(Note: This article was exported to PDF from our Support Wiki. We apologize for any imperfect formatting)

Asentria Installation and Operation Manual

SiteBoss 550 and 550A - Installation and Operation Manual

For Firmware Version 2.12.290 STD

►Conventions used in this manual

The following are the conventions that will be used throughout this document:

- Commands are printed in this format: COMMANDS (Arial font, caps, bold, black) although commands used in the unit are not case-sensitive.
- Setting Keys are printed in this format: **`setting.key`** (Courier New font, bold, blue). Key values displayed are in Courier New font, not bold, black.
- Red type indicates a safety or security warning.
- Hyperlinks to other sections in the manual are displayed in Arial font, blue, underline.
- Screen shots of menus are all taken from the command line interface and appear like this:

```
CLI Example:
A) Example Setting      [Example]
B) Example Setting      [Example]
```

- Some settings can only be changed with a Setting Key (no command line menu or web interface options). These are noted throughout Setup Menu section of the manual by Setting Key: **`<name of key>`** > with a description of the key and allowable values.

►For More Information

If the information contained in this user manual is not sufficient to resolve a problem you are having with your unit or to fully explain a feature, there is likely a feature guide covering it in more depth. These feature guides are available on line at the https://www.asentria.com/wiki/Feature Guides. Asentria Technical Support is also available to provide any assistance you might need.

Quick Start

This is a brief guide to help get your SiteBoss 550 (S550) or SiteBoss 550A (S550A) up and running quickly.

►Hardware Needed

- Asentria SiteBoss 550 or SiteBoss 550A
- 15VDC power adaptor (Included if AC power option)
- DC power source (if DC power option)
- Computer with a network port or a serial port and terminal emulation software
- Ethernet cable
- Optional, if connecting serially, RJ45 M-M unshielded serial cable and RJ45/DB9 straight thru adapter (included)

►Information Needed

- IP address(es) to assign to the S550
- Subnet mask
- Default router IP or gateway router IP address if on a WAN (Optional)

►Physically Install SiteBoss

» Note: THIS PRODUCT MUST BE INSTALLED WITHIN A RESTRICTED ACCESS LOCATION WHERE ACCESS IS THROUGH THE USE OF A TOOL, LOCK AND KEY, OR OTHER MEANS OF SECURITY, AND IS CONTROLLED BY THE AUTHORITY RESPONSIBLE FOR THE LOCATION.

Environmental Factors

Ensure conditions A-E will be met by the installation before proceeding.

1. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (TMA), which is 40C for standard units 65C for extended temperature units.
2. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. The SiteBoss needs enough airflow to prevent overheating. Maximum safe temperature is 40C for standard units and 65C for extended temperature units.
3. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing.
5. Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Installation Sequence

1. Physically install the SiteBoss into your site. Use the included Mounting Brackets to secure to a standardly grounded equipment rack.
2. If the unit is not mounted within a grounded rack system, connect the attached ground wire securely to an appropriate earth ground.
3. If a wireless modem is installed, attach the antenna to the SMA connector.
4. Connect your SiteBoss to power and power up the SiteBoss. See the Power Requirements & Options chapter for instructions and safety warnings.
   » Note: Proceed with connecting other equipment only after confirming that the SiteBoss has powered up normally per the Power Up Sequence section of this manual.
5. Connect an Ethernet cable into the RJ45 jack labeled ETH1.
6. If connecting to the SiteBoss using a serial cable, see the Access via a Serial Connection section for connection instructions.
7. If a POTS modem is installed, attach an RJ11 phone wire to the MODEM port.
8. Connect any EventSensors using the RJ45 Sensor port. See the EventSensor Installation Connections chapter for additional instructions.
9. Install any IO connections based on your site requirements.

Power Requirements & Options

The S550 can be configured with one or two options for incoming power.

The standard power option is the 15VDC power jack in the back of the unit. The supplied power jack connects via an AC power adaptor to a standard wall power plug.

There is an optional 24VDC or -48VDC power which is supported on a DC power card installed in the rear panel of the unit. If using a DC power source, the unit is configured with a 4-pin Phoenix style connector for use with a DC power source. The unit is shipped with the instructions for direct connection to a DC power source. The instructions are shown below, in case they are missing from the box:

Standard 15VDC via AC Power

If you are using a standard AC wall plug, the unit uses a barrel connector for connecting to the 15VDC power adapter. The 15VDC power adapter then connects to a standard AC wall plug. Asentria has options for a US, UK, European, Australian or Japanese AC power plug type. This power option ships with the unit unless a DC power option is ordered.

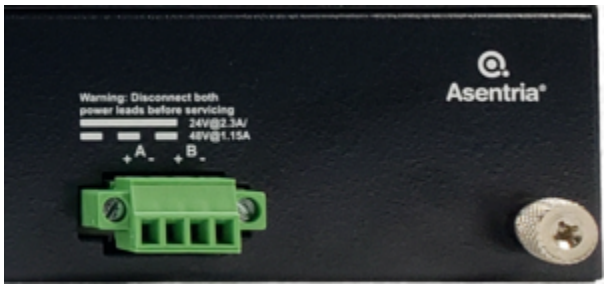
Battery Backup Module

A SiteBoss 550 can be ordered with an optional battery backup module. There are two options that can be used to power a unit after AC power is lost. The Lead acid battery module is indicated with "/BB" in the product number. A lithium battery backup option is indicated with a "/BB2".

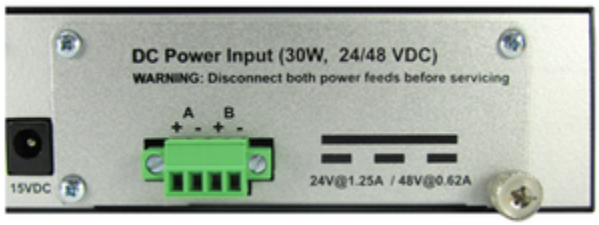
Once a unit with a battery backup module is installed and powered up on AC Power, simply move the slide switch to "Enable" to enable the run time battery backup feature.

An S550A does not have the power bay for a battery back up module. Use a Battery Backup Controller (BC1) if battery back up is need.

DC Power Card Wiring Instructions



S550A /DC Power connections



S550 /DC Power Connections

This section describes the connection to the 30 watt DC power card, which supports either 24VDC or -48VDC power options, and features a Phoenix terminal block with screw clamp connectors.

Wiring connections to DC power can be made using customer supplied wiring, or one of the two optional wiring kits that may be purchased with the unit.

This unit should be assembled and installed by a qualified technician who can ensure the power source is an isolated, SELV (Safety Extra Low Voltage) circuit for -48VDC installations. The 24VDC option does require an isolated circuit.

» Note: The DC input should be protected by an external 2A DC rated slow Blow Fuse suitable for branch circuit protection, at the power supply or within the building circuitry. The input DC power current limiting fuse circuit is provided for by the end user, and is required for unit operation in compliance with safety agency approvals.

The DC power supply option has 4 input connections. This gives the user the ability to connect this unit to a primary and an auxiliary DC power source.

» Caution: DANGER! FIRE HAZARD! DO NOT LEAVE AN UNCONNECTED WIRE EXPOSED! DO NOT CONNECT THE UNIT TO ANY OTHER EQUIPMENT UNTIL YOU KNOW THE UNIT POWERS UP CORRECTLY!

» Attention: DANGER! NE LAISSEZ PAS LES FILS NON CONNECTÉS EXPOSÉS ! NE PAS connecter l'appareil à tout autre équipement avant de savoir que l'appareil soit correctement!

Asentria SiteBoss/TeleBoss products purchased with the DC power option can also be purchased with one of two optional wiring kits, 5006-026 or 5006-025. Optionally, customer supplied cabling can be used. Wiring connection instructions for -48VDC and 24VDC are outlined below.

Connection to DC Power

Run two sets of wire to the SiteBoss power input. For A/B redundant systems one circuit should be feed from the A plant distribution, and one circuit from the B plant distribution. If A/B redundant power feeds are not required ignore all instructions for B side power feeds.

Ensure the rack that the unit is mounted in is properly grounded. Measure the resistance between the rack and building steel, aisle ground, or other properly grounded locations. The resistance should be <1 ohm. If this is not the case, connect the chassis ground point on the lower right hand corner of the A71 power supply to the facilities ground system.

» Ensure that the upstream circuit protection device for both circuits is off or removed before proceeding. Confirm this with a digital multi-meter. It should read 0V between the + and - feed cables in each circuit.

» Veillez à ce que le dispositif de protection des deux circuits amonts soit éteint ou retiré avant de poursuivre. Vérifiez le avec un multimètre numérique: la tension, entre les + et - des câbles d'alimentation de chaque circuit, doit être 0V.

» NOTE: Hot references the polarity with the farthest potential relative to ground. Return references the polarity closest to ground potential.

» NOTE: Peripheral equipment connections may cause a short circuit of your -48V supply if the power connections are reversed! Do not connect peripheral equipment connections until you know the unit is operational by observing the front panel Power LED. The LED does not light if connections are reversed.

For -48VDC power systems

1. Connect the A return feed from the plant, or most positive feed, to the A+ input on the power supply.

2. Connect the A hot feed from the plant, or most negative feed, to the A- input on the power supply.

3. Repeat steps 1-2 for the B side power feeder cables replacing all instances of "A" with "B".

4. Insert or turn on the A side overcurrent protection device to apply power to the A side input. The front power LED should be on to indicate the unit is powered. If no power LED turns on, remove the A feeder fuse and ensure the polarity of the connection is correct.

5. Remove or turn off the A side overcurrent protection device.

6. Insert or turn on the B side overcurrent protection device to apply power to the B side input. The front power LED should be on to indicate the unit is powered correctly. If no power LED turns on, remove or turn off the B side overcurrent protection device and ensure the polarity of the connection is correct.

7. Insert or turn on the A side overcurrent protection device.

8. Secure, dress, and label the power cables in accordance with customer standards.

For +24VDC power systems

1. Connect the A return, or most negative feed, to the A- input on the power supply.

2. Connect the A hot feed, or most positive feed, to the A+ input on the power supply.

3. Repeat steps 1-2 for the B side power feeder cables replacing all instances of "A" with "B".

4. Insert or turn on the A side overcurrent protection device to apply power to the A side input. The front power LED should be on to indicate the unit is powered. If no power LED turns on, remove the A feeder fuse and ensure the polarity of the connection is correct.

5. Remove or turn off the A side overcurrent protection device.

6. Insert or turn on the B side overcurrent protection deceive to apply power to the B side input. The front power LED should be on to indicate the unit is powered correctly. If no power LED turns on, remove or turn off the B side overcurrent protection device and ensure the polarity of the connection is correct.

7. Insert or turn on the A side overcurrent protection device. Both the A and B side inputs should have power applied to them at this point.

8. Secure, dress, and label the power cables in accordance with customer standards.

If there are any questions concerning this Wiring Instruction Sheet, or connecting your Asentria product to DC power, please contact Asentria Tech Support.

Power Up Sequence

On startup, the SiteBoss goes through the following boot sequence in approximately 55 seconds:

1. The power LED flashes once each second for 30 seconds.
2. The LEDs for Expansion Card 1 go through a 15 second flashing sequence.
3. All LED's then go off for approximately 5 seconds.
4. Power, Modem (if installed) and Ethernet LEDs light for 5 seconds, then Modem and Ethernet go off.
5. The S550A will beep twice indicating the unit has completed it's boot sequence.
6. Power LED will blink once every 5 seconds as a "heartbeat" while the SiteBoss is powered on.

Accessing the SiteBoss

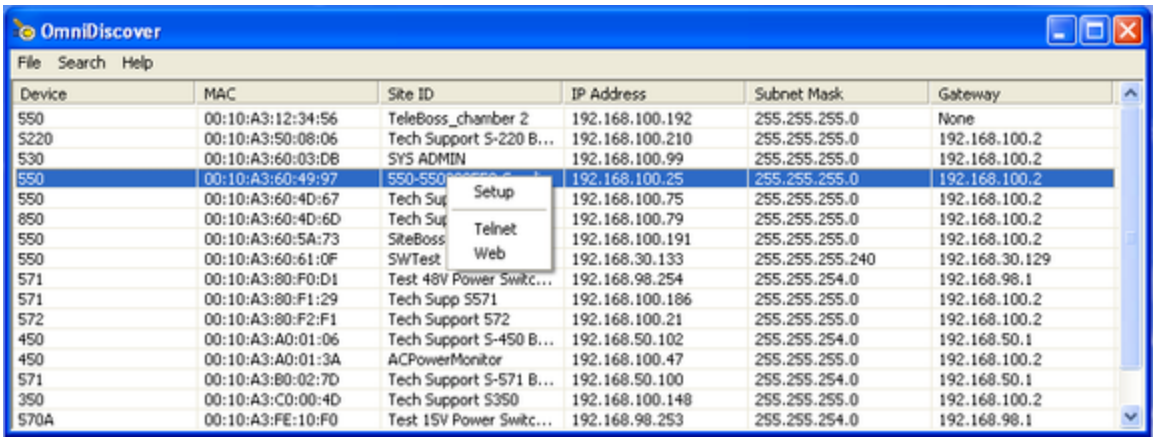
The SiteBoss has two interface options for command and control. There is an intuitive Web Interface that can be accessed via the Ethernet connection at ETH1 or via an optional wireless modem card. The SiteBoss can also be access via a Command Line Interface that can be accessed via Telnet or a serial connection.

►Access via a Network Connection

On the documentation drive that arrives with your SiteBoss there is a program called OmniDiscover. It is located in the Utilities folder on the CD or you can access it via the Asentria website (https://www.asentria.com/wiki/Public:OmniDiscover).

This program will allow you to locate devices with Asentria MAC addresses on your local area network, and allow you to assign the network settings directly over the network.

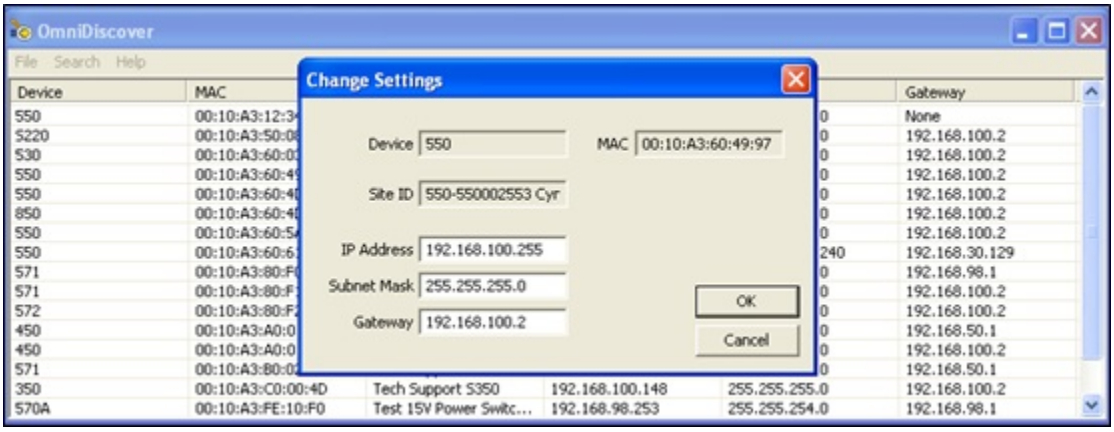
Open the OmniDiscover program. It will immediately display all Asentria devices on the LAN. Right clicking on the line for this unit displays three options: **Setup**, **Telnet** and **Web**.



Setup

Clicking the Setup button opens another window where the IP Address, Subnet Mask, and Gateway (router) can be configured. Press "OK" and these will be assigned to the unit and displayed in the previous window.

» Note: For Security reasons, this setup function is only available for the first 5 minutes the unit is powered on. If your SiteBoss has been powered on longer than that, either power cycle the unit to give yourself another 5 minutes or use the serial connection as covered in the Access via a Serial Connection below.



Web

Once the IP address has been assigned clicking the Web button opens an HTTP (web) connection to the device using your default browser. See the Default Passwords section for log in instructions. The Web Interface can also be reached by typing the configured IP address into an internet browser's address bar.

Telnet

Once the IP address has been configured, clicking the Telnet button will open a connection to the SiteBoss' Command Line Interface using your default Telnet client, if one is configured for your operating system. If your computer does not have a Telnet client configured any terminal emulator such as Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) or TeraTerm (http://ttssh2.sourceforge.jp/index.html.en) can be used.

If a default telnet client has been configured, you can simply navigate from your computer's command window:

- Type "Telnet" at the Windows command prompt.
- Then type "Open <IP Address>". This will take you to the SiteBoss Command Interface.
- Type in the password for the unit and return. See the Default Passwords section for login instructions.
- See the Command Line Interface section for instructions on how to control your SiteBoss using this interface.
- To exit from the SiteBoss Command Line Interface type **bye**.
- To exit from the Windows Telnet client type **quit**.

Contact Asentria Technical Support for any questions or assistance with OmniDiscover. Refer to the Telnet Feature Guide on the Asentria Information Portal for further information regarding a number of different types of Telnet connection options.

►Default Passwords

The SiteBoss uses a very flexible system for managing users, passwords, and access rights. By default, the User1 profile is the only one with a preconfigured username and password. The User Name is **admin** and the Password is **password**. For security reasons it is highly recommended that you change the password, and record all configured passwords in a secure location. The username and passwords are configured in the Security menu under User Profiles.

►Access via a Serial Connection

An alternate way to access your SiteBoss is using a serial port. This will allow an immediate connection to the Command Line Interface of the SiteBoss. The Serial Port labeled I/O2 is configured for command access.

For a serial connection to a Console Port of a PC or laptop running any terminal emulator:

USB Com port

From a USB connection, a USB to RS232 DB9M adapter will be needed. This is Asentria part no. 4161-021 or any commercially available adapter can be used.

a. Connect the USB adapter to a USB port on your computer.
b. Connect the DCE adapter to the RS232 end of the adapter.
c. Use an RJ45 cable to connect the DCE adapter to the SiteBoss I/O2 port.

» **Note**: If both LEDs on the SiteBoss I/O 2 do not light, add the null modem adapter (supplied with the SiteBoss) between the adapters.

DB9 Interface Com Port

a. Connect the RJ-45 serial cable or a straight through Ethernet cable to the DTE adapter (supplied with the SiteBoss).
b. If your computer has a DB9 interface port, the DTE adapter can connect directly to a serial

com port.
c. Connect the other end of the RJ-45 serial or Ethernet cable to the SiteBoss I/O2 serial port.

Connect to that serial port using any terminal emulator such as TeraTerm (http://ttssh2.sourceforge.jp/index.html.en) or Putty (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html). I/O 2 is set to 19200 baud, 8N1 (8 data bits, no parity, 1 stop bit, no flow control) by default.

The command port is not password protected by default. Press <Enter> and the command prompt ">" should display. From the command prompt enter **STATUS** and press <Enter>. You will be presented with a Status screen similar to the following. When the Status screen appears, the unit is successfully connected and ready for use. See the Command Line Interface chapter of the SiteBoss Users Manual for information on how to configure and control functions of the SiteBoss via this interface.

```
>S550>status
SiteBoss 550 2.12.290 STD     Serial #  : 550002553
Site Name : S550-550002553
Date      : FRI 02/09/21       1:  19200,8N1  I/O 1
Time      : 09:56:09           2:  19200,8N1  I/O 2
Modem     : Yes
Eth 1     : STATIC
IP Add    : 0.0.0.0
MAC Add   : 00:10:A3:60:49:97
IPv6      : OFF
Eth 2     : STATIC
IP Add    : 0.0.0.0
MAC Add   : 00:10:A3:60:49:98
IPv6      : OFF
```

►Configuring Ethernet Settings via IO2

For instructions on how to access the command line interface serially via IO2 see the Access via a Serial Connection section.

Once you have successfully connected to the Command Line Interface, configure the Ethernet Settings by taking the following steps:

a. Type **SETUP** and press <Enter> from the SiteBoss command prompt.
b. Type **A** to select Network Settings from the menu.
c. Type **A** at the Network Sub-Menu to select Ethernet Settings.
d. Type **A** from the Ethernet Sub-Menu to select Ethernet 1.

```
SiteBoss 550 - Ethernet 1 Settings
A) IPv4 Mode                          [STATIC]
B) IP Address                         [192.168.0.299]
C) Subnet Mask                        [255.255.255.0]
D) Router Address                     [192.168.0.1]
E) NAT                                [ON]
F) VLAN Settings
```

```
G) IPv6 Settings                        [OFF]
H) DHCP Server Settings
```

e. Set the Mode, as needed, to the desired setting by selecting **A**. The default is STATIC. The other options are DHCP CLIENT, VLAN, or DHCP SERVER
f. To set a static IP address, type **B** and enter an IP Address.
g. Enter a Subnet mask and router address, if needed, using options **C** and **D**.
H. Select **G** to configure IPv6 settings.

```
SiteBoss 550 - Ethernet 1 IPv6 Settings
A) Mode                          [OFF]
B) Static Address                []
C) Static Router Address         []
```

h. Press Enter to go back one level in the menu tree, or <CTRL + C> to exit the Main Setup Menu and return to the command prompt.

» **Note**: The SiteBoss does not heed changes to network configurations while you are connected to a command processor via Telnet. Changes are pended until all network-based command processor sessions have ended. To exit from the SiteBoss Command processer type **BYE** and press <Enter>. Optionally you may type **RESTART** and press <Enter> at the command prompt to restart the unit to ensure all command processors are closed.

►Testing Network Connectivity

Once the network settings are configured connect to the Web Interface by inputting the Ethernet address set for Ethernet 1 into a Chrome, Internet Explorer or Firefox browser. The SiteBoss password page will appear.

If you are connected serially to the Command interface you can verify that the network connectivity is available to the unit by typing the command **PING <IP_address>** at the SiteBoss command prompt. A router is always a good candidate for test pings but any reachable IP address can be used. The following screenshot is an example of a successful ping test.

```
>ping 192.168.100.25
PING 192.168.100.25 (192.168.100.25) 56(84) bytes of data.
64 bytes from 192.168.100.25: icmp_seq=1 ttl=64 time=0.375 ms
64 bytes from 192.168.100.25: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.100.25: icmp_seq=3 ttl=64 time=0.325 ms
64 bytes from 192.168.100.25: icmp_seq=4 ttl=64 time=0.317 ms
64 bytes from 192.168.100.25: icmp_seq=5 ttl=64 time=0.292 ms
64 bytes from 192.168.100.25: icmp_seq=6 ttl=64 time=0.318 ms
64 bytes from 192.168.100.25: icmp_seq=7 ttl=64 time=0.315 ms

--- 192.168.100.25 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 0.292/0.322/0.375/0.031 ms
```

Press <Ctrl+C> keys to stop the ping testing. If <Ctrl+C> is not pressed, the unit will continue pinging attempts until the active command process is closed. Alternately, a ping count can be defined in the command string, PING 192.168.100.88 -c5, to limit the ping requests.

If there is an error message or no response from the router, first check the network settings and connection, then consult your System Administrator or Asentria Technical Support for additional assistance.

Once the SiteBoss is successfully connected to the network the unit can be configured via either interface. The Web Interface can be accessed by inputting the Ethernet address set for Ethernet 1 into a Chrome, Internet Explorer or Firefox browser or you can proceed to configure your unit as needed via the Command Line Interface using the **SETUP** menu and/or settings keys.

What is a SiteBoss 550

►The Basics

The SiteBoss 550 is a versatile system used for monitoring and control of remote equipment sites. The S550 provides remote monitoring of serial devices, equipment I/O, and environmental conditions at these remote sites and forwards notification when conditions fall outside user defined limits. On-board I/O provides serial, Ethernet, and modem connectivity. The S550-2 (11-inch) and S550-6 (17-inch) models provide two or six expansion slots respectively to allow addition of various communications and monitoring interfaces (Expansion Cards).

Communication Methods

The SiteBoss has a diverse selection of communication methods available for different applications. The SiteBoss can provide an administrator transparent access to connected devices. This sort of access can be used to configure, maintain, or manipulate devices that would normally have no remote access.

- The Web interface can be accessed via HTTP or HTTPS.
- Port forwarding options are available to reach equipment on site that might not otherwise be accessible remotely. Port forwarding options can be via the Ethernet or using serial pass-through. Port Forwarding feature that allows the configuration to accept UDP and TCP frames on an interface and route them, translating their IP addresses and UDP/TCP ports according to configuration to a different address, even

on a different network interface than the request was received on.
- Using our new Secure Access Ethernet Card (SAEC) a user can Remote Desktop into any connected equipment or the SiteBoss GUI.
- Modems can be used to access the SiteBoss or connected equipment either as a primary route or as a backup communication route to the site.
- A Small Form-factor Pluggable port (SFP) can be added to an Asentria SiteBoss 550 base unit for connectivity to optical fiber networks.
- The SiteBoss can use SNMP and DNP3 protocols to communicate to a network operations center or to control other equipment. The SiteBoss can proxy SNMP PDUs to another agent. In other words, the unit responds to inbound SNMP PDUs on behalf of another agent. This facilitates a user to utilize the unit as the interchange between remote devices via SNMP.
- With some custom scripts the SiteBoss can communicate via MODBUS RTU to connected equipment. Additionally, the unit can use XML Proxy and display sensor readings from connected equipment.
- For customers with a knowledge of web programming the S550 has a RESTful application program interface (API) that can be used to monitor and control the SiteBoss and connected equipment.
- The command line interface can be accessed via Telnet, SSH, optional POTS modem, or serially. Any action that the SiteBoss can take using the web GUI can be accomplished using the text based command line interface. A user can telnet directly from the SiteBoss CLI to any other equipment on the network.

All methods of connecting to the unit can be secured via password for protection of data and hardware. Radius security server access features are also available.

Data may be retrieved from or through the SiteBoss by any of the following methods:

- Web Interface Status and Logs menus
- Serial or modem connection to command processor
- Serial or telnet pass-through to connected equipment
- Telnet to command processor
- Telnet real-time sockets
- FTP push (automatic delivery to FTP server)
- FTP get (manual retrieval from FTP server)
- SFTP push/get
- SNMP
- DNP3 Outstation via TCP only
- SCP
- REST API

Event Notification

Sensor event alarms generated or detected within the SiteBoss can be delivered through any of the following means:

- SNMP trap or inform
- Email
- DNP3 Outstation protocol
- SMS Messages via an optional wireless modem
- Serial POTS Modem callout

- Asentria Alarms
- Relay or Power Output toggles
- Script actions

Environmental Monitoring

Through the use of external EventSensor modules and/or internal Expansion Cards, a variety of environmental sensor monitoring and alarming capabilities are available in the SiteBoss. Each individual sensor can be configured with independent actions, counters and other unique settings. Sensor events triggered within the SiteBoss can be logged to an Event Log. This file can be viewed via the web interface, FTP, the Command Line Interface **`SETUP`** menu and the **`TYPE EVENTS`** command from the command prompt.

Site Security

The SiteBoss can have Wiegand Expansion card installed that will allow the SiteBoss to control the RFID reader cards and door access relays. Door access contact closure alarms, motion sensors and network cameras be be added to the site for additional security and instant notifications of unauthorized access to the remote locations.

Data Storage

Basic data storage in the SiteBoss is accomplished in a database of at least four files — FILE1, FILE2, EVENTS, and AUDIT. FILE1 and FILE2 are typically associated with Serial Port I/O 1 and Serial Port I/O 2, respectively, although either serial port can store to FILE1, FILE2, or both. EVENTS and AUDIT are log files generated from the Event Log Settings and Audit Log Settings menus per the parameters set there. If the unit has additional serial ports via an expansion card, a FILE location will be available for each port.

The contents of any of the files can be transferred via FTP to a server. The Events and Audit files can be viewed or downloaded via the web interface, the Command Line Interface SETUP menu and the **TYPE EVENTS** or **TYPE AUDIT** command from the command prompt. The contents of a file associated with a serial port can be released to a text editor by typing **SA FILE[number]**. The number of records stored in each of these files can be displayed using the **DIR** command at the command prompt.

The SiteBoss also features three "auxiliary" files for storage of data to be used in scripting functions, named AUX1, AUX2, and AUX3. For further explanation about processing data stored in AUX1, AUX2 and AUX3, refer to the Scripting Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.

Data Events

The SiteBoss has the capability to monitor incoming data for user-defined strings and then report the event via several avenues. Up to 1000 different data events can be configured. Each data event contains independent actions, counters, and other unique settings. Data events triggered within the SiteBoss can be logged to an Event Log. This file can be viewed through the Event Log on the web interface Logs section or via the Command Interface **`SETUP`** menu, FTP, or from the command prompt **`TYPE EVENTS`** command.

►Features and Accessories

Standard Equipment

The base SiteBoss 550 comes with the following standard on-board equipment:

- AC Power Input
- 32MB logging database for text records
- (2) RJ45 DTE serial I/O ports
- (1) RJ45 Sensor port for connection for Asentria EventSensors
- (2) 10/100Mb Ethernet interfaces with support for six 802.1Q VLAN interfaces on each
- (1) MMC memory I/O slot
- (2 or 6) Expansion Card slots
- (1) Reset button
- Internal lithium coin-cell type battery backup*

The S550A is a drop in replacement for an S550, but it has a slightly different hardware configuration

- AC Power Input
- (2) RJ45 DTE serial I/O ports
- (1) RJ45 Sensor port for connection for Asentria EventSensors
- (2) 10/100Mb Ethernet interfaces with support for six 802.1Q VLAN interfaces on each
- (1) Micro SD Slot
- (1) USB port
- (6) Expansion Card slots
- (1) Reset button
- Internal lithium coin-cell type battery backup*

* Battery backup preserves clock operation when power is not present. Data records and settings are stored in non-volatile memory and therefore do not require battery backup.

» CAUTION: THERE IS A RISK OF EXPLOSION IF THE BATTERY IS REPLACED BY AN INCORRECT TYPE. Replace with batteries of the same type or as recommended by the manufacturer. Dispose of used batteries according to the instructions.

» ATTENTION: Il Y A DANGER D?EXPLOSION SI LA BATTERIE ORIGINALE EST REMPLACEE PAR UNE BATTERIE D'UN AUTRE MODELE. N'UTILISER QUE DES BATTERIES DU MEME TYPE OU SUIVRE LES RECOMMANDATIONS DU CONSTRUCTEUR. LES BATTERIES USAGEES DOIVENT ETRE MISES AU REBUT SELON LES INSTRUCTIONS DU CONSTRUCTEUR.

In addition to the above standard on-board equipment, the SiteBoss may be shipped with the following accessories:

- This product manual on the Documentation and Software USB Drive
- External desktop AC power supply with power cord (if AC specified on order)
- (1) 6ft RJ45 Ethernet cable
- (2) 6 ft RJ45 M-M unshielded serial cable serial cables
- (1) RJ45/DB9 Male DTE Adapter
- (1) RJ45/DB9 Female DCE Adapter
- (1) DB9M/DB9F Null Modem Adapter

- Rack mount ears
- Screwdriver and terminal blocks for Expansion Cards with internal contacts

LEDs, Ports, Connectors, and Buttons

Front Panel - LEDs

PWR (Power)
The Power LED is green and has two operational states. During the boot up cycle, it will blink once every second until the boot sequence is complete. During normal operation, it is steady on with a blink every 5 seconds.

MDM (Modem)
The MDM LED lights a solid green whenever the POTS modem is connected and blinks when the modem is dialing out.

ETH (Ethernet)
The Link LED lights solid green whenever an active Telnet or FTP connection is made to the unit.

ALM (Alarm)
The Alarm LED should be lit if any input or output is in the event state.

25% - 75% - 100%
The SiteBoss has three LEDs to indicate file full status. A blinking percentage full LED indicates the database has less than the amount indicated by that LED, but more than the previous. A solid lit LED indicates the database percentage is at or over the value for that LED.

Expansion Card n
Each optional Expansion Card has eight LEDs associated with it that may or may not be used. Each optional Expansion Card has eight LEDs associated with it. A lit LED would indicate that IO point is in the alarm or active state. For high density cards the IO points are grouped in blocks of 8 per LED. If any one of 8 associated IO points go into the alarm state. Power output points (5V or 15V) do not have an alarm state, so LEDs would not light. The LEDs would not be used for a modem, Ethernet or serial expansion card.

Back Panel

Back panel S550-6

Back panel S550A-6

The Siteboss S550 back panel is configured (from right to left) with a bay for the optional run-time battery or DC power card, AC power jack, RJ45 Sensor port, bank of 8 DIP switches, MMC memory I/O card slot, two RJ45 Ethernet ports, two RJ45 RS232 serial ports, Reset button, one RJ11 POTS modem port, and either two or six expansion bays for optional Expansion Cards that expand the functionality of the unit with wireless modem and/or a variety of sensor and I/O options.

The Site Boss S550A back panel is configured (from right to left) with Dual DC power inputs, AC power jack, RJ45 Sensor port, bank of 8 DIP switches, two RJ45 Ethernet ports, two RJ45 RS232 serial ports, Reset button, USB port, and six expansion bays for optional Expansion Cards that expand the functionality of the unit with wireless modem and/or a variety of sensor and I/O options.

LEDs – Back Panel

The Serial I/O ports and the Ethernet ports on the back panel each has two LEDs associated with it — one on the Right of the port, one on the Left.

Ethernet Ports (ETH1 and ETH2) (and any additional Ethernet Port cards that may be installed)

- Right – Lights solid red when an Ethernet cable is connected to the port and an active Ethernet network. The LED is off when the cable is disconnected from the network, or the Ethernet Port.
- Left – Flashes yellow/green when network data (TCP packets) is being transmitted or received across the port. When no data is actually being transmitted/received, this LED is off.

I/O Port 1 & 2 (and any additional 4-I/O Port cards that may be installed)

- Right – Lights solid green when a correctly configured cable from another device is connected to it. Otherwise this LED remains off. As the I/O Port receives or transmits data, this LED will flash red.
- Left – Lights solid green when power is applied to the SiteBoss, regardless of whether a cable is connected to the I/O Port or not.

Ports

Memory I/O

On the original S550, the slot labeled Memory I/O can be used for the optional internal Temperature Sensor, which is a small MMC card. Firmware packages can also be flashed to

the SiteBoss via this port under very specific conditions.

On the S550A, in additional to the original capabilities, an SD memory card can be used for image storage from security cameras and other file data storage.

Sensor
The Sensor port is a RJ45 connector for use with Asentria EventSensors and SensorJack sensors.

Ethn
The Ethernet 10/100Mb interfaces are standard RJ45. Either of these standard connectors will connect the SiteBoss to an Ethernet hub or switch.

I/On (Serial Ports)
Each of the RS232 serial ports is configured as a DTE port using an RJ45 connector. This is the standard recommended pinout for EIA/TIA-561 for 8 pin RJ45 connector:

PIN1	RI	RING INDICATOR, INPUT to the S550
PIN2	DCD	CARRIER DETECT, INPUT to the S550
PIN3	DTR	DATA TERMINAL READY, OUTPUT from the S550
PIN4	SIGNAL GROUND	
PIN5	RXD	RECEIVED DATA, INPUT to the S550
PIN6	TXD	TRANSMITTED DATA, OUTPUT from the S550
PIN7	CTS	CLEAR to SEND, INPUT to the S550
PIN8	RTS	REQUEST to SEND, OUTPUT from the S550

The SiteBoss will come with adapters to connect the DTE serial ports with the DCE ports on a computer. Optional USB adapters are available. See the Access via a Serial Connection section for instructions.

The default settings for the serial ports are 19200-baud, 8-bit word length, no parity, and one stop bit (19200, 8N1). To adjust these settings you can use the Serial option from the Communication menu on the Web Interface or the Serial Settings option from the command interface main **SETUP** menu. If the user is not logged into the unit, the DIP Switches on the back panel can also be used to adjust the serial settings.

Internal Modem

On the S550, if a dialup POTS modem is installed, an RJ-11 (typical U.S. phone) connector is used. A POTS (analog) dialup phone line is inserted into this connector. The modem installed within this unit is FCC certified. For further information, consult the Internal Modem Guidelines appendix or the serial number label. The S550A does not have a POTS modem port.

» CAUTION: To reduce the risk of ?re, use only No. 26 AWG or larger telecommunication line cord.

» ATTENTION: Pour éviter tout risque d'incendie, n'utilisez que des câbles électriques de diamètre supérieur à 0,4 mm (AWG ? 26).

USB Port

On an S550A the POTs modem port has been replaced with a USB port. The USB port can be used to update settings and/or software using the root directory of a FAT32 formatted USB drive.

Expansion Card Bays

The SiteBoss 550 features two or six Expansion Card bays in which optional Expansion Cards can be installed to expand the capabilities of the SiteBoss. See the I/O points and Expansion Cards section of this manual for more information on Expansion Cards.

DIP Switches

The bank of 8 DIP switches on the back panel of the SiteBoss are used to control the baud and parity settings of I/O 2, and to set the operational mode for I/O 2. The following table shows how to set the various DIP switches to obtain certain settings:

I/O 2 Baud	SW1	SW2
2400	DOWN	DOWN
9600	UP	DOWN
19200	DOWN	UP
115200	UP	UP

I/O 2 Word, Parity	SW3
8N1	DOWN
7E1	UP

I/O 2 Mode	SW4
Command Mode	DOWN
Data Mode	UP

» Note: These settings that can be set via DIP switch, Command Interface, or the Web Interface, the SiteBoss always pays attention to the last setting, regardless of how it was done. So if the internal setting for I/O 2 Port Mode is Command, and someone flips SW4 to the UP position, the Mode is immediately set to Data.

Buttons

The only button on the SiteBoss is the reset button located on the back panel to the left of serial port I/O 2.

The Reset button can be used for two different functions:

1. To reboot the SiteBoss, press the Reset button for approximately 1 second and SiteBoss will begin the reboot process as described in the Power Up Sequence section.
2. To activate the Button Unlock feature, which resets the username and password back to the factory defaults. This feature can be disabled, and is intended to be used if you've locked yourself out of the unit.

Optional Hardware

The SiteBoss has a wide variety of optional cards and accessories. Options include DC Power Input, 64MB logging database for text records, an internal POTS modem, as well as two types of Run-time battery options.

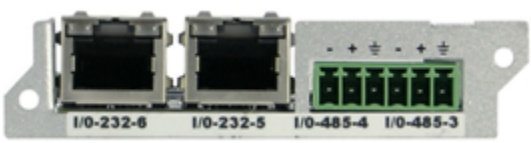
The various optional internal slot cards have appropriate wiring and accessories including with the shipment.

I/O points and Expansion Cards

The expansion cards in the two or six expansion card slots can be configured with multiple options. The terminal block ports will be marked to indicate how the slot card is configured. A single card can have more than one type of I/O option. The Expansion cards that are currently available are:

Expansion Cards - Communications Related	Catalog #
Wireless EDGE Modem (not recommended for US market)	ME
Wireless EvDO Modem -VERIZON with GPS	MCVA
Wireless LTE Modem - for EU with GPS	MLEU
Dial-Up Modem	MD
4X RS232 Serial Port	4S
2X RS485 2X RS232 Port	2DS2S
2X RS485, 5v Pwr, Voltage, F - Fuel Resistive, 2X Form C Relays	2DS5P1V1F2RC
4X EventSensor Expansion Card	4ES
4X 10/100 Ethernet Port (up to 2 per unit)	4E
8X 10/100 Ethernet Port (up to 2 per unit, each card occupies 2 vertical slots requires a 6 Expansion slot SiteBoss)	8E
Secure Access Ethernet Card, 4E Co-processor	SAEC
GPS Receiver	GPS
SFP Card - Small Form-factor Pluggable transceiver	1SFP

Serial, EventSensor and Ethernet ports will be labeled for ease of identification.



Expansion Cards - IO and Sensor Related	Catalog #
8C Card - (8) Contact Closure Inputs	8C
8CI Card - (8) Isolated Contact Closure Inputs	8CI
4VP Card - (4) Analog Voltage Inputs plus (4) +/-15 VDC Pwr Outputs	4VP
4VP5 Card - (4) Analog Voltage Inputs plus (4) + 5 VDC Pwr Outputs	4VP5
8V Card - (8) Analog Voltage Inputs	8V
8VI Card - (8) Isolated Voltage Inputs	8VI
8R Card - (8) Low Current Relays	8R
8M Card - (8) 4-20mA Analog Current Inputs	8M
8SR Card (8) Solid State Relays	8SR
4C4SR Card - (4) Contact Inputs and (4) Solid State Relays	4C4SR
4C4V Card - (4) Contact and (4) Voltage Inputs	4C4V
4VI4C Card - (4) Contact and (4) Isolated Voltage Inputs	4VI4C
4C4R Card - (4) Contact and (4) Low-Current Relay	4C4R
2C4RC Card - (2) Contact and (4) Low-Current Form C Relays (NO, NC)	2C4RC
4C1W1R Card - (4) Contact, (1) Wiegand int. w/ 15V power, (1) Low-Current Relay	4C1W1R
2W2R Card - (2) Wiegand int. 15V with power, (2) Low-Current Relay	2W2R
4V4M Card - (4) Voltage and (4) 4-20mA Sensor	4V4M
4C4M Card - (4) Contact and (4) 4-20mA Sensor	4C4M
4MI4C Card - (4) Contact and (4) Isolated 4-20mA Sensor	4MI4C
4C5P1V1F1M Card - (4) Contact (1) 5v Power (1) Voltage input (1) Resistive Sensor (1) 4-20mA Sensor	4C5P1V1F1M
4C5PA1VA1F1M Card - (4) Contact (1) 5v Power+ (1) V[0	4C5PA1VA1F1M

to 5V] Voltage input (1) Resistive (1) 4-20mA	
(2) Channel HVAC Voltage Control Card	2AC
4C4CT Card - (4) Contact and (4) AC Current Transformers Inputs	4C4CT
8CT Card - (8) AC Current Transformers Inputs	8CT
4C1VS3V Exp Card - (4) Contact (1) Voltage Sampling, (3) Voltage	4C1VS3V
64C Card - (64) Contact Inputs on SCSI Connector	64C
32C8V8R Card - (32) Contacts (8) Relay (8) Voltage	32C8V8R

The label markings on the IO Expansion card translate to:

Marking Code	Description
C	Standard dry Contact Closure Input
CI	Isolated Contact Closure Input
CT	AC Current Transformer
V	Analog Voltage Input
VI	Isolated Voltage Input
VA	Restricted 0 to 5V range for V input
M	4-20mA Current Input
MI	Isolated 4-20mA Current Input

R	Low-Current Form A Relay
SR	Solid State Relay
F	Resistive Fuel Sensor
15P or P	+/-15 VDC Power Output
5P	+ 5 VDC Power Output
5PA	Enhanced 5V power
D1 (or C) and D0 (or D)	Wiegand Access Control
RC	Form C Relay

For Form C relays, the relay points will be marked:

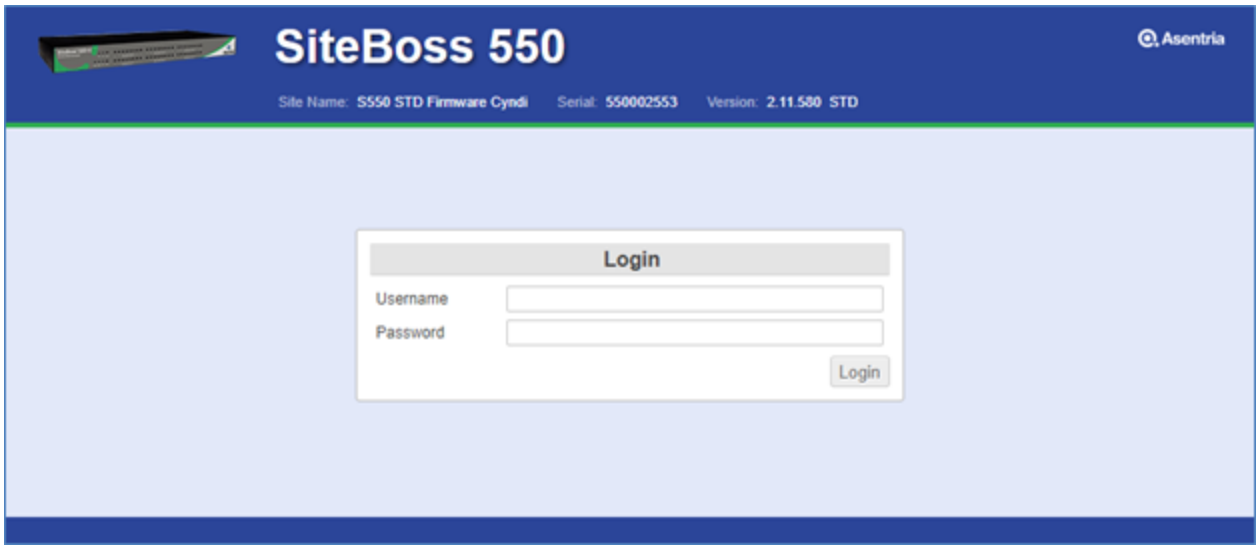
NC	Normally Closed
C	Common (always connected, hot)
NO	Normally Open

Navigating the Web Interface

There are two interface options for command and control of your SiteBoss. The Web Interface is an intuitive GUI interface that can be used for routine control and maintenance of your SiteBoss via HTTP or HTTPS using up to date versions of Chrome, Firefox, or Internet Explorer. The Command Line Interface can be reach via Serial, Telnet or SSH interface options. Some advanced debugging or control functions can only be accomplished via the Command Line Interface.

The SiteBoss has a built-in HTTP web server that can be used to configure the unit from anywhere the unit can be accessed on the network or Internet. This interface is enabled by default. Simply connect to **`http://<IP address of SiteBoss>`** *or* ***`https://<IP address of SiteBoss>`*** to use Secure Sockets Layer (SSL).

Upon connection, you will be greeted by a login screen. Log in with your Login ID (Username) and Password. These are the same credentials you would use to log into the command interface. By default the user name is **admin** and the password is **password**. It is highly recommended that the master password be changed via the User Profiles option from the Security menu.

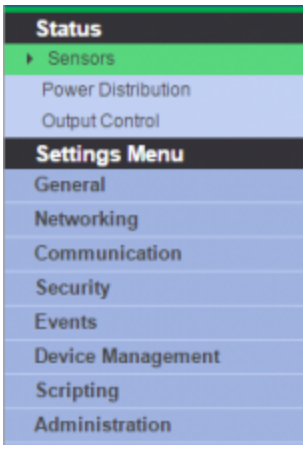


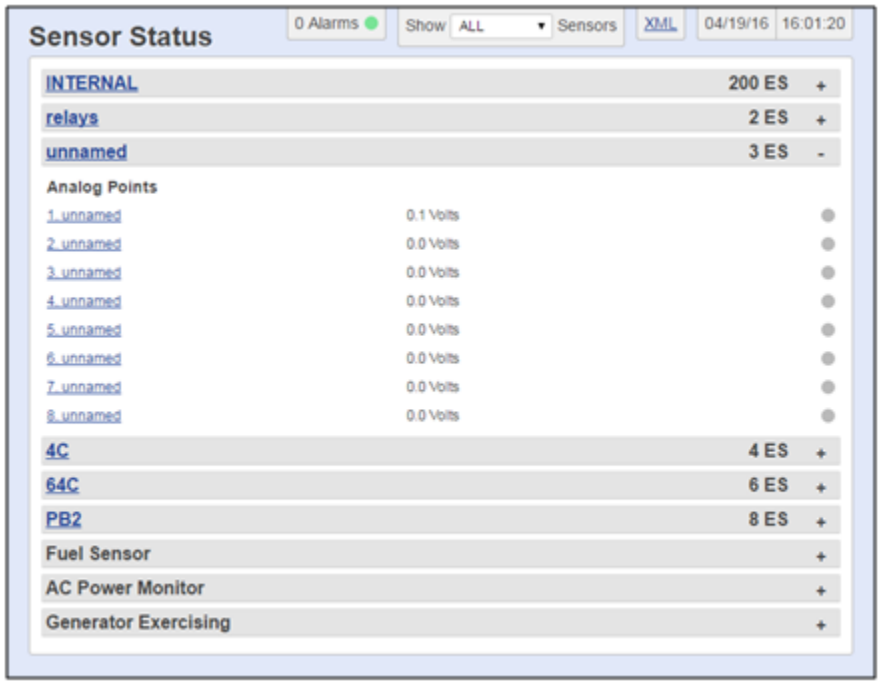
Once logged in, the Sensor Status screen will be displayed. There is a menu tree on the left side of the display to configure and control the SiteBoss. Using the menu tree you can alter most of the settings in the same way you could via the Command Line Interface.

This interface can be disabled. The configuration options for the Web Interface are located in the Web section of the Networking/Servers menu. If the Web Interface has been disabled it can be re-enabled at any time via the Command Interface SETUP menu at NETWORK SETTINGS/Server Settings/Web Server.

►Web Interface Control Features

The top section of the Web Interface display contains the type of Asentria Unit you have logged into, the configured Site Name, the unit's factory assigned Serial Number and the software version loaded on this SiteBoss. On the far right of the header you will see the user ID that you have logged in under and the Logout button.



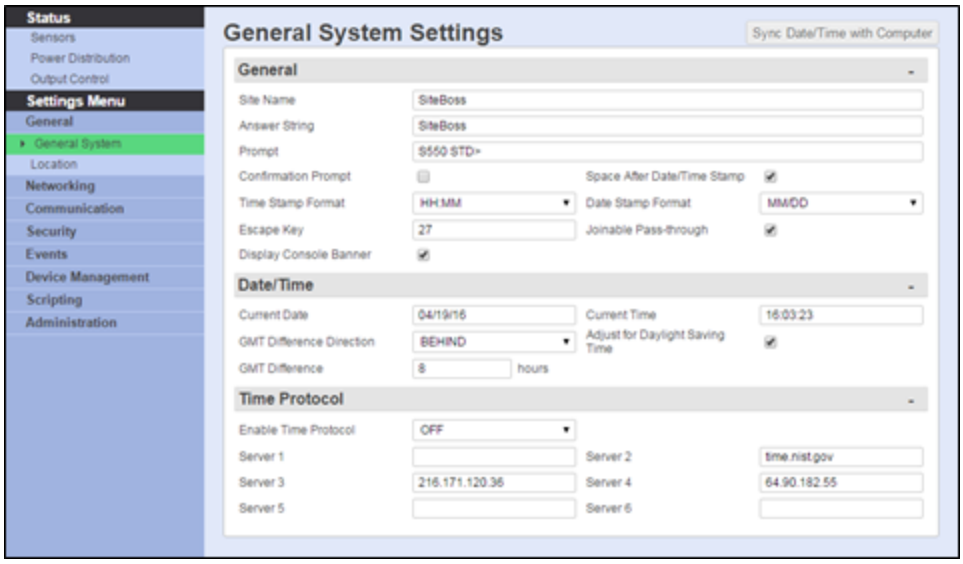


On the left side of the Web Interface display are navigation buttons.

Clicking on any of the "Status" options will bring up a status page displaying information regarding the subject of the button. For example the "Sensors" button will bring up a display that shows all of the installed EventSensors.

Most pages have sections separated by a colored bar. These sections are collapsible. Double click any bar and all sections will collapse for ease of handling long pages. A single click will collapse or expand any single section.

The buttons in the Settings Menu section will bring up a submenu of options under the subject heading listed. Clicking on one of the submenu options will change the page display, bringing up the settings page for the subject selected.



Settings Entry Functions

There are several different types of entry options for adjusting settings via the Web Interface.

Checkbox

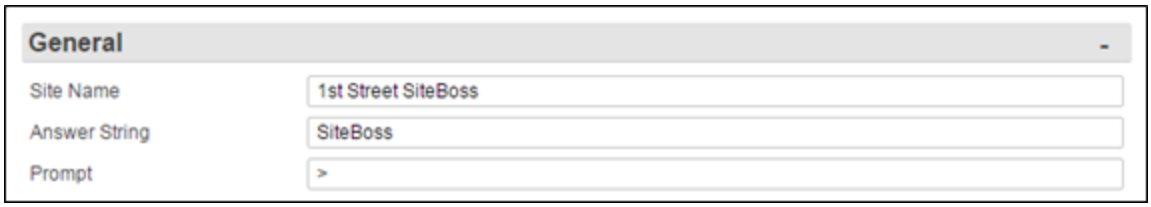
Checkboxes are common for enabling and disabling settings. They are ON/OFF type options. A check means ON. Click on the square to turn the option on or off.

Information Pop Up

Hovering over certain settings will cause informational pop up boxes to appear. These are designed to supply extra detail about the option.

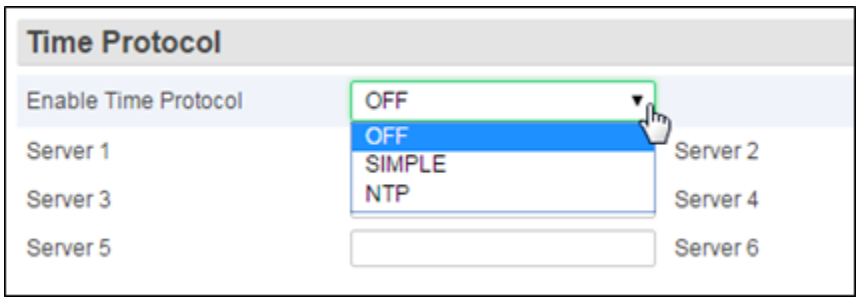
String Entry

String Entry fields are locations where you can type in text, such as a description. Site names, for example, are user definable descriptions that will display in emails and traps as well as displaying at the top of the web interface menu screen. This type of entry field will quite often have a default description. You can delete the default and type in your own unique descriptive text string. These usually have a maximum field size, which varies. The field sizes are defined in the function section of the user manual and will be truncated if oversized.



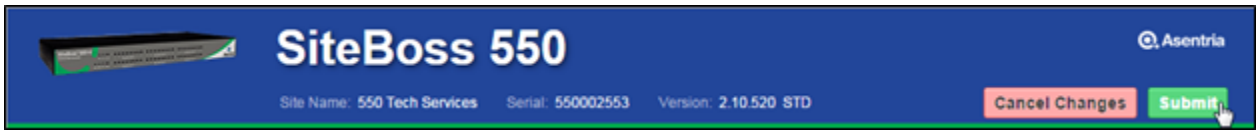
Drop-Down Menu

Another common input option is drop-down menu boxes. These typically give three or more options to choose from. Click the desired option and it will show in the display box.



Submit Button

Once you make a change to a setting, two buttons will appear in the upper right section of the page. If you are satisfied with the changes that you have made, click the Submit button. If you want to cancel the changes, and revert the settings to what they were before, click the "Cancel Changes" button.



» **Note**: Take care when making changes to Networking Settings. These changes are made immediately once the Submit button is clicked. The network connection could be lost and you will have to reconnect using the new configuration.

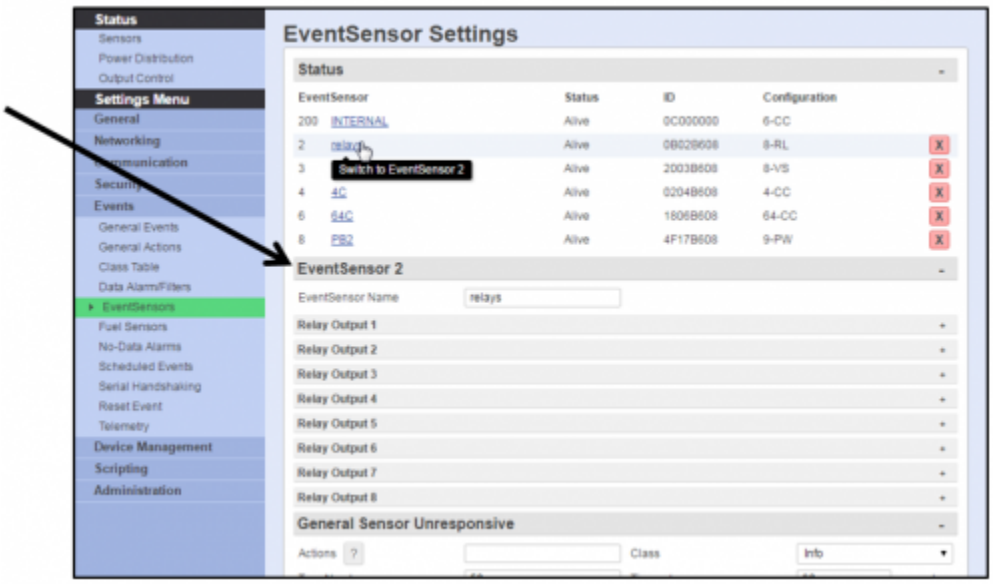
Notice Boxes

The unit will give informational type notices at the top of the page. These are color coded notices for the user. Informational notices, such as the unit letting you know something was completed successfully, will be in green. The notice will display for a few moments and disappear. The "x" can be clicked at any time to close the notice.

Yellow is a warning color. It will contain a message regarding a system settings change that needs to be adjusted. Warning notices will also display for a few moments and then disappear. The "x" can be clicked at any time to close the notice.

A message in red is a warning that the action attempted failed. Red warning notices stay at the top of the screen until manually closed by the user by clicking the "x" on the right hand side of the notice. The setting that failed will have the entry field colored red to denote the error.

Alternate Settings Fields



There are some locations which have menu options in the upper sections of the page, which when clicked, change the available options in the lower entry fields.

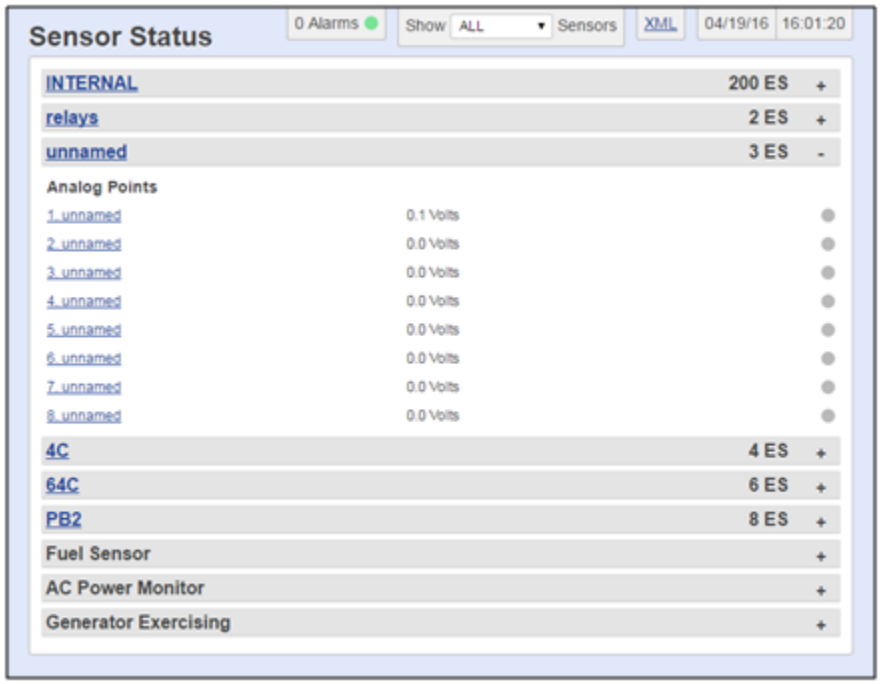
The name of the section whose settings are now displayed in the lower settings section will be in the header over that section.

To change the settings to another of the available menu options, simply click the menu hyperlink and the settings fields for the selected menu option will display below.

Save your changes before moving to another menu page.

►Status Pages

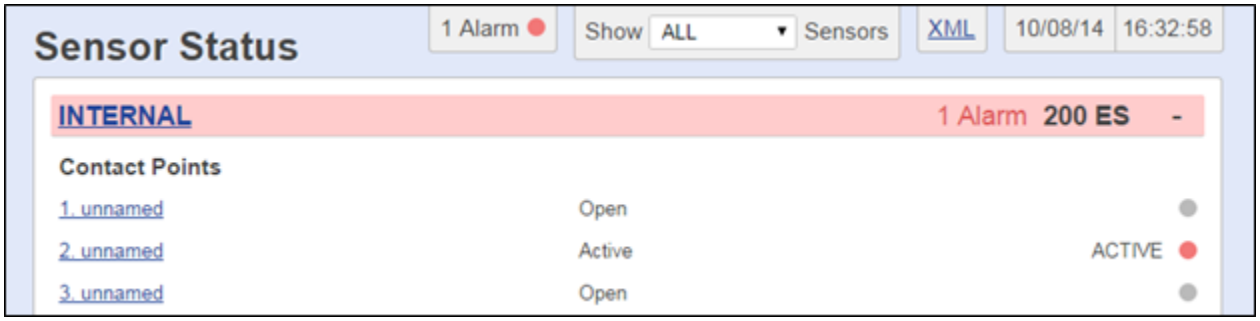
Sensors



The Sensor Status page is usually a long page with the status of all internal and external EventSensors. Double click on any grey bar to collapse all sections for easier navigation. A single click will expand or collapse a single section.

To configure the settings for any sensor, click the blue text associated with the sensor point and the user will be redirected to the EventSensor configuration page for that EventSensor. Alternately a user can use the menu tree on the left hand side of the screen. Select Events and then the submenu EventSensors. Click the EventSensor in the upper section to reach the configuration page for any specific sensor point.

The number of sensors in their alarm state will be displayed at the top of the page. The grey bar will be highlighted red for the section with a sensor in the alarm state and the virtual LED will be lit red.



Show <ALL/ENABLED> Sensors

The Show drop-down box at the top of the page toggles between ALL and ENABLED sensors. If toggled to ENABLED only the sensors that have been enabled in their configuration page will display. The default is ALL.

XML

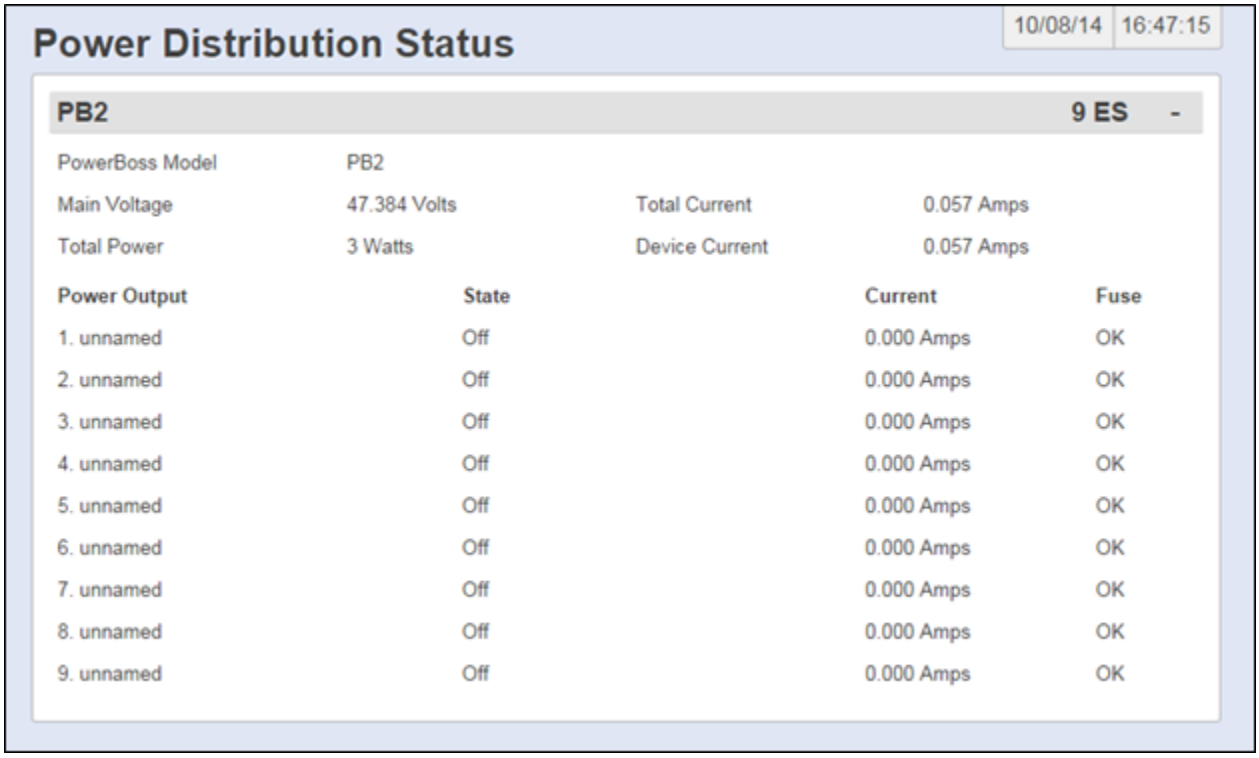
This link will display the page information in XML format.

Date/Time

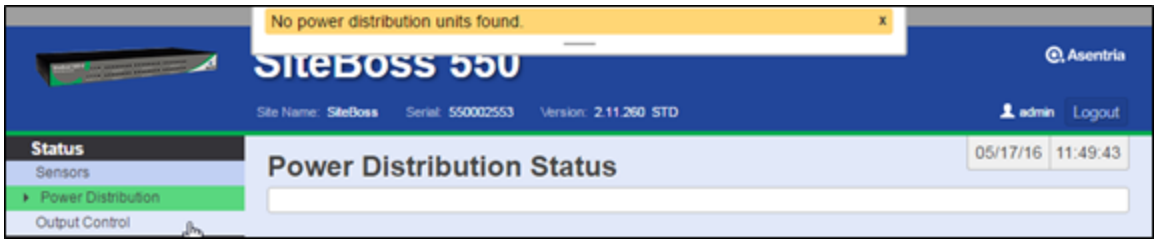
The date and time that the SiteBoss is set to are displayed in the upper right corner. The Date and Time can be adjusted in the Settings menu under General, General System.

Power Distribution

This menu option will display status on any connected PowerBoss2, PowerBoss4 or PowerBoss6. This status page provides information in real time for the current and voltage of both the Main and individual power outputs.



If no PowerBoss is installed you will get a page that looks the screen shot below. The page will have no functionality.



Main Voltage
The Main Voltage displays the voltage across the main power bus bars.

Total Current
Total Current displays the total current drawn by the PowerBoss and the devices connected to all of the power distribution outputs.

Total Power
Total Power displays the total power drawn by the PowerBoss and all of the power distribution outputs (Main Voltage x Total Current).

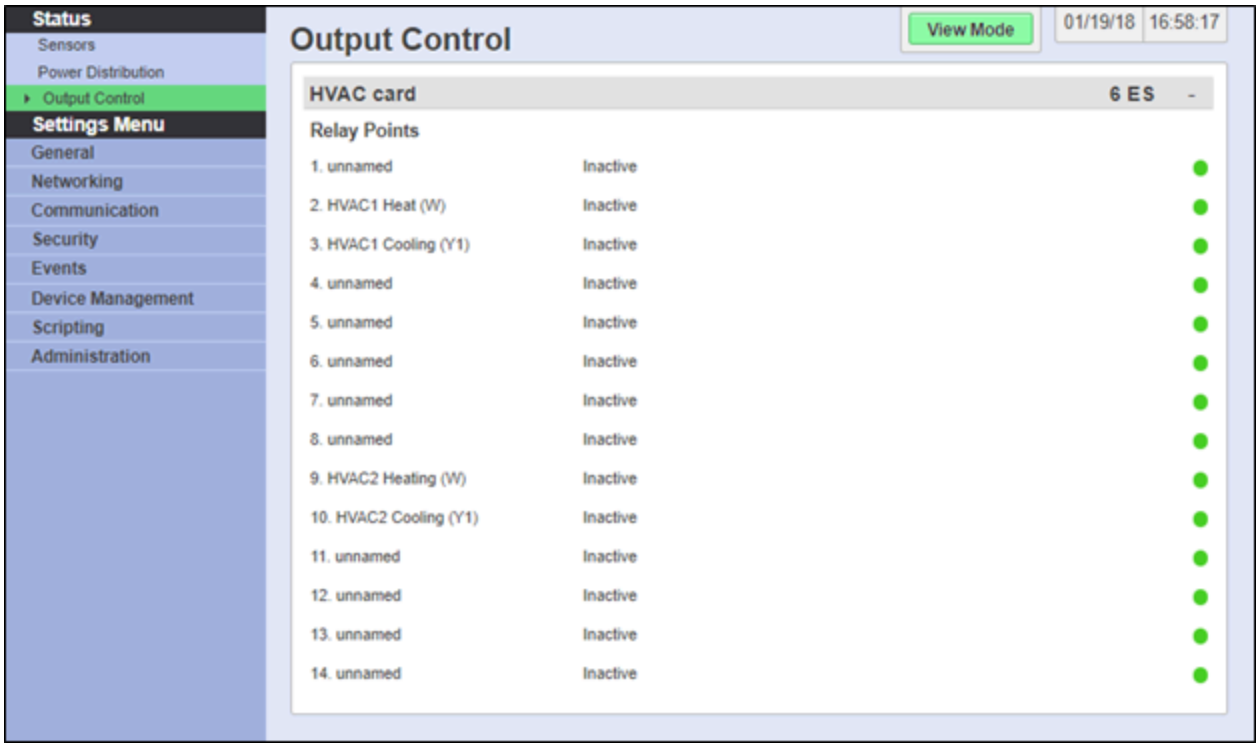
Device Current
Device Current displays only the current drawn by the PowerBoss itself.

Power Output
The Power Output section lists installed power distribution outputs showing their Name, State (ON or OFF), and the current that connected devices are drawing, and, for a PB2, the Fuse status of each (OK or BLOWN). If no fuse is installed it will be labeled OK.

Power Output Control

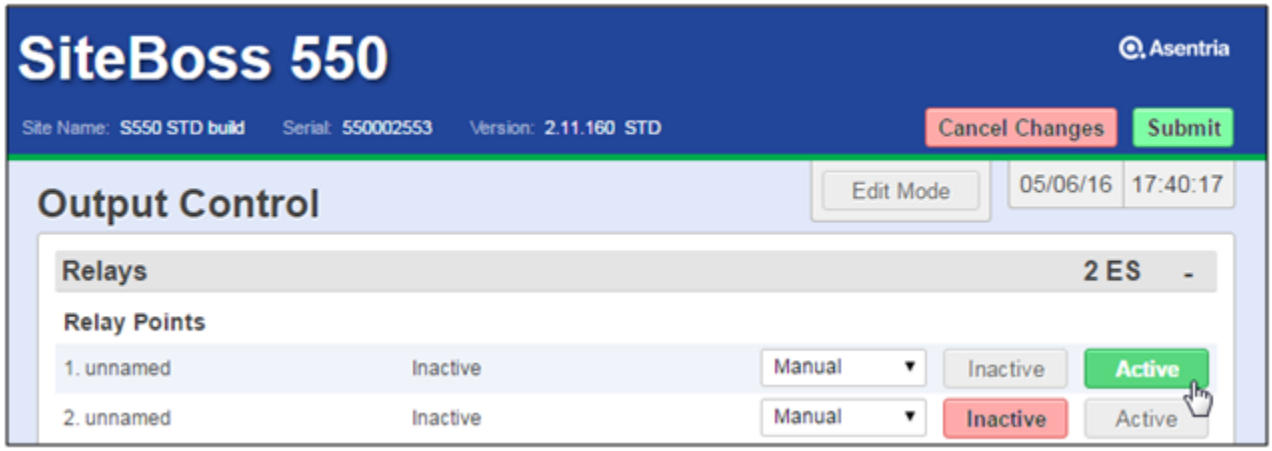
To toggle any relay or connected power outputs controlled by your SiteBoss, navigate to the Output Control Status display.

Click the View Mode button. This will change the mode to Edit. Off and On buttons for Power Outputs or Inactive and Active buttons for relays will display. You will also have Manual and Timer options in the Edit Mode.



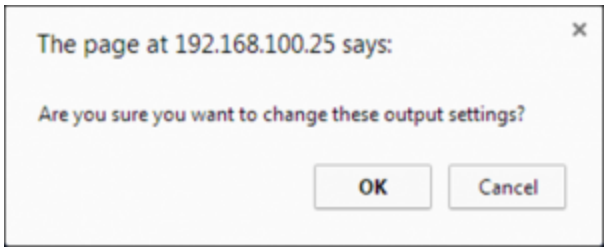
Manual Output Operation

Use the Edit Mode options to manually toggle a relay or power output.



To manually change the output to the opposite state, click the button corresponding to the desired output(s) and submit.

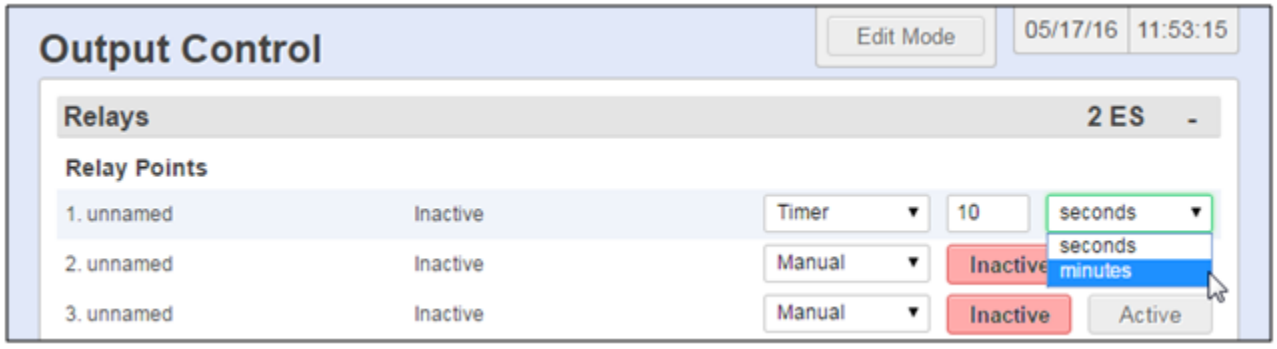
A challenge pop up will appear at the top of the page, click OK and the relay or power output state will change.



Timer Output Operation

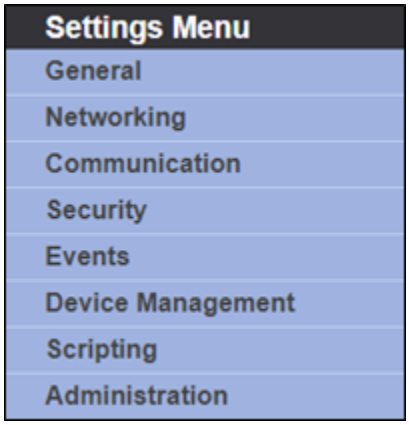
Use the Timer options to select a period of time you want the output(s) to switch from the current state to the opposite state. Once the defined time elapses the output will switch back to its original state.

Toggle Manual to Timer and you will get option boxes to define how many seconds or minutes you wish to toggle the power. Manually type in the number of desired seconds or minutes and click Submit at the top of the page.



A challenge pop up will appear at the top of the page. Click OK and the relay or power output state will change to the opposite state for the defined period of time and then return to its original state.

Settings Menu



This section will cover the menu options and settings configurations. This section covers using the Web Interface menu tree and structure. All of these settings can also be controlled via the Command Line Interface. For instructions on controlling your SiteBoss via the Command Line Interface see the Command Line Interface section of this manual.

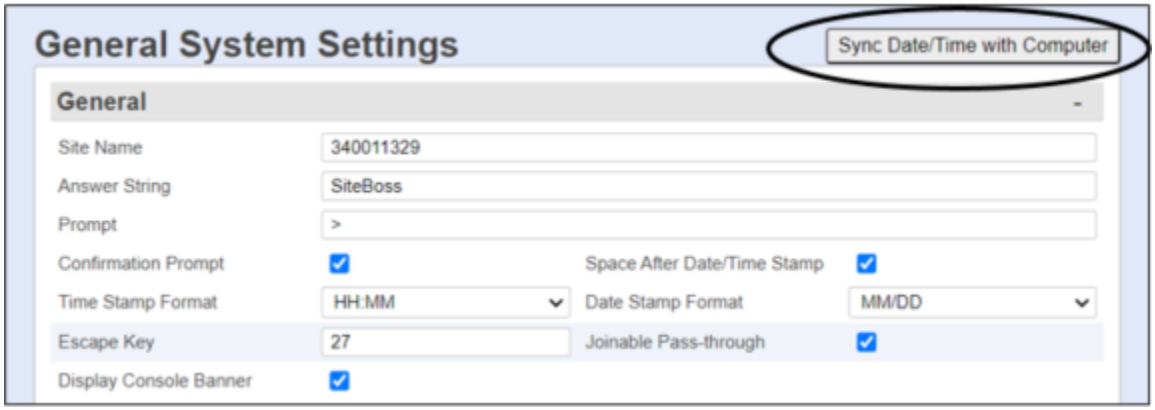
►General

General System

The General System page is where you can set the site name, answer string, confirmation prompt, date/time, and other general settings.

Sync Date/Time with Computer

This is a shortcut key on the top right side of the page to rapidly sync the date and time on the SiteBoss with the Date and Time on the clock of the user's computer. Click button and submit to update the date and time fields.



General System

Site Name

This is a text field to set the name assigned to the SiteBoss. This name is included with alarm messages (Traps, Emails, etc.) and is displayed at the top of the Web Interface. The name should be unique for clarity. The maximum length is 40 characters. The default setting is "340 - <serial number>".

Answer String
This is a text field to set the string that is presented when a user connects to the SiteBoss via the command line interface. The maximum length is 31 characters. The default setting is SiteBoss.

Prompt
The Prompt option sets the character(s) or settings values displayed as the command line interface prompt. The prompt characters can be customized, and includes the ability to embed one or more settings values in the prompt, for example the site name could be used in the prompt using a settings key of **`sys.sitename`**. A customized command prompt can help simplify administration of units, particularly where multiple units are involved.

The Prompt can be set as plain text characters or if using a settings key the syntax is: $(setting_key_name). If the setting key is not accessible for any reason (invalid key, insufficient user access level, etc.), "ERROR" is displayed instead.

The setting can contain up to 64 characters, but the prompt itself is limited to 30 characters. The default is >.

Confirmation Prompt
This checkbox is an ON/OFF toggle to set whether a confirmation prompt (Are you sure (y/n)?) is displayed when clearing the settings for an EventSensor in the EventSensor Setup menu and certain control functions in the Command Line Interface. The setting will not change without a positive response to the challenge question. The default setting is ON (checked).

Space After Date/Time Stamp
This checkbox is an ON/OFF toggle to set whether a space is appended to the end of the Date/Time stamp. The default setting is ON (checked).

Time Stamp Format
This is a drop-down box to choose the format for how time stamps are formatted. The options are HH:MM, HH:MM:SS, or BLANK. The default setting is HH:MM.

Date Stamp Format
This is a drop-down box to choose the option for how date stamps are formatted. The options are MM/DD, MM/DD/YY, MM/DD/YYYY, or BLANK. The default setting is MM/DD.

Escape Key
This is a text field to set the decimal ASCII character code of the key that must be pressed to escape from a pass-through mode in the Command Line interface. The default is 27, the <ESC> key.

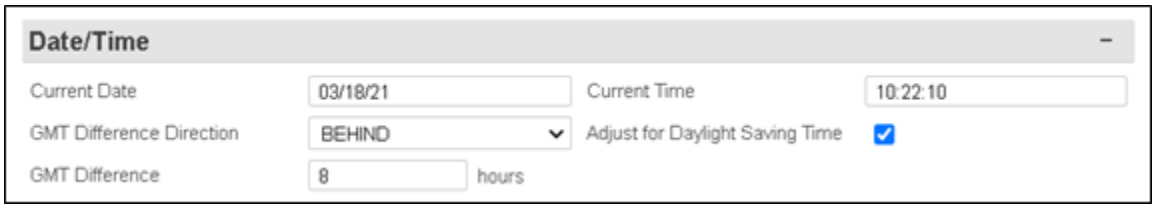
Joinable Pass-through
This checkbox is a toggle to allow or disallow multiple user pass-through sessions. Checking this checkbox sets the unit to allow more than one concurrent user to connect on a pass-through session. Un-checking this box sets the unit to only allow one concurrent pass-through session, and those attempting to join after the first user is connected will receive a "port in use"

error message. The default setting is allow (checked).

Display Console Banner
This checkbox enables and disables the Console Banner messages, such as Connected to I/O1, in the Command Line Interface. The default is enabled (checked).

Date/Time Section

»Note: There is a shortcut button to sync the date and time with the user's computer. Click the button on the top right hand side of the display and submit to update the date and time fields.



Current Date
This field is used to set the date. Use the format MM/DD/YY.

Current Time
This field sets the time, HH:MM:SS, in 24 hour clock format.

»Note: The date and time settings are maintained by means of an internal battery backup when power is removed from the SiteBoss.

GMT Difference Direction
Use this field to set whether you are east (AHEAD) or west (BEHIND) of GMT (Greenwich Mean Time). For example, Seattle time is behind (GMT -8), and Tokyo time (GMT +9) is ahead. The default setting is BEHIND.

GMT Difference (hours)
Use this field to set the number of hours the current time zone is offset from GMT. Valid input ranges from 0 to 12. The default setting is 8 hours.

Adjust for Daylight Savings
This is an ON/OFF toggle that allows automatic daylight savings time updating.

A brief explanation of daylight savings time: On the second Sunday in March, clocks are set ahead one hour at 2:00 a.m. local standard time, which becomes 3:00 a.m. local daylight time. On the first Sunday in November, clocks are set back one hour at 2:00 a.m. local daylight time, which becomes 1:00 a.m. local standard time.

Time Protocol Section

Enable Time Protocol
This is a drop-down menu to choose between OFF, SIMPLE, and NTP. The default setting is OFF.

SIMPLE - When network time is set to SIMPLE the unit attempts to contact the configured time servers (see Time Servers setting below) periodically, attempting to query each using Simple Network Time Protocol (SNTP), Time, and Daytime protocols, in that order. Once a response is received for any protocol, the unit sets the system clock to the new time, updates the real time hardware clock (RTC), then the network time process dies. The interval for checking network time is hard-coded to 12 hours plus or minus a random several hours.

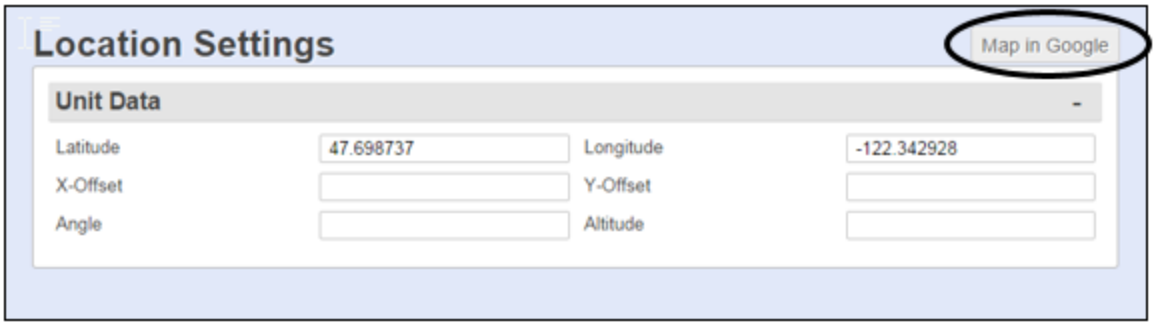
NTP - When network time is set to Network Time Protocol (NTP), the NTP daemon is kept running at all times. Unlike the SIMPLE setting, with NTP, the clock is not immediately set as soon as a time server is contacted. Rather, the NTP daemon utilizes various algorithms to set the time in an accurate and robust manner. Since the NTP daemon updates the system time asynchronously, the current time is stored in the RTC every 30 minutes while it is running. Note that if you change the clock manually, it may be a period of an hour or more before NTP resets it.

Time Servers
These fields are text fields to set the hostname or IP address of six time-servers. The maximum length is 64 characters. The SiteBoss uses the following servers by default:

- time.nist.gov
- 216.171.120.36
- 64.90.182.55

Location

Map in Google
This button will take the information from the Locations Settings section and open a tab in Google.com/maps displaying the information on a Google Map of the location.



Latitude
This is a text field where the Latitude of the unit can be entered.

Longitude
This is a text field where the Longitude of the unit can be entered.

X-Offset, Y-Offset, Angle, Altitude
These are additional text fields that can be used to more specifically define the location of the unit.

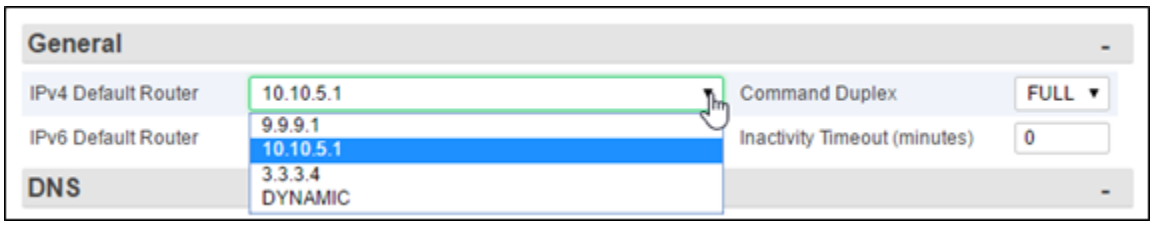
►Networking

The Network Settings menu contains all of the options pertaining to network communication. The IP Routing & Restrictions Feature Guide on the Asentria Information Portal will have additional information and configuration examples for various features covered under the Networking Settings menu

Network

The Network tab contains the settings for the Ethernet communications.

Network General

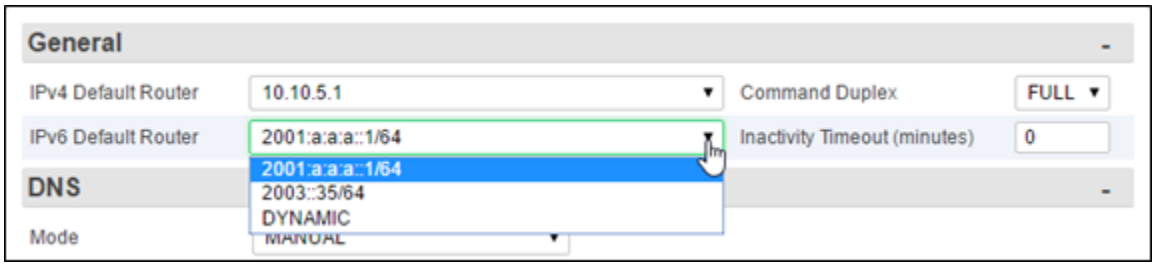


IPv4 Default Router
The IPv4 Default Router option displays a drop down list of any configured router address(es) and DYNAMIC. The default (Gateway) router can be defined by setting the Router Address for any Ethernet interface, see the IPv4 section of the Ethernet *n* chapter for instructions. Any configured router for an interface that is up will show up in the drop down list that can be selected for the default route.

DYNAMIC in the default router options simply means that the default router is set only according to the default routing rule of any dynamic network interfaces that may be up, such as the Dialup POTS modem or the Wireless modem. The rule for Dialup POTS modem PPP is that whenever that interface is up, it is always the default route and overrides any other default route. The rule for Wireless modem is that it is the default route when the Wireless default route is enabled. In other words, DYNAMIC default router means the default router will be whatever POTS/Wireless modem PPP decides when it is running. Any other value for the default router means that the default router will be that value (e.g., an Ethernet router).

IPv6 Default Router

If any Ethernet interface is set to AUTO, the list will only show DYNAMIC. This is because in AUTO mode, default routes are determined by router advertisements and set by the operating system. If AUTO is not set, and there is more than one static router in the list, the user should select the preferred default router. If DYNAMIC is set, the OS will pick a default router from the list.



Command Duplex

This option controls the echo settings for the command interface. Full duplex causes the unit to echo all characters sent to the remote device. Half duplex turns off character echo. The default setting is FULL.

Inactivity Timeout

The Inactivity Timeout sets the number of minutes (0 - 255) before a network connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. The default setting is 0.

DNS

The Name Resolutions Settings menu can be used to configure the IP Addresses of up to two Domain Name Servers (DNS).

DNS Mode

The DNS Mode toggles between MANUAL, ETH1-DHCP, and DSL. The default setting is MANUAL.

DNS Server 1 *and* ***DNS Server 2***

The DNS Servers are the IP addresses of Domain Name Servers that you may want to configure so that you can use host names rather than IP addresses in functions where name resolution may be needed, such as; Email server, RTS push hosts, action IP settings, network time servers, scripting TCP connections, etc. The default setting for each DNS Server is 0.0.0.0.

Ethernet *n*

The Ethernet Settings section is used to configure each of the two standard Ethernet ports as well as any of the six VLAN interfaces for each port. The drop-down menu in the grey section bar toggles between Ethernet 1 and Ethernet 2 to allow separate configurations for each port.

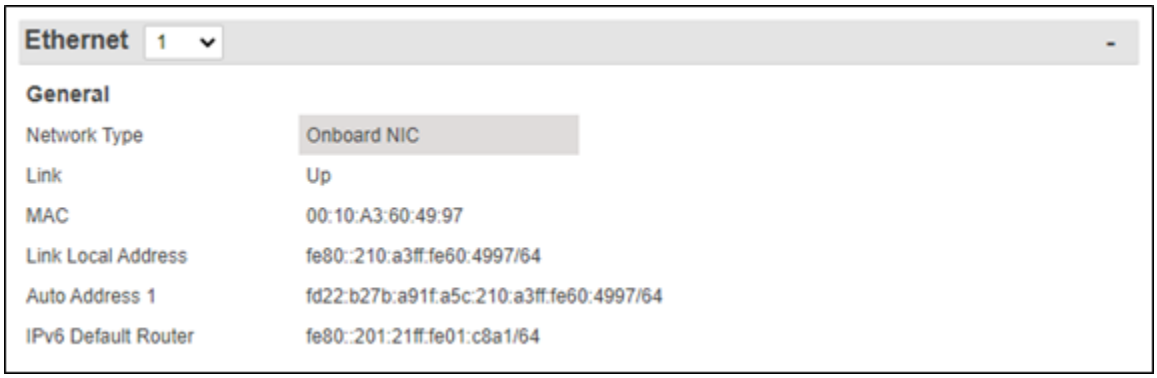
If an SFP (Small Form-factor Pluggable transceiver) expansion card is installed in the SiteBoss, there will be an additional option Ethernet 3. The SFP card is used on fiber optic network connections. Eth3 is always the SFP port. If no SFP card is installed there will not be an Ethernet 3 option displayed.

The on board Ethernet ports (1 and 2) as well as the SFP port can be set to bridge with any installed Ethernet Expansion interface. A bridge transparently relays traffic between multiple network interfaces; this means a bridge connects two or more physical Ethernet interfaces together to form one bigger (logical) Ethernet.

The Ethernet ports can be configured for either IPv4 or IPv6; they are dual stack so IPv4 and IPv6 can both be configured on the same port.

Any installed Ethernet Expansion cards are configured using the Ethernet Expansion menu selections covered in the section above.

Ethernet General



Network Type

This read only setting displays the NIC in use. Onboard NIC for the onboard Eth Port.

Link

This is a read only setting that reports whether the interface is up or down. It is used to determine if there is anything on the other end of the Ethernet cable. It displays "Up" if there is or "Down" if there is no connection.

MAC
The MAC field displays the factory defined MAC address of the Ethernet port.

Link Local Address
The unit automatically configures an IPv6 Link Local address for each interface where IPv6 is operating. This address can be used locally with other nodes on the link, even without specifying a STATIC address or AUTO (SLAAC) configuration.

Auto Address n
If the IPv6 mode is set to AUTO, the IPv6 default route is automatically configured and it is displayed here.

IPv6 Default Router
This field will display only if there is an IPv6 Default Route set in the unit. There is only one IPv6 Default route per unit. It is set using the General Settings at the top of the page, or if the Ethernet port is set to AUTO the IPv6 default route is automatically configured.

The OS will set a default route only if:

1. AUTO is enabled on at least one interface
2. AUTO is disabled on all interfaces, DYNAMIC is set AND the user has configured at least one IPv6 router.

IPv6

IPv6 operates independently from IPv4 configuration. For example, the user could have one interface in IPv4 VLAN mode and another interface operating in IPv6 AUTO mode. But the user could not have the same Ethernet interface operating in both IPv4 VLAN mode and IPv6 AUTO or STATIC mode.

Mode
Each Ethernet interface has 4 IPv6 modes: OFF, STATIC, AUTO and EXPANSION BRIDGE.

OFF disables IPv6 functionality.

STATIC means the interface has IPv6 enabled and the user should configure a Unicast Global address for it. It also has a link local address. A link local address will be created by the OS. If no static address is configured then it has only the link local address. If a static is configured then that router is added to the IPv6 default router list and can be selected as the default IPv6 router.

In AUTO mode the default routes are determined by router advertisements and set by the operating system. The only default route option in the General section at the top of the page

will be DYNAMIC if any IPv6 interface is set to AUTO.

If the mode is set to **EXPANSION BRIDGE**, the IPv4 settings for this port will be ignored and IPv4 network traffic will automatically be bridged (bridges are per network interface, not IP stack).

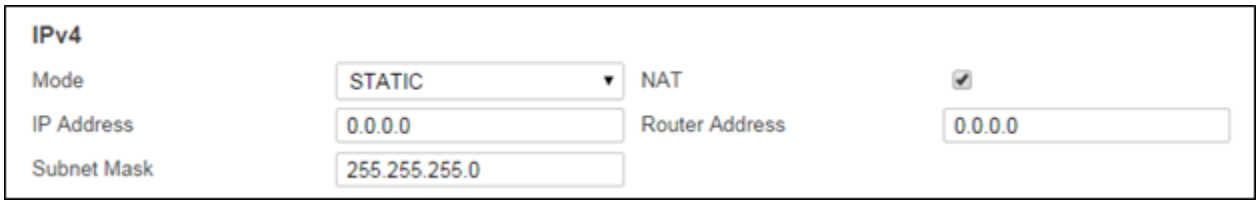
The default is OFF.

Static Address
If you configure the Mode to Static, use this field to set the static IPv6 address to use for this interface. This must be a valid IPv6 address with an optional prefix length in CIDR notation (CIDR notation is a slash at the end of the address that is followed by the prefix length in bits). The default prefix length is 64.

Static Router Address
The IPv6 address for the next hop IPv6 router. This must be a valid IPv6 address with an optional prefix length in CIDR notation. The default prefix length is 64. If set, it will be displayed as an option in the list of IPv6 default routers.

IPv4

The IPv4 mode function operates independently from IPv6 configuration.



Mode
The Mode option toggles between STATIC, DHCP CLIENT, VLAN, EXPANSION BRIDGE, ETH-BRIDGE or DHCP SERVER. The default setting is STATIC.

If the mode is set to VLAN, IPv6 must be disabled for the port. See the VLAN Settings section below for configuration instructions.

The Ethernet Expansion Bridge feature can be used to bridge either or both of the onboard Ethernet interface to the Ethernet Expansion network interface. This feature requires at least one Ethernet Expansion card (E4, 8E or SAEC card) to be installed.

If the mode is set to EXPANSION BRIDGE, IPv6 settings for the port will be ignored and IPv6 network traffic will automatically be bridged (bridges are per network interface, not IP stack)

If the Mode setting is toggled to DHCP SERVER some additional configuration options will be available. Please see the DHCP Server section below.

