



ContactAgent™

Model PBT-CA-1-R

Installation and Operation

Input	State	Input	State
S 1: Input 1	high	S 17: RIM 2, Input 3	high text
S 2: Input 2	low	S 18: RIM 2, Input 4	high text
S 3: Input 3	high	S 19: RIM 2, Input 5	high text
S 4: Input 4	high	S 20: RIM 2, Input 6	high text
S 5: Input 5	high	S 21: RIM 3, Input 1	high text
S 6: Input 6	high	S 22: RIM 3, Input 2	1.85 VDC
S 7: Input 7	high	S 23: RIM 3, Input 3	1.88 VDC
S 8: Input 8	high	S 24: RIM 3, Input 4	high text
S 9: RIM 1, Input 1	high text	S 25: RIM 3, Input 5	high text
S 10: RIM 1, Input 2	high text	S 26: RIM 3, Input 6	high text
S 11: RIM 1, Input 3	high text	S 27: RIM 4, Input 1	high text
S 12: RIM 1, Input 4	high text	S 28: RIM 4, Input 2	1.88 VDC
S 13: RIM 1, Input 5	high text	S 29: RIM 4, Input 3	1.88 VDC
S 14: RIM 1, Input 6	high text	S 30: RIM 4, Input 4	1.88 VDC
S 15: RIM 2, Input 1	high text	S 31: RIM 4, Input 5	high text
S 16: RIM 2, Input 2	low text	S 32: RIM 4, Input 6	high text

Agent Firmware Version: XPort 03.4, PIC 1.3
Agent MAC Address: 0-20-4a-91-8d-ca

9: 6: 5 10-3-2008

WebAgent-CA-1-R Ver 2.5
Copyright Phoenix Broadband Technologies, LLC 2008
All Rights Reserved

Applet cAgent started





Table of Contents

▪ Revision History _____	3
▪ Safety Notes _____	3
▪ Contact Information _____	3
▪ System Overview _____	4
▪ Unpacking the ContactAgent™ _____	5
▪ Mounting the ContactAgent™ _____	5
▪ Connecting the ContactAgent™ _____	6
Electrical Considerations _____	7
Inputs _____	7
Outputs _____	7
Connecting to the Network _____	7
Connecting the Power _____	7
LED Operation _____	7
▪ IP Address Options _____	8
▪ Configuring the ContactAgent™ _____	9
Running the Telnet Setup _____	10
Setting the IP Address (0) _____	11
Web Passwords (1) _____	12
SNMP Agent Configuration (3) _____	13
HMS Defaults (4) _____	14
Email Setup (5) _____	14
Time Server Configuration (6) _____	15
Restore Factory Defaults (7) _____	16
Exit (8) _____	16
Save and Exit (9) _____	16
▪ Using the Web Server _____	17
Computer Requirements _____	17
Accessing the Web Server _____	17
Ports _____	17
Main Web Page _____	18
Input and Output Screen _____	18
Password Screen _____	19
Input Setup _____	20
Output Setup _____	20
Digital Alarms _____	21
▪ SNMP _____	22
MIBs _____	22
Community Strings _____	22
Traps _____	22
MIB Browsers _____	23
▪ Firmware Updates _____	24
▪ Specifications _____	25



▪ **Revision History**

Release	Date	Revision Description
Rev 1	10/03/2008	Draft for review. Firmware version 3.41
Rev 2	10/15/2008	Walt's edits.
Rev 3	10/16/2008	Joe's edits. Removed Draft. Initial release.

▪ **Safety Notes**

- Except as explained in this manual, there are no user-serviceable parts inside the PBT System components. Opening the equipment could expose you to dangerous voltages and void the product warranty. All product servicing should be referred to factory-authorized personnel.
- Do not exceed the voltage specifications of the product.
- Make sure the equipment is grounded properly.
- The equipment should be protected from liquids, moisture, corrosive vapors.

Important Symbols:

	CAUTION! The use of CAUTION indicates safety information intended to prevent damage and/or injury
--	---

	NOTE: A NOTE to provide additional information to help complete a specific task or procedure
--	--

▪ **Contact Information**

If you have any questions about the installation or use of the equipment described in this manual, contact Phoenix Broadband Technologies at (215) 997-6007 or email marketing@phoenixbroadband.com.

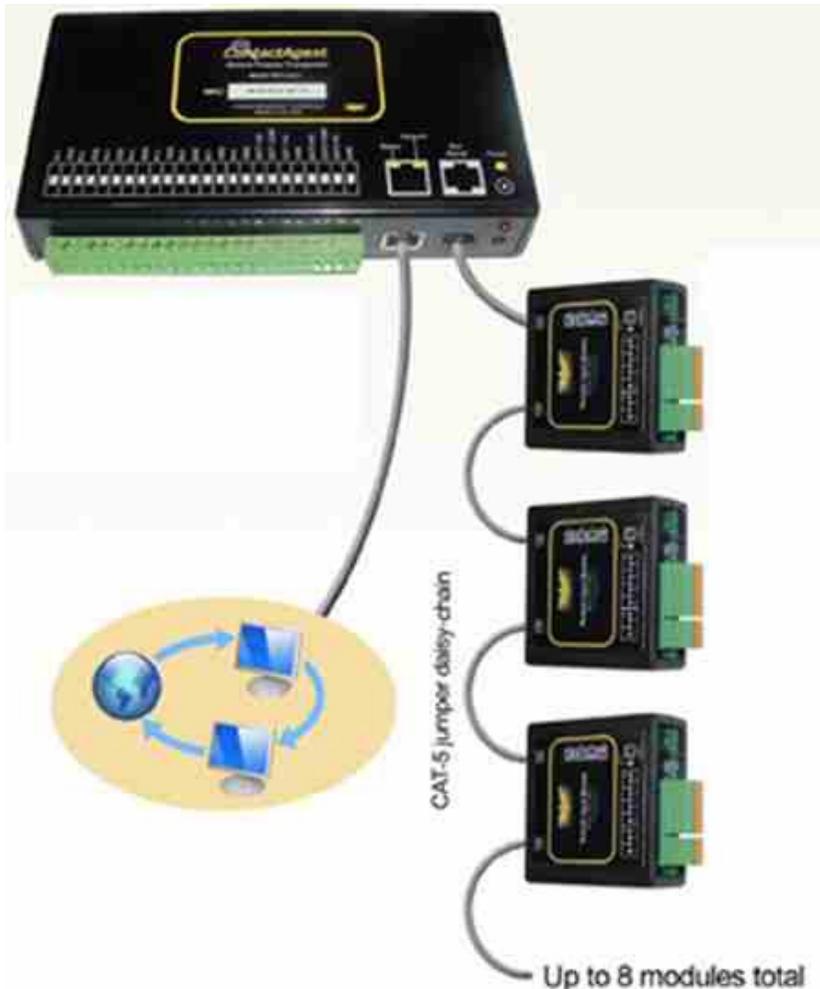
Phoenix Broadband Technologies, LLC.
589 Bethlehem Pike
Montgomeryville, PA 18936



▪ **System Overview**

The Phoenix Broadband Technologies (PBT) **ContactAgent™** General Purpose Transponder provides monitoring for 8 digital Inputs and controls 2 relay outputs. The **ContactAgent™** inputs and outputs can be completely configured and controlled using only a Web Browser. Inputs can be configured to alarm on either a high or low state. The **ContactAgent™** includes a Web Server, SNMP client, and Email client.

