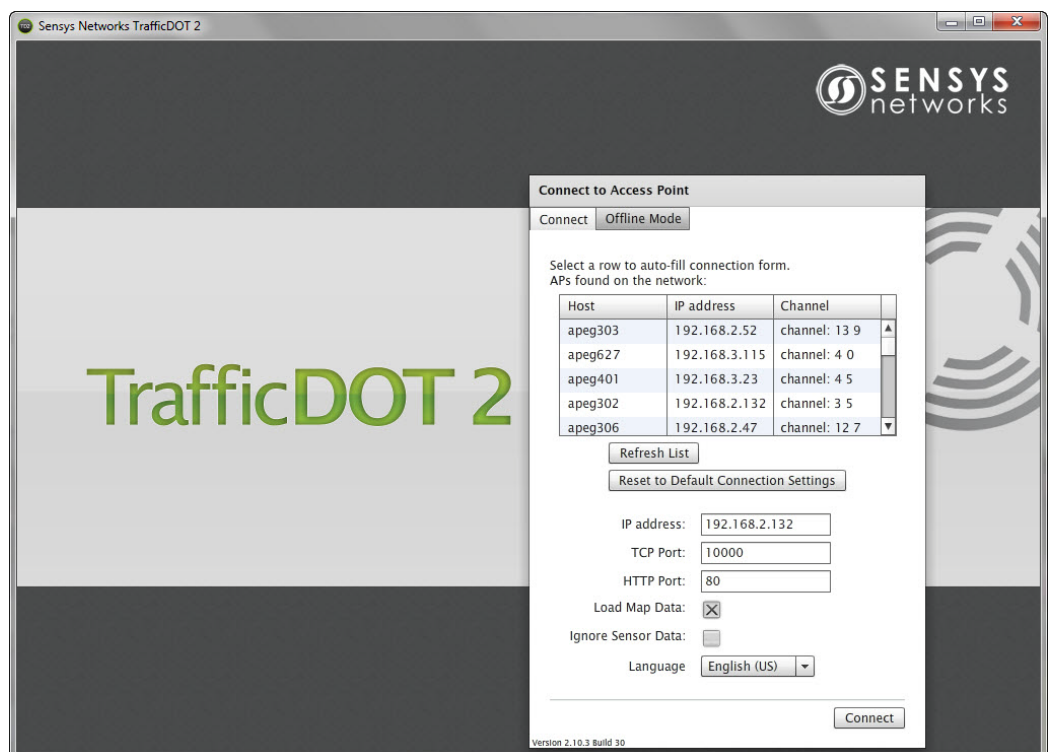


# Sensys Networks VDS240 Wireless Vehicle Detection System

## TrafficDOT v2.10.3 Set Up and Operating Guide

P/N 152-240-001-071, Rev B

August 2014



## Document Properties

This document is reference material for the Sensys Networks VDS240 wireless vehicle detection system from Sensys Networks, Inc.

P/N 152-240-001-071 Rev B

Sensys Networks, Inc. makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Sensys Networks reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Sensys Networks to notify any person or organization of such revisions or changes.

© 2007 - 2014 – All rights reserved.

Sensys Networks and the Sensys Networks logo are trademarks of Sensys Networks, Inc. All other products, names and services are trademarks or registered trademarks of their respective owners.

## Regulatory Statements

### FCC Compliance Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications to this product not authorized by Sensys Networks could void the EMC compliance and negate the authority to operate the product.

### RF Exposure Statement

This device has been tested and meets the FCC RF exposure guidelines. It should be installed and operated with a minimum distance of 20 cm between the radiator of RF energy and the body of users, operators or others.

Improper use or tampering with the device is prohibited and may not ensure compliance with FCC exposure guidelines.

## Warnings

### No Safety Switching

Sensys Networks **does not** allow its equipment to be used for safety applications such as controlling a mechanical gate or switching a train to avoid a collision.

## Lithium Thionyl Chloride Batteries

Sensys Networks uses Lithium Thionyl Chloride batteries in the following products:

- Sensors (VSN240-F, VSN240-T, VSN240-S, VSN240-M, VSN240-F-2, VSN240-T-2)
- Repeaters (RP240-B, RP240-BH, RP240-B-LL, and RP240-BH-LL, FLEX-RP-B)

Lithium batteries are widely used in electronic products because they contain more energy per unit -weight than conventional batteries. However, the same properties that deliver high energy density also contribute to potential hazards if the batteries are damaged. Improper use or handling of the batteries may result in leakage or release of battery contents, explosion or fire.

Following are the recommendations of the battery manufacturer for proper use and handling of batteries in the Sensys Networks devices mentioned above:

- **DO NOT** charge or attempt to recharge the batteries (they are NOT rechargeable)
- **DO NOT** crush or puncture batteries
- **DO NOT** short-circuit the batteries
- **DO NOT** force over-discharge of the batteries
- **DO NOT** incinerate or expose batteries to excessive heating
- **DO NOT** expose battery contents to water
- **DO** dispose of batteries and devices containing batteries in accordance with local regulations

---

### NOTE:

Sensys Networks wireless sensors contain no serviceable parts and should never be disassembled. Installation and removal of sensors from pavement should only be done by trained personnel and care should be taken to insure that the sensor casing is not punctured or crushed.

---

Additional safety information is available from the battery's manufacturer:

- Sensor battery cell: <http://www.ultralifecorporation.com/download/308>
- Repeater battery cell: <http://www.ewtbattery.com/en/DownView.asp?ID=9>

## Document Control

Sensys Networks continually reviews and revises its technical publications. Please address questions, suggestions or corrections to [support@sensysnetworks.com](mailto:support@sensysnetworks.com).

## **Sensys Networks Technical Publications**

For additional information regarding Sensys Networks products and applications, design guides, configuration guides, and best practices, refer to the Sensys Networks technical documents library available at [http://www.sensysnetworks.com/services\\_support/techdocs](http://www.sensysnetworks.com/services_support/techdocs).

## **Contact Information**

### **Sensys Networks, Inc.**

1608 Fourth Street, Suite 200

Berkeley, CA 94710 USA

+1 (510) 548-4620

[www.sensysnetworks.com](http://www.sensysnetworks.com)



---

# Contents

<b>Chapter 1: Introduction .....</b>	<b>1</b>
What's Inside .....	1
Differences From Prior Versions .....	2
<b>Chapter 2: Understanding TrafficDOT .....</b>	<b>3</b>
Overview .....	3
Configuring Equipment With TrafficDOT .....	4
Configuration Functions .....	4
Management Functions .....	4
Monitoring Detector Device Health and Performance .....	5
Remotely Managing Detector Networks and Device Properties .....	5
Configuring Complex Deployments in Advance of Installation .....	5
Troubleshooting Detection Network Behavior .....	6
<b>Chapter 3: Installing TrafficDOT .....</b>	<b>7</b>
What's Required for Installation .....	7
Hardware .....	9
Installation Procedure .....	9
<b>Chapter 4: Using TrafficDOT .....</b>	<b>13</b>
Overview .....	13
TrafficDOT Map View .....	14
Using TrafficDOT to Create a Network .....	16
Connecting to an Access Point .....	16
Connect Window Contents .....	17
Offline Mode Window Contents .....	17
Connecting at Start Up of TrafficDOT .....	18
Connecting via the Connect menu .....	19
Site Panel .....	19
Site Panel Contents .....	19
Entering Site Information .....	20
Uploading a Map Image .....	21
Creating Sensor Zones .....	22
Sensor Zone Panel Contents .....	22
Creating a Sensor Zone .....	23
Adding Key Components .....	25
Dragging a Sensor onto a Sensor Zone .....	25
Device Health Indicator .....	26
<b>Chapter 5: Configuring and Managing Components .....</b>	<b>29</b>

---

Overview .....	29
Configuring VSN240 Wireless Sensors .....	30
Introduction .....	30
Selecting Sensors .....	30
Selecting Parameters .....	30
Working with the Sensor Configuration Window .....	30
Position Window Contents .....	31
Setting a Sensor's Position .....	32
Configuring Card Addresses .....	33
Card Addresses Window Contents .....	33
Mapping Sensors to Contact Closures .....	33
Configuring Advanced Settings .....	34
Advanced Settings Window Contents .....	35
Configuring Commands to Sensor .....	38
Setting a Sensor's RF Channel .....	39
Setting a Sensor's Operating Mode .....	40
Performing a Soft Reset .....	40
Performing a Hard Reset .....	41
Downloading Sensor Firmware .....	41
Recalibrating a Sensor .....	41
Setting a Sensor IDs .....	41
Pairing Sensors .....	42
Pairing Window Contents .....	43
Configuring MicroRadar Sensors .....	44
Working in the Advanced Settings Window for MicroRadar Sensors .....	44
Recommended Advanced Settings .....	44
Configuring Detection Distance .....	44
Configuring Autobaseline .....	45
Working in the Commands to MicroRadar Sensor Window .....	46
Setting a MicroRadar Sensor's Operating Mode .....	46
Working with the Card Addresses Window .....	47
Mapping MicroRadar Sensors to Contact Closures .....	47
Configuring Access Points .....	49
Introduction .....	49
Working with the Access Point Configuration Window .....	49
Viewing the Access Point ID and Firmware Version .....	50
Configuring Radio Settings .....	50
Enabling Master Mode .....	51
Setting the RF Channel .....	52
Setting the PA Attenuation .....	52
Configuring Event Parameters .....	52
Setting the Transmit Interval .....	53
Setting the Maximum Reporting Latency .....	53
Enabling Synchronized Reporting .....	54
Setting a Watchdog Timeout .....	54
Configuring Event Reporting Buffer Controls (N Events / Near Full) .....	54
Configuring Extra Latency .....	55
Limiting Reporting to On (Detection) Events Only .....	55
Enabling the Magnetometer Sensor for MicroRadar .....	55
Configuring Detection Settings .....	55
Setting the Onset Filter .....	56
Setting Thresholds for Detection and Undetection .....	57

---

Setting the Holdover Attribute .....	57
Enabling a Swap of the X and Y Measurements .....	57
Setting the Recalibrate Timeouts .....	58
Setting the Stop Bar Recalibration Timeout .....	58
Setting the Count Recalibrate Timeout .....	58
Enabling International Mode .....	58
Selecting Disable Auto Re-baseline .....	58
Configuring Advanced Settings .....	59
Enabling Retransmission of RSSI and LQI .....	59
Enabling Packet Rewriting .....	59
Enabling Expectation of Acknowledgments .....	60
Entering Contact Closure Card Latency and Enabling Reverse Polarity .....	60
Assigning an Access Point Color Code .....	60
Configuring Command Settings .....	60
Configuring System Configuration Settings .....	61
Configuring with Network Settings .....	62
Setting the IP Mode .....	62
Setting the Ethernet Mode .....	62
Specifying the Network Mask .....	63
Specifying the IP Address .....	63
Designating the Gateway .....	63
Designating the DNS Servers .....	63
Designating the DHCP Monitor Host .....	63
Specifying the Network Time Sources .....	63
Configuring PTP Settings .....	63
Specifying the Sensys Networks Management Server .....	64
Selecting the PTP Mode .....	64
Defining the PTP User and Password .....	64
Specifying the Host to Monitor for PTP Communications .....	65
Configuring Push Settings .....	65
Destination servers .....	66
Individual Speed Mode .....	67
Units .....	67
Individual Car Reports .....	67
Report Interval .....	68
Maximum File Size .....	68
Average Speed .....	68
Speed Histogram .....	68
Length Histogram .....	68
Timestamp Option .....	69
Use Diagnostic to Correct Averages .....	69
Display Diagnostics .....	69
Show Radar Detail for Large Objects .....	69
Configuring Poll Settings .....	69
TCP Port Number .....	70
Operating Mode .....	70
Units .....	71
Individual Speed Mode .....	71
Individual Car Reports .....	71
Report Interval .....	71
Maximum File Size .....	71
Average Speed .....	71

Speed Histogram .....	72
Length Histogram .....	72
Timestamp Option .....	73
Use Diagnostic to Correct Averages .....	73
Display Diagnostics .....	73
Configuring California DOT District 3 Poll Servers .....	73
TCP Port Number .....	74
1st Drop Number .....	74
2nd Drop Number .....	74
Configuring California DOT District 4 Poll Servers .....	74
Port Number .....	75
Controller Address .....	75
Configuration Type .....	75
Configuring Marksman Poll Servers .....	75
Designating the Port Number .....	76
Selecting a Reporting Mode .....	76
Show Radar Detail for Large Objects .....	76
Configuring Memory Settings .....	76
Window Contents and Operation .....	77
Automatically Allocating Memory to the Processes .....	77
Manually Allocating Memory to the Processes .....	77
Configuring Other Properties .....	78
Time Settings .....	78
Serial Application Settings .....	79
Custom Application Settings .....	80
Event Proxy Settings .....	82
Advanced AP Diagnostic Settings .....	82
Configuring SncProxy Settings .....	84
Configuring Commands Settings .....	85
Backup/Restore an Access Point's Configuration .....	86
Selecting an Access Point License File .....	87
Downloading a Diagnostic File .....	87
Configuring Repeaters .....	88
Introduction .....	88
Tandem Repeaters .....	88
Working with the Repeater Configuration Window .....	88
Viewing the Repeater Firmware Version and Entering a Repeater Name .....	89
Selecting an External Antenna .....	90
Specifying the RF Channels .....	91
Setting the Time Slot of a Repeater .....	92
Performing a Soft Reset .....	93
Performing a Hard Reset .....	93
Downloading Repeater Firmware .....	93
Configuring Contact Closure Cards .....	94
Working with the Controller Card Configuration Window .....	94
Configuring Controller Card Channels .....	95
Performing a Soft Reset .....	97
Performing a Hard Reset .....	98
<b>Chapter 6: Monitoring Components Using the Table View .....</b>	<b>99</b>
Overview .....	99
Menus .....	100

Connect .....	100
Tools .....	100
Advanced .....	101
Help .....	101
System Display .....	101
<b>Appendix A: Configuring Cellular Modems on an AP or an APCC .....</b>	<b>105</b>
GSM/GPRS Modems .....	105
Cingular .....	107
T-Mobile .....	107
CDMA Modems .....	108
Verizon .....	109
Aeris .....	110
<b>Appendix B: Addon Configuration .....</b>	<b>111</b>
Addons Support .....	111
Supported USB Chipsets .....	112
Addons Panel .....	112
Addons .....	113
ASIX Ethernet Driver .....	113
Elements .....	113
Lonestar TSS .....	114
Elements .....	114
Modem Power Management .....	115
Elements .....	115
RTL8192 Wireless Driver .....	116
Elements .....	116
SD Card Sync .....	117
Elements .....	117
USB Drive Sync .....	118
Elements .....	118
<b>Appendix C: Anti-Vandalism .....</b>	<b>119</b>
Overview .....	119
Anti-Vandalism Functionality .....	119
Anti-Vandalism Configuration .....	120
Selecting Anti-Vandalism Option .....	120
Configuring Key Management .....	121
Configuring Application Settings .....	122



## Introduction

This guide provides information and procedures for installing and configuring TrafficDOT 2.10.3 in conjunction with the Sensys Networks VDS240 wireless vehicle detection system. This document is intended to be used by Sensys Networks customers, consultants, partners, dealers, and those who are interested in the application of wireless communication technology to the challenges of traffic detection, management, and control.

### What's Inside

This guide includes the following information:

- *Chapter 1: Introduction*, provides the purpose and scope of the guide, as well as an overview of each chapter. This chapter also provides information regarding the differences between the previous release of TrafficDOT.
- *Chapter 2: Understanding TrafficDOT*, describes the configuration, management, and monitoring functions of TrafficDOT.
- *Chapter 3: Installing TrafficDOT*, provides TrafficDOT hardware requirements, and an overview of the application's installation process.
- *Chapter 4: Using TrafficDOT*, provides information and instructions on using TrafficDOT to create a system network.
- *Chapter 5: Configuring and Managing Components*, provides information and instructions required to configure and manage Sensys Networks VDS240 vehicle detection system components using the map view.
- *Chapter 6: Monitoring Components Using the Table View*, provides information on monitoring system components using the table view.
- *Appendix A: Configuring Cellular Modems on an AP or an APCC*, provides the information required to configure cellular modems on either an access point or access point controller card (APCC).

- *Appendix B: Addon Configuration*, provides information regarding the built-in addons that configure access point controller card (APCC) features.
- *Appendix C: Anti-Vandalism*, provides the information required to configure the anti-vandalism functionality.

## Differences From Prior Versions

TrafficDOT 2.10.3 differs from prior versions of TrafficDOT. For detailed information, refer to the *TrafficDOT 2.10.3 Release Notes*.



# Understanding TrafficDOT

This chapter describes the configuration, management, and monitoring functions of TrafficDOT 2.10.3.

## Overview

TrafficDOT 2.10.3 is an Adobe® Flex, Windows-based application that is used in conjunction with wireless vehicle detection systems from Sensys Networks, Inc. A Sensys Networks wireless vehicle detection network uses a collection of magnetic sensors embedded in roadway pavement to detect the presence and passage of vehicles such as cars, trucks, trains, motorcycles, bikes, and others. Detection events are transmitted by wireless radio to Sensys Networks access points that function as management nodes, data collection points, and packet forwarders for the network.

TrafficDOT is a configuration manager and monitoring tool for an access point and all its associated devices (sensors, repeaters, and contact closure cards). TrafficDOT 2.10.3 provides a graphical user interface (GUI) to the network's devices, settings, and operations. The GUI simplifies both configuration and management of installations.

TrafficDOT is independent of the firmware resident in sensors, access points, repeaters, and contact closure cards. As a result, it can be updated to a newer version without affecting any installed devices. However, it is typical for TrafficDOT versions to mirror the functionality of device firmware so it is common to update device firmware and TrafficDOT at the same time.

## Configuring Equipment With TrafficDOT

TrafficDOT uses industry standard TCP/IP communications and makes a connection to an access point in one of the following ways:

- *Connection via a wired network path* – for example, bench configuration prior to installation, field access based on patching a technician's laptop to the access point via an Ethernet cable, or an available wide area network connection.
- *Connection via a wireless network path* – for example, using GSM cellular networks (EDGE/GPRS data services) or CDMA cellular networks (1xRTT data services).

Configuration settings are made via TrafficDOT's GUI to the access point which, in turn, stores its settings in its local memory and transmits them to remote sensors and repeaters via the RF channel and to controller interface cards via the required cabling.

### Configuration Functions

Configuration of network equipment is accomplished with the following TrafficDOT functions:

- Configuring an access point
- Configuring sensors
- Configuring repeaters
- Configuring contact closure cards
- Configuring system properties
- Configuring settings for events, detection thresholds, reporting, etc.

### Management Functions

TrafficDOT contains other functions that are not related to configuration, such as network management. The management functions are as follows:

- Forming a network by associating devices (sensors, repeaters, and contact closure cards) to an access point
- Rebooting an access point
- Updating a sensor, access point, repeater, or contact closure card's firmware

---

**NOTE:**

TrafficDOT is independent of the firmware resident in sensors, access points, repeaters, and contact closure cards. As a result, it can be updated to a newer version without affecting any installed devices. However it is typical for TrafficDOT versions to mirror the functionality of device firmware, so it is common to update device firmware and TrafficDOT at the same time.

---

- Backing up and restoring an access point's configuration
- Reviewing the processes executing on an access point
- Updating an access point's license file
- Discovering access points available on the network
- Maintaining information about sensor location
- Producing online graphs of detection experience

**NOTE:**

Refer to *Chapter 5: Configuring and Managing Components* for additional information.

## Monitoring Detector Device Health and Performance

TrafficDOT provides a central monitoring station capable of evaluating the health and performance of up to 96 individual detector network devices. The following capabilities are available:

- *Graphical depiction of network health* – health of remote networks depicted by color-coded health-state icons
- *Radio communications status* – display of wireless signal strength (RSSI) and link quality (LQI) for all devices
- *Battery level* – effective battery output displayed for repeaters and sensors

## Remotely Managing Detector Networks and Device Properties

TrafficDOT allows access to detector network devices for configuration and testing without requiring a visit to the physical location of the network. The following capabilities are available:

- *Centrally manage all Sensys Networks devices* – contact access points by unique IP address, issue configuration/management commands. A VPN service allows connections to be made over GPRS, CDMA, Ethernet, or other backhaul channels.
- *Remote firmware updates* – update device firmware from remote location
- *Remote backup/restore operations* – backup/restore access point configuration from remote location
- *Process and license management* – stop/start local access point processes and update access point license from remote location

## Configuring Complex Deployments in Advance of Installation

TrafficDOT allows detector networks to be configured before devices are installed at the job site. This can improve communication between entities involved in the installation. Additionally, in cases where detection equipment is kitted in a staging or lab environment, the TrafficDOT configuration and the device settings can be synchronized using TrafficDOT import/export capability.

## **Troubleshooting Detection Network Behavior**

TrafficDOT automatically monitors all detector network devices communicating through managed access points, and provides a range of performance parameters—including wireless radio characteristics, device restarts, battery life, and others for which custom thresholds can be set. This allows TrafficDOT to provide value to almost any detection situation, while providing administrators a simple means to refine the device behavior profiles for their networks over time.

# Installing TrafficDOT

This chapter lists the hardware requirements for TrafficDOT 2.10.3 and provides steps for the application installation process.

## What's Required for Installation

TrafficDOT is installed via a custom script provided on the distribution media. The computer hosting TrafficDOT must contain a Windows operating system. Prior to installation, ensure you are running VDS 1.6.15 or higher and your configuration is compatible with TrafficDOT 1.10.2.

**NOTE:**

VDS release 2.10.4 is recommended for customers using TrafficDOT 2.10.3. The following table provides the version numbers displayed on TrafficDOT for each component from VDS release 1.4.5 to 1.8.6.

VDS Release	Access Points	VSN240-F Sensor	VSN240-T Sensor	Repeaters	Controller Cards
1.4.5	11	33.3.3	N/A*	33.1.7	33
1.4.7	11	35.3.3	N/A*	35.1.7	33
1.6.0	14	42.3.3	42.3.8	42.1.7	36
1.6.7a	15	47.3.3	47.3.8	47.1.7	39
1.6.8	17	49.3.3	49.3.8	49.1.7	40
1.6.13	19	53.3.3	53.3.8	53.1.7	40
1.6.15	21	53.3.3	53.3.8	53.1.7	40
1.8.0	22	64.3.3	64.3.8	64.1.7	42
1.8.1	24	65.3.3	65.3.8	65.1.7	42

VDS Release	Access Points	VSN240-F Sensor	VSN240-T Sensor	Repeaters	Controller Cards
1.8.2	25	65.3.3	65.3.8	65.1.7	42
1.8.3	25	65.3.3	65.3.8	65.1.7	N/A
1.8.4	25	N/A	N/A	N/A	N/A
1.8.5	25	N/A	N/A	N/A	N/A
1.8.6	25	N/A	N/A	N/A	N/A

Table 1. VDS 1.4.5 to 1.8.6 component version numbers

N/A - Product not shipped in this VDS release.

The following table provides the version numbers displayed on TrafficDOT for each system component from VDS releases 2.6.0 and 2.10.1:

VDS Release	Radio Version	VSN240-F Sensor	VSN240-T Sensor	Repeaters	μRadar	Controller Cards
2.6.0	14	N/A	N/A	N/A	87.6.14	44
2.6.1	17	76.3.3 76.5.3	76.3.8 76.5.8	N/A	97.6.14	45
2.6.2	N/A	79.5.3	79.5.8	N/A	100.6.14	N/A
2.6.3	19	N/A	N/A	73.2.7	112.10.14	N/A
2.6.4	N/A	92.3.3 95.5.3	92.3.8 95.5.8	76.2.7	113.6.14	N/A
2.10.0	25	105.3.3 105.5.3	105.3.8 105.5.8	86.1.7 86.2.7	123.6.14	N/A
2.10.1	29	114.3.3 114.5.3	114.3.8 114.5.8	93.1.7 93.2.7	130.6.14	47

Table 2. VDS 2.6.0 to 2.10.1 component version numbers

**NOTE:**

All magnetometer/MicroRadar sensor firmware versions are compatible with both AP/APCC (i.e., v1.8.x/v2.10.x).

