AdvanceGuard

Witness Commissioning Guide

Document version 3.0g

NAVTECH RADAR

Contents

Welcome

The Navtech® AdvanceGuard® system provides high integrity detection, tracking and intelligent alarm generation for wide area intrusion detection systems.

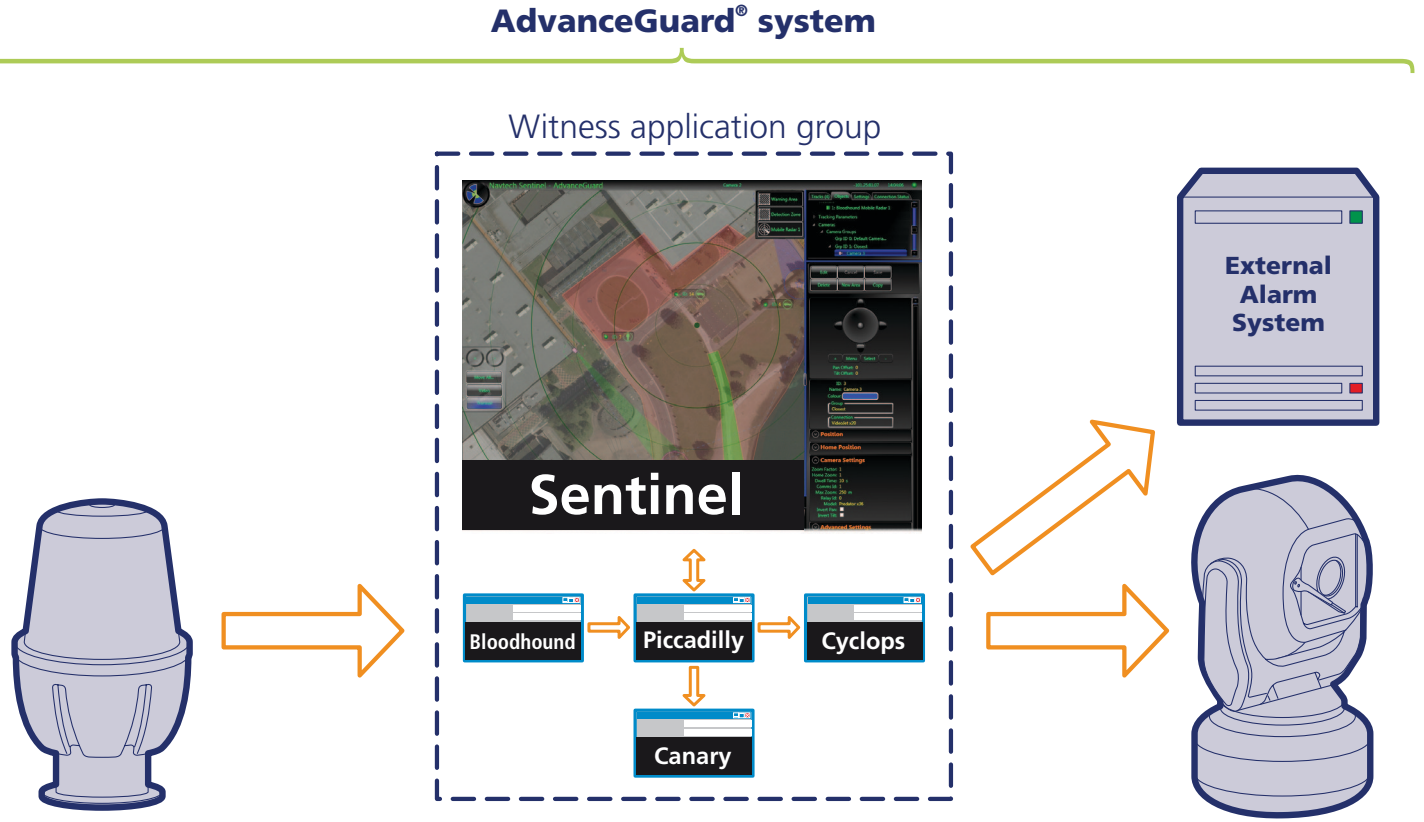
To achieve this feat, the Navtech AdvanceGuard system continually monitors the output from one or more radar sensors. It interprets the data received, intelligently decides when alarms should be raised (based on a set of programmed rules) and controls your Pan/Tilt/Zoom (PTZ) cameras. The result is a system that enables 'dumb' scanning cameras to become intelligent entities which track any targets that are moving within your defined areas of interest.

This guide provides full details about configuring and commissioning the Navtech AdvanceGuard system ready for use.

System overview

The diagram provides a view of the main elements of a complete AdvanceGuard installation: From radar sensor(s), via the software applications, through to the pan/tilt/zoom camera(s).

For a more detailed view of the software applications, please see the next page.



Signals from one or more radar sensors are fed into the Witness application group.

Objects detected by the radar sensor(s) are tracked and, if they coincide with defined areas, coordinate and distance data are calculated for the camera(s).

Control signals/alarm data can be sent to PTZ camera units and/or external alarm systems.

The Witness software components

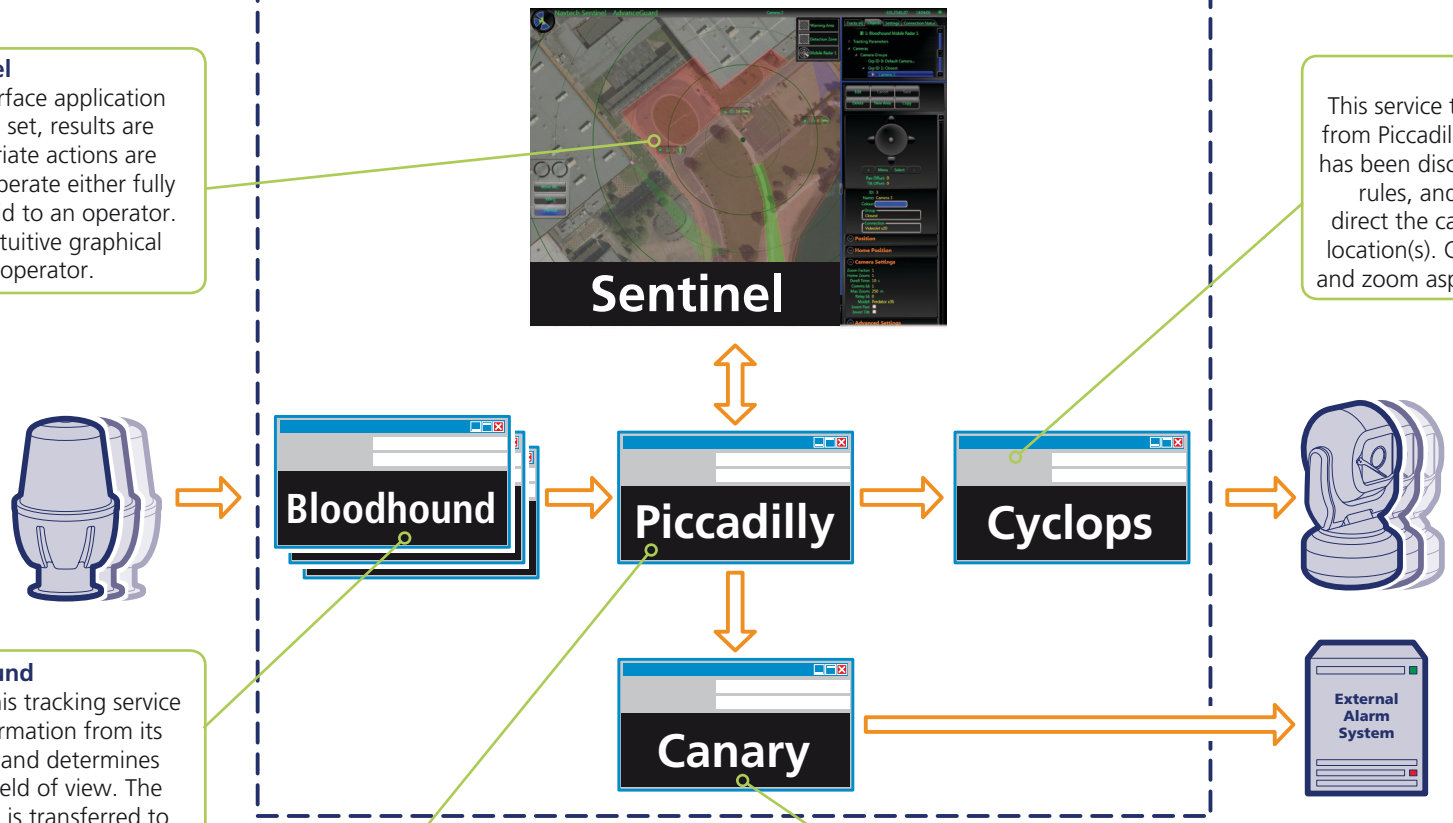
The Witness application group comprises a collection of applications and services, each with their own specialist areas. For the user, the visible component is the Sentinel application. Behind the scenes, the hub of the whole system is Piccadilly, acting as the data server through which all of the other components communicate.

Multiple sensors and cameras

The actions of radar sensors and cameras are not directly linked. Where multiple sensors and/or cameras are installed, a camera will be automatically chosen to respond to an area primarily by its proximity to the target and whether it has an unobstructed view, not because it slavishly responds to a particular radar sensor.

For details of the Sentinel application user interface, please see the next page.

Witness application group



Sentinel

The graphical user interface application where parameters are set, results are displayed and appropriate actions are initiated. Sentinel can operate either fully automatically or as an aid to an operator. Sentinel provides an intuitive graphical interface to the operator.

Cyclops

This service takes positional information from Piccadilly when a potential problem has been discovered, based upon defined rules, and uses the information to direct the camera(s) to view the correct location(s). Cyclops controls the pan, tilt and zoom aspects of all installed cameras.

Bloodhound

One per radar sensor. This tracking service processes the raw information from its allocated radar sensor and determines all objects within the field of view. The interpreted information is transferred to Piccadilly.

Piccadilly

The central hub through which all communications flow. This vitally important data server fulfils multiple roles: It ensures that information is reliably collected from, and delivered to, each of the other components; it maintains the database and configuration details; finally, it handles all of the rule processing that forms the key decision making when searching for potential incidents.

Canary

If an alarm needs to be raised, then Canary Alarm Server can convert the alarm into XML format and deliver it to any appropriate external system. Alongside, Canary Relay can energise one or more relay switches to directly control external equipment such as DVRs, sirens, external alarm systems, etc.

Sentinel user interface layout

The Sentinel application is where you set your parameters for the Witness group and then view real-time results as objects are tracked; all within an intuitive graphical interface.

Navtech menu icon
Click to display a menu of options.

Radar range rings
Concentric circles mark distances around the radar sensor

Tracked object
Click on a tracked object to view further information about it, such as its speed, direction, size, etc.

Quick commands panel
Zoom buttons allow you to alter the view magnification. Other controls are displayed according to the selected items.

Logs and alarms panel
Multiple tabs allow you to switch between lists of alarms, system alarms, logs and results.

Selection panel
Tabbed pages allow you to choose between *Tracks* (a list of detected targets); *Objects* (settings for various key components); *Settings* (various parameters for the Sentinel display) and *Connection Status* (quick indications that all AdvanceGuard components are communicating correctly).

Information panel
This area displays information and options for items that are selected either within the selection panel above or the site map.
In the panel shown left, the information displayed is related to the highlighted radar sensor within the site map.

Site map
Displays the radar scan(s), defined area(s), tracked targets and camera positions. Using the mouse pointer you can select items to view more detail or make parameter changes. A satellite image, map or scaled diagram of the scan region can be displayed as a background image. To move around the area, click and drag on any part of the background image.

Configuration

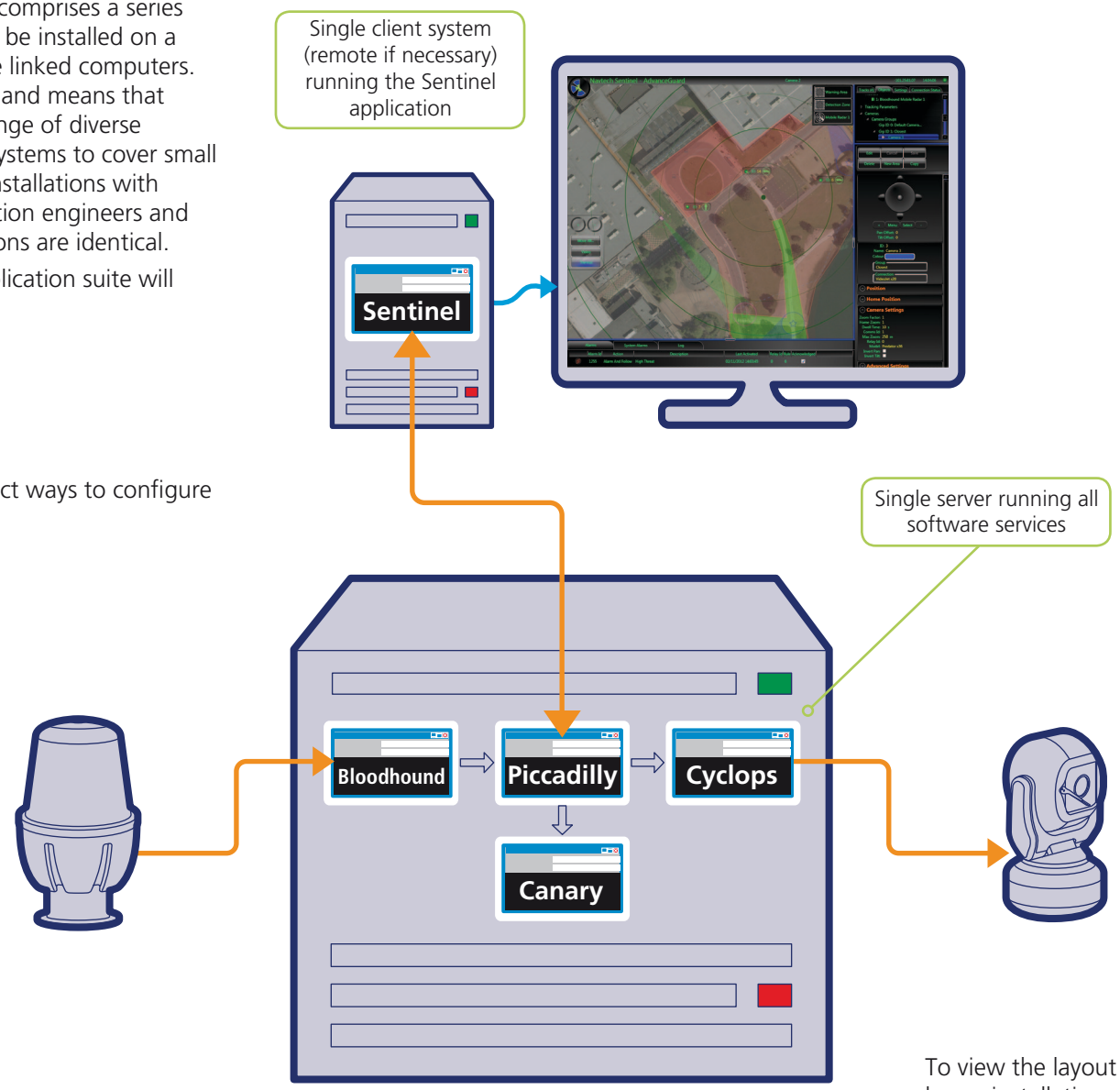
Module distribution: Small and large installations

As described within the Welcome section, the heart of the system comprises a series of (Witness) application modules, most of which could conceivably be installed on a single computer but in reality are distributed between two or more linked computers. The modular nature of the software provides unbeatable flexibility and means that the same application group can be configured to service a wide range of diverse installations. With hardware to suit, you can create cost effective systems to cover small areas at one end of the spectrum, rising to full coverage of large installations with complex mixes of sensors and cameras. The crucial fact for installation engineers and users alike is that the techniques used for small and large installations are identical.

The exact manner in which you configure and run the Witness application suite will generally be determined by the following factors:

- The number of radar sensors providing scanning data,
- The number of cameras to be controlled,
- The number and location of the operator(s),
- The distances between the sensor(s), camera(s) and operator(s).

The diagrams shown here and on the next page provide two distinct ways to configure the system as determined by the factors outlined above



Small installations

This installation could be viable where only a single radar sensor and a single PTZ camera are used. Here, all of the Witness system background services are installed on a single server computer while the Sentinel user interface is used on a client system linked to the server via an Ethernet connection.

Connections key

Ethernet link

Video link

To view the layout of a larger installation, please see the next page.

Larger installations

For installations that require multiple radar sensors, cameras and/or operators it becomes practical to install and run the various applications on their own dedicated computers. Ethernet connections (either dedicated links or within existing infrastructure) are used to form the data pathways between the various computers and devices.

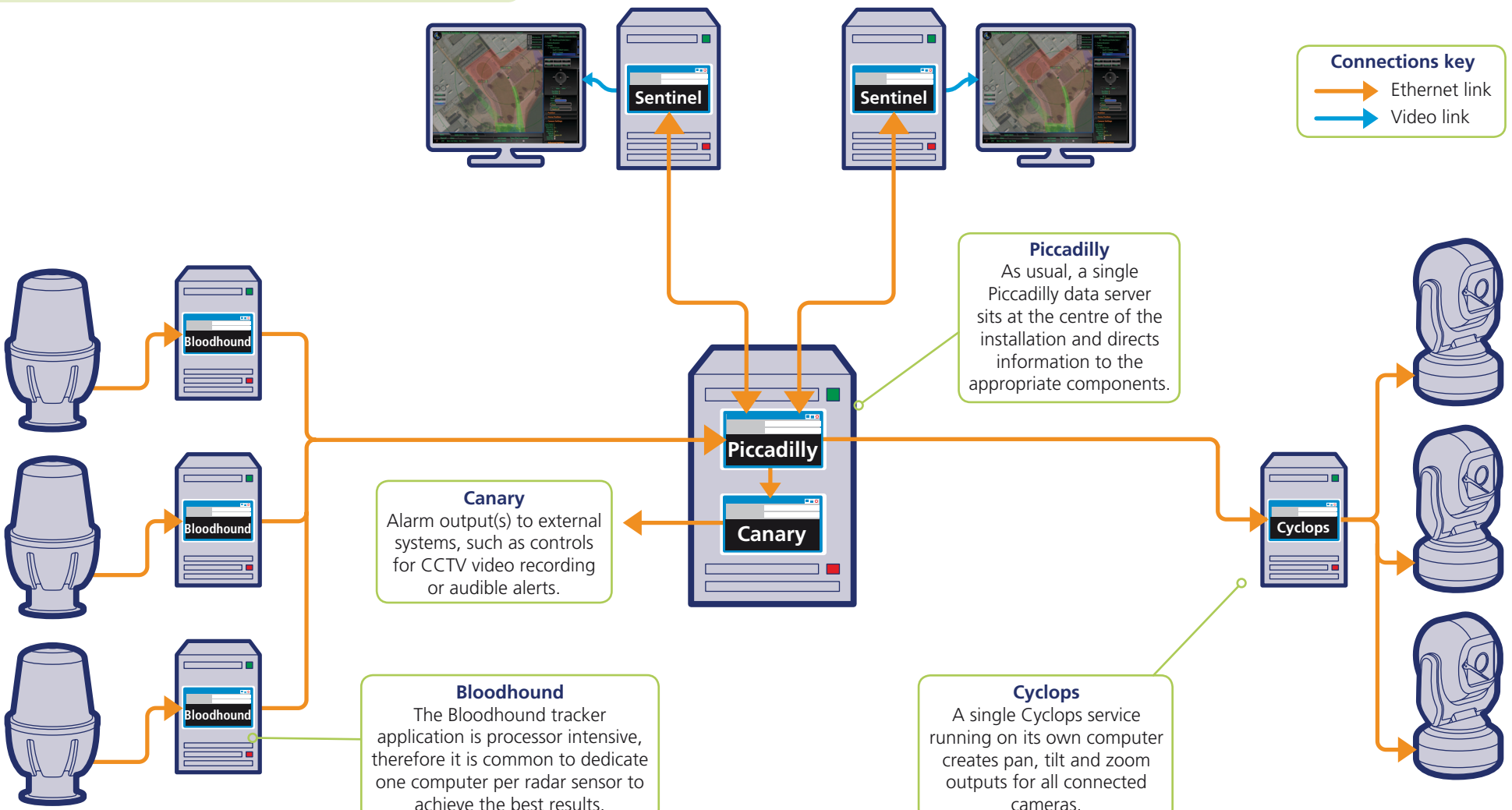
As these installations, by their nature, will often be of a mission critical nature, it is strongly recommended that all system layouts are correctly designed in order to minimise vulnerabilities. This includes security arrangements, power integrity (via UPS systems), regular data back ups plus data redundancy, which is discussed on the next page.

Sentinel

Where multiple operators are required, duplicate Sentinel installations may be created. The display characteristics can be customised to suit each operator.

Timing

It is vital that the individual systems comprising a complete installation are all timesynced to within millisecond accuracy in order to avoid false readings and the risk of missed observations.



Piccadilly

As usual, a single Piccadilly data server sits at the centre of the installation and directs information to the appropriate components.

Canary

Alarm output(s) to external systems, such as controls for CCTV video recording or audible alerts.

Bloodhound

The Bloodhound tracker application is processor intensive, therefore it is common to dedicate one computer per radar sensor to achieve the best results.

Cyclops

A single Cyclops service running on its own computer creates pan, tilt and zoom outputs for all connected cameras.

Creating data redundancy within the system

As mentioned previously, the core of any installation is formed by the Piccadilly module and its valuable database. For mission critical installations it is recommended to ensure data duplication and redundancy within the system. Due to the modular and flexible nature of the Witness applications, creating systems with in-built data redundancy is straightforward and can be achieved in a number of ways:

- Independent Piccadilly servers
- Paralleled Piccadillys with common database
- Fully replicated systems

Group name, Auto discovery and Piccadilly priority

These three related key features make data redundancy a straightforward task within the Witness group of applications.

The *Group name* option allows you to associate the various modules (Bloodhound, Sentinel, Cyclops and Canary) with Piccadilly through the use of a unique name, as opposed to using the network address of the Piccadilly server. The Group name option becomes available once the *Auto discovery* option is enabled on each module. With *Auto discovery* enabled, each module will search for and connect with the appropriately named Piccadilly server.

The option that actually enables data redundancy is the *Priority* setting within each instance of Piccadilly. A priority of **1** designates a Piccadilly server as a primary unit; a priority of **2** designates it as a secondary unit, 3 denotes a tertiary unit, etc. When other modules perform their Group name search for a Piccadilly server, they will initially seek a priority level of **1**. If a primary unit cannot be located, they will search for a priority of **2**, and so on.

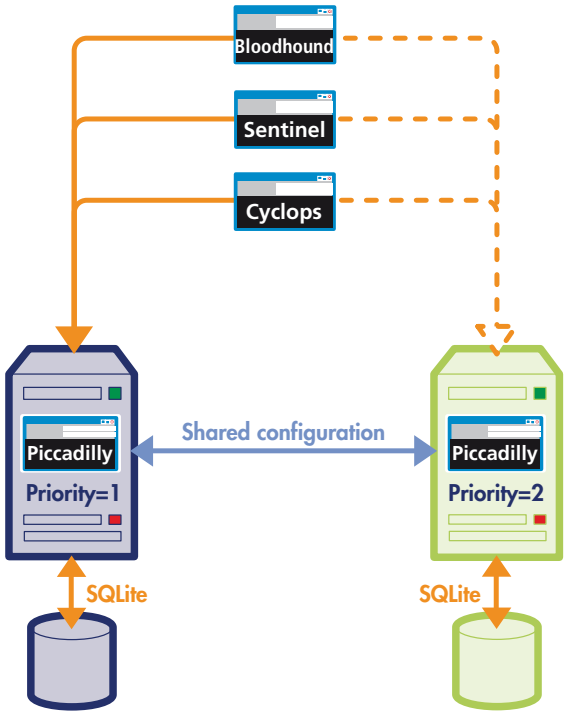
This hierarchical search action occurs automatically whenever communication is lost between Piccadilly and a related module. Thus, if any instance of Piccadilly becomes unavailable, operation will failover to the next available Piccadilly server.

Independent Piccadilly servers

This is the simplest and lowest cost method of creating data redundancy within the system. It requires two separate Piccadilly servers, each with their own database.

If the primary Piccadilly server fails, the other modules search for and failover to the secondary Piccadilly using the Group name, Auto discovery and Priority features described in the text box (left).

The disadvantage of this method is that the failover is not seamless. The databases of the primary and secondary Piccadilly servers are not duplicated; the secondary unit remains semi dormant until failover occurs, whereupon it begins operating in the same manner as the primary unit but without the benefit of the historical data. After a short period of operation, the secondary unit populates its own datalogs.

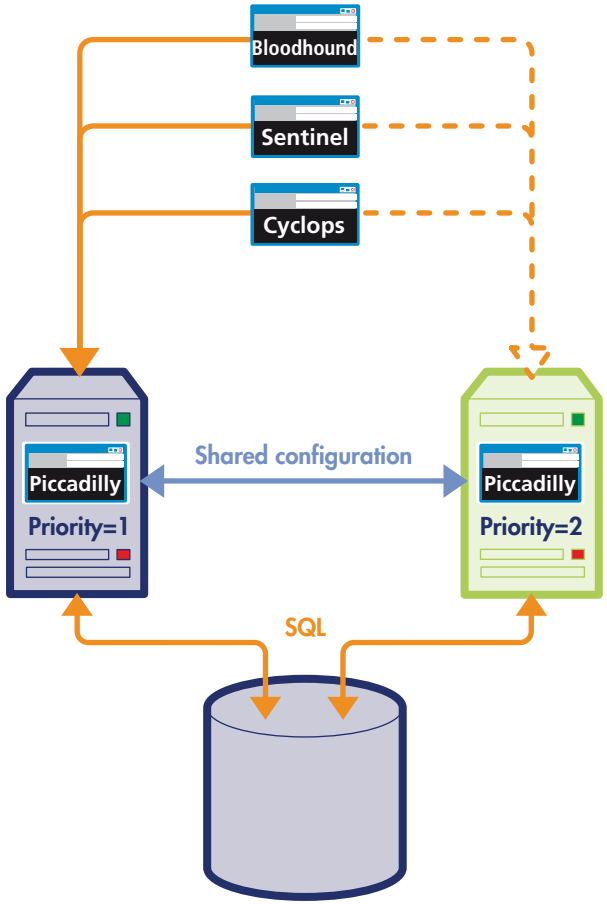


continued

Paralleled Piccadillys with common database

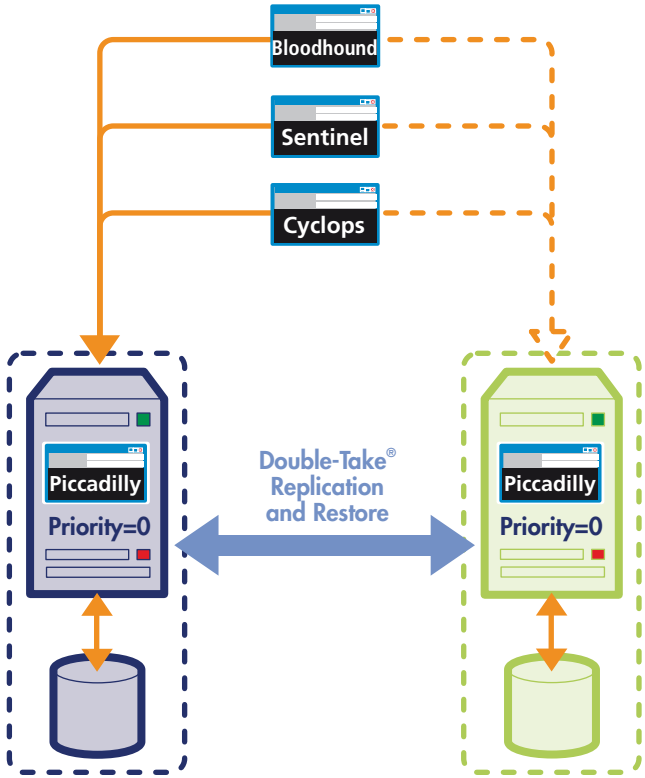
This method improves upon the previously described scheme because it makes use of a common database that is accessible by both Piccadilly servers. This means that if the primary server is lost, the secondary Piccadilly unit can takeover more or less immediately and use exactly the same historical data.

This implementation requires the use of full SQL as the access method between the Piccadilly servers and the common database. As required, the common database can be separately protected using standard data redundancy techniques, such as RAID.



Fully replicated systems

A third method uses a third party application such as Double-Take® to completely replicate the Piccadilly server and its database. In this case all configuration and operational data replication is handled in realtime by the third party application. The application also controls the switchover between the servers in the case of failure and so the Piccadilly priority system is not used.



Creating a new Witness group installation

As explained earlier in this guide, the Witness group comprises five main modules: Four hidden services plus the Sentinel user interface application. This section deals with installing and preparing each one to correctly coexist and to share data.

To alter a current Witness system, see Modifying an existing Witness group installation.

Software installation

The Witness group application and services are provided with an automated installer either on CD-ROM or packaged file for online distribution.

Generally, the Witness group services are installed on at least one server-type computer. Meanwhile the Witness group user application, Sentinel, is usually installed on a separate client system which connects to the server(s) via a network link. Where multiple radar sensors and cameras are used within the installation, the various services are split onto separate server machines. See Module distribution: Small and large installations.

IMPORTANT: Service account - During the installation process the installer will add a new Windows account for the services using the *Service Username* that you enter within the Service setup page (by default this is set as *Witness*). Be sure not to delete this new account or to use it as a standard logon account on the computer. There could be serious security implications and other possible problems if logged on users and the Witness services share the same account. **Always use a separate user account.**

You first need to determine where each service and application will be installed. It is not uncommon for all of the services except for Bloodhound to be installed on one server. Then separate instances of Bloodhound (the most processor and communication intensive of all the services) are installed on one or more dedicated servers.

For details about minimum and recommended computer hardware specifications, see Appendix 10 - Computer hardware recommendations.

Installation issues

- **Admin rights** – When running the Witness Suite Setup application, you must have local administration rights within Windows on the installation computer.
- **Security settings** – Certain security settings and security software can interfere with the installation and operation of Witness. If you experience any problems during installation please consult the Troubleshooting section at the end of this guide.
- **Prerequisites** – The following items are required on the installation computer:
  - MS .NET 4.0 Extended must be pre-installed.
  - MS Visual C++ 2010 x86 (for both x64 and x86 systems)
  - Other pre-requisites may be required depending on optional third-party software used, such as the camera viewers.

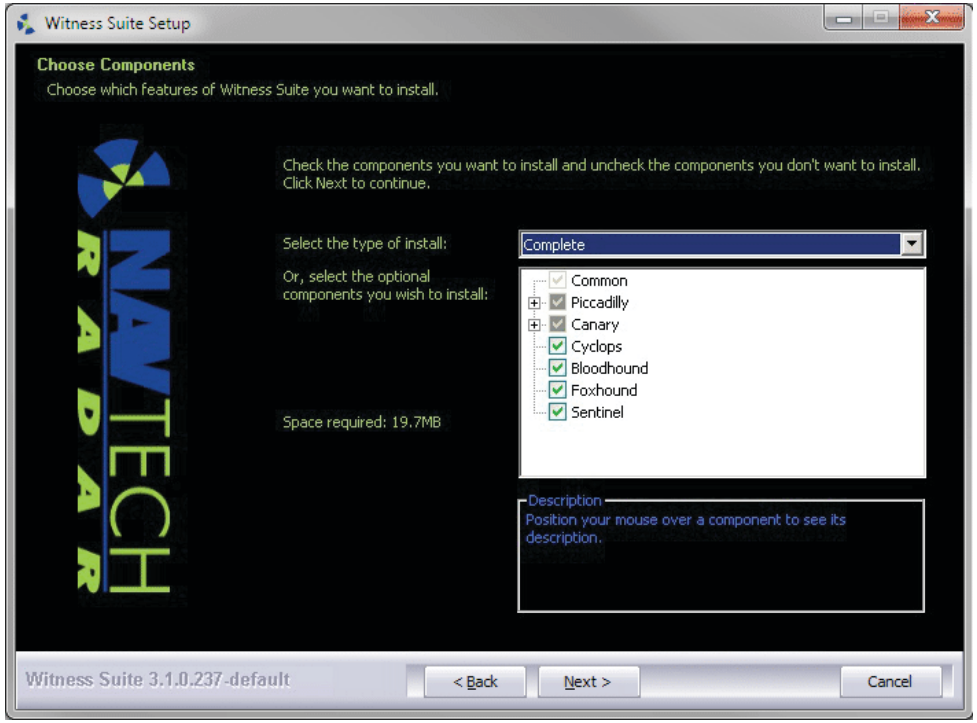
  Note: The installer will inform you if any prerequisite items are missing.

To install the Witness group

1 From the Witness group CD-ROM or USB stick (or packaged file), run the **Witness Suite x.x.x.yyyy Setup.exe** file on the client or server system. *Where x.x.x.yyyy is the version number*.

Note: If a Witness installation already exists on the system, you will first see a Maintenance screen which will provide four choices: Modify, Repair, Remove and Continue setup. For details, see Modifying an existing Witness group installation.

2 Once the licence agreement has been viewed and accepted, you will be prompted to choose the components to install:



*Note: The **Foxhound** module is not used for AdvanceGuard installations.*

continued

3 The most straightforward installation method is to use the *Select the type of install:* drop down box to determine which components need to be installed on the current computer, choices are:

- **Complete** - Installs all components.
- **Server** - Installs only the Piccadilly server component. Use this option when the current computer will act as the central server.
- **Bloodhound** - Installs only the Bloodhound component. Use this option when the current computer will act as a controller for a radar sensor.
- **Foxhound** - Not required for AdvanceGuard installations.
- **Client** - Installs only the Sentinel component. Use this option when the current computer will be used as an operator system.
- **Custom** - Allows you to choose which components are installed (see below).

Choosing custom components

When you set the '...type of install:' to be Custom, you can include or exclude any of the Witness components to suit your installation. The components include:

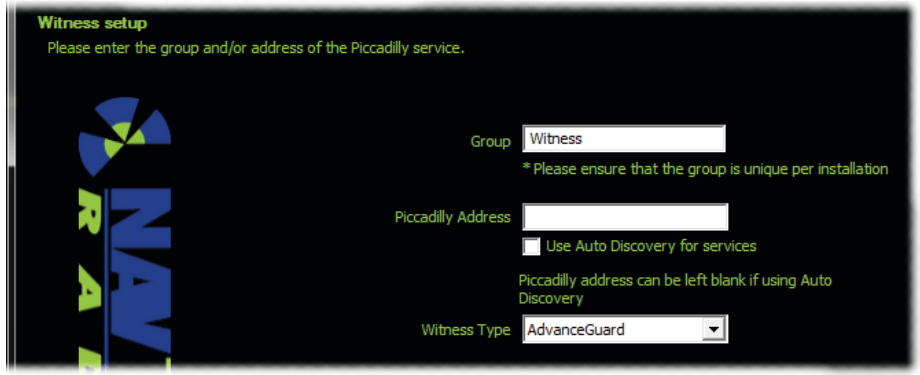
- **Piccadilly** - Installs the Piccadilly data server. Sub-options include the database management type to be used by Piccadilly. Choose the appropriate database option for your installation: *SQL Server* or *SQLite*.
  - *SQL Server* provides full support for client/server operation and is used when the database is located separately from the computer(s) running Piccadilly (as shown in the example Paralleled Piccadillys with common database).
  - *SQLite* offers a subset of SQL server command structure and is generally used when the database is located on the same computer as the Piccadilly server(s) (as shown in the example Independent Piccadilly Servers).
- **Canary** - Installs the Canary alarm module. Sub-options include Plugins for the various hardware interfaces that are supported.
- **Cyclops** - Installs the camera control module.
- **Bloodhound** - Installs the Bloodhound radar controller/tracker module.
- **Foxhound** - Not required for AdvanceGuard installations.
- **Sentinel** - Installs the Sentinel user interface module.

4 Choose the appropriate installation (or pick the components individually) and click the **Next** button.

You will be prompted to choose the installation location:

5 Click **Browse** to find a new destination folder or click the **Next** button to continue with the suggested location.

6 Confirm the location for the installation files and click the **Next** button. You will be prompted configure the group details:



7 Choose a suitable *Group* name for the installation. The default name is *Witness*. Whichever name is used, it is imperative that all systems that form the installation (i.e. server(s), client(s), bloodhound systems, etc.) all use exactly the same *Group* name and that no other installation, which could be commonly networked, uses the same name.

8 Either:

- Enter a valid network address for the Piccadilly server in the *Piccadilly Address* box,

  OR

- Tick the *Use Auto Discovery for services* checkbox to request that all modules locate Piccadilly using the common *Group* name.

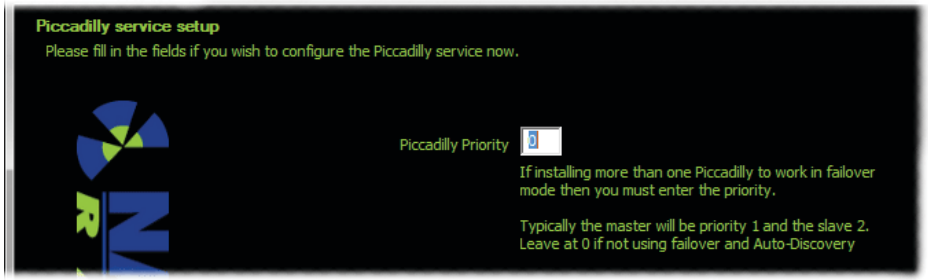
  Note: Do not enter a network address AND tick the auto discovery checkbox.

continued

9 Choose the type of Witness installation: Choose *AdvanceGuard* for security installations. The *ClearWay* option is used for highway monitoring.

10 Click the **Next** button.

- If the Piccadilly module option was not ticked, then please jump to step 11.
- If you have chosen to include the Piccadilly module you will next be asked to confirm the *Piccadilly Priority*:

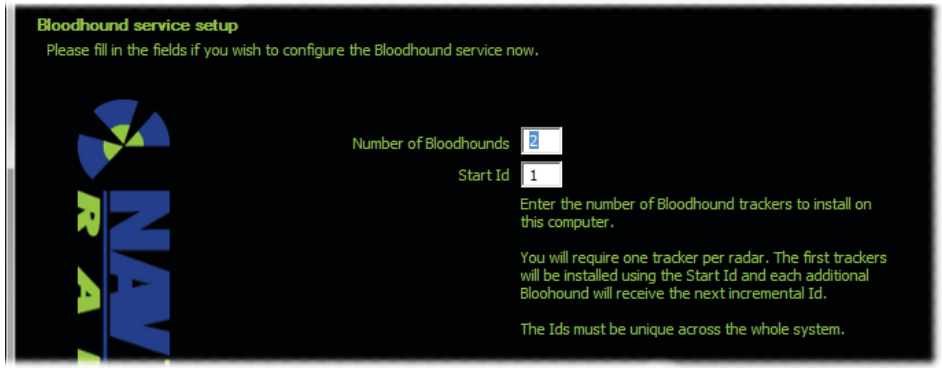


The *Piccadilly Priority* option allows modules to locate and use the correct instance of Piccadilly within installations which employ the redundancy (*Failover*) feature. Choose **1** to make this instance of Piccadilly a master and **2** to make it a slave.

IMPORTANT: If you are using only a single Piccadilly (or system redundancy is provided by a fully replicated system approach), leave this option as **0**.

11 Click the **Next** button.

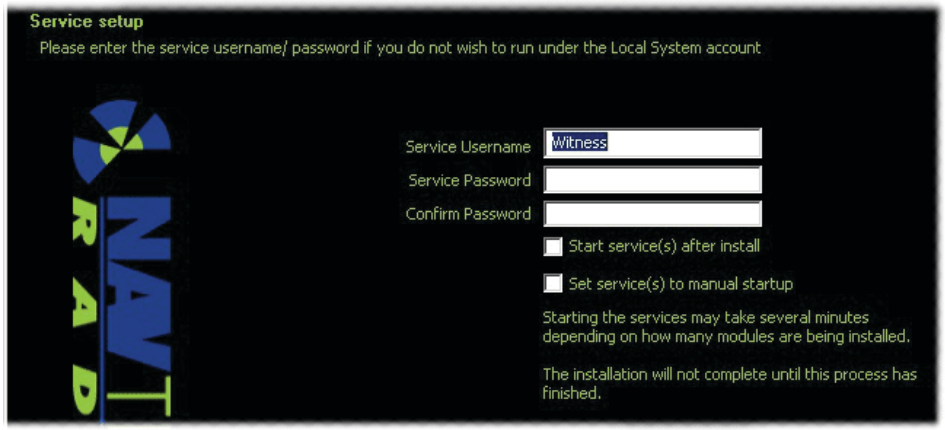
- If the Bloodhound module option was not ticked, then please jump to step 12.
- If you have chosen to include the Bloodhound module you will next be asked to confirm the *Number of Bloodhounds* and their *Start Ids*:



Confirm the number of Bloodhound modules that you wish to install on **this** computer. Every radar sensor requires a separate Bloodhound tracker module, sometimes on the same computer (see Appendix 10 - Computer hardware recommendations) or often on separate computers.

Every Bloodhound module within a complete Witness system (whether or not they are on the same computers) must be given a unique identity number. Use the *Start Id* entry to confirm the identity number that should be applied to the first of the Bloodhound modules on **this** computer. Be sure to check that identity numbers are never duplicated within the overall system.

12 Unless you are creating a Sentinel-only client system, you will next be prompted to define a *Service Username* and *Service Password* that will be used to create a new Windows system account for use by the Witness service modules:



13 Enter an appropriate *Service Username* (or retain the default *Witness* name). Also enter and confirm a suitable password for the new Windows account (see the important notes below).

14 If you wish to start the Witness system immediately after installation, tick the checkbox *'Start service(s) after install'*.

15 Click the **Next** button. The installation/update will commence using the chosen settings and will report when it is complete.

Important notes on accounts and passwords

- During the installation process the installer will add a new Windows account for the services using the *Service Username* that you enter within the Service setup page (by default this is set as *Witness*). Be sure not to delete this new account or to use it as a standard logon account on the computer. There could be serious security implications and other possible problems if logged on users and the Witness services share the same account. **Always use a separate user account.**
- After installation, do not alter the password that was set within the Services setup screen for the new Windows service account. Doing so will prevent the installed Witness services from accessing the Windows account.

