

INTELLIO VIDEO SYSTEM 4



Installation Manual

(Version: 4.7.2.1)

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Network Structure | 9 |
| 2 | Installing the Software..... | 10 |
| 2.1 | Installation of Intellio Server 4 | 10 |
| 2.1.1 | Steps of the Installation..... | 10 |
| 2.1.2 | Updating IVS..... | 11 |
| 2.1.3 | Determine the Status of the Software..... | 11 |
| 2.2 | Installation of Intellio Client 4 | 13 |
| 3 | Client Settings | 13 |
| 3.1 | Displays | 13 |
| 3.2 | General | 14 |
| 3.2.1 | Live..... | 14 |
| 3.2.2 | Alarms..... | 14 |
| 3.2.3 | Layout..... | 15 |
| 3.2.4 | Audio | 15 |
| 3.2.5 | Playback..... | 15 |
| 3.2.6 | Bandwidth | 16 |
| 3.2.7 | Joystick..... | 16 |
| 3.3 | Performance..... | 16 |
| 3.3.1 | Global | 16 |
| 3.3.2 | Playback..... | 17 |
| 4 | System Setup..... | 18 |
| 4.1 | Logging in to a Site..... | 18 |
| 4.2 | Creating a Video Buffer..... | 20 |
| 4.3 | Adding Cameras/Encoders to Intellio Video System 4 | 21 |
| 4.3.1 | Discovering Network Cameras with Scanning | 21 |
| 4.3.2 | Adding New Cameras/Devices Manually..... | 22 |
| 4.3.3 | Adding Camera with External IP Address | 31 |
| 4.4 | Registering Cameras and Devices | 34 |
| 4.4.1 | Camera/Device Replacement | 34 |
| 4.5 | Setting the Audio Input..... | 35 |
| 4.6 | Editing the Camera Index List | 36 |
| 5 | Storage | 37 |
| 5.1 | Storage Settings..... | 37 |
| 5.1.1 | Factors of Storage Capacity | 37 |
| 5.2 | Buffers | 37 |
| 5.3 | Storage Groups | 39 |
| 5.3.1 | Storage Mode..... | 39 |

| | | |
|----------|---|-----------|
| 5.3.2 | Week Scheduler | 40 |
| 5.3.3 | Exceptions | 40 |
| 5.3.4 | Retention Period..... | 41 |
| 5.3.5 | Long-term Storage..... | 42 |
| 5.3.6 | Moving Devices Between Groups | 43 |
| 5.3.7 | Enabling/Disabling Recording..... | 43 |
| 5.4 | Storing Footage on a Memory Card..... | 43 |
| 5.5 | Tools for Measuring the Storage Requirements..... | 45 |
| 5.6 | Managing Archive Files..... | 46 |
| 5.6.1 | Backing Up Buffers..... | 46 |
| 5.6.2 | Restoring Archive Files..... | 46 |
| 6 | Video Adjustment (<i>Image Settings</i>) | 47 |
| 6.1 | ILC and ILN series | 47 |
| 6.1.1 | Brightness | 47 |
| 6.1.2 | Exposure | 47 |
| 6.1.3 | Color..... | 48 |
| 6.1.4 | White Balance..... | 48 |
| 6.1.5 | Day/Night..... | 48 |
| 6.1.6 | Compression | 49 |
| 6.1.7 | Advanced..... | 49 |
| 6.1.8 | Sharpen | 50 |
| 6.1.9 | Graph..... | 50 |
| 6.2 | ILD series | 51 |
| 6.2.1 | Day and Night Profile..... | 51 |
| 6.2.2 | General | 51 |
| 7 | Sensor Settings..... | 55 |
| 8 | Display Settings | 55 |
| 9 | Encoder Settings..... | 55 |
| 9.1 | ORIO cameras..... | 55 |
| 9.1.1 | General | 55 |
| 9.1.2 | Frame Rate Control | 56 |
| 9.1.3 | Pre/Post Alarm | 56 |
| 9.2 | VISUS cameras..... | 56 |
| 9.2.1 | General | 56 |
| 9.2.2 | Frame Rate Control | 56 |
| 9.2.3 | Pre/Post Alarm | 57 |
| 9.2.4 | Secondary Encoder Settings..... | 57 |
| 9.3 | ONVIF Cameras..... | 57 |

| | | |
|-----------|--|-----------|
| 9.3.1 | Profile Settings | 57 |
| 9.3.2 | Editing Media Profile | 58 |
| 9.3.3 | Video Encoder Options | 58 |
| 9.3.4 | Audio Encoder Options..... | 59 |
| 9.4 | Datastream..... | 59 |
| 10 | Grouped Camera Setting..... | 60 |
| 11 | Motion Sensors..... | 61 |
| 11.1 | ILD Motion Sensor..... | 61 |
| 11.1.1 | Calibrating the Motion Sensors..... | 61 |
| 11.2 | Motion Detector for ONVIF, RTSP and MJPEG Videostreaming | 62 |
| 12 | EPTZ and PTZ..... | 63 |
| 13 | Privacy Zones..... | 63 |
| 14 | Camera Navigation..... | 64 |
| 14.1 | Editing Navigation Arrows | 64 |
| 14.2 | Navigation name..... | 65 |
| 14.3 | Target camera | 65 |
| 14.4 | Navigation arrows..... | 65 |
| 14.5 | Go to Target Camera | 65 |
| 14.6 | Back to Previous Camera..... | 65 |
| 14.7 | Place Backward Navigation..... | 65 |
| 14.8 | Delete Selected | 65 |
| 15 | Camera Groups..... | 66 |
| 16 | User Rights/User Roles..... | 66 |
| 16.1 | User Roles | 67 |
| 16.1.1 | Creating User Roles | 67 |
| 16.1.2 | Deleting User Roles..... | 67 |
| 16.2 | Users..... | 68 |
| 16.2.1 | Creating New Users..... | 68 |
| 16.2.2 | Editing User Details | 68 |
| 17 | System Log and Error Reporting | 69 |
| 18 | The Intellio System | 70 |
| 18.1 | Camera Takeover | 70 |
| 18.1.1 | Camera Locking..... | 70 |
| 18.2 | Load Balancing..... | 71 |
| 18.3 | Site..... | 71 |
| 18.3.1 | Add Server to the Site..... | 72 |
| 18.3.2 | Change Master Server | 72 |
| 18.3.3 | Modify the Data of Servers | 72 |

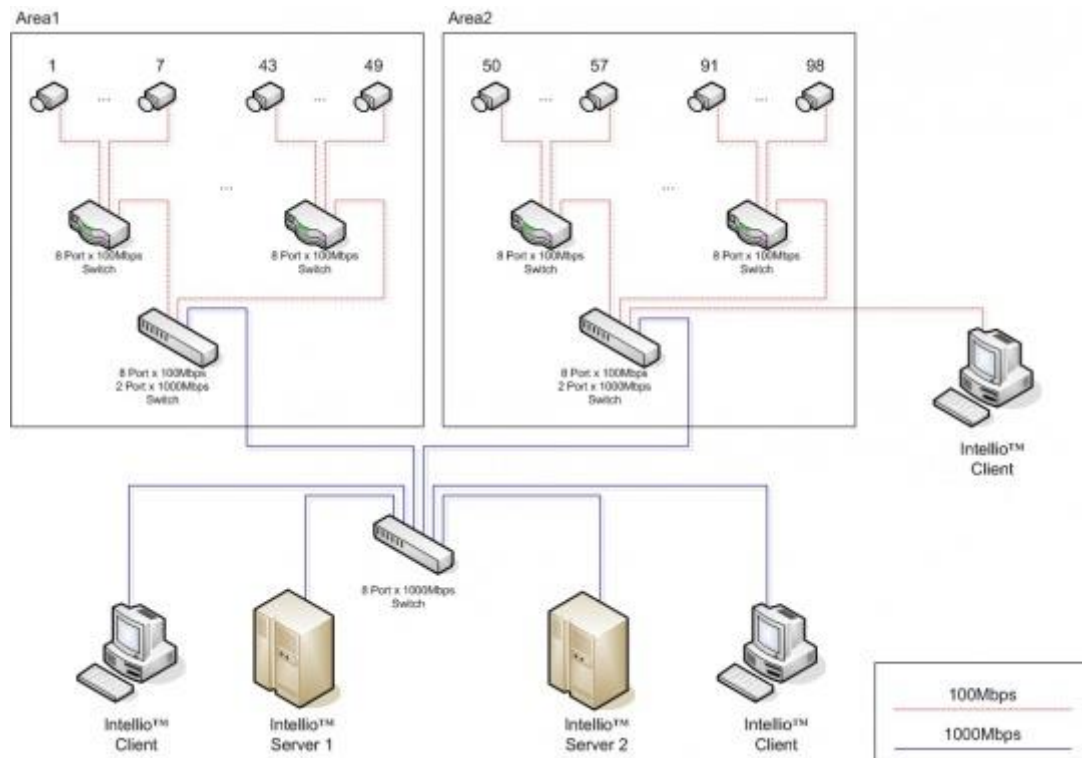
| | | |
|-----------|--|-----------|
| 18.3.4 | Delete Server | 73 |
| 18.3.5 | Clients | 73 |
| 18.4 | Domain..... | 74 |
| 18.4.1 | Domain Enlargement | 74 |
| 18.4.2 | Deleting Sites | 74 |
| 18.5 | Configuring Internet Access | 75 |
| 18.5.1 | General Server Side Settings..... | 75 |
| 18.5.2 | Server side settings for the IMC (<i>mobile client</i>)..... | 75 |
| 18.5.3 | IVS Client Internet Connection Configuration..... | 76 |
| 18.5.4 | IMC (<i>mobile client</i>) Internet Connection Configuration | 76 |
| 19 | Firmware Update | 77 |
| 19.1 | Updating Intellio Camera Firmware | 77 |
| 20 | The Alarm System | 78 |
| 21 | Actions..... | 78 |
| 21.1 | Creating Actions..... | 79 |
| 21.1.1 | General tab..... | 79 |
| 21.1.2 | Action tab..... | 79 |
| 21.1.3 | Servers tab | 79 |
| 21.1.4 | Event Filter tab | 79 |
| 21.2 | Internet Actions | 80 |
| 21.2.1 | Send E-mail | 80 |
| 21.3 | Camera Actions..... | 80 |
| 21.3.1 | Go to Preset Action | 80 |
| 21.4 | Server Actions | 81 |
| 21.4.1 | Log Events Action | 81 |
| 21.4.2 | Camera Alarm State Action..... | 81 |
| 21.4.3 | Multi IO Action | 82 |
| 21.4.4 | Database Action..... | 82 |
| 21.4.5 | Partition Arming Action..... | 83 |
| 21.4.6 | Launch Program Action | 83 |
| 21.4.7 | ANPR Database Action..... | 84 |
| 21.4.8 | Storage Group Action..... | 85 |
| 21.4.9 | Visiscanner Database Action | 85 |
| 22 | Partitions..... | 86 |
| 23 | Detectors..... | 87 |
| 23.1 | Installing a Detector | 87 |
| 23.2 | General Description of a Detector..... | 88 |
| 23.2.1 | Detector Types..... | 88 |

| | | |
|-----------|--|------------|
| 23.2.2 | Tracker Based Detectors..... | 88 |
| 23.2.3 | The Frame of a Detector | 88 |
| 23.2.4 | Creating Masks..... | 89 |
| 23.2.5 | Calibrating the Camera..... | 91 |
| 23.2.6 | Configuring the Tracker..... | 92 |
| 23.3 | Onboard Detectors..... | 94 |
| 23.3.1 | Sabotage Detector | 94 |
| 23.3.2 | Motion Detector..... | 94 |
| 23.3.3 | Object Removal/Theft Detector | 95 |
| 23.3.4 | Covering Detector..... | 96 |
| 23.3.5 | Rotation Detector..... | 97 |
| 23.3.6 | IO Input Detector..... | 97 |
| 23.3.7 | Built-in ANPR Detector..... | 98 |
| 23.4 | Tracker Based Onboard Detectors | 99 |
| 23.4.1 | Entry Detector | 99 |
| 23.4.2 | Direction Detector..... | 100 |
| 23.4.3 | Tripwire Detector..... | 101 |
| 23.4.4 | Intelligent Motion Detector | 102 |
| 23.5 | System Detectors..... | 103 |
| 23.5.1 | Camera Availability Detector..... | 103 |
| 23.5.2 | Site State Detector..... | 103 |
| 23.5.3 | Video Motion Detector | 103 |
| 23.5.4 | License Plate Detector..... | 104 |
| 23.5.5 | VisiScanner Analytics..... | 104 |
| 23.5.6 | TCP Event Receiver | 105 |
| 23.5.7 | Multi IO Input Detector..... | 105 |
| 23.5.8 | Device Event Detector (<i>ONVIF, Samsung</i>)..... | 106 |
| 24 | Hidden Detectors..... | 106 |
| 24.1 | Built-in Intelligent Motion Detector | 106 |
| 24.2 | Hidden PTZ Preset Detector..... | 106 |
| 25 | Virtual Detectors | 107 |
| 26 | Accessories..... | 107 |
| 26.1 | Multi I/Os..... | 107 |
| 26.1.1 | Specification | 107 |
| 26.1.2 | Setup..... | 108 |
| 27 | ANPR | 109 |
| 27.1 | The Carmen FreeFlow Engine..... | 109 |
| 27.1.1 | Installation of Carmen FreeFlow | 109 |

| | | |
|-----------|--|------------|
| 27.2 | Camera Positioning and Adjustment | 110 |
| 27.3 | Video Adjustment for ANPR | 111 |
| 27.4 | License Plate Recognition | 111 |
| 27.4.1 | Configure License Plate Recognition | 111 |
| 27.4.2 | Control of Functioning ANPR Process | 113 |
| 27.4.3 | Edit License Plate List | 116 |
| 27.4.4 | Edit License Plate Groups | 116 |
| 27.4.5 | Manual Entry | 116 |
| 28 | Map | 117 |
| 28.1 | Map Settings | 118 |
| 28.2 | Location | 119 |
| 28.3 | Building | 119 |
| 28.4 | Level | 119 |
| 28.5 | Camera | 120 |
| 28.6 | Detector | 121 |
| 29 | Panorama | 122 |
| 29.1 | Creating Panorama | 122 |
| 29.2 | Automatic Aligning | 123 |
| 30 | RTSP Users | 124 |
| 30.1 | RTSP Gateway Setup | 124 |
| 30.2 | Creating New Users | 124 |
| 30.3 | Connecting to RTSP | 125 |
| 30.4 | Supported videoformats | 125 |
| 31 | Backup, Restore and Documentation | 126 |
| 31.1 | Backup | 126 |
| 31.2 | Restore | 126 |
| 31.3 | Documentation | 127 |
| 32 | System Monitor | 128 |
| 32.1 | Performance Monitor | 128 |
| 32.1.1 | Creating a New Performance Counter Page | 128 |
| 32.1.2 | Performance Counter Interface Controls | 129 |
| 32.2 | System Status | 129 |
| 33 | Recommended Installation Order | 130 |
| ▪ | Cameras Installation, IP Addresses (page 21) | 130 |
| ▪ | ANPR USB Key and ANPR Engine Installation to the According Server (page 109) | 130 |
| ▪ | Servers Installation (page 10) | 130 |
| ▪ | Clients Installation (page 13) | 131 |
| ▪ | Connection (page 18) | 131 |

| | |
|---|------------|
| ▪ Creating Site (page 71)..... | 131 |
| ▪ Setting Storage Buffers (page 37)..... | 131 |
| ▪ Creating Storage Groups (page 39) | 131 |
| ▪ Adding Cameras (page 21), Registration (page 34) | 131 |
| ▪ Setting Intellio Cameras (Orio, Visus)..... | 131 |
| ▪ Setting ONVIF Cameras (page 57)..... | 132 |
| ▪ Setting Error Reporting (System Configuration/Site/Site page) (page 69) | 132 |
| ▪ Setting Alarm System (page 78)..... | 132 |
| ▪ Creating Roles / Users, and Setting (page 66) | 132 |
| ▪ Setting Internet Access (page 75) | 132 |
| ▪ Verifying..... | 132 |
| ▪ Backup, Documentation (page 124)..... | 132 |
| 34 Appendix..... | 133 |
| 34.1 Hexadecimal Conversion Chart..... | 133 |

1 Network Structure



Network architecture

The main requirement of a fully functional and reliable Intellio network camera system is a well-built Ethernet network. The architecture depends on the number of cameras, the number of servers and the number of client computers used.

The typical network bandwidth demand of an Intellio Camera is 4-32 Mbit/s, therefore you can connect up to 20 cameras to a 100Mbit/s link provided that there is no other communication on the network.

With more than 40 cameras connected to a server, it is practical to set up another server since this will enable the unique redundancy handling capabilities of the Intellio system, allowing continuous operation of all cameras in case one of the servers fail.

To provide for adequate power supply it is recommended either to power up each camera separately or to install a central power supply unit that can adequately power up all of the cameras. For proper working of the cameras a well-built power supply network is needed.

2 Installing the Software

The **Intellio Video System 4** software is designed to work under the most recent versions of the Windows Operating System (*meaning Windows 7 Professional and later versions*).

The system requires two programs: the **Intellio Server 4** and the **Intellio Client 4**. The Intellio Server keeps contact with the cameras, records the camera footage, and serves the clients. The Intellio Client is the visible interface of the system. Live monitoring, playback, event query and System Configuration is achieved through the client.

The software installation consists of two phases. First, the Intellio Server must be installed onto the server computer, then the Intellio Client program must be installed onto the client computer. For ease of configuration, it is advisable to install an Intellio Client onto the server computer as well.

2.1 Installation of Intellio Server 4

2.1.1 Steps of the Installation

Important: Before installing make sure that the time and time zone of Windows is set correctly (this has to be done on the server and client programs as well)!

Intellio Server is a Windows service which will run in the background after installing. Follow these steps to install:

- Put the installation disc into the DVD driver and check for any updates on the Intellio website.
- Run **Intellio Video System 4\IntellioServer4Setup.exe**.
- Select the language of the Install Wizard then click on **Next**.
- After accepting the License Agreement set the destination of the software (*recommended to leave it at default*).
- In case of a first install, select the type of installation.
- When selecting installation with a product key, input the product key.
- Select the components to be installed (*recommended option: **Full installation**; the Intellio Video System Gateway Server is used for mobile client playback and event browser features*).
- Start the installation.
- The server must be activated within 15 days after installation with the **Intellio Activation Tool**. If not activated, the server will shut down after 15 days and will only be operational after activation.
- The Intellio server after this is probably already installed. The computer may have to be restarted to this software to work properly.

If there are more than one server, install the **Intellio Server 4** to all of them one-by-one, then arrange them into a SITE according to the specifications described in the [Site](#) (page [71](#)) part of this installation guide.

2.1.2 Updating IVS

To update an already operating system, follow the recommended steps:

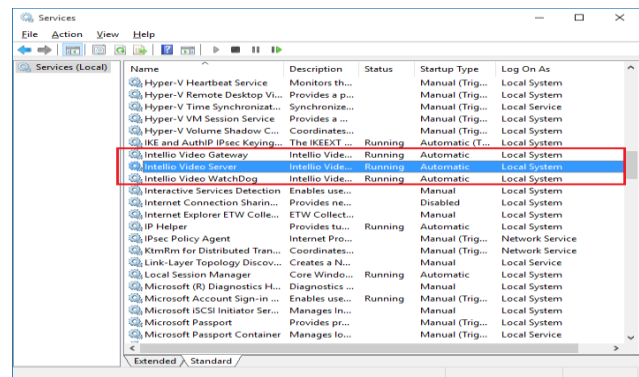
- Follow the instructions found in the chapter titled [Backup, Restore and Documentation](#) (page 124) to save your settings.
- Follow the instruction found in the chapter titled [Steps of the Installation](#) (page 10) to update the master server.
- Activate a new or updated product key (*IntellioActivationTool.exe*).
- Make sure that the updated server is operational by checking that the camera connections are restored, that storage is underway and that live view monitoring is operating.
- Individually update the slave servers.

When updating the Server make sure that each server of the SITE is of the same version.

2.1.3 Determine the Status of the Software

Since the Intellio server run in the background, the installation and the status of the server is expedient to verify. To do this, follow these steps:

- Go to **Start menu / Run...**, or press **Windows + R** keys.
- Type in **"services.msc"** then click on **OK**
- Search for the **Intellio** services (*Intellio Video Server, Intellio Video WatchDog, Intellio Video Gateway*).



Windows services, check for Intellio Video System 4

Intellio Video Server is basically the Intellio server itself. **Intellio Video WatchDog** is responsible to restart the server in case it is stopped. **Intellio Video Gateway** ensures mobile client playback.

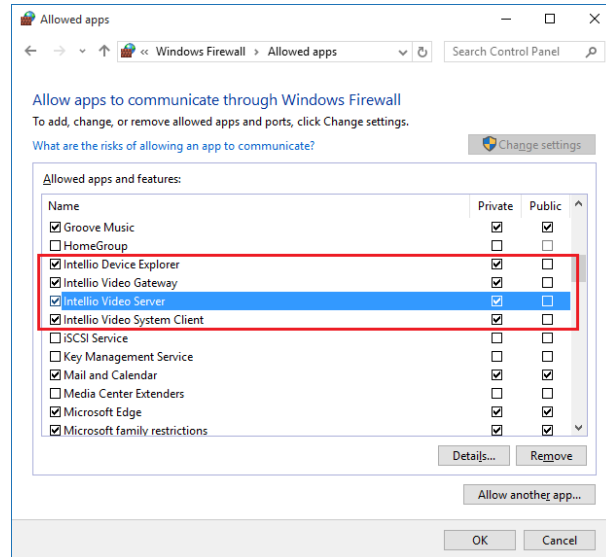
Note: If you were updated your already existing server to Intellio Server, the entry in the services will not change, and you may find it as **Intellio Video System Service**.

If the Status of both of them is **Started**, the system is running and is in working condition.

If Intellio Video Server does not start up, launch the **Intellio Activation Tool** program (... \Intellio Video System\Intellio Server\Intellio Activation Tool\IntellioActivationTool.exe) and check the status of the product key. If necessary, activate the product.

To be sure that Windows is not blocking the services, follow the steps below:

- Go to **Start menu / Run...**, or press **Windows + R** keys.
- Type in **"firewall.cpl"** then click on **OK**.
- Check the **Exceptions** to be sure that the **Intellio Video Server** are enabled.



2.2 Installation of Intellio Client 4

The Client can be installed by launching ***IntellioClient4Setup.exe*** in the ***IntellioClient*** folder. The installation steps are identical to those of the server installation. After starting up the client, you can log in to the Intellio Demo server or you can establish a connection to any other Site. This step is discussed further in the [System Setup](#) (page 18) chapter.

3 Client Settings

The ***Client Settings*** window can be accessed from the main menu. This is where all client settings can be made, which affect the quality of monitoring and the mode of display, but do not influence the internal operation of the system.

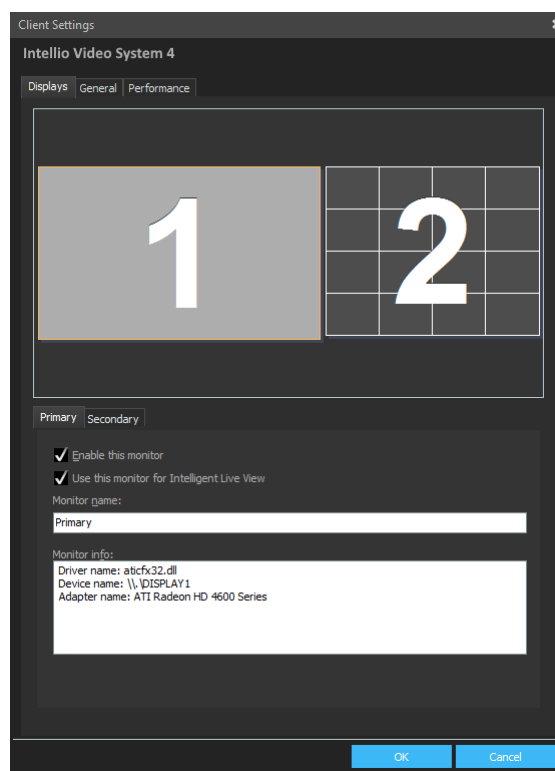
3.1 Displays

The settings related to the displays can be found on the ***Displays*** tab. The screens displayed signal the number of possible displays. The number of displays being used currently can be lower, but the first tab is always active and cannot be eliminated.

The display devices can be renamed, while the client displays the information regarding each display.

If ***Use this monitor for Intelligent Live View*** option is enabled, the selected monitor will be used for Intelligent Live View.

The layouts in the icons reflect the layouts of the displays.



3.2 General

The settings related to the display functions can be found on the **General** tab. In addition, the settings interface for the calibration of the joystick can also be accessed from here.

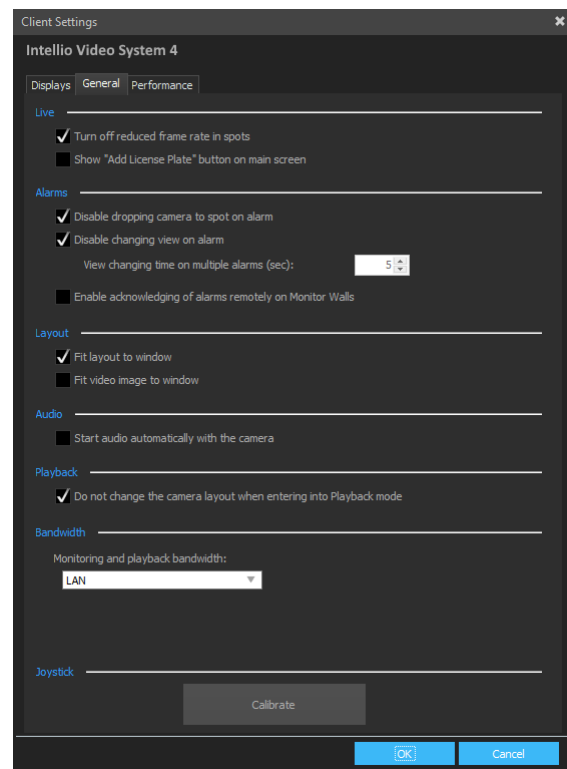
3.2.1 Live

Turn off reduced frame rate in spots

If this function is enabled, all settings resulting in an fps reduction in the video of the **Intellio** cameras displayed on the Spot panels will be temporarily suspended.

Show “Add License Plate” button on main screen

If this function is enabled, a button appears on the left bottom part of the live screen, which can be used to add a new license plate to the database.



3.2.2 Alarms

Disable dropping cameras to spot on alarm

This function disables camera images from being displayed on the Spot panels in case of alarms.

The Spot panel is a designated place, primarily to make it easily identifiable the alarm events, immediately showing the live image of the place where the alarm event occurred.

In the **Intellio Video System 4** the location of the Spot panel is freely changeable, the suggested places in the layout can be deactivated, and others activated. There is no limiting in any way.

To enable or disable a spot panel, move the mouse to the camera menu (*it will not work with an empty panel*), click on the monitor symbol, and choose the **Spot** option. To determine whether a camera is in a Spot panel or not, just check the upper right corner of the camera image. If there is a **Spot** designation there, then the function is active.

The priority of an alarm defines its appearance in the Spot panels. If a high priority and a low priority alarm arrive at the same time and there is only one Spot panel, only the high will be shown. If there is some time between them, the higher one will override the lower one, displaying it. The lower priority alarm will only show up, if there was no higher or equal priority alarm in the near past, and just until a higher priority alarm arrives to override it.

Disable changing view on alarm

The alarms triggered by detectors can be assigned a view change. Any view change previously assigned to an alarm can be disabled here (*e.g. in case of monitor walls*). Find more on the view change triggered by alarms in the [General Description of a Detector](#) (page 88) chapter.

View changing time on multiple alarms

In case there are multiple concurrent alarms, the client program will keep switching between the views affected. Here you can set the time interval between view switches.

Enable acknowledging of alarms remotely on Monitor Walls

By enabling this option when acknowledging the alarms, they will also be acknowledged on the connected Monitor Wall clients.

3.2.3 Layout

Fit layout to window

This function enables the dynamic resizing of panels and adjusting them to the proportions of the screen.

Fit video image to window

It fills the panel completely with the images transmitted by the camera. Consequently, it may result in the distortion of the image proportions.

3.2.4 Audio

Start audio automatically with the camera

This function enables automatically selecting an audio input assigned to a camera when that camera is selected in live video or playback. In other words, the audio assigned to the camera will start when the camera is in live video mode. In playback, the audio input track will appear on the timeline, with the audio starting when playback starts. If this option is disabled, the audio input needs to be selected manually.

3.2.5 Playback

Do not change the camera layout when entering into Playback mode

Select this to have all cameras from the live video displayed in playback mode. When left unselected, the camera displayed is the camera of the active panel, or - *if unavailable* – that of the Spot panel. In the lack of either of these, the first camera of the layout will be displayed.

3.2.6 Bandwidth

Depending on the available bandwidth a limit can be set for the client, a value to be adhered to by the images transmitted for surveillance or playback through the automatic decreasing of the refresh rate or increasing of the compression rate. These settings are recommended to be changed on clients where monitoring and/or playback is done online or through private networks with a low bandwidth. This way, monitoring or playback of multiple cameras simultaneously will be uninterrupted. Restricting the bandwidth also automatically disables the **Views** and **Layouts**, whose usage are not viable with low bandwidths.

The bandwidth of the connection between server and client can be selected from a dropdown list. The client tries to keep the bandwidth below the selected value in live monitoring and playback mode. During playback, this applies to the bandwidth of sending images for the client.

3.2.7 Joystick

Calibrate

Opens the settings interface to calibrate the joystick connected to the client.

3.3 Performance

3.3.1 Global

Custom Two-Channel Monitoring

Concurrently, two video channels can be handled by the system, which allows for a secondary monitoring channel, only queried from the camera by the server when necessary for the optimal display of the camera images. This offers the benefit of lowering the demand on the client when compressing images with low resolution transmitted through the secondary channel, allowing for the display of multiple cameras at the same time, while the resolution and the quality of the images stored remain unchanged.

There are various factors governing which video stream to display on the live video. A secondary channel is created if:

- Monitoring takes place on one monitor with more than 6 panels on it.
- Monitoring takes place on two or more monitors with more than 4 panels on the display.
- The IntelliZoom function is not active.
- The DPTZ function is not active.
- The Magnifier function is not active.
- It is not a Spot monitor.

If any one of the conditions above are unfulfilled, the image displayed is transmitted via the primary image stream in high resolution.

Optimize to performance

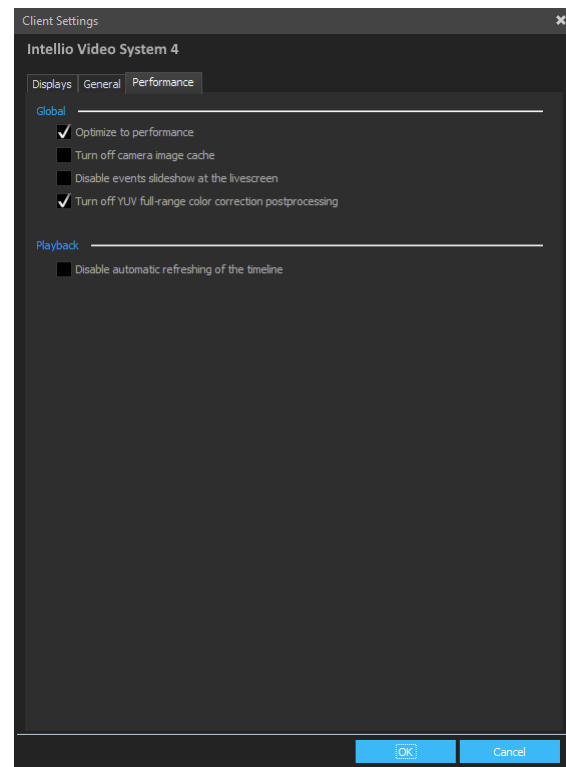
If this function is switched on, all the camera images which are not on the Spot panel will be transmitted through the secondary video channel, disregarding the other conditions required for secondary video channels. Thus, the live video displayed will display the images of the secondary video channel, except for the cameras on the Spot panel.

Turn off camera image cache

If this function is enabled, the images from cameras used at least once will not be remembered, resulting in a slightly slower views switch and smaller memory usage.

Disable events slideshow at the livescreen

This function disables the event images in the **Events** dropdown menu, resulting in smaller memory usage.



Turn off YUV full-range color correction postprocessing

This function disables the post processing of images, resulting in lower processor usage.

3.3.2 Playback

Disable automatic refreshing of the timeline

This function disables the automatic refreshing of the timelines on the playback interface.

4 System Setup

The system must be configured using the Client program. This consists of creating a connection to a Site, creating the video buffer and registering the cameras, setting the video adjustments, motion detectors, storage rules, etc.

4.1 Logging in to a Site

Starting the client program the **Login** window will automatically appear. Alternatively this window can be opened by clicking the **Connect** button in the client toolbar. To create a new connection:

- In the **Login** window click on the **...** button.
- In the **Select connection** window click on the **Add** button.
- In the **Connection Name** field type a name that will clearly identify the connection. In the **Connection addresses** list add a server using its name or IP Address (*default TCP port: 53540*).
- Confirm the validity of the data and make sure that each required field is filled in.
- Press **OK**.
- Select the previously created connection in the **Select connection** window.
- Type in the user name and password for the Site.

| | |
|--------------------------|---------------------------------|
| Default Username: | Administrator / Operator |
| Default Password: | admin / op |

Important: Remember to change the default password, keeping the default password constitutes to a great security threat!

When adding or editing a connection, it is possible to give the username and password and these data will be saved. In case of this kind of connection the system will ask just for the missing data during connection.

Note: be aware that saving username and password may impose a serious security threat, so use it only with limited user roles.

If the client will connect to a SITE and not a single server, it is advisable to enter all the addresses of the servers in the SITE. This can be done in the **Connection addresses** list, adding every single server one after the other. This step also necessary to create a connection to a single server, but if there are multiple servers in the SITE, check in the checkbox called **Automatically synchronize addresses**. This ensures the clients will be distributed evenly among the servers of the SITE, preventing the uneven network load.

In case there could be more than one client logged in the SITE, take it in consideration that any changes in the SITE can be detected only by refresh from any other client.

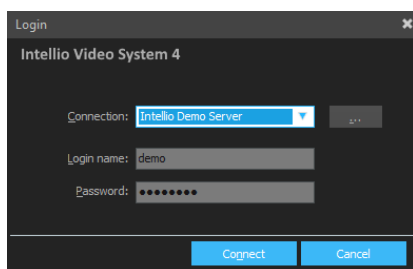
If the client will be connected to a Domain, check in another checkbox too, called **Connect to all sites**. This means, the client will connect to all SITES which are part of the same Domain.

In addition, the **Monitoring and playback bandwidth** of the connection can be adjusted, meaning the default bandwidth assigned by the Client to the particular connection. On a local network it is usually advisable to leave the LAN selected, while in case of an internet connection it is best to set it closer to the upload speed of the server.

By enabling **Acknowledge remote alarms** option, when the user acknowledges the alarms, they will be acknowledged on the connected monitor wall clients also.

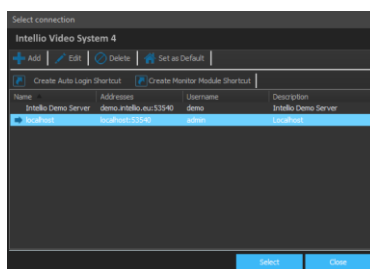
After pressing **OK** the connection should be established, which allows to connect to a SITE (*there can be more than one*). Select it and press the **Select** button. In the **Login** window press the **Connect** button.

Login



The Login window for Intellio Video System 4. It features a 'Connection' dropdown menu with 'Intello Demo Server' selected, a 'Login name' field with 'demo', and a 'Password' field with masked characters. At the bottom are 'Connect' and 'Cancel' buttons.

Login window

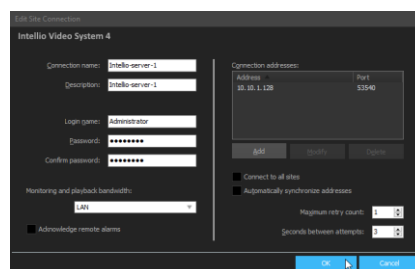


The Select connection window for Intellio Video System 4. It shows a table of available connections. The first connection is selected.

| Name | Address | Username | Description |
|---------------------|------------------------|----------|---------------------|
| Intello Demo Server | demo.intellio.eu:53540 | demo | Intello Demo Server |
| Intello Demo Server | 192.168.1.123:53540 | demo | Intello Demo Server |

Buttons at the bottom: 'Select' and 'Close'.

Select connection window



The Add Site Connection window for Intellio Video System 4. It contains fields for 'Connection name' (Intello-server-1), 'Description' (Intello-server-1), 'Login name' (Administrator), 'Password', and 'Confirm password'. It also has checkboxes for 'Connect to all sites' and 'Automatically synchronize addresses'. A 'Monitoring and playback bandwidth' dropdown is set to 'LAN'. At the bottom are 'OK' and 'Cancel' buttons.

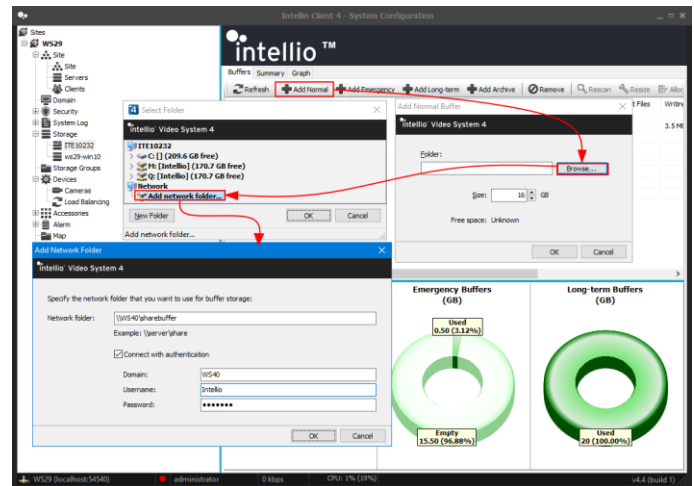
Add Site Connection window

After selecting a connection item, you can press the **Create Auto Login Shortcut** button to create a shortcut icon on Windows Desktop, which can be used to start the Intellio Client application and login to the Site by using the credentials of the connection item.

4.2 Creating a Video Buffer

Space must be reserved on the hard drives for the stored footage. For this purpose the system allocates some hard disc space on the server's storage, which is the so-called video buffer. The allocated buffer space is **at least 16GB**. Normal buffers can be created on local drives and in network folders.

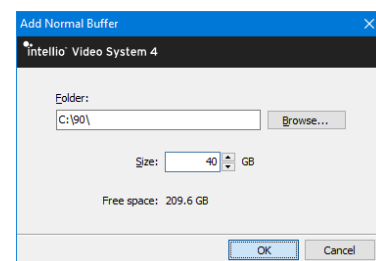
When connecting for the first time, if the server does not have a buffer, it will offer to create one. Creating a buffer is not mandatory, you can postpone this process by closing the window, but recording will not work until at least one **Normal buffer** is given. To create a buffer, click **Browse**, and in the window that appears, select the folder where you want to put the buffer. Previously attached network folders can be found under the **Network** node, and by using **Add network folder...** you can add a new one. After a folder has been selected, give the size of the buffer (*the system will offer a value, depending on the available free capacity, if necessary you can change this according to your needs*). By clicking **OK** the system will allocate the buffer immediately.