## Hardware

The computer hosting TrafficDOT should meet the minimum requirements provided in the following table:

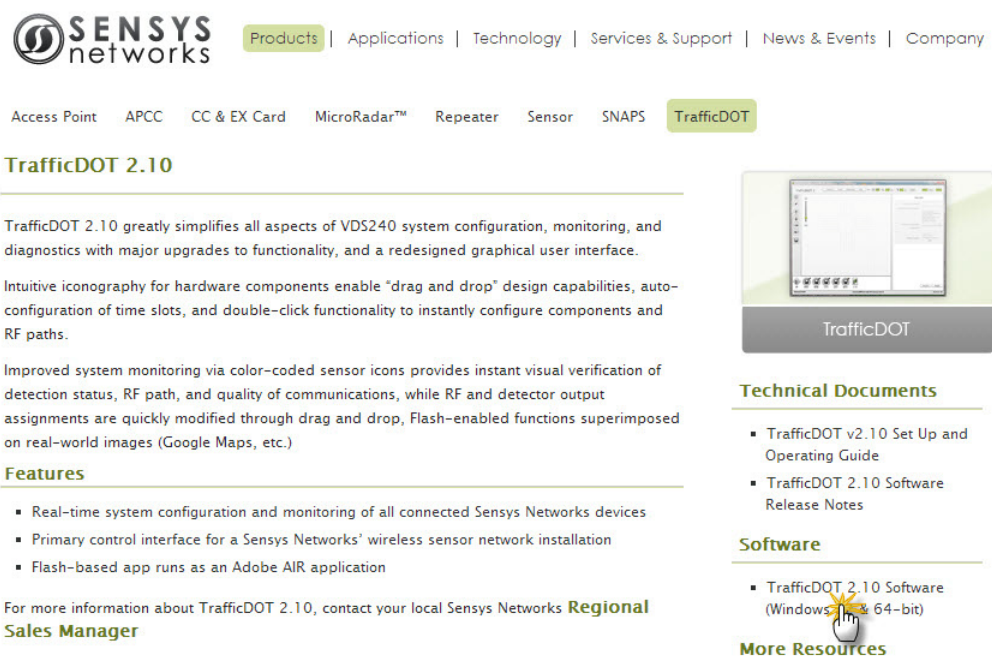
Component	Requirement
CPU	Intel® Pentium® III 1GHz or faster processor; Intel Pentium 4 2GHz or faster
RAM	1 GB recommended
HDD	1 GB (minimum)
Media	CD/DVD-ROM drive
Operating system	Microsoft® Windows® XP Professional or Windows 7 (including 64-bit editions)

Table 3. TrafficDOT minimum hardware requirements

## Installation Procedure

Use the following procedure to install TrafficDOT. The examples below are taken from an installation on a computer running Microsoft Windows 7.

1. Download the installation package from the Sensys Networks website (<http://www.sensysnetworks.com/products/trafficdot>).



**SENSYS networks** | Products | Applications | Technology | Services & Support | News & Events | Company

Access Point | APCC | CC & EX Card | MicroRadar™ | Repeater | Sensor | SNAPS | **TrafficDOT**

### TrafficDOT 2.10

TrafficDOT 2.10 greatly simplifies all aspects of VDS240 system configuration, monitoring, and diagnostics with major upgrades to functionality, and a redesigned graphical user interface.

Intuitive iconography for hardware components enable "drag and drop" design capabilities, auto-configuration of time slots, and double-click functionality to instantly configure components and RF paths.

Improved system monitoring via color-coded sensor icons provides instant visual verification of detection status, RF path, and quality of communications, while RF and detector output assignments are quickly modified through drag and drop, Flash-enabled functions superimposed on real-world images (Google Maps, etc.)

#### Features

- Real-time system configuration and monitoring of all connected Sensys Networks devices
- Primary control interface for a Sensys Networks' wireless sensor network installation
- Flash-based app runs as an Adobe AIR application

For more information about TrafficDOT 2.10, contact your local Sensys Networks **Regional Sales Manager**

#### Technical Documents

- TrafficDOT v2.10 Set Up and Operating Guide
- TrafficDOT 2.10 Software Release Notes

#### Software

- TrafficDOT 2.10 Software (Windows 7 & 64-bit)

**More Resources**

Figure 3.1. Download application

2. Navigate to **TrafficDOT2.exe** and double-click.
3. Click **Run**. The following *Installation Preferences* window displays.

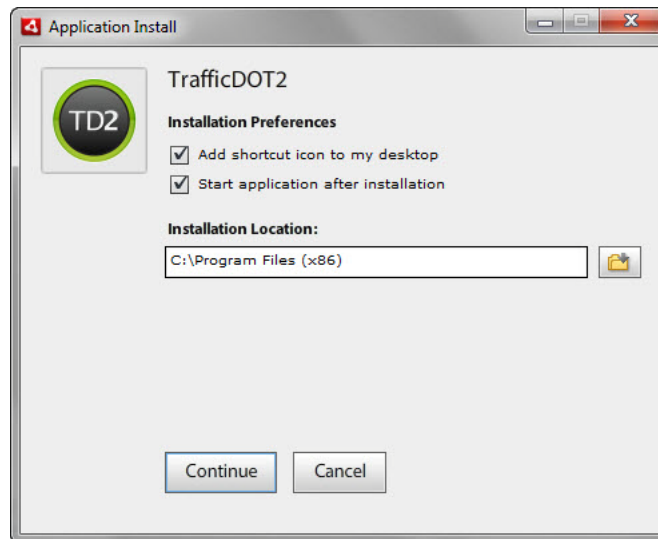


Figure 3.2. Selecting installation preferences

4. Click the checkboxes to select desired preferences.
5. Click **Continue** to accept the default installation location, or click the folder icon and follow the instructions to select another location for your TrafficDOT installation. The following installation window displays.

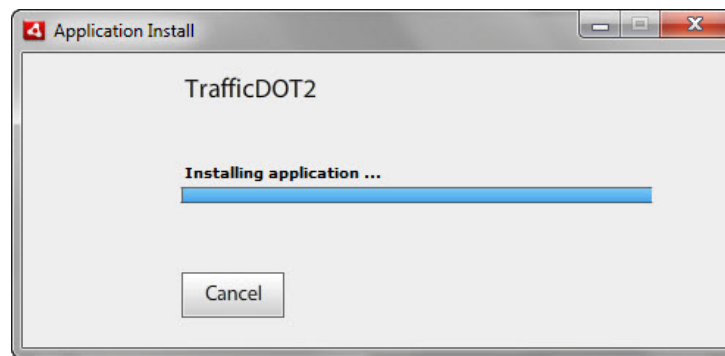


Figure 3.3. Installing application

If you selected the preferences shown in Figure 3.2, the *TrafficDOT 2 connection window* displays once the installation is complete.



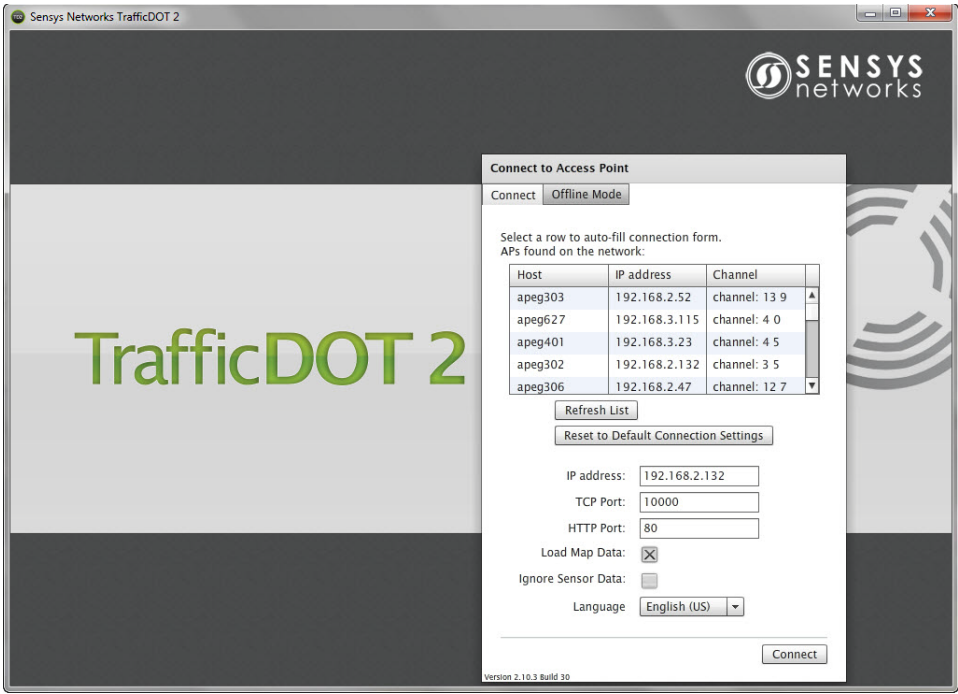


Figure 3.4. TrafficDOT 2 connection window



# Using TrafficDOT

This chapter provides an overview of creating a network of Sensys Networks VDS240 wireless vehicle detection components with TrafficDOT. It also provides an overview of the TrafficDOT map view window.

## Overview

TrafficDOT 2.10.3 provides a graphical user interface that enables you to create networks of Sensys Networks VDS240 wireless vehicle detection components. The user interface provides both a map and table view of the components. The map view provides a graphical representation of Sensys Networks key elements, which include sensors, access points, access point controller cards (APCC), SPP radios, repeaters, and contact closure cards.

### NOTE:

The table view provides similar functionality to the previous versions of TrafficDOT. For more information regarding the table view, refer to *Chapter 6: Monitoring Components Using the Table View*.

The map view allows you to:

- Drag and drop the elements in a graphical representation that approximate real-world deployment
- Draw an site layout using basic drawing tools
- Assign sensor zone directions
- Create map layers
- Adjust sensor zone widths and lengths
- Assign site names that appear in banner title
- Access all features from individual components

- Configure and monitor key components
- Select maps from a library of common application images or upload a map creation of your choice
- Assign sensor's primary application (e.g., *Count*, *MicroRadar*, *Speed*, *Stop Bar*, and *Travel Time*)

## TrafficDOT Map View

The following is a depiction of the TrafficDOT map view. The description of each callout is provided below the screen, and an example of how to use each component is provided later in the chapter.

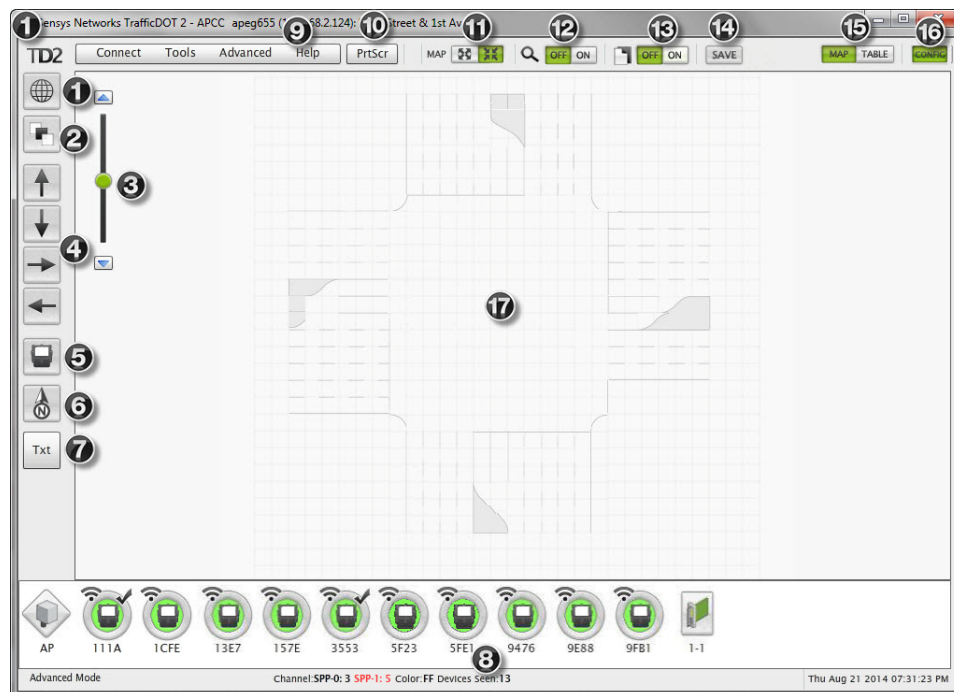


Figure 4.1. TrafficDOT map view

1. *Map Info and Image* – Displays both the *Site* panel.
2. *Map Layers* – Provides the ability to show or hide the following map layers:
  - Tool Tips
  - Controller Card Connections
  - RF Connections
  - Sensor Pairings
  - Controller Cards
  - Sensors, AP, Repeaters
  - Sensor Zones
  - Map Image

3. *Zoom In/Zoom Out* – Provides the ability to increase and decrease the map view.
4. *Sensor zone tools* – Provides the ability to create northbound, southbound, eastbound, and westbound sensor zones on the map image.
5. *Sensor* – Provides the ability to add sensors to a network.
6. *Compass* – Provides a directional arrow that can be dragged onto a map and rotated to align with the map's north direction.
7. *Text tool* – Provides the ability to create editable text such as titles, street names, landmarks, etc., on the map.
8. *Components tray* – Displays all the wireless vehicle detection components. The sensors images are color-coded. The colors (red, yellow, and green) indicate sensor status. When a detection is present the sensor color is black.
9. *Menu items* – The menus of the map and tables windows include:
  - *Connect* – Provides connect/disconnect operations.
  - *Tools* – Provides options for clearing sensors and repeaters from the components trays, clearing detection counts, scanning for devices, auto-assigning time slots, generating real-time detection charts and graphs, sending a command to multiple devices, clearing the dot table and the dot pair table, turning on SNC proxy logging, accessing the configure addons screen, viewing speed data, and setting system preferences.
  - *Advanced* – Allows you to set user mode. *Advanced Mode* allows for access to advanced device settings, and *Super User Mode* allows authentication for diagnostic mode access.
  - *Help* – Provides options to confirm the software version and access to user documentation.

**NOTE:**

For additional information regarding the menu items, refer to the *Menus* section in *Chapter 6: Monitoring Components Using the Table View*.

10. *PrtScr* – Enables you to save the current screen image.
11. *Map* – Enables you display a full map screen view without the tool bar or sensor tray.
12. *Discovery mode* – Enables you to turn discovery mode on and off. Discovery mode directs all network devices communicating with the access point to include additional information in the data packets they send. Discovery mode is required for utility operations, such as firmware updates and scanning for Sensys Networks equipment on RF channels other than the channel of the access point.
13. *Command log* – Toggles access to the command history log.
14. *Save* – Enables you to save all the items on your map and the dot and dot pair tables to an access point.

15. *Map/Table* – Enables you to toggle between the map and table views. The map and table windows provide a real-time view into the components of the network and the events they detect. All sensors in the network are shown, including sensors that communicate via repeaters.
16. *Config* – Shows or hides the configuration panel on the right side of the window. The configuration panel displays information about whatever item is selected on the map or in the table.
17. *Map image* – The map image is the main workspace of the TrafficDOT application.

## Using TrafficDOT to Create a Network

Creating a network using TrafficDOT consists of the following tasks:

- Connecting to an access point
- Entering site information
- Selecting a primary application (optional)
- Uploading a map image (optional)
- Creating sensor zones
- Adding sensors, access point(s), and controller cards to the map

## Connecting to an Access Point

Connecting to an access point can occur as (i) part of starting TrafficDOT or (ii) via the *Connect* menu on the *Main* window.

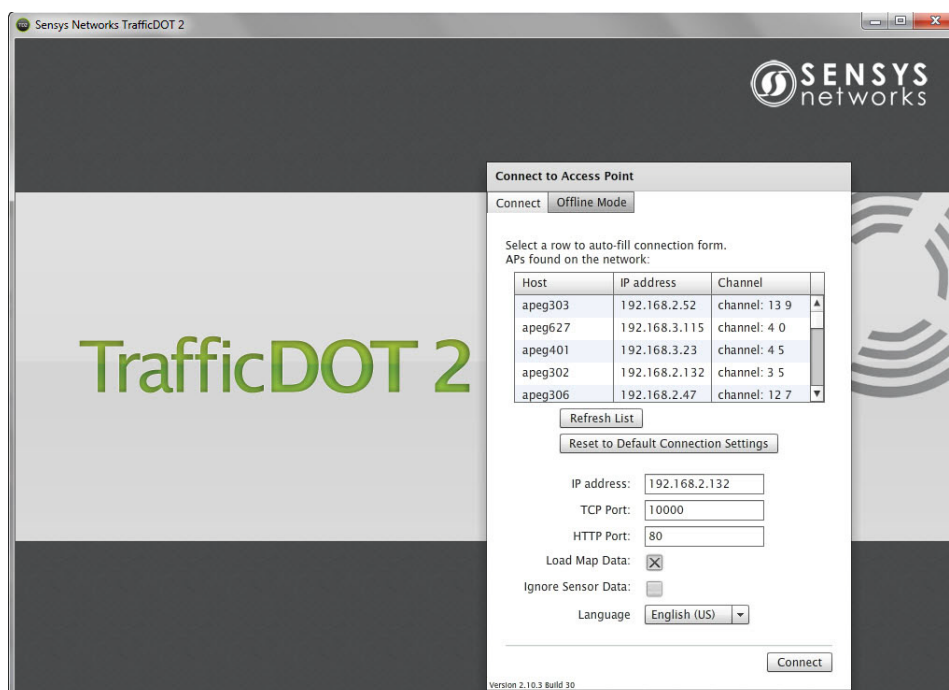


Figure 4.2. TrafficDOT 2 Connect window

## Connect Window Contents

The *Connect* window displays the access points available on the network, and collects data that identifies the access point to which TrafficDOT will connect. The window elements are shown in the following table:

Field Name	Description
IP Address	IP address of the access point or proxy server. DNS names are supported in environments where DNS services are available.
TCP Port	The TCP port number on which the connection is made. The default port number is 10000.
HTTP Port	The HTTP port number on which the connection is made. The default port number is 80.
Load Map Data	If unchecked, this option allows you to skip the loading of map data for situations where the data is stored locally and it is desirable to minimize the load time. If the option is checked, the preference is saved and persists through multiple launches of TrafficDOT.
Ignore Sensor Data	If checked, this option allows you to ignore sensor data for situations where the sensor is experiencing channel conflict issues. This allows you to access the <i>Access Point Configuration</i> window to resolve the issue.
Language	TrafficDOT supports drop-in internationalization. If the resource module for a supported language is installed, TrafficDOT will display that language in the UI. The supported languages are <i>French</i> , <i>German</i> , <i>Simplified Chinese (China)</i> , and <i>Traditional Chinese (Taiwan and others)</i> . The default TrafficDOT installation only supports English, so choosing another language will display the error <i>Chosen language does not have a translation file installed</i> .

Table 4. Connect window fields

Identify the access point you want to connect to by providing values in the *IP Address*, *TCP Port*, and *HTTP Port* fields.

### NOTE:

The *Connect* window displays the most recent use of TrafficDOT, so values may already appear in the window.

## Offline Mode Window Contents

The *Offline Mode* option enables users new to TrafficDOT to work with system components without an access point connection. This mode also enables installers to perform kitting prior to a new system installation. When using the *Offline Mode*, you can create sensor zones on map images, as well as create, configure, and position sensors and repeaters.

Unlike the *Connect* mode, where configuration data is saved to an access point, the contents created in the *Offline Mode* are saved to an offline directory on your hard drive and can be accessed during each connection. Multiple named configurations can be saved your computer for multiple access point configurations. The location of the offline directories is displayed in the *Offline Mode* panel.

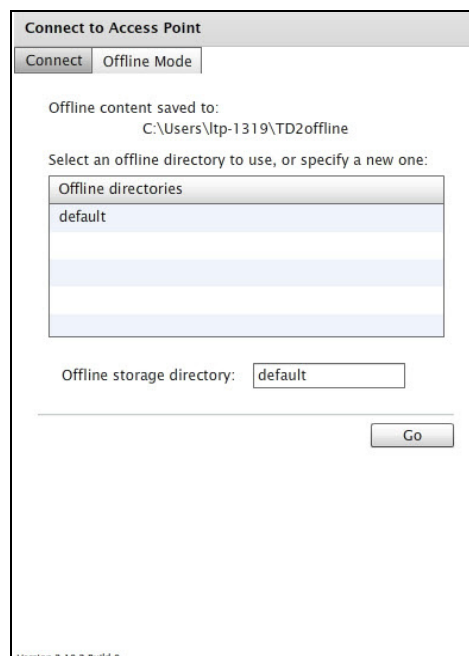


Figure 4.3. TrafficDOT 2 Offline Mode window

## Connecting at Start Up of TrafficDOT

Connect to the access point with TrafficDOT by performing the following steps:

1. On a Windows laptop or PC, start TrafficDOT by double-clicking its icon. TrafficDOT's *Main* window opens with the *Connect* window open in front of it.
2. Click **Connect**. The *Master Mode* window displays.



Figure 4.4. Master Mode window

3. Select the **SPP-O** checkbox, and then click **Turn On Selected** to enable master mode.



**NOTE:**

If this feature is disabled, the access point must be commanded to begin broadcasting. You will also receive a warning when the access point is rebooted. For additional information on enabling master mode, refer to the *Enabling Master Mode* section in the *Chapter 5: Configuring and Managing Components*.

## Connecting via the Connect menu

At anytime during a TrafficDOT session, you may connect to a different access point by disconnecting from the current access point by clicking **Disconnect** under the *Connect* menu.

## Site Panel

TrafficDOT provides a library of common application map images. When creating a new network of Sensys Networks VDS240 wireless vehicle detection components, the first step is to provide the information in the *Site* panel. The *Site* panel is the area where you enter the name and abbreviation of your mapped image, select a primary application and upload either a canned map image from the library or one of your own creation.

### Site Panel Contents

Elements for the *Site* panel are shown in the following table:

Field Name	Description
Name	The name of the site being monitored. This information also appears in the banner at the top of the TrafficDOT screen.
Abbreviation	The site abbreviation name of the site being monitored. The site abbreviation should be a version of the site name using seven characters or fewer.
Image File	The name of the image file currently in use.
Upload New Map/ Upload Current Map	Provides access to the library of map images and allows you to upload a canned image or one of your own creation.
Image Opacity	Determines how transparently the map image appears. The higher the opacity, the less transparent the image will be. This feature can be useful to fade a map image so your attention can focus on the sensors and other network elements.
Enable SAMS	If checked, enables SAMS functionality, which allows you to configure site geometry in order to create movement counts. For additional information, refer to the <i>Safety and Mobility System (SAMS) Quick Start Guide</i> .

Table 5. Site panel elements

## Entering Site Information

Enter site information by performing the following steps:

1. Enter an site name in the *Name* field.
2. Enter an abbreviation of the site name in the *Abbreviation* field.

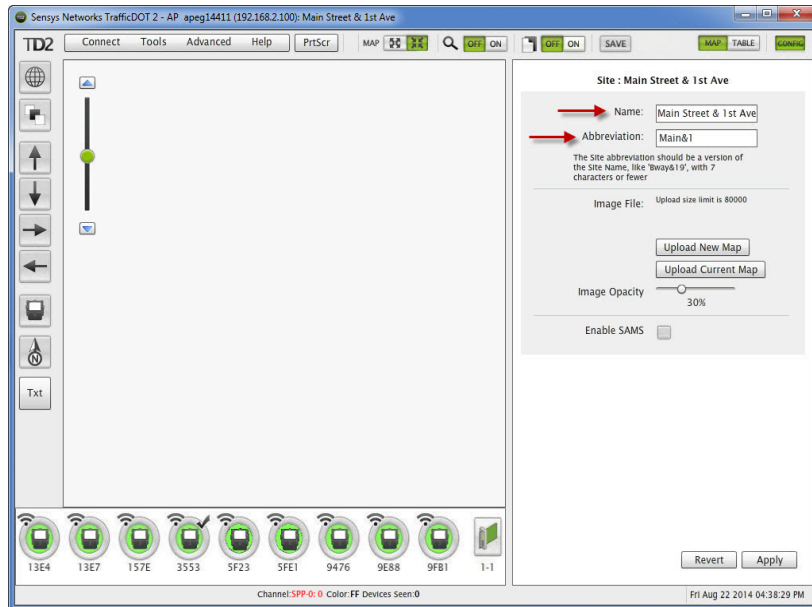


Figure 4.5. Entering site and abbreviation name

### NOTE:

The yellow background in the *Site* panel indicates an unsaved configuration. You cannot move on to another operation until you apply the information to the panel.

3. Click **Apply** to accept configuration changes or **Revert** to discard the changes.

### NOTE:

*Apply* accepts changes to the configuration. To save the changes to the access point, you must click the **SAVE** button at the top of the window.

