ADPRO® IntrusionTrace

Technical Manual

For FastTrace 2 Series and iFT Series

March 2017
Doc. 26472_02
Software version XO 4.00

ADPRO®
by xtralis®

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 Xtralis. 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 Xtralis.

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 Xtralis. 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. Xtralis 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 Xtralis 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 Xtralis.

Xtralis 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 Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis 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 Xtralis 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.

Document Conventions

The following typographic conventions are used in this document.

Convention	Description
Bold	Used to denote: emphasis Used for names of menus, menu options, toolbar buttons
Italics	Used to denote: references to other parts of this document or other documents. Used for the result of an action

The following icons are used in this document.

Icon	Description
ℹ	Note. This icon indicates information of special interest that will help the reader make full use of the product, optimise performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data.
!	Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details.
⚠	Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury.
⚡	Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury.
⚠	Warning! This icon indicates that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

Trade Name Statement

Xtralis, the Xtralis logo, The Sooner You Know, VESDA-E, VESDA, ICAM, ECO, OSID, HeiTel, ADPRO, IntrusionTrace, LoiterTrace, ClientTrace, SmokeTrace, XOa, XOh, iTrace, iCommand, iRespond, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Xtralis 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.

Contact Us

UK and Europe +44 1442 242 330 **D-A-CH** +49 431 23284 1 **The Americas** +1 781 740 2223

Middle East +962 6 588 5622 **Asia** +86 21 5240 0077 **Australia and New Zealand** +61 3 9936 7000

www.xtralis.com

Contents

1 Introduction

1.1 About IntrusionTrace

The Xtralis® IntrusionTrace™ application is designed to provide full outdoor perimeter detection analytics. IntrusionTrace is available as an add-on application to the Xtralis XO/XOh software that runs on the Xtralis Remotely Managed Multiservice Gateways (RMGs)[1].

It provides reliable and predictable detection of intrusion into secure outdoor areas. The system analyses images from strategically placed cameras to detect 'human-like'[2] movement, and if the movement fulfils a number of criteria, the system generates alarms. The RMG handles these alarms and can transmit them to a remote central monitoring station.

1.2 Purpose

The purpose of this Technical Manual is to describe the configuration of the IntrusionTrace application in the ADPRO XO client software for the ADPRO FastTrace 2 Series and iFT Series devices. The recommendations presented are designed to achieve optimal system performance and high reliability. Although there are many variations to the recommended scenarios, any departure from these recommendations may result in less than ideal system performance.

This document describes the configuration for typical scenes, for a medium security IntrusionTrace system. To provide a high security installation, where the intrusion is expected to be covert, detailed consultation with ADPRO staff is required.

Wherever **XO device** is mentioned in this document, it applies to both ADPRO FastTrace 2 Series and ADPRO iFT Series devices, unless specifically mentioned otherwise.

1.3 Scope

The following items are addressed in this Technical Manual:

- Configuration of the IntrusionTrace analytics in the ADPRO XO client software, for typical applications.

The following items are not discussed in this document:

- Configuration of the IntrusionTrace analytics on HeiTel Video Gateways with XOh software. For details, see the documentation of the XOh software.
- Additional guidelines for dealing with difficult scenes. For details, see the *IntrusionTrace Best Practices* guide (26033).
- IntrusionTrace license management (installing, revoking) in the Xtralis Xchange tool. For details, see the *Xchange Tool User Manual* (27816).
- Operational background information on the IntrusionTrace application, site survey and system design, equipment installation, system commissioning, and site and equipment maintenance. For details, see the *IntrusionTrace Design Guide* (21814).
- Design, installation, configuration, or maintenance of complementary detection technologies including PIRs supplied by Xtralis. For details, see the Xtralis PRO and PRO E PIR documentation, and the other manufacturer's technical and application information.
- Installation or configuration of ADPRO FastTrace 2 Series or iFT Series devices. For details, see the *Hardware Installation Manual* of your XO device (FastTrace 2 Series: 21790; iFT Series: 27817).
- Installation of the XO client software. For details, see the *XO Client Software User Manual* (21796).
- Installation or configuration of central monitoring software. For details, see the documentation of these software products.

[1] The Xtralis RMGs include the ADPRO devices of the FastTrace 2 and iFT Series, and the HeiTel Video Gateways of the CamDisk E/+ E and iVG Series.

[2] Human-like: a feature that is able to differentiate between human and non-human movement for intrusion detection.

You can find the latest versions of this document and any referenced document on the Xtralis Security Solutions Support site www.xtralissecurity.com (logon may be required). If a document number is indicated (between parentheses), you can enter it in the Keywords box on the site, and search for the document.

1.4 Intended Audience

The intended audience for this Technical Manual includes the following key stakeholders:

- Security consultants
- System integrators
- System installers
- Facilities/building/site managers.

1.5 Prerequisites

1.5.1 Camera Resolution and Frame Rate

Whatever the resolution of the camera, the system is providing the analytics with CIF (352 x 288) images (or the next available higher resolution with a maximum of 640 x 480), 5 fps, and quality ‘normal’. This is the **default** analytics stream.

As of ADPRO firmware version XO 4, you have more control over the aspect ratio and quality of the analytic stream:

- By specifying the stream to use for analytics, you can match the aspect ratio to that of the live and recorded views. In some cameras, your choice can be better than the default chosen by the system.
- By selecting a higher compression quality, the system may, in extreme circumstances, give fewer false alarms and more reliable detections because fewer compression artefacts are present. However, extensive testing shows that the default is typically sufficient, and consumes less bandwidth.
- The resolution of the selected stream does not affect analytics performance.

For details, see the *XO Client Software User Manual* (21796).

The resolution and frame rate used for monitoring or continuous/event recording have no influence at all on the perimeter detection analytic.

Note

If you will be using IP cameras with IntrusionTrace, make sure that they support the analytics stream. For details, check the chapter on managing the IP video streams in the *XO Supported IP Cameras* list (26742).

1.5.2 Corridor Mode

With ADPRO software version XO 4.0 and above, analytics work with corridor mode[3], where the image is taller than wide. In hallways and corridors, a larger part of the camera image is useful for analytics when using corridor mode. In addition, it reduces the dead zone beneath the camera.

Camera image in normal mode

Camera image in corridor mode, showing more of the foreground

If you have used a camera with analytics in normal mode before, you have to make new calibration pictures and recalibrate the scene when you switch to corridor mode.

Corridor mode affects the maximum horizontal field of view (FOV) because fewer pixels are available horizontally. For a 3:4 corridor image, the maximum horizontal FOV is 18 m (59 ft); for a 9:16 corridor image, it is 14 m (46 ft). For more information on the FOV, see the *IntrusionTrace Design Guide* (21814).

1.5.3 Fisheye Cameras

With ADPRO software version XOa 3.2.33 and above, analytics work with fisheye cameras. For optimal results with fisheye cameras, keep the detection area within a 5 m radius around the camera.

1.5.4 Thermal Cameras

IntrusionTrace also works with thermal cameras (XO device firmware version v2.08.0005 or above). With thermal cameras, in general, IntrusionTrace can detect smaller objects. For IntrusionTrace to recognise a camera as a thermal camera, you must select the **Thermal** option when you enable the thermal camera in the XO client software.

1.5.5 PTZ Cameras

Although it is possible to use IntrusionTrace on a PTZ camera, Xtralis does not recommend it.
If you want to run IntrusionTrace on a PTZ camera, consider the following restrictions:

- IntrusionTrace **only works when the camera is in the home position**. IntrusionTrace is suspended while the camera moves until it is back in the home position. You define the detection zones and calibrate the camera in the home position.
- You must set up the PTZ camera in the XO client so that it automatically returns to the home position after moving (using the **Auto-Home Expire Time** in the camera configuration window).
- Use IntrusionTrace on a PTZ camera only if the **PTZ function is used in exceptional cases**; for example only when the CMS wants to investigate an alarm. The more a PTZ camera moves, the more it may drift from its originally set home position over time. This in turn may affect the position of detection zones in the scene and the camera calibration, reducing IntrusionTrace's optimal performance.
- Even on PTZ cameras that rarely move, you must regularly check and adjust the detection zones and camera calibration.

[3] On supported IP cameras of the following brands: Honeywell, Axis, Dahua, Hikvision, Samsung, and Sony.

1.5.6 Licensing

For each camera that you want to use with IntrusionTrace, you need an IntrusionTrace application license. The latest IntrusionTrace on XO licenses always include a license for a PIR detector interface (PIR-HLI), so you can combine IntrusionTrace detection with PIR detection for double-knock configurations.

The IntrusionTrace menu in the XO client will not be available until you install at least one IntrusionTrace license on the XO device. For details on installing application licenses on your XO device, see the *Xchange Tool User Manual* (27816).

The number of analytics application licenses that can run simultaneously on your XO device, depends on the number of available analytic channels on your device. One analytics application (IntrusionTrace, LoiterTrace…) requires one analytic channel. The maximum number of analytic channels is:

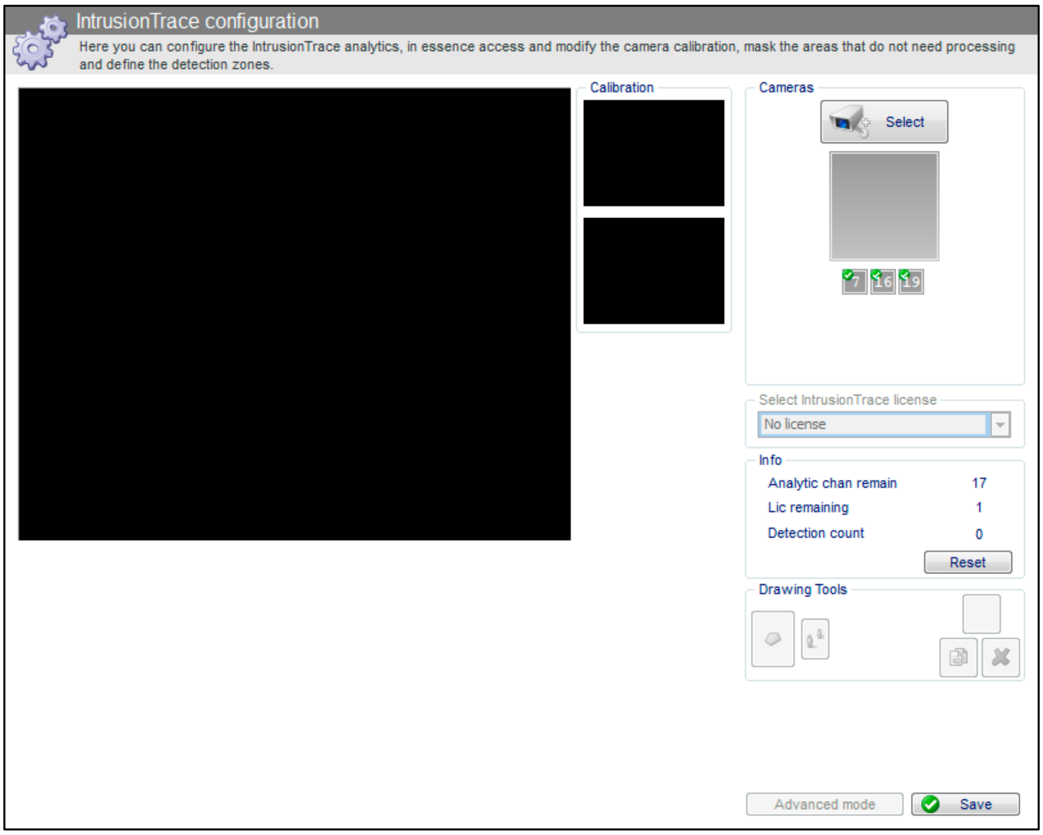
- FastTrace 2: up to 4 analytic channels
- FastTrace 2X: up to 16 analytic channels
- FastTrace 2E: up to 32 analytic channels
- iFT: up to 16 analytic channels (via trade-off with video channels)
- iFT-E: up to 32 analytic channels.

1.6 Information in the IntrusionTrace Configuration Window

The IntrusionTrace configuration window displays the cameras that have IntrusionTrace enabled, and the available analytic channels and licenses on the XO device.

To open the IntrusionTrace configuration window, proceed as follows:

- Open the XO client software, connect to the desired XO device, and then choose **System > Behaviour > Analytics > IntrusionTrace**.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the areas that do not need processing and define the detection zones.

Select IntrusionTrace license: No license

Info

Analytic chan remain 17

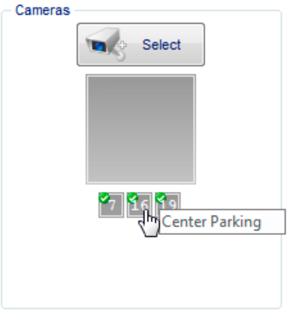
Lic remaining 1

Detection count 0

The **Info** section displays the following information:

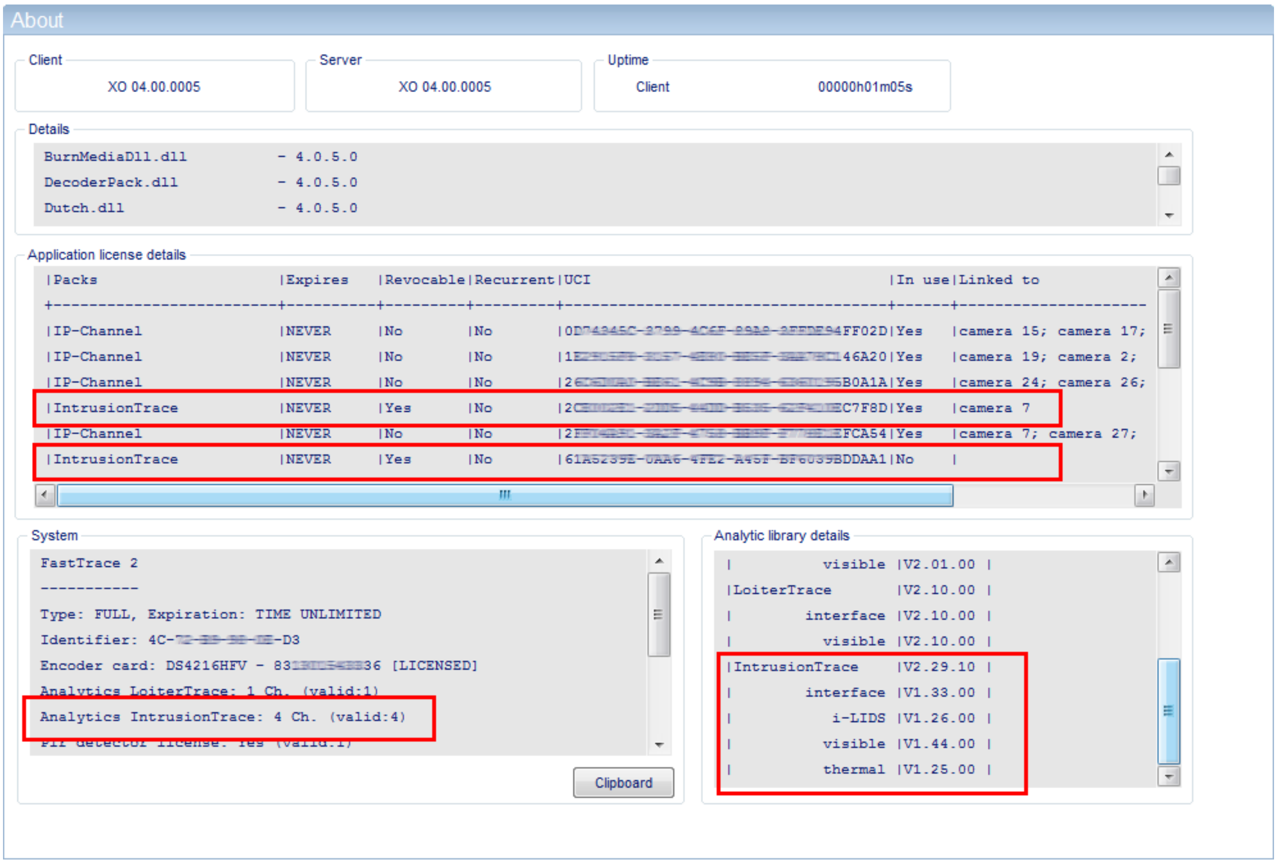
Item	Description
Analytic chan remain	The number of remaining analytic channels on the XO device = the maximum number of analytic channels available minus the channels that are already in use by analytic applications (17 in the example screen above). This includes all analytics: IntrusionTrace, LoiterTrace, and SmokeTrace. If there are no remaining analytic channels on the XO device (**Analytic chan remain** = 0), you cannot enable more analytic applications on the XO device.
Lic remain	The number of unused IntrusionTrace licenses on this XO device = the total number of IntrusionTrace licenses minus the IntrusionTrace licenses that are already assigned to a camera (1 in the example screen above). If there are no remaining licenses (**Lic remain** = 0), you can install additional IntrusionTrace licenses on the device using Xchange, or you can move an unused license from another XO device (revoke–install via Xchange).
Detection count	The detection counter is used for testing the configuration. For details, see *Testing the IntrusionTrace Configuration* on page 62.

The **Cameras** section displays the numbers of all the IntrusionTrace-enabled cameras on the XO device. Position the mouse cursor over the number to see the corresponding camera name.



1.7 Information in the About Window

The **About** window displays detailed information about IntrusionTrace. To open the **About** window, click **About** in the top menu in the XO client.



Client: XO 04.00.0005

Server: XO 04.00.0005

Uptime: Client 00000h01m05s

Details

```
BurnMediaDll.dll        - 4.0.5.0
DecoderPack.dll         - 4.0.5.0
Dutch.dll               - 4.0.5.0
```

Application license details

```
|Packs                    |Expires    |Revocable|Recurrent|UCI                                 |In use|Linked to
+-------------------------+-----------+---------+---------+------------------------------------+------+--------------------
|IP-Channel               |NEVER      |No       |No       |0D[redacted]FF02D|Yes    |camera 15; camera 17;
|IP-Channel               |NEVER      |No       |No       |1E[redacted]46A20|Yes    |camera 19; camera 2;
|IP-Channel               |NEVER      |No       |No       |26[redacted]B0A1A|Yes    |camera 24; camera 26;
|IntrusionTrace           |NEVER      |Yes      |No       |2C[redacted]C7F8D|Yes    |camera 7
|IP-Channel               |NEVER      |No       |No       |2F[redacted]FCA54|Yes    |camera 7; camera 27;
|IntrusionTrace           |NEVER      |Yes      |No       |61A5239E-0AA6-4FE2-A45F-BF6039BDDAA1|No     |
```

System

```
FastTrace 2
-----------
Type: FULL, Expiration: TIME UNLIMITED
Identifier: 4C-[redacted]-D3
Encoder card: DS4216HFV - 83[redacted]36 [LICENSED]
Analytics LoiterTrace: 1 Ch. (valid:1)
Analytics IntrusionTrace: 4 Ch. (valid:4)
PIR detector license: Yes (valid:1)
```

Analytic library details

```
|         visible |V2.01.00 |
|LoiterTrace      |V2.10.00 |
|       interface |V2.10.00 |
|         visible |V2.10.00 |
|IntrusionTrace   |V2.29.10 |
|       interface |V1.33.00 |
|          i-LIDS |V1.26.00 |
|         visible |V1.44.00 |
|         thermal |V1.25.00 |
```

The window displays the following information:

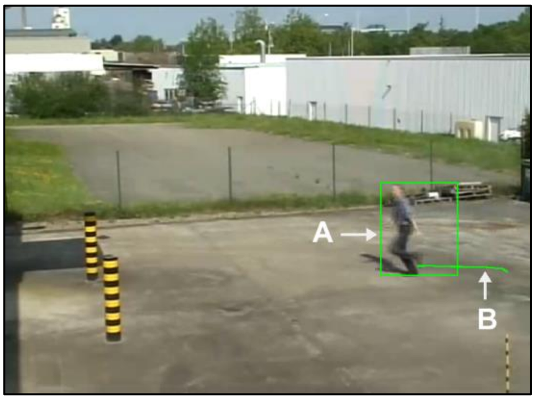
- Under **Application license details**, you find detailed information on the IntrusionTrace licenses that are installed on the XO device: expiry date, unique identifier, if they are in use or not, and on which camera.
- Under **System**, you find a summary with the number of IntrusionTrace licenses (**4 Ch.** in the example) that are installed on the XO device, and the number of valid licenses (**valid: 4** in the example).
- Under **Analytic library details**, you find technical information on the libraries that the IntrusionTrace analytic application uses.

1.8 Rendering Analytic Bounding Boxes

Analytic bounding boxes indicate the presence of detected objects in the scene, detected by the Xtralis analytic applications. The bounding boxes are:

- Green: when the alarm is not triggered
- Red: when the alarm is triggered.

Besides the bounding boxes around the detected object, IntrusionTrace also displays the path that the object follows in the scene. Just like the bounding boxes, the path is displayed in green when the alarm is not triggered, and in red when the alarm is triggered.

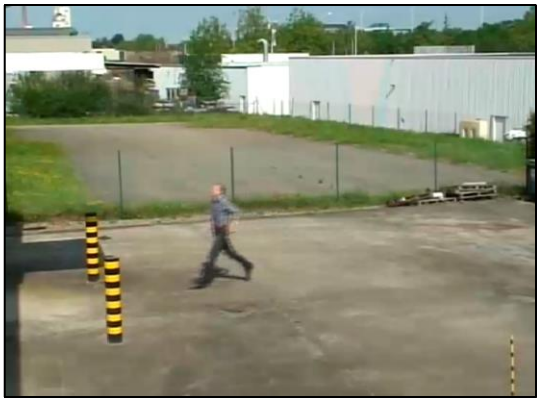
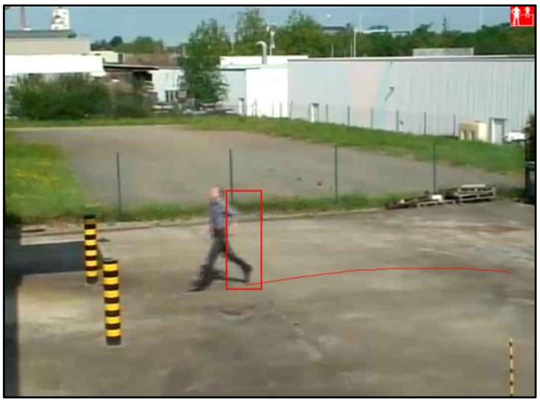
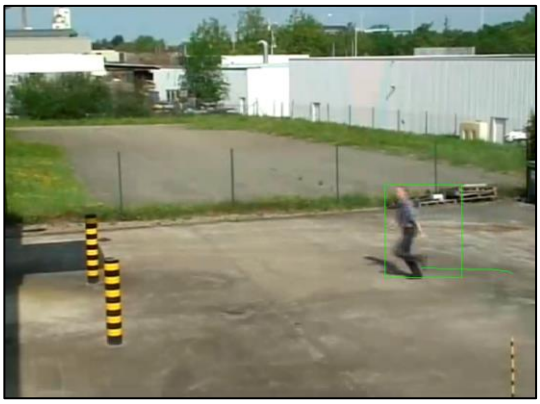
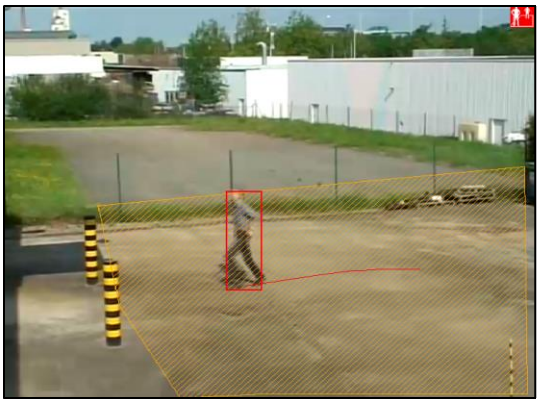


Analytic bounding box (**A**) and path (**B**)

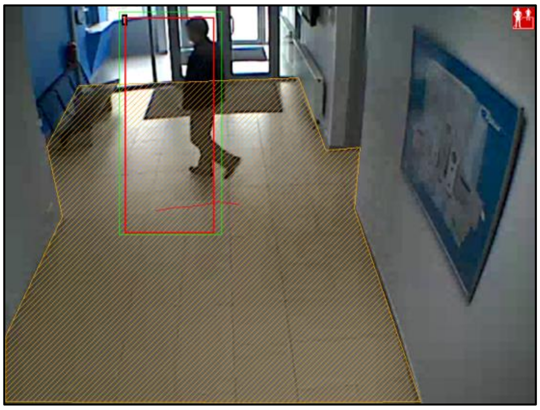
For live and recorded images in the **Live Video** and **Recorded video** windows, you can choose whether you want to render analytic bounding boxes and paths, or not. The following options exist:

- **Off**: the system does not display bounding boxes and paths.
- **Alarm only**: the system displays only the red bounding boxes and paths when an alarm occurs.
- **Alarm and tracking**: the system displays the green bounding boxes and paths for tracking (pre- and post-alarm), and the red bounding boxes and paths when the alarm occurs.
- **IntrusionTrace zone outline upon event**: the system highlights the IntrusionTrace detection zone where the alarm occurs.

Below, you can see several examples:

 Off: no bounding boxes or paths visible.	 Alarm only: red bounding box and path upon alarm.
 Alarm and tracking: green bounding boxes and path for tracking; bounding boxes and path will turn red upon alarm.	 IntrusionTrace zone outline (with alarm): red bounding boxes and path + IntrusionTrace detection zone highlighted.

If you have multiple analytic applications running on the same camera (for example, IntrusionTrace and LoiterTrace), the system will display bounding boxes for all analytics. The example below displays a red bounding box for IntrusionTrace (alarm) and a green bounding box for LoiterTrace (tracking), around the same object.

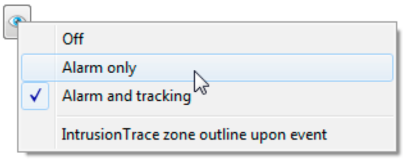


The following limitations apply to bounding box rendering:

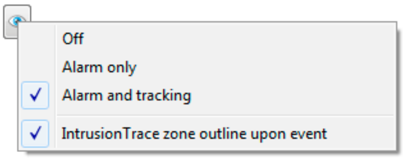
- When playing back recorded images, bounding boxes and paths only appear in **normal playback mode**, not during fast forward/backward.
- If bounding box rendering is switched off, the **IntrusionTrace zone outline upon event** option is unavailable.
- The player software that allows you to play downloaded recordings (.hbox files) from your local PC or from a USB drive, offers the same options for rendering analytic bounding boxes and paths. However, the **IntrusionTrace zone outline upon event** option is not available.
  If you need to see the highlighted IntrusionTrace zone, play the recordings from within the XO client.

