IntrusionTrace™

Best practices

Getting the most from IntrusionTrace™ — Video Analytic for Intelligent Perimeter Detection

User Guide

Honeywell

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Honeywell. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Honeywell.

Trade Name Statement

ADPRO, Xchange, FastTrace, iFT, eFT, iFT-E, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Honeywell. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Honeywell is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Honeywell accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Honeywell.

Honeywell is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Honeywell or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Honeywell in relation to the products is limited to:

(i) in the case of services, the cost of having the services supplied again; or

(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Honeywell harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

www.security.honeywell.com

TABLE OF CONTENTS

Chapter 1 - Best practices 1

Overview 1
- Careful setup 1
- Advanced settings 2

Designing for analytics 2
- Camera views 2
- Lighting 3
- Rain 4

Preventing issues through careful setup 4
- Calibration 5
- Detection areas 6

Resolving issues using directional areas 8

Resolving issues using advanced settings 9
- Small animals 12
- Snow and rain 13
- Sweeping headlights 15
- Shadows and lights from adjacent roads 16
- Mask areas 18
- Moving foliage and its shadows 19
- Spiders, webs, and insects 21
- Cloud shadows and thermal noise 22
- Double knock solutions on ADPRO platforms 24

Warning 26

CHAPTER

1 BEST PRACTICES

IntrusionTrace is designed to detect professional intruders who are intent on entering premises undetected. As such, the default settings of the video analytics were chosen to meet this requirement over a wide range of environmental, seasonal, day/night conditions, and to ignore false alarms from small animals. However, not every site is the same, and the suggestions outlined in this document aim to guide users with specific circumstances to modify/calibrate the settings to achieve reliable, superior detection and very low false alarm rates.

The following situations are the ones that occur most often and proper setup and use of IntrusionTrace can provide customers with a video detection and verification system that will prevent damage and/or loss to facilities.

The first part of this document looks at careful setup to ensure the best results from IntrusionTrace. The second part looks at the advanced settings, and shows how these can be adjusted to tackle more difficult problems.

Overview

Careful setup

The following are the IntrusionTrace setup recommendations:

Consideration	Recommendation
View	Up to 30m horizontal field of view at maximum detection distance (50m for thermal) Up to 75m maximum detection distance measured from camera (125m for thermal) Top of the scene excludes the sky The target height evident at the nearest detection distance (not aerial view) The target head and feet move up the screen as the target moves away
Lighting	Away from the camera (1.8m below camera is ideal) Not pointing at the camera Good, even illumination day and night
Calibration	The target height at the nearest point of detection The target height at the furthest point of detection The whole target must be visible for calibration (feet and head)

Consideration	Recommendation
Detection Area	On the ground – only the feet of targets are tracked Flush with bottom edge of image to catch targets on the edge

Advanced settings

Use the following recommendations based on your need:

Issue	Solution
Small Animals	Increase minimum height (eg 0.7m) Increase minimum area (eg 0.3 sq. m)
Snow and Rain	Faster shutter speed (camera setting) Reduce maximum speed (eg 7m/s) Increase minimum time (eg to 1s)
Sweeping Headlights Across Scene	Increase minimum time (eg 5s for car sales-yard application) Consider using a thermal camera
Adjacent Roadway	Use a directional area directed perpendicular to the roadway. Consider using a thermal camera
Moving Foliage and Shadows	Increase minimum distance (eg 3m) Reduce maximum speed (eg 7m/s) Use a lower contrast sensitivity for subtle shadows and movement Double knock detection area events
Spiders, Webs, and Insects	Get rid of the spider and its web with regular maintenance Don't use ring lighting on the camera (attracts insects) Use a directional area to reduce the frequency of false alarms Use a lower object sensitivity
Adjacent Movement Joins up with Target Movement	Move detection area away from the boundary Use mask areas, but leave minimum target height between bottom of mask and top of detection area so that targets are not truncated.

Designing for analytics

It is commonly believed that video analytics will work well with any site design. However, poor placement of cameras and lighting are significant causes of false alarms and missed detections for all video analytics products. Video analytic solutions are flexible and very effective, but good results require good site designs.

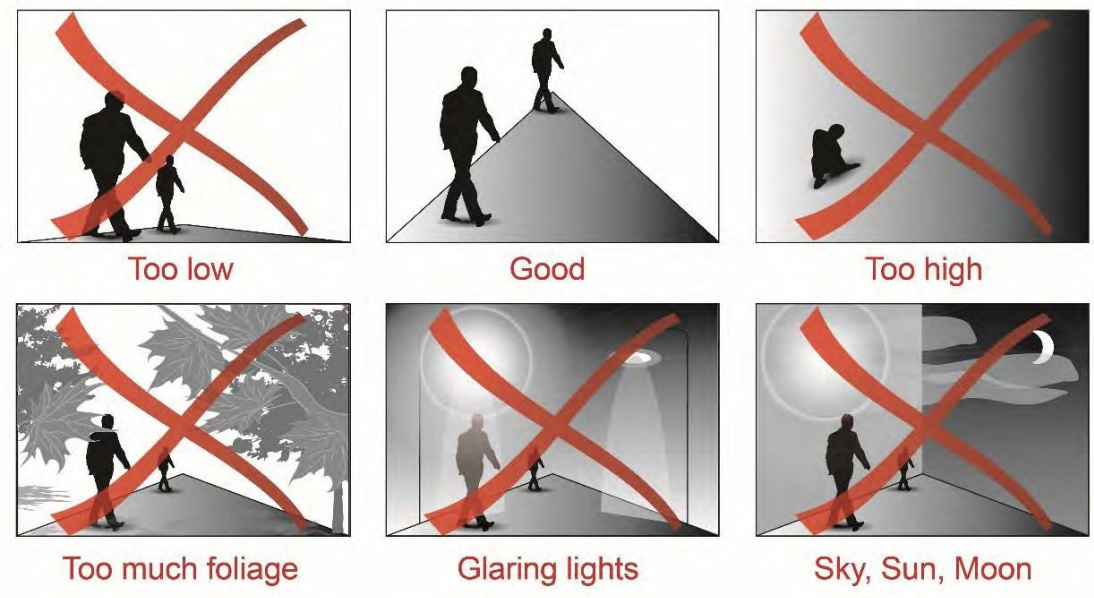
Camera views

The diagrams below show key issues to be aware of when mounting cameras. None of these prevent video analytics from being used, but it is important to understand the implications of each.

- If too low then movement towards or away from the camera is barely visible and cannot be detected.
- If the camera angle is too steep then height cannot be used to ignore small animals.

- Significant amounts of moving foliage or shadows can cause false alarms and should be avoided.
- Bright lights in the view can shut down the camera iris reducing visibility and detection performance.
- The sun and moon can be bright enough to blind a camera at certain times of the day.

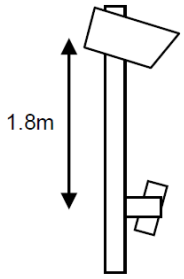
Keep in mind that the view needs to be suitable 24 hours a day throughout all seasons.



Camera placement considerations

Lighting

Except where thermal cameras are used, good lighting night and day is essential for reliable analytics. The best position for lighting is 1.8m below the camera so that insects from the ground do not pass the camera on the way to the light source. Camera mounted lights such as ring-lights should be avoided because they will attract insects and spiders and cause strong, bright reflections of nearby rain and insects. These situations will shut down the iris of the camera and decrease both the visibility and detection sensitivity.

