Manual

Version 3.2.1

Compiled on 10.12.2018

Contents

1 About C3 5
2 Node 6
2.1 Before installing C3 Node 6
2.1.1 System Requirements 6
2.1.2 Installation package contents 6
2.1.3 Network communication 6
2.2 Installation 6
2.2.1 Windows 6
2.2.2 Linux 8
3 Server 9
3.1 Before you install 9
3.1.1 System Requirements 9
3.1.2 What will be installed 9
3.1.3 Network communication 9
3.1.4 Upgrade from 3.0.x to 3.1.x 9
3.1.5 Upgrade from 3.1.x to 3.2.x 10
3.2 Installation 11
3.2.1 Windows 11
3.2.2 Linux 14
3.3 Licensing 15
3.3.1 The licensing page 15
3.3.2 Download a license request 15
3.3.3 Upload a license file 16
3.4 Snapshot / Live View Component (> 3.1.6) 18
3.5 Node Management 19
3.5.1 Node Overview 19
3.5.2 Automatic Node Detection 19
3.5.3 Adding a Node manually / Node options 20
3.5.4 Enable / Disable / Delete a Node 21
3.5.5 The Channel View 22
3.5.6 Add a channel 22
3.5.7 Enable / Disable / Delete a channel 23
3.5.8 Migrate channel(s) 23
3.5.9 Restart channel(s) 24

3.6 Cameras 25
3.6.1 Camera overview 25
3.6.2 Automatic camera detection 25
3.6.3 Add / Edit Cameras 26
3.7 Interfaces 29
3.7.1 Milestone VMS 29
3.7.2 Multieye VMS 30
3.7.3 SMTP Server 31
3.7.4 Modbus Server 32
3.8 Channel configuration 33
3.8.1 Overview and general settings 33
3.8.2 Stream Source 33
3.8.3 Alerts 36
3.8.4 areal^{vis} 38
3.8.5 object^{vis} 43
3.8.6 gate^{vis} 45
3.8.7 anonym^{vis} 45
3.8.8 count^{vis} 46
3.8.9 Motion Detectors 50
3.9 Event Log 55
3.9.1 Filter 55
3.9.2 Event Image / Alarm Sequence 56
3.10 System Log 58
3.10.1 Filter 58
3.11 User Management 60
3.11.1 The User View 60
3.11.2 The Group View 61
3.12 Server Administration 63
3.12.1 Network Configuration 63
3.13 Database Maintenance 64
3.13.1 Database Cleanup 64
3.13.2 Learning Data Export 64
3.14 count^{vis} Control 65
3.14.1 Dashboard 65
3.14.2 Counting statistics 66
3.14.3 Counting statistics filter menu 66

3.14.4 Heatmap 67
3.14.5 Occupancy monitor 69
3.14.6 Occupancy areas 70
3.14.7 Occupancy statistics 71
3.15 TCP Command Interface 73
3.15.1 General command structure 73
3.15.2 Targets, commands & parameters 73
3.16 SAIMOS C3 CORE Plugin 74
3.16.1 About 74
3.16.2 Requirements 74
3.16.3 Installation 74
3.16.4 Configuration 75
3.16.5 Licensing 78
3.17 SeeTec Cayuga Plugin 81
3.17.1 Installing the plugin 81
3.17.2 Adding a channel 84
3.17.3 Alert Management 85
3.17.4 Troubleshooting 86
4 System backup and restore 87
4.1 Backing up C3 using PGSQL commands 87
4.2 Restoring C3 from a backup using PGSQL commands 87
4.3 Using the C3 Scripts 87
4.3.1 Examples 88

1 About C3

C3 is the analytic framework of SAIMOS®. C3 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 C3 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 9 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 6 to get all the necessary information.

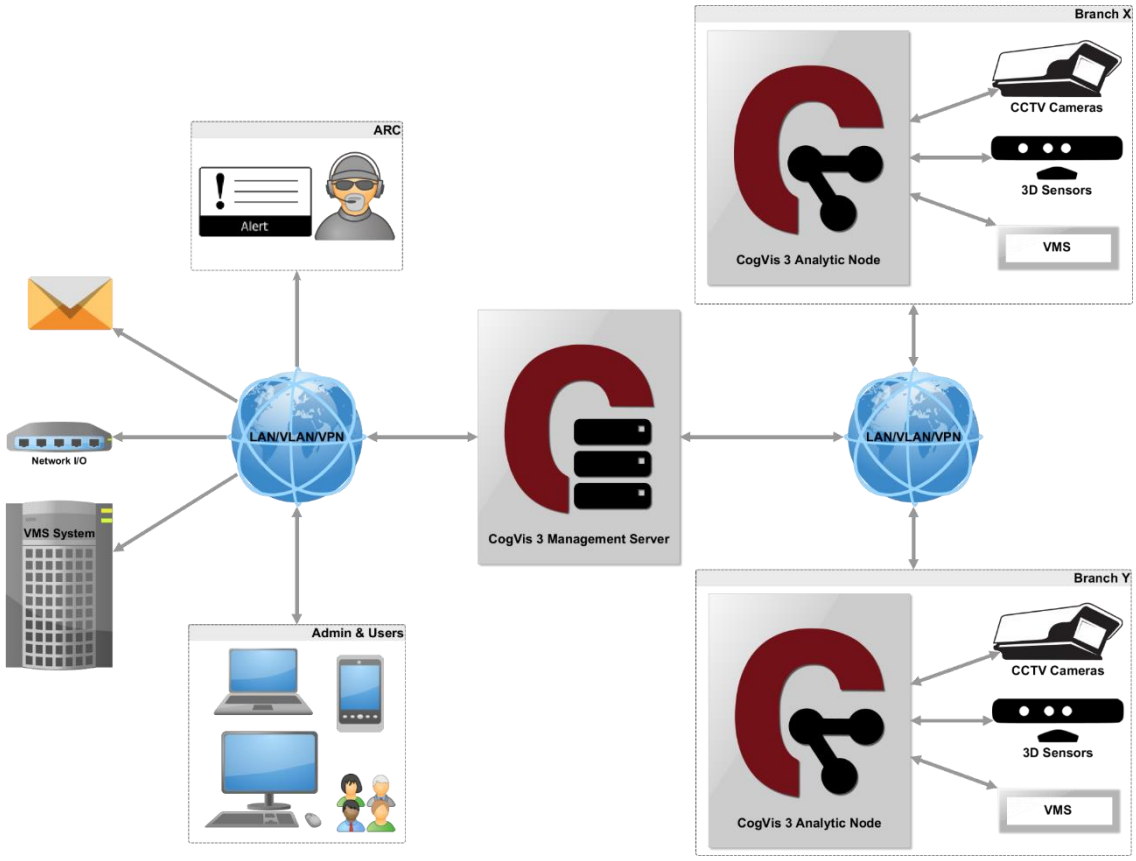


Image 1: The C3 architecture explained

2 Node

The C3 analytics node is a standalone service that will automatically manage channels that are added by the C3 Management Server. Therefore, as a prerequisite for managing a C3 Node a C3 Management Server has to be set up successfully (see below).

2.1 Before installing C3 Node

2.1.1 System Requirements

- OS (64 bit)
  - Windows: 7, 8, 8.1, 10; Server 2008 R2, 2012, 2012 R2, 2016
  - Linux: Ubuntu 16.04/18.04 LTS
- Memory
  - min. 2 GB RAM
- Harddisk
  - min. 4 GB
- Network
  - min. 100 Mbit network

2.1.2 Installation package contents

- Microsoft Visual C++ 2010 Redistributable Package (x64) --> Windows only
- CogVis 3 Node Package

2.1.3 Network communication

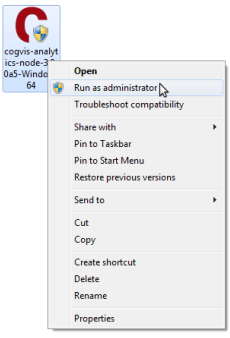
The following network ports are used by the C3 node & server and should not be blocked by a firewall:

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

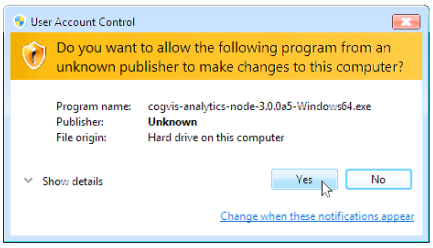
2.2 Installation

2.2.1 Windows

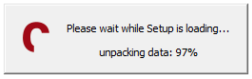
First, right-click the installer file and select “Run as administrator” to grant administrator rights to the installer.

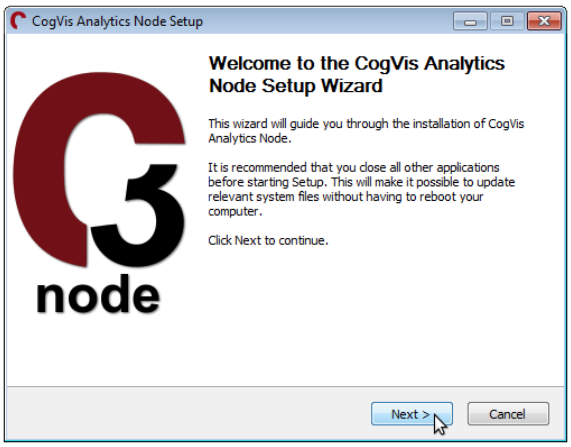


In case of a warning a dialog from “User Account Control”, select “Yes” to confirm administrator rights to the C3 installer.

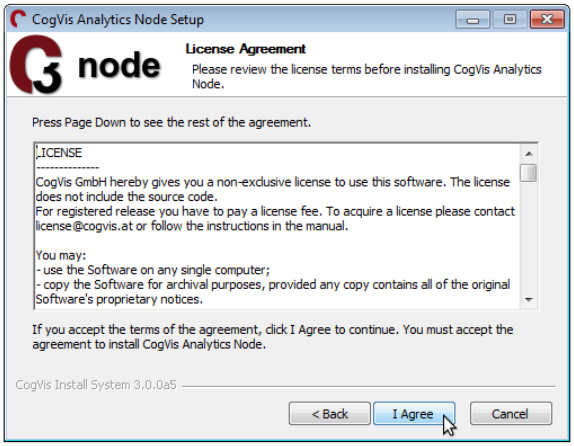


After the installer has loaded (i.e. checked its integrity and unpacked the compressed object) the (left), the welcome page of the Installer is displayed (right).

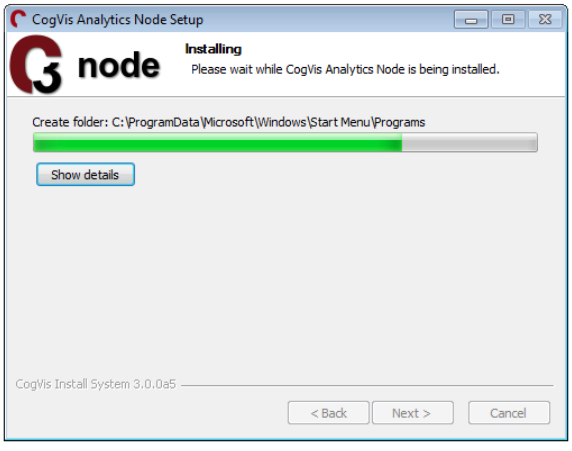




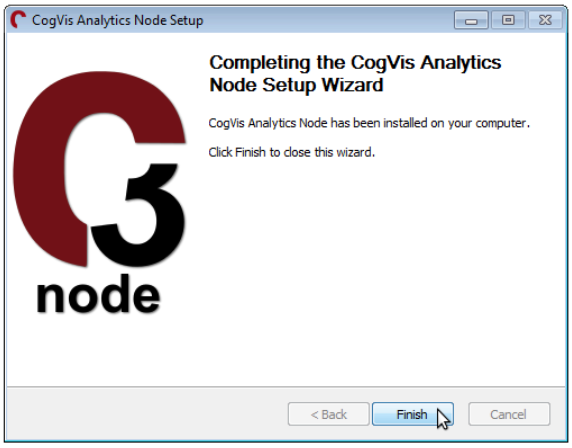
Click Next > to continue. This will land you on the License Agreement page.



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 C3 Node icon in the Windows Taskbar.

If you see the black node icon within red C3 C 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 C3 Server Manager to manage the newly installed node.

2.2.2 Linux

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

3 Server

The C3 Server is a single-page web interface for the management of distributed C3 Analytic Nodes.

3.1 Before you install

3.1.1 System Requirements

- OS (64 bit)
  - Windows: 7, 8, 8.1, 10, 2008 R2, 2012, 2012 R2
  - Linux: Ubuntu 16.04/18.04 LTS
- Memory
  - At least 4 GB RAM
- Harddisk
  - At least 50 GB free disk space
- Network
  - At least 100 Mbit network
- Browser
  - C3 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, Internet Explorer 11+

3.1.2 What will be installed

- Python 2.7 (if not already installed for all users)
- Microsoft Visual C++ 2010 Redistributable Package (x64) (Windows OS only)
- PostgreSQL 10.x
- C3 Server Package

3.1.3 Network communication

The following network ports are used by the C3 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 C3 server
4. Rename <C3>\db to something else, e.g. db-9.3
   On Windows it is located at C:\ProgramData\cogvis3\server\db
5. Install new C3 server package
6. Stop the new C3 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

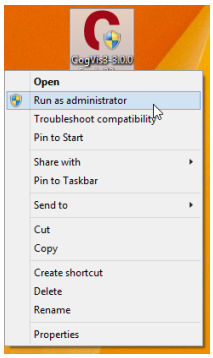
Due to a PostgreSQL upgrade from 9.5 to 10.5 the database has to be migrated before installing the new 3.2.x versions. To upgrade follow the following steps:

Use the same procedure as described in 3.1.4.

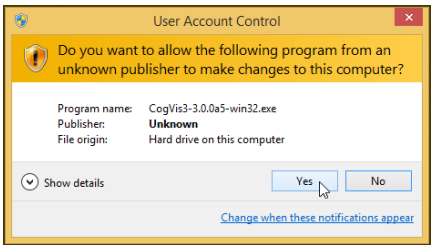
3.2 Installation

3.2.1 Windows

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

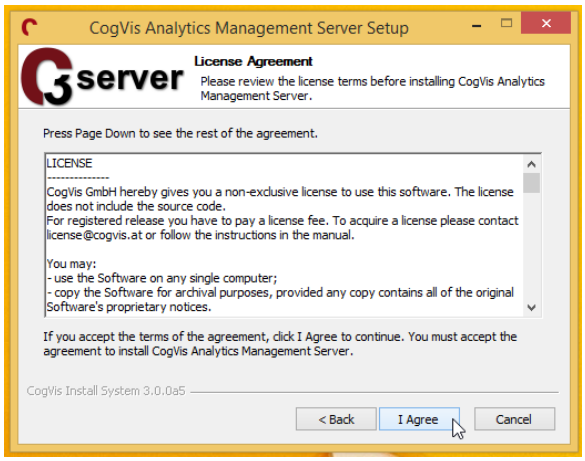


In case of a warning dialog displayed from *User Account Control*, select *Yes* to confirm the administration rights to the CogVis installer.

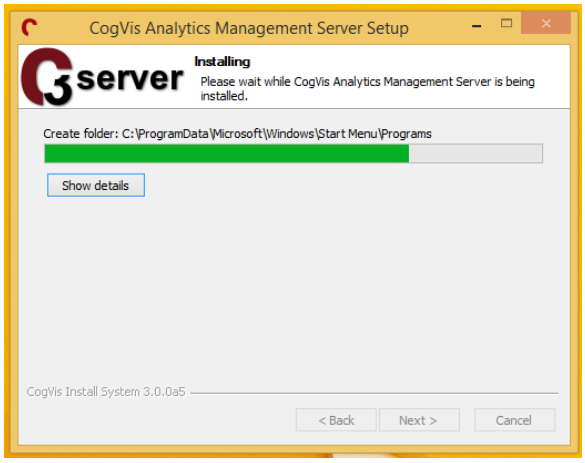


After that the installer is loading (i.e. checking its integrity and unpacking the compressed object). Once finished the Installer window is opened showing the welcome page for the installation. .

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.

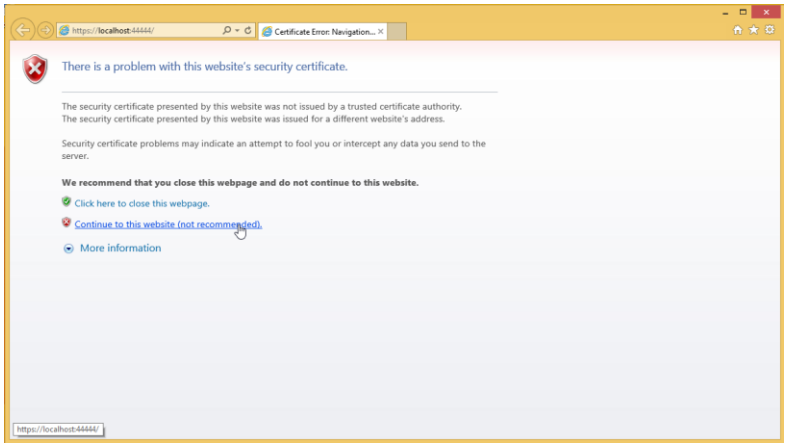


Be patient, this can take some time …

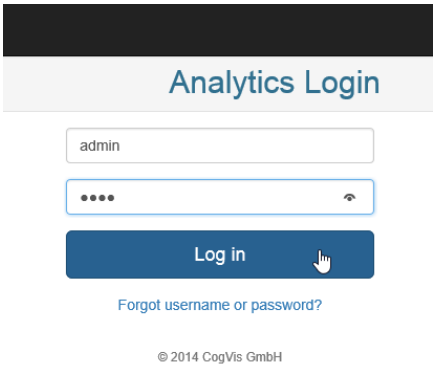
After the CogVis Analytics Management Server has been installed on your computer, click *Finish* to complete the installation process. If the installation was successful the CogVis Server Manager icon is displayed in the Windows taskbar.

A black server icon within the red CogVis “C” 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, to show the application (which will open the web UI in your default browser) or to exit the server service manager.

Clicking on *Show Application* will open your default browser. 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 CogVis Server web UI.

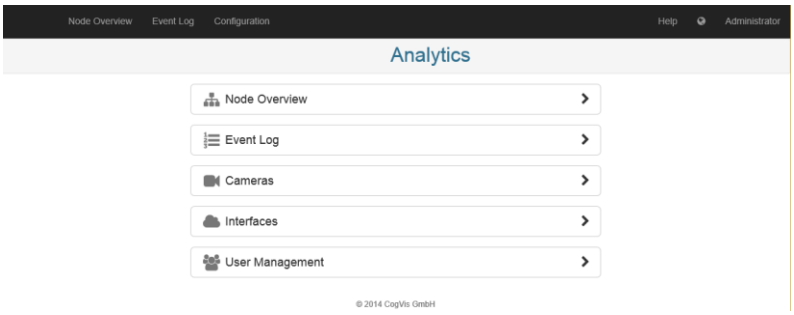


Enter the default credentials and click the *Log in* button:

