GANZ Bridge

Powered by VCA TECHNOLOGY

User Guide

Wednesday, July 05, 2017

Table of Contents

Chapter 1

Introduction

This is the user manual for the VCA Video Analytics system. This manual describes how to set up and configure the video analytics to detect events of interest while minimizing false alerts.

The menu on the left-hand-side provides shortcuts to the major topic areas. Alternatively, see the Getting Started topic for the essentials necessary to get started rapidly.

Chapter 2

Getting Started

This user guide documents each topic in detail, and each topic is accessible via the menu. However, to get started quickly, the essential topics are listed below.

2.1 Fundamentals

- Use the discovery tool to locate the VCA device on the network
- Learn how to navigate through the device's interface
- Check the software running on the device is fully up to date and upgrade it if necessary from the system settings page. Check for software updates at support.vcatechnology.com.
- Configure the network and time settings by using the system settings page
- The device should be pre-licensed for the most common functionality in the factory. However, if a different or non-standard feature set is required check the license on the activation page
- Create an input video source
- Assign the input to a channel
- Create some zones and detection rules. Calibrate the channel if necessary
- Create an output to send alerts to a third-party system. Review the list of integrations to see which 3rd party systems have built-in support

2.2 User Credentials

Note that the default username and password for the VCA device are:

- **Username:** admin
- **Password:** admin

2.3 Advanced Topics

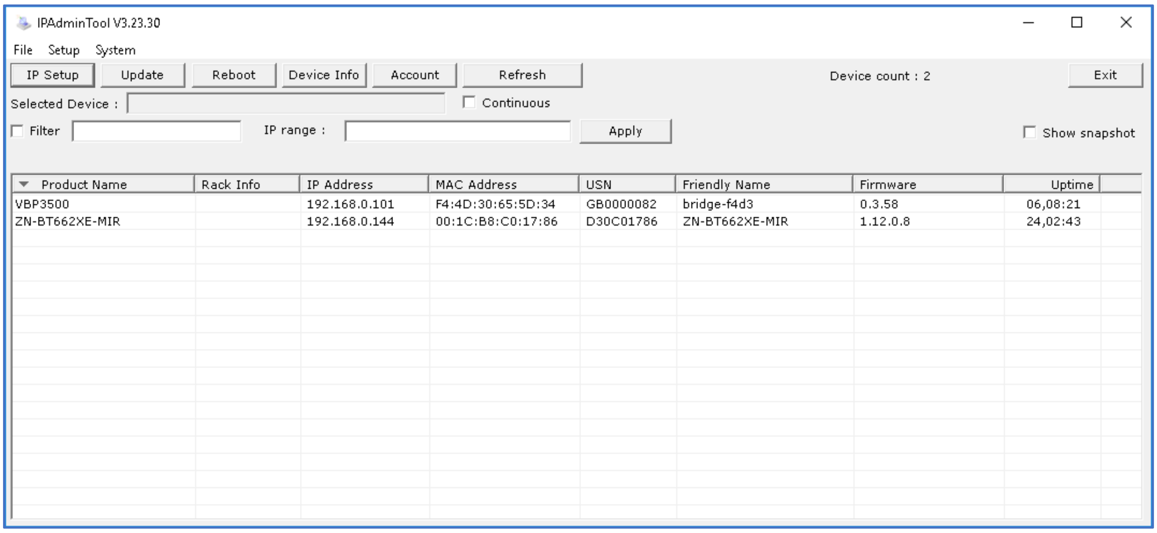
Once the basic settings are configured, the following advanced topics may be relevant:

- Set up custom classifiers by using the classification function
- Detect camera tampering or obscuration by using the tamper detect function
- Learn how the device detects gross scene changes with the scene change detection function
- Customize the annotation that's included in the video display by using the burnt-in annotation settings
- Adjust advanced settings such as alarm hold off time, detection point and camera shake cancellation by using the advanced settings page

Chapter 3

Device Discovery

The device discovery tool can be used to locate GANZ GXi devices on the network.



Device count : 2

Selected Device :

□ Continuous

□ Filter

IP range :

□ Show snapshot

Product Name	Rack Info	IP Address	MAC Address	USN	Friendly Name	Firmware	Uptime
VBP3500		192.168.0.101	F4:4D:30:65:5D:34	GB0000082	bridge-f4d3	0.3.58	06,08:21
ZN-BT662XE-MIR		192.168.0.144	00:1C:B8:C0:17:86	D30C01786	ZN-BT662XE-MIR	1.12.0.8	24,02:43

Locate the GANZ GXi device in the network and select the corresponding entry in the list in the discovery tool.

A number of options can then be performed by clicking the appropriate button:

- **IP Setup:** Set the device IP address and host name.
- **Update:** Update the device firmware (not currently supported by GANZ bridge devices).
- **Reboot:** Reboot the device.
- **Device Info:** Display all additional device information.
- **Refresh:** Refresh the list of devices

The discovery tool is available from the website www.ganzsecurity.com

3.1 Next Steps

Learn more about Navigation or go back to the Getting Started Guide.

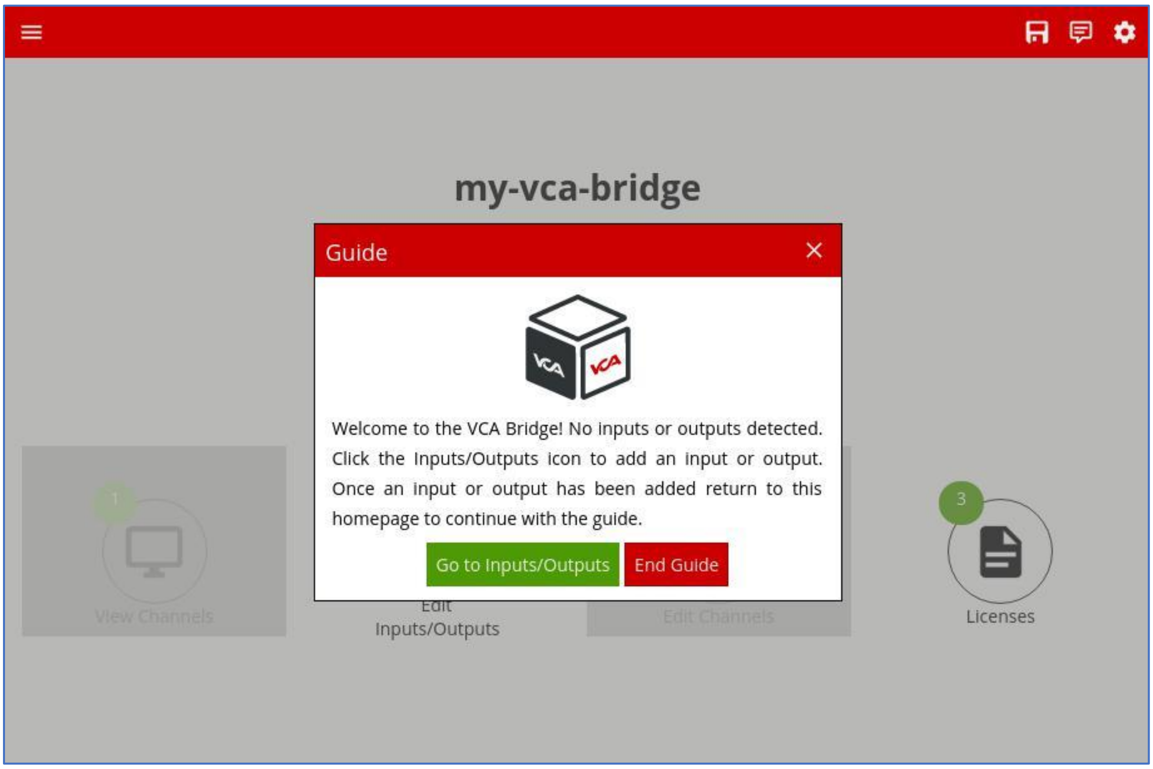
Chapter 4

Navigation

This topic provides a general overview of the VCA configuration user interface elements and controls.

4.1 Interactive User Guide

When connecting to a VCA device for the very first time, a user guide is displayed to assist with basic configuration:

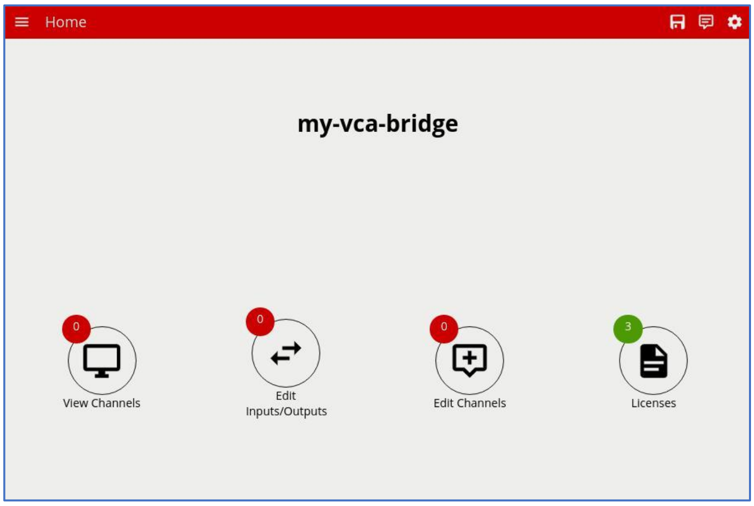


Welcome to the VCA Bridge! No inputs or outputs detected. Click the Inputs/Outputs icon to add an input or output. Once an input or output has been added return to this homepage to continue with the guide.

Following this guide is an effortless way to get started. When the guide is no longer required, it can be silenced permanently by clicking **End Guide**.

4.2 Home Page

The home page is the first page displayed when viewing the device in the web browser:

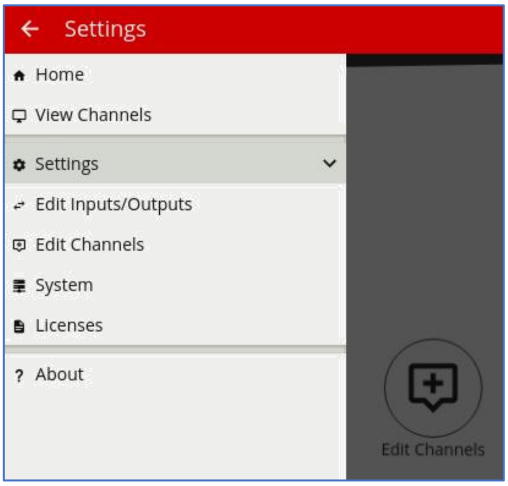


There are many elements on the page, each is described below:

- ≡: The menu icon. Click the menu icon to access the context menu of available configuration options
- 💾: The configuration state icon. Indicates the current state of synchronization of configuration between the user interface and the actual device. Can be one of three states: 💾: All configuration is synchronized between web interface and the device. ⟳: Configuration is currently being synchronized between the web interface and the device. ⚠: Configuration is out of sync between the web interface and the device. In this situation, any changes may not be applied to the device and the browser should be refreshed.
- 🗨: The notifications icon. Click and drag down to view any notifications from the device.
- ⚙: The system settings icon. Click to access device System Settings.

4.3 Context Menu

Clicking the ≡ icon displays the context menu:



The contents of the context menu change depending on the current location within the user interface. For example, here it displays the available options when in the settings area of the interface. However, when viewing a channel, the context menu displays different options such as zone configuration and calibration.

4.4 Shortcuts

The home page also displays a number of shortcut icons. These are:

- **View Channels:** Go to the channels overview page.
- **Edit Inputs/Outputs:** Go to the Inputs and Outputs configuration page.
- **Edit Channels:** Go to the Channels configuration page.
- **Licenses:** Go to the Activation page to add or remove VCA licenses.

4.5 Next Steps

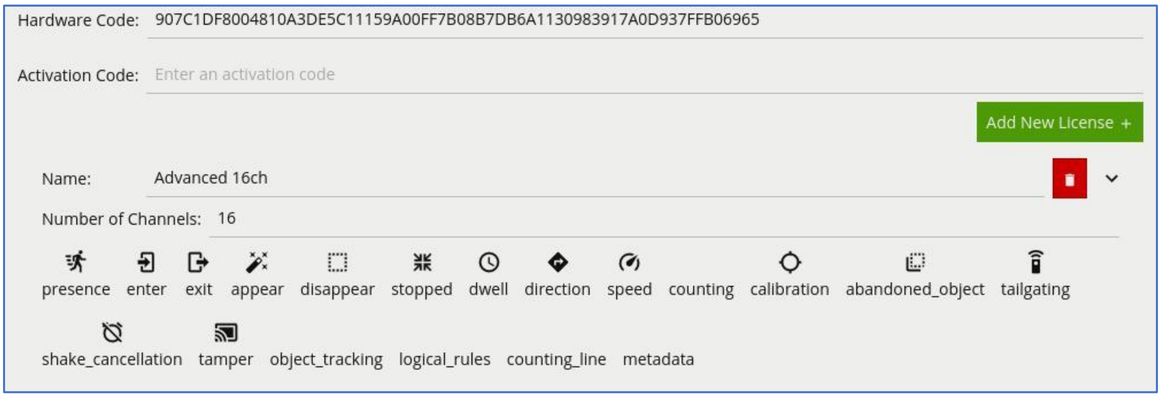
Learn more about Activation or go back to the Getting Started Guide.

Chapter 5

Activation

In many cases VCA is pre-activated in the factory and further activation is only necessary to enable additional functionality.

Additional features can be activated by applying an **activation code** to the device. Each license is only valid for a specific device and each device is uniquely identified by a **hardware code**.
To manage activation and hardware codes, navigate to the license settings page:



Hardware Code: 907C1DF8004810A3DE5C11159A00FF7B08B7DB6A1130983917A0D937FFB06965

Activation Code: Enter an activation code

Name: Advanced 16ch

Number of Channels: 16

- **Hardware Code:** The unique hardware code for this device. Needed to generate an activation code.
- **Activation Code:** Enter an activation code to enable additional functionality or channels.
- The list of installed licenses and features are displayed underneath.

5.1 Steps to Activate Additional Functionality

- Copy the hardware code and send it to the hardware reseller.
- The reseller sends an activation code by return.
- Apply the activation code to the device and verify the required features are activated.

5.2 More Information

For more information on the complete range of additional features available, please visit VCA Technology

Chapter 6

Inputs and Outputs

VCA operates on **channels**, and channels consume data (e.g. video) from **inputs** and produce data (e.g. metadata or events) to **outputs**.

Before a channel can be created on which VCA can operate, some inputs and/or outputs must first be configured.

6.1 Supported Inputs and Outputs

A variety of inputs and outputs are supported by VCA.

6.1.1 Inputs

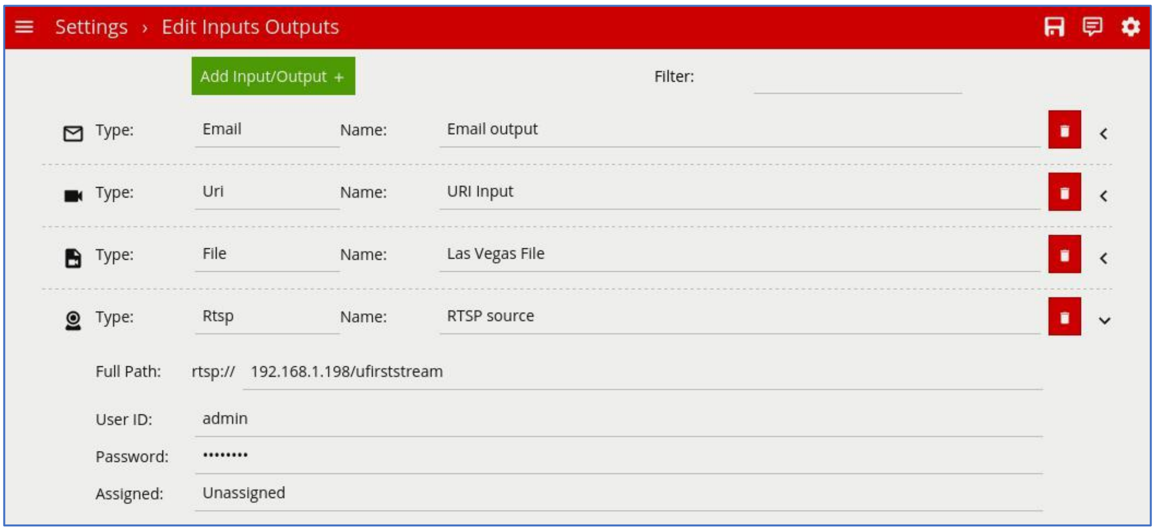
Input Type	Functionality
File	Streams video from a local sample file embedded within the VCA firmware
RTSP	Streams video from remote RTSP sources such as IP cameras and encoders
URI	Streams video from a remote source, specified by a URI. May not support all video formats
Milestone	Streams video from a Milestone XProtect VMS server
Input	

6.1.2 Outputs

Output Type	Functionality
HTTP	Executes a HTTP request on a remote API when an event occurs
TCP	Transmits a TCP message to a remote TCP server when an event occurs
Email	Sends an email with annotated snapshots to a remote SMTP server when an event occurs
Milestone	Sends an event to a Milestone XProtect Event Server, which is displayed in the
Output	Milestone Client
Output Type	Functionality
Digital Output	Triggers a digital output channel

6.2 Adding an Input

- Click the **Add Input/Output** drop menu and select the type of element to add. A default element will be added.
- Each element has a set of common properties and additional settings specific to the element type. The full list of element settings can be expanded or collapsed by using the expand/collapse control (<).



Type: Email Name: Email output

Type: Uri Name: URI Input

Type: File Name: Las Vegas File

Type: Rtsp Name: RTSP source

Full Path: rtsp:// 192.168.1.198/ufirststream

User ID: admin

Password: ••••••••

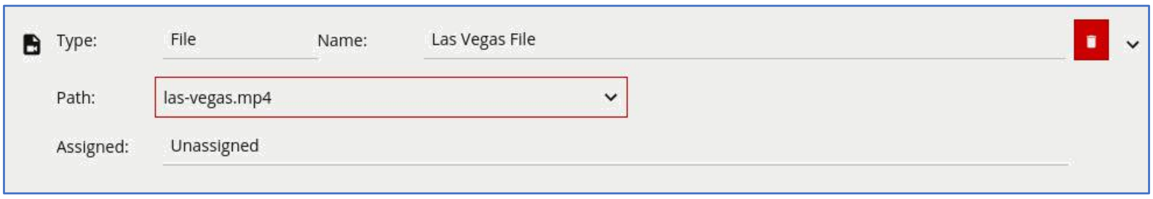
Assigned: Unassigned

6.2.1 Common Properties

- **Type:** The type of the element, e.g. File, RTSP, etc.
- **Name:** The user configured name for the input/output element.
- **Assigned:** Whether the element is assigned to a channel or not.

6.2.2 File Input

The file input supports streaming video from a local file. A range of files are included in the standard firmware for test purposes. Select the desired file from the drop menu:



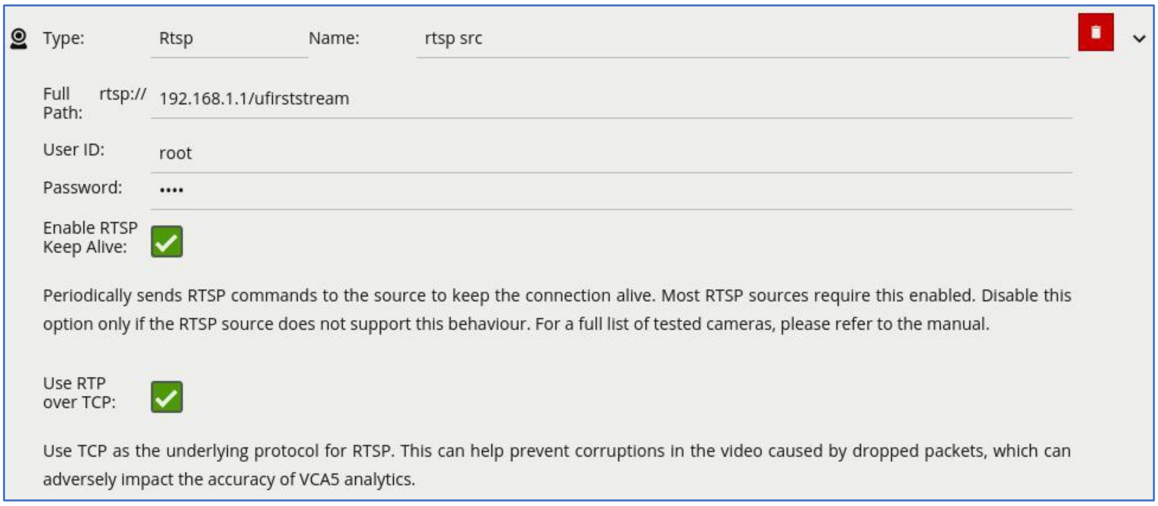
Type: File Name: Las Vegas File

Path: las-vegas.mp4

Assigned: Unassigned

6.2.3 RTSP Input

The RTSP input supports streaming video and audio streams from remote devices such as cameras and video encoders.



Type: Rtsp Name: rtsp src

Full Path: rtsp:// 192.168.1.1/ufirststream

User ID: root

Password: ••••

Enable RTSP Keep Alive: ☑

Periodically sends RTSP commands to the source to keep the connection alive. Most RTSP sources require this enabled. Disable this option only if the RTSP source does not support this behaviour. For a full list of tested cameras, please refer to the manual.

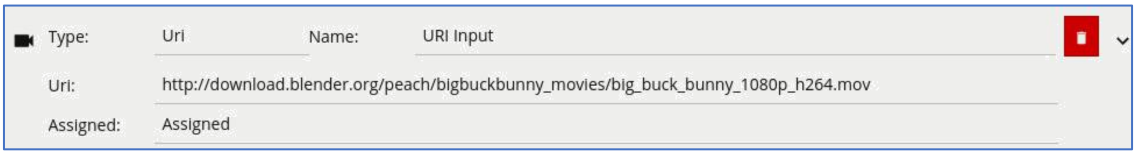
Use RTP over TCP: ☑

Use TCP as the underlying protocol for RTSP. This can help prevent corruptions in the video caused by dropped packets, which can adversely impact the accuracy of VCA5 analytics.

- **Full Path:** The fully qualified URI to the remote RTSP endpoint.
- **User ID:** The username to access the RTSP endpoint (if applicable).
- **Password:** The password to access the RTSP endpoint (if applicable).
- **Enable RTSP Keep Alive:** Periodically sends commands to the RTSP source to keep the RTSP connection alive. Most RTSP sources require this option to be enabled. Disable this option only if the RTSP source does not support this behavior.
- **Use RTP over TCP:** Force the RTP stream to be streamed via TCP (instead of UDP). Wherever possible, RTSP streams should be delivered over TCP and not UDP. This is because UDP transport is not robust against packet loss and dropped packets cause corrupt video which causes VCA to generate false positives.

6.2.4 URI Input

The URI input element supports a range of sources and protocols which can be described by a URI, for example HTTP or remote file sources:



Type: Uri Name: URI Input

Uri: http://download.blender.org/peach/bigbuckbunny_movies/big_buck_bunny_1080p_h264.mov

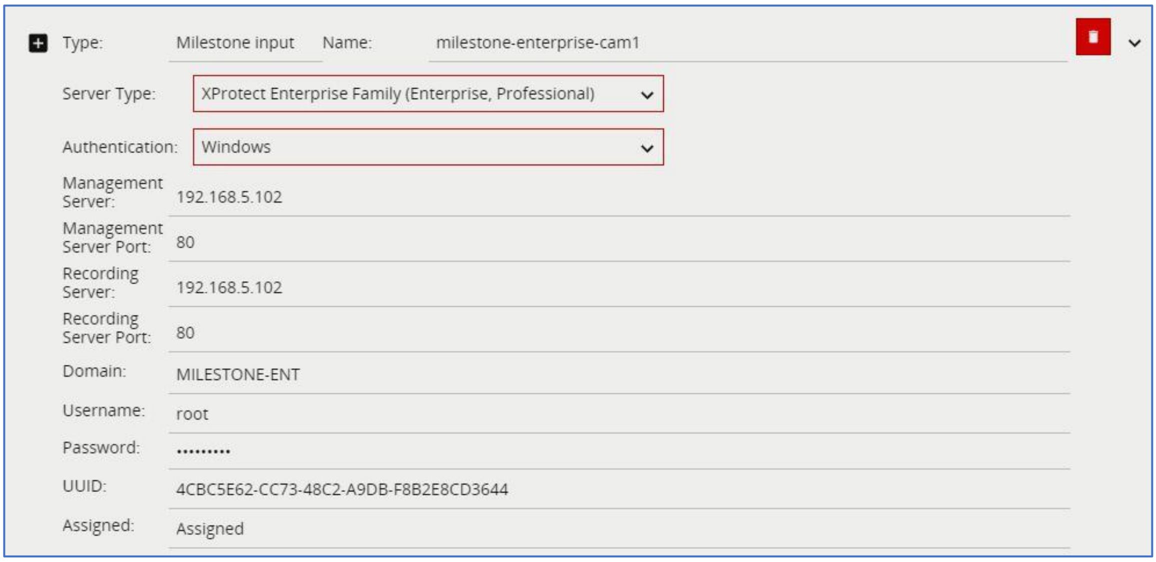
Assigned: Assigned

- **Uri:** The fully qualified URI to the media source containing the protocol, address, port and end-point.

6.2.5 Milestone XProtect VMS Input

The Milestone XProtect input allows video to be received from a compatible Milestone XProtect VMS.

See the Milestone XProtect topic for further details.



Type: Milestone input

Name: milestone-enterprise-cam1

Server Type: XProtect Enterprise Family (Enterprise, Professional)

Authentication: Windows

Management Server: 192.168.5.102

Management Server Port: 80

Recording Server: 192.168.5.102

Recording Server Port: 80

Domain: MILESTONE-ENT

Username: root

Password: ••••••••

UUID: 4CBC5E62-CC73-48C2-A9DB-F8B2E8CD3644

Assigned: Assigned

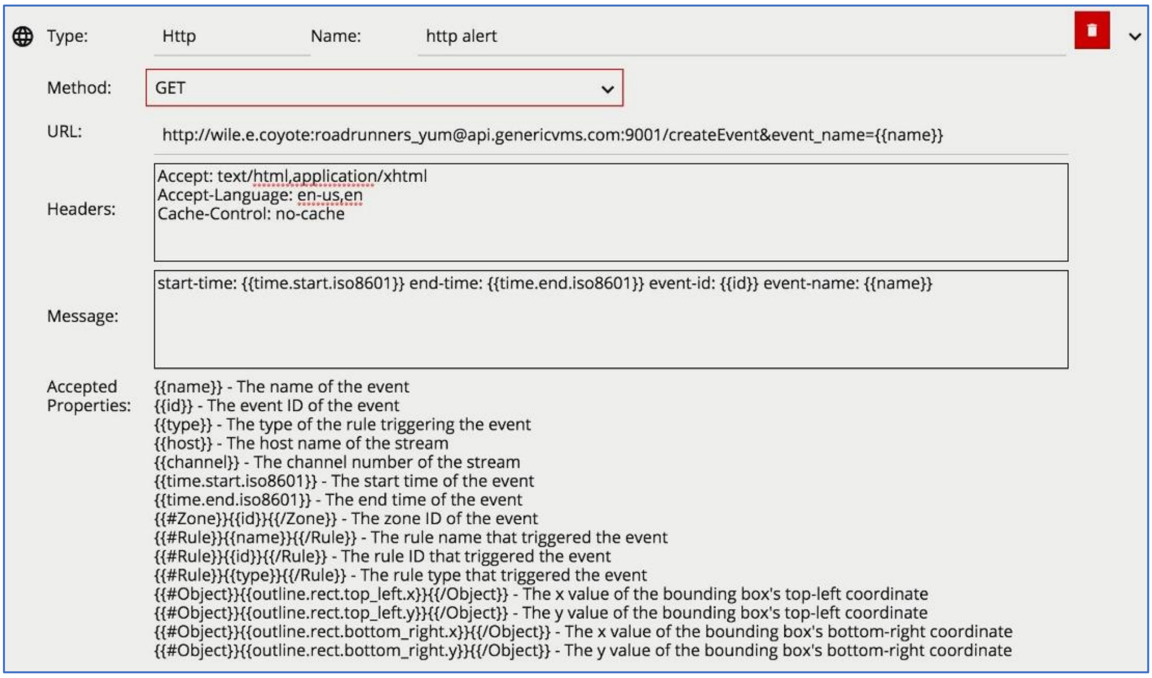
- **Server Type:** The type of the XProtect server(s).
- **Authentication:** The type of authentication to use with the Milestone Xprotect server. Can be either Basic Authentication or Windows Authentication. See the Milestone XProtect topic for more details.
- **Stream:** The video stream index (0-index based). Where the source camera supports multiple streams, this setting selects which camera stream to retrieve from the Milestone XProtect server.
- **Management Server:** The IP address or hostname of the XProtect Management Server.
- **Management Server Port:** The port that the XProtect Management Server is listening on.
- **Recording Server:** The IP address or hostname of the XProtect Recording Server.
- **Recording Server Port:** The port that the XProtect Recording Server is listening on.
- **Domain:** The Windows domain element of the user-id for the XProtect user.
- **Username:** The username to use to log into the XProtect server(s).
- **Password:** The password to use to log into the XProtect server(s).
- **UUID:** The UUID of the channel within XProtect (see the Milestone XProtect topic for more details).

6.3 Adding an Output

Outputs are added in the same way as inputs.

6.3.1 HTTP Output

The HTTP output sends HTTP requests to a remote endpoint when a VCA event occurs. The URL, HTTP headers and message body are all configurable with a mixture of plain text and Tokens, which are substituted with event-specific values at the time an event is generated.