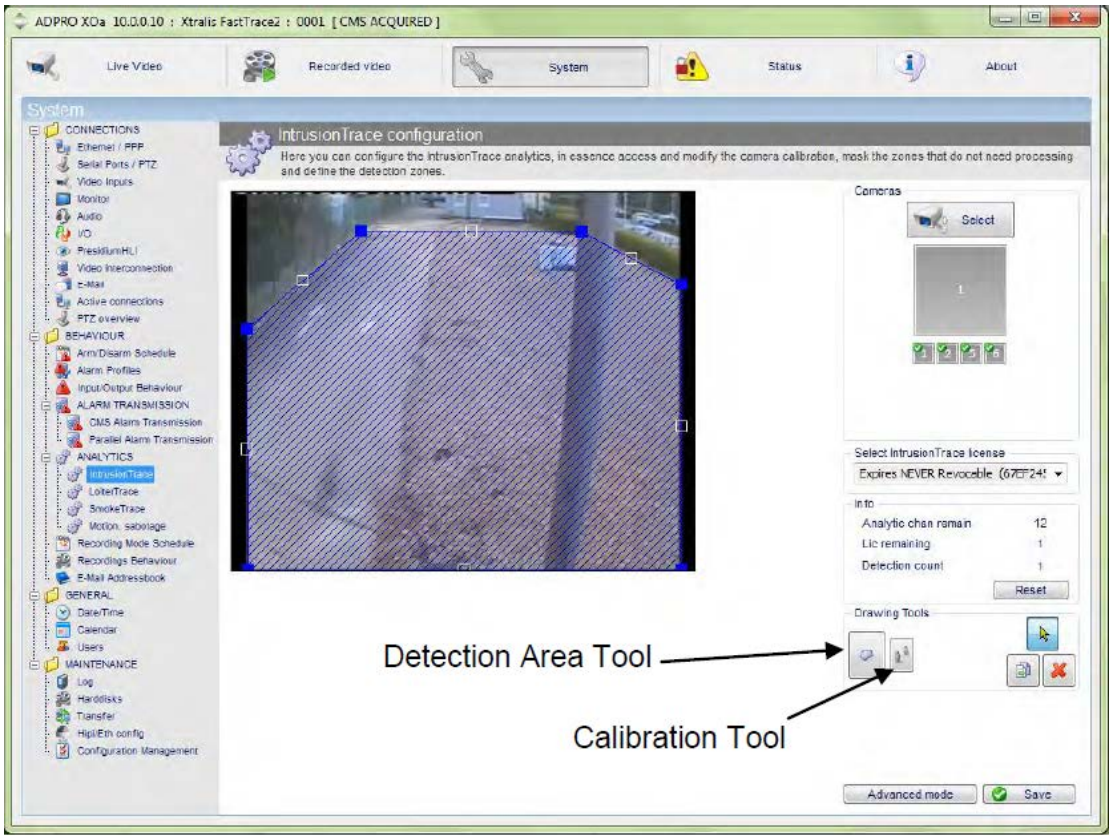


Rain

Raindrops on the camera lens reduce visibility and can refract nearby lights into the camera view. As many cameras come with inadequate rain hoods, they should be sheltered from the rain, or installed with well designed hoods that deflect raindrops away from the lenses in all weather conditions. Long lens hoods are effective and are commonly seen on motorway surveillance cameras for this reason.

Preventing issues through careful setup

When commissioning IntrusionTrace the installer is required to calibrate the scene and define detection areas. These steps must be done carefully to ensure reliable detection and low false alarm rate. When first adjusting a channel the simple mode screen is presented, as shown below, and the detection area and calibration tools are available through buttons as indicated. This is the default mode of operation and uses default parameters for target size and speed that are sufficient for most needs.

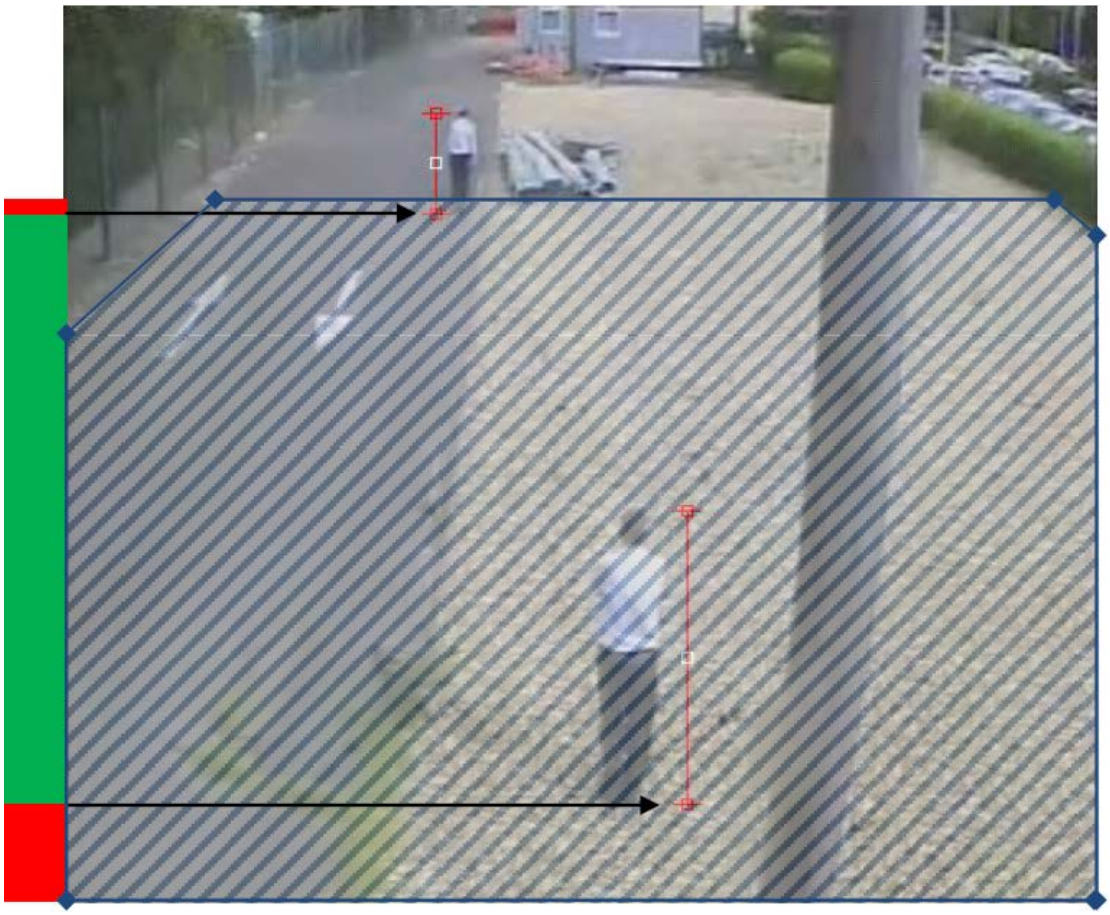


Simple Mode Screen

Calibration

Calibration determines the system's perception of object size in the scene. The height cursors must accurately represent the specified height at the nearest and furthest distances you wish to detect at. Speed and size calculations in the areas closer and further than these distances (the red bars below) are less accurate, and can lead to false alarms and missed targets there. Correct calibration will eliminate many false alarms and allow reliable detection as intended.

Poor calibration



Good calibration

Detection areas

Detection areas can be viewed as ground hugging carpets that are spread where intruders are to be detected. Since only the bottoms of the targets are tracked, the detection areas do not need to extend up the sides of buildings or fences. However, they do need to be flush with the bottom of the image if targets crossing there are to be detected, and they must be placed carefully to detect only what is intended. Each channel of IntrusionTrace supports multiple detection areas giving the installer significant flexibility.