Modifying an existing Witness group installation

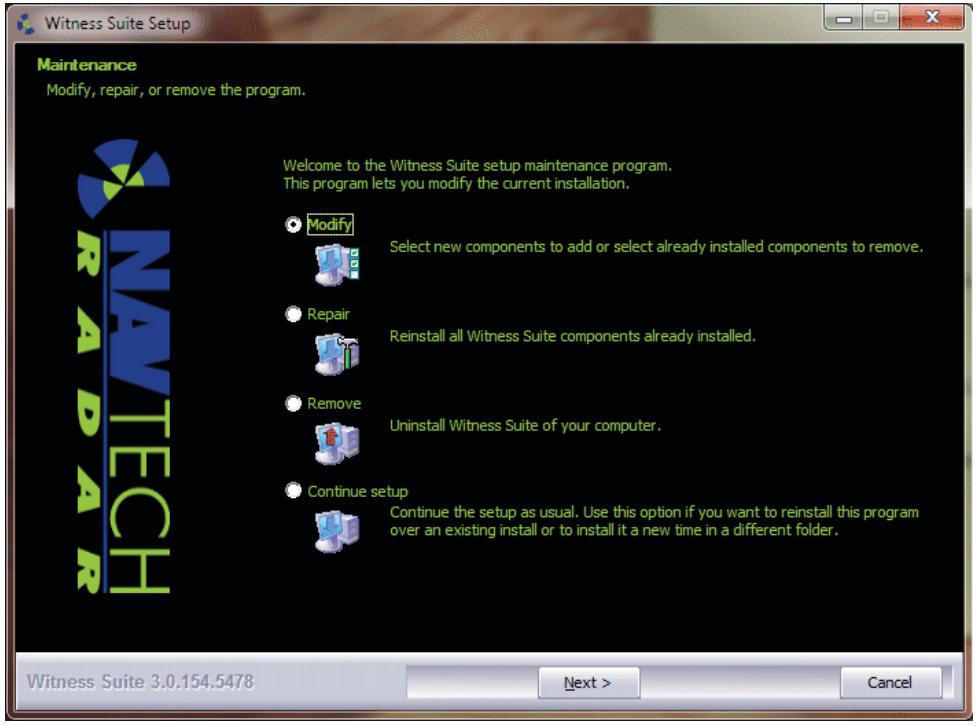
This section deals with modifying, repairing and removing an existing Witness installation.

To install a new Witness system, see Creating a new Witness group installation.

To modify a Witness group installation

1 From the Witness group CD-ROM or USB stick (or packaged file), run the **Witness Suite x.x.x.yyyy Setup.exe** file on the client or server system. *Where x.x.x.yyyy is the version number*.

Once the existing installation is located by the Witness Suite Setup program, you should see a screen similar to the following that offers four choices: *Modify*, *Repair*, *Remove* and *Continue* setup:

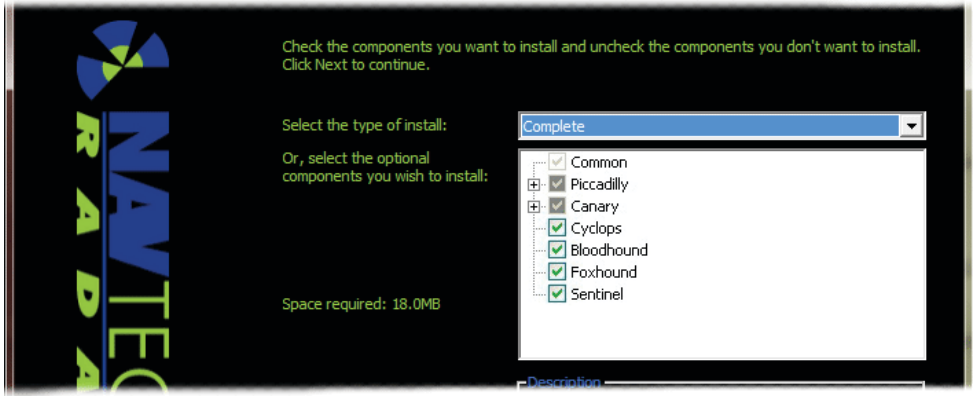


- To add new components or remove only selected components, choose **Modify**.
- To overwrite (upgrade/reinstall) all existing components, choose **Repair**.
- To uninstall the whole existing Witness system, choose **Remove**.
- To proceed with a standard installation, choose **Continue setup** (see Creating a new Witness group installation).

2 Choose the required option and click the **Next** button.

Modify option

If you chose the *Modify* option, you will be presented with the following screen:



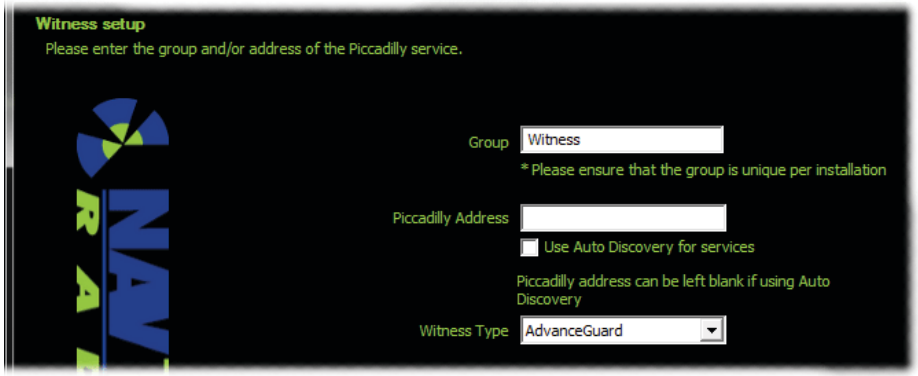
a Choose the components that you wish to add and/or remove. If a component is ticked and you untick it, that component will be removed in the subsequent steps. If an item is unticked and you tick it, that component will be installed.

Choosing custom components

When you set the '...type of install:' to be Custom, you can include or exclude any of the Witness components to suit your installation. The components include:

- **Piccadilly** - Installs the Piccadilly data server. Sub-options include the database management type to be used by Piccadilly. Choose the appropriate database option for your installation: *SQL Server* or *SQLite*.
  - *SQL Server* provides full support for client/server operation and is used when the database is located separately from the computer(s) running Piccadilly (as shown in the example Paralleled Piccadillys with common database).
  - *SQLite* offers a subset of SQL server command structure and is generally used when the database is located on the same computer as the Piccadilly server(s) (as shown in the example Independent Piccadilly Servers).
- **Canary** - Installs the Canary alarm module. Sub-options include Plugins for the various hardware interfaces that are supported.
- **Cyclops** - Installs the camera control module.
- **Bloodhound** - Installs the Bloodhound radar controller/tracker module.
- **Foxhound** - Not required for AdvanceGuard installations.
- **Sentinel** - Installs the Sentinel user interface module.

b Make your selections and click the **Next** button. You will be prompted configure the group details:



c Choose a suitable *Group* name for the installation. The default name is *Witness*. Whichever name is used, it is imperative that all systems that form the installation (i.e. server(s), client(s), bloodhound systems, etc.) all use exactly the same *Group* name and that no other installation, which could be commonly networked, uses the same name.

d Either:

- Enter a valid network address for the Piccadilly server in the *Piccadilly Address* box,

  OR

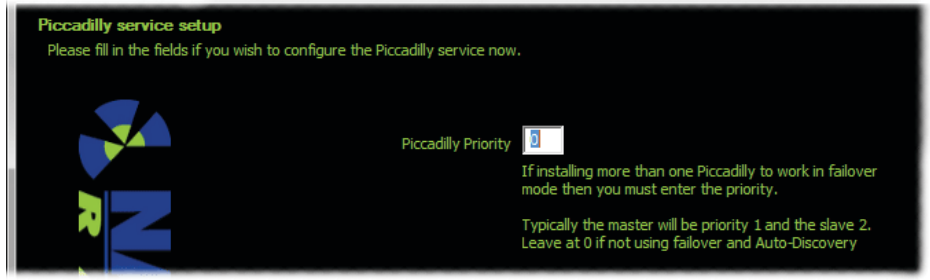
- Tick the *Use Auto Discovery for services* checkbox to request that all modules locate Piccadilly using the common *Group* name.

  Note: Do not enter a network address AND tick the auto discovery checkbox.

e Choose the type of Witness installation: *AdvanceGuard* (for highway monitoring) or *AdvanceGuard* (for security installations).

f Click the **Next** button.

- If the Piccadilly module option was not ticked, then please jump to step g.
- If you have chosen to include the Piccadilly module you will next be asked to confirm the *Piccadilly Priority*:

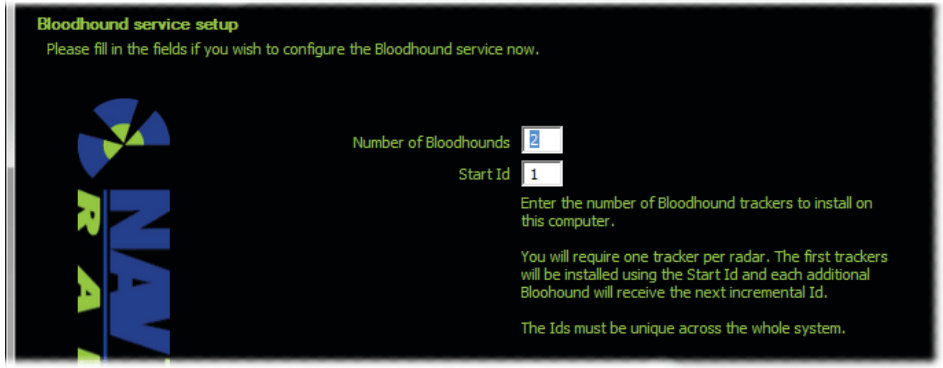


The Piccadilly Priority option allows modules to locate and use the correct instance of Piccadilly within installations which employ the redundancy (Failover) feature. Choose **1** to make this instance of Piccadilly a master and **2** to make it a slave.

IMPORTANT: If you are using only a single Piccadilly (or system redundancy is provided by a fully replicated system approach), leave this option as **0**.

g Click the **Next** button.

- If the Bloodhound module option was not ticked, then please jump to step h.
- If you have chosen to include the Bloodhound module you will next be asked to confirm the *Number of Bloodhounds* and their *Start Ids*:

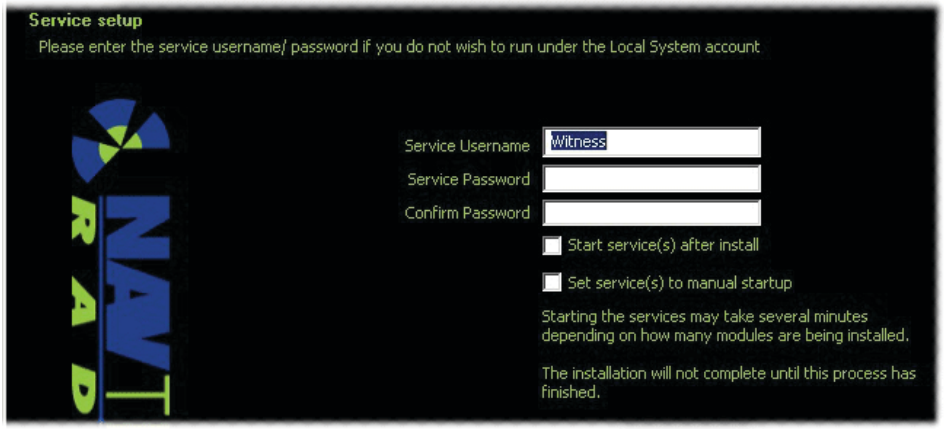


Confirm the number of Bloodhound modules that you wish to install on this computer. Every radar sensor requires a separate Bloodhound tracker module, sometimes on the same computer (see Appendix 10 - Computer hardware recommendations) or often on separate computers.

Every Bloodhound module within a complete Witness system (whether or not they are on the same computers) must be given a unique identity number. Use the Start Id entry to confirm the identity number that should be applied to the first of the Bloodhound modules on this computer. Be sure to check that identity numbers are never duplicated within the overall system.

continued

h Click the **Next** button. Unless you are modifying a Sentinel-only client system, you will next be prompted to define a *Service Username* and *Service Password* that will be used to create a new Windows system account for use by the Witness service modules:



i Enter an appropriate Service Username (or retain the default Witness name). Also enter and confirm a suitable password for the new Windows account (see the important notes below).

j If you wish to start the Witness system immediately after installation, tick the checkbox *'Start service(s) after install'*.

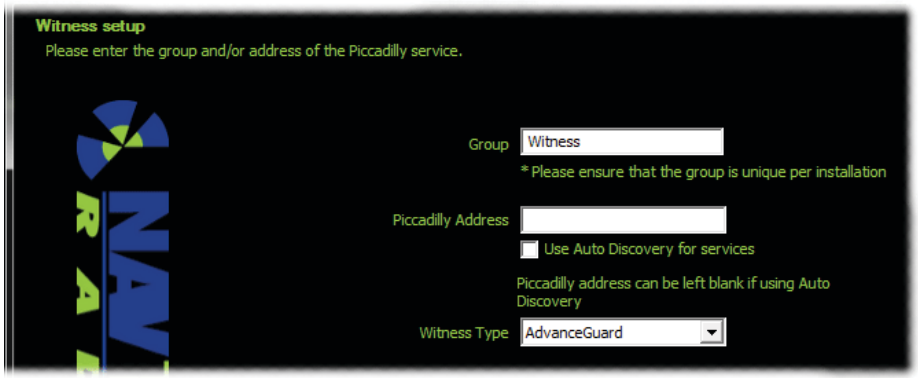
k Click the **Next** button. The installation/update will commence using the chosen settings and will report when it is complete.

Important notes on accounts and passwords

- During the installation process the installer will add a new Windows account for the services using the *Service Username* that you enter within the Service setup page (by default this is set as *Witness*). Be sure not to delete this new account or to use it as a standard logon account on the computer. There could be serious security implications and other possible problems if logged on users and the Witness services share the same account. **Always use a separate user account.**
- After installation, do not alter the password that was set within the Services setup screen for the new Windows service account. Doing so will prevent the installed Witness services from accessing the Windows account.

Repair option

a If you chose the *Repair* option, you will first be prompted to check/reconfigure the group details:



b Confirm or alter the *Group* name for the installation. It is imperative that all systems that form the installation (i.e. server(s), client(s), bloodhound systems, etc.) all use exactly the same *Group* name and that no other installation, which could be commonly networked, uses the same name.

c Either:

- Confirm/enter a valid network address for the Piccadilly server in the *Piccadilly Address* box,

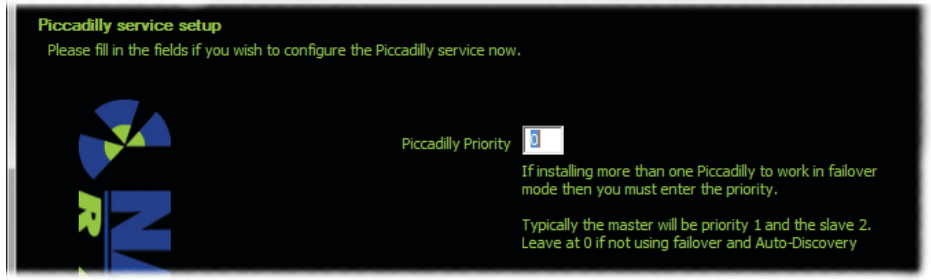
  OR

- Tick the *Use Auto Discovery for services* checkbox to request that all modules locate Piccadilly using the common *Group* name.

  Note: Do not enter a network address AND tick the auto discovery checkbox.

d Click the **Next** button.

- If the Piccadilly module option was not previously installed, then please jump to step e.
- If the Piccadilly module is present, you will next be asked to confirm the *Piccadilly Priority*:

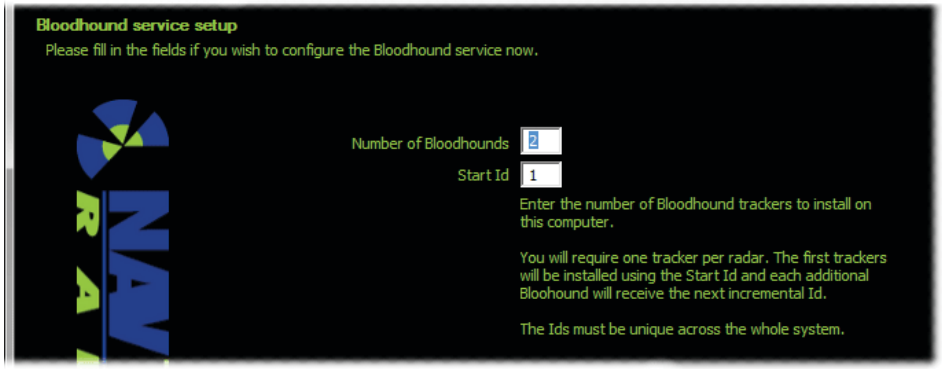


The Piccadilly Priority option allows modules to locate and use the correct instance of Piccadilly within installations which employ the redundancy (Failover) feature. Choose **1** to make this instance of Piccadilly a master and **2** to make it a slave.

IMPORTANT: If you are using only a single Piccadilly (or system redundancy is provided by a fully replicated system approach), leave this option as **0**.

e Click the **Next** button.

- If the Bloodhound module was not previously installed, then please jump to step f.
- If the Bloodhound module is present you will next be asked to confirm the *Number of Bloodhounds* and their *Start Ids*:

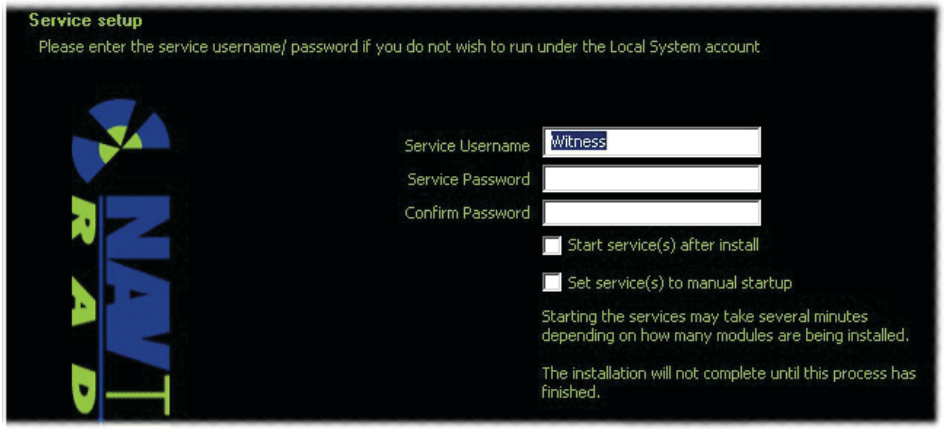


Confirm the number of Bloodhound modules that are present or that you wish to install on this computer. Every radar sensor requires a separate Bloodhound tracker module, sometimes on the same computer (see Appendix 10 - Computer hardware recommendations) or often on separate computers.

Every Bloodhound module within a complete Witness system (whether or not they are on the same computers) must be given a unique identity number. Use the Start Id entry to confirm the identity number that should be applied to the first of the Bloodhound modules on this computer. Be sure to check that identity numbers are never duplicated within the overall system.

continued

f Click the **Next** button. Unless you are repairing a Sentinel-only client system, you will next be prompted to confirm/define a *Service Username* and *Service Password* that will be used to create a new Windows system account for use by the Witness service modules:



g Confirm /enter the Service Username. Also enter and confirm a suitable password for the new Windows account.

h If you wish to start the Witness system immediately after installation, tick the checkbox *'Start service(s) after install'*.

i Click the **Next** button. The repair will commence using the chosen settings and will report when it is complete.

Remove option

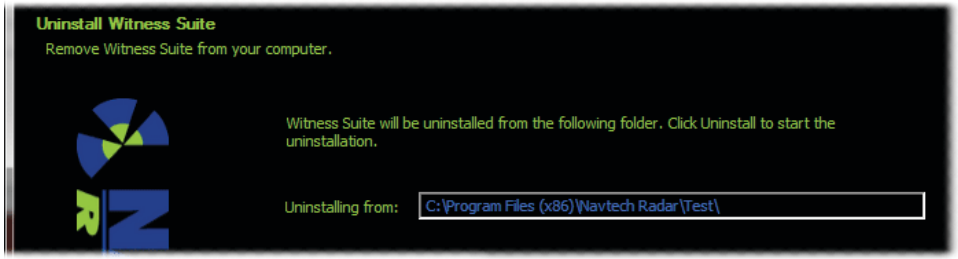
IMPORTANT: Take great care when using the Remove option. In addition to all modules being removed, it is possible to delete all database logs and backup configurations with no option of recovery. You are recommended to take backups of all required data before going ahead with the remove option.

a If you chose the *Remove* option, the Uninstall Wizard will be invoked:

b You can now choose to retain the existing configuration file and/or database after the remove procedure has been completed:

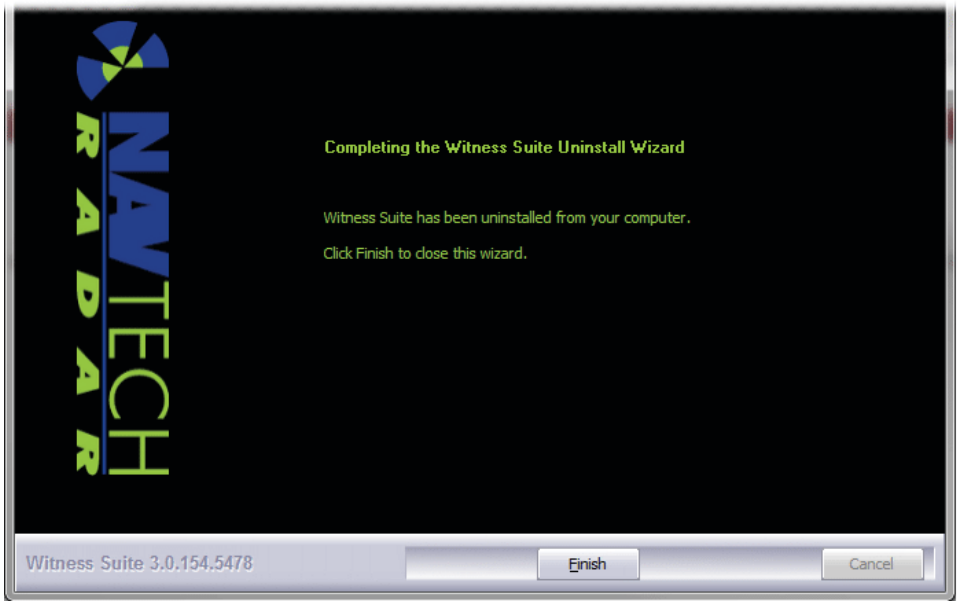
- Where a new installation will be required to follow a similar configuration, tick the 'Leave configuration file after uninstall' checkbox.
- Where a new installation will be required to continue using the current database files, tick the 'Leave database file after uninstall' checkbox.

c Click the **Next** button. You will be presented with the folder location that is to be removed. Take a moment to check that this is the correct Witness installation to be removed:



d When you are sure, click the **Uninstall** button. The chosen Witness installation will be removed and the following screen will be displayed when the process is complete.

e Click the **Finish** button to exit.



Note: The Uninstall Wizard will not remove the Windows service account that was previously created. If no further Witness installations are required on this system then you need to remove the service account using standard Windows procedures.

Creating additional User Accounts

During the Witness installation, three Windows user groups are created with a single user account in each group:

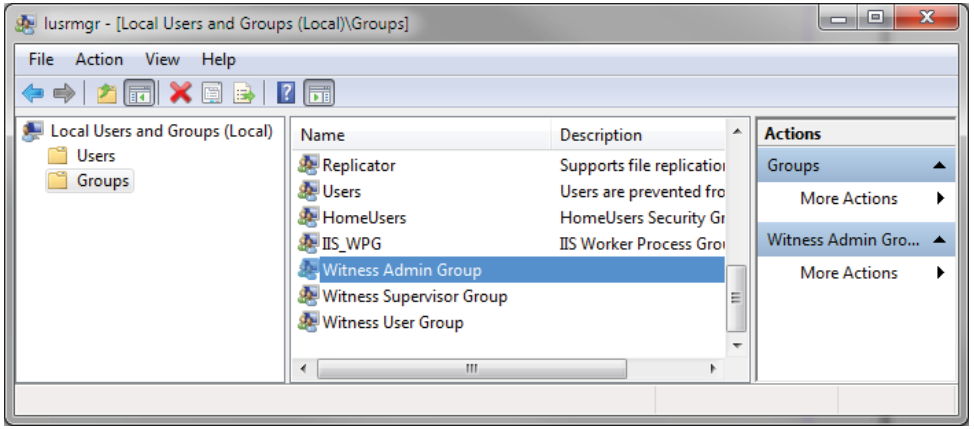
- **Witness Admin Group** (WitnessAdmin)
  Users in this group have full rights to the Witness system and can add, edit and view objects.
- **Witness Supervisor Group** (WitnessSupervisor)
  Users in this group have limited access and in general can only edit and view objects.
- **Witness User group** (WitnessUser)
  Users in this group have read-only access to the system.

Using groups

Users can either:

- Login using one of the pre-configured Witness user accounts, or
- Add an existing Windows user to a Witness group and login as this user.

If you are using a standalone PC, you can add new or existing users to groups using the Windows utility "Local Users and Groups manager" (lusrmgr.msc). You must be logged on with system administrator privileges to do this.



If the PC is on a domain, the users and groups are managed on the domain controller. You should ask your system admin team to manage these.

Integrated Security

With Integrated Security set to true, Witness will attempt to login automatically using the current Windows user credentials. If the current Windows user exists in one of the Witness groups, Sentinel will login automatically with the relevant privileges. Otherwise, the login window will be presented as normal

Note: As a minimum, any user of the system must belong to the WitnessUser group. If a user is only added to the WitnessAdmin group, Sentinel will not login automatically. For this to happen, the user would also need to be added to the WitnessUser group.

Logging on and entering admin mode

You need to logon and enter admin mode in order to make any configuration changes within Sentinel configuration.

To logon and enter admin mode

1 As you enter the Sentinel application afresh, the Logon popup will be displayed:

2 Enter your admin *User* name and *Password*:

The default admin User name is **WitnessAdmin**
The default admin Password is **Navtech Radar.**

Note the use of upper and lower case as well as the fullstop after Navtech Radar.

3 Click the **Login** button.

4 Within the main Sentinel screen, press and hold **Ctrl** and **Alt**, then press the **F5** key. A popup in the lower left corner of the screen will confirm that Admin mode is On. Additonally, whenever admin mode is selected, the following marker will be shown in the top right corner of the screen: 

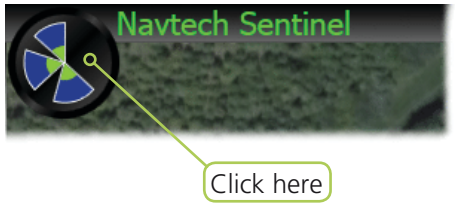
To leave admin mode

1 Within the main Sentinel screen, press and hold **Ctrl** and **Alt**, then press the **F5** key. A popup in the lower left corner of the screen will confirm that Admin mode is Off.

To logout

1 Click the Navtech logo located in the top left corner of the Sentinel window

2 In the main menu (see right), click the **Logout** button.

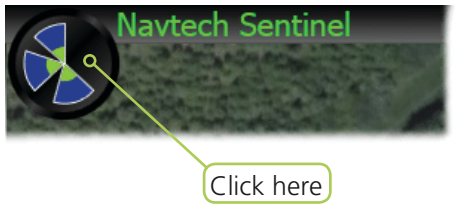


The Sentinel main menu

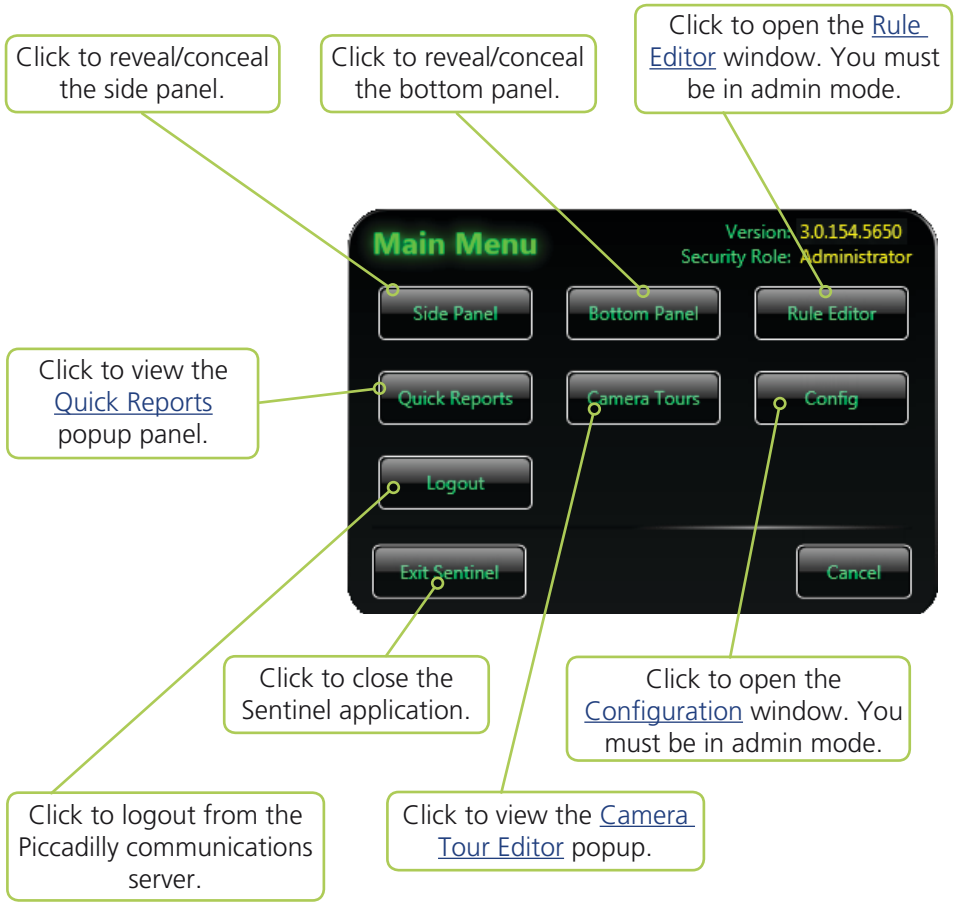
The main menu provides access to several important configuration as well as the exit button.

To access the Sentinel main menu

1 Click the Navtech logo located in the top left corner of the Sentinel window



The main menu will be displayed:



Overview of a new installation

When creating a new installation we suggest the following order of tasks to help produce a more efficient workflow in most cases:

Task 1 Add a background image and scale it *Temporarily (or permanently) add a satellite photograph, scaled map image or integrated mapping (such as Open Street Maps) of the site to be monitored. Using this you can establish an origin point as well as scale and orientate the overall site.*

Task 2 Add radar sensors and trackers *Add a radar/tracker for each installed sensor. The exact positioning of each sensor is determined relative to the origin point that was established in the previous task, approximately at first and then fine tuned later on. Each radar has its own dedicated tracker (usually Bloodhound) that is added to the installation at the same time.*

Task 3 Align the radar sensor(s) *With live data now possible from the radar sensor(s), you can now use the raw data to correctly align them.*

Task 4 Add the detection areas *Using the New Area Wizard, add the areas that encompass the outer limits of the monitored site. Initially, these will be roughly placed and shaped and will be refined once live radar data is made possible.*

Task 5 Fine tune the areas *Use the raw radar data to ensure that the areas are correctly shaped and located.*

Task 6 Create new tracking parameters *Tracking Parameters determine how the data outputs of the trackers are used to produce valid information about targets. Carry out this optional task if the default tracking parameters are not sufficient for your installation.*

Task 7 Create radar filter areas *Carry out this optional step to exclude data from unwanted regions within range of each radar sensor in order to reduce network bandwidth the sensors and their trackers.*

Task 8 Create clutter maps *For each radar sensor, you need to create a record of the static objects that are within range in order to improve the detection of moving objects.*

Task 9 Add cameras *For installations where the system will control automated cameras, use the New Camera Wizard to add them.*

Task 10 Add/edit camera areas *Carry out this optional step to define specific areas where cameras can view. This may be required because certain cameras cannot view particular locations or when cameras cover a particular area (such as an inclined slope) they need to adjust their pan/tilt settings accordingly.*

Task 11 Adjust camera home position(s) *Determine the zero point for each camera.*

Task 12 Add camera presets and camera tours *Carry out these optional steps to define a series of position presets for each camera to view; then create tours that links multiple presets together into a series of locations that each camera should visit in series when it is not involved in any other activity.*

Task 13 Add video viewers *Where pan/tilt/zoom and/or fixed cameras are to be used, video viewers allow their outputs to be integrated with the system. These can be added as part of the New Camera Wizard procedure.*

Task 14 Add static sensors *If the installation requires, add static sensors, such as PIR sensors.*

Task 15 Define rules *Rules form the core intelligence of the system, permitting automatic decisions to be made based upon observed behaviour in the field. This section deals with the basic steps required to create such powerful rules.*

Extending the edit time allowed

The Piccadilly server enforces a time limit on how long admin users can keep a section in edit mode in order to prevent others from being locked out for too long. Before beginning to create a new installation, you are recommended to increase the default edit time of 15 minutes. For details on extending the edit time, please see Appendix 12- Extending the edit time allowed.

You are also recommended to save your changes often.

Adding a background map/image for configuration

Adding, configuring and viewing the active elements of the system are made considerably more straightforward if you can view a scaled image of the area in the background. You can use a map, aerial photo, scaled diagram or an integrated mapping service of the area as your background. Aerial photos are the most useful for the initial configuration stage.

Note: You must be in admin mode to make changes - see Entering admin mode.

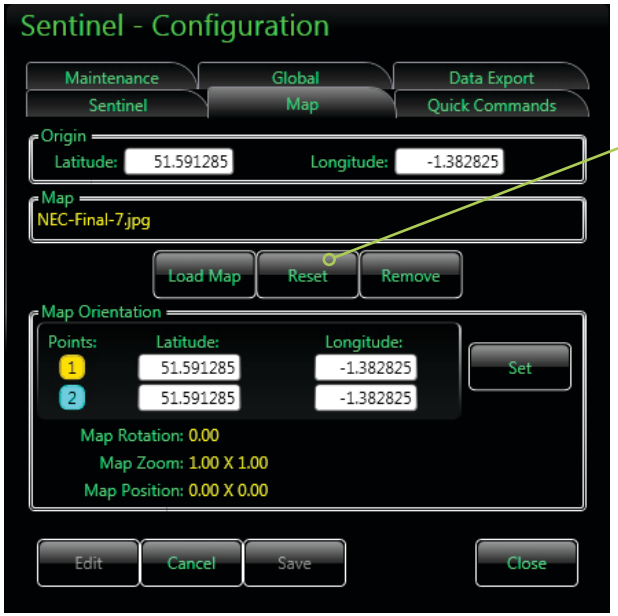
To add a background image

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Config** button to display the Sentinel - Configuration page.

3 Click the **Map** tab.

4 Click the **Edit** button. The various fields will now become editable:



If you encounter problems when scaling the background image, click the **Reset** button to return to the default location.

5 Click the **Load Map** button and then use the resulting file dialog to locate and **Open** a suitable image file. The top left corner of the image will be initially aligned with the current origin point of the site map.

You now need to scale the background image and determine a new origin point.

Scaling the background image (and changing the origin point)

In order to use the background image accurately, the system must calculate the scale and orientation of the image. To achieve this, you need to choose two separate points on the image and declare their true latitude and longitude values.

To achieve the best accuracy, choose two points that are as widely spread as possible within the image and are easily identifiable, both in reality and on the image, e.g. opposite corners of a building, etc. To determine the coordinates of the points you could use a GPS device or an application such as Google™ Earth.

Note: You must be in admin mode to make changes - see Entering admin mode.

Note: When using integrated mapping services, be aware that the maps may contain minor inaccuracies.

To scale the background image (and change the origin point)

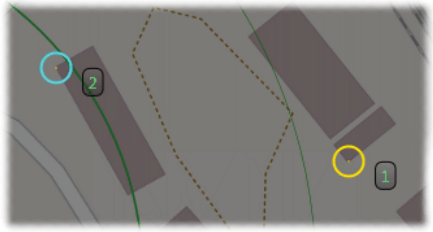
1 Display the *Sentinel - Configuration* page and ensure that it is in edit mode as discussed in *Adding a background image* opposite.

2 Ensure that the *Latitude* and *Longitude* that are set for the Origin correspond to a point that lies either on your background image or not too far away from it.

Why? Because when your two orientation points are entered, Sentinel will create the outer boundaries of the site map to incorporate the Origin plus your two orientation points. If these three locations are far apart, this will result in an unnecessarily large scan area of which you are only interested in a very small portion.

By default, the Origin point is set to the coordinates of the Navtech Radar headquarters near Wantage, Oxfordshire, UK. Change the *Origin Latitude* and *Longitude* to a point within your location (e.g. the first radar location) and then click the **Save** button. Then click the **Edit** button to re-enter edit mode. See the *Tips...* section on the next page.

3 Within the *Map Orientation* section, enter the *Latitude* and *Longitude* values for your two points (See the *Tips...* section on the next page). Two markers (one yellow, the other cyan) will be superimposed at the origin point. (See the Adjusting the map pin size section on the next page).



4 Use your mouse pointer to click and drag the centre point of each marker to lie over the points on your background image that correspond to the Latitude and Longitude values entered earlier. Zoom in, if necessary. Click the **Set** button to scale the map.

5 Click the **Save** button. Sentinel will now scale and orientate your background image so that it correctly aligns with the compass (North is always up).

continued

Tips for using Google™ Earth to gain coordinates

- Ensure that coordinates are displayed in Decimal Degrees. Within Google™ Earth, select **Tools** > **Options** > **3D View** tab. In the **Show Lat/Long** section, choose the **Decimal Degrees** option.
- Select **Add** > **Placemark** to display a map-pin marker and a dialog box. The coordinates given in the dialog correspond directly to the position of the map-pin point.

Adjusting the map pin size

When scaling the background image, depending on the level of zoom you are using, you may need to adjust the size of the two map pins used for the task.

To adjust the map pin size

1 Move the image within the site map so that you can see one or both of the small map pin images.
2 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.
3 Click the **Config** button to display the Sentinel - Configuration page.
4 Click the **Sentinel** tab.
5 Click the **Edit** button.
6 Scroll to the **Map Pin Size** option and move the slider or enter a value.
7 When the map pins are the required size, click the **Save** button and then the **Close** button to exit.

Next steps

- Add radars and trackers
- Align radar sensor(s)
- Create detection areas
- Fine tune detection areas
- Create new tracking parameters
- Create radar filter areas
- Create clutter maps
- Add cameras
- Add camera areas
- Add video viewers
- Add static sensors
- Define rules

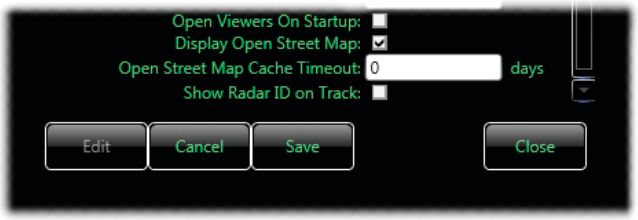
Using Open Street Maps

Once the initial scaling has taken place, as described on the previous page, you may find it more suitable to use an integrated mapping service, such as Open Street Maps as a background for operation.

Note: You must be in admin mode to make changes - see Entering admin mode.

To use Open Street Maps

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.
2 Click the **Config** button to display the Sentinel - Configuration page.
3 Click the **Sentinel** tab.
4 Click the **Edit** button.
5 Scroll to the bottom of the list and ensure that the **Display Open Street Map** option is ticked.



6 Optional step. You can set a value (in days) within the **Open Street Map Cache Timeout** field to determine how often Sentinel should use the Open Street Map web service to update the maps used.

Note: Internet access is required for map updates. If the system is to be isolated from external network connections then map updates will need to be carried out manually.

7 Click the **Save** button to exit.
8 If necessary, remove the original background image: Access the **Map** tab, click the **Edit** button and then click the **Remove** button.
9 Click the **Save** button and then the **Close** button to exit.

The OSM map should now be shown as the background within the site map.

Adding a radar sensor and tracker

For every radar sensor, the system requires a matching tracker service, therefore both are added and edited together within the **Radars & Trackers** section. To assist you, a wizard is available to guide you through the choices.

Note: You must be in admin mode to make changes - see Entering admin mode.

To add a radar sensor and tracker

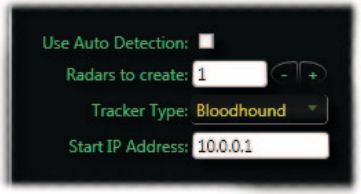
1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Trackers** entry and then click the **New** button. A popup will ask which tracker type to use, in addition to whether you want to use the wizard:

- If you do not tick the *Use wizard* option then a new entry (of the chosen tracker type) will be added to the Objects tab and will be made editable - see Manually adding a radar sensor and tracker for details.
- If you tick the *Use wizard* option, the opening page of the wizard will be displayed:

2 Begin by choosing the model of the radar sensor (or the closest equivalent) in the **Default Legacy Model** drop down.

3 On the left side, choose which Bloodhound to use (if more than one was created during the initial installation). Click the drop down button of the appropriate one and choose the **Legacy** option.

If you need to create more than one Bloodhound tracker, untick the *Use Auto Detection* option to display further setup controls ➲



When creating more than one Bloodhound, the following will occur:

- The *Address* entry will increment by 1 for each radar beginning with the *Start IP Address*,
- The *X* coordinate field will increase for each radar by the value shown in the *Position Offset* field,
- The *Model* type will be adjustable for each radar.

4 Using the options in the lower left corner, choose the appropriate action regarding the detection area. Choose either:

- **New detection area** - to create a new area and apply it as the detection area for each radar created by the wizard using the chosen **Parameters** and **Area Width** settings, or
- **Apply detection area** - to select an existing **Detection Area** (together with **Parameters**) and apply it as the detection area for each radar created by the wizard.

5 Click the **Next** button to display the next page of the wizard:

This is where you can fine tune the settings for each created radar entry.

6 Enter or adjust the IP address within the **Address** field as necessary and adjust any of the other settings (for each radar tab) to suit your installation.

7 When all settings have been made, click the **Finish** button. A popup will request confirmation to create a radar and tracker entry using your settings.

8 Click the **Yes** button. A new entry will be added to the **Radars & Trackers** section within the selection panel in the top right corner of the window.

Further changes can be made to all aspects of that entry at any time. For details see the Objects > Radars & Trackers section.

Note: When configuring or diagnosing a radar sensor, it is possible to record and replay its raw data. See the Appendix - Recording radar data *for details.*

Next steps

- Align radar sensor(s)
- Create detection areas
- Fine tune detection areas

Aligning a radar sensor

When a radar sensor is physically installed, it is quite likely that its alignment does not precisely match with due north, as used by Sentinel to align all elements. It is necessary to ensure that all radar data are referenced to north and Sentinel provides a straightforward process to bring each radar sensor into alignment.

To complete this process, you need to have first completed the following within the Sentinel application:

- Added and scaled a background image of the location,
- Added the radar sensor and tracker.

Note: You must be in admin mode to make changes - see Entering admin mode.

To align a radar sensor

1 Ensure that the radar sensor is powered on and is successfully sending data to its nominated Bloodhound tracker.

2 Within the Sentinel selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** entry and then click on the appropriate entry for the radar sensor. A quick commands panel should appear on the left side of the window.

