

# SAIMOS

## VA

# Manual

**Version** 2020 R2 (build 3.2.12.3)

**Compiled** on 09.09.2020

## Contents

1	About SAIMOS VA.....	6
2	Node .....	7
2.1	Before installing SAIMOS VA Node.....	7
2.1.1	System Requirements.....	7
2.1.2	Installation package contents.....	7
2.1.3	Network communication.....	7
2.2	Installation.....	7
2.2.1	Windows.....	7
2.2.2	Linux .....	9
3	Server.....	10
3.1	Before you install.....	10
3.1.1	System Requirements.....	10
3.1.2	What will be installed .....	10
3.1.3	Network communication.....	10
3.1.4	Upgrade from 3.0.x to 3.1.x.....	10
3.1.5	Upgrade from 3.1.x to 3.2.x.....	11
3.1.6	Upgrade to 2020 R2.....	11
3.2	Installation.....	12
3.2.1	Windows.....	12
3.2.2	Linux .....	15
3.3	Licensing .....	16
3.3.1	The licensing page .....	16
3.3.2	Download a license request .....	16
3.3.3	Upload a license file.....	17
3.4	Snapshot / Live View Component (> 3.1.6) .....	19
3.5	Node Management .....	20
3.5.1	Node Overview .....	20
3.5.2	Automatic Node Detection.....	20
3.5.3	Adding a Node manually / Node options .....	21
3.5.4	Enable / Disable / Delete a Node .....	22
3.5.5	The Channel View .....	23
3.5.6	Add a channel .....	23
3.5.7	Enable / Disable / Delete a channel .....	24
3.5.8	Migrate channel(s) .....	24

3.5.9	Restart channel(s).....	25
3.6	Cameras.....	26
3.6.1	Camera overview.....	26
3.6.2	Automatic camera detection.....	26
3.6.3	Add / Edit Cameras.....	27
3.7	Interfaces.....	30
3.7.1	Milestone VMS .....	30
3.7.2	Multieye VMS .....	31
3.7.3	SMTP Server .....	32
3.7.4	Modbus Server .....	33
3.8	Channel configuration .....	34
3.8.1	Overview and general settings .....	34
3.8.2	Stream Source .....	35
3.8.3	Alerts .....	38
3.8.4	Perimeter.....	41
3.8.5	Count .....	46
3.8.6	Object .....	50
3.8.7	Scrambler.....	52
3.8.8	Motion Detectors .....	54
3.8.9	Face.....	58
3.8.10	LPR .....	61
3.8.11	Count Stereo.....	63
3.8.12	Edge .....	64
3.8.13	Lidar .....	66
3.8.14	Count 3D and Gate .....	70
3.9	Event Log .....	71
3.9.1	Filter.....	71
3.9.2	Event Image / Alarm Sequence .....	72
3.10	System Log.....	74
3.10.1	Filter Bar .....	74
3.11	User Management.....	76
3.11.1	The User View.....	76
3.11.2	The Group View .....	77
3.12	Server Administration .....	79
3.12.1	Network Configuration.....	79
3.13	Database Maintenance .....	80

3.14	Count Control .....	82
3.14.1	Dashboard .....	82
3.14.2	Counting statistics .....	83
3.14.3	Counting statistics filter menu .....	83
3.14.4	Heatmap .....	84
3.14.5	Occupancy monitor .....	86
3.14.6	Occupancy areas.....	86
3.14.7	Occupancy statistics .....	87
3.15	Face Analytics Pro.....	89
3.15.1	Face Log.....	89
3.15.2	Person Database.....	93
3.15.3	Black-/Whitelists.....	93
3.15.4	Image Upload .....	94
3.16	SAIMOS® LPR .....	95
3.16.1	LPR Log.....	95
3.16.2	Black-/Whitelists.....	97
3.17	System Alerts.....	99
3.18	TCP Command Interface.....	101
3.18.1	General command structure .....	101
3.18.2	Targets, commands & parameters .....	101
3.19	SAIMOS VA Plugin.....	102
3.19.1	About .....	102
3.19.2	Requirements .....	102
3.19.3	Installation.....	102
3.19.4	Configuration.....	103
3.19.5	Licensing .....	107
3.19.6	Count Plugin .....	109
3.19.7	Face Plugin.....	109
3.20	SeeTec Cayuga Plugin .....	110
3.20.1	Installing the plugin .....	111
3.20.2	Adding a channel .....	114
3.20.3	Alert Management .....	115
3.20.4	Troubleshooting .....	116
4	System backup and restore .....	117
4.1	Backing up SAIMOS VA using PGSQL commands .....	117
4.2	Restoring SAIMOS VA from a backup using PGSQL commands .....	117

4.3	Using the SAIMOS VA Scripts .....	118
4.3.1	Examples.....	118

## 1 About SAIMOS VA

SAIMOS® VA is the analytic framework of SAIMOS®. SAIMOS® VA consists of a central management server managing one or many analytic nodes. This makes scaling of the system to the customers' needs very easy. Every dimension - from the classic single server setup to a fully distributed corporate architecture - is possible. As we focus on modern web architecture and multi-platform performance, migration of channels from node to node as well as scaling up is simple.

The SAIMOS® VA System consists of two main components, the management server and the analytic node. The management server is a fully web-based management interface usable on any device using a modern web browser (Edge, Chrome, Firefox). It manages the analytic nodes. Please visit the section Server on page 10 to find out more details about the management server. The analytic nodes and their channels perform the actual analytics work. They also communicate with the management server and report to it via network messaging. Please visit the section Node on page 7 to get all the necessary information.

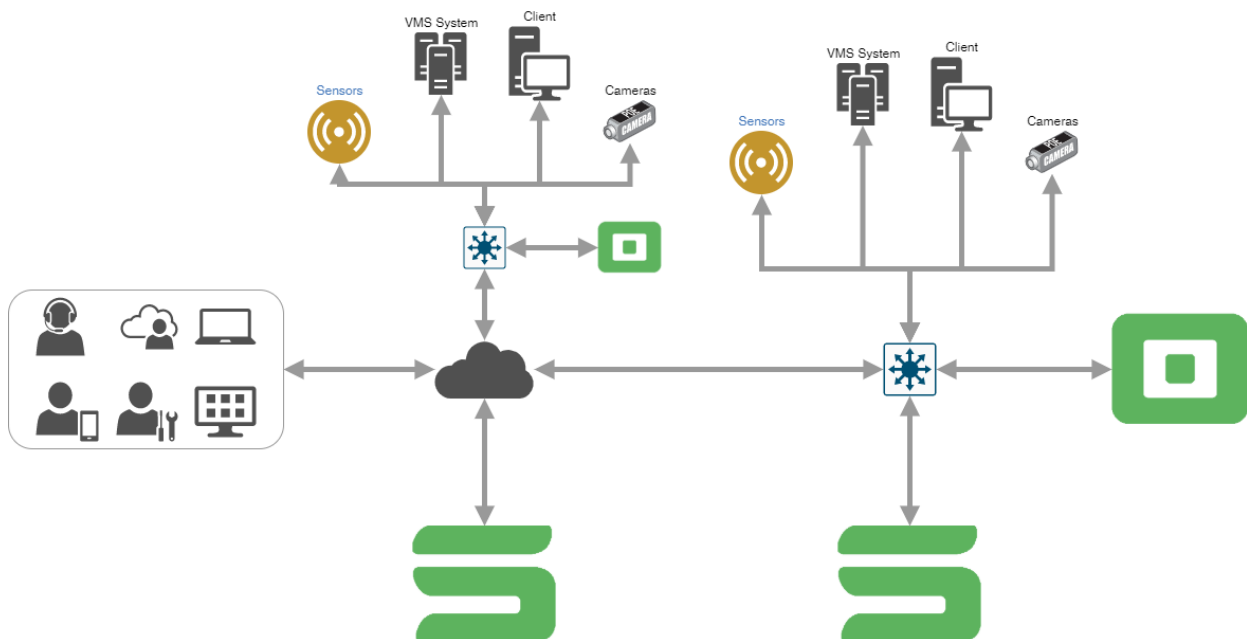


Image 1: The SAIMOS® VA architecture possibilities

## 2 Node

The SAIMOS® VA analytics node is a standalone service that will automatically manage channels that are added by the SAIMOS® VA Management Server. Therefore, as a prerequisite for managing a SAIMOS® VA Node a SAIMOS® VA Management Server has to be set up successfully (see below).

### 2.1 Before installing SAIMOS VA Node

#### 2.1.1 System Requirements

- OS (64 bit)
  - Windows: 8, 8.1, 10; 2012, 2012 R2, 2016, 2019
  - Linux: Ubuntu 18.04 LTS
- CPU
  - Intel i3/i5/i7/i9/Xeon CPU 6<sup>th</sup> generation or newer with at least AVX2 extensions enabled
- Memory
  - min. 2 GB RAM
- Harddisk
  - min. 4 GB
- Network
  - min. 100 Mbit network

#### 2.1.2 Installation package contents

- SAIMOS VA Node Package
- Intel® OpenVINO Redistributable

#### 2.1.3 Network communication

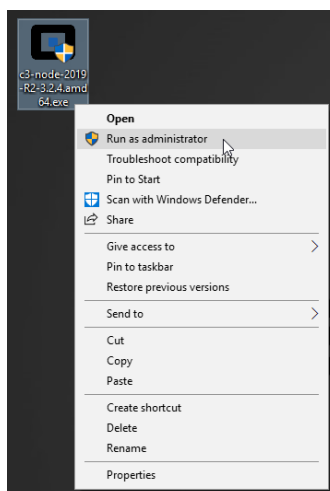
The following network ports are used by the SAIMOS VA node & server and should not be blocked by a firewall:

- 44444 (webserver)
- 44441 - 44443 (server-plugin communication)
- 45551, 45553, 45555 (server-node communication)

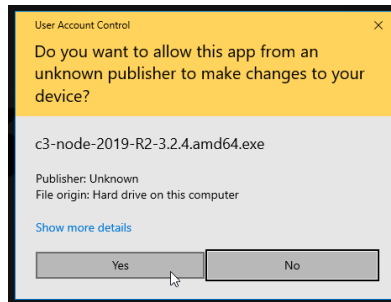
## 2.2 Installation

### 2.2.1 Windows

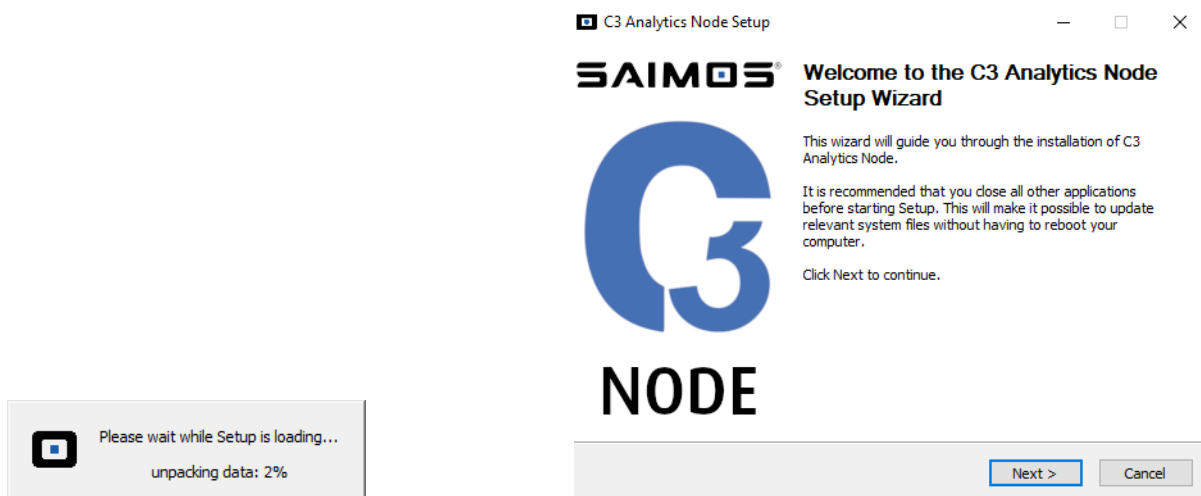
First, right-click the installer file and select “Run as administrator” to grant administrator rights to the installer.



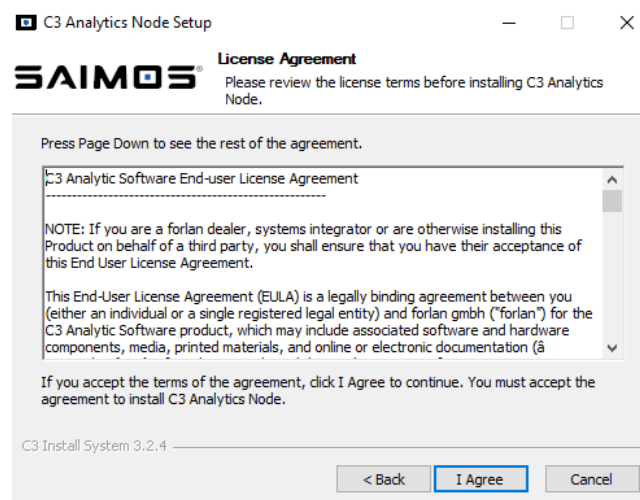
In case of a warning a dialog from “User Account Control”, select “Yes” to confirm administrator rights to the SAIMOS VA installer.



After the installer has loaded (i.e. checked its integrity and unpacked the compressed object) the (left), the welcome page of the Installer is displayed (right).

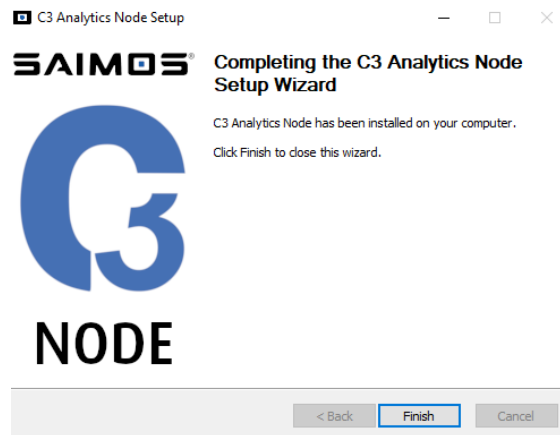


Click Next > to continue. This will land you on the License Agreement page.

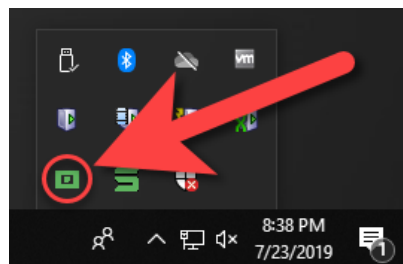



Read our EULA carefully. Once you have agreed to our EULA the installer starts the installation process. Be patient, this might take some time ...

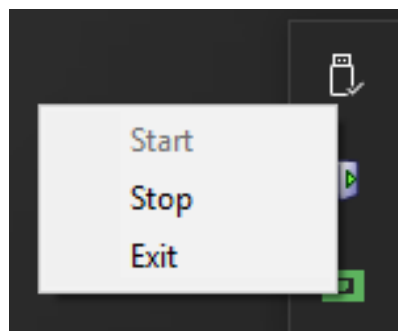




If the installer is finished, you have to click Finish to complete the installation process. If everything was successful you should see the SAIMOS VA Node icon in the Windows Taskbar.



If you see the green O icon you know the node service is running (otherwise this will be gray ). If you right or left click on the icon you can start the node service, stop the node service or exit the node service manager.



If everything was successful visit the SAIMOS VA Server Manager to manage the newly installed node.

## 2.2.2 Linux

```
sudo dpkg -i <path/to/package/package.deb>
```

## 3 Server

The SAIMOS VA Server is a single-page web interface for the management of distributed SAIMOS VA Nodes.

### 3.1 Before you install

#### 3.1.1 System Requirements

- OS (64 bit)
  - Windows: 8, 8.1, 10, 2008 R2, 2012, 2012 R2, 2016, 2019
  - Linux: Ubuntu 18.04 LTS
- Memory
  - At least 4 GB RAM
- Harddisk
  - At least 50 GB free disk space
- Network
  - At least 100 Mbit network
- Browser
  - SAIMOS VA management server relies on HTML5/JavaScript technology. Therefore, it is recommended to use the latest version of one of the following browsers:
  - Chrome, Firefox, Edge, Vivaldi

#### 3.1.2 What will be installed

- Python 3 (embedded, Windows OS only)
- Microsoft Visual C++ 2010 Redistributable Package (x64) (Windows OS only)
- Microsoft Visual C++ 2013 Redistributable Package (x64) (Windows OS only)
- Microsoft Visual C++ 2015 Redistributable Package (x64) (Windows OS only)
- PostgreSQL 10.x
- SAIMOS VA Server Package

#### 3.1.3 Network communication

The following network ports are used by the SAIMOS VA node & server and should not be blocked by a firewall:

- 44444 (webserver)
- 44441 - 44443 (server-plugin communication)
- 45551, 45553, 45555 (server-node communication)

#### 3.1.4 Upgrade from 3.0.x to 3.1.x

Due to a PostgreSQL upgrade from 9.3 to 9.5 the database has to be migrated before installing the new 3.1.x versions. To upgrade follow the following steps:

1. Stop the server service
2. Open console, create dump\*:
 

```
pg_dump -h localhost -U cogvis -d cogvis -Fd -f <dump-dir>
```
3. Uninstall old SAIMOS VA server
4. Rename <SAIMOS VA>\db to something else, e.g. db-9.3
 

On Windows it is located at C:\ProgramData\cogvis3\server\db
5. Install new SAIMOS VA server package
6. Stop the new SAIMOS VA server service

7. In the console, recreate and restore cogvis database\*:  
dropdb -h localhost -U cogvis cogvis  
createdb -h localhost -U cogvis -E UTF8 cogvis  
pg\_restore -h localhost -U cogvis -d cogvis <dump-dir>
8. Start server service

\*To use the PostgreSQL commands on Windows execute the commands from the following directory:  
C:\ProgramData\cogvis3\server\pgsql\bin

### 3.1.5 Upgrade from 3.1.x to 3.2.x

Due to a PostgreSQL upgrade from 9.5 to 10.5 the database has to be migrated before installing the new 3.2.x versions. To upgrade follow the following steps:

Use the same procedure as described in 3.1.4.

### 3.1.6 Upgrade to 2020 R2

Please ensure that you uninstall the previous version cleanly before installing 2020 R2 using the current versions uninstaller.

Please also make sure that you have backed up the current version fully before upgrading. This is a just in case measure, normally the upgrade should run smoothly if the uninstallation is done beforehand and the database holding the current configuration and data should be migrated without any problems.

If not needed on the current system by other software, the Python 2.7 installation on Windows OS systems can be removed manually as well. SAIMOS® VA 2020 R2 will use embedded Python 3.8 on Windows and has no use for Python 2.7 anymore.

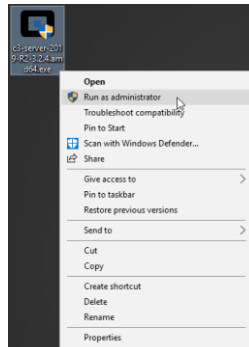
Please note that (while not supported for some time now) the installation on Windows 7 of SAIMOS® VA 2020 R2 has known problems and the libraries and languages used with this new version are reportedly not compatible with Windows 7 anymore.

DEPRECATION: Please note that, due to the inclusion of Intel OpenVINO, with 2020 R2 CPUs have to have at least AVX2 extensions enabled. CPUs without AVX2 support have been deprecated and will not be supported from 2020 R3 and onward. This means that Intel CPUs without AVX2 support (older than 6<sup>th</sup> generation) will not be supported anymore.

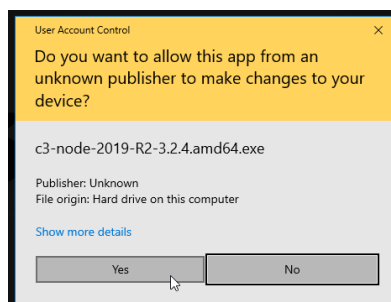
## 3.2 Installation

### 3.2.1 Windows

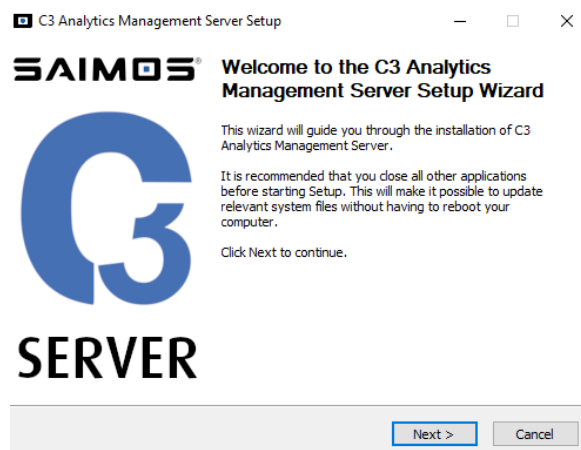
First, right click the installer file and select *Run as administrator* to grant administrator rights to the installer.



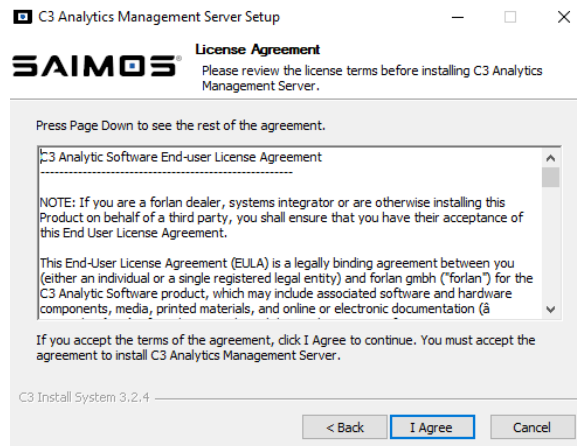
In case of a warning dialog displayed from *User Account Control*, select *Yes* to confirm the administration rights to the SAIMOS VA installer.



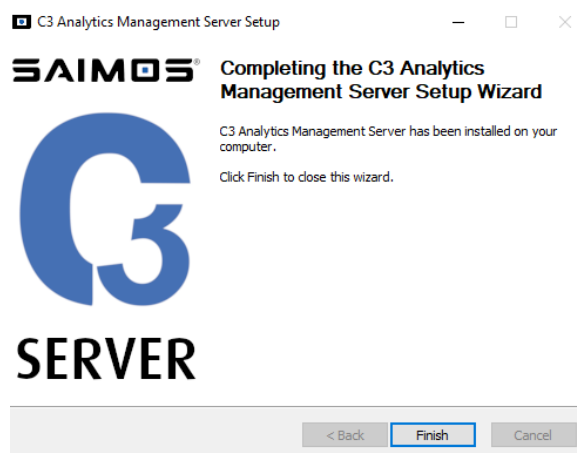
After that the installer is loading (i.e. checking its integrity and unpacking the compressed object). Once finished the Installer window is opened showing the welcome page for the installation.



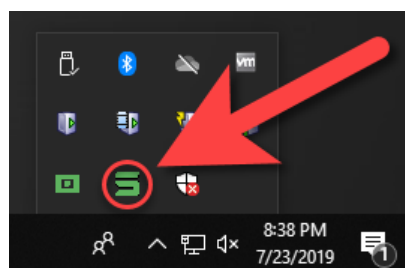
Click *Next >* to continue. This will take you to the License Agreement page.



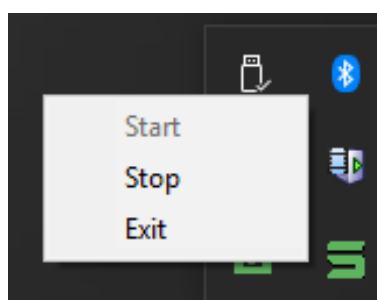
Please read our EULA carefully. Confirming your consent with I Agree will start the installation process. Be patient, this can take some time ...



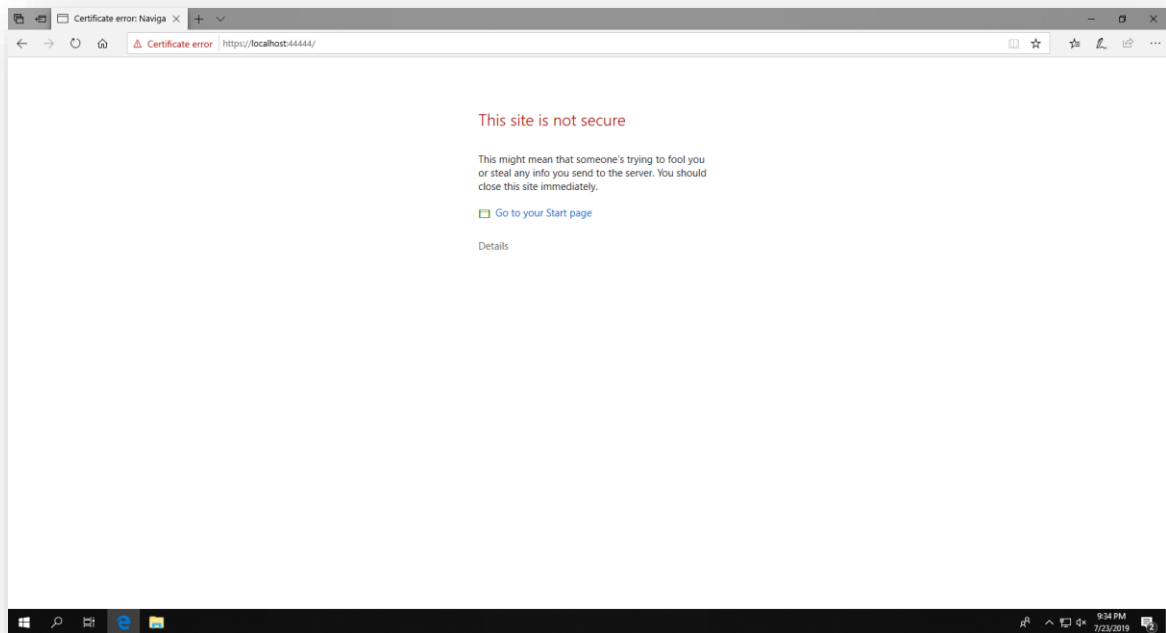
After the SAIMOS VA Analytics Management Server has been installed on your computer, click *Finish* to complete the installation process. If the installation was successful the SAIMOS VA Server Manager icon is displayed in the Windows taskbar.



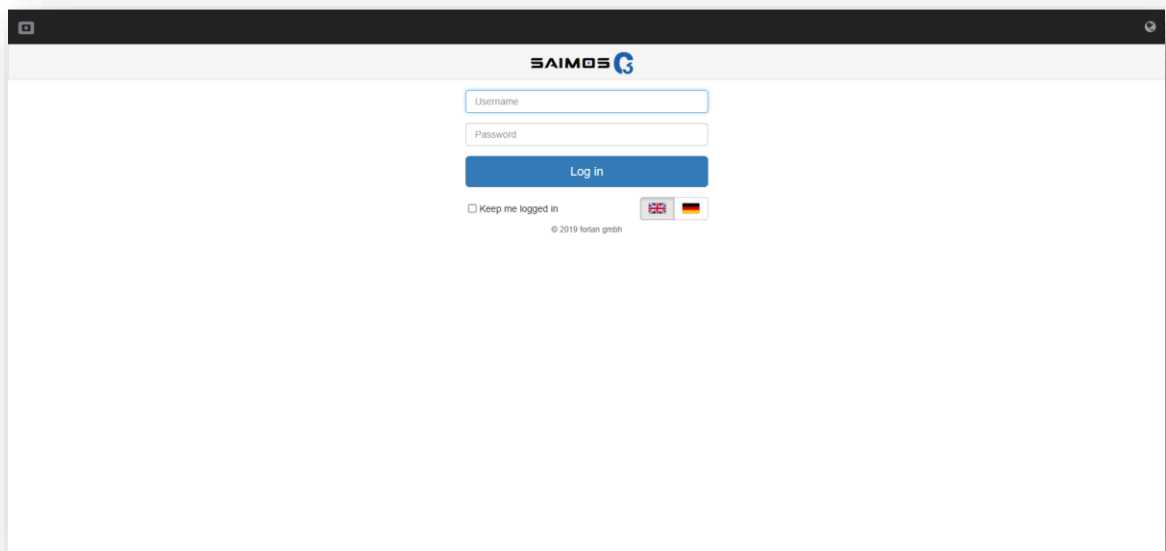
A green server icon indicates the server status as *running*, a gray icon as *stopped*, respectively. The server service is accessed by clicking the icon and allows to start or stop the server service or to exit the server service manager.



When opening the server within the browser (<https://localhost:44444>), there is a good chance that you will get an SSL error because of our self-signed certificate. Just tell the browser to ignore the error and load the page anyway.



After that you should see the login screen of the SAIMOS VA Server web UI.

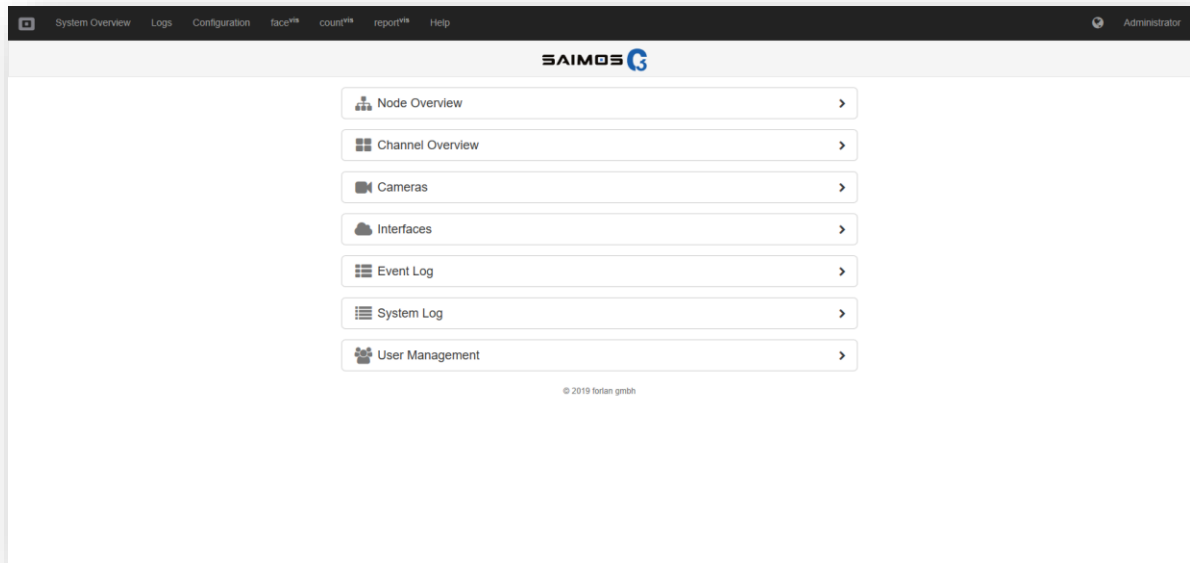


Enter the default credentials and click the *Log in* button:

*admin* (username)

*test* (password)

Now you should be logged in successfully and can start configuring the server, adding nodes to your system or changing the admin password.



### 3.2.2 Linux

`sudo dpkg -i <path/to/package/package-name.deb>`

## 3.3 Licensing

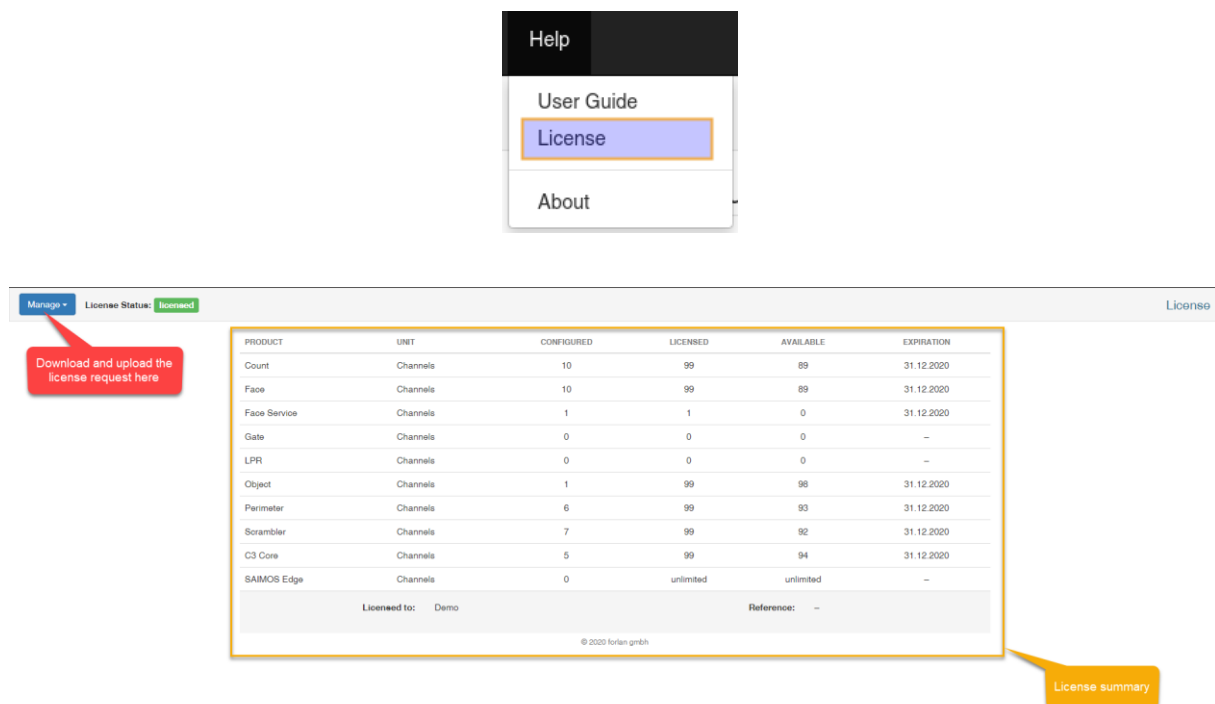
The SAIMOS VA installation comes with a 30-day trial period allowing for testing the system extensively with full functionality. After the trial period has expired a license has to be purchased for every channel to continue to operate them. In SAIMOS VA, all necessary licensing is handled by the management server, which distributes the licenses to the nodes automatically. Licenses can be purchased on a per-channel-and-product base and can be conferred. This means, that licensed channels can run on any node and can also be migrated to another node within the system. Furthermore, if a channel of a specific licensed product is disabled, the 'released' license can be transferred to another channel of the same product. Channels without active license are automatically disabled by the server and once a channel is disabled, it will not start again automatically, even if a license is available.