Detection area does not need to cover the fence

Poorly placed bottom edge misses foreground targets

Poor detection area placement

Detection area only needs to cover the ground

Flush with bottom so foreground targets are not missed

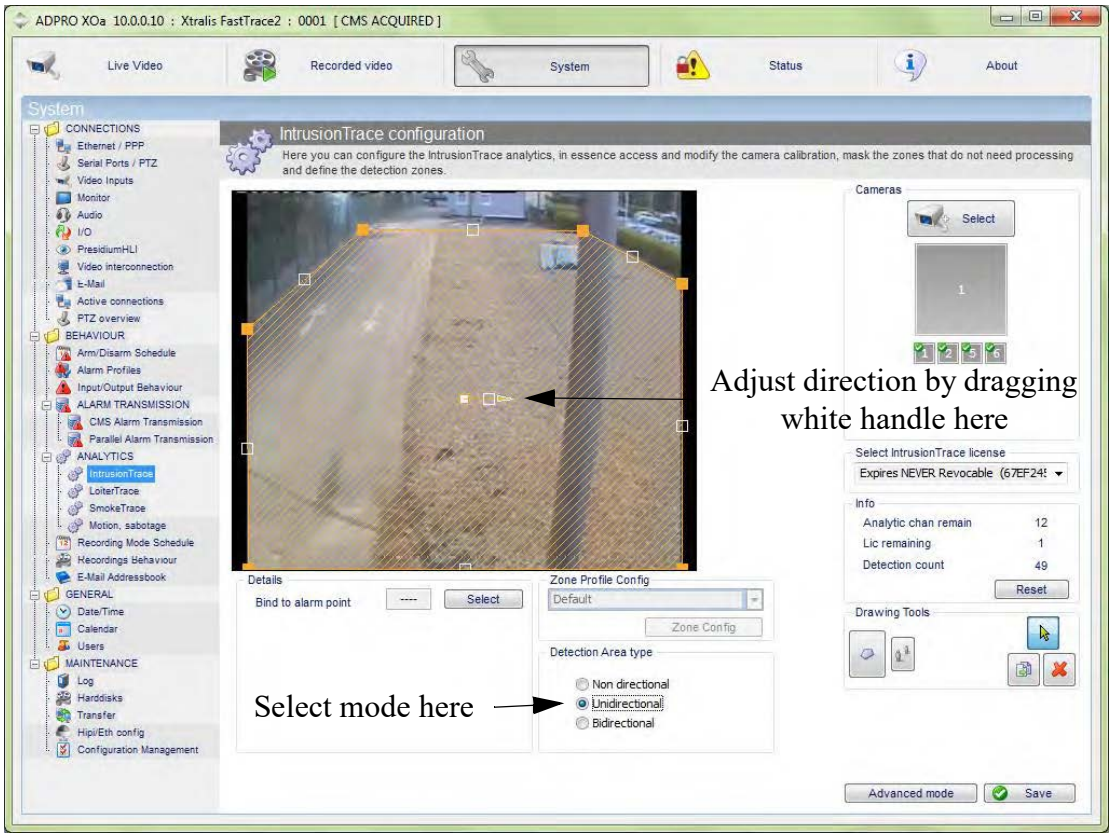
Good detection area placement

Resolving issues using directional areas

Detection areas in IntrusionTrace can be made directionally sensitive. The detection area will then only trigger when a target has gone sufficient distance in the direction selected. This feature is useful for eliminating false alarms that come from known directions. It also reduces the frequency of false alarms from random movement since many of these movements will not travel sufficiently far in the direction selected.

A directional area is created by first drawing a detection area in the normal way then selecting it, and choosing whether the area is to be unidirectional, bidirectional, or non-directional. If a directional mode is selected, then the direction can be set by dragging the white handle on the highlighted arrow on the detection area as shown below. The minimum distance that a target must travel in this direction is set by the minimum distance setting in the advanced parameters. By default, and in the simple mode, this is set at 2m.

Note that the directional sensitivity can be set independently for each of the detection areas in a channel. It is not uncommon to use several detection areas in a scene with some having directional sensitivity, and others being non-directional.

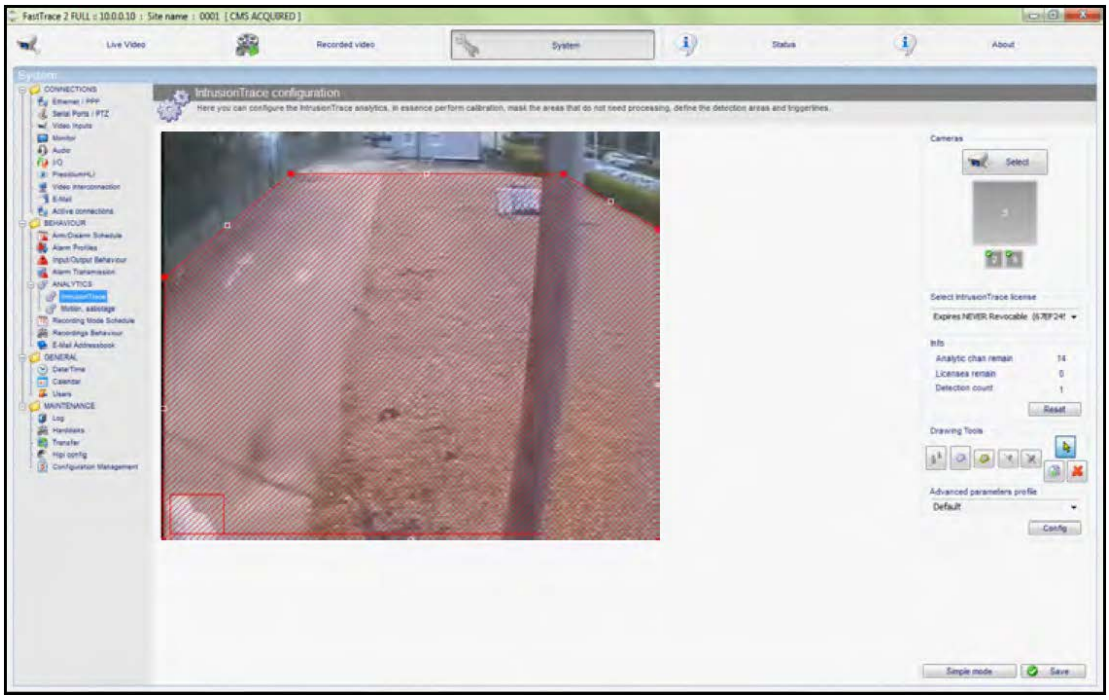


Setting directional areas

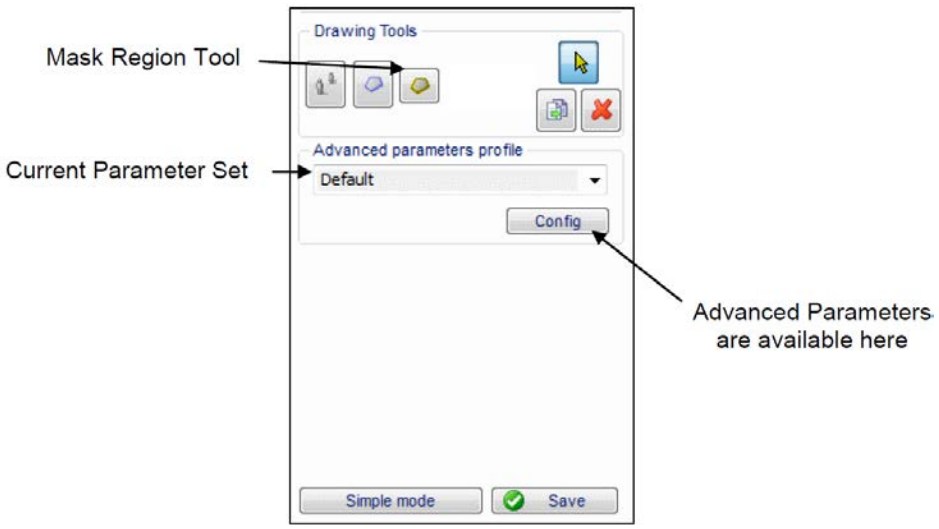
Resolving issues using advanced settings

IntrusionTrace has been designed for outdoor use and has default parameters chosen to meet most needs. However, every site is different, and there are many intuitive parameters available to the user for fine tuning its performance. If making any adjustments, be aware of what trade-offs are being made.

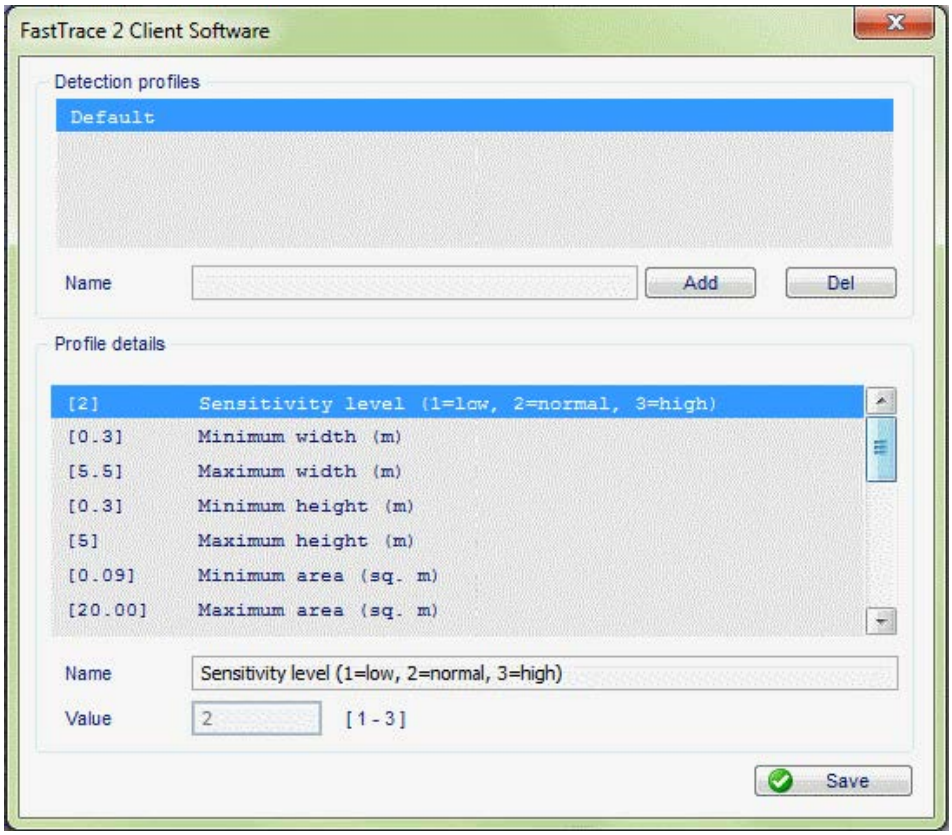
The advanced settings are available when the Advanced Mode button is clicked at the bottom of the Simple Mode page. The Advanced Mode page is shown below along with the tool bar it supports. The advanced settings can be viewed and edited by clicking on the Config button. The available settings are also shown below.