IP Address
Input the IPv4 network address assigned to this Ethernet port. The default setting is 0.0.0.0

Subnet Mask
Input the subnet mask provided by the network administrator. The default setting is 255.255.255.0

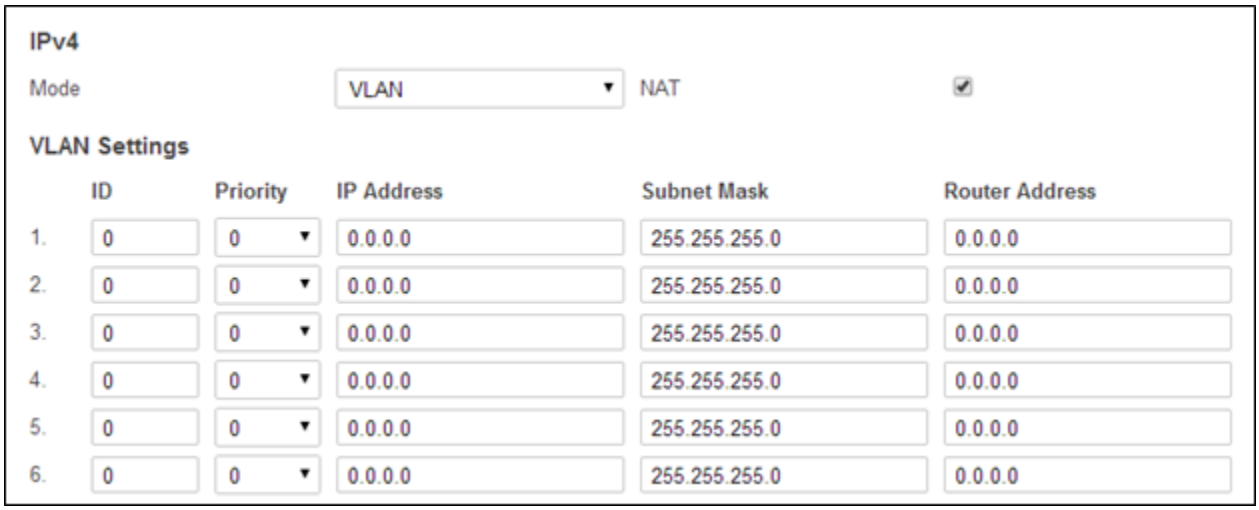
Router Address
Set the router address provided by the network administrator. The default setting is 0.0.0.0

NAT
This is an ON/OFF toggle to enable Network Address Translation. The default setting is ON.

VLAN Settings

If the IPv4 Mode is toggled to VLAN, the VLAN Settings fields are added to the Web Page. Use these fields to configure where any of six individual Virtual Local Area Network (VLAN) connections.

The following is a top-level overview of the SiteBoss VLAN settings. Refer to the IP Routing and Restrictions Feature Guide on the Asentria Product Information Portal for a more detailed explanation of VLANs.



ID
Input the identifier for the VLAN, 0 to 4094. The default is 0.

Priority
Set the priority assigned to egress frames, 0 to 7, with 0 being lowest to 7 highest. The default is 0.

IP Address
Input the IPv4 network address of this VLAN. The default setting is 0.0.0.0

Subnet Mask
Input the subnet mask provided by the network administrator. The default setting is 255.255.255.0

Router Address
Set the router address provided by the network administrator. The default setting is 0.0.0.0

DHCP Server

When an Ethernet interface is toggled to DHCP SERVER some additional settings fields are available for the DCHP Server. See the DHCP Server Feature Guide on the Asentria Information Portal for additional information.

Starting IP
This field sets the starting IP address for serving DHCP addresses. If this is default (0.0.0.0) then the unit will not run DHCP to serve addresses. The starting IP address MUST be on the same subnet as the interface IP

Max Clients
This field sets the maximum number of clients that can be configured for this subnet. Valid values are 1 - 253 with a default of 12.

Lease Time
Lease Time sets how long, in minutes, before the DHCP lease expires. The valid values are 4 - 240 with a default of 240.

IP Restrictions

The IP Address Restrictions section allows you to configure permissions and/or restrictions for communications to or from specific IP addresses.

IP Address Restriction is a primary defense against unauthorized access via a network or PPP connection. An administrator can restrict access by configuring specific IP addresses that will be the only ones allowed to access the unit. Restrictions can also be configured to deny access to larger groups of IP addresses using wildcards. IP Address Restrictions do not replace restrictions set by User Profiles, but they do provide an extra level of protection by causing the unit to ignore all network traffic except from the addresses allowed.

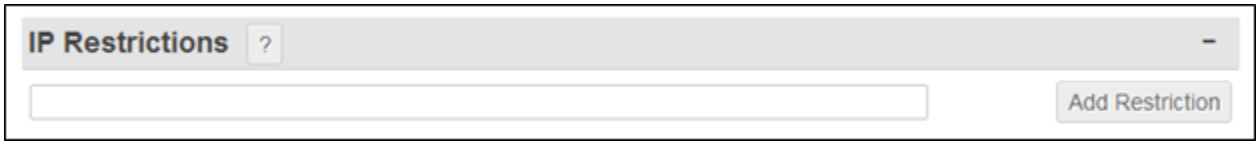
If no IP restrictions are defined in this menu, all incoming connections are allowed.

The Asentria unit evaluates the list of IP restrictions from top to bottom. When it finds an entry

that specifically allows or disallows access, it uses that entry and stops looking. Enter IP restrictions before the allowed addresses or subnets. However, if you enter any restrictions you **MUST** enter an allowed address or group, or you will lock yourself out.

»**CAUTION**: If any access restrictions are configured, a group or IP address that IS allowed access must be specifically defined. If no authorized access IP address or subnet is specifically defined BEFORE hitting Submit the unit will ignore communications from ALL IP Addresses. Serial access to the command line interface would then be required to regain access to the SiteBoss. See the Access via a Serial Connection section for instructions on how to connect via serial port.

Refer to the IP Routing and Restrictions Feature Guide on the Asentria Product Information Portal for a detailed explanation of IP Address Restrictions. By default, no address restrictions are configured.



The IPv4 wildcards are 0 and 255.
.0 is a wildcard that allows access to IP addresses in that group.
.255 is a wildcard that denies access to IP addresses in that group.

The IPv6 wildcards are :: (double colon) and ffff.
:: (double colon) allows IP addresses in that group.
ffff restricts IP address in that group.

Entering a specific IP address sets that address to be allowed access. There is no way to disallow a specific IP address, only a subnet group.

Where *n* represents a whole number:

For IPv4

- 0.0.0.0 sets the unit to allow all IP addresses.
- 255.255.255.255 restricts all IP addresses.
- *nnn.nnn.nnn*.0 allows all IP addresses in the specified a subnet.
- *nnn.nnn.nnn*.255 restricts all IP addresses the specified in subnet.

For IPv6

- :: (double colon) allows all IP addresses
- *nnnn:nnnn:nnnn:nnnn*:: allows all IPv6 addresses in a /64 subnet
- *nnnn:nnnn:nnnn:nnnn:ffff:ffff:ffff:ffff* blocks all IPv6 addresses in a /64 subnet
- *nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn* allows a specific IPv6 address

Automatic IP Blacklist

The Firewall Automatic Blacklist feature helps mitigate the risk of unauthorized access to the unit. It does this with a blacklist that is updated when a login fails consecutively. For example, if any network-based login fails the specified number of times in a row from the same IP address (regardless of user or method of connection), then any inbound IP packets from that IP address are dropped. If a legitimate user gets added to the blacklist, they have two options:

- Reboot the device. The blacklist is not saved when the system is restarted or rebooted.
- Login to the device from another IP and clear the blacklist using the "Clear Blacklist" button.

Enable

This checkbox will enable (checked) or disable (unchecked) the blacklist feature. The Default is unchecked (disabled).

Max Consecutive Failures

This field is used to set the number of consecutive login failures before an IP is blacklisted.

Clear Blacklist

This button Clears all blacklisted IPs.

Ethernet Expansion

The Ethernet Expansion settings apply if you have at least one Ethernet Expansion slot card (4E, 8E, or SAEC card) installed in the SiteBoss. If a card is not installed these settings will have no functional effect on the unit.

This feature allows the unit to operate a logical Ethernet interface. The SiteBoss can have up to two Ethernet Expansion cards and can potentially operate all available physical Ethernet ports on one logical interface.

The Ethernet Expansion Card is a subordinate interface. It is also a built-in 10/100 Ethernet switch. Any node plugged into one card can have its Ethernet traffic conveyed to any other node plugged into another card on the same unit; that is, all cards act together as one logical switch.

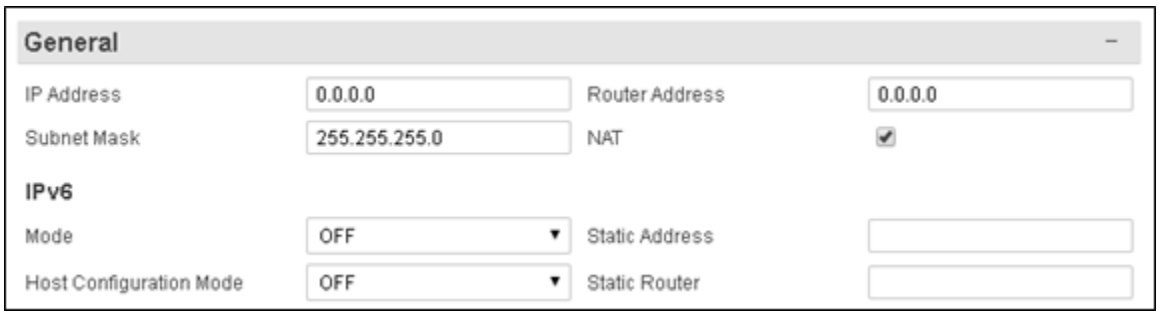
Unlike the on-board Ethernet interfaces, an Ethernet Expansion does not support VLANs or DHCP address acquisition. In other words, the Ethernet Expansion can be addressed only by statically assigning it an IP address.

» Caution: do not plug an Ethernet segment carrying a DHCP-managed IPv4 network into any ETHEXPAN subordinate interface while the unit serves DHCP on it. Doing so will cause conflicts with other nodes on that network and the already-existing DHCP server.

For more detailed configuration and use instructions please refer to the IP Routing & Restrictions Feature Guide.

Ethernet Expansion General

The main use case is that at a remote site the unit has one or more Ethernet Expansion interfaces attached, and facilitates network access to the network equipment nodes that are plugged into these subordinate interfaces. As such, the unit can be assigned an address that is reachable by these nodes and is independent of the unit's other network interfaces. The unit can be configured to serve IP addresses to these nodes via DHCP. The unit can be configured to use static routing and port forwarding with these nodes. Regardless of whether DHCP is in use, the unit serves as a "WAN router" for these nodes; that is, the unit routes (and NATs) IPv4 traffic from these nodes to other destinations defined by the usual routing configuration of the unit, if any.



IP Address

Use this field to set the IPv4 IP address of the unit reachable by nodes on the network interface consisting of the Ethernet Expansion Card(s). This address must be set for the DHCP function to work.

Subnet Mask

Sets the IPv4 subnet mask for the Ethernet Expansion network interface.

Router Address

IPv4 address of the next hop router for this subnet. If set, it will be displayed as an option in the list of IPv4 default routers.

NAT

This is an ON/OFF checkbox to enable network address translation on the forwarded frames. Without NAT, a server would receive a forwarded frame that is IP-addressed according to the network on the Ethernet interface. The default setting is ON (checked).

IPv6

Mode

The mode is either OFF or STATIC. The default is OFF.

Host Configuration Mode

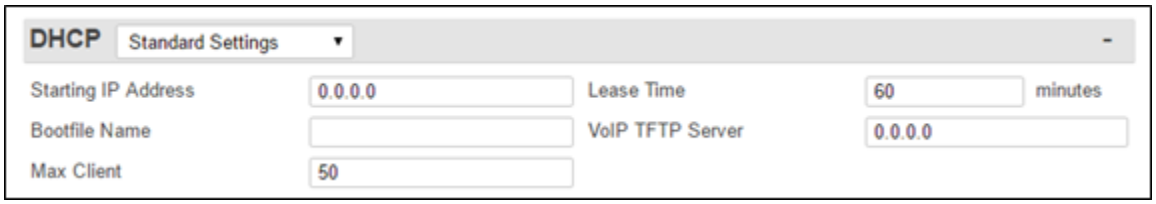
Host configuration mode controls how an IPv6 address is set on devices connected to the expansion card ports. Hosts can either use static IPv6 addresses, or if auto address configuration is supported, a router advertisement daemon is available (RADVD). The default is OFF.

Static Address
The static IP address for the expansion card. This must be a valid IPv6 address with an optional prefix length in CIDR notation (CIDR notation is a slash at the end of the address that is followed by the prefix length in bits). The default prefix length is 64.

Static Router
The IPv6 address for the next hop IPv6 router. This must be a valid IPv6 address with an optional prefix length in CIDR notation. The default prefix length is 64. If set, it will be displayed as an option in the list of IPv6 default routers.

DHCP [Standard Settings]

The unit can be configured to serve IP addresses to the devices connected to the expansion ports via DHCP. The unit can also be configured to use static routing. Regardless of whether DHCP is in use, the unit serves as a "WAN router" for these nodes; that is, the unit routes (and NATs) IPv4 traffic from these nodes to other destinations defined by the usual routing configuration of the unit, if any.



DHCP Starting IP Address
Sets the starting IP address for serving DHCP addresses on the Ethernet Expansion network interface. If this is default (0.0.0.0) then the unit will not run DHCP to serve addresses to unknown clients. This address is required for DHCP server to start and must be on the same subnet as Ethernet Expansion Card IP Address.

DHCP Lease Time (minutes)
This field sets the lease time for DHCP clients in minutes. The default is 60 minutes.

DHCP Bootfile Name
This option is used to identify a bootstrap file. Not all DHCP clients support it, others actually require it.

DHCP VoIP TFTP Server
Custom option for Cisco SIP phones

Max Client
This field sets the maximum DHCP IP addresses for unknown clients. The default is 50. The IP address range for unknown clients will be the DHCP Starting IP Address plus the max clients figure.

DHCP [Advanced Settings]

Toggle the drop down menu options in the DHCP grey bar to bring up this alternate settings field for advanced DHCP options.

These settings allow an IP address, or an IP address range to be assigned based on a client's MAC address (partial to full MAC addresses are allowed). For a partial MAC address, an IP address range must be specified; for a full MAC address, just one IP address is needed. All IP addresses must be on the same subnet as the Ethernet Expansion IP Address, set in the General section.

Class n
The Class drop down box allows for six separate Advanced DCHP IP Address configuration settings.

Class n Enable
Click box to enable this DHCP class IP Address settings configuration.

MAC (3 to 6 octets)
Input the client MAC address. MAC entries must have a minimum of 3 octets, each octet must be two characters. Octets must be separated by a semi-colon. For example, valid entries could be one of the following: 00:AA:B0, 10:0a:b0:04:55:60, 10:0a:b0:04:55.

Start IP
Use this field to set a Start IP address for the specified MAC address. If a full MAC address, this is the IP address that will be assigned to the client with that MAC address, and the end IP address is ignored. If partial MAC address, this is the starting IP of a range of IPs that will be assigned to clients that match the partial MAC address.

End IP
This field sets the End IP address for this MAC address range.

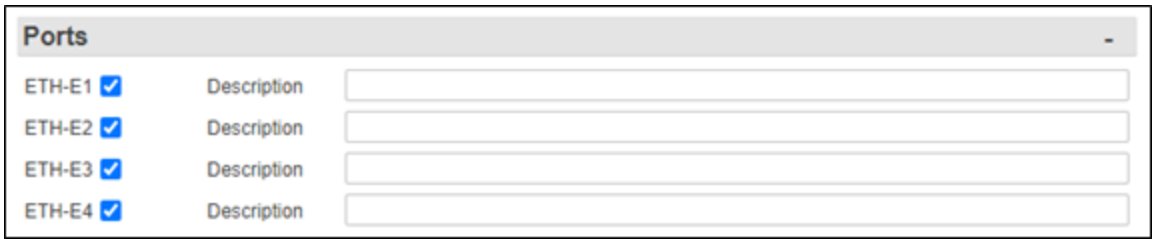
Ports

These fields will display only if you have a newer version Ethernet Expansion card and firmware after 2.11.210. A new hardware version of the Ethernet Expansion card started shipping early 2016. Older hardware does not have this functionality, so these fields will not display.

For one Ethernet expansion card, the ports are numbered 1-4 (right to left).

When looking at the back of a unit, expansion slots are numbered right to left. Given that, when 2 Ethernet expansion cards are inserted, the card in the lower numbered slot will have port numbers 1-4, the card in the higher numbered slot will have port numbers 5-8

» **Note:** This functionality is not currently available on the 8E expansion cards.

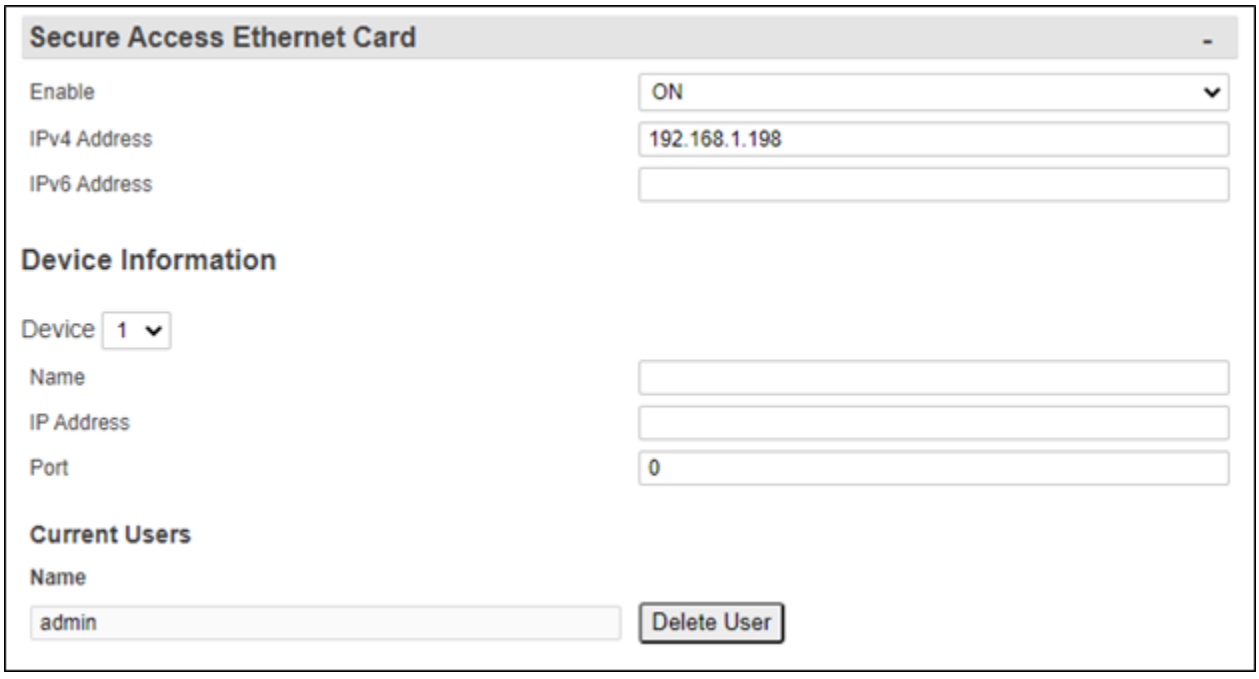


ETH-En
These check boxes are used to enable/disable individual ports on the expansion card. The default is enabled (checked).

Description
These are texts fields which allow the user to name the port. This allows for a description of the equipment connected to the Ethernet Expansion card.

Secure Access Ethernet Card

With a configured SAEC card, users can initiate a secure web session with a networked device using a Remote Desktop (RDP) session using the SiteBoss as a target. The RDP session can be initiated by a standard RDP client, or a Web browser that supports HTML5. After the RDP log in, the user is presented with a graphical desktop and can use the web browser on that desktop to access local devices. See the SAEC Feature Guide for more information



Enable
This is an ON/OFF toggle to enable the SAEC card. The default setting for this key is ON. A transition from ON to OFF will remove all SiteBoss RDP access to the SAEC, and then the SAEC will be rebooted. When the transition goes from OFF to ON, access to the SAEC via RDP is enabled.

IPv4 Address and Mask
The IP address needs to be an address within the range of subnet addresses for the SiteBoss Ethernet Expansion card. Per the default settings (in the General section) that range is from 192.168.1.1 thru 192.168.2.254. It is Recommended that the SAEC be assigned **IPv4 Address: 192.168.1.198, IPv4 Mask: 255.255.255.0**

IPv6 Address
This is used to set the IP Address if the Ethernet Expansion Card is set to IPv6. This should be on the same IPv6 subnet as devices connected to its ports.

Device Information

Information on devices connected on the SAEC subnet is set here. This information is used to create a web page of links to those devices. The drop down allows for configuring the Device Information for each device connected to the SAEC card.

Name
This is a text field to name the device connected to this port of the SAEC card.

IP Address
This is the IP address of the device connected to the port on the SAEC card.

Port
The port used to connect to the device.

Adding Users

When a user with Master privileges is added to the SiteBoss via the User Profile menu, that user will be automatically added as a SAEC user.

Adding Existing Users

Enhanced Security Builds
For SiteBoss firmware that supports enhanced security, the user must open their user profile (Security->User Profile) and enter their existing password, and then click on the Submit button.

Standard SiteBoss Builds
Existing users with Master privileges will be automatically added as a SAEC user.

Deleting Users
When a SiteBoss user is disabled or deleted, the user will automatically be removed from the SAEC.

» **Note**: If a user has a process still running on the SAEC, they may have to be removed via the SAEC menu. If the SAEC user list still displays a disabled user, please restart the SiteBoss, and then remove the user via the SAEC menu.

Displaying Users
From the Web UI navigate to: Networking -> Ethernet Expansion -> Secure Access Ethernet

Card -> Current Users

» **Note**: The Current Users section will only display if SAEC users exist.

Ethernet Bridge

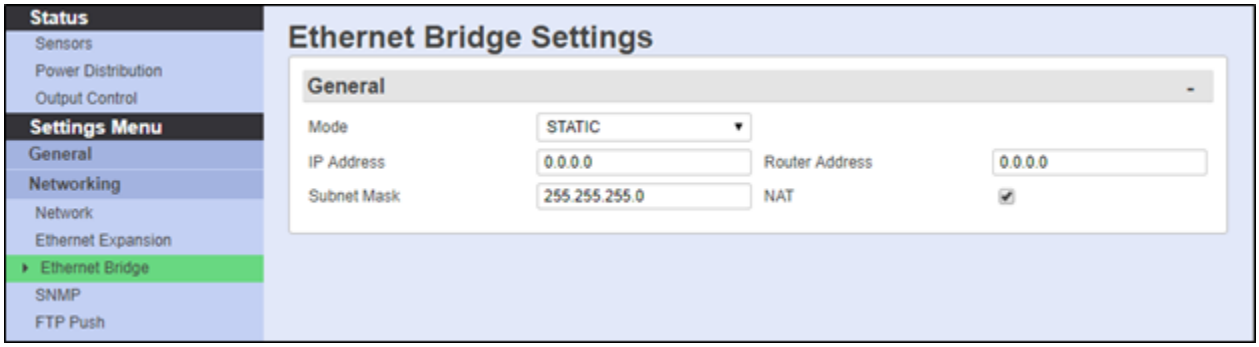
The Ethernet Bridge feature allows the onboard Ethernet interfaces, ETH1, ETH2, and (if an SFP Expansion card is installed) ETH3 to bridge with each other. Any combination of ETH1, ETH2, or ETH3 is supported. The bridge supports either Static or DHCP assigned IPv4 addressing.

» **Note**:IPv6 addressing is currently not supported.

Software version 2.11.710 STD or higher is required for this feature to work.

An Ethernet interface is added to the Ethernet Bridge by setting its mode to ETH-BRIDGE. In this mode, any settings (IP, Mask, etc.) on the physical interface are retained, but ignored and the interface is added to the bridge. Any configured interface settings (IP, Mask, etc.) are only used when the mode is set to STATIC.

See the Ethernet Bridge Feature Guide for more information.



Mode

Sets the IPv4 addressing mode, STATIC or DHCP CLIENT for the bridge. If set to static, the user inputs IP, mask and, if applicable, router IP. If set to DHCP client, the DHCP client service is started and waits for DHCP server response(s). The default mode is STATIC.

When switching modes from STATIC to DHCP CLIENT, the bridge's settings will be locked, zeroed, and reset to the settings supplied by the DHCP server (if acquisition is successful). 'Locked' means the settings can not be changed by the user, unless mode is set back to STATIC.

When switching modes from DHCP CLIENT to STATIC, the current IP, mask and router values will be unchanged and settings will be unlocked.

IP Address

If mode is static, this is set by the user to an IPv4 address. If the mode is DHCP client, it will be set when the DHCP client receives it from the DHCP server. The default is 0.0.0.0

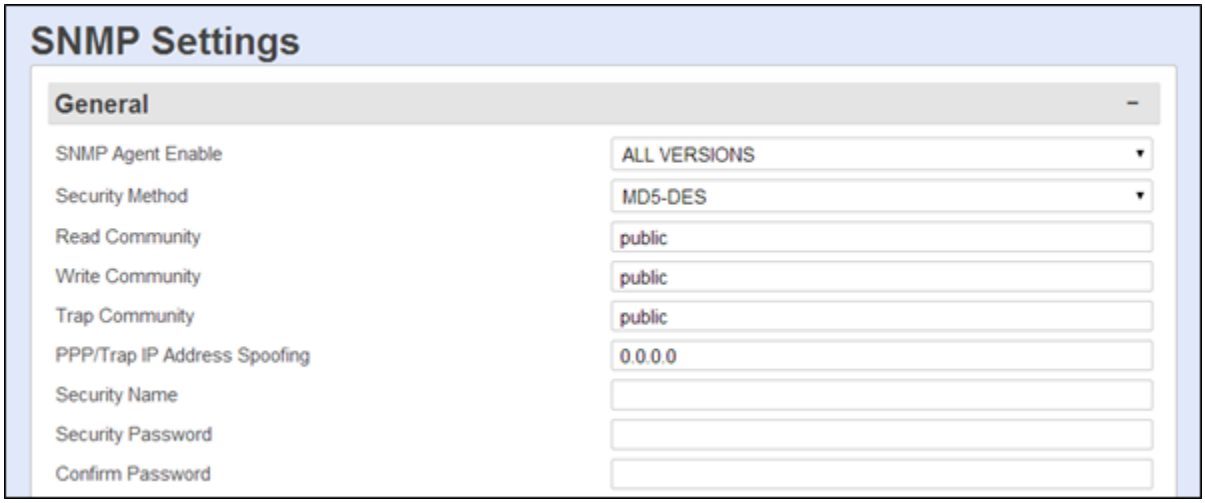
Subnet Mask
This is the Network mask. If mode is static, this is set by the user. If the mode is DHCP client, it is set by DHCP client. The default is 255.255.255.0

Router Address
This field sets the network router for the bridge. If mode is static, this is set by the user. If the mode is DHCP client, it is set by DHCP client. Default is 0.0.0.0

NAT
This checkbox is used to Enable / Disable NAT for the bridge. The default is enabled.

SNMP

The following is a top-level overview of the various SNMP features and settings. For more detailed configuration and use instructions see the SNMP Operations Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support.



SNMP General

SNMP Agent Enable
This is a drop-down box to choose between ALL VERSIONS, V3 ONLY, or OFF, and controls whether the unit responds to SNMP 'gets' and 'sets'in the selected version. Note that for V3 operation the user profile passwords are used for authentication (via MD5) and encryption (via DES). Passwords for user profiles intended for SNMPv3 use must be at least 8 characters. The default setting is ALL VERSIONS.

» Note: SNMP Agent Enable does NOT stop SNMP traps from being sent when it is set to OFF.

Security Method
This is a drop-down box to choose between MD5-DES and SHA-AES to controls whether MD5 and DES, or SHA and AES, are used for authentication and privacy, respectively, for SNMPv3 get/set/trap operations. The default setting is MD5-DES.

Read / Write / Trap Community

These fields set the SNMP trap community names to use. The default setting for all is public. The maximum length for each is 23 characters.

PPP/Trap IP Address Spoofing
This specifies what the source IP address field of v1 traps the unit transmits. If undefined then the unit will use the PPP interface address if it leaves the unit on PPP, otherwise it is the first non-0.0.0.0 IP address configured via the Ethernet Settings.

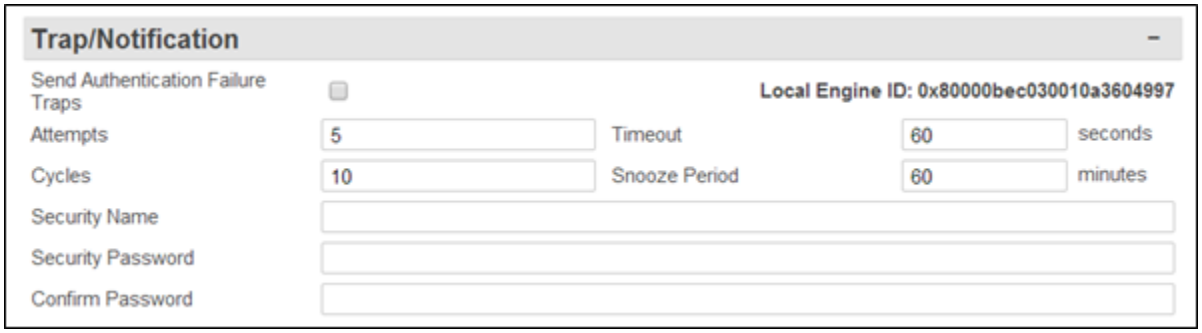
Security Name
This option is for inputting the authentication name for SNMPv3 operations and the field has a maximum Length 31 characters.

Security Password
This option is for inputting the authentication password for SNMPv3 operations. This field is required to be set to a minimum of 8 characters and 31 characters maximum.

Trap/Notification

These options are used to configure whether to send authentication failure traps and notification settings.

» Note: SNMP traps are *not* a guaranteed means of delivering notifications. Traps are a one-way IP network datagram and the device receiving traps does not acknowledge them. Therefore, if the trap does not reach its intended destination for whatever reason, the sending device has no way of recognizing this and resending the trap. To receive acknowledgments use SNMP Informs, available in SNMPv2 and SNMPv3.



Authentication Failure Traps
This is an ON/OFF checkbox to enable the sending of authentication traps. These are notifications of invalid community name usage in SNMP operations. The default setting is OFF (unchecked).

Attempts
This option sets the number of attempts (1 to 65535) of sending a notification (inform) per cycle (that is, the initial attempt + retries). If this is 0 then the unit will continue attempts infinitely. The default setting is 5.

Timeout
This field sets the number of seconds (3 to 60) between two attempts to send an SNMP inform in the same cycle. The default setting is 60.

Cycles
This field sets the maximum number of cycles (0 to 60) to try per notification action, where one notification action corresponds to one "inform" keyword in an action list for an event. A cycle is a set of notification attempts delimited by a successful action delivery or snooze period. The default setting is 10.

Snooze Period
This option sets the time in minutes (1 to 1440) between two SNMP notification cycles for any one notification action. That is, if you have two events generate informs, each inform will have its own timeouts for retries and cycles, and its own snooze period. The default setting is 60.

Security Name
This option is for inputting the authentication name for SNMPv3 operations and the field has a maximum Length 31 characters.

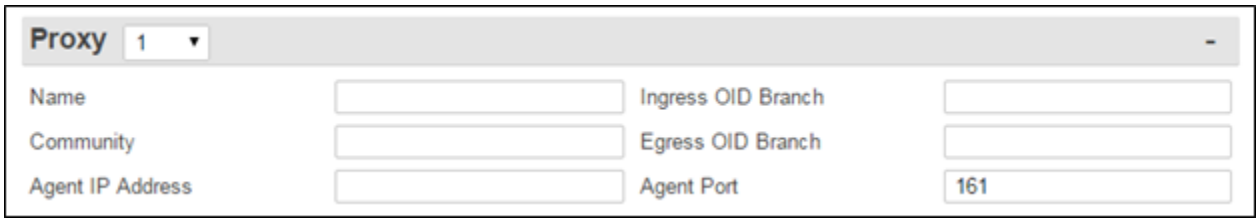
Security Password / Confirm Password
This option is for inputting the authentication password for SNMPv3 operations. This field is required to be set to a minimum of 8 characters and 31 characters maximum.

Proxy

SNMP Proxy means that the SiteBoss will proxy SNMP PDUs to another agent. In other words, the unit responds to inbound SNMP PDUs on behalf of another agent. This is different from IP routing in that the differentiator is at layer 7 instead of layer 3 or 4; the differentiator is the ingress SNMP OID branch instead of the IP address or UDP port.

This facilitates a user to use the unit as the interchange between remote devices via SNMP where routing or port forwarding is not an option.

The proxied agent will see the inbound SNMP PDU as SNMP version 1, and it will bear the community that is configured for the proxy entry (not the community that the user uses). The security configuration that the unit uses will be that which agrees with the unit, not with the proxied device. That is, SNMP v1/2 community or SNMPv3 security parameters which the user uses in constructing the SNMP query at their end must agree with the unit, not with the proxied device. Also, the proxied agent will see the PDU arrive from one of the unit's IP addresses, not from the user's IP address.



Proxy
This is a drop-down box to configure up to eight proxy entries.

Name
This is a text field to name the Proxy. The maximum number of characters is 30.

Community
Use this field to set the community which the device to proxy expects.

Agent IP Address
This field sets the IP address of the device to proxy.

Ingress OID Branch
This is the OID branch to be remapped to egress OID branch to trigger the proxy function. If blank (or the same as the egress OID branch) then the egress OID branch is proxied without remapping. If an ingress OID branch is configured then the ingress OID branch is remapped to the egress OID branch during proxy in order to facilitate proxying multiple like OID branches among multiple devices.

Since the ingress OID branch differentiates what device gets proxied, all non-blank ingress OID branches must be unique among each other.

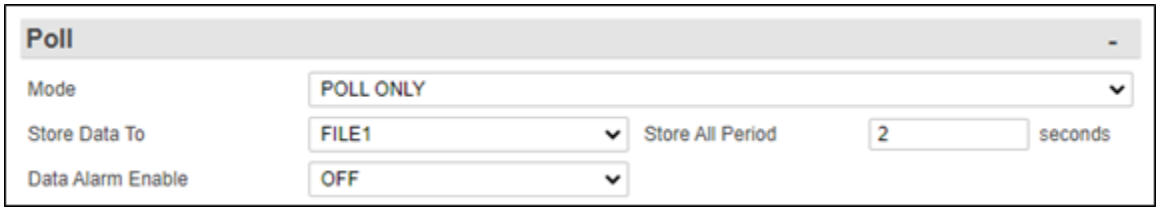
Egress OID Branch
Use this field to set the Egress OID. This should cover the device to proxy. A blank egress OID branch in the proxy entry disables the proxy entry. A non-blank egress OID branch enables the proxy entry.

Agent Port
This is the UDP port on which the device to proxy listens. (Not the port on which the unit listens.)

Poll

SNMP Polling is a feature used by an Asentria product to interrogate other SNMP capable devices and the information received can be buffered on the SiteBoss. Buffering the polled responses limits the need for frequent SNMP interrogation from the NOC and allows for continued buffering of data during a site service disruption.

For more information refer to the SNMP Operations Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support.



Mode
This is a drop-down menu to choose between OFF, POLL ONLY (just make the results available to view) and POLL BUFFER which stores the results in the file designated in the next menu option.

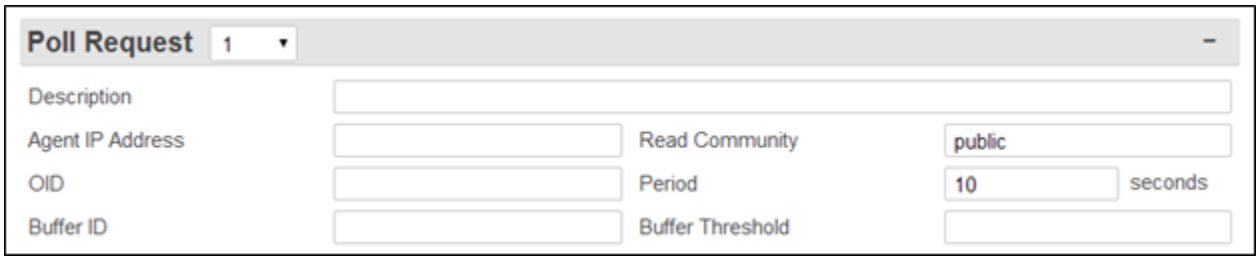
Store Data To
This option toggles through the available file options on the SiteBoss. The default is to FILE1.

Store All Period
If this field is set to a non-zero value then this time period (in seconds) will poll all configured SNMP Poll requests and buffer all values regardless of threshold.

Data Alarm Enable
This is and ON/OFF setting to enable/disable data alarming for SNMP polling records. The default setting is OFF.

Poll Request

Up to 64 individual SNMP Polling requests can be configured.



Poll Request
This drop-down box in the grey separation bar is used to select the settings fields for any of the 64 individual possible Polling Requests.

Description
This field is for entering a user-identifiable description to the SNMP Polling Request. This serves only to more easily identify individual requests on the SiteBoss' menus. The maximum length is 64 characters.

Agent IP Address
Input the Agent IP address or hostname for this request (maximum Length 64 characters).

{{header-settingsIRead Community
Enter the SNMP read community for this request. The default is public (maximum length for each is 32 characters).

OID
Enter the SNMP object identifier to be polled (maximum Length 64 characters).

Period (seconds)
This option configures the amount of time between SNMP requests to the agent, measured in seconds. Values are between 1 and 255 (defaults to 10).

Buffer ID
A textual field that is part of the record containing the telemetry result.

Buffer Threshold
This selection controls when new data is stored upon a successful telemetry request. The data stored depends on how the Buffer Threshold field is set:

- If the field is left blank then the telemetry is always stored.
- If set to "any difference" then the telemetry is stored only if it is different from the last value stored.
- If set to an integer (for example: 3) then it is treated as a hysteresis value (the span plus or minus the last stored value). This means that if the new telemetry does not exceed the threshold (either + or -) beyond the last stored value, then the new telemetry is not stored.
- If set to a floating point number (for example: 3.1) then it is treated as a hysteresis value for SNMP OCTET STRING types where the value looks like a floating point number. This means that if the last stored value is NOT a floating point number then the unit will ignore the threshold and store the new telemetry.

Trap Capture Settings

The SiteBoss can receive, buffer and forward SNMPv1 traps and SNMPv2c inform-requests (informs). Each notification can be subjected to data event evaluation, stored in the Event Log, and delivered via normal Event Log delivery.

When SNMP Trap Capture is enabled, the SiteBoss listens on port 162 for notifications. Those over 1024 bytes are ignored. The unit will respond to informs as soon as they arrive regardless of the content of the inform.

Refer to the SNMP Operations Feature Guide on the Asentria Product Information Portal for a detailed explanation of SNMP Trap Capture or contact Asentria Technical Support.

Enable

This is an ON/OFF checkbox to enable the capturing of SNMPv1 traps and SNMPv2c inform-requests (informs). The default setting is OFF (unchecked).

Store Collected Traps In

This is a drop-down menu containing all available data files in which the collected traps/informs could be stored. The default setting is FILE1.

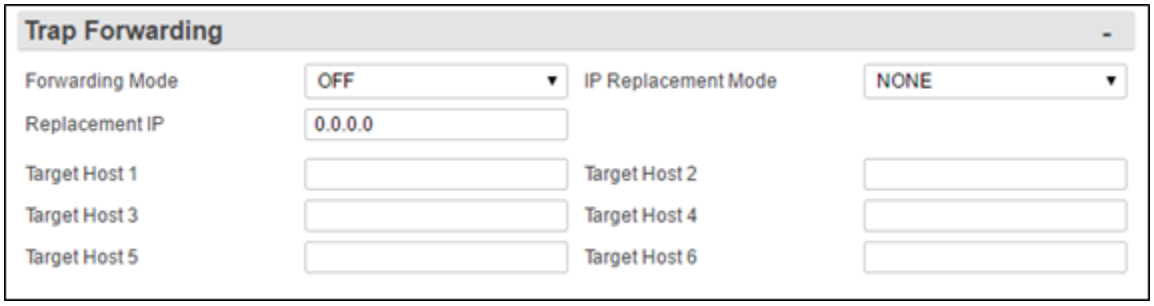
Trap Forwarding

The SiteBoss can receive, buffer and forward SNMPv1 traps and SNMPv2c inform-requests (informs). Each notification can be subjected to data event evaluation, stored in the Event Log, and delivered via normal Event Log delivery.

When SNMP Trap Capture is enabled, the SiteBoss listens on port 162 for notifications; those over 1024 bytes are ignored. The unit will respond to informs as soon as they arrive regardless of the content of the inform.

Refer to the SNMP Operations Feature Guide on the Asentria Product Information Portal for a

detailed explanation of SNMP Trap Capture or contact Asentria Technical Support.



Forwarding Mode
This drop-down box toggles between OFF and QUEUE. Off means do not forward. QUEUE will listen for a trap and then resend it to specified targets.

IP Replacement Mode
This toggles between NONE, IMPLICIT and EXPLICIT. When set to NONE, the IP address reflected in the forwarded trap is that of the original source device. The IMPLICIT setting will replace the SNMPv1 trap?s agent address field to the ETH1 interface address of the unit. EXPLICIT will replace the field with an explicit address defined in the Replacement IP field.

This functionality only works with SNMPv1 traps. Informs will be forwarded however the source IP will always transmit with the IP Address of the Ethernet Interface of the sending device.

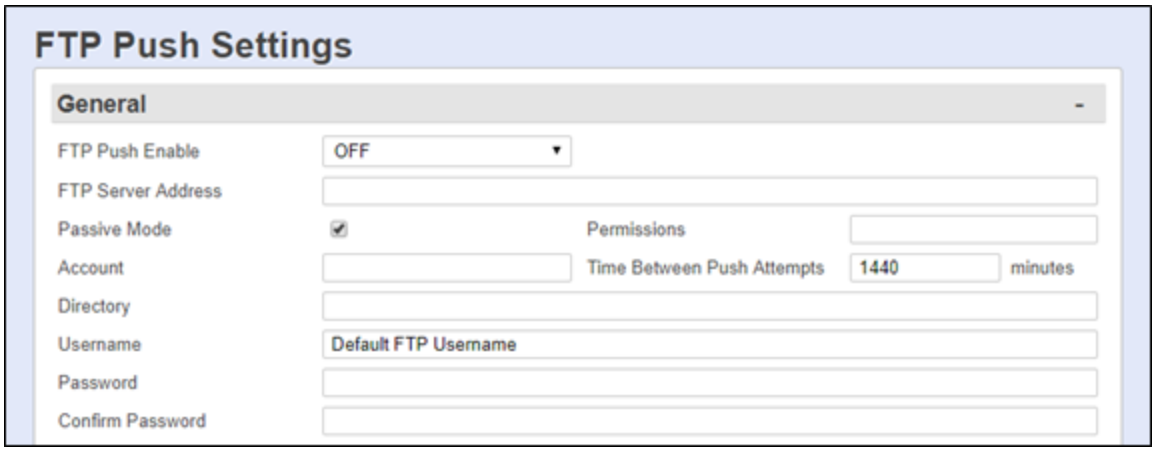
Replacement IP
This field is used to set a replacement IP address if you wish to replace the SNMPv1 trap?s agent address field to a specific address in the forwarded trap. The IP Replacement Mode must be set to EXPLICIT for this field to be used. The Default setting is 0.0.0.0.

Target Host n
These fields are used to input the SNMP manager(s) to define where the trap is being forwarded to.

FTP Push

This menu is used to configure automatic FTP pushes of buffered data.

» Note: This functionality is currently not on the S550A. Discuss with your sales reprehensive if FTP Push is required.



FTP Push General

FTP Push Enable
This is a drop-down menu to choose between OFF, REGULAR(FTP), and SECURE(SFTP). The default setting is OFF.

FTP Server Address
This field is used to set this field as the IP address or host name of the FTP server to push to (maximum length 64 characters).

Passive Mode
This is a checkbox to set the FTP Mode as Active or Passive. The default is checked (Passive).

SFTP Port
Use this option to set the SFTP Port. The default is 22.

Permissions
This field is used to set the permissions on the pushed file. Permissions are usable for both FTP and SFTP to the extent allowed by the server. If blank then no permissions change is attempted. The default is blank.

Account
This field is a third login option used only on some FTP servers. Consult your network administrator to see if this is necessary (maximum length 126 characters).

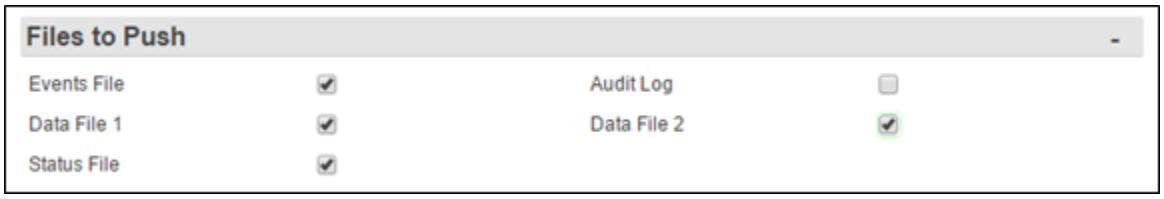
Time Between Push Attempts
This field sets the number of minutes (1 to 9999) between FTP push attempts. The default setting is 1440 minutes.

Directory
The Directory is the path used to transfer the file(s). The file(s) is transferred to the root login directory if this option is left blank (maximum length 253 characters).

Username / Password / Confirm Password
These options set the login credentials that are able to access the remote FTP server. The

maximum length Username is 126 characters and maximum length Password is 31 characters.

Files to Push

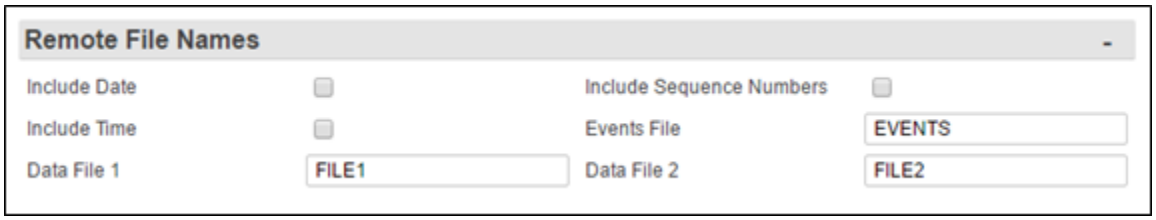


Each available file in the SiteBoss is listed with a checkbox to select which files are to be pushed. The default setting for all is checked (file to be pushed), except for Audit Log, which is unchecked (not pushed).

Remote File Names

These fields are used to configure options where you can give each file a name, other than the default name, and/or prepend a date, time, and unique sequence # to the file name. The number of Data File options will correspond to the number of serial ports on your unit, plus the Events File.

File names are restricted to alphanumeric characters and the following punctuation: dash, dot, underscore and tilde. Note that leading and trailing blank space is not allowed.



Include Date / Time

These are ON/OFF checkboxes to enable the addition of the file transfer date and/or time to the beginning of the name of each transferred file of data. The default settings are OFF (unchecked).

Include Sequence Numbers

This is an ON/OFF checkbox to enable the addition of a unique sequence number to the beginning of the name of each transferred file of data. This ensures that no two transfers will have the same file name. The default setting is OFF(unchecked).

Data File n / Events File

These fields are text-entry fields to configure the name each data file will have on the remote server (not including any date, time, or sequence numbers).

PPP

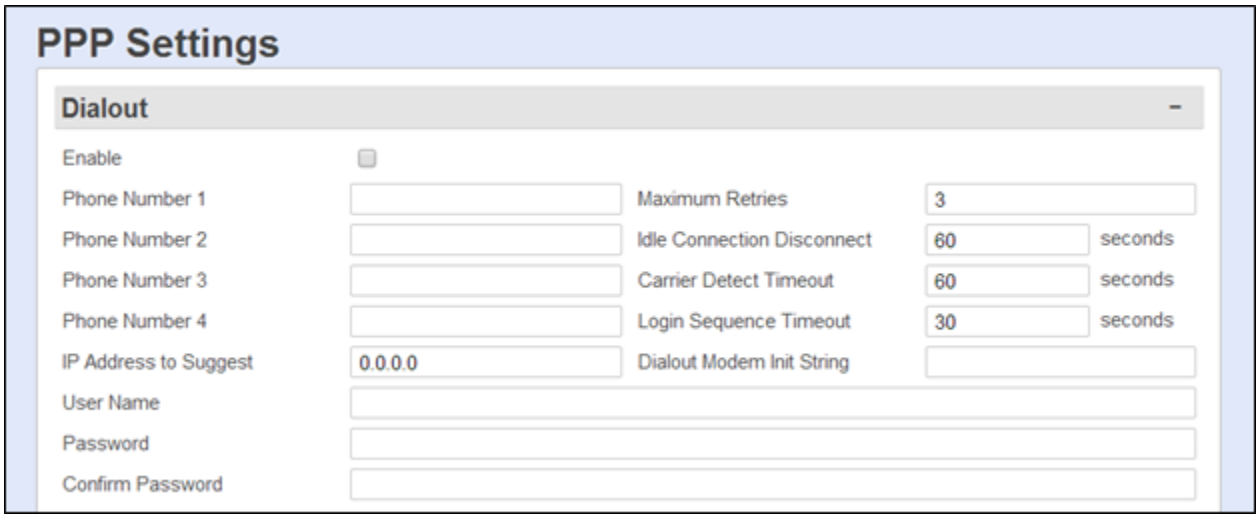
This menu option is used for configuring settings for the internal dialup, serial, POTS modem.

See the Dialup Modem Feature Guide on the Asentria Information Portal for more information.

» Note: This functionality is currently not on the S550A. Discuss with your sales reprehensive if a POTS dial up modem is needed.

Dialout

This menu is used to configure settings pertaining to making outbound PPP network connections for a serial dialup POTS modem. The settings fields will be present even if a modem is not installed, but in that case, changing the settings will have no functional effect on the unit.



Enabled

This is an ON/OFF checkbox to enable PPP dialout. The default setting is OFF (unchecked).

Phone Number n

These fields set the phone number(s) of the PPP host the SiteBoss is to dial into (maximum length 48 characters each). If the connection fails the SiteBoss will try the next phone numbers entered.

IP Address to Suggest

This field sets an IP to try to acquire, if defined. The default setting is 0.0.0.0.

User Name / Password

Use these fields to set the login credentials that are used to log into the PPP host (maximum length for each is 64 characters).

Maximum Retries

This field defines the maximum number of times to retry a failed connection for all phone numbers present. The default setting is 3.

Idle Connection Disconnect (seconds)

This field sets the number of seconds to wait before disconnecting an idle connection. A setting of 0 means the unit does not disconnect due to an idle connection. The default setting

is 60 seconds.

Carrier Detect Timeout (seconds)
This field sets the standard login timeouts, from 0 to 65535 seconds. The default setting is 60 seconds.

Login Sequence Timeout (seconds)
This field sets the standard login timeouts, from 0 to 65535 seconds. The default setting is 30 seconds.

Dialout Modem Init String
This field sets the modem initialization string (maximum length 48 characters).

Hosting

This menu is for configuring settings for hosting a PPP connection on the POTS dialup modem.

Enable
This is an ON/OFF checkbox to enable inbound PPP connection hosting. The default setting is OFF (unchecked).

Idle Connection Disconnect (sec)
This field sets the number of seconds (0 to 65535) to wait before disconnecting an idle connection. A setting of 0 means the unit does not disconnect due to an idle connection. The default setting is 60 seconds.

Local (Device) IP Address
This option sets the IP address of the SiteBoss for the PPP session. The default is 192.168.105.1

Remote (Caller) IP Address
This field sets the IP address of the calling device for the PPP session. The default is 192.168.105.2.

Route Test

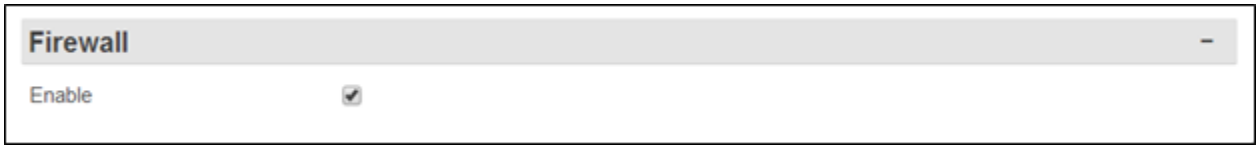
This menu allows you to configure up to three IP addresses to ping on a regular basis. If any of the configured addresses are up then the unit will assume Ethernet is a reliable way of sending SNMP traps. If all configured addresses are down then the unit will fall back to PPP dialout in order to maintain reliable network connectivity for sending SNMP traps.

Route Test Enable
This is an ON/OFF checkbox to enable route testing. The default setting is OFF (unchecked).

Duration Between Tests
This field sets the number of minutes (0 to 65535) to wait between each round of testing. The default setting is 10 minutes.

IP Address n
These fields set the hostnames or IP addresses to ping for the test.

Firewall



Firewall
This is an ON/OFF checkbox to enable or disable the PPP Modem firewall. This should be disabled if attempting to communicate with the unit from an outside device via a PPP connection. The default is ON (checked).

VPN

The following describes the menu options for configuring VPN Settings. A Virtual Private Network (VPN) is a network that is tunneled (the virtual part), typically across a public network, and secured (the private part), typically with IPsec or SSL. There is more information on SSL_VPN_Feature_Guide on the Asentria Product Information Portal or contact Asentria Technical Support.

The Asentria unit can be configured with up to 2 VPNs. Although the unit supports multiple VPN configurations, only 1 VPN can be operational at any one time.

VPN Settings
There are two separate VPN Settings options that can be configured. Select which VPN to configure using the drop-down box in the upper grey area.

VPN General

Mode

Mode drop-down box allows a selection between OFF, SSL CLIENT, and SSL SERVER to specify the VPN mode. The default setting is OFF.

Start Mode

The Start Mode toggles between MANUAL, AUTO-PASSIVE and AUTO-ACTIVE. The default is MANUAL.

- MANUAL means the user starts the VPN, it does not start automatically.
- AUTO-PASSIVE means that the unit listens for a VPN connection when the unit starts.
- AUTO-ACTIVE means that the unit starts connecting to a VPN peer when the unit starts.

Description

This is a user-defined string to server as a description for the tunnel. It has no functional impact.

Remote Host

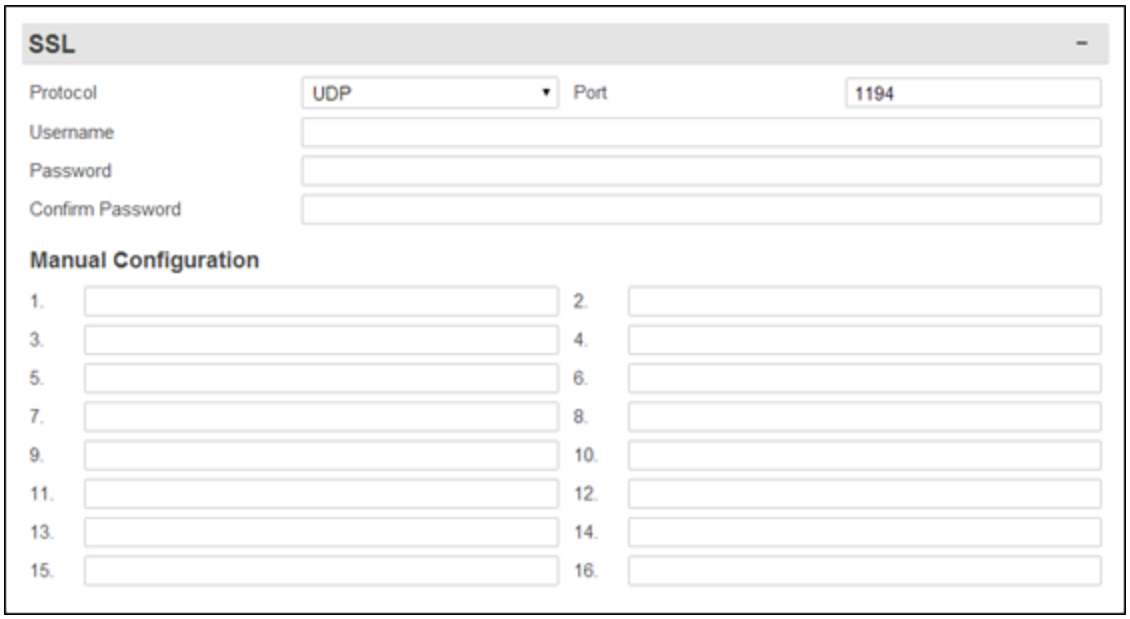
This is the IP address of the VPN peer on the opposite side of the tunnel to which the tunnel is bound.

Public Interface

This field sets the public interface to which the unit's side of the tunnel is bound. The drop-down options are ANY, ETH1, ETH2, PPPP, WIRELESS and DSL. The default is ANY.

SSL

Use this menu for configuring the settings if the Mode is SSL Client or SSL Server.



Protocol
This is a drop-down menu to choose between UDP and TCP to set the protocol SSL VPN uses to carry VPN traffic. The default setting is UDP.

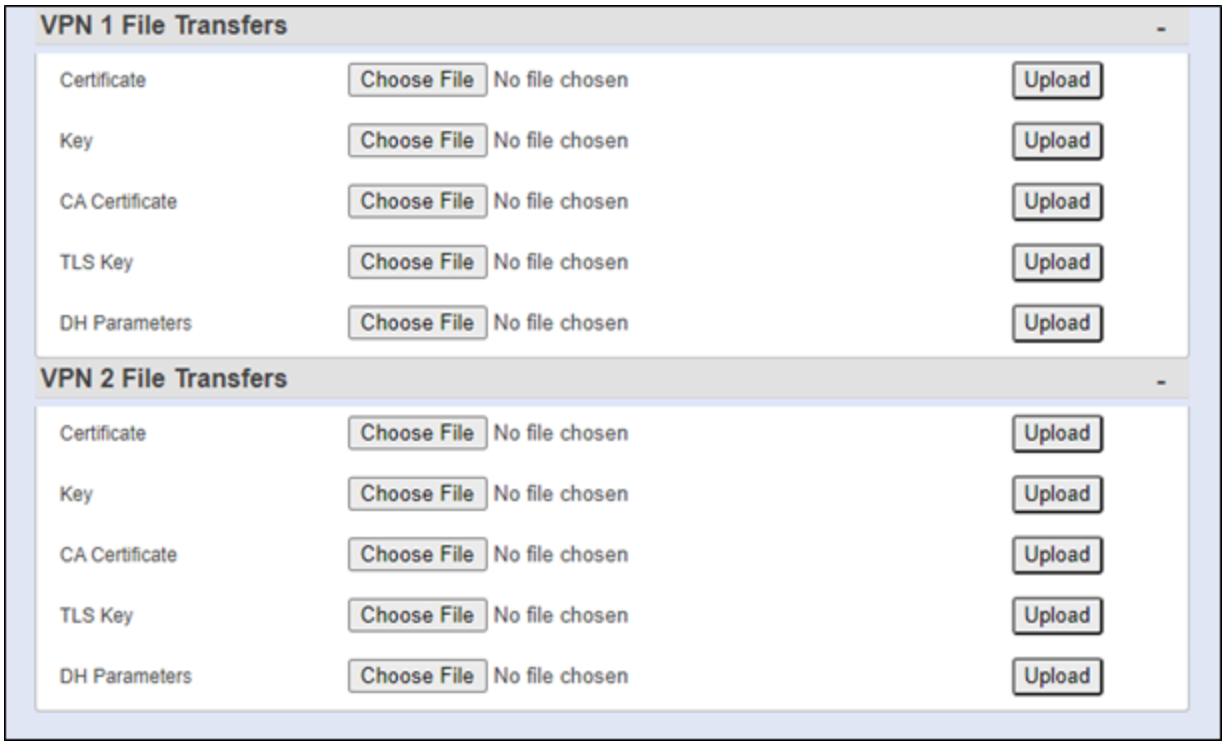
Port
This field is for setting what port (TCP or UDP, as determined by the SSL Protocol) the VPN uses. The default setting is 1194.

Username / Password / Confirm Password
These fields set the username and password that a VPN in SSL CLIENT mode uses when it connects to an OpenVPN server. If the username is blank then the username "u<*serial number*>" will be used. For example, "u550009999" is the username the unit sends to the OpenVPN server if this setting is blank and the SSL Password setting is not blank. The Username and Password add an extra layer of authentication to fulfill in order for the VPN to connect. Note: the OpenVPN server must be configured appropriately for this.

Manual Configuration
These fields are used to set up to 16 manual configuration items for OpenVPN, when the VPN mode is either SSL Client or SSL Server. Any configuration items you need which are not automatically handled for you by the unit (such as SSL port, SSL password, certificates, etc.) should be configured here.

VPN *n* File Transfers

The unit uses certificate based SSL/TLS security to authenticate the server (and the server uses the same thing to authenticate the client). This section is used to load certificate and key files onto the SiteBoss. The unit cannot generate its own SSL authentication key/certificate. These options will load the files needed by your VPN onto the unit.



Certificate
Use the Choose File button to select the client or server certificate text file (client.crt) and then click the Upload button to load it onto the SiteBoss.

Key
Use the Choose File button to select the key file (client.key) and then click the Upload button to load it onto the SiteBoss.

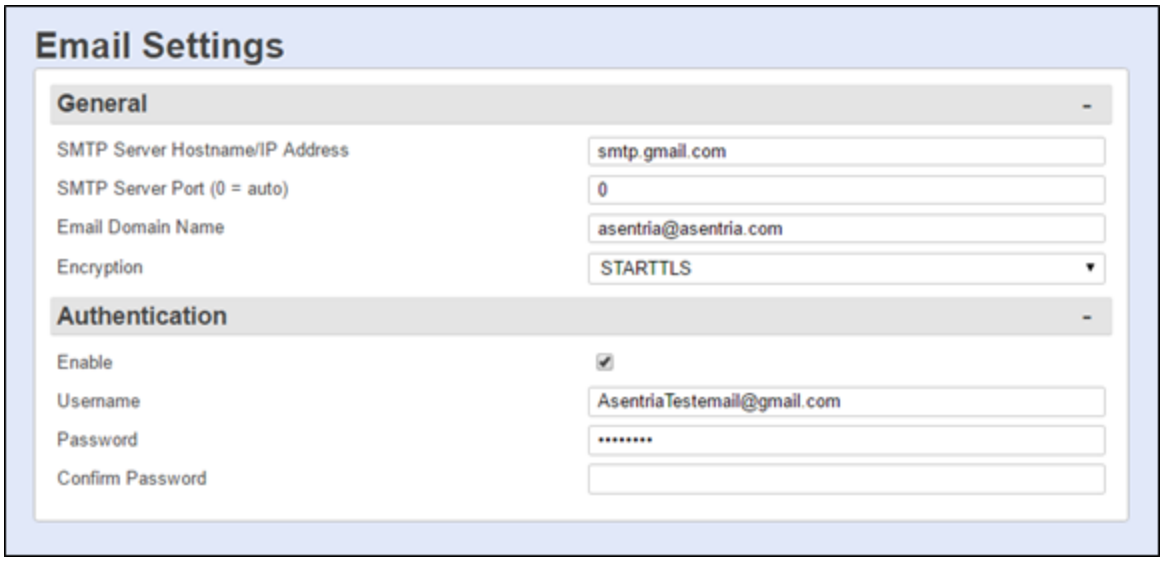
CA Certificate
Use the Choose File button to select the CA certificate text file (ca.crt) and then click the Upload button to load it onto the SiteBoss.

TLS Key
Use this option to load the TLS Authority key. If the server uses this, then the unit must use this too. Use the Choose File button to select the file and then click the Upload button to load it onto the SiteBoss.

DH Parameters
Use the Choose File button to select the DH1 Parameters text file, if this functionality is being used on your VPN, and then click the Upload button to load it onto the SiteBoss.

Email

The Email settings menu is used to configure the SMTP server address, Email domain name and authentication parameters. Additional information and examples are provided on the Email Feature Guide on the Asentria Information Portal or contact Asentria Technical Support for assistance.



General

SMTP Server Hostname/IP Address
Enter the hostname or IP address of the outbound mail server (Maximum length 64 characters).

SMTP Server Port
(0 = auto) This field sets the port to use for the connection to the SMTP server. A value of 0 means the port is automatically selected by the system. Default value is 0.

Email Domain Name
This field allows the user to adjust the "From:" address. If domain = aaaaa.bbb (a valid domain name with no @ symbol), then the unit sends as the From: address <site id>@aaaaa.bbb. If domain = @aaaaa.bbb (a valid domain name with an @ symbol as the first character), then the unit sends as the From: address <site id>@aaaaa.bbb. If domain = xxxx@aaaaa.bbb (a valid email address complete with @ symbol) then the unit sends as the From: address xxxx@aaaaa.bbb. Maximum length is 48 characters.

Encryption
Use the drop down box to select the encryption method. The choices are OFF, STARTTLS, and TLS. Most servers support STARTTLS; use the TLS setting for servers that don't. The default value is OFF.

Authentication

These options are used to configure the credentials that may be required by your server for SMTP authentication. Some SMTP servers require an authentication to relay Emails.

Authentication Enabled
This is an ON/OFF checkbox to enable Email authentication. The default setting is OFF (unchecked).

Username / Password / Confirm Password
Enter the login credentials as required (maximum length for each is 48 characters).

Routing

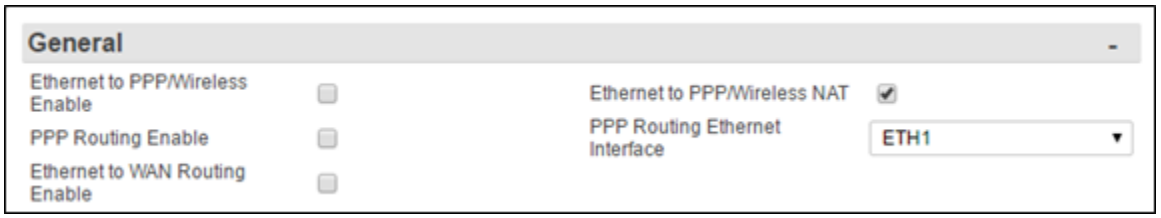
The following is a top-level overview of the SiteBoss' routing settings. For more detailed configuration and use instructions for all of these please refer to the IP Routing and Restrictions Feature Guide on the Asentria Product Information Portal.

Routing Settings
At the top of the Routing page is a drop down menu to toggle between Basic Routing and Advanced Routing options.

Basic Routing

Routing General

- Ethernet to PPP/Wireless Enable: When selected allows network traffic that originates from LAN connected to ETH1 or ETH2.
- PPP Routing Enable: When selected allows network traffic that originates from WAN connected to PPP to LAN
- If you want to establish connections both ways, you must select both settings.
- If you have port forwarding rules for PPP, you should not use either setting



Ethernet to PPP/Wireless Enable
Ethernet to Wireless Settings enable the SiteBoss to forward IP frames originating on Ethernet that are not IP-addressed to the unit as well as forward IP frames received on a wireless interface that are associated with forwarded frames that originated on Ethernet.

This is an ON/OFF checkbox to enable Ethernet to PPP/Wireless routing. The default setting is OFF (unchecked).

Ethernet to PPP/Wireless NAT
Ethernet to PPP/Wireless NAT is an ON/OFF checkbox to enable network address translation on the forwarded frames. Without NAT, a server on PPP would receive a forwarded frame that is IP-addressed according to the network on the Ethernet interface. The default setting is ON

(checked).

PPP Routing Enable
This is an ON/OFF checkbox to enable PPP to Ethernet routing. The default setting is OFF (unchecked). This feature allows forwarding IP frames originating on PPP that are not IP-addressed to the unit, as well as forwarding IP frames received on any Ethernet or VLAN interface that are associated with forwarded frames that originated on PPP.

PPP Routing Ethernet Interface
This is a drop-down menu to choose between ETH1, ETH2, ETHEXPAN, or any of the six VLAN interfaces on each Ethernet port, to indicate which interface to use for the PPP connection. The default setting is ETH1.

Ethernet to WAN Routing Enable
The feature allows port ETH2 to operate as a WAN port in the sense that it routes and NATs traffic arriving on ETH1, which is not destined for the unit, out ETH2.

This is an ON/OFF checkbox to enable ETH2 to WAN routing. The default setting is OFF (unchecked).

»Note: Just enabling ETH2 WAN Routing is not enough to route traffic out ETH2. You must also configure basic network settings for ETH2, as well as the default route or static routes. Configure the default router to be that of ETH2, or configure static routes for specific packet destinations of packets arriving on ETH1 to be routable via ETH2.

Static Route

Static routes are network routes that specify in a more or less permanent way (static) that traffic to a certain destination (destination host or destination network) gets routed out a certain interface or via a certain gateway.

Static routes give you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different IPv4 and up to eight IPv6 routes. You can specify a gateway or interface. If you specify a gateway only then the frame will be IP-addressed to the destination subnet and transmitted to the gateway, and the gateway needs to be either a local Ethernet subnet or the peer of a PPP connection (be it Wireless or Dialup Modem). If you specify an interface, regardless of specifying a gateway, then the frame will be transmitted out that interface.

» Note: Specifying that certain traffic goes out a PPP interface does not cause PPP to be raised when that traffic needs to leave the unit. If a PPP interface is down then any static routes that specify a PPP interface are effectively disabled.

» Note: Currently there is no support for Dialup Modem PPP and Wireless Modem PPP to be functional at the same time. The effect is that if you specify a static route with Wireless Modem PPP interface when the Dialup Modem PPP is up instead of the Wireless, then that traffic will go out the Dialup Modem PPP interface.

IPv4

Static Route
The drop-down box in the grey header bar is used to choose which of the eight possible Static Routes to configure.

Enable
This is an ON/OFF checkbox to enable the static route. The default setting is OFF (unchecked).

Interface
This is a drop-down menu providing the options from which to select any one of the interfaces available on this SiteBoss - NONE, ETH1, ETH2, ETH3, ETH1 VLAN 1, 2, 3, 4, 5, 6, ETH2 VLAN 1, 2, 3, 4, 5, 6, ETH3 VLAN 1, 2, 3, 4, 5, 6, ETH EXPAN, ETH-BRIDGE, POTS PPP, WIRELESS and SPPP (Serial PPP). The default setting is NONE.

You can specify a gateway or interface. If you specify a gateway only, then the frame will be IP-addressed to the destination subnet and transmitted to the gateway, and the gateway needs to be either a local Ethernet subnet or the peer of a PPP connection (be it wireless or PSTN). If you specify an interface, regardless of specifying a gateway, then the frame will be transmitted out that interface.

» Note: ETH3 is a SPF Expansion Card (Small Form-factor Pluggable transceiver) if installed.

Destination Network
Define the destination network notation, i.e., w.x.y.z/s, where s is the significant bits. The default is 0.0.0.0/0.

To configure a static ***host*** route specify a destination net with the significant bits set to 32. To configure a static ***network*** route specify a destination net with the significant bits set to a number less than 32.

Gateway
Enter the IP address of the gateway. The default setting is 0.0.0.0

IPv6

IPv6 Static Routes is currently supported only on interfaces ETH1, ETH2, ETH3 and ETHEXPANF. For Ipv6 the gateway is optional, but interface is required.

Static Route
The drop-down box in the grey header bar is used to choose which of the eight possible Static Routes to configure.

Enable
This is an ON/OFF checkbox to enable the specified static route. The default setting is OFF (unchecked).

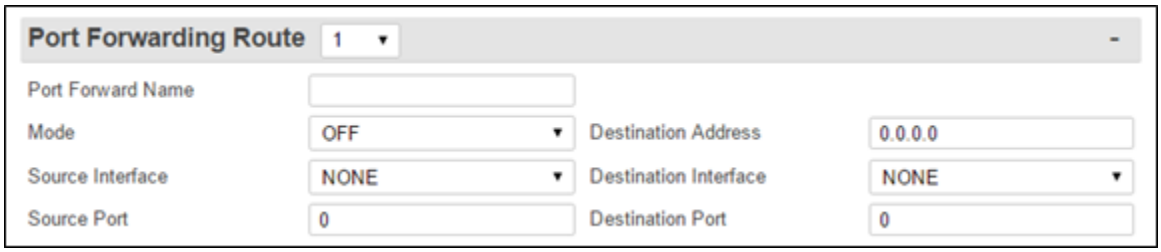
Interface
This is a drop-down menu providing the options from which to select any one of the interfaces available on this SiteBoss - NONE, ETH1, ETH2, ETH3, ETHERNET EXPANSION. An interface value other than NONE must be selected in order for the route to be applied. The default setting is NONE.

Destination Network
This field is used to designate the destination network in IPv6 network notation, i.e, 2001:1:2:3::2/64. The Default setting is blank.

Gateway
Enter the IP address of the gateway using a valid IPv6 address. The default setting is blank.

Port Forwarding

The Port Forwarding Settings are used for configuring the unit to accept UDP and TCP frames on an interface and route them, translating their IP addresses and UDP/TCP ports according to configuration to a different address on a different interface. Up to 32 individual routes can be configured. See the IP Routing and Restrictions Feature Guide for more additional instructions and examples for the Port Forwarding feature.



Port Forwarding Route
The drop-down box in the grey header section is used to choose which route is to be configured. There are 32 available routes.

Port Forward Name
This is a text field to name the Port Forward for ease in determining what is connected at that port. It has not functional affect. The maximum length is 23 characters.

Mode
Mode is a drop-down box to choose between OFF, TCP and UDP to select the protocol to be utilized. The default setting is OFF.

Destination Address

Set the IP address of the destination interface. The default setting is 0.0.0.0.

Source Interface
This option toggles between NONE, ETH1, ETH2, ETH3, ETHEXPAN, ETH-BRIDGE, ETH1 VLAN 1, 2, 3, 4, 5, 6, (E1V1- E1V6), ETH2 VLAN 1, 2, 3, 4, 5, 6, (E2V1-E2V6), ETH3 VLAN 1, 2, 3, 4, 5, 6, (E3V1-E3V6), Dialup Modem PPP (PPPP), Wireless Modem PPP (WIRELESS), Serial PPP (SPPP), or VPN. The default setting is NONE.

Destination Interface
The Destination Interface toggles between NONE, ETH1, ETH2, ETH3, ETHEXPAN, ETH-BRIDGE, ETH1 VLAN 1, 2, 3, 4, 5, 6, (E1V1- E1V6), ETH2 VLAN 1, 2, 3, 4, 5, 6, (E2V1-E2V6), ETH3 VLAN 1, 2, 3, 4, 5, 6, (E3V1-E3V6), Dialup Modem PPP (PPPP), Wireless Modem PPP (WIRELESS), Serial PPP (SPPP), or VPN. The default setting is NONE.

Source Port
Set the port on which the source interface communicates with the unit. Valid values are 0 to 65535. The default setting is 0.

Destination Port
Set the port on which the unit communicates with the destination interface. Valid values are 0 to 65535. The default setting is 0.

IPv6 to IPv4 Proxy

The IPv6 to IPv4 Proxy feature facilitates forwarding IPv6 packets to an IPv4 or IPv6 address. The proxy listens on the specified port and when a packet comes in it is routed to the destination. If the connection is TCP, two bidirectional streams are established and packets are transferred between them. Up to 8 proxies can be configured.

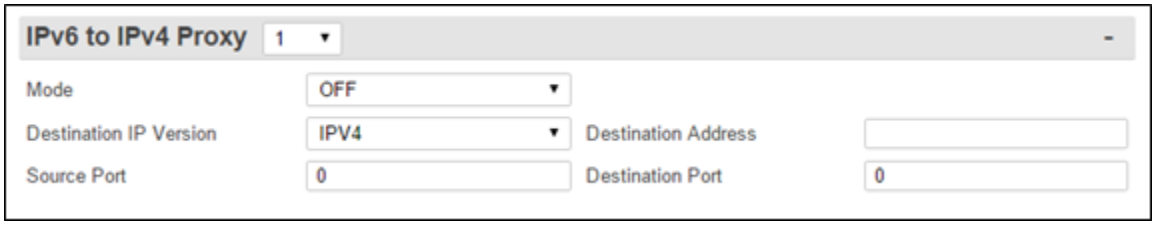
»When accessing the proxies via IPv6, please note the following:

There has been no success in accessing IPv6 proxies using Google Chrome. Only Firefox and IE10+

If your proxy device uses to https for the WebUI, the destination port of said proxy must be configured to Port 443, and you must use an "https://" prefix when entering your IPv6 address.

Similarly, if you are accessing a proxy device via http, Port 80, you will need to specify an "http://" prefix in your IPv6 initial address.

See the IPv6 to IPv4 Proxy Feature Guide on the Asentria Information Portal for additional information and an example configuration



IPv6 to IPv4 Proxy
This drop down box in the grey separation bar is used to select one of up to 8 IP Proxies that can be configured. Defaults to 1.

Mode
The Mode drop down box is used to select between the available options for this settings OFF, HTTP, HTTPS, SSH or TELNET. Defaults to OFF.

Destination IP Version
This drop down box is used to set the destination IP version, either IPv4 or IPv6. The default is IPv4

Source Port
The TCP port to listen for incoming packets. Note: this feature binds to the source port, so it MUST be an unused TCP port. Defaults to 0.

Destination Address
This text field is used to enter the destination IP. The default is blank.

Destination Port
This text field sets the destination port. The Default is 0.

NAT64

NAT64 is an IPv6 transition technology, allowing IPv6-only clients access to IPv4-only devices. This feature is available on the S550A and S360 only, and will not be on the routing page in the S550.

Enable
The options are OFF or ON. Default is OFF

IPv4 Pool
IPv4 subnet that must be unique on the LAN. It is used internally by NAT64 process and is automatically given a /24 mask, so the last octet should be "0". The default is 192.168.255.0

Interface In
This drop down sets the network interface for the IPV6 incoming packets. The options are ETH1, ETH2, ETH-EXPANSION, ETH-BRIDGE, or WIRELESS. The default is ETH1

Interface Out
This drop down sets the network interface for the translated IPV4 packets. Options are ETH1, ETH2, ETH-EXPANSION, or ETH-BRIDGE. The default is ETH-EXPANSION

IPv6 Address
This field sets the IPv6 address for the NAT64 tunnel. It must be on the same subnet as the incoming interface.

IPv6 Prefix
This text field sets the prefix is used to reserve a portion of the IPv6 subnet for NAT64 routing. It must be an unused /96 prefix from the same subnet as the incoming interface.

Advanced Routing

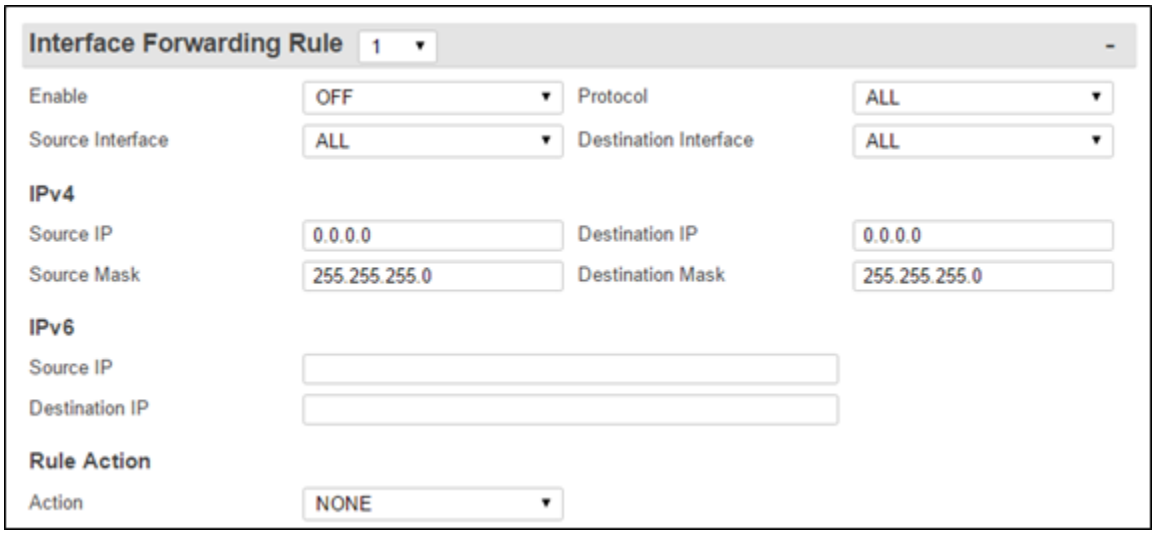
Toggle the drop down box at the top of the page to display the Advanced Routing Setting options.

Interface Forwarding Rule

The Interface Forwarding feature allows the user to control how packets are routed on a device with multiple network interfaces. Interface forwarding only applies to packets that are getting routed through the host device; not packets addressed to the host device (the IP restriction feature controls packets addressed to the host).

There are nine settings that together describe one rule. The rule is applied to an IP packet when it is being routed through the device. If it matches a rule then the unit applies that rule; otherwise the packet falls through to the next rule, and finally the default policy (which is always to DROP the packet). Up to twelve rules can be specified with the evaluation starting at the first enabled rule and continuing in order.

» Note: Interface Forwarding is an advanced routing feature that can affect network security. It can provide access to different areas of the network, thus there is a risk. This section of the manual provides direction for configuring this feature and assumes the user has full knowledge and understanding of the security concerns.



Interface Forwarding Rule

The drop down box is used to select one of the 12 possible rules that can be configured. Defaults to Rule 1.

Enable

A rule can be enabled for IPV4, IPV6 or both IPV6 and IPV4. If a rule set to OFF, it is ignored. The default is OFF.

Protocol
This drop down box is used to specify a protocol for this rule. Available options are ALL, TCP, UDP or ICMP. The default is ALL.

Source Interface
This drop down box is used to select from a list of possible network interfaces or ALL. The default is ALL.

Destination Interface
This drop down box is used to select from a list of possible network interfaces or ALL. The default is ALL.

IPv4

These Fields can be used to restrict incoming and outgoing packets by specifying IPv4 address or subnet.

Source IP
This field is used to set an IPv4 source address. This field can be used to restrict incoming packets by specifying an IPv4 address. The default is to 0.0.0.0, which specifies no restrictions.

Source Mask
This field sets the network mask for source IP address. These two settings can be used to restrict incoming packets. This setting is ignored if source IP is 0.0.0.0 (no restrictions).

Destination IP
IPv4 destination address. Can be used to restrict outgoing packets by specifying a destination IP address or subnet. Defaults to 0.0.0.0 -- no restrictions

Destination Mask
This field sets the network mask for destination IP. The setting will be ignored if destination IP is 0.0.0.0 (the default).

IPv6

Source IP
This text field sets the IPv6 source address. It can be used to restrict incoming packets by specifying an IPv6 address or prefix. If a prefix is not specified (e.g. 2001:2db:1:2:4:6::/96) /64 is used. The default is to blank, meaning no restrictions

Destination IP
IPv6 source address. Can be used to restrict incoming packets by specifying an IPv6 address or prefix. If a prefix is not specified (e.g. 2001:2db:1:2:4:6::/96) /64 is used Defaults to blank -- no restrictions

Rule Action

Action

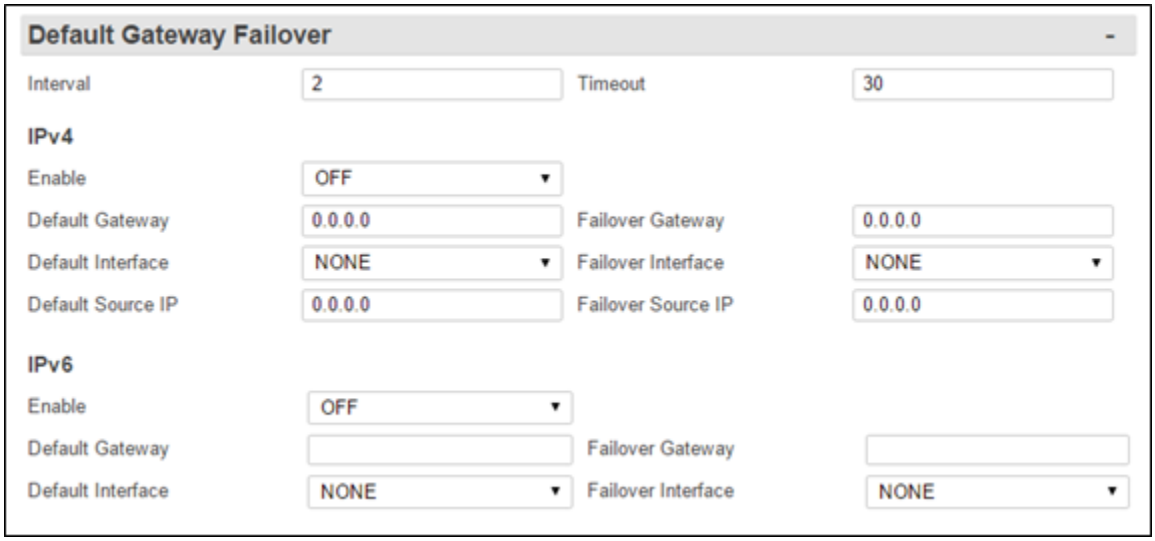
This drop down box is used to set the packet action if the rule is a match. The options are: NONE, ACCEPT, DROP or REJECT. If the option is none, the rule is ignored. The default is to NONE.

Default Gateway Failover

The Default Gateway Failover feature allows the user to specify the default gateway route and a failover route. The specified default gateway is monitored periodically. If it becomes unresponsive, the failover route is set as the default route. In that case, the default gateway is still monitored and, as soon as it becomes responsive, it is reset as the default route.

Note that when this feature is enabled, the default route set on the network page (net.default.router) is ignored.

Additional information on this feature is available on the Default Gateway Failover Feature Guide on the Asentria Information portal.



Interval

This text field is used to specify how often the default router should be checked for connectivity. The value can be from 2 to 120 seconds and defaults to 2 seconds.

Timeout

If the default router is unresponsive for this amount of time, in seconds, the failover route will be used. The value can be from 2 to 600 seconds and defaults to 30 seconds.

IPv4

Enable

The ON/OFF drop down box is used to enable or disable the feature. The default is OFF. When this feature is enabled, the default router on the network page (net.default.router) is ignored. When disabled, the unit goes back to using default router on the network page.

Default Gateway
This should be set to the IPv4 address of the default router. If the value is set to 0.0.0.0, the feature is disabled. The default is 0.0.0.0.

Failover Gateway
This field sets the IPv4 address of the failover router. If the value is 0.0.0.0, the feature is disabled. The default is 0.0.0.0.

Default Interface
This field sets the network interface to use. A list of possible interfaces is given in a drop down menu. The default is NONE.

Failover Interface
This field sets the network interface to use to reach the failover router. A list of possible interfaces is given in the drop down menu. The default is NONE.

Default Source IP
This is an optional setting meant to handle the case when an interface has multiple IPs. It will used by the system as a hint as to which IP address to select for a source address on outgoing packets. The default of 0.0.0.0 allows system to pick without user preference.

Failover Source IP
This is an optional setting meant to handle the case when an interface has multiple IPs. It will used by the system as a hint as to which IP address to select for a source address on outgoing packets. The default of 0.0.0.0 allows system to pick without user preference.

IPv6

Enable
This is an ON/OFF drop down box is used to enable or disable IPv6 for this feature. The defaults is disabled.

When this feature is enabled, the default router on the network page (net.default.router) is ignored. When disabled, the unit goes back to using default router on the network page.

Default Gateway
This should be set to the IPv6 address of the default router. If the value is empty, the feature is disabled.

Default Interface
This field sets the network interface to use. A list of possible interfaces is given in a drop down menu. The default is NONE.

Failover Gateway
The IPv6 address of the failover router. If the value is empty, the feature is disabled.

Failover Interface
This field sets the network interface to use to reach the failover router. A list of possible interfaces is given. If the value is NONE, the feature is disabled. The defaults is NONE.

Real-Time Sockets

Real-Time Sockets are used to collect data on TCP port 2201 from a serial port in real-time, while buffering data if the network connection goes down. Each file can be configured independently. Refer to the Telnet Feature Guide on the Asentria Product Information Portal for a detailed explanation of Real-Time Sockets or contact Asentria Technical Support.

The S550A does not have Real-Time Sockets capability.

File Setup

The File Setup drop-down box is used to select which File is being configured. The default is 1.

Mode

This is a drop-down box to choose the mode. The options are LISTEN, PUSH, and OFF. When set to LISTEN the option functions like traditional real-time sockets on TCP port 2201. When set to PUSH the unit tries to make a TCP connection on the TCP port specified at Push Port Number. As long as a connection exists, the unit sends all data in the specified file on the connection as data becomes available. The default setting is OFF.

Show Answer String on Connection

This is an ON/OFF checkbox to enable the prompt indicating successful connection to the Real-Time Socket (RTS) port. The default setting is ON (checked).

Require XON to Start Data Flow

This is an ON/OFF checkbox to enable the Xon/Xoff data flow control requirement. The default setting is OFF (unchecked).

Idle Connection Close Timer (Minutes)

This field sets the number of minutes (0 – 255) to wait before disconnecting an idle connection. A setting of 0 means the connection will never automatically close. The default setting is 0.

Push Hostname/IP

Use this field to set the hostname or IP address of the server where the unit will push the data if the Mode is set to PUSH (maximum length is 64 characters).

Push Port Number

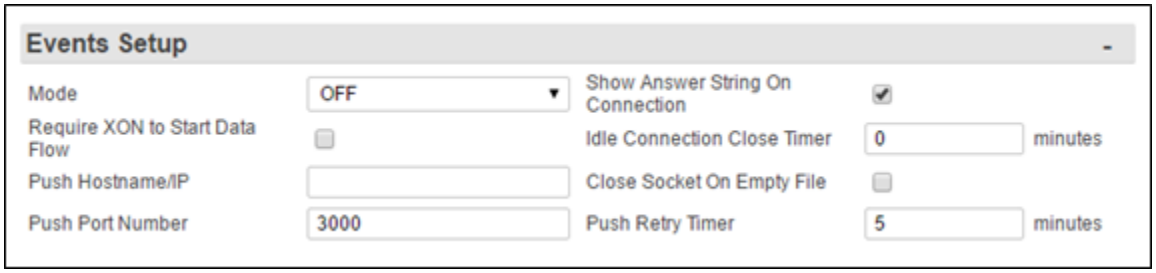
This option sets the TCP-port number that the RTS push should use. The default setting is port 3000.

Push Retry Timer
This option sets the number of minutes (1 to 255) to wait before retrying an RTS push that has previously failed. The default setting is 5 minutes.

Close Socket On Empty File
This is an ON/OFF checkbox to set whether or not the SiteBoss will automatically terminate the RTS connection when the file for this port has been emptied. The default setting is OFF (unchecked).

Event Setup

This menu configuration is to handle the Events Log information using the Real-Time Sockets functionality.



Mode
This is a drop-down box to choose the mode. The options are LISTEN, PUSH, and OFF. When set to LISTEN the option functions like traditional real-time sockets on TCP port 2201. When set to PUSH the unit tries to make a TCP connection on the TCP port specified at Push Port Number. As long as a connection exists, the unit sends all data in the specified file on the connection as data becomes available. The default setting is LISTEN.

Show Answer String On Connection
This is an ON/OFF checkbox to enable the prompt indicating successful connection to the Real-Time Socket (RTS) port. The default setting is ON (checked).

Require XON to Start Data Flow
This is an ON/OFF checkbox to enable the Xon/Xoff data flow control requirement. The default setting is OFF (unchecked).

Idle Connection Close Timer (Minutes)
This field sets the number of minutes (0 – 255) to wait before disconnecting an idle connection. A setting of 0 means the connection will never automatically close. The default setting is 0.

Push Hostname/IP
Use this field to set the hostname or IP address of the server where the unit will push the data if the Mode is set to PUSH (maximum length is 64 characters).

Close Socket On Empty File
This is an ON/OFF checkbox to set whether or not the SiteBoss will automatically terminate the RTS connection when the file for this port has been emptied. The default setting is OFF (unchecked).

Push Port Number
This option sets the TCP-port number that the RTS push should use. The default setting is port 3000.

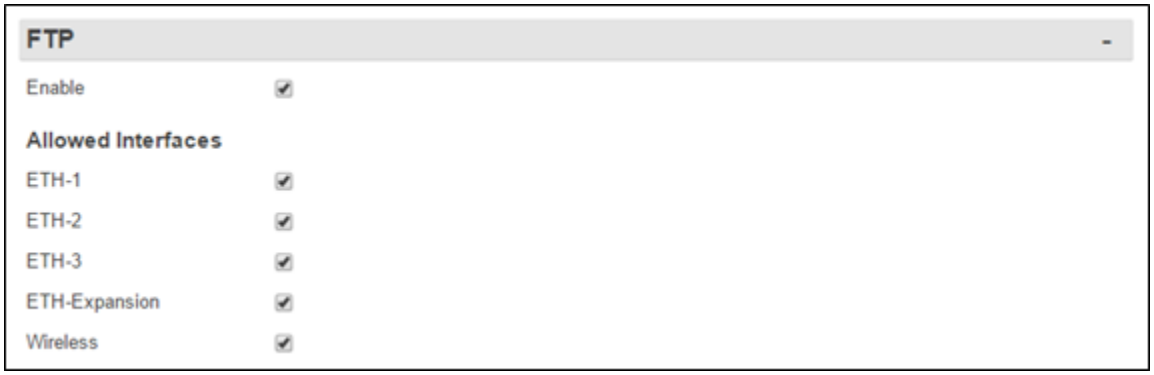
Push Retry Timer
This option sets the number of minutes (1 to 255) to wait before retrying an RTS push that has previously failed. The default setting is 5 minutes.

Servers

The Network Server Configuration feature currently applies to these services: FTP, SSH, Telnet, and Web. All of these services, when enabled, respond to requests on any active network interface. This is the default behavior. However, this feature allows the user to enable or disable which network interface(s) the service will "listen" on.

If a user makes changes to the network interfaces via a SSH, FTP, or Telnet session, the changes will not take effect until the session has ended. If the changes are made via a Web session, any Web interface changes will not take effect until the Web session has been closed.

FTP

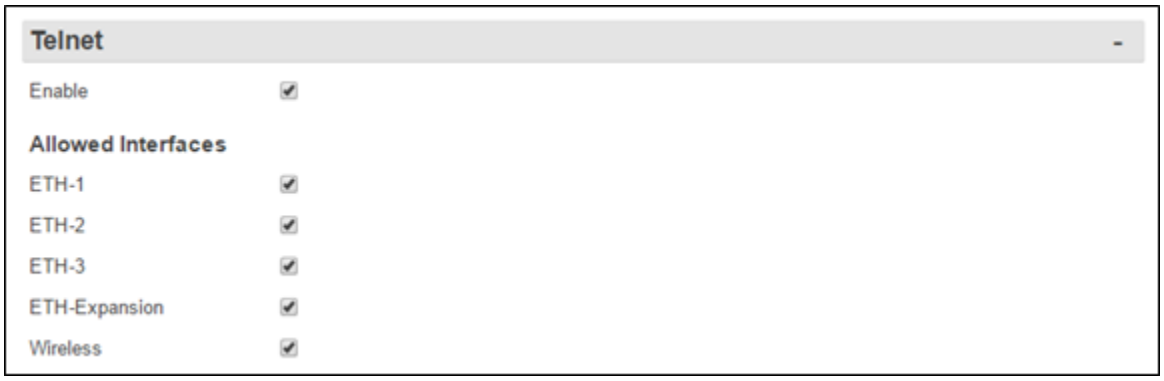


Enable
This checkbox will enable (checked) or disable (unchecked) the FTP server globally for all network interfaces. The default is checked, enabled.