To select the desired options for rendering bounding boxes, proceed as follows:

1. From the live or recorded images view, click the 👁 button, and then click the desired rendering option.



2. To highlight the IntrusionTrace detection zone where the alarm is triggered, click the 👁 button, and then click **IntrusionTrace zone outline upon event**. A check mark appears next to the option when it is active:



2 IntrusionTrace Configuration

2.1 CMS Priority

When you open the analytics configuration pages in the XO client software, the client takes CMS priority on the XO device. The analytics configuration then becomes unavailable to all other users. This prevents conflicts with the monitoring and alarm management software.

2.2 Summary

To configure a camera with IntrusionTrace, perform the following steps:

1. Install the IntrusionTrace license on the XO device. For details, see the *Xchange Tool User Manual* (27816).
2. Enable IntrusionTrace on the desired camera.
3. Draw the detection zones.
4. Calibrate the scene.
5. Advanced: set up a custom detection profile for the scene.
6. Advanced: set up custom detection profiles for the detection zones.
7. Advanced: set up i-LIDS certified detection.
8. Advanced: draw mask zones.
9. Test the configuration.
10. Optional: assign analytic detail inputs to the individual detection zones.
11. Configure the inputs and outputs for IntrusionTrace.
12. Back up the client configuration and calibration pictures.

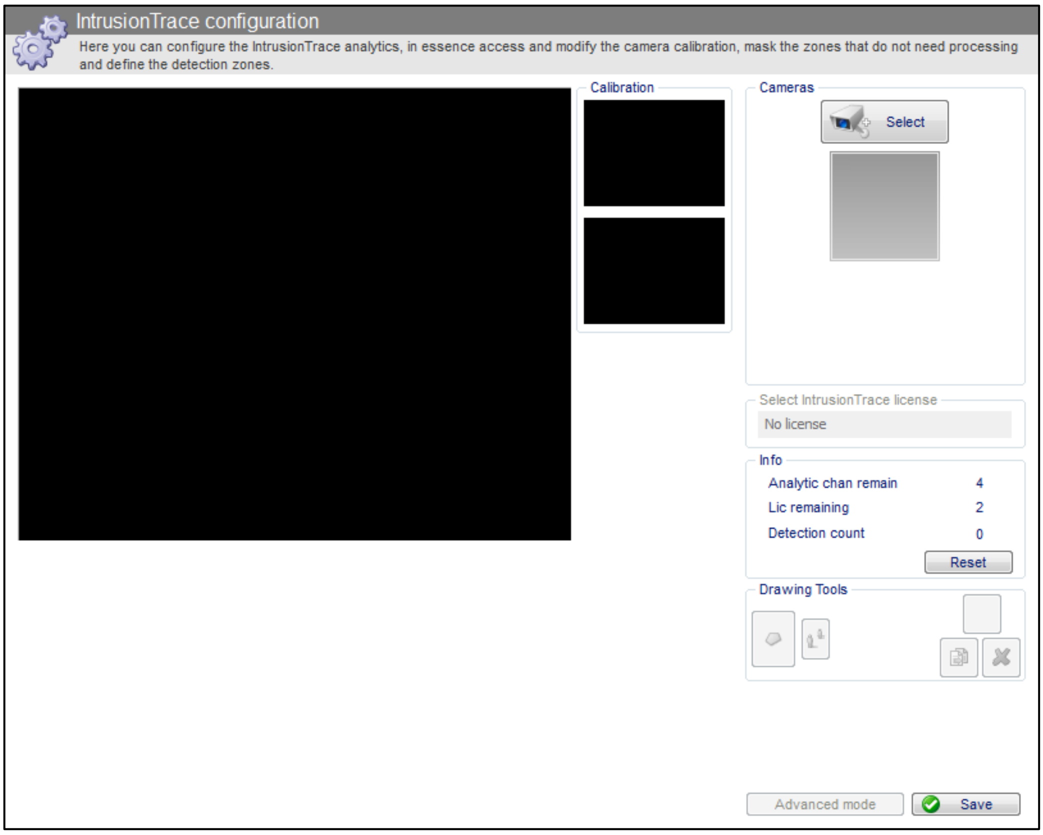
Each step is described in detail in the following chapters.

3 Enabling and Disabling IntrusionTrace on a Camera

3.1 Enabling IntrusionTrace on a Camera

To enable IntrusionTrace on a camera, proceed as follows:

1. Open the XO client software, connect to the desired XO device, and then choose **System > Behaviour > Analytics > IntrusionTrace**.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

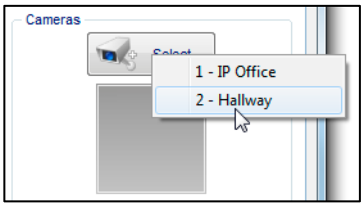
No license

Info

Analytic chan remain	4
Lic remaining	2
Detection count	0

The example screen above shows that there are 4 analytic channels remaining, and 2 IntrusionTrace licenses.

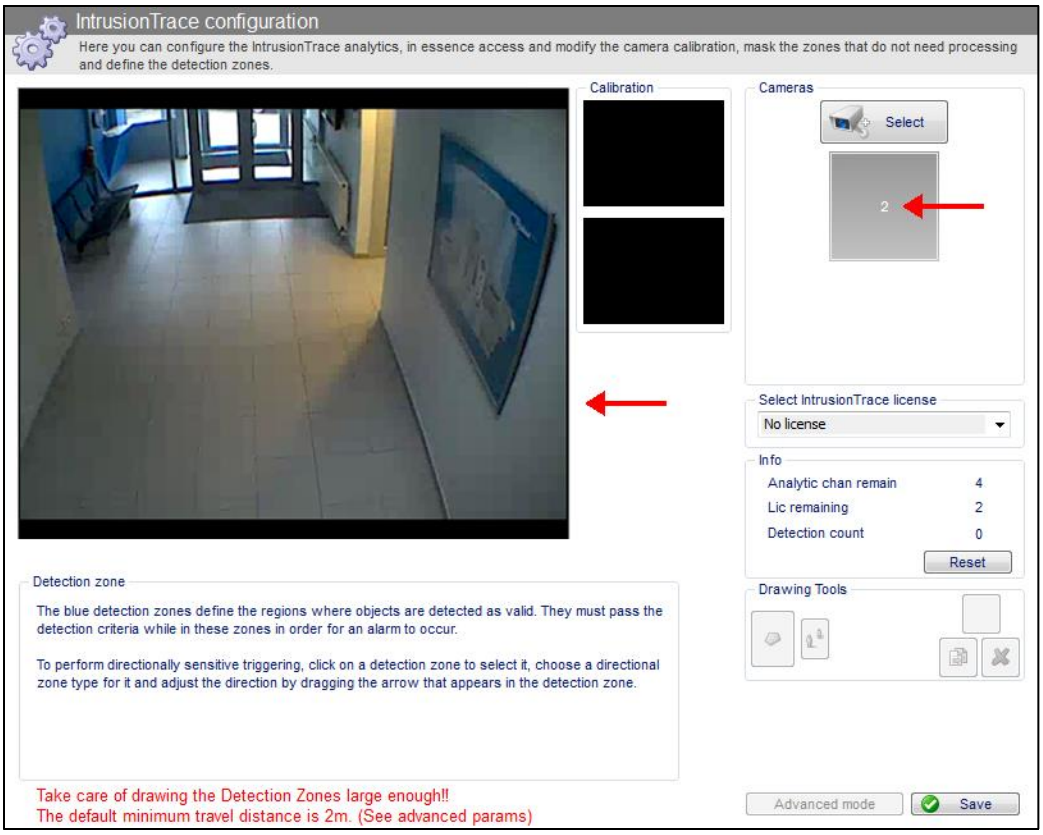
2. Under **Cameras**, click **Select**, and then click the desired camera.



Note

Before selecting a camera, check any restrictions and guidelines for camera usage as described in *Prerequisites* on page 8.

The system displays the camera's live image, and the selected camera number appears in the grey box under the **Select** button.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Info	
Analytic chan remain	4
Lic remaining	2
Detection count	0

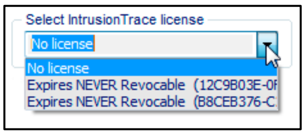
Detection zone

The blue detection zones define the regions where objects are detected as valid. They must pass the detection criteria while in these zones in order for an alarm to occur.

To perform directionally sensitive triggering, click on a detection zone to select it, choose a directional zone type for it and adjust the direction by dragging the arrow that appears in the detection zone.

Take care of drawing the Detection Zones large enough!!
The default minimum travel distance is 2m. (See advanced params)

3. In the **Select IntrusionTrace license** box, select one of the available licenses.

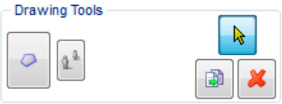


Select IntrusionTrace license

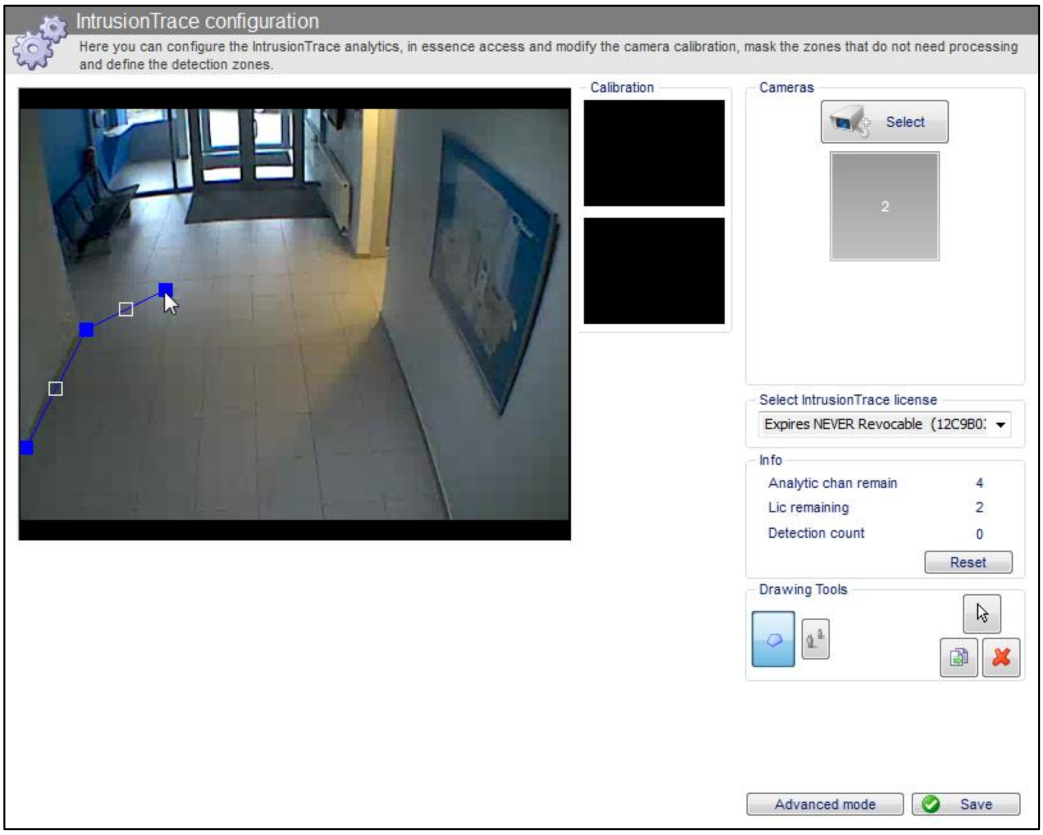
No license

- No license
- Expires NEVER Revocable (12C9B03E-0F
- Expires NEVER Revocable (B8CEB376-C

The drawing tools become available when you have selected a license.



4. Click the button and draw one detection zone: click on the live image in each corner of the detection zone. You can draw the first zone very roughly, and adjust later. For instructions, see *Drawing Detection Zones* on page 23.



Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Select IntrusionTrace license: Expires NEVER Revocable (12C9B0:

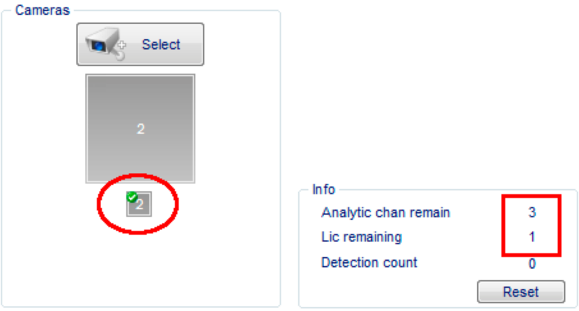
Info	
Analytic chan remain	4
Lic remaining	2
Detection count	0

5. Click **Save**.

Caution!

Do not click **Save** until you have drawn at least one detection zone for the camera. If there are no detection zones, the system **unlinks the license** from the camera when you click **Save**.

IntrusionTrace is now active on the camera, and will start its analysis using the drawn detection zone and the default detection parameters. The number of the camera appears in the **Cameras** section under the grey box. The number of available analytics channels and the number of remaining IntrusionTrace licenses is reduced by 1:



Info	
Analytic chan remain	3
Lic remaining	1
Detection count	0

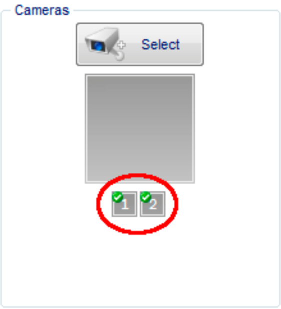
3.2 Disabling IntrusionTrace on a Camera

To disable IntrusionTrace on a camera, you unlink the license. You can then assign the license to a different camera, or move it to a different XO device using Xchange.

> ***Note***
>
> The system remembers the last saved IntrusionTrace configuration for the camera, and when you assign a license again to the camera, that configuration will be restored.

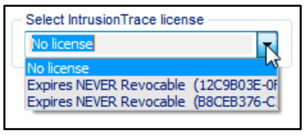
To disable IntrusionTrace on a camera, proceed as follows:

1. Choose **System > Behaviour> Analytics > IntrusionTrace**, and then click the desired camera in the **Cameras** section.



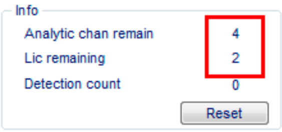
The configuration screen for the selected camera appears.

2. In the **Select IntrusionTrace license** box, select **No license**.


Select IntrusionTrace license
No license
No license
Expires NEVER Revocable (12C9B03E-0F
Expires NEVER Revocable (B8CEB376-C

3. Click **Save**.

The IntrusionTrace license is now available to assign to other cameras, or to move to a different XO device via Xchange. The number of available analytics channels and the number of remaining IntrusionTrace licenses is increased by 1:



Info

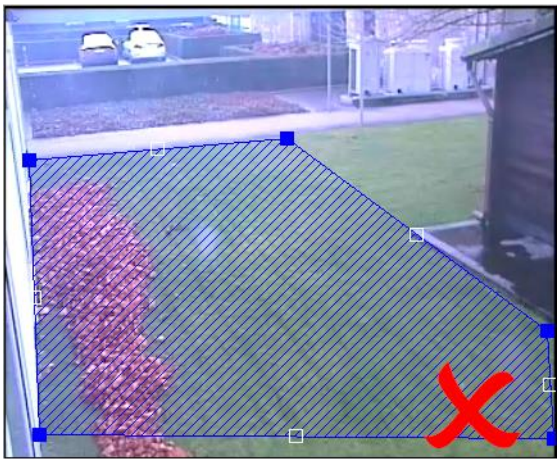
Analytic chan remain	4
Lic remaining	2
Detection count	0

4 Detection Zones

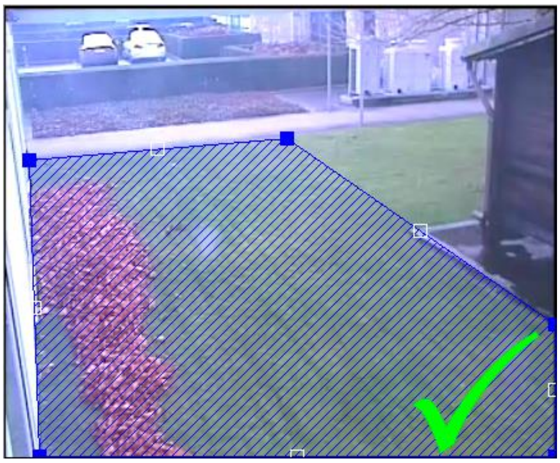
4.1 About Detection Zones

A detection zone is a zone **on the ground** where intruders shall trigger an alarm. You can draw up to 16 polygonal detection zones for one camera. The detection zones can overlap.

The system only monitors the path of the intruder, not their whole body, so detection areas do not usually need to be drawn on walls or fences. Conversely, there must not be any gap between the lower edge of the detection area and the lower edge of the image if you wish to detect intruders in the immediate foreground.



Detection zone does not reach edge of image. **Warning!** IntrusionTrace may not detect intruders in the foreground because their path can pass below the detection zone.

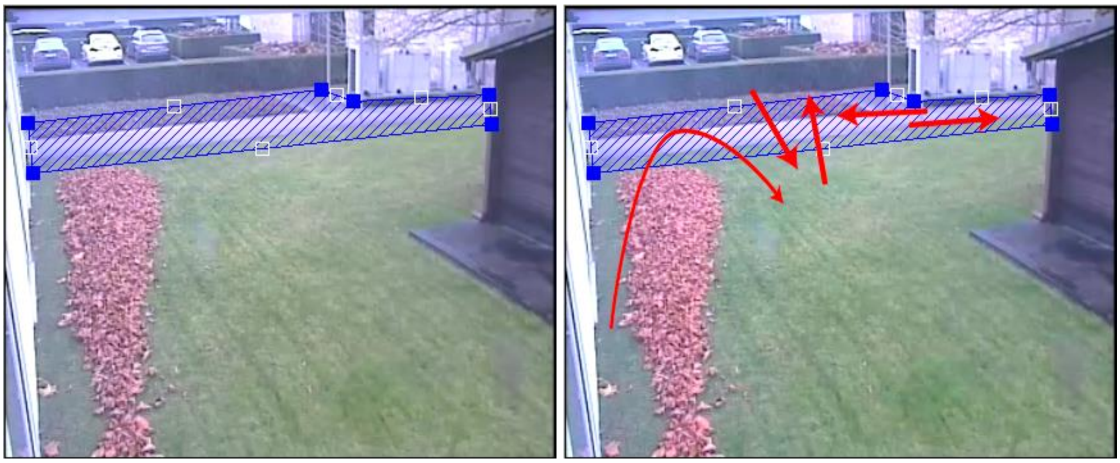


Detection zone reaches edge of image; intruders in the foreground can be detected.

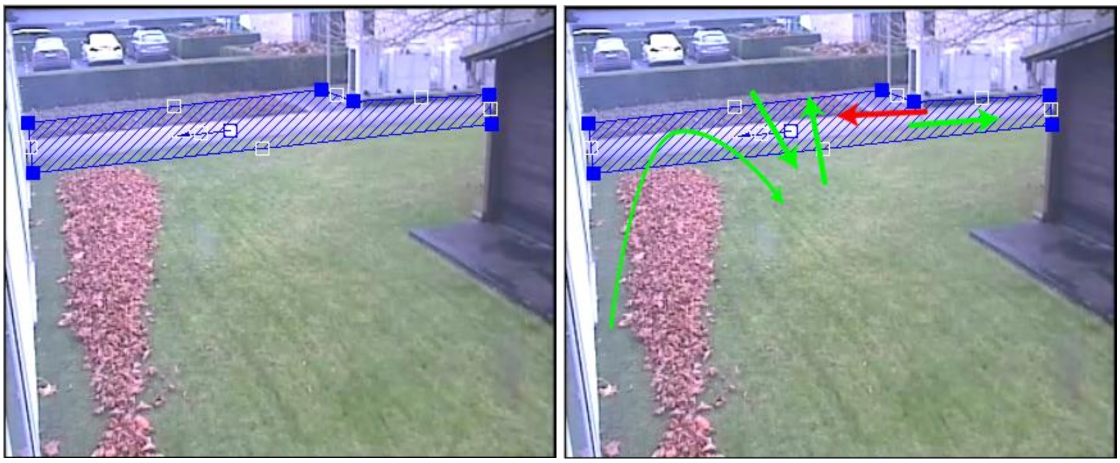
4.2 Directional Zones

For each detection zone, you can specify to detect intruders only if they move sufficiently far in a specific direction in the zone. The available options are:

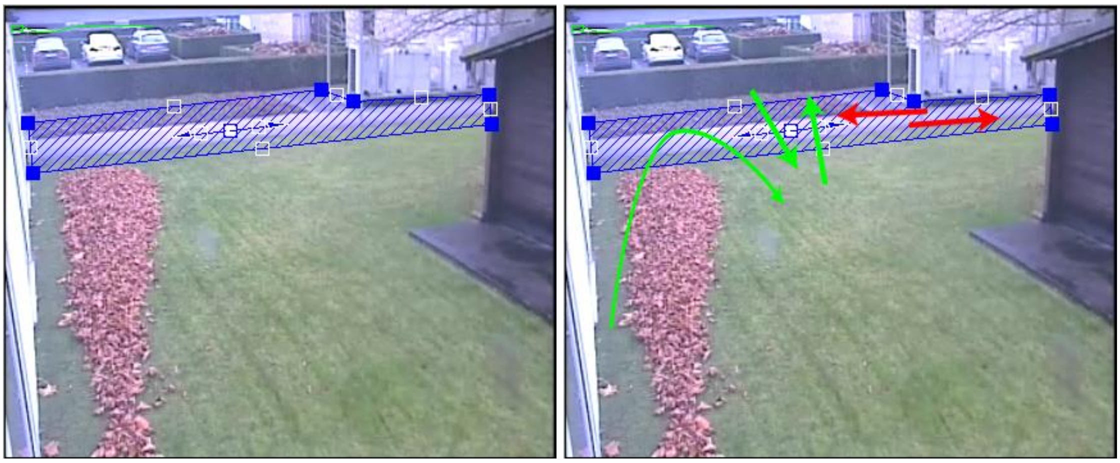
- **Non-directional zone**: intruders shall trigger the alarm, regardless of the direction in which they move in the detection zone.



- **Unidirectional zone**: intruders trigger the alarm only if they move in a specific direction, indicated by the direction arrow. You rotate the direction arrow until it points in the desired direction. For example, along a garden path. If the direction arrow points down the path, IntrusionTrace triggers the alarm only if the object moves down the path. If the object moves up the path, IntrusionTrace will not trigger the alarm. For example, you can use this to trigger an alarm when people enter a building, but not when they leave.



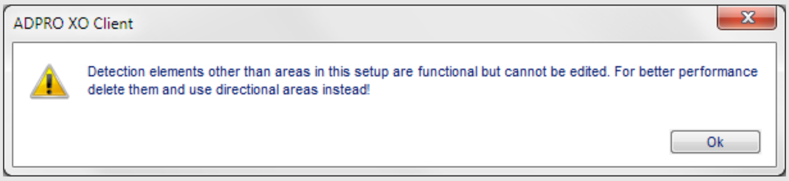
- **Bidirectional zone**: intruders trigger the alarm only if they move in a specific direction, indicated by the direction line in the detection zone. The direction line has two arrows and detection occurs in both ways. If you align the bidirectional line with a garden path, IntrusionTrace will trigger the alarm if objects move up or down the path, but not if they cross the path.



Note

As of ADPRO firmware version V2.11.0023, IntrusionTrace no longer uses trigger lines, but the more reliable directional zones. If you have upgraded, the existing trigger lines will still function. However, Xtralis recommends that you delete all trigger lines from your existing detection zones; and instead set the desired direction for the zone. There is no need to redraw the zone.

The following message will appear if you open an IntrusionTrace configuration that still uses trigger lines:



ADPRO XO Client

Detection elements other than areas in this setup are functional but cannot be edited. For better performance delete them and use directional areas instead!

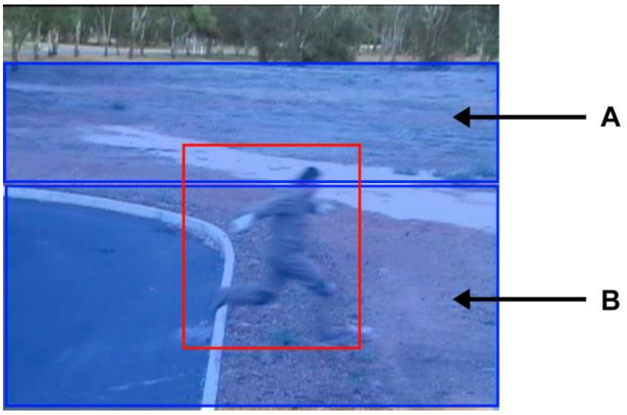
4.3 Settings per Detection Zone

If necessary, you can define a different detection profile (a set of detection parameters) for each detection zone (in advanced mode only). This allows for enhanced detection within the same scene if different parts of the scene require different settings. A few practical examples are described below.

For instructions on setting up detection profiles for individual zones, see *Zone Profiles* on page 48.

4.3.1 Different Minimum Time per Detection Zone

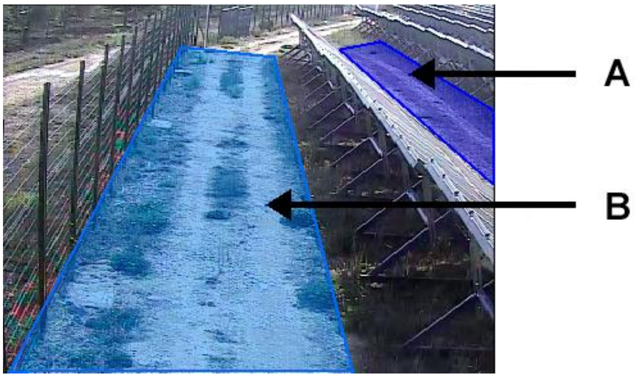
For large outdoor areas where it is equally important to detect fast moving objects in front of the camera, as well as objects moving far in the back, you can create two detection zones where the minimum time to trigger an alarm is different. By doing so, IntrusionTrace can filter short perturbations like tree shadows appearing in the back of the scene, while still detecting people in front of the camera, where it takes only one second to cross the scene.



