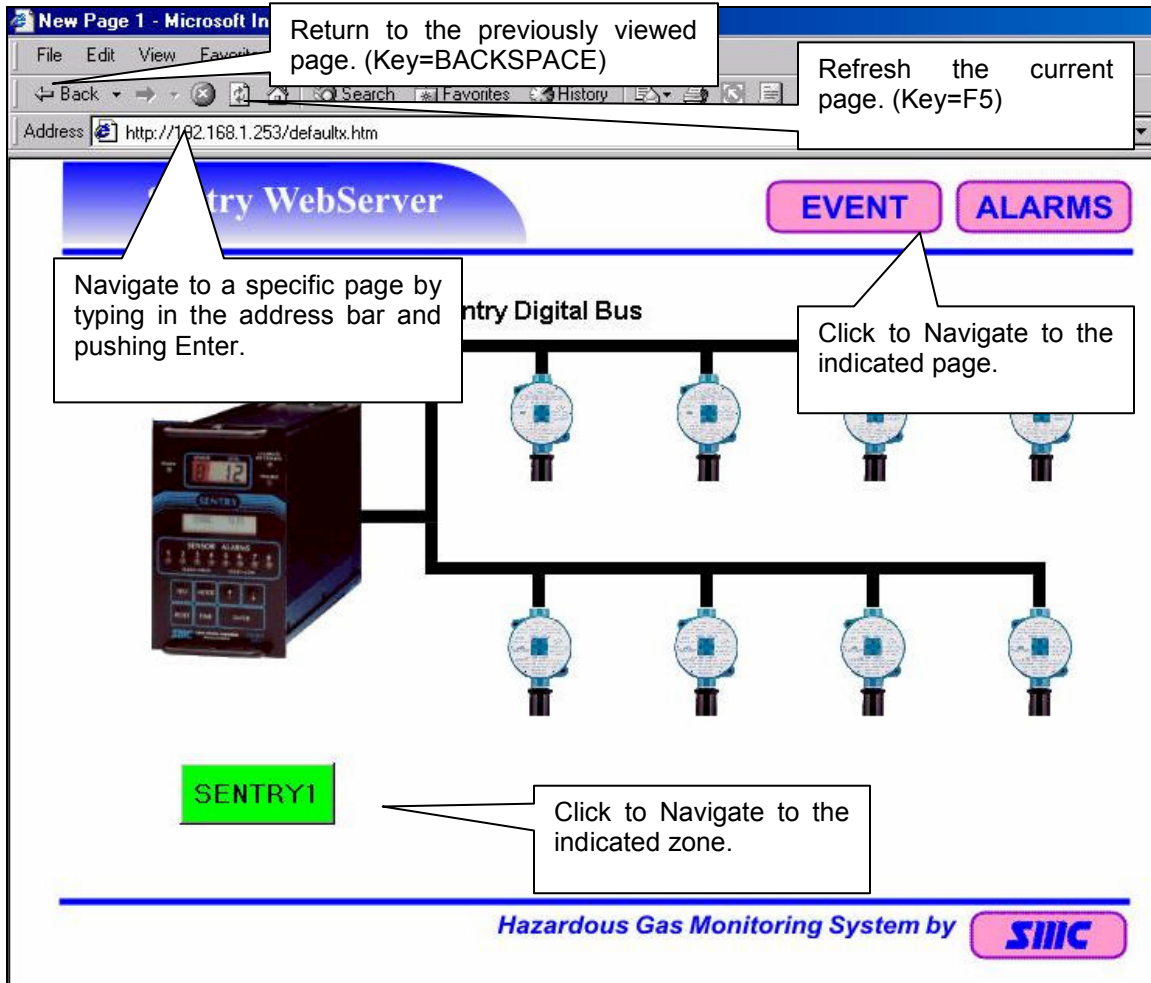
This is done with a utility called RUINET. This is fully described in the LANServer Troubleshooting guide. The main points of the procedure are repeated below.

- Set the PC to the date and time required.
- Connect to the LANServer using RUINET (installed with the Utility's CD shipped with the LANServer).
- Navigate to the Bridge Screen (B Key)
- Synchronize the time using the T Key.

The time zone of the LANServer is fixed in Pacific Standard Time.

5. Browsing and Interpreting Sentry Information

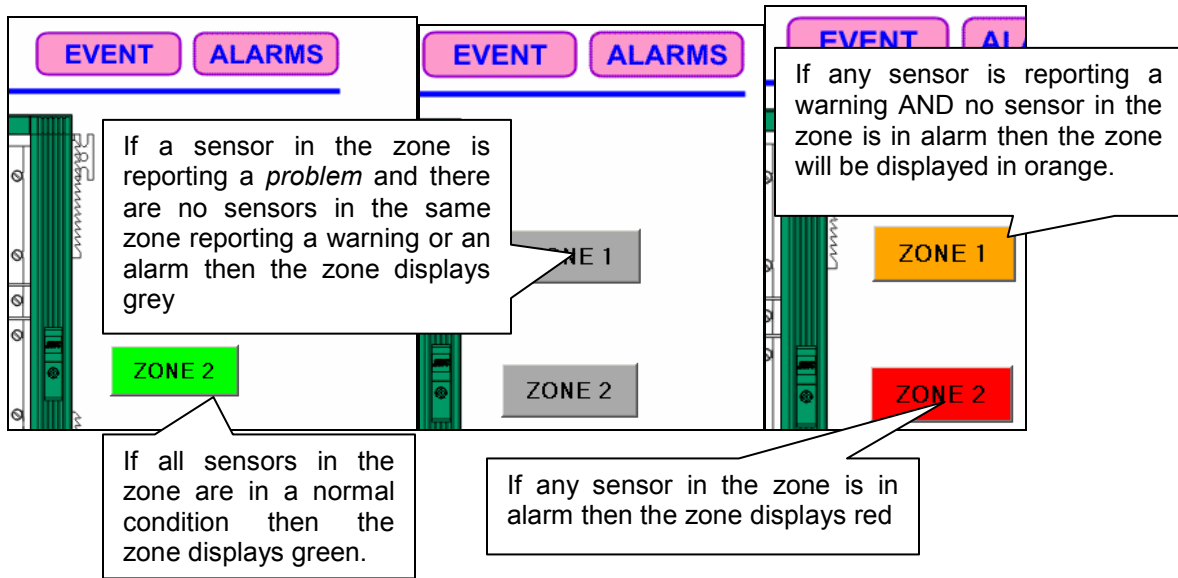
5.1. General Browsing - Navigating



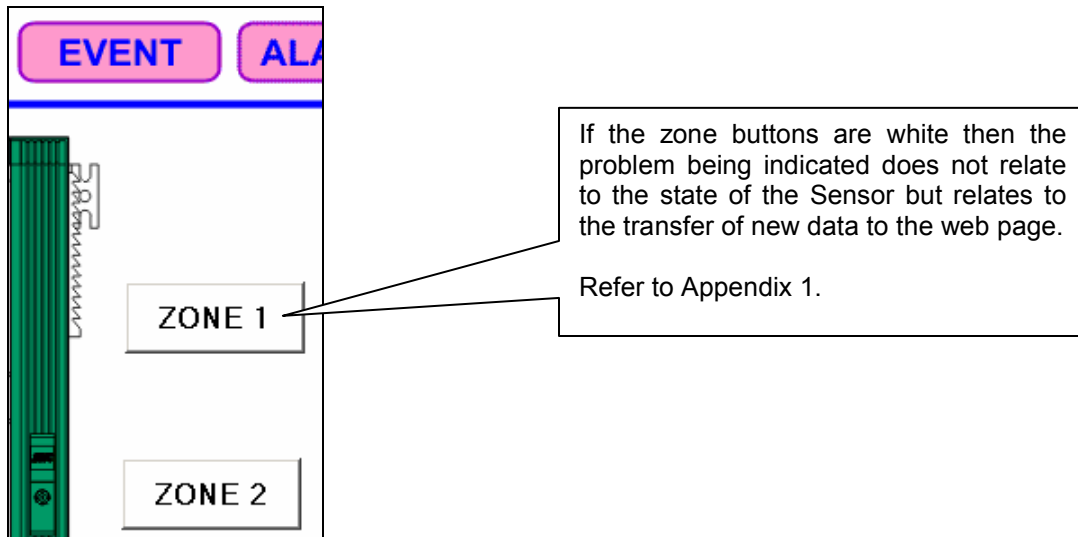
5.2. Interpreting Zone Buttons

Zone buttons report the status of a logical collection of Sentry-Sensor's. A sentry consists of up to 8 sensors. A Zone is a collection of sensors based on a logic grouping such as geographic location in a building, thus a zone can consist of:

- Some sensors from one Sentry
- All the sensors from one Sentry
- One or more sensors from one or more Sentry's.



Problem	The sensor reports that the analog value is invalid.
Warning	A concentration level above the warning set point. This also activates the warning relay on the Sentry.
Alarm	A concentration level above the alarm set point. This also activates the alarm relay on the Sentry.
Normal	None of the above.

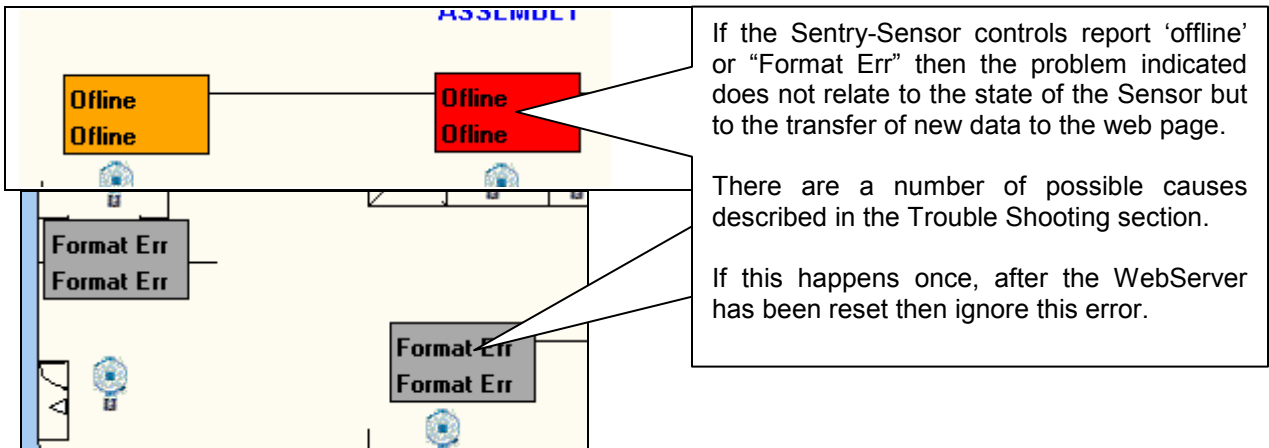
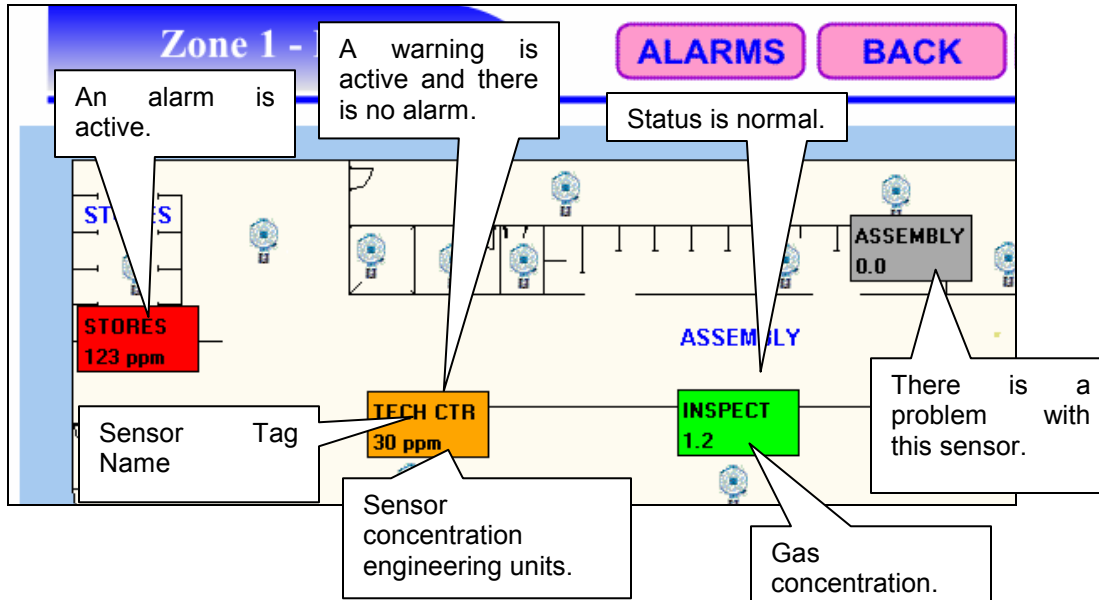


5.3. Interpreting Sentry-Sensor Controls

A Sentry-Sensor control presents data for one single sensor one single Sentry. The color changes to report the status, and the control displays the gas concentration, tag name and units.