Creating network folders

Important: If you are storing data on a NAS, it is strongly recommended to create an **Emergency buffer** on every server to keep the data storage uninterrupted even in cases when the network folder becomes unavailable!

The system can be extended by buffers at any time. To create a new video buffer, go to **System Configuration / Storage**. Select the server where the video buffer will be created. Press the **Add buffer** button. Set the space on the server's hard drive, and then specify the size (*several buffers on different hard disk partitions can be created*). After pressing **OK** the system automatically starts allocating the space of the video buffer on the servers' HDD.



Adding a buffer

Note that the system will not create directories with bigger than 1000 GB sizes. In this case, the system will automatically separate the buffer files in two or more subdirectories in order the search within these files to be faster. Of course, these directories can be resized, but doing so the speed of the software will decrease.

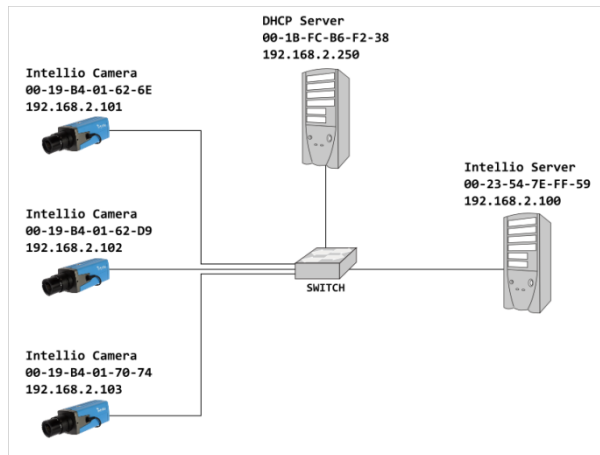
A buffer can be removed by clicking on **Remove**, the only limitation is that at least one buffer (*this can be an emergency buffer*) must exist.

Important: Never create a buffer in the root folder of a drive!

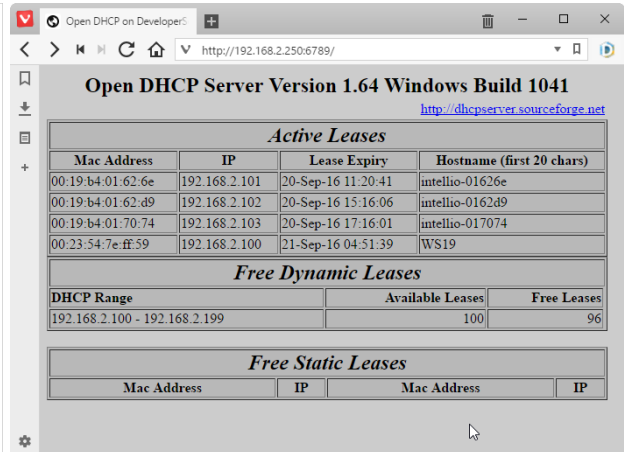
4.3 Adding Cameras/Encoders to Intellio Video System 4

To monitor / record the cameras' images first the cameras / encoders has to be discovered over the network. Each individual camera / encoder has its own physical address which is always unique of all network devices. This Address is called MAC address which is a 6 byte hexadecimal number like: *00-19-B4-01-62-6E*. Next to MAC address all network devices must have IP address to communicate over the network with other network devices. All of the network cameras' IP address has to be discovered before registering them to an Intellio server.

4.3.1 Discovering Network Cameras with Scanning



Scanning for cameras, DHCP server is present on the network



The screenshot shows the 'Open DHCP Server Version 1.64 Windows Build 1041' web interface. The 'Active Leases' section displays a table with columns: Mac Address, IP, Lease Expiry, and Hostname (first 20 chars). Below this, the 'Free Dynamic Leases' section shows a table with columns: DHCP Range, Available Leases, and Free Leases. The 'Free Static Leases' section is also visible but empty.

| Mac Address | IP | Lease Expiry | Hostname (first 20 chars) |
|-------------------|---------------|--------------------|---------------------------|
| 00:19:b4:01:62:6e | 192.168.2.101 | 20-Sep-16 11:20:41 | intellio-01626e |
| 00:19:b4:01:62:d9 | 192.168.2.102 | 20-Sep-16 15:16:06 | intellio-0162d9 |
| 00:19:b4:01:70:74 | 192.168.2.103 | 20-Sep-16 17:16:01 | intellio-017074 |
| 00:23:54:7e:ff:59 | 192.168.2.100 | 21-Sep-16 04:51:39 | WS19 |

| DHCP Range | Available Leases | Free Leases |
|-------------------------------|------------------|-------------|
| 192.168.2.100 - 192.168.2.199 | 100 | 96 |

Active DHCP leases

By default, Intellio cameras accept IP addresses got from a DHCP server.

In the example below there is an Intellio server (*WS19*) and three Intellio cameras connected to a broadband router. DHCP servers usually list the devices which are connected to them and have an IP assigned by the DHCP.

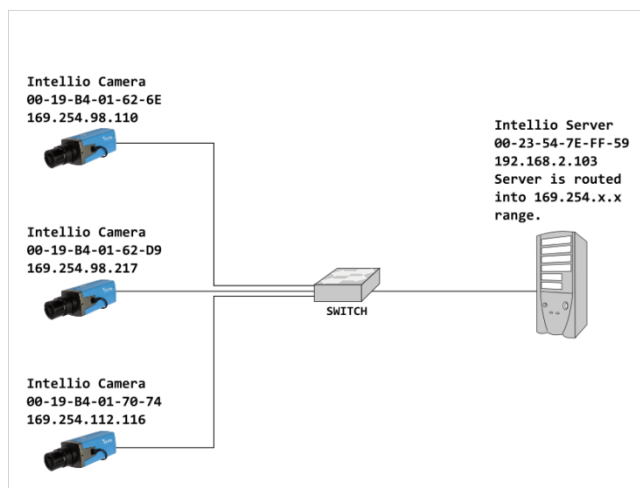
In this situation follow the steps below in order finding the cameras:

- Go to **System Configuration / Devices**.
- Click button **Scan** (or to filter out the unrequired cameras, on the arrow next to Scan, then the **Search ... devices**).
- Select the cameras you want to add to the server.
- Some cameras (for example **Intellio Initio**) requires a user name and password before registering. Type in the user name and password under the **Connection** tab of the device then press **Refresh**.

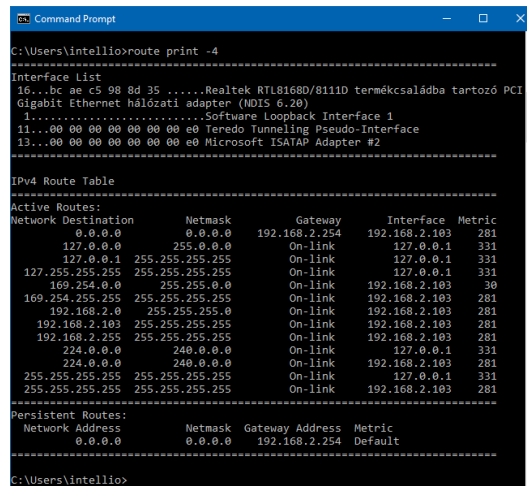
Sometimes the first attempt is unsuccessful so be sure to press **Scan** a few times. It is time consuming, but this is the easiest way to find a lot of devices. If the cameras still do not show up make sure that a firewall is not blocking the multicast protocol. If scan has no result, see [Adding New Cameras/Devices Manually](#) (page 22) for manually adding cameras.

There may be situations when there is no DHCP server on the network so the cameras do not get IP addresses automatically. In this case the cameras will get their default IP based on their MAC address (*Serial Number*): **169.254.(MAC 2. byte in decimal value).(MAC 1. byte in decimal value)**. Example: MAC address is **00-19-B4-00-42-1A** – IP address is **169.254.66.26**

The appendix at the end of this document will assist you with [Hexadecimal Conversion Chart](#) (page 133).



Scanning for cameras, DHCP server is not present on the network



```

C:\Users\Intellio>route print -4

Interface List
16...bc ae c5 98 8d 35 .....Realtek RTL8168D/8111D termékszálladba tartozó PCI
Gigabit Ethernet hálózati adapter (NDIS 6.20)
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Terezo Tunneling Pseudo-Interface
13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2

IPv4 Route Table

Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.2.254    192.168.2.103    281
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
169.254.0.0                255.255.0.0      On-link          192.168.2.103    30
169.254.255.255            255.255.255.255  On-link          192.168.2.103    281
192.168.2.0                255.255.255.0    On-link          192.168.2.103    281
192.168.2.103              255.255.255.255  On-link          192.168.2.103    281
192.168.2.255              255.255.255.255  On-link          192.168.2.103    281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.2.103    281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.2.103    281

Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
0.0.0.0                0.0.0.0          192.168.2.254    Default
  
```

Routes on the server

Go to **System Configuration / Devices** and use **Scan** button (or **Scan / Search ... devices**), to find the cameras on the network: The server automatically routes into the link local range when it is installed. This should ensure that camera discovery is successful.

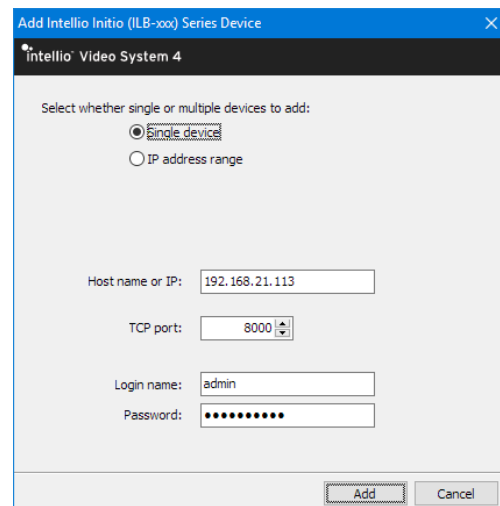
4.3.2 Adding New Cameras/Devices Manually

When **Scan** is not working.

Adding Intellio Initio Cameras

Follow these steps:

- Select **Add Intellio Initio (ILB-xxx) Series Device...**
- Enter the IP address manually into the **Host name** or **IP** field and enter the **Login name** and **Password** of the device.



Add Intellio Initio (ILB-xxx) Series Device

Intellio Video System 4

Select whether single or multiple devices to add:

☒ Single device

☐ IP address range

Host name or IP: 192.168.21.113

TCP port: 8000

Login name: admin

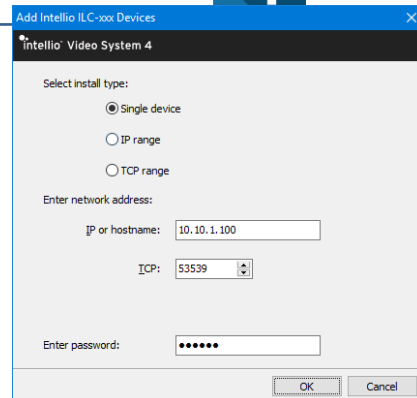
Password:

Add Cancel

Adding Intellio ILC Cameras

To add a device, follow these steps:

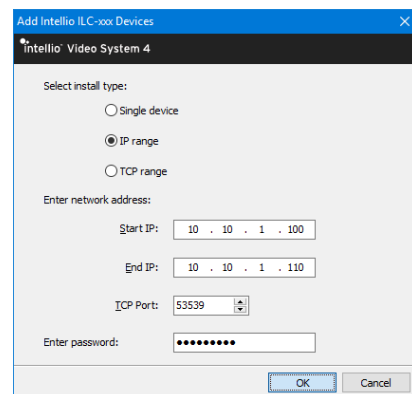
- Click on **Add / Add Legacy Device / Add Intellio ILC-xxx Series...** button.
 - Select radio button **Single device**.
 - Enter the **IP or hostname** of the camera.
- Click **OK** button.



Adding an ILC camera

The ILC cameras can be added to the SITE in a group. To do this, the steps to be followed are:

- Click on **Add / Add Legacy Device / Add Intellio ILC-xxx Series...** button.
- Select radio button **IP range**.
- Enter the **Start IP** and the **End IP** of the selected range of the cameras.
- Click **OK** button.



Adding multiple ILC cameras with IP range

Adding Intellio ILD Cameras

When ILD devices are manually added to the server, the cameras will get their default IP based on their MAC address (*Serial Number*): **169.254.(MAC 2nd byte in decimal value).(MAC 1st byte in decimal value)**

Note: the 6th, 5th and 4th byte of the ILD cameras' MAC address must start with: **00-19-B4**. If this is not true, the camera is not an authentic Intellio ILD device.

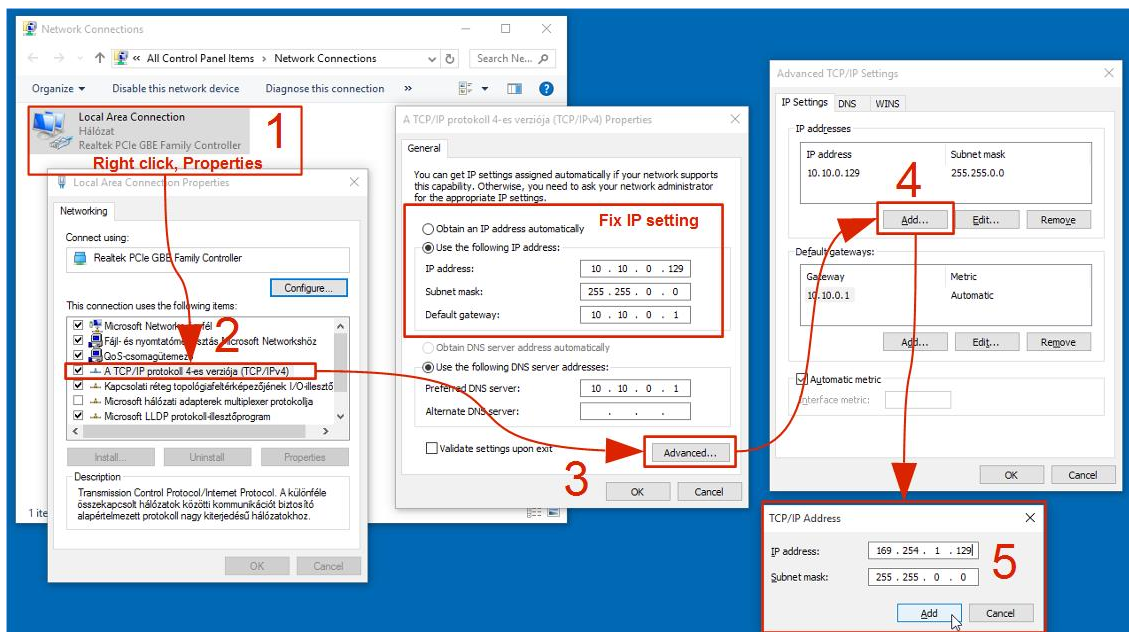
Example: MAC address is **00-19-B4-00-42-1A** – IP address is **169.254.66.26**

The appendix at the end of this document will assist you with [Hexadecimal Conversion Chart](#) (page [133](#)).

For ease of use, the MAC address of the camera can be entered instead of the IP address.

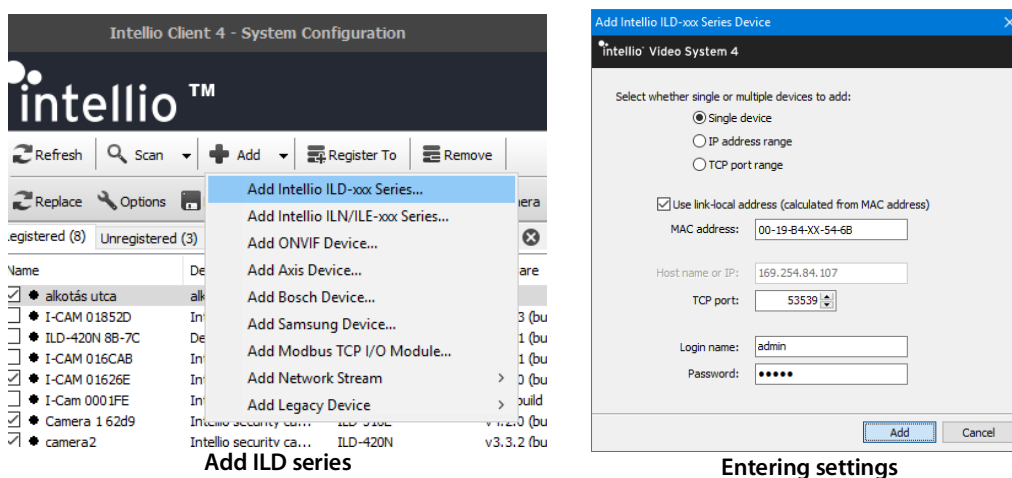
Before adding ILD cameras into the server, a link-local address must be set to the server PC. To do this, follow these steps:

- Select **Start menu / Run...** menu (**Windows + R** keys).
- Type in the **"ncpa.cpl"** command, then click on **OK**.

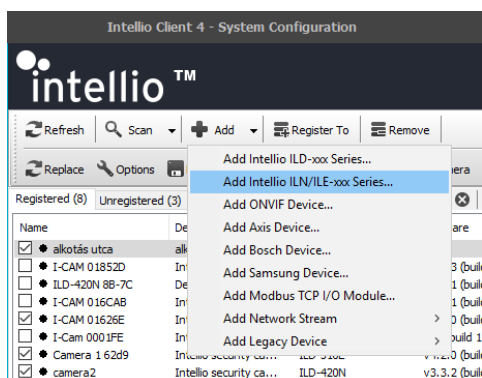


- Click on the icon of the connection in use with the right mouse button, and select the **Properties** menu item.
- Go to **Internet Protocol Version 4 (TCP / IPv4) / Properties** window and select the **Use the following IP address:** radio button. Set the following:
IP address: **169.254.x.x**
Subnet mask: **255.255.0.0**
Default gateway: **x.x.x.x**
- If there is already an IP address set here, click on **Advanced...** button then **Add...** Type the above listed settings here.
- After these settings are set use **Scan** or **Scan / Scan ILD devices** to find cameras on the network.

Alternatively, use **Add... / Add ILD-xxx Series...** to add cameras manually.



Adding Intellio ILN Cameras



Add ILN series camera menu



Configure ILN series camera

The ILN series has to be added manually to the system in the Intellio Client interface.

- Go to **System Configuration / Devices / Add / Intellio ILN/ILE-xxx Series...**
- In the popup window enter the IP address of the camera: **Host: 192.0.0.64**. (The port number can be added after a colon. For example: **192.0.0.64:8000**)

The ILN series has a built in web server so it is possible to connect to it and configure it by using a web browser:

IP address by default: **192.0.0.64**

User name: **admin**

Password: **12345**

Port: **8000**

Note: If there is an error message like: Login failed, try to stop the Intellio Video System Service and restart your web browser. After finishing the setup you can start the Intellio Video System Service.

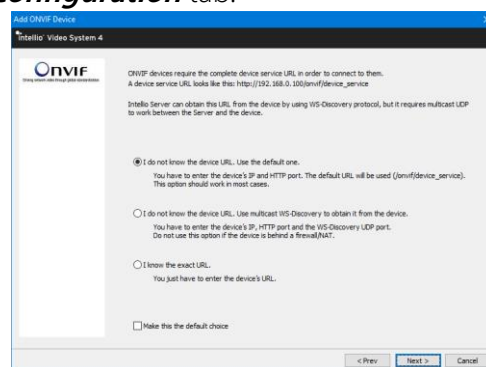
It is recommended to change the IP address because the next connected cameras' IP address will be the same (**192.0.0.64**). To this do the following:

- Click on the **Configure** button than select **Server configuration** tab.
- Enter the new IP address than click on **Save** than **Reboot** button.

Adding ONVIF Devices

Adding an ONVIF device to the system starts with these steps:

- **System Configuration / Devices / Add** button.
- Select **Add ONVIF Device...**
- From the pop-up window select the first option (**I do not know the device URL. Use the default one.**), then click **Next**.
- Enter the IP address manually into the **Host name** or **IP** field and enter the **Login name** and **Password** of the device.



Add ONVIF device

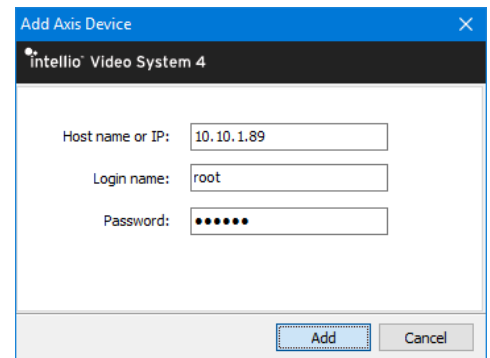
- **RTSP transport mode:** Determines the channel which is used to send video or audio. **RTP over RTSP** is selected by default; this is a reliable TCP connection. In some cases it can happen that the camera does not transmit images, this may be due to the lack of support for the default mode. In these cases use **RTP over UDP**, but please be aware that in this case the camera cannot be behind a firewall or a NAT. If the camera is behind a firewall or a NAT, use the **RTP over RTSP** option. The **RTP and RTSP over HTTP** setting is recommended if the camera is behind a firewall or a NAT and only the HTTP connection is permitted through the firewall.
- Leave the other option at default.

Note: There are cameras, where the default selection is not working. Its cause can be that the device service is not on the default route. If this route is unknown, use the second option (**I do not know the device URL. Use multicast WS-Discovery to obtain it from the device.**), or in case this route is known, the third option (**I know the exact URL.**). If the third option has been used, the URL has to be typed in.

Adding Axis and Bosch Devices

To add Axis or Bosch devices to the system, follow these steps:

- Click **System Configuration / Devices / Add** button, and select **Add Bosch Device...** or **Add Axis Device...**
- Enter the IP address manually into the **Host** field and enter the **Login name** and **Password** of the device.



Note: It is advised to use this connection type if the selected Axis or Bosch cameras do not support the ONVIF protocol.

Adding Samsung Devices

To add Samsung device, follow these steps:

- Click **System Configuration / Devices / Add** button, and select **Add Samsung Device...**
- Type the appropriate data into the **Host** or **IP**, **Communication port**, **Login name** and **Password** fields.
- If necessary the **Use explicit RTSP port** option can be used to change the value of default RTSP port.
- **Use RTP over RTSP:** Determines the channel which is used to send video or audio. It is unchecked by default which means the UDP connection, but please be aware that in this case the camera cannot be behind a firewall or a NAT. Enable this option to use the reliable TCP connection.

Note: It is advised to use this connection type if the selected Samsung cameras do not support the ONVIF protocol.

Adding Modbus TCP I/O Devices

By using Modbus TCP protocol it is possible to connect digital I/O devices (*e.g. Moxa E12xx*) to the IVS. In case of proper settings the IVS is able to receive the input signals of the connected devices, and control their outputs. As this protocol use TCP connection, the connected devices use the IVS [Camera Takeover](#) (page 70) feature automatically, thus ensuring high availability of controls.

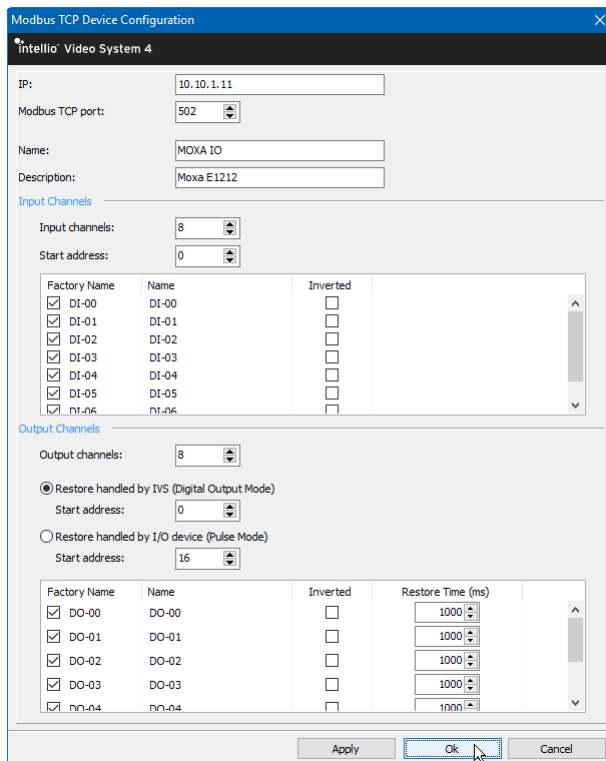
To add Modbus TCP device, follow these steps:

- Click **System Configuration / Devices / Add** button, and select **Add Modbus TCP I/O Module...**
- In the appearing wizard window type the **IP** address of the device, and press **Next** button.
- The server connects to the Modbus TCP device. In case of Moxa devices (*if the Restful API is enabled in the device*), the server is able to acquire the defaults settings, which are displayed in the next wizard window. In case of any other Modbus TCP device the default number of inputs and outputs are eight.
- After setting the parameters correctly (see [Setting Modbus TCP device](#) (page 28)), use the **Finish** button to add the device to the system.

Note: do not forget to register (page 34) the newly added device to one server of the SITE.

Setting Modbus TCP device

To set a Modbus TCP device click **Configure...** button on the **System Configuration / Devices / selected_device / I/O ports** page, and in the appearing window make the necessary changes.



The image shows the 'Modbus TCP Device Configuration' window for 'Intellio Video System 4'. It contains fields for IP (10.10.1.11), Modbus TCP port (502), Name (MOXA IO), and Description (Moxa E1212). Below these are sections for 'Input Channels' and 'Output Channels'. The 'Input Channels' section has a table with columns 'Factory Name', 'Name', and 'Inverted', listing DI-00 to DI-06. The 'Output Channels' section has a table with columns 'Factory Name', 'Name', 'Inverted', and 'Restore Time (ms)', listing DO-00 to DO-04. At the bottom are 'Apply', 'Ok', and 'Cancel' buttons.

- Type the IP address into the **IP** field.
- The standard Modbus TCP port is **502**. If necessary it can be changed in the **Modbus TCP port** field.
- Type the identification data into the **Name**, and **Description** fields.

Input channels:

- Enter the number of **Input channels** provided by device (0-128). The list of inputs is changed automatically according to the given number.
- Enter the **Start address** from which the inputs can be accessed on the device.

Note: the start address is depending on the device, so for the exact value use the installer manual of the device.

- The individual settings of the inputs can be found in the list. The state (enabled/disabled), the name, and the behavior (inverted/normal) can be changed per input. The IVS ignore the signals of the disabled inputs.

Output channels:

- Enter the number of **Output channels** provided by device (0-128). The list of inputs is changed automatically according to the given number.

The IVS supports two ways of restoring the outputs:

- **Restore handled by IVS (Digital Output Mode):** with this option the restoring of outputs is managed by IVS. In this case you must set the restore time (*in milliseconds*), and the inverted behavior also can be set per output.
- **Restore handled by I/O device (Pulse Mode):** in this mode the outputs are managed by device, and the IVS only activate the outputs. The parameters of the output (*timing, inverted behavior etc.*) must be set on the device own settings interface.

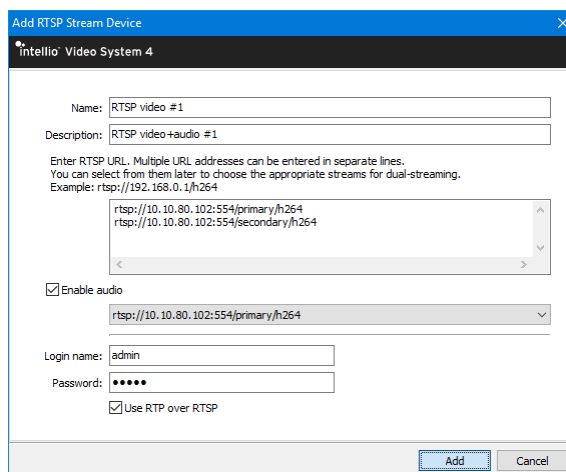
Note: Some device use different start addresses to access outputs depending in the operation mode (for the exact value use the installer manual of the device). Type the proper start address in the **Start address** field according to the selected mode.

The individual settings of the outputs can be found in the list. The state (*enabled/disabled*), the name can be changed per input. The IVS do not control the disabled outputs.

Use the [Multi IO Input Detector](#) (page [105](#)) to receive the input signals of a Modbus TCP device, and the [Multi IO Action](#) (page [82](#)) to control the outputs of Modbus TCP device.

Adding an RTSP and Other Videostream

RTSP or MJPEG streaming allows for monitoring the images of each camera which has a known RTSP or MJPEG URL. Monitoring options through these datastreams are very limited (*in contrast to ONVIF, there is no on-board motion detection or PTZ control mode, and the network URL also has to be known to install the device*), which is, therefore, only recommended in case the camera cannot be connected to the system in any other ways.



The Intellio system is capable of handling Dual-Stream, i.e. it can use different video compression values for storage and monitoring.

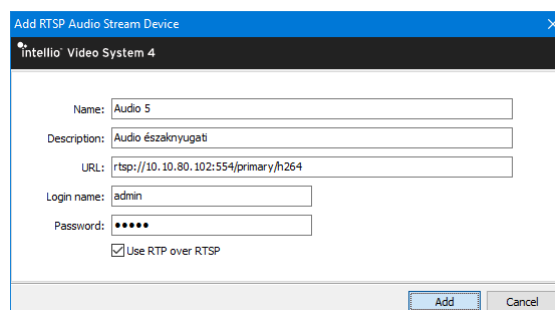
The RTSP-stream also supports handling audio besides the video, the settings of which can be adjusted.

Here's how to add a datastream:

- Press the **System settings / Devices / Add** button, then click **Add network stream** and **Add RTSP-stream** or **Add MJPEG over HTTP Stream**.
- Assign a name and a description to the video stream, then the RTSP or MJPEG URLs belonging to the stream. The more URLs you assign, the more settings options you will have when assigning monitoring and storage settings (*the URLs belonging to the device can be queried from the manufacturer or, in case of tested camera types, found in Intellio's database of supported cameras*).
- If necessary, assign a user name and password to the camera.
- Select the required audio channel and provide the URL to be used by the server with the audio channel. The audio will always be streamed from this URL, so in case of Dual-Stream it is recommended to provide the URL to be used for storing video.
- **Using RTP over RTSP:** Determines whether image or audio is transmitted via the TCP or UDP channel. It is turned on by default, meaning the more reliable TCP connection. Only turn off in case the camera fails to transmit images, since it may be due to a lack of support for this transmission mode.

Adding an RTSP Audio Device

You can add an audio-only RTSP stream, as well (*with no video*) by clicking the **Add Network Stream** menu and selecting the **Add RTSP Audio Stream** item in the menu.



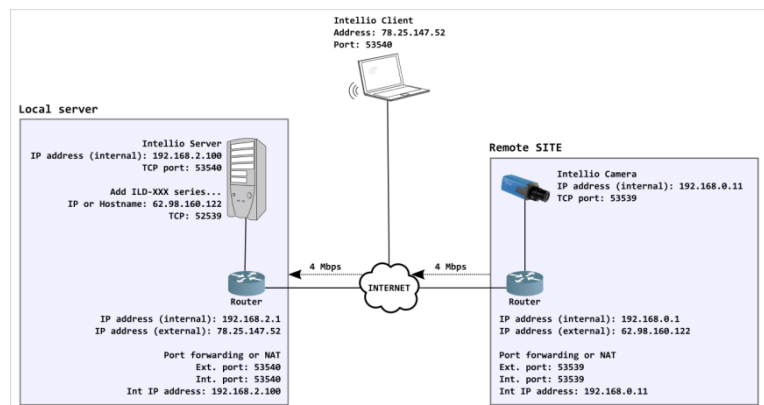
The settings can be adjusted in the same way as with the RTSP-videostream, but in this case you only need to provide an URL only for the audio stream.

4.3.3 Adding Camera with External IP Address

How to Register Intellio Camera into a Remote Intellio Server over the Internet?

This figure below demonstrates that an Intellio camera in a remote SITE is connected to one local server over the internet.

Please note that an ILD camera consumes between 4-32Mbps network bandwidth for transmitting images with the maximum frame rate and highest quality. The ILD cameras are requiring a higher bandwidth for optimal performance, up to 10Mbps.



Camera connected through internet

In case the camera is connected to an Intellio server over the internet the recommended **upload** bandwidth is around 4Mbps per camera. If the upload speed is less than the recommended value than the camera will automatically decrease the frame rate to be sent for the server.

Note: Certain frame rate drop or low image quality is not bad functionality of the Intellio cameras but could be caused by the low bandwidth between cameras and server.

Assign a Fix Internal (*local*) IP Address to the Camera

In the Remote SITE where the camera will be installed a fix internal IP address have to be assigned for the Intellio camera. It is very important that the camera and the router have to be in the same IP range. In most of the cases the local IT can help you in this.

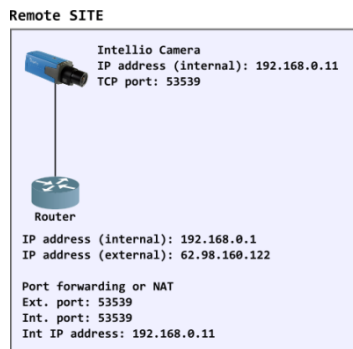
In our example the fix internal IP address of the camera is **192.168.0.11** (*mask: 255.255.255.0*). The router has the **192.168.0.1** internal IP address (*mask: 255.255.255.0*) which means the router and the camera can see each other. If you try to ping the camera on its address you must get answer.

You can ping a network device from a console window the following way:

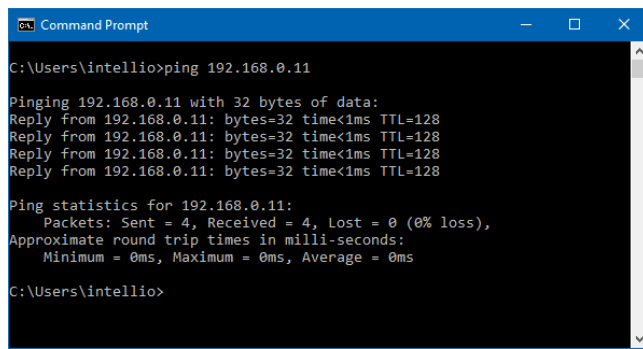
- Go to **Start** menu and click **Run...** button.
- Type in **"cmd"** and press **Enter**.
- Type **"ping xxx.xxx.xxx.xxx"** (*ping camera IP*) in the console and press **Enter**.

If you can see the replies there is connection with the network device.

Note: The fix IP address of the camera can be set before the installation in your office.



Assign a fix IP address to the camera

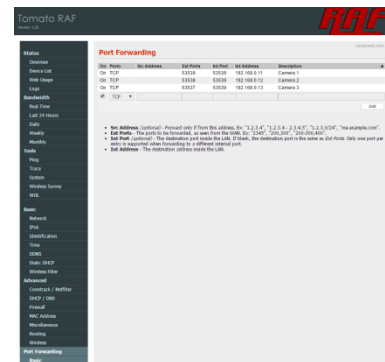


Ping the camera

Setup the Port Forwarding or NAT in the Router

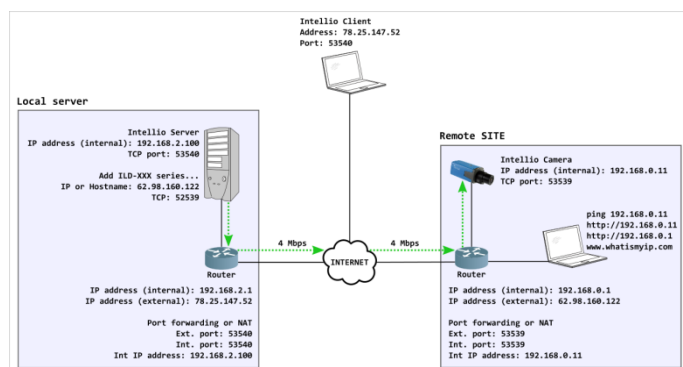
The main goal is to establish a connection from the Local server to the Intellio camera in the remote SITE. But in practice there are several different networks between them so we have to set our network devices correctly to be able to connect to the camera.

We can easily get what the external address of the Remote SITE is. This address clearly identifies the Remote SITE where the camera is installed. The easiest way to get this address by opening a web browser on the server PC and type the <https://www.google.com/search?q=ip&hl=en> URL.



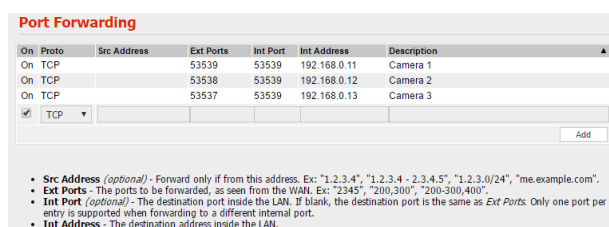
Port forwarding rules in the router

The external address is not enough to find the camera in the network because behind the router there are several other network devices which have different internal IP addresses. It has to be defined in the router that we are looking for our camera in the internal network (*LAN*) which has a fix IP address. In case the external IP address is dynamic (*changing all the time*), DNS can be used which will be translated to the current IP address.



Camera connected through its external address

At this phase the TCP Port of the camera will be used which will identify the camera in the internal network or LAN (*Local Area Network*) if the router is set up this way. The router has to be told that the request from the server is looking for a network device which has the **53539** TCP Port and **192.168.0.11** IP address.

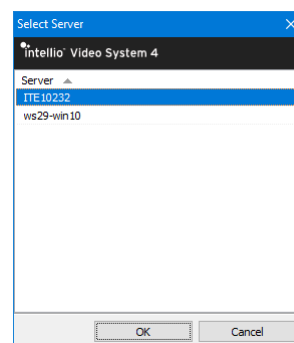


Setup port forwarding rules

This information can be set in the web interface of the router. In the example below the router has been set to send the request to the internal address and port of the camera. The External Port is a request *(to make setup easier the same port as the internal port of the camera had been set)*.

The connection request which is sent from the server to the router will be **62.98.160.122:53539** (*External address of the SITE and External Port*) which will be forwarded to the **192.168.0.11:53539** network device; so to the camera.

In case of several cameras the port forwarding has to be done in the same way just set a different External port number of the request. This means the **62.98.160.122:53538** request will be forwarded to the **192.168.0.12:53539** camera. The **62.98.160.122:53537** request will be forwarded to the **192.168.0.13:53539** camera.

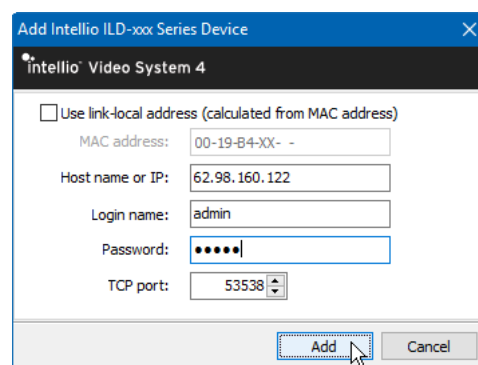


Selecting the server

Adding the Camera to the Server

In this phase every necessary setting is done so it can be tried to add the camera to the server. It can be done by connecting with the Intellio client to the local server. Go to ***System Configuration / Devices***, click on ***Add*** drop down button, and select ***Add Intellio... Series***

After this the camera will show up in the ***Unregistered*** tab. Clicking on the ***Refresh*** button the camera's information will appear on the list.