To purchase a license, a license request (see below) has to be sent to either a trusted SAIMOS partner or directly to [contact@saimos.eu](mailto:contact@saimos.eu). In return you will receive a valid license for the requested product channel(s). This license has to be uploaded to the management server. In case of any problems occurring during the licensing process, please do not hesitate to contact our support ([support@saimos.eu](mailto:support@saimos.eu)).

### 3.3.1 The licensing page

The license page is accessible through the menu item *Help* → *License*.

This will open the licensing page showing an overview about the system's licensing status: The number of configured and/or licensed channels are displayed as well as its expiration date (for trial licenses or temporarily limited licenses).



Help

User Guide

License

About

Manage License Status: **Issued** License

Download and upload the license request here

PRODUCT	UNIT	CONFIGURED	LICENSED	AVAILABLE	EXPIRATION
Count	Channels	10	99	89	31.12.2020
Face	Channels	10	99	89	31.12.2020
Face Service	Channels	1	1	0	31.12.2020
Gate	Channels	0	0	0	—
LPR	Channels	0	0	0	—
Object	Channels	1	99	98	31.12.2020
Perimeter	Channels	6	99	93	31.12.2020
Scrambler	Channels	7	99	92	31.12.2020
C3 Core	Channels	5	99	94	31.12.2020
SAIMOS Edge	Channels	0	unlimited	unlimited	—

Licensed to: Demo Reference: —

© 2020 forlan GmbH

License summary

Note: As mentioned above, the trial-version of SAIMOS VA is provided with full functionality. Also, the number of channels is not limited within the trial period. Hence, the test-system can be set up, modified and tested for any scenario or of any dimension.

### 3.3.2 Download a license request

The first step in licensing is to generate and download a license request:

Click *Manage* → *Download license* on the top left at the licensing page and a list containing all products with a license-selector is displayed.



Download
Cancel

License Request

1

Name: UP Xtreme Smart Surveillance SAIMOS C3 CORE

Address:

street address

ZIP

city

country

Notes:

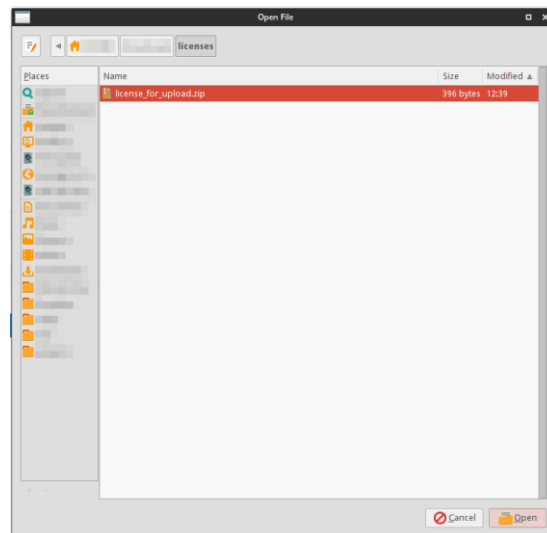
Select the number of licenses (channels) you would like to purchase of each product by either using the + and – buttons to increase or decrease the number of licenses (2) of a specific product or by overwriting the displayed number of licenses in the text field.

After you have finished selecting the licenses you want to purchase, click *Download* (1) to generate a license request package. Send the ZIP-file (as it is) to either your preferred SAIMOS reseller or to [contact@saimos.eu](mailto:contact@saimos.eu) to obtain the requested licenses.

### 3.3.3 Upload a license file

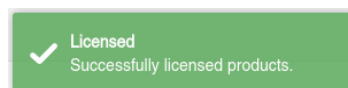
If the request was successful, you will have received a valid license file from SAIMOS or your SAIMOS reseller and are ready for the second and final step in licensing the channels:

Uploading the received file. Click *Manage* → *Upload License File* and select the license file from the directory you downloaded it to.



**Note: Please update the ZIP file as it is, i.e. do not unpack it before uploading.**

If the upload was successful the following message is displayed:

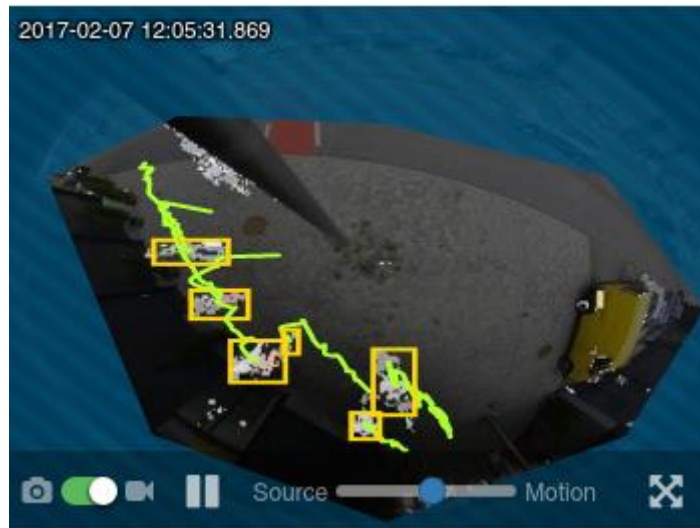


Furthermore, the license page is updated according to the newly acquired licenses.

In case there are products acquired with a temporally limited license period, the expiration date will be displayed in the rightmost column and the line of the product in the product overview table. Licenses without expiration are symbolized with an infinity ( $\infty$ ) symbol.

## 3.4 Snapshot / Live View Component (> 3.1.6)

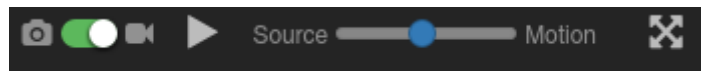
The new Snapshot / Live View component was introduced with C3 3.1.6 and is used throughout the system. It shows the analyzed area of the channel as well as metadata and a live view source/motion mix-in where applicable.










There are two modes, the snapshot mode



and the live view mode.



You can switch between the modes using the  switch. In snapshot mode you can refresh the snapshot using the  button or you can upload an image manually using the  button. In live view mode you can start or pause playback using the  or  buttons. The  control lets you mix-in the motion detection with the source image. Setting the slider to source will only show the source video and setting the slider to motion will only show the motion image. You can use the slider to choose the mix-in between the two sources. In both controls the  button will allow you to set the current component to full-screen.

**Attention: The live view component will only work on active channels and can use up a lot of resources. Do not attempt to start more than 2 - 3 components at once in live view.**

## 3.5 Node Management

### 3.5.1 Node Overview

The node overview is one of the central views within the SAIMOS VA server interface. Here the main configuration of the nodes can be done: to detect, add, delete, enable and disable nodes or add channels. For each node the node overview shows its name, the node IP-address and its current health status. It includes the CPU and RAM load in real-time as well as the number of channels and their status (running, disabled or stopped) per node. The node overview supports two different views: the list view and the grid view. The following screenshots show these two different views and describe the different elements and control options to configure the nodes.

#### 3.5.1.1 List View

Node	Host	CPU	MEM	STATUS	CHANNELS
C3 Demo Server	192.168.1.144	60%	41%	ONLINE	5
CogVis Win7 Demo Server	192.168.1.113	14%	38%	ONLINE	5
Milestone Enterprise Server	192.168.1.129	11%	28%	ONLINE	5
NUC i5 1	192.168.1.50	0%	4%	ONLINE	0
NUC i5 2	192.168.1.53	0%	4%	ONLINE	0

Total: 5 nodes

#### 3.5.1.2 Grid View

click to enter node

select node by clicking inside it

configure node

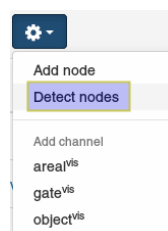
number of channels running/stopped/deactivated

Total: 5 nodes

© 2015 CogVis GmbH

### 3.5.2 Automatic Node Detection

SAIMOS VA server supports automatic node detection for nodes within the same network. To automatically detect nodes click the *option* symbol within the *node overview* and select the *Detect nodes* option.



A modal window will open to lead through the automatic node detection process.

Detect CogVis Analytics nodes

Start detection

Ready

Add nodes Cancel

To start the detection press *Start detection*. The detection takes a few seconds. If nodes within the network are found by the server were found within the network of the server will be listed in the modal window. Nodes that are already managed by another server are listed as well, but cannot be selected to be added to the server.

Add nodes Cancel
Node Detection

Start detection

5 new nodes detected

select nodes

<input type="checkbox"/>	IP ADDRESS	SYSTEM	VERSION
<input type="checkbox"/>	192.168.1.129	user-PC / Windows 7 SP1 (AMD64)	3.0.0b3
<input type="checkbox"/>	192.168.1.144	WIN-7CL11VEBQ4D / Windows 2012Server (AMD64)	3.0.0b3
<input type="checkbox"/>	192.168.1.145	cogvis-gatevis1 / Ubuntu 14.04 (x86_64)	3.0.0b3
<input type="checkbox"/>	192.168.1.50	nucone / Ubuntu 14.04 (x86_64)	3.0.0b3
<input type="checkbox"/>	192.168.1.53	nuctwo / Ubuntu 14.04 (x86_64)	3.0.0b3

1 node managed by 192.168.1.103

2 nodes managed by 192.168.1.149

1 node managed by 192.168.1.57

add selected nodes

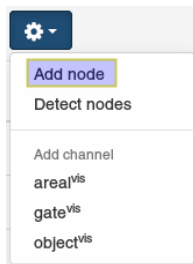
Add nodes Cancel

You can now select the required nodes you want to add to the management server: Check the box left of the respective node name and select *Add nodes*. The newly added nodes are then also listed in the node overview.

<input type="checkbox"/> NODE *	HOST *	CPU %	MEM %	STATUS *	CHANNELS			
<input type="checkbox"/> cogvis-gatevis1	192.168.1.145	0%	5%	ONLINE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> nucone	192.168.1.50	0%	4%	ONLINE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> nuctwo	192.168.1.53	0%	4%	ONLINE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> user-PC	192.168.1.129	20%	20%	ONLINE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> WIN-7CL11VEBQ4D	192.168.1.144	3%	25%	ONLINE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Total: 5 nodes								

### 3.5.3 Adding a Node manually / Node options

In case a node is not detected automatically or if it is not within the same network (e. g. : NAT, DynDNS) you can also add it manually. For that, select *Add node* from the options dropdown within the node overview.



In the *Add node* view select an arbitrary name for the node to be added and specify its network address and port (default port for node communication: 45555). You can also select if the node should be enabled (default) or disabled after adding.

Example for a valid configuration:

By clicking *Save*, the node is added to the node overview. To modify the values for an existing node access the node options either by clicking the *options* button of the node (on the right) from within the *Node Overview* or by selecting *Configuration* from the *options* menu within the node view.

Examples:

- *Options* button on the right of the node in the *Node Overview*:



- Select *Configuration* from within the *options* menu in the *channels* view of the node:



### 3.5.4 Enable / Disable / Delete a Node

You can enable, disable or delete nodes. Disabling a node results in all its channels being disabled as well and in showing the “disabled” status in the *Node Overview*. As a consequence, the disabled node will not send any health-data. Deleting node will remove it from the system. You can modify the status of a node by selecting the respective node within the *Node Overview* and *Enable/Disable/Delete*. You can also select multiple nodes to modify their statuses in one go.

HOST	CPU	MEM	STATUS	CHANNELS
192.168.1.145	0%	5%	ONLINE	
192.168.1.50	0%	4%	ONLINE	
192.168.1.53	0%	4%	ONLINE	
192.168.1.129	—	—	DISABLED	
192.168.1.144	5%	25%	ONLINE	

Total: 5 nodes

## 3.5.5 The Channel View

The channel view shows all channels assigned to a specific node and supports a *list view* and a *grid view*. Health-information, such as CPU and RAM usages, as well as the channel-status (running, starting, stopped) is displayed for each channel. From within this view it is possible to add or delete channels as well as to enable, disable or configure the node. In addition, channels can be migrated to other nodes from here.

### 3.5.5.1 List View

CHANNEL	STREAM DEVICE	NODE	UPTIME	CPU	MEM	STATUS
anonymvis axis streetview (keep 129) - anonym <sup>vis</sup>	AXIS M1114	Milestone Enterprise Server	27 minutes	3%	0%	RESTARTING
anonymvis sony streetview (keep 144) - anonym <sup>vis</sup>	Sony SNC-CH210	C3 Demo Server	3 days	4%	2%	RUNNING
Axis Streetview areavis standard - areavis <sup>vis</sup>	AXIS M1114	CogVis Win7 Demo Server	7 days	2%	8%	RUNNING

### 3.5.5.2 Grid View

refresh picture

upload screenshot

click to enter node

anonymvis axis streetview (keep 129) RUNNING

anonymvis sony streetview (keep 144) RUNNING

Axis Streetview areavis standard RUNNING

## 3.5.6 Add a channel

You can add a channel in the node overview as well as in the channel view within a node. For both views, use the *option* drop-down and select the requested product channel by clicking on it.

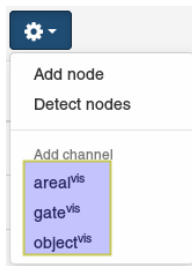
Examples:

from the channel view

Add channel

- area<sup>vis</sup>
- gate<sup>vis</sup>
- object<sup>vis</sup>
- Node nuctwo
- Enable
- Disable
- Configure

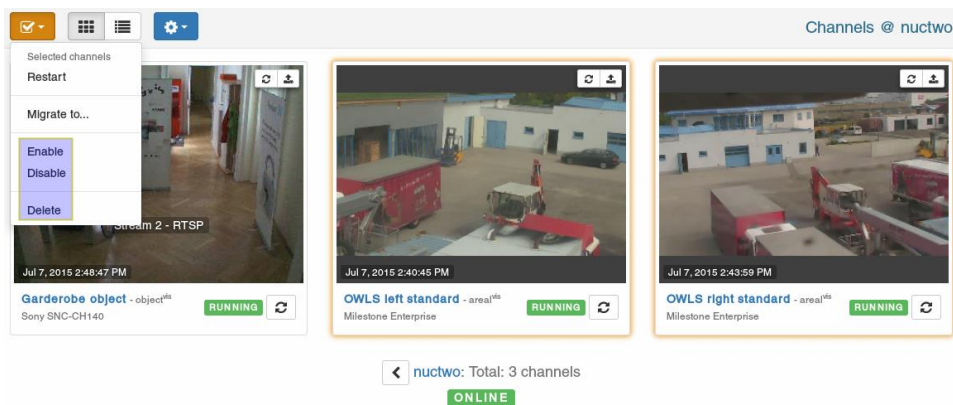
or from the node view



You then will be forwarded to the *Channel configuration* displayed in a modal window.

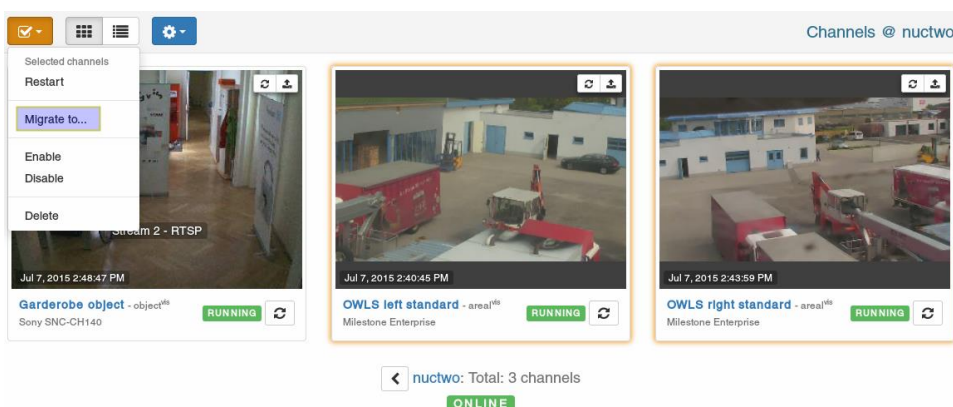
### 3.5.7 Enable / Disable / Delete a channel

Channels can be enabled, disabled or deleted. Disabling a channels stops it permanently and as a consequence it will also not send any health data anymore. Disabled channels can be spotted easily by their *disabled* status within the channel overview. Deleting a channel will remove it from the system. You can enable, disable or delete a channel by selecting it from within the *channel view* and selecting *Enable*, *Disable* or *Delete*, respectively. You can also select multiple channels to enable, disable or delete them in one go using the check-boxes at the left of each channel.



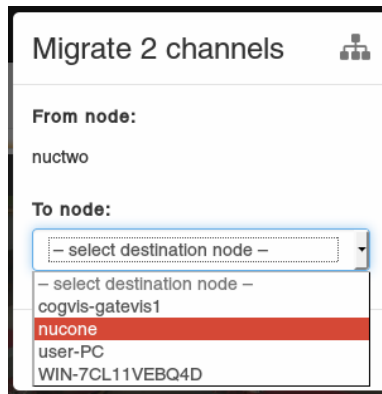
### 3.5.8 Migrate channel(s)

Channels can also be migrated from one node to another by selecting the desired channel(s) and clicking *Migrate to...* in the *select* drop-down menu.



In the now displayed modal window select the desired destination node for the channel(s) to be migrated to.





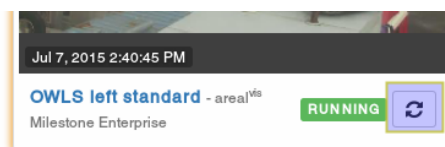
The channels will be stopped at the current node, migrated to the destination node and restarted there.

### 3.5.9 Restart channel(s)

You can restart a single channel by clicking the *Restart* icons within the channel grid/list overview.

Examples:

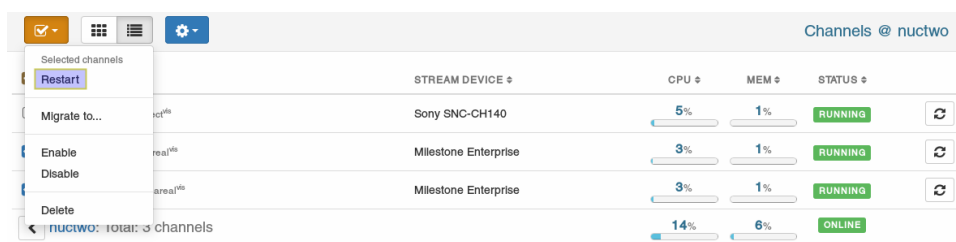
Restart using the grid overview



Restart using the list overview





To restart multiple channels select them in the channel view of the node, in either list or grid view, and choose the *Restart* option from the *Select* menu.













## 3.6 Cameras

SAIMOS VA supports video input either from a Video Management System or directly from cameras as video sources. This section describes how CCTV-cameras within your network can be detected and edited. If a camera cannot be detected automatically via ONVIF it is further explained how to add it manually.

### 3.6.1 Camera overview


The *Camera* page supports two views: grid or list view. They can be toggled using the   buttons. The grid view shows the cameras including their corresponding snapshots, which supports effectively in determining which camera faces where. For a neat overview of all installed cameras and especially if there is a larger number of them the list view might be the preferable choice. However, for both views, a click on the camera name will open the *Edit Camera* view.


#### 3.6.1.1 List View


delete selected items				add or detect cameras	Cameras
<input type="checkbox"/>	CAMERA NAME *	MODEL *	HOST *		
<input type="checkbox"/>	AXIS M1114	AXIS M1114	192.168.1.203		delete camera
<input type="checkbox"/>	AXIS M3007	AXIS M3007	192.168.1.214		
<input type="checkbox"/>	AXIS P1354	AXIS P1354	192.168.1.213		
<input type="checkbox"/>	Canon VB-S900F	Canon VB-S900F	192.168.1.240		
<input type="checkbox"/>	flir	asdf asdf	192.168.1.26		
<input type="checkbox"/>	Sony SNC-CH140 (Eingangsbereich)	Sony SNC-CH140	192.168.1.226		
<input type="checkbox"/>	Sony SNC-CH140 (Gang)	Sony SNC-CH140	192.168.1.225		

#### 3.6.1.2 Grid View

action for selection








add or detect cameras

Cameras

refresh snapshot

upload snapshot




AXIS M1114

192.168.1.203

AXIS M1114

click white space to select




AXIS M3007

192.168.1.214

AXIS M3007

click to enter camera



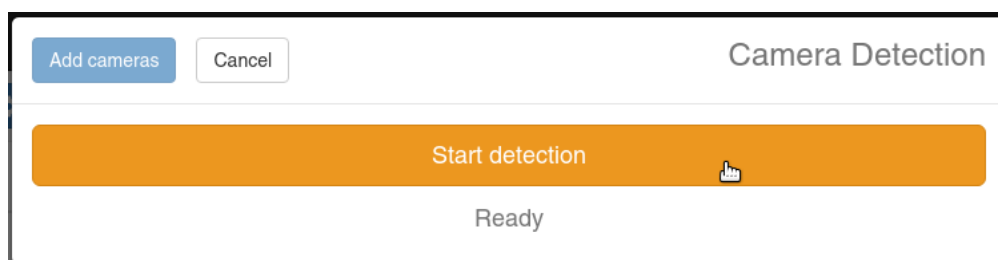
AXIS P1354

192.168.1.213

AXIS P1354

### 3.6.2 Automatic camera detection

SAIMOS VA server supports automatic camera detection. To execute it select *Detect cameras* from the *Options* button. In the separately opened view click *Start detection* to make the server automatically find cameras connected in your network.



After the SAIMOS VA server has finished searching the network for cameras, the detected cameras are listed in the window.

Cameras which have already been added to your system show with the IP address in gray instead of black and an *added* symbol next to it: ☐ 192.168.1.224 *added* .

To add one or more of the detected cameras to the system select the desired cameras using the check-boxes and press the *Add cameras* button.

**Camera Detection**

6 new cameras detected

IP ADDRESS	MODEL
<input checked="" type="checkbox"/> 192.168.1.203	AXIS M1114
<input type="checkbox"/> 192.168.1.213	AXIS P1354
<input type="checkbox"/> 192.168.1.214	AXIS M3007
<input type="checkbox"/> 192.168.1.221	Sony SNC-CH210
<input type="checkbox"/> 192.168.1.224	Sony SNC-CH220
<input type="checkbox"/> 192.168.1.240	Canon VB-S900F

3 known cameras

### 3.6.3 Add / Edit Cameras

- To add a camera manually select *Add camera* from the *Option* drop-down.
- To edit a camera select the respective camera by clicking its camera name from either the list or grid view.

For both tasks this will open the *add/edit* view for cameras.

If a camera has been auto-detected or to edit an already added camera, this view is already filled with the required parameters.

To add a camera manually all the required fields have to be filled. Furthermore, stream profiles have to be added in order to specify how to retrieve videos or snapshots from the camera.

Example for a completed camera view:

### 3.6.3.1 Stream profiles

To add or edit stream profiles use the *Options* button in the *Stream Profiles* section of the camera *add/edit* view. Here, details referring to the stream URL as well as to the video snapshot URL information for still images of the camera view can be specified or edited.

Example for the *Stream Profiles* view:

The stream profile view offers the following options:

- **Profile Name**  
Assign your profile a name for later selection
- **Streaming Protocol**  
The protocol for retrieving image data from the source:
  - **HTTP**

- **HTTPS**
- **RTSP**
- **Video File**
- **RTSP Transport**

Transport protocol to be used for the RTSP stream. Only shown when using RTSP is set as streaming protocol

  - **Auto (default)**

Choose the default setting of the camera (UDP works in most cases)
  - **TCP**

Use TCP as a transport layer. this TCP supports a more stable transport regarding package loss, though some latency as well as more bandwidth might be needed. TCP can be an alternative to UDP if a lot of interferences are experienced using auto or UDP.
  - **UDP Multicast**

Can be used in a multicast network
  - **HTTP**

Using HTTP as transport might add considerable latency and bandwidth, but it is very resistant against package loss. Use this option with caution.
- **Port**

Specifies the video streaming port (valid for HTTP, HTTPS, RTSP)
- **Path**

Specifies the path to the video file or stream. Be careful to always add a "/" at the beginning when using HTTP, HTTPS or RTSP.
- **Snapshot Protocol**
  - **HTTP**
  - **HTTPS**
  - **File**
  - **Port**

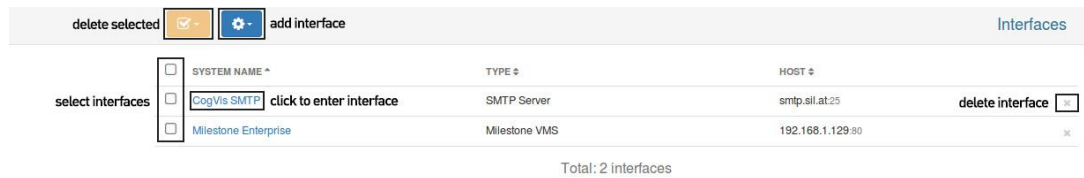
Specify the port where the snapshot can be acquired (valid for HTTP, HTTPS)
  - **Path**

Specifies the path to the snapshot file. Be careful to always add a "/" at the beginning when using HTTP or HTTPS

## 3.7 Interfaces

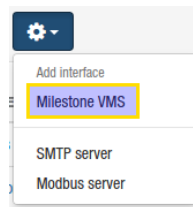
Interfaces are used for the communication with external systems, such as video management systems (VMS) or SMTP servers. All external interfaces are managed using the *Interfaces* view.

To add a new interface, select the type of interface to be selected from the *Option* drop-down.



### 3.7.1 Milestone VMS

Using the Milestone VMS interface, alerts can directly be forwarded to the Milestone system and camera streams can directly be retrieved from the Milestone image server. For image retrieval at least Milestone Express is needed. To add a Milestone Server to the system choose the Milestone VMS option in the options menu within the interface view. You can add as many Milestone Servers as you want.



In the empty Milestone interface mask fill in the information about the server. The following parameters are required for the Milestone interface:

- Name**  
 Assign a name for your Milestone interface to identify it later on.
- Host / Port**  
 Host network address and port on which the Milestone image server is listening. The default Milestone image server port is 80.
- Authentication**  
 There are two authentication options: Basic and Windows authentication. Newer Milestone XProtect systems will, though, only support Windows authentication. Note: If you use Windows authentication please make sure that the Windows user exists on the Milestone server machine and that it has at least viewing permissions within the Milestone System.
- Username**  
 Enter the username with which you want to log on to the Milestone system. If you use Windows authentication, don't forget to add the domain name followed by a backslash preceding the username (see example below).
- Password**  
 Enter the password for the user here.
- Analytics Events Port**  
 In this field the Analytics Event Port of the Milestone system has to be specified. Milestone default for the analytic function is port 9090.  
 Note: Don't forget to enable the analytics function in Milestone in order to successfully forward events.

**Edit Milestone VMS**

**Name:** Milestone Enterprise

**Host / Port:** 192.168.1.129 80

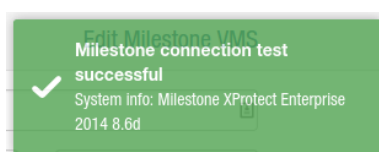
**Authentication:** Windows

**Username:** user-pc\user

**Password:** \*\*\*\*\* **Test**

**Analytics Events Port:** 9090 **Test**

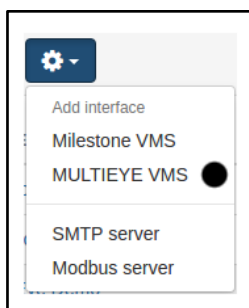
If you have entered all the data correctly you can test the connection to the Milestone server. If the test is successful a notification in the browser window similar to this one is displayed:



To complete a successful Milestone interface configuration don't forget to save before exiting.

### 3.7.2 Multieye VMS

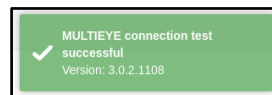
Using the MultiEye VMS interface, alerts can directly be forwarded to the MultiEye system and camera streams can directly be retrieved from the MultiEye server. To add a MultiEye Server to the system choose the MultiEye VMS option in the options menu within the interface view. You can add as many MultiEye Servers as you want.



In the empty MultiEye interface mask fill in the information about the server. The following parameters are required for the MultiEye interface:

- **Name**  
Assign a name for your MultiEye interface to identify it later on.
- **Host / Port**  
Host network address and port on which the MultiEye server is listening. The default MultiEye server port is 2840.
- **SSL**  
Check if you want to use an SSL encrypted connection.
- **Use Authentication**  
If yes, fill in the right username and password for the MultiEye server.

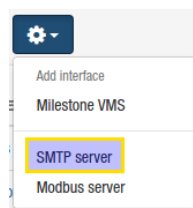
If you have entered all the data correctly you can test the connection to the MultiEye server. If the test is successful a notification in the browser window similar to this one is displayed:



To complete a successful MultiEye interface configuration don't forget to save before exiting.

### 3.7.3 SMTP Server

To send events via email at least one SMTP server has to be added to the SAIMOS VA system: Select *SMTP server* from the *Option* menu in the *Interfaces* view. You can add as many SMTP servers as you like.



This opens the SMTP server view holding a form to be filled with all necessary parameters specifying a SMTP connection. As these parameters vary for each service provider please contact your IT administrator or email service provider for the parameters for your specific SMTP. Following is a list of all possible options available within this view and an example configuration:

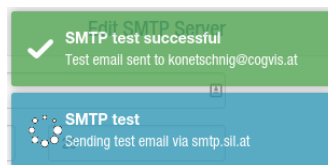
- **Name**  
Assign a name to your SMTP server configuration to identify it later on with.
- **Host / Port**  
Insert the SMTP server hostname or IP address and the port on which it is listening.
- **Connection Security**  
Select the used connection security protocol needed to connect to the SMTP server. If no connection security is required choose *None*.
  - None
  - SSL/TLS
  - StartTLS
- **Use Authentication**  
If the SMTP server requires authentication select *Yes*, otherwise *No*. For the former, in addition, the authentication username and password has to be inserted.
- **Default sender**  
Insert here the reply-to address to be used for the email events. Please make sure the email



address given here is supported by your email provider. Otherwise the emails could be blocked or classified as spam.

Once you have filled the mask with all necessary information you can send a test email to a recipient of your choice to test the SMTP functionality. To do this click the *Test* button. Enter the recipient email address for the test email in the dialog box and click *Send email*.

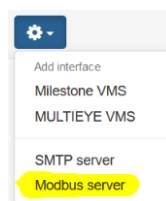
A successful test results in a notification such as the following:



Furthermore you receive an email to the address you entered before. To finish the configuration of the SMTP server correctly, please don't forget to save upon exit.

### 3.7.4 Modbus Server

To enable Modbus IP functionality for our products you can add a Modbus Server via *Add interface* → *Modbus Server*.



You should then fill out the information mask with the necessary information for the Modbus IP server.

After you have added the Modbus server successfully you can test it using the *Test* button. All products that have Modbus functionality (like Count) should have the server selectable.

## 3.8 Channel configuration

### 3.8.1 Overview and general settings

The *Edit Channel* overview holds the general channel settings as well as links to product specific settings:

Save, delete or reset a channel by selecting the respective action option from the *Save* drop-down menu. Resetting a channel will revert it to the previous configuration.

Assign a channel name to it and a node on which the channel should be executed. Changing the node will migrate the channel automatically on save to the selected node. With the *Enabled Yes/No* option the status of the channel can be toggled between enabled or disabled.

The lower sections of this view hold the product specific settings. Clicking them will open respective configuration modals, which are explained in the following sections.

Perimeter

Save

Cancel

Edit Channel

Channel Name:

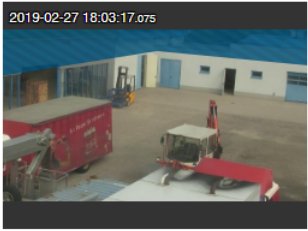
Node:

Groups:

Enabled:

No

Yes

2019-02-27 18:03:17.075


Stream Source – 320x180, Milestone-Interface (C3 Server 1)

Person Detection

Rules – intrusion - Rule 1

Alerts – Milestone

### 3.8.2 Stream Source

The stream source defines from where the analytic channel should get the video data for its analysis. Here you will find all possible options explained, followed by an example configuration for each source type.