Red: Sensor concentration is above the alarm set point.

Orange: Sensor concentration is above warning set point.



5.4. Interpreting Sentry -Combo Controls

Sentry-Combo controls are very similar to Sentry-Sensor controls.

Color	Read the notes in the previous section. The same considerations apply.
Sensor Tag Name	If the sensor tag name found in the Sentry is blank then the sensor tag name allocated during construction of the web page is displayed. May not be displayed –depends on the configuration of the control when the page was constructed.
Sensor Engineering Units	The engineering units as configured in the Sentry. If none are configured in the Sentry, then none are shown. May not be displayed –depends on the configuration of the control when the page was constructed.
Sensor Concentration	If the value is less than 10 then one decimal point is shown. May not be displayed –depends on the configuration of the control when the page was constructed.
Alm	Displays the alarm set point configured in the Sentry for the sensor. May not be displayed –depends on the configuration of the control when the page was constructed.
Wrn	Displays the warning set point configured in the Sentry for the sensor. May not be displayed –depends on the configuration of the control when the page was constructed.

Zone 1

ALARMS BACK HOME

ALM2

Alm: 10.0
Wrn: 20.0

ALM1 0.0 %

0.0 %LEL

ALM3 0.0 %LEL

ALM4 0.0 %LEL

ALM1 0.0 %
Alm: 10.0
Wrn: 20.0

ALM1 0.0 %

SENSOR 8 0.0 %LEL

TABLE

There is no difference between this Sentry-Combo control and a Sentry-Sensor control. In this case they show exactly the same information.

Different examples of the Sentry-Combo control. Each reports the status and concentration of one sensor.

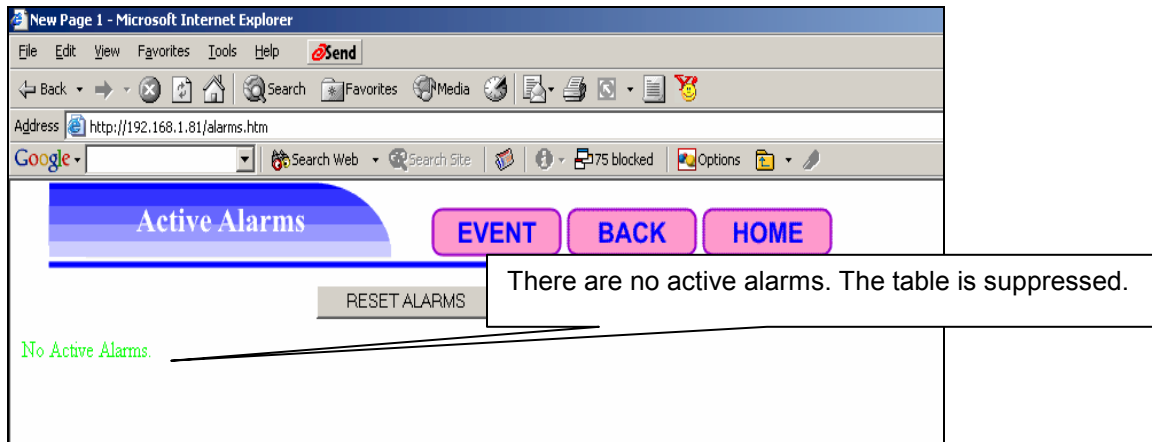
by **SIIC**

5.5. Interpreting Sentry Alarms

The Sentry alarm table reports Sentry-Sensor's that are in an alarm condition.

If the alarm conditions change while viewing the page, then the page will refresh itself. There is no alarm history. However, alarms are considered to be events and can be viewed in the event history. If there are no alarms, the table is not presented. A single line reports that there are no alarms.

The number of entries in the table depends on the number of active alarms.



The LANServer has a limited amount of memory to create alarms.htm. If, in the process of building this page, the limit is reached, before all the active alarms can be added to the table, the Server adds the following message to the bottommost row of the table: "Not enough space for all alarms!" and then stops processing additional alarms items. There is no corrective action that can be taken. While not a hard and fast rule, for version 1.08eB of the driver, a practical limit was 152 alarm items.

5.6. Understanding the Alarm Table Colors

Active Alarms

HOME

RESET ALARMS

State	tag	Value	Units
ALARM	N/A	123.4	
Warning	N/A	30.0	Units=ppm 1:2
Comm/Chan Error	N/A	0.0	Null (Unit)
Comm/Chan Error	N/A	0.0	Null (Unit)
Comm/Chan Error	N/A	0.0	Null (Unit)
Comm/Chan Error	N/A	0.0	Null (Unit)

A line in red reports an alarm.

A line in orange reports a warning.

A line in grey reports a bad channel or a loss of communication with the Sentry.

State	tag	Value	Units	Sentry.Channel
ALARM	ABCD	0.0	Units=PPM	1:1

Sentry:Sensor

Gas concentration value Engineering Units.

N/A=Null -> Engineering units could not be obtained from the Sentry

Reports the cause of the alarm.

The gas concentration value

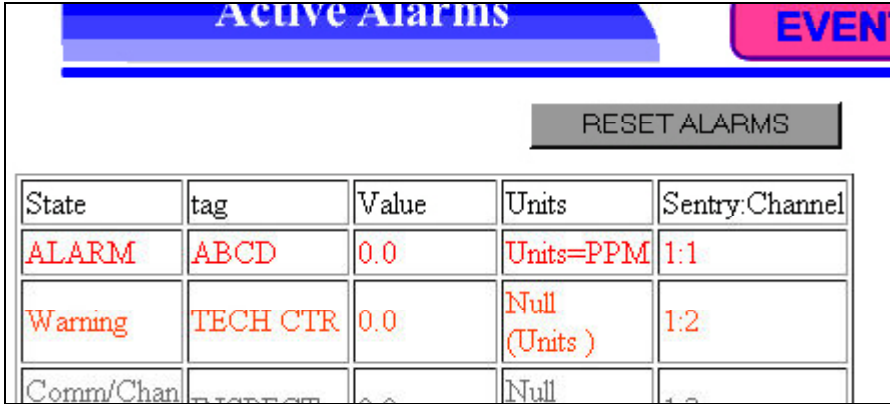
The Sensor's Tag Name. If no name has been allocated in the Sentry then the name displayed, is the name allocated by the web page builder.

5.7. Acknowledging Alarms

Normally, the LANServer project is built with an alarm acknowledge button on the alarm page. The button does not always have the same text on it – The project builder determines what text is displayed.

When pushing this button, it is effectively pushing the alarm reset button on the front panel of each Sentry connected to the LANServer.

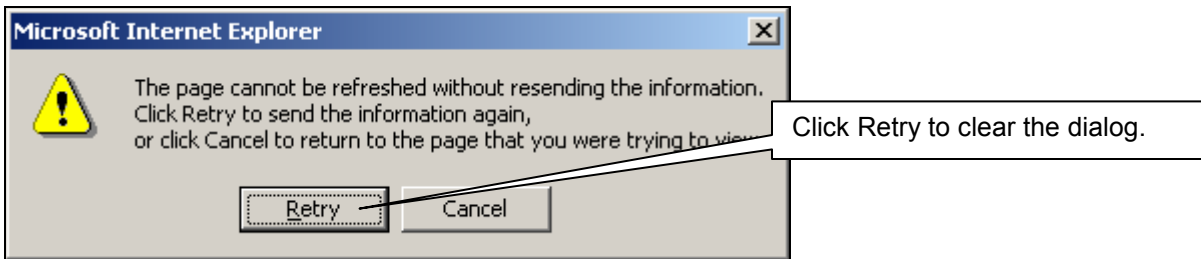
There is no harm in pushing it more than once.



The screenshot shows a web interface with a blue header bar containing the text "Active Alarms" and a pink button labeled "EVENT". Below the header is a grey button labeled "RESET ALARMS". Underneath is a table with the following data:

State	tag	Value	Units	Sentry.Channel
ALARM	ABCD	0.0	Units=PPM	1:1
Warning	TECH CTR	0.0	Null (Units)	1:2
Comm/Chan			Null	

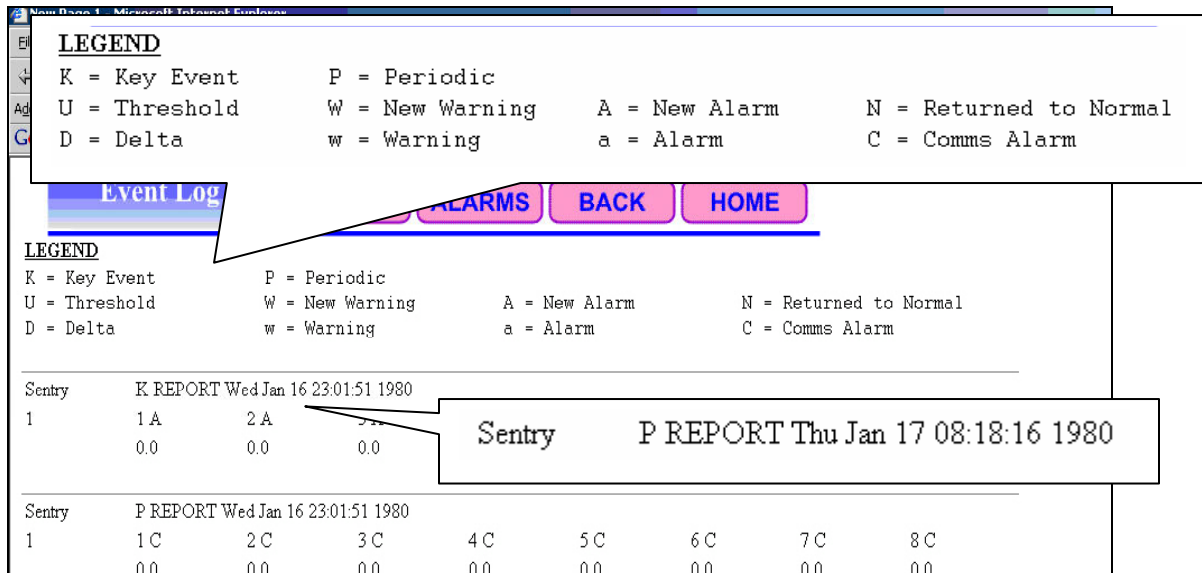
If pushing the alarm button and then Refresh, the following dialog may be presented



5.8. Interpreting Sentry Events

Sentry events are captured and stored on the LANServer’s flash disk in a file called events.dat. (Additional information on this file is provided in section 5.10 Not every LANServer project reports Sentry Events. If it isn’t present then this is a decision the web project designer made. In the template project supplied with the LANServer, sentry event logging is enabled. An events page must be part of the project and event logging must be enabled.