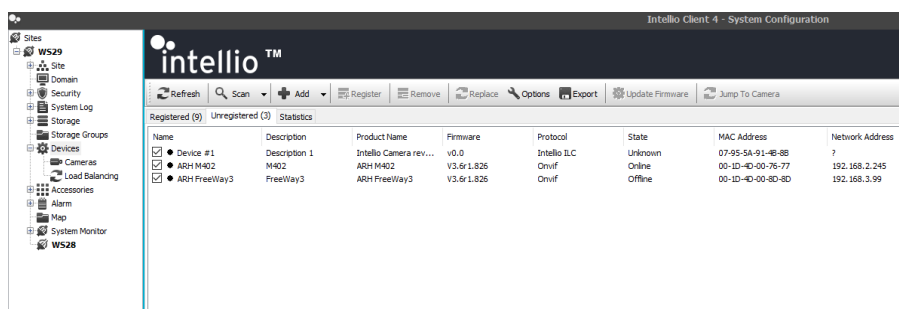


Add devices (ILD)

4.4 Registering Cameras and Devices

Each device must be registered to a SITE and be assigned to a primary server. The primary server will be the one storing the footage of the corresponding cameras.

Although the Client can find cameras on the network, there are instances when this option is not working, or this option is not supported for the selected device.



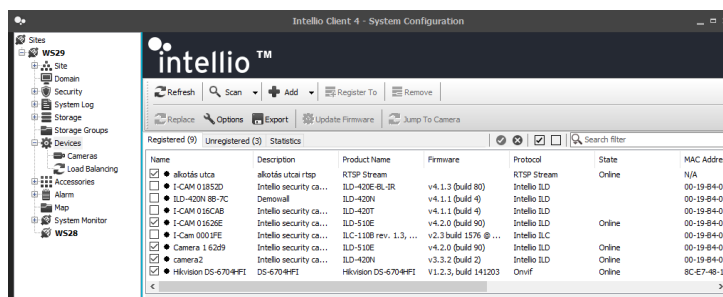
Unregistered cameras

To register, follow the instructions below:

- Go to ***System Configuration / Devices***
- Press the ***Scan*** button. This will locate any unregistered and available cameras connected to the network (*It may be required to repeat this step a few times*).
- In the ***Unregistered*** tab select the cameras and then press ***Register***
- In the pop-up window select the server intended as the primary server for the cameras
- Some cameras (*for example ***Intellio Initio****) requires a user name and password before registering. Type in the user name and password under the ***Connection*** tab of the device then press ***Refresh***.

If a camera is not appearing in the **Unregistered** tab after a few scan, it can be because the firewall is blocking this option, or the **Scan** command in this device is not supported. The camera still can be registered manually by clicking the **Add** button next to **Scan** and selecting the type of device to be registered.

After typing in the proper information (see [Adding New Cameras/Devices Manually](#) (page 22)), press **Add**.



Registered to a server

Registered cameras will appear under the **Registered** tab along with their status.

Important: Always set a unique password for the cameras!

4.4.1 Camera/Device Replacement

When replacing cameras, the onboard detectors will become unavailable and respond with an error message in case of an activation request. This is caused by onboard detectors being hosted on the replaced camera.

The system detectors will continue operating perfectly after the replacement.

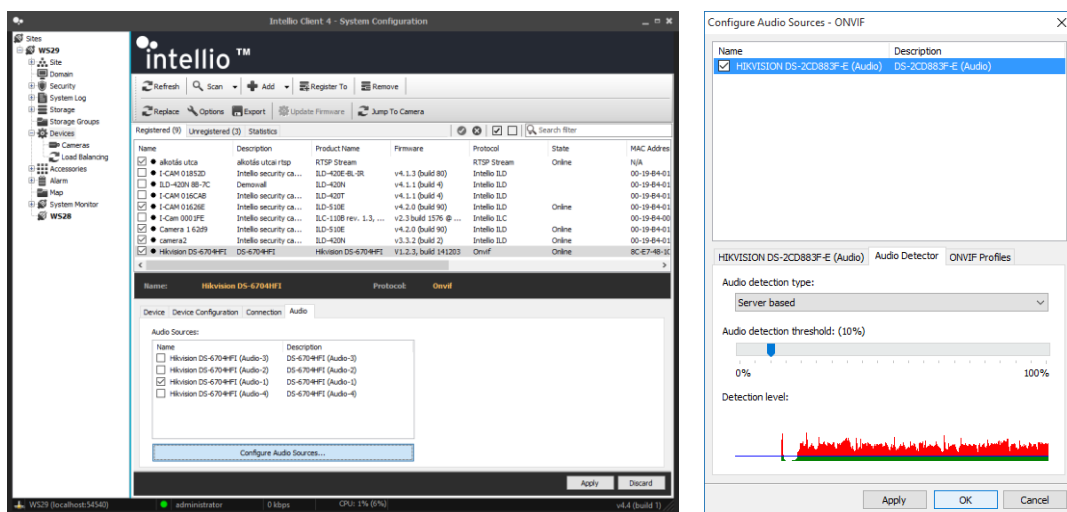
4.5 Setting the Audio Input

Managing audio inputs is an option with ONVIF, RTSP-streams and RTSP audio devices. Supported audio formats are as follows:

- G.711 PCM u-Law/A-Law (8000 Hz)
- G.726 ADPCM-16/24/32/40 Kbps (8000 Hz)
- AAC

The audio input settings can be found under the particular device: select the device in **System Configuration / Devices** and click on the **Audio** tab on the lower device settings interface. Here you can see an overview of the names and statuses of the inputs belonging to the device. To adjust the settings, click **Configure Audio Sources**.

In the next window, you can make the following adjustments:



- **Enable** checkbox: check/uncheck the box to enable/disable audio input. If no audio input is used, this is where it can be disabled to prevent the system from managing it.
- **Name** and **Description**: provide a name and description for the audio input.
- **Select Assigned Cameras...**: It is possible to configure which audio source we want to listen to with which camera image. This has a role when viewing live video and during playback. More cameras can be selected, however, by default an audio source is assigned to its own camera. An unassigned audio source is displayed in the audio source list, and can be turned on or off from there.
- **Audio Detector tab**: here you can adjust the sensitivity of the audio sensor used for storing.
 - **Disabled**: audio is not recorded, but on the live screen audio can still be monitored.
 - **Continuous**: continuous audio recording
 - **Server based**: in this case a detection threshold can be specified, which is given in percentages. The detected value and the threshold can be continuously seen on the bottom part of the window.
- **ONVIF Profiles** tab (only in case of ONVIF): select and edit ONVIF Media Profile to be used for audio channel. In case of audio/video, it is recommended to select the same media profile for the audio as for storing the camera images, since it will save you the trouble of creating a dedicated RTSP channel for the audio.

- **Audio URL** (only in case of RTSP-stream): selecting an RTSP URL used for the audio channel. In case of Dual-streaming – similarly to ONVIF – it is recommended to select the same URL as for storing video.

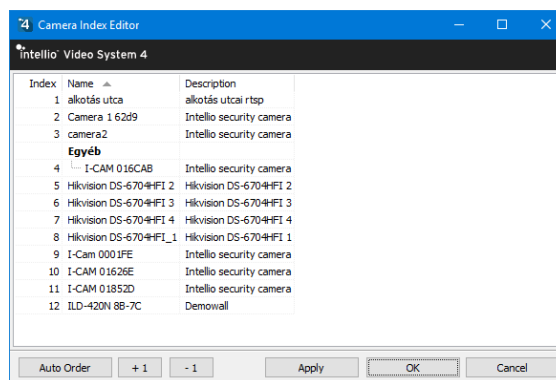
Audio is stored along with the camera images in accordance with the settings for Storage groups.

User access to audio sources can be managed under **Security**, separately for each audio input, as in case of cameras.

4.6 Editing the Camera Index List

With the help of the **Camera Index Editor** window we can assign a number to every camera in the system. This number can be typed in during live view, and the camera image connected to that value will be appearing on the active panel, avoiding the longer drag-and-drop method with the mouse.

The **Camera Index Editor** can be opened by clicking on the **Edit Index List** button on the **System Configuration / Devices / Cameras** menu.



Edited Index List

The easiest way to create the index numbers is the **Auto Order** button. This automatically orders a value to every camera, without any regards of the previous numbers. This order can be changed by clicking on the numbers and overwriting them, or by clicking on the **+1** and **-1** buttons (these will raise or lower the selected camera's number by one). Note, the Editor will not allow us to order the same number to two cameras. If there is a problem, the cameras in question will be highlighted.

5 Storage

5.1 Storage Settings

This section provides guidance on how to configure storage settings and use the available storage capacity more optimally. As opposed to an unconfigured system, a well configured system will store a lot more less events but the most important events will be stored as same as if a whole day's footage is being stored. Consequently a well configured system will waste considerably less storage capacity and hardware performance. As a result faster or *"capable of handling more cameras"* systems can be created that could be able of storing a few month longer footage.

5.1.1 Factors of Storage Capacity

In most cases it is almost impossible to provide an accurate estimate of the storage demand of a system that employs several cameras. This is due to the fact that a system's storage demand is determined by these factors:

- Frequency of motion in the scene
- Size of the moving objects
- The number of frames stored per second
- The bandwidth of the camera's stream

The **Intellio System Software 4** can be configured to filter out motion that is irrelevant from the aspect of security surveillance and thus conserve storage space.

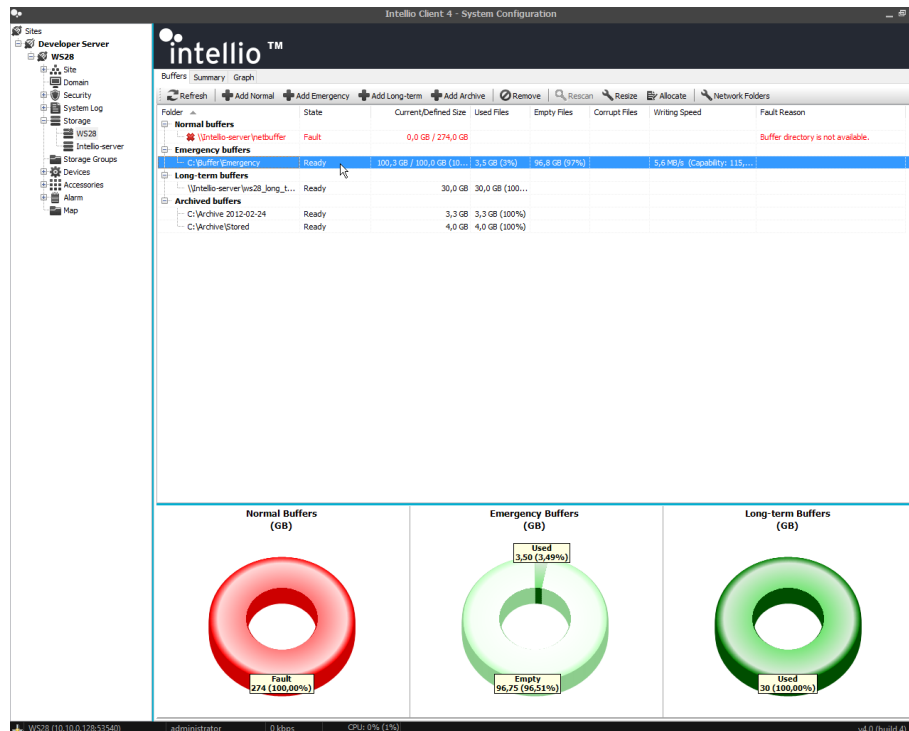
5.2 Buffers

There are four different kinds of buffers that can contain recorded images, as described below:

- **Normal buffers:** These buffers comprise the commonly used buffers. Their primary location is on the server computer, but they can be located on the network too (*the latter requires the route to the folder to be added using the **Network Folders** button, or by pressing the **Add Normal** button, then selecting the **Add network folder...** option*). If the buffer is full, the system automatically overwrites the oldest stored images. The buffer can be created using the **Add Normal** button.
- **Emergency buffers:** The server resorts to the emergency buffer only if the **Normal buffers** become unavailable for some reason. In other respects, emergency buffers work the same way as used buffers. It is recommended that these buffers should be located on server computers which do not store data locally (*NAS, RAID*), so as long as there is at least one server running, the recorded images will all be stored. The buffer can be created using the **Add Emergency** button.
- **Long-term buffers:** Depending on the settings the recordings can be transferred from the normal or emergency buffers to the long-term buffers (*instead of overwriting or deleting them*), thus extending the availability of some of the camera footage. Long-term buffers can be created by clicking the **Add Long-term** button. The settings of the Long-term buffers can be reached through the storage groups.

Note: to ensure proper operation, in case of a multi-server SITE, do not forget to create Long-term buffers on all the servers.

- **Archived buffers:** The archived buffers contain previously archived files, whose records can be replayed and whose events can be queried. The archived buffers can not be overwritten. For more information on the process of creating an archive, refer to [Managing Archive Files](#) (page 46).



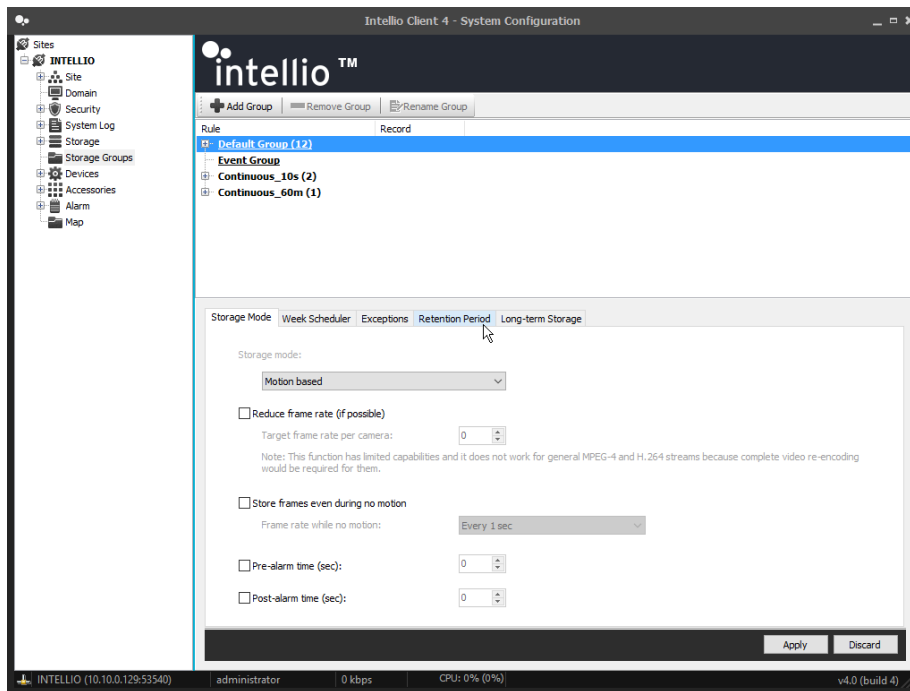
The system provides a lot of useful information about the status of the buffers, as follows:

- **State:** The current state of the buffer. Available values are *Ready*, *Fault*, *Allocation* or *Scanning*.
- **Current/Defined Size:** The current and defined size of the buffer. The two may differ.
- **Used Files:** The size of the files in the buffer folder which contain recorded images.
- **Empty Files:** The size of the unused (*empty of records*) files in the buffer library.
- **Corrupt Files:** The files which became damaged. These files are automatically erased after a server restart, unless they contain some usable records.
- **Writing Speed:** This column contains three important pieces of information. First, the average writing speed of the data. Second, the buffered writing speed (*the writing speed of the internal buffer where the incoming data arrives*). Third, the necessary writing speed for the incoming data.
- **Fault Reason:** In case there is a problem with the buffer folder, the system displays the cause of the problem.

Note: There cannot be a significant difference between the actual and the required writing speeds. If the required writing speed is higher than the actual writing speed, the program cannot write as fast as needed; as a result, frame loss may occur.

5.3 Storage Groups

Storage Groups define how incoming images, sounds and events are stored. By default all registered devices will fall under the **Default Group**. To create another rule press button **Add Group**. Every Group can have its own set of rules which apply on every device that are part of the rule.



Storage group / Default group

There are five main options available, these are:

5.3.1 Storage Mode

Here the basic rules concerning the framerate, and the stored data can be set.

- **Storage mode:** Three options can be selected from the drop down list.
 - **Motion based:** The server records only when the cameras are sensing some motion. This option is highly efficient, because it records only those events that may be relevant during playback (*i.e. a perimeter breach*) and will not bother recording the uneventful hours.
 - **No storage:** The cameras are working, but the server is not recording during this mode. That is no footage will be recorded that can be viewed at later times. As a result, the usage of this function is unadvised
 - **Continuous storage:** The server records continuously regardless of events or the lack thereof.
- **Reduce frame rate (if possible):** Adjust the maximum number of frames per second (*fps*) here. If transmission from the cameras is set at 10 fps, but the system is restricted to 4 fps, it could result in a decrease in the required storage by two thirds. Please note, however, that this is only an approximation, since the actual figure is a factor of the type of camera and video compression. No compression is made by the server upon storing – due to

performance considerations and keeping the original video. Therefore, this setting is inactive in case of certain video compression methods, e.g. H.264, MPEG-4 and MPEG-2.

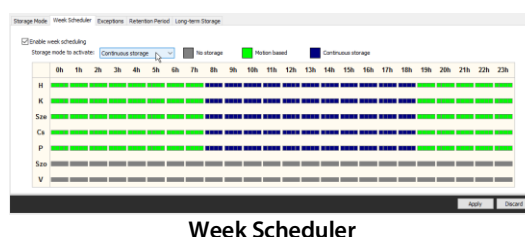
- **Store frames even during no motion:** in case of motion based recording, a time interval can be set (*from the dropdown list from 1 sec to 60 min.*) which will be used to store frames even if there is no motion.
- **Pre-alarm time** and **Post-alarm time:** Only works if the storage mode is motion based. These set whether the images before and after the movement get stored. This option is limited in four seconds, since the system can't store older images than this timeframe. Such a function exists in the ILD cameras ([Pre/Post Alarm](#) (page 56)), but this option is not limited to ILD cameras although less adjustable.

Note: the actual and the set value can be different (also depends on the camera's index frames distance).

5.3.2 Week Scheduler

This option is capable to create a weekly schedule, which repeats itself every week.

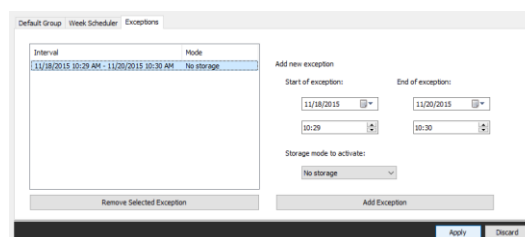
To configure this schedule, first **Enable week scheduling** and select one of the storage modes (*No storage; Motion based; Continuous storage*). By clicking on the squares the previously selected storage mode will be used during these intervals. If other storage modes are also needed, select another one from the drop down list, than get back to clicking on the selected time intervals represented by the squares.



Week Scheduler

5.3.3 Exceptions

This option can create exceptions to the rule set in the given Storage Group and the Week Scheduler. It could be useful occasionally in holidays or irregular events.

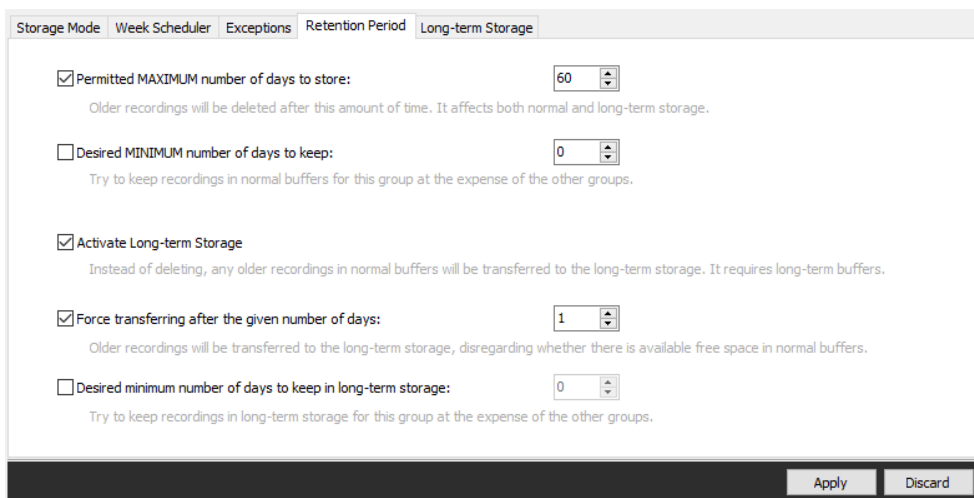


Setting exception

To create an exception, set the **Start of exception** and the **End of exception** dates and hours (*hh:mm*), then select the **Storage mode to activate** during this period.

A great number of exceptions can be set. To remove unnecessary exceptions from the list, select the exception and click **Remove Selected Exception**.

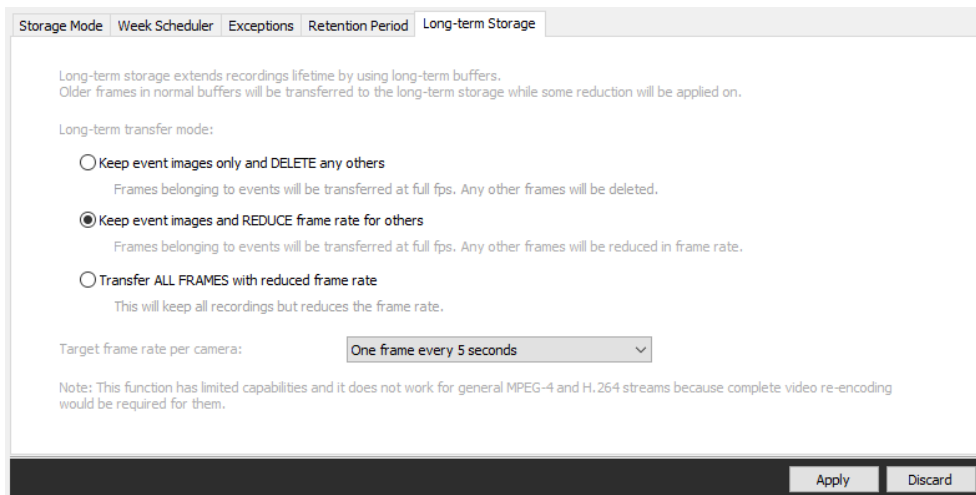
5.3.4 Retention Period



- **Permitted MAXIMUM number of days to store:** The server will delete stored images if the number of stored days reaches the selected value, even if there is free space in the buffers. This setting is applied on the normal and Long-term buffers.
- **Desired MINIMUM number of days to keep:** The server will always try to save the footage of this storage group; meaning that this storage group will always has priority over the rest. If no more storage space is available, then the system will delete footage from other storage groups to free up space.
- **Activate Long-term Storage:** the checkbox enables the long-term storage for the cameras belonging to this storage group (*the details of the settings can be found on the Long-term Storage tab*).
- **Force transferring after the given number of days:** if this option is enabled, the recordings older than the given value will be transferred to the long-term buffer, even if there is free space available in the normal buffers. Without this option the recordings would only be transferred to the long-term buffers when the system overwrites them in the normal buffer.
- **Desired minimum number of days to keep in long-term storage:** The setting is similar to the **Desired MINIMUM number of days to keep** setting; however it is applied only on the long-term buffer. The server will try to store the recorded footage in the Long-term buffer for at least the time set here. If there is no storage space available, the system will delete long-term footage from other storage groups.

5.3.5 Long-term Storage

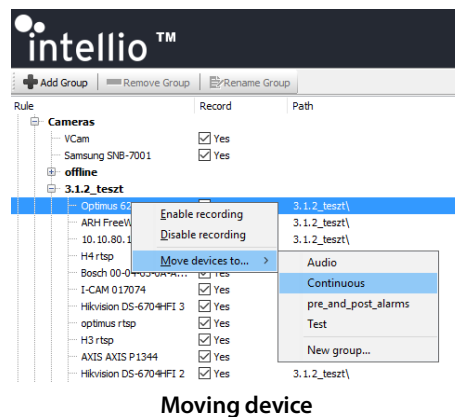
A bookmarked recording will always be automatically transferred to the long-term buffer (*all the footage of the cameras in the bookmark for the selected period without audio*) independently from the settings found below.



- **Keep event images only and DELETE any others:** the images belonging to events will be transferred to the long-term buffer without modification; any other images will be deleted.
- **Keep event images and REDUCE frame rate for others:** the images belonging to events will be transferred to the long-term buffer without modification; any other images will be transferred with reduced frame rates.
- **Transfer ALL FRAMES with reduced frame rate:** All the recordings will be transferred to the long-term buffer applying value of the **Target frame rate per camera** as the frame rate.
- **Target frame rate per camera:** when transferring footage with a reduced frame rate, the value set here will be applied as the frame rate. Less than 1 fps works with all cameras; more than 1 fps is supported only by Intellio cameras.

5.3.6 Moving Devices Between Groups

Each device can be transferred into any other storage group by using the drag-and-drop method. This also can be archived by clicking the right mouse button on the selected device and use **Move devices to...** option, selecting the target group or creating one.

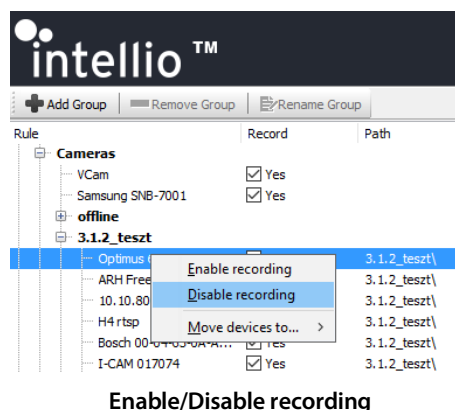


5.3.7 Enabling/Disabling Recording

To enable/disable recording from certain cameras, follow the steps below:

- Select a Group from **System Configuration / Storage Groups**.
- Select **Cameras** or select one camera of the **Group**.
- Right click with the mouse button, then select **Disable recording** or **Enable recording**.

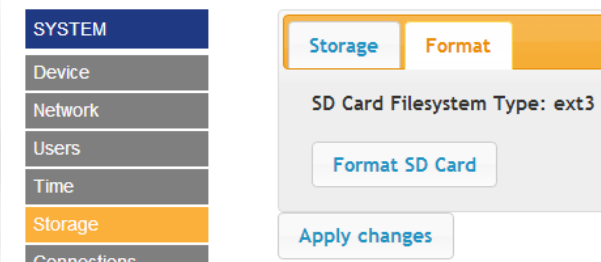
Recording can be stopped or started by using the check box next to the camera name.



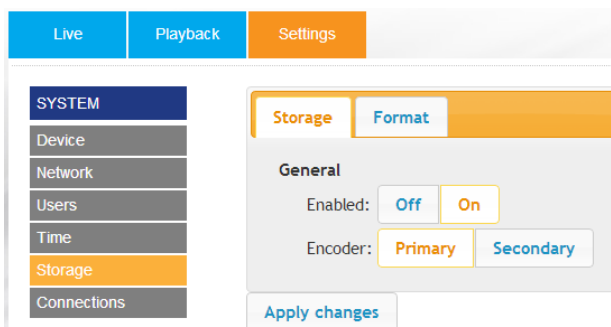
5.4 Storing Footage on a Memory Card

Intellio smart cameras capable of local storage are all equipped with a micro SD memory card slot. All such cameras require a microSD memory card (*suggested at least 8 GB*), for local data storage. The images will always be stored motion based for the sake of economy.

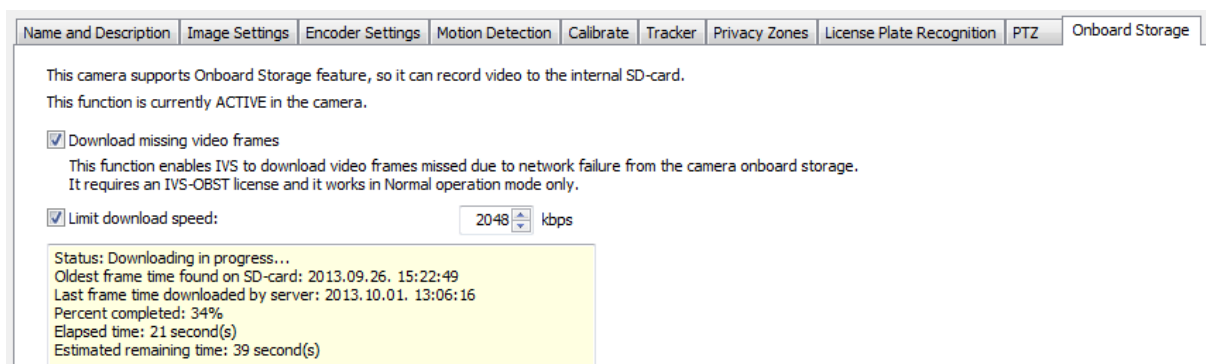
It is recommended to format the SD-cards first (*local storage works with factory-formatted SD cards, too, but it is less reliable*). Type into a browser the IP address of the camera connected to the system, then format the memory card through the **Settings / Format** tab.



Authorize storage on the **Storage** tab, then click **Apply changes** and wait for the process to be finished.

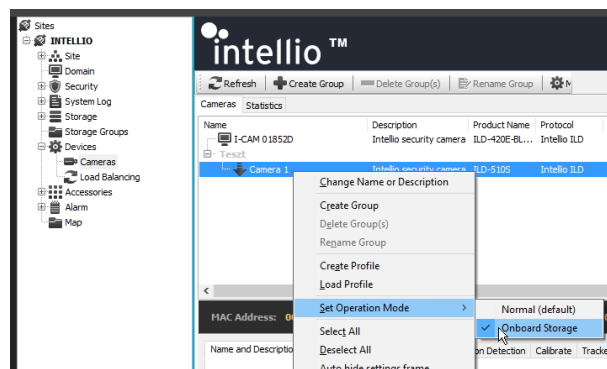


Then select the **System Configuration / Devices / Cameras** menu in the client program and click on the **Onboard Storage** tab of the authorized camera. The program detects the function being authorized.



Downloading can be authorized and the download speed of the omitted footage can be adjusted from the client side. This may come handy if the network is under a heavy load, which may threaten to disrupt the normal operation of the system.

If the camera is not available continuously (*e.g. it is installed on a vehicle*), it is recommended to enable **Onboard Storage** mode of operation. On a camera which has "Onboard Storage" enabled, live monitoring is not available, footage is exclusively recorded on an SD card. The recorded footage will be downloaded automatically when the connection is restored.



Changing operation mode

In **Normal** mode, the download of missing footage is limited to footage, which is recorded after the server start (*a possible server restart could result in loss of footage*), but if there is connection between the server and client, then live monitoring is possible.

5.5 Tools for Measuring the Storage Requirements

To summarize the storage demand of a system can be very useful. The program can calculate the size of the used storage space. It provides exact calculation about the size of the used storage space between two dates (*e.g.: one week time storage*). After such a summary it will be clear which cameras are sending considerably more events for storing comparing with the other ones. Sometimes these cameras can be set by considering stricter terms.

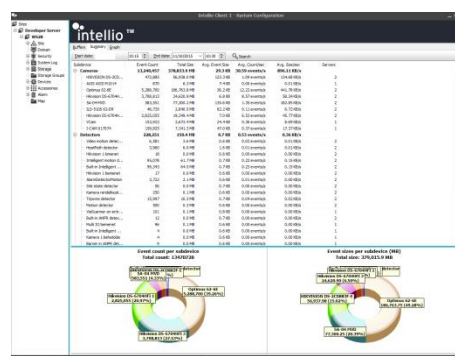
Following the steps below will get a summarized statistics from storage between two specified dates:

- Select **System Configuration / Storage** or one of the servers in **Storage**.
- Select **Summary**.
- Set the **Start date** and time and the **End date** and time.
- Click button **Search**.

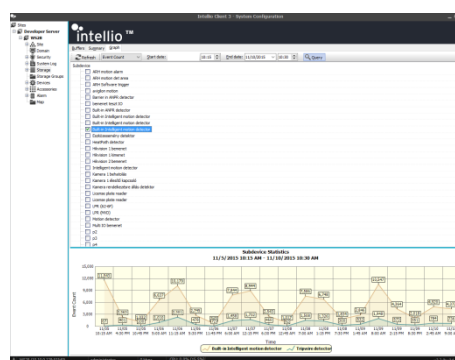
By using the graphical measurement it is easy to ask the number of recorded events between two dates from the selected cameras. For example by selecting a day time interval the graph will show those periods when the storage rate was the highest and the lowest.

Follow the steps below to get a graphic measurement from certain cameras and/or detectors:

- Select **System Configuration / Storage** or one of the servers in **Storage**.
- Select **Graph**.
- Select the data of the graph from the drop down list (**Event Count** or **Event Size**).
- By checking in the checkboxes select the camera(s) and/or detector(s).
- Set the **Start date** and time and **End date** and time.
- Click button **Query**.



Storage statistics



Graphical measurement

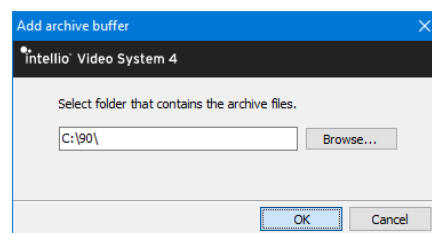
5.6 Managing Archive Files

5.6.1 Backing Up Buffers

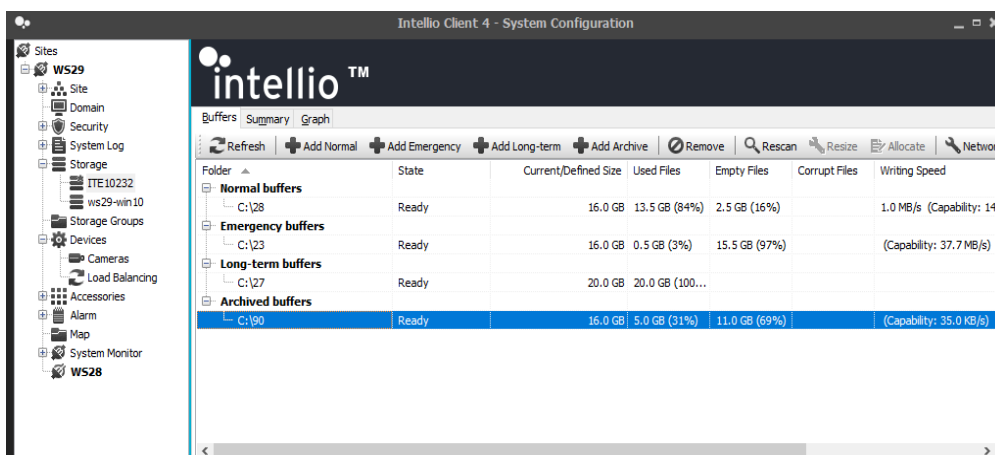
The backup process is a simple copy. Copy the ***.rcstore** files from your buffer directory to a separate directory (for example **c:\archive**). Do not delete the ***.rcstore** files from their original location, because those are the in-use buffer files.

5.6.2 Restoring Archive Files

Select **System Configuration / Storage** than select the server and press the **Add Archive** button. Browse to the directory where you store the previously backed up files and press **OK**. The system starts scanning the archive buffer. By pressing the **Refresh** button you can follow the process. If it reaches 100% you can use the archive buffer as a normal buffer, however in the archive buffer the footage will not be overwritten by the system. From this point you can reach the content of the archive buffer at the **Playback Mode**.



Add archive window



Archive buffer added

6 Video Adjustment (*Image Settings*)

Outstanding image quality is essential in video surveillance. To achieve this quality, it is necessary to adjust the image settings to the requirement of the environment. The video adjustment can be reached by go to **System Configuration / Devices / Cameras**, select a camera then **Video Adjustment** tab **Set Video Adjustment** button (*in ILC devices*), or **Image Settings** tab **Image Settings** button (*in ILD cameras*). These settings can be also reached from the live image, with the **Video Adjustment** button of the camera menu.

Since the layout of the ILD and the other kind of cameras is quite different from this version, we talk about them separately, although lots of the functions are basically the same in both types.

6.1 ILC and ILN series

6.1.1 Brightness

Auto Compensation: By default this brightness option is enabled. The camera automatically calibrates the **Optimal brightness value** level.

Optimal brightness value: The system set default value can be altered if the image of the camera is insufficient.



Brightness

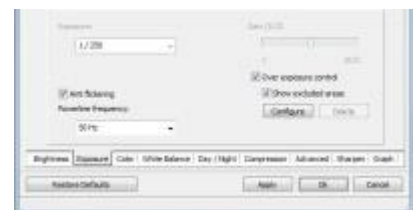
Manual brightness: To set the brightness level manually, disable the checkbox of **Auto compensation** and set it in the scale.

Iris Control: In **Auto** mode the iris is controlled automatically by the camera. In **Open**, or **Always Open** mode the iris is opened manually. Use this function when you are calibrating the sharpness of the camera.

Note: If **Auto compensation** is enabled it is not allowed to set exposure or gain values manually (**Exposure** tab).

6.1.2 Exposure

Anti-flickering: This function can be useful in an artificially illuminated environment, where the frequency of the light can be sensed through the cameras. By enabling it, this problem will be ceased to exist. Set the drop down list to the proper voltage standard (*can be find on the internet*)



Exposure

Over exposure control: If this option is enabled, the software will try to optimize the lighting conditions excluding the laid out areas (**Show excluded areas /Configure**, use mouse to set the border of the excluded part of the image).

Gain: With the help of this slide bar the brightness of the image can be altered. Mind during the settings that although the high value can brighten the image considerably, the noisier it will become. If the **Auto compensation** is enabled, this option is unavailable.

Exposure: It sets the amount of light the sensor gets. The defined possible values are the shutter speed times. The faster the exposure is, the darker the image gets, but the moving objects became more defined. This settings accessible only if the **Auto compensation** is disabled.

6.1.3 Color

Saturation: It allows the changing of the color richness.

Gamma: Accentuates details in low contrast areas without affecting shadows or highlights.

Contrast: Increase or decrease the contrast of colors. At high values the contrast will be sharper, but the image gets darker.



Color

6.1.4 White Balance

This function can be found exclusively in the ILC devices. It adjusts white balance to get the colors of your images as accurate as possible. If the **Auto compensation** is set, the white balance cannot be set. To use manual white balancing, disable **Enable white balancing**.



White Balance

6.1.5 Day/Night

Day/Night mode: It sets the basic attribute of the camera (*only camera series ending with a 10 has a physical IR filter e.g. ILC-110, ILC-210*).

- By selecting **Day** mode the IR filter is in front of the image sensor.
- By selecting **Night** mode the IR filter will be removed from the image sensor engaging higher sensitivity within low light circumstances and the capability to see within the range of infra light.
- By selecting **Auto** mode the camera will automatically adapt to the light conditions by controlling the IR filter automatically.



Day/Night

Day/Night threshold: The lower this value, the lower is the threshold when the camera switches to night mode, which means the camera switches to night mode even if the lighting condition is less dark.

Slow exposure: By enabling this checkbox the camera is allowed to set the exposure to 1/6 automatically if the lighting conditions are too low.

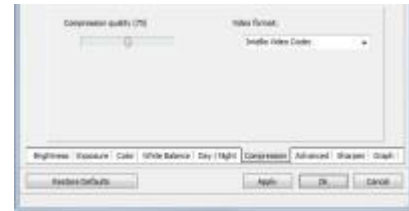
IR illuminator in night mode: It set whether the infra illuminator will switch on at night, or not.