Detection zone A: minimum time = 4 seconds
Detection zone B: minimum time = 0.5 seconds

4.3.2 Different Minimum Distance per Detection Zone

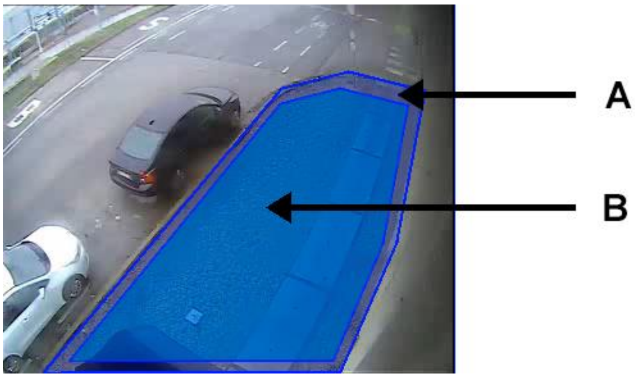
For areas where you have both narrow and large detection zones: IntrusionTrace must detect people walking in the narrow zone before they can cross, whereas people crossing the larger zone will necessarily travel a longer distance. IntrusionTrace can detect reliably in both conditions if you specify different minimum distance parameters for these zones, while still preventing false alarms from short perturbations in the large zone.



Detection zone A: minimum distance = 1 m
Detection zone B: minimum distance = 2 m

4.3.3 Different Behaviours Depending on Object Characteristics

If you need different behaviour for different objects in the same zone of the scene, you can create two detection zones on top of each other, each with a different detection profile. You can then trigger different detection signals from the same location. The detection signals can, for example, activate different outputs to inform users of the presence of a single person (small area, typically 1 m²), or a group of people (large area).



Detection zone A: minimum area = 1 m²
Detection zone B: minimum area = 5 m²

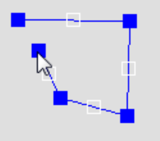
Detection zone A triggers for a single person

Detection zone B triggers for a group of people

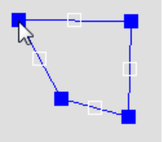
4.4 Drawing Detection Zones

To draw a detection zone, proceed as follows:

1. Click the ⬠ button (blue polygon).
2. In the camera image, draw the detection zone by clicking on the image everywhere you want to make a corner.

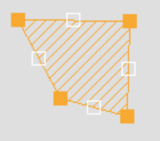


3. To close the detection zone:
   - Click on the first corner.

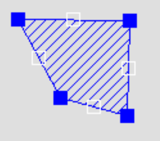


   - Alternatively, right-click anywhere.

The detection zone is still selected, so it appears hatched in orange lines:



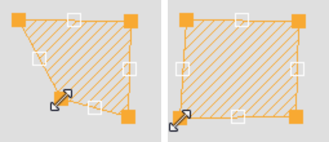
Click anywhere outside the detection zone to deselect it. It appears hatched in blue lines:



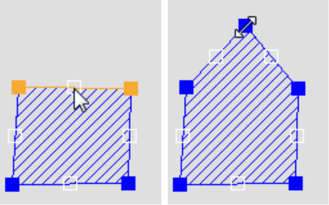
> ***Note***
>
> It may be difficult to draw on the edges of the camera image. If the detection has to run to the edge of the camera image, then first draw roughly near the edges. Finish the polygon, and then adjust it by dragging the corners to the edge of the image.

4. To adjust the zone, proceed as follows:

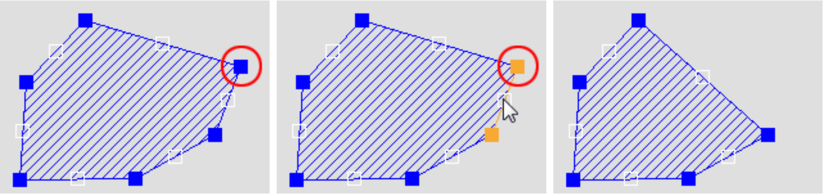
    - To move a corner, drag it to the desired position.

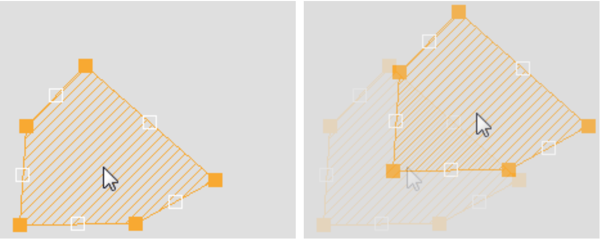
    - To add a corner to the polygon, click the white handle in the middle of the edge where you want to add a corner, and then drag the handle to the desired corner position.

    - To remove corner from the polygon, click the white handle in the middle of the edge that extends clockwise from the corner that you want to remove, and then click the ✖ button (or press Delete on the keyboard).

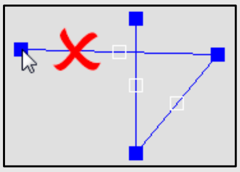
    - To move the whole zone, click anywhere in the zone and drag it to the desired position.

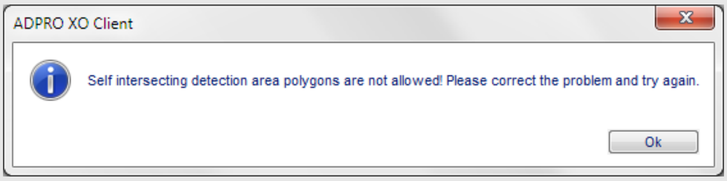
5. Click **Save**.

Note

The edges of the detection zone must not cross:



If you have drawn a detection zone with crossing edges, the following message will appear when you click **Save**:



ADPRO XO Client

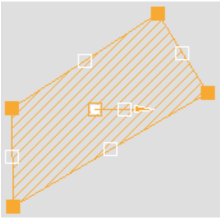
Self intersecting detection area polygons are not allowed! Please correct the problem and try again.

In this case, delete the detection zone. Draw several zones if necessary to cover the required areas.

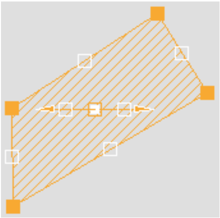
4.5 Setting Directionality

To set the directionality of a detection zone, proceed as follows:

1. Click the desired detection zone.
2. Under **Detection Area Type**, click the desired directionality:
   - **Unidirectional**: a directional line with one arrow appears in the middle of the detection zone.
   - **Bidirectional**: a directional line with two arrows appears in the middle of the detection zone.

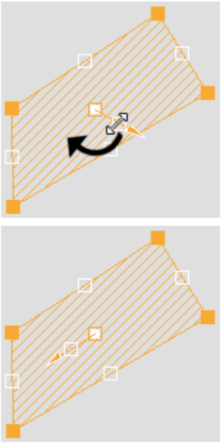


Unidirectional

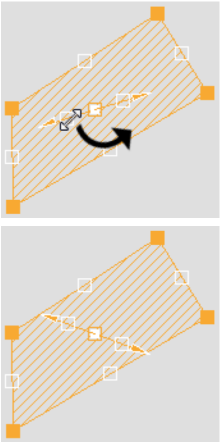


Bidirectional

3. Drag the white handle on the directional line until the arrow points in the desired direction.

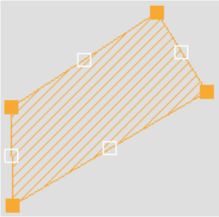


Unidirectional



Bidirectional

4. To remove directionality from a detection zone: click the detection zone, and then click **Non directional**. The directional line disappears.



5. Click **Save**.

4.6 Copying Detection Zones

When you copy a detection zone, you copy not only the shape, but also its directional type (non-directional, unidirectional, bidirectional), and its zone profile.

To copy a detection zone, proceed as follows:

1. Click the detection zone that you want to copy.
2. Click the button; or press Ctrl+C. The copy appears in the top left corner. The copy has the same shape, directional type, and zone profile as the original, but it does not have an alarm input assigned.

> ***Note***
>
> If you copy a detection zone that is located in the top left corner, the copy appears immediately on top of the original detection zone. It may look as if the copy is not there.

3. Drag the copy to the desired position.
4. Adjust the copied zone as required:
   - shape
   - directional type
   - assigned alarm input
   - zone profile.
5. Click **Save**.

4.7 Deleting Detection Zones

To delete a detection zone, proceed as follows:

- Click the detection zone, and then click the button, or press Delete.

5 Calibration

5.1 About Calibration

If you are using analytics, you may need to perform the following calibrations:

- **3D calibration**: this is **mandatory** for IntrusionTrace. The 3D calibration of a scene makes sure that IntrusionTrace can calculate the size of an object, the distance it travels through the scene, the speed… Correct detection depends on these parameters.
- **Bounding box calibration**: only for IP cameras that use different aspect ratios for the analytics stream and the live/recording stream. Bounding box calibration makes sure that the analytic bounding boxes appear correctly on all streams, regardless of their aspect ratio.

You can find detailed instructions for both calibrations further below.

> ***Caution!***
>
> If you change the aspect ratio of the analytics stream for a camera, **you have to make new calibration images and recalibrate that camera**.

5.2 3D Calibration

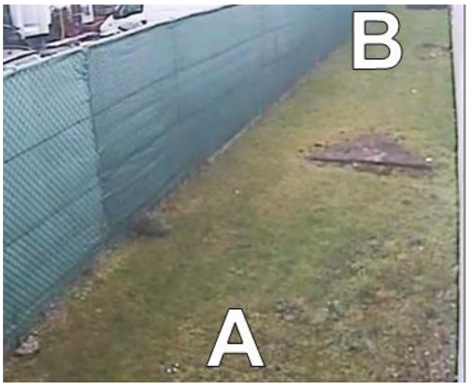
5.2.1 Overview

3D calibration allows analytics applications to identify the size, speed… of detected objects in the camera image. Setup requires two easy steps to mark:

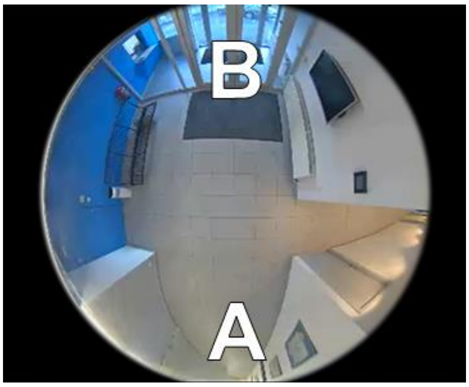
- the height of a known object at the front of the scene
- the height of that same object at the back of the scene.

Typically, you make a snapshot of the scene with a person/object standing at the front of the scene (**A**), at the bottom of the camera image, and another snapshot with the same person/object standing at the back of the scene (**B**), at the top of the camera image.
On a **fisheye** camera, you do the same: you make a snapshot with a person/object at the bottom of the scene (**A**), and another with the same person/object at the top of the scene (**B**). Although the objects will be similar in size at these two extremes, the measurements provide reliable detection across the scene.

Always perform walk tests to confirm detection.



Position of objects for 3D calibration in normal scene



Position of objects for 3D calibration in fisheye scene

You can either use live images, or you can first record images and take snapshots when you play back the footage, so that only one person can calibrate the scene.

You can calibrate a scene in the XO client:

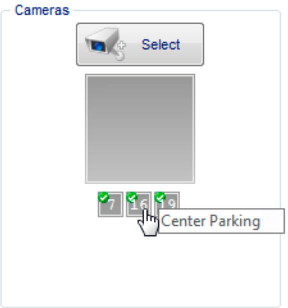
- from the IntrusionTrace configuration window
- from the LoiterTrace configuration window
- or from the video input configuration window.

You need to calibrate a scene only once. The calibration is valid for all analytics applications (IntrusionTrace, LoiterTrace). As of XOa 3.02.0017, the system displays thumbnails of the calibration pictures (if available) in the analytics configuration window. As of XO 4.00, the system also displays the resolution of the calibration pictures (= the analytics stream resolution) in the calibration window.

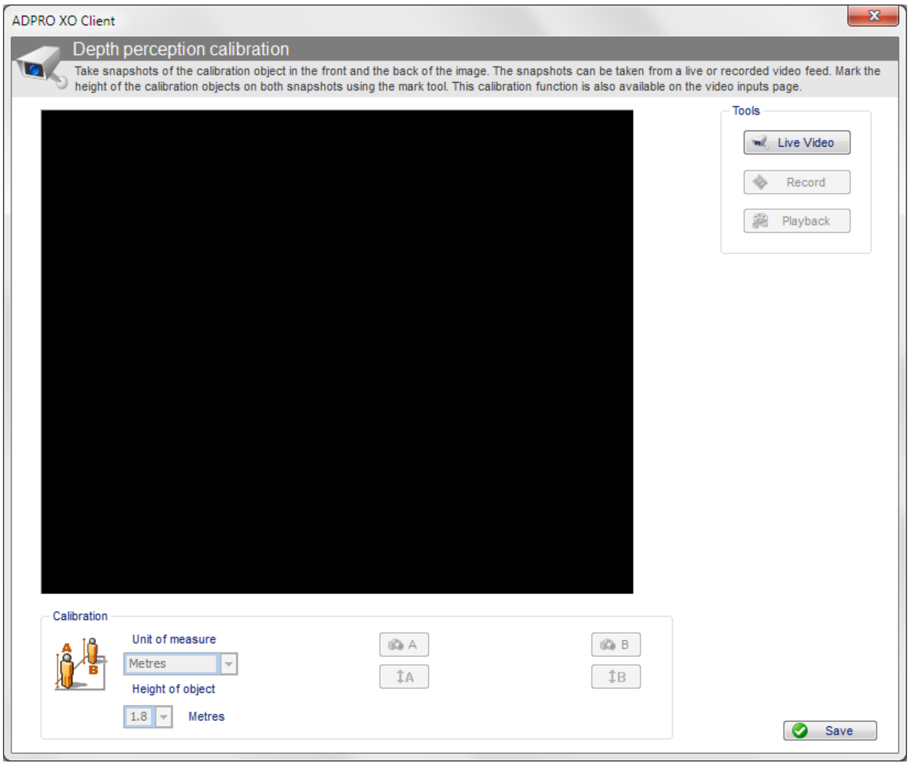
5.2.2 3D Calibration from Live Images

To calibrate a scene from live images, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. Click the button.

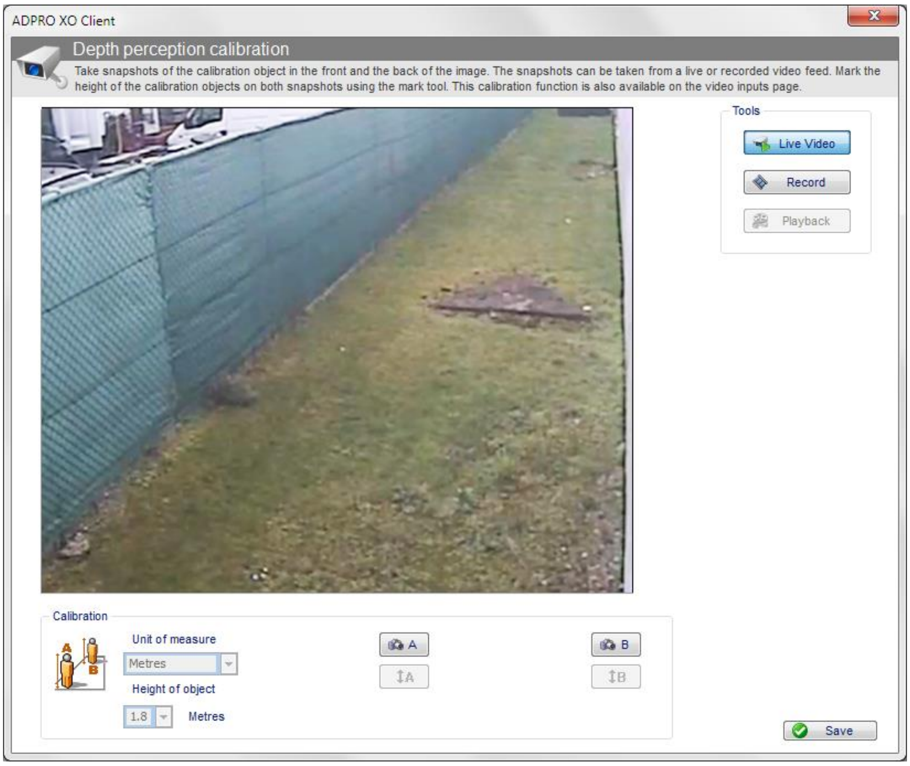


Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

Height of object: 1.8 Metres

3. Under **Tools**, click **Live Video**. The live camera image appears.



ADPRO XO Client

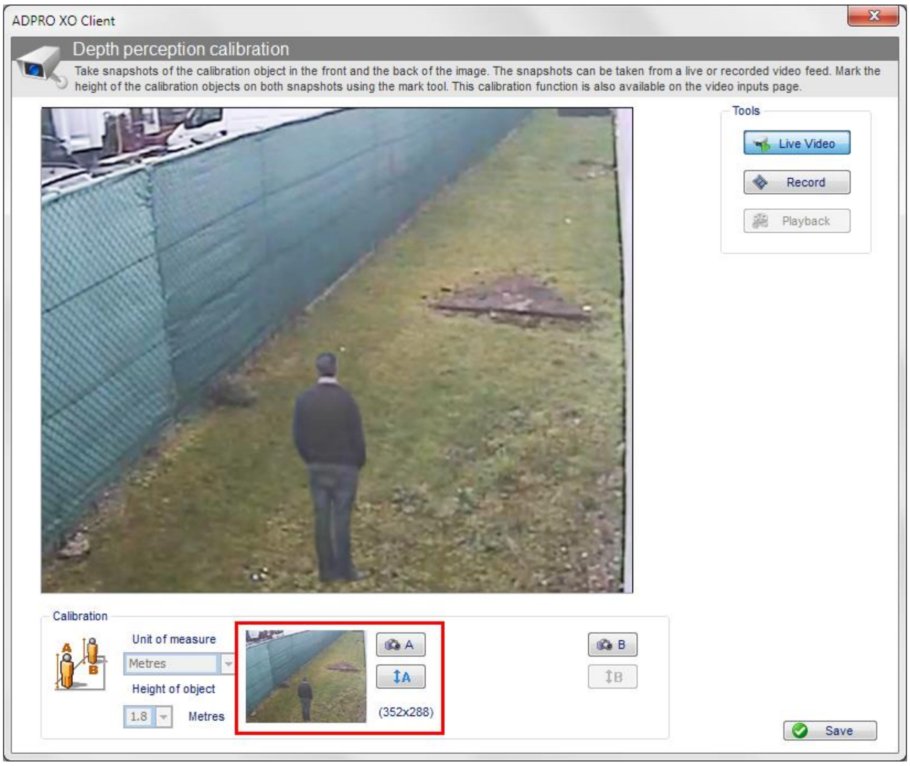
Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

Height of object: 1.8 Metres

4. When the person/object is standing **at the front** of the scene, click A to make a snapshot. Make sure that the person/object is completely visible (from head to toe). A miniature version of the snapshot appears at the bottom of the screen; the system indicates the image resolution.



ADPRO XO Client

Depth perception calibration

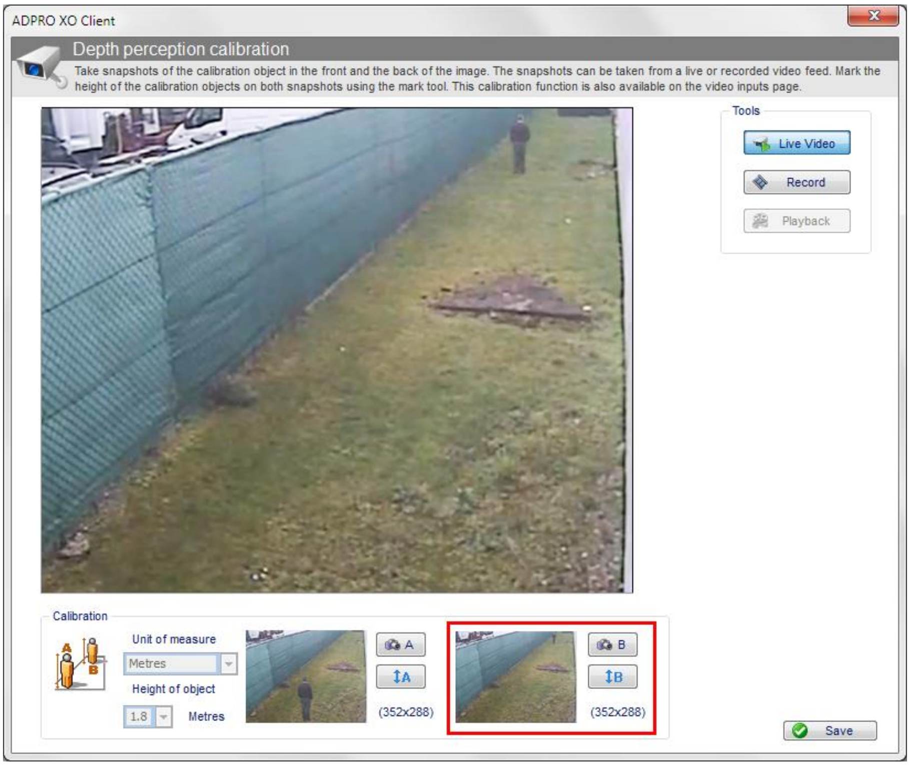
Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

Height of object: 1.8 Metres

(352x288)

5. When the person/object is standing **at the back** of the scene, click B to make a snapshot. Make sure that the person/object is completely visible (from head to toe). A miniature version of the snapshot appears at the bottom of the screen; the system indicates the image resolution.



ADPRO XO Client

Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

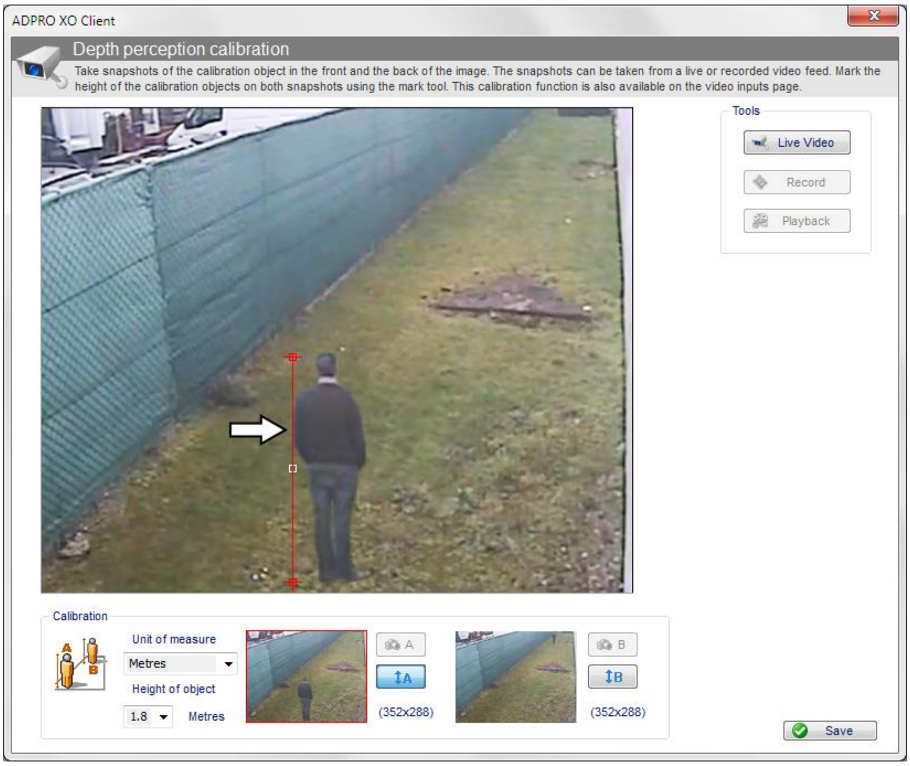
Unit of measure: Metres

Height of object: 1.8 Metres

(352x288) (352x288)

6. To calibrate the front of the scene, you need to draw a marker line with the same height as the object/person in the front: click ↥A. The front snapshot now appears as the camera image.

7. Click the camera image near the top of the person/object, and drag downward to the bottom of the person/object. A vertical, red marker line appears.



ADPRO XO Client

Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

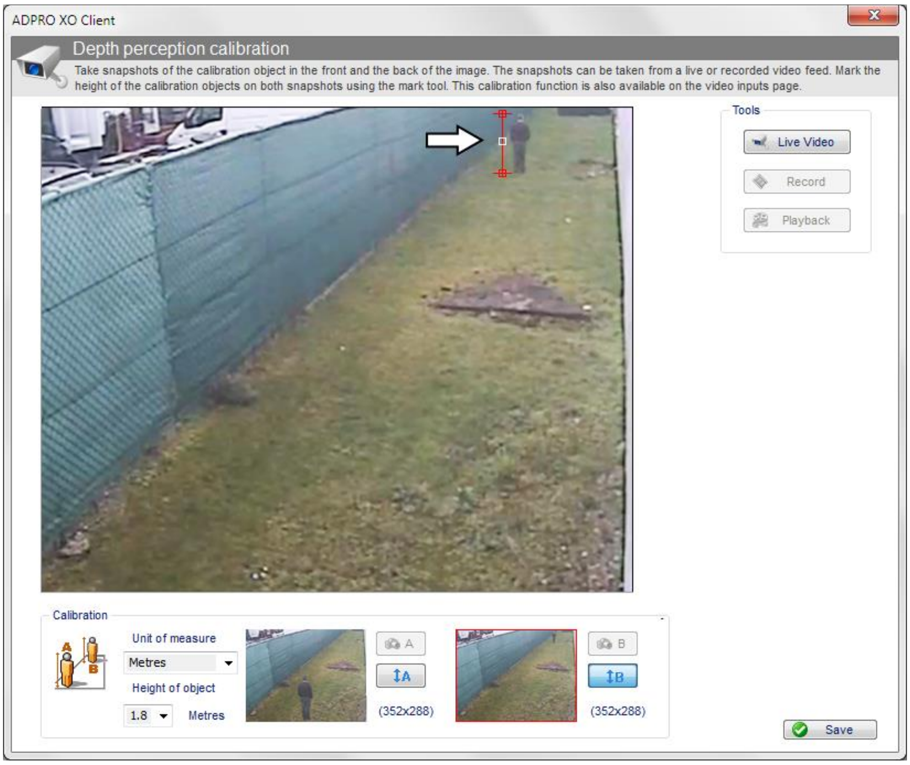
Height of object: 1.8 Metres

(352x288) (352x288)

Note

If you have calibrated the scene before, the vertical red marker is already visible. You only need to adjust it.