The event table is a human readable presentation of the event information. The most recent event is the topmost one.



5.8.1. Event Report Types

The two types of event report – K and P reports. P reports are triggered by time and K reports are triggered by a state change for a Sentry-Sensor or by a change of gas concentration.

P Reports

Periodically, the LANServer, records the gas concentration and state of each Sentry-Sensor. The period was configured by the developer who constructed the web project and can be changed. Having the P report allows the user to verify that the Sentry was being monitored during a period. If no K reports were generated because the gas levels remain normal for a long period of time then having the P reports raises the confidence that the system was working and online during that interval.

One P report will be generated each time the LANServer is restarted.

K Reports

K reports are based on Sensor state and gas concentration.

Alarm Type	Definition
Alarm (A or a)	Gas concentration is above the alarm set point. The alarm set point is commonly configured in the sentry using the font panel. Note that the LANServer reports an alarm if the sentry reports the alarm – the LANServer does not report an alarm by comparing the gas level to the set point. When reported on the event screen – the letter ' A ' indicates a new alarm and the letter ' a ' indicates the alarm is still active but this is not a new event.
Warning (W or w)	Gas concentration is above the warning set point. The warning set point is commonly configured in the sentry using the font panel. Note that the LANServer reports an warning if the sentry reports the warning – the LANServer does not report a warning by comparing the gas level to the set point. When reported on the event screen – the letter ' W ' indicates a new warning and the letter ' w ' indicates the warning is still active but this is not a new warning.
Comms (C)	This event is generated by the LANServer if a Sensor reports that the analog value is bad or if it loses communications with the Sentry. When reported on the event screen – the letter ' C ' indicates a new comms event is active.
Threshold (T)	The web project builder configured, for each Sentry-Sensor, a user threshold, which if the gas level rises above it, generated a threshold event. The evaluation of this event is performed by the LANServer; the Sentry does not report this event directly. When reported on the event screen – the letter ' T ' indicates a Threshold Event is active.
Delta (D)	The web project builder configured, for each sentry-sensor, an event delta value. If the gas level changes by more than this delta value then a delta event is generated. The gas level must be above the threshold level before delta events are evaluated. The evaluation of this event is performed by the LANServer; the Sentry does not report this event directly. When reported on the event screen – the letter ' D ' indicates Delta Event has just occurred.
Normal (N)	The LANServer reports a normal event when the state of sensor returns to normal – no alarms, no warnings, analog value is valid, no user threshold event and no delta event. The evaluation of this event is performed by the LANServer; the Sentry does not report this event directly. When reported on the event screen – the letter ' N ' indicates that the Sensor is in a normal condition.

5.9. Understanding the Events Page

One report for the Sentry, even if only one sensor on the Sentry generated the event.

The date and time the event was recorded.

There are important data and time considerations. See Section 5.9.1

Type of report.

Sentry	K REPORT Wed Jan 16 23:01:51 1980							
1	1 a DU	2 a	3 a	4 a	5 a	6 a	7 a	8 a
	12.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Event Trigger.

In this example, Sensor 1 is reporting a Threshold and Delta Event as well as indicating that an alarm event is still active (lower case). If the alarm event was new it would have been reported with an uppercase A

Notes on the previous page provide explanation of the event 'letters'

Sensor concentration levels.

gas

Sensor Numbers 1..8

5.9.1. Events Page and the Date / Time

When events are recorded, the LANServer records the event time as the number of seconds that have elapsed since Jan 1, 1970 UTC. This data is stored in the events.dat file. This provides an absolute, but inconvenient time.

When reported on the events web page, this time, is converted to a human readable form and reported in PST (Pacific Standard Time). The LANServer does not auto adjust for Daylight Savings time and hence is permanently fixed in PST.

It is important that the LANServer's data and time has been set to avoid invalid data and times in the events report. When LANServer's are shipped from the factory the date and time has not been set.

5.9.2. What happens if Event Logging is disabled?

If event logging is disabled then the events page will not update with new events and new events will not be recorded. Not every web project has event logging enabled. Furthermore the LANServer may disable event logging under certain circumstances.

If event logging is disabled then the LANServer prints a message to the Error Screen. "WEB:#42 FYI. Event storage disabled."

5.9.3. Potential Problems with Event Logging

5.9.3.1. File Problems

Events are written to file on the LANServer's flash disk. When the events page is viewed the file is read from the flash disk. Errors could occur with the file. These are reported on the error screen.

Produced when viewing events page

WEB:#19 Err. Reading event record file.

WEB:#20 Err. Bad file pos.

WEB:#21 Err. Opening event record file.

Produced when storing events

WEB:#31 Err. Cant open %s for append.

WEB:#32 Err. Event write failed.

WEB:#33 Err. Cant open %s for append

WEB:#34 Err. Cant open %s for read.

WEB:#35 Err. Event write failed.

Where %s is equal to 'events.dat' or 'events~.dat'

5.9.3.2. Space Problems

There is a limited amount of space on the flash disk. Event logging is not permitted to completely fill the free space – a minimum amount of free space is maintained.

If this threshold (currently set at 100k Bytes) is reached then event file maintenance is performed. If after the maintenance, the available space is still below the threshold then event logging is automatically disabled and the LANServer prints a message to the error screen.

5.9.3.3. Limited number of event records

The LANServer will only store a maximum (currently 400) event records. If this threshold is reached then event file maintenance is performed.

5.9.3.4. Event File Maintenance

This procedure is executed by the LANServer when there is too little space to write new event records or when the maximum number of event records has been exceeded.

The procedure is as follows:

If an event record is older than 1 day (current setting) then the record is discarded.

- If after they have been removed then if there are more than 350 records (current setting) then only the 350 most recent events are retained.
- If there is still too little space or too many records, the events.dat file is removed and all events are lost. If this happens then this message "WEB:#38 Err No space for Sentry Logging" is printed in the error log.

When event file maintenance is performed a message is printed in the error log.

5.10. Managing Sentry Events

5.10.1. Uploading

When the web project is built, the designer may place a special control on the events page allowing the user to upload a version of the events file converted for use with Microsoft Excel.

It is also possible to upload the events.dat file manually and to convert it for use with Excel using a utility provided by Sierra Monitor.

This button, when clicked will connect to a WebServer and upload events.dat to our pc and then create an Excel compatible file with the event log. The file can also be viewed using a text editor such as notepad.

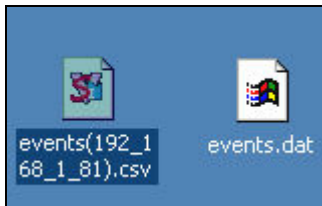
Upload

The web project may have more than one of these controls, each configured to upload events from a different LANServer.

When the operation is complete a dialog reporting “Done!” is presented. If errors occur during execution then a dialog reporting the error information is presented.

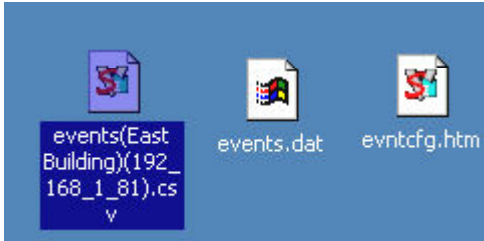
When the events.dat file has been uploaded its contents are read and converted to comma separated format (CSV). The uploaded records are appended to a file whose name is a combination of the IP address of the LANServer and events.csv (which is created if it didn't previously exist.)

Example 1: If an uploaded events.dat from a LANServer whose IP_Address is 192.168.1.81 then the name of the csv file will be “events(192_168_1_81).csv”



The file events.csv is human readable and can be opened with Excel to browse its contents. The file events.dat is a binary file whose contents cannot normally be understood by other applications. Previous versions of events.dat are overwritten. The top few rows of the events.csv file contain header and legend information.

Example: 2 Certain LANServer configurations will allocate the file name as a site name.



Example 3: The LANServer configuration is invalid. The site name was badly formatted. This does not affect the contents of the file



5.10.2. How Event Time Stamps are reported

When the events file is uploaded and converted to a CSV file, the timestamp information is printed in the CSV file in two columns; Local Time and GMT. The Local Time is always PST, despite the time zone the PC is set to. Thus the timestamp in the CSV file and the timestamp shown on the events.htm screen correspond.

If the PC's time zone is not PST, the utility will automatically attempt to adjust the printed timestamp to PST. If this adjustment cannot be made then a dialog reporting this fact is displayed and some additional information on the PC's time zone is printed in the CSV file to alert the user that the CSV time will not correspond to the events.htm screen time.

5.10.3. Manual upload

There are two possibilities:

- Use RUNET to upload the file events.dat and use the FST_Events_MFC.exe application to convert the file to a CSV file.
- Use the FST_Events_MFC.exe application to connect to a LANServer directly, upload and then convert the file.

Instructions for using this utility are provided in a separate manual.

5.10.4. Potential Problems with an Upload

Each upload control is configured to upload data from a particular LANServer. The person who built the web project configured the control by, amongst other things, specifying the IP address of the LANServer.

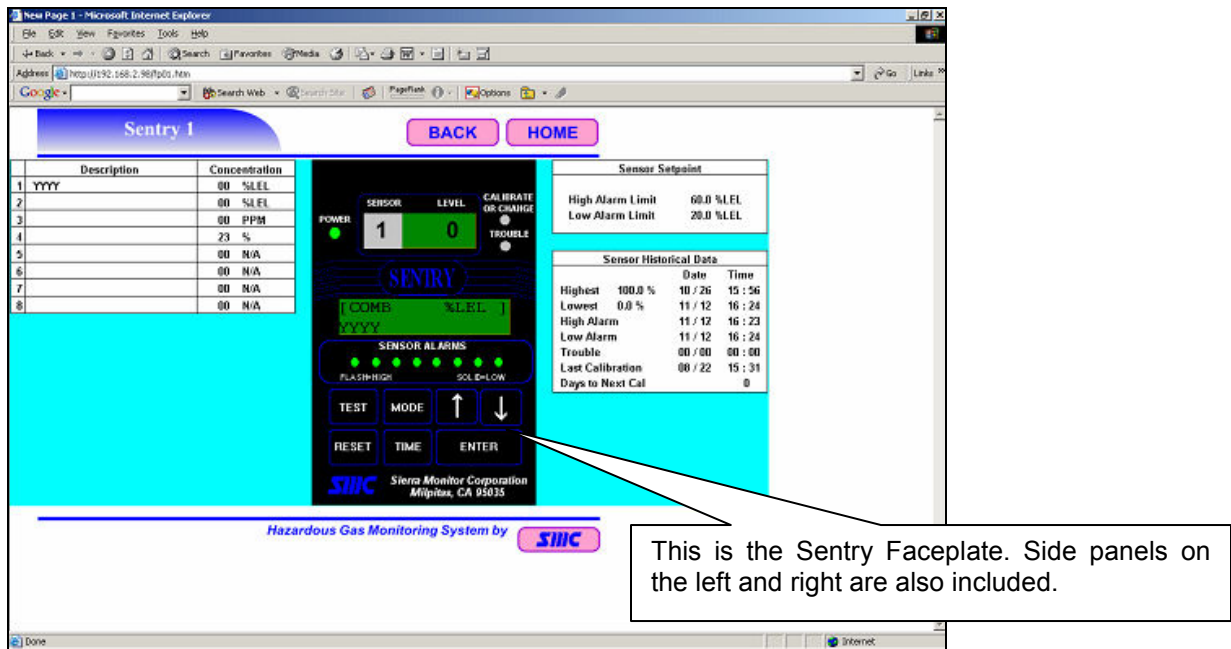
If the control cannot find that particular LANServer then it will look for another. If it only finds one other LANServer then it will upload from that one. If more than one is found then it doesn't know what to do. If either of these situations occurs then this is reported by a message on a dialog box.

Problems can occur during transmission of the file. These and other problems are reported on dialog boxes. If any occur then retry the upload.