## Uploading a Map Image

Upload an image map by performing the following steps:

1. Click **Upload New Map** to open the master template directory.

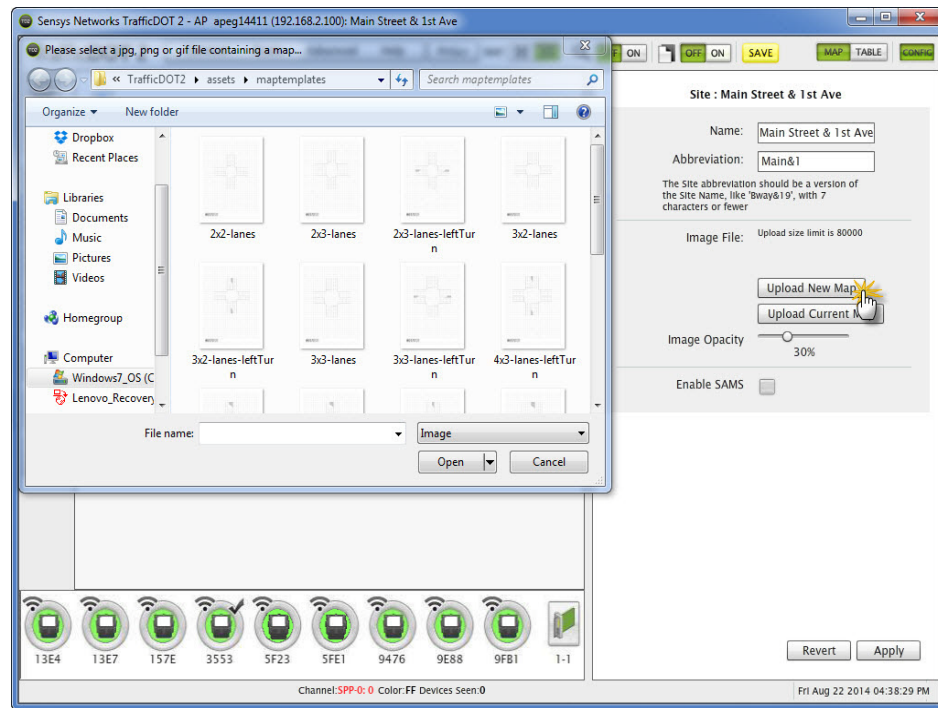


Figure 4.6. Selecting map image

### NOTE:

You can select the **Upload Current Map** button to upload a map you are sending to the access point without selecting a new map image from the map folder.

2. Select an image applicable to the primary application. For example, if you selected *Stop Bar*, you could select the *2x2-lanes.png* map image.

### NOTE:

You can also upload your own custom map image. The maximum map image file size is 80,000 bytes. TrafficDOT accepts .jpg, .png, and .gif image files.

3. Click **Open**. The map image displays in TrafficDOT.

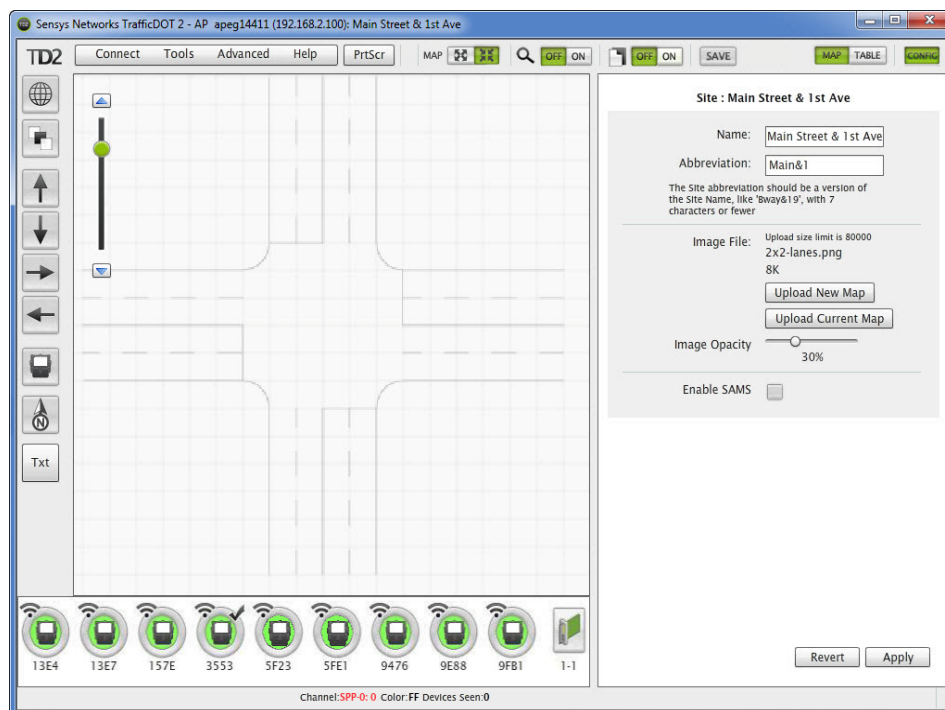


Figure 4.7. Unsaved map image

4. Click **Apply** to accept configuration changes.

**NOTE:**

*Apply* accepts changes to the configuration. To save the changes to the access point, you must click the **SAVE** button at the top of the window.

## Creating Sensor Zones

TrafficDOT provides drawing tools that allow you to create northbound, southbound, eastbound, and westbound sensor zones on your image map. Once you select a sensor zone direction, and drag and drop it onto your map image the *Sensor Zone* panel displays, which is the area where you configure the sensor zone(s) to be monitored.

### Sensor Zone Panel Contents

Elements for the *Sensor Zone* panel are shown in the following table:

Field Name	Description
Sensor Zones in Dot Table	The drop-down contains all the sensor zones defined in the dot table that are not on the map. You can choose one of these values for the sensor zone abbreviation.
Name	The name of the sensor zone being monitored.
Type	The type of sensor zone application being create. When configuring a sensor zone, you can select <i>Count</i> , <i>MicroRadar</i> , <i>Speed</i> , <i>Stop Bar</i> , and <i>Travel Time</i> .

Table 6. Sensor zone panel elements

## Creating a Sensor Zone

To create a sensor zone, perform the following steps:

1. Select one of the four sensor zone icons, and drag and drop the sensor zone in the location of your choice on the image map.

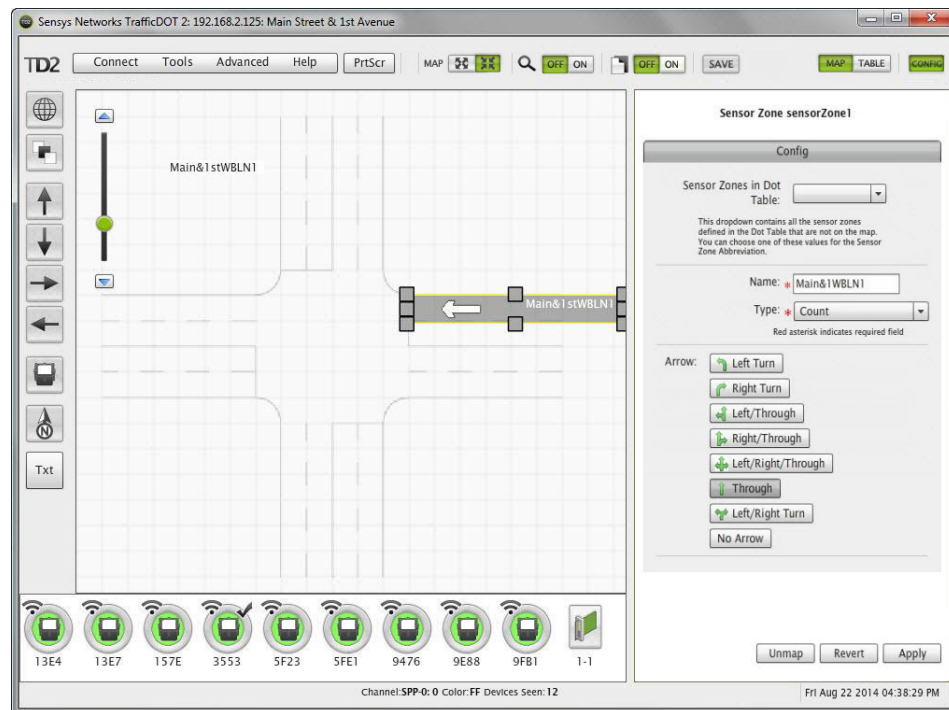


Figure 4.8. Creating a sensor zone

2. Use the handles to resize the sensor zone to your specifications.

You can also use the rotate handle to cause the sensor zone to rotate. This is useful when working with a map image where the sensor zones are at an angle.

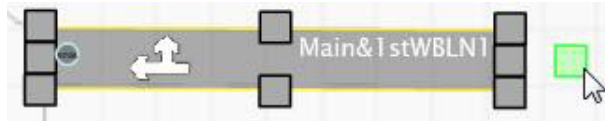


Figure 4.9. Sensor zone rotation handle

3. Enter a name for the sensor zone. (*Optional*)

Sensor zone names are created automatically, but they can be customized. The first sensor zone created is *sensorZone1*. Sensor zone names update by an increment of one for each sensor zone created (e.g., *sensorZone1*, *sensorZone2*, *sensorZone3*, etc.).

**NOTE:**

If you are working from an existing dot table, select an existing sensor zone name for the drop-down list. Also, selecting an existing sensor zone overwrites the *Abbreviation*.

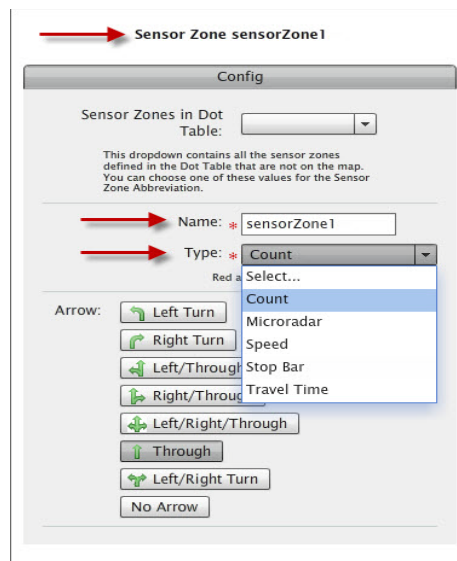


Figure 4.10. Configuring a sensor zone

4. Select the **Type** for the sensor zone. The available application types are *Count*, *MicroRadar*, *Speed*, *Stop Bar*, and *Travel Time*.
5. Select an arrow configuration to signify whether the sensor zone is: *Left Turn*, *Left Turn/Through*, *Left Turn/Right/Through*, *Left/Right Turn*, *Right Turn*, *Right Turn/Through*, *Through*, and *No Arrow*. (*Optional*)
6. Click **Apply** to accept configuration changes.

**NOTE:**

Repeat steps 1-6 to create multiple sensor zones.

## Adding Key Components

Once you have configured your sensor zone(s), add your active Sensys Networks wireless detection components. All active components are available in the component tray. With the exception of sensors, you can drag and drop the graphical representation of the components anywhere you like on the map. Sensors must be placed on the sensor zones.

## Dragging a Sensor onto a Sensor Zone

To drag a sensor onto a sensor zone, perform the following steps:

1. Left-click on the sensor icon on the left side of the screen.

### NOTE:

You can also select a sensor from the sensor tray. If you are configuring an site online, you would more than likely select a sensor from the sensor tray, and if you are configuring an site offline, your would more than likely select a sensor by clicking the sensor icon.

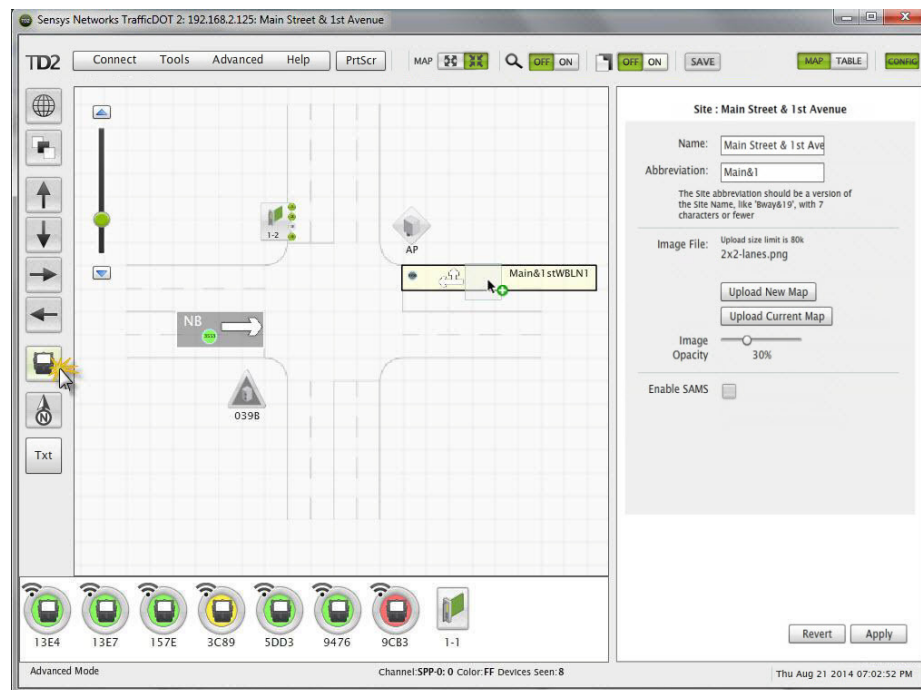


Figure 4.11. Dragging a sensor onto a sensor zone

2. Hold down the mouse button and drag the sensor image over the sensor zone.
3. Release the mouse button to place the sensor on the sensor zone.

**NOTE:**

If you change your mind about the sensor's placement, click **Delete** to remove it from the map and configuration. Sensors selected from sensor tray will reappear in the tray at the bottom of the map.

4. Provide a *Dot ID* for the sensor.

Figure 4.12. Assigning Dot ID

**NOTE:**

If you select a sensor by clicking the sensor icon, you do not need to provide a Dot ID.

5. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

**NOTE:**

You can also add additional sensors and other key components by dragging them from the component tray.

## Device Health Indicator

The colors in the map and table view, and in the component tray, visually represent the overall health of the device. Hovering the mouse over a configured sensor (either on the map or in the sensor tray) displays a tooltip with additional information about the sensor.



The colors represented in the following tables are applicable to all of the key network components.

Color	State	Description
Green	OK	RF communications are healthy; devices are operating normally.
Yellow	Monitor	RF communications are sub-standard. Monitor the situation because in many cases this is transient; no specific end-user action is called for.
Red	Take Action	RF communications have ceased. In most cases there is a problem with the device or its configuration that requires end-user intervention. Investigate and resolve the issue.
Gray	Inactive	The sensor is configured in the dot table, but is not currently detected.
Purple	Downloading	The sensor is in the process of downloading firmware.

Table 7. Device health indicators








Icon	Description
	Packet transmission within watchdog cycle
	MicroRadar sensor with package transmission
	Packet transmission and dot table entry
	Pending (configured with minimum attributes, but not in dot table)
	State is <i>Present</i> (detecting)
	Packet transmission but other parameters beyond threshold
	Packet transmission lost during current TrafficDOT session

Table 8. Active device legend



# Configuring and Managing Components

This chapter provides information about configuring the components of the Sensys Networks VDS240 wireless vehicle detection system.

Separate sections describe the configuration procedures for sensors, access points, contact closure cards, and repeaters. In addition, this chapter contains sections describing other TrafficDOT functions useful in managing networks.

## Overview

All configuration activities are performed with TrafficDOT. With TrafficDOT, a connection is made to an access point, from which all further configuration activity ensues. TrafficDOT supports configuration of access points, repeaters, sensors, and contact closure cards—whether or not they are already installed in the field. Thus, components can easily be added to existing installations.

Configuration of a network involves (i) coordinating the radio frequency settings of all devices in the network to achieve high quality communications over a sustained period, and (ii) selecting the event detection and reporting parameters necessary to achieve sensing performance that is optimal for the end user application.

Configuration settings for all Sensys Networks equipment are stored in local, non-volatile flash memory. The access point has the greatest number of settings and serves as the central authority for the settings used by network devices. Sensors inherit most, but not all of their settings from the access point to which they are associated. Repeaters have few settings beyond their RF channels.

Most configuration activity occurs at the time of network design and installation. Many customers find that once the network has been installed and its performance validated, no further configuration is necessary.

## Configuring VSN240 Wireless Sensors

Sensys Networks VSN240 magnetometer sensors ship with a factory default configuration for count applications. Most installations require changes to the default configuration to meet site-specific needs. However, once set, a sensor's configuration typically requires no further changes.

This section describes configuring sensors with TrafficDOT and provides information about the following activities:

- Selecting sensors to configure
- Setting a sensor's operating mode
- Assigning a sensor's time slot
- Setting sensor's RF channel
- Sending a recalibration command to a sensor
- Using advanced settings
- Updating sensor firmware

### Introduction

Sensor configuration involves dragging a sensor onto a lane on the map image or selecting a sensor from the sensor tray, and then selecting values for the following sensor parameters:

- Operating mode
- Radio frequency channel
- Transmission time slot

Other operations related to sensor management are also performed from the *Sensor Position* window.

### Selecting Sensors

Configuration and management commands can be applied to one, several or all of the sensors in a network. You must select the sensors to configure.

### Selecting Parameters

You must select the parameters to be configured. This allows you to update all, some or a single parameter at a time.

Changes are applied immediately and subject to the time slot and transmit interval of your SNP network. It may take up to 30 seconds for changes to be reflected in TrafficDOT's display.

### Working with the Sensor Configuration Window

The *Sensor Configuration* window consists of five tabs: *Position*, *Card Addresses*, *Adv*, *Cmds*, and *Pairing*. To select a sensor for configuration, click on a sensor on your image map. The *Sensor Configuration* window displays.

Figure 5.1. Sensor Configuration window

## Position Window Contents

The *Position* window consists of the following elements:

Elements	Description
Enabled	The field determines whether APSTAT and other Sensys Networks applications will include the sensor being configured in its configuration.
Dot ID	The factory assigned hardware device identifier. This displays the least significant 16 bits as a 4-character HEX string.
Dot ID 64	The factory assigned hardware device identifier. This displays all 64 bits as a 16-character HEX string.
Version	The firmware version on the device. (Note: use the VDS Release Notes from Sensys Networks to cross references firmware version IDs to VDS releases.)
Name	The name of the sensor. You can name the sensor any 8-character name that makes sense for your application.(Optional)
Description	Description of the sensor location and use. (Optional)
Horizontal Position	Sensor's horizontal position relative to other sensors in the same lane. Values may be -3, -2, -1, 0, 1, 2 or 3 where -3 indicates the far-left sensor; -2 indicates the mid-left sensor; -1 indicates the left; 0 indicates the center sensor; 1 indicates the right sensor; 2 indicates the mid-right, and 3 indicates the far-right sensor.

Elements	Description
Vertical Position	Sensor's vertical position relative to other sensors in the same lane. This element is used to identify sensor speed pairs. Values may be 0, 1, or 2 where 0 indicates the lead sensor, 1 indicates a trailing sensor, and 2 indicates a second trailing sensor.
Sensor Zone	The field is populated automatically using the lane abbreviation.

Table 9. Position window elements

## Setting a Sensor's Position

After providing a name and description of the sensor, select the position of the sensor. Enable the *Horizontal Position* by selecting a value of Far-Left (-3), Mid-Left (-2), Left (-1), Center (0), Right (1), Mid-Right (2), or Far-Right (3). Or, enable the *Vertical Position* by selection the value of Lead(0), Trail(1), or Trail(2).

### NOTE:

If you enable the horizontal position, you must disable the vertical position and vice versa. The horizontal position is used for Travel Time, while vertical position is used for the other applications.

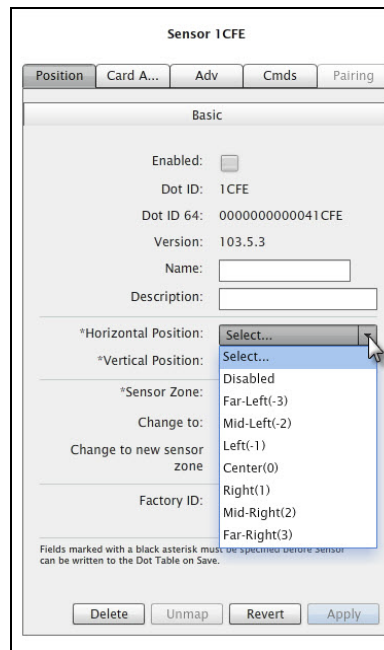


Figure 5.2. Selecting horizontal position

## Configuring Card Addresses

The sensor-to-contact closure channel mappings are stored in a sensor database that resides on the access point. The four channels represent independent contact closures which, in turn, are actuated by the vehicle detection events transmitted by a defined group of wireless sensors. Each sensor may be associated with up to four *Card Address / Channel combinations*.

Up to 15 wireless sensors can be associated with the same card/channel, in which case the sensors are logically *OR-ed* together—meaning that if any sensor on the channel detects a vehicle, the corresponding contact closes.

### Card Addresses Window Contents

The *Card Addresses* window consists of the following configurable elements:

Element	Description
Extension (milliseconds)	This entry extends the duration of a contact closure on a per-sensor basis. (Optional)
Delay (milliseconds)	This entry delays the duration of contact closure on a per-sensor basis. (Optional)
Shelf and Slot	The shelf number-slot number is a card address associated with the Sensys Networks contact closure card or expansion card.
Channel	Card address channel. The channel is between 1 and 4.

Table 10. Card Addresses window elements

### Mapping Sensors to Contact Closures

To map sensors to contact closure cards, perform the following steps:

1. Select a sensor from the image map.
2. Click the **Card Address** tab to open the *Card Addresses* window.

#### NOTE:

You can also access the *Card Addresses* window by dragging a sensor icon onto an available card channel icon on the map.

Sensor 1 CFE

Position Card A... Adv Cmds Pairing

Extension (milliseconds):

Delay (milliseconds):

Card Address 1:  
Shelf:  Slot:  Channel:

Card Address 2:  
Shelf:  Slot:  Channel:

Card Address 3:  
Shelf:  Slot:  Channel:

Card Address 4:  
Shelf:  Slot:  Channel:

Figure 5.3. Card Addresses window

3. Select a **Shelf** number, a **Slot** number, and a **Channel** from the drop-down lists.

**NOTE:**

The **C** button clears the data in these rows.

4. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

**NOTE:**

To assign a sensor to multiple controller channels, supply entries to the additional *Card Addresses* areas.

## Configuring Advanced Settings

In certain situations, the performance of a sensor's magnetic detectors may be impeded by sources of electro-magnetic energy in the local environment such as power lines, trains, or other sources. Advanced sensor settings can be used to mitigate the noise introduced by such sources. In order to change any values in the *Advanced Settings* window, you need to be in *Advanced Mode*.



To set *Advanced Mode*:

1. Click the **Advanced** menu item at the top of the screen.
2. Select **Set Advanced Mode**.

**NOTE:**

This mode will be enabled for your future sessions until you choose to cancel it.