8. Adjust the marker line until it has exactly the same height as the person/object at the front, as follows:
   - To move the position of the marker line in the scene, drag it by its white handle in the middle.
   - To change the height of the marker line, drag the red handles at the top and bottom.
9. Click **Save**. You will now calibrate the back of the scene.
10. To calibrate the back of the scene, click ↕B. The back snapshot now appears as the camera image.
11. Click the camera image near the top of the person/object, and drag downward to the bottom of the person/object. A vertical, red marker line appears.



ADPRO XO Client

Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Calibration

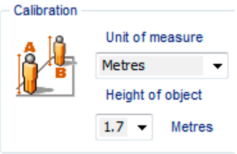
Unit of measure: Metres

Height of object: 1.8 Metres

Note

If you have calibrated the scene before, the vertical red marker is already visible. You only need to adjust it.

12. Adjust the marker line until it has the same height as the person/object at the back.
Next, you will indicate the height of the person/object.
13. Under **Calibration**, in the **Unit of Measure** list, choose the desired unit of measure (metres, yards, or feet). The unit of measure is valid for the back and front of the scene.
14. In the **Height of object** box, select the height of the person/object. Choose the value that is the closest to the person/object's exact height. The height is valid for the back and front of the scene.



Calibration

Unit of measure: Metres

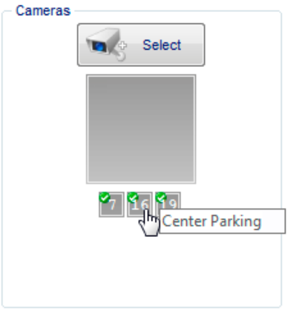
Height of object: 1.7 Metres

15. Click **Save**, and then close the calibration window.

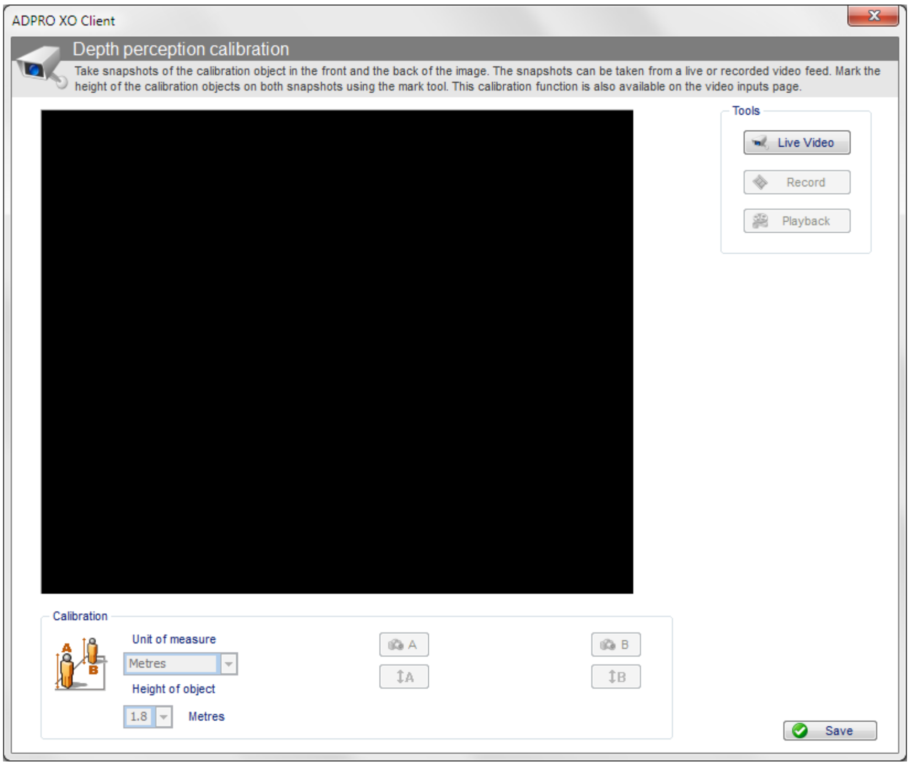
5.2.3 3D Calibration from Recorded Images

To calibrate a scene from recorded images, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. Click the button.

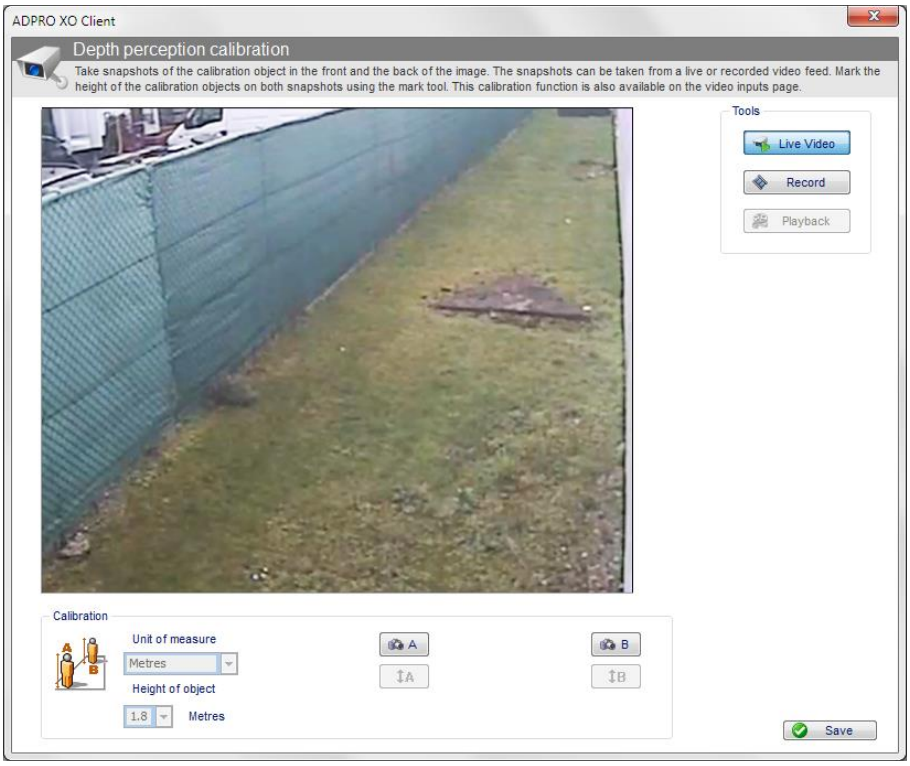


Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

Height of object: 1.8 Metres

3. Under **Tools**, click **Live Video**. The live camera image appears.



ADPRO XO Client

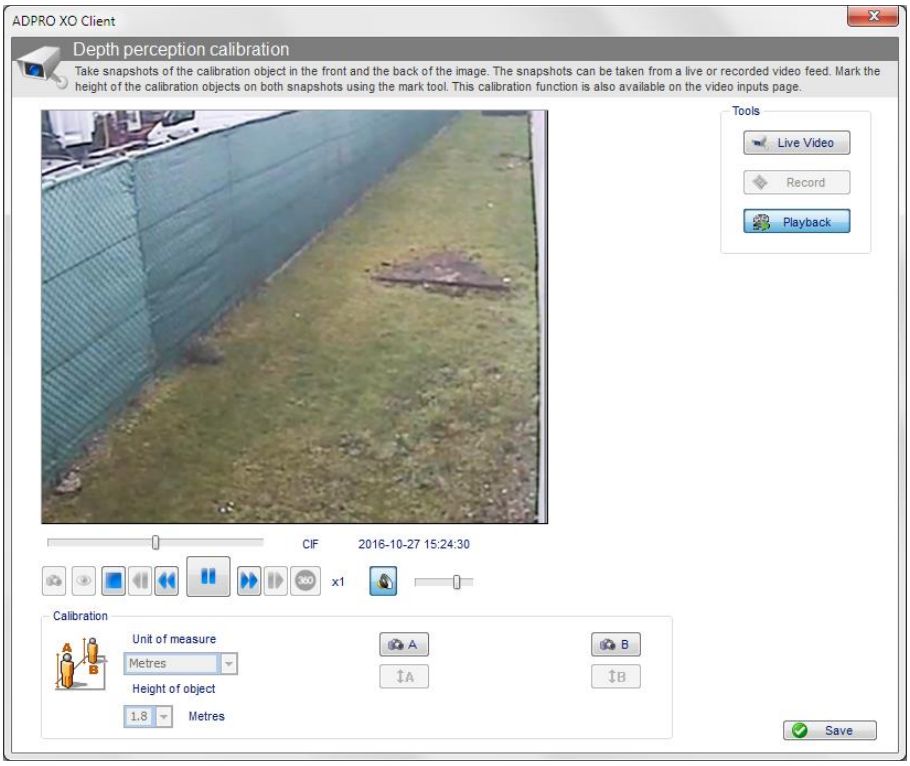
Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

Unit of measure: Metres

Height of object: 1.8 Metres

4. Click **Record**. The system starts recording the live images.
5. While recording, make the person/object stand still at the front and at the back of the scene.
6. When you have the required footage, click **Record** again to stop recording.
7. Click **Playback**. The system starts playing the recorded footage.



ADPRO XO Client

Depth perception calibration

Take snapshots of the calibration object in the front and the back of the image. The snapshots can be taken from a live or recorded video feed. Mark the height of the calibration objects on both snapshots using the mark tool. This calibration function is also available on the video inputs page.

CIF 2016-10-27 15:24:30

Unit of measure: Metres

Height of object: 1.8 Metres

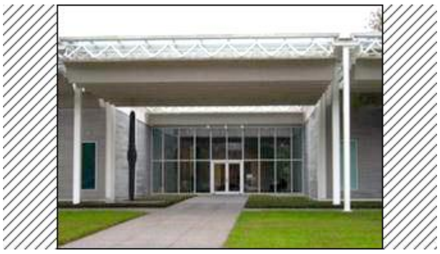
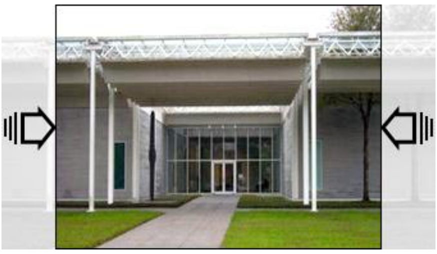
8. Making snapshots and calibrating the scene is identical as for live video. For details, see the procedure in *3D Calibration from Live Images*. Start at step 4 on page 29, and continue to the end.

5.3 Bounding Box Calibration

Bounding box calibration is only required for IP cameras that use different aspect ratios for the analytics stream and the live/recording stream. It makes sure that the analytic bounding boxes appear correctly on all streams, regardless of the aspect ratio.

Ideally, the aspect ratio of the low-resolution analytics stream is identical to the aspect ratio of the high-resolution live/recording streams. However, wide-screen cameras may not offer low-resolution streams with the same aspect ratio.

For example, a camera may offer low-resolution images (for the analytics stream) with aspect ratio 4:3, and high-resolution images with aspect ratio 16:9. Typically, a 4:3 camera image has a narrower field of view than the 16:9 image: the edges are cut off. However, some cameras take the wide image and squeeze it into a narrow image. This results in a full field of view in the 4:3 image, but the image is distorted.

16:9 image	16:9 image
	
4:3 image, cropped: edges are cut off, narrower field of view, image is not distorted	4:3 image, squeezed: full field of view (no cut-off edges), but distorted image

Correct bounding box calibration depends on the way the camera provides the low-resolution stream:

- To calibrate the bounding boxes for cameras that provide **cropped images**: see *Normal Bounding Box Calibration* on page 34.
- To calibrate the bounding boxes for cameras that provide **squeezed images**: see *Bounding Box Calibration for Squeezed Images* on page 36.

> ***Caution!***
>
> Set up the recording stream resolution **before** you calibrate the bounding boxes.

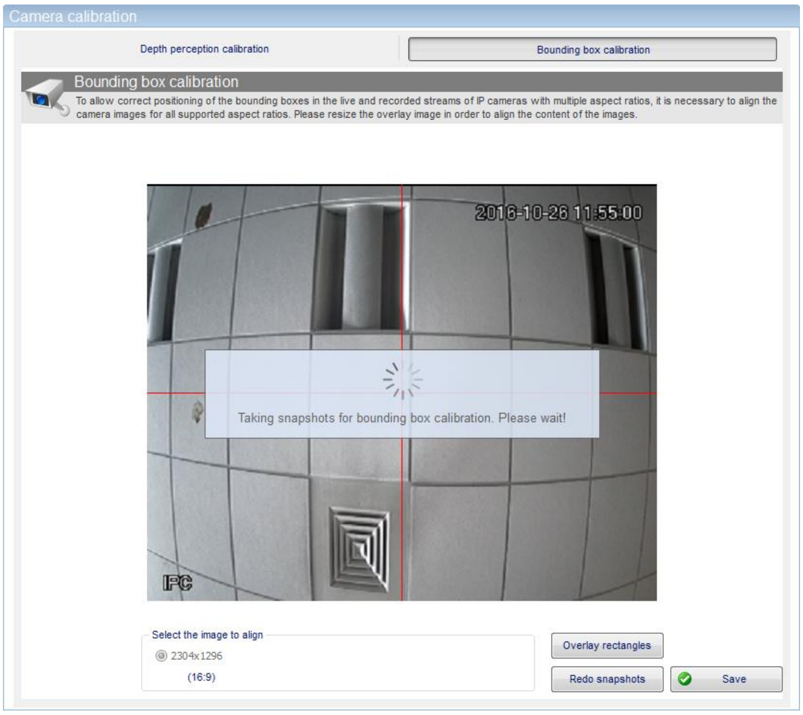
Bounding box calibration is available in firmware version V2.10 and above. If the analytics and recording streams have the same aspect ratio, then bounding box calibration is not required and the option is unavailable.

5.3.1 Normal Bounding Box Calibration

To calibrate the bounding boxes, proceed as follows:

1. Choose **System > Connections > Video Inputs**, and select the desired camera.
2. Under **Video Settings**, click **Camera calibration**.

3. Click the **Bounding box calibration** tab.

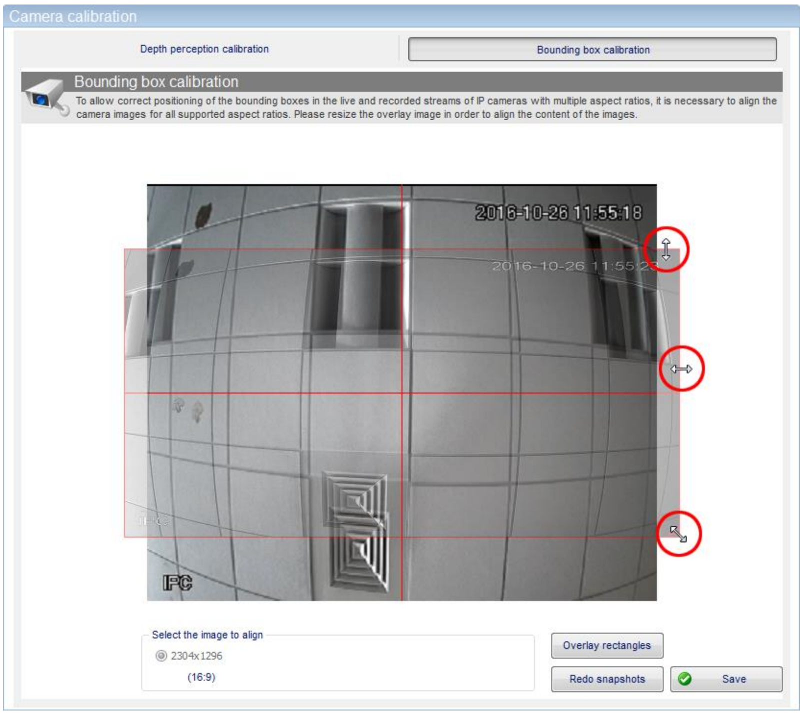


To allow correct positioning of the bounding boxes in the live and recorded streams of IP cameras with multiple aspect ratios, it is necessary to align the camera images for all supported aspect ratios. Please resize the overlay image in order to align the content of the images.

Taking snapshots for bounding box calibration. Please wait!

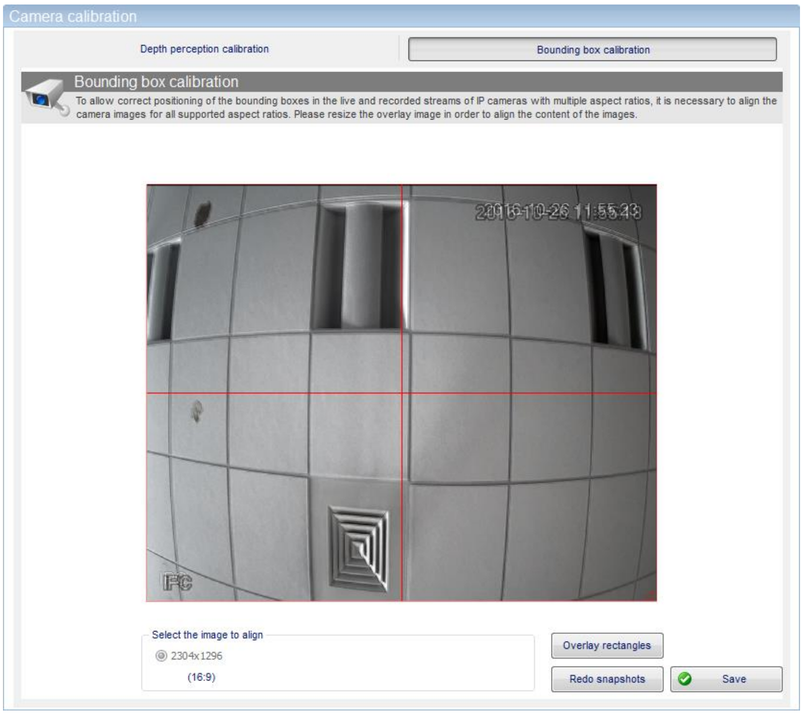
The system takes two screenshots, one at each resolution, and displays them on top of each other.

4. Drag the sides or the corner of the image until both images overlap perfectly.



To allow correct positioning of the bounding boxes in the live and recorded streams of IP cameras with multiple aspect ratios, it is necessary to align the camera images for all supported aspect ratios. Please resize the overlay image in order to align the content of the images.

The result should look like this:



To allow correct positioning of the bounding boxes in the live and recorded streams of IP cameras with multiple aspect ratios, it is necessary to align the camera images for all supported aspect ratios. Please resize the overlay image in order to align the content of the images.

Select the image to align
● 2304x1296 (16:9)

5. Click **Save**, and then close the calibration window.
6. Click **Save**, and then close the calibration window.

5.3.2 Bounding Box Calibration for Squeezed Images

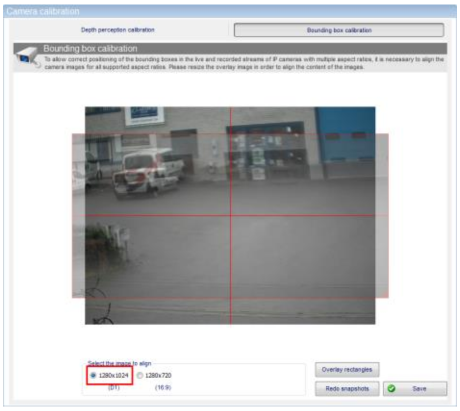
Bounding box calibration for squeezed images is available in firmware version XO 4.0 and above.

To calibrate the bounding boxes for squeezed images, proceed as follows:

1. Choose **System > Connections > Video Inputs**, and select the desired camera.
2. Under **Video Settings**, click **Camera calibration**.
3. Click the **Bounding box calibration** tab. The system takes two snapshots, one at each resolution, and displays them on top of each other.
4. Click **Overlay rectangles**. The system aligns the images automatically.
5. Click **Save**, and then close the calibration window.

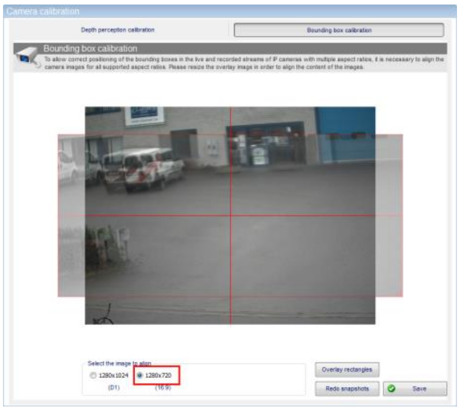
5.3.3 Bounding Box Calibration for Three-stream Cameras

If your camera provides 3 streams, and you have selected 3 different aspect ratios (for analytics, continuous, and event recording), then you have to perform calibration twice. The **Select the image to align** box will display two resolutions. Select each resolution in turn and perform calibration as required.



To allow correct positioning of the bounding boxes in the live and recorded streams of IP cameras with multiple aspect ratios, it is necessary to align the camera images for all supported aspect ratios. Please resize the overlay image in order to align the content of the images.

Select the image to align
● 1280x1024 (D1) ○ 1280x720 (16:9)



To allow correct positioning of the bounding boxes in the live and recorded streams of IP cameras with multiple aspect ratios, it is necessary to align the camera images for all supported aspect ratios. Please resize the overlay image in order to align the content of the images.

Select the image to align
○ 1280x1024 (D1) ● 1280x720 (16:9)

6 Advanced Mode

6.1 About Advanced Mode

Working in the normal, simple mode is suitable for many applications. The simple mode uses a standard set of analytic parameters for the whole scene. If these standard parameters do not suffice, you can work in advanced mode. The following extra functionality is available in advanced mode:

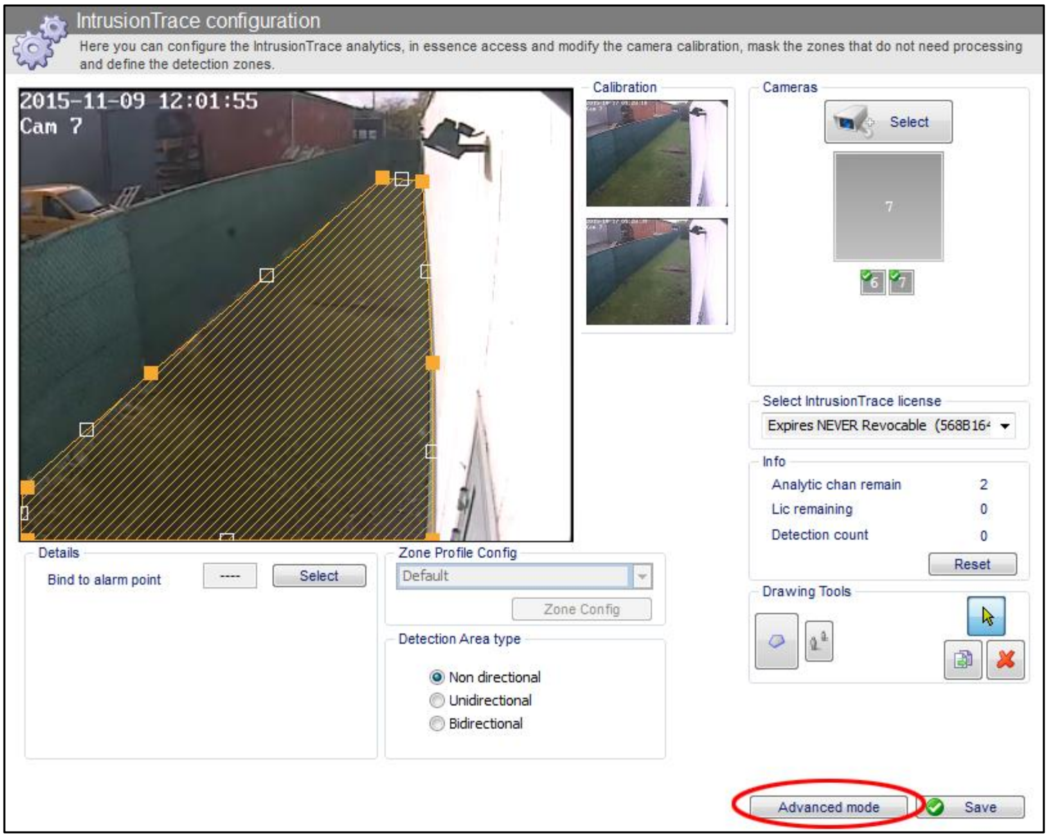
- Mask zones: to exclude certain areas in the camera image from the analysis
- Scene configuration profiles: sets of parameters for the whole scene
- Zone configuration profiles: sets of parameters for individual detection zones.

For each IntrusionTrace-enabled camera, you can choose simple or advanced mode.