In August 2004 a change was made to the way in which events were stored. A circular buffer was introduced. A consequence of this change is that the new versions of this ActiveX control prior to 1.04j cannot process events which were produced by LANServer firmware versions 1.08a or later.

5.11. Interpreting the Sentry Face Plate

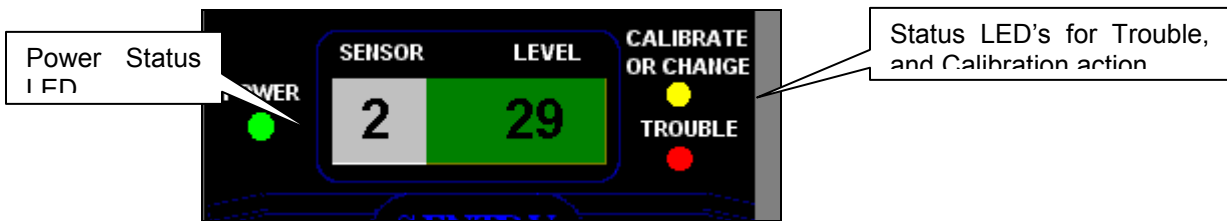
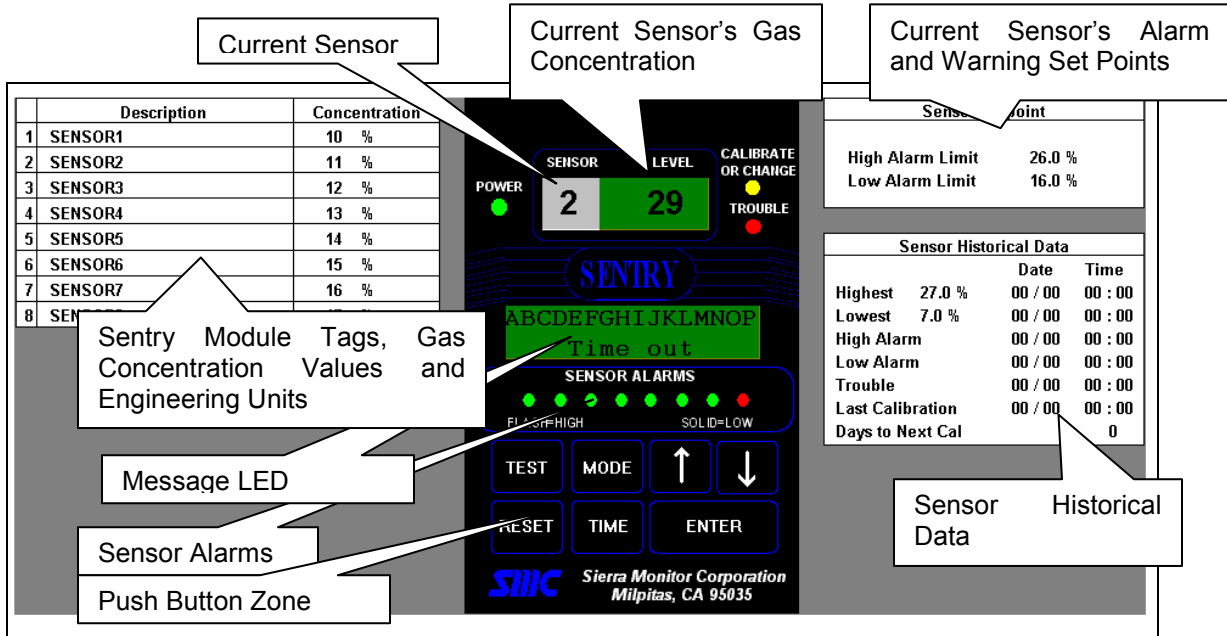
The Sentry Faceplate is an ActiveX Control which provides visualization of the Faceplate of Sentry. IT also allows the user to interact with the Sentry as if sitting in front of it. The only difference is the speed of response.



The Faceplate can only be seen on non Windows CE browsers. On a Windows CE browser the user will see an 'X' as illustrated below.



Notes on each area of the display follow on the next page.



Sentry Module Tags, Gas Concentration Values and Engineering Units

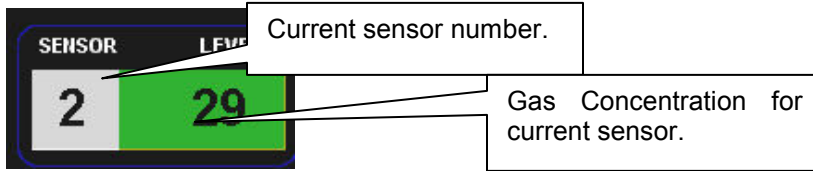
The Module Tag Name for each sensor, its current gas concentration level and the engineering units are displayed here. The data is obtained by the LANServer by reading the sentry.

	Description	Concentration
1	SENSOR1	10 PPM
2	SENSOR2	11 PPM
3	SENSOR3	12 PPM
4	SENSOR4	13 PPM
5	SENSOR5	14 PPM
6	SENSOR6	15 PPM
7	SENSOR7	16 PPM
8	SENSOR8	17 PPM

N/A maybe displayed if the information has not been defined in the Sentry.

Current Sensor

As the sentry operates its scrolls through Sensors 1 to 8. The current Sensor number is displayed here. When the Enter key has been pushed, the auto scroll stops and the Up/Dn Arrow keys may be used to scroll through Sensors 1 to 8.



Upper Display -- Current Sensor's Gas Concentration

Sometimes the level is not displayed but is replaced by error code as on the Sentry Controller. Refer to the Sentry instruction manual for information on these codes



Current Sensor's Alarm and Warning Set Points

This area displays the Alarm set point and the Warning set point. On this display the warning set point is termed the 'Low Alarm Limit'. These limits are used to control the alarm relays and affect Sentry Event Logging.

Sensor Setpoint	
High Alarm Limit	25.0 PPM
Low Alarm Limit	15.0 PPM

Sensor Historical Data

Sensor Historical Data			
		Date	Time
Highest	26.0 %	00 / 00	00 : 00
Lowest	6.0 %	00 / 00	00 : 00
High Alarm		00 / 00	00 : 00
Low Alarm		00 / 00	00 : 00
Trouble		00 / 00	00 : 00
Last Calibration		00 / 00	00 : 00
Days to Next Cal			0

If this area is filled with -1's, the data has not been read from the Sentry.

Lower Display

The information displayed in this section is the same as displayed on the Lower Display on the front of the Sentry controller. Normally the current Sensor's name and Engineering units are displayed here. If a 'Time Out' message is displayed then this means that the Faceplate has not obtained data from the LANServer. Other error messages may also be displayed here.

**Visual Sensor Alarm Indicators**

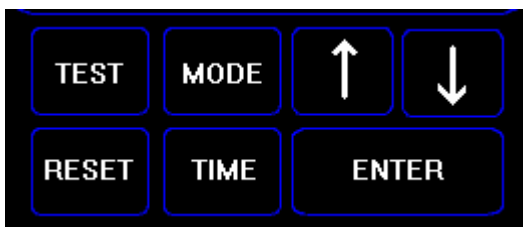
Normal: Solid Green

Warning: Solid Red

Alarm: Flashing Red/White

Key Pad Zone

The response time to the Key Pad is very slow and it is recommended if possible to perform any activity requiring the Key Pad at the Sentry Controller and not via the LANServer. It is recommended that the user wait for up to 30 seconds before trying another key. Pushing keys here is just the same as pushing keys on the front pad of the actual Sentry. Refer to the Sentry Instruction Manual for information on the Key Pad actions.

**Status LED's**

The LANServer Sentry Faceplate includes the LEDs indicating Power On, Trouble, and whether the system is in Calibrate/Change mode as on the controller. Refer to Sentry Instruction Manual for details on these LEDs.



5.11.1. Troubleshooting the Sentry FacePlate Screen

5.11.1.1. Communication Problems

The Sentry Faceplate can report a 'Timeout' for any one of the following reasons.

- Sentry configured with an IP address that does not match the LANServer.
- LANServer is not running.
- It cannot obtain the data it requires from the LANServer. Each LANServer is expected to have 5 Data Arrays for each Sentry that it is connected to (DA_V_SENxxx, DA_U_SENxxx, DA_T_SENxxx, DA_R_SENxxx, DA_FP_SENxxx). If these data arrays do not exist then the faceplate will not be able to read data correctly.
- It is reading data from the LANServer but the data is all zeros. This happens when the LANServer cannot read data from the Sentry's.
- It is reading data but network congestion is making the data reading intermittent and the responses take too long to reach the faceplate.
- The Ethernet port used to communicate with the LANServer is blocked by the router.
- The faceplate uses a protocol called SMT to communicate with the LANServer. If the PC is connected to the LANServer's N2 adapter then the protocol has to be enabled. This concern doesn't apply to N1 because it is enabled by default.

5.11.1.2. One User at a Time

Only one browsing PC may use the Sentry Faceplate keys at a time. As soon as someone pushes a key using one PC, the LANServer starts a timer. Key pushes from other browsing PC's are ignored until the timer has expired. Currently the setting is 60 seconds.

The control reports this message: "Someone else is actively controlling the Sentry. The user can continue to monitor the device but attempts to control the device will be ignored. Try again later. This message is only printed once."

5.11.1.3. LANServer Driver Ver. 1.05f Required

Different versions of the Sentry Faceplate require different versions of the LANServer. To ensure compatibility the Sentry faceplate checks the LANServer version number (The user can do this by using RUINET, going to the error screen, pushing the V key and looking for the version number of the HTTP driver.). If the versions are incompatible this is reported in the Lower Display area of the faceplate.

5.11.1.4. ActiveX Not Installed

The ActiveX Control must be installed on the browsing PC before it can be viewed or used. If it hasn't been installed it will appear as an empty frame with a red 'X' in the top left corner, as illustrated below.



Installation is a formal process. The following lists are possibilities;

- **Auto Install Failed:** Normally the Web Project is designed so that the control will install itself the first time that it is viewed. It is possible that process failed. Perform the following actions to retry.
 - (For I.E. 6.0) **Menu|Tools|Internet Options|General Tab|Temporary Internet Files**, Delete Files, Check Delete all files, OK. Now refresh the page using the Ctrl-F5 Key.
- **Auto Install Not Performed:** Some Web Projects are designed so that a special web page must be visited to perform the install. Browse the project looking for instructions on how to do this.
- **Manual Install not performed:** Some projects are designed, so that the ActiveX Controls must be installed manually. Typically an application (exe) file is supplied to authorized users.

5.12. Backing Up the Sentry Calibration Data

5.12.1. Calibration Backup Control

This control does **not** operate on Windows CE systems.

5.12.1.1. Description

The ActiveX Control is designed to backup and restore the calibration data from a Sentry. The utility is normally used when a firmware EEPROM in the Sentry is updated. Prior to the update, the user backs up the calibration information. The user then replaces the EEPROM, does a 'Clear All' using the menu system on the Sentry front panel and then after resetting the Sentry and waiting for the warm-up to complete, the utility is used to restore the calibration information.

While the utility can be used for the above purpose it has a more generic capability – It is capable of backing up and restoring the holding register memory (40000's) of any Modbus RTU capable device connected to a LANServer.

Using the control is simple. Click a button. EXERCISE EXTREME CAUTION before pushing the download button. Sending calibration data to the Sentry may change the way Sentry operates. It is important to download the correct data to the correct Sentry.

If there are any errors they are reported on a dialog box.