» Note: Disabling the Server would also disable FTP Push.

Allowed Interfaces
These checkboxes allow (checked) or disable (unchecked) FTP functionality on the specified interface only.

Telnet



Enable
This checkbox will enable (checked) or disable (unchecked) access globally via Telnet for all network interfaces. The default is checked, enabled.

Allowed Interfaces
These checkboxes allow (checked) or disable (unchecked) Telnet functionality on the specified interface only.

Web

This section is used to enable and configure the Web Interface. If you disable the Interface via the Web controls the setting change will not take effect until all control sessions are terminated.

Enable
This is an ON/OFF toggle to enable or disable the SiteBoss' internal web server. The default setting is ON (checked).

Web Session Timeout
This field sets the number of minutes (0 to 65535 minutes) a web connection may remain idle before expiring. A setting of 0 means the connection will never automatically expire. The default setting is 30.

HTTP Connection Port
This option sets the TCP port through which an HTTP connection is made. Set to 0 to prevent access. The default setting is 80.

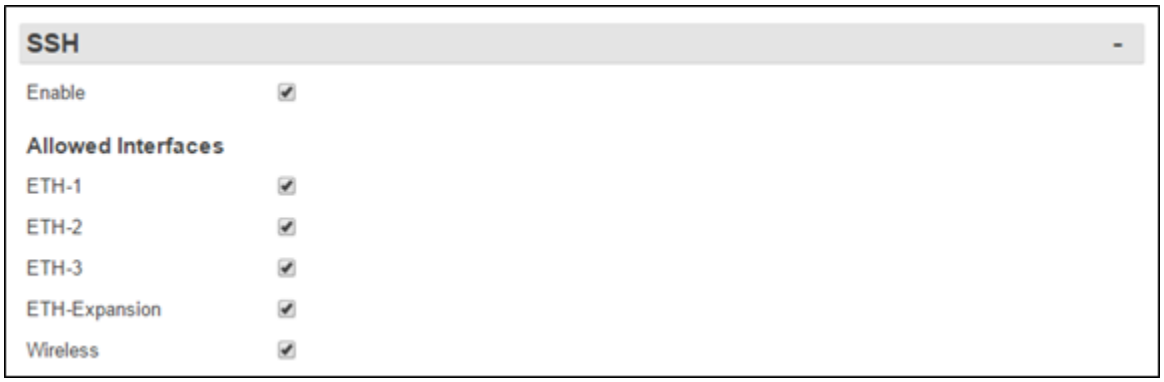
HTTPS Connection Port
This option is the TCP port through which an HTTPS connection is made. Set to 0 to prevent access. The default setting is 443.

TLS Version
This feature sets the TLS version. Options are TLSv1.1, and TLSv1.2. The Default is TLSv1.2

» Note: If using SSL, the SSL certificate will show "localhost" as the name, which may cause a certificate security warning to pop up, depending on the browser being used. The certificate may then be permanently accepted so the warning doesn't appear each time.

Allowed Interfaces
These checkboxes are used to Enable (checked) or Disable (unchecked) HTTP or HTTPS on the specified interface.

SSH



Enable
This checkbox will enable (checked) or disable (unchecked) access globally via SSH for all network interfaces. The default is checked, enabled.

Allowed Interfaces
These checkboxes allow (checked) or disable (unchecked) SSH functionality on the specified interface only.

SSH Advanced Options

Port
Use this option to set the port the server listens on for incoming connections, the default is 22

Session Timeout
This field sets an idle timeout, in minutes, for clients. If the server has not received any data from the client in the configured number of minutes, the client session is closed. The default is "0" which disables session timeouts.

»**Note**: When using the timeout option, the SSH client must also be configured to NOT send keepalive packets.

Cryptographic Options
Clicking the ?Show? button will display 3 groups of options: Ciphers, MACs, and Kex algorithms. If any options are selected in a group, then only those options will be used for client negotiations. If no options are selected, then all options in that group are used for client negotiation. The default is no options selected.

DNP3

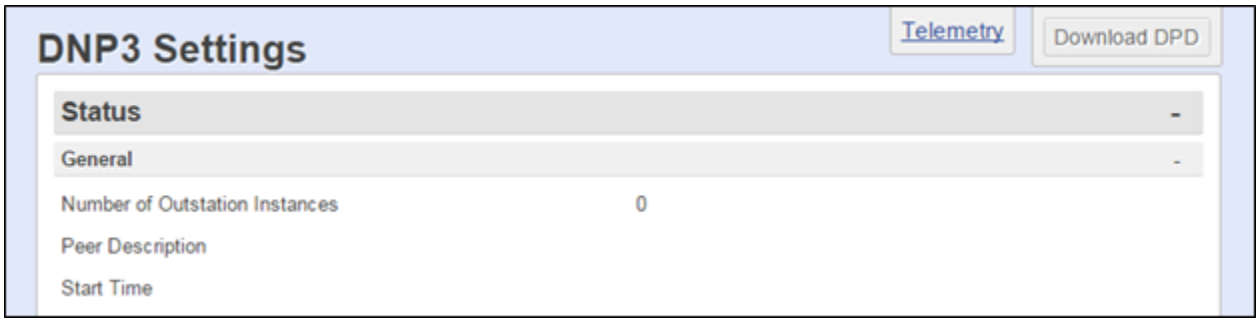
DNP3 is a remote telemetry automation protocol. Devices which support DNP3 are classified mainly as Master Stations or Outstations. A master polls the outstation (mainly for telemetry data) and performs automation tasks on the outstation (such as controlling relays). The outstation services requests from masters and sends (under certain circumstances) unsolicited messages to connected masters.

The SiteBoss:

- Supports DNP3 as an outstation conveyed via TCP only.
- Listens for TCP connections on port 20000 (by default). It is not a TCP dual end point; that is, it does not both listen for and initiate TCP connections to masters.
- Can support up to 5 concurrent master connections.
- Conveys sensor telemetry configured in the unit's Telemetry table.
- Conforms to DNP3 Level 1 implementation.

» **Note**: DNP3 events (which are elements of the DNP3 protocol) are completely independent of SiteBoss events (which have associated management and actions).

See the NP3 Feature Guide on the Asentria Information Portal for more information.



DNP3 Status

The Status Keys, except for Number of Outstation Instances, are all per-outstation status items. Despite the unit supporting multiple concurrent outstations, status keys can show only 1 outstation: these refer to the oldest outstation instance. That is, the outstation with the least recent time started.

DNP3 General

Number of Outstation Instances
This field is a count of running outstation instances.

Peer Description
This field is a description of the connected peer (the TCP socket endpoint of the master).

Start Time
This field displays when the outstation instance started.

Error Counters

Any of these items reflecting non-zero values indicates trouble. All these items being zero may indicate that, if any trouble exists, the trouble is not likely found in the processing of DNP3 traffic. These items only increment for as long as the outstation is running.

Error Counters			
RX Duplicate Fragments	0	RX Colliding Fragments	0
Solicited Confirms	0	Unsolicited Confirms	0
Object Parse Errors	0	Frame Parse Errors	0
RX Discarded Frames	0	RX Bad Frame Blocks	0
TX Unsolicited Retries	0	RX Unsupported Frames	0

RX Duplicate Fragments
This is a count of duplicate fragments received.

RX Colliding Fragments
This is a count of colliding fragments received.

Solicited Confirms
This is a count of solicited response confirmation failures.

'Unsolicited Confirms
This is a count of unsolicited response confirmation failures.

Object Parse Errors
This is a count of received data object parse errors.

Frame Parse Errors
This is a count of received frame parse errors.

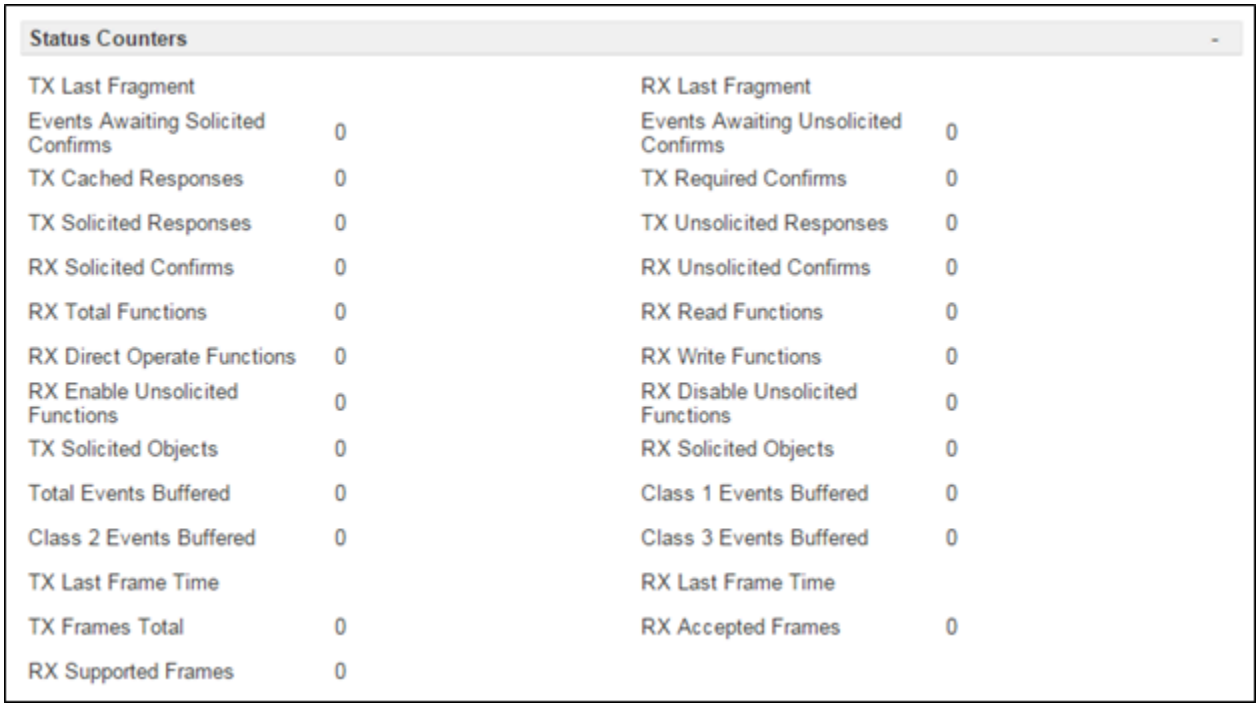
RX Discarded Frames
This is a count of received frames discarded.

RX Bad Frame Blocks
This is a count of received frame blocks with bad CRC.

TX Unsolicited Retries
This is a count of retried unsolicited responses.

RX Unsupported Frames
This is a count of received frames accepted (good CRC and addressed to the outstation) with an unsupported data link function code.

Status Counters
All of these items describe what's happening on the connection to the master on the oldest outstation instance. They don't necessarily indicate trouble.



Status Counters			
TX Last Fragment		RX Last Fragment	
Events Awaiting Solicited Confirms	0	Events Awaiting Unsolicited Confirms	0
TX Cached Responses	0	TX Required Confirms	0
TX Solicited Responses	0	TX Unsolicited Responses	0
RX Solicited Confirms	0	RX Unsolicited Confirms	0
RX Total Functions	0	RX Read Functions	0
RX Direct Operate Functions	0	RX Write Functions	0
RX Enable Unsolicited Functions	0	RX Disable Unsolicited Functions	0
TX Solicited Objects	0	RX Solicited Objects	0
Total Events Buffered	0	Class 1 Events Buffered	0
Class 2 Events Buffered	0	Class 3 Events Buffered	0
TX Last Frame Time		RX Last Frame Time	
TX Frames Total	0	RX Accepted Frames	0
RX Supported Frames	0		

TX Last Fragment
Time of the last fragment transmitted.

RX Last Fragment
Time of the last fragment received.

Events Awaiting Solicited Confirms
Number of events reported and awaiting solicited confirmation; usually 0.

Events Awaiting Unsolicited Confirms
Number of events reported and awaiting unsolicited confirmation; usually 0.

TX Cached Responses
Count of cached responses transmitted.

TX Required Confirms

Count of fragments transmitted that required confirmation.

TX Solicited Responses
Count of solicited responses transmitted.

TX Unsolicited Responses
Count of unsolicited responses transmitted.

RX Solicited Confirms
Count of solicited response confirmations received.

RX Unsolicited Confirms
Count of unsolicited response confirmations received.

RX Total Functions
Count of total application function codes received.

RX Read Functions
Count of read application function codes received.

RX Direct Operate Functions
Count of Direct Operate application function codes received.

RX Write Functions
Count of write application function codes received.

RX Enable Unsolicited Functions
Count of enable unsolicited application function codes received.

RX Disable Unsolicited Functions
Count of disabled unsolicited application function codes received.

TX Solicited Objects
Count of data objects transmitted in solicited responses.

RX Solicited Objects
Count of data objects received in solicited requests.

Total Events Buffered
Number of total events buffered (that is, existing, maybe reported, but not confirmed).

Class 1 Events Buffered
Portion of the total events buffered that are class 1 events.

Class 2 Events Buffered
The amount of the total events buffered that are class 2 events.

Class 3 Events Buffered
The amount of the total events buffered that are class 3 events.

TX Last Frame Time

Time of the last frame transmitted.

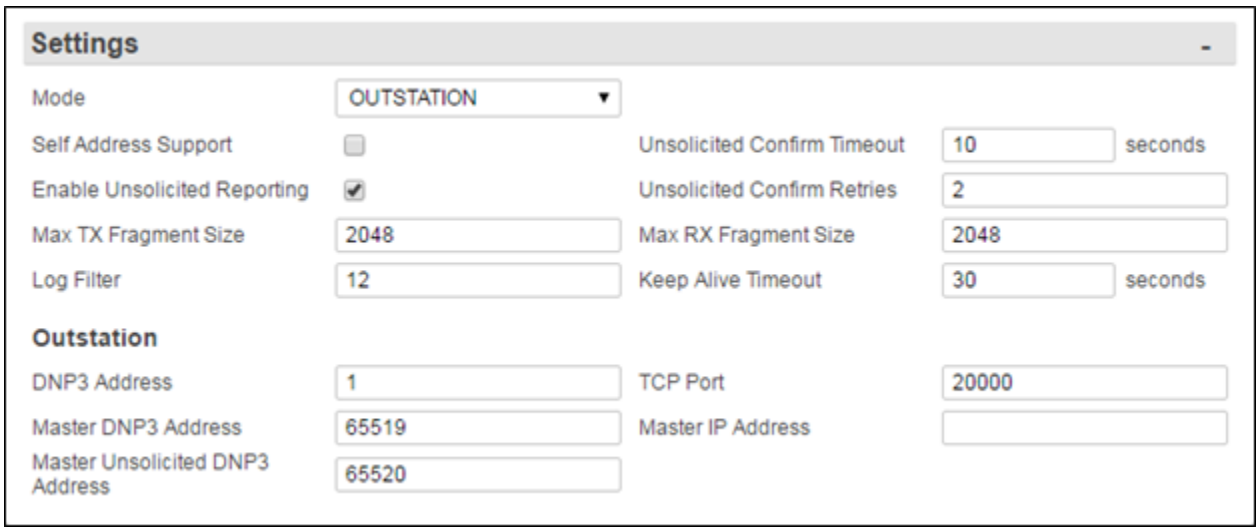
RX Last Frame Time
Time of the last frame received.

TX Frames Total
Count of total frames transmitted.

RX Accepted Frames
Count of total frames accepted.

RX Supported Frames
Count of total frames accepted with a supported data link function code.

Settings



Mode
This is a drop-down box to set the Mode to OUTSTATION. The default is OFF.

Self Address Support
This is an ON/OFF check box to enable self-address support in DNP3. The default is OFF (unchecked).

Unsolicited Confirm Timeout
This field sets the unsolicited response confirmation timeout in seconds. Setting range is from 1 to 60, with a default at 10 seconds.

Enable Unsolicited Reporting
This is an ON/OFF checkbox to enable unsolicited response fragments. The default ON (checked).

Unsolicited Confirm Retries
This field set the number of unsolicited response confirmation retries the SiteBoss will attempt.

Setting range is 0 - 10, with the default at 2.

Max TX Fragment Size
This field sets the maximum size of a transmitted fragment in bytes. Settings range from 249 to 2048, with a default at 2048.

Max RX Fragment Size
This field sets the maximum size of a received fragment in bytes. Settings range from 249 to 2048, with a default at 2048.

Log Filter
This is a numeric code to describe what gets logged and it is used for support/troubleshooting analysis only.

Keep Alive Timeout
This field sets the DNP3 Keep Alive timeout in seconds. Range 0 – 255 and the default is 30 seconds. Setting the Keep Alive to 0 disables the Keep Alive function. Upon expiration the unit initiates a Request Link Status data link transaction.

Outstation

The SiteBoss is an Outstation and expects connections from master(s). The unit expects a master to request operations on objects, and the master may expect the unit to send it autonomous messages (unsolicited responses) to convey important telemetry.

DNP3 Address
Use this field to set the DNP3 address of the outstation. Setting range from 0 to 65519, with the default set at 1.

TCP Port
Use this field to set the TCP port on which to listen for connections. Setting range is 0 - 65534, with the default at 20000.

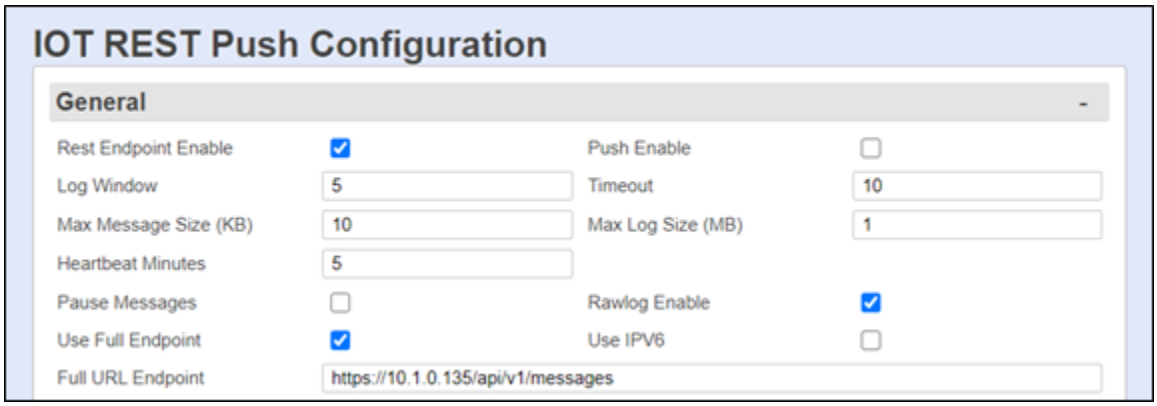
Master DNP3 Address
This field sets the DNP3 address of the intended master upon connection. Setting range is 0 - 65520, with a default at 65520. If set to 0 - 65519 then the outstation discards DNP3 data link frames not from this address. 65520 is not a valid DNP3 address, so, if set to 65520, it means that the outstation will accept frames from any address.

Master IP Address
This field sets the IP (v4 or v6) address (non-resolved) of the intended master. Default blank. If non-blank then the outstation drops connections from TCP clients not at this address.

Master Unsolicited DNP3 Address
This field sets the DNP3 destination address of unsolicited responses. Setting range is 0 - 65520, with a default at 65520. If set to 65520, then the outstation addresses data link frames of unsolicited responses to the source address of the last accepted frame received from the master.

IOT REST PUSH

IOT REST Push is a request that is sent from the SiteBoss to a RESTful interface. So these ?REST Push? messages are HTTP POST requests that are sent to the RESTful interface which would respond to them so the SiteBoss knows it doesn?t have to resend the alarm or other type of message. See the REST Message PUSH API Feature Guide for more information.



REST General

Rest Endpoint Enable

This is an ON/OFF checkbox option which enables/disables the SiteBoss function to receive and process REST interface message. The default is ON (checked).

Push Enable

This is an ON/OFF checkbox to enables REST Push. This sets the unit to send RESTful interface alarms and messages. The default is OFF (unchecked).

Log Window

This option sets seconds to listen before sending to the server.

Timeout

This sets the Server API timeout. This text box sets the seconds to wait for a response after attempting to push data to a server.

Max Message Size (KB)

This sets the maximum messages size to push when the log window expires in KB. Defaults to 10 KB.

Max Log Size (MB)

This text box set the maximum space to reserve for logging during network failure/stoppage in MB. Defaults to 1 MB.

Heartbeat Minutes

This sets the number of minutes in between heartbeat messages.

Use Full Endpoint

This ON/OFF checkbox set the unit to use full path set in the Use URL Endpoint setting.

If set to OFF (unchecked), then Full URL Endpoint is ignored. Additional settings options will become available and when the IP Address, IP Port and Base URL are set the SiteBoss will then combine IP + PORT + BASEURL to come up with something like 10.1.0.214:80/api/v1/ messages instead of using the full url setting.

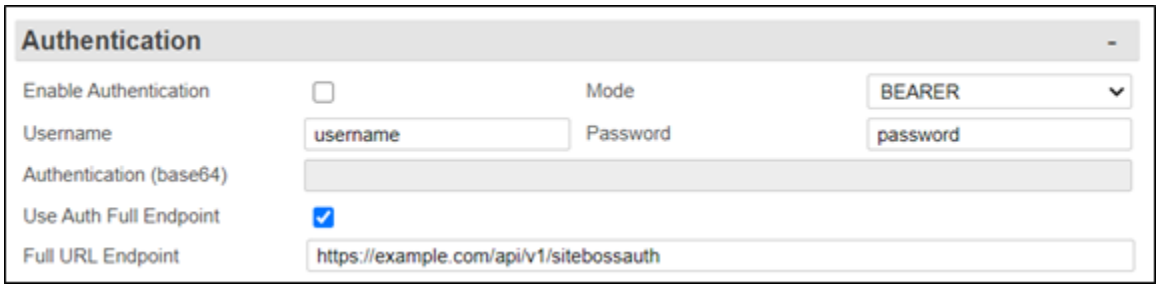
IP Address
If Use Full Endpoint is set to OFF this point is used by the SiteBoss to determine the IPv4 Push destination.

IP Port
This setting is used if the Use Full Endpoint is set to OFF (unchecked) to set the IP/Socket Port used with the IP Address setting.

Base URL
This setting is used if the Use Full Endpoint is set to OFF (unchecked) to set the URL Path after the domain name.

Full URL Endpoint
This text field sets the endpoint for push communications, e.g. https://localhost:8000/endpoint.

Bearer Authentication



Username
This text field sets the username to authenticate with the ASM (Asentria Site Manager) Server.

Password
This field sets the password for the Username for ASM (Asentria Site Manager) Server Authentication.

Use Auth Full Endpoint
This ON/OFF checkbox set the unit to use full path set in the Use ASM Full URL Endpoint setting.

If set to OFF (unchecked), then Full URL Endpoint is ignored. Additional settings options will become available and when the IP Address, IP Port and Base URL are set the SiteBoss will then combine IP + PORT + BASEURL to come up with something like 10.1.0.214:80/api/v1/ messages instead of using the full url setting.

IP Address
If Use Auth Full Endpoint is set to OFF (unchecked), this point is used by the SiteBoss to determine the IPv4 Push destination.

IP Port
This setting is used if the Use Auth Full Endpoint is set to OFF (unchecked) to set the IP/ Socket Port used with the IP Address setting.

Base URL
This setting is used if the Use Auth Full Endpoint is set to OFF (unchecked) to set the URL Path after the domain name.

ASM Full URL Endpoint
This text field sets the ASM endpoint for push communications, e.g. https://localhost:8000/ endpoint.

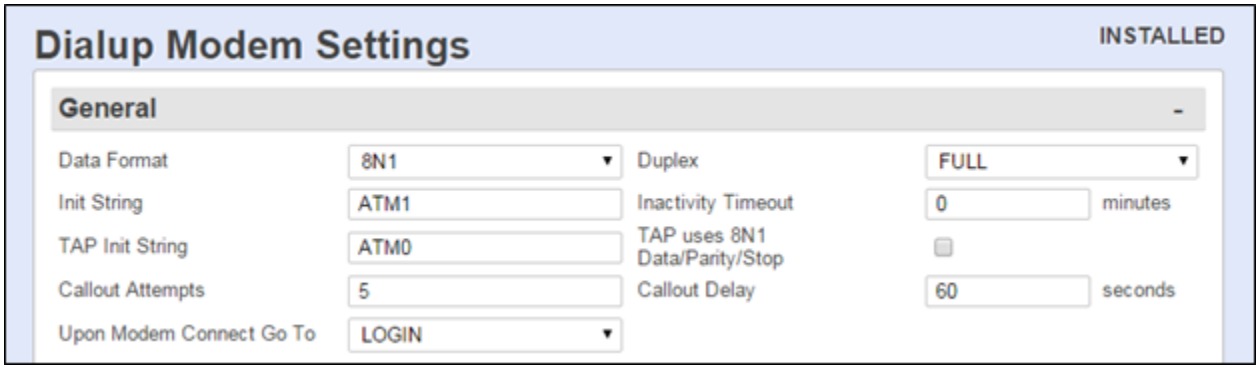
►Communication

Dialup Modem

The following is a top level settings configuration overview for the optional Dialup POTS modem. For additional information see the Dialup Modem Feature Guide on Asentria Product Information Portal or contact Asentria Technical Support.

The S550A does not have the POTS Modem functionality.

» Caution: To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
» Attention: Pour réduire les risques d'incendie, utilizer uniquement des conducteurs de télécommunications 26 AWG au de section supérleure.



Dial Up Modem General

Data Format
This is a drop-down menu to select word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, and 7N1. The default setting is 8N1.

Duplex
Duplex sets the echo settings for the modem Command Line Interface. Full duplex causes the SiteBoss to echo all characters sent to the remote device. Half duplex turns off character echo. The default setting is FULL.

Init String
This option sets the user-defined modem initialization string. This string is sent to the modem before important factory modem initialization settings, so certain settings in this init string may be overridden. The default setting is ATM1. The Maximum length is 126 characters.

» Note: Make sure to enter 'AT' at the beginning of this initialization string.

Inactivity Timeout
This selection sets the number of minutes (0 – 255) to wait before disconnecting an idle modem connection. A setting of 0 means the connection will never automatically expire. The default setting is 0.

TAP Init String
This option is the user-defined modem initialization string used only when the modem is making an alphanumeric modem callout. Default setting is ATM0. Maximum length is 126 characters

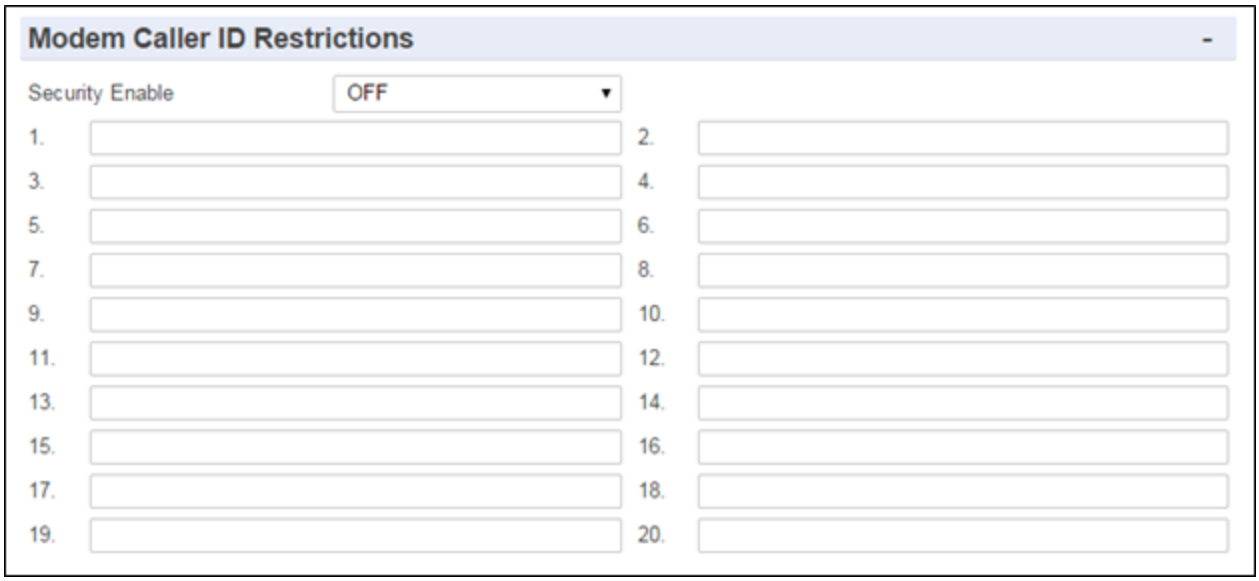
» Note: Make sure to enter 'AT' at the beginning of this initialization string.

TAP Uses 8N1 Data / Parity / Stop
This is an ON/OFF checkbox, to force the TAP initialization string data/parity/stop settings to 8N1. The default setting is OFF (unchecked).

Upon Modem Connect Go Directly To
This drop-down box sets what a user sees directly after connecting via modem. LOGIN requires the user to login with username and password, and will then take them to a command prompt. A serial port (I/O1, I/O2, etc.) redirects a modem user directly to that serial port upon connecting. In this pass-through mode to the serial ports, the command processor of the SiteBoss is transparent. The default setting is LOGIN.

Modem Caller ID Restrictions

» Note: Caller ID must be available on the phone line connected to the SiteBoss modem for this feature to work.



Security Enable
This is an ON/OFF toggle to enable caller ID restrictions. When enabled, the SiteBoss will only answer the modem if caller ID indicates one of the allowed phone numbers is connecting. The default setting is OFF.

n
Select one of these options to add or change a specific phone number. Simple wildcards are allowed in phone numbers: An asterisk (*) wildcard allows for any number of digits to appear to the right of that position. A question mark (?) matches any single digit. If no numbers are defined in this menu, all incoming calls are accepted. The maximum length is 47 characters.

Wireless Modem

Below is a brief description of the menu configurations options. For a complete description of the setup and operation of the Wireless Modem, please refer to the Wireless Modem Feature Guide on the Asentria Product Information Portal. Contact Asentria Technical Support for more information.

If the optional Wireless Modem is not installed in the SiteBoss, a basic settings menu will be displayed, but changing any of the settings will not do anything.

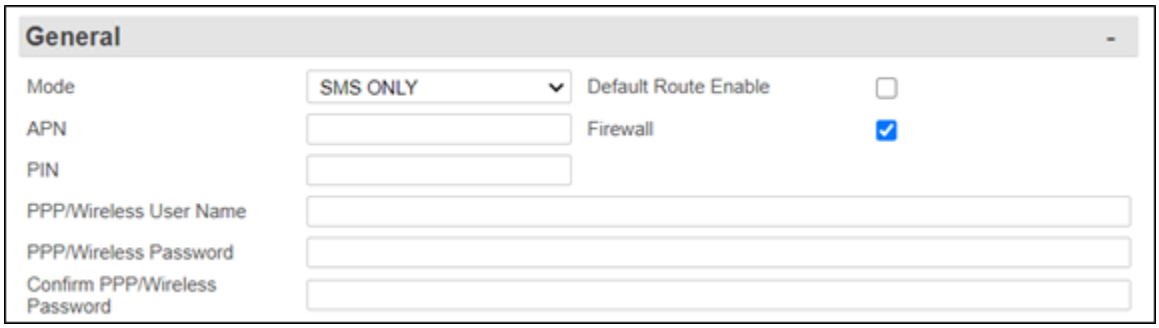
Status

The upper section of the Wireless Modem Web Page is a Status Page for the Wireless Modem. The information will be filled in based on the type of modem installed. For that reason, the status information section will vary.

This section displays information such as if the modem is connected with the wireless network, Signal Strength, the IP Address of the modem along with basic information on the modem itself and any installed SIM.

Wireless Modem Settings.jpg

Wireless Modem General



Mode
Mode toggles between SMS ONLY and PERMANENT. SMS ONLY means the modem is only available for out-bound SMS messaging. PERMANENT means the modem maintains an ?always on? connection with the network and is available for incoming connections. The default setting is SMS ONLY.

Default Route Enable
This is an ON/OFF toggle to enable the wireless interface to be the default route when connected. The default setting is OFF (unchecked). For wireless modem connectivity this box needs to be checked.

APN
This option sets the Access Point Name (APN) as defined by your wireless provider. The maximum length is 31 characters.

Firewall
This is an ON/OFF toggle to enable or disable the PPP Modem firewall for both PPP Dialout and PPP Hosting. The default is ON (checked). For wireless modem connectivity the firewall will need to be unchecked.

PIN
Set the PIN associated with the SIM card (if any). The maximum length is 15 characters.

PPP Wireless User Name / Password
These options set the login credentials for the PPP connection, as needed. The maximum length for each is 64 characters.

Advanced

PPP Debug Enable

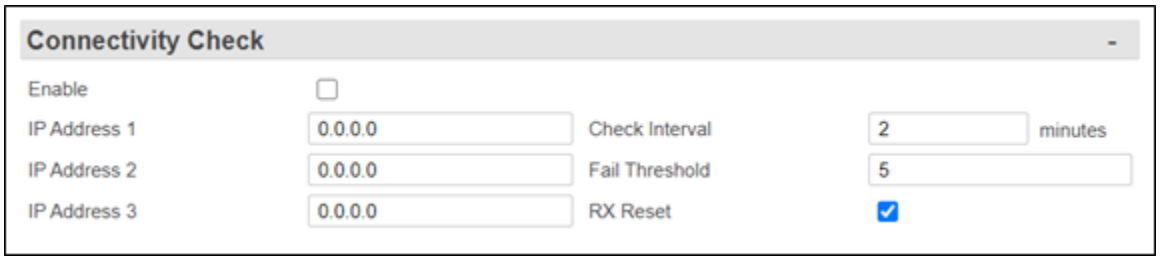
This is an ON/OFF toggle to enable capturing PPP traffic to a log file which can be extracted from the device and used for debugging purposes. The default setting is OFF (unchecked).

Idle Timeout
Idle Timeout sets the number of minutes (0 – 255) to wait before disconnecting an inactive modem connection. A setting of 0 means the connection will not be terminated. The default setting is 0 minutes.

Keep-Alive Threshold (minutes)
This option sets the length of time, in minutes, after which the wireless modem will send an outbound packet to maintain a connection, if no data has been transmitted. A setting of 0 disables this feature. The default is 0.

Connectivity Check
This section is used to configure the SiteBoss to ping up to two user-specified IP addresses at a user-specified interval. If the count of consecutive failed tests reaches a user-specified threshold, and the modem is not in use, the SiteBoss will power cycle the wireless modem. If the situation persists the SiteBoss will power cycle.

The modem will not power cycle more often than every 10 minutes. This interval increases on consecutive triggers to a maximum interval of 1 hour. If resetting the modem does not restore connectivity, then the SiteBoss will be power cycled on the next trigger. The SiteBoss will not power cycle more often than every 12 hours. A system message is displayed in any open command processor saying that the system is going to reboot in 30 seconds.



Enable
This is an ON/OFF checkbox to enable or disable the feature. The default is OFF (unchecked).

IP Address n
Use these fields to set the IP address(es) that will be pinged for the connectivity check. The default is 0.0.0.0. The unit will not ping 0.0.0.0.

Check Interval (minutes)
This field is used to set how often the IP address(es) will be pinged, in minutes. The range is 1 to 10 minutes. The default is 2.

Fail Threshold
This field sets how many ping checks in a row must fail before the modem or SiteBoss is power cycled. The range is 2 to 50 and the default is 5.

RX Reset
This is an ON/OFF check box setting that determines whether the connectivity check trigger is inhibited if any data is received on the wireless interface. The default is ON (checked).

Serial

This Menu is used to configure the on board serial ports as well as any additional serial ports installed using expansion slot cards.

Command Port

These options apply for Serial I/O 2 when the Port Mode set to Command. I/O 2 is set to Command by default.

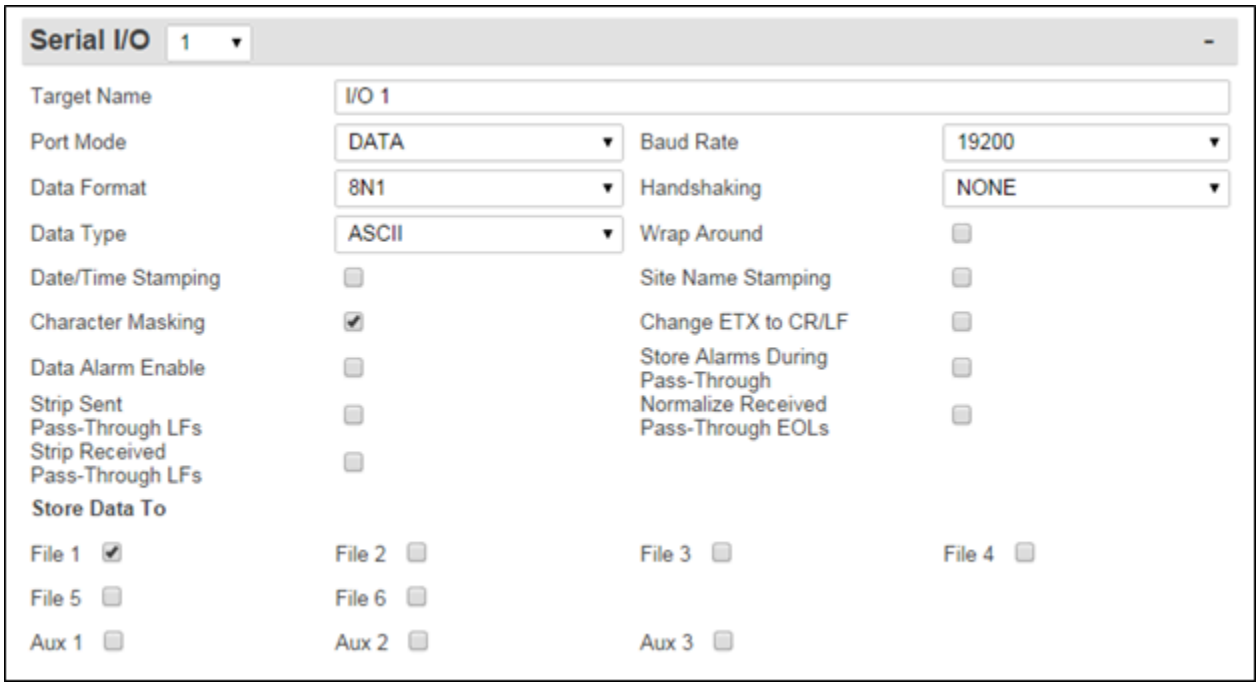
Duplex

Duplex controls the echo settings for the command line interface. It is a drop-down box to choose between FULL and HALF. Full duplex causes the unit to echo all characters sent to the connected terminal when in COMMAND mode. Half duplex turns off character echo. The default setting is FULL.

Inactivity Timeout

This option sets the number of minutes (0 - 255) to wait before a serial connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. The default setting is 0.

Serial I/O



Serial I/O
The drop-down box in the grey menu block area is used to select which installed serial port to configure. The default is I/O 1.

Target Name
This text field sets the name given to the device connected to the other end of the serial port. This field will accept up to 24 alphanumeric characters. The target name is used in event notifications. The default setting is I/O n.

Port Mode
Port Mode sets the port function.

- I/O 2 drop down allows a section between COMMAND, DATA, PPP HOST, PPP CLIENT and RESERVED. The default for I/O2 is COMMAND.
    - COMMAND allows for serial command processor access.
    - DATA configures the port as an inbound RS232 data port.
    - PPP HOST and PPP CLIENT configure the port to act as either a host or client in a PPP over Serial Port connection See the PPP Over Serial Port Feature Guide on the Asentria Information Portal for more information. The default setting is COMMAND.
    - RESERVED configures the port to communicate with certain 3rd party sensors using Modbus RTU.

- I/O n All other serial I/O ports toggle between DATA and RESERVED. DATA configures the port as an inbound data port. RESERVED configures the port to communicate with certain 3rd party sensors using Modbus RTU. The default setting is DATA.

Baud Rate
The Baud Rate option is a drop-down box to selection the baud rate for the port. These values range from 300 baud to 115200 baud. The default setting is 19200.

Data Format
The Data Format is a drop-down box to choose word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, 7N1, and 8O2. The default setting is 8N1.

Handshaking
Handshaking drop-down box is used to set how the port will handshake with the connected device. The available options are: NONE, XON/XOFF, BOTH, and DTR. The default setting is NONE.

Data Type
The Data Type drop-down box use used to choose the type of data being collected on this port. The options are ASCII and BINARY. The default setting is ASCII.

Wrap Around
Wrap Around is an ON/OFF checkbox to set whether the incoming data will wrap (overwrite) the oldest data in the file should it become full. The default setting is OFF (unchecked).

Date/Time Stamping
This is an ON/OFF checkbox to choose if the date and time are prepended to each incoming data string. The default is OFF (unchecked).

Site Name Stamping
This is and ON/OFF checkbox to choose if the Site Name is prepended to each incoming data string. The default is OFF (unchecked).

Character Masking
This is an ON/OFF checkbox to enable the character mask. The character mask allows you to block most non-printing ASCII characters. Specifically, the following ASCII character values are blocked: 0, 1, 4-9, 11, 12, 14-31, and 128-255. The default setting is ON (checked).

Change ETX to CR/LF
This is an ON/OFF checkbox to set whether ETX characters in the incoming data should be converted to CR/LF characters. The default setting is OFF (unchecked).

Data Alarm Enable
This option is an ON/OFF checkbox to enable data alarm monitoring for this port. The default setting is OFF (unchecked).

Store Alarms During Pass-Through
This is an ON/OFF checkbox to determine whether data strings that meet data alarm criteria are stored in the Events File when a pass-through session is active on this port. The default setting is OFF (unchecked).

Strip Sent Pass-Through LFs
This is an ON/OFF checkbox to enable the stripping of linefeeds on pass-through data sent out of the SiteBoss. The default setting is OFF (unchecked).

Strip Received Pass-Through LFs
This is an ON/OFF checkbox to enable the stripping of linefeeds on pass-through data received by the SiteBoss. The default setting is OFF (unchecked).

Normalize Received Pass-Through EOLs
This option is an ON/OFF checkbox to enable the following translations on data received on a serial port and sent to the pass-through client. Some pass-through devices have mixed/ inconsistent EOL output; this setting is intended to make it consistent. The default setting is OFF (unchecked).

- CR[non-LF]->CRLF[non-LF]
- [non-CR][LF]->[non-CR]CRLF
- CRLF->CRLF (i.e., no translation of CRLF)

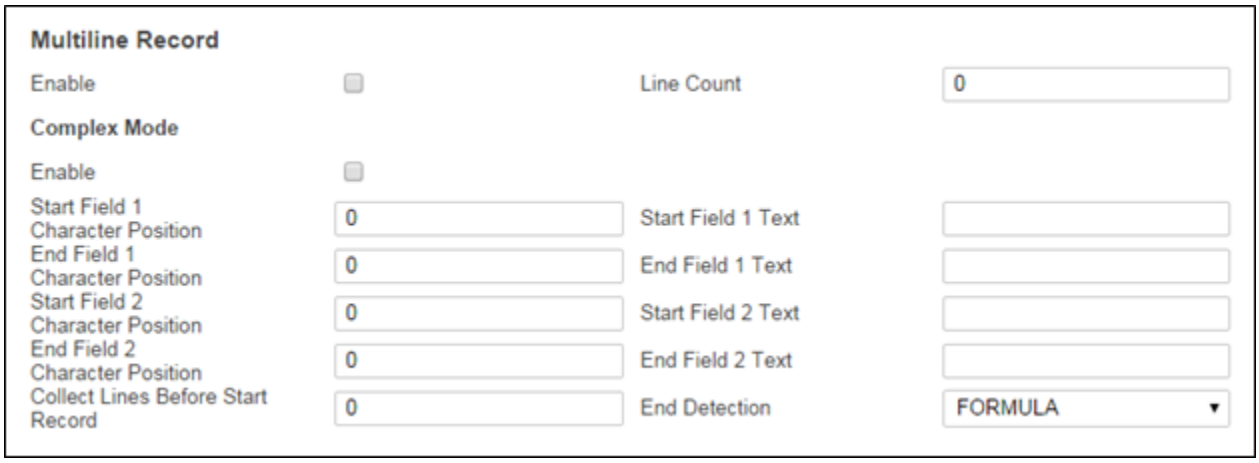
Store Data To

This selection displays a series of ON/OFF checkboxes to choose whether the data received on this port should be stored. The file number with the same number as the serial port number is set to ON by default and the other available options will be set to OFF (unchecked).

Multiline Record Setting

The SiteBoss has the ability to monitor incoming serial data for multi-line records (individual

records that are broken into multiple lines with carriage returns). If the records are separated by a specific number of blank lines, this basic configuration menu will suffice. If a more complex delineation scheme is used, enable Complex Multiline Detection.



Enable
This is an ON/OFF checkbox to enable multiline record detection. The default setting is OFF (unchecked).

Line Count
This option sets the number of blank lines that must come between records. Use this field to set the blank line count if the End Detection is set to BLANKs in the Complex Mode section. The default setting is 0.

Complex Mode

Enable
This is an ON/OFF checkbox to enable the advanced multiline detection. The default setting is OFF (unchecked).

Start Field n Character Position
These fields set the character position used to define the beginning of the multiline field. This option is used with "Count" method record end detection.

Start Field n Text
These fields set the text used to determine the beginning of the multiline field. This option is used with "Formula" method record end detection.

End Field n Character Position
This option is the counterpart to start character position option. This option sets the end delimiter for multiline records. This option is used with "Count" method record end detection.

End Field n Text
This option is the counterpart to start the text option. This option sets the end delimiter for multiline records. This option is used with "Formula" method record end detection.

Collect Lines Before Start Record

This option sets the number of blank lines that are between each record.

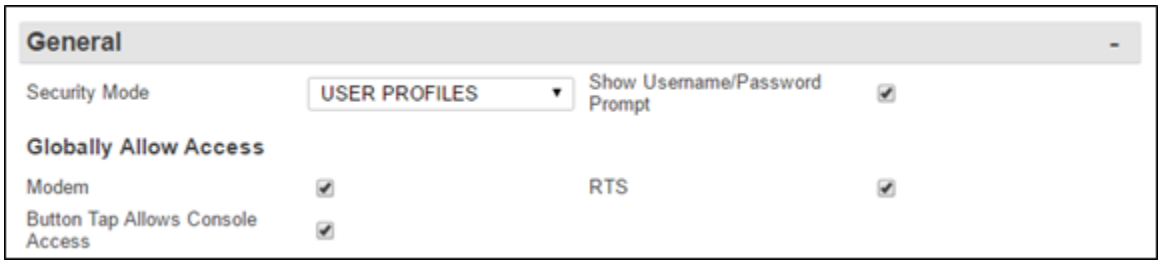
End Detection
End Detection is a drop-down box to choose between FORMULA, COUNT, and BLANKS to set the method of detecting the end of each record. The default setting is FORMULA.

►Security

The Security Settings menu displays options for setting the security mode, as well as specific and general security settings. See the Securing a SiteBoss Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.

» Note: The "Security Mode" setting controls if the settings under USER PROFILES or RADIUS are in effect by the SiteBoss. The menu options will be present and can be set regardless of how the function is toggled.

General Security



Security Mode
This is a drop-down box for choosing between USER PROFILES and RADIUS security settings. If USER PROFILES is selected the fields in the User Profiles menu section we be in use. If RADIUS is selected then the RADIUS menu options will be in effect for accessing your SiteBoss. The default setting is USER PROFILES.

Show Username / Password Promp
This is an ON/OFF checkbox to set whether a prompt for logging in is displayed when logging in via the Command Line Interface. The default setting is OFF (unchecked).

Globally Allow Access

Modem
This checkbox allows toggling ON or OFF user access to the SiteBoss via a POTS Modem (if installed). Not applicable to the S550A.

RTS
This checkbox Enables (checked) or Disables (unchecked) Real-Time Sockets functionality globally in the SiteBoss. The default setting is ON (checked). This setting is not present on the S550A, since it does not have the Real-Time Socket functionality.

Button Tap Allows Console Access

This is an ON/OFF toggle to give access to a user who has forgotten their log on credentials. This is an insurance policy against locking yourself out of the unit. When set to ON (checked), the user can tap the Reset button 5 times quickly (1-2 times per second), at which point the LEDs on the front panel will flash for a few seconds. The user will then have immediate access using the default MASTER username and password (admin/password). The default setting is ON.

If you lock yourself out and gain access again with the button unlock feature, remember to reconfigure the settings that were defaulted by the Button Unlock feature to maintain your prior security configuration.

These are the settings that are defaulted by this process:

- Security/ General Security/Security Mode set to USER PROFILES
- Security/ User Profiles/ User 1 User Name set to admin, Password set to password, and User Access Level set to MASTER
- Security/ User Profiles/ General/Requires Password/ Local Command set to OFF (unchecked). (This setting sets the unit to not require a password when logging in serially via IO2).

General Certificate

The purpose of the Certificate section of the Web UI is to allow a MASTER user to configure SSL certificates used to access the unit via HTTPS. This HTTPS Web UI section allows the MASTER user to create a self-signed certificate, create a certificate signing request (CSR), install an externally signed certificate, and check the status of these 3 things.

The benefit is that a user can install a certificate signed (externally) by a certificate authority that is by default trusted by web browsers, thus eliminating the SSL warning in the browser when you browse via HTTPS to the unit.

Common Name

This is a Text field to name the unit. The maximum number of characters is 64. The default is siteBoss.

Organization Unit

This is a text field. The maximum number of characters is 40. The default is Technical Services.

Organization

This is a text field. The maximum number of characters is 40. The default is Asentria.

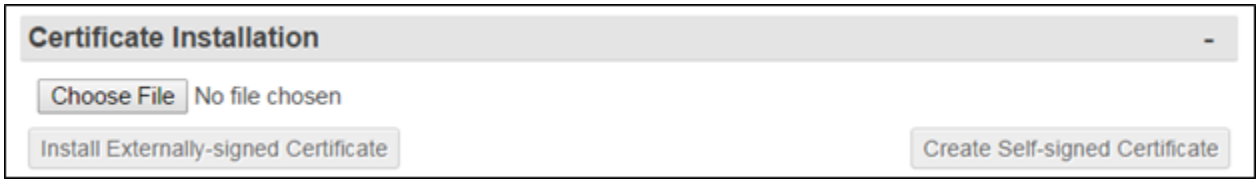
Key Length
This dropdown box allows the user to select the SSL key length. The options are 1024 bits or 2048 bits. The default is 1024 bits.

Locality
This is a text field. The maximum number of characters is 40. The default is Seattle.

State/Province
This is a text field. The maximum number of characters is 40. The default is Washington.

Country
This is a text field. The maximum number of characters is 2. The default is US.

Certificate Installation



Choose File
Use the functions in the Certificate Signing section of the page to generate a key for your third party certificate authority. Once the CA supplies a certificate key, install the file in the SiteBoss using this button. Once this is done the Install Externally-signed Certificate button will enable.

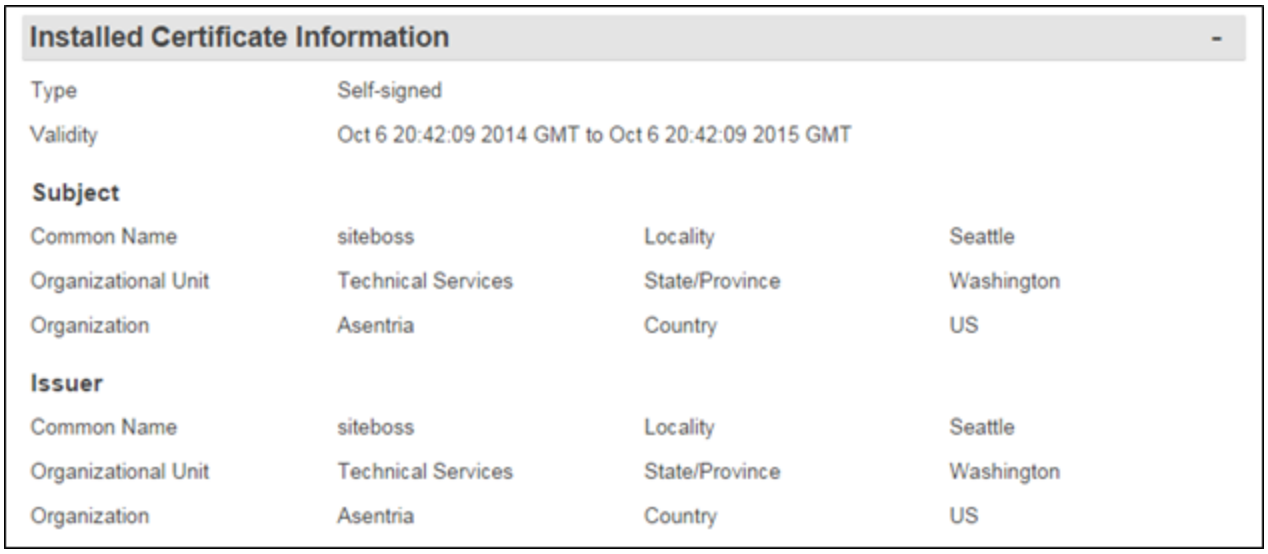
Install Externally-signed Certificate
The Install Externally-signed Certificate will be enabled only if user is logged in with MASTER credentials and a file is loaded with your certificate key from your third party certificate authority using the "Choose File" button above it. Click this button to install the certificate.

Create Self-signed Certificate
The Create Self-signed Certificate button will be enabled only if the user is logged in with MASTER credentials. If the button is clicked the information from the General Cerificate section will populate the read only "Installed Cerificate Information" fields.

Installed Certificate Information

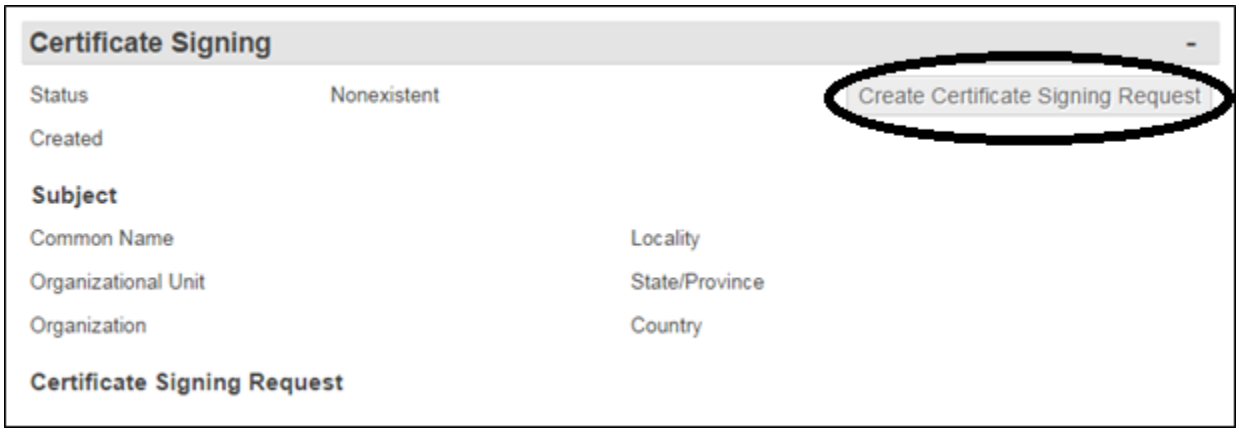
These fields are read only. These read-only items are refreshed in 3 circumstances:

1. Upon initial load.
2. Upon seeing that the user has clicked the "Install Certificate" button.
3. Upon seeing that the user has clicked the "Create Self-signed Certificate" button.



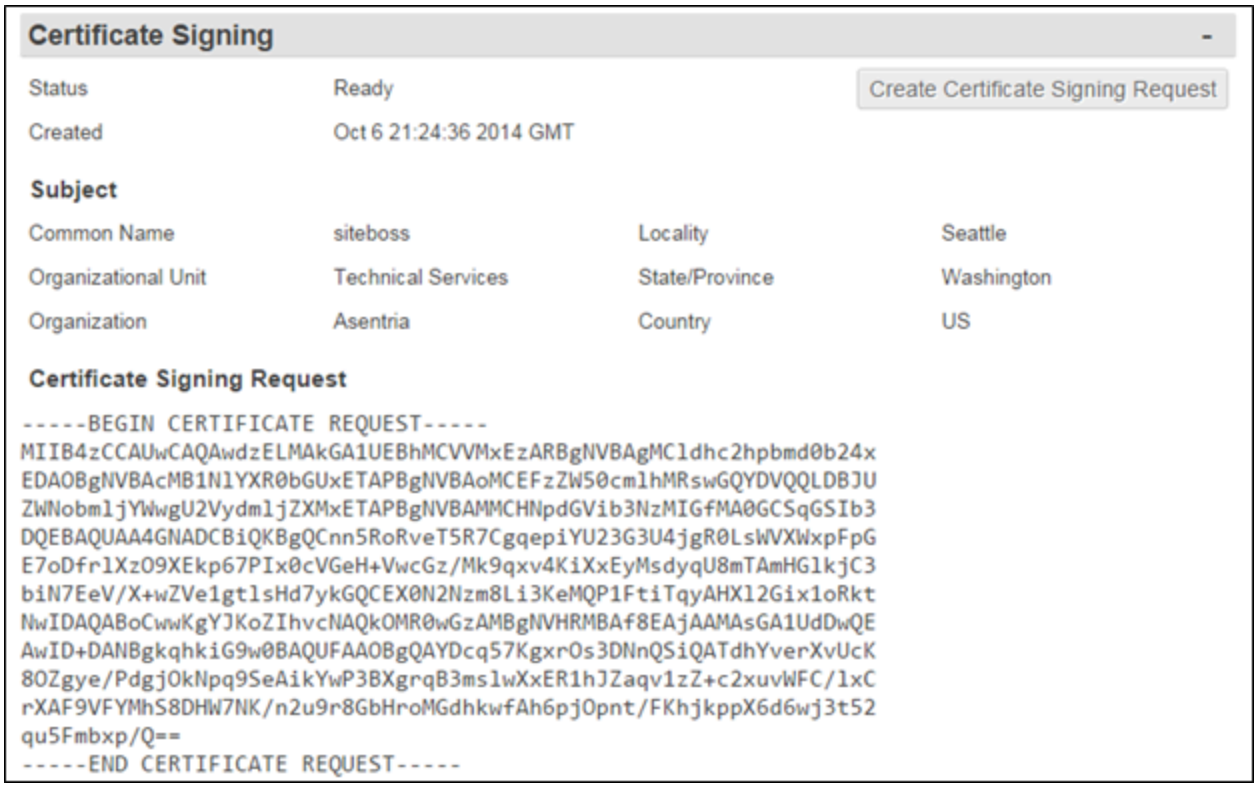
Certificate Signing

The Create Certificate Signing Request button is active only if the user is logged in as a user with the User Access Level set to MASTER.



Create Certificate Signing Request

Clicking this button will generate a Certificate Signing Request Key. This key would then be sent to your selected third party certificate authority. They will use this key to generate a file that is loaded by clicking the Choose File button in the "Certificate Installation" section of the page.



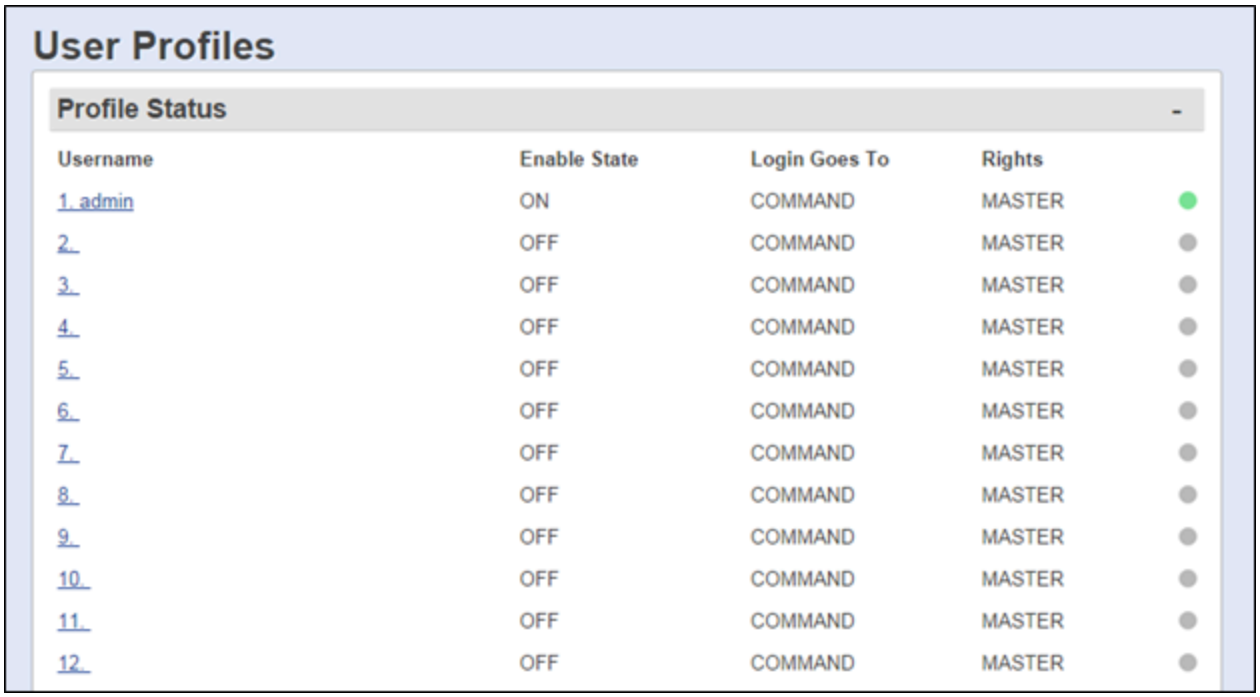
User Profiles

When the Security Mode in the General Security section is set to USER PROFILES, this menu option is used to set up the User Profile Settings.

» Note: By default, the User1 profile is the only one with a preconfigured username and password (admin/password). Usernames and passwords are not pre-configured for Users 2 thru 12. For security reasons it is highly recommended that you change the User 1 password, and record it and all other configured passwords in a secure location.

Profile Status

The top section of the page displays the Enable State, Where the Command Interface Login goes to and the user rights status that is configured for all 12 user options. To set up a user click the blue number in the Username column in the Profile Status section and the next lower section of the page will display the options to configure for that profile.



Profile *n*

User Information

Enable

This is an ON/OFF checkbox to enable access for this user profile. The default is ON (checked) for User Profile 1 and OFF (unchecked) for all other profiles.

User Name

This option is used to set the username this profile. Duplicate user names are not allowed. The maximum length is 31 characters.

Password / Confirm Password

These options are used to set the password for this profile. Maximum length is 31 characters.

» Note: Passwords are case sensitive and are masked in all menus and while typing them for security reasons. If a user without permissions accesses the User Profile Settings menus, they will see all fields in this menu either masked or with no data in them.

Expiration
This option is used to set a date and/or time that this profile may be automatically disabled. Use the format MM/DD/YYYY HH:MM:SS in 24 hour format. This option is only useable by a Master User on other User Profiles. If left blank the user profile will not expire.

User Access Level
This setting is a drop-down menu to set this user's access level. The options are MASTER, NONE, VIEW, ADMIN1, ADMIN2, and ADMIN3. See the User Profiles Feature Guide on the Asentria Information Portal for more information on each access level. The default setting is MASTER.

Upon Login Start
This is a drop-down menu selection to select the starting display option this user will be directed to upon logging in at the Command Line Interface. The options are: COMMAND, PASSTHROUGH and MENU and example displays as shown here:

Command

```
SiteBoss

READY
>
```

Pass-through

```
SiteBoss

Connected to I/O 1
```

Menu

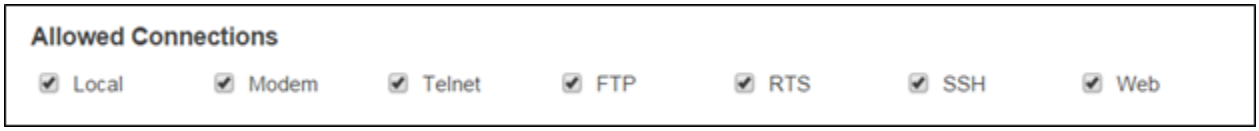
```
SiteBoss 550 Version 2.11.350
at 550-550001267

1. Pass-Through to I/O 1
2. Pass-Through to I/O 2
P. 550 Command Prompt
M. 550 Setup Menu
S. 550 Status Menu
X. Exit (end connection)
```

Default Pass-through Port
This selection specifies the destination if the ?Upon Login Start? action is set to PASSTHROUGH. This is a drop-down menu of all of the available serial ports and CPE devices (1 thru 4). The default setting is Serial Port I/O 1.

Upon Pass-through Exit
This drop-down box allows a selection of MENU (in the command line interface) or DISCONNECT to set where the user is sent when they exit out of a pass-through connection.

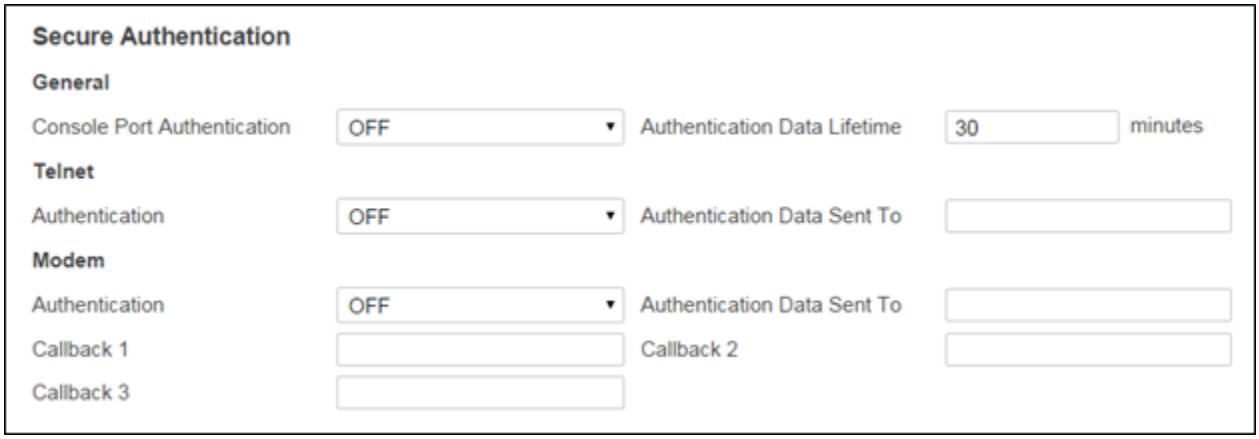
PPP Authorization Type
This is a drop-down menu option to select between LOCAL, ROUTING and NONE. LOCAL allows PPP access, but denies all routing to whatever LAN the SiteBoss is connected to. ROUTING enables Route Ethernet to PPP and Route PPP to Ethernet for the user, but only if those settings are enabled globally. NONE disables PPP access for the user. The default is ROUTING.

Allowed Connections



These are checkbox ON/OFF options allowing this user access via Local (Console Port), Modem, Telnet, FTP, Real-Time Socket, SSH (Secure Shell), and the Web interface. The default setting for all is ON (checked) for all options.

Secure Authentication



General

Console Port Authentication
This drop-down menu allows the selection between OFF, and CHALLENGE for Serial Port 2 (I/O2). The default setting is OFF.

OFF allows normal access via the console Port (I/O 2). By default there is no password

required for serial access via IO 2. Password access can be enabled by clicking the check box for Local Command in the General section, Requires Password, at the bottom of the User Profiles page on the Web Interface.

CHALLENGE requires the user enter their username/password and then they are prompted with a short challenge code. That code must be plugged into a program called Response Code Generator (RCG). This software can be found on the Documentation and Utilities Documentation Drive. Contact Asentria Technical Support for this, or download (named "Response Code Generator") from the download section on the Asentria customer support wiki: Response Code Generator. RCG requires a shared secret, set in the lower General section on this web page, as well as the challenge code generated by the SiteBoss. The user must then respond with the proper hash generated by RCG in order to gain access.

For the CHALLENGE setting to function on I/O2 (the Console Port for the SiteBoss) the check box for Local Command must be checked in the General section, Requires Password, at the bottom of the User Profiles page on the Web Interface.

Authentication Data Lifetime

This setting is used to set the number of minutes (0 – 180) before the single-use password expires. A setting of 0 means the password will never automatically expire. The default setting is 30.

Telnet

Authentication

This drop-down menu allows the selection between OFF (normal password mode), CHALLENGE, SEND PASSWORD authentication modes. The default setting is OFF.

OFF authentication requires only the configured username/password authentication.

CHALLENGE requires the user enter their username/password and then they are prompted with a short challenge code. That code must be plugged into a program called Response Code Generator (RCG). This software can be found on the Documentation and Utilities CD. Contact Asentria Technical Support for this, or download (named "Response Code Generator") from the download section on the Asentria customer support wiki: Response Code Generator. RCG requires a shared secret, set in the lower General Section on this web page, as well as the challenge code generated by the SiteBoss. The user must then respond with the proper hash generated by RCG in order to gain access.

SEND PASSWORD will generate a single-use password and send it to the Email address(es) specified by the Authentication Data Sent To field. That password will only allow a login for the user whom it was generated for.

Authentication Data Sent To

Use this field to set the Email address where the single-use password is to be sent. This field is used if the Authentication field is set to SEND PASSWORD.

Modem

These Modem settings relate to the internal Dialup POTS modem access only and do not

apply for any installed wireless modem. They are not applicable to the S550A.

Authentication

This drop-down menu will allow a selection between OFF, CHALLENGE, SEND PASSWORD and CALLBACK authentication modes. The default setting is OFF.

OFF authentication requires only the normal username/password authentication.

CHALLENGE requires the user enter their username/password and then they are prompted with a short challenge code. That code must be plugged into a program called Response Code Generator (RCG). This software can be found on the Documentation and Utilities CD. Contact Asentria Technical Support for this, or download (named "Response Code Generator") from the download section on the Asentria customer support wiki: Response Code Generator. RCG requires a shared secret, set in the lower General Section on this web page, as well as the challenge code generated by the SiteBoss. The user must then respond with the proper hash generated by RCG in order to gain access.

SEND PASSWORD will generate a single-use password and send it to the Email address(es) specified by the Send Password To option. That password will only allow a login for the user whom it was generated for.

CALLBACK (via Modem) will cause the SiteBoss to do an immediate callback to the Secure Callback number(s) configured further down in this menu.

Authentication Data Sent To

Use this field to set the Email address where the single-use password is to be sent. This field is used if the Authentication field is set to SEND PASSWORD.

Callback ***n***

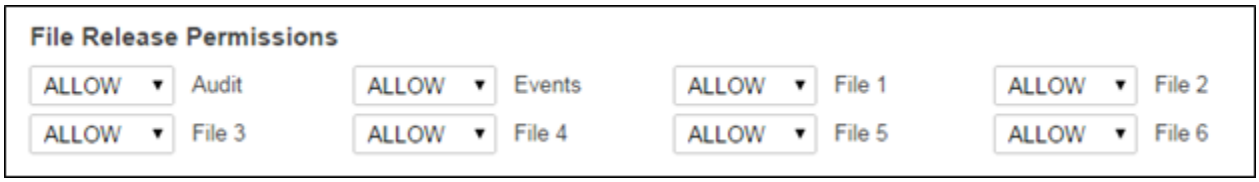
These options set the modem callback numbers if the Authentication option is set to CALLBACK. If configured, the SiteBoss will disconnect any modem connections from this user and then attempt to dial out to each of these numbers. If one of the numbers answers, the other end must respond with the login credentials of the user used to initiate the callback (maximum length 48 characters).

Pass-through Permissions

These options are in effect if the "Upon Login Start" action is set to Menu. All available serial ports and CPE devices 1 thru 4 will have an ALLOW or DENY drop-down box option. If a port is set as ALLOW, then that serial port or CPE device is displayed in the Command Line

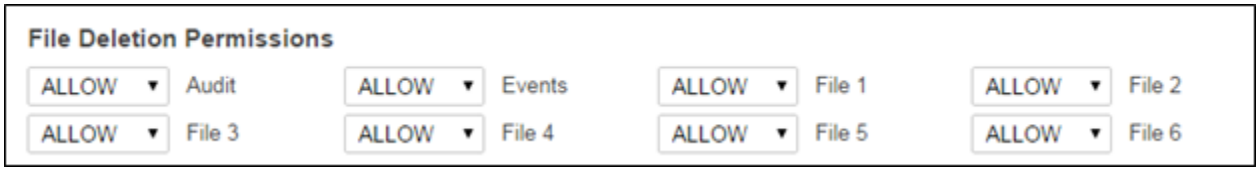
Interface Menu after the user logs in. If a port is set as DENY, then that serial port is not displayed in the Menu. The default setting for all ports is ALLOW.

File Release Permissions



All data files, Events Log and Audit Log will have a drop-down box to ALLOW or DENY release permission for this user. The default setting for all is ALLOW.

File Deletion Permissions



These options display a menu showing all data files, Events Log and Audit Log, and toggles ALLOW or DENY Deletion by this user. Default setting for all is ALLOW.

General

The options in this section set parameters for passwords and security that are required for ***every*** user who attempts to log into the SiteBoss.

Username and/or Password Required

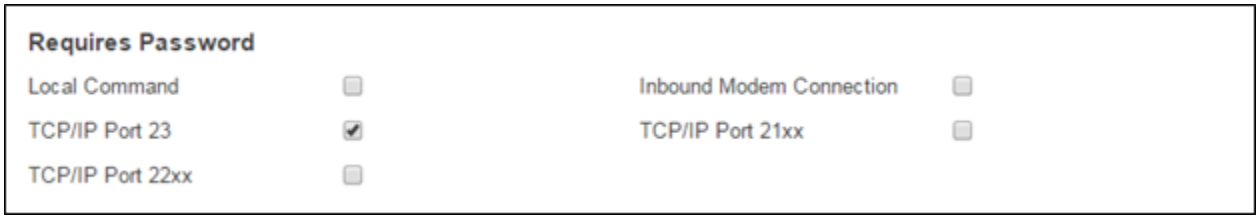
This option toggles between: PASSWORD ONLY, USERNAME/PASSWORD (PW), or PASSWORD(PW)/USERNAME. This field applies when logging onto the Command Line interface via the options selected in the Requires Password section. The default setting is PASSWORD ONLY.

Shared / Confirm Secret for Challenge/Response

This selection sets the shared secret used to generate Challenge/Response codes. The Maximum length is 48 characters. Challenge/Response requires the use of the free Asentria Response Code Generator program. Contact Asentria Technical Support for this, or download (named "Response Code Generator") from the download section on the Asentria customer

support wiki: Response Code Generator.

Requires Password



This section has ON/OFF check boxes to set whether a password is required when accessing the SiteBoss via the corresponding method. When any of the above options is set to OFF (unchecked), users connecting via that method are automatically granted Master access. By default all options are set to OFF (unchecked) except TCP/IP Port 23 which is set to ON (checked).

» **Note**: The Inbound Modem Connection is referring to an internal dialup POTS modem (if installed) and is not applicable to any optional Wireless Modem.

Cameras

The Security Camera must be configured with its own IP address on the same network as the SiteBoss. Configure the Security Camera per its instruction manual. The camera will stream an image live over the internet. The SiteBoss can then be configured to interface with the camera for monitoring and alarming purposes.

The SiteBoss can support up to 8 cameras and up to 80 images using internal storage. The max storage internally is 6MB. Firmware versions prior to 2.11.350 are limited to 3 cameras, 40 images and 2MB storage. The oldest images will be removed to make room for new ones.

All images are deleted when the unit is rebooted.

Only .jpg images via FTP are supported. Some cameras will have an FTP test. These FTP tests will not complete successfully. However, the FTP transfers and alarming within the SiteBoss will function as expected.

» **Note**: Viewing the live video stream from a camera, when routing to it through the SiteBoss, puts a large strain on the SiteBoss resources and is not recommended.

See the Camera Feature Guide on the Asentria Information Portal or contact Asentria Technical Support for additional information.

Security Cameras General

Media Storage Mode

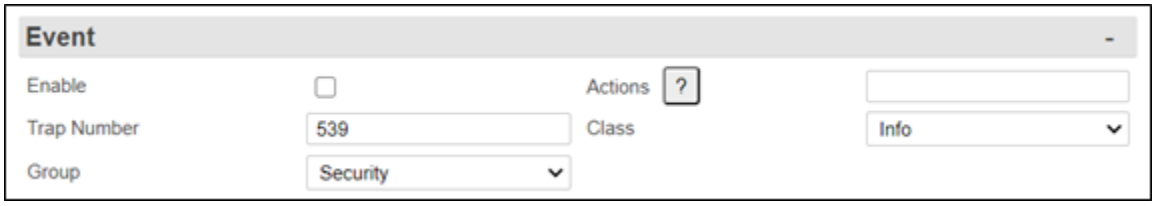
This drop-down box setting controls what storage media to use when receiving images. The options are NONE, INTERNAL and SD CARD SAEC. The Event functions will not work if this option is set to NONE. The default is NONE.

SD CARD SAEC refers to storage on a Secure Access Ethernet (SAEC) expansion card. That expansion card has an SD slot that allows for a greatly increased image storage capacity. The SD card capacity, usage, and space available is now displayed when the user selects "SD Card SAEC" as a storage option. When a user first selects the SD CARD SAEC option it can take up to 60 seconds for the SAEC SD information to be posted to this page. If an SD card is not available, "SD card not detected" message is displayed.

Max Image Total

This setting controls the maximum number of images that will be stored at one time on the selected storage media. Available options are 1 to 80. The default is 12. The amount of INTERNAL storage available for IP Camera images is 6MB.

Event



Enable

This checkbox is an ON/OFF toggle used to enable alarming actions for this camera. The default is OFF (unchecked).

Actions

This field is used to define the actions for the SiteBoss to take when it receives an image from the camera. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Trap Number

These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Camera Events is 539, but any number in the alternate range of 1000 - 1199 can be used.

Class

These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

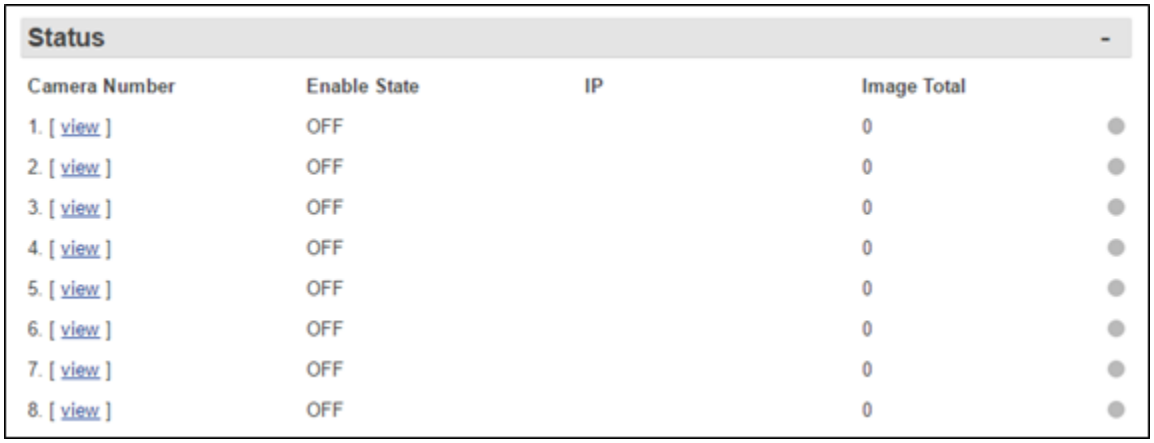
Group

This is a drop-down descriptive field that can be used to categorize the alarm point into subjective group types on custom pages or in Alarm Manager or other Network Management Software. The available drop-down options will be a list of the groups previously defined at the

Group Table page.

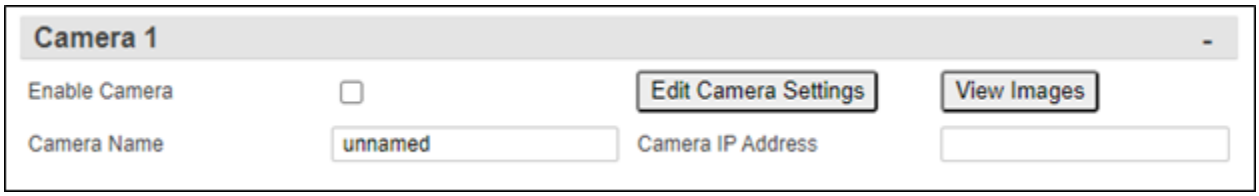
Status

This section displays basic status on up to 8 cameras. To configure any of the cameras click the blue "View" link and the lower section of the page will display configuration fields for that camera.



Camera *n*

These fields are used to configure the settings for the specific IP Camera selected using the Status / "view" hyperlink in the menu display option covered above.



Enable Camera

This is an ON/OFF checkbox for controlling whether or not this camera is enabled and its settings considered. The default value is OFF (unchecked).

Camera Name

This is a text field to identify the camera by a unique name. The camera name limited to 20 characters. Cameras that have not been named display will display as "unnamed" and the title over the individual camera settings will display as Camera *n*.

Edit Camera Settings

This button will take you to the installed camera, usually displaying the log in screen for the camera itself. Depending on your computer and browser settings, you may need to disable pop up blockers or designate the camera IP address to allow pop ups for the button to function. See the camera manual for settings within the camera itself.

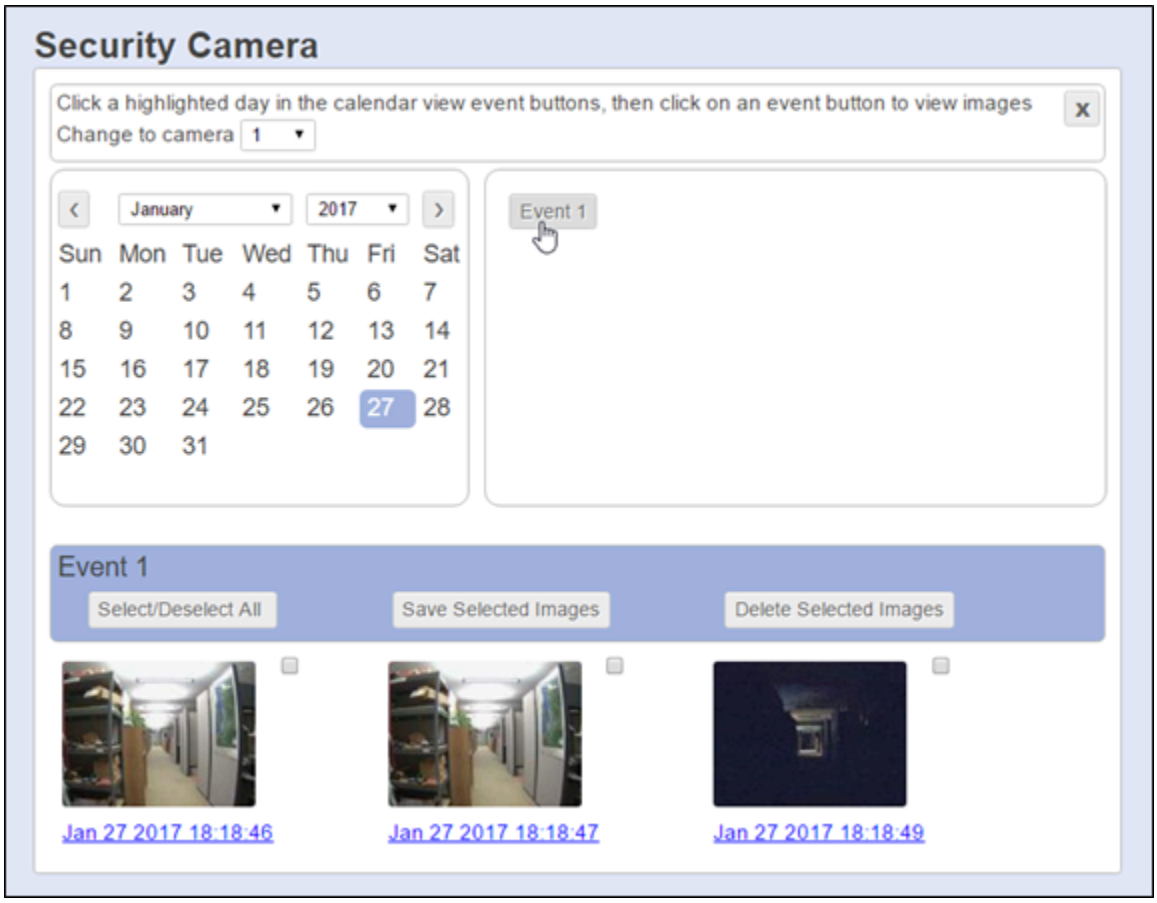
Camera Address

This field sets the internal or external IP of the camera. The default is blank (no IP Address).

View Event Images

The View Event Images button brings up a page where you can select the date to view any images. Click a date in the calendar section and if there are any event images for that date ?Event? box(es) will display in the right hand section of the page. Click the Event button to have the images display in the lower section of the page.

Click the "X" in the upper right hand corner to return to the Camera Settings page of the SiteBoss.



Event n

This section displays any saved event images. Each image is date and time stamped by the SiteBoss. Events can be selected individually by checking the box to the right of the image. Then that image can be saved or deleted using the save or delete buttons described below.

Select/Deselect All

This button is check (select) or uncheck (deselect) all images in the Event group.

Save Selected Images

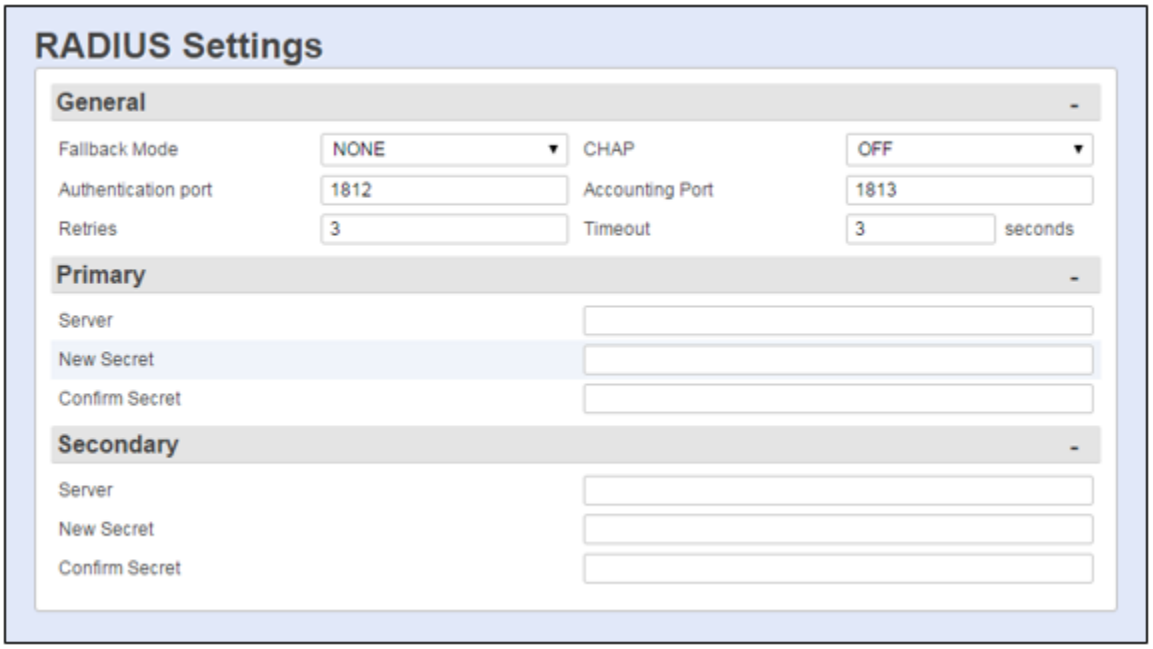
This button will download images to your computer where they can be saved in a desired location.

Delete Selected Images
This button will delete any selected images.

RADIUS Settings

If the Security Mode is set to RADIUS in the General Security section then the RADIUS Security Settings configurable in this section will be in use.

For a complete description and explanation of RADIUS security, please refer to the RADIUS Security Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.



Radius General

Fallback Mode
This menu toggles between NONE and USER PROFILES. If the unit gets no response from any RADIUS server when attempting to authenticate a user, no further action is taken if this option is set to NONE. The unit falls back to the User Profiles configuration for authentication if this is set to USER PROFILES. The default setting is NONE.

CHAP
This is an ON/OFF toggle to set whether the unit uses CHAP (Challenge-Handshake Authentication Protocol) authentication when using RADIUS. ON sets authentication to CHAP. OFF sets authentication to PAP (Password Authentication Protocol). The default setting is OFF.

Authentication Port
Set the UDP port (1 - 65535) that the RADIUS server uses for authentication/authorization. The default port is 1812.

Accounting Port
Set the UDP port (1 - 65535) that the RADIUS server uses for accounting traffic. Set to 0 to disable RADIUS accounting. The default port is 1813.

Retries
This option sets the number of times (1 - 30) the unit should try a RADIUS request again after getting no valid response. Valid meaning a response that is verified as really coming from the RADIUS server. The default setting is 3.

Timeout (seconds)
This option sets the number of seconds (1 - 30) the unit waits for a response from the RADIUS server. The default setting is 3 seconds.

Radius Servers

Primary / Secondary Server
Set the IP Address or host name of the primary and secondary RADIUS server.

Primary / Secondary New Secret / Confirm Secret
Set the secret for the primary and secondary RADIUS server. The secret is used to authenticate RADIUS network traffic. The maximum length for each is 16 characters.

Access Control

The Access Control function keeps a table of access control devices in the unit. On the current firmware version, up to three devices are supported.

The SiteBoss access control system can use a standard Wiegand interface or a more custom system can be configured using the units Scripting functions.

The SiteBoss listens for any transmissions from the Wiegand interface. If the SiteBoss receives a card serial number it is compared to the user table and schedules. If there is a match then the unit activates the door strike relay for the configured delay time and then deactivates it.

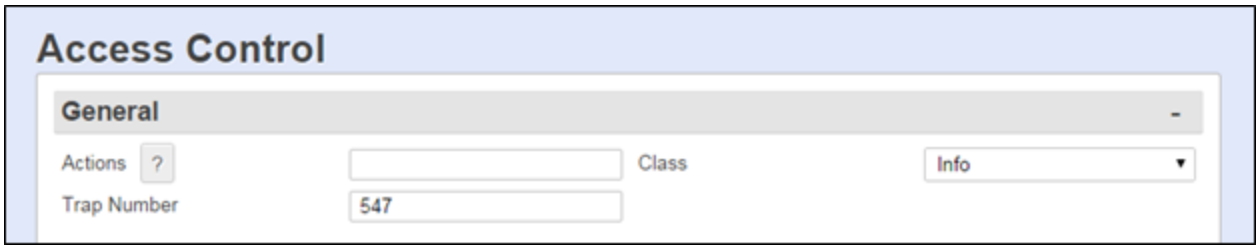
For additional information see the Wiegand Card Reader Feature Guide on the Asentria Information portal or contact Asentria Technical Support.

Access Control General

The Wiegand ACD runs on units equipped with a Wiegand interface. Each Access Control Device monitors:

Access granted
Access denied

The unit generates an event on these occurrences. It also posts these occurrences to the audit log, if the audit log is enabled. The unit does not post anything to the events log regarding this feature.



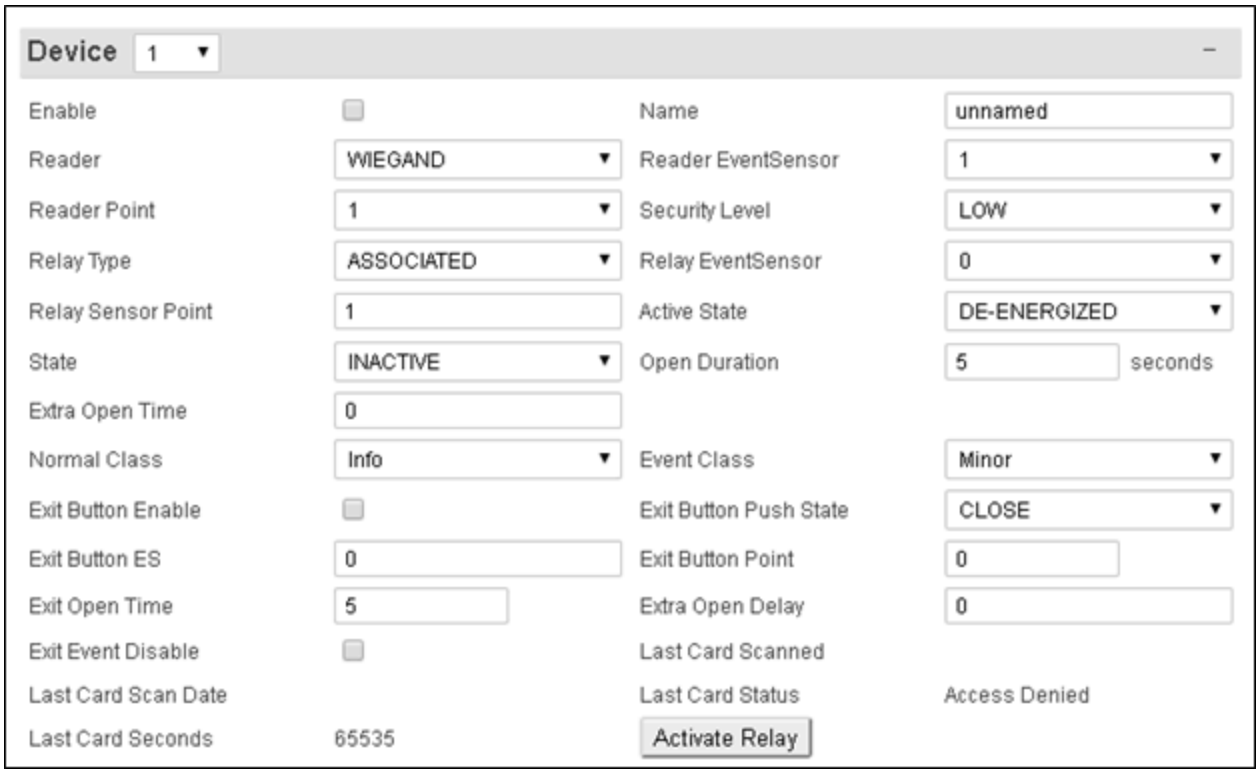
Actions
This text field is used to set the action(s) the SiteBoss should take upon an access granted or access denied event. The button with the "?" will displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Class
This drop-down menu allows for configuring the severity class for the Access Control event. The available drop-down options will be a list of the classes previously defined using the Class Table menu button.

