IVS - System detectors and the IVS alarm system

Table of Contents

1. Introduction, important information

This guide summarizes the details of the IVS Alarm system settings. For a complete overview of the system architecture and configuration, please refer to the ***IVS Installation Manual*** documentation.

2. The Alarm system

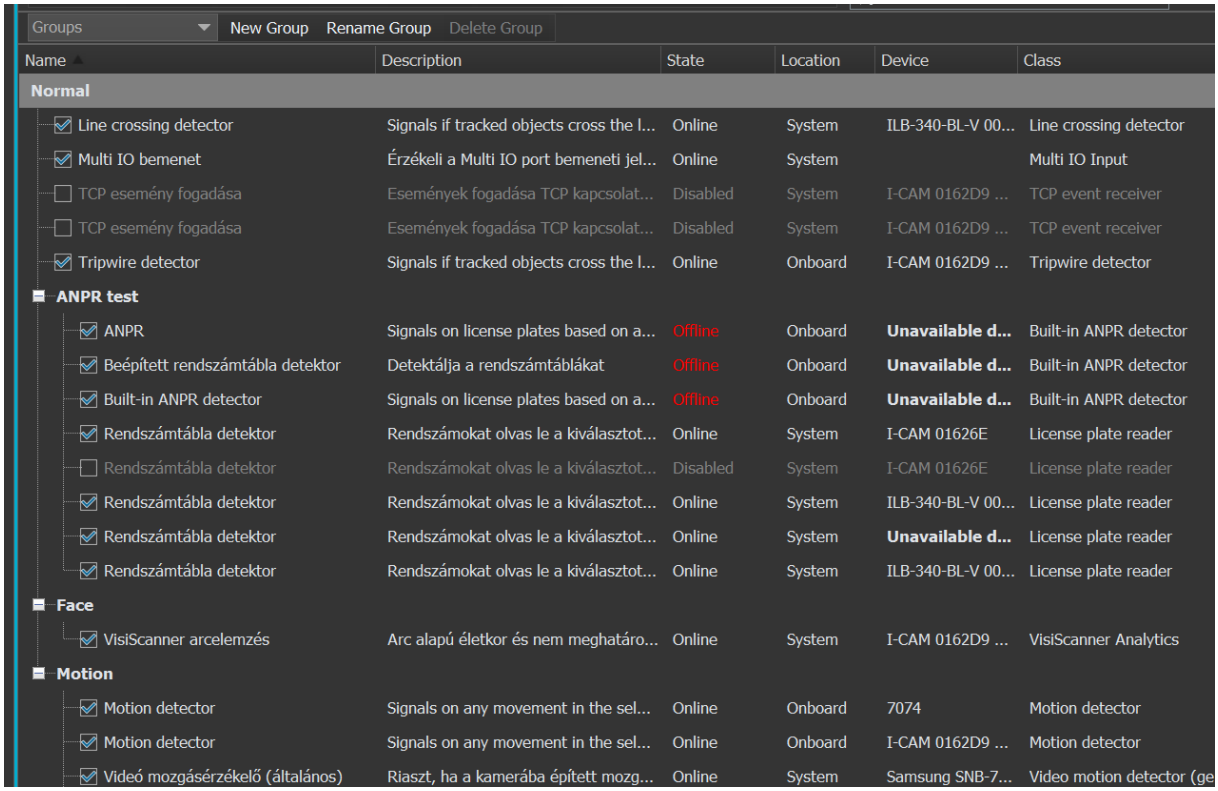
The Alarm System consists of Action, Partition and Detector.

- **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 ensure all your predefined Actions in the Partition will run if the Detector sends an Alert.

Certain buttons can be found in the header part of the above-mentioned functions, in **System Configuration / Alarms** menus':

- **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, duplicated item 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 message, simply uncheck the checkbox next to the event type. It only controls the display of events appearing in the **Events** window at the bottom of the **Live** interface. In the alarm system, Events can still be used for the creation of controls.
- **Alarm sounds:** This button is only found on detectors. Once pressed, you can set global default sounds. These sounds can be judged separately from the detectors.
- **Edit Index list:** for partitions and operations, it is possible to edit the index numbers after pressing the button.

In the alarm system, it is also possible to group the elements as needed, for this you can create any number of groups with any name.



New groups can be created with the **New Group** button, and then the selected elements can be transferred to the group using the mouse "drag and drop" method. The selected group can be renamed with the **Rename Group** button and deleted with the **Delete Group** button.

In the alarm system, detectors in an unavailable state are marked Offline in red, and those in a disabled condition are grey. This grey marking is typical for the rest of the alarm system.

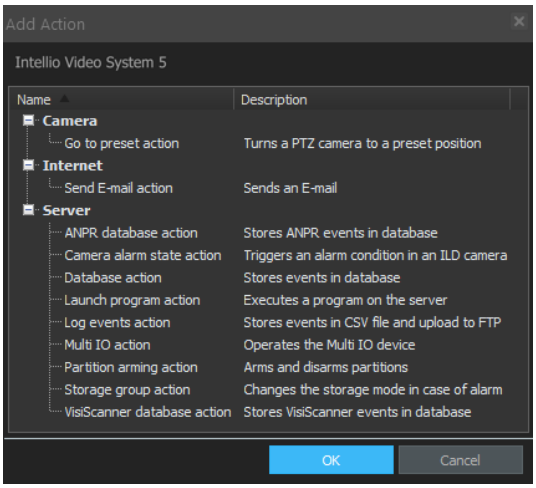
3. Actions

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, or the server. It could be even an internet action. These Actions are:

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

3.1. Create Actions

To create an Action, press the **Add** button in the **System Configuration / Alarm / Actions** menu, then select an action to add from the window that appears.



Each action is different, but they share several structural similarities. A brief description of these follows below.

3.1.1. General tab

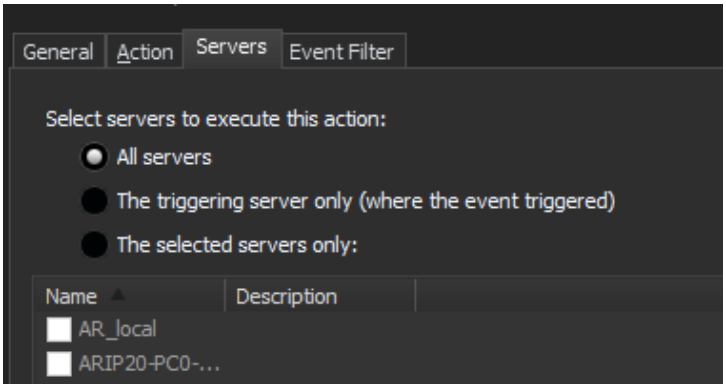
In the General tab, you can specify the unique name, description, and status of the action. Actions that are not enabled will not be executed.

3.1.2. Action tab

The Action tab contains the specific settings for the action. Detailed configurations can be found in the respective sections for each action.

3.1.3. Servers tab

The settings on this tab determine which server will execute the action. This tab is not available for the **Go to Preset** action, as it does not apply to a server.

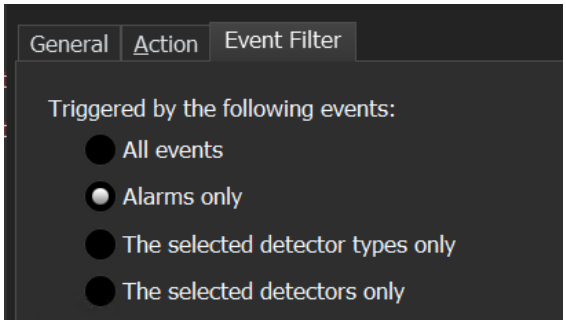


Options:

- **All Servers**: The action will be executed by all servers in the SITE. Use cautiously, as it may result in multiple data entries for database actions or repeated emails for email actions.
- **The triggering server only (where the event triggered)**: The action will be executed by the server where the triggering event occurred.
- **The selected servers only:** The action will only be executed on the selected servers.

3.1.4. Event Filter tab

On this tab, you can select which events will trigger the action.