The number of inputs can be expanded by adding Remote Input Modules (RIM) and the number of outputs can be expanded by adding Remote Output Modules (ROM).



The RIM has 6 inputs that can be configured to monitor analog or digital signals. Up to 4 RIMs can be daisy chained together, increasing the **ContactAgent™** inputs to a total of 32.

The ROM has 4 latched relay outputs. Up to 4 ROMs can be daisy chained together, increasing the **ContactAgent™** outputs to a total of 18.

RIMs and ROMs also provide AC Line Voltage, Temperature and optional Humidity measurements.

RIMs and ROMs can be combined in a daisy chain with other compatible PBT devices.

The RIM and ROM are completely configurable using only a Web Browser.



▪ **Unpacking the ContactAgent™**

Each **ContactAgent™** unit is individually packed in a corrugated cardboard container. The package also includes the power pack (Model PBT-WT-1) and a plastic bag containing 2 mounting screws.

A label on the outside of the individual shipping carton indicates the MAC address of the **ContactAgent™** unit contained inside. This MAC address matches the MAC address printed on the top of the **ContactAgent™**. It is suggested that MAC addresses be recorded before the unit is sent out for installation so that the provisioning process can proceed in parallel with the hardware installation process.



▪ **Mounting the ContactAgent™**

The **ContactAgent™** is shipped configured for table top use. An optional 19" rack shelf (Model PBT-RK-1) that mounts the **ContactAgent™** and the RIM/ROM is available.



To mount the **ContactAgent™** to the rack shelf remove the rubber feet and mount the **ContactAgent™** to the shelf from the bottom using the self tapping screws provided.



Use only the screws provided. Screws longer than 0.375 inches will damage the circuit board.



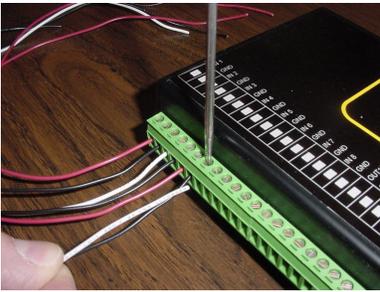
▪ **Connecting the ContactAgent™**

The **ContactAgent™** can monitor dry contact closure or low voltage digital signals. The voltage presented to the inputs must be ground referenced and no greater than +10 Volts DC.



Caution: Connecting the **ContactAgent™** inputs to voltages outside of this range may damage the **ContactAgent™** and void the warranty.

The **ContactAgent™** monitoring and control interface consists of 24 interface points arranged as two plug-removable 12-point interface blocks. See the picture to the right.



Each interface point consists of a wire clamping receptacle and a clamp screw. The interface is arranged as 8 contact-closure inputs and 2 sets of Form-C (SPDT) relay outputs. 10 common ground points are interspersed among the input and output interface points. See the picture to the left.

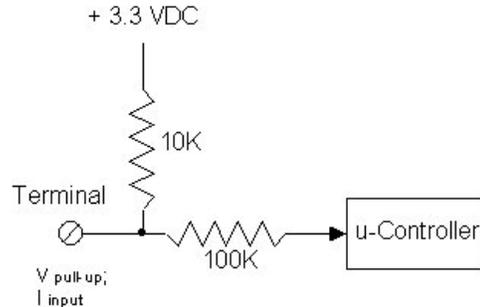
For dry contact closures connect one side of the contact to a **ContactAgent™** input and connect the other side to the **ContactAgent™** ground.



Electrical Considerations

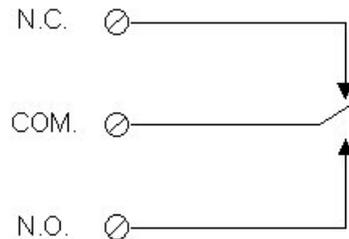
Inputs

The input interface points are designed to be connected to a switch, relay, or solid-state device that can provide a switched DC connection to the unit's common ground lines. The equivalent circuit of the inputs is shown to the right.



Outputs

The **ContactAgent™** has two sets of Form-C (SPDT) relay contact outputs that can be used to control devices that require a floating AC or DC switch path. The equivalent circuit of the outputs is shown to the right.



Contact Phoenix Broadband Technologies if you are unsure of how to connect your device to the **ContactAgent™**.

Connecting to the Network

Connect the **ContactAgent™** Ethernet connection to an Ethernet hub, switch, or router using a standard Ethernet cable. Make this connection before applying power to the **ContactAgent™**.

Connecting the Power

The **ContactAgent™** is powered from 5 volts DC provided by a plug-in switching power supply (Model PBT-WT-1). Connect the cable from the power supply to the PWR connector on the **ContactAgent™**. Make sure that the black plug is firmly seated in the power socket. Plug the power supply into an AC power outlet.

LED Operation

There are two LEDs on the Ethernet connector. The left LED is the Link LED, the right LED is the Activity LED.

Link LED Color	Meaning
Off	No Link
Amber	10 Mbps
Green	100 Mbps

Activity LED Color	Meaning
Off	No Activity
Amber	Half Duplex
Green	Full Duplex

There is also a green LED to the right of the Ethernet connector. This LED will light when the **ContactAgent™** is powered and is ready to begin operation. The LED will flash off momentarily when a good response is received from a Remote Module (RIM or ROM).



▪ **IP Address Options**

In order to communicate on Ethernet each device requires an IP address. The **ContactAgent™** is shipped from the factory configured to obtain an IP address automatically from a DHCP server. The MAC address is printed on the **ContactAgent™** label.

The IP address may be a public or private. Devices with public IP address are generally accessible over the internet. Devices with private IP addresses are only accessible on the local network. The **ContactAgent™** may be assigned a public or private IP address. Public IP addresses allow access over the internet but are less secure than private IP addresses.

There are several ways to handle the IP address.

- You can pre-configure your DHCP server to assign a reserved IP address to the **ContactAgent™** MAC Address.
- You can let your DHCP server assign an address and then interrogate the DHCP server to determine what address was used. This technique works well in the lab environment where the DHCP server may be in a router. For field installations you obviously do not want the IP address to keep changing.
- You can program a static IP address in the **ContactAgent™** using a temporary connection to a router with a built-in DHCP server and the **ContactAgent™** Telnet configuration port.
- You can program a static IP address in the **ContactAgent™** directly using a programming adapter and a PC as described in the next section.

PBT recommends the use of either a static or reserved IP address.