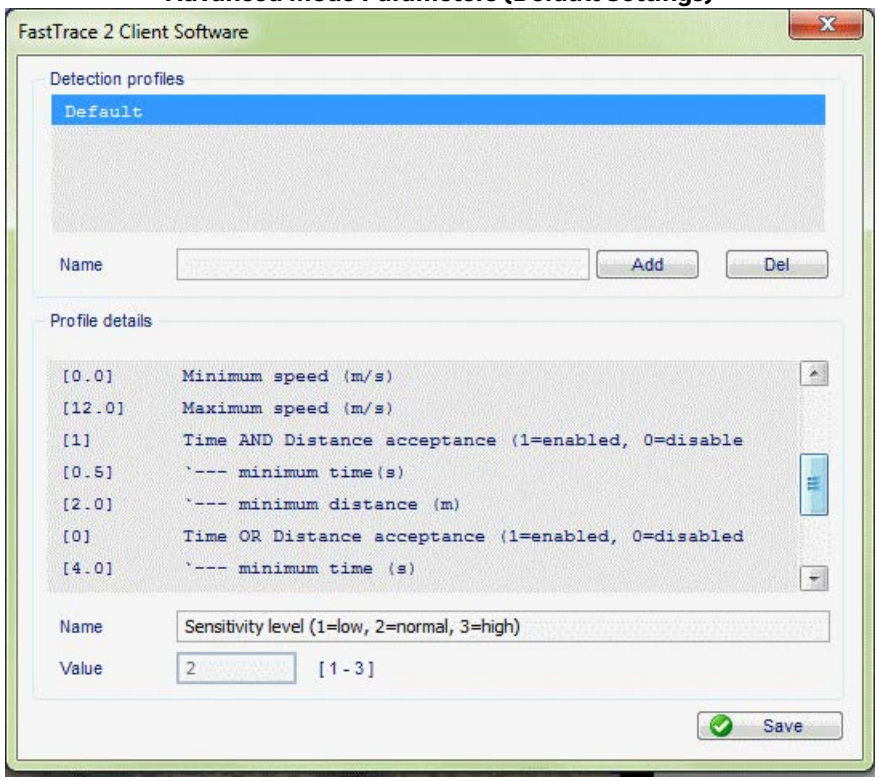
Advanced mode screen



Advanced mode tools

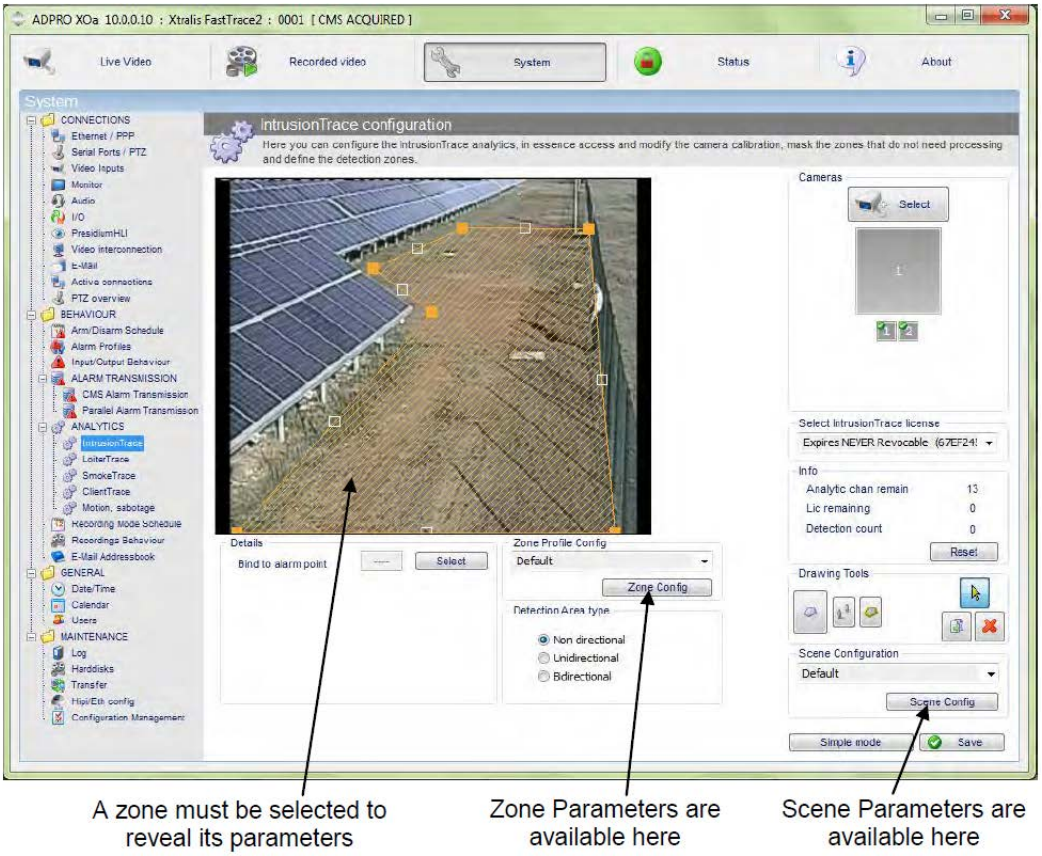


Advanced Mode Parameters (Default Settings)

