



**User's Manual  
Installation and Operation Guidelines**

**TeleBoss™ 830-0 Pollable Remote Access Unit**

---

Version 2.05.260

Asentria Corporation  
1200 North 96<sup>th</sup> Street  
Seattle, Washington, 98103  
U.S.A.  
Tel: 206.344.8800  
Fax: 206.344.2116  
[www.asentria.com](http://www.asentria.com)

# TeleBoss™ 830-0 Pollable Remote Access Unit Installation and Operation Guidelines

For firmware version 2.05.260\_STD  
Release Date: February 19, 2009

## Changes In This Version of the User Manual

- This is the initial manual for the new TeleBoss 830-0, a TeleBoss 830-0 with no expansion bays on the back panel for Expansion Cards, and the first Asentria product with a SensorJack port. Basic functionality remains the same as the TeleBoss 830-2 and 830-6 products, however all references to anything concerning Expansion cards has been removed from this manual, and further explanation regarding the SensorJack port and Type2 EventSensors has been added.

## Conventions used in this manual

- 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) but any key values displayed are in normal type.
- **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. Web interface shots are not displayed in the manual at this time.
- 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.

© 2009 Asentria Corporation. All rights reserved.

The content of this manual is provided for informational use only, and is subject to change without notice. Examples, data, and names used in this manual are examples and fictitious unless otherwise noted. No part of this document may be reproduced or electronically transmitted without permission from Asentria Corporation.

TeleBoss 830-0, T830-0, EventSensor and SitePath are trademarks of Asentria Corporation.

# Table of Contents

<b>Quick Start</b> .....	<b>1</b>
<b>What's Included</b> .....	<b>1</b>
Hardware Needed.....	1
Information Needed .....	1
<b>Connecting</b> .....	<b>1</b>
Cables and Power.....	1
Power Requirements .....	1
Accessing the Command Line .....	1
<b>Network Setup</b> .....	<b>2</b>
Setup.....	2
Testing Network Connectivity .....	2
<b>SNMP Trap Setup</b> .....	<b>2</b>
Setup.....	2
Testing SNMP Traps.....	2
<b>What is a TeleBoss 830-0</b> .....	<b>3</b>
<b>The Basics</b> .....	<b>3</b>
Communication Methods .....	3
Data Storage.....	3
Remote Access.....	4
Serial Monitoring (Data Events).....	4
Event Notification .....	4
Audit Log.....	4
Integration with SitePath .....	4
<b>Parts Identification</b> .....	<b>4</b>
Features and Accessories .....	4
LEDs, Ports, DIP Switches and Buttons .....	5
<b>Getting Connected</b> .....	<b>8</b>
<b>Power Up Sequence</b> .....	<b>8</b>
<b>Default Passwords</b> .....	<b>8</b>
<b>The Status Screen</b> .....	<b>8</b>
<b>Setup Menu</b> .....	<b>10</b>
<b>Overview</b> .....	<b>10</b>
<b>Option Types</b> .....	<b>10</b>
<b>Web Interface</b> .....	<b>11</b>
<b>Main Setup Menu</b> .....	<b>11</b>
Network Settings.....	12
Serial Settings.....	21
Modem Settings .....	22
Security Settings .....	23
Alarm/Event Definitions.....	27
Action Definitions .....	36
General Settings .....	38
Event Log Settings.....	40
Audit Log Settings.....	41
<b>Features and How To Use Them</b> .....	<b>42</b>
<b>Upgrading the T830-0</b> .....	<b>42</b>
<b>Setting Keys</b> .....	<b>43</b>
<b>Securing a TeleBoss 830-0</b> .....	<b>44</b>
<b>Telnet/TCP Connections</b> .....	<b>46</b>
<b>Secure Shell (SSH)</b> .....	<b>47</b>
Quick Start: SSH into the unit .....	47
Configuring authentication .....	47
Configuring a login banner for SSH. ....	47
<b>Default Router</b> .....	<b>48</b>
<b>Static Routes</b> .....	<b>49</b>

<b>Passthrough</b> .....	<b>50</b>
<b>Call Failure Tracking</b> .....	<b>51</b>
<b>RADIUS Security</b> .....	<b>52</b>
Description .....	52
Overview .....	52
Benefit .....	59
Configuration.....	59
Example .....	59
<b>Data Events</b> .....	<b>60</b>
<b>Configuring Data Alarm Equations</b> .....	<b>62</b>
<b>Data Alarm Macros</b> .....	<b>63</b>
<b>Action List</b> .....	<b>65</b>
<b>Types of Alarm Notices</b> .....	<b>67</b>
SNMP Traps .....	67
Email Alarms .....	68
Asentria Alarms.....	68
SMS Alarms .....	71
Pager Alarms .....	71
<b>Type2 EventSensor™ Configuration Setup</b> .....	<b>72</b>
Dip Switch Settings .....	72
Connections .....	72
Temperature Sensor Setup (ES-T).....	72
Humidity Sensor Setup .....	73
<b>Customizable Command Prompt</b> .....	<b>75</b>
<b>IP Record Collection (IPRC)</b> .....	<b>76</b>
<b>Generic Server</b> .....	<b>76</b>
<b>Avaya Definity RSP</b> .....	<b>77</b>
<b>Alcatel OmniPCX 4400</b> .....	<b>78</b>
<b>CCM 4 (Cisco CallManager version 4.x)</b> .....	<b>82</b>
<b>Generic Client</b> .....	<b>87</b>
Siemens HiPath 4000 .....	87
<b>Intecom Telari</b> .....	<b>88</b>
<b>Nortel BCM</b> .....	<b>89</b>
<b>Syslog</b> .....	<b>90</b>
<b>NEC NEAX2400</b> .....	<b>92</b>
<b>CCM 5 (Cisco CallManager version 5.x)</b> .....	<b>93</b>
<b>Command Reference</b> .....	<b>94</b>
<b>User Interface Commands</b> .....	<b>94</b>
<b>Setup Commands</b> .....	<b>94</b>
<b>System Commands</b> .....	<b>95</b>
<b>Numeric Commands</b> .....	<b>95</b>
<b>Usage Commands</b> .....	<b>96</b>
<b>Appendices</b> .....	<b>98</b>
<b>User Rights Table</b> .....	<b>98</b>
<b>Control Characters</b> .....	<b>99</b>
<b>Internal Modem Guidelines</b> .....	<b>100</b>
<b>Canadian Department of Communications</b> .....	<b>101</b>
<b>Warranty Information</b> .....	<b>103</b>

## Quick Start

### What's Included

This chapter is a brief guide to help get your TeleBoss 830-0 (T830-0) up and running quickly.

#### Hardware Needed

- Asentria TeleBoss 830-0
- 15VDC power adaptor (Included)
- DC power source (if DC power option)
- Computer with DB9 RS-232 Serial port and terminal emulation software
- Ethernet cable
- RJ45 M-M unshielded serial cable and RJ45/DB9 straight thru adapter (Included)
- A PC running any type of SNMP trap management software, if T830-0 will be sending SNMP traps as event actions

#### Information Needed

- IP address(es) to assign to the T830-0
- Subnet mask
- Default router IP or gateway router IP address if on a WAN (Optional)
- IP address of a PC running any type of SNMP trap management software, if T830-0 will be sending SNMP traps as event actions

## Connecting

#### Cables and Power

1. Connect the RJ45 serial cable and DTE adaptor together, and connect the RJ45 end to serial port I/O 2 of the T830-0, and the DB9 end to COM1 of a computer with a terminal emulator.
2. Connect the attached ground wire securely to an appropriate earth ground (this is essential).
3. Connect an Ethernet cable, if available, into the RJ45 jack labeled ETH1.
4. Connect the power supply to the unit (see Power Requirements section).

#### Power Requirements

The T830-0 is configured with a power jack for connecting the 15VDC power adapter shipped with the unit. If the optional DC power option is being used, a –48VDC to AC power adapter is provided.

#### Accessing the Command Line

1. Connect to I/O 2 with a serial terminal emulation program at 19200 baud, 8N1.
2. Enter **STATUS** or **?** and press <Enter>. You will be presented with a status screen similar to the following.

```

TeleBoss 830 2.05.260 STD - Status
Site Name      : 830-830000857
Serial Number  : 830000857      Eth 1      : STATIC
Date          : MON 02/16/2009  IP Addr     : 0.0.0.0
Time         : 12:53:03        MAC Addr   : 00:10:A3:60:01:20
Memory       : 2048K          Eth 2      : STATIC
% Full Alarm  : OFF           IP Addr     : 0.0.0.0
No-Data Alarm 1 : OFF        MAC Addr   : 00:10:A3:60:01:21
No-Data Alarm 2 : OFF        Modem      : Yes
Duplex        : HALF

-----
Port  Baud/Etc.  Recs   Bytes   Full Wrap Name
IO1  : 19200,8N1 00000000 00000000 0% OFF I/O 1
IO2  : 19200,8N1 00000000 00000000 0% OFF I/O 2

COMPLETE
>

```

When the status screen appears, the unit is successfully connected and ready for use.

## Network Setup

### Setup

1. Access the Main Setup Menu by typing **SETUP** and pressing <Enter>.
2. Select the Network Settings branch.
3. Select A) Ethernet Settings and select the Ethernet interface that corresponds to the one on the back panel that you plugged your network cable into (ETH1).
4. Enter an IP address, subnet mask and--if necessary--a router address.
5. Toggle NAT on/off as desired.
6. Press <ESC> to go back one level in the menu tree, or <CTRL + C> to exit the setup menu and return to the command prompt.

### Testing Network Connectivity

1. Verify that the network router is available to the unit by typing the command **PING <IP\_address>**. A router is always a good candidate to test pings. The following screenshot is an example of a successful ping test.

```
ping 192.168.100.59
PING 192.168.100.59 (192.168.100.59): 56 data bytes
64 bytes from 192.168.100.59: icmp_seq=0 ttl=128 time=8.0 ms
64 bytes from 192.168.100.59: icmp_seq=1 ttl=128 time=0.7 ms
64 bytes from 192.168.100.59: icmp_seq=2 ttl=128 time=1.8 ms
64 bytes from 192.168.100.59: icmp_seq=3 ttl=128 time=0.8 ms
64 bytes from 192.168.100.59: icmp_seq=4 ttl=128 time=0.7 ms
64 bytes from 192.168.100.59: icmp_seq=5 ttl=128 time=0.7 ms

--- 192.168.100.59 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.7/8.0 ms
```

2. Press <CTRL + C> to stop the ping testing. If <CTRL + C> is not pressed, the unit will continue pinging attempts indefinitely.
3. 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](#).
4. Using a Telnet client, connect to the IP address assigned to the unit.

## SNMP Trap Setup

If you will be using your T830-0 to send SNMP traps, this section will help you ensure it is set up correctly.

### Setup

1. Configure the network settings as described in the previous section.
2. Select the Network Settings then SNMP Settings sub-menu.
3. Verify the SNMP Community name is correct for your network.
4. Switch to the Actions Definitions menu and enter the host name or IP address of the computer to receive the traps into the field, "Hostname/IP Address 1".
5. Press <CTRL + C> to exit the Setup menu and return to the command prompt.
6. On the computer that will be receiving the SNMP traps, start your preferred SNMP trap manager.

### Testing SNMP Traps

1. Using a Telnet client, connect to the IP address assigned to the unit.
2. Enter the command **DOTRAP** from the T830-0 command prompt.
3. Verify that the trap manager receives the test trap.
4. 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](#).

# What is a TeleBoss 830-0

## The Basics



Fig 1: T830-0

The T830-0 is a powerful remote device management system which can collect and forward text records such as those used by Call Accounting and Telemangement billing applications. These records are collected by the T830-0 from PBX serial ports, and in some cases directly over a TCP/IP connection. The T830-0 can also make a passthrough connection directly to devices connected on one of its serial ports, and can also connect you via web or Telnet to other devices on the same remote network as the T830-0. The T830-0 provides versatile alarm management of text-based alarms as well as interfaces with environmental monitoring equipment and contact closure alarms at your remote site. The T830-0 is a powerful remote network management solution for Call Accounting systems, Service Bureaus, and end users who need to collect PBX data as well as get remote access, and collect alarms from equipment at remote sites.

### Communication Methods

The T830-0 has a diverse selection of communication methods available for different applications. The following methods can be used to either access the command processor or provide a passthrough connection to devices attached to the serial ports. All methods of connecting to the unit can be secured via password for protection of data and hardware.

- RS-232 serial
- Telnet
- Standard modem serial

Data may be retrieved from or through the T830-0 by any of the following methods:

- Serial or modem connection to command processor (using Line or Zmodem) or pass-through
- Inline Mode (data in I/O 1, data out I/O 2)
- Telnet to command processor or passthrough
- Telnet real-time sockets
- FTP push (automatic delivery to FTP server)
- FTP get (manual retrieval from FTP server)

Alarms generated or detected within the T830-0 can be delivered through any of the following means:

- Modem callout
- SNMP trap
- Asentria Alarms
- Email

### Data Storage

Basic data storage in the T830-0 is accomplished in a database of 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 either FILE1 and FILE2, or both. Data collected via IP Record Collection (IPRC) is also stored to either FILE1 or FILE2. EVENTS and AUDIT are log files generated from the Event Log Settings and Audit Log Settings menus per the parameters set there. The number of records stored in each these four files can be displayed using the **DIR** command on any connection to the command processor, including FTP.

### Remote Access

The T830-0 can provide an administrator transparent access to devices connected to the serial ports of the unit via passthrough connections or through the login menu in the web interface, Telnet and modem connections. This sort of access can be used to configure, maintain, or manipulate devices that would normally have no remote access.

### Serial Monitoring (Data Events)

The T830-0 has the capability to monitor incoming data for user-defined strings and then report the event via several avenues. The T830-0 allows for up to 200 different data events. Each data event contains independent actions, counters, and other unique settings. Data events triggered within the T830-0 can be logged to an Event Log. This file can be viewed through the Event Log section of the setup menu, via the **TYPE EVENTS** command, or through FTP.

### Event Notification

Actions generated or detected within the T830-0 can be delivered through any of the following means:

- Modem callout
- Asentria Alarms
- SNMP trap
- Email

### Audit Log

The T830-0 has the capability to log many types of administrative events, from DIP switch changes to login attempts. These Audit Log entries are stored in a file and can be viewed through the Audit Log section of the setup menu, via the **TYPE AUDIT** command, or through FTP.

### Integration with SitePath

Using the T830-0 in conjunction with Asentria's SitePath Remote Management System, you can create secure and controlled IP access to remote servers and appliances collocated on the same remote network as the T830-0. SitePath uses an integrated IPSEC VPN implementation which simplifies otherwise complex VPN setup down to a few easy steps, allowing users to access remote devices via the SitePath VPN Gateway. The T830-0 plus SitePath provide IP routing to authorized remote network addresses and prevents unauthorized access to any other addresses on the remote LAN.

## Parts Identification

### Features and Accessories

#### Standard Equipment

The base T830-0 comes with the following standard on-board equipment:

- AC Power Input
- Logging database for CDR or other text records
- 2 – RJ45 DTE serial I/O ports
- 2 – 10/100Mb Ethernet interfaces
- 1 – MMC memory I/O slot
- 1 – SensorJack port
- Internal lithium coin-cell type battery backup<sup>\*/\*\*</sup>

\* 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. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.** The instructions are that lithium batteries can be recycled, and you should contact a recycling organization in your area for details.

In addition to the above components, the standard unit is shipped the following accessories:

- This product manual on the Documentation and Software CD
- RJ45 M-M unshielded serial cable and RJ45/DB9 straight thru adapter for each serial port ordered
- RJ45 Ethernet cables for each Ethernet port
- Power supply adapter (for AC units), or adapter for units that will use –48VDC power



## Options

Each of the following components is optional and may be installed on a T830-0:

- On-board 56K dialup modem

The T830-0 may come with any of the following accessories as well, depending on the configuration or order:

- Modem cable if that option is ordered

## LEDs, Ports, DIP Switches and Buttons



Fig 2: Front panel (T830-0)

### LEDs – Front Panel

#### 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 solid green whenever the modem is connected and blinks when the modem is dialing out.

#### ALM (Alarm)

This LED is reserved for future use.

#### 25% - 75% - 100%

The T830-0 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.

### LEDs – Back Panel

Each RJ45 port on the back panel has two LEDs associated with it – one on the Right of the port, one on the Left of the port.

#### Ethernet Ports (ETH1 and ETH2)

- 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

- 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 T830-0, regardless of whether a cable is connected to the I/O Port or not.

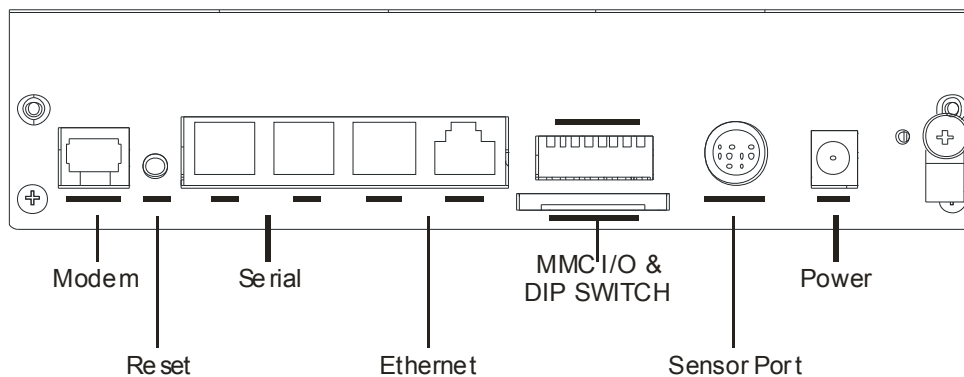


Fig 3: Back panel T830-0 (7.5"- wide model)

The above drawing shows the T830-0 configured (from right to left) with a grounding wire lug, AC power jack, 9-pin mini-DIN SensorJack port, bank of 8 DIP switches, MMC memory I/O card slot, two RJ45 Ethernet ports, two RJ45 RS232 serial ports, Reset button, and one RJ11 POTS modem port.

**Ports**

Sensor Port

The 9-pin mini-DIN port is for connecting up to 3 (eventually 8) Asentria Type 2 Event Sensors.

Memory I/O

The slot labeled Memory I/O is reserved for future use. Eventually T830-0's may be upgraded using a MultiMedia Card (MMC) in this slot.

Ethernet

The Ethernet 10/100Mb interfaces are standard RJ45. Either of these standard connectors will connect the T830-0 to an Ethernet hub or switch. Refer to the [Telnet/TCP Connections](#) section in the Features chapter for further information regarding a number of different types of telnet connection options. LEDs by each Ethernet connection on the back panel flicker when packets are being transmitted/received on that port.

Serial Ports

Each of the two 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 T830-0
- PIN2 =DCD =CARRIER DETECT, INPUT to the T830-0
- PIN3 =DTR =DATA TERMINAL READY, OUTPUT from the T830-0
- PIN4 =SIGNAL GROUND
- PIN5 =RXD =RECEIVED DATA, INPUT to the T830-0
- PIN6 =TXD =TRANSMITTED DATA, OUTPUT from the T830-0
- PIN7 =CTS =CLEAR TO SEND, INPUT to the T830-0
- PIN8 =RTS =REQUEST TO SEND, OUTPUT from the T830-0

The DB9 female cable end which mates with the serial port connectors of connected devices will often have a pair of screw-down cable screws. These cable screws should be used to assure a solid connection of the cable with the device.

Default settings for the serial ports are 19200-baud, 8-bit word length, no parity, and one stop bit (19200, 8N1). Use the internal setup menu to adjust these settings.

Internal Modem

If a dialup POTS modem is installed, an RJ11 (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 on the bottom of the T830-0.

**DIP Switches**

The bank of 8 DIP switches on the back panel of the T830-0 are used to control the baud and parity settings of I/O2, to set the operational mode for I/O2, and to put the unit into “boot load mode” where it can be forced to load a new application (firmware image). The following table shows how to set the various DIP switches to obtain certain settings:

<b>I/O 2 Baud</b>	<b>SW1</b>	<b>SW2</b>
2400	OFF	OFF
9600	ON	OFF
19200	OFF	ON
115200	ON	ON
<b>I/O 2 Word, Parity</b>	<b>SW3</b>	
8N1	OFF	
7E1	ON	
<b>I/O 2 Mode</b>	<b>SW4</b>	
Command Mode	OFF	
Data Mode	ON	
<b>Boot Load Mode</b>	<b>SW8</b>	<b>SW1 thru SW7</b>
No Forced App Reload (Default)	OFF	X (don't care)
Forced Application Reload	ON	ON

➤ **Note:** Boot Load Mode can only be set by flipping ALL DIP switches to the ON or UP position. This is not a setting that can be configured via internal menu settings, or Setting Keys.

➤ **Note:** For settings that can be set either via DIP switch, internal menu settings, or Setting Keys, the T830-0 always pays attention to the last setting, regardless of how it was done. So if the internal setting for I/O2 Mode is Command, and someone flips SW4 to the ON or UP position, the Mode is immediately set to Data.

**Buttons**

The only button on the T830-0 is the Reset button located on the back panel next to the left of serial port I/O 2.

## Getting Connected

### Power Up Sequence

On startup, the T830-0 goes through the following boot sequence in approximately 55 seconds:

- 1) The power LED flashes once each second for 45 seconds.
- 2) Power LED will blink once every 5 seconds as a "heartbeat" while the T830-0 is powered on.

### Default Passwords

The T830-0 uses a very flexible system for managing users, passwords, and access rights. By default, the following four user profiles are enabled. Note that if a password is defined without a user name, the profile is defined just by the user name. All of the default profiles are password-only. All passwords are masked: \*\*\*\*\*

**>> Note:** User 11 is also preconfigured in the unit, for use by SitePath.

The default settings are configured to low security for your convenience in setup. It is highly recommended that you change these passwords and record them in a secure location.

User	Password	Login To
User1	SMDR	Command processor
User2	SUPER	Command processor
User3	ACCESS1	Passthrough/File 1
User4	ACCESS2	Passthrough/File 2

### The Status Screen

The T830-0 Status screen is the unit's one-stop informational source. Most of the information that a user would need to know about the unit is available through this display. This section outlines this data and highlights why it is useful.

```

TeleBoss 830 2.05.260 STD - Status
Site Name      : 830-830000857
Serial Number  : 830000857      Eth 1      : STATIC
Date          : MON 02/16/2009 IP Addr    : 0.0.0.0
Time         : 12:53:03        MAC Addr   : 00:10:A3:60:01:20
Memory       : 2048K           Eth 2      : STATIC
% Full Alarm  : OFF            IP Addr    : 0.0.0.0
No-Data Alarm 1 : OFF          MAC Addr   : 00:10:A3:60:01:21
No-Data Alarm 2 : OFF          Modem      : Yes
Duplex       : HALF
-----
Port   Baud/Etc.  Recs    Bytes    Full Wrap Name
IO1   : 19200,8N1 00000000 00000000 0% OFF I/O 1
IO2   : 19200,8N1 00000000 00000000 0% OFF I/O 2
COMPLETE
>
    
```

**TeleBoss 830-0** indicates that this product is the T830-0, followed by **2.05.260**, the currently loaded firmware version.

**Site Name** is the identifier assigned to each T830-0 by the end user in the General Settings menu.

**Serial Number** is the factory-assigned, unique serial number for this T830-0.

**Date** and **Time** display the current date and time.

**Memory** indicates the amount of flash memory configured for storage of data.

**% Full Alarm / No Data Alarm *n*** indicates the current ON/OFF status of the % Full Alarm, and No Data Alarms 1 and 2, respectively.

**Duplex** controls the echo settings for the command processor. Full duplex causes the T830-0 to echo all characters sent to the remote device. Half duplex turns off character echo.

**Eth 1** and **Eth 2** displays STATIC, or DHCP, depending on which mode each of the two Ethernet interfaces is configured for.

**IP Add** and **MAC Add** immediately following Eth 1 and Eth 2 are the network IP address assigned to each Ethernet card, and that cards MAC address. The MAC address of both Ethernet cards can also be found on the unit's serial number label.

**Modem** indicates whether the optional internal modem is installed.

The default serial port names of **I/O 1, 2, etc** are displayed for each of the installed serial ports along with the following information:

**Baud/Etc.** displays the baud rate, word length, parity, and stop bit settings for each installed serial port.

**Recs** shows the number of carriage return-delimited records stored within the file associated with each serial port.

**Bytes** displays the amount of storage allocated for the above records.

**Full** is a rough percentage indicator of how much data is stored in a particular file.

**Wrap** indicates the ON/OFF status of whether file wrapping is enabled on a particular port. When ON, a unit that is 100% full will overwrite the oldest buffered records with new ones.

**Name** displays the target name, which is an optional name given to the device connected to the port. This target name is used in event notifications and can be configured in the Serial Settings menu for each port.

# Setup Menu

## Overview

This section displays screen shots and descriptions taken from the command prompt menu system. However, the menu structure and options are the same as the web interface.

The Setup menu contains all of the configuration options available on the T830-0. It is organized in a logical tree structure with all settings classified under the following groups:

```
TeleBoss 830 - 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

Enter your Selection:
```

Each section in this chapter will go over one of the above setup branches, outlining the options within.

Press either <ESC> or <Enter> to go back one level in the menu tree, or <CTRL + C> to exit any menu and return to the command prompt.

Since this product allows for multiple simultaneous command processors, two administrators could conceivably change the same option at the same time, but due to the multitasking nature of the T830-0, the changes are processed in the order received.