6.2 Switching to Advanced Mode

To switch to advanced mode, proceed as follows:

1. Click **Advanced mode**:



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Bind to alarm point ----

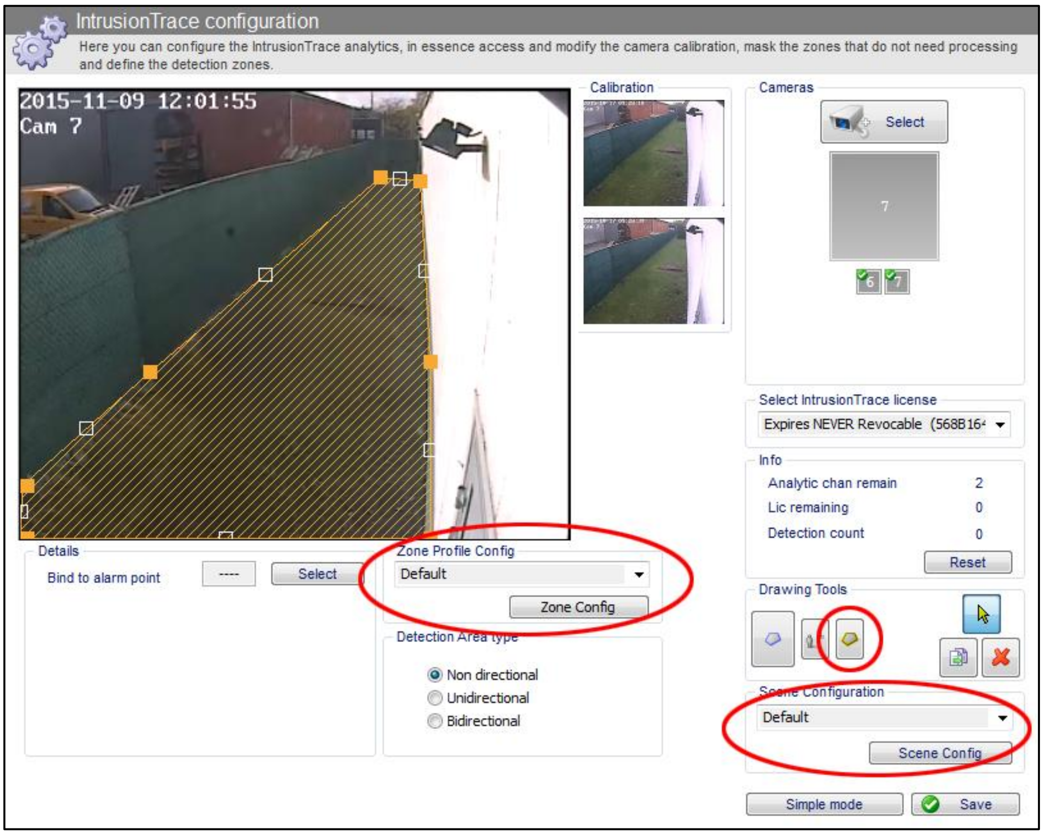
Zone Profile Config: Default

Detection Area type: ● Non directional ○ Unidirectional ○ Bidirectional

Select IntrusionTrace license: Expires NEVER Revocable (568B16‹

Info	
Analytic chan remain	2
Lic remaining	0
Detection count	0

In advanced mode, all functions are available.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

2015-11-09 12:01:55
Cam 7

Details
Bind to alarm point: ----

Zone Profile Config: Default

Detection Area type
- ● Non directional
- ○ Unidirectional
- ○ Bidirectional

Select IntrusionTrace license: Expires NEVER Revocable (568B164

Info
Analytic chan remain 2
Lic remaining 0
Detection count 0

Scene Configuration: Default

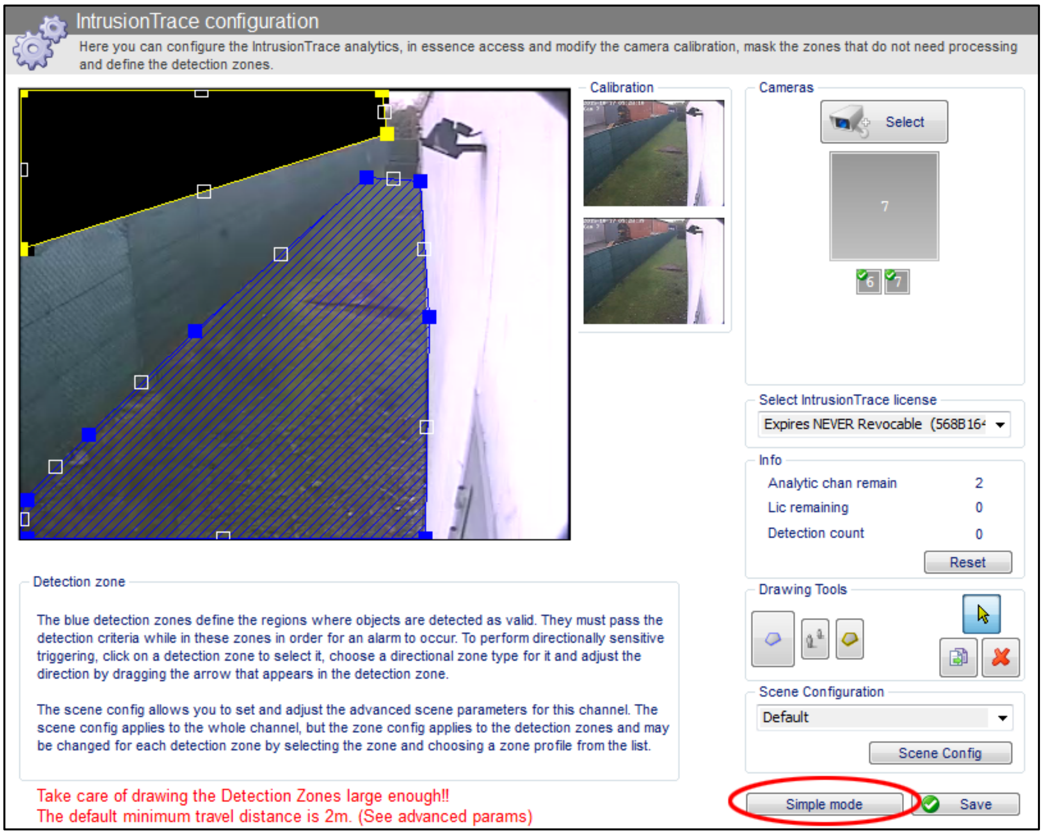
6.3 Switching Back to Simple Mode

When you switch back to simple mode, the system will:

- Delete all mask zones.
- Apply the default profile to the scene.
- Apply the default zone profile to the detection zones.

To switch back to simple mode, proceed as follows:

1. To switch back to simple mode, click **Simple mode**.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Select IntrusionTrace license: Expires NEVER Revocable (568B16‹

Info

Analytic chan remain 2

Lic remaining 0

Detection count 0

Scene Configuration: Default

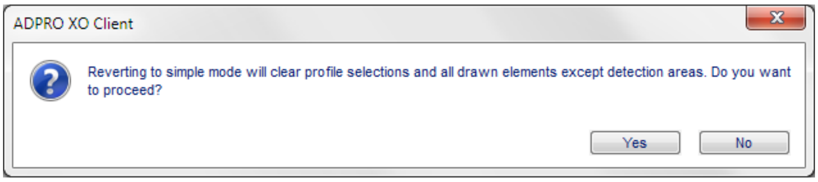
Detection zone

The blue detection zones define the regions where objects are detected as valid. They must pass the detection criteria while in these zones in order for an alarm to occur. To perform directionally sensitive triggering, click on a detection zone to select it, choose a directional zone type for it and adjust the direction by dragging the arrow that appears in the detection zone.

The scene config allows you to set and adjust the advanced scene parameters for this channel. The scene config applies to the whole channel, but the zone config applies to the detection zones and may be changed for each detection zone by selecting the zone and choosing a zone profile from the list.

Take care of drawing the Detection Zones large enough!!
The default minimum travel distance is 2m. (See advanced params)

The following message appears:



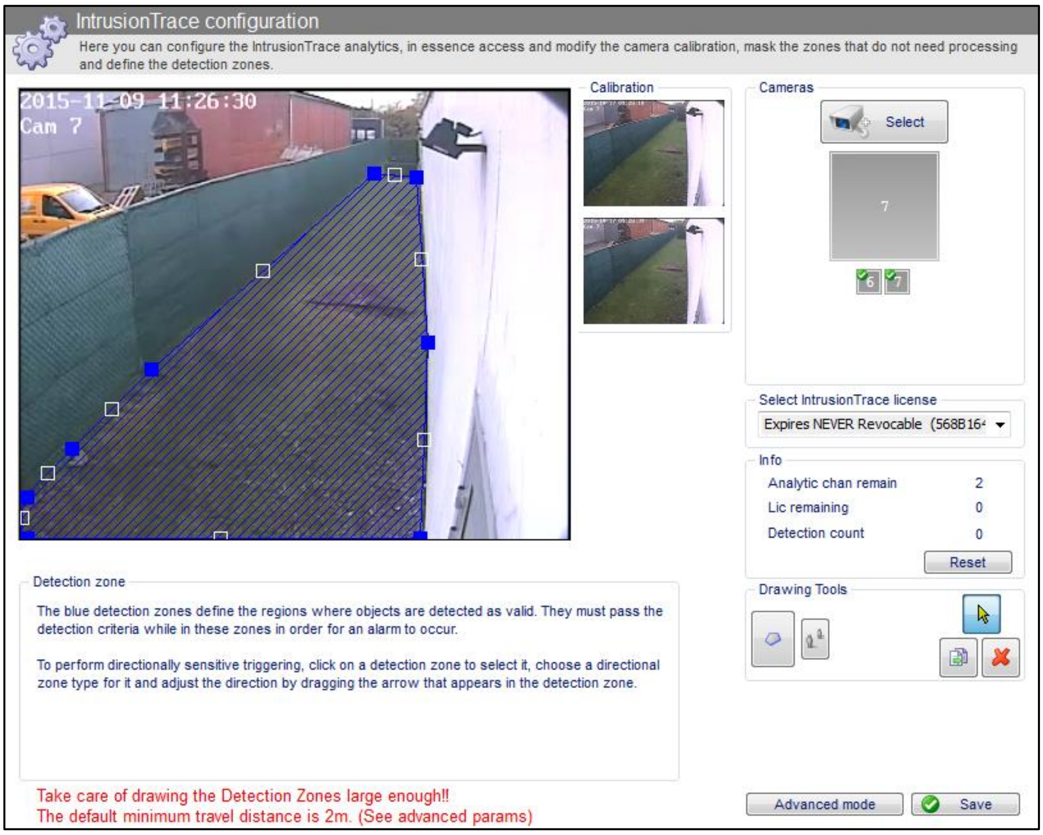
ADPRO XO Client

Reverting to simple mode will clear profile selections and all drawn elements except detection areas. Do you want to proceed?

Caution!

The system will delete all mask zones, and will reset the zone and scene profiles to the default values.

2. Click **Yes** to confirm.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Detection zone

The blue detection zones define the regions where objects are detected as valid. They must pass the detection criteria while in these zones in order for an alarm to occur.

To perform directionally sensitive triggering, click on a detection zone to select it, choose a directional zone type for it and adjust the direction by dragging the arrow that appears in the detection zone.

Take care of drawing the Detection Zones large enough!!
The default minimum travel distance is 2m. (See advanced params)

Select IntrusionTrace license: Expires NEVER Revocable (568B16

Info

Analytic chan remain	2
Lic remaining	0
Detection count	0

7 Detection Profiles

A detection profile is a set of criteria for triggering the intrusion alarm, such as the minimum/maximum size of an object, the time it remains in the detection zone…

By default, IntrusionTrace uses the default detection profile, which is usually suitable for the typical sterile zone scene. However, in advanced mode you can define custom detection profiles to better meet specific needs. From ADPRO firmware version XOa 3.02.0012, these profiles have been split into scene profiles and zone profiles:

- **Scene profile**: an advanced detection profile **for the whole scene**. The parameters in the scene profile apply to all the detection zones in the scene. The scene profile parameters are:
  - Contrast sensitivity
  - Object sensitivity
  - Time OR distance acceptance, with minimum time and minimum distance
  - Multiple detection filtering, with maximum time and maximum distance.
- **Zone profile**: an individual detection profile **for a specific detection zone** in the scene. The parameters in the zone profile apply only to that particular zone.
  - Minimum and maximum width of the object
  - Minimum and maximum height of the object
  - Minimum and maximum area of the object
  - Minimum and maximum speed of the object
  - Time AND distance acceptance, with minimum time and minimum distance
  - PTZ follow mode.
- **i-LIDS profile**: if you require an i-LIDS certified installation. The i-LIDS profile has certain restrictions. For details, see *i-LIDS Certified Detection* on page 54.

Each parameter is described in detail in the following chapters.

Caution!

The default profile is designed to detect a range of intrusion types over a range of conditions while ignoring a range of false alarm sources. Any deviation from the default profile risks affecting performance. You must verify performance with comprehensive walk tests of the site.

If you do need custom detection profiles, then keep the default values as much as possible, and adjust only the one or two parameters that make the difference for the issue you are facing. For guidelines to adjust parameters for difficult scenes, see the *IntrusionTrace Best Practices* guide (26033).

Note

If you had been using custom detection profiles with an ADPRO firmware version below XOa 3.02.0012, the system will automatically convert these profiles into scene and zone profiles when you upgrade to XOa 3.02.0012 or above.

8 Scene Profiles

8.1 Scene Profile Settings

8.1.1 Contrast and Object Sensitivity

As of software version XOa 3.02.0012, the IntrusionTrace sensitivity setting is split up in the following parts:

- **Contrast sensitivity**: determines the minimum contrast needed between an image point and the background to belong to an ‘object’.
  The higher the contrast sensitivity, the less contrast is needed to be an object.
- **Object sensitivity**: determines if the object is a ‘real’ object (human, vehicle…) or a disturbance (cloud shadow, blurred spider, lighting change…). To determine this, the system uses criteria such as object edges, object blur, etc.
  The higher the object sensitivity, the more objects are considered real.

Each sensitivity setting has 5 levels (1–5). Combining both sensitivity settings gives you 25 sensitivity levels, providing more control to suppress false alarms.

Note

With firmware versions below XOa 3.02.0012, there is only one general sensitivity setting with three levels (1 = low, 2 = normal, and 3 = high). When upgrading from below XOa 3.02.0012, the system converts the old sensitivity level to the new sensitivity settings as follows:

- From **1 = low** to contrast and object sensitivity **1 = low**
- From **2 = normal** to contrast and object sensitivity **3 = normal**
- From **3 = high** to contrast and object sensitivity **5 = high**.

8.1.2 Time OR Distance

Enable the time OR distance acceptance, if you want to generate an alarm as soon as **one of the conditions** below is fulfilled:

- The object spent longer than a minimum time (in seconds) in the scene.
- The object moved farther than a minimum distance (in metres) in the scene.

This setting is useful to detect people approaching a secured fence, either by running fast or by crawling slowly:

- If they run fast, they do not stay long enough in the scene to trigger on time, but the distance they travel will trigger the alarm.
- If they crawl slowly, they take too long to travel a small distance to trigger on distance, but the time they spend will trigger the alarm.

8.1.3 Multiple Detection Filtering

To avoid repetition of alarms, use multiple detection filtering. If IntrusionTrace detects an intruder, and then a second time within a specified time (in seconds) and distance (in metres), the system will not generate a second alarm.

Caution!

Xtralis recommends to keep multiple detection filtering enabled, because it prevents the CMS from being flooded with alarms from the same camera when there are multiple activities there.

You set the maximum time (in seconds) between two detections, and the maximum distance (in metres) between two detections.

For example: the maximum time = 10 seconds, and the maximum distance is 10 m.
If the same alarm occurs within 10 seconds of the start of the first alarm, there will be no second alarm. If the same alarm occurs after 11 seconds, there will be a new alarm.

If the same alarm occurs 9 m farther, there will be no second alarm. If the same alarm occurs 11 m farther, there will be a new alarm.

8.2 Default Scene Profile

The table below lists the settings in the default scene profile. You cannot change the default profile.

Parameter	Default value
Contrast sensitivity	3 (= normal)
Object sensitivity	3 (= normal)
Time OR distance acceptance	0 (disabled)
• Minimum time (if enabled)	4 seconds
• Minimum distance (if enabled)	4 metres
Multiple detection filtering	1 (enabled)
• Maximum time	10 seconds
• Maximum distance	4 metres

8.3 Creating a Custom Scene Profile

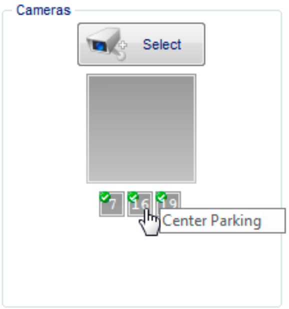
If the default scene profile is not suitable, you can create your own custom scene profile. If need be, you can create different scene profiles for different cameras. Any scene profile that you create is available to all IntrusionTrace-enabled cameras on the XO device, except the cameras that use i-LIDS certified detection.

> ***Caution!***
>
> If you assign the same scene profile to different cameras, make sure to test the settings on all these cameras.

To get a feel for how the different settings influence detection, adjust only one setting at a time, and then test detection.

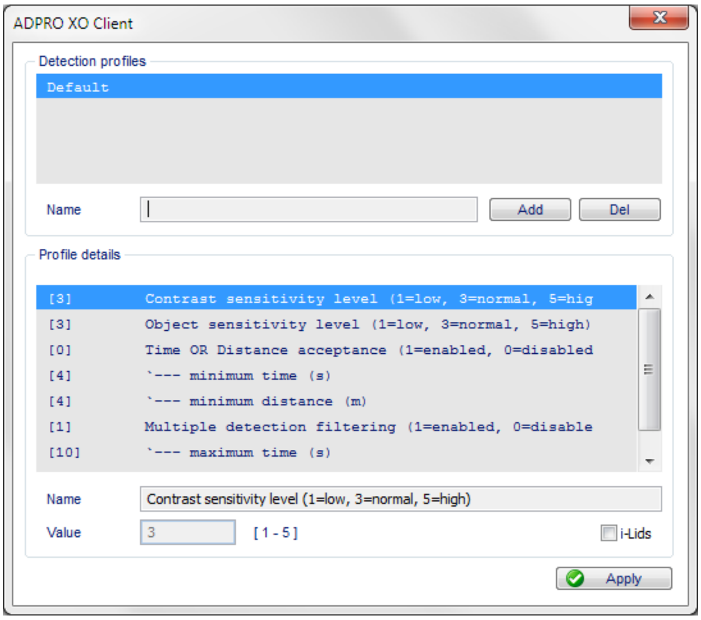
To create a custom scene profile, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.

3. Under **Scene Configuration**, click **Scene Config**.



ADPRO XO Client

Detection profiles

```
Default
```

Name:

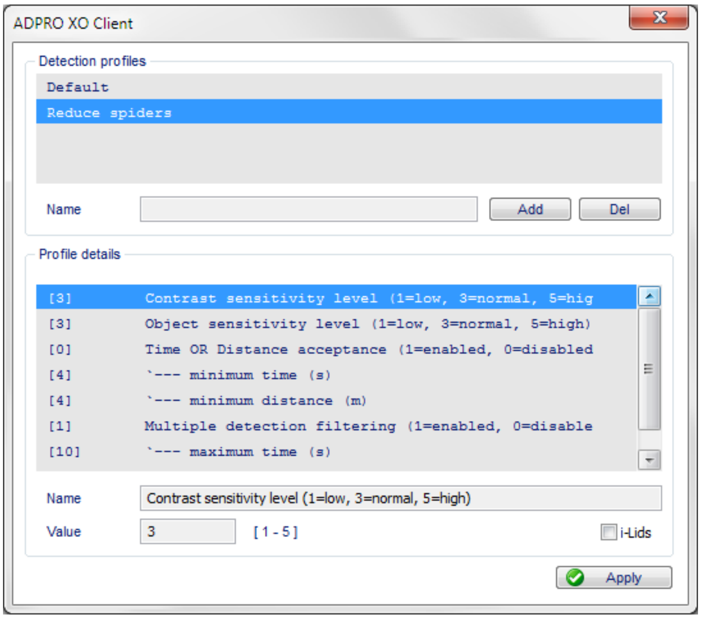
Profile details

```
[3]      Contrast sensitivity level (1=low, 3=normal, 5=hig
[3]      Object sensitivity level (1=low, 3=normal, 5=high)
[0]      Time OR Distance acceptance (1=enabled, 0=disabled
[4]      `--- minimum time (s)
[4]      `--- minimum distance (m)
[1]      Multiple detection filtering (1=enabled, 0=disable
[10]     `--- maximum time (s)
```

Name: Contrast sensitivity level (1=low, 3=normal, 5=high)

Value: 3 [1 - 5] □ i-Lids

4. In the **Name** box, type a meaningful name for your custom profile.
5. Click **Add**. The system adds a profile with the chosen name and the default settings.



ADPRO XO Client

Detection profiles

```
Default
Reduce spiders
```

Name:

Profile details

```
[3]      Contrast sensitivity level (1=low, 3=normal, 5=hig
[3]      Object sensitivity level (1=low, 3=normal, 5=high)
[0]      Time OR Distance acceptance (1=enabled, 0=disabled
[4]      `--- minimum time (s)
[4]      `--- minimum distance (m)
[1]      Multiple detection filtering (1=enabled, 0=disable
[10]     `--- maximum time (s)
```

Name: Contrast sensitivity level (1=low, 3=normal, 5=high)

Value: 3 [1 - 5] □ i-Lids

The **Profile details** list shows all the settings, and their current value on the left between brackets.

6. To adjust a setting: under **Profile details**, click the desired setting. The setting's name appears in the **Name** box below the **Profile details** list. (You cannot change the setting's name).
The current value appears in the **Value** box. The possible range of values appears to the right of the **Value** box.
7. In the **Value** box, type the desired value for the setting.
8. Repeat for all the settings. The options are as follows:

Setting	Description
Contrast sensitivity level	Set to any round number from 1 to 5.
Object sensitivity level	Set to any round number from 1 to 5.
Time OR distance acceptance	Set to 1 to enable; set to 0 to disable.
• **Minimum time (s)**	Set to any value (in seconds) from 0 to 99.9. You can use one decimal, for example: 0.5
• **Minimum distance (m)**	Set to any value (in metres) from 0 to 99.9. You can use one decimal.

Setting	Description
Multiple detection filtering	Set to 1 to enable; set to 0 to disable.
• **Maximum time (s)**	Set to any value (in seconds) from 0 to 999.9. You can use one decimal.
• **Maximum distance (m)**	Set to any value (in metres) from 0 to 99.9. You can use one decimal.

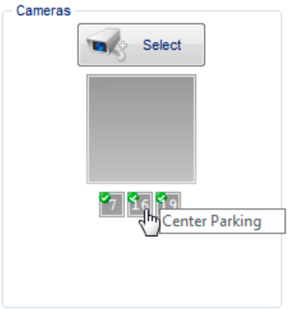
9. Click **Apply** to save the changes, and then close the profile window. The system automatically assigns the new profile to the scene.
10. Click **Save**.
11. Test the settings, and adjust if necessary. For more information on testing, see *Testing the IntrusionTrace Configuration* on page 62.

8.4 Assigning Existing Profiles to Cameras

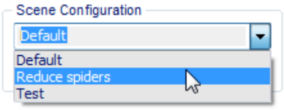
Once you have created a scene profile, you can assign it to any IntrusionTrace-enabled camera on the XO device (except for the cameras that use i-LIDS certified detection).

To assign an existing profile to a camera, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Under **Scene Configuration**, select the desired profile from the list.



4. Click **Save**.

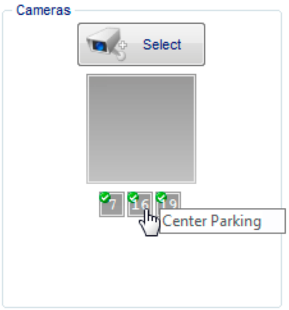
8.5 Changing an Existing Scene Profile

Note

You cannot change the default scene profile; it is fixed.

To change an existing scene profile, proceed as follows:

1. From the IntrusionTrace configuration window, click a camera that uses the desired scene profile.



2. Under **Scene Configuration**, click **Scene Config**.
3. Under **Profile details**, click the desired setting, and adjust its value in the **Value** box.
4. Click **Apply** to save the changes, and then close the profile window.
5. Click **Save**.
6. Test the new settings, and adjust again if necessary.

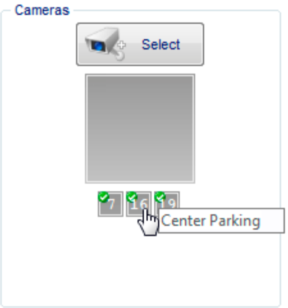
> ***Caution!***
>
> If you have assigned the same scene profile to different cameras, make sure to test the settings on all these cameras.

8.6 Deleting a Scene Profile

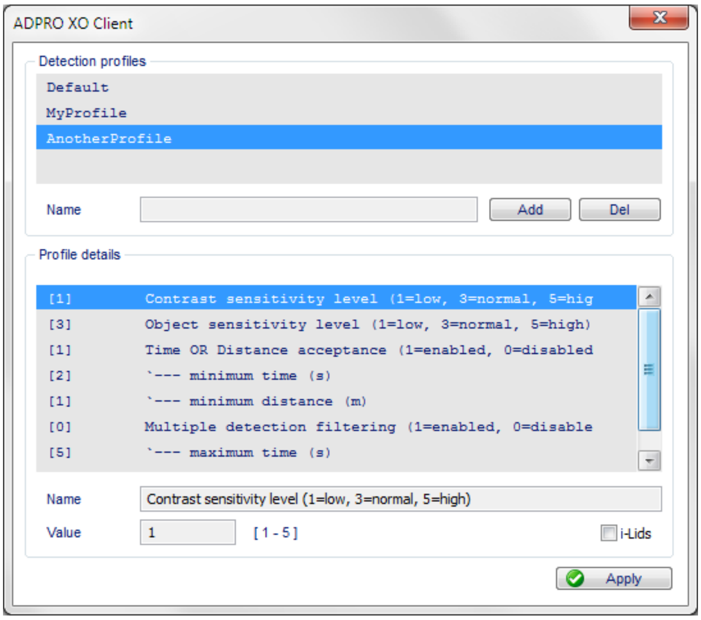
> ***Note***
>
> You cannot delete the default scene profile, or a custom scene profile that is still assigned to a camera. Make sure that all IntrusionTrace-enabled cameras on the XO device use a different profile (or the default profile).

To delete a scene profile, proceed as follows:

1. From the IntrusionTrace configuration window, click any camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Under **Scene Configuration**, click **Scene Config**.
4. Under **Detection profiles**, click the desired profile.



ADPRO XO Client

Detection profiles

```
Default
MyProfile
AnotherProfile
```

Name [ ] Add Del

Profile details

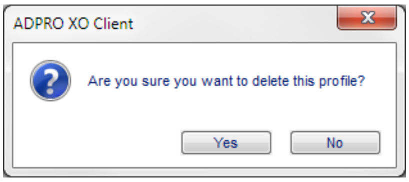
```
[1]        Contrast sensitivity level (1=low, 3=normal, 5=hig
[3]        Object sensitivity level (1=low, 3=normal, 5=high)
[1]        Time OR Distance acceptance (1=enabled, 0=disabled
[2]        `--- minimum time (s)
[1]        `--- minimum distance (m)
[0]        Multiple detection filtering (1=enabled, 0=disable
[5]        `--- maximum time (s)
```

Name: Contrast sensitivity level (1=low, 3=normal, 5=high)

Value: 1 [1 - 5] □ i-Lids

Apply

5. Click **Del**. The following message appears:



ADPRO XO Client

Are you sure you want to delete this profile?

6. Click **Yes** to confirm.
7. Click **Apply** to save the changes, and then close the profile window.
8. Click **Save**.

9 Zone Profiles

9.1 Zone Profile Settings

9.1.1 Minimum and Maximum Width

Set a minimum width to prevent detection of thin objects. An object will only generate an alarm if it is wider than the minimum width. The minimum width is expressed in metres.
For detecting humans, a typical minimum width is 0.3 metres.