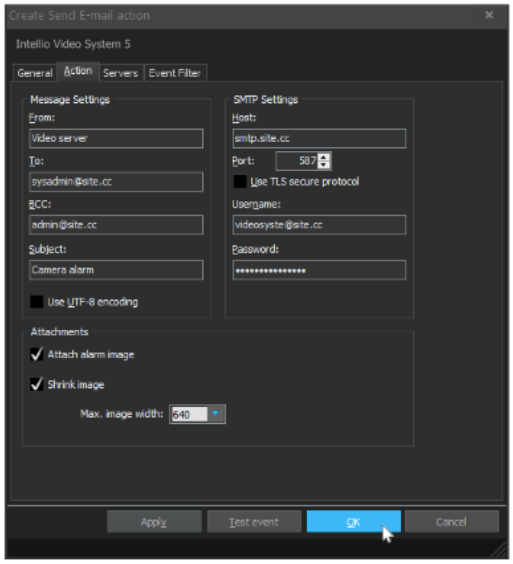


- **All Events**: The action will be triggered by any event.
- **Alarms Only**: The action will be triggered only by alarm events.
- **The selected detector types only**: The action will be triggered only by the selected event types.
- **The selected detectors only**: The action will be triggered only by the selected events.

3.2. Internet actions

These operations define actions to be executed via the internet.

3.2.1. Send E-mail



This action automatically sends an email message to pre-set addresses with the specified subject line. If there are multiple recipients, their email addresses should be separated by semicolons (**;**) in the **To** field.

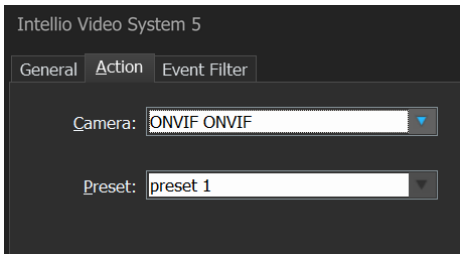
SMTP settings must be configured, including Host, Port number, possible secure TLS protocol, and the username and password of the email account used for sending the email.

If the message source is linked to a camera, there is an option to attach the camera's alarm image. To attach an image, enable the **Attach alarm image** option. To set a maximum width for the image, enable the **Shrink image** option.

In a multi-server SITE, it is recommended to select the triggered server setting to avoid multiple deliveries and ensure each server can send emails with the configured settings.

3.3. Camera actions

Camera actions instruct the camera to perform a specific operation.



3.3.1. Go to preset action

This action rotates the selected PTZ camera to a predefined preset position.

Creating a Preset in the Live Interface

Some important positions of PTZ cameras can be saved and recalled at any time. Create these presets before configuring the Go to Preset action:

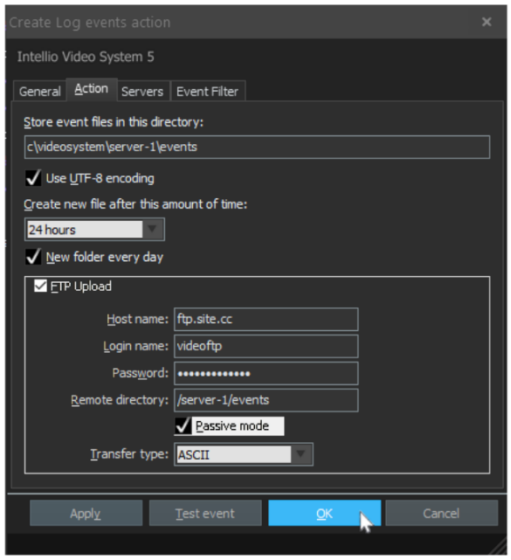
- Move the PTZ camera to the desired position.
- From the camera menu, select the third icon, then choose the **Create preset** option below the displayed presets.
- Enter the name of the preset in the popup window.

3.4. Server actions

These actions are executed on the server(s), altering certain functions or operations, potentially creating new files, or controlling other server-related devices.

3.4.1. Log events action

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



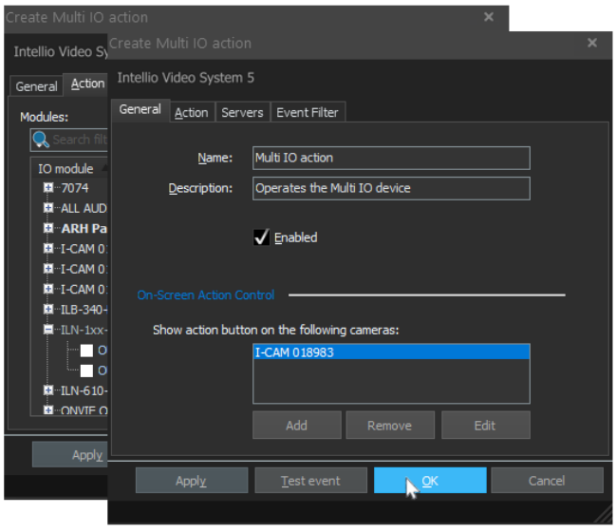
- **Store event files in this directory:** The location on the computer where the created file will be stored.
- **Use UTF-8 encoding:** Type of character encoding. Most programs support this encoding, but if issues arise with data display, it should not be enabled.
- **Create new file after this amount of time:** The duration after which the system will create a new file. It is recommended to set this interval based on how frequently the event is expected to occur. Too many entries in one file can be just as overwhelming as having too many files.
- **New folder every day:** A solution to the problem of too many files mentioned above.
- **FTP Upload:** When enabled, the created file will be uploaded to the specified FTP server.
- **Host name:** The name of the FTP server.
- **Login name** and **Password:** Credentials for logging into 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.

3.4.2. Camera alarm state action

This action overrides the speed limitations in the Camera encoder settings of the Intellio Orio/Visus camera, allowing the device to operate at its maximum frame rate. The effect of this action is temporary. If the action is not invoked again, the frame rate restrictions will revert to their original settings..

3.4.3. Multi IO action

The Multi IO action controls a multi IO device and sends signals to the appropriate ports (e.g., activates a relay output). This action can also be used to send a signal to the output port of an Intellio, Samsung/Hanwha, or ONVIF camera, as well as a Modbus TCP device.



Important: *this action can only turn the output on, so it should only be used with timed (monostable) outputs!*

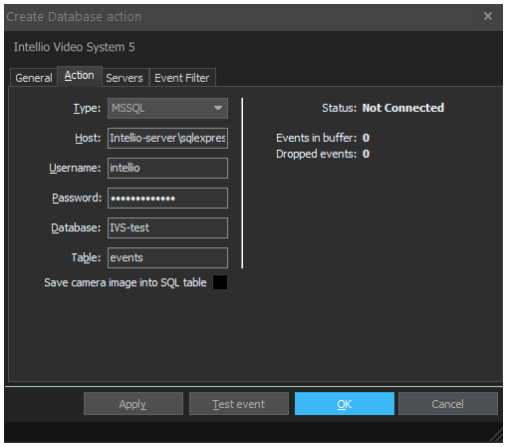
In the **On-Screen Action Control** from camera menu list, specify which cameras' menus should allow manual triggering of the operation. Use the **Edit** button to set the order of actions available in the selected camera menu.

If the action controls a camera output, enable its execution on all servers. The action will be performed by the server that is connected to the camera at the time of execution. This ensures proper action even if the camera is switched to a different server.

3.4.4. Database action

The action stores every event received by each server in an SQL database.

- **Type**: The type of database used for storage. This can be MySQL or MSSQL.
- **Host**: The database location. This can be a web server or a specific directory on the network.
- **Username**: The username required to access the database.
- **Password**: The password associated with the username for database access.
- **Database**: The name of the database.
- **Table:** The database table where the configured data will be stored.



The required fields for the table are as follows:

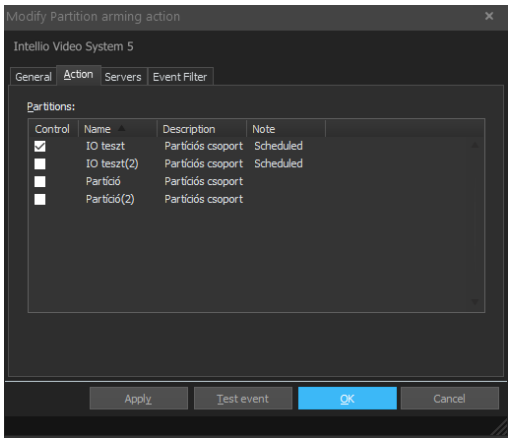
These field names must match exactly; otherwise, the database operation will not be able to store the required data.

Név	Típus	Illesztés	Tulajdonságok	Nulla	Alapértelmezett
DateTime	datetime			Nem	*Nincs*
DetectorClass	varchar(50)	utf8_hungarian_ci		Igen	*NULL*
Detector	varchar(255)	utf8_hungarian_ci		Nem	*Nincs*
Source	varchar(255)	utf8_hungarian_ci		Nem	*Nincs*
EventCode	int(4)			Igen	*NULL*
Message	varchar(4000)	utf8_hungarian_ci		Nem	*Nincs*
Gender	char(1)	utf8_hungarian_ci		Igen	*NULL*
Age	int(4)			Igen	*NULL*
FrontalTime	float			Igen	*NULL*

Important: *In a multi-server SITE setup, it is recommended to choose the triggered server configuration to avoid duplicate data entries. However, it is important to verify that all servers can communicate with the database server.*

3.4.5. Partition arming action

This action activates one or more partitions. It is possible for multiple actions to activate the same partition simultaneously; however, the partition will immediately become inactive as soon as the first "alarm end" event is received.



