

**Digifort Explorer Manual**  
**Administration Client**  
**Version 7.4.2**  
**Rev. A**

# Index

<b>Part I Welcome to Digifort Explorer Manual</b>	<b>7</b>
1 Screen Shots.....	8
2 Who is this manual intended for?.....	8
3 How to Use this Manual.....	8
4 Prerequisites.....	8
<b>Part II Service Manager</b>	<b>9</b>
1 How To Run The Services Manager.....	10
2 How To Start Services.....	11
3 How To Stop Services.....	11
<b>Part III Basic Features of the Administration Client</b>	<b>12</b>
1 How to run the Administration Client.....	13
Interface .....	14
2 How to Configure the Servers to be Managed.....	14
3 How to Connect to a Server for Management.....	16
4 Multiple Object Configuration.....	17
5 Duplicate Objects.....	18
6 Extra Columns on Registration Screens.....	18
7 Export Data to CSV.....	19
8 Import Objects from Other Servers.....	20
9 Shortcuts to Registration Lists.....	21
<b>Part IV Licensing</b>	<b>22</b>
1 How to Configure Licenses.....	23
How to add a License .....	25
How to Send Registration Data .....	25
How to install licenses through Online Licenses .....	26
How to Install Licenses from License Files .....	27
Activating a Temporary License .....	27
Requesting a Demo license .....	29
<b>Part V Registering the software</b>	<b>31</b>
1 How to register the software.....	32
2 Registering the software Online.....	33
3 Registering the software Offline.....	34
<b>Part VI Recording Server</b>	<b>35</b>
1 How to Add a Camera.....	36

<b>Camera</b>	<b>37</b>
General	37
Extra Ports	39
Lenses	39
Panomorph Lenses	41
Fisheye Lenses	41
Motion Detection	42
Use Motion Detection by Software	42
Auto disable motion detection during PTZ	45
Use motion detection by device	45
Use motion detection by external notification	46
End detection interval and motion duration	46
Audio	47
Image Filters	47
<b>Streaming</b>	<b>48</b>
Media Profiles	48
How to add Media Profiles	49
How to view the functioning of the configured media profile	50
Disk space usage calculator	51
Audio	54
Recording	54
Snapshot Buffer	55
Live View	55
<b>Recording</b>	<b>56</b>
Settings	56
Recording Type	56
How to configure the recording schedule	56
Recording Cycle	61
<b>Rights</b>	<b>61</b>
Users	61
<b>PTZ</b>	<b>62</b>
Settings	62
PTZ Usage	63
Operation Scheduling	63
Presets	64
How to create a preset	65
Auxiliary	66
Joystick	67
Menu Control	68
Visual Joystick	69
<b>Events</b>	<b>70</b>
Communication	70
Communication Failure Event	70
Connection restore event	70
Device failure report	70
Recording Failure Event	71
Motion Detection	71
How to configure motion detection event	72
Event Variables	72
<b>Privacy</b>	<b>74</b>
Privacy Mask	74
<b>Multi-Channel Device Registration</b>	<b>76</b>
<b>Import Cameras From Other Servers</b>	<b>79</b>
<b>Finding and Registering Cameras Automatically</b>	<b>80</b>

Single Camera Registration.....	81
Multiple Camera Registration.....	82
<b>2 How to Delete a Camera.....</b>	<b>83</b>
<b>3 How to Change Parameters for Multiple Cameras Simultaneously.....</b>	<b>83</b>
Recording Directory .....	84
Add, Modify or Delete Media Profiles .....	85
Grant and Deny User Rights .....	86
<b>4 Camera Groups.....</b>	<b>87</b>
<b>5 Monitoring Recording Server Status.....</b>	<b>89</b>
Individual Camera Details .....	90
Recording Connection.....	90
Connections.....	91
Schedulings .....	92
Disk .....	93

## **Part VII Alerts and Events 95**

<b>1 How to Access Alerts and Events.....</b>	<b>96</b>
How To Configure Contacts .....	96
How To Add A Contact.....	97
How To Set Up Contact Groups .....	98
How To Add A Contact Group.....	98
<b>2 How to configure event actions.....</b>	<b>99</b>
Send an email to a group of people when an alarm occurs .....	101
Display images from cameras on the operator screen .....	102
Play an alarm sound in the Surveillance Client .....	103
Send instant message to operator .....	103
Call camera presets .....	104

## **Part VIII User Management 105**

<b>1 Adding, Changing, and Deleting Users.....</b>	<b>106</b>
User Account Info .....	108
2 Factor Authentication.....	109
User Rights .....	110
Video Playback and Search.....	110
Live Audio.....	110
Surveillance View s.....	110
System Cameras.....	111
Alarms .....	111
System Users .....	111
Alerts and Events.....	111
Server .....	111
Surveillance Client Features .....	111
Policies .....	113
Ownership Identification .....	113
Web Customization.....	114
General User Remarks .....	114
Groups View .....	115
Rights View .....	115
<b>2 Monitoring User Activities.....</b>	<b>116</b>
<b>3 How To Change Parameters For Multiple Users Simultaneously.....</b>	<b>117</b>



<b>4 Adding, Changing, and Deleting Groups.....</b>	<b>118</b>
Group Rights .....	120
Surveillance Client Features .....	120
Policies .....	120
Rights View .....	121
<b>5 Options.....</b>	<b>121</b>
Security .....	121
Force use of strong password.....	121
OTP .....	122

## **Part IX Layouts Management 123**

<b>1 How To Access Layouts Management.....</b>	<b>124</b>
How To Add A Layout .....	124

## **Part X Settings 127**

<b>1 System.....</b>	<b>128</b>
General .....	128
Recordings .....	129
Recording Encryption.....	129
Advanced.....	129
Multicast .....	130
Backup .....	130
Backup Structure.....	131
Restoring Backups.....	132
Settings .....	132
Folders .....	132
Database .....	133
Database .....	133
SMTP .....	134
Disk Limits .....	135
Network Units .....	136
Protocols .....	137
<b>2 Server Events.....</b>	<b>138</b>

## **Part XI Server Information 140**

<b>1 Disk Usage.....</b>	<b>142</b>
<b>2 Monitoring.....</b>	<b>142</b>

## **Part XII Web Server 144**

<b>1 Settings.....</b>	<b>145</b>
<b>2 File Server.....</b>	<b>145</b>

## **Part XIII RTSP Server 147**

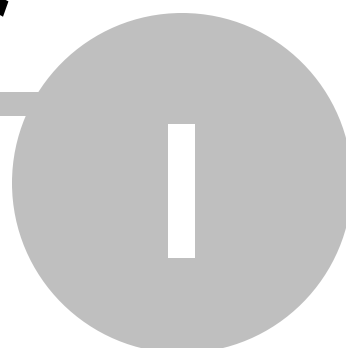
<b>1 Settings.....</b>	<b>148</b>
<b>2 Status.....</b>	<b>148</b>

## **Part XIV Logs 151**

<b>1 System Logs.....</b>	<b>152</b>
---------------------------	------------

How To Configure System Logs .....	152
How To View System Logs .....	152
2 Event Logs.....	153
How To Configure Event Logs .....	153
How To View Event Logs .....	154
3 Audit.....	154
<b>Part XV SSL Certificates</b>	<b>157</b>
1 How to Generate a Self-Signed Certificate.....	158
2 Converting Certificates to PFX Format.....	160
<b>Part XVI Clients auto-update</b>	<b>162</b>
<b>Part XVII Database Maintenance</b>	<b>165</b>
1 Backup.....	166
2 Restore.....	166
3 Maintenance .....	167
<b>Part XVIII Centralized Server List</b>	<b>168</b>
<b>Part XIX Mobile Camera</b>	<b>171</b>
1 How to start the Mobile Camera Server service.....	172
2 How to configure the servers to be managed.....	173
3 Configuring the Mobile Camera server.....	174
Mobile Devices .....	174
Settings .....	175
Status .....	176
4 Configuring the Application.....	177
5 Registering the Camera on the VMS Server.....	180
<b>Index</b>	<b>0</b>

# Chapter



# 1 Welcome to Digifort Explorer Manual



This User Manual and Technical References provide all the information necessary to effectively implement and use all the basic and advanced features found in the Digifort System Administration Client.Explorer.

This manual is constantly updated and does not describe the functionality of the Beta and DEV versions of the system.

## 1.1 Screen Shots

The screen shots contained in this manual may not be identical to the interface you will see using the software. Some differences may appear, not affecting the use of this manual. This is due to the fact that frequent updates and inclusion of new features are carried out aiming at the continuous improvement of the system.

## 1.2 Who is this manual intended for?

This manual is intended for administrators of the system.

## 1.3 How to Use this Manual

This manual is structured into chapters, topics and subtopics.

### **Important:**

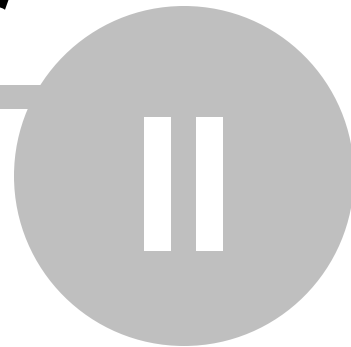
- If your edition is not Enterprise, some features shown may have limitations. To find out the differences of your edition, consult the Feature Matrix table on the website <https://www.digifort.com/>
- The screenshots in this manual are originally taken from the Enterprise edition. For this reason, even in other versions, some resource may present a snapshot with a different screen of the version of your software. We are constantly updating this manual and improving its content.

## 1.4 Prerequisites

For the complete absorption of the content of this manual some prerequisites are necessary:

- Handling computers and their peripherals.
- Microsoft Windows operating system handling.
- Knowledge of client-server architecture.
- Knowledge of computer network architecture.

# Chapter



## 2 Service Manager

The Digifort System is a VMS software developed on the client-server platform, taking advantage of all the resources and benefits that this platform provides.

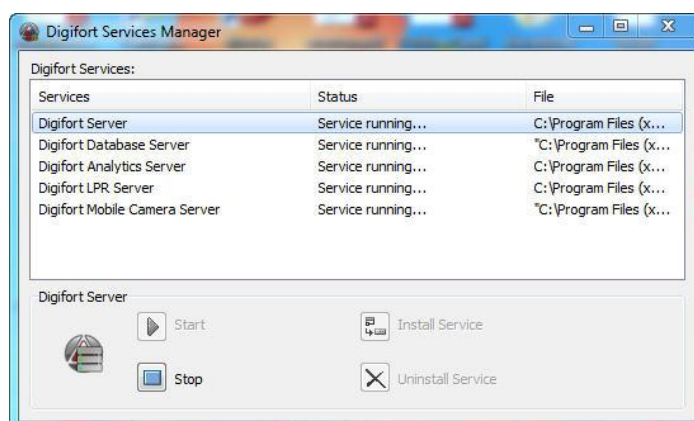
In the client-server platform, all information is stored on a central server responsible for its management. In the case of the Digifort System, the server is the component responsible for, among other functions, keeping the recordings generated by the images provided by the cameras, managing disk space, alerting operators and administrators about system anomalies and providing information to customers.

The Digifort Server is an application that runs as a Windows service, so it runs automatically when Windows starts, without the need for user intervention.

The Service Manager is the software responsible for controlling its execution, showing information about its operating status and providing installation and service startup controls.

### 2.1 How To Run The Services Manager

To run the Service Manager, locate the Service Manager icon on your Desktop, or in the start menu and run it. The Service Manager will start by opening the screen illustrated in the figure below:



The Service Manager provides the following functionality:

- **Digifort Services:** Displays the list of available services that can be managed.
- **Start:** Starts the selected service. Only available if the service is installed and stopped.
- **Stop:** Stops the selected service. Only available if the service is installed and started.
- **Install Service:** Installs the selected service, also allowing the selection of the architecture (32 or 64 bits) to be installed. Only available if the service is uninstalled.
- **Uninstall Service:** Uninstalls the selected service. Only available if the service is installed and stopped.

For the system to function, the following services must be in operation:

"**Digifort Server**" responsible for managing recordings and communicating with clients.

"**Digifort Database Server**" responsible for managing the system database.

For the video analysis modules to work, the "**Digifort Analytics Server**" must be running on any machine on the network.

For the LPR modules to work, the "**Digifort LPR Server**" must be running on any machine on the network.

For the Digifort Mobile Camera module to work, the "**Digifort Mobile Camera Server**" must be running.

## 2.2 How To Start Services

To start the a system service, it must first be installed, follow the steps below to correctly start the service:

1. Select the desired service
2. Click "**Install Service**", a confirmation window will appear, informing you that the service has been successfully installed. The "**Install Service**" button will only be available if the service manager is running in the same folder as the service to be installed.
3. Click Start and wait while the server starts. The boot process ends when the message "**Service is running...**" appears in the status bar.

### Note

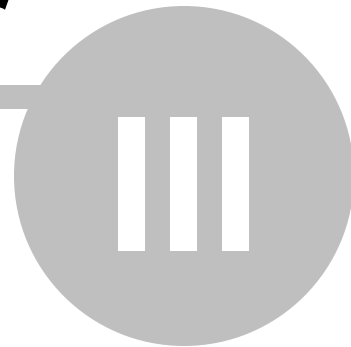
If the server has been stopped for some reason and started again, the initialization process can be time consuming, as a check is performed on all existing recordings, creating a map of the disk structure.

## 2.3 How To Stop Services

At any time, the execution of system services may be interrupted. By performing this action, the server will no longer perform any function, such as managing alarms and recording cameras.

The process of stopping services is quite simple, just clicking the **Stop** button. If the service is stopped successfully, the message "**Service stopped...**" should appear in the status bar.

# Chapter





## 3 Basic Features of the Administration Client

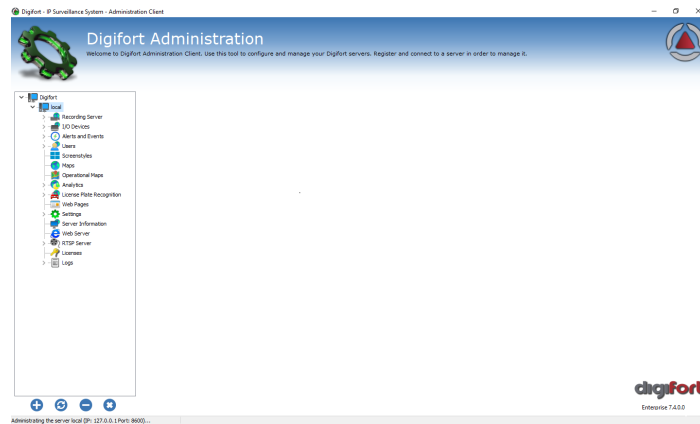
The Administration Client is the system module responsible for configuring the server. In this module you can, among other functions, register cameras, program alarms, check the server status and define the users who will have access to the system, among other administrative activities.

The Administration Client can manage unlimited servers simultaneously, simply by registering the desired servers.

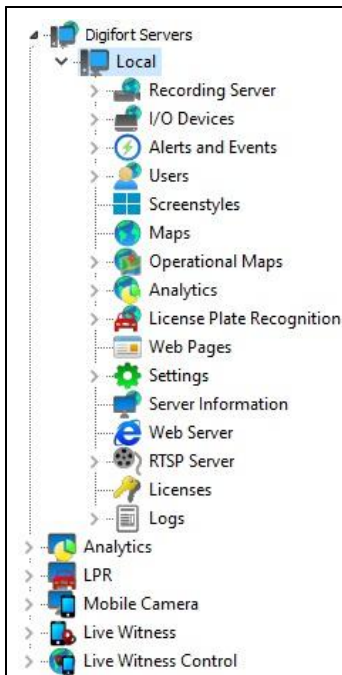
The Administration Client can be used to manage and configure different types of system servers, such as VMS Server, LPR Server, Analytics Server, among other modules.

### 3.1 How to run the Administration Client

To access the Administration Client, locate the Administration Client icon on your Desktop or in the Start Menu->Programs->Digifort->Administration Client and run it. The Administration Client will start as shown in the figure below:



The Administration Client provides the following initial settings:



**Settings menu:** This menu displays the settings available for the selected server. Settings are displayed in a tree format, that is, with items and sub-items. To access some server configuration, click on the desired menu. Settings related to the selected item will be displayed in the reserved area to the right of this item.

### 3.1.1 Interface



**Add Server:** Starts adding a server. Use this button to add servers that will be managed by the Administration Client.



**Change Server:** With the server selected, when activated, the option opens the screen to change the server settings.



**Delete Server:** Deletes selected server.



**Disconnect from server:** Terminates connection and management of the selected server. To disconnect from a server, select it in the Settings Menu and then click this button.

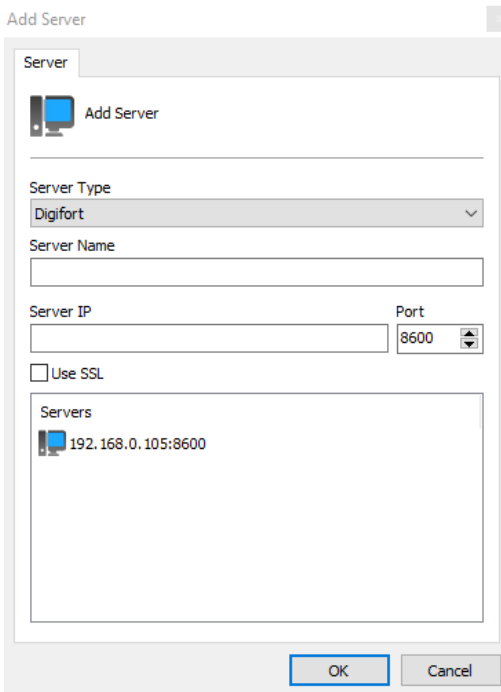


**About:** Displays system version information

## 3.2 How to Configure the Servers to be Managed

The first step to be carried out when configuring a server is to add it to the list of servers to be managed by the Administration Client.

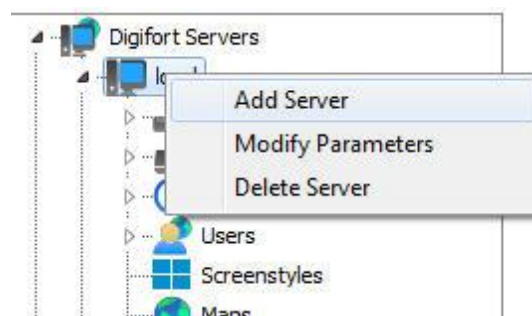
To add a server, click on the **Add Server** button, opening the server registration screen, as shown below:



- **Server Type:** The system has different types of services and modules. Select the type of server to add.
- **Server Name:** Enter the name of the server to be added. After confirming the data, the server name cannot be changed.
- **Server IP:** Enter the communication port with the server. By default the port is 8600 for standard connection or 8400 for secure connection with SSL/TLS.
- **Port:** Type the communication port with the server. By default the port is 8600
- **Use SSL:** Select this option to connect securely via SSL/TLS. The communication port will be changed to the default port 8400 and the server list will be updated to display only servers running with SSL/TLS.
- **Servers:** In this list, all servers of the selected type that the administration client found on the network will be available. By clicking on one of the servers, the **IP** and **Port** field described above will be automatically filled in, leaving only the Server Name field to complete the registration.

After entering all the data correctly, click **OK**.

After adding the server, it will be shown in the **Settings Menu** as shown in the figure below:

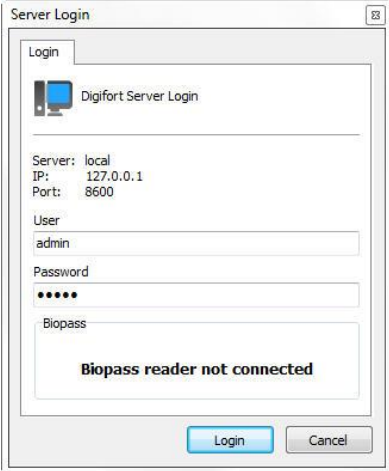


To change the parameters of an already saved server, right-click on the desired server and then click on **Modify Parameters**. In the window that opens, change the data as necessary and click **OK**.

To delete a server, right-click on the desired server and then click **Delete Server**. In the confirmation message that appears, click **Yes**.

### 3.3 How to Connect to a Server for Management

After adding the server, locate it in the Settings Menu and double-click on it or click on the arrow to the left of the server icon. Once this is done, a username and password will be required to access the server settings, as shown in the figure below:



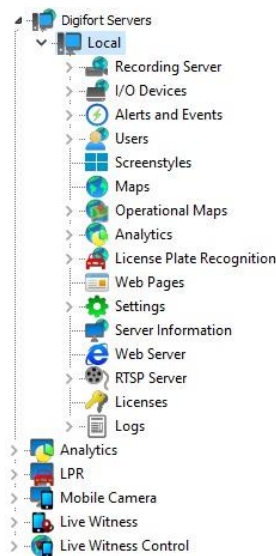
- **User:** Login User Name.
- **Password:** Access Password.