3 Within the quick commands panel, click the **Data** button (the green indicator on the button should be on) to overlay the live radar signal within the site map

4 Click the coloured square on the **Data** button and select the *Raw* option.

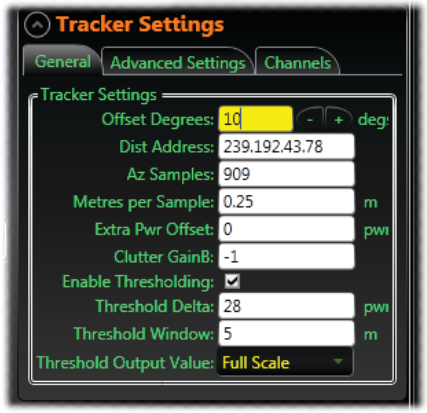
5 Adjust the view within the site map until you can see the radar sensor and its immediate surroundings, preferably so that you can see several fixed objects such as buildings, fences, etc.

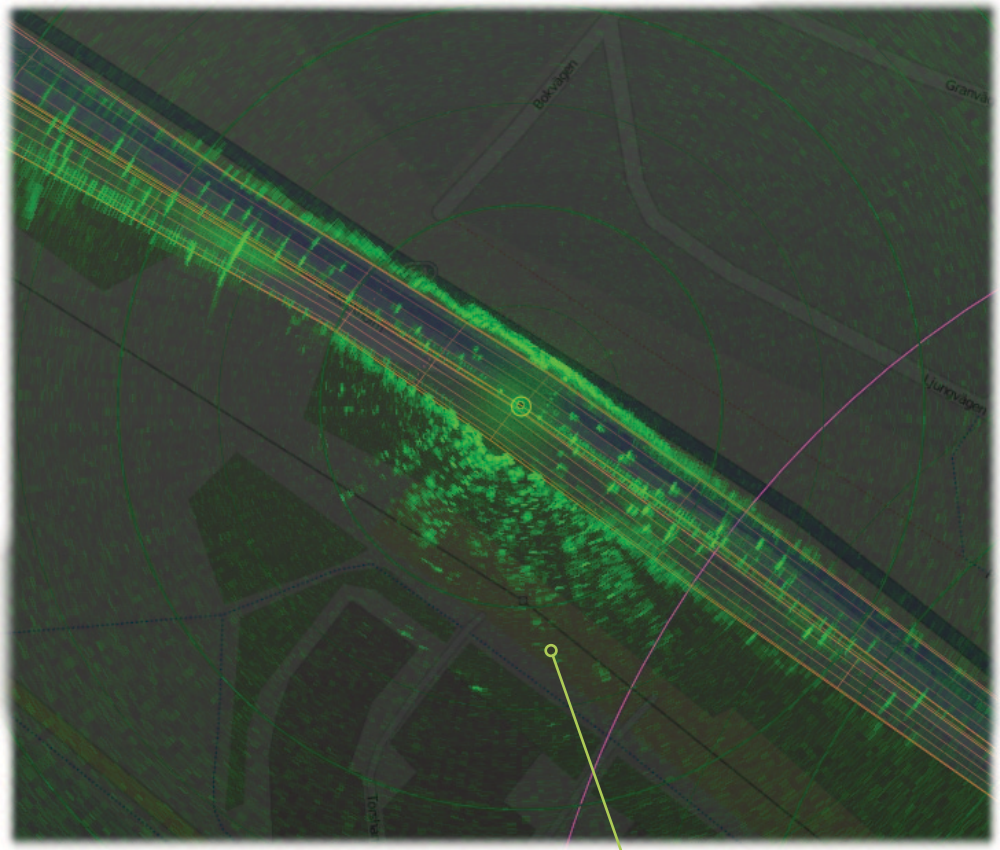
6 Within the radar image, search for traces of the fixed objects that are present within the background image. You now need to rotate the former so that it aligns precisely with the latter. If they are already aligned then you do not need to make any further alterations.

7 In the information panel on the right side of the window, click the **Edit** button for the radar entry and then ensure that your mouse pointer is within the site map. Either enter a value into the *Offset Degrees* field or press and hold the **Alt** button on your keyboard and then slowly roll the mouse wheel to rotate the radar image. You will notice that the value within the *OffsetDegrees* property changes in 0.5 degree steps as you rotate the radar image

8 When the radar image is correctly superimposed over the background image, click the **Save** button and also click the **Data** button (on the quick commands panel) to remove the overlay. The radar sensor is now correctly aligned within Sentinel.

9 Whenever the radar offset is changed, you need to capture/recapture a new Clutter Map. See Creating and viewing clutter maps.





Raw radar data overlaid onto the background image.

If necessary, use the *Data Brightness* control within the *Settings* tab to adjust the intensity of the radar and map images.

Note: When configuring or diagnosing a radar sensor, it is possible to record and replay its raw data. See the Appendix - Recording radar data *for details.*

Next steps

- Create detection areas and Fine tune detection areas
- Create new tracking parameters
- Create clutter maps
- Add cameras and Add camera areas
- Define rules

Adding a detection area

Detection areas are how you inform the system of the outer limits of where you wish it to pay particular attention. You can define one or more areas and apply rules to specifically monitor the movement of people or objects within those areas. You can also layer one or more areas to create exclusion zones within the main area.

The creation of new detection areas is generally achieved in two stages:

1 Create rough initial outlines for the detection area(s).

2 Use live data to fine tune the area outline according to the viewed tracks and radar background data in order to isolate the area(s) fully from the surrounding land and/or roads.

Note: You must be in admin mode to make changes - see Entering admin mode.

To add a detection area

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Areas** entry and then click the **New** button.

A popup will ask whether you want to use the wizard:

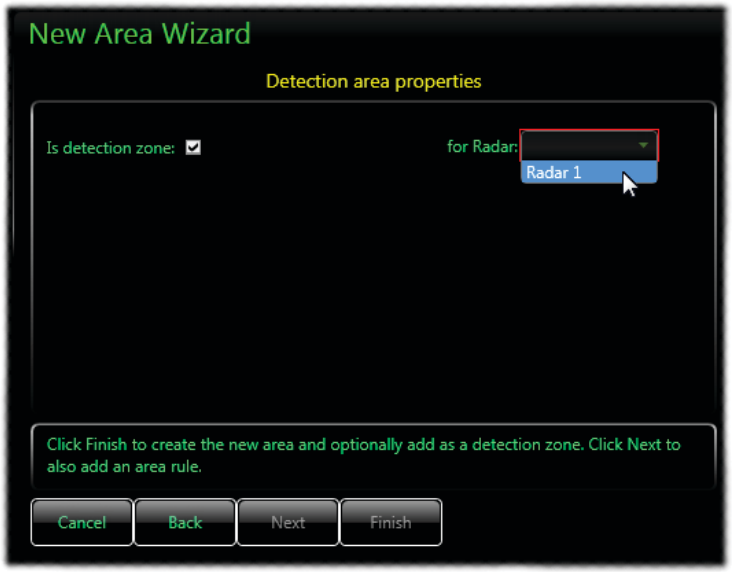
- If you click **No** then a new area entry will be added to the Objects tab and will be made editable - see Manually adding a detection area for details.
- If you click the **Yes** button to display the opening page of the wizard:

2 Enter a **Name** for the new area and optionally click the **Colour** button to choose a background shade for the new area.

3 If you know the size and/or the position coordinates for your area, use the remaining fields to determine these aspects of the new area. Otherwise leave these fields untouched and edit the area later within the site map.

4 You can now either click the **Finish** button to create a basic unlinked area (jump to step 9) or click the **Next** button to link it with a particular radar sensor.

The next page of the wizard will be displayed:



5 Place a tick in the **Is detection zone** checkbox to display the **for Radar** dropdown list. If you do not wish to create the area as a detection zone at this time, click the **Next** button to continue (jump to step 9).

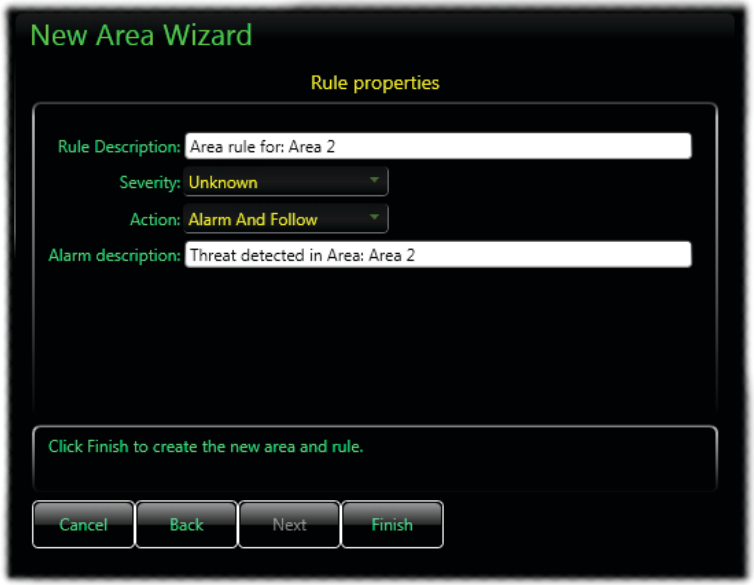
6 Click the **for Radar** dropdown list and choose the radar sensor that you wish to link this area with. As you do so, a new field will be displayed.

7 Click the **Parameters** dropdown and choose which tracking parameters you'd like to link with the new area.

8 You can now either click the **Finish** button to create the area without rules (jump to step 11) or click the **Next** button to apply rule properties to it.

continued

The next page of the wizard will be displayed:

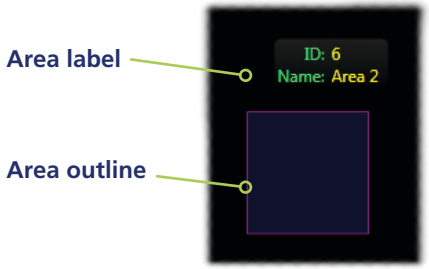


9 Use the fields to create a basic outline rule for the area:

- **Rule description** - a basic explanation of the rule that is used when configuring and editing the installation.
- **Severity** - choose the level of alarm that should be indicated/sounded whenever the rule conditions are met.
- **Action** - choose the action that should be carried out whenever the rule conditions are met: sound the alarm; follow the target with the nearest camera, or both.
- **Alarm description** - this is the text that will be displayed to the operator and placed in the log whenever the rule conditions are met. In addition to static text that will remain the same regardless of where the rule is broken, you can add placemarkers that will call dynamic text to indicate the particular information, such as the area, sensor, etc. See Appendix 4 for details of alarm placemarkers.

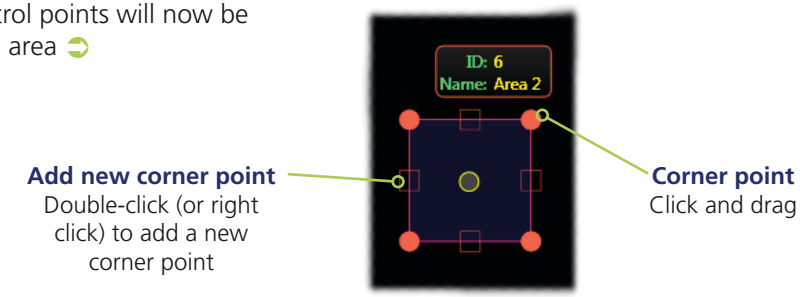
10 Click the **Finish** button and confirm the subsequent popup message to create the new area.

The new square area will be placed into the site map



11 Within the selection panel in the top right corner (Objects tab, Areas section), ensure that the name of the new area is highlighted and click the **Edit** button.

Editable control points will now be added to the area



12 You can now alter the shape of the detection area:

- To move the whole area: Click and hold anywhere within the area and drag it to the required position.
- To move a corner point: Click and hold on one of the solid circular corner points and drag it to the required position.
- To add another corner point: Double-click (or right-click) on one of the hollow square points which are mid-way along each line.
- To remove a corner point: Right-click on the solid circular node that you wish to remove.
- To move the label, click and drag on the label.

13 When your area is the correct shape and in the right location, click the **Save** button.

14 Before a new detection area can be used with a radar sensor, it must be linked to a set of tracking parameters within the tracker of the radar sensor. If you did not carry out the linking step within the wizard, you will need to complete this separately. For details see Manually inking areas and tracking parameters within trackers.

Next steps

- Fine tune detection areas
- Create new tracking parameters
- Create radar filter areas
- Create clutter maps
- Add cameras and Add camera areas
- Add video viewers and Add static sensors
- Define rules

Fine tuning detection areas

Once each radar sensor has been aligned and valid data is being received, it should then be possible to see the objects such as fences, hedges, trees, buildings, road boundaries and the surroundings. You can now use these images to ensure that the rough outer areas created earlier are shaped as tightly as possible around the area(s) that they need to monitor.

Note: You must be in admin mode to make changes - see Entering admin mode.

To fine tune an area

1 Within the Sentinel selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** entry and then click on an appropriate entry.

2 Within the quick commands panel, click the **Data** button (the green indicator on the button should be on) to overlay the live radar signal within the site map

Note: It is possible to simultaneously overlay the output from two or more radar sensors. However, this uses a sizeable amount of processing power so it is advisable to show no more than two or three sensor outputs at a time.

3 Click the coloured square on the **Data** button and select the *Raw* option.

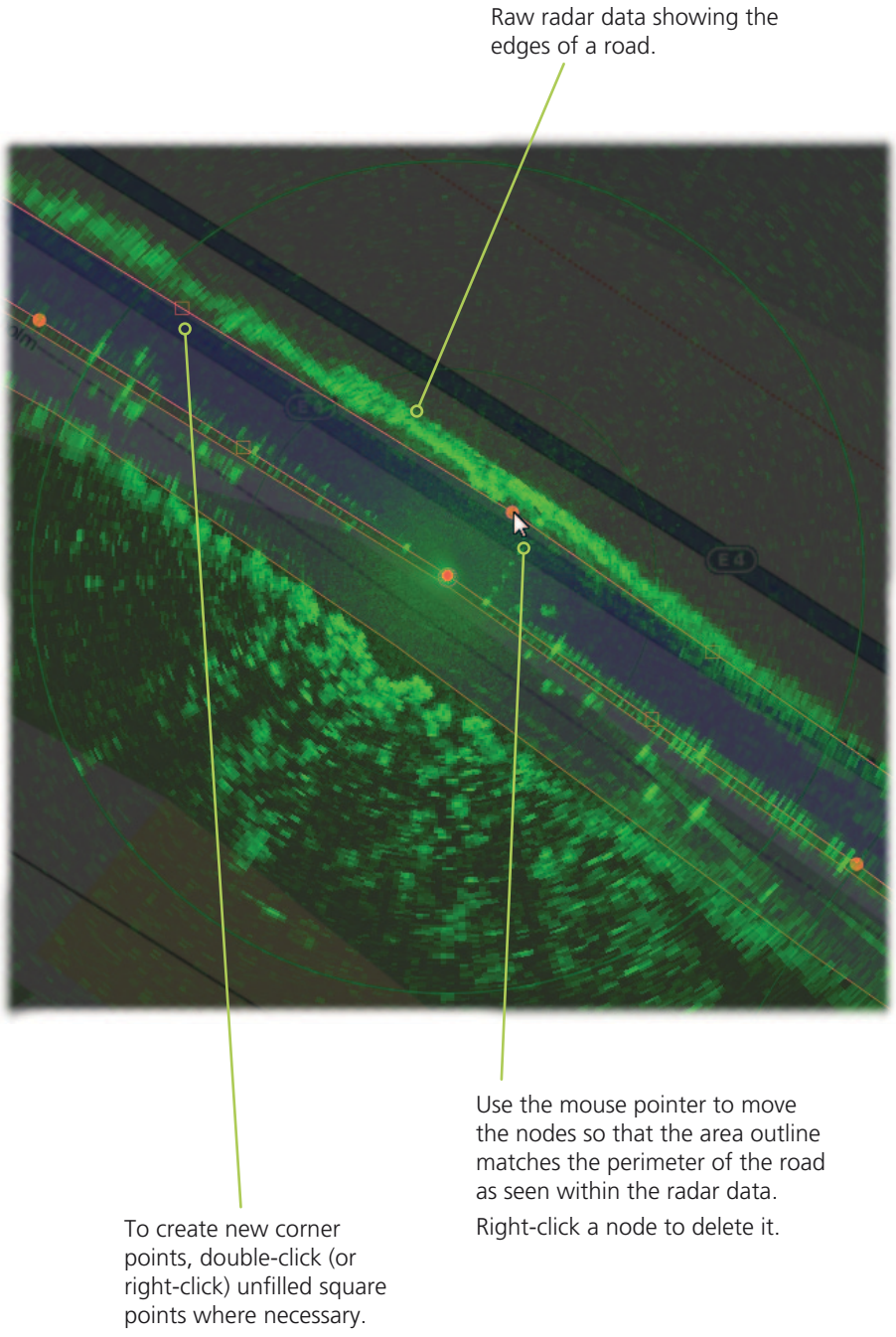
4 Adjust the view within the site map until you can see the detection area boundary you wish to edit.

5 Click on the detection area to select it - the details will appear in the information panel.

6 Edit the information panel details as required. Also, use your mouse to click on and move the corner points to the required positions.

Note: For parts of the area that are further from the radar sensor, any given object will produce a wider trace due to the beamwidth of the sensor. Therefore, it may be necessary to widen the area as it stretches away further from the sensor.

7 When the area has been fine tuned, click the **Save** button to store the new area shape.



Next steps

- Create new tracking parameters
- Create radar filter areas
- Create clutter maps
- Add cameras and Add camera areas
- Add video viewers
- Define rules

Creating new tracking parameters

Tracking parameters determine how the radar data conditioned by the tracker is used to produce valid information about tracked targets. Think of tracking parameters as a set of filters that determine how objects seen within that area are converted into valid targets to which logical rules can be applied.

Note: You must be in admin mode to make changes - see Entering admin mode.

To create tracking parameters

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Tracking Parameters** entry and then click the **New** button. A set of standard tracking parameters will be shown

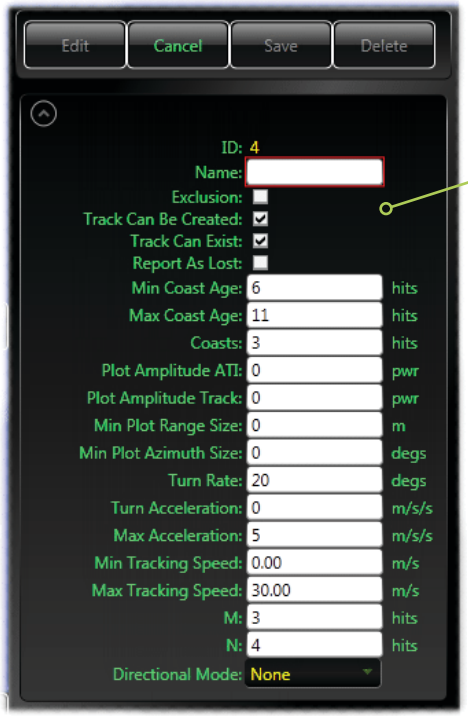
2 Enter a **Name** for the new set of parameters.

Alter the settings indicated here as required, leave all others in their default state. For more details on the functions of all settings, see the section Objects > Tracking Parameters.

3 Click the **Save** button.

4 To be actively used, the tracking parameters need to be linked to the area(s) that are to be monitored within one or more trackers. This can be done in any of the following ways:

- Within the New Tracker & Radar Wizard, or
- Within the New Area Wizard, or
- Manually using the Objects > Radars & Trackers section of the selection panel. See Manually linking areas and tracking parameters within trackers.



ID
The **ID** number is automatically set by Sentinel.

Name
Enter a descriptive name for the new tracking parameters.

Turn rate
Set this to a value of zero to prompt the use of the Lateral Acceleration value to determine the expected maximum rate of change of direction for tracked objects.

Turn Acceleration
This is an alternative way to determine the Turn Rate and is typically set to a value of 1 m/s/s.

Max Acceleration
Determines the maximum acceleration expected from objects in the monitored area.

Min/Max Tracking Speed
Determines the minimum and maximum speed of travel expected from vehicles in the monitored area.

Directional mode
This is typically set to *None* for security use because tracked objects will generally emerge and exit in any direction.

Note: For all other settings, use the default values to get the system running and then return to fine tune them, if necessary, once system behaviour can be observed.

Next steps

- Create radar filter areas
- Create clutter maps
- Add cameras and Add camera areas
- Add video viewers
- Add static sensors
- Define rules

Creating a radar filter area

In operation, radar sensors create large quantities of data from each scan revolution which must be transferred to the respective trackers. It is often the case that only a portion of each sensor's full scan range is relevant to a given installation and this is where *Filter Areas* become invaluable. Using a filter area, you can instruct a radar sensor to ignore all but the area that it is required for the installation. This has the effect of greatly reducing the volume of data created and sent across the communication link, often by many megabytes per second.

Note: Radar sensors must be aligned before adding filters - See Aligning a radar sensor.

To create a radar filter area

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** section and then click the entry for the required radar sensor.

2 Click the **New Area** button. A new entry will be added to the Objects > Areas section, with an information panel below it and a new triangular filter area outline will be added to the graphical representation within the site map

Corner point Click and drag

Add new corner point Double-click (or right click) to add a new corner point

3 Alter the shape of the filter area so that it fully encompasses all of the regions to be monitored by the radar sensor:

- To move the whole area: Click and hold anywhere within the area and drag it to the required position.
- To move a corner point: Click and hold on one of the solid circular corner points and drag it to the required position.
- To add another corner point: Double click (or right-click) on one of the hollow square points which are mid-way along each line.
- To remove a corner point: Right-click on the solid circular node that you wish to remove.

4 When your area is the correct shape and in the right location, enter a name for it within the information panel

5 When all details for the area are complete, click the **Save** button.

6 Click on the radar sensor entry within the Objects > Radars section and click the **Update Filter Area** button to send the coordinates of the new filter area to the radar sensor.

Once done, the sensor will only send data from within the boundaries of the filter area. Where appropriate, this procedure will need to be completed for each radar sensor.

To edit a filter area

1 Within the Objects tab, click the **Areas** entry and then click the entry for the required filter area.

2 Click the **Edit** button and make the necessary changes to the shape and/or accompanying information panel details.

3 Click the **Save** button.

4 Within the Objects > Radars & Trackers section, click the entry for the radar sensor and then click the **Update Filter Area** button to register the altered details with the sensor.

To remove a filter area

1 Within the Objects tab, click the **Radars & Trackers** entry and then click the entry for the required radar sensor.

2 Click the **Clear Filter Area** button to remove the area details from the sensor.

Note: The above action only informs the radar sensor to return to sending all scan data. To remove the filter area details from Sentinel, select the entry for the filter area within the Objects > Areas section and click the **Delete** *button.*

Limitations

The filter area is tied to its specific radar and is not aware of any radar rotation. Therefore the filter area should be removed and re-created if the radar is moved or the rotation is changed.

Next steps

- Create clutter maps
- Add cameras
- Add camera areas
- Add video viewers
- Add static sensors
- Define rules

Creating and viewing clutter maps

A *Clutter Map* is a record of the static objects within range of a radar sensor. Clutter maps are created and used as reference points for radar sensors and their trackers so that they can better concentrate on objects that are moving.

For a new installation you need to create a new clutter map for each radar sensor. During operation it is also good practice to periodically update each clutter map to take account of objects that have moved in the interim.

Note: You must be in admin mode to make changes - see Entering admin mode.

To create a clutter map

1 Within the Sentinel selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** entry and then click on an appropriate entry.

2 Within the quick commands panel, click the **Data** button (the green indicator on the button should be on). The radar data should now be overlaid onto the site map in red (processed data) or green (raw data).

3 Click the coloured square on the **Data** button and select the *Clutter Map* option. You should see the clutter map data overlaid onto the radar scan region

4 Within the Sentinel selection panel in the top right corner (Objects tab > Radars & Trackers), click the **Edit** button. In the Tracker Settings section, change to the Advanced Settings tab and scroll down to the **Clutter Map** sub-section.

5 Adjust the **Clutter Map Time** to a value of 0.98.

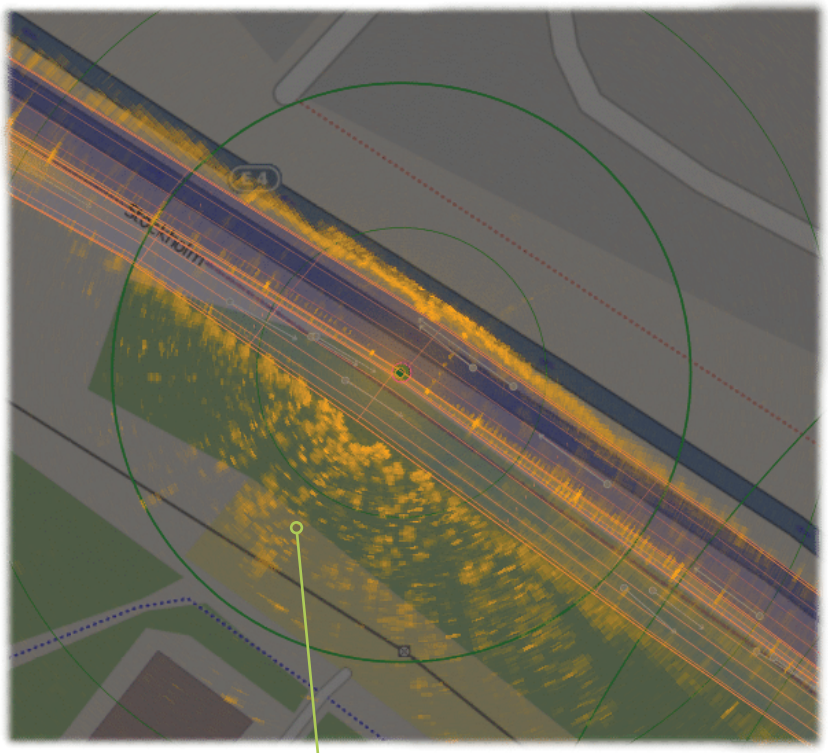
This value dictates how much of the radar data coming in contributes towards movement detection. Its unit is data per revolution of the radar (i.e. per 1 scan). For a value of 0.8, this means 20% of the data from the scan goes to form the clutter (background radar picture). Therefore 80% is analysed for movement. The higher the number, the more the data is analysed for movement, and the more sensitive it is to movement. Recommended setting is between 0.8 and 0.95.

6 Leave the system running for roughly one minute in this state to allow new clutter data to be recorded.

7 Adjust the **Clutter Map Time** back to a suitable operational value of between 0.8 and 0.95.

8 Click the **Save** button and then click the **Save Clutter Map** button. The new clutter map data will be saved using the file name stated in the Clutter Map section. The new map will be used by the tracker. Also, click the Data button within the quick commands panel to remove the radar data from the site map.

IMPORTANT: If the offset for any radar sensor is changed, you will need to create a new clutter map for that sensor.



Clutter data shown in orange overlaid onto the radar scan region

Next steps

- Add cameras
- Add camera areas
- Add video viewers
- Add static sensors
- Define rules

Adding a camera

A Witness system can control many individual Pan/Tilt/Zoom (PTZ) cameras. In order to manage potentially large numbers of devices, each individual camera is made to be a member of two different types of groups: *Camera Groups* and *Camera Connections*. The two group types affect different aspects of camera operation:

- **Camera Groups** determine how cameras react to multiple tracked objects, according to how the group is globally configured: *Closest* mode causes all cameras within the group to follow only the objects that are in their immediate vicinity; while *Timeshare* mode causes all cameras within the group to spread themselves between tracks, spending an adjustable amount of time on each, before moving to the next tracked object.
- **Camera Connections** determine how cameras are connected to the computer that is running the Cyclops service. Connections can be any of several types. All cameras within a particular connection group will share the same connection and will be differentiated by their given ID numbers.

You can create any number of each type of group and then place your cameras into mixtures of the group types, for instance:

Camera 1 could be a member of Camera Group X (set to use 'Closest' mode) and also to Connection Group A (to specify an Ethernet connection). Meanwhile Camera 4 could also be a member of Camera Group X (to use the same tracking behaviour as Camera 1) but also a member of Connection Group B (to specify a Serial connection).

IMPORTANT: The way in which you create your groups and distribute the cameras between them is purely a matter of choice and circumstance, however, every camera must belong to one (and one only) of both types of group, i.e. one *camera group* and one *camera connection group*.

Note: There are default entries for both types of group: Default Camera Group *and* No Connection. *These act as temporary receptacles for cameras that have been created within one group type, but not yet assigned to the other type of group. For instance, if you create a new Camera Group called 'Cam Group 1' and then create a new camera belonging to it but do not assign it to a connection group, then the camera will be placed within the* No Connection *group. At a later time you can then edit the unassigned camera and add it to a real connection group of your choice. A camera will not operate correctly until it is a member of one of each type of real group. Also, you cannot initiate a new camera from within either of the default groups.*

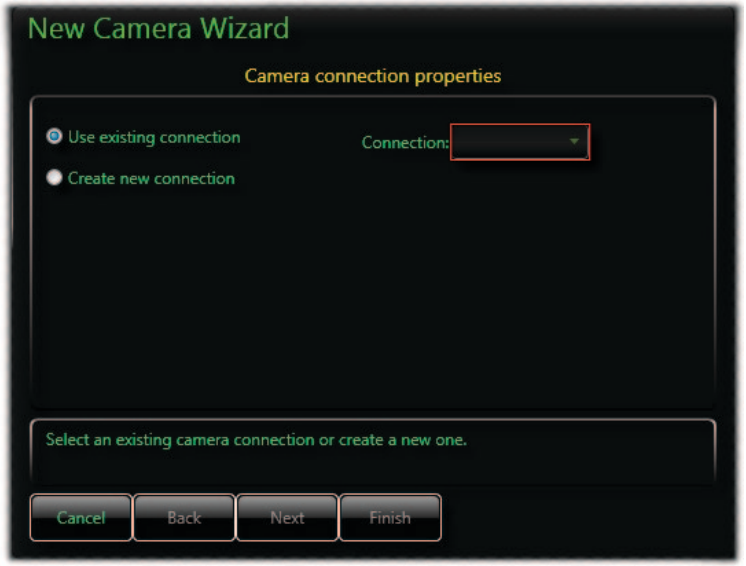
To add a camera

Note: You must be in admin mode to make changes - see Entering admin mode.

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), choose the **Objects** tab and click on the **Cameras** entry.

2 Click the **New** button. A popup will ask whether you want to use the wizard:

- If you click **No** then no further action will be taken. If you wish to add a camera without using the wizard, see Manually adding a camera for details.
- If you click the **Yes** button to display the opening page of the wizard:



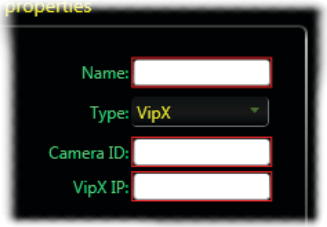
3 Your first choice is whether to use an existing camera connection or create a new one:

- To use an existing connection: Ensure that the **Use existing connection** option is selected and then click the **Connection** dropdown. Choose the required connection from the list.

  OR

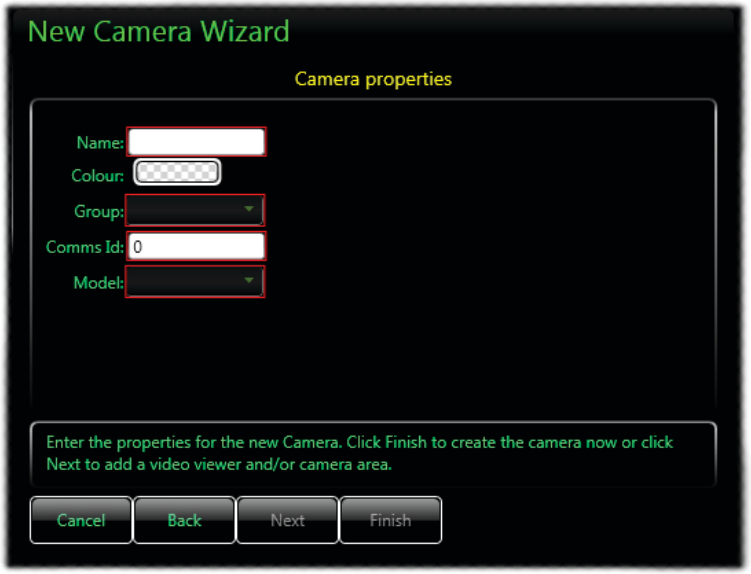
- To create a new connection: Click the **Create new connection** option to display new fields on the right side of the window

  Enter a **Name** and then choose the appropriate connection **Type**. The fields presented below will alter according to the chosen connection type. Enter the appropriate connection details.



continued

4 Once the connection details have been declared, click the **Next** button to continue. The next page of the wizard will be displayed. Whereas the previous page dealt with the connection details, this page is concerned with the camera itself:



5 Enter a name for your new camera and optionally edit the colour that will be used for the camera and its beam within the site map.

6 Choose a **Group** for the new camera. There are three standard types in the list. The latter two determine how cameras react to multiple tracked objects:

- *Default camera group* - this is a temporary placeholder for new cameras that have yet to be assigned to one of the other groups. A camera placed in this group will not function.
- *Closest* - All cameras in this group will follow only the objects that are in their immediate vicinity.
- *Timeshare* - All cameras in this group will view spread themselves between multiple targets, spending an adjustable amount of time on each, before moving to the next tracked object.

7 Enter the **Comms Id**. This must match the value that is set on the camera hardware otherwise camera control messages will not reach the correct camera.

8 Choose the **Model** that matches, or most closely resembles, that of your camera.

9 You can now either click the **Finish** button to create a basic camera entry (jump to step 15) or click the **Next** button to apply a video viewer and/or camera area.

The next page of the wizard will be displayed:

10 If you wish to associate a video viewer with the camera, click the **Add Video Viewer** option. Otherwise click the **Next** button to advance to the next page (jump to step 15)

11 Enter a **Name** for the video viewer connection.

12 Choose the required viewer type from the list of available **Video Plugins**.

13 Enter the **Address** of the video feed from the camera.

14 Optionally enter a valid **Video ID**. This is used for camera systems that provide two or more separate video streams (e.g. multi-channel video encoder) that are switched between. Where different IDs are needed to select the required stream(s), enter the valid ID here.

continued

15 You can now either click the **Finish** button (jump to step 21) or click the **Next** button to create a camera area.

The next page of the wizard will be displayed:

16 Click the **Add Camera Area** option to reveal the necessary property fields.

17 Enter a **Name** for the new camera area.

18 Optionally adjust the **Width** option to affect the size of the area, or leave the default value and later adjust the area graphically within the site map - see next page for details.

19 Optionally enter a **Height Offset**. See right for explanation.

20 Optionally enter a **Relay Id** that can be activated whenever the camera is active. This option is most often used to activate a video recorder.

21 When all fields are complete, click the **Finish** button and confirm the subsequent popup message to create the new camera entry.

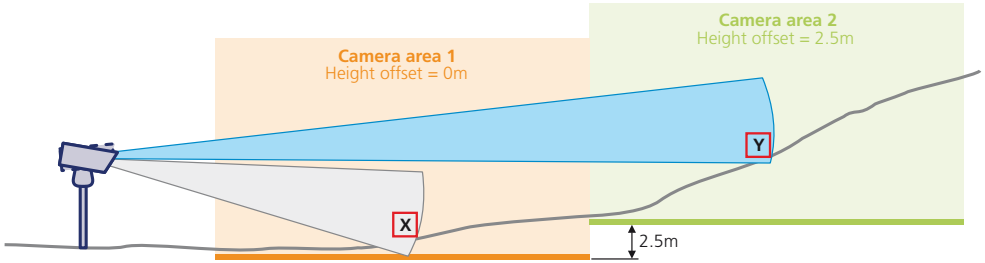
The new camera will be added to the site map and new entries made within the Cameras section of the selection panel.

If you created a camera area within the wizard, its entry within the selection panel (Objects tab > Areas section) in the top right corner of the screen will now be highlighted. If you need to edit its size and shape, click the **Edit** button. See the next page for further details about editing a camera area.

What are camera areas and height offsets?

Within installations there can sometimes be situations where you need to limit or adjust how cameras view the areas around them. Typical reasons are that radar sensors and cameras are often located separately and so the former may be able to 'see' regions that the latter cannot. Also, there may be trees, fences, walls forming visual obstacles through which one or more cameras cannot view. For these reasons you can create camera areas in which you define the regions that any cameras can operate within.

Camera areas are also very useful where a single camera needs to cover an area that has differing ground heights within it. Each camera area has a *Height Offset* option which allows you to inform the camera that when it is viewing that area it should make tilt adjustments to account for the height difference. In the example below two camera areas are used: Camera area 1 for the flat ground nearest the camera and Camera area 2 for the raised ground further away. For the second area a Height Offset = 2.5m.



When viewing object X, the camera will use area 1 and when viewing object Y it will use area 2, with its 2.5m height offset to ensure that the camera tilts itself upwards.

Next steps

- Add camera areas
- Add camera presets and tours
- Add video viewers
- Add static sensors
- Define rules

Adding/editing a camera area

If you added a camera area while using the New Camera Wizard, there is a good chance that you will now need to edit that area so that it is the correct size and shape for your installation. See What are camera areas and height offsets? for an explanation of why they are needed.

Alternatively, if you did not create a camera area within the wizard and need to add one now, use the procedure below.

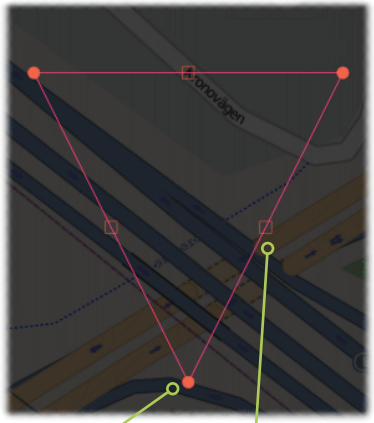
To add/edit a camera area

Note: You must be in admin mode to make changes - see Entering admin mode.

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), either:

- To add a new area: Choose the **Objects** tab and double-click the **Cameras** entry. In either the Camera Groups or the Camera Connections sections, select the required camera entry and click the **New Area** button.
- To edit an existing area: Choose the **Objects** tab and click the **Areas** entry to reveal all available areas. Click to highlight the required area and then click the **Edit** button.

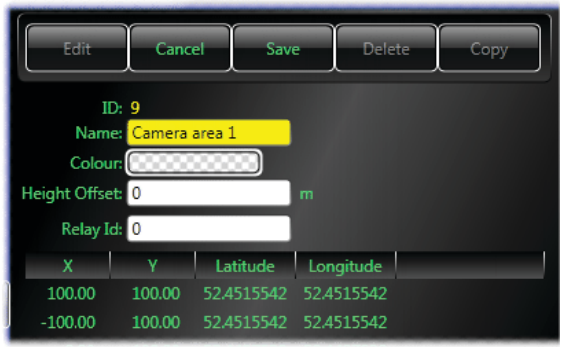
The camera area outline will become editable within the site map ➲



2 Alter the shape of the camera area so that it fully encompasses all of the locations that the camera will need to view:

- To move the whole area: Click and hold anywhere within the area and drag it to the required position.
- To move a corner point: Click and hold on one of the solid circular corner points and drag it to the required position.
- To add another corner point: Double-click (or right-click) on one of the hollow square points which are mid-way along each line.
- To remove a corner point:
  Right-click on the solid circular nodes that you wish to remove.

3 When your area is the correct shape and in the right location, enter a name for it within the information panel ➲



4 Optional step. Where necessary enter a *Height Offset* to account for ground height differences.

5 Optional step. You can adjust the colour shading of the filter area that will be shown on the graphical representation. This is useful when there are numerous areas as it helps you (and the operator) to distinguish them.

6 Optional step. Where a DVR or other device must be activated along with the camera, enter a valid ID for the relay that will prompt the DVR to begin recording the video feed. Choose '0' to disable.

7 When all required settings have been made, click the **Save** button.

Next steps

- Add camera presets and tours
- Add video viewers
- Add static sensors
- Define rules

Adjusting a camera home position

When a new camera is added, it is given a home position, essentially a position preset with default pan, tilt and zoom settings, to which it should return whenever a *Home* command is issued - it is the camera's 'zero point'. Following installation, the exact orientation of the camera will probably be unknown and will almost certainly not be aligned with what Sentinel considers to be the home position.

The initial home position is centred on the camera position itself (denoted by a five pointed star image) but is easily moved to best suit the installation.

You can adjust the home position 'graphically' within the site map or 'numerically' within the Object tab - or using a mixture of both methods.

To adjust a camera home position

Note: You must be in admin mode to make changes - see Entering admin mode.

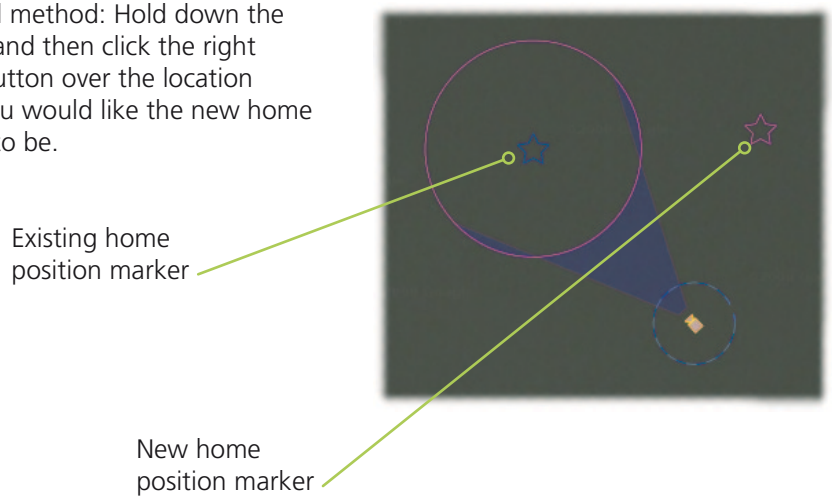
1 Position and zoom the site map so that you clearly see the camera that you wish to edit.

2 Choose the required camera, either:

- Click on the camera icon within the site map and then click the **Edit** button below the **Objects** tab, or
- Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), choose the **Objects** tab and double-click the **Cameras** entry. In either the Camera Groups or the Camera Connections sections, select the required camera entry and click the **Edit** button.

3 Select the new home position either graphically or numerically:

- Graphical method: Hold down the **Ctrl** key and then click the right mouse button over the location where you would like the new home position to be.



- Numerical method: Locate the *Objects tab > Camera section > Home Position* sub section.

The *Latitude* and *Longitude* fields state the absolute coordinates of the camera home position.

The *X* and *Y* fields here allow you to compensate for any differences between the camera and the Sentinel home positions.

Adjust the home position fields as required. The purple star will move accordingly as you adjust the coordinates.

4 When the home position is as required, click the **Save** button within the Camera section. The camera will move to view the new home position.

Homing a camera

In order to send a camera to its home position, you must ensure that the appropriate button is enabled within the quick commands panel, see below.