6.1.6 Compression

Note: this tab cannot be found in the **ILD** Video Adjustment window because in these devices the compression settings are discussed under the [Compression](#) (page 49) part.

Video format: Intellio is using two kinds of compression methods for image transmitting

- **Intellio MJPEG** compression method has the same quality as JPEG compression. Every frame is compressed separately so frames can be dropped from the stream if it is necessary. Intellio MJPEG contains some additional features namely multi layering and uncompressing in reduced resolution.
- **Intellio Video** compression method is optimal for fixed cameras. Talking about video compression this method compresses only the difference of the image content. It causes a very optimal bandwidth and storage demand.

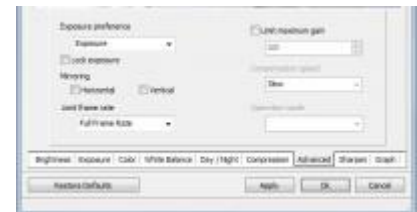


Compression

Compression quality: The image is less compressed by setting this to higher value; the quality of the image will be better. The image is more compressed by setting this to lower value; the quality of the image will be worse.

6.1.7 Advanced

Exposure preference: Noisy or blurred images operating under low light conditions have always been an issue in video surveillance. Now you have the option to choose the image to be less noisy against blurred or less blurred against noisy.



Advanced

- Selecting **Gain** the moving objects in the video will not be blurred.
- Selecting **Exposure** the quality of video will be less noisy, but could be blurred.

Lock exposure: By enabling it, the exposure will be set to a predefined value. This value is different for each option of the **Exposure preference**. Depending on these settings the exposure will be 1/100 in **Exposure** mode or 1/400 in **Gain** mode.

Limit maximum gain: An upper limit can be set to the gain.

Compensation speed: This function available only if the iris is manually controlled. If the iris is set to **Auto (Brightness/Iris control)**, the compensation speed is slow by default.

Intelligent functions' reliability is better if the video content analyzing can run in constant light conditions because the background doesn't change all the time. The **Compensation speed** function is able to automatically adjust the video adjustments thus the background changes without disturbing the real time video analytics. It can be said that the fast compensation speed will react to fast, temporary changes on the lighting condition, such as car reflectors at night.

- By selecting **Slow** the background changes as slowly as it doesn't affect to real time analytics.

- By selecting **Fast** the camera adapts to the lighting conditions the fastest way. This option is useful only if there is no intelligence used in these cameras.

Operation mode (ILC-1xx cameras)

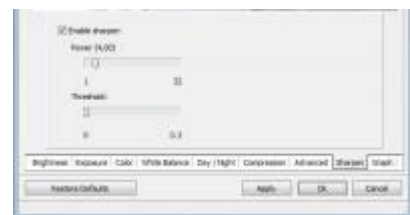
- By selecting **Optimized for quality** the camera will send better quality images but fewer frames.
- By selecting **Optimized for speed** the camera will send more frames but worse quality images.

Limit frame rate: Set an upper limit on how many image will be sent to the server.

6.1.8 Sharpen

It is a graphical feature of the client program to see the images more sharp. This has no effect on the recorded images. This adjustment takes effect just in the Intellio client.

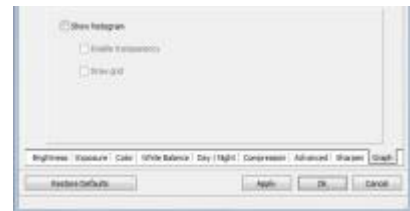
- **Power:** It sets how strong the sharpness of the edges is displayed.
- **Threshold:** Basically this is the noise filter, it filter out the non-edge contour lines (*and the edges too, if set too high*).



Sharpen

6.1.9 Graph

If enabled, a histogram will show up on the upper left side of the image, displaying the day/night mode, the exposure and the gain values, and on the histogram shows the brightness of the pixels.



Graph

6.2 ILD series

6.2.1 Day and Night Profile

The Day and the Night profile basically the same. The difference is that the camera can use different settings during night mode, than during the day. To enable this, check the Night profile (**Enable night profile** checkbox). The rules of the day and the night mode can be found in the **Day / Night Profile** tab of the **General** page.

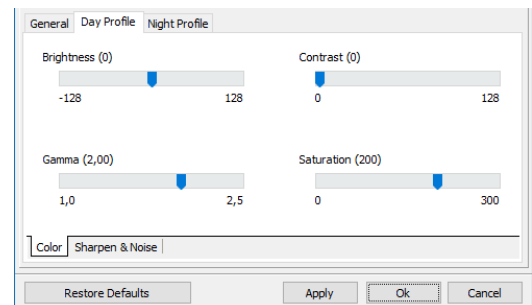
Color

Brightness: Increase or decrease the overall brightness of the image.

Contrast: Increase or decrease the contrast of colors. At high values the contrast will be sharper, but the image gets darker.

Gamma: Accentuates details in low contrast areas without affecting shadows or highlights.

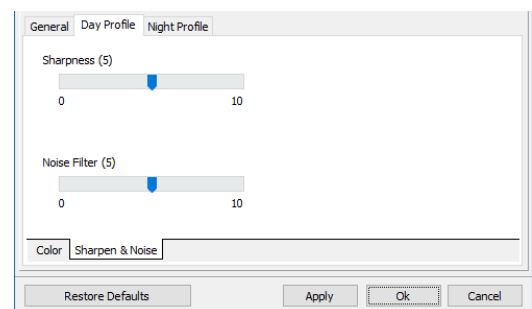
Saturation: It allows the changing of the richness of colors (*only for Day Profile*).



Sharpen & Noise

Sharpness: It sets the sharpness of the displayed image.

Noise filter: Sets the strength of the filter, which means the higher this value is, the image will be less noisy, but more blurred.



6.2.2 General

Iris

Iris Control: In **Auto** mode the iris is controlled automatically by the camera. In **Always Open** mode the iris is opened to the maximum. Use this function when you are calibrating the sharpness of the camera.

In case of VISUS cameras the Iris Control can be found on the **Miscs.** tab.

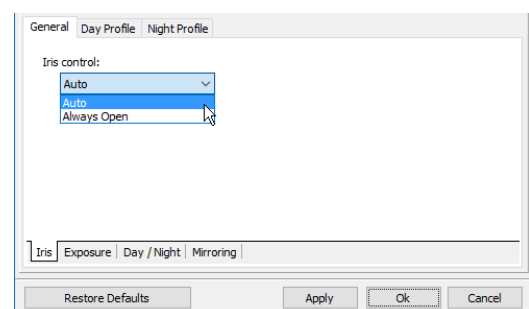


Image Control

The settings are available only for VISUS cameras.

Mode: Standard or Intelligent mode. In Intelligent mode, the camera will use the tracker information to control the image properties.

Auto Exposure Zone: Basic and Tracker options are available. When the Tracker option is selected, the camera will use the tracker information to continuously change the exposure zone.

Exposure

Max Exposure: Defines the maximum shutter speed, so it cannot be slower than the set value. Although if the shutter time is set low, the images will be brighter, but the fast movements will not be seen clearly in any images.

Max Gain: Sets the maximum of the gain value. If the gain is high, the image will be brighter, although noisy.

The following section outlines the key differences between the ORIO and the VISUS models:

ORIO

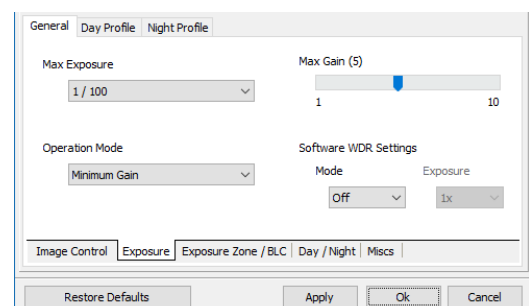
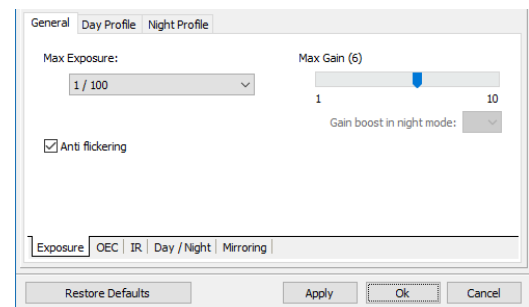
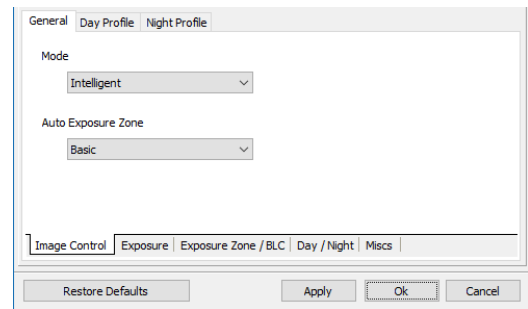
Gain boost in night mode: Gain can be boosted in nighttime mode, although this will also cause the images to be noisier.

Anti flickering: This function can be useful in an artificially illuminated environment, where the frequency of the light can be sensed through the cameras. By enabling it, this problem will be ceased to exist. Set the drop down list to the appropriate voltage standard (*can be find in the internet, for example here:* https://en.wikipedia.org/wiki/Mains_electricity_by_country)

VISUS

Operation Mode: This option allows for specifying the mode of operation of the camera, which will be used automatically later on (*minimum exposure, minimum gain and antiflickering*).

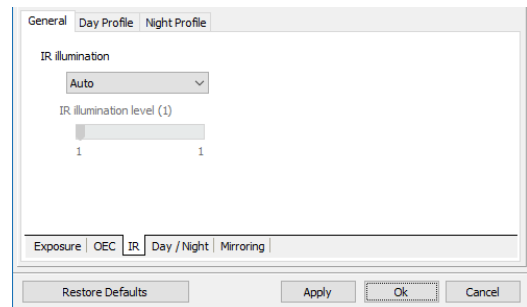
Software WDR Settings: Adjusts the "wide dynamic range" function. With the WDR on, the camera makes two images with differing exposure *times (a short and a long one)* and finally merges the two. The resulting image will be of optimum exposure in every part of the image. The multiplier next to the exposure value refers to the value by which the shorter exposure time will be multiplied to yield the longer exposure time.



In automatic mode the camera will employ the same multiplier. In anti-flickering mode the camera will set the exposure to a value of integer multiples of the frequency value.

IR

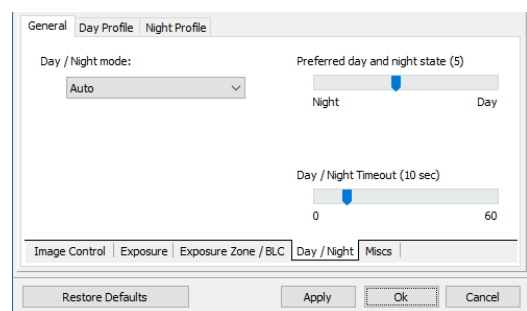
IR illumination: In this drop down list can be set, whether the IR illumination is **Enabled**, **Disabled**, or left to the system to decide when to switch it on or off by selecting the **Auto** option. The strength of the illumination can also be adjusted, avoiding the too much light.



Day/Night

Day/Night mode: It sets the basic attribute of the camera.

- By selecting **Day** mode the IR filter is in front of the image sensor.
- By selecting **Night** mode the IR filter will be removed from the image sensor engaging higher sensitivity within low light circumstances and the capability to see within the range of infra light.
- By selecting **Auto** mode the camera will automatically adapt to the light conditions by controlling the IR filter automatically.

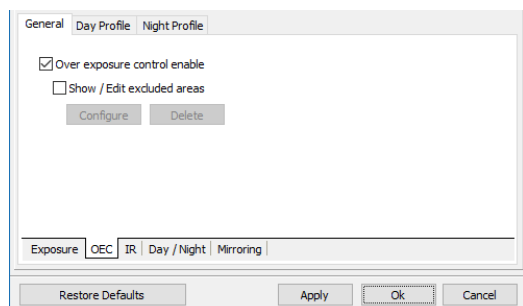


Preferred day and night state: The lower this value, the lower is the threshold when the camera switches to night mode, which means the camera switches to night mode even if the lighting condition is less dark.

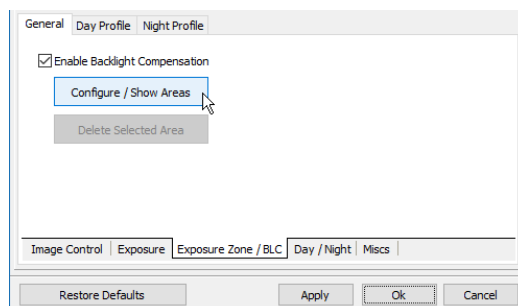
Day/Night Timeout: The amount time before the camera switches from day to night mode. This helps to avoid the false switches caused by irregular, temporary changes in the illumination of the observed area (*e.g. car reflectors, black-clothed man before the camera, etc.*)

Backlight Compensation or OEC (BLC)

This function allows for optimizing the light conditions of a SITE, especially useful when the monitored area is partly lit and partly dark. In case of ORIO cameras the selected area is ignored during the optimization process. In case of VISUS cameras only the selected area will be used during the optimization process.



ORIO camera



VISUS camera

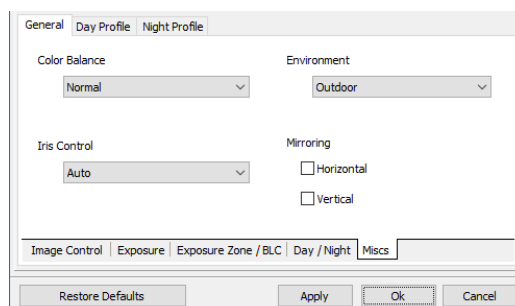
Misc (Miscellaneous)

Color Balance: There are seven settings options with various color modes to select from here. These settings are not client sided, and affect the recorded images as well.

Environment: *Indoor* / *Outdoor* options are available.

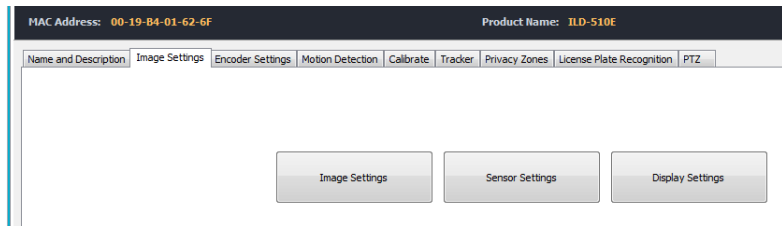
Iris Control: In *Auto* mode the iris is controlled automatically by the camera. In *Always open* mode the iris is fully opened. Use this function when you are calibrating the sharpness of the camera.

Mirroring: The displayed image can be mirrored horizontally and vertically. To set the mirroring axis, check in the proper checkbox next to the mirroring direction.



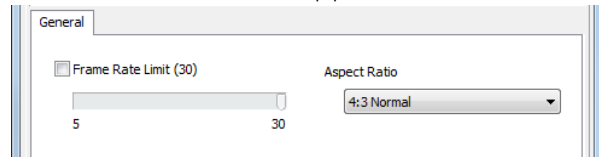
7 Sensor Settings

These settings are only available with the VISUS camera series. Similarly to the video settings, the settings interface can be accessed from the **Image Settings** tab.



After clicking the button, these values can be set on the popup window:

- **Frame Rate Limit:** The highest frame rate that the camera supports; it will not be exceeded even if the camera is capable of higher frame rates. Switched off by default.
- **Aspect Ratio:** The ratio of images transmitted by the camera.



8 Display Settings

This feature allows for the rotation of images produced by ORIO and VISUS cameras. When using this feature, the only detector running will be the onboard motion detector. Hence, you will either have to do without the other detectors or modify the camera position.

9 Encoder Settings

This chapter discusses the modification of the resolution of the images transmitted by the camera, the compression of the images, the custom settings of the various compression methods and the framerate settings.

9.1 ORIO cameras

The ORIO cameras' many configuring options are located in the **System Configuration / Devices / Cameras** menu. Just select an ORIO camera and the **Encoder Settings** tab will appear. The **Encoder Settings** window can also be reached through the camera menu, in the **Live** function. This is an extremely important part of the camera configuration, considering that several related functions are placed here.

9.1.1 General

- **Codec:** The used codec type can be selected (H264, Intellio Video Codec or MJPEG). Depending on the codec the bandwidth limit, the quality of the images, the I frame distance and other things can be modified.
- **Resolution:** Every ORIO camera, except the 100 series support three different kind of resolution. The smaller resolution means better fps, but worse image quality.
- Other settings peculiar to the compression method chosen.

9.1.2 Frame Rate Control

- **Reduced frame rate control:** Here can be set the trigger event of the reduced frame rate. The camera will turn on the high frame rate only if the selected event happens.
- **Target frame rate on event or motion:** If the defined event in the **Reduced frame rate control** happens, this is the frame rate the camera sends the images on.
 - **Basis of the reduced frame rate:** This can be an **alert**, a **motion** or **both**. If it is set to movement, the camera will only increase the framerate if it senses movement. If it is set to alerts, the framerate will only change is there is an alert event.
 - **Target frame rate if no event:** If there is no event in effect, this is the frame rate the camera transmits.

9.1.3 Pre/Post Alarm

This function can only be activated, if you using Intellio video Codec in the camera. This function means that the camera stores the images onboard (*SD card for example*) and in case of an alarm signal sends these images to the server to store. The post alarm means it is going to store for a while after the alarm ends.

The function is not affected by the storage function with a similar name (see [Storage Mode](#) (page 39)).

9.2 VISUS cameras

9.2.1 General

- **Codec:** H.264 is the exclusive compression method of the camera.
- **I frame distance:** The distance between key frames. The smaller this value, the smoother the frame rate lowering settings work, but increases the network demand.
- **Resolution:** The resolution of the image with the given compression method
- **Target Bitrate:** The approximate compression value of the video transmitted by the camera. The higher the value, the higher the image quality, but also the larger the network demand.

9.2.2 Frame Rate Control

The enabling and disabling of the functions on the tab can be done using a single check box. If the frame rate control functions are disabled, the highest possible frame rate will be provided by the camera.

- **Reduced frame rate control:** The type of events can be set here that trigger the higher frame rate mode.
- **Target frame rate on event or motion:** If one of the conditions set under **Reduced frame rate control** is met, the images will be transmitted at the frame rate set here.
- **Target frame rate if no event:** In the lack of a pre-set trigger event the camera operates at this frame rate.

9.2.3 Pre/Post Alarm

On the VISUS this function works even with the H264 codec, in exactly the same way as the previous generation pre- and post-alarm, see [Pre/Post Alarm](#) (page 56).

9.2.4 Secondary Encoder Settings

It shares all the settings of the Primary encoder settings. The only difference is that the secondary encoder settings is set to low resolution as a factory default.

9.3 ONVIF Cameras

ONVIF cameras comprise the ONVIF-certified cameras of various manufacturers, whose video compression settings can be adjusted on the **Profile settings** tab of the ONVIF camera.

9.3.1 Profile Settings

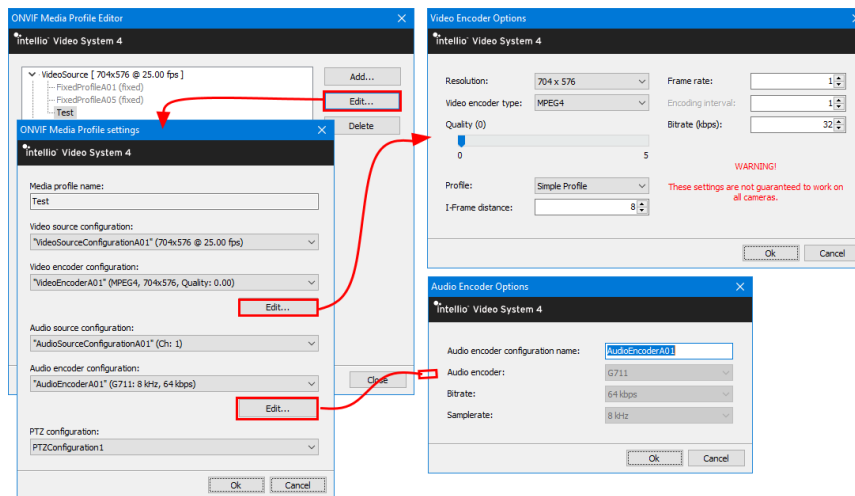
On the **Profile Settings** tab two **Monitoring Profiles** and the **Recording Profile** can be set.

- The **Monitoring Profile** is the high resolution, primary stream which can be displayed in Live video mode (*read more on the rules in the [Global](#) (page 16) section*).
- The **Monitoring Profile (low resolution)** is the low resolution, secondary stream which can be displayed in Live video mode when performance optimization is necessary.
- The **Recording Profile** refers to the images to be stored, their resolution, image quality and framerate. This is identical to the primary, high resolution stream. The **<Same as Monitoring>** option refers to the high resolution, so-called primary stream.

These profiles can be customized from the dropdown list, while new ones can be added and modified using the **Edit Profiles...** button on the tab.

PTZ-control: in case of an ONVIF camera, IVS decides whether or not the camera supports PTZ functions. It does this based on the PTZ settings of the live monitoring profile. However, this behavior can be overwritten here (*Auto/Enabled/Disabled*).

9.3.2 Editing Media Profile



Press the **Edit profile** button to add a new profile and edit/delete existing ones in the **ONVIF Media Profile Editor** pop-up window. The same parameters must be provided when adding or editing profiles.

- **Media profile name:** It can be selected on the **Profile Settings** tab.
- **Video source configuration:** Transmits the video stream. Evident in case of cameras.
- **Video encoder configuration:** Selecting from the list the video stream belonging to the profile.
 - **Edit...:** Editing the properties of the selected video stream.
- **Audio source configuration:** identifies the source of the audio stream.
- **Audio encoder configuration:** audio encoder selection for this profile from a list
 - **Edit...:** Edit the properties of the selected audio stream.
- **PTZ configuration:** If you are using a PTZ camera, then the PTZ configuration is entered here.

9.3.3 Video Encoder Options

The encoder settings of video streams can be set in this window.

- **Resolution:** the resolution of the images to be transmitted
- **Video encoder type:** the compression method (*H.264, JPEG, MPEG4*)
- **Quality:** the degree of the image quality loss (*the lower the value, the more the loss in quality*)
- **I-frame distance:** the distance between key images. Reference images, but significantly larger in size with a more significant processor demand. A maximum distance of 100 is allowed by the Intellio system, but the recommended value is 30 (*H.264*).
- **Frame rate:** the number of images per second.
- **Encoding interval:** determines which images are encoded and transmitted (*1- all, 2 – every second, etc.*).
- **Bitrate (kbps):** the maximum allowed file size of transmitted images. Sizes over the limit are compressed resulting in a loss in quality.

It may occur that certain settings are not applicable, therefore it is recommended to reopen and check the settings interface after approval. If the settings are not as intended, it is recommended to adjust the settings on the camera's own settings interface (*the camera may not support a given fps at certain resolutions*).

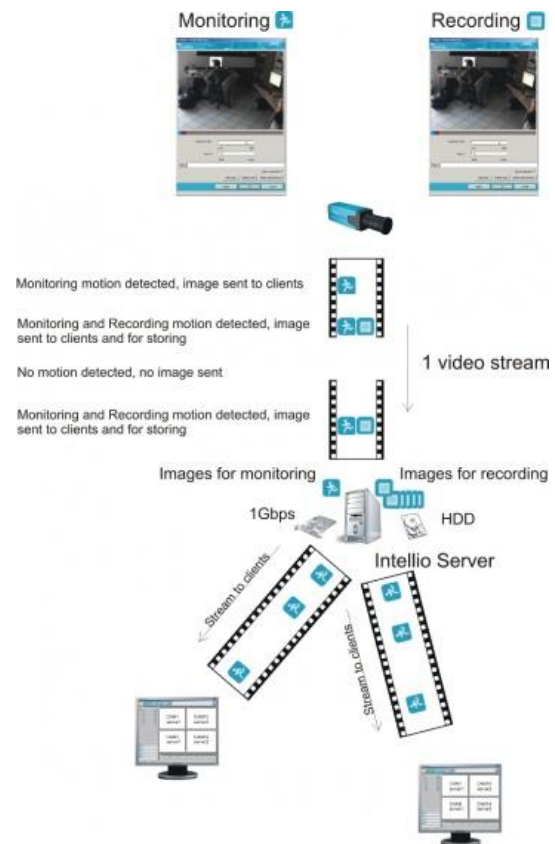
9.3.4 Audio Encoder Options

If the camera allows it, the properties of the audio encoder can be configured in this window.

- **Audio encoder:** method of encoding process (e.g. G711, G726).
- **Bitrate (kbps):** the maximum amount of data that can be sent within 1 second.
- **Samplerate:** frequency of sampling can be set.

9.4 Datastream

In datastreams the stream properties cannot be adjusted through the client, only through the camera's own settings interface. In case of RTSP- and MJPEG-streams the same three profiles can be set as in case of ONVIF cameras, see [Profile Settings](#) (page 57). The URL of the stream can only be selected from the ones that were associated with it when adding the device or later on the **Connection** tab of the registered device. If you change the URLs of the stream, check the profile settings of the camera on the **Cameras / Encoder** page (*Monitoring, Monitoring (low-res), Recording*).



10 Grouped Camera Setting

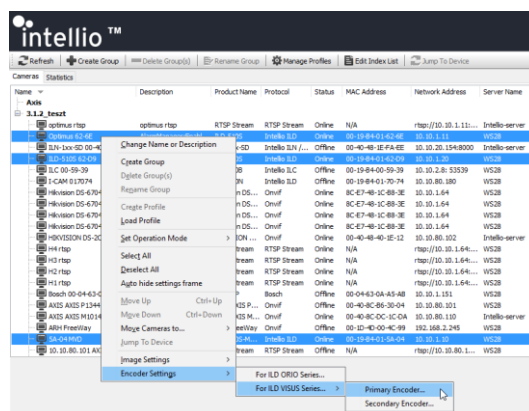
When using Intellio ORIO and VISUS cameras it is possible to configure the video image and encoder parameters in groups. When doing this, more of the same type of camera adjustments can be configured in one step, with this method a significant amount of time can be saved and your settings will also be consistent.

On the **System Configuration / Devices / Camera** page select the cameras you want to configure. To select multiple cameras press **Ctrl** or **Shift** during selection. By pressing and holding down the **Ctrl** key you can select multiple cameras one by one. To select multiple cameras that are adjacent to each other, press and hold down **Shift** then select the cameras.

Right click with the mouse on the selected cameras and select the function you want to change.

The grouped setting is available for the following parameters:

- **Image Settings**
- **Encoder Settings**
 - **For ILD ORIO series...**
 - **For ILD VISUS series...**
 - **Primary Encoder...**
 - **Secondary Encoder...**



When editing, a familiar window will appear, which can be used to configure the chosen parameters. The modified data will appear in highlighted letters. This way changes are easily trackable. When the changes are accepted, only the changed data will be authorized on each and every camera.

11 Motion Sensors

11.1 ILD Motion Sensor

The motion sensor is placed into the camera and it controls the image sending. There are two motion sensors; one is for monitoring and one is for recording:

If the motion sensor for monitoring senses motion the images are being sent to the clients for monitoring but will not be stored.

If the motion sensor for recording senses motion the images are being sent for the servers for storing but will not be sent for monitoring.

If both of motion sensors are sensing motion the images are being sent for the clients for monitoring and the servers for storing.



Configuring the motion sensor

11.1.1 Calibrating the Motion Sensors

Configuring the motion sensors can be done from **System Configuration / Devices / Cameras** menu. Choose a camera, then select the **Motion Detection** tab with two button inside. Select either the **Configure Motion Detector for Monitoring**, or **Configure Motion Detector for Recording** buttons. One of them forwards the images for live viewing, the other oversee the images sent for recording. These functions can be accessed from the live view through the camera menu from the **Motion Detector / Monitoring**, or **Motion detector / Recording** menupoints.

In the appearing window set the area in which the sensors will be operating. Several polygons can be created in one mask; also there can be more than one mask with different settings.

- The **Sensitivity** defines how low the threshold limit of small changes is in the background the value. On small values, a man walking in a similar shade as a wall could be undetected. On high values this never happens, but signals on small light changes.
- The **Motion Percent** defines a percent of the selected area, where if there is a change between the image, it is considered alerted. On small values, little moving objects and even small light changes could be detected as motion. On high values, too small objects might get filtered out.

Create as many masks as necessary. By creating several masks, different sensitivity and size values can be set.

11.2 Motion Detector for ONVIF, RTSP and MJPEG Videostreaming

Several of the ONVIF cameras are capable of using the camera-side motion detector, which reduces the load on the server processor, but also makes several functions unavailable due to insufficient data input. Data streams do not allow for a camera-side motion detector. Therefore, the type of motion detection must be well considered in case of such cameras.

- **On-board motion detector:** motion detection runs on-board the camera; the detector signals to the server when motion is detected, allowing the user to select a signal type from the camera from the ones that are available in the **On-board motion detector** dropdown menu.

Important: It can provide sufficient information for the operation of motion-based storage, however neither the Intelligent Motion Search, nor the Intelligent Event Browser functions work with such settings! In case of the data streams these options cannot be used. Similarly, neither can the ONVIF cameras be used which do not have this function.

- **Server-side:** motion detection running on the server side.

Important: Imposes an extra load on the server processor to an extent depending on the server-side motion detector used and the key image frequency set during the encoding of the video!

After selection the **Configure Server-side Motion Detector** button is activated. Press the button to open the pop-up settings window. Its setting is the same as described in the previous page.

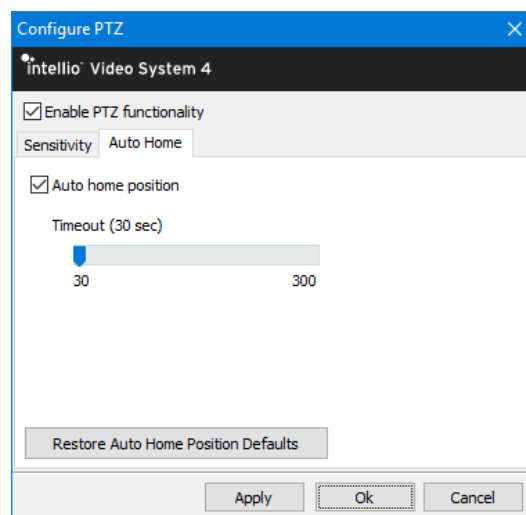
- **For I-frames only:** Motion detection only runs on the key images, which requires considerably less CPU performance, while Intelligent Object Detection is enabled.

Important: Intelligent Motion Detection and the Event Browser functions are still disabled!
- **For all frames:** During motion detection each image is inspected, regardless of whether it is a key image or not.

Important: This method is the most demanding on the processor, but each client function works with it!
- **Continuous motion:** This option only applies for the data streams, with the images being detected as if there is continuous motion (*i.e. in case of motion-based storage each image is recorded*).
- **Disabled:** The system does not detect motion for this camera (*i.e. in case of motion based storage the images are not recorded*).

12 EPTZ and PTZ

In the **System Configuration / Devices / Cameras** menu, in the **PTZ** tab of a camera there is a **Configure PTZ** button. The help of the opening window the EPTZ function and its **Auto home position** time can be authorized or forbidden. The EPTZ will log out of the function automatically after the timeout limit is reached, if the auto home position is authorized. If the EPTZ function is in use and not just authorized, the detectors will cease operation for that period, and the displaying of masks is suspended for the duration of this function.



On the VISUS cameras the Home Position can be set, which means its default state. If this is an EPTZ position, the camera will always revert to this position.

The movement speed of the EPTZ can be adjusted on the **Sensitivity** tab.

In case of cameras that are able to use motorized Zoom and Focus, these functions can be adjusted from the PTZ panel of the live view. The focus and zoom settings can be adjusted provided that the PTZ function is switched on and the camera is displayed on the active panel.

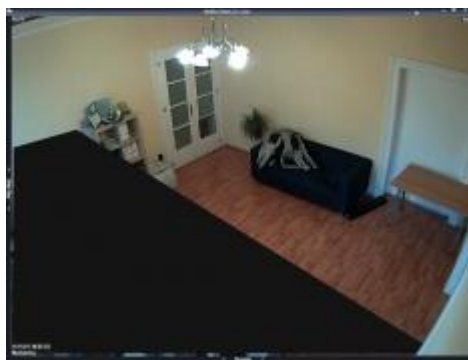


13 Privacy Zones

By using privacy mask a part of the image can be hiding from some users. Those users who have specified rights can see behind the privacy zones. To create privacy zones do the following: **System Configuration / Devices / Cameras / Privacy Zones** tab **Configure Privacy Zones** button. Start draw masks then click **Apply**. If you connect as an **Operator** you should not see behind the privacy zones.



Configuring privacy zones

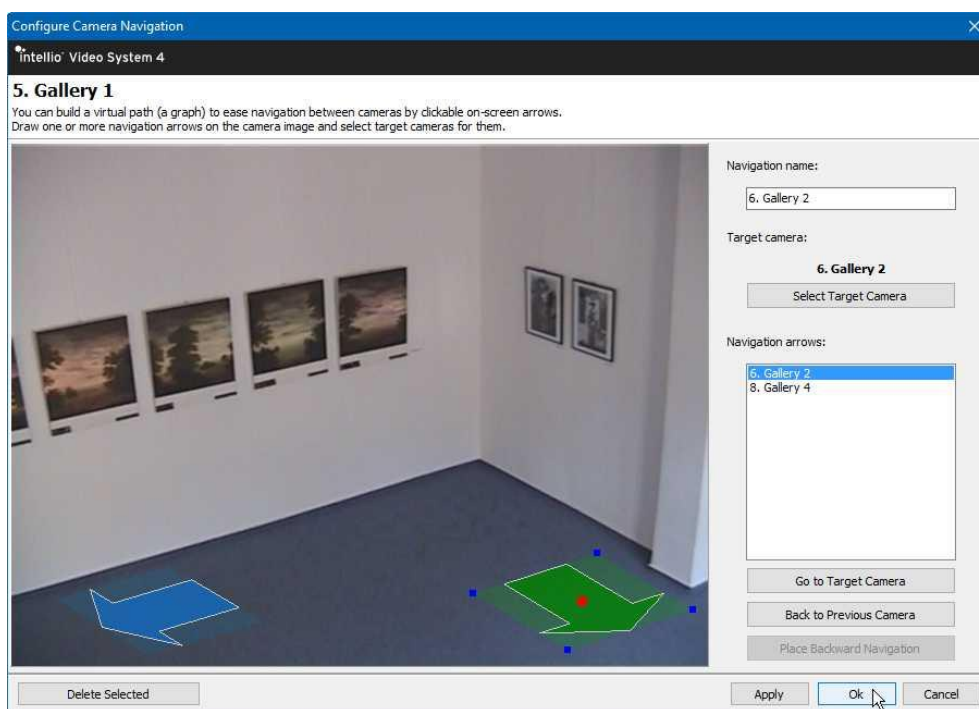


Privacy zones

14 Camera Navigation

With this feature you can set up clickable on-screen arrows with the help of which it is possible to efficiently navigate between the cameras. The camera navigation is camera independent, so it can be used with any kind of camera. To set the camera navigation, select the desired camera on the **System Configuration / Devices / Cameras** page, then select the **Navigation** tab, and press the **Configure Navigation** button.

The live view of the selected camera will be displayed in the **Configure Camera Navigation** window. The arrows which have already been configured will also be displayed. The camera title will be visible in the upper portion of the window. On the right side, you will find the controls which can be used to configure navigation.



14.1 Editing Navigation Arrows

To select an arrow, simply click with the left mouse button on the arrow or select it from the **Navigation arrows** list. The arrow that is selected will have a red dot in the middle.

To draw a new arrow, move the mouse to the point where you would like the arrow to begin and press the left mouse button. Next, move the mouse in the desired direction while holding down the left mouse button. When you reach the desired end point, release the left mouse button. The newly created arrow will be automatically selected.

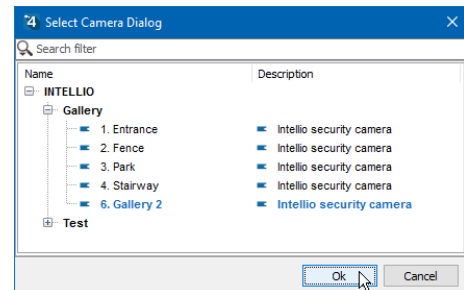
The size of the selected arrow can be modified. To do so, simply drag an edge or a corner of the bounding area of the arrow with left mouse button. To change the whole position of the arrow, drag the bounding area with the left mouse button and move it to the new position.

14.2 Navigation name

The caption of the navigation can be changed in the **Navigation name** field. This caption will be displayed in the live view if the mouse hovers over the arrow (*this can be enabled and disabled from the camera menu*). If you leave this field empty, the default name will be the name of the target camera.

14.3 Target camera

The target camera is the camera which will be displayed when you click on an arrow. To change the selected camera, click on the **Select Target Camera** button and select the desired camera in the **Select Camera Dialog** window and press **Ok**.



14.4 Navigation arrows

To ease identification and selection, all arrows placed on the camera image are visible in the **Navigation arrows** list.

14.5 Go to Target Camera

By clicking on the **Go to Target Camera** button, you can jump directly to the target camera of the selected arrow. This feature is useful if you would like to build a path from the selected camera.

14.6 Back to Previous Camera

If the visible camera image is displayed as a result of the **Go to Target Camera** navigation, by clicking on the **Back to Previous Camera** button, you can jump back to the previous camera.

14.7 Place Backward Navigation

If the visible camera image is displayed as a result of the **Go to Target Camera** navigation, by clicking on the **Place Backward Navigation** button, you can create a new arrow to the camera from where the navigation has happened. The name and the target camera of this kind of arrow will be set automatically, but they can be changed later. The button is disabled, if an arrow already exists to the previous camera, or if there is no previous camera.

14.8 Delete Selected

To delete a selected navigation arrow, use the **Delete Selected** button.

Note: the PTZ camera control takes precedence over the camera navigation. If the arrows are placed in the PTZ control circle, they will not work. If you would like to place a navigation arrow on a PTZ camera, put it outside of the PTZ control circle.

15 Camera Groups

It is possible to order cameras into camera groups. It could be useful if there are several cameras in one location; e.g.: the cameras are grouped according to which floor they are placed. To create camera group(s) and order cameras to groups click on the **Create Group** icon in the **System Configuration / Devices / Cameras** menu, then type in the name of the new group.

To order cameras into groups, select a camera(s) (*alt: select more cameras by holding the **Ctrl** button*), click with the right mouse button and select the **Move cameras to...** option. Select **Root** to get out the camera(s) from the group. To change the position of a camera on the list, use the two other options up next to **Move cameras to...** (**Move up**, **Move down**).

The order of the groups can be changed. Do the same steps just like with the cameras, but instead of the camera names, select a group name. In the opening menu, with the help of the bottom three options this order can be changed, or sub-groups can be created. You can replicate this affect with the help of the mouse: just drag it to the selected place.

To delete a group make sure that the selected group is empty select the group name, click on it with the right mouse button, and from the opening menu select the proper option.

16 User Rights/User Roles

The system is equipped with a global authentication management which can grant user rights not only on local SITES but on the whole Domain.

Each user has a unique user name and password. Every user has their own user role with uniquely configurable user rights. A user may only have one user role, while any given user right belonging to a user role may be assigned to multiple users (*e.g. every operator has their own user name, and each of them has the same operator user rights*).