## Advanced Settings Window Contents

The *Advanced Settings* window consists of the following configurable elements:

Element	Description
Linear Filter	<p>Applying a linear filter has the effect of eliminating high-frequency energy in the waveform; this filter is particularly beneficial when installations are impacted by 60Hz energy produced by power lines.</p> <p>Two filter options are available that differ by the number of samples taken. Use <i>Filter3</i> (three samples) for freeway sites and <i>Filter4</i> (four samples) for arterials. This element can be enabled independently of other advanced settings.</p>
Axis Detection	<p>The axes of detection can be limited via this element. Options include the default combination (Z and X axes), or any of the X, Y, and Z axes used by themselves.</p> <p>This property is particularly useful when installations are impacted by magnetic radiation sources that are significant and effect a particular axis. This element can be enabled independently of other advanced settings.</p>
Reorder Axes	<p>This element is a binary switch that directs a sensor to perform a one-time change or orientation of its axes. It is particularly useful when installations are impacted by a static energy source significant enough to saturate an detector's axis.</p>
Color Codes (hex 01 - FF)	<p>The color code option allows the allocation of any of 255 possible codes to a vehicle detection system, thus making it possible for multiple signals to be carried over the same RF channel. The default is FF.</p>

Element	Description
Change Time Slot To	<p>This option allows the user to change the sensor's time slot and is the value displayed on the <i>Position</i> window. Each sensor uses only one time slot to communicate with its access point or repeater. TrafficDOT assists in enforcing proper time slot usage by filtering the drop-down list of available time slots.</p> <p><i>Note:</i> This entry is for manual adjustments to time slot for individual sensors. It is recommended that you use the <i>Auto-assign All</i> option to set all sensor time slots.</p>

Table 11. Advanced Settings window elements

To configure advanced sensor settings, perform the following steps:

1. Click the **Adv** tab to open the *Advanced Settings* window.

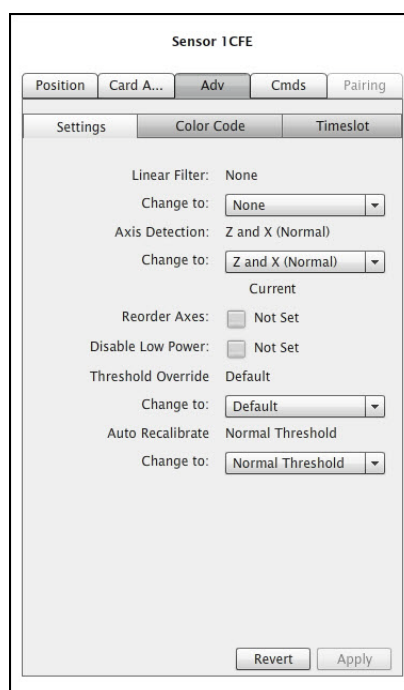


Figure 5.4. Advanced Settings window

2. Choose the required values from the drop-down lists.
3. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

To configure color codes, perform the following steps:

1. From the *Advanced Settings* window, click the **Color Code** tab.

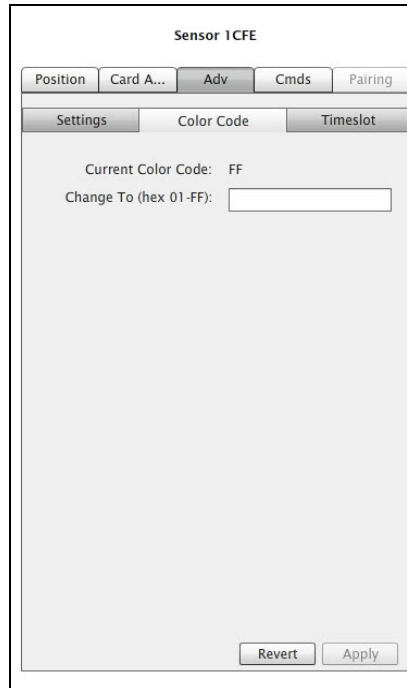


Figure 5.5. Color Code window

2. Enter a color code value in the *Change To (hex 01-FF)* field.

**NOTE:**

The default is FF.

3. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

To configure time slots, perform the following steps:

1. From the *Advanced Settings* window, click the **Timeslots** tab.

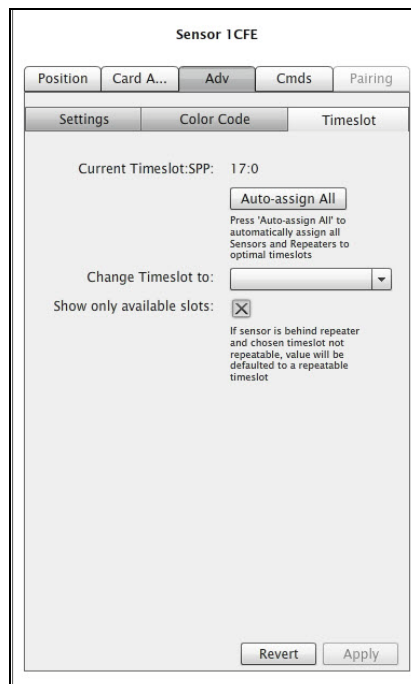


Figure 5.6. Timeslots window

2. Choose the required value from the drop-down list.

**NOTE:**

This entry is for manual adjustments to time slot for individual sensors. It is recommended that you use the *Auto-assign All* option to set all sensor time slots.

3. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Configuring Commands to Sensor

TrafficDOT's *Cmds* window includes other operations related to managing sensors including:

- Setting sensor's RF channel
- Changing sensor operating mode
- Performing a soft reset
- Performing a hard reset
- Downloading sensor firmware
- Recalibrating a sensor
- Setting a sensor ID

**IMPORTANT!**

These operations are not common, therefore screen element descriptions are not provided. Perform the following operations only when directed by Sensys Networks.

To configure the command to sensor settings, click the **Cmnds** tab to open the *Command to Sensor* window.

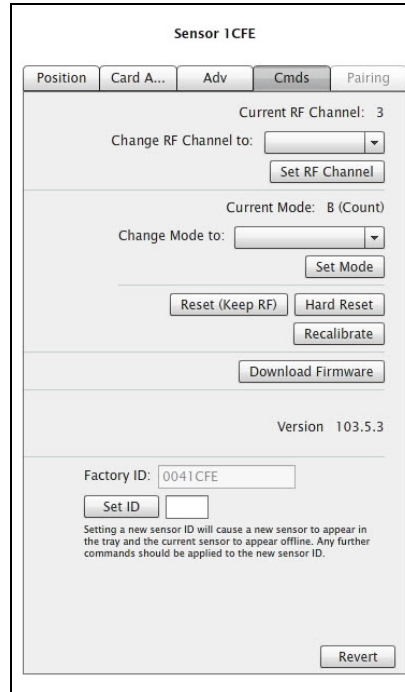


Figure 5.7. Command to Sensor window

## Setting a Sensor's RF Channel

All sensors associated with an access point must use the same RF channel as the access point; all sensors associated with a repeater must use the same frequency designated as the downstream channel on that repeater.

To set the RF channel, perform the following steps:

1. Select the **Change RF Channel** to drop-down list. The 16 RF channels available for use display.
2. Select an entry from the list by clicking it.

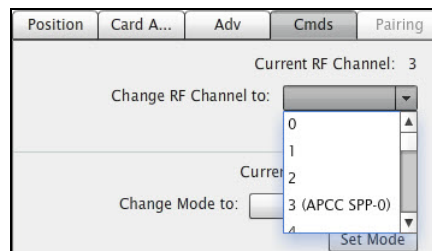


Figure 5.8. Changing RF channel

If you set the RF channel to one that is not used by the access point or any repeater, the sensor is no longer seen and communication to it is lost.

3. Click **Set RF Channel** to save configuration. The current channel displays in the *Current RF Channel* field. The default is zero.

## Setting a Sensor's Operating Mode

The sensor's operating mode defines the type of detection data it transmits.

To set the operating mode, perform the following steps:

1. Select the **Change Mode to** drop-down list. The operating modes available for sensors display.
2. Select an entry from the list by clicking it.

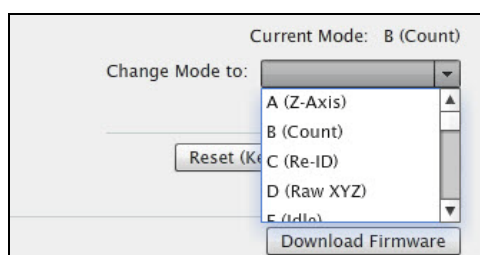


Figure 5.9. Setting operation mode

For typical detection scenarios use *Count (B)* or one of the Stop Bar modes; *Idle (E)* mode may also be useful for pre-installation kitting activities.

Other modes are available to support more specialized situations such as arterial travel time measurement, interfacing to specific devices, or field work by authorized Sensys Networks technicians. Additionally, in some rare cases, measurement of the local magnetic field (using the reserved mode D) may be requested by Sensys Networks. Always check with Sensys Networks if you are unsure about which mode to specify.

### NOTE:

Only model VSN240-F sensors support count mode; although TrafficDOT may appear to allow setting the mode of other sensors to count mode, the command fails.

3. Click **Set Mode**.

## Performing a Soft Reset

On occasion, a sensor may need to be reset without changing its RF communication parameters. This may occur as a result of a firmware download that was interrupted, an unexpected magnetic event in the local area or other reason. To perform a soft reset, select the sensor and click the **Reset (Keep RF)** button.

## Performing a Hard Reset

A sensor may need to be reset back to its factory default configuration. This operation resets the sensor's RF channel assignment to channel zero.

Reconfiguration may be required in order for the sensor to communicate with the network's access point. To perform a hard reset, select the sensor and click the **Hard Reset** button.

## Downloading Sensor Firmware

Updates to sensor firmware are sent from the access point via the wireless communication channel.

---

**NOTE:**

Sensor firmware updates must occur independent of repeater or access point firmware updates.

---

Firmware updates become operational immediately and can be reversed only by performing the firmware update procedure specifying a prior version of the appropriate firmware image. It is not necessary to reconfigure sensors after updating their firmware, although in many cases, new firmware enables additional device functionality that may require initial configuration. To download sensor firmware, select the sensor and click the **Download Firmware** button.

---

**NOTE:**

Refer to *Configuring Command Settings* for information on starting the access point broadcasting firmware.

---

## Recalibrating a Sensor

Sensors operate by evaluating changes in the local magnetic field. They establish a reference value known as a baseline to which detected changes are compared.

Setting the baseline is called recalibration and occurs automatically. On occasion, you may want to recalibrate a sensor. To recalibrate a sensor, select the sensor and click the **Recalibrate** button.

## Setting a Sensor IDs

Individual sensors can be renamed by assigning them a user-defined identifier. This identifier serves as an alias for the device in lieu of its factory assigned identifier.

Renaming sensors can be useful in situations where a sensor must be replaced and the original sensor's event history must be preserved. Renaming the replacement sensor with the device identifier of the original associates the event history to the new device.

### Considerations for Setting Sensor IDs

Consider the following when setting sensor IDs to user-defined strings:

- User assigned sensor IDs must be four characters in length and may consist only of hexadecimal characters. Spaces and special characters are not allowed.
- The Sensor ID tool operates only on sensors whose VDS firmware version is release 1.8 or above. Update sensors to this release level or above before attempting to set their device identifiers.
- The Sensor ID tool allows multiple sensors to be aliased to the same ID, although only one of them will appear in the TrafficDOT *Main* window. A window displays a warning of this outcome when appropriate.
- In the event the firmware of a sensor that has already been aliased is downgraded to a VDS release earlier than VDS 1.8.0, the user-defined id is discarded and the device id reverts to its factory assigned value. (VDS versions prior to release 1.8.0 do not support user-defined identifiers.)
- To set a sensor's ID, select the sensor. Type a new device identifier string into the *Current Factory ID* and click the **Set ID** button.

---

**NOTE:**

The string must be four characters in length and may consist only of hexadecimal characters.

---

### Pairing Sensors

The *Pairing* window provides the ability to create and display sensor pairs (also known as dot pairs) in TrafficDOT. Sensor pairs provide additional detection information such as speed, length, gap, etc. This information can only be derived by knowing the relative distance between two sensors sharing the same sensor zone location.



**Sensors 4145, 2809**

Position Card A... Adv Cmds **Pairing**

This pairing is in the DotPair table.  
To update this pairing in the DotPair Table hit Apply.

Enabled: ☒ This field determines whether APSTAT will include this Dot Pair in its calculations.

Trailing Sensor:

Leading Sensor:

Sensor Separation (mm):

Vehicle Length Correction (mm):

Delete Revert Apply

Figure 5.10. Pairing window

## Pairing Window Contents

The *Pairing* window consists of the following elements:

Element	Description
Enabled	This checkbox determines whether APSTAT will include this Dot Pair in its calculations.
Trailing Sensor	The factory assigned hardware device identifier of a following sensor. This column displays as a 4-character HEX string.
Leading Sensor	The factory assigned hardware device identifier of a leading sensor. This column displays as a 4-character HEX string.d.
Sensor Separation (mm)	The distance between the leading and trailing sensor in millimeters. You must enter a value from 1 to 32767.
Vehicle Length Correction (mm)	This is an optional correctional value from -3000 to 3000.

Table 12. Pairing window elements

## Configuring MicroRadar Sensors

The MicroRadar sensor, which was designed to look like the VSN240 wireless magnetometer sensor, is capable of detecting bicycles and vehicles. Configuring MicroRadar sensors is very similar to configuring magnetometer sensors; however, additional configuration settings provided on the *Adv*, *Cmds*, and *Card Addresses* configuration panels are required.

This section describes configuring MicroRadar sensors with TrafficDOT and provides information about the following activities:

- Configuring sensor's detection distance
- Configuring sensor's autobaseline value
- Setting sensor's operating mode
- Mapping sensor to contact closure card

### Working in the Advanced Settings Window for MicroRadar Sensors

The *Advanced Settings* window for the MicroRadar sensor enables configuration of the sensor's detection distance and autobaseline. The additional operations in the *Advanced Settings* window are not common, and the default settings are appropriate for most situations. Alter these setting only when directed.

**NOTE:**

To access the elements in the *Adv* window, select **Set Advanced Mode** from *Advanced* menu option.

### Recommended Advanced Settings

The recommended *Adv* settings for bicycle detection and count are:

- **Alternate Sample Rate** - Enabled
- **Detection Distance** - 6 Ft or 10 Ft depending on the width of the bicycle lane. Detection distance varies based on application and lane dimensions.
- **Autobaseline** - 5 min
- **Autobaseline Sensitivity** - 0

### Configuring Detection Distance

MicroRadar sensors have a programmable detection range between 4 feet and 10 feet. The width of a detection zone is approximately 90 degrees and the default range is 6 feet. To configure the *Detection Distance* for MicroRadar sensors, perform the following steps:

1. Click the **Adv** tab to open the *Advanced Settings* window.

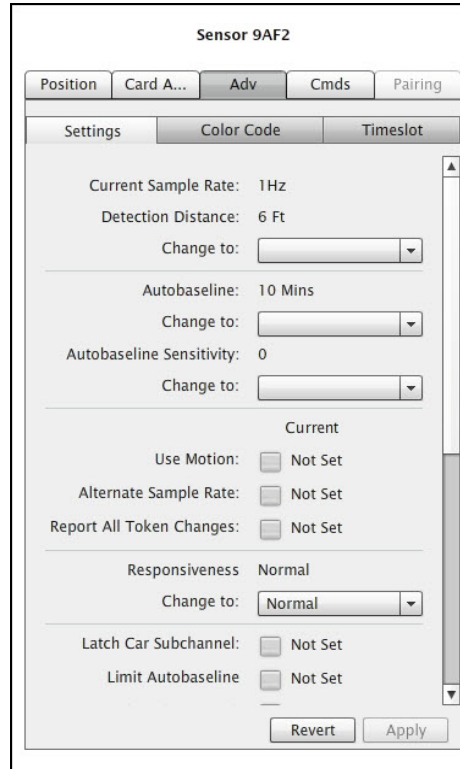


Figure 5.11. MicroRadar Advanced Settings window

2. Select the **Detection Distance Change to** drop-down list. The available programmable ranges are:
  - 6 Ft (default)
  - 10 Ft
  - 4 Ft
  - 8 Ft
3. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Configuring Autobaseline

Environmental anomalies can make it difficult to determine a one-time baseline. The autobaseline is an adaptive detection baseline that can be configured to update continuously. To configure the *Autobaseline* for MicroRadar sensors, perform the following steps:

1. Click the **Adv** tab to open the *Advanced Settings* window. Refer to Figure 5.11.
2. Select the **Autobaseline Change to** drop-down list. The autobaseline values available for sensors display. The available values are:
  - 3 Mins
  - 5 Mins (Default)

- 10 Mins
  - Manual
3. Select **0-7** from the *Change to* drop-down list to set the *Autobaseline Sensitivity*. The default is **0**.
  4. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Working in the Commands to MicroRadar Sensor Window

The *Cmds* window is used to set the mode for MicroRadar sensors. The additional operations in the *Cmds* window are not common, and the default settings are appropriate for most situations. Alter these setting only when directed.

### Setting a MicroRadar Sensor's Operating Mode

The MicroRadar sensor's operating mode defines the type of detection data it transmits. To set the operating mode, perform the following steps:

1. Click the **Cmds** tab to open the *Command to Sensor* window.



Sensor 9AF2

Position Card A... Adv **Cmds** Pairing

Current RF Channel: 3

Change RF Channel to:

Current Mode: µA (Detect)

Change Mode to:

☐

Version 123.6.14

Factory ID:

Setting a new sensor ID will cause a new sensor to appear in the tray and the current sensor to appear offline. Any further commands should be applied to the new sensor ID.

Figure 5.12. MicroRadar Command to Sensor window

2. Select the **Change to** drop-down list. The operating modes available for the sensor display. The available MicroRadar sensor modes are:

- $\mu A$  (*Detect*)
- $\mu B$  (*IF Display*)
- $\mu C$  (*Debug*)
- $\mu D$  (*Parking*)
- $\mu E$  (*Idle*)

*MicroRadar A* is for normal street operation and is the mode used for bicycle and vehicle detection. The other modes, such as *MicroRadar B* and *MicroRadar C* are used for debugging firmware; *MicroRadar D* is used for parking applications, and *MicroRadar E* is an idle mode.

3. Select a mode from the list by clicking it.
4. Click **Set Mode**.

After TrafficDOT has received a packet of information from the sensor identifying it as a MicroRadar sensor, the MicroRadar sensors appear in both the tray and on the map with a  $\mu$  symbol.

## Working with the Card Addresses Window

The *Card Addresses* window is used to map MicroRadar sensors to contact closure cards. The *Card Addresses* window contains three sub-channel tabs:

- *Any*, which detects all vehicles
- *Car*, which detects large vehicles, such as cars and trucks
- *Bicycle*, which detects all bicycles (including stationary bicycles)

Each MicroRadar sub-channel can be assigned up to four card addresses. Detection information for these tabs display in the *Present* column in the table view of TrafficDOT. Refer to *Chapter 6: Monitoring Components Using the Table View*.

## Mapping MicroRadar Sensors to Contact Closures

To map sensors to contact closure cards, perform the following steps:

1. Select a MicroRadar sensor from the image map.
2. Click the **Card Addresses** tab to open the *Card Addresses* window.

Figure 5.13. MicroRadar Card Addresses window

3. Select either **Any**, **Car** or **Bicycle**.

**IMPORTANT!**

When assigning a MicroRadar sensor *Bicycle* detection sub-channel to a card address, **do not** add a millisecond delay. Refer to the *VSN240-M MicroRadar™ Sensor Installation Quick Start Guide (Count)* for additional information.

**IMPORTANT!**

When assigning a MicroRadar sensor *Bicycle* sub-channel for presence detection on shared lanes with differentiation to a card address, it is recommended that at least a 1000 millisecond delay be added. Refer to the *VSN240-M MicroRadar™ Sensor Installation Quick Start Guide (Presence)* for additional information.

4. Select a **Shelf** number, a **Slot** number, and a **Channel** from the drop-down lists.

**NOTE:**

The **C** button clears the data in that row.

5. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

To assign a MicroRadar sensor to multiple controller channels, supply entries to the additional *Card Addresses* areas.

## Configuring Access Points

This section describes configuring and working with access points via TrafficDOT. The following activities are discussed:

- Retrieving an access point's configuration
- Configuring RF settings
- Configuring event parameters
- Configuring detection settings
- Inspecting the access point ID and firmware version
- Setting system preferences
- Working with advanced properties
- Saving the configuration

### Introduction

Access point configuration involves dragging an access point onto the map image or selecting the access point icon in the sensor tray, and then defining behavior and tolerances for the entire network. The configuration is implemented through a set of property collections. The collections group similar or related properties together; each collection is discussed in the sections that follow.

The property collections for access point and network configuration are as follows:

- RF communications
- Event thresholds
- Detection sensitivities

Access points ship with a default configuration suitable for a wide variety of situations. Using defaults reduces the amount of custom configuration and ensures that all critical elements have values assigned to them.

Other operations performed with TrafficDOT related to access point and network management are also discussed in this section.

### Working with the Access Point Configuration Window

Before you can configure an access point, a connection to it must be established. Make a connection as described in *Chapter 4: Connecting to an Access Point*.

To select an access point for configuration, click on an access point on your image map. The *Access Point Configuration* window displays. The *Access Point Configuration* window consists of four main tabs: *AP Config*, *System Config*, *Pairings*, and *Command Line*, and six sub-tabs: *Info*, *Radio*, *Event*, *Detection*, *Advanced*, and *Cmds*.

Since the *Access Point Configuration* window contains a number of elements that are not configurable, tables with window element descriptions are not provided; however, all configurable elements are described in the upcoming sections.

**NOTE:**

To access the *Advanced* window, you must select **Set Advanced User** from the *Tools* menu, and to access the *Command Line* window, you must select **Set Super User** from the *Tools* menu and provide a password.

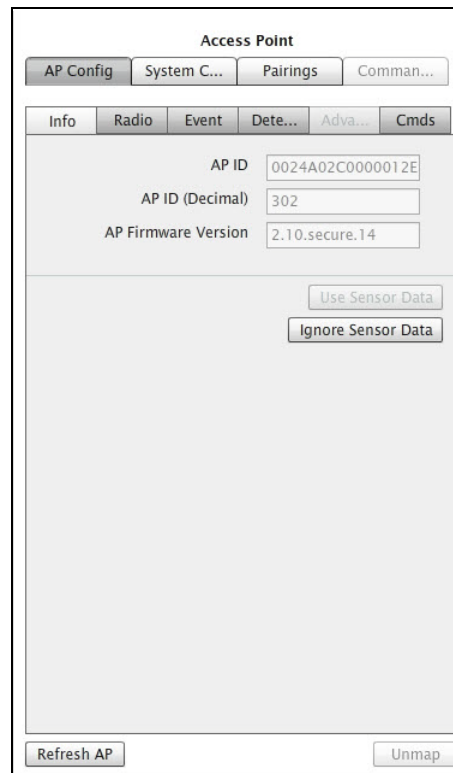


Figure 5.14. Access Point Configuration window

## Viewing the Access Point ID and Firmware Version

The unique factory assigned access point ID and version of the access point's firmware can be reviewed on the *Info* tab as shown in Figure 5.14. The *AP ID* is expressed as a 16-character HEX string and as a decimal number; these elements are for reference only.

## Configuring Radio Settings

The radio frequency channel of the access point defines the frequency channel for the entire network. Each device that communicates with the access point must be configured to use the same RF channel.



The *Radio* window has the following configurable elements:

- Set Master Mode to
- RF Channel
- PA Attenuation
- Rx Sensitivity
- Minimum Rx RSSI
- Baud Rate

The screenshot shows the 'Access Point' configuration window with the 'Radio' tab selected. The window is divided into two sections: 'SPP-0' and 'SPP-1'. The 'SPP-1' section is active, showing the following configuration options:

- Radio ID: 123456FE000030C
- Radio Version: 25
- Current Master Mode: Master
- Set Master Mode to: (dropdown menu)
- RF Channel: 3
- LNA Gain: 0 dB
- PA Max Power: 0 dBm
- PA Attenuation: 0 dB
- Rx Sensitivity: Nominal
- Minimum Rx RSSI: None
- 120 Ohm Termination Off: ☒
- Base 64 Packet On: ☒
- Global Synchronization On: ☒
- Baud Rate: 460800

At the bottom of the window are four buttons: 'Refresh AP', 'Unmap', 'Revert', and 'Apply'.

Figure 5.15. Radio window

**NOTE:**

The APCC has two radios, so there are two radio tabs: *SPP-0* and *SPP-1*. Each radio is configured separately.

## Enabling Master Mode

*Master Mode* directs access points to commence broadcasting as soon as they receive power. If this feature is disabled, the access point must be explicitly commanded to begin broadcasting. To enable this feature, select **Master** from the drop-down list, and click **Apply**. To disable this feature, select **Command** from the drop-down list.

**NOTE:**

If you disable the feature, you will receive a warning when the access point is rebooted.

---

## Setting the RF Channel

To configure the RF channel, perform the following steps:

1. The entries in the *RF Channel* drop-down list correspond to the 16 channels available for use. Select an entry from the list by clicking it. The factory default channel is zero.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Setting the PA Attenuation

The entries in the *PA Attenuation* drop-down list provide a range of limiting values expressed in db. To configure the power amplifier attenuation, perform the following steps:

1. Select an entry from the list by clicking it.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

**NOTE:**

Reducing the performance of the power amplifier is not a common requirement. Leave the setting at the factory default of zero unless directed otherwise by Sensys Networks.

---

## Configuring Event Parameters

*Event* reporting pertains to the act of sensors transmitting detection data to the access point. *Event* reporting parameters are global attributes, stored in the access point's configuration, that dictate how event reporting occurs on a given network.