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>
```

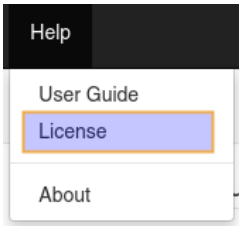
3.3 Licensing

The C3 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 C3, 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.

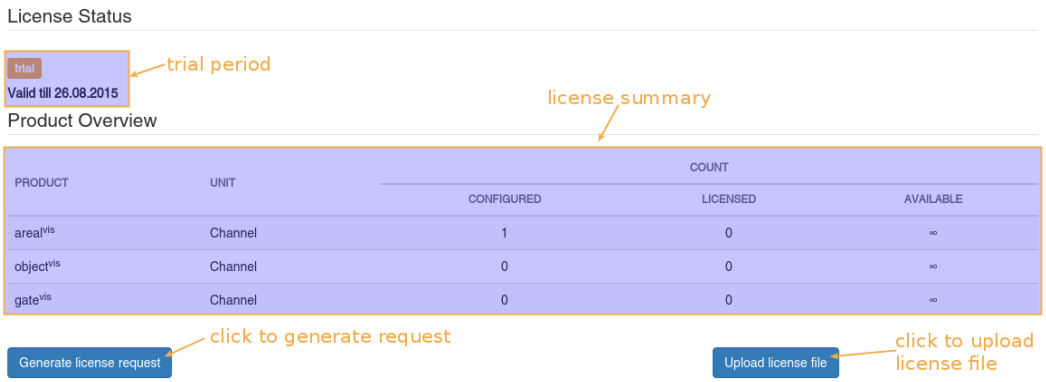
To purchase a license, a license request (see below) has to be sent to either a trusted CogVis partner or directly to office@for-lan.at. In return you will receive a valid license for the requested product channel(s). This license has to be uploaded to the management server. In case of any problems occurring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

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).

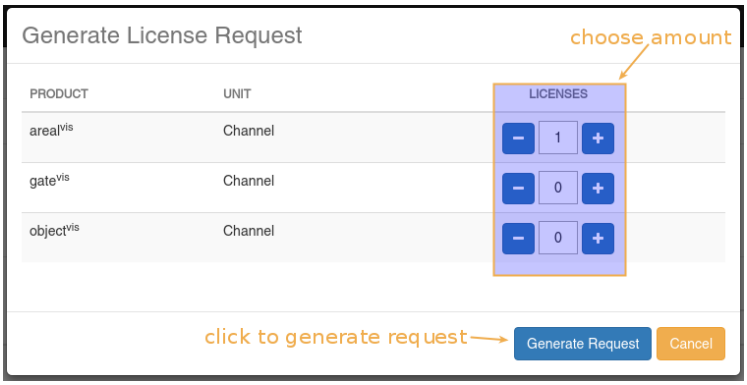


Note: As mentioned above, the trial-version of CogVis C3 is provided with full functionality. Also, the number of channels is not limited within the trial period. Hence, the test-system can be set up, modified and tested for any scenario or of any dimension.

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. 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 of a specific product or by overwriting the displayed number of licenses in the text field.

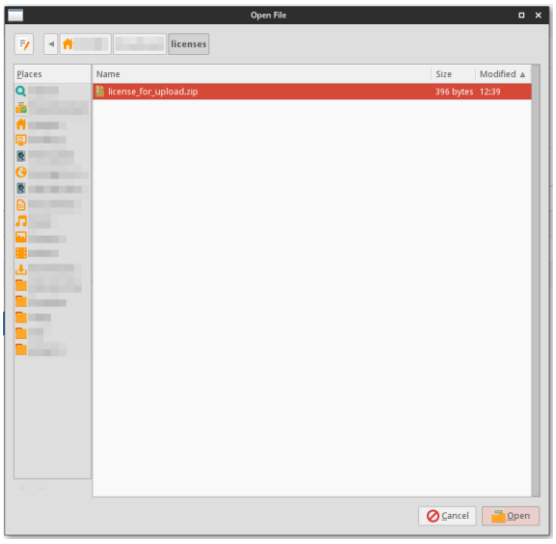


After you have finished selecting the licenses you want to purchase, click *Download* to generate a license request package. Send the ZIP-file (as it is) to either your preferred CogVis reseller or to license@cogvis.at to obtain the requested licenses.

3.3.3 Upload a license file

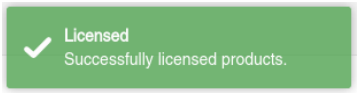
If the request was successful, you will have received a valid license file from CogVis or your CogVis reseller and are ready for the second and final step in licensing the channels:

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

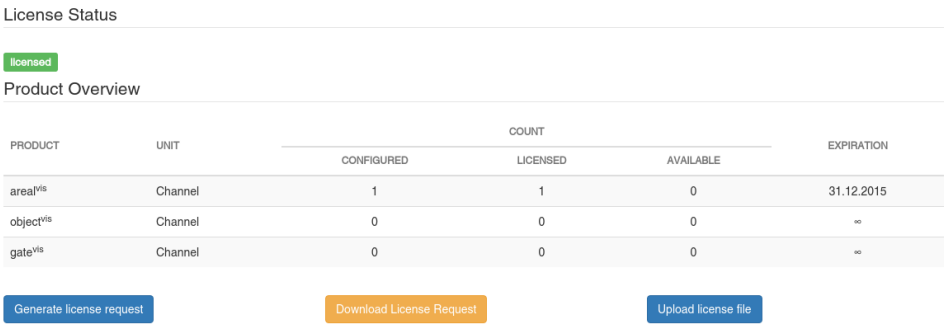


Note: Please update the ZIP file as it is, i.e. do not unpack it before uploading.

If the upload was successful the following message is displayed:



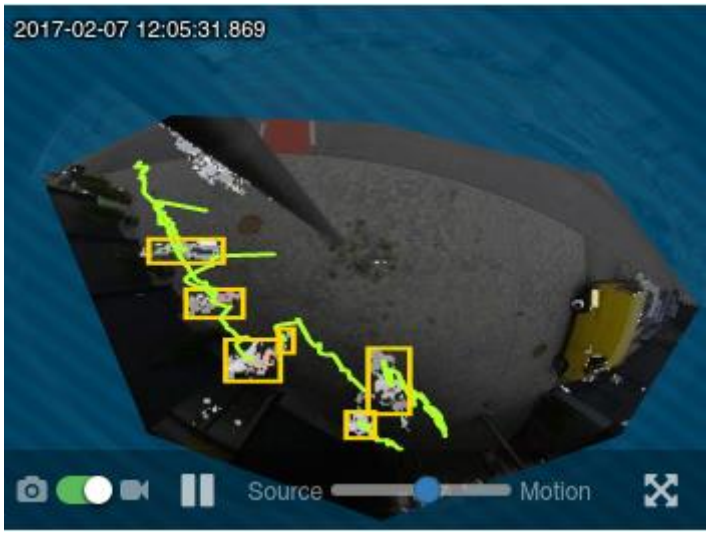
Furthermore, the license page is updated according to the newly acquired licenses. An example for a successful licensed server could look as in the picture below:



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 (∞) 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.

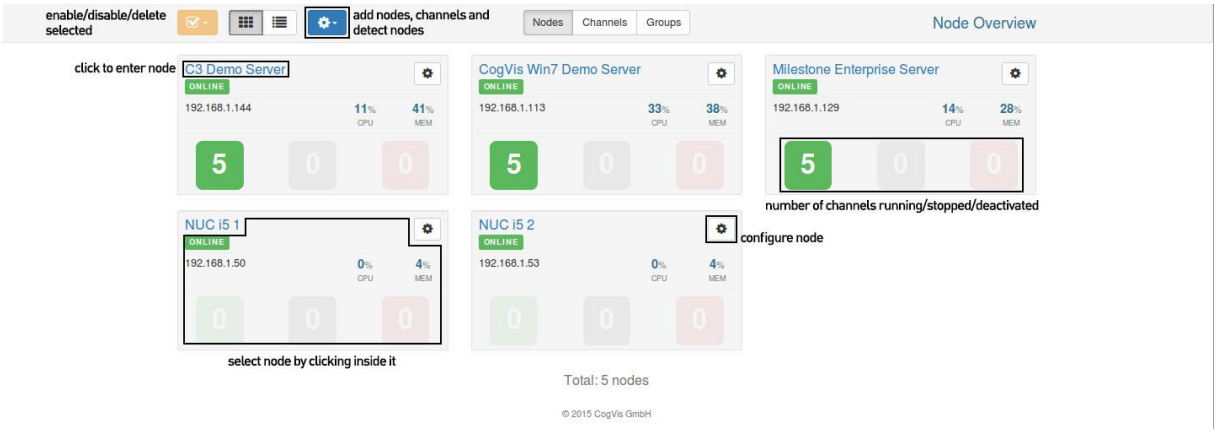
3.5 Node Management

3.5.1 Node Overview

The node overview is one of the central views within the C3 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.

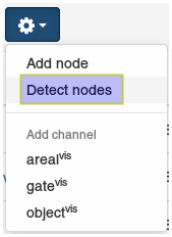
3.5.1.1 List View

3.5.1.2 Grid View

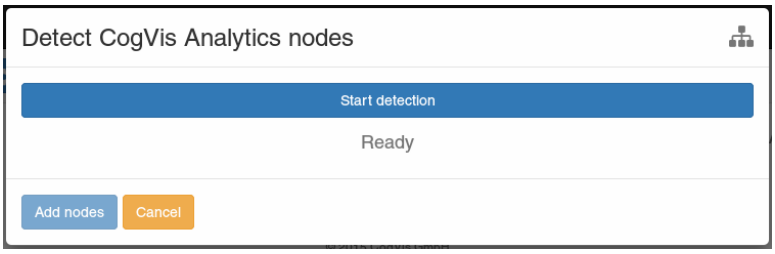


3.5.2 Automatic Node Detection

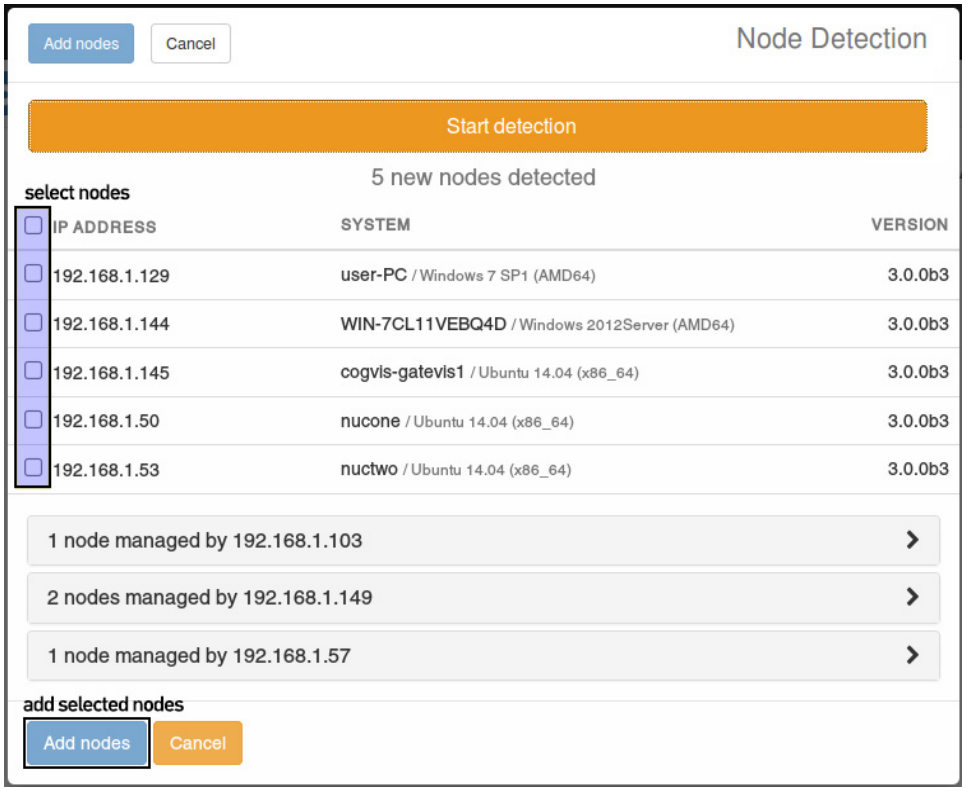
C3 server supports automatic node detection for nodes within the same network. To automatically detect nodes click the *option* symbol within the *node overview* and select the *Detect nodes* option.



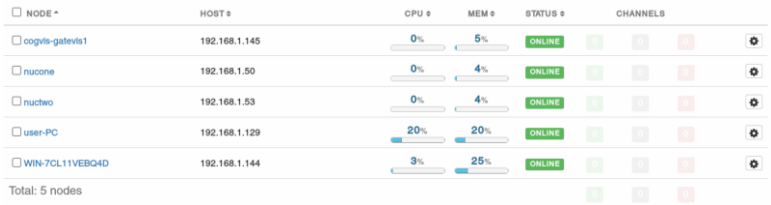
A modal window will open to lead through the automatic node detection process.



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 are 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.

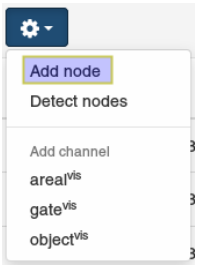


You can now select the required nodes you want to add to the management server: Check the box left of the respective node name and select *Add nodes*. The newly added nodes are then also listed in the node overview.

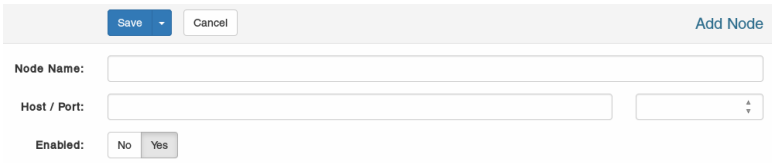


3.5.3 Adding a Node manually / Node options

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.

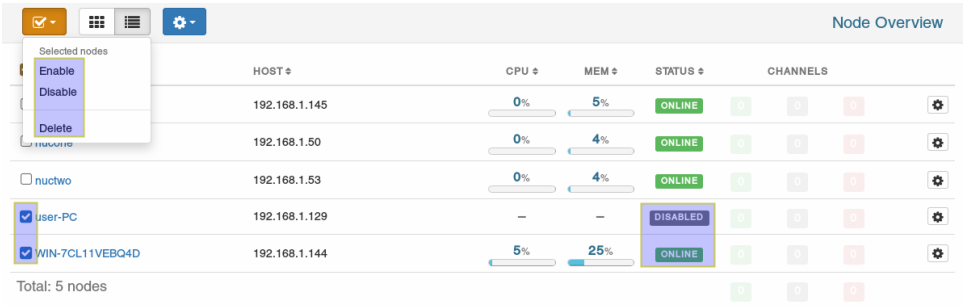
Examples:

- *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

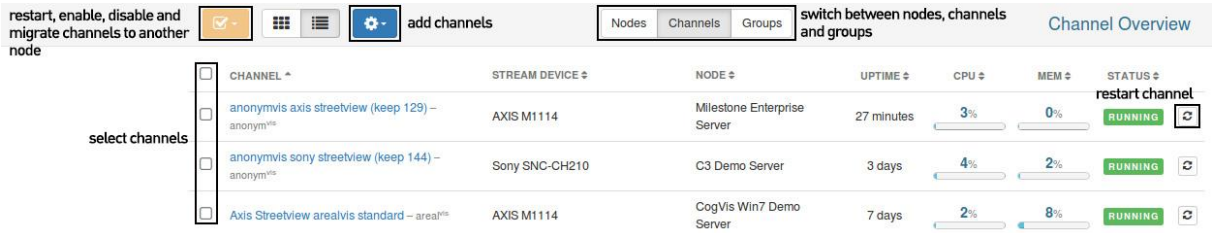
You can enable, disable or delete nodes. Disabling a node results in all its channels being disabled as well and in showing the "*disabled*" status in the *Node Overview*. As a consequence, the disabled node will not send any health-data. Deleting node will remove it from the system. You can modify the 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.



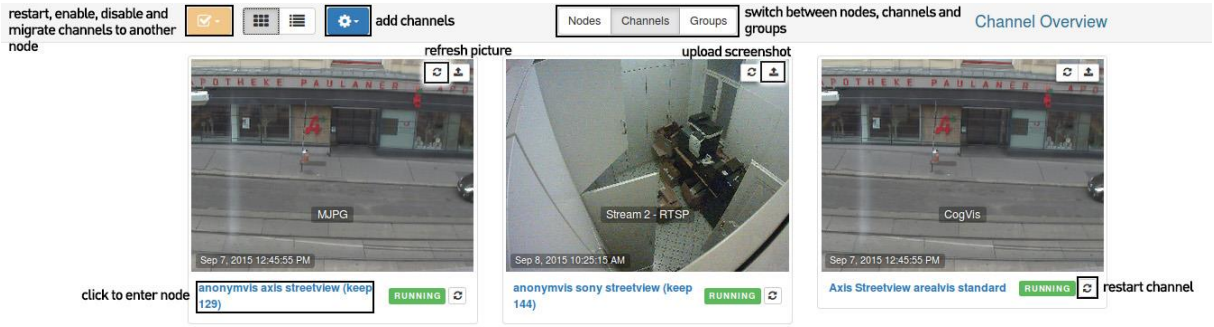
3.5.5 The Channel View

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



3.5.5.2 Grid View



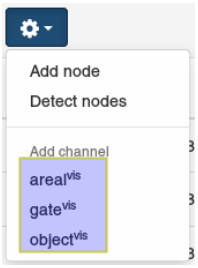
3.5.6 Add a channel

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

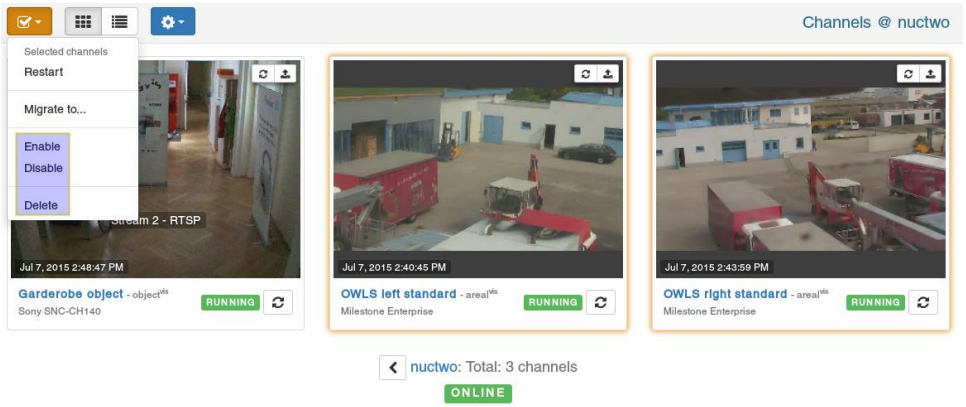
or from the node view



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

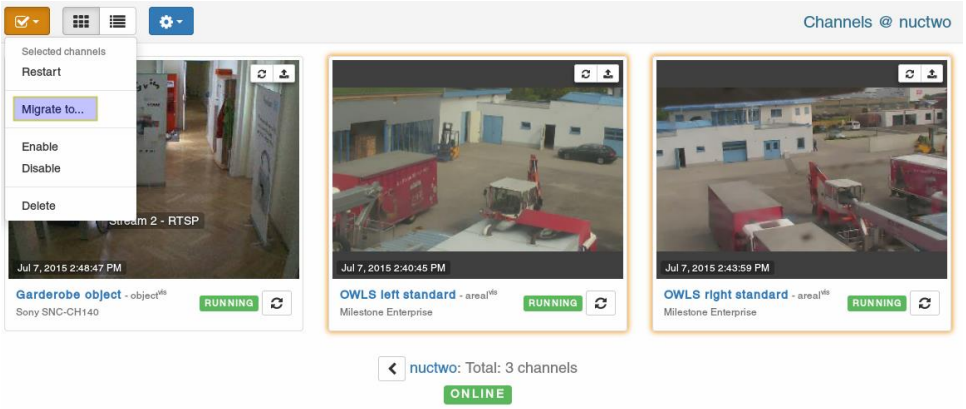
3.5.7 Enable / Disable / Delete a channel

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.

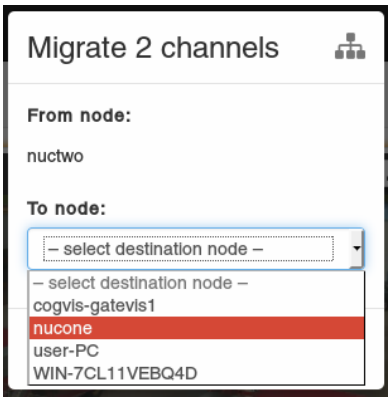


3.5.8 Migrate channel(s)

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.



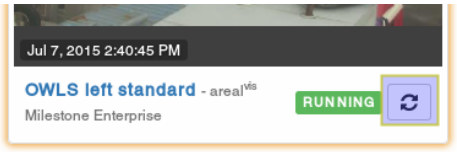
The channels will be stopped at the current node, migrated to the destination node and restarted there.

3.5.9 Restart channel(s)

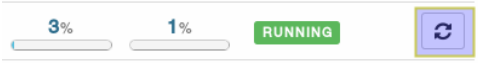
You can restart a single channel by clicking the *Restart* icons within the channel grid/list overview.

Examples:

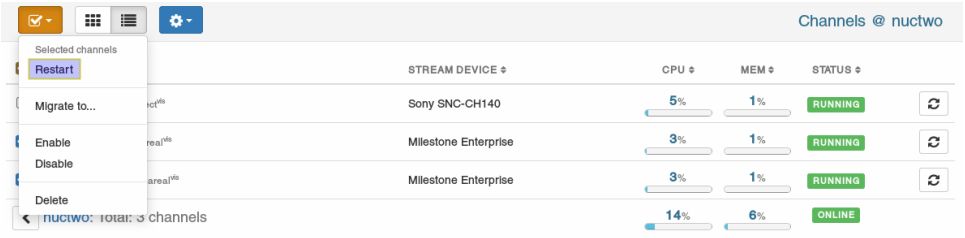
Restart using the grid overview



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.



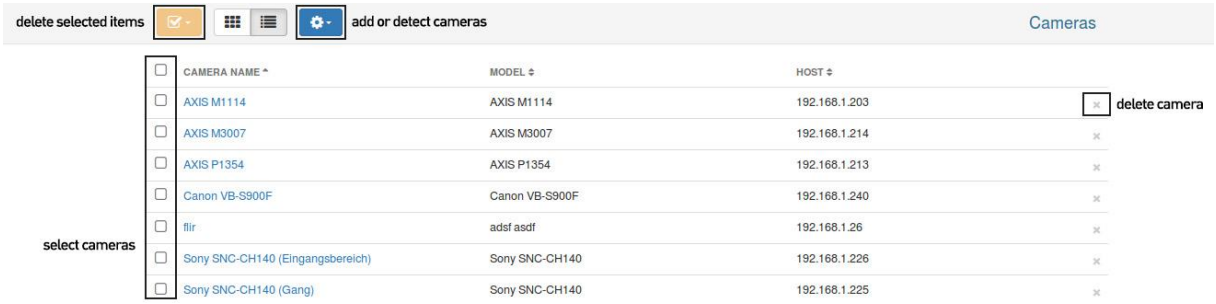
3.6 Cameras

C3 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.

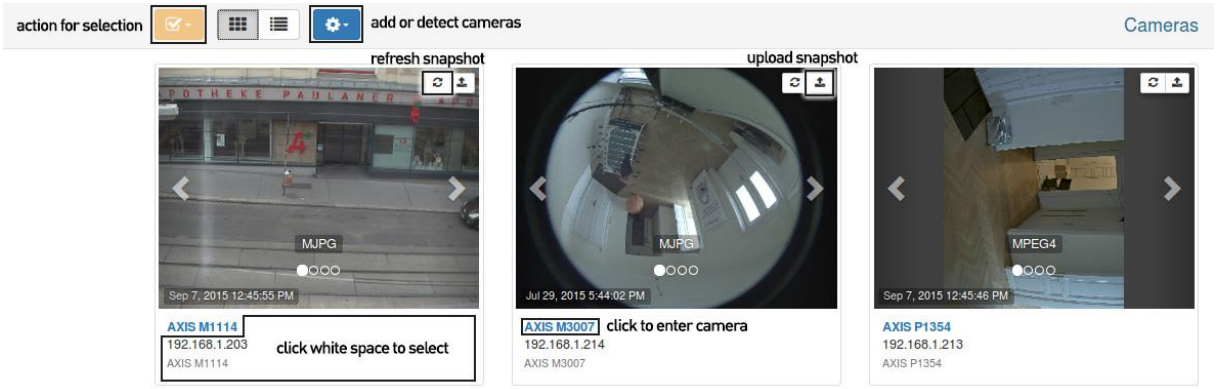
3.6.1 Camera overview

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