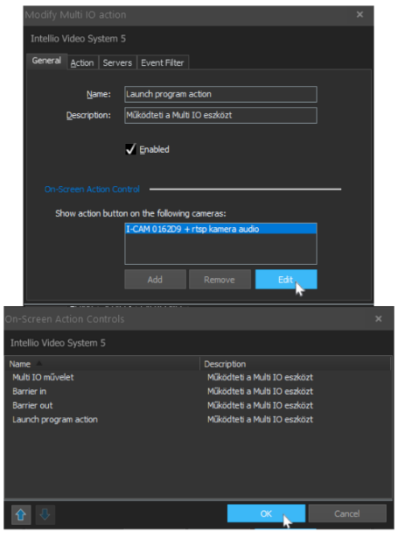
Note: *A partition's status can also be modified by the user or the scheduler.*

Note: *In a multi-server SITE setup, the correct execution mode for this action is* ***All Servers****.*

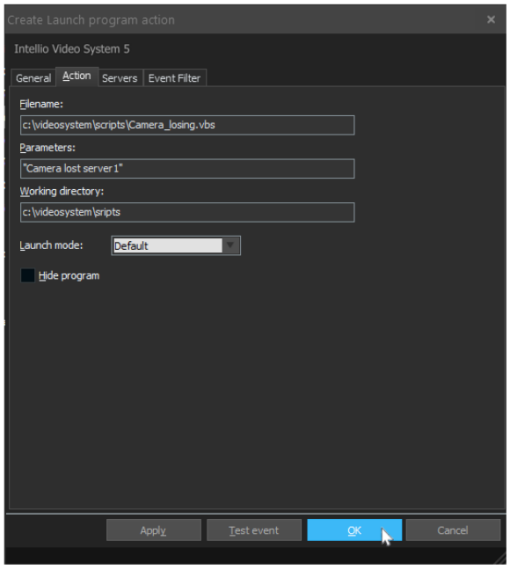
3.4.6. Launch program action

The action starts a program. This can be a batch file or any other standard program, such as printing (print.exe). The file name and path (working directory) must be specified for proper action.

In the **On-Screen Action Controls** from camera menu list, specify which camera menus you want to use to manually start the action. Use the appropriate buttons to add or remove items. The **Edit** button allows you to set the order of actions that can be started from the selected camera menu.



Action parameters:



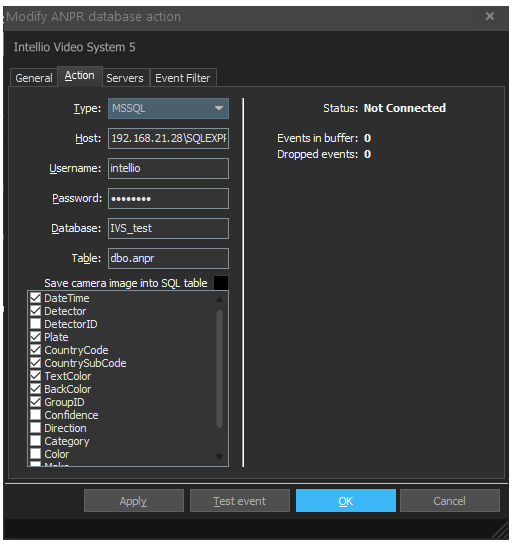
- **Filename**: The name of the program to be executed.
- **Parameters**: Essentially DOS command-line parameters. These are usually not required but can be useful (e.g., when passing parameters to a batch file).
- **Launch Mode**: Useful if the selected file is not intended to be used in the default, standard way (e.g., printing a document).
- **Hide Program**: The program will run in the background without drawing attention.

Note: *If the operation is executed by multiple servers, the specified program must be available on each server with the given parameters.*

Keep in mind that the program will run under the SYSTEM user account that also runs the server service (which, for example, does not have Desktop access).

3.4.7. ANPR database action

The action stores the data of license plates identified by the license plate detector and the built-in license plate detector in a database. At the beginning of the configuration, the information to be stored must be specified cell by cell, which can later be used for search purposes. The data to be configured includes:



- **Type**: The type of the storage database. This can be MySQL or MSSQL.
- **Host**: The accessibility of the database. This can be a web server, a specific directory on the network, or a computer.
- **Username**: The username used to access the database.
- **Password**: The password associated with the username to access the database.
- **Database**: The name of the database.
- **Table**: The table in the database where the configured data will be stored.

Users overview

	User	Host	Password	Global privileges	Grant	Action
☐	Any	%	--	USAGE	No	Edit Privileges Export
☐	Any	localhost	No	USAGE	No	Edit Privileges Export
☐	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 match the ones shown in the image!

MySQL database is natively supported.

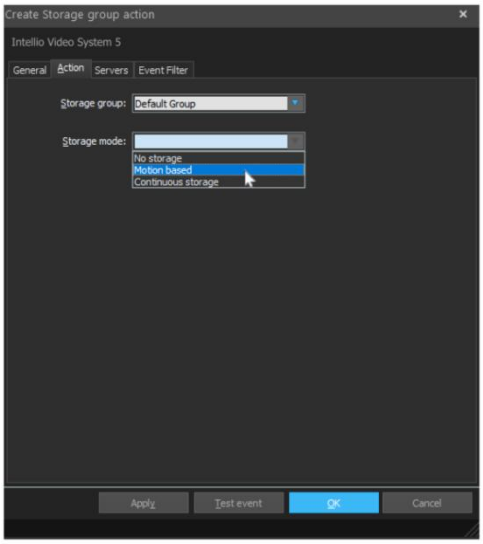
Fontos: *In a multi-server SITE, it is recommended to choose the triggered server setting to avoid multiple insertions of the data. However, it is essential to check that each server is able to communicate with the database server!*

Column Name	Data Type	Allow Nulls
DateTime	datetime	☐
Detector	nvarchar(30)	☑
DetectorID	nvarchar(38)	☑
Plate	nvarchar(10)	☑
CountryCode	nvarchar(3)	☑
CountrySubCode	nvarchar(15)	☑
TextColor	nvarchar(15)	☑
BackColor	nvarchar(15)	☑
GroupID	int	☑

3.4.8. Storage group action

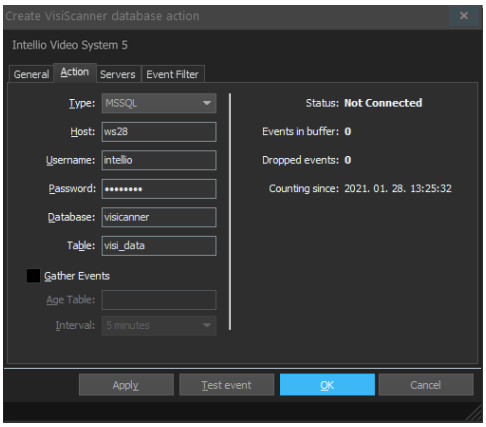
This action changes the storage mode of the specified storage group. The change is temporary, and once the triggering alarm event ends, the storage mode will revert.

- **Storage Group**: The storage group whose storage mode will be changed by this action.
- **Storage Mode**: The type to which the storage mode of the storage group will change as a result of this action.



3.4.9. VisiScanner Database action

The VisiScanner detector events can be stored in an SQL database.



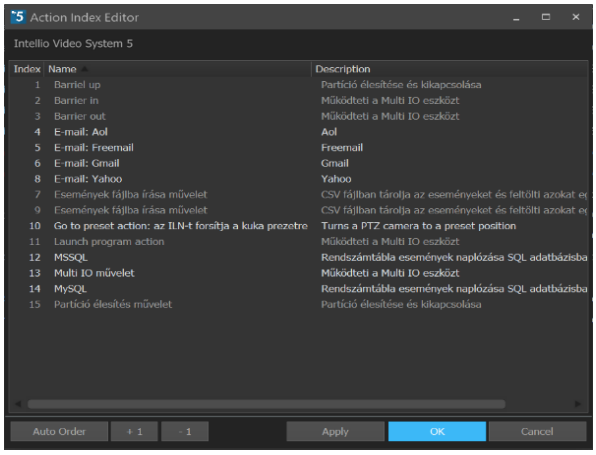
- **Type**: The type of the storage database. It can be MSSQL, MSSQL2008, or MySQL.
- **Host**: The accessibility of the database. It can be a web server or a specific directory on the network.
- **Username**: The username used to access the database.
- **Password**: The password associated with the username used to access the database.
- **Database**: The name of the database.
- **Table**: The database table where the configured data will be stored.