Type: Http
Name: http alert
Method: GET
URL: http://wile.e.coyote:roadrunners_yum@api.genericvms.com:9001/createEvent&event_name={{name}}

Headers:

```
Accept: text/html,application/xhtml
Accept-Language: en-us,en
Cache-Control: no-cache
```

Message:

```
start-time: {{time.start.iso8601}} end-time: {{time.end.iso8601}} event-id: {{id}} event-name: {{name}}
```

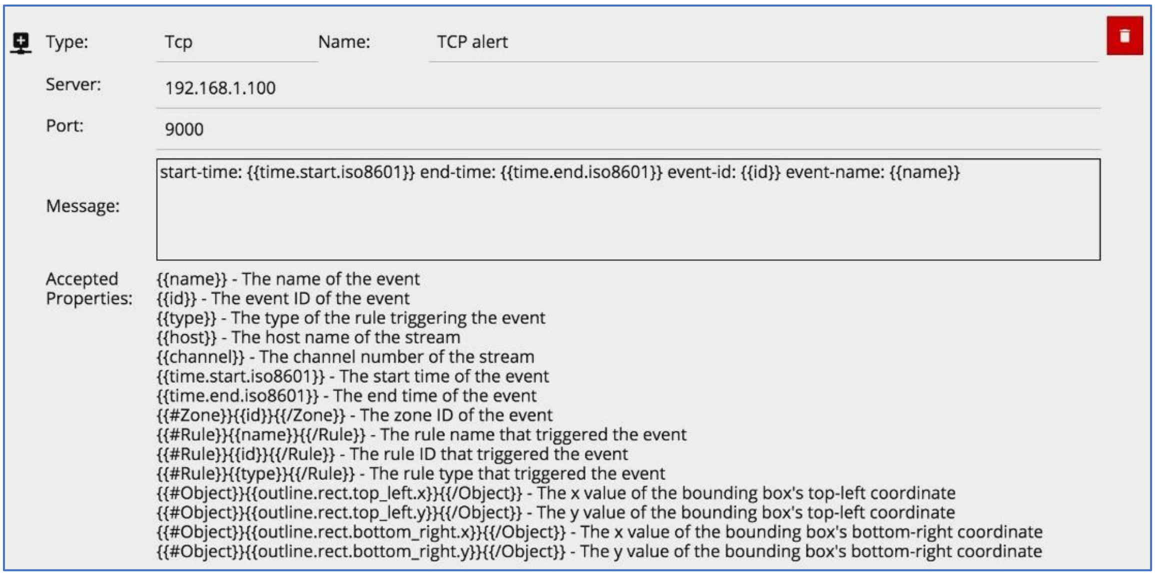
Accepted Properties:
{{name}} - The name of the event
{{id}} - The event ID of the event
{{type}} - The type of the rule triggering the event
{{host}} - The host name of the stream
{{channel}} - The channel number of the stream
{{time.start.iso8601}} - The start time of the event
{{time.end.iso8601}} - The end time of the event
{{#Zone}}{{id}}{{/Zone}} - The zone ID of the event
{{#Rule}}{{name}}{{/Rule}} - The rule name that triggered the event
{{#Rule}}{{id}}{{/Rule}} - The rule ID that triggered the event
{{#Rule}}{{type}}{{/Rule}} - The rule type that triggered the event
{{#Object}}{{outline.rect.top_left.x}}{{/Object}} - The x value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.top_left.y}}{{/Object}} - The y value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.bottom_right.x}}{{/Object}} - The x value of the bounding box's bottom-right coordinate
{{#Object}}{{outline.rect.bottom_right.y}}{{/Object}} - The y value of the bounding box's bottom-right coordinate

- **Method:** The HTTP request method (verb). Can be one of GET, POST, PUT, DELETE, HEAD. This setting will normally be specified by the remote server API.
- **URL:** The remote URL to request when executing the HTTP action. As illustrated in the figure, the URL can contain embedded user credentials, remote server port, and any supported Tokens, which will be replaced with event-specific data at the time an event is generated. If specifying user credentials in plain text is undesirable, they can be specified in the Header section encoded as a base 64 string as part of a standard HTTP Authorization header.
- **Headers:** Specifies any HTTP headers to send in the HTTP request. Examples may include Authorization or Content-Type headers. Any necessary headers will normally be specified by the remote server API. Each header should be placed on a new line. When the headers are transmitted a CRLF (\r\n) is automatically inserted between each header, and between the last header and the message body.
- **Message:** Specifies the body of the HTTP request. Can be a mixture of plain text and any supported Tokens, which will be replaced with event-specific data at the time an event is generated. A default template is automatically added when an HTTP output is created.

See the Tokens topic for full details about the token system and example templates.

6.3.2 TCP Output

The TCP output sends data to a remote TCP server when a VCA event occurs. The format of the body is configurable with a mixture of plain text and Tokens, which are substituted with event-specific values at the time an event is generated.



Type: Tcp
Name: TCP alert
Server: 192.168.1.100
Port: 9000
Message: start-time: {{time.start.iso8601}} end-time: {{time.end.iso8601}} event-id: {{id}} event-name: {{name}}

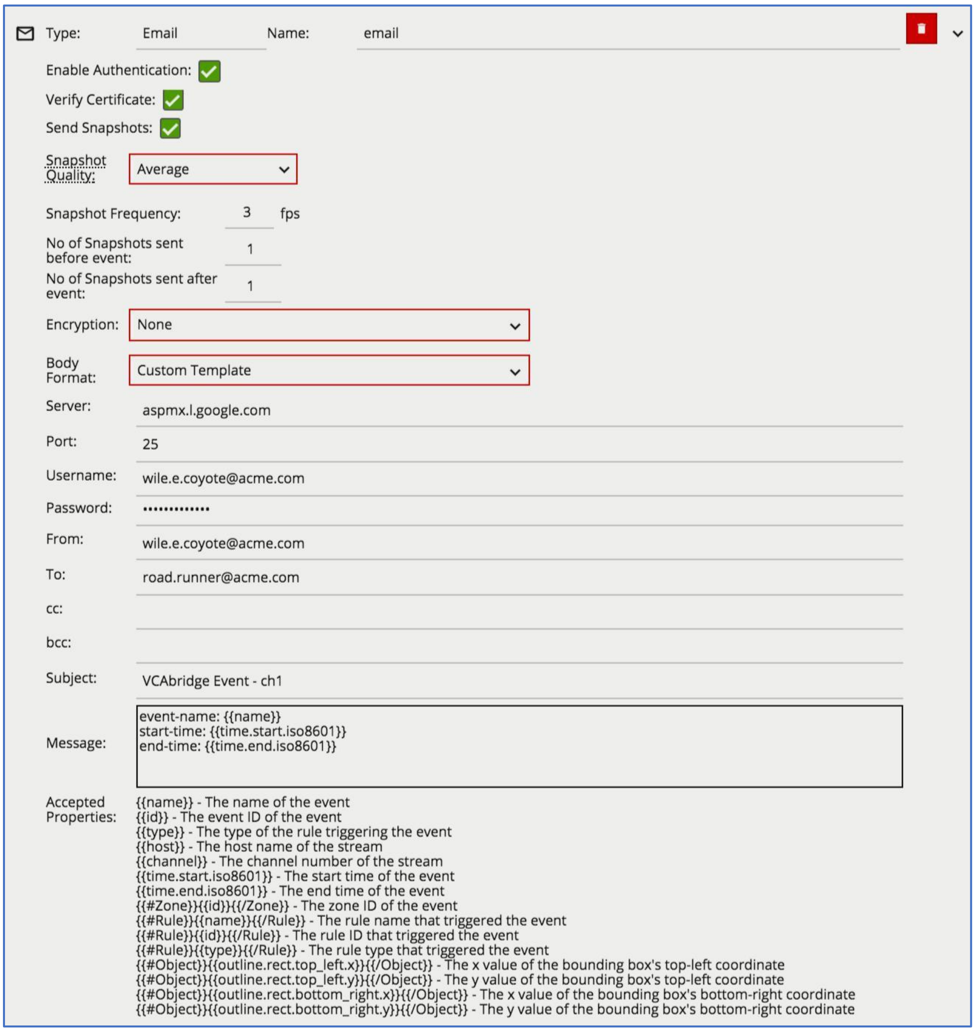
Accepted Properties:
{{name}} - The name of the event
{{id}} - The event ID of the event
{{type}} - The type of the rule triggering the event
{{host}} - The host name of the stream
{{channel}} - The channel number of the stream
{{time.start.iso8601}} - The start time of the event
{{time.end.iso8601}} - The end time of the event
{{#Zone}}{{id}}{{/Zone}} - The zone ID of the event
{{#Rule}}{{name}}{{/Rule}} - The rule name that triggered the event
{{#Rule}}{{id}}{{/Rule}} - The rule ID that triggered the event
{{#Rule}}{{type}}{{/Rule}} - The rule type that triggered the event
{{#Object}}{{outline.rect.top_left.x}}{{/Object}} - The x value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.top_left.y}}{{/Object}} - The y value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.bottom_right.x}}{{/Object}} - The x value of the bounding box's bottom-right coordinate
{{#Object}}{{outline.rect.bottom_right.y}}{{/Object}} - The y value of the bounding box's bottom-right coordinate

- **Server:** The IP address or hostname of the remote TCP server where the event data should be transmitted.
- **Port:** The port on which the remote TCP server is listening for incoming TCP connections.
- **Message:** The body of the TCP message to transmit. Can be a mixture of plain text and any supported Tokens, which will be replaced with event-specific data at the time an event is generated. A default template is automatically added when a TCP output is created.

See the Tokens topic for full details about the token system and example templates.

6.3.3 Email Output

The email output sends events in pre- or user-configured formats to remote email servers. If an email output is added to a channel, a VCA event causes a corresponding email to be sent to the configured recipient.



Type:	Email
Name:	email
Enable Authentication:	☑
Verify Certificate:	☑
Send Snapshots:	☑
Snapshot Quality:	Average
Snapshot Frequency:	3 fps
No of Snapshots sent before event:	1
No of Snapshots sent after event:	1
Encryption:	None
Body Format:	Custom Template
Server:	aspmx.l.google.com
Port:	25
Username:	wile.e.coyote@acme.com
Password:	•••••••••••••
From:	wile.e.coyote@acme.com
To:	road.runner@acme.com
cc:	
bcc:	
Subject:	VCAbridge Event - ch1

Message:

```
event-name: {{name}}
start-time: {{time.start.iso8601}}
end-time: {{time.end.iso8601}}
```

Accepted Properties:

```
{{name}} - The name of the event
{{id}} - The event ID of the event
{{type}} - The type of the rule triggering the event
{{host}} - The host name of the stream
{{channel}} - The channel number of the stream
{{time.start.iso8601}} - The start time of the event
{{time.end.iso8601}} - The end time of the event
{{#Zone}}{{id}}{{/Zone}} - The zone ID of the event
{{#Rule}}{{name}}{{/Rule}} - The rule name that triggered the event
{{#Rule}}{{id}}{{/Rule}} - The rule ID that triggered the event
{{#Rule}}{{type}}{{/Rule}} - The rule type that triggered the event
{{#Object}}{{outline.rect.top_left.x}}{{/Object}} - The x value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.top_left.y}}{{/Object}} - The y value of the bounding box's top-left coordinate
{{#Object}}{{outline.rect.bottom_right.x}}{{/Object}} - The x value of the bounding box's bottom-right coordinate
{{#Object}}{{outline.rect.bottom_right.y}}{{/Object}} - The y value of the bounding box's bottom-right coordinate
```

- **Enable Authentication:** Check to enable SMTP authentication.
- **Send Snapshots:** Check to attach annotated snapshots to the email.
- **Verify Certificate:** Check to verify the remote SSL certificate.
- **Snapshot Quality:** Select the quality of the snapshots attached to the email. Refer to the table below for further information regarding snapshot sizes in KB
- **Snapshot Frequency:** Set the snapshot capture rate in Frames Per Second (FPS).
- **No of Snapshots sent before event:** Set the number of pre-event snapshots to attach to the email.
- **No of Snapshots sent after event:** Set the number of post-event snapshots to attach to the email.
- **Encryption:** The type of encryption used for SMTP communication. Valid options are None, SSL and STLS.
- **Body Format:** The format of the email alert. Valid options are: Custom Template or SureView Immix. Select SureView Immix to send email alerts to a SureView Immix System. See below for further details regarding the configuration of custom email templates with the Custom Template option.
- **Server:** SMTP server address.
- **Port:** SMTP server port.
- **Username:** The username of the email account used to send emails on the SMTP server.

- **Password:** The password of the email account used to send emails on the SMTP server.
- **From:** The email address of the sender.
- **To:** The email address of the recipient.
- **Cc:** Email address(es) of any carbon-copy recipients.
- **Bcc:** Email address(es) of any blind carbon-copy recipients.
- **Subject:** The subject of the email.
- **Body Template:** Tokenized template of the email body. See below for further details.

6.3.3.1 Custom Templates

The email output supports the configuration of custom templates for the email body. Templates define the content of the message which is sent in response to an event. The template consists of plain text and a range of Tokens, which are substituted for event-specific values at the time the event is generated.

See the Tokens topic for full details of the range of tokens supported and example email body templates. A list of common tokens is provided on the email output configuration page for quick reference.

6.3.3.2 Snapshot Size Lookup Table

The size of the snapshots (in KB) depends on a combination of the resolution of the image and the quality setting. Approximate average snapshot sizes (in KB) for a complex scene at various resolutions are listed in the following table:

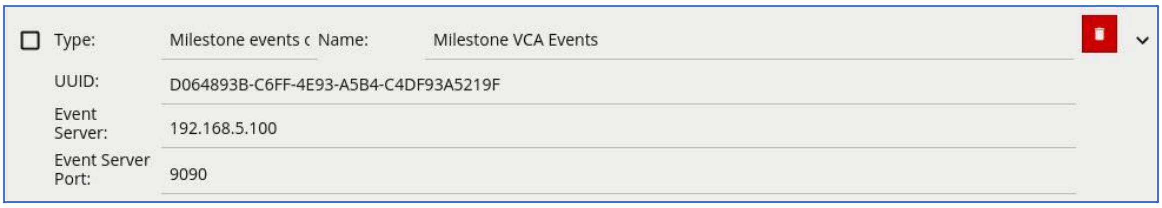
Resolution	Best	Good	Average	Low	Worst
1080p (1920x1080)	635	390	300	225	120
720p (1280x720)	336	202	156	117	63
480p (864x480)	190	115	89	67	36
D1 (720x576)	190	115	89	67	36
VGA (640x480)	160	97	75	56	30

Note that these figures are for guidance only and will vary in practice depending on the complexity of the scene.

6.3.4 Milestone XProtect Event Server Output

The Milestone XProtect Event Server output sends VCA events to a Milestone XProtect VMS Event Server.

For more details, refer to the Milestone XProtect topic.



□ Type: Milestone events c Name: Milestone VCA Events

UUID: D064893B-C6FF-4E93-A5B4-C4DF93A5219F

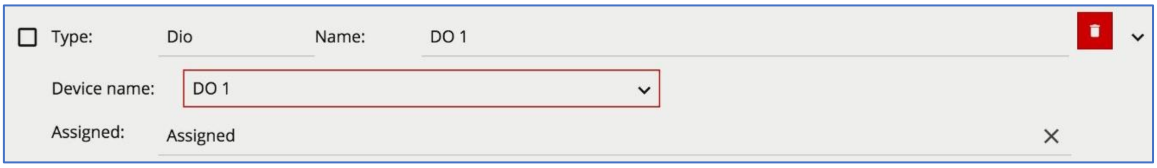
Event Server: 192.168.5.100

Event Server Port: 9090

- **UUID:** The XProtect UUID that identifies the channel to which VCA events correspond. This should match the UUID specified for the Milestone XProtect Input.
- **Event Server:** The IP address or hostname of the XProtect Event Server.
- **Event Server Port:** The port on which the XProtect Event Server is listening for events.

6.3.5 Digital Output

A digital output is a logical representation of a digital output hardware channel. To configure the properties of a physical digital output channel, such as activation time, refer to the Digital IO page.



□ Type: Dio Name: DO 1

Device name: DO 1

Assigned: Assigned ✕

- **Device Name:** The physical digital output channel assigned to the logical digital output.

Once the logical digital output has been created, it must be assigned to a channel in order to be triggered. When assigned to a channel, any VCA event will trigger the digital output. Multiple logical digital outputs are supported, and physical digital output channels can be assigned to more than one logical digital output. This may be useful where there are fewer digital output channels than VCA channels.

6.4 Next Steps

Once inputs and outputs have been created, they must be added to a channel in order to start a VCA stream.

Go to the channel settings page

Chapter 7

Digital IO

VCA supports digital input and output hardware for interfacing with third party systems. Digital inputs can be used as triggers for events in VCA, and digital outputs can be triggered by a VCA or other system event.

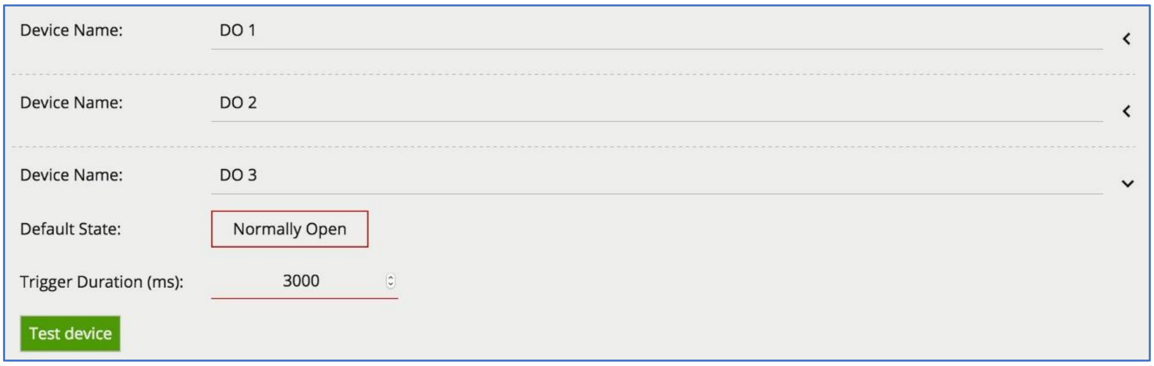
NOTE: Digital inputs are not currently supported. Only digital outputs can currently be used.

Configuration of the digital inputs and outputs consists of three tasks:

- Configure the physical digital IO channels
- Assign physical digital IO channels to logical inputs and outputs
- Assign logical inputs and outputs to specific VCA channels

7.1 Digital IO Device Configuration

From the Home page select **Edit Digital Inputs/Outputs** to access the digital IO device configuration page.



Device Name: DO 1

Device Name: DO 2

Device Name: DO 3

Default State: Normally Open

Trigger Duration (ms): 3000

The digital IO device configuration page contains a section for each digital IO device. Note that the number of digital IO channels available depends on the specific hardware device in use.

7.1.1 Digital Outputs

Digital outputs can be triggered by a range of analytics event sources. Each digital output channel has the following properties:

- **Device Name:** The name of the digital output channel.

- **Default State:** The default state of the digital output when it’s not triggered. Can be one of Normally Open or Normally Closed. When configured as Normally Open, the digital output will be open (low) when inactive and closed (high) when activated. When configured as Normally Open, the behavior is inverted. Refer to the table for more information.

Default State	DO Inactive	DO Active
Normally Open	Open (Low)	Closed (High)
Normally Closed	Closed (High)	Open (Low)

- **Trigger Duration(ms):** The duration of activation of the digital output in milliseconds. When the digital output is triggered, it will be activated for the specified duration, after which time it will be deactivated. Triggers received while the digital output is already active are ignored.
- **Test Device:** Clicking the button activates the digital output for the specified duration. This is useful to test that external devices are correctly connected to the digital output.

Once the digital output hardware has been configured, digital output hardware channels must be assigned to logical outputs on the Inputs and Outputs page.

7.2 Digital IO Connections

On a VCA bridge device, a number of built-in digital IO channels are provided. Different models support different numbers of IO channels. Refer to the quick start guide that came with the device for details of the digital IO connector pinout. The quick start guides are also available from the VCA support portal

7.3 Logical Digital IO

Once the physical digital IO hardware has been configured, logical inputs and outputs must be created.

Refer to the Inputs and Outputs page for more information.

7.4 Assigning Digital IO to a Channel

In order for digital IO channels to interact with VCA and system events, the logical digital inputs and outputs must be assigned to a channel. Refer to the Channels page for more information.

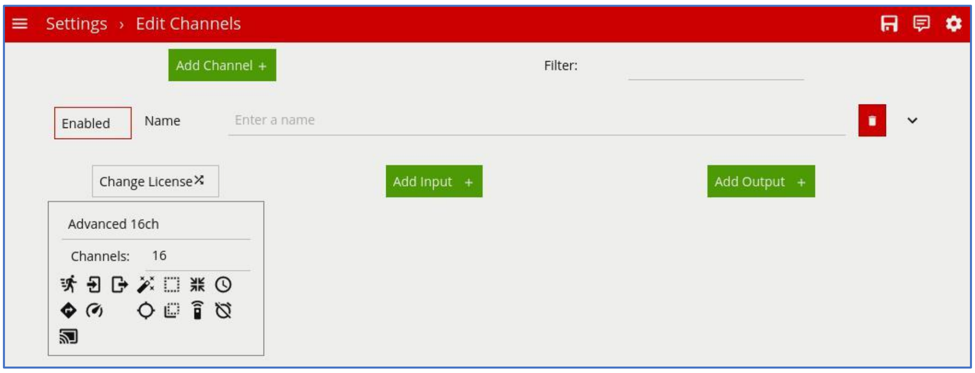
Chapter 8

Channels

A channel consumes media from **inputs**, performs some analysis (VCA) and produces metadata which is passed to **outputs**. Thus, channels are the entities which link inputs to outputs and on which VCA processing takes place. At least one channel must be configured for the system to perform any useful work.

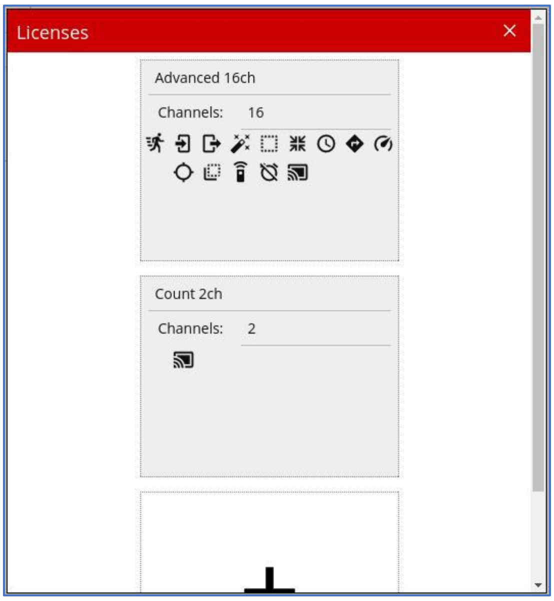
8.1 Adding a Channel

Clicking the **Add Channel** button adds an empty channel to the configuration. Click the expand/collapse icon ‹ to expand and collapse the channel configuration parameters.



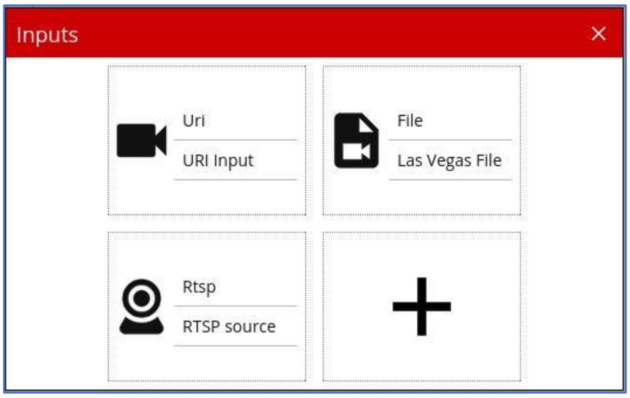
8.2 Changing the License Assigned to the Channel

Every channel needs a valid license to perform VCA processing. Licenses can be configured from the Activation page. When a new channel is added a default, license is assigned based on the unused licenses available. If there are multiple licenses configured which support different features it may be necessary to change the license by clicking the **Change License** button and selecting the corresponding license from the list:

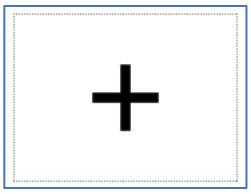


8.3 Adding Inputs and Outputs to a Channel

Click the **Add Input** or **Add Output** button and select the corresponding input or output from the list.



If there are no inputs or outputs configured, or a new input/output is required, clicking the **+** icon navigates directly to the Inputs and Outputs page where a new input/output element can be configured.

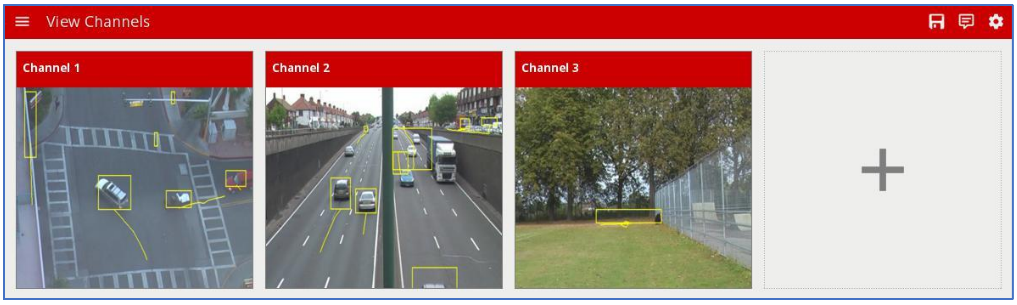


8.4 Deleting a Channel

To delete a channel, click the delete button 🗑.

8.5 Viewing Channels

Once a channel has been configured with a valid input it can be viewed on the **View Channels** page. A thumbnail (or an error message) is displayed for each configured channel.



Click a thumbnail to view the channel and configure VCA related settings.

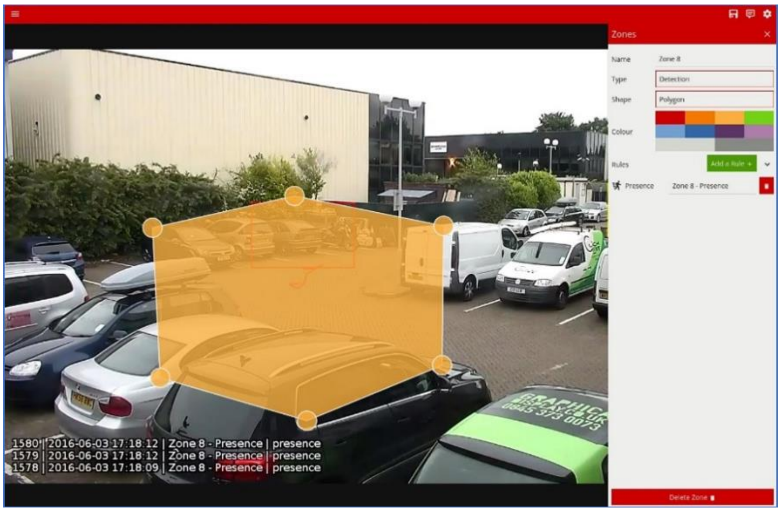
8.6 Next Steps

Once a channel has been configured, **zones** and **rules** can be configured to detect specific scenarios.

Chapter 9

Zones

Zones are the detection areas on which VCA **rules** operate. In order to detect a specific behavior, a zone must be configured to specify the area where a rule applies.



```
1580 | 2016-06-03 17:18:12 | Zone 8 - Presence | presence
1579 | 2016-06-03 17:18:12 | Zone 8 - Presence | presence
1578 | 2016-06-03 17:18:09 | Zone 8 - Presence | presence
```

Zones

Name: Zone 8

Type: Detection

Shape: Polygon

Presence: Zone 8 - Presence

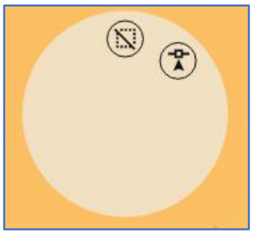
9.1 Adding a Zone

Zones can be added in multiple ways:

- Double-click anywhere on the video display.
- Click the **Create Zone** button in the zone settings menu.
- Right-click or tap-hold to display the context menu and select the add zone icon

9.2 The Context Menu

Right-clicking or tap-holding (on mobile devices) displays a context menu which contains commands specific to the current context.



The possible actions from the context menu are:

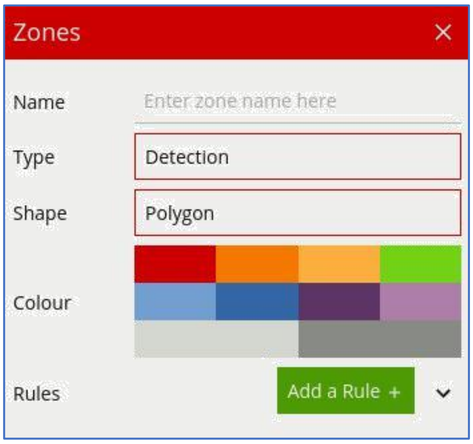
- Adds a new zone.
- Deletes an existing zone.
- Adds a node to a zone.
- Deletes an existing node from a zone.

9.3 Positioning Zones

To change the position of a zone, click and drag the zone to a new position. To change the shape of a zone, drag the nodes to create the required shape. New nodes can be added by double-clicking on the edge of the zone or clicking the add node icon from the context menu.

9.4 Zone Specific Settings

The zone configuration menu contains a range of zone-specific configuration parameters:



Zones ×

Name: Enter zone name here

Type: Detection

Shape: Polygon

Colour

Rules: Add a Rule +

- Name: The name of the zone, which appears in event notifications.
- Type: The type of the zone. Can be one of:
- Detection: A zone which detects tracked objects and to which rules can be applied.
- Non-detection: A zone which specifies an area that should be excluded from VCA analysis. Objects are not detected in non-detection zones. Useful for excluding areas of potential nuisance alarms from a scene (e.g. waving trees, flashing lights, etc).
- Shape: The shape of the zone. Can be one of:
- Polygon: A polygonal detection area with at least three nodes. Rules apply to the whole area.
- Line: A single- or multi-segment line with at least two nodes. Rules apply to the length of the line.
- Colour: The colour of the zone.
- Rules: The rules applied to the zone. See the Rule Configuration for more information.

9.5 Deleting a Zone

Zones can be deleted in the following ways:

- Select the zone and click the **Delete Zone** button from the zone settings menu.
- Select the zone, display the context menu and select the delete zone icon

9.6 Next Steps

Once a zone has been configured, **rules** can be applied to detect specific scenarios. See Rule Configuration for more information.

Chapter 10

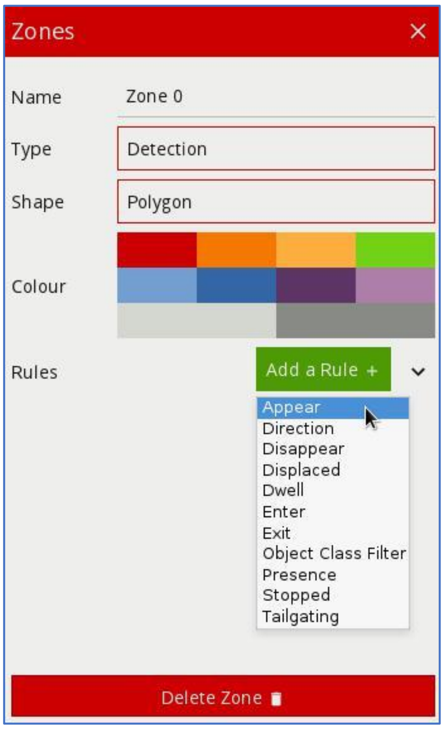
Rules

Rules are applied to zones to detect specific events. Examples of the kind of rules that can be applied are detection of the presence of an object within a zone, or detection of an object moving in a specific direction within a zone.

Rules are configured in the same place as **zones** on the Zones Page.

10.1 Adding a Rule

Select the zone to which the rule should be added and click the **Add a Rule** button Add a Rule + . Select the desired rule from the drop menu.



Zones

Name: Zone 0

Type: Detection

Shape: Polygon

Colour

Rules

To delete a rule, click the corresponding delete icon 🗑

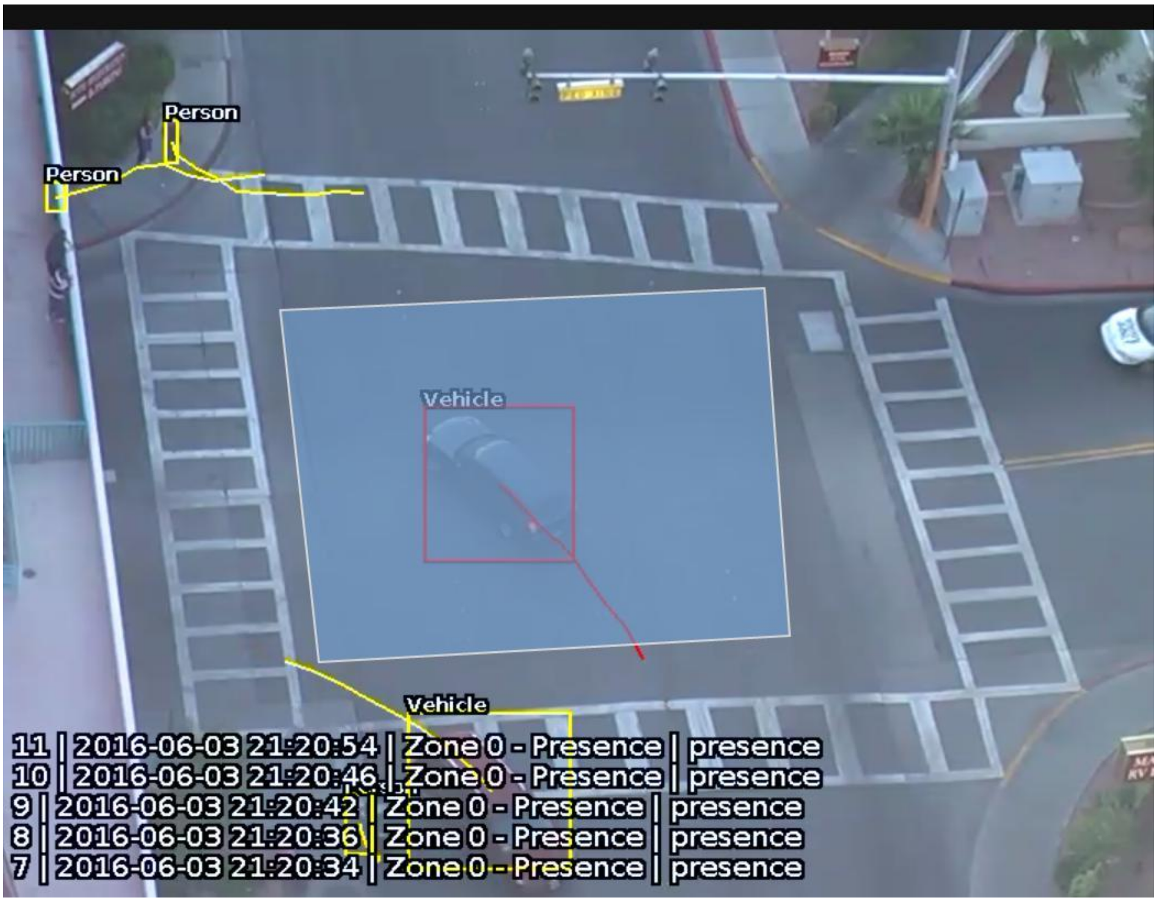
10.2 General Concepts

10.2.1 Object Display

Detected objects are annotated with a **bounding box** and a **trail**. Objects can be rendered in two states:

- **Non-alarmed:** Default rendered in yellow. A detected object which does not meet any criteria to trigger a rule and raise an event.
- **Alarmed:** Default rendered in red. A detected object which has triggered one or more rules. Causes an event to be raised.