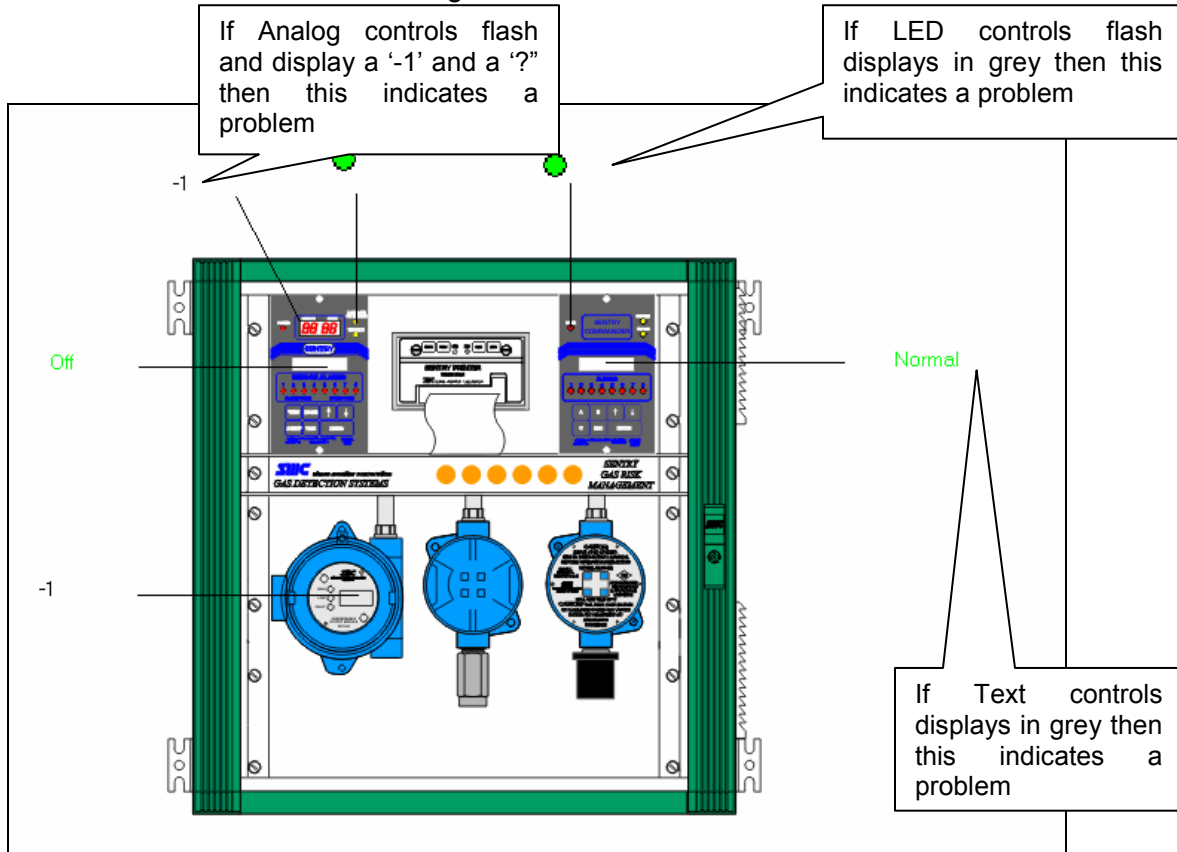
5.12.1.2. How the Control Operates

- The control logs its activity to the following file: C:\Program Files\FST_SentryBK\index.txt. This file can be opened with Notepad or Word.
- The Control uses the log file to determine which registers to backup. It connects to the LANServer and uses it as a conduit to read the register memory of the Sentry. The memory is read in chunks - as each chunk is read, a line is appended to the following file.
- C:\Program Files\FST_SentryBK\backup_n.csv - where n is equal to the node number it has just backed up.
- At the end of the process the file is closed and saved. Previous versions of the file are overwritten. The file is comma separated and can be opened with Excel.

5.13. Interpreting Analog, Text and LED controls

These controls are part of the Advanced Feature Pack and are ordered separately from part 8706-01.

The example page below has an image and on its borders are two analog, two text and two LED controls. This page is not part of the template project provided with the LANServer. It was created to illustrate the Analog, Text and LED Controls.

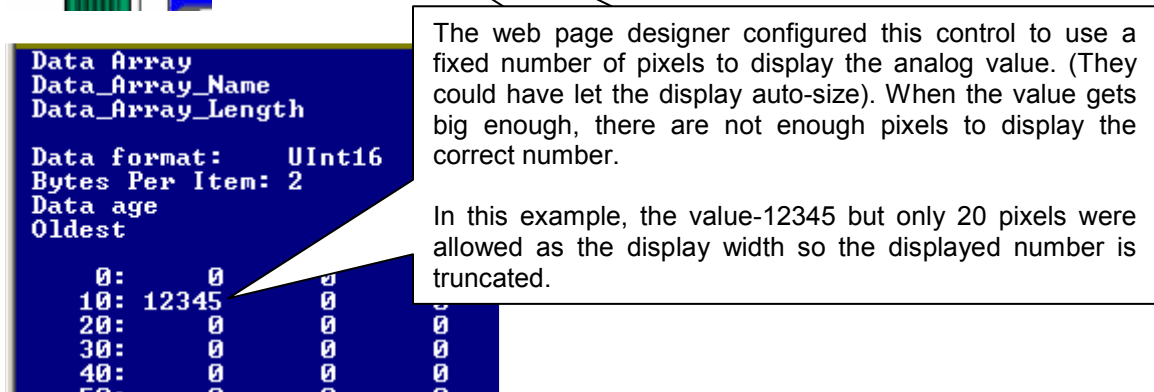
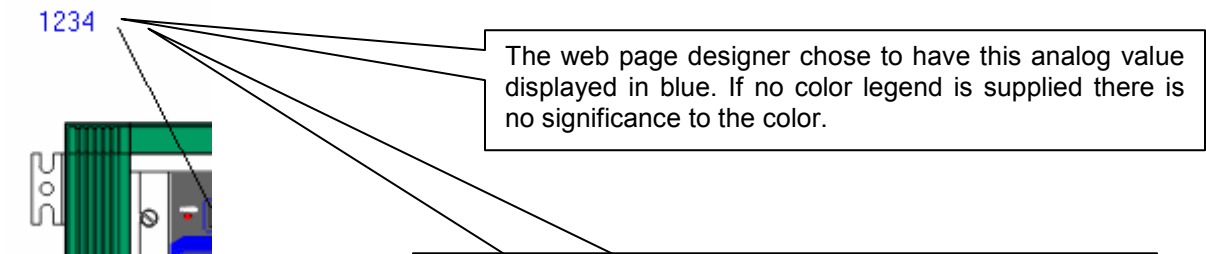
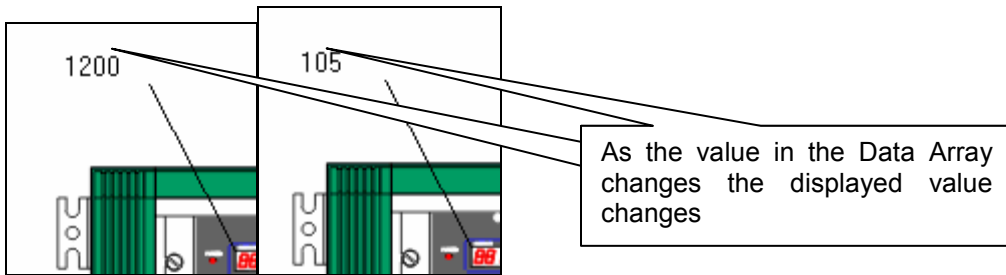


Flashing controls indicate a problem. Flashing means, rapidly toggling from one state to another. In the case of Text controls this means flashing between the 'on' and 'off' text. In the case of LED controls this means flashing between the 'on' and 'off' images and in the case of an Analog control, flashing means toggling between a '-1' and '?'

Each control is configured by specifying the name of a Data Array and an offset into that Data Array. If the Data Array does not exist or if the offset is invalid then the controls will 'flash'

If the Browser is 'offline' from the LANServer then the controls will flash. Offline means, disconnected or that cookies have expired.

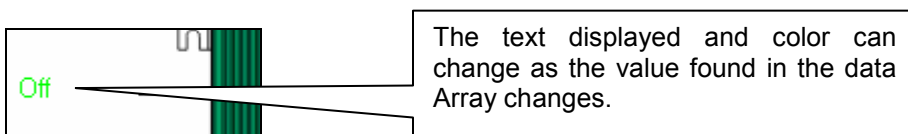
5.13.1. Analog Controls



5.13.2. Text Controls

These controls are configured with the name of a Data Array in the LANServer and an offset into that array. If the value found at that location is zero then one text string, the so called 'off' text is displayed. If the value is non-zero then the so called 'on' text is displayed. The web project designer can also specify the following properties

- Size: Limit the width of the control to a specific pixel count or allow the control to use as much space as is required to display the text. If a fixed pixel width has been specified then it's possible that the displayed text will be truncated.
- Colors: A different color for the 'on' and 'off' states can be configured.
- Font family and font size.
- Background color.
- 'On' and 'Off' Text.



5.13.3. LED Controls

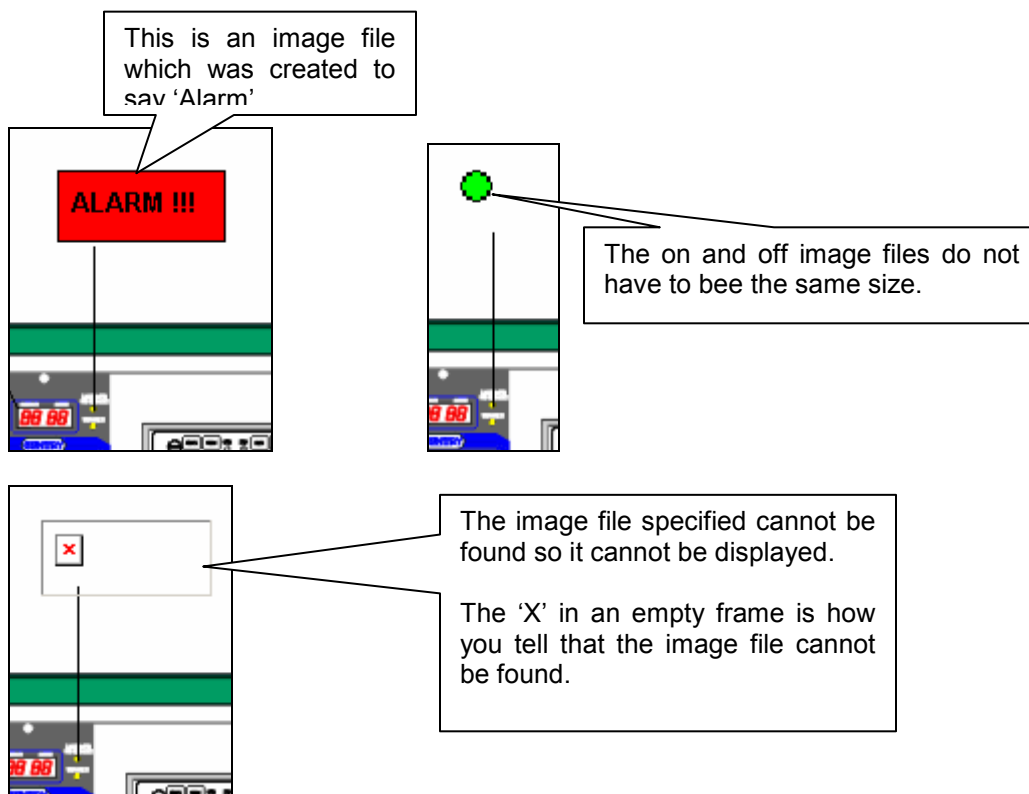
LED controls display an image file based on the value found in a LANServer Data Array.

These controls are configured with the name of a Data Array in the LANServer and an offset into that array. If the value found at that location is zero then the so called 'off' image file is displayed. If the value is non-zero then the so called 'on' image file is displayed.

The web project designer can also specify the following properties

- Size: Limit the width of the control to a specific pixel count or allow the control to use as much space as is required to display the image files.

If the control display's in grey then this means that there is no valid live data for the control and its state should not be trusted.