The T830-0 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 a 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.

## Option Types

### String entry

There are several different types of inputs employed within the setup menu. The most common is the string type 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 an you 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".

### Alarm actions (action list)

Alarm actions have their own unique method of entry. Refer to the [Action List](#) section in the Features chapter for more information.

### Option list

The option list type is similar to the toggle type in that it has a list of options to choose from:

```
TeleBoss 830 - 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.

## Web Interface

The T830-0 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. Once you have enabled it through the network section of the setup menu, simply connect to <http://<IP address of T830-0>> or <https://<IP address of T830-0>> to use Secure Sockets Layer (SSL). See [Web Interface Settings](#) menu for further description.

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 prompt. Once logged in, the General Status screen will be displayed, with a menu bar across the top of the page that displays the same menu options as the command prompt menu system. From here, you can alter any setting in the same way you could via the prompt.

## Main Setup Menu

```
TeleBoss 830 - 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
```

[Network Settings](#) contains settings for network communication, SNMP, FTP, PPP, Email, and more.

[Serial Settings](#) contains settings pertaining to the function of each serial port.

[Modem Settings](#) contains modem init settings and modem-specific security options.

[Security Settings](#) contains all user profiles, RADIUS configuration, and general security settings.

[Alarm/Event Definitions](#) contains all of the settings that define events within the T830-0.

[Action Definitions](#) contains configurations for all of the actions possible when events are detected.

[General Settings](#) contains the site name, answer string, confirmation prompt, date/time, and other general settings.

[Event Log Settings](#) allows for configuration and displaying of the Events Log.

[Audit Log Settings](#) allows for configuration and displaying of the Audit Log.

## Network Settings

The Network Settings menu contains all of the options pertaining to network communication.

```
TeleBoss 830 - Network Settings
A) Ethernet Settings
B) Default Router                []
C) Name Resolution Settings
D) Telnet Duplex                 [FULL]
E) Inactivity Timeout           [0]
F) IP Record Collection Settings [GENERIC CLIENT]
G) Web Interface Settings       [ON]
H) SNMP Settings
I) FTP Settings
J) PPP Settings
K) Email Settings
L) Real-Time Socket Settings
M) Static Route Settings
N) DSL Settings
O) VPN Settings
P) CPE Settings
  Note: Changes to IP Address, Subnet Mask, or Router
        Address will not take effect until any open
        Telnet command processor sessions are ended.
```

[Ethernet Settings](#) displays the menu where you can configure each of the two Ethernet interfaces.

**Default Router** displays the configured default router (gateway) for the unit. Refer to the [Default Router](#) section in the Features chapter for more information.

[Name Resolution Settings](#) allows you to configure the IP addresses of up to two Domain Name Servers (DNS).

**Telnet Duplex** controls the echo settings for Telnet. Full duplex causes the unit to echo all characters sent to the remote device. Half duplex turns off character echo. Default setting is Full.

**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. Default setting is 0.

[IP Record Collection Settings](#) displays the IP Record Collection Settings menu where an IPRC protocol can be selected and configured to collect data from various types of IP-enabled switches.

[Web Interface Settings](#) displays the Web Interface Settings menu where you can toggle the web interface ON or OFF, set the session timeout (0 - 65535 minutes), and set the TCP port number for the web connection.

[SNMP Settings](#) displays the SNMP Settings menu where you can configure the SNMP community name, and spoofed PPP/Trap IP address.

[FTP Settings](#) displays the FTP Settings menu, where you can configure automatic FTP pushes of buffered data.

[PPP Settings](#) displays the PPP Settings menu, where you can configure settings for PPP Dialout and PPP Hosting.

[Email Settings](#) displays the Email settings menu, where you can configure the SMTP server address, Email domain name, and authentication parameters.



[Real-Time Socket Settings](#) 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.

[Static Route Settings](#) displays the Static Route Settings menu where you can configure static network routes.

[DSL Settings](#) displays the DSL Settings menu where settings are configured so the T830-0 can communicate using the optional ADSL Modem (not supported in T830-0).

[VPN Settings](#) displays the VPN Settings menu where settings are configured so the T830-0 can communicate with the optional Asentria SitePath secure, unified administration portal software.

[CPE Settings](#) displays the Customer Premises Equipment (CPE) Settings menu where up to 64 different networked devices can be configured to communicate with the optional Asentria SitePath secure, unified, administration portal software.

## **Ethernet Settings**

Ethernet Settings displays the following menu where each of the two installed Ethernet cards can be configured:

**» Security Note:** If the T830-0 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. The other security features are SSH, Strong Passwords, Challenge and Responses. Also shutdown unsecure connections such as Telnet and FTP.

```

TeleBoss 830 - Ethernet Settings
A) Ethernet 1
B) Ethernet 2

Enter your Selection: a

TeleBoss 830 - Ethernet 1 Settings
A) 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** toggles between STATIC or DHCP – whichever is appropriate for this Ethernet port. Default setting is STATIC.

**IP Address** is the network address assigned to this Ethernet card. Default setting is 0.0.0.0

**Subnet Mask** sets the network subnet mask provided by the network administrator. Default setting is 255.255.255.0

**Router Address** sets the router address provided by the network administrator. Default setting is 0.0.0.0

**NAT** is an ON/OFF toggle to enable Network Address Translation. Default setting is ON.

**» Note:** The T830-0 does not heed changes to network configurations while you are connected to a command processor via Telnet web interface, or SSH. 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.

## **Name Resolution Settings**

```

TeleBoss 830 - Name Resolution Settings
A) DNS Server 1 [0.0.0.0]
B) DNS Server 2 [0.0.0.0]
C) DNS Mode [MANUAL]

```

**DNS Server 1 / 2** 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, etc. Default setting for each DNS Server is 0.0.0.0.

**DNS Mode** toggles between MANUAL, ETH1-DHCP and ETH2-DHCP. Default setting is MANUAL.

### IP Record Collection Settings

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [OFF]
B) Store Collected Data In      [FILE1]
```

**IP Record Collection** selects and displays a configuration menu for each of the IPRC protocols that the T830-0 supports: Generic Server, Avaya Reliable Session Protocol, Alcatel OmniPCX, Cisco CallManager 4.x, Generic Client (supports Siemens HiPath 4000), Intecom Telari, Nortel BCM, Syslog, NEC NEAX2400, and Cisco CallManager 5.x. Default setting is OFF.

**Store Collected Data In** sets the data file in which to store records received via IPRC. Default setting is FILE1.

» **Note:** Refer to the [IPRC](#) chapter for a detailed explanation of IP Record Collection.

### Web Interface Settings

```
TeleBoss 830 Web Interface Settings
A) Enable Web Interface           [ON]
B) Web Session Timeout           [30]
C) Web Connection Port           [80]
```

**Enable Web Interface** is an ON/OFF toggle to enable the T830-0's internal web server. Default setting is ON.

**Web Session Timeout** sets the number of minutes (0 - 65535 minutes) a connection may remain idle before expiring. A setting of 0 means the connection will never automatically expire. Default setting is 30.

**Web Connection Port** is the TCP port through which the web connection is made. Default setting is Port 80.

Connect using ***http://<IP address of T830-0>*** or ***https://<IP address of T830-0>*** to use Secure Sockets Layer (SSL). 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 prompt. Once logged in, the General Status screen will be displayed, with a menu bar across the top of the page that displays the same menu options as the command prompt menu system.

» **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.

### SNMP Settings

```
TeleBoss 830 - SNMP Settings
A) SNMP Community                 [public]
B) PPP/Trap IP Address Spoofing   [0.0.0.0]
```

**SNMP Community** sets the SNMP community name to use. Default setting is Public. (Max length is 23 chars)

**PPP/Trap IP Address Spoofing** allows you to configure the IP address to be displayed in an SNMP trap sent over a PPP connection. If undefined, the T830-0 PPP IP is used. Default setting is 0.0.0.0

➤ **Note:** SNMP traps are *not* a guaranteed means of delivering notifications. Traps are a one-way 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 T830-0 has no way of recognizing this and resending the trap.

### FTP Settings

```
TeleBoss 830 - FTP Settings
A) FTP Push Enable           [OFF]
B) FTP Server Address       []
C) Username                  [Default FTP Username]
D) Password                  [*****]
E) Account                   []
F) Directory                 []
G) Minutes Between Push Attempts [1440]
H) Select Files to Push
I) Remote File Names
```

**FTP Push Enable** toggles between OFF and REGULAR. Default setting is OFF.

**FTP Server Address** is the IP address or host name of the FTP server to push to. (Max length 64 chars)

**Username / Password** defines the login credentials that are able to access the remote FTP server. (Max length Username is 126 chars) (Max length Password is 31 chars)

**Account** is a third login option used only on some FTP servers. Consult your network administrator to see if this is necessary. (Max length 126 chars)

**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. (Max length 253 chars)

**Minutes Between Push Attempts** sets the number of minutes (1 to 9999) between FTP push attempts. Default setting is 1440 minutes.

**Select Files to Push** displays the FTP File Selection menu where you can select which files are pushed by toggling ON or OFF. Default setting for all is ON, except for Audit Log, which is OFF.

```
TeleBoss 830 - FTP File Selection
A) Data File 1              [ON]
B) Data File 2              [ON]
C) Events File              [ON]
D) Audit Log                 [OFF]
```

**Remote File Names** 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/or unique sequence # to the file name.

```
TeleBoss 830 - 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** is an ON/OFF toggle to enable the addition of the file transfer date and/or time to the beginning of the name of each transferred file of data. Default setting is OFF.

**Include Sequence #s in Filename** 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. Default setting is OFF.

**Data File n / Events File** 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.

Once FTP Push has been configured, entering the **PUSHTEST** command 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.

### **PPP Settings**

```
TeleBoss 830 - PPP Settings
A) PPP Dialout Settings
B) PPP Hosting Settings
C) Route Test Settings
```

[PPP Dialout Settings](#) displays settings pertaining to making outbound PPP network connections.

[PPP Hosting Settings](#) displays settings for hosting a PPP connection.

[Route Test Settings](#) displays settings for network monitoring/PPP backup connection settings. This menu allows you to configure up to three IP addresses to ping on a regular basis. If any of the IPs are down, the unit will fall back to a PPP dialout in order to maintain reliable network connectivity for sending SNMP traps.

#### PPP Dialout Settings

```
TeleBoss 830 - PPP Dialout Settings
A) PPP Dialout Enabled           [OFF]
B) Telephone Number             []
C) User Name                     []
D) Password                      [*****]
E) Idle Connection Disconnect (sec) [60]
F) Maximum Retries               [3]
G) Carrier Detect Timeout (sec)  [60]
H) Login Sequence Timeout (sec)  [30]
I) Dialout Modem Init String     []
J) IP Address to Suggest         [0.0.0.0]
```

**PPP Dialout Enabled** is an ON/OFF toggle to enable PPP dialout. Default setting is OFF.

**Telephone Number** sets the phone number of the PPP host the T830-0 is to dial into. (Max length 48 chars)

**User Name / Password** sets the login credentials that are used to log into the PPP host. (Max length for each is 64 chars)

**Idle Connection Disconnect (sec)** 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. Default setting is 60 seconds.

**Maximum Retries** defines the maximum number of times to retry a failed connection. Default setting is 3.

**Carrier Detect/Login Sequence Timeout (sec)** configure standard login timeouts, from 0 to 65535 seconds. Default setting is 60 seconds for Carrier Detect, and 30 seconds for Login Sequence.

**Dialout Modem Init String** sets the modem initialization string. (Max length 48 chars)

**IP Address to Suggest** sets an IP to try to acquire, if defined. 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**

```
TeleBoss 830 - 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]
```

**PPP Hosting Enabled** is an ON/OFF toggle to enable inbound PPP connection hosting. Default setting is OFF.

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

**Local (Device) IP Address** sets the IP address of the T830-0 for the PPP session. Default is 192.168.105.1

**Remote (Caller) IP Address** sets the IP address of the calling device for the PPP session. Default is 192.168.105.2.

**Route Test Settings**

```
TeleBoss 830 - 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** is an ON/OFF toggle to enable route testing. Default setting is OFF.

**Minutes Between Tests** sets the number of minutes (0 – 65535) to wait between each round of testing. Default setting is 10 minutes.

**IP Address *n*** sets the hostnames or IP addresses to ping for the test.

**Email Settings**

```
TeleBoss 830 - Email Settings
A) SMTP Server Hostname/IP Address []
B) Email Domain Name             [asentria.com]
C) Authentication (LOGIN)        [OFF]
```

**SMTP Server Hostname/IP Address** sets the hostname or IP address of the outbound mail server. (Max length 64 chars)

**Email Domain Name** sets the *@domain\_name.com* to use when the T830-0 sends an Email. Default setting is "asentria.com". (Max length 48 chars)

**Authentication (LOGIN)** 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. Default setting is OFF.

```
TeleBoss 830 - Email Authentication Settings
A) Authentication Enabled      [OFF]
B) Username                   []
C) Password                   [*****]
```

**Authentication Enabled** is an ON/OFF toggle to enable Email authentication. Default setting is OFF.

**Username / Password** defines the login credentials. (Max length for each is 48 chars)

**Real-Time Socket Settings**

```
TeleBoss 830 - Real-Time Socket Setup
A) FILE1
B) FILE2
C) EVENTS

Enter your Selection: a

TeleBoss 830 - FILE1 Real-Time Data Socket Setup
A) Real-Time Socket Mode      [LISTEN]
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** can be toggled to LISTEN, PUSH, and OFF. When set to LISTEN this 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. Default setting is LISTEN.

**Show Answer String on Connection** is an ON/OFF toggle to enable the prompt indicating successful connection to the Real-Time Socket (RTS) port. Default setting is ON.

**Require Xon to Start Data Flow** is an ON/OFF toggle to enable the Xon/Xoff data flow control requirement. Default setting is OFF.

**Idle Connection Close Timer** 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. Default setting is 0.

**Close Socket When File Empty** is an ON/OFF toggle to set whether or not the T830-0 will automatically terminate the RTS connection when the file for this port has been emptied. Default setting is OFF.

**Real-Time Socket Push Hostname/IP** sets the hostname or IP address of the server where the unit will push the data if the RTS Mode is set to Push. (Max length is 64 chars)

**Real-Time Socket Push Port Number** sets the TCP port number the RTS push should use. Default setting is port 3000.

**Real-Time Socket Push Retry Timer** sets the number of minutes (1 – 255) to wait before retrying an RTS push that has previously failed. Default setting is 5 minutes.

## Static Route Settings

```

TeleBoss 830 - Static Route Settings
A) Route 1
. . .
H) Route 8

Enter your Selection: a

TeleBoss 830 - Static Route 1 Settings
A) Enable [OFF]
B) Destination Network [0.0.0.0/0]
C) Gateway [0.0.0.0]
D) Interface [NONE]

Enter your Selection:

```

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 gives you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different routes.

**Enable** is an ON/OFF toggle to enable a static route. Default setting is OFF

**Destination Network** is the network notation, i.e., w.x.y.z/s, where s is the significant bits. Default is 0.0.0.0/0.

**Gateway** is the IP address of the gateway. Default setting is 0.0.0.0

**Interface** toggles through all of the interfaces' available on this T830-0 – NONE, Ethernet 1, Ethernet 2, Dialup Modem PPP, and Wireless Modem PPP. Default is NONE.

Refer to the [Static Routes](#) section in the Features chapter for a detailed explanation of Static Routes.

## DSL Settings

```

TeleBoss 830 - DSL Settings
A) Start Mode [MANUAL]
B) Type [PPPOA]
C) VPI [0]
D) VCI [0]
E) Encapsulation [VCM]
F) Mode [BRIDGED]
G) Username []
H) Password [*****]
I) IP Address [0.0.0.0]
J) Mask [0.0.0.0]
K) Router [0.0.0.0]

```

**Note:** The T830-0 does not support the optional ADSL modem expansion card. This menu is still displayed, but changing any of the settings will not do anything and the settings are not discussed in this manual.

## VPN Settings

```

TeleBoss 830 - VPN Settings
A) VPN 1
B) VPN 2
C) Commissioning Settings

```

Following describes the menu options for configuring VPN Settings. These settings are only for use with the Asentria SitePath secure, unified administration portal software and set up is beyond the scope of this manual. Contact [Asentria Technical Support](#) for further information.

**VPN 1** and **VPN 2** display a sub-menu where each of two VPN connections can be configured.

**Commission Settings** displays a sub-menu where all the parameters for commissioning the T830-0 with the SitePath application are configured. Commissioning is the process of automatically configuring a unit and making SitePath aware of it at the same time.

### **CPE Settings**

```
TeleBoss 830 - 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:

TeleBoss 830 - CPE Settings
A) CPE 1 [0.0.0.0]
.. ..
P) CPE 16 [0.0.0.0]

Enter your Selection:

TeleBoss 830 - CPE 1 Settings
A) IP Address [0.0.0.0]
B) Name []
C) Description []
D) Alarm Keep-alive Period (seconds) [0]
E) Alarm Threshold [1]
F) Enable SitePath Access [ON]
```

Following describes the menu options for configuring CPE Settings. These settings are only for use with the Asentria SitePath secure, unified administration portal software and set up is beyond the scope of this manual. Contact [Asentria Technical Support](#) for further information.

**IP Address** sets the IP address of the CPE. Value is a dotted quad IP address. Default setting is 0.0.0.0

**Name** sets the name given to the CPE. The only restriction on the name is that it cannot have any double or single quotes ( ' or " ) in it. (Max length is 24 chars)

**Description** sets a description of what the CPE device is. The only restriction on the description is that it cannot have any double or single quotes ( ' or " ) in it. (Max length is 64 chars)

**Alarm Keep-alive Period (seconds)** set the number of seconds between periodic pings (ping cycle) sent by the T830-0 to the CPE to make sure it is "alive". 1 ping frame is transmitted per CPE per ping cycle. Values are: 0 to 65535. Default setting is 0.

**Alarm Threshold** 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. Default setting is 1.

**Enable SitePath Access** is an ON/OFF toggle to enable SitePath to communicate with the CPE through the unit.



## Serial Settings

```
TeleBoss 830 - Serial Settings
A) 1-I/O 1 Settings
B) 2-I/O 2 Settings
```

» **Note:** Both serial ports can be set to function in Data mode, and I/O 2 can also be set to function in one of two other modes: Command and Inline. Default is Command Mode. Therefore the I/O 2 Settings menu has all the options of I/O 1, plus a few others that I/O 1 does not have. Those options that are exclusive to I/O 2 will be indicated as such below.

```
TeleBoss 830 - Serial Settings
A) 1-I/O 1 Settings
B) 2-I/O 2 Settings

Enter your Selection: b

TeleBoss 830 - 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) Inline Mode Handshaking    [XON/XOFF]
O) Strip Sent Pass-Through LFs [OFF]
P) Strip Received Pass-Through LFs [OFF]
Q) Disable Serial Setup via DIP Switch [OFF]
R) Data Type                  [ASCII]
S) Change ETX to CR/LF        [OFF]
```

**Target Name** is the name given to the device connected to the other end of each port. The target name is used in event notifications. Default setting is I/O n. (Max length is 24 chars)

**Baud Rate** displays a selection menu for baud rates available for the port. These values range from 300 baud to 115200 baud. Default setting is 19200.

**Data Format** toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, 7N1, and 8O2. Default setting is 8N1.

**Handshaking** is a toggle item with the following options: None, Xon/Xoff, Both, and DTR. Default setting is None.

**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. Default setting is OFF.

**Record Stamping** displays a menu that allows you to select whether the Date/Time and/or the Unit ID are pre-pended to each incoming data string. Default setting for Date/Time and Unit ID is OFF.

**Character Masking** 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. Default setting is ON.

**Data Alarm Enable** is an ON/OFF toggle to enable data alarm monitoring for this port. Default setting is OFF.

**Store Data To** displays a menu that allows you to toggle ON/OFF the files to which incoming data on this port should be stored, if any.

**Store Alarms During Pass-Through** 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. Default setting is OFF.

**Duplex (Port 2 only)** 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. Default setting is FULL.

**Inactivity Timeout (Port 2 only)** is the time (1 - 255 minutes) before a serial connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. Default setting is 0.

**Port Mode** sets the port function. This is set to DATA for I/O 1 and cannot be changed. This can be toggled between COMMAND, DATA, and INLINE for I/O 2. COMMAND allows for serial command processor access, DATA configures the port as an inbound data port just like I/O 1, and INLINE causes the unit to perform a direct connection between I/O 1 and I/O 2.

**Inline Mode Handshaking (Port 2 only)** toggles the handshaking method used during Inline mode operation. Available options are XON/XOFF, DTR, and Both. Default setting is XON/XOFF.

**Strip Sent Pass-Through LFs** is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data *sent out* of the T830-0. Default setting is OFF.

**Strip Received Pass-Through LFs** is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data *received* by the T830-0. Default setting is OFF.

**Disable Serial Setup via DIP Switch** is an ON/OFF toggle to disable the DIP switches. Default setting is OFF.


**Data Type** toggles between ASCII and Binary to indicate the type of data being collected on this port. Default setting is ASCII.

**Change ETX to CR/LF** is an ON/OFF toggle to set whether ETX characters in the incoming data should be converted to CR/LF characters. Default setting is OFF.

## Modem Settings

```
TeleBoss 830 - Modem Settings
A) Dialup Modem
B) Wireless Modem
```

The Modem Settings menu displays two sub-menus for configuring either the internal 56K modem, or a optional wireless modem expansion card.

 **Note:** The T830-0 does not support the optional wireless modem expansion card. This menu is still displayed, but changing any of the settings will not do anything and the settings are not discussed in this manual.

### Dialup Modem

```
TeleBoss 830 - 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 [0]
```

➤ **Note:** If the optional 56K dialup modem is not installed in the T830-0, this menu is displayed, but changing any of the settings will not do anything.

**Data Format** toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, and 7N1. Default setting is 8N1.

**Duplex** controls the echo settings for the modem command processor. Full duplex causes the T830-0 to echo all characters sent to the remote device. Half duplex turns off character echo. Default setting is FULL.

**Init String** 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. Default setting is ATM1. (Max length 126 chars) Note: Make sure to enter 'AT' at the beginning of this initialization string.

**Inactivity Timeout** 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. Default setting is 0.

**Upon Modem Connect Go Directly To** 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 passthrough mode, the command processor of the T830-0 is transparent. Default setting is LOGIN.

**TAP Init String** is the user-defined modem initialization string used only when the modem is making an alphanumeric modem callout. Default setting is ATM0. (Max length 126 chars) Note: Make sure to enter 'AT' at the beginning of this initialization string.

**TAP Uses 8N1 Data/Parity/Stop** toggles between 1, to force the TAP initialization string data/parity/stop settings to 8N1, and 0 to not force this setting. Default setting is 0.

**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.

## Security Settings

```
TeleBoss 830 - Security Settings
A) Security Mode [USER PROFILES]
B) Specific Security Settings
C) General Security Settings

Enter your Selection:
```

The Security Settings menu displays options for setting the security mode, as well as specific and general security settings.

**Security Mode** toggles between `USER PROFILES` and `RADIUS` to determine which Specific Security Settings menu to be displayed.

**Specific Security Settings** menu is 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. Default setting is `USER PROFILES`.

[General Security Settings](#) displays a menu with options that apply to **every** user of this T830-0.

**Specific Security Settings – User Profile Security Settings**

```

TeleBoss 830 - User Profile Security Settings
A) User 1: User1/*****/COMMAND/FILE1
B) User 2: User2/*****/COMMAND/FILE1
C) User 3: User3/*****/PASSTHROUGH/FILE1
D) User 4: User4/*****/PASSTHROUGH/FILE2
E) User 5:
F) User 6:
G) User 7:
H) User 8:
I) User 9:
J) User 10:
K) User 11: admin/*****/COMMAND/FILE1
L) User 12:
M) Authentication Settings
    
```

[User n](#) displays the configuration menu for each user profile.

**» Note:** User 11 is preconfigured in the unit, for use by SitePath.

[Authentication Settings](#) displays a menu of global authentication options.

**» Note:** Passwords are case sensitive and 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 username, and an invalid or duplicate username is entered, the T830-0 responds as follows:

```

Invalid Entry.
Press any key to continue...
    
```

**» Note:** When configuring a new password, the T830-0 will ask you to re-enter the password. If the second entry of the password does not match the first, the T830-0 responds as follows:

```

Invalid Entry - Confirm Password does not match.
Press any key to continue...
    
```

**User Setup Menu**

```

TeleBoss 830 - User Setup Menu
A) Enable This User Access           [ON]
B) User Name                         [User1]
C) Password                         [****]
D) Allow User Connection via         [LMTFRSs]
E) Upon Login then Go To            [COMMAND]
F) Set Access/Pass-through Pointer To [FILE1]
G) Pass-through Permissions
H) After PT, ESC Takes User To      [MENU]
I) PPP Connection                   [LOCAL]
J) Setup/Status Rights              [ADMIN1]
K) File Release Permissions
L) File Delete Permissions
    
```

**Enable This User Access** is an ON/OFF toggle to enable access for this user profile.

**User Name / Password** sets the username and/or password for this profile. (Max length for each is 31 chars)

**Allow User Connection via** displays a menu allowing you to toggle ON or OFF access via Local (Console Port), Modem, Telnet, FTP, Real-Time Socket, and SSH (Secure Shell). These are abbreviated: LMTFRSs and default setting for all is ON.