These settings can be found in **System Configuration / Security**.

The IVS contains 2 roles and 2 users by default (*Administrator(s) and Operator(s)*). Number of the available roles and users depends on the version of IVS4 (*Corporate: 6-4, Enterprise: unlimited*).

RTSP users' permission settings also can be found here, which described under [RTSP Users](#) (page [124](#)).

16.1 User Roles

User roles define the actions that a user is entitled to do in the system. Users with the same role are endowed with the same user rights, which allows for creating an easily adaptable system.

16.1.1 Creating User Roles

Within the system, Local and Global user roles can be created. Local user roles exist and have rights on the SITE, which they were created on. Global user roles appear on the SITE they were created on and also on the lower level SITES in the domain hierarchy. They grant inheritable rights to the users with the same role.

User roles have **local** and **inheritable rights**. Local rights (*regardless the type of the role*) are granted on the SITE where the modification of the role is performed, while inheritable rights are granted on the given SITES and on the SITES situated lower in the Domain hierarchy. Hence, a user may have administrator rights on the user's own SITE, but only operator rights on the other SITES of the Domain.

The inheritable rights of a Global user role can only be modified on the SITE the user role was created.

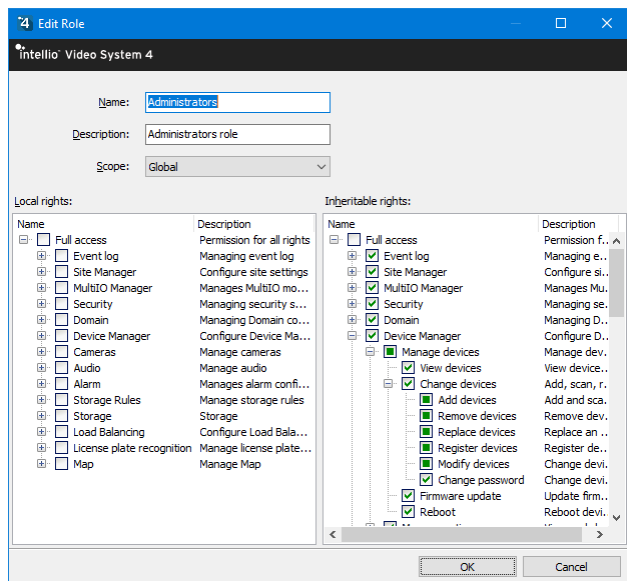
On the SITES where the Global user role appears as an inherited user role, the inherited rights cannot be restricted, but can be extended with local rights.

A user / user role which is accessible on every SITE on the Domain has to be created on the highest level of the Domain.

Local rights have to be configured separately on every SITE.

16.1.2 Deleting User Roles

User roles can only be deleted if they contain no users. If you wish to delete a user role with users belonging to it, first you need to remove all the users from it.



Editing a user role

16.2 Users

Each user has their unique **Login name** and **Password** (required for connecting to a *SITE*), as well as a **User name**, which is the full name of the user. The login name and the user name can be identical.

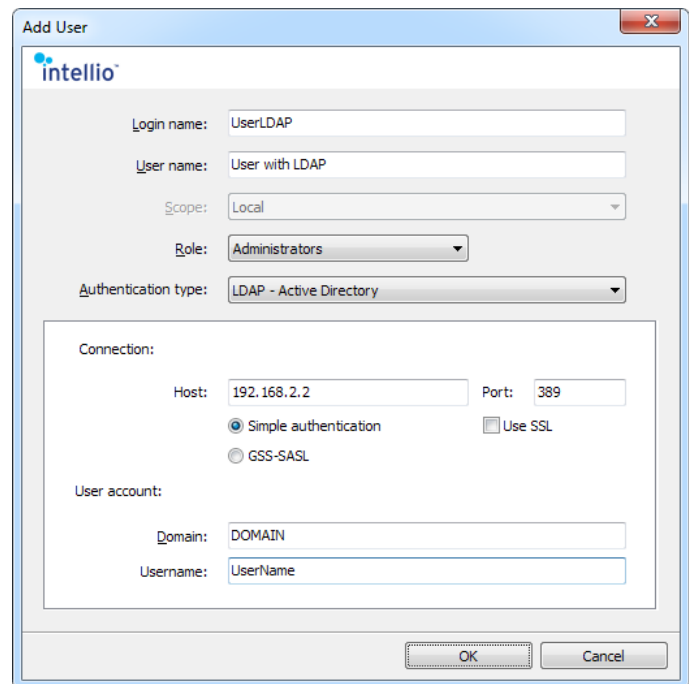
User access rights depend on the user roles assigned to the user. Make sure to always have at least one user with all the rights, otherwise some of the functions will not be available anymore. By default it is the **Administrator** who has all the rights.

16.2.1 Creating New Users

When creating a new user, its **User type** (*Global or Local*) has to be defined, while a **User role** has to be assigned to it from the **Role** drop down menu. In addition, a **Login name**, **User name** and **Password** have to be selected for the new user.

Since every user has to be assigned a user role, make sure that the necessary role is available.

Local users exist solely on the *SITE*, they cannot be reached from other *SITE*-s of the *DOMAIN* and cannot log in to other *SITE*s of the *DOMAIN*. If you wish to log in with the same user from multiple computers, create a **Global** user. A Global user profile will be available on *SITE*s found deeper in both the *SITE* and *DOMAIN* hierarchy. A Global user can only have a Global user role.



Authentication type

Default is **IVS – Intellio Video System**, where the IVS system will deal with user authentication. You can select **LDAP** authentication for a user, which is based on forwarding the user details to the domain driver of the computer, which, in turn, authenticates or declines login (for the appropriate Windows user). It is important to note that only the password is verified during verification; the user rights are stored by IVS. LDAP authentication only works with a Local user profile.

Note: LDAP authentication is available only in the IVS4-Enterprise version.

16.2.2 Editing User Details

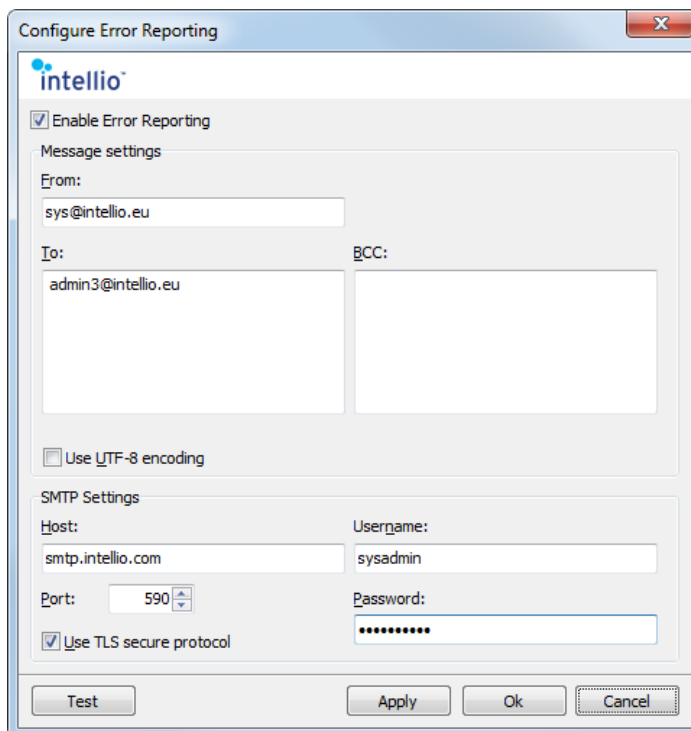
The **Login name** of an already existing user cannot be modified. In order to rename, the user has to be deleted and another user has to be created.

Important: Do not forget to change the default passwords!

17 System Log and Error Reporting

During the logging every server of the SITE has a separate log. This makes it easier to observe the communication between the servers, and the events of a single server too.

In case of multiple cameras or multiple servers, the use of error reporting can make the detection of an error much easier. Due to the redundant nature of the system's operation, the operator may not notice that one server went down, because other servers will take over the tasks of that server. It is in these cases when error reporting proves useful. It allows the operators to be notified of errors without the need to continuously browse the system logs.



In the log, some of the entry can appear either as a warning or as an error. This is deliberate, because while server restarts do warrant a warning, if the said server starts properly, and does reconnect to the SITE, an error message is not necessary (*the SITE can function with losing one server*). If the said server cannot restart properly, after a while the system detects this as an error. There is a similar logic behind the lost camera entries.

The system is able to transmit every error entry through the internet in the form of an email. To configure this option, go to the **System Configuration / Site / Site** menu and push the **Configure Error Reporting** button, then set the page just like you would an email client.

The **From** and the **To** fields require the input of e-mail addresses with the @ symbol in them, and they cannot contain a space character.

When you input your settings, make sure that all the servers are capable of transmitting data. The appropriate operation can be verified in the **Configure Error Reporting** window with the help of the **Test** button, when the button is pushed, all servers of the SITE will send a test message.

18 The Intellio System

Intellio Video System has two important basics. The first one is the network the second one is the hardware of the server computers. If one of these two breaks down the system becomes unstable. Except if we prepare for it in advance.

Namely if there is redundancy in the system, the breakdown of a malfunctioning device will not cause any problem for the operation of the system. By creating a SITE which contains more than one server the following "SITE features" will be available.

18.1 Camera Takeover

It is an automatic algorithm which registers cameras of the malfunctioning server to the remaining server(s). The recording will not stop from cameras in the SITE which is probably the most important expectation towards a camera system.

Required assumptions to make this function work:

- At least one network route is necessary from the cameras to every server.
- The network speed between servers should be as fast as to be capable to provide all the cameras.

It is practical to prepare the servers' configuration to be stronger than it is necessary for the planned camera number.

If the malfunctioning device is working again the system automatically detects it and recovers the original state of the system.

18.1.1 Camera Locking

Sometimes it is necessary that particular cameras be continuously registered at a certain server, whether the server is working or not (*e.g. server-side license plate recognition*).

In such cases the cameras can be excluded from the automatic camera takeover.

- Select the particular camera on the **System Configuration / Devices** page.
- Check in the **Server Name** column whether the camera is registered at the server for which you wish to lock it.
- If necessary, register the camera at the desired server, by clicking the **Register** button.
- Right-click on the device, and select **Lock Device** from the appearing menu.

To release the locking follow the same steps.

18.2 Load Balancing

Server resources are mostly consumed by storing the camera images and serving different requests from connected clients. Load balancing is a technique to spread work between two or more Intellio servers in order to get optimal resource demand. Using load balancing the reliability is increasing, the response time decreasing.

By enabling load balancing function the system is able to calculate the burden of connected servers' retrospectively, based on the stored records in the past. If one of the servers is storing a lot more images than the others, load balancing is the perfect tool to compensate this.

This action does not take negative effect on playback. Although re-registering is a few second of losing the connection with the server, the time interval and the minimum days between two registrations can be selected, minimizing the problems caused by this. Probably the best setup if the registering happens when the traffic is the lowest in the protected SITE.

Before enabling load balancing it is recommended to start with making statistics about the storage of servers in the SITE. It can be made in the following way:

- **System Configuration / Devices / Load Balancing / Statistics.**
- Set the **Start** and **End** time between you want to get the results.
- Click on the **Query** button.

To set load balancing follow the instructions below:

- Check in the **Enable Load Balancing** box.
- Set the value of **Calculate based on the given past days** retrospectively.
- Set the value of **Minimal days between registrations.**
- Set the value of **Start time of load balancing (in hours).**
- Set the value of **End time of load balancing (in hours).**
- Select those days when registering is allowed .
- Select those cameras which are allowed to be registered to another server .
- Click on **Launch** button.

18.3 Site

The basic element of the architecture is the Intellio server. This program represents the core of the system. It communicates with the cameras and records the footage and events that are being received from the cameras. All the data is stored on the server hard disk. The server program runs on each server computer as a Windows service, which means it starts automatically on the start of the system and operates in the background.

The SITE handles the data to be consistent between servers. One master server has to be dedicated always in the SITE which coordinates the synchronization of data. The rest of the servers are Slaves.

In case the SITE contains several servers provide fast LAN (*1Gbps*) between servers for continuous communication and data synchronization.

To merge multiple servers into a SITE, all the servers must have the IVS-SITE license.

To check the actual licenses and modules of the servers, use the **Intellio Activation Tool** application, or take a look at the **License** column of the **System Configuration / Site / Servers** page.

Important: the supported maximum number of the servers in a SITE is 4!

18.3.1 Add Server to the Site

An existing SITE can be expanded with additional servers. The server you add to a SITE must be default configured. Do not configure a server until it is added into a SITE. Use the default **Login name** and **Password** for adding a server. Provide fast LAN between servers before adding. The steps of adding the servers are the following:

- Click the **Add server** button.
- Enter the server's network address (*IP or name*).
- Enter the default **Login name** (*Administrator*) and **Password** (*admin*).
- Click the **OK** button.

Important: The added server's previous settings will be lost and replaced by the Master server's settings! It is not worthwhile to configure the servers of a SITE and then organize them into one SITE! SITES can be expanded by servers that are not configured.

If a SITE contains more than one server, it is important to synchronize the clock of the servers. The **Automatic time synchronization between servers** can be enabled on the **System Configuration / Site / Site** page, if this is enabled the IVS system provides the time synchronization. This option should be disabled if you would like to synchronize the clock in a different way (*e.g. with an NTP server*).

18.3.2 Change Master Server

It is necessary to dedicate another server to a Master if the existing one is not functioning.

Important: The configuration of the system is done through the master server. If the master server is not available, no modification is possible in the system's settings!

In the interface you can see which server has been dedicated as a Master. To change the master server follow the steps below:

- Select a server.
- Click on **Mark as Master** button.

After the change a few seconds will elapse until the change is confirmed. Use the function **Refresh** to get up-to-date information from the state of servers.

18.3.3 Modify the Data of Servers

To modify an already existing server, go **System Configuration / Site / Servers**, then click on **Edit** button

By default the name of a server is always will be the name of the computer itself. The address of the server mostly is the name of the server also. In networking if entering the name of the computer as network address then the DNS can translate it to the devices' unique IP address in decimal digits.

Mostly from networking aspect the servers sometimes must be configured differently as it is default configured:

- The **Name** of the server is just a simple ID of it.
- Adding a **Description** could be helpful sometimes.
- The **Address** of the server is the network address of the computer which will be used by Intellio Server. It could be important if a server computer has more IP addresses.
- **Port** is the TCP communication port of the Intellio server (*at default 53540*).
- **External address** must be added if the SITE wants to be monitored from a remote location from a WAN. In case there are several servers in the SITE please set different TCP **ports** to every Intellio server and make sure the port forwarding rules are set properly (see [IVS Client Internet Connection Configuration](#) (page 76)).

Important: For Domain control all of the Intellio servers' must have an external address to be set!

18.3.4 Delete Server

The servers can be removed from a SITE with the help of the **Delete** button. The rules concerning the disconnection are the following:

- There can't be any camera registered to this server.
- The server cannot be Master.
- The user cannot disconnect a server, if he/she is logged on in it.

Important: The number of the SITE's camera licenses decreases by the number of removed server camera licenses!

If you would like to reuse the removed server at a different location as a stand-alone or SITE server, it is recommended that you fully reinstall the system.

18.3.5 Clients

Several clients can connect to a SITE simultaneously. In this case the bigger data transmitting could load on the servers and the response time of the system could decrease. The burden of the system is optimal if the connecting clients are distributed equally among the servers. To ensure this, be sure to check the [Logging in to a Site](#) (page 18) part to see the proper configuration of the client. If setting up correctly, when a user logs in into a SITE the client connects to a server randomly to ensure the optimal burden distribution of the servers.

Go to **System Configuration / Site / Clients** to see how many clients are connecting to the SITE.

18.4 Domain

The Domain is able to logically connect numerous SITES together in order to manage them in one integrated system. It makes possible to handle remotely the SITES through one client program.

Go to **System Configuration / Domain** to see which SITES are connected and what kind of hierarchical connection is between them. The green background square areas demonstrate the SITES. The name of SITES and the servers within the SITES are seen in the squares.

The items of System Configuration menu are always belonging to one SITE. In the hierarchical list of System Configuration as many name of SITES are seen as many are connected in the domain.

Before creating a domain, please make sure that the servers of the connecting SITES own external addresses. If they do not, the SITES cannot connect.

To create a DOMAIN, all the SITE-s servers must have an IVS-DOMAIN license.

To check the current licenses and modules of the servers, use the **Intellio Activation Tool** application, or take a look at the **License** column of the **System Configuration / Site / Servers** page.

18.4.1 Domain Enlargement

To enlarge the domain, SITES can be added to the existing domain. Because of the hierarchical architecture of the domain a SITE must be selected and the added SITE will be its inferior. To enlarge a SITE, follow the steps below:

- Select a SITE.
- Click the **Add Site** button.
- Enter one of the SITE's master server's network address in the **Port** and **Address** fields.
- Add the **Login name** and **Password** for that SITE.
- Click on **OK**.

The added SITE name appears in the System Configuration menu. Click the right button of the mouse on the icon next to the SITE name. You can **Connect** to it and the System Configuration menu belonging to it appears.

18.4.2 Deleting Sites

To delete a SITE from the Domain follow the steps below:

- Select the area of SITE in the user interface (*the background turns red*).
- Click on the **Delete Site** button.
- Confirm the progress.

18.5 Configuring Internet Access

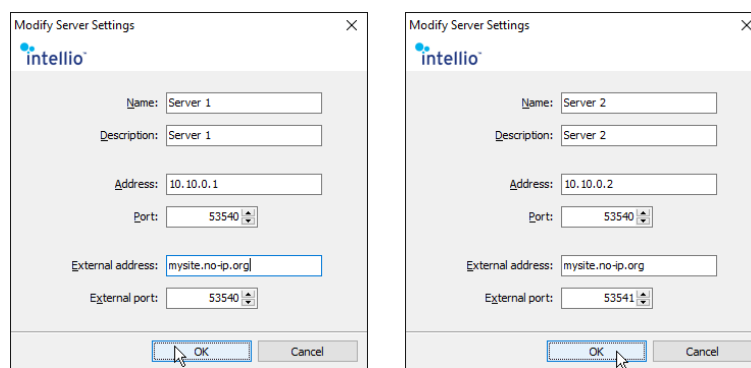
To reach servers from an external (*internet*) network, all the SITE's server must have an external address and an external port. A server cannot be accessed from an outside network if it does not have an external address / port.

18.5.1 General Server Side Settings

Configure the SITE's router in such a way that all the servers, which have to be accessed have an open port. Now, forward the port's traffic to port **53540** on the corresponding server.

To set the external parameters (*external address, external port*) of the servers that are also accessible externally, open the **Modify Server Setting** window by clicking **Edit** on the **System Configuration / Site / Servers** page. Type the IP address or domain name of the internet gateway into the external address field. Dynamic DNS (*Dyndns, No-IP, etc.*) services can be used if there is no fix IP address or domain name.

Set the external port to the port that was assigned to the server.



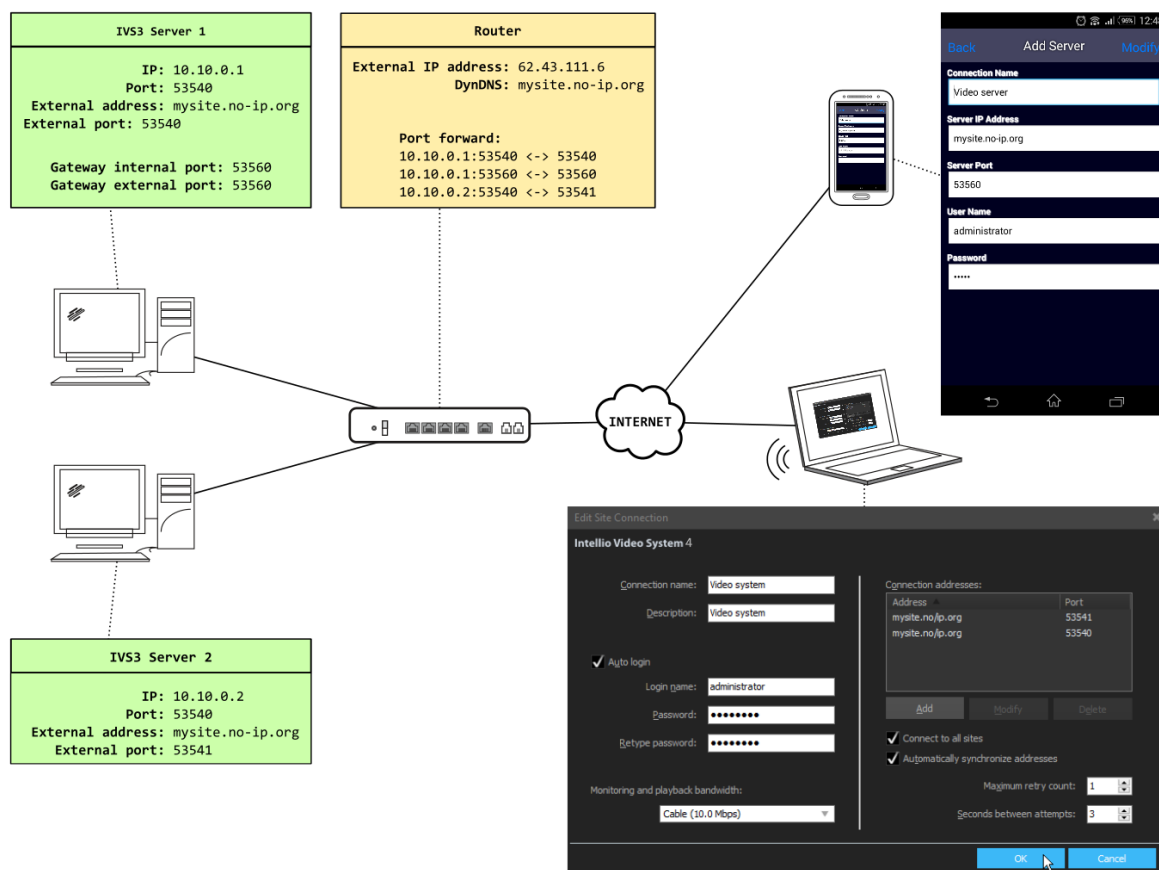
18.5.2 Server side settings for the IMC (*mobile client*)

If you do not want to use playback or event browser features of the Intellio mobile Client, you do not need to configure any other settings. Simply enter the external address and port in the mobile client's connection settings.

For playback and events browsing in the mobile clients, you will need at least one Intellio Video Gateway service per SITE.

For more information on how to check the status of the Intellio Video Gateway, read [Determine the Status of the Software](#) (page 11), if necessary it can be installed by **IntellioServerSetup.exe**.

Configure the SITE's router in such a way that all the installed Intellio Video Gateway services have an open port. Now, forward the port's traffic to port **53560** on the corresponding server.



18.5.3 IVS Client Internet Connection Configuration

When establishing the connection enter the external address and port of the servers in the IVS client. It is recommended to set the maximum bandwidth of the connection according to the available bandwidth.

18.5.4 IMC (*mobile client*) Internet Connection Configuration

In the connection settings of the mobile client enter the external address of the SITE and the external port of the gateway / server, depending on whether or not you want to use the playback / event browser function.

19 Firmware Update

The firmware is a software running on Intellio cameras that ensure the cameras operation. From time to time *(for the implementation of new features or for bug fixes)* the cameras firmware may need to be replaced. A firmware update for Intellio cameras can be performed directly from the IVS4 Client application *(recommended)*, or through the camera's web interface.

19.1 Updating Intellio Camera Firmware

First of all download the newest firmware from <http://intellio.eu/>.

The earlier firmware versions can be downloaded via [ATSS: http://arh.hu/index.php/en/support.html](http://arh.hu/index.php/en/support.html)

After downloading the firmware, follow these steps:

- Start the client program, and connect to the server or the SITE where the cameras are registered.
- In the **System Configuration / Devices** menu select the camera or cameras you want to upload the new firmware. The device has to be online, and registered. You can upload the new firmware to more than one camera at the same time by holding down the **Shift** or the **Ctrl** while marking them and then pressing the **Update firmware** button on the upper toolbar.
- Browse to your firmware by using the standard windows method then open it.
- Now check if the camera is on the list of supported devices. If it is then press **Yes**. The update process takes about 1-2 minutes per device, but in rare occasion it could take up to half an hour *(some ORIO firmware version)*.
- If the firmware update is successful, the camera *(or cameras)* will reboot while the client will display a dialog box about the successful update.

Note: *It could happens, that the camera cannot update the firmware at the first time. Simply repeat these steps, and be sure that the cameras are registered and online. Firmware updates can be performed through the web interface of the camera.*

20 The Alarm System

The Alarm System consists of Action, Partition and Detector.

- **Action:** The lowest level of this hierarchy is the Action. An Action is a basic operation, for example: e-mail sending, application launch etc.
- **Partition:** You can manage your defined Actions into a Partition. A Partition is a group of Actions. So one alarm can trigger more actions.
- **Detector:** By assigning a Partition to a Detector you can make sure all your predefined Actions in the Partition will run if the Detector sends an Alert.

There are certain buttons that can be found in the header part of the above mentioned functions. Since these buttons have the same effect for these functions, they are discussed here.

- **Refresh:** Refreshes the page, showing every change that had happened since the last loading of the page.
- **Enable:** Enable the selected detectors, partitions or actions.
- **Disable:** Disable the selected detectors, partitions or actions.
- **Add:** Creates a detector, partition or action.
- **Modify:** Modifies an already existing detector, partition or action. To change a disabled item, first enable it.
- **Duplicate:** This button doesn't exist for detectors; its function is to create copy of an existing action or partition. The new duplicate is identical with the original, except it is disabled. Perfect and fast, if there is a need for a large number of nearly identical actions or partitions.
- **Delete:** Delete the selected detectors, partitions or actions.
- **Event filter:** After pressing the button a window appears in which you can configure event notifications. If you do not want to receive a certain type of notification, simply uncheck the checkbox next to the event type. This setting only affects the **Live video / Events** window. In the alarm system, Events can still be used for the creation of controls.

21 Actions

The Actions are basically triggered commands. These commands can be activated by embedding them into the Detectors, through Partitions. If the detector sends an alarm, the partition, and through it the action will be executed. This way the program will be able to react to any situation even better. There are several types of actions, executed by either the camera, the server. It could be even an internet action. These actions are:

| | |
|------------------------|---|
| Camera Action | Go to preset |
| Internet Action | Send E-mail |
| Server Action | ANPR database, Camera alarm state, Database, Launch program, Log events, Multi I/O, Partition arming, Storage group, VisiScanner database |

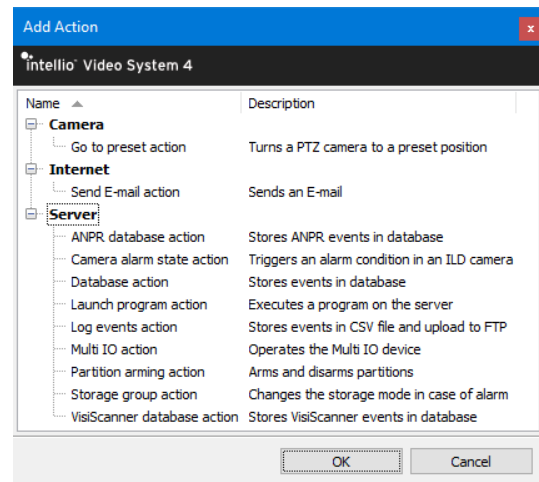
21.1 Creating Actions

To create an action, select **System Configuration / Alarm / Actions**, press button **Add** and select an action from the appearing window.

Every Action is different, but there are similarities in the build-up. A quick rundown for these:

21.1.1 General tab

A unique name, description and state can be assigned here for this action, which will be displayed on the list of the actions. Actions which are not authorized will not be performed.

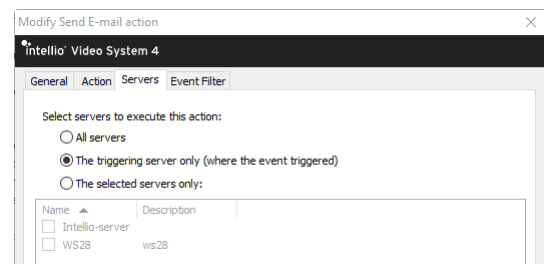


21.1.2 Action tab

The Action tab is different depending on the type of action that created it.

21.1.3 Servers tab

Depending on these settings, the Action will run on the specified servers. The naming is pretty obvious; you won't have a problem interpreting them (*This tab is missing from the **Camera Actions**, simply because there is no use of it in these cases*).



Possibilities:

- **All servers:** the action is run by all the servers. Use it carefully, because for example in case of a database action it may result in multiple insertion of data, or in email action multiple delivery!
- **The triggering server only:** the action is run by the server, on which the event was triggered.
- **The selected servers only:** the action is run only by the selected servers

21.1.4 Event Filter tab

In this tab you specify the event that triggers the action.

- **All events:** all the signal events will activate the action
- **Alarms only:** only the alarms signal will activate the action.
- **The selected events only:** only the selected events will activate the action.

21.2 Internet Actions

These actions will initiate a procedure that will be operating through the internet (*such as sends an E-mail*).

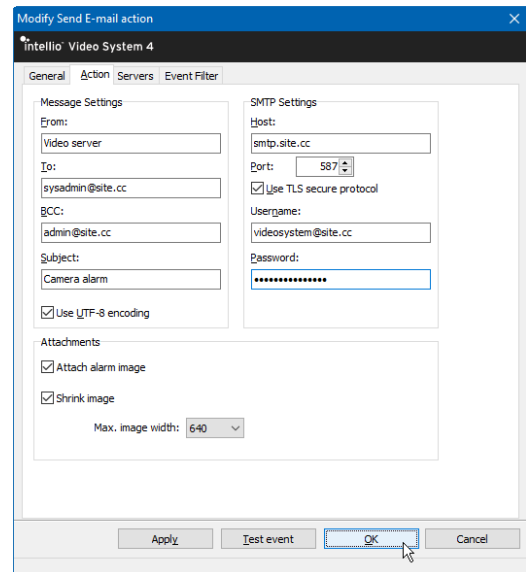
21.2.1 Send E-mail

This alarm will automatically send an e-mail to a pre-set account (*or accounts*) with a pre-defined subject (*preferably the type of the event that triggered the Action*). If there are multiple recipients, separate the given email addresses with a semicolon (;) in the **To** field.

The SMTP settings have to be configured: host, port number, possible secure TLS protocol, and of course the username and the password of the user account from which the message will be sent (eg: intellioserver@intellio.eu).

If the message comes from a camera, it is possible to attach an alarm image to the email. To attach the alarm image, check the **Attach alarm image** option, and by checking **Shrink image** option, the maximum width of the image can be set.

If the SITE contains more than one server, it is recommended to use the triggered server setting, preventing multiple deliveries, and to check whether or not all servers are capable of sending e-mails with these settings.



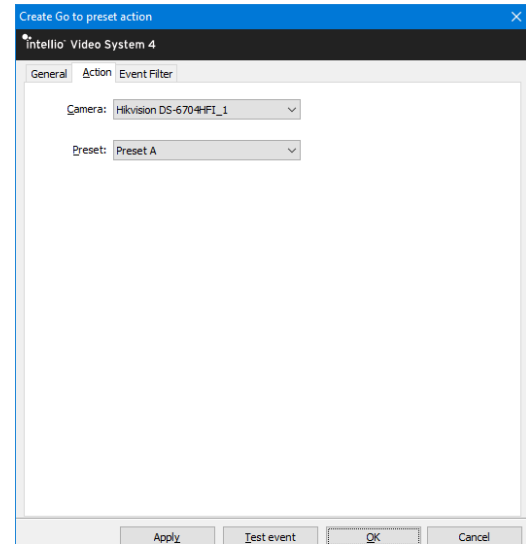
21.3 Camera Actions

The camera actions instruct the cameras to do something.

21.3.1 Go to Preset Action

This action turns a PTZ camera in a preset position.

The action tab of this Action first have to be selected the controlled PTZ camera, then the desired preset where the camera will turn.



Creating Presets

In order to save and load various important functions of PTZ cameras, follow the instructions below:

- Move the PTZ camera into the desired position.
- Select the third symbol from the camera menu, then the option **Create preset** under the presets displayed.
- Type in the name of the preset in the new window.

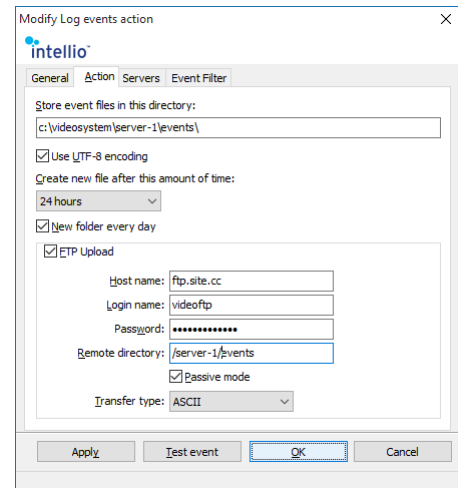
21.4 Server Actions

These actions run on the server (*or servers*), modifying its operation or creating new files on the hard drive. They can even operate other devices connected to the server.

21.4.1 Log Events Action

This action creates an Excel (*csv*) file and stores the alarm events what triggered the action in it (one line, one action, the data is separated by a semicolon (;)).

- **Store event files in this directory:** The location of the file created.
- **Use UTF-8 encoding:** Character coding type. Usually everything supports it, but if there are problems with the displayed data, do not enable it.
- **Create new file after this amount of time:** The time interval between creating a new file. It is suggested, that setting this interval consider, how often the action is supposed to make an entry in this log. If there are too many entries in the file, it can be confusing. It also can be confusing, if there are too many files.
- **New folder every day:** A solution for the previously mentioned 'too much file' problem.
- **FTP Upload:** Enabling this option the CSV file will be created or updated in the selected FTP server. Useful for backup.
- **Host name:** The name of the FTP server.
- **Login name** and **Password:** The login name and the password of the FTP server.
- **Remote directory:** The directory of the file (*or folder, if the New folder every day option is enabled*) in the FTP server.



Log events action configuration

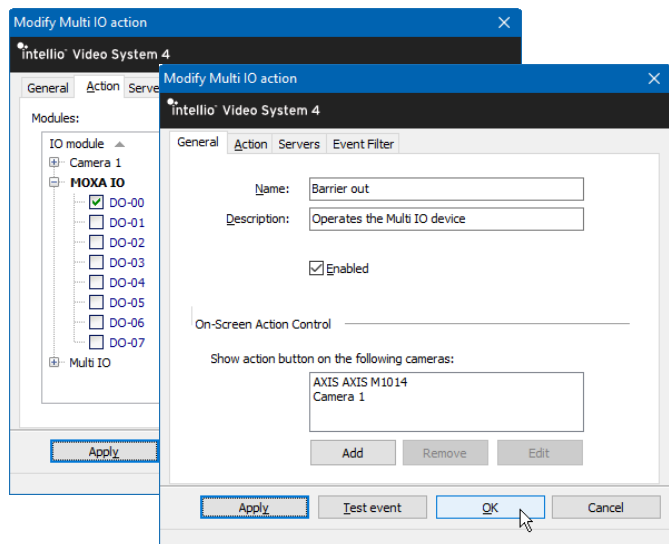
21.4.2 Camera Alarm State Action

This action overrides the reduced frame rate and the frame rate limit *settings* (*Camera encoder settings*) of a selected Intellio camera, enabling it to work to its maximum potential. The change is not permanent, if the Action will not get repeated, the temporarily overridden rules will return.

21.4.3 Multi IO Action

The Multi IO action operates a multi I/O device, and sends signals on the selected ports. If this action is executed the camera should give out a signal. E.g.: activate a relay. This tab also allows for sending a signal to the output port of an Intellio, Samsung or ONVIF camera and Modbus TCP device.

Important: this action can only be used to enable an output, therefore use this action only with monostable outputs.



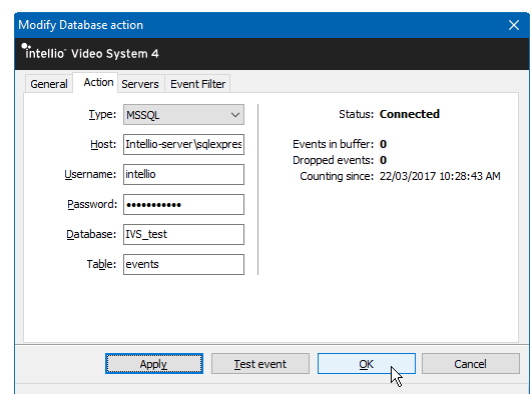
The list on the **On-Screen Action Control** part of interface can be used to associate cameras to the action. The action can be launched manually from the menu of the listed cameras. To add/remove cameras, use the appropriate buttons. Use the **Edit** button to set the order of the actions that can be launched from the selected camera menu.

If the action controls camera outputs, enable the execution of the action for all servers. The action will be performed by the server which is at that time connected to the camera, this way I/O controlling will work properly even in case of a camera take over.

21.4.4 Database Action

The process stores each event received by the server in an SQL database.

- **Type:** The type of the database. It can be *MySQL* or *MSSQL*.
- **Host:** The location of the database. It could be a web server or a specific directory on the network.
- **Username:** The user name for accessing the database.
- **Password:** The password belonging to a user name used for accessing the database.
- **Database:** The name of the database.
- **Table:** The table in the database storing the set data.



The required fields of the table are as follows:

These field names must be matching, otherwise the database process will not be able to store the necessary data.

Important: If the SITE contains more than one server, it is recommended to use the triggered server setting, this way multiple data insertion can be avoided. However, it has to be verified that all the servers can communicate with the database server!

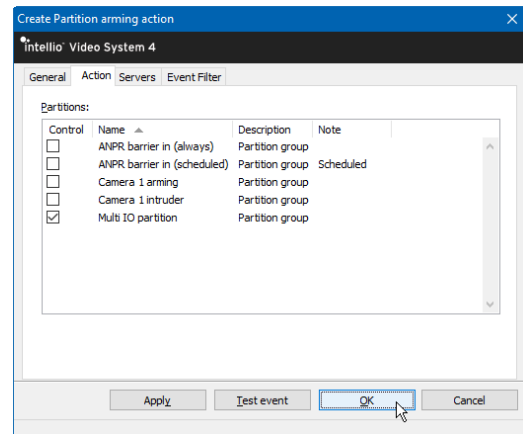
| Name | Type | Collation | Attributes | Null | Default |
|---------------|---------------|-------------------|------------|------|---------|
| DateTime | datetime | | | No | None |
| DetectorClass | varchar(50) | utf8_hungarian_ci | | Yes | NULL |
| Detector | varchar(255) | utf8_hungarian_ci | | No | None |
| Source | varchar(255) | utf8_hungarian_ci | | No | None |
| EventCode | int(4) | | | Yes | NULL |
| Message | varchar(4000) | utf8_hungarian_ci | | No | None |
| Gender | char(1) | utf8_hungarian_ci | | Yes | NULL |
| Age | int(4) | | | Yes | NULL |
| FrontalTime | float | | | Yes | NULL |

21.4.5 Partition Arming Action

This action activates a partition. It is possible, that there is more than one arming action activating the same partition. In this case the partition remains active until the partition arming actions signal, that the trigger event is over.

Note: the state of a partition can be changed by the user or the scheduler.

Note: in case of SITE with multiple servers, the proper way to run the action is **All servers**.



