Wi-Fi Terminus SLT Configuring for Wi-Fi Networks

JANUS REMOTE COMMUNICATIONS

Bulletin	JA11-WiFi
Revision	P01
Date	25 May 2011

Table of Contents

Introduction

The Wi-Fi Terminus SLT (Wi-Fi Terminus) is a device that combines the GPS technology, for position information (longitude and latitude) and UTC time, with Wi-Fi 802.11b/g for NMEA stream transport. The 802.11b/g supports WPA2 encryption and is fully configurable to a specific network.

In addition to these features, the Wi-Fi Terminus can be used for indoor positioning with the Ekahau Positioning Engine. The indoor environment represents a challenge for the GPS based location devices due to low signal strengths which lead to the inability of a device to come up with a location or the poor accuracy of such an implementation. The Wi-Fi Terminus represents a successful blend of the two concepts of positioning:

- outdoor, GPS based location and
- indoor, Wi-Fi based location

Used together, these two technologies would offer 100% coverage in any environment.

Purpose of the Document

This document is not intended to be an exhaustive description of the Wi-Fi Terminus' features and configuration options. Instead this document presents general guidelines and examples for a better understanding on how to set up the Wi-Fi Terminus unit for a specific Wi-Fi network that has security enabled. Consult the Wi-Fi Terminus Data Sheet for more in-depth features and configuration options.

Pre-Requisites

It is assumed that the user is familiar with the process of connecting to the Wi-Fi Terminus unit, detailed in the "Wi-Fi Terminus – Quick Start Guide" document. The Wi-Fi Terminus unit comes with a predefined set of default parameters that the unit looks for upon power up. These parameters and required infrastructure represent the minimum necessary in order to be able to further access and configure the unit for a specific Wi-Fi environment.

Topology:	Infrastructure Mode
Source IP:	192.168.1.3 (Default IP of each Wi-Fi Terminus unit)
Network SSID:	CW85_Setup
Channel:	6
Security:	Disabled
Data Rate:	1 Mbps
Packet type:	UDP (type of packet used for relaying NMEA stream)
Dest. IP:	192.168.1.2 (IP where the NMEA data is being sent)
Dest. Port:	9999 (Destination port of the NMEA data being sent)

Pre-Requisites continued

Once the wireless access point configuration has been performed, the Wi-Fi Terminus will unit connect to the access point when switched “On”. The Status LED will give an indication of network status and GPS status as indicated in Table 1.

Condition	Status LED
No Network detected and no GPS fix	OFF
Network detected but no GPS Fix	Blinks once every 2.5 seconds
No network detected but GPS Fix	Blinks once every 5 seconds
Network detected and GPS Fix	Blinks once every 0.5 seconds

Table 1- Status LED

As soon as the Wi-Fi Terminus associates with the network it will try to resolve the destination IP. Once this has been accomplished, the Wi-Fi Terminus will begin sending UDP packets to the destination IP.

Net-SNMP installation

The Wi-Fi Terminus parameters are configured via a Simple Network Management Protocol (SNMP) manager. The Wi-Fi Terminus supports version 1 (SNMPv1). We recommend using Net-SNMP software as an easy method to understand and manage the Wi-Fi Terminus parameters using SNMP. The Net-SNMP homepage is http://www.net-snmp.org. The latest version can be downloaded free of charge from http://www.net-snmp.org/download.html.

For Windows™ based users, select the “binaries” link, which will point you to “SourceForge” web address. From here the appropriate binary installation file is to be selected, depending on the operating system currently running on the SNMP machine:

- 32-bit - net-snmp-(version_number)-1.x86.exe
- 64-bit - net-snmp-(version_number)-2.x64.exe

Once installed, the net-SNMP software can be used to read (get) and write (set) to the Wi-Fi Terminus parameter database using the “snmpget” and “snmpset” commands. For more information on the structure of these commands please consult the Net-SNMP documentation or the Wi-Fi Terminus Data Sheet.

*Note: Linux *.rpm packages are available at the same location under the same “binaries” link.*

Configuring the Wi-Fi Terminus for the New Network

Network Settings

These network settings take effect on a power cycle, so they should all be changed (including encryption, if necessary) and then the unit should be rebooted for these settings to take effect. It is highly recommended to change just the settings for SSID1 so that if something is not right, it is easy to go back into the device using the "CW85_Setup" on SSID2. IMPORTANT - once the network settings are modified and the Wi-Fi Terminus is ready to be rebooted - bring down the "CW85_Setup" network so that the device can no longer see it and try to connect.