When an event is raised, the default settings render details of the event in the lower half of the video stream.



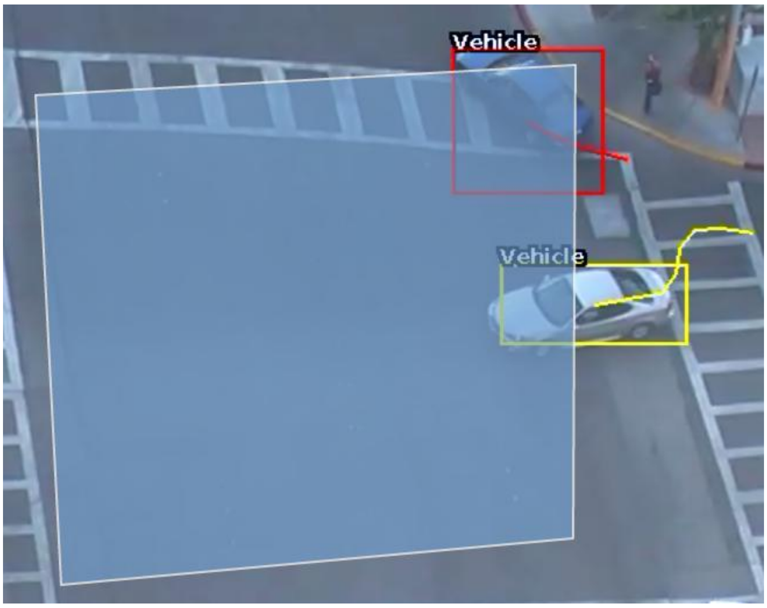
```
11 | 2016-06-03 21:20:54 | Zone 0 - Presence | presence
10 | 2016-06-03 21:20:46 | Zone 0 - Presence | presence
9 | 2016-06-03 21:20:42 | Zone 0 - Presence | presence
8 | 2016-06-03 21:20:36 | Zone 0 - Presence | presence
7 | 2016-06-03 21:20:34 | Zone 0 - Presence | presence
```

10.2.2 Object Trails

The **trail** shows the history of where the object has been. Depending on the **calibration** the trail can be drawn from the **centroid** or the **mid-bottom** point of the object. (See Advanced Settings for more information).

10.2.3 Trail Importance

The trail is important for determining how a rule is triggered. The intersection of the trail point with a zone or line determines whether a rule is triggered or not. The following image illustrates this point: the blue vehicle's trail intersects with the detection zone and is rendered in red. Conversely, while the white vehicle intersects the detection zone, its trail does not (yet) intersect and hence it has not triggered the rule and is rendered in yellow.

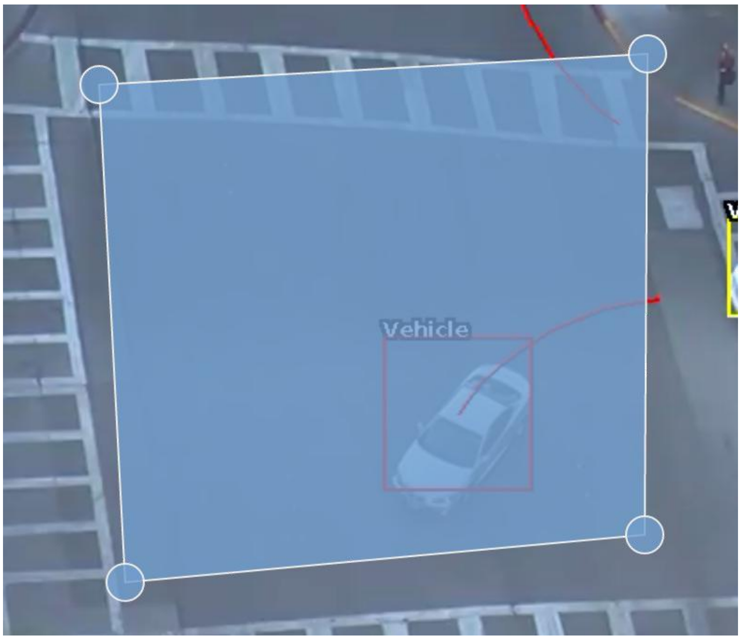


10.3 Rule Types

The behavior of each of the rule types is explained below.

10.3.1 Presence

Objects that are present inside a zone or pass over a line trigger the rule and raise an event.

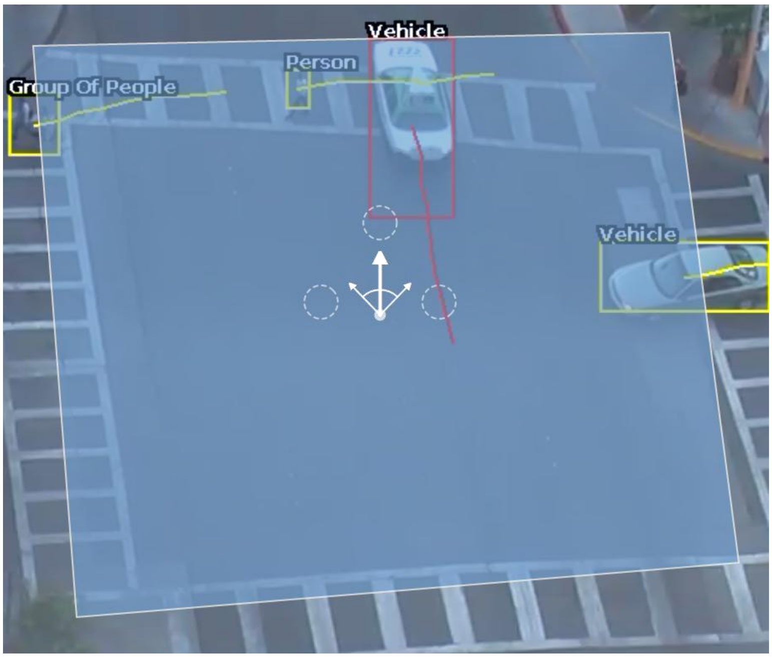


10.3.2 Direction

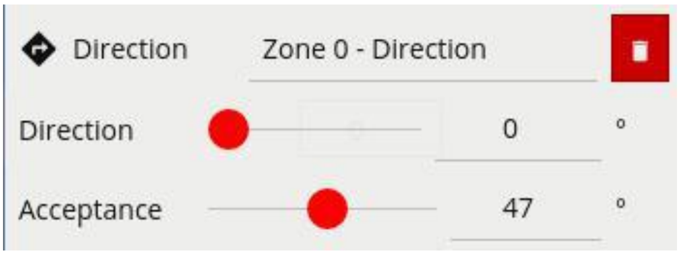
The direction rule detects objects moving in a specific direction. Configure the direction and acceptance angle by moving the arrows on the direction control widget. The primary direction is indicated by the large central arrow. The acceptance angle is the angle between the two smaller arrows.

Objects that travel in the configured direction (within the limits of the acceptance angle), through a zone or over a line trigger the rule and raise an event.

The following image illustrates how the white car moving in the configured direction triggers the rule whereas the other objects do not.



The rule parameters can also be configured in the zones control menu:



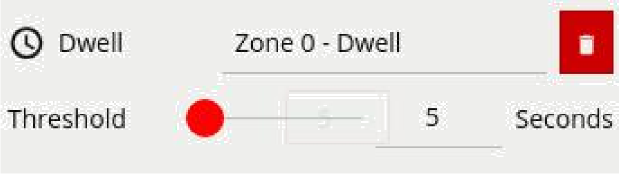
Direction Zone 0 - Direction

Direction 0 °

Acceptance 47 °

10.3.3 Dwell

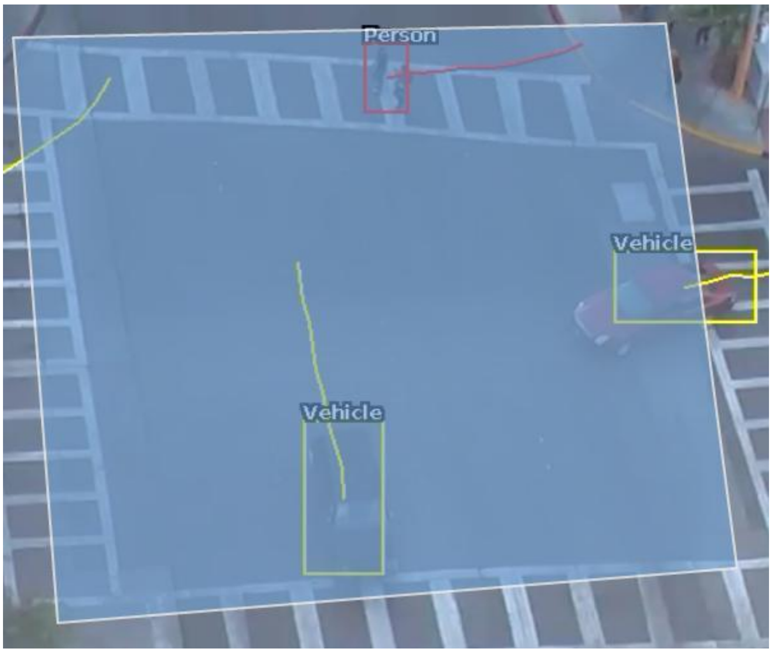
Objects that dwell inside a zone for longer than the defined amount of time will trigger the rule and raise an event.



Dwell Zone 0 - Dwell

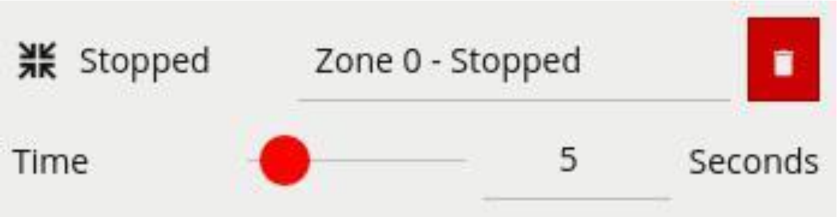
Threshold 5 Seconds

In the following image, the person has been in the zone for longer than 5 seconds, whereas the vehicle has not. Hence the person generates an event but the vehicle does not.



10.3.4 Stopped

The stopped rule detects objects which are stationary inside a zone for longer than the specified amount of time. **Note:** The stopped rule does not detect abandoned objects. It only detects objects which have moved at some point and then become stationary.



Stopped Zone 0 - Stopped

Time 5 Seconds

10.3.5 Enter and Exit

The enter rule detects when objects enter a zone. In other words, when objects cross from the outside of a zone to the inside of a zone.
Conversely, the exit rule detects when an object leaves a zone: when it crosses the border of a zone from the inside to the outside.

Note: Enter and exit rules differ from appear and disappear rules, as follows:

- Whereas the enter rule detects already-tracked objects crossing the zone border from outside to inside, the appear rule detects objects which start being tracked within a zone (e.g. appear in the scene through a door).
- Whereas the exit rule detects already-tracked objects crossing the zone border from inside to outside, the disappear rule detects objects which stop being tracked within the zone (e.g. leave the scene through a door).

10.3.6 Appear and Disappear

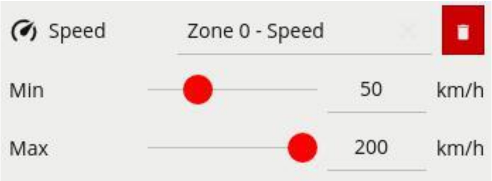
The appear rule detects objects that start being tracked within a zone, e.g. a person who appears in the scene from a doorway.

Conversely, the disappear rule detects objects that stop being tracked within a zone, e.g. a person who exits the scene through a doorway.

Note: The appear and disappear rules differ from the enter and exit rules as detailed in the enter and exit rule descriptions.

10.3.7 Speed

The speed rule detects objects that are moving in the range of speeds defined by a lower and upper boundary.



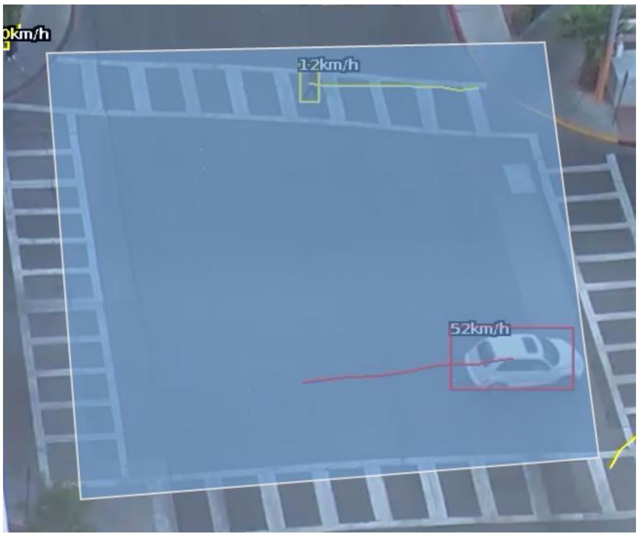
Speed: Zone 0 - Speed

Min: 50 km/h

Max: 200 km/h

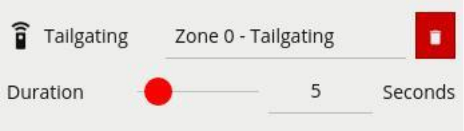
Note: The channel must be **calibrated** in order for the speed filter to be available.

The following image illustrates how the speed rule triggers on the car moving at 52km/h but the person moving at 12km/h falls outside the configured range (50-200km/h) and thus does not trigger the rule.



10.3.8 Tailgating

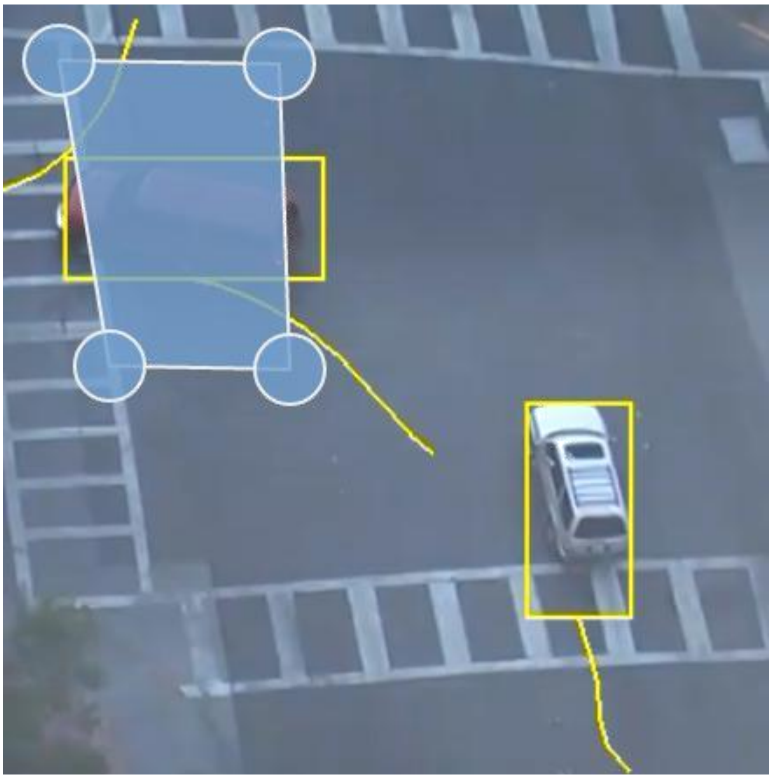
The tailgating rule detects objects which cross through a zone or over a line within quick succession of each other. The time limit for an object to pass without triggering the tailgating rule is configured in the zones control:



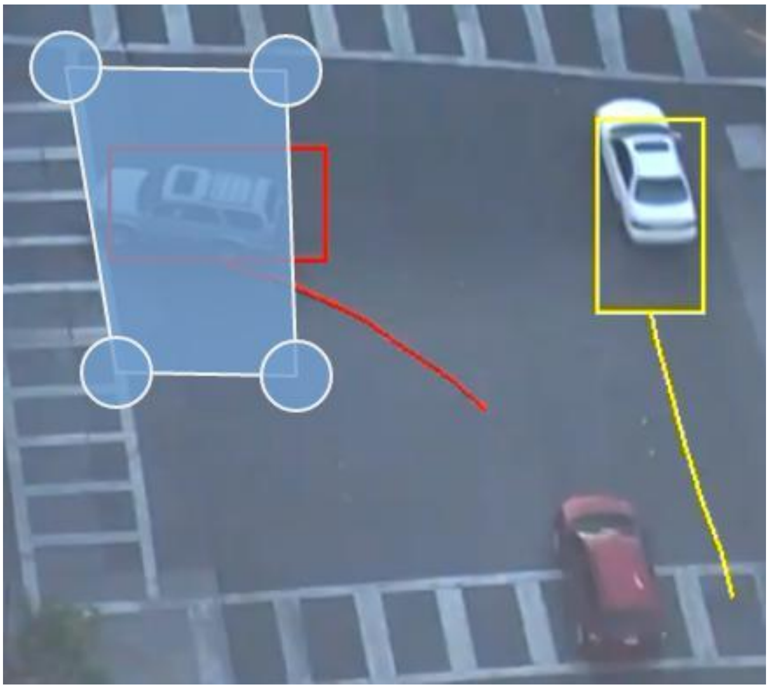
Tailgating: Zone 0 - Tailgating

Duration: 5 Seconds

In this example, object 1 is about to cross a detection line. Another object (object 2) is following closely behind. The tailgating detection threshold is set to 5 seconds. That is, any object crossing the line within 5s of an object having already crossed the line will trigger the object tailgating rule.

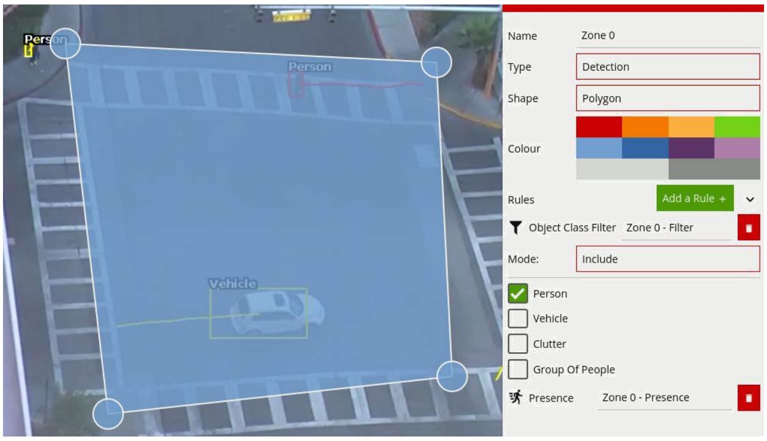


Object 2 crosses the line within 5 seconds of object 1. This triggers the tailgating filter and raises an event.



10.3.9 Object Classification Filter

The object classification filter allows rules to operate on a selection of object classes (e.g. person, vehicle).



Name: Zone 0

Type: Detection

Shape: Polygon

Colour

Rules: Add a Rule +

Object Class Filter: Zone 0 - Filter

Mode: Include

☑ Person

□ Vehicle

□ Clutter

□ Group Of People

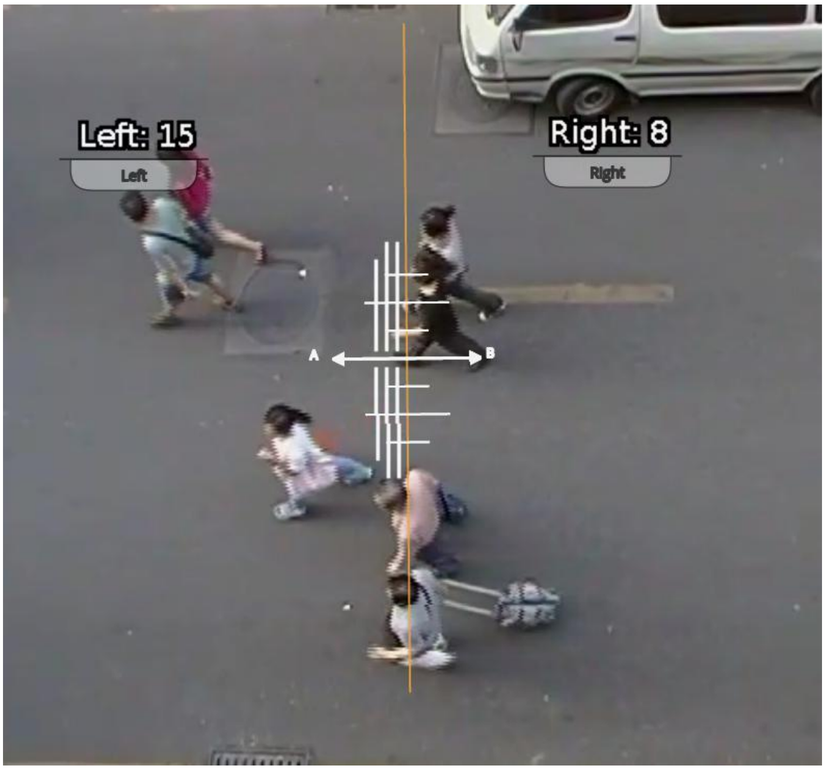
Presence: Zone 0 - Presence

- **Mode:** Selects whether to include or exclude the object class from the rule.
- **Include** only allows selected object classes to trigger any configured rules.
- **Exclude** allows all object classes except those selected to trigger any configured rules.

The previous image illustrates how an **Include** rule with the **Person** class selected includes only Person objects in the presence rule. The vehicle in the zone is filtered out since the **Vehicle** class is not included in the classification filter selection.

Note: the channel must be **calibrated** for the object classification filter to be available.

10.3.10 Counting Line



A counting line is a detection filter optimized for bi-directional object counting (e.g. people or vehicles)

in busier detection scenarios. Examples of such applications may include:

- People counting with overhead cameras in a retail environment.
- Vehicle counting with overhead cameras on public highways.

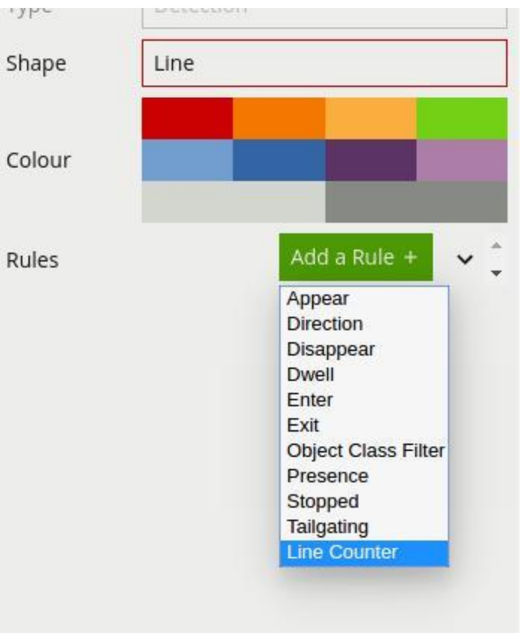
In some scenes such as entrances with camera installed overhead, the counting line typically will generate a higher accuracy count than using the counters connected to an e.g. presence rule.

An event is generated every time an object crosses the line in the selected direction. If multiple objects cross the line together, multiple corresponding events are generated. The events generated by the counting line can be tied to counters in the normal manner.

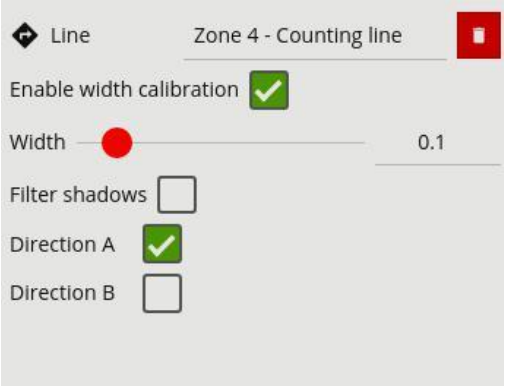
NOTE: The maximum number of counting line filters that can be applied per video channel is 5.

10.3.10.1 Enabling the Counting Line

The counting line is enabled by adding the **Line Counter** rule to a detection line. Click on the line and add the Line Counter rule:



The counting line has a number of configuration options, each of which is described below:



- **Direction A:** Enable counting in the 'A' direction (one direction of the line).
- **Direction B:** Enable counting in the 'B' direction (the opposite of the 'A' direction).
- **Filter Shadows:** Toggles the shadow filter (see below for more information including the limitations of the shadow filter).
- **Enable Width Calibration:** Enables the width calibration which allows more accurate counting. See below for further information about how to calibrate the counting line.
- **Width Slider:** Sets the calibration width. Can also be performed by dragging the calibration lines displayed orthogonal to the counting line. See below for further information regarding counting line calibration.

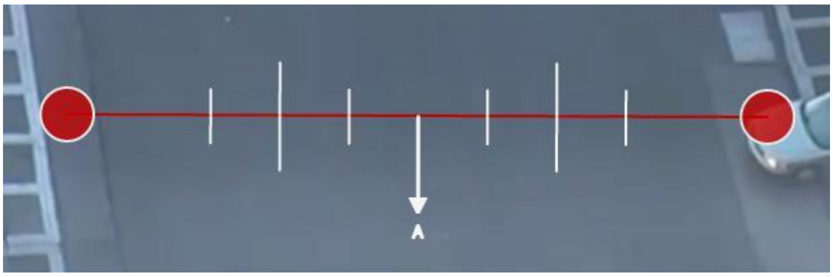
10.3.10.2 Assigning Counters to Counting Lines

A counting line by itself simply generates events when an object to be counted is detected. In order to actually count the events, counters (one for each direction) can be created and configured to count the events generated by the line. To create counters, see the Counters topic.

10.3.10.3 Calibrating the Counting Line

In order to generate accurate counts, the counting line requires calibration. Unlike the object tracking function engine, this cannot be performed at a general level for the whole scene using the 3D calibration tool. This is because the counting line is not always placed on the ground plane: it may be placed at any orientation at any location in the scene. For example, a counting line could be configured vertically with a side-on camera view.

Instead of the 3D calibration tool, the counting line has its own calibration setting. Two bars equidistant from the center of the line represent the width of the expected object. This allows the counting line to reject noise and also count multiple objects.



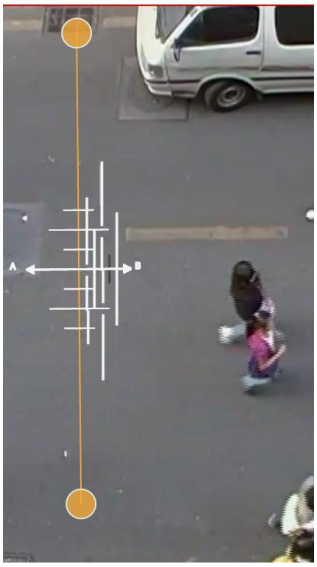
To calibrate the counting line:

- Select the counting line.
- Check the **Width Calibration** option.
- Use the mouse wheel or drag the calibration markers to adjust the distance between the calibration markers until the distance is approximately the size of the objects to be counted. Alternatively, move the **Width Calibration** slider to achieve the same result.
- The calibration width is displayed on the settings panel under the counting line rule. This figure can also be edited directly to change the calibration width.
- The small markers on either side of the big markers indicate the minimum and maximum width which is counted as a single object.

10.3.10.4 Counting Line Calibration Feedback

To enable the user to more accurately configure the calibration for the counting line, the widths of detected objects are displayed as an overlay next to the counting line when objects pass over it. By default, this display option is enabled. However, if it does not appear, ensure that the option is enabled on the Burnt-in Annotation settings.

The calibration feedback is rendered as black and white lines on either side of the counting line on the Zones configurations page. Each line represents an object detected by the counting algorithm. The width of the line shows the width of the object detected by the line. The last few detections are displayed for each direction with the latest one appearing closest to the counting line.



Each detection is counted as a number of objects based on the current width calibration. This is displayed as follows:

- Black line: Event not counted
- Solid white line: Event counted as one object
- Broken white line: Event counted as multiple objects indicated by the number of line segments.

Using the feedback from the calibration feedback annotation, the width calibration can be fine-tuned to count the correct sized objects and filter out spurious detections.

10.3.10.5 Shadow Filter

The counting line features a shadow filter which is designed to remove the effects of object shadows affecting the counting algorithm. Shadows can cause inaccurate counting results by making an object appear larger than its true size or by joining two or more objects together. If shadows are causing inaccurate counting, the shadow filter should be enabled by selecting the **Shadow Filter** check box for the line. It is recommended that the shadow filter only be enabled when shadows are present because the algorithm can mistake certain parts of an object for shadows and this may lead to worse counting results. This is especially the case for objects that have little contrast compared to the background (e.g. people wearing black coats against a black carpet).

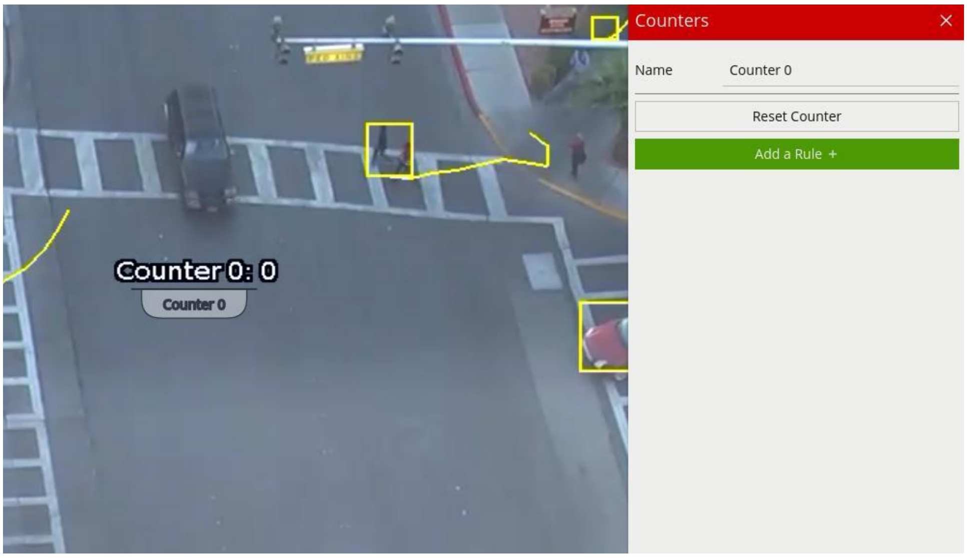
10.4 Next Steps

Learn how to configure counters on a channel.