The *Event* window has the following configurable elements:

- Transmit Interval
- Maximum Reporting Latency
- Synchronized Reporting
- Watchdog Timeout
- N Events / Near Full
- Extra Latency
- Report Only 'ON' Events
- Enable Magnetometer for uRadar

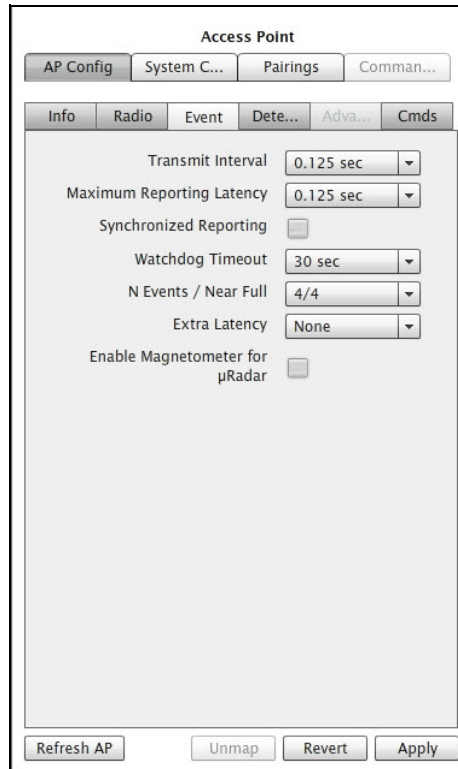


Figure 5.16. Event window

## Setting the Transmit Interval

The transmit interval sets the frame size for the network and, in so doing, dictates the number of time slots available for device transmissions. To set the transmit interval, perform the following steps:

1. The entries in the *Transmit Interval* drop-down list are the available frame sizes for SNP networks. Select an entry from the list by clicking it. The factory default is 0.125 sec.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Setting the Maximum Reporting Latency

The *Maximum Reporting Latency* is the maximum amount of time that may pass between successive transmissions from a given sensor. To set the maximum reporting latency, perform the following steps:

1. The entries in the *Maximum Reporting Latency* drop-down list are the available reporting latencies. Select an entry from the list by clicking it.

**NOTE:**

The factory default is 0.125 sec; however, when configuring *Maximum Reporting Latency* for count stations, a setting of 1 to 5 seconds is recommended.

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Enabling Synchronized Reporting

The *Synchronized Reporting* attribute globally enables (or disables) transmission of data by sensors on a fixed clock basis. When enabled, all sensors report their data (subject to their respective time slots) as of a fixed interval equal to *Maximum Reporting Latency* (or multiple thereof) relative to the network's system clock maintained by the access point.

1. To enable *Synchronized Reporting*, select the checkbox. To disable the function (the default setting), clear the checkbox.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Setting a Watchdog Timeout

The *Watchdog Timeout* attribute specifies a number of seconds of inactivity a sensor will wait before transmitting a packet. To set a *Watchdog Timeout*, perform the following steps:

1. The entries in the *Watchdog Timeout* drop-down list are the available timeout intervals. Select an entry from the list by clicking it. The factory default is 30 seconds.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Configuring Event Reporting Buffer Controls (N Events / Near Full)

These parameters set the buffer in the sensors and two global attributes that govern the event queue monitoring process. The attributes are as follows:

- *N Events* – the maximum number of events that may be queued.
- *Near Full* – the maximum number of events that may be queued before the queue is flushed by transmitting a packet.

To set event reporting buffer controls, perform the following steps:

1. The entries in the N Events/Near Full drop-down list are the available combinations of maximum event reports and reporting trigger points. Select an entry from the list by clicking it.

**NOTE:**

The factory default is 4/4; however, when configuring *N Events / Near Full* for count stations, a setting of 16/12 is recommended.

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Configuring Extra Latency

Additional latency may be required in environments there are a lot of RF channels and the access point interfaces with a traffic signal controller. Extra latency allows for the recreation of the timing transmission. To configure *Extra Latency*, perform the following steps:

1. The entries in the *Extra Latency* drop-down list are the available latency increments. Select an entry from the list by clicking it. The factory default is None.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Limiting Reporting to On (Detection) Events Only

This attribute globally enables (or disables) a constraint on the nature of the data reported for a detection. Enabling this attribute results in reporting only the rising edge of a detection pulse.

1. To enable this feature, select the checkbox. To disable the feature (the default setting), clear the checkbox.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Enabling the Magnetometer Sensor for MicroRadar

This attribute globally enables (or disables) the ability for a MicroRadar sensor to perform as a magnetometer sensor.

1. To enable this feature, select the checkbox. To disable the feature (the default setting), clear the checkbox.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Configuring Detection Settings

Vehicles are detected by inference. Sensors continuously monitor the X, Y, and Z axes of the earth's magnetic field. When no vehicles are present, a sensor calibrates itself by measuring the values of the background magnetic field and establishing a reference value. The passage and presence of vehicles are detected by measuring the magnitude of deviations from that value.

The *Detections* window has the following configurable elements:

- Onset Filter
- Detect Z Threshold
- Undetect Z Threshold
- Undetect X Threshold
- Holdover
- Swap X/Y
- Stop Bar Recalibrate Timeout
- Count Recalibrate Timeout
- International Mode
- Disable Auto Re-baseline

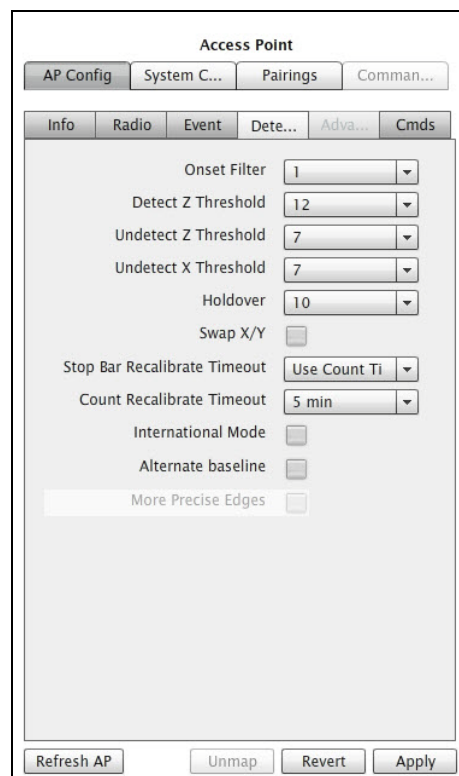


Figure 5.17. Detection window

## Setting the Onset Filter

The *Onset Filter* specifies the number of consecutive samples for which the ON condition must be true before a detection event is true. To set this attribute, perform the following steps:

1. The entries in the *Onset Filter* drop-down list are the available number of consecutive samples. Select an entry from the list by clicking it. The factory default is 1.

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Setting Thresholds for Detection and Undetection

*Thresholds* specify the magnitude of change from a sensor's reference value (representing its current estimate of the local background magnetic field) necessary to declare a detect or undetect event. There are three threshold attributes.

### Detect Z Threshold

Detection events are declared when the local magnetic field deviates from the baseline reference value by more than this threshold. The default value is 12.

### Undetect Z Threshold, Undetect X Threshold

Undetect events are declared when the local magnetic field deviates from the baseline reference value by this threshold or less. The default value is 7. To set the threshold attributes, perform the following steps for each of the two elements:

1. The entries in the threshold drop-down lists are the available threshold values. Select an entry from the list by clicking it.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Setting the Holdover Attribute

Holdover specifies the number of consecutive samples for which the ON condition for both the X and Z magnetic axes are no longer true before an OFF event is declared. To set this attribute, perform the following steps:

1. The entries in the *Holdover* drop-down list are the available number of consecutive samples. Select an entry from the list by clicking it. The factory default is 10.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Enabling a Swap of the X and Y Measurements

This property logically swaps the readings from the X and Y magnetic axes. (This is not common.)

1. To enable this feature, select the Swap X/Y checkbox. To disable it (the default setting), clear the Swap X/Y checkbox.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Setting the Recalibrate Timeouts

The *Recalibrate Timeout* is an optional parameter that specifies a duration such that, if an ON condition is true for a period greater than the timeout duration, the sensor is recalibrated. There are two recalibrate timeouts—one for stop bar applications and another for count applications.

### Setting the Stop Bar Recalibration Timeout

This setting applies to all sensors operating in any of the stop bar operating modes. To set the timeout, perform the following steps:

1. The entries in the drop-down list are the available recalibration timeouts. Select an entry from the list by clicking it.

---

**NOTE:**

The factory default is *Use Count Timeout* which means that the timeout value for the element *Count Recalibrate Timeout* is used.

---

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Setting the Count Recalibrate Timeout

This setting applies to all sensors operating in the count operating mode. To set the timeout, perform the following steps:

1. The entries in the drop-down list are the available recalibrate timeouts. Select an entry from the list by clicking it. The factory default is Off.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Enabling International Mode

The *International Mode* attribute is related to the recalibrate timeout elements described above. This element dictates which set of timeout values are available for selection from the *Count Recalibrate Timeout* drop-down list.

Clear the checkbox for installations in North America. Select the checkbox for installations outside of North America that require the recalibrate timeout feature.

---

**NOTE:**

Changing the *International Mode* setting will change the assigned recalibrate timeout values.

---

## Selecting Disable Auto Re-baseline

This property disables a sensor's mode of operation so that it does not detect other objects when in a stalled state.



1. To enable this feature, select the **Disable Auto Re-baseline** checkbox. To disable it (the default setting), clear the **Disable Auto Re-baseline** checkbox.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

## Configuring Advanced Settings

The *Advanced Settings* window enables the configuration of advanced properties. Advanced properties dictate system behavior that is considered default in the sense that Sensys Networks recommends it in almost all cases. These elements allow tuning of the system behavior.

The screenshot shows the 'Access Point' configuration window with the 'Advanced' tab selected. The settings are as follows:

Setting	Value/State
Retransmit RSSI/LQI	<input checked="" type="checkbox"/>
Rewrite Packet	<input checked="" type="checkbox"/>
Expect Acks	<input checked="" type="checkbox"/>
CC Fixed Latency	0
Reverse CC Polarity	<input type="checkbox"/>
AP Color Code	FF

Buttons at the bottom: Refresh AP, Unmap, Revert, Apply.

Figure 5.18. Advanced Settings window

### Enabling Retransmission of RSSI and LQI

*Retransmit RSSI/LQI* tells repeaters to append the RSSI and LQI measurements of the messages received from sensors to the packets forwarded to the access point. To enable this feature, select the checkbox. To disable the feature, clear the checkbox. The default is checked.

### Enabling Packet Rewriting

*Rewrite Packet* instructs the access point to replace its measures for RSSI and LQI (which relate to message from the repeater) with the RSSI and LQI values the repeater has appended to its messages (as they represent an assessment of the

sensor to repeater RF communications.) To enable this feature, select the checkbox. To disable the feature, clear the checkbox. The default is checked.

### **Enabling Expectation of Acknowledgments**

*Expect Acks* directs sensors to report detection events as they occur and to expect acknowledgment packets from the access point. To enable this feature, select the checkbox. To disable the feature, clear the checkbox. The default is checked.

### **Entering Contact Closure Card Latency and Enabling Reverse Polarity**

A fixed amount of latency can be applied to all signals sent to a traffic controller via a contact closure card. Additionally, the polarity of a contact closure card can be reversed. The default is leaving *CC Fixed Latency: 0* and *Reverse CC: Polarity* unchecked. Consult with Sensys Networks before using these features.

### **Assigning an Access Point Color Code**

The *Color Code* option allows the assignment any of 255 possible codes to an access point, thus making it possible for multiple signals to be carried over the same RF channel. To assign an access point color code, type in a value between hex 01 and FF. The default is FF.

## **Configuring Command Settings**

The *Commands* window enables the configuration of command properties by providing the following functions:

- Rebooting and running the access point
- Saving access point data to flash memory
- Updating access point firmware
- Refreshing access point configuration
- Choosing an SPP to use for broadcast
- Starting and stopping the broadcast of SPP firmware
- Starting and stopping the broadcast of sensor/repeater firmware
- Upgrading CC/EX firmware
- Exporting and importing dot tables
- Exporting and importing dot pair tables

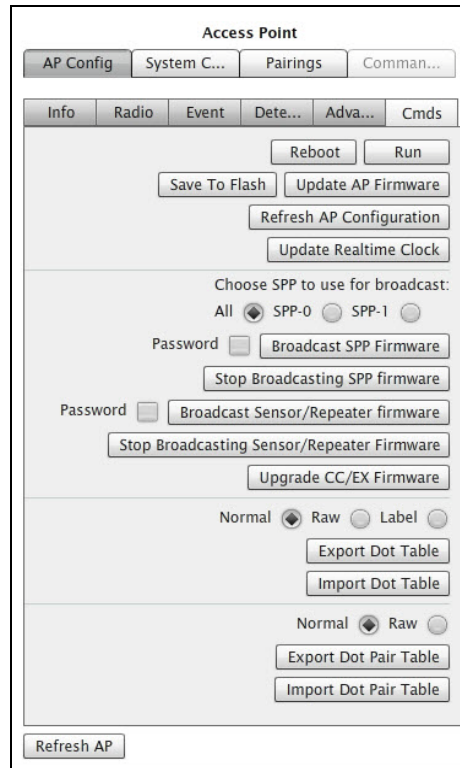


Figure 5.19. Cnds window

To perform any of functions provided in the *Cnds* window, click the desired task button and follow the on screen instructions.

Click **Refresh AP** to accept configuration changes.

## Configuring System Configuration Settings

*System Configuration* parameters are external properties of the network, and the elements communicate with other networks and systems. *System Configuration* parameters are grouped into the following collections:

- Network properties
- PTP (point-to-point) properties
- Modem properties
- Push settings
- Poll settings
- Memory management properties
- Other properties
- Command properties

## Configuring with Network Settings

*Network* properties define the settings necessary to conduct IP communications with the access point including IP address, network mask, gateway and hosts providing DHCP, DNS, and time services.

Figure 5.20. Network window

### Setting the IP Mode

*IP Mode* specifies how the access point will receive its IP address such as via DHCP (the system default), a cellular ISP or other means. Click an entry from the drop-down list to select it.

#### NOTE:

The *Modem* option displays only when the *IP Mode* element is set to *Modem*. For additional modem information, refer to *Appendix A: Configuring Cellular Modems on an AP or an APCC*.

### Setting the Ethernet Mode

*Ethernet Mode* designates the estimated bandwidth of the network link between the management station and the access point that operates on the access point's Ethernet interface. Click an entry from the drop-down list to select it.

## Specifying the Network Mask

*Network Mask* identifies the local portion of a local area network (LAN), and in so doing, identifies which hosts are communicated to through gateways. The system default is 255.255.255.0.

Type in a network mask only if the specified IP mode is static or if instructed by a service provider.

## Specifying the IP Address

*IP Address* is a unique network address for IP communications to and from the access point over the Ethernet port. Type an IP address for the access point only if the specified IP mode is static or if instructed by a service provider.

## Designating the Gateway

*Gateway* identifies by IP address a network node to which the access point directs traffic destined for external networks. Type an IP address of a gateway server only if the specified IP mode is static or if instructed by a service provider.

## Designating the DNS Servers

*DNS* identifies by IP address a network node providing domain name services to the access point. Type an IP address of a DNS server only if the specified IP mode is static or if instructed by a service provider.

## Designating the DHCP Monitor Host

*DHCP Monitor Host* identifies by IP address a network node used by the access point to evaluate its connection to a host providing *Dynamic Host Control Protocol* services. Typically, the device used as the monitoring host is the DHCP server itself.

## Specifying the Network Time Sources

*NTP Servers* specifies by hostname(s) a minimum of one server providing the current time via NTP (Network Time Protocol), a draft Internet standard for computer clock synchronization (see RFC1305). Type a minimum of one NTP host that provides network time services.

## Configuring PTP Settings

*PTP* characteristics define the settings necessary to establish a virtual private network connection between the access point and an external server such as a management (SNAPS) server from Sensys Networks.

The PTP communication model is required in situations where the access point is positioned behind a firewall or router performing NAT (network address translation) services, receives its IP address via dynamic assignment, or is managed over a cellular packet data network.

The screenshot shows the 'Access Point' configuration window. At the top, there are four tabs: 'AP Config', 'System C...', 'Pairings', and 'Comman...'. Below these is a row of sub-tabs: 'Net', 'Poi...', 'Push', 'Poll', 'Me...', 'Other', and 'Cmds'. The main area contains the following fields:

- SNAPS**: An empty text input field.
- PTP Mode**: A dropdown menu with 'PTP' selected.
- PTP User**: A text input field containing 'apeg331'.
- PTP Password**: A text input field with asterisks (\*\*\*\*\*).
- PPP Monitor Host**: A text input field containing '192.168.3.254'.

At the bottom of the window, there are three buttons: 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.21. PTP window

## Specifying the Sensys Networks Management Server

*SNAPS* identifies the host that acts as the PTP server. Type the host name or IP address of the management server.

### NOTE:

This is an optional component.

## Selecting the PTP Mode

*PTP Mode* specifies the protocol used for creating the PTP connection. Click an entry from the drop-down list to select it.

## Defining the PTP User and Password

Some PTPs require a user ID and password for authentication and access to the PTP. These elements capture the values if they are required. Type a user ID and password string adhering to the formatting rules of the PTP provider.

## Specifying the Host to Monitor for PTP Communications

*PPP Monitor Host* names the host used by the access point to maintain the PTP connection. If the access point cannot contact this host for a duration of one minute or more, it drops the PTP connection and attempts to reconnect. Typically, this entry points to the PTP server itself. Type a host name or IP address.

## Configuring Push Settings

A common requirement of event data statistics is the need to transfer it to other hosts or platforms. A typical technique to do this is referred to as push.

*Push* refers to movement of processed sensor data (i.e., statistical data) from one host to another initiated by the statistical server (typically an access point). This section describes the settings used by an access point's push process.

### NOTE:

Use of this feature requires an appropriate license.

The screenshot shows the 'Access Point' configuration window with the 'Push' tab selected. The '1st Destination Server' section contains the following fields and options:

- 1st Destination Server:** 192.168.3.205
- Destination Port (required):** 14002
- Buffer Reports:** ☐
- Stay Connected:** ☐
- Use Acknowledged Message Passing:** ☐
- 1st Acknowledgement Timeout (s):** (empty field)

Below this section is the '2nd Destination Server' section with an 'Other' label. At the bottom of the window are three buttons: 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.22. Push window (1st Destination Server)

## Destination servers

The hosts that act as the recipients of pushed data are referred to as destination servers. A destination server is a host that is equipped to receive processed sensor data for display, analysis or other purpose. Access points, when hosting the processes to generate statistical data from raw sensor reports, support up to two destination servers. At least one destination server must be designated; the second is optional.

### 1st Destination Server

Designates the target host by IP address or DNS name.

---

**NOTE:**

At least one entry is required in situations where the access point processes the raw sensor data.

---

### Destination Port

The port number of the target server that the push process uses to communicate with it.

### Buffer Reports

Designates the behavior of the access point in regard to how disconnections between the access point and the target host are handled.

### Stay Connected

Designates the behavior of the access point in regard the status of the TCP connection during the idle time between separate pushes of the data from the access point to the destination servers.

### Use Acknowledged Message Passing

Directs the behavior of the access point in regard to messages from the destination server that acknowledge receipt of the data transfers.

### Acknowledgment Timeout

Specifies the number of seconds the push process waits for an acknowledgment packet from the destination host before declaring a transmission failure and retransmitting. An acknowledgment timeout value is available for each destination host.



The screenshot shows the 'Access Point' configuration window with the 'Push' tab selected. The 'Other' section contains the following settings:

- 1st Destination Server: (empty)
- 2nd Destination Server: (empty)
- Other: (empty)
- Individual Speed Mode: All cars (dropdown)
- Units: Imperial (dropdown)
- Individual Car Reports: Standard (dropdown)
- Report Interval: 30 sec (dropdown)
- Maximum File Size: 1000 (text input)
- Average Speed: ☒ (checkbox)
- Speed Histogram: Disable (dropdown)
- Length Histogram: Disable (dropdown)
- Timestamp Option: End of Interval (dropdown)
- Use Diagnostics to Correct Averages: ☐ (checkbox)
- Display Diagnostics: ☒ (checkbox)
- Show Radar Detail for Large Objects: ☒ (checkbox)

Buttons at the bottom: Refresh ..., Revert, Save To AP.

Figure 5.23. Push window (Other)

## Individual Speed Mode

Determines how detection data is compiled in situations where vehicle speed and length cannot be calculated.

- *Calculable speed only* – reports only vehicles that have calculable speeds and lengths
- *All cars* – reports all vehicles regardless of the availability of speeds or lengths

## Units

Specifies the unit scale used in generating statistics. Select from the drop-down list one of the following:

- *Imperial* – denotes use of feet, miles, and miles per hour (mph)
- *Metric* – denotes use of meters, kilometers, and kilometers per hour (kph)

## Individual Car Reports

This element allows the designation of real-time report mode in which statistics are generated based on individual vehicle detections. Select from the drop-down list one of the following:

- *Disabled* – turns off the function
- *Standard* – produces output in Sensys Networks default format

## Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate statistical report entries. In real-time report mode, this element specifies the time duration between creating separate statistical files. Select from the drop-down list one of the following:

- 10 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

## Maximum File Size

Specifies the maximum file size (in bytes) of any single statistical archive file.

## Average Speed

Enables/disables the inclusion of the calculated average speed in the collection of data outputs. When *Average Speed* is enabled, this element also qualifies how the calculation of the average is performed.

## Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. Select from the drop-down list one of the following *Imperial* mode options:

- *Disable* – disables the function
- 1 mph
- 5 mph
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

---

**NOTE:**

The *Metric* mode options are *Disable*, *1 km/h*, *10 km/h*, and *TTI*.

---

## Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. Select from the drop-down list one of the following *Imperial* mode options:

- *Disable* – disables the function
- 1 foot
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

**NOTE:**

The *Metric* mode options are *Disable*, *0.5m*, and *AusRoads*.

---

**Timestamp Option**

Designates the point in time relative to the entire length of reporting interval that corresponds to the timestamp of the report entry. Select from the drop-down list one of the following:

- End of interval
- Start of interval
- Middle of interval

**Use Diagnostic to Correct Averages**

Enables/disables the use of sensor diagnostic data to generate smart averages when calculating averages for speeds and lengths. Smart averages disregard non-reporting sensors.

**Display Diagnostics**

Enables/disables inclusion of the sensor diagnostic values in the output data collection.

**Show Radar Detail for Large Objects**

Enables/disables the differentiate between large and small output.

**Configuring Poll Settings**

A common requirement of event data statistics is the need to transfer it to other hosts or platforms. An accepted technique to do this is referred to as poll. Poll refers to movement of processed sensor data from the statistical server (typically, an access point) to another host based on a request by the consuming host. This section describes the settings that comprise the generic polling interface of Sensys Networks.

**NOTE:**

Use of this feature requires an appropriate license.

---

**Access Point**

AP Config System C... Pairings Comman...

Net Poi... Push Poll Me... Other Cmds

**Poll**

TCP Port (required) 12345

Operating Mode Connection-based Po

Units Imperial

Individual Speed Mode All cars

Individual Car Reports Disabled

Report Interval 5 min

Maximum File Size 10000

Average Speed ☐

Speed Histogram Disable

Poll (cont.)

Caltrans D3 Poll Server

Caltrans D4 Poll Server

Marksman Poll

Refresh ... Revert Save To AP

Figure 5.24. Poll window

## TCP Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

## Operating Mode

Specifies the nature of the connection between an access point's poll process and the remote host. Select from the drop-down list one of the following:

- *Persistent Connection* – indicates that once a connection is established it remains in force. Reports are available at the end of the report interval (discussed below). For example, given a report interval of 30 seconds, if a connection is made 16 seconds into the interval, the first report would be available 14 seconds after the connection was made.
- *Connection-based Polls* – indicates that a connection is built, used, and closed for each successive poll from the remote host.
- *Poll Sampling* – (default) indicates that a connection is treated as a request. Upon receiving a request, the most recent report is delivered to the client and the connection is closed. There is no built-in processing to prevent sending duplicate reports. If a subsequent connection is made before a new report is available, the same report is sent to the subsequent connection.

## Units

Specifies the unit scale used in generating statistics. Select from the drop-down list one of the following:

- *Imperial* – denotes use of feet, miles, and miles per hour (mph)
- *Metric* – denotes use of meters, kilometers, and kilometers per hour (kph)

## Individual Speed Mode

Determines how detection data is compiled in situations where vehicle speed and length cannot be calculated.