Set a maximum width to prevent detection of large objects. An object will only generate an alarm if it is less wide than the maximum width. The maximum width is expressed in metres.
The default value is suitable for detecting vehicles.

9.1.2 Minimum and Maximum Height

Set the minimum height to prevent detection of small objects. An object will only generate an alarm if it is taller than the minimum height. The minimum height is expressed in metres.
For detecting humans, a typical minimum height is 0.3 metres, because they may be crawling or rolling.

Set the maximum height to prevent detection of tall objects. An object will only generate an alarm if it is smaller than the maximum height. The maximum height is expressed in metres.
For detecting vehicles, a typical maximum height is 5 metres. This value allows for detecting vehicles and their shadows.

9.1.3 Minimum and Maximum Area

Set the minimum area to prevent detection of small objects. An object will only generate an alarm if its surface is larger than the minimum area. The value is expressed in square meters.
For detecting humans, a typical minimum area is 0.09 square meters, because a rolling human may have a very small surface (0.3 m width x 0.3 m height).

Set the maximum area to prevent detection of large objects. An object will only generate an alarm if its surface is smaller than the maximum area. The value is expressed in square metres.
For detecting vehicles, a typical maximum area is 20 square meters (4 m width x 5 m height).

9.1.4 Minimum and Maximum Speed

Set the minimum speed to prevent detection of slow objects. An object will only generate an alarm if it moves faster than the minimum speed. The value is expressed in metres per second (m/s).

Set the maximum speed to prevent detection of fast objects. An object will only generate an alarm if it moves slower than the maximum speed. The value is expressed in metres per second (m/s).
For detecting humans and slow vehicles, a typical maximum speed is 12 metres per second (43 km/h).

9.1.5 Time AND Distance

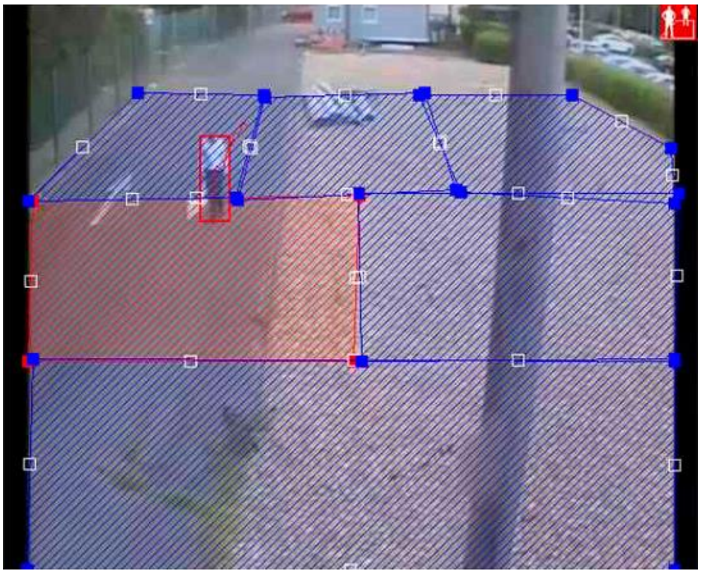
Enable the time AND distance acceptance, if you want to generate an alarm only if **both the conditions** below are fulfilled:

- The object spent longer than a minimum time (in seconds) in the detection zone.
- The object moved farther than a minimum distance (in metres) in the detection zone.

The default values allow for reducing alarms from swaying trees, flags, or shadows.

9.1.6 PTZ Follow Mode

You use the PTZ follow mode for tracking objects. With PTZ follow mode enabled, an object that is already in alarm will immediately trigger any zone it enters, thereby allowing the events from each zone in turn to drive a PTZ camera to consecutive presets. The PTZ camera then 'follows' the object quickly and reliably.



PTZ follow mode is enabled: the object in alarm immediately triggers the zone on entry.

If you disable PTZ follow mode, then the object has to meet all the criteria for each consecutive zone that it passes through. In this case, it will take longer for each zone to trigger, because the object has to travel the minimum distance in the zone and be in the zone for long enough. The PTZ camera may then not be able to follow the object quick enough.
Disabling PTZ follow mode may be useful if you are using different zones with different detection criteria. This can prevent zones being triggered that would not normally have been triggered.

The PTZ follow mode option is available from ADPRO firmware version XOa 3.02.0012. In previous versions, you cannot disable the PTZ follow mode; it is always active.

9.2 Default Detection Zone Profile

The table below lists the settings in the default zone profile. You cannot change the default profile.

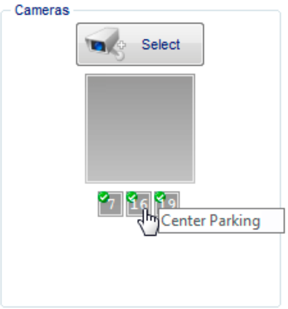
Parameter	Default value
Minimum width	0.3 metres
Maximum width	5.5 metres
Minimum height	0.3 metres
Maximum height	5 metres
Minimum area	0.09 square metres
Maximum area	20 square metres
Minimum speed	0 m/s
Maximum speed	12 m/s
Time AND distance acceptance	1 (enabled)
• Minimum time	0.5 seconds
• Minimum distance	2 metres
PTZ follow mode	1 (enabled)

9.3 Creating a Custom Zone Profile

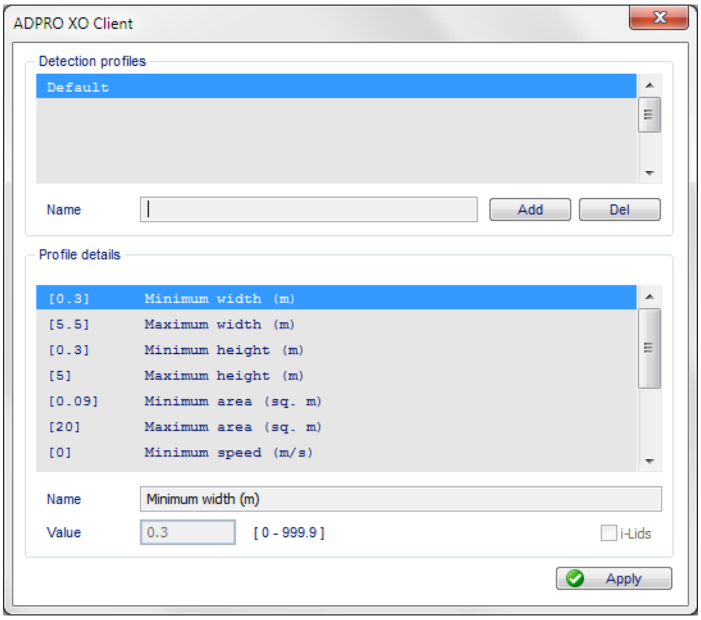
If the default zone profile is not suitable, you can create your own custom zone profile. If need be, you can create different zone profiles for different zones. Any zone profile that you create is available to all detection zones on all IntrusionTrace-enabled cameras on the XO device, except on the cameras that use i-LIDS certified detection.

To create a custom detection zone profile, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Click the desired detection zone.
4. Under **Zone Profile Config**, click **Zone Config**.



ADPRO XO Client

Detection profiles

Default

Name □ Add Del

Profile details

[0.3]	Minimum width (m)
[5.5]	Maximum width (m)
[0.3]	Minimum height (m)
[5]	Maximum height (m)
[0.09]	Minimum area (sq. m)
[20]	Maximum area (sq. m)
[0]	Minimum speed (m/s)

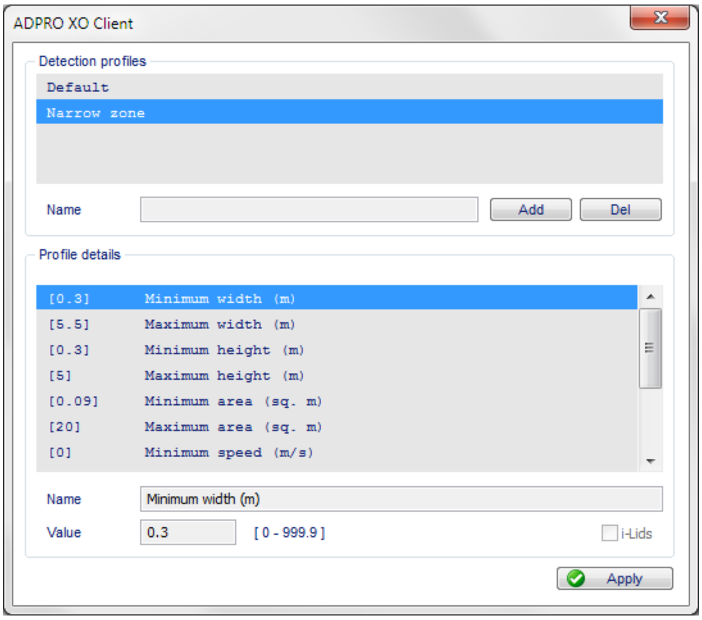
Name: Minimum width (m)

Value: 0.3 [0 - 999.9] □ i-Lids

Apply

5. In the **Name** box, type a meaningful name for your custom profile.

6. Click **Add**. The system adds a profile with the chosen name and the default settings.



ADPRO XO Client

Detection profiles

Default
Narrow zone

Name □ Add Del

Profile details

```
[0.3]     Minimum width (m)
[5.5]     Maximum width (m)
[0.3]     Minimum height (m)
[5]       Maximum height (m)
[0.09]    Minimum area (sq. m)
[20]      Maximum area (sq. m)
[0]       Minimum speed (m/s)
```

Name: Minimum width (m)

Value: 0.3 [0 - 999.9] □ i-Lids

Apply

The **Profile details** list shows all the settings, and their current value on the left between brackets.

7. To adjust a setting: under **Profile details**, click the desired setting. The setting's name appears in the **Name** box below the **Profile details** list. (You cannot change the setting's name).
The current value appears in the **Value** box. The possible (range of) values appears to the right of the **Value** box.

8. In the **Value** box, type the desired value for the setting.

9. Repeat for all the settings. The options are as follows:

Setting	Description
Minimum width (m)	Set to any value (in metres) from 0 to 999.9. You can use one decimal, for example: 0.2
Maximum width (m)	Set to any value (in metres) from 0 to 999.9. You can use one decimal.
Minimum height (m)	Set to any value (in metres) from 0 to 99.9. You can use one decimal.
Maximum height (m)	Set to any value (in metres) from 0 to 99.9. You can use one decimal.
Minimum area (sq. m)	Set to any value (in square metres, m²) from 0 to 99.99. You can use two decimals, for example: 0.09
Maximum area (sq. m)	Set to any value (in square metres, m²) from 0 to 99.99. You can use two decimals.
Minimum speed (m/s)	Set to any value (in metres per second) from 0 to 999.9. You can use one decimal.
Maximum speed (m/s)	Set to any value (in metres per second) from 0 to 999.9. You can use one decimal.
Time AND distance acceptance	Set to 1 to enable; set to 0 to disable.
• **Minimum time (s)**	Set to any value (in seconds) from 0 to 99.9. You can use one decimal.
• **Minimum distance (m)**	Set to any value (in metres) from 0 to 99.9. You can use one decimal.
PTZ follow mode	Set to 1 to enable; set to 0 to disable.

10. Click **Apply** to save the changes, and then close the profile window. The system automatically assigns the new profile to the scene.

11. Click **Save**.

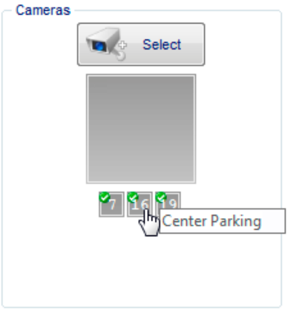
12. Test the settings, and adjust if necessary. For more information on testing, see *Testing the IntrusionTrace Configuration* on page 62.

9.4 Assigning Existing Profiles to Detection Zones

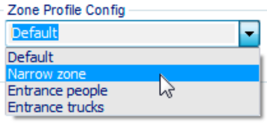
Once you have created a zone profile, you can assign it to any detection zone on any camera on the XO device (except for the cameras that use i-LIDS certified detection).

To assign an existing profile to a detection zone, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Click the desired detection zone.
4. Under **Zone Profile Config**, select the desired profile from the list.



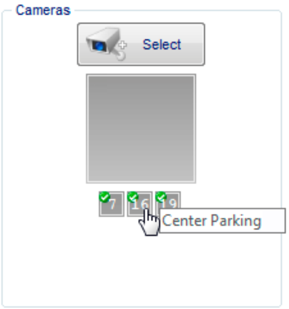
5. Click **Save**.

9.5 Changing an Existing Zone Profile

> ***Note***
>
> You cannot change the default zone profile; it is fixed.

To change an existing zone profile, proceed as follows:

1. From the IntrusionTrace configuration window, click the camera that uses the desired zone profile.



2. Click the desired detection zone.
3. Under **Zone Profile Config**, click **Zone Config**.
4. Under **Profile details**, click the desired setting, and adjust its value in the **Value** box.
5. Click **Apply** to save the changes, and then close the profile window.
6. Click **Save**.
7. Test the new settings, and adjust again if necessary.

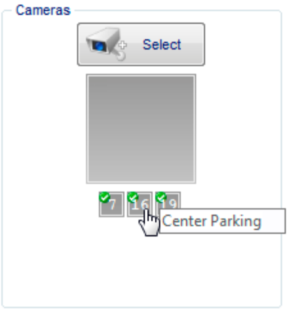
> ***Caution!***
>
> If you have assigned the same zone profile to different detection zones, make sure to test the settings on all these detection zones, on all the IntrusionTrace-enabled cameras.

9.6 Deleting a Zone Profile

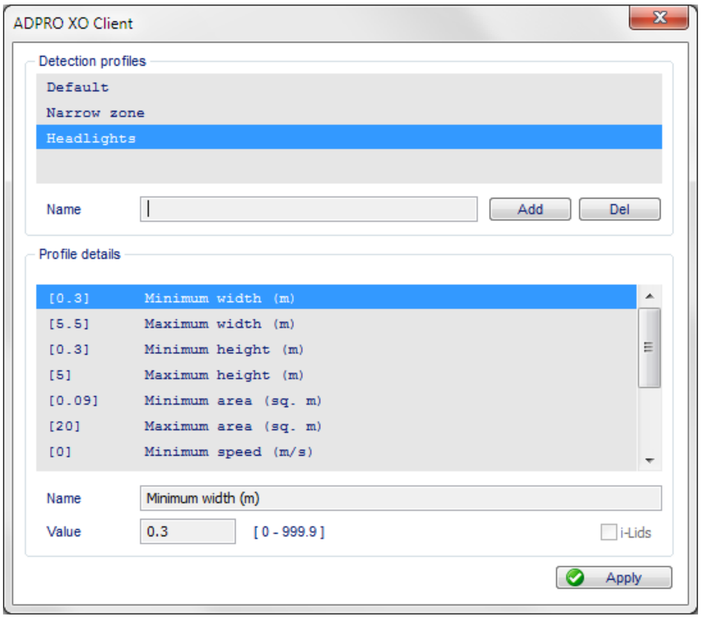
> ***Note***
>
> You cannot delete the default zone profile, or a custom zone profile that is still assigned to a detection zone. Make sure that all the detection zones for all IntrusionTrace-enabled cameras on the XO device use a different profile (or the default profile).

To delete a zone profile, proceed as follows:

1. From the IntrusionTrace configuration window, click any camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Click any detection zone.
4. Under **Zone Profile Config**, click **Zone Config**.
5. Under **Detection profiles**, select the desired profile.



Default
Narrow zone
Headlights

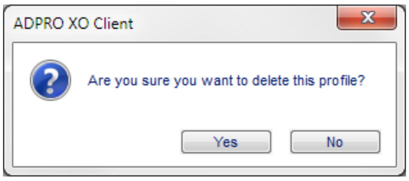
Name

[0.3]	Minimum width (m)
[5.5]	Maximum width (m)
[0.3]	Minimum height (m)
[5]	Maximum height (m)
[0.09]	Minimum area (sq. m)
[20]	Maximum area (sq. m)
[0]	Minimum speed (m/s)

Name Minimum width (m)

Value 0.3 [0 - 999.9] □ i-Lids

6. Click **Del**. The following message appears:



Are you sure you want to delete this profile?

7. Click **Yes** to confirm.
8. Click **Apply** to save the changes, and then close the profile window.
9. Click **Save**.

10 i-LIDS Certified Detection

10.1 About i-LIDS Certified Detection

If the installation requires i-LIDS certification, then you can use IntrusionTrace's i-LIDS certified engine for detection. The i-LIDS certified engine has the following restrictions:

- It uses the general sensitivity setting. There is no separate contrast and object sensitivity.
- All other parameters work as they are described in the scene and zone profiles in this manual; except that they are always valid for the whole scene.
- You cannot use the custom scene profiles created for non-i-LIDS detection.
- You cannot use custom profiles per detection zone.

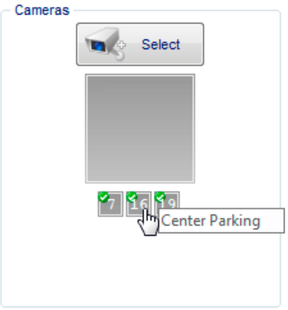
For each IntrusionTrace-enabled camera on the XO device, you can choose to use normal or i-LIDS certified detection. When switching to i-LIDS certified detection on a camera, keep the following in mind:

- The system will unlink all assigned zone profiles (if any) from the existing detection zones. The system keeps the zone profiles; they remain available for cameras without i-LIDS certified detection.
- The system preserves the directionality of the existing detection zones.
- The system preserves the analytic detail inputs assigned to existing detection zones.

10.2 Enabling i-LIDS Certified Detection

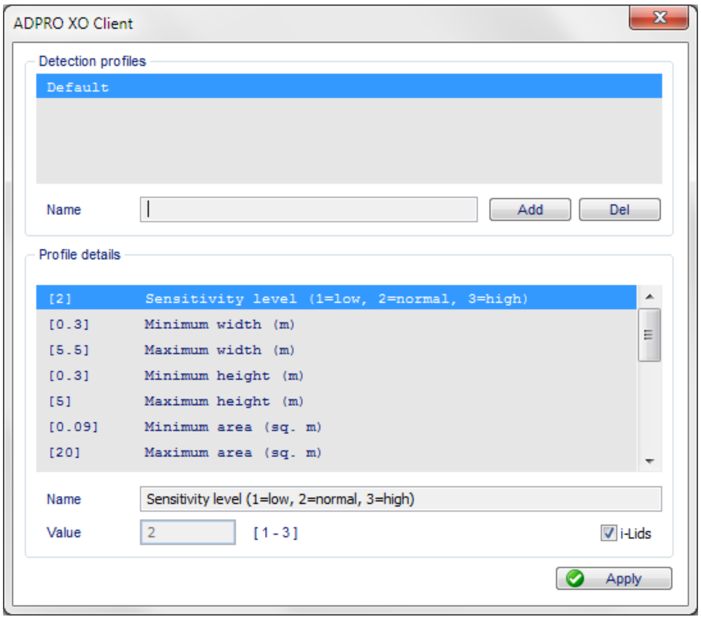
To enable i-LIDS certified detection, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Under **Scene Configuration**, click **Scene Config**.

4. Select the **i-Lids** check box.



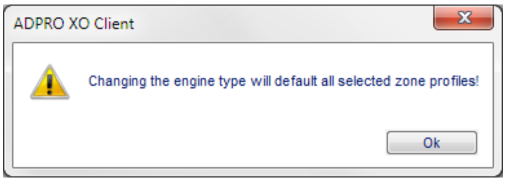
```
[2]       Sensitivity level (1=low, 2=normal, 3=high)
[0.3]     Minimum width (m)
[5.5]     Maximum width (m)
[0.3]     Minimum height (m)
[5]       Maximum height (m)
[0.09]    Minimum area (sq. m)
[20]      Maximum area (sq. m)
```

Name: Sensitivity level (1=low, 2=normal, 3=high)

Value: 2 [1 - 3] ☑ i-Lids

The system removes all custom scene detection profiles from the list, and activates the default profile for i-LIDS certified detection.

5. Click **Apply** to save the changes, and then close the profile window. The following message appears:



Changing the engine type will default all selected zone profiles!

6. Click **OK** to confirm.

7. Click **Save**.

10.3 Default i-LIDS Detection Profile

The table below indicates the settings in the default i-LIDS detection profile.

Parameter	Default value
Sensitivity level	2 = normal
Minimum width Maximum width	0.3 metres 5.5 metres
Minimum height Maximum height	0.3 metres 5 metres
Minimum area Maximum area	0.09 square metres 20 square metres
Minimum speed Maximum speed	0 m/s 12 m/s
Time AND distance acceptance	1 (enabled)
• Minimum time	0.5 seconds
• Minimum distance	2 metres
Time OR distance acceptance	0 (disabled)
• Minimum time (if enabled)	4 seconds
• Minimum distance (if enabled)	4 metres

Parameter	Default value
Multiple detection filtering	1 (enabled)
• Maximum time	10 seconds
• Maximum distance	4 metres

10.4 Creating a Custom i-LIDS Detection Profile

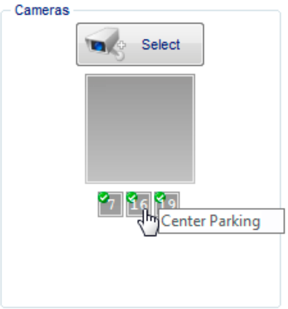
If the default i-LIDS profile is not suitable, you can create your own custom profile. If need be, you can create different profiles for different cameras. Any i-LIDS profile that you create is available to all IntrusionTrace-enabled cameras on the XO device that use i-LIDS detection.

> ***Caution!***
>
> If you assign the same scene profile to different cameras, make sure to test the settings on all these cameras.

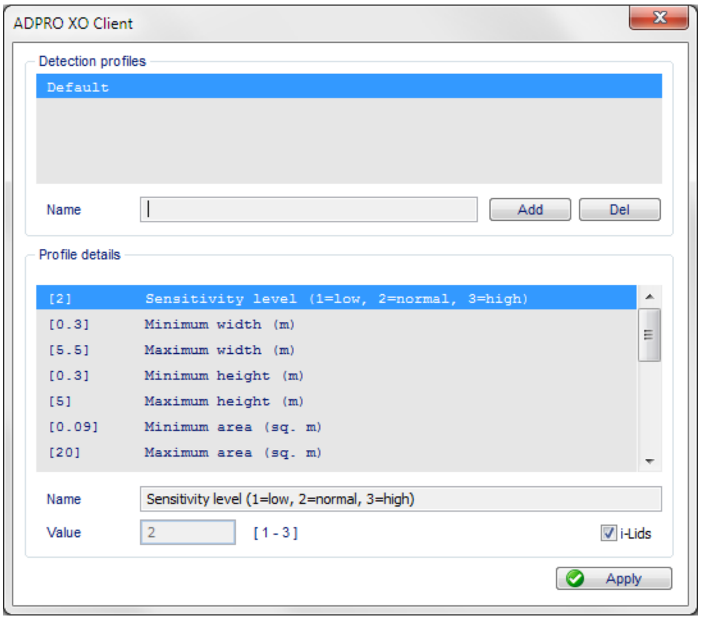
To get a feel for how the different settings influence detection, adjust only one setting at a time, and then test detection.

To set up a custom i-LIDS detection profile, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. Under **Scene Configuration**, click **Scene Config**.



ADPRO XO Client

Detection profiles

Default

Name

Add Del

Profile details

[2]	Sensitivity level (1=low, 2=normal, 3=high)
[0.3]	Minimum width (m)
[5.5]	Maximum width (m)
[0.3]	Minimum height (m)
[5]	Maximum height (m)
[0.09]	Minimum area (sq. m)
[20]	Maximum area (sq. m)

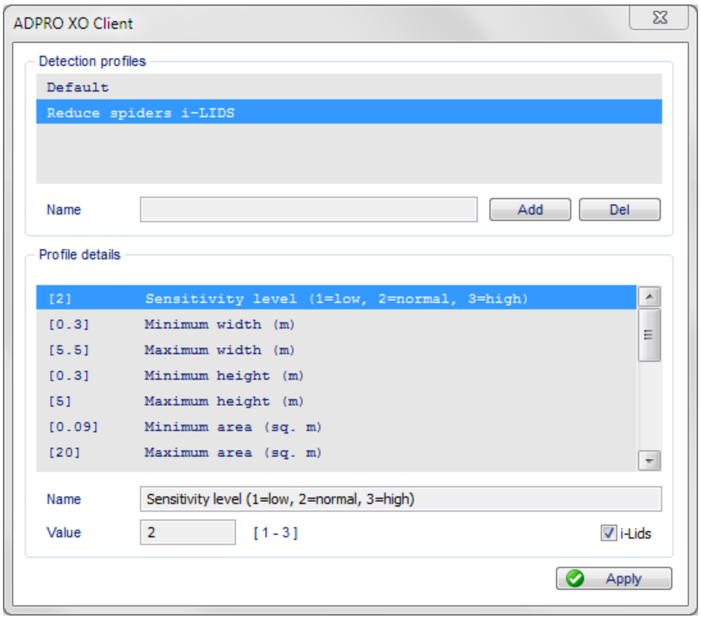
Name: Sensitivity level (1=low, 2=normal, 3=high)

Value: 2 [1-3] ☑ i-Lids

Apply

4. Make sure that the **i-Lids** checkbox is selected.
5. In the **Name** box, type a meaningful name for your custom profile.

6. Click **Add** to confirm. The system adds a profile with the chosen name and the default settings.



ADPRO XO Client

Detection profiles

```
Default
Reduce spiders i-LIDS
```

Profile details

```
[2]       Sensitivity level (1=low, 2=normal, 3=high)
[0.3]     Minimum width (m)
[5.5]     Maximum width (m)
[0.3]     Minimum height (m)
[5]       Maximum height (m)
[0.09]    Minimum area (sq. m)
[20]      Maximum area (sq. m)
```

Name: Sensitivity level (1=low, 2=normal, 3=high)

Value: 2 [1 - 3] ☑ i-Lids

The **Profile details** list shows all the settings, and their current value on the left between brackets.