The settings below are most likely to change such that the Wi-Fi Terminus would work in a network (full OIDs are specified in parenthesis):

- GSNIPADDRESS (.1.3.6.1.4.1.28295.1.1.3.1.0) – IP address
- GSNSUBNETADDRESS (.1.3.6.1.4.1.28295.1.1.3.2.0) – subnet address
- GSNGATEWAYIPADDRESS (.1.3.6.1.4.1.28295.1.1.3.3.0) – gateway IP address
- STATICIPENABLED (.1.3.6.1.4.1.28295.1.1.3.4.0) - to set the device for DHCP, leave the above OIDs as they are and set this OID to 0 (default is 1).
- GSNPRIMARYSNMPMGRIP (.1.3.6.1.4.1.28295.1.1.4.3.0) – SNMP Manager
- GSNAPSSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.2.1) - change the SSID1.
- GSNAPCHANNEL1 (.1.3.6.1.4.1.28295.1.1.4.5.1.3.1) - channel should match SSID1

Wi-Fi Security Settings

Encryption may need to be added for the new network. Please note that these options are read-disabled - so close attention must be paid to the response string when setting these options for confirmation that they are set appropriately for the network.

WEP Settings for SSID1 (note that there is no passphrase option - only hex key):

- GSNWEPKEYIDSSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.4.1) – WEP key ID
- GSNWEPKEYLENSSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.5.1) – WEP key length
- GSNWEPKEYAUTHMODESSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.8.1) - Authentication
- GSNENCRYPTIONMODESSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.9.1) – Encryption control
- GSNAPWEPKEYVALSSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.6.1) – WEP key value

WPA/WPA2 settings for SSID1

- GSNAPPSKPASSPHRASESSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.7.1) – WPA passphrase

or

- GSNPSKKEY1 (.1.3.6.1.4.1.28295.1.1.2.10.0) – Pre-computed PSK key
- GSNENCRYPTIONMODESSID1 (.1.3.6.1.4.1.28295.1.1.4.5.1.9.1) - Encryption control

Configuring the Wi-Fi Terminus for the New Network continued

Terminal Server Settings

To send data to the new server, you may need to change the IP and Port for the real-time GPS data stream.

- GSNSENSORSERVERIP (.1.3.6.1.4.1.28295.99.1.2.1.6.5) - IP address of the sensor data server
- GSNSENSORDATAPORTNUM (.1.3.6.1.4.1.28295.99.1.2.1.9.5) - Port number of the sensor data server

To change the IP and port for the logged GPS data use

- NTLOGSERVERIPADDR (.1.3.6.1.4.1.28295.99.1.2.1.6.3) - IP for the data log server
- NTLOGSERVERPORTNUM (.1.3.6.1.4.1.28295.99.1.2.1.9.3) - Port for the data log server

GPS Configurations

- NTGPSUPDATERATE (.1.3.6.1.4.1.28295.99.1.2.1.16.5) - Data transmission rate in seconds
- NTMSGENABLE (.1.3.6.1.4.1.28295.99.1.2.1.21.5) - controls which GPS messages are enabled.

In order to be able to change any of the parameters above, Net-SNMP is used through the **“snmpset”** command and **“Command Prompt”** window. The format of a snmpset command is:

```
snmpset [OPTIONS] AGENT OID TYPE VALUE
```

The [OPTIONS] include:

- The SNMP version specifier, ‘-v 1’. The Wi-Fi Terminus uses SNMPv1.
- An output format specifier, ‘-O a’, which requests string values to be printed as ASCII text.
- The community name, ‘-c GSN_SET’. The community name for setting a Wi-Fi Terminus device is “GSN_SET”.

The TYPE of the VALUE parameter must be specified in a single character, as shown in the following “Data Type” table (see Table 2). The data type for each Wi-Fi Terminus parameter appears in the in the Wi-Fi Terminus OID Table available in the data sheet.

Type	Type Specifier	Description
Integer	i	A whole number
String	s	Character string
IpAddress	a	Four-octet string of hexadecimal data
HEX	x	Hexadecimal string

Table 2- Data Type

The parameter value itself should be enclosed in quotations. It is not always necessary to enclose the parameter in quotations, but it is required if the parameter value has spaces. It is recommended to always use quotations and to verify that the response string on a set matches the intended input type and value.

Configuring Examples

In the example below we'll be configuring the Wi-Fi Terminus parameters outlined above. Remember that it is imperative to be connected to the Wi-Fi Terminus first in order to be able to change these parameters. The procedure to connect to the defaulted Wi-Fi Terminus has been outlined in the "Quick Start Guide."

The commands that will follow in the two examples below can be copied and pasted in the command prompt window. The parameters have to be changed in order to match the specific network the Wi-Fi Terminus is going to be configured for.