Enter the user name and password to access the server. If this is the first access to the system, inform the user equal to admin and a blank password.

If the user has 2-factor authentication, the 2-factor authentication screen will be displayed and you will be asked to provide the unique access password for your authentication application:



After filling in the access data, click **OK**. If the access authentication is successfully completed, the **Settings Menu** will be expanded, showing the available settings for the server, as shown in the figure below:

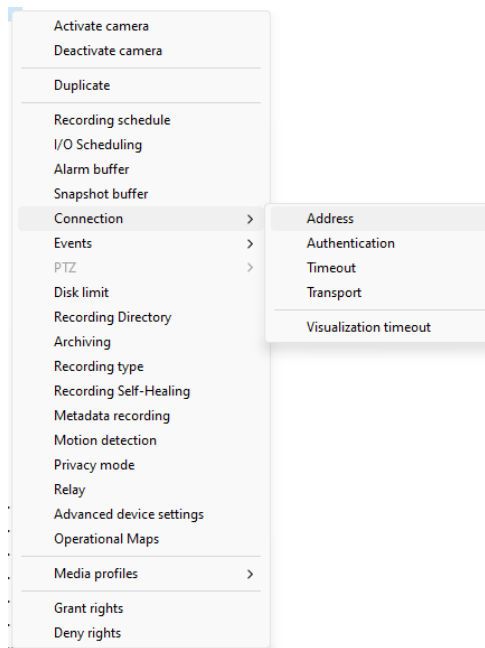


#### +Note

The admin user is the only user that cannot be removed from the system and has full access rights. For security reasons, a password must be entered to prevent access by unauthorized personnel.

## 3.4 Multiple Object Configuration

All main object registration screens in the system have an option for configuring multiple objects simultaneously, allowing common configurations to be applied to several selected objects. To access this feature, simply select the desired objects on a registration screen and click with the right mouse button. A popup menu will be displayed with options that you can change and apply simultaneously to all selected objects.

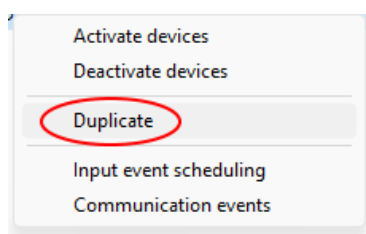


The example above is the camera registration options menu, where you can select multiple cameras and apply these settings to all cameras simultaneously. This feature is extremely useful for managing a large number of objects and will speed up the system administration process.

### 3.5 Duplicate Objects

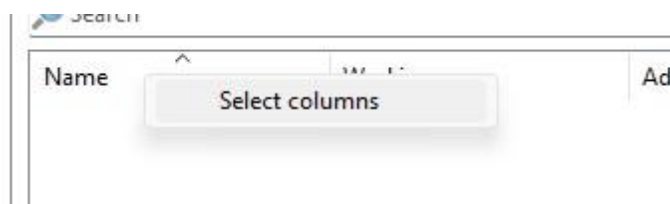
All of the system's main object registration screens allow duplication of objects, creating a new registration with the same information, just adding "-Copy" to the end of the name, allowing the creation of "templates" of already pre-configured objects and facilitating server administration.

To duplicate an object, on a registration screen, select the object, right-click and select the **Duplicate** option:

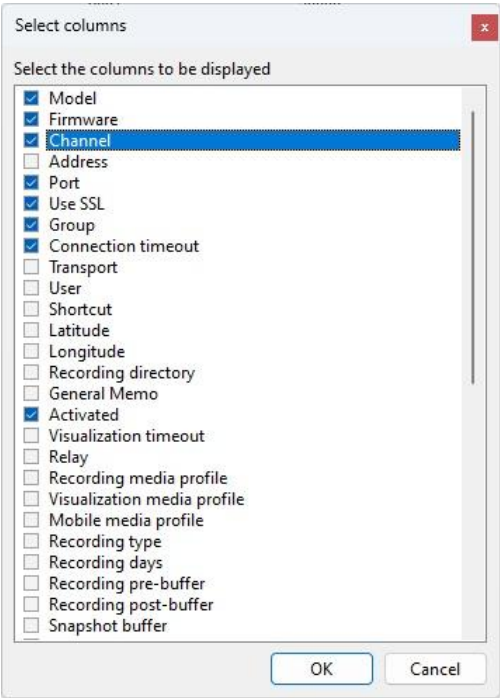


### 3.6 Extra Columns on Registration Screens

The vast majority of object registration or status screens allow the visualization of extra columns with extended object information. To access this feature, on a **registration** or **object status** screen, right-click on a column in the list and click on the **Select Columns** option:



A screen with the available columns will be displayed:



This feature becomes indispensable, providing a broad view of configuration parameters or object status:

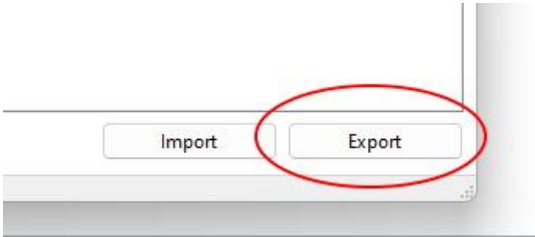
Port	Connection timeout	Use SSL	Recording Self-Healing	Metadata recording	Metadata type	Archiving days	Activated	Transport
8631	30000	Inactive	Inactive	Inactive		0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Inactive	Analytics	0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Active	Motion or Event	0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Active	Motion or Event	0	No	Auto
8601	30000	Inactive	Inactive	Active	Motion or Event	0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Active	Motion or Event	0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Active	Motion or Event	0	No	Auto
8601	30000	Inactive	Active (Camera Record...	Active	Analytics	0	Yes	Auto

You can also change the display order of columns by dragging and dropping them. The display order will be stored locally for each registration screen and will be remembered the next time you open the screen.

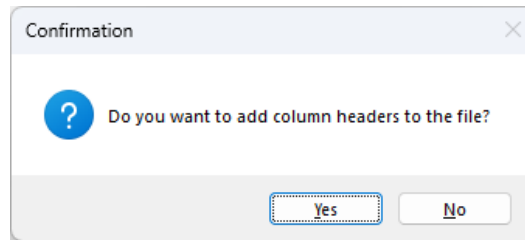
You can sort the list by clicking on a column.

3.7 Export Data to CSV

All main object registration and status screens have a button to export the object data on the screen in CSV format. The exported data will only be the data displayed on screens (with extra columns) and can be used for reports, controls or information. To export data from a registration or status screen, click the **Export** button, in the lower right corner of the list:



On the following screen you will select the .CSV file you want to create and then the system will ask you if you want to add the column names in the first line of the CSV file:



	A	B	C	D	E	F
1	Nome	Descrição	Modelo	Porta	Usuário	
2	Teste	Teste	Axis Q6124-E	80		
3	teste2	teste2	3S Vision N1071	80	root	
4	teste3	teste3	AeroGuard DJI	80	root	
5						
6						

#### +Note

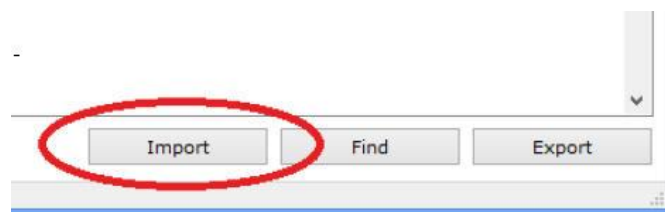
The exported data is informative only, contains only the information on screen and cannot be used to import the objects again on the same or another server. To import objects from another server, see the [Object Import feature](#)

## 3.8 Import Objects from Other Servers

Importing objects from a remote server is a tool that will help manage large system installations, greatly speeding up the configuration of a new server.

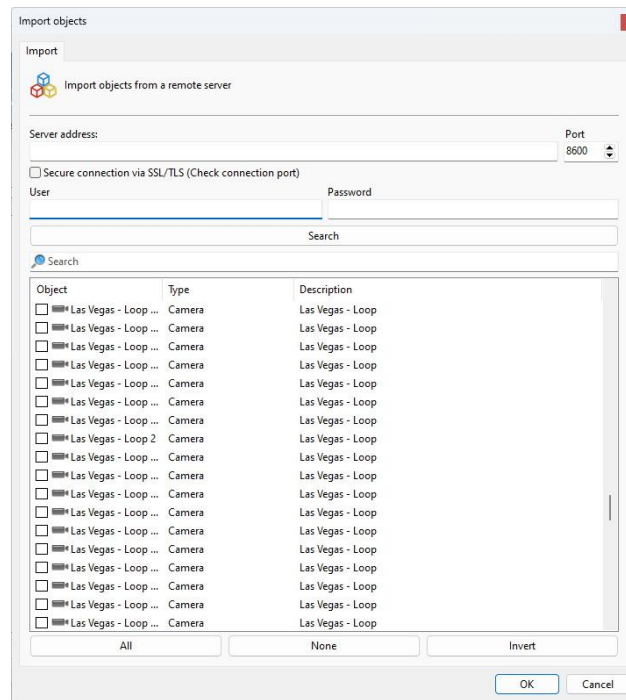
The system allows the import of any object such as Cameras, I/O Devices, Users, Analytics Settings, LPR, among others.

Every configuration screen that allows the import of objects has an **Import** button.



The object import screen will be displayed:





To import, simply enter the **IP** of the source server, the **server's communication port** and a system **username** and **password**. The objects that will be loaded will be those that the user has [management rights](#) under that type of object. Click **Search** and the objects will be shown in a list as shown in the image above.

Select the desired objects and click **OK** to import.

- **Server address:** Enter the address of the server from which you want to import the objects.
- **Port:** Enter the communication port with the server
- **SSL / TLS:** Select this option to make a secure connection to the server (Make sure the connection port is correct for the desired option).
- **User:** Authentication User
- **Password:** Authentication password
- **Search:** Download the list of objects for selection
- **All:** Selects all objects in the list to import
- **None:** Deselects all objects
- **Reverse:** Inverts the selection of objects

### 3.9 Shortcuts to Registration Lists

All system object lists have the following shortcuts:

- **INSERT:** Add a new object
- **SPACE:** Modify the selected object
- **DELETE:** Delete the selected object
- **F5:** Refresh the list by re-downloading objects from the server

# Chapter



IV

## 4 Licensing

To unlock the system and some functions, it is necessary to execute the software licensing.

There are several types of licenses and license packages. For more information, consult your reseller.

Licenses only work on the server for which the registration request was made, this is due to the fact that each server generates a different machine codes and licenses are generated based on this machine code, making them unique.

There are two methods of licensing, online licensing and offline licensing.

Licensing carried out over the internet is the safest and recommended, but if your server cannot access the internet, use licensing through license files.

### +Tip

As the system works on the Client-Server platform, the registration request does not need to be made by the server itself, that is, any other computer on the network can make this request through the Administration Client.

### +Important

If the recording server is formatted, a new machine code is generated by the server. Therefore, a new registration request must be made

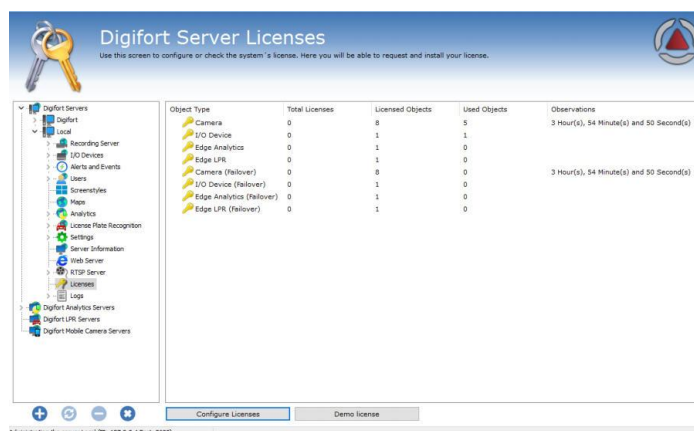
### 4.1 How to Configure Licenses

Before starting your server, make sure the HardKey (USB Dongle) that is sold together with the software is connected to your machine correctly.

To start licensing the system, after logging in to the server, locate the item Licenses in the Server Settings Menu, as illustrated in the figure below:



Once this is done, information on the current status of server licensing will appear on the right side, as shown in the figure below:



From this screen we can get the following information:

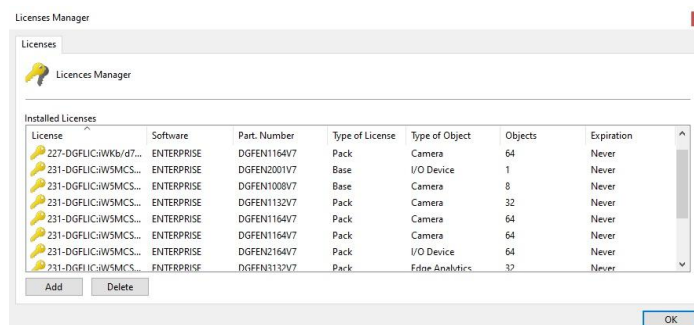
- **Total licenses:** Number of licenses installed on the server for a certain type of object.
- **Licensed objects:** Number of licensed objects for the object type.
- **Objects Used:** How many objects are currently using the licenses.
- **Observations:** Important license notes (If available) such as expiration time (of temporary license).

License types:

- **Camera:** License that allows you to record camera images.
- **I/O Device:** License to use the I/O devices.
- **Edge Analytics:** License to use embedded analytics.
- **LPR on Edge:** License for the use of LPR on board.
- **LPR Bridge:** License for the use of LPR middleware integration.
- **Multi-Channel Device:** License to use multi-channel devices such as NVRs
- **Camera (Failover):** Allows the use of the Failover feature for a certain number of cameras.
- **I/O Devices (Failover):** Allows the use of the Failover feature for a specified number of I/O devices.
- **Edge Analytics (Failover):** Allows the use of the Failover feature for a specified number of edge analytics.
- **Edge LPR (Failover):** Allows the use of the Failover feature for a specified number of Edge LPRs.
- **Multi-Channel Device (Failover):** Allows the use of Failover feature for a specified number of multi-channel devices such as NVRs

To learn more about licensing, consult your reseller.

To configure server licenses, click on Configure Licenses button. This action will run the License Manager, as shown in the figure below:



This screen displays all the licenses installed on the server. To add a license, click on the **Add button** and to remove a license, select the desired license and click on the **Remove button**.

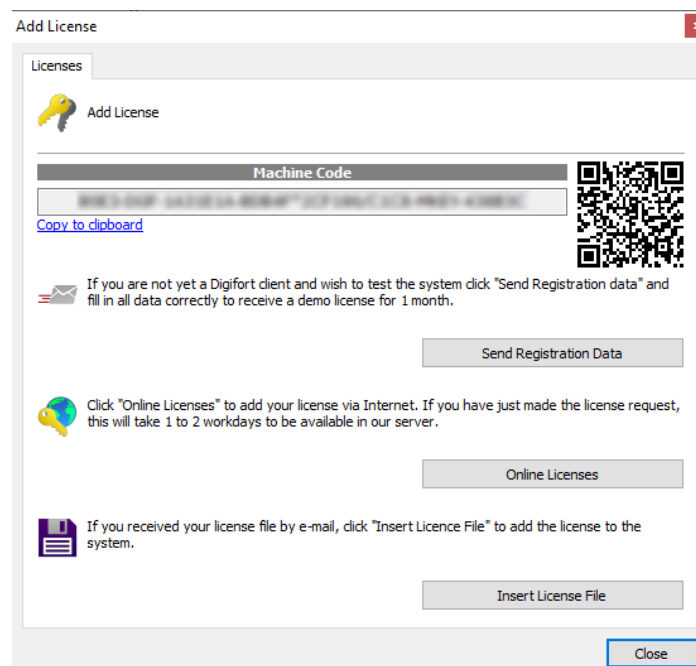
At the end of the settings, click on the **OK** button to close this screen.

### + Notes

- Each server has a unique machine-key and licenses are linked to each server's machine-key.
- The server machine-key is provided via software-key (using unique identifiers of the hardware where the server is installed) or via hard-key (USB key provided with the purchase of the system). When using software-key, the machine-key may be changed when the system detects a hardware change on the server. If the software-key is being used and the machine-key changes, contact your reseller.
- If the base license is removed, the pack licenses will not be loaded and will automatically disappear from the screen. Pack licenses are only loaded if the base license is installed.

## 4.1.1 How to add a License

To add a license, click on the Add button in the License Manager. The license addition screen will be displayed as shown in the figure below:



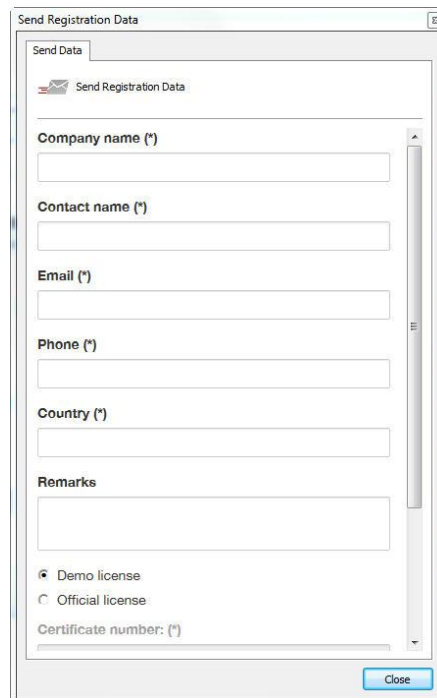
This screen shows the machine code generated by the software and provides resources for licensing. If you need to send the password to your reseller, just copy it by clicking **Copy to clipboard** or use a QR code reader to copy your machine code.

## 4.1.2 How to Send Registration Data

The first step in licensing the system is sending data for registration. This process consists of filling in the user data that will be sent together with the server password to the Licensing Center.

With the data in hand, the Licensing Center will generate the requested licenses and a confirmation that will be sent to the email provided.

To start the process of sending data to the registry, click **Send data to Registry**. This action will open a form for filling in the customer's data, as shown in the figure below:



After filling in the fields correctly, click on the **Submit button**. Your license will be generated within a maximum of two business days.

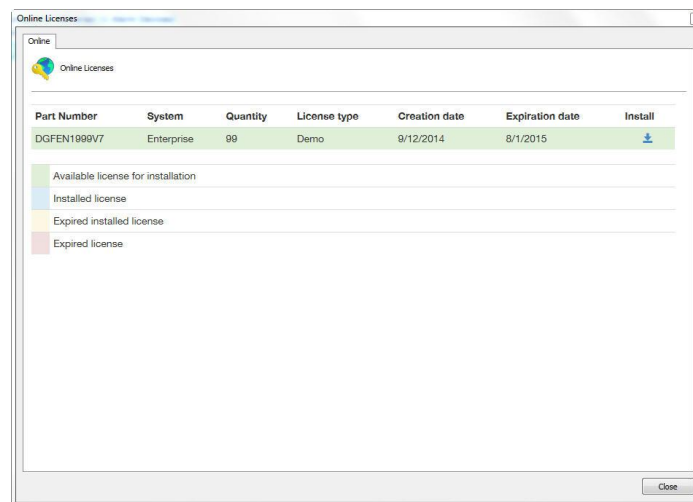
When your license is ready, you will receive a confirmation email with all license installation instructions.

These instructions will also be described on the next pages of this manual.

### 4.1.3 How to install licenses through Online Licenses

Licensing through "**Online Licenses**" is the safest and most practical method to license the system.

After receiving the license confirmation e-mail, click on the **Online Licenses** button. A window will open listing all licenses available for your server, as shown in the figure below:



To install the licenses, locate the desired license and then click on the icon in the Install column. In the case of installing official licenses, first install the base license and then all the pack licenses. And in case of installation of demo licenses install it normally.

After installing the licenses, click on the **Close** button.

#### 4.1.4 How to Install Licenses from License Files

If your server does not have internet access, you must use licensing through license files. To carry out this process, copy your server's machine code and send it by e-mail to Digifort, mentioning the version and edition used. Your license will be generated from this machine code. Soon after the license files will be sent to your email.

To install the license files on the server, copy these files to the server or any network drive that it has access to and click **Insert License File**. A window will open asking for the location of the license files.

Locate the files and open the base license file first and then all the other pack license files.

#### +Note

Some errors may occur using this licensing method. This is due to the fact that the licensing process is being carried out by means external to the server. The most common errors are: sending the wrong machine code and corrupting the license files sent by email. Therefore, if possible, always use the online licensing method

#### 4.1.5 Activating a Temporary License

The temporary license feature was created to facilitate the demonstration of the software. When activating the temporary license, the software will work for **FOUR HOURS**.