If you enable the **Gather Events** checkbox, also provide the following:

- **Age Table**: The table will store the arithmetic average of the database's age groups, as well as the number of people in the specified age group below the given interval.
- **Interval**: The period after which a new aggregation will occur.

Important: *For multi-server SITE setups, it is recommended to choose the triggered server setting to avoid multiple insertions of the data, but you must verify that all servers can communicate with the database server!*

3.5. Creating an index of Actions



In the **Action Index Editor** window, you can assign a number to each action. During Live view, entering the number activates the action.

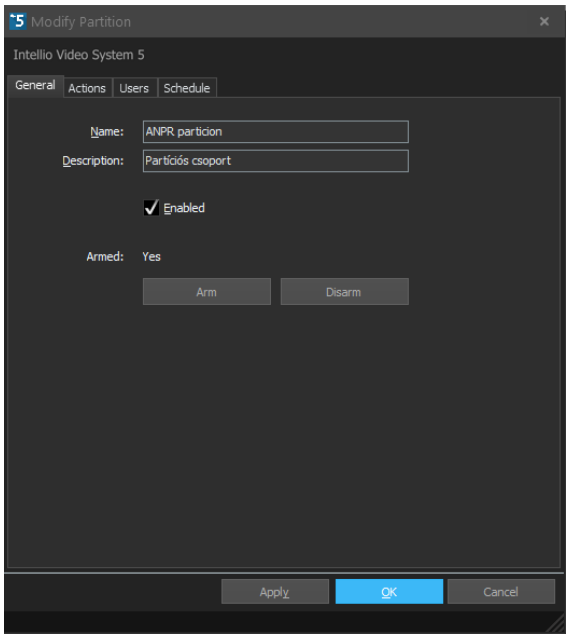
The **Action Index Editor** can be opened by clicking the **Edit Index List** button under the **System Configuration / Alarm / Actions** menu.

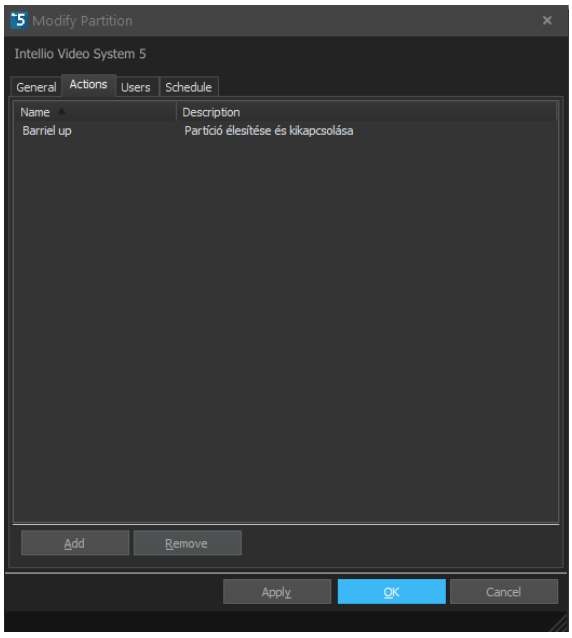
The simplest way to assign index values is by using the **Auto Order** button. This automatically associates a number with each action in increasing order, overriding previous settings.

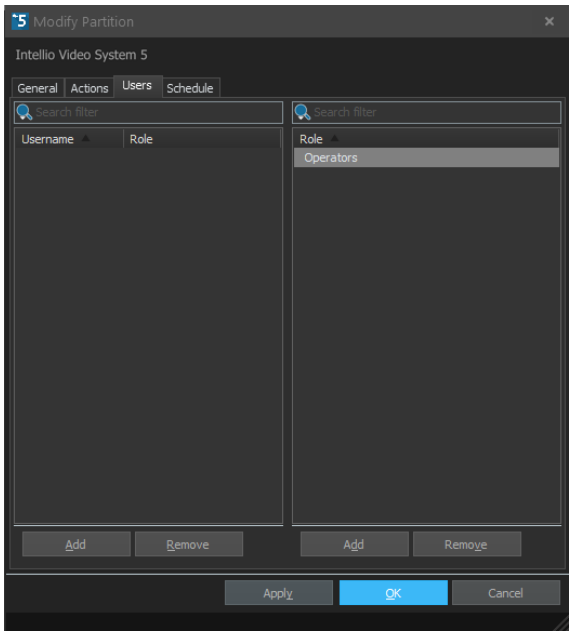
The order can be changed by clicking on the action's index number and editing it to the desired number. It is also possible to increase or decrease the index value by one using the **+1** and **-1** buttons. The client will not allow two actions to have the same index. If this occurs, the names of the conflicting actions will be highlighted.

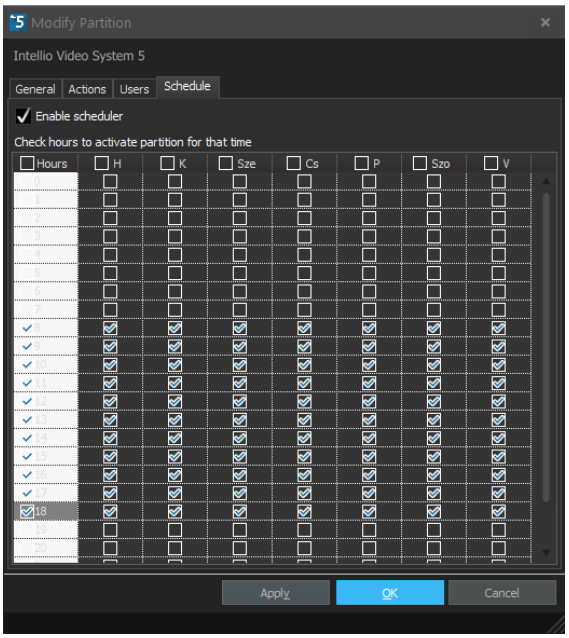
4. Partitions

To create a partition, press the **Add** button in the **System Configuration / Alarm / Partitions** menu. In the window that opens, the partition can be configured using four tabs. These tabs are as follows:









- **General**: In this tab, the partition's name, description, and status can be configured. Disabled partitions will not execute the assigned actions and will not notify users. The partition's current status (armed or disarmed) is displayed and can be manually changed using the **Arm** and **Disarm** buttons. Armed partitions will execute the assigned actions and notify the specified users about events. A partition's status can change in four ways:

- Manually, through the Live view main page using the Toolbar on the left side partition list,
- Manually, via the command issued by right-clicking on the Partition model placed on the 3D map,
- By the Partition arming action,
- By the Scheduler, according to the settings in the **Schedule** tab.

- **Actions**: Existing actions can be assigned to the partition here. When the partition is activated, all of its actions will be executed, provided that the partition is armed at the time of the alarm event.
- **Users**: This is where you can set which users and roles should be notified about detector events that trigger the partition. If no users are specified here, and the specific detector has not been overridden, then everyone will receive these notifications.

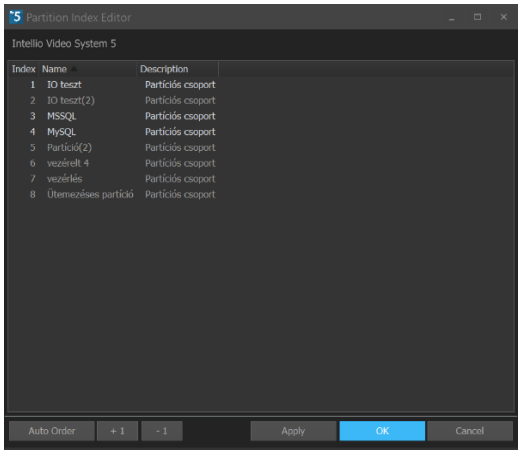
> ***Note:*** *Users can be specified separately for detectors, and they may receive detector events regardless of the partition's state.*

- **Schedule:** The partition will be armed at the selected times and disarmed at unselected times.

> ***Note:*** *The partition's state can be changed at any time by the user or an operation.*

4.1. Creating an index of partitions

In the **Partition Index Editor** window, you can assign a serial number to each partition. During Live view, entering the serial number allows you to arm the partition.