**Upon Login then Go To** toggles the action this user will be directed to upon logging in, with the following options: Command, Menu, and Passthrough as shown here:

#### Command

```
TeleBoss
Password: *****
READY
>
```

#### Menu

```
TeleBoss 830 Version 2.05.260 at 830-830000050

1. Pass-Through to I/O 1
2. Pass-Through to I/O 2
P. 830 Command Prompt
M. 830 Setup Menu
S. 830 Status Menu
X. Exit (end connection)
```

#### Passthrough

```
TeleBoss
Password: *****
Connected to I/O 1
```

**Set Access/Pass-through Pointer To** is in effect if the “Upon Login then Go To” action is set to Passthrough. This option toggles the serial port the user will be routed to. Default setting is FILE1.

**Pass-through Permissions** 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 toggles ALLOW or DENY for each port as needed. If a port is set as ALLOW, then that serial port 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. Default setting for all ports is ALLOW.

**After PT, ESC Takes User To** sets the action this user can perform when they exit out of a pass-through connection.

**PPP Connection** toggles between LOCAL and NONE. LOCAL allows PPP access, but denies all routing to whatever LAN the T830-0 is connected to. NONE disables PPP access for the user.

**Setup/Status Rights** 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 Rights Table](#) for more information on each access level. Default setting is MASTER.

**File Release / Delete Permissions** displays a menu showing all data files, Events Log and Audit Log, and toggles ALLOW or DENY for each as needed. Default setting for all is ALLOW.

## Authentication Settings

```

TeleBoss 830 - 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 210x Requires Password [OFF]
E) TCP/IP Port 220x Requires Password [OFF]
F) Username and/or Password Required [PASSWORD ONLY]
    
```

Authentication Settings set parameters for passwords and security that are required for **every** user who attempts to log into the T830-0.

**Local Command Requires Password** is an ON/OFF toggle to set whether a password for I/O 2 users is required. Default setting is OFF.

**Modem Callin Requires Password** is an ON/OFF toggle to set whether a password for modem users is required. Default setting is OFF.

**TCP/IP Port 23 Requires Password** is an ON/OFF toggle to set whether a password for Telnet (port 23) users is required. Default setting is ON.

**TCP/IP Port 210x Requires Password** is an ON/OFF toggle to set whether a password for passthrough (port 210x) users is required. Default setting is OFF.

**TCP/IP Port 220x Requires Password** is an ON/OFF toggle to set whether a password for Real-Time Socket (port 220x) users is required. Default setting is OFF.

**» Note:** When any of the above options is set to OFF, users connecting via that method are automatically granted all access.

**Username and/or Password Required** toggles between: PASSWORD ONLY, USERNAME/PASSWORD (PW), or PASSWORD(PW)/USERNAME. Default setting is PASSWORD ONLY.

### Specific Security Settings – RADIUS Security Settings

```

TeleBoss 830 - RADIUS Security Settings
A) Primary Server []
B) Primary Secret []
C) Secondary Server []
D) Secondary Secret []
E) Fallback Mode [NONE]
F) Authentication Port [1812]
G) Accounting Port [1813]
H) CHAP [OFF]
I) Timeout [3]
J) Retries [3]
    
```

**Primary / Secondary Server** sets the IP Address or host name of the primary and secondary RADIUS server.

**Primary / Secondary Secret** sets the secret for the primary and secondary RADIUS server. The secret is used to authenticate RADIUS network traffic. (Max length for each is 16 chars)

**Fallback Mode** 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. Default setting is NONE.

**Authentication Port** sets the UDP port (1 – 65535) that the RADIUS server uses for authentication/authorization. Default port is 1812.

**Accounting Port** sets the UDP port (1 – 65535) that the RADIUS server uses for accounting traffic. Set to 0 to disable RADIUS accounting. Default port is 1813.

**CHAP** 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). Default setting is OFF.

**Timeout** sets the number of seconds (1 – 30) the unit waits for a response from the RADIUS server. Default setting is 3.

**Retries** 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.) Default setting is 3.

» **Note:** For a complete description and explanation of RADIUS security, please refer to the [RADIUS Security](#) section in the Features chapter.

### **General Security Settings**

```
TeleBoss 830 - Global Password/Security Settings Menu
A) Show Username/Password Prompt      [OFF]
B) Globally Allow Access via          [MTRFSs]
C) Button Tap Allows Console Access   [ON]
```

Global Password/Security Settings set security options that are required for **every** user who attempts to log into the T830-0.

**Show Username / Password Prompt** is an ON/OFF toggle to set whether a prompt for logging in is displayed. Default setting is OFF.

**Globally Allow Access via** 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: MTRFSs. Default setting for all is ON.

**Button Tap Allows Console Access** 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 front-panel LEDs will flash briefly for several seconds, giving the user immediate Console access (via I/O 2) using the default MASTER username and password. Refer to the [Securing a TeleBoss 830-0/Button Unlock](#) section for more details about this. Default setting is ON.

### **Alarm/Event Definitions**

» **Note:** Refer to the [Data Events](#) section in the Features chapter for an example-driven approach to defining alarm definitions.

```
TeleBoss 830 - 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) Percent Full Alarm Settings        [OFF]
G) Scheduled Event 1 Settings          [OFF]
H) Scheduled Event 2 Settings         [OFF]
I) CPE Alarm Settings
J) Data Filter Action                 [REJECT]
K) Event Message Settings
```

[Class Table](#) displays the menu for configuring event classification settings.

[Data Alarm/Filter Settings](#) displays the menus for configuring serial data event monitors.

[EventSensor Device Settings](#) displays the menus for configuring internal sensors and any Type 2 Event Sensors that may be connected via the SensorJack Port.

[No-Data n Alarm Settings](#) displays the menus for configuring alarms based on period of time when no-data is received on a specific serial port.

[Percent Full Alarm Settings](#) displays the menu for configuring alarms based on how full the call record database of the T830-0 is.

[Scheduled Event n Settings](#) displays the menus for configuring alarm notifications for specific times and days of the week.

[CPE Alarm Settings](#) displays the menu for configuring “CPE Down” events. These are used in conjunction with devices managed by the Asentria SitePath application.

**Data Filter Action** toggles between REJECT and ACCEPT to indicate whether data filters are configured to reject or accept specific incoming data string(s). Default setting is REJECT.

[Event Message Settings](#) displays the menu that permits customization of the event message that appears in traps, Emails, pages, etc.

### **Class Table**

TeleBoss 830 - Class Table	
A) Class 1	[Info]
B) Class 2	[Minor]
C) Class 3	[Major]
D) Class 4	[Critical]
E) Class 5	[]
...	
L) Class 12	[]

**Class n** defines the event classification assignable to events detected by the T830-0. (Max length 47 chars)

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 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**

TeleBoss 830 - 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](#) displays the menu for configuring up to 16 data alarm fields.

[Data Alarm Macro Settings](#) displays the menu for configuring up to 100 macros to be used for data alarming.

[Data Alarm/Filter Settings](#) displays the menu for configuring up to 200 data alarms or filters.

**Display Alarm Status** displays real time information on data event monitors you've configured.



**Exit Upon True Data Alarm** is an ON/OFF toggle to set whether the T830-0 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.

### Data Alarm Field Settings

```

TeleBoss 830 - Data Alarm Field Definition Table
      Start   Length   Type      Name
A) Definition A      0       0    [Alpha]
B) Definition B      0       0    [Alpha]
...
P) Definition P      0       0    [Alpha]

Enter your Selection: a

TeleBoss 830 - Data Alarm Field Definition
Data Field: A
A) Start Position                [0]
B) Field Length                   [0]
C) Field Name                     []
D) Field Type                     [Alpha]

Enter your Selection:


```

**Start Position** sets the number of the characters to begin a particular alarm field starting from position 1. Field definition is disabled if set to 0.

**Field Length** sets the length of this particular alarm field.

**Field Name** 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 its field letter (A,B, etc...).

**Field 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. Default setting is Alpha.

 **Note:** The T830-0 does not perform error checking to ensure that no two fields have the same name. Please make sure your fields all have unique names to avoid conflicts.

### Data Alarm Macro Settings

```

TeleBoss 830 - Data Alarm Macro Settings
A) Macro 1                      []
B) Macro 2                      []
...
P) Macro 16                     []
Q) Next Macro Page

Enter your Selection: a

TeleBoss 830 - Settings for Data Alarm Macro 1
A) Name                         []
B) Equation                     []

```

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 Macros](#) section in the Features chapter for more information.

Data Alarm/Filter Settings

```

TeleBoss 830 - Data Alarm/Filter Settings
A) Alarm/Filter Page 1 (Alarms 1-16)
B) Alarm/Filter Page 2 (Alarms 17-32)
. . .
L) Alarm/Filter Page 12 (Alarms 177-192)
M) Alarm/Filter Page 13 (Alarms 193-200)

Enter your Selection:
    
```

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). This will display a menu where you can select from those 16 data alarm options as follows:

```

TeleBoss 830 - 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]

Enter your Selection:
    
```

[Alarm/Filter n](#) displays the menu where an individual data alarm or filter can be configured.

**Next or Previous Alarm/Filter Page** displays either the next or previous set of 16 Data Alarm/Filters.

**Setup Alarm/Filter Fields** displays 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** displays real time information on data event monitors you've configured.

**Exit Upon True Data Alarm** is an ON/OFF toggle to set whether the T830-0 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.

Data Alarm/Filter n Settings

```

TeleBoss 830 - 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** is an ON/OFF toggle to enable each individual data event. Default setting is OFF.

**Alarm/Filter Mode** toggles between Alarm and Filter to indicate whether the T830-0 will recognize this data event as an Alarm and take some action, or as a Filter and either accept or reject the data string. Default setting is ALARM.

**Alarm/Filter Name** sets the name for the event monitor. This name is reported with the specified actions. (Max length 16 chars)

**Alarm/Filter Equation** defines the event equation using the event fields defined in the previous menu. (Max length 160 chars) Refer to the [Configuring Data Alarm Equations](#) section in the Features chapter for more information.

**Threshold** 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** is an ON/OFF toggle to control whether the unit will clear the event counter each time the threshold is met. Default setting is ON.

**Alarm Counter Clear Interval** sets 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. Default setting is 12 Hours.

**Alarm Counter Reset Time** 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. Default setting is 00:00.

**Actions** 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.

**Class** sets 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 data alarm.

**Data Alarm Trap Number** sets the number to be sent with any SNMP traps for this event. Default is 503, but trap number can also be set in the range of 1000 – 1199 as needed.

**Clear This Alarm Counter Now** 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.

#### Actions List

```

Enter one or more actions using this format:
(For more details see the users manual)
-----
Cancel : cancel(idname)
Dialup Pager : dpage(index)
Dispatcher : dispatch(phone# or index)
Email : email(email or index)
Group : group(groupname)
ID : id(id name)
Malert : malert(phone# or index)
Modem : modem(phone# or index)
Postpone : postpone(idname, seconds)
Pause : pause(seconds)
Relay : relay(action, eventsensor, point)
Talert : talert(ipaddress or index)
Trap : trap(ipaddress or index)
(separate multiple actions using semicolon)

Current Actions:
Enter Actions:

```

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. It's comprised of a list of keywords and parameters separated by semicolon. Each keyword specifies a certain action and has its own parameter set, which is enclosed in parentheses. Refer to [Action List](#) in the Features chapter for more information.

### Type 2 EventSensor Settings

The Sensor Events Menu is used to configure and control both internal serial port contact closures, and external Type 2 EventSensors connected to the SensorJack Port. Each serial port can function as a contact closure with the optional adapter available from Asentria, but these are not commonly used. If you don't use the internal serial port contact closures, or external Type 2 EventSensors, this menu will be unpopulated. Because various Type 2 EventSensor configurations are possible, menus shown in this section probably will not look exactly like the ones for your T830-0. (The menu below shows a T830-0 with 2-CC, which represents the two serial ports that could be configured as contact closures and two Type 2 EventSensors – an ES-T in slot 1, and an ES-TH in slot 2.)

```

TeleBoss 830 - Sensor Events Menu
  Name          ID          Alive      Number      Configuration
A) INTERNAL    -----    -          200         2-CC
B) Type2 ES-T    01100000    Y          1           1-TS
C) Type2 ES-TH    08110000    Y          2           1-TS 1-HS
D) <none>
. . .
Q) <none>
R) Sensor Unresponsive Settings
    
```

[EventSensor Slots](#) (A thru Q) displays the settings menu for each ES.

[Sensor Unresponsive Settings](#) displays the Sensor Unresponsive Menu where you can configure the actions the T830-0 takes if an ES becomes unresponsive.

#### EventSensor Slots

```

TeleBoss 830 - External Events Menu
Device Number: 1      Device ID: 01100000
A) Device Name                [Type2 ES-T]
B) Temperature Sensor
C) Clear Settings for This EventSensor
    
```

The display for each EventSensor (ES) will vary depending on configuration. For example, an ES could be either internal or external. EventSensors can be configured with varying combinations of I/O types.

**➤ Note:** As of the publishing date for this manual, only Temperature (ES-T) and Temperature/Humidity (ES-TH) Type 2 Event Sensors are available.) Refer to the [Type 2 EventSensor Configuration Setup](#) section in the Features chapter for more information.

#### Sensor Unresponsive Settings

```

TeleBoss 830 - 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** sets the time (10 - 65535 seconds) to wait before declaring a non-communicative EventSensor unresponsive. Default setting is 30.

**Sensor Unresponsive Actions** 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 [Action List](#) in the Features chapter for more information.

**Sensor Unresponsive Trap Number** sets the number to be sent with any SNMP traps for this event. Default is 50, but trap number can also be set in the range of 1000 – 1199 as needed.

**Sensor Unresponsive Class** sets 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 alarm.

### **No-Data *n* Alarm Settings**

No Data Alarms can be configured on the T830-0 to monitor data coming in via the serial ports, and take an alarm action if a certain period of time passes with no data.

```

TeleBoss 830 - 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             []

```

**No-Data *n* Alarm Settings** allows 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.

**Alarm Enable** is an ON/OFF toggle to enable the no-data monitor. Default setting is OFF.

**Alarm Actions** 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 [Action List](#) in the Features chapter for more information.

**Alarm Message** sets the text string to be delivered with this event’s alarms. Default setting is “No-Data Timeout *n*”. (Max length 126 chars)

**Alarm Class** sets 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** sets the number to be sent with any SNMP traps for this event. Default is 505, but trap number can also be set in the range of 1000 – 1199 as needed.

**Schedule *n* Begin Time/End Time** sets the beginning and ending times (24 hr clock) for each of two ranges of time.

**Schedule *n* Duration** is the number of minutes (0-65535) the unit will wait without receiving data before alarming.

**Apply Alarm on Days** 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. Default setting is ON for Monday thru Friday, and OFF for Saturday and Sunday.

**Enable Ports** 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. Default setting is OFF for all ports.

**Add Exclusion / Delete Exclusion** 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, 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. 15 dates can be entered to be excluded.

**Percent Full Alarm Settings**

```
TeleBoss 830 - Percent Full Alarm Settings
A) Alarm Enable [OFF]
B) Percent Full Threshold [80]
C) Alarm Actions []
D) Alarm Message [DB Exceeds Threshold]
E) Alarm Class [Info]
F) Trap Number [501]
```

**Alarm Enable** is an ON/OFF toggle to enable the percent full alarm. Default setting is OFF.

**Percent Full Threshold** set the percent full level at which the alarm will be triggered. Default setting is 80 percent.

**Alarm Actions** 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 [Action List](#) in the Features chapter for more information.

**Alarm Message** sets the text string to be delivered with the percentage full alarm. Default setting is DB Exceeds Threshold. (Max length 111 chars)

**Alarm Class** sets 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 percent full alarm.

**Trap Number** sets the number to be sent with any SNMP traps for this event. Default is 501, but trap number can also be set in the range of 1000 – 1199 as needed.

**Scheduled Event Settings**

Scheduled Events allow you to schedule specific a specific date/time for an alarm action to occur. For example, you might want the T830-0 to send you an Email every morning at 8:00 just so you know it is live on the network.

```
TeleBoss 830 - 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
[]
[]
```

**Scheduled Event n Setup** 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 Event** is an ON/OFF toggle to enable the Scheduled Event. Default setting is OFF.

**Event Actions** 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 [Action List](#) in the Features chapter for more information.

**Event Message** sets the text string to be delivered with this event's action. Default setting is "Scheduled Event *n*". (Max length 126 chars)

**Event Class** sets 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** sets the number to be sent with any SNMP traps for this event. Default is 506, but trap number can also be set in the range of 1000 – 1199 as needed.

**Event Time *day*** sets 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.

**Add Exclusion/Delete Exclusion** 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. 15 dates can be entered to be excluded.

### **CPE Alarm Settings**

TeleBoss 830 - 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]

These settings are only for use with Customer Premises Equipment (CPE) managed via the Asentria SitePath secure, unified administration portal software. Contact [Asentria Technical Support](#) for further information.

**Alarm Enable** is an ON/OFF toggle to enable the CPE Down Event. Default setting is OFF.

**Alarm Actions** 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 [Action List](#) in the Features chapter for more information.

**Alarm Trap Number** sets the number to be sent with any SNMP traps for this event. Default is 511, but trap number can also be set in the range of 1000 – 1199 as needed.

**Alarm Class** sets 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 alarm.

**Return to Normal Actions** 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 [Action List](#) in the Features chapter for more information.

**Return to Normal Trap Number** 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 CPR Down Events is 511, but any number in the alternate range of 1000 – 1199 can be used.

**Return to Normal Class** sets 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 event.

## Event Message Settings

TeleBoss 830 - Event Message 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]

**Include Date and Time / Site Name / Sensor ID / User Defined Name / User Defined State** are each ON/OFF toggles to permit customization of the event message that appears in SNMP traps, Emails, pages, etc. sent by the T830-0. Default setting for each is ON.

## Action Definitions

TeleBoss 830 - Actions Definition Menu	
A) Hostname/IP Address 1	[]
B) Hostname/IP Address 2	[]
C) Hostname/IP Address 3	[]
D) More Hostnames/IP Addresses	[]
E) Email Address 1	[]
F) Email Address 2	[]
G) Email Address 3	[]
H) More Email Addresses	[]
I) Phone Number 1	[]
J) Phone Number 2	[]
K) Phone Number 3	[]
L) Phone Number 4	[]
M) Pager Number 1	[]
N) Pager Number 2	[]
O) Pager Number 3	[]
P) Pager Number 4	[]
Q) Action Settings	[]

This menu is where you configure all of the actions possible when events are detected.

**Hostname/IP Address *n*** sets the hostname or IP address of the device(s) receiving SNMP Traps. The number (1,2,3) corresponds to the “index” number for Traps as discussed in the [Action List](#) section of the Features chapter.

**More Hostnames/IP Addresses** displays the Hostname/IP Address Definition Menu where three more hostnames or IP Addresses (index 4,5,6) can be configured.

**Email Address *n*** sets the Email address of the person(s) receiving Email alerts. The number (1,2,3) corresponds to the “index” number for Email alerts as discussed in the [Action List](#).

**More Email Addresses** displays the Email Address Definition Menu where three more Email Addresses (index 4,5,6) can be configured.

**Phone Number *n*** sets the phone number (index 1,2,3,4) to call for each dispatch, malert or modem callout as discussed in the [Action List](#).

**[Pager Number \*n\*](#)** displays the Pager *n* Settings menu where each of four individual pager settings (index 1,2,3,4) can be configured.

**[Action Settings](#)** displays the Action Settings menu where specific settings to manage actions can be configured.



**Pager Number *n***

TeleBoss 830 - 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** toggles between NUMERIC and ALPHA to set the type of pager being called.

**Pager Callout Number** sets the phone number for the pager.

**Pager ID** is used only with paging systems where many pagers share the same phone number. This is common with alphanumeric pagers. (Max length is 19 chars)

**Numeric Message** sets the series of digits (typically callback number) sent to a numeric pager. (Max length is 19 chars)

**Post Callout Delay** sets the number of seconds (0 to 255) the unit will wait before sending the pager ID. Default setting is 15 seconds.

**Post ID Delay** sets the number of seconds (0 to 255) the unit will wait before sending any message data. Default setting is 5 seconds.

**Action Settings**

TeleBoss 830 - 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** sets the total number of times to attempt dispatch, Malert or modem callouts if previous attempts fail. Default setting is 5.

**Callout Delay** sets the time in seconds (0 - 400) to wait between callout attempts. Default setting is 60 seconds.

[Action Schedule](#) displays the Action Schedule Settings menu where actions can be limited to defined days and times.

**Reminder Interval** 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. Default setting is 120 minutes.

**Asentria Alarm Version** toggles between 1.1 and 1.0 to indicate which type of Asentria Alarm notification will be displayed. Refer to the [Types of Alarm Notices](#) section in the Features chapter for a detailed explanation of Asentria Alarms. Default setting is 1.1.

**Require AsentriaAlarm ACKs** 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 T830-0 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 T830-0. Refer to the [Types of Alarm Notices](#) section for more information about CRC and non-CRC modes. Default setting is OFF.

## Action Schedule

```

TeleBoss 830 - 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** is an ON/OFF toggle to enable the action schedule. Default setting is OFF.

**Begin Time / End Time** sets the beginning and ending times (24 hr clock) during which alarm actions can be taken. Default settings are 08:00 (Begin Time) and 17:00 (End Time).

**Weekdays Only** toggles whether actions are only performed Monday thru Friday. Default setting is ON.

## General Settings

```

TeleBoss 830 - General Settings
A) Site Name                   [830-830000085]
B) Answer String               [TeleBoss]
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) Legacy Settings
    
```

**Site Name** sets the name assigned to this T830-0. 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. (Max length 40 chars) Default setting is "830 - <serial number>"

**Answer String** sets the string that is presented when a user connects to the T830-0 via Telnet or modem. (Max length 31 chars) Default setting is TeleBoss.

**Escape Key** is the decimal ASCII character code of the key you must press three times to escape from passthrough or other transparent modes. Default is 27, the <ESC> key.

**Confirmation Prompt** 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. If there is no response within 30 seconds, the T830-0 will cancel the command. Default is ON.

**Time Stamp Format** toggles through three options for how time stamps are formatted: HH:MM, HH:MM:SS, or Blank. Default setting is HH:MM.

**Date Stamp Format** toggles through four options for how date stamps are formatted: MM/DD, MM/DD/YY, MM/DD/YYYY, or Blank. Default setting is MM/DD.

**Space After Date/Time Stamp** is an ON/OFF toggle to set whether a space is appended to the end of the Date/Time stamp. Default setting is ON.

**Prompt** sets the character(s) or settings values displayed as the command line prompt. Refer to the [Customizable Command Prompt](#) section in the Features chapter for more information. (Max length 63 chars)

[Date/Time Setup](#) displays the System Date/Time menu where you can manage the clock, daylight savings control, and configure a networked time server.

[Legacy Settings](#) displays a menu for configuring legacy products that may be connected to the T830-0.

**Date/Time Settings**

```

TeleBoss 830 - System Date/Time
A) Current Date           [01/26/2009]
B) Current Time           [09:53:39]
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** sets the date. The unit automatically calculates the day of the week to display on the Status screen.

**Current Time** sets the time (24 hr clock).

**» Note:** The date and time settings are maintained by means of an internal battery backup when power is removed from the T830-0.

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

A brief explanation of daylight savings time (effective 2007): 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)** sets the number of hours the current time zone is offset from GMT. Valid input ranges from 0 to 12. Default setting is 8 hours.

**GMT Difference Direction** sets 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. Default setting is BEHIND.

**Enable Time Protocol** toggles between OFF, SIMPLE, and NTP.

**SIMPLE** - With network time 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** – With network time 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** displays a menu where the hostname or IP address of six time-servers can be configured. (Max length 64 chars) The T830-0 uses the following servers by default:

- time.nist.gov - 192.43.244.18 - Boulder, CO
- time-b.nist.gov - 129.6.15.29 - Gaithersburg, MD

## Legacy Settings

```

TeleBoss 830 - Legacy Settings
A) Release Compressed           [OFF]
B) Autodelete After Polling     [OFF]
C) Wait for NEXT                [OFF]
D) Omit END DATA               [OFF]
E) Line Tag                     [OFF]
F) Release Mode                 [LINE]
G) CBB DLE Stuffing            [OFF]
H) CBB Retransmits             [5]
I) CBB Timeout                 [15]
    Note: These settings are for support of older systems and
          should NOT be used for new implementations. We do
          not guarantee that these settings will be present in
          future versions or products.
    
```

**Released Compressed** is an ON/OFF toggle to enable release of data in a compressed or uncompressed format. Default setting is OFF.

**Autodelete After Polling** is an ON/OFF toggle to enable the deletion of data from the call record database once it has been polled. Default setting is OFF.

**Wait for NEXT** is an ON/OFF toggle that causes the unit to wait for the NEXT command before sending data once the RL command has been issued. Default setting is OFF.

**Omit END DATA** is an ON/OFF toggle that causes the unit to send or omit the string "END DATA" when a command processor poll is complete. Default setting is OFF.

**Line Tag** is an ON/OFF toggle that adds or omits the serial number line tags on each line of stored data. Default setting is OFF.

**Release Mode** toggles the following modes of releasing stored data: LINE, XMODEM, and CBB. Unless your application specifically uses XMODEM or CBB, leave this set to the default setting of LINE.