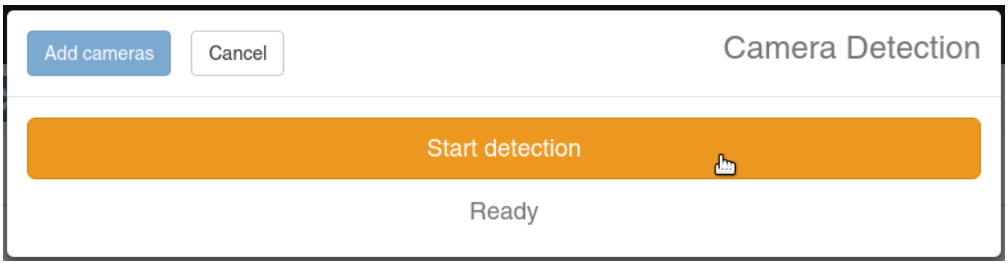


3.6.1.2 Grid View



3.6.2 Automatic camera detection

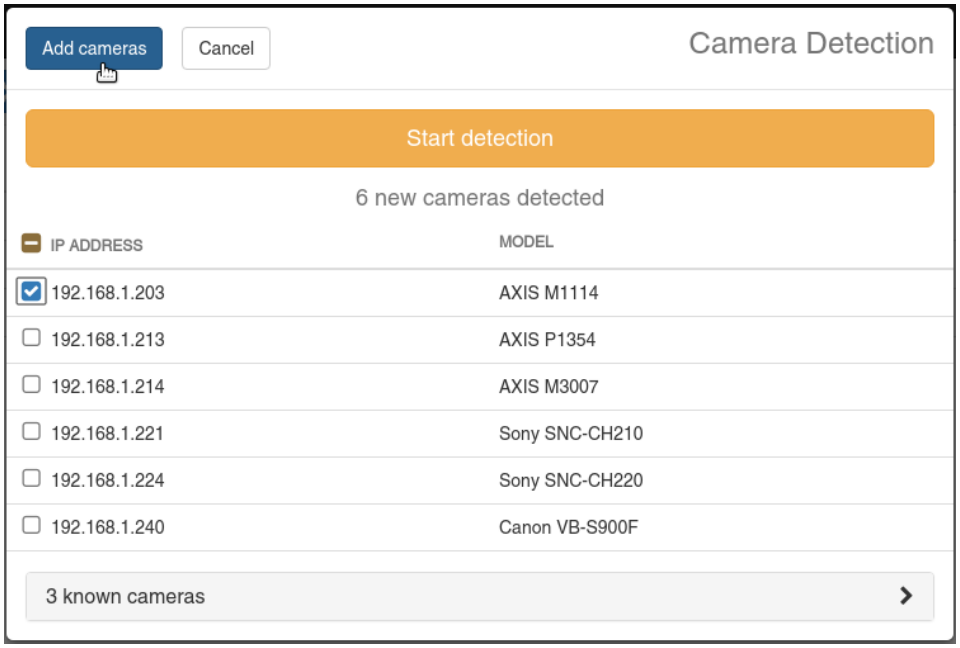
C3 server supports automatic camera detection. To execute it select *Detect cameras* from the *Options* button. In the separately opened view click *Start detection* to make the server automatically find cameras connected in your network.



After the C3 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: .

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.



3.6.3 Add / Edit Cameras

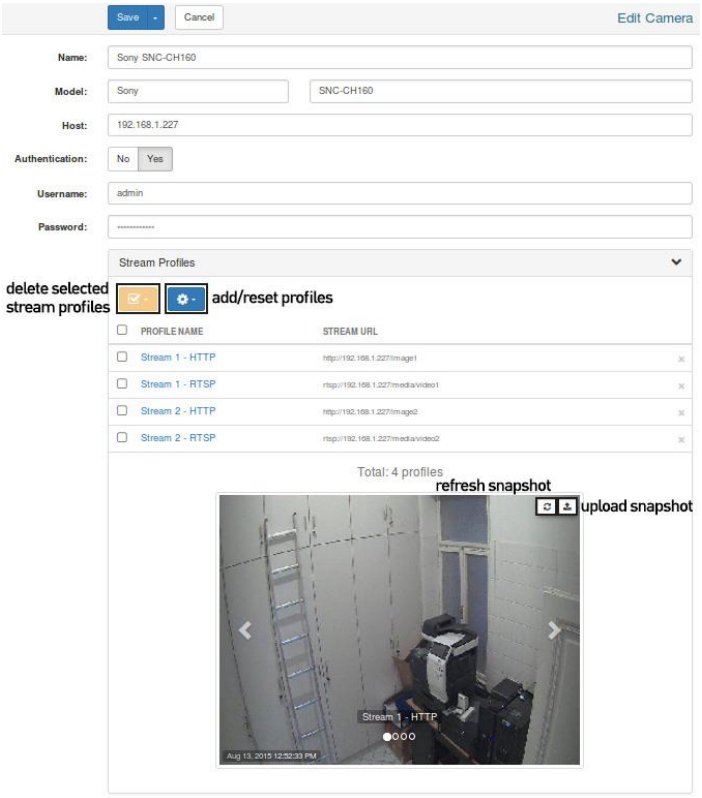
- To add a camera manually select *Add camera* from the *Option* drop-down.
- To edit a camera select the respective camera by clicking its camera name from either the list or grid view.

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.

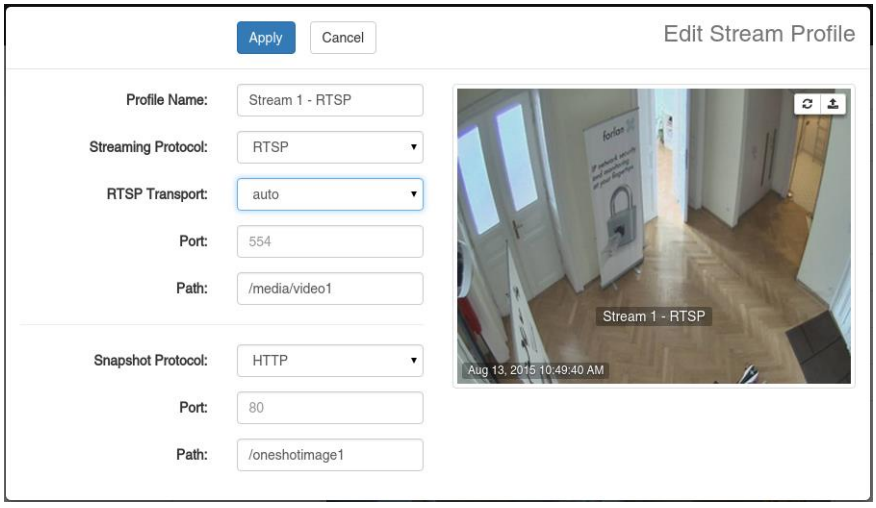
Example for a completed camera view:



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**

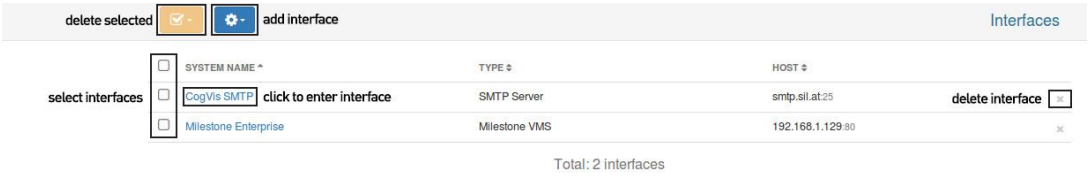
- **HTTPS**
- **RTSP**
- **Video File**

- **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

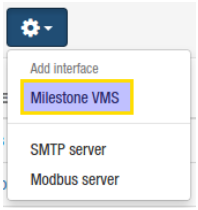
Interfaces are used for the communication with external systems, such as video management systems (VMS) or SMTP servers. All external interfaces are managed using the *Interfaces* view.

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



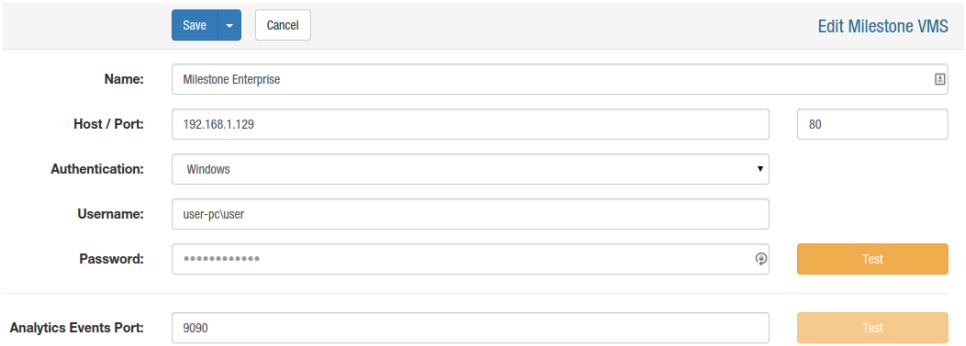
3.7.1 Milestone VMS

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.

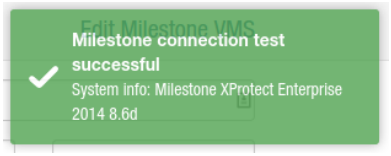


In the empty Milestone interface mask fill in the information about the server. The following parameters are required for the Milestone interface:

- **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.



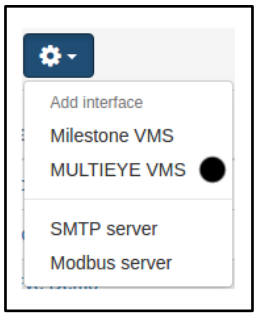
If you have entered all the data correctly you can test the connection to the Milestone server. If the test is successful a notification in the browser window similar to this one is displayed:



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

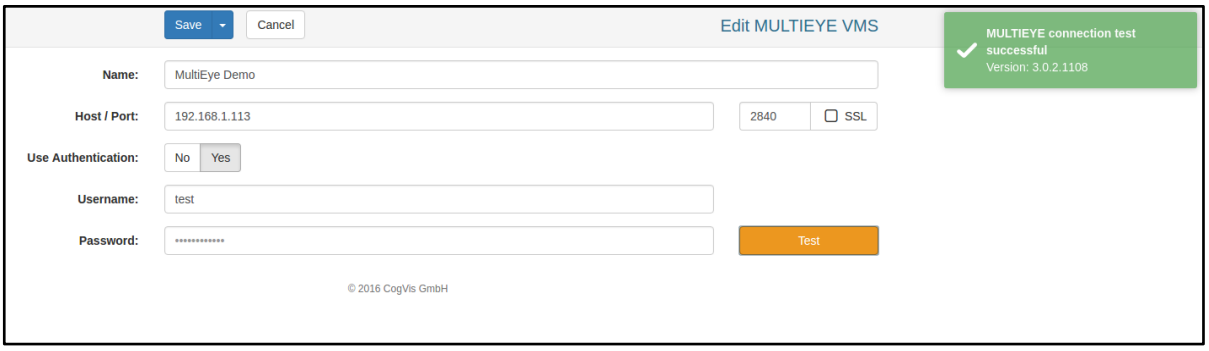
3.7.2 Multieye VMS

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.

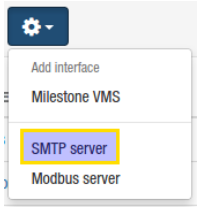


If you have entered all the data correctly you can test the connection to the MultiEye server. If the test is successful a notification in the browser window similar to this one is displayed:

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

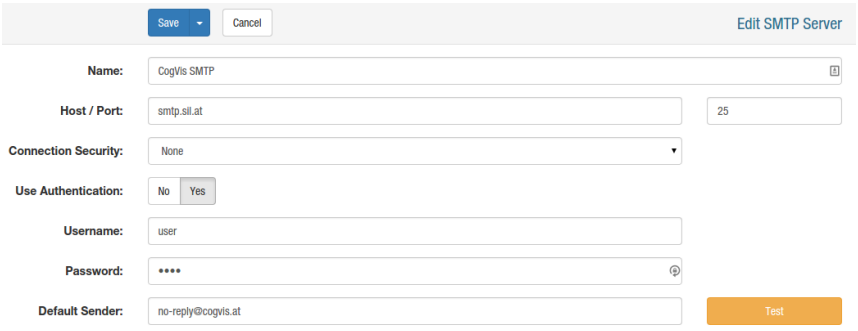
3.7.3 SMTP Server

To send events via email at least one SMTP server has to be added to the C3 system: Select *SMTP server* from the *Option* menu in the *Interfaces* view. You can add as many SMTP servers as you like.



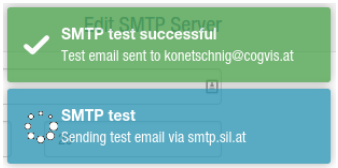
This opens the SMTP server view holding a form to be filled with all necessary parameters specifying a SMTP connection. As these parameters vary for each service provider please contact your IT administrator or email service provider for the parameters for your specific SMTP. Following is a list of all 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*.

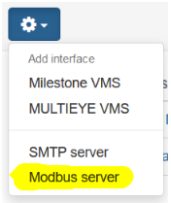
A successful test results in a notification such as the following:



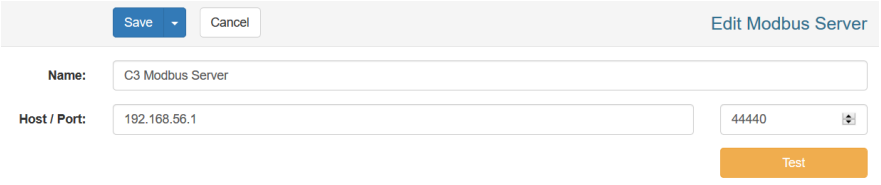
Furthermore you receive an email to the address you entered before. To finish the configuration of the SMTP server correctly, please don't forget do save upon exit.

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^{vis}) should have the server selectable.

3.8 Channel configuration

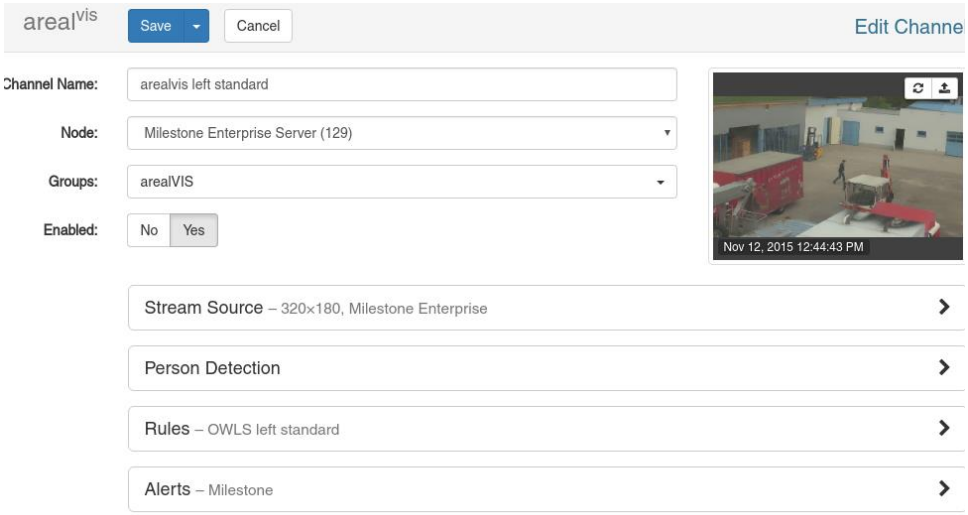
3.8.1 Overview and general settings

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.



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 *C3 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.

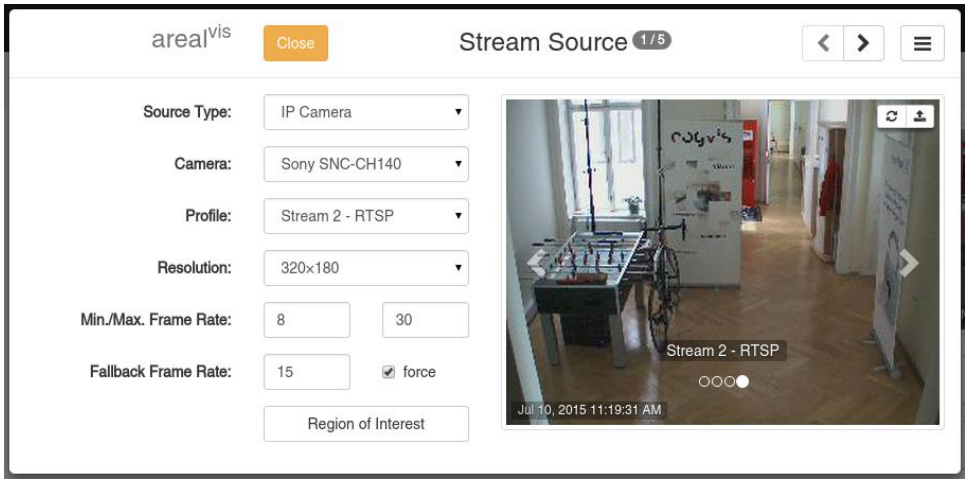
3.8.2.4 Fallback Frame Rate

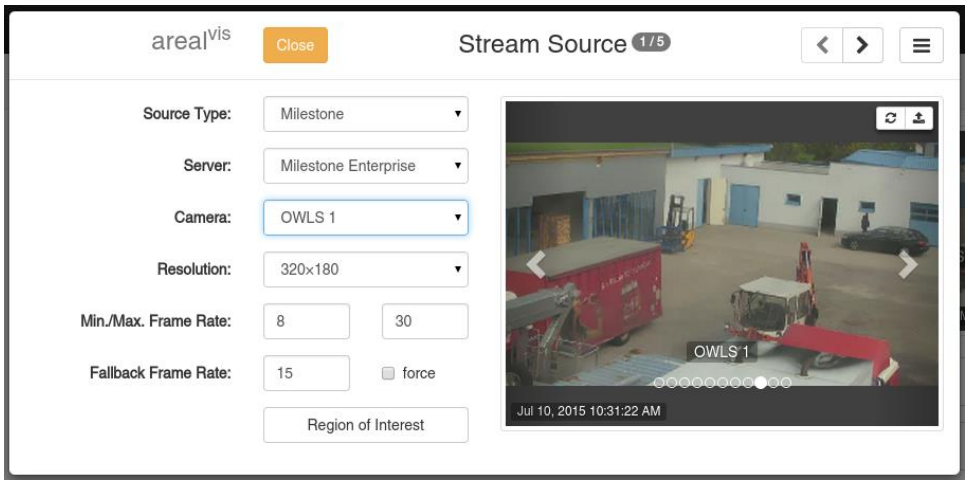
In case the maximum frame rate is exceeded, the analytics will set the frame rate back to the one specified in the *Fallback Frame Rate* parameter. This value should be set to the frame rate the stream is set to deliver.

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

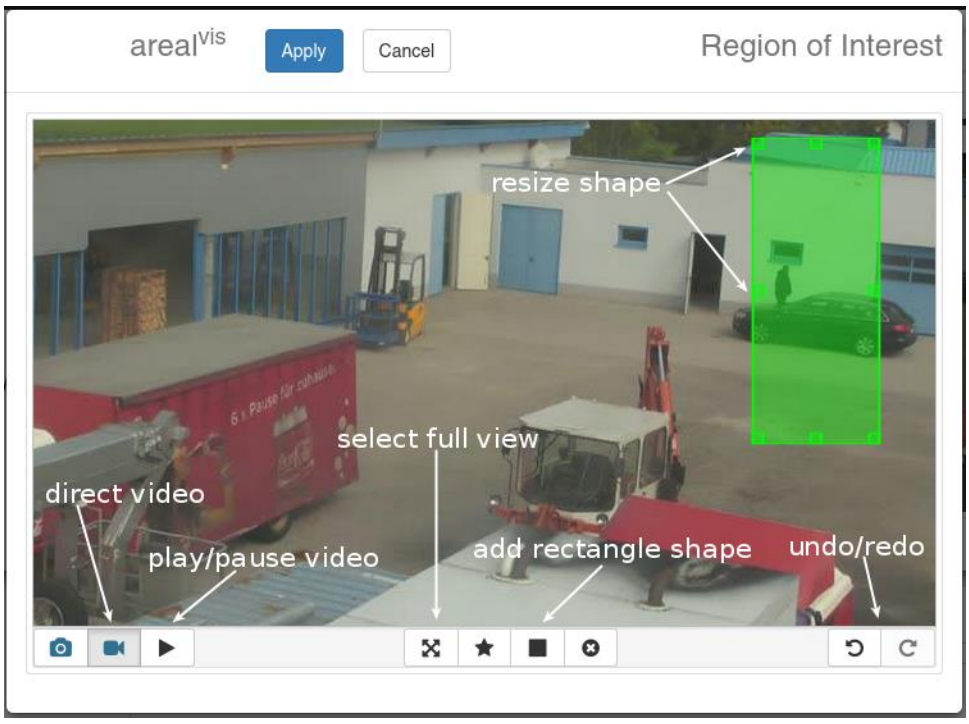


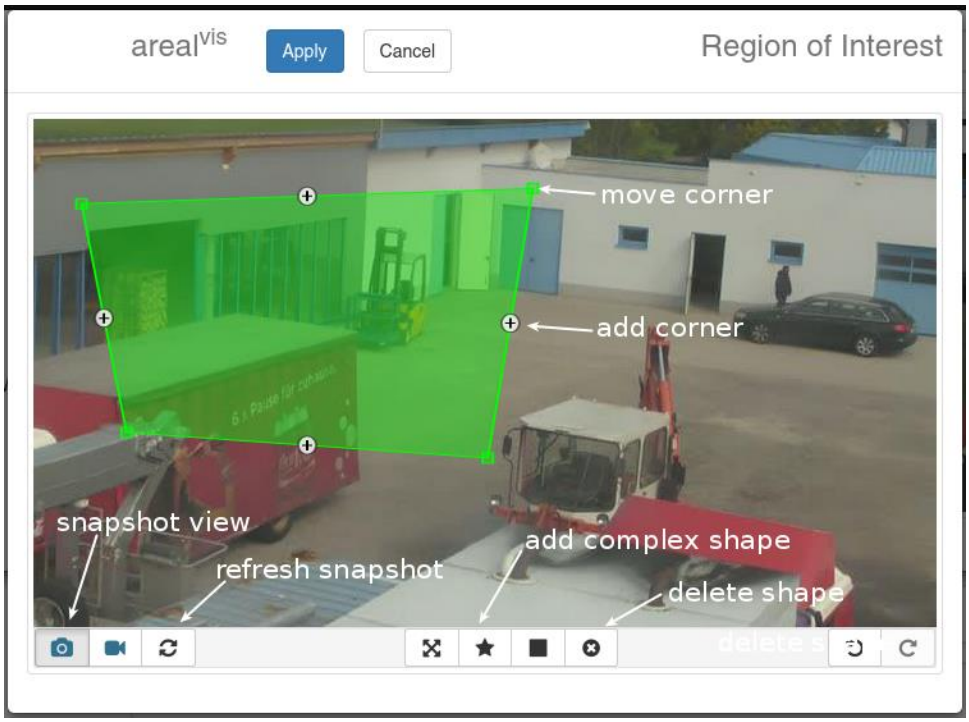


3.8.2.5 *Region of Interest*

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.

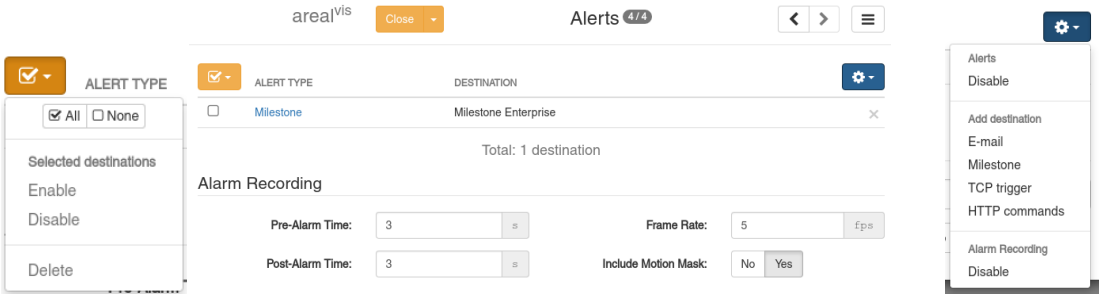
The ROI is defined by adding one or multiple polygonal and/or rectangular shapes. Alternatively, (per default) the whole scene is set as the ROI. ROIs don't need to be overlapping. The following screenshots show possible options and interactions within the modal view.





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.

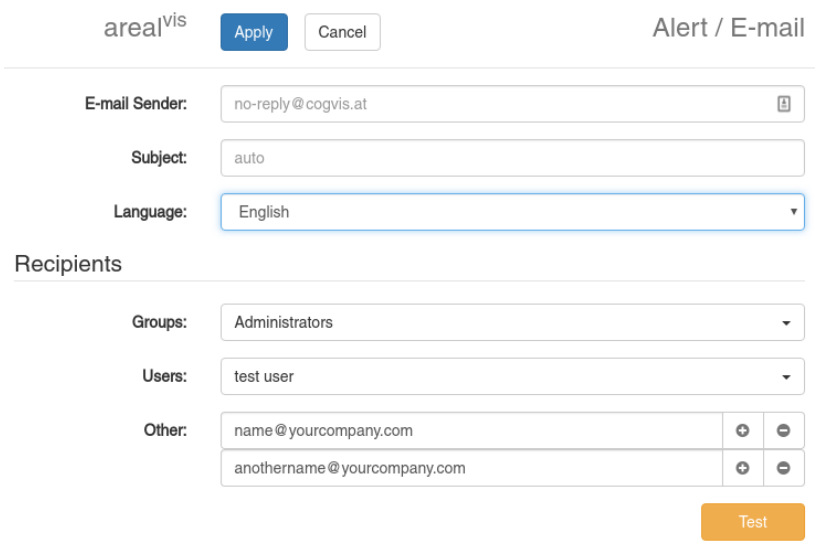


3.8.3.1 Alarm Recording

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.

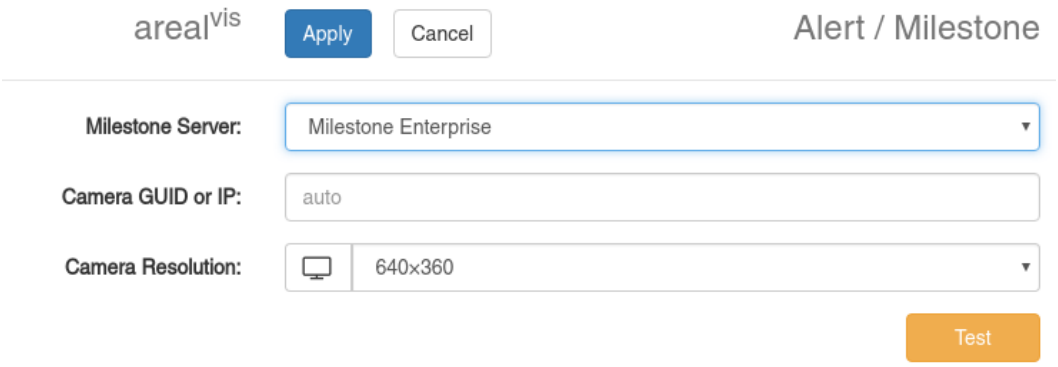
3.8.3.2 E-Mail

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:



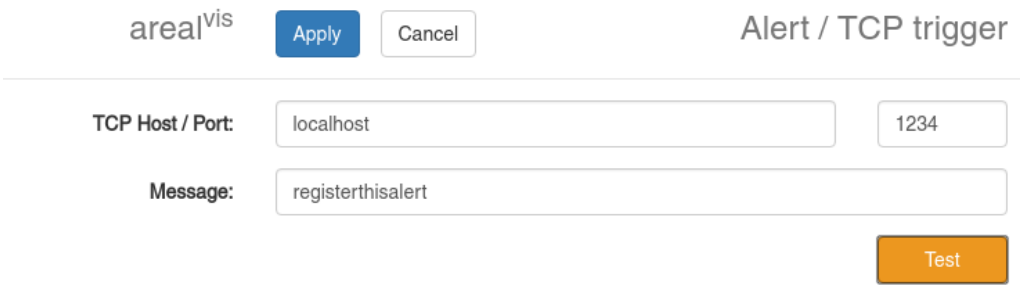
3.8.3.3 *Milestone*

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.



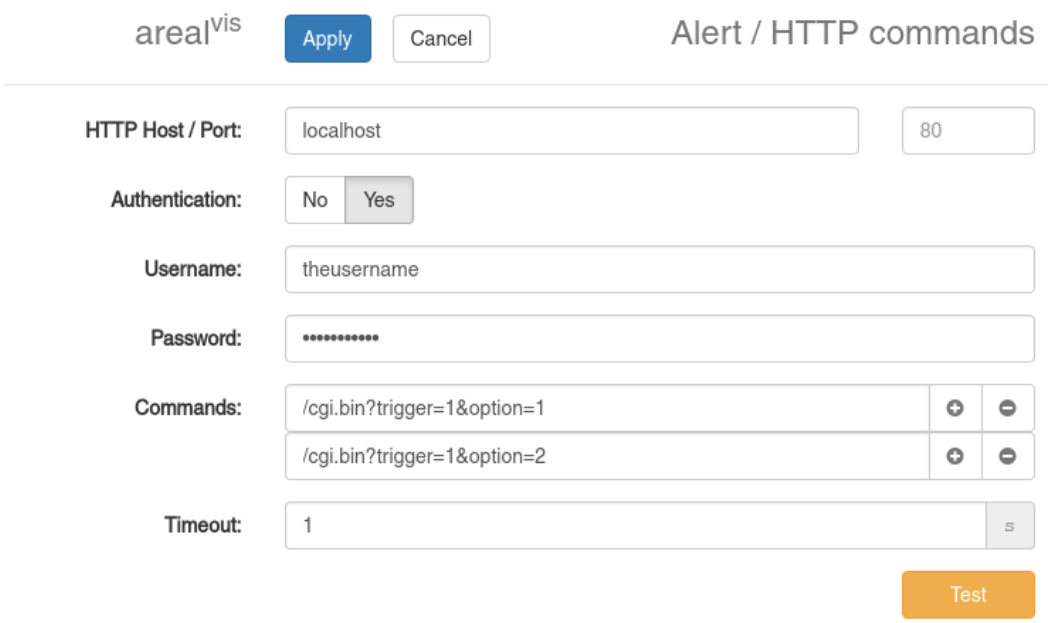
3.8.3.4 *TCP-Trigger / TCP-Message*

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.



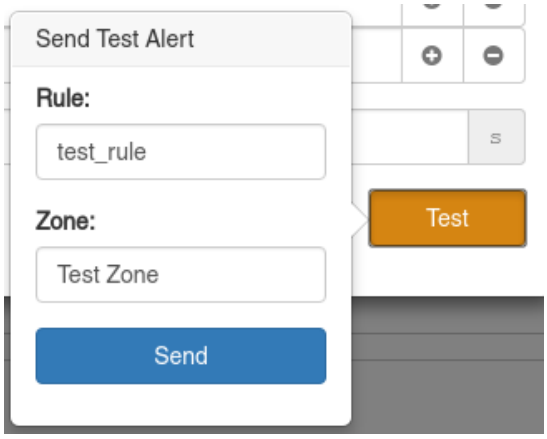
3.8.3.5 *HTTP Commands*

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.



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.



3.8.4 areal^vis