#### 3.8.2.1 Source Type

The source type defines the type of source the images are retrieved from for the analytics. Depending on the source type the following options can vary on select. The following source types are currently available:

- IP-Camera
- Milestone
- SeeTec Plugin

The following subsections provide detailed descriptions for the options of the different source types.

##### 3.8.2.1.1 IP-Camera

When selecting the *IP Camera* option, a video stream directly received from the camera is used as video source. Select the desired camera from the *Camera* drop-down, which lists all cameras added to the system (see *SAIMOS VA Server Cameras* for more details about adding cameras to the system). The stream profile of the selected camera can be selected either by picking it from the *Profile* drop-down or by using the arrow navigators within the stream preview on the right hand-side of the stream source modal window.

##### 3.8.2.1.2 Milestone

Choosing the *Milestone* option, you can select the desired Milestone server from the *Server* drop-down list holding all Milestone servers added to the system (see *Interfaces* for more information on how to add a Milestone VMS server to the system). You can then select the desired camera from all available cameras on the Milestone server using either the *Camera* drop-down or using the arrow navigators within the stream preview on the right hand-side of the stream source modal.

#### 3.8.2.2 Resolution

Using the *Resolution* drop-down the video resolution for the analysis for the respective channel is set. The higher the resolution, the higher will be the CPU load of the particular channel. Is the resolution different compared to the resolution provided by the original stream of the camera or interface, the analysis automatically scales the input stream to the selected resolution. However, the necessary scaling also leads to higher CPU loads for the particular channel.

#### 3.8.2.3 Min./Max. Frame Rate

The fields *Min./Max. Frame Rate* allow for the definition of the minimum and maximum frame rates delivered by the stream. If the frame rate decreases below the minimum frame rate or if it delivers a higher frame rate than the maximum frame rate set, the channel writes a warning to the system log. Additionally, if the maximum frame rate is exceeded the analytics will force a fallback to the *Fallback Frame Rate* (see below). The default values for minimum/maximum frame rate are set to 8(min)/30(max) and it is the recommended setting for most systems.

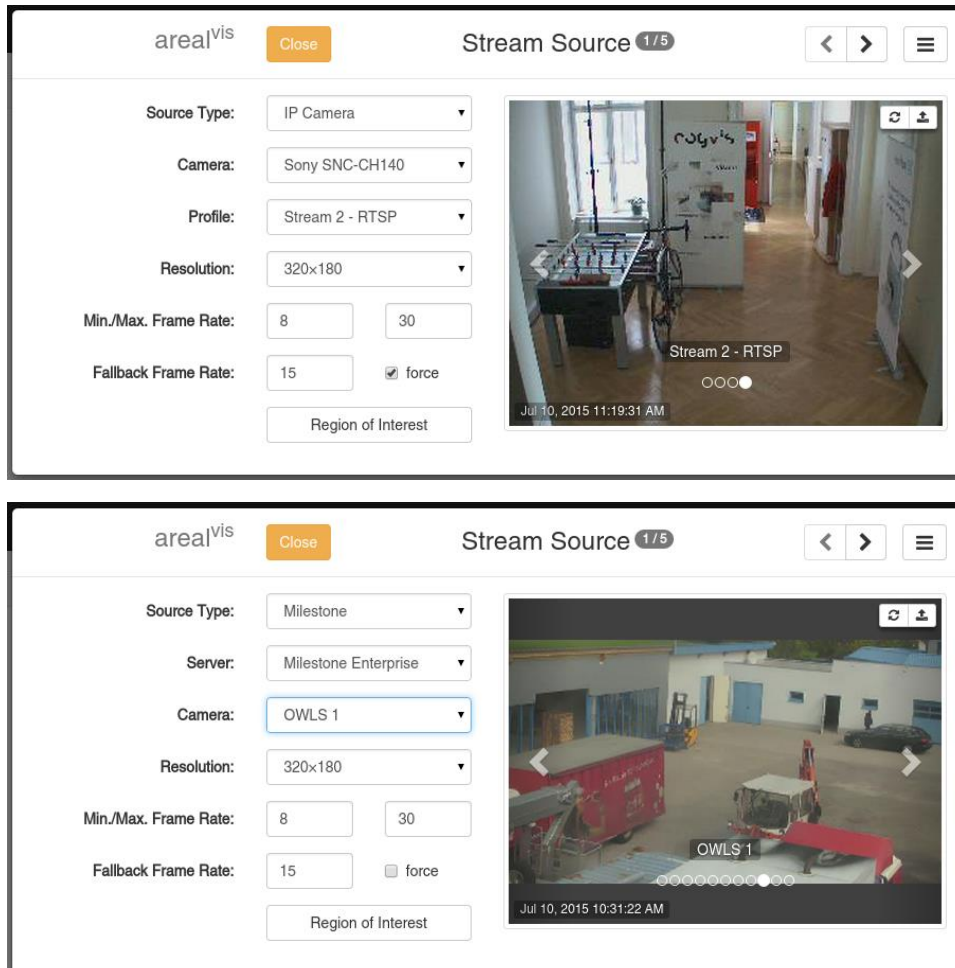
#### 3.8.2.4 Fallback Frame Rate

In case the maximum frame rate is exceeded, the analytics will set the frame rate back to the one specified in the *Fallback Frame Rate* parameter. This value should be set to the frame rate the stream is set to deliver.

## 3.8.2.4.1 Force fallback

Sometimes the system may not be able to determine the frame rate of a stream automatically or the frame rate sent by the stream is not correct. The *force* option forces the system to use only the *fallback frame rate*. For most systems it is recommended to disable the *force* option.

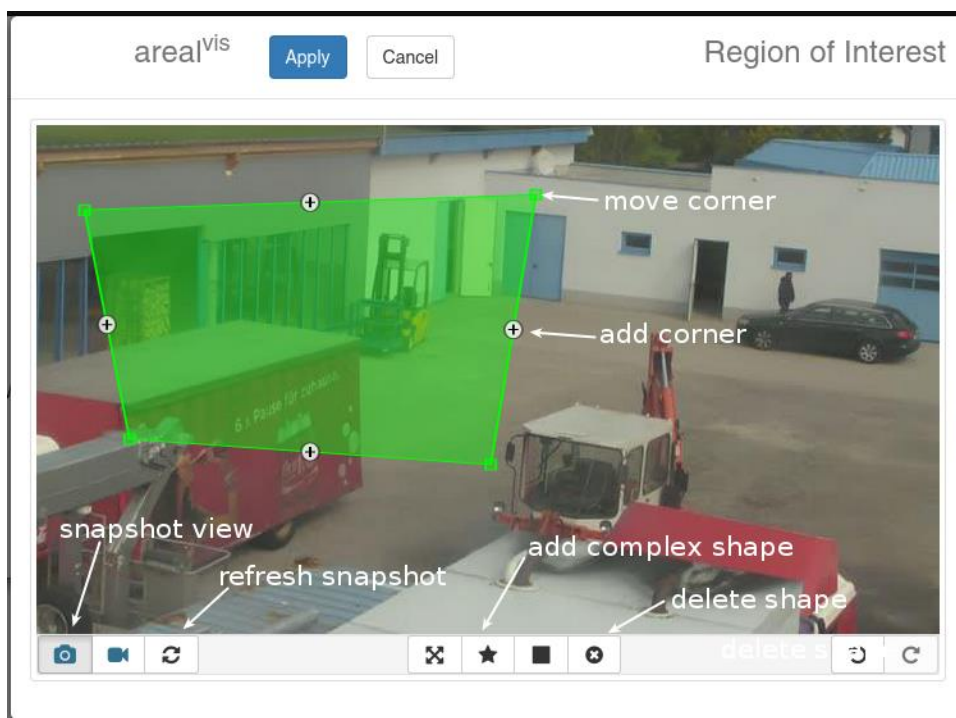
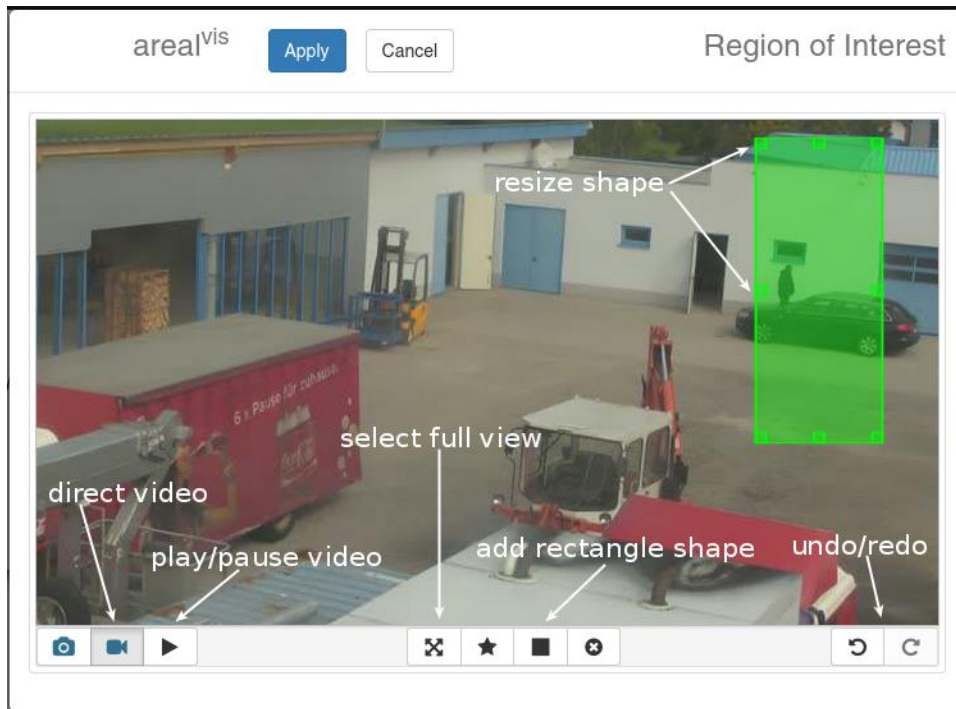
## 3.8.2.4.2 Example configurations



## 3.8.2.5 Region of Interest

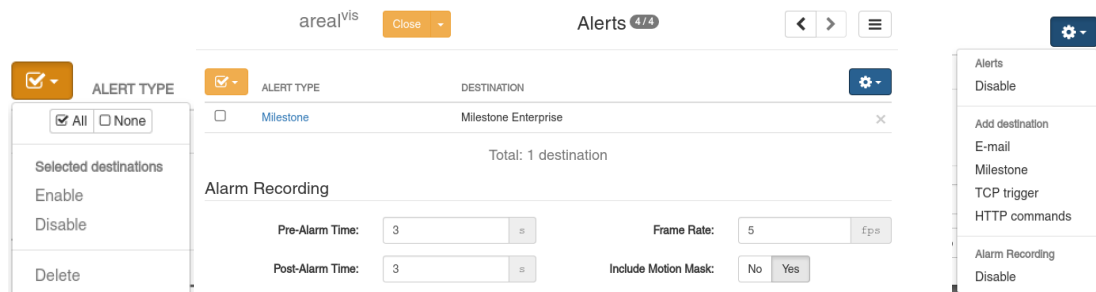
The *Region of Interest* button opens a modal window for the definition of the so-called region of interest (ROI) of the channel. The ROI specifies the regions of a scene to be taken into account for the analytics. The remaining areas in the scene are discarded for the analytics, respectively. Therefore, please be careful to include all areas within the ROI which might be relevant for the analytics.

The ROI is defined by adding one or multiple polygonal and/or rectangular shapes. Alternatively, (per default) the whole scene is set as the ROI. ROIs don't need to be overlapping. The following screenshots show possible options and interactions within the modal view.



## 3.8.3 Alerts

Alerts handle the communication of the channel with external sources. Multiple alerts per channel can be added. In case of an event triggered by the channel all configured enabled alerts will be raised. Furthermore, timeout between alerts can be set. The following subsections describes all possible alert options and their settings.



### 3.8.3.1 Alarm Recording

If alarm recording is activated, every trigger event in the Event Log has the option to view the alarm sequence of the event. Alarm recording within the event log will work regardless if an alert for the channel is active or not. You can set the *Pre- and Post-Alarm Time* in seconds as well as the *Frame Rate* for the recording. Also, there is the option to include the motion mask in the recording. When this option is enabled you will be able to see the output of the motion detector in the alarm recording.

### 3.8.3.2 E-Mail

Send an email on alert. This option requires a valid SMTP configuration as a prerequisite to send emails (see Interfaces). As recipients either users from the system can be chosen or custom email addresses can be added. Users must have a valid e-mail address configured to receive e-mail alerts. Additionally, the language of the e-mail as well as the e-mail sender can be selected (default: SMTP server settings). Here is an example configuration:

### 3.8.3.3 Milestone

Send alerts to the Milestone Analytic interface. This requires as a prerequisite a valid Milestone server configuration (see Interfaces). Select the appropriate server to send the alerts to and specify the resolution the analyzed stream has within the Milestone System. The Camera GUID or IP address has to be set manually only if the channel does not use Milestone as a stream source.

Perimeter

Apply

Cancel

Alert / Milestone

Milestone Server:

Milestone-Interface (SAIMOS)

Camera:

— auto —

Test

### 3.8.3.4 TCP-Trigger / TCP-Message

Send alerts via TCP message or trigger. Define the host and port of the TCP receiver and add the message to be sent. If no message is defined for the alert, the TCP trigger will only open and close the defined port.

areal<sup>vis</sup>

Apply

Cancel

Alert / TCP trigger

TCP Host / Port:

localhost

1234

Message:

registerthisalert

Test

### 3.8.3.5 HTTP Commands

Send sequential HTTP commands to a receiver (e. g. Network I/O). Define the host and port of the HTTP interface and add a username and password in case an authentication is required. Define one or more commands to be sent to the receiver in sequential order and set the timeout in seconds between commands.

areal<sup>vis</sup>

Apply

Cancel

Alert / HTTP commands

HTTP Host / Port:

localhost

80

Authentication:

No

Yes

Username:

theusername

Password:

\*\*\*\*\*

Commands:

/cgi.bin?trigger=1&option=1

+

-

/cgi.bin?trigger=1&option=2

+

-

Timeout:

1

s

Test

### 3.8.3.6 Test Alerts

You can test every alert by clicking on the *Test* switch and pressing *Send*. For some alerts it is important to send the correct rule name and zone therefore this can be set manually before sending.

Send Test Alert

Rule:

test\_rule

Zone:

Test Zone

Send

S

Test



## 3.8.4 Perimeter

Perimeter is a powerful and precise solution for 24/7 area security. It is specially designed for outdoor scenarios and for all weather conditions and offers robust event detection in live-video streams from standard IP, IR, thermal or embedded camera systems. Its detection accuracy and its seamless integration into VMS systems allow for an easy direct alarm forwarding to security centers.

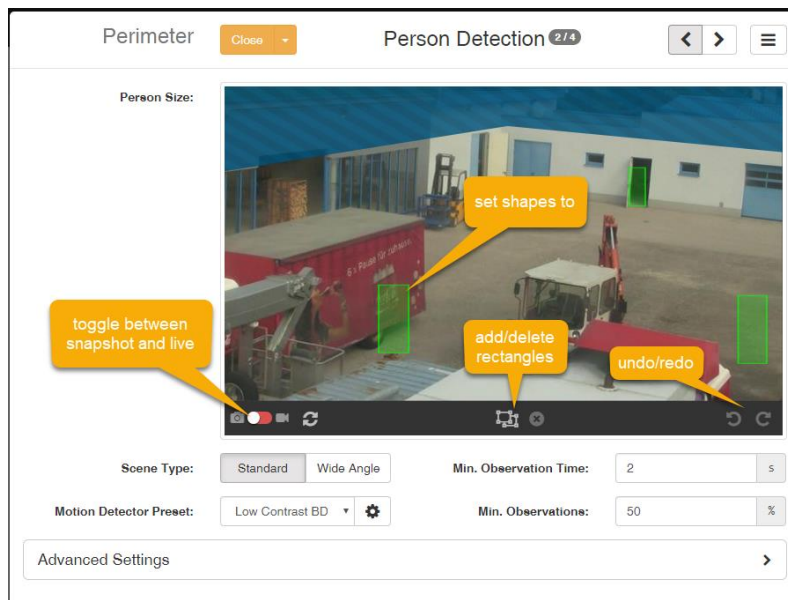
To achieve its precise object classification, Perimeter takes advantage of several years of joint research with leading European research institutes in computer vision. The solution uses a special scene model, machine learning technologies and is based on a simplified scene configuration based on as few parameters as possible.

In contrast to the general settings applicable to every channel described above, this section contains descriptions for all product-specific options and views needed to configure Perimeter.

### 3.8.4.1 Person Detection

The *Person Detection* configuration card is the center part of the Perimeter configuration handling the scene calibration and type as well as observation and motion detection settings.

Here is an example configuration:



In order to detect persons reliably the scene needs to be calibrated before its first use. This is done by placing rectangles to different positions in the camera still, whereas every rectangle refers to an average body height of a person. It needs to be adjusted in its width and height to match a person's dimensions at the specific position in the scene.

A minimum of 3 rectangles are required. They will already be added to the canvas on channel creation and have to be resized by the user according to the body heights at the specific scene positions. Still, you can add as many rectangles as you like - the more, the better, especially for uneven scenes.

For your convenience during the configuration the canvas supports *snapshot refresh* as well as a *direct video* functions. The former is available as soon as a stream source is defined. For the latter the channel has to be running.

The *Scene Type* setting specifies if you are using a standard scene (> 4 mm focal length lense) or a wide angle camera (<= 4mm focal length). Depending on this setting, different trackers will be selected to adapt to the image distortion.

### 3.8.4.1.1 Min. Observations and Min. Observation Time

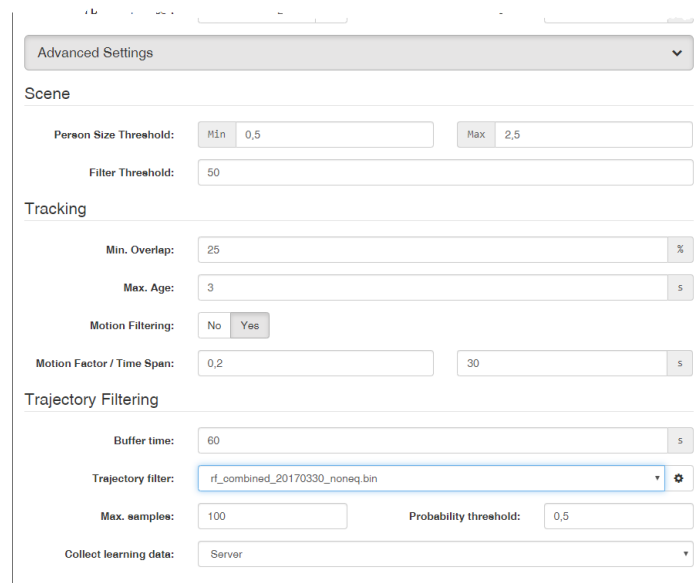
The min. observation time defines how long at least a person has to be tracked in seconds (default: 2 seconds). The min. observation defines the minimum number of required observations within the min. observation time the system has to have. (50% should be a good default value)

### 3.8.4.1.2 Motion Detection

Please see 0 for more details on Motion Detection.

### 3.8.4.1.3 Advanced Settings

*Note: the advanced settings dig deep into the tracking configuration of Perimeter. They are for expert users only and it is not recommended to change these settings by yourself. If you have problems configuring Perimeter with the standard options please do not hesitate to contact us at office@for-lan.at for support with the advanced settings. If you changed anything and the system does not work properly anymore, here is a snapshot of the default parameter values for the advanced section (Scene options do not appear when using Wide angle configuration).*



The screenshot shows the 'Advanced Settings' window with the following configuration:

- Scene:**
  - Person Size Threshold: Min 0,5, Max 2,5
  - Filter Threshold: 50
- Tracking:**
  - Min. Overlap: 25 %
  - Max. Age: 3 s
  - Motion Filtering: No (selected), Yes
  - Motion Factor / Time Span: 0,2, 30 s
- Trajectory Filtering:**
  - Buffer time: 60 s
  - Trajectory filter: rf\_combined\_20170330\_nonsq.bin
  - Max. samples: 100
  - Probability threshold: 0,5
  - Collect learning data: Server


**Scene:** Here you can change the *Person Size Threshold* and the *Filter Threshold*. The *Person Size Threshold* defines the minimum and maximum multiplier of area an object is allowed to have with respect to the configured person size to be considered valid by the tracker. So, the configuration *Person Size Threshold* min 0.5 max 2.5 and *Filter Threshold* 50 means: An object has to be within the boundaries of 0.5 – 2.5 the configured area of *Person Size* for at least half of all observations of a track to be considered a valid observation.


**Tracking:** The *Match Threshold* option tells the tracker how much distance between two consecutive bounding boxes is allowed (in %) to be considered within the same track (100% means maximum distance, 0% means 100% overlap). The *Max. Age* option tells the tracker how long the time between two observations can be at max.

If you have *Motion Filtering* enabled, the object observed has to move by a certain *Motion Factor* within a defined *Time span*. The *Motion Factor* is the dx/dy distance in pixel relative to width plus height from the first to the last observation within *Time Span*. For example, an object with size 10x5 pixels has to move at least 4.5 pixels within the last 30 seconds to be considered as valid, if the *Motion Factor* is 0.3 and the *Time Span* is 30sec.

**Trajectory Filtering and collecting learning data:** this section handles the learning and post event filtering of Perimeter. It uses random forests to optimize false positives filtering. If you want to know more about how our filtering works please contact office@for-lan.at.

The *Buffer time* tells the system how long to buffer individual tracks for learning. 60 seconds should be sufficient here. You can use the provided random forest files from SAIMOS to activate the trajectory filtering by selecting them from the drop-down list:

If you don't have any random forest files uploaded yet you can get to the upload model by using the  button on the right of the drop-down field. You will then be presented with the trajectory modal.

You can upload files by selecting *Upload random forest file* using the  drop-down button. The random forest file will appear in the list then and you can select it in the advanced configuration.

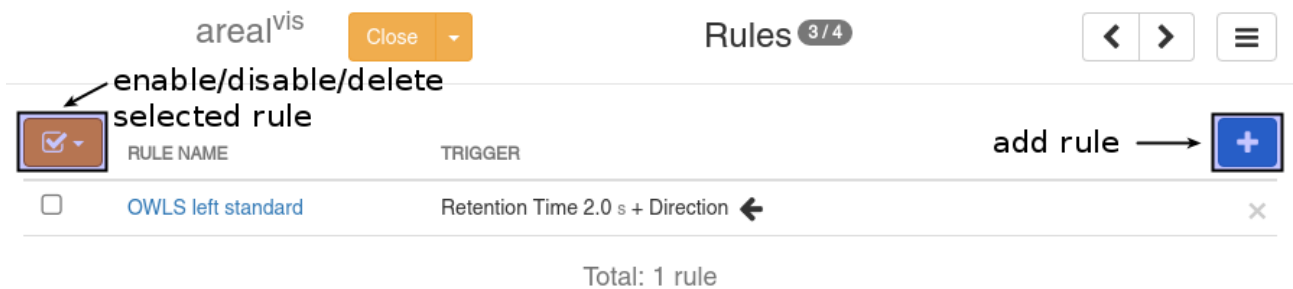
If you don't have the standard SAIMOS random forest files please contact [office@for-lan.at](mailto:office@for-lan.at).

## Collect learning data

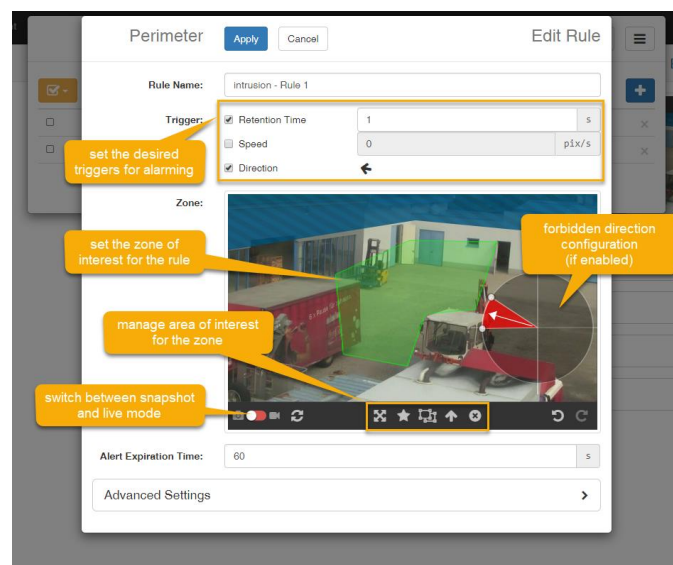
To get your own personal random forest file or if you want to help SAIMOS with the collection of learning data you can activate the learning mode by selecting where you want to store your learning data. You can either choose *Server* or *Node* from the drop-down menu. When you choose *Server* all data will be managed by the server and can be downloaded by using the *Server Administration*. When choosing *Node* learning data will be stored on the node on which the channel is run. You can choose a folder where to store the data or use our default directory. If you want to know more about learning for your installation please contact [office@for-lan.at](mailto:office@for-lan.at).

### 3.8.4.2 Rules

Rules are the central element of a Perimeter channel. Without a rule there are no alerts. You can create as many rules as you like for one channel. If a rule is validated by the analytic engine an event is triggered which will be forwarded as an alert, if configured. A full validation of the rule means that every trigger within the rule for the set zone has to be satisfied. Every rule acts independently from the other rules and has its own timeout (*Alert Expiration Time*). Every newly created channel will start with one active rule.



To edit a rule configuration, click its name from within the rule overview. In the additional modal window, a rule name can be assigned to the rule; rules can be defined, edited, enabled or disabled and the region of interest for these rules can be defined here as well. These topics are explained in the following subsections.



### 3.8.4.2.1 Event Triggers

Currently the following three event triggers are available:

- Retention Time**  
 Number of seconds a person is allowed to stay within the region of interest before an alert is triggered.
- Max. Speed**  
 How fast is a person allowed to move within the region of interest (pixels per second); if the speed is exceeded an alert is triggered.

### Forbidden Direction



Which directions persons are not allowed to move to within the region of interest. The prohibited directions are represented by two angles. A person moving in the direction which lies in between which a trajectory of a person will raise an alarm. The arrow shown within the direction angles represents the principle direction between these two angles. You can add as many such directions as you want.

### 3.8.4.2.2 Zone

The region of interest can consist of one or multiple polygon-shaped areas at any position within the scene. The shapes can, but don't have to, overlap. As a default upon creation of a rule the whole scene

is selected as a region/area of interest. Whenever a person enters the region of interest, the system analyzes for fulfilled/unfulfilled triggers and raises events accordingly. If the forbidden direction rule is activated also directions can be added to the region of interest window. All event triggers are combined in the rule using an AND operation. Hence, whenever a person enters the region of interest the system analyzes the scene for the activated event triggers and it raises alerts only when ALL activated event triggers are triggered.

#### 3.8.4.2.3 Alert Expiration Time

The Alert Expiration Time defines the minimum time span between rule events. If an event is triggered by the rule no other event will be sent by the system for the given time.

#### 3.8.4.2.4 Milestone Rule

If you use Milestone VMS as an alert receiver you can define the Milestone rule name for every rule separately. If you don't change anything the rule name will always be *intrusion*. This rule name can then be added as Analytics Event in Milestone. If an Alert for Milestone is defined for this channel the Analytics Event will be forwarded to the Milestone System.

## 3.8.5 Count

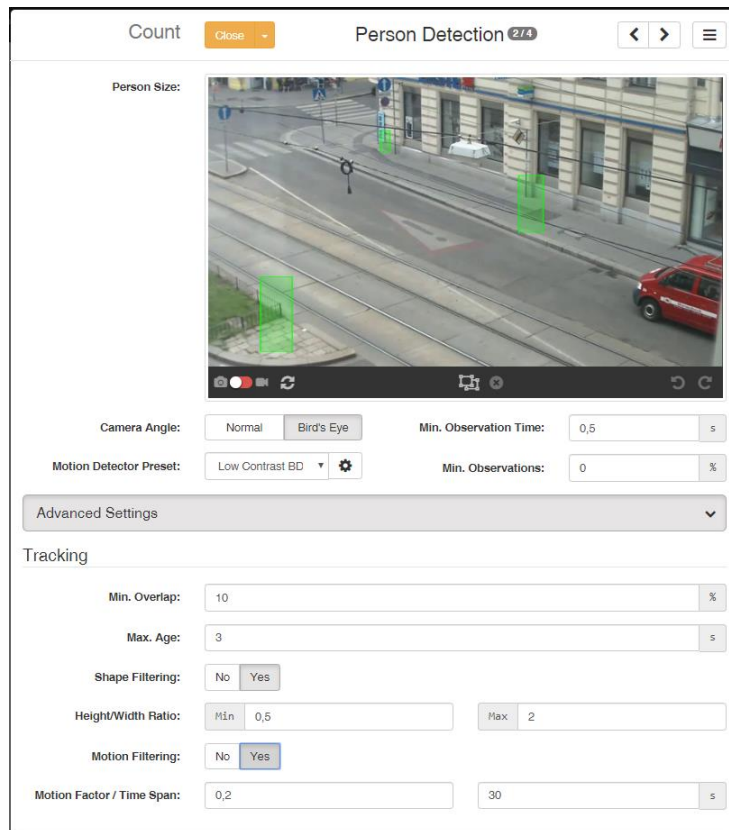
Effective marketing, staff management and customer experience optimization require – especially in retail and gastronomy – knowledge and awareness of customer behavior. Based on comprehensive state-of-the-art real-time video analytics functionalities SAIMOS® Count delivers quantitative results.

Count stands for the reliable and accurate counting of people entering or leaving user-defined regions within the video image its visualization using user-friendly real-time statistics including variable filter and export options. Heatmaps make patterns of movements, hot spots, or areas with potential for marketing-related improvements visible at a glance. The occupancy monitoring feature calculates the number of people in a certain region and displays them in real-time. This makes Count also an excellent solution as a guiding system.

This section contains all Count-specific settings and views for its configuration.

### 3.8.5.1 Person Detection

The Person Detection configuration card is the center of Count configuration. Here you will have to tell the system how big persons are within the surveilled scene. Here is an example configuration:



Count Close Person Detection 2/4 < > ≡

Person Size:

Camera Angle: Normal Bird's Eye Min. Observation Time:  s

Motion Detector Preset: Low Contrast BD ⚙️ Min. Observations:  %

Advanced Settings ▼

Tracking

Min. Overlap:  %

Max. Age:  s

Shape Filtering: No Yes

Height/Width Ratio: Min  Max

Motion Filtering: No Yes

Motion Factor / Time Span:   s

### 3.8.5.2 Person Size

Define the approximate sizes for the objects you want to track here (doesn't have to be persons per se). You have to define 3 rectangles. The tracker will then define the minimum and maximum tracking size from these 3 rectangles. The Count tracker works by minimum and maximum area of an object so you don't have to (but you can) define more than 3 rectangles.

### 3.8.5.3 Camera Angle

Here you should define if your camera angle is a normal CCTV angle (Normal) or more or less an overhead view (Bird's Eye). If you choose Normal the tracker will track objects using the lower middle

point of the bounding rectangle. With Bird's Eye view chosen the tracker will track by the center point of the object.

### 3.8.5.4 Motion Detection

Here you can change the motion detector parameters. We recommend using the Groove or Groove Color motion detector for tracking. For more information about the motion detectors please refer to the Motion Detectors section at the end of this chapter.


### 3.8.5.5 Min. Observation Time

Define the maximum observation time a track should have at least to be considered a valid track here.



### 3.8.5.6 Min. Observations



Define the minimum amount of tracker hits in percent within the given observation time here.

### 3.8.5.7 Advanced Settings

Advanced Settings 



Tracking



Min. Overlap:    %

Max. Age:    s

Shape Filtering:



Height/Width Ratio: 



Min   

Max   

Motion Filtering:

Motion Factor / Time Span: 

  s

#### 3.8.5.7.1 Tracking

- **Min. Overlap**

The Min. Overlap option tells the tracker how much distance between two consecutive bounding boxes is allowed in percent to be considered within the same track (100 % means maximum distance, 0 % means 100 % overlap).

- **Max. Age**

The Max. Age options tells the tracker how long the time between two observations can be at max.

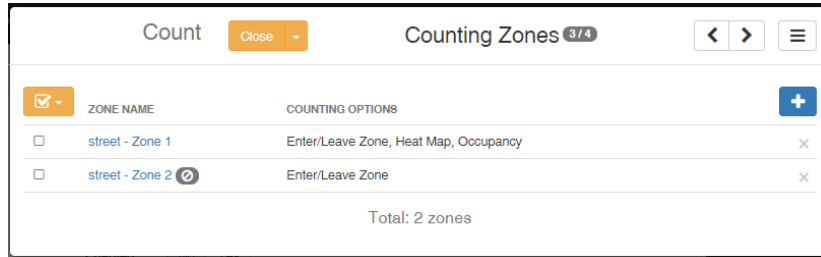
- **Shape Filtering**

If the shape filtering option is enabled, the track will be analyzed for height to width ratio. Only bounding boxes with the right height to width ratio will be considered for a valid track.