5.14. Using the LANServer to allow customers to upload files

The LANServer can serve a file in such a way that your browser will open the 'Open/Save As' Dialog to allow a user to save the file on their local computer. All that is necessary to achieve this is:

- Ensure the file is present on the LANServer
- Have a web page with a link to the file.

When the user browses such a page and clicks the link, the LANServer will serve the file, causing the Browser to ask the user if they want to open the file or save it on their local disk.

Note the following restrictions;

- Only certain file types will produce this dialog.
 - Image files (bmp, gif, jpg) are served as images
 - OCX files are served as plain text
 - Other files are served as applications (this is what produces the 'Save As' dialog)
- There are limits on the amount of disk space available to store these files.
- The file name must adhere to the DOS8.3 naming convention which, requires that a file name may not consist of special characters, that there may only be one period in the file name and that there may be no more than 8 characters before and three after the period. Thus these are valid file names abcdefgh.xyz a.zip. These file names are invalid. ab%%.qoqoq long_file_name.zip

Appendix 1. Troubleshooting

Appendix 1.1. Objects Report 'Offline'

Click Refresh or change to another page and return to the screen and see if the problem persists. If it does then check the state of the LANServer by checking the error screen and the overview screen using Ruinet. Check the network connection.

Appendix 1.2. Objects report 'Not Found'

If this problem persists after a refresh then report to Technical Support as it may indicate that the version LANServer software and the version of the software used to prepare the project for downloading are not compatible.

Appendix 1.3. Page login.htm not found

If access control is enabled and a user has not been logged in then the LANServer will change the web page to a page called 'login.htm'. In the event that access control is activated without the system-builder having built a page called 'login.htm' then the browser will display a HTTP 404 error.

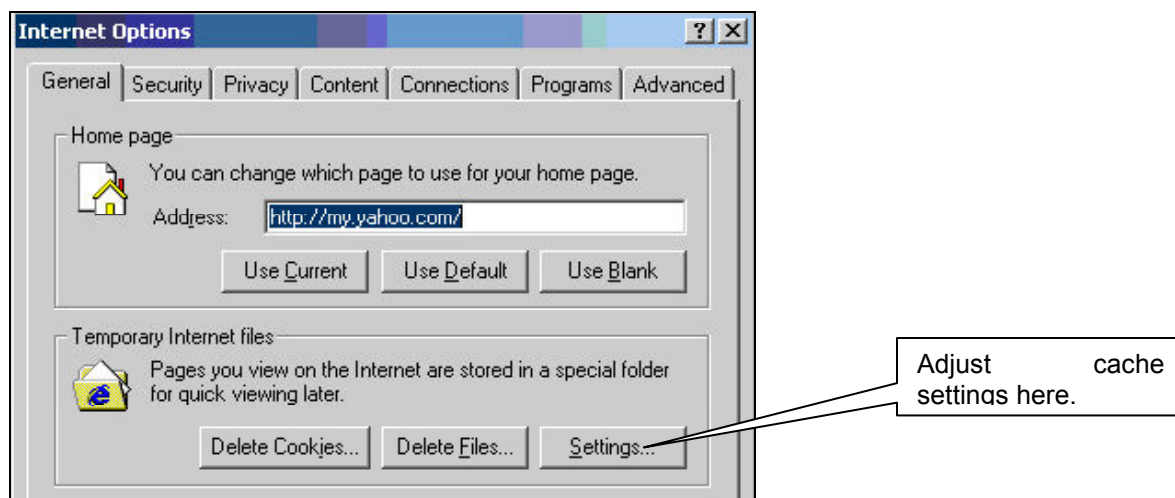
Appendix 1.4. User ids and passwords are not available for validation. Try again.

The access control system uses cookies to transfer data between the browser and the LANServer. If one of the cookies hasn't been delivered to the browser yet, this message is displayed. Use the Back button on the browser to go back to one of the project screens and try again.

Appendix 1.5. Alarm Page doesn't auto refresh when there is a new alarm.

This problem can be corrected by adjusting the browser settings. The browser's cache system is telling the browser used use the cached copy of a page instead of reading a refreshed copy from the LANServer.

In the browser 'Tools' menu, select the 'Internet Options'

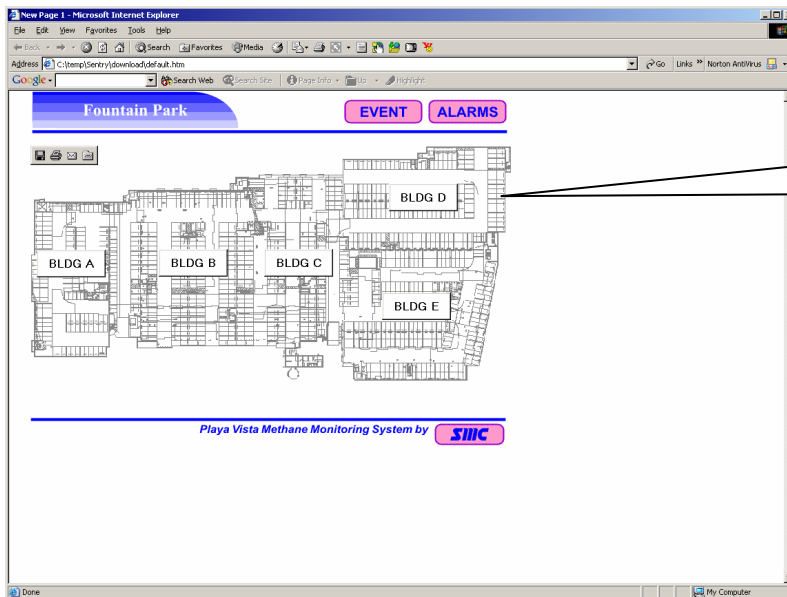




Make sure this option is selected.

Appendix 1.6. Buttons Display in White

The Windows CE 3.0 operating system does not automatically adjust daylight savings time correctly; therefore 'Daylight Savings Time' should be disabled on Windows CE computers. Failure to do this could result in cookie expiry when a transition occurs. This will result in the screens indicating that the display objects are offline (white).



White buttons indicate (amongst other things) expired cookies.

Ensure Daylight Savings Time is disabled. Set the time and date correctly. Now refresh the page and wait a few seconds. If the buttons remain white then repeat this refresh a few times.

Appendix 1.7. Cookie Length

The following statements are true irrespective of the operating system of the browsing computer.

For many of the Sentry Controls, the HTML screens get data from the LANServer in the form of cookies. The maximum cookie length is 3500 bytes. If the cookie length exceeds this limit then the screens will not update correctly.

The driver prints a message in the error log if the cookie length nears this limit.

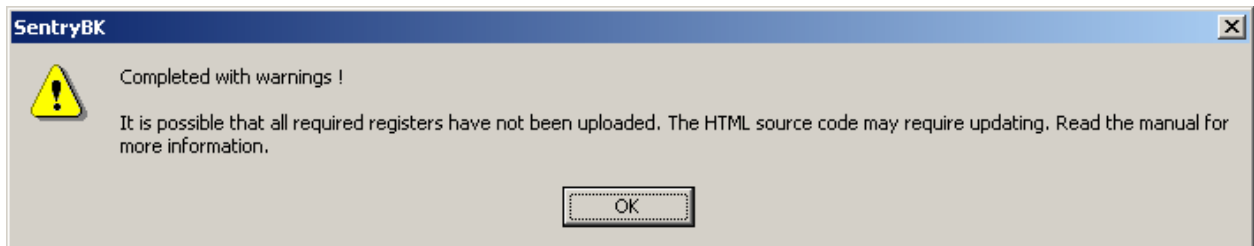
WEB: #60 Err. Web Pages won't update properly. Cookie Length Max/Rqd=%d/%d

There is no corrective action to be taken other than to reduce the number of controls on the various screens that form the project, reprocess the whole project and download the modified files to the LANServer.

As a guideline it is suggested that the user budget 20-25 bytes per Sentry-Sensor. The actual number used per Sentry-Sensor is dependent on the length of the tag name and the length of the units field.

Appendix 1.8. Sentry Calibration Backup (SentryBK) produces a warning message on completion.

If the following warning dialog is produced on completion of the backup then the user needs to read and act on the following notes.



This warning is produced if the register 40977 is not backed-up. This register is one of the new registers backed-up in rev 1.03a of the control.

Depending on the configuration, this may be what is desired. However, if backing up the registers prior to a firmware change in the Sentry then take the following actions before changing the firmware.

1. Edit C:\Program Files\FST_SentryBK\index.txt and add the following lines to the file. If the file doesn't exist, then ignore this step.

```
40159, 8,
40977, 8,
40985, 8,
```

2. Browse to the web screen which contains the SentryBK control.
3. In the Internet Explorer menu, select VIEW, Source. Notepad will start and the html source code will be displayed.
4. Save the file to the computer
5. Find the list of registers which get backed up.
6. Add the new registers. Save the file.
7. Transfer the saved file back to the LANServer. (RuiNet -i192.168.1.81 -u1 -lfilename.htm) or back to the standard web-server that served the file.

Appendix 1.9. LANServer Configuration LED

When the error message "WEB:#26 Err. Cant open required file 'nodes.htm'". is printed, the configuration LED is turned on. This is done once each time the LANServer is reset.

Appendix 2. LANServer Error Messages

Error Message	User Action / Notes
WEB:#01 Err. Reset was ignored. Don't know which sentries require reset	
WEB:#02 Err. No Sentry data available.	One of the causes of this error is a non existent, non functioning or non initialized serial port on the device. (This error will also cause "WEB:#59 FYI. Sentry Functions inactive" The reason that this error occurs is that the field server can not create the ports for the map descriptors. Existent, non
WEB:#03 FYI. Reset was pushed.	
WEB:#05 Err. Error Opening file [%s] %sThe url=%s The reason is: %s %s\r\n	This message is not printed if the missing file is favicon.ico
WEB:#06 Err. No Bytes Read [%s]	
WEB:#07a Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07b Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07c Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07d Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07e Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07f Err. Cant tcp_send.	
WEB:#07g Err. Cant tcp_send. File=[%s] Sent %d of %d bytes. TCPErr=%d	
WEB:#07h Err. Cant tcp_send. File=[%s] TCPErr=%d	
WEB:#07i Err.tcp_send. ndx=%d TCPErr=%d Rtry=%d Done=%d Remain=%d	
WEB:#08 FYI. Opened [%s]	
WEB:#09 FYI. Refresh of live data disabled.(todo)	
WEB:#10 FYI. Sent %d bytes. [%s]	
WEB:#11 FYI. Read %d bytes. [%s] f0err=%d feof=%d %x %x	
WEB:#12 Err. Not enough space for alarm page.	