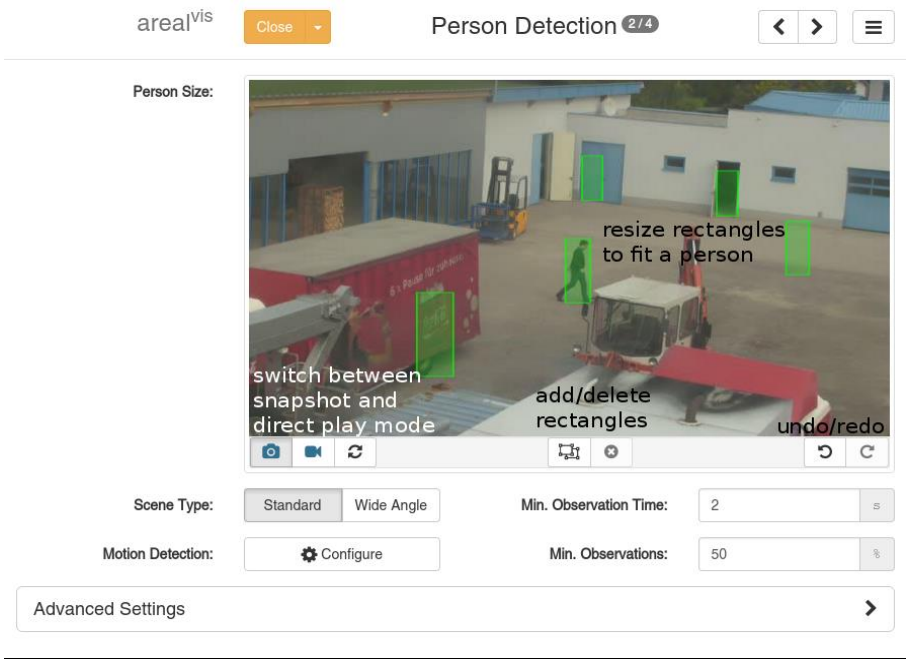
areal^vis is a powerful and precise solution for 24/7 area security. It is specially designed for outdoor scenarios and for all weather conditions and offers robust event detection in live-video streams from standard IP, IR, thermal or embedded camera systems. Its detection accuracy and its seamless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

To achieve its precise object classification, areal^vis 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 areal^vis.

3.8.4.1 *Person Detection*

The *Person Detection* configuration card is the center part of the areal^vis' 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

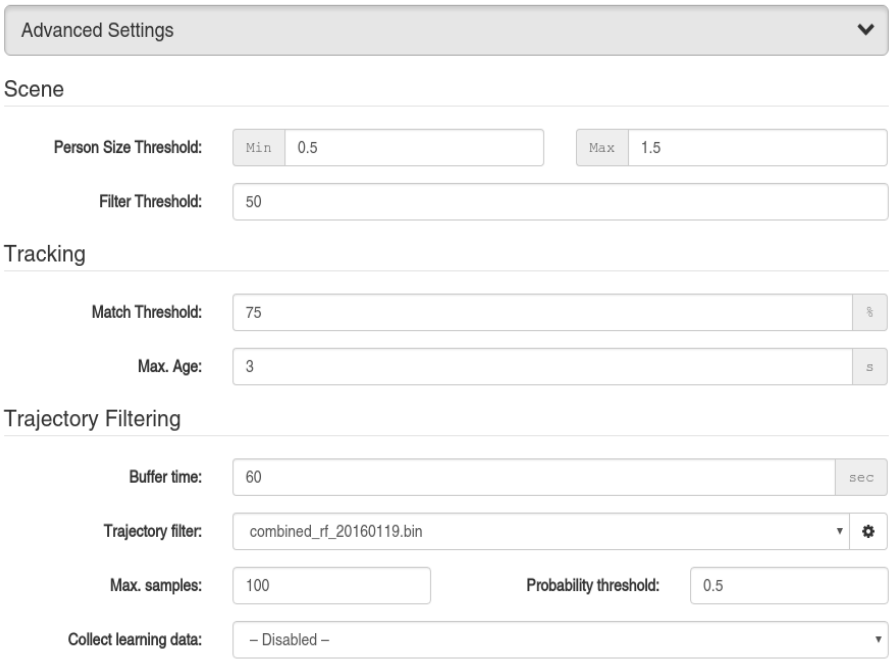
The min. observation time defines how long at least a person has to be tracked in seconds (default: 2 seconds). The min. observation defines the minimum number of required observations within the min. observation time the system has to have. (50% should be a good default value)

3.8.4.1.2 Motion Detection

See Motion Detectors on page 50 for further details.

3.8.4.1.3 Advanced Settings

Note: the advanced settings dig deep into the tracking configuration of areal^vis. They are for expert users only and it is not recommended to change these settings by yourself. If you have problems configuring areal^vis 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).



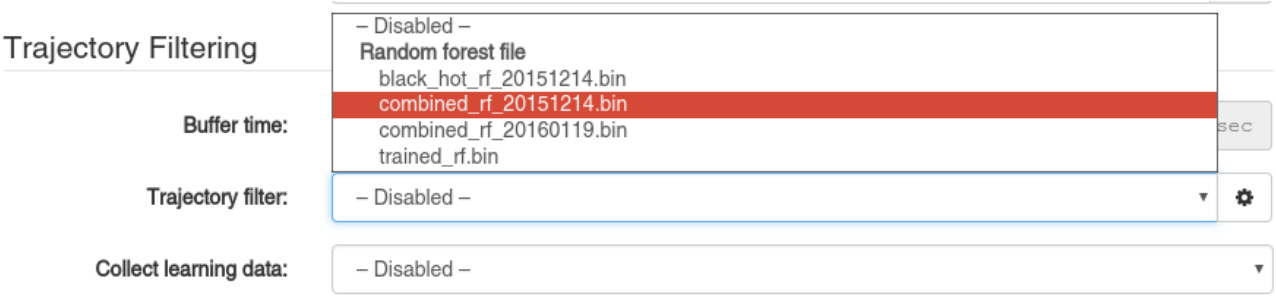
Scene: Here you can change the *Person Size Threshold* and the *Filter Threshold.* The *Person Size Threshold* defines the minimum and maximum multiplier of area an object is allowed to have with respect to the configured person size to be considered valid by the tracker. So, the configuration *Person 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.

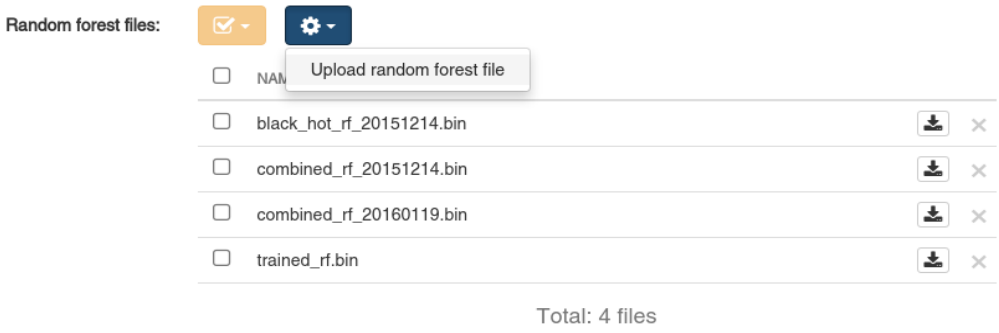
If you have *Motion Filtering* enabled, the object observed has to move by a certain *Motion Factor* within a defined *Time span*. The *Motion Factor* is the dx/dy distance in pixel relative to width plus height from the first to the last observation within *Time Span*. For example, an object with size 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 arealvis. 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 CogVis 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.

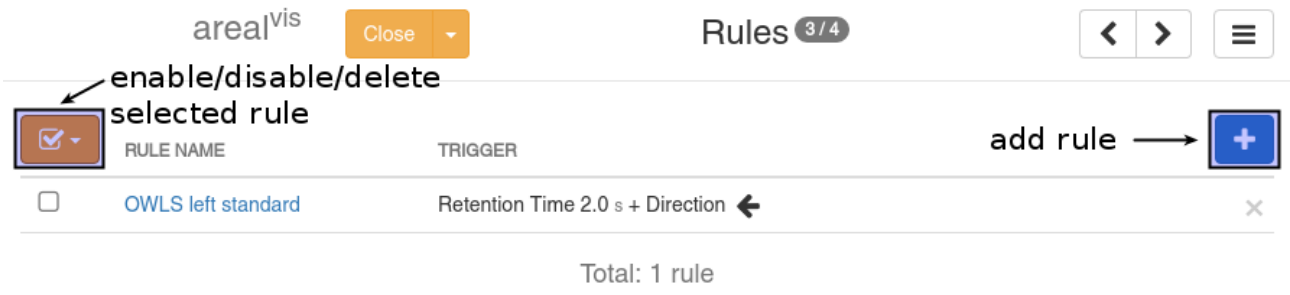
If you don't have the standard CogVis random forest files please contact office@for-lan.at.

Collect learning data

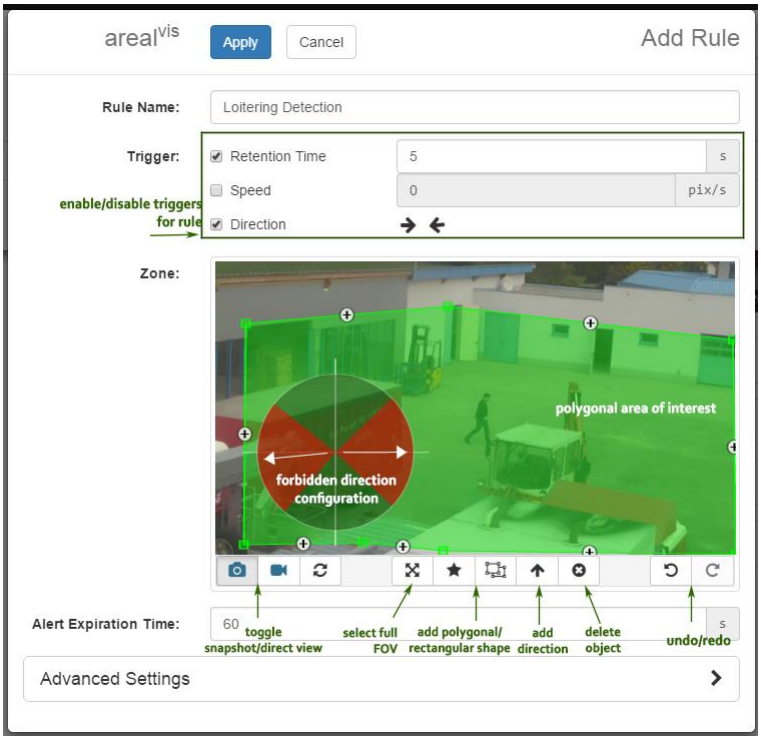
To get your own personal random forest file or if you want to help CogVis with the collection of learning data you can activate the learning mode by selecting where you want to store your learning data. You can either choose *Server* or *Node* from the drop-down menu. When you choose *Server* all data will be managed bey the server and can be downloaded by using the *Server Administration*. When choosing *Node* learning data will be stored ion 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.

3.8.4.2 Rules

Rules are the central element of an areal[vis] 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.

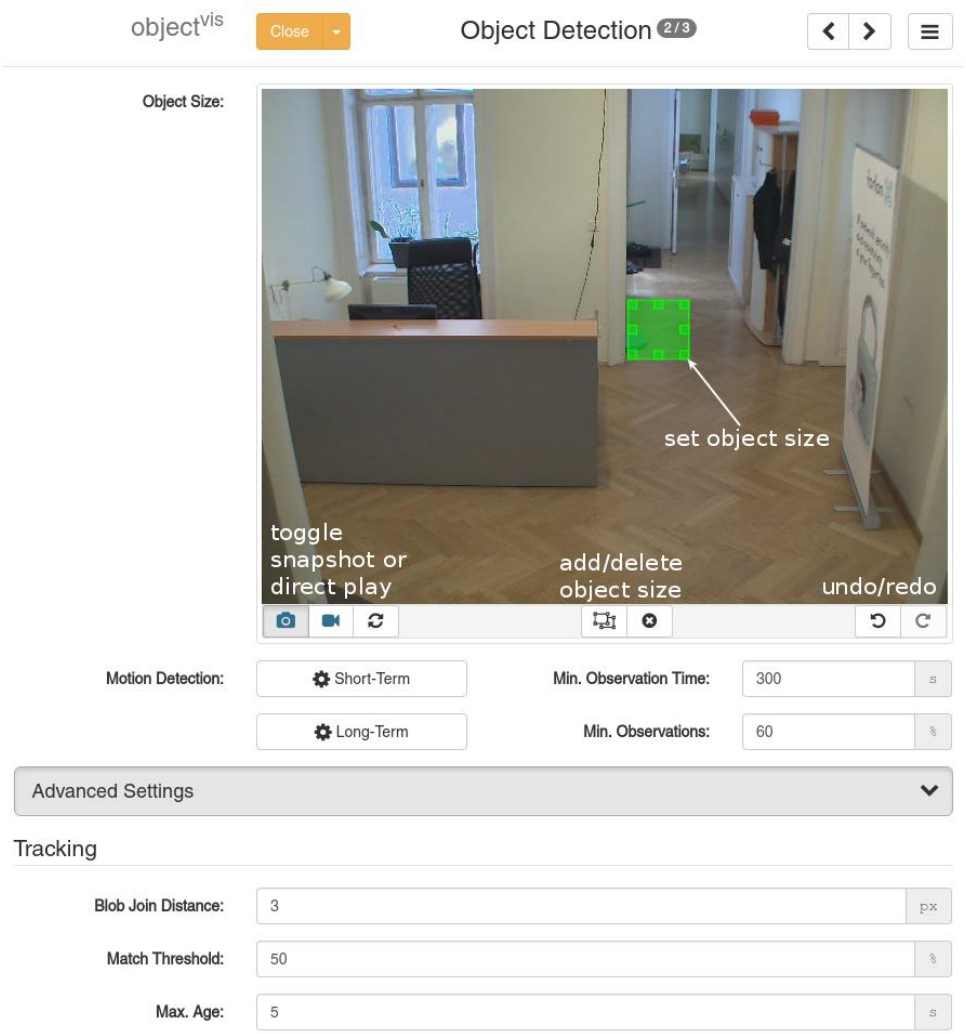
3.8.5 object^{vis}

object^{vis} 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^{vis} specific settings.

To setup object^{vis} 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 longterm and shortterm motion detectors have to be configured (see *Motion Detector* section).



3.8.5.1 *object^{vis} 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.
  - **Match Threshold**
    The *Match Threshold* 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.

3.8.6 gate[vis]

Please contact the Forlan support team (office@for-lan.at) or your Forlan partner of choice for gate[vis] configuration support.

3.8.7 anonym[vis]

Surveilling security-critical areas while still protecting privacy - anonym[vis] makes it possible by offering consistent and reliable privacy protection for persons, vehicles, and critical areas under surveillance. anonym[vis] 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.

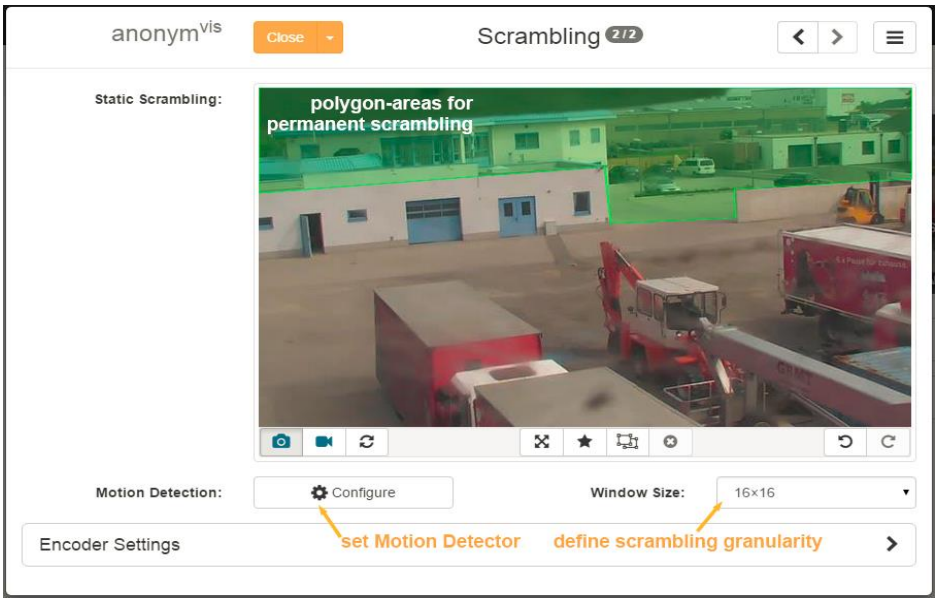
The video analytics core detects motion and pixilates moving persons, vehicles and objects in outdoor- or indoor environments. It automatically pixilates these areas in real-time using a selected window-size defining the dimensions of the resulting color-homogeneous areas. In addition, users can define 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, anonym[vis] allows for the detection of security-critical events at a glance from the anonymized video while consistently protecting privacy.

This section contains all anonym[vis] -specific settings and views for its configuration.

3.8.7.1 Scrambling

The Scrambling modal window holds all anonym[vis] specific configuration parameters.

- **Static Scrambling:**
  In addition to motion-based scrambling, anonym[vis] 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 coarser 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 count^vis

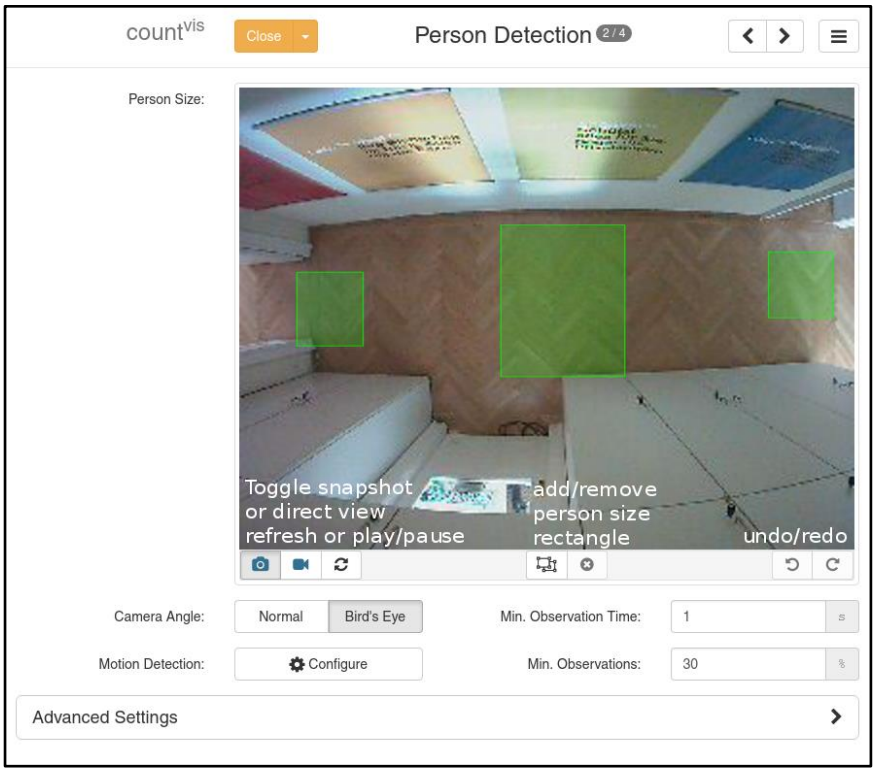
Effective marketing, staff management and customer experience optimization require – especially in retail and gastronomy – knowledge and awareness of customer behavior. Based on comprehensive state-of-the-art real-time video analytics functionalities countvis delivers quantitative results.