Trap Number
This text box sets the Trap Number to be sent with any SNMP traps for this event. The default is 547, but this can be set in the range of 1000 ? 1199 as needed.

Device

Device
This is a drop-down box to choose which device to configure. On the current firmware version, up to 3 devices are supported.



Enable
This is an ON/OFF checkbox to enable management for the selected access control device. The default is OFF (unchecked).

Name
This text field is used to configure a name of the access control device. This field is for information purpose only and has no effect on the Access Control functionality. The name will be displayed on any configured event messages. The maximum length is 48 characters.

Reader
This setting allows for selecting the type of Access Control device. The available options are WIEGAND and SCRIPTED. The Default is WIEGAND.

Reader EventSensor
This drop-down box is used to select which EventSensor slot in the SiteBoss is used to control access. This is the slot the Wiegand point is in or the EventSensor slot the script is using. The default is 1.

Reader Point
This drop down allows for setting which sensor point on the defined device is connected to the card reader. The Wiegand card on an S360 only has one Weigand point (D1 and D0), so this should be set to 1. The default is 1.

Security Level
The Security Level drop down is used to set the security level a user will need to have in order to open the access point.

Relay Type
This drop-down box sets the type of relay used to control the door strike. The RW relay on the Wiegand EventSensor card would be set to ASSOCIATED. Any other relay on the unit can be used, but this setting would be set to EVENTSENSOR.

Relay EventSensor
This drop-down box is used to select which EventSensor has the relay connected to the door strike. This would be the number of the card, or external EventSensor, that is wired to the door strike. The default is 200, meaning a one of the lower main unit relay points.

Relay Sensor Point
This drop-down box defines which relay on the expansion card or EventSensor selected in the "Relay EventSensor" setting is connected to the door strike. If the RW point is used, this setting should be set to 1.

Active State
This field defines what the access point open state is. ENERGIZED is used for a door strike type lock, where the relay is energized to unlock the door. DE-ENERGIZED is used for an Electromagnetic lock that is uses the energized relay to maintain the door locking magnets. It De-Energizes to unlock the access point.

State
This in an unused setting drop down and has no functional use at this time.

Open Duration
This text field sets how many seconds that the lock should be held open once access is granted. The default is 5 seconds.

Extra Open Time
This settings is used to give a user that needs extra time for access some additional seconds beyond the Open Duration setting.

Normal Class
The drop-down boxes are used to set the severity class for the returning to normal event for this device. The available drop-down options will be a list of the classes previously defined at the Class Table option.

Event Class
The drop-down boxes are used to set the severity class for the access event for this device. The available drop-down options will be a list of the classes previously defined at the Class Table option.

Exit Button Enable
This is an ON/OFF checkbox to enable a door exit button.

Exit Button Push State
This drop down box sets the state of the contact closure for the Exit Button setting, OPEN or CLOSE. This would set to identify if the button is closing the contact closure to trigger the door unlock (Close) or opening the contact closure to trigger the door unlock (Open)

Exit Button ES
This setting defines the EventSensor connected to the Exit Button. Available settings are

NONE, 200 (internal) or 1-16.

Exit Button Point
This setting defines the point on the EventSensor defined at Exit Button ES that is connected to the Exit Button.

Exit Open Time
This text field sets how many seconds that the Exit will remain unlocked after the Exit Button is pushed. The default is 5 seconds.

Extra Open Delay
This option set a delay in seconds after exit button is pushed before starting the Exit Open Time. The default is 0, no delay.

Exit Event Disable
This checkbox is an ON/OFF to disable sending exit button events. The default is OFF (unchecked).

Last Card Scanned
Displays the serial number of the last card scanned.

Last Card Scan Date
This displays the date of the last card scanned.

Last Card Status
This displays the status of the last card read.

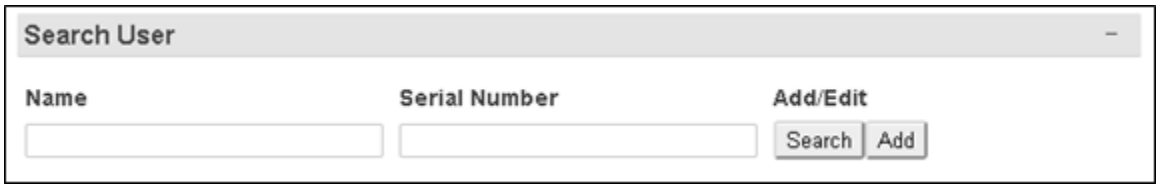
Last Card Seconds
This field displays how many seconds since the last GOOD card was read.

Activate Relay
Clicking this button causes the relay corresponding to that device to activate per the settings configured. The unit causes the door mechanism to behave in a manner similar to an actual, successful card scan - unlock the door for the amount of time configured in the Open Duration and then lock the door after that time has elapsed.

Search User

Click Search with blank fields to show all the users. To look for a specific user, type in part of a name to show users with that exact string in their name. The system will also search using all or part of a serial number.

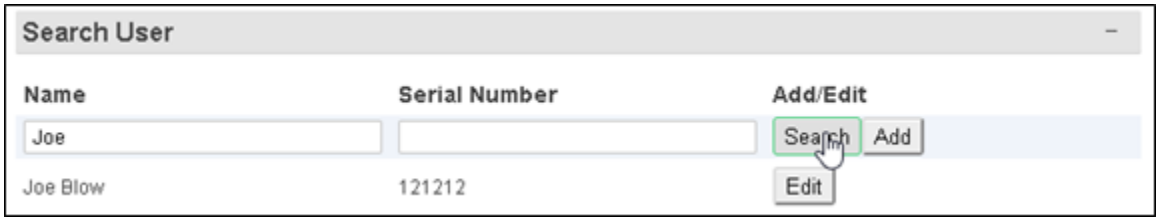
The results of a search will have an Edit button next to each user.



Name
Enter a name or partial name string for the system to search for, then click Search.

Serial Number
Enter a serial number or a partial number for the system to search for, then click Search.

Search
To look for a user already in the SiteBoss Access Control system enter a partial or full name and/or serial number in those fields and click **Search**.



Add
To Add a new user, click the Add button and the Edit User options are available to enter a new user. Enter per the instructions below and click Submit at the top of the page.

Edit
To Edit and existing user, use the Search button to locate the user in the system and click the ?Edit? button associated with the name on right. The existing settings for that user will appear in the Edit User Section. Make needed changes and click the Submit button at the top of the page.

Edit User

Enable
This is an ON/OFF checkbox to enable the user. The default is OFF (unchecked). A disabled user is never granted access.

Name
This is a text field to enter or edit a Name for the user. The maximum length is 50 characters.

Serial Number
This text field is the Serial Number, RFID number, of the card associated with the user.

Pin

Enter any Keypad Pin number required for this user to access a site.

Schedule
This a dropdown box to select the schedule as configured in the next section that will apply to this user.

Extra Time
This is an ON/OFF toggle to add the Extra Open Time for this user if additional time is needed for access. The default is OFF (unchecked).

Security Level
This drop down box is used to set the Security Level this user can access. The Default is Low.

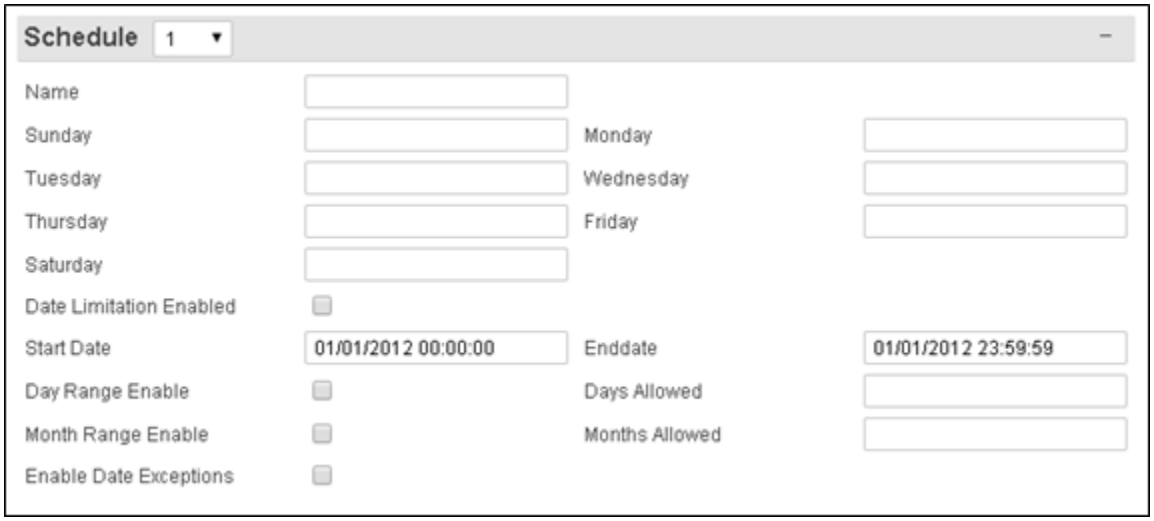
Times Allowed
How many times the user can will be allowed access. Set to 0 (zero) for unlimited access. Defaults to 100.

Times Accessed
This displays how many times a user has been allowed access.

Schedule

Schedules are used to limit access for users to specific times and days. These Schedules are then used when setting up Access Rules.

To and From dates and times are inclusive, access will be granted on the From date and time through the To date and time configured.



Name
This is a text field to name the schedule. The maximum length is 48 characters.

Day
For each day option, enter times the user should be allowed access to the site. Up to three periods a day can be configured. Example: 6:00-12:00,13:00-17:00,18:00-21:00

Date Limitation Enabled
This checkbox is an ON/OFF setting to enable/disable date limitations. The default is OFF (unchecked).

Start Date
This field sets the date and time to start allowed access inclusive, example 01/01/2012 00:00:00.

End Date
This field sets the date and time to end allowed access exclusive, example 01/01/2012 00:00:00.

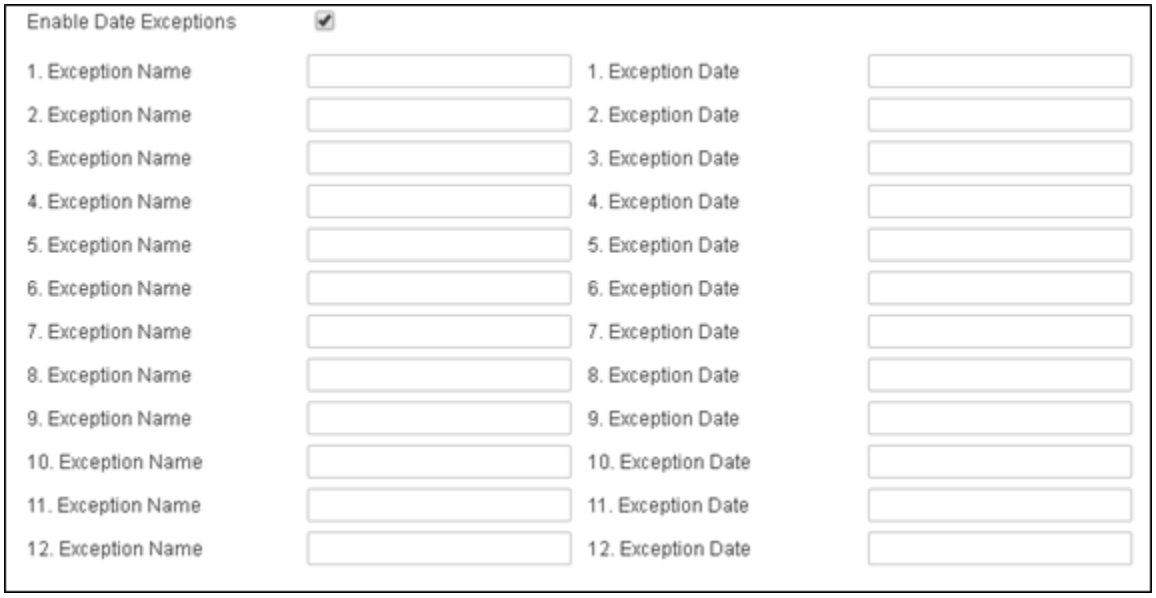
Day Range Enable
This checkbox is an ON/OFF to enable/disable the day limitations.

Days Allowed
This field sets the days when access is allowed, i.e. 3,4,10-15.

Month Range Enable
This check box is an ON/OFF setting to enable/disable month limitations.

Months Allowed
This field sets the Months when access is allowed, i.e. 1,3,5,10-12

Enable Date Exceptions
This is an ON/OFF setting to enable/disable date exceptions, when access will be denied. When checked additional settings options to define dates (like holidays) on which access is denied.



Exception Name
This is a text field to name the date, such as Christmas.

Exception Date
This field defines dates when the user will be denied access, month day and year are required (MM/DD/YYYY). The program just uses the month and day the year is required only because the structure and validation of the input requires this but it is not considered when checking the exception. So 12/25/2018 will work for last year as well as for next year on the same month/day.

Site Security

Site security options are used to manage intrusion alarms and related functionality.

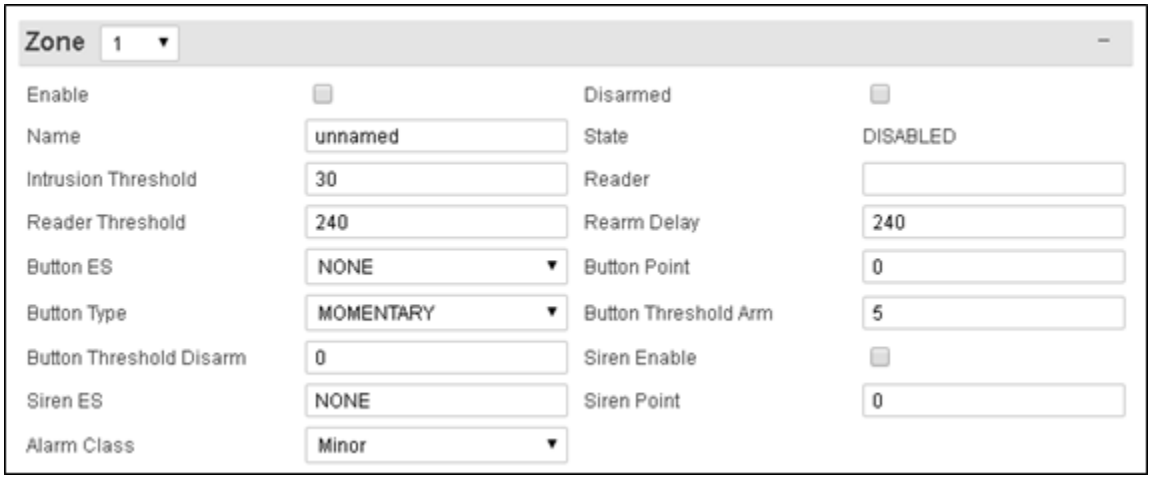
Zone

Up to 10 sensor zones can be configured individually with their own sensors and threshold settings.

If the zone is in the INTRUDER state, it can be set to the disarmed state by a valid entry of the selected reader, and/or via a button if one is installed and configured.

When the zone is disarmed and any sequence is executed to rearm the zone, the zone will become rearmed after Rearm Delay threshold is reached. However, it the zone is rearmed by an override from the NOC this occurs immediately.

Access control using card readers or other scripting electronic access function is handled by the Access Control settings. If there is no reader of any type and instead we are using a hidden button, we interface to that button here.



Enable
This is an ON/OFF checkbox to enable or disable the zone security settings for this zone.

Disarmed
This is an ON/OFF checkbox to Disarm or Arm the zone.

Name
This is a text field to name the zone with a maximum length of 48 characters.

State
This is a display field display the current state of the zone. Possible states are ARMED, DISARMED, DISABLED, INTRUDER, and REARMING.

Intrusion Threshold
This sets a threshold for how long the unit will wait for a disarm input before triggering the alarm functions.

Reader
This field sets which reader(s) arm and disarm this zone. This would be defining the reader device(s) configured in Access Control. The options are 1, 2 or 3.

Reader Threshold
This setting sets how much time the user has between a reader event to enter a pin or press a button for disarming the site.

Rearm Delay
This setting sets a threshold to wait for no motion before rearming the zone. This would configure the SiteBoss to automatically rearm a zone. Set to zero to disable the feature.

Button ES
If the site does not use a card reader a button contact can be used to manually arm/disarm site. This setting defines which EventSensor is connected to the button.

Button Point
This setting defines which contact point is connected to the button contact defined at Button ES that is used to manually arm/disarm site.

Button Type
This defines the type of button used to manually disarm the site. The options are MOMENTARY or TOGGLE. Momentary supports a momentary push button that toggles between the two states, Armed and Disarmed which would use the Button Threshold Arm and Button Threshold Disarm settings to define how long to hold the button to arm or disarm the zone. Toggle would be an ON/OFF type switch which would manually set the state to Armed or Disarmed.

Button Threshold Arm
This setting configures how long a MOMENTARY type button would need to be pressed to arm the zone. It is expected that the arm threshold is longer than the disarm threshold. If the site is armed and the button is held down for configured seconds or more to arm the site, the site would stay armed.

Button Threshold Disarm
This setting configures how long a MOMENTARY type button would need to be pressed to disarm the zone. It is expected that the disarm threshold is shorter than the arm threshold, e.g. 1 vs 5 seconds. If the site is armed and the button is held down for 5 seconds, the site would stay armed.

Siren Enable
This is an ON/OFF check box to enable or disable a relay output controlling a Siren.

Siren ES

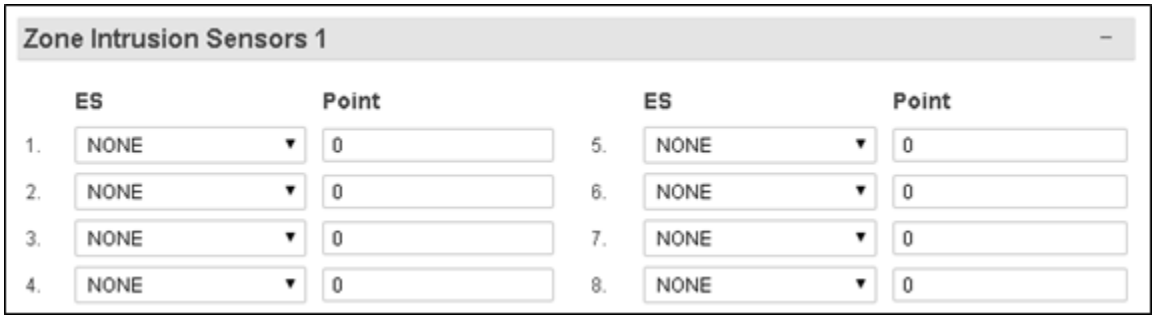
This setting defines which EventSensor has the relay controlling the siren. The options are 200 (on board relay) or 1 through 16.

Siren Point
This setting defines what point on the EventSensor is the relay connected to a siren.

Alarm Class
The drop-down boxes are used to set the severity class for the alarm. The available drop-down options will be a list of the classes previously defined at the Class Table option.

Zone Intrusion Sensors

The Intrusion Sensors are sensors that tell the unit that there is a person in the zone. These are usually motion sensors.



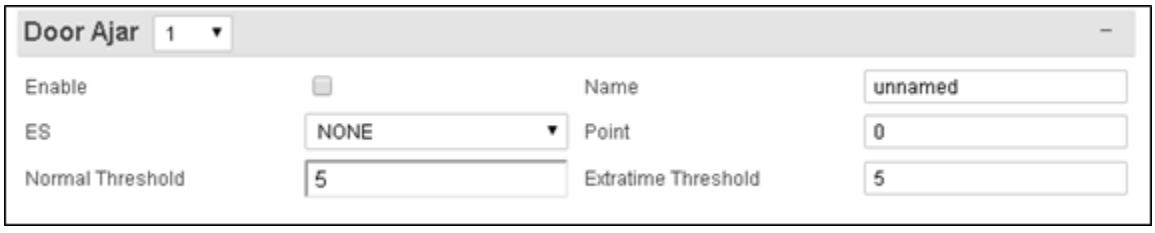
ES
This is the EventSensor connected to the motion sensor. The options are 200 (on board contact point) or 1 through 16.

Point
This defines the sensor point on the defined ES which is connected to the motion sensor.

Door Ajar

These settings are used to configure an alarm if a door is left open.

Door Ajar n
The drop down in the grey bar us used to configure multiple entry points with separate alarm settings. Up to 10 separate alarm configurations can be set.



Enable

This is an ON/OFF check box to enable or disable this ajar sensor.

Name
This is a text field to name the access point. There is a maximum length of 48 characters.

ES
This is the EventSensor connected to the door sensor. The options are 200 (on board contact point) or 1 through 16.

Point
This defines the sensor point on the defined ES which is connected to the door sensor.

Normal Threshold
This setting sets a threshold of an allowable amount of time for door left open. If the door is open longer than the defined number of seconds a Door Ajar alarm is triggered.

Extra Time Threshold
A user that needs some extra number of seconds to access or door entry can be configured to have an extra time threshold to delay any alarm trigger using this setting.

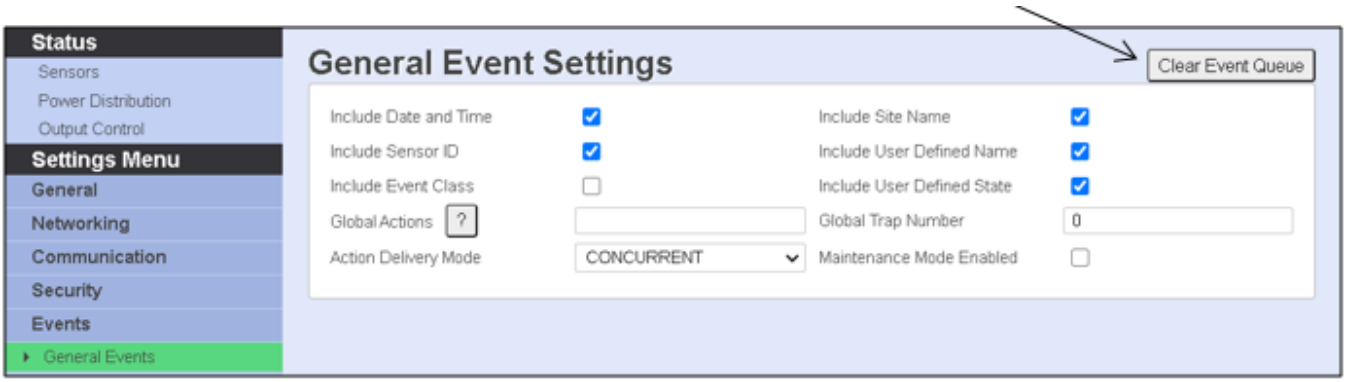
►Events

The Event section is used to set up actions the SiteBoss should take in response to sensor events, scheduled events, serial handshaking events as well as actions the unit should take in response to a reset or a power cycle.

General Events

This menu that permits customization of the event message that appears in traps and Emails as well as setting global action parameters.

Clear Event Queue
This button deletes any event that has been triggered but the delivery actions have not yet been completed. You will get a "Are you sure you want to clear the event queue?" prompt. Clicking OK will clear any undelivered event messages.



Include Date and Time / Site Name / Sensor ID / User Defined Name / Event Class /

User Defined State
These are each ON/OFF checkboxes that permit customization of the event message that appears in SNMP traps, Emails, SMS messages, pages, etc. sent by the SiteBoss. Default setting for each is ON (checked) except for Include Event Class which is OFF (unchecked).

Global Actions
The Global Actions feature enables an administrator to configure actions that are automatically appended to any other action list when that other action list executes. If all actions for all events on a unit are to be the same then using global actions and trap number means easier management.

An action called "NONGLOBAL" can be inserted at the beginning of any event's action list to mean that any global actions and global trap number should not apply to that event. If the NONGLOBAL action is inserted in the action list, it must be inserted first in order to unambiguously tell the unit that actions to process should be excepted from global treatment.

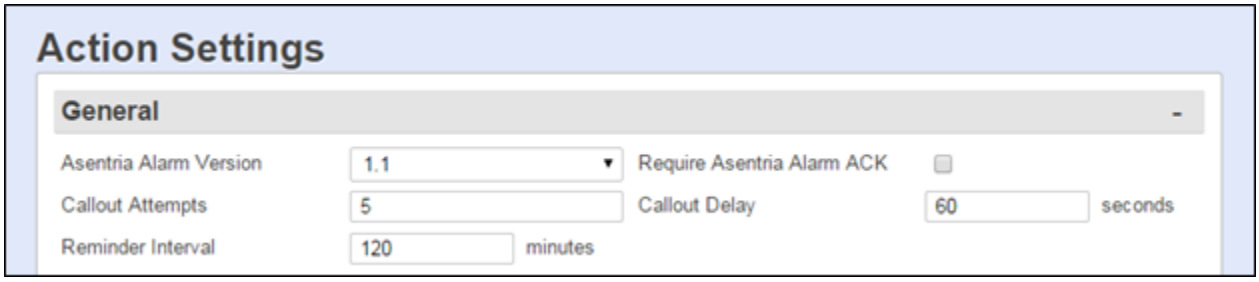
This is a text field. See the Actions List or click the large "?" for specific syntax to define the Global Action(s) for the SiteBoss.

Global Trap Number
This trap number overrides the trap number defined for any other event, even if there are no global actions configured. Setting this value to 0 disables the effect. The default setting is 0.

Action Delivery Mode
This is a drop-down box to choose between CHRONOLOGICAL or CONCURRENT. The CONCURRENT configures the unit to process multiple event actions immediately, regardless of whether previous actions have been completed or not. CHRONOLOGICAL configures the SiteBoss to process event actions in the order in which they occur, so that one action does not get processed until the previous action is completed. The default is CONCURRENT.

Maintenance Mode Enabled
Maintenance mode ON (checked) means that while enabled, no alarms whatsoever are sent; no traps, no REST Push messages, no alarms. When its OFF (unchecked) then everything works as normal. OFF is the default.

General Actions
This menu is used to configure a majority of the possible actions that could occur when events are detected.



Asentria Alarm Version

This drop-down box toggles between 1.0 and 1.1 to indicate which type of Asentria Alarm notification will be displayed. Set this 1.0 for the dialup POTS modem, which is not applicable for an S550A. Set it at 1.1 for TCP when using other delivery methods for your alarm actions. The default setting is 1.1

Require Asentria Alarm ACKs
This checkbox is an ON/OFF toggle to enable or disable forcing the unit to require an acknowledgment when first connecting, and after each Asentria Alarm. If disabled, the SiteBoss will allow non-CRC mode where Asentria Alarms are delivered without waiting for any indication that the messages were properly delivered. If enabled, CRC mode is required by the SiteBoss. The default setting is OFF (unchecked).

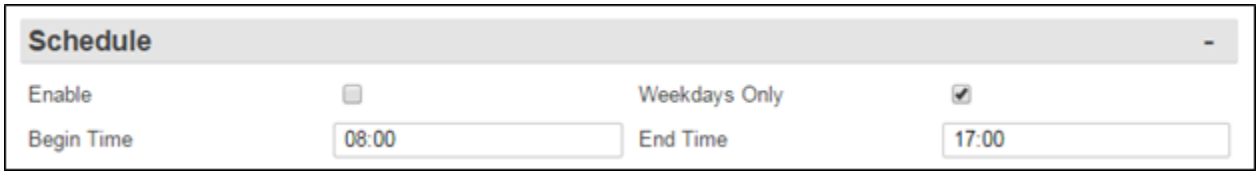
Callout Attempts
Use this field to set the total number of times to attempt dispatch, Malert or POTS modem callouts if previous attempts fail. The default setting is 5. This setting is not present on an S550A.

Callout Delay
This field sets the time in seconds (0 - 400) to wait between POTS modem callout attempts. The default setting is 60 seconds. This setting is not present on an S550A.

Reminder Interval
This field sets the time in minutes (0 – 65535) to repeat an action if the sensor (contact closure, temperature, humidity, or voltage) that triggered the alarm is still in the active or alarm state. When the sensor has been returned to the inactive state, the reminder interval is no longer in effect. The default setting is 120 minutes.

Schedule

The Action Schedule Settings menu allows event actions to be limited to defined days and times. If the Schedule is not Enabled the rest of the settings will not be active in the SiteBoss.



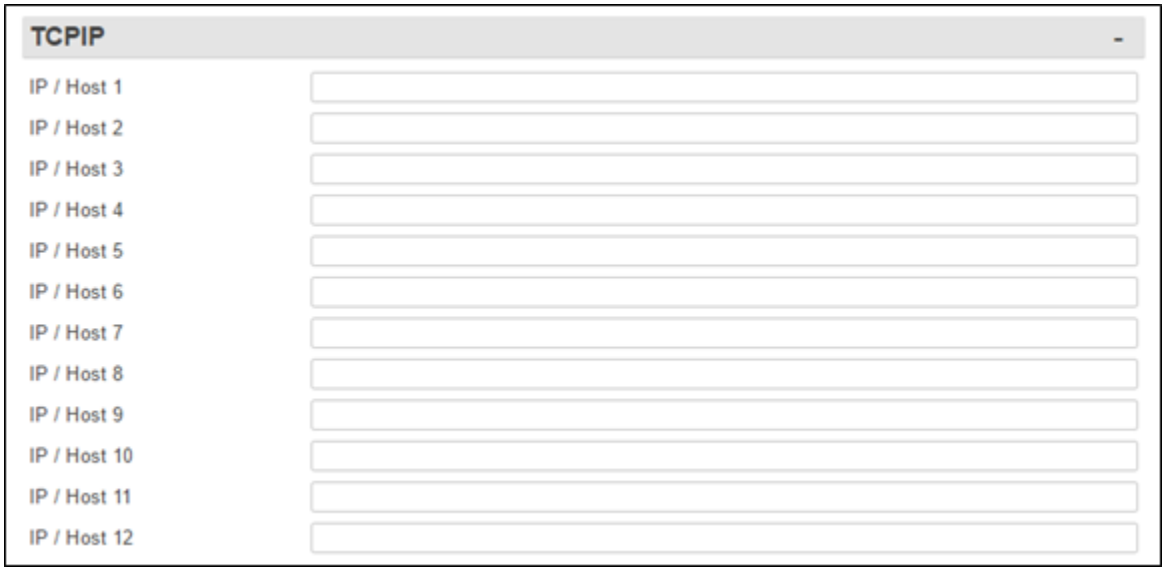
Enable
This checkbox is an ON/OFF toggle to enable the action schedule. The default setting is OFF (unchecked).

Weekdays Only
This checkbox is an ON/OFF toggle to set whether actions are only performed Monday thru Friday. The default setting is ON (checked). This option is only active if the Action Schedule has been Enabled.

Begin Time / End Time
Use these options to set the beginning and ending times (24 hour clock) during which alarm actions can be taken. The default settings are 08:00 (Begin Time) and 17:00 (End Time). These fields are only active if the Action Schedule has been Enabled.

TCPIP

Use these menu options to configure the IP addresses or Host names to use for easier reference in event actions. Additional network settings may need to be configured so that your unit can reach any defined IP address or host. See the Network section of this manual for additional information and settings instructions.

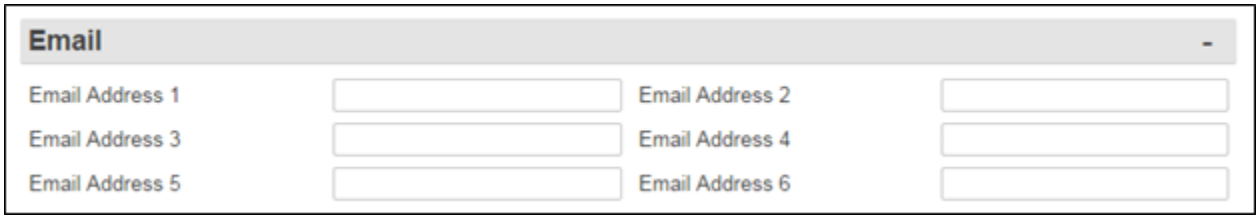


IP / Host n

Use these menu options to configure the IP addresses or Host names to use for easier reference in event actions. The number (1,2,3, etc.) corresponds to the "index" number for Traps and informs as discussed in the Actions List chapter. These can be any relevant server, such as an SNMP management system.

Email

This section is used to define email destinations for event actions. Additional network settings will need to be configured for the unit to be able to send SMTP traffic. See the Email section in the Networking chapter for additional details.



Email Address n

Use this option to configure Email Addresses to use for easier reference in event actions. These email addresses can also be set to cell phone numbers, using the service provider's SMS gateway address, to allow for SMS alerts to be sent. Ex: 2065555555@vtext.com. The

number (1, 2, 3, etc.) corresponds to the "index" number for Email alerts as discussed in the Actions List chapter.

Dialout

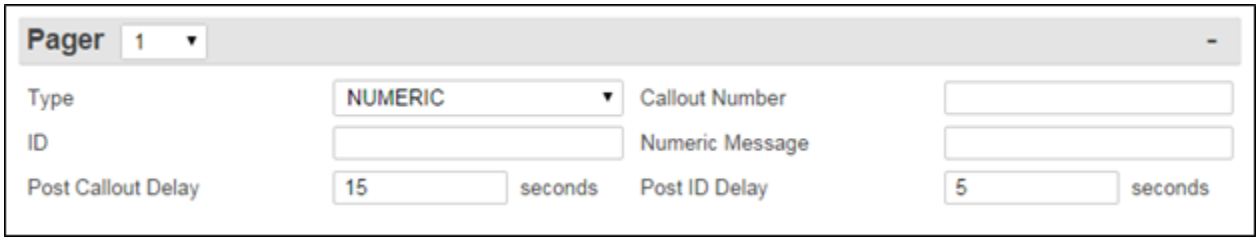
These options are used to set the phone numbers for the serial POTS modem or to use for SMS messages if a wireless modem is installed. These settings are used for the event action strings. Additional network configurations will need to be set to allow for the messages to be successfully delivered. See the PPP section in the Networking chapter for a serial modem and the Wireless Modem section for information on connect the Wireless Modem.

Phone Number n

Use these fields to set the phone numbers (index 1,2,3,4) to call for each dispatch, malert or modem callout as discussed in the Actions List. These actions can only be used if the optional POTS modem card has been installed.

Pager

This menu is used to configure pager call outs used in event actions. Pager call outs can only be used if an optional POTS dialup modem card is installed in the SiteBoss. These settings are not present in an S550A



Pager

The drop-down box in the Pager section header allows for up to four separate Pager call out configurations.

Pager Type

This drop-down box toggles between NUMERIC and ALPHA to select the type of pager to call. The default is NUMERIC.

Pager Callout Number

Use this field to set the phone number for the pager.

Pager ID

This function is used only with paging systems where many pagers share the same phone number. This is common with alphanumeric pagers.

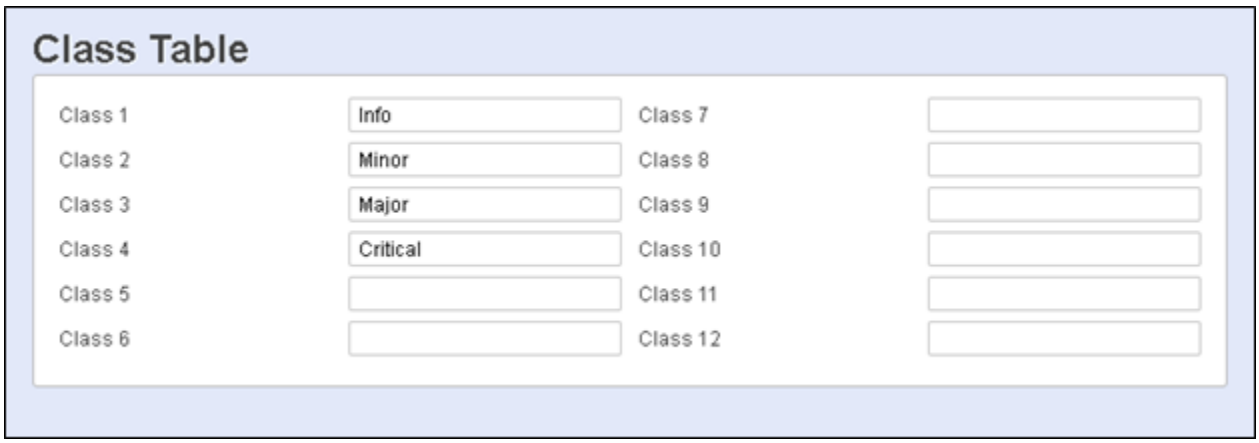
Numeric Message
This option is the series of digits (typically callback number) sent to a numeric pager.

Post Callout Delay
This field sets the number of seconds the unit will wait before sending the pager ID. The default is 15 seconds.

Post ID Delay
This field sets the number of seconds the unit will wait before sending any message data. The default is 5 seconds.

Class Table

The Class Table is used to set the Class severity levels used for event notifications.

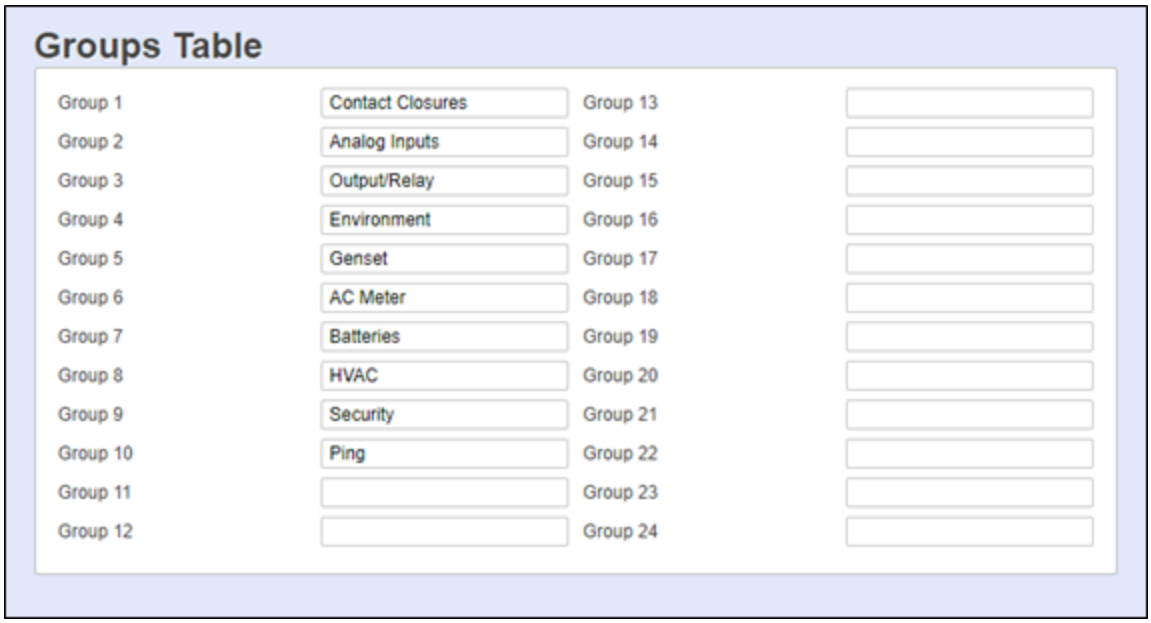


Class n
These fields are used to define the severity levels that are assignable to events detected by the SiteBoss. Maximum length is 47 characters. Info, Minor, Major, and Critical are the default class names assigned to the first four classes. These can be changed and others added as desired to meet your specific needs.

The class number and name are reported in SNMP traps, emails and Talerts. It is a mechanism for you to provide varying severities for different alarms so that you can act on them upon receipt.

Group Table

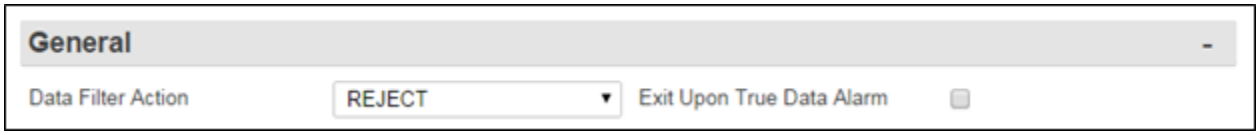
Each EventSensor will have a "Group" drop down to categorize the alarm point into subjective group types on custom pages or in Alarm Manager or other Network Management Software.



Data Alarm/Filters

A Data Event is a group of settings configured to generate an alarm when specified characters or alpha/numeric strings are received by the SiteBoss. For more information on Data Alarms see the Data Alarm and Event Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support.

Data Alarm General



Data Filter Action

The Data Filter Action option toggles between REJECT and ACCEPT to indicate whether data filters are configured to reject or accept specific incoming data string(s). The default setting is REJECT.

» **Note:** If no Data Filters are configured, and the Data Filter Action option is toggled to ACCEPT, then no incoming data will be buffered in any of the files. This field should always be set to REJECT unless there are Data Filters specifically configured for accepting only certain data.

Data Alarm functionality is not on the S550A at this time.

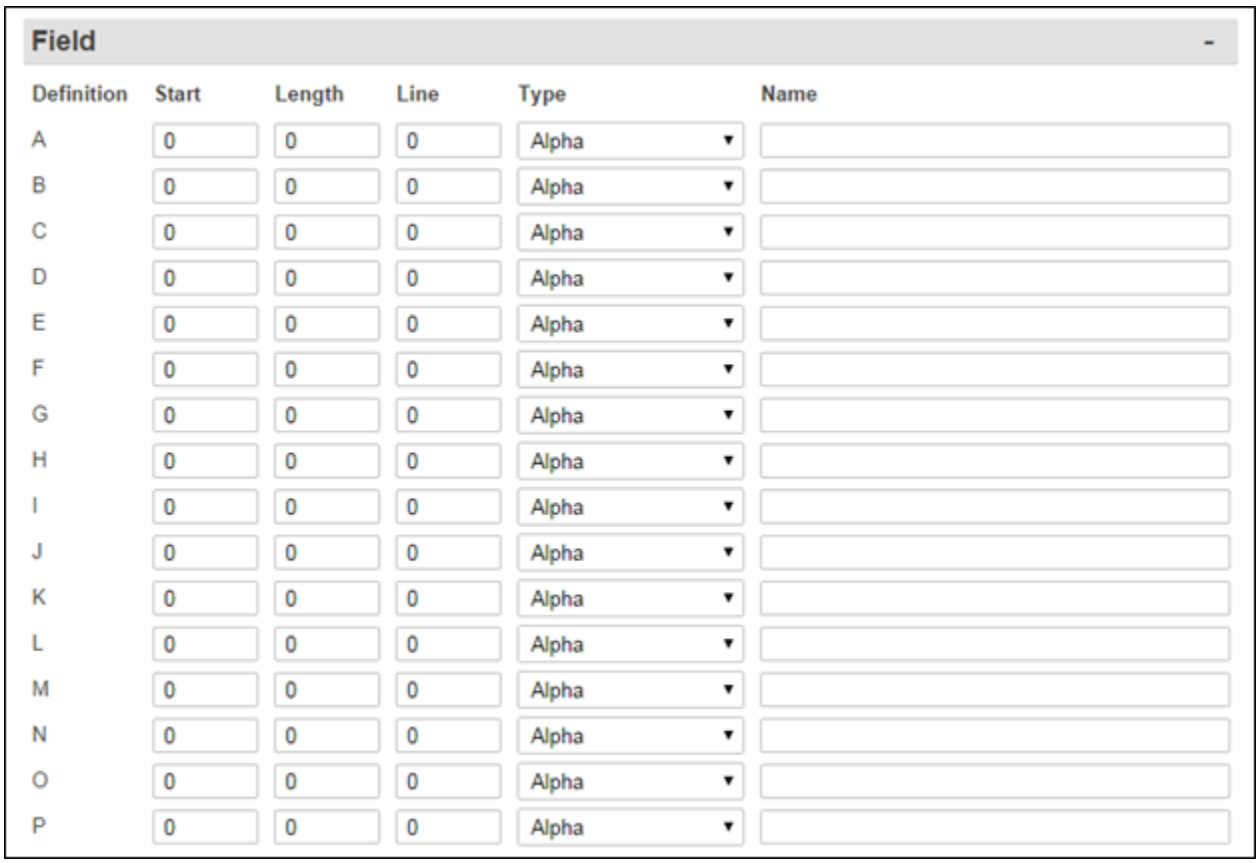
Exit Upon True Data Alarm

This is an ON/OFF checkbox to set whether the SiteBoss will stop processing more data event evaluations on a single record after it has found one match. This should be disabled if it is possible to have more than one event in a single record. This is a global setting – it applies to

ALL configured data alarms. The default setting is OFF (unchecked).

Field

This section is used to set up to 16 data alarm fields. These fields define an exact field, text or number, to be used in a data equation.



Start

Use this text box to set the number of the characters to begin a particular alarm field starting from position 1. The Field is disabled if set to 0. The default setting is 0.

Length

This text box is used to set the length of this particular alarm field. The default setting is 0.

Line

This text box is used to set the optional line number the field should be limited to in multiline records. Default setting is 0.

Type

This drop-down box option toggles between Alpha and Numeric. Alpha is used for most alphanumeric data alarming, and Numeric is used if you need to alarm on a range of numbers. The default setting is Alpha.

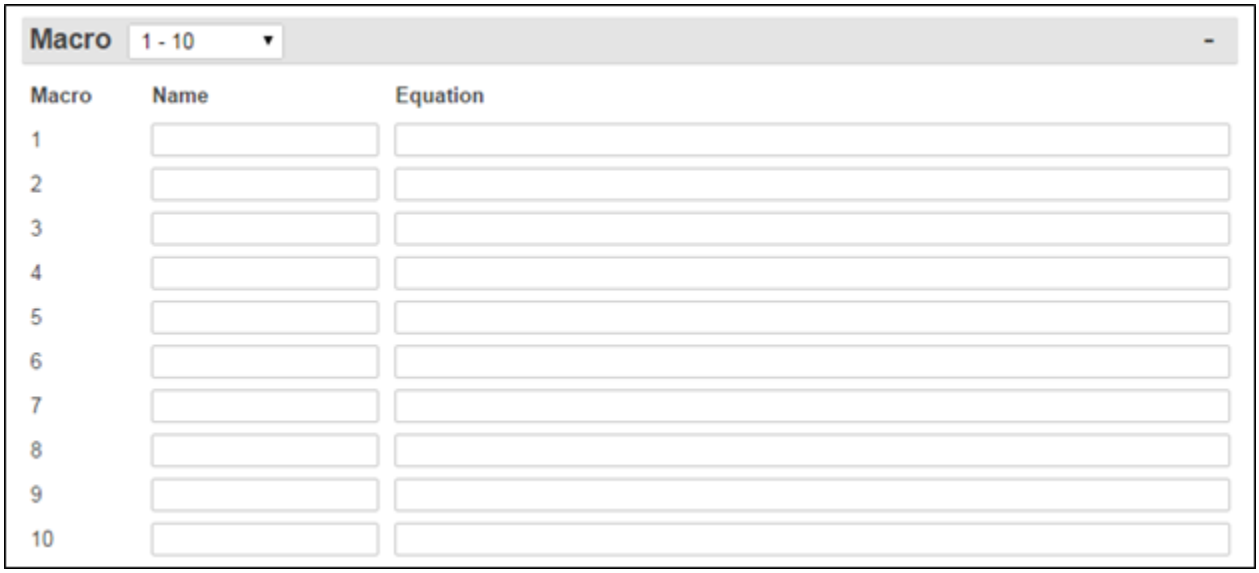
Name

This text box is used to define the name the alarm field. This name must be unique, is limited to 12 characters, and it must not contain any spaces. It can contain alphanumeric characters and the underscore, but *it must start with a letter*. Field names are case sensitive. If left blank, you can refer to the field by its field letter (A, B, etc. …).

» **Note:** Field names cannot start with $.
» **Note:** Do not start a field with AND or OR.

Macro

Data alarm macros provide a way to define up to 100 equations that can be used in one or more data alarm equations. Each macro consists of an equation and an associated name that can be used to reference the macro in a data alarm equation. They simplify the creating of data alarm events, particularly where more than one event uses the same expression in its equation. Refer to the Data Alarm and Event Feature Guide Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.



Name

The macro name is the name by which the macro is referenced in any data alarm equation, and can be up to 16 characters in length. Macro names and data field names are not case sensitive. A macro cannot be given the same name as a data field or another macro.

Equation

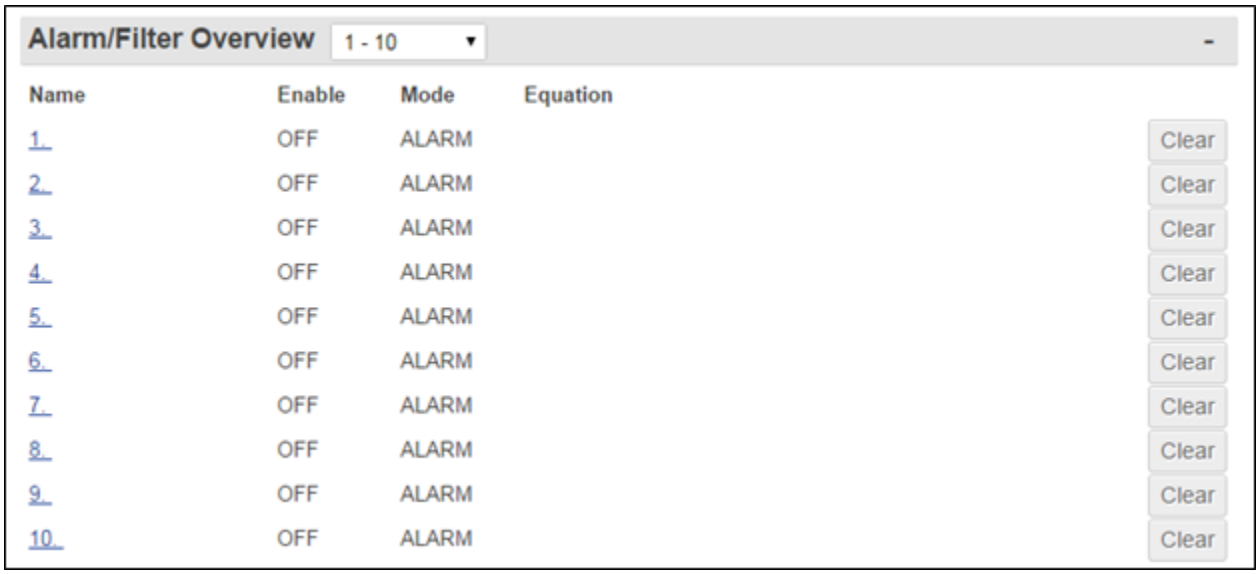
The macro equation is entered the same way as a data alarm equation. A macro equation cannot refer to another macro. The macro equation can be up to 160 characters in length.

» **Note:** Macro names cannot start with $.
» **Note:** Do not start a macro name with AND or OR.

Alarm/Filter Overview

Data alarms are configured by selecting an option from the Alarm/Filter Overview section of

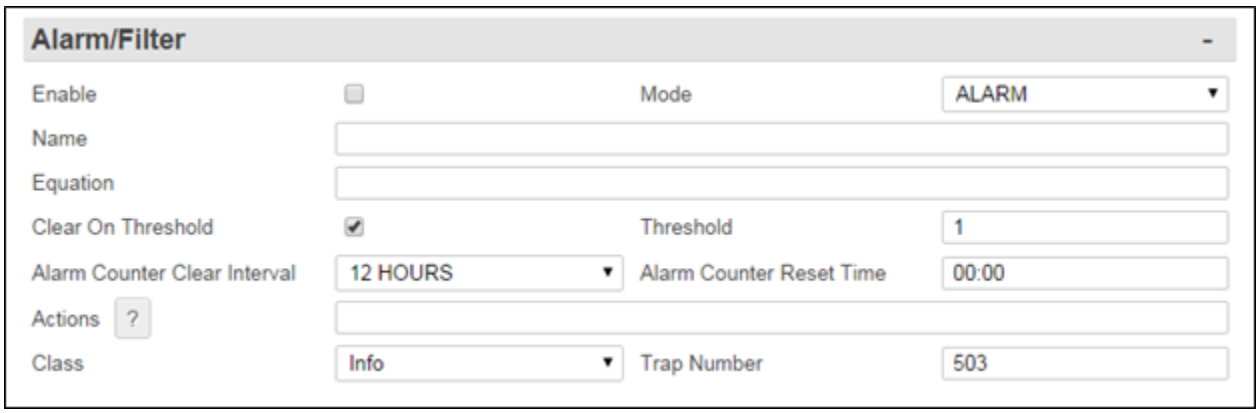
the page. The grey bar has a drop-down menu to choose a group of options in batches of ten. Select an Alarm/Filter option from 1 to 100 by clicking the blue number hyperlink. The next lower section of the page will display a menu where the settings for that specific Data Alarm can be configured.



Clear

The Clear button will clear the counter for the selected data alarm. This happens as soon as this option is selected.

Alarm/Filter



Enable

This is an ON/OFF checkbox to enable this data event monitor. The default setting is OFF (unchecked).

Mode

This drop-down box toggles between ALARM and FILTER to indicate whether the SiteBoss will recognize this data event as an Alarm and take some action, or as a Filter and either accept or reject the data string. The default setting is ALARM.

Name
This is a text box to set the name for the event monitor. This name is reported with the specified actions. The Maximum length is 16 characters.

Equation
This text box defines the event equation using the event fields defined in the previous menu. The Maximum length is 160 characters. Refer to the Data Alarm and Event Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.

Clear On Threshold
This is an ON/OFF checkbox to control whether the unit will clear the event counter each time the threshold is reached. If the event counter is allowed to grow beyond the threshold, the unit will not trigger an event again until after the counter is reset. The default setting is ON (checked).

Threshold
This field sets the number of times the event equation must be matched before an event is triggered. The default setting is 1.

Alarm Counter Clear Interval
This is a drop-down box to set an interval at which the unit should clear the match counter for an individual data event. The available options are: 2 hours, 4 hours, 6 hours, 8 hours, 12 hours, Daily, and Never. The first clear occurs at midnight. The default setting is 12 Hours.

Alarm Counter Reset Time
This field is used to set the time at which the daily clear should take place if it is enabled in the Alarm Counter Clear Interval. This value is in 24-hour format. The default setting is 00:00.

Actions
This text field is used to set the action(s) the SiteBoss should take if the defined Alarm threshold is reached. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Class
This drop-down box is used to set the class for the alarm. The available drop-down options will be a list of the classes previously defined at the Class Table tab.

Data Alarm Trap Number
This box is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number is 503, but any number in the alternate range of 1000 – 1199 can be used.

EventSensors

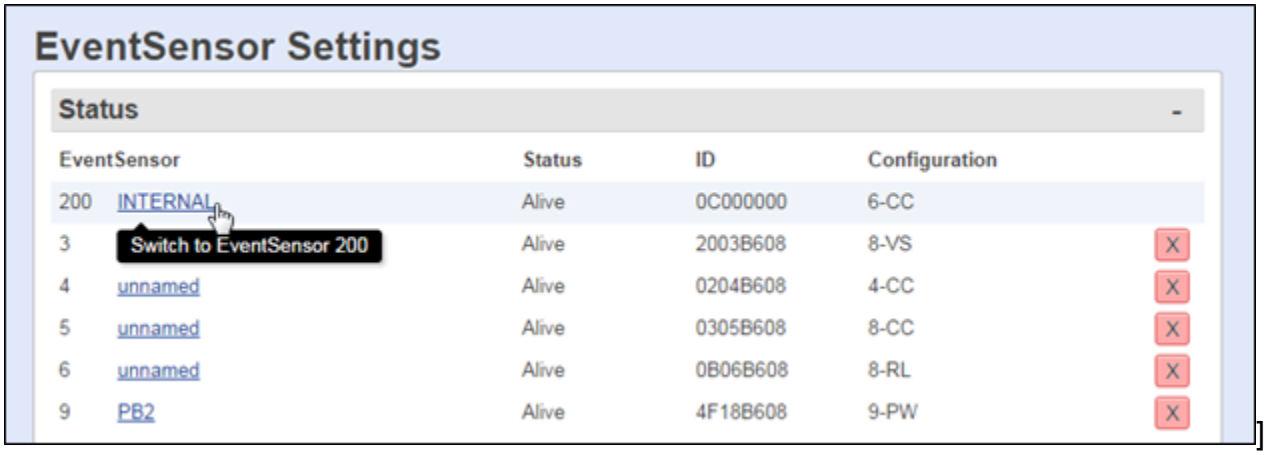
The SiteBoss supports a wide variety of internal and external sensor devices and relays, including contact closures, temperature and humidity sensors, analog voltage and current sensors. For the purposes of clarity, all of these will be generally referred to as "EventSensors" (ES) unless a specific type of sensor or relay is being described.

If there are no internal sensors or relays, or remote ES modules connected, this menu will be unpopulated except for the two internal serial I/O ports shown as "2-CC". The two serial ports can be configured as contact closures.

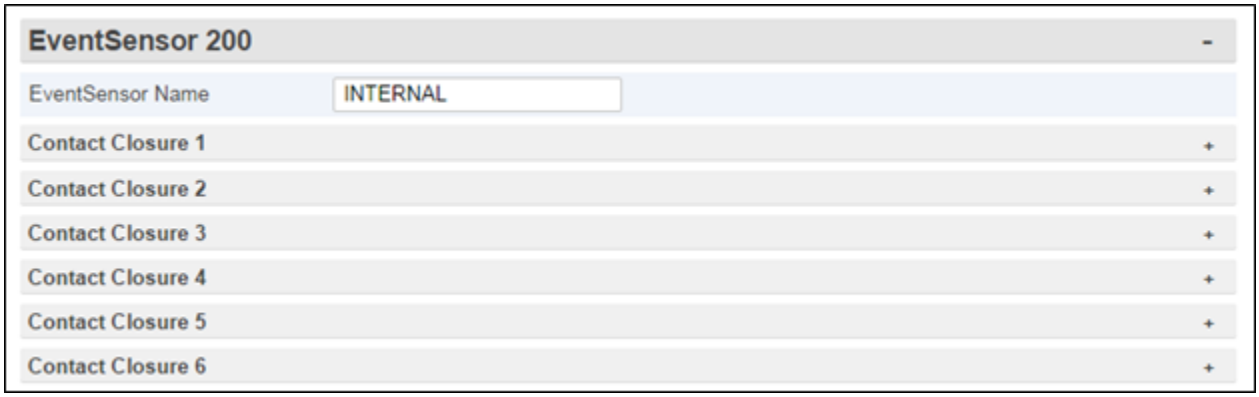
Because of the numerous ES configurations possible, example menus shown in this section will not look exactly like the ones for your SiteBoss.

The example menu below shows EventSensor Settings Status screen for an SiteBoss with the two internal serial I/O ports and a 4S RS232 Serial Port expansion card in slot 2 (which makes the internal option a 6-CC), an 8V Analog Voltage Input card in slot 3, a Wiegand Access Control card in slot 4, an 8C Contact Closure Card in slot 5, an 8R Relay card in slot 6 and it has a PowerBoss 2 connected to the Sensor port set to slot 9. It also has a Modem slot card in slot 1, which does not display in the EventSensor menus, since it is not a sensor.

The SiteBoss supports a maximum of 16 EventSensor slots.



To configure the sensor and event settings click the blue text associated with the slot and the lower section of the page will display the event settings for that EventSensor.



EventSensor Name

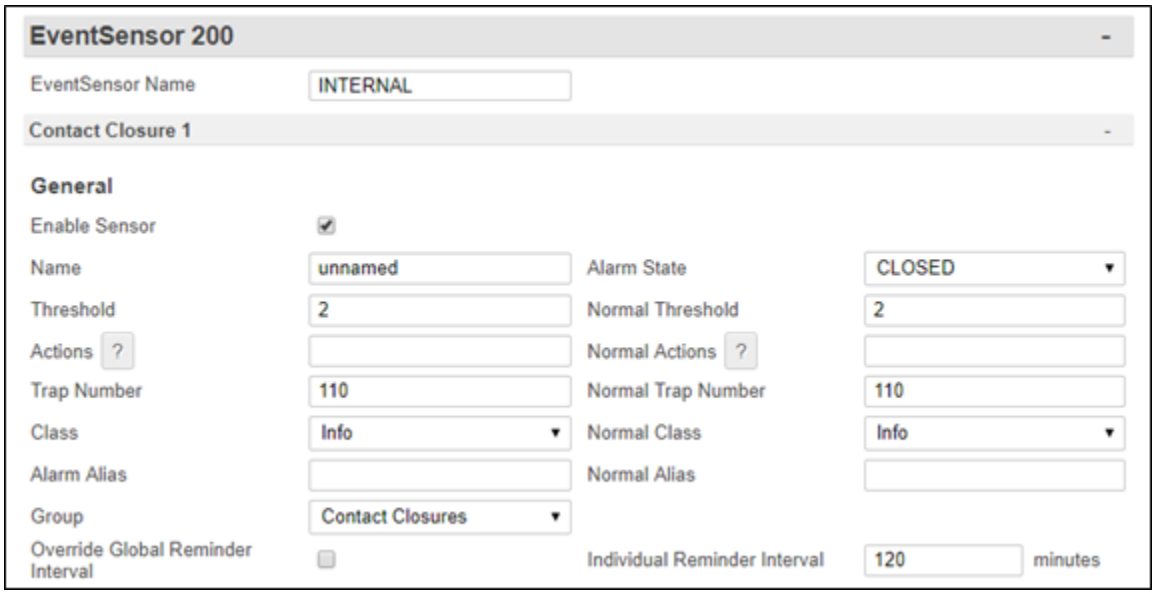
The EventSensor Name is a text field will names the sensor and will display in the upper menu section as well as in traps, e-mails and on the EventSensor Status page. The maximum length is 60 characters.

Click any grey bar to configure the settings for the desired EventSensor point. See the EventSensor Feature Guide on the Asentria Portal for detailed information on configuring different types of EventSensors.

If any setting is changed, click the Submit button before navigating away from that sensors setting page option or the changes will not be saved.

Depending on the type of EventSensor different settings will display. As an example, a Contact Closure point Event Settings page is displayed.

Contact Closure *n*



Enable Sensor
The Enable checkbox is an ON/OFF toggle to enable the Sensor. The default is OFF (unchecked).

Name
Text field to name this contact closure point. The default setting is unnamed. The maximum length is 60 characters.

Alarm Stat
This drop-down box is an OPEN/CLOSED toggle that determines whether an event will be triggered when the contact closure circuit is opened or closed. The default state is CLOSED.

Threshold / Threshold / Normal Threshold
These two fields set the number of seconds (0-255) that the contact closure must remain in the referred to state before the event Actions defined for the alarm or return to normal occur.

Actions / Return to Normal Actions
These two fields are text fields to define the actions for the SiteBoss to take in response to the contact closure moving into and/or out of the Alarm state. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to

Actions List chapter for more information.

Trap Number / Normal Trap Number
This box is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number is 110, but any number in the alternate range of 1000 – 1199 can be used.

Class / Normal Class
The drop-down boxes are used to set the severity class for the alarm. The available drop-down options will be a list of the classes previously defined at the Class Table tab.

Alarm Alias / Normal Alias
These text fields are used to set customized names that represent the active alarm state or the return to normal state, used when reporting active events for this sensor.

Group
This is a drop-down descriptive field that can be used to categorize the alarm point into subjective group types on custom pages or in Alarm Manager or other Network Management Software. The available drop-down options will be a list of the groups previously defined at the Group Table page.

Override Global Reminder Interval
This checkbox is an ON/OFF toggle to override the global reminder interval. If this is set to ON a specific reminder interval can be set for this event. The default setting is OFF (unchecked).

Individual Reminder Interval (minutes)
This field sets the time in minutes (0 – 65535) for an action to be repeated if the contact closure that triggered the alarm is still in the defined active state. When the sensor has been returned to the inactive state, the reminder interval is no longer in effect. The default setting is 120 minutes.

EventSensor Installation Connections

EventSensors are connected to the host unit and daisy-chained to each other using the provided EventSensor cables or standard CAT5E Ethernet cable. One RJ45 end of the cable plugs in to the Sensor port on the back panel of the host unit. The other RJ45 end of the cable plugs in to the EventSensor port labeled Control. Additional EventSensors are chained together with cable from the Sensor port on the first EventSensor to the Control port on the next EventSensor.

Some older units may have a round DIN connector Sensor port. To use the current RJ45 style EventSensors use the ES-CAB8 adapter kit.

Be sure to check power usage requirements to see if additional power cables are required for the sensor string. See the EventSensor Power Consumption Feature Guide for calculation instructions.

EventSensor do not need to be connected in any type of physical order, the dip switch settings will define their display and setting sequence. See the EventSensor DIP Switch Configuration chapter for instructions on setting the DIP Switches.

EventSensor DIP Switch Configuration

The SiteBoss supports a maximum of 16 external EventSensor slots.

Some external EventSensors have dip switches on the EventSensor that will need to be set to the slot number you wish that sensor to display at.

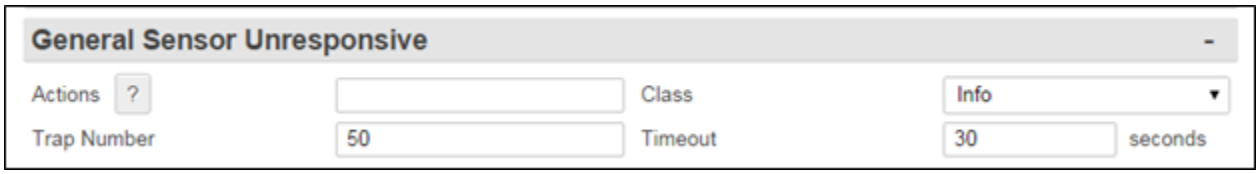
1 = DIP Switch up 0 = DIP Switch down

DIP SW	Slot	DIP SW	Slot	DIP SW	Slot	DIP SW	Slot
0000	= 1	0100	= 5	1000	= 9	1100	= 13
0001	= 2	0101	= 6	1001	= 10	1101	= 14
0010	= 3	0110	= 7	1010	= 11	1110	= 15
0011	= 4	0111	= 8	1011	= 12	1111	= 16

For ESJ style SensorJack sensors, the settings slot will automatically be assigned to it if one is available.

General Sensor Unresponsive Settings

These settings are used to configure the actions the SiteBoss should take if an EventSensor becomes unresponsive.



Actions

This text field is used to set the action(s) the SiteBoss should take if any EventSensor becomes unresponsive. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Class

This drop-down menu allows for configuring the severity class for the Sensor Unresponsive event. The available drop-down options will be a list of the classes previously defined using the Class Table menu button.

Trap Number

This text box sets the Trap Number to be sent with any SNMP traps for this event. The default is 50, but this can be set in the range of 1000 – 1199 as needed.

Timeout

This field defines the time (10 - 65535 seconds) to wait before declaring a non-communicative EventSensor unresponsive. The default setting is 30 seconds.

EventSensor Reporting

EventSensor Reporting is a feature that allows an EventSensor connected to one Asentria product to transmit data to another Asentria product via a TCP connection. This feature does not need to be enabled in order to allow for normal alarm notice delivery.

The **client** unit is the SiteBoss with the sensor physically connected to it and the **host** unit is the SiteBoss to whom the client unit will report when there is a change in the status of its sensor.

In addition to configuring the settings defined below, each sensor on the client unit will need to have EventSensor Reporting Enabled in the Event / EventSensor / Configuring an EventSensor Point settings.

The Host unit will need to have the EventSensor slots selected using the Command Line Interface. Instructions for this step are in the Set the EventSensor Slot on Host Unit section of

the EventSensor Reporting chapter CLI section of this manual.

For a further explanation of EventSensor Reporting and how to configure both the Host and Client units, refer to the EventSensor Reporting Feature Guide on the Asentria Information Portal or contact Asentria Technical Support.

Enable Reporting Host
This is an ON/OFF checkbox to enable this SiteBoss to be a host for EventSensor reporting from another Asentria device. The Default is OFF (unchecked).

Reporting Host Port
This is used to set the TCP Port that this SiteBoss would use for receiving sensor reports from another Asentria device. The Default is 4000.

Report To IP
This field would be used if this SiteBoss is the client. Set the IP address of the host SiteBoss that a sensor connected to this SiteBoss would report to.

{{header-settingsIReport To Port This field would be used if this SiteBoss is the client. Set the TCP port this SiteBoss would use to report to a host unit. The Default is 4000.

»Note: Both Client and Host need the Port settings set to the same port number.

Fuel Sensors

Up to three different Fuel Sensors can be configured. Refer to the Fuel Sensor Monitoring Feature Guide for a more in-depth explanation of configuring fuel sensing.

Fuel Sensor Settings
Select which of three possible fuel sensors you are configuring using the drop-down button at the top of the Fuel Sensor Settings page.

Fuel Sensors General

Enable
This is a checkbox to enable fuel sensor events. The default value is OFF (unchecked).

Sensor Type
This is a drop-down box containing the options of CURRENT, RESISTIVE FLOAT and VOLTAGE to indicate the type of fuel sensor being used. The default value is CURRENT.

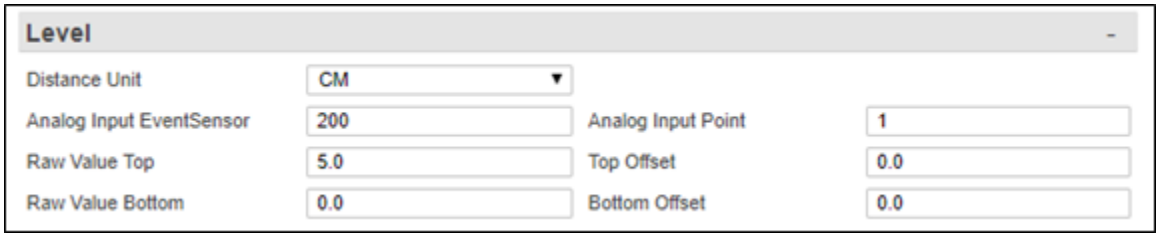
Name
The Name option is an alphanumeric field that allows you to name this fuel sensor (maximum length is 60 characters). The default setting is ?unnamed?.

Fuel Type
This is a drop down menu option to define the type of fuel being monitored. The options are DIESEL, PROPANE, NATURAL GAS, HYDROGEN, GASOLINE, and OTHER. The Default is Diesel.

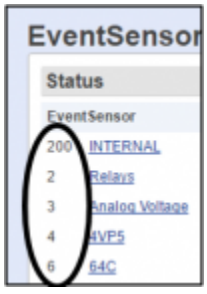
Group
This is a drop-down descriptive field that can be used to categorize the alarm point into subjective group types on custom pages, in Alarm Manager, or other Network Management Software. The available drop-down options will be a list of the groups previously defined at the Group Table page.

Level

This section of the page is used to configure the fuel level measurement settings.



Distance Unit
This is a drop-down box to toggle between INCH and CM. This specifies the distance unit to be used when setting the tank dimension. The default value is CM.



Analog Input EventSensor

This field sets the slot number of the EventSensor associated with this fuel sensor. Allowed values are 200 (for Internal IO points) or 1 ? 16. The number associated with each EventSensor can be located using the EventSensor page. The default value is 200 (internal).

Analog Input Point
This field sets the input point on the EventSensor that is associated with this fuel sensor. Range is 1-48. The number can be located by viewing the EventSensor page. The default value is 1.

Raw Value Top
This field sets the analog input reading that corresponds to the SENSOR FULL point. This is an integer with range of 0 to 1,000,000. The default value is 5.0.

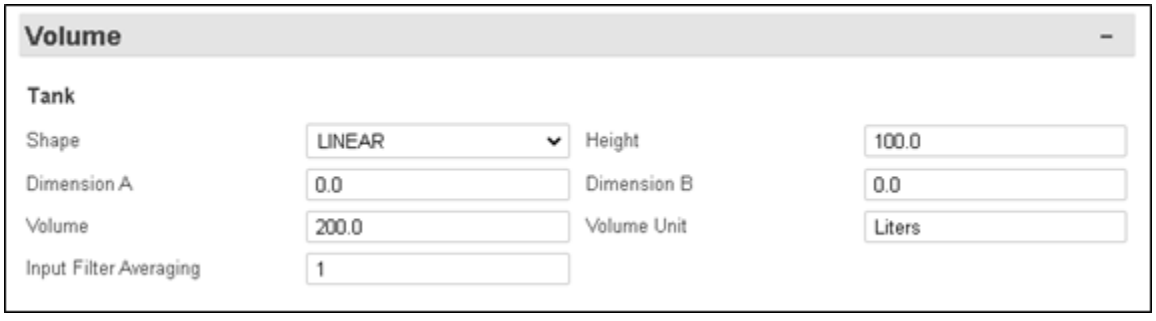
Top Offset
The Top Offset defines the distance, in the specified distance unit, between the SENSOR FULL point and the TANK FULL point. This is a floating-point value with range of -1,000 to +1,000. A positive value means the SENSOR FULL point is above the TANK FULL point, and a negative value means it is below. The default value is 0.0.

Raw Value Bottom
This field sets the analog input reading that corresponds to the minimum fluid height measurable by the fuel sensor. This is an integer with range of 0 to 1,000,000. The default value is 0.0.

Bottom Offset
The Bottom Offset defines the distance, in the specified distance unit, between the SENSOR EMPTY point and the TANK EMPTY point. This is a floating-point value with range of -1,000 to +1,000. A positive value means the SENSOR EMPTY point is above the TANK EMPTY point and a negative value means it is below the TANK EMPTY point. The default value is 0.0.

Volume

The Volume section of the page is used to configure the prerequisite dimensional measurements that apply the fuel tank.



Shape
The Shape drop-down box allows the selection between LINEAR, HORIZ CYL, VERT OVAL and CUSTOM to set the shape of the fuel tank. The default value is LINEAR.

Height

This field sets the height of the tank, from the TANK EMPTY point to the TANK FULL point, in the specified distance unit. This is a floating-point value with range of 0.0 to 1000. The default value is 100.0.

Dimension A

This field sets tank dimension measurement "A" for certain tank profiles, in the specified distance unit. For VERT OVAL this is the horizontal length of the tank. This is a floating-point value with range of 0.0 to 1000. The default value is 0.0.

Dimension B

This field sets tank dimension measurement "B" for certain tank profiles, in the specified distance unit. For VERT OVAL this is the width of the tank. This is a floating-point value with range of 0.0 to 1000. The default value is 0.0.

Volume

This field sets the number of volume units the tank contains when full. Range is 0 to 1,000,000. The default value is 200.0.

Volume Unit

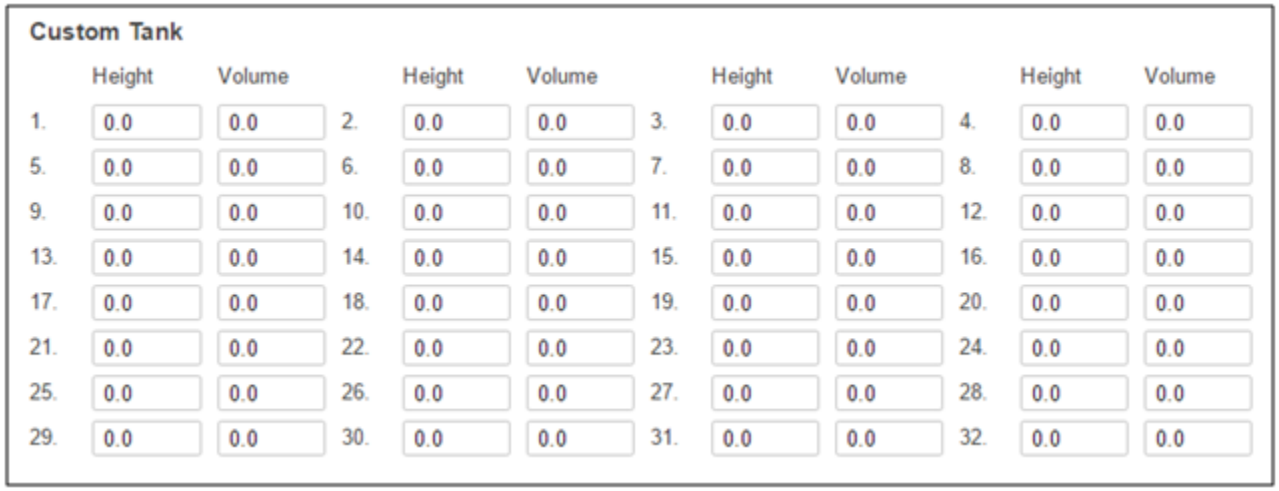
This field sets the name of the unit representing fluid volume in the tank. This is only used for display purposes and it does not affect the volume calculation in any way. The default value is "Liters?.

Input Filter Averaging

This option sets the number of samples used to filter the analog input value that is used for the tank volume calculation. The filtering is applied after the adjusted raw value. Range is 1 to 300; default is 1 (no filtering).

Custom Tank

When CUSTOM is selected for tank Shape, the system uses user-provided data to calculate the volume of fluid in the tank. The data is entered into a table of height/volume pairs, where a fluid height and corresponding tank volume are entered. Up to 32 height/volume pairs can be entered.



Event

This section of the page is used for configuring alarm notifications based on changes in the fuel level.

Event Enable

This is an ON/OFF checkbox to enable Volume Events. The default setting is OFF (unchecked).

Deadband

The Deadband sets a range (in volume units) on either side of a fuel volume setting that prevents the event from repeatedly going in and out of the alarm state as the actual fuel volume fluctuates above and below the setting. The default value is 6.0.

Very High / High / Low / Very Low Volume

These fields set the fuel volume (in volume units) threshold at which the Event Action(s) will be triggered.

Very High / High / Return to Normal / Low / Very Low Actions

These text fields are used to set the action(s) that will be triggered once the fuel level crosses the defined threshold. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Very High / High / Return to Normal / Low / Very Low Trap Number

Use this text field to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all fuel volume events is 519, but any number in the alternate range of 1000 - 1199 can be used.

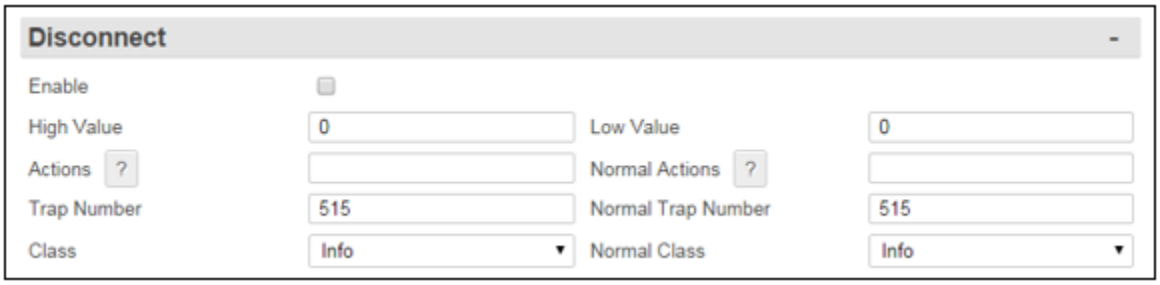
Very High / High / Return to Normal / Low / Very Low Class

Use this drop-down box to set the severity class for the event. When these drop-down options are selected, a list of the classes previously defined via the Class Table button is displayed. The default for all is Info.

Disconnect

This section of the page is for configuring alarm notifications of the fuel sensor being

disconnected.



Enabled
This is an ON/OFF checkbox to enable Volume Events. The default setting is OFF (unchecked).

High / Low Value
These menu options are used to set the High end and low end of normal for the analog input associated with the fuel sensor. If the input value falls outside the delineated range, then the sensor is considered "disconnected". If both high and low values are set to 0 (the default value), then the sensor will always be considered "connected".

Actions
This text field is used to set the action(s) that will be triggered if the fuel level sensor is disconnected. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Normal Actions
This option is used to set the action(s) that will be triggered once the fuel sensor is no longer disconnected. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Event Trap Number
This option is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for disconnect events is 515, but any number in the alternate range of 1000 - 1199 can be used.

Normal Trap Number
This option is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number is 515, but any number in the alternate range of 1000 - 1199 can be used.

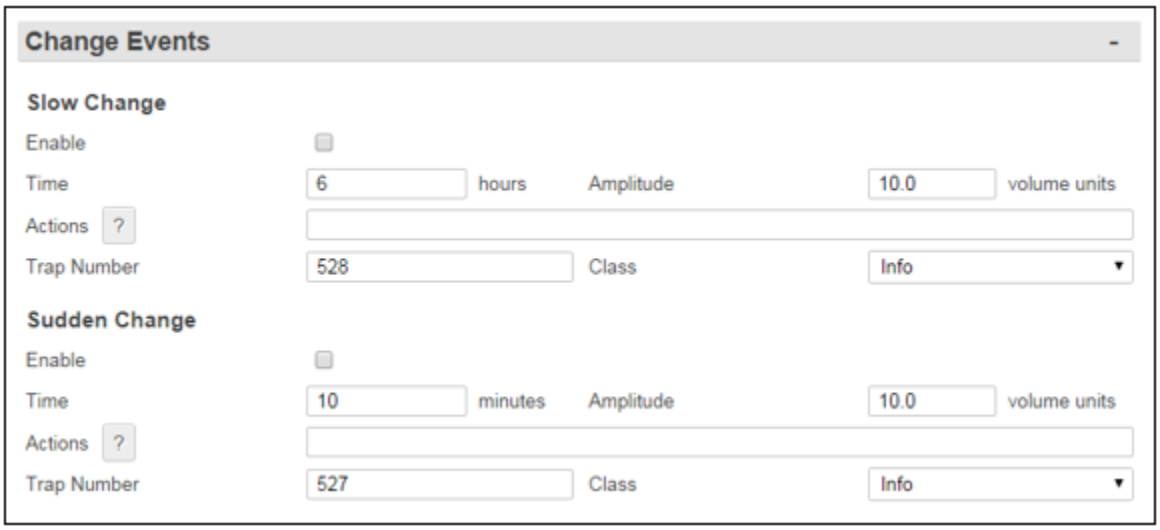
Class
Use this drop-down box to set the severity class for the event. When these drop-down options are selected, a list of the classes previously defined via the Class Table button is displayed. The default is Info.

Normal Class
Use this drop-down box to set the severity class for the event. When these drop-down options

are selected, a list of the classes previously defined via the Class Table button is displayed. The default is Info.

Change Events

The Slow Change and Sudden Change Event settings are used to trigger an event if the change in volume in the fuel level readings moves out of configured settings.



Enable

These are ON/OFF checkboxes used to enable the Change Event. The default values are OFF.

Time

This field is used to define a time window that would trigger the Change Event. For a Sudden Change Event the time is measured in minutes. The default is 10 minutes. For a Slow Change the time is measured in hours and the default is 6 hours.

Amplitude (volume units)

The Amplitude is the amount of change, in volume units, that triggers an event.

Actions

These options set the action(s) that will be triggered if there is a sudden or slow change in the fuel level readings. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Trap Number

These options are for setting the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for a Sudden Change event is 527 and for a Slow Change the trap number is 528. Any number in the alternate range of 1000 - 1199 can be used.

Class

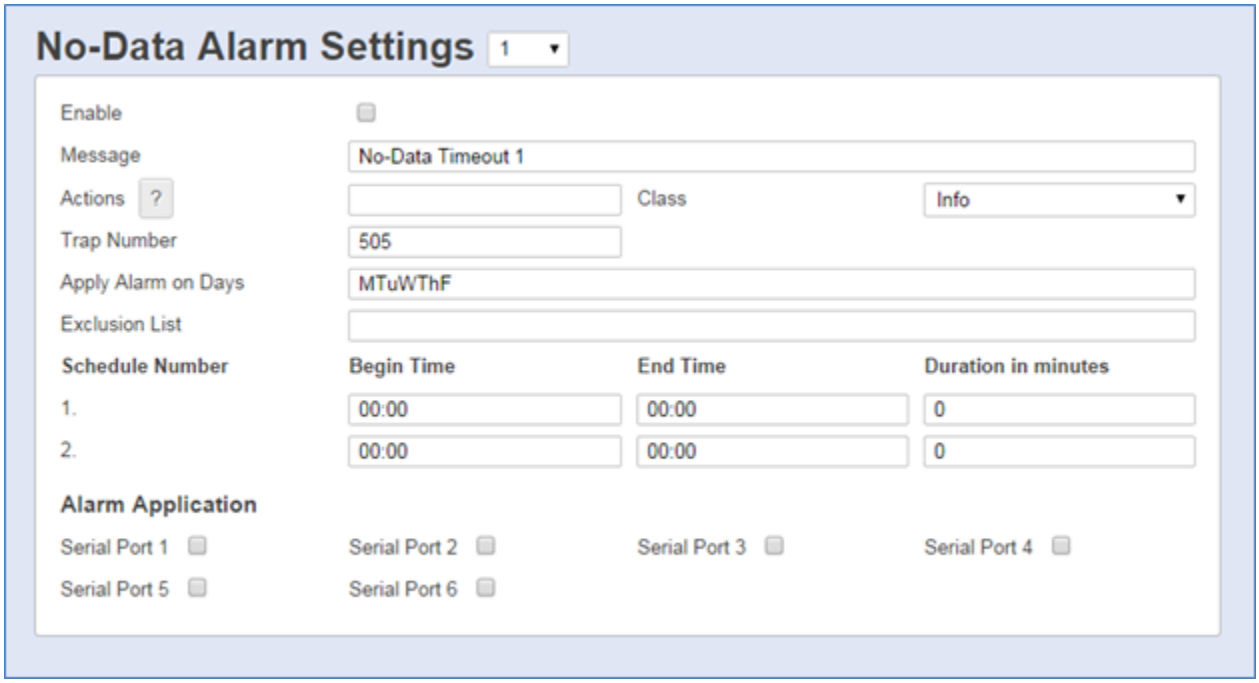
These options are for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info for both Slow and Sudden Change Events.

No-Data Alarms

No-Data Alarms can be configured on the SiteBoss to monitor data coming in via the serial ports, and take an alarm action if a certain period of time passes with no data.

This functionality is not on the S550A.

These menu options allow you to configure two separate No-Data Alarms, each of which can be configured for two different ranges of times with different time durations. The periods of time should be configured to match the calling patterns of your business or organization. For example, if your normal business hours are M-F 8:00 to 5:00, you will want to set lower time durations during those hours than you would "after hours" when call volumes are lighter and the periods of time where there is "no data" might be longer.



No-Data Alarm Settings

The drop-down menu in the upper grey section allows the selection between the two possible No-Data alarm options.

Enable

This check box is an ON/OFF toggle to enable the no-data monitor. The default setting is OFF (unchecked).

Message

This field is a text box to configure a message that is delivered with this event alarm message. The default setting is "No-Data Timeout *n*". The maximum length is 126 characters.

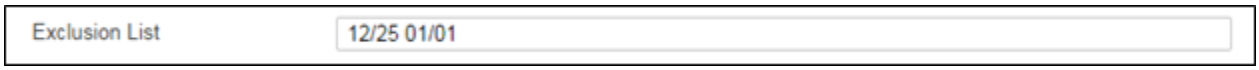
Actions
This option sets the action(s) that will be triggered if there is no data on the selected serial ports. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Class
This option is for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Trap Number
This field is used to set the number to be sent with any SNMP traps for this event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default is 505, but trap number can also be set in the range of 1000 – 1199 as needed.

Apply Alarm on Days
This is a text box to define the days of the week this alarm applies to. The days can be abbreviated Su for Sunday, M for Monday, Tu for Tuesday, W for Wednesday, Th for Thursday, F for Friday and Sa for Saturday. The default setting is Monday thru Friday (MTuWThF).

Exclusion List
This field is used to specify specific dates when this No-Data Alarm should "take the day off". For example, Christmas is a day you might want to add here. The entries should be entered as MM/DD followed by a space for each entry. For an example excluding Christmas and New Year's Day would look like this:



No dates are excluded by default.

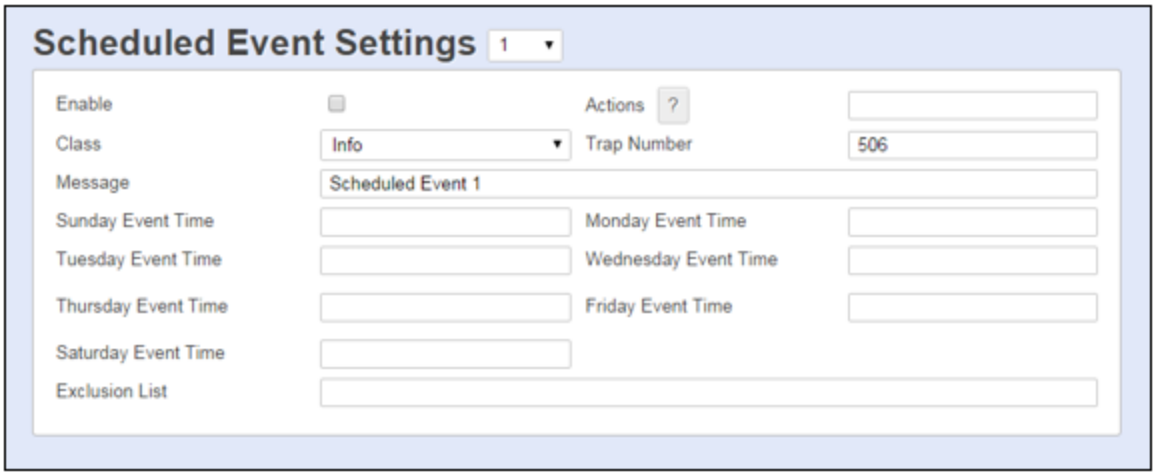
Begin Time / End Time
These fields are to set the beginning and ending times (24 hour clock) for each of two ranges of time.

Duration in minutes
These fields set the number of minutes (0-65535) that the SiteBoss should wait without receiving data before executing the specified Actions.

Alarm Application
The checkbox options are used to toggle ON or OFF the installed serial ports to designate whether this particular No-Data Alarm is active on that Serial Port. The default setting is OFF (unchecked) for all ports.

Scheduled Events

Scheduled Events allow you to schedule a specific date/time for an alarm action to occur. For example, you might want the SiteBoss to send you an Email every morning at 8:00 just so you know it is live on the network.



Scheduled Event Settings
The drop-down box in the upper grey area allows you to configure two separate Scheduled Events, each of which can be configured for any one time on any day of the week. Each day?s time can be scheduled independently from the others.

Enable
This checkbox is an ON/OFF toggle to enable the Scheduled Event. The default setting is OFF (unchecked).

Actions
This text box option is used to set the action(s) that the SiteBoss will take on the scheduled days and times. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Message
This text box sets the text string to be delivered with this event message. The default setting is "Scheduled Event n?. The maximum length is 126 characters.

Event Class
This option is for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Trap Number
This field is used to set the number to be sent with any SNMP traps for this event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default is 506, but trap number can also be set in the range of 1000 - 1199 as needed.

(Day) Event Time
These fields set the time each day for the scheduled event action to occur. The time should be entered in HH:MM in 24 hour clock format. No times are entered by default for any day.

Exclusion List
This field is used to specify specific dates when the scheduled event should ?take the day off?. For example, Christmas is a day you might want to add here. The entries should be entered as

MM/DD followed by a space for each entry. For example excluding Christmas and New Year's Day:

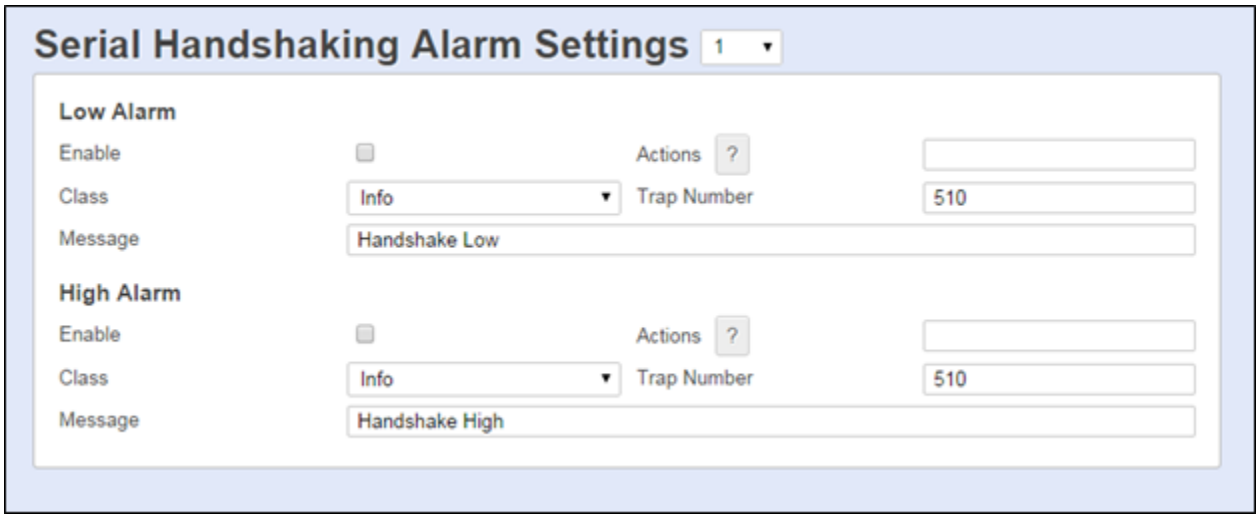
No dates are excluded by default.

Serial Handshaking

Serial Handshaking Alarms allows the SiteBoss to monitor each of its serial ports and alert you if the Data Terminal Ready (DTR) signal from the connected device drops low. This would be an indicator that the connected device has failed, or the cable between the SiteBoss and the device has been disconnected, or a number of other reasons depending on the device. It can also alert you when the DTR signal goes high again.

Serial Handshaking Alarms Settings

The drop-down box in the upper grey section of the page allows for the selection to configure the Serial Handshaking Alarms for any installed Serial Port.



Enable

The Low Alarm and High Alarm Enable check boxes are ON/OFF toggles to enable alarming on high or low handshaking levels. The default settings are OFF (unchecked).

Actions

The Actions text boxes are used to set the action(s) that the SiteBoss will take if the DTR signal drops low or returns to the higher level. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Class

These options are for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default values are

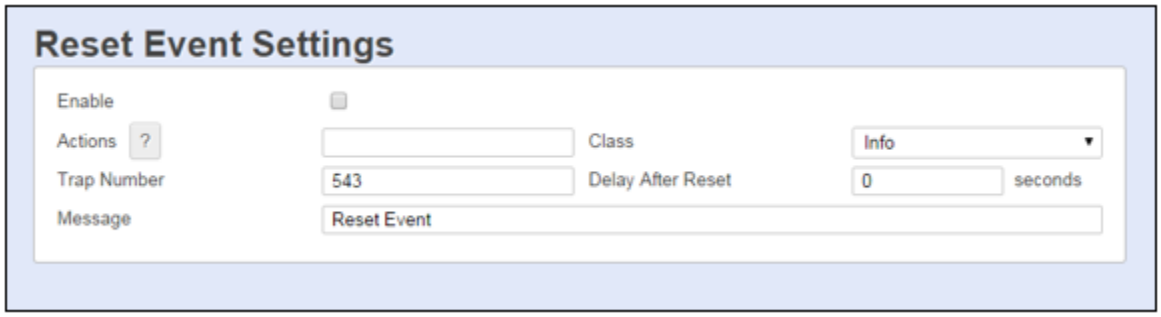
Info.

Trap Number
These fields are used to set the number to be sent with any SNMP traps for the event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The defaults are 510, but trap number can also be set in the range of 1000 – 1199 as needed.