Partition arming action

21.4.6 Launch Program Action

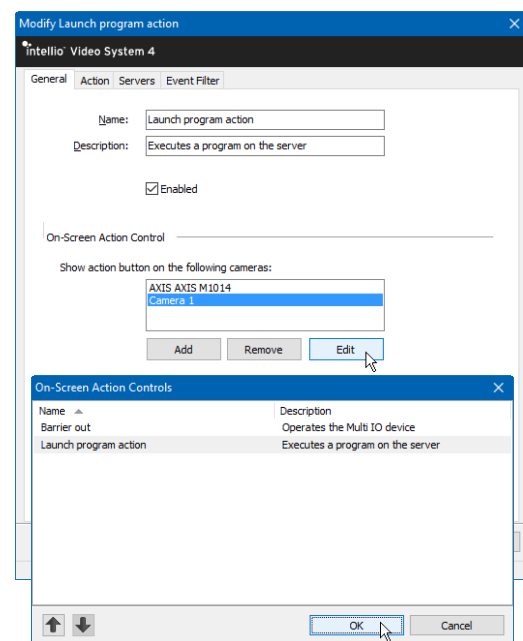
With this action a program can be started. This could be a batch file, or an ordinary program, such as the print (*print.exe*). The filename and the working directory fields are need to be filled also.

The list on the **On-Screen Action Controls** part of interface can be used to associate cameras to the action. The action can be launched manually from the menu of the listed cameras. To add/remove cameras, use the appropriate buttons. Use the **Edit** button to set the order of the actions that can be launched from the selected camera menu.

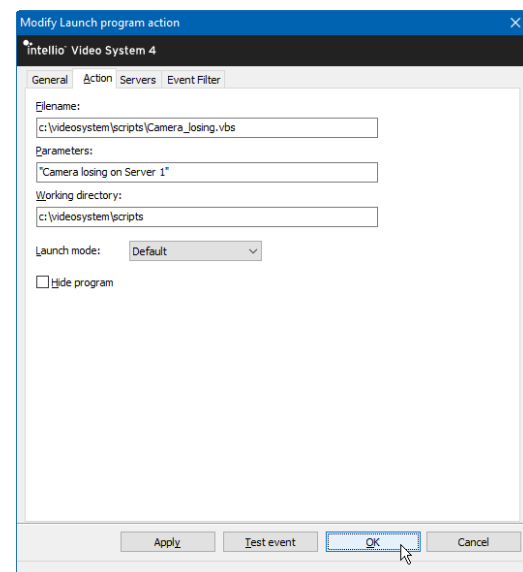
Parameters of the action:

- **Filename:** the name of the program to run.
- **Parameters:** Basically DOS command parameters. Not necessary for ordinary use, but can be useful (*adding parameters to a batch file, for example*).
- **Launch mode:** Quite useful, if we want something to do with the selected file, other than simply open it, for example important event logs can be printed out, or edited.
- **Hide program:** Means that the program will run in the background, and will not call attention for itself.

Note: if the action is performed by multiple servers, then the program must exist on all the selected servers, according to the given parameters.



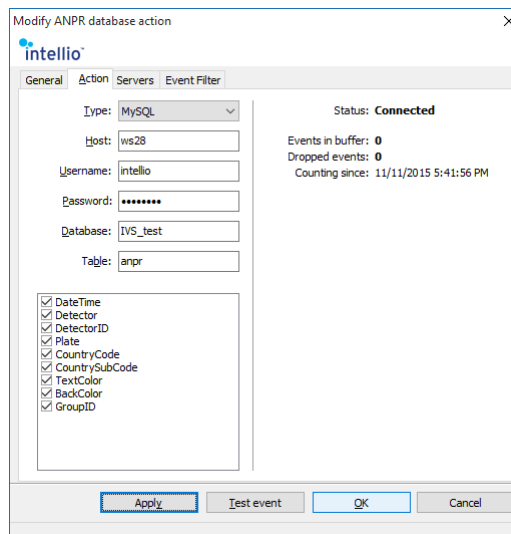
Action configuration



21.4.7 ANPR Database Action

The process stores in a database the license plate data detected by the license plate recognition detector and Built-in ANPR detector. At the start of the configuration, the information to be stored must be input cell by cell for later usage. The data to be input:

- **Type:** The type of the database. It can be *MySQL* or *MSSQL*.
- **Host:** The location of the database. It could be a web server or a specific directory on the network.
- **Username:** The user name for accessing the database.
- **Password:** The password belonging to a user name used for accessing the database.
- **Database:** The name of the database.
- **Table:** The table in the database storing the set data.



Users overview

| User | Host | Password | Global privileges | Grant | Action |
|-----------------------------------|-------------|----------|-------------------|-------|-------------------------|
| <input type="checkbox"/> Any | % | -- | USAGE | No | Edit Privileges Export |
| <input type="checkbox"/> Any | localhost | No | USAGE | No | Edit Privileges Export |
| <input type="checkbox"/> intellio | 10.10.0.128 | Yes | ALL PRIVILEGES | Yes | Edit Privileges Export |

The structure of the SQL database:

When creating the table, the field names must be the same as above!

The MySQL database has native support.

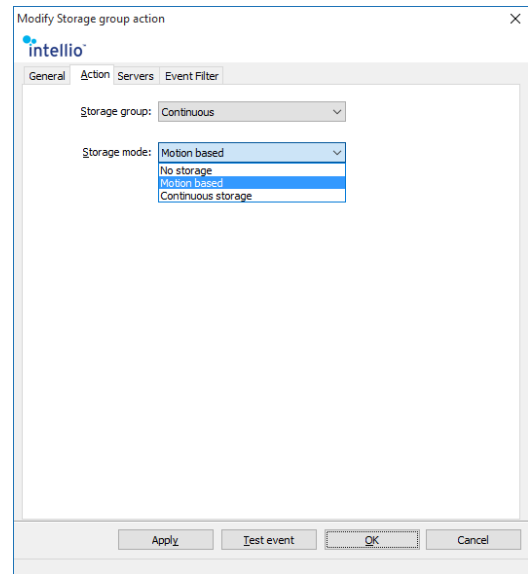
| Column Name | Data Type | Allow Nulls |
|----------------|--------------|-------------------------------------|
| DateTime | datetime | <input type="checkbox"/> |
| Detector | nvarchar(30) | <input checked="" type="checkbox"/> |
| DetectorID | nvarchar(38) | <input checked="" type="checkbox"/> |
| Plate | nvarchar(10) | <input checked="" type="checkbox"/> |
| CountryCode | nvarchar(3) | <input checked="" type="checkbox"/> |
| CountrySubCode | nvarchar(15) | <input checked="" type="checkbox"/> |
| TextColor | nvarchar(15) | <input checked="" type="checkbox"/> |
| BackColor | nvarchar(15) | <input checked="" type="checkbox"/> |
| GroupID | int | <input checked="" type="checkbox"/> |

Important: If the SITE contains more than one server, it is recommended to use the triggered server setting, this way multiple data insertion can be avoided. However, it has to be verified that all the servers can communicate with the database server!

21.4.8 Storage Group Action

This action alters the storage mode of a selected storage group. This change is not permanent, the cease of the detector alarm event what caused the activation of this action will result in the altered storage mode to return to its previous state.

- **Storage group:** The storage group what will be altered.
- **Storage mode:** The new storage mode of the selected storage group.

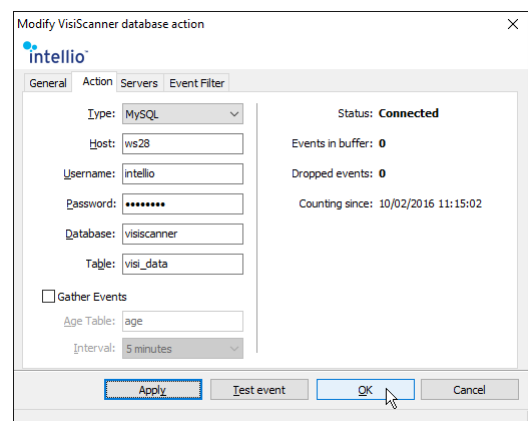


Storage group action

21.4.9 Visiscanner Database Action

It stores the events received from the VisiScanner detector in an SQL database.

- **Type:** The type of the database. It can be *MySQL*, *MSSQL2008*, or *MySQL*.
- **Host:** The location of the database. It could be a web server or a specific directory on the network.
- **Username:** The user name for accessing the database.
- **Password:** The password belonging to a user name used for accessing the database.
- **Database:** The name of the database.
- **Table:** The table in the database storing the set data.



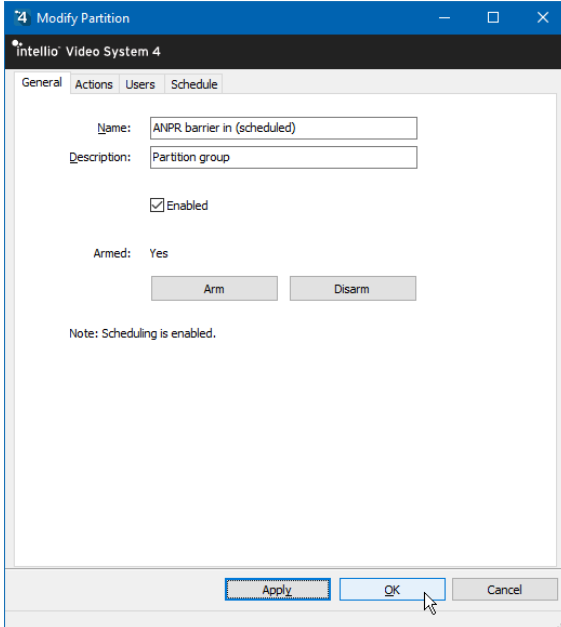
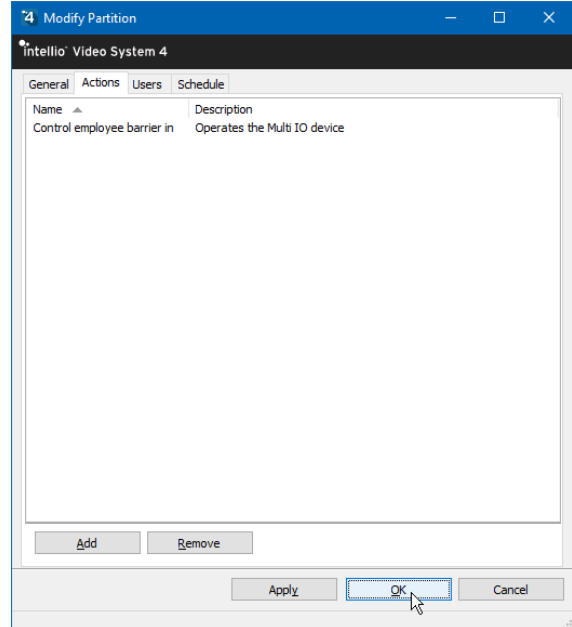
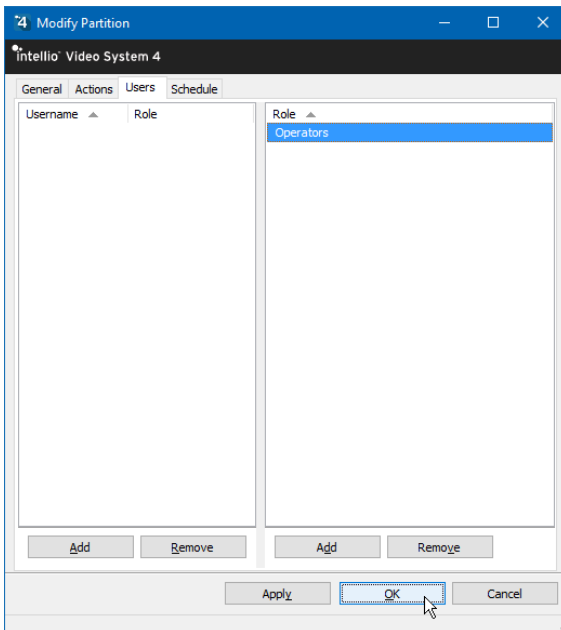
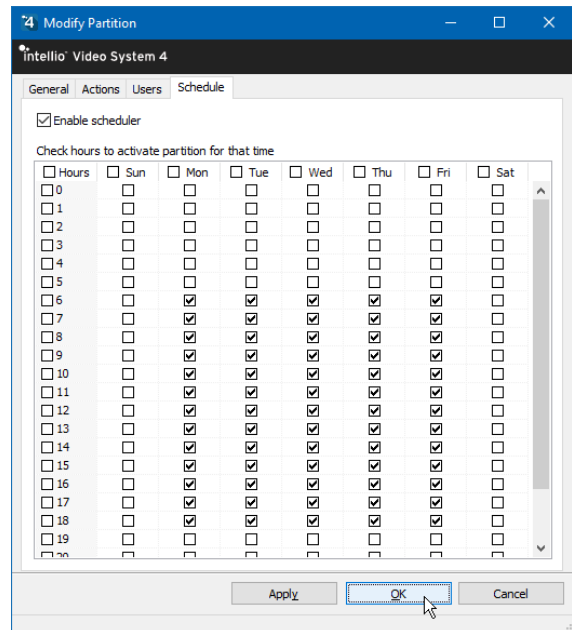
If you check in the **Gather Events** checkbox then also set these:

- **Age Table:** The table stores the arithmetic average of the age groups in the database, and the number of individuals of a specific age group during the set interval.
- **Interval:** The time period after which another summing up occurs.

Important: If the SITE contains more than one server, it is recommended to use the triggered server setting, this way multiple data insertion can be avoided. However, it has to be verified that all the servers can communicate with the database server!

22 Partitions

To create a partition, select **System Configuration / Alarm / Partition**, and press button **Add**. This opens up a window with four tabs, where the partition can be configured. These tabs are:

- General:** Here can be defined the name, description and the armed status. The disabled partitions will not launch the associated actions, and also will not notify users. The actual state of the partition is visible (*Armed: Yes/No*), and can be changed by the corresponding buttons (*Arm/Disarm*). The armed partitions launch the associated actions, and notify the users about the events. The state of partition is changeable in three kind of way:

- Manually: on the user interface using the partition list.
- By using a **Partition arming** action.
- By scheduler: according to the settings on **Schedule** page in the Modify Partition window.
- **Actions:** Existing actions can be added to the partition. The partition will execute every actions listed here, if the partition is called up, and the partition is armed at the time.
- **Users:** In this tab can be configured whether a certain user should get the events of the detector which activated the partition. If there are no users or roles defined, every user will get the event notification in **Live** mode.
 - Note:** *this behavior can be overridden in the detector settings. There may be users who are notified about events independently of the state of partition.*
- **Schedule:** Just select the days and hours of the time when the partition will be armed, in any other time the partition will be disarmed.
 - Note:** *the state of partition can be changed anytime by the user or an action.*

23 Detectors

Intelligent functions built into the Intellio cameras provide significant help to the operators and improves the efficiency of the monitoring staff. This built-in, distributed intelligence gives some level of automatism and autonomy to the video surveillance. Intellio's state of the art event detection and alerting method is a more complex procedure than today's usual ones. However you can keep it very simple to use for the operators with the help of the sophisticated configuration screens.

Prudential design is essential to establish an easy-to-use alarming method in the Intellio video surveillance system. This chapter drives you through the basic principles of the design and configuration of Intellio's event detection and alerting system. A few example of detectors:

| | |
|---------------------------|--|
| Onboard detectors: | Motion, Sabotage, Object removal, Entry, Tripwire, Direction, Intelligent motion, I/O input, Built-in ANPR detector |
| System detectors: | License plate, Multi I/O Input, Camera availability, ONVIF Event, SITE state, VisiScanner Analytics, TCP Event receiver, Video motion (<i>general</i>) |

23.1 Installing a Detector

Detector management is available in the client software and the installation process is the same for all detectors.

- Press the **Add** button on **System Configuration / Alarms / Detectors**, select **System** or **Onboard** detector type and press next.
- Select the camera you would like to add the detector to (*this step is sometimes missing from the system detectors*), then select the detector type.

Important: If the desired detector is not listed, it means that you either have a camera which is incapable of running that type of detector, or the Intellio System Software does not have the proper module software (e.g. LPR module)!

23.2 General Description of a Detector

Considering that every detector possesses a lot of similarities, and their primary functions are the same (*drawing attention on a certain kind of behavior on the monitored area or in the system*), during the installation we can encounter a lot of repetitive steps. These steps are described here for the easier perspicuity and probably give a comprehensive idea of the detectors.

23.2.1 Detector Types

There are several types of *detectors* (*Sabotage, Motion, Object based, Tracker based, I/O input, Traffic and System*) based on the scope of the detector, or place of function. These categories help us to find a specific detector, but during configuration the difference among them are slim to none. There are three categories that must be distinguished; these are the **Tracker based**, the **System** and everything else. The main difference between the System detectors and the others is that the **System** detectors work on the server and won't strain the camera processor, but requires bigger network capacity.

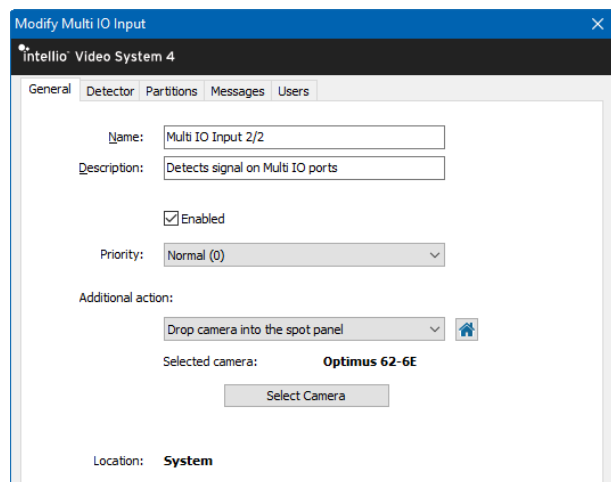
23.2.2 Tracker Based Detectors

The only reason the tracker based detectors are a different category is that for these detectors (*Entry, Tripwire, Direction and Intelligent motion*) to work properly — or sometimes at all —, we have to configure the **tracker** and **calibrate** the camera.

23.2.3 The Frame of a Detector

Every detector has four tab, these are:

- **General:** The detector name, description and location can be found here. The camera name and the description are generic, so we strongly suggest to change them, so it can be identified even among several other detectors, even if it is the same kind (*useful to display here somewhere the name of the camera where the detector located, avoiding the confusion later on*). There is a **Priority** drop down list here, wherewith the detector alarms can



be prioritized. A low priority alarm will not appear in the spot, if there is a higher priority alarm in effect. A more prioritized alarm can interrupt a lower one, displaying it on the spot monitor. Click on **Additional action** to adjust a different camera than the default one to be displayed in case of alarms (*e.g. if a sensor connected to the I/O input of a camera is relevant to an area monitored by another camera*). Besides, you can set to change to a complete view with multiple cameras to be displayed concurrently for a particular alarm.

- **Detector:** The mask of the detector and the unique settings can be configured in this tab. There are detectors, where this tab does not exist, due to the lack of necessary settings; which means this tab is unnecessary.
- **Partitions:** Here can be added the partitions that will be activated as soon as an alarm event arrives from this detector. There can be more than one partition here, but these partitions will only react to normal alarm events. Technical alarms or any kind of non-alarm events will not activate the partitions listed here.
- **Important:** If all the partitions linked to a detector are inactive, no events and alarms will be transmitted to the client! If a detector needs to be running at all times, it is recommended to add an always active partition containing no actions to the partitions linked to the detector.
- **Messages:** It can be set here whether a certain type of event arriving from this detector is considered alarm event, or not. It is also possible to import or export the messages settings from here. With the help of this possibility becomes easier to archive your settings, or import them into a lot of cameras.
- **Users:** On this tab it can be set which users and/or roles will be notified about detector events.
 - **Users defined at PARTITION (default):** In this case, only those will get the event messages who are listed in the related partitions.
 - **Partition with INCLUDING the selected users:** same as the list in the default settings, but listed users and roles are added to the list.
 - **Partition but EXCLUDING the selected users:** same as the list in the default settings, but the listed users and roles are taken away from the list.
 - **The SELECTED users only (empty list means nobody):** only the users and roles listed will be notified about the detector events. An empty list means nobody will be get messages.
 - **All users EXCEPT the selected ones (empty list means all users):** All users will be notified about detector events, except the users and roles listed here. An empty list means everybody will get messages.

23.2.4 Creating Masks

Creating a mask can only be done on a camera preview. This can be found in the second, **Detector** tab.

There are three kinds of masks in the detectors, where masks are available: The first one creates polygons, the second one creates straight lines and the third one creates a longer, continuous line. It might be a misnomer to call the lines this way due the lack of an actual mask (*in this case we create lines*), but in this case the mask is a term we use to visually created rules.

Polygons

About half the detectors have this masking mode.

To select a polygon click on the selected corner with the mouse and move around the object by clicking on the neighboring corner. The corners of the polygon can be moved later, but removing or adding corners is not possible. To do that, erase the polygon and redraw it. Steps of the drawing:

- Click with the **left mouse button** in the starting point.
- Move to the next corner of the polygon, then click again with the **left mouse button**.
- Repeat this process until all of the corners have been selected, then click on the **right mouse button**.



Example for a polygon type mask

You can drag the whole polygon by clicking on the green area anywhere.

You can create several polygons. The detector will function according to its definition within the selected area.

The Motion detector and the two monitoring sensor (*Monitoring, Recording*) can handle several masks. In this case, each mask can contain polygons with each mask applying different rules.

Straight Lines

The second way to create masks, or in this case lines is to press the **left mouse button** on one end of the line, move the mouse to the other end point, then release it. With this method you can create a lot of lines.



Example for a straight lines type mask

Continuous Line

Click on the end point of the line then use the **left mouse button** on the next point. This could be either an end point, or a breaking point. It depends on whether we want to continue it or not. If we do, then select the next breaking point and click with the **left mouse button**. Continue this until the end point, where use the left click, then the **right mouse button**, signaling that there will be no more point of the line.

To modify a created mask, just click on it. If a mask is alterable, the corners (*break points*) become blue, and in the middle of the mask a red dot will appear (*in case of polygons*).

Make the necessary adjustment by clicking on a corner or breaking point with the **left click** and dragging it to the proper position.

Moving an edge or line is also possible, just click on it, and drag.

To delete a mask or line, select it to become active then click on the **Delete Mask** or **Delete Line** button.



Example for a continuous line type mask

23.2.5 Calibrating the Camera

Calibration is an essential step to calculate the real spatial distances and the sizes of objects in the images captured by the cameras. Based on this information the camera can decide in the whole perspective whether the object is a vehicle, human, small object, or something it cannot identify or insert into these categories.

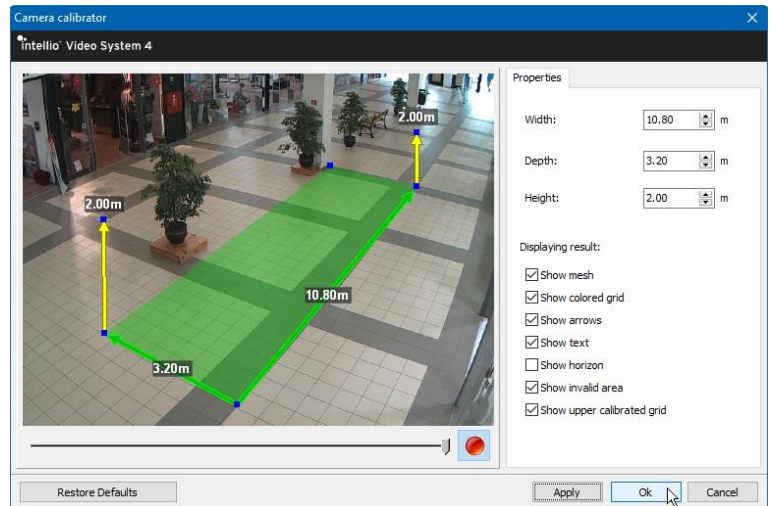
The calibration is done one by one, every camera has to be calibrated separately (*considering that two cameras rarely have the same field of view from the same perspective, this method seems unambiguous*). The steps are the following:

- Select **System Configuration / Devices / Cameras**.
- Select the camera which will be calibrated.
- Click on the **Calibrate** tab and push the **Calibrate Camera** button.

On the preview window you have to set the direction and the length of the *coordinates* (*it is not an easy process, but do it carefully; you only have to do it once, and a good calibration means higher precision in the detectors*). A more precise setting resulting in more effective detector operation. The process is hard to explain, so just a few pointer:

- Use the **left mouse button** to start the settings of the directions, and keep pressing it while doing the direction and length calibration
- Be careful that the end points of the directions are not leaving the preview field area (*it would still work, but you can't calibrate the direction if you can't grab the end point*)
- During the calibration try to use existing objects or distinctions of the field to help the precision of the calibration; it will not be always available, but where it is, it helps significantly
- Try to use long directions; these will help to minimize the errors of the calibration (*10 cm mistake is not the same in case the direction arrow is one meter in length, or ten meters*)
- The directions have to be set according to reality; what seems to be at right angles in the camera view, is not necessary right
- The direction arrows have to be at the right angles (*90° to each other*)

After the calibration click on **Apply**. With the help of the **Displaying result** check the effect of the calibration (*the better the results, the smaller the invalid areas are smaller and the upper calibrated grid is touching the end point of the two yellow arrows*). If the results are satisfactory (*probably it will never be perfect*), click **Ok**.



23.2.6 Configuring the Tracker

Configuring the tracker means setting up rules concerning the moving objects. These rules helps to track object movements, identify objects according their size, set up filters to disregard movements that are the result of shadows or moving leaves in the breeze, or defining whether two objects are the same or not. These settings are quite important, and each camera has to be configured differently according the placement and the field of view.

The next three parameters define the term of the tracking. All of them have to come true for a moving object to become tracked:

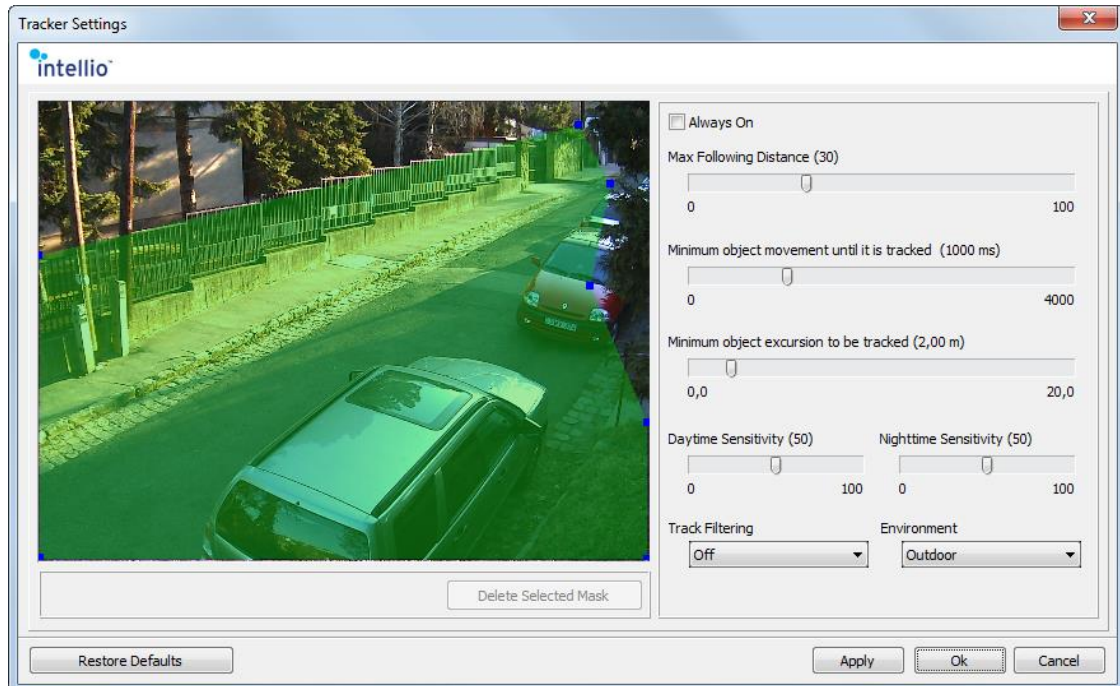
- The movement time of the object before it become tracked
- The excursion of the object before it become tracked
- Max following distance

If any one of these requirements is not met, the object will not be tracked, and the detectors will not react to them. It is important to set these parameters according to not lose any important event.

To configure the tracker of a camera, follow these steps:

- Select **System Configuration / Devices / Cameras**.
- Select the camera which will be configured.
- Click on the **Tracker** tab and push the **Configure Tracker** button.

In the case of ILD VISUS cameras, only the mask has to be set (*if the tracker is not needed within the whole field of view*), whereas in the case of ILD ORIO cameras the following parameters can be used to set the tracker:



Configure tracker panel

- **Always On:** By enabling this checkbox the tracker will work all the time, not just if it is necessary for the working of a detector.
- **Max Following Distance:** The maximum distance from the object. If in two following image the excursion of the object is within this range, it will be tracked as the same object. If the object is outside of this range, it will be considered a new object, and get a new identification.
- **Minimum object movement until it is tracked:** The minimum amount of time before the object becomes tracked.
- **Minimum object excursion to be tracked:** The minimum required excursion of the object to be become tracked.
- **Daytime Sensitivity:** With this can be set the daytime sensitivity of the trackers. At low sensitivity there is low probability of the false alarm events, but it can cause missing alarms too. At the other side of the scale it will be highly sensitive, but will generate quite a lot of false alarm. This sensitivity works only during the time the camera is on day mode.
- **Nighttime Sensitivity:** Same as Daytime Sensitivity, but works in night mode.
- **Track Filtering:** This drop down list set the strength of the filtering, which means that with **Strict** settings the camera will compare the movement directions to a lot of statistical data to decide whether the movement is a real moving object, or just a tracking error. We suggest to not turn on the filtering because although it filters out the false alarms, can result in filtering out real events too.
- **Environment:** This drop down list takes over the job of most of the setting options placed in the ILC cameras, using the predefined environmental settings on the selected locations.

23.3 Onboard Detectors

23.3.1 Sabotage Detector

The sabotage detector detects the turning and covering of the camera, or the blurring of the image.

Note: This detector can only be added to cameras in the **VISUS** series.

Onboard; Mask type: none

The detector can detect any circumstances affecting the image quality, while it only sends an alarm in predefined cases. The detector is capable of ignoring the following circumstances:

- **Image is too dark:** The detector does not send an alarm if the image is too dark.
- **Image is too bright:** The detector does not send an alarm if the image is too bright.
- **Out of focus:** The detector ignores blurry, unfocused images.
- **Redirected:** The detector does not send an alarm if the area under surveillance drastically alters.

The detector only sends an alarm after the **Violation Time** is over, in order to avoid sending false alarms. The alarm will be over as soon as the **Restore Delay Time** is up.

If you aren't familiar with the general process of the detector installment, you can learn about it here: [General Description of a Detector](#) (page 88).

23.3.2 Motion Detector

Motion detector alerts if there is motion sensed in the masked area.

Onboard; Mask type: polygons

To this detector several masks can be added and each mask can be set to different parameters. The parameters of the detector can be fine-tuned:

- The **Sensitivity** defines how low the threshold limit of small changes is in the background the value.
- The **Motion Percent** defines a percent of the selected area, where if there is a change between the image, it is considered alerted.

Pressing the **Apply** button the detector initializes and starts working. From this point the detector sends Alerts to the system.



Motion Detector

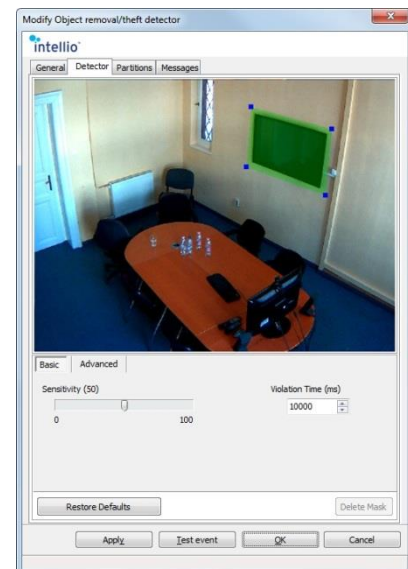
23.3.3 Object Removal/Theft Detector

Theft Detection is useful to protect objects. It is able to send alarm if protected objects are removed or stolen from their original place.

Onboard; Mask type: polygons

Make sure when setting the detector that the mask covers not only the protected object but some of its surroundings, too, which should contrast to some level with the object itself for easier detection (*in an ideal case, a dark object in a white background*). It largely enhances the efficiency of the detector.

In the detector configuration there is a difference between ILC and ILD cameras.



ILD

- **Sensitivity:** The higher the sensitivity, the smaller change will cause an alarm event. It also means that too high sensitivity will be more likely to cause false alarms. Too low sensitivity, on the other hand, will not alert even if the protected object is stolen.
- **Violation Time:** The delay period between the alarm event and the point in time when the protected object disappeared. If during this time the object is restored, the alarm event will not happen.

23.3.4 Covering Detector

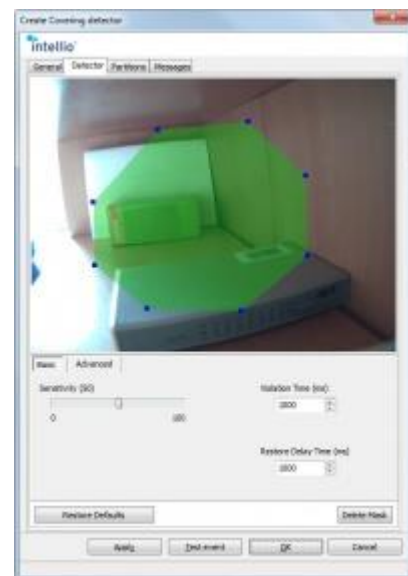
The Covering detector is a sabotage detector: it alerts if the camera's field of view becomes limited.

Note: This detector can only be added to cameras in the **ORIO** series.

Onboard; Mask type: polygons

The Covering detector watches the masked area (or the whole FOV, if there is no mask created), and alerts if there is something obscuring it (box in front of the camera, baseball cap ...etc.). Since the detector works in the principle of contrast monitoring, it become too dark for the camera, it will shut down with a message called *"Unable to operate in low light"*. This could also happen if the lens of the camera is painted over, so this message can indicate serious problems.

- **Sensitivity:** It sets how sensitive the detector is to the changes of the masked area. With higher value it is easier to set an alarm off.
- **Violation Time:** The time between the alarm event and the point when the covering happened. If during this time the FOV restored, the alarm event will not happen.
- **Restore Delay Time:** The time before the detector sends the restored event message in case the restoration is only temporary. With this it can be stopped the repeated alarm event.



Covering detector settings

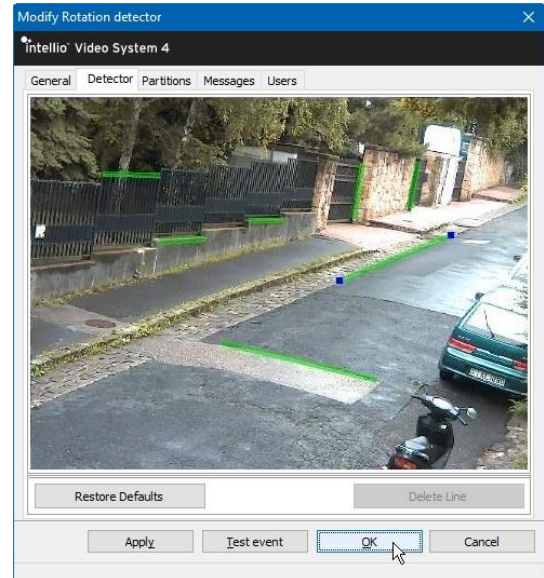
23.3.5 Rotation Detector

Rotation detector is a sabotage detector. It alerts if the camera is turned or removed from its original fixed position.

Note: This detector can only be added to cameras in the **ORIO** series.

Onboard; Mask type: single lines

During the setting of the lines make sure that the lines, or edges have contrast in every time of the day. The bigger the contrast, the better this detector will work. The control lines supposed to be seen all the times, and the more lines we can set, the better. After the lines are set, click on **Apply**, then wait for the lines to turn from red to green. If this doesn't happen in a few seconds, then that particular line is quite possibly wrong, because it can't find an edge. Since these lines will define the stationary area to which the camera will compare, do not set them along possibly moving objects, such as cars, crates, etc.



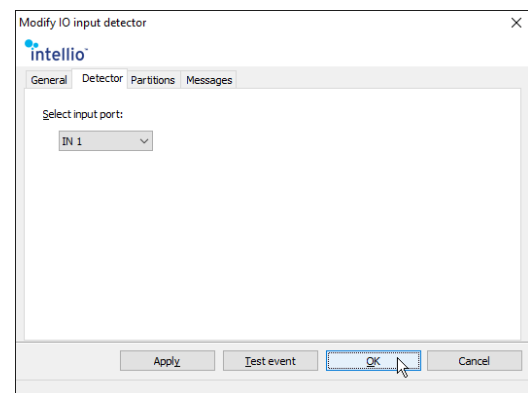
23.3.6 IO Input Detector

The I/O Input Detector generates an alert if a signal arrives on the Intellio camera's input port or if the incoming data stream ceases.

The camera input can be configured in the **System Configuration / Devices** page on the **I/O ports** tab.

Onboard

The only thing that has to be configured in this detector is the port that it watches. Because you do not need to analyze the images, there is no need for a mask.



IO Input detector settings

23.3.7 Built-in ANPR Detector

Onboard; Mask type: polygons

The Built-in ANPR detector was developed to support recognition of Hungarian license plates, primarily for access control purposes (*e.g. barrier control*). The detector must recognize a license plate twice in a row otherwise it will not send it to the server as an event. It is recommended to enable the camera OSD during configuration.

- **Plate size (in pixels):** Minimum and Maximum values. Number plates are not recognized if lower than minimum and higher than maximum size.
- **Direction filter:** With the help of this feature the license plates of unwanted cars entering or leaving can be filtered. However, if there are not any cars like this, the feature can be disabled.
- **Mask:** One polygon mask can be configured, which can be used to limit the license plate searching in the covered area.

The Built-in ANPR detector does not recognize colors and it also removes hyphens. As a result, number plates with colors and / or hyphens will not be properly assigned to a license plate group. If you want to use the Built-in ANPR detector, input the number plates without colors and hyphens.

23.4 Tracker Based Onboard Detectors

Traffic detector, Entry detector, Intelligent Motion detector, Tripwire detector and Direction detector are tracker based, which means the foundation of these detectors are categorizing and memorizing the movement of the moving objects.

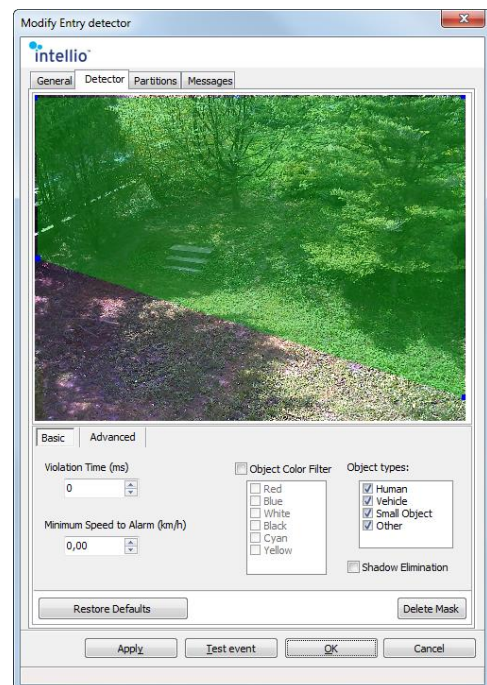
To set these detectors first you have to calibrate the camera and configure the tracker.