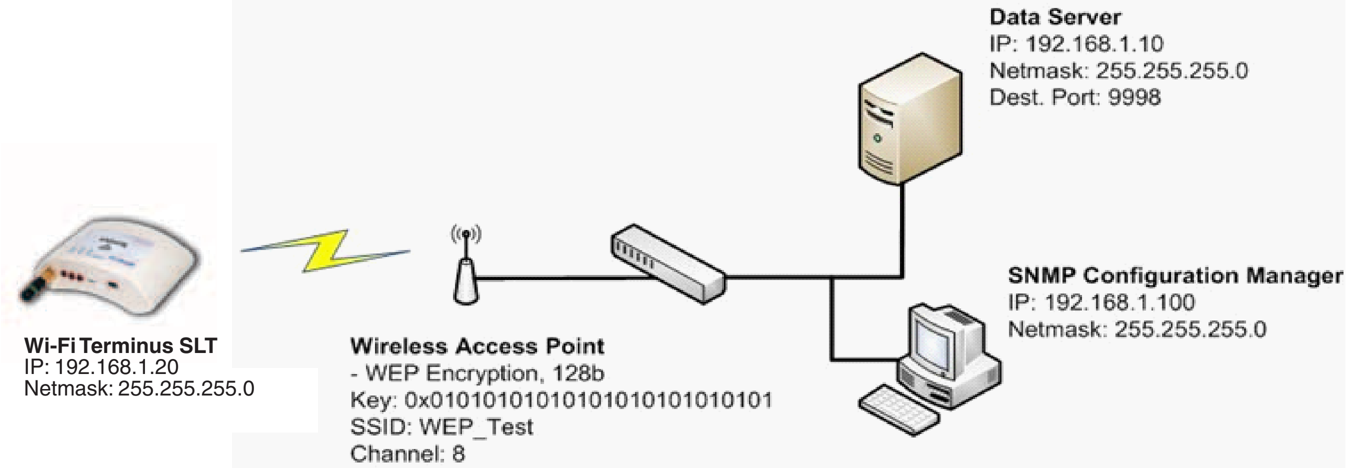
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\          \NavTrac v4>
```

Figure 1: Command Prompt

Example 1

The basic diagram for the first example can be seen below, in Figure 2.



Data Server
IP: 192.168.1.10
Netmask: 255.255.255.0
Dest. Port: 9998

SNMP Configuration Manager
IP: 192.168.1.100
Netmask: 255.255.255.0

Wi-Fi Terminus SLT
IP: 192.168.1.20
Netmask: 255.255.255.0

Wireless Access Point
- WEP Encryption, 128b
Key: 0x01010101010101010101010101
SSID: WEP_Test
Channel: 8

Figure 2: WEP Example

It is imagined that the Wi-Fi Terminus would be working in a Wi-Fi network with a 128bit WEP encryption key. The SSID of the Wi-Fi is "WEP_Test" while the channel used is number 8. The Wi-Fi Terminus unit will be configured to send the GPS NMEA stream to a local "Data Server" with the IP: 192.168.1.10, on UDP port 9998. Since it's a local data server a gateway is not required. The SNMP configuration manager will be represented by a PC in that network with the IP 192.168.1.100. Finally the Wi-Fi Terminus will be provided with a static IP of: 192.168.1.20.

Configuring Examples continued

Example 1 continued

LAN Settings

GSNIPADDRESS

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.1.0 a “192.168.1.20”
```

GSNSUBNETADDRESS

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.2.0 a “255.255.255.0”
```

```
SNMPv2-SMI::enterprises.28295.1.1.3.2.0 = IpAddress: “new subnet”
```

STATICIPENABLED

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.4.0 i 1
```

GSNPRIMARYSNMPMGRIP - change the SNMP manager to the machine on the new network that will control the Wi-Fi Terminus. Leave the GSNSECONDARYSNMPMGRIP at 192.168.1.2 so that the unit will default back to the “CW85_Setup” SSID if needed. Once the unit has been brought up on the new network, the GSNSECONDARYSNMPMGRIP can be changed to a new IP or set to 0.0.0.0 in order to disable it, or leave it at the default.