Before installing the **ContactAgent™** discuss this with your IT department and determine what kind of IP address you should use and obtain a static or reserved IP address if either of these options are selected. If the DHCP option is selected make arrangements with the IT department to tell you what IP address is assigned to your device. You can also see what IP address was assigned to you device using the Programming Adapter described below.



▪ **Configuring the ContactAgent™**

The **ContactAgent™** is normally configured over the network through a telnet connection. Support of telnet is a standard part of Windows so virtually any PC can configure the **ContactAgent™**. The configuration program is described in the following section of this document.

The **ContactAgent™** is also equipped with a local interface that allows a PC to be connected to the **ContactAgent™** through a Programming Adapter (PBT Model PBT-PRG-USB) to access the configuration program. A PC with a USB Port, a serial communications program such as HyperTerminal, and a Programming Adapter are required.

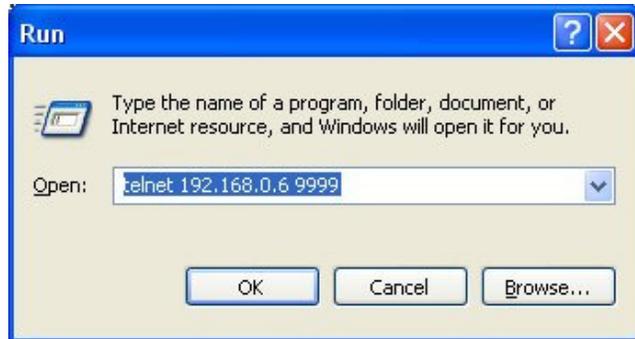
HyperTerminal which has been part of Microsoft Windows since the beginning, is no longer included with Microsoft Vista. There are many other terminal programs available on the internet that will work. We recommend Teraterm which can be downloaded for free at <http://www.ayera.com/teraterm/>. Be sure to comply with all licensing requirements.

Following the directions provided with the PBT-PRG-USB, install the Programming Adapter on the PC, and verify that it is working properly. Connect the Programming Adapter to the Aux Serial port on the **ContactAgent™** and hold down the “x” key (lower case) while connecting the power to the **ContactAgent™**. Follow the Telnet instructions below.



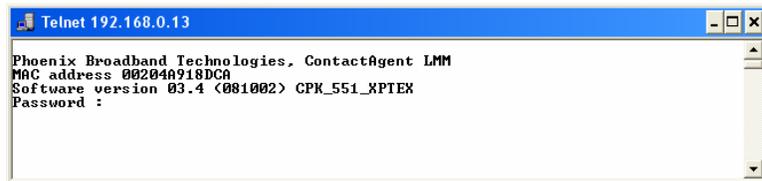
Running the Telnet Setup

To open a telnet connection to the **ContactAgent™** select “Run” from the Windows “Start” menu. Enter “telnet” followed by a space, then, the IP address on the **ContactAgent™** followed by a space, and then the port number “9999” followed by “Enter”.

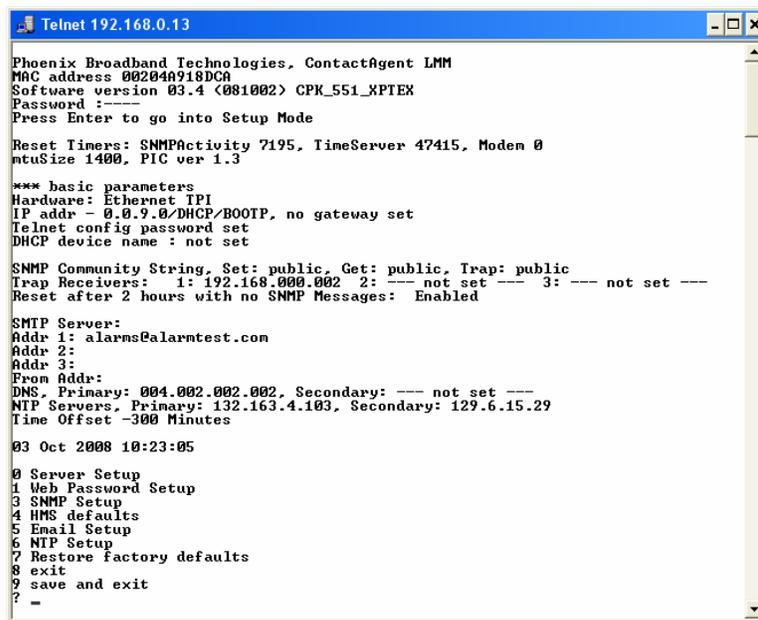


If the **ContactAgent™** is on-line and the telnet password is enabled, the following screen will be displayed. If the telnet password is not enabled skip to the next step.

Enter the password. You only have a few seconds before the session times out. If the password is accepted the following screen will be displayed, if the password is not accepted the telnet session will be terminated.



Press the “Enter” key to begin the setup process. If “Enter” is not typed in a few seconds the telnet session will time out.



The Setup Menu will then be displayed as shown to the left.

The top two thirds of the screen displays the present configuration. The menu at the bottom of the screen displays the setup menu.

Closing the telnet window will terminate the telnet session and reset the **ContactAgent™**. To avoid resetting the **ContactAgent™** exit by pressing “8” followed by “Enter”.



Setting the IP Address (0)

Various options can be controlled by setting the IP address. For static IP address operation the IP address should be set to the address assigned by the IT department or other authority. Other IP address options are as follows.

If the IP address is set to 0.0.0.0 DHCP is enabled. (Factory Default)

If the IP address is set to 0.0.1.0 DHCP is enabled and AutoIP is disabled.

If the IP address is set to 0.0.9.0 DHCP is enabled, DHCP option 81 is disabled, and AutoIP is disabled.

To change the IP Address select option 0 from the setup menu by typing a 0 followed by “Enter”. The following screen will appear.

```
Telnet 192.168.0.13
0 Server Setup
1 Web Password Setup
3 SNMP Setup
4 HMS defaults
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> _
```

The current value of the first octet of the IP address will be shown in parenthesis. This indicates that the first octet of the IP address is 0. To change the octet, type the new number followed by “Enter”. To move on without making any changes, just type “Enter”.

```
Telnet 192.168.0.13
4 HMS defaults
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> 192.<000>
```

In this example the first octet of the IP address was changed to 192.

```
Telnet 192.168.0.13
4 HMS defaults
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> 192.<000> 168.<009> 0.<000> _
```

Continue entering each octet of the IP address until all 4 octets have been entered. To skip any entry without making any changes type “Enter” without typing any numbers.

Next the **ContactAgent™** will ask if you would like to set the Gateway IP Address. The Gateway address is required for the **ContactAgent™** to initiate communications with other devices on the

```
Telnet 192.168.0.13
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> 192.<000> 168.<009> 0.<000>
Set Gateway IP Address <N> ? Y
Gateway IP Address : <000> _
```

network; such as the time or email servers. This address is obtained automatically when running with DHCP, however when a static IP address is assigned to the **ContactAgent™** the Gateway Address must be set

manually. The Gateway Address is normally set to the IP Address of the first router encountered by outbound network traffic. To change the address, type a “Y” and enter the IP address as described above. To skip the address, type an “N”.