**CBB DLE Stuffing/Retransmits/Timeout** are specific configuration options for polling via Compressed Binary Block (CBB) mode. CBB is a release method included for compatibility and is not otherwise documented in this manual.

## Event Log Settings

The Event Log is a record of all data events that occur within the T830-0.

```

TeleBoss 830 - 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 [OFF]
H) Prepend Data Alarm Name     [OFF]
    
```

**List Events File** displays the contents of the Events file, if any records exist.

**Clear Events File** 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.

**Enable Events Log File** is an ON/OFF toggle to enable Event logging. Default setting is ON.

**Maximum File Size** 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. Default setting is 32.

**Store Data Alarm Records** is an ON/OFF toggle to enable storing data alarm records. Default setting is OFF.

**Store Sensor Events** is an ON/OFF toggle to enable storing records generated by environmental sensors. Default setting is OFF.

**Date/Time Stamp Data Alarm Records** is an ON/OFF toggle to prepend a Date/Time stamp to the beginning of data alarm records. Default setting is OFF.

**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. Default setting is OFF.

## Audit Log Settings

The Audit Log is a record of a variety of actions that occur within the T830-0.

TeleBoss 830 - 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 Pass-through Activity	[ON]
L) Store Inactivity Timeouts	[ON]
M) Store Polling Activity	[ON]
N) Store DIP Switch Changes	[ON]

**List Audit Log File** displays the contents of the Audit Log file, if any records exist.

**Clear Audit Log File** 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.

**Enable Audit Log File** is an ON/OFF toggle to enable Audit logging. Default setting is ON.

**Maximum File Size** is 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. Default setting is 32.

The remaining options are ON/OFF toggles to enable logging of the action described. Default settings for all is ON.

## Features and How To Use Them

### Upgrading the T830-0

Save the update file (830-2.05.260-std-a71.udf) to a directory on your PC or an FTP server. FTP upgrades can be done in either of two ways: by using the T830-0's FTP client to get the update file, or sending the update file from another host to the T830-0's FTP server. Following are the instructions for both methods.

**» Note:** Before upgrading it is always a good idea to make a copy of the Setting Keys file in your T830-0, in case settings are lost during the upgrade. This usually does not happen, but it's better to be safe than sorry.

#### T830-0 as FTP server method:

- 1) Make an FTP connection to the T830-0 using a username and password that has MASTER rights.
- 2) 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.)
- 3) At the next ftp prompt type: **put drive:\directory\<update filename>**  
For example: put C:\upgrades\830-2.05.260-std-a71.udf
- 4) 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.
- 5) 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. When the unit detects the update file and begins processing it. Wait until the unit reboots before proceeding.
- 6) After the T830-0 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.
- 7) Check your settings to be sure none have been lost. If they have, reload the Setting Keys file.

#### T830-0 as FTP client method:

From the command line type: **xf f get <update filename> <host> <username>**

(note: you can type 'xf' at the command prompt to get usage for this command.)

Here is an actual session:

```
> xf f get 830-2.05.260-std-a71.udf 10.10.5.32 anonymous
Receiving 830-2.05.260-std-a71.udf via FTP
Anonymous's password:
.....
COMPLETE
```

<and the update starts here>

## 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.

Setting Keys is abbreviated when used on the command line as **SK**. Following are commands when working with the Setting Keys File from the command line of the unit.

**SK [KEY[=*value*]]** allows for reading or setting a single Setting Key. If the value portion of the command is omitted, the T830-0 will report back the value stored in that key. If the value is given, it will be stored in the key.

**SK GET [X|A [CUSTOM] [*filter*]]** initiates a download of unit settings. This listing can be retrieved either by Xmodem or plain ASCII using the X and A attributes, respectively. If the transfer mode attribute is omitted, the unit will prompt for the download method. The CUSTOM tag may be used to retrieve only the settings that are not set to factory defaults. A filter may be applied to limit the keys output to just the branch specified. For example, to retrieve an ASCII listing of all EventSensor settings, use the command: **SK GET A EVENT.SENSOR**

**SK SET [X|A]** puts the unit in bulk Settings Keys upload mode. Any of the settings retrieved by **SK GET** can be manipulated and uploaded with new values. The unit will process settings in any order or number; not all settings need to be uploaded each session. As with **SK GET**, both ASCII and Xmodem transfer methods may be used to upload settings to the unit. These transfer methods are indicated by using the X and A attributes, respectively. The T830-0 monitors for invalid Setting Keys and will notify you after the upload if any invalid data was received.

When using **SK SET** in ASCII mode, the data uploaded must end with a line consisting of the word "END" followed by a return.

**SK HERE** 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.

Setting Keys can also be retrieved and loaded via FTP.

**FTP> GET SKALL FILENAME.TXT** retrieves all of the Setting Keys for the unit, similar to the **SK GET A** command described above.

**FTP> GET SKCUSTOM FILENAME.TXT** retrieves any settings that are not set to factory default, similar to the **SK GET A CUSTOM** command described above.

**FTP> PUT FILENAME.TXT SKALL** and **PUT FILENAME.TXT SKCUSTOM** load the settings in FILENAME.TXT onto the T830-0.

Upon successful completion of loading the settings FTP will respond with "226 - Transfer complete". If there is a problem in the Setting Keys file then FTP will respond with "226 - Transfer complete; errors in setting key file! Type Get SKLOG to view"

**FTP> GET SKLOG** retrieves the Setting Keys log as described above.

## Securing a TeleBoss 830-0

This section discusses all facets of security that must be considered when installing a TeleBoss 830-0. For adequate security, you must consider the following:

- [Security mode](#)
- [Telnet/FTP](#)
- [SSH \(Secure Shell\)](#)
- [RTS \(Real Time Sockets\)](#)
- [Web UI \(User Interface\)](#)
- [Button unlock](#)
- IP restrictions (only available on the T850, not the T830-0)
- [VPN \(Virtual Private Network\)](#)

### **Security mode**

The security mode (`sec.mode`) tells the unit how to control users' access to it. You can configure either User Profiles mode or RADIUS mode. (See [Security Settings Menu](#)). For either mode, you can restrict by what methods a user can connect, as well as whether the user receives "Username:" and/or "Password:" when prompted for those items. Be careful to always preserve a way to access the unit as a MASTER user (that is, a user with rights=MASTER). This is the user with full access to configure all settings and invoke all commands. If you are using User Profiles, ensure, before you log out, that you have a MASTER user configured and that you don't forget its password. If you are using RADIUS then you can configure a MASTER user any time as long as you can configure users on the RADIUS server. Before logging out of the unit when configuring RADIUS, ensure the unit can ping the RADIUS server, and that you verify that a user can access the unit via RADIUS. If the user cannot log in to the unit via RADIUS then you will need your existing login in order to gather data to help troubleshoot why the RADIUS user cannot log in.

If you are logged into the unit, you can put traffic on any network to which the unit is connected. For example, pinging a host on the network, FTP-ing to it, SSH-ing to it, Telnet-ing to it. Therefore good security comes from making it so no unauthorized persons have access to the unit. This is something you must ensure with the User Profiles or RADIUS security mode configurations.

### **Telnet/FTP**

Keep in mind that like SNMP, login credentials (and all application content) are transmitted in the clear for Telnet and FTP, so anyone eavesdropping on the network could gain unauthorized access to the unit. Therefore, to tighten security on Telnet, either do not use it, forbid it (with `sec.connectvia`), or use it with RADIUS/CHAP or User Profiles with one-time password or challenge response (only available on the T850, not the T830-0).

### **SSH (Secure Shell)**

To enable SSH access to the T830-0, you must generate a host key with the SSHC command (see the section on [SSH](#) for details). This is the preferred network access method over telnet of course because the traffic is encrypted.

### **RTS (Real Time Sockets)**

Out of the box the T830-0 allows connections to TCP port 220x unauthenticated. So unauthorized access to FILEx data is possible unless you tighten RTS via the authorization controls in RADIUS or User Profiles security modes. Remember that just like SNMP, Telnet, and FTP, any login credentials you require for RTS connections are passed in the clear, so anyone eavesdropping on the network could gain unauthorized access. To limit exposure of the user password, use RADIUS/CHAP or User Profiles with one-time password or challenge response (only available on the T850, not the T830-0). Alternatively, you can forbid RTS connections altogether with the `sec.connectvia` setting.

### **Web UI (User Interface)**

The T830-0 supports both HTTP and HTTPS. Like SNMP, Telnet, and FTP, HTTP is vulnerable to eavesdropping. Therefore to tighten security for web UI access, do not use it or only access the unit via HTTPS (which is encrypted with SSL).



**Button unlock**

With the Button Unlock feature, you can regain access to a unit that you have been locked out of. This is meant as an insurance policy against the only other resort to locking yourself out, which is returning the unit to Asentria.

When this feature is set to ON (default setting), the user can tap the Reset button 5 times quickly (1-2 times per second), at which point the front-panel LEDs will flash briefly for several seconds, giving the user immediate command line access via I/O 2 using the default MASTER username and password.

These are the settings that are defaulted by this process:

`sec.mode` (reset to USER PROFILES)

`sec.consolereq` (reset to OFF)

`sec.connectvia` (reset to every method of connecting)

"admin/password/MASTER" credentials for the user profile appropriate to the product

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 (`sk sec.button.unlock=OFF`), or set the Button Tap Allows Console Access in the [Security Settings/General Security Settings](#) menu to 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.

**VPN**

For the highly secure, flexible, and centralized network access control (aside from unplugging the network cable), use IPsec VPNs to SitePath (Asentria's secure, unified administration portal software). VPNs are disabled and unconfigured by default. Refer to SitePath documentation for details on how to manage units with SitePath via VPN.

## Telnet/TCP Connections

The T830-0 provides support for Telnet/TCP connections via two internal Ethernet interfaces. Refer to the [Ethernet Settings](#) menu for information on how to configure these.

All Telnet connections are TCP connections but not all TCP connections are Telnet connections. A Telnet connection is made to the T830-0 by using the Telnet protocol and by specifying a TCP port address. 'Telnet' refers to a TCP connection made on port address 23, which specifies that characters are supposed to be handled a certain way. The T830-0 supports Telnet connections and also supports some custom assigned port numbers to facilitate certain connection features.

The following information assumes that you know how to run your computer to establish and use Telnet/TCP connections and only require the specific information relating to the T830-0 features. Port numbers below include "x" where "x" is the corresponding T830-0 file or port number. (ie; 2101 refers to the telnet passthrough connection made on serial port 1.)

- **Port Address 200x**: A connection to port 200x is just like a regular Telnet connection to port 23, except it sets the default file for retrieving data or the default port when the **BYPASS** command is given.
- **Port Address 210x** : A connection to port 210x routes you directly to the device connected to the corresponding serial (I/O) port. A banner message will be displayed indicating you are connected to that I/O port. To disconnect from this access mode press the <ESC> key twice. Refer to the Passthrough section in this chapter for more information.
- **Port Address 220x**: A connection to port 220x is referred to as a Real-Time Socket. These are sockets that are dedicated to exporting data from file "x" in the T830-0. If there is any data already stored in a particular file, it will first be transferred out of the T830-0 to the user or machine initiating the connection. After all the data currently in the file is transferred out, any data that is coming into the T830-0 will be immediately transmitted out and across this connection. Refer to the [Real-Time Socket Settings](#) menu for information on how to configure these.

## Secure Shell (SSH)

» **Note:** The T830-0 supports Secure Shell (SSH) but does not currently support SFTP.

### Quick Start: SSH into the unit

The T830-0 supports Secure Shell (SSH) version 2. SSH version 1 is not supported. Some configuration steps are necessary before the initial SSH connection to the unit. Connect to the unit via a conventional method (serial port, telnet, modem) to make these configuration changes. The changes are:

1. Make a user profile with a username and password (required)
2. Configure network settings (required)
3. Generate the host key (optional)

These are the steps in detail:

1. Make a user profile with a username and password (required). This is done via the Setup->User Profile Settings menu.

2. Configure network settings (required) - By default the unit ships with static IP address 0.0.0.0. Change this to an appropriate static IP address on your network, as well as the default router and subnet mask if necessary.

3. Generate the host key (optional) - By default the T830-0 requires password authentication and does not require public key authentication. If you are not certain that you fully understand what public key authentication is, call [Asentria Technical Support](#) and ask them to explain it to you. The T830-0 ships with a host key already generated. You may decide to generate the host key yourself so you can be sure you are the only possessor of the host key. To generate the host key yourself, enter **SSHC -HT RSA** to create the 1024-bit rsa host key.

At this point the unit is ready to receive SSH connections. You can do the same tasks you can do on a conventional connection, like unit administration and passthrough, only now it is secured by SSH.

### Configuring authentication

By default the unit requires password authentication and does not require public key authentication in SSH. For added security you may decide to require public key authentication when connecting to the unit. Do this with the following steps:

1. Enable public key authentication by entering: **SK SEC.SSH.AUTH.PUBKEY=ON**
2. Obtain the public key of the SSH client you intend to use.
3. Make the unit aware that your client is authorized to connect.
  - a. On the unit, enter: **SSHC -AO**
  - b. Input the public key of the client. It should be a long line of ASCII text starting with "ssh-".
  - c. Ensure there is a new line after the key (enter LF or CRLF if you're not sure)
  - d. Enter **END** on a line by itself followed by LF or CRLF.

At this point the unit should be able to authenticate your client with public keys. You may decide that public key authentication alone is sufficient, and password authentication is not required. If so, you may disable password authentication by entering: **SK SEC.SSH.AUTH.PASSWORD=OFF**

### Configuring a login banner for SSH.

The unit can display a standard message when users log in via SSH. Configure this with the following steps:

1. Enter **SSHC -AN**
2. Input your authentication banner as printable ASCII text; multiple lines are allowed.
3. Input **END** on a line by itself followed by LF or CRLF

## Default Router

The Default Router setting allows you to select the default router (gateway) for the T830-0. This tells the T830-0 which router to use if a packet is not on any of the LANs defined on the network port. The default router is selected from the routers defined for the Ethernet ports.

### More information for advanced users:

The Default Router setting allows you to select the default router (gateway) for the unit. The unit uses a routing table to determine how to send any outbound IP frame. Each entry in the routing table tells the unit how to send a frame whose destination address matches a rule in the routing table. Routing table entries are examined from most-restrictive to least-restrictive, so the default routing table entry is the last entry in the table since it is the least restrictive. It is the catch-all route: it tells the unit how to send a frame when it doesn't know how else to send it. The only routes on the unit are network interface routes, any static routes you configure, and the default route. Network interface routes tell the unit how to send a frame bound for a machine on one of the unit's local networks (subnets). These routes are automatically configured when you configure the address of a network interface. If an outbound frame is destined for a machine off all local networks then it is sent according to what the default route specifies. The default route specifies the default router to use for these frames.

Each network interface has a router setting which you can configure; this is the machine on that interface to which frames will be sent if they do not route to the local network of that interface. However the unit uses only one of those configured routers at a time - - the default router setting specifies which router the unit will use at a time. As you configure router settings the unit will choose a default router for you. This is available for you to see (and override) via this `net.default.router` setting. The values you may choose for this setting (i.e., router addresses) are:

- the set of routers which you have specified for Ethernet
- the [ADSL](#) interface peer, if you have ADSL hardware installed, represented as "DSL"
- that which is determined by dynamic network interfaces, represented as "DYNAMIC".

DYNAMIC is always a possible value for the default router. It 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 PPP via the POTS modem or PPP via the Wireless modem. The rule for 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 PPP is that it is the default route if the `net.wireless.defaultrouteenable` setting is enabled. (If it's disabled then the default route will not be set when the default router is "DYNAMIC".) If the default router is set to anything besides "DYNAMIC", then the default router will be either that (e.g., an Ethernet router) **or** that which is determined by the rules of the dynamic network interfaces. In other words, DYNAMIC default router means the default router will be whatever POTS/Wireless modem PPP decides when it is running, and it there will be no default router when POTS/Wireless modem PPP is not running (or when Wireless PPP is running but `net.wireless.defaultrouteenable` is off). Any other value for the default router means that the default router will be that value (e.g., an Ethernet router), unless POTS/Wireless modem PPP may be running and thus may override the default route. When POTS/Wireless modem PPP stops and the default router is not set to DYNAMIC, then the default router will revert to the value of the default router setting.

The default router setting is special in that its set of allowed values (the routers for the various network interfaces) are determined at runtime.

### Values

Values are dotted-quads and must be in the set of routers configured with `net.eth.router` and `net.eth.vlan.router`, or they are the special values "DSL" (when ADSL hardware is installed) and "DYNAMIC".

### Key syntax

`net.default.router`

## Static Routes

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. These give you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different routes.

### Configuration

The T830-0 has a set of 8 static route slots. Each slot has an option to enable it, set the destination net, set the gateway, and set the interface.

- **Enable** is ON/OFF, default OFF.
- **Destination Network** is network notation, i.e., w.x.y.z/s, where s is the significant bits. Default is 0.0.0.0/0.
- **Gateway** is the IP address of the gateway. Default setting is 0.0.0.0
- **Interface** is one of the allowed values: Ethernet 1, Ethernet 2, Dialup Modem PPP, Wireless Modem PPP (WPPP), and NONE. Default is NONE.

To configure a static **host** route you

1. Enable it
2. Specify a destination net with sigbits == 32
3. Specify gateway or interface

To configure a static **network** route you

1. Enable it
2. Specify a destination net with sigbits < 32
3. Specify gateway or interface

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. If it is an Ethernet interface then the destination address (which matches the destination net of the route) will be arped. If it is a PPP interface then the frame which matches its route will be transmitted to the PPP peer.

➤ **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. Eventually this will not be the case, but in the meantime 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.

### Setting Keys

- `net.staticroute.enable`
- `net.staticroute.destnet`
- `net.staticroute.gateway`
- `net.staticroute.if`

### Example

Configure to route traffic to the the host 10.90.90.2 to go out via a special gateway 10.90.80.67.

```
net.staticroute[1].enable=on
net.staticroute[1].destnet=10.90.90.2/32
net.staticroute[1].gateway=10.90.80.67
```

Configure to route traffic to 192.168.1.0/24 (which means a subnet of 255.255.255.0) to go out the wireless interface, whenever wireless is up.

```
net.staticroute[1].enable=on
net.staticroute[1].destnet=192.168.1.0/24
net.staticroute[1].if=WPPP
```

## Passthrough

Passthrough (also known as “Bypass”) is a bi-directional communication link for either a modem or Telnet connection through the T830-0 to a device attached to a serial port. Pass-through is useful for configuring or maintaining devices connected to the T830-0 without having to be in the same physical location.

Passthrough to a serial port is available on TCP ports 210*n* where ‘*n*’ is the number of the serial port.

Passthrough to a serial port is available via modem using the **BYPASS*n*** command where ‘*n*’ is the number of the serial port.

To terminate a passthrough session, press the Escape Key three times.

Following is a table showing what passthrough sub-features/behaviors are applicable to the T830-0 and a detailed description of each sub-feature below the table.

Sub-feature	T830-0
<b>Bypass command</b>	<b>Yes</b>
<b>Adjustable end sequence pause</b>	<b>Yes</b>
<b>End sequence for network passthrough</b>	<b>3 escapes (via login menu) or 1 escape (via bypass command)</b>
<b>End sequence for modem passthrough</b>	<b>1 escape (via bypass command)</b>
<b>Joinable sessions</b>	<b>Yes</b>
<b>Buffered pass-through</b>	<b>No</b>

### **Bypass command**

The command **BYPASS*n***, where ‘*n*’ is the number of the serial port, is used on a modem passthrough connection.

### **Adjustable end sequence pause**

This feature means you can control the minimum amount of time between entering escape characters that the unit will register as an authentic escape sequence. That is, you can set this to 1/4 second, meaning that in order to escape passthrough, you must enter the escape sequence with at least 1/4 second between each escape. The point is to make the unit disregard escape sequences that happen from the pass-through data itself, which is assumed to travel across the link without pauses between the escape characters. The sys.pt.endpause setting controls this.

### **Joinable sessions**

Up to 3 pass-through sessions can be joined in that they all connect to the same serial port. Data arriving on the serial port gets passed through to all parties, and data arriving from any one party gets passed through to the connected serial port as well as the other parties.

### **Buffered pass-through**

Buffered pass-through is where upon connecting to a passthrough session, the first thing the unit does is dump all data that has been buffered in that port's database file, instead of connecting to the port right away. Once all data from that file is output then unit connects you to the port. If no data has been buffered (or this feature is turned off) then the unit initially connects you to the port. This option is not available on the T830-0.

By default the unit provides passthrough access to anyone and can be further defined in the [User Profile Settings](#) menus. Various settings control its behavior, as discussed above with each sub-feature.

## Call Failure Tracking

### Description

Call failure tracking is a feature added for A-tick compliance that limits the number of times the T830-0 calls any one number that doesn't appear to work. Each number dialed is tracked for how many consecutive failures it has racked up. Each time a call is attempted, this number's failure count is checked before dialing. If the failure count  $\geq 15$  then the number will not be dialed for until reset or its blackout period expires. After dialing, if the call is a failure then the called number's failure count is incremented. When it increments to 15 then a blackout timer is set for 2 hours, meaning that this number is forbidden to be dialed for the next 2 hours.

"Call is a failure" means:

- for ppp, ppp was not negotiated
- for other modem calls and alphanumeric pages, carrier was not negotiated.
- 

Numeric pages do not fail to dial since nothing is actually negotiated.

After dialing, if the call is successful then called number's failure count is set to 0.

### Benefit

This enables the unit to not continually dial a number if the number has been shown to be unresponsive, in order to be a good citizen on the telephone network.

### Configuration

There are no settings or UI associated with this feature.

### Usage

If a number has reached its failure limit (and thus turned into a forbidden number to dial) then a message is appended to the Audit Log. Any future attempt to dial a forbidden number results in a message appended to the Audit Log. The only way to make the unit dial any forbidden number again is wait until the 2-hour blackout expires for that number or reset the unit (power cycle, **RESTART** command, **RESTART ALL** command, push reset button). When dialing is attempted after the blackout period expires then a message is appended to the Audit Log saying that forbidden number x was granted permission to be dialed again.

## RADIUS Security

### Description

RADIUS (Remote Authentication Dial In User Service) is feature is used to offload authentication, authorization, and accounting (AAA) work to a RADIUS server, instead of doing that work on the unit. Prior to the introduction of the RADIUS feature, AAA was done on the unit via the User Profiles settings and the Audit Log, although it was never explicitly called AAA in our documentation up to this point. With the introduction of the RADIUS feature, AAA can now be done with a RADIUS server via the RADIUS protocol. A RADIUS server is one instance of a AAA server in that it offers authentication, authorization, and accounting services to client machines, such as the unit. The next few sections go into more detail about how the RADIUS feature works.

### Overview

The RADIUS feature is enabled by setting the `sec.mode` Setting Key to RADIUS or setting the Security Settings/Security Mode option to RADIUS. You configure a primary and/or secondary RADIUS server address (or hostname), as well as secrets for each. The secret is for authenticating the network traffic between the unit and the RADIUS server. The unit makes transactions with the RADIUS server in order to:

- authenticate a user ([Authentication](#))
- determine what an authentic user is authorized to do ([Authorization](#))
- log information about when an authentic user started and stopped a login session ([Accounting](#))

Each transaction has a timeout that specifies how long the unit will wait for a response from the server. (This is configured with the `sec.radius.timeout` Setting Key or in the RADIUS Security Settings menu.) "A response from the server" means a response that is authentic; i.e., the response network frame is verified as trusted. If a response is not authentic, it could be due to an attacker, or corrupted network frame, or misconfiguration of the server secret. A server can respond but if the secret is configured wrong then the unit will find it not authentic, and silently discard the response. In this case, it is as if the unit had received no response at all. So from the perspective of the unit, a response from a RADIUS server is one that is both received **and** authentic.

If no response arrives after the timeout, or if the unit could not transmit to the server in the first place (the server was unreachable, because, for example, no network link, or no network configured on the unit), the unit can try again, up to a limit as configured with `sec.radius.retries` Setting Key or in the RADIUS Security Settings menu. If the unit exhausts all retries for authentication/authorization transactions, it has three options determined in this order:

1. try the same transaction with the secondary server (if its address/hostname and secret are configured). If the secondary server responds, authentication/authorization will succeed/fail according to that server's response. In any other case (secondary server unconfigured or configured but unreachable), the unit proceeds to step 2.
2. try to authenticate and authorize the user using the local User Profiles configuration (if its configured, when `sec.radius.fallback.mode=USER PROFILES`). If the user fails to authenticate with the User Profiles configuration (or if `sec.radius.fallback.mode=NONE`) then the unit proceeds to step 3.
3. give up; the unit cannot authenticate the user so the user cannot log in.

If a RADIUS server deems a user authentic then it passes back authorization info to the unit. So authentication and authorization happen in one transaction. Accounting happens in a separate transaction. Once the unit sees that an authentic user is authorized to do what they intend to do, the unit sends a RADIUS accounting start message to the RADIUS server that originally authenticated the user. When the user's session ends, the unit sends an accounting stop message to that same server.

In sum, the RADIUS feature enables the unit do AAA transactions with a RADIUS server in order to:

- determine if a user is actually who they claim to be
- determine if a user is authorized to do what they want to do, and
- log when that user starts and stops their session



The remaining subsections discuss details of each part of AAA.