To enable the Go Home button

Note: You must be in admin mode to make changes - see Entering admin mode.

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Config** button and then choose the **Quick Commands** tab.

3 Click the **Edit** button and ensure that the **Go Home** checkbox is ticked. Also ensure that the *Quick Panel Is On* option is also ticked.

4 Click the **Save** button and then click **Close**.

The *Go Home* button should now appear on the popup quick commands panel whenever a camera is selected.

To home a camera

1 Select the required camera.

2 The quick command panel should appear on the left side of the screen

3 Click the **Go Home** button.

Creating camera presets

Camera presets allow you to define one or more camera positions (each comprising pan, tilt, height and zoom coordinates). Those camera presets can then be used as the building blocks for creating camera tours.

To create a camera preset

Note: You must be in admin mode to make changes - see Entering admin mode.

1 Position and zoom the site map so that you clearly see the camera that you wish to edit.

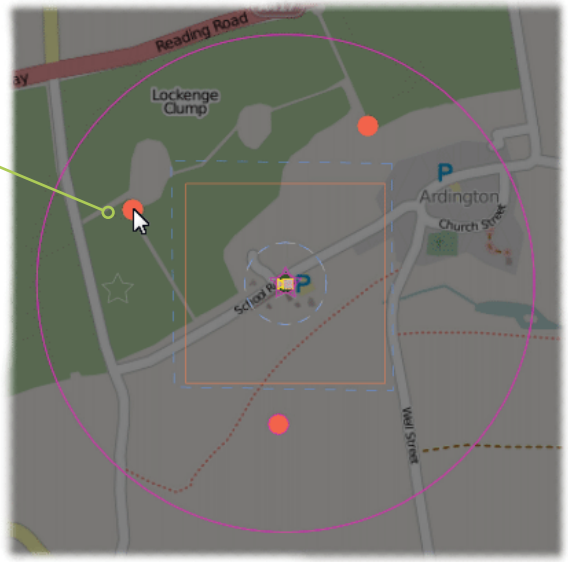
2 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), choose the **Objects** tab and double-click the **Cameras** entry.

3 In either the Camera Groups or the Camera Connections sections, select the required camera entry and click the **Edit** button.

4 Place the mouse pointer on the site map (within range of the selected camera).Hold the **Ctrl** button and then click the left mouse button to define the camera preset position. Two things will occur as a result:

An orange preset node will be placed on the map/ background image in the location that you clicked,

and...



... a corresponding entry will be added to the Presets section at the base of the *Camera* section within the *Objects* tab.

5 You can edit presets as follows:

- Create a new preset node - Ctrl and left mouse click,
- Delete a preset node - Right mouse click on the preset node,
- Move a preset node - Click and hold the left mouse button on a preset node and drag it to a new position.
- Edit preset coordinates - In the Presets section of the Camera entry within the Objects tab, click on a preset entry and edit the stored values.

  Note: The Height coordinate represents the vertical height (in metres) that the camera should centre upon above the given X and Y coordinates. This value is in addition to any Height offset that has been given to the camera within the Camera area.

  Similarly, the Zoom coordinate determines the zoom level to be used when viewing a given preset position. It can be affected by any default zoom that has already been applied to the camera.

6 When all required settings have been made, click the **Save** button.

To view camera presets

In operation, the camera preset positions are not normally shown within the site map. However, it is possible to view them when you zoom in very close to the camera. Once zoomed in to a camera that has presets, you should see the following:

Each preset node shows the camera Id number in the upper half and the preset number in the lower half.

If required, double click on a preset node to make the camera point towards it.

Creating camera tours

Camera tours provide a quick way to program and run a series of movements for cameras to run through when they are otherwise idle. The starting point for any camera tours are two or more camera preset nodes, as discussed in the section Creating camera presets. Using the *Camera Tour Editor* popup, you then string together the required camera presets and decide how long to dwell at each. Once a camera tour is programmed and enabled, the camera will cycle through the various preset positions whenever it is not requested to perform any other task.

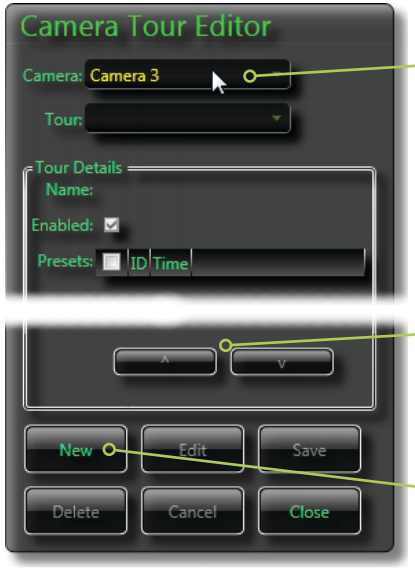
To create a camera tour

Note: You must be in admin mode to make changes - see Entering admin mode.

1 Create two or more position presets for a camera. See Creating camera presets for details.

2 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

3 Click the **Camera Tours** button to display the following:



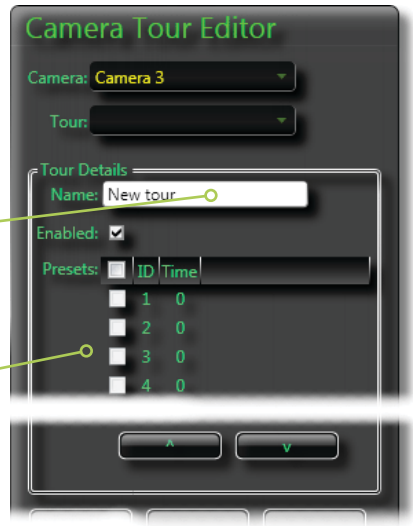
Choose the required camera

Use these buttons to change the order of preset positions within the list

Click the **New** button to begin creating a new tour

4 Click the **Camera** field at the top of the popup and choose the required camera from the drop down list.

5 Click the **New** button at the base of the popup. At this point, all available position presets for the chosen camera should be displayed within the popup:



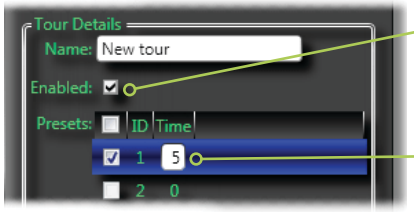
Add a descriptive name for the new tour

All position presets for the chosen camera will be listed here

6 Use the *Name* field to enter a description for the new tour.

*Note: As you create any new tour, it is automatically enabled as the current tour for the chosen camera (with any existing tour being deselected as a result). If necessary, you can change this using the **Enabled** checkbox within this and other tours for the same camera.*

7 Tick the checkbox of a position preset that you wish to include within the tour:



This checkbox determines which camera tour is the current one to use for a particular camera

All position presets for the chosen camera will be listed here

As you include the preset, the editor will automatically enter the minimum dwell time of 5 seconds. If required, alter the dwell time (up to a maximum of 999 seconds).

8 Optional step. If you wish to change the order in which a chosen preset position is visited within the list, use the **^** and **v** buttons move the highlighted entry up or down.

9 Repeat steps 7 and 8 until all required presets have been included. Check that the **Enabled** option is checked and click the **Save** button. Then, click the **Close** button to leave the *Camera Tour Editor*.

Please see Using camera tours in the Operation chapter for further details.

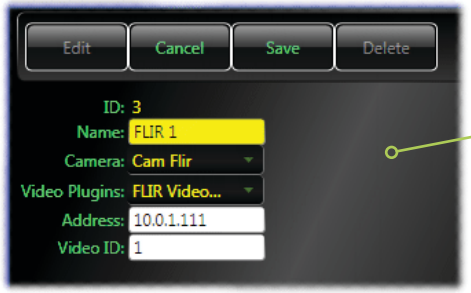
Adding a video viewer

Video viewers allow video inputs from cameras to be displayed for the operator when required. Most usually, video viewers are used in conjunction with optical or thermal imaging cameras that can be called upon when an incident occurs in the areas that they cover. If a video viewer was not added within the New Camera Wizard, use the procedure outlined here to add one where necessary.

To add a video viewer

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Video Viewers** entry and then click the **New** button. A blank video viewer configuration will be shown

2 Once you have completed the settings, click the **Save** button.



ID
The **ID** number is automatically set by Sentinel.

Name
The text entered here will be used to label the video viewer within the system.

Camera
Select the configured camera to associate with the viewer.

Video Plugins
Choose the appropriate video player plugin that matches the output type of the chosen camera.

Address
Enter the IP address or URL (Uniform Resource Locator) of the video feed from the camera.

Video ID
Optionally defines the video stream ID. This is used for camera systems that provide two or more separate video streams (e.g. multi-channel video encoder) that are switched between. Where different IDs are needed to select the required stream(s), enter the valid ID here.

Next steps

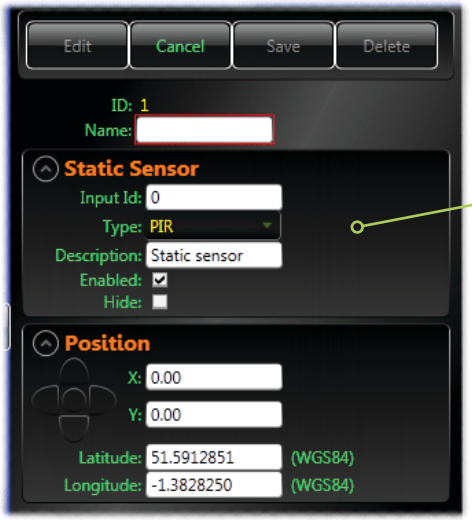
- Add static sensors
- Define rules

Adding a static sensor

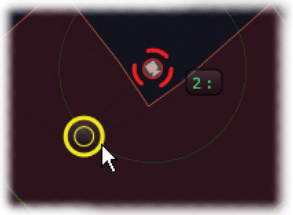
In addition to using dynamic sensors such as radars, the system can also monitor the outputs of static sensors such as light beams and PIR units. When a static sensor is triggered, an unmoving track is generated on top of the sensor within the Sentinel graphical representation. If the static sensor lies within an existing area and rule configuration for a radar, then the static track might be suitably handled by the system in the same way as tracks generated by the radar. If not, you can create a small dedicated area which encompasses the static sensor and then apply a simple area movement rule in order to produce the required alarm response.

To add a static sensor

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Static Sensor** entry and then click the **New** button. A blank static sensor configuration will be shown



2 Position the new sensor. Either enter the **X** and **Y** offsets from the installation origin point, or drag the yellow circle icon (that has been added within the site map) to the required location



3 Once you have completed the settings, click the **Save** button.

4 If the static sensor does not lie within an existing defined area, or the existing area uses an unsuitable rule (such as one that detects movement), create a new area and rule for the static sensor.

See the Adding an area and the Defining rules sections for details.

ID
The **ID** number is automatically set by Sentinel.

Name
The text entered here will be used to label the sensor within the graphical representation within the site map.

Input Id
Enter the identification of the hardware interface digital input to which the static sensor is connected. This Id number will uniquely link the sensor input with the configuration details stored for it.

Type
Choose the appropriate sensor type from the list, e.g. Broken Beam (sensors which are triggered when their invisible light beams are interrupted) or PIR (Passive InfraRed sensors which are triggered when they detect changes in radiated heat).

Description
This text field allows you to optionally add more detail about the sensor. This is particularly useful for location and differentiation purposes in large multi-sensor installations.

Enabled
Ensure that this option is ticked.

Hide
Allows you to simplify the clutter within the site map by concealing this item while leaving it working as usual. It can still be selected within the Object list whereupon it will be temporarily revealed within the site map.

X and Y (plus Latitude and Longitude)
Each new static sensor is initially assigned the default Latitude and Longitude of the installation origin. You can then adjust the **X** and **Y** settings to define the offset position (in metres) of the sensor from the origin point. You can adjust the **X** and **Y** settings either by typing the offsets into the fields or you can drag the sensor icon to the required position on the graphical representation.

The Lat. and Long. values for the sensor position are calculated using the known origin point plus the X and Y offsets.

Next step

- Define rules

Defining rules

One of the great strengths of the Sentinel application is its ability to assist the operator by making decisions in response to sensed target movements. As a result, a continual watch can be placed upon all areas of interest, with the operator being alerted (or other actions initiated) only when particular criteria are met. The key factor in enabling such intelligent automated behaviour is the use of *rules*.

Rules consist of basic conditions, such as:

- 'If a target enters this area then sound an alarm',

  or

- 'If a target is moving faster than 4 meters per second then follow it with a camera'.

These are useful enough, however, within the Sentinel application you can also combine two or more rules to apply very specific controls to particular regions. In addition to a set of adjustable default rules, you can also create any number of new rules using logical operators and other properties to achieve almost any desired outcome.

Rules are defined within the Sentinel application using the Rule Editor. To use the Rule Editor you must be in admin mode - see Entering admin mode.

Types of rules

There are various types of rules to suit different situations:

- **Approach rules** ask 'Is a tracked target closer than x metres to this location and moving towards it?'
- **Area rules** (Deprecated) ~~ask 'Is a tracked target inside or outside a specified area?' This most basic type of rule is solely concerned with where targets are located.~~

  Note: The Area rule has been replaced with the 'Area movement rule'. Existing area rules will be honoured, however, new ones cannot be created. See below.
- **Area movement rules** ask 'Is a tracked target inside or outside a specified area?' and (optionally) 'Does the behaviour (e.g. speed, direction) or appearance (e.g. size, radar signal strength) of a tracked target meet a given value (or range of values)?'
- **Compound rules** ask 'Have two selected rules been broken simultaneously?' A compound rule can reference any two other rules (including other compound rules) and respond when one, both or neither (e.g. selectable logic: *A OR B*, or *A AND B, or A NOR B*) are broken.
- **History rules** ask 'Have any selected rules (or combinations of selected rules) been broken now or in the past?' This type of rule is very useful when two or more conditions need to be met, but not simultaneously. For example: 'Has a tracked target passed through area A and then entered area B? If so, follow with a camera'. Historic rules are not normally used in conjunction with alarms themselves; they are best used as building blocks within other compound rules.
- **Numeric rules** ask 'Does the behaviour (e.g. speed, direction) or appearance (e.g. size, radar signal strength) of a tracked target meet a given value (or range of values)?' This rule provides the tools to search for various traits that can be defined numerically. For each property you define one (or two) limit value(s) plus a condition which, when met will cause an alarm to be raised.
- **Proximity rules** are primarily used to interpret the behaviour of vehicles and ask 'Is the vehicle moving slowly, stopped, reversing or in a queue?'
- **Static sensor rules** simply ask 'Has the static sensor been triggered'.

Rule conditions

Rule conditions form the core of each rule. The automated decision to take or not take action is determined using the properties that you combine within the Rule Editor. The choices of properties that you make will be determined by the type of behaviour that you need to isolate and also the type of rule that you use to achieve it.

Below are examples that demonstrate how various properties are combined to create valid decision making conditions for each type of rule. In every case, when the chosen conditions are met by one or more observed targets, a selected alarm and/or follow action can be instigated:

Numeric rule

Target **Size** **Is Greater Than** **1.0** metre

Property Name | Breaking Condition | Property Value

rule property setting

rule property label

Historic rule

Target **Entered the perimeter** and **Is at the checkpoint** . **All** conditions met

Linked Rule 1 | Linked Rule 2

Area movement rule

Target **Is Inside** **Outer Perimeter** and **Target Size (m)** and **Is Larger Than** **2** metres and its **Speed (m/s)** **Is Greater Than** **5** metres/second

Breaking Condition | Area | Property Name 1 | Breaking Condition 1 | Property Value 1 | Property Name 2 | Breaking Condition 2 | Property Value 2

Optional extra rule conditions

Approach rule

Target **LessThan** **50** metres (with a tolerance of +/- **5** metres) from an object

Distance check | Distance | Target +/-

Proximity rule

Target **Vehicle** is **Stopped**

Classification | Sub Type

Compound rule

Target **Is in the checkpoint area** **And** **Is moving faster than 4 Mps**

Rule 1 | Section Name | Rule 2

Static sensor rule

Sensor **Sensor Name** is **True**

Sensor | Trigger Value

For further details about each rule property, see Appendix 3 - Rule properties.

continued

Rule severity, actions and classification

You can determine what should happen whenever the conditions of a rule are met by the behaviour of one or more tracked targets.

Severity

The **Severity** setting allows you to define how a target should be marked when it breaks a rule. Such markings allow targets which present a warning or threat to be easily differentiated from friendly and unclassified targets. The severity choices are:

- **Unknown** - Use this setting when the rule is to be used as a building block for other compound and/or historic rules, where the severity level will be separately applied.
- **Friend** - Marks the target in **green**. Not generally used for highways use.
- **Warning** - Marks the target in **orange**.
- **Threat** - Marks the target in **red**.

Note: The severity setting only alters the appearance of the tracked target, it has no effect on the response to a broken rule; response is handled by the Action setting.

Action

The **Action** setting is where you determine the appropriate action to take when a rule is broken. The appropriate choice is generally determined by the nature of the installation and the area under consideration, but can also be influenced by the type of rule. For example, for simple rules (such as a basic Area movement rule) to be used in isolation, an alarm response is usually required. However, for rules that are destined to be included within compound rules, the norm is to leave the action configured as *None*. The *Action* choices are:

- **None** - No response.
- **Alarm** - Display a message and sound an audio alert within the Sentinel application.
- **Follow** - Instruct the nearest camera to follow the target - do not raise an alarm.
- **Alarm and Follow** - Display a message, sound an audio alert and instruct the nearest camera to follow the target.

Note: If neither 'Follow' nor 'Alarm and Follow' are selected then no cameras will respond to the target.

Classification

As part of the tracking process, attempts are continually made to differentiate between tracked objects of different types and to classify them accordingly: Person, Vehicle, Debris, etc. It may be the case that you wish to trigger alternate alarms for different types of objects in particular areas. The *Classification* option allows you to achieve this. For instance, it may be required to trigger a warning alarm for people in an area and a threat alarm for vehicles in the same area. By creating two similar rules with alternative Classifications and Severity settings, this task is made straightforward.

The related *Classification Probability* option allows you to define a confidence level which must be matched or exceeded for a given classified track before it can be considered within the rule. The main probability value is created during the tracking and classification process and is displayed against each entry within the *Tracks* tab.

Other rule settings

In addition to the main rule settings mentioned above, there are numerous other settings that allow you to tailor each rule to suit your installation. Below are brief descriptions of the other settings. For further details, see Appendix 3 - Rule properties.

- *Description* - shown on the operator's display when a rule is broken - see Appendix 4.
- *Persists* - target remains marked with the *Severity* when no longer breaking the rule.
- *Enabled* - must be ticked for the rule to be active.
- *Hide Tracks* - allows targets to be optionally hidden either: before they break the rule, after they break the rule, never or always.
- *Time Restriction* - optional operating periods for the rule, such as 'only on weekdays'.
- *Relay* - optionally enter the ID for a relay switch to activate when a rule is broken.
- *Allowance settings* - a collection of properties which enable you to define an 'allowance' which is the number of times a target is permitted to break a rule before an action is triggered.
- *Send SMS* - allows an SMS message to be sent to one or more telephone numbers containing the text entered in the *Alert description* field.
- *Disarm by Sensor* - allows you to create a temporary disarm mechanism (e.g. button or PIR sensor) so that the rules covering a detection area can be suspended to allow personnel to move through an area without triggering an alarm. This option is located within the *Disarm* tab.

continued

To define rules

Note: You must be in admin mode to make changes - see Entering admin mode.

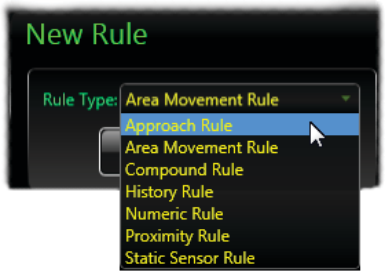
1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Rule Editor** button to display the following:

The page shows any currently stored rules in the upper section. You can edit any aspect of the current rules; copy and edit an existing rule to create a new one or define new rules from scratch.

3 Either:

- Edit an existing rule: Click on a rule entry in the upper section and then click the **Edit** button.
- Copy an existing rule: Click on a rule entry in the upper section and then click the **Copy** button. Then edit the copy to make any necessary adjustments.
- Create a new rule: Click the **New** button to reveal the Rule Type popup. Select the appropriate *Rule Type* (see the section Types of rules for details) and then click the **OK** button.



4 Use the properties (distributed across four tabbed pages) in the lower section to define the required behaviour of the rule. Many properties are common across the different types of rules, whereas others change depending upon the type of rule chosen. For a complete list of all rule options, see Appendix 3 - Rule properties.

Here are the general steps that need to be taken when defining a rule:

- Create a distinctive *Description* for the rule
- Determine the conditions that need to be met in order to consider the rule as broken. These vary according to the type of rule being defined - see Rule conditions.
- Choose the appropriate *Severity* marking for a rule-breaking target.
- Set the *Action* to be carried out if the rule is broken.
- Create a *Description* to be shown on the operator's display - see Appendix 4.
- Configure the other properties as appropriate for your installation (other properties are contained within the other tabs: *Advanced, Alerts* and *Disarm*) - see Appendix 3 - Rule properties.

5 Click the **Save** button.

6 Click the **Close** button to exit the Rule Editor.

Adding time restrictions/schedules to a rule

In situations where one or more rules need to be applied for limited time periods, use the related *Time Restriction* and *Schedule* options to define the required periods of inclusion or exclusion for any particular rule.

To apply a time restriction

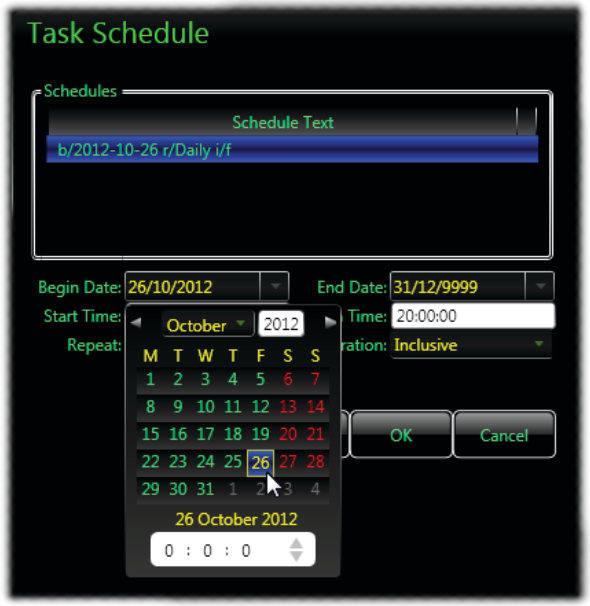
1 Display the required rule within the *Rule Editor* and click the **Edit** button.

2 Click the **Time Restriction** drop down list and select the **Custom** option.

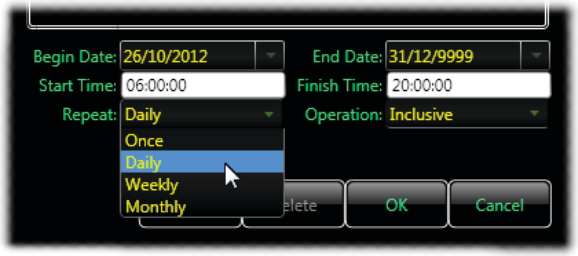
3 The **Schedule** button will become available at the bottom of the dialog, click it to display the *Task Schedule* pop up.

4 Click the **Begin Date** drop down list and choose an appropriate start date.

5 Click the cursor into the **Start Time** field and enter the required start time.



6 Click the **Repeat** drop down list and choose how the schedule should be applied: *Once, Daily, Weekly* or *Monthly*.



7 Click the **End Date** drop down list and choose an appropriate date.

8 Click the cursor into the **Finish Time** field and enter the required end time.

9 Click the **Operation** drop down list and choose whether the defined schedule period is **Inclusive** (i.e. the rule will only be active during this period) or **Exclusive** (i.e the rule will only be active outside of this period).

10 Click the **OK** button to save the settings.

Operation

Sentinel screen layout

The system processes potentially vast quantities of data as it monitors the areas within its view. It is the job of the Sentinel application to provide the operator with a clear view of the proceedings with easy-to-use controls and also deliver automated overview and alarm facilities.

Navtech menu icon
Click to display a menu of options.

Object picker
Popup buttons that allow you to choose between displayed objects.

Selection panel
Includes a *Settings* tab where you can adjust various key display settings.

Site map
Displays the radar scan(s), defined area(s), identified tracks and camera positions. To move around the area, click and drag on any part of the background image.

Tracked object
Click on a tracked object to view further information about it, such as its speed, direction, size, etc.

Quick commands panel
Zoom buttons allow you to alter the view magnification. Other buttons are also displayed with functions related to the currently selected item.

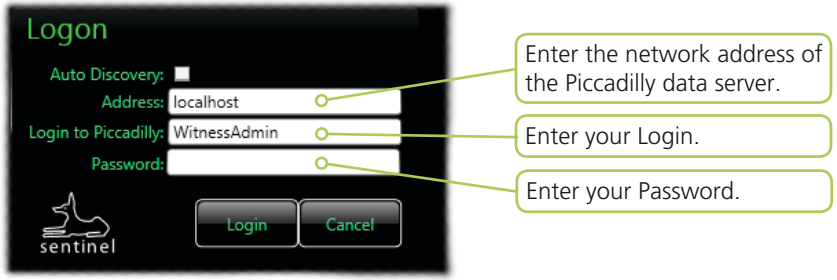
Logs and alarms panel
Four tabs allow you to switch between lists of alarms, system alarms, logs and manual (historic) logs.

Information panel
Displays information and options for items that are selected either within the selection panel above or the site map.

Logging on

When you first enter the Sentinel application, you may need to logon to the Piccadilly data server.

The logon popup appears as follows:



To logon

1 Either:

- Enter the valid **Address** for the Piccadilly data server (enter 'localhost' if the server is on the same system as your Sentinel viewer), or
- [Where multiple Witness installations are present] Place a tick in the **Auto Discovery** checkbox. The **Address** field will change to **Group Name**, whereupon you can enter the unique name for the appropriate server group and the application will search for the appropriate server.

2 Enter your **Login** name and **Password**.

3 Click the **Login** button.

Login levels

There are three login levels, each with their own abilities:

- **Admin** Can alter any aspect of setup or operation.
- **Supervisor** Can edit existing items but cannot create or delete any.
- **User** Is able to view system operation only. No access to configuration.

Getting help

The Navtech Sentinel application has a built-in help system.

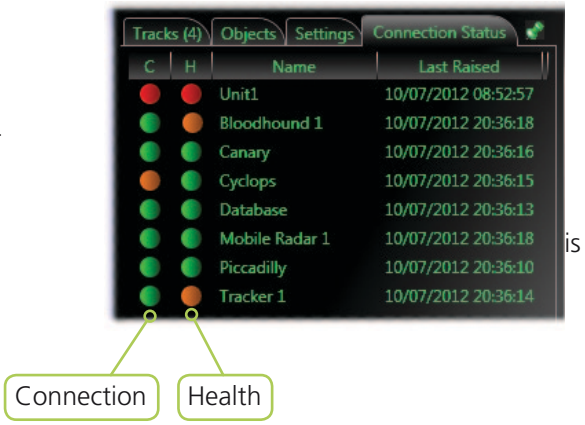
To access help

- Press the F1 key.

Checking status

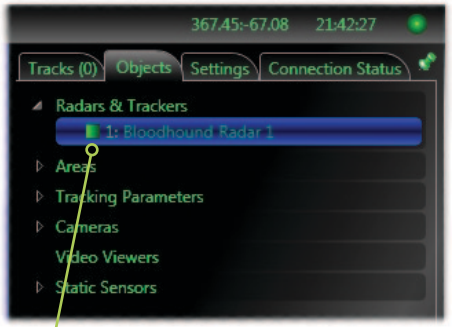
When logging in and periodically, you are recommended to check the Connection Status tab in the top right corner of the screen. This simple list will quickly show whether any main system components are currently in error.

If communication with a module is lost, the corresponding indicator will show amber for 30 seconds and, if the link is not restored, the indicator in the second column will turn to red until the problem is resolved.



Other status indicators

In addition to the full list of status indicators provided within the *Connection Status* tab, certain items within the *Objects* tab also provide quick visual feedback on their condition. Each radar and its tracker provide a single status square which effectively combine their respective connection and health monitors into one. The single indicator shows the lowest condition of the two contributing factors, e.g. if Connection is green but Health is amber, the single indicator will show amber. You can then check the Connection Status tab to discover which factor has a potential issue.



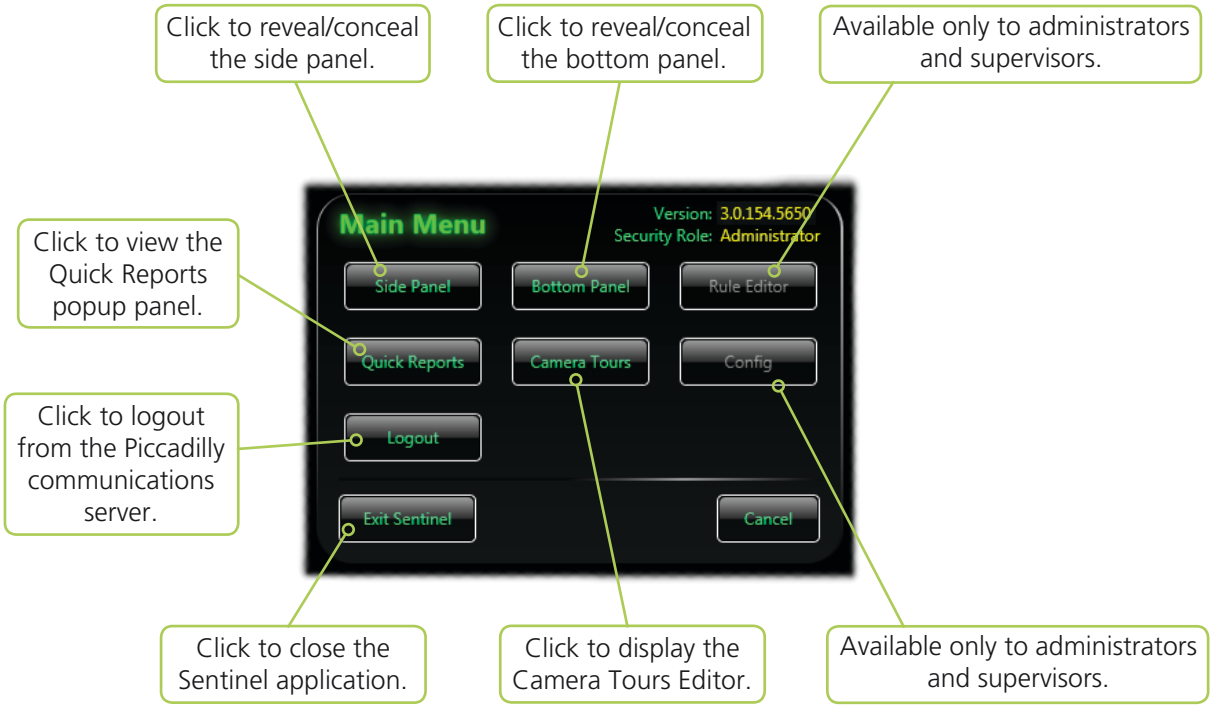
Main menu

The main menu allows you to hide/reveal the side and bottom panels as well as logout from the Piccadilly server and exit from the Sentinel application.

To access the Sentinel main menu

1 Click the Navtech logo located in the top left corner of the Sentinel window ➲

The main menu will be displayed:

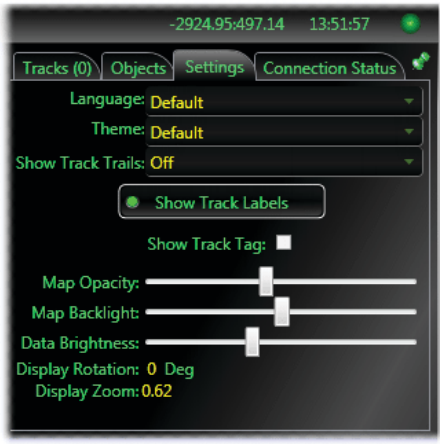


General screen navigation

The Sentinel application provides several controls that allow you to quickly adjust how items appear within the site map.

To adjust your screen view

1 In the selection panel in the top right hand corner, click the **Settings** tab.



The following options are provided:

- **Show Track Labels** - Determines whether the information labels for each track are displayed. When there are many tracked vehicles in an area, their labels can obscure the view. This is a quick way to temporarily hide them.
- **Show Track Trails** - Determines whether each track should show a short series of trail markers to highlight the direction of travel. *Note: You can also apply a trail to an individual track. Click on the track and then click the **Trail** button on the Quick commands panel on left side of the site map.*
- **Map Opacity** - Allows you to adjust the transparency/opacity of a static background image to allow other details to be seen more clearly. The *Open Street Map Opacity* setting performs a similar task for dynamic map backgrounds.
- **Map Backlight** - Allows you to adjust the brightness of the background image.
- **Data Brightness** - Allows you to adjust the brightness of the radar data that is overlaid onto the background image when aligning a radar sensor.
- **Display Rotation** - Indicates the level of rotation of the background image.
- **Display Zoom** - Indicates the current level of zoom applied to the site map.

To move around the map

You can quickly move to any region of the graphical representation using your mouse.

- Click and hold the left mouse button on any part of the graphical representation and drag to reveal the required region of the screen.

To zoom in and out

There are two ways to change the site map zoom level:

- Click on the **+** and **-** buttons at the top of the quick commands panel,

  or

- Use the scroll wheel on your mouse (if fitted) when the pointer is in the site map.

The current zoom level is indicated within the **Settings** tab in the top right corner.

To select an object

Selecting an object (e.g. an area, a camera, a radar sensor, etc.) is usually as simple as clicking on it with your mouse. However, where numerous different items are overlaid in busy areas of the site map, the Sentinel application may display an object picker panel in the top right corner of the site map:

Click on the required item to confirm your choice.

Once the object is selected, its outline will be highlighted and relevant options for that item will be made available in the information panel and/or quick commands panel, as appropriate.

Monitoring tracks

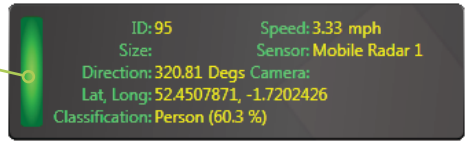
During operation there could be peak periods when many tracks are shown moving within the site map as people and vehicles are identified and monitored. Accordingly, each detected object is listed within the Tracks tab of the selection panel.

To select a displayed track

1 In the site map, click on the required track:

Highlighted and un-highlighted tracks

A track detail panel will be displayed in the top left corner of the site map, with further information such as the size (if calculated), direction and precise position of the track.



Also, any relevant actions for the track will be added to the quick commands panel on the lower left side of the site map.

See the next page for details about using these command buttons.

The selected track's entry within the Tracks tab will be highlighted.

The panel below the Tracks tab will show a wide variety of details for the track, including any rules that it is currently breaking...

... as well as a running total of break counts for rules that have previously been impinged.

2 To release the track, click anywhere else within the site map.

While a track is highlighted

As discussed left, when a track is highlighted, the quick commands panel provides a variety of relevant options.

To follow a selected track

In the quick commands panel on the left side of the site map, click the **Follow** button. This action will cause the track to remain highlighted (with pulsating white rings) within the site map as it progresses through the monitored area.

Additionally, where suitable camera facilities exist, this action will request the closest camera to 'lock' onto the track and follow it. If the track moves closer to another camera or moves out the current camera's field of view then it will be handed over to the next most suitable camera. The track will maintain at least one dedicated camera for as long as the radar can see it. Click the **Follow** button again to cancel the exclusive tracking and return to normal operation.

To turn on/off the trail for a selected track

In the quick commands panel on the left side of the site map, click the **Trail** button. The trail maps out the recent movements of the track. Together with the direction arrow that is always applied to each track, this may assist with determining the track movements.

Note: You can apply trails to all tracks using the Show Track Trails button within the Settings tab. However, where there are many tracks, the screen can quickly become very congested.

To change the severity for a selected track

If a track is spotted behaving in an unusual manner that does not contravene any configured rules, you can mark it using the quick commands panel on the left side of the site map. Click on the track and then click on either Warning or Threat. The new classification will remain with the track.

Using the Tracks list

You can quickly locate a track.

To locate a listed track

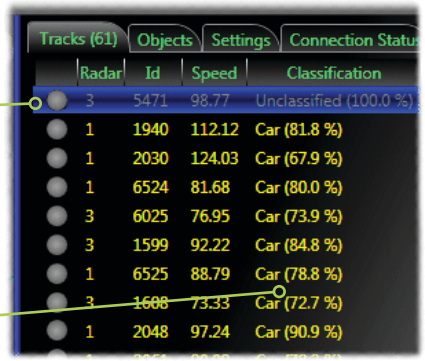
1 In the selection panel in the top right hand corner, click the **Tracks** tab.

2 Next, either:

- Single click on any listed track entry. The chosen track will be highlighted within the site map, or
- Double click on any listed track entry. The site map will pan and zoom in to show the highlighted tracked vehicle at the centre of the screen.

Single- or double- click a track entry to highlight the related track entry within the site map.

The percentage values shown indicate the level of confidence in the classification that has been applied to each target. The higher the value, the more confident the tracker has been in identifying the type of target.



3 See left for details about what you can achieve once a track is highlighted.

*Note: You can also locate any object, e.g. an area, a radar, a static sensor, a camera, etc. by double clicking an entry within the **Objects** tab.*

Classified tracks

Once a sufficient level of certainty is achieved for each track, a symbol will be added to the track label within the site map, for example:

Classifications:
Vehicle
Person

The colour of each symbol changes according to the severity status for the track

Grey	Unknown
Green	Friend
Amber	Warning
Red	Threat

Controlling cameras

Although the cameras are usually controlled automatically, you can also take direct control.

Move the closest camera to a chosen location (absolute positioning)

- Move the mouse cursor to the required location in the site map and click the right mouse button. The nearest camera to the location will move to view your chosen location. The camera will remain viewing your location until it is commanded by the system to follow a new tracked vehicle or will return to its home position after a timeout period.

Move a selected camera to a chosen location (absolute positioning)

1 Click (left mouse button) on the image of a camera ( ) within the site map.

2 Move the mouse cursor to the required location in the site map and click the right mouse button. The selected camera will move to view your chosen location. The camera will remain viewing your location until it is commanded by the system to follow a new tracked vehicle or will return to its home position after a timeout period.

Move a camera using the joystick control (relative positioning)

1 Click (left mouse button) on the image of a camera ( ) within the site map.

Note: If there are multiple items nearby (e.g. areas, radar sensors, other cameras, etc.), two or more view buttons will be displayed in the upper right corner of the site map to help you choose the required item. Click the view button that has the name of the required camera.

2 The selection panel will change to the **Objects** tab and will show the details for the chosen camera. Use the joystick within the panel to pan and tilt the camera ➲

Note: A 'view circle' will be overlaid on the graphical representation indicating the approximate area currently being viewed by the camera.

Camera control tips

- Click the outer horizontal buttons to pan (x-axis).
- Click the upper/lower buttons to tilt (y-axis).
- Click and drag the middle button to move the camera in any direction.
- To reset the camera to its home position, click (and release) the middle button.
- **+/-** In operation, these buttons zoom in and out.
- Menu**/**Select - Available only in admin mode and only then if the selected camera supports their use. These control access to, and navigation within, the internal menu of the camera. When menu mode is invoked, you can then use the joystick controls and Select button to control the camera menu, as you would with a standard camera controller.

Control cameras using quick command buttons

- Click (left mouse button) on the image of a camera ( ) within the site map.

Note: If there are multiple items nearby (e.g. areas, radar sensors, other cameras, etc.), two or more view buttons will be displayed in the upper right corner of the site map to help you choose the required item. Click the view button that has the name of the required camera.

In the quick commands panel on the left side of the site map, click the required camera control button:

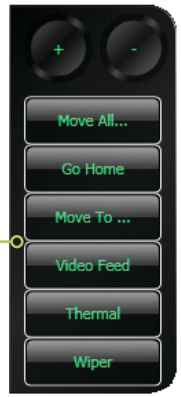
Move All...
Instructs all cameras within range to focus upon the location that you next click (left mouse button) within the site map.

Go Home
Instructs the selected camera to return to its pre-programmed home position.

Move To...
Instructs the selected camera to focus upon the location that you next click (left mouse button) within the site map.

Video Viewer (Video Feeds) buttons
For cameras that have multiple video feeds, e.g. optical and thermal, multiple buttons will be displayed to allow the required feed to be viewed.

Wiper
For cameras with a lens wiper, instructs the wiper to operate.



Home a camera

1 Click (left mouse button) on the image of a camera ( ) within the site map.

2 The quick command panel should appear on the left side of the screen ➲

3 Click the **Go Home** button.

Using camera tours

Running a camera tour

Once a camera tour has been created and enabled, you can set it running at any time. Camera tours are given the lowest priority within the operation of each camera, which means that while a tour is running, any other automated or operator-induced request will cause the tour to be paused while the higher priority task is carried out. The camera will then return to the tour once the other task has timed out.

In order to switch camera tours on and off, you must ensure that the appropriate button is enabled within the quick commands panel, see below.

To enable the Touring button

Note: You must be in admin mode to make changes - see Entering admin mode.

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.
2 Click the **Config** button and then choose the **Quick Commands** tab.
3 Click the **Edit** button and ensure that the **Touring** checkbox is ticked. Also ensure that the *Quick Panel Is On* option is also ticked.
4 Click the **Save** button and then click **Close**.

The *Touring* button should now appear on the popup quick commands panel whenever a camera is selected.

To run a camera tour

1 Select the required camera.
2 The quick command panel should appear on the left side of the screen
3 Click the **Touring** button. The Green indicator within the button should illuminate.

Note: If the button appears but is greyed out, check within the Camera Tour Editor popup that a tour for the current camera is enabled.

If the button does not appear at all when the camera is selected, see 'To enable the Touring button' above.

Once the camera tour begins, you should see the camera image within the site map changing between the various preset positions defined within the tour

The superimposed beam line shows the preset position that is currently being viewed

To stop a camera tour

1 Select the required camera.
2 The quick command panel should appear on the left side of the screen.
3 Click the **Touring** button. The Green indicator within the button should extinguish.

To edit a camera tour

Note: You must be in admin mode to make changes - see Entering admin mode.

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.
2 Click the **Camera Tours** button.
3 Click the **Camera** field at the top of the popup and choose the required camera from the drop down list.
4 Click the **Tour** field at the top of the popup and choose the appropriate tour from the drop down list. The position presets within the tour will be listed within the middle section of the popup.
5 Click the **Edit** button.
   - To move a preset - Click on the preset to highlight it and then use the **^** and **v** buttons move the highlighted entry up or down.
   - To add/remove a preset from the tour - Click on the preset to highlight it and then click on its checkbox to tick (include) or untick (exclude).
   - To add/remove all presets - Click the checkbox that is at the top of the list, adjacent to the *Presets:* heading.

   When you have made your changes, click the **Save** button.

   To remove the whole camera tour, click the **Delete** button.
6 Click the **Close** button to exit.