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.3.0 a “192.168.1.100”
```

Wireless Settings

GSNAPSSID1

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.2.1 s “WEP_Test”
```

GSNAPCHANNEL1

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.3.1 i 8
```

WEP Settings

GSNWEPKEYIDSSID1

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.4.1 i 0
```

GSNWEPKEYLENSSID1

This sets WEP64 or WEP128 - default is WEP64. 13 sets to WEP128

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.5.1 i 13
```

GSNWEPKEYAUTHMODESSID1 - Default is Open Key (1), can be changed to Shared Key (2)

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.8.1 i 1
```

Configuring Examples continued

GSNENCRYPTIONMODESSID1 - This OID controls which encryption types are allowed on SSID1. By default, all possible encryption types are enabled. This should be reduced to only the appropriate type. The bitmap, of the binary equivalent, controls which encryption methods are allowed can be seen in Table 3. WPA Enterprise encryption modes (bit 3 and 6) are currently not available.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Open Encryption	WPA2-Enterprise	RESERVED	WPA2 - Personal	WPA-Enterprise	RESERVED	WPA-Personal	WEP

Table 3 - Encryption Bitmap

Binary of 16 (00010000b) - corresponds with bit 4 – WPA2-Personal Encryption

Binary of 2 (00000010b) - corresponds to bit 1 – WPA Personal Encryption

Binary of 1 (00000001b) - corresponds to bit 0 – WEP Encryption

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.9.1 i 1
```

GSNAPWEPKEYVALSSID1 -

This OID sets the encryption key, in hexadecimal. There is no passphrase option for WEP.

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.6.1 x
0x01010101010101010101010101
```

Once all of the appropriate settings have been changed, bring the CW85_Setup network down and reboot the Wi-Fi Terminus device. You should see the status indicator flash appropriate that it is able to associate with the new network. You should also be able to communicate with the device with the newly configured SNMP manager (192.168.1.100 – in our example). If the device fails to associate with the new network, bring that network down and restore the CW85_Setup network and double check the settings. For the security settings, you need to pay close attention to the SNMP response when you set them as this is the only way to confirm that it used the right values - you cannot read them back over SNMP for protection.

Example 2

Example 2 is similar with the first one, the only difference being a change in the wireless encryption protocol and hence a change in the pass phrase.

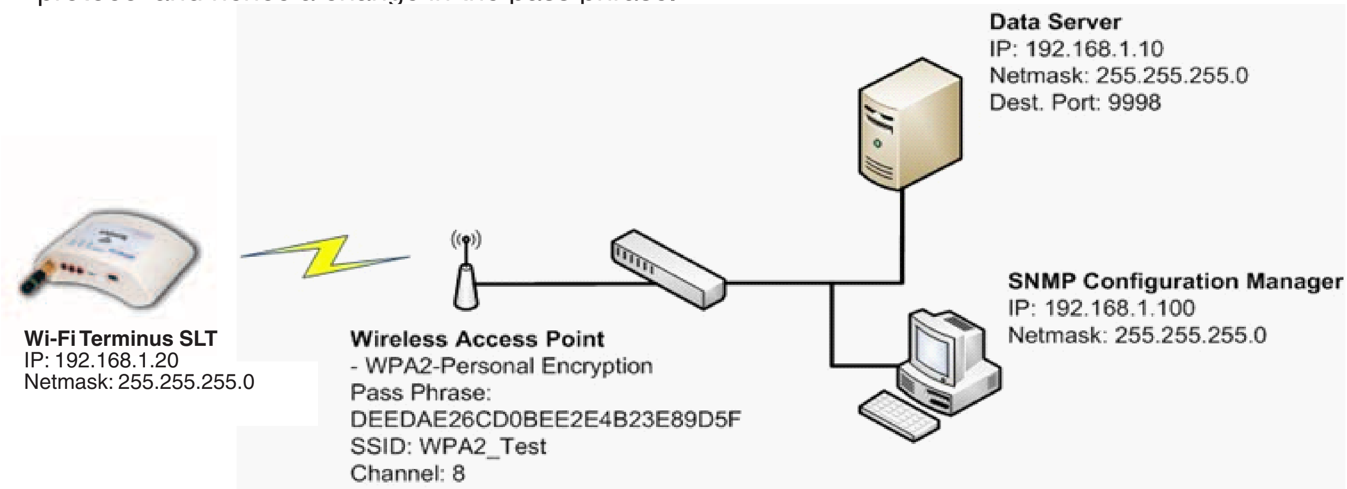


Figure 3: WPA2 Example

Configuring Examples continued

Example 2 continued

WPA/WPA2 Settings

GSNAPPSKPASSPHRASESSID1

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.7.1 s
“DEEDAE26CD0BEE2E4B23E89D5F”
```

Be sure to enclose the passphrase in quotes or it may be truncated. Other parameter that can be changed is: GSNPSKKEY1. Use this OID to set the key INSTEAD of using a passphrase. It is not necessary to use this if you use the passphrase.

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.2.10.0 x 0x(64digits)
```