Chapter 11

Counters

VCA supports counters which can be configured to count various things such as the number of times a rule has triggered or the number of people crossing a line.



Counters ×

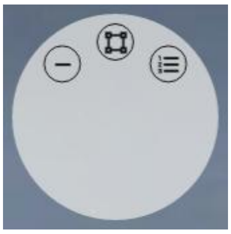
Name Counter 0

Reset Counter

Add a Rule +

11.1 Adding a Counters

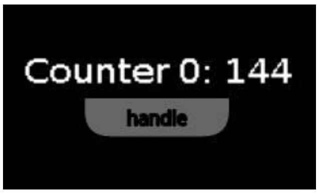
Counters can be added by right clicking (or tap-holding on mobile devices) on the video to show the context menu:



- ☰ Click or tap to add a counter.

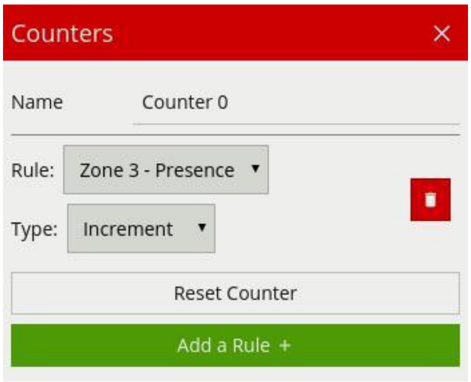
11.2 Positioning Counters

Counters can be repositioned by grabbing the ‘handle’ beneath the counter name and moving the counter to the desired location.



11.3 Counter Specific settings

The counter configuration menu contains a range of counter-specific configuration parameters:



Counters

Name: Counter 0

Rule: Zone 3 - Presence

Type: Increment

- **Name:** The name of the counter. Editing this field changes the counter name displayed on the video.
- **Add a Rule:** Adds a new rule as a counter source trigger.
- **Rule:** A pre-existing counter trigger source (which was previously added by the **Add a Rule** button).
- **Type:** The type of the counter trigger. Can be one of **Increment, Decrement** or **Occupancy**. See below for more information about the different types.
- **Reset Counter:** Resets the counter value to zero.

11.3.1 Counter Source Types

Counter trigger sources can be configured to be **Increment, Decrement** or **Occupancy**. Each mode is described below:

- **Increment:** When the rule is triggered the counter, value will be incremented.
- **Decrement:** When the rule is triggered the counter, value will be decremented.
- **Occupancy:** The counter will show the current number of active triggers in the zone. E.g. if a presence rule is triggered and two objects are currently triggering the presence rule, the counter will show the value of ‘2’.

11.4 Next Steps

Learn how to calibrate a channel.

Chapter 12

Calibration

Camera calibration is required in order for VCA to classify objects into different object classes. Once a channel has been calibrated, VCA can infer real-world object properties such as speed, height and area and classify objects accordingly.

Camera calibration is split into the following sub-topics:

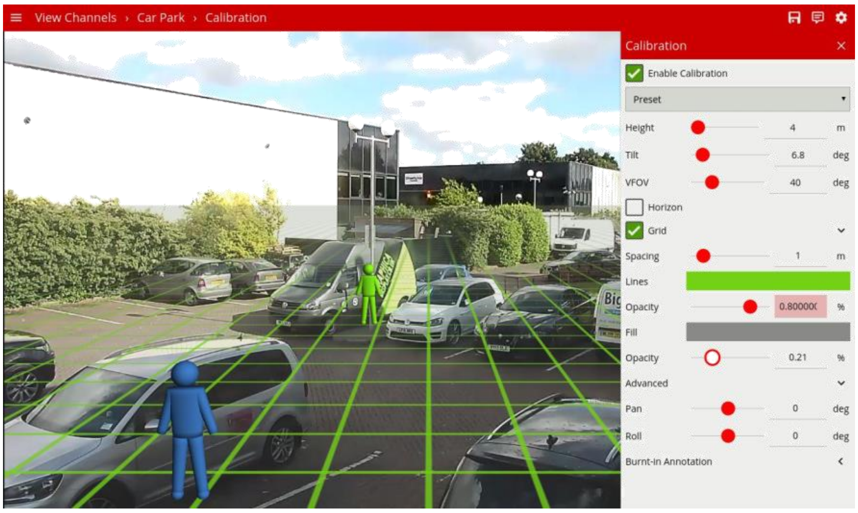
- Enabling Calibration
- Calibration Controls
- Calibrating a Channel
- Advanced Calibration Parameters

12.1 Enabling Calibration

By default, calibration is disabled. To enable calibration on a channel, check the **Enable Calibration** checkbox.

12.2 Calibration Controls

The calibration page contains a number of elements to assist with calibrating a channel as easily as possible. Each is described below.



☑ Enable Calibration

Height 4 m

Tilt 6.8 deg

VFOV 40 deg

□ Horizon

☑ Grid

Spacing 1 m

Lines 🟩

Opacity 0.80000(%

Fill ▨

Opacity 0.21 %

Pan 0 deg

Roll 0 deg

12.2.1 3D Graphics Overlay

During the calibration process, the features in the video image need to be matched with a 3D graphics overlay. The 3D graphics overlay consists of a green grid that represents the ground plane. Placed on the ground plane are a number of 3D mimics (people-shaped figures) that represent the dimensions of a person with the current calibration parameters. The calibration mimics are used for verifying the size of a person in the scene and are 1.8 meters tall.

The mimics can be moved around the scene to line up with people (or objects which are of a known, comparable height) to a person.

12.2.2 Mouse Controls

The calibration parameters can be adjusted with the mouse as follows: - Click and drag the ground plane to change the camera tilt angle. - Use the mouse wheel to adjust the camera height. - Drag the slider to change the vertical field of view.

Note: The sliders in the control panel can also be used to adjust the camera tilt angle and height.

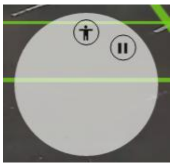
12.2.3 Control Panel Items

The control panel (shown on the right-hand side in the image above) contains the following controls:

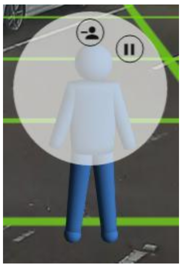
- **Height:** Adjusts the height of the camera
- **Tilt:** Adjusts the tilt angle of the camera
- **VFOV:** Adjusts the *vertical* field of view of the camera. **Note:** A correct value for the camera vertical field of view is important for accurate calibration and classification.
- **Horizon:** Enables/disables the horizon display. Useful to line up against a horizon in a deep scene.
- **Grid:** Enables/disables the ground plane grid display. The expand/collapse control (<) exposes additional settings to vary the colour, opacity and size of the ground plane grid.
- **Advanced:** Exposes advanced settings for controlling the pan and roll of the camera.
- **Burnt-in Annotation:** Exposes the Burnt-in Annotation controls for convenience.

12.2.4 Context Menu Items

Right-clicking the mouse (or tap-and-hold on a tablet) on the grid displays the context menu:



Performing the same action on a mimic displays the mimic context menu:



The possible actions from the context menu are:

- ⏸ Pause the video. Pausing the video can make it easier to align mimics up with objects in the scene.
- ▶ Re-starts playing the video after it was previously paused.
- 🧍 Adds an extra mimic to the ground plane.
- −👤 Removes the currently selected mimic from the ground plane

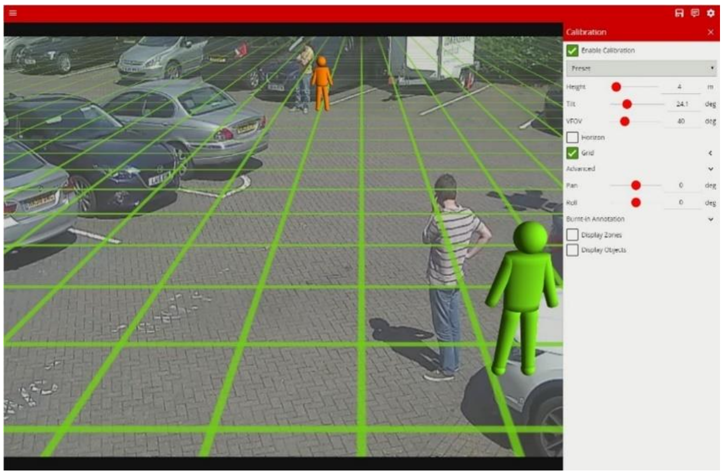
12.3 Calibrating a Channel

Calibrating a channel is necessary in order to estimate object parameters such as height, area, speed and classification. If the height, tilt angle and vertical field of view corresponding to the installation are known, these can simply be entered as parameters in the appropriate fields in the control panel.

If, however, these parameters are not explicitly known this section provides a step-by-step guide to calibrating a channel.

12.3.1 Step 1: Find People in the Scene

Find some people, or some people-sized objects in the scene. Try to find a person near the camera, and a person further away from the camera. It is useful to use the play/pause control to pause the video so that the mimics can be accurately placed. Place the mimics on top of or near the people:



Calibration

☑ Enable Calibration

Preset

Height 4 m

Tilt 24.1 deg

VFOV 40 deg

☐ Horizon

☑ Grid

Advanced

Pan 0 deg

Roll 0 deg

Burnt-in Annotation

☐ Display Zones

☐ Display Objects

12.3.2 Step 2: Enter the Camera Vertical Field of View

Determining the correct vertical field of view is important for an accurate calibration. The following table shows pre- calculated values for vertical field of view for different sensor sizes.

	Focal Length(mm)	1	2	3	4	5	6	7	8	9	10	15	20	30	40	50
CCD Size (in)	CCD Height(mm)															
1/6“	1.73	82	47	32	24	20	16	14	12	11	10	7	7	7	7	7
1/4“	2.40	100	62	44	33	27	23	19	17	15	14	9	7			
1/3.6“	3.00	113	74	53	41	33	28	24	21	19	12	11	9	6		
1/3.2“	3.42	119	81	59	46	38	32	27	24	21	16	13	10	7		
1/3“	3.60	122	84	62	48	40	33	29	25	23	20	14	10	7	5	
1/2.7“	3.96	126	89	67	53	43	37	32	28	25	22	15	11	8	6	
1/2“	4.80	135	100	77	62	51	44	38	33	30	27	18	14	9	7	5
1/1.8“	5.32	139	106	83	67	56	48	42	37	33	30	20	15	10	8	6
2/3“	6.60		118	95	79	67	58	50	45	40	37	25	19	13	9	8
1“	9.60		135	116	100	88	77	69	62	56	51	35	27	18	14	11
4/3“	13.50			132	119	107	97	88	80	74	68	48	37	25	19	15

If the table does not contain the relevant parameters, the vertical FOV can be estimated by viewing the extremes of the image at the top and bottom. Note that without the correct vertical FOV, it may not be possible to get the mimics to match people at different positions in the scene.

12.3.3 Step 3: Enter the Camera Height

If the camera height is known, type it in directly. If the height is not known, estimate it as far as possible and type it in directly.

12.3.4 Step 4: Adjust the Tilt Angle and Camera Height

Adjust the camera tilt angle (and height if necessary) until both mimics are approximately the same size as a real person at that position in the scene. Click and drag the ground plane to change the tilt angle and use the mouse wheel or control panel to adjust the camera height.

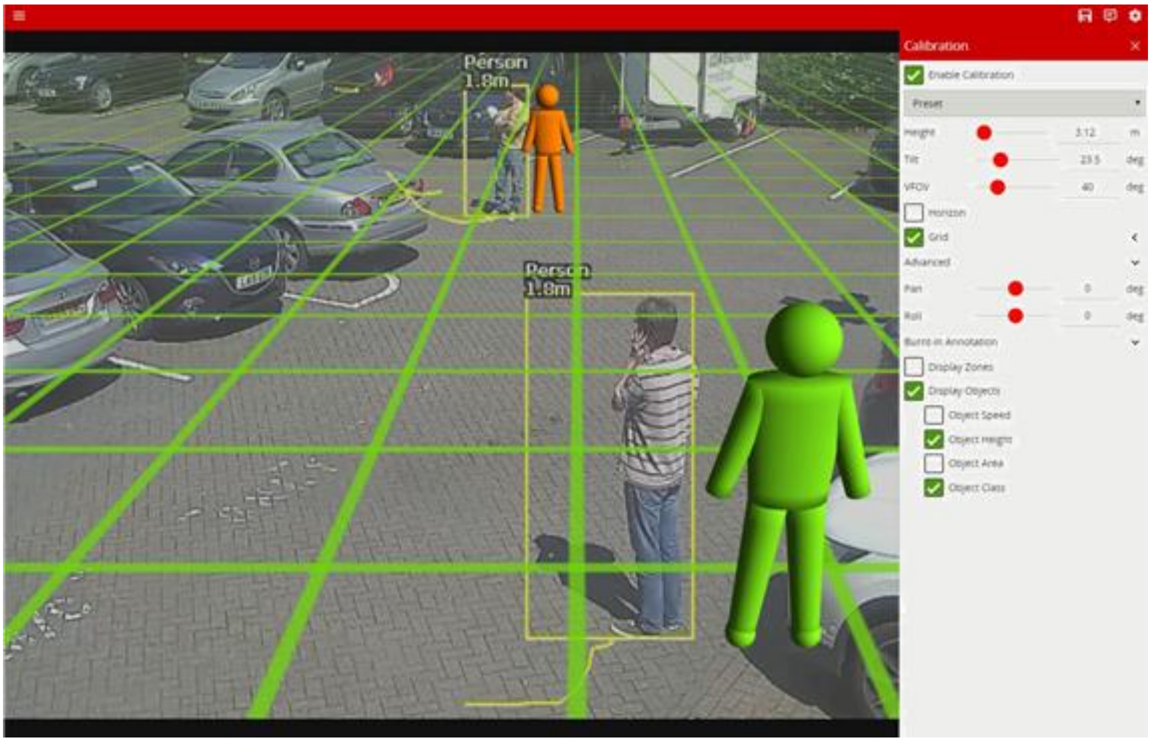
The objective is to ensure that mimics placed at various locations on the grid line up with people or people-sized- objects in the scene.

Once the parameters have been adjusted, the object annotation will reflect the changes and classify the objects accordingly.

12.3.5 Step 5: Verify the Setup

Once the scene is calibrated, drag or add mimics to different locations in the scene and verify they appear at the same size/height as a real person would. Validate that the height and area reported by the VCA annotation looks approximately correct. Note that the burnt-in -annotation settings in the control panel can be used to enable and disable the different types of annotation.

Repeat step 4 until the calibration is acceptable.



Calibration

☑ Enable Calibration

Preset

Height 3.12 m

Tilt 23.5 deg

VFOV 40 deg

□ Horizon

☑ Grid

Advanced

Pan 0 deg

Roll 0 deg

Burnt-in Annotation

□ Display Zones

☑ Display Objects

□ Object Speed

☑ Object Height

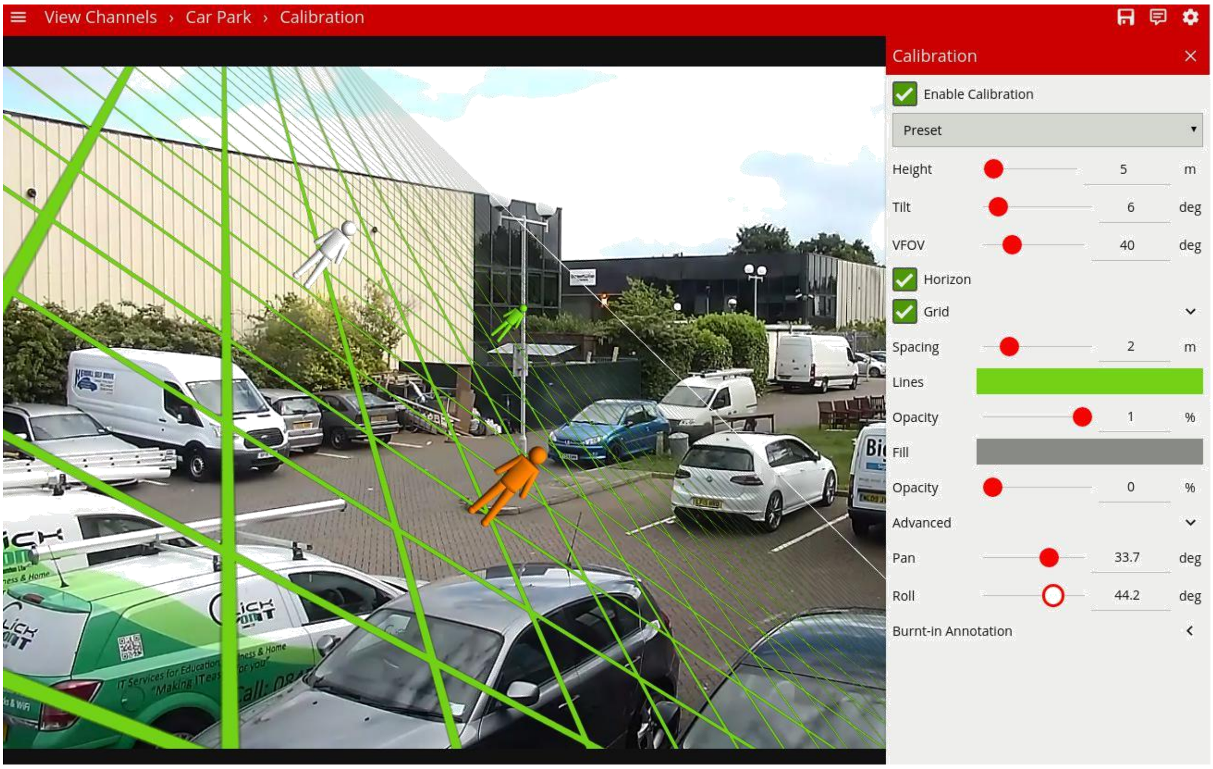
□ Object Area

☑ Object Class

Tip: If it all goes wrong and the mimics disappear or get lost due to an odd configuration, select one of the preset configurations to restore the configuration to normality.

12.4 Advanced Calibration Parameters

The advanced calibration parameters allow the ground plane to be panned and rolled without affecting the camera calibration parameters. This can be useful to visualize the calibration setup if the scene has pan or roll with respect to the camera.



≡ View Channels › Car Park › Calibration

Calibration ×

☑ Enable Calibration

Preset ▾

Height 5 m

Tilt 6 deg

VFOV 40 deg

☑ Horizon

☑ Grid

Spacing 2 m

Lines 🟩

Opacity 1 %

Fill ▨

Opacity 0 %

Advanced

Pan 33.7 deg

Roll 44.2 deg

Burnt-in Annotation

Note: the pan and roll advanced parameters only affect the orientation of the 3D ground plane so that it can be more conveniently aligned with the video scene, and does not actually affect the calibration parameters.

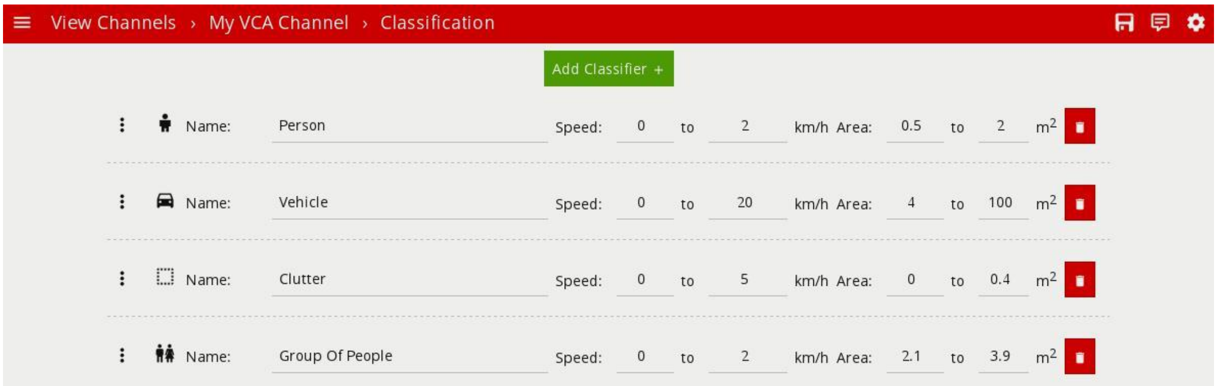
12.5 Next Steps

Once the channel has been calibrated, the **Classification Settings** can be configured.

Chapter 13

Classification

VCA can perform object classification once the camera has been calibrated. The object classification is based on properties extracted from the object including object area and speed. VCA comes pre-loaded with the most common object classes, and in most cases, these will not need to be modified. In some situations, it might be desirable to change the classification parameters, or add new object classes.



View Channels › My VCA Channel › Classification

Add Classifier +

Name:	Person	Speed:	0	to	2	km/h	Area:	0.5	to	2	m^2
Name:	Vehicle	Speed:	0	to	20	km/h	Area:	4	to	100	m^2
Name:	Clutter	Speed:	0	to	5	km/h	Area:	0	to	0.4	m^2
Name:	Group Of People	Speed:	0	to	2	km/h	Area:	2.1	to	3.9	m^2

Each of the UI elements are described below:

- ⋮ : Click and drag to rearrange the order of the classification groups.
- **Icon:** Click the icon to set an icon for the classification group.
- **Name:** Specifies the name of the classification group.
- **Speed:** Sets the speed range for the classification group. Objects which fall within the speed and area ranges will be classified with this group.
- **Area:** Sets the area range for the classification group. Objects which fall within the speed and area ranges will be classified with this group.
- 🗑: Deletes the classification group.

To add a new classification group, click the **Add Classifier** button Add Classifier +

13.1 Object Classification

Objects are classified according to how their calibrated properties match the classification groups. Each classification group specifies a speed range and an area range. Objects which fall within both ranges of speed and area will be classified as being an object of the corresponding class.

Note: If multiple classes contain overlapping speed and area ranges then object classification may be ambiguous (since an object will match more than one class). In this case the actual classification is not specified and may be any one of the overlapping classes.

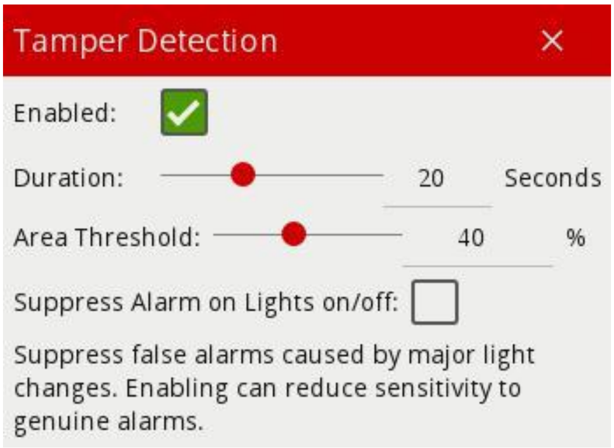
13.2 Next Steps

Learn more about Tamper Detection.

Chapter 14

Tamper Detection

The Tamper Detection module is intended to detect camera tampering events such as bagging, de-focusing and moving the camera. This is achieved by detecting large persistent changes in the image.



Tamper Detection ×

Enabled: ☑

Duration: 20 Seconds

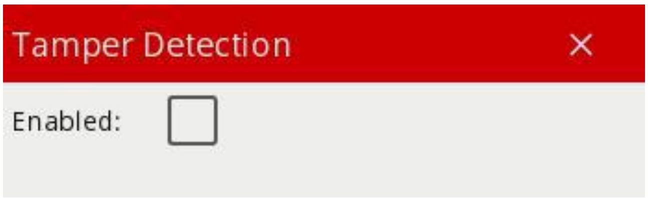
Area Threshold: 40 %

Suppress Alarm on Lights on/off: □

Suppress false alarms caused by major light changes. Enabling can reduce sensitivity to genuine alarms.

14.1 Enabling Tamper Detection

To enable tamper detection, click the **Enabled** checkbox.



Tamper Detection ×

Enabled: □

14.2 Advanced Tamper Detection Settings

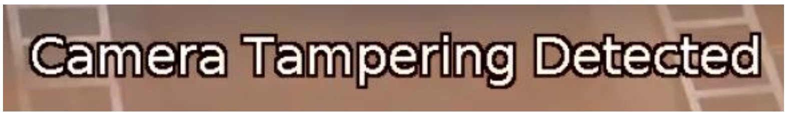
In the advanced tamper detection settings, it is possible to change the thresholds for the area of the image which must be changed and the length of time it must be changed for before the tamper event is triggered.

- **Duration:** the length of time that the image must be persistently changed before the alarm is triggered.
- **Area Threshold:** the percentage area of the image which must be changed for tampering to be triggered.
- **Suppress Alarm on Lights on/off:** Large fast changes to the image lighting such as switching on/off indoor lighting can cause false tamper events. Enable this option if this is likely to be a problem in the area where the camera is installed. However, this option will reduce sensitivity to genuine alarms so it is not recommended to be used if rapid light changes are not likely to be a problem

If false alarms are a problem the duration and/or area should be increased so that large transient changes such as close objects temporarily obscuring the camera do not cause false alarms.

14.3 Notification

When a tamper event is detected, a tamper event is generated. This event is transmitted through any output elements as well as being displayed in the video stream:



Camera Tampering Detected

14.4 Next Steps

Learn more about Scene Change Detection.

Chapter 15

Scene Change Detection

The scene change detection module resets the tracking algorithm when it detects a large persistent change in the image. This prevents the tracking engine from detecting image changes as tracked objects which could be potential sources of false alarms.

The kinds of changes the scene change detection module detects are as follows:

- Sudden movement of a camera (e.g. due to repositioning or the use of a pan-tilt camera).
- Sudden obscuration of a camera (e.g. a vehicle parking in front of a camera obscuring most of its view).
- Gross illumination changes (e.g. lights being switched on/off, dazzling from car headlights).
- Day/night transitions (e.g. when a camera switch's from colour to black/white during a night-day transition)

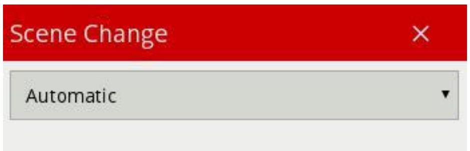
15.1 Scene Change Settings

There are 3 options for the scene change detection mode:

- **Automatic:** Detects scene changes automatically. This is the recommended setting unless the automatic mode is causing difficulties (e.g. re-learning the scene when unnecessary).
- **Manual:** Allows the user to adjust the parameters used by the scene change detection algorithm.
- **Disabled:** Disables the scene change detection.

15.1.1 Automatic

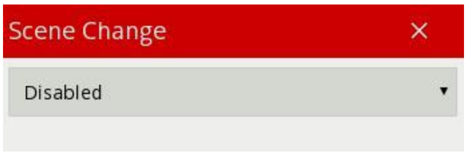
This is the default setting and will automatically use the recommended settings. It is recommended to use the automatic setting unless the scene change detection is causing difficulties.


Scene Change

Automatic

15.1.2 Disabled

Scene change detection is disabled.


Scene Change

Disabled

Note that when the scene change detection is disabled, gross changes in the image will not be detected. For example, if a truck parks in front of the camera the scene change will not be detected and false events may occur as a result.

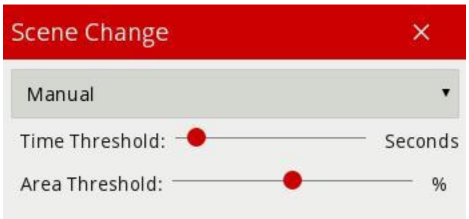
15.1.3 Manual

Allows user configuration of the scene change detection algorithm parameters.

If automatic mode is triggering in situations where it's not desired (e.g. it's too sensitive, or not sensitive enough) then the parameters can be adjusted to manually control the behavior.

In the manual mode, the following settings are available:

- **Time Threshold:** the length of time that the image must be persistently changed before the scene change is triggered and the tracking algorithm is reset.
- **Area Threshold:** the percentage area of the image which must be changed for the scene change to be triggered and the tracking algorithm to be reset.



When both the time and area thresholds are exceeded the scene is considered to have changed and will be reset.

If false scene change detections are a problem, the time and/or area should be increased so that large transient changes such as a close object temporarily obscuring the camera does not cause false scene change detections.

15.2 Notification

When a scene change is detected, the scene is re-learnt and a message is displayed in the event log and annotated on the video

15.3 Next Steps

Learn more about Burnt-in Annotation.

Chapter 16

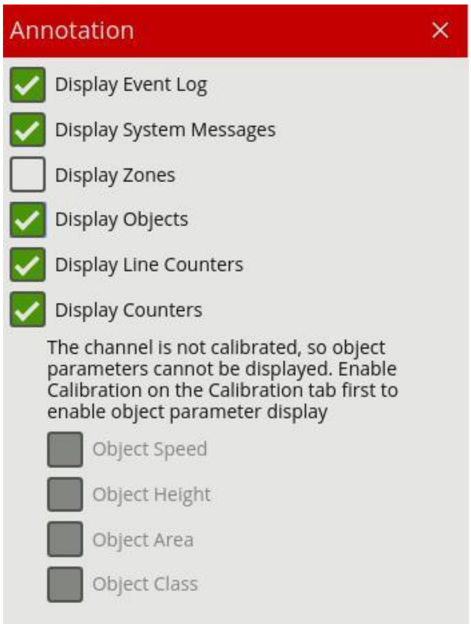
Burnt-in Annotation

The Burnt-in Annotation setting allows the VCA annotation to be burnt in to the raw video stream.

Annotations can include tracked objects, counters and system messages.

16.1 Burnt-in Annotation Settings

The burnt-in annotation settings control which portions of the VCA metadata (objects, events, etc) are rendered into the video stream.



Annotation

☑ Display Event Log

☑ Display System Messages

☐ Display Zones

☑ Display Objects

☑ Display Line Counters

☑ Display Counters

The channel is not calibrated, so object parameters cannot be displayed. Enable Calibration on the Calibration tab first to enable object parameter display

☐ Object Speed

☐ Object Height

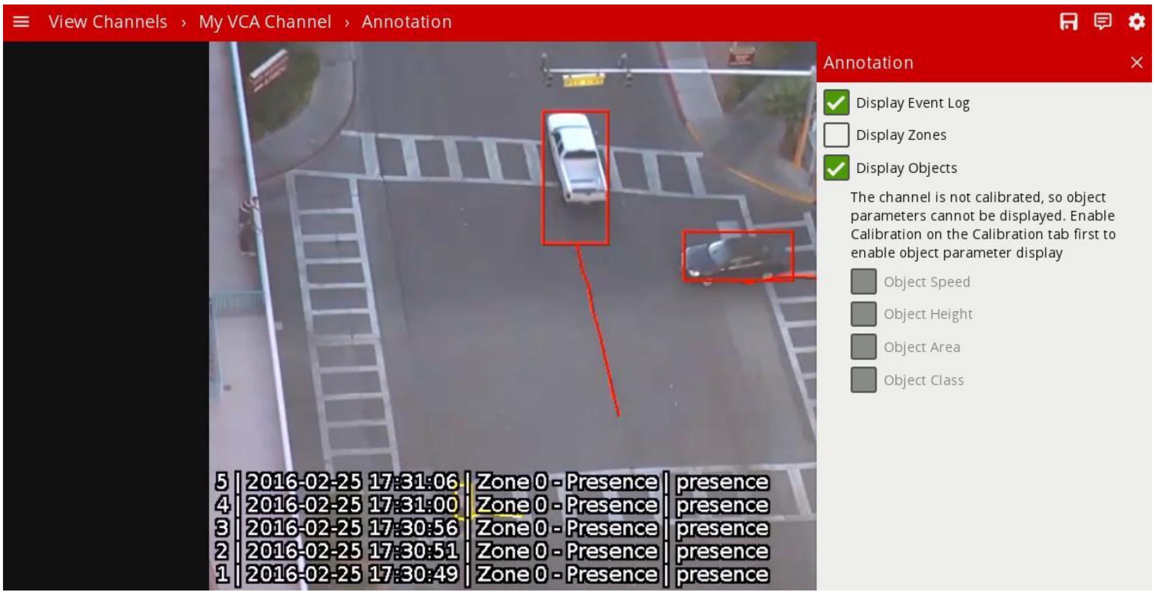
☐ Object Area

☐ Object Class

Note: to display object parameters such as speed, height, area and classifications, the channel must first be calibrated.