Alarms

The Sentinel application provides clear information to the operator when alarms are triggered. The precise nature of an alarm condition is determined by the rules that are applied to each area.

When an alarm is triggered

When one or more tracks meet certain pre-determined conditions, then the affected area(s) will go into alarm. Such instances will be reported to the operator in several ways:

- An audible alert may be sounded.
- One or more popup panels will appear at the top right corner of the site map and slide down the screen until they are removed at the lower right corner:

Alarm notifications appear at the top right corner of the site map, then slide down the screen...

...and disappear at the lower right corner.

Red panels indicate the start of an alarm while green panels are displayed when the alarm condition has been resolved.

To locate an alarm using a popup panel

When an alarm occurs you can click directly on the corresponding popup panel. This will cause the panel to expand and show two buttons:

- Click the **Locate** button to instruct the nearest camera to pan, tilt and zoom so that the cause of the alarm can be viewed. The site map will also respond accordingly.

- All alarms are also logged within the Alarms tab at the base of the screen:

For each entry, the following details are listed:

- **Alarm Id** - Shows the id number given to each alarm.
- **Action** - Determined within the rule associated with the area under surveillance. Possible actions are: *None*, *Follow*, *Alarm* or *Alarm and Follow*. Follow means that the nearest camera should follow the track. Alarm means raise a specified alarm, e.g. audible for the operator and/or trigger an external system.
- **Description** - Explains the nature of the alarm.
- **Last Activated** - Indicates when the alarm was triggered by the track.
- **Relay Id** - Shows the identification number of the output relay that was programmed to be triggered as part of the alarm response.
- **Rule** - Indicates the rule that was broken by the track and triggered the alarm.
- **Acknowledged** - Becomes ticked when the user acknowledges the alarm.

To respond to an alarm using the Alarms tab

1 When an alarm occurs, change to the **Alarms** tab at the base of the site map.
2 Click on the alarm entry within the list to highlight it.
3 Click one of the two buttons located on the at the right side of the Alarms tab:
   - Click the **Locate** button to instruct the nearest camera to pan, tilt and zoom so that the cause of the alarm can be viewed. The site map will also respond accordingly.

     OR
   - Click the **Dismiss** button to acknowledge and silence the alarm.

continued

Alarm acknowledge panel

Depending upon the configuration of the installation, it may be necessary for the operator to acknowledge alarms as they occur. When this option is enabled, whenever an alarm occurs, a pulsating alarm acknowledge icon will be displayed in the top centre of the screen:

When you click the icon, the Alarm acknowledge panel will be displayed:

Place a tick by each alarm to be acknowledged (click the top tick box to select all) and then click the **Acknowledge Selected Alarms** button to close the panel.

A timed (and attributed) entry is placed into the log for each acknowledged alarm.

Note: It is also possible for the admin user to invoke an automatic acknowledge feature where alarms can be cleared after a set period of time.

System Alarms tab

The System Alarms tab maintains a list of any issues that were encountered within the various modules that make up the system.

If a system alarm entry is not automatically cleared, you can manually clear an entry. To do this: Click on the red circle to the left of an alarm entry and then click OK in the resulting popup to confirm the action. Once cleared, an alarm for the same problem will only occur if the fault is resolved and is then freshly detected.

Log tab

The Log tab maintains a listing of all significant events related to the operation of the Witness system.

For each entry, the following details are listed:

- **Alarm Id** - Automatically assigned index number for each alarm.
- **Time** - The date and time that the event first occurred.
- **Last Seen Time** - The last date and time that the same event was triggered.
- **Type** - Indicates the type of event: *User* (an action carried out by the operator) or *Alarm* (the status of triggered alarms).
- **Description** - A brief explanation of the event.

Database Queries

Sentinel logs and retains all monitored track data within a central database for selected periods of time. To make that archived data particularly useful, the system also features powerful query tools as well as an export function so that information can be studied externally.

Note: You must either be in admin mode (or access must be specifically granted by admin) to access the Data History functions - see Entering admin mode.

Using Quick Reports

The Quick Reports popup provides immediate access to some very powerful database search tools that can help you to find various occurrences. Data searches can operate on either of two main sources of information held by the system:

- **Tracks** - includes all recorded movements of targets,

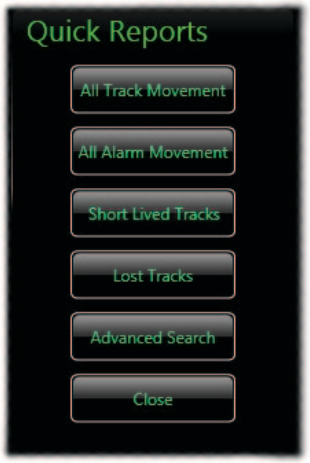
  and

- **Incidents/Alarms** - includes only those target movements and/or occurrences that caused rules to be broken.

To make a quick report query

1 Click the Navtech logo located in the top left corner of the Sentinel window to display the main menu.

2 Click the **Quick Reports** button to display the *Quick Reports* popup



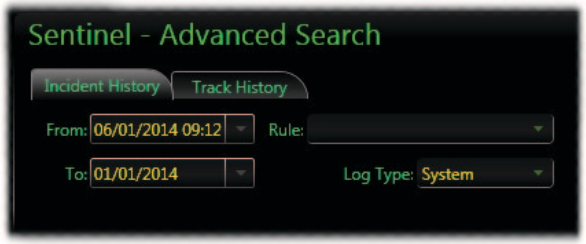
The first four buttons: *All Track Movement, All Alarm Movement, Short Lived Tracks* and *Lost Tracks* are all quite self explanatory. When clicked, each of these produce three additional buttons so that you can choose the appropriate time period: *Last hour, Last 30 minutes* or *Last minute*.

The fifth button causes the **Advanced Search** dialog to be displayed whereupon you have access to more wide ranging and powerful search tools. See right.

3 Choose the required option. The results from any query will be displayed at the bottom of the site map in either the *Incident Results* tab or the *Track Results* tab depending on which type of data you are searching for. See the next page for details.

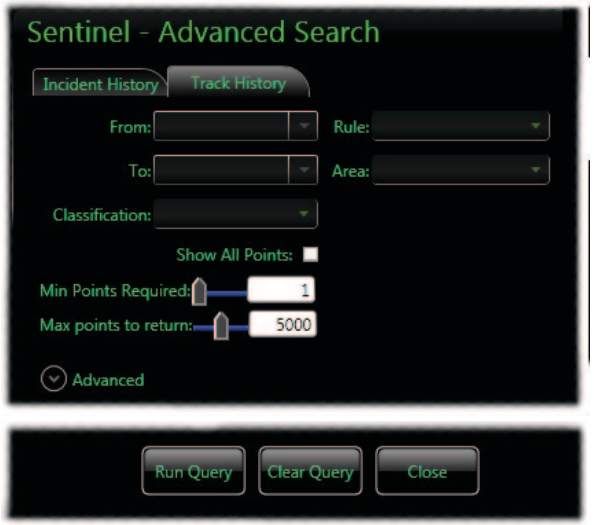
The Advanced Search dialog

The Advanced Search dialog is reached via the Quick Reports popup - see left.



The two tabs within the Advanced Search provide quick access to either *Incident* or *Track* Histories, as required.

In both tabs you can define a time period for your search. Additionally, the Incident History tab allows you to also search by Rule and/or specific Log Type (e.g. Alarm, System, User, etc.).



The *Track History* tab provides many additional query items such as *Area*, target *Classification* (e.g. *Vehicle, Person*, etc.). In the dropdown *Advanced* section you can also refine your search for tracks using *Speed*, *Size* and/or specific track *Tag* details.

In the *Track History* tab you can also determine how many track points (individual sightings by the sensor(s) that you wish to include) in the results.

When your criteria are set, click the **Run Query** button. The results from your query will be displayed at the bottom of the site map in either the *Incident Results* tab or the *Track Results* tab depending on which type of data you are searching for.

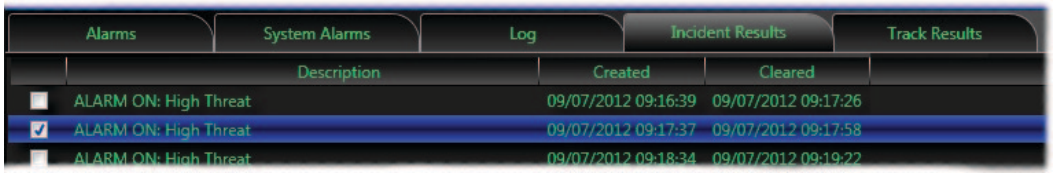
See the next page for details.

Notes about creating searches

- Beware of large databases. Depending on how long the installation has been running and the way that the rules have been established, it is possible that the log contains many thousands of entries. For this reason you are recommended to initially define quite tight criteria and widen the search gradually if that does not encompass the required data.
- Where criteria are left blank, they will not be applied as limiting factors to the search.
- Searches within a large database may take a long period to complete.

Viewing the results of a quick report or advanced search

Once your quick report search or advanced search (see previous page for details) has completed, the results will be posted at the bottom of the site map in either the *Incident Results* tab or the *Track Results* tab depending on which type of data you are searching for:



A typical result from an incident/alarms search shown in the Incident Results tab

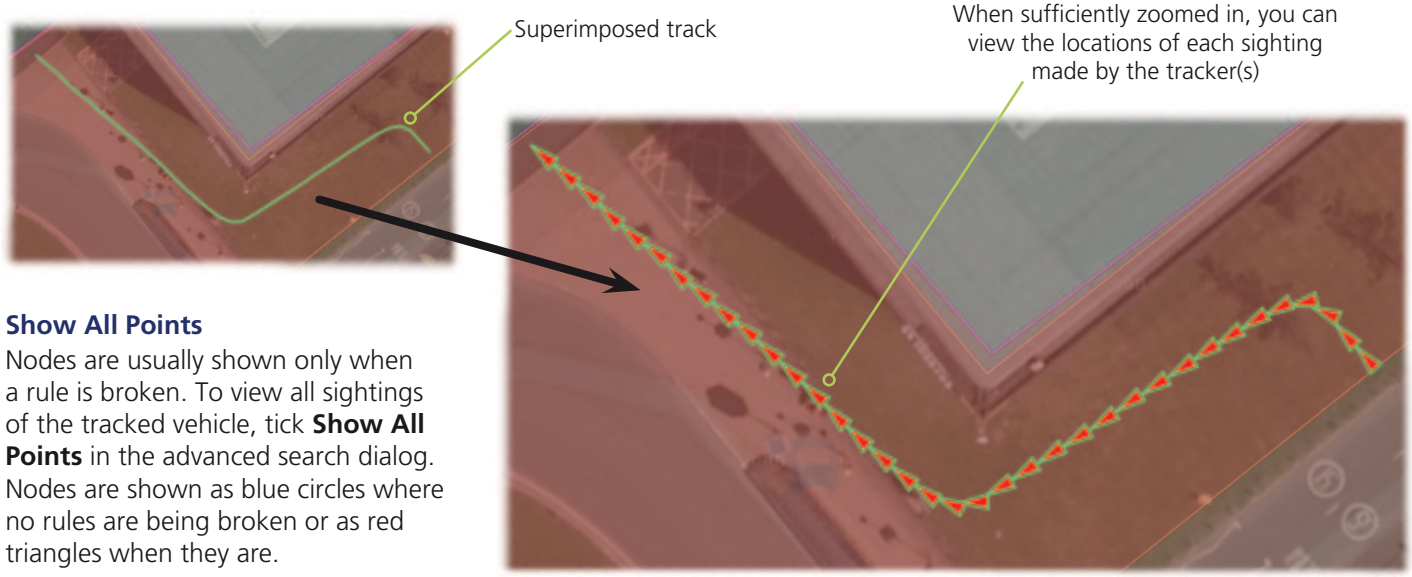
Tip: You can click a column heading in either tab to relist the entries within that tab in either ascending or (click again) descending order.

A typical result from a tracks search shown in the Track Results tab

Once search results are listed you can investigate them further or use the **Data Export** button to copy them to a file.

To view tracks

- If you searched for tracks, click on the **Track Results** tab. Tick the entries that you wish to view (or tick the box at the top to select them all). Then click the **Show Tracks** button to superimpose the selected points onto the site map.
- If you searched for alarms or incidents, click on the **Incident Results** tab. To search for tracks related to an alarm/incident, tick that entry and click the **Find Tracks** button. The results will be shown in the **Track Results** tab. Use the procedure described above to view the tracks.



Show All Points

Nodes are usually shown only when a rule is broken. To view all sightings of the tracked vehicle, tick **Show All Points** in the advanced search dialog. Nodes are shown as blue circles where no rules are being broken or as red triangles when they are.

Further information

This chapter contains various useful reference sections:

- **Appendix 1 - Object panels**
  Objects > Static Sensors
  Objects > Areas
  Objects > Radars & Trackers
  Objects > Tracking Parameters
  Objects > Cameras
  Objects > Video Viewers
- **Appendix 2 - Configuration options**
  Configuration > General
  Configuration > Map
  Configuration > Quick Commands
  Configuration > Maintenance
  Configuration > Global
  Configuration > Data Export
- **Appendix 3 - Rule properties**
- **Appendix 4 - Alarm description placemarkers**
- **Appendix 5 - Adding items without wizard assistance**
- **Appendix 6 - Using the allowance curve**
- **Appendix 7 - Recording radar data**
- **Appendix 8 - Object classification**
- **Appendix 9 - FAQs**
- **Appendix 10 - Computer hardware recommendations**
- **Appendix 11 - Additional runtime modules required**
- **Appendix 12 - Extending the edit time allowed**
- **Appendix 13 - Troubleshooting**
- **Appendix 14 - Radio frequency energy statement**

Appendix 1 - Object panels

This appendix lists all of the options available within the Object tab of the side panel. Many of the options within this area are fundamental to the base-level operation of the system and so care should be taken when editing such items.

To view/edit options within the Object panels

Note: You must be in admin mode to access this section - see Entering admin mode.

1 In the selection panel in the top right corner (if not shown, click the small panel button on the right hand edge to reveal), click the **Objects** tab to reveal the list of key items within the system

The headings within the list (e.g. Areas, Radars & Trackers, etc) are expandable items which can each contain multiple items to reflect the contents and complexity of the installation.

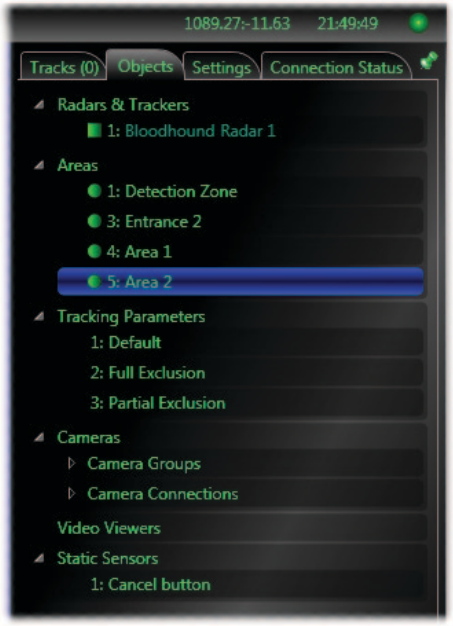
The buttons and the options shown within the information panel immediately below the headings will change depending on what is highlighted within the selection panel.

2 Use the selection panel as follows:

- Click a heading to select it.
- Double-click a heading to reveal / conceal its contents (or click the small arrow to reveal/conceal the contents).

You can then, for instance, add an entry to a selected heading, by clicking the **New** button that becomes available.

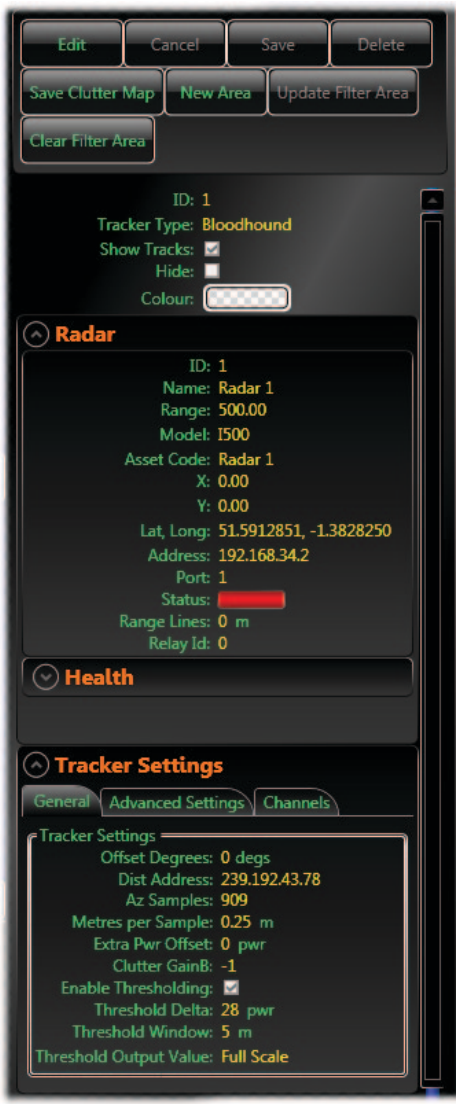
- Double-clicking an object that is visible within the site map will automatically pan the display to the selected item.



The options contained within the following Object panels are covered within this appendix:

Objects > Radars & Trackers

This panel allows you to determine the base-level settings for each radar/ tracker pair and also to view important status information.



Save Clutter Map

The *Clutter Map* is a record of static, unchanging objects that are within view of the radar sensor. For efficient operation of the system, a new clutter map should be periodically created using this button and then used to inform the tracker to ignore those static objects. See Creating and viewing clutter maps for more information.

New Area button

Click to create a new filter area for radar data. This creates a new entry within the Object > Areas section that allows you to define an area of interest within the total radar scanning zone. Once the filter area is defined it is sent to the radar sensor whereupon only data from within the area is transferred to the tracker, thus considerably reducing the network bandwidth consumed. See Adding a radar filter area for details.

Update Filter Area button

Once the filter area has been defined (using the New Area button), click this button to send the coordinates to the radar sensor. When any changes are made to the filter area, use this button again to ensure that the sensor is kept up to date.

Clear Filter Area button

Use this button to inform the radar sensor to return to sending full sweep data.

Identification details

- **ID** - This number uniquely links the tracker and the radar sensor to an appropriate copy of Bloodhound.
- **Tracker Type** - Determines the type of tracker being used. Options include: *SPx Tracker*, *Navtech*, *Navtech Highway*, *Bloodhound*.
- **Show Tracks** - Must be ticked for tracks to appear within the site map.
- **Hide** - Allows you to simplify the clutter within the site map by concealing this item while leaving it working as usual. It can still be selected within the Object list whereupon it will be temporarily revealed within the site map.
- **Colour** - Use to optionally apply shading to the radar range area.

Radar

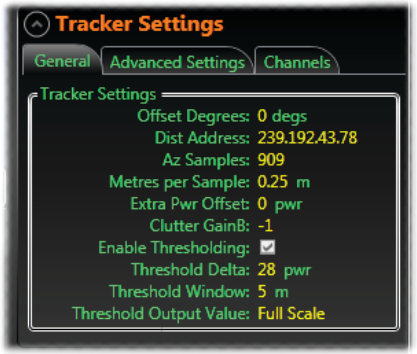
- **ID** - This number uniquely links the tracker and the radar sensor to an appropriate copy of Bloodhound.
- **Name** - Enter a distinctive name for the radar sensor. This name will be displayed on the graphical representation within the site map.
- **Range** - Defines the outer range of the radar sensor in metres. This value is used on the graphical representation within the site map.
- **Model** - Displays the model name/number of the radar sensor.
- **Asset Code** - Required serial number of the radar sensor. If none exists, is unknown or not required, then enter any text string as a placeholder.
- **X**, **Y** - Defines the position (X, Y) of the radar sensor from the origin point in metres.
- **Latitude**, **Longitude** - States the absolute coordinates of the radar sensor. These figures are derived from the origin point and the X and Y values.
- **Address** - Enter a valid IP *Address* for the radar sensor.
- **Port** - This is usually set at 700.
- **Status** - Provides a visual indication of the link quality between the radar sensor and the Bloodhound tracker.
- **Range Lines** - Defines the distance between the range lines that are shown on the graphical representation within the site map.
- **Relay Id** - Defines the ID of the relay that should be activated if the connection is lost between the radar sensor and the tracker. Choose '0' to disable.

Objects > Radars & Trackers (continued)

Health

This section provides useful feedback from the radar sensor, including the ambient Temperature within the radar sensor, the current speed of Rotation of the scanning element and the speed (Packet Rate) at which information is being transferred from the radar sensor to the tracker service.

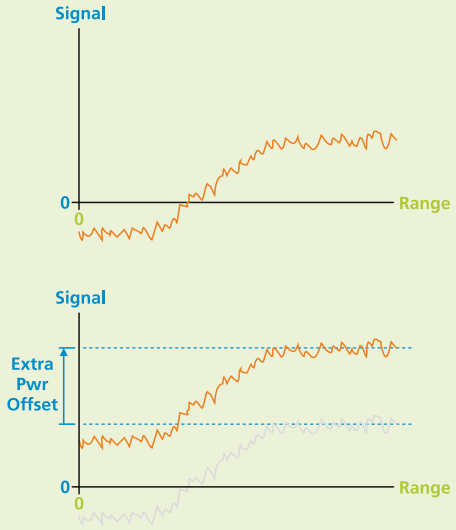
Tracker Settings (General tab)



- **OffsetDegrees** - Defines the angular offset required to ensure the radar data is aligned to North. If the radar sensor is pointing North then this value would be zero. It is essential that this value is accurate as it directly impacts upon how details seen by the radar sensor are represented within witness.
- **DistAddress** - Indicates the multicast or unicast IP address that should be used to distribute radar data when the *DistActive* option is ticked. This entry is automatically set by the system when a new tracker is created.
- **Az Samples** - This value tells Witness how many azimuth samples to expect from the radar. If the amount of samples received does not match the specified amount, the samples will be averaged so they do.
- **Metres per Sample** - This value shows the range resolution of the current radar.
- **Extra Pwr Offset** - Used to increase all incoming power readings by a fixed amount. This is typically used for the AGS model of radar. See below.

Extra Pwr Offset

This option is used when the signal levels being received by the radar sensor are tailing off to such a point that they drop below the baseline level.

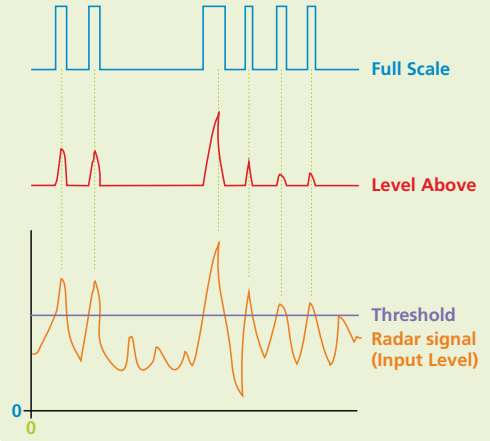


By applying an *Extra Pwr Offset* value, the received signal can be raised to such a level that the full range is above zero and can be fully interpreted.

- **ClutterGainB** - Adjusts the way in which the tracker processes the background clutter information. A lower figure means more of the signal from each scan is incorporated into the background clutter. This helps reduce false alarms from trees/foliage moving in the wind, etc. However, it also reduces sensitivity by being less concerned with minor fluctuations in the clutter, which could be genuine movement. Typical values are between -1.0 and -1.5. Values lower than this can affect tracking performance while values higher than -1.0 can cause too many false alarms.
- **Enable Thresholding** - When ticked, enables the threshold feature whose settings are explained below.
- **Threshold Delta** - Defines the threshold above which the signal will be included for track processing. Signal levels below this threshold will be discarded. Setting a lower threshold value provides greater detection capability but can correspondingly increase the level of false alarms.
- **Threshold Window** - The moving window size over which to calculate the dynamic threshold. The noise is averaged over this window size and the threshold delta is applied to this averaged value to check for significant power returns.
- **Threshold Output Value** - Defines the value that will be sent through to the tracker when a radar input signal exceeds the ThresholdDelta value. See below.

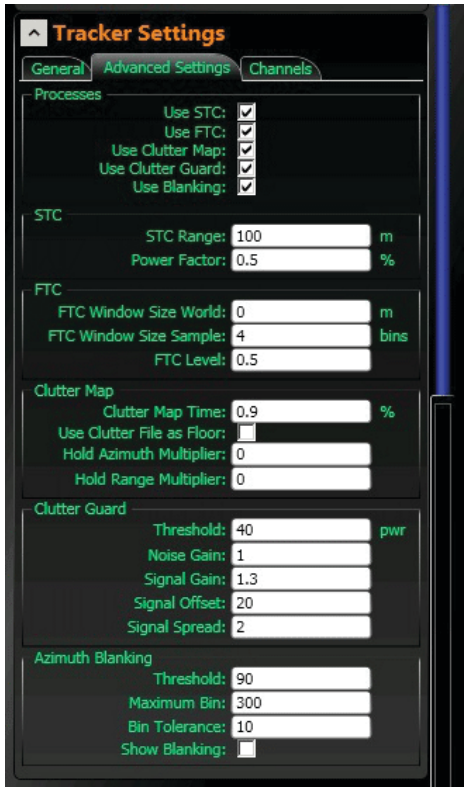
Threshold Output Value

This determines how the input signal from a radar should be conditioned before being passed on to the next stage. *Input Level* simply passes on the radar signal unchanged. *Level Above* subtracts the Threshold value from the radar signal to isolate only the signal that exceeds the threshold. *Full Scale* converts any signal that exceeds the Threshold essentially into a binary signal (i.e. either zero or 255).



continued

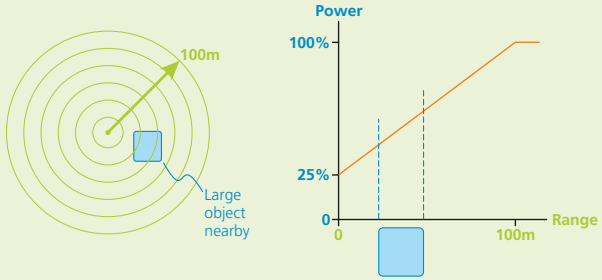
Tracker Settings (Advanced tab)



- **Use STC** - When ticked, enables the STC feature to reduce clutter from nearby static objects. See right.
- **STC Range** - Defines the distance up to which the attenuation specified in the *Power Factor* field should be applied.
- **Power Factor** - Determines the attenuation that should be applied to operation within the distance to local objects that are specified in the *STC Range* field.
- **Use FTC** - When ticked, the tracker will use a *Fast Time Constant* high-pass filter to help reduce the impact of rain on radar results.
- **FTC Window Size World** - Defines the width of the window (in metres) used for the high-pass filter.

STC (Sensitivity Time Control)

This is a feature that helps to reduce clutter by selectively attenuating the radar signal power to allow for nearby interfering factors, such as buildings, gantries and even rain.



Once the *Use STC* option is ticked, the tracker will apply the chosen Power Factor (from 0 to 1 where 1=100%) to a range of zero metres and scale up (in linear fashion) to 100% at the stated STC Range. As a result, the effect of nearby objects is reduced.

- **FTC Window Size Sample** - Defines the number of samples used for the high-pass filter.
- **FTC Level** - Range 0 to 1. Defines the local average that must be subtracted from the input signal to achieve the high-pass filter.
- **Use Clutter Map** - When ticked, the tracker will use the saved clutter map. See Creating and viewing clutter maps for details.
- **Clutter Map Time** - This value dictates how much of the radar data coming in contributes towards movement detection. Its unit is data per revolution of the radar (i.e. per 1 scan). For a value of 0.8, this means 20% of the data from the scan goes to form the clutter (background radar picture). Therefore 80% is analysed for movement. The higher the number, the more the data is analysed for movement, and the more sensitive it is to movement. Recommended setting is between 0.8 and 0.95.
- **Use Clutter Map as Floor** - When ticked, the tracker will use the saved clutter map as the base template of static objects (to be ignored) within sight of the radar sensor.
- **Hold Azimuth Multiplier** and **Hold Range Multiplier** - These parameters are used to prevent tracks that become stationary for a period of time from being absorbed into the clutter map. To do this the clutter map process holds open a hole in the clutter map to prevent the clutter building up where the track is.

  These two parameters define the size of the 'hole' as a factor of the reported track size. A value of 1 for both range and azimuth holds an area in range and azimuth that is the same size as the track. If they are both set to 2 then the area would be twice the size of track and so on. Using a value slightly larger than 1 allows for any variation in the reported size of track. It also allows for very small movement when the track is stationary. If both values are set to zero then track holding is disabled.
- **Use Clutter Guard** - When ticked, adds a margin of error to established clutter in order to avoid false alarms being created from real-time fluctuations in signal return.
- **Threshold** - A threshold above which samples are considered to be signals rather than noise.
- **Noise Gain** - Gain that is applied to samples that are considered to be noise. Unless otherwise instructed, this value should remain at the default value of 1.
- **Signal Gain** - Gain that is applied to samples that are considered to be signal and have exceeded the threshold. This gain in conjunction with signal offset provides the margin of error for the clutter guard process.

continued

- **Signal Offset** - Offset to be added to samples which are considered to be signal and have exceeded the threshold. This offset in conjunction with the gain provides the margin of error for the clutter guard process. To use offset in isolation ensure signal gain is set to 1.0
- **Signal Spread** - Number of samples to spread the gain/offset by in the range dimension where a signal is detected. This spreads the configured margin of error around detected areas of clutter.
- **Use (Azimuth) Blanking** - Azimuth blanking removes all raw radar data from the processing chain behind large returns close to the radar, to avoid unnecessary false alarms.
- **Threshold (Azimuth)** - A threshold above which signal returns are considered to belong to a large target.
- **Maximum Bin** - The maximum range in bins that the process will look for large signal returns.
- **Bin Tolerance** - The number of bins behind a large signal return where blanking should start
- **Show Blanking** - If enabled then the raw data display in Sentinel will show removed blanking data.

Tracker Settings (Channels tab)

- **Min Amplitude** - Determines the minimum amplitude of a plot to be considered for extraction.
- **Min Plot Range** - Determines the minimum size in range of a plot to be considered for extraction.
- **Min Range Span** - Determines the minimum number of consecutive range samples that must be in a plot before it is considered for extraction.
- **Min Blob Weight** - Determines the minimum number of cells (where a cell is a single power reading in either range or azimuth) that must be in a plot before it is considered for extraction.
- **Min Blob Plot Az Degs** - Determines the minimum size of a plot in azimuth degrees before it is considered for extraction.
- **Min Blob Plot Az M** - Determines the minimum size of a plot in azimuth metres before it is considered for extraction.
- **Min Blob Plot Range** - Determines the minimum size of a plot in range (metres) before it is considered for extraction.
- **Centroid Mode** - The mechanism by which the tracker identifies the central point of a target. There are 3 options:

  Weighted (the default setting) - Report the weighted centre of the plot assuming all samples are equal.

  Intensity - Report the intensity-based centroid, giving additional emphasis to samples with higher signal levels. When using this option, incoming samples must have intensity preserved by the earlier process. Specifically, the Thresholding process should not be configured to set all samples to 255.

  Leading Edge - Report the leading edge of the plot in range dimension and weighted centre in azimuth).
- **Merge Plots** - Once plots are extracted (using the 'minimum' settings mentioned above) – this option determines whether plots that are in close proximity to each other should be merged into larger plots using the method selected in the *Mode* setting. For example: A large articulated truck might return several plots (cab, trailer, etc) but the operator needs to see this as a single object – i.e. one truck. To achieve this, plots need to be intelligently merged together without combining smaller individual vehicles.

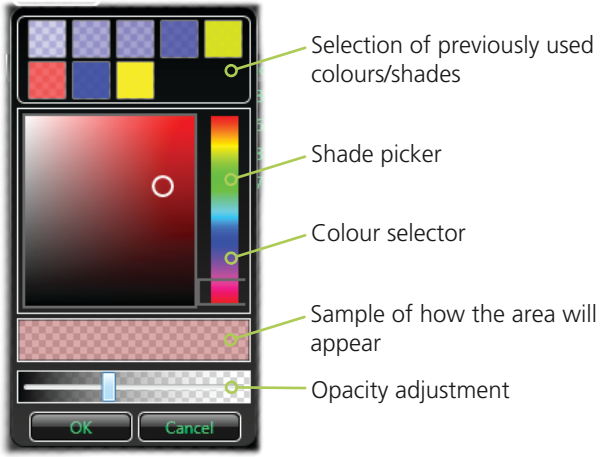
Objects > Radars & Trackers (continued)

- **Mode** - Type of merging:
  - *Azimuth* – Merges in azimuth and produces an 'eyebrow' affect as plots are merged. This option provides good performance for highway monitoring due to the fixed movement of vehicles in straight lines past the radar.
  - *Distance* – Merges in range distance (a line running to and from radar).
  - *Shape Distance* – Merges in azimuth and range. Attempts to draw a containing boundary around relevant plots. This is a good general purpose option and works well for most situations.
- **Merge Range** - How far to look for the next plot to merge in range. Merging 'hops' from plot to plot – so these figures only need to look for closest adjacent plot.
- **Merge Azimuth** - How far to look for the next plot to merge in azimuth.
- **Min Merge Az Degs** - Determines the minimum size (in azimuth degrees) for a combined plot that has been created from other individual plots and merged together.
- **Min Merged Azimuth Metres** - Determines the minimum size (in azimuth metres) for a combined plot that has been created from other individual plots and merged together.
- **Min Merge Range** - Determines the minimum size (in range metres) for a combined plot that has been created from other individual plots and merged together.
- **Initial Delay** - A timeout period after start up, during which Witness will not generate any tracks to allow a grace period whilst the tracker establishes the background clutter, etc.
- **Load Control** - Enables/disables the below setting.
- **Show Radar Plot Count** - When ticked, this option shows the current number of plots being processed within the object label for each radar (object labels appear top left of the site map when certain items are selected).
- **Tracking Areas** - This area is where you associate each area that will be monitored by the radar sensor with a set of Tracking Parameters. See Manually linking areas and tracking parameters within trackers.

Objects > Areas

This panel works in conjunction with the graphical editing of area shapes within the main site map.

- **ID** - A unique area ID number which is automatically applied.
- **Name** - Enter a distinctive name for the area. This name will be displayed on the graphical representation within the site map.
- **Colour** - When creating or editing an area, you can optionally adjust the colour shading of the area that will be shown on the graphical representation. This is useful when there are numerous areas as it helps you (and the operator) to distinguish them.

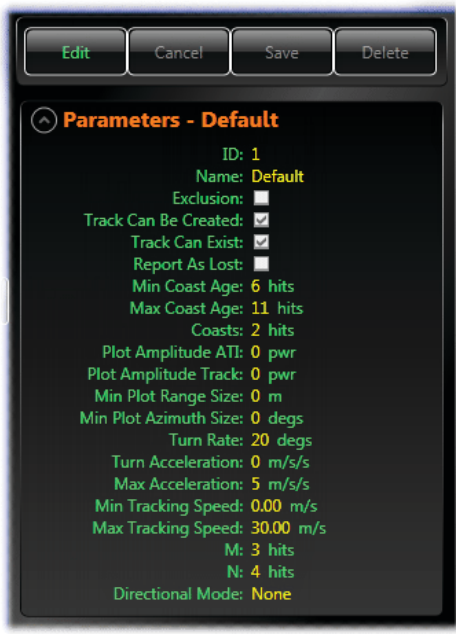


- Click the **Colour** button to the right of the name field to display the colour dialog.
- Use the controls to choose a colour and opacity setting and then use the shade picker to obtain the required shade.
- Click the **OK** button.

- **Area type** - Indicates the function of the selected area. Options are: *Normal*, *Camera* and *Packet Filter*. The *Area type* is set at the time that the Area is created and cannot be changed later.
  - *Normal* sets the area as a standard detection/alarm/rule area.
  - *Camera* defines the area as the field of view for a camera.
  - *Packet Filter* is used to filter the detection area of the radar. This area is actually stored in the radar and is used to restrict the data being sent to only include the packet filter area.
- **Hide** - Allows you to simplify the clutter within the site map by concealing this item while leaving it working as usual. It can still be selected within the Object list whereupon it will be temporarily revealed within the site map.
- **Hide Tracks** - When ticked, targets are not shown within the area, although they continue to be tracked within the Witness software.

Objects > Tracking Parameters

Tracking Parameters determine how the radar data that have been interpreted by the tracker are used to produce valid information about targets.



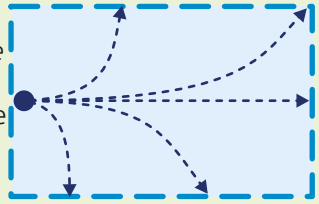
- **ID** - A unique identification number which is automatically applied.
- **Name** - Enter a distinctive name for the set of parameters.
- **Exclusion** - When ticked, targets will be ignored within the associated area. This option can be useful when debugging an installation because it allows you to quickly isolate an area. For instance, if an unexpectedly large number of targets were being created in one location served by several areas, you could quickly suspend each one to help locate an issue.
- **Track Can Be Created** - When ticked, new target tracks can be created within the designated tracking area, i.e. if a new vehicle is detected, that has not previously been seen in another area, then it will be created as a target track and shown within the site map.
- **Track Can Exist** - When ticked, target tracks created elsewhere can continue to exist within this designated tracking area.
- **Report As Lost** - When ticked, if a track disappears without leaving the detection area then the track is flagged as being lost. The Quick Report – "Lost Tracks" returns such lost tracks.
- **Min/Max Coast Age** - Defines the number of times the radar has to have seen the target before the above coasts value is applied. If Min/Max are the same value, the coasts will apply at this value. If they are different values, the coast amount will be set linearly as the target goes from Min to Max (and beyond).
- **Coasts** - Defines the number of times the radar will "predict" the position of a track that it can no longer see. If this is set to 2 then the tracker will maintain a track for two radar sensor rotations after losing it, to account for instances such as a vehicle being obscured by a gantry and then emerging within a couple of radar rotations. The result is that the operator will not know that the track was temporarily obscured.
- **Plot Amplitude Track** - Determines the minimum power amplitude of the plot before it is considered for tracking.
- **Plot Amplitude ATI** - Defines the threshold level required of a plot to be promoted to a track. This value will be set per tracking parameter, and can therefore be used to apply a different threshold per detection zone. This parameter is only activated if the *ThresholdOutput* parameter is set to *Input Level* within the tracker settings.
- **Min Plot Range Size** - Determines the minimum size of the plot (in range metres) before it is considered for tracking. This process of rejection is similar to plot extraction in the advanced tracker settings. However, this gives the opportunity to allow a plot through the plot extraction process but discard it prior to use for tracking.
- **Min Plot Azimuth Size** - Determines the minimum size of the plot (in azimuth metres) before it is considered for tracking. This process of rejection is similar to plot extraction in the advanced tracker settings. However, this gives the opportunity to allow a plot through the plot extraction process but discard it prior to use for tracking.

Objects > Tracking Parameters (continued)

- **Turn Rate** - Determines the maximum expected turn rate of any target in degrees between sightings.
- **Turn Acceleration** - Determines the maximum expected rate of change of speed during changes of direction.

Minimising the track gate size

In order to determine and follow tracks, the system attempts to predict where each track will next be positioned. Part of this process involves creating a track gate for each object which is large enough to encompass the next expected position. For accuracy it is important to keep the track gate as small as possible while still keeping the track within its borders. The *Turn Rate* and *Turn Acceleration* options help to define the size of the track gates.



- **Max Acceleration** - Determines the maximum expected acceleration of any target at any point. Anything outside this parameter will not be tracked.
- **Min/Max Tracking Speed** - Determines the minimum and maximum expected speeds of targets during tracking. Anything outside these parameters will not be tracked.
- **M** and **N** - These two values define the number of times a target must be seen within a given number of sensor rotations before it is considered to be a track. *M* represents the number of times an object is seen while *N* represents the number of scans (sensor rotations). The default values of M=3 and N=4 mean that an object must have been seen at least 3 times in 5 scans. If so, then the tracker creates it as a proper target track and shows it within Sentinel. If not, then the object remains provisional and is not sent to Sentinel. The lower this ratio, the more false alarms will be caused. Thus a ratio of 2/5 will create more false alarms than say 4/5. The maximum values for each are 30, however, the larger the numbers, the longer it will take for new targets to appear.

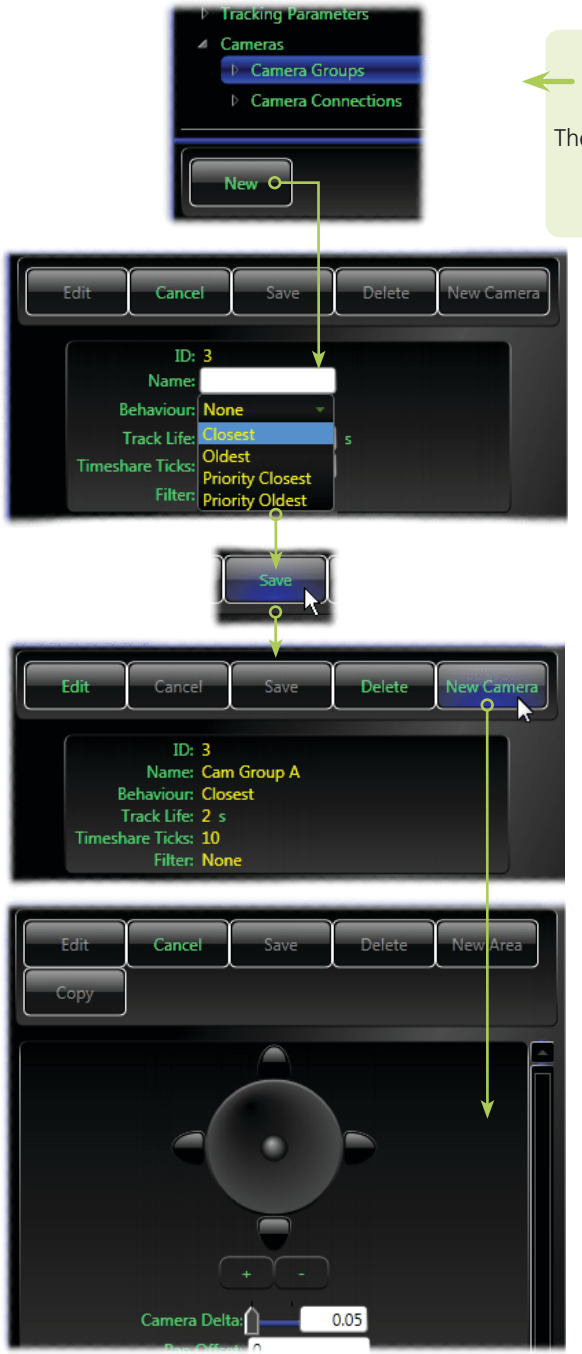
Advanced Settings

- **Directional Mode** - Determines whether tracks should be detected travelling both ways along a monitored area, such as a road. Generally, this is set to Unidirectional (with separate tracking parameters for the opposite side of the road) as it helps to increase the efficiency of detection.
- **Direction** - Determines the overall angle of the monitored road, measured clockwise relative to North. (Displayed only when *Directional Mode* setting is *Unidirectional* or *Bidirectional*).
- **Direction Error** - Establishes the tolerance of deviation from the stated angle of the monitored road within the *Direction* field. This tolerance is applied + and - to the direction value. (Displayed only when *Directional Mode* setting is *Unidirectional* or *Bidirectional*).
- **Max Tracking Speed Reverse** - Defines the maximum expected speed that a target is expected to travel in the opposite direction from the norm (Displayed only when *Directional Mode* setting is *Unidirectional*).