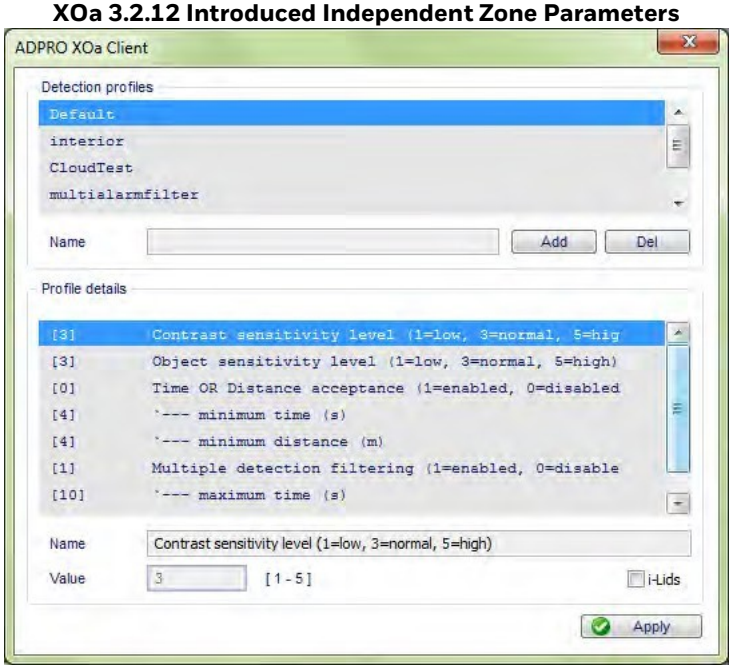


Advanced Mode Parameters (Default Settings) – continued

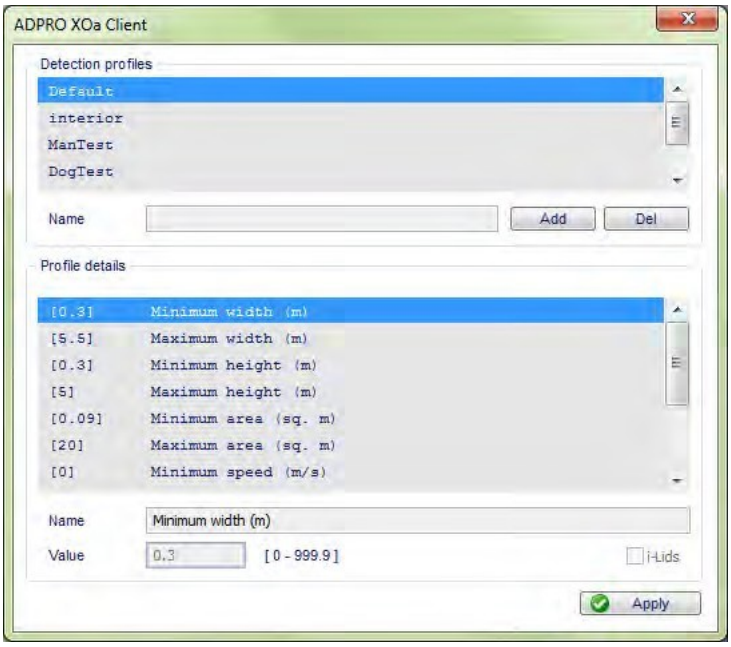
Since XOa 3.2.12 the advanced parameters have been split into detection zone parameters and scene parameters. This allows different parameters to be used for each zone and provides considerable flexibility. The zone parameters become visible when you select the zone you wish to adjust, as shown below.



XOa 3.2.12 Introduced Independent Zone Parameters



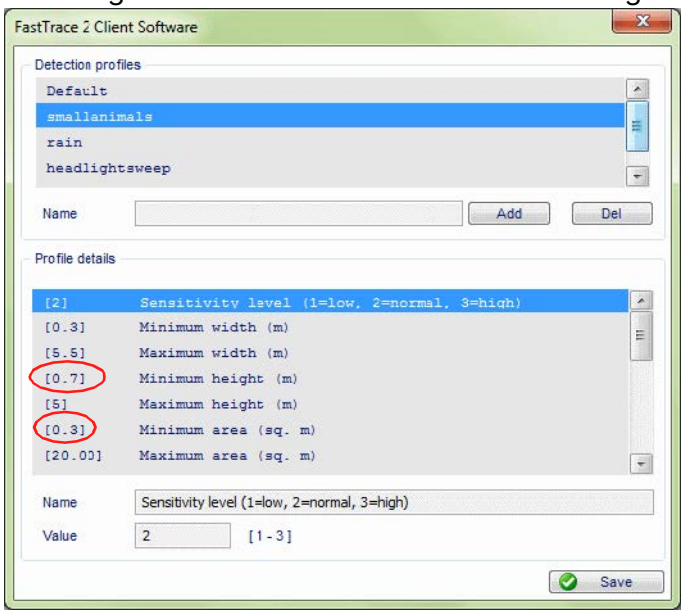
The multiple alarm, sensitivity and time OR distance filters, apply to the whole scene



The size, speed, and the distance AND time filter, apply only to the 'selected' zone

Small animals

If small animals are being detected as false alarms, the simplest solution is to increase the minimum height and/or area to be bigger than the largest animal you wish to ignore. However it also needs to be no smaller than the smallest form of any intruder that needs to be detected. For example, 0.7m minimum height may be suitable if crawling and rolling intruders are unlikely. To provide more discrimination, consider using the minimum area. A minimum height of 0.3m and a minimum area of 0.3 sq. m would mean that a 0.3m high target must be 1m wide before it will be detected. This could ignore small animals but not a crawling man.



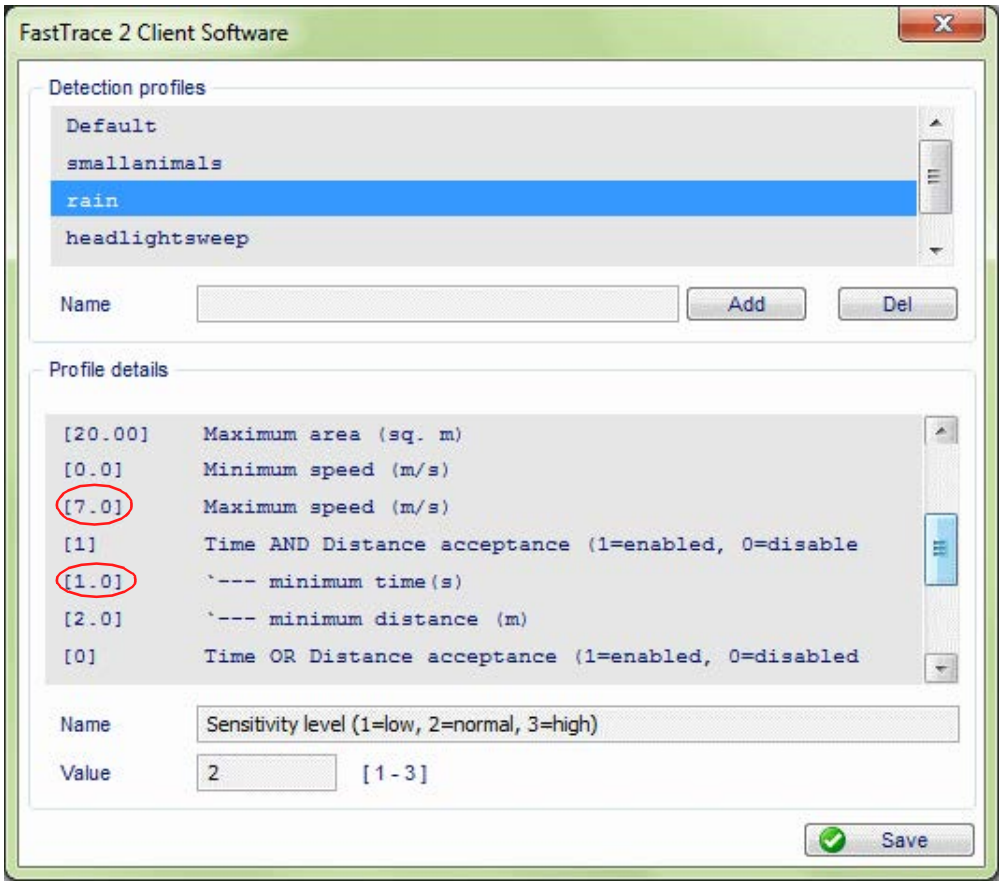
Advanced settings for better small animal filtering

Example showing man detected while dog is ignored

Snow and rain

If snow and rain are being detected, perhaps due to camera mounted lighting, then it is likely that the shutter speed of the camera is not fast enough. Selecting a faster shutter speed on the camera will reduce blur and make the rain drops and snow smaller, which can often eliminate the problem.

If issues persist then reducing the maximum speed (eg to 7.0m/s) or increasing the minimum time (eg to 1 or 2 seconds) can help. The trade-off is that if the speed is made too small or the minimum time too large then fast moving intruders and vehicles may not be detected. The approach taken will depend on the site needs.