Message
The Message fields are used to set the message sent with any text-based action for this event. The default settings are "Handshake Low" and "Handshake High". The maximum length for each is 126 characters.

Reset Event

The Reset Event Settings are used to configure event actions to be performed after the unit has been restarted. These actions would be executed regardless of whether the unit was restarted via a restart command, pressing the reset button or by power cycling.



Enable Event
This checkbox is an ON/OFF toggle to enable the Reset Event. The default setting is OFF (unchecked).

Event Actions
This text box option is used to set the action(s) that the SiteBoss will take on if it is restarted. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Event Class
This option is for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Event Trap Number
This field is used to set the number to be sent with any SNMP traps for this event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default is 543, but trap number can also be set in the range of 1000 - 1199 as needed.

Delay After Reset (seconds)
Enter the number of seconds for the SiteBoss to wait after unit finishes booting before

executing the Event Action(s) that have been set for this event. The default is 0 and the maximum is 3600 (1 hour).

Event Message
This text box is used to configure a text string to be delivered with this event message. The default setting is "Reset Event". The maximum length is 80 characters.

Telemetry

The telemetry table is a table of things to monitor on the unit for which telemetry is made available to other features on the same unit such as DNP3. DNP3 motivated the initial contents of the table, but it also has content for other non-DNP3 functionality. The entire telemetry table is configured via Settings Keys. Each row in the table is called a point. The SiteBoss supports 256 telemetry points.

All telemetry table settings are located in the **`event.point`** settings key branch. Each row in the table is a "point". This point nomenclature is inherited from the DNP3 point definition where a point is an "instance of a point type". A point type is a classification for entities having a common set of characteristics and attributes. Examples include binary inputs and analog inputs. Asentria adds other metadata to the point entity to support other non-DNP3 telemetry management methods.

Auto-Configure
This button automatically populates the unit's Telemetry Table with all EventSensors (not including Fuel or AC Power Monitor sensors).

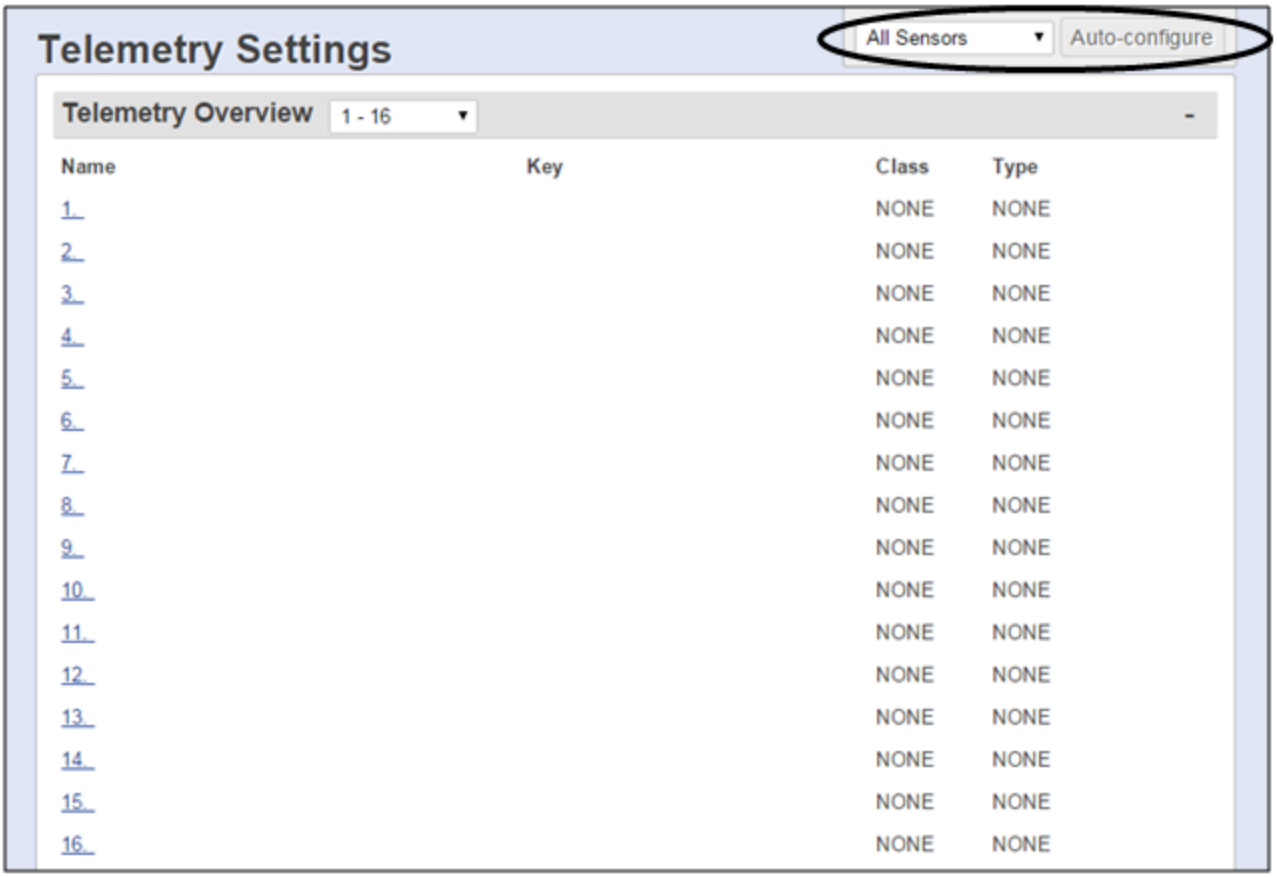
»**Note**: When configuring the telemetry table, manually configure DNP3 Deadbands appropriate to the sensor telemetry.

The drop-down box in the upper Telemetry Settings section is a toggle the Auto-Configure function to Enabled Sensors only or All Sensors.

This function will not work unless the DNP3 Network Settings are toggled to OUTSTATION.

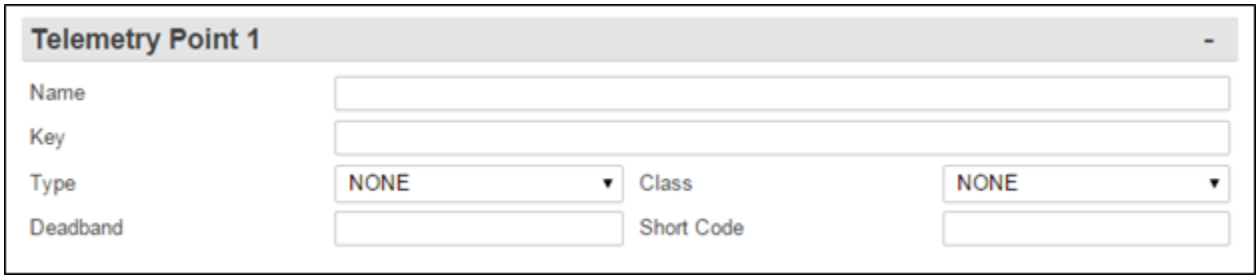
Telemetry Overview

The drop-down box allows toggling the displayed telemetry points from 1 to 256. To manually configure settings for a specific point click the blue text in the "Name" column and the lower section will display setting options for that point.



Telemetry Point *n*

DNP3 identifies telemetry via points, which are entities that have characteristics like index, name, type, deadband, and class. Any telemetry is uniquely identified in DNP3 via its index and type. Index is a number the SiteBoss uses the row number of the Telemetry Table.



Name

This text box is used to name the Telemetry point. The maximum length is 60 characters.

Key

Use this field to set the Settings Key name of telemetry to monitor. Typically, this key name is for an EventSensor value, but most keys on the unit can be used here including scripting variable keys. Servicing telemetry for a point requires this setting be configured.

Type
This drop-down box is used to set the DNP3 point type. The SiteBoss supports three of the 5 DNP3 point types. Available options are: BINARY INPUT (contact closure), ANALOG INPUT, and BINARY OUTPUT (relay or power output).

By default a point has no type (NONE). Servicing telemetry for a point requires this setting configured.

Class
DNP3 point class (0, 1, 2, 3, or NONE). Point classes govern from which points DNP3 events can be generated. DNP3 events can be packed in DNP3 Unsolicited Responses, which are analogous to autonomous (instead of polled) telemetry reporting. This is analogous to SNMP Trap vs SNMP Get. Servicing DNP3 unsolicited reporting for a point requires this setting configured to 1, 2, or 3.

Deadband
This field sets the value by which the telemetry value must change in order for a DNP3 event to be generated, if the point class is 1, 2, or 3. The deadband is default blank (meaning no deadband, or a deadband of essentially 0 for ANALOG INPUT point types. Regardless of how the configure the telemetry table (manually or via DNP3 auto-configure), you should configure an appropriate deadband for each point.

Short Code
This field is reserved for future use.

►Device Management

Job Scheduling

The SiteBoss can be configured for starting up to 8 jobs scheduled to run automatically. These schedules include start dates and times, and settings for repeating those schedules on a daily, weekly, monthly, or yearly basis.

The Schedule Number is used when configuring Generator Exercising functions in the Exercising menu. It can also be used with LUA Scripts to configure SiteBoss actions on a regular schedule.

The upper section of the page shows the general Status of any configured schedules. Once a schedule has been configured, the Enabled Status will show "ON" and the "LED" on the right hand side of the display will turn from grey to green. The Upcoming Schedule shows the next time this schedule is configured to start its assigned actions.

Select the job to configure by clicking the blue "view" text in the upper section of the screen. This will display its settings in the lower portion of the screen.

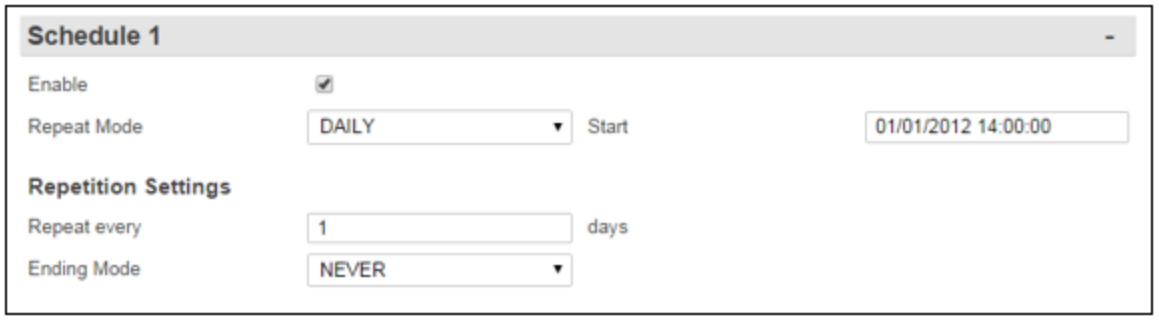
Enable
This checkbox is an ON/OFF toggle to turn on this particular Job Schedule. The default setting is OFF (unchecked).

Repeat Mode
This is a drop-down box is used to select the specific submenu with options to set the repetition of the Job Schedule. The five options for how often the Job Schedule is to be repeated are NONE, DAILY, WEEKLY, MONTHLY and YEARLY. Each option displays different configuration options for your schedule. The default is NONE.

Start
This text box sets the date (mm/dd/yyyy) and time in 24 hour clock format (hh:mm:ss) that controls the date and time this schedule starts.

Repeat Mode - DAILY

Setting the Repeat Mode drop-down box to DAILY will allow the user to schedule the job to run once during a 24 hour period and then have that job repeated some number of days later at that same time of day. Additional options are provided for when the repeat mode for this Job Schedule will end.



Repetition Settings - Daily

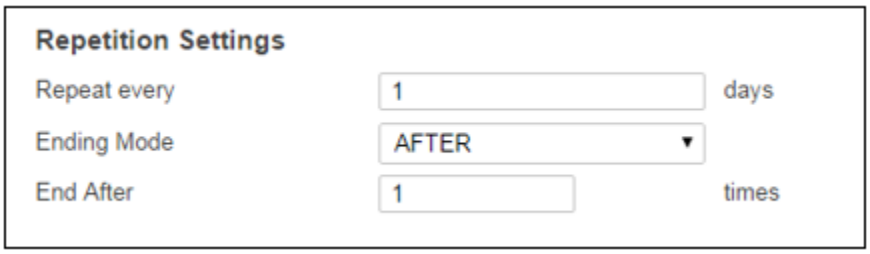
Repeat Every

Use this field to set how many days should pass before the job repeats. This option will set the job to repeat after that many days. If set to 1 then it will repeat daily. The values options are 1 - 400. The default setting is 1.

Ending Mode

This drop-down box has three options: NEVER, AFTER, and ON DATE.

- NEVER - means this Job Schedule never ends. It will repeat after the number of days set at the "Repeat every" setting until manually changed.
- AFTER - means this Job Schedule ends after being repeated a certain number of times. Toggling this box to AFTER will cause a new options field to appear to set the number of times this schedule should repeat.



End After

The End After field sets the number of times this job will be repeated when the Ending Mode is set to AFTER. The available values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

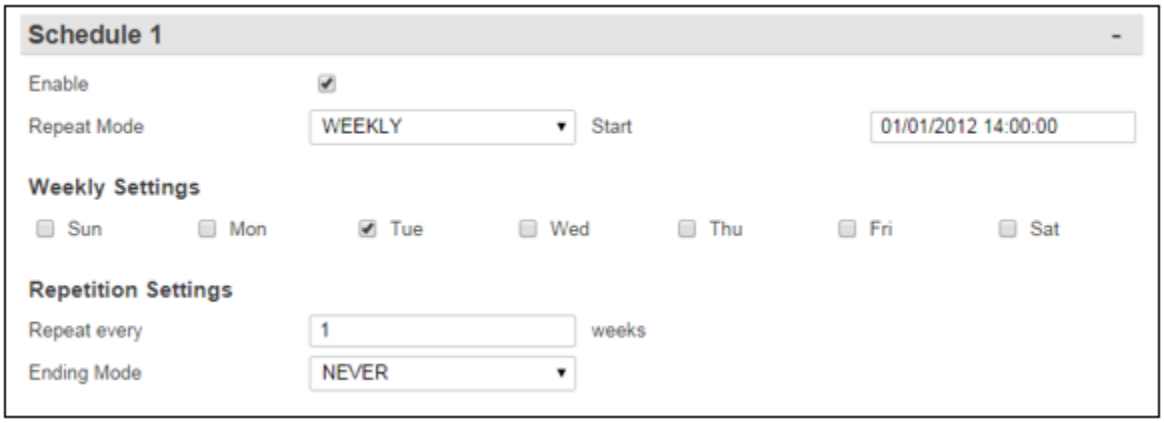
- ON DATE - means this Job Schedule ends after a specific date and time. Toggling this box to ON DATE will cause a new options field to appear to set the date this schedule should stop repeating.

End Date

The End Date should be entered (mm/dd/yyyy) and time (hh:mm:ss), in 24 hour format. This field sets the date this schedule should stop repeating. The default is blank which means no end date.

Repeat Mode - WEEKLY

Repeat Mode WEEKLY allows the user to schedule the job for a specific day(s) during the week and then have that job repeated the same day(s) each week. Additional options are provided for when the repeat mode for this Job Schedule will end.



Weekly Settings

This section contains ON/OFF toggles for each day of the week. ON (checked) means this Job Schedule will be repeated on that day of the week. OFF (unchecked) means this Job Schedule does not get run on that day. The default for all is OFF (unchecked), except for Tuesday which is ON (checked).

Repetition Settings - Weekly

Repeat every

This text field sets how often this Job Schedule will repeat. This means how many weeks after the job executes should it repeat. Values are 1 ? 255. The default setting is 1, weekly.

Ending Mode

This drop-down box toggles through three options: NEVER, AFTER, and ON DATE.

- NEVER - means this Job Schedule never ends. It will repeat based on the "Repeat every" setting until manually changed.
- AFTER - means this Job Schedule ends after being repeated a certain number of times. Toggling this box to AFTER will cause a new options field to appear to set the number of times this schedule should repeat.

End After

The End After field sets the number of times this job will be repeated when the Ending Mode is set to AFTER. The available values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

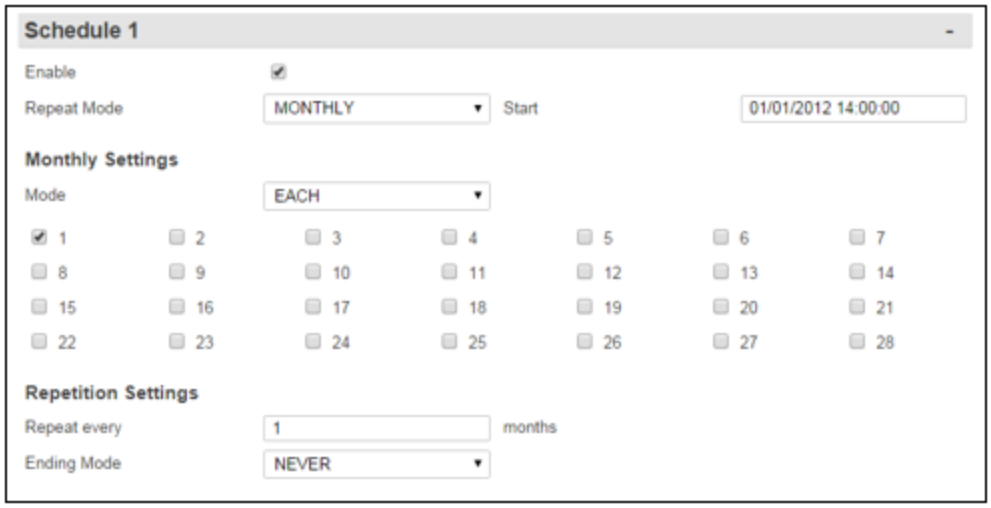
- ON DATE ? means this Job Schedule ends after a specific date and time. Toggling this box to ON DATE will cause a new options field to appear to set the date this schedule should stop repeating. The date should be entered (mm/dd/yyyy) and time (hh:mm:ss), in 24 hour format, for the repeat mode to end. The default is blank which means no end date.

End Date

The End Date should be entered (mm/dd/yyyy) and time (hh:mm:ss), in 24 hour format. This field sets the date this schedule should stop repeating. The default is blank which means no end date.

Repeat Mode - MONTHLY

Repeat Mode MONTHLY allows the user to schedule the job for a specific day of the month and then have that job repeated the same day each month. Additional options are provided for when the repeat mode for this Job Schedule will end.



Monthly Settings

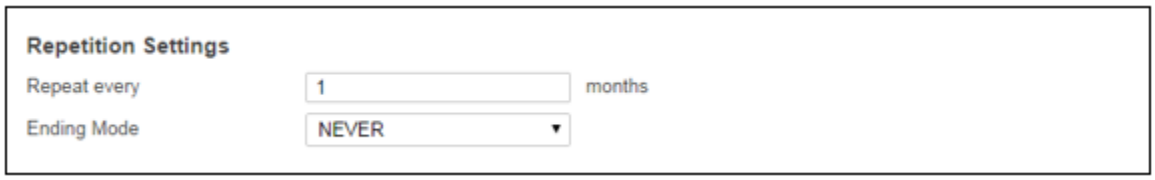
Mode

The Mode drop down box allows a selection between EACH and ON DATE.

- EACH - means the schedule runs on specific dates of the month. When the Mode is toggled to EACH checkboxes will be available to schedule the action on the specific dates of the month. By default, the 1st is ON (checked) and all other days are OFF (unchecked).
- ON DATE - means the schedule runs on calculated dates of the month according to which day that month starts. When the Mode is toggled to "ON THE" two drop-down options will be displayed. These two options are configured together to provide a precise day of the week on which this Job Schedule will be run.

- The first drop-down box contains the options FIRST, SECOND, THIRD, FOURTH and LAST. The default setting is FIRST.
- The second drop-down box contains the options DAY, WEEKDAY, WEEKEND DAY, SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY and SATURDAY to indicate the day of the week this schedule will run. The default setting is TUESDAY.

Repetition Settings - Monthly



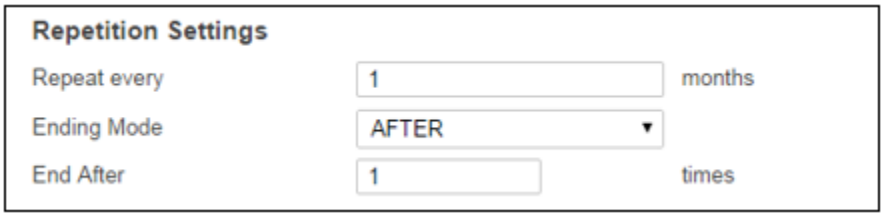
Repeat Every

This text box sets how often this Job Schedule will repeat. In the Monthly mode, this means how many months should pass before the job repeats. The available options are 1 ? 255. The default setting is 1, Monthly.

Ending Mode

This drop-down box has the options: NEVER, AFTER, and ON DATE.

- NEVER - means this Job Schedule never ends. It will repeat per the Repeat every" option until the setting is manually changed.
- AFTER - means this Job Schedule ends after being repeated a certain number of times. Toggling the drop-down box to AFTER displays a new End After text box.



End After

The End After field sets the number of times this job will be repeated when the Ending Mode is set to AFTER. The available values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

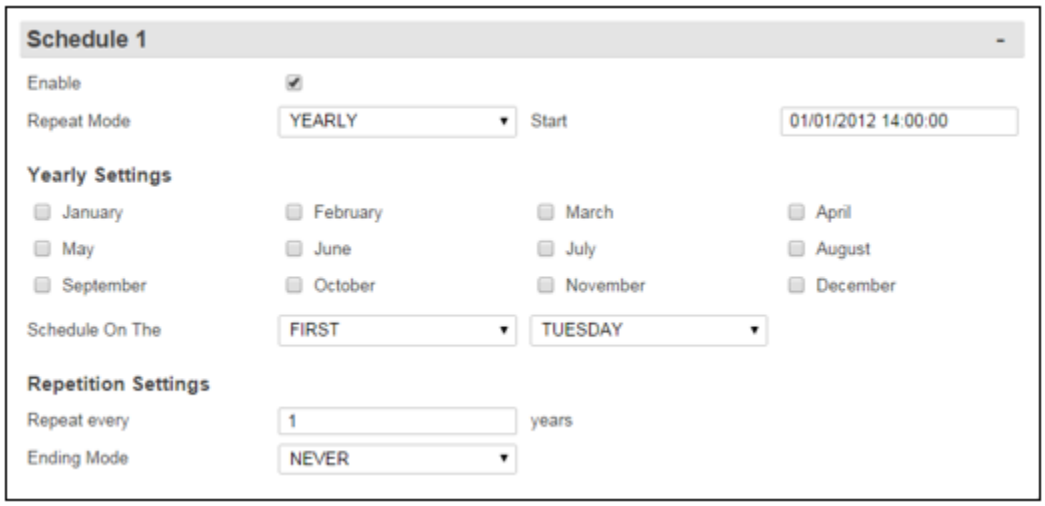
- ON DATE - means this Job Schedule ends after a specific date and time. Toggling this box to ON DATE will cause a new options field to appear to set the date this schedule should stop repeating.

End Date

The End Date should be entered (mm/dd/yyyy) and time (hh:mm:ss), in 24 hour format. This field sets the date this schedule should stop repeating. The default is blank which means no end date.

Repeat Mode - YEARLY

Repeat Mode YEARLY allows the user to schedule the job for a specific day of the month and then have that job repeated the same day during specific months throughout the year, and maintain that schedule for a specific number of years. Additional options are provided for when the repeat mode for this Job Schedule will end.



Yearly Settings

An ON/OFF checkbox is displayed for each month of the year. ON (checked) means this Job Schedule will be repeated in that month. OFF (unchecked) means this Job Schedule does not get run in that month. The default for all months is OFF (unchecked).

Schedule On The

Contains two drop-down boxes. These are used together to designate a precise day on which this Job Schedule is to be run.

- The first drop-down box contains the options: FIRST, SECOND, THIRD, FOURTH and LAST to indicate on which day of the month this schedule will run. The default setting is FIRST.
- The second drop-down box contains the options: DAY, WEEKDAY, WEEKEND DAY, SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY and SATURDAY to indicate the day of the week on which this schedule will run. The default setting is TUESDAY.

Repetition Settings - Yearly

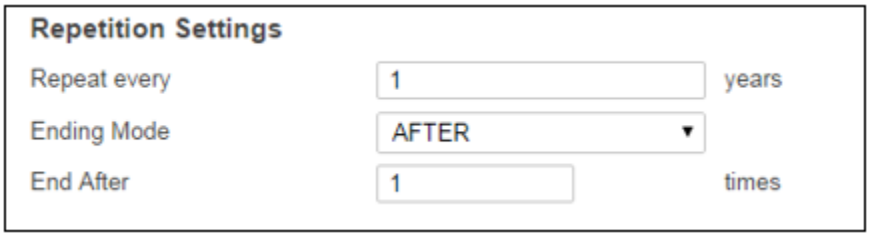
Repeat every

This field sets how often this Job Schedule will repeat. For Yearly, this sets how many years should pass before the schedule repeats. Values are 1 ? 255. The default setting is 1, yearly.

End Mode

This drop-down box contains three options: NEVER, AFTER, and ON DATE.

- NEVER - means this Job Schedule never ends. It will repeat per the Repeat every setting until manually changed.
- AFTER - means this Job Schedule ends after being repeated a designated number of times. Toggling the drop-down box to AFTER displays a new End After text box.



End After

The End After field sets the number of times this job will be repeated when the Ending Mode is set to AFTER. The available values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

- ON DATE - means this Job Schedule ends after a specific date and time. Toggling this box to ON DATE will cause a new options field to appear to set the date this schedule should stop repeating.

End Date

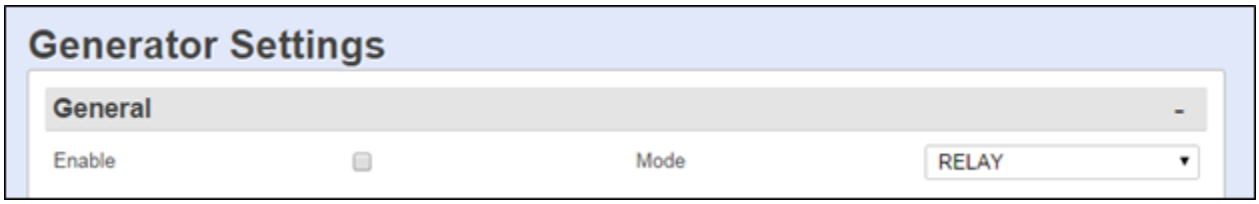
The End Date should be entered (mm/dd/yyyy) and time (hh:mm:ss), in 24 hour format. This field sets the date this schedule should stop repeating. The default is blank which means no end date.

Generator

SiteBoss provides the ability to remotely schedule and control generator exercising and to create Generator Running and Generator Failure alarms for visibility in most SNMP trap managers. To accomplish this, generator exercise functions are taken away from the Automatic Transfer Switch (ATS) and given to the SiteBoss, and a connection is established between the generator?s control panel and contact closures on the back of SiteBoss.

The following is a top level overview of generator related settings. For more detailed configuration and use instructions please see the Generator Control Feature Guide.

Generator General

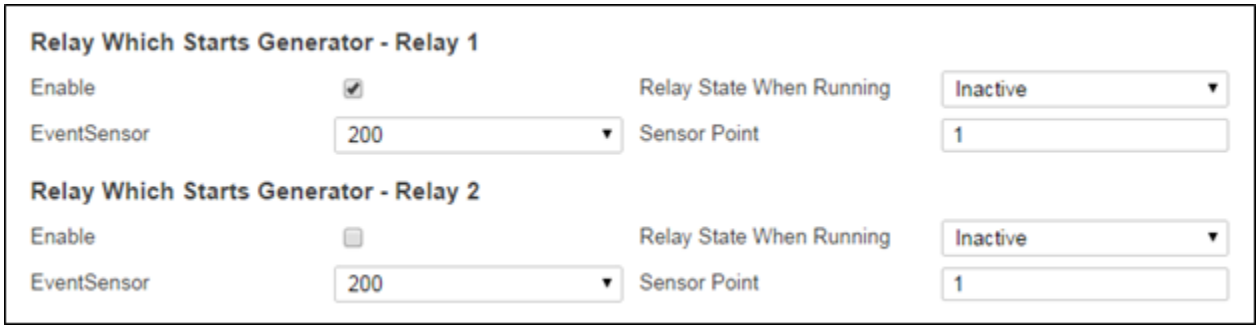


Enable
This checkbox is an ON/OFF toggle to enable generator set management. The default setting is OFF (unchecked).

Mode
The Mode drop-down box toggles between RELAY and SCRIPT. This setting controls by what mechanism the generator is started and stopped. The default is RELAY.

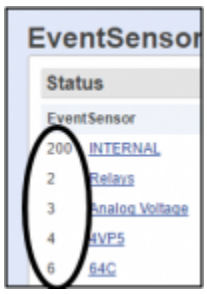
Relay Which Starts Generator – Relay *n*

These fields are used to specify which relay starts the generator. Some generators require two relays to start.



Enable
These are ON/OFF checkboxes to enables the detection of whether the generator is really running or not. The default settings are ON (checked) for Relay 1 and OFF (unchecked) for Relay 2.

Relay State When Running
These two drop-down boxes set which relay state (Active or Inactive) that corresponds with the generator running. The default settings are Inactive.



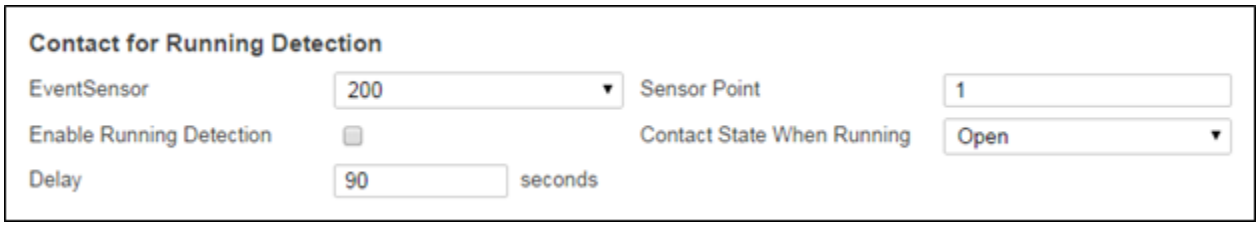
EventSensor
These drop-down boxes set the slot number of the EventSensor that has the relay which starts the generator. Values are 1 – 16, and 200 (internal). The default settings are 200.

The EventSensor number is usually the slot number for the slot card that has the relay used to start the generator. You can look up the EventSensor number under Events and then EventSensor on the left hand menu and locate the number next to the relay slot card being used.

Sensor Point
These fields are used to set the relay point number on the specified EventSensor that will be used to control a generator. The physical relay points read right to left on the SiteBoss. The defaults are both 1.

Contact for Running Detection

This section is used to define which contact closure is used to detect that the generator is running.



EventSensor
This drop-down box sets the slot number of the EventSensor that has the contact closure (CC) which is connected to the "generator is running" monitor. Available values are 1 – 16, and 200 (internal). The default setting is 200.

Sensor Point
This field sets the number of the contact closure (CC) point on that EventSensor that is used to determine if the generator is running. The physical contact points read right to left on the back of the SiteBoss. The default setting is 1.

Enable Running Detection
This is an ON/OFF checkbox to enable the Generator Is Running Detection function. The default setting is OFF (unchecked).

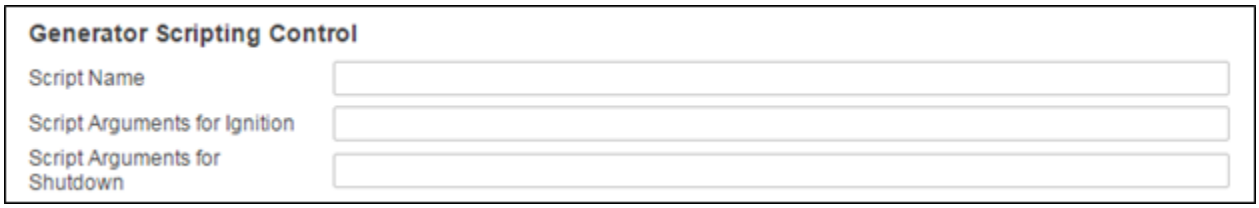
Contact State When Running
This drop-down box toggles between OPEN and CLOSED to set which physical state

corresponds with the generator running. The default setting is OPEN.

Delay
This text box sets how long (in seconds) the SiteBoss will to wait for the generator to indicate itself as "running" after engaging the generator starting mechanism. This field is relevant only when generator running detection is enabled. If the generator has not started after this delay time, the unit disengages the starting mechanism and creates a Generator Non-Start Event. Settings range is 0 to 600 seconds and the default is 90 seconds.

Generator Scripting Control

The Generator Scripting Control feature provides the option to use a script to start and stop the generator. This is to support generator ignition mechanisms that relay on MODBUS or IP. Note this function is independent of Generator Running Detection. See the Configuring and Using LUA Scripting on Asentria Products Feature Guide or Asentria Tech Support for more information on using Scripts on the SiteBoss.



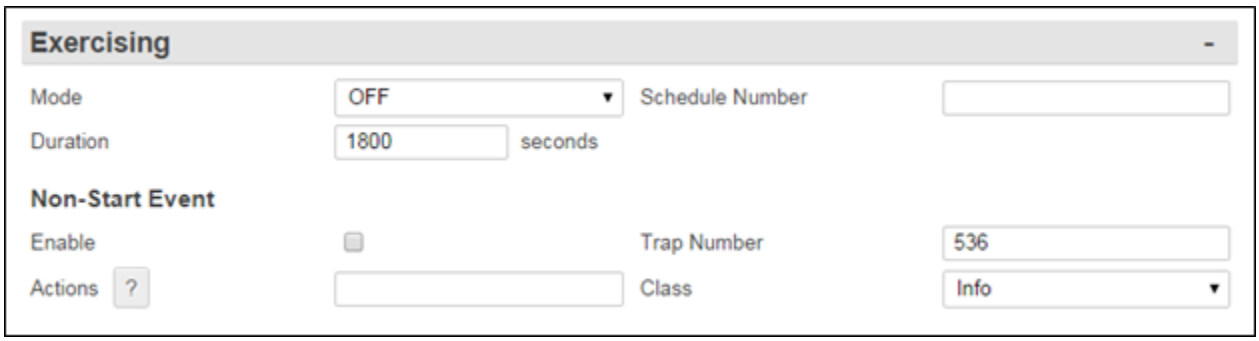
Script Name
This is the name of the script that controls the generator.

Script Arguments for Ignition
Input the arguments to pass to the script to tell it to start the generator.

Script Arguments for Shutdown
Input the arguments to pass to the script to tell it to stop the generator.

Exercising

The purpose of this function is to simply run the generator periodically. This is part of normal Generator maintenance to abide by manufacturer maintenance requirements.



Mode
This drop-down box allows the selection between OFF, SCHEDULE and INHIBIT. The default setting is OFF.

- OFF – means that the generator exercising function has been disabled.
- SCHEDULE – means that generator exercising is being conducted via a Job Schedule.
- INHIBIT – means that the Job Schedule is temporarily overridden.

Schedule Number
This field is a string setting that references one or more Job Schedule(s) configured in the Job Scheduling menu. This is either blank for no schedule, or a single number assigning a single configured schedule, or a comma-delimited string of numbers from 1 to 8. The default setting is blank (no schedule).

Duration (seconds)
This field defines the number of seconds that the generator will run either when started via a Job Schedule, or using a command interface forced start. The values range from 600 – 3600 seconds. The default setting is 1800 seconds.

Non-Start Event

Enabled
This is an ON/OFF checkbox to enable the Generator Non-start Event. The default setting is OFF (unchecked).

Actions
This text box option is used to set the action(s) that the SiteBoss will take if it detects that the generator failed to start. The button with the "?" displays the Actions List which lists the possible actions and the text string format requirements. Refer to Actions List chapter for more information.

Trap Number
This field is used to set the number to be sent with any SNMP traps for this event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default is 536, but trap number can also be set in the range of 1000 – 1199 as needed.

Class
This option is for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

AC Power Monitoring

The AC Power Monitor Settings menu is used to configuring up to six AC Power Monitors. Refer to the AC Power Monitoring Feature Guide for a more in-depth explanation of configuring AC power monitoring or contact Asentria Technical Support for more information.

AC Power Monitor Settings
The drop-down box at the top of the page toggles from 1 to 6 to allow configurations and Status readings for up to 6 AC Power Monitors.

AC Power Monitoring Status

The Status section of the page displays available readings from the AC Power Monitor selected via the AC Power Monitor Settings drop-down box. The values will display as 0 if no AC Power Monitor is configured or connected.

Status

Attribute	Present	Average	Minimum	Maximum
Average Voltage (Volts)	120.80	120.75	117.40	124.30
Average Current (Amps)	9.84	9.86	3.64	35.08
Frequency (Hz)	60.00	60.00	59.80	60.10
Real Power (Watts)	3120	3137	1040	11600
Reactive Power (VAR)	40	287	-640	2240
Apparent Power (VA)	3560	3579	1360	12240
Power Factor	0.88	0.86	-0.96	1.00
Energy (Wh)	67235200			
Reactive Energy (VARh)	2194040			
Apparent Energy (VAh)	78884400			
Phase Data	**Phase A**	**Phase B**	**Phase C**	
Voltage (Volts)	121.00	120.30	121.10	
Current (Amps)	5.72	12.28	11.40	
Real Power (Watts)	524	1352	1256	
Reactive Power (VAR)	16	-496	540	
Apparent Power (VA)	696	1492	1384	
Power Factor	0.75	-0.91	0.91	

AC Power Monitoring General

Enable

This is an ON/OFF checkbox to enable the AC Power Monitor selected via the AC Power Monitor Settings drop-down box. The default setting is OFF (unchecked).

Device Type

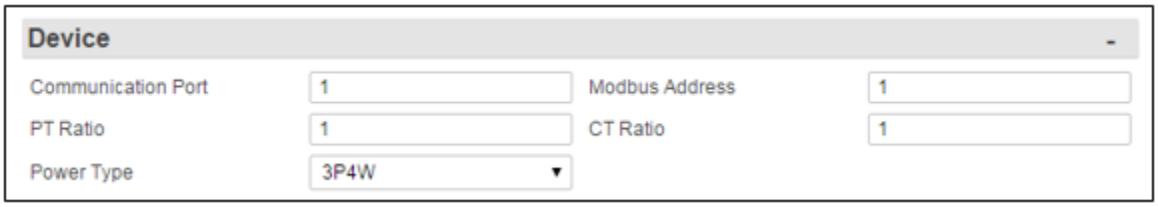
This option is used to define the model of the AC Power Monitoring Device. It toggles between YD2010, WATTSON, WATTSON MK II, CT-2EMG, ETA3.RTU, EM270 and WATTNODE. The default is YD2010.

Name
This is an alphanumeric field that allows you to name this Power Monitor. The maximum length is 60 characters. The default setting is 'unnamed'.

Group
This is a drop-down descriptive field that can be used to categorize the alarm point into subjective group types on custom pages, in Alarm Manager, or other Network Management Software. The available drop-down options will be a list of the groups previously defined at the Group Table page.

Device

This is a menu where you can configure the settings for your AC Power Device.



Communication Port
This field sets the serial port that the AC power monitoring device is connected to. 1 for the RS-485 port or 2 for the RS-232 port.

Modbus Address
This option sets the Modbus Address of the AC power monitor device. This is an integer setting with a range of 1 to 247. The default value is 1.

PT Ratio
Ratio of secondary turns to primary turns on potential transformers (PT). This is an integer setting with a range of 1 to 10000. The default value is 1.

CT Ratio
Ratio of secondary turns to primary turns on current transformers (CT). This is an integer setting with a range of 1 to 10000. The default value is 1.

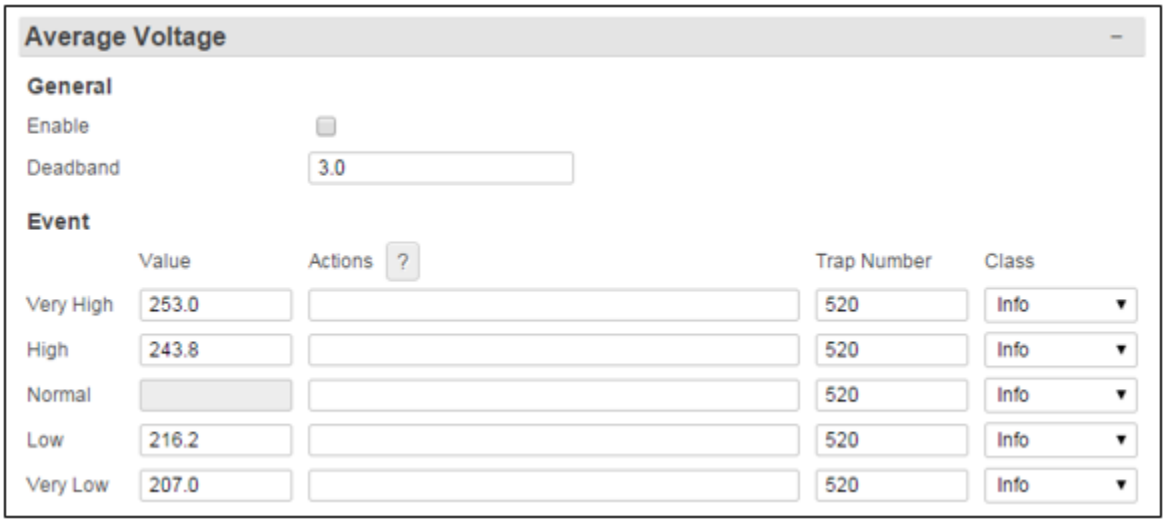
The CT can be gotten from the label on the Current Transformer. For the Split Core Current Transformer 5004-080 sold with the YADA AC Power Monitor the Primary current is 200A and the Secondary current is 5A. To get the correct setting for the CT Ratio divide the primary current by the secondary current, 200 / 5 = 40.

The CT Ratio is 40 for most Current Transformers.

Power Type
This is a toggle to define the type of power being monitored. The possible values are 1P2W, 1P3W, 3P3W, and 3P4W. The default value is 3P4W.

Average Voltage

These fields are used to configure the Average Voltage Event Settings.



Average Voltage General

Enable

This is an ON/OFF checkbox to enable the Average Voltage Event. The default setting is OFF (unchecked).

Deadband

The Deadband option allows you to set a range that prevents the event from repeatedly going in and out of the "alarm state" as the voltage reading fluctuates above and below the alarm setting. The average voltage would have to drop below the alarm state setting plus the deadband to clear the alarm. The default value is 3.0.

These settings are only for use with Customer Premises Equipment (CPE).

Average Voltage Event

These fields are used to configure actions for the SiteBoss to take if the Voltage crosses the configured thresholds.

Very High / High / Low / Very Low Value

These fields are used to set the average voltage value which triggers the Event Action(s). The range for each tier setting is 0 to 1000 with the defaults shown above in the screen shot.

Very High / High / Return to Normal / Low / Very Low Actions

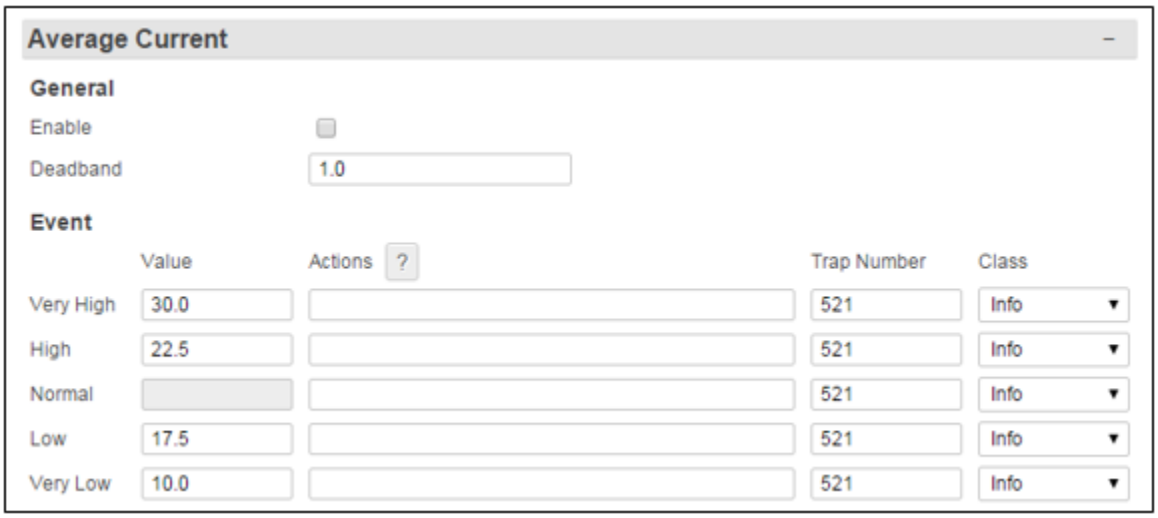
These fields are used to set the action(s) that will be triggered when the average voltage crosses a set threshold. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Very High / High / Return to Normal / Low / Very Low Trap Number
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Voltage Events is 520, but any number in the alternate range of 1000 - 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Class
These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Average Current

This menu contains the options to configure the Average Current Events.



Average Current General

Event Enable
This is an ON/OFF checkbox that enables the Average Current Event settings. The default setting is OFF (unchecked).

Deadband
The Deadband option allows you to set a range that prevents the event from repeatedly going in and out of the event state as the current readings fluctuate above and below the alarm setting. The average current value would need to drop below the alarm state value plus the deadband value to clear the alarm. The default value is 1.0.

Average Current Event

These fields are used to configure actions for the SiteBoss to take if the Average Current crosses the configured thresholds.

Very High / High / Low / Very Low Value
These fields are used to set the average current, in amps, which trigger the Event Actions. The range for each tier setting is 0 to 1000 with the defaults shown above in the screen shot.

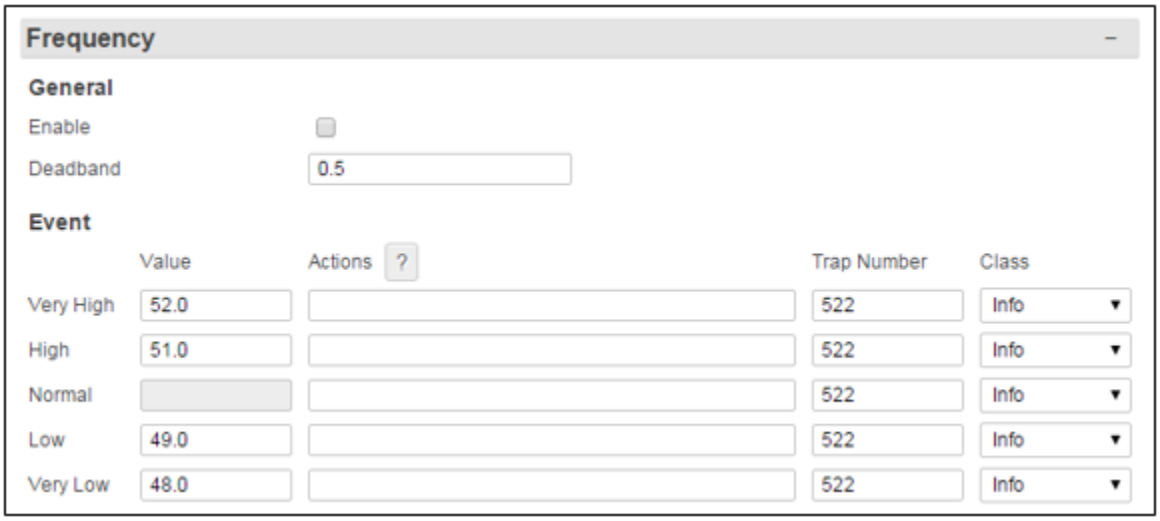
Very High / High / Return to Normal / Low / Very Low Actions
These fields are used to set the actions that will be triggered when the average current crosses a set threshold. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Very High / High / Return to Normal / Low / Very Low Trap Number
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Current Events is 521, but any number in the alternate range of 1000 - 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Class
These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Frequency

The Frequency Settings menu is where the Event Settings for the frequency variations can be configured.



Frequency General

Event Enable
This is an ON/OFF checkbox to enable the Frequency Event. The default setting is OFF (unchecked).

Deadband

The Deadband option allows you to set a range that prevents the event from repeatedly going in and out of the "alarm state" as the frequency fluctuates above and below the alarm setting. The frequency value would have to drop below the alarm state plus the deadband value to clear the alarm. The default value is 0.5.

Frequency Event

Very High / High / Low / Very Low Event Value

These fields are used to set the frequency, in hertz, which triggers the Event Actions. The range is 0 to 1000 with the default for each range setting pictured above in the screen shot.

Very High / High / Return to Normal / Low / Very Low Actions

These fields are used to set the actions that will be triggered when the frequency crosses a set threshold. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Very High / High / Return to Normal / Low / Very Low Trap Number

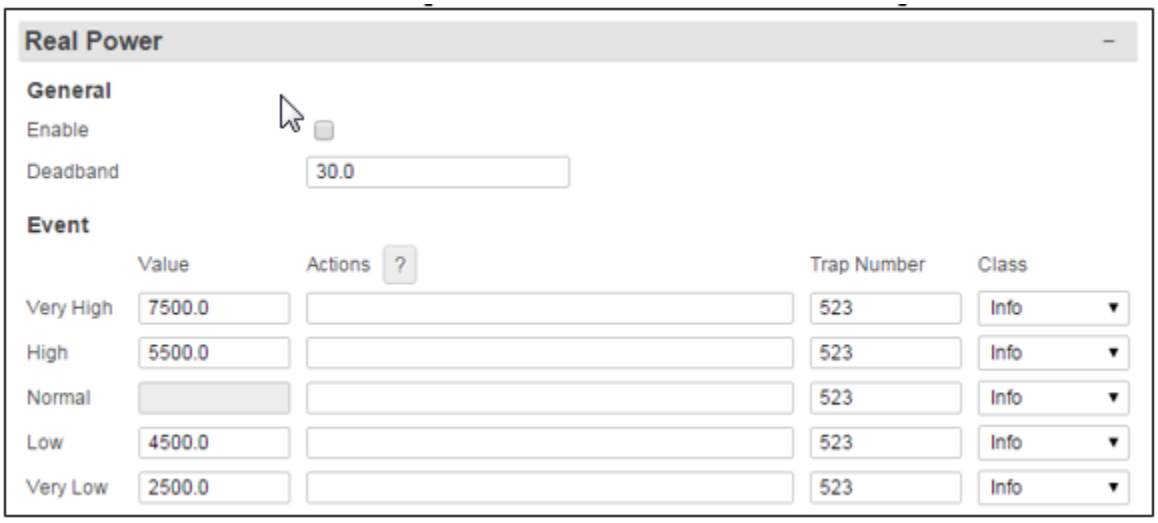
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Frequency Events is 522, but any number in the alternate range of 1000 - 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class

These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Real Power

This menu is where the Event Settings for the total Real Power can be configured.



Real Power General

Event Enable

This is an ON/OFF checkbox to enable Real Power Events. The default setting is OFF (unchecked).

Deadband

The Deadband option allows you to set a range that prevents the event from repeatedly going in and out of the alarm state as the real power readings fluctuate above and below the alarm setting. The real power value would have to drop below the alarm state value plus the deadband value to clear the alarm. The default value is 30.0.

Real Power Event

Very High / High / Low / Very Low Value

These fields are used to set the Real Power readings, in watts, which trigger the Event Actions. The range is 0 to 100,000 with the defaults in the screen shot above.

Very High / High / Return to Normal / Low / Very Low Actions

These fields are used to set the actions that will be triggered when the Real Power readings cross the set thresholds. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number

These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Real Power Events is 523, but any number in the alternate range of 1000 - 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class

These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Power Factor

The Power Factor event settings are configured at this menu location. Note that the power factor can be reported as a positive or negative value. For the purposes of event alarming, only the absolute value is used.

Power Factor General

Enable

This is an ON/OFF checkbox to enable the Power Factor Event. The default setting is OFF (unchecked).

Deadband

The Deadband option allows you to set a range that prevents the event from repeatedly going in and out of the "alarm state" as the Power Factor readings fluctuate above and below the Event value setting. The power factor value would need to drop below the alarm setting plus the deadband value to clear an alarm. The default value is 0.1.

Power Factor Event

Low / Very Low Value

These fields are used to set the Power Factor settings which trigger the Event Actions. The range is 0.0 to 1.0. The defaults are 0.9 for low and 0.70 for very low event.

Return to Normal / Low / Very Low Actions

These fields are used to set the action(s) that will be triggered when the Power Factor crosses the set threshold. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Return to Normal / Low / Very Low Trap Number

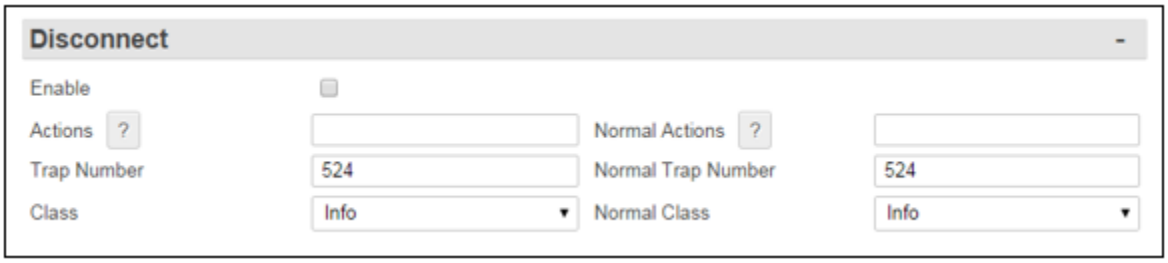
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Power Factor Events is 540, but any number in the alternate range of 1000 - 1199 can be used.

Return to Normal / Low / Very Low Class

These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Disconnect Event Settings

The disconnect event is triggered if communication with the AC power monitor device fails for one minute. The return to normal event is triggered upon the first subsequent successful communication attempt.



Enable

This is an ON/OFF checkbox to enable the Disconnect Event. The default setting is OFF (unchecked).

Actions/ Normal Actions

These fields set the actions that will be triggered when the AC power monitor fails or returns to normal. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Event / Normal Trap Number

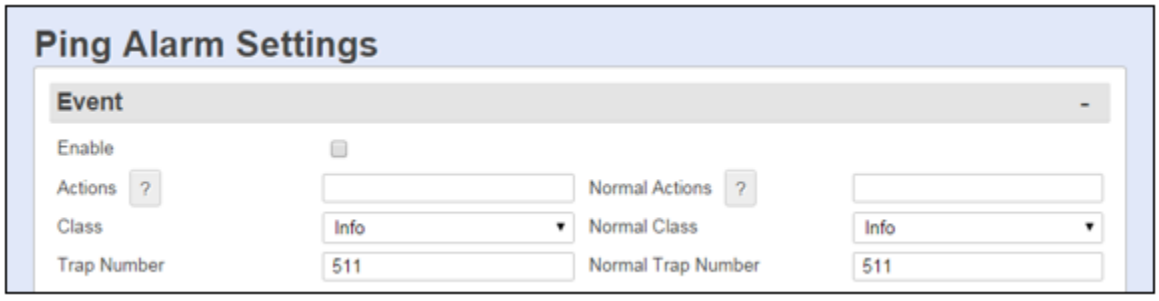
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Disconnect Events is 524, but any number in the alternate range of 1000 - 1199 can be used.

Event / Normal Class

These user-configurable optional settings define the severity of the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default value is Info.

Ping Alarms

The Ping Alarm Settings menu is where up to 64 different the Customer Premises Equipment (CPE) devices can be configured for connectivity alive monitoring by the SiteBoss.



Event

Enable

This checkbox is an ON/OFF toggle to enable a device down event. The default setting is OFF (unchecked).

Actions / Normal Actions

These fields are used to define the actions for the SiteBoss to take if a device is determined to be down or when it returns to the normal configured state. The button with the "?" will display the Actions List which lists the possible actions and the text string format requirements. Refer to the Actions List chapter for more information.

Class / Normal Class

These options are for setting the severity class for the event. Use the drop-down box to select one of the classes that are defined in the Class Table settings menu. The default values are Info.

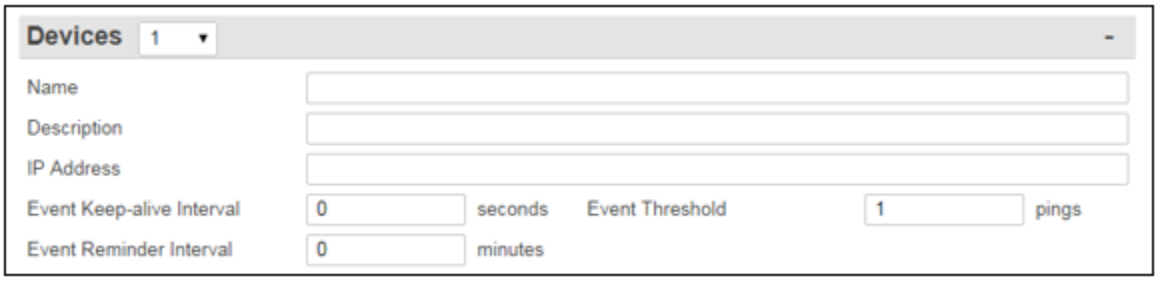
Trap Number / Normal Trap Number

These fields are used to set the number to be sent with any SNMP traps for the event. The Trap numbers are helpful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default is 511, but trap number can also be set in the range of 1000 - 1199 as needed.

Devices

Devices

The drop-down box in the grey menu bar area is to choose which device to configure for connectivity monitoring.



Name

Set the name given to the device. The only restriction on the name is that it cannot have any double or single quotes (' or ") in it. The maximum length is 24 characters.

Description

This text field sets a description of what the device is. The only restriction on the description is that it cannot have any double or single quotes (' or ") in it. The maximum length is 64 characters.

IP Address

This field sets the IP address of the device. The value is a dotted quad IP address.

Event Keep-alive Interval (seconds)

This field sets the number of seconds between periodic pings (ping cycle) sent by the SiteBoss to the device to make sure it is responsive. 1 ping frame is transmitted per ping cycle. Values are: 0 to 65535. The default setting is 0.

Event Threshold
This option sets the number of times that the unit receives no response to the keep-alive ping from the device before triggering the Actions configured in the Event section of the page. Available values are 1 to 255. The default setting is 1.

Event Reminder Interval (minutes)
This field sets the number of minutes for the associated device to be unresponsive before a reminder alarm is sent. The reminder alarm shares the same event configuration (actions/trap number/class) as a CPE Down event, but includes the text ?Reminder?. 0 means no reminder event is configured. The default setting is 0.

SSH to Telnet Bridging

SSH to Telnet Bridging is used to allow authorized telnet access to specific machines from the unit, upon successfully connecting to the unit via SSH.

Template:Header-settingsEnable This checkbox is an ON/OFF toggle on CPE 1 thru 4 only that enables an authorized user to make a Telnet connection to a Telnet-only device while on an SSH connection to the SiteBoss. SSH to Telnet Bridging is used to allow authorized Telnet access to specific machines from the unit, upon successfully connecting to the unit via SSH. The benefit of this feature is that if the SiteBoss is in a network environment where users can be enabled to have access to certain machines via Telnet (via an SSH connection to the SiteBoss) without being allowed access to any other Telnet hosts. The default setting is OFF (unchecked).

Template:Header-settingsSSH to Telnet Bridging Port Use this field to set the port for the Telnet Bridging function.

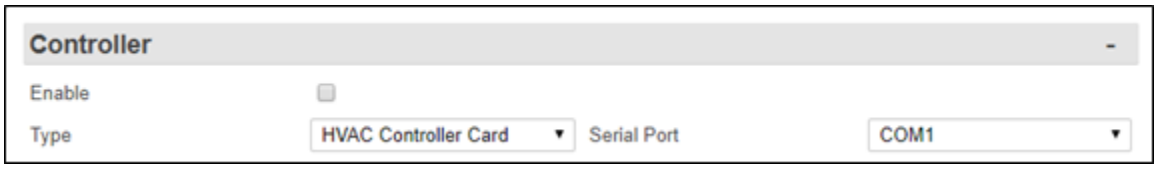
HVAC Monitoring

This manual will specifically go over the control settings of the HVAC Controller Card options, which are the settings to use if the SiteBoss is using the 2AC HVAC SiteBoss slot card. Togging the "Type" setting will bring up different options for an Airsys or Bard HVAC controller. See the HVAC Monitoring Feature Guide for additional information regarding the settings for the Airsys or Bard controllers as well as additional installation instructions for an Asentria HVAC Controller Card.

If your HVAC system is not on the list of pre-set controllers the SiteBoss can be used to control most HVAC systems using our LUA Scripting functions. Contact Asentria Technical Support for scripting assistance see the Scripting Training page on the Asentria Information Portal.

Controller

These are the basic settings used to enable the HVAC Monitoring functionality and select the controller interface system used at your site.



Enable

This is an On/Off check box to enable the HVAC Monitoring functionality. The Default is Off.

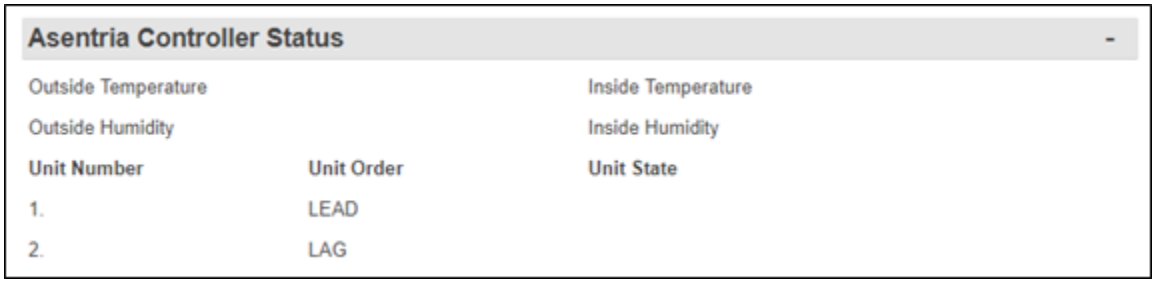
Type

This drop down menu allows the selection of the type of system to be monitored. Current options are HVAC Controller Card, BARD, AIRSYS and Asentria. By default, the HVAC Monitoring page opens displaying the HVAC Controller Card page. Toggling this setting changes the setting options lower on the page to match the controller option being used on site.

Serial Port

This drop down menu is used to define which serial port your HVAC system is connected to. Your available options are all the serial ports on your unit. If your HVAC is not connected via a serial port then this setting does not need to be changed and it will not affect the HVAC operation if changed. The default is COM1 (I/O1).

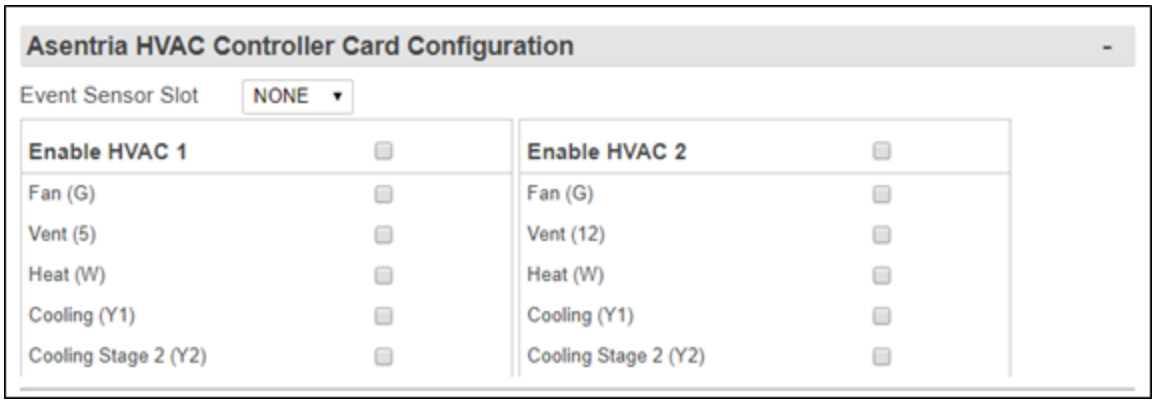
Asentria Controller Status



This section displays the status of the Asentria controlled HVAC units, along with available temperature and humidity sensor reading.

Asentria HVAC Controller Card Configuration

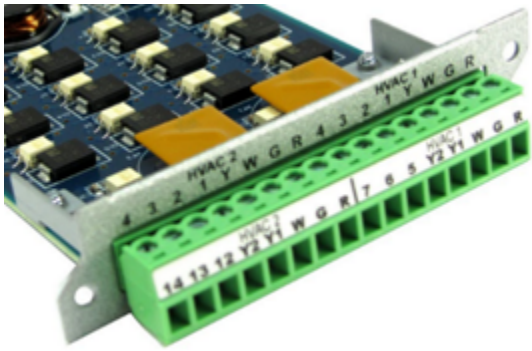
The top section is to let the SiteBoss know how the HVAC and SiteBoss are physically connected.



Event Sensor Slot

This drop down box tells the SiteBoss where the HVAC expansion card is installed. Slots are numbered right to left look at the back panel of the SiteBoss.

Enable HVAC 1/ Enable HVAC 2



These two check boxes are used to enable connected HVAC units. Click to enable either or both connected HVAC units.

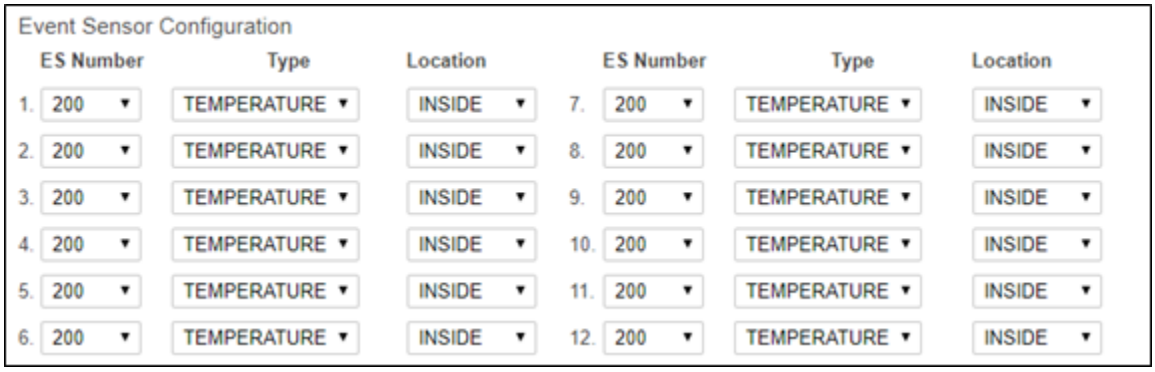
The remaining check boxes are used to tell the SiteBoss what wires are connected from the HVAC systems to the HVAC Controller card.

The "R" points should always be connected and the HVAC controls will not work unless it is. That is the 24V power used by the HVAC systems. There is no check box associated with that wire connection.

Event Sensor Configuration

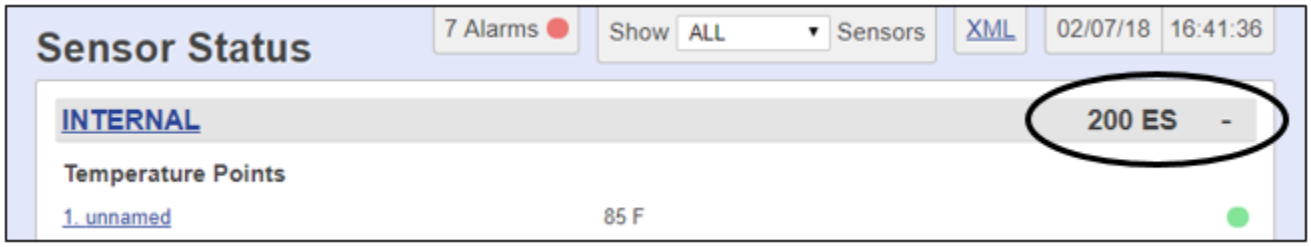
This section tells the SiteBoss what temperature and/or Temp/Humidity sensors to use to

control the HVAC systems. Minimally at least one inside temperature sensor must be installed.



ES Number

Use this drop down box to tell the SiteBoss which sensor slot has the Temperature or Temp/ Humidity sensor. The ES number will be on the Sensors Status page in the right side of the grey bar.



Type

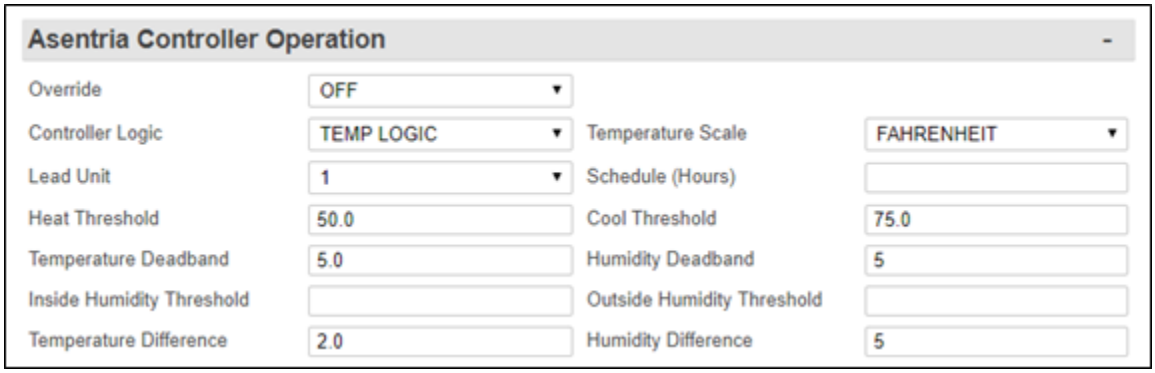
Select Temperature or Humidity for this sensor point. If you are using a dual Temperature and Humidity sensor use two Event Sensor Configuration points and set one to Temperature and the second one to Humidity and reference the same ES Number.

Location

Use this drop down box to define if the sensor is located inside the shelter or outside.

Asentria Controller Operation

These are the settings to tell the SiteBoss how you want your HVAC units to function.



Override
This drop down box is used to override the automatic system. It can be used to manually turn on the heating or cooling or vent. This setting should be set to OFF for normal HVAC operation. The Default is OFF.

Controller Logic
This sets the HVAC logic. The only available option at this time is TEMP LOGIC.

Lead Unit
This setting sets the AC unit to use as the primary HVAC unit for heating and cooling. The default is set to HVAC unit 1.

Heat Threshold
This sets the temperature threshold to turn on heating. The default is 50 degrees.

Temperature Deadband
The Deadband is the range, in degrees, that prevents the unit from having the heating or cooling rapidly turning on and off as the actual temperature fluctuates above and below the temperature setting. For heating or cooling to turn off the temperature reading will need to reach the heat or cooling threshold plus the deadband value. The default is 5 degrees.

Inside Humidity Threshold
This setting is not used in the controller TEMP LOGIC setting. In future versions, the HVAC could turn on if the Humidity reaching a defined threshold.

Temperature Difference
This setting is used to determine if secondary cooling or heating is needed. If the temperature does not change by at least the degrees set with this setting then a secondary stage heating or cooling would be initiated (if available).

Temperature Scale
This drop down box sets the temperature scales to Fahrenheit or Celsius. If toggled to Celsius, the thresholds should be adjusted to the correct temperature scale. The default is Fahrenheit.

Schedule (Hours)
Any nonzero value will define how often the lead and lag HVAC units should swap positions. This would be a value in hours, e.g. 24 for 1 day or 168 for once a week.

Cool Threshold
This field is used to set the temperature which would trigger HVAC cooling.

Humidity Deadband
The Deadband is a range that prevents the unit from having the HVAC system rapidly turning on and off as the actual humidity sensor readings fluctuates above and below the threshold setting. For the HVAC system to turn off the sensor reading would need to reach the sensor threshold plus the deadband value. The default is 5 percent. This firmware version does not use the Humidity reading to control the HVAC function.

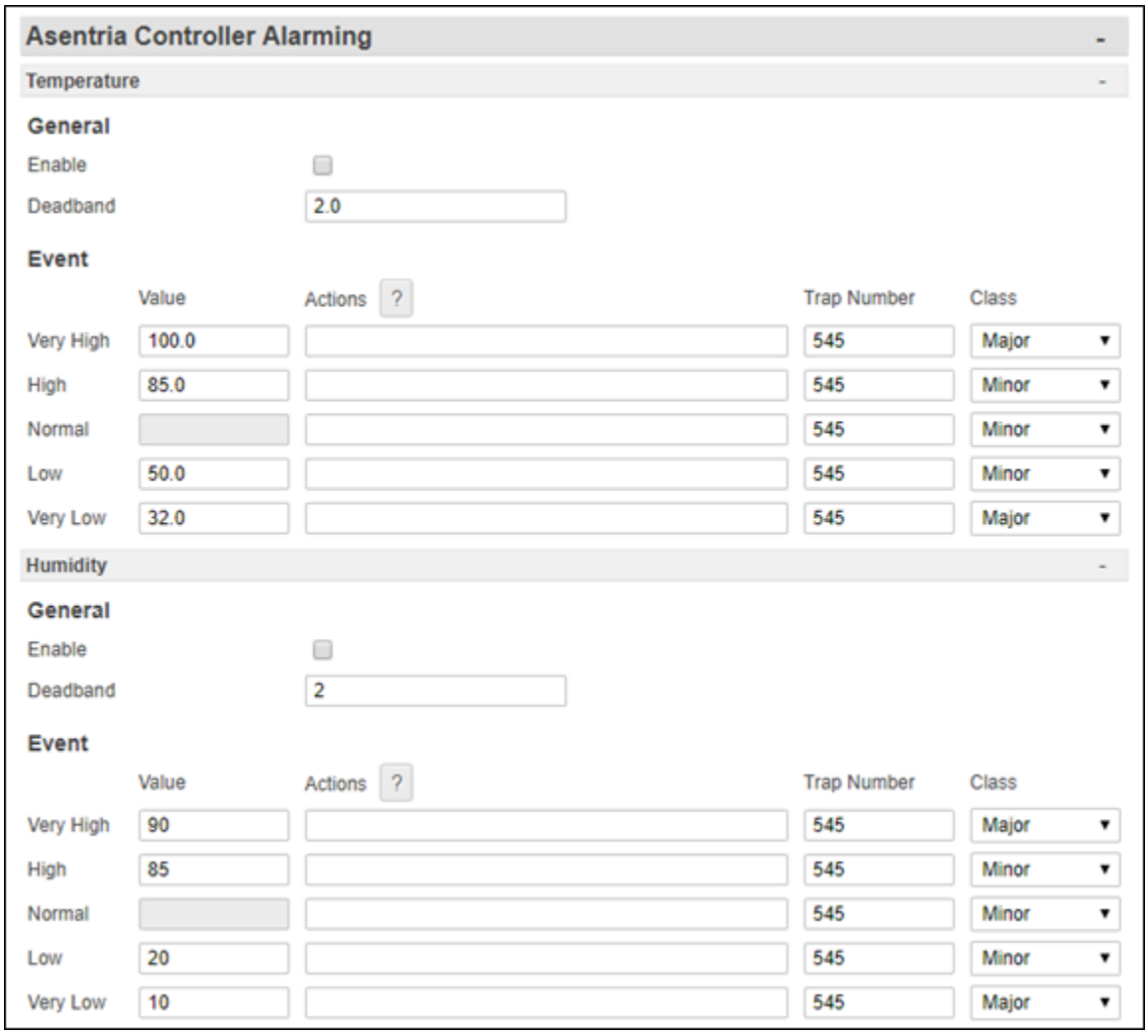
Outside Humidity Threshold
This setting is not used for the controller TEMP LOGIC setting. In future HVAC logic settings this sensor reading would be used to determine if Vent cooling would be an economic option to cool the shelter.

Humidity Difference

The controller TEMP LOGIC setting does not use the humidity readings to control the HVAC system. This setting may be used in with a different controller setting to determine if secondary cooling or heating is needed. If the humidity sensor reading does not change by at least the degrees set with this setting then a secondary stage heating or cooling would be initiated (if available).

Asentria Controller Alarming

If you wish to receive SNMP traps or Email alarms when the temp and/or humidity reach defined levels, these sections can be configured.



Enabled

The check boxes toggle ON or OFF to enable/disable the alarming functions. The default for both Temperature and Humidity is OFF (unchecked).

Deadband

The Deadband is the range on either side of a sensor setting that prevents the event from

repeatedly going in and out of the "alarm state" as the actual temperature or humidity fluctuates above or below the threshold setting. For the alarm to clear the actual sensor reading would have to pass the threshold figure plus the deadband setting. The deadband default is 2 for both temperature and humidity.

Event
The Very High, High, Normal, Low, and Very Low fields are used to set alarming actions based on user configurable temperature or humidity thresholds.

Value
These are temp or humidity threshold settings in the Scale chosen in the Asentria Controller Operation section. Once or if the temperature or humidity reaches the chosen value, then the SiteBoss would take the actions defined in the Action fields.

Actions
These text fields are used to set the action(s) that will be triggered once the temperature or humidity readings cross the defined value threshold. The "?" button will display the Actions List which lists the possible actions the SiteBoss could take and the text string format requirements. Refer to Action List chapter for more information.

Trap Number
These fields sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for HVAC Events is 545, but any number in the alternate range of 1000 — 1199 can be used.

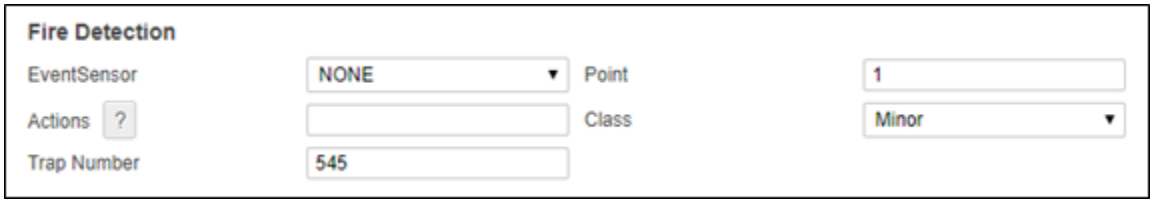
Class
The Class drop down boxes set the severity class for the event. When this drop down box is selected, a list of the classes previously defined in the Class Table is displayed.

Other

This section contains Fire Detection settings as well as Lag Unit Events.

Fire Detection

If fire detection equipment is connected to your SiteBoss, specific actions can be defined in this section.



EventSensor
This dropdown box defines the EventSensor that has the contact closure connected to the fire detection equipment.

Point

This is the point on the defined EventSensor that is connected to the Fire Detection equipment.

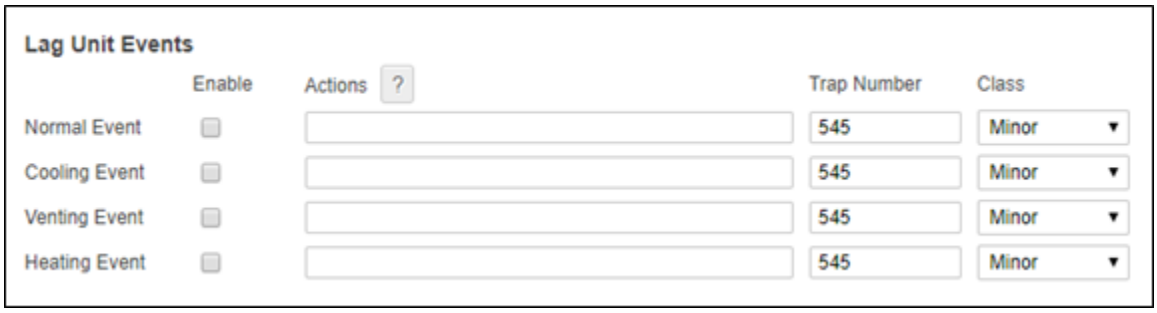
Actions
This text field is used to set the action(s) that will be triggered if the fire detection contact closure is triggered. The "?" button will display the Actions List which lists the possible actions the SiteBoss could take and the text string format requirements. Refer to Actions List chapter for more information.

Trap Number
This field sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for HVAC Events is 545, but any number in the alternate range of 1000 — 1199 can be used.

Class
The Class drop down boxes set the severity class for the event. When this drop down box is selected, a list of the classes previously defined in the Class Table is displayed.

Lag Unit Events

These fields are used to configure event actions should the Lag Unit be activated by the SiteBoss.



Enable
These are On/Off checkboxes to enable event actions for each type of possible action the lag HVAC may take.

Actions
These text field is used to set the action(s) that will be triggered if the lag HVAC unit takes the defined action. The "?" button will display the Actions List which lists the possible actions the SiteBoss could take and the text string format requirements. Refer to Actions List chapter for more information.

Trap Number
This field sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for HVAC Events is 545, but any number in the alternate range of 1000 — 1199 can be used.

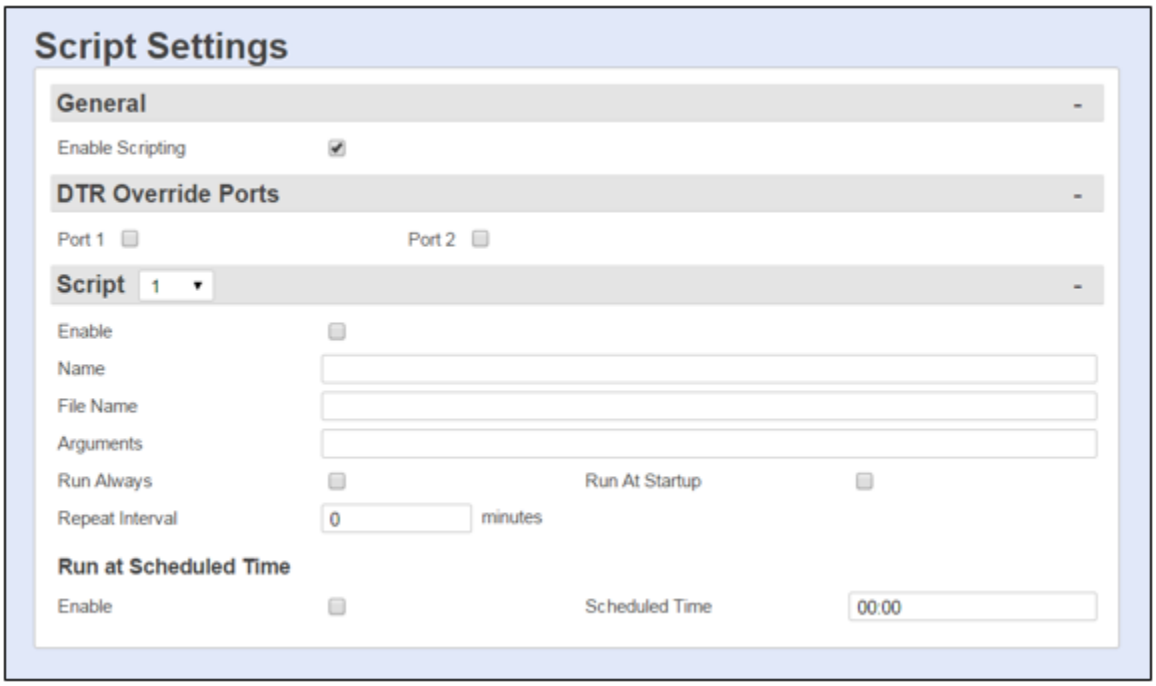
Class
The Class drop down boxes set the severity class for the event. When this drop down box is selected, a list of the classes previously defined in the Class Table is displayed.

►Scripting

Scripting provides the ability to customize the operation of an Asentria device. Scripts are written in the Lua scripting language, with access to Asentria specific functionality via a rich set of library functions. Scripts can read or change any setting on the SiteBoss, and can also create custom settings that can be accessed via setting keys.

Utilizing Lua scripting on a SiteBoss can be a complex process. In order to assist in the implementation of custom Lua scripts, Asentria has created a Feature Guide on the Asentria Product Information Portal, which goes into further detail regarding the creation and usage of Lua scripts on a SiteBoss product.

General Scripting



General Scripting

Enable Scripting

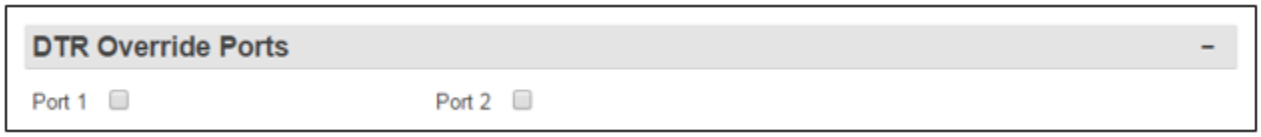
This is an ON/OFF checkbox that controls whether scripts are allowed to run on the unit at all. The default is OFF (unchecked).

»**Note**: If scripting is disabled, then scripts cannot be started either automatically or manually, and other scripting functionality such as record collection and DTR override will not happen regardless of the related settings.

»**Note**: If scripting is disabled while scripts are running, they will be issued the STOP command which could take up to 20 seconds to complete. If re-enabled, scripting will not function until after the previous scripting session is completely shut down (i.e. all scripts are stopped).

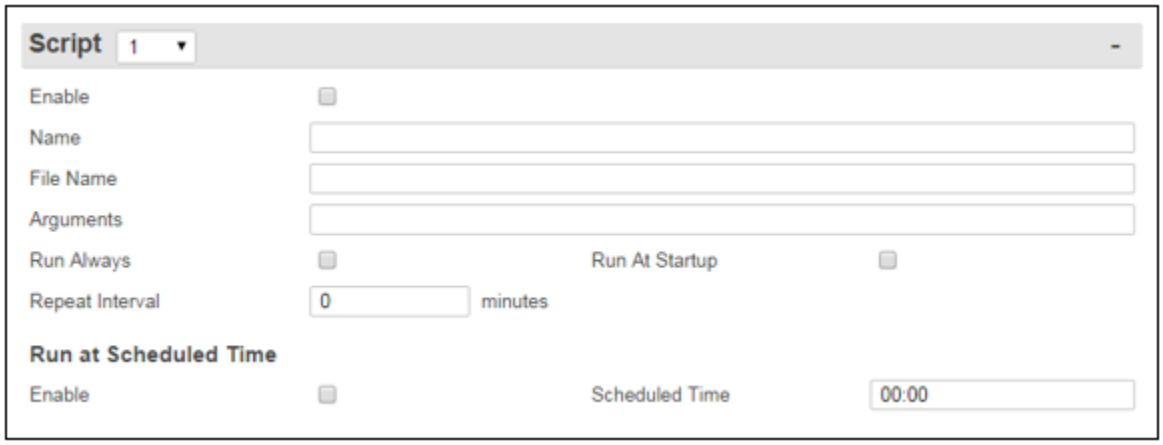
DTR Override Ports

This selection contains ON/OFF toggles to specify IO port DTR handling to be under script control. Normally the state of the DTR output pin on the IO ports is kept high. If this option is set to ON (checked), the DTR will stay low until a script changes it to the high state.



Script

Up to 20 configured scripts can be displayed by selecting the number via the drop-down box in the grey Script section.



Enable

This checkbox enables/disables the script. If disabled, the script will not run on schedule and cannot be run manually.

Name

This text box is the name of script. This is the name that is used when referring to the script, and should not be confused with the name of the script file associated with the script.

File Name

The name of the script file associated with this script. The same script file can be used with any number of scripts.

Arguments

The specified arguments are passed to the script when it is invoked on a schedule, manually from the setup menu, or via command interface commands SCRIPT START or SCRIPT TEST with no arguments specified. Prior to the script being run, the arguments are scanned for name=value pairs. For each one found, a global variable is created with that name and its value is set to the scanned value.

Run Always

If enabled (checked), the script starts after the unit starts up, and is restarted automatically if it stops for any reason.

Run At Startup
If enabled (checked), the script starts after the unit starts up. If it stops for any reason, it is not restarted unless the unit itself is restarted.

Repeat Interval (minutes)
If a non-zero value is entered, the script is run at the specified interval, measured from the last time the script was started on a schedule. The default is 0.

Run at a Scheduled Time

Enable
This is an ON/OFF checkbox to enable the scrip to run at a specified time daily. The default is OFF (unchecked).

Scheduled Time
This field sets the time each day the script should run. Specify the time in 24 hour format HH:MM

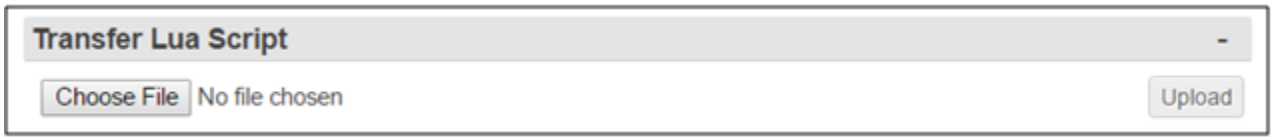
Script Editor

Scripts can be created in any text editor as long as they are saved in pure text format. Both DOS and Unix end-of-lines are supported. Before a script can be run, it must be transferred to the box and then configured. Simply putting the script file on the box will not allow it to be run.

A maximum of 20 scripts can be used on the box.

Transfer Lua Script

This option is used to load an existing Script file onto the SiteBoss. Once the Script is loaded onto the SiteBoss the General Scripting Settings will have to be configured for the script to operate on the SiteBoss.

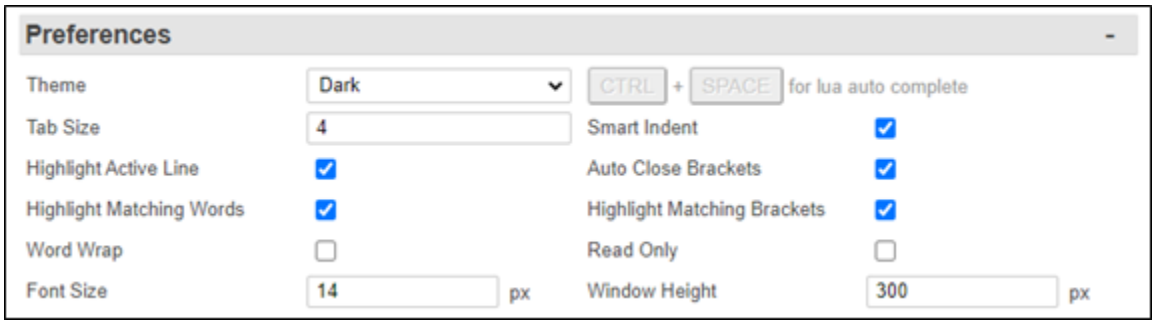


Choose File
Use the Choose File button to select a .lua script file.

Upload
Once an existing file has been selected using the Choose File button, then click ?Upload? to upload the script file to the SiteBoss.

Preferences

Clicking this bar opens up text editor setting preference options that can be changed as desired.



Theme

This drop-down box toggles between Dark and Light. Dark sets the back ground color to black and Light sets the background color to white. The default is Dark.

CTRL + SPACE for lua auto complete

This is a non-changeable setting. Typing the CTRL plus the Space bar will cause the text editor to complete the text you have started.

Tab Size

This text field sets the number of spaces for each tab. The Default is 4.

Smart Indent

This is an ON/OFF checkbox to turn on the Smart Indent feature in the text editor.

Highlight Active Line

This is an ON/OFF checkbox that turns on a highlight for the line you are working on in the text editor field. The default is ON (checked).

Auto Close Brackets

This is an ON/OFF checkbox to auto close brackets. The default is ON (checked).

Highlight Matching Words

This is an ON/OFF checkbox that causes the same word to be highlighted in the script editor. The default is ON (checked).

Highlight Matching Brackets

This is an ON/OFF checkbox to that causes the text editor to highlight a matching set of brackets. The default is ON (checked).

Word Wrap

This is an ON/OFF checkbox to cause the text editor to wrap any line too long to fit in the text field rather than shifting the view to the right. The default is OFF (unchecked).

Read Only

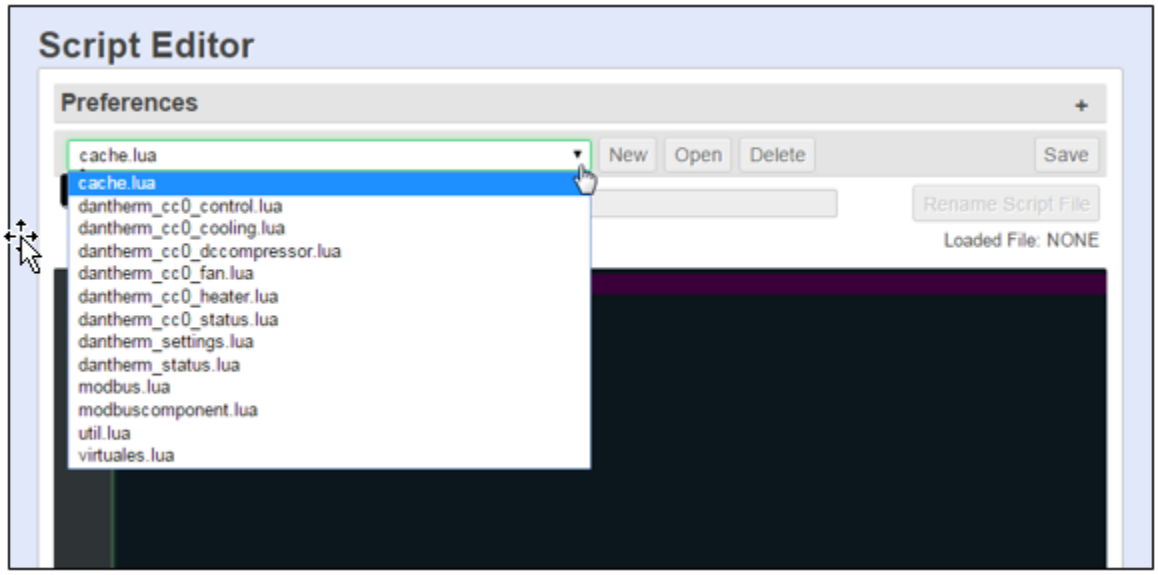
Will set the text editor to Read Only and the script will not be editable.

Font Size
This field sets the size of the font in the text editor. The default is 14 pixels.

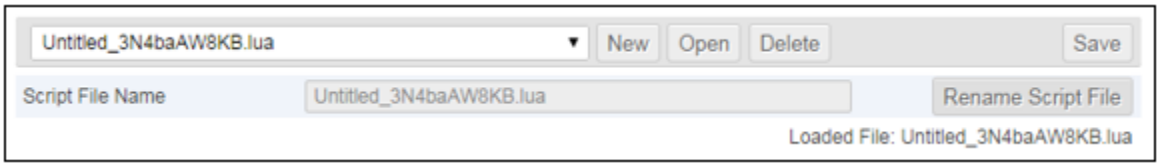
Window Height
This field controls the vertical size of the text editor window. The default is 300 pixels.

Script Editor

The drop-down box will list all scripts that have been loaded onto this SiteBoss. If "New" is clicked a randomly generated "Untitled" document will be created. Click Rename and the default name can then be edited in the "Script File Name" field. Then click "Confirm Rename".



If an existing script name is chosen then click Open to display the existing script file. A "Rename Script File" button is available to change the name of the script. Click "Confirm Rename" to save the change.



To delete a script, select it from the drop-down box and click the Delete button. A pop up confirmation box will appear. Click OK to confirm and delete the file.