To activate the Temporary License, click on the **Demo License** button as shown in the figure below:

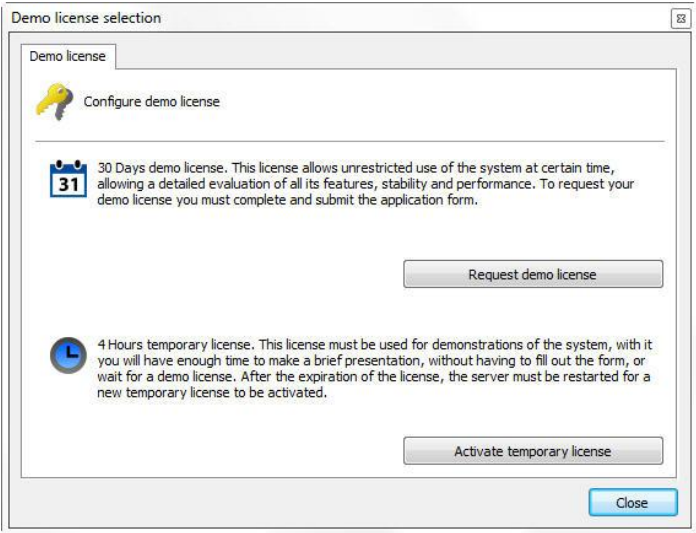
Total number of Licenses: 0 License(s) (0 Cameras) (0 Alarm Devices)

Temporary License: 0 Hour(s), 0 Minute(s) and 0 Second(s)

Configure Licenses

Demo license

Then click on **Activate Temporary License** as shown in the image below:



After clicking in the **"Activate Temporary License"** the following licenses will be activated for **4 hours**:

Object Type	Total Licenses	Licensed Objects	Used Objects	Observations
Camera	0	8	0	3 Hour(s), 59 Minute(s) and 59 Second(s)
I/O Device	0	1	0	
Edge Analytics	0	1	0	
Edge LPR	0	1	0	
LPR Bridge	0	0	0	3 Hour(s), 59 Minute(s) and 59 Second(s)
Camera (Failover)	0	8	0	
I/O Device (Failover)	0	1	0	
Edge Analytics (Failover)	0	1	0	
Edge LPR (Failover)	0	1	0	
LPR Bridge	0	0	0	

The system will allow you to use the following licenses for four hours:

- 8 Cameras
- 1 I/O Device
- 1 Edge Analytics
- 1 Edge LPR
- 1 LPR Bridge

And it's respective Failover Licenses.

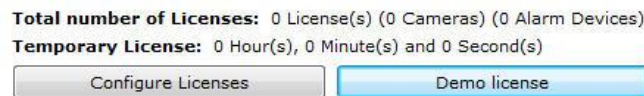
**+Note**

The temporary license is a free non feature-restricted license (only time-restricted), which means you can use an unlimited number of times. Once the period of 4 hours is expired, just simply stop the server service and start it again.

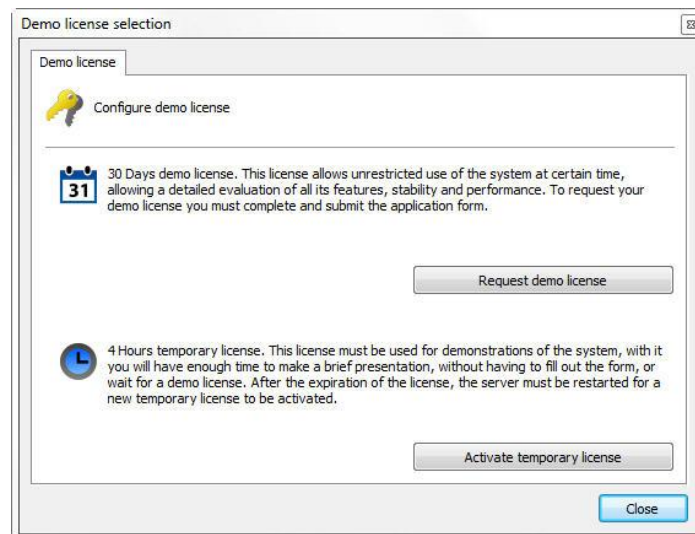


### 4.1.6 Requesting a Demo license

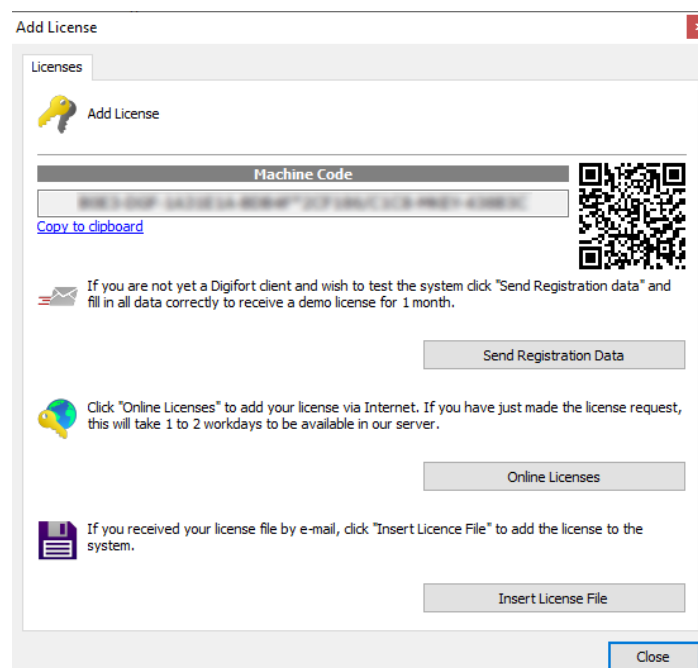
To request a Demo License click on the Demo License button as shown in the figure below:



Then click on **Request Demo License** as shown in the image below:

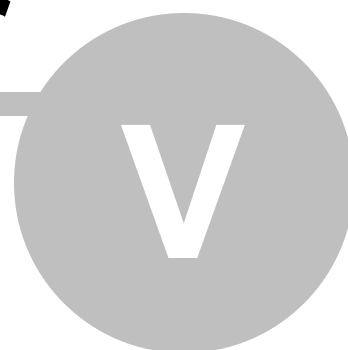


The main licensing window will appear. Click on **"Send Data for Registration"** and fill in the form details:



After filling out the form details, you will receive an email informing you that your license has been generated and you can install it following the steps previously described.

# Chapter



## 5 Registering the software

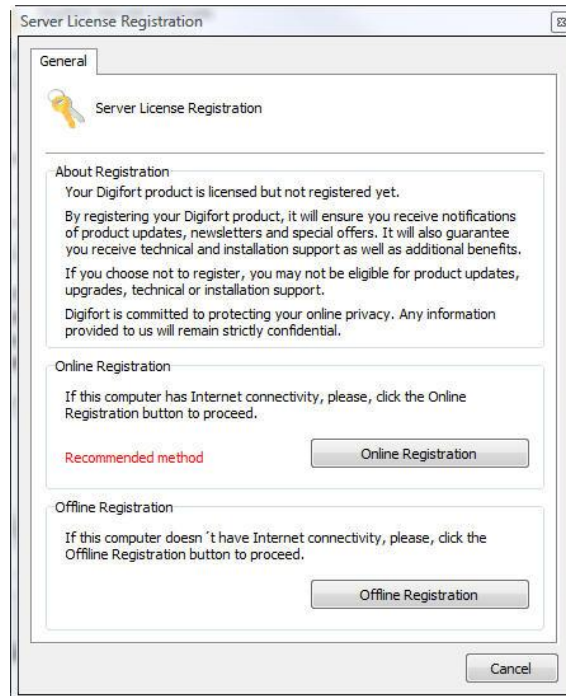
After licensing the software, it is necessary to register it. Software registration will ensure that you receive notifications of product updates, news and special offers. It will also ensure that you receive technical and installation support, as well as additional benefits.

If you choose not to register, you may not be eligible for updates, upgrades, technical or installation support.

By registering the software, you will receive a registration code that, for security purposes, will also be stored in our licensing center. If you use a hard key and it is necessary to format the server or reinstall the server, our licensing center will identify your server and automatically register it again.

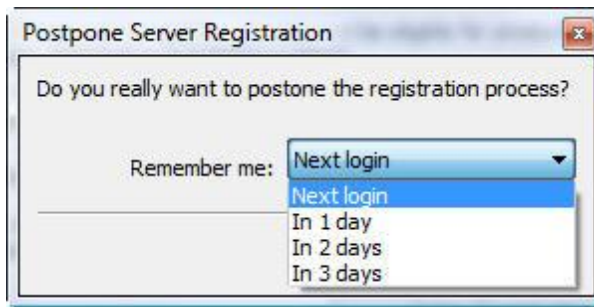
### 5.1 How to register the software

After inserting your official software license, the software registration window will be automatically displayed, as shown in the figure below. To learn how to install licenses, see [Licensing](#)



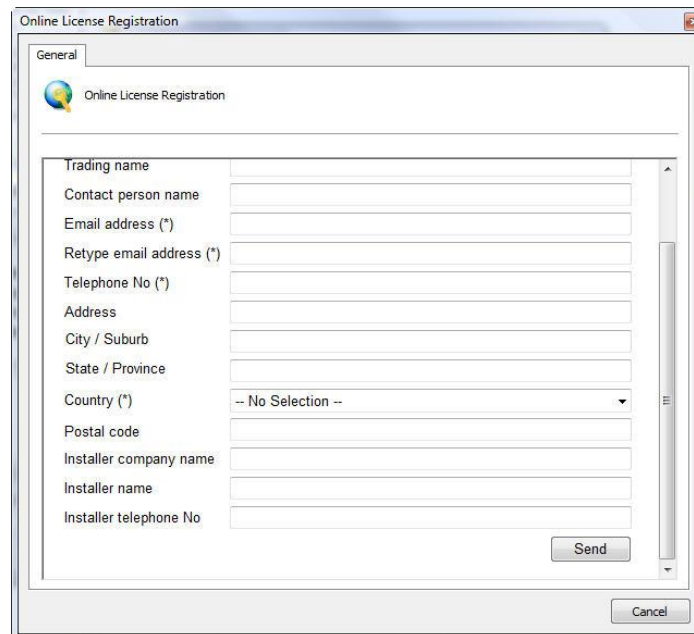
Server registration can be done in two ways, Online and Offline. The Online method is recommended, but it can only be used when the computer running the Administration Client is connected to the internet. The Offline method should be used when the computer does not have internet access.

If you want to register later, close this window and select the desired option, as shown in the image below:

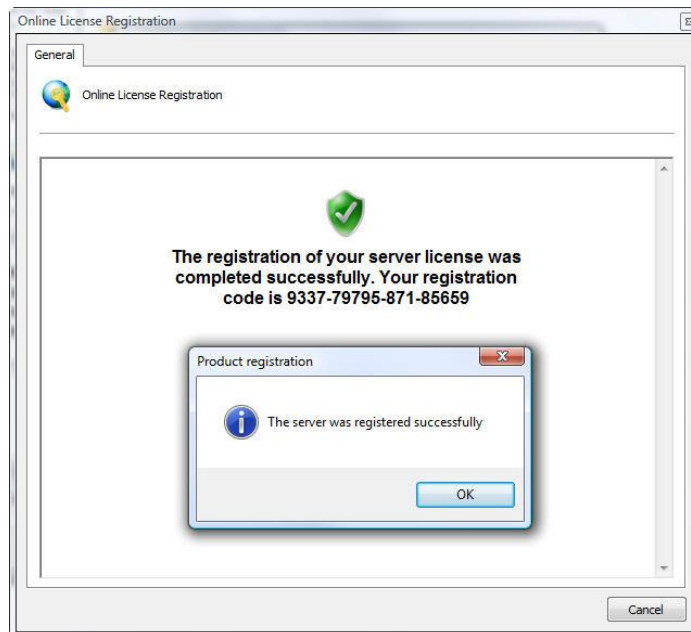


## 5.2 Registering the software Online

To register the server online, click on the Online Registration button. A window will appear with a form that must be filled out, as shown in the figure below:

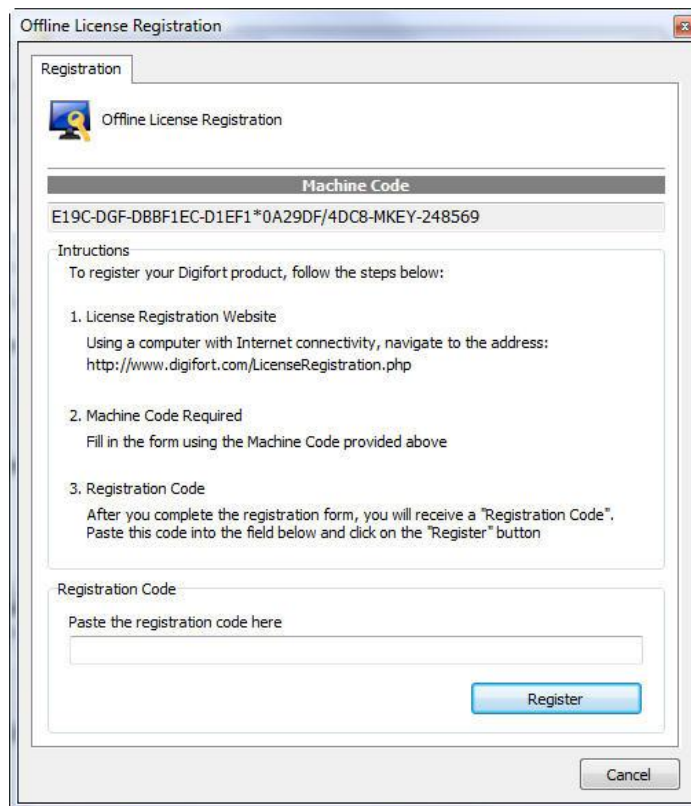
A Windows-style window titled "Online License Registration". It has a "General" tab selected. The window contains a form with the following fields: "Trading name", "Contact person name", "Email address (\*)", "Retype email address (\*)", "Telephone No (\*)", "Address", "City / Suburb", "State / Province", "Country (\*)" (with a dropdown menu showing "-- No Selection --"), "Postal code", "Installer company name", "Installer name", and "Installer telephone No". There are "Send" and "Cancel" buttons at the bottom right of the form area.

Fill in all fields and click Submit. The registration confirmation screen will be displayed along with your registration code, as shown in the figure below.



### 5.3 Registering the software Offline

To register the server offline, click the Offline Registration button. A window will appear with instructions on how to register the server. Follow the on-screen instructions and click **Register**.



# Chapter



VI

## 6 Recording Server

This chapter is dedicated to the system's Recording Server. It is in this module where the cameras are registered and their functioning is monitored.

The Recording Server is divided into two modules, the Cameras module, where the cameras are registered, and the Status module, where the functioning of the cameras is monitored. A single server can perform recording and monitoring functions. In addition, the system is able to work with two or more processors, dividing the processing and consequently increasing performance. There is no daily recording limit, that is, it is not necessary to move recordings to another disk drive and data transmission can be performed via local network, internet, wireless network or IP network.

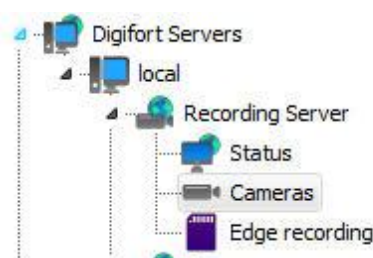
The system operates with the main brands of digital cameras on the market and accepts analog cameras as long as they are connected through the video-server device. These cameras can be located on the same site as the server or they can be remote, connected through some network connection. The main camera configuration attributes, such as image resolution, number of frames per second and viewing rights, are configured in the system and automatically applied to the cameras, regardless of their location and without stopping the recording of other cameras. In addition, some camera models allowing such settings to be made directly from the administration client, as can be seen in Advanced Device Settings.

Performing tasks such as recording, video playback, system settings, event consultation, live monitoring, image location are possible so that one task does not generate reflections on another.

The Camera Register is one of the most critical parts of the system, as a wrong configuration can lead to system malfunction. Therefore, good planning must be carried out in advance, gathering data such as the number of cameras, desired frames per second, days of storage, available disk space, etc.

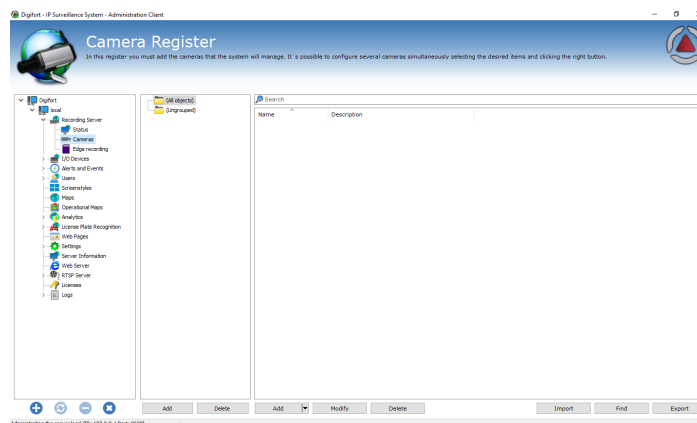
### 6.1 How to Add a Camera

To access the Camera Register, locate the Recording Server icon and then click on the Cameras icon, as shown in the figure below:



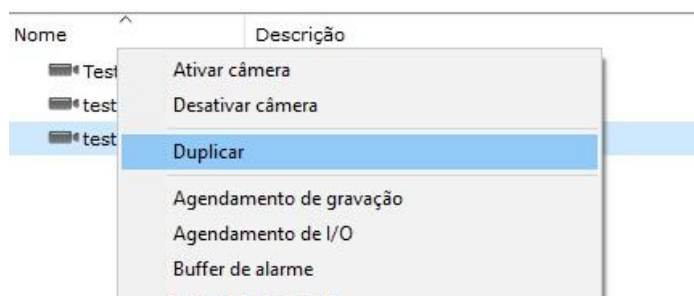
Once this is done, the registration of cameras will be executed, as shown in the figure below:





To add a camera, click **Add**. To change or remove a camera, select the desired camera and click on the corresponding button.

**Tip:** After adding a camera to the server, the administrator will be able to duplicate it, if necessary, by right-clicking on its registration and clicking on Duplicate:



## 6.1.1 Camera

### 6.1.1.1 General

General camera settings

Camera name	Camera description				
Cam1	Test camera				
Manufacturer	Digifort - IP Surveillance System				
Camera model	RTSP Server	Firmware	6.7.0.0 or greater		
Camera address	192.168.0.1	Port (8601)	80	User	admin
				Password	*****
				Preferred transport	Auto
<input type="checkbox"/> Secure connection via SSL/TLS (Check connection port)					
Camera shortcut	1	Latitude	0.000000	Longitude	0.000000
Recording directory	C:\Recording\Cam1\			Connection timeout (ms)	30000
General Memo					
<input checked="" type="checkbox"/> Activate camera					

- **Camera Name:** Enter a name for the camera. This name will be used as an internal reference of the system, therefore, after saving, it cannot be changed.

- **Camera Description:** Enter a short description for the camera that will help you identify it. In the Surveillance Client, this description will help you to identify each camera. It can be edited whenever you need.
- **Manufacturer:** Select the manufacturer of the camera to be inserted.
- **Camera Model:** Select the camera model to be inserted.
- **Firmware:** Select the camera firmware version to enter. By default, when selecting the camera model, the latest firmware version is automatically selected. In most cases, selecting the most current firmware allows the camera to work perfectly with all its features.
- **Channel:** If the selected device is multi-channel, you must specify the desired channel number in this field.
- **Camera Address:** IP or DNS address of the camera. The IP address to be used must already be previously configured internally in the camera.
- **Ping Button:** Performs a ping test on the specified address.
- **Port:** Communication port with the camera. Most cameras on the market use port 80 for connection. The port to be used must be previously configured internally in the camera. The default port used in the integration of the camera with the system will be shown in parentheses.
- **Extra Ports Settings Button:** Configure the camera's [extra ports](#).
- **User and Password:** Enter the user that the server will use to perform authentication on the camera. Consult your camera's manual for the default user and how to add more users. Enter the password that the server will use to perform authentication on the camera. Consult your camera's manual for the default password and how to change it.

**Important:** For the server to have access to all camera features, provide the camera administrator user. For this information, consult your camera's user manual.