16.2 Display Event Log

Check the **Display Event Log** option to show the event log in the lower portion of the image.

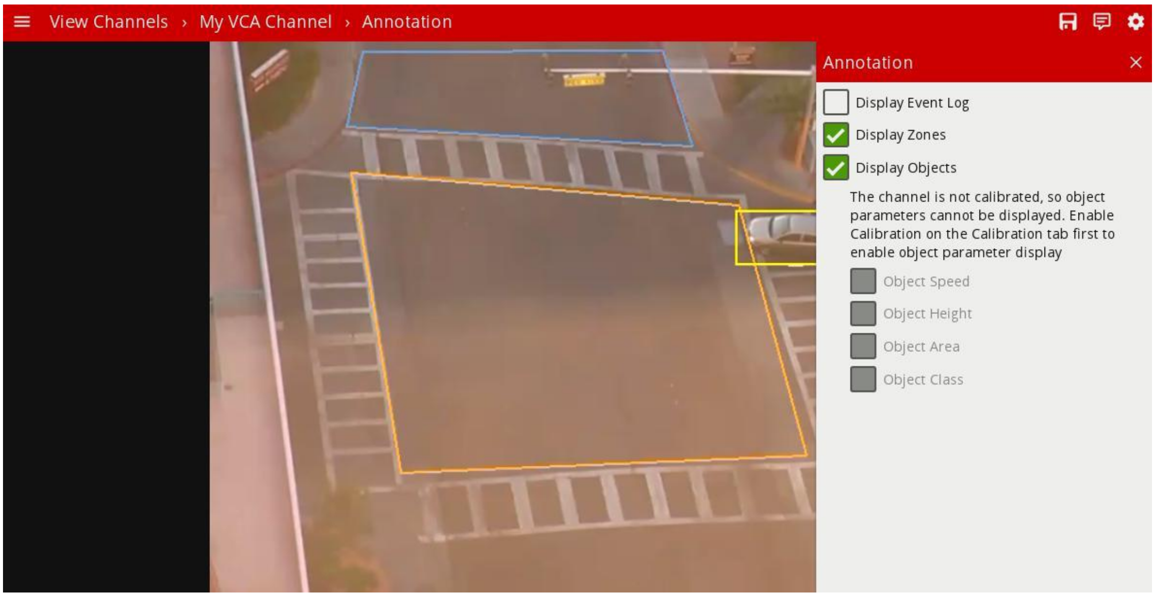


The channel is not calibrated, so object parameters cannot be displayed. Enable Calibration on the Calibration tab first to enable object parameter display

```
5 | 2016-02-25 17:31:06 | Zone 0 - Presence | presence
4 | 2016-02-25 17:31:00 | Zone 0 - Presence | presence
3 | 2016-02-25 17:30:56 | Zone 0 - Presence | presence
2 | 2016-02-25 17:30:51 | Zone 0 - Presence | presence
1 | 2016-02-25 17:30:49 | Zone 0 - Presence | presence
```

16.3 Display Zones

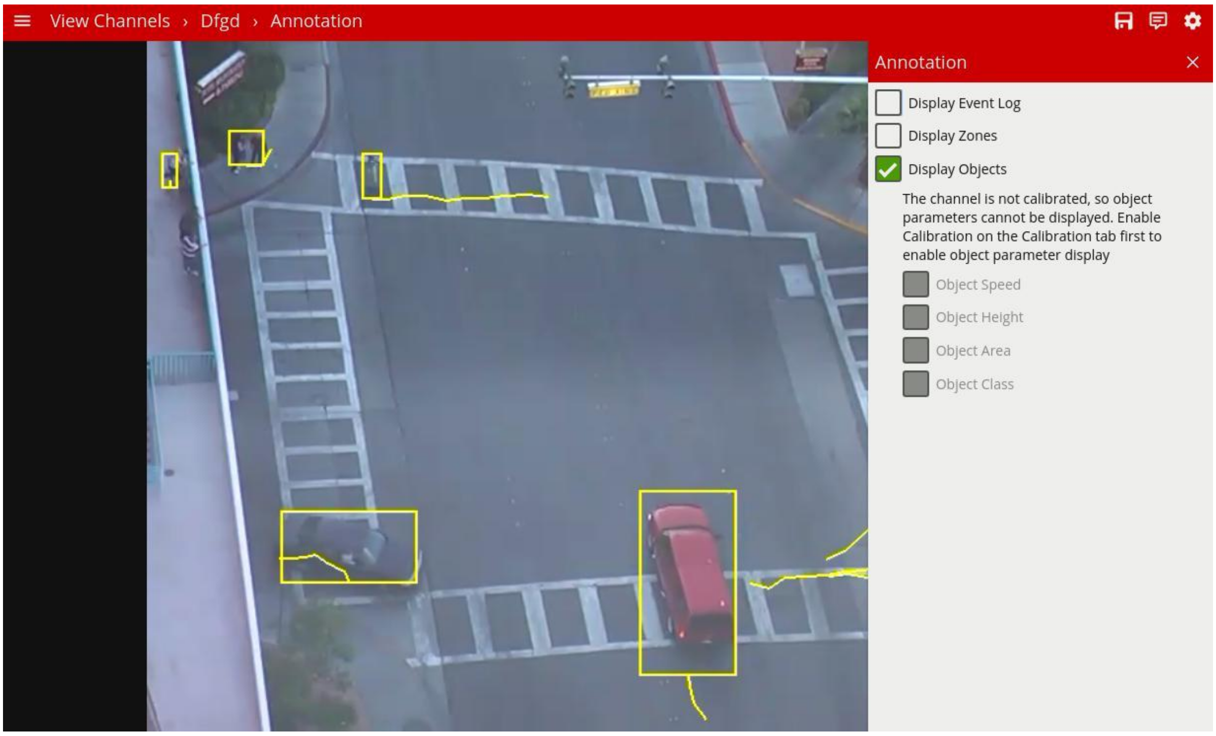
Check the **Display Zones** option to show the outline of any configured zones.



The channel is not calibrated, so object parameters cannot be displayed. Enable Calibration on the Calibration tab first to enable object parameter display

16.4 Display Objects

Check the **Display Objects** option to show the bounding boxes of tracked objects. Objects which are not in an alarmed state are rendered in yellow. Objects rendered in red are in an alarmed state (i.e. they have triggered a rule).



Annotation

□ Display Event Log

□ Display Zones

☑ Display Objects

The channel is not calibrated, so object parameters cannot be displayed. Enable Calibration on the Calibration tab first to enable object parameter display

□ Object Speed

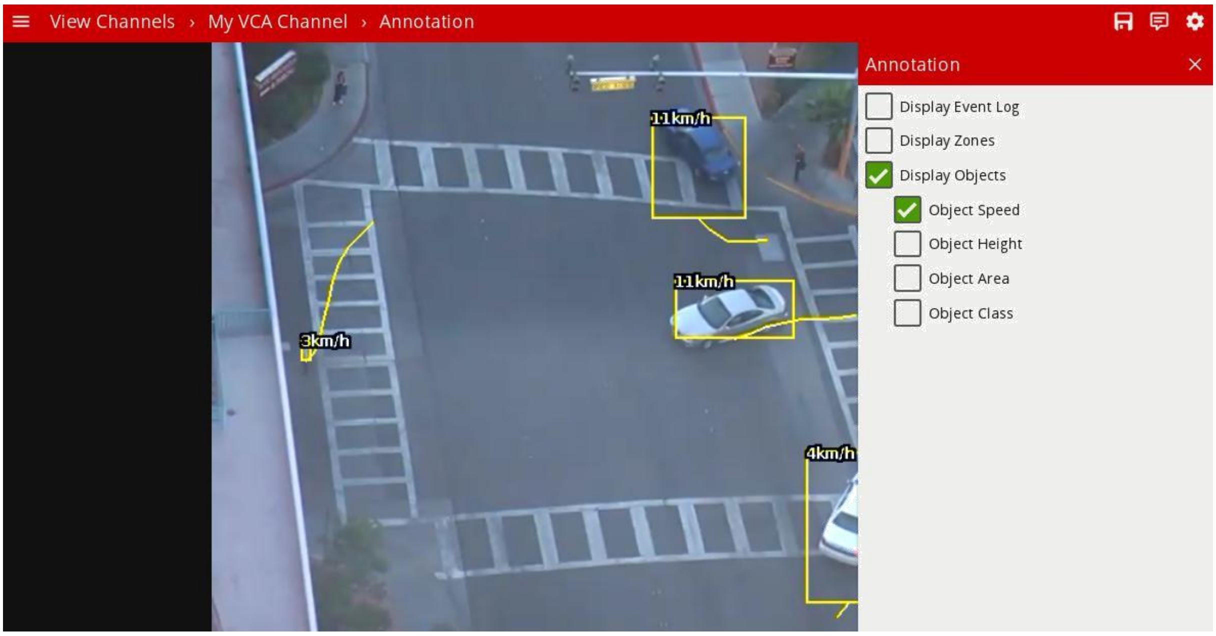
□ Object Height

□ Object Area

□ Object Class

16.4.1 Object Speed

Check the **Object Speed** option to show the object speed.



Annotation

□ Display Event Log

□ Display Zones

☑ Display Objects

☑ Object Speed

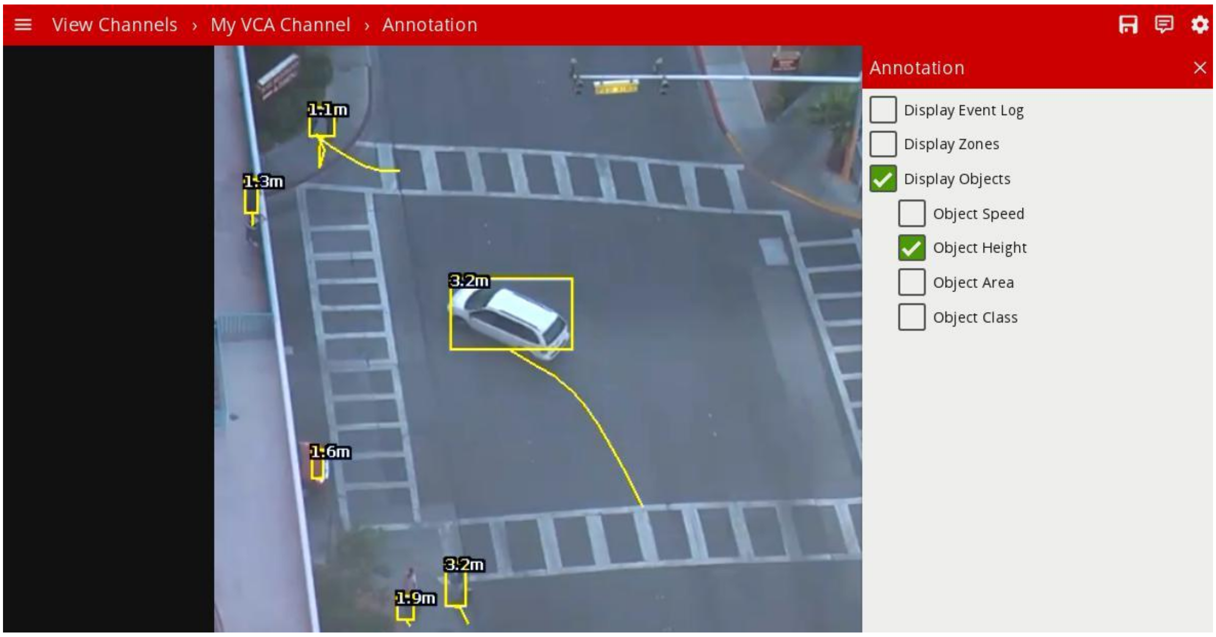
□ Object Height

□ Object Area

□ Object Class

16.4.2 Object Height

Check the **Object Height** option to show the object height.

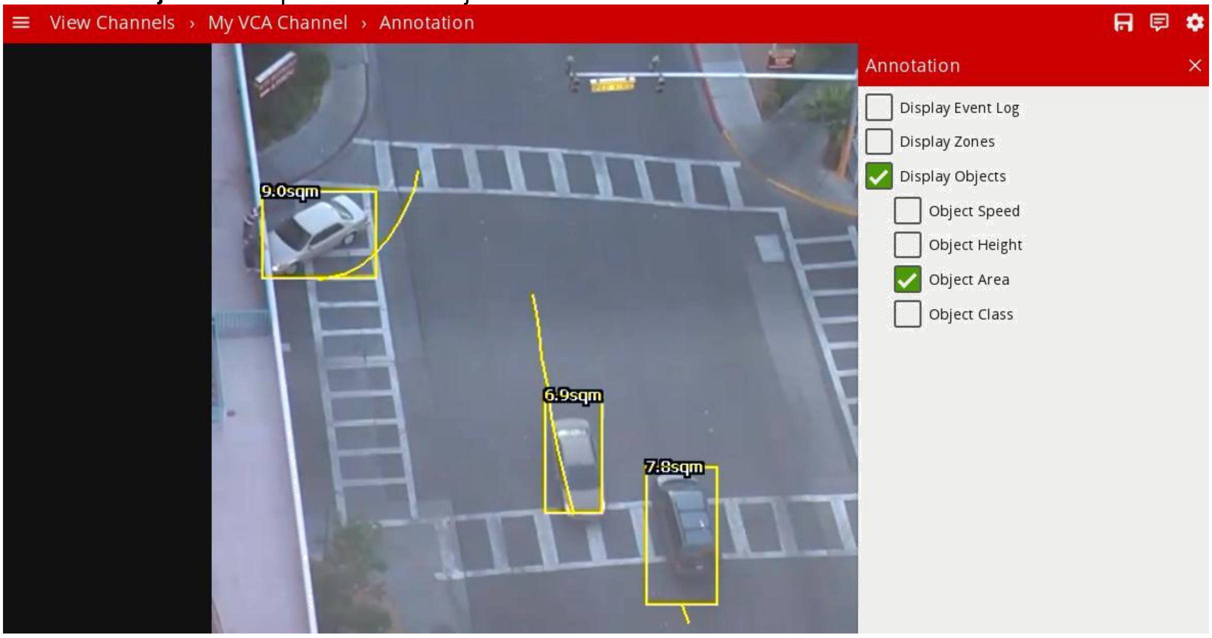


Annotation

- □ Display Event Log
- □ Display Zones
- ☑ Display Objects
  - □ Object Speed
  - ☑ Object Height
  - □ Object Area
  - □ Object Class

16.4.3 Object Area

Check the **Object Area** option to show object area.

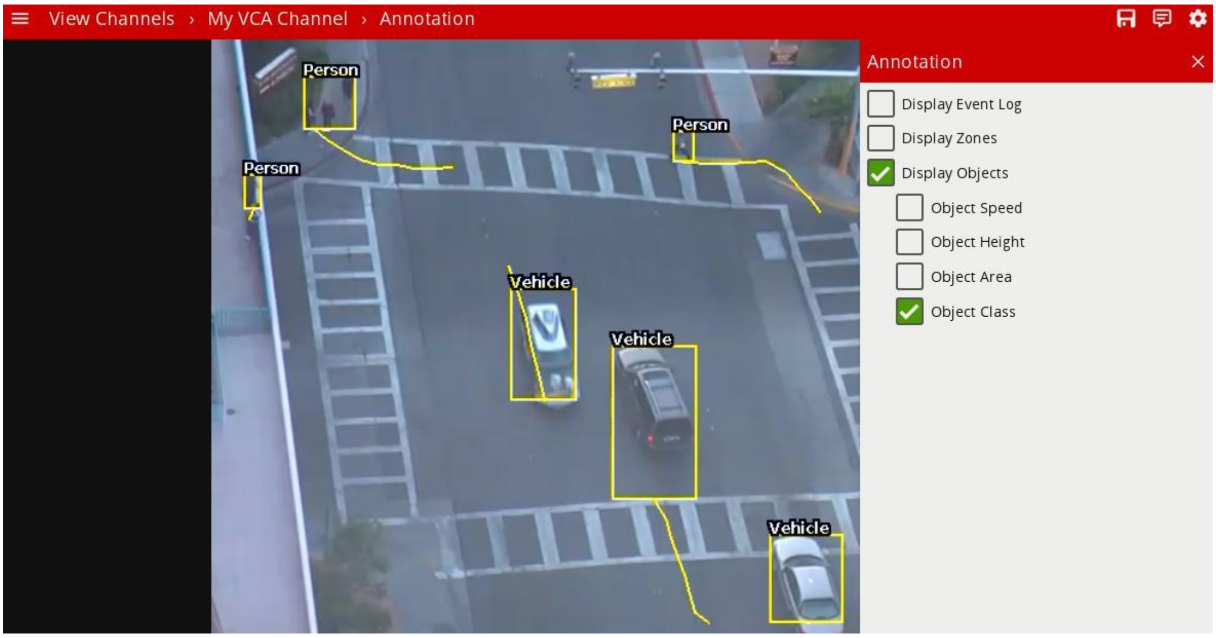


Annotation

- □ Display Event Log
- □ Display Zones
- ☑ Display Objects
  - □ Object Speed
  - □ Object Height
  - ☑ Object Area
  - □ Object Class

16.4.4 Object Classification

Check the **Object Class** to show the object classification.



Annotation

- ☐ Display Event Log
- ☐ Display Zones
- ☑ Display Objects
  - ☐ Object Speed
  - ☐ Object Height
  - ☐ Object Area
  - ☑ Object Class

16.5 Display Line counters

Check the **Display Line Counters** option to display the line counter calibration feedback information.

See the Rules for more information.

16.6 Display Counters

Check the **Display Counters** option to display the counter names and values. See the Counters topic for more information.

16.6.1 System Messages

System messages (e.g. ‘Learning Scene’) are currently always rendered into the video stream.

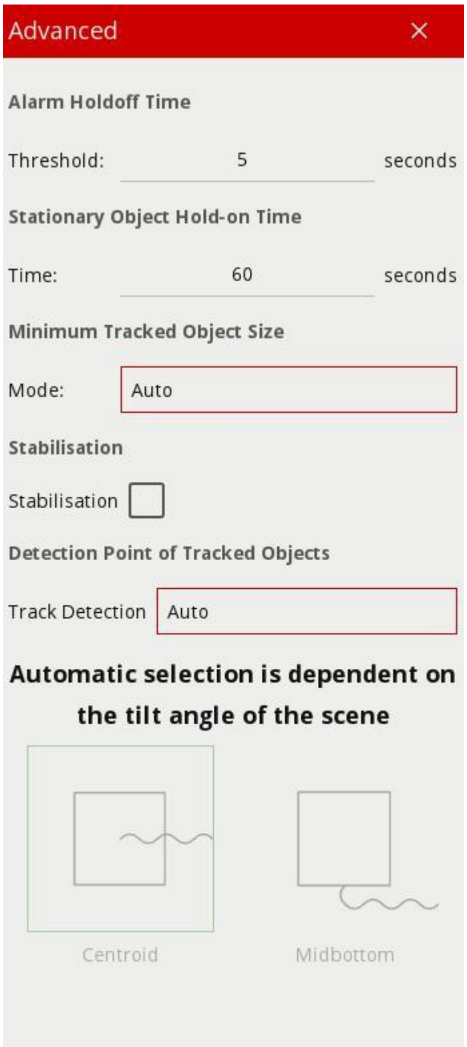
16.7 Next Steps

Learn more about Advanced Settings.

Chapter 17

Advanced Settings

In most installations, the default VCA configuration will suffice. However, in some cases, better performance can be achieved with modified parameters. The Advanced VCA Settings page allows configuration of the advanced VCA parameters.



Advanced ×

Alarm Holdoff Time

Threshold: 5 seconds

Stationary Object Hold-on Time

Time: 60 seconds

Minimum Tracked Object Size

Mode: Auto

Stabilisation

Stabilisation □

Detection Point of Tracked Objects

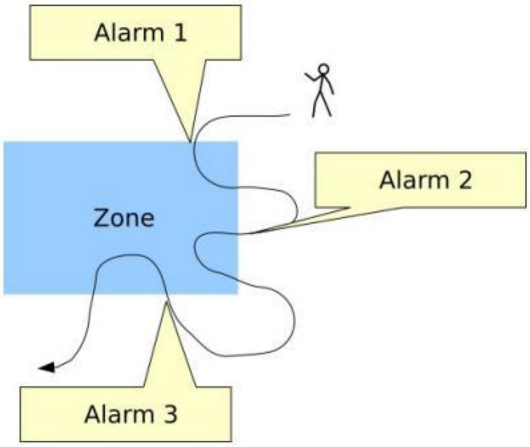
Track Detection Auto

Automatic selection is dependent on the tilt angle of the scene

17.1 Parameters

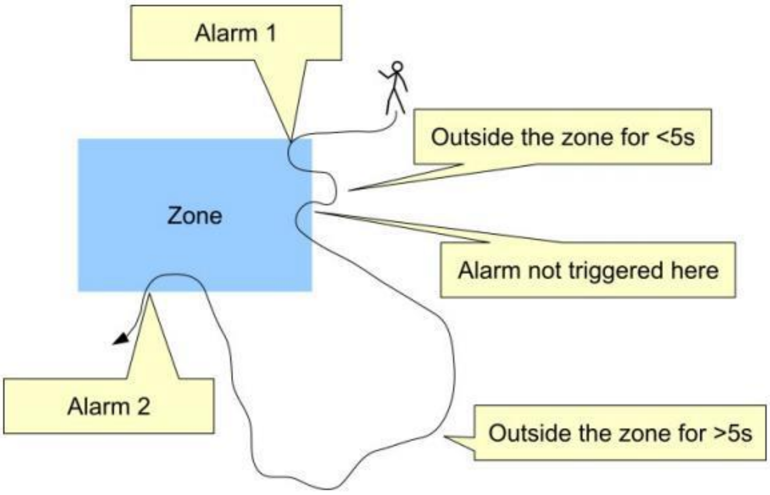
17.1.1 Alarm Holdoff Time

The Alarm Holdoff Time defines the time between the successive re-triggering of an alarm generated by the same object triggering the same rule. To explain this concept, consider the following diagram where no Alarm Holdoff Time is configured:



In this detection scenario, the person enters the zone 3 times. At each point an alarm is raised, resulting in a total of 3 alarms. With the Alarm Holdoff Time configured, it's possible to prevent re-triggering of the same rule for the same object within the configured time period.

Consider the same scenario, but with an Alarm Holdoff Time of 5 seconds configured:



In this case, an alarm is not raised when the person enters the zone for the second time, because the time between the occurrence of the last alarm of the same type for the object is less than the Alarm Holdoff Time. When the person re-enters the zone for a third time, the elapsed time since the previous alarm of the same type for that object is greater than the Alarm Holdoff time and a new alarm is generated. In essence, the Alarm Holdoff Time can be configured to prevent multiple alarms being generated because an object is loitering on the edge of a zone. Without Alarm Holdoff Time configured, this scenario would cause so called "Alarm chatter".

The default setting for Alarm Holdoff Time is 5 seconds

17.1.2 Stationary Object Hold-on Time

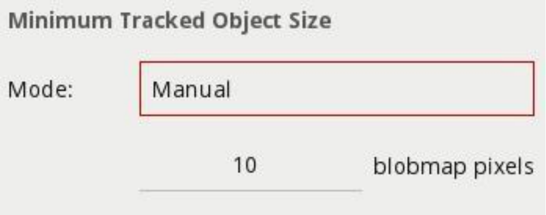
The Stationary Object Hold-on Time defines the amount of time that an object will be tracked by the engine once it becomes stationary. Since objects which become stationary must be "merged" into the scene after some finite time, the tracking engine will forget about objects that have become stationary after the Stationary Object Hold-on Time.

The default setting is 60 seconds.

17.1.3 Minimum Tracked Object Size

The Minimum Tracked Object Size defines the size of the smallest object that will be considered for tracking.

For most applications, the default setting of ‘Auto’ is recommended as this allows the algorithm to automatically select the best value. In some situations, where extra sensitivity is required, the value can be manually specified. While lower values allow the engine to track smaller objects, it may increase the susceptibility to false detections.



Minimum Tracked Object Size

Mode: Manual

10 blobmap pixels

17.1.4 Camera Shake Cancellation

Enabling Camera Shake Cancellation stabilizes the video stream before the analytics process runs. This can be useful where the camera is installed on a pole or unstable platform and subject to sway or shake.

It’s recommended to only enable this option when camera shake is expected in the installation scenario.

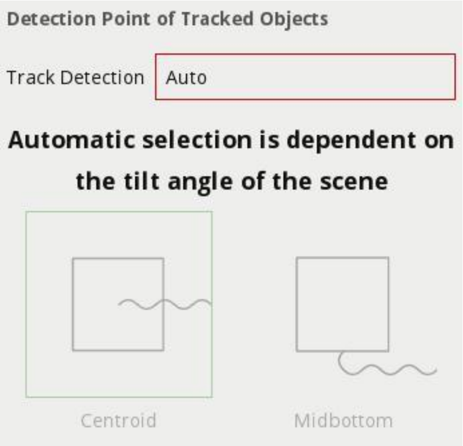
17.1.5 Detection Point of Tracked Objects

For every tracked object, a point is used to determine the object’s position, and evaluate whether it intersects a zone and triggers a rule. This point is called the **detection point**.

There are 3 modes that define the detection point relative to the object:

17.1.5.1 Automatic

In automatic mode, the detection point is automatically set based on how the channel is configured. It selects ‘Centroid’ if the camera is calibrated overhead, or ‘Mid bottom’ if the camera is calibrated side-on or uncalibrated.



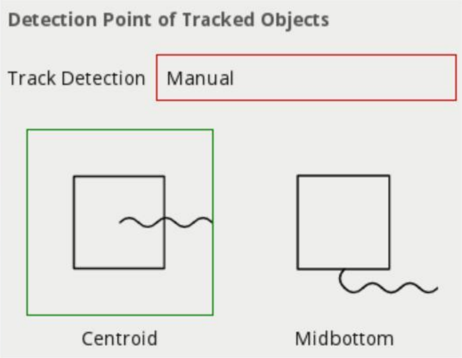
Detection Point of Tracked Objects

Track Detection Auto

Automatic selection is dependent on the tilt angle of the scene

17.1.5.2 Centroid

In this mode, the detection point is forced to be the centroid of the object.



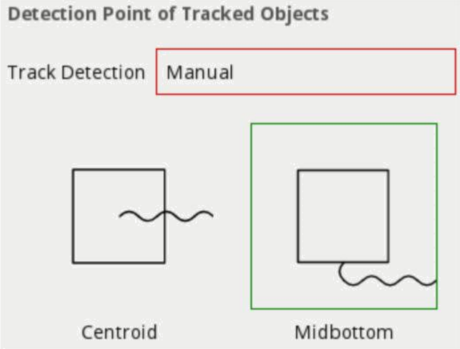
Detection Point of Tracked Objects

Track Detection: Manual

17.1.5.3 Mid bottom

In this mode, the detection point is forced to be the middle of the bottom edge of the tracked object.

Normally this is the ground contact point of the object (where the object intersects the ground plane).



Detection Point of Tracked Objects

Track Detection: Manual

17.2 Next Steps

Learn more about the System Settings.

Chapter 18

System Settings

The system settings page facilitates administration of system level settings such as network configuration, system time and software upgrade.

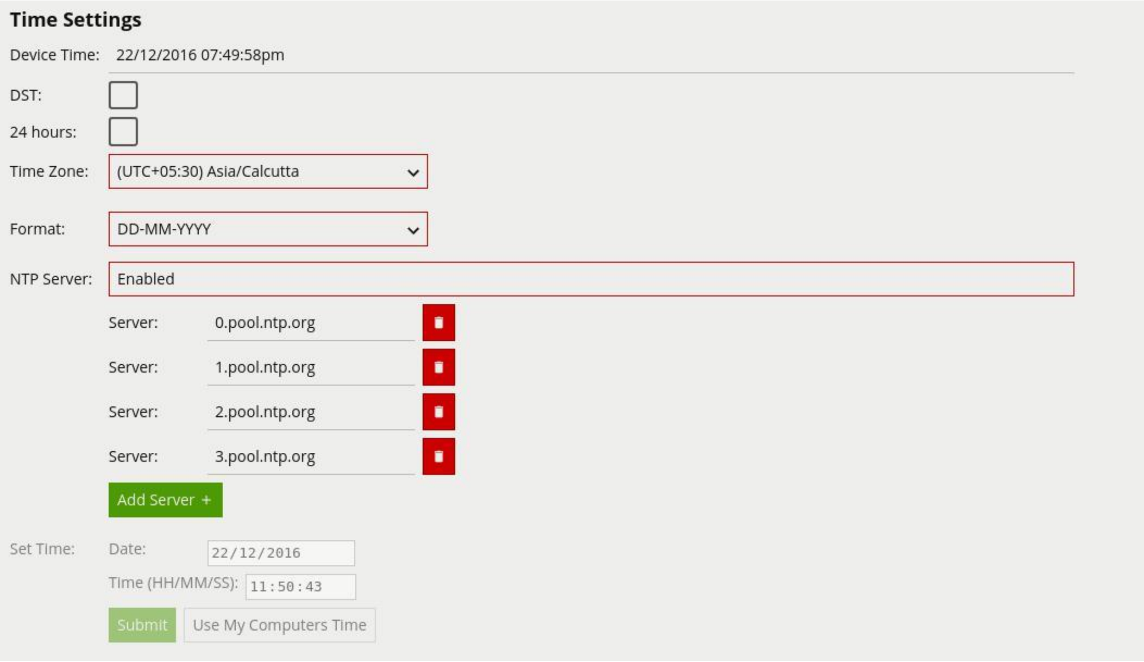
18.1 Network Settings

The network configuration of the device can be changed in the network settings configuration section:

- **Host Name:** Sets the hostname of the device. This is a unique identifier by which the device can be located on the network, and with the discovery tool.
- **DHCP/Manual:** Determines whether an IP address is obtained automatically via DHCP or specified manually. If DHCP is selected but there is no DHCP server on the network the device will revert to the default static IP address 192.168.10.10 with subnet mask 255.255.0.0. For manual configuration, the **subnet mask**, **default gateway** and **DNS server(s)** must also be specified.
- In order to apply the configuration, click the **Save** button. This is different from the rest of the interface which automatically applies changes immediately but is necessary to ensure the IP address is only changed in a single step.
- If the IP address is changed, the interface will redirect to the new IP address if possible. In some cases (e.g. when changing from manual to DHCP) the new IP address may not be known and should be re-entered in the address bar.

18.2 Time Settings

The system time settings of the device can be changed in the time settings configuration section:



Time Settings

Device Time: 22/12/2016 07:49:58pm

DST: □

24 hours: □

Time Zone: (UTC+05:30) Asia/Calcutta

Format: DD-MM-YYYY

NTP Server: Enabled

Server: 0.pool.ntp.org

Server: 1.pool.ntp.org

Server: 2.pool.ntp.org

Server: 3.pool.ntp.org

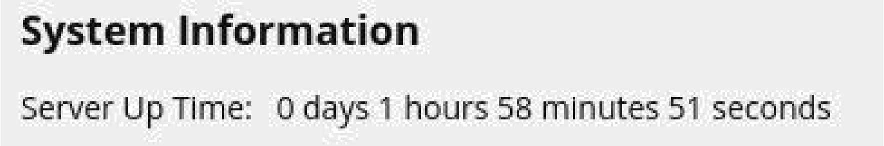
Set Time: Date: 22/12/2016

Time (HH/MM/SS): 11:50:43

- **Device Time:** The current system time according to the device.
- **DST:** Checked if daylight savings is currently in effect for the selected timezone.
- **24 Hours:** Check to enable 24-hour time format. Uncheck to enable 12-hour AM/PM time format.
- **Time Zone:** The timezone configuration of the device. Select to change the current timezone.
- **Format:** The time format to use on the device.
- **NTP Server:** Toggle this option to enable/disable automatic time configuration with Network Time Protocol (NTP). When NTP is enabled, the NTP servers can be specified in the **Server** options below.
- **Set Time:** Manual time configuration (only available when NTP is disabled). Specify the time manually and apply it by clicking the **Submit** button.