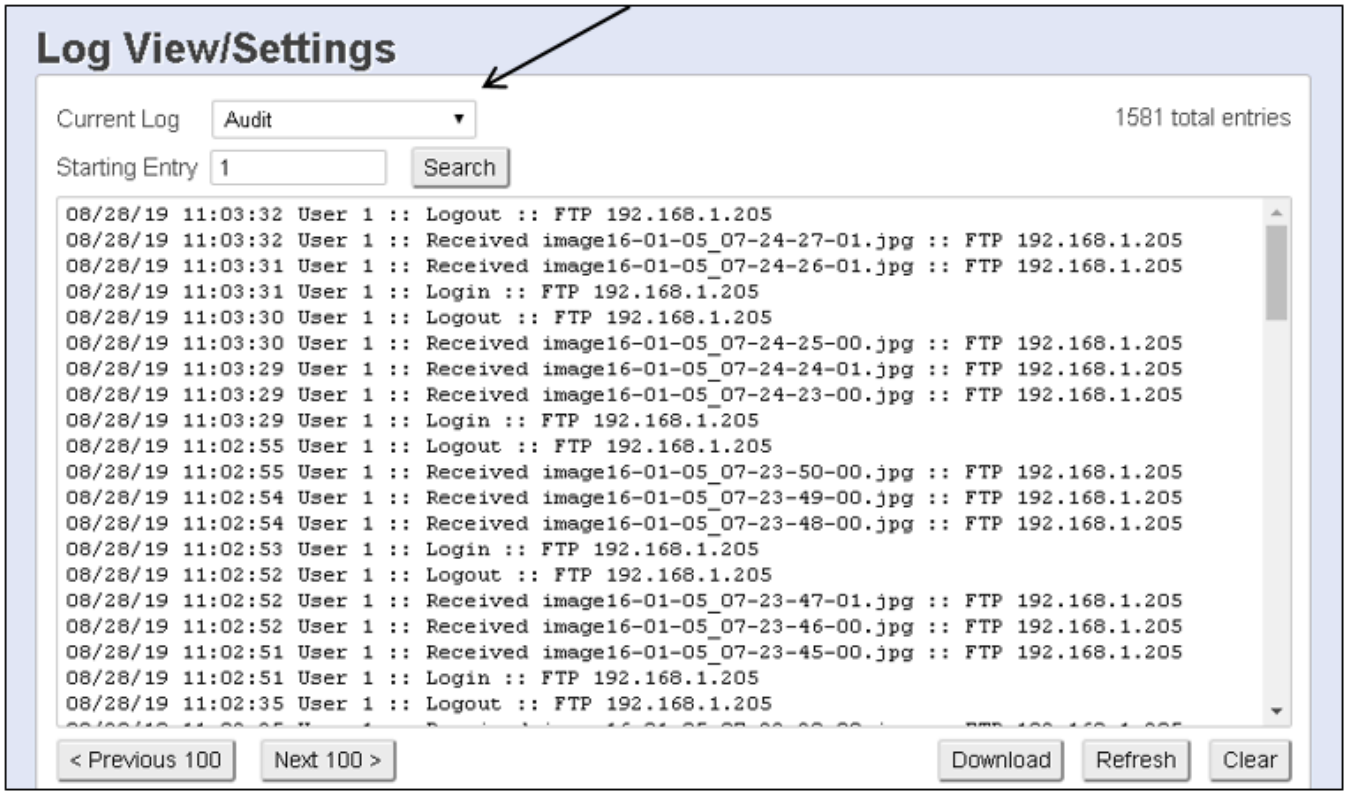
A script can be written using the Script Editor or any text file can simply be cut and pasted into the field. Click the "Save" button before leaving the page to save your work.

For a script to be run, it will need to be configured in the General Scripting section.

►Administration

System Logs

There are two available logs to view in the upper section of the page. The drop-down box allows you to toggle the view between the Audit and the Event Logs.



Starting Entry

This field allows the view to be rapidly moved between views. The view is 100 entries per page. The total number of entries available entries to view is listed on the right side of the display. To move to a specific entry enter the number in the text field and click the Search button.

< Previous 100 / Next 100 >

The previous 100 and Next 100 buttons will retrieve and display the Previous 100 or the Next 100 log entries, as clicked.

Refresh

The Refresh button will retrieve and reload the log file to view. The display will update with any new entries. The display will begin at entry number 1.

Clear

This button purges the records within the Events File.

» Caution: All of the records in the Log File are deleted immediately when this option is selected. The button deletes the records in the SiteBoss, not just the displayed records.

Event Log Settings

The Event Log is a record of all sensor events that occur within the SiteBoss.

The Event Log overwrites itself when it becomes full. ?Full? has meaning that you can control with the Maximum File Size setting. This setting controls the maximum size (in KB) to which the file should be limited. If the setting is 0 then the audit log?s only constraint on size will be the available physical memory.

Enable Events Log File
This checkbox is an ON/OFF toggle to enable Event logging. The default setting is ON (checked).

Store Sensor Events
This checkbox is an ON/OFF toggle to enable storing records generated by environmental sensors. The default setting is ON (checked).

Date/Time Stamp Data Alarm Records
This checkbox is an ON/OFF toggle to prepend a Date/Time stamp to the beginning of data alarm records. The default setting is ON (checked).

Prepend Data Alarm Name
This checkbox is an ON/OFF toggle to prepend the name of the Data Alarm to the beginning of the data alarm record. This aids in identifying which Data Alarm an alarm record is associated with. The default setting is ON (checked).

Store Data Alarm Records
This checkbox is an ON/OFF toggle to enable storing data alarm records. The default setting is OFF (unchecked).

Maximum File Size
This drop-down box sets the maximum number of KB the Event Log can reach before overwriting the oldest records. The available options are 0, 32, 64, 128, 256, 512 and 1024. The default setting is 64 KB.

Audit Log Settings

The Audit Log is a record of a variety of actions that occur within the SiteBoss. The File is accessed and controlled under the same policies which govern how you would generally access buffered data. For example, you can have the audit log FTP-pushed.

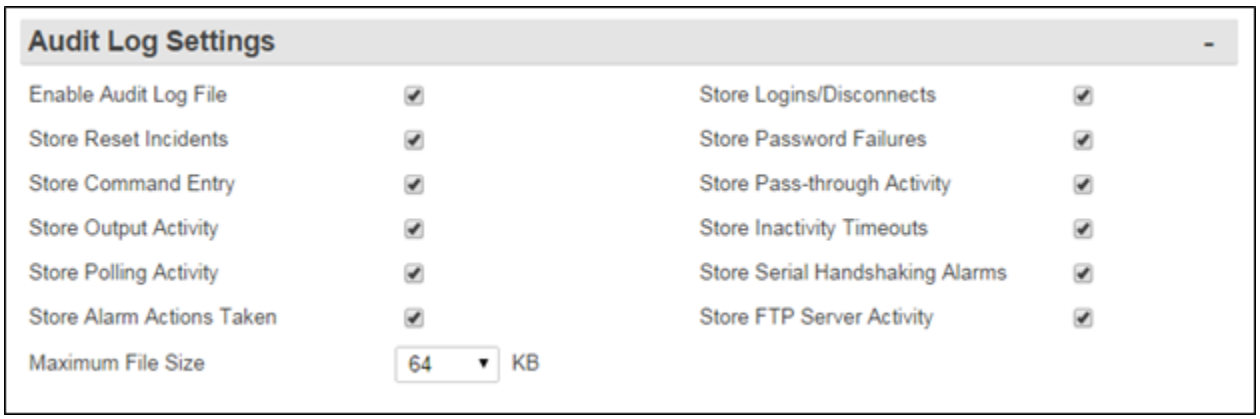
The Audit Log overwrites itself when it becomes full. ?Full? has meaning that you can control

with the Maximum File Size setting in the lower section of the page. This setting controls the maximum size (in KB) to which the file should be limited. If the setting is 0 then the audit log?s only constraint on size will be the available physical memory.

Automatic Logging of Certain Actions

Certain actions are automatically written to the Audit Log anytime it is enabled. These actions are:

- When a user changes the configuration via a Setting Key
- When a user connects, disconnects, or transfers a file via the unit?s FTP server
- When a GPS positional fix is acquired or lost by the optional installed GPS card
- When the wireless modem connects or disconnects (due to failure in the latter case) from the wireless network



Enable Audit Log File

This checkbox is an ON/OFF toggle to enable Audit logging. The default setting is ON (checked).

Store?

The checkbox options beginning with the word Store are ON/OFF toggles to enable logging of the specific action described. The default setting for all is ON (checked).

Maximum File Size

This drop-down box sets the maximum number of KB the event log can reach before overwriting the oldest records. Available options are 0, 32, 64, 128, 256, 512, and 1024. The default setting is 64 KB.

System Administration

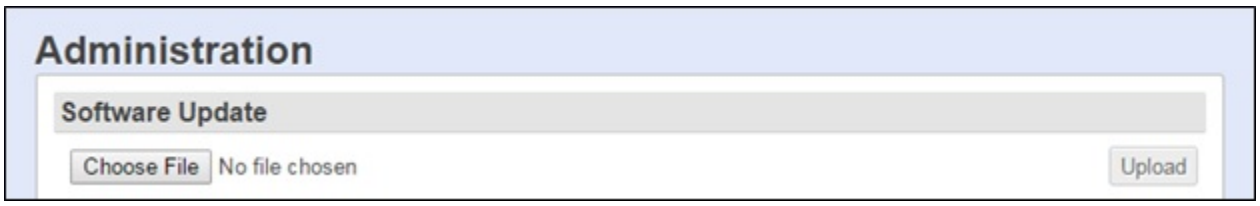
This menu selection allows the update of the software on the SiteBoss, Transferring settings to or from the unit, resetting settings to factory defaults and a button to restart the SiteBoss.

Software Update

You must be logged in with a MASTER security setting for this field to be visible. Software updates are occasionally available from Asentria Technical Support. Save the file on a computer or server accessible by the SiteBoss.

»Note: It is advisable to back up your settings before a software update. Use the instructions at the Get Settings from Unit section for instructions.

Click the "Choose File" button and navigate to your saved software file and select it. You will see the file name next to the button.



Click the "Upload" button. This is a large file so it may take a few minutes to load depending on the connection speed of your network. Do not navigate away from the Administration page until the SiteBoss completes loading the file.

Once the file loads the SiteBoss will begin to process the update. After approximately a minute the unit will become unresponsive. All of the lights on the unit will flash during the update, and then the SiteBoss will reboot. This process takes approximately five minutes. Once the unit reboots the user will need to log back into the unit and it will be available to use normally.

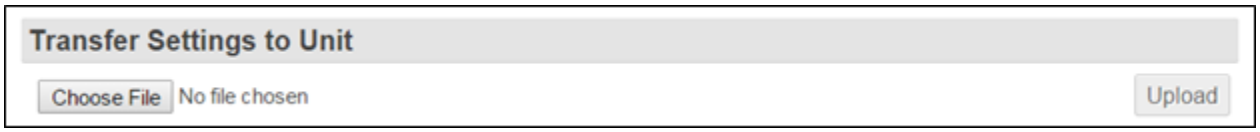
» Note: DO NOT REMOVE THE POWER TO THE SITEBOSS DURING THE SOFTWARE UPDATE PROCESS. Powering down a SiteBoss mid-update will likely disable the unit. If the unit loses power during the upgrade process and becomes uncommunicative contact Asentria Technical Support.

Transfer Settings to Unit

Settings from one SiteBoss can be transferred to another. This is a way to quickly configure multiple units with the same settings.

Save the text file with settings you wish to transfer to this SiteBoss on a computer or server accessible by the unit.

Use the Choose File button to navigate to your saved settings file. Click the Upload button. The settings will be installed immediately.

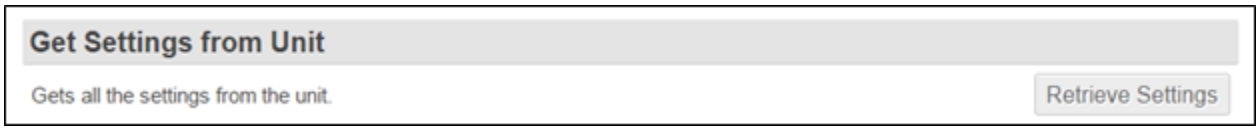


» Note: If you using a full settings file from another unit, remove or update settings that would not apply to the new unit, such as the network settings and event sensor IDs, before transferring the file to the SiteBoss.

Get Settings from Unit

Clicking this button will download a large text file will all of the settings from your SiteBoss.

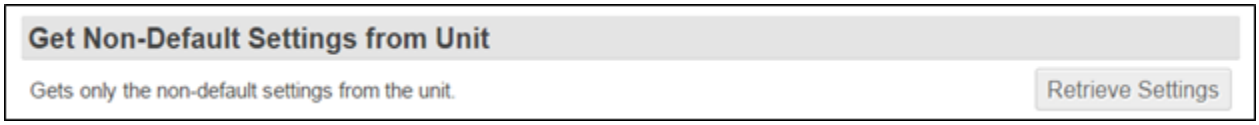
Save the file as a backup for this unit or the settings can be used to configure another SiteBoss.



» **Note:** If you are going to use this file to update another SiteBoss, remove or update settings that would not apply to the new unit, such as the network settings and event sensor IDs, before transferring the file to the new unit.

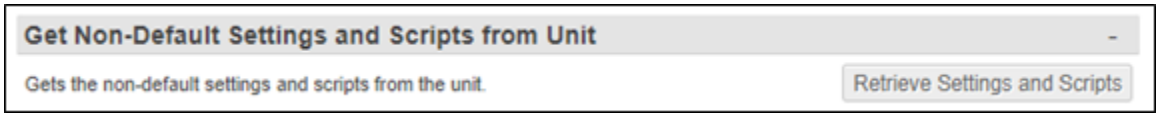
Get Non-Default Settings from Unit

Clicking this button will download a text file of all the settings that are not set to the factory defaults. This file is much smaller than a full settings key file that is retrieved with the "Get Settings from Unit" button. Since this file is considerably smaller it is easier to work with for transferring to another SiteBoss. It is most appropriate in configuring a unit that has its setting set to the factory defaults.



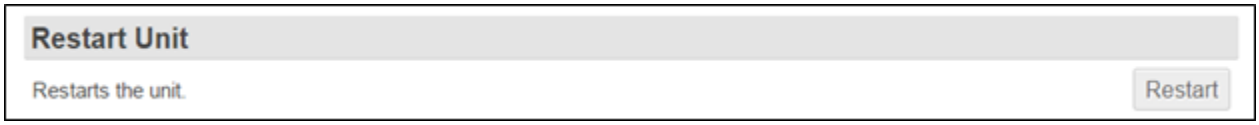
Get Non-Default Settings and Scripts from Unit

Clicking this Retrieve Settings and Scripts button will download a text file of all the settings that are not set to the factory defaults plus any Script files that are on the unit.



Restart Unit

Clicking this button will restart the SiteBoss. It will take approximately 60 seconds to complete the reboot process and the users will need to log in again once the reboot is complete.



» **Note:** If the unit has been up for less than 5 minutes, then the restart operation will pend until the unit's uptime reaches 5 minutes.

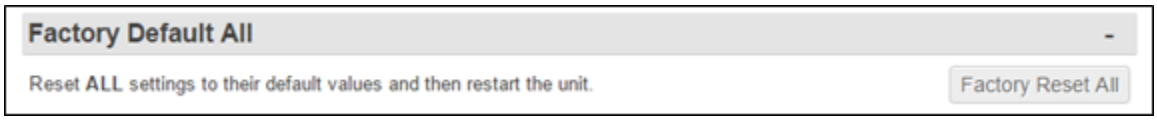
Factory Default

This button will reset most settings EXCEPT network, serial, and data alarms to their factory default values and then restart the unit. All other settings will need to be reconfigured or downloaded from a backup file.

You will get a "Are you sure you want to reset all custom settings EXCEPT network, serial, and data alarms?" popup message. Click OK to reset your settings.

Factory Default All

This button clears all custom settings from the SiteBoss and sets all settings to their factory defaults.



You will get an "Are you sure you want to reset all custom settings?" popup message. Click OK to reset your settings.

Actions List

The Actions List provides you with a flexible mechanism to tell the unit how to react to events. An action list is a text string that specifies what the unit should do upon an event. These action strings are used both in the Web Interface Actions text boxes and the Command Line Interface Event Actions options. It is a list of keywords and parameters separated by semicolons. Each keyword specifies a certain action and has its own parameter set, which is enclosed in parentheses.

```
Action fields accept one or more commands separated by a semicolon.

ASM Event: asme or asme(now|later)
Cancel : cancel(idname)
Check Alive : checkalive(CPE# or host, delay)
Continue: continue(id)
Dialup Pager : dpage(index)
Dispatcher : dispatch(phone# or index)
Email : email(email or index)
Group : group(groupname)
ID : id(id name)
Inform : inform(ipaddress or index)
Malert : malert(phone# or index)
Modem : modem(phone# or index)
Non-global : nonglobal
Pause : pause(seconds)
Postpone : postpone(idname, seconds)
Power : power(action, eventsensor, point)
Relay : relay(action, eventsensor, point)
Script : script(action, name or number)
```

```
SMS : sms(phone# or index)
Stop if any/all actions OK : okstop(any|all)
Syslog : syslog(ipaddress or index, optional facility,level)
Talert : talert(ipaddress or index)
Trap : trap(ipaddress or index)
```

ASM Event

Send a KRP SIREN message via network to a KRP server.

- ASME or ASME(NOWILATER)

Cancel

This action cancels any running action, identified by idname.

- CANCEL(IDNAME)

Check Alive

This action causes the unit to ping a host, identified using the Ping Alarms settings in the web GUI or CPE Settings in the CLI or by an IP address specified in the action. The Delay parameter is optional, if omitted then the unit assumes 60 seconds for a timeout. If the first parameter is a Device/CPE number then this action means the unit will wait for the device to be alive, up to the defined timeout number of seconds, using that Device's configured keep-alive (ping) interval. If the first parameter is a hostname or IP address, then the unit will wait for this host to be alive, up to the defined timeout number of seconds, using a ping interval of 3 seconds. This action holds up subsequent actions in the same action list from processing until the timer expires or the device is seen as alive. If the device is not alive for the timeout period then it is noted in the audit log. If a Ping Alarm Device number (CPE number) is used, the Ping Alarm Event (CPE Alarm) does not need to be enabled, but the device settings must be configured.

- CHECKALIVE(CPE# OR HOST, [DELAY])

Continue

Continue any event identified by idname that has either paused or postponed its action processing.

- CONTINUE(ID)

Dialup Pager

Send a pager callout via Dialup POTS modem to a number specified by index number. This option is available on units with a Dialup POTS moden only.

- DPAGE(INDEX)

Dispatcher

Send a Dispatcher alarm via a Dialup POTS modem to a number specified by index number.

This option is available on units with a Dialup POTS moden only.

- DISPATCH(PHONE# or INDEX#)

Email
Send an email notification to an address specified by index number which can be configured in Actions Settings/Email section or delineated in the action.

- EMAIL(EMAIL or INDEX#)

Group
Group is used to identify this action list as part of a group identified by group name, not currently used.

- GROUP(GROUPNAME)

ID
Identify this action by a descriptor, for reference in other action.

- ID(IDNAME)

Inform
Send an SNMP inform to a specific IP address or index which refers to an IP address or host name configured in the Actions Settings/TCPIP section.

- INFORM(IPADDRESS or INDEX#)

Malert
Malert sends a malert (Asentria Alarm via modem) to a number specified by index number. This option is available on units with a Dialup POTS moden only.

- MALERT(PHONE# or INDEX#)

Modem
Make the unit dial a phone number via the POTs modem to a specified index number and start a login session (to the unit's command processor) with the answering machine. This option is available on units with a Dialup POTS moden only.

- MODEM(PHONE# or INDEX#)

Non-global
Insert this action at the beginning of any event's action list to exempt this event from any global actions or global trap number that is configured. If the nonglobal action is inserted in the action list, it must be inserted first in order to unambiguously tell the unit that actions to process

should be excepted from global treatment.

- NONGLOBAL

Pause

Pause operation for a duration specified by seconds.

- PAUSE(SECONDS)

Postpone

Postpone an already-running action identified by idname for a duration specified by seconds.

- POSTPONE(IDNAME, SECONDS)

Power

Using this action puts a power output into a defined state, determined by the action parameter.

Action: one of the following two words, by case-insensitive exact match: ON or OFF

EventSensor: the number of the EventSensor that has the specified output, where it is the same as that referred to by the index in an EventSensor key (e.g., 200 for an internal EventSensor).

Point: the number of the output (1-based) on the specified EventSensor.

- POWER(ACTION, EVENTSENSOR, POINT)

Relay

Put a relay in a certain state specified by the action indicator.

Action: one of the following two words, by case-insensitive exact match or partial unambiguous match

ACTIVE or INACTIVE. ?Active? means to put the relay in the Event State. For a relay this could be energized or de-energized depending on the relay configuration.

EventSensor: the number of the EventSensor that has the specified relay, where it is the same as that referred to by the index in an EventSensor key (e.g., 3 an EventSensor in slot 3).

Point: the number of the relay (1-based) on the specified EventSensor.

- RELAY(ACTION, EVENTSENSOR, POINT)

Script

Starts or stops a script

Action: the case-insensitive exact match of EXEC or KILL

Name: the registered name of the script

Number: the number of the registered script

- SCRIPT(ACTION, NAME OR NUMBER)

SMS

Send an SMS message to a specific phone number or index which refers to a phone number configured in the Actions Settings/Dialout menu.

- SMS(PHONE# or INDEX#)

Syslog

Send a syslog message (via UDP port 514) to the specified address. The facility and level parameters are optional numbers but both must be supplied if either is necessary. The default facility is 1 ("user") and the default level is 6 ("informational").

- SYSLOG(IPADDRESS or INDEX#, optional FACILITY,LEVEL)

Stop

Conditionally stop action processing based on the outcome of actions prior to this keyword in the actions list. The parameter specifies how much of the prior actions for this even must be successful in order for the unit to stop processing the actions list: any action or all actions.

- OKSTOP(ANY|ALL)

Talert

Send a talert (Asentria Alarm via TCP) to a server identified by a hostname index defined in Actions Settings/TCPIP section or by an IP address specified in the action list.

- TALERT(IPADDRESS or INDEX#)

Trap

Sends an SNMP Trap to a server identified by a hostname index defined in the Actions Settings/TCPIP section, or by an IP address specified in the actions list.

- TRAP(IPADDRESS or INDEX#)
- To send a SNMPv3 trap, the correct syntax is: TRAP(INDEX/IPADDRES,3)

Command Line Interface (CLI)

►Basics

The CLI is structured in a series of menus and submenus. Most of the elements you will interact with will be under the setup menu which you reach by typing SETUP at the command prompt. Unless overridden by your terminal emulator local echo is enabled by default. This means that you will be able to see commands as you type them. To select a menu item enter the corresponding letter next to the item. You will be immediately taken to that item's configuration menu. Use <Enter> or <Esc> to go back a level, or <Ctrl+C> to return directly to the command prompt.

»Note: Be aware that the <Esc> key is (by default) coded as the escape character for certain operations (such as serial bypass). As such, there may be times where the use of the <Esc> key to go back a level will result in unexpected behavior.

Setup Menu Inputs

There are several different types of inputs employed within the Setup menu. This section will discuss the different types you will encounter.

String

The most common is the string type of option you will find. Below is an example of a string entry:

```
A) Site Name                    [Test Site]
```

When selected, this setting will provide a prompt requesting a new value. You may press < Enter > or <ESC> to abort the option entry or press <SPACE> and < Enter > to delete the current value and leave it blank. Some numerical or required settings will not allow a user to leave an option blank, so pay attention to the unit's response when attempting to delete a setting's value.

Toggle

The second most common option type is the toggle type option:

```
A) Enable Web Interface      [OFF]
```

When selected, this option will not prompt for a new value. It will simply cycle to the next available option in its list. This switch type is typically used for options with two or three

choices. Most often it is in an ON/OFF form, but could be a series of options such as "NONE", "1" and "2".

Option list

The option list type is similar to the toggle type in that it has a list of options to choose from. The letter adjacent to the option would be selected to choose that option.

```
SiteBoss 340 - Serial Port 2 Baud Rate
A) 300
B) 600
C) 1200
D) 2400
E) 4800
F) 9600
G) 19200
H) 38400
I) 57600
J) 115200
```

After selecting an option, you are immediately returned to the previous menu. The new value will be displayed to the right of the setting name, letter, or number.

Alarm Actions (Action list)

Alarm actions have their own unique method of entry. Refer to the Actions List section for more information.

►CLI Status Pages

The SiteBoss status pages are informational displays. Most of the information that a user would need to know about the unit is displayed on these screens. This section outlines the different status screens, how to display them and defines the displayed fields.

General Status

You reach this status screen by typing **`STATUS`** or **`?`** at the command prompt followed by <Enter>.

```
SiteBoss 550 2.12.290 STD     Serial #  : 550002553
Site Name : 550002553
Date      : THU 03/27/21       1:  19200,8N1  I/O 1
Time      : 14:25:51           2:  19200,8N1  I/O 2
Modem     : Yes
Eth 1     : STATIC
IP Add    : 0.0.0.0
MAC Add   : 00:10:A3:60:49:97
IPv6      : OFF
Eth 2     : STATIC
IP Add    : 0.0.0.0
```

```
MAC Add    : 00:10:A3:60:49:98
IPv6       : OFF
```

SiteBoss 550
This indicates that this product is the SiteBoss, followed by *2.11.430 STD*, which is the currently loaded firmware version.

Site Name
This field displays the identifier assigned to each SiteBoss by the end user in the General Settings menu. It defaults to the units factory assigned Serial Number.

Date** and **Time
These two fields display the current date and time. The Date and Time can be set in the General Settings menu under the Date/Time Setup option.

odem
This field indicates whether the optional internal modem is installed. It will indicate "Yes" if the POTS modem is installed. It will indicate "None" if no modem or if a Wireless modem card is installed.

Eth n
These fields displays STATIC, DHCP, VLAN or EXPANSION BRIDGE, depending on which mode each of the two Ethernet interfaces is configured for. The settings can be configured in the Network Settings menu under Ethernet Settings.

IP Add and MAC Add
The fields immediately following the Eth fields are the network IP address assigned to each Ethernet port, and that cards MAC address. The MAC address of the Ethernet interfaces can also be found on the unit?s serial number label.

IPv6
These field will display OFF, STATIC or AUTO to indicate how the Ethernet Ports are configured. Use the Ethernet Settings Menu in the Network Settings section to adjust the settings.

Serial Number
The Serial # field displays the factory-assigned, unique serial number for this SiteBoss.

n: 19200,8N1 I/O n
These fields are a listing of all installed serial ports in order. They display the current baud rate and parity settings (19200, 8N1) followed by the target name of the port. This target name is used in event notifications. The serial port settings can be configured in the Serial Settings menu for each port. An asterisk following the baud rate and parity indicates that there is data stored in the file associated with that port.

EventSensor Status

This status menu is accessed by typing **Sensors** or an **!** at the command prompt followed by <Enter>. It serves as a quick-access menu to all of the EventSensors installed in your SiteBoss, and allows you to read their current status. Configuration of these sensors must still

be done in the Alarm/Event Definitions menu using the EventSensor Device Settings submenu options. Below is a screenshot of a SiteBoss 550 configuration. Your setup will likely differ significantly depending on installed sensors and slot cards.

```
SiteBoss 550 Current EventSensor Status
    Configuration           Location  Name                  ID        Alive
A)  1-TS, 6-CC              Internal  INTERNAL              --------  -
B)  8-VS                    Slot 4    unnamed               2004B608  Y
C)  4-VS                    Slot 5    unnamed               3F05B608  Y
D)  8-RL                    Slot 6    R3                    0B06B608  Y
E)  9-PW                    External  unnamed               4F17B608  Y
F)  4-CC                    Remote    unnamed               02050000  Y

Selection?
```

Configuration
This column is the shorthand name of the sensor. Common examples include CC for contact closures, VS for voltage sensors, RL for relays, TS for Temperature Sensor and HS for Humidity Sensor.

Location
This column refers to where the sensor is installed. Internal sensors would include any serial port installed in the SiteBoss (which can be configured as contact closures) as well as the temperature sensor if one is installed in the MMC Memory IO slot. External refers to sensors installed in the SENSOR port. The Slot n locations are the slot cards oriented right to left per figure in the Back Panel section of this manual. Remote would refer to sensors connected to another Asentria unit that is configured to report to this unit using our EventSensor Reporting functionality..

Name
This field is the user-defined name for the sensor. It is listed as "unnamed" if the user has not defined one, or in some cases can be a pre-defined string that the sensor reports by default until changed by the user. The names can be changed via the Alarm/Event Definitions Menu under EventSensor Device Settings.

ID
This field displays a unique identifier for all EventSensors connected to the unit. These identifiers are factory defined.

Alive
This field reports whether or not the sensor is currently functioning (recognized by the system). Its values can be "Y" for yes or "N" for no. The internal CC (Serial Port) locations will simply have a dash "–" mark.

Detailed EventSensor Status

To view more detailed information about a sensor, such as the status of a specific point on a card, enter the letter corresponding to the sensor. The information displayed will vary as it is specific to the sensor. These are display only fields, the EventSensors are configured via the Alarm/Event Definitions/EventSensor Device Settings submenu.

```
Selection? D

EventSensor ID: 2004B608
Name: unnamed

Analog Inputs:
 1 unnamed                -48.0 Volts
 2 unnamed                  0.0 Volts
 3 unnamed                  0.0 Volts
 4 unnamed                  0.0 Volts
 5 unnamed                  0.0 Volts
 6 unnamed                  0.0 Volts
 7 unnamed                  0.0 Volts
 8 unnamed                  0.0 Volts


Press Enter to return to the EventSensor Status Menu or any other key to quit.
```

Power Distribution Status

If you have a PowerBoss attached to the SiteBoss via the sensor port you can view the status of the power output via the Power Distribution status screen. This display provides information in real time for the current and voltage of any attached power outputs.

To view the Power Distribution Status screen, from the command prompt enter the command **?POWER** (or **?POW** or even **?P**) plus the slot number of that attached PowerBoss. The slot number is set with the DIP Switches on the PowerBoss. You can check for the current setting at SETUP? Alarm/Event Definitions? EventSensor Device Settings. The "Number" column is a display of the configured slot number.

```
>?power 9
SiteBoss 550 Power Distribution Status for Controller 9

Main Voltage   : 44.614 Volts
Total Current  : 0.064 Amps
Total Power    : 3 Watts

PB2 Current : 0.064 Amps

Power Output
   Name              State      Current        Fuse
 1 unnamed           OFF          0.000 Amps    OK
 2 unnamed           OFF          0.000 Amps    OK
 3 unnamed           OFF          0.000 Amps    OK
 4 unnamed           OFF          0.000 Amps    OK
 5 unnamed           OFF          0.000 Amps    OK
 6 unnamed           OFF          0.000 Amps    OK
 7 unnamed           OFF          0.000 Amps    OK
 8 unnamed           OFF          0.000 Amps    OK
 9 unnamed           OFF          0.000 Amps    OK
```

Power output states can be toggled at SETUP ? E) Alarm/Event Definitions ? Select the letter adjacent to the Power Boss ? Select the letter adjacent to the output to toggle ? Select B) State and confirm the "Are you sure" prompt with a "y".

Main Voltage
The Main Voltage displays the voltage across the main power bus bars.

Total Current
Total Current displays the total current drawn by the PowerBoss and the devices connected to all of the power distribution outputs.

Total Power
Total Power displays the total power drawn by the PowerBoss and all of the power distribution outputs (Main Voltage times Total Current).

PB2 Current
PB2 Current displays only the current drawn by the PowerBoss.

Power Output
The Power Output section lists each of the 9 on-board and any optional installed power distribution outputs showing their Name, State (ON or OFF), and the Current that connected devices are drawing, and the Fuse status of each (OK or BLOWN).

Wireless Modem Status

This status screen will display general information and connection status of any installed wireless modem. It is reach by typing **?W INFO** at the command prompt. Depending on the type of wireless modem installed different fields will display.

```
>?w info
Wireless Modem Information:

  General State:
     State                  : Modem is connected, link is established.
     Modem Status           : Connected
     Signal Strength        : 67% (rssi 21, ber 99) (19:16:25 ago)

  Network Registration:
     Registration Status    : Registered to home network

  Subscriber and Equipment:
     Phone Number           : 2065959162
     Local IP Address       : 166.161.141.999
     Manufacturer ID        : Sierra Wireless, Inc.
     Model ID               : MC5728V Rev 1.0 (0)
     ESN                    : 09612854006 (0x60C422F6)
     Revision ID            : p2811301,53477 [Jul 15 2009 15:51:31]
```

All modems should display the "General State" and "Network Registration Status" fields which display information regarding the connection status with the wireless carrier.

The Subscriber and Equipment section will display information regarding the modem installed including any assigned Static IP address and the ESN of the modem.

AC Power Monitors

The status of all AC power monitors can be displayed using the **STATUS AC** command, or **?A** for short.

```
>?A
SiteBoss 550 AC Power Monitor Status

                                 Average    Average                Total
ACMon Name                 Alive  Voltage    Current   Frequency  Real Power
===== ==================== ===== ========== ========== ========== ==========
  1   Watson               Yes    120.50 V    11.44 A   60.00 Hz     3680 W
  2   Yoda                 Yes    120.70 V    11.88 A   60.02 Hz     3728 W
```

Only AC power monitors with **device** set to something other than "NONE" will show up in this list. If the device name is more than 18 characters it will be truncated.

Single AC Power Monitor

The status of a single AC power monitor can be displayed using the **STATUS AC *n'*** *command, or* ***? A*** **n** *for short, where n is the number corresponding to the desired AC power monitor (between 1 and 6). This status page will display the available power readings from the selected monitor.*

```
>status ac 1
SiteBoss 550 AC Power Monitor 1 Status

Name: Watson
State: Alive

Totals                       Present      Average    Minimum    Maximum
========================== ============== ========== ========== ==========
Average Voltage (Volts)       120.60       120.91     117.40     124.30
Average Current (Amps)          6.48         9.63       3.12      35.08
Frequency (Hz)                 60.00        60.00      59.80      60.10
Real Power (Watts)              1760         3073        880      11600
Reactive Power (VAR)             120          285      -1320       2680
Apparent Power (VA)             2360         3506       1160      12240
Power Factor                    0.75         0.76      -1.00       1.00
Energy (Wh)                 69190040
Reactive Energy (VAR)        2377000
Apparent Energy (VA)        81114840

Phase Data                  Phase A    Phase B    Phase C
========================== ========== ========== ==========
Voltage (Volts)             120.80     120.10     121.00
Current (Amps)                5.92       8.48       5.00
Real Power (Watts)             544        764        452
Reactive Power (VAR)            36         76         -4
Apparent Power (VA)            724       1016        612
Power Factor                  0.75       0.75      -0.74
```

If the specified AC power monitor has the **device** configured to "NONE", or the number is illegal (not between 1 and 6), an error message will be displayed.

CPE Status

CPE (Customer Premises Equipment) status. If the CPE Alarm Settings functionality has been configured a status of configured equipment will display. To display the CPE Status type ?CPE or ?C for short and any configured devices will display.

Up in the St column indicates the device is answering Pings as set up at Network Settings/ CPE Settings. If the device is not responding the ST column will have an !.

```
>?c
SiteBoss 550 CPE Status - All Devices

 #   Device          St |  #   Device          St |  #   Device          St |
====================== | ====================== | ====================== |
 1 : Desktop         UP |  2 : S571           UP |  3 : S350           UP |
 4 : S450            !  |  5 : S550 NKR       UP |  6 : VZW S550       UP |
 7 : S220            UP |  8 : S340           !  |  9 : S550 Classic   UP |
---------------------- | ---------------------- | ---------------------- |
10 : T850 JITC       UP | 11 : Camera         !  | 12 : Asentrium      !  |
```

►Setup Menu

This section will cover the menu options and settings configurations. This section covers using the Command Line Interface menu tree and structure. Most of these settings can also be controlled via the Web Interface. See the Settings Menu section for specifics using the Web Interface.

This section of the manual displays screen shots and descriptions taken from the command prompt menu system. This menu can be accessed via Telnet, SSH or serially via IO2. See the Accessing the SiteBoss Telnet section for instructions on accessing the SiteBoss via Telnet or the Access via a Serial Connection for instructions on accessing the SiteBoss via IO2.

The Main Setup Menu is accessed by typing **SETUP** followed by <Enter> at the SiteBoss command prompt, and is organized in a logical tree structure. To use the menu tree enter the letter adjacent to the desired menu option and the menu associated with that option will display. Use <Enter> or <Esc> to go back one menu level, or <Ctrl+C> to return directly to the command prompt.

```
>SETUP

SiteBoss 550 - Main Setup Menu
A) Network Settings
B) Serial Settings
C) Modem Settings
D) Security Settings
E) Alarm/Event Definitions
F) Action Definitions
G) General Settings
H) Event Log Settings
I) Audit Log Settings
J) Scripting Settings
```

```
Enter your Selection:
```

Each section in this chapter will go over one of the above setup branches, outlining the options within.

The SiteBoss processes setup changes in real time. In other words, the unit begins to implement changes to its configuration as soon as they are entered. There is no need to exit the Setup menu or reboot the unit to apply changes. The exception to this rule is IP-specific network settings. Changes to these settings are implemented only after all open Telnet command processors are closed.

Network Settings
This menu tree contains settings for network communication, routing, VPN ,SNMP, Email and more.

Serial Settings
Choosing this option displays a menu which contains settings options pertaining to the function of the serial ports.

Modem Settings
Choosing this option displays a menu where all of the modem settings and modem-specific security options can be configured.

Security Settings
Choosing this option displays a menu which contains all user profiles, RADIUS configurations and general security settings.

Alarm/Event Definitions
This will display a menu tree which contains all of the event settings options.

Action Definitions
This option displays a menu to configure all of the actions possible when events are detected.

General Settings
The General Settings option displays a menu where you can set the site name, answer string, confirmation prompt, date/time, and other general settings. This menu also contains settings for job schedules and generator management.

Event Log Settings
This option brings up menu for configuring and displaying the Events Log.

Audit Log Settings
This option brings up menu for configuring and displaying the Audit Log.

Scripting Settings
The Scripting Settings option displays the menu for the management of scripts.

Network Settings

The Network Settings menu contains all of the options pertaining to network communication. The IP Routing & Restrictions Feature Guide on the Asentria Information Portal will have additional information and configuration examples for various features covered under the Networking Settings menu

» Note: The SiteBoss does not heed changes to network configurations while you are connected to a command processor via Telnet. Changes, including population of the candidate default router set, are pended until all network-based command processor sessions have ended. Open FTP connections will fail if these settings are changed during an open connection. A Web Interface connection will fail if the ETH1 IP address is changed as soon the submit button is pressed.

```
SiteBoss 550 - Network Settings
A) Ethernet Settings
B) IPv4 Default Router                  [192.168.90.1]
C) IPv6 Default Router                  [DYNAMIC]
D) Name Resolution Settings
E) Network Command Processor Duplex     [FULL]
F) Inactivity Timeout                   [0]
G) Server Settings
H) EventSensor Reporting Settings
I) SNMP Settings
J) FTP Push Settings
K) PPP Settings
L) Email Settings
M) Real-Time Socket Settings
N) SNMP Trap Capture Settings
O) IP Address Restrictions
P) Routing Settings
Q) VPN Settings
R) CPE Settings
S) DNP3 Settings                        [OFF]
T) Ethernet Expansion Settings
U) Ethernet Bridge Settings
V) IP Blacklist Settings                [ON]
   Note: Changes to IP Address, Subnet Mask, or Router
         Address will not take effect until any open
         network command processor sessions are ended.
```

Ethernet Settings

This option displays the menu where you can configure the two Ethernet interfaces, and if a SFP card is installed, Ethernet 3, as well as any of the VLAN interfaces associated with those Ethernet Ports.

» Note: If an Ethernet Expansion card is installed the Ethernet ports are configured at option U) Ethernet Expansion Settings.

IPv4 Default Router

The IPv4 Default Router option toggles through any configured router address(es) and DYNAMIC. The default (Gateway) router can be defined by setting the Router Address for any Ethernet interface, see the IPv4 section of the Ethernet Settings chapter for instructions. Any configured router for an interface that is up will show up in the drop down list that can be selected for the default route.

DYNAMIC in the default router options simply means that the default router is set only according to the default routing rule of any dynamic network interfaces that may be up, such as the Dialup POTS modem or the Wireless modem. The rule for Dialup POTS modem PPP is that whenever that interface is up, it is always the default route and overrides any other default route. The rule for Wireless modem is that it is the default route when the Wireless default route is enabled. In other words, DYNAMIC default router means the default router will be whatever POTS/Wireless modem PPP decides when it is running. Any other value for the default router means that the default router will be that value (e.g., an Ethernet router).

IPv6 Default Router
If any Ethernet interface is set to AUTO, the only option will be DYNAMIC. This is because in AUTO mode, default routes are determined by router advertisements and set by the operating system. If AUTO is not set, and there is more than one static router in the list, the user should select the preferred default router. If DYNAMIC is set, the OS will pick a default router from the list.

Name Resolution Settings
This option brings up a submenu that can be used to set up to two DNS Servers which are the IP addresses of Domain Name Servers. DSN servers allow for the use of host names rather than IP addresses in functions where name resolution may be needed, such as; Email server, action IP settings, network time servers, scripting TCP connections, etc. The DNS Mode can also be toggled between MANUAL, ETH1-DHCP, ETH2-DHCP, ETH3-DHCP (SFP Card, if installed), and DSL.

Network Command Processor Duplex
This option controls the echo settings for the command interface. Full duplex causes the unit to echo all characters sent to the remote device to display characters as typing occurs. Half duplex turns off character echo. The default setting is FULL.

Inactivity Timeout
The Inactivity Timeout sets the number of minutes (0 - 255) before a network connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. The default setting is 0.

Server Settings
This option opens a submenu of servers (FTP, SSH, Telnet, and Web) on the unit which allows enabling/disabling the server completely or setting which network interface(s) the service will "listen" on.

EventSensor Reporting Settings
EventSensor Reporting is a feature that allows an EventSensor connected to one Asentria product to transmit data to another Asentria product via a TCP connection. This feature does not need to be enabled in order to allow for normal alarm notice delivery.

SNMP Settings
The SNMP Settings option displays a menu where you can enable the SNMP agent, configure community names, and other SNMP trap settings.

FTP Push Settings
This menu option displays the FTP Settings menu, where you can configure automatic FTP pushes of buffered data.

PPP Settings
This option displays the PPP Settings menu for the internal dialup POTS modem. There are submenus where you can configure settings for PPP Dialout, PPP Hosting, and Route Testing.

Email Settings
This option displays the Email settings menu, where you can configure the SMTP server address, Email domain name, and authentication parameters.

Real-Time Socket Settings
This menu option displays the Real-Time Socket Settings menus where you can configure real-time socket settings for each file of buffered data. Real-Time Sockets are used to collect data on TCP port 2201 from a serial port in real-time, while buffering data if the network connection goes down.

SNMP Trap Capture Settings
This option displays the SNMP Trap Capture Settings menu where you can toggle this feature ON or OFF, and select which file to store the traps in and set up SNMP Trap Forwarding.

IP Address Restrictions
The IP Address Restrictions option displays a menu where you can limit Ethernet and PPP communications to or from specific IP addresses.

Routing Settings
The Routing Settings option displays a menu where you can configure settings for static network routes, port forwarding and other network routing parameters.

VPN Settings
This selection displays the VPN Settings menu where you can configure settings for up to two VPNs.

CPE Settings
This menu displays the Customer Premises Equipment (CPE) Settings menu where up to 64 different networked devices can be configured for keep-alive monitoring by the SiteBoss. This function is called Ping Alarms on the Web Interface.

DNP3 Settings
DNP3 is a remote telemetry automation protocol. This option brings up a submenu to configure the mode and other communication protocols as well as the outstation settings.

Ethernet Expansion Settings
This menu is used to configure one or two optional four port Ethernet Expansion Card(s) (4E cards).

Ethernet Bridge Settings
This brings up a menu to configure a network bridge between the onboard Ethernet interfaces, ETH1, ETH2, and if installed, ETH3 to bridge with each other.

IP Blacklist Settings
This option will open a submenu to configure the Automatic Blacklist feature which helps mitigate the risk of unauthorized access to the unit.

Ethernet Settings

This menu is used to configure the two Ethernet interfaces, and if a SFP card is installed, Ethernet 3, as well as any of the VLAN interfaces associated with these Ethernet Ports.

»**Note**: If an Ethernet Expansion card is installed the Ethernet ports are configured at option U) Ethernet Expansion Settings.

»**Note**: The SiteBoss does not heed changes to network configurations while you are connected to a command processor via Telnet. Changes, including population of the candidate default router set, are pended until all network-based command processor sessions have ended. Open FTP and RTS connections will fail if these settings are changed during an open connection. A Web Interface connection will fail if the ETH1 IP address is changed as soon the submit button is pressed.

»**Security Note**: If the SiteBoss is going to be exposed to the Internet, make sure to use the other security features available within the unit to prevent unauthorized access to your network, including strong passwords. See the Securing a SiteBoss Feature Guide for additional information.

```
SiteBoss 550 - Ethernet Settings
A) Ethernet 1
B) Ethernet 2

Enter your Selection: A


SiteBoss 550 - Ethernet 1 Settings
A) IPv4 Mode                          [STATIC]
B) IP Address                         [0.0.0.0]
C) Subnet Mask                        [255.255.255.0]
D) Router Address                     [0.0.0.0]
E) NAT                                [OFF]
F) VLAN Settings
G) IPv6 Settings                      [OFF]
H) DHCP Server Settings
```

IPv4 Mode

The Mode option toggles between STATIC, DHCP and VLAN. The default setting is STATIC.

IP Address

Use this option to set the network address assigned to this Ethernet interface. The default setting is 0.0.0.0

Subnet Mask

This field sets the network subnet mask provided by the network administrator. The default setting is 255.255.255.0

Router Address

This option sets the router address provided by the network administrator. The default setting is 0.0.0.0

NAT

This is an ON/OFF toggle to enable network address translation on the forwarded frames.

Without NAT, a server would receive a forwarded frame that is IP-addressed according to the network on the Ethernet interface. The default setting is ON.

VLAN Settings
Displays a menu where any of six individual Virtual Local Area Network (VLAN) connections can be configured.

IPv6 Settings
This option will open a submenu to enable and configure IPv6 functionality.

DHCP Server Settings
Settings to configure the units DHCP Server.

VLAN Settings

What follows is a top-level overview of the SiteBoss VLAN settings. Refer to the [IP Routing and Restrictions Feature Guide] for a detailed explanation of VLANs.

```
SiteBoss 550 - VLAN Settings
A) VLAN 1
. . .
F) VLAN 6

Enter your Selection: A


SiteBoss 550 - VLAN 1 Settings
A) ID                                [0]
B) Priority                          [0]
C) IP Address                        [0.0.0.0]
D) Subnet Mask                       [255.255.255.0]
E) Router Address                    [0.0.0.0]
```

ID
Input the identifier for the VLAN, 0 to 4094. The default is 0.

Priority
Set the priority assigned to egress frames, 0 to 7. The default is 0.

IP Address, Subnet Mask and Router Address
Configure like any other interface. See the Ethernet Settings above for more information.

IPv6 Settings

IPv6 operates independently from IPv4 configuration. For example, the user could have one interface in IPv4 VLAN mode and another interface operating in IPv6 AUTO mode. But the user could not have the same Ethernet interface operating in both IPv4 VLAN mode and IPv6 AUTO or STATIC mode.

```
SiteBoss 350 - Ethernet 1 IPv6 Settings
```

```
A) Mode                                [OFF]
B) Static Address                      []
C) Static Router Address               []
```

Mode
The Ethernet interface has 3 IPv6 modes: OFF, STATIC, and AUTO.

OFF sets the interface to IPv4 mode and disables IPv6 functionality.

STATIC means the interface has IPv6 support and that you must configure a Unicast Global address for it. It also has a link local address. It also has the static IPv6 address, if that is configured. If no static address is configured then it has only the link local address. If a static router is also configured then that router is used to configure the IPv6 default route.

In AUTO mode, the IPv6 default route is automatically configured.

The default is OFF.

Static Address
If you configure the Mode to Static set the static IPv6 address to use for this interface.

Static Router Address
If you configure the Mode to Static use this option to set the IPv6 default router.

DHCP Server Settings

These settings are used to configure the units DHCP server.

```
SiteBoss 550 - DHCP Server
A) DHCP Starting IP Address      [0.0.0.0]
B) DHCP Maximum Clients          [12]
C) DHCP Lease Time (minutes)     [240]
```

DHCP Starting IP Address
Sets the starting IP address for serving DHCP addresses. If this is default (0.0.0.0) then the unit will not run DHCP to serve addresses. The starting IP address MUST be on the same subnet as the interface IP

DHCP Maximum Clients
This field sets the maximum DHCP IP addresses for unknown clients. The default is 50. The IP address range for unknown clients will be the DHCP Starting IP Address plus the max clients figure.

DHCP Lease Time (minutes)
Lease time for DHCP clients in minutes (default 60).

Server Settings

Selecting this option displays a list of servers, FTP, SSH, Telnet, and Web. All of these services, when enabled, respond to requests on any active network interface. This is the default behavior. However, this menu system allows the user to enable or disable which network interface(s) the service will "listen" on.

If a user makes changes to the network interfaces via a SSH, FTP, or Telnet session, the changes will not take effect until the session has ended. If the changes are made via a Web session, any Web interface changes will not take effect until the Web session has been closed.

```
SiteBoss 550 - Server Settings
A) FTP
B) SSH
C) Telnet
D) Web

Enter your Selection: A


SiteBoss 550 - FTP
A) FTP Server            [ON]
B) Allowed Interfaces
```

FTP Server

This is an ON/OFF toggle setting to completely disable the server selected. This will be the first option for all of the server options.

Allowed Interfaces

This option displays a submenu to toggle ON/OFF which interfaces the unit will listen on.

```
SiteBoss 550 - FTP
A) FTP Server            [ON]
B) Allowed Interfaces

Enter your Selection: B


SiteBoss 550 - Allowed Interfaces
A) ETH1                  [ON]
B) ETH2                  [ON]
C) ETH3                  [ON]
D) ETH-Expansion         [ON]
E) Wireless              [ON]
F) ETH-BRIDGE            [ON]
```

Web Server

This section is where you can toggle the web interface ON or OFF, set the session timeout and set the TCP port numbers for the web connection.

```
SiteBoss 550 Web Interface Settings
A) Web Server            [ON]
B) Web Session Timeout   [30]
C) HTTP Port             [80]
D) HTTPS Port            [443]
E) TLS version           [TLSv1.2]
F) Allowed Interfaces
```

Web Server
This is an ON/OFF toggle to enable the S550's internal web server. The default setting is ON.

Web Session Timeout
This field sets the number of minutes (0 to 65535 minutes) a web connection may remain idle before expiring. A setting of 0 means the connection will never automatically expire. The default setting is 30.

HTTP Connection Port
This option sets the TCP port through which an HTTP connection is made. Set to 0 to prevent access. The default setting is 80.

HTTPS Connection Port
This option is the TCP port through which an HTTPS connection is made. Set to 0 to prevent access. The default setting is 443.

TLS version
This option allows the user to select between TLSv1.1 or TLSv1.2, with TLSv1.2 the default.

Allowed Interfaces
This option displays a submenu to toggle ON/OFF which interfaces the unit will listen on.

```
SiteBoss 550 - Allowed Interfaces
A) ETH1                  [ON]
B) ETH2                  [ON]
C) ETH3                  [ON]
D) ETH-Expansion         [ON]
E) Wireless              [ON]
F) ETH-BRIDGE            [ON]
```

EventSensor Reporting Settings

EventSensor Reporting is a feature that allows an EventSensor connected to one Asentria product to transmit data to another Asentria product via a TCP connection. This feature does not need to be enabled in order to allow for normal alarm notice delivery.

This functionality is currently only functional from the Command Line Interface

For a further explanation of EventSensor Reporting and how to configure both the Host and Client units, refer to the EventSensor Reporting - Feature Guide on the Asentria Information

Portal or contact Asentria Technical Support.

The *client* unit is the SiteBoss with the sensor physically connected to it and the host unit is the SiteBoss to whom the client unit will report when there is a change in the status of its sensor.

In addition to configuring the settings defined below, each sensor on the Client unit will need to have EventSensor Reporting Enabled in the Alarm/Event Definitions / EventSensor Device Settings / Individual EventSensor Slot configurations settings

```
SiteBoss 550 EventSensor Reporting Settings
A) EventSensor Report To IP                    []
B) EventSensor Report To Port                  [4000]
C) Enable EventSensor Reporting Host           [OFF]
D) EventSensor Reporting Host Port             [4000]
```

EventSensor Report To IP
This field would be used if this SiteBoss is the client. Set the IP address of the host SiteBoss that a sensor connected to this SiteBoss would report to.

EventSensor Report To Port
This field would be used if this SiteBoss is the client. Set the TCP port this SiteBoss would use to report to a host unit. The Default is 4000.

Enable EventSensor Reporting Host
This is an ON/OFF toggle to enable this SiteBoss to be a host for EventSensor reporting from another Asentria device. The Default is OFF.

EventSensor Reporting Host Port
This is used to set the TCP Port that this SiteBoss would use for receiving sensor reports from another Asentria device. The Default is 4000.

SNMP Settings

The SNMP Settings option displays a menu where you can enable the SNMP agent, configure community names, and other SNMP trap settings. Trap and Proxy settings are also located in this menu tree. For more detailed configuration and use instructions see the SNMP Operations Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support.

Testing SNMP Traps
Using the command interface enter the command DOTRAP from the command prompt. Verify that the trap manager receives the test trap.

```
SiteBoss 550 - SNMP Settings
A) SNMP Agent Enable                    [ALL VERSIONS]
B) Read Community                       [public]
C) Write Community                      [public]
D) Trap Community                       [public]
E) Trap Settings
F) Security Method                      [MD5-DES]
```

```
G) Security Name                    []
H) Security Password                [********]
I) Proxy Settings
J) SNMP Poll                        [OFF]
```

SNMP Agent Enable
This option toggles between ALL VERSIONS, V3 ONLY and OFF and controls whether the unit responds to SNMP 'gets' and 'sets' in the selected version. Note that for V3 operation the user profile passwords are used for authentication (via MD5) and encryption (via DES). Passwords for user profiles intended for SNMPv3 use must be at least 8 characters. The default setting is ALL VERSIONS. This setting does NOT stop SNMP traps from being sent when it is set to OFF.

»Note: SNMP Agent Enable does NOT stop SNMP traps from being sent when it is set to OFF.

Read / Write / Trap Community
These fields set the SNMP trap community names. The default setting for all is ?public? (maximum length for each is 23 characters).

Trap Settings
The Trap Settings option displays a menu that allows you to configure whether to send authentication failure traps and notification settings.

Security Method
This option toggles between MD5-DES and SHA-AES to controls whether MD5 and DES, or SHA-1 and AES, are used for authentication and privacy for SNMPv3 operations. The default setting is MD5-DES.

Security Name
This option is for inputting the authentication name for SNMPv3 operations (maximum Length 31 characters).

Security Password
This option is for inputting the authentication password for SNMPv3 operations. This field is required to be set to a minimum of 8 characters and 31 characters maximum.

Proxy Settings
Proxy Settings displays a menu which is used to configure SNMP Proxying. This feature allows a SiteBoss to receive SNMP requests from a NMS that are intended for another device, forward the SNMP request to the appropriate device and pass the response from the queried device back to the NMS as if it originated from the queried device.

SNMP Poll
Displays a menu which is used to enable and configure the SNMP Polling feature. The SNMP Polling feature allows a SiteBoss to query other devices using SNMP.

Trap Settings

This menu is used to configure whether to send authentication failure traps and notification settings.

Testing SNMP Traps

At the command prompt enter DOTRAP. Verify that the trap manager receives the test trap.

»Note: SNMP traps are not a guaranteed means of delivering notifications. Traps are a one-way IP network datagram and the device receiving traps does not acknowledge them. Therefore, if the trap does not reach its intended destination for whatever reason, the sending device has no way of recognizing this and resending the trap. To receive acknowledgments use SNMP Informs, available in SNMPv2 and SNMPv3.

```
SiteBoss 550 - Trap Settings
A) Authentication Failure Traps                    [OFF]
B) Notification Attempts (0=infinite)              [5]
C) Notification Timeout (seconds)                  [60]
D) Notification Cycles (0=infinite)                [10]
E) Notification Snooze Period (minutes)            [60]
F) Notification Security Name                      []
G) Notification Security Password                  [********]
```

Authentication Failure Traps

This is an ON/OFF toggle to enable the sending of authentication failure traps. These are trap notifications of invalid community name usage in SNMP operations. The default setting is OFF.

Notification Attempts

This option sets the number of attempts (1 to 65535) for the unit to attempt a notification. The number will include the initial trap attempt plus the retries. If this field is set to 0 then the unit will continue to attempt to send the trap endlessly. The default setting is 5.

Notification Timeout

This field sets the number of seconds (3 to 60) between two attempts to send an SNMP notification in the same cycle. The default setting is 60.

Notification Cycles

The Notification Cycles field sets the maximum number of cycles (0 to 60) to try per notification action, where one notification action corresponds to one "inform" keyword in an action list for an event. A cycle is a set of notification attempts delimited by a successful action delivery or snooze period. The default setting is 10.

Notification Snooze Period

This option sets the time in minutes (1 to 1440) between two SNMP notification cycles for any one notification action. That is, if you have two events generate informs, each inform will have its own timeouts for retries and cycles, and its own snooze period. The default setting is 60.

Notification Security Name/Password

When sending SNMPv3 traps set the name and password used for authentication (maximum length for each is 31 characters).

Proxy Settings

This feature allows a SiteBoss to receive SNMP requests from a NMS that are intended for another device, forward the SNMP request to the appropriate device and pass the response

from the queried device back to the NMS as if it originated from the queried device. This feature is useful when the SiteBoss is the only accessible device on a network.

```
SiteBoss 550 - Proxy Settings
A) Proxy Entry 1                    [ ]
. . .
H) Proxy Entry 8                    [ ]
```

Proxy Entry n
Select the proxy entry you wish to configure using the letter to the left of the option.

```
SiteBoss 550 - Proxy Entry 1
A) Name                             []
B) Ingress OID Branch               []
C) Egress OID Branch                []
D) Agent IP Address                 []
E) Agent Port                       [161]
F) Community                        []
```

Name
This is a text field to name the Proxy. The maximum number of characters is 30.

Ingress OID Branch
Enter the object identifier of the variable binding on the device to be proxied. Since the OID branch is the differentiator, it must be unique among the set of proxy entries. A blank OID branch in the proxy entry disables the entry.

Egress OID Branch
Use this field to set the Egress OID. This should cover the device to proxy. A blank egress OID branch in the proxy entry disables the proxy entry. A non-blank egress OID branch enables the proxy entry.

Agent IP Address
Enter the IP Address of the SNMP Agent to be proxied.

Agent Port
Identifies the Port that the agent expects SNMP requests to be received on. This is set to Port 161 by default.

Community
Input the SNMP Community String that the proxied device expects to receive with SNMP requests.

SNMP Poll

The SNMP Polling feature allows a SiteBoss to query other devices using SNMP. For more information refer to the Operations Feature Guide] or contact Asentria Tech Support.

```
SiteBoss 550 - SNMP Poll Settings
A) Mode                                [OFF]
B) Store Data To                       [FILE1]
C) Store All Period                    [0]
D) Request Settings
```

Mode
The Mode toggles between OFF, POLL ONLY (just make the results available to view) and POLL BUFFER store the results in the file designated in the next menu option.

Store Data To
This option toggles through the available file options on the SiteBoss. The default is to FILE1.

Store All Period
If this field is set to a non-zero value then this time period (in seconds) will poll all configured SNMP Poll requests and buffer all values regardless of threshold

Request Settings
This option opens a series of sub-menus where you can configure up to 64 individual SNMP Polling requests.

```
SiteBoss 550 - SNMP Poll Request Settings
A) Requests 1-16
B) Requests 17-32
C) Requests 33-48
D) Requests 49-64

Enter your Selection: A
```

```
SiteBoss 550 - SNMP Poll Request Settings
A) Request 1                           []
. . .
P) Request 16                          []

Enter your Selection: A
```

```
SiteBoss 550 - SNMP Poll Request 1 Settings
A) Description                         []
B) Agent IP Address                    []
C) Read Community                      [public]
D) OID                                 []
E) Period (seconds)                    [10]
F) Buffer ID                           []
G) Buffer Threshold                    []
```

Description
This field is for entering a user-identifiable description to the SNMP Polling Request. This serves only to more easily identify individual requests on the SiteBoss' menus. The maximum length is 64 characters.

Agent IP Address
Input the Agent IP address or hostname for this request (maximum Length 64 characters).

Read Community
Enter the SNMP read community for this request. The default is public (maximum length for each is 32 characters).

OID
Enter the SNMP object identifier to be polled (maximum Length 64 characters).

Period (seconds)
This option configures the amount of time between SNMP requests to the agent, measured in seconds. Values are between 1 and 255 (Defaults to 10)

Buffer ID
This is a textual field that is part of the record containing the telemetry result.

Buffer Threshold
This selection controls when new data is stored upon a successful telemetry request. The data stored depends on how the Buffer Threshold field is set:

- If the field is left blank then the telemetry is always stored.
- If set to "any difference" then the telemetry is stored only if it is different from the last value stored.
- If set to an integer (for example: 3) then it is treated as a hysteresis value (the span plus or minus the last stored value). This means that if the new telemetry does not exceed the threshold (either + or -) beyond the last stored value, then the new telemetry is not stored.
- If set to a floating point number (for example: 3.1) then it is treated as a hysteresis value for SNMP OCTET STRING types where the value looks like a floating point number. This means that if the last stored value is NOT a floating point number then the unit will ignore the threshold and store the new telemetry.

FTP Push Settings
This menu is used to configure automatic FTP pushes of buffered data. This is not applicable to the S550A units.

Testing FTP Push
Once FTP Push has been configured, entering the **PUSHTEST** command from the command prompt will test the connectivity to the FTP server and write a "log in" and "log out" entry to the Status File in the directory you configured. No data is pushed with this command. Connection data displayed on the terminal screen is useful if the connection fails.

An immediate push of data can be done using the **PUSHNOW** command from the command prompt.

```
SiteBoss 550 - FTP Settings
A) FTP Push Enable                  [OFF]
B) FTP Server Address               []
C) Passive Mode                     [ON]
D) SFTP Port                        [22]
E) Username                         [Default FTP Username]
F) Password                         [********]
```

```
G) Account                          []
H) Directory                        []
I) Minutes Between Push Attempts    [1440]
J) Permissions                      []
K) Select Files to Push
L) Remote File Names
```

FTP Push Enable
FTP Push Enable toggles between OFF, REGULAR, and SECURE. The default setting is OFF.

FTP Server Address
Set this field as the IP address or host name of the FTP server to push to (maximum length 64 characters).

Passive Mode
This is an on off toggle to set the FTP Mode as Active or Passive. The default is ON (Passive).

SFTP Port
Use this option to set the SFTP Port. The default is 22.

Username / Password
These two options set the login credentials that are able to access the remote FTP server (maximum length Username is 126 characters and maximum length Password is 31 characters)

Account
This field is a third login option used only on some FTP servers. Consult your network administrator to see if this is necessary (maximum length 126 characters).

Directory
The Directory is the path used to transfer the file(s). The file(s) is transferred to the root login directory if this option is left blank (maximum length 253 characters).

Minutes Between Push Attempts
This field sets the number of minutes (1 to 9999) between FTP push attempts. Default setting is 1440 minutes.

Permissions
This field is used to set the permissions on the pushed file. Permissions is usable for both FTP and SFTP to the extent allowed by the server. If blank then no permissions change is attempted. The default is blank.

Select Files to Push
This option displays the FTP File Selection menu where you can select which files are pushed by toggling ON or OFF. The default setting for all is ON, except for Audit Log, which is OFF.

```
SiteBoss 550 - FTP File Selection
A) Data File 1                      [OFF]
B) Data File 2                      [OFF]
C) Events File                      [ON]
D) Audit Log                        [ON]
```

```
E) Status File                          [ON]
```

Remote File Names

This menu option displays the FTP File Names menu where you can give each file a name, other than the default name, and/or prepend a date, time, and unique sequence # to the file name.

```
SiteBoss 550 - FTP File Names
A) Include Date in Filename             [OFF]
B) Include Time in Filename             [OFF]
C) Include Sequence #s in Filename      [OFF]
D) Data File 1                          [FILE1]
E) Data File 2                          [FILE2]
F) Events File                          [EVENTS]
```

Include Date / Time in Filename

These are ON/OFF toggles to enable the addition of the file transfer date and/or time to the beginning of the name of each transferred file of data. The default settings are OFF.

Include Sequence #s in Filename

This is an ON/OFF toggle to enable the addition of a unique sequence number to the beginning of the name of each transferred file of data. This ensures that no two transfers will have the same file name. The default setting is OFF.

Data File n / Events File

These fields are text-entry fields where the name each data file will have on the remote server (not including any date, time, or sequence numbers) can be configured.

PPP Settings

This option displays the PPP Settings menu for the internal dialup POTS modem. There are submenus where you can configure settings for PPP Dialout, PPP Hosting, and Route Testing.

The settings will not change any functionality unless a POTS modem is installed in the unit. These settings are not applicable to an S550A.

```
SiteBoss 550 - PPP Settings
A) PPP Dialout Settings
B) PPP Hosting Settings
C) Route Test Settings
```

PPP Dialout Settings

This selection displays settings pertaining to making outbound PPP network connections.

PPP Hosting Settings

This selection displays settings for hosting a PPP connection.

Route Test Settings

This selection displays settings for network monitoring/PPP backup connection settings.

PPP Dialout Settings

This menu is used to configure settings pertaining to making outbound PPP network connections for a POTS modem.

```
SiteBoss 550 - PPP Dialout Settings
A) PPP Dialout Enabled                [OFF]
B) Phone Number 1                     []
C) Phone Number 2                     []
D) Phone Number 3                     []
E) Phone Number 4                     []
F) User Name                          []
G) Password                           [********]
H) Idle Connection Disconnect (sec)   [60]
I) Maximum Retries                    [3]
J) Carrier Detect Timeout (sec)       [60]
K) Login Sequence Timeout (sec)       [30]
L) Dialout Modem Init String          []
M) IP Address to Suggest              [0.0.0.0]
N) Firewall                           [OFF]
```

PPP Dialout Enabled

This is an ON/OFF toggle to enable PPP dialout. The default setting is OFF.

Phone Number n

These fields set the phone number(s) of the PPP host the SiteBoss is to dial into (maximum length 48 characters each). If the connection fails the SiteBoss will try the next phone numbers entered.

User Name / Password

Use these fields to set the login credentials that are used to log into the PPP host (maximum length for each is 64 characters).

Idle Connection Disconnect (sec)

This field sets the number of seconds to wait before disconnecting an idle connection. A setting of 0 means the unit does not disconnect due to an idle connection. The default setting is 60 seconds.

Maximum Retries

This field defines the maximum number of times to retry a failed connection for all phone numbers present. The default setting is 3.

Carrier Detect / Login Sequence Timeout (sec)

These fields set standard login timeouts, from 0 to 65535 seconds. The default setting is 60 seconds for Carrier Detect, and 30 seconds for Login Sequence.

Dialout Modem Init String

This field sets the modem initialization string (maximum length 48 characters).

IP Address to Suggest
This field sets an IP to try to acquire, if defined. The default setting is 0.0.0.0.

Setting Key: **net.pppdial.downafter.ftppush**
Values are ON or OFF (default OFF). ON means that if FTP Push raised PPP, then it kills PPP when finished.

PPP Hosting Settings

This menu is for configuring settings for hosting a PPP connection on the POTS Dial-Up Modem.

```
SiteBoss 550 - PPP Hosting Settings
A) PPP Hosting Enabled                [OFF]
B) Idle Connection Disconnect (sec)   [60]
C) Local (Device) IP Address          [192.168.105.1]
D) Remote (Caller) IP Address         [192.168.105.2]
E) Firewall                           [OFF]
```

PPP Hosting Enabled
This is an ON/OFF toggle to enable inbound PPP connection hosting. The default setting is OFF.

Idle Connection Disconnect (sec)
This field sets the number of seconds (0 to 65535) to wait before disconnecting an idle connection. A setting of 0 means the unit does not disconnect due to an idle connection. The default setting is 60 seconds.

Local (Device) IP Address
This option sets the IP address of the SiteBoss for the PPP session. The default is 192.168.105.1

Remote (Caller) IP Address
This field sets the IP address of the calling device for the PPP session. The default is 192.168.105.2.

Firewall
This is an ON/OFF toggle to enable or disable the PPP Modem firewall. The default is ON.

» Note: The firewall for PPP Hosting and PPP Dialout are the same setting. Changing the setting in one menu will update the PPP firewall for all POTS modem functions.

Route Test Settings

This menu allows you to configure up to three IP addresses to ping on a regular basis. If any of the configured addresses are up then the unit will assume Ethernet is a reliable way of sending SNMP traps. If all configured addresses are down then the unit will fall back to PPP dialout in order to maintain reliable network connectivity for sending SNMP traps.

```
SiteBoss 550 - Route Test Settings
A) Route Test Enable                    [OFF]
B) Minutes Between Tests                [10]
C) IP Address 1                         []
D) IP Address 2                         []
E) IP Address 3                         []
```

Route Test Enable
This is an ON/OFF toggle to enable route testing. Default setting is OFF.

Minutes Between Tests
This field sets the number of minutes (0 to 65535) to wait between each round of testing. Default setting is 10 minutes.

IP Address n
These fields set the hostnames or IP addresses to ping for the test.

Email Settings

This option displays the Email settings menu, where you can configure the SMTP server address, Email domain name, and authentication parameters.

```
SiteBoss 340 - Email Settings
A) SMTP Server Hostname/IP Address      [ ]
B) SMTP Server Port                     [0]
C) Email Domain Name                    [ASENTRIA.COM]
D) Encryption                           [OFF]
E) Authentication (LOGIN)               [OFF]
```

SMTP Server Hostname/IP Address
Enter the hostname or IP address of the outbound mail server (Maximum length 64 characters).

SMTP Server Port
This specifies the TCP port on which the SMTP server listens. It must be an integer between 1 and 65535. A value of 0 means the port is automatically selected by the system. Default value is 0.

Email Domain Name
This field is used to sets the Email domain name, e.g. @domain_name.com, which is used when the SiteBoss sends an Email. The default setting is "ASENTRIA.COM". The maximum length is 48 characters.

Encryption
This option toggles through the choices of OFF, STARTTLS, and TLS. Most servers support STARTTLS; use the TLS setting for servers that don't. The default value is OFF.

Authentication (LOGIN)

This option displays a menu to configure the credentials that may be required by your server for SMTP authentication. Some SMTP servers require an authentication to relay Emails. The default setting is OFF.

```
SiteBoss 340 - Email Authentication Settings
A) Authentication Enabled              [OFF]
B) Username                            []
C) Password                            [********]
```

Authentication Enabled
This is an ON/OFF toggle to enable Email authentication. The default setting is OFF.

Username / Password
Enter the login credentials as required. The maximum length for each is 48 characters.

Real-Time Socket Settings

This menu option displays the Real-Time Socket Settings menus where you can configure real-time socket settings for each file of buffered data. Real-Time Sockets are used to collect data on TCP port 2201 from a serial port in real-time, while buffering data if the network connection goes down.

Each file can be configured independently. Refer to the Telnet Feature Guide on the Asentria Product Information Portal for a detailed explanation of Real-Time Sockets or contact Asentria Tech Support.

These settings are not available on an S550A.

```
SiteBoss 550 - Real-Time Socket Setup
A) FILE1
B) FILE2
C) EVENTS

Enter your Selection: A

SiteBoss 550 - FILE1 Real-Time Data Socket Setup
A) Real-Time Socket Mode               [OFF]
B) Show Answer String on Connection    [ON]
C) Require Xon to Start Data Flow      [OFF]
D) Idle Connection Close Timer         [0]
E) Close Socket When File Empty        [OFF]
F) Real-Time Socket Push Hostname/IP   []
G) Real-Time Socket Push Port Number   [3000]
H) Real-Time Socket Push Retry Timer   [5]
```

Real-Time Socket Mode
The Mode can be toggled to LISTEN, PUSH, and OFF. When set to LISTEN the option functions like traditional real-time sockets on TCP port 2201. When set to PUSH the unit tries to make a TCP connection on the TCP port specified in G) Real-Time Socket Push Port Number. As long as a connection exists, the unit sends all data in the specified file on the connection as data become available. The default setting is OFF.

Show Answer String on Connection
This is an ON/OFF toggle to enable the prompt indicating successful connection to the Real-Time Socket (RTS) port. The default setting is ON.

Require Xon to Start Data Flow
This is an ON/OFF toggle to enable the Xon/Xoff data flow control requirement. The default setting is OFF.

Idle Connection Close Timer
This field sets the number of seconds (0 ? 255) to wait before disconnecting an idle connection. A setting of 0 means the connection will never automatically close. The default setting is 0.

Close Socket When File Empty
This is an ON/OFF toggle to set whether or not the SiteBoss will automatically terminate the RTS connection when the file for this port has been emptied. The default setting is OFF.

Real-Time Socket Push Hostname/IP
Use this field to set the hostname or IP address of the server where the unit will push the data if the RTS Mode is set to Push (maximum length is 64 characters).

Real-Time Socket Push Port Number
This option sets the TCP-port number the RTS push should use. The default setting is port 3000.

Real-Time Socket Push Retry Timer
This option sets the number of minutes (1 to 255) to wait before retrying an RTS push that has previously failed. The default setting is 5 minutes.

SNMP Trap Capture Settings

The SiteBoss can receive, buffer and forward SNMPv1 traps and SNMPv2c inform-requests (informs). Each notification can be subjected to data event evaluation, stored in the Event Log, and delivered via normal Event Log delivery.

When SNMP Trap Capture is enabled, the SiteBoss listens on port 162 for notifications; those over 1024 bytes are ignored. The unit will respond to informs as soon as they arrive regardless of the content of the inform.

Refer to the SNMP Operations Feature Guide on the Asentria Product Information Portal for a detailed explanation of SNMP Trap Capture or contact Asentria Technical Support.

```
SiteBoss 550 - SNMP Trap Capture Settings
A) SNMP Trap Capture Enable             [OFF]
B) Store Collected Traps In             [FILE1]
C) Forwarding                           [OFF]
```

SNMP Trap Capture Enable
This is an ON/OFF toggle to enable the capturing of SNMPv1 traps and SNMPv2c inform-

requests (informs). The default setting is OFF.

Store Collected Traps In
This field toggles through all available data files in which the collected traps/informs are stored. The default setting is FILE1.

Forwarding
Selecting this option will bring up a menu to configure your SiteBoss to forward informs and traps to specific target SNMP Manager.

```
SiteBoss 550 - SNMP Trap Forwarding Settings
A) Forwarding Mode                      [OFF]
B) IP Replacement Mode                  [NONE]
C) Replacement IP                       [0.0.0.0]
D) Target 1                             []
E) Target 2                             []
F) Target 3                             []
```

Forwarding Mode
This option toggles between OFF and QUEUE. Off means do not forward. QUEUE will listen for a trap and then resend it to specified targets.

IP Replacement Mode
This toggles between NONE, IMPLICIT and EXPLICIT. When set to NONE, the IP address reflected in the forwarded trap is that of the original source device. The IMPLICIT setting will replace the SNMPv1 trap?s agent address field to the ETH1 interface address of the unit. EXPLICIT will replace the field with an explicit address defined in the Replacement IP field.

This functionality only works with SNMPv1 traps. Informs will be forwarded however the source IP will always transmit with the IP Address of the Ethernet Interface of the sending device.

Replacement IP
This field is used to set a replacement IP address if you wish to replace the SNMPv1 trap?s agent address field to a specific address in the original trap. The IP Replacement Mode must be set to EXPLICIT for this field to be used. The Default setting is 0.0.0.0

Target n
These fields are used to input the SNMP manager(s) that the trap is getting forwarded to.

IP Address Restrictions

The IP Address Restrictions section allows you to configure permissions and/or restrictions for communications to or from specific IP addresses.

IP Address Restrictions are a defense against unauthorized access via a network or PPP connection. An administrator can restrict access by configuring one or more IP addresses that will be the only ones allowed to access the unit. Restrictions can also be configured to deny access to larger groups of IP addresses using wildcards. IP Address Restrictions do not replace restrictions set by User Profiles, but they do provide an extra level of protection by causing the unit to ignore all network traffic except from the addresses allowed.

If no IP restrictions are defined in this menu, all incoming connections are allowed.

The Asentria unit evaluates the list of IP restrictions from top to bottom. When it finds an entry that specifically allows or disallows access, it uses that entry and stops looking. Enter IP restrictions before the allowed addresses or subnets. However, if you enter any restrictions you MUST enter an allowed address or group, or you will lock yourself out.

»CAUTION: If any access restrictions are configured, a group or IP address that IS allowed access must be specifically defined. If no authorized access IP address or subnet is specifically defined BEFORE hitting Submit the unit will ignore communications from ALL IP Addresses. Serial access to the command line interface would then be required to regain access to the SiteBoss. See the Access via a Serial Connection section for instructions on how to connect via IO2.

Refer to the IP Routing & Restrictions Feature Guide on the Asentria Product Information Portal for a detailed explanation of IP Address Restrictions. By default, no address restrictions are configured.

```
SiteBoss 340 - IP Address Restrictions
 No IP Restrictions Established
A)        Add Item to Table
```

This menu is used to manipulate the IP Restrictions table.

The IPv4 wildcards are 0 and 255. .0 is a wildcard that allows access to IP addresses in that group. .255 is a wildcard that denies access to IP addresses in that group.

The IPv6 wildcards are :: (double colon) and ffff. :: (double colon) allows IP addresses in that group. ffff restricts IP address in that group.

Entering a specific IP address sets that address to be allowed access. There is no way to disallow a specific IP address, only a subnet group.

Once there are entries into the table of restrictions/permissions two more control options are displayed in the menu which can be used to delete options from the table.

```
SiteBoss 340 - IP Address Restrictions
 1. 0.0.0.0
A) Add Item to Table
B) Delete an Item from Table
C) Delete All Items from Table
```

Refer to the IP Routing & Restrictions Feature Guide for a detailed explanation of IP Address Restrictions. By default, no address restrictions are configured.

Routing Settings

The following is a top-level overview of the SiteBoss routing settings. For more detailed configuration and use instructions for all of these please refer to the IP Routing and Restrictions Feature Guide on the Asentria Product Information Portal.

```
SiteBoss 550 - Routing Settings
A) Static Route Settings - IPv4
B) Static Route Settings - IPv6
C) IPV6 <--> IPV4 Proxy
D) Port Forwarding Settings
E) Ethernet to PPP/Wireless Settings
F) PPP to Ethernet Settings
G) Ethernet to WAN Settings
H) Interface Forwarding
I) Default Gateway Failover
```

Static Route Settings ? IPv4

This selection will display the IPv4 Static Route Settings menu where you can configure static network routes. Eight different IPv4 routes can be configured.

Static Route Settings ? IPv6

This selection will display the IPv6 Static Route Settings menu where you can configure static network routes. Eight different IPv6 routes can be configured.

IPV6 <--> IPV4 Proxy

This option open a menu to configure IPv6 to IPv4 Proxy options.

Port Forwarding Settings

The Port Forwarding Settings menu is for configuring the unit to accept UDP and TCP frames on an interface and route them, translating their IP addresses and UDP/TCP ports according to configuration to a different address on a different interface.

Ethernet to PPP/Wireless Settings

Ethernet to Wireless Settings displays a menu that enables the SiteBoss to forward IP frames originating on Ethernet that are not IP-addressed to the unit as well as forward IP frames received on a wireless interface that are associated with forwarded frames that originated on Ethernet. There is also an option to enable NAT on the forwarded frames.

PPP to Ethernet Settings

This option displays a menu to enable the SiteBoss to forward IP frames originating on PPP that are not IP-addressed to the unit, as well as forward IP frames received on any Ethernet or VLAN interface that are associated with forwarded frames that originated on PPP.

Ethernet to WAN Settings

This option is used to enable the ETH2 port to operate as a WAN port by routing and NAT?ing traffic arriving on ETH1 not destined for the unit out ETH2, much the same way a home Wi-Fi unit operates.

»Note: Just enabling ETH2 WAN Routing is not enough to route traffic out ETH2. You must also configure basic network settings for ETH2, as well as the default route or static routes. Configure the default router to be that of ETH2, or configure static routes for specific packet

destinations of packets arriving on ETH1 to be routable via ETH2.

Interface Fowarding

This option opens a submenu to set up the Interface Forwarding feature. This feature allows the user to control how packets are routed on a device with multiple network interfaces. Interface forwarding only applies to packets that are getting routed through the host device; not packets addressed to the host device

Default Gateway Failover

This option opens a submenu to configure the Default Gateway Failover feature which allows the user to specify the default gateway route and a failover route.

Static Route Settings IPv4

Static routes are network routes that specify in a more or less permanent way (static) that traffic to a certain destination (destination host or destination network) gets routed out a certain interface or via a certain gateway.

Static routes give you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different IPv4. You can specify a gateway or interface. If you specify a gateway only then the frame will be IP-addressed to the destination subnet and transmitted to the gateway, and the gateway needs to be either a local Ethernet subnet or the peer of a PPP connection (be it Wireless or Dialup Modem). If you specify an interface, regardless of specifying a gateway, then the frame will be transmitted out that interface.

»Note: Specifying that certain traffic goes out a PPP interface does not cause PPP to be raised when that traffic needs to leave the unit. If a PPP interface is down then any static routes that specify a PPP interface are effectively disabled.

»Note: Currently there is no support for Dialup Modem PPP and Wireless Modem PPP to be functional at the same time. The effect is that if you specify a static route with Wireless Modem PPP interface when the Dialup Modem PPP is up instead of the Wireless, then that traffic will go out the Dialup Modem PPP interface.

```
SiteBoss 550 - Static Route Settings
A) Route 1
...
H) Route 8

Enter your Selection: A

SiteBoss 550 - Static Route 1 Settings
A) Enable                           [OFF]
B) Destination Network              [0.0.0.0/0]
C) Gateway                          [0.0.0.0]
D) Interface                        [NONE]
```

Enable

This is an ON/OFF toggle to enable a static route. The default setting is OFF.

Destination Network

Define the destination network notation, i.e., w.x.y.z/s, where s is the significant bits. The default is 0.0.0.0/0. To configure a static ***host*** route specify a destination net with sigbits == 32. To configure a static ***network*** route specify a destination net with sigbits < 32.

Gateway
Enter the IP address of the gateway. The default setting is 0.0.0.0

Interface
This option toggles through the options, ETH1, ETH2, ETH3, the VLAN Options for each, ETHEXPAN, ETH-BRIDGE, PPPP (POTS Modem), WIRELESS, SPPP (Serial PPP), and NONE, from which to select any one of the interfaces available on this SiteBoss. The default setting is NONE.

»Note: ETH3 is a SPF Expansion Card (Small Form-factor Pluggable transceiver), if installed.

You can specify a gateway or interface. If you specify a gateway only, then the frame will be IP-addressed to the destination subnet and transmitted to the gateway, and the gateway needs to be either a local Ethernet subnet or the peer of a PPP connection (be it wireless or PSTN). If you specify an interface, regardless of specifying a gateway, then the frame will be transmitted out that interface

Static Route Settings IPv6

Static routes give you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different IPv6 routes in addition to any configured IPv4 routes.

Pv6 Static Routes is currently supported only on interfaces ETH1, ETH2, ETH3 and ETHEXPANF. For Ipv6 the gateway is optional, but interface is required.

```
SiteBoss 550 - Static Route Settings - IPv6
A) Route 1
...
H) Route 8

Enter your Selection: A


SiteBoss 550 - Static Route 1 Settings
A) Enable                              [OFF]
B) Destination Network                 []
C) Gateway                             []
D) Interface                           [NONE]
```

Enable
This is an ON/OFF toggle to enable or disable the specified static route. The default setting is OFF .

Destination Network
This field is used to designate the destination network in IPv6 network notation, e.g. 2001:1:2:3::2/64. The Default setting is blank.

Gateway

Enter the IP address of the gateway using a valid IPv6 address. The default setting is blank.

Interface
The interface option will toggle through the options from which to select any one of the interfaces available on this SiteBoss ? NONE, ETH1, ETH2, ETH3, ETHERNET EXPANSION. An interface value other than NONE must be selected in order for the route to be applied. The default setting is NONE.

IPV6 <--> IPV4 Proxy

The IPv6 to IPv4 Proxy feature facilitates forwarding IPv6 packets to an IPv4 or IPv6 address. The proxy listens on the specified port and when a packet comes in it is routed to the destination. If the connection is TCP, two bidirectional streams are established and packets are transferred between them. Up to 8 proxies can be configured.

If your proxy device uses to https for the WebUI, the destination port of said proxy must be configured to Port 443, and you must use an "https:// " prefix when entering your IPv6 address. Similarly, if you are accessing a proxy device via http, Port 80, you will need to specify an "http:// " prefix in your IPv6 initial address.

See the IPv6 to IPv4 Proxy Feature Guide on the Asentria Information Portal for additional information and an example configuration.

```
SiteBoss 550 - IPv6 <--> IPv4 Proxy Settings
A) Proxy 1
...
H) Proxy 8

Enter your Selection: A


SiteBoss 550Proxy
A) Mode                                [OFF]
B) Source Port                         [0]
C) Destination IP Version              [IPV4]
D) Destination Address                 []
E) Destination Port                    [0]
```

Mode
The Mode toggles through the available modes OFF, HTTP, HTTPS, SSH or TELNET. The default is OFF.

Source Port
The TCP port to listen for incoming packets. Note: this feature binds to the source port, so it MUST be an unused TCP port. The default is 0.

Destination IP Version
This option toggles between IPv4 and IPv6. The default is IPv4

Destination Address
This option is used to enter the destination IP. The default is blank.

Destination Port
This option sets the destination port. The Default is 0.

Port Forwarding Settings
The Port Forwarding Settings menu is for configuring the unit to accept UDP and TCP frames on an interface and route them, translating their IP addresses and UDP/TCP ports according to configuration to a different address on a different interface. Up to 32 individual routes can be configured.

See the IP Routing & Restrictions Feature Guide for more additional instructions and examples for the Port Forwarding feature.

```
SiteBoss 550 - Port Forwarding Settings
A) Port Forwarding Page 1 (1-16)
B) Port Forwarding Page 2 (17-32)

Enter your Selection: A


SiteBoss 550 - Port Forwarding Settings
A) Route 1
...
P) Route 16

Enter your Selection: A


SiteBoss 550 - Port Forwarding Settings for Route 1
A) Mode                              [OFF]
B) Source Interface                  [NONE]
C) Source Port                       [0]
D) Destination Interface             [NONE]
E) Destination Address               [0.0.0.0]
F) Destination Port                  [0]
```

Mode
Mode toggles between OFF, TCP and UDP to select the protocol to be utilized. The default setting is OFF.

Source Interface
This option toggles between NONE, ETH1, ETH2, ETH3, the ETH VLAN 1, 2, 3, 4, 5, 6, (E1V1- E1V6, E2V1-E2V6, E3V1-E3V6), ETHEXPAN, Dialup Modem PPP (PPPP), Wireless Modem PPP (WIRELESS), Serial PPP (SPPP), or VPN. The default setting is NONE.

Source Port
Set the port on which the source interface communicates with the unit. Valid values are 0 ? 65535. The default setting is 0.

Destination Interface
The Destination Interface toggles between NONE, ETH1, ETH2, ETH3, the ETH VLAN 1, 2, 3, 4, 5, 6, (E1V1- E1V6, E2V1-E2V6, E3V1-E3V6), ETHEXPAN, Dialup Modem PPP (PPPP), Wireless Modem PPP (WIRELESS), Serial PPP (SPPP), or VPN. The default setting is NONE.

Destination Address
Set the IP address of the destination interface. The default setting is 0.0.0.0.

Destination Port
Set the port on which the unit communicates with the destination interface. Valid values are 0 to 65535. The default setting is 0.

Port-Forward Name
This is a text field to name the Port Forward for ease in determining what is connected at that port. The maximum length is 23 characters.

Interface Forwarding

The Interface Forwarding feature allows the user to control how packets are routed on a device with multiple network interfaces. Interface forwarding only applies to packets that are getting routed through the host device; not packets addressed to the host device (the IP restriction feature controls packets addressed to the host).

There are nine settings that together describe one rule. The rule is applied to an IP packet when it is being routed through the device. If it matches a rule then the unit applies that rule; otherwise the packet falls through to the next rule, and finally the default policy (which is always to DROP the packet). Up to twelve rules can be specified with the evaluation starting at the first enabled rule and continuing in order.

»Note: Interface Forwarding is an advanced routing feature that can affect network security. It can provide access to different areas of the network, thus there is a risk. This section of the manual provides direction for configuring this feature and assumes the user has full knowledge and understanding of the security concerns.

```
SiteBoss 550 - Interface Forwarding
A)  Rule 1
...
L)  Rule 12

Enter your Selection: A


SiteBoss 550 - Interface Forwarding
A) Enable                              [OFF]
B) Protocol                            [ALL]
C) Interface In                        [ALL]
D) Interface Out                       [ALL]
E) IPv4 Source Address                 [0.0.0.0]
F) IPv4 Source Mask                    [255.255.255.0]
G) IPv4 Destination Address            [0.0.0.0]
H) IPv4 Destination Mask               [255.255.255.0]
I) IPv6 Source Address                 []
J) IPv6 Destination Address            []
K) Action                              [NONE]
```

Enable
This option toggles through IPV4, IPV6 or both IPV6 and IPV4 to enable the functionality. If a rule set to OFF, it is ignored. The default is OFF.

Protocol
This option toggles through ALL, TCP, UDP or ICMP. The setting is used to specify a protocol for this rule. The default is ALL.

Interface In
This option toggles through all possible network interfaces or ALL to select the interface for arriving traffic to apply this rule to. The default is ALL.

Interface Out
This option toggles through all possible network interfaces or ALL to select the destination interface for this rule. The default is ALL.

IPv4 Source Address
This field is used to set an IPv4 source address. This field can be used to restrict incoming packets by specifying an IPv4 address. The default is to 0.0.0.0, which specifies no restrictions.

IPv4 Source Mask
This field sets the network mask for source IP address. These two settings can be used to restrict incoming packets. This setting is ignored if source IP is 0.0.0.0 (no restrictions).

IPv4 Destination Address
The IPv4 destination address can be used to restrict outgoing packets by specifying a destination IP address or subnet. Defaults to 0.0.0.0 -- no restrictions

IPv4 Destination Mask
This field sets the network mask for destination IP. The setting will be ignored if destination IP is 0.0.0.0 (the default).

IPv6 Source Address
This text field sets the IPv6 source address. It can be used to restrict incoming packets by specifying an IPv6 address or prefix. If a prefix is not specified (e.g. 2001:2db:1:2:4:6::/96) /64 is used. The default is blank, meaning no restrictions

IPv6 Destination Address
This setting can be used to restrict incoming packets by specifying an IPv6 address or prefix. If a prefix is not specified (e.g. 2001:2db:1:2:4:6::/96) /64 is used. The defaults is blank -- no restrictions.

Action
This option toggles through NONE, ACCEPT, DROP or REJECT to set the packet action if the rule is a match. If the option is set to NONE, the rule is ignored. The default is to NONE.

Default Gateway Failover

The Default Gateway Failover feature allows the user to specify the default gateway route and a failover route. The specified default gateway is monitored periodically. If it becomes unresponsive, the failover route is set as the default route. In that case, the default gateway is still monitored and, as soon as it becomes responsive, it is reset as the default route.

Note that when this feature is enabled, the default route set on the network page

(net.default.router) is ignored.

Additional information on this feature is available on the Default Gateway Failover Feature Guide on the Asentria Information portal.

```
SiteBoss 550 - Default Gateway Failover
A) Interval                    [2]
B) Timeout                     [30]
C) IPv4 Settings               [OFF]
D) IPv6 Settings               [OFF]
```

Interval
This field is used to specify how often the default router should be checked for connectivity. The value can be from 2 to 120 seconds and defaults to 2 seconds.

Timeout
If the default router is unresponsive for this amount of time, in seconds, the failover route will be used. The value can be from 2 to 600 seconds and defaults to 30 seconds.

Default Gateway Failover - IPv4
This option brings up a submenu to set the IPv4 failover options.

Default Gateway Failover - IPv6
Selecting this option brings up a submenu for setting the IPv6 failover settings.

Default Gateway Failover - IPv4

When this feature is enabled, the default router on the network page (net.default.router) is ignored. When disabled, the unit goes back to using default router on the network page.

```
SiteBoss 550 - Default Gateway Failover - IPv4
A) Enable                      [OFF]
B) Default Gateway             [0.0.0.0]
C) Default Interface           [NONE]
D) Default Source IP           [0.0.0.0]
E) Failover Gateway            [0.0.0.0]
F) Failover Interface          [NONE]
G) Failover Source IP          [0.0.0.0]
```

Enable
This is an ON/OFF toggle to enable or disable the feature. The default is OFF.

Default Gateway
This should be set to the IPv4 address of the default router. If the value is set to 0.0.0.0, the feature is disabled. The default is 0.0.0.0.

Default Interface

This field sets the network interface to use. The unit toggles through all possible interface options. The default is NONE.

Default Source IP
This is an optional setting meant to handle the case when an interface has multiple IPs. It will used by the system as a hint as to which IP address to select for a source address on outgoing packets. The default of 0.0.0.0 allows system to pick without user preference.

Failover Gateway
This field sets the IPv4 address of the failover router. If the value is 0.0.0.0, the feature is disabled. The default is 0.0.0.0.

Failover Interface
This field sets the network interface to use to reach the failover router. The unit toggles through all possible interface options. The default is NONE.

Failover Source IP
This is an optional setting meant to handle the case when an interface has multiple IPs. It will used by the system as a hint as to which IP address to select for a source address on outgoing packets. The default of 0.0.0.0 allows system to pick without user preference.

Default Gateway Failover - IPv6

When this feature is enabled, the default router on the network page `(net.default.router)` is ignored. When disabled, the unit goes back to using default router on the network page.

```
SiteBoss 550 - Default Gateway Failover - IPv6
A) Enable                              [OFF]
B) Default Gateway                     []
C) Default Interface                   [NONE]
D) Failover Gateway                    []
E) Failover Interface                  [NONE]
```

Enable
This is an ON/OFF toggle to enable or disable IPv6 for this feature. The defaults is disabled.

Default Gateway
This should be set to the IPv6 address of the default router. If the value is empty, the feature is disabled.

Default Interface
This field sets the network interface to use. The unit toggles through all possible interface options. The default is NONE.

Failover Gateway
The IPv6 address of the failover router. If the value is empty, the feature is disabled.

Failover Interface

This field sets the network interface to use to reach the failover router. The unit toggles through all possible interface options. If the value is NONE, the feature is disabled. The defaults is NONE.