Objects > Cameras

This section deals with all aspects of camera communication, control and behaviour.

Creating a new camera group (and camera)



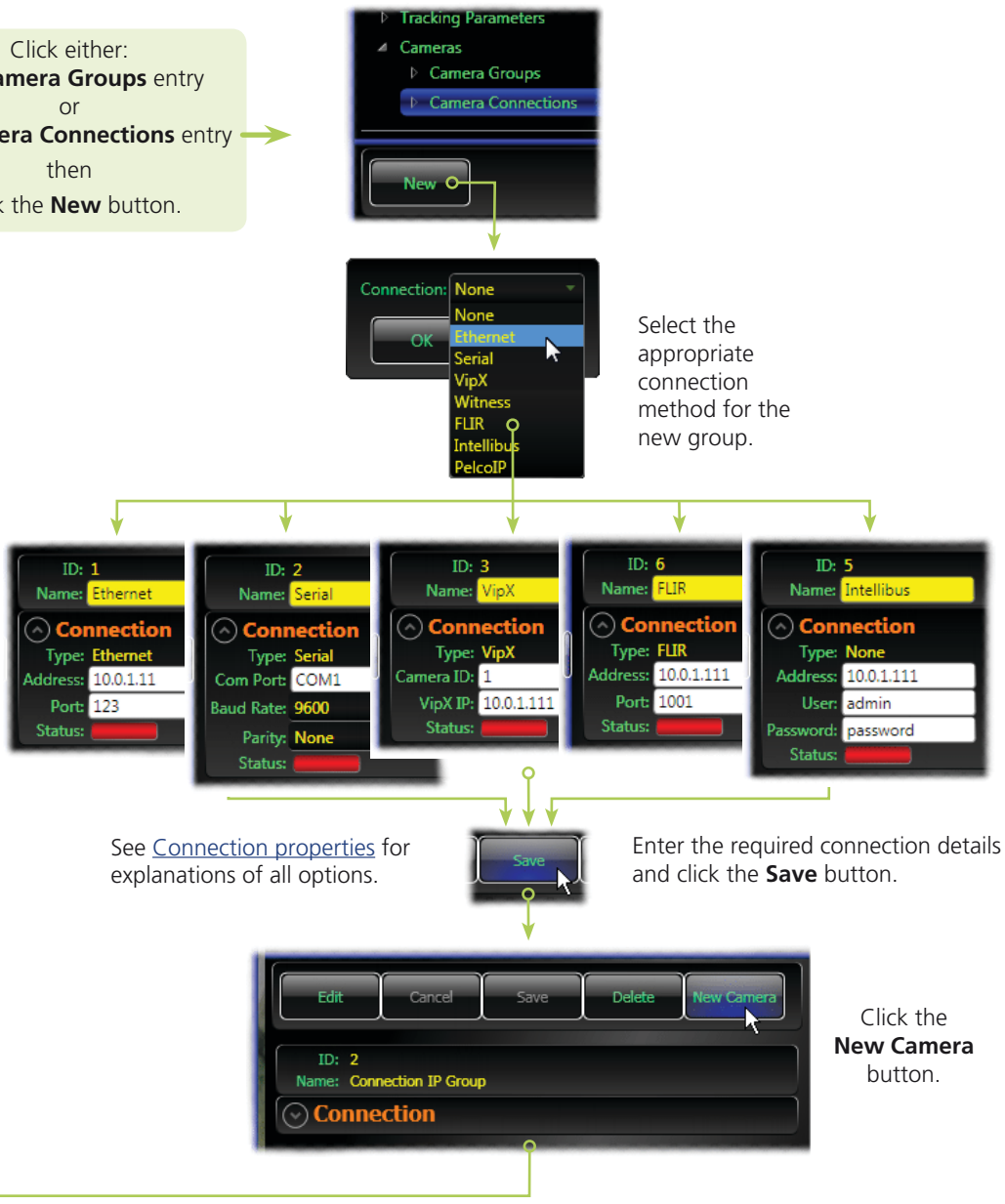
Define the new camera group name and behaviour. See New camera group dialog for details.

Click the **New Camera** button.

Create a new camera within the group. See Camera properties for explanations of all options.

Click either:
The **Camera Groups** entry
or
The **Camera Connections** entry
then
Click the **New** button.

Creating a new camera connection (and camera)



Select the appropriate connection method for the new group.

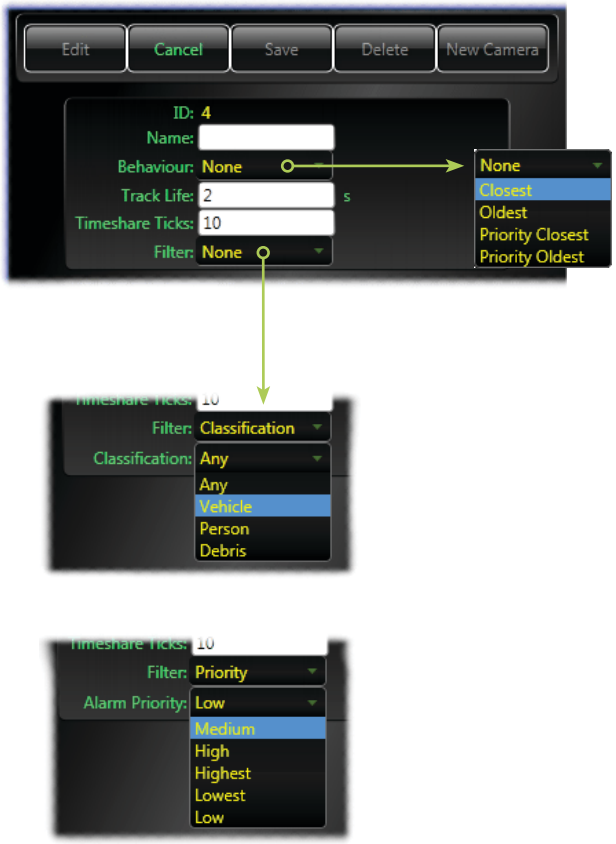
See Connection properties for explanations of all options.

Enter the required connection details and click the **Save** button.

Click the **New Camera** button.

New camera group dialog

When creating a new Camera group, the following dialog is shown to allow you to configure the basic behaviour of the group:



- **ID** number is automatically set by Sentinel.
- **Name** - This field is useful for identification purposes in a multi-camera installation.
- **Behaviour** - Determines how cameras belonging to this group should respond to multiple tracks within their vicinity:

  Closest: Tracks are chosen according to their proximity to the camera position.

  Oldest: Tracks are chosen according to those that were least recently viewed.

  Priority Closest: Tracks are chosen according to the highest priority classification (i.e. warning, threat...) that are in the closest proximity to the camera.

  Priority Oldest: Tracks are chosen according to the highest priority classification (i.e. friend, warning, threat...) that were least recently viewed.
- **Track Life** - Defines the time that a track should remain buffered within the Cyclops camera control application. If a message is not received from Piccadilly (stating either an updated position for the track or the end of the track) within the time period stated here, then Cyclops will flush the track details from its buffer. This value does not usually need to be altered.
- **Timeshare Ticks** - Determines the time period that each track should be viewed by a given camera before moving to the next track (as determined by the *Behaviour* setting). Each tick represents roughly one second.
- **Filter** - The optional filter setting allows you to further prioritise the tracks that the camera should follow. In addition to *None*, the *Filter* option provides two choices, each of which cause a related drop down list to be displayed:

  Classification: Allows you to restrict camera following to tracks of a particular classification, e.g. Vehicle, Person, Debris, etc.

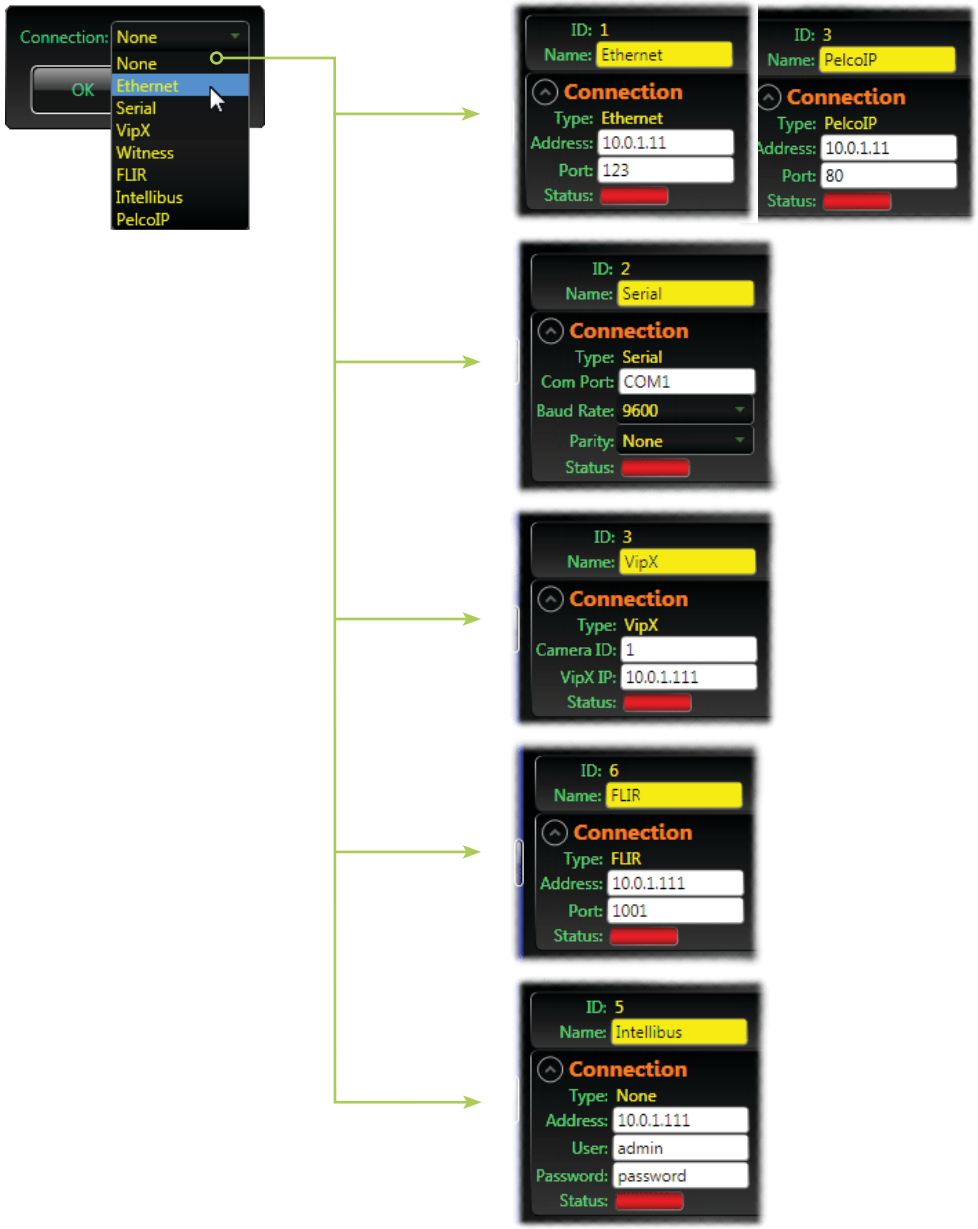
  Alarm Priority: Allows you to restrict camera following to tracks only of a particular alarm severity. The available *Alarm Priority* options (e.g. *Low, Lowest, Medium, High* or *Highest*) relate to the Alarm Priority setting that is available within the rules* that cause camera responses. Within the rules, the Alarm Priority setting provides a weighting system whereby their respective severities can be determined. Within the camera group, the Alarm Priority setting allows you to choose a **minimum** priority to which the camera should respond. Thus, when a camera group has an Alarm Priority setting of *Medium*, the camera(s) within that group will only respond to broken rules that have an Alarm Priority of *Medium*, *High* or *Highest*.

* For the Alarm Priority setting to be available within a rule, that rule must have an action (e.g. *Follow*, *Alarm*, *Alarm and Follow*) selected within it.

Objects > Cameras (continued)

Camera connection properties

When creating a new Camera Connections group, click the required connection type to view the relevant settings:



Ethernet/Pelco IP connection

- **Address** - Defines the IP address of the camera.
- **Port** - Defines the port number used by the camera.

Serial connection

- **Com Port** - Defines the COM port used on the computer running the Cyclops service that is used to control the camera.
- **Baud Rate** - Defines the communication speed of the serial connection to the camera.
- **Parity** - Defines the parity checking method used within the serial connection to the camera.

VipX connection

- **Camera ID** - Defines the video channel for the camera within the VipX encoder.
- **VipX IP** - Defines the IP address used by the VipX connection.

FLIR connection

- **Address** - Defines the IP address of the camera.
- **Port** - Defines the port number used by the camera.

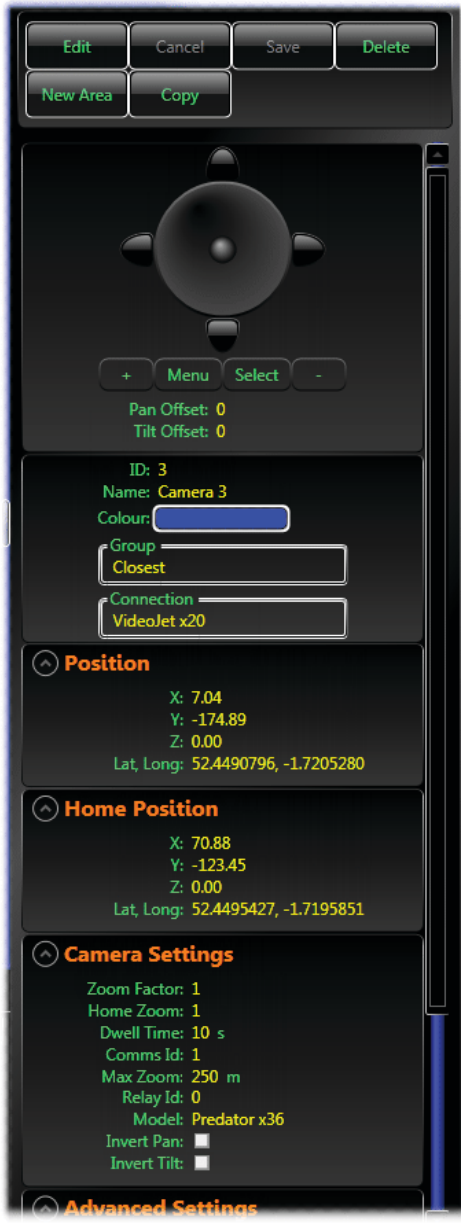
Intellibus connection

- **Address** - Defines the IP address used by the camera.
- **User** - Defines the username required by the camera.
- **Password**- Defines the password required by the camera.

Objects > Cameras (continued)

Camera properties

Click the **New Camera** button from within a *Camera Group* or *Connection Group* (see the previous page), or highlight an existing camera and click the **Edit** button.



- **Pan and tilt controls** - In operation, these allow you to manually control the camera. The outer horizontal buttons control the pan x-axis and the upper/lower buttons control the tilt y-axis. The middle button can be clicked and dragged to move the camera in any direction.
- **+/-** In operation, these buttons zoom in and out.
- **Menu/Select** - Available only in admin mode and only then if the selected camera supports their use. These control access to, and navigation within, the internal menu of the camera. When menu mode is invoked, you can then use the joystick controls and Select button to control the camera menu, as you would with a standard camera controller.
- **ID** number is automatically set by Sentinel.
- **Name** - This field is useful for identification purposes in a multi-camera installation.
- **Colour button** - Allows you to apply a colour to the camera representation within the site map - useful when multiple cameras are installed
- **Group** - If the required camera group is not already shown here, click this box to choose one. If no camera group is set, the camera will be made a member of the 'Default Camera Group' but will need to be added to a valid camera group before operation can commence.
- **Connection** - If the required connection group is not already shown here, click this box to choose one. If no camera connection is set, the camera will be made a member of the default 'No Connection' group but will need to be added to a valid connection group before operation can commence.

Position

- **X**, **Y**, **Z** - Defines the position (X, Y) of the camera from the origin point in metres. The Z axis defines the height of the camera above ground level in metres.
- **Latitude**, **Longitude** - States the absolute coordinates of the camera.

  Note: The camera position can be adjusted using either the X,Y,Z or Lat/Long values.

Home Position

The home position is the pan and tilt orientation to which the camera will return when it is issued with a home command. It is the camera's 'zero point'. Following installation, the exact orientation of the camera will probably be unknown and will almost certainly not be aligned with what Sentinel considers to be the home position. The **X** and **Y** fields here allow you to compensate for any differences between the camera and the Sentinel home positions. The **Z** field is not used.

Latitude and **Longitude** state the absolute coordinates of the camera home position. These figures are derived from the origin point and the X and Y values.

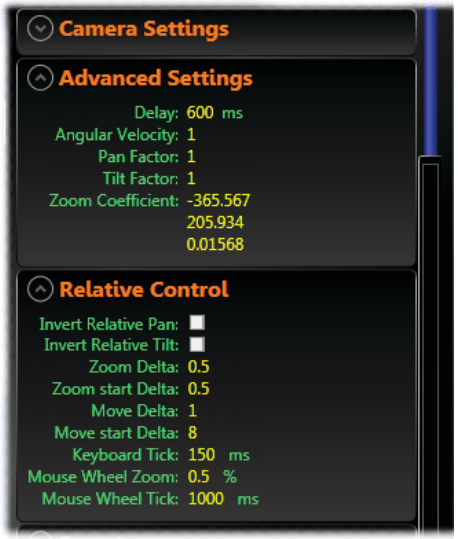
See Adjusting a camera home position for details.

continued

Objects > Cameras (continued)

Camera Settings

- **Zoom factor** - Defines the ratio used to determine how the zoom commands requested by the application are translated into zoom movement by the camera. The range usually lies between 0.01 to 1, although values up to 2 can be used in certain circumstances. The default setting is 1.
- **Home Zoom** - Defines the zoom level to which the camera should return when a home command is received. The default setting is 1.
- **Dwell Time** - Defines a time period for which the camera should remain on a view before moving to the next position. The default setting is 10 seconds.
- **Comms Id** - A unique identification number that allies the camera control section of the Witness group with the camera.
- **Max Zoom** - Defines the maximum zoom distance (in metres) that the camera should be taken to when tracking distant objects. When tracking moving targets at long zoom levels it is possible to miss the target altogether. By reducing the zoom level, a larger field of view provides greater opportunity to keep the target within the frame.
- **Relay Id** - Defines the ID of the relay that should be activated whenever the camera is activated (most often used to prompt a DVR to begin recording the video feed). Choose '0' to disable.
- **Model** - Choose the appropriate camera model from a drop down list. The choice of model will determine numerous operational aspects including the appropriate Zoom Coefficient values for the camera.
- **Invert Pan** - When ticked, all pan controls for the camera will be reversed. Used for cameras that are mounted in an inverted position.
- **Invert Tilt** - When ticked, all tilt controls for the camera will be reversed. Used for cameras that are mounted in an inverted position.



Advanced Settings

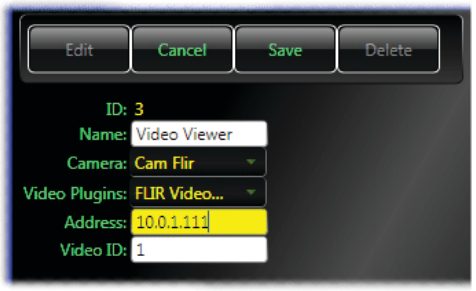
- **Delay** - Allows you to define a delay to the movement commands in order to allow the positioning mechanisms of the camera to respond. The default setting is 600 milliseconds.
- **Angular Velocity** - When set to 1, the speed that the camera moves is based on a prediction of where the target will be next seen with a small 'look ahead' adjustment to take into account the time for the message to get the camera and the camera to move. In situations where fast moving objects are close to the camera, the angular velocity of these targets increases significantly. To compensate, this value will adjust the speed of movement and the amount of 'look ahead' to take account of targets with high angular velocity.
- **Pan/Tilt Factor** - These values can be used to adjust the calculated pan and tilt movements by a fixed factor (i.e. 0.5 would move the camera through half of the pan or tilt angle that has been automatically calculated, 2 would move it through twice the angle, and so on). This setting is only used in special circumstances where different cameras with the same protocol use different pan and tilt resolutions.
- **Zoom Coefficient** - These three values are derived from the model number of the camera and define the manner in which the zoom reacts to changing distance. These values are generally not altered.

Relative Control

- **Invert Relative Pan/Tilt** - For relative movement (when using joystick) they reverse direction.
- **Zoom Delta** - Determines the percentage rate at which the camera zoom will increase in speed when the operator holds down either the mouse button on the screen joystick or a keyboard control. This increase will be applied once per mouse or keyboard tick.
- **Zoom start Delta** - Sets the initial zoom speed.
- **Move Delta** - Determines the percentage rate at which the camera pan and tilt movements will increase in speed when the operator holds down either the mouse button on the screen joystick or a keyboard control. This increase will be applied once per mouse or keyboard tick.
- **Move start Delta** - Sets the initial movement speed.
- **Keyboard Tick** - Determines the period (in milliseconds) between each 'tick' of the keyboard - used to determine how long a key has been held.
- **Mouse Wheel Zoom** - Determines the increase in camera zoom for every step movement of the mouse wheel.
- **Mouse Tick** - Determines the period (in milliseconds) between each 'tick' of the mouse button(s) - used to determine how long a button has been held.

Objects > Video Viewers

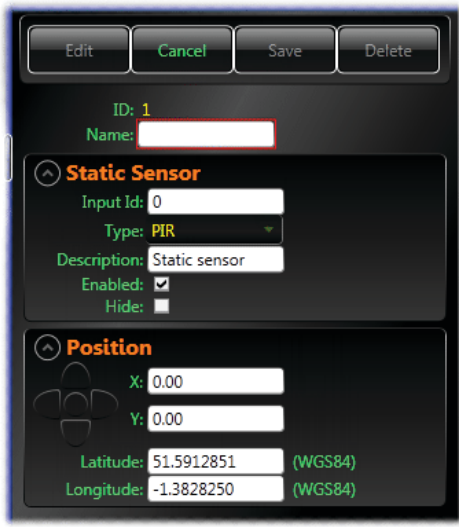
This section deals with adding a camera viewer. This is essentially a connection to a digital video stream, be it a media encoder or IP camera feed.



- **ID** - A unique identification number which is automatically applied.
- **Name** - Enter a distinctive name for the viewer. This will be used as the viewer shortcut label when clicking within the main sentinel window.
- **Camera** - Click this box to choose the camera connection top which this video viewer relates.
- **Video Plugins** - Select the plugin applicable to the camera.
- **Address** - The IP address of the camera (if IP), or the address of the media server being used to convert analog video.
- **Video ID** - The ID of the video stream at the above IP address. For example, a dual encoder may have standard video on ID 1 and thermal video on ID 2.

Objects > Static Sensors

This panel allows you to determine the settings for each static sensor (e.g PIR sensors, light beams) within the AdvanceGuard installation.



ID

The **ID** number is automatically set by Sentinel.

Name

The text entered here will be used to label the sensor within the graphical representation within the site map.

Static Sensor

- **Input Id** - Enter the identification of the hardware interface digital input to which the static sensor is connected. This Id number will uniquely link the sensor input with the configuration details stored for it.
- **Type** - Choose the appropriate sensor type from the list, e.g. Broken Beam (sensors which are triggered when their invisible light beams are interrupted) or PIR (Passive InfraRed sensors which are triggered when they detect changes in radiated heat).
- **Description** - This text field allows you to optionally add more detail about the sensor. This is particularly useful for location and differentiation purposes in large multi-sensor installations.
- **Enabled** - Enables/disables the sensor.
- **Hide** - Allows you to simplify the clutter within the site map by concealing this item while leaving it working as usual. It can still be selected within the Object list whereupon it will be temporarily revealed within the site map.

Position

- **X, Y (plus Latitude and Longitude)** - Each new static sensor is initially assigned the default Latitude and Longitude of the installation origin. You can then either enter new Lat and Long values or alternatively adjust the **X** and **Y** settings to define the offset position (in metres) of the sensor from the origin point. You can adjust the **X** and **Y** settings either by typing the offsets into the fields or you can drag the sensor icon to the required position on the graphical representation.

  The Lat. and Long. values for the sensor position are calculated using the known origin point plus the X and Y offsets.

Appendix 2 - Configuration options

The Sentinel application is highly configurable to ensure that it can be customised to fit a wide variety of installations. Many of the key settings are located within the Configuration section.

To view/edit configuration options

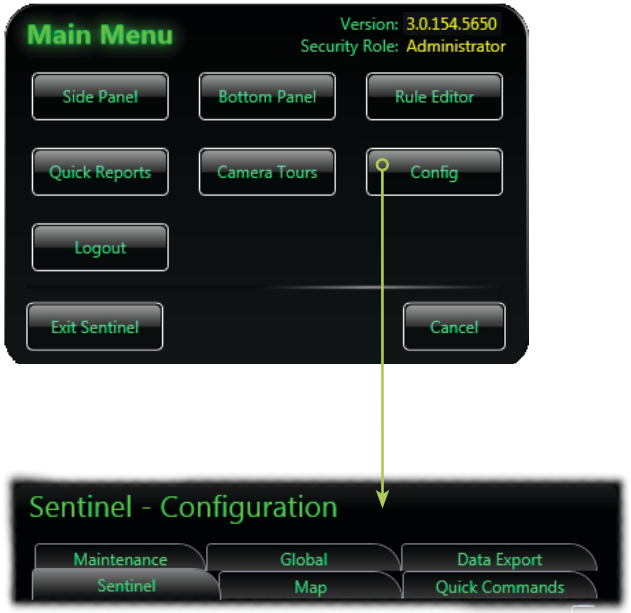
Note: You must be in admin mode to access this section - see Entering admin mode.

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Config** button.

3 Click a tab to access any of the five sections:

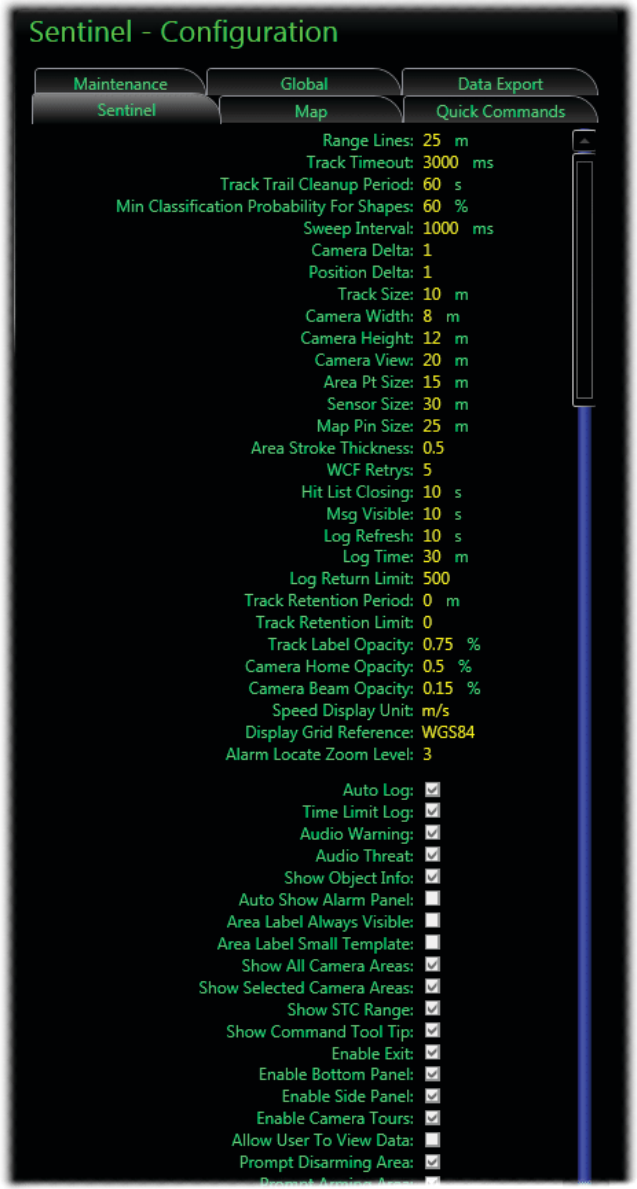
- Configuration > Sentinel (General)
- Configuration > Map
- Configuration > Quick Commands
- Configuration > Maintenance
- Configuration > Global)
- Configuration > Data Export



continued

Configuration > Sentinel (General)

Contains a range of options, many of which are concerned with how the Sentinel application displays and logs information:



Click the Edit button to alter settings.

- **Range Lines** - Specifies the distance required between the superimposed radar range lines on the scan display (in metres). The default setting is 25 metres.
- **Track Timeout** - Defines the time period after which, if a target track has failed to be seen, it will be deleted. The default setting is 2500 milliseconds.
- **Track Trail Cleanup Period** - The time period to leave track trails before they start fading out and eventually disappear. Each trail slowly rolls up behind the track – and therefore remains even after the track itself has disappeared.
- **Min Classification Probability for Shapes** - Determines the percentage confidence level required before a classification icon (e.g. person, vehicle, etc.) can be applied to a tracked object.
- **Sweep Interval** - Defines how often tracks are checked to ensure they are still active. Tracks are checked using the 'Track Timeout' parameter and if they have expired, they are removed.
- **Camera Delta** - Defines the size of movement of the camera when performing fine adjustments (otherwise known as *bias adjustment*). The default setting is 1.
- **Position Delta** - The distance an object will move when clicking on the direction buttons next to the position field being edited – default is 1 metre.
- **Track Size** - Defines how large the track should appear within the site map. The default setting is 10 metres.
- **Camera Width** - Defines the width of cameras within the site map. The default setting is 8 metres.
- **Camera Height** - Defines the height of cameras within the site map. The default setting is 10 metres.
- **Camera View** - Defines the size of the camera view circle as shown within the site map. The default setting is 20 metres.
- **Area Pt Size** - Defines the size of the points (circular and squares) used to drag vertices around and/or create new vertices within areas. The default setting is 10 points.
- **Sensor Size** - Size to display static sensors within the Sentinel display (radius of static sensor ring).
- **Map Pin Size** - Determines the size of the two map pins that are used to orientate the background map.
- **Area Stroke Thickness** - Determines the thickness of the line used to mark the boundaries of areas. The default setting is 0.5.
- **WCF Retrys** - Defines the number of attempts that Sentinel will make to reconnect with the Piccadilly data server in the event of a disconnection. The default setting is 3.
- **Hit List Closing** - Defines the time period that the object selection list should remain displayed (the object selection list appears in the top right of site map whenever you click on a point which contains a number of overlapping objects). The default setting is 10 seconds.
- **Msg Visible** - Determines the time period that new messages are displayed. The default setting is 10 seconds.
- **Log Refresh** - Determines the interval between updates to the log. The default setting is 10 seconds.
- **Log Time** - Determines the time period that entries are held within the *Log* tab before they are cleared (when *Time Limit Log* is set to on.). The default setting is 30 minutes.
- **Log Return Limit** - The maximum amount of records displayed in the Log tab in the bottom panel.
- **Track Retention Period** - Determines the time period (in minutes) that tracks should remain displayed within the site map after the actual tracked objects have disappeared.

continued

Configuration > Sentinel (continued)

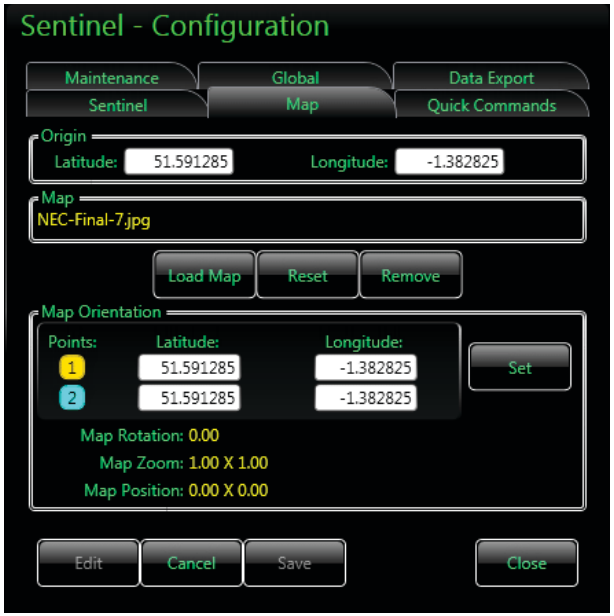
- **Track Retention Limit** - Determines the maximum number of tracks that should be permitted to remain displayed (for the period defined in the *Track Retention Period* setting) within the site map after the actual tracked objects have disappeared.
- **Track Label Opacity** - Determines the opacity of the label backgrounds that are applied to targets. A fully transparent label (setting = 0) may make it difficult to read the label text, whereas a fully opaque label (setting = 1) may block other details in zoomed out views. The default setting is 0.3
- **Camera Home Opacity** - Determines the opacity of the star icon representing the cameras home position. A setting of 0 is fully transparent, whereas a setting of 1 is fully opaque. The default setting is 0.5.
- **Camera Beam Opacity** - Determines the level of opacity for the beam used to represent the direction of the camera view. A setting of 0 is fully transparent, whereas a setting of 1 is fully opaque. The default setting is 0.15
- **Speed Display Unit** - Determines how the speed of travel of each tracked vehicle should be displayed. Options are: m/s, mph and kph.
- **Display Grid Reference** - Determines the mapping coordinate system to be used. Options include: WGS84, SWEREF90 and RT90. *Note: Changing this setting will affect Latitude and Longitude values.*
- **Alarm Locate Zoom Level** - When clicking the locate button (on alarm notification message or in bottom panel), the UI pans and zooms to centre on the location of the incident. The zoom level specifies the zoom factor.
- **Auto Log** - Determines whether Sentinel should actively query the Piccadilly communications server for log updates. The default setting is on.
- **Time Limit Log** - When ticked, Sentinel will restrict the time that entries are held within the *Log* tab before removing them, according to the time limit set within the *Log Time* property. The default setting is on. Note: Older logs can still be retrieved via the *Manual Log* tab.
- **Audio Warning** - When ticked, an audio alert will be sounded whenever a target is designated as a warning. The default setting is on.
- **Audio Threat** - When ticked, an audio alert will be sounded whenever a target is designated as a threat. The default setting is on.
- **Show Object Info** - Some objects (eg. Radar, Tracks) have extra information which displays in the top left corner. This setting determines whether this info is displayed or not.
- **Auto Show Alarm Panel** - When ticked, this option will cause the alarm panel in the bottom section of the site map to be displayed when an alarm occurs.
- **Area Label Always Visible** - Determines whether the labels for each area should be visible during normal operation or only when selected. The default setting is off.
- **Area Label Small Template** - When ticked, reduces the area label size and text to the bare minimum (showing only the area name). Useful when in conjunction with *Area Label Always Visible* property so that labels are not too obtrusive. The default setting is off.
- **Show All Camera Areas** - When ticked, will show the areas associated with all cameras, regardless of whether the camera is selected.
- **Show Selected Camera Areas** - When ticked, shows the area associated with the currently selected camera.
- **Show STC Range** - When ticked, will show the range circle for each radar using STC.
- **Show Command Tool Tip** - When ticked, short explanatory sentences will be displayed when your mouse pointer hovers over a button or option. The default setting is on.
- **Enable Exit** - Determines whether the Exit Sentinel button is available within the main menu when admin mode is off. When unticked, the button will be greyed out in non-admin mode. The default setting is on.
- **Enable Bottom Panel** - Determines whether the bottom information panel can be revealed or concealed by the operator when admin mode is off. When unticked, the status of the bottom panel will be determined by how it is arranged during admin mode. During normal operation, the operator may (if the panel is shown) resize it, but not hide it. The default setting is on.
- **Enable Side Panel** - Determines whether the side panel can be revealed or concealed when admin mode is off. When unticked, the status of the side panel will be determined by how it is arranged during admin mode. During normal operation, the operator may (if the panel is shown) resize it, but not hide it. The default setting is on.
- **Enable Camera Tours** - This setting determines whether the Camera Tours button (on the main menu) is visible to standard Users.
- **Allow User to View Data** - Determines whether standard User can use Data button. Admin and supervisor can always use the data button.
- **Prompt Disarming Area** - When ticked, the operator will be shown a popup menu offering differing time periods to disarm whenever an area is selected for disarming. When unticked, no menu will be shown and the area will remain disarmed until it is next manually re-armed. The default setting is on.
- **Prompt Arming Area** - When ticked, the operator will be shown a popup menu offering differing time periods to re-arm whenever an area is selected for arming. When unticked, no menu will be shown and the area will be armed until it is next manually disarmed. The default setting is on.
- **Prompt Disarming Sensor** - When ticked, a notification occurs when the sensor is automatically disarmed after being set by the user to "armed" for a specific interval.
- **Prompt Arming Sensor** - When ticked, a notification occurs when the sensor is automatically armed after being set by the user to "disarmed" for a specific interval.

Configuration > Sentinel (continued)

- **Show Main Menu Clock** - When ticked, a clock is shown in the top right corner of the screen.
- **Background Map Image Enabled** - When ticked, the selected background image
- **Camera Control Priority** - Cameras can be manually controlled within Sentinel. When using more than one Sentinel, this setting determines which Sentinel has priority to move the cameras.
- **Open Viewers On Startup** - Opens existing video viewers on Sentinel startup.
- **Display Open Street Map** - When ticked, Sentinel will display background images provided by the Open Street Maps service providing the appropriate settings have been made within the Configuration > Maps section.
- **Open Street Map Cache Timeout** - Determines the time period that the Open Street Map data will be used before an attempt is made to update from the OSM servers.
- **Show Radar ID on Track** - When ticked, shows the RadarId as well as the TrackId on the track in the site map (format is RadarId-TrackId).

Configuration > Map

Contains all options relating to the background image upon which all information is overlaid within the site map. For more information about using this page, see the section Adding a background image.

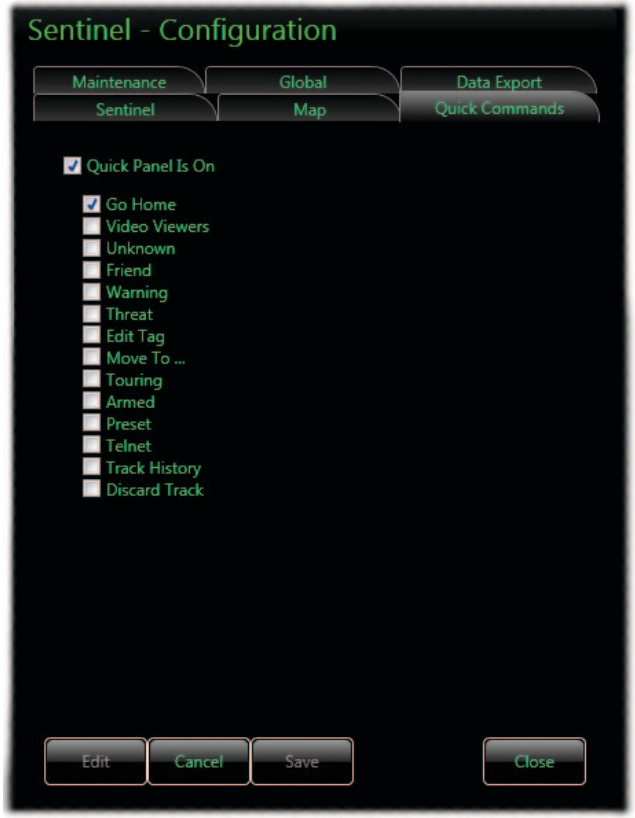


Click the Edit button to alter settings.

- **Origin Latitude and Longitude** - Indicates the lat and long coordinates for the 0,0 Origin point of the scan area. By default, the Origin point is set to the coordinates of the Navtech Radar headquarters near Wantage, Oxfordshire.
- **Map** - Indicates the filename of the background image used (if any).
- **Load Map** - Click to load a new background image.
- **Reset** - Click to return the background image back to its default position and orientation.
- **Remove** - Click to remove the current background image.
- **Map Orientation Latitude and Longitude** - Use these fields to declare valid lat and long coordinates for two points that can be identified on the background image. This allows the Sentinel application to correctly scale and orientate the image to the reality as sensed by the radar detectors.
- **Set** - Click to orientate the map once the valid lat and long coordinates have been entered.

Configuration > Quick Commands

Contains all options relating to the quick command buttons that are displayed within the site map when relevant objects are selected.

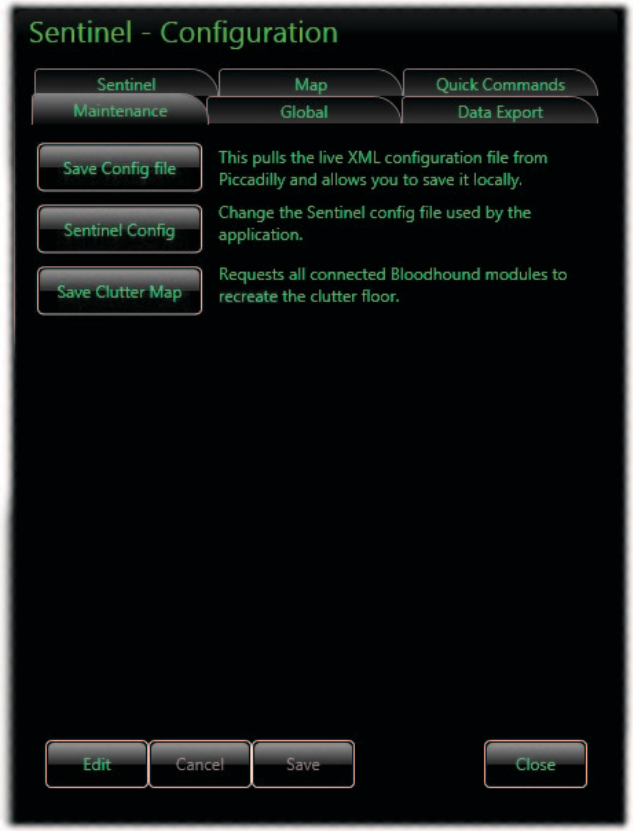


Click the Edit button to alter settings.