- **Motion Filtering**


If you have Motion Filtering enabled, the object observed has to move by a certain Motion Factor within a defined Time span. The Motion Factor is the dx/dy distance in pixel relative to width plus height from the first to the last observation within *Time Span*. For example, an object with size 10x5 pixels has to move at least 4.5 pixels within the last 30 seconds to be considered as valid, if the *Motion Factor* is 0.3 and the *Time Span* is 30sec.

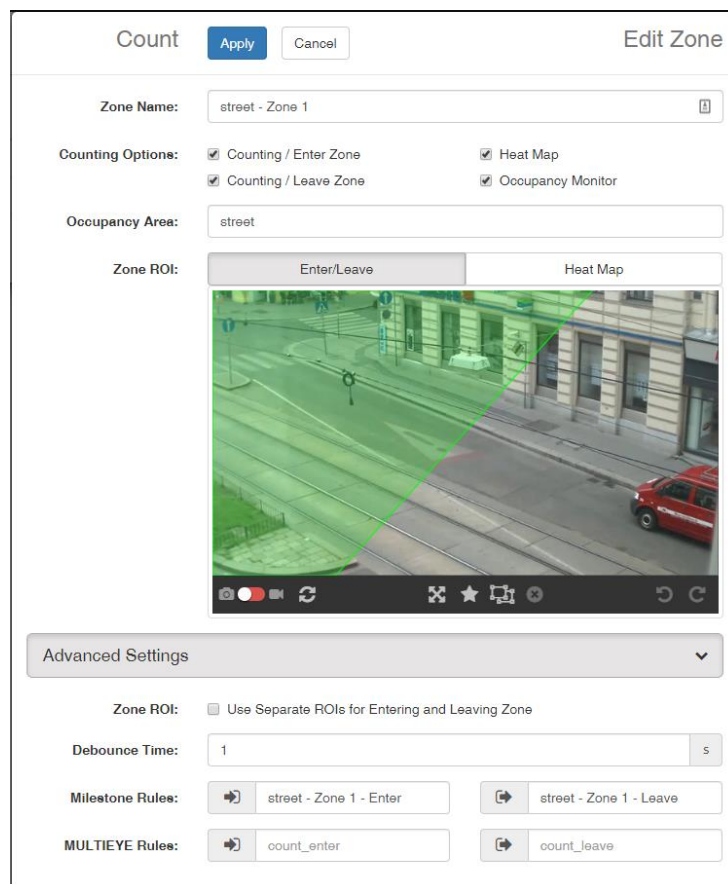
## 3.8.5.8 Counting Zones



Counting zones will tell the tracker where to count. You can create as many counting zones per channel as you want but most of the time one or two zones will suffice. You can add zones by clicking the



button. Zones can be enabled/disabled or deleted by selecting them and using the  menu button. By clicking on the zone name, you can edit the zone. Here you can see the edit view and in the following sections will explain all the options:



### 3.8.5.8.1 Standard settings

- **Zone Name**  
Give your zone a meaningful name. The name will be the identification for the counting statistics.
- **Counting Options**  
You can activate/deactivate different options here. If an option is not selected it will not be available for data analysis
  - Counting / Enter Zone  
Count when objects enter the defined zone (ROI)
  - Counting / Leave Zone  
Count when objects leave the defined zone (ROI)



- Heatmap  
Add heatmapping data from the defined heatmapping ROI of the zone.
- Occupancy Monitor  
Monitors the occupancy of the zone for a certain occupancy area (the area has to be defined in the Occupancy Area option)
- **Occupancy Area**  
Define the occupancy area. Type a meaningful name for the area as it will be represented in the occupancy view with this name later (default is the Zone Name). All zones with the same occupancy area name will be joint together within the occupancy area. Start typing in the field to view already existing areas.
- **Zone ROI**  
Here you can define the zone ROI for the Enter/Leave counting zones and the Heatmap. If *Use Separate ROIs for Entering and Leaving Zone* within the advanced settings is enabled there will be the possibility to define a separate zone for Enter and Leave.

#### 3.8.5.8.2 [Advanced settings](#)

- **Zone ROI**  
Select *Use Separate ROIs for Entering and Leaving Zone* if you want to define separate ROI zones for Enter and Leave zones.
- **Debounce Time**  
Timeout between object in and out count for the zone. The tracker will only count the same object in one direction, if there was no count in the other direction within Debounce Time.
- **Rule Type**  
Here you can define custom rule names for count\_in and count\_out if you want to send counts as alerts to other systems (e. g. Milestone).

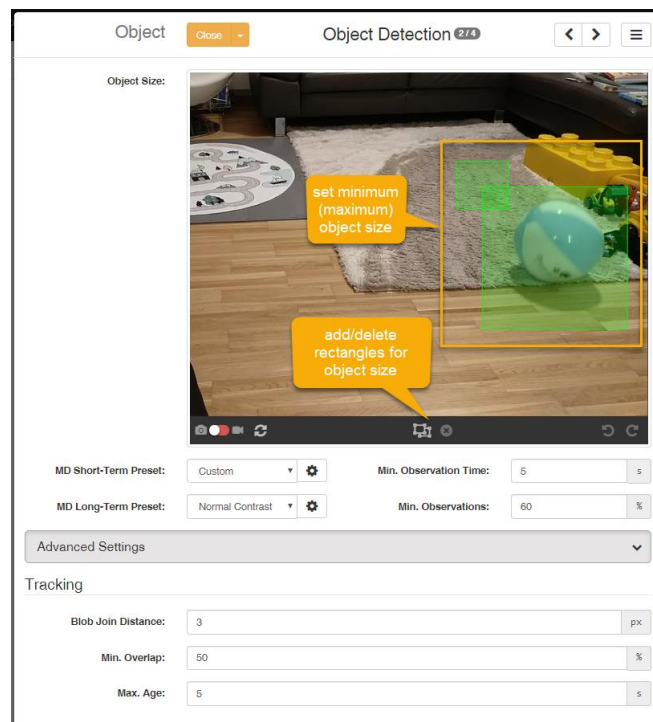
## 3.8.6 Object

Object is a highly accurate left-object detection video analysis optimized for indoor applications. It detects objects which have been left in or taken from the scene.

This section includes descriptions for the Object specific settings.

To setup Object the minimum size of the objects to be detected has to be defined. This is done by adjusting the size of the green rectangle object marker in the *Min. Object Size* canvas. Additionally, the distance between neighboring blobs until they are joined together can be specified in pixels (*Blob Join Distance*).

Finally, the long-term and short-term motion detectors have to be configured (see *Motion Detector* section).



### 3.8.6.1 Object parameters

- **Object Size**  
Defines the minimum size an object has to have to be considered
- **Motion Detection**  
Settings for the short-term and long-term motion detector. The short-term motion detector should refresh fast, the long-term motion detector should refresh very slow. See the section Motion Detector (below) to get more information on the motion detector settings.
- **Min. Observation Time**  
The minimum amount of time in seconds an object must be tracked before an alarm is considered.
- **Min. Observations**  
The minimum amount of tracker hits in percent within the given observation time.
- **Tracking**
  - **Blob Join Distance**  
The maximum distance between two objects that leads to a join within the tracker.

- **Min. Overlap**

The *Min. Overlap* tells the tracker how much distance between two consecutive bounding boxes is allowed in percent to be considered within the same track (100% means maximum distance, 0% means 100% overlap).

- **Max. Age**

The *Max. Age* option tells the tracker how long the time between two observations can be at maximum.

### 3.8.7 Scrambler

Surveilling security-critical areas while still protecting privacy – SAIMOS® Scrambler makes it possible by offering consistent and reliable privacy protection for persons, vehicles, and critical areas under surveillance. SAIMOS® Scrambler is your choice to protect privacy in public areas and facilities, in semi-public zones in companies or in locations where conventional video surveillance is prohibited.

The video analytics core detects motion and pixilates moving persons, vehicles and objects in outdoor- or indoor environments. It automatically pixilates these areas in real-time using a selected window-size defining the dimensions of the resulting color-homogeneous areas. In addition, users can define static areas, which are permanently scrambled using the same window-size settings and based on drawing polygons. During the anonymization process, the scrambled areas are destroyed irreversibly, so that a reconstruction of the original data from the pixilated video is impossible. Access to the original video data is only possible, if the video had been recorded previously using a video management system and by following the two-person rule. Hence, Scrambler allows for the detection of security-critical events at a glance from the anonymized video while consistently protecting privacy.

This section contains all Scrambler-specific settings and views for its configuration.

#### 3.8.7.1 Scrambling

The Scrambling modal window holds all Scrambler specific configuration parameters.

- **Static Scrambling:**

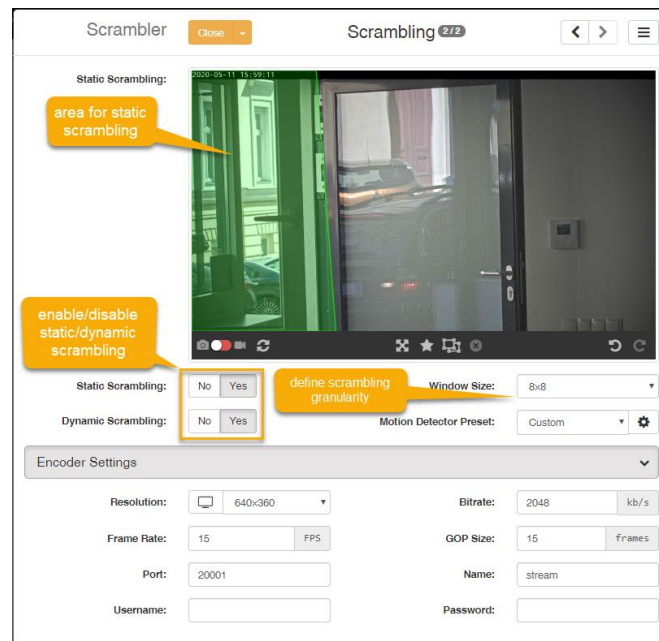
In addition to motion-based scrambling, Scrambler also supports a permanent scrambling of user-defined areas in the video image. These areas can be defined by drawing (multiple, also non-connecting or overlapping) polygons in the camera still / live-video view.

- **Motion Detection:**

Select the motion detector here to be used for the anonymization. For details on the supported motion detectors and each of their applications, advantages and disadvantages, please refer to the Motion Detector section below.

- **Window Size:**

The Window Size specifies the dimensions of grid, in which the areas are divided for the scrambling. For example, 16x16 means that the area to be scrambled is divided into small windows of 16 pixels width and 16 pixels height each. For these areas the respective average color value is calculated and the color of all pixels within it is replaced by the average color. As a consequence, the smaller the window size is, the more and finer details are recognizable and, respectively, the bigger the window size is, the bigger the scrambled areas will appear.



### 3.8.7.2 Encoder Settings

**Resolution:** resolution of the scrambled stream

**Bitrate:** bitrate of the scrambled stream. The higher the bitrate is set, the better will the quality be at high network performance.

**Framerate:** Number of images per second of the scrambled stream. The value set here should be the same as the image rate of the original stream.

**GOP Size:** Specifies the interval of key images. This setting should be set to 1 per default. The maximum possible value is the image rate of the stream.

**Port:** Defines at which port the scrambled stream should be available. This results then in a stream URL structured as *rtsp://{IP}:{PORT}/{Name of the Stream}*

**Name:** name assigned to the stream. This parameter is used for the stream name (see example in "Port"), therefore changing the stream name will also result in a different stream URL.

**Username:** username for stream authentication; leave empty to disable user authentication

**Password:** password for stream authentication; leave empty to disable user authentication

### 3.8.8 Motion Detectors

Some products use motion detectors for the video analysis. It is important to customize the motion detector parameters with respect to the current scene of the channel to optimize the analytics performance. The next subsections go through all motion detectors implemented in SAIMOS VA and explains their settings.

The motion detector modal looks the same for every product channel using it. All motion detectors come with a *direct play* option to directly compare the input images for the motion detector with its raw output images. To start direct play the channel has to be running. Everything that is shown white in the motion detector direct play window is foreground.

Also, every motion detector is equipped with the same post-processing options for erosion (makes objects thinner, i.e. removes pixels from the blob boundaries and small noise speckles) and dilation (thickens objects, i.e. adds pixels to blob boundaries). If you use erosion and dilation at the same time this will result in an opening (erosion followed by dilation) which will make your motion image have less speckles (lots of small dots in the image) while preserving big blobs. While these two options can be very handy if you have a bad motion image, they can also seriously affect the effectiveness of the analysis. So, use this option with caution and only if you know what you are doing.

#### 3.8.8.1 Presets

Motion detector presets should help you to get started fast with the right motion detector settings. Currently the following motion detector presets are available:

- Gray
  - High Contrast
  - Normal Contrast
  - Low Contrast
  - Low Contrast BD
- Color
  - High Contrast
  - Normal Contrast
  - Low Contrast
  - Low Contrast BD
- Custom

You should select Gray presets for scenes where night vision cameras or thermal cameras are used. Color presets are best used for day and indoor scenarios where color is present in the image 24/7. If you change the settings of a preset your changes will be saved automatically as a custom preset.

#### 3.8.8.2 Groove

The *Groove* motion detector (MD) is a sample-based motion detector using samples and randomization to determine if a pixel belongs to background or foreground. It is high-performing and currently the standard motion detector used by SAIMOS.

Parameters for *Groove MD*:

- **Threshold**

The Threshold determines how severe a change in contrast or color has to in order to be classified as foreground compared to the current background. The lower this option the more motion visible within the image. For scenes with low contrast, the value should be very low (< 20). For indoor scenes with very good contrast and light, higher values (> 20) may be set. You can change the threshold for both color and gray-value separately, but it is not recommended unless you are an image processing expert user.

- **Number of Samples**

Defines the number of samples a pixel should use to compare itself to its neighbors. Note: Changing this option might have significant impact to the MD performance and for most scenarios the default value should be the optimum.

- **Min. Background Samples**

Specifies the number of samples minimally used for the background. Note: Changing this option might have significant impact to the MD performance and for most scenarios the default value should be the optimum.

- **Replace Chance**

This option determines how soon a single pixel should be taken as background. The higher this option (100 is max, 0 is min) the longer it will take for a still object classified as foreground to be classified as background again. The lower this value, the faster the motion detector will adapt to changing conditions within the image, but the shorter an object will appear as foreground.

Motion Detector

Preset: Low Contrast BD

Type: Groove Gray

Threshold: 16

Replace Chance: 5

Blindness Detection

Active: No Yes

Send Alert After: 20 s

Min. Area in Motion: 90 %

Min. Rain/Snow Motion: 8 %

Reinitialize After: 10 s

Post-processing

Erosion: disabled

Dilation: disabled

Advanced Settings

Motion Detector

Number of Samples: 12

Min. Background Samples: 4

Blindness Detection

Decision History Size: 9

Max. Re-init Attempts: 3

Within Time Frame of: 30 s

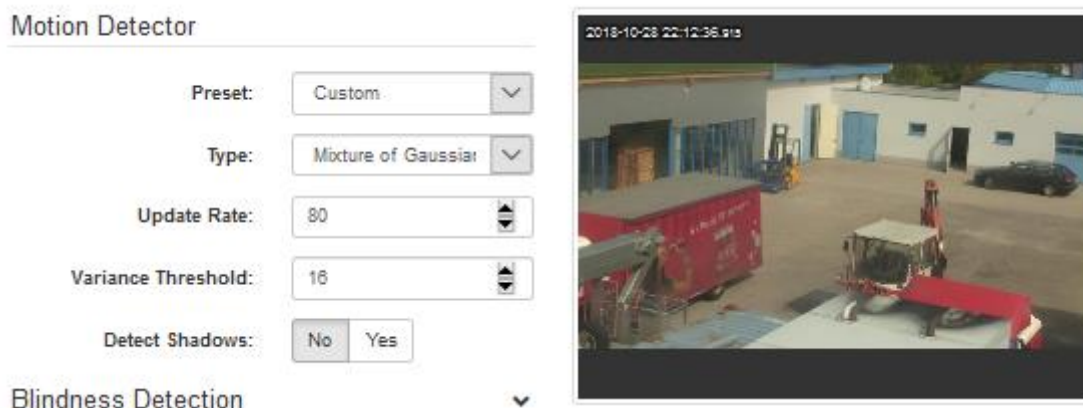


### 3.8.8.3 Mixture of Gaussians

The *Mixture of Gaussians* motion detector (MD) uses a Gaussian Mixture Model to model foreground and background for every pixel. It is not as high-performing and controllable as the *Groove* MD but performs very well in outdoor perimeter setups with changing conditions. It was used before Groove was introduced.

Options for the Mixture of Gaussians MD:

- Update Rate**  
 Specifies for the motion detector how long it should keep pixel values in the history for model generation. The lower this value, the more influences of the environment (changing backgrounds) can be accounted for, but the longer it will take to build the background model itself. Normally 80 frames are sufficient to build a good model.
- Max. Gaussian Mixtures**  
 This option defines the maximum number of Gaussian Mixtures to be used. The more mixtures possible, the more environmental change can be modeled. For standard scenarios the value will be around 5-7.
- Variance Threshold**  
 The Variance Threshold influences how prone the motion detector be should be to changes. The lower this value, the more motion will appear within the motion image. For low contrast scenarios a value below 20 can improve the motion detection. For indoor scenarios this value can be above 20.
- Detect Shadows**  
 This value toggles between whether the motion detector should try to eliminate shadows and highlights from the motion image or not. Note, that enabling this option will result in a more fragmented motion image. Use this option with caution.



### 3.8.8.4 Blindness Detection

Blindness detection allows the motion detector to adapt to strong changes within the environment (rain/snow or lights on/off) or total blindness. The motion detector will reset or stop analyzing as it detects such changes.

#### Parameters

- Send Alert After**  
 Determines the seconds of blindness to happen until an event is triggered.



- **Min. Area in Motion**  
Sets the minimum size of the area relative to the image size that has to be accounted for motion to trigger blindness.
- **Min. Rain/Snow Motion**  
Sets the relative amount of motion pixels that have to be active to trigger snow/rain blindness
- **Decision History Size**  
Size of the decision history event stack
- **Reinitialize After**  
Defines the time in seconds to wait before a re-initialization will occur within the time set in *Within Time Frame of*
- **Within Time Frame of**  
Sets the amount of time in seconds for the *Max. Re-init Attempts* option

#### 3.8.8.5 *Milestone Analytic Event Names*

To connect Blindness Alerts to the Milestone system, create the following Analytic Events and connect them to Alerts within Milestone:

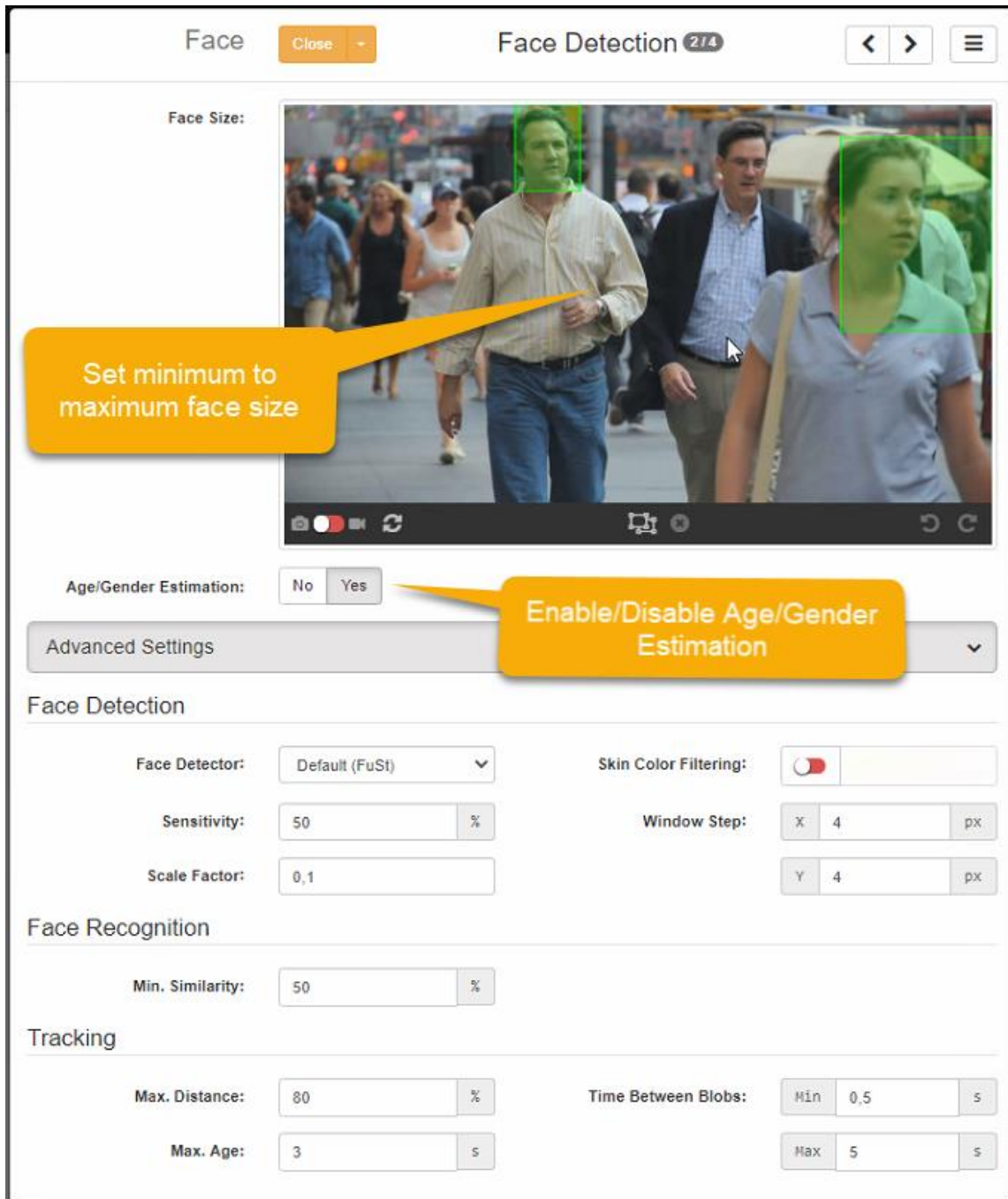
- md\_blind
- md\_recovered
- md\_reinit

## 3.8.9 Face

SAIMOS Face Analytics Pro uses state of the art AI systems to detect, recognize and compare faces. The user-friendly interface provides step by step configuration enabling fast setup times and reporting. The Face Pro use case specializes on Black-/Whitelist real time alerting and flexible reporting of detected and recognized faces for investigation as well as forensic analysis.

### 3.8.9.1 Face Detection

The Face Detection modal will enable you to configure Face for optimal performance and results.



The screenshot displays the 'Face Detection' configuration window. At the top, there's a 'Face' tab and a 'Close' button. The main video feed shows two faces with green bounding boxes. Below the video, there's a 'Face Size' section with a callout box saying 'Set minimum to maximum face size'. To the right, there's an 'Age/Gender Estimation' section with 'No' and 'Yes' buttons, and a callout box saying 'Enable/Disable Age/Gender Estimation'. Below these are 'Advanced Settings' and 'Face Detection' sections. The 'Face Detection' section includes 'Face Detector' (Default (FuSt)), 'Sensitivity' (50%), 'Scale Factor' (0,1), 'Skin Color Filtering' (toggle), and 'Window Step' (X: 4, Y: 4). The 'Face Recognition' section includes 'Min. Similarity' (50%). The 'Tracking' section includes 'Max. Distance' (80%), 'Max. Age' (3s), and 'Time Between Blobs' (Min: 0,5s, Max: 5s).

#### 3.8.9.1.1 Face Size

Setting the face sizes is very easy just set at least two boxes for the minimal and maximal face size. The more the two sizes (min, max) differ the more performance the algorithm will need. That said, the minimal face size is more important than the maximum face size.

## 3.8.9.1.2 Age/Gender Estimation

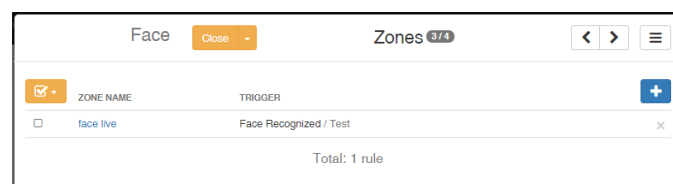
If Age/Gender Estimation is enabled each face detection will be analyzed for age and gender and respective outputs of this analysis can be found within the face log as well as the statistics engine. Detection of Age/Gender will use more resources than standard face detection.

## 3.8.9.1.3 Advanced Settings

- **Face Detection**
  - **Face Detector**  
Sets the face detector engine to be used. If not otherwise informed by SAIMOS do not deviate from the default as it might lead to less overall algorithmic performance.
  - **Skin Color Filtering**  
Do not activate unless the false positive rate is too high or recommended by SAIMOS. Do not activate this option for the default detector.
  - **Sensitivity**  
Sets the sensitivity of the face detection. High values will lead to more faces detected but a higher false positive rate. Lower values will lead to less faces detected and also lower the false positive rate.
  - **Scale Factor**  
The scale factor will set the scaling pyramid size of the convolutional system. It is scaled between 0 – 1 and higher values will lead to increased performance needs but might enable the system to find smaller faces.
  - **Window Step**  
This option will set the granularity of the face search. Higher values will improve the performance but might lead to a less amount of detected faces due to higher pixel jumps for the search.
- **Face Recognition**
  - **Min. Similarity**  
Will set the minimal similarity that is needed for the system to achieve a successful match. Lower values will lead to higher false positive rates.
- **Tracking**
  - **Max. Distance**  
Sets the maximum distance between two consecutive face detections to be still considered the same face.
  - **Max. Age**  
Sets the maximum age of a track
  - **Time Between Blobs**  
Sets the minimum and maximum time between reported face observations.

## 3.8.9.2 Zones

Multiple Face Zones can be created per channel. Each zone can have an independent setting and alarm time out as well as Face Lists assignments.



The screenshot shows the 'Face' configuration window with the following elements:

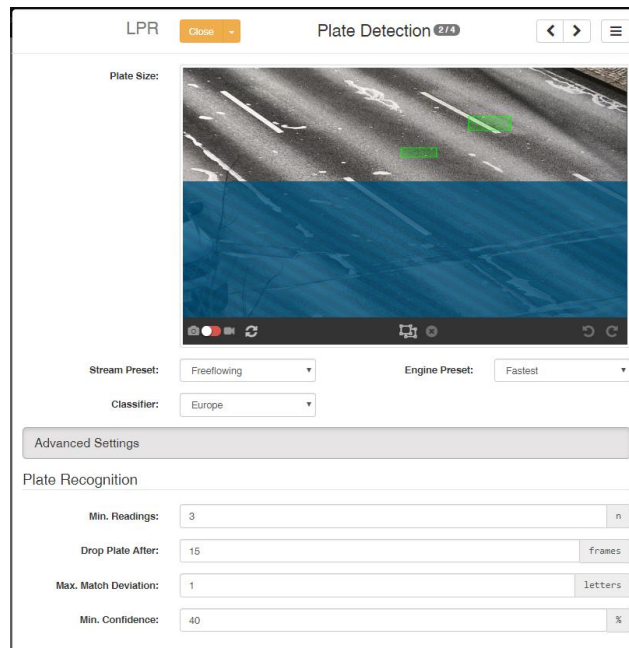
- Zone Name:** A text field containing 'face live'.
- Trigger:** Two radio buttons: 'Face Detected' and 'Face Recognized' (selected).
- Face Lists:** A dropdown menu showing 'Test'.
- Zone ROI:** A video feed showing a person at a desk, with a green bounding box around the person.
- Alert Expiration Time:** A text field containing '60' and a unit selector set to 's'.
- Advanced Settings:** A button with a right-pointing arrow.

1. **Trigger**  
The trigger defines if an event should be triggered on mere detection or on recognition. If recognition is chosen the Face Lists option (2) will appear.
2. **Face Lists**  
If the recognition option is chosen the associated face lists for this recognition channel can be chosen from a drop-down list. To have Face Lists option you first have to create a face list (see 3.15.3).
3. **The zone ROI** will define the region where faces should be reported. Only faces within this region will be considered.
4. **The Alert Expiration Time** will set the time between face events (Recognition or Detection likewise)
5. **The Advanced options** will handle the messages for 3<sup>rd</sup> party rule propagation (like the Milestone Analytic Rule)

### 3.8.10 LPR

SAIMOS LPR provides License plate detection and recognition for free flow and parking scenarios. The following sections will show the LPR specific configuration within the SAIMOS VA system.

#### 3.8.10.1 Plate Detection



##### 3.8.10.1.1 Standard Settings

- Plate Size**  
 The Plate Size handles the minimum and maximum height of characters that should be considered for the scene. Please put at least two boxes representing the minimum and maximum size of a plate that should be detected by the algorithm.
- Stream Preset**  
 You can choose between Freeflowing, Parking and Offline where Freeflowing is the least accurate detection but the fastest and Offline is the slowest method offering the best detection rate (frame by frame).
- Classifier**  
 You can choose the required classifier for your region here.
- Engine Preset**  
 You can choose between the fastest or best classification method for the license plates. If you are not sure what is best for your scene choose Standard as a default.

##### 3.8.10.1.2 Advanced Settings

- Min. Readings**  
 This setting represents the minimum amount of readings that have to be present for a license plate to create a valid detection.
- Drop Plate After**  
 This value defines after how many frames a plate should be dropped from memory whether it was detected as a valid observation or not.
- Max. Match Deviations**  
 This option represents the maximum amounts of letters that are allowed to deviate to create a valid recognition match.
- Min. Confidence**

The minimum confidence for a plate detection in percent. Higher confidence will lead to less detections and recognitions.

### 3.8.10.2 Rules

Each SAIMOS LPR channel can have multiple independent rules. Currently Rules do not support visual separation of the LPR rules so each rule will work on the stream specified in the overall ROI.

The top screenshot shows the 'LPR Rules' window with a table of rules. The bottom screenshot shows the 'Edit Rule' form with the following fields and annotations:

- 1. Rule Name: lpr
- 2. Trigger: Plate Recognized
- 3. Plate Lists: test
- 4. Alert Expiration Time: 60
- 5. Advanced Settings

1. The rule name should be wisely chosen and will represent the rule within the LPR log for further inspection
2. The Trigger defines if each detection of a plate should trigger events or recognized plates set in a Plate List only.
3. Plate Lists option will only appear if the Plate Recognized Trigger is chosen and will enable the selection of one or more lists for the plate recognition. Plate lists have to be created before to be assignable from within this interface.
4. Alert Expiration time will set the minimum time between two consecutive events triggered by the rule in question.
5. The Advanced options will handle the messages for 3<sup>rd</sup> party rule propagation (like the Milestone Analytic Rule)

## 3.8.11 Count Stereo

SAIMOS® Count Stereo enables you to connect the counting data of external 3D stereo cameras to the SAIMOS® Count database and profit from the extended statistics and occupancy management it offers.

Count Stereo has no snapshot capabilities and will only connect to SAIMOS® VA system on a protocol level. Therefore, it has only 2 option layers which will be described in the following subsections.

### 3.8.11.1 Counting Data Source

The counting data source sets up the connection to the 3D sensor. Currently only the Vivotek SC8131 is supported. You can see an example for a configuration in the following screenshot.

- Source Type → currently only Vivotek is supported
- Host/Port → Set the right host/port combination to connect to the 3D camera

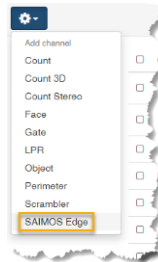
### 3.8.11.2 Counting Zones

The counting zone configuration is analogue to the zone configuration of SAIMOS Count (see 3.8.5.8). It will only allow for the configuration of counts and occupancy. Please make sure that the name of each configured zone has the exact same name as set on the 3D camera device.

## 3.8.12 Edge

SAIMOS® Edge channels enable you to integrate the SAIMOS® Edge products for Security and Safety Things (<https://store.securityandsafetythings.com/shop/catalog/c/main>) Intrusion, Count, Count & Heatmap into the server-side management of the SAIMOS® VA System. The channel will use the server-side node for a permanent connection to the camera. After a channel has been successfully added to the system it will integrate seamlessly into the SAIMOS VA system using the event management as well as server-side statistics and dashboard engine.

Creating and configuring a channel is quite easy. Just add a SAIMOS® Edge channel from the channel/node/group menu:



You will then see the general configuration view (below). You can give the channel a name (1) and you will have to assign it to a node (2). After that you can configure the Edge Device itself (3) and add some Alerts (4) if you want to.

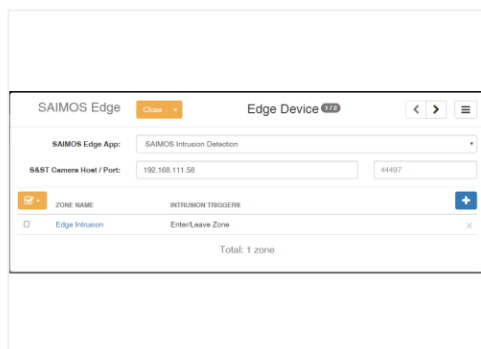
The configuration of the Edge Device will include the selection of the Edge App type you want to connect to (1) the IP of the camera (2) as well as the connection port (3). Do not change the default port of the connection unless you have manually changed it within the edge application itself.