VPN Settings

The following describes the menu options for configuring VPN Settings. A Virtual Private Network (VPN) is a network that is tunneled (the virtual part), typically across a public network, and secured (the private part). There is more information on SSL VPNs on the Asentria Product Information Portal or contact Asentria Tech Support.

The Asentria unit can be configured with up to 2 VPNs. Although the unit supports multiple VPN configurations, only 1 VPN can be operational at any one time.

```
SiteBoss 550 - VPN Settings
A) VPN 1                                []
B) VPN 2                                []

Enter your Selection: A


SiteBoss 550 - VPN 1 Settings
A) Mode                                 [OFF]
B) Start Mode                           [MANUAL]
C) Description                          []
D) Remote Host                          []
E) Public Interface                     [ANY]
F) SSL Settings
```

Mode

Mode toggles between OFF, IPSEC PRIVATE SUBNET, SSL CLIENT, and SSL SERVER to specify the VPN mode. Default setting is OFF.

Start Mode

The Start Mode toggles between MANUAL, AUTO-PASSIVE and AUTO-ACTIVE. The default is MANUAL.

- MANUAL means the user starts the VPN, it does not start automatically.
- AUTO-PASSIVE means that the unit listens for a VPN connection when the unit starts.
- AUTO-ACTIVE means that the unit starts connecting to a VPN peer when the unit starts.

Description

This is a user-defined string to server as a description for the tunnel. It has no functional impact.

Remote Host

This is the IP address of the IPsec peer on the opposite side of the tunnel to which the tunnel is bound.

Public Interfac

This is the public interface to which the unit's side of the tunnel is bound. The unit toggles

through the available interface options. The default is ANY.

SSL Settings

This option brings up a menu for configuring the settings if the Mode is SSL Client or SSL Server.

```
SiteBoss 550 - VPN 1 SSL Settings
A) Protocol                          [UDP]
B) Port                              [1194]
C) Username                          []
D) Password                          [********]
E) Manual Configuration
```

Protocol

This toggles between UDP and TCP to set the protocol SSL VPN uses to carry VPN traffic. The default setting is UDP.

Port

This sets what port (TCP or UDP, as determined by the SSL Protocol) the VPN uses. The default setting is 1194.

Username / Password

This sets the username and password that a VPN in SSL CLIENT mode uses when it connects to an OpenVPN server. If the username is blank then the username "u<serial number>" will be used. E.g., "u550009999" is the username the unit sends to the OpenVPN server if this setting is blank and the SSL Password setting is not blank. The Username and Password make it so there is an extra layer of authentication to fulfill in order for the VPN to connect. Note: the OpenVPN server must be configured appropriately for this.

Manual Configuration

This displays a menu to set up to 16 manual configuration items for OpenVPN, when the VPN mode is either SSL Client or SSL Server. Any configuration items you need which are not automatically handled for you by the unit (such as SSL port, SSL password, certificates, etc.) should be configured here.

```
SiteBoss 550 - SSL Manual Configuration
A) SSL Configuration 1               []
B) SSL Configuration 2               []
C) SSL Configuration 3               []
D) SSL Configuration 4               []
E) SSL Configuration 5               []
F) SSL Configuration 6               []
G) SSL Configuration 7               []
H) SSL Configuration 8               []
I) SSL Configuration 9               []
J) SSL Configuration 10              []
K) SSL Configuration 11              []
L) SSL Configuration 12              []
M) SSL Configuration 13              []
N) SSL Configuration 14              []
O) SSL Configuration 15              []
P) SSL Configuration 16              []
```

CPE Settings

The CPE Settings menu is where up to 64 different the Customer Premises Equipment (CPE) devices can be configured for keep-alive monitoring by the SiteBoss.

Activate the Alarm functions in the Alarm/Event Definitions/CPE Alarm Settings. Once the devices are configured in this menu and the CPE Alarm Settings are enabled the status of the devices configured for monitoring can be viewed from the command line by typing **?CPE** at the command prompt.

Contact Asentria Tech Support for further information.

```
SiteBoss 550 - CPE Pages
A) CPE Page 1 (CPEs 1-16)
B) CPE Page 2 (CPEs 17-32)
C) CPE Page 3 (CPEs 33-48)
D) CPE Page 4 (CPEs 49-64)

Enter your Selection: A


SiteBoss 550 - CPE Settings
A) CPE 1                                [0.0.0.0]
.. . .
P) CPE 16                               [0.0.0.0]

Enter your Selection: A


SiteBoss 550 - CPE 1 Settings
A) IP Address                           [0.0.0.0]
B) Name                                 []
C) Description                          []
D) Alarm Keep-alive Interval (seconds)  [0]
E) Alarm Threshold                      [1]
F) Alarm Reminder Interval (minutes)    [0]
G) SSH to Telnet Bridging               [OFF]
H) SSH to Telnet Bridging Port          [23]
```

IP Address

This field sets the IP address of the device to monitor. The value is a dotted quad IP address. The default setting is 0.0.0.0

Name

This field sets a name for the equipment. The only restriction on the name is that it cannot have any single or double quotes (' or ") in it. The maximum length is 24 characters.

Description

This field is a description of what the device is. The only restriction on the description is that it cannot have any single or double quotes (' or ") in it. The maximum length is 64 characters.

Alarm Keep-alive Period (seconds)

This field sets the number of seconds between periodic pings (ping cycle) sent by the SiteBoss to the defined device to make sure it is "alive". 1 ping frame is transmitted per CPE per ping

cycle. Values are: 0 to 65535. The default setting is 0.

Alarm Threshold
This option sets the number of times that the unit receives no response to the keep-alive ping from the device before triggering the CPE down event. Values are: 1 to 255. The default setting is 1.

Alarm Reminder Interval (minutes)
This field sets the number of minutes for the associated device to be unresponsive before a reminder alarm is sent. The reminder alarm shares the same event configuration (actions/trap number/class) as a CPE Down event, but includes the text "Reminder". 0 means no reminder event is configured. The default setting is 0.

SSH to Telnet Bridging
This is an ON/OFF toggle on CPE 1 thru 4 only that enables an authorized user to make a Telnet connection to a Telnet-only CPE device while on an SSH connection to the SiteBoss. SSH to Telnet Bridging is used to allow authorized Telnet access to specific machines from the unit, upon successfully connecting to the unit via SSH. The benefit of this feature is that if the SiteBoss is in a network environment where users can be enabled to have access to certain machines via Telnet (via an SSH connection to the SiteBoss) without being allowed access to any other Telnet hosts. The default setting is OFF.

SSH to Telnet Bridging Port
Use this field to set the port for the Telnet Bridging function.

DNP3 Settings

DNP3 is a remote telemetry automation protocol. The network settings for the DNP3 functionality is configured in this menu. The Telemetry Table is configured from the SETUP menu at Alarm/Event Definitions/Telemetry.

The SiteBoss:

- Supports DNP3 as an outstation conveyed via TCP only.
- Listens for TCP connections on port 20000 (by default). It is not a TCP dual end point; that is, it does not both listen for and

initiate TCP connections to masters.

- Can support up to 5 concurrent master connections.
- Conveys sensor telemetry configured in the unit's Telemetry Table.
- Conforms to DNP3 Level 1 implementation.

»**Note**: DNP3 events (which are elements of the DNP3 protocol) are completely independent of SiteBoss events (which have associated management and actions).

See the DNP3 Feature Guide on the Asentria Information Portal for more information.

```
SiteBoss 550 - DNP3 Settings
A) Mode                                [OFF]
```

```
B) Outstation Settings
C) Self Address Enable                [OFF]
D) Keepalive Timeout (seconds)        [30]
E) Max RX Fragment Size               [2048]
F) Max TX Fragment Size               [2048]
G) UR Enable                          [ON]
H) UR Confirm Timeout                 [10]
I) UR Confirm Retries                 [2]
J) Log Filter                         [12]
```

Mode
This toggles the mode between OFF and OUTSTATION to set the DNP3 operation mode. The default is OFF.

Outstation Settings
This option brings up a submenu to configure the Outstation settings.

Self Address Enable
This is an ON/OFF toggle to enable self-address support in DNP3. The default is OFF.

Keepalive Timeout (seconds)
This field sets the DNP3 Keep Alive timeout in seconds. Range 0 ? 255 and the default is 30 seconds. Setting the Keep Alive to 0 disables the Keep Alive function. Upon expiration the unit initiates a Request Link Status data link transaction.

Max RX Fragment Size
This field sets the maximum size of a received fragment in bytes. Settings range from 249 to 2048, with a default at 2048.

Max TX Fragment Size
This field sets the maximum size of a transmitted fragment in bytes. Settings range from 249 to 2048, with a default at 2048.

UR Enable
This is an ON/OFF toggle to enable/disable unsolicited response fragments. The default ON.

UR Confirm Timeout
This field sets the unsolicited response confirmation timeout in seconds. Setting range is from 1 to 60, with a default at 10 seconds.

UR Confirm Retries
This field set the number of unsolicited response confirmation retries the SiteBoss will attempt. Setting range is 0 - 10, with the default at 2.

Log Filter
This is a numeric code to describe what gets logged and it is used for support/troubleshooting analysis only.

Outstation Settings

The SiteBoss is an Outstation and expects connections from master(s). The unit expects a master to request operations on objects, and the master may expect the unit to send it

autonomous messages (unsolicited responses) to convey important telemetry.

```
SiteBoss 550 - DNP3 Outstation Settings
A) TCP Listen Port                    [20000]
B) DNP3 Address of Outstation         [1]
C) IP Address of Master               []
D) DNP3 Address of Master             [65520]
E) DNP3 UR Address of Master          [65520]
```

TCP Listen Port
Use this field to set the TCP port on which to listen for connections. Setting range is 0 - 65534, with the default at 20000.

DNP3 Address of Outstation
Use this field to set the DNP3 address of the outstation. Setting range from 0 to 65519, with the default set at 1.

IP Address of Master
This field sets the IP (v4 or v6) address (non-resolved) of the intended master. Default blank. If non-blank then the outstation drops connections from TCP clients not at this address.

DNP3 Address of Master
This field sets the DNP3 address of the intended master upon connection. Setting range is 0 - 65520, with a default at 65520. If set to 0 - 65519 then the outstation discards DNP3 data link frames not from this address. 65520 is not a valid DNP3 address, so, if set to 65520, it means that the outstation will accept frames from any address.

DNP3 UR Address of Master
This field sets the DNP3 destination address of unsolicited responses. Setting range is 0 - 65520, with a default at 65520. If set to 65520, then the outstation addresses data link frames of unsolicited responses to the source address of the last accepted frame received from the master.

Ethernet Expansion Settings

The Ethernet Expansion settings apply if you have at least one Ethernet Expansion slot card (4E, 8E or SAEC card) installed in the SiteBoss. This feature allows the unit to operate a logical Ethernet interface. If a card is not installed these settings will have no functional effect on the unit.

The Ethernet Expansion Card is a subordinate interface. It is also a built-in 10/100 Ethernet switch. Any node plugged into one card can have its Ethernet traffic conveyed to any other node plugged into another card on the same unit; that is, all cards act together as one logical switch.

Unlike the on-board Ethernet interfaces, an Ethernet Expansion does not support VLANs or DHCP address acquisition. In other words, the Ethernet Expansion can be addressed only by statically assigning it an IP address.

»Caution: do not plug an Ethernet segment carrying a DHCP-managed IPv4 network into any

ETHEXPAN subordinate interface while the unit serves DHCP on it. Doing so will cause conflicts with other nodes on that network and the already-existing DHCP server.

For more detailed configuration and use instructions please refer to the IP Routing and Restrictions Feature Guide.

```
SiteBoss 550 - Ethernet Expansion Settings
A) IP Address                          [0.0.0.0]
B) Subnet Mask                         [255.255.252.0]
C) Router Address                      [0.0.0.0]
D) NAT                                 [ON]
E) DHCP Starting IP Address            [0.0.0.0]
F) DHCP Maximum Clients                [50]
G) DHCP Lease Time (minutes)           [240]
H) DHCP Bootfile Name                  []
I) DHCP VoIP TFTP Server               [0.0.0.0]
J) DHCP Client Classes
K) IPv6 Settings                       [OFF]
L) Secure Access Ethernet Card         [ON]
```

IP Address
Sets the IPv4 address of the unit reachable by nodes on the network interface consisting of the Ethernet Expansion Card(s). If this is default (0.0.0.0), then each card will still convey Ethernet traffic (acting as Ethernet switch) among its nodes but those nodes will not be able to communicate with the unit.

Subnet Mask
Sets the IPv4 subnet mask for the Ethernet Expansion network interface. The default is 255.255.252.0

Router Address
This option sets the IPv4 address of the next hop router for this subnet. If set, it will be displayed as an option in the list of IPv4 default routers.

NAT
This is an ON/OFF toggle to enable/disable network address translation on the forwarded frames. Without NAT, a server would receive a forwarded frame that is IP-addressed

DHCP Starting IP Address
Sets the starting IP address for serving DHCP addresses on the Ethernet Expansion network interface. If this is default (0.0.0.0) then the unit will not run DHCP to serve addresses. This address is required for DHCP server to start and must be on the same subnet as Ethernet Expansion Card IP Address.

DHCP Maximum Clients
This field sets the maximum DHCP IP addresses for unknown clients. The default is 50. The IP address range for unknown clients will be the DHCP Starting IP Address plus the max clients figure.

DHCP Lease Time (minutes)
Lease time for DHCP clients in minutes (default 60).

DHCP Bootfile Name
This option is used to identify a bootstrap file. Not all DHCP clients support it, others actually require it.

DHCP VoIP TFTP Server
Custom option for Cisco SIP phones

DHCP Client Classes
This option brings up DHCP menu configuration to set IP address, or an IP address range to be assigned based on a client's MAC address.

IPv6 Settings
This menu option bring sup a submenu to set IPv6 DHCP settings.

Secure Access Ethernet Card
This option will bring up a menu to setup a Secure Access Ethernet Card (SAEC). The SAEC card is used to facilitate secure web access to local devices that are connected to its ports.

DHCP Client Classes

These settings allow an IP address, or an IP address range to be assigned based on a client's MAC address (partial to full MAC addresses are allowed). For a partial MAC address, an IP address range must be specified; for a full MAC address, just one IP address is needed. All IP addresses must be on the same subnet as the Ethernet Expansion IP Address, set in the Ethernet Expansion Settings section above. Up to 6 different classes can be configured.

```
SiteBoss 550 - DHCP Client Classes
A) Class 1
...
F) Class 6

Enter your Selection: a


SiteBoss 550 -- DHCP Class
A) Class Enable                         [OFF]
B) MAC address (3 to 6 octets)          []
C) Start IP                             []
D) End IP                               []
```

Class Enable
This is an ON/OFF toggle to enable/disable this DHCP class IP Address settings configuration.

MAC address (3 to 6 octets)
Input the client MAC address. MAC entries must have a minimum of 3 octets, each octet must be two characters. Octets must be separated by a semi-colon. For example, valid entries could be one of the following: 00:AA:B0, 10:0a:b0:04:55:60, 10:0a:b0:04:55.

Start IP
Use this field to set a Start IP address for the specified MAC address. If a full MAC address, this is the IP address that will be assigned to the client with that MAC address, and the end IP address is ignored. If partial MAC address, this is the starting IP of a range of IPs that will be

assigned to clients that match the partial MAC address.

End IP
This field sets the End IP address for this MAC address range.

IPv6 Settings

```
SiteBoss 550 IPv6 Settings
A) Mode                          [OFF]
B) Static Address                []
C) Static Router Address         []
D) Host IP Configuration         [OFF]
```

Mode
The mode is either OFF or STATIC. The default is OFF.

Static Address
The static IP address for the expansion card. This must be a valid IPv6 address with an optional prefix length in CIDR notation (CIDR notation is a slash at the end of the address that is followed by the prefix length in bits). The default prefix length is 64.

Static Router Address
The IPv6 address for the next hop IPv6 router. This must be a valid IPv6 address with an optional prefix length in CIDR notation. The default prefix length is 64. If set, it will be displayed as an option in the list of IPv6 default routers.

Host IP Configuration
This option controls how an IPv6 address is set on devices connected to the expansion card ports. Hosts can either use static IPv6 addresses, or if auto address configuration is supported, a router advertisement daemon is available (RADVD). The default is OFF.

Secure Access Ethernet Card

The SAEC card is used to facilitate secure web access to local devices that are connected to its ports.

After the SAEC has been configured, users can initiate a secure web session with a device via an RDP session using the SiteBoss as a target. The RDP session can be initiated by a standard RDP client, or a Web browser that supports HTML5. After the RDP log in, the user is presented with a graphical desktop, and can use the web browser on that desktop to access local devices.

This method allows the user to securely access the local devices from a remote location, even if the device itself does not support secure communication. Only the remote desktop session data is passed onto the insecure public network, and this is encrypted when using RDP.

`net.saec.version`
Read only key which displays the version number of the customized OS image running on the SAEC.

Version Notes

Unknown	SAEC is not responding to requests. Check audit log for more information
1.00	Initial release. SAEC SD card not supported
1.01	Supports SAEC SD card storage for camera images

net.saec.status
Read only status key for the SACE. Any value above 1 implies the SAEC is not ready and the Audit logs will contain more information.

Key value	Meaning
0	Card not detected
1	Ready
2	Could not read setting keys
3	Rebooting
4	Initializing
5	Offline
6	Data error
100	Disabled

See the SAEC Feature Guide for more information.

```
SiteBoss 550A - Secure Access Ethernet Card
A) Enable                       [ON]
B) IP Address                   [0.0.0.0]
C) IPv6 Address                 []
D) Device Settings
E) User Settings
```

Enable
The default setting for this key is ON. A transition from ON to OFF will remove all SiteBoss RDP access to the SAEC, and then the SAEC will be rebooted. When the transition goes from OFF to ON, access to the SAEC via RDP is enabled.

IP Address
IPv4 address of the SAEC. This must be on the same subnet as the Ethernet Expansion IP. Any devices that are connected to SAEC ports must also be on the same subnet.

IPv6 Address
IPv6 address of the SAEC. This should be on the same IPv6 subnet as devices connected to its ports.

Device Settings
This brings up a menu to enter a Name, IP Address, and Port number(80 or 443) for each networked device connected to the SAEC card. If information for a device is not entered here, is will not be remotely accessible via the SAEC card.

User Settings
This option brings up a menu to manage users of the SAEC card.

Device Settings
Information on devices connected on the SAEC subnet is set here. This information is used to create a web page of links to those devices. In the Device Information section, enter a Name, IP Address, and Port number(80 or 443) for each networked device connected to the SAEC card. If information for a device is not entered here, is will not be remotely accessible via the SAEC card.

```
SiteBoss 550A - Device Settings
A) Device 1
. . .
H) Device 8

Enter your Selection: A


SiteBoss 550A - Device Settings
A) Name                                 []
B) IP Address                           []
C) Port                                 [0]
```

Name
This text field allows a user to add a descriptive name of a device connected to a SAEC port

IP Address
This field configures the IPv4 or IPv6 address of the device.

Port
This setting sets the port of the desired network service on the device. Currently only web servers are supported.

User Settings
Existing users with Master privileges will be automatically added as a SAEC user. When a user with Master privileges is added to the SiteBoss via the User Profile menu, that user will be automatically added as a SAEC user.

```
A) Display Users
B) Delete User
```

Display Users
This option will display current users of the SAEC card.

Delete User
When a SiteBoss user is disabled or deleted, the user will automatically be removed from the SAEC card.

» **Note** If a user has a process still running on the SAEC, they may have to be removed via the SAEC menu. If the SAEC user list still displays a disabled user, please restart the SiteBoss, and then remove the user via the SAEC menu.

Ethernet Bridge Settings

The Ethernet Bridge feature allows the onboard Ethernet interfaces, ETH1, ETH2, and (if an SFP Expansion card is installed) ETH3 to bridge with each other. Any combination of ETH1, ETH2, or ETH3 is supported. The bridge supports either Static or DHCP assigned IPv4 addressing.

» **Note**:IPv6 addressing is currently not supported.

Software version 2.11.710 STD or higher is required for this feature to work.

An Ethernet interface is added to the Ethernet Bridge by setting its mode to ETH-BRIDGE. In this mode, any settings (IP, Mask, etc.) on the physical interface are retained, but ignored and the interface is added to the bridge. Any configured interface settings (IP, Mask, etc.) are only used when the mode is set to STATIC.

See the Ethernet Bridge Feature Guide for more information.

```
SiteBoss 550 - Ethernet Bridge Settings
A) IPv4 Mode                    [STATIC]
B) IP Address                   [0.0.0.0]
C) Subnet Mask                  [255.255.255.0]
D) Router Address               [0.0.0.0]
E) NAT                          [ON]
```

Mode
Sets the IPv4 addressing mode, STATIC or DHCP CLIENT for the bridge. If set to static, the user inputs IP, mask and, if applicable, router IP. If set to DHCP client, the DHCP client service is started and waits for DHCP server response(s). The default mode is STATIC.

When switching modes from STATIC to DHCP CLIENT, the bridge's settings will be locked, zeroed, and reset to the settings supplied by the DHCP server (if acquisition is successful). 'Locked' means the settings can not be changed by the user, unless mode is set back to STATIC.

When switching modes from DHCP CLIENT to STATIC, the current IP, mask and router values will be unchanged and settings will be unlocked.

IP Address
If mode is static, this is set by the user to an IPv4 address. If the mode is DHCP client, it will be set when the DHCP client receives it from the DHCP server. The default is 0.0.0.0

Subnet Mask
This is the Network mask. If mode is static, this is set by the user. If the mode is DHCP client, it is set by DHCP client. The default is 255.255.255.0

Router Address
This field sets the network router for the bridge. If mode is static, this is set by the user. If the mode is DHCP client, it is set by DHCP client. Default is 0.0.0.0

NAT
This checkbox is used to Enable / Disable NAT for the bridge. The default is enabled.

Serial Settings

This Menu is used to configure on board serial ports as well as any additional serial ports installed via 4S slot cards.

```
SiteBoss 550 - Serial Settings
A) 1-I/O 1 Settings
B) 2-I/O 2 Settings
```

»Note: Because I/O2 has all the settings the other serial ports have, plus a few more, it will be described in the section below with differences in other ports mentioned when necessary.

```
SiteBoss 550 - Serial 2
A) Target Name                          [I/O 2]
B) Baud Rate                            [19200]
C) Data Format                          [8N1]
D) Handshaking                          [NONE]
E) Wrap Around                          [OFF]
F) Record Stamping
G) Character Masking                    [ON]
H) Data Alarm Enable                    [OFF]
I) Store Data To                        [2]
J) Store Alarms During Pass-Through     [OFF]
K) Duplex                               [FULL]
L) Inactivity Timeout                   [0]
M) Port Mode                            [COMMAND]
N) Strip Sent Pass-Through LFs          [OFF]
O) Strip Received Pass-Through LFs      [OFF]
P) Multiline Record Settings            [OFF]
Q) Data Type                            [ASCII]
R) Change ETX to CR/LF                  [OFF]
```

Target Name
Set the name given to the device connected to the other end of each port. This field will accept

up to 24 alphanumeric characters. The target name is used in event notifications. The default setting is I/O n.

Baud Rate
The Baud Rate option displays a selection menu for baud rates available for the port. These values range from 300 baud to 115200 baud. The default setting is 19200.

Data Format
The Data Format toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, 7N1, 8O2 and 8N2. The default setting is 8N1.

Handshaking
Handshaking toggles settings for how the port will handshake with the connected device. The available options are: NONE, XON/XOFF, BOTH, and DTR. The default setting is NONE.

Wrap Around
Wrap Around is an ON/OFF toggle to set whether the incoming data will wrap (overwrite) the oldest data in the file should it become full. The default setting is OFF.

Record Stamping
This option displays a menu that allows you to select whether the Date/Time and/or the Site Name are pre-pended to each incoming data string. The default setting for Date/Time Stamping and Site Name Stamping is OFF.

Character Masking
This is an ON/OFF toggle to enable the character mask. The character mask allows you to block most non-printing ASCII characters. Specifically, the following ASCII character values are blocked: 0, 1, 4-9, 11, 12, 14-31, and 128-255. The default setting is ON.

Data Alarm Enable
This option is an ON/OFF toggle to enable data alarm monitoring for this port. The default setting is OFF.

Store Data To
This selection displays a menu that toggles ON/OFF whether the data received on this port should be stored to each of the available files or not. The file number that is the same number as the serial port number will be set to ON by default and the other available options will be set to OFF.

Store Alarms During Pass-Through
This is an ON/OFF toggle to determine whether data strings that meet data alarm criteria are stored in the Events File when a pass-through session is active on this port. The default setting is OFF.

Duplex (I/O 2 only)
Duplex controls the echo settings for the command processor. It toggles between FULL and HALF. Full duplex causes the unit to echo all characters sent to the connected terminal when in COMMAND mode. Half duplex turns off character echo. The default setting is FULL.

Inactivity Timeout (I/O 2 only)
This option sets the number of minutes (0 - 255) to wait before a serial connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated.

The default setting is 0.

Port Mode
Port Mode sets the port function.

- I/O 2 toggles between COMMAND, DATA, PPP HOST, PPP CLIENT and RESERVED. The default for I/O2 is COMMAND.
  - COMMAND allows for serial command processor access.
  - DATA configures the port as an inbound RS232 data port.
  - PPP HOST and PPP CLIENT configure the port to act as either a host or client in a PPP over serial port connection See the PPP Over Serial Port Feature Guide on the Asentria Information Portal for more information. The default setting is COMMAND.
  - RESERVED configures the port to communicate with certain 3rd party sensors using Modbus RTU.
- I/O ***n*** All other serial I/O ports toggle between DATA and RESERVED. The Default for all is DATA.

Strip Sent Pass-Through LFs
This is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data sent out of the SiteBoss. The default setting is OFF.

Strip Received Pass-Through LFs
This is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data received by the SiteBoss. The default setting is OFF.

Multiline Record Settings
This selection displays the Multiline Record Settings menu.

Data Type
Data Type toggles between ASCII and BINARY to indicate the type of data being collected on this port. The default setting is ASCII.

Change ETX to CR/LF
This is an ON/OFF toggle to set whether ETX characters in the incoming data should be converted to CR/LF characters. The default setting is OFF.

Multiline Record Settings

The SiteBoss has the ability to monitor incoming serial data for multi-line records (individual records that are broken into multiple lines with carriage returns). If the records are separated by a specific number of blank lines, this basic configuration menu will suffice. If a more complex delineation scheme is used, enable Complex Multiline Detection.

```
SiteBoss 550 - Serial Port 1 Multiline Record Settings
A) Multiline Record Enable              [OFF]
B) Blank Line Count                     [0]
C) Complex Multiline Detection          [OFF]
```

Multiline Record Enable
This is an ON/OFF toggle to enable multiline record detection. The default setting is OFF.

Blank Line Count
This option sets the number of blank lines that must come between records. The default setting is 0.

Complex Multiline Detection
This selection displays settings for detecting complex multiline records. The default setting is OFF.

```
SiteBoss 550 - Serial Port 1 Complex Multiline Record Settings
A) Complex Multiline Record Enable      [OFF]
B) Start Field 1 Character Position     [0]
C) Start Field 1 Text                   []
D) Start Field 2 Character Position     [0]
E) Start Field 2 Text                   []
F) Collect Lines Before Start Record    [0]
G) End Detection                        [FORMULA]
H) Line Count                           [0]
I) End Field 1 Character Position       [0]
J) End Field 1 Text                     []
K) End Field 2 Character Position       [0]
L) End Field 2 Text                     []
```

Complex Multiline Record Enable
This is an ON/OFF toggle to enable advanced multiline detection. The default setting is OFF.

Start Field n Character Position
These fields set the character position used to define the beginning of the multiline field. This option is used with "Count" method record end detection.

Start Field n Text
These fields set the text used to determine the beginning of the multiline field. This option is used with "Formula" method record end detection.

Collect Lines Before Start Record
This option sets the number of blank lines that are between each record.

End Detection
End Detection toggles between FORMULA, COUNT, and BLANKS to set the method of detecting the end of each record. The default setting is FORMULA.

Line Count
Line Count is the number of lines to meter each record at. This option is used with "BLANKS" record end detection.

End Field n Text/Character Position
These options are the counterpart to start the text or character position option. This option sets the end delimiter for multiline records.

Modem Settings

The Modem Settings menu displays two sub-menus for configuring either the optional POTS Dialup Modem or the optional Wireless Modem expansion card. These menu settings will display even if a modem is not installed. If the POTS modem or Wireless modem card are not installed, changing the settings will have no effect on the SiteBoss' functionality.

```
SiteBoss 550 - Modem Settings
A) Dialup Modem
B) Wireless Modem
```

Dialup Modem
This option brings up a menu for configuring the settings for an optional POTS modem card.

Wireless Modem
This option will bring up a menu for configuring an optional wireless modem card.

Dialup Modem

The following is a top level settings configuration overview for the optional Dialup POTS modem. For additional information see the Dialup Modem Feature Guide on Asentria Product Information Portal or contact Asentria Tech Support.

»CAUTION ? To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

»ATTENTION ? Pour réduire les risques d'incendie, utilizer uniquement des conducteurs de télécommunications 26 AWG au de section supérleure.

```
SiteBoss 550 - Dialup Modem Settings
A) Data Format                          [8N1]
B) Duplex                               [FULL]
C) Init String                          [ATM1]
D) Inactivity Timeout                   [0]
E) Upon Modem Connect Go Directly To    [LOGIN]
F) TAP Init String                      [ATM0]
G) TAP Uses 8N1 Data/Parity/Stop        [OFF]
H) Caller ID Security                   [OFF]
```

Data Format
This option toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, and 7N1. The default setting is 8N1.

Duplex
Duplex sets the echo settings for the modem command processor. Full duplex causes the SiteBoss to echo all characters sent to the remote device. Half duplex turns off character echo. The default setting is FULL.

Init String
This option sets the user-defined modem initialization string. This string is sent to the modem

before important factory modem initialization settings, so certain settings in this init string may be overridden. The default setting is ATM1. The Maximum length is 126 characters.

»Note: Make sure to enter "AT" at the beginning of this initialization string.

Inactivity Timeout
This selection sets the number of minutes (0 ? 255) to wait before disconnecting an idle modem connection. A setting of 0 means the connection will never automatically expire. The default setting is 0.

Upon Modem Connect Go Directly To
This menu option toggles through a list of actions to control what a user sees directly after connecting via modem. LOGIN requires the user to login with username and password, and will then take them to a command prompt. A serial port (I/O1, I/O2, etc.) redirects a modem user directly to that serial port upon connecting. In this pass-through mode to the serial ports the command processor of the SiteBoss is transparent. The default setting is LOGIN.

Setting Key: : **modem.hsk**
Values are RTS (default), None and Xon. RTS means that on serial pass-through, the modem uses RTS handshaking, None means no handshaking is used, and Xon means XON/XOFF characters are used.

TAP Init String
This option is the user-defined modem initialization string used only when the modem is making an alphanumeric modem callout. Default setting is ATM0. Maximum length is 126 characters

»Note: Make sure to enter 'AT' at the beginning of this initialization string.

TAP Uses 8N1 Data / Parity / Stop
This is an ON/OFF toggle, to force the TAP initialization string data/parity/stop settings to 8N1. The default setting is OFF.

Caller ID Security
This selection displays a menu that allows configuration of from one to twenty inbound phone numbers. If this feature is enabled then the modem will only answer calls from the specified numbers.

»Note: Caller ID must be available on the phone line connected to the SiteBoss for this feature to work.

```
SiteBoss 550 - Caller ID Security
A) Enable                          [OFF]
B) Caller ID 1                     []
   ...
U) Caller ID 20                    []
V) Add Number From Log List
```

Enable

This is an ON/OFF toggle to enable caller ID restrictions. When enabled, the SiteBoss will only answer the modem if caller ID indicates one of the allowed phone numbers is connecting. The default setting is OFF.

Caller ID n

Select one of these options to add or change a specific phone number. Simple wildcards are allowed in phone numbers: An asterisk (*) wildcard allows for any number of digits to appear to the right of that position. A question mark (?) matches any single digit. If no numbers are defined in this menu, all incoming calls are accepted. The maximum length is 47 characters

Add Number From Log List

Choosing this displays a list of phone numbers that have recently dialed into the SiteBoss. These numbers can then be used for addition to the caller ID list.

Wireless Modem

Below is a brief description of the menu configurations options. For a complete description of the setup and operation of the Wireless Modem, please refer to the Wireless Modem Feature Guide on the Asentria Product Information Portal. Contact Asentria Tech Support for more information.

If the optional Wireless Modem expansion card is not installed in the SiteBoss, this menu is displayed, but changing any of the settings will not do anything, except for the PPP/Wireless User Name and Password settings.

```
SiteBoss 550 - Wireless Modem Settings
A) Mode                                [PERMANENT]
B) APN                                 []
C) PIN                                 []
D) PPP/Wireless User Name              []
E) PPP/Wireless Password               [********]
F) Default Route Enable                [ON]
G) Firewall                            [OFF]
H) Advanced Settings
```

Mode

Mode toggles between SMS ONLY and PERMANENT. SMS ONLY means the modem is only available for out-bound SMS messaging. PERMANENT means the modem maintains an ?always on? connection with the network and is available for incoming connections. The default setting is SMS ONLY.

APN

This option sets the Access Point Name (APN) as defined by your wireless provider. The maximum length is 31 characters.

PIN

Set the PIN associated with the SIM card (if any). The maximum length is 15 characters.

PPP Wireless User Name / Password

These options set the login credentials for the PPP connection, as needed. These settings are identical to the same settings in the PPP Dialout Settings menu ? so a change in one menu will

change the settings in the other. The maximum length for each is 64 characters.

Default Route Enable
This is an ON/OFF toggle to enable the wireless interface to be the default route when connected. The default setting is OFF.

Firewall
This is an ON/OFF toggle to enable or disable the PPP Modem firewall for both PPP Dialout and PPP Hosting. The default is ON. For wireless modem connectivity the firewall will need to be changed to OFF.

Advanced Settings
The Advanced Settings displays a menu allowing for additional configuration of Wireless Modem Settings.

```
SiteBoss 550 - Wireless Modem Advanced Settings
A) Idle Timeout (minutes)               [0]
B) Keep-Alive Threshold (minutes)       [0]
C) PPP Debug Enable                     [OFF]
D) Connectivity Check Settings          [OFF]
```

Idle Timeout
Idle Timeout sets the number of minutes (0 ? 255) to wait before disconnecting an inactive modem connection. A setting of 0 means the connection will not be terminated. The default setting is 0 minutes.

Keep-Alive Threshold (minutes)
This option sets the length of time, in minutes, after which the wireless modem will send an outbound packet to maintain a connection, if no data has been transmitted. A setting of 0 disables this feature. The default is 0.

PPP Debug Enable
This is an ON/OFF toggle to enable capturing PPP traffic to a log file which can be extracted from the device and used for debugging purposes. The default setting is OFF.

{{header-settingslConnectivity Check Settings
This option brings up a menu to set up the unit to check wireless connectivity. The SiteBoss can be configured to ping up to two user-specified IP addresses at a user-specified interval. If the count of consecutive failed tests reaches a user-specified threshold, and the modem is not in use, the SiteBoss will power cycle the wireless modem. If the situation persists the SiteBoss will power cycle.

The modem will not power cycle more often than every 10 minutes. This interval increases on consecutive triggers to a maximum interval of 1 hour. If resetting the modem does not restore connectivity, then the SiteBoss will be power cycled on the next trigger. The SiteBoss will not power cycle more often than every 12 hours. A system message is displayed in any open command processor saying that the system is going to reboot in 30 seconds.

```
SiteBoss 550A - Connectivity Check Settings
```

```
A) Enable                              [OFF]
B) IP Address 1                        [0.0.0.0]
C) IP Address 2                        [0.0.0.0]
D) IP Address 3                        [0.0.0.0]
E) Check Interval (minutes)            [2]
F) Fail Threshold                      [5]
G) RX Reset                            [ON]
```

Enable
This is an ON/OFF toggle to enable or disable the feature. Default is OFF.

IP Address n
Use these fields to set the IP address(es) that will be pinged for the connectivity check. The default is 0.0.0.0, note the unit will not ping 0.0.0.0.

Check Interval (minutes)
This field is used to set how often the IP address(es) will be pinged, in minutes. Range is 1 to 10 minutes. The default is 2.

Fail Threshold
This field sets how many ping checks in a row must fail before the modem or SiteBoss is power cycled. Range is 2 to 50, default is 5.

RX Reset
This check box is an on/off setting that determines whether the connectivity check trigger is inhibited if any data is received on the wireless interface. The default is ON (checked).

Security Settings

The Security Settings menu displays options for setting the security mode, as well as specific and general security settings. See the Securing a SiteBoss Feature Guide on the Asentria Product Information Portal or contact Asentria Technical Support for more information.

```
SiteBoss 550 - Security Settings
A) Security Mode                       [USER PROFILES]
B) Specific Security Settings
C) General Security Settings
```

Security Mode
This option toggles between USER PROFILES and RADIUS to determine which Specific Security Settings menu to be displayed.

USER PROFILES causes option B) Specific Security Settings to display the User Profile Security Settings menu where twelve individual User Profiles can be configured along with Authentication Settings.

RADIUS causes option B) Specific Security Settings to display the RADIUS Security Settings menu where RADIUS authentication server settings can be configured.

The default setting is USER PROFILES.

Specific Security Settings

The contents of this menu are determined by toggling Security Mode.

USER PROFILES causes option B) Specific Security Settings to display the User Profile Security Settings menu where twelve individual User Profiles can be configured along with Authentication Settings.

RADIUS causes option B) Specific Security Settings to display the RADIUS Security Settings menu where RADIUS authentication server settings can be configured. The default setting is USER PROFILES.

General Security Settings

This section contains global Password/Security Settings that set security options that are required for ***every*** user who attempts to log into the SiteBoss.

User Profile Security Settings

When the Security Mode is toggled to USER PROFILES the User Profile Settings will display at Specific Security Settings. This menu is used to configure up to twelve User Names and Passwords along with user specific access permissions and routing.

```
SiteBoss 550 - User Profile Security Settings
A) User 1: admin/********/COMMAND/FILE1
B) User 2:
C) User 3:
D) User 4:
E) User 5:
F) User 6:
G) User 7:
H) User 8:
I) User 9:
J) User 10:
K) User 11:
L) User 12:
M) Authentication Settings
```

User n

All 12 User selections display the configuration menu for that user profile.

Authentication Settings

The Authentication Settings selection displays a menu of global authentication options. Authentication Settings set parameters for passwords and security that are required for every user who attempts to log into the SiteBoss.

User *n* Setup Menu

Use this menu option to configure log in credentials as well as security access permissions for up to twelve users.

```
SiteBoss 550 - User Setup Menu
```

```
A) Enable This User Access              [ON]
B) User Name                            [admin]
C) Password                             [********]
D) User Profile Expiration Date/Time    []
E) Allow User Connection via            [LMTFRSsW]
F) Upon Login then Go To                [COMMAND]
G) Set Pass-through Pointer To          [I/O 1]
H) Pass-through Permissions
I) After PT, ESC Takes User To          [MENU]
J) PPP Connection                       [ROUTING]
K) Setup/Status Rights                  [MASTER]
L) File Release Permissions
M) File Delete Permissions
N) Additional Authentication Options
```

Enable This User Access

This is an ON/OFF toggle to enable access for this user profile.

User Name / Password

These options are used to set the username and/or password for this profile. Maximum length for each is 31 characters.

»Note: By default, the User1 profile is the only one with a preconfigured username and password (admin/password). Usernames and passwords are not pre-configured for Users 2 thru 12. For security reasons it is highly recommended that you change the User 1 password, and record it and all other configured passwords in a secure location.

»Note: User Name and Passwords are case sensitive. Passwords are masked in all menus and while typing them from the command line, for security reasons. If a user without permissions accesses the User Profile Settings menus, they will see all fields in this menu either masked or with no data in them. If they select an option, a message will be displayed that says: ?You do not have permission to change this setting.?

»Note: When configuring a new user name and an invalid or duplicate user name is entered, the SiteBoss responds as follows.

```
Invalid Entry.
Press any key to continue...
```

»Note: When configuring a new password, the SiteBoss will ask you to re-enter the password. If the second entry of the password does not match the first, the Siteboss responds as follows.

```
Invalid Entry - Confirm Password does not match.
Press any key to continue...
```

User Profile Expiration Date / Time

This option is used to set a date and/or time that this profile may be automatically disabled. This menu also provides an option to adjust the current date/time that is on the SiteBoss. Selecting that option will transfer you to the System Date/Time Menu. If left blank, this user profile will not expire. The default setting is blank.

Allow User Connection via

This option displays a menu allowing you to toggle ON or OFF access via Local (Console Port), Modem, Telnet, FTP, Real-Time Socket, SSH (Secure Shell), and the Web interface. These are abbreviated: LMTFRSsW and default setting for all is ON.

```
SiteBoss 550 - Allowed User Connection Via
A) Modem                                [ON]
B) Telnet                               [ON]
C) FTP                                  [ON]
D) Local                                [ON]
E) Real Time Socket                     [ON]
F) SSH                                  [ON]
G) Web                                  [ON]
```

Upon Login then Go To

This menu selection toggles the action this user will be directed to upon logging in, with the following options: COMMAND, PASSTHROUGH and MENU as shown here:

Command

```
SiteBoss
Password: ********
READY
>
```

Pass-through

```
SiteBoss
Password: ********
Connected to I/O 1
```

Menu

```
SiteBoss 550 Version 2.10.420
at 550-550001267
1. Pass-Through to I/O 1
2. Pass-Through to I/O 2
P. 550 Command Prompt
M. 550 Setup Menu
S. 550 Status Menu
X. Exit (end connection)
```

Set Pass-through Pointer To

This selection specifies the destination if the ?Upon Login then Go To? action is set to Pass-Through. This option toggles through the available serial ports and CPE devices (1 thru 4). The default setting is Serial Port I/O 1.

Pass-through Permissions

This option is in effect if the ?Upon Login then Go To? action is set to Menu. This option displays a menu showing all serial ports and CPE devices 1 thru 4, and toggles ALLOW or DENY for each port as needed. If a port is set as ALLOW, then that serial port or CPE devices is displayed in the Menu after the user logs in. If a port is set as DENY, then that serial port is not displayed in the Menu. The default setting for all ports is ALLOW.

After PT, ESC Takes User To

This toggles between MENU and DISCONNECT to set where the user is sent when they exit out of a pass-through connection. The default is MENU.

PPP Connection

This option toggles between LOCAL, ROUTING and NONE. LOCAL allows PPP access, but denies all routing to whatever LAN the SiteBoss is connected to. ROUTING enables Route Ethernet to PPP and Route PPP to Ethernet for the user, but only if those settings are enabled globally. NONE disables PPP access for the user.

Setup / Status Rights

This selection toggles through the actions available to the user if they are given access to the command prompt. Options are MASTER, NONE, VIEW, ADMIN1, ADMIN2, and ADMIN3. See the User Profiles Feature Guide on the Asentria Information Portal for more information on each access level. The default setting is MASTER.

File Release / Delete Permissions

These options set this user?s permissions level to transfer or delete data stored in the units files. Selecting a File option will display a menu showing all data files as well as the Events Log and Audit Log. Selecting one of these options toggles the setting between ALLOW and DENY. The default setting for all is ALLOW.

Additional Authentication Options

This selection displays extra-high security options.

```
SiteBoss 550 - Additional Authentication Options
A) Secure Authentication via Telnet             [OFF]
B) For Telnet, Send Password To                 []
C) Secure Authentication via Modem              [OFF]
D) For Modem, Send Password To                  []
E) Secure Authentication via Local Command Port [OFF]
F) Password Expires After                       [30]
G) Secure Callback 1                            []
H) Secure Callback 2                            []
I) Secure Callback 3                            []
```

Secure Authentication via Telnet/Modem

These two menu options toggle between OFF (regular), CHALLENGE, SEND PASSWORD and CALLBACK (via Modem only) authentication modes. The default setting for each is OFF.

OFF (regular) authentication requires only the normal username/password authentication.

CHALLENGE requires the user send their username/password and then they are prompted with a short challenge code. That code must be plugged into a program called Response Code Generator (RCG). This software can be found on the Documentation and Utilities CD. Contact

Asentria Tech Support for more information on how to use or obtain this application. RCG requires a shared secret as well as the challenge code generated by the SiteBoss. The user must then respond with the proper hash generated by RCG in order to gain access.

SEND PASSWORD will generate a single-use password and send it to the Email address(es) specified by the Send Password To option. That password will only allow a login for the user whom it was generated for.

CALLBACK (via POTS Modem) will cause the SiteBoss to do an immediate callback to the Secure Callback number(s) configured further down in this menu.

For Telnet / Modem, Send Password To
Use these fields to set the Email address(es) where the single-use password is to be sent.

Secure Authentication via Local Command Port
This option toggles between OFF (regular), and CHALLENGE. Because the user is connected via the local Console port, Send Password is not an option. The default setting is OFF.

Password Expires After
This setting is used to set the number of minutes (0 ? 180) before the single-use password expires. A setting of 0 means the password will never automatically expire. The default setting is 0.

Secure Callback n
This option sets the POTS Dial Up modem callback numbers. If configured, the SiteBoss will disconnect any modem connections from this user and then attempt to dial out to each of these numbers. If one of the numbers answers, the other end must respond with the login credentials of the user used to initiate the callback. (Maximum length 48 characters)

Authentication Settings

Authentication Settings set parameters for passwords and security that are required for every user who attempts to log into the SiteBoss.

```
SiteBoss 550 - Authentication Settings
A) Local Command Requires Password      [OFF]
B) Modem Callin Requires Password       [OFF]
C) TCP/IP Port 23 Requires Password     [ON]
D) TCP/IP Port 21xx Requires Password   [OFF]
E) TCP/IP Port 22xx Requires Password   [OFF]
F) Username and/or Password Required    [PASSWORD ONLY]
G) Shared Secret for Challenge/Response [********]
```

Local Command Requires Password
This is an ON/OFF toggle to set whether a password for I/O 2 users is required. The default setting is OFF.

Modem Callin Requires Password
This is an ON/OFF toggle to set whether a password for modem users is required. The default setting is OFF.

TCP/IP Port 23 Requires Password
This is an ON/OFF toggle to set whether a password for Telnet (Port 23) users is required. The default setting is ON.

TCP/IP Port 210x Requires Password
This is an ON/OFF toggle to set whether a password for pass-through (Port 210x) users is required. The default setting is OFF.

TCP/IP Port 220x Requires Password
This is an ON/OFF toggle to set whether a password for Real-Time Socket (Port 220x) users is required. The default setting is OFF.

»Note: When any of the above options is set to OFF, users connecting via that method are automatically granted Master access.

Username and/or Password Required
This option toggles between: PASSWORD ONLY, USERNAME/PASSWORD (PW), or PASSWORD(PW)/USERNAME. The default setting is PASSWORD ONLY.

Shared Secret for Challenge/Response
This selection sets the shared secret used to generate Challenge/Response codes. The Maximum length is 48 characters. Challenge/Response requires the use of the free Asentria Response Code Generator program.

Contact Asentria Tech Support for this, or download (named Response Code Generator) from the Product Resources page on the Asentria website: Response Code Generator

RADIUS Security Settings

If the Security Mode is set to RADIUS the RADIUS Security Settings menu will display under the Specific Security Settings option.

For a complete description and explanation of RADIUS security, please refer to the RADIUS Security Feature Guide on the Asentria Product Information Portal or contact Asentria Tech Support for more information.

```
SiteBoss 550 - Authentication Settings
A) Local Command Requires Password      [OFF]
B) Modem Callin Requires Password       [OFF]
C) TCP/IP Port 23 Requires Password     [ON]
D) TCP/IP Port 21xx Requires Password   [OFF]
E) TCP/IP Port 22xx Requires Password   [OFF]
F) Username and/or Password Required    [PASSWORD ONLY]
G) Shared Secret for Challenge/Response [********]
```

Primary / Secondary Server
Set the IP Address or host name of the primary and secondary RADIUS server.

Primary / Secondary Secret
Set the secret for the primary and secondary RADIUS server. The secret is used to

authenticate RADIUS network traffic. Maximum length for each is 16 characters.

Fallback Mode
This menu toggles between NONE and USER PROFILES. If the unit gets no response from any RADIUS server when attempting to authenticate a user, no further action is taken if this option is set to NONE. The unit falls back to the User Profiles configuration for authentication if this is set to USER PROFILES. The default setting is NONE.

Authentication Port
Set the UDP port (1 ? 65535) that the RADIUS server uses for authentication/authorization. The default port is 1812.

Accounting Port
Set the UDP port (1 ? 65535) that the RADIUS server uses for accounting traffic. Set to 0 to disable RADIUS accounting. The default port is 1813.

CHAP
This is an ON/OFF toggle to set whether the unit uses CHAP (Challenge-Handshake Authentication Protocol) authentication when using RADIUS. ON sets authentication to CHAP. OFF sets authentication to PAP (Password Authentication Protocol). The default setting is OFF.

Timeout
This option sets the number of seconds (1 ? 30) the unit waits for a response from the RADIUS server. The default setting is 3.

Retries
This option sets the number of times (1 ? 30) the unit should try a RADIUS request again after getting no valid response. Valid meaning a response that is verified as really coming from the RADIUS server. The default setting is 3.

General Security Settings

This section contains global Password/Security Settings that set security options that are required for ***every*** user who attempts to log into the SiteBoss.

```
SiteBoss 550 - Global Password/Security Settings Menu
A) Show Username/Password Prompt        [OFF]
B) Globally Allow Access via            [MTFRSs]
C) Button Tap Allows Console Access     [ON]
```

Show Username / Password Prompt
This is an ON/OFF toggle to set whether a prompt for logging in is displayed. The default setting is OFF.

Globally Allow Access via
This selection displays a menu allowing you to toggle ON or OFF access via Modem, Telnet (Ports 23, 200x, 210x), FTP, Real-Time Socket, and Secure Shell (SSH). These are abbreviated: MTFRSs. The default setting for all is ON.

Button Tap Allows Console Access

This is an ON/OFF toggle to give access to a user who has forgotten their log on credentials. This is an insurance policy against locking yourself out of the unit. When set to ON, the user can tap the Reset button 5 times quickly (1-2 times per second), at which point the LEDs on the front panel will flash for a few seconds. The user will then have immediate Console access using the default MASTER username and password (admin/password). The default setting is ON.

If you do not want the Button Unlock feature enabled, for example in environments where physical access is not assumed to be trusted with access, then be sure to turn it OFF.

If you lock yourself out and gain access again with the Button Unlock feature, remember to reconfigure the settings that were defaulted by the Button Unlock feature to maintain your prior security configuration!

These are the settings that are defaulted by this process:

From the SETUP Menu ?Security Settings menu:

- Security Mode set to USER PROFILES
- Specific Security Settings? User 1: ?User Name set to admin, Password set to password and Setup/Status Rights set to MASTER
- Specific Security Settings? Authentication Settings? Local Command Requires Password set to OFF
- General Security Settings? Globally Allow Access via set to every method of connecting

Alarm/Event Definitions

This will display a menu tree which contains the event settings options. The Event section is used to set up actions the SiteBoss should take in response to sensor events, scheduled events, serial handshaking events as well as actions the unit should take in response to a reset or a power cycle

```
SiteBoss 550 - Alarm/Event Definitions Menu
A) Class Table
B) Data Alarm/Filter Settings
C) EventSensor Device Settings
D) No-Data 1 Alarm Settings             [OFF]
E) No-Data 2 Alarm Settings             [OFF]
F) Scheduled Event 1 Settings           [OFF]
G) Scheduled Event 2 Settings           [OFF]
H) Serial Handshaking Alarm Settings
I) CPE Alarm Settings                   [OFF]
J) Data Filter Action                   [REJECT]
K) Reset Event Settings                 [OFF]
L) General Event Settings
M) Global Event Settings
N) Telemetry Settings
```

Class Table
The Class Table option displays the menu for configuring event classification settings. These fields are used to define the severity levels that are assignable to events detected by the SiteBoss. The class number and name are reported in Asentria Alarms, and SNMP traps. It is a mechanism for you to provide varying severities for different alarms so that you can act on them upon receipt.

Data Alarm/Filter Settings
Displays the menus for configuring data event monitoring settings..

EventSensor Device Settings
Displays the menus for configuring any internal or external EventSensors that may be installed.

No-Data n Alarm Settings
These selections displays the menus for configuring alarms based on the period of time when no-data is received on a specific serial port.

Scheduled Event n Settings
These selections display the menus for configuring alarm notifications for specific times and days of the week.

Serial Handshaking Alarm Settings
This option displays the menu for enabling serial handshaking alarms for specific ports.

CPE Alarm Settings
This option displays the menu for configuring Customer Premises Equipment (CPE) monitoring functions. This function is referred to as "Ping Alarms" on the Web interface.

Data Filter Action
The Data Filter Action option toggles between REJECT and ACCEPT to indicate whether data filters are configured to reject or accept specific incoming data string(s).

The filters are configured in the Data Alarm/Filter Settings / Data Alarm Settings / Alarm/Filter Page n / Alarm Filter *n* menu. The default setting is REJECT.

» Note: If no Data Filters are configured, and the Data Filter Action option is toggled to ACCEPT, then no incoming data will be buffered in any of the files. They should always be set to REJECT unless there are Data Filters specifically configured for accepting only certain data.

Reset Event Settings
The Reset Event Settings option displays the menu that is used to configure event actions to be performed after the unit has been reset, either via a restart command, or by power cycling.

General Event Settings
This option displays the menu that permits customization of the event messages that appear in event notifications.

Global Event Settings
The Global Event Settings option displays the menu that is used to configure event settings that will be applied to all events, except those that are designated non-global.

Telemetry Settings

The telemetry table is a table of things to monitor on the unit for which telemetry is made available to other features on the same unit such as DNP3. DNP3 motivated the initial contents of the table, but it also has content for other non-DNP3 functionality.

Class Table CLI

This section describes how to setup or alter the Class Severity levels used for event notifications.

```
SiteBoss 550 - Class Table
A) Class 1                          [Info]
B) Class 2                          [Minor]
C) Class 3                          [Major]
D) Class 4                          [Critical]
. . .
L) Class 12                         []
```

Class n

These fields are used to define the event classification assignable to events detected by the SiteBoss. The maximum length is 47 characters. Info, Minor, Major, and Critical are the default class names assigned to the first four classes. These can be changed and others added as desired to meet your specific needs.

The class number and name are reported in SNMP traps and Emails. It is a mechanism for you to provide varying severities for different alarms so that you can act on them upon receipt.

Data Alarm/Filter Settings

This is the menus for configuring serial data event monitors. A Data Event is a group of settings configured to generate an alarm when specified characters or alpha/numeric strings are received by the SiteBoss. For more information on Data Alarms see the Data Alarm and Event Configuration Feature Guide on the Asentria Product Information Portal or contact Asentria Tech Support.

An S550A will not have these settings.

```
SiteBoss 550 - Data Alarm/Filter Settings
A) Data Alarm Field Settings
B) Data Alarm Macro Settings
C) Data Alarm Settings
D) Display Alarm Status
E) Exit Upon True Data Alarm            [OFF]
```

Data Alarm Field Settings

Selecting this option displays the menu for configuring up to 16 data alarm fields.

Data Alarm Macro Settings

This option displays the menu for configuring up to 100 macros to be used for data alarming. Data alarm macros provide a way to define up to 100 equations that can be used in one or more data alarm equations. Each macro consists of an equation and an associated name that can be used to reference the macro in a data alarm equation. Refer to the Data Alarm and Event Configuration Feature Guide for a more in-depth explanation of configuring data alarm equations. Contact Asentria Tech support for more information.

»**Note**: Macro names and data field names cannot start with $.

»**Note**: Do not start a macro name or data field with AND or OR.

Data Alarm Settings
This selection displays the menu for configuring up to 1000 data alarms or filters.

Display Alarm Status
This menu option prints to the terminal emulator real time information on data event monitors you've configured.

Exit Upon True Data Alarm
This is an ON/OFF toggle to set whether the SiteBoss will stop processing more data event evaluations on a single record after it has found one match. This should be disabled if it is possible to have more than one event in a record. This is a global setting ? it applies to ALL configured data alarms. The default setting is OFF.

Data Alarm Field Settings
This menu is used to set up to 16 data alarm fields.

```
SiteBoss 550 - Data Alarm Field Definition Table
                     Start    Length   Line     Type       Name
A) Definition A      0        0        0        [Alpha]
   ...
P) Definition P      0        0        0        [Alpha]

Enter your Selection: a

SiteBoss 550 - Data Alarm Field Definition
Data Field: A
A) Start Position                     [0]
B) Field Length                       [0]
C) Field Name                         []
D) Field Line Number                  [0]
E) Field Type                         [Alpha]
```

Start Position
This option sets the number of the characters to begin a particular alarm field starting from position 1. Field definition is disabled if set to 0. The default is 0.

Field Length
This sets the length of this particular alarm field. The default setting is 0.

Field Name

This option sets the name given for the alarm field. This name must be unique, is limited to 12 characters, and it must not contain any spaces. It can contain alphanumeric characters and the underscore, but it must start with a letter. These field names are case sensitive. If left blank, you can refer to the field by it?s field letter (A,B, etc?).

»Note: To avoid naming conflicts, the SiteBoss does not allow duplicate field names. The SiteBoss will respond with ?Invalid Entry, Press any key to continue? if a duplicate field name is entered.

Field Line Number
The Line Number sets the optional line number the field should be limited to in multiline records. The default setting is 0.

Field Type
Type toggles between Alpha and Numeric. Alpha is used for most alphanumeric data alarming, and Numeric is used if you need to alarm on a range of numbers. The default setting is Alpha.

Data Alarm Settings

Data alarms are configured by selecting an option from the main Data Alarm/Filter Settings menu, then selecting one of the options which will give you a group of 16 data alarm/filters (1-16, 17-32, etc.) electing the Next or Previous Page Selection Screen. This will display a menu where you can select from those 16 data alarm options.

```
SiteBoss 550 - Data Alarm/Filter Settings
A) Alarm/Filter Page 1 (Alarms 1-16)
...
Q) Next Page Selection Screen

Enter your Selection: A


SiteBoss 550 - Data Alarm/Filter Settings
A) Alarm/Filter 1           []                      [OFF]   [ALARM]
...
P) Alarm/Filter 16          []                      [OFF]   [ALARM]
Q) Next Alarm/Filter Page
R) Setup Alarm/Filter Fields
S) Display Alarm Status
T) Exit Upon True Data Alarm                        [OFF]
```

Alarm/Filter n
These options will display a menu where an individual data alarm or filter can be configured.

Next or Previous Alarm/Filter Page
These options will display either the next or previous set of 16 Data Alarm/Filters.

Setup Alarm/Filter Fields
This option will display the identical Data Alarm Field settings menu as described above. This is simply an easy way to access that menu without having to exit back through the previous menus.

Display Alarm Status

This selection displays real time information on data event monitors you've configured.

Exit Upon True Data Alarm
This is an ON/OFF toggle to set whether the SiteBoss will stop processing more data event evaluations on a single record after it has found one match. This should be disabled if it is possible to have more than one event in a record. This is a global setting ? it applies to ALL configured data alarms. Default setting is OFF.

Alarm/Filter *n* Settings

This is the menu for configuring individual data alarms or filters. Refer to the Data Alarm and Event Configuration Feature Guide on the Asentria Product Information Portal or contact Asentria Tech Support for more information.

```
SiteBoss 550 - Settings For Data Alarm/Filter 1
A) Alarm/Filter Enable                  [OFF]
B) Alarm/Filter Mode                    [ALARM]
C) Alarm/Filter Name                    []
D) Alarm/Filter Equation                []
E) Threshold                            [1]
F) Auto-Clear when Threshold Reached    [ON]
G) Alarm Counter Clear Interval         [12 HOURS]
H) Alarm Counter Reset Time             [00:00]
I) Actions                              []
J) Class                                [Info]
K) Data Alarm Trap Number               [503]
L) Clear This Alarm Counter Now
```

Alarm/Filter Enable
This toggles each individual data event monitor ON or OFF. The default setting is OFF.

Alarm/Filter Mode
This toggles between ALARM and FILTER to indicate whether the SiteBoss will recognize this data event as an Alarm and take some action, or as a Filter and either accept or reject the data string. The Default setting is ALARM.

Alarm/Filter Name
Use this field to set the name for the event monitor. This name is reported with the specified actions. The maximum length is 16 characters).

Alarm/Filter Equation
Set the event equation using the event fields defined in the Data Alarm Field Settings menu. The maximum length is 160 characters.

Refer to the Data Alarm and Event Configuration Feature Guide for a more in-depth explanation of configuring data alarm equations. Contact Asentria Tech Support for more information.

Threshold
This field sets the number of times the event equation must be matched before an event is triggered. If the event counter is allowed to grow beyond the threshold, the unit will not trigger an event again until after the counter is reset. Default setting is 1.

Auto-Clear when Threshold Reached
This is an ON/OFF toggle to control whether the unit will clear the event counter each time the threshold is met. The efault setting is ON.

Alarm Counter Clear Interval
Use this option to set an interval at which the unit should clear the match counter for an individual data event. Available options are: 2 HOURS, 4 HOURS, 6 HOURS, 8 HOURS, 12 HOURS, DAILY, and NEVER. The first clear occurs at midnight. The default setting is 12 HOURS.

Alarm Counter Reset Time
This field sets the time at which the daily clear should take place if it is enabled in the Alarm Counter Clear Interval. This value is in 24-hour format. The default setting is 00:00.

Actions
This selection will display the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured.

Class
This option is used to set the severity class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this data alarm. The default is Info.

Data Alarm Trap Number
This field sets the number to be sent with any SNMP traps for this event. The default is 503, but trap number can also be set in the range of 1000 ? 1199 as needed.

Clear This Alarm Counter Now
This option allows you to clear the counter for the selected data alarm manually. This happens as soon as this option is selected, so make sure you really want to clear the counter before selecting it.

EventSensor Device Settings

The SiteBoss supports a wide variety of internal and external sensor devices including contact closures, temperature and humidity sensors, analog voltage and current sensors and relays. For the purposes of clarity, all of these will be generally referred to as ?EventSensors? (ES) unless a specific type of sensor or relay is being described.

Internal sensors would include any serial port installed in the SiteBoss (which can be configured as contact closures) as well as the temperature sensor if one is installed in the MMC Memory IO slot.

The Sensor Events Menu is used to configure and control EventSensors. There will be a lettered menu option for all EventSensors reporting to the SiteBoss. Because of the numerous ES configurations possible the menus shown in this section will probably not look exactly like the ones for your SiteBoss.

The SiteBoss supports a maximum of 16 external EventSensor slots. This would include any type if IO in the expansion slots as well as any virtual sensors configured by a script and any

sensor reporting to this SiteBoss using the EventSensor Reporting functionality.

Some external EventSensors have dip switches on the EventSensor that will need to be set to the slot number you wish that sensor to display at. On the command interface menu shown below option "B" is slot "1" and option "Q" would be slot "16". Option "A" is the Internal IO, which is referred to as slot "200". In an S550 this refers to the serial ports which can be configured as contact closures for alarming.

1 = DIP Switch up 0 = DIP Switch down

DIP SW	Slot	DIP SW	Slot	DIP SW	Slot	DIP SW	Slot
0000	= 1	0100	= 5	1000	= 9	1100	= 13
0001	= 2	0101	= 6	1001	= 10	1101	= 14
0010	= 3	0110	= 7	1010	= 11	1110	= 15
0011	= 4	0111	= 8	1011	= 12	1111	= 16

For one wire SensorJack sensors the settings slot will automatically be assigned to it if one is available.

```
SiteBoss 550 - Sensor Events Menu
   Name                 ID         Alive      Number     Configuration
A) INTERNAL             --------   -          200        1-TS 6-CC
B) unnamed              03030000   Y          1          8-CC
C)  <none>
D)  <none>
E) unnamed              2004B608   Y          4          8-VS
F) unnamed              3F05B608   Y          5          4-VS
G) R3                   0B06B608   Y          6          8-RL
H)  <none>
I) unnamed              4F17B608   Y          8          9-PW
J)  <none>
K)  <none>
L) unnamed              02050000   Y          11         4-CC
M)  <none>
N)  <none>
O)  <none>
P)  <none>
Q)  <none>
R) Auxiliary Sensor Settings
S) Sensor Unresponsive Settings
```

EventSensor Slots (A thru Q)

The A-Q options display the settings menu for the EventSensor set to the numbered slot. "A" is always reserved for the internal or on-board sensors and is number 200. If an Expansion card is installed it will occupy slot 1 and will be accessed via option B. Any external EventSensors will be listed at menu options B ? Q and will be numbered 1 ? 16. The number refers to the slot number set with the DIP Switches as outlined above.

Auxiliary Sensor Settings

This menu option contains submenus for the non-EventSensor sensors including the Fuel Sensor and AC Power Monitor.

Sensor Unresponsive Settings

This option displays the Sensor Unresponsive Menu where you can configure the actions the SiteBoss takes if an EventSensor becomes unresponsive.

EventSensor Slots

The display for each EventSensor will vary depending on configuration. EventSensors can be configured with varying combinations of sensors. This manual will go over just one of the many types of EventSensor setups. The different types of EventSensors will have different options to configure but each will have a similar set up page. Refer to the EventSensor and SensorJack Sensor Feature Guide for more information.

»**Note**: if you are installing a new EventSensor into a slot that was previously occupied by another sensor the settings need to be cleared. Choose the B-Q option that needs to be cleared then select option ?Clear Settings for This EventSensor? and respond to the confirmation question. Once the slot is clear a new sensor can be configured for that. A restart or a power cycle would be required for the new EventSensor to be recognized by the SiteBoss.

```
SiteBoss 550 - Internal Events Menu
A) Device Name                                  [unnamed]
B) Contact Closure 1                            [unnamed]
C) Contact Closure 2                            [unnamed]
D) Contact Closure 3                            [unnamed]
E) Contact Closure 4                            [unnamed]
F) Contact Closure 5                            [unnamed]
G) Contact Closure 6                            [unnamed]
H) Contact Closure 7                            [unnamed]
I) Contact Closure 8                            [unnamed]
I) EventSensor Reporting Enabled                [OFF]
K) Clear Settings for This EventSensor
```

Device Name

The Device Name is a text field that names the sensor. It is used in traps, e-mails and on the EventSensor Status page. The maximum length is 60 characters.

Contact Closure

Any of the options in the sensor point options in the Internal Events Menu will open a configuration page for that sensor point. This manual will go over only type of EventSensor.

EventSensor Reporting Enabled

This is an ON/OFF toggle to enable a sensor to report to another SiteBoss over a network connection using the EventSensor Reporting functionality.

Clear Settings for This EventSensor

This option is used to clear the EventSensor slot. If an EventSensor is being changed out for a different type of sensor, the slot will need to be cleared then install the new sensor or expansion card and the unit will need to be rebooted. You will get a "Are you sure (y/n)? prompt. Answer with a "y" if you would like to clear the slot.

```
Clearing sensor settings...
Are you sure (y/n)?
```

Contact Closure

Contact Closures (CC) sense the state of a circuit. A weak voltage is applied to the source pin and if pulled to ground by a connection on the circuit, the sensor reports a "closed" state. If it remains high, the sensor reports an "open" state. The contact closures may be configured to alarm in either the open or closed state, depending on the needs of the attached devices.

```
SiteBoss 550 - Internal Contact Closure Event 1
A) Sensor Name                                [unnamed]
B) Contact Closure Enabled                    [OFF]
C) Event State                                [CLOSED]
D) Event Threshold                            [2]
E) Return to Normal Threshold                 [2]
F) Event State Actions                        []
G) Return to Normal Actions                   []
H) Event State Class                          [Info]
I) Return to Normal Class                     [Info]
J) Event Trap Number                          [110]
K) Return to Normal Trap Number               [110]
L) Active Alarm Alias                         []
M) Inactive Alarm Alias                       []
N) Override Global Reminder Interval          [OFF]
O) Individual Reminder Interval (minutes)     [120]
```

Sensor Name

An alphanumeric field that allows you to name this contact closure (maximum length 60 characters). The default setting is 'unnamed'.

Contact Closure Enabled

This is an ON/OFF toggle to enable this contact closure. The default setting is OFF.

Event State

This is an OPEN/CLOSED toggle that determines whether an event will be triggered when the contact closure circuit is opened or closed. The default state is CLOSED.

Event / Return to Normal Threshold

A field that sets the number of seconds (0-255) the sensor must remain in, or be out of, the event state before an event action occurs. The default setting is 2 seconds.

Event State / Return to Normal Actions

Choosing this option displays the Action List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to the Actions List for more information.

Event State / Return to Normal Class

This option is to set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Event / Return to Normal Trap Number
This option is for setting the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Contact Closure Events is 110, but any number in the alternate range of 1000 ? 1199 can be used.

Active Alarm Alias
You can use this option to define a customized name representing the active alarm state. This would be used when reporting active events for this sensor (maximum length 60 characters).

Inactive Alarm Alias
This option functions the same as Active Alarm Alias, but used with Return to Normal events (maximum length 60 characters).

Override Global Reminder Interval
This option is an ON/OFF toggle to override the global reminder interval. If this is set to ON a specific reminder interval can be set for this event. The default setting is OFF.

Individual Reminder Interval (minutes)
This field sets the time in minutes (0 ? 65535) for an action to be repeated if the contact closure that triggered the alarm is still in the "active" state. When the sensor has been returned to the inactive state, the reminder interval is no longer in effect. The default setting is 120 minutes.

Auxiliary Sensor Settings

The Auxiliary Sensor Settings contains submenus for the non-EventSensor sensors including the Fuel Sensor and AC Power Monitor.

```
SiteBoss 550 - Auxiliary Sensor Settings
A) Fuel Sensor Settings
B) AC Power Monitor Settings
```

Fuel Sensor Settings
The Fuel Sensor Settings option displays a submenu for configuring up to three Fuel Sensors.

AC Power Monitor Settings
The AC Power Monitor Settings menu displays a submenu for configuring up to six AC Power Monitors.

Fuel Sensor Settings

The Fuel Sensor Settings option displays a submenu for configuring up to three Fuel Sensors. Refer to the Fuel Sensor Feature Guide for a more in-depth explanation of configuring fuel sensing. Contact Asentria Tech Support for more information.

```
SiteBoss 550 - Fuel Sensor Settings
```

```
A) Fuel Sensor 1
B) Fuel Sensor 2
C) Fuel Sensor 3

Enter your Selection: A


SiteBoss 550 - Settings for Fuel Sensor 1
A) Enable                              [OFF]
B) Sensor Type                         [CURRENT]
C) Name                                [unnamed]
D) Fuel Type                           [DIESEL]
E) Level Measurement Settings
F) Volume Calculation Settings
G) Volume Event Settings
H) Disconnect Event Settings
I) Sudden Change Event Settings
J) Slow Change Event Settings
```

Enable
This is an ON/OFF toggle to enable the fuel sensor. The default setting is OFF.

Sensor Type
The Sensor Type toggles between CURRENT, VOLTAGE and RESISTIVE FLOAT. The default is Current.

Name
The Name option is an alphanumeric field that allows you to name this fuel sensor (maximum length 60 characters). The default setting is ?unnamed?.

Fuel Type
This toggles through DIESEL, PROPANE, NATURAL GAS, HYDROGEN, GASOLINE, and OTHER to define the type of fuel being monitored. The Default is Diesel.

Level Measurement Settings
This option displays a submenu to set up the fuel level measurement settings.

Volume Calculation Settings
This option displays the menu for configuring the prerequisite measurements taken that apply to the dimensions of the fuel tank, including custom tank settings.

Volume Event Settings
This option displays the menu for configuring alarm notifications based on changes in the fuel level.

Disconnect Event Settings
This option displays the menu for configuring alarm notifications of the fuel sensor being disconnected.

Sudden and Slow Change Event Settings
These are settings to trigger an event if there is a sudden change in volume in the fuel level readings.

Level Measurement Settings

This menu is used to configure the fuel level measurement settings.

```
SiteBoss 550 - Level Measurement Settings for Fuel Sensor 1
A) Analog Input EventSensor             [200]
B) Analog Input Point                   [1]
C) Distance Unit                        [CM]
D) Raw Value Top                        [5.0]
E) Top Offset                           [0.0]
F) Raw Value Bottom                     [0.0]
G) Bottom Offset                        [0.0]
```

Analog Input EventSensor

This field sets the slot number of the EventSensor associated with this fuel sensor. Allowed values are 200 (for Internal EventSensor) or 1 ? 16. The default value is 200.

Analog Input Point

This field sets the input point on the EventSensor that is associated with this fuel sensor. Range is 1-48. The default value is 1.

Distance Unit

This option toggles between INCH or CM to specify the distance unit to be used when setting an indicated tank dimension. The default value is CM.

Raw Value Top

This field sets the analog input reading that corresponds to the SENSOR FULL point. This is an integer with range of 0 to 2,147,483,647. The default value is 5.0.

Top Offset

The Top Offset defines the distance, in the specified distance unit, between the SENSOR FULL point and the TANK FULL point. This is a floating-point value with range of -1,000 to +1,000. A positive value means the SENSOR FULL point is above the TANK FULL point, and a negative value means it is below. The default value is 0.0.

Raw Value Bottom

This field sets the analog input reading that corresponds to the minimum fluid height measurable by the fuel sensor. This is an integer with range of 0 to 2,147,483,647. The default value is 0.0.

Bottom Offset

The Bottom Offset defines the distance, in the specified distance unit, between the SENSOR EMPTY point and the TANK EMPTY point. This is a floating-point value with range of -1,000 to +1,000. A positive value means the SENSOR EMPTY point is above the TANK EMPTY point and a negative value means it is below the TANK EMPTY point. The default value is 0.0.

Volume Calculation Settings

The Volume Calculations Settings is the menu for configuring the prerequisite measurements taken that apply to the dimensions of the fuel tank, including custom tank settings.

```
SiteBoss 550 - Volume Calculation Settings for Fuel Sensor 1
A) Tank Shape                          [LINEAR]
B) Tank Height                         [100.0]
C) Tank Dimension A                    [0.0]
D) Tank Dimension B                    [0.0]
E) Tank Volume                         [200.0]
F) Volume Unit                         [Liters]
G) Input Filter Averaging              [1]
H) Custom Tank Settings
```

Tank Shape
The Shape toggles between LINEAR, HORIZ CYL, VERT OVAL, and CUSTOM to set the shape of the fuel tank. The default value is LINEAR.

Tank Height
This field sets the height of the tank, from the TANK EMPTY point to the TANK FULL point, in the specified distance unit. This is a floating-point value with range of 0.0 to 1000. The default value is 100.

Tank Dimension A
This field sets tank dimension measurement A for certain tank profiles, in the specified distance unit. For VERT OVAL this is the horizontal length of the tank. This is a floating-point value with range of 0.0 to 1000. The default value is 0.0.

Tank Dimension B
This field sets tank dimension measurement B for certain tank profiles, in the specified distance unit. For VERT OVAL this is the width of the tank. This is a floating-point value with range of 0.0 to 1000. The default value is 0.0.

Tank Volume
This field sets the number of volume units the tank contains when full. Range is 0 to 2,147,483,647. The default value is 200.0.

Volume Unit
This field sets the name of the unit representing fluid volume in the tank. This is only used for display purposes and it does not affect the volume calculation in any way. The default value is "Liters?.

Input Filter Averaging
This option sets the number of samples used to filter the analog input value that is used for the tank volume calculation. The filtering is applied after the adjusted raw value. Range is 1 to 300; default is 1 (no filtering).

Custom Tank Settings
When CUSTOM is selected for tank shape, the system uses user-provided data to calculate the volume of fluid in the tank. The data is entered into a table of height/volume pairs, where a fluid height and corresponding tank volume are entered. Up to 32 height/volume pairs can be entered.

Volume Event Settings

This menu is used for configuring alarm notifications based on changes in the fuel level.

```
SiteBoss 550 - Volume Event Settings for Fuel Sensor 1
A) Event Enabled                        [OFF]
B) Deadband                             [6.0]
C) Very High Event Settings             [180.0]  []        [519]  [Info]
D) High Event Settings                  [160.0]  []        [519]  [Info]
E) Return to Normal Settings            [-]      []        [519]  [Info]
F) Low Event Settings                   [40.0]   []        [519]  [Info]
G) Very Low Event Settings              [20.0]   []        [519]  [Info]
```

Event Enable

This is an ON/OFF toggle to enable Volume Events. The default setting is OFF.

Deadband

The Deadband sets a range (in volume units) for the fuel volume setting. This prevents the event from repeatedly going in and out of the alarm state. For the alarm to clear the volume must cross the threshold plus the deadband value. The default deadband is 6.0.

Very High / High / Return to Normal / Low / Very Low Event Volume Settings

These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 - Volume Event Settings
A) Very Low Event Volume                [20.0]
B) Very Low Event Actions               []
C) Very Low Event Trap Number           [519]
D) Very Low Event Class                 [Info]
```

Very High / High / Low / Very Low Event Volume

Set the fuel volume (in volume units) threshold at which the Event Action(s) will be triggered.

Very High / High / Return to Normal / Low / Very Low Event Actions

Set the action(s) that will be triggered once the fuel level crosses the threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number

Set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all fuel volume events is 519, but any number in the alternate range of 1000 ? 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class

Set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Disconnect Event Settings

This menu is for configuring alarm notifications of the fuel sensor being disconnected.

```
SiteBoss 550 - Disconnect Event Settings for Fuel Sensor 1
A) Event Enabled                        [OFF]
B) High Value                           [0.0]
C) Low Value                            [0.0]
D) Event Actions                        []
E) Event Trap Number                    [515]
F) Event Class                          [Info]
G) Normal Actions                       []
H) Normal Trap Number                   [515]
I) Normal Class                         [Info]
```

Event Enabled

This is an ON/OFF toggle to enable Disconnect Events. The default setting is OFF.

High / Low Value

These menu options are used to set the High end and low end of normal for the analog input associated with the fuel sensor. If the input value falls outside the delineated range, then the sensor is considered "disconnected". If both high and low values are set to 0 (the default value), then the sensor will always be considered "connected".

Event Actions

This menu option is used to set the action(s) that will be triggered if the fuel level sensor is disconnected. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Event Trap Number

This option is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for disconnect events is 515, but any number in the alternate range of 1000 ? 1199 can be used.

Event Class

This option is used to set the class for the event. This user-configurable optional setting defines the severity of the event. An event severity is defined in the user configurable Class Table.

Normal Actions

This option is used to set the action(s) that will be triggered once the fuel sensor is no longer disconnected. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Normal Trap Number

This option is used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number is 515, but any number in the alternate range of 1000 ? 1199 can be used.

Normal Class

This option is used to set the class for the event. This user-configurable optional setting defines the severity of the event. Enter one of the classes that are defined in the Class Table settings menu. The default value is Info.

Sudden and Slow Change Event Settings

The Sudden and Slow Change Event settings are used to trigger an event if the change in volume in the fuel level readings moves out of configured settings.

```
SiteBoss 550 - Sudden Change Event Settings for Fuel Sensor 1
A) Event Enabled                        [OFF]
B) Time (minutes)                       [10]
C) Amplitude (volume units)             [10.0]
D) Actions                              []
E) Trap Number                          [527]
F) Class                                [Info]
```

Event Enabled

This is an ON/OFF toggle used to enable the Change Event. The default value is OFF.

Time

This field is used to define a time window that would trigger the Change Event. For a Sudden Change Event the time is minutes. The default is 10 minutes. For a Slow Change the time is hours and the default is 6 hours.

Amplitude (volume units)

The Amplitude is the amount of change, in volume units, that triggers an event.

Actions

This option sets the action(s) that will be triggered if there is a sudden or slow change in the fuel level readings. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to the Actions List for more information.

Trap Number

This option is for setting the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for a Sudden Change event is 527 and for a Slow Change the trap number is 528. Any number in the alternate range of 1000 ? 1199 can be used.

Class

This option is for setting the class for the event. This user-configurable optional setting defines the severity of the event. Enter one of the classes that are defined in the Class Table settings menu. The default value is Info.

AC Power Monitor Settings

The AC Power Monitor Settings menu is used to configuring up to six AC Power Monitors. Refer to the AC Power Monitoring Feature Guide for a more in-depth explanation of

configuring AC power monitoring. Contact Asentria Technical Support for more information.

```
SiteBoss 550 - Settings for AC Power Monitor 1
A) Enable                              [OFF]
B) Device Type                         [YD2010]
C) Name                                [unnamed]
D) Device Settings
E) Average Voltage Settings
F) Average Current Settings
G) Frequency Settings
H) Total Real Power Settings
I) Total Power Factor Settings
J) Disconnect Event Settings
```

Enable
This is an ON/OFF toggle to enable the AC Power Monitor. The default setting is OFF.

Device Type
This option is used to define the model of the AC Power Monitoring Device. It toggles between YD2010, WATTSON, WATTSON MKII, CT-2EMG, ETA3.RTU, EM270, WATTNODE, and PM1200. The default is YD2010.

Name
This is an alphanumeric field that allows you to name this Power Monitor (maximum length 60 characters). The default setting is ?unnamed?.

Device Settings
This option displays a menu containing device settings.

Average Voltage Settings
This option displays a menu where the Average Voltage Event Settings can be configured.

Average Current Settings
Displays a menu where the Average Current Event Settings can be configured.

Frequency Settings
The Frequency Settings option displays a menu where the Event Settings for the frequency, in hertz, can be configured.

Total Real Power Settings
This option displays a submenu where the Event Settings for the Total Real Power, in watts, can be configured.

Total Power Factor Settings
This option displays a submenu where the Event Settings for the Total Power Factor can be configured.

Disconnect Event Settings
This option displays a menu where an AC Power Disconnect Event can be configured

Device Settings

This is a menu where you can configure the settings for your AC Power Device.

```
SiteBoss 550 - Device Settings for AC Power Monitor 1
A) Comm Port                          [1]
B) Modbus Address                     [1]
C) PT Ratio                           [1]
D) CT Ratio                           [1]
E) Power Type                         [3P4W]
```

Comm Port

Command port that the AC power monitor is connected to. This refers to the serial port number that the monitor is connected to.

Modbus Address

Modbus address of the AC power monitor device. This is an integer setting with a range of 1 to 247. The default value is 1.

PT Ratio

Ratio of secondary turns to primary turns on potential transformers (PT). This is an integer setting with a range of 1 to 10000. The default value is 1.

CT Ratio

Ratio of secondary turns to primary turns on current transformers (CT). This is an integer setting with a range of 1 to 10000. The default value is 1.

The CT can be gotten from the label on the Current Transformer. For the Split Core Current Transformer 5004-080 sold with the YADA AC Power Monitor the Primary current is 200A and the Secondary current is 5A. To get the correct setting for the CT Ratio divide the primary current by the secondary current, 200 / 5 = 40. The CT Ratio is 40 for most Current Transformers.

Power Type

This is a toggle to define the type of power being monitored. The possible values are 1P2W, 1P3W, 3P3W, and 3P4W. The default value is 3P4W.

Average Voltage Settings

This menu contains the options for configuring Average Voltage Events.

```
SiteBoss 550 - Average Voltage Event Settings for AC Power Monitor 1
A) Event Enabled                      [OFF]
B) Deadband                           [3.0]
C) Very High Event Settings           [253.0]  []       [520]  [Info]
D) High Event Settings                [243.8]  []       [520]  [Info]
E) Return to Normal Settings          [-]      []       [520]  [Info]
F) Low Event Settings                 [216.2]  []       [520]  [Info]
G) Very Low Event Settings            [207.0]  []       [520]  [Info]
```

Event Enable
This is an ON/OFF toggle to enable the Average Voltage Event. The default setting is OFF

Deadband
The Deadband option allows you to set a voltage figure to prevent the event from repeatedly going in and out of an "alarm state" as the voltage reading fluctuates above and below the alarm setting. For the alarm to clear the voltage reading must cross the threshold plus the deadband value. The default value is 3.0.

Very High / High / Return to Normal / Low / Very Low Average Voltage Event Settings
These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 - Average Voltage Event Settings for AC Power Monitor 1
A) Very High Event Value               [253.0]
B) Very High Event Actions             []
C) Very High Event Trap Number         [520]
D) Very High Event Class               [Info]
```

Very High / High / Low / Very Low Event Volume
These fields are used to set the average voltage value which triggers the Event Action(s). The range for each tier setting is 0 to 1000 with the defaults shown above in the screen shot.

Very High / High / Return to Normal / Low / Very Low Event Actions
These fields are used to set the action(s) that will be triggered when the average voltage crosses the set threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Voltage Events is 520, but any number in the alternate range of 1000 ? 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class
These fields are used to set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Average Current Settings

This menu contains the options to configure the Average Current Events.

```
SiteBoss 550 - Average Current Event Settings for AC Power Monitor 1
A) Event Enabled                       [OFF]
B) Deadband                            [1.0]
C) Very High Event Settings            [30.0]  []        [521]  [Info]
D) High Event Settings                 [22.5]  []        [521]  [Info]
E) Return to Normal Settings           [-]     []        [521]  [Info]
```

```
F) Low Event Settings                  [17.7]  []        [521]  [Info]
G) Very Low Event Settings             [10.0]  []        [521]  [Info]
```

Event Enable
This is an ON/OFF toggle to enable the Average Current Event. The default setting is OFF

Deadband
The Deadband option allows you to set a current figure to prevent the event from repeatedly going in and out of an "alarm state" as the current value fluctuates above and below the alarm setting. For the alarm to clear the amperage reading must cross the threshold plus the deadband value. The default deadband value is 1.0.

Very High / High / Return to Normal / Low / Very Low Average Voltage Event Settings
These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 - Average Current Event Settings for AC Power Monitor 1
A) Very High Event Value               [30.0]
B) Very High Event Actions             []
C) Very High Event Trap Number         [521]
D) Very High Event Class               [Info]
```

Very High / High / Low / Very Low Event Volume
These fields are used to set the average current, in amps, which triggers the Event Action(s). The range for each tier setting is 0 to 1000 with the defaults shown above in the screen shot.

Very High / High / Return to Normal / Low / Very Low Event Actions
These fields are used to set the action(s) that will be triggered when the average current crosses the set threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Current Events is 521, but any number in the alternate range of 1000 ? 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class
These fields are used to set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Frequency Settings

The Frequency Settings menu is where the Event Settings for the frequency variations can be configured.

```
SiteBoss 550 - Frequency Event Settings for AC Power Monitor 1
A) Event Enabled                        [OFF]
B) Deadband                             [0.5]
C) Very High Event Settings             [52.0]   []        [522]  [Info]
D) High Event Settings                  [51.0]   []        [522]  [Info]
E) Return to Normal Settings            [-]      []        [522]  [Info]
F) Low Event Settings                   [49.0]   []        [522]  [Info]
G) Very Low Event Settings              [48.0]   []        [522]  [Info]
```

Event Enable
This is an ON/OFF toggle to enable the Frequency Event. The default setting is OFF

Deadband
The Deadband option allows you to set a frequency Hz figure to prevent the event from repeatedly going in and out of an "alarm state" as the reading fluctuates above and below the alarm setting. For the alarm to clear the Hz reading must cross the threshold plus the deadband value. The default value is 0.5.

Very High / High / Return to Normal / Low / Very Low Event Settings
These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 ? Frequency Event Settings for AC Power Monitor 1
A) Very High Event Value                [52.0]
B) Very High Event Actions              []
C) Very High Event Trap Number          [522]
D) Very High Event Class                [Info]
```

Very High / High / Low / Very Low Event Value
These fields are used to set the frequency, in hertz, which triggers the Event Actions. The range is 0 to 1000 with the default for each range setting pictured above in the screen shot.

Very High / High / Return to Normal / Low / Very Low Event Actions
These fields are used to set the action(s) that will be triggered when the frequency crosses the set threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number
These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Current Events is 522, but any number in the alternate range of 1000 ? 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class
Set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Total Real Power Settings

This menu is where the Event Settings for the Total Real Power can be configured.

```
SiteBoss 550 - Total Real Power Event Settings for AC Power Monitor 1
A) Event Enabled                        [OFF]
B) Deadband                             [30.0]
C) Very High Event Settings             [7500.0] []        [523]  [Info]
D) High Event Settings                  [5500.0] []        [523]  [Info]
E) Return to Normal Settings            [-]      []        [523]  [Info]
F) Low Event Settings                   [4500.0] []        [523]  [Info]
G) Very Low Event Settings              [2500.0] []        [523]  [Info]
```

Event Enable

This is an ON/OFF toggle to enable the Total Real Power Event. The default setting is OFF

Deadband

The Deadband option allows you to set a Watts figure to prevent the event from repeatedly going in and out of an "alarm state" as the Watt reading fluctuates above and below the alarm setting. For the alarm to clear the Watts must cross the threshold plus the deadband value. The default value is 30.0.

Very High / High / Return to Normal / Low / Very Low Event Settings

These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 ? Total Real Power Event Settings for AC Power Monitor 1
A) Very High Event Value                [7500.0]
B) Very High Event Actions              []
C) Very High Event Trap Number          [523]
D) Very High Event Class                [Info]
```

Very High / High / Low / Very Low Event Value

These fields are used to set the Real Power readings, in watts, which trigger the Event Actions. The range is 0 to 100,000 with the defaults in the screen shot above.

Very High / High / Return to Normal / Low / Very Low Event Actions

These fields are used to set the action(s) that will be triggered when the Real Power readings cross the set threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Very High / High / Return to Normal / Low / Very Low Event Trap Number

These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Current Events is 523, but any number in the alternate range of 1000 ? 1199 can be used.

Very High / High / Return to Normal / Low / Very Low Event Class

Set the class for the event. When this option is selected, a list of the classes previously defined

in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Total Power Factor Settings

The Power Factor Settings can be configured at this menu location. Note that the power factor can be reported as a positive or negative value. For the purposes of alarming, only the absolute value is used.

```
SiteBoss 550 - Total Power Factor Event Settings for AC Power Monitor 1
A) Event Enabled                        [OFF]
B) Deadband                             [0.10]
C) Return to Normal Settings            [-]      []        [540]  [Info]
D) Low Event Settings                   [0.90]   []        [540]  [Info]
E) Very Low Event Settings              [0.70]   []        [540]  [Info]
```

Event Enable

This is an ON/OFF toggle to enable the Total Power Factor Event. The default setting is OFF

Deadband

The Deadband option allows you to set a figure to prevent the event from repeatedly going in and out of an "alarm state" as the readings fluctuates above and below the alarm setting. For the alarm to clear the Power Factor figure must cross the threshold plus the deadband value. The default value is 0.1.

Return to Normal / Low / Very Low Event Settings

These options display submenus where the event action settings can be configured for each event level.

```
SiteBoss 550 - Total Power Factor Event Settings for AC Power Monitor 1
A) Low Event Value                      [0.90]
B) Low Event Actions                    []
C) Low Event Trap Number                [540]
D) Low Event Class                      [Info]
```

Low / Very Low Event Value

These fields are used to set the Power Factor settings which trigger the Event Actions. The range is 0.0 to 1.0. The default is 0.90 for low and 0.70 for very low event.

Return to Normal / Low / Very Low Event Actions

These fields are used to set the action(s) that will be triggered when the Power Factor crosses the set threshold. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Return to Normal / Low / Very Low Event Trap Number

These fields are used to set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Average Current Events is 540, but any number in the alternate range of 1000 ? 1199 can be used.

Return to Normal / Low / Very Low Event Class

These fields are used to set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Disconnect Event Settings

The disconnect event is triggered if communication with the AC power monitor device fails for one minute. The return to normal event is triggered upon the first subsequent successful communication attempt.

```
SiteBoss 550 - Disconnect Event Settings for AC Power Monitor 2
A) Event Enabled                        [OFF]
B) Event Actions                        []
C) Event Trap Number                    [524]
D) Event Class                          [Info]
E) Normal Actions                       []
F) Normal Trap Number                   [524]
G) Normal Class                         [Info]
```

Event Enable

This is an ON/OFF toggle to enable the Disconnect Event. The default setting is OFF

Event / Normal Actions

Set the action(s) that will be triggered when the AC power monitor fails. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Event / Normal Trap Number

Set the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for all Disconnect Events is 524, but any number in the alternate range of 1000 ? 1199 can be used.

Event / Normal Class

Set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Sensor Unresponsive Settings

The Sensor Unresponsive Menu is where you can configure the actions the SiteBoss takes if an EventSensor becomes unresponsive.

```
SiteBoss 550 - Sensor Unresponsive Menu
A) Sensor Unresponsive Timeout                  [30]
B) Sensor Unresponsive Actions                  []
C) Sensor Unresponsive Trap Number              [50]
D) Sensor Unresponsive Class                    [Info]
```

Sensor Unresponsive Timeout
Set the time (10 - 65535 seconds) to wait before declaring a non-communicative EventSensor unresponsive. The default setting is 30.

Sensor Unresponsive Actions
Choosing this option displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

ensor Unresponsive Trap Number
Set the trap number to be sent with any SNMP traps for this event. The default is 50, but the trap number can also be set in the range of 1000 ? 1199 as needed.

Sensor Unresponsive Class
Set the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

No-Data *n* Alarm Settings

No Data Alarms can be configured on the SiteBoss to monitor data coming in via the serial ports, and take an alarm action if a certain period of time passes with no data.

These menu options allow you to configure two separate No-Data Alarms, each of which can be configured for two different ranges of times with different time durations. The periods of time should be configured to match the calling patterns of your business or organization. For example, if your normal business hours are M-F 8:00 to 5:00, you will want to set lower time durations during those hours than you would ?after hours? when call volumes are lighter and the periods of time where there is "no data? might be longer.

```
SiteBoss 550 - No-Data Alarm 1 Settings
A) Alarm Enable                         [OFF]
B) Alarm Actions                        []
C) Alarm Message                        [No-Data Timeout 1]
D) Alarm Class                          [Info]
E) Trap Number                          [505]
F) Schedule 1 Begin Time                [00:00]
G) Schedule 1 End Time                  [00:00]
H) Schedule 1 Duration (minutes)        [0]
I) Schedule 2 Begin Time                [00:00]
J) Schedule 2 End Time                  [00:00]
K) Schedule 2 Duration (minutes)        [0]
L) Apply Alarm on Days                  [MTuWThF]
M) Enable Ports
N) Add Exclusion
O) Delete Exclusion
   []
   []
```

Alarm Enable
This is an ON/OFF toggle to enable the no-data monitor. The default setting is OFF.

Alarm Actions
This option displays the Actions List, a menu where the action string for the event is

configured. In the No-Data Alarm n Settings menu shown above, this field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Alarm Message
This menu option sets the text string to be delivered with this event?s alarms. The default setting is "No-Data Timeout n". The maximum length is 126 characters.

Alarm Class
Set the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this no-data alarm.

Trap Number
Set the number to be sent with any SNMP traps for this event. The default is 505, but trap number can also be set in the range of 1000 ? 1199 as needed.

Schedule n Begin Time / End Time
Use these menu options to set the beginning and ending times (24 hour clock) for each of two ranges of time.

Schedule n Duration
These fields set the number of minutes (0-65535) the unit will wait without receiving data before alarming.

Apply Alarm on Days
This option displays a menu where the seven days of the week are listed, and each can be toggled ON or OFF to designate whether this particular No-Data alarm is active on that day. The default setting is ON for Monday thru Friday, and OFF for Saturday and Sunday.

Enable Ports
This selection displays a menu where the installed serial ports are listed and each can be toggled ON or OFF to designate whether this particular No-Data alarm is active on that port. The default setting is OFF for all ports.

Add Exclusion / Delete Exclusion
These fields allow you to add or delete specific dates when this No-Data Alarm should "take the day off". For example Christmas is a day you might want to add here. Select Add Exclusion and type in 12/25. To delete a date, select Delete Exclusion and type in the date you want to remove. After an exclusion date is added it appears in the brackets at the bottom of the menu. Up to fifteen dates can be entered to be excluded.

Scheduled Event *n* Settings

Scheduled Events allow you to schedule specific a specific date/time for an alarm action to occur. For example, you might want the SiteBoss to send you an Email every morning at 8:00 just so you know it is live on the network.

There are two separate Scheduled Event options which allow for the configuration of two separate Scheduled Events, each of which can be configured for any one time on any day of the week. Each day?s time can be scheduled independently from the others.