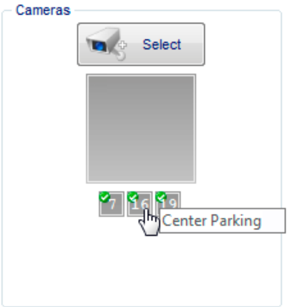
7. To adjust a setting: under **Profile details**, click the desired setting. The setting's name appears in the **Name** box below the **Profile details** list. (You cannot change the setting's name).
   The current value appears in the **Value** box. The possible (range of) values appears to the right of the **Value** box.
8. In the **Value** box, type the desired value for the setting.
9. Repeat for all the settings.
10. Click **Apply** to save the changes, and then close the profile window. The system automatically assigns the new profile to the scene.
11. Click **Save**.
12. Test the settings, and adjust if necessary. For more information on testing, see *Testing the IntrusionTrace Configuration* on page 62.

10.5 Assigning Existing i-LIDS Profiles to Cameras

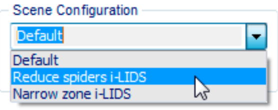
Once you have created an i-LIDS detection profile, you can assign it to any IntrusionTrace-enabled camera on the XO device.

To assign an existing i-LIDS detection profile to a camera, proceed as follows:

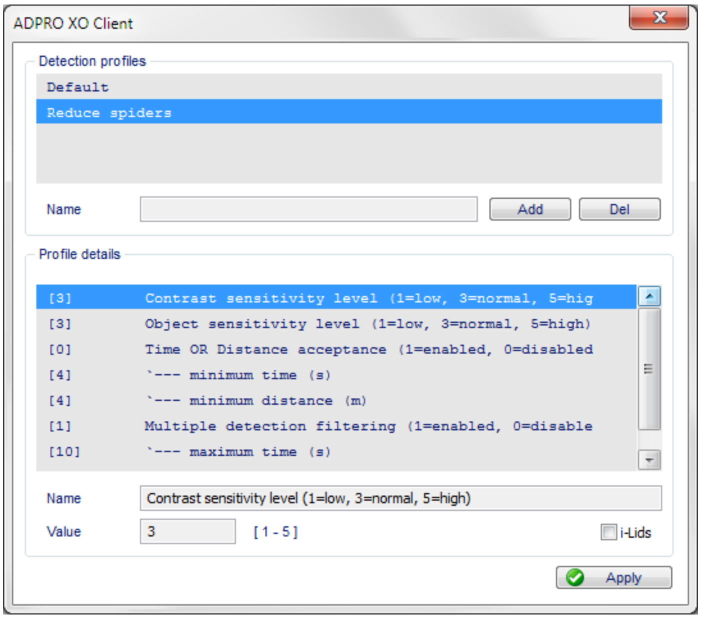
1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not yet active, click **Advanced mode**.
3. If the camera is already using i-LIDS certified detection: under **Scene Configuration**, select the desired i-LIDS profile from the list, and then click **Save**. You can skip all following steps.



4. If the camera is not yet using i-LIDS certified detection: under **Scene Configuration**, click **Scene Config**. The **Detection profiles** box lists the normal scene profiles.



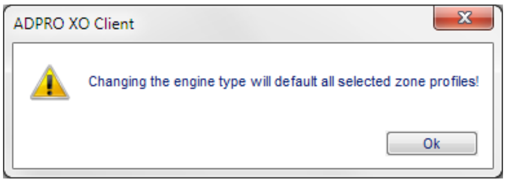
```
Default
Reduce spiders
```

```
[3]     Contrast sensitivity level (1=low, 3=normal, 5=hig
[3]     Object sensitivity level (1=low, 3=normal, 5=high)
[0]     Time OR Distance acceptance (1=enabled, 0=disabled
[4]     `--- minimum time (s)
[4]     `--- minimum distance (m)
[1]     Multiple detection filtering (1=enabled, 0=disable
[10]    `--- maximum time (s)
```

Name: Contrast sensitivity level (1=low, 3=normal, 5=high)

Value: 3 [1 - 5] ☐ i-Lids

5. Select the **i-LIDS** checkbox. The **Detection profiles** box now lists the i-LIDS profiles.
6. In the **Detection profiles** box, click the desired profile.
7. Click **Apply**, and then close the profile window. The following message appears:



Changing the engine type will default all selected zone profiles!

8. Click **OK** to confirm.
9. Click **Save**.

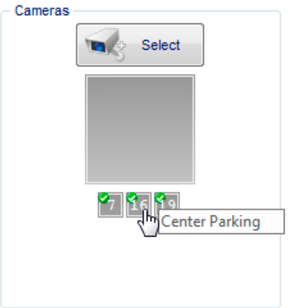
10.6 Changing an Existing i-LIDS Detection Profile

Note

You cannot change the default i-LIDS profile; it is fixed.

To change an existing i-LIDS profile, proceed as follows:

1. From the IntrusionTrace configuration window, click the camera that uses the desired i-LIDS profile.



2. Under **Scene Configuration**, click **Scene Config**.
3. Under **Profile details**, click the desired setting, and adjust its value in the **Value** box.
4. Click **Apply** to save the changes, and then close the profile window.
5. Click **Save**.
6. Test the new settings, and adjust again if necessary.

Caution!

If you have assigned the same i-LIDS profile to different cameras, make sure to test the settings on all these cameras.

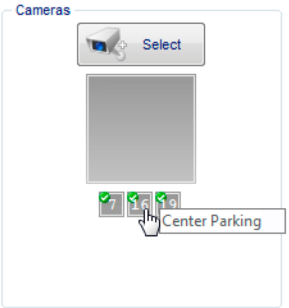
10.7 Deleting an i-LIDS Detection Profile

Note

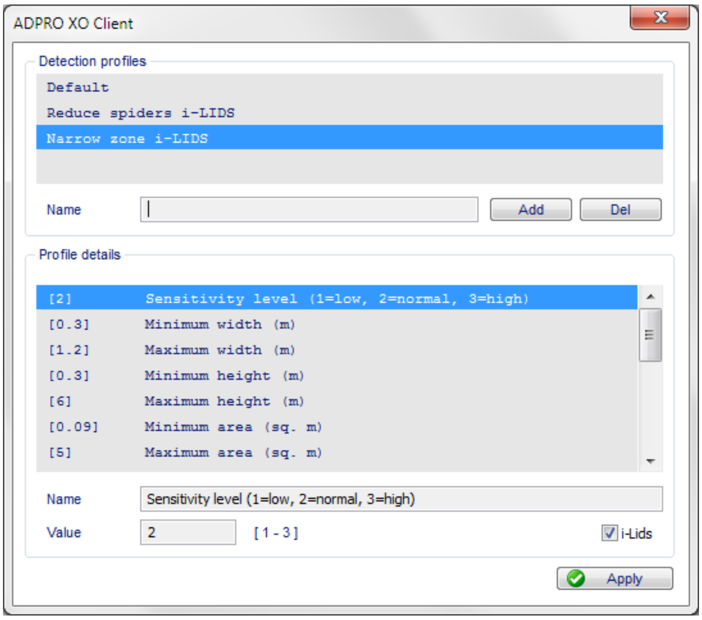
You cannot delete the default i-LIDS profile, or a custom i-LIDS profile that is still assigned to a camera. Make sure that all IntrusionTrace-enabled cameras on the XO device use a different profile (or the default profile).

To delete a scene profile, proceed as follows:

1. From the IntrusionTrace configuration window, click any camera that uses i-LIDS certified detection.



2. Under **Scene Configuration**, click **Scene Config**.
3. Under **Detection profiles**, click the desired i-LIDS profile.



ADPRO XO Client

Detection profiles

```
Default
Reduce spiders i-LIDS
Narrow zone i-LIDS
```

Name | Add | Del

Profile details

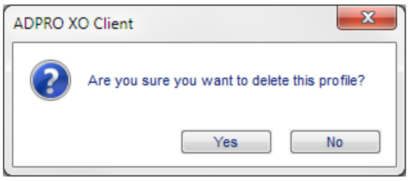
```
[2]        Sensitivity level (1=low, 2=normal, 3=high)
[0.3]      Minimum width (m)
[1.2]      Maximum width (m)
[0.3]      Minimum height (m)
[6]        Maximum height (m)
[0.09]     Minimum area (sq. m)
[5]        Maximum area (sq. m)
```

Name: Sensitivity level (1=low, 2=normal, 3=high)

Value: 2 [1 - 3] ☑ i-Lids

Apply

4. Click **Del**. The following message appears:



ADPRO XO Client

Are you sure you want to delete this profile?

Yes No

5. Click **Yes** to confirm.
6. Click **Apply** to save the changes, and then close the profile window.
7. Click **Save**.

11 Mask Zones

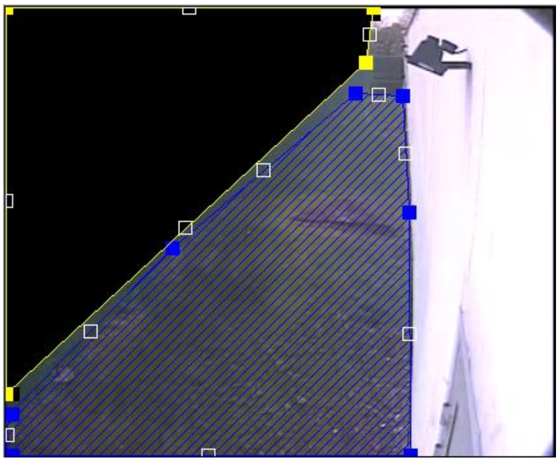
11.1 About Mask Zones

> ***Note***
>
> Mask zones are only available in advanced mode.

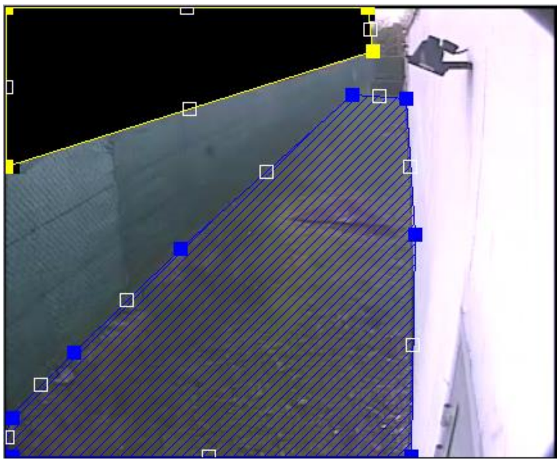
Mask zones define the areas in the camera image that IntrusionTrace will not analyse. Use mask zones sparingly, because they distort the shapes and sizes of bounding boxes. You can achieve much of what is intended by moving the detection area instead.
Mask zones are most useful for stopping moving trees from making people's bounding boxes too large to be detected. This can happen when a tree is on the far edge of the detection zone and is moving as a person walks that way.

You can draw up to 5 mask zones. The mask zones can overlap.

However, the mask zones must not overlap with the detection zones. You draw detection zones on the ground area, and mask zones in other areas. Mask zones must not cover the upper part of the intruder’s body when they are in a detection zone: keep the distance between the top of the detection zone and the bottom of the mask large enough to detect an intruder.

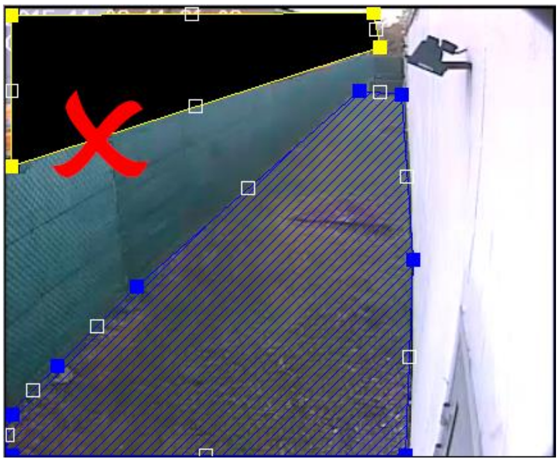


Mask zone too close to detection zone

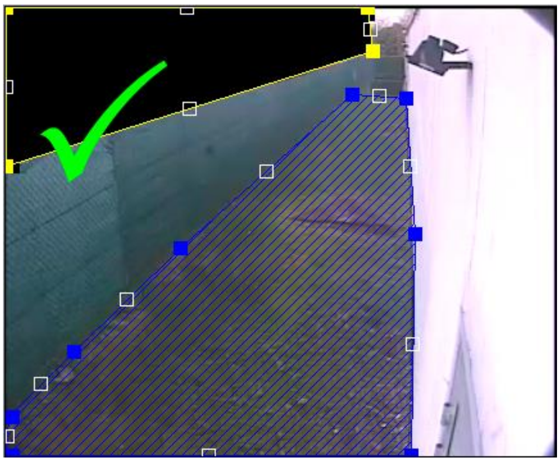


Mask zone at sufficient distance from detection zone

Just like detection zones, mask zones near the edge of the camera image must reach the edges. If not, IntrusionTrace may detect any activity at the edge. It occasionally happens that bounding boxes span the corner of a mask and cause problems.



Mask zone does not reach edge of image.
Warning! IntrusionTrace may detect activity at the edge.

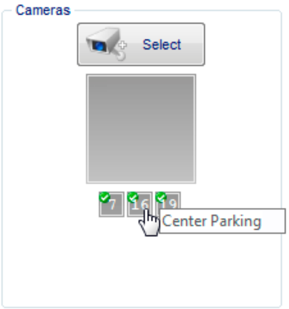


Mask zone reaches edge of image

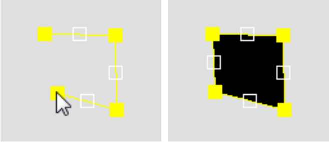
11.2 Drawing Mask Zones

To draw a mask zone, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. If advanced mode is not active, click **Advanced mode**.
3. Click the button (yellow polygon).
4. Draw and adjust the mask zone in the same way as a detection zone. For details, see *Drawing Detection Zones* on page 23. The finished mask zone appears in black on the camera image.



5. To draw another mask zone, click the button again and start drawing.

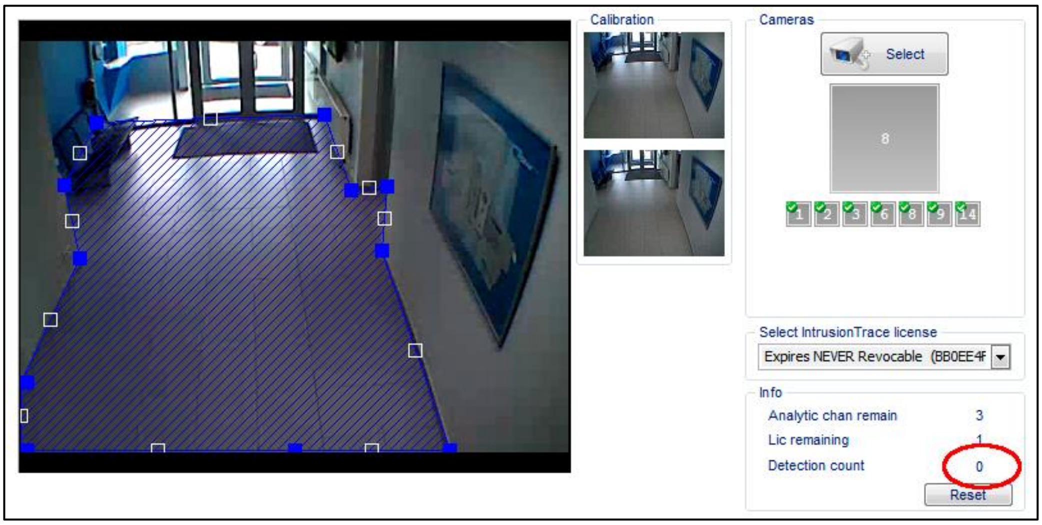
   You can also copy an existing mask zone: click the mask zone, and then click the button (or press Ctrl+C).
6. Click **Save**.
7. Test detection with the mask zones, and adjust the mask zones if necessary.

12 Testing the IntrusionTrace Configuration

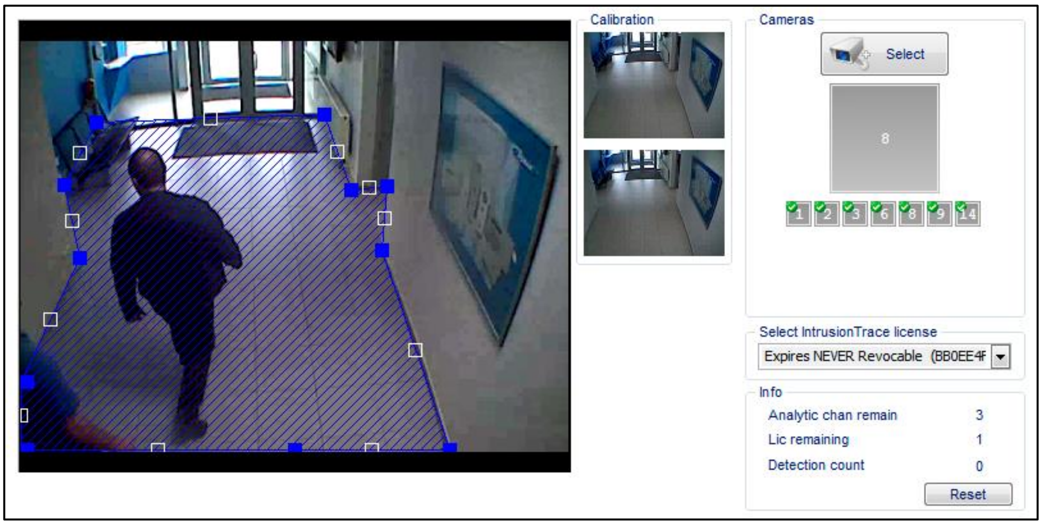
You need to test the configuration carefully before going live. You can do this from the IntrusionTrace configuration screen, which always displays the analytic bounding boxes, and always highlights the detection zone where the alarm occurs.

However, unlike the live or recorded video windows, it displays only the IntrusionTrace bounding boxes; it does not display bounding boxes of other analytic applications. Because there cannot be any confusion with other analytics, the configuration screen is the most suitable environment for testing your settings.

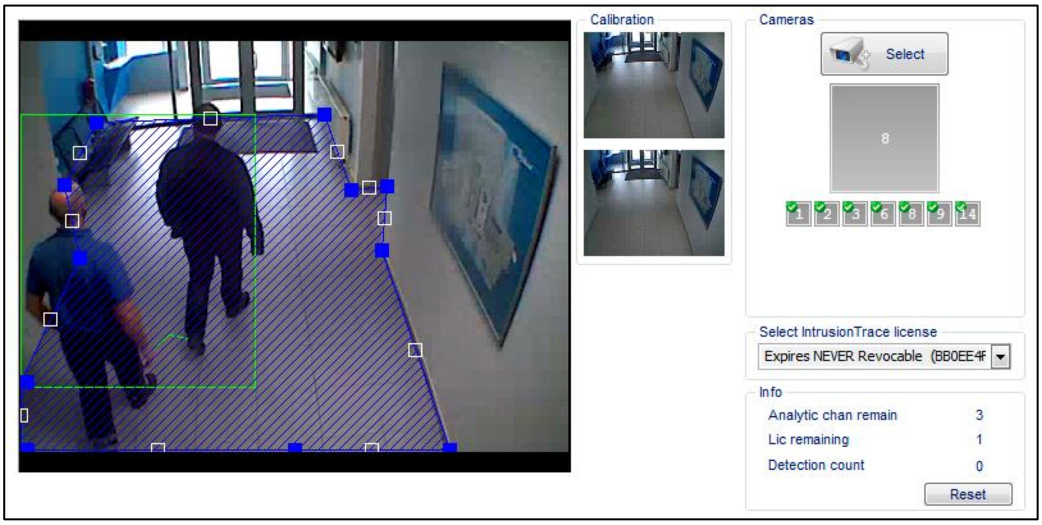
Furthermore, a **detection counter** in the configuration screen indicates the number of detections made on the selected camera during configuration. The system automatically resets the counter to 0 when you select a different camera or when you leave the IntrusionTrace configuration screen.
To manually reset the counter, click **Reset**.



The screen below shows a person entering the detection zone, but IntrusionTrace did not yet detect the object; there is no bounding box around the object:



The screen below shows the green bounding box, indicating that IntrusionTrace has detected the object, but has not yet triggered the alarm:

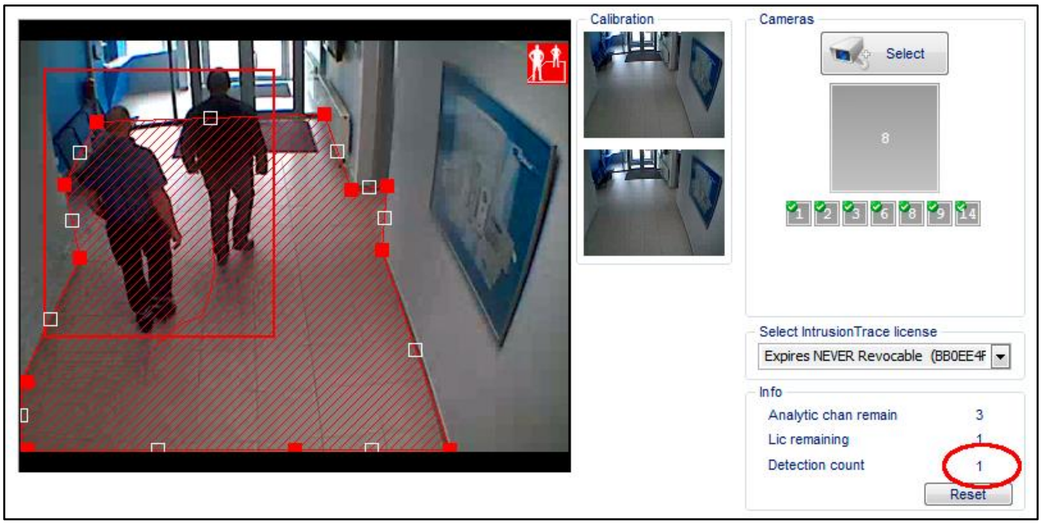


Select IntrusionTrace license: Expires NEVER Revocable (BB0EE4F

Info

Analytic chan remain	3
Lic remaining	1
Detection count	0

The screen below shows the red bounding box, indicating that IntrusionTrace has detected the object and triggered the alarm. The system highlights the detection zone, and the detection counter has increased by 1:

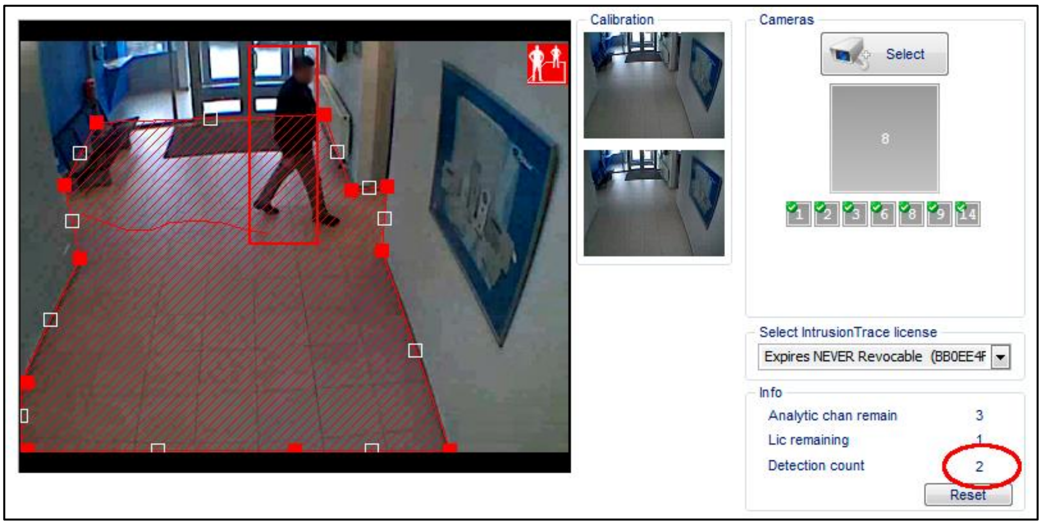


Select IntrusionTrace license: Expires NEVER Revocable (BB0EE4F

Info

Analytic chan remain	3
Lic remaining	1
Detection count	1

The detection counter increases upon each alarm:



Select IntrusionTrace license: Expires NEVER Revocable (BB0EE4F

Info

Analytic chan remain	3
Lic remaining	1
Detection count	2

Make sure to test the settings for all situations when IntrusionTrace should trigger an alarm:

- Objects coming from different directions
- Objects moving at different speeds
- Objects crawling
- Object of different sizes, single objects/persons or groups
- Different times of day (dusk, dawn, day, night)
- Different weather conditions
- …

13 IntrusionTrace Alarms

13.1 Overview

The following inputs (alarms) are available in the XO client with IntrusionTrace:

General IntrusionTrace input:

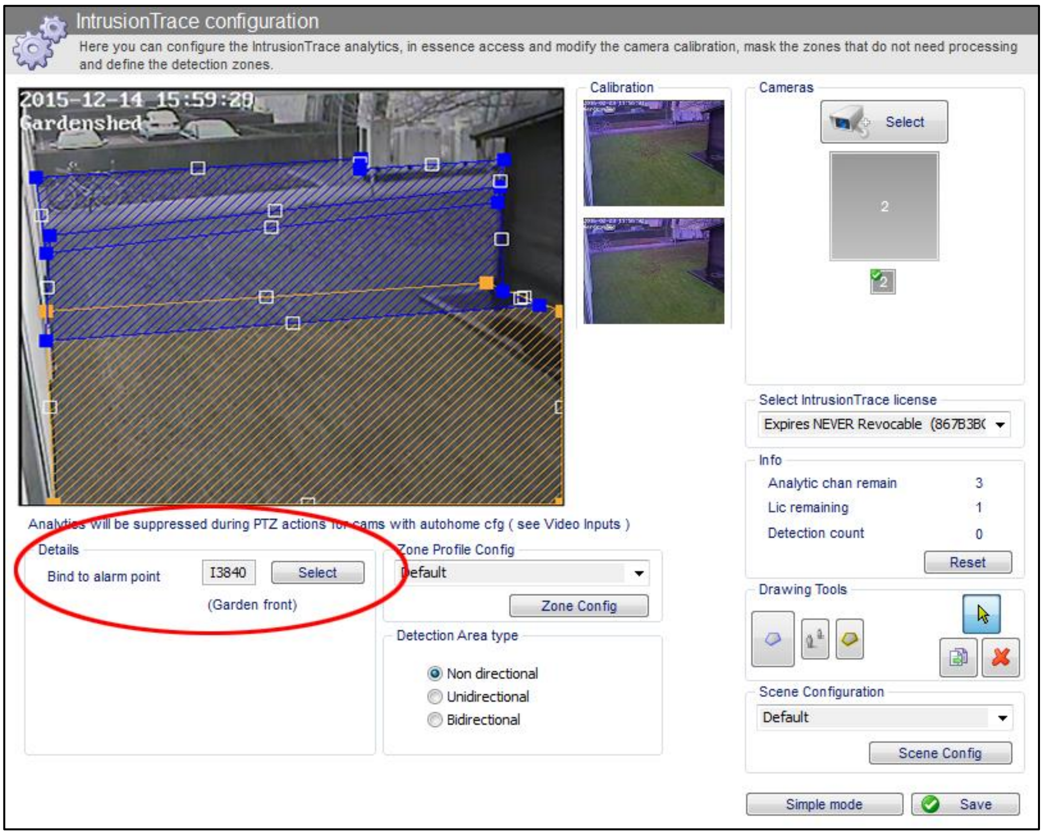
For each camera that runs IntrusionTrace, there is a general IntrusionTrace input.
For camera 1, this is:
I1048 – [REAL] – CAM01 PERIMETER
For camera 2:
I1080 – [REAL] – CAM02 PERIMETER
...