You can currently choose between the following app types:

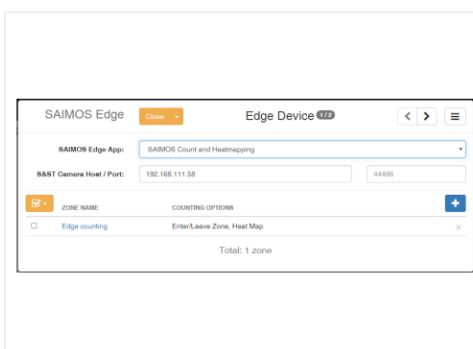
- Intrusion  
Will enable alarms for entering / leaving all configured intrusion zones.
- Counting  
Will enable counting statistics and occupancy management inclusion to SAIMOS VA for all configured zones.
- Count & Heatmapping  
Will enable counting statistics, occupancy management and heatmapping inclusion to SAIMOS VA for all configured zones.



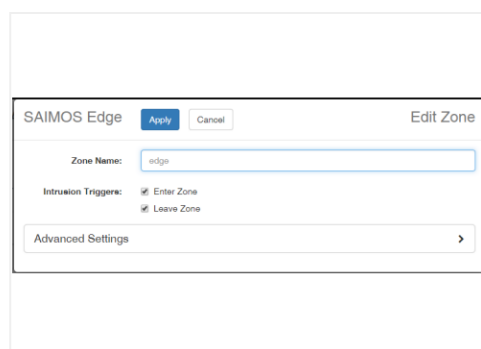
As soon as you have selected the edge app you will want to include with the device the respective zone configuration will appear. Each zone you add will have to have the same name of a zone also configured on the Edge App side. Within the zone the different options can be selected.



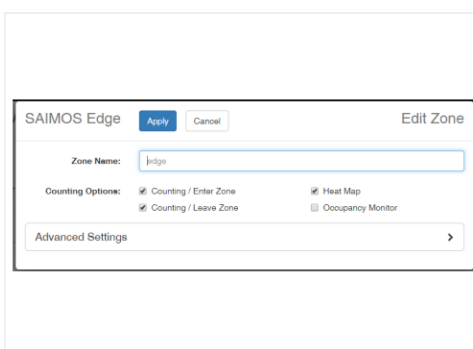
**1** Intrusion configuration & zone display



**2** Count & Heatmapping configuration & zone display



**3** Intrusion zone configuration



**4** Count & Heatmapping zone configuration

Alarm handling of the SAIMOS Edge channel is analog to all other channels within SAIMOS VA.

## 3.8.13 Lidar

SAIMOS® Lidar channels have the ability to connect to Lidar servers and use zone and tracking information to generate statistical input or event data for the SAIMOS VA system. A SAIMOS® Lidar channel can either do counting or occupancy management or intrusion detection for multiple zones within a channel.

Each rule set within a SAIMOS® Lidar channel will have to have the same name as the zone within the Lidar management server.

Currently SAIMOS® Lidar can connect to the following Lidar systems:

- Quanergy QORTEX DTC™
- Generic

### 3.8.13.1 Channel

A Lidar channel will have a similar structure to a normal channel but, as the technology used is different from camera technology, there are a few differences in the overall structure and how it is configured.

The screenshot shows the SAIMOS Lidar channel configuration interface. At the top, there is a header bar with the title 'Lidar', a 'Save' button, a 'Cancel' button, and an 'Add Channel' link. Below the header, the configuration is organized into several sections. On the left, there are four main configuration items: 'Channel Name' (1) with a text input field containing 'Lidar channel', 'Node' (2) with a dropdown menu showing 'DESKTOP-S1CE4S1', 'Groups' (3) with a dropdown menu showing '- None -', and 'Enabled' with 'No' and 'Yes' radio buttons. To the right of these is a large placeholder image showing 'Snapshot not available' (3). Below the main configuration items, there are three expandable sections: 'Lidar Device - QORTEX DTC' (4), 'Scenario - Counting' (5), and 'Alerts - None' (6). Each of these sections has a right-pointing arrow to indicate it can be expanded.

1. The channel name is as important with other channels and can be completely independent from the actual lidar devices you are using.
2. The Lidar channel will still run as a sandboxed executable like any other channel. However, it will only do metadata analysis and therefore uses only very low power on the Nodes' system.
3. There is no snapshot capability as the lidar data is not connected to any video source that can be displayed easily in 2D space.
4. The lidar device needs to be set. This is the respective server handling one or more Lidar devices. Communication ports will vary between products.
5. SAIMOS® Lidar currently has two scenarios. Depending on the scenario you set you will have different zone configurations. However, zones have to have the same name as defined in the respective Lidar server software to communicate successfully.
6. The same Alert interfaces exist as with every other channel within SAIMOS® VA. However, when using Milestone Alarms the camera device associated with the Alarm within Milestone XProtect® has to be set as the Lidar device is not coupled to a visual output within the Milestone XProtect® system. For more information about Alerts see 3.8.3.

### 3.8.13.2 Lidar Device

The Lidar Device section sets the main communication of the Lidar channel to the respective sensor management.

## 1. Source Type

For the source type there is currently QORTEX DTC available. When changing the source type, the standard communication port will switch automatically to match the desired Lidar software communication port needed for communication to SAIMOS® VA.

## 2. Host

Set the IP to the Lidar management software.

## 3. Port

Set the communication port to the Lidar management software. Normally the set standard ports do not need to be changed. When using a QORTEX DTC system, make sure that JSON communication and network byte order is set within the Lidar systems configuration.

## 4. Max. Message Rate

Sets the maximum message rate and respectively the query frequency towards the Lidar system. Standard is 2 Hz (2 queries per second).

### 3.8.13.3 Scenario

The scenario section will set the scenario for the lidar channel. Once the scenario for the channel is set and saved, it cannot be changed as the setup zones etc. are persistent in the database. So please make sure that you select the right scenario for your use case before saving the channel.

## 1. Scenario

Select between the scenario Counting or Intrusion.

## 2. Add a Zone

Click the + to add a new zone to the system. You can add as many zones as you like. However, there should always be a respective zone within the Lidar system defined to have successful communication.

## 3. Zone manipulator

Enable/Disable/Delete one or more selected zones.

## 4. Zone element

Configure the zone by clicking on its name or select the zone to Enable/Disable/Delete using the zone manipulator.

## 3.8.13.3.1 Count

Except for Heatmapping the Lidar counting zone offers the same possibilities as every other counting channel within the SAIMOS® VA system. So, it is possible to count in / out and relate the counts to a certain occupancy area if wanted.

The screenshot shows the 'Lidar' configuration window with 'Edit Zone' in the top right. The 'Zone Name' field is set to 'SAIMOS Backoffice'. Under 'Counting Options', both 'Counting / Enter Zone' and 'Counting / Leave Zone' are checked, and 'Occupancy Monitor' is also checked. The 'Occupancy Area' field is also set to 'SAIMOS Backoffice'. The 'Advanced Settings' section is expanded, showing 'Milestone Rules' and 'MULTIEYE Rules' for both 'count\_enter' and 'count\_leave' events.

### 1. Zone Name

The zone name is central for the zone configuration. This name has to match the zone name within the Lidar system you want to surveil exactly. Otherwise the communication to the Lidar system will fail.

### 2. Counting Options

Counting Enter/Leave to the zone as well as occupancy monitoring for the zone can be selected. When Occupancy Monitor is selected the Occupancy Area option will appear.

### 3. Occupancy Area

This option will appear, if Occupancy Monitor is selected. It is identical with other counting channels that use Occupancy Monitoring. For more information see 3.8.5.8.1 and 3.14.6.

### 4. Advanced Settings

Within the advanced settings the Milestone Rule name can be set for Milestone Analytic event propagation. Make sure that the rule name for entering and leaving matches the Milestone Analytic Events within the Milestone XProtect® system and that Analytic Event retrieval is enabled within XProtect®.

## 3.8.13.3.2 Intrusion

The SAIMOS® Lidar Intrusion scenario will analyze a given Lidar zone for its occupancy and will trigger an alert if the Object count exceeds its limit within the retention time tolerance.

Lidar
Apply
Cancel
Edit Zone

Zone Name: SAIMOS Backoffice 1

Alert Expiration Time: 60 2 s

Intrusion Trigger

Object Count: 1 3

Retention Time: 0 4 s

Advanced Settings 5

Milestone Rule: thelidar

MULTIEYE Rule: intrusion

## 1. Zone Name

The zone name is central for the zone configuration. This name has to match the zone name within the Lidar system you want to surveil exactly. Otherwise the communication to the Lidar system will fail.

## 2. Alert Expiration Time

Define the time period that has to pass until the next alert can be sent for this zone.

## 3. Object Count

Define the minimum number of objects that have to be detected in a zone by the Lidar within the defined retention time to trigger an alert.

## 4. Retention Time

Define the maximum retention time for objects within the Lidar zone until they become active for alerting.

## 5. Advanced Settings

Within the advanced settings the Milestone Rule name can be set for Milestone Analytic event propagation. Make sure that the rule name for intrusion matches the Milestone Analytic Events within the Milestone XProtect® system and that Analytic Event retrieval is enabled within XProtect®.

#### 3.8.14 Count 3D and Gate

Please contact the Forlan support team ([contact@saimos.eu](mailto:contact@saimos.eu)) or your SAIMOS® partner of choice for Gate configuration support.

## 3.9 Event Log

The event log aggregates and shows all events triggered by SAIMOS VA. You can sort the events ascending or descending by clicking on

- timestamp,
- channel,
- rule and
- zone.

The toggle image button will show/hide the alert image.

auto-refresh toggle filter results Event Log

Date Range: Last Hour Max. Records: 100

sort list

TIMESTAMP	CHANNEL	RULE	ZONE	IMAGE
14.09.15 11:15:56	objectvis Serverraum	Left Object		toggle image
14.09.15 11:15:34	Sony Serverraum arealvis wide	Retention Time	Something moving	

### 3.9.1 Filter

When clicking on the button in the event log view the filter modal will open.

Apply Cancel

Date Range: Last Hour

Rule: - All -

Channel: - All -

Max. Records: 100

You can filter by

- Date Range
- Rule
- Channel

You can also define the maximum amount of records. The *Date Range* filter has multiple presets and a *Custom* option.

Apply Cancel 🔍

**Date Range:**

⌵

Last 6 Hours (11:18—17:17)

📅

**Rule:**

Custom

▼

**Channel:**

Last 15 Minutes

▼

**Max. Records:**

Last 30 Minutes

▼

ony Gang standard

richtung Küche

alvis left standard

OWLS left standard

alvis right standard

5 s im Bereich

is streetview standard direct

Axis streetview standard direct

is streetview standard

Axis streetview standard

ärbild standard

Zum Gelände

ärbild standard

weg vom Gelände

alvis right standard

5 s im Bereich

ärbild standard

Aufenthalt im Bereich

is streetview standard direct

Axis streetview standard direct

When using the *Custom* option within *Date Range* filter option you will be able to define the start and end date for the filter manually.

Apply Cancel 🔍

**Date Range:**

⌵

16.06.2016 11:16 18.06.2016 17:15

📅

**Rule:**

– All –

▼

**Channel:**

– All –

▼

**Max. Records:**

300

▼

is streetview 2

Intrusion

alvis right standard

Intrusion

< June >

< 2016 >

MO	TU	WE	TH	FR	SA	SU
22	30	31	1	2	3	4
23	6	7	8	9	10	11
24	13	14	15	16	17	18
25	20	21	22	23	24	25
26	27	28	29	30	1	2
27	4	5	6	7	8	9

📅
Today
Cancel

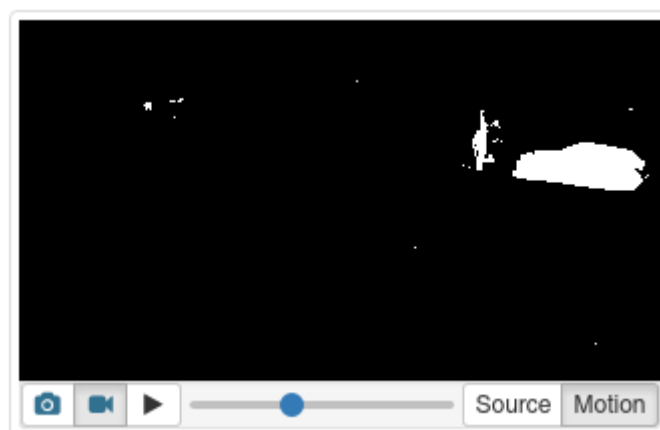
Filtered results will only remain static as long as the auto refresh is disabled. When auto refresh is enabled new events will be added to the filtered view regardless if they fit the filter or not.

### 3.9.2 Event Image / Alarm Sequence

If alarm sequence recording is activated you can switch between the metadata alert image and the alarm sequence by pressing either the photo- or video-camera button. The Play button starts and stops the playback and with the slider you can scan faster or slower through the alarm sequence. With the



*Source/Motion* toggle you can switch between the source image and the output of the motion detector.



### 3.10 System Log

The system log shows all aggregated logs from the server, nodes and channels within the system. You can sort the logs ascending or descending by clicking on *Timestamp* or *Source*.

The screenshot shows the SAIMOS System Log interface. On the left, there is a sidebar with various filters: 1. Filter Bar Toggle (magnifying glass icon), 2. Export button, 3. Filter Bar (date range, time of day, log level, source type, node, channel). The main area displays a table of log entries with columns: Timestamp, Source, and Message. 4. Search bar at the top right. 5. Log entry details. 6. Pagination bar at the bottom showing 'Total: 3175 records' and navigation controls. 7. Page size selector.

#### 1. Filter Bar Toggle

Click the magnifying glass to toggle the Filter bar on the left side of the system log.

#### 2. Export

Click the Export button to download the selected logs (or all logs defined by the filter) as CSV, HTML, Excel or PDF file.

#### 3. Filter Bar

See 3.10.1 Filter Bar.

#### 4. Free text search

Enter any text and log entries that have similar text will be filtered automatically. This is a useful feature to only display log entries you are interested in.

#### 5. The log entry

The log entry will show you the time stamp, source and message. You can also select it using the tick box for selective exporting.

#### 6. Paging element

This element enables you to step between pages of the filtered log output.

#### 7. Page size

The page size will define how many log entries are allowed per page.

#### 3.10.1 Filter Bar



When clicking on the button in the system log view the filter bar will open / close.

The image shows a filter panel for SAIMOS with the following components:

- 1. Date Range:** A dropdown menu currently showing 'Today' with a calendar icon to its right.
- 2. Time of Day:** Two input fields showing '00:00' and '24:00' with an 'x' button to clear the range.
- 3. Log Level:** A dropdown menu currently showing '- All -'.
- 4. Source Type:** A dropdown menu currently showing '- All -'.
- 5. Node:** A dropdown menu currently showing '- All -'.
- 6. Channel:** A dropdown menu currently showing '- All -'.
- 7. Max. Records:** A text input field containing the value '5000'.

At the bottom of the panel are two buttons: a blue 'Apply' button and a grey 'Reset' button.

## 1. Date Range

You can select a date range preset by using the  button or select a custom date range by using the date picker tool . Either way logs will only be displayed for the time period selected.

## 2. Time of Day

You can filter by a certain time of day within the date range. This means that only logs within this time of day period will be shown.

## 3. Log Level

You can filter by the log level (Error, Warning, Info, Debug). Only logs will be shown matching the selected log level. Multiple choices are possible of course.

## 4. Source Type

You can select the source types to be displayed. Currently the following source types are available: Server, Nodes, Channels, Plugins. Only the selected source types will be displayed in the resulting list. Multiple selections are possible.

## 5. Node

You can specifically filter by a certain SAIMOS® Node. Only log messages will be displayed concerning the Node(s) selected.

## 6. Channel

You can specifically filter by a certain SAIMOS® Channel. Only log messages will be displayed concerning the Channel(s) selected.

## 7. Max. Records

You can define the maximum number of records displayed within the log list.

## 3.11 User Management

SAIMOS VA supports comprehensive user management including user groups to assign different levels of rights to different users. When entering the User and Group Management page you can toggle between the user view and the group view. The basic operations for the user or group are:

- Add a user or group
- Delete a user or group
- Enable or disable a user or group
- Switch between user and group view

### 3.11.1 The User View

The screenshot shows the 'Users' management interface. At the top, there are three main buttons: 'enable, disable or delete selected users' (with a checkmark icon), 'switch between users and groups' (with a group of people icon), and 'add a user or group' (with a plus icon). Below these buttons is a table of users. The table has three columns: 'USERNAME', 'FULL NAME', and 'MEMBER OF'. The first row is for 'admin' (Administrator) with a 'click to edit' link and a 'delete user' button. The second row is for 'guest' (The guest) with a 'delete user' button. The third row is for 'testuser' (test user) with a 'delete user' button. A 'select users' checkbox is on the left of each row. At the bottom, it says 'Total: 3 users'.

USERNAME	FULL NAME	MEMBER OF
admin	Administrator	Administrators
guest	The guest	Guest
testuser	test user	Guest

Total: 3 users

By clicking a username of a certain user or by clicking the *Add user* button you will enter the *Edit User* mode for the user. You can create a new user or edit an existing user here. Permissions for the user are inherited by the user group the user is a member of. The *Permissions* drop-down will lists the current permissions of the user. You can also delete a user or reset to its previous configuration by selecting the options in the sub menu of the *Save* button.

Save

Cancel

Edit User

delete or reset the user to the previous configuration

Username:

testuser

Full Name:

test user

Email:

test@cogvis.at

Password:

\*\*\*\*\*

Enabled:

No

Yes

Member of:

select the groups the user should be a member of

Guest

Permissions

show the current permissions of this user

System Management

✓ View Node Status

✓ View Event Log

✓ View System Log

✗ Edit Node Configuration

✓ Start/Stop Channels

Channel Setup

✓ View Channel Configuration

✗ Edit Channel Configuration

Reports

✗ View Reports

✗ Edit Reports

✗ Execute Reports

System Configuration

✓ View Camera Configuration

✗ Manage Cameras

✓ View Interfaces

✗ Manage Interfaces

✗ View Server Configuration

✗ Edit Server Configuration

✗ View License Information

✗ Upload License

User Management

✓ View Users/Groups

✗ Edit Users/Groups

### 3.11.2 The Group View

enable, disable or delete selected users

switch between users and groups

GROUP NAME ^

Administrators

click to edit group

add a user or group

Groups

	MEMBERS	
<input type="checkbox"/>	Administrator	delete group ✕
<input type="checkbox"/>	test user, The guest	

Total: 2 groups

By clicking the name of a group or by adding a group using the *Add Group* button you enter the group edit view. Users can be added to groups here and group permissions can be edited. For faster permission editing permissions can also be copied from another group. By using the submenu of the *Save* button you can also select to delete the group or reset it to its previously saved settings.

Save

Cancel

Edit Group

delete or reset the group to its previous settings

Group Name:

Enabled:

add members to your group

Members:

Permissions

Copy from group -

copy permissions from another group

System Management

☒ View Node Status
☒ View Event Log
☒ View System Log
☐ Edit Node Configuration
☒ Start/Stop Channels

Channel Setup

☒ View Channel Configuration
☐ Edit Channel Configuration

Reports

☐ View Reports
☐ Edit Reports
☐ Execute Reports

System Configuration

☒ View Camera Configuration
☐ Manage Cameras
☒ View Interfaces
☐ Manage Interfaces
☐ View Server Configuration
☐ Edit Server Configuration
☐ View License Information
☐ Upload License

User Management

☒ View Users/Groups
☐ Edit Users/Groups

## 3.12 Server Administration

The server administration page can be found at *Configuration --> Server Administration*.

Save and Restart

Cancel

Server Administration

### Network Configuration

Web Server:	<div style="border: 1px solid #ccc; padding: 2px;">All network interfaces</div>	<div style="border: 1px solid #ccc; padding: 2px;">44444</div>	<input checked="" type="checkbox"/> SSL								
Node Management:	<div style="border: 1px solid #ccc; padding: 2px;">All network interfaces</div>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; width: 20px;">+</td> <td style="border: 1px solid #ccc; padding: 2px;">44443</td> </tr> <tr> <td style="text-align: center;">+</td> <td style="border: 1px solid #ccc; padding: 2px;">44442</td> </tr> <tr> <td style="text-align: center;">+</td> <td style="border: 1px solid #ccc; padding: 2px;">44441</td> </tr> <tr> <td style="text-align: center;">Q</td> <td style="border: 1px solid #ccc; padding: 2px;">45555</td> </tr> </table>		+	44443	+	44442	+	44441	Q	45555
+	44443										
+	44442										
+	44441										
Q	45555										
TCP Server:	<input type="checkbox"/> <div style="border: 1px solid #ccc; padding: 2px;">All network interfaces</div>	<div style="border: 1px solid #ccc; padding: 2px;">44450</div>									
Send Responses To:	<input type="checkbox"/> <div style="border: 1px solid #ccc; padding: 2px;"></div>	<div style="border: 1px solid #ccc; padding: 2px;"></div>									
Modbus Server:	<input type="checkbox"/> <div style="border: 1px solid #ccc; padding: 2px;">All network interfaces</div>	<div style="border: 1px solid #ccc; padding: 2px;">44440</div>									

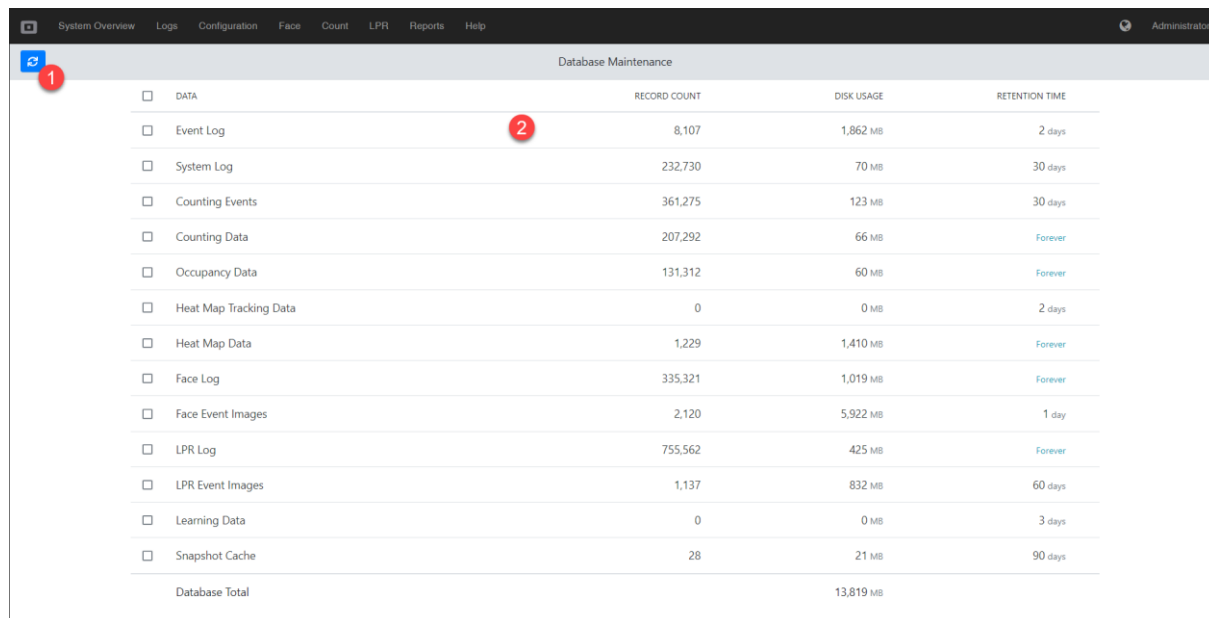
### 3.12.1 Network Configuration

- **Web Server**  
You can bind the web server to different interfaces and define another port. You can also toggle SSL encryption. If SSL is on (default) you have to address the web interface via HTTPS.
- **Node Management**  
You can bind the internal node management to different interfaces (0.0.0.0 --> all interfaces is default) and change the internal communication ports. Do not change these unless you know the implications.
- **TCP Server**  
Enable/Disable the internal TCP Command Interface server and bind it to a network interface and port.
- **Send Responses To**  
Enable/Disable responses from the TCP Command Interface to a certain receiver and bind it to a host and port.
- **Modbus Server**  
Enable/Disable the internal Modbus server and bind it to a network interface and port.

After saving the configuration the server will attempt to restart with the new settings. On Windows the service will stop but not start again. You will have to start the service manually after saving.

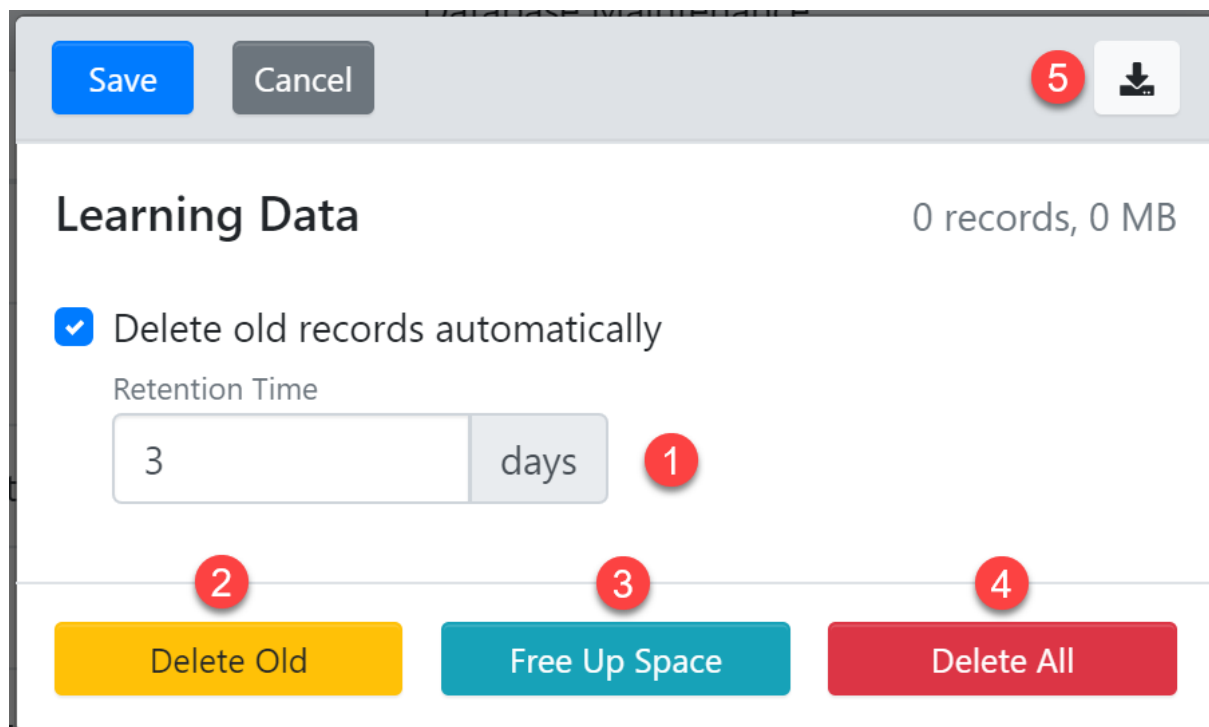
## 3.13 Database Maintenance

The database maintenance view can be found under *Configuration -> Database Maintenance*. It will give you information about what space is currently estimated to be occupied within the database and it will give you the possibility to clear up space or automatically delete old data after a certain time period.



	RECORD COUNT	DISK USAGE	RETENTION TIME
<input type="checkbox"/> DATA			
<input type="checkbox"/> Event Log	8,107	1,862 MB	2 days
<input type="checkbox"/> System Log	232,730	70 MB	30 days
<input type="checkbox"/> Counting Events	361,275	123 MB	30 days
<input type="checkbox"/> Counting Data	207,292	66 MB	Forever
<input type="checkbox"/> Occupancy Data	131,312	60 MB	Forever
<input type="checkbox"/> Heat Map Tracking Data	0	0 MB	2 days
<input type="checkbox"/> Heat Map Data	1,229	1,410 MB	Forever
<input type="checkbox"/> Face Log	335,321	1,019 MB	Forever
<input type="checkbox"/> Face Event Images	2,120	5,922 MB	1 day
<input type="checkbox"/> LPR Log	755,562	425 MB	Forever
<input type="checkbox"/> LPR Event Images	1,137	832 MB	60 days
<input type="checkbox"/> Learning Data	0	0 MB	3 days
<input type="checkbox"/> Snapshot Cache	28	21 MB	90 days
Database Total		13,819 MB	

You can refresh the status of the space calculation/estimation using the refresh button (1) and you can manage each database item by clicking on it (2).



Save

Cancel

5

Download

Learning Data

0 records, 0 MB

☒ Delete old records automatically

Retention Time

days

1

2

Delete Old

3

Free Up Space

4

Delete All

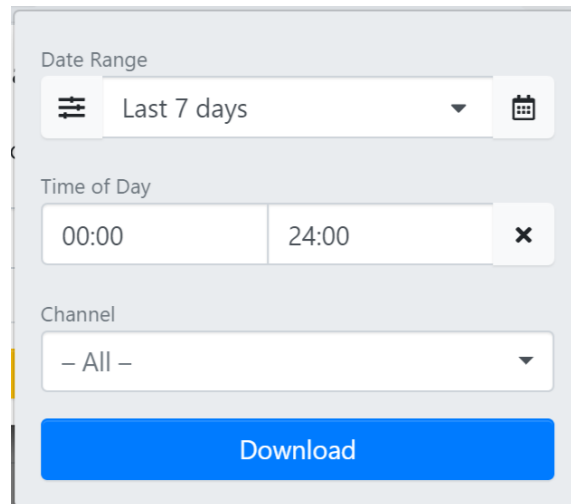
If you have clicked on an item the modal for storage management will appear. If you select to delete old records automatically (1) the old records will be cleaned up after the time period of x days has passed. Be careful with applying this (outside of the standard settings) for data as once deleted the data will be gone. If you select Delete Old (2) you will trigger an immediate delete of data older than the retention time value given. The Free Up Space (3) option will do a vacuum on the data to clear up



data that has already been marked for deletion but is not deleted yet. The Delete All (4) button will delete all data for the selected data entry. Please beware that this button (4) is dangerous and should only be used if you know that the data you are deleted is not needed by the system/user anymore.

All cleanup operations will happen async and do not require you to stay on the page. Once you have triggered a job you can just work on and the cleanup will happen in the background. Please note, that deletions might take some time depending on the amount of records that have to be deleted.

For the Learning Data entry there is also the possibility to download the learning data as a ZIP file by pressing the download (5) button. It will give you a filter view so you can also select for certain learning data files.



The screenshot shows a filter view for downloading data. It includes three filter sections: 'Date Range' with a dropdown set to 'Last 7 days' and a calendar icon; 'Time of Day' with two input fields showing '00:00' and '24:00' and a clear button 'x'; and 'Channel' with a dropdown menu set to '- All -'. At the bottom is a large blue 'Download' button.

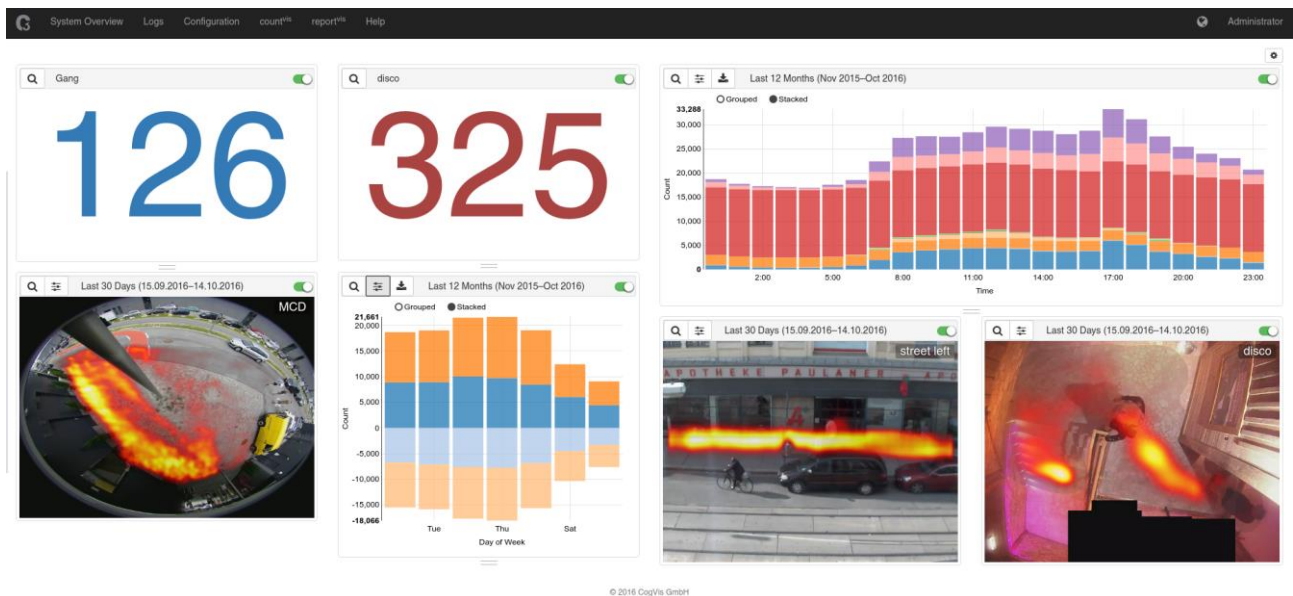
If you hit the Download button the selected filtered data will be downloaded as a ZIP file.