The **ContactAgent™** will now ask for the Network Mask. To change the mask, enter the number

```
Telnet 192.168.0.13
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> 192.<000> 168.<009> 0.<000>
Set Gateway IP Address <N> ? Y
Gateway IP Address : <000> 192.<000> 168.<000> 0.<000> 1
Netmask: Number of Bits for Host Part <0=default> <0>
```

of bits required for the local host. Example; For 255.255.255.0 enter 8, for 255.255.252. 0 enter 10. Verify the Net Mask was set correctly by observing the displayed value when the

menu returns to the screen. The table below shows the value to be entered for common Net Masks.

Value	Net Mask
2	255.255.255.252
3	255.255.255.248
4	255.255.255.240
5	255.255.255.224
6	255.255.255.192
7	255.255.255.128
8	255.255.255.0
9	255.255.254.0
10	255.255.252.0

Next the **ContactAgent™** will ask if a telnet password is desired. A four character password can be selected to secure telnet access to the Agent. Use caution when selecting a password. If you forget the password or enter it incorrectly the **ContactAgent™** must be returned to the factory for repair. To set the password enter a “Y” and then the password following the prompt. To remove a password enter a “Y” and then an enter at the prompt.

```
Telnet 192.168.0.13
7 Restore factory defaults
8 exit
9 save and exit
? 0
IP Address : <000> .<000> .<000> .<000>
Set Gateway IP Address <N> ?
Netmask: Number of Bits for Host Part <0=default> <10>
Change telnet config password <N> ?
Change DHCP device name <not set> ? <N> ?
```

Finally the **ContactAgent™** will ask if you would like to change the DHCP device

name. We recommend that you do not change this setting. Type enter to return to the menu.

To save your changes type “9” from the menu. The changes will be saved in nonvolatile memory, the telnet session will be terminated, and the **ContactAgent™** will reset.

Web Passwords (1)

To change the Passwords used for Web Page access type “1” followed by “Enter”. The user Password will be displayed. To change the user password type the new password followed by “Enter”. To keep the present password type “Enter”. Passwords can be 20 characters long and are case sensitive.

```
Telnet 192.168.0.13
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 1
Web Password 1: <user>: _
```

Change the administrator password in a similar fashion.

```
Telnet 192.168.0.13
7 Restore factory defaults
8 exit
9 save and exit
? 1
Web Password 1: <user>:
Web Password 2: <admin>: new admin
```

The password changes will immediately be saved to

nonvolatile memory and become effective. Type “8” followed by “Enter” to close the telnet session without resetting the **ContactAgent™**.



SNMP Agent Configuration (3)

The SNMP Community Strings and Trap destinations are configured from the SNMP Configuration.

```
Telnet 192.168.0.13
4 HMS defaults
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 3
Set Community <public>: NewString_
```

The default community strings are set to “public”. To change the community string type “3” followed by “Enter”. The present read (Set) community string will be displayed in parenthesis as shown. To change the community string, type the new string followed by “Enter”. To move to the next item without changing the community string just type “Enter”. The write (Set)

```
Telnet 192.168.0.13
? 3
Set Community <public>: NewSetString
Get Community <public>: NewGetString
Trap Community <public>: NewTrapString
Trap Receivers:
1: <192> _
```

community string is next and is handled the same way, followed by the Trap community string.

Community strings are case sensitive.

Up to 3 Trap destinations can be configured. The IP addresses of the Trap destinations are set

```
Telnet 192.168.0.13
Get Community <NewGetString>:
Trap Community <NewTrapString>:
Trap Receivers:
1: <192> .<168> .<000> .<002>
2: <000> 192.<000> 168.<000> 0.<000> 12
3: <000> .<000> .<000> .<000>
```

similar to the IP address described above. To disable sending Traps to any of the three IP address enter zeros for the IP address.

The **ContactAgent**[™] includes a feature that will reset the device if a SNMP message is not

```
Telnet 192.168.0.13
Get Community <NewGetString>:
Trap Community <NewTrapString>:
Trap Receivers:
1: <192> .<168> .<000> .<002>
2: <192> .<168> .<000> .<012>
3: <000> .<000> .<000> .<000>
Enable 'Reset after 2 hours with no SNMP Messages'? <Y/N>_
```

received for approximately 2 hours. This safety feature is primarily used when the device is located in a remote unmanned location. If the SNMP firmware hangs this may recover the device

without a visit to the remote location. The default setting is disabled. To enable the reset Type a “Y”, to disable the feature type a “N” or “Enter”.

The menu will be redisplayed at the end of the SNMP Configuration. Select “9” to save the changes and close the telnet session.



HMS Defaults (4)

To restore the factory default settings for all SNMP objects, type a “4” followed by “Enter”. The SNMP, Email, NTP, Gateway, Net Mask, and IP Address will not be changed. The telnet session will be closed and the **ContactAgent™** will be reset.

Email Setup (5)

The Email system will mail alarm messages to up to 3 email addresses.

To setup the Email system select 5 from the setup main menu. Enter the outgoing Email server name. If there is no server name the email system is disabled. If a server name was previously entered it will be shown. To change the server name just type the new name followed by “Enter”. To keep the server name shown type “Enter”. To remove the server name type any character, then “Backspace” followed by “Enter”.

```
Telnet 192.168.0.13
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 5
SMTP Server Name (<): _
```

To change the server name just type the new name followed by “Enter”. To keep the server name shown type “Enter”. To remove the server name type any character, then “Backspace” followed by “Enter”.

```
Telnet 192.168.0.13
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 5
SMTP Server Name (<): smtp.server.net
Addr 1 (<alarms@alarmtest.com>):
```

Up to 3 Email address may now be entered. The address are changed the same as the server name.

Next enter the From Address. This is the address that will show up in the Email when it is received.

```
Telnet 192.168.0.13
? 5
SMTP Server Name (<): smtp.server.net
Addr 1 (<alarms@alarmtest.com>):
Addr 2 (<):
Addr 3 (<):
From Addr (<): mike@pbt.com_
```

- The From Address should generally be set to an address that is registered on the SMTP server. Many servers use this to authenticate the outgoing Email.

Finally set the Domain Name Server (DNS) IP address. The DNS allows the Email application to obtain the IP address of the specified server so it can send the mail. There are fields for a primary and secondary DNS. The IP Address are set as described in the IP Address section of this document. The default is a commonly used DNS (4.2.2.2). Change this to your local DNS if you prefer. As long as the **ContactAgent™** can see the internet the default DNS will work. If the DNS IP addresses are set to zeros, the Email will be disabled.

```
Telnet 192.168.0.13
SMTP Server Name (<): smtp.server.net
Addr 1 (<alarms@alarmtest.com>):
Addr 2 (<):
Addr 3 (<):
From Addr (<): mike@pbt.com
Primary DNS: <004> _
```

To save your changes type “9” from the menu. The changes will be saved in nonvolatile memory, the telnet session will be terminated, and the **ContactAgent™** will reset.