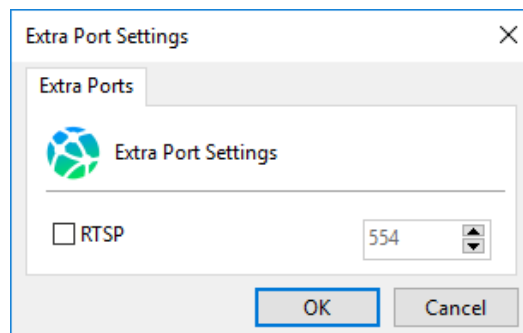
- **Preferred Transport:** Select the preferred transport method among Auto, UDP and TCP.
  - **Auto** - Transport used will generally be TCP, unless during device integration performance was not satisfactory, then transport will be done via UDP
  - **TCP** - Transport will be done by TCP when possible
  - **UDP** - Transport will be done via UDP when possible
- This option is a transport preference and not mandatory, that is, even if you specifically configure TCP or UDP, the system will not necessarily follow the configuration, as the device's media driver must support the desired protocol.
- **Extra Parameters Button:** Opens the camera's extra parameters screen (if supported).
- **Connection via SSL/TLS:** If the camera has support to secure connection, check the box to activate the SSL communication method between the camera and the Server, it is important to check the port for such communication. If the camera does not have the feature, this option will appear as inaccessible.
- **Camera shortcut:** Type a shortcut for the camera so that in the Surveillance Client this camera can be quickly shown on the screen through this shortcut.
- **Latitude and Longitude:** Both options are used to mark the positioning of a camera on a map, this feature serves several purposes, such as tracing vehicle routes using an LPR server (for more information about the feature, check the Surveillance Client User Manual).
- **Connection timeout (in ms):** This parameter is used by the system when the connection with the camera is lost in some way. The server will attempt to re-establish the connection after the configured time. To convert this value to seconds, simply divide the value by 1000. By default, this parameter is set to 30000ms (30 seconds).
- **Directory for recording:** The system makes it possible to record cameras distributed on several disks, for that, select the directory for recording images of the camera to be inserted. It is possible to record on network drives, that is, on disks of other computers on the network. To learn how to use this feature see Network Units.
- **General Notes:** If necessary, use the field to add additional information about the camera.
- **Activate Camera:** Indicates whether the system should activate this camera

### Note

The server is responsible for managing the structure of directories used for camera recording, therefore, no file in its database must be manually deleted, and the camera recording directory cannot be created by methods external to the server, such as For example, Windows Explorer.

#### 6.1.1.1.1 Extra Ports

Communication with certain types of devices can occur through different communication ports. Generally speaking, the system can automatically establish a connection with the camera using its main port (assigned on the General Settings screen), but you can manually configure additional communication ports for the device using the Extra Ports Configuration screen:



This screen will display a list of all ports used by the camera. To specify a port, select the corresponding checkbox for the port you want to configure. Only ports with the checkbox selected will use the specified value; if the checkbox is not selected, the default value (or the port configured directly on the device) will be used.

#### 6.1.1.2 Lenses

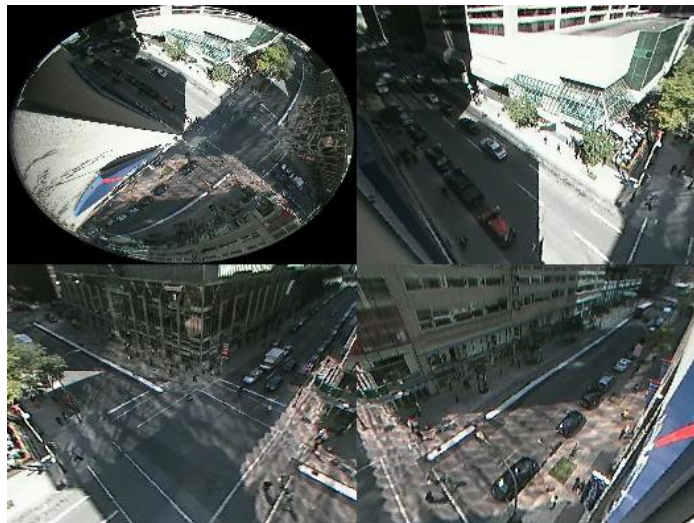
The system allows the use of three types of integrated camera lenses: **Normal**, **Panomorph**, **Fisheye**

The Normal standard is the lens that most cameras use, that is, with an aperture that does not create a large image distortion.

The Panomorph lens uses an aperture that focuses a full 360 degrees. In this case, the image looks oval and distorted. See the image below:



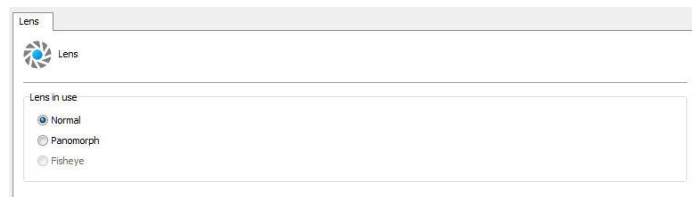
With this integration, the system performs the so-called "dewarping", that is, it removes the distortion and it is possible to see the image normally. This type of lens works very well with mega-pixel cameras, as with just one camera it is possible to focus on all angles of a room and divide the image as if it were several cameras. See the example below:



**NOTE:** Panomorph lenses do not work like "Fisheye" lenses, that is, a Fisheye camera must be integrated according to its manufacturer. The advantage of the Panamorph lens is that it can be used on any camera.

To learn how to use this feature live, see the Surveillance Client manual.

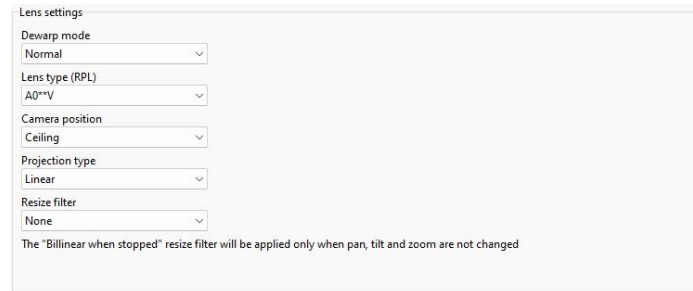
See the Administration Client settings in the screen below:



**Lens used:** Select the type of lens to be used

#### 6.1.1.2.1 Panomorph Lenses

If your camera lens is Panomorph, you must configure the parameters to adjust to the type of lens:

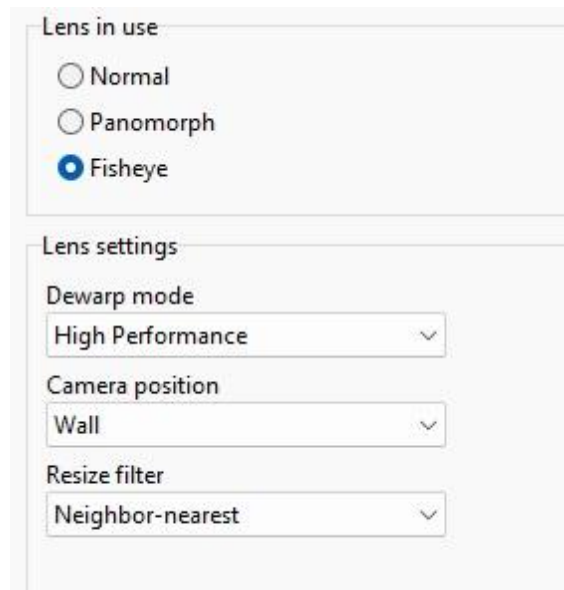


- **Dewarp Mode:** Select dewarp mode for higher quality or higher rendering performance
- **Lens type:** Select the panomorph lens type
- **Camera position:** Select the position where the camera is installed. Wall, Ceiling, Ground.
- **Projection Type:** Scene projection type
- **Resize Filter:** The resizing filter may improve image quality, but reduce performance:
  - **None:** No resizing filter (Best performance)
  - **Bilinear:** Bilinear resizing for greater visual quality
  - **Bilinear when stopped:** Bilinear resize filter will be applied only when camera is still (During PTZ it will be disabled)

#### 6.1.1.2.2 Fisheye Lenses

If your camera has a fisheye lens, configuration options will vary depending on the manufacturer's dewarping library. As the system has many integrated libraries, we will not describe the options for each library. Consult your camera manufacturer for more information.

Fisheye lens setup example:



The screenshot shows a configuration window with two sections. The first section, 'Lens in use', contains three radio buttons: 'Normal', 'Panomorph', and 'Fisheye'. The 'Fisheye' option is selected, indicated by a blue dot. The second section, 'Lens settings', contains three dropdown menus. The first dropdown, 'Dewarp mode', is set to 'High Performance'. The second dropdown, 'Camera position', is set to 'Wall'. The third dropdown, 'Resize filter', is set to 'Neighbor-nearest'.

#### +Nota

For fisheye lenses, a specific integration with the camera manufacturer's dewarping library is required, for this reason the Fisheye option may not be available if integration with the manufacturer's dewarping library has not yet been done.

### 6.1.1.3 Motion Detection

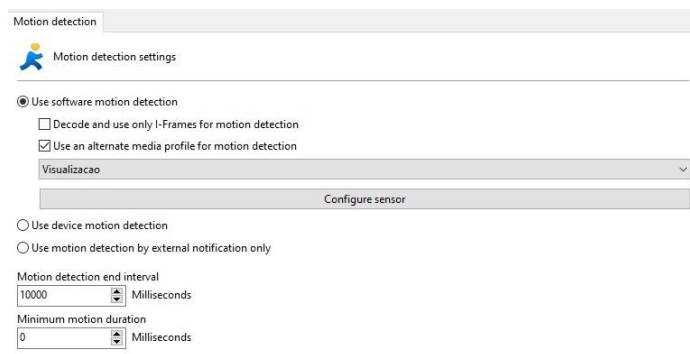
#### 6.1.1.3.1 Use Motion Detection by Software

When we use motion detection via software, we have to take some precautions in relation to server processing and even identify areas of interest in the image for detection.

We must bear in mind that motion detection via software will always increase the processing of the image recording server. This happens because for each camera in which motion detection is activated, the server has to decode an entire chain of frames and from this chain only 2 frames are compared. An example of a CPU boost: decoding a whole chain of frames every second from a megapixel camera with H264 compression.

To reduce processing on the server, an option was developed that allows performing motion detection on a lower resolution media profile. In this way, images can be recorded in high resolution and motion detection in low resolution. The lower the resolution used for motion detection, the less processing used. It is recommended to get good detection at minimum CIF resolution. As for the frames per second, only 3 frames per second are recommended, because in a sequence of 30 frames only 2 frames would be analyzed.

To select a media profile for motion detection, select the option **Use an alternative profile to detect motion** and select the desired media profile as shown in the figure below.



The screenshot shows the 'Motion detection' settings window. It has a title bar 'Motion detection' and a sub-header 'Motion detection settings' with a person icon. There are three radio buttons: 'Use software motion detection' (selected), 'Use device motion detection', and 'Use motion detection by external notification only'. Under 'Use software motion detection', there are two checkboxes: 'Decode and use only I-Frames for motion detection' (unchecked) and 'Use an alternate media profile for motion detection' (checked). Below these is a dropdown menu labeled 'Visualizacao' and a 'Configure sensor' button. At the bottom, there are two input fields: 'Motion detection end interval' set to '10000' and 'Minimum motion duration' set to '0', both with 'Milliseconds' units.

To learn how to create media profiles see the chapter [Media Profiles](#)

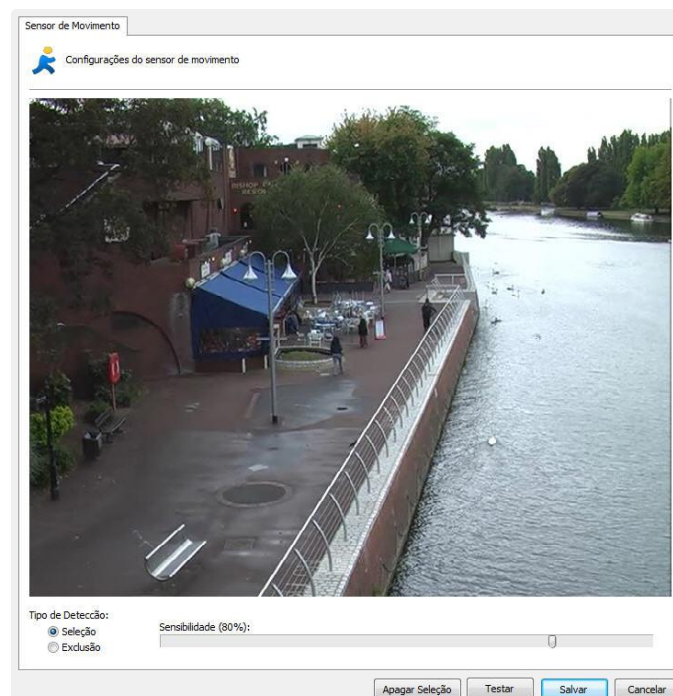
Another option that helps to reduce CPU usage is the **use of I-Frames only to detect movement**. This option should offer a significant reduction in server CPU usage, however we recommend using a minimum of 1 I-Frame per second for the best motion detection performance. Just enable the option as in the image above (**Decode and use only I-Frames for motion detection**).

The **Motion Sensor** consists of a tool that allows the user to define areas of the image that will be sensitive or not sensitive to movement.

Setting the motion sensor is very important to save disk space used by the camera. If in the Camera tab you chose the motion detection recording method, it is recommended to adjust the sensor as needed.

By default, if the sensor is not configured, the entire image will be motion sensitive. To access this feature, click the Configure Sensor button.

To configure the motion sensor, click on the **Configure Sensor** button. When clicking this button, the motion sensor configuration window will be opened with a real camera image, as shown in the figure below:



The screenshot shows the 'Sensor de Movimento' configuration window. It has a title bar 'Sensor de Movimento' and a sub-header 'Configurações do sensor de movimento' with a person icon. The main area is a live camera feed showing a park area with a river. Below the feed, there are two radio buttons: 'Seleção' (selected) and 'Exclusão'. To the right of these is a slider labeled 'Sensibilidade (80%)'. At the bottom, there are four buttons: 'Apagar Seleção', 'Testar', 'Salvar', and 'Cancelar'.



On this screen you can select areas that will be motion sensitive or areas that will not be motion sensitive.

To select areas that will be sensitive to motion, select the Selection detection type and click on the image, dragging the mouse, forming a selection square. To select areas that will not be sensitive to movement, select the Exclusion button, repeating the process.

To delete already configured areas, right-click the mouse and select the selection square to be deleted or click the **Clear Selection** button to delete all defined areas.

After selecting the desired areas, configure the motion sensitivity. By default the sensitivity is 80%, with this value it is already possible to detect any type of sudden movement in the image.

Once this is done, click on the Test button to view the operation of the selected motion detection. For performance reasons, the server analyzes the camera images at two frames per second, that is, motion detection is not necessary in all frames, only one image is analyzed every 500ms. With this pattern any type of movement is detected.

The figure below demonstrates how the motion sensor works with selection of motion-sensitive areas:



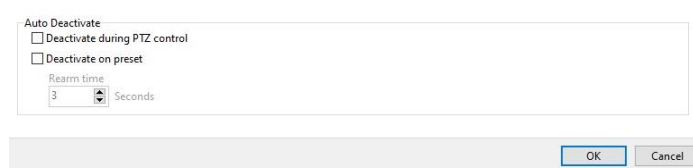
The figure below demonstrates how the motion sensor works with selection of non-motion sensitive areas:





#### 6.1.1.3.1.1 Auto disable motion detection during PTZ

The system allows motion detection on the server to be temporarily disabled if the camera's PTZ is being used or when changing presets. This option should bring greater performance to the server that is processing the images during PTZ control or can also be used to not generate recording records or events during preset changes (where there will always be movement).



- **Disable during PTZ control:** Disable motion detection during PTZ control.
- **Disable on Preset:** Disables motion detection when a preset is activated.
- **Rearm Time:** Configure the time to rearm the motion detection after being disabled by the previous options. In the case of PTZ use, the rearm will be counted from the moment the PTZ stops being used. As for the preset option, the time will count from the moment the preset command is sent.

#### 6.1.1.3.2 Use motion detection by device

Motion detection via device is a method that allows the system to receive notification of motion detection being sent directly by the device itself, thus saving processing resources and allowing your system to support a greater number of cameras per server.

To activate this function, just select it in the motion detection options:

Motion detection settings

☐ Use software motion detection

☐ Decode and use only I-Frames for motion detection

☒ Use an alternate media profile for motion detection

Visualizacao

Configure sensor

☒ Use device motion detection

☐ Use motion detection by external notification only

You'll need to configure motion detection options like zones and sensitivity directly in your camera's configuration interface.

### + Note

Device motion detection functionality will only be available for models that have this functionality built-in. It is possible to check which models have such functionality directly in our website

#### 6.1.1.3.3 Use motion detection by external notification

The option to use motion detection via external notification is a feature that is deprecated and has been replaced by the "Use motion detection by device" option.

If your device has not been integrated with support for motion detection, you can use this option that allows motion notification through the server's HTTP API.

This is a complex configuration and does not fall within the scope of this administration manual. We have a specific manual for this type of configuration. If necessary, consult the document **Using Hardware Motion Detection.pdf** for a better understanding of the subject.

#### 6.1.1.3.4 End detection interval and motion duration

This option allows you to configure the time for the movement to end as well as the minimum duration for it to be considered a movement.

Motion detection end interval

1500 Milliseconds

Minimum motion duration

1000 Milliseconds

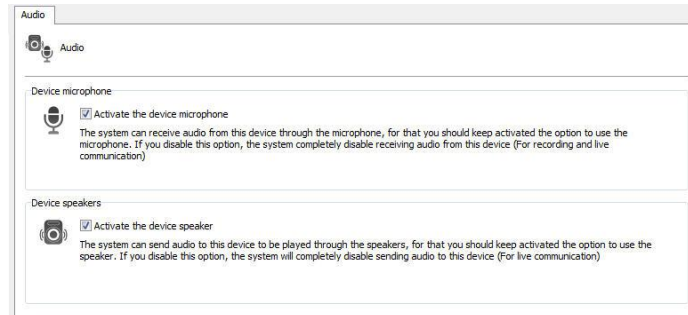
- Motion Detection End Interval:** Configure the time that the system will continue to consider that the camera has motion, even after the motion ends. This is an important system fine-tuning option, especially if the **motion detection via device** option is selected, as the camera does not send frequent continuous notification of motion detection, there is a time interval between notifications, which can cause so that the system understands that the camera is no longer detecting movement, even though it is detecting movement. The default value of 1500 milliseconds is optimized for software detection.
- Minimum Motion Duration:** This value is used to determine the start of motion detection. For the system to consider that movement has occurred in the camera, there must be uninterrupted movement for at least X milliseconds, thus preventing image artifacts from triggering the motion sensor, reducing false alarms.

#### 6.1.1.4 Audio

The system allows the use of a camera's audio features.

You can listen and record the audio that the camera's microphone picks up or send the audio to your speakers.

With this feature, the operator can listen and communicate remotely through a microphone connected to the monitoring client. To learn how to use the audio in the surveillance client, see its manual.



On the screen above the following features are available:

- **Activate the Device Microphone:** Enable this option if you want to hear the audio that the camera is capturing. When activating this feature, the audio will automatically be recorded synchronized with the video from the camera. (If the media profile is configured with audio).
- **Activate the Device Speaker:** Enable this option if you want to send audio to the camera speakers

**NOTE:** Not all camera models have the integrated audio feature, as these integrations will be made on demand. However, most cameras that work over RTSP may or may not work correctly without prior integration.

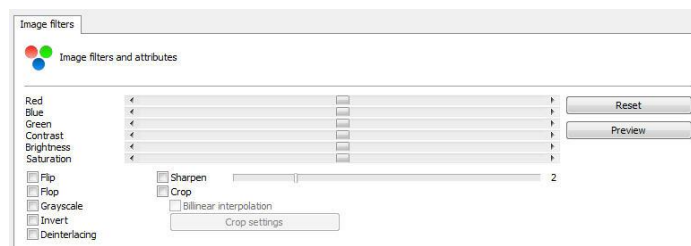
**Supported audio formats:** PCM, G.711, G.726 and AAC

#### 6.1.1.5 Image Filters

The system has a set of effects that can be applied to the image so that cameras whose image is impaired can be improved.

This set of effects is only applied when viewing the camera in the Surveillance Client, that is, the original camera image is saved on the server.