## 3.14 Count Control

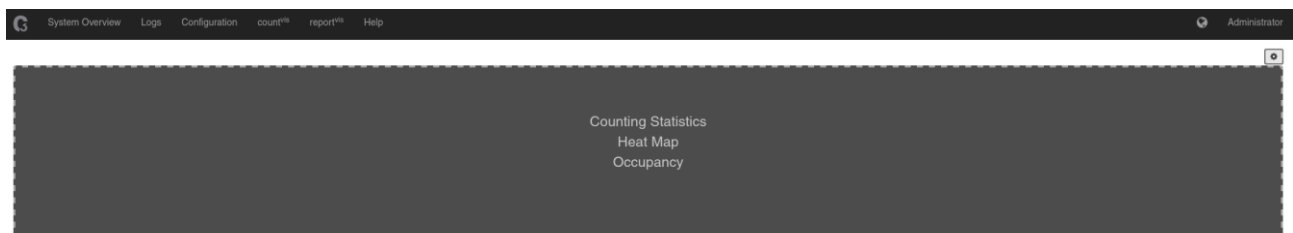
The Count menu in the main menu bar gives you access to the different views to view your acquired counting and heatmap data. It will give you access to the counting statistics, the occupancy monitor, heatmap and the control for the occupancy areas. The coming sections will give you an overview on how to use the several views.


### 3.14.1 Dashboard

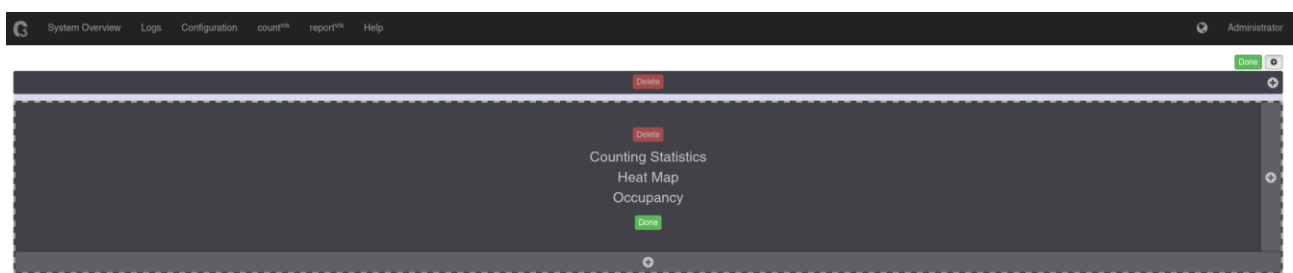
The dashboard is a fully customizable view for your statistical data, heat map data and occupancy areas. The view is based on columns and will automatically adjust to the size of your browser. The view is nested, so each column can hold new rows and columns. Beware, be sure you have a capable system if you pack your dashboard with lots of different views.




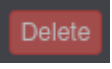



You will start with an empty one column view.



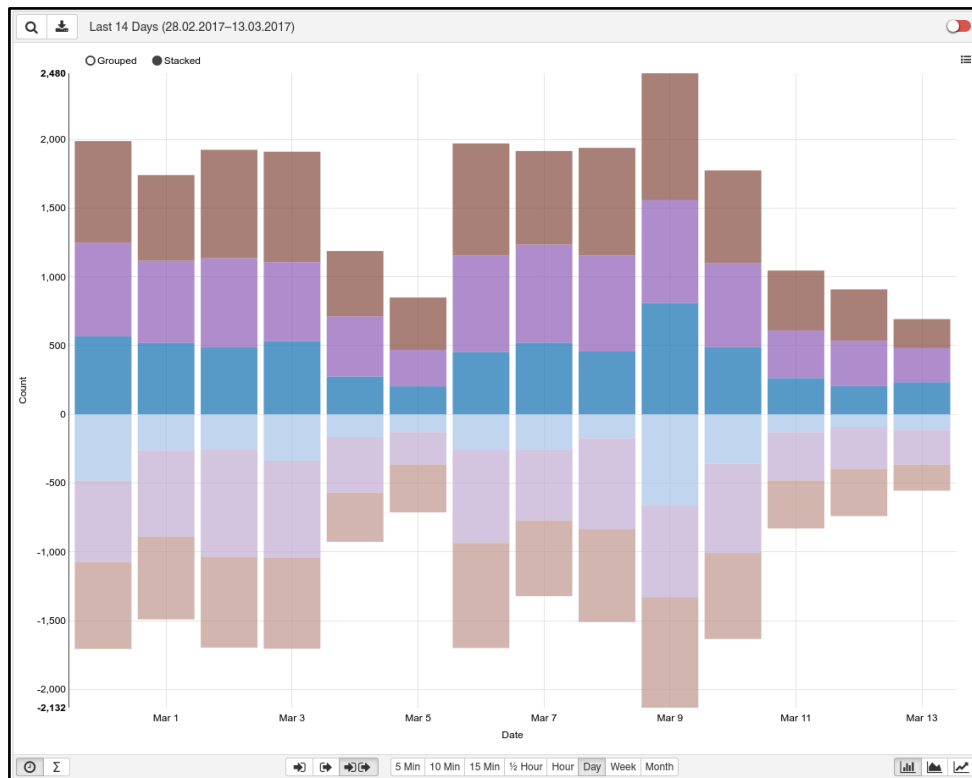
For each dashboard item you can choose between Counting Statistics, Heat Map and Occupancy. To customize your dashboard view hit the edit button  at the top right to enter edit mode.



Once you're in edit mode you can add global columns for the view by clicking  within the top column item. Within each item you can also add rows or columns by either clicking the column  on the bottom of the element or clicking the  on the right area of the element. You can delete items or columns by clicking the  button. As soon as you are done with your setup you can click  anywhere you find it to exit the edit mode of the dashboard. Have fun creating your own dashboard.

### 3.14.2 Counting statistics


The Counting Statistics page is the main view to view the collected counting data. It consists of a statistics interface where you can filter, download and view your data.

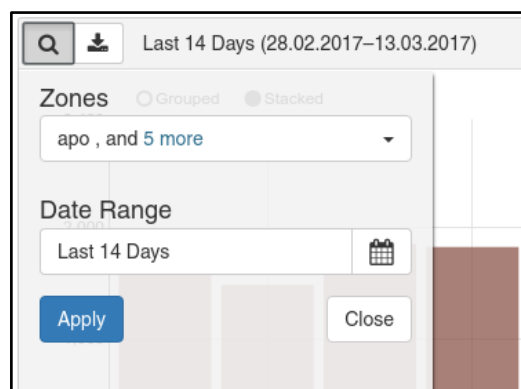





### 3.14.3 Counting statistics filter menu

The counting statistics filter menu consists of several buttons that enable you to filter the live statistics.

#### 3.14.3.1 Zone / time filter modal

The  button will open the zone / time filter panel.



You can choose the desired Date Range by choosing a pre-defined filter using the menu  or you can choose a custom Date Range using the  button or select Custom in the  menu. Using the Zones dropdown enables you to select specific zones.

### 3.14.3.2 Timeline mode (raw live data)

The timeline mode shows the raw live counting data of selected areas in the chosen granularity.

### 3.14.3.3 Aggregation mode (SUM, AVG, MIN, MAX)

The aggregation menu lets you choose to display either the sum, the average, the minimum or the maximum counts for the chosen granularity.

### 3.14.3.4 Direction menu

The direction menu will let you choose to display either *Enter*, *Leave* or *Enter and Leave* counts.

### 3.14.3.5 Granularity menu (5 min - 1 Month)

The granularity menu defines the granularity for the statistics you can choose several presets between 5 minutes and one month here. The available granularity in the bottom toolbar will depend on the graph mode.

### 3.14.3.6 Chart type menu

Choose the desired type of the chart here. You can choose between bar chart, area chart and line chart.

### 3.14.3.7 Download menu

Here you can download the current filtered data to the following formats: CSV, Excel, HTML, PDF. If you choose Excel the downloaded file will also contain sheets with pre-defined charts similar to the current chart.

### 3.14.3.8 Auto Update selector


Click to activate or deactivate the auto update functionality.

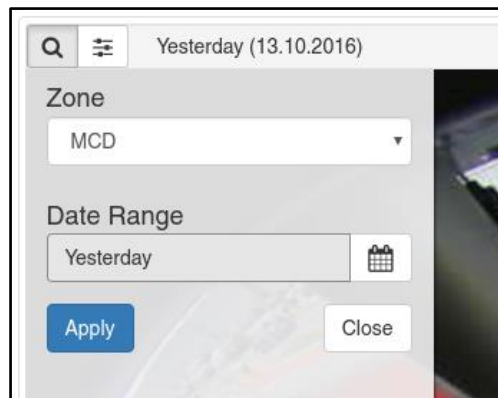
## 3.14.4 Heatmap


Within the heat map view you can view your accumulated and weighted tracking data as an abstract heat map. The data can be filtered by time periods and is scaled by occupancy time within the scene and size of the objects.




## 3.14.4.1 Zone/time filter panel


The  button will open the zone / time filter panel.

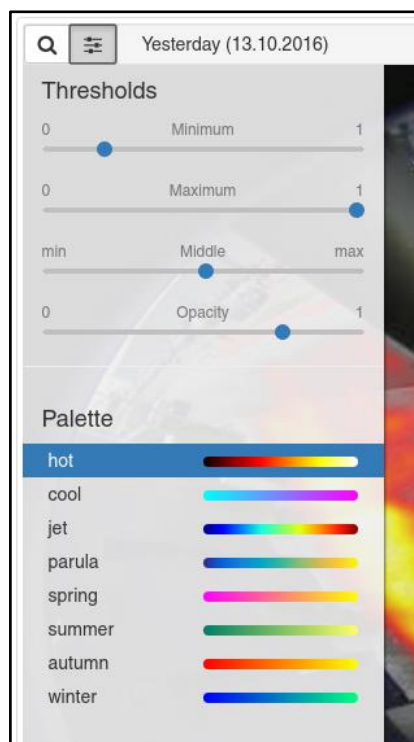


You can choose the desired Date Range by choosing a pre-defined filter using the menu  or you

can choose a custom Date Range using the  button. Using the *Zone* drop down enables you to select specific zones.

Heat map data control panel



The  button will enable the heat map data control panel.



Here you can adapt the thresholds of your heat map. You can change the minimum and maximum threshold levels as well as the min/max scaling and the opacity of the heat map. Additionally you can change the color palette to fit your needs.

## 3.14.4.2 Snapshot/Video control toggle

If you hover over the heat map the image/video control will appear at the bottom of the heat map.

You can toggle between snapshot () and video () mode. In Snapshot mode you can refresh the snapshot by clicking the refresh icon on the right of the control and in video mode you can hit play/pause to control the video on the right of the control.


## 3.14.4.3 Auto Update selector


Click to activate or deactivate the auto update functionality.


## 3.14.5 Occupancy monitor


The occupancy monitor will give you an overview on how many people currently occupy an area. All zones you have added to the same occupancy area will be accounted for. So, you can add e. g. several entrances of a building to the same occupancy area to see how many persons entered the building.

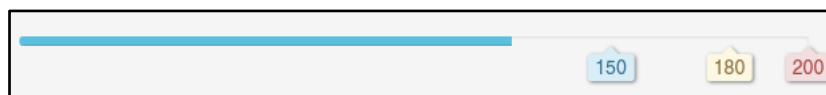


By design, the occupancy area view will show all areas configured for occupancy management. You can use the  button to filter the occupancy areas you want to show within the view and you can

use the size slider  to adjust the occupancy areas to your screen. If you have

proper rights to correct areas you can do so by clicking the  button. You will be presented with

the occupancy edit menu . You can now use the +1, +10 or -1, -10 button to increase or decrease the area count or you can use the reset button to set it to 0 again. Only after you hit apply the new settings will be applied to the occupancy area. If you set any occupancy limits for the areas the area will blink red if the limits area exceeded. Additionally if you have set proper limits for an occupancy area a progress bar and limit indicators will give an overview on how filled the area is.



## 3.14.6 Occupancy areas

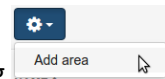
In the occupancy areas view you can manage your occupancy areas. You can add/delete/modify areas to your liking and define reset times and thresholds for the different occupancy areas. Also, if you have Modbus enabled, you will be able to specify Modbus registers for the several occupancy areas. This will enable third party applications to get the occupancy information. If you have enabled a occupancy monitor area for a zone within a Count channel it will be automatically added here.

Occupancy Areas			
<input type="checkbox"/> AREA NAME ^	COUNTING ZONES	RESET TIME	
<input type="checkbox"/> apo	apo	04:00	×
<input type="checkbox"/> disco	disco	04:00	×
<input type="checkbox"/> Gang	Gang	04:00	×
<input type="checkbox"/> gang küche	gang küche	04:00	×
<input type="checkbox"/> gang rezeption	gang rezeption	03:00	×
<input type="checkbox"/> MCD	MCD	06:00	×
<input type="checkbox"/> street	street left, street right	00:01	×
Total: 7 areas			

Deleting a zone is very easy, just hit the x on the right side of the zone row to delete it.

### 3.14.6.1 Add/Edit zone view

You can edit a zone by clicking on its name or you can add a zone by clicking



Save Cancel

Edit Occupancy Area

Area Name: disco

Counting Zones: disco

Auto-reset Times: 08:30 13:00

Occupancy Thresholds: 180 200 150

Modbus: C3 Modbus Server 201 202

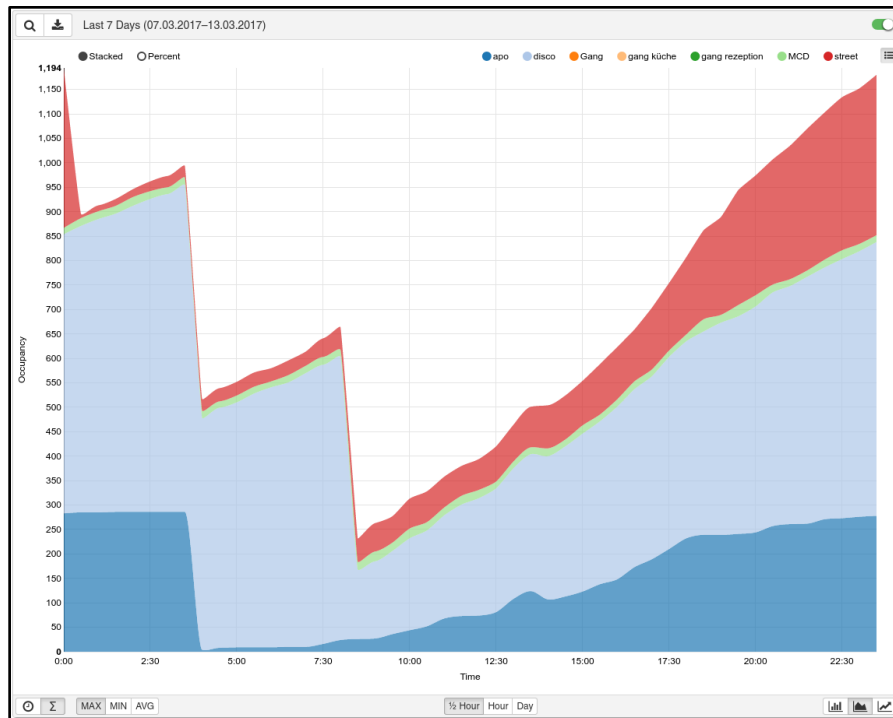
Alerts

Alert Destinations: DESTINATION E-mail konetschnig@cogvis.at

Give the area a useful name and add/remove zones from the area by using the select drop down menu for *Counting Zones*. If you want to reset the zone automatically at certain times a day you can do so by setting *Auto-reset Times*. If you want to add another time just do so by hitting the + symbol on the right side of the previous zone. You can also add *Occupancy Thresholds* to define when the occupancy for a zone is "high", "full" or when a zone has a normal occupancy again. If you added at least one Modbus server to the system you will also be presented with the possibility to define a *Modbus* server where the *occupancy register* as well as the *error register* can be filled according to the current area status. You can also send alerts if the occupancy threshold limit is reached and/or if the occupancy of the area has recovered again. Just hit the + for the Alert Destinations and you can select between Email, Milestone, TCP Trigger or HTTP commands. You can send as many different alerts as you like per occupancy area. There is no defined time out for alerts. A new alert will be sent every time the alert status of the area has changed.

### 3.14.7 Occupancy statistics

The occupancy statistics page will enable you to get detailed statistic about the occupancy of areas. The control will work analogue to the 3.14.2 Counting statistics control.

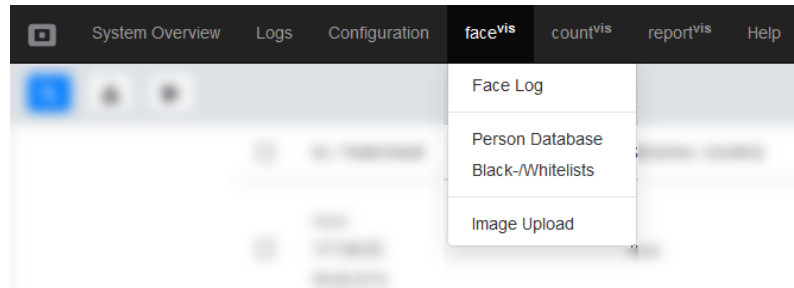




## 3.15 Face Analytics Pro

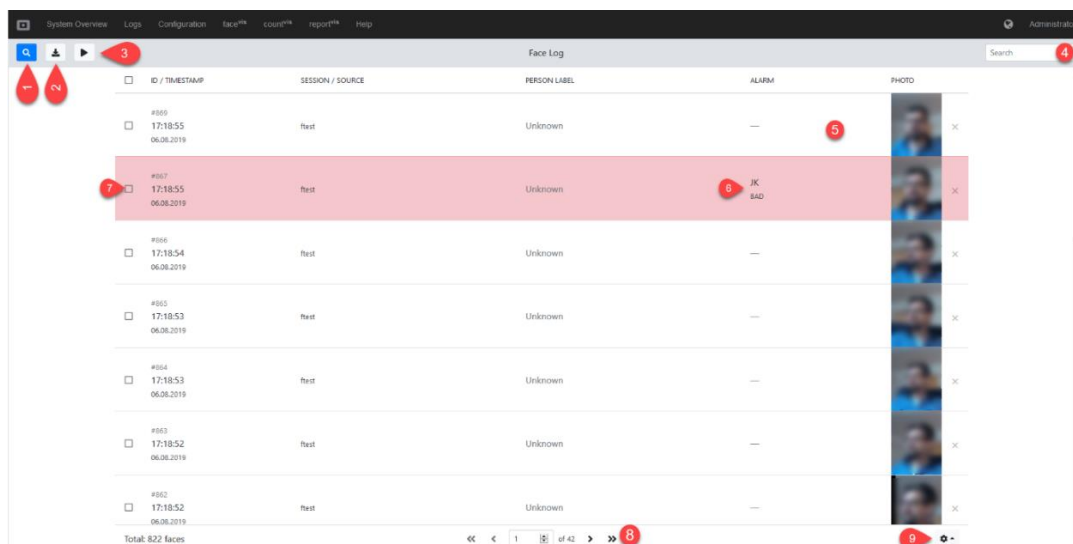
SAIMOS Face Analytics Pro uses state of the art AI systems to detect, recognize and compare faces. The user-friendly interface provides step by step configuration enabling fast setup times and reporting. The Face Pro use case specializes on Black-/Whitelist real time alerting and flexible reporting of detected and recognized faces for investigation as well as forensic analysis.

The following sections will introduce the different views that are available with Face Pro.



### 3.15.1 Face Log

The face log is the central interface for Face Pro. It shows all detected faces as well as the black-/whitelist recognitions. The following screenshot shows an example of the face log and the different types of controls filters that are available will be explained in the following sections.



#### 1. Filter control

The filter control enables you to filter detections and recognitions. For more information about this control see 3.15.1.2 below.

#### 2. Export control

The export control enables you to export selected or all faces currently in the face log. For more information see 3.15.1.3 below.

#### 3. Session control

The session control enables you to create new sessions within the face log. Sessions help you to keep different detection observation sessions and enable a faster search. For more information see 3.15.1.4 below.

#### 4. Live search field

The live search field will help you to find detections or recognitions very fast. Just type some text in the search field and the current list will be limited to everything that matches the text.

#### 5. Detail view control

By clicking on a detection, the detailed view control will open and give further possibilities to label faces, comment on the detection or look at the full scene view of the detection. For further details see 3.15.1.1 below.

## 6. Recognition indicator

If a face is recognized it will be labeled with the recognition result and colored differently. Only alarms are currently labeled so don't worry if not all detections are labeled this way. Every recognition needs time and performance and so we are skipping recognitions within the alarm timeout.

## 7. Selector control

The selector control enables you to limit actions to selected items only. The possible actions are: Export, comment, label and delete.

## 8. Page control

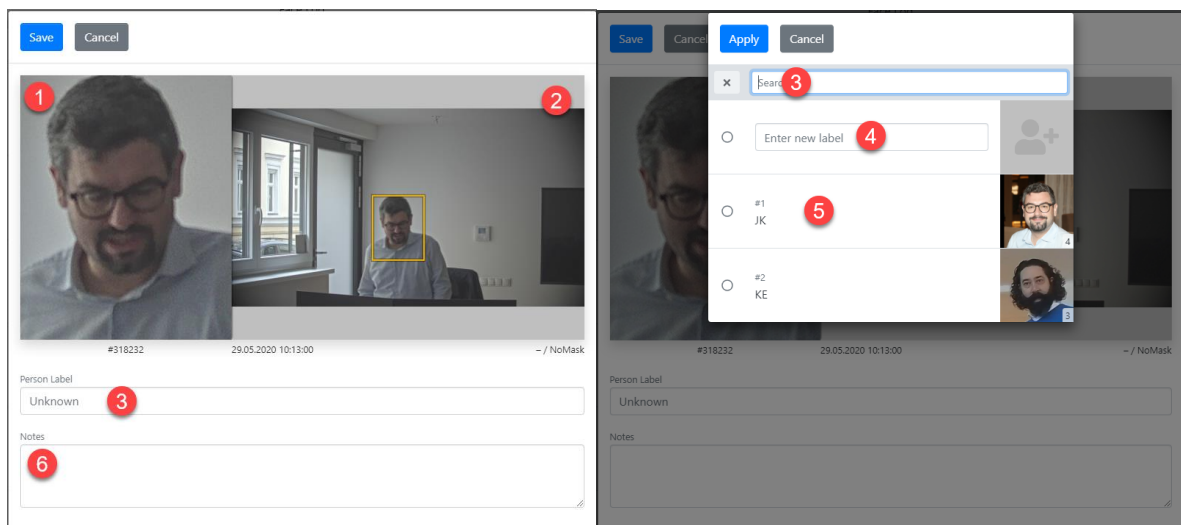
The page control simply allows you to switch between pages. Don't worry, selections are persistent even if you switch the page.

## 9. Page size control

The page size control gives you the option to look at more or less faces per page. Be aware that the more faces you will display on one page the more time it will need to display the individual pages.

### 3.15.1.1 Detailed detection view

The detailed detection view enables you to watch and edit a single detection. It offers the possibility to label the current detection with an existing or new label and also to comment on the detection.



## 1. Detection cut out photo with optional recognition label

Shows the digitally cut photo of the person detected. It will also contain a label if the person is recognized on one of the available lists.

## 2. Full snapshot of the detection with the detection bounding box overlaid

Shows the full snapshot of the time of the detection with an overlaid bounding box of where the system expects the face to be.

## 3. Live search for labels

This is the live search field for the labels available. If you have many labels in the system this will help you to find the right label faster, just click the person label section to open the live view and search for labels, add new ones or select existing ones already shown.

## 4. New label field

If the current detection should be added as a new label just type the name of the label in the new label field and after saving the detection the face will be added as a new label.

## 5. Existing label selection fields

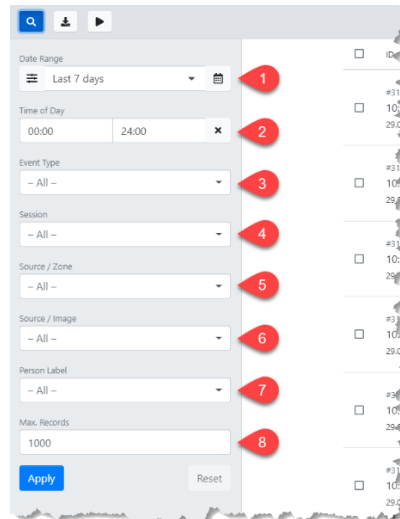
If the current detection should be added to an existing label just click on the existing label of your choice and save the detection.

## 6. Comment field

This field enables you to add comments to the current detection. The comment will be displayed in the face list and the exports.

### 3.15.1.2 Filter

The filter control enables you to filter the face log results by several criteria. This can help with searching and exports. The different filter options will be explained below.



#### 1. Date Range

The date range filter will enable you to filter by predefined date ranges (today, yesterday, last seven days) or a custom date range. To select a custom date range just click on the calendar day one time to select the start of the range and then a second time on the day for the end of the range. If you only click on one day, this day will be selected as the range.

#### 2. Time of Day

The Time of Day filter enables you to select only a certain time of day period for the selected date range.

#### 3. Event Type

You can filter by event type (Non-Alarm, Recognition Alarm, Detection Alarm).

#### 4. Session

You can filter the result by a certain session. If you have no sessions the Unassigned session will be the only item to select. You can also multiselect different sessions. If you have many sessions, just use the live search to find the right session name.

#### 5. Source/Zone

Limit the search result to certain configured zones. If you have many zones, use the integrated live search to find the right zones. Multiple selections are possible.

#### 6. Source/Image

Filter the search result by certain uploaded images. You can also use the live search to find the right images, if you have multiple images in the system. Multiple selections are possible.

#### 7. Person Label

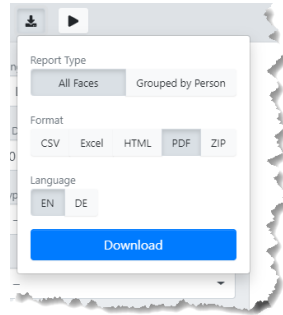
Filter by certain person labels. Use the live search if you want to find your desired labels faster. Multiple selections are possible.

#### 8. Max. Records

Set the amount of records that should be shown in the search result. Be aware that the more results are selected the less performant the page will be.

### 3.15.1.3 Export

The export control enables you to export the face log result. You can select multiple faces for export or export the whole log if you made no selections. There are multiple ways to export faces which are explained below.



#### 1. Report Type

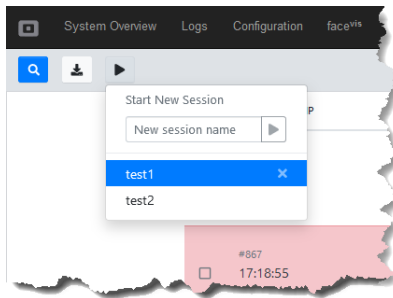
- a. All Faces  
Will export all faces in the list.
- b. Grouped by Person  
Will export a grouped report of the selected faces. Faces that are similar will be grouped together and the count of these faces will be reported in a first seen – last seen style. Creating such report might take longer than the standard All Faces report. The grouping will only be done for document type exports and not the ZIP Download.

#### 2. Download

- a. CSV  
A simple CSV file will be exported.
- b. Excel  
An excel containing the face pictures will be exported.
- c. HTML  
A HTML file for viewing in a browser will be exported.
- d. PDF  
A PDF file will be exported (might take longer than the other document downloads as the PDF needs to be rendered beforehand).
- e. ZIP (Images)  
A zip file will be downloaded containing the face images as well as the scene images for the selected detections. This type of Download might be very big and take a while. Do not export too many pages if you are in a hurry. We have dedicated scripts for a speedier export of raw image data. If you need support on export scripts, please contact us via email on [contact@saimos.eu](mailto:contact@saimos.eu).

### 3.15.1.4 Sessions

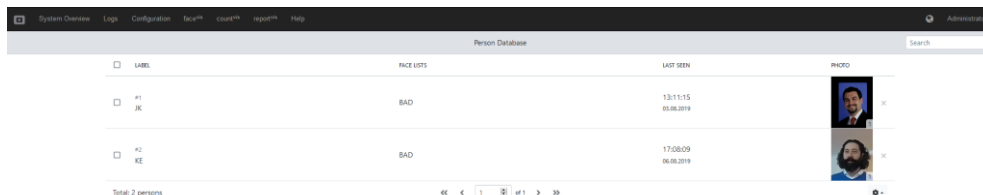
Sessions are a great way of grouping or limiting face log results (for example in observation scenarios where you want to search by observations). By default, all logs will be saved to the default session *Unassigned*.



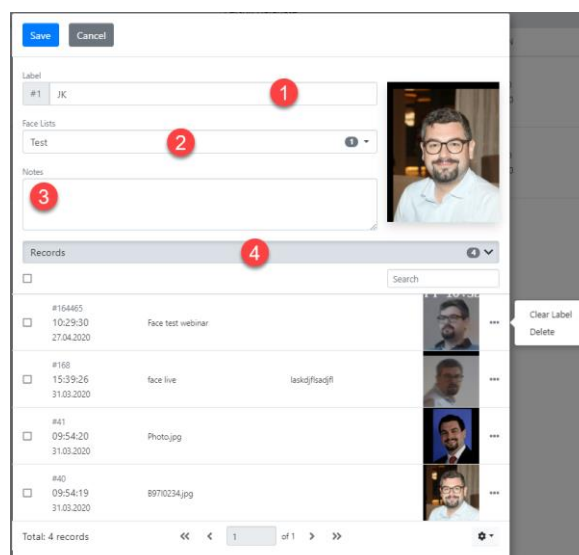
To start a session just click the session control, enter a session name and hit the play button. All results will immediately be assigned to the new session. If you want to switch a session just select the session you want to switch to and this will be the new session. If you want to delete a session just click the x beside the session name and the session and all associated faces will be deleted (don't worry, we will ask a second time if you really want to do it).

### 3.15.2 Person Database

The person database gives an overview of all labeled faces in the database. Its design is analogue to the face log and should be very intuitive to use. To get into the detailed view of a person, just click the list entry and the detailed view will pop up.

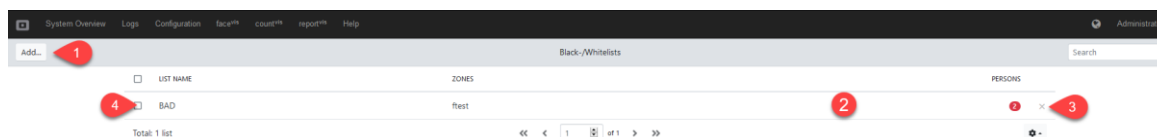


If you have selected a person the detailed view will pop up. It will enable you to change the label name of the person (1) to select the face lists that the person should be included in (2) and to comment on the person (3). Additionally, you will have an overview of all the labeled photos of the person (4) where you can manage the existing label easily.



### 3.15.3 Black-/Whitelists

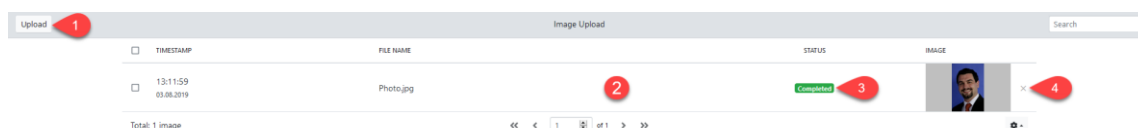
Black-/Whitelist view enables you to manage all lists within Face Pro. You can add a new list (1), edit the list by clicking its entry in the list (2), delete the list (3) or select it for multi delete (4).



The detailed view of a black-/whitelist enables you to edit/set the lists name (1), to edit/set the list type (2), to connect the list to certain face zones (3) and, of course, to set the persons that should be included in the list (4).

### 3.15.4 Image Upload

The image upload view enables you to upload and manage external images to the Face Pro system (for example to label certain persons that are not detected by the system yet. The image will be uploaded and sent to the least busy face server available automatically.



You can upload one or multiple images by clicking the upload button (1). After you have uploaded the images successfully, they will appear in the list (2) where you can select them for viewing individually if you want. As soon as the processing of the face is completed (this might take some time as we will search the picture for faces very thoroughly) the completed batch will appear left of the face in the list (3). If you want to delete a face from the system you can just do it by clicking the x in the list item (4). Images that have been uploaded will appear in the face log (see 3.15.1 above) for further processing.

### 3.16 SAIMOS® LPR

SAIMOS® LPR uses state of the art AI systems to detect, recognize and compare license plates. The user-friendly interface provides step by step configuration enabling fast setup times and reporting. LPR specializes on Black-/Whitelist real time alerting and flexible reporting of detected and recognized plates for free flow, parking and investigation.