count^vis 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^vis also an excellent solution as a guiding system.

This section contains all count^vis -specific settings and views for its configuration.

3.8.8.1 Person Detection

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



3.8.8.2 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[vis] tracker works by minimum and maximum area of an object so you don't have to (but you can) define more than 3 rectangles.

3.8.8.3 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.

3.8.8.4 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.

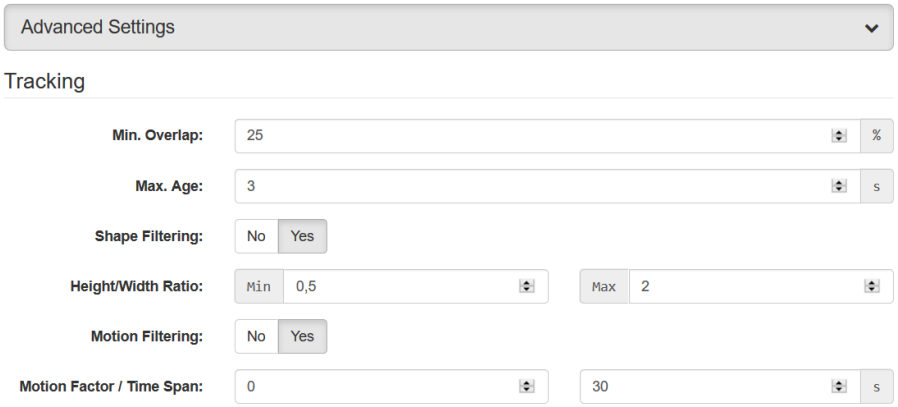
3.8.8.5 Min. Observation Time

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

3.8.8.6 Min. Observations

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

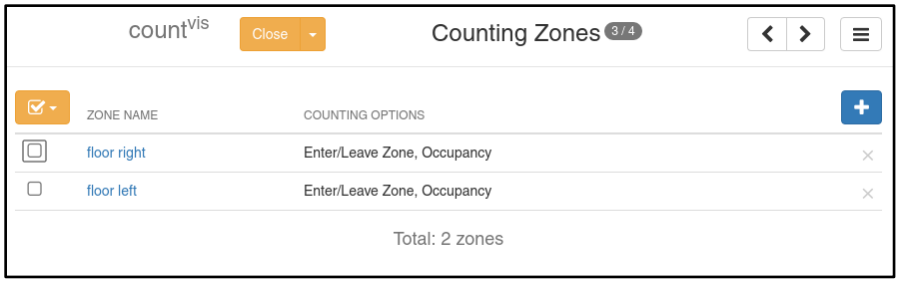
3.8.8.7 Advanced Settings



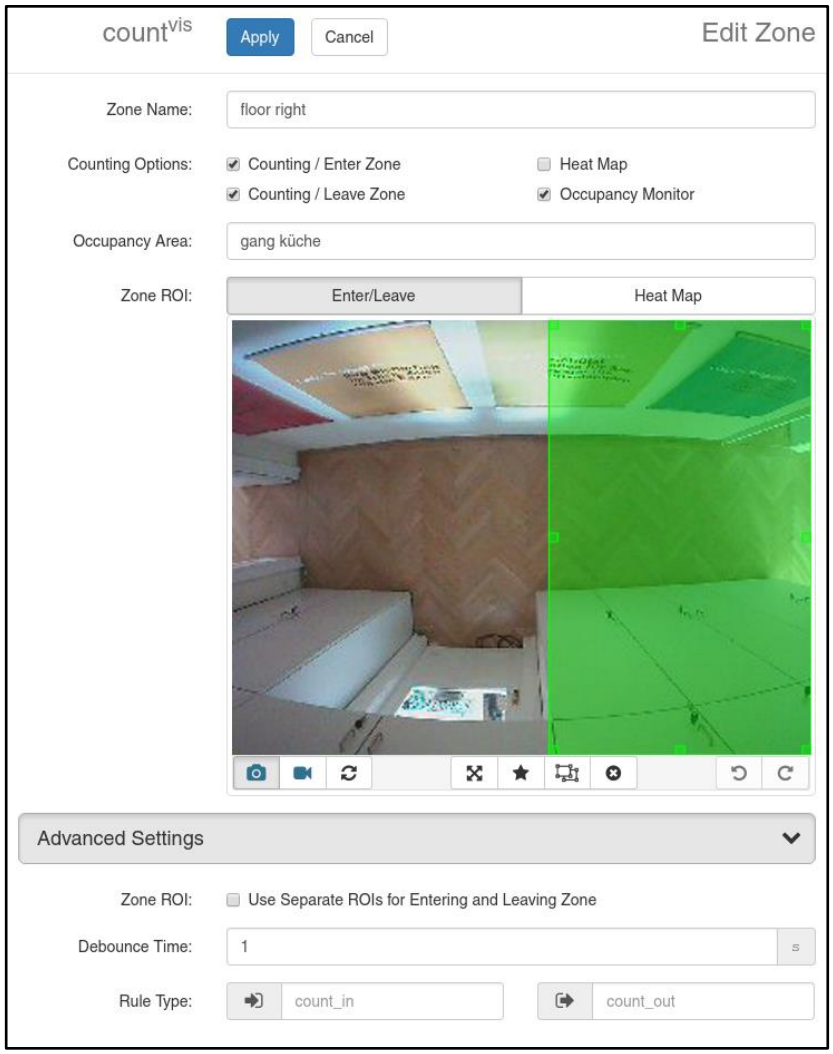
3.8.8.7.1 Tracking

- **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.

3.8.8.8 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:



3.8.8.8.1 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
    Monitor occupancy of the zone for a certain occupancy area (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.

3.8.8.8.2 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).

3.8.9 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 goes through all motion detectors implemented in CogVis C3 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 are 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.

3.8.9.1 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

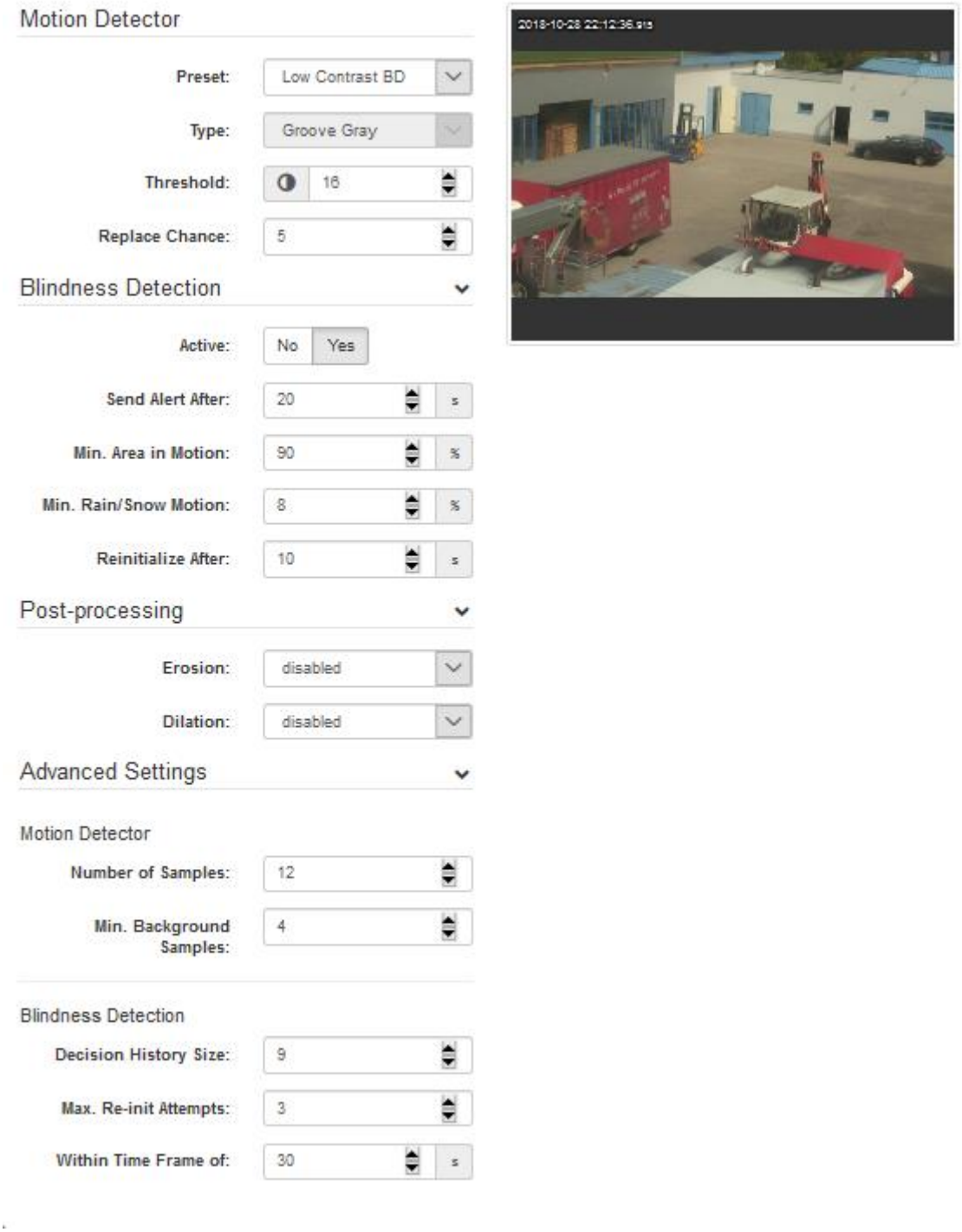
You should select Gray presets for scenes where night vision cameras or thermal cameras are used. Color presets are best used for day and indoor scenarios where color is present in the image 24/7. If you change the settings of a preset your changes will be saved automatically as a custom preset.

3.8.9.2 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 CogVis.

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.



3.8.9.3 Mixture of Gaussians

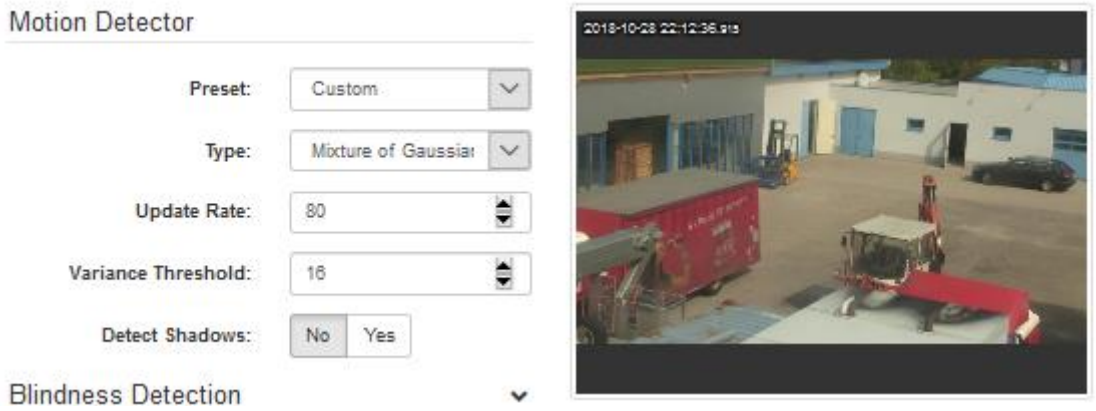
The *Mixture of Gaussians* motion detector (MD) uses a Gaussian Mixture Model to model foreground and background for every pixel. It is not as high-performing and controllable as the *Groove* MD but performs very well in outdoor perimeter setups with changing conditions. It was used before Groove was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



3.8.9.4 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

3.8.9.5 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

3.9 Event Log

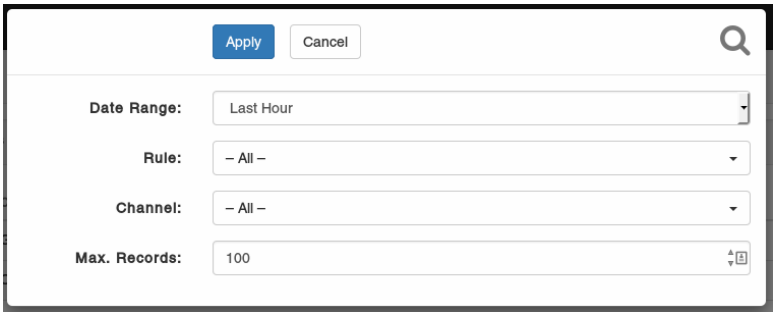
The event log aggregates and shows all events triggered by C3 analytics. You can sort the events ascending or descending by clicking on

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

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

3.9.1 Filter

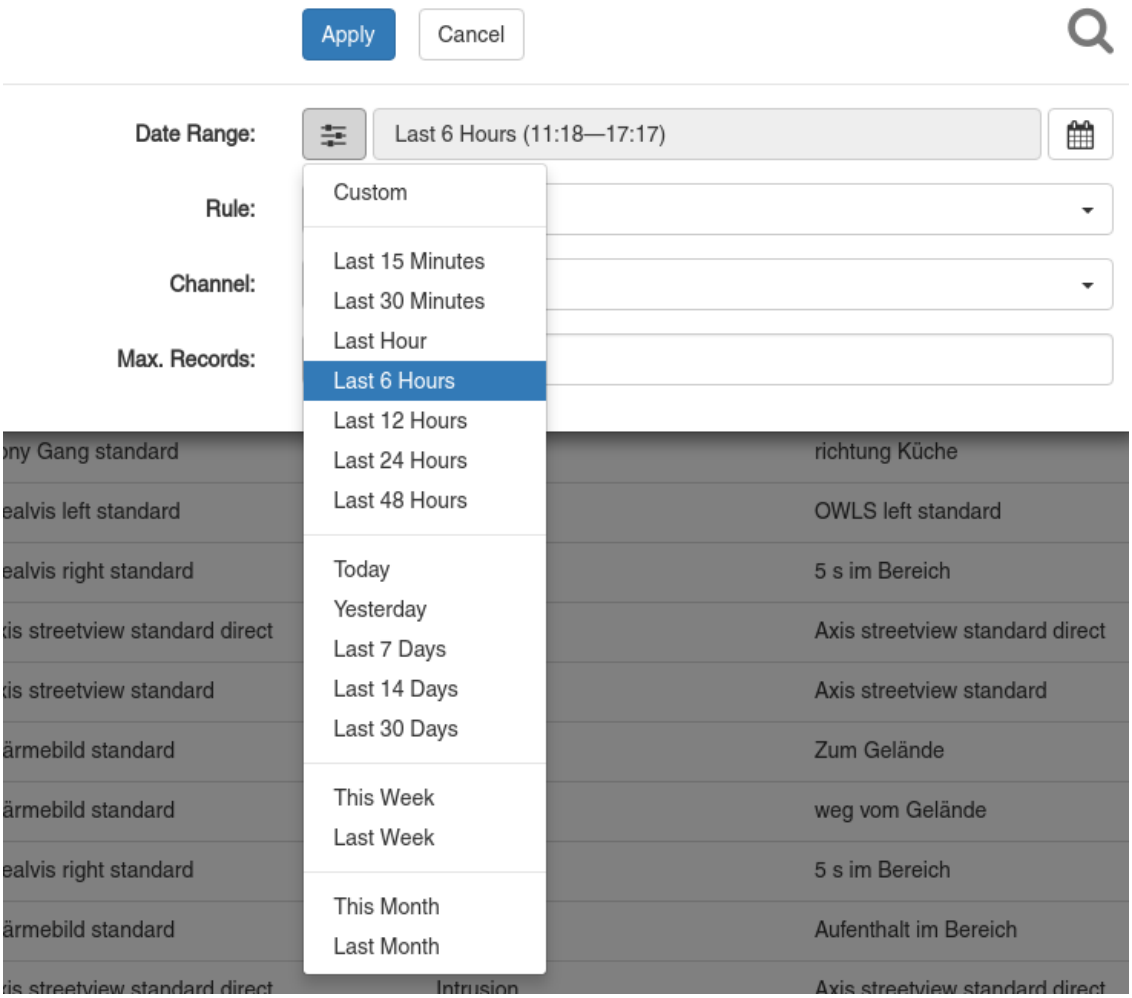
When clicking on the button in the event log view the filter modal will open.



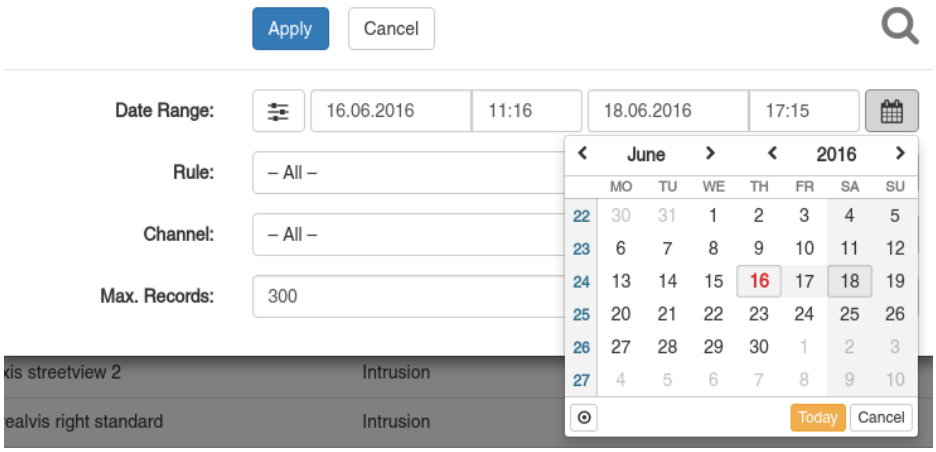
You can filter by

- Date Range
- Rule
- Channel

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



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.

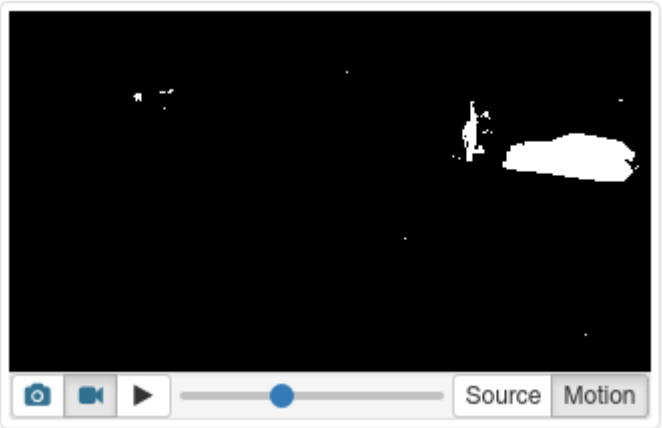


Filtered results will only remain static as long as the auto refresh is disabled. When auto refresh is enabled new events will be added to the filtered view regardless if they fit the filter or not.

3.9.2 Event Image / Alarm Sequence

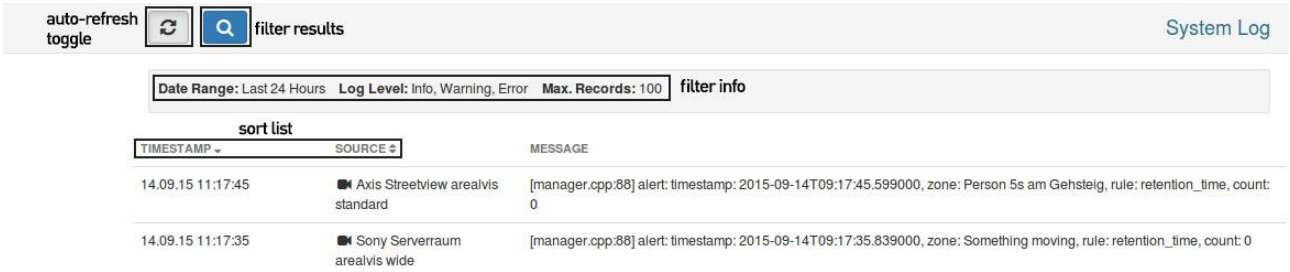
If alarm sequence recording is activated you can switch between the metadata alert image and the alarm sequence by pressing either the photo- or video-camera button. The Play button starts and stops the playback and with the slider you can scan faster or slower through the alarm sequence. With the

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



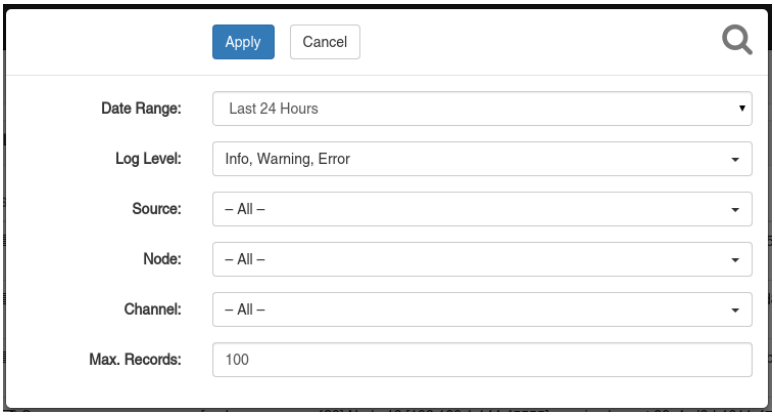
3.10 System Log

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*.



3.10.1 Filter

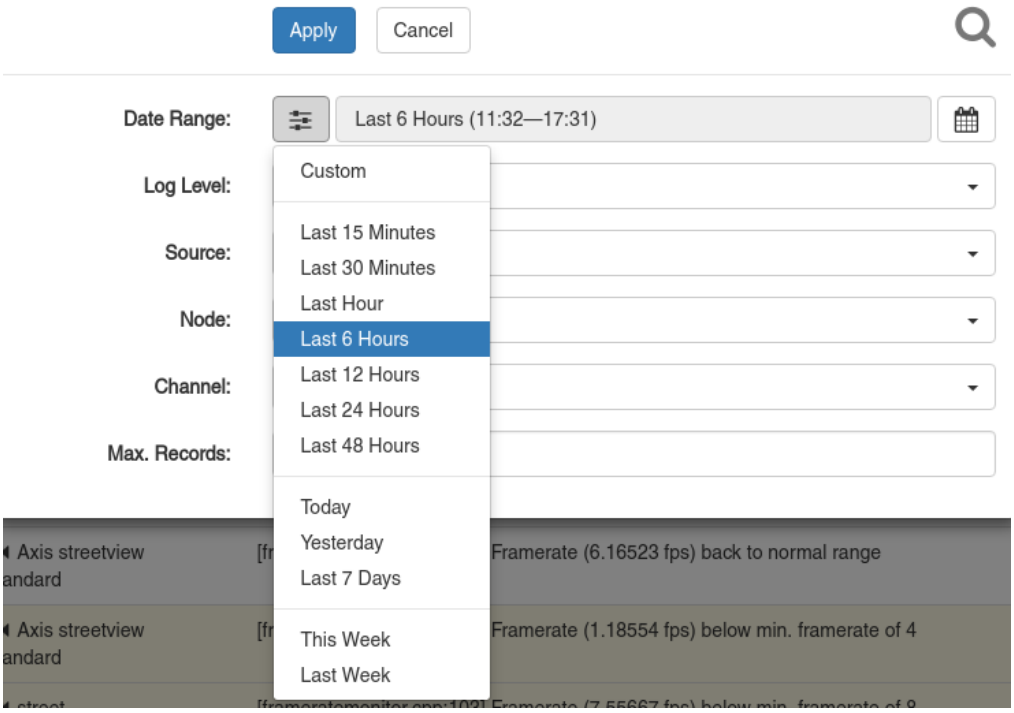
When clicking on the button in the system log view the filter modal will open.



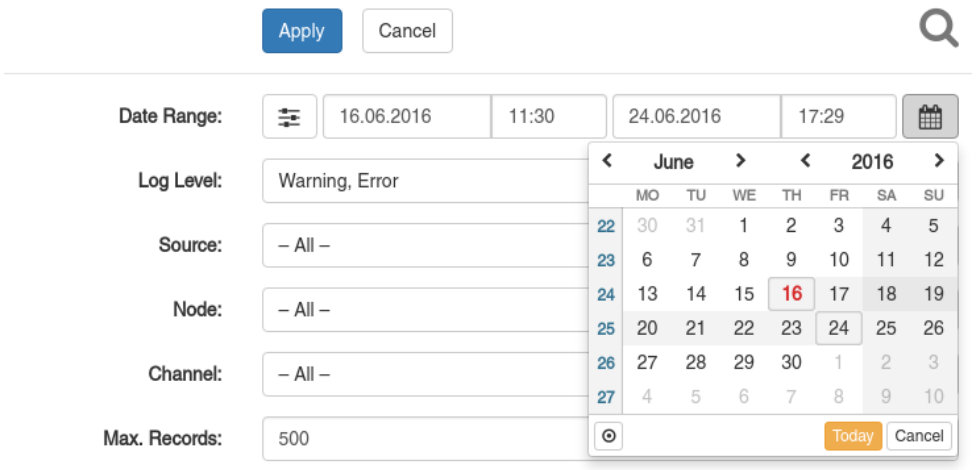
You can filter by

- Date Range
- Log Level
- Source
- Node
- Channel

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



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.



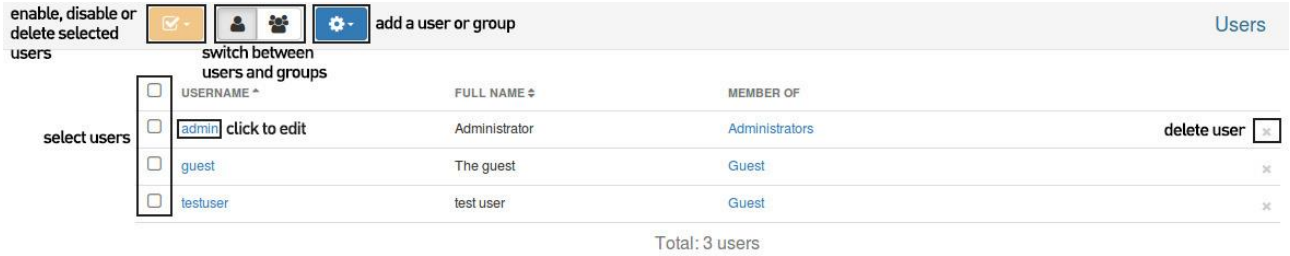
Filtered results will only remain static as long as the auto refresh is disabled. When auto refresh is enabled new logs will be added to the filtered view regardless if they fit the filter or not.

3.11 User Management

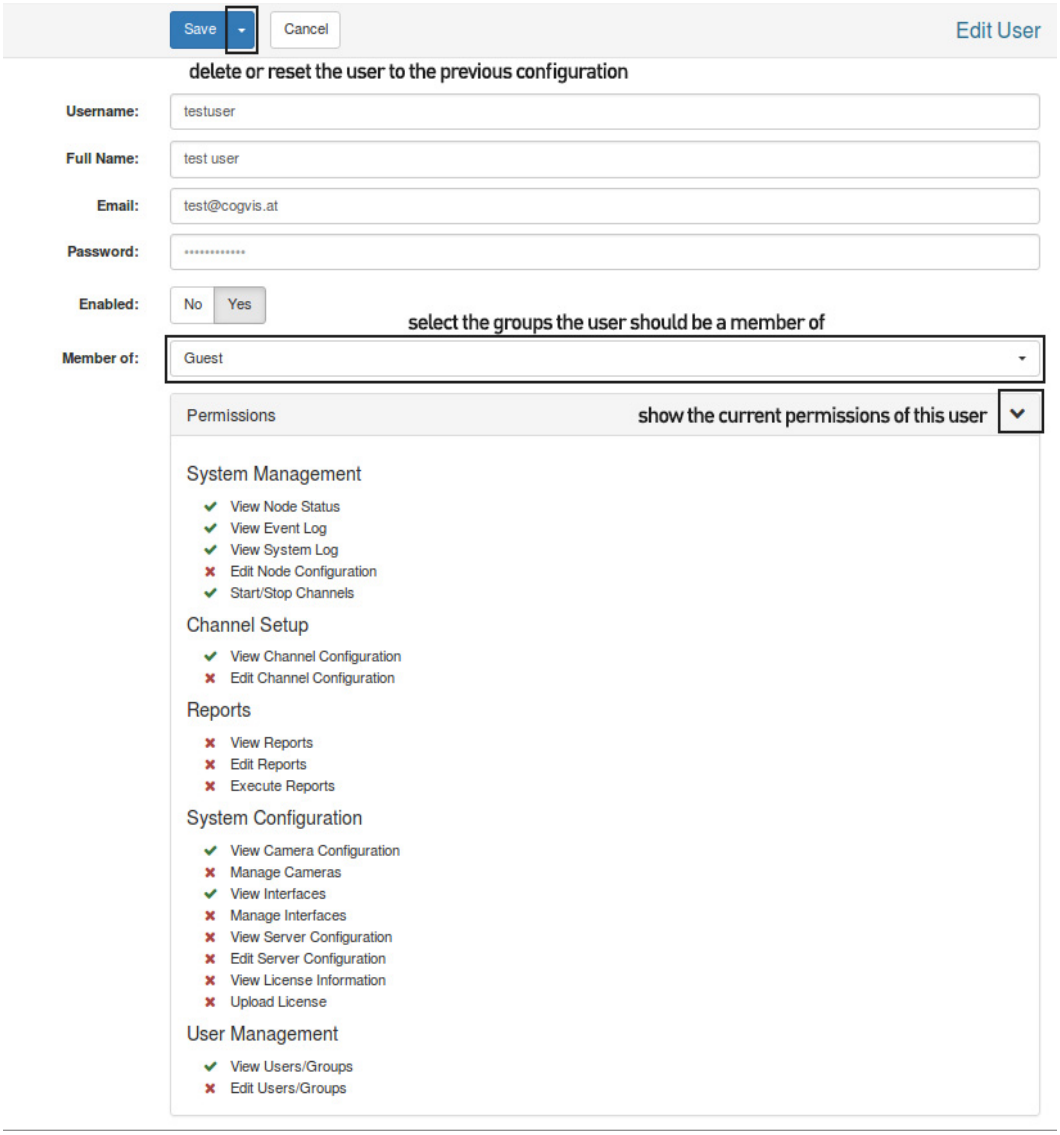
CogVis C3 supports comprehensive user management including user groups to assign different levels of rights to different users. When entering the User and Group Management page you can toggle between the user view and the group view. The basic operations for the user or group are:

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

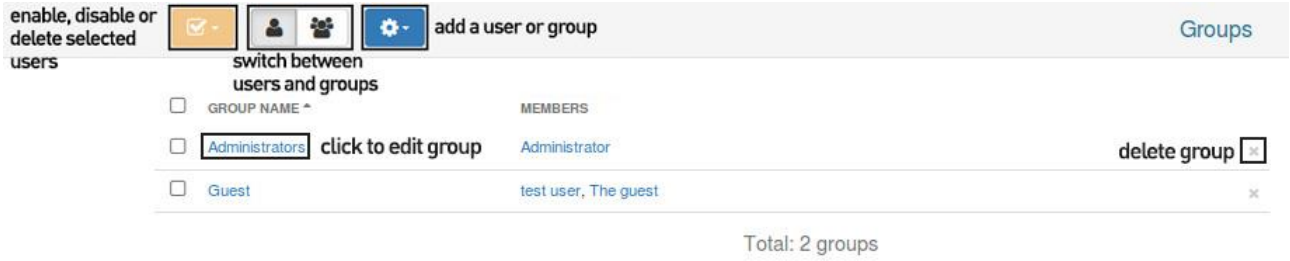
3.11.1 The User View



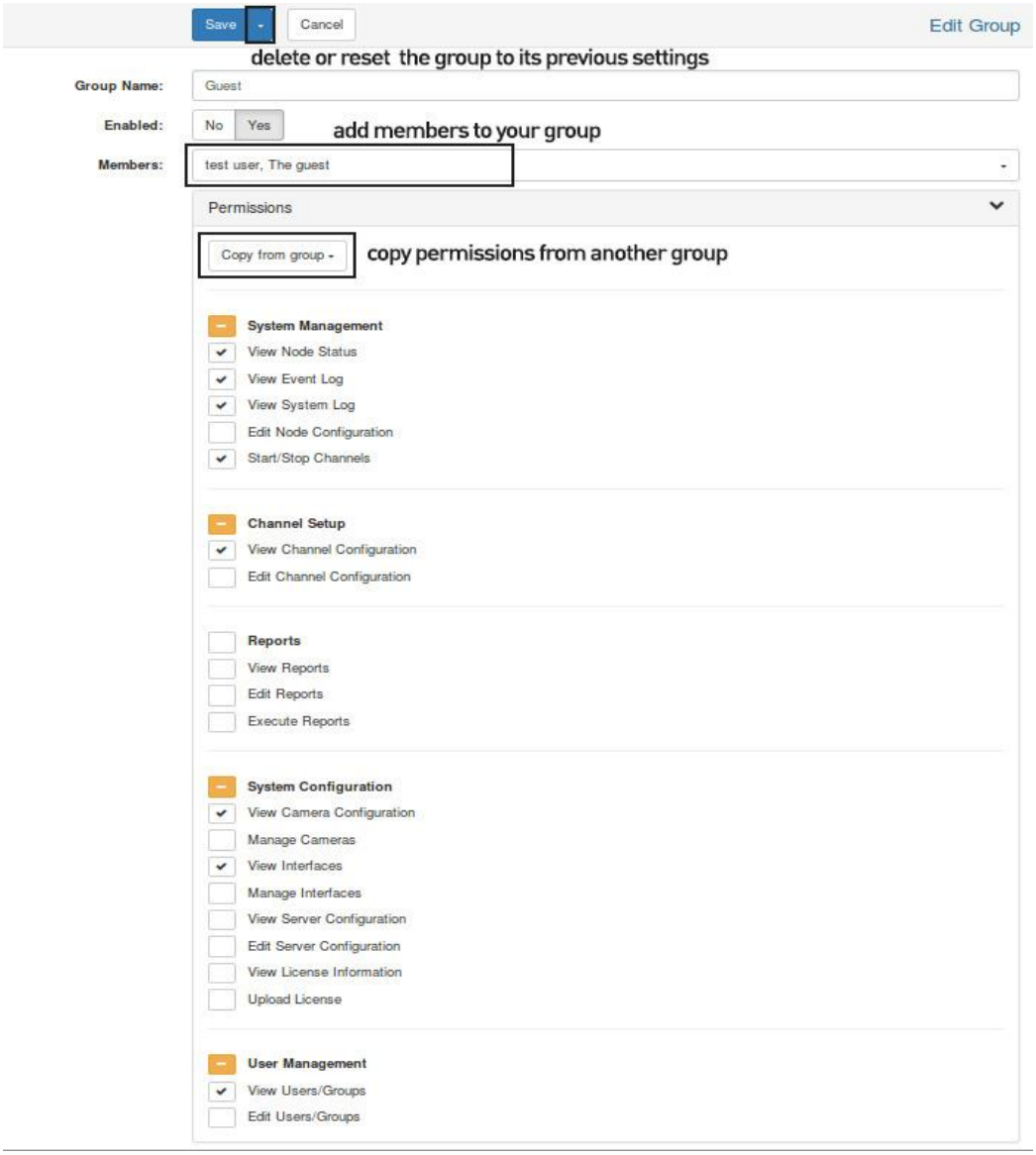
By clicking a username of a certain user or by clicking the *Add user* button you will enter the *Edit User* mode for the user. You can create a new user or edit an existing user here. Permissions for the user are inherited by the user group the user is a member of. The *Permissions* drop-down will lists 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.