To access this feature, click on the **Image Filters** tab, as shown in the figure below:



- **Red:** Adjusts the red color level of the image.
- **Blue:** Adjusts the blue color level of the image.
- **Green:** Adjusts the green color level of the image.
- **Contrast:** Adjusts the contrast level of the image.
- **Brightness:** Adjusts the brightness level of the image.
- **Saturation:** Adjusts the color level of the image.
- **Reset:** Returns the above mentioned values to the starting position.
- **Preview:** Opens the camera video with the settings applied.
- **Flip:** Flips the image horizontally. Recommended when the camera is installed upside down.
- **Flop:** Flips the image vertically. Recommended when the camera is installed upside down.
- **Grayscale:** Makes the image grayscale.
- **Invert:** Invert the colors of the image
- **Sharpen:** Applies an edge enhancement effect to the image.
- **Deinterlacing:** The Deinterlacing filter can be used for cameras that generate line interlacing effects.
- **Crop:** Select a smaller field of view in the image that will be displayed in the surveillance client.
  - **Bilinear Interpolation:** Use bilinear interpolator for better image quality

## 6.1.2 Streaming

### 6.1.2.1 Media Profiles

A media profile consists of a set of individual camera parameters such as image resolution, frames per second and image quality, which are associated with Recording, Motion Detection and Live View. The system allows multi-streaming configuration, that is, the use of multiple configurations (streams) for recording, motion detection or live viewing.

For a better understanding, let's assume the following scenario: A recording profile can be created, which will be associated with the camera's recording event. In this profile we can define that we want to record five frames per second, with a resolution of 320x240 and high image compression. A visualization profile can also be created, which will be associated with the camera visualization event. In this profile we can define that we want to visualize the camera at ten frames per second with a resolution of 640x480 and low image compression.

By default, when registering a new camera, two pre-configured media profiles are created, one for recording and one for viewing. The preconfigured parameters of each profile are only the parameters common to all devices. The Media Profiles of all cameras and video-servers have common parameters and individual parameters for each equipment. Common parameters are:

- **Video Compression:** Video compression to be used when recording the images on disk. The system currently supports **Motion JPEG**, **MPEG4**, **MxPEG**, **H263**, **H264** and **H265** formats.
- **Image resolution:** Image resolution that will be used in the profile. When selecting the camera model, this list of resolutions automatically starts showing only the resolutions supported by the camera. A very high image resolution will consume a lot of disk space and network bandwidth, but the image will have a higher quality where it is possible to recognize more details in the image, such as a person's face. A very small image resolution will consume little disk space and network bandwidth, but the image will have a lower quality, providing little detail. This parameter must be configured as needed. The system has a disk space consumption calculator that will help you better configure image resolution and frames per second. To learn how to use system calculator, see [Disk Space Usage Calculator](#)
- **Image quality:** The images coming from the cameras go through a compression process. The higher the image compression level, the less quality this image will have, and the lower the image compression level, the more quality.

- **Frames per second:** Frames per second to be recorded. A higher frames per second rate will consume more network bandwidth and disk space, but will give smoother motion. A lower rate of frames per second will consume little network bandwidth and disk space, but the movement will be more robotic. It is proven that from three to seven frames per second it is already possible to recognize all the movements of a person. In some cases, the camera may not be able to send the configured amount of frames per second, especially with high frame rates per second. This is due to several factors such as internal network malfunction, number of connections made to the camera and camera processing power.

Some specific parameters of each equipment, among others, we can exemplify the insertion of texts in the image, image rotation, color levels, etc.

Some cameras may not support dynamically adjusting common parameters such as frame rate and image quality. In this case, these adjustments must be made directly on the camera through its own interface, where in this case you can select which Camera Stream you want to associate with the media profile.

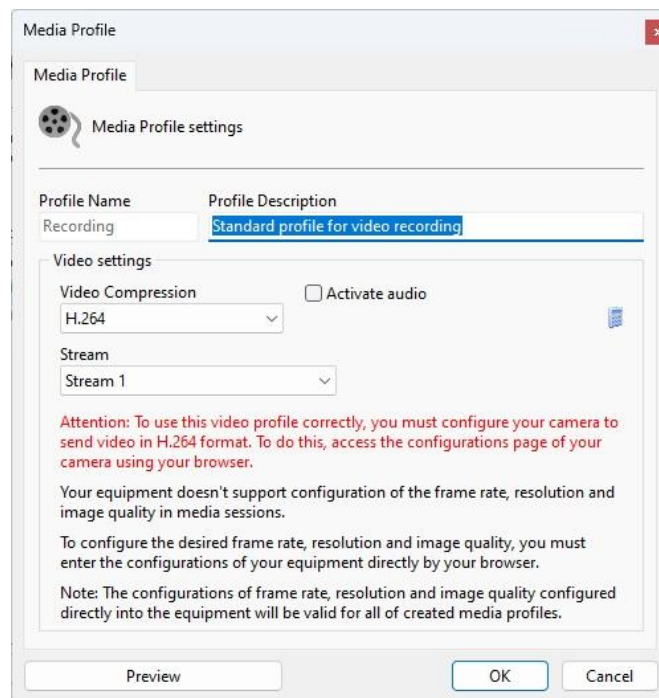
#### 6.1.2.1.1 How to add Media Profiles

To add a media profile, click **Add**, and the media profile addition screen will be executed as shown in the figure below:

It is important to note that this screen may vary from camera to camera, as each one has its own set of configuration parameters.

In the example above, the selected camera supports different types of settings such as Resolution, Compression, Frame Rate, among others.

However, the vast majority of cameras do not allow requesting video with dynamic parameters, for these cameras, you will generally see the following profile:



In this profile you must select the camera stream, which must have been previously configured using the camera's configuration interface.

#### 6.1.2.1.2 How to view the functioning of the configured media profile

To view the results of the configurations of the parameters of the media profile being edited, click on the **Preview** button, opening a screen with the camera's live image, as shown in the figure below:

This function will only work if the camera connection address is provided in advance.



This screen also contains the following information:

- **Frames per Second**
- **Resolution**
- **Transmission Rate (Bandwidth Consumption)**
- **Video Codec used**
- **Status message with connection information**

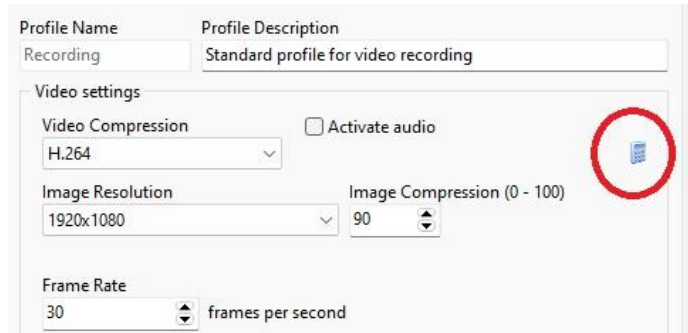
#### **Note**

All information contained in the image is updated every second.

#### 6.1.2.1.3 Disk space usage calculator

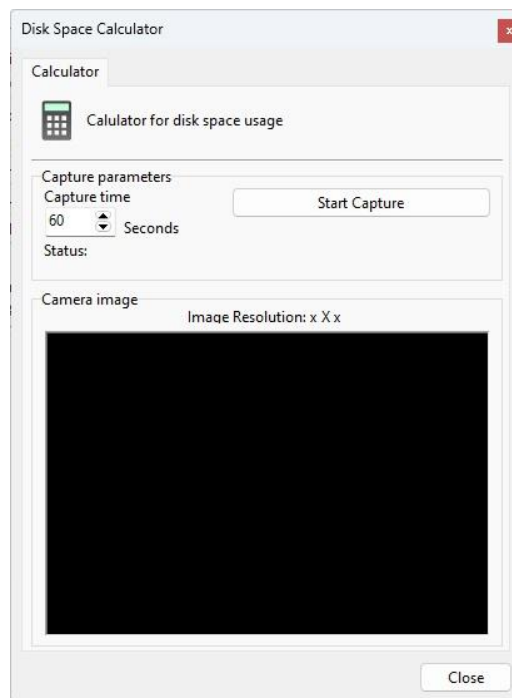
The system has a very useful tool to help dimensioning the disk space to be reserved for each camera, which is the disk space usage calculator. To access this feature, click on the button identified by a “calculator” on the media profiles configuration screen, as shown in the figure below:

This function will only work if the camera connection address is provided in advance.



The screenshot shows a configuration window for a media profile. At the top, there are two fields: 'Profile Name' with the value 'Recording' and 'Profile Description' with the value 'Standard profile for video recording'. Below these is a section titled 'Video settings'. Inside this section, there are several controls: 'Video Compression' is a dropdown menu set to 'H.264'; 'Image Resolution' is a dropdown menu set to '1920x1080'; 'Image Compression (0 - 100)' is a slider set to '90'; 'Frame Rate' is a dropdown menu set to '30' with the unit 'frames per second' next to it; and there is an unchecked checkbox labeled 'Activate audio'. On the right side of the 'Video settings' section, there is a small blue icon of a calculator, which is circled in red.

By clicking on this button, the disk space calculator will be executed as shown in the figure below:



To calculate the disk space required for camera recording, the calculator captures an original temporary video from the camera with the image quality and resolution parameters, configured in the media profile being edited, and the capture time, entered on this screen. Based on the received video, a calculation is made of the size of disk space needed to store the images generated by this camera in a certain number of days and a certain expected motion detection rate.

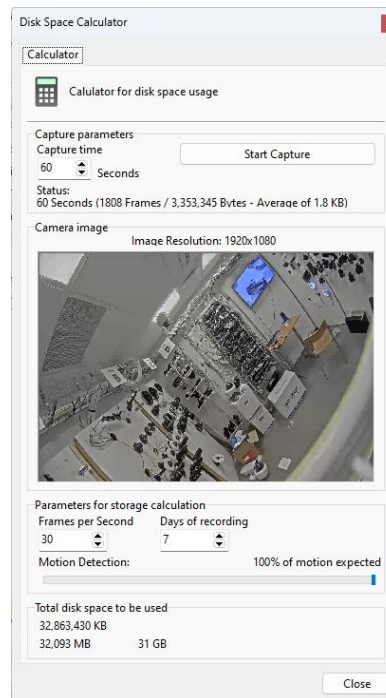
For compressions such as **MPEG-4**, **MxPEG**, **H.263**, **H.264** and **H.265** the recommended capture time is **60 seconds**.

For **Motion JPEG**, the recommended capture time is **5 seconds**.

To start the disk space calculation process, enter the capture time value and then click Start Capture.

Once this is done, the video will be captured and analyzed, displaying the screen below:





After the analysis of the captured video is finished, the calculator fills in the maximum value of frames per second that the camera was able to send, that is, if a media profile is configured for recording at 30 frames per second, but the camera is only able to send 12 frames, this value will be 12.

Change the values for frames per second, recording days and motion detection estimation to obtain an estimate of disk space occupation to be used by the camera.

### + Important

- Changing the "Frames per Second" field is only recommended for Motion JPEG compression as all frames have the same size and it is easy to extrapolate bandwidth usage. For other video compressions, instead of changing the Frames per Second value, we recommend changing the media profile, so the system will calculate a more accurate storage value.
- Depending on your camera's streaming settings, the calculated storage value may change. We recommend doing the calculation during different periods, with and without motion.

Below will be described how each parameter of the space calculator works.

- **Recording days:** Enter the number of days to be stored for this camera. The higher this value, the more disk space used.
- **Frames per second:** Enter the number of frames per second to be used by the camera recording.
- **Motion Detection:** Enter the percentage of movement expected at the camera's location in a day. For example, if the normal operation of a camera does not detect movement at night, then we can slide this control by adjusting this value to 50%.
- **Total disk to be used:** Informs the disk space required to store the images generated by the camera with the parameters configured in the media profile being edited, the number of days of storage and the configured movement percentage.
- **Start Capture:** Click this button to recalculate the disk space needed to store this camera's images with a new image.

## 6.1.2.1.4 Audio

If your camera supports audio, you can select the "Activate audio" option so that the system requests audio for the desired profile.

You can enable audio in different media profiles, allowing you, for example, to enable audio only for live viewing (by selecting audio in the live viewing profile and deselecting it in the video recording profile), or configuring audio for recording only (in the video recording profile).

## 6.1.2.2 Recording

On this screen, settings related to the camera recording stream on the server are available.

- **Media Profile:** Choose the default media profile that will be used by the software to record images.

#### 6.1.2.2.1 Snapshot Buffer

The Image Buffer is used when you want to send still images from the cameras via email or popup when an alarm occurs.

In case your edition supports the map feature, the system can display the image preview in the camera status on the map (See the Surveillance Client manual).

By default this option is disabled to save server resources.

- **Activate the snapshot buffer:** Activate the Image Buffer and the server will keep the images in memory for X seconds so that they can be sent along with the email. If there are many cameras related to an alarm, it is advisable to increase the seconds because when sending the email there might not be enough time for these images to be attached to the email.

#### 6.1.2.3 Live View

To access this configuration, click on the Live View tab, as illustrated in the figure below:

The screenshot shows a configuration window titled "Live visualization parameters". It includes the following fields and controls:

- Private IP address:** A text input field.
- Port (80):** A numeric input field with a value of 80.
- Connection timeout (Millisecond):** A numeric input field with a value of 4000.
- Public IP address:** A text input field.
- Port (80):** A numeric input field with a value of 80.
- Media Profile:** A dropdown menu currently showing "Visualization".
- Mobile access media profile:** A dropdown menu currently showing "Visualization".
- Switch media profile on camera selection:** An unchecked checkbox.
- Media Profile:** A dropdown menu currently showing "Recording".
- Access using relay:** A checked checkbox.

The configuration made here will be applied to the Surveillance Client, it will use this information to capture the image from the cameras and display it on the screen.

The parameters to be configured are described below.

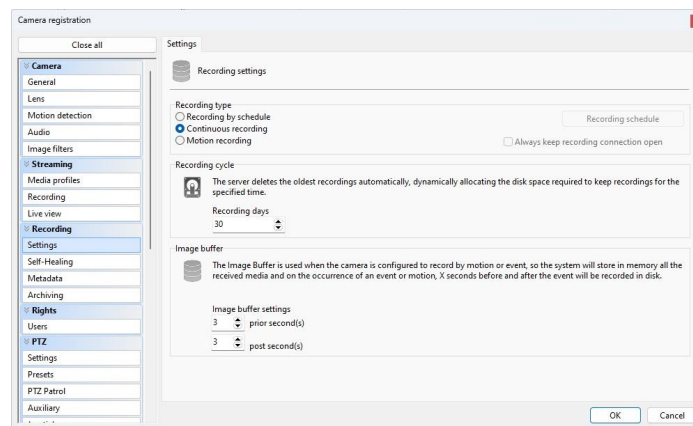
- **Access via Relay:** When using this option (Selected by default), the client will receive images from the cameras through the system server instead of connecting directly to the camera. This is the recommended connection method as it allows greater security of the solution (As the cameras can be placed on a separate network from clients and other devices, accessible only by the server), lower use of bandwidth and camera resources (As all communication will be made through the server and there will be no duplicate streams on the network) and greater accessibility. With this option checked, the address and connection port options do not need to be configured. If this option is disabled, the Surveillance Client will connect directly to the cameras, therefore parameters such as address and port must be provided according to the network topology for client access.
- **Private IP Address:** If you do not use access to the camera through the relay server, enter the IP address of the camera's local network.
- **Private IP Port:** Enter the communication port with the camera on your internal network.
- **Public IP Address:** If the client is accessing through an external network, such as the internet, for example. Fill in your external IP address here. For this option to work, your router must be configured to provide access to the camera externally.
- **Public IP Port:** Enter the communication port with the camera via the external network.
- **Connection Timeout:** This parameter is used by the system when the connection to the camera is lost in some way. The server will attempt to re-establish the connection after the configured time. To convert this value to seconds, simply divide the value by 1000. By default, this parameter is set to 4000ms (4 seconds).
- **Media Profile:** Select the media profile to be used in the camera view.

- **Mobile Media Profile:** The system allows the use of a different media profile for viewing on mobile devices. Access via mobile devices generates a processing load on the server as the system needs to transcode the video before sending it to the device. If the camera is configured to record megapixel images the transcoding process can be cumbersome, generating an unwanted processing load on the server. This option will allow the selection of a media profile with a lower resolution to perform the transcoding, resulting in lower processor consumption.

## 6.1.3 Recording

### 6.1.3.1 Settings

On this screen you can configure the recording options:



#### 6.1.3.1.1 Recording Type

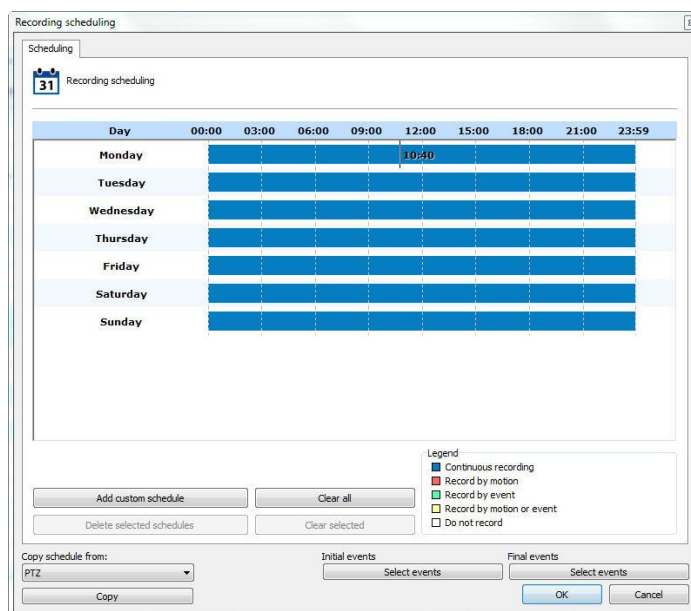
The system provides three types of recording, continuous recording (always record), motion detection recording, and schedule recording. Continuous recording will record all images received by the camera to the disk. Motion detection recording will only record images with motion. With scheduling recording, it is possible to configure times when the camera will always record, record by motion detection or event, or not record at all. In most cases, motion detection recording is the most recommended, as it drastically reduces the disk space used.

- **Always keep recording connection open:** Keep the camera recording stream always streaming in case of event recording. This way the recording pre-buffer will work normally. This option is also required to send audio to cameras via the Monitoring Client or through the send audio to cameras event action.

##### 6.1.3.1.1.1 How to configure the recording schedule

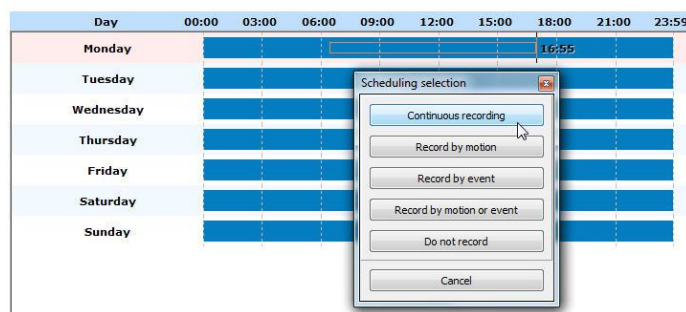
To configure the recording schedule, click on the Recording Schedule button.

The scheduling screen below will open:



The operation of this screen is standard for all other schedules available in the software. Initially we have the days of the week and their respective times.

To create a schedule, select the day of the week and keep the left mouse button pressed over some time of the day, dragging it to another time, forming a rectangle. After this action, a window will open asking for the type of schedule to be created, select the most convenient option.



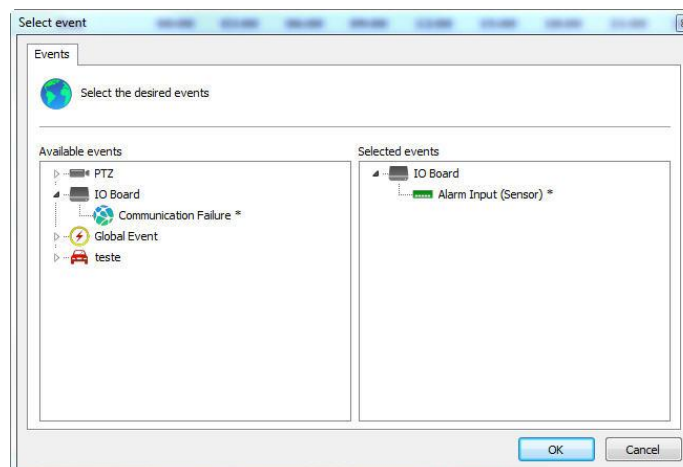
You can select multiple days to apply a setting to all at the same time Just click on the desired days of the week.