The **Partition Index Editor** can be accessed by pressing the **Edit Index List** button within the **System Configuration / Alarm / Partitions** menu.

The easiest way to assign index values is by using the **Auto Order** button. This automatically assigns a number to each partition in ascending order, overriding previous settings.

The order can be changed by clicking on the partition's serial number and entering the desired value. Alternatively, you can use the **+1** and **-1** buttons to increase or decrease the index value by one. The client does not allow two partitions to have the same index value. If this happens, the names of the affected partitions will be highlighted.

5. Detectors

The built-in Intellio camera detectors and server-side (system) detectors with intelligent functions provide significant assistance to operators and enhance the efficiency of surveillance personnel. The integrated intelligence introduces a level of automation and independence to video surveillance.

Intellio's advanced event detection and alarm system is sophisticated, yet remains easy to operate thanks to its refined configuration interfaces. The detectors that can be added to the system are divided into two major groups, each containing the following types of detectors:

Onboard (camera-side) detectors:	Motion Sabotage Object removal IO-input Built-in ANPR Intrusion Line crossing Direction Intelligent motion Hidden, built-in intelligent motion
System (server-side) detectors:	License plate Multi IO input Camera availability Device Event (ONVIF/Hanwha) SITE state VisiScanner Analytics TCP Event receiver Video motion (general) Hidden PTZ preset detecktors Detectors based on Smart MetaData: Motion, Entry, Direction, Line crossing

The detailed settings and availability of **Onboard (camera-side) detectors** vary significantly depending on the device/camera group type. For a detailed description and more information, please refer to the relevant documentation:

- ***Intellio INITIO cameras***
- ***ONVIF devices***
- ***EINAR cameras***
- ***Hanwha devices***
- ***Registration and management of custom devices, cameras***

5.1. Add a System detector

The detector settings can be accessed through the Client program. The process for modifying or adding detectors is the same after selecting the appropriate detector and camera pair.

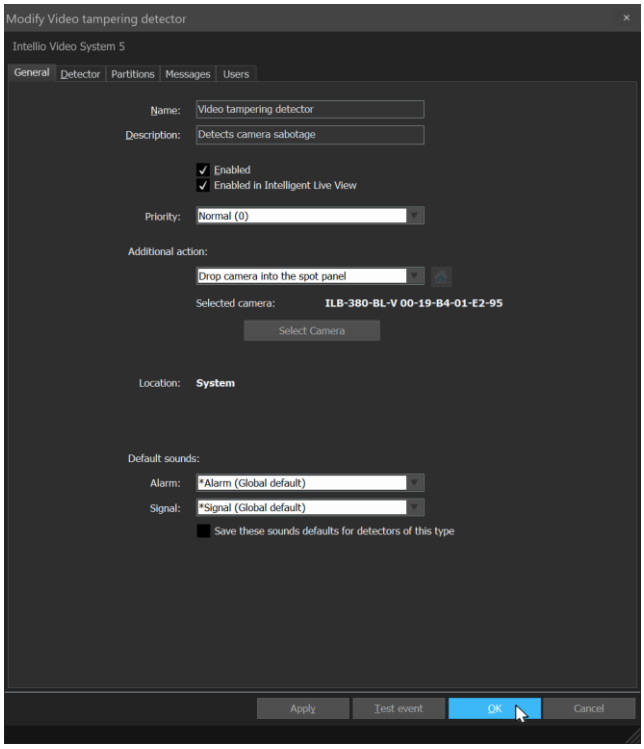
- Click the **Add** button in the **System Configuration / Alarm / Detectors** menu, then select the **System** detector type.
- Choose the detector you want to use.
- Finally, select the camera on which you want to apply the detector.

Important: *After selecting the detector, only cameras that support the selected detector will be available for selection.*

5.2. General structure of a detector

Each detector includes configuration settings across the following five tabs.

5.2.1. General



The detector's **name** and **description** are general by default, so it's recommended to change them for easier identification later (including the associated camera in the name or description can be helpful). Below the name and description, you can **enable** the detector and specify whether the **Intelligent Live View** function should consider it.

Priority controls how events from the detector appear in Spot panels in Live View; higher-priority events will override lower-priority ones.

Additional action allow you to display even a different camera's feed instead of the default one when an event is triggered. This is useful if a sensor is connected to a camera's I/O input, but monitors a different camera's field of view. You can also configure complete view changes, displaying multiple cameras simultaneously when the detector triggers an event.

You can assign a custom sound to the detector's events.

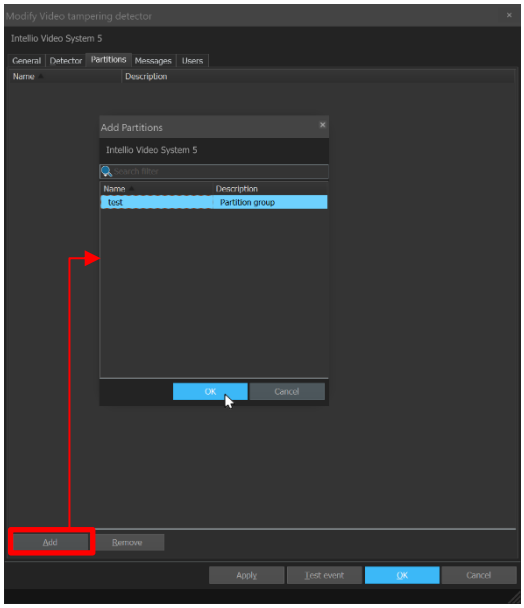
If it is not necessary for each event to have a separate sound, you can simply set the **Default Sounds** for the detector. These will be the default sounds for detector events: **Alarm** for alarm events, and **Signal** for signal events.

If you want these default sounds to apply to all detectors of this type, check the **Save these sounds defaults for detectors of this type** checkbox. You can also provide your own custom sound file by selecting **Add...** from the dropdown menu at the bottom. The selected sound file will be uploaded by the client to the SITE servers, from where other clients will download it upon their first login (see the **File repository**).

If you want each event to have a different sound, you can set the sounds for each event on the Messages tab.

5.2.2. Partitions

The list of partitions to be activated by the detector alarm can be specified here. The partitions only respond to normal events, ignoring technical events.



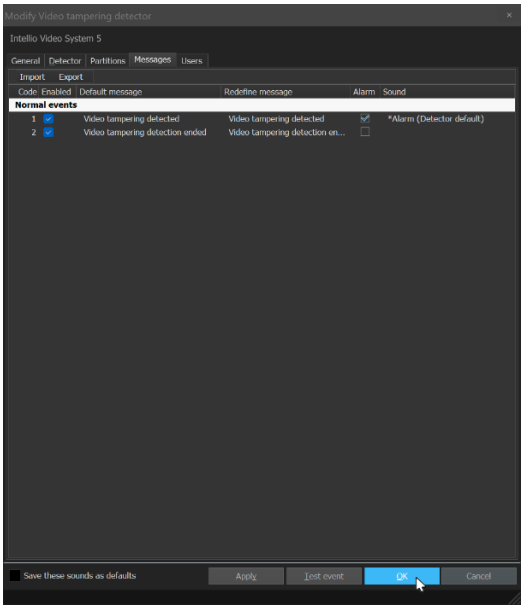
***Important**: **if all the partitions associated with a detector are inactive, the detector will not transmit events and alarms!** If the detector must always be active, it is recommended to add an always-active partition without any actions to the list of partitions associated with the detector.*

5.2.3. Messages

It is possible to set which events of a given detector are allowed and whether they appear as alarms or simple signals.

If an event type is checked in the **Alarm** column, an alarm will be triggered when the corresponding event occurs (e.g., the alarm will appear with a red background in the Events panel at the bottom of the Live View).

If only the left-side Enabled box is checked, then only a **signal** will occur (e.g., the signal will appear in yellow in the Events panel).