- **Quick Panel Is On** - Determines whether the quick panel is displayed within the site map.
- **Go Home** - When ticked, displays a button when a camera is selected. If the button is clicked, a home command is sent to the chosen camera.
- **Video Viewers** - When ticked, displays a button when a camera is selected. If the button is clicked, all associated video viewers for the camera will be enabled.
- **Unknown** - When ticked, displays a button when a target is selected. If the button is clicked, the target will be marked as *Unknown*.
- **Friend** - When ticked, displays a button when a target is selected. If the button is clicked, the target will be marked as *Friend*.
- **Warning** - When ticked, displays a button when a target is selected. If the button is clicked, the target will be marked as *Warning*.
- **Threat** - When ticked, displays a button when a target is selected. If the button is clicked, the target will be marked as *Threat*.
- **Edit Tag** - When ticked, displays a button when a target is selected. If the button is clicked, the tag associated with the target can be edited within the site map.
- **Move To...** - When ticked, displays a button when a camera is selected. If the button is clicked, the camera will move to view the position where the mouse is next clicked.
- **Touring** - When ticked, displays a *Touring* button when a camera is selected. If the button is clicked, the camera will step through a camera tour that has been pre-programmed. If no tour is available for the selected camera, the button will be greyed out.
- **Armed** - When ticked, displays a button when an area is selected that allows the area to be armed/disarmed.
- **Preset** - When ticked, displays a button which, when clicked moves the nearest camera to the preset location of the selected area.
- **Telnet** - When ticked, displays a button when a radar is selected. The button opens a Telnet window and attempts to connect to the selected radar.
- **Track History** - When ticked, displays a button when a retained track is selected in the site map. The button displays the track history for the selected track.
- **Discard Track** - When ticked, displays a button when a retained track is selected in the site map. The button discards the selected track.

Configuration > Maintenance

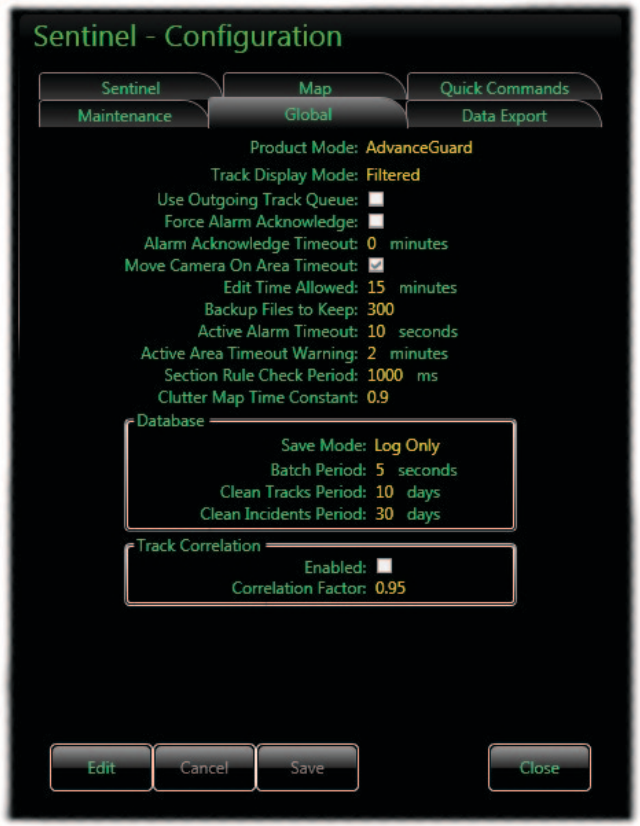
This tab contains various configuration maintenance options.



- **Save Config file** - Allows you to export a copy of the current configuration file for backup purposes or to share common configurations between multiple installations. The file may also be sent to Navtech for troubleshooting purposes.
- **Sentinel Config** – Allows you to reset or copy an existing Sentinel configuration. Selecting *New* will reset the Sentinel config to default values. Other configured Sentinel installations will be listed and can be selected to duplicate these settings.
- **Save Clutter Map** - Requests all connected Bloodhound modules to recreate the clutter floor. The clutter floor capture process may take several minutes. During this period, configuration changes are disabled. Sentinel will display a message once the process is complete.

Configuration > Global

This tab includes various key settings that affect overall behaviour of the system.



Click the Edit button to alter settings.

- **Product Mode** - Determines which mode of operation the system should adopt: ClearWay (for highway use) or Advance Guard (for security installations).
- **Track Display Mode** - When set to *Filtered* this function uses an algorithm within Piccadilly to determine which tracks get sent to all copies of Sentinel. In certain situations, operators do not need to see tracks that present no cause for concern. For example, in highway monitoring, most tracks can be ignored because the main task is to locate vehicles that are travelling too slowly or have stopped. The *Show All* setting sends all data to all copies of Sentinel without filtering.
- **Use Outgoing Track Queue** - When enabled, outgoing tracks from Piccadilly are buffered in a queue in order to allow new tracks to be accepted. This option is suitable for use within installations where there are likely to be large numbers of tracks occurring in quick succession. The use of the queue does introduce a latency overhead and so is not suitable for all installations.
- **Force Alarm Acknowledge** - When ticked, a pulsating alarm symbol will be displayed in the top centre of the screen. The operator must click on the symbol to display a dialog where all current alarms are listed and can be acknowledged.
- **Alarm Acknowledge Timeout** - When the *Force Alarm Acknowledge* option is enabled, this setting allows you to optionally determine a time period after which the system will begin to auto acknowledge them. This prevents too many alarm acknowledgement requests building up if the operator does not keep up with them.
- **Move Camera On Area Timeout** - Areas can be set to arm and disarm on timeouts. This option enables the closest camera to move to an area that has reached its timeout warning period.
- **Edit Time Allowed** - Determines how long an admin user can keep a particular section of the system in edit mode (which automatically locks out any other user from that section), after which edit mode will be automatically ended (Time refreshes automatically based upon user input).
- **Backup Files to Keep** - Determines the number of backup configuration files to keep (within the Backup folder of the main application folder). A backup is made after every configuration change.
- **Active Alarm Timeout** - Indicates how long an alarm should be held open for after it has been triggered. Any re-triggering of this alarm during the timeout period ensures this timeout is reset. So the alarm will only clear if no further alarms occur for the duration of this timeout.
- **Active Area Timeout Warning** - Warning timeout for an area disarm / arm event. Typically this occurs a set period of time before the actual timeout and can be used to trigger a camera to look at the area. A warning message is also sent to operator via Sentinel.
- **Section Rule Check Period** - Determines the frequency (in milliseconds) at which all 'section-type' rules are checked to see if any tracks in the selected sections have broken the rule. Tracks are checked as they arrive but the rule is only considered broken if one or more tracks meets the rule criteria during this check period. In addition the break allowance is only incremented and decremented when this periodic check is performed. Usually this period is set to the rotation speed of the radar (i.e 1Hz = 1000 ms).
- **Clutter Map Time Constant** - The percentage of the historical clutter map that is retained on every scan.

continued

Configuration > Global (continued)

Database

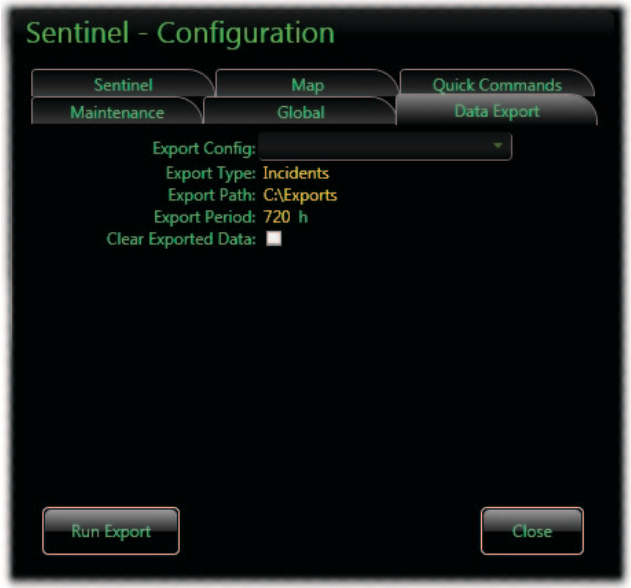
- **Save Mode** - Determines which details are saved in the database. Options are: None, Log Only (retains only the log description of each incident), Incident Only (retains track details from each alarm plus limited track movements from before and after the incident) or Save All (retains log entries and track details for all movement).
- **Batch Period** - If using batch updates, this option determines how often to process database update batches.
- **Clean Tracks Period** - Determines the time period for which track records are removed from the database (only items older than the stated period are removed).
- **Clean Incidents Period** - Determines the time period for which items from the main log are removed (only items older than the stated period are removed).

Track Correlation

- **Enabled** - Determines whether the Correlation Factor feature is applied. See below.
- **Correlation Factor** - When there is overlapping radar coverage with correlation enabled, tracks are effectively analysed to establish whether it's the same target being reported by one or more radars. If the probability of multiple tracks being the same target is greater than the correlation factor, then the track correlation process will remove duplicates. This process ensures track Ids are maintained when targets move from one radar's coverage to an adjacent one.

Configuration > Data Export

This tab enables you to quickly carry out a full export of data sets from the past 30 days. You can choose the type of data set and also choose whether to remove the exported data from the internal database.



- **Export Config** - Choose which data set to export: *Incidents, Statistics* or *Tracks*. All are for the last 30 days and the internal database will not be cleared unless you tick the *Clear Exported Data* checkbox below.
- **Export Type** - Confirms the chosen export set.
- **Export Path** - Displays the target folder for all quick exports.
- **Export Period** - Confirms the chosen export period: 720 hours = 30 days.
- **Clear Exported Data** - When ticked, the exported data will be cleared from the internal database.

To perform a data export

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.
2 Click the **Config** button.
3 Choose the **Data Export** tab.
4 Use the **Export Config** dropdown to choose the required data set.
5 Click the **Run Export** button. A .csv file will be created within the *C:Exports* folder.

Appendix 3 - Rule properties

Rules allow AdvanceGuard to carry out automated monitoring of any or all parts of the area under surveillance. Rules are constructed from simple options and arguments to collectively form a comprehensive and intelligent control system.

To edit/create rules

Note: You must be in admin mode to make changes - see Entering admin mode.

1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Rule Editor** button.

3 Either:

- Edit an existing rule: Click on a rule entry in the upper section and then click the **Edit** button.
- Define a new rule: Click the **New** button, select the appropriate *Rule Type* and then click the **OK** button.

Rule property explanations

Many properties are common across the various different types of rules, whereas others alter depending upon the type of rule chosen. The properties are listed here in alphabetical order:

- **Action** - Defines the action that should be taken when a rule is broken. There are four options: *None* (used primarily for rules that will be used to form a compound rule); *Alarm* (display a message and sound an audio alert); *Follow* (instruct the nearest camera to follow the target); *Alarm and Follow* (display a message, sound an audio alert and instruct the nearest camera to follow the target).
- **Alarm Description** - Determines the text that will be presented to the operator (and entered in the activity log) when the rule is broken and an alarm is raised.
- **Alarm Priority** - Allows you to optionally apply a 'weighting' to any rules that invoke an *Action*. There are five priority levels: *Lowest, Low, Medium, High* and *Highest*. A similar setting is available within the Camera Group section so that individual cameras can be instructed to only follow tracks that have broken rules with a particular priority (or above).
- **Allowance Decrement** - (used only when *Use Allowance Curve* is enabled) Defines the amount by which the break count should be decremented every time a target ceases to break the rule.
- **Allowance Increment** - (used only when *Use Allowance Curve* is enabled) Defines the amount by which the break count should be incremented every time a target breaks the rule.
- **Allowance Reset** - Defines the number of seconds after which time the *Break Allowance* count should be reset. A reset will only occur if the target has ceased breaking the rule. This option is useful to prevent false alarms and yet keep the alarm trigger ready in situations where a target has broken a rule but has not yet exceeded the Break Allowance. If that target then begins to break the rule again before the reset time has elapsed, the alarm will be raised more quickly because the count is closer to the Break Allowance trigger value. The default value of 0 will reset the Break Allowance as soon a target ceases to break the rule.
- **All radars** - Allows you to optionally define particular radar sensors for use with the current rule. This allows you to exclude radar sensors that may be in range but which cause unwanted effects when used with a particular rule. When unticked, the *Sender Radars* sections will be displayed so that you can specifically include/exclude radar sensors in relation to the current rule.
- **Angle +/-** - (Tail Gate only) Defines the arc ahead (either side of the centre line) of each vehicle where the rule should look for other vehicles that might be considered to be too close.
- **Areas** - (Area movement only) Allows you to select the area(s) that will be monitored by the rule. Place a tick against all areas that you wish to associate with the current rule. See also *Description* regarding the naming of area movement rules.
- **Audible Alarm** - Determines whether an audible alert is sounded for the operator when the rule is broken or just a screen notification (together with any camera requirements that may be set).
- **Break Allowance** - Allows you to alter the number of times that the rule can be broken before the defined *Action* is triggered. The default value of *0* will trigger an alarm at the first instance.
- **Breaking Condition** - (Area Movement and Numeric only) Determines the main argument used by the rule in combination with the *Property Name* and *Property Value*(s) options. *Breaking Condition* options for area movement rules are either *Is Inside* or *Is Outside* (the area). *Breaking Condition* options for numeric rules include *Is Smaller Than*, *Is Equal To*, *Is Between*, *Is Outside* etc. (the latter two options require two *Property Values* to form a range).
- **Classification** - Allows you to optionally dedicate the rule to objects of a particular type (debris, person, car, etc.) as differentiated during the tracking process.

continued

- **Classification Probability** - Allows you to optionally define a confidence level which must be matched or exceeded for a given track (of the type selected within the *Classification* option discussed above) before it can be considered within the rule. The use of this option provides an opportunity to filter out potential nuisance alarms. The main probability value is created during the tracking and classification process and is displayed against each entry within the *Tracks* tab. When this option is set to zero, the requested *Classification* type will be accepted at any level of probability (as determined by the tracker), rendering this filter inactive.
- **Count Coasted Tracks** - When the tracker loses sight of a track, it estimates where the track should be based on previous sightings. This is called coasting. If this setting is on then such sightings count towards the break allowance, otherwise they are ignored.
- **Description** - The text entered here will become your primary method of identification for the rule within the list. You are strongly recommended to create concise yet distinctive names for your rules. In situations where numerous rules are listed it will make it much easier to locate the required one. For area movement rules in particular, it can be advantageous to include the name of the monitored area within the rule description for easy identification.

  In addition to static text that will remain the same regardless of where the rule is broken, you can add placemarkers that will call dynamic text to indicate the particular information, such as the area, sensor, etc. See Appendix 4 for details of alarm placemarkers.
- **Disarm by Sensor** - Allows you to define a static sensor that can be used to temporarily or permanently disarm the current rule. This option is most often used to provide a timed-disarm button that allows authorised personnel to walk through a radar monitored area without causing an alarm. Once a sensor is selected other related options will be displayed: *Disarm Sensor State* and *Use Disarm Timer*.
- **Disarm Sensor State** - Displayed when the *Disarm by Sensor* option is ticked. This option defines whether the disarm action should be triggered from a *True* or *False* state from the chosen static sensor.
- **Disarm Time Period** - Displayed when the *Use Disarm Timer* option is ticked (which in turn is displayed only when the *Disarm by Sensor* option is chosen). Enter a time period (in seconds) after which the current rule will be rearmed.
- **Distance** - (Approach only) Determines the distance between two vehicles or vehicles and a particular area, below (or above) which an alarm should be created.
- **Distance Check** - (Approach only) Determines the relevant breaking condition for the rule: *Less Than* or *Greater Than* for use with the *Distance* value.
- **Enabled** - The rule is active when this option is ticked. This is a useful way to quickly deactivate rules that are not needed, either temporarily or permanently.
- **Hide Tracks** - Allows you to specify whether targets should be hidden in particular cases. This property is useful to allow you to create a pair of similar rules which act upon the same area (e.g. a location that is very busy during the day). By alternating the times of day that the two similar rules operate within the same area could have the combined effect of hiding targets during the day and then showing them during the night. Options are *Never* (always show all targets), *If Broken* (only show targets that break the rule), *If Not Broken* (only show targets that are not breaking the rule), *Always* (keep all targets hidden).
- **Linked Type** - (Historic only) Defines how the historic rule should respond to the conditions of its constituent rules, i.e. 'when should the historic rule be considered to be broken?' The options are: *All* (when selected, all of the constituent rules must be broken within their respective time restrictions to cause a response trigger), *Any* (when selected, the historic rule will be considered broken as soon as any of the constituent rules are broken) or *None* (when selected, the historic rule will be considered broken when none of the constituent rules are broken - this is equivalent to a logic NAND operation - and would be used where the constituent rules are configured to be broken for the majority of the time, e.g. ensuring that there is always at least one person within a certain area).
- **Latitude/Longitude** - (Approach only) Used to define the centre of a location/ region that you need to detect being approached by a tracked person, vehicle, etc.
- **Min Dynamic Break Count** - This field is displayed only when the *Use Dynamic Break Count* option is ticked. The value entered here will be used to modulate the usual Break Allowance value according to how many times a track has been sighted outside the monitored area. For example, if the Break Allowance is set to 5 and the Min Dynamic Break Count is set to 3; providing the track has been seen three times externally to the area, the number of sightings required within the area to cause an alarm will be 5 - 3 = 2. Thus, after only two sightings of the track within the area, the rule will be considered broken.
- **Min/Max Speed** - Determines the minimum and/or maximum speed of travel that should be used as the threshold(s) for a breaking condition.
- **Persists** - When selected, once a target breaks the rule, that target will continue to be marked with the *Severity* level that is defined within the rule, even when the target ceases to break the rule. In certain circumstances the severity level may go up (e.g. from *Warning* to *Threat*) but it cannot fall below the stated Severity level (e.g from *Warning* down to *Friend*).

continued

- **Property Name** - (Area Movement and Numeric only) - Defines the numeric property that will be monitored by the rule. In each case, the *Property Value 1* entry (and in some cases *Property Value 2*) are where you enter the corresponding value(s) to be ruled against for the chosen property. The options are: *SpeedMps* (monitors the speed of travel of a target in metres per second), *DirDegrees* (monitors the direction of travel of a target in degrees clockwise from due North), *Size* (monitors the size of a target stretching away from the radar sensor in metres), *SizeDegrees* (monitors the size [azimuth] of a target measured across the radar scan in degrees), *Seen* (monitors the number of times that a target has been viewed by the radar sensor, i.e. the number of radar sweeps in which a target has been present), *Strength* (monitors the radar signal strength for a target).
- **Property Value 1 / 2** - (Area Movement and Numeric only) Defines the numeric quantity (or quantities) that is/are related to the chosen *Property Name* and *Breaking Condition*. For instance, if the chosen Property Name is SpeedMps, then the *Property Value* must contain the value of the speed in metres per second. Where the Breaking Condition is set to either *Is Between* or *Is Outside*, there will be two *Property Values* in order to form a range.
- **Relay** - Defines the ID of the relay that should be activated when the rule is broken. Choose '0' to disable.
- **Rule 1 / 2** - (Compound only) Defines the two constituent rules that will form the basis of the compound rule.
- **Rules Operator** - (Compound only) Defines the logical operator that will be used in combination with the two constituent rules to determine whether the compound rule has been broken. Options are And (both constituent rules must be broken to break the compound rule), Or (either of the constituent rules can be broken to break the compound rule) or Nor (the compound rule is broken when neither of the constituent rules are broken).
- **Send SMS** - Allows you to define one or more phone numbers to which the *Alarm description* should be sent by text message when an alarm condition occurs.
- **Sender Radars** - Displayed when the *All Radars* option is unticked. This section allows you to exclude radar sensors that may be in range but which cause unwanted effects when used with a particular rule. Use the checkboxes to include/exclude radar sensors in relation to the current rule.
- **Sensor** - (Static Sensor only) - Links a particular static sensor to the rule.
- **Severity** - Defines how a target should be marked when it breaks a rule. Such markings allow a target which presents a *Warning* (orange) or *Threat* (red) to be easily differentiated from a *Friend* (green) or *Unknown* (neutral colour).
- **Show Area in Alarm** - When ticked, the area or section in which the rule has been broken will be highlighted within the site map.
- **Sub Type** - Optionally allows you to define a particular movement classification (that should cause an alarm state) for vehicles within the detection area(s) under surveillance. Options are: *Default, Stopped, Slow, Debris, Reversing* and *Queue*.
- **Time Restriction** - Allows you to optionally define a time period when the rule is to be active. Options are: *None*, *Custom*, *Apply During 9 to 5*, *Do Not Apply During 9 To 5*, *Apply On Weekdays* and *Do Not Apply on Weekdays*. When the *Custom* option is chosen, additional date and time selectors are displayed. *None* indicates that the rule should always be active, subject to the setting of the *Enabled* option.
- **Target +/-** - (Approach only) Allows you to define a tolerance zone around the perimeter of the stated *Distance* to the location being monitored.
- **Trace Logging** - Outputs more information about what causes the rule to break. Mainly used in Highways where rules are usually more convoluted.
- **Trigger Value** - (Static Sensor only) Defines whether the alarm should be triggered from a *True* or *False* state from the linked static sensor. *Note: If you change the trigger value property for a rule, you will need to restart Canary before the sensor behaves correctly.*
- **Use Allowance Curve** - This option works in conjunction with the *Break Allowance*. When this option is enabled, the break count is permitted to go down as well as up. The break count will be incremented when a target is breaking the rule and then decremented when it is not. Additionally, you can set the *Allowance Increment* and *Allowance Decrement* values so that you can weight the rate at which a target increases and decreases its break count. The alarm will only be activated once the *Break Allowance* value is reached. This option is useful in situations where you expect targets to momentarily break rules but not to continue doing so and so prevent false alarms. For worked examples, see Appendix 6 - Using the allowance curve.
- **Use Disarm Timer** - Displayed when the *Disarm by Sensor* option is ticked. Tick this option to set a *Disarm Time Period* after which the current rule will be rearmed.
- **Use Dynamic Break Count** - When ticked, this option permits previous sightings of a track (prior to it entering the monitored area) to be taken into account when deciding whether the Break Allowance has been exceeded. The logical argument for using this option is: If a track has been sighted several times prior to entering the area then it is known to be genuine, so there is no need to wait for the full number of *Break Allowance* sightings within the area to take place. When this option is ticked, a *Min Dynamic Break Count* field will be displayed to allow the minimum number of required external sightings to be defined.

Adding time restrictions/schedules to a rule

In situations where one or more rules need to be applied for limited time periods, use the related *Time Restriction* and *Schedule* options to define the required periods of inclusion or exclusion for any particular rule.

To apply a time restriction

1 Display the required rule within the *Rule Editor* and click the **Edit** button.

2 Click the **Time Restriction** drop down list and select the **Custom** option.

3 The **Schedule** button will become available at the bottom of the dialog, click it to display the *Task Schedule* pop up.

4 Click the **Begin Date** drop down list and choose an appropriate start date.

5 Click the cursor into the **Start Time** field and enter the required start time.

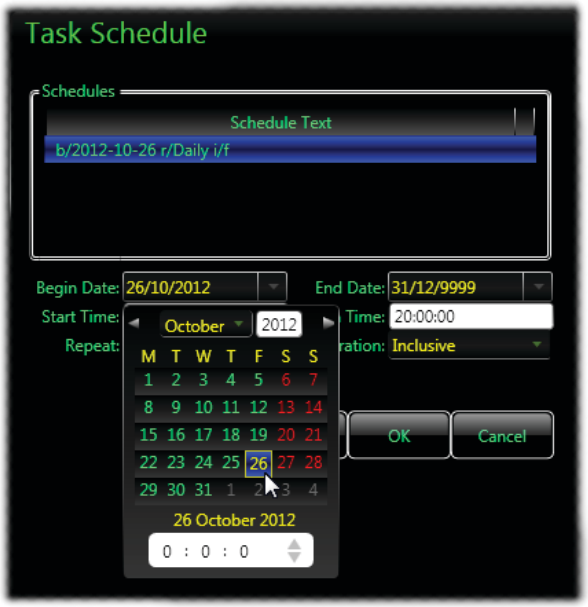
6 Click the **Repeat** drop down list and choose how the schedule should be applied: *Once, Daily, Weekly* or *Monthly*.

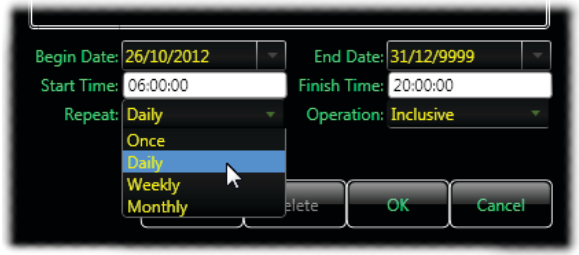
7 Click the **End Date** drop down list and choose an appropriate date.

8 Click the cursor into the **Finish Time** field and enter the required end time.

9 Click the **Operation** drop down list and choose whether the defined schedule period is **Inclusive** (i.e. the rule will only be active during this period) or **Exclusive** (i.e the rule will only be active outside of this period).

10 Click the **OK** button to save the settings.





Appendix 4 - Alarm description placemarkers

When a rule is broken the text that has been placed into the *Description* field of the rule (see To define rules) is displayed on the operator's console and is also recorded within the alarm log. This text can be completely static (causing it to give the same message regardless of where, or by what means, the rule was broken). Alternatively, it can also include placemarkers that will be replaced by contextual references (when the rule is broken) that may help to pinpoint the nature of the alarm.

There are four placemarkers that can be added to the *Description* field within any rule:

- {AREA} This marker will be replaced with the name of the area within which the rule was broken.
- {AREAID} This marker will be replaced with the identity (ID) number of the area within which the rule was broken.
- {RULEID} This marker will be replaced with the identity (ID) number of the rule being broken.
- {SENSORID} This marker will be replaced with the identity (ID) number of the sensor that monitored the rule break.

To use an alarm description placemarker

1 Create the rule as usual.

2 Within the *Description* field, place one or more of the placemarkers shown above with supporting text such that it assists the operator to make better sense of the alarm. For instance:

"Threat in area {AREA}"

"Sensor {SENSORID} has triggered rule {RULEID} in area {AREA}"

Appendix 5 - Adding items without wizard assistance

This appendix contains procedures for adding and configuring various Witness items independently of the assistance wizards:

Manually adding a radar sensor and tracker

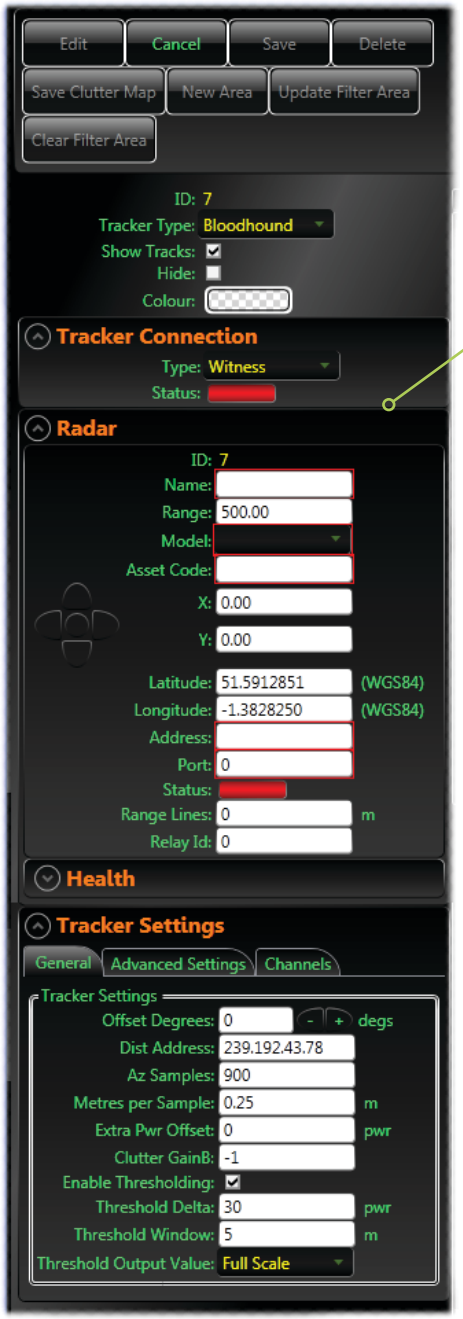
For every radar sensor, the system requires a matching tracker service, therefore the addition of one is accompanied by the other - both are added and edited together within the **Radars & Trackers** section.

A wizard is available to guide you through the process of adding a new radar sensor and tracker - click here for details. Otherwise, use the procedure outlined here to add the details manually.

Note: You must be in admin mode to make changes - see Entering admin mode.

To add a radar sensor and tracker

1. Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** entry and then click the **New** button. A popup will ask whether you wish to use the wizard.
2. Click the **No** button to bypass the radars and trackers wizard. A new radar and tracker configuration will be shown
3. Click the **Radar Type** box and select the appropriate entry. A new set of options will be added to the display.
4. Once you have completed the primary settings (Tracker Type, Radar Model, Radar Address and Tracker Settings), click the **Save** button.



ID
The **ID** number is automatically set by Sentinel and is the bond between the radar and the tracker.

Tracker Type
Choose the appropriate tracker. *Foxhound* is not used with AdvanceGuard installations, so ensure this option is set to *Bloodhound*.

Tracker Connection
Defines the communication link between the tracker and the Piccadilly data server. If you are using Bloodhound then choose *Witness*.

Radar
Enter a **Name** for the radar sensor. This is particularly useful in a multi-sensor installation.

Choose the appropriate **Model** from the list. As you do so, you will be asked whether you wish to apply the default tracker settings. Click the **Yes** button.

Optionally enter an **Asset Code** for identification purposes.

X and Y
Each new radar sensor is initially assigned to the default Latitude and Longitude of the origin point of the installation. You can adjust the **X** and **Y** settings to define the offset position (in metres) of the radar sensor from the origin point either by typing the offsets into the fields or you can drag the image of the radar sensor to the required position within the site map or use the joypad button controls.

Address
Enter the IP address of the radar sensor.

Range Lines
Defines the distance between the range lines that are shown on the graphical representation within the site map.

Health
These items remain blank until the connection to the radar sensor becomes fully active.

Tracker Settings
DistAddress The default is a multicast address and can be picked up by all systems. However, some networks may block, or not support, multicasts, in which case you will need to change this address to the unicast IP address of the PC running Sentinel.

Advanced Settings
At this stage, most advanced settings can remain at their default values.

Later, the advanced settings section will be used to link this tracker with the areas and tracking parameters - see Manually linking areas and tracking parameters within trackers.

For more details about all settings, see the Objects > Trackers section.

Next steps

- Align radar sensor(s)
- Create detection areas
- Fine tune detection areas

Manually adding a detection area

Detection areas are how you inform the system of the outer limits of where you wish it to pay particular attention. You can define one or more areas and apply rules to specifically monitor the movement of people or objects within those areas. You can also layer one or more areas to create exclusion zones within the main area. A wizard is available to guide you through the process of adding a detection area - click here for details. Otherwise, use the procedure outlined here to do it manually.

The creation of new detection areas is generally achieved in two stages:

1 Create rough initial outlines for the detection area(s).

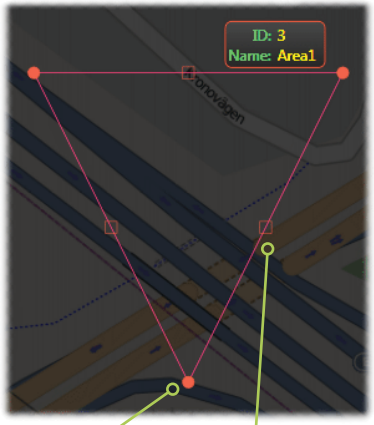
2 Use live data to fine tune the area outline according to the viewed tracks and radar background data in order to isolate the area(s) fully from the surrounding land and/or roads.

Note: You must be in admin mode to make changes - see Entering admin mode.

To add a detection area

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), choose the **Objects** tab and click the **Areas** entry. Click the **New** button. A popup will ask whether you wish to use the wizard.

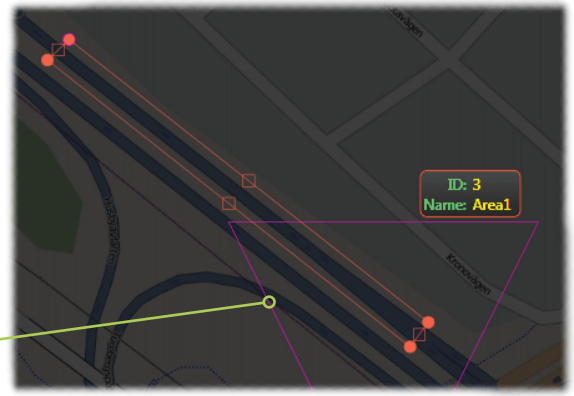
2 Click the **No** button to bypass the area wizard. A new triangular detection area will be added to the graphical representation within the site map ➲



3 Alter the shape of the detection area:

- To move the whole area: Click and hold anywhere within the area and drag it to the required position.
- To move a corner point: Click and hold on one of the solid circular corner points and drag it to the required position.
- To add another corner point: Double click (or right-click) on one of the hollow square points which are mid-way along each line.
- To remove a corner point: Right-click on the solid circular that you wish to remove.

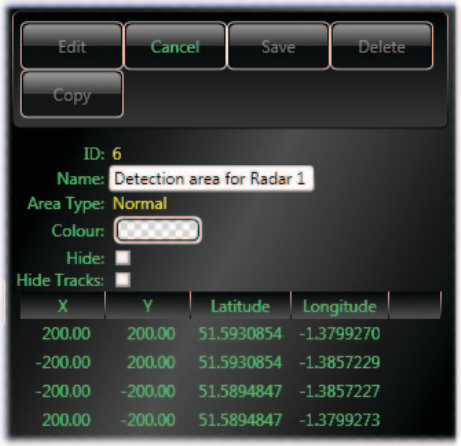
As you add corner points and drag them, your area will begin to take shape ➲



4 When your area is the correct shape and in the right location, enter a name for it within the information panel ➲

5 Optional step. A new label will be created (containing the name that you enter) near to the new area. You can click and hold on it to drag it to the required position within the site map, where it will remain once the area is saved.

6 Optional step. You can adjust the colour shading and opacity of the area that will be shown on the graphical representation. This is useful when there are numerous areas as it helps you (and the operator) to distinguish them.



7 When all details for the area are complete, click the **Save** button.

8 Before a new detection area can be used with a radar sensor, it must be linked to a set of tracking parameters within the tracker of the radar sensor. For details see Manually linking areas and tracking parameters within trackers.

Next steps

- Fine tune detection areas
- Create new tracking parameters
- Manually link an area to tracking parameters
- Create radar filter areas

Manually linking areas and tracking parameters within trackers

This optional step may be required if new tracking parameters have been created and have not been linked to areas with the assistance of the wizards.

Before a tracker can provide useful information to the system, it needs to be linked to at least one detection area plus a set of tracking parameters (tracking parameters determine how the interpreted radar data should produce relevant tracks). This linking takes place within the **Advanced Settings** section of each **Tracker**.

Note: You must be in admin mode to make changes - see Entering admin mode.

To link a detection area and tracking parameters within a tracker

Note: If you are already viewing the appropriate tracker details, start at step 3.

1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab. If the list of trackers is not already shown, double click the **Radars & Trackers** entry.

2 Click on the name of the required radar/tracker entry and then click the **Edit** button.

3 Within the *Tracker Settings* section, change to the Channels tab and then scroll to the bottom of the list where you will find the *Tracking Areas* sub-section.

4 To make a new link between an area and a set of tracking parameters, click the **+** button.

5 In the resulting popup, click the **Area** list and choose the appropriate detection area name ➲

For details about manually creating a new area, see the section Adding an area.

Use this section to link an Area to a set of Tracking Parameters.

6 Within the same popup, click the **Parameters** list and choose the tracking parameters that you wish to link with the selected area (see explanation right).

7 Click the **OK** button. The chosen area and tracking parameters will be listed within the *Tracking Areas* list.

This action has now linked the radar, the tracker, the area and the tracking parameters.

Note: You can use any single set of Tracking Parameters with as many detection areas as required (duplicate tracking areas cannot be used). However, be aware that if a change is made to a set of tracking parameters (to suit a requirement in one area) all other areas that use the same tracking parameters will be similarly affected.

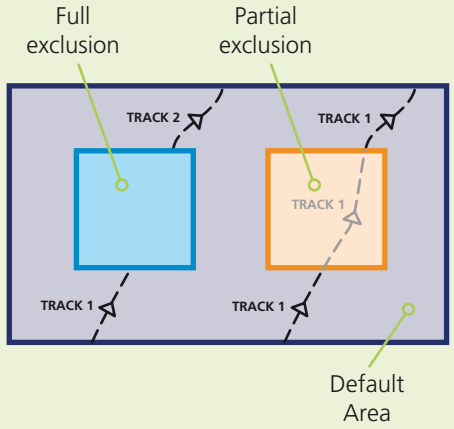
8 Optional step. Where necessary, use the ^ v buttons to rearrange the order of the area/parameter entries within the list. This determines the order in which they are processed and is very important when areas with mixed parameters are used (see explanation right).

9 Click the **Save** button.

Area parameters and ordering

Certain situations can cause false tracks to be created and/or alarms triggered: Most commonly: trees moving in the wind. One solution is to adjust the affected tracking areas in order to isolate the cause(s) of false tracks.

The Tracking Areas section (Objects > *Trackers* > Advanced Settings) allows you to apply one of three *Parameters* to each area:



- **Full Exclusion** - This type of area is the equivalent of a black hole to the system; everything within its borders is completely ignored. Any track entering a full exclusion will be lost and created as a completely new track upon exiting the area.
- **Partial Exclusion** - When an area is classified thus, existing tracks will be followed through the area, however, new tracks cannot be created within the area.
- **Default** - This is the standard classification for areas and allows tracks to be created and followed in the usual manner.

Where a track enters a location covered by overlapping area types (and monitored by a single tracker), it is the area that is highest in the list (within the *Tracking Areas* section) that will be solely used to process the track within that location. The area types must be placed in this order:

1st: Full Exclusion,

2nd: Partial Exclusion and

3rd: Default. *As demonstrated here* ➲

Area	Parameters
Building	Full Exclusion
Tree 1	Partial Exclusion
Tree 2	Partial Exclusion
Main zone	Default

Next steps

- Add cameras
- Add camera areas
- Add video viewers

Manually adding a camera

A wizard is available to guide you through the process of adding a new camera - click here for details (this section also details the relationship between camera groups and camera connections. Otherwise, use the procedure outlined here to add the details manually.

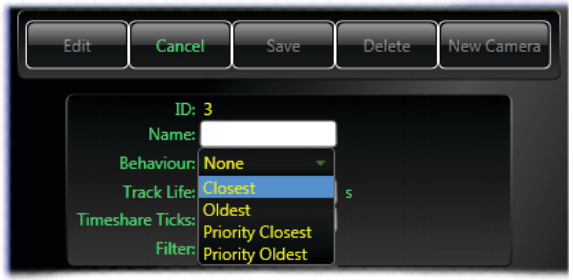
To add a camera

Note: You must be in admin mode to make changes - see Entering admin mode.

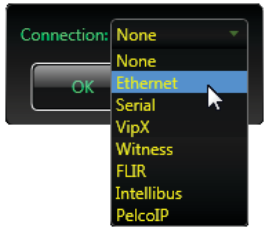
1 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), choose the **Objects** tab and double-click the **Cameras** entry.

If required:

- To create a new Camera group: Click the **Camera Groups** entry and then click the **New** button. In the information panel, enter a name for the new camera group and then choose the appropriate behaviour mode. Optionally choose a Filter. Click the **Save** button.

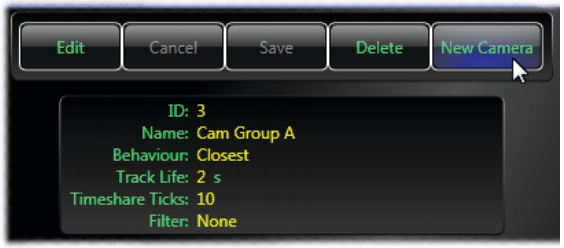


- To create a new Connection group: Click the **Camera Connections** entry and then click the **New** button. In the information panel, choose the required connection type and click the **OK** button.

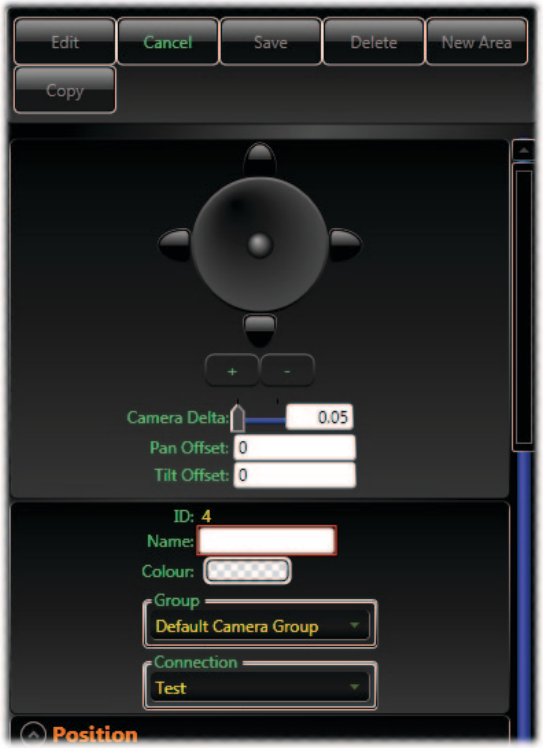


A new entry will be created in the information panel. Enter a name for the new connection group and then configure the appropriate connection properties. Click the **Save** button.

2 Click the required camera group or connections group and then click the **New Camera** button



A blank camera configuration will be shown within the information panel



3 Edit the various options to suit the camera installation. See Objects > Cameras for details about all options.

4 When all required options are set, click the **Save** button. The new camera entry will be listed as a member of the chosen *Camera Group* and *Camera Connections*.

Next steps

- Add cameras
- Add camera areas
- Add video viewers
- Add static sensors
- Define rules

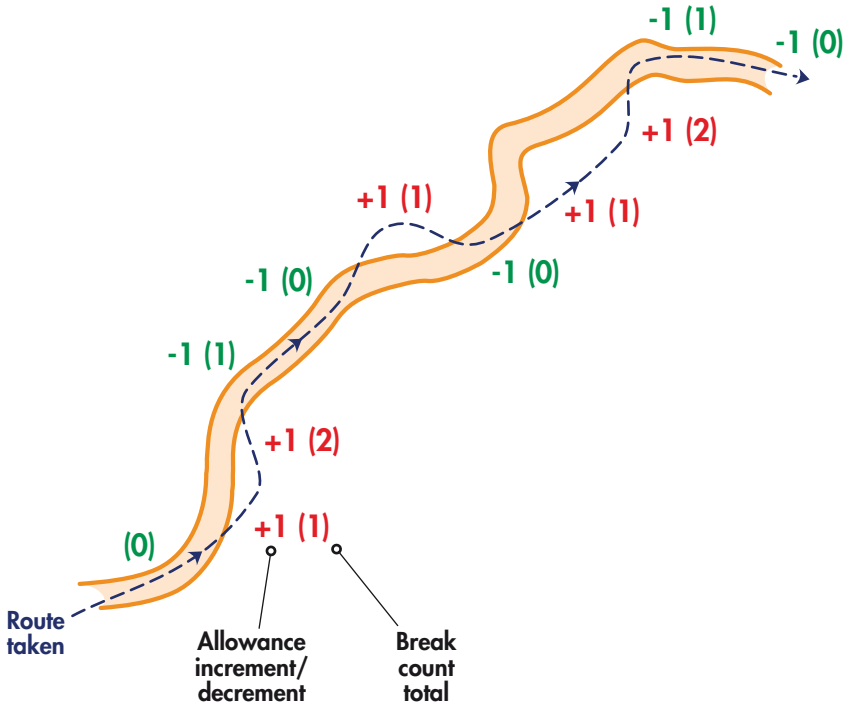
Appendix 6 - Using the allowance curve

When the *Use Allowance Curve* option is enabled within a rule, the break count (the number of times that the rule has been broken) is permitted to fall as well as rise. This allows some leeway (allowance) to be built into the rule to avoid unnecessary alarms.