### **Authentication**

The RADIUS feature enables the unit to offload (and centralize) user authentication responsibilities to a RADIUS server. The unit does this for the following services in Phase 2 implementation:

- Local (console) command processor
- Telnet command processor
- Modem command processor
- Telnet pass-through
- Real-time sockets
- FTP
- Web UI

» **Note:** Phase 3 implementation will support PPP while Phase 4 will support SSH. Neither Phase 3 nor Phase 4 are supported in this version of the T830-0.

When the unit uses the USER PROFILES security mode, there can be at most 12 users configured, and the unit must be configured with authentication and accounting details. With RADIUS security mode however, as many users can log in to a unit as can be supported on the RADIUS server, and a manner completely independent of the User Profiles configuration on the unit. Additionally, the unit may be just one of many machines that a user would need access to. If all machines supported AAA, user management can be configured more easily and centrally via the RADIUS server, instead of at the unit or other machines configured with their own security mechanisms.

### **PAP vs CHAP**

Authentication can happen via PAP (Password Authentication Protocol) or CHAP (Challenge-Handshake Authentication Protocol). Configured `sec.radius.chap=ON` for CHAP, or `OFF` for PAP.

PAP is where the user provides a username and password. Both the username and password are transmitted to the unit from the user in clear text (unless protected by the application layer's security, such as SSL (for the web UI) or SSH). The username is transmitted to the RADIUS server from the unit in clear text (the password is not).

CHAP is more complex but more secure because the password is not transmitted to the unit from the user (unlike PAP). Instead, the unit first provides the user with a CHAP challenge. The user provides the username, CHAP ID, and CHAP response (which is generated from both the challenge and the user's password). The user uses some local program to generate a CHAP response based on the user's password, CHAP ID, and CHAP challenge. The CHAP ID is just a number between 0 and 255 that the user chooses and provides to both the unit and the CHAP-response-generating program. The unit passes the challenge, username, CHAP ID, and CHAP response to the RADIUS server, which then authenticates the user based on this data.

When logging in to the command processor, pass-through, Web UI, or real-time sockets, the user is prompted for three things when CHAP is enabled: username, CHAP ID, and CHAP response. When logging in to the FTP server, the UI is more standardized as "username and password" and hence requires some special attention when using CHAP. In the case of logging in to the unit via FTP, enter as the FTP password the concatenation of the ASCII-hex CHAP ID value and CHAP response. For example, if the user chooses CHAP ID 225 and generates CHAP response DD0F3C51116B74CFFEC4379BA6D03507, then the FTP password is 225 in ASCII-hex (which is "E1") concatenated with that response: E1DD0F3C51116B74CFFEC4379BA6D03507.

For all login services, the CHAP challenge is presented as a 32-byte ASCII-hex value, representing 16 bytes of the actual challenge value. This is so the challenge can be a pseudo-random bit sequence of the same size as the RADIUS frame authenticator, and also cut-and-pastable by the user between their login UI and their CHAP-response-generating program.

In sum, PAP is as simple as traditional authentication methods. CHAP is more secure but more complex and requires the user to have a local CHAP-response-generating program. This program is anything that can create a 16-byte MD5 hash of the CHAP ID (as an 8-bit value), user password, and challenge (as a 16-byte value).

### **Authorization**

Once a RADIUS server deems a user is authentic, its necessary to determine what the user is authorized to do. For example, a certain user may be, on the RADIUS server, configured and authorized to log in to the unit via telnet command processor but not via the web UI. So if that user attempts to log in to the unit via the web UI, they will be authenticated by the RADIUS server, but denied access by the unit. This happens because upon authentication, the unit requires the RADIUS server to send it certain authorization data about the user. (If the RADIUS server does not respond with all the required authorization data, the user is not allowed to log in to the unit, even though they were authenticated by the RADIUS server.) The authorization data received by the unit essentially says "this user is not allowed access via the web UI". The unit interprets this data by rejecting the user's web UI login attempt. To remedy, the configuration on the RADIUS server would have to change to allow web UI access for that user. This is an example of just one of the pieces of authorization data that the unit requires. The full set of data is detailed later in this document.

When configuring users for access, be sure to limit their user rights (i.e., authorize them for sub-MASTER rights). MASTER users have enough privilege to change the security settings on the unit, including creating their own user profiles and changing the security mode away from RADIUS. If a user connects via RADIUS and is given MASTER rights, then that user can change the security settings to fit what may be malicious intent. Rights are allocated by the Asentria-User-Rights vendor-specific attribute defined later in this document.

### **Accounting**

When a user is authentic and authorized, the unit sends RADIUS accounting start and accounting stop messages to the RADIUS server that authenticated the user, when that user's login session begins and ends, respectively. If the RADIUS accounting UDP port `sec.radius.acct.port` is set to 0 then the unit will not send accounting information. For example, when a user logs in with RADIUS (in PAP mode) to the console port, the unit does the following four things to or for the user:

1. authenticates
2. authorizes
3. sends accounting start information
4. starts a command processor

When the command processor session ends (either by the user explicitly disconnecting or lowering the handshaking on the RS232), then the unit sends accounting stop information to the RADIUS server that authenticated that user (but only if the unit had successfully sent accounting start information for that user when they logged in). Accounting information being "successfully sent" means the unit could reach the RADIUS server and the server responded.

When the unit sends the RADIUS server accounting start and stop messages, it is actually sending RADIUS Accounting-Request frames with the following RADIUS attributes:

- Standard attribute: Acct-Status-Type, which is integer 1 for start or 2 for stop.
- Standard attribute: Acct-Session-Id: the unit uses an RFC 4122 GUID as the value for this attribute; it is used to correlate start and stop messages.
- Standard attribute: User-Name (to specify who logged in or logged out)
- Vendor-specific attribute: Asentria-Service-Type, which is a string that describes the kind of login session the user started.

### **Limits of support**

The unit does not support RADIUS Access-Challenge frame (which the RADIUS server can send in response to an Access-Request frame); the unit interprets Access-Challenge as Access-Reject.

The unit does not support any Accounting-Request frames other than those with Acct-Status-Type set to 1 or 2.

SNMPv3 works only with users specified in the User Profiles configuration when the security mode is set to USER PROFILES; SNMPv3 does not work with RADIUS.

## Locking yourself out

Be careful when you are configuring RADIUS, you may lock yourself out of the unit, which means there is no way to gain access to the unit again: you must return it in order for it to be reinitialized at the factory. There are four ways around this:

1. If you are locked out because there is something wrong with the primary RADIUS server (i.e., it is reachable but it is incorrectly rejecting authentication requests), then configure a secondary (redundant) one, if you have the resources for that.
2. The unit attempts to detect an invalid RADIUS configuration, and if it finds it, it automatically authenticates you using User Profiles. An invalid RADIUS configuration is one where (primary server or secret is not configured) and (secondary server or secret is not configured). So if you have misconfigured the unit in this way, you can still get into the unit provided you know the credentials for a MASTER-rights user profile.
3. Configure the unit to fall back to User Profiles (`sec.radius.fallback.mode=USER PROFILES`). This means when all RADIUS servers configured are unreachable or reachable but unresponsive, the unit will authenticate and authorize the user with its User Profiles configuration. If any RADIUS servers (primary or secondary) are responsive, then when they reject a user, the unit will reject a user and **not** fall back to authenticating with User Profiles. On the one hand this is an insurance policy against locking yourself out, but on the other hand it still means you must maintain some local authentication/authorization security configuration of the unit, which erodes the purpose of centralized AAA.
4. If you end up in a situation where you cannot log in to the unit at all, there is one last resort before returning the unit. There is a way to gain access with the [Button Unlock](#) feature. The user can tap the Reset button 5 times quickly (1-2 times per second), at which point the front-panel LEDs will flash briefly for several seconds, giving the user immediate command line access via I/O 2 using the default MASTER username and password
  - `sec.mode` (to USER PROFILES)
  - `sec.consolereq` (to OFF)
  - `sec.connectvia` (to every method of connecting)
  - "admin/password/MASTER" credentials for the user profile appropriate to the product
  - IO2 mode set to COMMAND (if applicable to product)

### Note:

- The button unlock feature can only be used if `sec.button.unlock=ON` (which it is by default). If you do not want the unit to grant access via this feature, then turn it off. However, if you subsequently lock yourself out then there is no way to gain access to the unit: you must return it.
- 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!
- When tapping the Reset button, tap it 5 times at a frequency of 1-2 times per second. Do not hold in the Reset button otherwise that will reset the unit. Just tap it like you click a mouse button.

## RADIUS server configuration

Some configuration for the RADIUS server is vendor-dependent, such as how you configure client machines and users. Likewise there is vendor-independent configuration that tells the RADIUS server what vendor-specific RADIUS attributes should be included in Access-Accept frames. All authorization data is encapsulated by these vendor-specific attributes in a file called the RADIUS dictionary. The Asentria RADIUS dictionary (named dictionary.asentria) is included on the resource CD that ships with the unit, or can be requested from [Asentria Technical Support](#). It is meant to be input into your RADIUS server. The attributes are listed below. When you configure a user on the RADIUS server, you must in some way specify values for these attributes -- this is how you tell the RADIUS server (and the unit) explicitly what a user is authorized to do. The values for each attribute correspond exactly to the traditional settings used on the unit for User Profiles authorization.

Attribute	Allowed values	Corresponding User Profiles Setting	Required by connection method
Asentria-Connect-Via-Local	ON,OFF	sec.user[x].connectvia.local	L

Asentria-Connect-Via-Modem	ON,OFF	sec.user[x].connectvia.modem	M
Asentria-Connect-Via-Telnet	ON,OFF	sec.user[x].connectvia.telnet	TP
Asentria-Connect-Via-FTP	ON,OFF	sec.user[x].connectvia.ftp	F
Asentria-Connect-Via-RTS	ON,OFF	sec.user[x].connectvia.rts	R
Asentria-Connect-Via-SSH	ON,OFF	sec.user[x].connectvia.ssh	N/A in phase 2
Asentria-Log-In-To	COMMAND, PASSTHROUGH, MENU	sec.user[x].loginto	FTMLP
Asentria-Access-File	FILE1, FILE2, ... FILEn	sec.user[x].accessfile	TML
Asentria-PPP-Type	NONE, LOCAL, ROUTING	sec.user[x].ppptype	N/A in phase 2
Asentria-User-Rights	NONE, VIEW, ADMIN1, ADMIN2, ADMIN3, MASTER	sec.user[x].rights	FTMLPW
Asentria-File1-Read-Access	DENY, ALLOW	sec.user[x].file[1].readaccess	FTMLWR
Asentria-File2-Read-Access	DENY, ALLOW	sec.user[x].file[2].readaccess	FTMLWR
Asentria-File3-Read-Access	DENY, ALLOW	sec.user[x].file[3].readaccess	FTMLWR
Asentria-File4-Read-Access	DENY, ALLOW	sec.user[x].file[4].readaccess	FTMLWR
Asentria-File5-Read-Access	DENY, ALLOW	sec.user[x].file[5].readaccess	FTMLWR
Asentria-File6-Read-Access	DENY, ALLOW	sec.user[x].file[6].readaccess	FTMLWR
Asentria-File7-Read-Access	DENY, ALLOW	sec.user[x].file[7].readaccess	FTMLWR
Asentria-File8-Read-Access	DENY, ALLOW	sec.user[x].file[8].readaccess	FTMLWR
Asentria-File9-Read-Access	DENY, ALLOW	sec.user[x].file[9].readaccess	FTMLWR
Asentria-File10-Read-Access	DENY, ALLOW	sec.user[x].file[10].readaccess	FTMLWR
Asentria-File11-Read-Access	DENY, ALLOW	sec.user[x].file[11].readaccess	FTMLWR
Asentria-File12-Read-Access	DENY, ALLOW	sec.user[x].file[12].readaccess	FTMLWR
Asentria-File13-Read-Access	DENY, ALLOW	sec.user[x].file[13].readaccess	FTMLWR
Asentria-File14-Read-Access	DENY, ALLOW	sec.user[x].file[14].readaccess	FTMLWR
Asentria-File15-Read-Access	DENY, ALLOW	sec.user[x].file[15].readaccess	FTMLWR
Asentria-File16-Read-Access	DENY, ALLOW	sec.user[x].file[16].readaccess	FTMLWR

Asentria-Events-Read-Access	DENY, ALLOW	sec.user[x].events.readaccess	FTMLWR
Asentria-Audit-Read-Access	DENY, ALLOW	sec.user[x].audit.readaccess	FTMLWR
Asentria-File1-Write-Access	DENY, ALLOW	sec.user[x].file[1].writeaccess	FTMLWR
Asentria-File2-Write-Access	DENY, ALLOW	sec.user[x].file[2].writeaccess	FTMLWR
Asentria-File3-Write-Access	DENY, ALLOW	sec.user[x].file[3].writeaccess	FTMLWR
Asentria-File4-Write-Access	DENY, ALLOW	sec.user[x].file[4].writeaccess	FTMLWR
Asentria-File5-Write-Access	DENY, ALLOW	sec.user[x].file[5].writeaccess	FTMLWR
Asentria-File6-Write-Access	DENY, ALLOW	sec.user[x].file[6].writeaccess	FTMLWR
Asentria-File7-Write-Access	DENY, ALLOW	sec.user[x].file[7].writeaccess	FTMLWR
Asentria-File8-Write-Access	DENY, ALLOW	sec.user[x].file[8].writeaccess	FTMLWR
Asentria-File9-Write-Access	DENY, ALLOW	sec.user[x].file[9].writeaccess	FTMLWR
Asentria-File10-Write-Access	DENY, ALLOW	sec.user[x].file[10].writeaccess	FTMLWR
Asentria-File11-Write-Access	DENY, ALLOW	sec.user[x].file[11].writeaccess	FTMLWR
Asentria-File12-Write-Access	DENY, ALLOW	sec.user[x].file[12].writeaccess	FTMLWR
Asentria-File13-Write-Access	DENY, ALLOW	sec.user[x].file[13].writeaccess	FTMLWR
Asentria-File14-Write-Access	DENY, ALLOW	sec.user[x].file[14].writeaccess	FTMLWR
Asentria-File15-Write-Access	DENY, ALLOW	sec.user[x].file[15].writeaccess	FTMLWR
Asentria-File16-Write-Access	DENY, ALLOW	sec.user[x].file[16].writeaccess	FTMLWR
Asentria-Events-Write-Access	DENY, ALLOW	sec.user[x].events.writeaccess	FTMLWR
Asentria-Audit-Write-Access	DENY, ALLOW	sec.user[x].audit.writeaccess	FTMLWR
Asentria-Port1-PT-Access	DENY, ALLOW	sec.user[x].port[1].ptaccess	TMLWP
Asentria-Port2-PT-Access	DENY, ALLOW	sec.user[x].port[2].ptaccess	TMLWP
Asentria-Port3-PT-Access	DENY, ALLOW	sec.user[x].port[3].ptaccess	TMLWP
Asentria-Port4-PT-Access	DENY, ALLOW	sec.user[x].port[4].ptaccess	TMLWP
Asentria-Port5-PT-Access	DENY, ALLOW	sec.user[x].port[5].ptaccess	TMLWP

Access			
Asentria-Port6-PT-Access	DENY, ALLOW	sec.user[x].port[6].ptaccess	TMLWP
Asentria-Port7-PT-Access	DENY, ALLOW	sec.user[x].port[7].ptaccess	TMLWP
Asentria-Port8-PT-Access	DENY, ALLOW	sec.user[x].port[8].ptaccess	TMLWP
Asentria-Port9-PT-Access	DENY, ALLOW	sec.user[x].port[9].ptaccess	TMLWP
Asentria-Port10-PT-Access	DENY, ALLOW	sec.user[x].port[10].ptaccess	TMLWP
Asentria-Port11-PT-Access	DENY, ALLOW	sec.user[x].port[11].ptaccess	TMLWP
Asentria-Port12-PT-Access	DENY, ALLOW	sec.user[x].port[12].ptaccess	TMLWP
Asentria-Port13-PT-Access	DENY, ALLOW	sec.user[x].port[13].ptaccess	TMLWP
Asentria-Port14-PT-Access	DENY, ALLOW	sec.user[x].port[14].ptaccess	TMLWP
Asentria-Port15-PT-Access	DENY, ALLOW	sec.user[x].port[15].ptaccess	TMLWP
Asentria-Port16-PT-Access	DENY, ALLOW	sec.user[x].port[16].ptaccess	TMLWP
Asentria-Service-Type	LOCAL, MODEM, TELNET, PASSTHROUGH, FTP, RTS, WEB, PPP, SSH	N/A	N/A

The final column, "Required by connection method", lists the connection methods that require the attribute. Here is what the letters mean for this column:

- **F**=FTP
- **T**=Telnet command processor
- **M**=Modem command processor
- **L**=Local (console) command processor
- **W**=Web UI
- **R**=Real time sockets
- **P**=Telnet pass-through (to port 210x)

For example, Asentria-Access-File has "TML", which means if you configure a user on the RADIUS server that you intend to connect by Telnet, Modem, or Local, then you **must** configure this attribute to be returned to the unit upon successful authentication, otherwise the unit cannot authorize the user, and will therefore reject the user's login even though they are authentic.

The Asentria-Service-Type attribute is N/A for the last two columns because it does not deal with authorization -- it is used in accounting RADIUS transactions only.

Note that the Asentria-Filex-\* and Asentria-Portx-\* attributes are required for only however many serial ports on the unit. For example, if you have a unit with only 2 ports, then only Asentria-File1-\*, Asentria-File2-\*, Asentria-Port1-\*, and Asentria-Port2-\* attributes are required by that unit for the given connection method.

Note that "N/A in phase 2" means that this attribute is not used in phase 2 of the RADIUS feature (phase 2 supports everything except PPP and SSH).

**Benefit**

In a typical application environment for these units, there is hardware from other vendors too, and each piece of hardware probably has its own way of doing AAA operations. As the number of disparate machines rises, so does the administration headache of maintaining AAA for each machine for each user. If all machines use a standard, centralized AAA architecture however, then that simplifies administration of all of them and makes each one fit more easily into the entire application environment. Therefore, having a unit support AAA (via RADIUS, one of the most-deployed and most-mature of AAA servers) makes it easier for organizations to fit units into their environments.

**Configuration**

To configure RADIUS on the unit (minimum required configuration) enter the Setting Key values as shown below, or onfigure using the [RADIUS Security Settings](#) menu:

```
sec.mode=RADIUS
sec.radius.server[1]=<address or hostname>
sec.radius.server[1].secret=<secret>
```

To configure other parts of RADIUS (optional):

```
sec.radius.server[2]=<address or hostname>
sec.radius.server[2].secret=<secret>
sec.radius.fallback.mode=<NONE or USER PROFILES>
sec.radius.auth.port=<UDP port that server uses for authentication/authorization>
sec.radius.acct.port=<UDP port that server uses for accounting, or 0>
sec.radius.chap=<ON or OFF>
sec.radius.timeout=<timeout in seconds, 1 to 30>
sec.radius.retries=<number of retries, 0 to 30>
```

**Example**

Say you want to configure user "bob" to access the unit's modem command processor via RADIUS. First configure "bob" on the RADIUS server. He may already be configured on your RADIUS server because his duties may include administering other RADIUS-supporting machines besides the unit. Either way, you must configure the following attributes for "bob" on the RADIUS server (this list is generated by looking at the table above and seeing which attributes are required by the "T" method (telnet command processor). (Say the unit has only 2 serial ports to minimize the File/Port authorization attributes listed here.)

```
Asentria-Connect-Via-Telnet = ON
Asentria-Log-In-To = COMMAND
Asentria-Access-File = FILE1
Asentria-User-Rights = ADMIN3
Asentria-File1-Read-Access = ALLOW
Asentria-File2-Read-Access = ALLOW
Asentria-File1-Write-Access = ALLOW
Asentria-File2-Write-Access = ALLOW
Asentria-Events-Read-Access = ALLOW
Asentria-Audit-Read-Access = ALLOW
Asentria-Events-Write-Access = DENY
Asentria-Audit-Write-Access = DENY
Asentria-Port1-PT-Access = ALLOW
Asentria-Port2-PT-Access = ALLOW
```

This list of attributes for user "bob" on the RADIUS server specifies that he can access the unit's telnet command processor with ADMIN3 rights, the access file set to FILE1 and all files/ports readable and writable except that he cannot write the events and audit files.

Also configure a user for yourself that gives you MASTER rights to the unit should you need access to it.

Then configure RADIUS on the unit according to the Configuration section above, verify the unit can reach the RADIUS server by pinging it, and then log out. Then try logging in to test the RADIUS setup. If you or "bob" cannot log in then you have locked yourself out of the unit. If the reason you cannot log in cannot be attributed to a configuration error on the RADIUS server then you must use the unit's fallback options for getting access to the unit again: the RADIUS fallback mode or the button unlock feature. From there troubleshooting steps can be taken to see why login failed.

Please contact [Asentria Technical Support](#) for assistance in troubleshooting RADIUS connection problems.

## Data Events

This section offers a brief tutorial on how to set up a functional data event that will send an SNMP trap when the word "test" is received over a data port. Full details on how to configure data alarm equations are available in the next section, [Configuring Data Alarm Equations](#).

### Set Up a Data Event

1. From the command prompt, access the Setup menu. Select "Alarm/Event Definitions", "Data Alarm/Filter Settings", and then "Data Alarm Field Settings". The following menu allows a user to define up to 16 data event fields to be used when scanning for event data. Below is an abbreviated example of this menu:

```
TeleBoss 830 - Data Alarm Field Definition Table
```

	Start	Length	Line	Type	Name
A) Definition A	0	0	0	[Alpha]	
B) Definition B	0	0	0	[Alpha]	
...					
O) Definition O	0	0	0	[Alpha]	
P) Definition P	0	0	0	[Alpha]	

2. Select field A. The menu in the following example will be displayed.

```
TeleBoss 830 - Data Alarm Field Definition
```

Data Field: A

A) Start Position	[0]
B) Field Length	[0]
C) Field Name	[ ]
D) Field Type	[Alpha]