18.3 System Information

The system information section shows the device up-time (how long the device has been running without restarting):



System Information

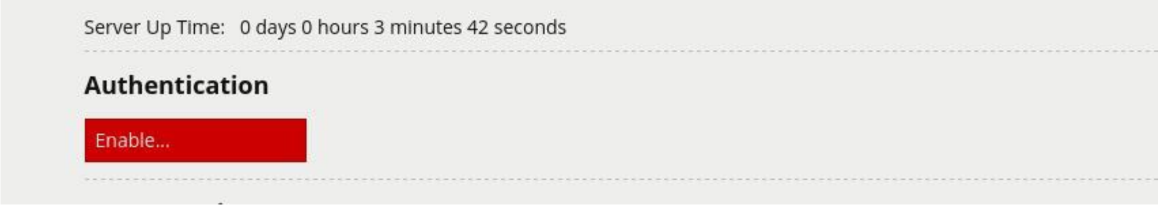
Server Up Time: 0 days 1 hours 58 minutes 51 seconds

18.4 Authentication Settings

The VCA system can be protected against unauthorized access by enabling authentication. By default, authentication is enabled and the default credentials must be entered when accessing the device for the first time. Authentication applies to all functions including the web interface and API, RTSP server and discovery interfaces.

18.4.1 Enabling Authentication

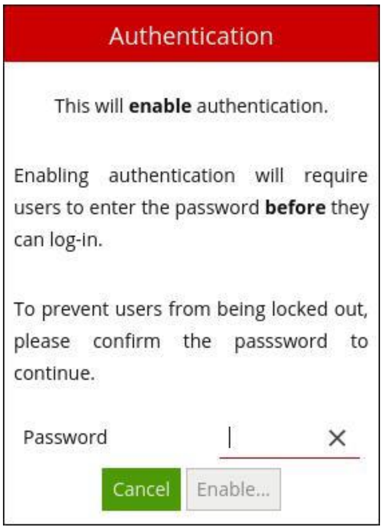
Click the **Enable** button to enable authentication.



Server Up Time: 0 days 0 hours 3 minutes 42 seconds

Authentication

The password must be confirmed before authentication can be enabled in order to prevent the user being locked out of the device.



Authentication

This will **enable** authentication.

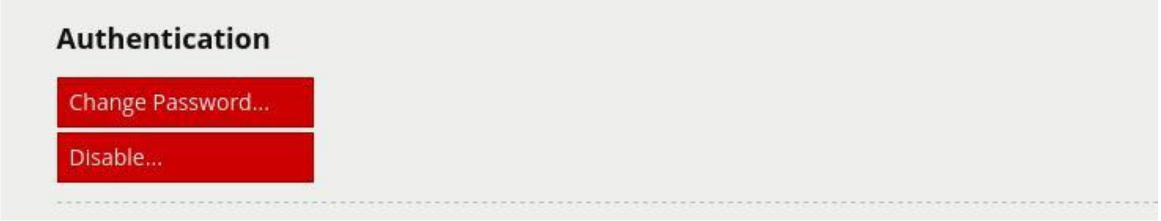
Enabling authentication will require users to enter the password **before** they can log-in.

To prevent users from being locked out, please confirm the passsword to continue.

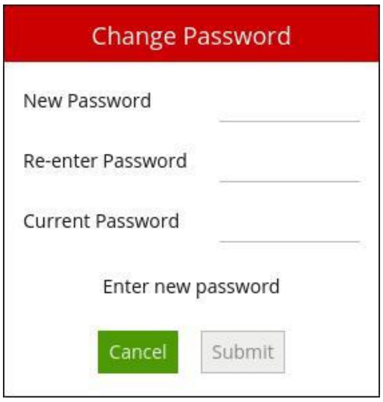
Password

18.4.2 Changing the Password

Click the **Change Password** button to change the password.



Enter the new password, and confirm the current password in order to apply the changes.



Change Password

New Password

Re-enter Password

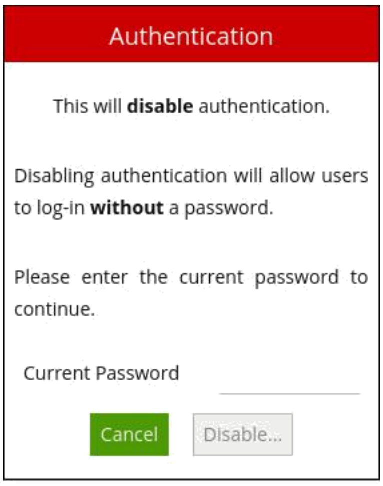
Current Password

Enter new password

WARNING: If the password is forgotten, the device will not be accessible. The only way to recover access to a device without a valid password is to perform a physical reset as described in the Forgotten Password section.

18.4.3 Disabling Authentication

Click the **Disable** button to disable authentication and allow users to access the device without entering a password. The password is required to disable authentication.



Authentication

This will **disable** authentication.

Disabling authentication will allow users to log-in **without** a password.

Please enter the current password to continue.

Current Password

18.4.4 Default Credentials

The default credentials are as follows:

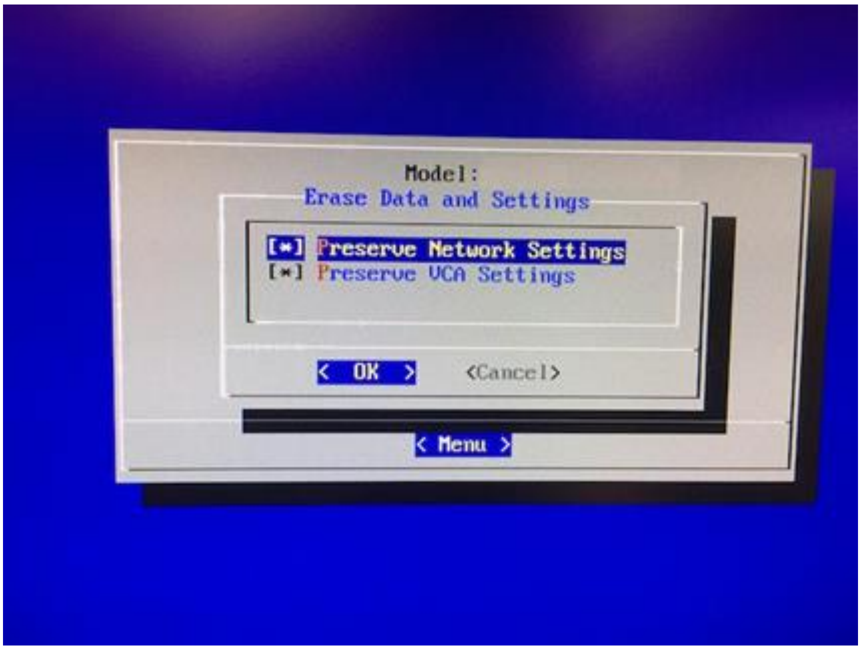
- **Username:** admin
- **Password:** admin

18.4.5 Forgotten Password

If a system becomes inaccessible due to a lost password, the only way to recover access to the device is to perform a hard reset, which will restore the default credentials.

To perform a hard reset:

- Connect a monitor and keyboard to the device to access the kiosk mode.
- Select the **Menu** option, then **Erase Data and Settings**.
- Select **OK** and reboot the device.



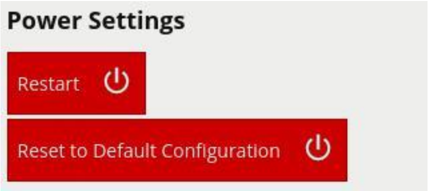
Model:

Erase Data and Settings

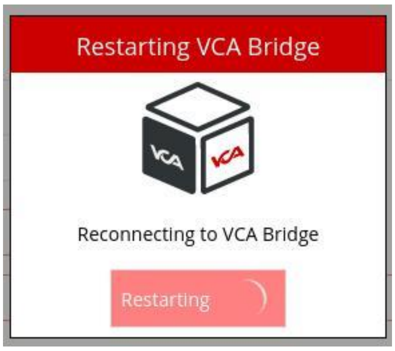
[*] Preserve Network Settings
[*] Preserve VCA Settings

18.5 Power Settings

The power settings section supports device maintenance functions:



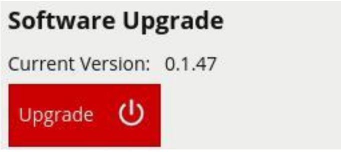
- **Restart:** Restarts the device. The interface will wait for the device to come back on-line and reconnect automatically:


Restarting VCA Bridge

Reconnecting to VCA Bridge

- **Reset to Default Configuration:** Resets the device to its default configuration. Note that network settings and any installed licenses are not affected.

18.6 Software Upgrade



Current Version: 0.1.47

- **Upgrade:** Upgrades the device firmware. Select a VCA package file (. vcapkg) to upload to the device. Following a successful upgrade, the interface will wait for the device to come back on-line and reconnect automatically.

Chapter 19

Template Tokens

VCA can be set up to perform a specific action when an analytic event occurs. Examples include sending an email, TCP or HTTP message to a server.

VCA allows templated messages to be written for email, TCP and HTTP actions which are automatically filled in with the metadata for the event. This allows the details of the event to be specified in the message that the action sends, e.g. the location of the object, type of event, etc.

19.1 Syntax

The templating system uses mustache, which is widely used and well-documented online.

A brief overview of the templating syntax will be provided here.

Templated messages can be written by using tokens in the message body. For example:

Hello {{name}}!

is a template with a name token. When the template is processed, the event metadata is checked to see if it has a name entry. If it does, the {{name}} token is replaced with the name of the event. If it isn't present, the token will be replaced with blank space.

If an event with the name Presence occurs, the processed template will be Hello Presence! but if it doesn't have a name, it will be Hello!

Some tokens may also have sub-properties which can be accessed as follows:

It happened at {{time.start.hours}}!

19.1.1 Conditionals

Tokens can also be evaluated as boolean values, allowing simple conditional statements to be written:

{{#some_property}}Hello, world!{{/some_property}}

In this example, if some_property is present in the event metadata, then "Hello, world!" will appear in the message. Otherwise, nothing will be added to the message.

If some_property is a boolean, then its value will determine whether or not the conditional is entered.

If some_property is an array property, it will only evaluate as true if the array is not empty.

19.1.2 Arrays

Finally, tokens can also be arrays which can be iterated over. For example:

{{#object_array}}

{{name}} is here!

{{/object_array}}

This template will iterate through each item in object_array and print its name, if it has a name property. For example, the array [{"name": "Bob"}, {"name": "Alice"}, {"name": "Charlie"}] will result in the following output:

Bob is here!

Alice is here!

Charlie is here!

19.2 List of tokens

Lower case names represent tokens that can be used with the {{token}} syntax. Upper case names represent boolean or array properties that should be used with the {{#token}}...{{/token}} syntax.

19.2.1 {{name}}

The name of the event

19.2.2 {{id}}

The unique id of the event

19.2.3 {{type}}

The type of the event. This is usually the type of rule that triggered the event

19.2.4 {{is.type.*name*}}

This is a Boolean property that allows conditionals to be performed on the given type *name*.

For example, to print something only for events of type “presence”:

{{#is.type.presence}}My text{{/is.type.presence}}

19.2.5 {{time.start}}

The start time of the event. It has the following sub properties:

- time.start.iso8601
- time.start.year
- time.start.month
- time.start.day
- time.start.hours
- time.start.minutes

- time.start.seconds
- time.start.milliseconds
- time.start.microseconds
- time.start.nanoseconds
- time.start.epoch
- time.start.offset.sign
- time.start.offset.hours
- time.start.offset.minutes

The iso8601 property is a date string in the ISO 8601 format.

The offset property is the timezone offset.

19.2.6 {{time.end}}

The end time of the event. Same properties as time.start

19.2.7 {{host}}

The hostname of the device that generated the event

19.2.8 {{channel}}

The id of the channel that the event occurred on

19.2.9 {{#Zone}}

An array of the zones associated with the event.

Sub-properties:

- id: The id of the zone
- name: The name of the zone
- channel_id: The id of the channel the zone is attached to
- colour: The RGBA colour of the zone
- detection: 0 if the zone is non-detection zone, 1 otherwise
- type: 0 for a closed polygon, 1 for a line
- outline: The outline of the object (see the outline token for more details)

Example:

{{#Zone}}

id: {{id}}

name: {{name}}

channel:{{channel_id}}

colour: ({{colour.r}}, {{colour.g}}, {{colour.b}}, {{colour.a}}) {{/Zone}}

19.2.10 {{#Rule}}

An array of the rules associated with the event.

Sub-properties:

- id: The id of the rule that triggered the event
- name: The name of the rule that triggered the event
- type: The type of the rule that triggered the event

Example:

{{#Rule}}

id: {{id}}

name: {{name}}

type:{{type}}

{{/Rule}}

19.2.11 {{#Object}}

An array of the objects that triggered the event.

Sub-properties:

- id: The id of the object
- outline: The outline of the object (see the outline token for more details)

Example:

{{#Object}}

id: {{id}}

Top left corner: ({{outline.rect.top_left.x}}, {{outline.rect.top_left.y}}) {{/Object}}

19.2.12 {{outline}}

The bounding box outline of an object or zone

Sub-properties:

- outline.rect.top_left.x: x-coordinate of the top left corner
- outline.rect.top_left.y: y-coordinate of the top left corner
- outline.rect.bottom_right.x: x-coordinate of the bottom right corner

- outline.rect.bottom_right.y: y-coordinate of the bottom right corner

19.2.13 {{#LineCounter}}

An array of line counter counts.

Sub-properties:

- rule_id: The id of the line counter rule
- width: The calibration width of the line counter
- position: The position at which the object crossed the line
- count: The number of objects that crossed the line
- direction: The direction in which the object(s) crossed the line. 0 for A, 1 for B

Example:

{{#LineCounter}}

rule_id: {{rule_id}}

calibration width: {{width}}

position: {{position}}

count: {{count}}

direction: {{direction}}

{{/LineCounter}}

19.2.14 {{#Counter}}

An array of counter counts.

Sub-properties:

- id: The id of the counter
- name: The name of the counter
- count: The number of counts

Example:

{{#Counter}}

id: {{id}}

name: {{name}}

count: {{count}}

{{/Counter}}

19.2.15 {{#Tampered}}

A boolean that is true if a camera tamper has been detected

Example:
{{#Tampered}}The camera has been tampered with!{{/Tampered}}

19.2.16 {{#Area}}

The estimated area of the object. This token is a property of the object token. It is only produced if calibration is enabled.

Sub-properties:

- value: The estimated area of the object

Example:

{{#Object}}{{#Area}}{{value}}{{/Area}}{{/Object}}

19.2.17 {{#Height}}

The estimated height of the object. This token is a property of the object token. It is only produced if calibration is enabled.

Sub-properties:

- value: The estimated area of the object

Example:

{{#Object}}{{#Height}}{{value}}{{/Height}}{{/Object}}

19.2.18 {{#GroundPoint}}

The estimated position of the object. This token is a property of the object token. It is only produced if calibration is enabled.

Sub-properties:

- value.x: The estimated normalised x-axis position of the object
- value.y: The estimated normalised y-axis position of the object

Example:

{{#Object}}{{#GroundPoint}}Position: ({{value.x}}, {{value.y}}){{/GroundPoint}}{{/Obj

19.2.19 {{#Speed}}

The estimated speed of the object. This token is a property of the object token. It is only produced if calibration is enabled.

Sub-properties:

- value: The estimated speed of the object Example:

{{#Object}}{{#Speed}}{{value}}{{/Speed}}{{/Object}}

19.2.20 {{#Classification}}

The classification of the object. This token is a property of the object token. It is only produced if calibration is enabled.

Sub-properties:

- value: The classification of the object

Example:

{{#Object}}{{#Classification}}{{value}}{{/Classification}}{{/Object}}

19.3 Examples

The following is an example of a template using most of the available tokens:

Event #{{id}}: {{name}}

Event type: {{type}}

Start time (ISO 8601 format): {{time.start.iso8601}}

End time:

day: {{time.end.day}}

time: {{time.end.hour}}:{{time.end.minutes}}:{{time.end.seconds}}.{{time.end.microsec

Device: {{host}}

Channel: {{channel}}

{{#is.type.presence}}

{{#Object}}

Object ID: {{id}}

{{#Classification}}Object Classification: {{value}}{{/Classification}}

{{#Height}}Object Height: {{value}}m{{/Height}}

Object bounding box: [

({{outline.rect.top_left.x}}, {{outline.rect.top_left.y}}), ({{outline.rect.bottom_right.x}}, {{outline.rect.top_left.y}}), ({{outline.rect.bottom_right.x}}, {{outline.rect.bottom_right.y}}), ({{outline.rect.top_left.x}}, {{outline.rect.bottom_right.y}})

]

{{/Object}}

{{/is.type.presence}}

{{#Counter}}

Counter triggered.

id: {{id}}

name: {{name}}

count: {{count}}

{{/Counter}}
{{#LineCounter}}

rule_id: {{rule_id}}

calibration width: {{width}}

position: {{position}}

count: {{count}}

direction: {{direction}}

{{/LineCounter}}

In this example, the object information is only printed for events of type “presence”.

This template might result in the following message:

Event #350: My Bad Event

Event type: presence

Start time (ISO 8601 format): 2017-04-21T10:09:42+00:00

End time:

day: 21

time: 10:09:42.123456

Device: mysecretdevice

Channel: 0

Object ID: 1

Object Classification: Person

Object Height: 1.8m

```
Object bounding box: [
   (16000, 30000),
   (32000, 30000),
   (32000, 0),
   (16000, 0)
]
Counter triggered.
id: 10
name: My Counter
count: 1
rule_id: 350
calibration width: 1
position: 1
count: 1
direction: 0
```

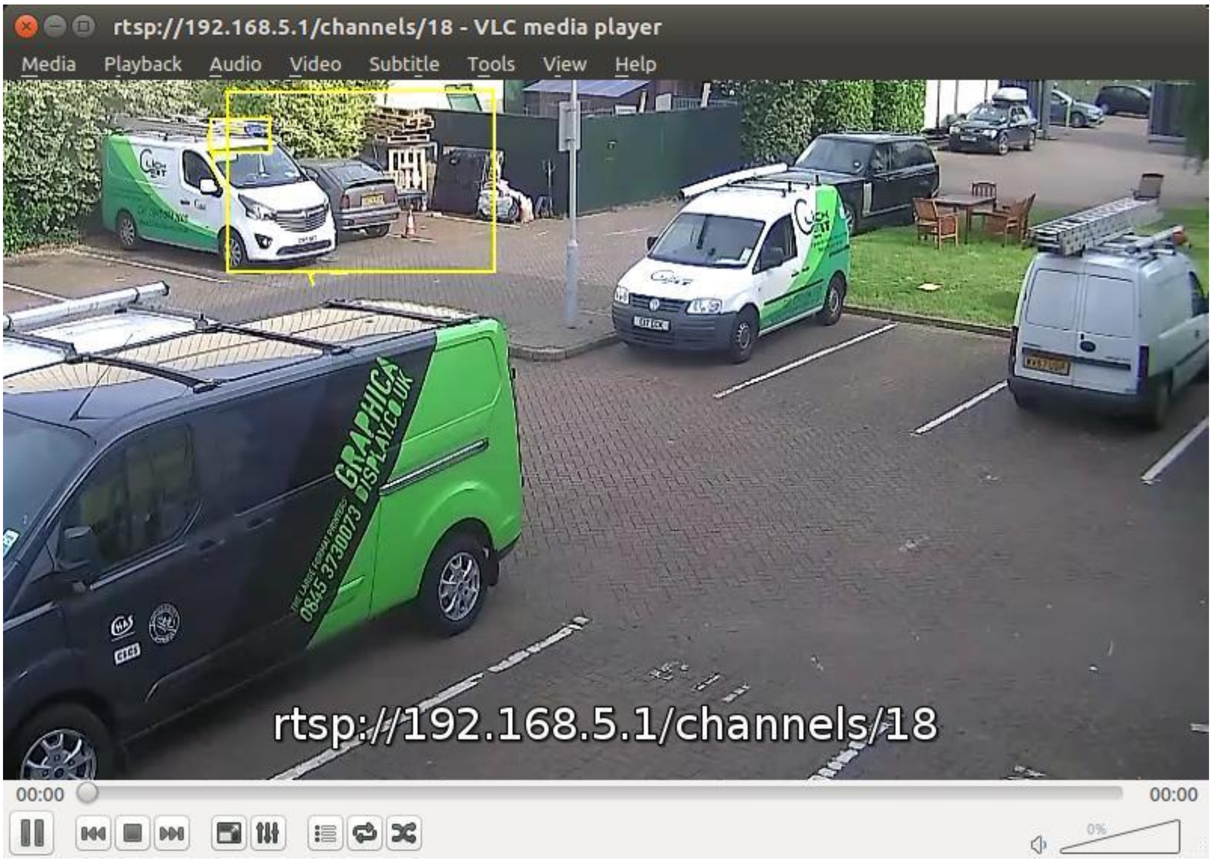
Chapter 20

RTSP Server

VCA devices support an RTSP server that streams annotated video in RTSP format.

The RTSP URL for channels on a VCA device is as follows:

rtsp://\<device ip\>:554/channels/\<channel id\>


rtsp://192.168.5.1/channels/18 - VLC media player
Media
Playback
Audio
Video
Subtitle
Tools
View
Help
rtsp://192.168.5.1/channels/18
00:00
00:00
0%

Chapter 21

SureView Immix

VCA supports the notification of events with annotated snapshots and streaming of real-time annotated video to SureView Immix.

21.1 Prerequisites

The following ports need to be accessible on the VCA device from the Immix server:

- 80: TCP web requests
- 554: TCP/UDP annotated RTSP video stream

21.2 Limitations

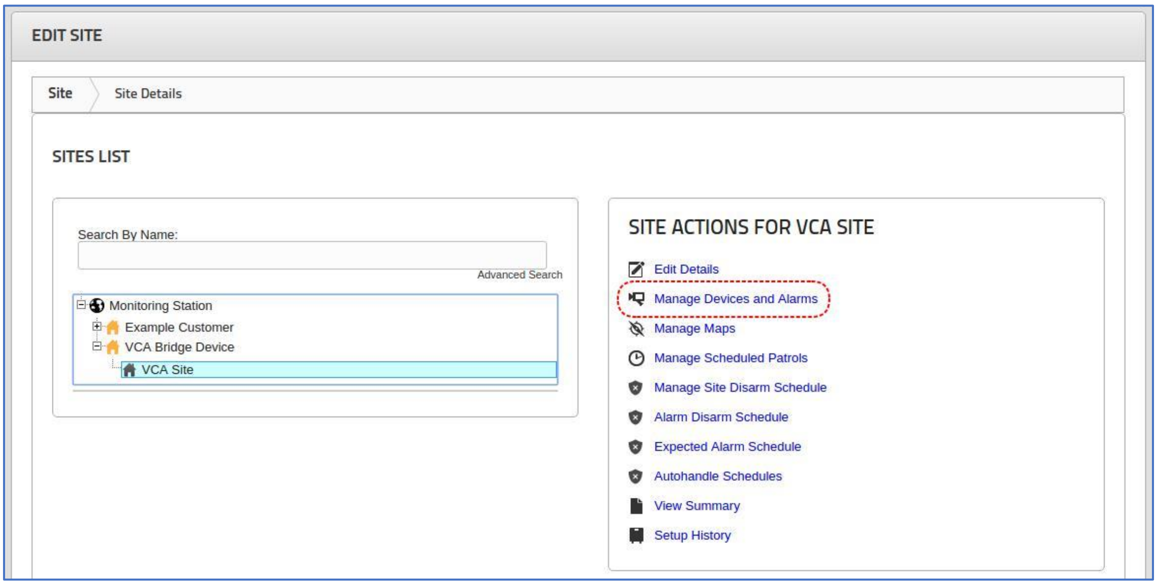
- Only one camera is supported per VCA device. This means that a device has to be configured in Immix for each channel on a VCA device. E.g. if a VCA device has 8 channels, the Immix configuration must consist of 8 devices with one channel each.

21.3 Immix Configuration

21.3.1 Add VCA Device

The first step is to add the VCA device.

In the Immix site configuration tab, click **Manage Devices and Alarms**, then **Add Device**:



EDIT SITE

Site › Site Details

SITES LIST

Search By Name:

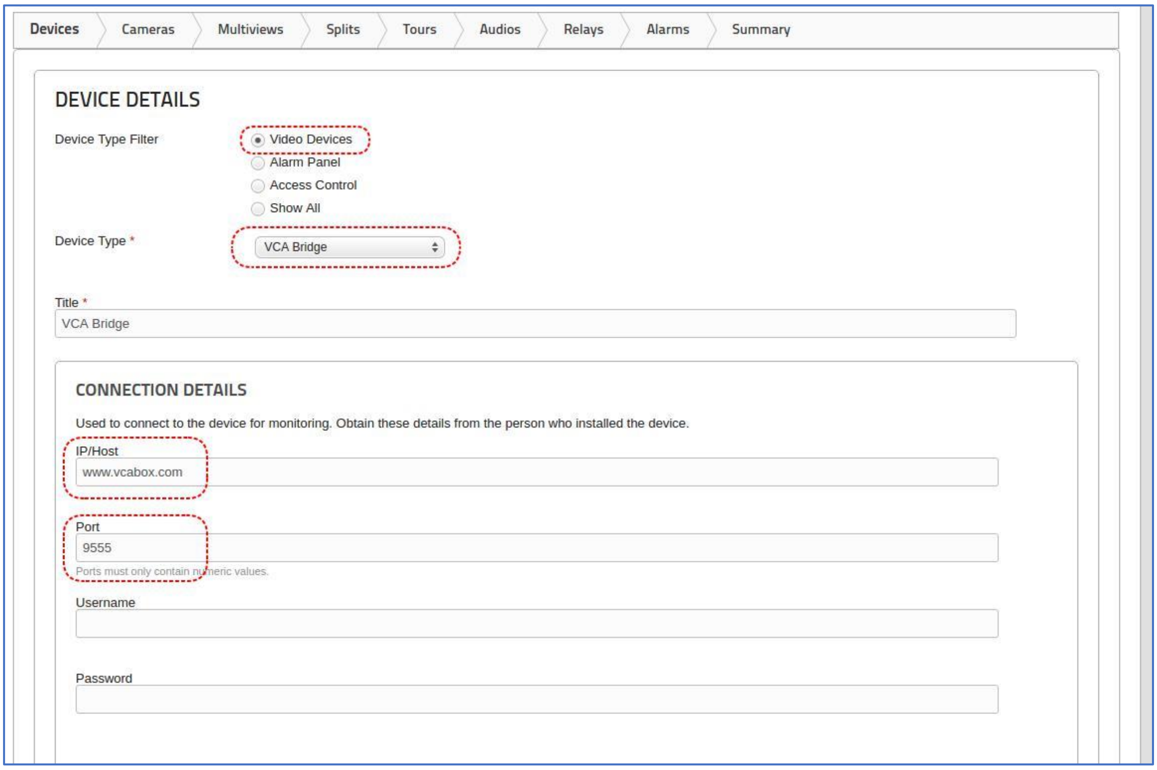
Advanced Search

- Monitoring Station
  - Example Customer
  - VCA Bridge Device
    - VCA Site

SITE ACTIONS FOR VCA SITE

- Edit Details
- Manage Devices and Alarms
- Manage Maps
- Manage Scheduled Patrols
- Manage Site Disarm Schedule
- Alarm Disarm Schedule
- Expected Alarm Schedule
- Autohandle Schedules
- View Summary
- Setup History

On the Add Device page, set the following options:



Devices › Cameras › Multiviews › Splits › Tours › Audios › Relays › Alarms › Summary

DEVICE DETAILS

Device Type Filter: ● Video Devices ○ Alarm Panel ○ Access Control ○ Show All

Device Type *: VCA Bridge

Title *: VCA Bridge

CONNECTION DETAILS

Used to connect to the device for monitoring. Obtain these details from the person who installed the device.

IP/Host: www.vcabox.com

Port: 9555

Ports must only contain numeric values.

Username:

Password:

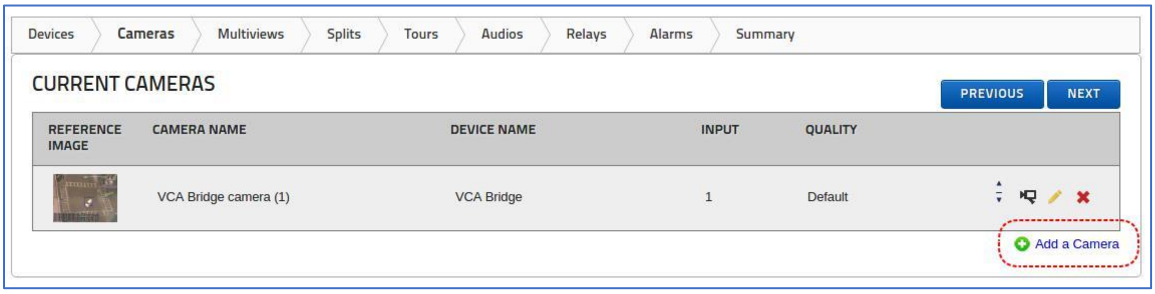
- **Device Type Filter:** Select **Video Devices**
- **Device Type:** Select **VCA Bridge**
- **Title:** Give the device a suitable name
- **IP/Host:** Enter the IP address or hostname of the VCA device
- **Port:** Enter the RTSP port of the VCA device. In this case the device is behind a firewall and port 9555 on www.vcabox.com is forwarded to the standard RTSP port (554) on the VCA device. The RTSP server on the VCA device runs on the standard RTSP port (554).

21.3.2 Add Camera

Once the device has been added, channels from the VCA device can be added.

Note: Immix currently supports only one VCA channel per device. To support more channels, simply add more devices.

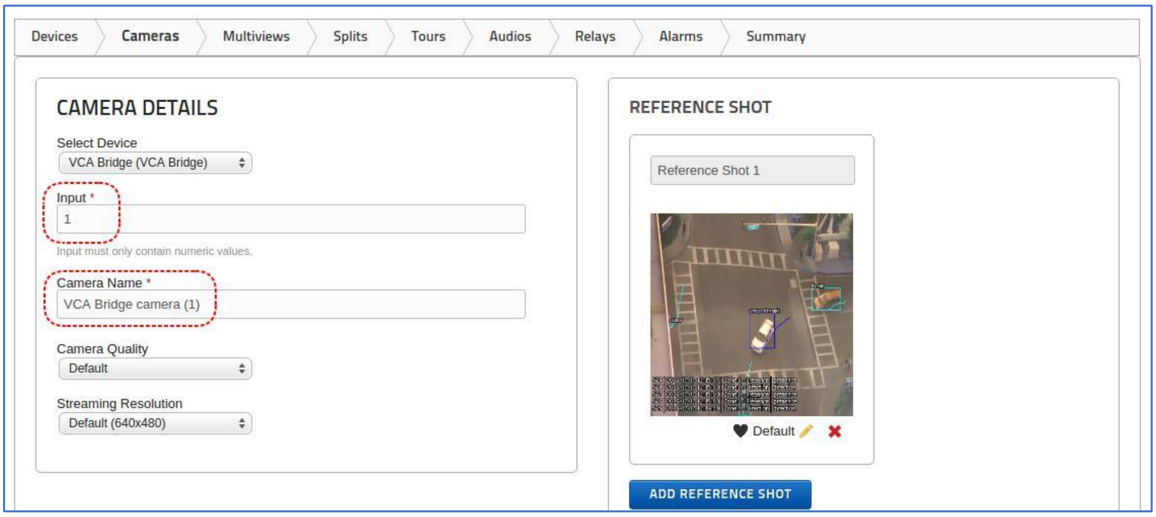
Click the **Cameras** tab and **Add a Camera** to add a new channel:



CURRENT CAMERAS

REFERENCE IMAGE	CAMERA NAME	DEVICE NAME	INPUT	QUALITY
	VCA Bridge camera (1)	VCA Bridge	1	Default

On the **Camera Details** page set the following options:



CAMERA DETAILS

Select Device: VCA Bridge (VCA Bridge)

Input *: 1

Input must only contain numeric values.