- *Calculable speed only* – reports only vehicles that have calculable speeds and lengths
- *All cars* – reports all vehicles regardless of the availability of speeds or lengths

## Individual Car Reports

This element allows the designation of real-time report mode in which statistics are generated based on individual vehicle detections. Select from the drop-down list one of the following:

- *Disabled* – turns off the function
- *Standard* – produces output in Sensys Networks default format

## Report Interval

In aggregate report mode, this element specifies the time duration between writing of separate statistical report entries. In real-time report mode, this element specifies the time duration between creating separate statistical files. Select from the drop-down list one of the following:

- 10 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

## Maximum File Size

Specifies the maximum file size (in bytes) of any single statistical archive file.

## Average Speed

Enables/disables the inclusion of the average speed in the collection of data outputs.

## Speed Histogram

Enables/disables the inclusion of speed bins suitable for building a histogram graph. Select from the drop-down list one of the following *Imperial* mode options:

- *Disable* – disables the function
- 1 mph
- 5 mph
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

### NOTE:

The *Metric* mode options are *Disable*, *1 km/h*, *10 km/h*, and *TTI*.

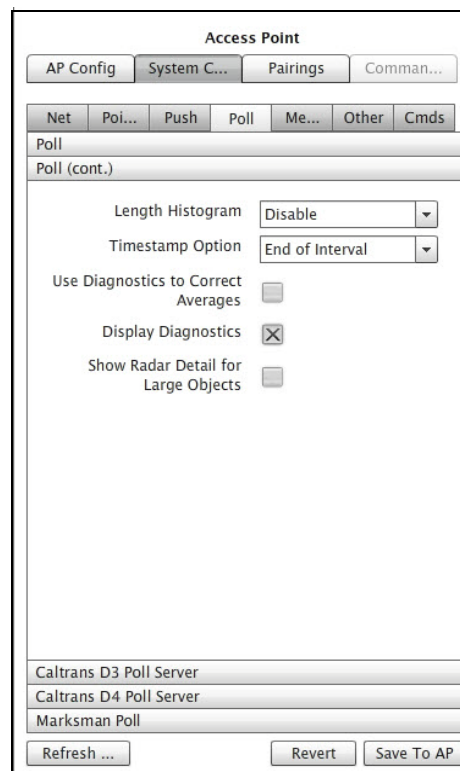


Figure 5.25. Poll window (cont)

## Length Histogram

Enables/disables the inclusion of length bins suitable for building a histogram graph. Select from the drop-down list one of the following *Imperial* mode options:

- *Disable* – disables the function
- 1 foot
- *TTI* – presents data in bin widths from the Texas Traffic Institute specification

**NOTE:**

The *Metric* mode options are *Disable*, *0.5m*, and *AusRoads*.

---

**Timestamp Option**

Designates the point in time relative to the entire length of reporting interval that corresponds to the timestamp of the report entry. Select from the drop-down list one of the following:

- End of interval
- Start of interval
- Middle of interval

**Use Diagnostic to Correct Averages**

Enables/disables the use of sensor diagnostic data to generate smart averages when calculating averages for speeds and lengths. Smart averages disregard non-reporting sensors.

**Display Diagnostics**

Enables/disables inclusion of the sensor diagnostic values in the output data collection.

**Configuring California DOT District 3 Poll Servers**

This section describes the settings that comprise the Sensys Networks polling interface developed for CalTrans D3 Poll Servers. Use of this feature requires an appropriate license.

Figure 5.26. Poll window (Caltrans D3 Poll Server)

### TCP Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

### 1st Drop Number

A required value originated by the polling client used by the statistical server to formulate a response message.

### 2nd Drop Number

A required value originated by the polling client used by the statistical server to formulate a response message.

## Configuring California DOT District 4 Poll Servers

This section describes the settings that comprise the Sensys Networks polling interface developed for CalTrans D4 Poll Servers. Use of this feature requires an appropriate license.



Figure 5.27. Poll window (Caltrans D4 Poll Server)

### Port Number

A required value specifying the port number on which poll requests arrive. The Sensys Networks statistical host listens for requests on this port.

### Controller Address

A required value used by the statistical server to formulate a response message. Must be an integer between 1 and 255.

### Configuration Type

Indicates the layout of the traffic site via a series of predefined configurations.

- 71: 8 Mainline lanes, 0 Ramp lanes
- 72: 8 Mainline lanes, 4 Ramp lanes
- 74: 12 Mainline lanes, 4 Ramp lanes
- 78: 16 Mainline lanes, 8 Ramp lanes

## Configuring Marksman Poll Servers

Event statistics can be formatted to adhere to the Marksman protocol portion of the Australian Roads specification. Specifying these values results in a new instance of the APSTAT process being invoked the next time the access point is rebooted. Use of this feature requires an appropriate license.

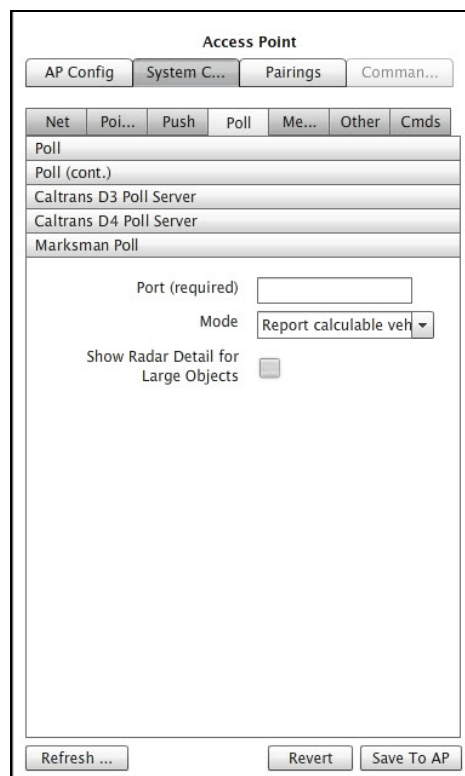


Figure 5.28. Poll window (Marksman Poll)

## Designating the Port Number

Port stores a required integer value that specifies the port the access point listens to for report requests.

## Selecting a Reporting Mode

*Mode* specifies the scope of the output data collection. From the *Mode* drop-down list select either of the following:

- Report calculable vehicles
- Report all

## Show Radar Detail for Large Objects

Enables/disables the differentiate between large and small output.

## Configuring Memory Settings

Access points typically host application processes that perform data transfer and formatting; the processes are configured on the *Push*, *Poll*, *CalTrans D3 Poll*, *CalTrans D4 Poll*, and the *Marksman Poll* tabs. A total of 500KB of memory is allocated to local applications. The memory allocation is configured via the *Memory* tab.

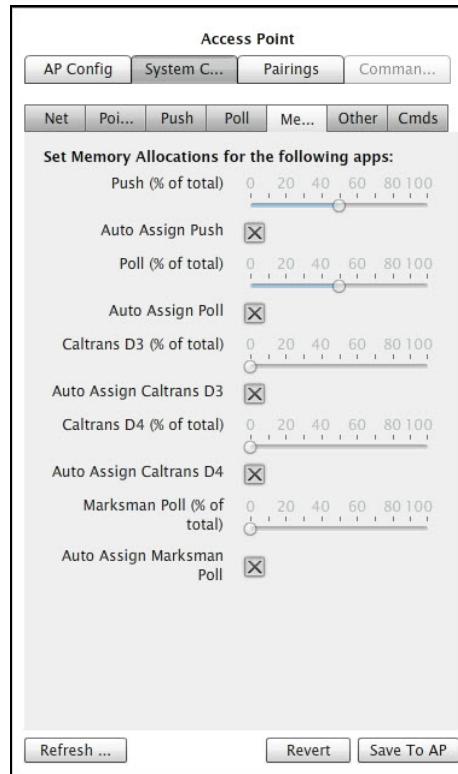


Figure 5.29. Memory window

## Window Contents and Operation

The tab displays a slide bar and checkbox related to memory allocation to the application processes that may execute on an access point. The slide bar and checkbox are active only for processes that are executing on the access point. If the window elements are not accessible, the access point is not licensed for the processes or they are not running.

## Automatically Allocating Memory to the Processes

By default, the system automatically allocates memory equally among each of the executing processes. Select the **Auto Assign** checkbox(es) to specify this.

## Manually Allocating Memory to the Processes

To manually set the memory allocated to one or more of the processes, uncheck the **Auto Assign** and perform the following:

1. Locate the slide bar related to the desired application and move it to indicate the desired percentage of application memory (500 KB) allocated to that process.
2. Click **Save To AP**. This writes the change to the access point's configuration file but does not reallocate memory.

3. Reboot the access point to allocate memory according to the configuration settings.

## Configuring Other Properties

The Other tab provides an opportunity to configure elements that are more advanced or specialized. These elements include:

- Enabling the access point to interface to traffic signal controllers
- Enabling the high accuracy speed mode for the access point
- Enabling the direct interface to Siemens signal controllers
- Direct access to sensor event data via a proxy process
- Time synchronization settings
- Configuring serial mode settings
- Configuring advanced access point diagnostics settings

The screenshot shows the 'Access Point' configuration window. At the top, there are tabs: 'AP Config', 'System C...', 'Pairings', and 'Comman...'. Below these, there are more tabs: 'Net', 'Poi...', 'Push', 'Poll', 'Me...', 'Other', and 'Cmds'. The 'Other' tab is selected, and the 'Time Settings' section is visible. It contains two dropdown menus: 'Timezone (required)' set to 'GMT' and 'Time Synchronization' set to 'Synchronized'. Below these, there is a list of settings: 'Serial Application Settings', 'Custom Application Settings', 'Event Proxy Settings', 'AP Diagnostic Settings', 'SncProxy Settings', and 'STS Settings'. At the bottom, there are three buttons: 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.30. Other tab (Time Settings)

## Time Settings

Time is used throughout networks for a variety of purposes. An access point can be configured to enforce on the entire network a uniform timebase sourced from a trusted timeserver.

## Time Zone

A required setting that designates the access point as residing in a particular time zone. A range of common North American time zones, as well as an array of offsets from GMT (Greenwich Mean Time) are supported.

## Time Synchronization

Enables/disables synchronizing the radio clocks of all network devices to the Linux timekeeping process on the access point. Sensys Networks recommends enabling this feature and configuring the access point to acquire time from a trusted, external time server. The options supported are:

- *Synchronized* – where a base time is acquired from a timeserver and distributed throughout the network by the access point
- *Free Running* – each device uses its own internal clock

## Serial Application Settings

Access points support serial communications over two on-board serial ports for communications with traffic controller equipment, cellular data networks, GPS systems, or maintenance consoles.

### NOTE:

Serial port A is configured by hardware settings only.

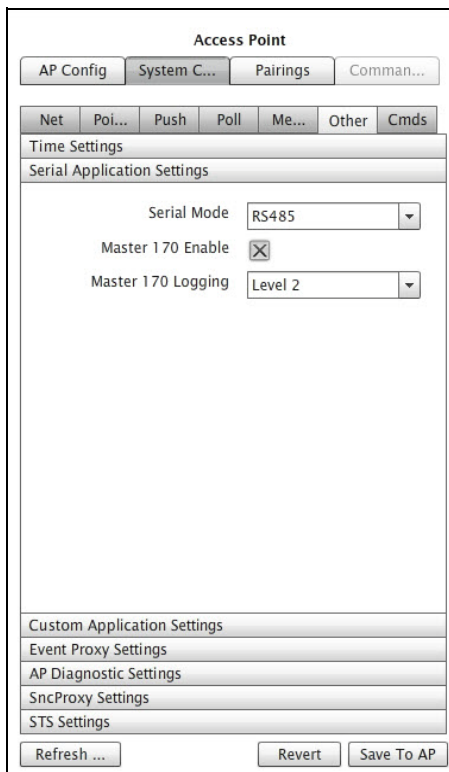


Figure 5.31. Other window (Serial Application Settings)

### Serial Mode

Specifies how the access point configures the serial port “B” for use. Supported options include:

- *Disable* – removes the port from the active configuration of the access point
- *GPS* – sets the port for communications with a GPS system
- *RS485* – sets the port for communications with traffic signal control equipment via a contact closure card from Sensys Networks. This setting is mandatory for using the access point with signal controllers.

### Enabling the Master 170 Interface for Traffic Signal Controllers

Access points can be interfaced to a variety of popular traffic signal controllers. Enable this setting on access points that will interface to such systems by filling the checkbox.

---

**NOTE:**

This setting only results in the execution of software on an access point required for traffic signal controller interfaces. Additional equipment from Sensys Networks is required to physically interface Sensys Networks to a traffic signal controller.

---

### Enabling Logging for the Master170 Interface

System logging records a range of operations between an access point and a traffic signal controller to which it is interfaced. Select via the drop-down list a logging level ranging from no logging (level zero) to extensive logging (level two).

---

**NOTE:**

Logging requires more disk space so the typical practice is to use this feature only for monitoring a new system at start up or for troubleshooting.

---

## Custom Application Settings

TrafficDOT offers the custom applications: *High Accuracy Speed* and *Wrong Way Detection*. The elements in *Custom Applications Settings* allow for the configuration of these applications.

Figure 5.32. Other window (Customer Application Settings)

### Enabling High Accuracy Speed Mode

*High Accuracy Speed* (HAS) mode is useful for networks implemented for red-light enforcement. Select the checkbox to enable the feature.

#### NOTE:

Enabling this feature requires that sensors are configured to operate using mode H.

### Enabling RS485 for HAS

*RS485 for HAS* sets the port for communications with traffic signal control equipment via a contact closure card from Sensys Networks for high accuracy speed. Select the checkbox to enable the feature.

### Enabling the Interface to Siemens Traffic Systems (STS)

*Enable STS* directs an access point to operate with a Siemens traffic controller over a proprietary interface. Select the checkbox to enable the feature. Do not enable this feature unless the access point is used with the appropriate Siemens equipment.

## Enabling Wrong Way Detection

*Wrong Way Detection* is a Sensys Networks application that detects the direction of vehicles entering a section of road the wrong way, and allows for an emergency warning to oncoming vehicles, as well as the immediate notification of the appropriate emergency response. Select the checkbox to enable the feature.

## Event Proxy Settings

Sensor event data can be accessed by a simple line-oriented interface over TCP/IP. End users can use clients to access and display event data as ASCII text.

The screenshot shows a web-based configuration interface for an 'Access Point'. At the top, there are tabs: 'AP Config', 'System C...', 'Pairings', and 'Comman...'. Below these is a row of sub-tabs: 'Net', 'Poi...', 'Push', 'Poll', 'Me...', 'Other', and 'Cmds'. The 'Other' tab is selected. Underneath, there are several expandable sections: 'Time Settings', 'Serial Application Settings', 'Custom Application Settings', 'Event Proxy Settings' (which is expanded), 'AP Diagnostic Settings', 'SncProxy Settings', and 'STS Settings'. In the 'Event Proxy Settings' section, there is a text input field for 'Event Proxy Server Port (required)' with the value '23444', and a dropdown menu for 'Adaptive Holdover' with the value '10 Ft'. At the bottom of the interface are three buttons: 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.33. Other tab (Event Proxy Settings)

## Direct Access to Sensor Event Data

*Event Proxy Server Port* provides a text/line oriented interface to event data. It is intended for use by field technical staff.

## Adaptive Holdover

Enables/disables the automatic adjustment of the downhold parameter. When enabled, the value specifies in feet the magnitude of the adjustment.

## Advanced AP Diagnostic Settings

These elements are used in regard to the automatic performance diagnostic reporting done by the access point by the instance of APDIAG that executes on the access point.



The screenshot shows a web-based configuration interface for an 'Access Point'. At the top, there are tabs: 'AP Config', 'System C...', 'Pairings', and 'Comman...'. Below these is a row of sub-tabs: 'Net', 'Poi...', 'Push', 'Poll', 'Me...', 'Other', and 'Cmds'. The 'Other' tab is selected, displaying a list of settings categories: 'Time Settings', 'Serial Application Settings', 'Custom Application Settings', 'Event Proxy Settings', 'AP Diagnostic Settings', 'SncProxy Settings', and 'STS Settings'. The 'AP Diagnostic Settings' section is expanded, showing four input fields with their default values: 'Adaptive Downhold (ft) default: 10' (value: 10), 'Stuck Time (s) default: 60' (value: 60), 'Downhold (s) default: 0' (value: 0), and 'Uphold (s) default: 0' (value: 0). At the bottom of the window are three buttons: 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.34. Other window (AP Diagnostic Settings)

### **Adaptive Downhold (feet)**

Type the length in feet used by the adaptive downhold calculation.

The algorithm calculates the amount of time the count, speed, and occupancy calculations must holdover based on an average of the five most recent speeds calculated. Time is derived from the entered length, using average speed. The default value is 10 feet.

### **Stuck Time (seconds)**

Type a number of seconds a sensor must report a continuous vehicle present state before it is considered non-reporting. The default is 60 seconds.

### **Downhold (seconds)**

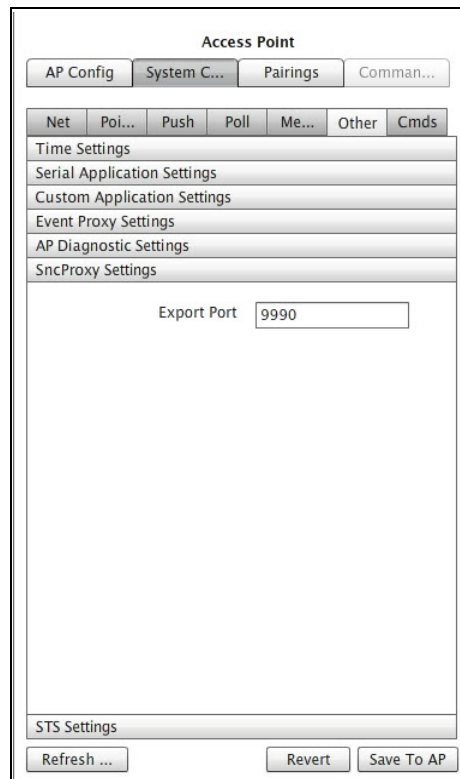
Type a number of seconds an undetection signal must last before it is considered to represent an undetection event. The default value is zero seconds.

### **Uphold (seconds)**

Type a number of seconds a sensor must report a continuous vehicle present state before it is considered to represent a detection event. The default value is zero seconds.

## Configuring SncProxy Settings

The *SncProxy Settings* window provides the ability to specify an export port for an access point's sensor data.



The screenshot shows the 'Access Point' configuration window. At the top, there are tabs: 'AP Config', 'System C...', 'Pairings', and 'Comman...'. Below these are sub-tabs: 'Net', 'Poi...', 'Push', 'Poll', 'Me...', 'Other', and 'Cmds'. The 'SncProxy Settings' section is selected, showing a list of settings: 'Time Settings', 'Serial Application Settings', 'Custom Application Settings', 'Event Proxy Settings', 'AP Diagnostic Settings', and 'SncProxy Settings'. The 'SncProxy Settings' section is expanded, showing an 'Export Port' field with the value '9990'. At the bottom, there are buttons for 'Refresh ...', 'Revert', and 'Save To AP'.

Figure 5.35. Other window (*SncProxy Settings*)

### Export Port

A value specifying the remote port SncProxy uses to connect to the access point. The default is 10000.

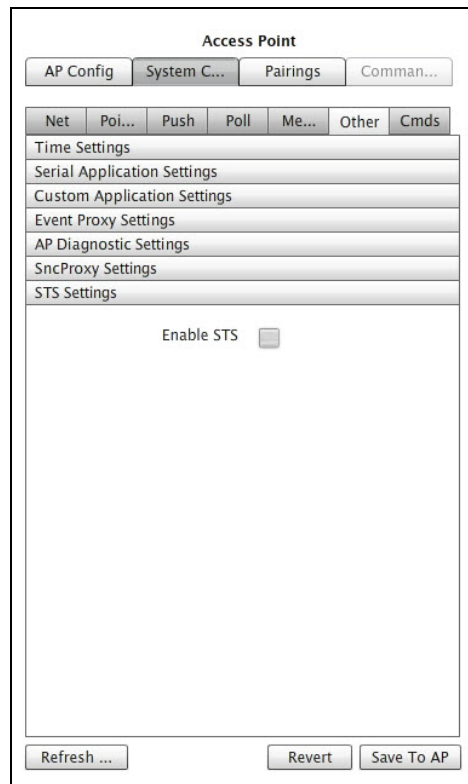


Figure 5.36. Other window (STS Settings)

## Configuring Commands Settings

The *Cmds* window provides the ability to backup and restore access point configuration, install and/or update an access point's license file, and download a diagnostic file.



Figure 5.37. Cmds window

## Backup/Restore an Access Point's Configuration

Sensys Networks recommends backing up the configuration of an access point once it has been finalized, as well as immediately before and after any significant changes are made.

By default, backups are stored on the file system of the platform that hosts TrafficDOT.

### Backup Procedure

To backup the current access point configuration, perform the following steps:

1. Click **Backup** from the *Cmds* tab. The *Save Backup* window displays.
2. Name the file to store the backup. Optionally, store the file to a different folder than the default.
3. Click **Save To AP** to backup the access point.

### Restore Procedure

To restore an access point configuration and data, perform the following steps:

1. Click **Restore** from the *Cmds* tab. The *Select file to use for restore* window displays.
2. Select the file that contains the backup that will serve as the source for the restore. Optionally, navigate to a different folder than the default.
3. Click **Open** to restore the access point from the file.

### Selecting an Access Point License File

Sensys Networks stores customer permissions and product access keys in a license file stored on the access point. From time to time, there may be a need to update it.

To install/update an access point license file, perform the following steps:

1. From the *Cmds* tab, click **License**. The *Select License file* window displays.
2. Select the file that contains the license for the access point. Optionally, navigate to a different folder than the default.
3. Click **Open** to install or update the license file.
4. After the license file has been transferred to the access point, reboot the access point.

---

**NOTE:**

The license will not take effect until the access point is rebooted.

---

### Downloading a Diagnostic File

On rare occasions, Sensys Networks Technical Support group may request a diagnostic file. This is a special type of backup that facilitates analysis of the access point and its processes.

This operation follows a procedure very similar to that of performing a backup. Work with the Technical Support group to determine the best means to transfer the file to Sensys Networks.

## Configuring Repeaters

Sensys Networks repeaters ship with a factory-installed default configuration. In most cases, the configuration is modified to fit the specific needs of an installation. However, once set, a repeater's configuration typically requires no further changes.

This section describes configuring repeaters with TrafficDOT and provides information about the following activities:

- Selecting a repeater to configure
- Specifying which time slot configuration a repeater will use
- Specifying the repeater's two RF channels
- Assigning a time slot to a repeater
- Downloading firmware to a repeater
- Adding a repeater to a network
- Removing a repeater from a network
- Performing other operations

### Introduction

Repeater configuration involves dragging a repeater onto the map image and selecting values for the following parameters:

- Repeater configuration
- Radio frequency of the upstream (access point) channel
- Radio frequency of the downstream (sensor) channel
- Transmission time slot (optional)

Other operations related to management of repeaters are also performed from the *Repeater Configuration* window.

### Tandem Repeaters

Repeaters used to forward the signals of other repeaters (tandem repeaters) are configured in the same way as repeaters communicating directly with an access point. Tandem repeater topologies are implied by the RF channel assignments made to separate repeaters.

### Working with the Repeater Configuration Window

To select a repeater for configuration, click on a repeater on your image map. The *Repeater Configuration* window displays.

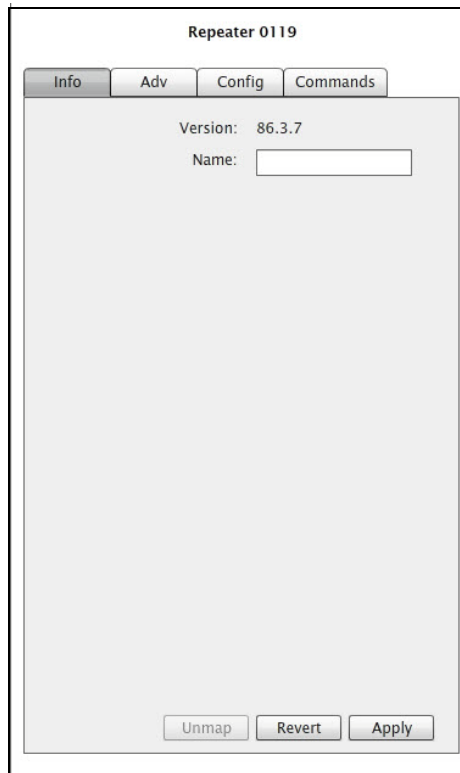


Figure 5.38. Repeater Configuration window (*Position* tab)

### Viewing the Repeater Firmware Version and Entering a Repeater Name

The repeater's firmware version can be reviewed on the *Position* tab as shown in Figure 5.37. Also, a unique user-defined repeater name can be entered into the *Name* field.

Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

---

**NOTE:**

The repeater firmware version is for reference only.

---

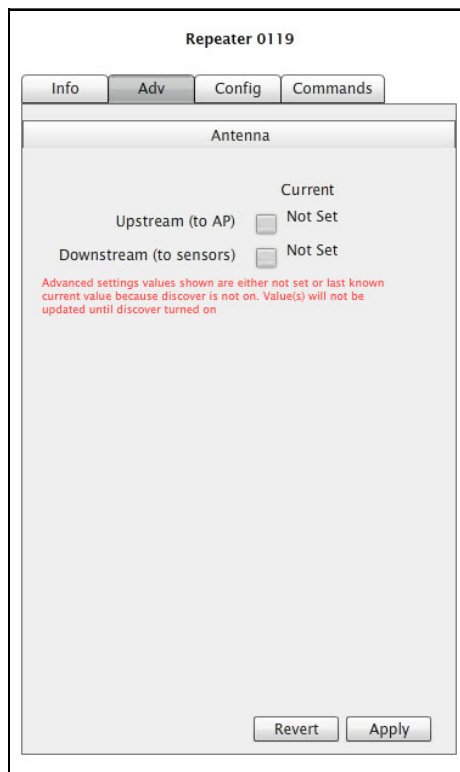


Figure 5.39. Repeater Configuration window (Adv tab)

## Selecting an External Antenna

The **Adv** tab provides the ability to choose an antenna for an external upstream connection the access point or an external downstream connection to the sensors. Click **Upstream (to AP)** to select an upstream connection to the access point or click **Downstream (to sensors)** to select a downstream connection to the sensors.

Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.



The image shows a software window titled "Repeater 0119". It has four tabs: "Info", "Adv", "Config" (which is selected), and "Commands". The "Config" tab contains several configuration fields:

- Current Upstream Ch:** 4, with a "Change to:" dropdown menu.
- Current Downstream Ch:** 10, with a "Change to:" dropdown menu.
- Current Timeslot:SPP:** 20:0, with an "Auto-assign All" button and a "Change Timeslot to:" dropdown menu. A note below the button says: "Press 'Auto-assign All' to automatically assign all Sensors and Repeaters to optimal timeslots".
- Show only available slots:** A checkbox that is checked.
- Current Config:** 1, with a "Change to:" dropdown menu.
- Current Color Code:** A text field.
- Change To (hex 01-FF):** A text field.

At the bottom right of the window are two buttons: "Revert" and "Apply".

Figure 5.40. Repeater Configuration window (Config tab)

## Specifying the RF Channels

Repeaters are configured with two RF channels. The first channel, which is known as the access point or upstream channel is used to communicate with an access point. This channel is set in the access point's configuration. The second channel, which is known as the sensor or downstream channel is used to communicate with sensors. This channel must not be the same channel as the access point channel.

### Specifying the Access Point (Upstream) Channel

To specify the RF channel for access point transmissions, perform the following steps:

1. Click an entry from the upstream *Change to* drop-down list.

The selected channel must be the same RF channel that the target access point is configured to use. (Refer to the *Configuring Access Points* section in this chapter for more information.)

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Specifying the Sensor (Downstream) Channel

To specify the RF channel for transmissions in the direction of sensors, do the following:

1. Click an entry from the downstream *Change to* drop-down list.  
The selected channel must not be the same than the channel selected as the access point channel. In addition, all sensors serviced by the repeater must be configured to use the repeater's sensor channel.
2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.

### Setting the Time Slot of a Repeater

In addition to forwarding event data packets to the access point and management packets to the sensors it services, repeaters originate packets of their own. Normally, repeaters transmit repeater packets via a sensor time slot when the repeater detects that a sensor is not transmitting.

In some instances, however, it may be beneficial to restrict the repeater's use to a defined time slot as a means to eliminate competition to transmit. To set the time slot, do the following:

1. Click an entry from the *Change Timeslot to* drop-down list.  
By default, TrafficDOT filters the contents of the drop-down list so that only available time slots (time slots that are consistent with the network's transmit interval and not already assigned) are displayed.  
To change the drop-down list to include all time slots in the network (both assigned and unassigned), remove the check in the *Show only available slots*.

---

**NOTE:**

The list does not include time slots that are, by definition, reserved for use by access points.

---

2. Click **Apply** to accept configuration changes. To save the changes to the access point, click the **SAVE** button at the top of the window.



Figure 5.41. Repeater Configuration window (Commands tab)

### Performing a Soft Reset

On occasion, a repeater may need to be reset without changing its RF communication parameters. To perform a soft reset, select the repeater and click the **Reset (Keep RF)** button.

### Performing a Hard Reset

A repeater may need to be reset back to its factory default configuration. This operation resets the repeater's RF channel assignment to channel zero. Reconfiguration may be required in order for the repeater to communicate with the network's access point. To perform a hard reset, select the repeater and click the **Hard Reset** button.

### Downloading Repeater Firmware

Updates to repeater firmware are sent from the access point via the wireless communication channel.

---

**NOTE:**

Repeater firmware updates must occur independent of sensor or access point firmware updates.

---

Firmware updates become operational immediately and can be reversed only by performing the firmware update procedure specifying a prior version of the appropriate firmware image. It is not necessary to reconfigure repeaters after updating their firmware, although in many cases, new firmware enables additional device functionality that may require initial configuration.

To download repeater firmware, start broadcasting the appropriate firmware; select the repeater, and then click the **Download Firmware** button.

## Configuring Contact Closure Cards

The Sensys Networks VDS240 wireless vehicle detection system can be interfaced directly to local traffic signal controllers such as the CalTrans Type 170, Type 2070 ATC and NEMA TS-1 and TS-2 controllers via a hardware interface card installed into the controller cabinet. The interface allows detection events collected by an access point to activate contact closure relays in the controller.

This section describes configuring and working with contact closure cards via TrafficDOT. The following activities are discussed:

- Entering controller card information
- Configuring channel state
- Configuring channel mode
- Configuring presence mode modifier
- Configuring channel holdover duration
- Setting watchdog fail mode
- Working with command properties

## Working with the Controller Card Configuration Window

To select a controller card for configuration, click on a controller card on your image map. The *Controller Card Configuration* window displays.

The screenshot shows a web-based configuration window titled "Controller Card 1-1". It has three tabs: "Card Info", "Channels", and "Card Commands". The "Card Info" tab is active, displaying a list of configuration parameters for a specific card. The parameters and their values are: Card Type (CC Card), Checksum Failure Count (2), Channel Count (4 Channel), Controller Type (170 Controller), and Firmware Version (42). At the bottom right of the window, there are two buttons: "Delete" and "Unmap".

Figure 5.42. Controller Card Configuration window (Card Info tab)

**NOTE:**

The *Card Info* panel is read-only and for informational purposes only.

## Configuring Controller Card Channels

*Channels* refer to the vehicle detection relays of contact closure cards. Each channel consists of an optically isolated contact closure and, for cards in TS2 compatibility mode, a status contact closure to ground. Channels are independent of one another and are referred to by number (one through four).

A predetermined set of sensors (and the vehicle detection events they transmit) are grouped together by the access point and supplied to a contact closure card via one of the channels. The contact closure card, in turn, activates the channel's contact closure relay based on the vehicle detection data.

A single channel may support up to 15 sensors whose detection events are evaluated in combination (in a logical or operation). If any one of the sensors detects a vehicle, the corresponding contact closes.

Contact closure cards are available in four-channel versions. Each channel may be individually enabled/disabled and configured.

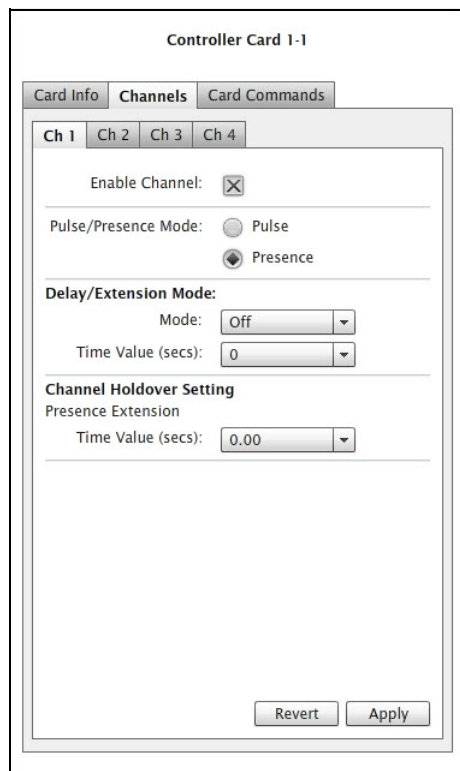


Figure 5.43. Controller Card Configuration window (Channels tab)

### Configuring Channel State

Contact closure card channels are independent of one another and are individually configured. Each channel occupies one of the following states:

- *Enabled* – the channel is operational; sensor event data collected by the access point is transmitted to the contact closure card
- *Disabled* – the channel is not operational. (When a channel is disabled, its contact closure relay and status relay are continuously open.)

The factory default configuration enable channels one and two. Ensure that any unused or unavailable channels are disabled.

### Configuring Channel Mode

Enabled channels operate in one of the following modes:

- *Pulse* – the contact closure relay pulses for 0.125 seconds each time the leading edge of a vehicle is detected.
- *Presence* – the contact closure relay remains closed while a vehicle is detected.
- The factory default setting is pulse mode.

### Configuring Presence Mode Modifier

The behavior of a channel operating in presence mode may be adjusted by applying one of the following modifiers:

- *Delay* – defers the onset of the contact closure by a specified duration. If a vehicle moves off of the sensor before the specified delay expires, the contact does not close. *Delay* is expressed in seconds from zero to 31.
- *Extension* – increases the duration of the contact closure by a specified increment. *Extension* is expressed in half-seconds from zero to 7.5.

The modifiers do not apply to channels operating in pulse mode.

### Configuring Channel Holdover Duration

The *Channel Holdover* parameter allows an extension to the channel holdover duration when it is activated by the events from a particular sensor. Values from 0.0 to 0.75 seconds are available for selection.

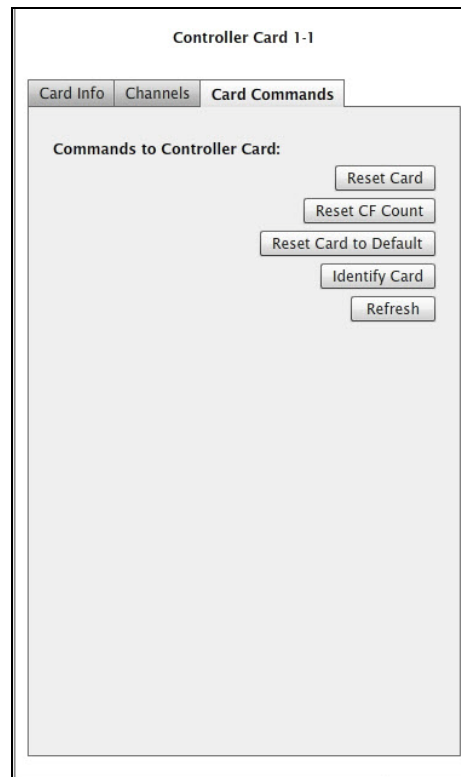


Figure 5.44. Controller Card Configuration window (Card Commands tab)

### Performing a Soft Reset

On occasion, a controller card may need to be reset without changing its RF communication parameters. To perform a soft reset, select the controller card and click the **Reset Card** button.

## Performing a Hard Reset

A controller card may need to be reset back to its factory default configuration. This operation resets the controller card's RF channel assignment to channel zero. Reconfiguration may be required in order for the controller card to communicate to with the network's access point. To perform a hard reset, select the controller card and click the **Reset Card to Default** button.



# Monitoring Components Using the Table View

This chapter provides information on *monitoring* Sensys Networks VDS240 wireless vehicle detection components using the *table view* in TrafficDOT.

## Overview

Like the map view, the *table view* in TrafficDOT provides a real-time view into the components of the network and the events they detect. All sensors in the network are shown, including sensors that communicate via repeaters. Detection counts, detection events, RF quality metrics, version and battery information are shown in dedicated columns updated at one second intervals.

The table view consists of three display areas:

- *Menus* – drop-down options providing access to specific functions
- *System Display* – tabular, real-time display of the network including RF quality indicators, detection events, and other information
- *Configuration panels* – the configuration panels for the key components discussed in the *Chapter 5: Configuring and Managing Components* are also accessible in the table view

ID	Channel	Battery Level	Idle	RSSI	LQI	Present	#Detections	Mode	Timeslot	Sensor Zone	2A	PER	Color Code	Adv Settings
0055	?		1	-67	97			μC	31:1			0%		
009C	?		1	-57	97			μC	18:1			0%		
0036	?		3	-69	97			μC	18:1			83.33%		
0096	?		1	-70	97			μC	6:1			0%		
0099	?		1	-67	97			μC	12:1			0%		
001A	?		1	-67	97			μC	15:1			0%		
0044	?		29	-77	97			B	56:1			--		
978E	?		19	-70	97			μA	54:1			--		
DC8D	?		17	-56	97			B	54:1			--		
00AB	?		14	-61	97			μA	52:1			--		
97FF	?		8	-69	97			μA	61:1			--		
9B9D	?		12	-74	97	A	B	μA	20:1			--		
C9D1	?		15	-71	97		1	SB5	22:1			--		
DC03	?		18	-62	97			B	57:1			--		
00C2	?		21	-58	97			μA	49:1			--		
005F	?		1	-69	97			μC	55:1			0%		
0079	?		2	-59	70			μC	40:1			10%		
DC81	?		2	-67	97			B	49:1			--		
0068	?		5	-73	97			μC	15:1			83.33%		
2180	?		0	?	?			?	7:0	HAS		--		
2167	?		0	?	?			?	7:0	HAS		--		
2143	?		0	?	?			?	7:0	HAS		--		

Figure 6.1. Table view

## Menus

The menus in TrafficDOT are related commands and functions organized into logical groups. The menus, which are available in both map and table view include:

### Connect

- *Connect* – Connects TrafficDOT to an access point
- *Disconnect* – Disconnects TrafficDOT from an access point

### Tools

- *Clear Sensors and Repeaters from View* – Removes all sensors and repeaters from the component tray
- *Clear Detection Counts* – Removes all detection counts
- *Scan For Devices...* – Performs device scans on selected or all RF channels
- *Auto-assign Timeslots* – Automatically assigns device timeslots
- *Charts...* – Provides the ability to create diagnostic real time diagrams indicating sensor detection data

- *Send Command* – Enables the ability to send commands to all devices whether they are seen or not
- *Clear Dot Table* – Clears the database that stores entries that describe the sensors in a network
- *Clear Dot PairTable* – Clears the database that stores entries that describe the sensors pairs in a network
- *Turn on SNC Proxy Logging* – Enables logging for the SNC proxy process
- *Browse to ...* – Activates a local HTTP browser
- *Addons ...* – Provides access to the built-in XML addons that enable access point controller card (APCC) configuration
- *Speed Data* – Provides access to extracted speed data from APSTAT output files
- *Import Kitting Data* – Enables the ability to import kitting data prior to a new installation
- *Preferences* – Enables the ability to set system preferences for connection timeout and RF quality thresholds. Also allows for setting user ID and password for FTP services hosted by the access point
- *Log Packet Error* – Starts the logging of the packet error rate (displayed in the PER column) of sensors
- *Stop Logging Packet Error Rate* – Stops the logging of the packet error rate (displayed in the PER column) of sensors

## Advanced

- *Set Advanced Mode* – Allows for access to advanced device settings
- *Set Super User Mode* – Allows authentication for diagnostic mode access
- *Password Protect File...* – Allows the loading of an older firmware package that requires the package to be password protected onto a sensor

## Help

- *About* – Provides access point version information
- *Help* – Provides access to the *TrafficDOT 2.10.3 Set Up and Operating Guide* (this document)

## System Display

The system display consists of sortable columns that can be displayed in ascending or descending order by clicking on the column's heading. The system display can be rearranged by selecting one of the **Group by:** and **View** options.

There are two **Group by:** options:

- *Repeater*
- *Sensor Zone*

Selecting either of the options groups the network repeaters or sensor zones in the *Id* column, and the group that is selected displays toward the top of column. Selecting one of the *View* options displays the *Group by:* information in either *Dot Table*, *Activity*, or *Normal* view.

The columns of the display are identified in the following table:

**NOTE:**

The order of the columns in the table are for *Normal* view.

Column Name	Description
Id	The factory assigned hardware device identifier. Sensors and repeaters are uniquely identified by a 64-bit value. This column displays the least significant 16 bits as a 4-character HEX string.
Repeater	The device id of the repeater servicing a sensor (if applicable). AP indicates a sensor is transmitting to the access point without using a repeater.
Channel	The RF channel on which the device is transmitting.
Sensor Zone	The field is populated automatically using the information in the <i>Position</i> window and the lane abbreviation.
H Position	Sensor's horizontal position relative to other sensors in the same lane. Values may be -3, -2, -1, 0, 1, 2 or 3 where -3 indicates the far-left sensor; -2 indicates the mid-left sensor; -1 indicates the left; 0 indicates the center sensor; 1 indicates the right sensor; 2 indicates the mid-right, and 3 indicates the far-right sensor.
V Position	Sensor's vertical position relative to other sensors in the same lane. This element is used to identify sensor speed pairs. Values may be 0, 1 or 2 where 0 indicates the lead sensor, 1 indicates a trailing sensor, and 2 indicates a second trailing sensor.
Battery Level	An estimate of the remaining battery level, expressed in volts.
Idle	The number of seconds since the latest packet was received from the device.
RSSI	Received Signal Strength Indicator – a measure of the radio signal strength.
LQI	Line Quality indicator – a statistical measure of the radio link quality.
Present	A graphical indication of the state of detection of the sensor.
# Detections	Total number of detections since TrafficDOT established a connection to the access point.
Mode	The operating mode of the device.
TimeSlot:SPP	The time slot on the access point used by the sensor, repeater, or SPP radio.

Column Name	Description
Config	Indicates that a sensor exists in the configured and saved Dot Table.
PER	Packet Error Rate – a statistical measure of the data loss due to errors, dropped packets, noise, etc.
Adv Settings	Depicts the settings configured via the Adv tab on the Sensor Configuration panel.
Color Code	Displays the RF channel codes for a vehicle detection system.
Version	The firmware version on the device. (Note: use the VDS Release Notes from Sensys Networks to cross references firmware version ids to VDS releases.)
Factory ID	The factory assigned hardware device identifier. This displays all 64 bits as a 16-character HEX string.
Description	Additional description for sensor location and use. (Optional)
CC Ext	Specifies a duration of extension (in milliseconds) applied to a contact closure card channel when activated by events detected by this sensor. This element implements a per-sensor extension. If the sensor is a MicroRadar sensor the field is formatted to accommodate the three sub-channels (e.g., 0/0/0). (Optional)
CC Delay	Specifies a channel delay duration for this sensor only (in milliseconds). If the sensor is a MicroRadar sensor the field is formatted to accommodate the three sub-channels (e.g., 0/0/0). (Optional)
Active	Devices that are transmitting during a TrafficDOT session.
Address 170	Maps a sensor table entry to a contact closure card channel. If the sensor is a MicroRadar sensor the field is formatted to accommodate the three sub-channels (e.g., 0-00-0/0-00-0/0-00-0). (Required)
Address 170 2	Maps a sensor table entry to a contact closure card channel. (Optional)
Address 170 3	Maps a sensor table entry to a contact closure card channel. (Optional)
Address 170 4	Maps a sensor table entry to a contact closure card channel. (Optional)

Table 13. Descriptions of columns in the table view



# Configuring Cellular Modems on an AP or an APCC

This section provides the information required to configure cellular modems on either an access point or access point controller card (APCC) using TrafficDOT 2.10.3. Both the AP and APCC support two types of embedded cellular modems: GSM/GPRS and CDMA.

In order to use a cellular service, you must have the following:

1. A service contract with a service provider
2. An AP or APCC that has the correct type of modem installed

## GSM/GPRS Modems

GSM/GPRS modems can be used by any GSM/GPRS service providers. Once you sign up for GSM/GPRS service, your service provider provides you with a SIMM card that needs to be inserted into the modem.

When configuring a GSM/GPRS, you need to provide the following information:

- APN
- Username
- Password

---

**NOTE:**

The above information is provided by your service provider.

---

To configure a GSM/GPRS modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab.
3. Select **Modem** from the *IP Mode* drop-down list.
4. Enter **custom** in the *Modem ISP* field.

The following fields display:

- ISP APN
- ISP User
- ISP Password

The screenshot shows the 'Access Point' configuration window with the 'System Config' tab selected. The 'IP Mode' is set to 'Modem'. The 'Modem ISP' field is set to 'custom'. The 'ISP APN', 'ISP User', and 'ISP Password' fields are empty. The 'Modem Phone #' and 'Modem PIN' fields are also empty. The 'Modem Type' is set to 'Unknown'. The 'Network Mask' is '255.255.252.0', 'IP Address' is '192.168.2.143', 'Gateway' is '192.168.2.1', and 'DNS' is '192.168.2.38'. The 'NTP Servers' field contains '1.us.pool.ntp.org 2.u'. The 'DHCP Monitor Host' field is empty. The 'Start C' button is visible next to the 'IP Mode' dropdown. At the bottom, there are 'Refresh Config', 'Revert', and 'Save To AP' buttons.

Figure A.1. GSM/GPRS modem configuration

**NOTE:**

The *Modem Phone #* field not required for GSM/GPRS modems, but is useful if you need to contact your service provider. The *Modem PIN* field is only required if your SIMM card is programmed with a personal identification number.



TrafficDOT recognizes the following GSM/GPRS providers:

- Cingular
- T-Mobile

For these service providers, you can simplify the modem configuration process by providing the name of the service provider in the *Modem ISP* field; TrafficDOT uses the default values for the APN, user name, and password.

## Cingular

For *Cingular*, the default fields are:

- ISP APN: isp.cingular
- ISP User: ISP@CINGULARGPRS.COM
- Password: CINGULAR1

---

**NOTE:**

If you are using *Cingular*, but the parameters are different than the defaults, you must use the custom *Modem ISP* to set the parameters.

---

## T-Mobile

For T-Mobile, the default fields are:

- ISP APN - internet3.voicestream.com
- ISP User - tmobile
- ISP Password - none

---

**NOTE:**

If you are using T-Mobile, but the parameters are different than the defaults, you must use the custom *Modem ISP* to set the parameters.

---

There are various types of GSM/GRPS modems for different access speed. You must select the correct modem type from the *Modem Type* drop-down list in order for the modem to work properly.

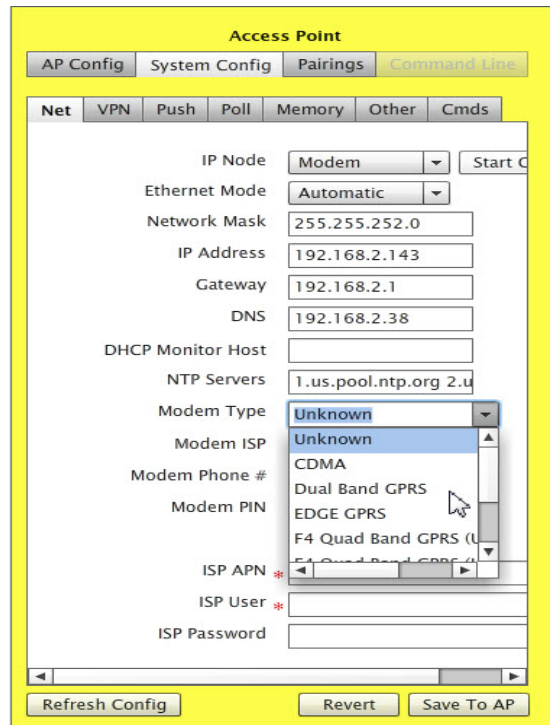


Figure A.2. GSM/GPRS modem type selection

Your package list should contain the part number of the access point. Access points with various modems installed have a different part number. For the new modems starting with G2, specific carriers are no longer supported, so you must configure the APN, user name, and password when configuring those modems.

## CDMA Modems

Unlike the GSM/GPRS modems, CDMA modems are built specifically for a service provider, hence configuration of CDMA modems differ depending on the service provider. You must ensure that you order the correct modem for your service provider.

In order to use a CDMA service, you must have the following:

1. A service contract with a service provider
2. A CDMA modem that is specific for your service provider

### NOTE:

Your service provider requires the ESN# or the MEID# from your modem in order for them to provision the service.