3. Select Start Position. When prompted to enter a new value, enter "1" and press <Enter>.
4. Select Field Length. When prompted to enter a new value, enter "4" and press <Enter>.
5. Select Field Name and enter **TEST\_FIELD**, then press <Enter>.
6. Press <Enter> to return to the Field definition Table. If configured properly, the data event field should appear in this menu.
7. Press <Enter> to return to the Data Alarm/Filter Settings menu. From here, select the Data Alarm Settings menu, Alarm/Filter Page 1, then Alarm/Filter 1. The following menu will be displayed:

```
TeleBoss 830 - 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	

8. Press "A" to toggle Alarm/Filter Enable to ON.
9. Alarm/Filter Mode should be set to ALARM. If it is set to FILTER, press "B".
10. Select Alarm/Filter Name and enter **Test Event 1**.
11. Select Alarm/Filter Equation and enter **TEST\_FIELD="test"**. This will cause an event to occur any time the word "test" is received.




12. Select Actions and enter "**TRAP(1)**" to cause this data event to send a trap to SNMP manager #1, as configured below in the Hostname/IP Address menu.

### Other Setup

1. Return to the Main Setup Menu, select "Action Definitions", select "Hostname/IP Address 1" and enter either the hostname or IP address of the SNMP Manager where the trap will be sent.
2. Go to the Serial Setup Menu for serial port I/O 1 (or whichever port incoming data will be monitored) and set the Data Alarm Enable setting to ON.
3. Press <CTRL> + C to return to the command processor.

### Testing

Connect to the unit serially on I/O 1 and type the word **test** followed by <Enter>. This should trigger the above data event, and an SNMP trap should be sent to SNMP Manager #1. If this is not the case, double check the network and data event settings and then call [Asentria Technical Support](#).

 **Note:** There will be a 30 second delay in alarming if the terminal emulator being used does not send a LF with the CR. This may be circumvented by pressing <CTRL + J> to generate a LF.


## Configuring Data Alarm Equations

The equation is the heart of any data event. The following are a few examples event equations:

- `alarm_code = "L31"`
- `ext >= "A 600" AND exit_code = "DN"`
- `(alarm_code > "1051" OR exit_code = "10w74x") AND switch = " 001.1.9*.**"`
- `@ = "CRITICAL"`

Here are a few tips to help you create your own data event equations:

- Multiple field references are acceptable, as long as both fields are the same length. For example, `d=c` is a valid equation if the fields that both 'd' and 'c' represent are two characters long
- Variable names are case sensitive
- Equation literals (the data contained within quotation marks) are case sensitive
- If any rule is violated in a equation, an alarm will not be generated, nor will an error be presented

 **Note:** There may be times when two or more fields are necessary to analyze one piece of data. For example, if a time is represented in hh:mm format, some calculations may require two different fields. Other times, wildcards will do the job of masking out non-important characters just fine.

The data alarm equations used in the T830-0 are standard Boolean-type operators. The following table outlines each of the supported operators and their function.

Operator	Function
>	Greater Than
<	Less Than
>=	Greater Than or Equal to
<=	Less Than or Equal to
! or <>	Not Equal to
=	Equal to
*	Single character wildcard (matches any character or space)
()	Parenthesis used to combine operations
OR	Logical OR
AND	Logical AND
@	Positional wildcard (used in place of a field name to match anywhere within an incoming record)

## Data Alarm Macros

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. Also, since the macro expression is evaluated only once per record, it improves the efficiency of alarm processing.

Data alarm macros can be configured using the setup menu or setting keys:

### Menu

Setup -> Alarm/Event Definitions -> Data Alarm/Filter Settings -> Data Alarm Macro

### Settings Keys

`event.macro[ ].name`  
`event.macro[ }.equation`

The macro equation is entered the same way as a data alarm equation. A macro equation cannot refer to another macro; in such a case, the expression involved will always evaluate to FALSE. The macro equation can be up to 160 characters in length.

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 are subject to these restrictions:

- Macro names and data field names are not case sensitive; therefore DLT35 and Dlt35 are equivalent.
- A macro cannot be given the same name as a data field or another macro.
- The following names are reserved and should not be used as macro names or data field names:
 

°IOx (where x is a number)	°FALSE
°IPRC	°AND
°TRAP	°OR
°FTP	°IS
°TRUE	°ISNOT

Using a macro name or data field name that starts with AND or OR will cause that part of the expression to always evaluate to FALSE.

Macro names and data field names cannot start with \$.

When used in a data alarm equation, macros are always compared to TRUE or FALSE. Any other comparison yields a result of FALSE.

### Example Settings

- `event.data[1].enable=ON`
- `event.data[2].enable=ON`
- `event.data[1].equation=m1=true`
- `event.data[2].equation=m1 = true and f2 = "0"`
- `event.field[1].start=7`
- `event.field[2].start=6`
- `event.field[1].length=1`
- `event.field[2].length=1`
- `event.field[1].name=f1`
- `event.field[2].name=f2`
- `event.macro[1].name=m1`
- `event.macro[1].equation=f1="1"`

**Incoming records**

0000001	N	019	00	DN1042	T001034	02/25	09:21	00:00:50	A	5558481677
0000002	N	020	00	DN5280	T001033	02/25	09:22	00:00:08	A	5551377443
0000003	N	021	00	T002014	DN6502	02/25	09:22	00:00:10		
0000004	N	022	00	T007002	DN5700	02/25	09:19	00:02:36		
0000005	E	023	00	T002024	DN1006	02/25	09:22	00:00:58		
0000006	N	024	00	T002042	DN6000	02/25	09:21	00:00:46		
0000007	N	025	00	DN5154	T001035	02/25	09:04	00:17:50	A	5558451000
0000008	N	026	00	DN1192	T001031	02/25	09:22	00:01:10	A	5558406776
0000009	N	027	00	DN1048	T001034	02/25	09:23	00:00:26	A	5556426898
0000010	N	028	00	DN1197	T001020	02/25	09:19	00:04:30	A	5552550948
0000011	N	029	00	DN6063	T001033	02/25	09:23	00:00:16	A	5557458535
0000012	N	030	00	T002019	DN6447	02/25	09:23	00:00:10		

**Alarm records**

0000001	N	019	00	DN1042	T001034	02/25	09:21	00:00:50	A	5558481677	(DA 1)
0000001	N	019	00	DN1042	T001034	02/25	09:21	00:00:50	A	5558481677	(DA 2)
0000011	N	029	00	DN6063	T001033	02/25	09:23	00:00:16	A	5557458535	(DA 1)

- The first record matches data alarm 1, because macro 'm1' is true. Macro 'm1' is true any time the character in the 7th position is '1'.
- The first record also matches data alarm 2, because macro 'm1' is true and field 'f2' contains a '0' character.
- The eleventh record matches data alarm 1, again because macro 'm1' is true. It does not match data alarm 2 because field 'f2' does not contain a '0' character.

## Action List

An action list is a text string that specifies what the unit should do upon an event. It's comprised of a list of keywords and parameters separated by semicolon. Each keyword specifies a certain action and has its own parameter set, which is enclosed in parentheses.

**Note:** Not all actions on the Action List may be available in this product. Contact [Asentria Tech Support](#) if you have questions concerning this.

For example, the keyword *trap* has a parameter <address or index>, and has syntax *trap(address or index)* in an action list. This keyword means send a trap to the specified parameter. If the parameter is an address then it uses that address as the trap destination. If the parameter is an index then it uses the address specified in the IP action setting list, indexed by the specified index. (This IP action setting list is [action.ip](#), so *trap(1)* means send a trap to the address in setting [action.ip\[1\]](#).)

- *cancel(idname)*  
Cancel any running action list identified by *idname*.
- *dialup pager(dpage[index])*  
Send a pager callout via modem; *index* is the phone number configured with [action.page.number](#)
- *dispatcher(phone# or index)*  
Send a Dispatcher alarm via modem; *index* is the phone number configured with [action.call.number](#).  
E.g., [action.call.number\[index\]](#).
- *email(email or index)*  
Send an email to the address specified by *email*; *index* is the email address configured with [action.email](#)
- *group(groupname)*  
Identify this action list as part of a group identified by *groupname*; not currently used. In a future version this will be used to cancel or postpone groups of action lists.
- *id(idname)*  
Identify this action list by *idname*.
- *malert(phone# or index)*  
Send an malert (Asentria Alarm via modem); the parameters are the same as for the dispatch keyword.
- *modem(phone# or index)*  
Make the unit dial a phone number and start a login session (to the unit's command processor) with the answering machine. The parameters are the same as for the dispatch keyword.
- *postpone(idname, seconds)*  
Postpone an already-running action list identified by *idname* for a duration specified by *seconds*.
- *pause(seconds)*  
Pause operation for a duration specified by *seconds*.
- *relay(action, EventSensor, point)*  
Put a relay in a certain state specified by *action*.
  - *action*: one of the following words, by case-insensitive exact match or partial unambiguous match: *open*, *close*, *active*, or *inactive*
  - *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., 200 in [event.sensor\[200\].\\*](#) for the internal EventSensor) as well as that referred to by the SNMP esIndex object.
  - *point*: the number of the relay (1-based) on the specified EventSensor. E.g., this is the same number *x* in ["event.sensor\[200\].relay\[x\].\\*"](#)
- *talert(ipaddress or index)*  
Send a talert (Asentria Alarm via TCP).
  - *ipaddress* is the destination machine;
  - *index* is the IP address configured with [action.ip](#). E.g., [action.ip\[index\]](#).
- *trap(ipaddress or index)*  
Send an SNMP trap. The parameters are the same as for the talert keyword. In order to send a trap there must be a route for it. Since a trap is an unacknowledgable action, the way the unit knows if a trap is successful is if it was able to leave the unit. In order for a trap to leave the unit there must be an IP route to its host. A trap action without a route to its host is considered a failure. "Without a route" means, for example, that:

- if the host is meant to be on a local net but cannot be ARPed
- if the host is meant to be off all local nets but the router cannot be ARPed
- if the above two conditions exist and PPP cannot be raised as a backup route.

Each action can take a varying amount of time depending on what's going on in the unit. E.g., a trap may take less than a second to send if there is a route for it on a network interface that is already up (like Ethernet). Otherwise, if the unit is configured to bring up PPP in case the trap cannot be sent on an already-up interface, then the trap may take a minute to send while the unit brings up PPP.

The unit starts all actions up to the first pause keyword at the same time. E.g., if you have an action list like *trap(1);email(1);modem(1);pause(60);trap(2)* then the unit will start the first 3 actions, pause for a minute, then start the last action.

Wherever you can configure an event you can configure its actions. Generally this is with the **\*.actions** setting key that applies to the event you want to monitor. You can also configure email actions (in the action list syntax) for a user profile's login challenge destination (e.g., **sec.user.challenge.telnetstodto**). Not all actions are applicable to all events: relay actions can be caused only by sensor events and data events.

## Types of Alarm Notices

When alarms are detected by the T830-0 and a notification event is warranted, you have a choice of a number of different alarm methods. Specifically these are:

- [SNMP Trap](#)
- [Email Alarms](#)
- [Asentria Alarms](#)
- [SMS](#) (requires wireless modem and is not supported by the T830-0)
- [Pager Alarms](#) (requires dialup modem)

The following section describes these messages and how to use them.

### SNMP Traps

SNMP Traps are alarm notices which are sent using TCP/IP and which conform to the requirements of the SNMP protocol. In essence, the SNMP Trap is a TCP/IP alarm message using the SNMP protocol, which contains a number of name/value pairs in its payload. In this payload the “name” is an SNMP Object ID and the “value” is the value of that OID.

In the case of the T830-0 product, there are two defined SNMP traps that you can choose from. These traps are defined in the SNMP MIB that is provided with the T830-0 product (or which is available through the Asentria website or [Asentria Technical Support](#)).

The first trap is a ‘Standard’ SNMP trap. This is the original SNMP trap format supported by Asentria products. In this trap there are two name/value pairs in the trap payload; ‘siteName’ which is the sitename of the device sending the trap and ‘stockTrapString’ which is a string value, which is the standard concatenated alarm message string used for this and other alarms messages in the T830-0.

The stockTrapString message format looks like this:

```
Date Time :: SiteName :: Sensor Pod/Bank name :: Sensor Point Name :: Alarm Alias
```

For example, the stockTrapString might actually look like this

```
10/24 06:43 :: San Diego Site #12 :: Sensor Pod 12 :: Cabinet Temp :: Temperature Very High
```

For users familiar with SNMP, the actual SNMP MIB definition of the Standard SNMP looks like this:

```
t830StockTempTrap TRAP-TYPE
    ENTERPRISE t830
    VARIABLES { siteName, stockTrapString }
    DESCRIPTION
        "A stock temperature trap is issued when a temperature event
        happens."
    ::= 120
```

The other kind of SNMP trap which you can use what we call a ‘User Defined Trap’. In this trap we provide for a series of traps which each have an individual “Trap number”. This can be easier to integrate with management systems because the manager can have rules setup to kick in when you get “trap # 1000” or “trap # 1001” or so on. When using User Defined Traps, the trap number to use is assigned as part of the Event Definition Setup. In the case of User Defined Traps, the payload of the trap contains a number of OID variables, essentially anything that might be relevant to the particular alarm being transmitted. If the variable is not relevant for the alarm being transmitted then that variable is null.

For users familiar with SNMP, the actual trap definition in the SNMP MIB looks like this:

```
t830UserTrap1000 TRAP-TYPE
  ENTERPRISE t830
  VARIABLES { siteName, esIndex, esName, trapEventTypeName,
    trapEventTypeId, esIndexPoint, esPointName, esID,
    clock, trapIncludedValue, trapIncludedString,
    trapEventClassNumber, trapEventClassName }
  DESCRIPTION
    "This user-defined trap is issued when an event happens that causes a
    trap with specific trap type 1000."
  ::= 1000
```

In the above there are various alarm values in this trap including the trapIncludedString referenced in the Standard Trap.

## Email Alarms

Email alarms contain a concatenated alarm string, which follows the format of:

```
Date Time :: SiteName :: Sensor Pod/Bank name :: Sensor Point Name :: Alarm Alias
```

For example, a typical Email notification for a temperature alarm might look like the following:

```
From: Asentria TeleBoss 830
Sent: Friday, October 24, 2008 3:59 PM
To: support@Asentria.com
Subject: Event
```

```
10/24 15:59 :: San Diego Site #12 :: Sensor Pod 12 :: Cabinet Temp :: Temperature Very High
```

## Asentria Alarms

### Version 1.1 (default) for TCP

An Asentria Alarm sent via TCP is called a Notice. A notice is a piece of data formatted in printable ASCII: a set of lines delimited by CRLF. Each line is of the format <field>: <data>CRLF. The first line has <field> = "ID" (without the quotes). The last line has <field> = "TEXTx" (without the quotes, where x is some number between 1 and 30). The particular format the describes the alarm, and is one of the actions that can be configured for each alarm. A notice that rides on TCP/IP is called a "talert", short for "TCP alert". Talerts are delivered according to the Asentria Alarm Protocol, which over tcp is just a specification of message format.

Notices ride on an IP network. The IP network is facilitated by broadband internet connection or PPP in this model. When riding on a network from a unit to SitePath, it is assumed that a notice is normally tunneled over a VPN via a VPNG. In situations where the VPN is unavailable, the notice rides on a PPP link to SitePath via the PPPG. When riding on a network from a VPNG to the notice receiver (or on a network from a PPPG to the notice receiver), a notice travels in plaintext (i.e., not encrypted).

The format below is common to all events that can trigger a notice:

```
<Answer string (i.e., the value of sys.answer)>
<Sitename (i.e., the value of sys.sitename)>
Asentria Alarm Notice ver. 1.1

ID : 00
Date : mm/dd/yy
Time : hh:mm:ss
TargetPort:
TargetName:
AlarmType :
AlarmMsg :
Severity : {as specified by class/severity}
AlarmNum : {the value of the trap number setting for the triggering event}
Threshold :
Current :
Text1 :
```



Hardware: (the value of `sys.hardware`)  
 Product: (the value of `sys.product`)  
 Version: (the value of `sys.version`)  
 Build: (the value of `sys.build`)  
 Serial #: (the value of `sys.serial`)

**Note:** There are 3 blank lines before "Hardware:" and 2 blank lines after "Serial #".

Other more specific types of Asentria Alarm Notice formats are: (contact [Asentria Technical Support](#) for sample format)

- Data Alarm notice
- No-data Alarm notice
- CPE Down Alarm notice
- VPN Down Alarm notice
- VPNG Down Alarm notice

### Version 1.0 for modem dialout

An Asentria Alarm can also be sent over dialup modem when the Asentria Alarm Version is set to 1.0. Details of this alarm follow:

When an Asentria Alarm is initiated, the box dials into the callout number specified by the action. Once connected, it sends a header and waits for a specific response. If the T830-0 receives a specific response to the header, it delivers alarms in CRC mode; otherwise, alarms are delivered in non-CRC mode. In CRC mode, each Asentria Alarm is transmitted with some extra control characters and a CRC, and the remote host is required to acknowledge each alarm in a certain format.

After all Asentria Alarms have been delivered, the box waits for 20 seconds for any type of keystroke. If a keystroke is detected, the box will present a login menu.

### Initial header

**Note:** Please see the Control Characters appendix for more information about special characters used within this section.

Upon dialing into the receiver, the T830-0 will send a message similar to the following:

```
TeleBoss 830
Server Room B
Asentria Alarm Notice ver. 1.00
(CR/LF) (ENQ)
```

The first line of the output is the T830-0's answer string.

The second line is the T830-0's unit ID.

The third line indicates the version of Asentria Alarm.

The final line is the (ENQ) control code.

### Non-CRC Mode

After sending the initial header, the T830-0 pauses for 10 seconds to wait for an ACK from the receiver. Non-CRC mode requires the Require Asentria Alarm ACKs setting to be turned off. If the T830-0 sees no response or the receiver replies with:

```
(ACK) 00 (ACK)
```

then non-CRC mode is assumed and the sender will transmit the alarms. The control characters (SOH), (SOT), and (ETX) are not transmitted in non-CRC mode.

### CRC Mode

CRC mode exists to ensure that event notifications are delivered intact. Asentria Alarms delivered in CRC mode have extra control characters and a 16-bit CRC included in each alarm to allow for error detection by the receiver. Additionally, CRC mode causes the T830-0 to store and later retry each alarm until a proper acknowledgement is received from the receiver.

If Require Asentria Alarm ACKs is enabled, the T830-0 will require a positive CRC mode response or it will disconnect and retry the call. To enable CRC, the receiver must respond with the following after the header is received:

```
(ACK) 01 (ACK)
```

Once CRC mode is enabled, each alarm must be acknowledged by a message in the following format:

```
(ACK) XX (ACK)
```

XX represents the alarm ID to acknowledge. The ID can be found in the first line of each record sent by the T830-0.

### Alarm Transmission

After successfully initiating a session, alarms are delivered in the following format:

```
(SOH) ID=XX (SOT)
Date=12/25/07
Time=10:30:02
TargetPort=
TargetName=
AlarmType=Data Alarm
AlarmName=Test Alarm
Threshold=0
Severity=Critical
Text1=text record line
Text2=text record line
(ETX) XX
(CR/LF)
(CR/LF)
```

The alarm ID indicates the index number of each alarm delivered during a call. This number restarts at 1 for each new call.

The severity line represents the Class value defined for this alarm.

Up to twelve lines of Text $n$  may be sent.

XX represents the 16-bit CRC if CRC mode is enabled. If not, this line will contain two spaces.

If additional alarms are queued to send in the same transmission, the above output is repeated, and the ID incremented with each alarm. When non-CRC alarm transmission is selected, alarms are sent with a 5 second delay between each. When all alarms and been transmitted, then T830-0 sends the following:

```
(EOT)
(CR/LF)
(CR/LF)
```

At this point, the T830-0 waits 20 seconds for the receiver to send any input, and then hangs up. If any commands are received, a command prompt is established and the connection will remain active.

### **Action Definition**

Asentria Alarm actions are designated by "Modem" in action definitions. The numbers correspond to callout numbers.

Example: Modem(1), Modem(2), etc

## SMS Alarms

**>> Note:** requires wireless modem and is not supported by the T830-0

SMS alarm messages contain a concatenated alarm string, which follows the format of:

```
Date Time :: SiteName :: Sensor Pod/Bank name :: Sensor Point Name :: Alarm Alias
```

For example, a typical SMS notification for a temperature alarm might look like the following:

```
10/24 15:59 :: San Diego Site #12 :: Sensor Pod 12 :: Cabinet Temp :: Temperature Very High
```

## Pager Alarms

**>> Note:** requires dialup modem

Pager alarm messages contain a concatenated alarm string, which follows the format of:

```
Date Time :: SiteName :: Sensor Pod/Bank name :: Sensor Point Name :: Alarm Alias
```

For example, a typical Pager notification for a temperature alarm might look like the following:

```
10/24 15:59 :: San Diego Site #12 :: Sensor Pod 12 :: Cabinet Temp :: Temperature Very High
```

## Type2 EventSensor™ Configuration Setup

As of the publishing date for this User Manual:

- a) only Temperature (ES-T) and Temperature/Humidity (ES-TH) Type 2 Event Sensors are available.
- b) only three Type2 EventSensor's are supported

### Connections

The 9-pin mini DIN cable end of the EventSensor cable plugs in to the SensorJack port on the back panel of the T830-0. The RJ45 end of that cable plugs in to the RJ45 port on the Type2 EventSensor labeled Control. Additional Type2 EventSensors are chained together from the port labeled Sensor on the first EventSensor, to the port labeled Control on the next EventSensor, using Cat-5 straight-thru cable. Be sure to set the dip switches for each additional EventSensor so that each occupies it's own Slot as per the chart below.

### Dip Switch Settings

Defines up to 16 address locations (however only Slots 1 thru 8 are currently available for maximum 3 EventSensors) Note that the dip switch is numbered from left to right 1 through 4. The Most Significant Bit (MSB) is switch location 1.

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

### Temperature Sensor Setup (ES-T)

```

TeleBoss 830 - External Temperature Event
Device Number: 1            Device ID: 01100000            Device Name: Type2 ES-T
A) Temperature Sensor Enabled            [OFF]
B) Sensor Values Represented in            [FAHRENHEIT]
C) Temperature Deadband                    [3]
D) Very High Event Settings                [100] []                                    [120] [Info]
E) High Event Settings                     [80] []                                    [120] [Info]
F) Return to Normal Settings               [-] []                                    [120] [Info]
G) Low Event Settings                      [50] []                                    [120] [Info]
H) Very Low Event Settings                 [30] []                                    [120] [Info]
    
```

**Temperature Sensor Enabled** is an ON/OFF toggle to enable the temperature sensor. Default setting is OFF.

**Sensor Values Represented In** toggles either FAHRENHEIT or CELSIUS for the desired temperature scale.

**Temperature Deadband** is the range, in degrees, on either side of a temperature setting that prevents the alarm from repeatedly going in and out of the "alarm state" as the actual temperature fluctuates above and below the temperature setting. Default setting is 3 degrees.

**Very High/High/Low/Very Low Event Settings** display a menu where the temperature at each level can be configured to alarm along with the action(s) to occur, trap number, and class. In the case of Very High or High levels, the alarm will occur as the temperature rises above the setting. In the case of Low or Very Low, the alarm will occur as the temperature drops below the setting.

**Return to Normal Settings** displays a menu where the actions to occur when the temperature returns to normal (drops below the High/Very High settings, or rises above the Low/Very Low settings) can be configured.

### **Very High/High/Low/Very Low Event Settings Setup**

```

TeleBoss 830 - External Temperature Event Settings
Device Number: 1      Device ID: 01100000      Device Name: Type2 ES-T
A) Very High Event Temperature      [100]
B) Very High Event Actions           []
C) Very High Event Trap Number       [120]
D) Very High Event Class              [Info]

```

The menu for setting Very High Temperature settings is shown. Menus for High/Low/Very Low are identical.

**Very High Event Temperature** sets the temperature at which the Very High Event Actions will be triggered.

**Very High Event Actions** 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 [Action List](#) in the Features chapter for more information.

**Very High Trap Number** 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 Temperature Events is 120, but any number in the alternate range of 1000 – 1199 can be used.

**Very High Event Class** sets 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 event.

### **Return to Normal Settings Setup**

```

TeleBoss 830 - External Temperature Event Settings
Device Number: 1      Device ID: 01100000      Device Name: Type2 ES-T
A) Return to Normal Event Actions    []
B) Return to Normal Event Trap Number [120]
C) Return to Normal Class            [Info]

```

**Return to Normal Event Actions** 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 [Action List](#) in the Features chapter for more information.

**Return to Normal Event Trap Number** 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 Temperature Events is 120, but any number in the alternate range of 1000 – 1199 can be used.

**Return to Normal Class** sets 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 event.

### **Humidity Sensor Setup**

```

TeleBoss 830 - External Humidity Event
Device Number: 2      Device ID: 08110000      Device Name: Type2 ES-TH
A) Humidity Sensor Enabled           [OFF]
B) Humidity Deadband                 [3]
C) Very High Event Settings          [90] [] [130] [Info]
D) High Event Settings               [80] [] [130] [Info]
E) Return to Normal Settings         [-] [] [130] [Info]
F) Low Event Settings               [20] [] [130] [Info]
G) Very Low Event Settings           [10] [] [130] [Info]

```

**Humidity Sensor Enabled** is an ON/OFF toggle to enable the humidity sensor. Default setting is OFF.

**Humidity Deadband** is the range on either side of a humidity setting that prevents the alarm from repeatedly going in and out off the "alarm state" as the actual humidity fluctuates above and below the humidity setting. Default setting is 3 percent.

[Very High/High/Low/Very Low Event Settings](#) display a menu where the humidity at each level can be configured to alarm along with the action(s) to occur, trap number, and class. In the case of Very High or High levels, the alarm will occur as the humidity rises above the setting. In the case of Low or Very Low, the alarm will occur as the humidity drops below the setting.

[Return to Normal Settings](#) displays a menu where the actions to occur when the humidity returns to normal (drops below the High/Very High settings, or rises above the Low/Very Low settings) can be configured.

**Very High/High/Low/Very Low Event Settings Setup**

```

TeleBoss 830 - External Humidity Event Settings
Device Number: 2          Device ID: 08110000      Device Name: Type2 ES-TH
A) High Event Humidity           [80]
B) High Event Actions             []
C) High Event Trap Number        [130]
D) High Event Class               [Info]
    
```

The menu for setting High Humidity settings is shown. Menus for Very High/Low/Very Low are identical.

**High Event Humidity** sets the humidity at which the High Event Actions will be triggered.

**High Event Actions** 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 [Action List](#) in the Features chapter for more information.

**High Trap Number** 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 Humidity Events is 130, but any number in the alternate range of 1000 – 1199 can be used.

**High Event Class** sets 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 event.

**Return to Normal Settings Setup**

```

TeleBoss 830 - External Humidity Event Settings
Device Number: 2          Device ID: 08110000      Device Name: Type2 ES-TH
A) Return to Normal Event Actions  []
B) Return to Normal Event Trap Number [130]
C) Return to Normal Event Class     [Info]
    
```

**Return to Normal Event Actions** 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 [Action List](#) in the Features chapter for more information.

**Return to Normal Event Trap Number** 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 Humidity Events is 130, but any number in the alternate range of 1000 – 1199 can be used.

**Return to Normal Class** sets 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 event.

## Customizable Command Prompt

This feature allows the prompt in the command processor to be customized, and includes the ability to embed one or more settings values in the prompt. A customized command prompt can help simplify administration of units, particularly where multiple units are involved.

The command prompt setting is available in the General setup menu section, and via the Setting Key `sys.prompt`. The setting can contain up to 64 characters, but the prompt itself is limited to 30 characters; any additional characters are truncated.

In addition to specifying plain text to be included in the command prompt, setting values can be embedded using a special syntax: `$(setting_key_name)`. If this construct is used, the value of the specified setting key replaces the construct. If the setting key is not accessible for any reason (invalid key, insufficient user access level, etc), "ERROR" is displayed instead.

Note: T830-0 only supports the 'sys.sitename' setting key; all others return "ERROR".  
To make the system prompt blank, set `sys.prompt` to a null value (i.e. "`sk sys.prompt =`").

### Examples:

Set prompt to be ">"

Via Setup menu: Enter new prompt: >  
Via Setting Key: `sk sys.prompt = >`

Set prompt to be "Site Name"

Via Setup menu: Enter new prompt: TeleBoss (or whatever the site name is)  
Via Setting Key: `sk sys.prompt = "$(sys.sitename) "`

Set prompt to be "System Date and Time>"

Via Setup menu: The date and time entered via the Prompt option do not change as the actual date and time progress. What you enter here will always be displayed as the prompt, until you change it. If you want the date/time prompt to change with the system clock, then change it via the Setting Key entry describe below.

Via Setting Key: `sk sys.prompt = $(sys.clock.date) $(sys.clock.time)>`

## IP Record Collection (IPRC)

The T830-0 supports the following IP Record Collection protocols/IP-enabled switches:

[Generic Server](#)

[Avaya – Reliable Session Protocol](#)

[Alcatel OmniPCX](#)

[CCM4 \(Cisco CallManager version 4.x\)](#)

[Generic Client](#)

- [Siemens HiPath 4000](#)

[Intecom Telari](#)

[Nortel BCM](#)

[Syslog](#)

[NEC NEAX2400](#)

[CCM5 \(Cisco CallManager version 5.x\)](#)

### Generic Server

#### Definition

Generic Server is plain text record collection that offers no handshaking or quality control above that of the TCP/IP protocols. Therefore, this method of record collection is not specific to Avaya Definity in that there is no application-layer protocol. Plain Text IPRC data is received on TCP port 5000 (user-adjustable).

#### Commands

Command	Function
IPRC	Displays a status report of the active IPRC mode.
IPRC STATUS	
IPRC ?	

#### Status Display

The IPRC command brings up a status report similar to the following report for Generic Server:

```
iprc
Record Collection Server
Status: Listening on port 5000
```

This report simply indicates the status of the RCS. The TCP port is displayed for informational purposes only.



## Avaya Definity RSP

### Definition

Reliable Session Protocol (RSP) is Avaya's solution to the problem of lost connections while transferring valuable call record data. This protocol is used on both the client (PBX) and server (Data-Link) sides to ensure that if the data connection breaks, no records are lost. This is accomplished by the two devices repeatedly checking in with one another. If the connection is lost, an alarm sent out by the Data-Link (and the PBX if so configured), and the PBX will begin to buffer its own data until the connection is restored.

### Commands

Command	Function
IPRC or IPRC STATUS or IPRC ?	Displays a status report of the active IPRC mode.
IPRC PORT n	Changes the TCP port on which to listen for RSP connections.
IPRC RESET	Manually disconnects the current session (if connected), closes the socket (if established), and reinitializes the server.

### Status Display

The IPRC command brings up a status report similar to the following report for RSP:

```
RSP Server
Status: Listening on port 9000
SAMs tx      : 0
ACKs tx      : 0
SDMs tx      : 0
SCMs rx      : 0
New data rx  : 0
Blocks rx    : 0
Dup. blocks rx : 0
```

### IPRC Terms

The following terms are used in the status display accessed by the IPRC command for RSP:

Term	Meaning
<b>SAM (Session Accept Message)</b>	A message transmitted by the T830-0 to acknowledge the client's Session Connect Message.
<b>ACK (session Acknowledgement message)</b>	A response transmitted by the T830-0 to acknowledge data blocks.
<b>SDM (Session Disconnect Message)</b>	A command sent from the T830-0 to terminate the current session. This happens when the T830-0 encounters an anomaly in the protocol or the user resets the server.
<b>SCM (Session Connect Message)</b>	A request transmitted from the client to establish a session with the T830-0's IPRC server.
<b>New Data Blocks</b>	The number of non-duplicate bytes received by the server. Represents the number of blocks (including duplicates) received by the unit.
<b>Dup. Blocks</b>	The number of duplicate blocks received by the unit. If this number is high relative to the number of blocks received, either the SPDU Response Timer (ST2) on the switch needs to be increased or the T830-0 is full and needs to be polled.

## Alcatel OmniPCX 4400

### Definition

The T830-0 supports the Alcatel OmniPCX 4400 ticket system of IPRC. This method involves receiving large data packets or tickets via TCP. These tickets contain many different data fields that may not be useful to a system administrator. The T830-0 allows an administrator to use a configuration file that selects exactly which records to store in the CDR database.

### Commands

Command	Function
SK SET X	Initiates a settings key file upload via Xmodem.
SK SET A	Initiates a settings key file upload via plaintext ASCII.
SK LOG	Displays results of uploading the settings key file.
IPRC START	Opens a connection to the PBX if not already open. This is required if the unit was unable to connect to the PBX at boot because of improper settings.
IPRC STOP	Places the client into an idle state. Closes any open connection.
IPRC or IPRC STATUS or IPRC ?	Displays a status report of the active IPRC mode.
IPRC FIELDS	Displays the list of compiled output fields.
IPRC DEBUG ON	Show the ticket data as it is parsed.
IPRC DEBUG OFF	Disables showing ticket data as it is parsed.

### Status Display

The following is an example status display for Alcatel OmniPCX IPRC:

```
Alcatel OmniPCX 4400 Real Time Client
Status: Idle
Last Error: No fields active (0/00:00:06 ago)
Seconds until next state: 0
Tickets processed: 00000000
```

### The Configuration File

The ticket parsing functionality is configured via a configuration file. This configuration file is a list of setting keys, where a setting key is a "<setting> = <value>" statement. <setting> is a period-delimited string of keywords. These keys can name all of the setup variables of the product. These include the generic operational parameters of the box such as these below, as well as specialized parameters such as those for the OmniPCX:

```
net.ip=192.168.100.32
net.subnet=255.255.255.0
net.router=192.168.100.100
net.snmp[1]=192.168.100.36
net.snmp[2]=0.0.0.0
net.snmpcomm=public
```

The unit assembles output fields into records defined by their end-of-line characters. Using this method we can specify output fields using the specific ticket field numbers (1-48) or by character start position and length within the ticket structure. For example, if the user wants to create an output record which contains these fields:

Call Type, Start Date Time, End Date Time, Effective Call Duration (converted from seconds to HH:MM:SS format), Acting Extension Number, Trunk 1 and the user wants to specify the record using TICKET FIELD NUMBERS, the setup would look like this:

```
alcatel.ip=22.23.212.12
alcatel.port = 2533
alcatel.timeout = 30
alcatel.field[1]=10,2,L // Call Type
alcatel.field[2]=40,17,L // Start Date Time
alcatel.field[3]=12,17,L // End Date Time
alcatel.field[4]=38,10,L,STOHMS // Effective Call Duration
alcatel.field[5]=41,25,R // Acting Extension Number
alcatel.field[6]=16,5,5,L // Trunk Identity
alcatel.field[7]=9,30,L // Calling Number
alcatel.field[8]=2,30,L,OD0A // Called Number
```

In the above, the field definition arguments are:

<field>=<ticket field # , length of that field to take, justification[,end of line chars][,conversion]>

The OD0A terminator on field 8 tells the unit to store all assembled output fields up to and including that output field (in ascending order of field definition number) as 1 record. Note that the OD0A optional value places the end-of-line characters on the last field, but you could include the EOL characters at other fields also so as to make multiple records. If the final field definition does not have any EOL characters, then the unit stores whatever it has assembled so far as 1 record, appended with either:

1. the first EOL character set found in any other field definition starting with the first field, or
2. CRLF, if no other field definitions have EOL characters.

If we wanted to use explicit character position values, the setup would look like this:

```
alcatel.ip=22.23.212.12
alcatel.port = 2533
alcatel.timeout = 30
alcatel.field[1]=166,2,2,R // Call Type
alcatel.field[2]=441,17,17,L // Start Date Time
alcatel.field[3]=169,17,17,L // End Date Time
alcatel.field[4]=430,10,10,R,STOHMS // Effective Call Duration
alcatel.field[5]=458,30,20,L // Acting Extension Number
alcatel.field[6]=211,5,5,R // Trunk Identity
alcatel.field[7]=136,30,30,L // Calling Number
alcatel.field[8]=5,30,30,L,OD0A // Called Number
```

In the above, the field definition arguments are:

<field>=<start pos, how long the field is, length of that field to take, justification[,end of line chars][,conversion]>

Once a configuration file is uploaded to the unit, the T830-0 indicates that it is processing the data. It returns "COMPLETE" when all settings are processed. The unit gives no other progress or status feedback to the user while it is processing the file. Instead, it logs feedback to a file that the user can view after processing is complete. If there were any problems, the unit will display an error message after processing is complete.

To view the log, enter the **SK LOG** command. This will display which settings, if any, it failed to process because of bad value, key name, or syntax. Bear in mind, this upload process does not attempt to error check the output field definitions, it only stores them. Instead, the real time client verifies these field definitions when it is started. If the client is idle (you can tell the client's state by entering the **IPRC STATUS** command), you must start the client in order to tell it to compile the settings (**IPRC START** command).

**Limits of field definitions**

There is room for up to 3 EOL characters for each field definition. Null is an invalid EOL character. There are 2 available conversion options, if conversion is desired, for each field definition: STOHMS and MTOHMS. STOHMS assumes the input data from the ticket is a value represented in seconds, and it will convert this value to hh:mm:ss format in the output field. MTOHMS works like STOHMS except it assumes the value to be converted is in minutes. The maximum output field length is 300 characters. The maximum record length is 520 characters.

Aside from the up to 48 output fields, there are 6 other items to configure:

Setting	Function
alcatel.ip	IP address of PBX.
alcatel.port	TCP port of PBX real time interface. Default is 2533.
alcatel.timeout	Timeout (in seconds) used for waiting for packets and connection retries. Default is 30.
alcatel.delim	Output field delimiter. This is a 1-byte value, expressed as ASCII-HEX. If it is non-zero, then this byte is appended to each unterminated output field. For example, to separate each output field with a space, assign this key the value of "20". Default is "00".
net.iprc.mode = ALCATEL OMNIPCX	Selects the client as the active IPRC service.
Net.iprc.file	Selects the database file used for record storage.

**Standard Ticket Fields**

There are 47 ticket fields to choose from when paring down which data you would like to keep from the incoming tickets. This section covers each of the fields, their location and size in the ticket, and the alignment of the data within the field. When specifying an output field using TICKET FIELD NUMBERS, the unit uses this standard ticket format:

**Note:** Ticket structure is subject to change by Alcatel. You should refer to the latest Alcatel documentation if there is any problem or question.

Field	Name	Position	Size	Alignment
1	Ticket Version	0-4	5	L
2	Called Number	5-34	30	L
3	Charged Number	35-64	30	L
4	Charged User Name	65-84	20	L
5	Charged Cost Center	85-94	10	L
6	Charged Company	95-110	16	L
7	Charged Party Node	111-115	5	R
8	Charged Party Subaddress	116-135	20	L
9	Calling Number	136-165	30	L
10	Call Type	166-167	2	R
11	Cost Type	168	1	NA
12	End Date-Time	169-185	17	NA
13	Charge Units	186-190	5	R
14	Cost Info	191-200	10	R
15	Duration	201-210	10	R
16	Trunk Identity	211-215	5	R
17	Trunk Group ID	216-220	5	R
18	Trunk Node	221-225	5	R
19	Personal/Business Call	226	1	NA
20	Access Code	227-242	16	L
21	Specific Charge Info	243-249	7	NA
22	Bearer Capability	250	1	NA
23	High Level Compatibility	251-252	2	R
24	Data Volume	253-262	10	R
25	User To User Volume	263-267	5	R
26	External Facilities	268-307	40	NA
27	Internal Facilities	308-347	40	NA
28	Call Reference	348-357	10	R
29	Segments-Rate 1	358-367	10	R

30	Segments-Rate 2	368-377	10	R
31	Segments-Rate 3	378-387	10	R
32	Com Type	388	1	NA
33	X25 In Flow Rate	389-390	2	R
34	X25 Out Flow Rate	391-392	2	R
35	Carrier	393-394	2	R
36	Initial Dialed Number	395-424	30	L
37	Waiting Duration	425-429	5	R
38	Effective Call Duration	430-439	10	R
39	Redirected Call Indicator	440	1	NA
40	Start Date-time	441-457	17	NA
41	Acting Extension Number	458-487	30	L
42	Called Number Node	488-492	5	R
43	Calling Number Node	493-497	5	R
44	Initial Dialed Number Node	498-502	5	R
45	Acting Extension Number Node	503-507	5	R
46	Transit Trunk Group ID	508-512	5	R
47	EndOfLine (0x0A)	513	1	NA

### The Real Time Client

The client is idle whenever there are no configured OmniPCX settings. After you upload a configuration file for the first time, type **"IPRC START"** to start the client. Then type **"IPRC STATUS"** or **"IPRC ?"** to check the current status. It will either indicate a working status (e.g., "Established - awaiting packet") or if something is wrong (e.g., unable to connect to the OmniPCX, or a certain output field definition doesn't make sense). All output field definitions must compile correctly in order for the unit to accept the configuration and attempt to connect to the OmniPCX.

Once the client has accepted a valid configuration, it will attempt to connect to the OmniPCX whenever the unit is reset. If the user manually stops the client with the **IPRC STOP** command, then the client will remain in the idle state until either the unit is reset or the user enters the **IPRC START** command.

If a new configuration is uploaded while the client is connected to the PBX, then it will:

1. Disconnect from the PBX if the configuration is invalid.
2. Stay connected to the PBX using the new configuration, if the configuration is valid and the PBX IP address or TCP port did not change.
3. Disconnect from the PBX and reconnect using the new configuration, if the configuration is valid and the PBX IP address or TCP port changed.

## CCM 4 (Cisco CallManager version 4.x)

### Definition

The T830-0 supports the Cisco CallManager 4.x software. This method involves querying the Cisco CallManager database using SQL commands. The database contains many different fields that may not be useful to a system administrator. The T830-0 allows an administrator to use a configuration file that selects exactly which fields to retrieve from the Cisco CallManager database.

### Commands

Command	Function
SK SET X	Initiates a settings key file upload via Xmodem.
SK SET A	Initiates a settings key file upload via plaintext ASCII.
SK LOG	Displays results of uploading the settings key file.
IPRC START	Causes immediate connection to CallManager to retrieve any new records, followed by automatic connection at the interval specified by the connection interval setting. When the T830-0 starts up in Cisco CallManager IPRC mode, and a non-zero connection interval is set, automatic connection is enabled. This command is only required if automatic connection was previously stopped using the IPRC STOP command, or the connection interval was changed from zero to a non-zero value.
IPRC STOP	Disables automatic connection to CallManager, and terminates any open connection. Automatic connection is re-enabled if the T830-0 is restarted.
IPRC NOW [value]	Causes the T830-0 to connect to CallManager immediately and retrieve any available new records. If value is specified, it will only retrieve that many records even if more are available.
IPRC DBINFO	Causes the T830-0 to connect to CallManager immediately and retrieve and display the total number of records present, and the date/time stamp of the first and last records.
IPRC or IPRC STATUS or IPRC ?	Displays a status report of the active IPRC mode.
IPRC FIELDS	Displays the list of compiled output fields.
IPRC LOG	Shows any messages returned by the CallManager server during the last non-interactive connection attempt. This information can be useful for troubleshooting.
IPRC INTERACTIVE	Causes the T830-0 to connect to CallManager, and then present an interface for entering SQL commands to be sent to CallManager. The results of any SQL commands are displayed on-screen, and are not stored in the T830-0 database. Field settings do not apply in interactive mode.

### Status Display

The following is an example status display for Cisco CallManager IPRC:

```
Cisco CallManager IPRC Status
State: Waiting
Last result: Retrieved 5 records (connected 0/00:00:23 ago for 00:00:07)
Time until next connection: 00:09:36
Records processed: 00000730
```

## Configuration File

The record retrieving functionality is configured via a configuration file. This configuration file is a list of setting keys, where a setting key is a "<setting> = <value>" statement. <setting> is a period-delimited string of keywords. These keys can name all of the setup variables of the product. These include the generic operational parameters of the box such as these below, as well as specialized parameters such as those for the Cisco CallManager:

```
net.ip=192.168.100.32
net.subnet=255.255.255.0
net.router=192.168.100.100
net.snmp[1]=192.168.100.36
net.snmp[2]=0.0.0.0
net.snmpcomm=public
```

The unit queries the CallManager database and, for each available record, retrieves the values (columns) specified in the field table. The retrieved values are assembled into records as defined in the field table. Using this method we can specify output fields using the specific database column numbers (shown in the tables below), or by specifying the exact name of the database column.

Values can be retrieved from two CallManager tables: CallDetailRecord (CDR), and CallDetailRecordDiagnostic (CMR). When CMR values are specified, values are retrieved only from CMR records that are related to CDR records included in the query. When specifying fields, each field name/number is prefixed by "cdr." or "cmr." depending on which table the field is coming from.

For example, if the user wants to create an output record which contains these fields:

cdr.dateTimeDisconnect, cdr.originalCalledPartyNumber, cdr.finalCalledPartyNumber, cdr.dateTimeOrigination (converted to MM/DD/YYYY HH:MM:SS format), cdr.origIPAddr (converted to 4-dot notation), cdr.duration, cmr.jitter, and cmr.latency, and the user wants to specify the fields using COLUMN NUMBERS, the field setup would look like this:

```
iprc.field[1]=cdr.38,10,R // Date/time disconnect (integer format)
iprc.field[2]=cdr.26,25,R // Original called party number
iprc.field[3]=cdr.28,25,R // Final called party number
iprc.field[4]=cdr.5,17,R,NTOD // Date/time origination (date/time format)
iprc.field[5]=cdr.10,15,R,NTOIP // Orig IP address (4-dot notation)
iprc.field[6]=cdr.39,10,R // Duration
iprc.field[7]=cmr.13,10,R // Jitter
iprc.field[8]=cmr.14,10,R,OD0A // Latency
```

In the above, the field definition arguments are:

```
<field>=<column#, length of that value to take, justification[,end of line chars][,conversion]>
```

If the specified length is greater than the length of the returned value, then the returned value is padded with spaces and justified within the output field based on the justification specification. 'L' means the value is left-aligned, 'R' means the value is right-aligned, and 'N' means the output field retains the size of the returned value and is not padded with spaces.

The OD0A terminator on field 8 tells the unit to append CRLF to the end of that field. Note that in this example the OD0A optional value places the end-of-line characters on the last field, but you could include the EOL characters at other fields also so as to break the record into multiple lines. If the final field definition does not have any EOL characters specified, then the unit appends CRLF automatically.

If we wanted to use explicit column names (if, for example, a column is desired that is not in the COLUMN NUMBER table), the setup would look like this:

```

iprc.field[1]= cdr.dateTimeDisconnect,10,R // Date/time disconnect (integer format)
iprc.field[2]= cdr.originalCalledPartyNumber,25,R // Original called party number
iprc.field[3]= cdr.finalCalledPartyNumber,25,R // Final called party number
iprc.field[4]= cdr.dateTimeOrigination,17,R,NTOD // Date/time origination (date/time
format)
iprc.field[5]= cdr.origIPAddr,15,R // Orig IP address (4-dot notation)
iprc.field[6]= cdr.duration,10,R // Duration
iprc.field[7]= cmr.jitter,10,R // Jitter
iprc.field[8]= cmr.latency,10,R,0D0A // Latency
    
```

In the above, the field definition arguments are: <field>=<column name, length of that field to take, justification[,end of line chars][,conversion]>

Once a configuration file is uploaded to the unit, the T830-0 indicates that it is processing the data. It returns "COMPLETE" when all settings are processed. The unit gives no other progress or status feedback to the user while it is processing the file. Instead, it logs feedback to a file that the user can view after processing is complete. If there were any problems, the unit will display an error message after processing is complete.

To view the log, enter the **SK LOG** command. This will display which settings, if any, it failed to process because of bad value, key name, or syntax. This upload process does not attempt to error check the output field definitions, it only stores them. Instead, the fields are verified when a connection attempt is made to the CallManager server.

**Limits of field definitions**

There is room for up to 3 EOL characters for each field definition. Null is an invalid EOL character. There are 2 available conversion options, if conversion is desired, for each field definition: NTOD and NTOIP. NTOD assumes the value is a coordinated universal time (UTC) value that represents the number of seconds since midnight (00:00:00) Jan. 1, 1970, and it will convert this value to "mo/dd/year hh:mm:ss" format in the output field. NTOIP assumes the value is a 32-bit representation of an IP address with the bytes reversed, so that the high-order byte contains the low-order IP address octet, and so on; the value is converted to a standard 4-dot IP address representation. The maximum output field length is 160 characters. The maximum total record length is 800 characters.

Aside from the up to 48 output fields, there are some other items to configure:

Setting	Function
iprc.mode	Selects the client as the active IPRC service.
iprc.file	Selects the database file used for record storage.
iprc.ccm.database	The name of the CallManager database containing call detail records.
iprc.ccm.username	The username for logging into the CallManager server.
iprc.ccm.password	The password for logging into the CallManager server.
iprc.ccm.interval	Determines how often the T830-0 connects to the CallManager server to retrieve new records, in minutes. Setting this value to 0 effectively disables automatic connection.
iprc.ccm.delimiter	Output field delimiter. This is a 1-byte value, expressed as ASCII-HEX. If it is non-zero, then this byte is appended to each unterminated output field. For example, to separate each output field with a space, assign this key the value of "20". Default is "00".
iprc.ccm.startdate	The date and time, in "MM/DD/YYYY HH:MM:SS" format, that determines which records in the CCM database are considered new records. By default, when CCM IPRC is enabled for the first time, the T830-0 retrieves records that are time stamped on or after midnight the day before, according to the T830-0 system clock. After each non-interactive connection to the CCM server, this setting is updated to reflect the last "new record" date/time.

There are 67 columns to choose from in the CallManager database – 50 in the CDR table, and 17 in the CMR table. When specifying an output field using COLUMN NUMBERS, the unit uses these standard CallManager columns:

**Note:** The CallManager database structure is subject to change by Cisco. You should refer to the latest Cisco documentation if there is any problem or question.



## CallDetailRecord Fields

Field	Name	Max Length*	Data Type
1	cdrRecordType	10	Number
2	globalCallID_callId	10	Number
3	globalCallID_callManagerId	10	Number
4	origLegCallIdentifier	10	Number
5	dateTimeOrigination	10/19	Number
6	origNodeid	10	Number
7	origSpan	10	Number
8	callingPartyNumber	25	Text
9	origIpPort	10	Number
10	origIpAddr	10/15	Number
11	originalCallingPartyNumberPartition	50	Text
12	origCause_location	10	Number
13	origCause_value	10	Number
14	origMediaTransportAddress_IP	10/15	Number
15	origMediaTransportAddress_Port	10	Number
16	origMediaCap_payloadCapability	10	Number
17	origMediaCap_maxFramesPerPacket	10	Number
18	origMediaCap_g723BitRate	10	Number
19	lastRedirectDn	25	Text
20	lastRedirectDnPartition	50	Text
21	destLegIdentifier	10	Number
22	destNodeid	10	Number
23	destSpan	10	Number
24	destIpAddr	10/15	Number
25	destIpPort	10	Number
26	originalCalledPartyNumber	25	Text
27	originalCalledPartyNumberPartition	50	Text
28	finalCalledPartyNumber	25	Text
29	finalCalledPartyNumberPartition	50	Text
30	destCause_location	10	Number
31	destCause_value	10	Number
32	destMediaTransportAddress_IP	10/15	Number
33	destMediaTransportAddress_Port	10	Number
34	destMediaCap_payloadCapability	10	Number
35	destMediaCap_maxFramesPerPacket	10	Number
36	destMediaCap_g723BitRate	10	Number
37	dateTimeConnect	10/19	Number
38	dateTimeDisconnect	10/19	Number
39	duration	10	Number
40	origDeviceName	129	Text
41	destDeviceName	129	Text
42	origCallTerminationOnBehalfOf	10	Number
43	destCallTerminationOnBehalfOf	10	Number
44	origCalledPartyRedirectOnBehalfOf	10	Number
45	lastRedirectRedirectOnBehalfOf	10	Number
46	origCalledPartyRedirectReason	10	Number
47	lastRedirectRedirectReason	10	Number
48	joinOnBehalfOf	10	Number
49	destConversationId	10	Number
50	globalCallID_ClusterID	50	Text

» **Note:** Max Length specifies the number of characters to represent the maximum possible value. Where two numbers are supplied, the second number specifies the number of characters after performing the usual conversion on that particular type of value.

**CallDetailRecordDiagnostic Fields**

Field	Name	Max Length*	Data Type
1	cdrRecordType	10	Number
2	globalCallID_callManagerId	10	Number
3	globalCallID_callId	10	Number
4	nodeId	10	Number
5	directoryNum	50	Text
6	callIdentifier	10	Number
7	dateTimeStamp	10/19	Number
8	numberPacketsSent	10	Number
9	numberOctetsSent	10	Number
10	numberPacketsReceived	10	Number
11	numberOctetsReceived	10	Number
12	numberPacketsLost	10	Number
13	jitter	10	Number
14	latency	10	Number
15	directoryNumPartition	50	Text
16	globalCallID_ClusterID	50	Text
17	deviceName	129	Text

**CallManager Operation**

After the T830-0 is reset, or Cisco CallManager IPRC mode is selected, the unit attempts to connect to the CallManager server using the settings provided. Once successfully connected, the unit will retrieve any new records and store them into the specified T830-0 database file, and then disconnect from the CallManager. This operation is repeated at the interval specified in the settings, regardless of whether the previous connection attempt was successful. If a record retrieval session is in progress when the interval expires (that is, either automatic or via **IPRC NOW** command), the interval timer is reset and the next connection is deferred until the next interval expires.

The IPRC status command (**IPRC**, **IPRC STATUS**, or **IPRC ?**) provides information about the current state, as well as the result of the last connection attempt. Additional information may be available via the **IPRC LOG** command.

When a connection is made to the CallManager server, the settings in effect at the beginning of that session are used; IPRC settings changes that are made during the session are ignored.

## Generic Client

### Definition

Generic Client IPRC is a TCP/IP client that runs on the T830-0 and attempts connections to a specified host to download records. This connection is a clear text telnet protocol, typically over port 1752.

### Commands

Command	Function
IPRC	Displays a status report of the active IPRC mode.
IPRC STATUS	
IPRC ?	

### Status Display

The IPRC command brings up a status report similar to the following report:

```
Record Collection Client
Status: Waiting to open connection
Last error: None
```

### Siemens HiPath 4000

The Siemens HiPath 4000 uses the Generic Client protocol in the T830-0. Setup is as described below:

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection      [GENERIC CLIENT] <<<<<<
B) Store Collected Data In  [FILE1]
C) Data Alarm/Filter Enable  [OFF]
D) Target Name               [IPRC 1]
E) Hostname/IP Address       [192.0.2.3] <<<<<<
F) Port                      [1201] <<<<<<
G) Time Stamping            [OFF]
H) Multiline Record Enable   [OFF]
```

The HiPath sends CDR via Plain text Telnet. Use **Generic Client** in the T830-0 to connect to the PBX "Atlantic" Port - an Ethernet port that is dedicated for CDR only. It is always set to 192.0.2.3.