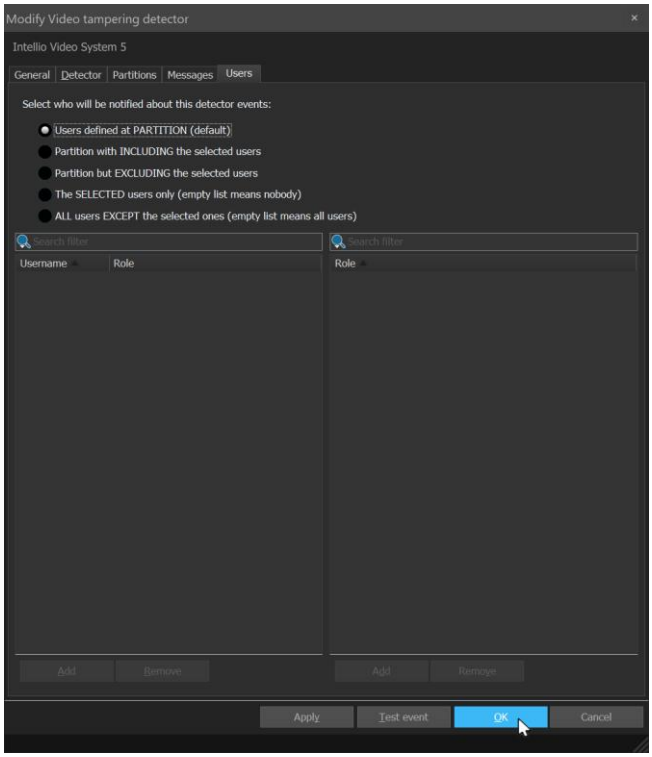
You can override the default sounds with custom event sounds. In the **Sound** column, you can open the dropdown menu and select any sound that will play when the event occurs. You can also select your own sound file by clicking the **Add** option at the bottom of the list.

These settings can also be saved to the detector type by checking the **Save these sound as defaults** checkbox at the bottom.

The settings in the Messages tab can be exported and imported, allowing the same message settings to be imported into multiple cameras with the same type of detector.

5.2.4. Users

On this tab, you can specify which users or roles should receive notifications about detector events:

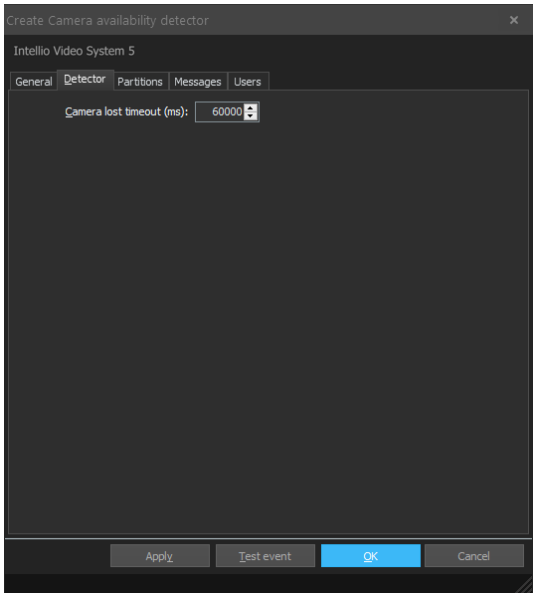


- **Users defined at PARTITION (default):** In this case, only the users and roles specified for the partitions assigned to the detector will receive detector events.
- **Partition with INCLUDING the selected users:** Users and roles specified for the partitions assigned to the detector will receive events, supplemented by those listed here.
- **Partition but EXCLUDING the selected users:** Only the users and roles specified for the partitions assigned to the detector will receive events; those listed here will be excluded.
- **The SELECTED users only (empty list means nobody):** In this case, users and roles specified for the partitions assigned to the detector will not be considered; only those listed here will receive notifications. An empty list means nobody will be notified.
- **ALL users EXCEPT the selected ones (empty list means all users):** In this scenario, everyone will receive events except those listed here. An empty list means everyone will receive notifications.

5.2.5. Detector

The unique settings specific to the detector can be configured on this tab, following the sections below.

5.3. Camera Availability detector



This detector triggers an alarm if any registered camera becomes unavailable for any reason (power outage, malfunction, vandalism, etc.). The detector does not identify the cause of the issue; it only indicates the loss of connection. Additionally, the detector signals when a camera becomes available again and notifies when all cameras in the system are accessible.

The detector has a single configuration option:

- **Camera lost timeout:** The duration after which the detector triggers an alarm if the camera is still unresponsive to the server. The default value is one minute (60,000 ms).

5.4. Site state detector

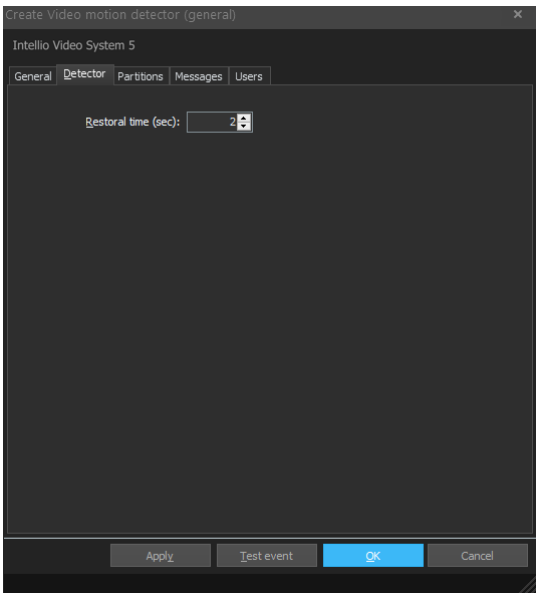
This detector monitors the SITE itself and immediately triggers an alert if one of the SITE's servers becomes unavailable. Since the detector operates automatically, the Detector tab is entirely absent.

Additionally, the detector notifies when a connection is established between two servers. In a multi-server SITE, this can generate a significant number of messages, as each server connection event is reported separately.

In multi-server SITE setups, this detector can be highly useful for early detection of server failures. Due to redundant operation, short server outages may go unnoticed by operators, depending on the configuration. However, with this detector, the system administrator will be notified of such events.

5.5. Video motion detector (general)

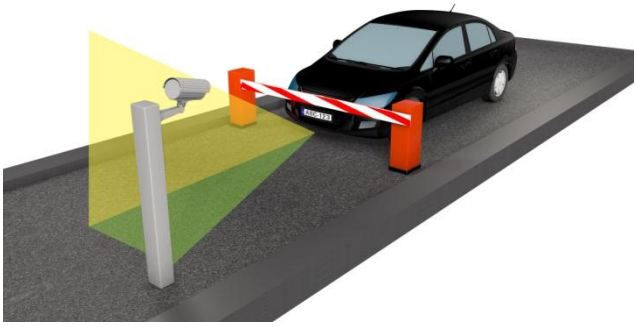
It essentially converts the camera's built-in motion detection signals into events. These generated events can then be used within the alarm system to trigger various actions.



- **Restoral time:** The duration the detector waits before sending the restore signal. If the monitored area has significant movement, it is recommended to set a higher value. Conversely, if motion detection is infrequent, a lower value can be used. This helps prevent excessive repeated alerts.

5.6. Automatic number plate recognition (ANPR/ALPR)

License plate recognition is performed on the server side. For configuration, be sure to read the ***License Plate Recognition*** documentation.



The detector tab is completely absent from the configuration window; the settings for recognition properties must be done at the camera associated with the detector, under the **System Configuration / Devices / Cameras** menu, in the **License Plate Recognition** tab.

5.7. VisiScanner analytics

It is a complex gender and face detection detector that can estimate a person's gender and age based on their facial structure. This detector is not suitable for real-time filtering, but it is an ideal tool for statistical data collection.

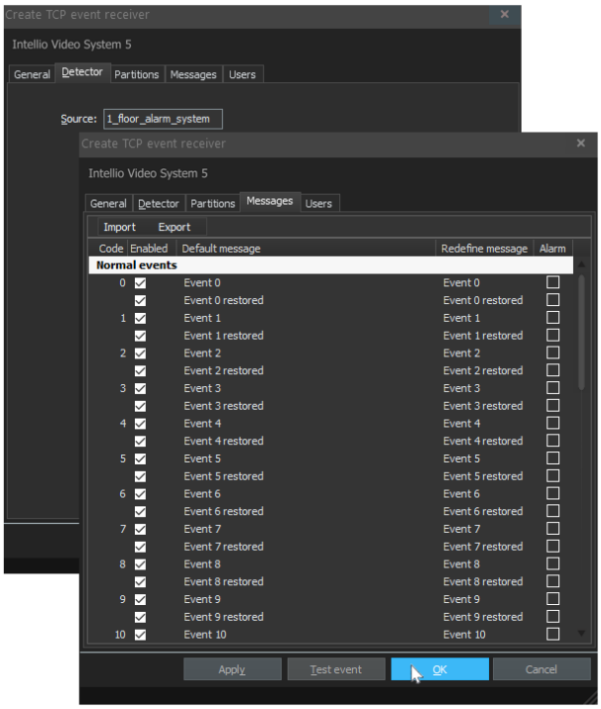
Configuration options:

- **Search levels:** Defines the area within which the detector searches for facial characteristics. The pixel-based size is displayed above the i symbol. Smaller target faces (with fewer pixels) require more processing time and result in lower accuracy.
- **Path selection:** Specifies the direction of movement for detected individuals. With proper configuration, the detector will only analyze faces of individuals moving in the selected direction, reducing unnecessary detections.