Error Message	User Action / Notes
WEB:#13 Err. Not enough space for alarm page.	
WEB:#15 FYI. Taglist.ini is absent. This is a non-sentry config.	
WEB:#16 Err. No Sentry Objects	
WEB:#17 Err. No Sentry Objects	
WEB:#18 Err. Open file handle, closed socket.	
WEB:#19 Err. Reading event record file.	
WEB:#20 Err. Bad file pos.	
WEB:#21 Err. Opening event record file.	
WEB:#24 Err. Too many Sentry nodes for Port. Max=%d <%s>	Max number of nodes per port 25 from version 1.08nf, 20 for previous versions.
WEB:#25 Err. Too many Sentry Ports. Max=%d <%s>	Max number of nodes per port 25 from version 1.08nf, 20 for previous versions.
WEB:#26 Err. Cant open required file 'nodes.htm	The file nodes.htm is essential to the operation of the LANServer when it is used for Sentry applications. It should have been prepared and downloaded by the tows.exe application. Use that application again to download your project to the LANServer. When this error is printed, the configuration LED is turned on. This is done once each time the LANServer is reset.
WEB:#27 Err. Sentry Port badly formatted. <%s>	
WEB:#28 Err. Sentry Port must be P or R. <%s>	
WEB:#29 Err. Sentry Port has no nodes.	
WEB:#30 FYI. No Sentry Ports defined.	
WEB:#31 Err. Cant open %s for update.	
WEB:#32 Err. Event write failed.	
WEB:#32 Err. Event index write failed.	
WEB:#42 FYI. Event storage disabled.	
WEB:#42 FYI. Event storage disabled.	
WEB:#45-4 Err. Open file found. File [Quest.htm] idx=0	This 'error' is printed when the driver closes a reply state-engine and finds an open file. A common reason for seeing this 'error' is that a user pushed 'Stop' / Refresh or clicked a link before a file and been fully served. It is not an error and may be safely ignored.
WEB:#45-%d Err. Open file found. File [%s] idx=%d	
WEB:#47 Err. Security.htm invalid (no users). Read Manual	

Error Message	User Action / Notes
WEB:#47 FYI. Security.htm invalid (no time). Set to 2 mins.	
WEB:#49 Err. Tag Rejected. Sentry=%d Channel=%d invalid	
WEB:#50 Err. Array Name is greater than %d characters. Rejected.	
WEB:#51 Err. Object limit reached. (max=%d)	
WEB:#52 Err. Data Array=<%s> not found.	
WEB:#53 Err. Security.htm invalid (no file). Read Manual	
WEB:#54 Err. Security.htm invalid (Multiple definition of users). Read Manual	
WEB:#55 Err. Security.htm invalid (Users formatted incorrectly). Read Manual	
WEB:#56 Err. Security.htm invalid (no time). Read Manual	
WEB:#57 Err. Security.htm invalid (Multiple definition of time). Read Manual	
WEB:#58 FYI. Access control not enabled.	
WEB:#59 FYI. Sentry Functions Inactive.	
WEB:#60 Err. Web Pages won't update properly. Cookie Length Max/Rqd=%d/%d	
WEB:#61 FYI. Compact Cookies. Use htmlToWinCE.exe 1.06a or later.	This (and similar) message(s) are used to help user's synch the toWS (formally htmlToWinCE) tool with the driver version. toWS.exe adds javascript to each htm file to read and interpret cookies - the driver produces the cookie. The cookie contents have been optimized a few times.
WEB:#62 FYI. Original Cookies. Use htmlToWinCE.exe 1.05d or earlier.	
WEB:#63a FYI. ASO Operation. Sentry Faceplate not supported.	
WEB:#63b FYI. ASO Operation. Sentry not supported.	
WEB:#64 FYI. Set the Bridge Time. Use Ruinet - Bridge Screen	

Error Message	User Action / Notes
WEB:#65 Err. Html Page limit reached. %sThe url=%s The reason is: %s %s\r\n	
WEB:#66 Err. Html Page tag limit reached. Max=%d	
WEB:#67 FYI. Max Html Tags per page = %d (%d)	
Web:#68 FYI. Max page limited to %d	
Web:#68 FYI. Full Mode Server. No page limits.	
Web:#69. FYI. IP Address Substitution Active.	
WEB:#70 FYI. LiveData.htm refresh=%d (Default).	Reports the live data refresh time in use. Also reports if the default or an override value is being used. The Sentry LANServer Developers manual has additional information.
WEB:#71 FYI. Base Cookie Expiry Time=%d (Default).	Reports the Cookie Expiry Time in use. Also reports if the default or an override value is being used. The Sentry LANServer Developers Manual has additional information.
WEB:#72 FYI. No config.htm. Using Defaults. Read Manual	Reports that the LANServer is using defaults. The file config.htm can be used to override defaults for Parameters like cookie expiry time, live data refresh rate.
WEB:#73 Err. Too may Sentry Objects. Limit=%d	The maximum number of Sentry controls permitted in a Web Project is limited to the number printed in the message. (Typically 200). Extra controls must be removed for you project to execute correctly. The LANServer will not process the remaining controls. Opening taglist.ini provides a list of all the controls found in all the web pages that form the project. To correct the problem, revisit the project in FrontPage, remove the excess and re-download to the LANServer.
WEB:#74 FYI. IFrame Refresh Method=%d.	
WEB:#75 Err. Event storage disabled. No config file.	
WEB:#76 Err. Cant open %s for validation.	
WEB:#77 FYI. %s has space for %d events	
WEB:#78 Err. No space for event file creation.	
WEB:#89a/b Err. Too much data.	Message 89a is printed if the Sentry Specification is too long to be processed. 89b if the caption is too long. The driver prints these messages as it loads taglist.ini (produced by toWS.exe). Some controls require the configuration to specify Sentries, Sentry:Sensor combinations or a caption. There is a limited amount of space to store these text fields. If there isn't sufficient space this message is printed and the data is truncated. This could mean that the project will not monitor all the sensors or sentries you expect it too. We suggest uploading taglist.ini and finding the line that contains the string printed with the message.

Error Message	User Action / Notes
WEB:#93 FYI. favicon.ico not present	<p>The file favicon.ico is requested and then displayed by some browsers. For example, Firefox displays the icon just to the left of the page URL. The browser doesn't mind if the field is absent - in these cases it uses a default icon.</p> <p>You can make a 10x10 (or even 16x16) icon and store it on the WebServer as favicon.ico. The WebServer will serve the file each time it is requested.</p> <p>If the file is absent then this SDO is printed once and then suppressed. The message may be safely ignored.</p> <p>To add the file to your project for download by toWS.exe simply place the file in the same folder as the config.csv file inside the project folder which is itself a sub folder of C:\Program Files\SMC\Sentry_Projects\Projects</p>
Web:#94b FYI. Memory allocated for Sentry Taglist" Web:#94c FYI. Memory for Sentry Taglist freed"	<p>These messages may be safely ignored. They simply confirm that the driver allocated/freed memory for the sentry list. If you have a GAS application and 94b is not printed then expect other errors too.</p>
WEB:#95 FYI. HTTP Packet Size=%d (non-default). Max=%d	<p>The default value for HTTP TCP packet size is 1450. That is also the max value (unless otherwise indicated). This may be overridden by setting a parameter in the file config.htm which may be part of a WebServer project.</p> <p>Set the parameter by having a line with the following contents.</p> <p>HTTPpacketSize=xxxx where xxxx is some number between 1 and 1450. The smallest value tested was 800.</p>

Appendix 3. WinSock Error Messages

The following is a list of possible error codes returned by the **WSAGetLastError** call, along with their extended explanations. Errors are listed in alphabetical order of error macro. Error codes defined in WINSOCK2.H not returned from any function have not been listed here.

Macro	Code	Message	Description
WSAEACCES	10013	Permission denied.	An attempt was made to access a socket in a way forbidden by its access permissions. An example is using a broadcast address for sendto without broadcast permission being set using setsockopt (SO_BROADCAST) .
WSAEADDRINUSE	10048	Address already in use	Only one usage of each socket address (protocol/IP address/port) is normally permitted. This error occurs if an application attempts to bind a socket to an IP address/port that has already been used for an existing socket, or a socket that wasn't closed properly, or one that is still in the process of closing. For server applications that need to bind multiple sockets to the same port number, consider using setsockopt (SO_REUSEADDR) . Client applications usually need not call bind at all - connect will choose an unused port automatically. When bind is called with a wild-card address (involving ADDR_ANY), a WSAEADDRINUSE error could be delayed until the specific address is "committed." This could happen with a call to other functions later, including connect , listen , WSAConnect or WSAJoinLeaf .
WSAEADDRNOTAVAIL	10049	Cannot assign requested address	The requested address is not valid in its context. Normally results from an attempt to bind to an address that is not valid for the local machine. This can also result from connect , sendto , WSAConnect , WSAJoinLeaf , or WSASendTo when the remote address or port is not valid for a remote machine (e.g. address or port 0).

Macro	Code	Message	Description
WSAEAFNOSUPPORT	10047	Address family not supported by protocol family	An address incompatible with the requested protocol was used. All sockets are created with an associated "address family" (i.e. AF_INET for Internet Protocols) and a generic protocol type (i.e. SOCK_STREAM). This error will be returned if an incorrect protocol is explicitly requested in the socket call, or if an address of the wrong family is used for a socket, e.g. in sendto .
WSAEALREADY	10037	Operation already in progress	An operation was attempted on a non-blocking socket that already had an operation in progress - i.e. calling connect a second time on a non-blocking socket that is already connecting, or canceling an asynchronous request (WSAAsyncGetXbyY) that has already been canceled or completed
WSAECONNABORTED	10053	Software caused connection abort	An established connection was aborted by the software in the host machine, possibly due to a data transmission timeout or protocol error.
WSAECONNREFUSED	10061	Connection refused	No connection could be made because the target machine actively refused it. This usually results from trying to connect to a service that is inactive on the foreign host - i.e. one with no server application running.
WSAECONNRESET	10054	Connection reset by peer	An existing connection was forcibly closed by the remote host. This normally results if the peer application on the remote host is suddenly stopped, the host is rebooted, or the remote host used a "hard close" (see setsockopt for more information on the SO_LINGER option on the remote socket.) This error may also result if a connection was broken due to "keep-alive" activity detecting a failure while one or more operations are in progress. Operations that were in progress fail with WSAENETRESET . Subsequent operations fail with WSAECONNRESET .

Macro	Code	Message	Description
WSAEDESTADDRREQ	10039	Destination address required	A required address was omitted from an operation on a socket. For example, this error will be returned if sendto is called with the remote address of ADDR_ANY.
WSAEFAULT	10014	Bad address	The system detected an invalid pointer address in attempting to use a pointer argument of a call. This error occurs if an application passes an invalid pointer value, or if the length of the buffer is too small. For instance, if the length of an argument which is a struct <code>sockaddr</code> is smaller than <code>sizeof(struct sockaddr)</code> .
WSAEHOSTDOWN	10064	Host is down	A socket operation failed because the destination host was down. A socket operation encountered a dead host. Networking activity on the local host has not been initiated. These conditions are more likely to be indicated by the error WSAETIMEDOUT.
WSAEHOSTUNREACH	10065	No route to host	A socket operation was attempted to an unreachable host. See WSAENETUNREACH
WSAEINPROGRESS	10036	Operation now in progress	A blocking operation is currently executing. Windows Sockets only allows a single blocking operation to be outstanding per task (or thread), and if any other function call is made (whether or not it references that or any other socket) the function fails with the WSAEINPROGRESS error.
WSAEINTR	10004	Interrupted function call	A blocking operation was interrupted by a call to WSACancelBlockingCall .
WSAEINVAL	10022	Invalid argument	Some invalid argument was supplied (for example, specifying an invalid level to the setsockopt function). In some instances, it also refers to the current state of the socket - for instance, calling accept on a socket that is not listening .

Macro	Code	Message	Description
WSAEISCONN	10056	Socket already connected is	A connect request was made on an already connected socket. Some implementations also return this error if sendto is called on a connected SOCK_DGRAM socket (For SOCK_STREAM sockets, the to parameter in sendto is ignored), although other implementations treat this as a legal occurrence.
WSAEMFILE	10024	Too many open files	Too many open sockets. Each implementation may have a maximum number of socket handles available, either globally, per process or per thread.
WSAEMSGSIZE	10040	Message too long	A message sent on a datagram socket was larger than the internal message buffer or some other network limit, or the buffer used to receive a datagram into was smaller than the datagram itself.
WSAENETDOWN	10050	Network down is	A socket operation encountered a dead network. This could indicate a serious failure of the network system (i.e. the protocol stack that the WinSock DLL runs over), the network interface, or the local network itself.
WSAENETRESET	10052	Network dropped connection on reset	The connection has been broken due to "keep-alive" activity detecting a failure while the operation was in progress. It can also be returned by setsockopt if an attempt is made to set SO_KEEPALIVE on a connection that has already failed.
WSAENETUNREACH	10051	Network unreachable is	A socket operation was attempted to an unreachable network. This usually means the local software knows no route to reach the remote host.
WSAENOBUFS	10055	No buffer space available	An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.
WSAENOPROTOOPT	10042	Bad protocol option	An unknown, invalid or unsupported option or level was specified in a getsockopt or setsockopt call.