IntrusionTrace activates the input if it detects an intruder in any of the detection zones of that camera.

Analytics detail inputs:

Furthermore, the XO software offers an extra set of 256 inputs (**analytics detail inputs**) that you can freely assign to individual IntrusionTrace detection zones. These inputs are:
I3840 – [REAL] – ANALYTICS DET. 001
to
I4095 – [REAL] – ANALYTICS DET. 256

IntrusionTrace activates the input if it detects an intruder in the assigned detection zone.
These inputs can provide more information about the exact location of the intrusion detection, and they can trigger a PTZ camera to zoom in on the detection zone.



IntrusionTrace configuration

Here you can configure the IntrusionTrace analytics, in essence access and modify the camera calibration, mask the zones that do not need processing and define the detection zones.

Analytics will be suppressed during PTZ actions for cams with autohome cfg (see Video Inputs)

Details
Bind to alarm point: I3840
(Garden front)

Zone Profile Config: Default

Detection Area type
● Non directional
○ Unidirectional
○ Bidirectional

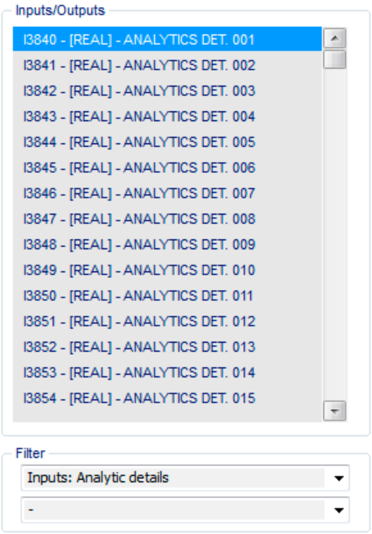
Select IntrusionTrace license: Expires NEVER Revocable (867B3B(

Info
Analytic chan remain 3
Lic remaining 1
Detection count 0

Scene Configuration: Default

The screen above shows three overlapping detection zones; an alarm in the zone at the bottom (selected, displayed in orange) will activate input number 3840 with description ‘Garden front’.

In the inputs/outputs list, use the **Inputs: Analytic details** filter to display only these 256 inputs.



Inputs/Outputs

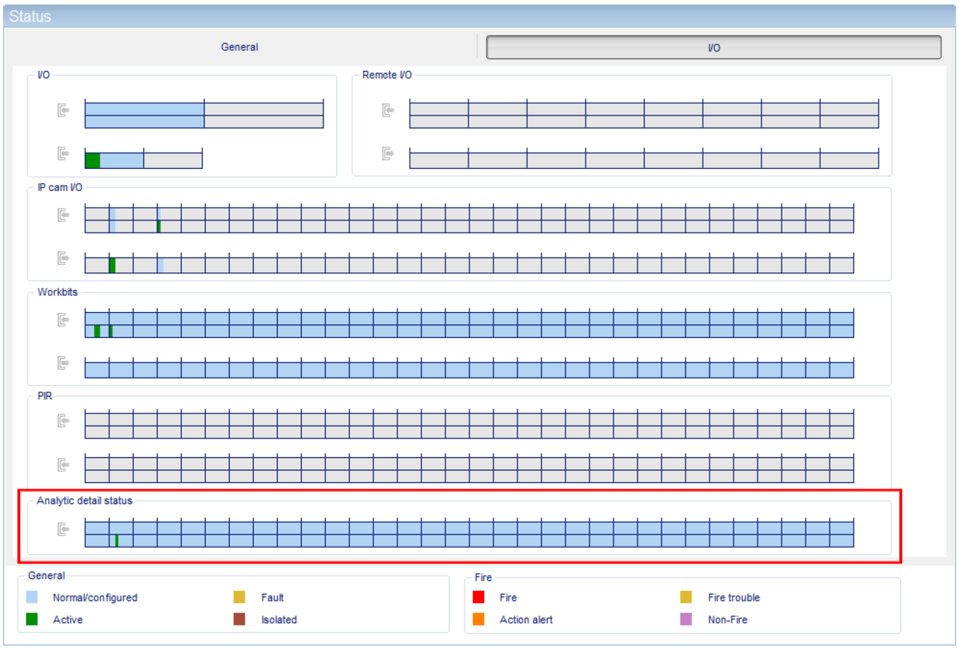
I3840 - [REAL] - ANALYTICS DET. 001
I3841 - [REAL] - ANALYTICS DET. 002
I3842 - [REAL] - ANALYTICS DET. 003
I3843 - [REAL] - ANALYTICS DET. 004
I3844 - [REAL] - ANALYTICS DET. 005
I3845 - [REAL] - ANALYTICS DET. 006
I3846 - [REAL] - ANALYTICS DET. 007
I3847 - [REAL] - ANALYTICS DET. 008
I3848 - [REAL] - ANALYTICS DET. 009
I3849 - [REAL] - ANALYTICS DET. 010
I3850 - [REAL] - ANALYTICS DET. 011
I3851 - [REAL] - ANALYTICS DET. 012
I3852 - [REAL] - ANALYTICS DET. 013
I3853 - [REAL] - ANALYTICS DET. 014
I3854 - [REAL] - ANALYTICS DET. 015

Filter

Inputs: Analytic details

-

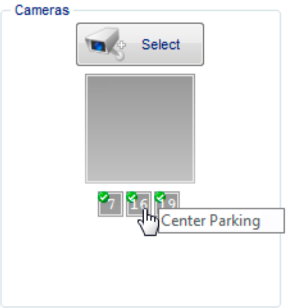
The **Status** screen displays the analytic detail inputs at the bottom of the I/O tab:



13.2 Assigning Analytic Detail Inputs to IntrusionTrace Detection Zones

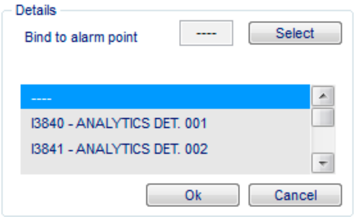
To assign an analytic detail input to a detection zone, proceed as follows:

1. From the IntrusionTrace configuration window, click the desired camera.



2. Click the desired detection zone.

3. In the **Details** section, click **Select**. The list of inputs appears.



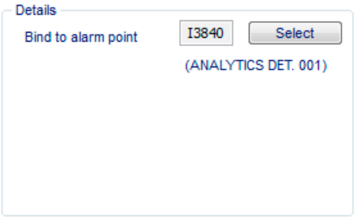
Details

Bind to alarm point ---- Select

I3840 - ANALYTICS DET. 001
I3841 - ANALYTICS DET. 002

Ok Cancel

4. Select the desired input, and click **OK**.
The input number appears in the **Bind to alarm point** box, and the input name appears below. You will change the input name later, to a more meaningful description.



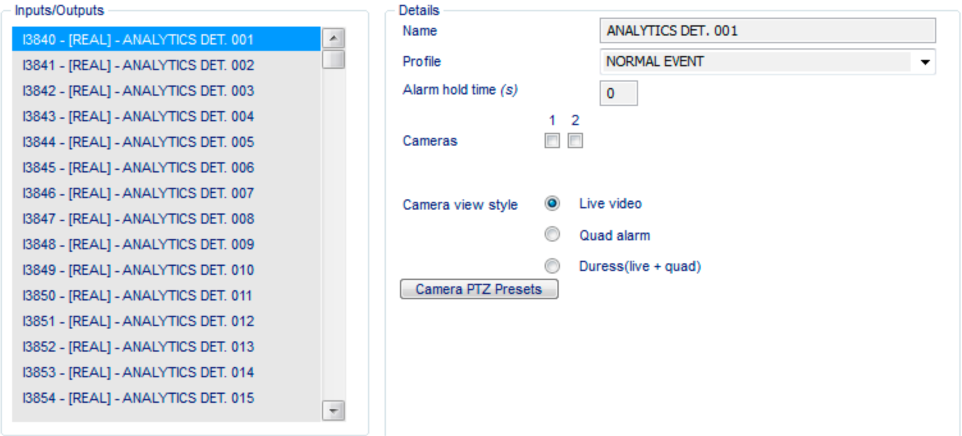
Details

Bind to alarm point I3840 Select

(ANALYTICS DET. 001)

5. Click **Save**.
Next, you will configure the input, to make sure that the system transmits the corresponding alarm message to the required destinations.

6. Choose **System > Behaviour > Input/Output Behaviour**, and then click the input in the **Inputs/Outputs** list.
Tip: use the **Inputs: Analytic details** filter to reduce the list.



Inputs/Outputs

I3840 - [REAL] - ANALYTICS DET. 001
I3841 - [REAL] - ANALYTICS DET. 002
I3842 - [REAL] - ANALYTICS DET. 003
I3843 - [REAL] - ANALYTICS DET. 004
I3844 - [REAL] - ANALYTICS DET. 005
I3845 - [REAL] - ANALYTICS DET. 006
I3846 - [REAL] - ANALYTICS DET. 007
I3847 - [REAL] - ANALYTICS DET. 008
I3848 - [REAL] - ANALYTICS DET. 009
I3849 - [REAL] - ANALYTICS DET. 010
I3850 - [REAL] - ANALYTICS DET. 011
I3851 - [REAL] - ANALYTICS DET. 012
I3852 - [REAL] - ANALYTICS DET. 013
I3853 - [REAL] - ANALYTICS DET. 014
I3854 - [REAL] - ANALYTICS DET. 015

Details

Name: ANALYTICS DET. 001

Profile: NORMAL EVENT

Alarm hold time *(s)*: 0

Cameras: 1 □ 2 □

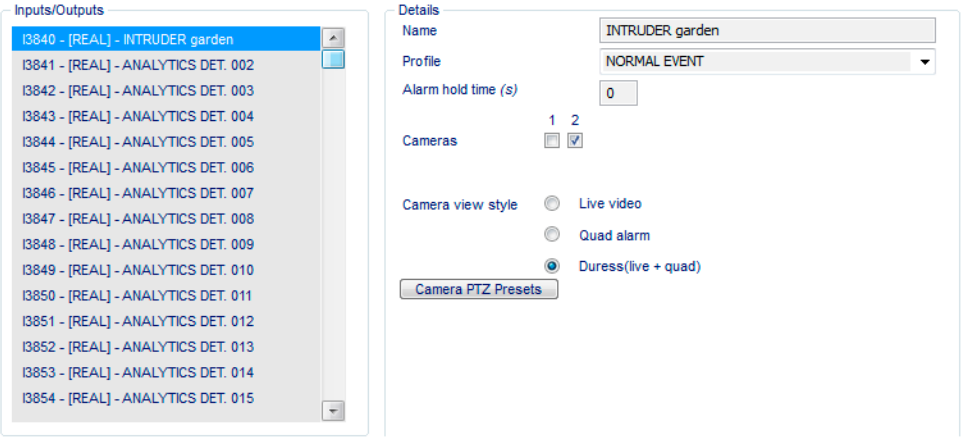
Camera view style: ● Live video ○ Quad alarm ○ Duress(live + quad)

Camera PTZ Presets

7. In the **Name** box, type a name (max. 20 characters) to describe the input. Use a name that is meaningful and relevant. The name appears not only in the screens in the client software, but also in the alarm message to the CMS. For example, ‘INTRUDER garden’.

8. Set up the input as required: alarm profile, cameras for quad/live alarm images, PTZ positions… For details, see the *XO Client Software User Manual* (21796).

9. Click **Save**.



Inputs/Outputs

I3840 - [REAL] - INTRUDER garden
I3841 - [REAL] - ANALYTICS DET. 002
I3842 - [REAL] - ANALYTICS DET. 003
I3843 - [REAL] - ANALYTICS DET. 004
I3844 - [REAL] - ANALYTICS DET. 005
I3845 - [REAL] - ANALYTICS DET. 006
I3846 - [REAL] - ANALYTICS DET. 007
I3847 - [REAL] - ANALYTICS DET. 008
I3848 - [REAL] - ANALYTICS DET. 009
I3849 - [REAL] - ANALYTICS DET. 010
I3850 - [REAL] - ANALYTICS DET. 011
I3851 - [REAL] - ANALYTICS DET. 012
I3852 - [REAL] - ANALYTICS DET. 013
I3853 - [REAL] - ANALYTICS DET. 014
I3854 - [REAL] - ANALYTICS DET. 015

Details

Name: INTRUDER garden

Profile: NORMAL EVENT

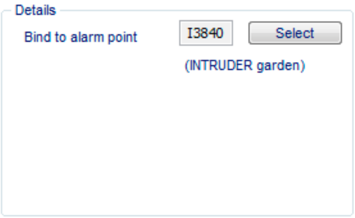
Alarm hold time *(s)*: 0

Cameras: 1 □ 2 ☑

Camera view style: ○ Live video ○ Quad alarm ● Duress(live + quad)

Camera PTZ Presets

The new name will be visible in the IntrusionTrace configuration screen:



Details

Bind to alarm point I3840

(INTRUDER garden)

14 Double-Knock Scenarios with PIR Detectors

A tried and tested method of reducing false alarms is the double-knock configuration. In a double-knock configuration, the system only triggers an alarm if another alarm occurs simultaneously. The typical double-knock configuration combines a PIR detector alarm with the IntrusionTrace alarm from a camera to trigger the PIR detector’s double-knock event.

With the ADPRO PRO E PIR detector models, you can also easily combine the alarms from two PIR detectors in the so-called intelligent double-knock configuration (from firmware version XOa 3.02.0012). You can then combine both methods (two PRO E PIR detectors, and IntrusionTrace) to create a triple-knock configuration.

For details, see the *XO Client Software User Manual* (21796).

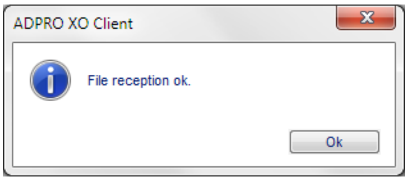
15 Client Configuration and Calibration Pictures Backup

15.1 Backup

Xtralis recommends to back up the client configuration and the calibration pictures when the IntrusionTrace configuration is complete and fully tested. You can then reload the configuration or pictures in case of a system malfunction, or use the data to quickly configure another system.

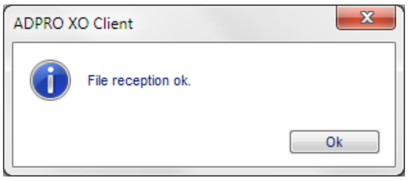
To back up the client configuration and calibration pictures, proceed as follows:

1. Choose **System > Maintenance > Transfer**.
2. In the **Receive from server** section, click **Configuration**.
3. Select the correct configuration from the list, and then click **Get**.
4. Select the destination folder where you want to store the configuration, and then click **Save**. The following message appears if saving is successful:



File reception ok.

5. Click **OK** to close the message box.
6. Click **Calibration pictures**, and then click **Get**.
7. Select the destination folder where you want to store the calibration pictures, and click **OK**. The following message appears if saving is successful:



File reception ok.

8. Click **OK** to close the message box.

15.2 Restore

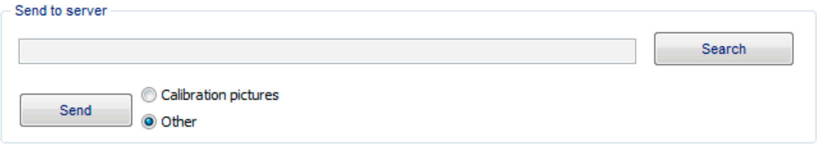
Caution!

When you restore the configuration file, you restore not only the IntrusionTrace configuration, but also the other settings in the **System** menu (except settings for MIO/EIO cards and Net I/O modules, users, and licences).

Restoring the configuration file requires a system restart.

To restore the calibration pictures and configuration file, proceed as follows:

1. Choose **System > Maintenance > Transfer**. For uploading, you will work in the **Send to server** section.

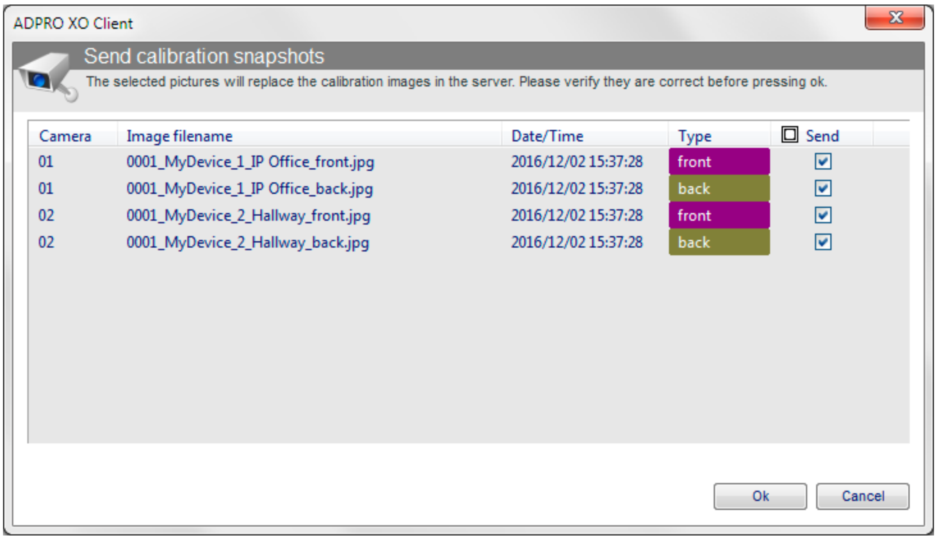


○ Calibration pictures
● Other

First you will upload the calibration pictures.

2. Click **Calibration pictures**.
3. Under **Send to server**, click **Search**.
4. Select the file(s) that you want to upload, and then click **Open**.

5. Click **Send**. The system will now check the files you selected, and then present an overview of the calibration pictures that it will upload:



ADPRO XO Client

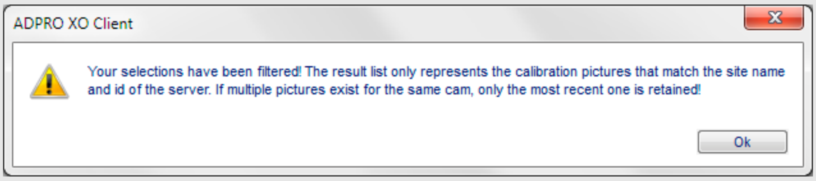
Send calibration snapshots

The selected pictures will replace the calibration images in the server. Please verify they are correct before pressing ok.

Camera	Image filename	Date/Time	Type	□ Send
01	0001_MyDevice_1_IP Office_front.jpg	2016/12/02 15:37:28	front	☑
01	0001_MyDevice_1_IP Office_back.jpg	2016/12/02 15:37:28	back	☑
02	0001_MyDevice_2_Hallway_front.jpg	2016/12/02 15:37:28	front	☑
02	0001_MyDevice_2_Hallway_back.jpg	2016/12/02 15:37:28	back	☑

Note

If the system detects one or more files that are not suitable calibration pictures (their site name and ID do not match that of the XO device, or they are snapshots), of if you have selected more than one front or back picture for the same camera, the following message appears:



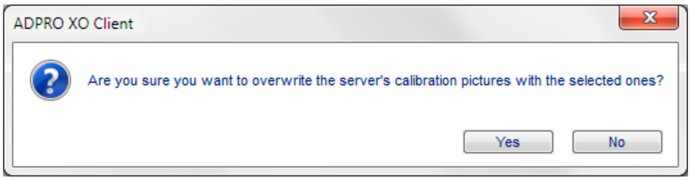
ADPRO XO Client

Your selections have been filtered! The result list only represents the calibration pictures that match the site name and id of the server. If multiple pictures exist for the same cam, only the most recent one is retained!

Click **OK** to close the message box. The system filters out the unsuitable pictures, and takes only the most recent version of the suitable pictures.

6. Carefully check the overview, and clear the checkboxes of the listed pictures that you do not want to upload.

7. Click **OK** to confirm. The following screen appears:



ADPRO XO Client

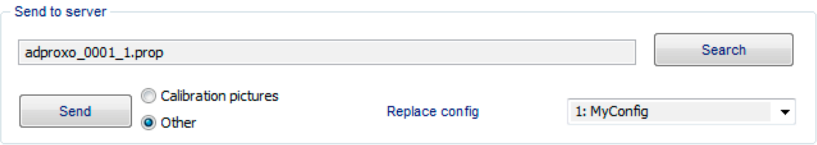
Are you sure you want to overwrite the server's calibration pictures with the selected ones?

8. Click **Yes** to confirm.
The system uploads the selected calibration pictures.
Next, you will upload the configuration file.

9. In the **Send to server** section, click **Other**.

10. Click **Search**.

11. Select the configuration file that you want to upload, and then click **Open**.



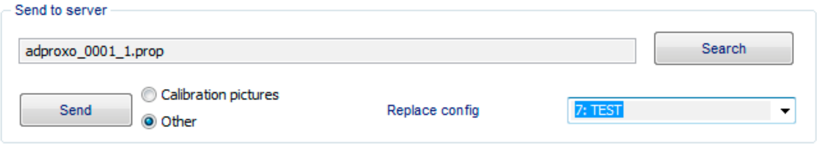
Send to server

adproxo_0001_1.prop

○ Calibration pictures
● Other

Replace config: 1: MyConfig

12. In the **Replace config** box, select the configuration that you want to overwrite.



Send to server

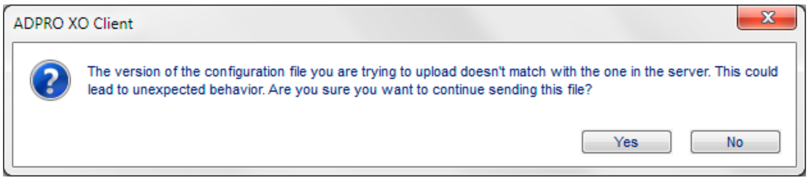
adproxo_0001_1.prop

○ Calibration pictures

● Other

Replace config: 7: TEST

13. Click **Send** to upload the file to the XO device. If the configuration file has a different version than the active configuration, the following screen appears:



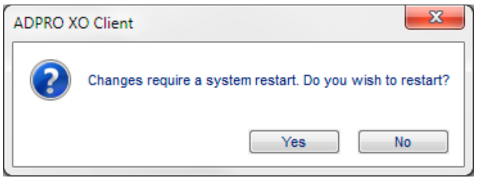
ADPRO XO Client

The version of the configuration file you are trying to upload doesn't match with the one in the server. This could lead to unexpected behavior. Are you sure you want to continue sending this file?

Caution!

Settings from different versions may cause conflicts and unexpected behaviour in the system. Proceed at your own risk.

14. If you are sure that you want to upload the configuration, click **Yes**. The following screen appears:



ADPRO XO Client

Changes require a system restart. Do you wish to restart?

15. Click **Yes** to restart the XO device.

16 Troubleshooting

IntrusionTrace is not available in the System menu

You must install at least one IntrusionTrace license on the XO device. Purchase your licenses via your regular channel, and install the license using Xchange.

IntrusionTrace license is no longer assigned to a camera

In the IntrusionTrace configuration window, you have to draw at least one detection zone before saving the settings. If you click **Save** when there is no detection zone available, the system automatically unlinks the IntrusionTrace license from the camera.

The assigned scene or zone profile is incorrect

When you are working in the profile window to create or change scene/zone profiles, the system assigns the profile that is currently selected in the profile window to the camera when you close the window.

Detection zone profiles are not available

- Advanced mode is not active for the selected camera. To the left of the **Save** button, click **Advanced mode**.
- The configuration uses i-LIDS certified detection (the **i-Lids** checkbox is selected in the scene profile). You cannot use zone profiles with i-LIDS certified detection.

Mask zones are not available

Advanced mode is not active for the selected camera. To the left of the **Save** button, click **Advanced mode**.

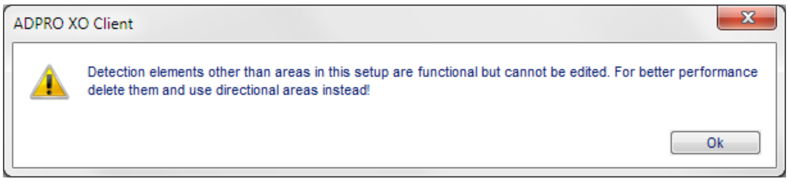
Cannot add a mask zone

You can draw maximum 5 mask zones.

Using the trigger lines from previous versions

As of ADPRO firmware version V2.11.0023, IntrusionTrace no longer uses trigger lines, but the more reliable directional zones. If you have upgraded, the existing trigger lines will still function. However, Xtralis recommends that you delete all trigger lines from your existing detection zones; and instead set the desired direction for the zone. There is no need to redraw the zone.

The following message will appear if you open an IntrusionTrace configuration that still uses trigger lines:



ADPRO XO Client

Detection elements other than areas in this setup are functional but cannot be edited. For better performance delete them and use directional areas instead!

Custom scene profile is not available

If a custom scene profile is not visible in the list of scene profiles, check if the camera uses i-LIDS certified detection. For such cameras only the i-LIDS profiles are available.

www.xtralis.com

UK and Europe +44 1442 242 330 **D-A-CH** +49 431 23284 1 **The Americas** +1 781 740 2223
Middle East +962 6 588 5622 **Asia** +86 21 5240 0077 **Australia and New Zealand** +61 3 9936 7000

A *Disclaimer* about this document, statements about *Intellectual Property, Copyrights*, and *Liability*, as well as a *General Warning* are available in an earlier section of this document.

Doc. 26472_02