23.4.1 Entry Detector

The Entry Detector alerts if a tracked object enters into the protected area. It does not alert for objects moving inside the protected area or for objects moving outside the protected area. It also does not alert for objects leaving it.

Tracker based, Onboard; Mask type: polygons

- **Violation Time**: If the tracked object leaves the protected area before the set time is up, the alarm event will not happen.
- **Minimum Speed to Alarm***: If the tracked object's speed is below this, the alarm event is not happening, even if the object is entering the protected area.
- **Object color Filter***: When enabling, the detector will alert if the tracked object's base color is one of the selected color (*or a mix of them*).
- **Shadow Elimination***: The detector will try to determine whether the object entering the area is a shadow or not.
- **Object types***: The camera will send alarm if one of the selected object types enters into the protected area. For e.g. if the Human type is selected and a Vehicle enters into the area it will be ignored and so on.



ILD entry detector settings

*: the object filtering options can vary depending on camera type and firmware version.

On the ILC cameras the settings is different, there is an option for whether the detector disable itself in low lighting conditions, and the object type filter.

23.4.2 Direction Detector

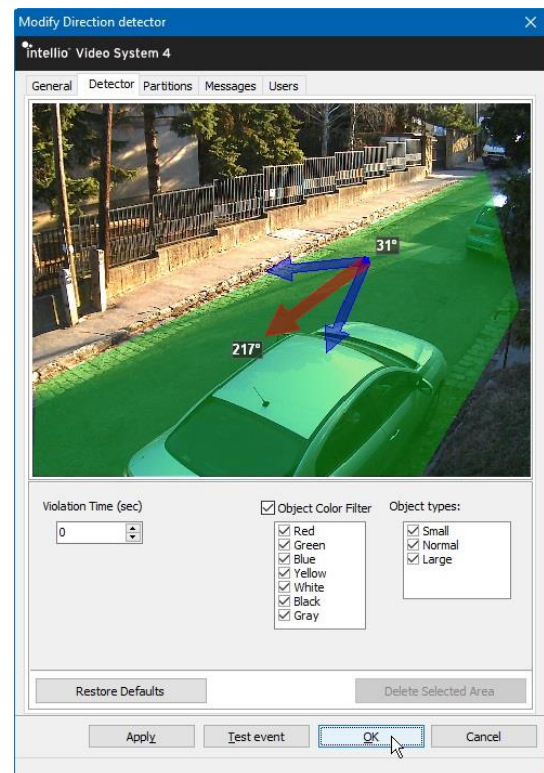
The Direction Detector's main function is to alert if an object moves to the wrong direction in the masked area. This can be useful in monitoring one-way traffic for example.

Tracker based, Onboard; Mask type: polygons

During the masking there is only one polygon can be set. The forbidden direction can be set with the help of the arrows appearing on the preview display. This "trident" can be dragged by pressing the left mouse button on base of the arrows. The forbidden direction can be set by rotating the "trident" to that way (*the red arrow shows the wrong direction*) by dragging the arrowhead. The two blue aide arrows show the tolerance. If the angle is low, the detector will only alert, if the moving object's track is almost exactly in line with the forbidden direction. With high angle, the detector alert more often. The highest angle is 90°, which means that the detector will alert even if the moving object's track is normal to the forbidden direction.

- **Violation Time:** The time between the alarm event and the point when the protected object disappeared. If during this time the object is restored, the alarm event will not happen.
- **Object color Filter*:** When enabling, the detector will alert if the tracked object's base color is one of the selected color (*or a mix of them*).
- **Shadow Elimination*:** The detector will try to determine whether the object entering the area is a shadow or not.
- **Object types*:** The camera will send an alarm if one of the selected object types is moving in the prohibited direction. For e.g. if the Human type is selected and a Vehicle enters into the area it will be ignored and so on.

*: the object filtering options can vary depending on camera type and firmware version.



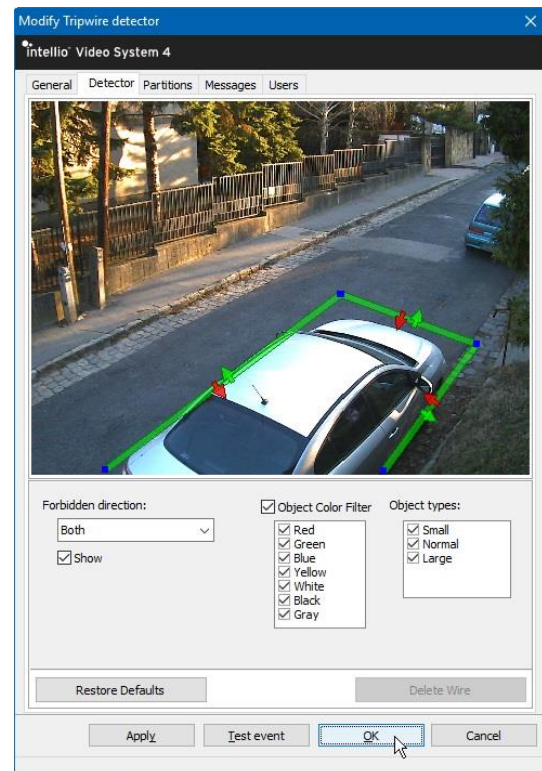
23.4.3 Tripwire Detector

The Tripwire Detector alerts if the defined line is crossed from the forbidden direction.

Tracker based, Onboard; Mask type: single line

Before setting up the tripwire, make a plan based on the defended perimeter's layout. Consider the possibility of the crossing of the line from both ways, and set the forbidden direction accordingly. The Tripwire will alert at every crossing if it comes from the forbidden direction.

- **Forbidden direction:** This drop down list contains the forbidden directions. This can be **Left to right**, **Right to left**, or **Both**. The left and right side depends on the order of the set break points, for example if the first end point of the tripwire is in the top of the image, and the next is on the bottom, the left side will be right side of the image. If an object crosses the tripwire from the wrong side, it alerts.
- **Show:** This checkbox helps the settings by showing the forbidden directions. With the help of this it is easy to see the directions of the crossings.
- **Object Color Filter*:** When enabling, the detector will alert if the tracked object's base color is one of the selected color (*or a mix of them*).
- **Shadow Elimination*:** The detector will try to determine whether the object entering the area is a shadow or not.
- **Object types*:** The camera will send alarm if the tracked object is one of the selected object types.



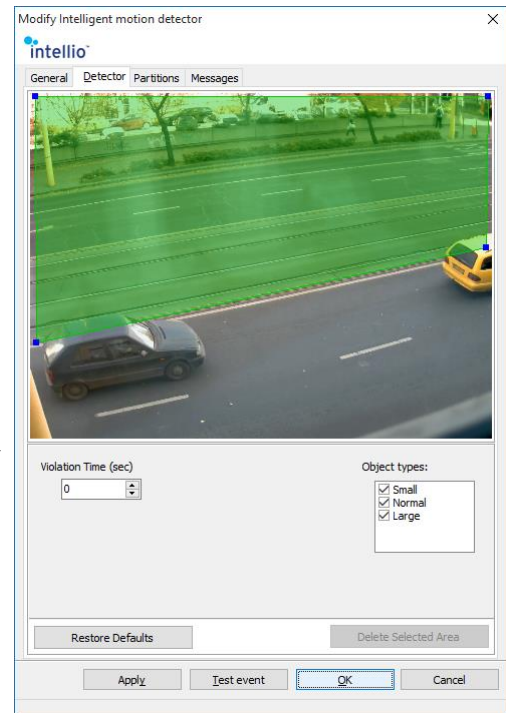
*: the object filtering options can vary depending on camera type and firmware version.

23.4.4 Intelligent Motion Detector

The Intelligent Motion Detector detects motion, the same as the Motion Detector, but the Intelligent Motion tracker based, so it is able to differentiate between different sizes, able to detect movement speed, etc. It is useful in an outdoor environment, where the constant movement of the vegetation would result in a constant alarm with an ordinary Motion Detector

Tracker based, Onboard; Mask type: polygons

- **Violation Time:** The time between sensing movement and the alarm event. If the movement stops during the masked area during this time, the alarm will not sound.
- **Minimum Speed to Alarm*:** If the tracked object's speed is below this, the alarm event is not happening, even if the object is moving in the selected area.
- **Object Color Filter*:** When enabling, the detector will alert if the tracked object's base color is one of the selected color (*or a mix of them*).
- **Shadow Elimination*:** The detector will try to determine whether the object entering the area is a shadow or not.
- **Object types*:** The camera will send alarm if the tracked object is one of the selected object types.



Intelligent Motion detector settings

*: the object filtering options can vary depending on camera type and firmware version.

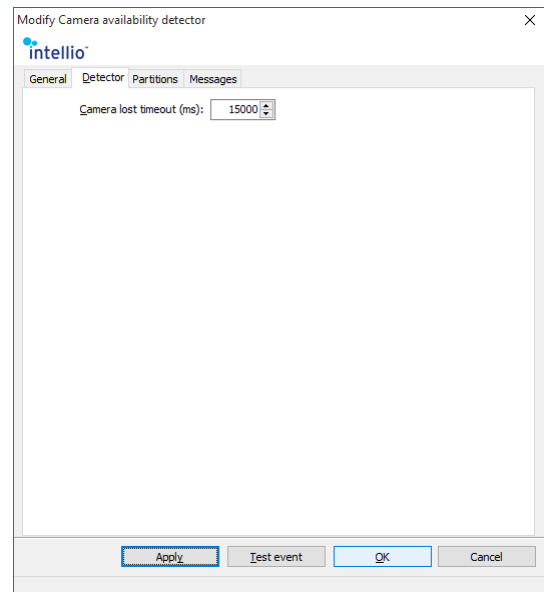
23.5 System Detectors

23.5.1 Camera Availability Detector

This detector alert if a registered camera became unavailable due to any reason (*power failure, camera breakdown, vandalism, etc...*). The alarm does not know the cause of the lost connection. The detector is also notifies the operator about the available cameras, and signal if every camera is available.

There is only one settings for this detector

- **Camera lost timeout:** This is in default is set to one minute (*60 000 ms*), define the time after if the camera is not answering to the server, it will sent an alarm signal.



23.5.2 Site State Detector

The SITE State detector monitors the servers of the SITE. This detector does not have any special settings; its function is automatic so it lacks the detector tab. If a server is disconnected from the SITE, the other servers in that SITE will send an alarm, notifying the operator.

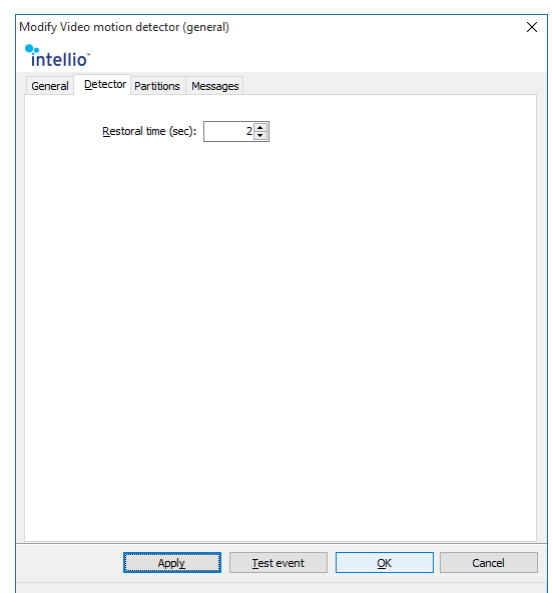
The detector also notifies if a connection between two servers is built. Since in the SITE there could be multiple servers, it easily could mean several messages, since each server signals the new connections, both the new one and the old ones.

With the help of the "SITE state detector" a possible server error can be detected early on a multi-server SITE. Due to the system's redundant operation, the operators, depending on settings, will not notice a shorter server downtime. However, with the detector, the system administrator will still be notified of these events.

23.5.3 Video Motion Detector

This detector transforms the signals of the camera's storage motion detector to events. The events recorded can be used in the future to perform various actions in the alert system.

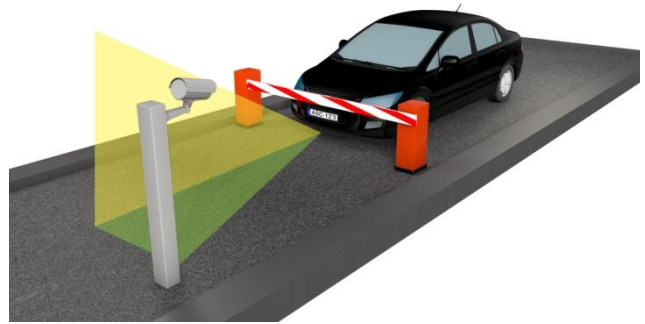
Restoral time: The amount of time the detector will wait before sending a restore signal. If there are a lot of people moving in the field of view, this time is recommended to set low. If the probability of a single moving object to pause from time to time, but otherwise there is rarely any movement in the area, set this value higher to avoid the repeated alarm events.



23.5.4 License Plate Detector

The license plate detector is done by a Windows system based program called Carmen FreeFlow.

The detector tab is absent, the settings for the recognition properties need to be configured at the camera which the detector is assigned to. To read more on the recognition settings, refer to the subsection on [Configure License Plate Recognition](#) (page 111).



23.5.5 VisiScanner Analytics

The VisiScanner Analytics is a complex highly accurate gender and age recognition detector which gives an estimate on the gender and age of the detected person based on recognizable and measurable characteristics. This detector is not applicable to screen these people real time, but excellent for statistical purposes.

There are a few setting option in this detector:

- **Search levels:** This defines the size of the faces the detector will recognize, or even search. The size in pixel can be known by moving the mouse pointer above the *i* symbol. Please note, the smaller (and farther) the searched face, the more time this application will require, and also the far away faces are less likely to give an accurate result given the limited number of pixels it can base its calculations.
- **Path selection:** The direction of the passing people.
- **Show frontal time in event:** This option allows for displaying among the event logs the time period for which the individual monitored was looking directly toward the camera (and thus, contributed to more reliable results).

Please contact our support for further information through [ATSS](#) about configuring this detector (<http://arh.hu/index.php/en/support.html>).

23.5.6 TCP Event Receiver

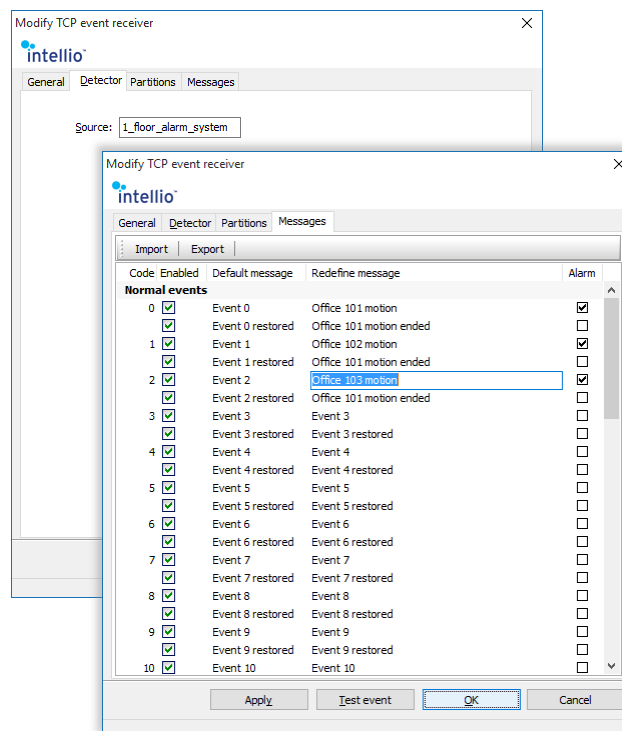
The TCP Event receiver is a listening detector. If a preset string arrives from an external source at the default port (**53541**) with an event code, the detector sends an event signal to the operator. The event messages can be different depending on the arriving event code.

It is possible to display a message on the live view of the camera sent through the detector.

To the detector to work properly, it has to set.

- **Source:** A string has to be entered here. This string will be the one the detector will look for in the source of the arriving messages.

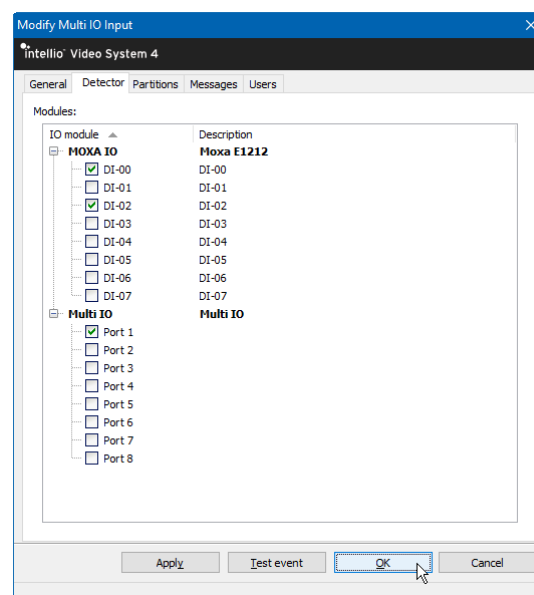
The exact format of the TCP message can be learned from the *IVS4 TCPEventReceiver ENG.pdf* document.



23.5.7 Multi IO Input Detector

The Multi I/O Input detector also a listening detector, but while the TCP Event Receiver watches a specific string on the TCP port, the Multi I/O Input will alert, if there is any activity on the selected ports. To this detector to work properly, you need at least one [Multi I/Os](#) (page 107) or [Adding Modbus TCP I/O Devices](#) (page 27).

There is only one thing that has to be set and that is the ports that will be watched over. One detector can watch a multiple number of Multi I/O devices.

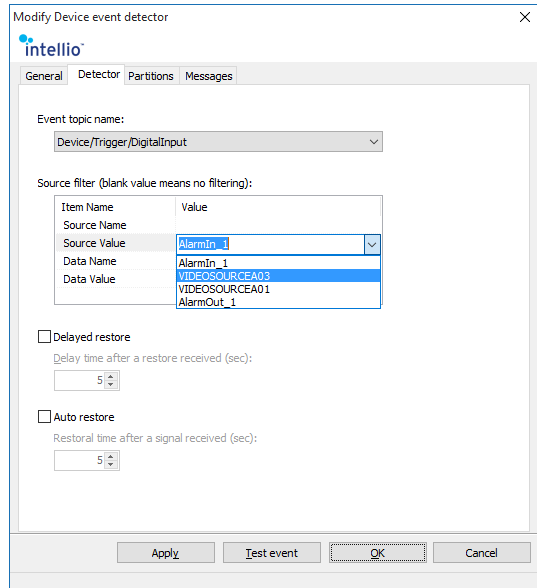


23.5.8 Device Event Detector (ONVIF, Samsung)

It sends a signal if the monitored ONVIF or Samsung camera detects the specific event.

For the detector to work the event monitored on the ONVIF or Samsung camera has to be selected from the available list.

- **Delayed restore:** The time span set defines the period after which the detector returns to normal mode.
- **Auto restore:** The time period after the start of an alarm event after which the detector returns to normal mode. The detector may be active for the whole period without repeated alert signals (*e.g. continuous motion in the field of view*), so it is recommended to set a high value.
- **Source filter:** Enables the filtering of the alarm event by source and data on the server's side. The detector will only signal the server if the events match the configured values. Empty fields are not filtered.



24 Hidden Detectors

Hidden detectors help to create a more effective system. Usually the user does not have to do anything with hidden detectors. Hidden detectors are created automatically by the system. Hidden detectors can be configured the same way as normal detectors; their signals can be used in the alarm systems. The hidden detectors can be found in the **System Configuration / Alarm / Detectors** page under the **Hidden** group

24.1 Built-in Intelligent Motion Detector

The hidden built-in intelligent motion detector supports the "Smart playback" feature of the system. With the help of this detector, the user can use the "Smart playback" feature even if no intelligent motion detector was created. The built-in intelligent motion detector can only be removed if the corresponding camera has been already removed.

24.2 Hidden PTZ Preset Detector

The Hidden PTZ preset detector is needed to support preset playback. The PTZ preset detector is created automatically for each and every created preset (*they cannot be created manually*). By deleting a preset, the corresponding PTZ preset detector is also deleted. If a PTZ camera is removed, all the related PTZ preset detector are also deleted.

25 Virtual Detectors

The Virtual Detectors are used, when we need to find a specific action in the past, which did not get caught by the existing detectors. In this case we create a virtual detector which covers the area in question (*for example, a tripwire in front of the window where the robber came in*). It doesn't matter that the detector has been added after the event, for this is the purpose of these detectors.

Virtual detectors can be created on the **Intelligent Motion Search** interface, and under the **System Configuration / Alarm / Virtual Detectors** menu. Virtual detectors are subject to the *IVS-SPB* license. The creatable detectors on the ILD cameras are the tracker based detectors and the motion detector, on the ONVIF cameras only the motion detector, if the camera uses server-side motion detector (*it cannot be created on cameras with onboard motion detectors*). These are the only ones where virtual detectors can be created. With the help of these detectors a certain event in the past is easily and quickly retrievable. They work the same way normal detectors do, aside from that these work on the recorded footage.

The selected time period will be examined by the detector and thumbnails will be displayed for events triggering an alarm. The search can be performed by selecting the virtual detector and running a query for the selected time period (*Virtual detectors can also be queried on the **Event Query** interface, where the available detectors are displayed in italic font for the sake of easier identification*).

Important: The tracker based virtual detectors only yield results in case the **Tracker** had been working in the selected period and the motion data was stored along with the images! With the ONVIF cameras they have to use **server-side motion detection**.

26 Accessories

26.1 Multi I/Os

A Multi I/O is a unique device that can be connected to the server's RS-232 port. It has 8 independent inputs and 8 independent relay outputs. The number of Multi I/O devices that can be connected to a server is only limited by the number of RS-232 ports on the server.

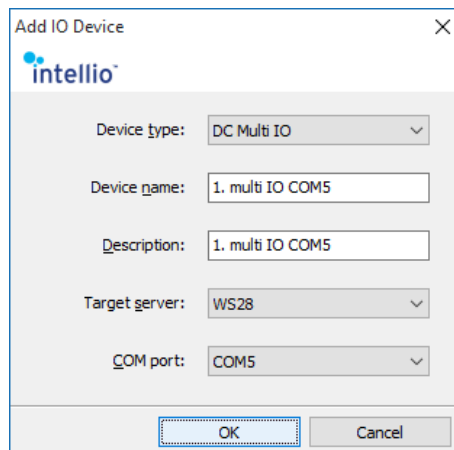
26.1.1 Specification

You can see the pin out of the Multi I/O device on the figure. The power plug is a standard 12V DC plug. On the left side of the device there are 8, 24V 1A relay outputs, on the right, you can find the inputs. The jumpers can be found between the normal and relay outputs. With the help of the jumpers you can either set the relays to NO or NC. If the jumper is on the upper pins then the output is NO, if it is not, then it is NC.



26.1.2 Setup

- Add a Multi I/O port by pressing the **System Configuration / Accessories/ Multi IOs / Add** button.
- In the **Add IO Device** window, add the **Device name** and **Description**.
- In the **Target server** drop down list select the server where the Multi I/O is connected and will be operational.
- In the **COM port** drop down list select the COM port where the Multi I/O is connected.
- Press **OK**.
- Switch to the **Outputs** tab and enable the ports needed.
- Add a **Description**. Select the **Output signal** type. By selecting **Impulse** the Multi I/O will provide an impulse for the **Output** impulse interval in milliseconds.
- Press **Apply** button.



Add IO Device

intellio™

Device type: DC Multi IO

Device name: 1. multi IO COM5

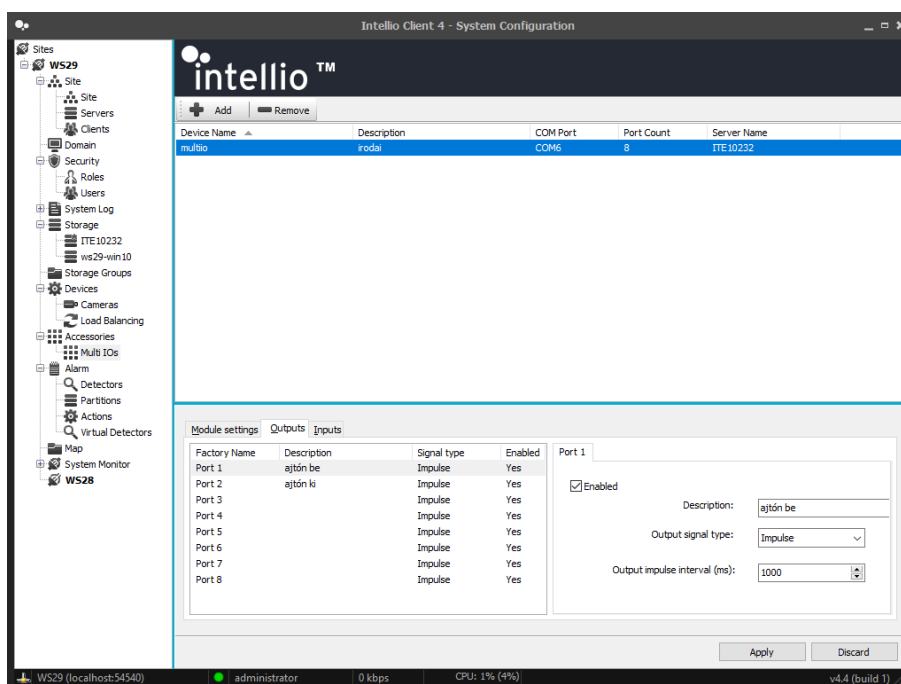
Description: 1. multi IO COM5

Target server: WS28

COM port: COM5

OK Cancel

After the Multi I/O device is configured, the Multi IO Input detector can be added (*is this case a server restart may be needed*).



Intellio Client 4 - System Configuration

intellio™

Device Name Description COM Port Port Count Server Name

| Device Name | Description | COM Port | Port Count | Server Name |
|-------------|-------------|----------|------------|-------------|
| multio | irodal | COM6 | 8 | ITE10232 |

Module settings Outputs Inputs

| Factory Name | Description | Signal type | Enabled |
|--------------|-------------|-------------|---------|
| Port 1 | ajtón be | Impulse | Yes |
| Port 2 | ajtón ki | Impulse | Yes |
| Port 3 | | Impulse | Yes |
| Port 4 | | Impulse | Yes |
| Port 5 | | Impulse | Yes |
| Port 6 | | Impulse | Yes |
| Port 7 | | Impulse | Yes |
| Port 8 | | Impulse | Yes |

Port 1

☒ Enabled

Description: ajtón be

Output signal type: Impulse

Output impulse interval (ms): 1000

Apply Discard

WS29 (localhost:54540) administrator 0 kbps CPU: 1% (4%) v4.4 (build 1)

27 ANPR

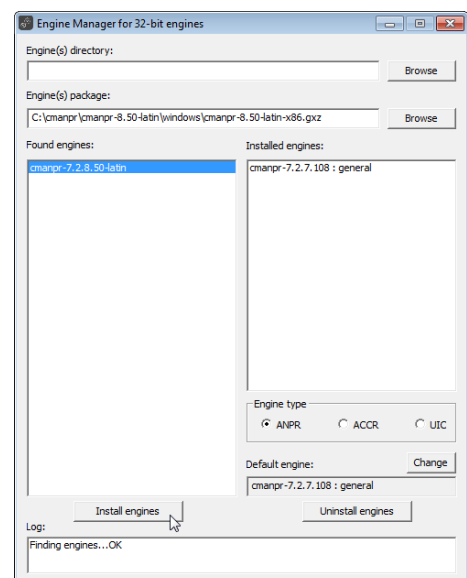
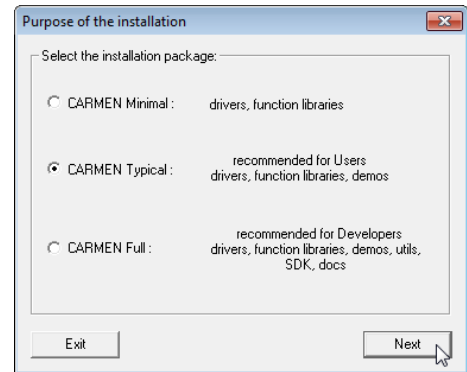
27.1 The Carmen FreeFlow Engine

If you are using Intellio server computers and you have ordered an ANPR license, then Intellio technicians should have already installed the ANPR USB key and the ANPR engine on your server. The only thing you have to do is to install the camera properly.

27.1.1 Installation of Carmen FreeFlow

If a version of Carmen FreeFlow earlier than 7.2.7-22 had already been installed, it is recommended to uninstall it before installing the new version.

- Shut down the Intellio Video Watchdog service on the server.
- Shut down the Intellio Video Server service on the server.
- Plug the ANPR hardware key into a free USB slot on the server.
- Start the **setup.exe** file, from the downloaded SETUP folder.
- After accepting the end user license agreement, select the **CARMEN Typical** option. Clicking on **Next** will start the installation.
- From this point forward the installation is automatic. Depending on the operating system (32 / 64 bit) Carmen will automatically install the appropriate version. On a 64 bit OS's both 32 and 64 bit versions will be installed.
 - After installation has completed, if there is an update for the search engine, start the **CARMEN GX / 32 bit version / Engine manager** application from the start menu and install the update!
 - Enter the location of the downloaded engine file in the **Engine(s) package** field.
 - The engines found in the file are displayed on the left list.
 - Select the engines you want to install, and click on the **Install engines** button.
 - The installed engines are displayed on the right list. To change the default engine, select the engine you want to use by default and click on the **Change** button. By clicking on **Uninstall engine** the old engines can be removed (*only do this after you made sure that the new one is working reliably*).
- If you want to confirm that the engine is working, start the **CARMEN GX / 32 bit version / ANPR Demo for Images (32-bit)** application from start menu. If the license plate that appears is recognized properly by the program, then the installation was successful.

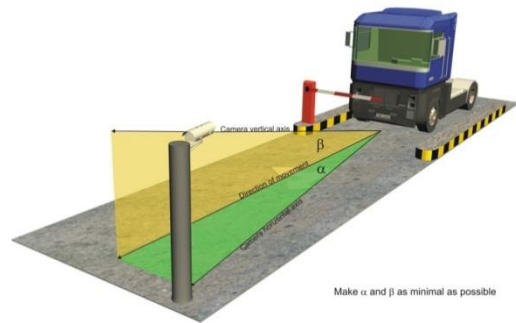


- Launch the Intellio Video Watchdog service (*the Intellio Video Server service will be started automatically by Watchdog service*).

Install FreeFlow on each of the servers of the SITE, which have hardware key, and make sure to install the same version of the program on all of them to avoid potential version conflicts.

27.2 Camera Positioning and Adjustment

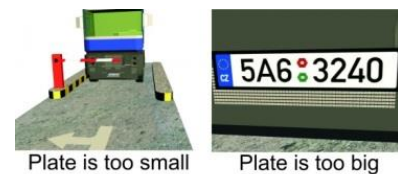
The accuracy and speed of license plate recognition depends largely on the position of the camera. The camera should ideally be positioned so as to directly face oncoming vehicles in a way that the angle of the camera axis and the axis of the vehicle's direction is as small as possible.



An additional factor in terms of accuracy and speed is the distance between the camera and the license plate. If the camera is too far away, the characters of the license plate will be too small resulting in low resolutions. If the camera is too close, the characters will be oversized.

The most significant factor influencing the efficiency of license plate recognition is the size of the characters in the image.

- In case of Latin characters it is recommended to adjust the camera in a way that license plate numbers will be 20 pixels tall on average (*min. 16*).
- In case of Arabic characters it is recommended to adjust the camera in a way that license plate numbers will be 30 pixels tall on average (*min. 20*).



Optimal size

To measure pixel parameters you can use any of the popular image editors, such as Paint or IrfanView (<http://www.irfanview.com/>).

In order to further increase the accuracy of the results, license plate numbers should be:

- high resolution,
- sharp,
- highly contrasted,
- and visible amidst normal lighting conditions.



A good example: the characters are 20 pixels tall and brightly lit.

27.3 Video Adjustment for ANPR

In case of license plate recognition it is crucial to use the proper video settings. Under normal circumstances license plate recognition must work in both day- and nighttime conditions and amidst changing light conditions. We recommend the following default settings, which of course, may be altered to suit unique needs:

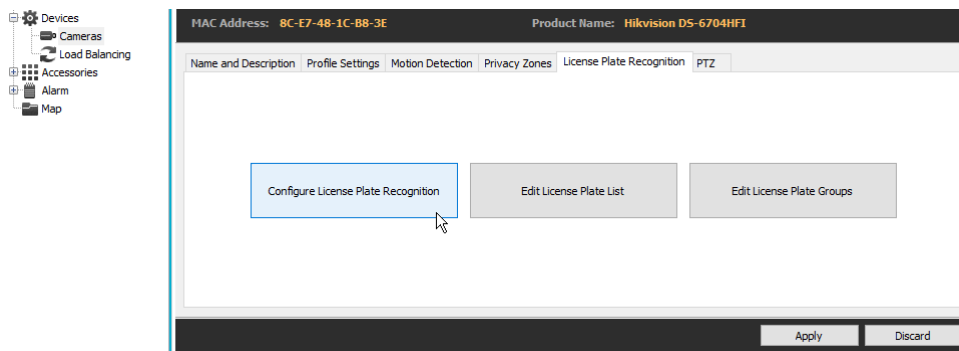
- The **Iris** should be always open.
- **Flashing removal** on the **Exposure** tab should be turned on.
- The maximum exposure on the **Exposure** tab should not exceed 1/500.

27.4 License Plate Recognition

Instead of the interface of the [License Plate Detector](#) (page 104), license plate recognition can be adjusted on the **License Plate Recognition** tab of the camera in charge of detection (**System Configuration / Cameras / License Plate Recognition** on the selected camera).

To read more about the querying of recognized license plates, refer to the chapter entitled **Event querying / License plate** in the *User's Manual*.

There are three buttons on the **License Plate Recognition** tab, whose settings and functions are as follows...



27.4.1 Configure License Plate Recognition

There are four tabs, along with the camera image, on the window that pops up after pressing the button. A mask can be created on the image, after which license plates will be detected only in the selected area. It is recommended to limit the searching area as much as possible, thus facilitating recognition.

Basic

On the default **Basic** tab we can authorize license plate recognition for a specific camera.

Important: The number plate scan will run only those images on which the motion detector of the camera (*recording*) signals motion!

- **Accept only consecutive hit number:** This is the value that indicates how many images of a license plate is needed for safe recognition by the program. The higher the

value, the slower the detection will be, but at the same time, the more accurate it will become.

- **Limit recognition frequency:** Limits the number of images the engine should scan for license plates within 1 second. The **Limit recognition frequency** is time based, so for example setting to 5 fps, the time between the images which are given to the engine will be at least 200 ms (*milliseconds*). If the camera works exactly 5 fps, but the time between the images is sometimes less than 200ms, then the image will be dropped (*omit from the ANPR process*). If the camera works with low fps, and it is expected to run ANPR process on all the images, turn off the **Limit recognition frequency**, or set it a bit higher than the camera fps. Please note that it is recommended to enable **Limit recognition frequency** even if the camera works with low fps, to prevent the malfunction of ANPR process (*increasing delay time*), if the camera fps is increased later.
- **Select engine:** Here can be selected the used ANPR engine. The engine which recognizes country codes, and thus displaying them in the events cannot recognize the colors of the license plates, and gives less rapid detection compared to a general recognition engine. If that is an issue, use another engine instead.
- **Enable color recognition:** Authorize it to allow the system to recognize the background and caption color of license plates, which is needed in case of certain Arabic countries where the color can distinguish between two identical license plate numbers. The **Color identification based on database** sub function is based on the color database of the search engine, and it tends to yield better results, but it may yield false values if the database is not prepared for certain colors.
- **Include separator into the license plates:** This is just a tool to make the license plate easier to read visually, and does not influence recognition. The separator can be selected as preferred.

Advanced

- **Image scale down size to use:** The image size used for recognition. The smaller this image, the faster the engine works, but the results could also be worse.
- **Timeout:** If the speed of the recognition is beyond the set time, the event will not be displayed.
Note: the engine tries to finish the ANPR process within the set time period, however sometimes runs out of it, so the maximum recognition time displayed on the statistics page can be higher than this value.
Note: The engine with the country code detection algorithm requires the default values to be increased to around 500 ms. It is recommended to set the value in accordance with the number of cameras and the Limit Speed property.
- **Minimum confidence to accept:** While detecting characters the search engine considers only the results that are recognizable or reliable to a reasonable degree, meaning a high level of similarity between the characters to those stored in its own database. This is in order to filter out erroneous results, but it may also increase the accuracy in the license plates recognized. The value can be decreased to 30% in case the reliability of license plates recognized is low.
- **Plate size (in pixels):** Average, minimum, and maximum values. Number plates are not recognized if lower than minimum and higher than maximum size. The size must be set according to the original image size. On OSD layers (*detector, LPR*) the sizes are

always displayed according to the original image size, even if the ANPR process works with halved or quartered images.

- **Number of characters:** The minimum and maximum character count of the recognized license plates. If a license plate comprises more characters than the maximum value, the engine will not recognize it as a license plate.
- **Filter identical license plates for the given period of time:** It helps to avoid the same license plate to be counted multiple times.

Direction detection and filtering

Detects direction of movement of the vehicle (*moving away and getting closer*).

- **Disabled:** Disables the direction detecton.
- **Basic:** Depends on the size change of characters on the license plate. Fast but less accurate. To use this function, you need to set **Accept only consecutive hit number** greater than 1 (*for more reliable direction detection, set it to 3-4*). Compares the 1st and Nth (*where N is the setting value*) detected character size to figure out the direction.
- **Advanced:** More accurate but causes high latency. You can decrease this latency by lowering the **Maximum latency**. Select the approximate 2D direction vector of the vehicle which is getting closer towards the camera in the camera image between the three arrows. Direction detection depends on the license plate's position change. Requires position change to be confident enough or expiry of the Maximum latency, otherwise no license plate will be recognised.

Direction filtering: When direction detected, use this to filter out vehicles' license plate events moving to a given direction (*moving away or getting closer*).

Statistics

The **Statistics** tab contains the statistical information from calculations done by the engine, such as maximum and average waiting time, number of recognitions, timeouts and resets.

The statistics values are reset after each modification (**Apply / Ok**).

27.4.2 Control of Functioning ANPR Process

There are three sources, which can be used to check the functioning of ANPR process, and help to change the settings.

- ANPR statistics values of the camera.
- Information of LPR OSD layer of the camera.
- OSD information of the ANPR detector of the camera

Statistics values

Recognized plates (*unfiltered*): XXXX

Count of the all recognized number plates.

| | |
|---|---|
| Recognition | |
| Count: XXXX | Count of the images on which the ANPR process has run. |
| Time (<i>min/max/avg</i>):XX/ XXX / XX ms | Minimum, maximum, and average times of the recognition. |
| Timed out XX | Count of the interrupted recognition because of timeout. |
| Character size | |
| Size (<i>min/max/avg</i>):x / x / x px | Minimum, maximum, and average sizes of the recognized number plates.. |
| Delay | |
| Time (<i>max/avg</i>):xxx / xxx ms | Minimum, maximum, and average values of the delay time. |
| Drop Counts | |
| By low confidence: x | Count of the dropped number plates because of low confidence. |

Delay time

The delay time means the entire processing time of the image (*decoding, waiting for CARMEN, recognition, etc.*). If delay time exceeds the 3000 ms, the newest images will be dropped, until the delay goes below 3000 ms. The ANPR process will not run on dropped images, and these images will not contain LPR OSD layer. The appropriate settings of ANPR process keep the delay time continuously low level (*100-300 ms*), it can be increased periodically for short time, but stays below 3000 ms.