Advanced settings for rain and snow filtering

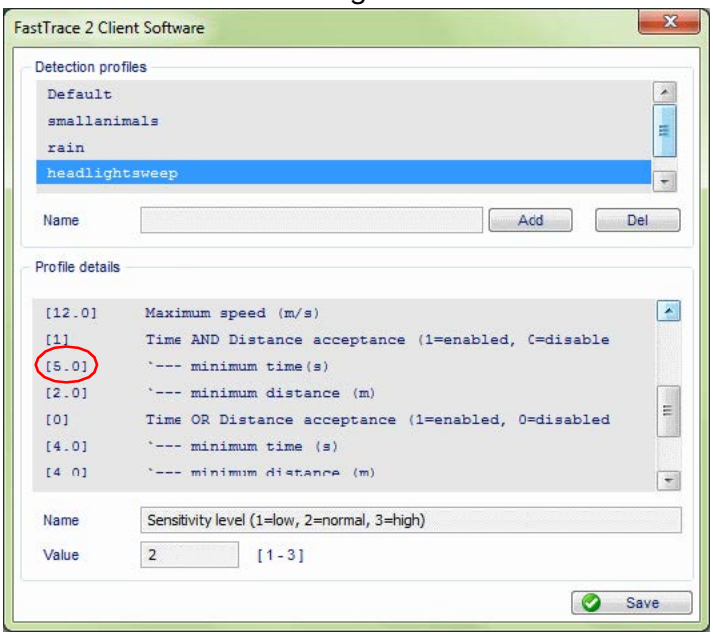
Example of snow being ignored

Sweeping headlights

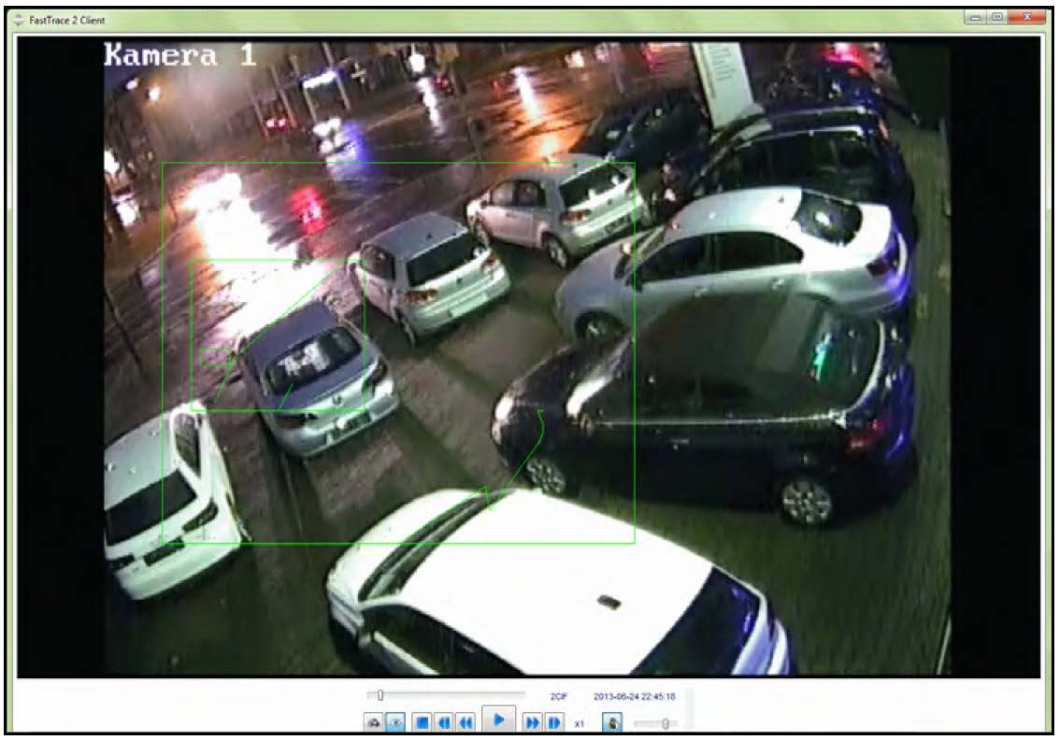
Headlights that sweep through the scene are common in some city applications such as car sales yards. In these applications, it may be acceptable to increase the minimum time to a value greater than the time it takes for headlights to sweep the scene, and less than the time that an intruder would remain in view. A value of 5 seconds has been used successfully but be aware that larger times will require the intruder to remain in view longer before an alarm is raised. It is therefore more suitable for wider fields of view and wide detection areas than for narrow scenes and narrow detection areas.

With XOa 3.2.12, it is possible to have one set of settings for detection areas near the road and affected by headlights, and other sets of settings for other detection areas further from the road that are not affected. This graduated response may be useful in some scenes.

As a third possibility, it should be noted that IntrusionTrace supports thermal cameras and these are not sensitive to headlight beams.



Advanced settings for sweeping headlight filtering



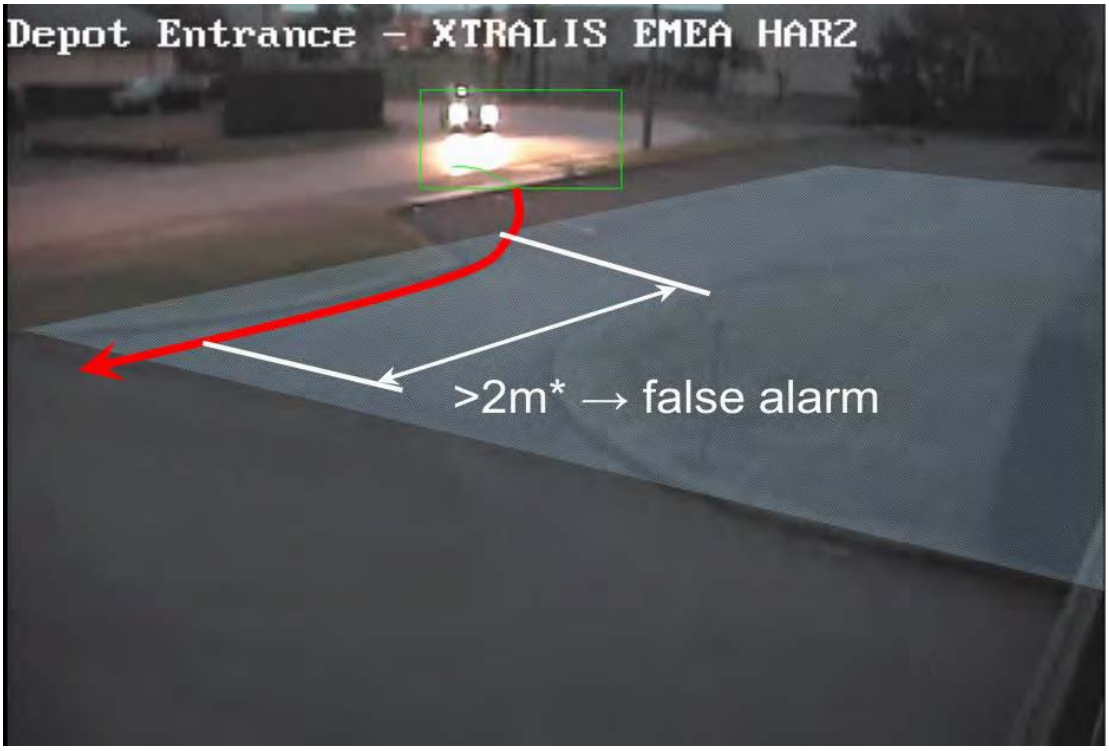
Example of headlights being ignored

Shadows and lights from adjacent roads

Often a site is adjacent to a road and vehicle or pedestrian shadows may extend into the site's detection area and cause false alarms. One solution to this is to move the detection area away from the road, and to set its direction sensitivity at right angles to the road. As the vehicle shadows or lights travel parallel to the road, they do not move far enough in the direction of interest to cause an alarm, but an intruder that enters and approaches the property will travel far enough to be detected.

Note that more than one zone can be used and some can be made directional while others, perhaps nearer the protected structure, could be non-directional. This can provide a graduated response that may be appropriate in some applications.

It should also be noted that IntrusionTrace supports thermal cameras and these are not sensitive to headlight beams.



Example of a car headlight entering the detection area

The use of a directional area to filter these false alarms where 2m is set by the minimum distance setting in the advanced configuration

Mask areas

Mask areas are often over-used. Detections will only occur where the bottom of the target is in the detection area, so it is usually not necessary to mask out the remainder of the image. However, masks can separate unwanted detections from wanted detections where the combined bounding box is too large to be detected. They can also reduce the sizes of detected objects to less than the minimum size to prevent them being detected, or to prevent the bottom edges of neighboring bounding boxes extending into the detection area.

The example below shows how a car and pedestrians combine and are too large to be detected, but with careful masking, the pedestrians are detected reliably. Here a gap taller than the minimum target height has been left above the detection area so that targets at the edge of the area can be detected correctly.