Time Server Configuration (6)

The **ContactAgent**[™] can set its internal clock from any internet time server that supports Network Time Protocol (NTP). There are many such servers around the world. Many of these servers are operated by government standards organizations. Most private networks also have time servers.

The **ContactAgent**[™] is shipped with the NTP configuration set to get the time from two different US National Institute of Standards time servers. The IP addresses of these servers can be changed in the NTP Configuration. If the time server addresses are not configured or the **ContactAgent**[™] is unable to contact either time server the **ContactAgent**[™] will initialize the time to 00:00:00 1/1/2008. If communications is not established with a time server the internal clock will run from this point.

The time provided by most time servers is Greenwich Mean Time (GMT). The **ContactAgent**[™] will convert this to Local Time using a time offset that can be entered in the NTP Configuration.

```
Telnet 192.168.0.13
5 Email Setup
6 NTP Setup
7 Restore factory defaults
8 exit
9 save and exit
? 6
Primary NTP Server: <132> .<163> .<004> .<103>
Secondary NTP Server: <129> .<006> .<015> .<029>
Local Time offset from GMT (Minutes): <65236> ? _
```

To configure the NTP select option 6 from the Configuration Main Menu. Enter the IP addresses as described in the IP Address section of this manual. There

are two Time Server addresses. The **ContactAgent**[™] will use the primary server unless it fails to respond and then it will switch to the secondary. It will not switch back unless the secondary server fails to respond or the **ContactAgent**[™] is reset. To change a default Time Server IP Address to undefined enter zeros for the IP address.

The **ContactAgent**[™] will reset itself if there is no communications with either time server for approximately 2 hours. To disable the reset function enter zero for all 4 octets of the primary time server IP address. The **ContactAgent**[™] will use the secondary Time Server to set the time if the second IP Address valid.

The time read from the time servers is GMT. There is an option in the NTP Setup to enter a time offset to correct the time to read local time. If the time offset is positive, east of the UK, simply enter the offset in minutes. If the time offset is negative, west of the UK, the offset must be entered in 2's complement form. To compute the value subtract the time offset in minutes from 65536 and enter the result. For example the offset to Eastern Daylight time is 4 hours. 65536 - 240 = 65296 Enter 65296 as the time offset for Eastern Daylight time.

To save your changes type "9" from the menu. The changes will be saved in nonvolatile memory, the telnet session will be terminated, and the **ContactAgent**[™] will reset.



Restore Factory Defaults (7)

To restore the factory default settings type a 7. All SNMP, Email, NTP, and HMS values will be set to the factory defaults. The IP Address will not be changed, however the Gateway and Net Mask settings will be changed.



Be careful. Changing the Gateway and Net Mask settings could prevent communications with the **ContactAgent™**, requiring a site visit.

Exit (8)

Type a "8" followed by an "Enter", to exit the setup program, close the telnet window without saving the changes to nonvolatile memory, and without resetting the **ContactAgent™**. Some changes will take affect (SNMP) others will not (Email).

Save and Exit (9)

Type a "9" followed by an "Enter", to save all changes to nonvolatile memory, close the telnet window, exit the setup program, and reset the **ContactAgent™** so all changes take affect.



▪ **Using the Web Server**

Computer Requirements

The **ContactAgent™** Web Server uses a Java applet to communicate between the Web Browser on your PC and the **ContactAgent™**. For this to operate, the Java Runtime Environment (JRE) must be installed on your PC. This is a common function of many Web Sites so it is likely that the Java Runtime Environment is already loaded on your PC.

If you need to load the Java Runtime Environment go to the Sun Java Web Site at:

http://java.com/en/download/windows_automatic.jsp

and follow the directions to download and install the latest version of the JRE. This is a free download.

The *ContactAgent™* web server has been tested to work with Sun Java Runtime Environment Version 1.4.2. Older versions of the Java Runtime Environment may not function properly with the *ContactAgent™* Web Server. Most newer java versions appear to work properly.

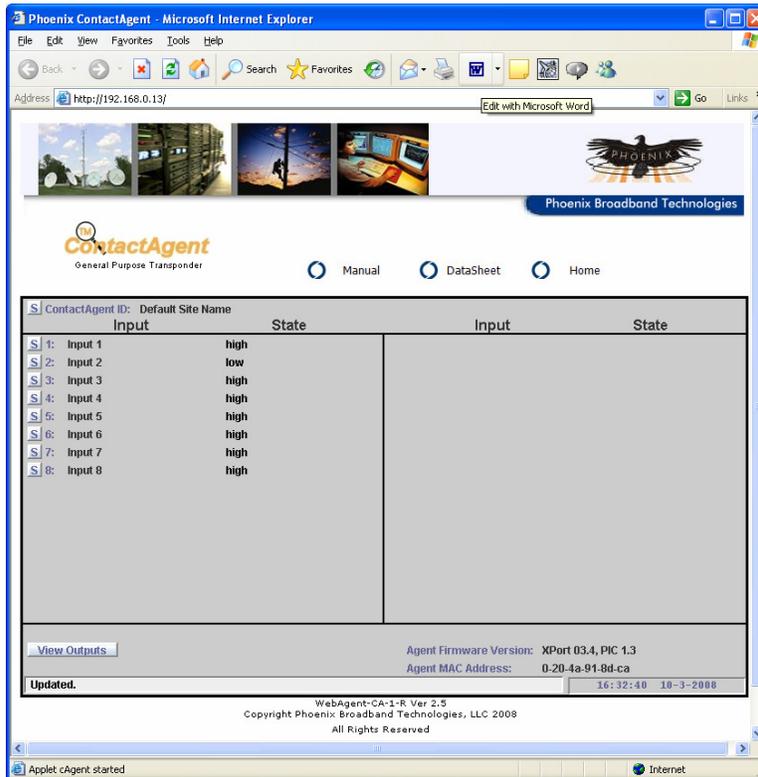
To check which version you are using on your PC open a Microsoft Internet Explorer and select Tools -> Internet Options -> Advanced. Scroll down to the line that displays Java (Sun). The version number of the Java Runtime environment installed on your PC will be shown. If this line is not present the Sun Java Runtime Environment is not installed on your PC.

Accessing the Web Server

To access the **ContactAgent™** Web page type: "http://192.168.0.5" from your web browser. This IP Address is an example, substitute your **ContactAgent™**'s IP address in place of "192.168.0.5".

Ports

The Web server uses Ports 80 and 30704. Port 80 is the normal HTTP port. Port 30704 is used by the Java applet to get data from the **ContactAgent™** for the real time screen updates. If the Web page draws but the applet is unable to connect to the **ContactAgent™** chances are good that port 30704 is being blocked by a firewall or router. This could be on your PC or somewhere in the network.