Camera Name *: VCA Bridge camera (1)

Camera Quality: Default

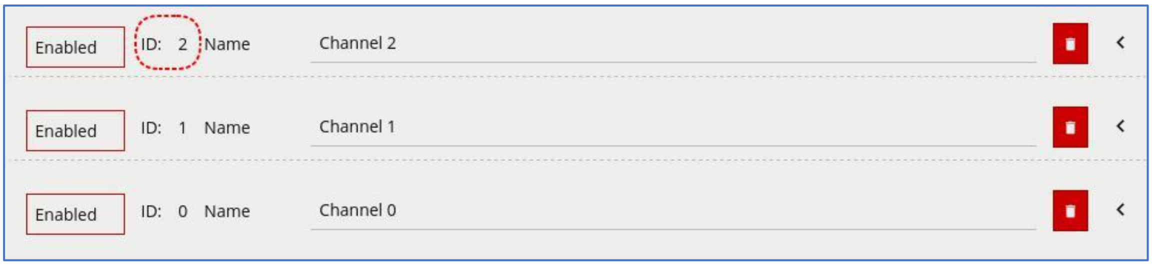
Streaming Resolution: Default (640x480)

- **Input:** Enter the VCA channel Id + 1 (see below for more details)
- **Camera Name:** Enter a suitable name for the channel
- Leave the other settings with default values

21.3.3 Setting the Input in Immix

In order to set the Input value correctly in Immix, the following steps should be followed:

- Find the channel Id in VCA. The channel Id is displayed on the Edit Channels page:



Enabled ID: 2 Name Channel 2

Enabled ID: 1 Name Channel 1

Enabled ID: 0 Name Channel 0

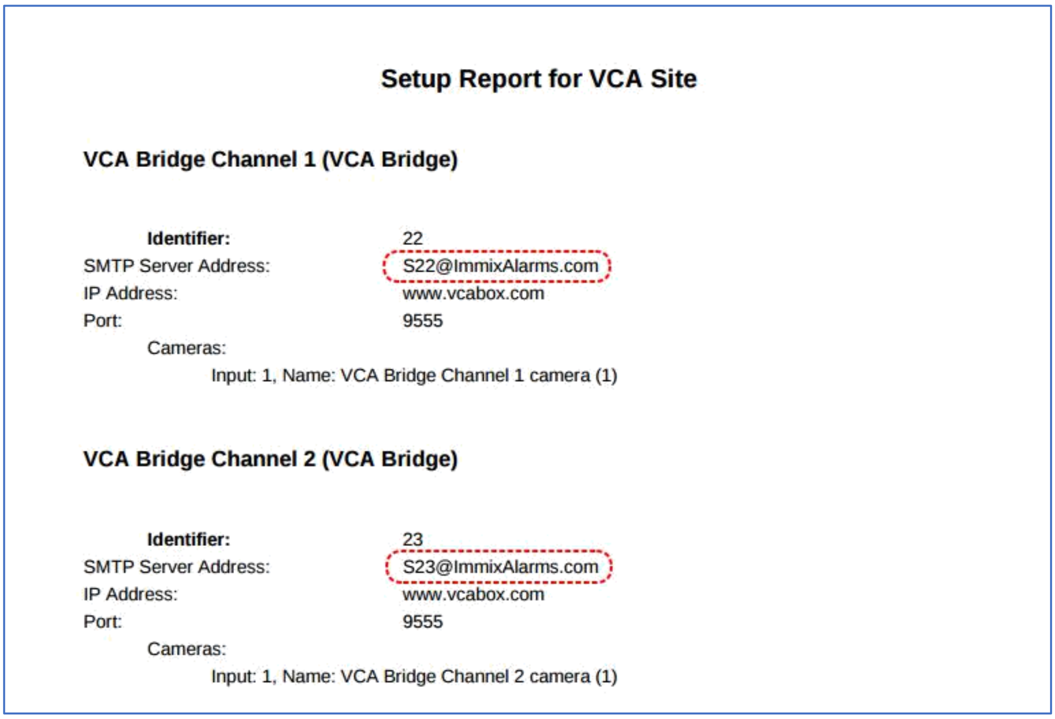
- Set the value of the **Input** field in Immix to the channel Id in VCA + 1, i.e. as illustrated in the table below:

Channel Id in VCA	Input in Immix
0	1
1	2
2	3
5	6
100	101

The reason that the Immix Input is 1 higher than the VCA channel Id is that Immix uses 1-based inputs but VCA uses 0-based channel Ids.

21.3.4 Retrieve a Summary

Generating a summary provides a single document with all of the details necessary to configure the VCA device. Click the **Summary** tab and a PDF report is created:



Setup Report for VCA Site

VCA Bridge Channel 1 (VCA Bridge)

Identifier:	22
SMTP Server Address:	S22@ImmixAlarms.com
IP Address:	www.vcabox.com
Port:	9555
Cameras:	

Input: 1, Name: VCA Bridge Channel 1 camera (1)

VCA Bridge Channel 2 (VCA Bridge)

Identifier:	23
SMTP Server Address:	S23@ImmixAlarms.com
IP Address:	www.vcabox.com
Port:	9555
Cameras:	

Input: 1, Name: VCA Bridge Channel 2 camera (1)

Make a note of the email addresses highlighted in red. These email addresses need to be entered in the VCA device configuration (see next section).

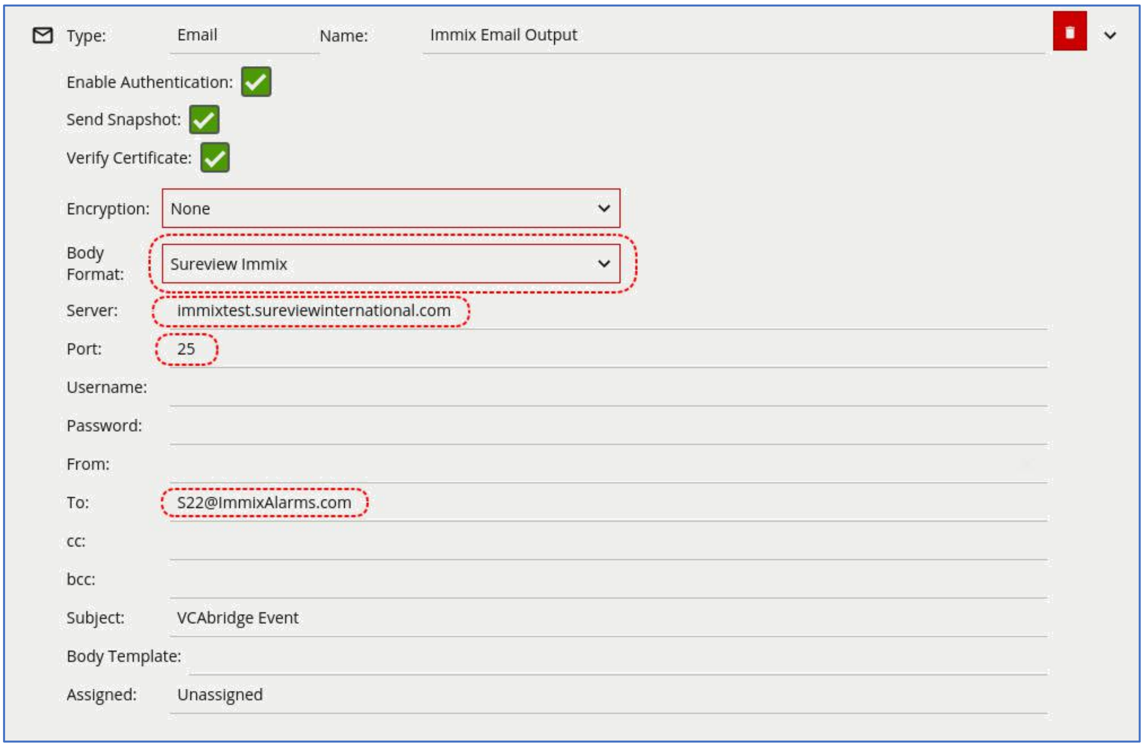
21.4 VCA Device Configuration

Once a device and camera are configured in Immix, the email addresses generated as part of the summary need to be added to the VCA channel configuration.

The VCA device notifies Immix of events via email, so each channel configured for Immix needs to have an email output element configured. For more details on how to configure Inputs and Outputs or Channels see the corresponding topics.

21.4.1 Add an Email Output Element

On the channel configured for Immix, add an email output element with the following configuration:



Type: Email
Name: Immix Email Output
Enable Authentication: ✓
Send Snapshot: ✓
Verify Certificate: ✓
Encryption: None
Body Format: Sureview Immix
Server: immixtest.sureviewinternational.com
Port: 25
Username:
Password:
From:
To: S22@ImmixAlarms.com
cc:
bcc:
Subject: VCAbridge Event
Body Template:
Assigned: Unassigned

- **Body Format:** Set to SureView Immix
- **Server:** Enter the IP address or hostname of the Immix server
- **Port:** Enter the port of the Immix server (Default 25)
- **To:** Enter the email address generated in the Immix summary report. Here S22@ImmixAlarms.com corresponds to Immix Input 1 (which is VCA channel Id 0).

21.4.2 Add the Email Output to the Channel

Once the email output has been configured, simply add it to the right channel. Remember that there is a difference of the Immix inputs with respect to VCA channel Ids (they are 1 higher). Hence, for this example:

- S22@ImmixAlarms.com corresponds to Immix Input 1

- Immix input Ids are 1 higher than VCA channel Ids, so input id 1 in Immix is channel 0 in VCA
- Therefore, the email output element should be assigned to channel 0

21.4.3 Event Type Mappings

The event types reported in the VCA interface are slightly different to the event types reported in the Immix client. The events are mapped as follows:

Event in VCA	Event in Immix
Presence	Object Detected
Enter	Object Entered
Exit	Object Exited
Appear	Object Appeared
Disappear	Object Disappeared
Stopped	Object Stopped
Dwell	Object Dwell
Direction	Object Direction
Speed	Object Speed
Tailgating	Tailgating
Tamper	Tamper Alarm

Chapter 22

Milestone Xprotect

VCA is integrated against the range of Milestone XProtect video management systems. This topic describes how to configure VCA and Milestone XProtect to retrieve video from XProtect and display events with annotation within the XProtect Smart Client.

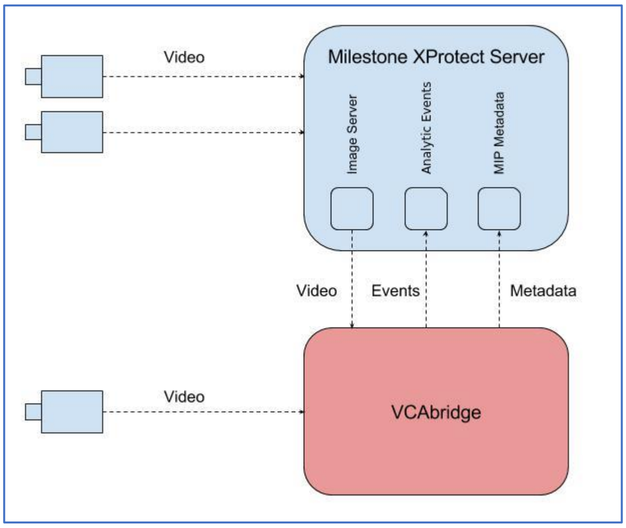
22.1 Prerequisites

- A VCA device such as VCA bridge or VCA core
- Milestone XProtect Corporate, Enterprise, Professional or Expert

22.2 Supported Features and Versions

Milestone Compatibility	Expert	Professional	Enterprise	Corporate
Analyze XProtect video sources	*	*	*	*
View analytics events	*	*	*	*
Basic authentication		*	*	
Windows authentication	*	*	*	*
Video sub streams				*

22.3 System Architecture



22.4 Configuring the Video sources

Video can be streamed from either cameras or from the Milestone Image Server. For best results, it's recommended that the Milestone Image Server is used. To configure a regular camera, refer to the Channels page. To configure the video to be received from Milestone, proceed as follows.

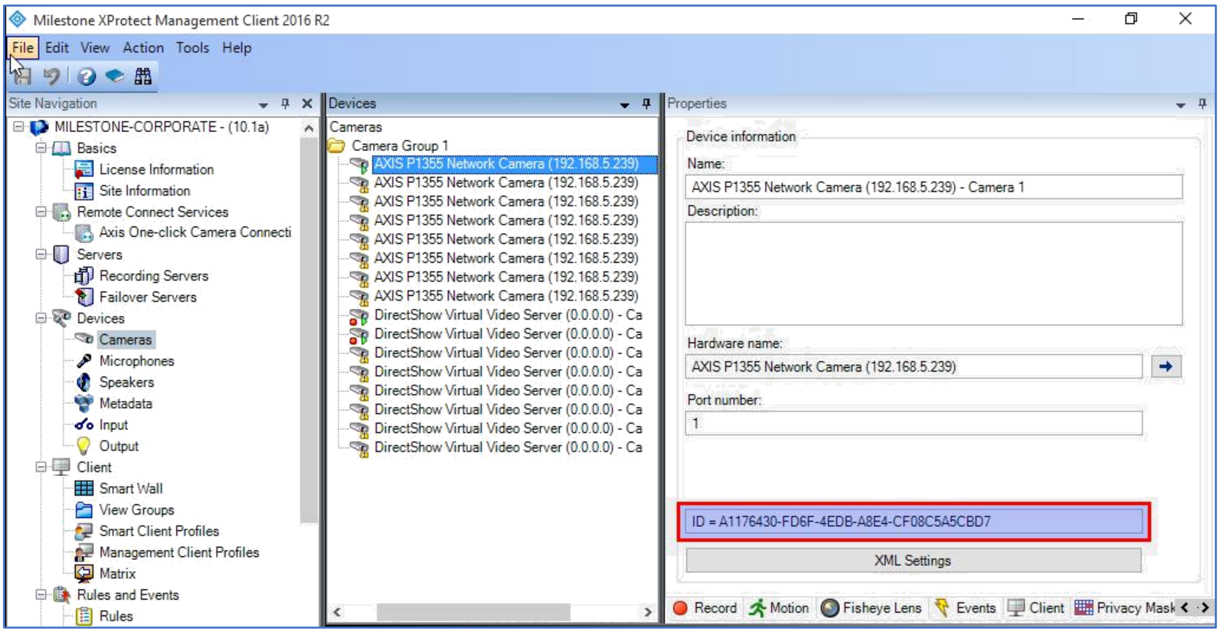
The first step is to identify the UUID (Universally Unique Identifier) used to identify the channel within

XProtect. The method to do this varies by XProtect Version. Each method is described below:

22.4.1 XProtect Corporate and Expert

There are two methods to discover the UUIDs corresponding to configured channels on an XProtect server. One uses the Management Client, the other interrogates the XProtect Management Server directly by issuing a HTTP request.

Using the Management Client GUI In the XProtect Management Client GUI, locate the camera (and specific stream in the case of multi-stream cameras). Then hold down CTRL and click the stream. The UUID is displayed at the bottom of the right-hand panel. Note that if CTRL is not held down when selecting the stream, the UUID is not displayed.



Name: AXIS P1355 Network Camera (192.168.5.239) - Camera 1

Description:

Hardware name: AXIS P1355 Network Camera (192.168.5.239)

Port number: 1

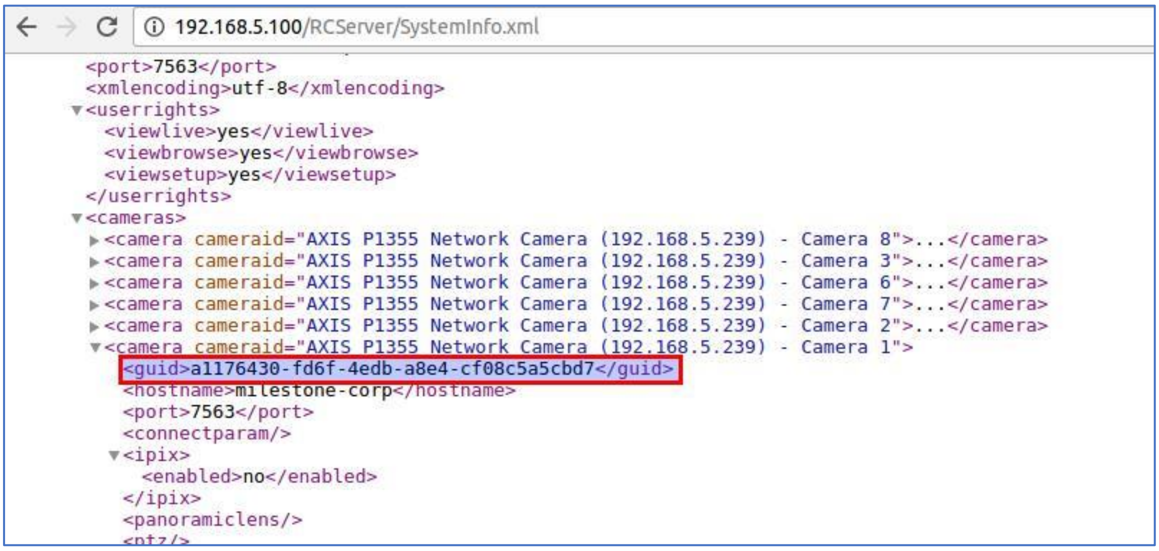
ID = A1176430-FD6F-4EDB-A8E4-CF08C5A5CBD7

Using a Web Browser to Interrogate the XProtect Server Using a web browser, navigate to the following URL:

http://<xprotect-server-hostname>/RCServer/SystemInfo.xml

The web browser may prompt for user credentials. If the server is configured to use Windows authentication, ensure to enter the username including the domain, e.g. as DOMAIN\username.

The description of the server configuration is returned in XML format. From here, locate the stream that VCA should use and copy out the value of the <guid> element:



192.168.5.100/RCServer/SystemInfo.xml

```
    <port>7563</port>
    <xmlencoding>utf-8</xmlencoding>
  ▼<userrights>
      <viewlive>yes</viewlive>
      <viewbrowse>yes</viewbrowse>
      <viewsetup>yes</viewsetup>
    </userrights>
  ▼<cameras>
    ▶<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 8">...</camera>
    ▶<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 3">...</camera>
    ▶<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 6">...</camera>
    ▶<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 7">...</camera>
    ▶<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 2">...</camera>
    ▼<camera cameraid="AXIS P1355 Network Camera (192.168.5.239) - Camera 1">
        <guid>a1176430-fd6f-4edb-a8e4-cf08c5a5cbd7</guid>
        <hostname>milestone-corp</hostname>
        <port>7563</port>
        <connectparam/>
      ▼<ipix>
          <enabled>no</enabled>
        </ipix>
        <panoramiclens/>
        <ptz/>
```

22.4.2 Xprotect Enterprise and Professional

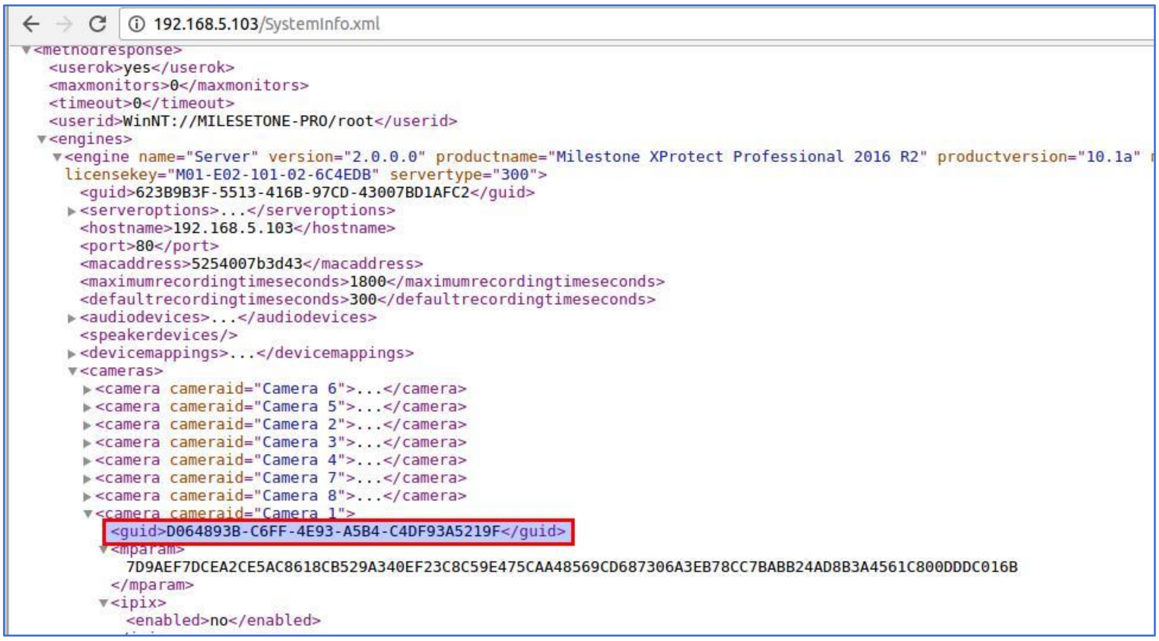
The recommended method for Enterprise and Professional versions of XProtect is to use the web browser to retrieve the system configuration in XML format.

Using a Web Browser to Interrogate the XProtect Server Using a web browser, navigate to the following URL:

http://<xprotect-server-hostname>/SystemInfo.xml

The web browser may prompt for user credentials. If the server is configured to use Windows authentication, ensure to enter the username including the domain, e.g. as DOMAIN\username.

The description of the server configuration is returned in XML format. From here, locate the stream that VCA should use and copy out the value of the <guid> element:

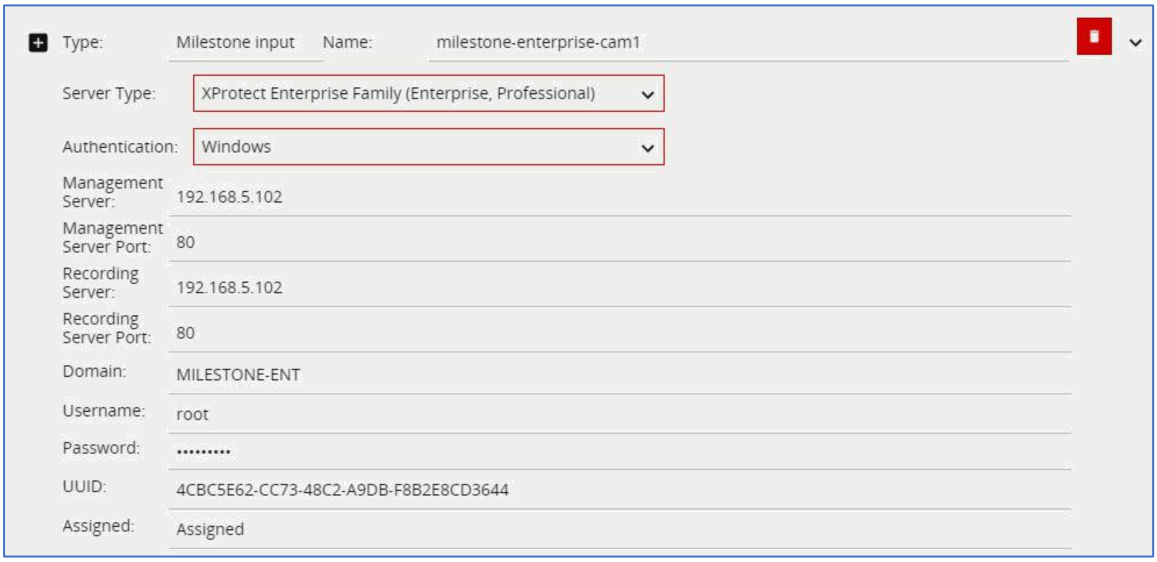


192.168.5.103/SystemInfo.xml

```
▼<methodresponse>
    <userok>yes</userok>
    <maxmonitors>0</maxmonitors>
    <timeout>0</timeout>
    <userid>WinNT://MILESETONE-PRO/root</userid>
  ▼<engines>
    ▼<engine name="Server" version="2.0.0.0" productname="Milestone XProtect Professional 2016 R2" productversion="10.1a"
      licensekey="M01-E02-101-02-6C4EDB" servertype="300">
        <guid>623B9B3F-5513-416B-97CD-43007BD1AFC2</guid>
      ▶<serveroptions>...</serveroptions>
        <hostname>192.168.5.103</hostname>
        <port>80</port>
        <macaddress>5254007b3d43</macaddress>
        <maximumrecordingtimeseconds>1800</maximumrecordingtimeseconds>
        <defaultrecordingtimeseconds>300</defaultrecordingtimeseconds>
      ▶<audiodevices>...</audiodevices>
        <speakerdevices/>
      ▶<devicemappings>...</devicemappings>
      ▼<cameras>
        ▶<camera cameraid="Camera 6">...</camera>
        ▶<camera cameraid="Camera 5">...</camera>
        ▶<camera cameraid="Camera 2">...</camera>
        ▶<camera cameraid="Camera 3">...</camera>
        ▶<camera cameraid="Camera 4">...</camera>
        ▶<camera cameraid="Camera 7">...</camera>
        ▶<camera cameraid="Camera 8">...</camera>
        ▼<camera cameraid="Camera 1">
            <guid>D064893B-C6FF-4E93-A5B4-C4DF93A5219F</guid>
          ▼<mparam>
              7D9AEF7DCEA2CE5AC8618CB529A340EF23C8C59E475CAA48569CD687306A3EB78CC7BABB24AD8B3A4561C800DDDC016B
            </mparam>
          ▼<ipix>
              <enabled>no</enabled>
```

22.4.3 Configuring the Channel within VCA

Having identified the UUID within XProtect, this needs to be added to VCA. On the Inputs and Outputs page add a Milestone Input:



Type:	Milestone input	Name:	milestone-enterprise-cam1
Server Type:	XProtect Enterprise Family (Enterprise, Professional)		
Authentication:	Windows		
Management Server:	192.168.5.102		
Management Server Port:	80		
Recording Server:	192.168.5.102		
Recording Server Port:	80		
Domain:	MILESTONE-ENT		
Username:	root		
Password:	·········		
UUID:	4CBC5E62-CC73-48C2-A9DB-F8B2E8CD3644		
Assigned:	Assigned		

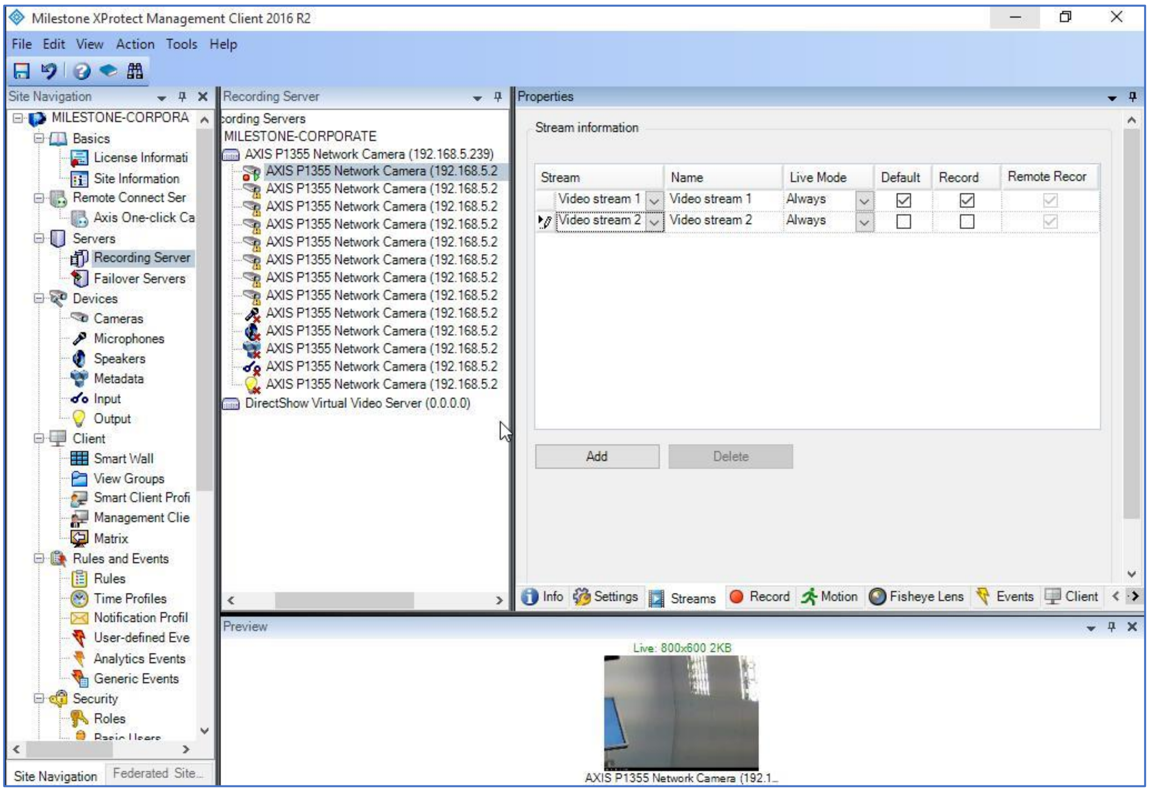
- **Server Type:** The type of the XProtect server(s).
- **Authentication:** The type of authentication to use with the Milestone Xprotect server. Can be either Basic Authentication or Windows Authentication. For Windows Authentication, the Domain must also be entered in the corresponding field. All versions of XProtect support Windows Authentication. Basic Authentication is only supported by XProtect Professional and Enterprise.
- **Stream:** The video stream index (0-index based). Where the source camera supports multiple streams, this setting selects which camera stream to retrieve from the Milestone XProtect server. Sub streams are only supported by XProtect Corporate. If the selected stream is not found, the default stream will be used. See below for further details.
- **Management Server:** The IP address or hostname of the XProtect Management Server.
- **Management Server Port:** The port that the XProtect Management Server is listening on.
- **Recording Server:** The IP address or hostname of the XProtect Recording Server.
- **Recording Server Port:** The port that the XProtect Recording Server is listening on.
- **Domain:** The Windows domain element of the user-id for the XProtect user. Only applicable when using Windows Authentication.
- **Username:** The username to use to log into the XProtect server(s).
- **Password:** The password to use to log into the XProtect server(s).
- **UUID:** The UUID of the channel within XProtect (determined in the previous step).

When the details are populated, assign the input to a Channel to view video from XProtect within VCA.

If video is not displayed, an error message will indicate the cause.

22.4.3.1 Using a Video Sub Stream for XProtect Corporate Only

To receive a sub stream from a channel in XProtect Corporate (for example where the camera supports multiple streams and only a low-resolution stream is required for VCA), the sub stream must be configured within the XProtect Management Client. Select the video source in the Recording Server Section and add the sub stream(s) as required.