Note: in practice the ANPR process on the server side needs to decode all the camera images. In case of high resolution cameras which work high fps, the entire ANPR process can be too long, prevent the efficient ANPR process. For this camera it is advised to decrease the camera FPS instead of or next to enabled **Limit speed** option.

Information of LPR OSD layer

| | |
|--|---|
| RUN | ANPR scan has run on the frame, the next lines contain the result. |
| Skipped by FPS limit, last result: | The frame will be omitted from ANPR process, because FPS limit. |
| DROP! Reason: Plate position | ANPR scan has run on the frame, but the result is dropped because of number plate position. There must be one character space between the edge of ANPR area and the number plate (<i>according to the recognized character size</i>). |
| LPR DROP! Reason: Timeout(> XXX) | Engine has not found number plate on the frame during the set time, so it is dropped. |
| LPR DROP! Reason: Engine is busy (<i>since XXX ms</i>) | Frame is dropped, because engine still processes previous image. It can occur, if engine does not finish the image processing during the set time, so the next image is dropped. Between parentheses time since engine is busy. |
| Plate: ABCxyz (XX) | The found number plate, confidence value between parentheses. |
| Country: HUN | In case of engine with country code, the recognized country code. |
| CharSize: xx; RecogTime: xxx; Delay: xxx | Character size, recognition time, delay time. |

27.4.3 Edit License Plate List

Certain license plates can be grouped, with separate alert settings for each. The license plate list can be imported and exported, so it is not necessary to type these in. There are filters available to filter license plates and groups.

One license plate can be a part of multiple groups at a time: when the license plate is recognized, the corresponding detector event is triggered in every license plate group (*however more filters can be configured at the detectors*).

If you set up a limitation period, the license plate will be automatically deleted from the group after this time has passed.

The license plates entered are case-sensitive, so every entry has to be entered in capital letters.

In terms of the SITE, the license plate list is global. This list can be edited on each camera's **License Plate Recognition** page with the help of the **License Plate List** button.

The **Edit groups** button opens the **Edit License Plate Groups**.

27.4.4 Edit License Plate Groups

License plates can be divided into groups with differing rules, e.g. vehicles with license plates on the white list are automatically allowed through the barrier, while the ones on the black list trigger an alarm. (*This requires a [Multi IO Input Detector](#) (page 105) in the system, a [License Plate Detector](#) (page 104) and the [Multi IO Action](#) (page 82) to control the barrier*).

License plate groups and their corresponding colors can be easily created, altered or deleted. Please note that deleting a group will not entail the deletion of its containing license plates from the license plate list.

In terms of the SITE, the list of the license plate groups is global. This list can be edited on each camera's **License Plate Recognition** page with the help of the **License Plate Groups** button.

27.4.5 Manual Entry

Automatic license plate recognition may produce false or no outcomes at all in particular problem cases. In such instances the operator can enter the correct license plate number manually, which is going to trigger a "manual entry" event for such license plates in the detector. The alarm system can handle these events in the same way as other events.







The **Manual Entry** function is accessible in **Live** video mode from the camera menu by authorized personnel.

28 Map

If you want to use the map feature, then all the SITE's servers must have an IVS-MAP license. In the map, you can overview every cameras of every SITE and look at them from an aerial viewpoint.

For navigating on the Map, use the mouse. Moving in the directions is done by the left mouse key, rotating by the right mouse key. By using the mouse wheel, it can be zoomed in, or out.

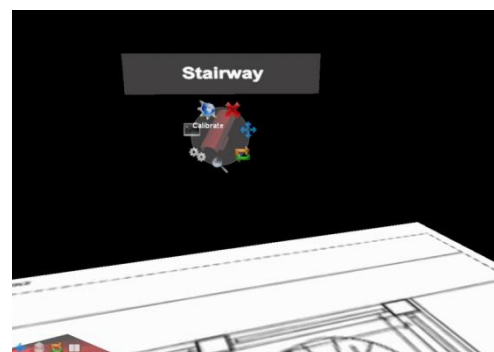
There are four buttons in the Map, these are:

-  **Back:** This function takes back one level, "zooms out". The help of this function there is possible to switch levels of a building, or take a look at the outer area of a building. It is also possible to switch locations.
-  **Change View:** Switches between the axonometric and the "over the top" view type.
-  **Switch Images:** Changes the background picture to one of the other. If there is only one picture added to a location or a level, this function has no effect.
-  **Show/Hide Captions:** With this button the names of the cameras, buildings and locations can be displayed, or hide.

Every object on the map has its own menu. This appears only if you move the mouse above the object (*it should become red*), then click with the right mouse key. From this menu several object-related actions can be reached, like **Delete**, **Move**, **Rotate**, **Scale** and **Properties**. If the selected object is a camera, there are a few other options available too, namely **Video Adjustment** and **Calibrate**. If the selected object is a floor, there are only two options, the **Delete** and the **Properties**, since the other ones make no sense considering the type of object.

Description of the options:

- **Delete:** This option erase the camera from the map
- **Move:** By clicking on this, the camera placement can be changed (*e.g. to the other side of the room*)
- **Rotate:** The camera, and with it the FOV can be rotated (*e.g. if we move the camera to the other side of the room, it is unlikely to face it to the wall – if it is not facing down*)
- **Scale:** Strictly cosmetic feature, the displayed camera size can be changed



- **Properties:** It brings up the same window as the **Add Camera** or the **Add Detector** button
- **Video Adjustment:** It brings up the **Set Video Adjustment** window
- **Calibrate:** Configure the camera's field of view on the map. Use the **Hint** button for further help.

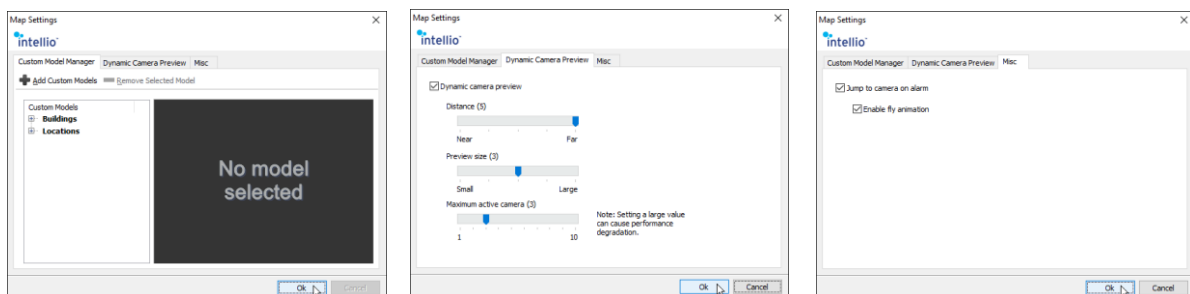
28.1 Map Settings

It is important to mention this part of the map, since there are visual components depending on these settings.

Custom Model Manager: In this tab, you can add your own custom models to the default ones. Of course, you can also remove a model. *(About the custom models please contact our support specialist for further information through [ATSS http://arh.hu/index.php/en/support.html](http://arh.hu/index.php/en/support.html))*

Dynamic Camera Preview: By enabling this option, above every camera in a certain distance appears its live image with low FPS. The distance, the size of the image and the cameras showing these images can all be set. This function can cause performance degradation in older computers.

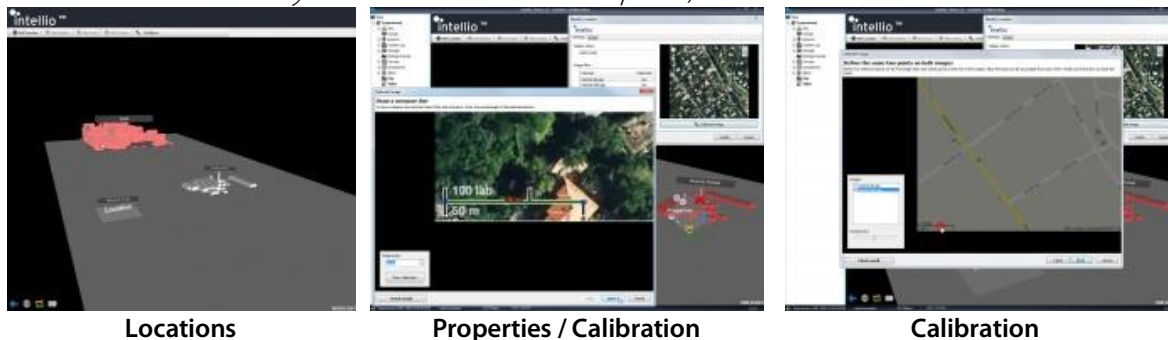
Misc: In this tab the Jump/Fly function can be enabled or disabled. The **Jump to camera on alarm** function detects if an alarm is in process, and immediately displays the camera in question. The **Enable fly animation** function does something similar to this, but instead of displaying the camera and the projected area immediately, it shows the distance and the route too from the actual location to the alarm event with a short animation.



28.2 Location

The first step to configure the map is adding a location to it. This location symbolizes an area, where the building, or buildings of a SITE is located; a definable geographical area. The **Model** of a location basically symbolizes the SITE on that area. The **Display name** is the name that will appear above the location. The **Image files** is the background of the area, quite often some kind of map. For the proper distance display it is suggested to calibrate the image. To do this, click on the **Calibrate Image** button and follow the instructions.

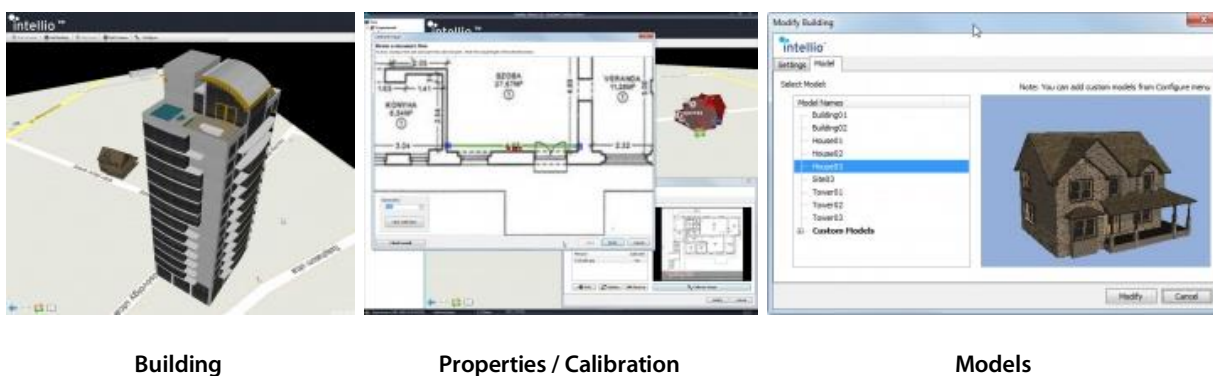
Note: The image calibration is not able to calibrate in three dimensions, so if the real distance is not the same in every direction from a certain point, then the calibration is useless.



By clicking on the location you move down on level, into the level of buildings.

28.3 Building

To add a building to a location, you have to have at least a layout of the lowest floor, this is necessary to create the building. After adding the first floor (*the lowest floor, even when it is the -1, -2, etc.*), calibrate the image (*just like with the locations*), then select the model representing the building (*or select your own custom model*).

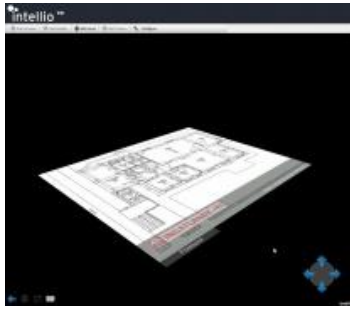


In this level it is possible to place out outside cameras with the same way you can in the inside of a building. The way to do it will be described on the next page.

The default floor of a building can be adjusted by selecting **Properties** in the building menu, but new floors can only be created above previously created floors.

28.4 Level

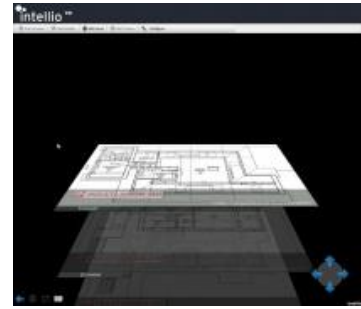
To create a level of a building, you have to add the layout of the floor and calibrate it.



Level



Properties / Calibration



Levels

28.5 Camera

Once the buildings and the floors are added, it is time to add the cameras to the system. Select a floor then click on it then click on the **Add Camera** button. After this, a window will appear, with three tabs.

- **Cameras:** You can choose the camera you want to add to the map.
- **Model:** The camera's model appearance can be selected here.
- **Projection:** The settings of the camera. Here can be selected, whether the camera should project an image or not, display motion information or not, etc. Here are the possible settings:
 - **Project camera image:** By enabling this option the camera live image will be projected to the layout. To this it is expedient to fit the projected image to the layout for the near-perfect covering. The **Opacity** function can help with that. It is also useful if you would like to see the layout too under the projected image.
 - **Show camera frustum:** This option displays the camera's field of view, with the selected color. This option is unnecessary if you had enabled the camera image projection.
 - **Limit frustum distance:** A useful tool, if the camera's field of view is too big and the projected image would reach over to the next room. With this, you can set a distance from the camera. Anything is a longer distance than the set value will not be displayed.
 - **Project selected motion information:** If you select the motion information under it, on the map the movement will be displayed on the projected image.
- **Note:** Camera requires a tracker for this function to work.
- **Downfacing camera:** In case the camera is not a dome camera, but is facing downward, use this option.

After adding the camera to the map, it has to be calibrated. This can be done by using the object menu of the camera, using the **Calibrate** function. Calibrate the camera: The mouse wheel set the angle of the FOV. By pressing the left mouse button the high can be set, and during pressing the right mouse button the image and the layout can be aligned (*the actual altitude and the FOV are displayed on the monitor to avoid any guessing*).



Calibrate button



Before calibration

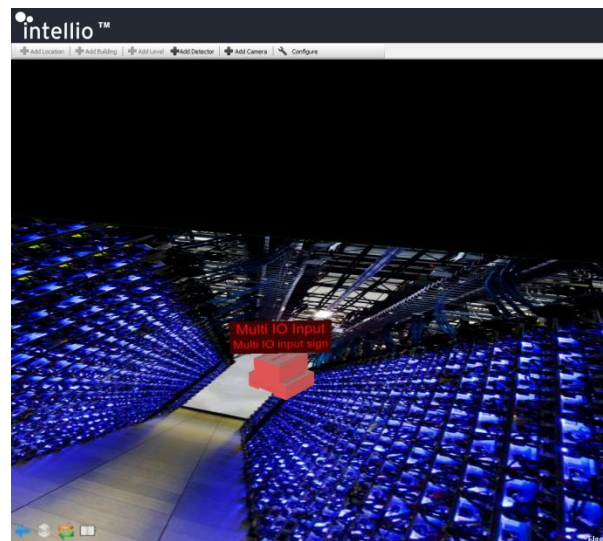


After calibration

28.6 Detector

Likewise cameras, detectors can also be added to the map. Since the cameras display the alarms of related detectors, in this case only the detectors linked to the system (*as opposed to the ones linked to the cameras*) can be added to the map, which received their own dedicated models.

The model corresponding to a given detector can be found on the second tab of the window which pops up after clicking on the **Add Detector** button. This is recommended to select, but the display selected can be modified later at any time under the **Properties** menu of the model.



29 Panorama

A panoramic image is a large image created by stitching together images of multiple cameras. Typically, it is rendered using images from cameras beneath or next to one another, with the cameras covering a larger premise together and with minor overlaps between the cameras. If you have cameras deployed in such a way, you can create a panoramic view in the Intellio Video System software in order to manage the combined images as a single large image in the client.

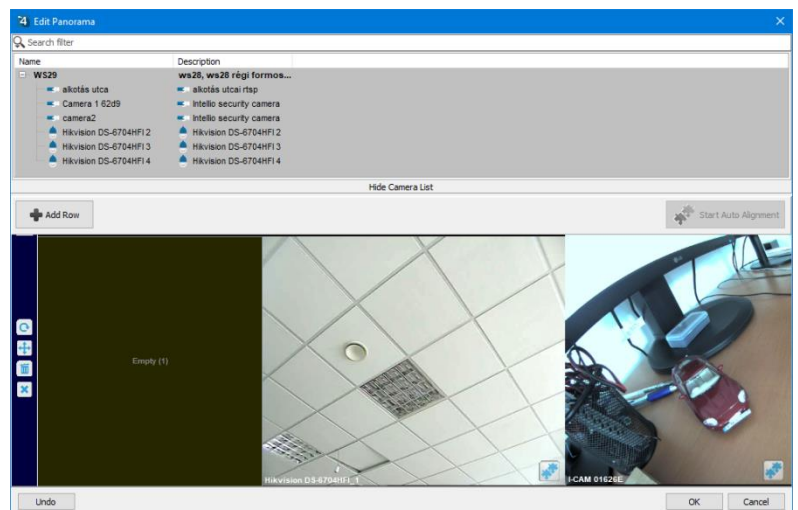
29.1 Creating Panorama

Every panoramic view is attached to a map location; therefore panoramic views can be created on the map, as is the case with cameras and detectors. Select a location in **System Configuration / Map**, then click on **Add Panorama**. In the next dialog panel, assign a name to the panoramic image, and select a model for it to identify it on the map. Next, click on **Edit Panorama**.

The editor window is comprised of two parts: the camera listing on the top and the editor field in the bottom. You can select cameras from the domain to be placed within the editor field. The lower section contains one or more rows of panels, which represent the constituents of the panoramic image.

Any number of new rows can be created using the **Add Row** button.

The toolbar on the left allows for deleting, emptying, shifting relative to the other rows, or reverting to the original horizontal position. Horizontal shifting may be useful if the cameras in adjacent rows are physically shifted, which can be offset by this function.



Cameras from the upper section can be dragged onto the panels. In Live mode the whole panorama image will appear based on the position of the camera on the upper left hand side. Next, the camera images can be stitched to the adjacent camera images in the following way:

- Moving any corner points
- Moving any sides
- Moving the whole image (*while holding the **right mouse button** pressed*)
- By automatic aligning (*see next page*)

Every panel containing a camera has its own toolbar, which becomes visible when the cursor hovers over the panel. The buttons in the toolbar are:

- **Remove camera:** empties the panel by removing the camera assigned to it
- **Reset corners:** reverts the four corner points to default position
- **Fill area:** useful when cameras with various aspect ratios are to be placed next to each other in multiple rows. In this case the panels with the higher aspect ratios will adapt to the one with lower ratios, thus filling the empty space that would normally result from differing aspect ratios.
- **Assign PTZ preset:** if a PTZ camera has a preset assigned for the area being monitored by that camera, the PTZ camera can be set to pan & tilt to the area that has been clicked (**Shift+Left mouse button**) on within a live panoramic view. After pressing the button, select the PTZ camera and the required preset.

29.2 Automatic Aligning

Adjacent images can be stitched together automatically, as well. In order for automatic aligning, select a few anchor points that allow the software to run the necessary calculations and transformations. An anchor point is a point in the image that is also found in the adjacent camera image, i.e. in an overlapping section between the two images.

To stitch two adjacent images, select 2-2 such points in both images, at both ends of the overlapping area. The farther the two points from each other (*within the image*), and the more accurate the marking of the reference points in the image, the more accurate the stitching will be.

To start automatic stitching, select the images to be stitched using the **Select for Auto Alignment** button in the lower right corner of the images. This button is only visible in images that are adjacent to the camera already selected.

The images selected will contain two buttons that allow for deleting existing anchor points or remove the image from automatic stitching. There will be a darkened area where no anchor points can be placed, while settings instructions are also displayed here.

To define a new anchor point, click anywhere on the active area in the image. To modify an existing anchor point, simply grab it and move it to the required position. The anchor points to be stitched together will be marked with the same color.

After defining all anchor points in the selected image, a green/red frame around the inactive field will signal whether the stitching has been successful or not. In case of failure while stitching, an error message will contain instructions to correct the problem. If all frames are green, click **Start Auto Alignment** in the top right corner of the window to initiate automatic stitching.

If the outcome is not satisfactory, do manual fine-tuning using any of the above methods or revert to the original state before stitching by clicking **Reset corners** in the toolbar of the window.

30 RTSP Users

Intellio Video System 4 has an RTSP server function which is provided by the IntellioGateway service. These users are independent from existing IVS users, you need to create new users. You can modify the access to different cameras per users.

IVS-RGW license is required for this feature.

Each user has their unique **Login name** and **Password**. RTSP User access rights depend on the list under the selected user's informations in the **Add RTSP User** window. The default **Camera rule type** is **Allow all (devices)**.

30.1 RTSP Gateway Setup

The configuration is stored at **c:\Program Files (x86)\Intellio Video System\Intellio Server\IntellioGateway.ini**. If you want to edit, you will need to restart the **Intellio Video Gateway** service to apply.

The default configuration is the following:

```
[Options]
Port=53560

[Servers]
Server1=localhost:53540

[RtspServer]
Port=8554
HttpPort=80
TranscodeKbps=1024
```

Restarting Intellio Video Gateway:

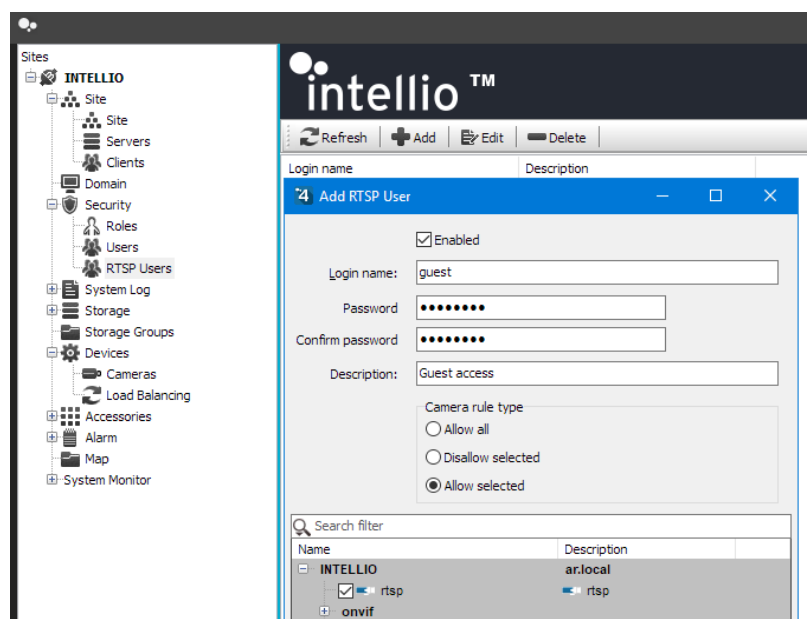
- Go to **Start menu / Run...**, or press **Windows + R** keys.
- Type in **"services.msc"** then click on **OK**.
- Search for the **Intellio Video Gateway** and click on **Restart**.

30.2 Creating New Users

To add a new RTSP User:

- Go to **System Configuration / Security / RTSP Users** menu.
- Click on **Add** button and fill in the User's informations.
- Click **OK** to save.

You can change here the **Camera Rule Type** to allow/disallow different Cameras.



You can edit existing RTSP Users by clicking on the **Edit** button or deleting with **Delete** button.

30.3 Connecting to RTSP

To connect, use one of the two possible URL formats, where **IP** is the Server1's IP under [Servers] and **RtspPort** is Port under [RtspServer]. When using a Router/NAT, the TCP port needs to be forwarded.

rtsp://IP:RtspPort/CameraID

- **CameraID** is the ID of the Camera from **System Configuration / Devices / Cameras**. You can select the text and copy it to the clipboard.

rtsp://IP:RtspPort/CameraName

- **CameraName** is the name of the Camera in URL encoded form. Camera name can be obtained from **System Configuration / Devices / Cameras**. Use <https://www.urlencoder.org/> to encode it.
- Some special characters can't be encoded, in this case, use the former URL format.

Using the following example with default configuration, the two URLs will be:

| Name and Description | Encoder | Motion Detection | Privacy Zones | License Plate Recognition | Navigation |
|--|---------|------------------|---------------|---------------------------|------------|
| Name: <input type="text" value="rtsp"/> Description: <input type="text" value="rtsp"/> Camera ID: 7bae273e-0123-4614-8d72-13990a2be649 | | | | | |

rtsp://localhost:8554/7bae273e-0123-4614-8d72-13990a2be649

rtsp://localhost:8554/rtsp

30.4 Supported videoformats

The following videoformats are supported through RTSP:

H.264: The original stream remains untouched.

MJPEG and Intellio IVC: The Gateway transcodes it to H.264 using the bitrate setting (*TranscodeKbps*).

Other videoformats (*for example MPEG2 or MPEG4*) are not supported.

31 Backup, Restore and Documentation

After we have set all the necessary settings and the system is working well it is recommended to make a backup from the system in case of a system crash the system can be easily restored.

31.1 Backup

The Intellio Server **4** is storing the system settings in the so called ***SystemConfig.rce*** and a ***LocalConfig.rce*** files like:

- Camera names
- Camera IDs
- IP addresses
- Video Adjustment settings
- Tracker and Calibration settings
- Motion Sensor and Detector settings
- Storage Rules
- Site and Domain settings

To save the configuration files go the following inside Intellio Client **4**:

System Configuration / Site / Servers / Backup Config button / Select server

Then a window appears where we can set the destination of the configuration files. The above mentioned two configuration files will be zipped into the desired location. Make sure these files are in a safe place.

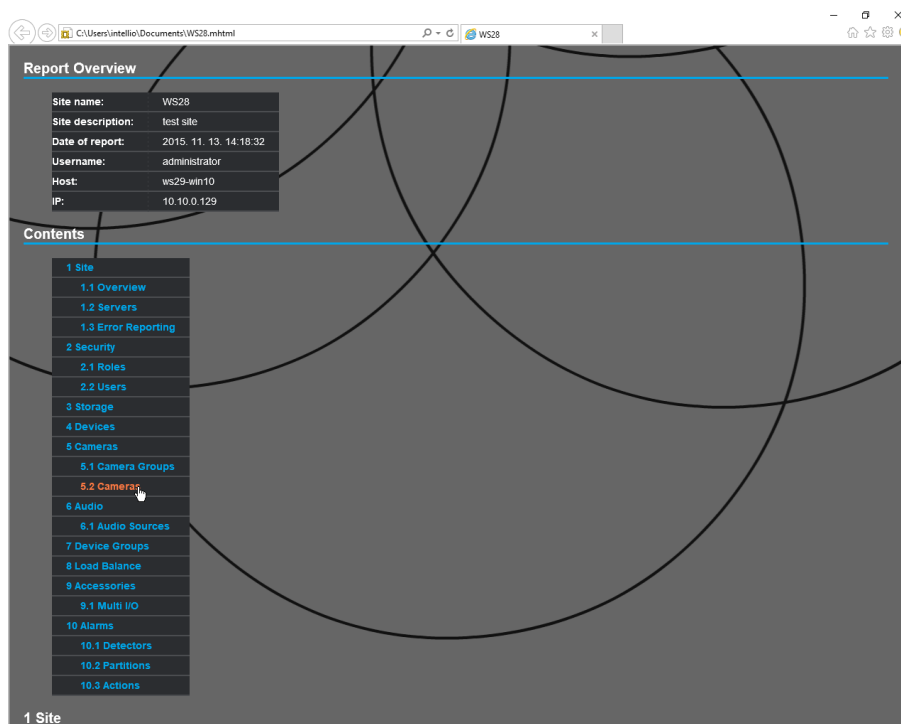
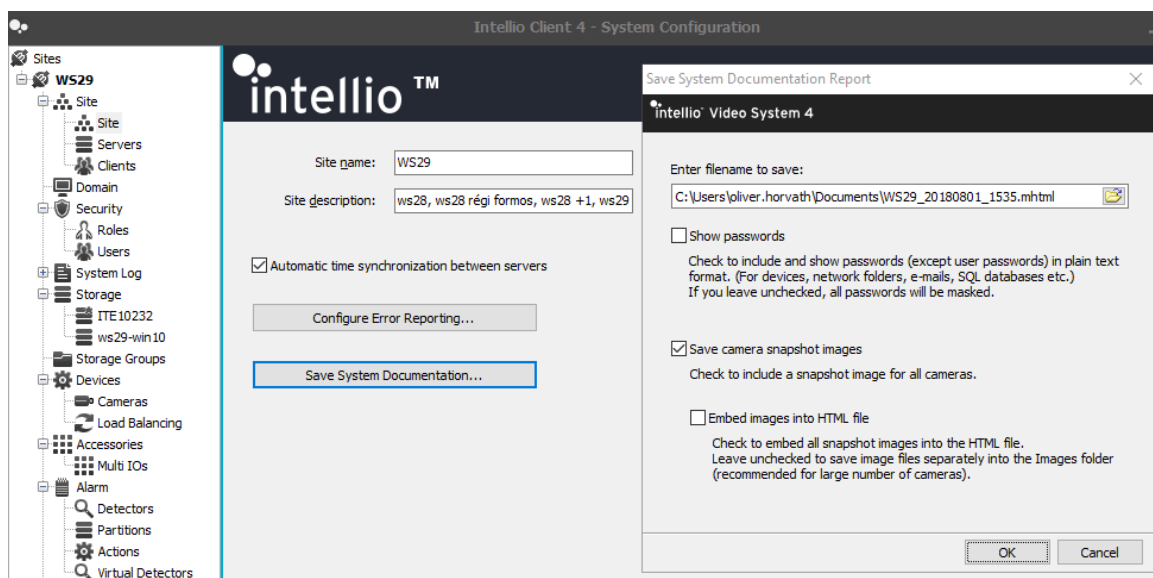
In case you are using the 3D Map feature in the IVS**4** it is also recommended to create a backup from the ***MapData.rce*** file and the ***MapStore*** folder. This file and folder contains the settings and parts of the 3D Map. This file is found in the Intellio Server folder (*check it in the location where you have installed the application, by default it is here: c:\Program Files (x86)\Intellio Video System\Intellio Server*).

31.2 Restore

- **Install** the Intellio Server with default settings.
- After installing **STOP** the Intellio Server service.
- **Copy** the saved backup files into the Intellio Server folder by overwriting the default configuration files.
- **START** the Intellio Server service.

31.3 Documentation

IVS is capable of saving the system's configuration in MHTML format (*e.g. for archival purposes*). Go to the **System Configuration / Site / Site** page and press the **Save System Documentation...** button. Select the documentation folder and type the filename in the window that appears. With the **Show passwords** checkbox display of the camera's passwords can be controlled (*the user passwords are not included in the documentation*).



32 System Monitor

*This feature is not available in all editions.

32.1 Performance Monitor

Performance Monitor is a visualization tool in Intellio Video System for measuring performance data and to monitor the behavior of the SITE. It may help to check whether the system is working properly and to localize potential anomalies easily. Accessing this function requires the **Site Manager / System Monitor** right.

Real time data is updated every second, while history data is stored and retrieved in 5 seconds interval. History data is retained up to 40 days, depending on the available storage space.

The first page on the Performance Monitor is the default **Dashboard** tab where the most important counters of the system are shown. You can create your own custom pages where you can place several performance counters of a given category (*one category per page*). The available categories are the followings:

- **Servers:** performance counters related to individual servers.
(CPU, RAM, storage and bandwidth counters per server, etc.)
- **Global:** overall performance counters related to the whole SITE.
(overall storage speed, overall network bandwidth, etc.)
- **Devices:** performance counters related to individual devices.
(for eg. device connection lost counts).
- **Cameras:** performance counters related to individual cameras.
(for eg. various camera network bandwidth and frame rate speed data)

32.1.1 Creating a New Performance Counter Page

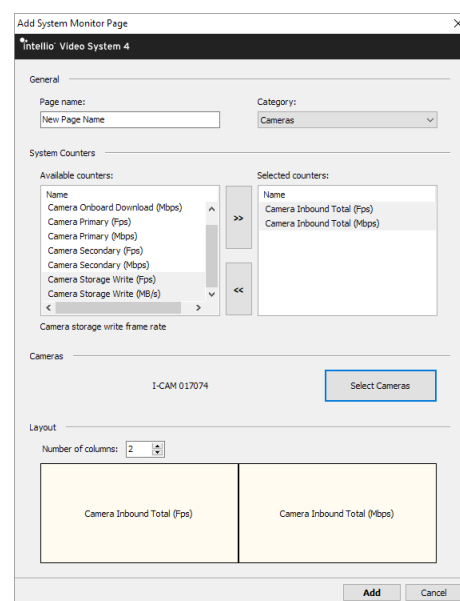
To create a new page press the **New Page** button located on the toolbar of the **Dashboard** tab.

Choose the category of the desired counters to be displayed in the page, then select the counters in the **Available counters** list and click on the >> button (or drag-and-drop the items) to take them to the **Selected counters** list.

Then select which servers/devices/cameras would you like to be displayed (*up to 6*).

There is a **Layout** diagram at the bottom of the page, which illustrates the actual layout of the selected counters. The number of counters in a single row can be increased or decreased by changing the value of **Number of columns**, while their arrangement can be modified by reordering the items in the **Selected counters** list (*by drag-and-drop*).

To change settings on an already existing page press the **Modify** button on the toolbar.



32.1.2 Performance Counter Interface Controls

You can show or hide the counters for each item (*server/device/camera*) in the graph by clicking the appropriate item button on the toolbar. To change the visibility of the real time data use the **Show/Hide Real Time Data** button located on each graph.

Drag the graph by the right mouse button to scroll it horizontally. Select area from left to right with the left mouse button to zoom in and select right to left to zoom out. Default zoom and position can be restored by pressing the **Reset Zoom** button on the toolbar.

32.2 System Status

The other item under the **System Monitor** menu is the **Status** page, which is for giving you an overview state about the whole SITE with its main system components and their healthy states. These are:

- The servers of the SITE and their availability
- The devices registered to each server and their connected states
- The storage buffers belonging to each server and their availability

The components working properly are marked by green color, while fault states are shown in red. Hoover the mouse over an item to get the detailed status description about the item, or click on it to get to its configuration page.

Furthermore, the status of each SITE you logged in is also indicated on the status bar of Intellio Client, so the status feedback is immediately shown after connection. By clicking on each status icon you can get directly to the **Status** page of that SITE.



33 Recommended Installation Order

- ***Cameras Installation, IP Addresses (page [21](#))***

Use static IP addresses if possible.

In case of a multi-server SITE, be aware of the fact that in order for camera takeover to work properly, all of the SITE's servers have to have access to the cameras.

- ***ANPR USB Key and ANPR Engine Installation to the According Server (page [109](#))***

- **Setting ANPR Properties**

- ***Servers Installation (page [10](#))***

If you are using Intellio's server computers, the IVS server application is preinstalled for you by Intellio's experts, so you just have to configure the system. To log into the OS use the following **username / password: Administrator / Intellio1234**.

- **Server IP Address Checking**

Intellio's server computers use dynamic IP addresses (DCHP) by default. It is recommended to use static IP addresses for the servers.

- ***Server Installation, License Key Setting, Activation (page [10](#))***

- Check the computer's clock settings before server installation.
 - Before installation check, whether the cameras can be reached on the corresponding IP-addresses from the server (*ping*, *IntellioDeviceExplorer.exe*).
 - After installation, check the firewall settings. If the firewall is enabled, grant network access to the following applications: Intellio Video Server (*RCServerSvc.exe*), Intellio Video Gateway (*IntellioGatewaySvc.exe*)
 - Do not forget to activate the server within 15 days from the first installation. The server stops working after 15 days without activation. For activation and inspection, use the ***IntellioActivationTool.exe*** application.

- **Installation of More Servers, License Key Input, Activation**

- Install all the servers according to point [30](#), and check whether the servers on one SITE can reach each other (*ping*).

- ***Clients Installation (page [13](#))***

It is recommended to install client application on all server computers, as it is used to configure the server.

- ***Connection (page [18](#))***
- ***Creating Site (page [71](#))***
- ***Setting Storage Buffers (page [37](#))***
- ***Creating Storage Groups (page [39](#))***
- ***Adding Cameras (page [21](#)), Registration (page [34](#))***

ANPR cameras should be registered with the server, which is equipped with an ANPR key.

Only functioning cameras can be added to the system. The system will not allow camera registration until it can communicate with them; this is true even if the IP address of the camera is known.

- ***Setting Intellio Cameras (Orio, Visus)***

- **General Settings**

- *Image Settings (page [47](#))*
 - *Encoder / Sensor Setting (Orio: page [55](#), Visus: page [56](#))*
 - *Setting Base Motion Detector (page [61](#))*

- **Orio Cameras:**

- *Calibration (page [91](#))*
 - *Setting Tracker (page [92](#)). Only when needed, or lower fps is not an issue.*

- **Visus Cameras:**

- *Calibration (page [91](#)). Only when needed for searching with virtual detector.*
 - *Setting Tracker (page [92](#))*

- ***Adding Detectors, and Setting (page [87](#))***

- ***Setting ONVIF Cameras (page [57](#))***
- ***Setting Error Reporting (System Configuration/Site/Site page) (page [69](#))***
- ***Setting Alarm System (page [78](#))***

We recommend that you create the following 2 detectors on all SITES!

- ***Camera Availability Detector (page [103](#))***
- ***Site State Detector (page [103](#))***
- ***Adding other detectors, partitions, actions if necessary (page [78](#))***
- ***Creating Roles / Users, and Setting (page [66](#))***
- ***Setting Internet Access (page [75](#))***
- ***Verfiying***

The following steps should be done regularly.

- Revise the system log per server. After set-up is complete, there cannot be any existing error messages in the system log.
- Check the writing speed on the ***System Configuration / Storage*** page per server. There cannot be a substantial difference between the actual and required writing speeds, otherwise frame loss may occur. If the required writing speed is higher than the actual, create more storage groups with the same settings as the original, and evenly distribute the cameras between them. Check the writing speed of the storage folders, in case of a NAS its load.
- Check state of the devices on the ***System Configuration / Devices*** page. The registered cameras should be ***Online***.
- Check the events statistics on the ***Summary*** and ***Graph*** tabs of the ***System Configuration / Storage*** page. The graphs can help the discovery of a poorly configured detector for example.
- ***Backup, Documentation (page [124](#))***

34 Appendix

34.1 Hexadecimal Conversion Chart

Find the first character of the byte in the corresponding row, and the second character of the byte in the corresponding column. The decimal value of hexadecimal byte can be found where the rows and columns intersect.

e.g.: **0x42** = **66**, **0x7B** = **123**

| | | Second digit | | | | | | | | | | | | | | | |
|-------------|---|--------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| First digit | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | 1 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| | 2 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| | 3 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| | 4 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| | 5 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| | 6 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 |
| | 7 | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| | 8 | 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| | 9 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| | A | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| | B | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |
| | C | 192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 |
| | D | 208 | 209 | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 |
| | E | 224 | 225 | 226 | 227 | 228 | 229 | 230 | 231 | 232 | 233 | 234 | 235 | 236 | 237 | 238 | 239 |
| | F | 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 254 | 255 |