Main Web Page

The **ContactAgent™** is completely configurable through a series of Web pages. The Main Web page is shown to the left. The state of the 8 inputs with their user defined names and state names are displayed. The inputs are color coded with their alarm status if the alarms are enabled. If RIMs are connected to the **ContactAgent™** the RIM inputs are also shown on this page. Refer to the RIM Manual for information on using the RIMs.

The three buttons at the top of the page are links to Internet sites containing the **ContactAgent™** Manual and Data Sheet. There is also a

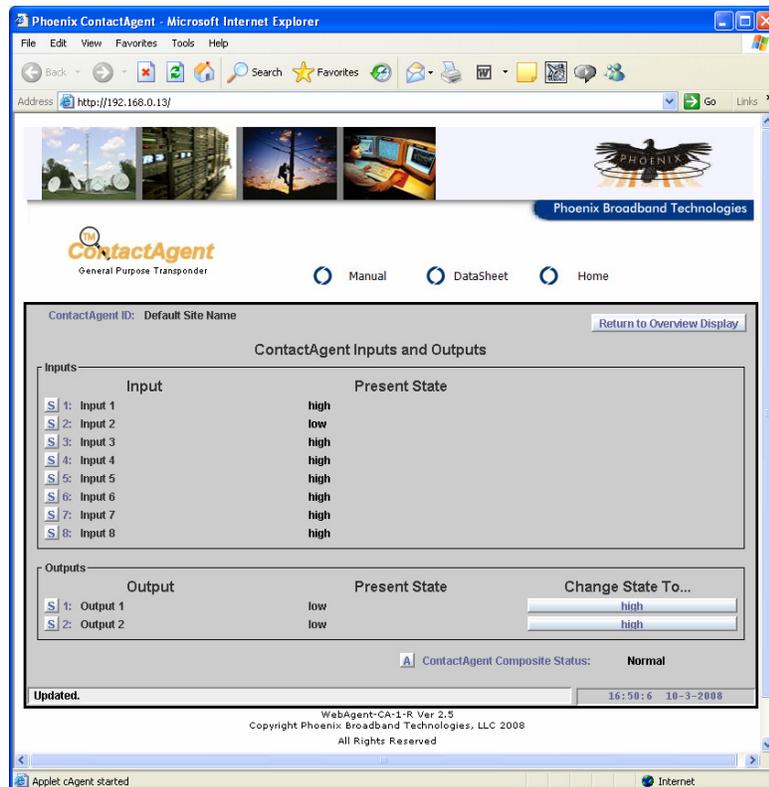
link to the PBT Web Site.

Input and Output Screen

This screen displays the present state of the Input and Outputs. When an input alarm is enabled the value for the input will be color coded with its alarm status, Black for Normal, Yellow for Minor Alarm, and Red for Major Alarm.

To setup an input or output click on any of the **S** (Setup) buttons. Either the **Password**, **Input Setup**, or **Output Setup** screen shown below will appear.

To control an Output push either of the **Change State To...** buttons. If the password has not been entered previously the



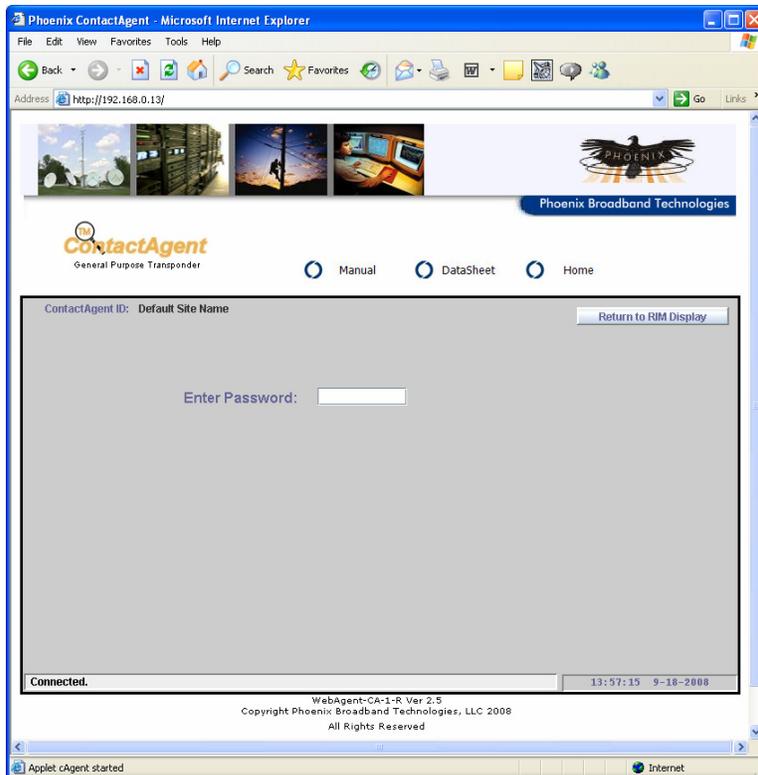


Password Screen will appear, otherwise the output will be switched.

The **Composite Status** is a roll up of the analog and digital input alarms. If any input alarm, of any severity is present the **Composite Status** will indicate Alarm. If there are no input alarms the Composite Status will indicate Normal. To setup alarms for the **Composite Status** press the **A** button adjacent to the **Composite Status** and refer to the Digital Alarms section of this document.

Password Screen

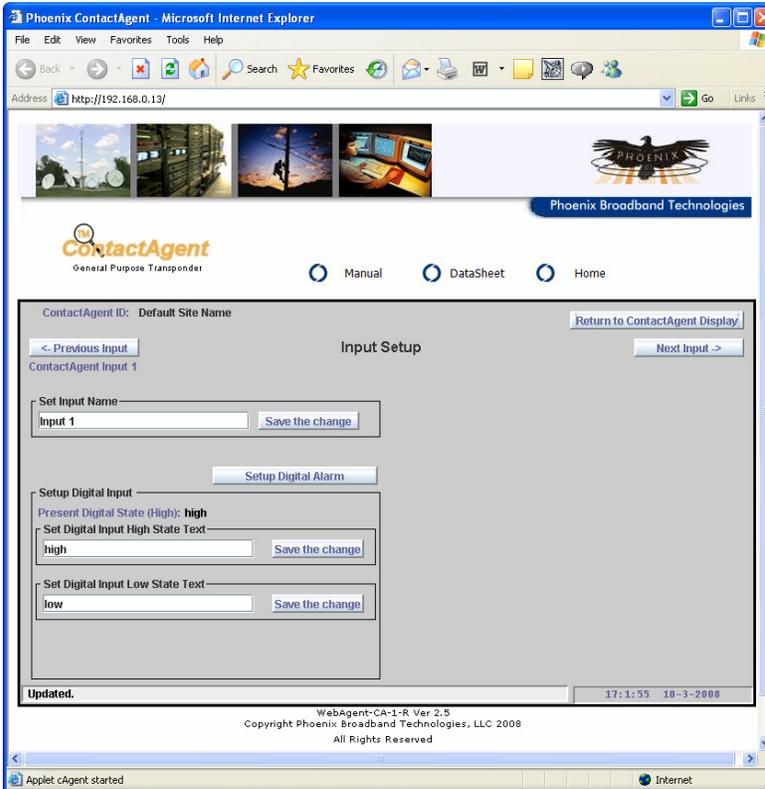
Type the password followed by enter. The password is case sensitive. There are two passwords, one for User access and one for Administrative access. The default passwords are “user” and “admin”. The Web passwords can be changed from the telnet setup interface.