```
SiteBoss 550 - Scheduled Event 1 Setup
A) Enable Event                          [OFF]
B) Event Actions                         []
C) Event Message                         [Scheduled Event 1]
D) Event Class                           [Info]
E) Trap Number                           [506]
F) Event Time Sunday                     [OFF]
G) Event Time Monday                     [OFF]
H) Event Time Tuesday                    [OFF]
I) Event Time Wednesday                  [OFF]
J) Event Time Thursday                   [OFF]
K) Event Time Friday                     [OFF]
L) Event Time Saturday                   [OFF]
M) Add Exclusion
N) Delete Exclusion
   []
   []
```

Enable Event
This is an ON/OFF toggle to enable the Scheduled Event. The default setting is OFF.

Event Actions
This option displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Event Message
Use this field to set the text string to be delivered with this event?s action. The default setting is "Scheduled Event *n*". The maximum length is 126 characters.

Event Class
Set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this event.

Trap Number
Set the number to be sent with any SNMP traps for this event. The default is 506, but trap number can also be set in the range of 1000 ? 1199 as needed.

Event Time day
Use this option to set the time (24 hour clock) each day at which the Scheduled Event action will occur. If no time is configured for any day, this menu displays OFF. The default setting is OFF for each day.

Add Exclusion / Delete Exclusion
These fields allow you to add or delete specific dates when this Scheduled Event should ?take the day off?. For example Christmas is a day you might want to add here. Select Add Exclusion and type in 12/25. To delete a date, you select Delete Exclusion and type in the date you want to remove. After an exclusion date is added it appears in the brackets at the bottom of the menu. Up to fifteen dates can be entered to be excluded.

Serial Handshaking Alarm Settings

Serial Handshaking Alarms allows the SiteBoss to monitor each of its serial ports and alert you

if the DTR signal from the connected device drops low. This would be an indicator that the connected device has failed, the cable between the SiteBoss and the device has been disconnected, or a number of other reasons depending on the device. It can also alert you when the DTR signal goes high again.

The menu will list all available serial ports that could be configured for serial handshaking monitoring. Selecting one of the options brings up a submenu as shown below.

```
SiteBoss 550 - I/O 1 Serial Handshaking Alarms
A) Serial Handshaking Low Alarm Enable  [OFF]
B) Serial Handshaking Low Alarm Actions []
C) Serial Handshaking Low Alarm Message [Handshake Low]
D) Serial Handshaking Low Alarm Class   [Info]
E) Serial Handshaking Low Trap Number   [510]
F) Serial Handshaking High Alarm Enable [OFF]
G) Serial Handshaking High Alarm Actions[]
H) Serial Handshaking High Alarm Message[Handshake High]
I) Serial Handshaking High Alarm Class  [Info]
J) Serial Handshaking High Trap Number  [510]
```

Serial Handshaking Low / High Alarm Enable

These are ON/OFF toggles to enable alarming on high or low handshaking levels. The default settings are OFF.

Serial Handshaking Low / High Alarm Actions

These options display the Action List, a menu where the action string for the alarm is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions LIst for more information.

Serial Handshaking Low / High Alarm Message

These fields are used to set the messages to be sent with any text-based action for this event. The default setting is ?Handshake Low/High?. The maximum length for each is 126 characters.

Serial Handshaking Low / High Alarm Class

These options set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this event.

Serial Handshaking Low / High Trap Number

Set the number to be sent with any SNMP traps for this event. Default is 510, but trap number can also be set in the range of 1000 ? 1199 as needed

CPE Alarm Settings

This menu is used for configuring Customer Premises Equipment (CPE) monitoring functions. Configure the equipment to monitor under Network Settings/CPE Settings. Contact Asentria Tech Support for more information.

This functionality is called Ping Alarms in the Web Interface.

```
SiteBoss 350 - CPE Alarm Settings
A) Alarm Enable                         [OFF]
B) Alarm Actions                        []
C) Alarm Trap Number                    [511]
D) Alarm Class                          [Info]
E) Return to Normal Actions             []
F) Return to Normal Trap Number         [511]
G) Return to Normal Class               [Info]
```

Alarm Enable
This is an ON/OFF toggle to enable the CPE Down Event. The default setting is OFF.

Alarm Actions / Return to Normal Actions
Choosing one of these options will display the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Actions List for more information.

Alarm Trap Number / Return to Normal Trap Number
These options set the number to be sent with any SNMP traps for this event. The default is 511, but the trap number can also be set in the range of 1000 ? 1199 as needed.

Alarm Class / Return to Normal Class
These options are used to set the class for the alarm. When one of these options is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this alarm.

Reset Event Settings

The Reset Event Settings are used to configure event actions to be performed after the unit has been restarted. These actions would be executed regardless of whether the unit was reset via a restart command or by power cycling.

```
SiteBoss 550 - Reset Event Settings
A) Enable Event                         [OFF]
B) Event Actions                        []
C) Event Message                        [Reset Event]
D) Event Class                          [Info]
E) Event Trap Number                    [543]
F) Delay After Reset (seconds)          [0]
```

Event Actions
Choosing this option displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to the Actions List for more information.

Event Message
Set the text string to be delivered with this event?s action. The default setting is "Reset Event". The maximum length is 80 characters.

Event Class
Set the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed. Select one to be assigned to this event. The default is Info.

Event Trap Number
Set the number to be sent with any SNMP traps for this event. The default is 543, but the trap number can also be set in the range of 1000 ? 1199 as needed.

Delay After Reset (seconds)
Enter the number of seconds to wait after unit finishes booting before executing the Event Action(s) that have been set for this event. The default is 0, maximum is 3600 (1 hour).

General Event Settings
This menu permits customization of the event messages that appear in event notifications.

```
SiteBoss 550 - General Event Settings
A) Include Date and Time                    [ON]
B) Include Site Name                        [ON]
C) Include Sensor ID                        [ON]
D) Include User Defined Name                [ON]
E) Include User Defined State               [ON]
F) Include Event Class                      [OFF]
G) Action Delivery Mode                     [CONCURRENT]
```

Include Date and Time / Site Name / Sensor ID / User Defined Name / User Defined State / Event Class
Each option is an ON/OFF toggle to permit customization of the event message that appears in SNMP traps, Emails and SMS messages sent by the SiteBoss. The default setting for each is ON except for Include Event Class which is OFF.

Action Delivery Mode
This toggles between CHRONOLOGICAL and CONCURRENT. The CONCURRENT configures the unit to process multiple event actions immediately, regardless of whether previous actions have been completed or not. CHRONOLOGICAL configures the SiteBoss to process event actions in the order in which they occur, so that one action does not get processed until the previous action is completed. The default is CONCURRENT.

Global Event Settings
The Global Actions feature enables an administrator to configure actions that are automatically appended to any other action list when that other action list executes. If all actions for all events on a unit are to be the same then using global actions and trap number means easier management.

An action called "NONGLOBAL" can be inserted at the beginning of any event's action list to mean that any global actions and global trap number should not apply to that event. If the NONGLOBAL action is inserted in the action list, it must be inserted first in order to unambiguously tell the unit that actions to process should be excepted from global treatment.

See the Global Actions Feature Guide for more information.

```
SiteBoss 550 - Global Event Settings
A) Global Actions                       []
B) Global Trap Number                   [0]
```

Global Actions
Global Actions are used to set the default event actions that will be performed by all events that do not include the "nonglobal" action at the BEGINNING of the actions string.

Global Trap Number
Set the default SNMP Trap number that will be used by all events that do not include another, individually defined SNMP Trap number. Setting this value to 0 disables the effect. The default setting is 0.

Telemetry Settings

The telemetry table is a table of things to monitor on the unit for which telemetry is made available to other features on the same unit such as DNP3. DNP3 motivated the initial contents of the table, but it also has content for other non-DNP3 functionality. The entire telemetry table is configured via Settings Keys. Each row in the table is called a point. The SiteBoss supports 256 telemetry points.

All telemetry table settings are located in the `event.point` setting key branch. Each row in the table is a "point". This point nomenclature is inherited from the DNP3 point definition where a point is an "instance of a point type". A point type is a "classification for entities having a common set of characteristics and attributes. Examples include binary inputs, analog inputs ...." Asentria adds other metadata to the point entity to support other non-DNP3 telemetry management methods.

Setting Keys:

`? d autoconf`
Automatically populates the unit's Telemetry Table with all EventSensors (non-auxiliary sensors only).

`? d autoconf-enabled`
Automatically populate the unit's Telemetry Table with enabled EventSensors (enabled non-auxiliary only).

»Note: that the deadbands for any analog inputs are automatically populated to be 3.0. When you configure the telemetry table, regardless of whether you use the autoconf feature, you should manually configure DNP3 deadbands appropriate to the sensor telemetry (event.point[].deadband).

```
SiteBoss 550 - Telemetry Settings
A) Telemetry Points 1-16
...
```

```
P) Telemetry Points 241-256

Enter your Selection: A


SiteBoss 550 - Telemetry Settings
A) Point 1                          []
...
P) Point 16                         []

Enter your Selection: A


SiteBoss 550 - Telemetry Point 1 Settings
A) Name                             []
B) Key                              []
C) Type                             [NONE]
D) Class                            [NONE]
E) Deadband                         []
F) Shortcode                        []
```

Name
This text field is for informational purpose only.

Key
Key name of telemetry to monitor. Typically, this key name is for an EventSensor value, but most keys on the unit can be used here. E.g., scripting variable keys. Servicing telemetry for a point requires this setting configured.

Type
DNP3 point type. DNP3 specifies 5 point types: BINARY INPUT,ANALOG INPUT,COUNTER INPUT,BINARY OUTPUT,ANALOG OUTPUT. The unit supports all types except COUNTER INPUT and ANALOG OUTPUT. By default a point has no type (NONE). Servicing telemetry for a point requires this setting configured.

Class
DNP3 point class (0, 1, 2, 3, or NONE). Point classes govern from which points DNP3 events can be generated. DNP3 events can be packed in DNP3 Unsolicited Responses, which are analogous to autonomous (instead of polled) telemetry reporting. This is analogous to SNMP Trap vs SNMP Get. Servicing DNP3 unsolicited reporting for a point requires this setting configured to 1, 2, or 3.

Deadband
Value by which the telemetry value must change in order for a DNP3 event to be generated, if the point class is 1, 2, or 3. (This is a DNP3 rule.) The deadband is default blank (meaning no deadband, or a deadband of essentially 0 for ANALOG INPUT point types. Regardless of how the configure the telemetry table (manually or via DNP3 autoconf), you should configure an appropriate deadband for each point.

Shortcode
Reserved for future use.

DNP3 Command Set

These commands can be entered at the Command Prompt.

Command	Description	Usage	Purpose
? D STATUS	DNP3 Outstation Status	?D OR ?D STATUS	DNP3 outstation status report for current connections. If no connections are active then the port merely states how many DNP3 events are currently buffered (awaiting delivery to a master).
? D REPEAT STATUS	DNP3 Repeat Status	?D REPEAT STATUS	DNP3 outstation status report for current connections.
? D [REPEAT] STATUS-LOG	DNP3 Outstation Status w/log	? D [REPEAT] STATUS-LOG	DNP3 outstation status report that includes the 100 most recent interesting protocol transactions and any errors. If "repeat" is supplied then the report repeatedly updates.
? D [REPEAT] STATUS-HISTORY	DNP3 Status with current and historical connections	? D [REPEAT] STATUS-HISTORY	DNP3 outstation status report that includes current connections as well as up to 5 of the most recent closed connections.
? D [REPEAT] STATUS-FULL	Full DNP3 Status report	? D [REPEAT] STATUS-FULL	DNP3 outstation status report that includes current connections, the logs for them, as well as up to 5 of the most recent closed connections, and the logs for them.
? D SUPPORT	Create a	? D SUPPORT	Create support file

	support file		which can subsequently be packed into a log archive for offline troubleshooting analysis.
? D AUTOCONF	Auto-populate Telemetry Table	? D AUTOCONF	Automatically populate the unit's Telemetry Table with all EventSensors (non-auxiliary sensors only).
? D AUTOCONF-ENABLED	Auto-populate Telemetry Table, Enabled sensors only	? D AUTOCONF-ENABLED	Automatically populate the unit's Telemetry Table with enabled EventSensors (enabled non-auxiliary only).
? D AUTOCLEAR	Clear the Telemetry Table	? D AUTOCLEAR	Automatically default the unit's Telemetry Table to original factory settings.
? D DPD	XML DNP3 Device Profile Document	? D DPD	Generate the XML DNP3 DPD (Device Profile Document) according to the unit's current DNP3 configuration. This is a machine-readable and more current instance of the human-readable DPD.

Action Definitions Menu

This menu is where you configure all of the actions possible when events are detected.

```
SiteBoss 550 - Actions Definition Menu
A) Hostnames/IP Addresses              []
```

```
B) Email Addresses                    []
C) Phone Number 1                     []
D) Phone Number 2                     []
E) Phone Number 3                     []
F) Phone Number 4                     []
G) Pager Number 1                     []
H) Pager Number 2                     []
I) Pager Number 3                     []
J) Pager Number 4                     []
K) Action Settings
```

Hostname/IP Addresses

This menu option opens a submenu to configure up to twelve hostname/IP addresses to use for easier reference in event actions. The number (1,2,3) corresponds to the ?index? number for Traps as discussed in the Action List section. These can be any relevant server, such as an SNMP management system.

Email Addresses

This option opens a submenu to configure up to six Email Addresses to use for easier reference in event actions. These email addresses can also be set to cell phone numbers, using the service provider's SMS gateway address, to allow for SMS alerts to be sent. Ex: 2065555555@vtext.com. The number (1, 2, 3, etc.) corresponds to the ?index? number for Email alerts as discussed in the Actions List section.

Phone Number n

Select these options to set the phone numbers (index 1,2,3,4) to call for each dispatch, malert, modem callout or SMS event message as discussed in the Actions List chapter.

Pager Number n

Select these options to configure up to 4 Pager Numbers to use for easier reference in event actions as discussed in the Actions List.

Action Settings

This menu is used to configure various general action parameters, such as action schedules and event reminder intervals.

Pager Number *n*

```
SiteBoss 550 - Pager 1 Settings
A) Pager Type                         [NUMERIC]
B) Pager Callout Number               []
C) Pager ID                           []
D) Numeric Message                    []
E) Post Callout Delay (seconds)       [15]
F) Post ID Delay (seconds)            [5]
```

Pager Type

This option toggles between NUMERIC and ALPHA to select the type of pager to call. The default is NUMERIC.

Pager Callout Number

This field sets the phone number for the pager.

Pager ID
This ID is used only with paging systems where many pagers share the same phone number. This is common with alphanumeric pagers.

Numeric Message
This field is the series of digits (typically callback number) sent to a numeric pager.

Post Callout Delay
This option is the number of seconds the unit will wait before sending the pager ID. The default is 15 seconds.

Post ID Delay
This option sets the number of seconds the unit will wait before sending any message data. The default is 5 seconds.

Action Settings

These general actions settings that would apply for all applicable sensor event actions.

```
SiteBoss 550 - Action Settings
A) Callout Attempts                          [5]
B) Callout Delay (seconds)                   [60]
C) Action Schedule                           [OFF]
D) Reminder Interval (minutes)               [120]
E) Asentria Alarm Version                    [1.1]
F) Require Asentria Alarm ACKs               [OFF]
```

Callout Attempts
This option sets the total number of times to attempt dispatch, Malert or modem callouts if previous attempts fail. The default setting is 5.

Callout Delay
This sets the time in seconds (0 - 400) to wait between callout attempts. The default setting is 60 seconds.

Action Schedule
This option displays the Action Schedule Settings menu where actions can be limited to defined days and times.

Reminder Interval
This option sets the time in minutes (0 ? 65535) at which an action is repeated if the sensor (contact closure, temperature, humidity, or voltage) that triggered the alarm is still in the ?active? state. When the sensor has been returned to the inactive state, the reminder interval is no longer in effect. The default setting is 120 minutes.

Asentria Alarm Version
This toggles between 1.0 and 1.1 to indicate which type of Asentria Alarm notification will be displayed. Set this 1.0 for the dialup POTS modem. Set it at 1.1 for TCP when using other delivery methods for your alarm actions. The default setting is 1.1

Require Asentria Alarm ACKs

This is an ON/OFF toggle to enable or disable forcing the unit to require an acknowledgment when first connecting, and after each Asentria Alarm. If disabled, the SiteBoss will allow non-CRC mode where Asentria Alarms are delivered without waiting for any indication that the messages were properly delivered. If enabled, CRC mode is required by the SiteBoss. The default setting is OFF.

Action Schedule

The Action Schedule Settings menu allows event actions to be limited to defined days and times. If the Schedule is not Enabled the rest of the settings will not be active in the SiteBoss.

```
SiteBoss 550 - Action Schedule Settings
A) Action Schedule Enable              [OFF]
B) Begin Time                          [08:00]
C) End Time                            [17:00]
D) Weekdays Only                       [ON]
```

Actions Schedule Enable

This ON/OFF toggle enables/disables the action schedule. The default setting is OFF.

Begin Time / End Time

These fields set the beginning and ending times (24 hour clock) during which alarm actions can be taken. The default settings are 08:00 (Begin Time) and 17:00 (End Time).

Weekdays Only

This ON/OFF toggle is used to set whether actions are only performed Monday thru Friday. The default setting is ON.

General Settings

The General Settings option displays a menu where you can set the site name, answer string, confirmation prompt, date/time, and other general settings. This is also where the Job Scheduling Settings and Generator Settings are located in the Command Line Interface.

```
SiteBoss 550 - General Settings
A) Site Name                           [550-550002904]
B) Answer String                       [SiteBoss]
C) Escape Key                          [27]
D) Confirmation Prompt                 [ON]
E) Time Stamp Format                   [HH:MM]
F) Date Stamp Format                   [MM/DD]
G) Space After Date/Time Stamp         [ON]
H) Prompt                              [>]
I) Date/Time Setup
J) Joinable Pass-through               [ON]
K) Job Scheduling Settings
L) Generator Settings
```

Site Name

This field sets the name assigned to this SiteBoss. This name is included with alarm messages (Traps, Emails, etc.) and is displayed at the top of the Status screen. The name should be unique for clarity. The maximum length is 40 characters. The default setting is "S550 - <"serial number">"

Answer String
This option sets the string that is presented when a user connects to the SiteBoss via Telnet or modem. The maximum length 31 is characters. The default setting is SiteBoss.

Escape Key
This option is used to set the decimal ASCII character code of the key you must press three times to escape from pass-through or other transparent modes. The default is 27, the <ESC> key.

Confirmation Prompt
This is an ON/OFF toggle to set whether a confirmation prompt (`Are you sure (y/n)?`) is displayed when the commands **`DEFAULT`** or **`COLDSTART`** are issued, and when clearing the settings for an EventSensor in the EventSensor Setup menu. If there is no response within 30 seconds, the SiteBoss will cancel the command. The default setting is ON.

Time Stamp Format
This menu option toggles through three options for how time stamps are formatted: HH:MM, HH:MM:SS, or BLANK. The default setting is HH:MM.

Date Stamp Format
This selection toggles through four options for how date stamps are formatted: MM/DD, MM/DD/YY, MM/DD/YYYY, or BLANK. The default setting is MM/DD.

Space After Date/Time Stamp
This is an ON/OFF toggle to set whether a space is appended to the end of the Date/Time stamp. The default setting is ON.

Prompt
The Prompt option sets the character(s) or settings values displayed as the command line prompt. The prompt characters can be customized, and includes the ability to embed one or more settings values in the prompt, for example the site name could be used in the prompt using a settings key of **`sys.sitename`**. A customized command prompt can help simplify administration of units, particularly where multiple units are involved.

The Prompt can be set as plain text characters or if using a settings key the syntax is: $(setting_key_name). If the setting key is not accessible for any reason (invalid key, insufficient user access level, etc.), "ERROR" is displayed instead.

The setting can contain up to 64 characters, but the prompt itself is limited to 30 characters. The default is >.

Date/Time Setup
This selection displays the System Date/Time menu where you can manage the clock, daylight savings control, and configure a networked time server.

Joinable Pass-through

This is an ON/OFF toggle to allow or disallow multiple user pass-through sessions. ON allows more than one user to connect on a pass-through session. OFF does not allow more than one concurrent pass-through session, and those attempting to join after the first user is connected will receive a "port in use" error message. The default setting is ON.

Job Scheduling Settings

Choosing this option displays the Job Schedule menu where up to 8 schedules can be configured for starting "jobs" that are scheduled to be run automatically. These schedules include date and start time, but also settings for repeating those schedules on a daily, weekly, monthly, or yearly basis. Job schedules are used for Generator Exercising and can be used by customer scripts.

Generator Settings

The Generator Settings option displays the Generator Settings menu where general settings can be configured for an attached generator, as well as settings for automatically exercising that generator according to a pre-configured job schedule.

Date/Time Setup

This menu displays the System Date/Time menu where you can manage the clock, daylight savings control, and configure a networked time server.

```
SiteBoss 550 - System Date/Time
A) Current Date                         [08/17/2015]
B) Current Time                         [14:44:20]
C) Adjust for Daylight Savings          [ON]
D) GMT Difference (hours)               [8]
E) GMT Difference Direction             [BEHIND]
F) Enable Time Protocol                 [OFF]
G) Time Servers
```

Current Date

The date can be manually set. The unit automatically calculates the day of the week to display on the Status screen.

Current Time

The time of day can be manually set (24 hour clock).

»Note: The date and time settings are maintained by means of an internal battery backup when power is removed from the SiteBoss.

Adjust for Daylight Savings

This is an ON/OFF toggle that allows automatic daylight savings time updating in the US.

»Note: On the second Sunday in March, clocks are set ahead one hour at 2:00 a.m. local standard time, which becomes 3:00 a.m. local daylight time. On the first Sunday in November, clocks are set back one hour at 2:00 a.m. local daylight time, which becomes 1:00 a.m. local standard time.

GMT Difference (hours)

Set the number of hours the current time zone is offset from GMT. Valid input ranges from 0 to 12. The default setting is 8 hours.

GMT Difference Direction

Set whether you are east (AHEAD) or west (BEHIND) of GMT. For example, Pacific Time (GMT-8) is behind, and Tokyo time (GMT +9) is ahead. The default setting is BEHIND.

Enable Time Protocol

This option toggles between OFF, SIMPLE, and NTP. The default setting is OFF.

- SIMPLE - When network time is set to SIMPLE the unit attempts to contact the configured time servers (see Time Servers setting below) periodically, attempting to query each using Simple Network Time Protocol (SNTP), Time, and Daytime protocols, in that order. Once a response is received for any protocol, the unit sets the system clock to the new time, updates the real time hardware clock (RTC), then the network time process dies. The interval for checking network time is hard-coded to 12 hours plus or minus a random several hours.

- NTP - When network time is set to Network Time Protocol (NTP), the NTP daemon is kept running at all times. Unlike the SIMPLE setting, with NTP the clock is not immediately set as soon as a time server is contacted. Rather, the NTP daemon utilizes various algorithms to set the time in an accurate and robust manner. Since the NTP daemon updates the system time asynchronously, the current time is stored in the RTC every 30 minutes while it is running. Note that if you change the clock manually, it may be a period of an hour or more before NTP resets it.

Time Servers

This selection will display a menu where the hostname or IP address of six time-servers can be configured (maximum length 64 characters). The SiteBoss uses the following servers by default:

```
SiteBoss 550 - Time Servers
A) Server 1                          []
B) Server 2                          [time.nist.gov]
C) Server 3                          [216.171.120.36]
D) Server 4                          [64.90.182.55]
E) Server 5                          []
F) Server 6                          []
```

NTP log

Implementation Notes

1. NTP logging is controlled by the setting **`sys.time.net.ntp.log.enable`** which can be ON or OFF. When ON, NTP logs data to /tmp/ntp.log, and the log can be accessed via the "**ntplog**" command. When OFF, log data only goes into the syslog files, and /tmp/ntp.log is deleted if present. This setting is OFF by default.

2. When enabled, the log file is limited to 128KB in size; once this size is reached, approximately the first 25% of the file is deleted (on a line boundary).

3. Due to the way NTP works, sometimes it takes a while for anything to show up in the log. Be patient. If you just can't wait, try rebooting the unit (not just restart).

4. The NTP log is volatile; if you reboot the box (not restart), it will start over.

Job Scheduling Settings

The SiteBoss can be configured for starting up to 8 jobs scheduled to run automatically. These schedules include start dates and times, and settings for repeating those schedules on a daily, weekly, monthly, or yearly basis.

The Schedule Number is used when configuring Generator Exercising functions in the Generator Exercising Settings menu. It can also be used with LUA Scripts to configure SiteBoss actions on a regular schedule.

```
SiteBoss 550 - Job Scheduling Settings
A) Schedule 1
. . .
H) Schedule 8

Enter your Selection: A


SiteBoss 340 - Schedule 1 Settings
A) Enable                              [OFF]
B) Start                               [01/01/2012 14:00:00]
C) Repeat Settings                     [NONE]
```

Enable

This is an ON/OFF toggle to turn on this particular Job Schedule. The default setting is OFF.

Start

Set the date (mm/dd/yyyy) and time (hh:mm:ss) for this scheduled event to start.

Repeat Settings

This option displays a menu where specific settings regarding the repetition of the Job Schedule can be configured.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                         [NONE]
B) End Mode                            [NEVER]
C) End After                           [1]
D) End On                              []
```

Repeat Mode

This selection toggles through five options for configuring the repeat actions for the Job Schedule: NONE, DAILY, WEEKLY, MONTHLY, YEARLY. Each option displays a unique

menu for configuring that type of repeat setting. The default setting is NONE.

Repeat Mode ? NONE

If the Repeat Mode is set to NONE, then none of the other options in this menu apply. The action does not repeat.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                          [NONE]
B) End Mode                             [NEVER]
C) End After                            [1]
D) End On                               []
```

Repeat Mode ? DAILY

Repeat Mode DAILY allows the user to schedule the job to run once during a 24 hour period and then have that job repeated some number of days later. Additional options are provided for when the repeat mode for this Job Schedule will end.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                          [DAILY]
B) Repeat Every n Days                  [1]
C) End Mode                             [NEVER]
D) End After                            [1]
E) End On                               []
```

Repeat Every n Days

This field is for setting how many days until this Job repeats. Values are 1 ? 400. The default setting is 1 (daily).

{{header-settingslEnd Mode} This selection toggles through three options for: NEVER, AFTER, and ON DATE.

- NEVER ? means this Job Schedule never ends. It will repeat Every n Days.
- AFTER ? means this Job Schedule ends after being repeated a certain number of times.
- ON DATE ? means this Job Schedule ends after a specific date and time.

End After

Set the number of times this job will be repeated. This setting is only valid when End Mode is set to AFTER. Values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

End On

Set the date (mm/dd/yyyy) and time (hh:mm:ss) for the repeat mode to end. This setting is only

valid when End Mode is set to ON DATE. The default is blank which means no end date.

Repeat Mode ? WEEKLY

Repeat Mode WEEKLY allows the user to schedule the job for a specific day(s) during the week and then have that job repeated the same day(s) scheduled in future weeks. Additional options are provided for when the repeat mode for this Job Schedule will end.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                          [WEEKLY]
B) Repeat Every n Weeks                 [1]
C) On Sunday                            [OFF]
D) On Monday                            [OFF]
E) On Tuesday                           [ON]
F) On Wednesday                         [OFF]
G) On Thursday                          [OFF]
H) On Friday                            [OFF]
I) On Saturday                          [OFF]
J) End Mode                             [NEVER]
K) End After                            [1]
L) End On                               []
```

Repeat Every n Weeks

Set how often this Job Schedule will repeat. For the weekly setting, the inputted figure represents how many weeks until this job will repeat. Values are 1 ? 255. The default setting is 1 (weekly).

On Sunday thru On Saturday

These are ON/OFF toggles for each day. ON means this Job Schedule will be repeated on that day each week that this job is scheduled for. OFF means this Job Schedule does not get run on that day. The default for all is OFF, except for Tuesday which is ON.

End Mode

This selection toggles through three options for: NEVER, AFTER, and ON DATE.

- NEVER ? means this Job Schedule never ends.
- AFTER ? means this Job Schedule ends after being repeated a certain number of times.
- ON DATE ? means this Job Schedule ends after a specific date and time.

End After

Set the number of times this job will be repeated. This setting is only valid when End Mode is set to AFTER. Values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

End On

Set the date (mm/dd/yyyy) and time (hh:mm:ss) for the repeat mode to end. This setting is only valid when End Mode is set to ON DATE. The default is blank which means no end date.

Repeat Mode ? MONTHLY

Repeat Mode MONTHLY allows the user to schedule the job for a specific day of the month and then have that job repeated the same day scheduled for future months. Additional options are provided for when the repeat mode for this Job Schedule will end.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                          [MONTHLY]
B) Repeat Every n Months                [1]
C) Monthly Repeating Mode               [EACH]
D) Each Date                            [1]
E) On The                               [FIRST]
F) On Day                               [TUESDAY]
G) End Mode                             [NEVER]
H) End After                            [1]
I) End On                               []
```

Repeat Every n Months

Set how often this Job Schedule will repeat. For Monthly, this means every n months after it is started, this job will repeat. Values are 1 ? 255. The default setting is 1 (monthly).

Monthly Repeating Mode

This selection toggles between EACH and ON THE.

- EACH ? means the schedule runs on specific dates of the month.
- ON THE ? means the schedule runs on calculated dates of the month according to which day that month starts.

Each Date

The Each Date allows the user to set a comma-separated list of dates during a month on which this schedule will run. This setting is only valid when the Monthly Repeating Mode is set to EACH. The default setting is 1.

On The** and **On Day

These fields are configured together to provide a precise day of the week on which this Job Schedule will be run. These settings are only valid when the Monthly Repeating Mode is set to ON THE.

- ON THE ? toggles through FIRST, SECOND, THIRD, FOURTH and LAST to indicate on which day of the month this schedule will run. The default setting is FIRST.
- ON DAY ? toggles through DAY, WEEKDAY, WEEKEND DAY, SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY and SATURDAY to indicate the day of the week on which this schedule will run. The default setting is TUESDAY. (The defaults mean 1st Tuesday of the month, if the repeat mode is set to ON THE)

End Mode

This selection toggles through three options for: NEVER, AFTER, and ON DATE.

- NEVER ? means this Job Schedule never ends. It will repeat as scheduled.
- AFTER ? means this Job Schedule ends after being repeated a certain number of times.
- ON DATE ? means this Job Schedule ends after a specific date and time.

End After
This selection sets the number of times this job will be repeated. This setting is only valid when End Mode is set to AFTER. Values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

End On
This selection sets the date (mm/dd/yyyy) and time (hh:mm:ss) for the repeat mode to end. This setting is only valid when End Mode is set to ON DATE. The default is blank which means no end date.

Repeat Mode ? YEARLY

Repeat Mode YEARLY allows the user to schedule the job for a specific day of the month and then have that job repeated the same day during specific months throughout the year, and maintain that schedule for a specific number of years. Additional options are provided for when the repeat mode for this Job Schedule will end.

```
SiteBoss 550 - Repeat Settings
A) Repeat Mode                          [YEARLY]
B) Repeat Every n Year(s)               [1]
C) In January                           [OFF]
D) In February                          [OFF]
E) In March                             [OFF]
F) In April                             [OFF]
G) In May                               [OFF]
H) In June                              [OFF]
I) In July                              [OFF]
J) In August                            [OFF]
K) In September                         [OFF]
L) In October                           [OFF]
M) In November                          [OFF]
N) In December                          [OFF]
O) On The                               [FIRST]
P) On Day                               [TUESDAY]
Q) End Mode                             [NEVER]
R) End After                            [1]
S) End On                               []
```

Repeat Every n Years
Set how often this Job Schedule will repeat. For Yearly, this means every n years after it is started, this job will repeat. Values are 1 ? 255. The default setting is 1 (yearly).

In January *thru* ***In December***
This is an ON/OFF toggle for each month of the year. ON means this Job Schedule will be repeated on a specific day that month. OFF means this Job Schedule does not get run on that day. The default for all is OFF

On The *and* ***On Day***
These fields are configured together to designate a precise day on which this Job Schedule is to be run.

- ON THE ? toggles through FIRST, SECOND, THIRD, FOURTH and LAST to indicate on which day of the month this schedule will run. The default setting is FIRST.
- ON DAY ? toggles through DAY, WEEKDAY, WEEKEND DAY, SUNDAY, MONDAY,

TUESDAY, WEDNESDAY, THURSDAY, FRIDAY and SATURDAY to indicate the day of the week on which this schedule will run. The default setting is TUESDAY.

End Mode
This selection toggles through three options for: NEVER, AFTER, and ON DATE.

- NEVER ? means this Job Schedule never ends. It will repeat continuously as scheduled.
- AFTER ? means this Job Schedule ends after being repeated a certain number of times.
- ON DATE ? means this Job Schedule ends after a specific date and time.

End After
Set the number of times this job should be repeated. This setting is only valid when End Mode is set to AFTER. Values are 1 ? 1000. The default setting is 1, which means the Job Schedule runs once with no repetition.

End On
Set the date (mm/dd/yyyy) and time (hh:mm:ss) for the repeat mode to end. This setting is only valid when End Mode is set to ON DATE. The default is blank which means no end date.

Generator Settings

The following is a top level overview of generator related settings. For more detailed configuration and use instructions please see the Generator Control Feature Guide.

Setting Key
This settings key can only be used on the Command Line interface. It has no Web Interface equivalent.

Setting Key:
`gen.run.force`
This is a status key which, when written to any non-zero integer value, makes the function behave as if the schedule for it just fired. Reading it just returns 0.

Generator Status: SK ? GEN

```
SiteBoss 550 - Generator Settings
A) General Generator Settings
B) Generator Exercising Settings
```

General Generator Settings
This selection displays a menu where the specific generator settings can be configured.

Generator Exercising Settings
This selection displays a menu to configure the settings for exercising the generator per a specific job schedule.

General Generator Settings

Use this menu option to set specific generator settings

```
SiteBoss 550 - General Generator Settings
A) Enable                              [OFF]
B) Generator Starting Settings
C) Generator Running Detection Settings
```

Enable

This is an ON/OFF toggle to enable generator set management. The default setting is OFF.

Generator Starting Settings

This selection displays a menu to define the Generator Starting relay point.

Generator Running Detection Settings

This selection displays a menu to identify the exact monitoring point to which the generator is connected.

Generator Starting Settings

This menu function is for defining the Generator Starting relay point. Up to two relays can be configured to activate simultaneously.

```
SiteBoss 550 - Generator Starting Settings
A) Mode                                [RELAY]
B) Relay 1 Starting Enable             [ON]
C) Relay 1 EventSensor                 [14]
D) Relay 1 Point                       [1]
E) Relay 1 Starting State              [Active]
F) Relay 2 Starting Enable             [OFF]
G) Relay 2 EventSensor                 [200]
H) Relay 2 Point                       [1]
I) Relay 2 Starting State              [Inactive]
J) Script Name                         []
K) Script Arguments for Ignition       []
L) Script Arguments for Shutdown       []
```

Mode

This option toggles between RELAY and SCRIPT. This setting controls by what mechanism the generator is started and stopped. The default is RELAY.

Relay n Starting Enable

These are ON/OFF toggles to enable the relay for generator exercising. Some generators require two relays to start. The default is ON for Relay 1 and OFF for Relay 2.

Relay n EventSensor

These options toggle through all available EventSensor options. They set the slot number of the EventSensor that has the relay which starts the generator. Values are 1 ? 16, and 200 (internal). The default settings are 200.

Relay n Point
These options set the number of the relay point on that EventSensor. Values are 1 ? 12. The default setting is 1.

Relay n Starting State
These options toggle between Active/Inactive to set which relay state corresponds with the generator running. The default setting for both is Inactive.

Script Name
This is the name of the script that controls the generator.

Script Arguments for Ignition
Input the arguments to pass to the script to tell it to start the generator.

Script Arguments for Shutdown
Input the arguments to pass to the script to tell it to stop the generator.

Generator Running Detection Settings
This menu is used to setup the Generator Running Detection settings.

```
SiteBoss 550 - Generator Running Detection Settings
A) Enable                              [OFF]
B) CC EventSensor                      [200]
C) CC Point                            [1]
D) Running CC State                    [Open]
E) Delay (seconds)                     [90]
```

Enable
This is an ON/OFF toggle that enables the detection of whether the generator is really running or not. The default setting is OFF.

CC Event Sensor
This option set the slot number of the EventSensor that has the contact closure (CC) which is connected to the &quote;generator is running&quote; monitor. The default setting is 200.

CC Point
Set the number of the contact closure (CC) point on that EventSensor. The default setting is 1.

Running CC State
This option toggles between OPEN/CLOSED to set which physical state corresponds with the generator running. The default setting is Open.

Delay (seconds)
This field sets how long (in seconds) to wait for the generator to indicate itself as "running" after engaging the generator starting mechanism. This field is active only when generator running detection is enabled. When the generator has not started after this delay time, the unit disengages the starting mechanism and creates a Generator Non-Start Event. Available range is 0 ? 600 with the default at 90 seconds.

Generator Exercising Settings

This is the menu for configuring the settings for exercising the generator per a specific job schedule.

```
SiteBoss 550 - Generator Exercising Settings
A) Mode                                [OFF]
B) Schedule                            []
C) Duration (seconds)                  [1800]
D) Generator Non-start Event Settings
```

Mode

This option toggles between OFF, SCHEDULE and INHIBIT. The default setting is OFF.

- OFF ? means that the generator exercising function has been disabled.
- SCHEDULE ? means that generator exercising is being conducted via a Job Schedule.
- INHIBIT ? means that the Job Schedule is temporarily overridden.

Schedule

A string setting that references one or more Job Schedule(s) configured in the Job Schedule Settings menu. This is either blank for no schedule, a single number, or comma-delimited string of numbers from 1 to 8. The default setting is blank.

Duration (seconds)

The number of seconds that the generator will run either when started via a Job Schedule, or forced using a settings command. Values range from 600 seconds (10 minutes) ? 3600 seconds (1 hour). The default setting is 1800 (30 minutes).

Generator Non-start Event Settings

Choosing this option will display a sub-menu with settings for the notification(s) that will occur should the generator not start when it is supposed to.

```
SiteBoss 550 - Generator Non-start Event Settings
A) Event Enabled                       [OFF]
B) Event Actions                       []
C) Event Trap Number                   [536]
D) Event Class                         [Info]
```

Event Enabled

This is an ON/OFF toggle to enable the Generator Non-start Event. The default setting is OFF.

Event Actions

Choosing this option displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to the Action List for more information.

Event Trap Number

Set the number to be sent with any SNMP traps for this event. The default is 536, but the trap

number can also be set in the range of 1000 ? 1199 as needed.

Event Class
This sets the severity class for the event. When this option is selected, a list of the classes previously defined in the Class Table menu is displayed. The default is Info.

Event Log Settings

The Event Log is a record of all data events that occur within the SiteBoss.

The Event Log overwrites itself when it becomes full. ?Full? has meaning that you can control with the Maximum File Size setting. This setting controls the maximum size (in KB) to which the file should be limited. If the setting is 0 then the audit log?s only constraint on size will be the available physical memory.

```
SiteBoss 550 - Event Log Settings
A) List Events File
B) Clear Events File
C) Enable Events Log File                [ON]
D) maximum File Size                     [32]
E) Store Data Alarm Records              [OFF]
F) Store Sensor Events                   [OFF]
G) Date/Time Stamp Data Alarm Records    [ON]
H) Prepend Data Alarm Name               [ON]
```

List Events File
This option displays the contents of the Events File, if any records exist.

Clear Events File
This selection purges the records within the Events File. Records in the Events File are deleted immediately when this option is selected, so make sure you want to do this before selecting.

» Caution: All of the records in the Log File are deleted immediately when this option is selected.

Enable Events Log File
This is an ON/OFF toggle to enable Event logging. The default setting is ON.

Maximum File Size
This field will set the maximum number of KB the Event Log can reach before overwriting the oldest records. Available options are 0, 32, 64, 128, 256, 512 and 1024. The default setting is 64.

Store Data Alarm Records
This option is an ON/OFF toggle to enable storing data alarm records. The default setting is OFF.

Store Sensor Events
This is an ON/OFF toggle to enable storing records generated by environmental sensors. The default setting is ON.

Date/Time Stamp Data Alarm Records
This is an ON/OFF toggle to prepend a Date/Time stamp to the beginning of data alarm records. The default setting is ON.

Prepend Data Alarm Name
is an ON/OFF toggle to prepend the name of the Data Alarm to the beginning of the data alarm record. This aids in identifying which Data Alarm an alarm record is associated with. The default setting is ON.

Audit Log Settings

The Audit Log is a record of a variety of actions that occur within the SiteBoss. The File is accessed and controlled under the same policies which govern how you would generally access buffered data. For example, you can have the audit log FTP-pushed.

The Audit Log overwrites itself when it becomes full. ?Full? has meaning that you can control with the Maximum File Size setting in the lower section of the page. This setting controls the maximum size (in KB) to which the file should be limited. If the setting is 0 then the audit log?s only constraint on size will be the available physical memory.

Certain actions are automatically written to the Audit Log anytime it is enabled. These actions are:

- When a user changes the configuration via a Setting Key
- When a user connects, disconnects, or transfers a file via the unit?s FTP server
- When a GPS positional fix is acquired or lost by the optional installed GPS card
- When the wireless modem connects or disconnects (due to failure in the latter case) from the wireless network

```
SiteBoss 550 - Audit Log Settings
A) List Audit Log File
B) Clear Audit Log File
C) Enable Audit Log File                [ON]
D) maximum File Size                    [32]
E) Store Reset Events                   [ON]
F) Store Command Entry                  [ON]
G) Store Relay Activity                 [ON]
H) Store Alarm Actions Taken            [ON]
I) Store Password Failures              [ON]
J) Store Logins/Disconnects             [ON]
K) Store Serial Handshaking Alarms      [ON]
L) Store Pass-through Activity          [ON]
M) Store Inactivity Timeouts            [ON]
N) Store Polling Activity               [ON]
```

List Audit Log File

This option displays the contents of the Audit Log file, if any records exist.

Clear Audit Log File

This selection purges the records within the Audit Log file. Records in the Audit Log File are deleted immediately when this option is selected, so make sure you want to do this before

selecting.

» Caution: All of the records in the Log File are deleted immediately when this option is selected.

Enable Audit Log File
This is an ON/OFF toggle to enable Audit logging. The default setting is ON.

Maximum File Size
This option is used to set the maximum number of KB the event log can reach before overwriting the oldest records. Available options are 0, 32, 64, 128, 256, 512, and 1024. If the setting is 0 then the audit log?s only constraint on size will be the available physical memory. The default setting is 128.

Store . . .
These remaining options are ON/OFF toggles to enable logging of the action described. The default setting for all is ON.

Scripting Settings
Scripting provides the ability to customize the operation of an Asentria device. Scripts are written in the Lua scripting language, with access to Asentria specific functionality via a rich set of library functions. Scripts can read or change any setting on the SiteBoss, and can also create custom settings that can be accessed via setting keys.

Utilizing Lua scripting on a SiteBoss can be a complex process. In order to assist in the implementation of custom Lua scripts, Asentria has created a Scripting Feature Guide on the Asentria Product Information Portal, which goes into further detail regarding the creation and usage of Lua scripts on a SiteBoss product.

```
SiteBoss 550 - Scripting Settings
A) Enable Scripting                    [OFF]
B) Clear Pending Records               [0]
C) DTR Override Ports
D) List Allocated Devices
E) List Scripts
F) Manage Script Files
```

Enable Scripting
This is an ON/OFF toggle that controls whether scripts are allowed to run on the unit at all.

» Note: If scripting is disabled, then scripts cannot be started either automatically or manually, and other scripting functionality such as record collection and DTR override will not happen regardless of the related settings.

» Note: If scripting is disabled while scripts are running, they will be issued the STOP command which could take up to 20 seconds to complete. If re-enabled, scripting will not function until after the previous scripting session is completely shut down (i.e. all scripts are stopped).

Clear Pending Records
This option will display the number of script records pending and when selected will clear them, setting the counter back to 0.

DTR Override Ports
This selection will display ON/OFF toggles for each port to specify IO port DTR handling to be under script control. Normally the state of the DTR output pin on the IO port 1 is kept high. If this this option is set to ON the DTR will stay low until a script changes it to the high state after a power-cycle or reset.

List Allocated Devices
This selection will display a list of I/O devices that are currently allocated to a running script.

List Scripts
This option displays a menu that lists of all of the 20 script entries. It will display the name, current state, and configured arguments. Selecting a script opens up a submenu with detailed settings and status for that script.

Manage Script Files
This option displays a menu which allows the user to manage script files.

List Scripts
This submenu lists the name, current state, and configured arguments. Selecting a script opens up a submenu with detailed settings and status for that script. Refer to the Scripting Feature Guide for a more complete description and usage instructions for the LUA scripts and the scripting menu options and functions.

```
SiteBoss 550 - Script List
   Name                              State       Arguments
A)                                   Disabled
. . .
T)                                   Disabled

SiteBoss 550 - Script 1 Settings
A) Enable                               [OFF]
B) Name                                 []
C) File Name                            []
D) Run Always                           [OFF]
E) Run At Startup                       [OFF]
F) Run At Scheduled Time                [OFF]
G) Repeat Interval (minutes)            [0]
H) Arguments                            []
I) Start Script Now
J) Stop Script Now
K) Detailed Status                      [Disabled]
```

Enable
This toggle enables/disables the script. If disabled, the script will not run on schedule and cannot be run manually.

Name
This field sets the name of script. This is the name that is used when referring to the script, and should not be confused with the name of the script file associated with the script.

File Name
The name of the script file associated with this script. The same script file can be used with any number of scripts.

Run Always
This is an ON/OFF toggle. If it is set to ON the script will start after the unit boots up, and the script will restart automatically if it stops for any reason.

Run At Startup
This is an ON/OFF toggle. If it is set to ON, the script will start after the unit boots up. If the script stops for any reason, it will not restart unless the unit itself is restarted.

Run At Scheduled Time
This will bring up menu options to set up a scheduled daily run time. There is an ON/OFF toggle to enable/disable the script to run at a specific time of day and a field to set the time each day for the script to run. Set field HH:MM.

```
SiteBoss 550 - Script 1 Scheduled Time
A) Run At Scheduled Time                [OFF]
B) Scheduled Time                       [00:00]
```

Repeat Interval (minutes)
If a non-zero value is entered, the script is run at the specified interval, measured from the last time the script was started on a schedule. The default is 0.

Arguments
The specified arguments are passed to the script when it is invoked on a schedule, manually from the setup menu, or via command interface commands SCRIPT START or SCRIPT TEST with no arguments specified. Prior to the script being run, the arguments are scanned for name=value pairs. For each one found, a global variable is created with that name and its value is set to the scanned value.

Start Script Now
This will start the script.

Stop Script Now
This will stop the script.

Detailed Status
The Detailed Status option displays the status of the script.

```
Current state: Not loaded
Name:
File Name:
Schedule: Manual
Arguments:
Open devices:
Last start time: <never>


Press a key to continue...]
```

Manage Script Files

This option displays a menu which allows the user to manage script files.

Refer to the Scripting Feature Guide for a more complete description and usage instructions for the LUA scripts and the scripting menu options and functions.

```
SiteBoss 550 - Manage Script Files
A) List Script Files
B) View Script File
C) Edit Script File
D) Delete Script File
E) Download Script File to Unit
F) Upload Script File From Unit
```

List Script Files

This option will displays a list of all script files contained on the unit. Equivalent to the SCRIPT DIR command.

View Script File

This option will display the list of loaded scripts to choose from and displays the contents of the selected script file. Equivalent to the SCRIPT SHOW [script name] command.

Edit Script File

This option will display the list of loaded scripts to choose and an option to enter a new file. Equivalent to the SCRIPT EDIT [script name] command.

» Note: To exit the text editor type :q!<enter>

Delete Script File

This option will display the list of loaded scripts to choose from and deletes the selected script file. Equivalent to the SCRIPT DELETE [script name] command.

Download Script File to Unit

This option transfers a script file to the unit. Equivalent to the SCRIPT GET command.

Upload Script File From Unit

This option transfers a script file from the unit. Equivalent to the SCRIPT PUT command.

Script Management Commands

These commands are used at the Command Interface prompt

Command	Usage	Purpose

SCRIPT	SCRIPT management commands list	SCRIPT [HELP]
SCRIPT LIST	SCRIPT LIST	Display a list of configured scripts
SCRIPT START	SCRIPT START <script> [<args>...]	Start a script
SCRIPT STATUS	SCRIPT STATUS <script>	Display detailed status of a script
SCRIPT STOP	SCRIPT STOP <script>	Stop a running script
SCRIPT RECORDS	SCRIPT RECORDS [CLEAR]	Show/clear pending script records
SCRIPT DEVICES	SCRIPT DEVICES	Show script device allocations
SCRIPT GET/PUT	SCRIPT GET/PUT <file> [<args>...]	Transfer script file to/from the unit
SCRIPT DELETE	SCRIPT DELETE <file>	Delete a script file
SCRIPT EDIT	SCRIPT EDIT <file>	Edit a script file (using VI editor)
SCRIPT DIR	SCRIPT DIR	List script file directory
SCRIPT SHOW	SCRIPT SHOW <file>	Display script file
SCRIPT TEST	SCRIPT TEST <script>	Enter interactive script interpreter

►Device Administration Via the CLI

Setting Keys

Setting Keys (SK) provide a flat file, human readable means of setting and retrieving settings within the unit. Setting Keys are commonly used to clone settings across multiple units or in automated processes. All of the settings that can be set using the Web Interface or the SETUP menu in the Command Interface can also be set using the Settings Key commands from the Command Prompt.

Setting Key is abbreviated when used on the command line as SK.

There are settings that can only be configured using a settings key command.

SK GET at the command prompt will list the Settings Keys on the SiteBoss. Use SK GET A for an ASCII list on your terminal emulator or X for Xmodem.

When downloading keys, if all settings referred to by a single key are the same, the unit will

give only one key, but specify the keyword "all" as the index (e.g., `event.data[all].enable=ON` means all data event alarms are enabled).

The unit always adds "end" at the end of downloading keys.

SK GET CUSTOM will list only the non-default settings. SK GET A CUSTOM for an ASCII output to the terminal emulator.

SK GET [PARTIAL KEY] to get a list of all keys of a partial setting type SK GET and part of the setting key and the unit will output all settings that begin with that settings syntax. For example, SK GET A `event.class` will output all event classes configured in the unit.

SK [KEY[=value]] from the command prompt allows for reading or setting a single Settings. If the value portion of the command is omitted, the SiteBoss will report back the value stored in that key. If the value is given, it will be stored in the key. Example: Typing `sk event.class[1]` at the command prompt will report back "Info". To set it as something else type `sk event.class[1]=TEST` and the unit will report back COMPLETE and that setting will now be set to TEST.

SK GET CUSTOM SCRIPT will list the non-default settings plus any scripts loaded on the SiteBoss.

SK HERE at the command prompt allows you to set or get individual keys interactively. Typing just the key name will cause the value to be displayed. Typing the key name plus a new value will set that key. The unit will keep prompting for a new key or key/value pair until you press <Esc> or <Enter>.

SK LOG displays a list of any errors generated during an SK Set.

SK <key>#: displays a list of the possible values of a key, for example:

```
>sk serial.1.baud#

300,600,1200,2400,4800,9600,19200,38400,57600,115200
```

There are settings that can only be configured using a settings key command.

Command Set

This table lists the Command Set for the SiteBoss. The commands are used at the command prompt in the Command Interface.

Command	Description	Usage	Purpose
? D STATUS	DNP3 Outstation Status	?D OR ?D STATUS	DNP3 outstation status report for current connections. If no connections are

			active then the port merely states how many DNP3 events are currently buffered (awaiting delivery to a master).
? D REPEAT STATUS	DNP3 Repeat Status	?D REPEAT STATUS	DNP3 outstation status report for current connections.
? D [REPEAT] STATUS-LOG	DNP3 Outstation Status w/log	? D [REPEAT] STATUS-LOG	DNP3 outstation status report that includes the 100 most recent interesting protocol transactions and any errors. If "repeat" is supplied then the report repeatedly updates.
? D [REPEAT] STATUS-HISTORY	DNP3 Status with current and historical connections	? D [REPEAT] STATUS-HISTORY	DNP3 outstation status report that includes current connections as well as up to 5 of the most recent closed connections.
? D [REPEAT] STATUS-FULL	Full DNP3 Status report	? D [REPEAT] STATUS-FULL	DNP3 outstation status report that includes current connections, the logs for them, as well as up to 5 of the most recent closed connections, and the logs for them.
? D SUPPORT	Create a support file	? D SUPPORT	Create support file which can subsequently be packed into a log archive for offline troubleshooting analysis.

? D AUTOCONF	Auto-populate Telemetry Table	? D AUTOCONF	Automatically populate the unit's Telemetry Table with all EventSensors (non-auxiliary sensors only).
? D AUTOCONF-ENABLED	Auto-populate Telemetry Table, Enabled sensors only	? D AUTOCONF-ENABLED	Automatically populate the unit's Telemetry Table with enabled EventSensors (enabled non-auxiliary only).
? D AUTOCLEAR	Clear the Telemetry Table	? D AUTOCLEAR	Automatically default the unit's Telemetry Table to original factory settings.
? D DPD	XML DNP3 Device Profile Document	? D DPD	Generate the XML DNP3 DPD (Device Profile Document) according to the unit's current DNP3 configuration. This is a machine-readable and more current instance of the human-readable DPD.
?W	Wireless modem status	?WIRELESS OR ?W	Basic status of any installed wireless modem
?W INFO	Wireless Modem Information	?W INFO	Status screen for any installed wireless modem
?POWER(SLOT)	Power Distribution Status	?POWER (SLOT) or ?P (SLOT)	Status display for any installed power outputs
ADDLF	Control CR/LF translation	ADDLF (ON,OFF)	Adds LFs when releasing data - for use when data release overwrites itself

BYE	Disconnect from Command session	BYE	Disconnects CLI session (Local, Telnet, and Modem)
BYPASS	Access devices serially	Bypass (port#)	Allows pass-through through serial port directly from the command line
CLOG	Compress Log File	CLOG	Compresses several diagnostic logs into Log.tgz file
COLDSTART	Cold Boot Unit	COLDSTART	Resets to Default settings and Reboots unit (IP, Data Alarm, Serial Port and Action Queue settings remain)
DEFAULT	Resets most settings to default	DEFAULT	Resets settings to factory defaults except for Networking, Serial Port Baud rate/ Parity, Data Alarms, Action queue, and record data.
DEFAULT ALL	Resets ALL settings to Default	DEFAULT ALL	Resets all settings to default BUT does not affect the Record data and does NOT reboot the unit
DELETE	Used to clear files	DELETE <filename>	Used to delete various files such as the AUDIT, TCPLOG, etc
DIR	Lists number of records in various files	DIR	Lists record count for FILEn, EVENTS, and AUDIT
DOMAIL	Send Test Email	DOMAIL	Sends test email

DOPAGE	Sends test page	DOPAGE	Sends test page
DOSMS	Sends test SMS	DOSMS	Sends test SMS text message
DOTRAP	Sends test SNMP trap	DOTRAP	Send test trap
DUPLEX	Sets Local Echo	DUPLEX (half, full)	Sets Local echo for CLI (Telnet, Serial, Modem)
EXIT	Enter and Exit special Login Menu	EXIT	EXIT issued at command line opens login menu, EXIT issued from Login menu ends session
HELP	Lists Command Set	HELP	Lists command set
LOGOFF	Logs off current user	LOGOFF	Logs off current User and allows another user to login
MODEMTALK	Allows one to query the modem	MODEMTALK	Allows you to query the modem for testing purposes
PING	performs standard ping	PING<IP Address>	Performs standard ping function to specified IP address(from command line of the box)
PPP	Tells state of PPP	PPPUP, PPPDOWN	PPP returns the current state, PPPUP raises PPP, PPPDOWN drops PPP connection
PUSHTEST	tests the path to the FTP server	PUSHTEST	FTP pushes a Log file to confirm connectivity w/ FTP server
PUSHNOW	Elicits FTP PUSH	PUSHNOW	Initiates an immediate FTP

			push of the data
RESTART	Restarts the Firmware	RESTART	Restarts the box by command
RESTART ALL	Reboots the OS, then reloads the Firmware	RESTART ALL	Reboots the box by remote command
SA	Send ASCII	SA (FILEn)	SA <filename> will release the data to the screen
SA [FILE*n*] d	Send ASCII then deletes record	SA (FILEn) d	SA <filename> will release the data to the screen then delete it from the records.
SCRIPT	SCRIPT HELP	SCRIPT	Displays scripting command options with descriptions
SETUP	Open Setup Menu	SETUP	Opens main Setup menu
SK	Setting Key command	SK (GET,SET A,X)	Sets and Gets the boxes config (SK GET A to get an ASCII config file, SK SET X to upload a config file via xmodem)
SK ? GEN	Generator Status	SK ? GEN	Displays current status of the generator
SENSORS	Shows Sensor status	SENSORS or !	Shows ES status
SSHC	SSH HELP	SSHC	Displays SSH options and example commands.
STATUS	Shows general STATUS of box	STATUS or ?	Shows boxes general status
TCPLOG	TURNS ON Network log	TCPLOG (ON,OFF)	Turns TCPLOG ON/OFF
TELNET	Allows one to	TELNET <IP address>	One can Telnet to

	Telnet to a device from the command line		any other device on the same Network from the command line
TESTTIME	Tests NTP	TESTTIME	Queries all Network Time servers
TYPE	Releases files to screen	Type (AUDIT,EVENTS)	Allows you to release various log files to the screen
VER	gives Version of FW on box	VER	Tells HW and FW revs of unit
WIRELESS ACTIVATE (CARRIER)	Connects CDMA modem with the specified carrier	WIRELESS ACTIVATE (CARRIER)	Connect a CDMA modem with the carrier network
XF	file transfer via various protocols	XF[X,Y,Z][PUT,GET]<log>	Transfer via xmodem, ymodem, zmodem - RX,TX

Backing Up & Restoring Settings

CLI Backup

Backing up using Xmodem or ASCII

For an [X]modem or [A]SKII settings back up, using a terminal emulator that supports either session logging or Xmodem transfer is recommended. Examples of open source emulators that support at least one of these are TeraTerm (http://ttssh2.sourceforge.jp/index.html.en) and PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

Steps:

1. Establish a Telnet/SSH/Serial connection to the unit.
2. Issue the command **`SK GET`**
3. Decide whether you will be using **`[X]modem`** or **`[A]SCII`** and follow the relevant instructions below.

OPTIONAL: Using the command SK GET CUSTOM (as opposed to SK GET) will retrieve only the non-default settings (as opposed to *all* settings). This results in a significantly smaller and easier to read file, and is best when the settings will be used to configure a unit that is at factory defaults.

Xmodem

When prompted "[X]modem or [A]scii?" Press X for [X]modem. The SiteBoss will now prepare the settings and prompt the user to give the receive command. Using the menus in your terminal emulator find the Xmodem settings and receive the file, placing it anywhere you wish on your local file system. This process is different for every emulator.

ASCII

Enable logging on your terminal emulator and configure the terminal emulator to create a file in an appropriate directory. The process for doing this is different for every emulator. When prompted, "[X]modem or [A]scii?" Press A for ASCII. All setting keys will be printed to the screen. Once this has completed either suspend logging or terminate the connection (close the emulator).

If you do not wish to use the terminal emulator logging function, some emulators allow the ASCII output to be cut and pasted from the screen and into a text file.

Backing up settings using FTP

1. Open a command prompt window on a computer or server that has network access to your SiteBoss.
2. Type **FTP <IP address of unit>**
3. You will be prompted for the user name and password. Ensure you log in using a User ID with MASTER rights.
4. Once user credentials have been input you will get: ?230 Login accepted; user restrictions apply.? and an FTP command prompt.
5. Type **get skall** for all settings or **get skcustom** (for only the non-default settings) followed by a path to a desired directory and a file name. The path is the absolute path to the file on the other machine including any extensions. Use backslashes (\) for path strings. The file name is the exact name of the file including any extensions (.txt).

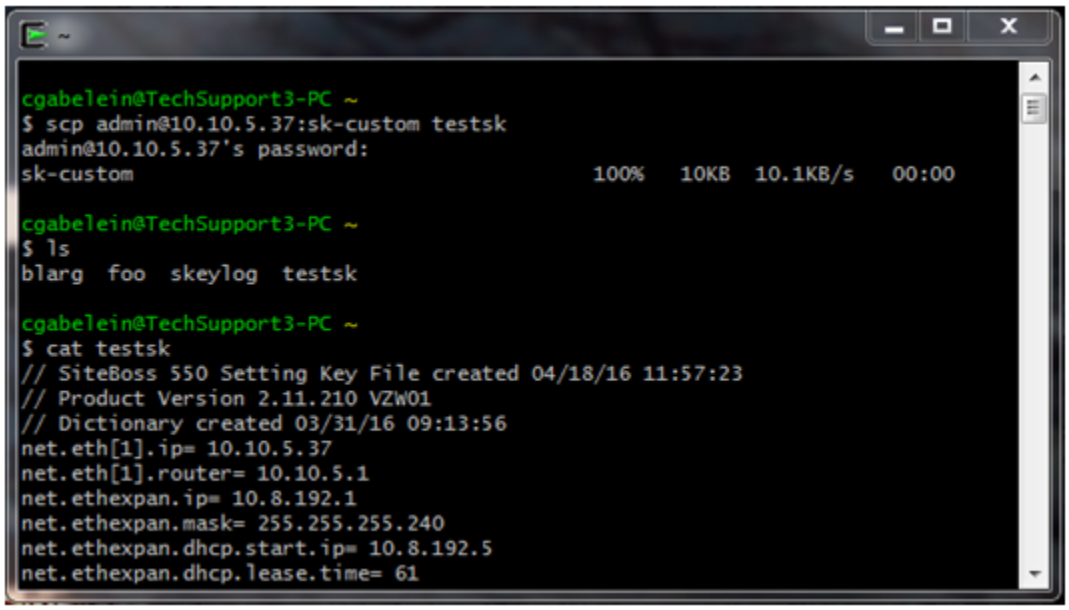
```
J:\>ftp 192.168.100.244
Connected to 192.168.100.244.
220- SiteBoss FTP Server Active (550001122 02/12/17)
220  Please enter user name to proceed...
User (192.168.50.100:(none)): admin
331 Password required for admin
Password:
230 Login accepted; user restrictions apply.
ftp> get skall c:\temp\Siteboss.txt
200 Port OK
150-Please stand by...
150 Opening Data Connection...
226 Transfer complete.
ftp: 49833 bytes received in 0.20Seconds 249.16Kbytes/sec.
ftp>bye
221 Goodbye.
J:\>
```

SCP

On a machine with which you want to connect to a unit via SSH. The selected user will need MASTER-level credentials. Using the example command below the "**user**" needs to be changed to your master level user name, which is **admin** by default. The "**unit**" would be changed to the unit?s IP address.

To transfer all settings from unit (and scripts, if any): **scp user@unit:skall <file name>**.

It is also possible to transfer settings from unit with some filter options:
scp user@unit:sk-<filter> <file name> Used to get a subset of settings. E.g. sk-event.sensor
scp user@unit:sk-custom <file name> Used to get only the settings that are not set to factory defaults
scp user@unit:sk-custom-script <file name> Used to get the non-factory default settings plus any scripts
scp user@unit:sk-script <file name> Used to download script files
scp user@unit:sk-net.dnp3 <file name> Used to download the dnp3 settings
scp user@unit:sk-event.point <file name> Used to download the event sensor point settings
scp user@unit:sk-status <file name> Used to download a status file



CLI Restore

Restore using Xmodem or ASCII

In order for the described [X]modem or [A]scii steps to work, a terminal emulator that supports XModem or ASCII file transfer is required. An example of an open source emulator that supports these is TeraTerm (http://ttssh2.sourceforge.jp/index.html.en). PuTTY does not.

Steps:

1. Establish a Telnet/SSH/Serial connection to the unit.

2. Issue the command SK SET
3. Decide whether you will be using [X]modem or [A]SCII and follow the relevant instructions below.

Xmodem

After an SK set the SiteBoss will prompt "[X]modem or [A]scii?", press X for Xmodem. Using your terminal emulator's menus find the option to send a file via Xmodem. For TeraTerm, click the "File" option in the upper left corner and select "Transfer" then "XMODEM", then "Send". Use the pop up box to select the correct Settings Key file and click Open. Once you begin the transfer the unit will recognize it, and apply the settings immediately.

ASCII

After an SK set the SiteBoss will prompt "[X]modem or [A]scii?" Press A for ASCII. Using your terminal emulator's menus find the option to send a file. In TeraTerm Click the "File" option in the upper left corner and choose "Send File?" and use the pop up box to locate the correct Settings Key file and click Open. Once you begin the transfer the unit will recognize it and apply the settings immediately.

4. (Optional) After the restore is complete type **SK LOG** to see a summary of any errors generated during an SK Set.

Restoring Settings via FTP

To transfer settings to the SiteBoss using FTP:

1. Open a command prompt window on a computer or server that has network access to your SiteBoss.
2. Type **FTP <IP address of unit>**
3. You will be prompted for the user name and password. In order to set settings via FTP you will have to use the user name **omni** and your master level password.
4. Once the user credentials have been input you will get: ?230 Login accepted.? and an FTP command prompt.
5. The syntax for receiving files from another machine to the SiteBoss is: **put [path to file] [filename]**. The path is the absolute path to the file on the other machine including any extensions. Use backslashes (\) for path strings. The file name is the exact name of the file including any extensions (.txt).

```
J:\>ftp 192.168.100.244
Connected to 192.168.100.244.
220- SiteBoss FTP Server Active (550001122 02/12/17)
220  Please enter user name to proceed...
User (192.168.50.100:(none)): omni
331 Password required for omni
Password:
230 Login accepted.
ftp> put c:\temp\Siteboss.txt
200 Port OK
150-Please stand by...
150 Opening Data Connection...
226 Transfer complete.
ftp: 49837 bytes received in 0.04Seconds 1245.93Kbytes/sec.
ftp>bye
221 Goodbye.
J:\>
```

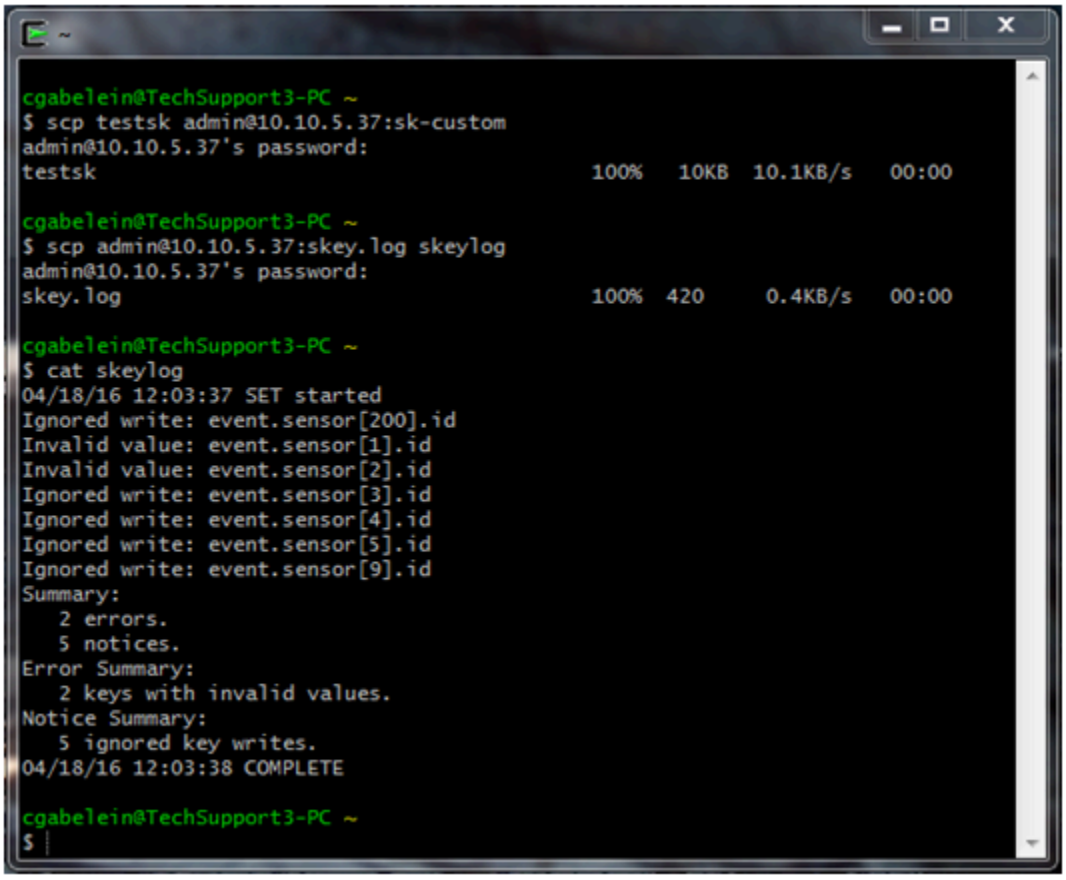
SCP

On a machine with which you want to connect to a unit via SSH. The selected user will need MASTER-level credentials. Using the example command below the "**user**" needs to be changed to your master level user name **admin** by default. The "**unit**" would be changed to the unit?s IP address.

Transfer settings (and/or scripts) to unit: **scp <sk file name> user@unit:<sk file name>**.

Remote file name must start with "sk" or end with ".sk". E.g.: **scp skall user@unit:skall**
scp sk-net.dnp3 user@unit:sk-net.dnp3
scp sk-event.point user@unit:blarg.sk

To check the result of the last SK file transfer to the unit, get the skey.log file: **scp user@unit:skey.log <file name>**



Firmware Upgrades

Upgrades using FTP

Server Method

1. Open a command prompt window on a computer or server that has network access to your SiteBoss.
2. Type **FTP <IP address of unit>**
3. You will be prompted for the user name and password. Ensure you log in using a User Profile with MASTER rights.
4. Once user credentials have been input you will get: ?230 Login accepted; user restrictions apply.? and an FTP command prompt.
5. Type **" hash "** at the FTP prompt. (This is optional - it just creates hash marks (###) while the file is transferring so you can see something happening.)
6. At the next FTP prompt type: **put drive:\directory\<update filename>**. For example: **put C:\upgrades\340- 2.10.850-spr01-a71.udf**
7. Hash marks will now appear to show you that the file is transferring. When the transfer is complete you will be returned to an FTP prompt.
8. Type: **bye** at the FTP prompt. The unit still has to process this file, which takes about 5 minutes, at which time the unit will reboot. Wait until the unit reboots before proceeding.
9. After the SiteBoss reboots, connect to it and either check the top line of the Status screen, or type **VER** at the command line. You should see that the unit is now upgraded to the new version.
10. Check your settings to be sure none have been lost. If they have, reload the Settings Key file; see the CLI Restore section for instructions.

```
C:\Windows>ftp 192.168.100.223
Connected to 192.168.100.223.
220- SiteBoss FTP Server Active (550001267 04/30/17)
220  Please enter user name to proceed...
User (192.168.100.223:(none)): admin
331 Password required for admin
Password:
230 Login accepted; user restrictions apply.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put C:\Temp\550-2.11.480-std-a71.udf
200 Port OK
150 Opening Data Connection...
################################################################
################################################################
################################################################
. . .
226 Transfer complete.
ftp: 11327768 bytes sent in 29.97Seconds 377.98Kbytes/sec.
ftp>
```

Client Method

To use this method you will need an FTP server.

1. Place the update file in the configured shared folder that the unit will be able to access via FTP.
2. Log into your unit's command line interface. Ensure you log in using an ID with MASTER rights.
3. At the command line type: **xf f get <update filename> <host> <username>**

The username needed is the username for the FTP server and the unit will prompt for the password for that user.

Here is an actual session:

```
> xf f get 550-2.12.290-std-a71.udf 192.168.100.71 user
Receiving 550-2.12.290-std-a71.udf via FTP
user's password:
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................................................
.............................
COMPLETE
```

SFTP client method

SFTP as a client method is accomplished in a similar fashion.

1. Place the update file in the configured shared folder that the unit will be able to access via SFTP.
2. Log into your unit's command line interface. Ensure you log in using an ID with MASTER rights.
3. At the command line type: **xf s get <update filename> <host> <username>**

The username needed is the username for the SFTP server and the unit will prompt for the password for that user.

```
>xf s get 550-2.11.480-std-a71.udf 192.168.100.30 john
Receiving 550-2.11.480-std-a71.udf via SFTP
john's password:
......................
COMPLETE
```

Upgrades using X/Y/Z Modem

Updates can be done using X, Y or Z modem. In order for this process to work a terminal emulator that supports X, Y or Zmodem, such as TeraTerm (http://ttssh2.sourceforge.jp/index.html.en). This process will be faster by Telnet or SSH but it can also be done using a serial connection.

If you are using the serial port, it is recommended to increase the Baud Rate to 115200 using the SETUP menu, since this is a large file. To do that:

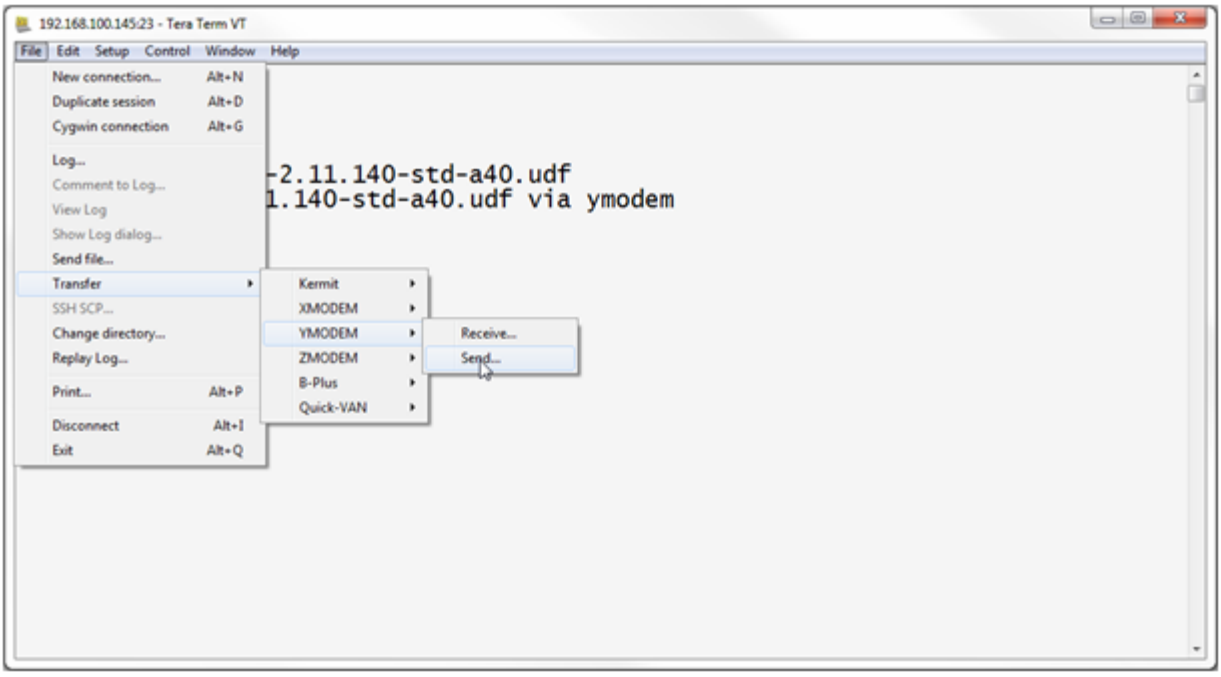
1. Type SETUP at the command prompt.
2. Select B) Serial Settings.
3. Select A) 1-I/O 1 Settings
4. Select B) Baud Rate
5. From the drop down options select J) 115200

You will also need to set your Terminal Emulator to the same speed. If you are using Tera Term:

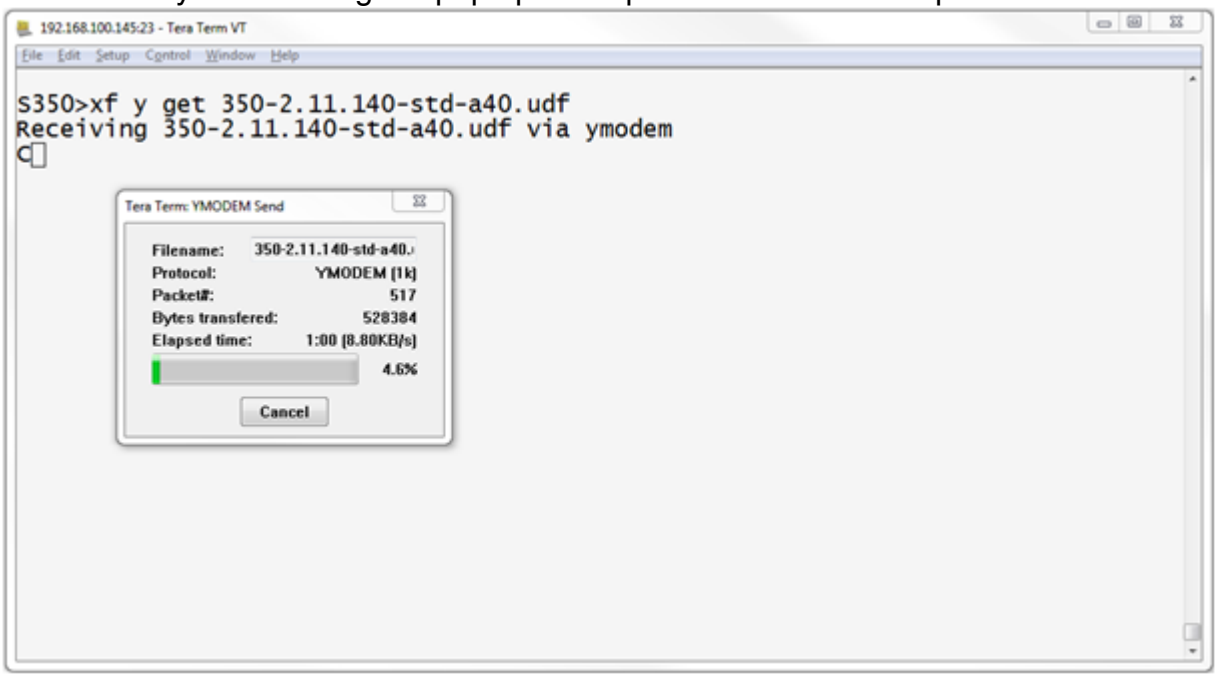
1. Select Setup in the upper menu bar and from the drop down select Serial Port.
2. Adjust the Baud rate to 115200 to match.

Upgrade Steps:

1. Establish a Telnet/SSH/Serial connection to the unit.
2. Use the SiteBoss XF command followed by the transfer method, then the file name. Example: **xf y get 550-2.11.480-std-a40.udf**
3. In Tera Term use the top menu bar select File, then Transfer, then your select transfer method, then send



4. Then select your file using the pop up file explorer box and click Open.



Advanced Log Files

These log files may be requested by Tech Support on occasion to help troubleshoot problems. It is important to know how to retrieve them if needed. In situations where these logs would help in diagnosing a problem it is also important to acquire them as close to the problem occurring as possible as many of them are constantly running in the background, and will

eventually overwrite themselves.

Sys Log

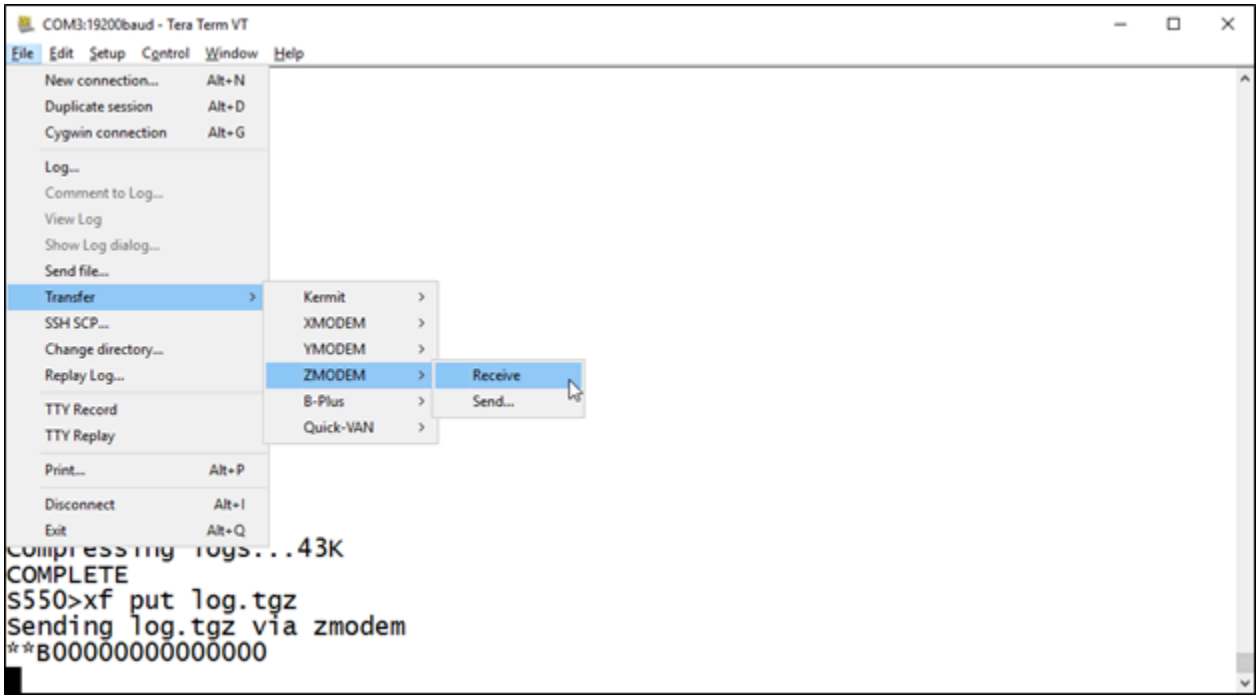
Below are the instructions for getting the SYSLog off of your unit:

```
>CLOG
Compressing logs...5K
COMPLETE
```

1. Log onto the unit?s command line using Telnet, SSH or a Serial connection with IO2 using TeraTerm (http://ttssh2.sourceforge.jp/index.html.en)
2. From the SiteBoss command prompt type **CLOG** and press <Enter> to generate the log file. This will create log.tgz and place it in the root directory of the device.
3. Type **xf put log.tgz** at the command prompt
4. Navigate to the File menu in the upper left hand corner of TeraTerm.
5. Select Transfer > ZMODEM > RECEIVE

»**NOTE**: TeraTerm should automatically transfer the file. To see where it put the file go to File > Change directory? The pop up box will tell you the Current Dir:\ it will be a file called log.

6. Attach the log.tgz file to an email and send it to support@asentria.com



TCP Log

Below are the instructions for getting the TCP log off of your unit:

1. Connect to the unit via Telnet, SSH, or the console port.
2. Issue the command "tcplog on". This enables TCP logging.
3. Attempt some network actions with the box, such as pinging the host unit from a remote location, and pinging 8.8.8.8 (Google's DNS Server) from within the SiteBoss. To ping an address from within the SiteBoss command line, type "ping 8.8.8.8". This will begin a recurring ping test. Press ctrl + C in order to stop the test. If experiencing a specific problem perform the steps to reproduce the problem.
4. Issue the command "tcplog off".
5. Issue the **CLOG** command to generate the log file.

The output of **CLOG** will look like this:

```
>CLOG
Compressing logs...5K
COMPLETE
```

6. Type ?xf put log.tgz? at the command prompt
7. Navigate to the ?File? menu in the upper left hand corner of TeraTerm.
8. Select Transfer > ZMODEM > RECEIVE

»**NOTE**: TeraTerm should automatically transfer the file. To see where it put the file go to File > Change directory? The pop up box will tell you the Current Dir:\ it will be a file called log.

9. Attach the log.tgz file to an email and send it to support@asentria.com

LOG.TGZ via FTP

To get these logs, you must compress the files and download the Log.tgz file. This is done by issuing the **CLOG** command at the command line.

You can download the Log.tgz file via FTP.

1. Issue a CLOG command at the SiteBoss command prompt.
2. Go to the CMD window on you computer and issue FTP xxx.xxx.xxx.xxx (where xxx.xxx.xxx.xxx is the IP address of the SiteBoss). Use username: **omni**, and password: your MASTER password (**password** by default).
3. Issue an LS and you should see Log.tgz listed among the files. Do a get command of Log.tgz. This would be ?get log.tgz C:exact file path using\destination file name. e.g. get log.tgz C:temp\log.tgz
4. Attach the log.tgz file to an email and send it to support@asentria.com

General Specifications

S550-2

Width: 11in / 27.94cm
Height: 1.75in / 4.45cm Depth: 7.80in / 19.812cm
Weight: (depending on configuration) 3 - 5lbs / 1.36 - 2.27kg
Mounting: Shelf or 19in rack
Operating Temperature: 0° to +40° C standard, -40° to +60°C extended range
Storage Temperature: -40° to +85°C
Power: 15VDC Desktop Supply or optional -48VDC
Current: 1.5A (Max)
Operating and Storage Humidity: 0 to 95% (non-condensing)
DC Voltage In: 20VDC to 60VDC
RoHS/CE/CSA/A-tick Certification: Yes
Mean Time Between Failure: 70,000hr
Power Consumption (Typical): 5.25W
Power Consumption (Max): 24W
BTU?s (Nominal): 18 BTU/Hour
BTU?s (Max): 82 BTU/hour

S550-6

Width: 17in / 43.2cm
Height: 1.75in / 4.45cm
Depth: 7.8in / 19.812cm
Weight: (depending on configuration) 3 - 5lbs / 1.36 - 2.27kg
Mounting: Shelf or 19in rack
Operating Temperature: 0° to +40° C standard, -40° to +60°C extended range
Storage Temperature: -40° to +85°C
Power: 15VDC Desktop Supply or optional -48VDC
Operating and Storage Humidity: 0 to 95% (non-condensing)
RoHS/CE/CSA/A-tick Certification: Yes
Mean Time Between Failure: 70,000hr

Power Specifications

Voltage In: 36VDC (Min) / 60VDC (Max)
Current: 1.5A (Max)
Power Consumption (Typical): 5.25W
Power Consumption (Max): 24W
BTU?s (Nominal): 18 BTU/Hour
BTU?s (Max): 82 BTU/hour

►Expansion Card Insertion Procedures

The SiteBoss can be purchased with a variety of optional Expansion Cards that are normally inserted in the expansion bays of the unit when it is assembled at the factory. Expansion Cards can also be purchased separately and inserted by field technicians after the unit has been installed in the field. When doing this, there are some specific precautions and steps that must

be followed in a specific order when inserting Expansion Cards in the field:

- The field technician must take precautions to ensure he/she is electrically grounded so as not to damage the Expansion Card circuit board, or the main circuit board of the unit. Follow normal Electrostatic Discharge (ESD) procedures for handling electronics per IPC-610.
- The Expansion Card should remain in its protective ESD bag until it is time to actually insert it into the expansion bay.

Follow these steps to install an Expansion Card:

1. Unplug the power cable from the SiteBoss.
   Expansion Cards are NOT hot-swappable.
2. Unplug the telephone cord from the internal modem (if connected). This MUST be done before removing any expansion port cover plates.
3. Remove the two screws for any expansion bay cover plate and set the plate aside.
4. Carefully remove the Expansion Card from its protective ESD bag and slide it into the plastic rails inside the expansion bay. Visually confirm the Card is in both rails and properly aligned.
5. Push the card until it is fully inserted in its slot.
6. Replace the two screws previously removed so the Card is held securely in the bay.
7. Place the Expansion Card label on the back panel directly above or below the Expansion Card, taking care to align the markings on the label with appropriate I/O points or ports on the Card.
   Note: If installing a Wireless Modem Expansion Card, screw the rubber GMS antenna (or cable to an external antenna) to the SMA connector on the modem. The unit should not be powered up without an antenna connected to the modem.
8. Replace the telephone cord in the internal modem jack (if used).
9. Plug the power cable into the host unit.
10. After the unit reboots, proceed with connecting devices to, and configuring the Expansion Card, as necessary for the type of Card it is.

Note: Some expansion cards have significantly higher power requirements than others. It is important to ensure the power supply is adequate when changing a configuration that was shipped from the factory. If using more than 4 Isolated Contact Cards ("-8CI option"), 3 non-isolated 4-20mA Cards ("-8M" option) or more than 2 Isolated 4-20mA Cards ("-4C4MI" option) with the -48VDC power supply configuration, the higher power 30W version of the -48VDC Power Supply should be ordered from Asentria Corporation. Adding Wireless Modem expansion cards - outside of the factory to 6 slot units - may also require the higher power supply.

Please contact Asentria Technical Support if any questions.

►FCC Requirement: Part 15

INFORMATION PROVIDED TO CONSUMER CLASS A DIGITAL DEVICE OR PERIPHERAL
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful

interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Internal Modem Guidelines

The internal modem supplied with this product complies with Part 68 of the FCC Rules and Regulations. The labeling on the modem provides the FCC Registration number and the Ringer Equivalence Number (REN) for the modem. This information is also listed below. You must provide, upon request, this information to your telephone company.

The REN is useful to determine the quantity of devices you may connect to a telephone line and still have all of the devices ring when the number is called. In most, but not all areas, the sum of the RENs of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to a line, as determined by the REN, you should contact the local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance. If advance notification is not possible, you will be notified as soon as possible.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with the modem, contact Asentria at (206) 344-8800 for information on obtaining service or repairs. The telephone company may ask you to disconnect the device from the network until the problem has been corrected or until you are sure that the device is not malfunctioning.

This device may not be used on coin service lines provided by the telephone company (this does not apply to private coin telephone applications which use standard lines). Connection to party lines is subject to state tariffs.

Modem	FCC ID	REN
2400 Baud Modem	EUD-5U9-BRI4480	0.8B
33.6K Baud Radicomm Modem	406CHN-31735-PT-E REN 1.1B	1.1B
33.6K Baud OmniModem	6KMUSA-34184-MME REN 0.9B	0.9B
33.6K Baud MultiModem	AU7-USA-46014-MD-E	0.1B

Canadian Department of Communications

NOTICE: The Canadian Department of Communications Label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protections that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of total load to be connected to a telephone loop, which is used by the device, to prevent overloading.

The termination of a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100. The load number of this unit is five.

This digital apparatus does not exceed the Class A limits for Radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.

AVIS: - L'étiquette du ministère des Communications du Canada identify le materiel homologué. Cette étiquette certifie que le matériel est conforme a certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. Le Ministère n'assure toutefois pas que le matériel fonctionnera a la satisfaction de l'utilisateur.

Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'entreprise locale de télécommunication. le matériel doit également etre installé en suivant une méthod acceptée de raccordement. Dans certains cas, les fils intérieurs de l'entreprise utilisés pour un service indivuduel a linge unique peuvent etre prolongés au moyen d'un dispositif homologué de raccordement (cordon prolongateur téléphonique interne). L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empechent pas la dégradation du service dans certaines situations. Actuellement, les entreprises de télécommunication ne permettent pas que l'on raccorde leur matériel a des

jacks d'abonné, sauf dans les cas précis prévus pas les tarrifs particuliers de ces entreprises.

Les réparations de matériel homologué doivent etre effectuées pas un centre d'entretien Canadien autorisé designé par le fournisseur, La compagnie de télécommunications puet demander a l'utilisateur de débrancher un appareil a la suite de réparations ou de modifications effectuées par l'utilisateur ou a cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise a la terre de la source d'energie electrigue, des lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particuliérement importante dans les régions rurales.

Avertissement. - L'utilisateur ne doit pas tenter de faire ces raccordements lui-meme; il doit avior recours a un service d'inspection des installations électriques, ou a electricien, selon le cas.

L'indice de charge (IC) assigné a chaque dispositif terminal indique, pour éviter toute surcharge, le pourcentage de la charge totale qui peut etre raccodée a un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit bouclé peut etre constituée de n'import quelle combinaision de dispositif, pourvu que la somme des indices de charge de l'ensemble des dispositifs ne dépasse pas 100. L'indice de charge de cet produit est 5.

Cet appereil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur :"Appareils Numériques", NMB-003 édictée par le ministre des Communications.

Warranty Information

Asentria Corporation hereby warrants that it will, as the buyers sole remedy, repair or replace, at its option, any part of the Siteboss which proves to be defective by reason of improper materials or workmanship, without charge for parts or labor, for a period of 12 (twelve) months. This warranty period commences on the date of first retail purchase, and applies only to the original retail purchaser.

To obtain service under this warranty, you must obtain, by telephone, postal letter, or email, a return authorization number from Asentria Technical Support. This authorization number may be obtained by contacting Asentria Technical Support at the address and/or phone number below. The defective unit is to be returned to Asentria with shipping prepaid, and the return authorization number must be clearly marked on the outside of the package containing the defective unit.

The dealer's bill of sale or other satisfactory proof of the date of purchase may be required to be presented in order to obtain service under this warranty.

This warranty applies if your Siteboss fails to function properly under normal use and within the manufacturer's specifications. This warranty does not apply if, in the opinion of Asentria Corporation, the unit has been damaged by misuse; neglect; or improper packing, shipping, modification, or servicing by other than Asentria or an authorized Asentria Service Center.

In no event shall Asentria Corporation be liable for any loss, inconvenience or damage,

whether direct, incidental, consequential or otherwise, with respect to the Siteboss. Asentria Corporation's liability shall be limited to the purchase price of the Siteboss. No warranty of fitness for purpose, or of fitness of the Siteboss for any particular application is provided. It is the responsibility of the user to determine fitness of the Siteboss for any particular application or purpose.

Asentria Technical Support

The Asentria Techical Support department can be reached free of charge between the hours of 8AM to 5PM (USA Pacific time) via the following methods:

- Phone: 1 (206) 344-8800 Ext. 3
- Email: support@asentria.com

e-mails will be answered within 24 hours.

Asentria Technical Support

1200 North 96th St.
Seattle, WA 98103
206.344.8800
support@asentria.com

www.asentria.com