3.11.2 The Group View

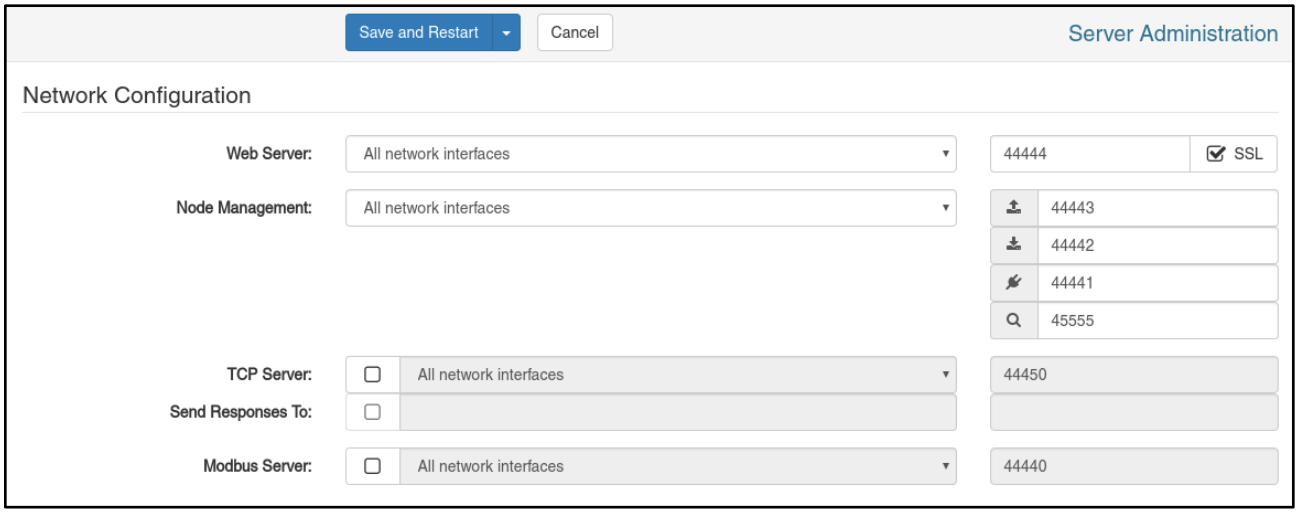


By clicking the name of a group or by adding a group using the *Add Group* button you enter the group edit view. Users can be added to groups here and group permissions can be edited. For faster permission editing permissions can also be copied from another group. By using the submenu of the *Save* button 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:
Guest
Enabled:
No
Yes
add members to your group
Members:
test user, The guest
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*.



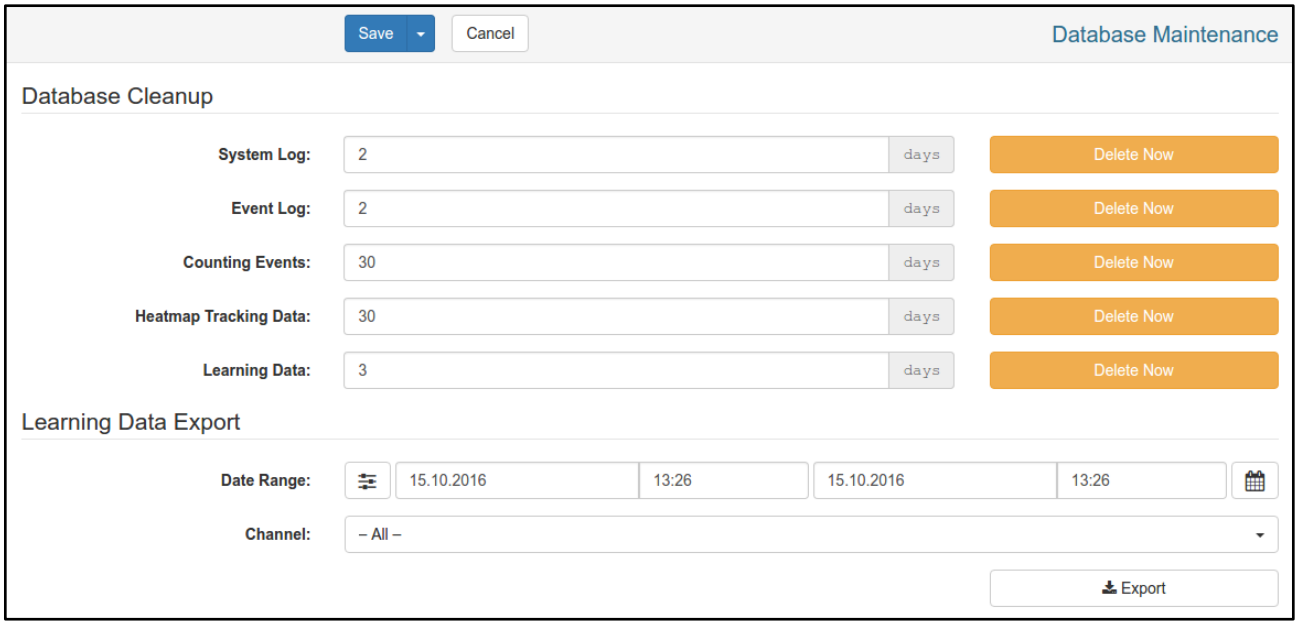
3.12.1 Network Configuration

- **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*.



3.13.1 Database Cleanup

The database cleanup section enables you to configure when the internal database should delete event logs and system logs. By default the system will delete events after 14 days, Logs after 31 days and learning data after 3 days. Counting and Heatmap Tracking Data will be kept in the database for 30 days by default. The system will automatically clean up the database every day but you can also trigger an immediate deletion using the *Delete Now* button. Beware, the deletion can take some time depending on the amount of data you have already stored. If you have little HDD space available you should use smaller cleanup intervals especially for the event log.

3.13.2 Learning Data Export

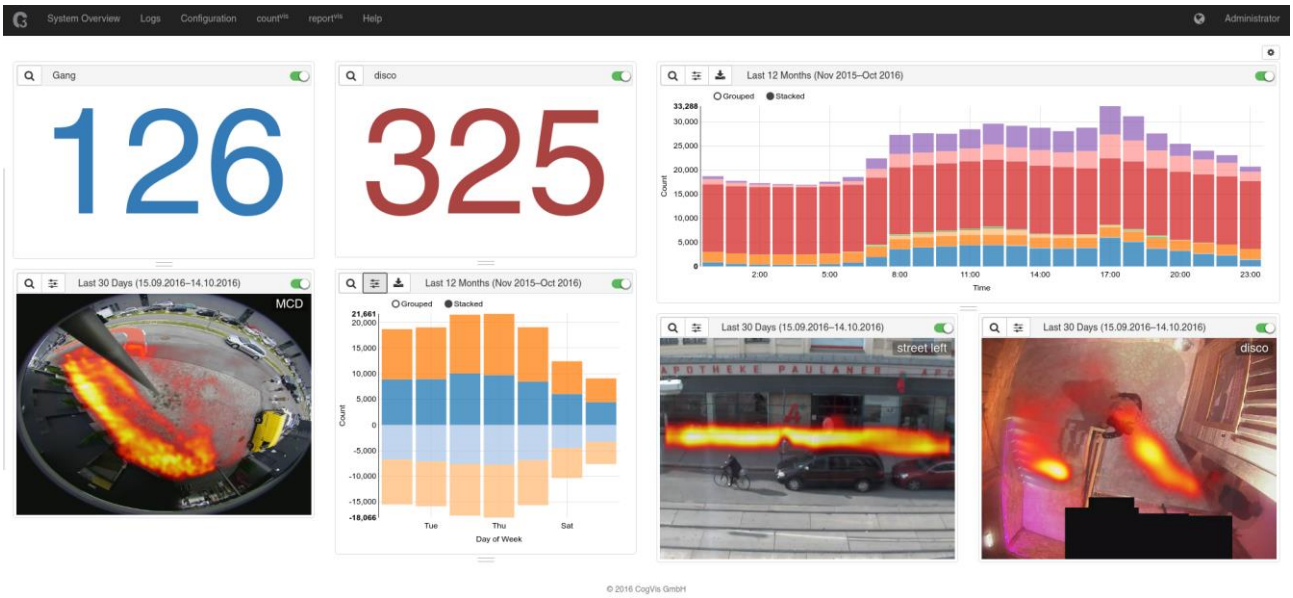
You can export learning data acquired by the server for a certain date range and certain channels. When you click on *Export* you will receive a ZIP file as download from the server. Please beware, if you download a big date range or lots of data, the browser could crash because of the large download file.

3.14 countvis Control

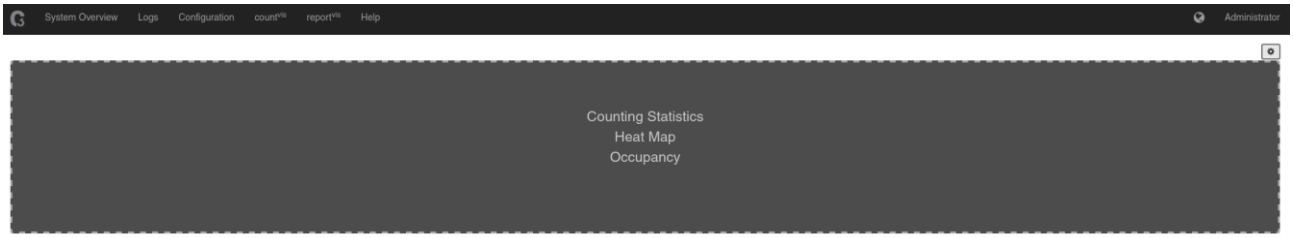
The countvis menu in the main menu bar gives you access to the different views to view your acquired counting and heatmap data. It will give you access to the counting statistics, the occupancy monitor, heatmap and the control for the occupancy areas. The coming sections will give you an overview on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

3.14.1 Dashboard

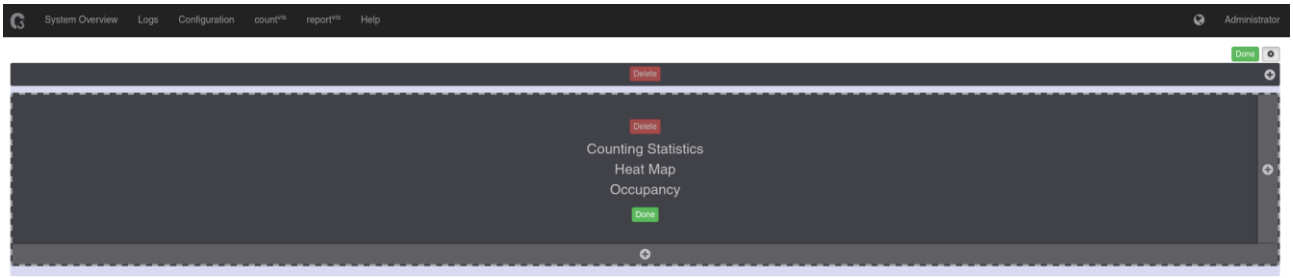
The dashboard is a fully customizable view for your statistical data, heat map data and occupancy areas. The view is based on columns and will automatically adjust to the size of your browser. The view is nested, so each column can hold new rows and columns. Beware, be sure you have a capable system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

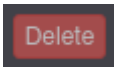


You will start with an empty one column view.



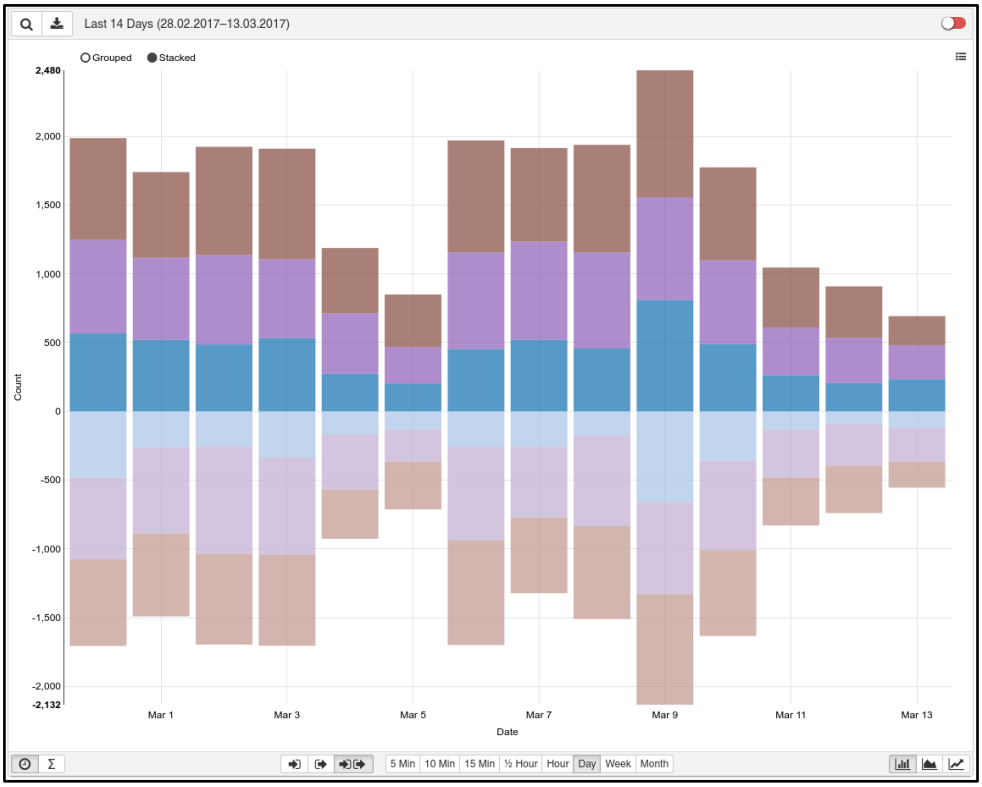
For each dashboard item you can choose between Counting Statistics, Heat Map and Occupancy. To customize your dashboard view hit the edit button at the top right to enter edit mode.



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.

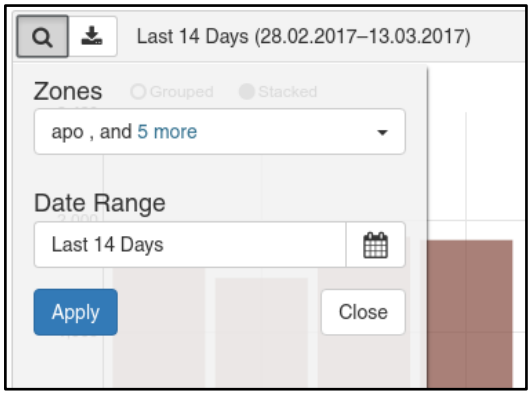


3.14.3 Counting statistics filter menu

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

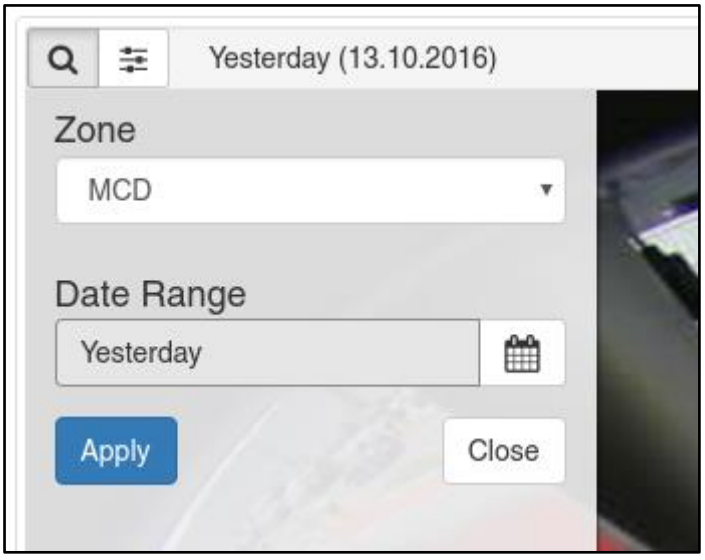
Click to activate or deactivate the auto update functionality.

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

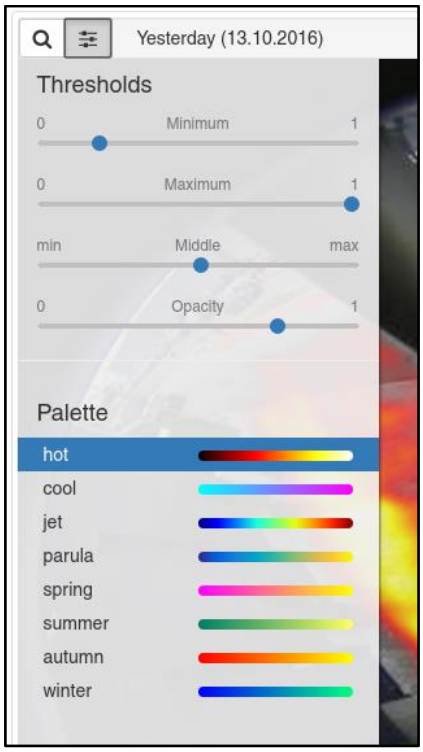
The button will open the zone / time filter panel.



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.

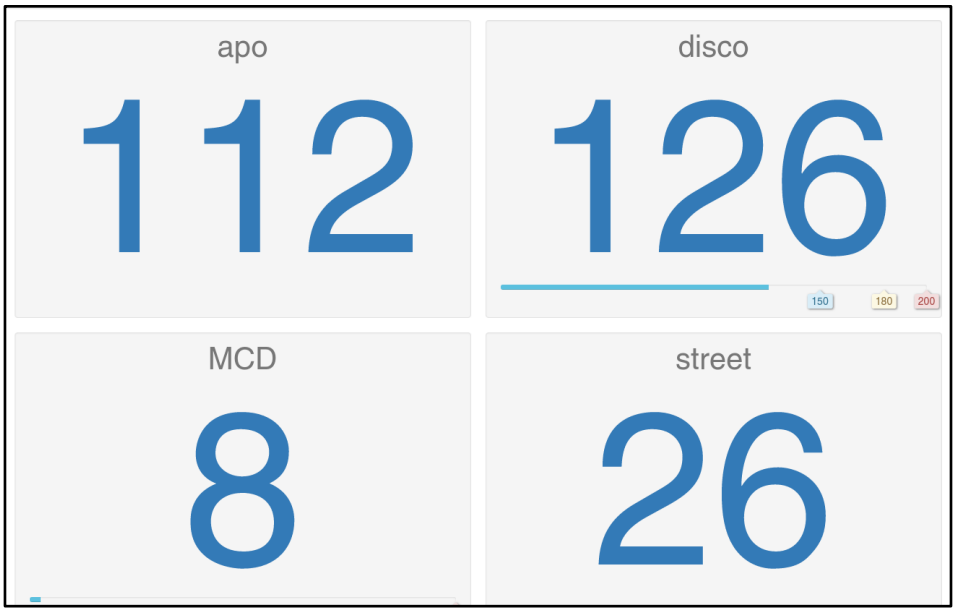
You can toggle between snapshot ( ) and video ( ) mode. In Snapshot mode you can refresh the snapshot by clicking the refresh icon on the right of the control and in video mode you can hit play/pause to control the video on the right of the control.

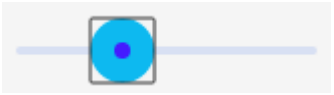
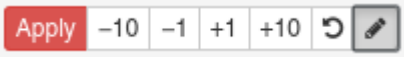
3.14.4.3 Auto Update selector

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 

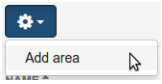
. You can now use the +1, +10 or -1, -10 button to increase or decrease the area count or you can use the reset button to set it to 0 again. Only after you hit apply the new settings will be applied to the occupancy area. If you set any occupancy limits for the areas the area will blink red if the limits 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

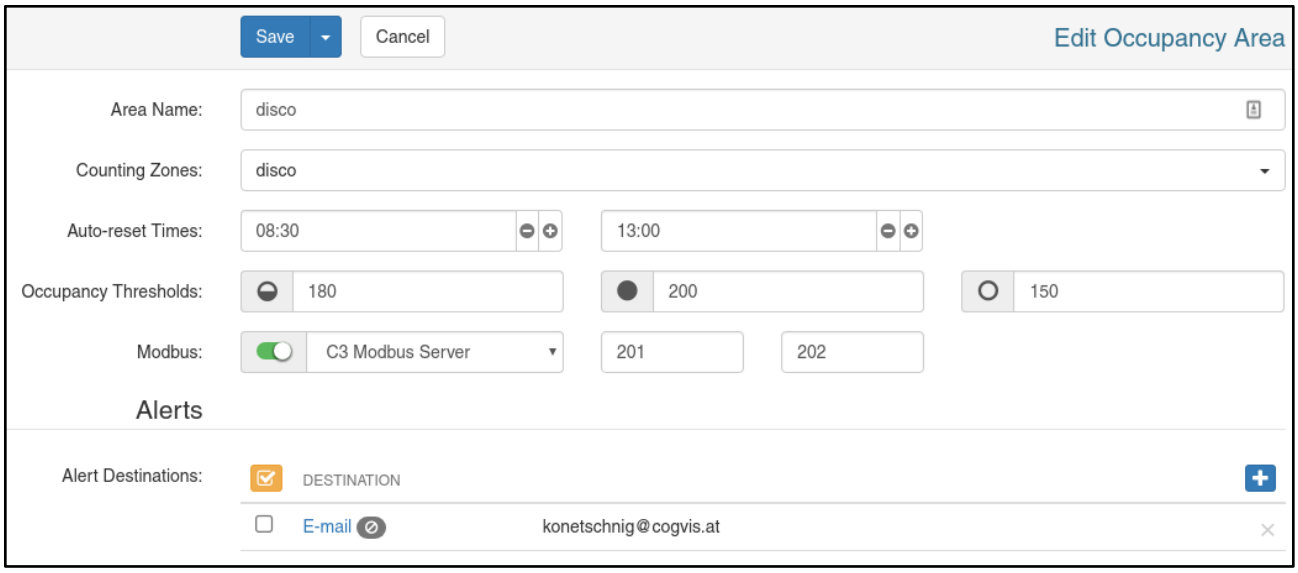
In the occupancy areas view you can manage your occupancy areas. You can add/delete/modify areas to your liking and define reset times and thresholds for the different occupancy areas. Also, if you have Modbus enabled, you will be able to specify Modbus registers for the several occupancy areas. This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

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 

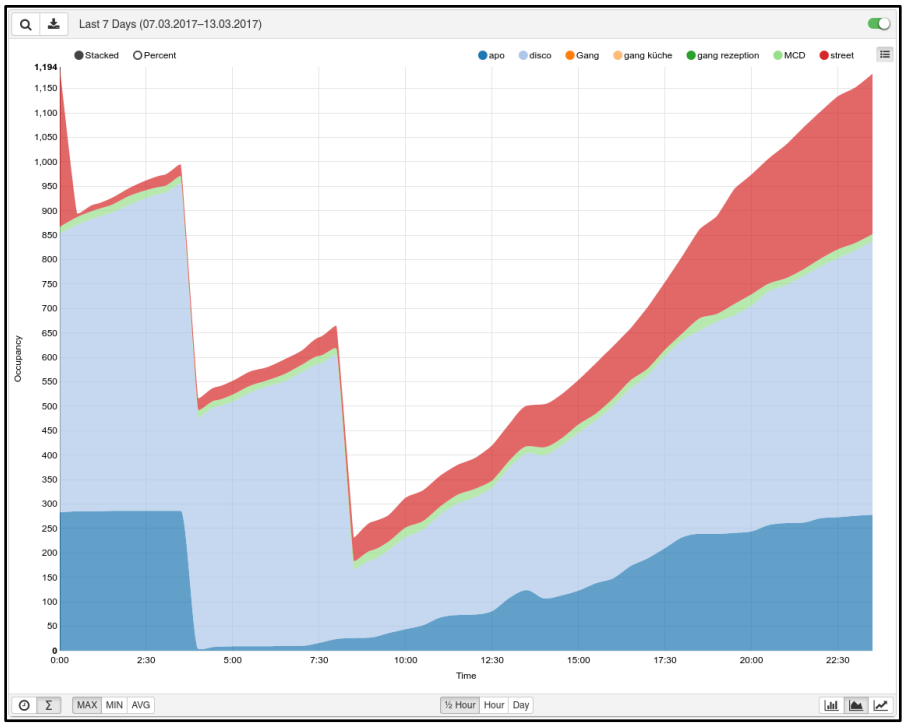
.



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.


Last 7 Days (07.03.2017–13.03.2017)
Stacked
Percent
apo
disco
Gang
gang küche
gang rezeption
MCD
street
Occupancy
1,194
1,150
1,100
1,050
1,000
950
900
850
800
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
0
0:00
2:30
5:00
7:30
10:00
12:30
15:00
17:30
20:00
22:30
Time
MAX
MIN
AVG
½ Hour
Hour
Day

3.15 TCP Command Interface

The TCP command interface can parse plain ASCII Text commands and relay them to the C3 server. This enables you to interact with the C3 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 C3 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.