Where the 64 digits are 0-9 and A-F

Terminal Servers Settings

GPS Data Server

GSNSENSORSERVERIP - This OID sets the destination IP for the real-time GPS data is being sent to.

```
snmpset -v1 -Oa -c GSN_SET <Device IP addr> .1.3.6.1.4.1.28295.99.1.2.1.6.5 a “destination”
```

Please use decimal dot notation for the IP addresses, eg - 192.168.1.3. For both examples above

```
snmpset -v1 -Oa -c GSN_SET 192.168.1.20 .1.3.6.1.4.1.28295.99.1.2.1.6.5 a 192.168.1.10
```

GSNSENSORDATAPORTNUM - This OID sets the destination port for the real-time GPS data.

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.9.5 i newPort
snmpset -v1 -Oa -c GSN_SET 192.168.1.20 .1.3.6.1.4.1.28295.99.1.2.1.9.5 i 9998
```

Log Server

NTLOGSERVERIPADDR - This OID sets the destination IP for the logged GPS data. Same server as above could be used.

```
snmpset -v1 -Oa -c GSN_SET <Device IP addr> .1.3.6.1.4.1.28295.99.1.2.1.6.3 a “destination”
```

Please use decimal dot notation for the IP addresses, eg - 192.168.1.3

NTLOGSERVERPORTNUM - This OID sets the destination port for the logged GPS data.

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.9.3 i newPort
```

No change is required to the packet type if you want to use UDP. To use TCP for either the real time data or the data log, use one or both of the following:

NTDATASERVERPORTTYPE - This OID sets the data server port type (real-time data).

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.7.5 i 2
```

For this OID, 2 is TCP and 1 is UDP. No other options are valid.

NTLOGSERVERPORTTYPE - This OID sets the log server port type (logged GPS data)

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.7.3 i 2
```

For this OID, 2 is TCP and 1 is UDP. No other options are valid.

GPS Configuration

NTGPSUPDATERATE - This OID controls the rate at which the GPS gives real-time updates to position.

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.16.5 i rate
```

The rate is in seconds. Setting rate as 2 sets the device to report every other second, 3 sets the device to report every three seconds... etc.

NTMSGENABLE - This OID controls the enabling of the GPS messages by the bitwise binary representation of the integer "msgs".

```
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.21.5 i msgs
```

Order of the bitwise binary representation (MSB to LSB):

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	GPVTG	GPZDA	GPRMC	GPGSV	GPGSA	GPGLL	GPGGA

Table 4 - GPS messages enable/disable bitmap

GPRMC only is 0001 0000b, which is the integer 16

GPGLL only is 0000 0010b, which is the integer 2

GPGGA only is 0000 0001b, which is the integer 1

For GPRMC, GPGLL and GPGGA, you would send 19 (16+2+1) in this string.

If all of the messages are disabled, the power indicator will no longer flash. The flash interval is based on the GPS update rate and if the rate is 0 or the messages are all disabled, this light will no longer flash. If the message rate changes, the rate that this LED flashes will also change. The duration of the flash is based on the number of messages that are enabled - a longer flash indicates more messages are being sent.

Unlike the network settings, which need a reboot to take effect, these changes are all immediate EXCEPT for packet type. Also, if the TCP connection is already established, the new IP/Port won't take effect until a new socket connection is made.

The document provided a more in depth view on the configurations available for the Wi-Fi Terminus GPS module. It highlighted, with two simple examples, the main OIDs and configuration settings in order to have this module set up in a wide variety of wireless networks with different security, encryption settings and terminal servers. Ultimately it is the task of these terminal servers to process the location information sent by the Wi-Fi Terminus devices over the wireless networks and present it in a user friendly way.

Wi-Fi Terminus SLT Configuring for Wi-Fi Networks

References

1. Wi-Fi Terminus Product Brief - General description of the Wi-Fi Terminus and its features
2. Wi-Fi Terminus Datasheet - More information on all the available features and settings. (also see Appendix I)
3. Wi-Fi Terminus Quick Start Guide - Get connected to a Wi-Fi Terminus unit in the minimum amount of time.

Revision	Revision Date	Notes
P00	11/12/10	Preliminary Release
P01	05/25/11	Name Change & Updates

JANUS REMOTE COMMUNICATIONS

Division of The Connor-Winfield Corporation
2111 Comprehensive Drive • Aurora, Illinois 60505
630.499.2121 • Fax: 630.851.5040
www.janus-rc.com

Janus Remote Communications Europe

Bay 143
Shannon Industrial Estate
Shannon, Co. Clare, Ireland
Phone: +353 61 475 666