Macro	Code	Message	Description
WSAENOTCONN	10057	Socket is not connected	A request to send or receive data was disallowed because the socket is not connected and (when sending on a datagram socket using sendto) no address was supplied. Any other type of operation might also return this error - for example, setsockopt setting SO_KEEPALIVE if the connection has been reset.
WSAENOTSOCK	10038	Socket operation on non-socket	An operation was attempted on something that is not a socket. Either the socket handle parameter did not reference a valid socket, or for select , a member of an fd_set was not valid.
WSAEOPNOTSUPP	10045	Operation not supported	The attempted operation is not supported for the type of object referenced. Usually this occurs when a socket descriptor to a socket that cannot support this operation, for example, trying to accept a connection on a datagram socket.
WSAEPFNOSUPPORT	10046	Protocol family not supported	The protocol family has not been configured into the system or no implementation for it exists. Has a slightly different meaning to WSAEAFNOSUPPORT , but is interchangeable in most cases, and all Windows Sockets functions that return one of these specify WSAEAFNOSUPPORT .
WSAEPROCLIM	10067	Too many processes	A Windows Sockets implementation may have a limit on the number of applications that may use it simultaneously. WSAStartup may fail with this error if the limit has been reached.
WSAEPROTONOSUPPORT	10043	Protocol not supported	The requested protocol has not been configured into the system, or no implementation for it exists. For example, a socket call requests a SOCK_DGRAM socket, but specifies a stream protocol.
WSAEPROTOTYPE	10041	Protocol wrong type for socket	A protocol was specified in the socket function call that does not support the semantics of the socket type requested. For example, the ARPA Internet UDP protocol cannot be specified with a socket type of SOCK_STREAM .

Macro	Code	Message	Description
WSAESHUTDOWN	10058	Cannot send after socket shutdown	A request to send or receive data was disallowed because the socket had already been shut down in that direction with a previous shutdown call. By calling shutdown a partial close of a socket is requested, which is a signal that sending or receiving or both has been discontinued.
WSAESOCKTNOSUPPORT	10044	Socket type not supported	The support for the specified socket type does not exist in this address family. For example, the optional type SOCK_RAW might be selected in a socket call, and the implementation does not support SOCK_RAW sockets at all.
WSAETIMEDOUT	10060	Connection timed out	A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.
WSATYPE_NOT_FOUND	10109	Class type not found	The specified class was not found.
WSAEWOULDBLOCK	10035	Resource temporarily unavailable	This error is returned from operations on non-blocking sockets that cannot be completed immediately, for example recv when no data is queued to be read from the socket. It is a non-fatal error, and the operation should be retried later. It is normal for WSAEWOULDBLOCK to be reported as the result from calling connect on a non-blocking SOCK_STREAM socket, since some time must elapse for the connection to be established.
WSAHOST_NOT_FOUND	11001	Host not found	No such host is known. The name is not an official hostname or alias, or it cannot be found in the database(s) being queried. This error may also be returned for protocol and service queries, and means the specified name could not be found in the relevant database.
WSA_INVALID_HANDLE	OS dependent	Specified event object handle is invalid	An application attempts to use an event object, but the specified handle is not valid.

Macro	Code	Message	Description
WSA_INVALID_PARAMETER	OS dependent	One or more parameters are invalid	An application used a Windows Sockets function which directly maps to a Win32 function. The Win32 function is indicating a problem with one or more parameters.
WSAINVALIDPROCTABLE	OS dependent	Invalid procedure table from service provider	A service provider returned a bogus proc table to WS2_32.DLL. (Usually caused by one or more of the function pointers being NULL.)
WSAINVALIDPROVIDER	OS dependent	Invalid service provider version number	A service provider returned a version number other than 2.0.
WSA_IO_INCOMPLETE	OS dependent	Overlapped I/O event object not in signaled state	The application has tried to determine the status of an overlapped operation which is not yet completed. Applications that use WSAGetOverlappedResult (with the fWait flag set to false) in a polling mode to determine when an overlapped operation has completed will get this error code until the operation is complete.
WSA_IO_PENDING	OS dependent	Overlapped operations will complete later	The application has initiated an overlapped operation which cannot be completed immediately. A completion indication will be given at a later time when the operation has been completed.
WSA_NOT_ENOUGH_MEMORY	OS dependent	Insufficient memory available	An application used a Windows Sockets function which directly maps to a Win32 function. The Win32 function is indicating a lack of required memory resources.
WSAHOST_NOT_FOUND	11001	Host not found	No such host is known. The name is not an official hostname or alias, or it cannot be found in the database(s) being queried. This error may also be returned for protocol and service queries, and means the specified name could not be found in the relevant database.
WSA_INVALID_HANDLE	OS dependent	Specified event object handle is invalid	An application attempts to use an event object, but the specified handle is not valid.
WSA_INVALID_PARAMETER	OS dependent	One or more parameters are invalid	An application used a Windows Sockets function which directly maps to a Win32 function. The Win32 function is indicating a problem with one or more parameters.

Macro	Code	Message	Description
WSA_INVALIDPROCEDURETABLE	OS dependent	Invalid procedure table from service provider	A service provider returned a bogus proc table to WS2_32.DLL. (Usually caused by one or more of the function pointers being NULL.)
WSA_INVALIDPROVIDER	OS dependent	Invalid service provider version number	A service provider returned a version number other than 2.0.
WSA_IO_INCOMPLETE	OS dependent	Overlapped I/O event object not in signaled state	The application has tried to determine the status of an overlapped operation which is not yet completed. Applications that use WSAGetOverlappedResult (with the fWait flag set to false) in a polling mode to determine when an overlapped operation has completed will get this error code until the operation is complete.
WSA_IO_PENDING	OS dependent	Overlapped operations will complete later	The application has initiated an overlapped operation which cannot be completed immediately. A completion indication will be given at a later time when the operation has been completed.
WSA_NOT_ENOUGH_MEMORY	OS dependent	Insufficient memory available	An application used a Windows Sockets function which directly maps to a Win32 function. The Win32 function is indicating a lack of required memory resources.
WSA_NOT_INITIALIZED	10093	Successful WSAStartup not yet performed	Either the application hasn't called WSAStartup or WSAStartup failed. The application may be accessing a socket which the current active task does not own (i.e. trying to share a socket between tasks), or WSACleanup has been called too many times.
WSA_NO_DATA	11004	Valid name, no data record of requested type	The requested name is valid and was found in the database, but it does not have the correct associated data being resolved for. The usual example for this is a hostname -> address translation attempt (using gethostbyname or WSAAsyncGetHostByName) which uses the DNS (Domain Name Server), and an MX record is returned but no A record - indicating the host itself exists, but is not directly reachable.

Macro	Code	Message	Description
WSANO_RECOVERY	11003	This is a non-recoverable error	This indicates some sort of non-recoverable error occurred during a database lookup. This may be because the database files (e.g. BSD-compatible HOSTS, SERVICES or PROTOCOLS files) could not be found, or a DNS request was returned by the server with a severe error.
WSAPROVIDERFAILEDINIT	OS dependent	Unable to initialize a service provider	Either a service provider's DLL could not be loaded (LoadLibrary failed) or the provider's WSPStartup/NSPStartup function failed.
WSASYSCALLFAILURE	OS dependent	System call failure	Returned when a system call that should never fail does. For example, if a call to WaitForMultipleObjects fails or one of the registry functions fails trying to manipulate the protocol/namespace catalogs.
WSASYSNOTREADY	10091	Network subsystem is unavailable	This error is returned by WSAStartup if the Windows Sockets implementation cannot function at this time because the underlying system it uses to provide network services is currently unavailable. Users should check that the appropriate Windows Sockets DLL file is in the current path; that they are not trying to use more than one Windows Sockets implementation simultaneously. If there is more than one WINSOCK DLL on the system, be sure the first one in the path is appropriate for the network subsystem currently loaded. Consult the Windows Sockets implementation documentation to be sure all necessary components are currently installed and configured correctly.
WSATRY_AGAIN	11002	Non-authoritative host not found	This is usually a temporary error during hostname resolution and means that the local server did not receive a response from an authoritative server. A retry at some time later may be successful.

Macro	Code	Message	Description
WSAVERNOTSUPPORTED	10092	WINSOCK.DLL version out of range	The current Windows Sockets implementation does not support the Windows Sockets specification version requested by the application. Check that no old Windows Sockets DLL files are being accessed.
WSAEDISCON	10094	Graceful shutdown in progress	Returned by WSARecv and WSARecvFrom to indicate the remote party has initiated a graceful shutdown sequence.
WSA_OPERATION_ABORTED	OS dependent	Overlapped operation aborted	An overlapped operation was canceled due to the closure of the socket, or the execution of the SIO_FLUSH command in WSAIoctl .

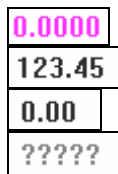
Appendix 4. FieldServer ActiveX Controls

Appendix 4.1. Ana1

The Ana1 ActiveX displays the value of a data array element in a FieldServer. With appropriate permission a user may interact with the control to have the control change the value of the data array element in the FieldServer

- The 'foreground' and 'background' colors are configurable
- The control listens passively for messages sent by a FieldServer.
- The control reports its 'comm.' status by changing to grey and displaying '?????' if no recent data has been received.

Examples

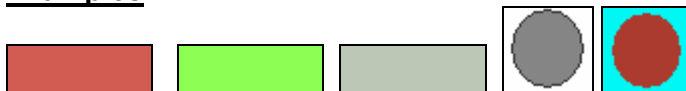


Appendix 4.2. LED1

The LED1 ActiveX control changes color to indicate the value of a data array element in a FieldServer. With appropriate permission a user may interact with the control to have the control change the value of the data array element in the FieldServer

- The 'on' and 'off' color are configurable
- The 'background' color is configurable
- The control listens passively for messages sent by a FieldServer.
- The control reports its 'comm.' status by changing to grey if no recent data has been received.

Examples



Appendix 4.3. Char1

The Char1 ActiveX control displays a chart of up to 2 variables with a max of 300 points. With appropriate permission a user may store the most recent data set to a disk file.

- The axis labels are configurable
- Some formatting is configurable. For example, the user may select a format which treats the X-axis data set as a set of time values.
- The X and Y axes are auto scaled.
- The control listens passively for messages sent by a FieldServer.
- The control reports its 'comm.' status so that viewer's can tell if no recent data has been received.

Appendix 4.4. Limitations and Supported Environments

A full statement of the limitations and supported environment is provided in the manual 'FST Win32 Toolbox – User Manual'. The following notes are a guide only.

Operating System: Microsoft Windows 2000 Professional
ActiveX Container: Microsoft Internet Explorer version 6.0

The controls have been tested to the following limitations

Maximum number of controls running on one PC:	200
Maximum number of any single control running on one PC:	200
Maximum number of Containers running on one PC:	50
Maximum number of PC's running containers connected to a single FieldServer:	4

Supported screen Resolutions: 1152 x 864 and 800 x 600

Appendix 5. General

Appendix 5.1. 9.1 Browser Caching

The WebServer supports browser caching by filling in the Served File's date and Last-Modified date as required.

The WebServer does not use the file date and time to support caching. It uses the FieldServer reboot time. This is considered the file creation / last-modified date for all files.

HTML files are never cached. They are always served with a HTTP-200 response.

Other files may be cached. When the browser fills in the 'If-Modified-Since' header field with a date that is newer than the reboot date then the FS responds with an HTTP-304 response and does not serve the file as it knows the browser has cached the file. To clear the cache reboot the FieldServer or use Ctrl-F5 to force a re-read without caching.

THIS PAGE INTENTIONALLY LEFT BLANK