3.15.1 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.

3.15.2 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 (anonymvis) for groups/channels by group/channel IDs/names		groups:[id,name],...:scrambling_[enabled,disabled]
	static_scrambling_[enable,disable]_[id,name]	enable/disable static scrambling (anonymvis) 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 (anonymvis) 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

3.16 SAIMOS C3 CORE Plugin

3.16.1 About

SAIMOS C3 CORE brings the power of the C3 Analytics 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 C3 CORE and Milestone XProtect® enables users to profit from field proven analytics functionality of C3 while using the full capabilities of Milestone XProtect® for a comprehensive solution experience. The C3 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.

3.16.2 Requirements

3.16.2.1 Minimal Software versions & prerequisites

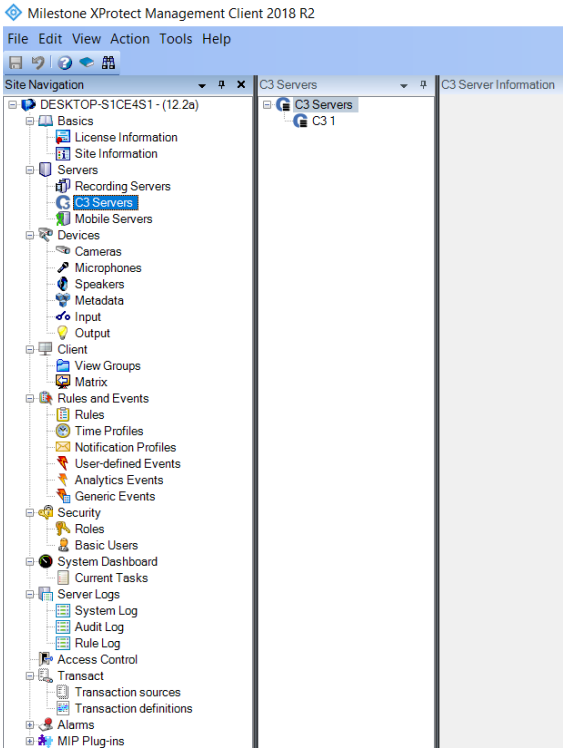
Software	Version
C3 Server	3.2.0
C3 Node	3.2.0
Milestone XProtect	2018 R2 • Essential+ • Express+ • Professional+ • Expert • Corporate
SAIMOS C3 CORE Plugin	2018 R3

3.16.2.2 Minimal Performance requirements for C3

Component	min
CPU	Intel or AMD based CPU with 4 physical cores Passmark: 5000 Single Thread Performance: 1900
RAM	4 GB
HDD	50 GB
Network	Gigabit Ethernet
OS	Windows 7+ 64 Bit Ubuntu 16.04/18.04 64 Bit

3.16.3 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 C3 core from within the Milestone XProtect Management Client. Within the Milestone Management Client the C3 Server icon should be visible in the Servers section ( ). If you click on the C3 Server section you will be able to add C3 Servers and start with your configuration.

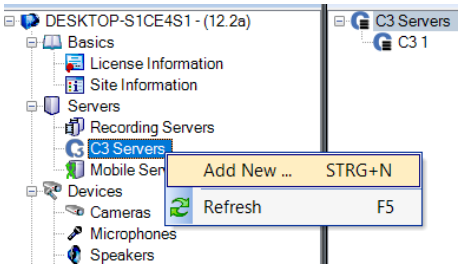


3.16.4 Configuration

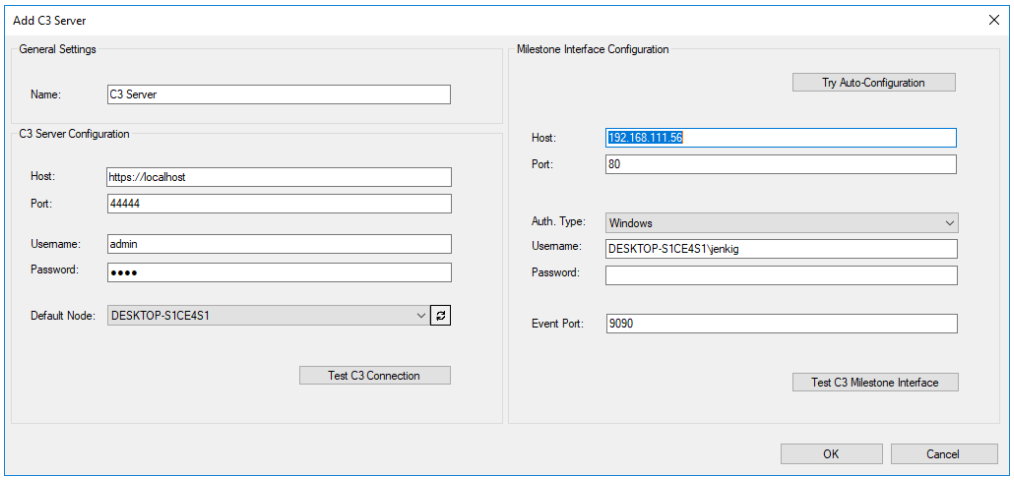
This section will show you how to get a C3 Server configured with Milestone XProtect and how to create a channel. It will give you some details on how channels work and what the most important settings are.

3.16.4.1 Add C3 Server

To add a C3 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:



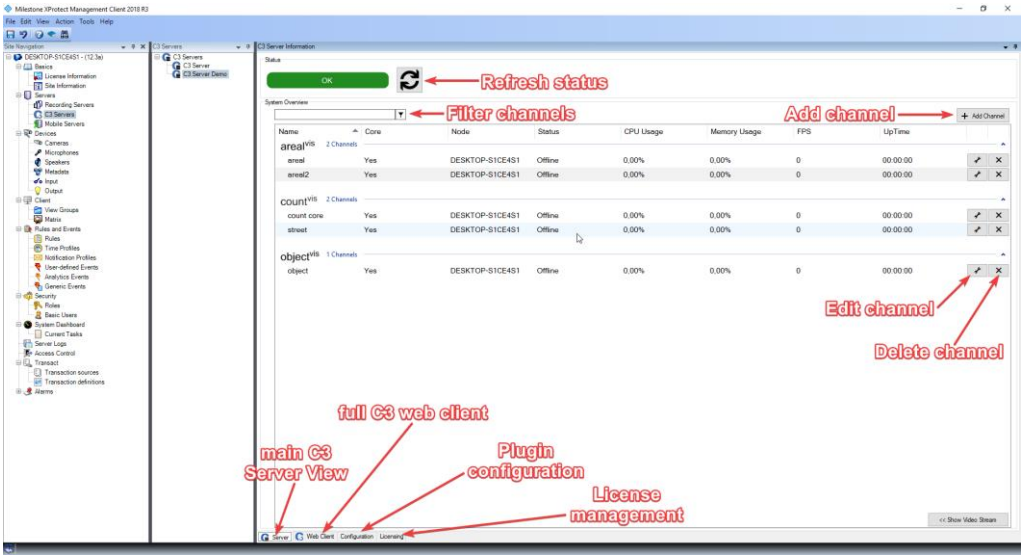
Section	Field	Description
General Settings	Name	Your name for the new C3 Server. Choose wisely.
C3 Server Configuration	Host	Host address on which the C3 Server is running Standard: https://localhost If the server runs on a different machine localhost has to be switched for the IP of the host machine
	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
	Auth. Type	Choose the authentication type. Currently only Windows is working properly with Milestone + Products
	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
	Events Port	Port where Analytic Events can be sent to XProtect Standard: 9090 Be sure the port is activated.
	Test C3 Milestone Interface	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 C3 for communication is automatically generated.

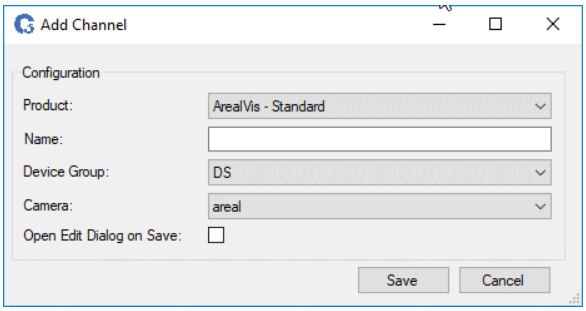
3. Initial configuration is fetched from the C3 Server

Now you should have successfully added the C3 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.



3.16.4.2 Add CORE Channel

To add a CORE channels simply click on the *New* button on the bottom of the *C3 Core Channels* view. A new dialogue will open and you will have to provide the following information:



Field	Description
Product	Choose the product you would want the channel to run. Options are • arealvis (perimeter and areal security) • countvis (people and object counting) • objectvis (left and removed object detection) For each option you can choose between a standard channel (full C3 channel) and a C3 CORE channel.
Name	Choose a name for your channel (choose wisely)
Device Group	Select the device group the chosen camera runs in

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.

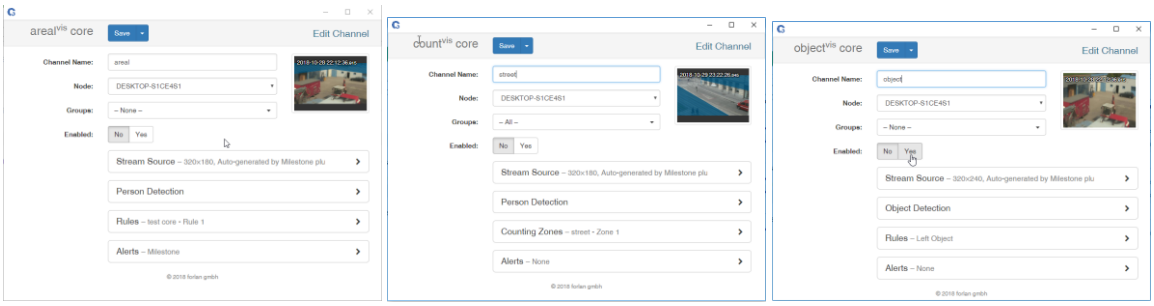
After you have entered the necessary information you can click OK to start the channel creation process. The following things will then happen automatically:

- 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 arealvis) 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.

3.16.4.3 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:

- arealvis
    - Person Detection and Rules
- countvis
    - Person Detection and the Counting Zones
- objectvis
    - Object Detection and Rules

Everything else should be set for a first channel configuration.

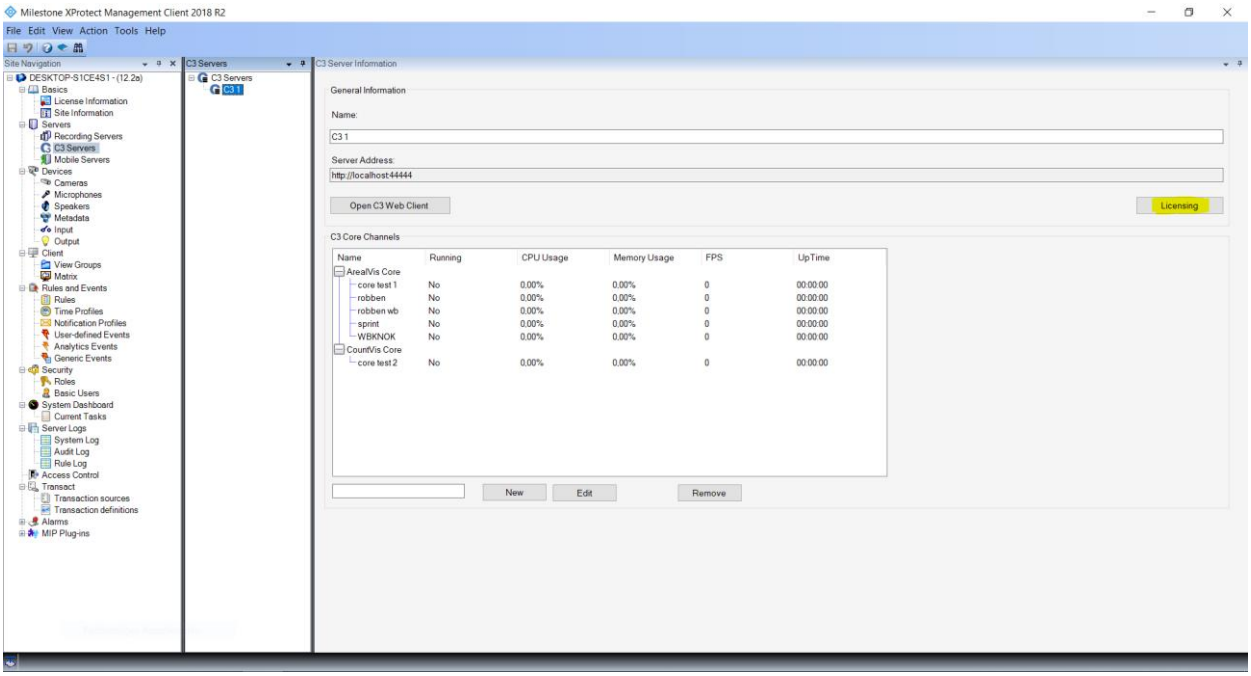
3.16.5 Licensing

The CORE plugin does not need to be licensed and is free to use. After installing the C3 Server and at least one C3 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.

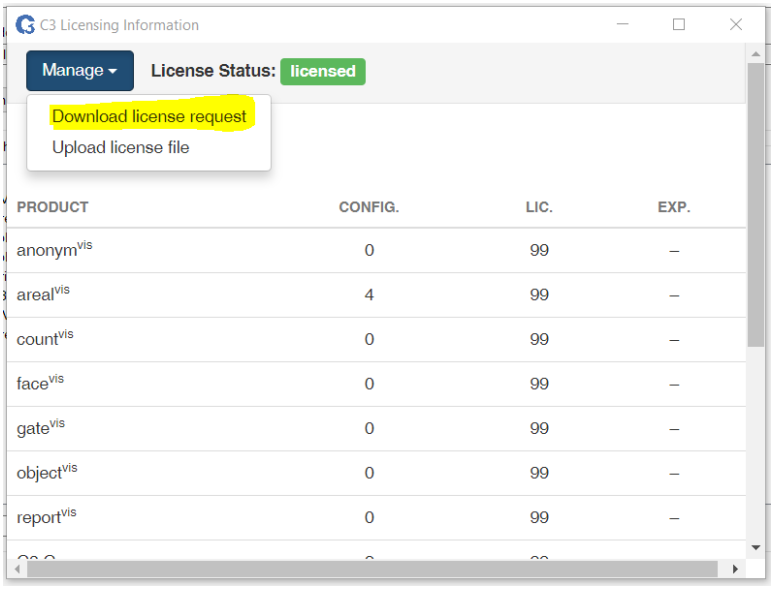
To License the product you will need to complete the following steps:

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

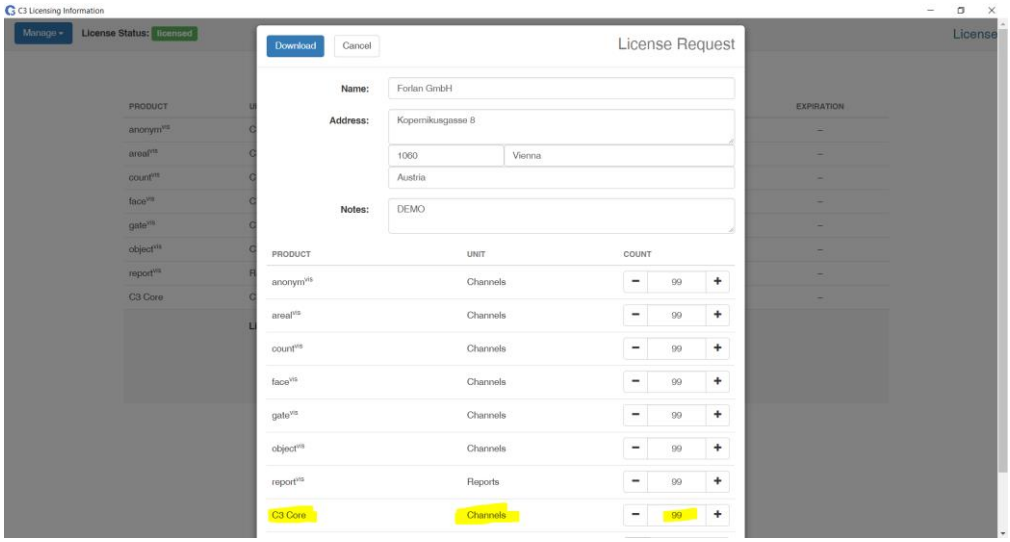
From within the XProtect Management Client use the *Licensing* button in the *General information* field to open the License Management.



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 C3 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.

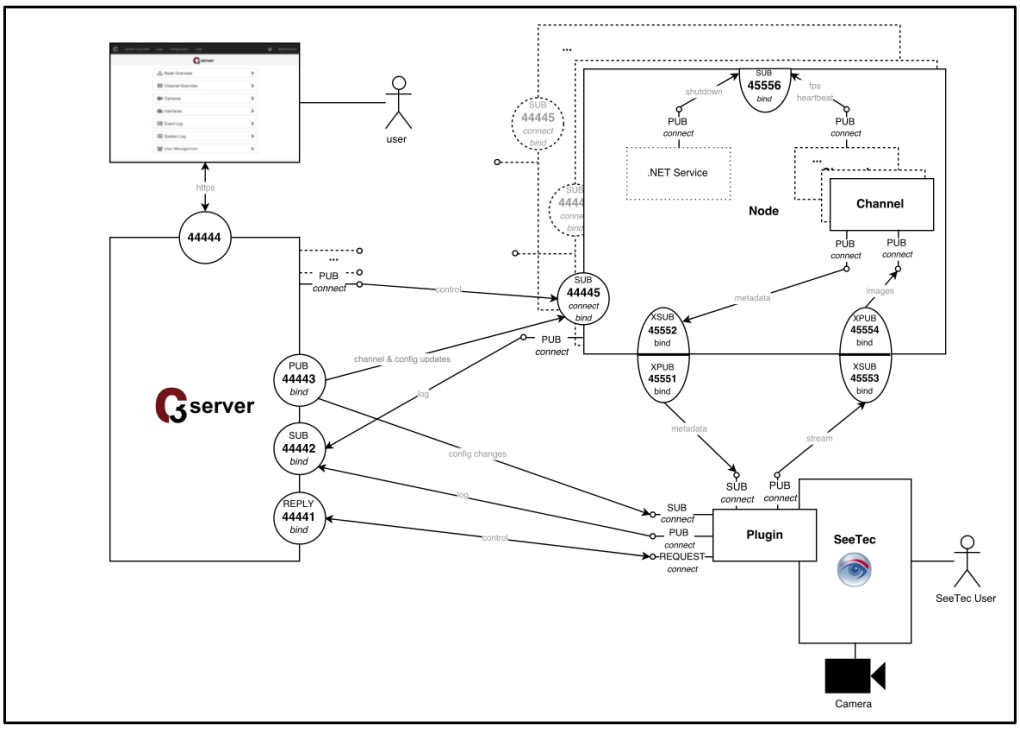