In the figure below, the first three were selected:



Scheduling options are:

- **Always Record:** Enables continuous recording from the camera at the specified time. This option is represented by the color blue.
- **Motion Record:** Activate camera motion recording at the specified time. This option is represented by the color red.
- **Record by Event:** Enable event recording of the camera at specified times. This option is represented by the color green.
- **Motion & Event:** Enables recording by motion detection and camera event detection. This option is represented by the color yellow.
- **Do Not Record:** Disables camera recording at the specified time. This option is represented by the color white.
- **Cancel:** Cancels the creation of the schedule for the specified time.
- **Button select start events and select end events:** If the type of schedule is configured to record by event, click this button to configure the event that will start or end the recording of camera images on the server. When clicking on this button, the following screen will be displayed:



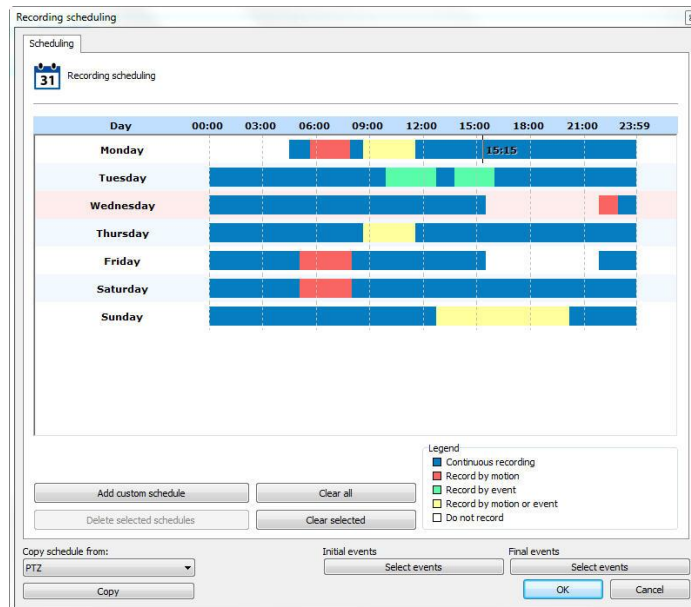
This screen presents two lists, the list of available events and the list of selected events.

The list of available events displays the list of all system objects that trigger events, and the list of selected events displays all events that are selected.

The events that have the “\*” symbol next to them are the events that will actually occur, that is, suppose we have chained timer events, in this case it is not all the events that will occur, but the one with the symbol “\*” next to. Timer events are events that occur at a certain user-defined time to trigger another event. To learn about timer events see Timer Events.

To select an event, select it from the list of available events and drag it to the list of selected events. To remove an event, follow the same process in reverse.

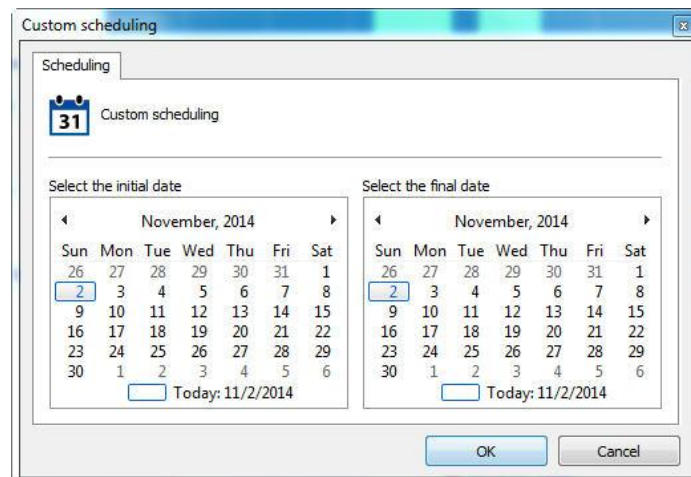
In the image below, we have different types of appointments on different days:



The scheduling screen allows scheduling to be made for a specific day of the year, such as a holiday or a special event.

To add a custom schedule, click the Add custom schedule button.

**It is possible to choose a single day as shown in the images below:**



Day	00:00	03:00	06:00	09:00	12:00	15:00	18:00	21:00	23:59
Monday									
Tuesday									
Wednesday									
Thursday									
Friday									
Saturday									
Sunday									
Sunday, 11/2/2014	00:00								

Or add a range:

Custom scheduling

Scheduling

31 Custom scheduling

Select the initial date

November, 2014

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 11/2/2014

Select the final date

November, 2014

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 11/2/2014

OK Cancel

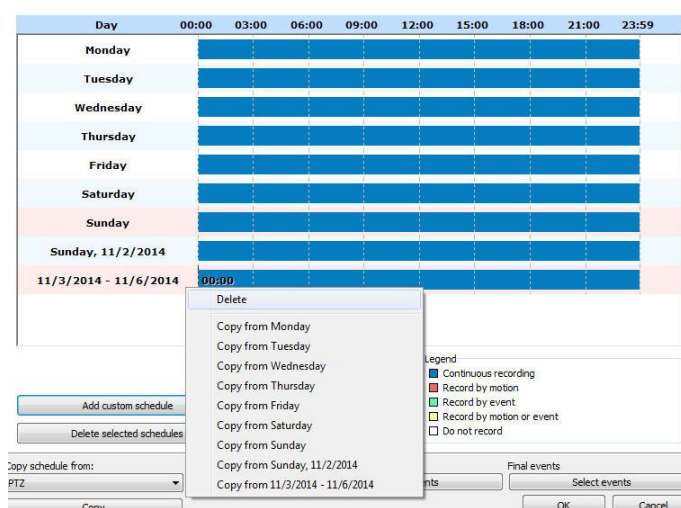
Day	00:00	03:00	06:00	09:00	12:00	15:00	18:00	21:00	23:59
Monday	00:00								
Tuesday									
Wednesday									
Thursday									
Friday									
Saturday									
Sunday									
Sunday, 11/2/2014									
11/3/2014 - 11/6/2014									

### + Note

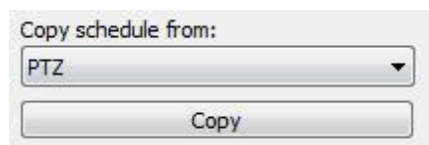
Custom schedules will have priority over regular schedules. For example: In a custom schedule that is scheduled on a Monday, it will override the settings already made for Monday on that specific day.

By right-clicking on one or more selected schedules, you can delete custom schedules or copy settings from other schedules:





It is also possible to copy the scheduling of another system object, just select it and click copy:



To delete a custom schedule, select the custom schedule and click **"Delete selected schedules"**

To return to the default scheduling settings for one or more days, select the desired days and click **"Clear Selected"**

#### 6.1.3.1.2 Recording Cycle

In this option, define the number of days that the server will keep the camera recordings on disk.

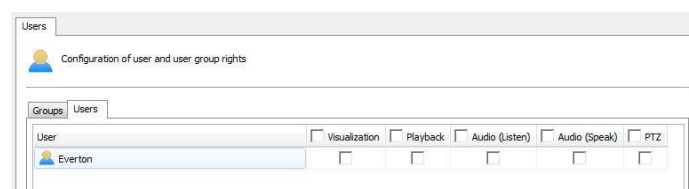
The recycling precision is 30 minutes, that is, when the limit is reached, the system will erase the oldest 30 minutes to record another 30 minutes.

## 6.1.4 Rights

This area of the camera registration is reserved for defining user rights over the camera.

### 6.1.4.1 Users

System Users and Groups will be listed automatically and may have 5 rights:



- **View:** Check this option if this user or group will be able to see the camera in live mode in the surveillance client.

- **Playback:** Check this option if the user or group can view the recorded images.
- **Audio (Listen):** Check this option if the user or group will be able to hear the audio captured by the camera.
- **Audio (Speak):** Check this option if the user or group will be able to speak through the camera speaker.
- **PTZ:** Check this option if the user or group will have PTZ control over the camera.

## 6.1.5 PTZ

### 6.1.5.1 Settings

On this screen you can configure the options for PTZ cameras:

- **Enable PTZ controls for this camera:** Enable this option (Enabled by default) to provide PTZ control for Surveillance Client users. If this option is disabled, operators will not have access to the camera's PTZ and the camera icon in the Surveillance Client will be displayed as a fixed camera.
- **Use the device's embedded PTZ control:** Select this option only if the camera being registered is an IP camera. In this case, the system will send PTZ commands directly to the camera. In this mode, the system will send PTZ control commands using the equipment's native protocol. If you are using an analog PTZ camera (connected via RS-485 for example) on a video server, DVR or NVR, by checking this option the system will send the commands in the device protocol (video server, NVR, DVR...) and the device should translate these commands to the camera protocol (For example Pelco-D), however some devices do not support this type of control and only have a pass-through option through the serial port, in these cases, you must choose the option **Use the device's COM port to control PTZ directly**.
- **Use the device's COM port for PTZ control directly:** By checking this option (If available), the system will send native commands in the chosen PTZ protocol (For example Pelco-D) through the connected equipment, using the pass-through commands of the device. Use this option only if the device to which the analog camera is connected does not have the ability to natively control the cameras.

- **PTZ Protocol:** Select which PTZ protocol your analog camera is configured for (Only for direct pass-through control)
- **Camera ID (RS-485):** Enter the ID of your analog camera (Configured in the camera)
- **Device COM Port:** Select the COM port number of the network device (Video server, DVR, NVR) if the device has more than 1 port

#### 6.1.5.1.1 PTZ Usage

When using PTZ on the Surveillance Client, the system shows all other users who is currently in control of the camera.

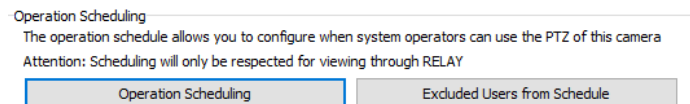
In this option you can configure **X seconds** after which the system will understand that the PTZ is no longer in use if it is not moved by the operator.

- **Keep a record of the last user who used PTZ:** The system allows you to display, in the Surveillance Client, the record of the last user who moved a camera using the PTZ controls.

The icon for using PTZ controls in the Sonitoring Client will be semi-transparent, indicating that no one else is using the controls and will inform the user name and station IP of the last operator who moved the camera when the user holds the pointer mouse over the icon:



#### 6.1.5.1.2 Operation Scheduling



The Operation Scheduling allows configuring when system operators will be able to use the PTZ of this camera.

- **Operation Scheduling:** Opens a basic calendar menu, so that the PTZ usage days and times can be defined:

Day	00:00	03:00	06:00	09:00	12:00	15:00	18:00	21:00	23:59
Monday		02:05							
Tuesday									
Wednesday									
Thursday									
Friday									
Saturday									
Sunday									

- **Exclusion of Users from the Schedule:** Allows the system administrator to define users or groups to exclude from the schedule, in this case, create exceptions:

Grupos

Grupo de Teste

Adicionar Grupos

Excluir Grupos

Usuários

teste

Adicionar Usuários

Excluir Usuários

### Note

To use Operation Scheduling, the camera must be configured to view via the Relay Server.

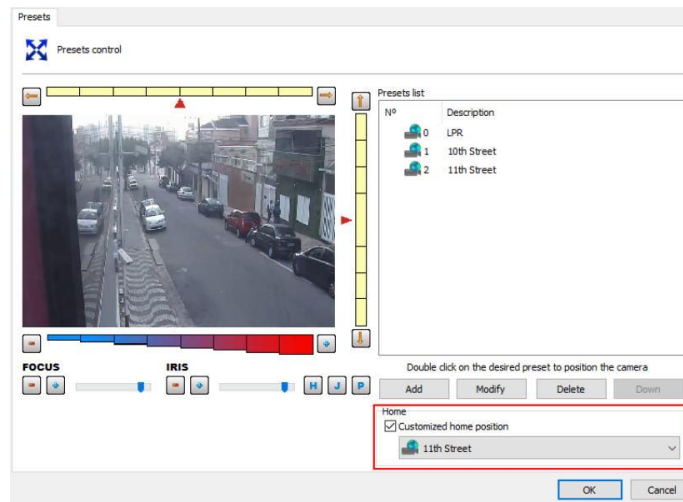
#### 6.1.5.2 Presets

Presets are memorized positions of a PTZ camera. With this feature we can memorize positions, and at any time send the camera's focus to the desired position quickly.

Each camera model supports a certain number of presets. The system role is to maintain an internal list of positions created by the user, referencing the camera's internal list of presets, that is, position 1, created by the user, is associated with internal position 1 of the camera, for example. When the user adds a preset, the two positions are linked.

The presets will be available for use in the Surveillance Client. Consult the Surveillance Client manual to learn how to call the configured presets. The preset limit will depend on the camera used.

To access this feature, click on the **Presets** button, opening the screen below:



- **PAN Bar:** Moves the camera left and right.
- **TILT Bar:** Moves the camera up and down.
- **ZOOM bar:** Moves the camera zoom back and forth.
- **Focus Bar:** Adjusts the camera's focus if it doesn't do so automatically.
- **Iris Bar:** Adjusts the camera's iris if it doesn't do it automatically.
- **Home Button:** This button is located on the button identified by the "H" symbol. By clicking on this button, the camera will position itself in its factory initial position.
- **Visual Joystick Button:** This configuration is located on the button identified by the "J" symbol. By clicking on this button, the visual joystick will be displayed over the image, allowing you to control its movement with the mouse. To learn how to use this feature see [Visual Joystick](#).
- **Pause PTZ Patrol:** If PTZ Patrol is running, this button allows you to pause so you can control the camera and create presets.
- **List of presets:** This list lists the presets registered for this camera. To position the camera on a preset, double-click on it.
- **Add button:** Memorizes the current position of the camera. To learn how to use this feature see [How to create a preset](#)
- **Modify button:** Modify the selected preset.
- **Delete button:** Deletes the selected preset.
- **Download button:** Download the list of presets already configured on the camera.
- **Custom Home Position:** Allows customization of the Home position of PTZ cameras. Many cameras do not have/support the home position, so for cameras that do not support this option, you can configure a camera preset as home.

### +Important

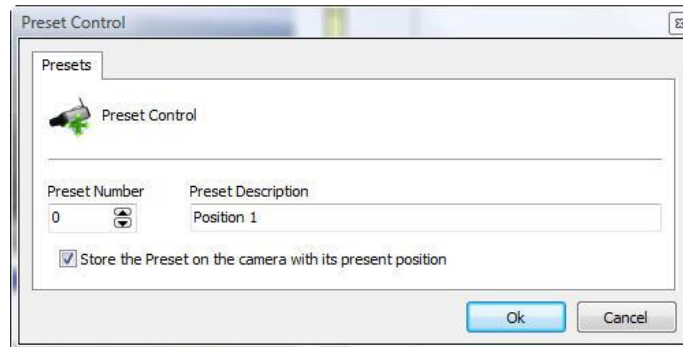
The preset list only displays the list of presets belonging to the camera. All presets created by the system are saved in the camera itself. The system associates the list item with the camera preset using its number.

### +Tip

You can position the camera by simply clicking on the image at the point you want to center it or using a desktop joystick.

#### 6.1.5.2.1 How to create a preset

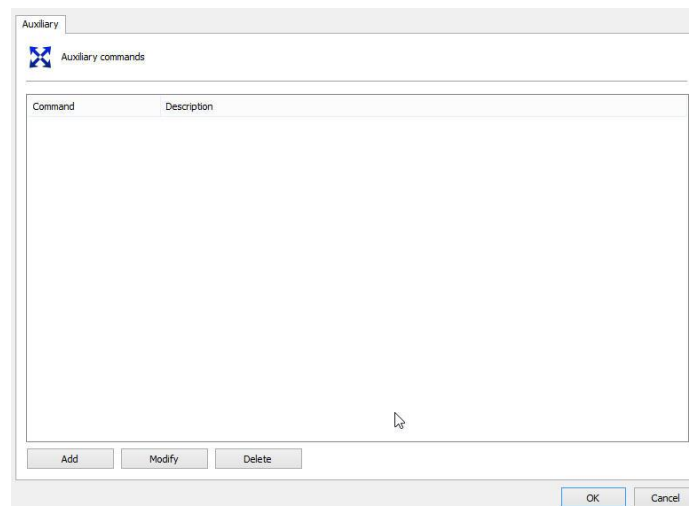
The process of creating presets is quite simple, just position the camera with the controls presented in the previous topic and click Add, as illustrated in the figure below:



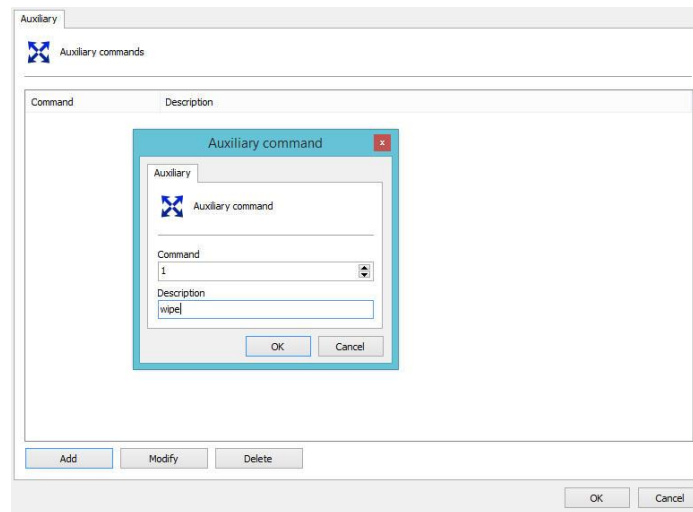
- **Preset Number:** Preset number that the system will associate with the camera's internal preset list.
- **Preset Description:** A description of the preset being added. This name will be displayed to the user in the Surveillance Client.
- **Save the preset to the camera with its current positions:** By checking this option the system will replace the camera position of the preset with the number entered. In the example in the figure above, the camera position will be saved in the camera's preset number zero. If you do not check this option, the system will only associate the preset description with the current position of the preset zero camera. If you want to change the name of a preset, deselect this option so that the system does not change the camera position as well.

#### 6.1.5.3 Auxiliary

Some PTZ cameras have auxiliary commands to access specific camera functions. For these cameras, it is possible to pre-register the auxiliary commands supported by the driver, the user simply having to activate them through the Surveillance Client.



Just click **Add**, put the ID referring to the camera command and type the desired name.

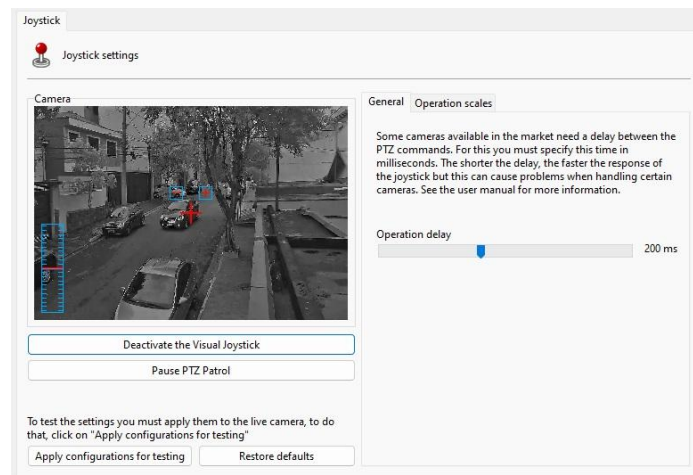


#### 6.1.5.4 Joystick

Joystick settings allow you to calibrate it with the aim of customizing it in order to operate according to the user's taste.

These settings involve parameters such as joystick sensitivity and operation delay.

To access this configuration, click on the **Joystick** button, located in the camera's PTZ settings, opening the screen below:

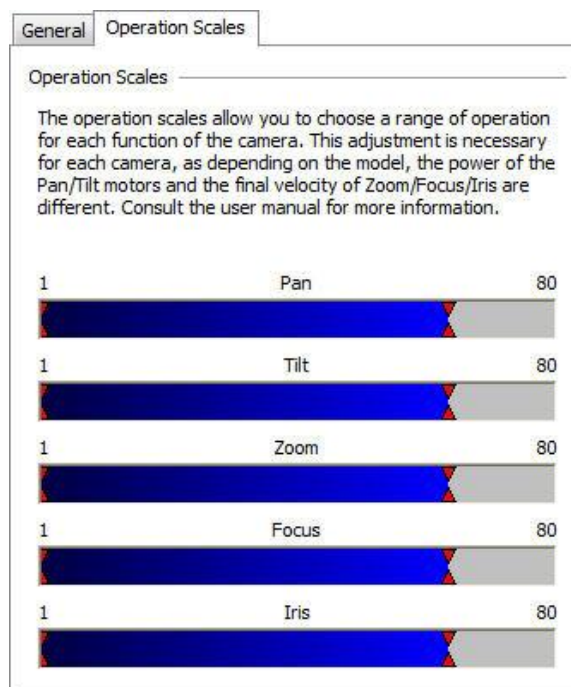


- **Activate / Deactivate the Visual Joystick:** Enable or disables the visual joystick. To learn what the visual joystick is and how it works, see [Visual Joystick](#).
- **Pause PTZ Patrol:** Pauses current PTZ Patrol to allow PTZ control.
- **Apply settings for testing:** Apply the settings made only for testing. Camera movement tests with the adjustments made must be performed on the camera image on the configuration screen.
- **Restore Defaults Button:** Restores the default settings for joystick adjustments.
- **General tab:** Allows you to access the operation delay settings.
- **Operation Scales tab:** Allows accessing the operation scales settings, defining the sensitivity for the joystick.