Port is 1201 by default.

The T830-0 ETH1 IP Address **MUST** be set to 192.0.2.x.

Use of a Default Router is also very difficult w/ this IP setup; it is best to leave it blank.

To setup a T830-0 for the HiPath, one merely needs to configure the T830-0 Ethernet IP address as directed by the Siemens Tech, and configure IP Record Collection for Generic Server as shown above.

Polling via network (FTP push, FTP "get", Real Time Sockets) can be accomplished using the 2<sup>nd</sup> Ethernet Port on the T830-0.

## Intecom Telari

### Definition

Intecom Telari is IPRC from EADS (f.k.a. Intecom) E and Telari switches. In this method of IP record collection, a TCP/IP client on the unit attempts connections and accepts CDR via the connection. This method of IPRC differs from Generic Client in that it employs a proprietary application-layer protocol to transmit records.

### Configuration:

```

TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [INTECOM TELARI]
B) Store Collected Data In      [FILE1]
C) Data Alarm/Filter Enable     [OFF]
D) Target Name                   [IPRC 1]
E) Hostname/IP Address          []
F) Port                          [8186]
G) Connection Interval (minutes) [1]
H) Time Stamping                 [OFF]
    
```

**IP Record Collection** sets the protocol to be used to Intecom Telari.

**Store Collected Data In** toggles the FILE to which all incoming Syslog data will be stored. Options are FILE1, FILE2, AUX1, AUX2, and AUX3. Default setting is FILE1.

**Data Alarm/Filter Enable** is an ON/OFF toggle to set whether configured Data Alarms or Filters will be applied to the incoming data. Default setting is OFF.

**Target Name** is the name used to identify the switch when an IPRC Connection Lost Alarm is sent via an AsentriaAlarm. (The T830-0 does not support IPRC Connection Lost Alarms' therefore this field is not used)

**Hostname/IP Address** sets the hostname or IP Address of the Telari Record Collection Server (RCS).

**Port** set the TCP port used by the Telari RCS. Default setting is port 8186.

**Connection Interval (minutes)** sets the number of minutes (1 – 65535) to wait before disconnecting an idle connection. Default setting is 1.

**Time Stamping** is an ON/OFF toggle to set whether each individual call record is stamped with the Date and Time received in the T830-0. Default setting is OFF.

### Commands

Command	Function
IPRC	Displays a status report of the active IPRC mode.
IPRC STATUS	
IPRC ?	
IPRC Connect	Forces the client to connect from a state where it's waiting to connect.
IPRC Start	Causes immediate connection to the server to retrieve any new records and to resume regular checking. This command is only required if automatic connection was previously stopped using the IPRC STOP command.
IPRC Stop	Disables automatic connection and terminates any open connection. Automatic connection is re-enabled if the T830-0 is restarted.

### Status Display

The IPRC command brings up a status report similar to the following report:

```

Intecom CDR Client
Status:      Idle
Time now:    12/16 12:24:10
COMPLETE
    
```

## Nortel BCM

The Nortel Business Communications Manager (BCM) sends call records to the T830-0 using FTP. Therefore, the T830-0 must be configured to allow an incoming FTP connection from the BCM, including logging in with a user name and password. To do this, there are three things to configure – two on the T830-0 and one on the BCM.

### On the T830-0:

1) Configure IPRC for Nortel BCM as shown:

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [NORTEL BCM]
B) Store Collected Data In      [FILE1]
```

2) Configure any unused user with User Name: **bcm**, Password: **bcm**, Allow User Connection via **FTP**, and Upon Login the Go To **COMMAND**. The remaining menu options do not matter.

```
TeleBoss 830 - User Setup Menu
A) Enable This User Access       [ON]
B) User Name                     [bcm]
C) Password                      [*****]
D) Allow User Connection via     [F]
E) Upon Login then Go To        [COMMAND]
F) Set Access/Pass-through Pointer To [FILE1]
G) Pass-through Permissions
H) After PT, ESC Takes User To  [MENU]
I) PPP Connection               [LOCAL]
J) Setup/Status Rights          [MASTER]
K) File Release Permissions
L) File Delete Permissions
```

### On the BCM:

The user should consult with the Nortel BCM technical personnel for exactly how to configure the BCM, but here is a brief outline of the Data File Transfer parameters that must be configured:

Transfer Type: (your preference)

- Push – Daily
- Push – Weekly
- Push – Monthly
- None

IP Address: **<the IP address of the T830-0>**

Remote User: **bcm**

Remote Password: **bcm**

Compress File Before Transfer: **NO**

Other settings on the BCM are your preference and Asentria cannot give advice as to how any of those should be set.

## Syslog

The Syslog IP Record Collection protocol allows the T830-0 to receive syslog messages from any Cisco voice-enabled router, including **Cisco CallManager Express**.

```

TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [SYSLOG]
B) Store Collected Data In      [FILE1]
C) Data Alarm/Filter Enable     [OFF]
D) Target Name                   [IPRC 1]
E) TCP Port                      [1468]
F) UDP Port                      [514]
G) Time Stamping                [OFF]
H) Multiline Record Enable      [OFF]
I) Division Target 1            []
J) Division Target 2            []

```

Syslog IP Record Collection protocol is based on the BSD Syslog protocol. Messages are typically a single line of text, however, they are occasionally longer than one line of text (> 506 bytes) so the T830-0 features an option to break the oversize record into multiple lines, and assemble the component single lines into one multiline record. The impact of this is that the user has to take this into account when defining data alarms. To make it more predictable to the user where the unit divides an oversize message, there are additional settings called **division targets** (strings up to 8 characters). If the unit needs to divide an oversize message, it tries to make it so that the division target is the beginning of the remainder piece. The BSD syslog protocol specifies that a message can be 1024 bytes. So the worst case is that the unit must store a 1024-byte single-line record. The minimum number of divisions necessary to break a 1024-byte message into records of acceptable size is 2. Therefore there are 2 division target settings. If the division targets fail to work through misconfiguration then the unit divides the message such that the 1st, 507th, and 1013th bytes are the first bytes of each of the new records.

**IP Record Collection** sets the protocol to be used to Syslog.

**Store Collected Data In** toggles the FILE to which all incoming Syslog data will be stored. Options are FILE1, FILE2, AUX1, AUX2, and AUX3. Default setting is FILE1.

**Data Alarm/Filter Enable** is an ON/OFF toggle to set whether configured Data Alarms or Filters will be applied to the incoming data. Default setting is OFF.

**Target Name** is the name used to identify the switch when an IPRC Connection Lost Alarm is sent via an AsentriaAlarm. (The T830-0 does not support IPRC Connection Lost Alarms' therefore this field is not used) Default setting is IPRC 1.

**TCP Port** sets the TCP port used by the sending Cisco device. Default setting is port 1468.

**UDP Port** sets the UDP port used by the sending Cisco device. Default setting is port 514.

**Time Stamping** is an ON/OFF toggle to set whether each individual call record is stamped with the Date and Time received in the T830-0. Default setting is OFF.

[Multiline Record Enable](#) displays the Multiline Record Settings menu.

**Division Target 1 / 2** are eight characters text strings used to designate the beginning of a section of a divided oversize record. Default settings are blank.

### Multiline Record Settings

```

TeleBoss 830 - IPRC Multiline Record Settings
A) Multiline Record Enable      [OFF]
B) Blank Line Count             [0]
C) Complex Multiline Detection  [OFF]

```

The T830-0 has the ability to monitor incoming Syslog CDR 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.

**Multiline Record Enable** is an ON/OFF toggle to enable multiline record detection. Default setting is OFF.

**Blank Line Count** sets the number of blank lines that must come between records. Default setting is 0.

**Complex Multiline Detection** displays settings for detecting more complex multiline records. Default setting is OFF.

TeleBoss 830 - IPRC 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** is an ON/OFF toggle to enable advanced multiline detection. Default setting is OFF.

**Start Field *n* Character Position** sets 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** sets 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** sets the number of blank lines that are between each record.

**End Detection** toggles between FORMULA, COUNT, and BLANKS to set the method of detecting the end of each record. Default setting is FORMULA.

**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** is the counterpart to start the text or character position option. This option sets the end delimiter for multiline records.

## NEC NEAX2400

The T830-0 collects data from the NEC NEAX2400 by opening a socket on a specific port. Generally, only the Hostname or IP Address of the switch is all that needs to be configured on the T830-0. Two other settings on the T830-0 that have the same default values as the corresponding settings in the switch: Port and Device Number. In certain cases where the switch is not configured to default port and device number, you may have to adjust these either on the switch or on the T830-0 to get IPRC running. The Device Number ranges from 0 to 3 (default 0 on the unit) and controls what kind of data the unit retrieves from the switch; refer to the NEAX2400 SMDR reference manual for details.

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [NEC NEAX2400]
B) Store Collected Data In      [FILE1]
C) Data Alarm/Filter Enable     [OFF]
D) Target Name                   [IPRC 1]
E) Hostname/IP Address          []
F) Port                          [60010]
G) Request Period (seconds)     [5]
H) Device Number                 [0]
I) Time Stamping                 [OFF]
```

**IP Record Collection** sets the protocol to be used to NEC NEAX2400.

**Store Collected Data In** toggles the FILE to which all incoming data will be stored. Options are FILE1, FILE2, AUX1, and AUX2. Default setting is FILE1.

**Data Alarm/Filter Enable** is an ON/OFF toggle to set whether configured Data Alarms or Filters will be applied to the incoming data. Default setting is OFF.

**Target Name** is the name used to identify the switch when an IPRC Connection Lost Alarm is sent via an AsentriaAlarm. (The T830-0 does not support IPRC Connection Lost Alarms' therefore this field is not used) Default setting is IPRC 1.

**TCP Port** sets the TCP port used by the sending Cisco device. Default setting is port 1468.

**UDP Port** sets the UDP port used by the sending Cisco device. Default setting is port 514.

**Time Stamping** is an ON/OFF toggle to set whether each individual call record is stamped with the Date and Time received in the T830-0. Default setting is OFF.



## CCM 5 (Cisco CallManager version 5.x)

Cisco CallManager version 5.x sends call records to the T830-0 using FTP. Therefore, the T830-0 must be configured to allow an incoming FTP connection from the CCM, including logging in with a user name and password. To do this, there are three things to configure – two on the T830-0 and one on the CCM.

### On the T830-0:

1) Configure IPRC for CCM 5 as shown:

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection           [CCM 5]
B) Store Collected Data In      [FILE1]
```

2) Configure any unused user with User Name: **ccm**, Password: **ccm**, Allow User Connection via **FTP**, and Upon Login the Go To **COMMAND**. The remaining menu options do not matter.

```
TeleBoss 830 - User Setup Menu
A) Enable This User Access       [ON]
B) User Name                     [ccm]
C) Password                      [*****]
D) Allow User Connection via     [F]
E) Upon Login then Go To        [COMMAND]
F) Set Access/Pass-through Pointer To [FILE1]
G) Pass-through Permissions
H) After PT, ESC Takes User To   [MENU]
I) PPP Connection               [LOCAL]
J) Setup/Status Rights          [MASTER]
K) File Release Permissions
L) File Delete Permissions
```

### On the CCM:

The user should consult with the Cisco technical personnel for exactly how to configure the CCM, but here is a brief outline of the Data File Transfer parameters that must be configured:

Transfer Type: (your preference)

- Push – Daily
- Push – Weekly
- Push – Monthly
- None

IP Address: **<the IP address of the T830-0>**

Remote User: **ccm**

Remote Password: **ccm**

Compress File Before Transfer: **NO**

Other settings on the CCM are your preference and Asentria cannot give advice as to how any of those should be set.

## Command Reference

### User Interface Commands

➤ **Note:** The HELP command can give helpful context sensitive information for most commands.

Command	Summary	Syntax	Description
<b>BYE</b>	Disconnect from unit	BYE	Disconnect a processor session.
<b>EXIT</b>	Exit command processor	EXIT	Ends the console session.
<b>HELP</b>	Show help menu	HELP [ <i>command</i> ]	Displays a list of commands or context sensitive help for a specific command.
<b>PING</b>	Ping IP address	PING <i>target_address</i>	Performs a standard network ping function on the specified IP address.
<b>RESTART</b>	Restart unit	RESTART	Reset the system, same as pressing the physical reset button.
<b>SENSORS or !</b>	Display status of internal or external sensors	SENSORS or !	Display the status of internal or external sensors
<b>STATUS or ?</b>	Display status screen	STATUS or ?	Display the status screen

### Setup Commands

Command	Summary	Syntax	Description
<b>BYPASS</b>	Access serial ports	BYPASS [ <i>port_number</i> ]	Provide pass-through terminal access between the user and the input port.
<b>SK</b>	Set/get key	SK [KEY[= <i>value</i> ]]	Set or get a single key See Setting Keys for more information.
<b>SK GET</b>	Read keys	SK GET [X A [CUSTOM] [ <i>filter</i> ]]	SK GET initiates a download of Setup menu options. See Setting Keys for more information.
<b>SK HERE</b>	Manage individual keys	SK HERE	SK HERE allows you to set or get individual keys interactively. See Setting Keys for more information.
<b>SK LOG</b>	Show SK error log	SK LOG	SK LOG outputs a list of any errors generated during an SK set. See Setting Keys for more information.
<b>SK SET</b>	Set keys	SK SET [X A]	SK SET puts the unit in bulk settings key upload mode. See Setting Keys for more information.
<b>SETUP</b>	Enter setup menu	SETUP	Opens the setup menu.

## System Commands

Command	Summary	Syntax	Description
<b>COLDSTART</b>	Cold boot unit	COLDSTART	Resets the same settings as the DEFAULT command and then reboots the unit.
<b>DEFAULT</b>	Restore factory defaults	DEFAULT	Resets all settings to factory default values, except does not change the following settings: <ul style="list-style-type: none"> <li>• IP address</li> <li>• Subnet mask</li> <li>• Router address</li> <li>• Serial port baud rate and data format</li> <li>• Data alarm fields</li> <li>• Data alarm settings</li> <li>• Action queue</li> </ul> Does not affect record data
<b>DOMAIL</b>	Test emails	DOMAIL	Sends a test email to all defined email addresses.
<b>DOPAGE</b>	Test pagers	DOPAGE	Sends a test page to all defined pagers.
<b>DOTRAP</b>	Test traps	DOTRAP	Sends a test trap to all defined trap managers.
<b>PUSHNOW</b>	Initiate an immediate FTP push of data	PUSHNOW	Initiates an immediate FTP push of data
<b>PUSHTEST</b>	Test connectivity to the FTP server	PUSHTEST	Tests connectivity to the FTP server
<b>TYPE</b>	Print events file contents	TYPE [EVENTS AUDIT]	Print the contents of the Events or Audit file.
<b>VER</b>	Print unit version	VER	Displays unit hardware and software versions as well as the product and version build.

## Numeric Commands

The T830-0 supports numeric (Ctrl-B) commands as follows:

Numeric (Ctrl-B)	Word	Numeric (Ctrl-B)	Word
00	PRT (partition)	59	TAG
01	RL (release)	59,1	TAG OFF
02	NEXT	59,2	TAG ON
06	RESEND	62	RLMODE
09	BYE	62,1	LINE
20	COUNT	62,2	CBB
21	FREE	62,3	CBB
25	CLEAR	62,4	XMODEM
29	BYPASS	63	CRC
39	ZERO	63,1	CRC OFF
50	DEFAULT	63,2	CRC ON
53	COMPRESS	68	DUPLEX
53,1	COMPRESS ON	68,1	DUPLEX HALF
53,2	COMPRESS OFF	68,2	DUPLEX FULL
54	WAIT		
54,1	WAIT OFF		
54,2	WAIT ON		

## Usage Commands

Usage for certain functions ([SK](#), [SSHHC](#), and [XF](#)) can be displayed by simply entering the function command without any arguments, as shown below:

### **SK**

>**SK**

Usage:

```
sk key[<operator>[value]] |
  get [x|a][ filter|custom|@] |
  set [x|a] |
  here |
  help |
  log |
  shortcut [filter|custom|@]
```

Where key:

segment1.segment2....

where segment:

word | word[index] | word.index

where word:

defined by factory or scripting dictionaries

where index:

number | 'all'

where referenced as:

static: referring to one value

indexed: referring to multiple values depending on index(es)

enumerated: referring to a finite set of values

Where operator:

=: write value

@: read/write access levels

#: read key possible values where enumerated

\$: read key restriction class

?: read key instance count where indexed

+: read eventsensor index instance set

-: reset to default value

Where shortcut:

g: get a

c: get a custom

s: set a

?: get a status

Examples:

sk get: read all keys and be prompted for transfer method

sk get a: read all keys at terminal

sk get x: read all keys via xmodem transfer

sk set: write keys and be prompted for transfer method

sk set a: write keys at terminal, delimit with 'end' on line by itself

sk set x: write keys by transferring a file of them via xmodem to the unit

sk get a custom: read non-default keys at terminal

sk get a net: read all net keys at terminal

sk g: same as 'sk get a'

sk s: same as 'sk set a'

sk c: same as 'sk get a custom'

sk ?: same as 'sk get a status'

sk here: perform key operations in interactive interface

sk help: display this help screen

sk <key>: read a key setting value

sk <key>=<value>: write a key setting value

sk <key>@: read key access levels

sk <key>@<read level,write level>: write key access levels

sk get a @: read all access levels at terminal

sk <indexed-key>^: read the next key instance of an indexed key

sk log: output log of last 'set' operation

sk serial.i-: reset all settings under index branch 'serial' to default

sk net-: reset all settings under non-indexed branch 'net' to default

sk event.sensor[16]-: reset all settings for eventsensor 16 to default

>

**SSHC****>SSHC**

No client key exists. Use "sshc -t rsa" to make an RSA key.

Usage: sshc [options]

Options:

```

-h          Specify Host key
-o          Specify Authorized key
-c          Specify Client key (default)
-k          Specify Known host key
-n          Specify authentication banner
-t key_type Type of key to generate (rsa|dsa)
-b bits    Bits to use (1024|2048) default=1024
-s url     URL to send public client key to
(ftp://user:password@host/directory)
-d         Delete keys/banner (default is key)
-dd        Delete everything
-a         Add item (authorized key, known host key, or banner)
-l         List key(s)/banner
-i         Use FTP active mode
-m hostname Specify hostname

```

Examples:

1. Create the host key as 2048-bit RSA: sshc -h -t rsa -b 2048
2. Delete the host key: sshc -dh
3. List the host key: sshc -lh
4. Create the client key as 1024-bit RSA: sshc -t rsa
5. Create the client key as 1024-bit DSA and transfer as "Asentria <key-type> <serial-number>" to an FTP server:  
sshc -t dsa -s "ftp://user:password@some.ftp.server/some/directory"  
(note quotes around URL)
6. Delete the client key: sshc -d
7. List the client key: sshc -l, or sshc with no arguments
8. Add authorized key(s): sshc -ao
9. Delete all authorized keys: sshc -do
10. List authorized keys: sshc -lo
11. Add authentication banner: sshc -an
12. Delete authentication banner: sshc -dn
13. List authentication banner: sshc -ln
14. Add known host key: sshc -ak
15. Delete known host key for host 'myhost': sshc -dkm myhost
16. List known host keys: sshc -lk

Note: If SFTP push discovers a known host key has changed then you must reestablish its authenticity to the unit manually: first delete its known host key (sshc -dkm <host>) and then invoke PUSHTEST.

&gt;

**XF****>XF**

Usage: XF [X|Y|Z|T|F|S|A] GET|PUT [filename] [host] [user] [directory]

&gt;

# Appendices

## User Rights Table

The following tables contain the rights available to each access level within the user profiles.

### Command Permissions

Command	None	View	Admin1	Admin2	Admin3	Master
			X	X	X	X
BYE	X	X	X	X	X	X
COLDSTART						X
DEFAULT						X
DELETE			X	X	X	X
DIR		X	X	X	X	X
DOMAIL		X	X	X	X	X
DOPAGE		X	X	X	X	X
DOTRAP		X	X	X	X	X
EXIT	X	X	X	X	X	X
FTP		X	X	X	X	X
GET		X	X	X	X	X
HELP	X	X	X	X	X	X
MODEMTALK						X
PING			X	X	X	X
RELOADALL	X	X	X	X	X	X
RESTART			X	X	X	X
RZ			X	X	X	X
SET			X	X	X	X
SETUP			X	X	X	X
SK		X	X	X	X	X
STATUS, ?		X	X	X	X	X
SUPPORT		X	X	X	X	X
TESTTIME		X	X	X	X	X
TYPE		X	X	X	X	X
VER		X	X	X	X	X

### Setup Menu Permissions

Settings	View	Admin1	Admin2	Admin3	Master
Most settings	View	X	X	X	X
Authentication				View	X
Passwords					X
Event log	View	View	View	X	X
Audit log	View	View	View	X	X
PPP dial username		View	View	View	X
PPP dial password					X
Caller ID				View	X

## Control Characters

Some of the following control characters may be used in various functions within the T830-0, including CRC mode for AsentriaAlarms and the Escape Key.

Char	Dec	Hex	Control Key	Control Action
NUL	0	00	^@	Null
SOH	1	01	^A	Start of heading
STX	2	02	^B	Start of text
ETX	3	03	^C	End of text
EOT	4	04	^D	End of transmission
ENQ	5	05	^E	Enquiry
ACK	6	06	^F	Acknowledge
BEL	7	07	^G	Bell
BS	8	08	^H	Backspace
HT	9	09	^I	Horizontal tab
LF	10	0A	^J	Line feed
VT	11	0B	^K	Vertical tab
FF	12	0C	^L	Form feed
CR	13	0D	^M	Carriage return
SO	14	0E	^N	Shift Out
SI	15	0F	^O	Shift In
DLE	16	10	^P	Data link escape
DC1	17	11	^Q	XON
DC2	18	12	^R	Device control 2
DC3	19	13	^S	XOFF
DC4	20	14	^T	Device control 4
NAK	21	15	^U	Negative acknowledge
SYN	22	16	^V	Synchronous idle
ETB	23	17	^W	End transmission block
CAN	24	17	^X	Cancel
EM	25	19	^Y	End of medium
SUB	26	1A	^Z	Substitute
ESC	27	1B	^[	Escape
FS	28	1C	^\	File separator
GS	29	1D	^]	Group Separator
RS	30	1E	^^	Record Separator
US	31	1F	^_	Unit Separator

## 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 these 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.

<b>Modem</b>	<b>FCC ID</b>	<b>REN</b>
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 identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme à certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. Le Ministère n'assure toutefois pas que le matériel fonctionnera à 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 être installé en suivant une méthode acceptée de raccordement. Dans certains cas, les fils intérieurs de l'entreprise utilisés pour un service individuel à ligne unique peuvent être 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'empêche pas la dégradation du service dans certaines situations. Actuellement, les entreprises de télécommunication ne permettent pas que l'on raccorde leur matériel à des jacks d'abonné, sauf dans les cas précis prévus par les tarifs particuliers de ces entreprises.

Les réparations de matériel homologué doivent être effectuées par un centre d'entretien Canadien autorisé désigné par le fournisseur. La compagnie de télécommunications peut demander à l'utilisateur de débrancher un appareil à la suite de réparations ou de modifications effectuées par l'utilisateur ou à cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise à la terre de la source d'énergie électrique, des lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

**Avertissement.** - L'utilisateur ne doit pas tenter de faire ces raccordements lui-même; il doit avoir recours à un service d'inspection des installations électriques, ou à un électricien, selon le cas.

L'indice de charge (IC) assigné à chaque dispositif terminal indique, pour éviter toute surcharge, le pourcentage de la charge totale qui peut être raccordée à un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit

bouclé peut être constituée de n'importe quelle combinaison 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 appareil 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 T830-0 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 T830-0 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 T830-0. Asentria Corporation's liability shall be limited to the purchase price of the T830-0. No warranty of fitness for purpose, or of fitness of the T830-0 for any particular application is provided. It is the responsibility of the user to determine fitness of the T830-0 for any particular application or purpose.

This warranty gives you specific legal rights. These rights may vary from state to state, as some states do not allow limitations on liability.

You may request information on how to obtain service under this warranty by contacting Asentria Technical Support at the address and phone number below:

### **Asentria Technical Support**

1200 North 96th St.

Seattle, WA 98103

206.344.8800

[support@asentria.com](mailto:support@asentria.com)

[www.asentria.com](http://www.asentria.com)