The password will time out after 10 minutes of inactivity. If the password is required following the timeout the Password screen will reappear.

Once the password is entered the Input Setup Screen shown below will appear.

If your forget the password there is a back door password that can be obtained by contacting PBT.

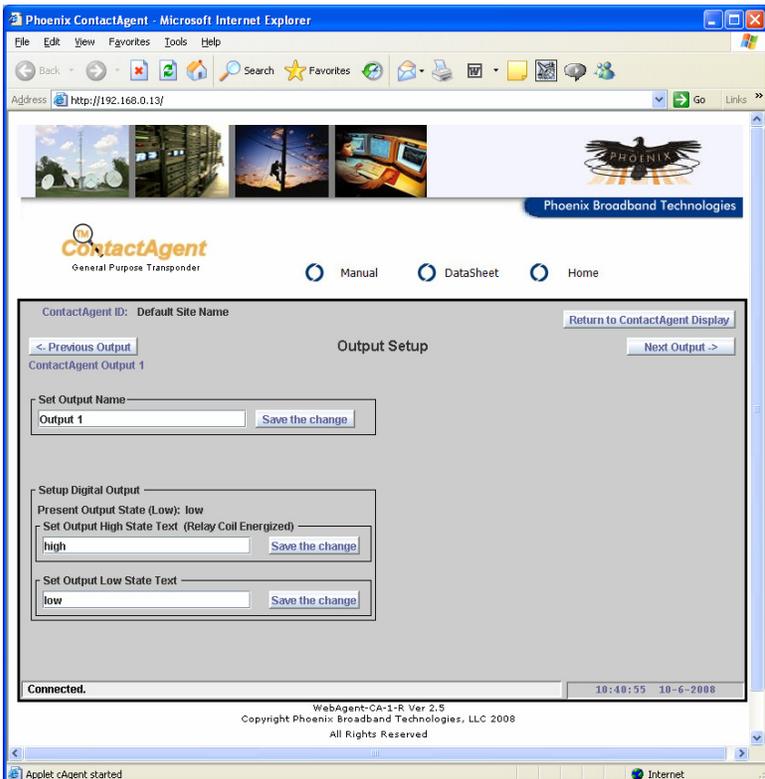


Input Setup

This screen is used to set the **Input Name** and Input State Names as well as control the alarming. To change the **Input Name**, type the desired name in the text box and press the Save the Change button.

A digital input can be in one of two states. We refer to these states as High or Low. When the DC voltage at the input is above approximately 1.5 VDC, that input is in the High state. When the input is below the threshold the input is in the Low state. To set the text displayed when the input is in the High state, type the desired string in the **Set Digital Input High State Text** box and press the **Save the Change** button. To set the text displayed when the input is in the Low state, type the desired string in the **Set Digital Input Low State Text** box and press the **Save the Change** button.

To setup the Digital Alarms press the **Setup Digital Alarms** button and refer to Digital Alarms section further on in this document.



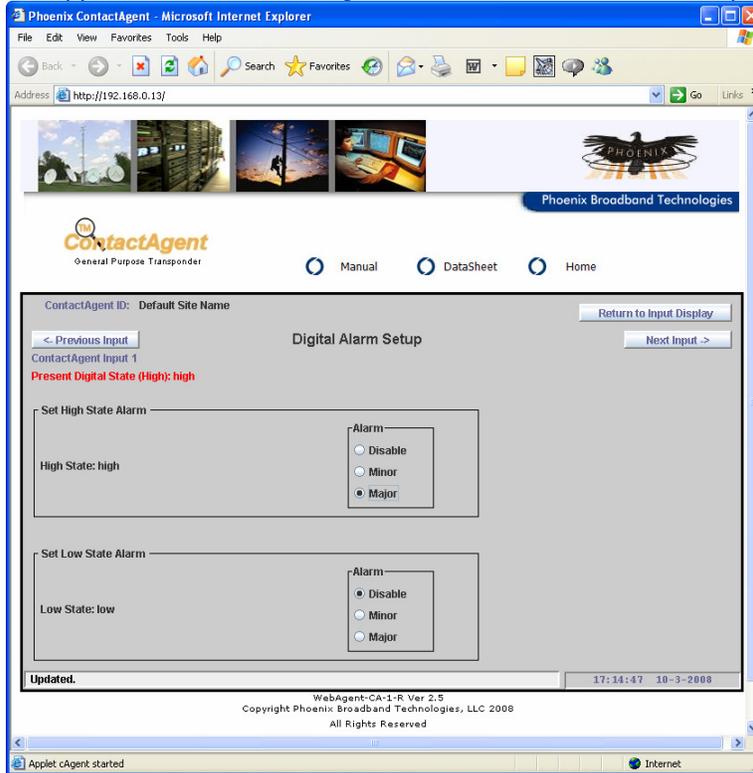
Output Setup

This screen is used to set the names of the outputs and the output states. Operation is similar to the **Input Setup Screen**.



Digital Alarms

When the **Setup Digital Alarms** button is pressed the Digital Alarm Setup screen shown below will appear. The **Present Digital State** of the selected RIM input is displayed, along with the user



defined text for the present state. Digital alarms may be set independently for each state of the input. Each alarm can be set to Disabled, Minor, or Major by selecting the radio button. Normally the alarm is enabled (Major or Minor) for only one state, however it is possible to have one state report a Minor alarm and the other state report a Major alarm.

In the example to the left the major alarm is enabled for the high state and the alarm is disabled for the low state. Since the input is in the high state the major alarm is being reported as indicated by the red text.

A SNMP Trap and/or an Email may be sent when the alarm occurs and when the alarm

returns to the normal state. Refer to the manual for the Host device for information on setting the Trap destinations and the Email addresses.



▪ **SNMP**

All of the information presented on the Web pages and complete configuration capability is available from SNMP.

SNMP uses the standard UDP ports 161 and 162. If the device does not respond to SNMP Requests or does not appear to send Traps, confirm that these ports are not blocked.

MIBs

The **ContactAgent**[™] uses a combination of standard and proprietary MIBs which can be found at <http://www.PhoenixBroadband.com/Downloads/MIBs/ContactAgent/ContactAgentMIBs.zip>. These MIBs can also be obtained at no charge by contacting Phoenix Broadband.