#### 3.16.1 LPR Log

The LPR log is the central interface for SAIMOS® LPR. It shows all detected license plates as well as the black-/whitelist recognitions. The following screenshot shows an example of the LPR log and the different types of controls filters that are available will be explained in the following sections.

The screenshot shows the 'LPR Log' interface with the following components highlighted by numbered red circles:

- 1**: Filter control (checkbox icon)
- 2**: Export control (download icon)
- 3**: Live search field (search bar)
- 4**: Detail view control (row selection)
- 5**: Recognition/Alarm indicator (checkbox icon)
- 6**: Selector control (row selection)
- 7**: Page control (pagination)
- 8**: Page size control (dropdown menu)

TIMESTAMP	SOURCE	PLATE TEXT	ALARM	PHOTO
15:16:27 27.05.2020	lpr	W-1234567	—	
15:16:26 27.05.2020	lpr	W-1234567	—	
15:16:25 27.05.2020	lpr	W-1234567	—	
15:16:24 27.05.2020	lpr	W-1234567	—	
15:16:22 27.05.2020	lpr	W-1234567	—	
15:16:21 27.05.2020	lpr	W-1234567	Wohnung test	
15:16:20 27.05.2020	lpr	W-1234567	Familie test	
15:16:19 27.05.2020	lpr	W-1234567	—	
15:16:18 27.05.2020	lpr	W-1234567	—	
15:16:17 27.05.2020	lpr	W-1234567	—	

Total: 300 records

##### 1. Filter control

The filter control enables you to filter detections and recognitions. For more information about this control see 3.16.1.2.

##### 2. Export control

The export control enables you to export selected or all license plates currently in the LPR log. For more information see 3.16.1.3.

##### 3. Live search field

The live search field will help you to find detections or recognitions very fast. Just type some text in the search field and the current list will be limited to everything that matches the text.

##### 4. Detail view control

By clicking on a detection, the detailed view control will open and give further information about the detection / recognition (see 3.16.1.1).

##### 5. Recognition/Alarm indicator

If a plate is recognized it will be labeled with the recognition result and colored differently. Only alarms are currently labeled so don't worry if not all detections are labeled this way.

##### 6. Selector control

The selector control enables you to limit actions to selected items only. The possible actions are: Export and delete.

##### 7. Page control

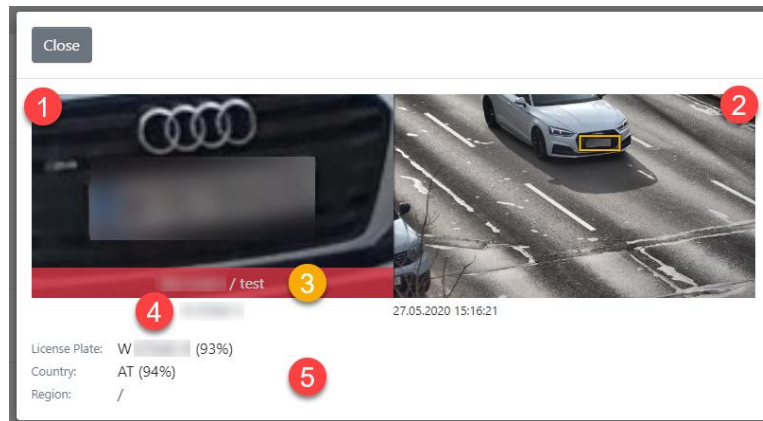
The page control simply allows you to switch between pages. Don't worry, selections are persistent even if you switch the page.

##### 8. Page size control

The page size control gives you the option to look at more or less faces per page. Be aware that the more plates you will display on one page the more time it will need to display the individual pages (all the images have to be loaded for a smooth display).

### 3.16.1.1 Detailed detection view

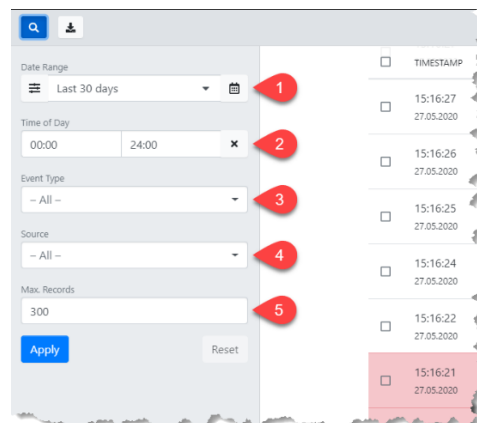
If you click on a detection within the LPR Log, the detailed view of this detection will be shown which gives you further information about the detected / recognized plate.



1. Cropped/Zoomed Plate image.
2. Overview image showing the detection of the plate with a yellow bounding box.
3. Recognition result and label (only if a recognition was successful).
4. The plate text that was detected.
5. Full License plate information with confidences of the detection.

### 3.16.1.2 Filter

The filter control enables you to filter the face log results by several criteria. This can help with searching and exports. The different filter options will be explained below.



#### 1. Date Range

The date range filter will enable you to filter by predefined date ranges (today, yesterday, last seven days) or a custom date range. To select a custom date range just click on the calendar day one time to select the start of the range and then a second time on the day for the end of the range. If you only click on one day, this day will be selected as the range.

#### 2. Time of Day

The Time of Day filter enables you to select only a certain time of day period for the selected date range.

#### 3. Event Type

You can filter by event type (Non-Alarm, Recognition Alarm, Detection Alarm).



## 4. Source

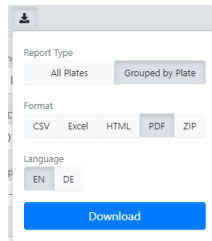
Filter the search for certain LPR zones only. Multiple selections are possible.

## 5. Max. Records

Set the amount of records that should be shown in the search result. Be aware that the more results are selected the less performant the page will be.

### 3.16.1.3 Export

The export control enables you to export the LPR log result. You can select multiple plates for export or export the whole log if you made no selections. There are multiple ways to export plates which are explained below.



## 1. Report Type

- a. All Plates  
Will export all plates in the list.
- b. Grouped by Plate  
Will export a grouped report of the selected plates. Same plates will be grouped together and the count of these plates will be reported in a first seen – last seen style. Creating such report might take longer than the standard All plates report. The grouping will only be done for document type exports and not the ZIP Download.

## 2. Download

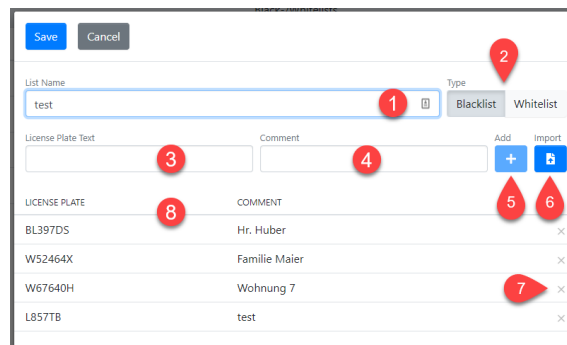
- a. CSV  
A simple CSV file will be exported.
- b. Excel  
An Excel containing the plate pictures will be exported.
- c. HTML  
A HTML file for viewing in a browser will be exported.
- d. PDF  
A PDF file will be exported (might take longer than the other document downloads as the PDF needs to be rendered beforehand).
- e. ZIP (Images)  
A zip file will be downloaded containing the plate images as well as the scene images for the selected detections. This type of Download might be very big and take a while. Do not export too many pages if you are in a hurry. We have dedicated scripts for a speedier export of raw image data. If you need support on export scripts, please contact us via email on [contact@saimos.eu](mailto:contact@saimos.eu).

### 3.16.2 Black-/Whitelists

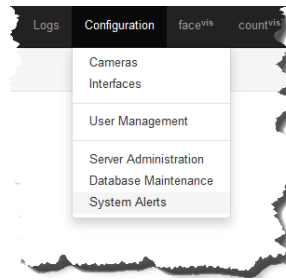
Black-/Whitelist view enables you to manage all lists within SAIMOS® LPR. You can add a new list (1), edit the list by clicking its entry in the list (2), delete the list (3) or select it for multi delete (4).



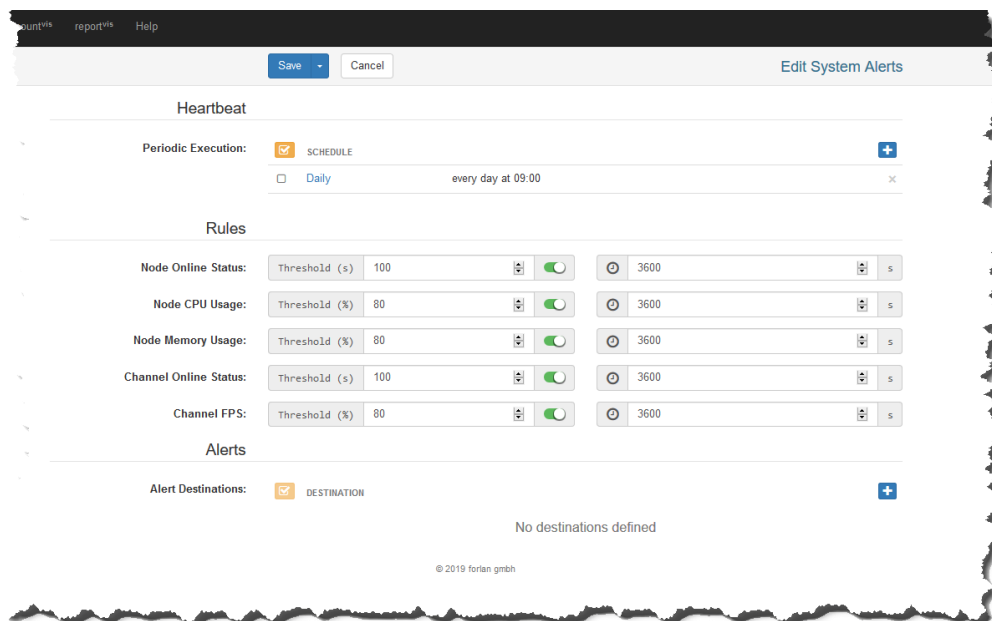
The detailed view of a black-/whitelist enables you to edit/set the lists name (1) and to edit/set the list type (2). You can add a new License Plate Text (3) and a comment for the plate (4). If you click the Add button (5) the license plate alongside with the comment will be saved to the current list (8). If you want to remove an entry from the list use the delete button (7). You can import a CSV file containing the License plate text and the comment for a mass import of plates (6).



### 3.17 System Alerts



System Alerts enable you to create alerts on critical system events or send a heartbeat report so you know the system is healthy. System alerts use the standard SAIMOS event reporting tools like email, http(s) command(s), TCP Trigger/Message and Milestone XProtect Analytic Events. You can configure the events and their trigger threshold to your liking.



#### 3. Heartbeat

Create a heartbeat report or trigger that sends an alive status to a third-party system. Configure one or multiple periodic executions to set the frequency of the heartbeat.

##### a. Periodic Execution

Set the schedule for your heartbeat by adding one or more periodic execution triggers. To add a trigger, click the + button. To remove a trigger, click the x button. Daily, weekly and monthly execution triggers are available.

#### 4. Rules

Configure the rules on what thresholds should be used to trigger alerts.

##### a. Node Online Status

Configure the maximum time a node is allowed to be offline in seconds and set the retrigger time (how much time should be between consecutive alerts).

##### b. Node CPU Usage

Set the maximum CPU usage that is allowed for the node in percent and set the retrigger time (how much time should be between consecutive alerts).

##### c. Node Memory Usage

Set the maximum memory usage of the node in percent and set the retrigger time (how much time should be between consecutive alerts).

##### d. Channel Online Status

Configure the maximum time a channel is allowed to be offline in seconds and set the retrigger time (how much time should be between consecutive alerts).

**e. Channel FPS**

Set the minimum percentage of frame rate compared to the average frame rate of the channel in percent and set the retrigger time (how much time should be between consecutive alerts).

**5. Alerts**

Set the desired alert types that should be sent and configure them accordingly. The following alert types are available:

- E-Mail
- Milestone
- HTTP(S)
- TCP

### 3.18 TCP Command Interface

The TCP command interface can parse plain ASCII Text commands and relay them to the SAIMOS VA server. This enables you to interact with the SAIMOS VA server via simple TCP commands (e. g. by using the Milestone Event Proxy or a Network I/O). Be aware that by enabling the TCP command interface you allow interaction with the SAIMOS VA system without authentication, therefore, be sure only to use the TCP command interface in networks that are secured. The TCP command interface is disabled by default.

On how to enable the TCP Command Interface look at the section [Server Administration](#).

#### 3.18.1 General command structure

**Command:**

TARGET:REQUEST:ARGS, . . .

**Answer:**

TARGET:ARGS, . . .:REQUEST\_ANSWER

**Example:**

groups:enable\_name:group1,group2

Enables Groups with the name group1 and group2 and will answer with:

groups:group1,group2:enabled

The command must not contain non ASCII characters.

#### 3.18.2 Targets, commands & parameters

Target	Command	Description	parameters	Answer
[groups,channels]	[enable,disable]_[id,name]	enable/disable groups/channels by group/channel IDs/names	[group_id,group_name],...	groups:[id,name],...:[enabled,disabled]
	events_[enable,disable]_[id,name]	enable/disable alarms for groups/channels by group/channel IDs/names		groups:[id,name],...:events_[enabled,disabled]
	scrambling_[enable,disable]_[id,name]	enable/disable scrambling (Scrambler) for groups/channels by group/channel IDs/names		groups:[id,name],...:scrambling_[enabled,disabled]
	static_scrambling_[enable,disable]_[id,name]	enable/disable static scrambling (Scrambler) for groups/channels by group/channel IDs/names		groups:[id,name],...:static_scrambling_[enabled,disabled]
	dynamic_scrambling_[enable,disable]_[id,name]	enable/disable dynamic_scrambling (Scrambler) for groups/channels by group/channel IDs/names		groups:[id,name],...:dynamic_scrambling_[enabled,disabled]
external	milestone	send milestone alert to a milestone event server	milestone_event_host, milestone_event_port, camera_ip, location, rule	NONE

### 3.19 SAIMOS VA Plugin

#### 3.19.1 About

SAIMOS VA CORE brings the power of the SAIMOS VA Framework to Milestone XProtect® in a fully integrated way. It provides different algorithms for several use cases like perimeter security, people counting and left/removed object detection. The combination of SAIMOS VA CORE and Milestone XProtect® enables users to profit from field proven analytics functionality of SAIMOS VA while using the full capabilities of Milestone XProtect® for a comprehensive solution experience. The SAIMOS VA CORE system is fully integrated into Milestone XProtect® Essential+ or higher via Plug-In and can be configured directly within the Milestone XProtect® Management Client.

#### 3.19.2 Requirements

##### 3.19.2.1 Minimal Software versions & prerequisites

Software	Version
SAIMOS VA Server	2020 R2
SAIMOS VA Node	2020 R2
Milestone XProtect	2018 R3 <ul style="list-style-type: none"> <li>• Essential+</li> <li>• Express+</li> <li>• Professional+</li> <li>• Expert</li> <li>• Corporate</li> </ul>
SAIMOS VA CORE Plugin	2020 R2 <ul style="list-style-type: none"> <li>• Visual C++ Redistributable 2015</li> <li>• .NET Framework 4.7</li> </ul>

##### 3.19.2.2 Minimal Performance requirements for SAIMOS VA

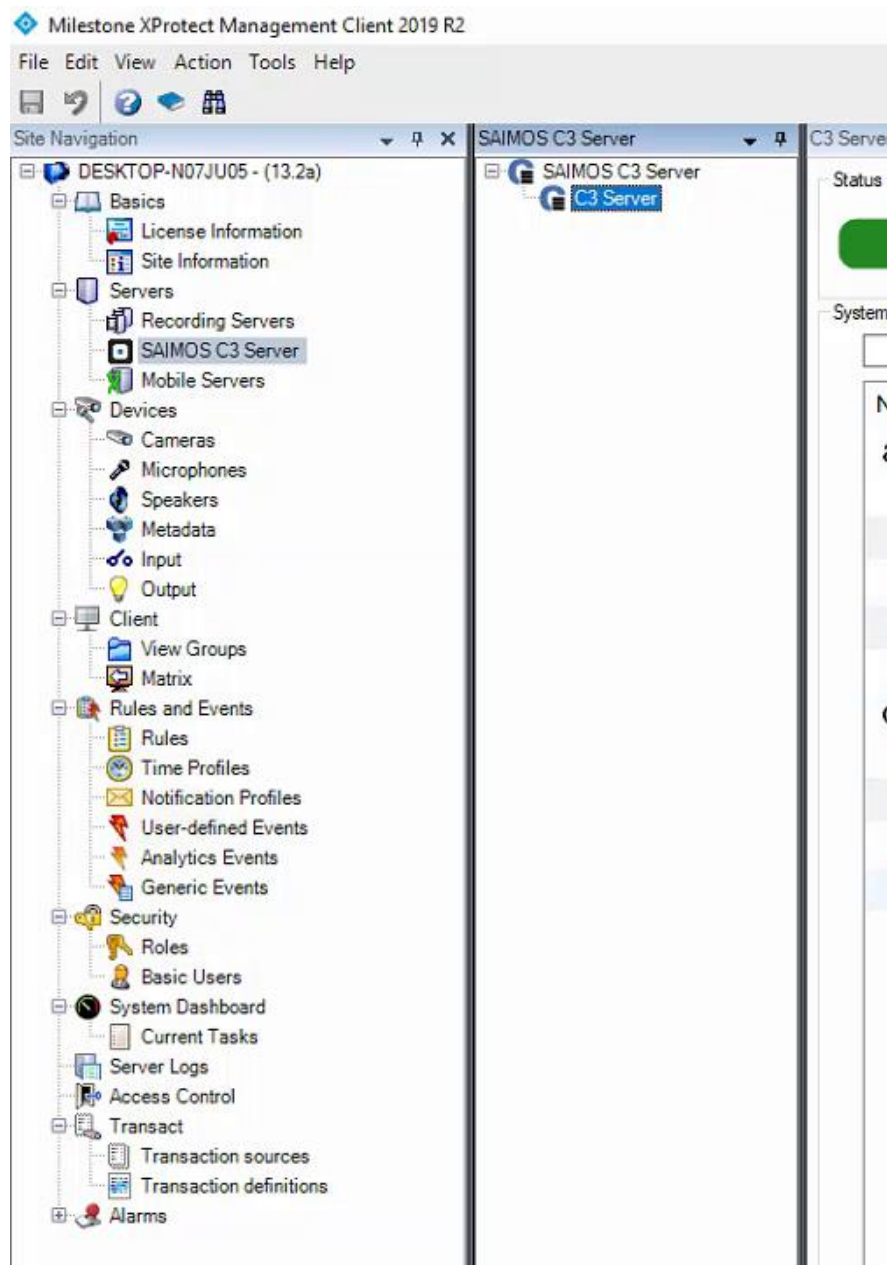
Component	min
CPU	Intel or AMD based CPU with 4 physical cores <a href="#">Passmark</a> : 5000 <a href="#">Single Thread Performance</a> : 1900
RAM	4 GB
HDD	50 GB
Network	Gigabit Ethernet
OS	Windows 10+, Windows Server 2016+ 64 Bit Ubuntu 18.04 64 Bit

#### 3.19.3 Installation

Just follow the guided installer of the plugin and it will do the rest for you. After successful installation of all components you should be able to configure SAIMOS VA core from within the Milestone XProtect Management Client. Within the Milestone Management Client the SAIMOS VA Server icon should be



visible in the Servers section ( ). If you click on the SAIMOS VA Server section you will be able to add SAIMOS VA Servers and start with your [configuration](#).

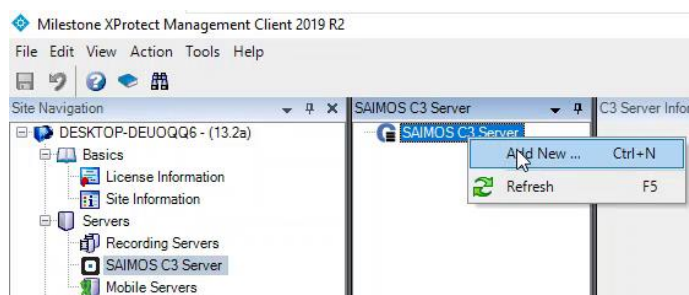


## 3.19.4 Configuration

This section will show you how to get a SAIMOS VA Server configured with Milestone XProtect and how to create a channel. It will give you some details on how channels work and what the most important settings are. Everything else you can find in our SAIMOS VA CORE Manual.

### 3.19.4.1 Add C3 Server

To add a SAIMOS VA Server to XProtect right click on the *C3Servers* entry in the *Servers* section of the Milestone XProtect Management Client and select *Add New ...*



A new dialogue will open where you can fill out the necessary information:

Section	Field	Description
General Settings C3 Server Configuration	Name	Your name for the new C3 Server. Choose wisely.
	Host	Host address on which the C3 Server is running Standard: <a href="https://localhost">https://localhost</a> If the server runs on a different machine localhost has to be switched for the IP of the host machine
	Port	The port on which the C3 Server is running Standard: 44444
	Username	Username for C3 Server authentication Standard: admin
	Password	Password for C3 Server authentication Standard: test
	Default Node	The default node to run C3 CORE channels on. If no node has been created yet, the plugin will create a node on localhost automatically.
	Test C3 Connection	Test your connection to C3.
Milestone Interface Configuration	Try Auto-Configuration	Try to find the best settings for Milestone configuration automatically (recommended)
	Host	IP or hostname of the Milestone Management Server
	Port	Port of the Milestone Management Server
	Username	Username with which the C3 Server should log into Milestone XProtect to communicate Windows authentication is required (basic users are not supported)
	Password	Password for the above username

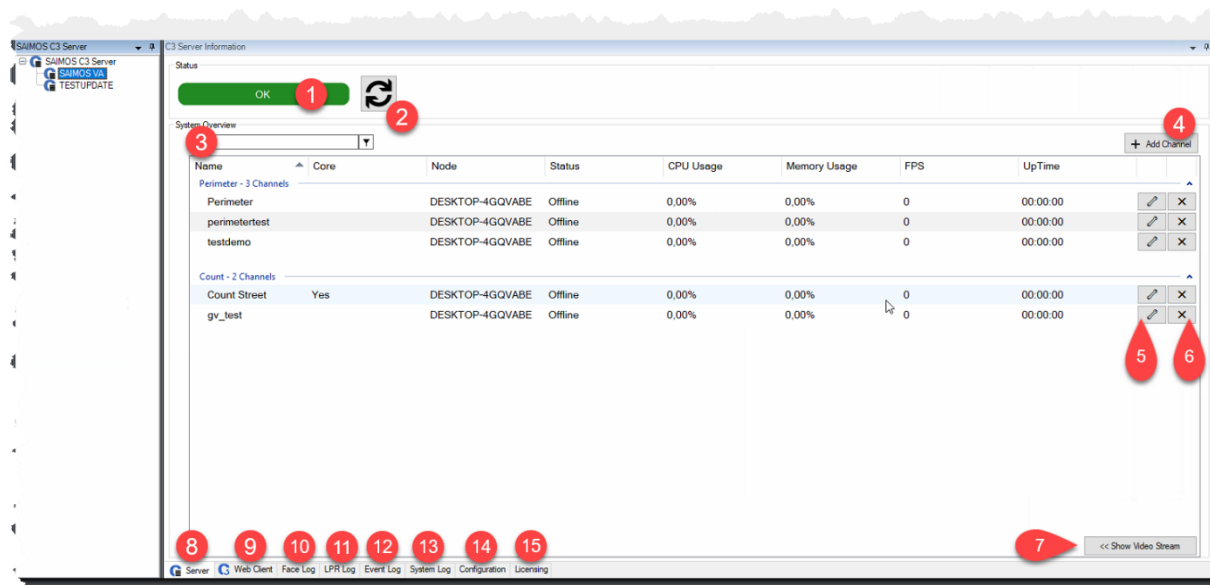


Section	Field	Description
	Events Port	Port where Analytic Events can be sent to XProtect Standard: 9090 Be sure the port is activated.
	Test Milestone Interface	C3 Test if the connection to Milestone from C3 is successful.

After you have entered the necessary information click **OK** to confirm. Now it can take a few seconds to add the server as the following automatic tasks are performed for you:

1. Server connection is tested
2. Milestone Interface within SAIMOS VA for communication is automatically generated.
3. Initial configuration is fetched from the SAIMOS VA Server

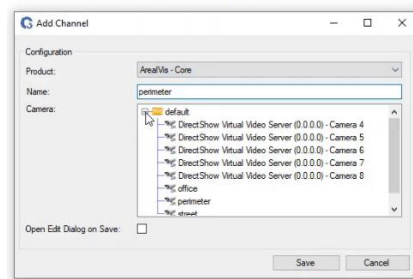
Now you should have successfully added the SAIMOS VA Server and you should see an empty Server view (if it is a fresh installation without any channels) and you are ready to create channels.



1. System Status shows you green if everything is OK, if it is not green something might not be right.
2. Use the refresh button to refresh the system status as well as the channel status.
3. Use the live search field to display only channels with certain text features.
4. Add a channel to the system.
5. Configure the channel.
6. Delete the channel.
7. Show the live video of the selected channel.
8. Server Tab with channel view. This is the central view of the plugin.
9. Use the Web Client for everything you cannot do from within other tabs in the plugin.
10. Take a look at the Face Log.
11. Take a look at the LPR Log.
12. Take a look at the Event Log.
13. Take a look at the System Log.
14. Show and change the server's plugin configuration.
15. Show the licensing of the SAIMOS® System.

## 3.19.4.2 Add CORE Channel

To add a CORE channels simply click on the *New* button on the bottom of the *SAIMOS VA Core Channels* view. A new dialogue will open and you will have to provide the following information:




Field	Description
Product	<p>Choose the product you would want the channel to run. Options are</p> <ul style="list-style-type: none"> <li>• Perimeter (perimeter and areal security)</li> <li>• Count (people and object counting)</li> <li>• Object (left and removed object detection)</li> </ul> <p>For each option you can choose between a standard channel (full SAIMOS VA channel) and a SAIMOS VA CORE channel.</p>
Name	Choose a name for your channel (choose wisely)
Camera	Select the camera from the chosen device group
Open Edit dialog on save	Check if you want to configure the channel immediately after creation. The plugin will open the edit dialogue automatically.

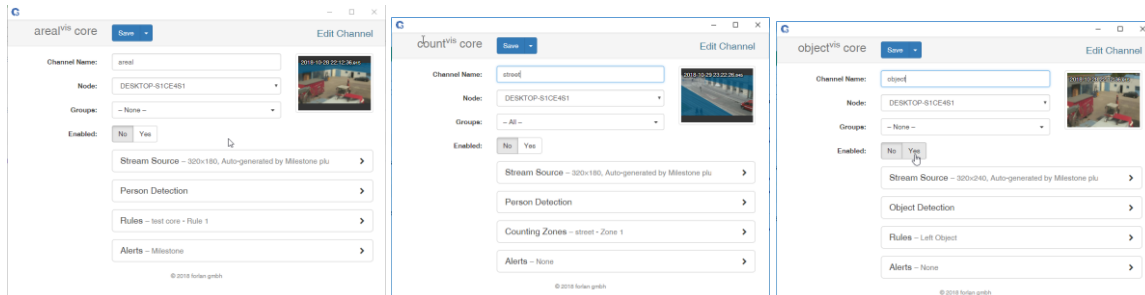
After you have entered the necessary information you can click OK to start the channel creation process. The following things will then happen automatically:

- The channel will be preconfigured with the chosen camera and the standard configuration
- Two zones/rules will be added to the channel (if applicable to the product)
- The Milestone Event forwarding will be created and activated (only Perimeter) for the channel
- The created zones/rules will be added to the Analytic Events of the XProtect systems in the following format
  - CHANNEL NAME - RULE/ZONE X
- The created Analytic Events will be added as Milestone Alarms automatically

The channel will be started automatically and is ready for final configuration using the *Edit* mode.

### 3.19.4.3 Configure a CORE channel

To configure an CORE channel select it within the *Core Channel View* and then right click and choose *Edit Channel* or click the  button on the right side of the channel. A new dialogue will open that will enable you to configure the channel.



As most things are done automatically on channel creation the most important things to define are:

- Perimeter
  - Person Detection and Rules
- Count
  - Person Detection and the Counting Zones
- Object
  - Object Detection and Rules

Everything else should be set for a first channel configuration.

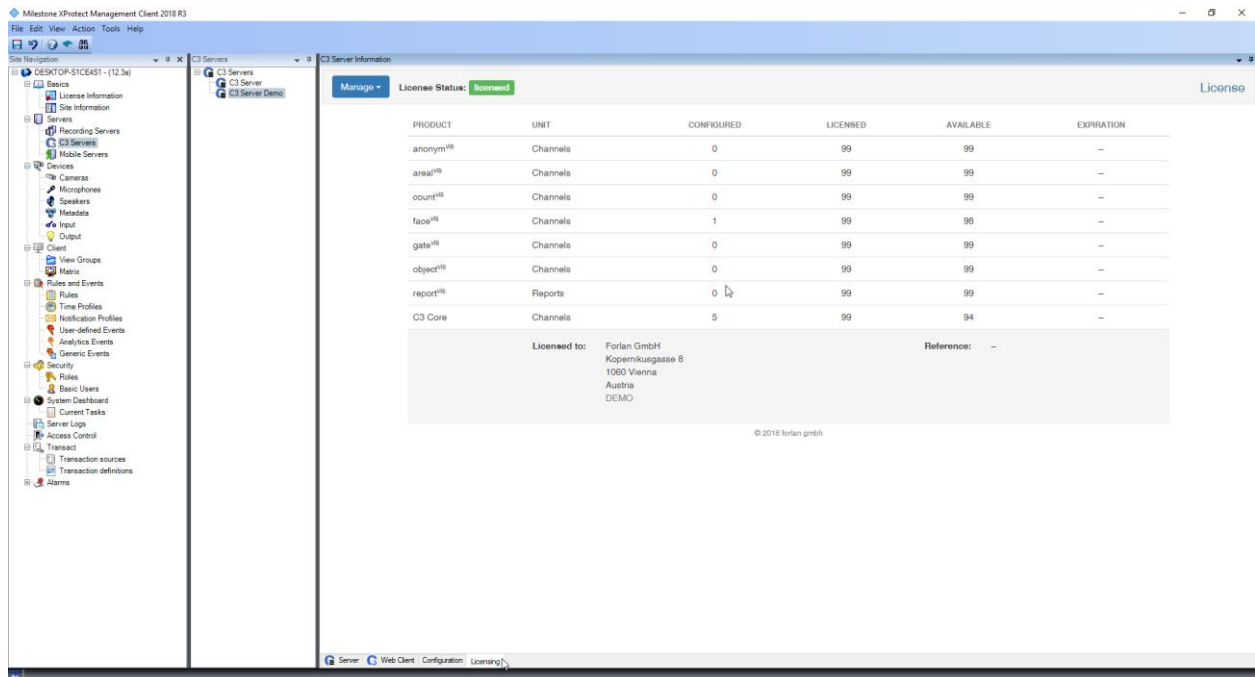
### 3.19.5 Licensing

The CORE plugin does not need to be licensed and is free to use. After installing the SAIMOS VA Server and at least one SAIMOS VA Node you will be able to use all product features for 30 days after installation without any limitations. After the trial period you will need to license your channels. After a license is expired (also the trial) all channels will stop working and will not start without a new license.

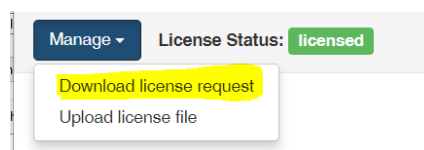
To License the product, you will need to complete the following steps:

1. Create a license request and download its ZIP file via the license management
2. Send the license request with your reference to [license@saimos.eu](mailto:license@saimos.eu)
3. Upload the license file once you received it from us (IMPORTANT: upload the license file as you receive it, do not UNZIP!)

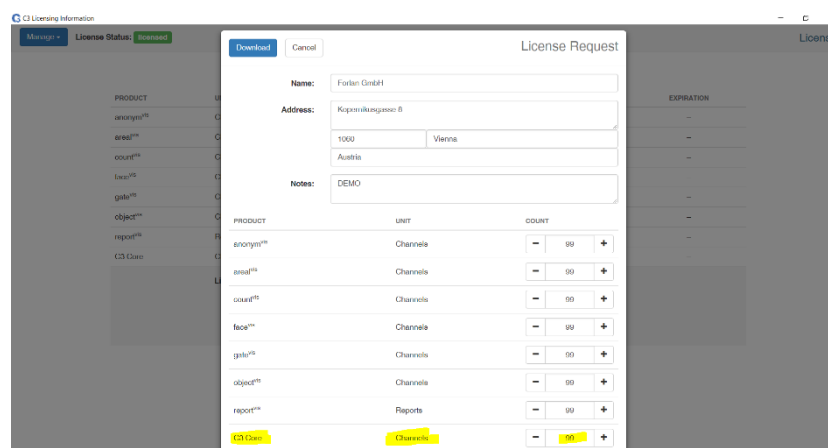
From within the XProtect Management Client click the *Licensing* to open the License Management.