The operation delay is the time the system waits for the command to be sent to the camera. The default for this configuration is 200ms, that is, the system will send 1 command every 200ms while the joystick is being operated. This value is necessary so that the system does not overload the camera with many PTZ commands.

Operating ranges allow you to choose an operating range for each camera function. All values are expressed as a percentage.

To access this feature, click on the Operation Scales tab, as shown in the figure below:



These settings apply to the power of the engines. For a better understanding of this configuration let's look at the PAN bar. If you hold the joystick all the way to the left, the camera's speed will be 80% of its maximum speed. It is also possible to specify a minimum movement speed, that is, if you hold the joystick just a few centimeters to the left, the camera speed will be 5% of the minimum camera speed.

#### 6.1.5.5 Menu Control

The system allows operation of the analog camera settings menu remotely. This feature is very useful when we have a camera that is difficult to access and it is necessary to carry out a configuration.

To access this feature, click on the **Menu Control** button, located in the camera's PTZ settings, opening the screen below:





- **Open Menu button:** Opens the camera settings menu.
- **Close Menu button:** Closes the camera settings menu.
- **Navigation Buttons:** Navigates through the camera settings menu. Click on the central button to enter a configuration.
- **Enable Visual Joystick Button:** Enables the visual joystick

#### 6.1.5.6 Visual Joystick

The visual joystick is a tool that simulates the operation of a desktop joystick.

When activating the visual joystick on a camera, it will look like the figure below:



To use the visual joystick, keep the mouse left-clicked and move it to any position in the image. The further away from the center of the image the mouse is, the faster the camera will move, and vice versa.

To perform zoom operations, click the + and - buttons located in the center of the image. You can also use the mouse wheel, turning it forward will bring the image closer and backward the image will move away. Using the mouse wheel you can also set the zoom speed (Viewed by the control on the left side of the image). The closer the red marking is to the center, the faster the zoom will be, and vice versa.

The movement and zoom sensitivity can be adjusted in the operating scale settings on the page [How to configure the Joystick](#)

## 6.1.6 Events

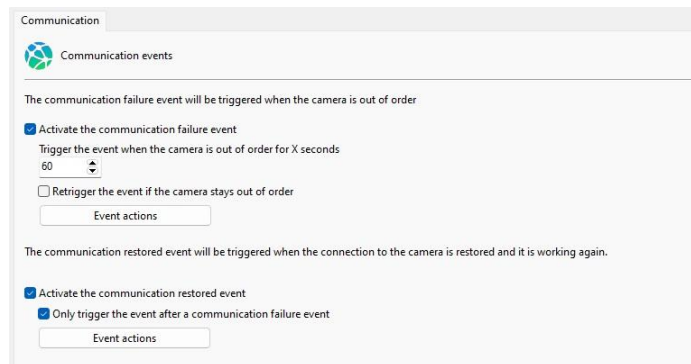
During camera operation in the system, several events occur with it. These events can be communication failures or alarm input events, for example.

By configuring the camera's events, it is possible to specify a set of actions that the system will take when a certain event occurs.

The system provides control over automatic events, that is, events that occur without user intervention, and manual events, which are events generated from user intervention.

### 6.1.6.1 Communication

The system can generate an alert when a camera is out of operation and when it is back in operation.



#### 6.1.6.1.1 Communication Failure Event

The communication failure event consists of checking how long the device is out of operation, so the system will only generate the communication failure event if the device remains out of operation for more than X seconds.

The system still allows the event to continue firing every X seconds while the device is offline, if the option is disabled the system will generate the event only 1 time.

To learn how to configure event actions see [How to configure event actions](#)

#### 6.1.6.1.2 Connection restore event

The connection restore event consists of generating an event when the device returns to function in the system.

The system also allows events to only be triggered if a **communication failure event** for the same object has been triggered previously..

To learn how to configure alarm actions see [How to configure alarm actions](#)

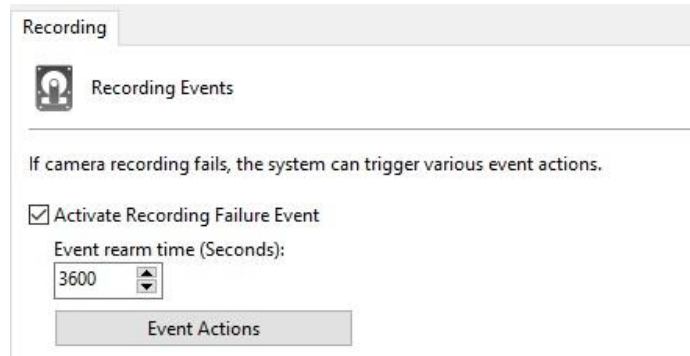
#### 6.1.6.1.3 Device failure report

The Device Failure Report will list all failures and communication recovery with devices in the system, also providing the total failure time for each device.

This report uses the communication recovery event to list and calculate failures, so this event must be enabled for all devices.

To learn how to generate the report, consult the Surveillance Client manual.

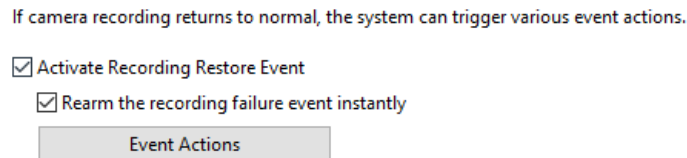
#### 6.1.6.2 Recording Failure Event



The recording failure event is triggered whenever a failure occurs while writing received images to disk.

- **Activate Recording Failure Event:** Activates the recording failure event
- **Event Rearm Time:** Select the desired rearm time (In seconds), where the system will only trigger this event again after the reset time.

To learn how to configure event actions see [How to configure event actions](#)



The "Recording Restore" event can be triggered when the camera successfully resumes recording after a Recording Failure.

- **Activate Recording Restore Event:** Activates the recording restore event
- **Rearm the Recording Failure Event Instantly:** With this option enabled, the Recording Failure Event will reset instantly (Instead of waiting for the previously set reset time) when the Recording Restore Event occurs after a failure.

#### 6.1.6.3 Motion Detection

Motion detection can be used in the system to start a recording or even trigger an alarm. The configuration of this detection can be done in two ways that are explained in the next topics

The following options will be displayed on the Motion Detection tab:

#### 6.1.6.3.1 How to configure motion detection event

To configure the motion detection event, check the **Activate** motion detection event option. Configuring this event involves the following parameters:

- **Activate Motion Detection Event:** Activates the motion detection event.
- **Event rearm time:** Specify the value in seconds that the system will recognize new events after an event has occurred.
- **Time to rearm sending emails:** Specify the time interval in which the system will send another email if the movement event is still recognized.
- **Event Actions button:** Click this button to define the actions that the system will take when the motion detection event is detected. To learn how to configure alarm actions see [How to configure event actions](#)
- **Scheduling:** Click this button to define the times and days of the week when the system should recognize motion events. If this setting is not done, motion events will be recognized 24 hours a day and 7 days a week. The motion detection schedule screen works like the previously discussed recording schedule screen, with the difference that the selection options will only be to Enable or Disable motion detection. To learn how to configure the schedule see [How to configure the recording schedule](#)

#### Note

Enabling motion detection may have a negative effect on the server's CPU. See the [Motion Detection](#) topic for techniques on how to reduce CPU usage

#### 6.1.6.4 Event Variables

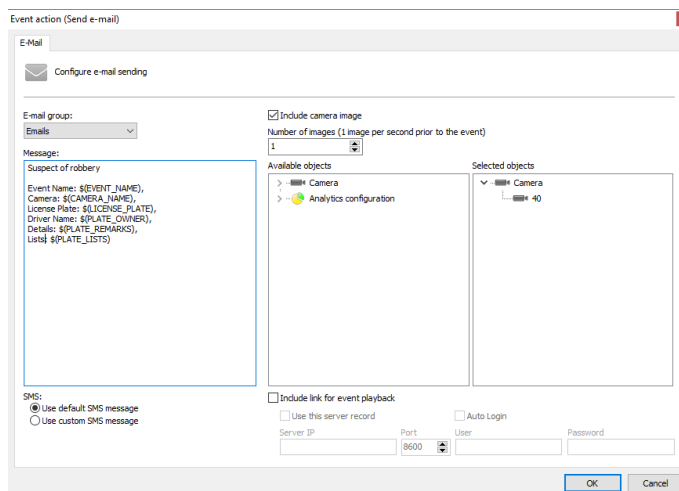
The Event Variables feature allows the use of dynamic variable values within event actions.

The Event Variable value can be accessed by referencing the variable name using a variable name identifier: \$(VARIABLE\_NAME)

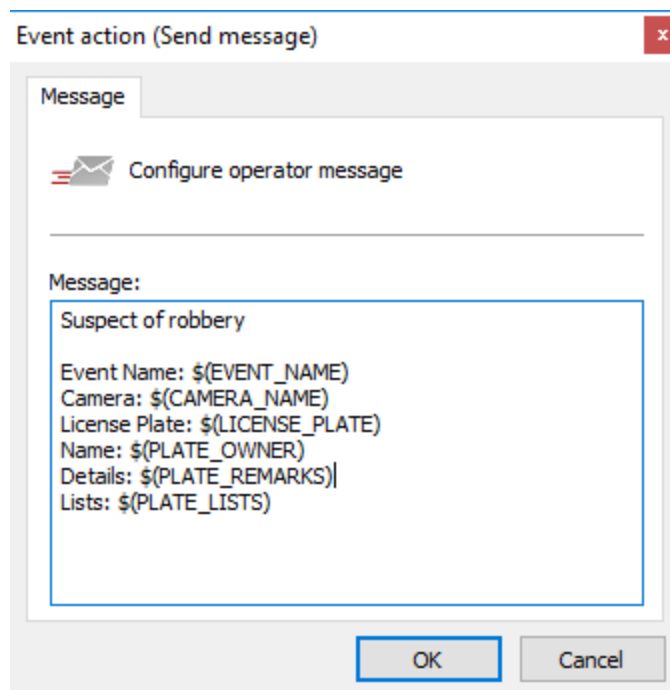
Each system event introduces different types of variables whose values can be used in event actions.

- The following event actions support the use of variables:
- Send Email
- Send Message to Operator
- Send a Push Notification
- Send HTTP Request
- Create Bookmark

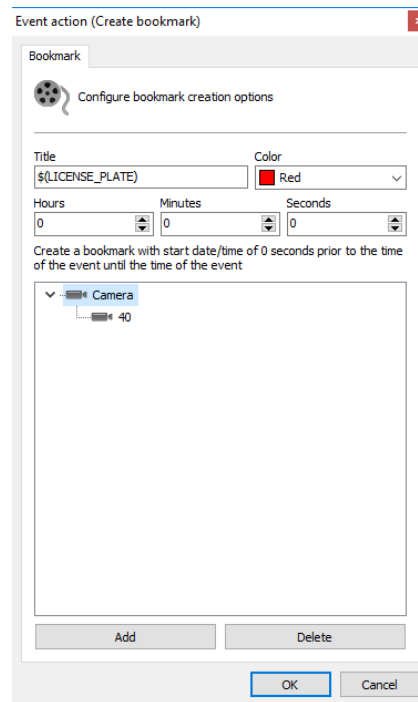
In the example below, an email will be automatically sent with specific data from the LPR event that includes the license plate number and the driver's name if the recognized license plate is marked as stolen:



The same can be configured for messages sent to system operators, adding precious information in the alarm popup:



In the following example, we can create a bookmark with the value of the recognized license plate, which will be displayed in the video player:



To receive the complete document with all system event variables, please contact our support team.

## 6.1.7 Privacy

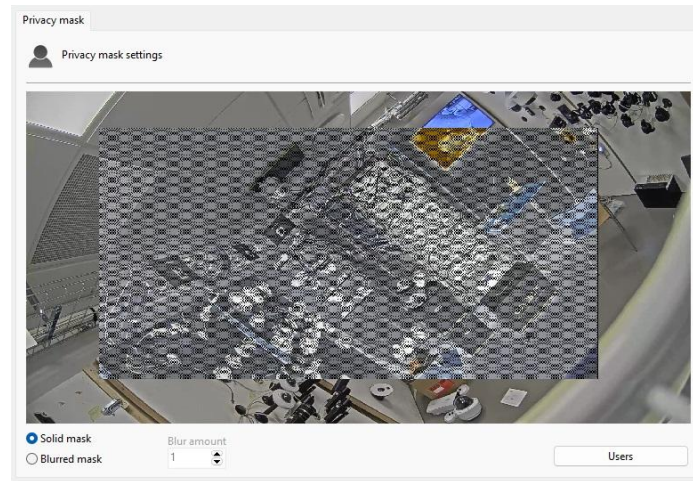
### 6.1.7.1 Privacy Mask

The Privacy Mask consists of a tool that makes it possible to hide areas of the image that cannot be observed by the operator.

It is important to point out that the privacy mask is not saved on the server, on the contrary, the original image is saved and when the image is displayed on the screen the privacy mask is applied.

This feature should only be used on fixed cameras because being an image filter, the mask will not move if a PTZ camera moves, for PTZ cameras you should look for some privacy feature within the camera itself.

To access this feature, click on the **Privacy Mask** tab, as shown in the figure below:



To add a privacy mask, click with the left mouse button on the image and drag it forming a rectangle. To remove a selected area, right-click a rectangle encompassing the entire area of the mask to be removed, or right-click on the image and select **Erase Areas** to delete all created masks. By clicking on the Users button, it is possible to define which users or groups of users will be affected by the mask.

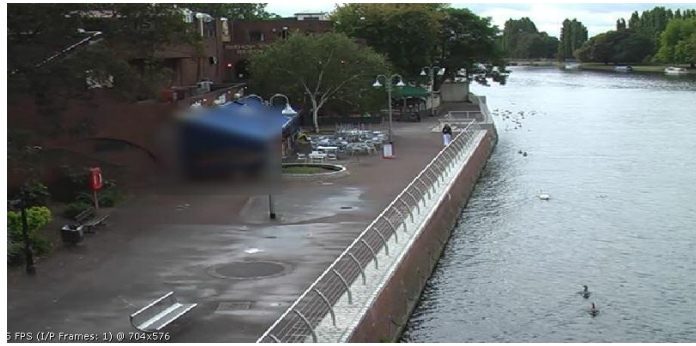
You can select two types of privacy mask: **Solid** or **Blurred**.

**Solid** will generate a completely black mask. The effect of the opaque mask is shown in the figure below:



The **Blurred** mask can generate a mask with levels of transparency that can be configured within a scale of 1 to 10. The image below shows the application of the blurred mask:

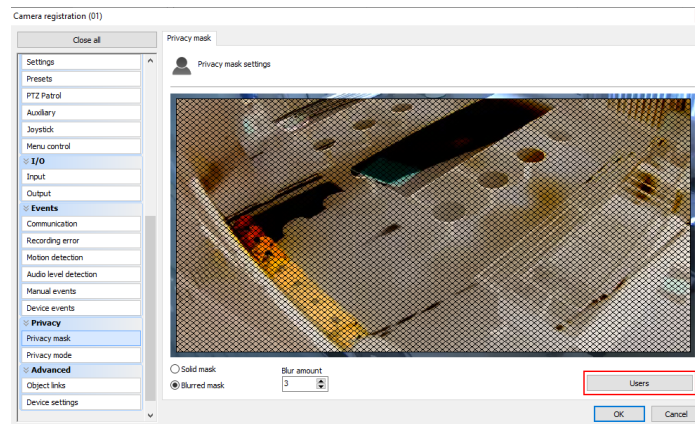




Another usage example:



Privacy Mask can be conditionally applied to specific users / user groups.



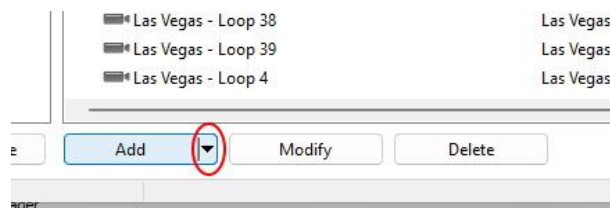
### 6.1.8 Multi-Channel Device Registration

The system enables easy registration for multi-channel devices such as: DVRs, NVRs, Video Servers, Cameras with multi-lenses, etc.

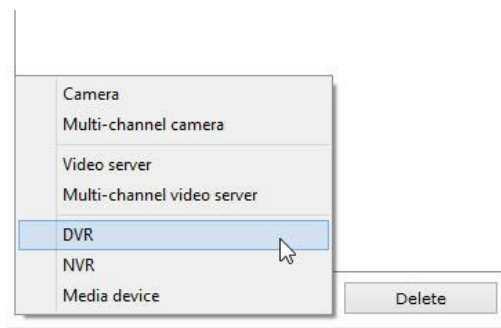
This option allows all channels on a device to be registered at once.

To access this option, simply click on the arrow available next to the **Add** button as shown in the image below:



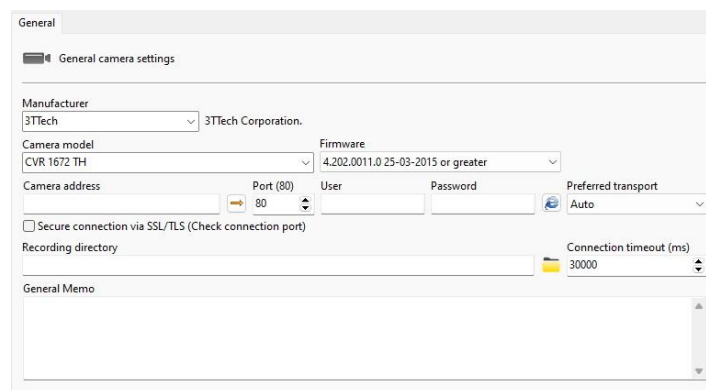


The options for supported devices that can be registered will be shown as in the image below:



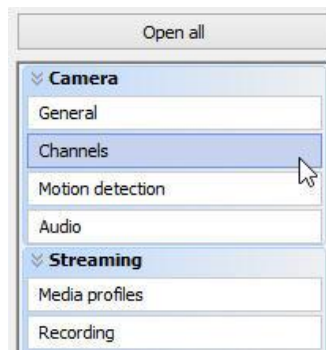
Select the option compatible with the equipment you want to register, for example, DVR.

After selecting the device type, the system will filter the list of models containing only the selected device type:



On this screen, the basic information of the equipment must be filled in, as already discussed in the [General](#) topic of camera registration

After filling in the data, click on the **Channels** option located in the side menu as shown below:



The following screen will be displayed:

The following options will be available:

**Automatically Name Channels:** Allows a naming pattern to be applied to all channels on the device.

- **Channel Name:** Desired name for the channel. Use the /i shortcut in the text to be replaced by the channel number.
- **Initial:** Initial number that will be applied to channels.
- **Digits:** Number of Digits that will be applied in the nomination.
- **Apply only to activated channels:** Applies the naming sequence only to channels activated at the bottom of the screen.
- **Execute:** Applies the naming pattern to all channels.

**Example:** To register a DVR with the naming pattern: Cam 01, Cam 02, Cam 3, etc., we must perform the following configuration:

In the **Channels** area it is possible to check/modify the appointment applied. It is important to remember that each channel will be registered as an independent device, thus consuming 1 recording license per registration.

### +Note

The device name cannot be changed after registration.

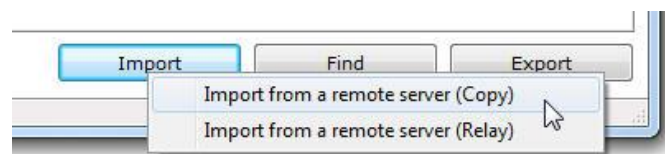
Recording folders will be created with the chosen names for the channels within the chosen root folder.

To complete the registration, simply click OK and all channels on the device will be included simultaneously.

Name	Description	Port	Connection timeout	Recording Self-Healing
Cam 01	Cam 01	80	30000	Inactive
Cam 02	Cam 02	80	30000	Inactive
Cam 03	Cam 03	80	30000	Inactive
Cam 04	Cam 04	80	30000	Inactive
Cam 05	Cam 05	80	30000	Inactive
Cam 06	Cam 06	80	30000	Inactive
Cam 07	Cam 07	80	30000	Inactive
Cam 08	Cam 08	80	30000	Inactive
Cam 09	Cam 09	80	30000	Inactive
Cam 10	Cam 10	80	30000	Inactive

## 6.1.9 Import Cameras From Other Servers

The system allows you to import objects from other servers, as described in the [Object Import](#) topic, but the system offers extra options for importing cameras:



**Import cameras from a remote server (copy):** When the import is made as a copy, the settings will come exactly as from the imported server. An important example is the recording unit: if on the source

server the cameras are recording in the E: directory and on the current server this unit does not exist, the camera will not record.