- **Show frontal time in event:** When enabled, this option records the **timestamp** of the moment when the detected person was facing directly toward the camera. This helps improve facial recognition accuracy.

Important: *The VisiScanner consumes significant server resources, requiring careful planning before deployment. For precise configuration, ask the detailed setup guide!*

5.8. TCP event receiver



With the TCP event receiver detector, it is possible to transmit externally received **camera alarm events** and **overlay text** to the IVS system via a TCP connection. Each TCP event receiver detector must be assigned to a specific camera, ensuring that the triggered event or overlay text is linked to the selected camera. Therefore, the TCP event receiver detector must be configured for both functions.

You can add as many TCP event receiver detectors to the system as the number of **TCER licenses** available in the product key.

The **Source** specified on the **Detector** tab is the identifier used to match incoming TCP events with the appropriate detector and, through it, the corresponding camera. The identifier can be any text and may be assigned to multiple detectors. In this case, the incoming signal will appear in multiple detectors, allowing multiple cameras to be triggered into an alarm state.

On the Messages tab, you can assign a user-defined message to **Event Codes** and configure whether the detector should enter an alarm state. This setting is only necessary when triggering an alarm event; if you only intend to use the overlay text function, these settings are not relevant.

The Intellio server TCP event receiver detector listens on **TCP port 53541**. The external application must connect to this TCP port.

Trigger an alarm event:

<EVENT>

<SOURCE> *source identifier string*</SOURCE>

<CODE> *event code (0-31)*</CODE>

<TYPE> *event type (signal/restore/event)*</TYPE>

</EVENT>

Add an overlay text:

<EVENT>

<SOURCE> *source identifier string***</SOURCE>**

<CODEPAGE> *character codepage identifier (optional)***</CODEPAGE>**

<FIXEDFONT>*true (optional)***</FIXEDFONT>**

<OVERLAYTEXT> *overlay text, can be multiline* **</OVERLAYTEXT>**

<OVERLAYTIME> *display time in milliseconds (optional)* **</OVERLAYTIME>**

</EVENT>

When formatting, ensure that values are always placed between the opening element's > and the closing element's </ marks (e.g., do not add spaces or line breaks to the identifier text).

- **Source identifier (SOURCE):** Every TCP event receiver detector must have this specified, determining which detector receives the message. Multiple TCP event receiver detectors can be created with different source IDs, or multiple detectors can share the same source ID. In the latter case, if a message arrives with that ID, all matching detectors will receive it.
- **Event code (CODE):** Must be a value between 0–31. The detector allows setting a text message for the event code and whether it should trigger an alarm or just a notification.
- The **TYPE** element is optional. If omitted, the IVS will interpret the message as a simple **event**. However, if **signal** is used, a corresponding **restore** must also be sent with the same event code!
- The "**overlay text**" will appear on the camera feed. It can be multiline, in which case it will display accordingly.
- **CODEPAGE** defines the character encoding for the OVERLAYTEXT. It can be "UTF8" or a code page number (e.g., 1250). If ANSI (7-bit) is sufficient, this can be omitted.
  More info: https://learn.microsoft.com/en-us/windows/win32/intl/code-page-identifiers
- **FIXEDFONT**: If set to "true," the text will use a monospaced font. If omitted, a variable-width font will be used.
- Display time (**OVERLAYTIME**): Specifies how long (in milliseconds) the overlay remains on the camera feed. If omitted, the text stays until the next OVERLAYTEXT message (to clear it, send an empty <OVERLAYTEXT></OVERLAYTEXT> message).

5.9. Multi IO Input detector

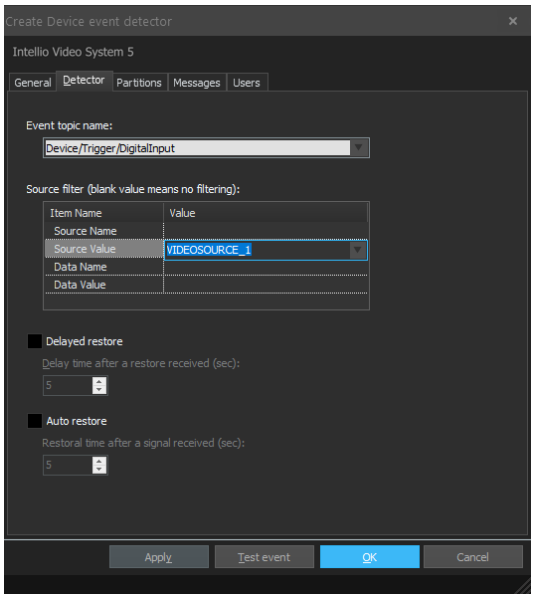
This detector triggers an immediate signal/alarm when activity is detected on the specified input Multi I/O or Modbus device port(s).

Configure the ports to be monitored on the appropriate device. A single detector can monitor multiple different ports.

5.10. Device event detector (ONVIF, Hanwha)

An event is triggered when a predefined alarm event occurs on the camera monitored by the detector.

To enable the detector, first configure the desired camera-side detector on the camera's web interface, then set the following parameters in the IVS:



- **Event topic name:** Select the detector signal channel set in the camera, through which the camera sends the signal for the specific detector. For example, if you want to receive the signal from the camera's contact input, you typically need to select the signal type named **Device/Trigger/DigitalInput**.
- **Source filter:** Allows server-side filtering based on the event source and data. The detector will only signal events that match the configured values. Fields left blank will not be filtered.
- **Delayed restore:** The time it takes for the detector to return to its idle state after the event ends.
- **Auto restore:** The time elapsed since the start of the alarm event after which the detector returns to its idle state. Since it's possible that the detector remains in the active state continuously during this period without additional alarms (e.g., continuous movement in front of the camera), it is advisable to set a high value.

5.11. SmartLive: server-side, live, Smart MetaData-based detectors

Based on the metadata of moving objects detected by **Intellio Initio**, as well as certain **Hanwha** and **Hikvision** cameras, **server-side Motion, Area Entry/Exit, Direction Detection**, and **Line Crossing** SmartLive detectors can be created to trigger immediate alerts. Within these detectors, the object category information detected by the cameras can be expanded or validated using the **SmartAI** feature.

For detailed information on SmartLive detectors and basic requirements, refer to the ***Smart features*** documentation.

5.12. Hidden PTZ preset detectors

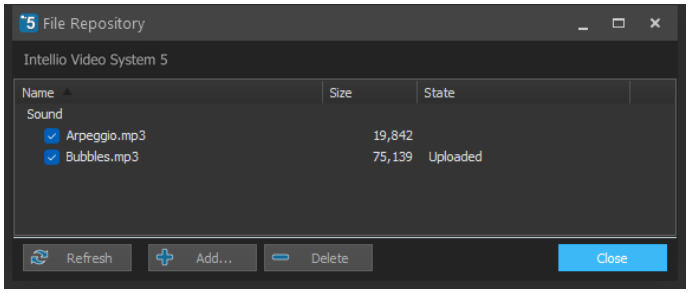
Hidden detectors help improve system efficiency, and under normal circumstances, users do not need to interact with them. The system automatically creates hidden detectors. Their parameters can be configured similarly to regular detectors, and their alerts can be used within the alarm system. Hidden detectors can be found under the **Hidden** group on the **System Configuration / Alarm / Detectors** page.

The hidden PTZ preset detector is required to support preset-based playback. A PTZ preset detector is automatically created for each preset (it cannot be created manually) and is deleted when the corresponding preset is removed. When a camera is removed, all associated PTZ preset detectors are also deleted.

6. File repository

Files uploaded from the client are stored on the servers in the **File Repository**. The SITE servers automatically synchronize the files with each other, and clients download them upon their first login. Currently, the File Repository only supports audio files.