TrafficDOT recognizes the following CDMA providers:

- Verizon
- Aeris

## Verizon

To configure a Verizon modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab
3. Select **Modem** from the *IP Mode* drop-down list.
4. Select **CDMA** from the *Modem Type* drop-down list.
5. Enter **verizon** as the *Modem ISP*.
6. Enter the **Tower Phone #**.

### NOTE:

You must enter **verizon** as the *Modem ISP* in order to see the *Tower Phone #* field. The *Tower Phone #* is usually is 22899.

The screenshot shows the 'Access Point' configuration window with the 'System Config' tab selected. The 'IP Mode' is set to 'Modem' and 'Ethernet Mode' is set to 'Automatic'. The network settings are: Network Mask (255.255.252.0), IP Address (192.168.2.143), Gateway (192.168.2.1), and DNS (192.168.2.38). The 'Modem Type' is set to 'CDMA' and the 'Modem ISP' is set to 'verizon'. The 'Tower Phone #' is set to '22899'. The 'Modem Phone #' and 'Modem PIN' fields are empty. The 'Refresh Config', 'Revert', and 'Save To AP' buttons are at the bottom.

Figure A.3. Verizon modem configuration

7. Click **Save To AP** to save your configuration.

## Aeris

To configure an Aeris modem, perform the following steps:

1. Select an AP or APCC from the map image or components tray to open the *Access Point Configuration Window*.
2. Select the *System Config* tab.
3. Select **Modem** from the *IP Mode* drop-down list.
4. Select **CDMA** from the *Modem Type* drop-down list.
5. Enter **custom** in the *Modem ISP* field.
6. Enter **NNNNNNNNNN@tspo8.sprintpcs.com** as the *ISP APN* where *NNNNNNNNNN* is the phone number for your service.
7. Enter **guest** in the *ISP User* field.
8. Enter **guest** in the *ISP Password* field.
9. Enter the phone number provided to you by your service provider. The phone number you enter should be 10 digits and consist only numbers (e.g., 1112223333).
10. Click **Save To AP** to save your configuration.

# Addon Configuration

## Addons Support

This section provides information regarding the built-in addons that configure access point controller card (APCC) features. Using the addons, TrafficDOT can configure additional programs that run on the APCC without external code changes.

The following XML addons are supported:

- ASIX Ethernet Driver
- Lonestar TSS
- Modem Power Management
- RTL8192 Wireless Driver
- SD Card Sync
- USB Drive Sync

---

**NOTE:**

Not all thumb drives are supported. Refer to *Supported USB Chipsets* for additional information.

---

## Supported USB Chipsets

The following USB chipsets are supported:

- ID 090c:1000 Silicon Motion, Inc. (formerly Feiya Technology Corp)
- ID 090c:6200 Feiya Technology Corp
- ID 058f:6387 Alcor Micro Corp. Transcend JetFlash Flash Drive
- ID 0c76:0004 JMTEK, LLC. Mass Storage Controller

To find out the chipset of any USB drive:

- For Linux users, plug in the USB drive and type the command `lsusb`.
- For Windows users, download **Lsusb 1.0** from the Web to acquire the `lsusb` command that assesses all of the USB devices plugged into your system.

## Addons Panel

The Addons panel is accessed via *Tools -> Addons*, and given the XML definition TrafficDOT draws the appropriate configuration panel as shown in the following screen.

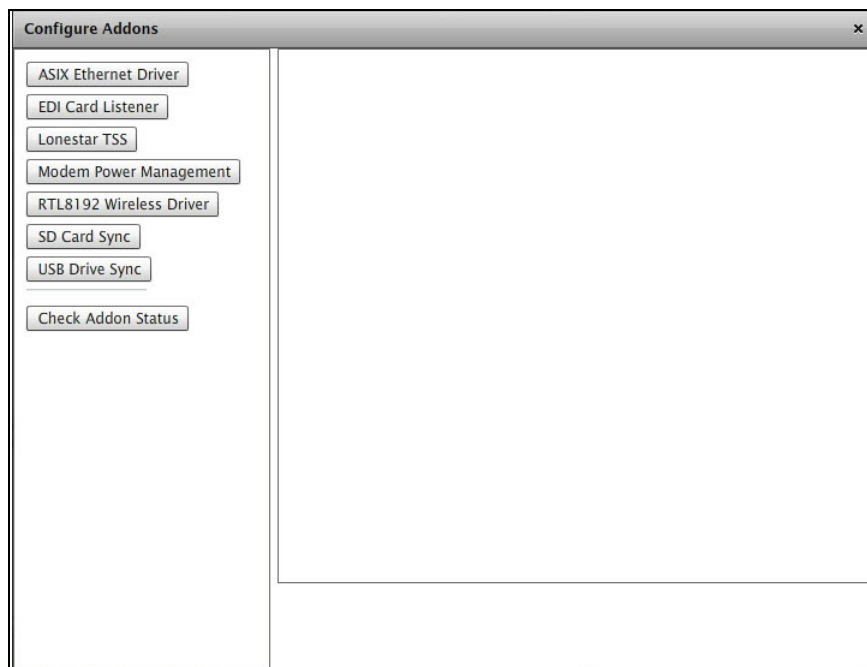


Figure B.1. Addons configuration panel

## Addons

### NOTE:

Any change saved with *Apply* has its new configuration values stored to the configuration file; however, these changes will not take effect until the next reboot of the APCC.

All addons have the following buttons; however *mmc/thumb* addons have extra buttons.

- *Apply* – saves the configuration to the file. It does not activate any settings. Usage of new settings is done at boot time.
- *Revert* – populates the panel with the last known configuration file content.
- *Diagnostics* – shows diagnostic information for the addon.

The *Check Addon Status* button on the left panel brings up a popup data grid containing information about the last diagnostic status of all the addons.

## ASIX Ethernet Driver

This addon set ups the ASIX Ethernet driver.

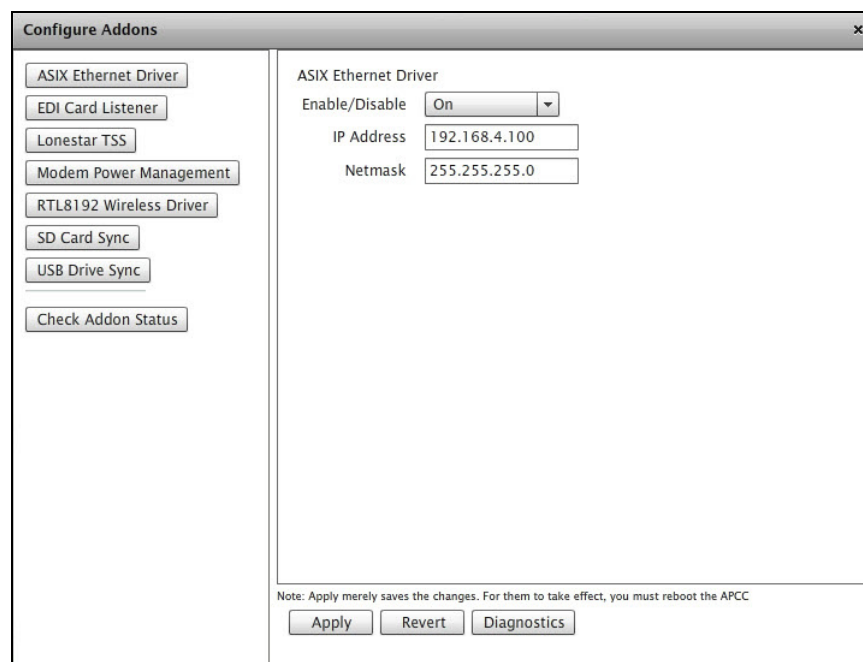


Figure B.2. ASIX Ethernet Driver window

## Elements

*Enable/Disable* – specifies if element is enabled or disabled. If this field is set to *On*, the addon program starts at boot time. Default is *Off*.

*IP Address* – defines the address of the driver. Default is 192 . 168 . 2 . 100.

*Netmask* – defines the netmask. Default is 255 . 255 . 255 . 0.

## Lonestar TSS

This addon sets up the program that communicates with the Lonestar TSS (Texas DOT).

Figure B.3. Lonestar TSS window

### Elements

*Enable/Disable* – specifies if element is enabled or disabled. If this field is set to *On*, the addon program starts at boot time. Default is *Off*.

*Port* – defines the port on which the APCC is listening for Lonestar requests. Default is 10100.

*Address* – defines the Lonestar TSS's network address. Default is 1.



## Modem Power Management

This addon configures the power management for the modem (SolarConnect).

The screenshot shows a window titled "Configure Addons" with a sidebar on the left containing buttons for various addons: ASIX Ethernet Driver, EDI Card Listener, Lonestar TSS, Modem Power Management (highlighted), RTL8192 Wireless Driver, SD Card Sync, USB Drive Sync, and Check Addon Status. The main area is titled "Power Management for Modem" and contains the following fields:

- Enable PMM: A dropdown menu set to "Off".
- Host: A text field containing "192.168.3.24".
- Username: A text field containing "apsync".
- Password: A text field containing "\*\*\*\*\*".
- APCC Name: An empty text field.
- Enable Interval: A text field containing "600".
- Disable Interval: A text field containing "21600".

At the bottom of the window, there is a note: "Note: Apply merely saves the changes. For them to take effect, you must reboot the APCC." Below the note are three buttons: "Apply", "Revert", and "Diagnostics".

Figure B.4. Power Management for Modem window

### Elements

*Enable PMM* – specifies if the PMM is enabled or disabled. Default is Off.

*Host* – defines the SNAP host. Default is 192 . 168 . 3 . 24 .

*Username* – defines SNAPS *Username* authentication. Default is *apsync*.

*Password* – defines the SNAPS authentication. The default displays with '\*' characters.

*APCC Name* – defines the logical name on SNAPS. No default.

*Enable Interval* – enables the modem intervals, in sec. Default is 600 (in sec, so this is 10 mins).

*Disable Interval* – disables the modem intervals, in sec. Default is 21600 (equals to 6 hrs).

## RTL8192 Wireless Driver

This add-on configures the RTL 8192 wireless driver (i.e., the wireless dongle).

The screenshot shows a window titled "Configure Addons" with a sidebar on the left and a main configuration area on the right. The sidebar contains buttons for "ASIX Ethernet Driver", "EDI Card Listener", "Lonestar TSS", "Modem Power Management", "RTL8192 Wireless Driver" (which is highlighted), "SD Card Sync", "USB Drive Sync", and "Check Addon Status". The main area is titled "RTL 8192 Wireless Driver" and contains the following settings:

- Enable/Disable:** A dropdown menu set to "On".
- IP Address:** A text field containing "192.168.5.100".
- Netmask:** A text field containing "255.255.255.0".
- ESSID:** A text field containing "apcc".
- Channel:** A text field containing "4".
- Key:** A text field containing "\*\*\*\*\*".

At the bottom of the main area, there is a note: "Note: Apply merely saves the changes. For them to take effect, you must reboot the APCC." Below the note are three buttons: "Apply", "Revert", and "Diagnostics".

Figure B.5. RTL8192 Wireless Driver window

### Elements

*Enable/Disable* – specifies if element is enabled or disabled. If this field is set to *On*, the add-on program starts at boot time. Default is *Off*.

*IP Address* – defines the address. Default is 192 . 168 . 5 . 100.

*Netmask* – defines netmask of the new wireless endpoint. Default is 255 . 255 . 255 . 0.

*ESSID* – defines a 32-character (maximum) alphanumeric key identifying the name of the wireless local area network. Default is *apcc*.

*Channel* – defines the wireless channel (1-11). Default is 4.

*Key* – defines the authentication key. Default is 1234567890.

## SD Card Sync

This addon sets up the interface for performing external storage into the SD slot (SD card).

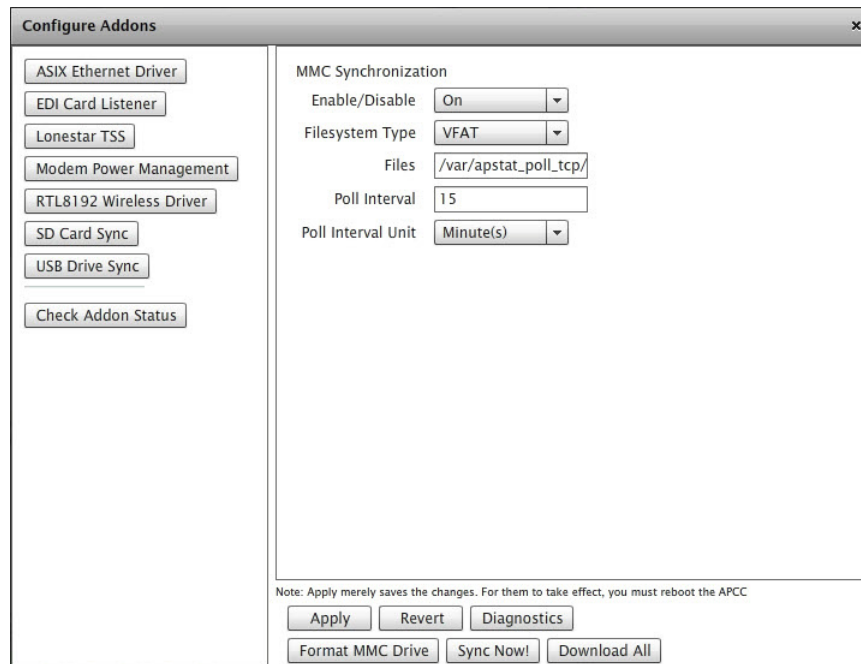


Figure B.6. SD Card Sync window

### Elements

*Enable/Disable* – specifies if element is enabled or disabled. If this field is set to *On*, the addon program starts at boot time. Default is *Off*.

*Filesystem Type* – specifies which storage type is formatted on the APCC, *VFAT*, or *ext2*. This enables proper reading, and also as the basis for the *Format Drive* command button. Default is *VFAT*.

*Files* – defines the space separated list of directories or files to sync. Default is */var/apdiag*.

*Poll Interval* – defines a number of either *Hours/Minutes* (depending on which *Poll Interval Unit* chosen) between auto-syncs. Default is *1*.

*Poll Interval Unit* – specifies *Hours/Minutes*. Default is *Hours*.

## USB Drive Sync

This addon sets up the interface for the performing external storage to a USB thumb drive.

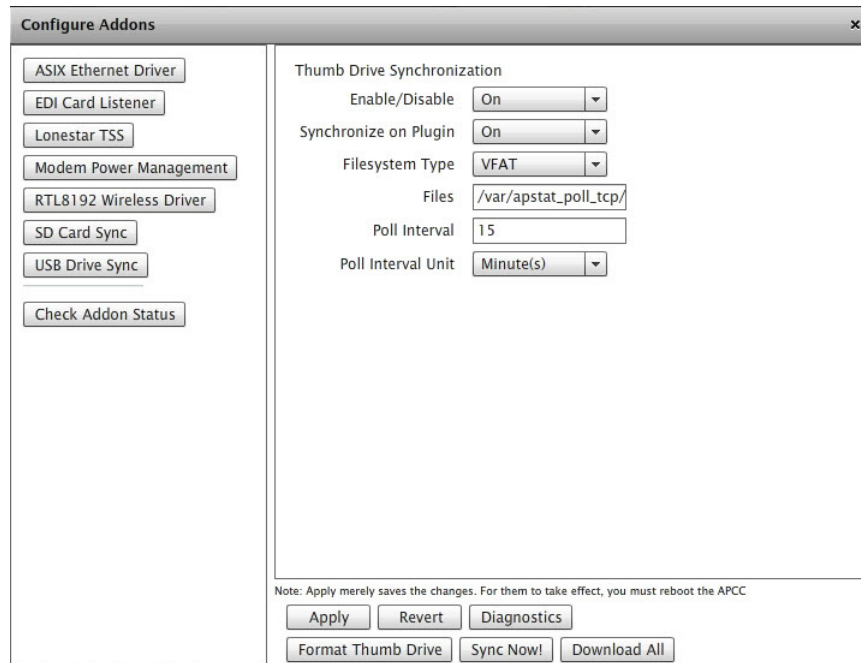


Figure B.7. Thumb Drive Synchronization window

### Elements

*Enable/Disable* – specifies if element is enabled or disabled. If this field is set to *On*, the addon program starts at boot time. Default is *Off*.

*Filesystem Type* – specifies which storage type is formatted on the APCC, *VFAT*, or *ext2*. This enables proper reading and is also the basis for the *Format Thumb Drive* command button. Default is *VFAT*.

*Files* – defines the space separated list of directories or files to sync. Default is */var/apdiag*.

*Poll Interval* – defines a number of either *Hours/Minutes* (depending on which *Poll Interval Unit* chosen) between auto-syncs. Default is 1.

*Poll Interval Unit* – specifies *Hours/Minutes*. Default is *Hours*.

*Synchronize on Plugin* – if set prior to last reboot, this auto-syncs specifies files to the thumb drive when it is initially plugged in. Default is *Off*.

*Format Thumb Drive* – formats the device and causes any existing data to be lost.

*Sync Now!* – writes files to the thumb drive.

*Download All* – shows a listing of the specified files, and enables you to choose which ones to download to local storage (i.e. to the connected laptop, rather than the external storage device).

# Anti-Vandalism

## Overview

This appendix provides information regarding TrafficDOT 2.10.3 anti-vandalism capabilities, which allow for encrypted software downloads for sensors and authentication for data received from sensors.

The anti-vandalism functionality prevents the ability to:

- Download unofficial code
- Insert false detections into a system

## Anti-Vandalism Functionality

The anti-vandalism feature offers the following:

1. All over-the-air software downloads are now encrypted.
  - Once you load the encrypted software onto a sensor or repeater it will no longer accept older or unencrypted software updates.
  - A 128-bit cryptographic signature is used to validate encrypted software.
2. Each sensor now contains a key that is shared between the sensor and the AP.
  - TrafficDOT 2.10.3 software, in conjunction with the access point, automatically manages the generation and distribution of those keys.
  - The access point will not accept controller-bound packets that are not signed with the proper key.
  - Repeaters are keyless and transparent.
  - Signatures and encryption use AES128 federal standard.
3. Intrusion detection:

- The access point analyzes incoming packets looking for unusual or inconsistent information that indicates someone is attempting to manipulate the system.
- Can detect partially, intelligently, or fully jammed RF.
- You can select the type of action to take in case such manipulation is detected. This selection is configured by a drop-down menu in TrafficDOT 2.10.3.

**NOTE:**

These capabilities are available for customers using VDS 2.10.1 for all sensors, repeaters, SPPs, and APCCs. These capabilities will be available for the AP family in VDS 1.8.8. The anticipated release date for VDS1.8.8 is end of September 2014.

## Anti-Vandalism Configuration

By default TrafficDOT configures keys for enabled sensors that are configured and saved to the dot table, and are in the appropriate mode. Refer to *Chapter 5: Setting a Sensor's Operating Mode* for additional information.

You can also manually configure keys if:

- a sensor is configured and in the dot table, but not enabled when *Configure Key* is run, and later, user enables that sensor and wants to set its key
- a sensor is newly configured and saved into the dot table and you want to set its key
- you need to reset a particular sensor's key for any other reason

To configure the anti-vandalism functionality, perform the steps outlined in this section.

### Selecting Anti-Vandalism Option

From the *Advanced* menu option, select **Anti-Vandalism**.

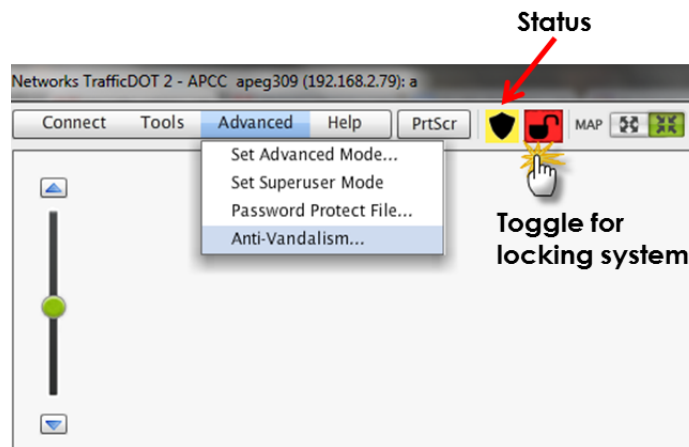


Figure C.1. Selecting Anti-Vandalism option

**IMPORTANT!**

Note that in the previous figure there is an indication of security displayed as a colored shield icon at the top of the screen. Unless you have previously configured keys, TrafficDOT does not display the shield and lock icon at the top of the screen.

The following are the descriptions of the icon colors.

Color	Description
Green	Anti-vandalism and intrusion detection are enabled and the system is locked.
Red	Anti-vandalism is not enabled. The keys are on the AP, but authentication messages are not working properly.
Yellow	Anti-vandalism is enabled and intrusion detection is not enabled, or intrusion detection is enabled but the system is unlocked.
Gray	There is no anti-vandalism information; however, keys exist on the AP.

Table 14. Status icon colors

The lock icon toggles from locked (green) to unlocked (red). When toggling from unlocked from locked, TrafficDOT runs a security check to verify all sensors in the dot table are sending authentication messages.

- If all the sensors are sending authentication messages, you are informed, and the lock index is incremented.
- If not all the sensors are sending authentication messages you are informed and prompted to re-key the sensors in question.

**NOTE:**

You are also informed that authentication messages are not being received due to temporary conditions, such as the sensor not being seen.

## Configuring Key Management

After you select the *Anti-Vandalism* menu option the following screen displays.

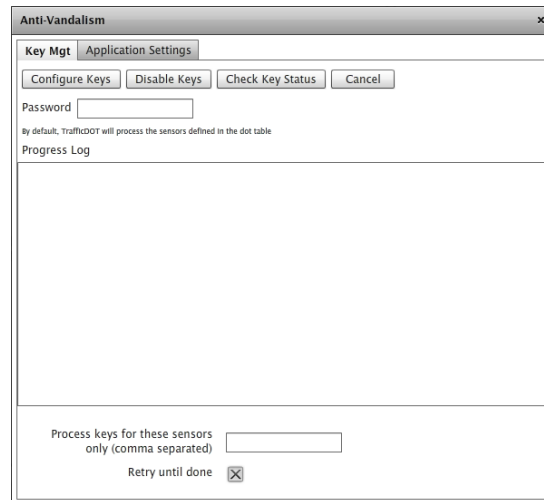


Figure C.14. Anti-Vandalism Key Mgt screen

In order for the anti-vandalism system to work properly, keys need to be distributed to all sensors in the system. The process is managed via the following options:

- *Configure Keys* – Distributes keys to all applicable VDS components
- *Disable Keys* – Turns off anti-vandalism capabilities
- *Check Keys* – Checks the operational status of the sensors' anti-vandalism capabilities
- *Cancel* – Stops any of the above operations
- *Password* – Decrypts internal key
- *Process keys for these sensors only (comma separated)* – Allows for the processing of keys for additional sensors

### Configuring Application Settings

Once the key management process is complete, click the **Applications** tab.



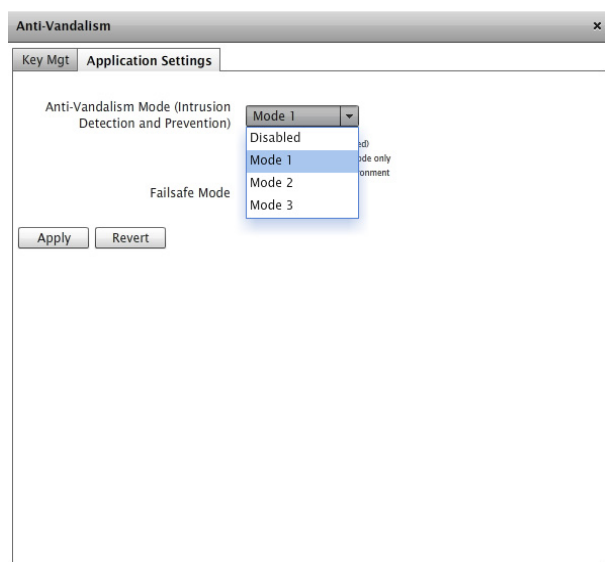


Figure C.15. Application Settings screen

Select one of the following *Anti-Vandalism Intrusion and Protection* modes:

- *Mode 1* – Basic (recommended)
- *Mode 2* – Stop-bar sensor mode only
- *Mode 3* – Mixed sensor environment

**NOTE:**

*Failsafe Mode* shows the action to be taken as a result of vandalism attempts.

Click **Apply** to save your changes.