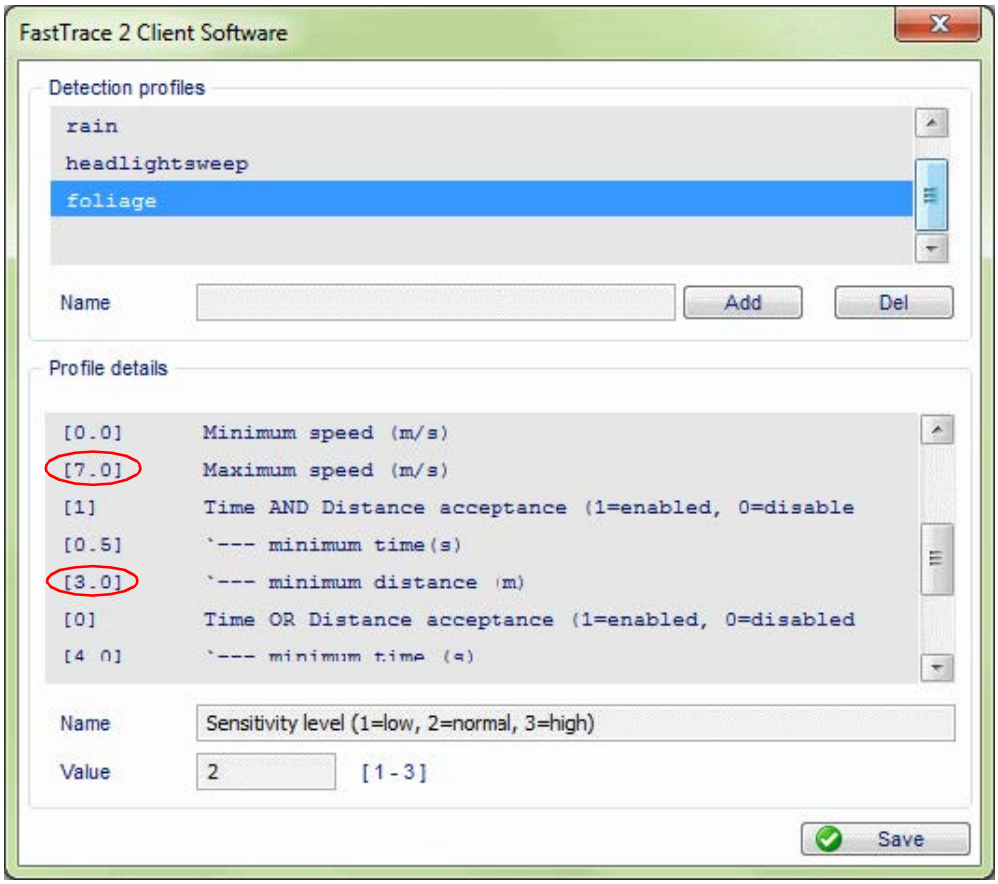
Traffic interfering with pedestrian detection

Effective masking of traffic

Moving foliage and its shadows

IntrusionTrace is designed to operate with sterile zones where movement is not expected. Frequent movement of animals, people, vehicles, foliage and shadows throughout a scene can decrease the system sensitivity, so scenes like this are not recommended when using IntrusionTrace with visible light cameras. However the likelihood of false alarms can be reduced by increasing the minimum distance (eg to 3m) and/or reducing the maximum speed (eg to 7m/s), and/or by using a directional area. Double-knocking, or triple- knocking multiple zones may also provide a solution.

A more effective solution, if detection is required in areas where there are moving shadows, may be to consider thermal cameras. As these are only sensitive to thermal radiation, moving shadows are less likely to be an issue.



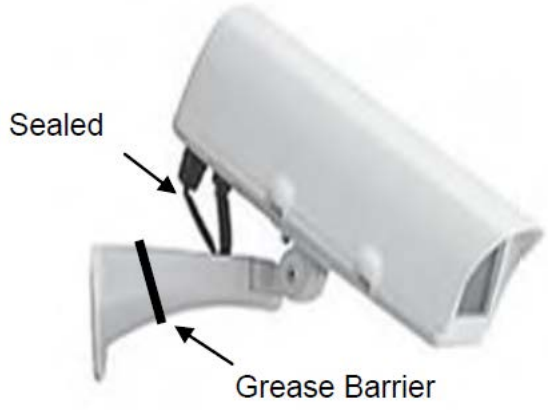
Advanced settings for moving foliage suppression

Example of a non-sterile zone where these settings may help a little

Spiders, webs, and insects

Because spiders and insects can crawl or fly anywhere across the field of view, at any speed, for short or long periods of time, and webs are frequently re-spun in different locations, changing size and speed parameters will not permanently prevent false alarms from these causes. Directional areas can help reduce the frequency of alarms because not all spider movement will be in the direction the area is sensitive to. However, the best solution is to remove the spiders and to position lighting away from the camera to attract insects elsewhere. Regular cleaning of the camera and housing can help reduce the problem, and creating a barrier on the camera housing with a bead of grease or petroleum jelly to prevent new spiders from reaching the lens area may work. However this will need to be reapplied at regular intervals.

Example of a spider being detected



Possible solution using a grease barrier

Since XOa 3.2.12 the new “Object Sensitivity” parameter can be used. Reducing it from its default level 3 to level 2 can reduce false alarms from clearly visible spiders like the one below. Because the legs and shape vary as this spider moves across the scene it appears less like a consistent object and can be filtered out by the lower setting. Targets such as people walking are more consistent and continue to be detected.

Object Sensitivity 3 – Spider is Detected

Object Sensitivity 2 – Spider is Ignored

Cloud shadows and thermal noise

In some scenes subtle intensity variations that are difficult to detect with the naked eye may be detected by IntrusionTrace. Examples include shadows of moving clouds, and subtle thermal variations across areas of grass (when using thermal cameras). Since XOa 3.2.12 the new “Contrast Sensitivity” parameter can be used to address these issues. Reducing the level from the default of 3 to a level of 2 has been found to be effective as shown in the example below. Note that the Contrast Sensitivity determines what objects are tracked. A green bounding box will not appear around an object, or any subtle intensity change, if the Contrast Sensitivity is too low for that target. This feedback can be useful to determine the optimum setting.

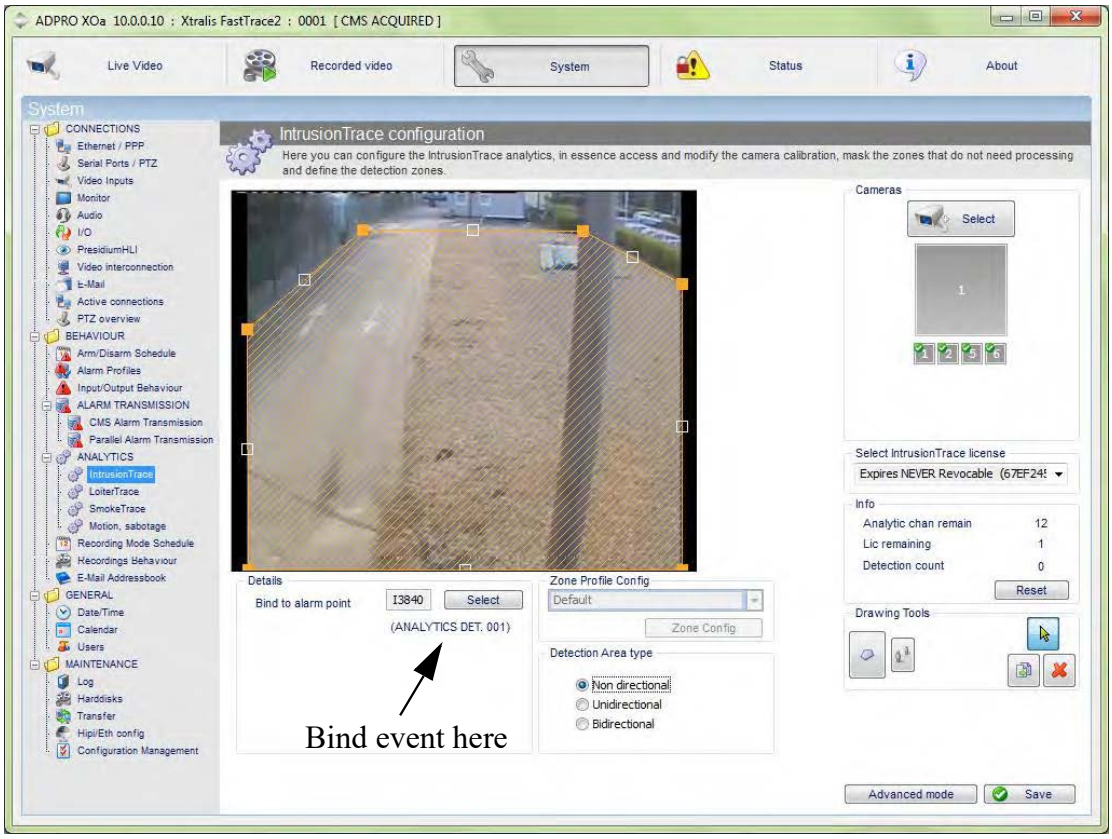
Contrast Sensitivity 3 – Cloud is Detected