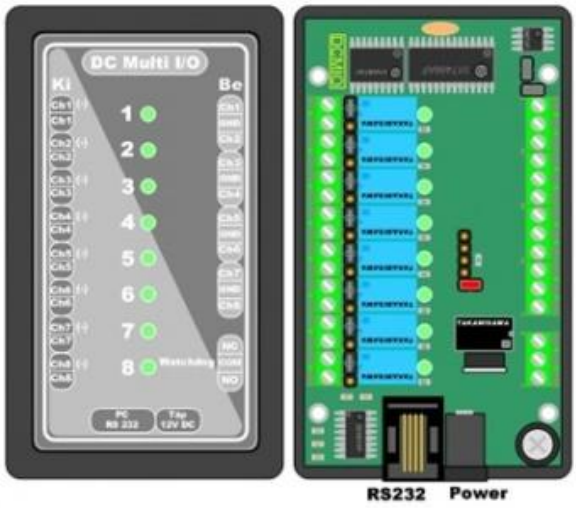
In the **Site / File Repository** window, you can edit the list of uploaded files. Use the **Add** button to upload a new file to the File Repository and the **Delete** button to remove it. The latter will physically delete the file from the servers. Use the **Refresh** button to update the list. If you do not want to delete a file but also do not want it to be synchronized to clients, uncheck the checkbox next to the file name.



7. Connection with other systems – the Input / Output Modules

7.1. Multi I/O module

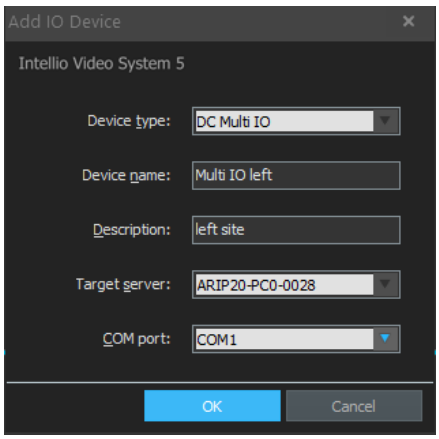
The Multi I/O is a specialized device that can be connected to the server's RS-232 port. It features 8 independent inputs and 8 independent relay outputs. The number of Multi I/O devices that can be connected to a single server is only limited by the number of RS-232 ports available on the server.



7.1.1. Specification

The diagram shows the layout of the Multi I/O device's inputs and outputs. The device requires a 12V DC power supply. On the left side of the device, there are eight relays (load capacity: 24V DC / 1A), while the inputs are located on the right side. The jumpers on the PCB allow you to configure the relay's default state: it is NO (Normally Open) if the jumper is placed, and NC (Normally Closed) if the jumper is removed.

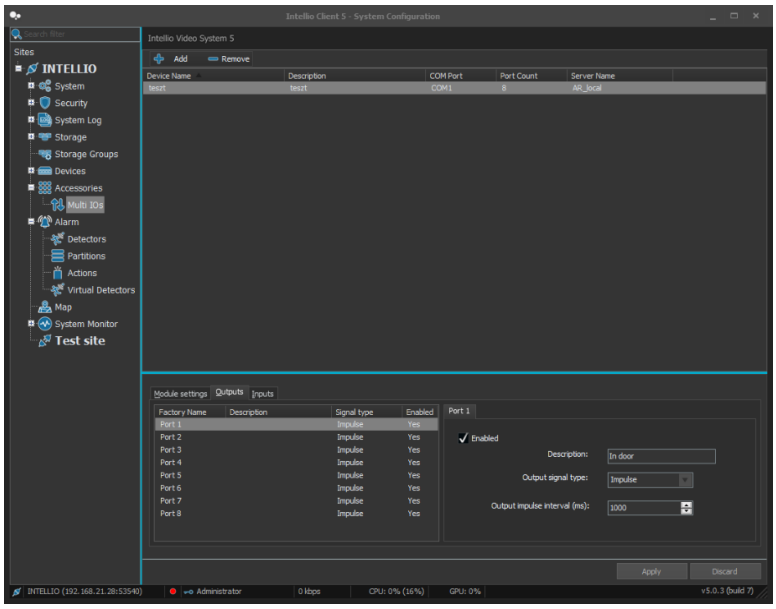
7.1.2. Configuration



- Add a Multi I/O device to the system in the **System Configuration / Accessories / Multi IO** menu using the **Add** button.
- In the **Add IO Device** window, enter the device name and description.
- Select the server to which the Multi I/O device is connected.
- Choose the communication port to which the device is connected.

After adding the device, further configuration is required. Select the added device and refine the settings:

- Enable the ports you want to activate.
- Enter the description and specify the output signal type. If set to **Pulse**, configure its duration.



After adding and configuring the device, creating a Multi I/O Input Detector is required to receive input signals, and creating a Multi I/O Action is necessary to control the output.

7.2. Modbus TCP I/O device

Using the Modbus TCP protocol, digital I/O devices (e.g., Moxa E12xx) can be connected to the IVS. With proper configuration, the IVS can receive input signals from these connected devices and also control their outputs. Since this protocol uses a TCP connection for communication, the connected devices automatically utilize the IVS **Camera Takeover** function (see ***Connect more servers – Site and Domain configuration*** documentation), ensuring high availability of controls.

Steps required to add a Modbus TCP device:

- Press the System Configuration / Devices / Add button, then select Add Modbus TCP I/O Device...
- In the wizard window that appears, enter the device's IP address, then press the Next button.
- The server will establish a connection with the Modbus TCP device at the specified IP address. For Moxa devices (if the Restful API is enabled), the server can query the default settings, which will appear in the next window of the wizard. When adding other Modbus TCP devices, 8 inputs and 8 outputs will be set by default.
- After precisely setting the parameters (see Modbus TCP device settings), you can add the device to the system by pressing the Finish button.

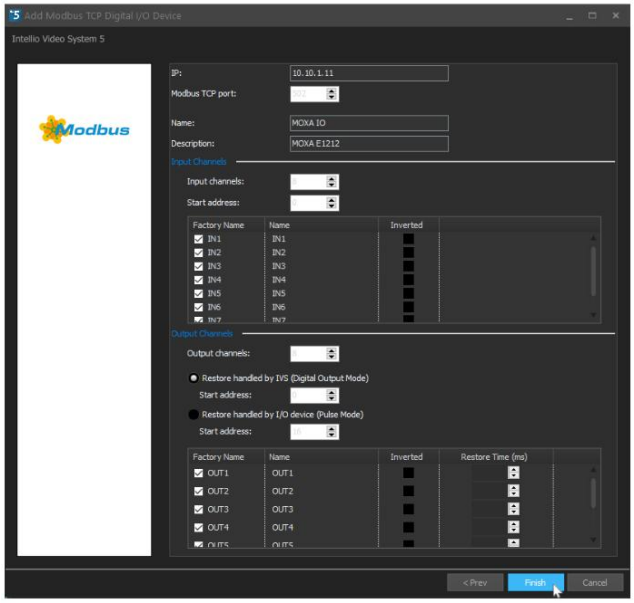
Note: *Do not forget that for proper functionality, the added device must be registered to one of the servers in the SITE, just like cameras.*

Modbus TCP device settings

To configure the parameters of a Modbus TCP device, press the **Configure** button on the **System Configuration / Devices / selected_device / I/O Ports** page, then make the necessary changes in the window that appears.

- In the **IP** field, enter the IP address used by the device.
- By standard, the default Modbus TCP port is **502**. If needed, modify it in the **Modbus TCP Port** field.
- In the **Name** and **Description** fields, enter the information used to identify the device.

Input channels:



- In the **Input channels** field, enter the number of inputs provided by the device (0–128). The input list will automatically update according to the value entered.
- In the **Start address** field, enter the address from which the inputs become available on the device.
  Note: *The start address may vary depending on the device. You can find the exact value for the digital inputs in the device's installation manual.*
- The list shows the settings for each input. For each input, you can change the name, enable or disable it individually, and invert its operation. Signals from disabled inputs will be ignored by the IVS.

Output channels:

- In the **Output channels** field, enter the number of outputs provided by the device (0–128). The output list will automatically update according to the value entered.

The IVS supports two ways of restoring the outputs:

- **Restore handled by IVS (Digital Output Mode):** In this case, the IVS server manages the output restoration. You must specify the restoration delay (in ms) for each output in the output list. You can also set the output to operate in inverted mode.
- **Restore handled by I/O device (Pulse Mode):** In this mode, the device fully controls the outputs. The IVS only activates the outputs. Other parameters (timing, inverted mode) must be configured through the device's own setup interface.

> ***Note:*** *Some devices use different start addresses depending on the mode (these can be found in the device's installation manual). Be sure to enter the correct start address for the selected mode in the* ***Start Address*** *field.*

The list shows the settings for each output. Each output can be renamed, enabled or disabled individually. IVS will not control disabled outputs. Depending on the selected mode, timing and default state inversion can also be configured.

To receive input signals from Modbus TCP devices, use the server-side **Multi IO Input detector**. To control the device's outputs, use the **Multi IO Action**.

8. Further steps

For an overview of additional system settings, please refer to the ***IVS Installation Manual*** documentation and continue configuring Users and access roles.