Stream	Name	Live Mode	Default	Record	Remote Recor
Video stream 1	Video stream 1	Always	☑	☑	☑
Video stream 2	Video stream 2	Always	☐	☐	☑

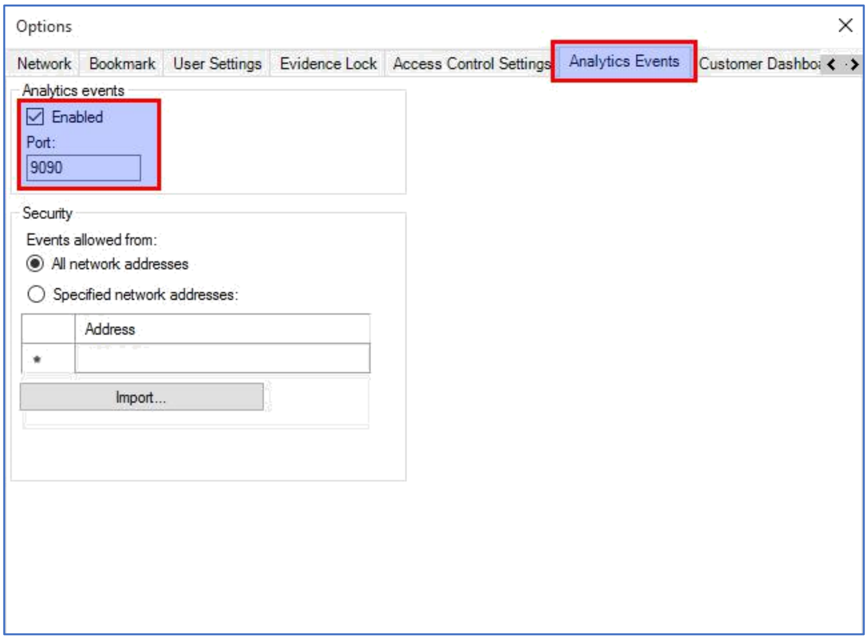
Make a note of the position of the sub stream in the Management Client, and enter this value (where the first position in the list corresponds to 0) in the **Stream** option of the Milestone input. For example, where the required sub stream is at the third position in the list, set the value of **Stream** to 2.

22.5 Configuring Event Outputs

In order to display events in the XProtect client, configuration is necessary in both the XProtect Management client and the VCA system.

22.5.1 Enable Analytics Events in XProtect

Analytics events must be enabled in Milestone XProtect in order to receive events from VCA. In the XProtect (Corporate Family) Management Client top menu select ‘Tools’ then ‘Options’. The options window pops up. Scroll to the right to select the ‘Analytics Events’ tab:



Analytics events

☑ Enabled

Port: 9090

Security

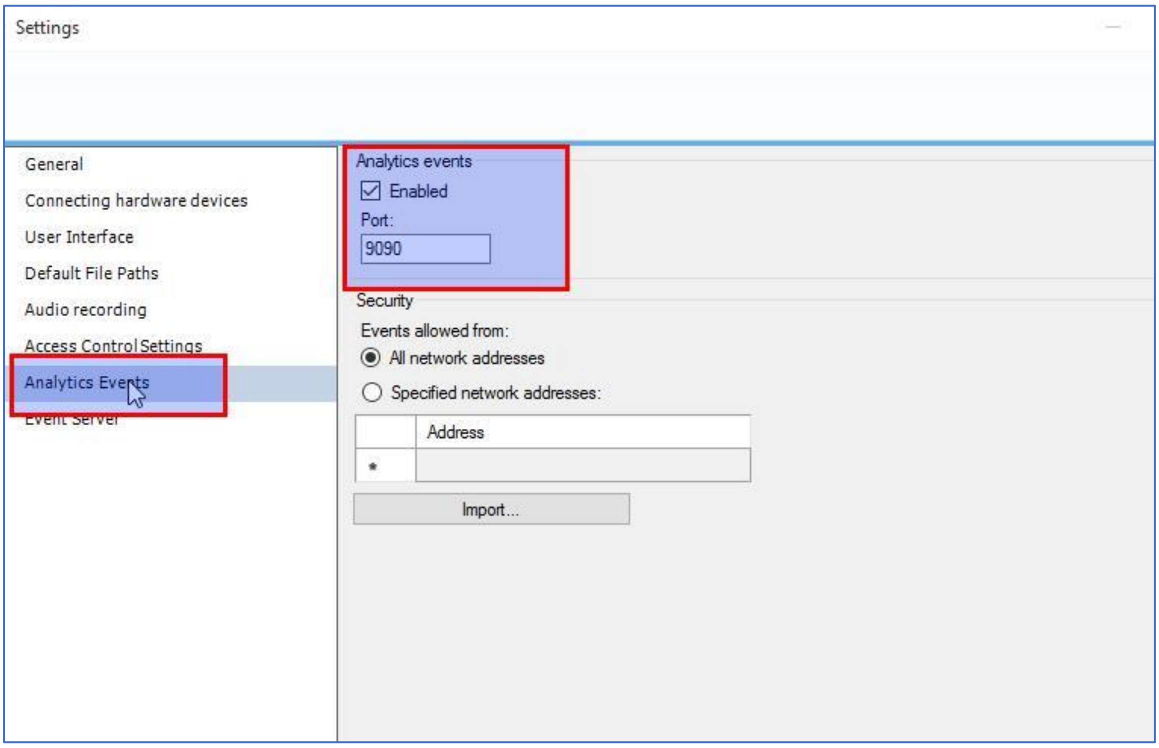
Events allowed from:

● All network addresses

○ Specified network addresses:

	Address
*	

In XProtect (Enterprise Family), Select ‘Settings’, then ‘Analytics Events’:



Analytics events

☑ Enabled

Port: 9090

Security

Events allowed from:

● All network addresses

○ Specified network addresses:

	Address
*	

Check the ‘Enabled’ box. It’s recommended to leave the default port setting of 9090 unless there is a specific reason to use a different value.

For additional security it is possible to add the IP addresses of known VCA devices in the ‘Security’ section. In this case, only events received from IP address in the list will be processed by the XProtect Event Server.

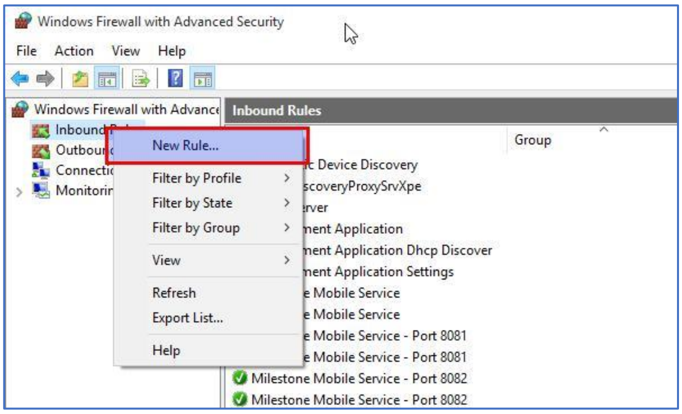
22.5.2 Configure Windows Firewall to Allow Events to be Received by Xprotect Event Server

The default configuration of the Windows Firewall is to block any traffic on port 9090. Therefore, a rule has to be added to the Firewall to allow events through to the XProtect Event Server.

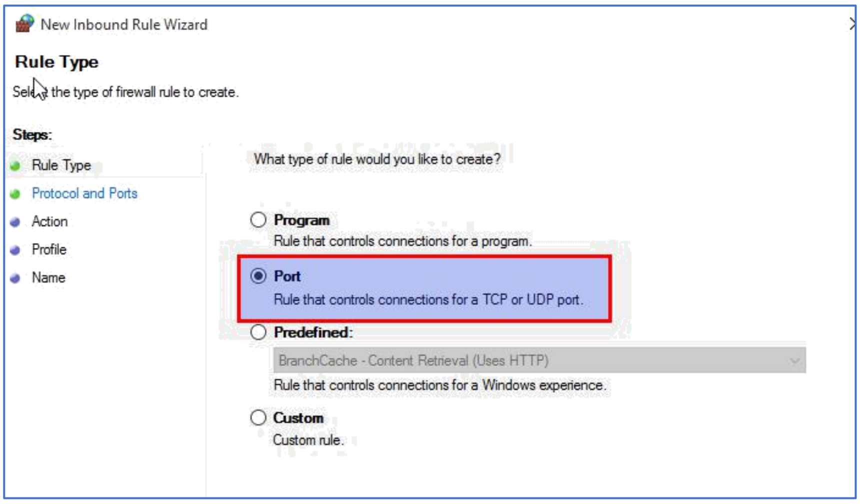
Note: The instructions below are for Windows 7 and Windows 10. For earlier versions please refer to the manual for your version of Windows

Open the Windows Firewall Advanced Settings (Control Panel -> Windows Firewall -> Advanced Settings)

Right-click on ‘Inbound Rules’ and ‘Add New Rule’:


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Ru
Outbound
Connectio
Monitorin
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Group
t Device Discovery
scoveryProxySrvXpe
erver
nent Application
nent Application Dhcp Discover
nent Application Settings
e Mobile Service
e Mobile Service
e Mobile Service - Port 8081
e Mobile Service - Port 8081
Milestone Mobile Service - Port 8082
Milestone Mobile Service - Port 8082

On the wizard that pops up select ‘Port’:



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

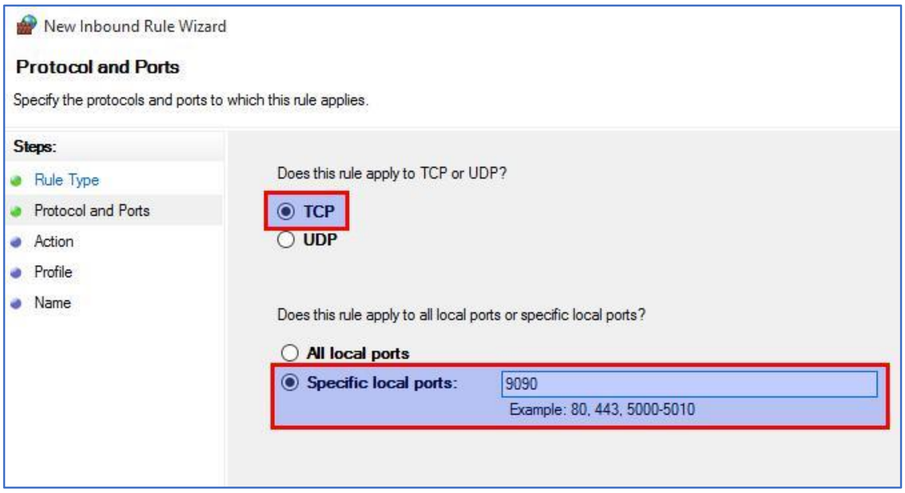
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

On the next page select ‘TCP’ and enter the port number to open. In this case, 9090:



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP

○ UDP

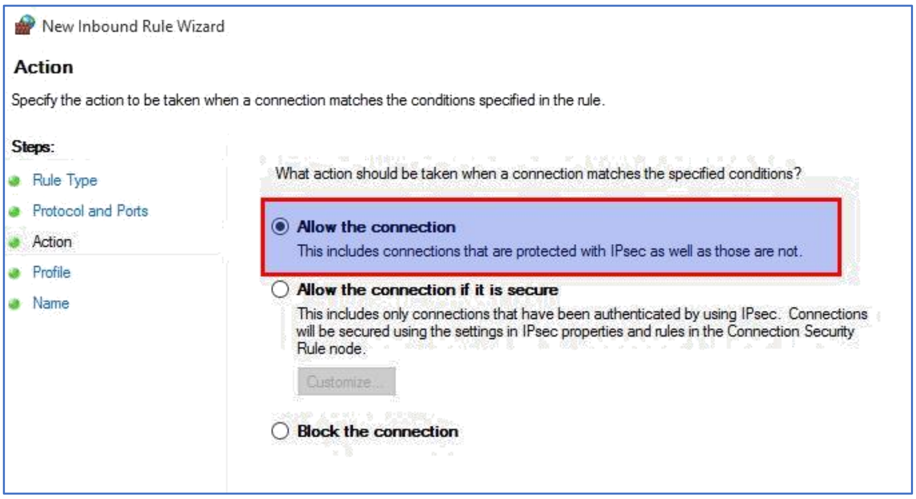
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 9090

Example: 80, 443, 5000-5010

On the next page, select 'Allow the connection':



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● Allow the connection

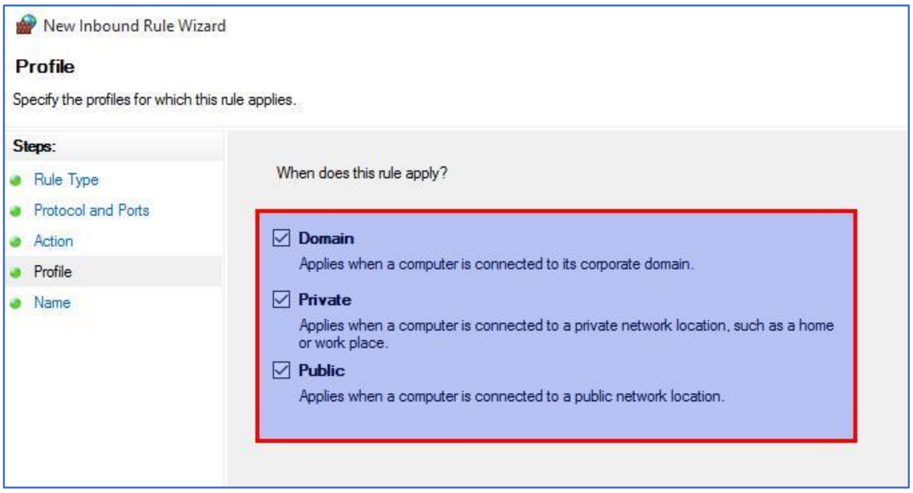
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

Then ensure that all relevant networks are selected. The local requirements may differ from the setup shown here. Here, everything is enabled:



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ Domain

Applies when a computer is connected to its corporate domain.

☑ Private

Applies when a computer is connected to a private network location, such as a home or work place.

☑ Public

Applies when a computer is connected to a public network location.

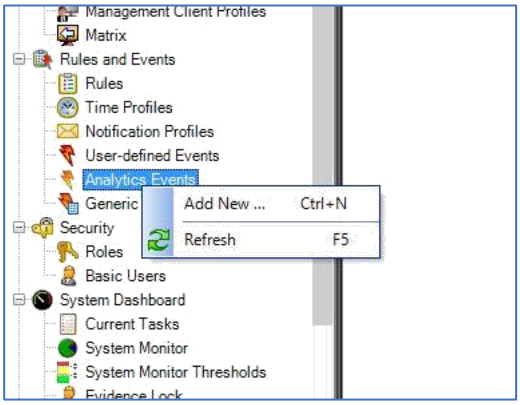
Finally, give it a suitable name so the rule can be easily identified in future, and click 'Finish':

22.5.3 Create the Analytics Event Type in XProtect

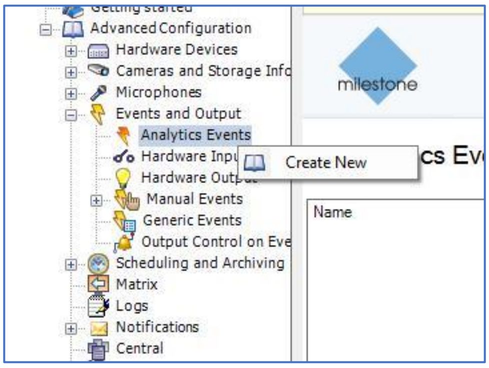
This step creates a new event type within XProtect that are used to identify events that come from VCA bridge.

In the XProtect Management Client select ‘Analytics Events’ and ‘Add New’/‘Create New’:

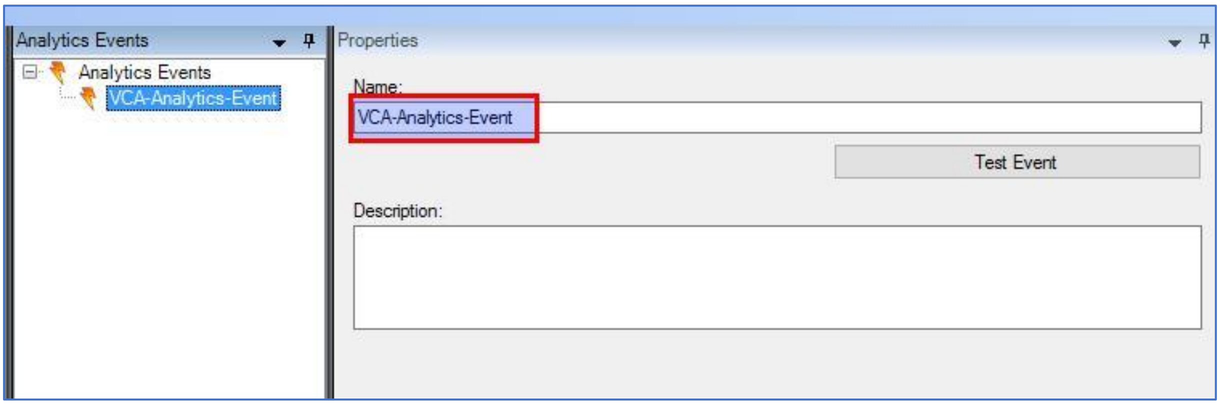
In XProtect, Corporate Family:



In XProtect Enterprise Family:



Name the event ‘VCA-Analytics-Event’. Double check the spelling. **If the event name does not exactly match ‘VCA-Analytics-Event’, events will not be received by the XProtect event server:**



Name: VCA-Analytics-Event

Description:

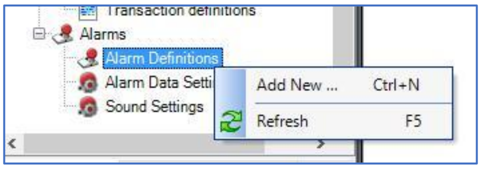
Note that the ‘Test Event’ function won’t work just yet. The event will be tested after the following step.

22.5.4 Create the Alarm Definitions in XProtect

This step maps the new event type created in the previous step (**VCA-Analytics-Event**) to the channels on which events are to be received.

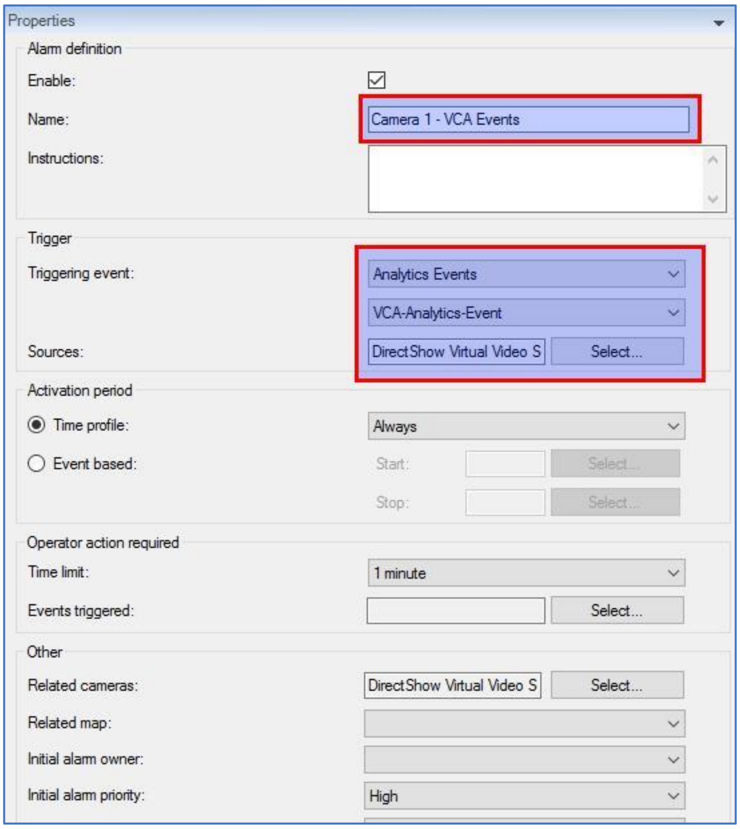
In the XProtect Management Client select ‘Alarm Definitions’ and ‘Add New’/‘Create New’:

In XProtect, Corporate Family:



In XProtect Enterprise Family:

Complete the alarm definition as illustrated below:



Properties

Alarm definition

Enable:	☑
Name:	Camera 1 - VCA Events
Instructions:	

Trigger

Triggering event:	Analytics Events VCA-Analytics-Event
Sources:	DirectShow Virtual Video S Select...

Activation period

● Time profile:	Always
○ Event based:	Start: Select... Stop: Select...

Operator action required

Time limit:	1 minute
Events triggered:	Select...

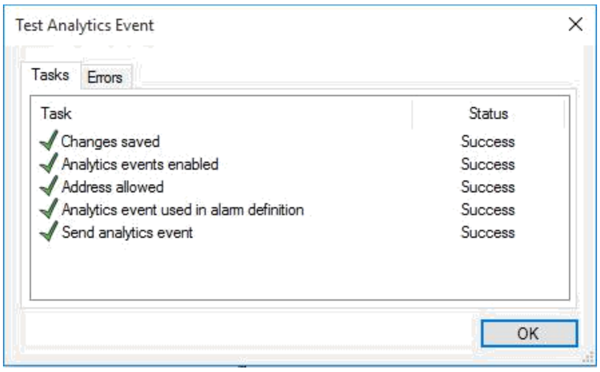
Other

Related cameras:	DirectShow Virtual Video S Select...
Related map:	
Initial alarm owner:	
Initial alarm priority:	High

- **Name:** Use a meaningful name. It does not have to be any specific value. Here it’s specified as ‘Camera 1 - VCA Events’.
- **Triggering Event:** Set the ‘Triggering Event’ to ‘Analytics Events’ and then select the specific event type to ‘VCA-Analytics-Events’ (the new event type that was created in the previous step).
- **Sources:** Select the video source (channel) with which this event will be associated. This event is associated with Camera 1, so click the ‘Select’ button to choose Camera 1:

Save the alarm definition.

The VCA-Analytics-Event created in the previous step can now be tested by clicking the 'Test Event' button:

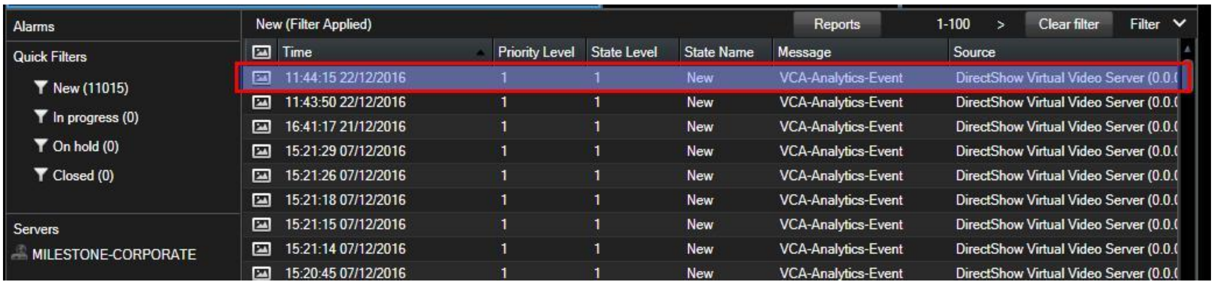


Test Analytics Event

Tasks | Errors

Task	Status
✓ Changes saved	Success
✓ Analytics events enabled	Success
✓ Address allowed	Success
✓ Analytics event used in alarm definition	Success
✓ Send analytics event	Success

Verify that the event also appears in the Milestone XProtect Smart Client Alarm Manager panel:



Time	Priority Level	State Level	State Name	Message	Source
11:44:15 22/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
11:43:50 22/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
16:41:17 21/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:21:29 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:21:26 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:21:18 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:21:15 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:21:14 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(
15:20:45 07/12/2016	1	1	New	VCA-Analytics-Event	DirectShow Virtual Video Server (0.0.(

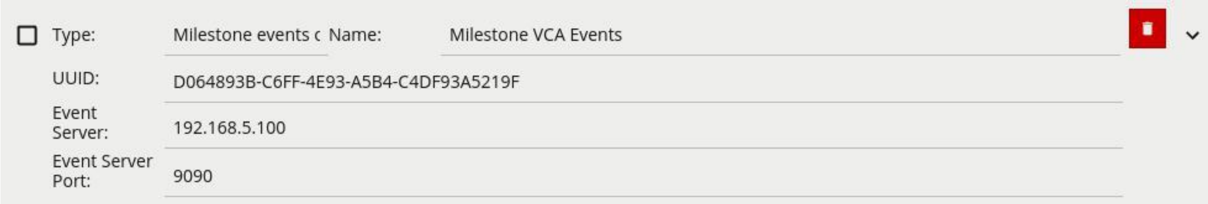
This concludes the necessary configuration within the XProtect Management Client. The next step is to configure VCA to send events to the XProtect Event Server.

22.5.5 Configure the Milestone Events Output to Send VCA Events to the XProtect

Event Server

Once the XProtect configuration is complete, the next step is to configure VCA to send **VCA-Analytics-Event** events to the XProtect Event Server.

In the Inputs and Outputs page add a 'Milestone Events Output' element:



☐ Type: Milestone events (Name: Milestone VCA Events

UUID: D064893B-C6FF-4E93-A5B4-C4DF93A5219F

Event Server: 192.168.5.100

Event Server Port: 9090

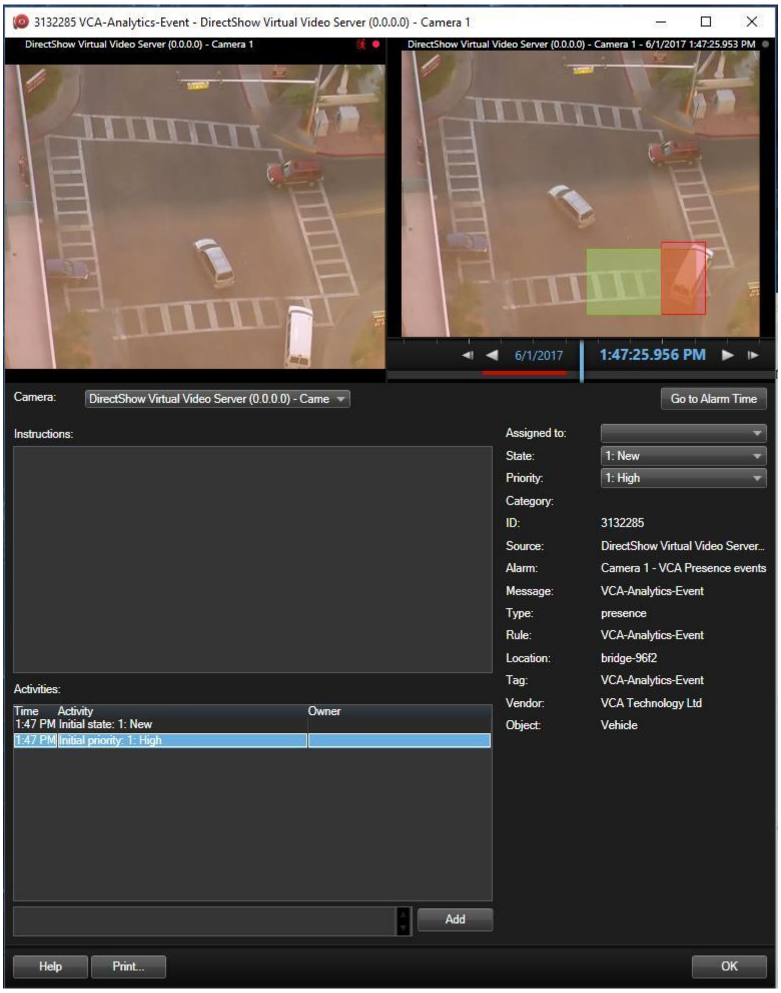
The values should be configured as follows:

- **UUID:** The XProtect UUID that identifies the channel to which VCA events correspond. This should match the UUID specified for the Milestone Input. In this illustration, both values are the same.
- **Event Server:** The IP address or hostname of the XProtect Event Server.
- **Event Server Port:** The port on which the XProtect Event Server is listening for events.

Assign the Milestone Events Output to the channel. See the Channels page for more details.

Provided that at least one VCA Rule is configured on the channel, VCA events should now appear in the XProtect Smart Client Alarm Log panel.

Note: In order for events to correctly play back with annotation inside the XProtect Smart Client, the channel must be set to be continuously recording, or triggered recording with the VCA-Analytics-Event as the trigger. The default setting for XProtect is to only record on motion detection (as detected by the XProtect Recording Server). With the default setting the events will not be recorded and cannot be reviewed from the XProtect Smart Client.


3132285 VCA-Analytics-Event - DirectShow Virtual Video Server (0.0.0.0) - Camera 1

DirectShow Virtual Video Server (0.0.0.0) - Camera 1

DirectShow Virtual Video Server (0.0.0.0) - Camera 1 - 6/1/2017 1:47:25.953 PM

6/1/2017 1:47:25.956 PM

Camera: DirectShow Virtual Video Server (0.0.0.0) - Came

Instructions:

Assigned to:
State: 1: New
Priority: 1: High
Category:
ID: 3132285
Source: DirectShow Virtual Video Server...
Alarm: Camera 1 - VCA Presence events
Message: VCA-Analytics-Event
Type: presence
Rule: VCA-Analytics-Event
Location: bridge-96f2
Tag: VCA-Analytics-Event
Vendor: VCA Technology Ltd
Object: Vehicle

Activities:

Time	Activity	Owner
1:47 PM	Initial state: 1: New	
1:47 PM	Initial priority: 1: High	

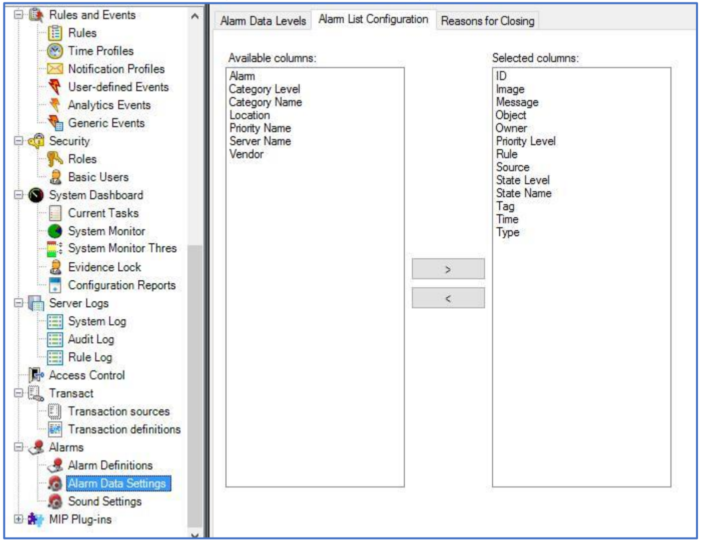
Here the event is annotated in the XProtect Smart Client Alarm Manager panel with a red bounding box. The Zone on which the VCA event was triggered is also rendered in green. Details of the event such as object type and rule name are also listed in the alarm list and the event review popup.

Note: If events do not appear in the XProtect Smart Client, it may be necessary to restart the XProtect Server processes or the Smart Client.

22.5.6 Analytics Events Details

Each analytics event is transmitted to the XProtect Event Server with a range of properties. To enable the event properties to be displayed in the Smart Client, it may be necessary to enable them in the Management Client.

Select ‘Alarms’, then ‘Alarm Data Settings’ from the configuration tree:

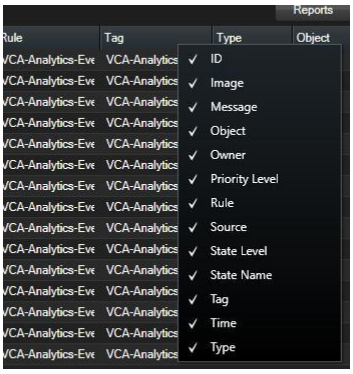


Available columns:
Alarm
Category Level
Category Name
Location
Priority Name
Server Name
Vendor

Selected columns:
ID
Image
Message
Object
Owner
Priority Level
Rule
Source
State Level
State Name
Tag
Time
Type

Select the desired event properties and move them from the left to the right panel.

To display the event properties in the Smart Client, right click on the event list header and select the fields to display:



✓ ID
✓ Image
✓ Message
✓ Object
✓ Owner
✓ Priority Level
✓ Rule
✓ Source
✓ State Level
✓ State Name
✓ Tag
✓ Time
✓ Type

Available fields are:

- **Type:** The type of the VCA event (presence, direction, etc).
- **Rule/Tag:** The rule name of the event.
- **Location:** The name of the device where the event was triggered.
- **Object:** The classification of the object that triggered the event.