In the example given here, the target is moving along a path through a golf course. However, the target does not stick rigidly to the path and wanders onto the greens. Using the allowance curve, the break count increments when the target deviates from the track and decrements once the target returns to the track.

Using the *Break Allowance* property you can determine the maximum allowable break count before an alarm condition is raised. Additionally you can use the *Allowance Increment* and *Allowance Decrement* properties to determine the size of increment and decrement, thus 'weighting' desirable and undesirable behaviour accordingly.

In the example, the Allowance increment and decrement values are both set to 1 (thus, 1 is added when the rule is broken and 1 is removed every time the target is seen not breaking the rule). The *Break Allowance* is set to 3.



The result of the example is that although the target occasionally moves off the path, the break count never reaches the Break Allowance value of 3, therefore, no alarm is raised. If the target did stay off the path for 3 consecutive observations or strayed off the path five times out of seven (+2-2+3), then an alarm would be raised.

Appendix 7 - Recording radar data

For commissioning and diagnostic purposes it is possible to record the raw data from any particular radar sensor. This facility is available to admin users only.

To record radar data

1 Ensure that you are logged in as admin user.

2 Within the selection panel in the top right corner (if hidden, click the small panel button on the right hand edge to reveal), select the **Objects** tab, click the **Radars & Trackers** entry.

3 Click the **Recording Control** button to reveal a popup

After a short delay, the available radar sensors should all be listed within the popup.

4 Click the radar that you wish to record and click the **Start** button.

5 After the required time period, click the **Stop** button.

The recorded data are stored as a file within the same folder as the Bloodhound that serves the recorded radar sensor. The filename will take the following form:

BH-*{tracker Id}*-Data-*{timestamp}*.cpr

Appendix 8 - Object classification

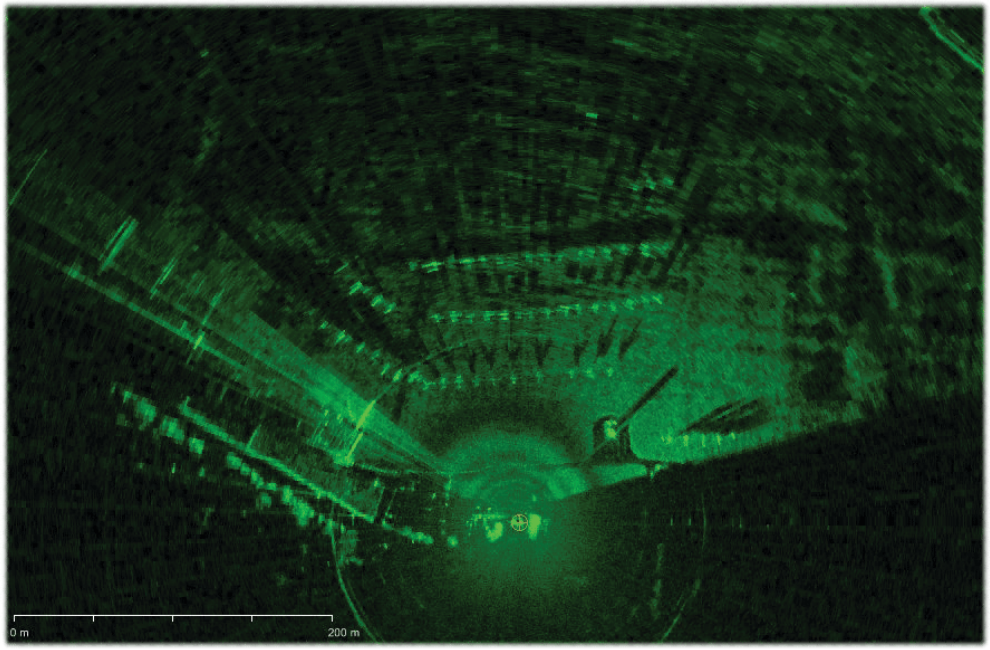
This appendix provides an overview of the key stages that are required to interpret the mass of incoming radar data into valid and accurate object tracks in preparation for interpretation by the rule engine.

Basic tracker processing

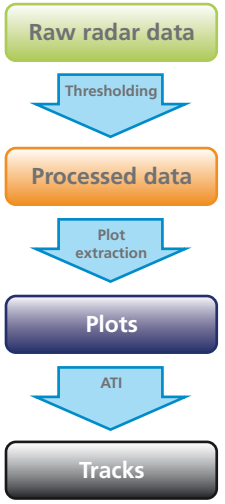
All Navtech Radar sensors emit raw data at up to 11Mbits/s (depending on the model). This results from (up to) 3200 range samples over up to 909 azimuths, quantised at 8 bits. This data in effect represents a polar JPEG of the surrounding radar reflective objects (persons, vehicles, trees, grass, buildings etc).

This polar JPEG is generated once per revolution and for the majority of Navtech sensors this happens to be 1Hz, i.e. one revolution per second. For instance, an I500 radar sensor uses 909 azimuths, with 2000 per azimuth and a 1Hz rotation rate.

An example of raw data is shown below, showing approx 300m radius of data:



This raw data goes through three levels of processing in order to generate a track, i.e. an object of interest. This processing chain is shown here:

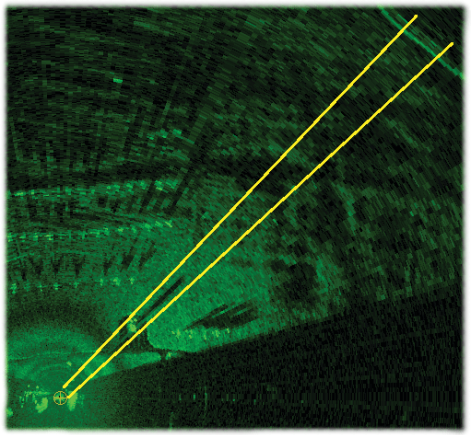


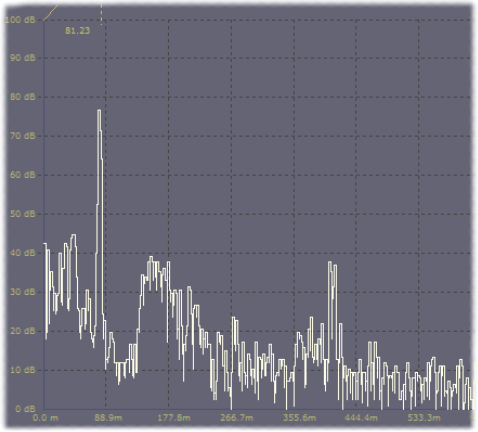
Thresholding

The raw radar data first undergoes *Thresholding*. Essentially, this is a filter which only passes reflections that meet or exceed a pre-determined amplitude. All amplitude data is quantised at 8 bits, giving a range of 0 to 255. The gain at the input of the ADC onboard the radar is such that 1 quantisation level equals 0.5dB of signal. Therefore 0 to 255 represents 0 to 127.5dB of signal (to noise).

A typical thresholding value for any radar is in the range 28 to 34 (or 14 to 17dB signal/noise).

The image below shows a radar plot of a civil airfield. The yellow lines (crudely) denote a single azimuth measurement at an approximate bearing of 45 degrees from North. The amplitude of samples along this bearing are shown to the right:

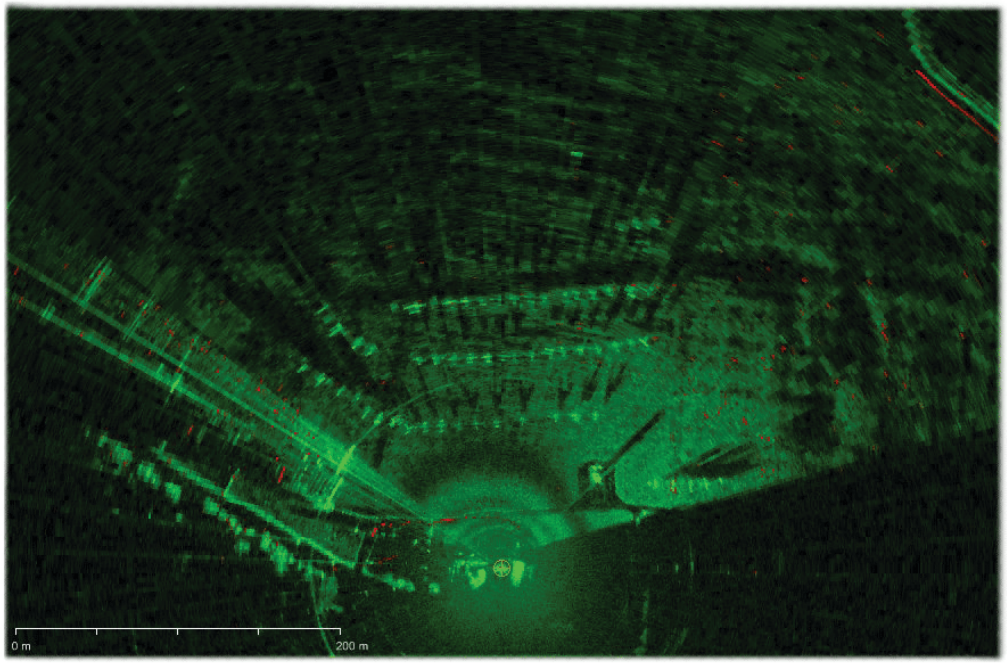




Observe the two large (narrow) peaks, which are returns from a small petrol refilling station and a tree lined perimeter. Both should be obvious in the radar data as bright green spots within the yellow lines.

Also note the 'shadow' behind the petrol station shows as a dip in the signal immediately after the peak, followed by a rise in the signal level caused by radar return from a grass surface (which slopes upwards, though this is not visible in the radar image).

Basic thresholding looks for any part of the signal which exceeds a certain signal to noise ratio, for instance 17dB. The noise in this case being an average value of clutter, i.e. radar return from other objects nearby which are of no interest. The threshold process results in processed radar data, which is shown below as red pixels in the display. It should be noted that thresholding applies other related operations (such as removing stationary information), but that is beyond the scope of this explanation.



In the above image, red processed data is now overlaid on top of the raw radar data. You can clearly see an object trail paralleling the perimeter at the top right. Other red pixels may be actual objects of interest, or could be clutter data which has (unintentionally) breached the thresholding process.

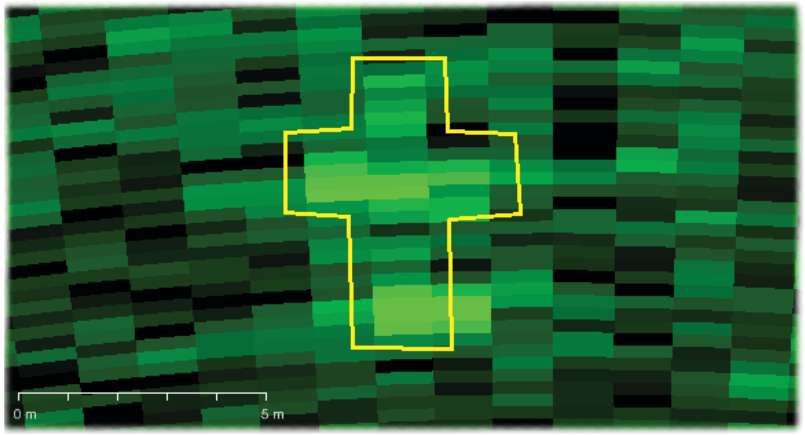
Is important to note that the default thresholding process now converts all processed data to have an intensity value of 255, i.e. maximum. This ensures that intensity checks further along the processing chain are bypassed. Note that it is possible to turn this 'ceiling' step off and therefore the next two parts of the processing chain can make their own evaluation based on intensity, however, this complicates matters.

Plot Extraction

We now have a smaller data set, representing objects which exceeded a specified signal to noise ratio. *Plot extraction* now analyses the physical size of the processed data 'pixels' in order to (most likely) exclude very small pixels which are generated from i.e. grass, trees, water etc. If left unfiltered these would potentially lead to false alarms.

Plot extraction therefore uses physical dimension values, mostly, to filter the data. These can be specified in metres, degrees or pixels.

Refer to the image below. This shows a light aircraft facing South. A yellow box has been drawn to emphasise the aircraft.



You should be able to see that the aircraft is brighter than the surrounding area. Note that if the aircraft were moving, it would be marked in red – having been turned into processed data following thresholding.

In order to remove false alarms plot extraction now applies filters based on size:

- Dimension in metres in range (the axis towards/away from the radar)
- Dimension in metres in azimuth (the circular axis around the radar)
- Dimension in bins in range (the axis towards/away from the radar)
- Dimension in degrees in azimuth (the circular axis around the radar)
- Number of 'pixels' making up the object (each pixel having been passed through thresholding). This is known as the weight.

Note that a 'bin' is a sample over range. In the case of the I500 radar, this is 25cm. You can see that bin count and range in metres are linked, so you may use either. For example, a plane of length 10m would be the same as 40 bins on the I500. Likewise an azimuth value in metres is related to the azimuth degrees (but varies as the object gets closer or further away).

Typically we wish to week out anything less than a person, so the default values of 1 range bin and 2 weight cells is sufficient to allow the tracker to ignore most false alarms. We now have a plot.

Automatic Track Initiation

The above series of processing has led us to a collection of objects with sufficient amplitude and physical size to be considered an object of interest, or track. However, everything we have done so far has been confined to a single scan image. We have no concept of how fast an object is travelling, or in which direction, or how many times we have seen it previously. To achieve these values we must analyse several adjacent scans.

Automatic Track Initiation (ATI) is therefore concerned with movement and history of an object. ATI serves as the final processing stage, the output of which is a track.

ATI is configured (mainly) with the variables below (there are many, many more)

- Of the last N scans, only create a track if we have seen it M times (default M=3/N=5)
- Only create a track from the plot if it's travelling at a certain minimum and maximum speed (calculated as distance elapsed between scans divided by the scan time).
- Only create a track if it is travelling in a straight line, +/- a certain error margin in degrees, called the turn rate (calculated as angle of direction change between scans).

It is only tracks which are shown within witness, and only tracks can break a rule, trigger an alarm, and only tracks can be classified. This is because classification relies not only on plot size, but on track speed and turn rate.

Tracks and models

We have seen above that in order to become a track, an object needs to exhibit various attributes and behaviour, i.e. physical size, speed, directional change rate etc.

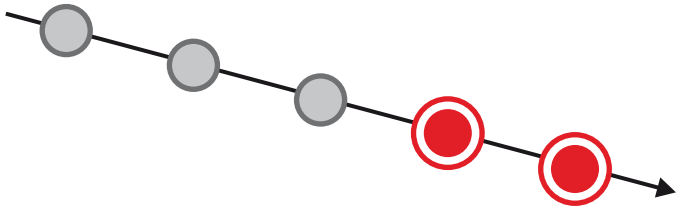
The classification study postulated that different object types would exhibit a certain set of attributes, and thus would be clearly different from other object types. For example people are smaller than vehicles. Vehicles travel faster than people. People can make quicker turns than vehicles, and so on.

These attributes led to the creation of a classification model, described in more detail in section 3. A model is created for each possible object type. The model lists likely values for each attribute (both a minimum and maximum, giving a range, or just a minimum).

Each track generated within witness is 'scored' against this model using those values. Whichever model ultimately scores higher is deemed the correct model for that track.

Use of provisional tracks

We have discussed that classification takes place once an object reaches the state of becoming a track. This is ostensibly the point at which it appears in witness, however in reality a track exists several seconds before appearing in witness. Take the below image for example.



This image shows the process of "ATI'ing" a plot. Using an M/N of 3/5, we get 3 plots (i.e. objects which satisfy the threshold and plot extraction criteria) leading to a track on the 4th plot onwards.

We have already stated that classification uses track data (as it needs speed/turn rate information), so in the example above, classification could not start until the 4th sample unless we use provisional track information.

Use of provisional tracks simple means to include the track-type information available from those plots which ultimately led to a track. In the above example this leads to a classification result 3 seconds earlier.

The downside (for a very low M/N) could be that the track is actually the result of a false alarm, so we end up with a classified false alarm. This should not be a problem if the tracker is tuned correctly.

Use of provisional tracks can be turned off in the classification XML file.

Classification sample count

Just as the M/N count avoids false alarms from random plots, so classification has a similar method to avoid false classifications.

A sample count tells the classification engine how many tracks to use. The default is 6 samples, optionally including provisional tracks as discussed above.

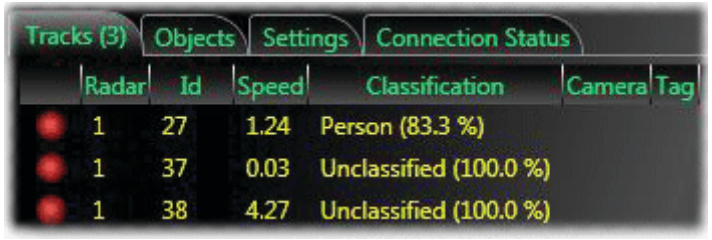
Percentage confidence and retriggering

The above process results in a score per track per classification model. Assuming the models are sufficiently different (with mutually exclusive values, mostly) then a high score for one model should result in a low score for all others.

There may be situations where a track doesn't score highly at all in any model category. Regardless this track would still be classified according to the one with the highest score.

To prevent this, the user is able to configure a percentage confidence rate to which the classification should aim. You may set this very strict, however a satisfactory rate may be 70%. (Details of the scoring are covered in section 3).

If the classification doesn't attain this confidence value, then subsequent tracks will be analysed and added to the score until such time as the confidence percentage is achieved. During this initial period the track will be marked as 100% unclassified as shown below in a screen capture from Sentinel.



The number of extra tracks analysed in the event of no classification occurring is configured in the classification XML file. The default is 3.

Classification icons

The end result of the above processing is that a standard track dot changes to a classified icon, as shown below.

Two tracks classified as persons

A track classified as a vehicle

The classification state of all tracks is shown in the object pane.

A warning about plot merging

Users should be careful about correct usage of plot merging. Two extreme cases are possible:

- A large vehicle may generate many large plots (as the radar beam sweeps the vehicle, it could hit it in several places). With plot merging turned off (or misconfigured) these plots would appear to be unconnected to each other, and would be more likely to be classified as several persons.
- At the other end of the spectrum, several persons, standing close to each other could be merged into a single track if plot merging is turned on and set too aggressively. In this case a group of people, merged, would have the potential to be classified as a vehicle.

Note that false classifications are made harder by using multiple attributes, not just size of the plot.

Attributes are explained further in the next section.

Classification attributes & weighting

We have discussed above how each track sighting is analysed in terms of its classification 'score' against each model in the system. This score is calculated by determining if certain attributes are within a specified range. For each attribute that is within the range, that model gets 1 attribute point. Each attribute point is then weighted according to how important that attribute is to the model. This gives each track a score. The default classification uses 6 tracks (or samples), so a track's final score is given as a percentage of achieved score against possible total score (over those 6 tracks). A worked example is given shortly, but first a brief listing of the available attributes, followed by a table summarising the system defaults.

Attributes

Speed

Speed is expressed in metres per second (and is calculated as the distance between two tracks divided by the time between those two samples (i.e. the radar rotation time in seconds)).

Each model specifies a minimum and maximum value for speed. If the track speed is within this range, it gets a point against that model.

Expected Speed

Similar to the above, though Expected Speed allows an extra point towards a model if an object is travelling at a speed determined to be ideal (or more typical of a certain model).

For example, a vehicle may be able to travel at speeds from 0m/s to 44m/s (100 miles or 160km per hour) but in an urban road environment it's more likely to be travelling from 4 to 14m/s (10mph to 30mph).

Acceleration

Acceleration is expressed in m/s^2.

Each model specifies a minimum and maximum value. If the track acceleration is within this range, it gets a point against that model. The minimum value may be negative, i.e. allowing deceleration values to be expressed also.

Weight

Weight specified the number of 'pixels' making up the track.

Each model specifies a minimum and maximum value. If the track weight is within this range, it gets a point against that model.

Strength

Strength is a value made up of weight and radar return intensity (as per thresholding). Note that in an earlier section it was mentioned that all processed data exits thresholding with a value of 255. Therefore the Strength, by default, is weight multiplied by 255.

If other forms of thresholding were used and the real intensity was output, then the current strength values would need to be revisited. This is unnecessary for relatively short range such as the I500 has.

Strength is specified in each model as a minimum and maximum.

Seen Moving

This attribute aims to be an indicator as to whether the object has been seen moving. This is determined by looking for a speed above a specified minimum, and is expressed in metres per second.

Direction change

Direction change is the same as track turn rate, i.e. for each track we analyse how much the direction of travel has changed compared to the previous track.

This value is expresses as a minimum value in degrees.

(As an example, a person may change direction more quickly than a vehicle, so would have a higher value).

Weighting

Following a track's score against each attribute, it is possible to bias or weight the results in favour of certain attribute.

Four keywords exist to determine attribute weight, each with a different multiplier for the attribute point.

- Critical gives a multiplier of 5
- Desirable gives a multiplier of 3
- Optional gives a multiplier of 1
- Ignore gives a multiplier of 0

Note that ignore effectively 'turns off' certain attributes from having an effect on classification without the need to remove those segments of XML from the classification XML file.

Group Weighting

To complicate matters, attributes are grouped. Each group is then given additional weighting. The groups are shown in the table on the next page.

Suggested default values

The table below shows default values for each attribute for the model class person and car. Note that some attributes do not have a maximum specified, but this may be added if required.

These values are the results of careful study of radar data files collected from several sources. It may be that they require further tuning for certain locations.

	Weight	Person (min)	Person (max)	Car (min)	Car (max)
Speed and Acceleration	Critical				
Speed	Critical	0.1	5	2	55
Expected Speed	Critical	0.1	1.3	9	NA
Acceleration	Desirable	0	2	0	4
Weight and Strength	Critical				
Weight	Critical	1	20	30	NA
Strength	Critical	1500	5000	7000	NA
Behaviour	Critical				
Seen Moving	Critical	0.1	NA	1.4	NA
Direction Change	Optional	5		3	

Classification scoring

We have discussed above how 6 tracks (by default, including provisional tracks) make up a classification set. Each track is analysed to see if it's attributes fall within the specified range for each model. Each score is then weighted and totalled over the 6 samples, and expressed as a percentage of the maximum possible. The highest model percentage wins.

Note that the number of samples for Acceleration, Direction Change and Seen Moving are all automatically decreased by one as we require seeing two tracks before we can calculate the values.

It can be deduced from the table in section 3.3 that the maximum score is 825 for 6 samples. This is derived from 5 points from a critical attribute, 3 from a desirable and 1 from an optional, multiple by critical weight for each category, and by 5 or 6 for the number of samples.

5 points per category x (5 points x 5 attributes) x (3 points x 1 attribute) x (1 point x attribute) x 6 samples = 825 points. Note this working doesn't show the distinction between 5 and 6 sample values.

Any classification percentage is therefore results from the actual score against this maximum of 825.

This maximum would change if any of the attributes were deleted or ignored.

Global variables & files

Classification information is modified in two places within witness: Sentinel (and stored in the standard configuration XML file as used by all modules) and a new classification specific configuration file (located in the plugins folder).

ClassificationConfiguration.xml

<MinProbabilityRequired> - defines the % score a track must exceed for any one model in order to be classified.

<Samples> - defines how many tracks are used to determine the model score.

<ExtraSampleIncrement> - defines how many extra samples to add to the classification attempt if the first 6 result in a classification % score less than that specified above.

<DoNotUseProvisionalTracks> - defines whether to use provisional tracks in creating the classification score. Note that TRUE turns off the use of provisional tracks.

Sentinel (stored in Configuration.xml)

<MinClassificationProbabilityForShapes> - defines at which % confidence level the track icons are allowed to be set to a graphical representation of the model. This value is adjustable in Sentinel. You would typically set this to be the same value as MinProbabilityRequired.

Classification as applied to rules

With classification comes the ability to make witness rules more targeted. Each rule now has a classification menu, as below, which allows you to specify if the rule applies to all tracks, or only those classified as a certain type of object.

You may also set a confidence level that the classification has to exceed to trigger the rule. This allows creation of multiple copies of a rule, which trigger based on different confidences of classification (i.e. a warning rule for 50% person and a threat rule for 90% person).

Animals

This section briefly explains why it was not possible to achieve classification values for animals, and persons crawling.

Unambiguous classification relies on models having attributes which are not the same as other models. You can imagine though that a car may travel as slow as a person. A person may change direction in some circumstances, with a turn rate the same as a car.

Critically it was discovered that an animal is indistinguishable from a crawling person using the simple track attributes we have. It is likely that a good model could be reached for an object name 'animal or person crawling', though of course this ambiguity is undesirable in a security system. Furthermore the lowered threshold/plot extraction settings required to confidently detect these objects leads unfortunately to higher false alarms. In the grand scheme of achieving reliable classification, this requirement was therefore omitted.

Appendix 9 - FAQs

The questions answered in this FAQ are as follows:

Q1 - How many bloodhounds do I need?

Each radar needs its own tracker so each radar requires one copy of bloodhound.

Q2 - How many bloodhounds can I install on the same server platform?

This is a complex question and is affected by the following factors:

- **Processing power** - The tracker uses sophisticated algorithms that are processor and memory intensive.
- **Network capacity** - If lots of radars have to send their raw network data to the same server platform then it may exceed the default capacity of the hardware.
- **Radar range** - Radars with greater range will generate more data and therefore more network traffic (see previous factor).
- **Size of tracking area and total number of targets per minute** - Busy sites with lots of movement, i.e. a highway, will generate lots of targets for tracking. This will put a heavy load on the tracker and therefore greater demands on the hardware.

As a guideline we recommend a physical CPU core and 256MB of RAM per tracker*. In addition we recommend using more than one network card should the total radar data exceed 75% of the available bandwidth. See next question for bandwidth planning figures.

* This does not include memory required for the OS or other applications.

Q3 - How many cameras does Witness support?

The number of cameras is unlimited and is in no way related to the number of radars. Practically there is a maximum number that Cyclops can sensiblly control and this is largely dependent on how busy each of the cameras will be. For planning purposes we would recommend working on a maximum of 80 cameras. Other factors do apply, such as the bandwidth and speed required for telemetry and the bandwidth required for the video feeds.

continued

Q4 - What network capacity will bloodhound require?

Bloodhound itself outputs track data. This data is only generated when the tracker is following a target, the amount of data per track is very small (approximately 112bytes per track) so the total requirement is entirely dependent on the number of targets being tracked.

However, Bloodhound consumes raw data from the radar. The amount of data generated by each radar is dependent on its range. For planning purposes you can use these worst case figures**:

- 200m W & I Series: 6Mbps
- 500m W & I Series: 14.5Mbps
- 800m W & I Series: 23Mbps

From this data you can see that four W800 series radars would almost completely saturate a single 100Mbps network interface card.

** Certain modes on the radar can significantly reduce network bandwidth but use of these settings is governed by specific requirements for each site.

Q5 - What bandwidth requirements do the other Witness modules have?

The bandwidth for other modules is governed by the number of targets being tracked. This will increase for busy sites and with each additional radar. The amount of data being sent per target is very small so overall network bandwidth is modest. There is also a certain amount of regular health and status data being sent between modules. Typically the impact of this data can be ignored unless the system is utilising a large number of radars (e.g. greater than 20).

Q6 - Can I install different modules on the same server platform?

Yes. Each module can be installed on separate servers connected via Ethernet or all on the same hardware. Each module will provide a load on the server but this will be largely dependent on how busy the overall system is. Special consideration needs to be given to Bloodhound and Piccadilly - see questions 2,3 and 6.

Q7 - What hardware requirements does Piccadilly have?

Piccadilly is the main server component for whole Witness suite. This means all communication from other models passes through Piccadilly. In addition Piccadilly is capable of recording log and track data to a database. This does provide an overhead which is directly related to the number of targets being processed by the entire system. The key considerations for Piccadilly are as follows:

- **Disk space and access speed** - The speed of the internal database will be affected by hard disk speed. Unlike many database applications, Witness will typically write more information to the database, rather than read. This means good disk speed is important.
- **Memory (RAM)** - Piccadilly holds quite a lot of temporary data in memory and also the database access library requires additional RAM. The more load on the system, the greater the memory use.
- **Network Bandwidth** - Piccadilly deals primarily with target/track data and therefore the bandwidth requirements are not large. However, as the number of radars attached to the system increases so the overall number of tracks will increase.

We would recommend a RAID sub-system for speed and redundancy. In addition, the size of the storage will dictate how much data can be stored. The level at which space is consumed is entirely dependent on the number tracks going into the database. We would also recommend at least 512MB RAM for Piccadilly.

Q8 - Can I install any module on a virtualised server?

Yes, with the exception of Sentinel. Sentinel requires a capable 3D accelerated graphics card which generally excludes the use of virtualised platforms. Also be aware that Cyclops may require serial ports (422/485) to connect to cameras so these will need to be made available through the virtual hardware.

Q9 - Can I install the modules on Windows Server?

Yes, all modules including Sentinel will work on the server OS, but as already mentioned it does require a capable graphics card and the overall responsiveness of Sentinel may be affected if the server is prioritising background processes. The Piccadilly, Bloodhound, Cyclops and Canary services are ideally suited to the server platform.

Q10 - Does Witness have an SDK?

Witness does not have an SDK for integrating code directly into a third party application. However it does have an API which is capable of receiving and generating data as XML over Ethernet. This enables third party software to receive data about tracks and alarms and also to provide commands to affect the behaviour of the software. There is an Interface Control Document (ICD) which outlines the data reports and command instructions. Please contact Navtech Radar for more information.

continued

Q11 - What video encoders does the Witness software support?

At the moment we have built-in support for the Bosch Vipx and VideoJet encoders*. However we are looking to integrate the Axis range of encoders and would be happy to consider other manufacturers, if required.

* Note that the use of Bosch encoders does not limit the system to Bosch cameras. We do not use Bosch protocols and therefore any make of camera, assuming we support the protocol, can be used with a Bosch encoder.

Q12 - Will the Witness software work on a network domain?

Yes. The software will work on a peer-peer network as well as a network domain. Sentinel will utilise the underlying Windows security model and will choose the domain model if the user account is domain-based. If the user account is local then Sentinel will switch to using the local users and groups. Please note that for this reason, the 'Home' editions of Windows are not supported.

Q13 - Does the software support any other sensors?

Yes. Version 1.1 supports the use of simple static sensors such as PIR. This can be connected to Canary via the Advantech Digital IO hardware. Witness will simulate track movement in a pre-defined location if a static sensor is triggered.

Q14 - How many radar sensors will Witness support?

It does depend on the level of activity each radar is expected to monitor, but in an average system we would expect a standard installation to support thirty radars.

Q15 - How many Sentinel clients can be connected to the same Piccadilly server?

A standard installation should support at least fifty Sentinel clients.

Q16 - Why doesn't Bloodhound have a user interface like NS3?

The Witness system is designed to be a modular security and tracking system based on a sophisticated client-server model. It has been designed to run as series of background applications that will operate 24x7 without user interaction. The system is designed to be configured and operated remotely so the UI has been intentionally removed from the tracker. Raw radar data, tracks and configuration data can all be accessed through Sentinel.

Q17 - Can I use wireless data links with Witness?

In certain circumstances – yes. Typically we do not recommend using wireless as a means of connecting the radar to Bloodhound. Other aspects of the software can be connected wirelessly, e.g. Sentinel or Cyclops connecting to Piccadilly.

Using wireless technology exposes a system to a range of issues which a normal wired network would not experience. This varies from bandwidth and latency problems through to interference. Navtech does not provide any direct support for Wireless networks so we recommend using a wireless specialist for installation and support.

Appendix 10 - Computer hardware recommendations

This appendix provides specification recommendations for the computer hardware that is used to host the Witness server and client systems. See also Appendix 9 - FAQs for further details about hardware requirements that are dependant on various aspects of the installation.

Storage

Storage must be suitable for the quantity of data and the length of time it is being stored. This is based on the number of radars and the number of targets being tracked. For example, if the system is recording all track data for two radars monitoring a busy highway then you can expect the database to grow by up to a 1GB a day. The type of storage system should be suitable for the size and required speed of the database and should include hardware redundancy (RAID). Large database installations may require separate hardware platforms with more specialised storage configurations.

Server system specifications

- **Processor**: High speed multicore processor. As a rough guideline, there should be one processor core per copy of the Bloodhound/tracker service running on it.
- **Memory**: 256MB per Witness service running on it. *Note: This does not include the memory requirements of the operating system.*
- **Operating system**: Windows 7 x64 Professional or Windows Server 2008 R2
- **Network connection**: 100Mbps or 1Gbps Ethernet link (require roughly 23Mbps bandwidth per radar sensor).
- **Graphic adapter**: Standard specification.

Typical server configuration for up to 6 radars

- **Processor**: Minimum Intel Core i7 or equivalent CPU @ 3.4GHz. Four cores with eight threads.
- **Memory**: Minimum 8GB RAM.
- **Storage**: Hardware RAID with battery support. RAID 5 configuration with minimum of three SATA hard drives @ 500GB each.
- **Operating system**: Windows 7 x64 Professional or Windows Server 2008 R2
- **Network connection**: 2 x 1Gbps NIC.
- **Graphic adapter**: Standard specification.

Client system specifications (minimum)

- **Processor**: Intel Core i3 or equivalent @ 3.3GHz or above.
- **Memory**: 4GB RAM (with at least 1GB available for Sentinel).
- **Storage**: 30GB HDD minimum.
- **Operating system**: Windows 7 x64 Professional.
- **Network connection**: 1Gbps Ethernet link.
- **Graphic adapter**: Accelerator with support for DirectX 9 or above. 256MB VRAM minimum. Note: CPU integrated Intel HD 3000 or above will suffice.
- **Display**: 1280 x 1024.

Client system specifications (recommended)

- **Processor**: Intel Core i5 or equivalent @ 3.6GHz or above.
- **Memory**: 6GB RAM (with at least 1GB available for Sentinel).
- **Storage**: 30GB HDD minimum.
- **Operating system**: Windows 7 x64 Professional.
- **Network connection**: 1Gbps Ethernet link.
- **Graphic adapter**: Accelerator with support for DirectX 10 or above. 512MB VRAM minimum. Note: CPU integrated Intel HD 4000 or above will suffice.
- **Display**: 1920 x 1080 HD with touch capability.

Appendix 11 - Additional runtime modules required

Various aspects of the Witness Group rely upon redistributable modules. Ensure that each installation has the following modules:

On each system:

- **VC++ 2010 x32 redistributable** - available for download from Microsoft at:

  http://www.microsoft.com/downloads/en/details.aspx?FamilyID=a5c84275-3b97-4ab7-a40d-3802b2af5fc2&displaylang=en

  Note: This is required even on x64 Windows.

- **.NET Framework 4.0** - available for download from Microsoft (comes as standard on Windows 7) at:

  http://msdn.microsoft.com/en-us/netframework/cc378097.aspx

On each system running Sentinel (if required):

- **Bosch SDK redistributable** - included with the Witness software but can also be obtained from Navtech.

When using FLIR cameras:

- **FLIR video player** - included with the Witness software but can also be obtained from Navtech.

When using Pelco cameras:

- **Pelco media player redistributable** - included with the Witness software but can also be obtained from Navtech.

VLC Viewer:

- **VLC player** - included with the Witness software but can also be obtained from Navtech or download from the VLC website at:

  http://www.videolan.org

Appendix 12 - Extending the edit time allowed

In order to prevent any one administrator blocking access to a configuration area for others users, the Piccadilly server enforces a time limit on how long an admin user can keep a section in edit mode. The auto edit timer counts down from when the mouse was last moved or clicked.

Once the time limit is reached, the edit mode for the item that you have open will be terminated, regardless of whether you have saved your changes or not. Therefore, before beginning to create a new installation, you are strongly recommended to increase the default edit time of 15 minutes. You are also recommended to save your changes often.

To change the edit time

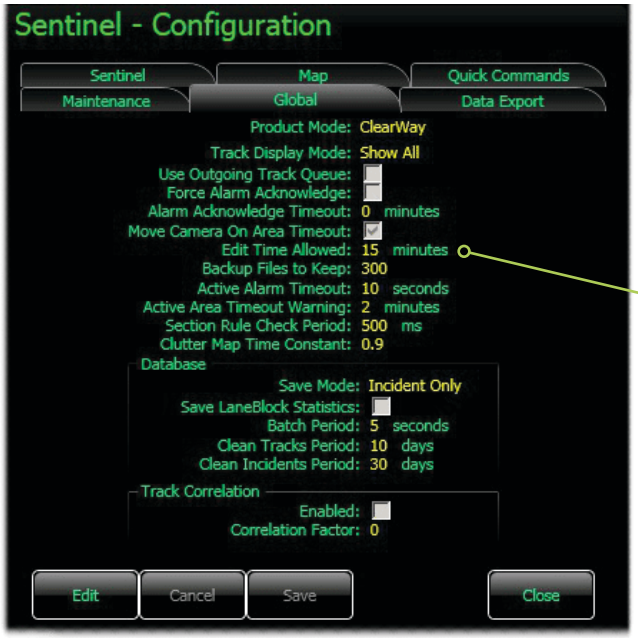
1 In the top left corner of the Sentinel window, click the Navtech logo to reveal the **Main Menu**.

2 Click the **Config** button to display the Sentinel - Configuration page.

3 Click the **Global** tab.

4 Click the **Edit** button.

5 Change the **Edit Time Allowed** option to a suitable level (range is 5 to 60 minutes).



Increase the time limit to lessen the chances of losing your configuration settings.

6 Click **Save** and then **Close** to exit.

For the benefit of other users, remember to restore the setting to a reasonable level once you have completed your edits.

Appendix 13 - Troubleshooting

Issue	Problem	Cause	Suggestions
1	Piccadilly won't start	Security failure	The user account which has been assigned to the Piccadilly service does not have the correct permissions or the password is wrong. a) Check that the service account (normally "Witness") is in the local Windows admin group. b) Check that the password for the Windows user account and the password used on the service match. If necessary renter both.
		Invalid configuration, typically as a result of an incorrect manual edit.	Attempt to identify the invalid XML in the configuration file and correct it. Alternatively rename the current configuration file and allow Piccadilly to create a default config when it starts.
2	Sentinel won't login	Piccadilly has not been started	Check Windows Services and ensure the Piccadilly service has started correctly.
		The IP address is incorrect	Ensure the server address entered in Sentinel login dialog matches the IP address of Piccadilly.
		Piccadilly is not listening on an external interface	When trying to connect Sentinel from a separate PC, Piccadilly must be configured to use an accessible interface and IP address. "localhost" should NOT be used.
		No network connection	The PC running Sentinel must be able to physically connect to the Piccadilly server PC. If the network allows ICMP traffic, try to ping the Piccadilly server PC to verify the connection.
		Firewall or other security software is blocking the connection	Ensure that the security software on the Piccadilly server PC is not blocking the Sentinel application. If using Windows Vista or 7 we recommend UAC is switched off.
3	Pressing Ctrl+Alt+F5 in Sentinel has no effect	Another software application is using the same combination.	Disabled this key combination in the other software application. The most common is the Intel Graphics control software. This uses Hot Keys and by default one of the keys is configured to use Ctrl+Alt+F5. These Hot Keys can be disabled or re-configured.
4	Bloodhound, Cyclops or Canary modules won't connect to Piccadilly	Piccadilly has not been started	Check Windows Services and ensure the Piccadilly service has started correctly.
		The IP address is incorrect	Ensure the server address entered during the Witness installation is still valid. You can check which IP address a module, such as Cyclops, is using by looking at the service in the Windows Service Manager.
		Piccadilly is not listening on an external interface	When trying to connect a module which is installed on different separate PC to Piccadilly, Piccadilly must be configured to use an accessible interface and IP address. "localhost" should NOT be used.
		No network connection	The PC running the modules must be able to physically connect to the Piccadilly server PC. If the network allows ICMP traffic, try to ping the Piccadilly server PC to verify the connection.

		Firewall or other security software is blocking the connection	Ensure that the security software on the Piccadilly server PC is not blocking the other modules. If using Windows Vista or 7 we recommend UAC is switched off.
5	Bloodhound won't connect to the radar	Incorrect IP address	Check that the IP address for radar is correctly entered in the tracker settings.
		Another software client is already connected to the radar	The radar only supports a single connection. Bloodhound will continue to try and connect to a radar even if another client is connected. Once that client is closed, Bloodhound should connect successfully.
		Bad data from the radar	In some circumstances the radar may output incomplete data packets. Typically this only happens after a configuration change. The most appropriate action is to hard reset the radar.
6	A camera won't move when you right click in Sentinel	Incorrect camera model	Check the model on the camera configuration settings is correct.
		Camera is not in the correct behaviour group	The camera must be in a valid behaviour group. If it is in the default behaviour group then the camera will not operate correctly. Move it to either the "Closest" or "Timeshare" groups or create a custom group.
		Camera is not in a valid connection group	If the camera is the "No Connection" group then the camera will not function. A valid connection group must be created which is appropriate for the type of connection (i.e. Vipx).
		Cyclops is not running	Check Windows Services and ensure the Cyclops service has started correctly.
		Incorrect Camera Id	On analogue cameras that connect via RS485/422 each camera that shares a serial link must have a unique comms id. This is typically set on the camera hardware but the same id must also be included within the Witness camera settings.
7	A camera won't zoom or the zoom is incorrect	Incorrect camera model	Check the model on the camera configuration settings is correct.
		Incorrect zoom values	The camera (or the specific lens type) has not been calibrated so the zoom coefficients are wrong. The camera needs to be properly zoom calibrated.
8	Radar data is not visible in Sentinel	Bloodhound is not connected to the radar	Ensure Bloodhound has connected successfully to the radar.

Appendix 14 - Radio frequency energy statement

FCC compliance statement (United States)

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, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

The operation of this device is limited to a fixed position at airport locations for foreign object debris detection on runways and for monitoring aircraft as well as service vehicles on taxiways and other airport vehicle service areas that have no public vehicle access. This equipment must be mounted in a fixed location maintaining a minimum separation distance of 46cm from personnel when in general operation. This restriction of operation is specific for use in North America. For use in other regions aligned to the FCC regulations, specific country restrictions should be reviewed.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Index