Contrast Sensitivity 2 – Cloud is Ignored

Double knock solutions on ADPRO platforms

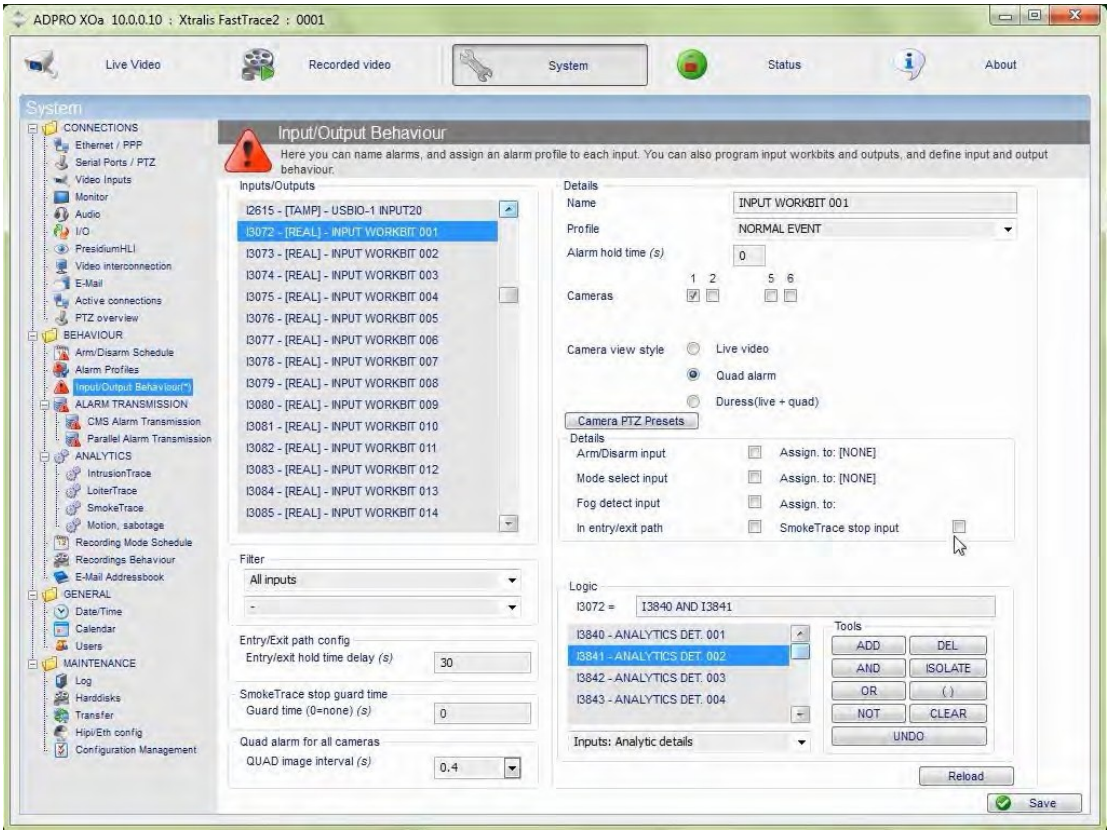
The ADPRO FastTrace2/2X/2E and iFT/iFTE platforms run XOa firmware which provides an Input/Output Behaviour setup for defining how events are processed. This can be used to implement double-knock or higher levels of advanced logic between zones and/or external sensors, and provides a powerful way to control what generates an alarm.

IntrusionTrace on XOa supports up to sixteen zones per channel, and each of these zones can be bound to a unique “analytics detection” event. To double-knock zones they must first be selected and then bound to different events using the bind button as shown in the screenshot below.



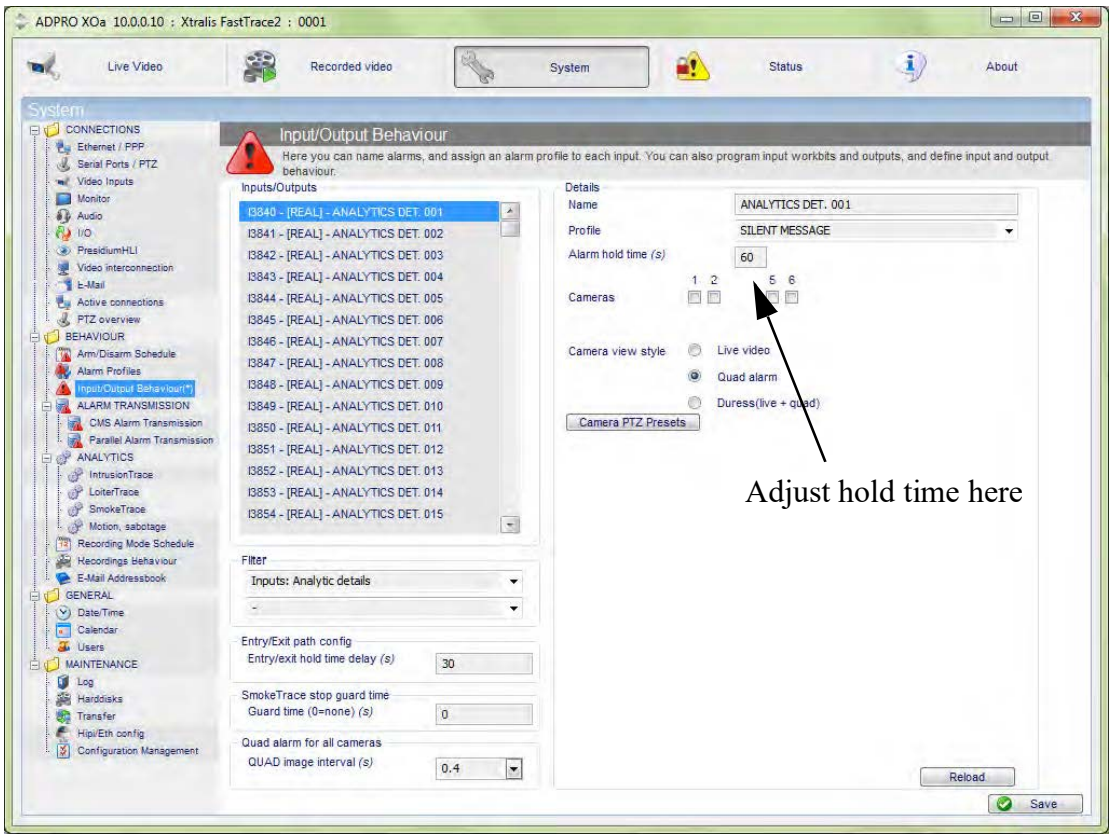
Example showing the selected zone bound to Analytics Detection event 001

The I/O Behaviour page can then be used to program a “Workbit” to be the logical AND of the two bound events from the two zones. That Workbit may then be programmed to generate a “Normal Alarm” with quad display of a selected camera in the same way that other events can be reported. Note that the Perimeter event for this camera should be set to Silent Alarm so that it does not generate alarms for each of the double-knock zones – this will ensure that only the double-knock alarm is sent.



Example showing Input Workbit 1 set to produce a Quad Alarm on Camera 1 when the Analytics Events 001 and 002 occur together.

When double-knocking two non-overlapping zones it may be necessary to hold the duration of each detection to ensure they overlap in time as the target moves from one zone to another. This can be achieved by setting the hold time for each of the detection events. For example, if each hold time is set to 60 seconds, then an intruder that is detected by both zones within 60 seconds will generate the double-knock event. Setting the hold time is done on the I/O Behaviour page as shown below.



Example showing the hold time for Analytics Detection event 001 being set to 60s

Warning

With careful and accurate installation, set-up and calibration, IntrusionTrace can provide low false alarm rates and highly reliable detection capabilities. While carefully calibrated settings can ensure better protection at your site, we encourage all users to read the documentation in its entirety, participate in the Xtralis training courses, consult our technical support staff and consider your site requirements carefully prior to making a change to the settings. All settings have trade-offs, and it is important to implement the proper settings that are best for your site and needs.

www.security.honeywell.com