The **ContactAgent**[™] uses the following MIBs:

- HMS 028, SCTE 36 2002, SCTE Root MIB
- HMS 072, SCTE 37 2002, HMS Tree MIB
- HMS 026, SCTE 38-1 2002, HMS Property MIB
- HMS 023, SCTE 38-2 2002, HMS Alarm MIB
- HMS 024, SCTE 38-3 2002, HMS Common MIB
- pbtRootMIB
- pbtContactAgentMIB

For each input the label can be changed as well as the text associated with the high and low states. These strings can be found in the pbtCaInputTable. The pbtCaInputText object is the label displayed for each input. The pbtCaInputLowText object is the text displayed when the input is pulled low. The pbtCaInputHighText object is the text displayed when the input is pulled High or not connected. Each of these can be a maximum of 32 characters. All of these objects are stored in nonvolatile memory.

A similar set of objects for the output labels can be found in the pbtCaOutputTable.

The alarms are configured using the discreteAlarmEnable object in the discretePropertyTable. There are two objects for each input. The first object (.1) is used to enable alarms on the low state of the input. The second object (.2) is used to enable alarms on the high state of the input. Each alarm can be set to one of 3 states Disabled(1), EnableMajor(2), or EnableMinor(3). Major Alarms appear in red on the Web page, and Minor Alarms appear in yellow.

Community Strings

The community strings are configured from the Telnet interface described in the configuration section of this document. The default community strings are set to "public".

If the device does not respond to SNMP Requests or does not appear to send Traps, confirm that the community strings are set properly in the SNMP Manager.

Traps

SNMP Traps are sent to up to 3 trap receivers. The Trap Destinations are configured from the telnet interface described earlier in this document. The traps are defined in the heCommonMIB.



For Input traps the trap text is taken from the user programmable fields. The text comes from pbtRaInputLowText (Digital Input Low State Text) or pbtRaInputHighText (Digital Input High State Text). Only the first 20 characters of these objects are used. These objects can be configured using SNMP or the Web Page. When changes are made to these objects the device must be reset before the new text will appear in the traps.

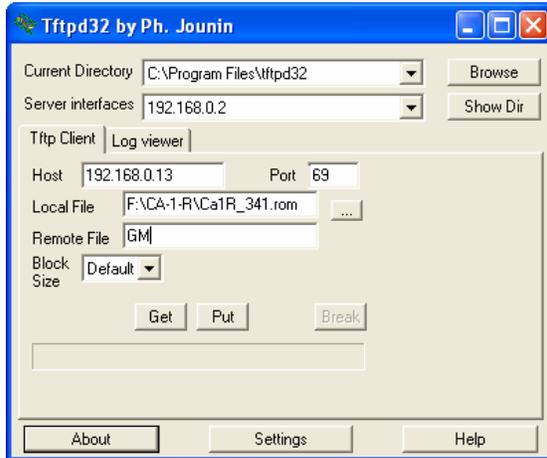
MIB Browsers

SNMP devices are normally managed by a software system containing a SNMP Manager. The simplest method of evaluating SNMP operation is with a MIB Browser. A free evaluation version of a MIB browser can be downloaded from <http://www.ndt-inc.com/SNMP/MIBrowser.html> or <http://www.mg-soft.com/download.html>.



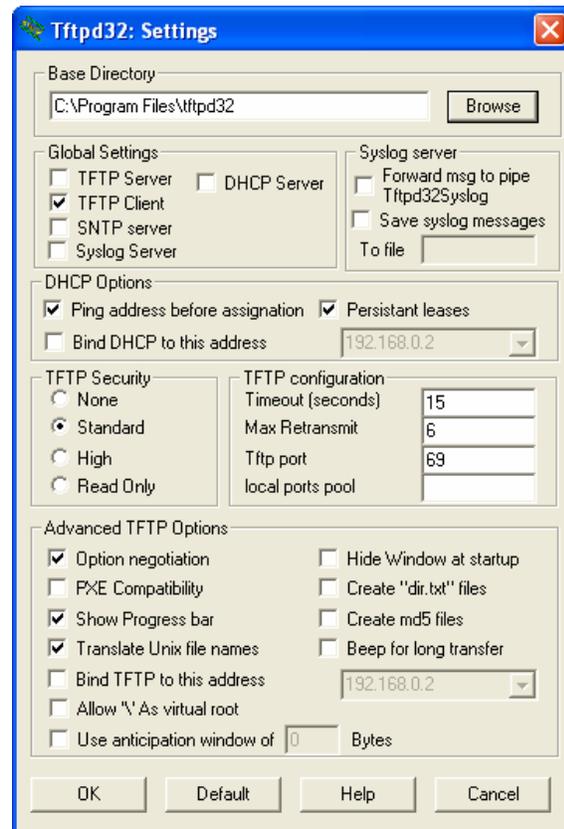
■ Firmware Updates

The **ContactAgent™** Firmware can be updated remotely using TFTP. To perform this update you will need a TFTP Client. A free TFTP Client can be downloaded from <http://moo.akacrasher.com/~philippej/tftpd32.html>. Be sure to read and comply with the licensing agreement. Other free TFTP clients are available on the internet. This TFTP client is used in the following example.



Run the TFTP Client and the window to the left will appear. Press the settings button and the window below will appear. Ignore the **Base Directory** setting and set all other options exactly as shown. Then press **OK**.

Select the **Tftp Client** tab and enter the IP Address of the device being updated in the **Host** field. The **Port** field should be set to 69. The **Local File** field should be set to the Firmware or Web file to be downloaded. If the Firmware is to be loaded it should be loaded first. All WEB files must be reloaded whenever the firmware loaded. Set the Remote file name to **GM** and the **Block Size** to default.



Press the **Put** button to upload the file to the **ContactAgent**. A progress bar will appear as the upload starts. The firmware upload normally takes about 20 seconds. A Window similar to the one below will appear when the upload is complete.



Press **OK** and continue with the next file. The local and remote files names for the 4 **ContactAgent** files are shown in the table below.

	Local File Name	Remote File Name
Firmware	Ca1R_341.rom	GM
Web files	Ca1Rweb1_250.rom	WEB1
Web files	Ca1Rweb2_250.rom	WEB2
Web files	Ca1Rweb3_250.rom	WEB3



▪ **Specifications**

Electrical:

Inputs (8 ea)	Contact closure to ground or CMOS logic levels
Outputs (2 ea)	Form-C floating relay contacts; 100V, 1A max
Power	5-12 volts AC or DC; 500ma max; typically powered by wall transformer

Network Interface 10/100 Ethernet

Monitoring Protocol SNMP

Other Monitoring Interfaces

Web Server
SMTP E-mail

Mechanical:

Size	8.4"x 4.2"x1.5"
Construction	Molded plastic
Connectors	
Contact I/O	Plug-in terminal block
Serial I/O	RJ-45
Ethernet	RJ-45
Power	Male coaxial barrel type 5.5x2.5 mm
Weight	1.0 lb nominal

Indicators:

Ethernet link activity
Power/Status LED

Environmental:

Operating Temperature -40C to +60C
Humidity 0 to 95%; non-condensing