The License Management dialogue will open and you will be able to see an overview of your licensing situation. To create a license request click *Manage* → *Download license request*.



The sub dialogue will enable you to enter your customer information as well as enables you to select how many licenses you want to acquire for your license. CORE channel licenses are managed under SAIMOS VA Core.

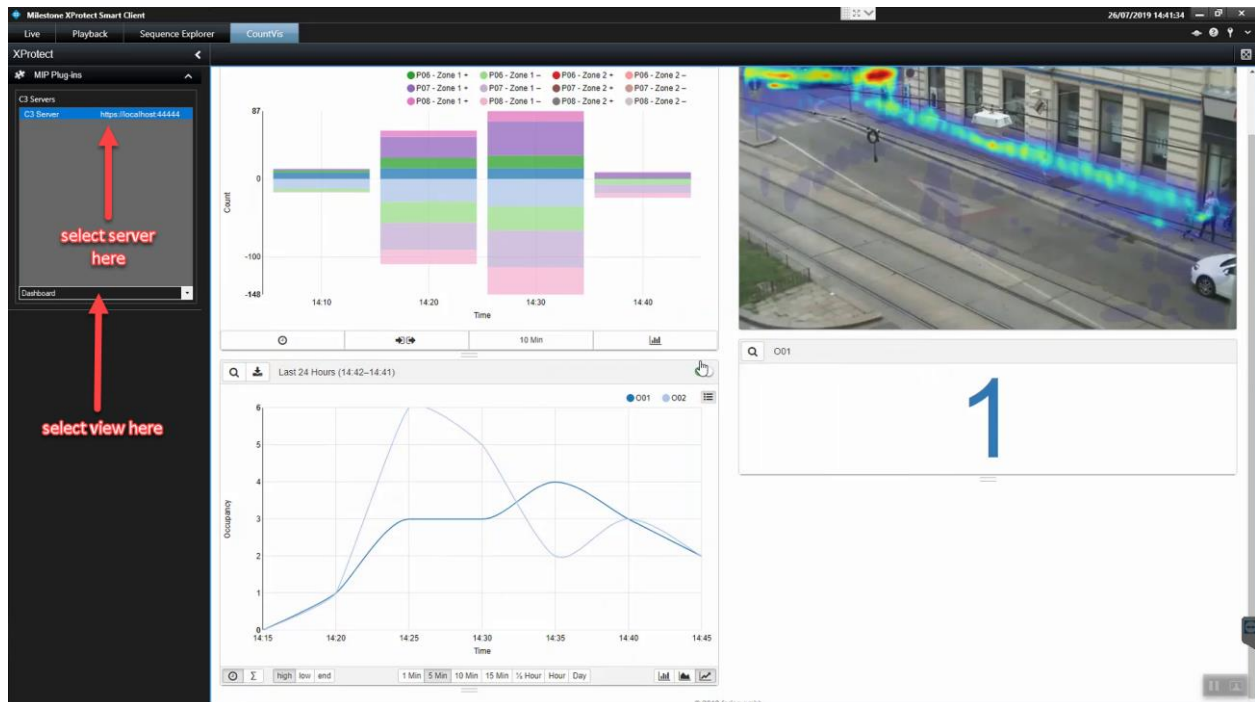


If you entered all necessary information. Click download to download the license request (license\_request.zip). Use the system dialogue to find a proper place to save it. After you have sent the license request to [license@saimos.eu](mailto:license@saimos.eu) after some time you will receive a license file back (ZIP). Use the ZIP file (don't extract) and upload it via the license manager. Using the

command *Manage* → *Upload license file*. After you have successfully uploaded the license file your system will be licensed.

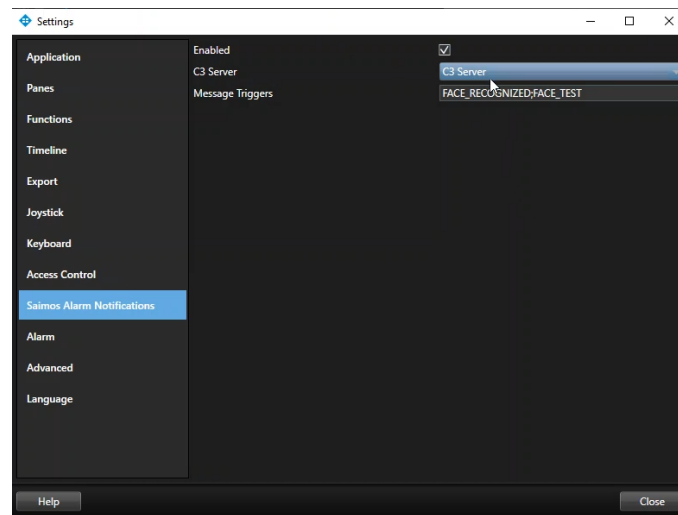
### 3.19.6 Count Plugin

If you have chosen a full install or chose to install the count plugin with custom installation, the Milestone Smart client will get an extension tab showing the count interfaces of SAIMOS VA Count within this tab. The usage of the plugin is pretty straight forward. If you have a SAIMOS VA Server already created you can choose this server and select the different count views the server provides. You can also fully make use of the Dashboard and combine different views. For further information on the count views please refer to the full SAIMOS VA Manual.



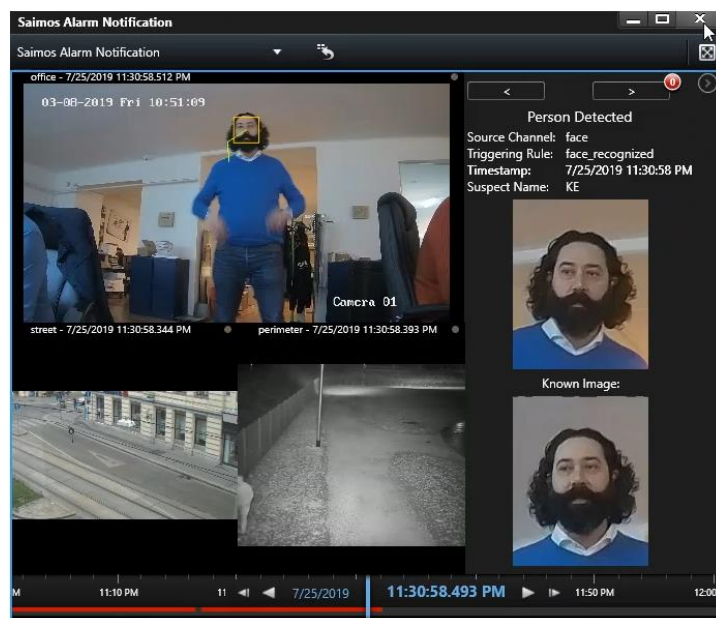
### 3.19.7 Face Plugin

If you have chosen a full install or chose to install the face pro plugin with custom installation, you will get the possibility to present face alerts from SAIMOS Face Analytics live with a special pop up view/custom view within the Milestone XProtect Smart Client. The pop up alarm is disabled by default, to enable it, go to the Milestone Smart Client *Settings* menu and tick the *Enabled* box within the *SAIMOS Alarm Notifications* section. You can also choose the appropriate SAIMOS VA Server you want to receive alarms from as well as the analytics message to listen for. The standard is *face\_recognized*.



If you have successfully configured the plugin for the right SAIMOS VA Server and analytics message and the Face Pro Analytics is sending Black- or Whitelist alerts to Milestone, you will be presented with a pop-up view that shows:

- The alarm camera with metadata (face and track)
- The person found with the archived image
- The person alerted with the current alert image
- A grid view of all related cameras of the Milestone Alert
- A control field to move to the next/previous alarm
- An alarm sound on pop-up creation (if alarm sounds are enabled within the smart client)



The pop-up view can also be permanently added to Milestone Smart Client as an independent view by using the setup menu and selecting the *SAIMOS Alarm View*.

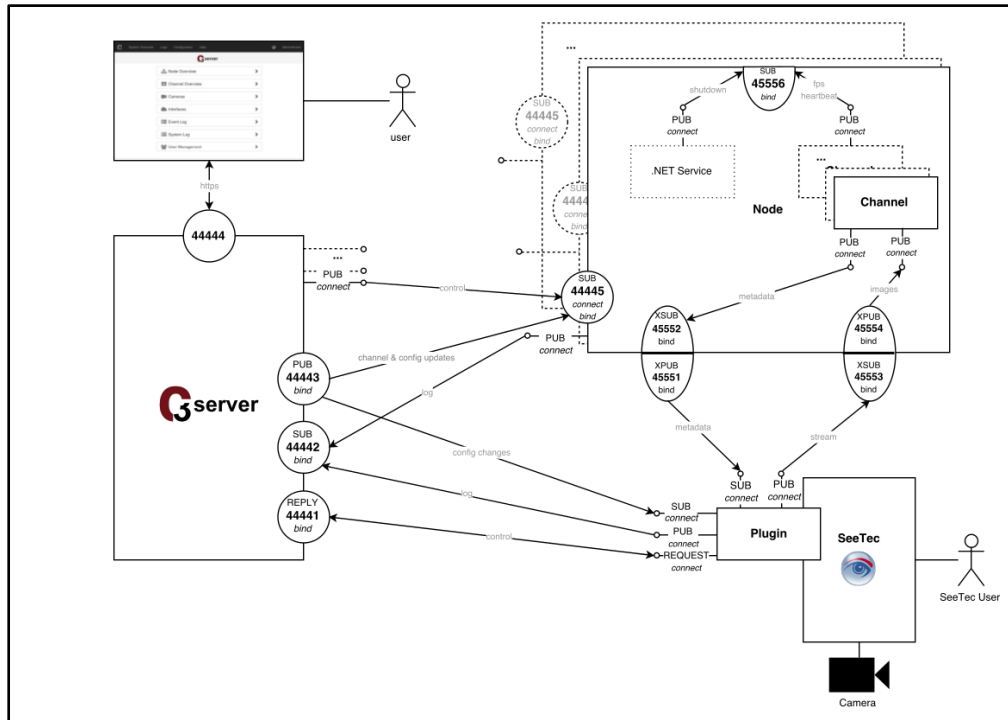
### 3.20 SeeTec Cayuga Plugin

The SAIMOS VA SeeTec Cayuga plugin enables the SAIMOS VA Server & Node to communicate with SeeTec Cayuga directly. You will be able to:

- add SAIMOS VA channels from directly within SeeTec

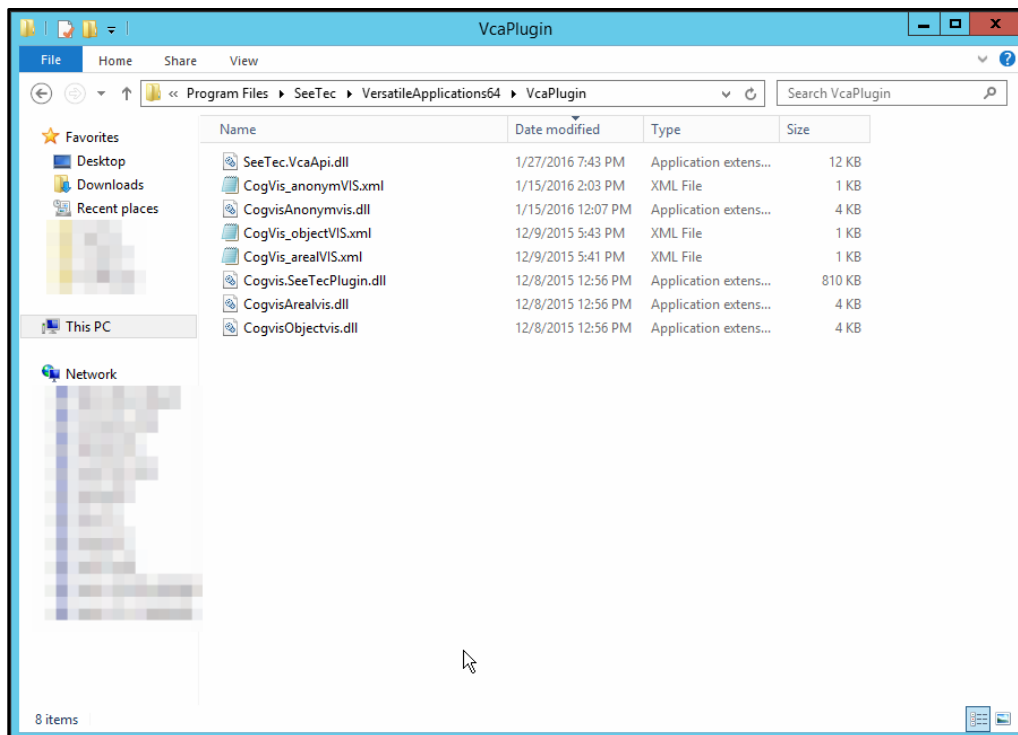
- get CCTV footage directly from SeeTec
- use SAIMOS VA rules as triggers from within the SeeTec Alarm management
- see metadata produced by SAIMOS VA channels using overlays directly in the Camera views of the SeeTec client

The SAIMOS VA SeeTec Cayuga plugin communicates via TCP/IP with the SAIMOS VA Server & Node(s). The communication architecture looks as follows:

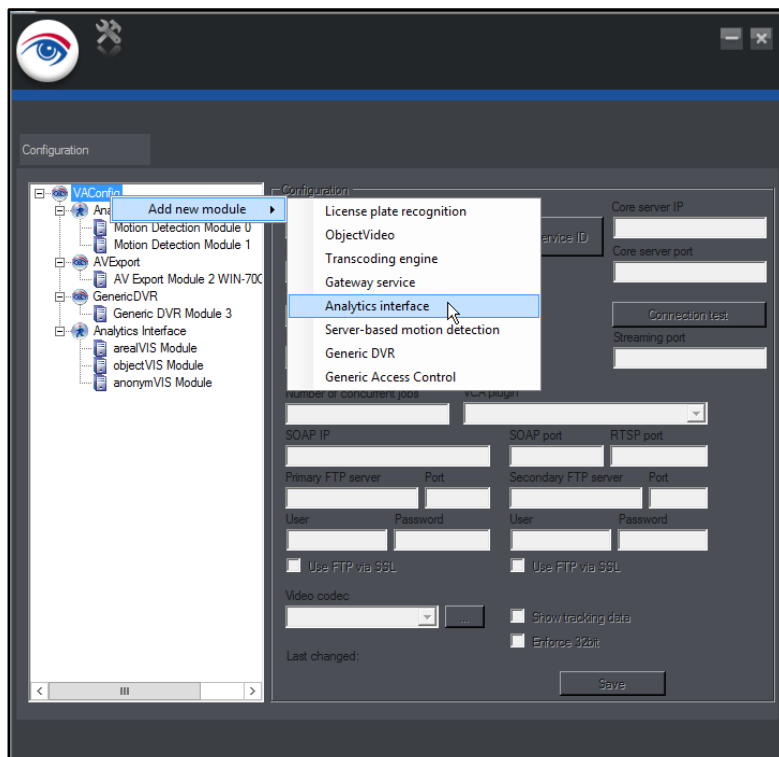


### 3.20.1 Installing the plugin

Before you install the plugin be sure that SAIMOS VA server and node have already been installed properly. To install the plugins first copy all the necessary plugin files (CogVis.SeeTec.Plugin.dll, CogVis\*.dll, CogVis\_\*.xml) to the SeeTec Plugin folder (VersatileApplications64\VcaPlugin for 64 bit or VersatileApplications\VcaPlugin for 32 bit). Normally this folder is located within the SeeTec installation folder (C:\Program Files\SeeTec). We recommend to use the 64-bit plugin.

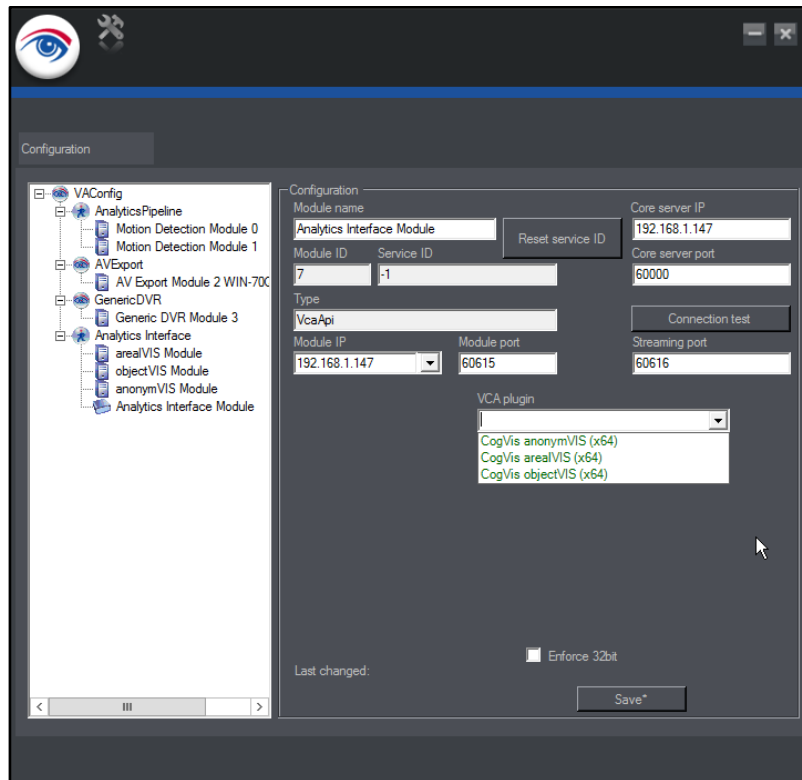


After copying the files open the SeeTec VA Administration and add a new Analytics interface. To do that right-click on the *VAConfig* entry in the left tree view and choose *Add new module --> Analytics interface*.

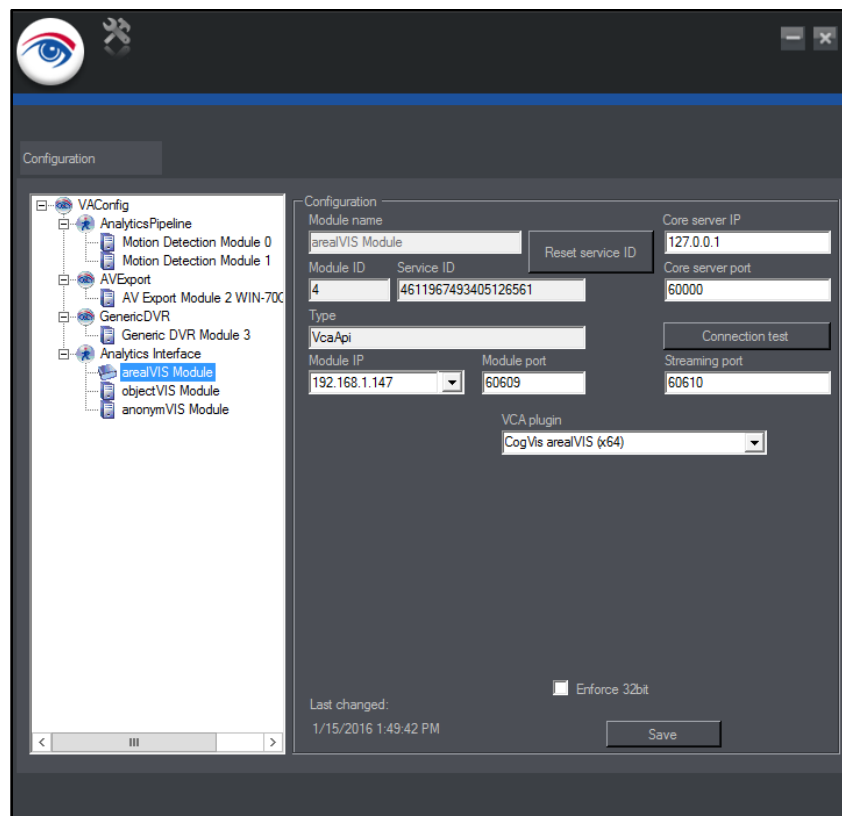


A new module will be added. You can now name the module by choosing a *Module name*. After that check that *Core server IP* and *Module IP* are configured correctly for your system. You now only have to select the correct VCA plugin within the drop down menu and click *Save*.

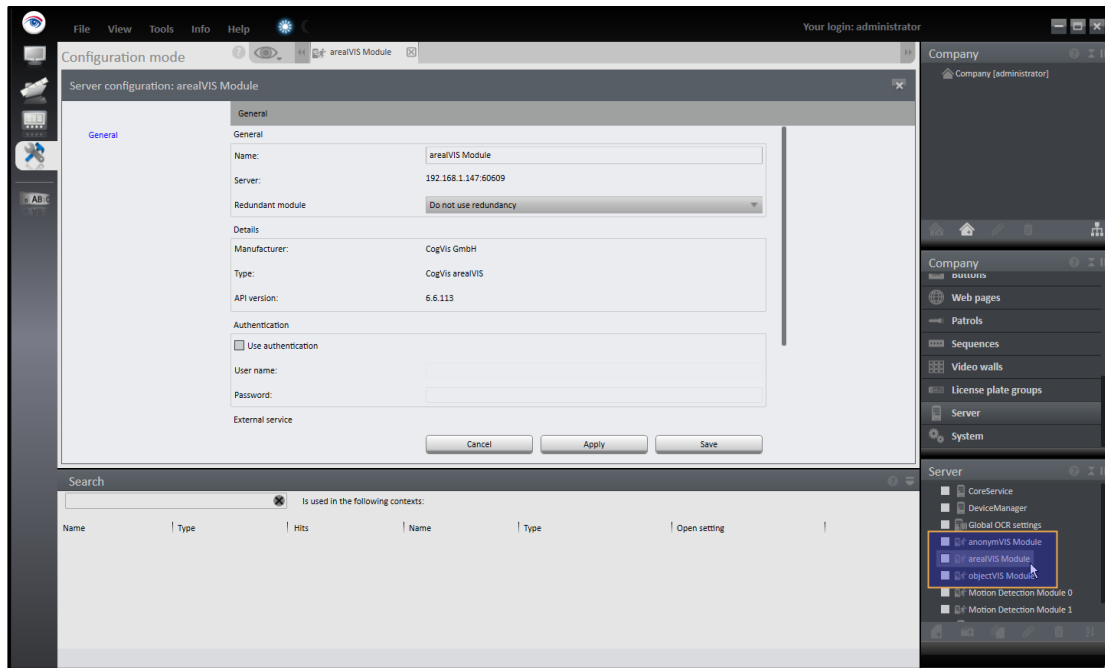




A correctly added module can look like this:

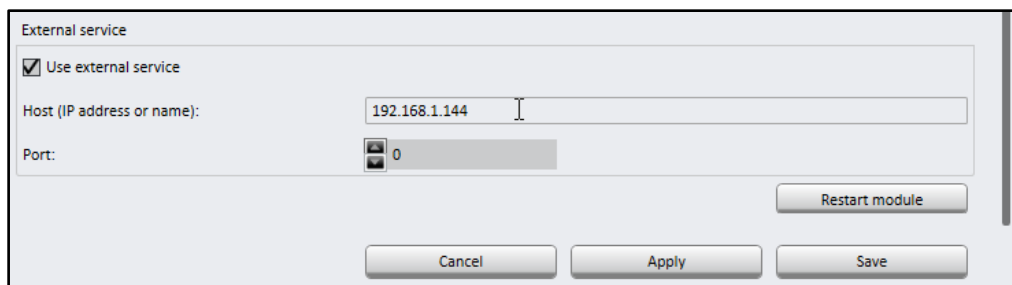


To ensure proper functionality, finally, please restart the *SeeTec* VA service. If everything worked well you should see the new SAIMOS VA interface within the *SeeTec* configuration under *Server*.



After you have found the correct Server module within the configuration, open its properties by clicking on it. Check the checkbox *Use external service* and enter the IP address of the SAIMOS VA server into the field *Host (IP address or name)*. After that restart the module or the *SeeTec VA* service. Now you are ready to install channels from within the *SeeTec* configuration.

*Note: If you did not change any standard Ports within the SAIMOS VA system you can leave the Port option at 0. Otherwise you would have to insert the communication port to the server in this field.*



### 3.20.2 Adding a channel

Before adding a channel, be sure you installed the plugin correctly. You can add a channel by adding a new item in *Other Hardware* within the *SeeTec* configuration. Choose a good Name for the channel (you cannot change it afterwards without hassle). The *Manufacturer* is *SeeTec Video Analytics* and the *Type* is *Generic VCA Channel*. Then you will be presented with the module options under *Video analysis module*. Be sure you select the correct module for the corresponding SAIMOS VA product and click *OK*.

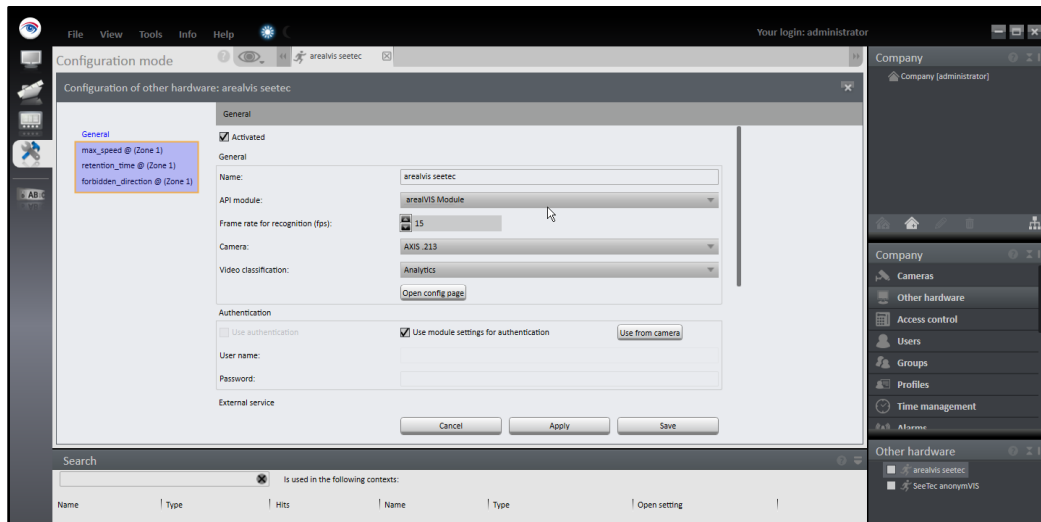
The module will be added and you will be presented with a configuration view of the module. Check the Entries for Name and *API module* (you can still change them before the module has been activated). Set *Frame rate for recognition (fps)* to your desired recognition frame rate (we recommend 15 fps), choose your *Camera and Video classification* (if you have a second stream configured just for the analytics). Now, be sure *Activated* is checked (top left checkbox) and click *Save*.

The channel should then come to live within the SAIMOS VA server interface on a node and you can start configuring it there.

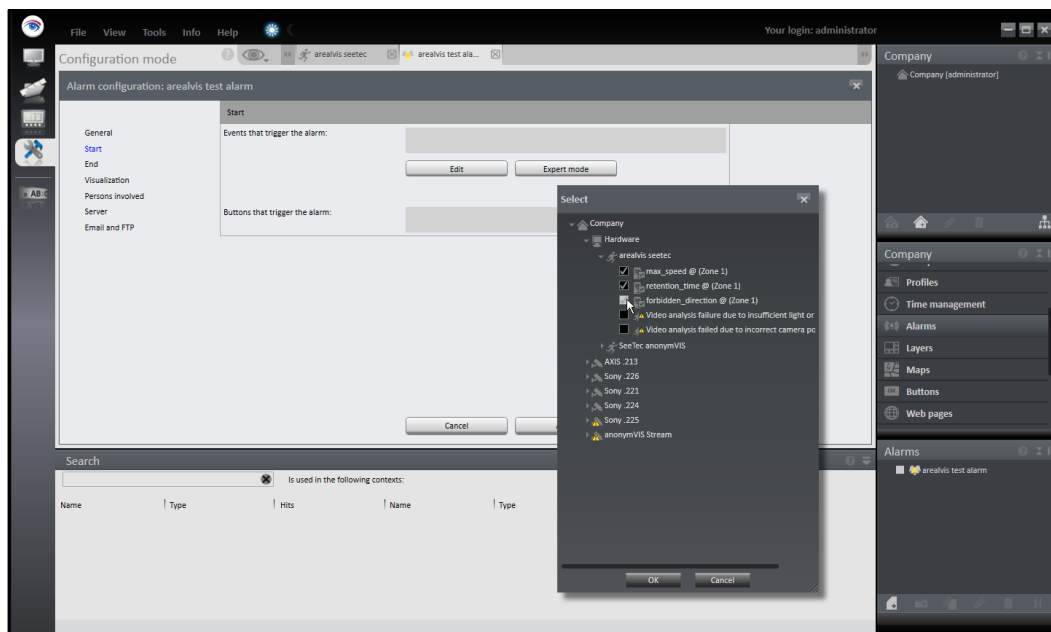
*Important: The channel will be already added with the correct stream source so you only need to change the Region of Interest within the Stream Source settings of the channel. Also, metadata and event forwarding to SeeTec will be handled automatically, you don't have to add a separate alert for that.*

### 3.20.3 Alert Management

If a channel has been successfully added to the system you can see the standard rules added to the channel within the *Other hardware* configuration (this will only apply to SAIMOS VA channels that actually send metadata).



The rules will comply with the rules added within the web configuration of SAIMOS VA. You can now connect these rules to a SeeTec alert. Therefore, you first have to add a new alarm within SeeTec or you can configure an existing alarm. Within the SeeTec alarm configuration you can then add the SAIMOS rules as a start event by selecting the channel within the *Hardware* section like here:



After clicking **OK** you can then continue to configure the alarm to your need.

### 3.20.4 Troubleshooting

If you have troubles, try to restart the VA service of SeeTec and check the plugin log of SAIMOS VA. It will be located on the Server where the SAIMOS VA plugin is installed in the folder `C:\ProgramData\CogVis3\plugin\log`. If you contact [office@for-lan.at](mailto:office@for-lan.at) please attach this log to the email/ticket.

## 4 System backup and restore

This section will help you in creating your backup strategy for SAIMOS VA using either the backup and restore routines of the SAIMOS VA package or simple Postgres backup strategy.

### 4.1 Backing up SAIMOS VA using PGSQL commands

Backing up SAIMOS VA is as simple as creating a DB dump of the SAIMOS VA system. You can use the in package PGSQL commands of SAIMOS VA (on windows) or the in System PGSQL commands on Ubuntu to back up. On windows the PGSQL binaries are located in C:\ProgramData\cogvis3\server\pgsql\bin

Full back up command example (all data is saved):

```
C:/ProgramData/cogvis3/server/pgsql/bin/pg_dump -h localhost -d cogvis -U cogvis -p 5432 -Fc -Z9 -f  
C:/ProgramData/cogvis3/server/c3_db_backup.dmp
```

### 4.2 Restoring SAIMOS VA from a backup using PGSQL commands

To restore a SAIMOS VA from a previous dump you will have to stop the SAIMOS VA server service first. After that you have to delete the old DB, create the new DB and dump the result into the new database. An example for the necessary commands (for Windows) can be found below:

Stop the Server Service:

```
net stop C3ServerService
```

Drop the old DB from the DB Server:

```
C:/ProgramData/cogvis3/server/pgsql/bin/dropdb -h localhost -U cogvis -p 5432  
cogvis
```

Create a new DB on the PGSQL server:

```
C:/ProgramData/cogvis3/server/pgsql/bin/createdb -h localhost -U cogvis -p 5432 -E  
UTF8 cogvis
```

Restore the dump into the new Database:

```
C:/ProgramData/cogvis3/server/pgsql/bin/pg_restore -h localhost -U cogvis -p 5432  
-d cogvis C:\Programdata\CogVis3\server\c3_db_backup_20181101T230942.dmp
```

Start the Server service again:

```
net start C3ServerService
```

### 4.3 Using the SAIMOS VA Scripts

On Windows you can make use of the additional script for backup and restore c3br.exe (c3br.py) in the server root folder (C:\ProgramData\cogvis3\server).

Script options:

SAIMOS C3 DB backup and restore script

positional arguments:

{backup,restore}      select between backup or restore

optional arguments:

-h, --help              show this help message and exit

backup options:

-o OUTPUT, --output OUTPUT

Output path of the backup file

-e, --essential          Backup only essential configuration data instead of fully

restore options:

-i INPUT, --input INPUT

Full path to the backup file

general options:

-b BINARY, --binary BINARY

Binary path for postgresql

-u USER, --user USER    User for PGSQL C3 user

-p PASSWORD, --password PASSWORD

Password for PGSQL C3 user

#### 4.3.1 Examples

Full back up to the C:\ProgramData\cogvis3\server folder:

```
C:\ProgramData\cogvis3\server\c3br.exe backup
```

Essential backup saving only the necessary configuration files (small backup) to a user folder:

```
C:\ProgramData\cogvis3\server\c3br.exe backup -e -o C:\Users\user\Documents\c3backups
```

Restore from a backup dump in the C:\ProgramData\cogvis3\server folder:

```
net stop C3ServerService
```

```
C:\ProgramData\cogvis3\server\c3br.exe restore -i
```

```
C:/ProgramData/cogvis3/server/c3_db_backup_20181103T222458.dmp
```

```
net start C3ServerService
```