After you have sent the license request to office@for-lan.at after some time you will receive a license file back (ZIP). Use the ZIP file (don't extract) and upload it via the license manager. Using the command *Manage → Upload license file*. After you have successfully uploaded the license file your system will be licensed.

3.17 SeeTec Cayuga Plugin

The C3 SeeTec Cayuga plugin enables the C3 Server & Node to communicate with SeeTec Cayuga directly. You will be able to:

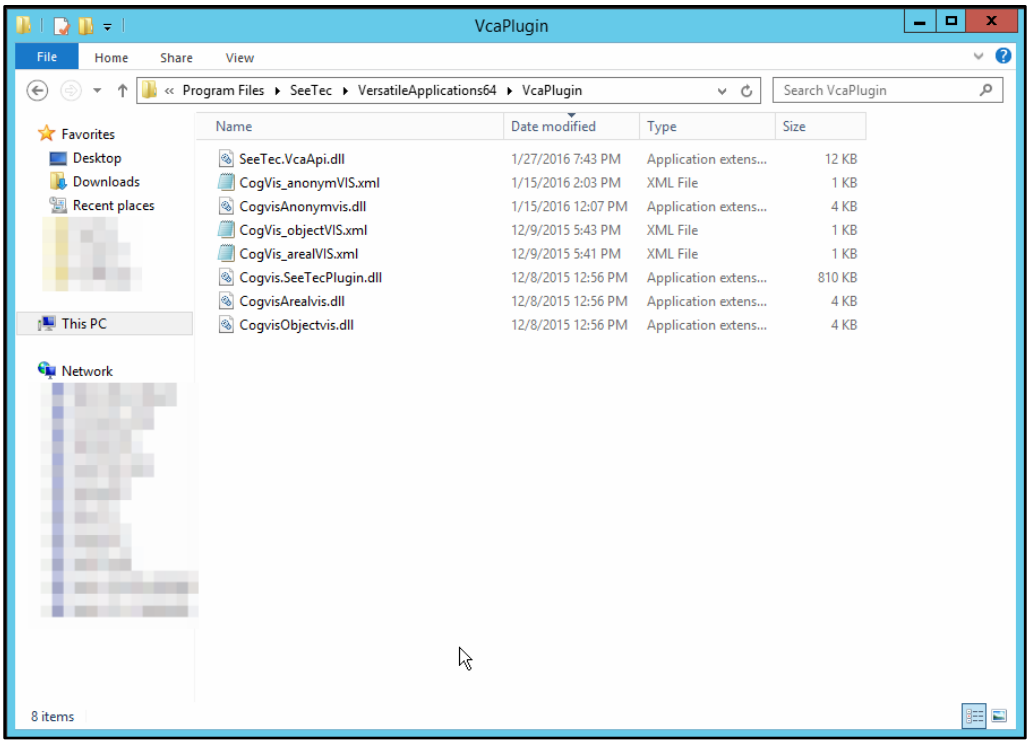
- add C3 channels from directly within SeeTec
- get CCTV footage directly from SeeTec
- use C3 rules as triggers from within the SeeTec Alarm management
- see metadata produced by C3 channels using overlays directly in the Camera views of the SeeTec client

The C3 SeeTec Cayuga plugin communicates via TCP/IP with the C3 Server & Node(s). The communication architecture looks as follows:

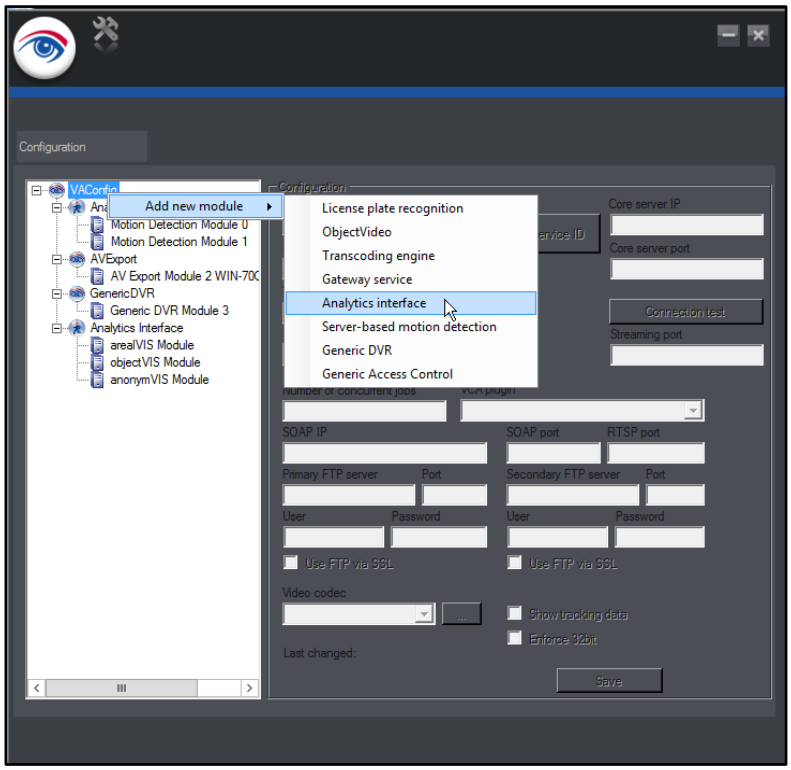


3.17.1 Installing the plugin

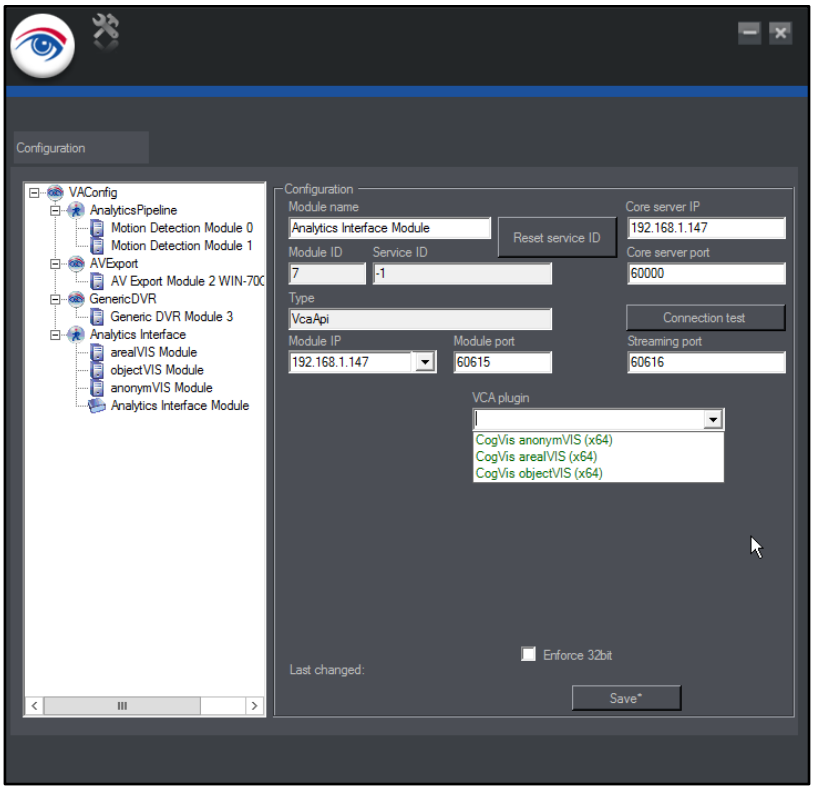
Before you install the plugin be sure that C3 server and node have already been installed properly. To install the plugins first copy all the necessary plugin files (CogVis.SeeTec.Plugin.dll, CogVis*.dll, CogVis_*.xml) to the SeeTec Plugin folder (VersatileApplications64\VcaPlugin for 64 bit or VersatileApplications\VcaPlugin 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.



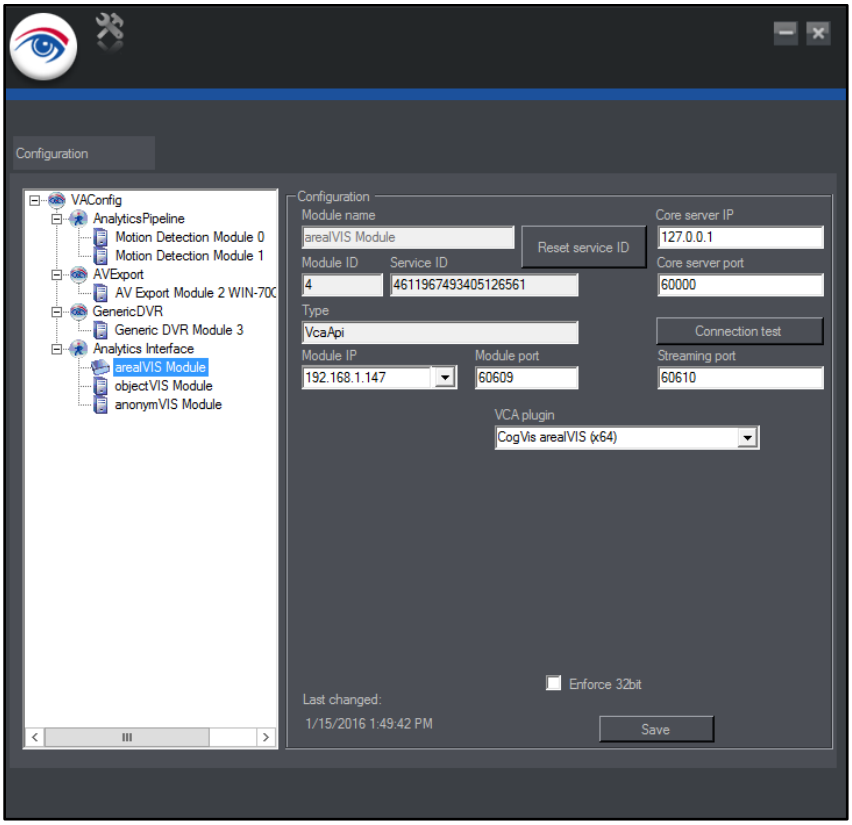
After copying the files open the SeeTec VA Administration and add a new Analytics interface. To do that right-click on the *VAConfig* entry in the left tree view and choose *Add new module --> Analytics interface*.



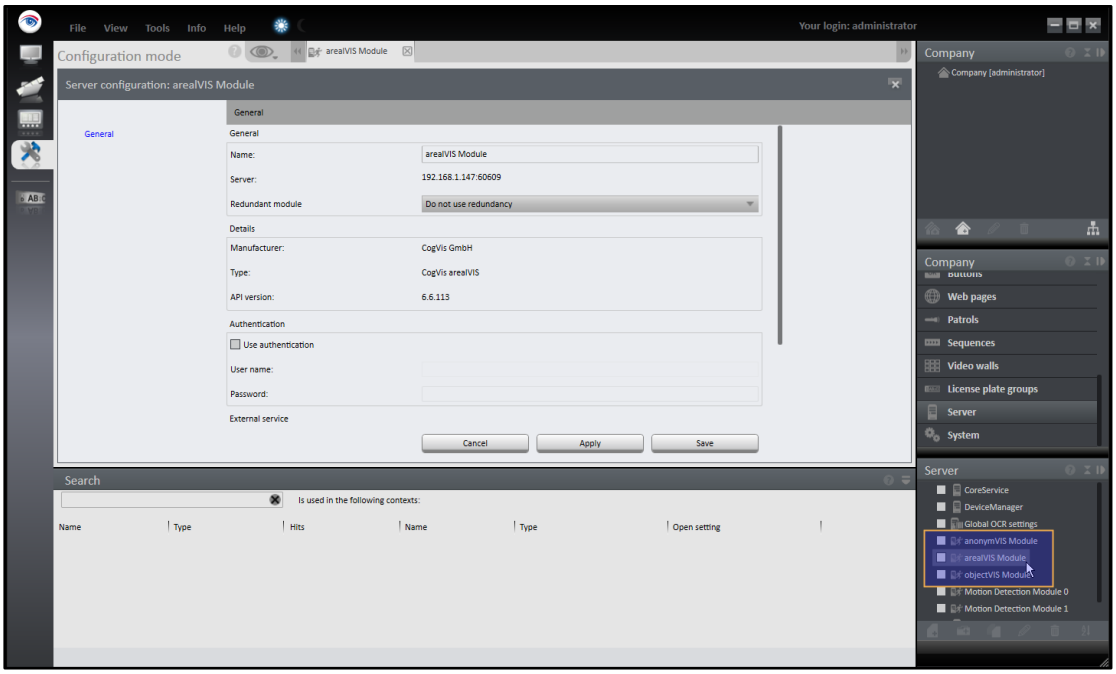
A new module will be added. You can now name the module by choosing a *Module name*. After that check that *Core server IP* and *Module IP* are configured correctly for your system. You now only have to select the correct VCA plugin within the drop down menu and click *Save*.



A correctly added module can look like this:

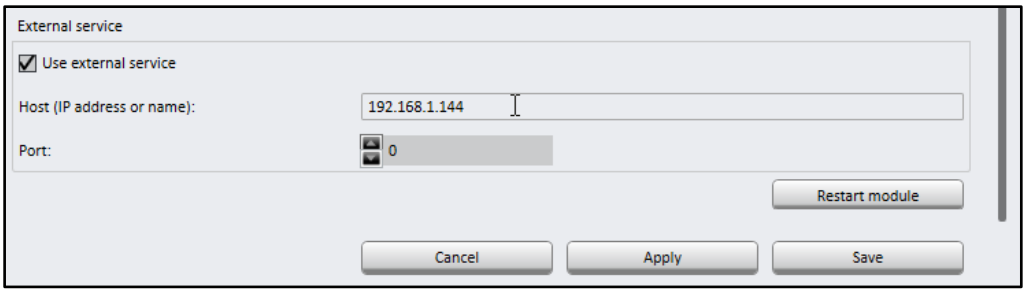


To ensure proper functionality, finally, please restart the *SeeTec VA* service. If everything worked well you should see the new C3 interface within the SeeTec configuration under *Server*.



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 C3 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.

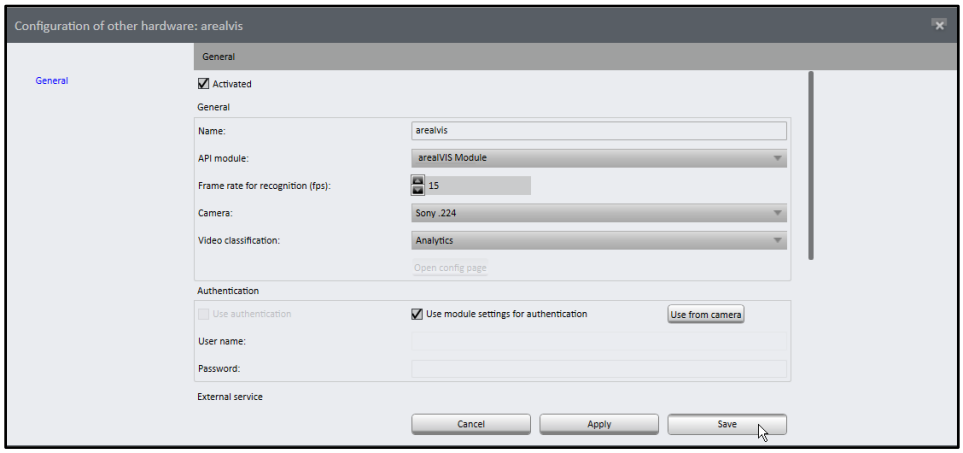
Note: If you did not change any standard Ports within the C3 system you can leave the Port option at 0. Otherwise you would have to insert the communication port to the server in this field.



3.17.2 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 C3 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*.

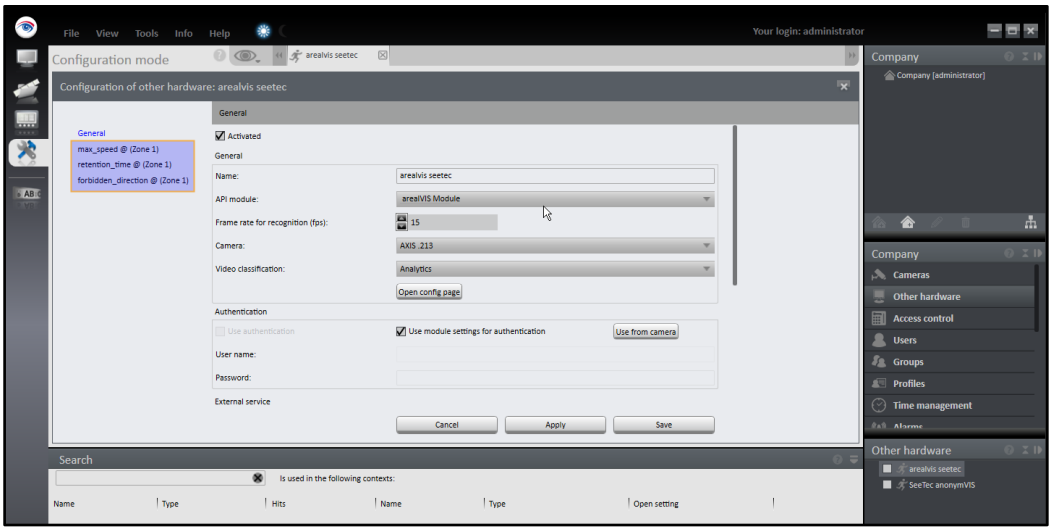


The channel should then come to live within the C3 server interface on a node and you can start configuring it there.

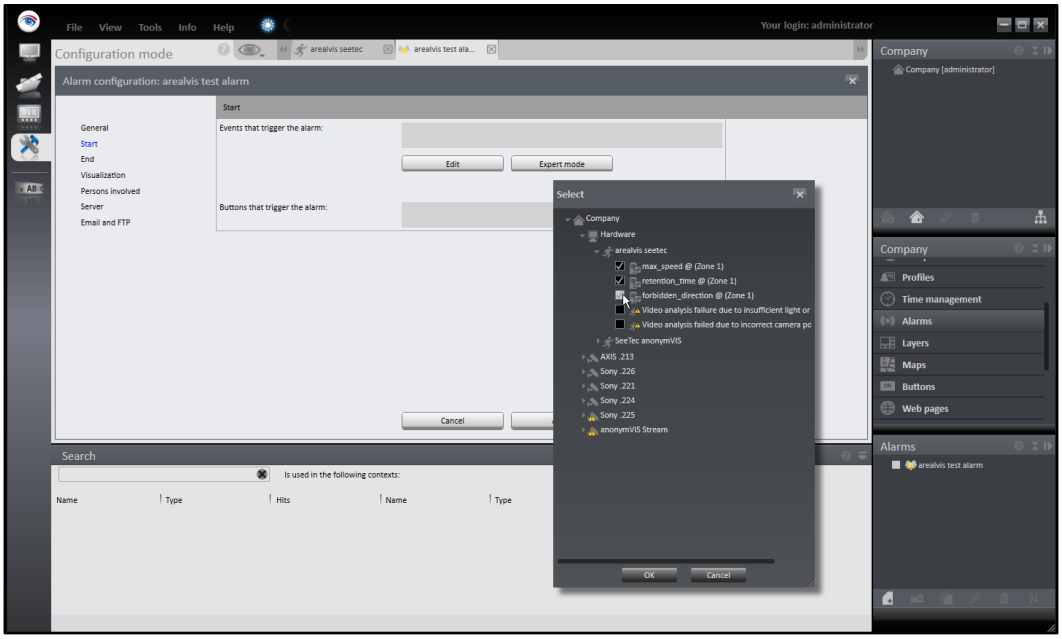
Important: The channel will be already added with the correct stream source so you only need to change the Region of Interest within the Stream Source settings of the channel. Also, metadata and event forwarding to SeeTec will be handled automatically, you don't have to add a separate alert for that.

3.17.3 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 C3 channels that actually send metadata).



The rules will comply with the rules added within the web configuration of C3. 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 CogVis 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.

3.17.4 Troubleshooting

If you have troubles, try to restart the VA service of SeeTec and check the plugin log of C3. It will be located on the Server where the C3 plugin is installed in the folder *C:\ProgramData\CogVis3\plugin\log*. If you contact 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 C3 using either the backup and restore routines of the C3 package or simple Postgres backup strategy.

4.1 Backing up C3 using PGSQL commands

Backing up C3 is as simple as creating a DB dump of the C3 system. You can use the in package PGSQL commands of C3 (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 backup 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
```

Essential backup command example (only essential configuration 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_20181103T211951.dmp --exclude-table-data=snapshot_cache --
exclude-table-data=system_log --exclude-table-data=count_event_log --exclude-table-data=counting_data -
-exclude-table-data=counting_data_5min --exclude-table-data=counting_data_10min --exclude-table-
data=counting_data_15min --exclude-table-data=counting_data_30min --exclude-table-
data=counting_data_hourly --exclude-table-data=counting_data_daily --exclude-table-
data=counting_data_weekly --exclude-table-data=counting_data_monthly --exclude-table-data=heatmap_data
--exclude-table-data=heatmap_hourly --exclude-table-data=heatmap_daily --exclude-table-data=event_log -
-exclude-table-data=event_sequences --exclude-table-data=face_event_log --exclude-table-data=faces --
exclude-table-data=learning_data
```

4.2 Restoring C3 from a backup using PGSQL commands

To restore a C3 from a previous dump you will have to stop the C3 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 C3 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 pgsql
  -u USER, --user USER  User for PGSQL C3 user
  -p PASSWORD, --password PASSWORD
                        Password for PGSQL C3 user
```

4.3.1 Examples

Full backup 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
```