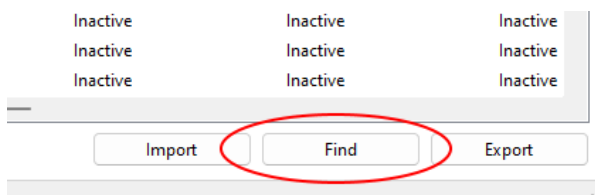
**Import cameras from a remote server (relay):** When the import is done as a relay, the current server will register the cameras with the Digifort RTSP Server driver, which in this case will fetch the images from the source server.

See the [Object Import](#) topic for more information on how to import objects.

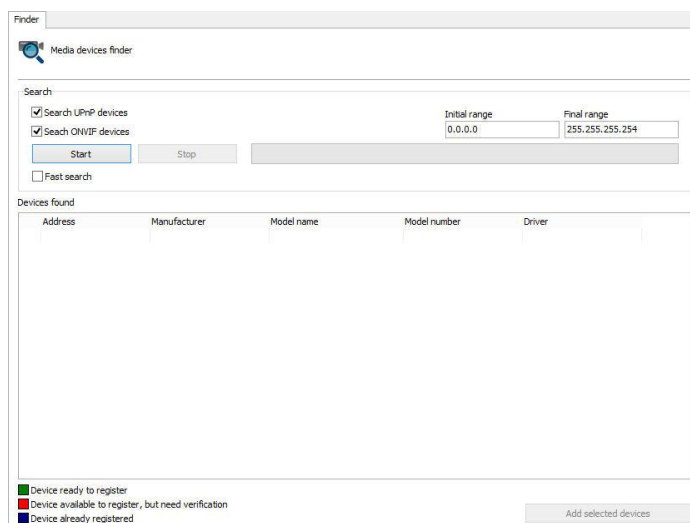
### 6.1.10 Finding and Registering Cameras Automatically

The system has the option for cameras that support the UPnP and ONVIF protocols to be located and registered automatically.

On the camera registration screen, click the **Search** button as shown in the image below:



The following screen will be displayed:



On this screen the search for equipment is carried out. The UPnP equipment search takes an average of 40 seconds to find the equipment. This happens because in addition to finding the equipment that responded to a request, this search searches for UPnP broadcast packets on the network, making the search find more devices.

- **Search for UPnP Devices:** Enable device search via UPnP
- **Search for ONVIF Devices:** Enables searching for ONVIF devices
- **Fast Search:** The quick search takes an average of 15 seconds to find the equipment. This search only finds devices that responded to the UPnP request made by the system. To activate quick search just click on the **Fast Search** check box

- **Initial Range and Final Range:** Limits the search within the established IP range.

To start the search, click **Start** and the message **Wait, locating devices (wait, location devices)** will appear while the equipment is being located. Once found, the equipment will be listed as shown in the figure below:

Address	Manufacturer	Model name	Model number	Driver
192.168.10.121	Pelco	IX30DN	IX30DN	Pelco Sarix IX30DN
192.168.5.120	Zavio	Fixed CMOS Camera (Two way a	F312A	Zavio P312A
192.168.5.105	Panasonic	Network Camera	BB-HCM311A	Panasonic BB-HCM311
192.168.5.104	Panasonic	Network Camera	BB-HCM515A	Panasonic BB-HCM515
192.168.5.124	Panasonic	Network Camera	BB-HCM705A	Panasonic BB-HCM705A
192.168.5.109	Vivotek	Network Camera	TC5330	Vivotek TC5330
192.168.5.118	Vivotek	Mega-Pixel Network Camera	IP7151	Vivotek IP7151
192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138
192.168.5.114	Vivotek	Network Camera	TC5330	Vivotek TC5330
192.168.5.103	Panasonic	Network Camera	BL-C160A	Panasonic BL-C160A
192.168.5.123	Panasonic	Network Camera	BB-HCM527A	Panasonic BB-HCM527A
192.168.5.111	VIVOTEK INC.	Network Camera with Pan/Tilt/Zoom	PZ71X1	
192.168.10.102	Microsoft Corporation	Windows Media Player Sharing	12.0	
192.168.5.108	UPnP IGD Project	test	0.92	
192.168.5.130	Brickcom	WPB-100Ap	v3.0.4.0	Brickcom WPB-100Ap
192.168.5.131	Axis	AXIS P1346	P1346	Axis P1346
192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534

Three types of statuses can be found according to the captions in the lower left corner of the screen:

- **Green - (Device ready to register):** These are the cameras found that have their manufacturers and models already supported by the system. These camera equipment are ready to be added.
- **Red - (Device available to register but needs verification):** These are devices that were not found in the system driver base. This case may occur because the equipment is not actually approved or because the name of the manufacturer/driver is written differently than what is registered in the system. If the name is incorrect, it can be corrected on the screen using a selection box as shown in the figure below:

Address	Manufacturer	Model name	Model number	Driver
192.168.5.105	Panasonic	Network Camera	BB-HCM311A	
192.168.5.111	VIVOTEK INC.	Network Camera with Pan/Tilt/PZ71X1		
192.168.5.131	AXIS P1346	P1346		
	Windows Media Player Sharing	12.0		

- **Blue - (Device already registered):** These are devices that are already registered on the server.
- **Gray - (Device cannot be registered):** In this case, the located equipment or program did not return any IP address and cannot be added automatically.

There are two ways to register the equipment found.

#### 6.1.10.1 Single Camera Registration

Select a device using the selection box as shown in the figure below:

Address	Manufacturer	Model name	Model number	Driver
<input checked="" type="checkbox"/> 192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
<input type="checkbox"/> 192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138

After selecting the equipment, click on the **Add Selected Equipment** button and the camera registration screen will be shown with the **Manufacturer**, **Camera model**, **IP** and **Port** fields already filled in.

### 6.1.10.2 Multiple Camera Registration

This feature can register several cameras at the same time with sequential numbers. To start, select several devices using the selection box as shown in the figure below:

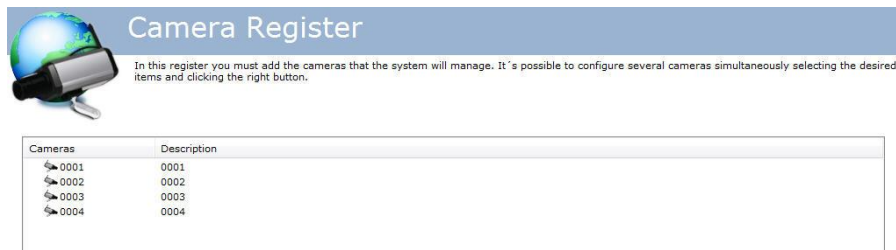
	Address	Manufacturer	Model name	Model number	Driver
<input checked="" type="checkbox"/>	192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
<input checked="" type="checkbox"/>	192.168.5.131	Axis	AXIS P1346	P1346	Axis P1346
<input checked="" type="checkbox"/>	192.168.5.120	Zavio	Fixed CMOS Camera (Two way F312A		Zavio F312A
<input checked="" type="checkbox"/>	192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138
<input type="checkbox"/>	192.168.5.115	3S Vision	Internet Camera		3S Vision N1071

After selecting the equipment, click the **Add Selected Equipment** button and the following screen will appear:

The information provided on this screen will be applied to all cameras to be registered:

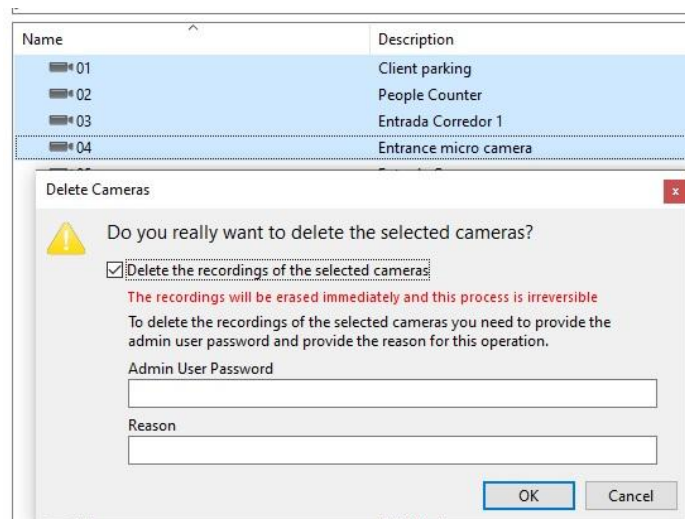
- **Device Name:** Allows you to name one or more cameras. To add the numbering after the initial name, simply place the key "/" in the text.
- **Device Initial Number:** The name of the cameras will be registered in the form of a sequence of numbers. In this field, the initial number from which the count will begin is defined.
- **Digit Count:** Number of desired houses. **Ex:** If the count starts with the number 1 and the number of decimal places is 4, then the name of the first registered camera will be 0001.
- **Device Username:** User that will be used for the server to authenticate to the devices.
- **Device Password:** Senha que será usado para o servidor autenticar-se nos dispositivos.
- **Recording Root Directory:** Enter a directory where the system will create a folder for each camera where your recordings will be stored. This folder will have the same name as the camera (Ex: 0001, 0002, etc.).

After registering the various cameras, their respective status will automatically change to **BLUE (Camera already registered)**. This way, the cameras were successfully registered as shown in the image below:



## 6.2 How to Delete a Camera

To delete registered devices, simply select one or more and click the **Delete** button.

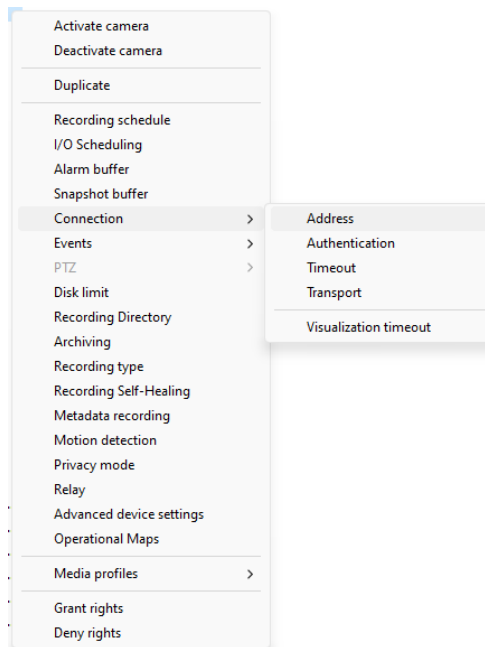


- **Delete recordings from selected cameras:** With this option checked, the system will delete recordings from the cameras that are being deleted. For security reasons, the **Admin** user password must be provided for this process.
  - **Admin User Password:** Provide the **Admin** user password to delete camera recordings.
  - **Reason:** Provide a reason for camera recordings to be deleted. This information will be recorded in the [Audit Log](#) along with the date/time and user information that deleted the cameras.

## 6.3 How to Change Parameters for Multiple Cameras Simultaneously

As already explained in the [Multiple Object Configuration](#) topic, the system allows basic configurations common to all selected cameras to be applied simultaneously.

Select the desired cameras and right-click, opening the **Options Menu**, as shown in the figure below:



Most of the options you can change are self-explanatory and you can consult the [Camera Registration](#) topic to learn more about each option. Some options require a little more explanation and will be described in sub-topics.

### 6.3.1 Recording Directory

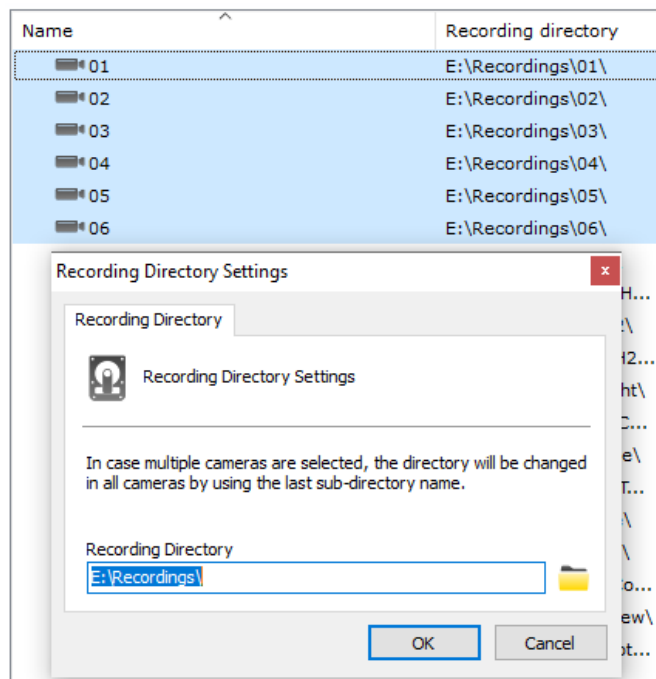
Allows changing the recording root directory of multiple cameras simultaneously.

The system allows you to define a "Root" directory that will be used as a base for all cameras. The name of the last subdirectory (usually the camera name) will be kept. For example, if the camera is currently recording at "E:\Recordings\01" and you want to change it to "E:\NewRecordings", the system will change the directory of this specific camera to "E:\NewRecordings\01", and so on for all selected cameras.

#### Important

Changing directories will not move recordings from the old directories to the new ones, this procedure must be done manually, with the server service stopped.





### 6.3.2 Add, Modify or Delete Media Profiles

This feature allows Adding, Modifying or Deleting Media Profiles for multiple cameras simultaneously as long as they have the same media profile options.

#### +Tip

You can select all cameras that share a media profile driver, select a desired camera and press **Ctrl + M**. If there are cameras with the same media profile driver as the selected camera, it will automatically be selected

Let's exemplify how the logic works in case of multiple selection for profiles. In our example we will use two cameras with the following configurations:

#### Camera 1

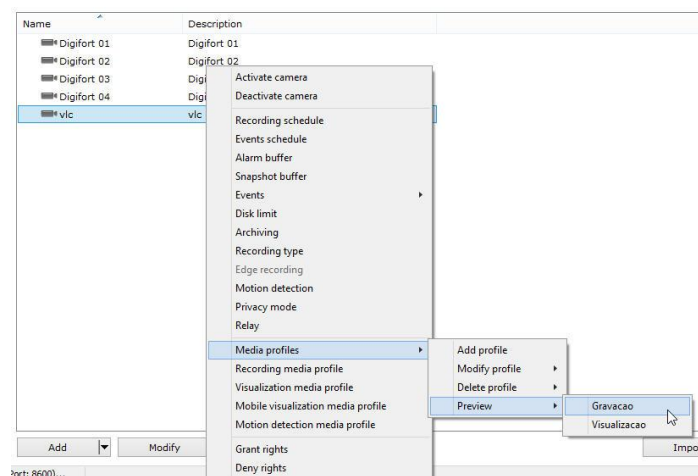
View Profile  
Recording Profile  
Mobile Profile

#### Camera 2

Recording Profile

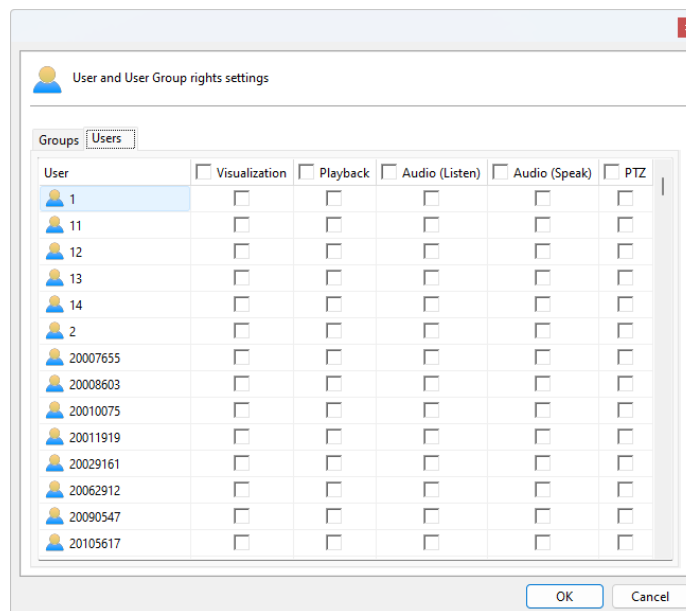
Let's analyze the following hypotheses separately:

- If a **View Profile** is added, this profile will only be included in **Camera 2** and the existing one in **Camera 1** will be **modified** according to the new configuration;
- In the case of **Modifying** the **View Profile**, the changes will only be made on **Camera 1**;
- In the case of **Modifying** the **Recording Profile**, the changes will be made in both Cameras;
- In the case of **Mobile Profile Deletion**, it will only take effect on camera 1;
- In the case of **Deletion** of the **Recording Profile**, both cameras will have their profile deleted;
- You can also see the camera image from the list by clicking on Preview:



### 6.3.3 Grant and Deny User Rights

This option will allow you to grant or deny user rights to multiple cameras simultaneously. When selecting the **Grant** or **Deny Rights** option, the following screen will be displayed:



In both **Grant** and **Deny Rights** operations, rights will be added or subtracted from the selected cameras.

In the **Grant Rights** operation, select the rights you want to **assign** to users or groups of users. The selected rights will be **added** to the current list of rights for each camera. selected.

In the **Deny Rights** operation, select the rights you want to **remove** from users or user groups. The selected rights will be **removed** from each camera's current list of rights.

## 6.4 Camera Groups

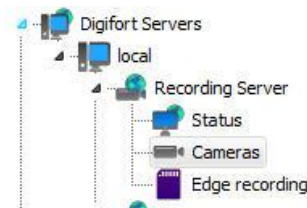
The system allows the creation of Camera Groups for better organization of objects.

In the Surveillance Client, the groups will be part of the object list and the cameras belonging to the groups will be added below them.

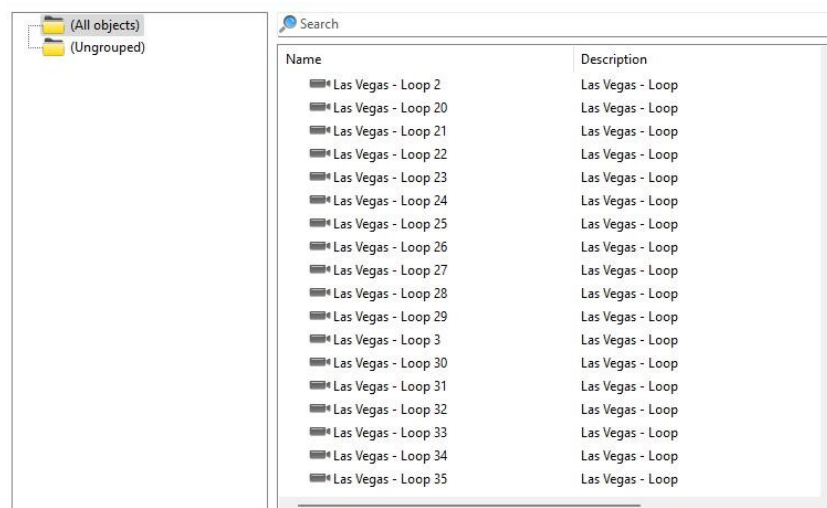
The Surveillance Client offers great flexibility to work with groups:

- You can drag and drop a group onto the screen and the cameras in that group will be added to the monitoring.
- To add the group's cameras and all cameras from all subgroups to the screen, simply press and hold the Shift button while dragging and dropping the desired group.
- You can drag and drop a group into the media player for playback from the group's cameras. To add subgroup cameras, simply hold down the Shift key while dragging and dropping.
- By right-clicking on the group, you can playback all the cameras in the group and, if desired, the cameras in all subgroups as well.
- By right-clicking on the group, it is possible to send all cameras in the group to the virtual matrix, and if desired, cameras from all subgroups as well.

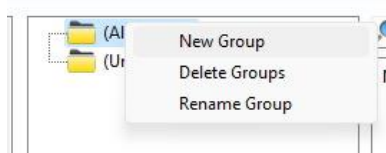
To create groups of cameras, access the Camera Registration, locating the Recording Server icon and then click on the Cameras icon, as shown in the figure below:



Once this is done, the camera registration will be displayed, as shown in the figure below:

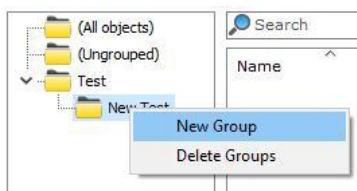


To add a group, click the add button in the groups section, on the left, or right-click on the group zone as shown in the image below



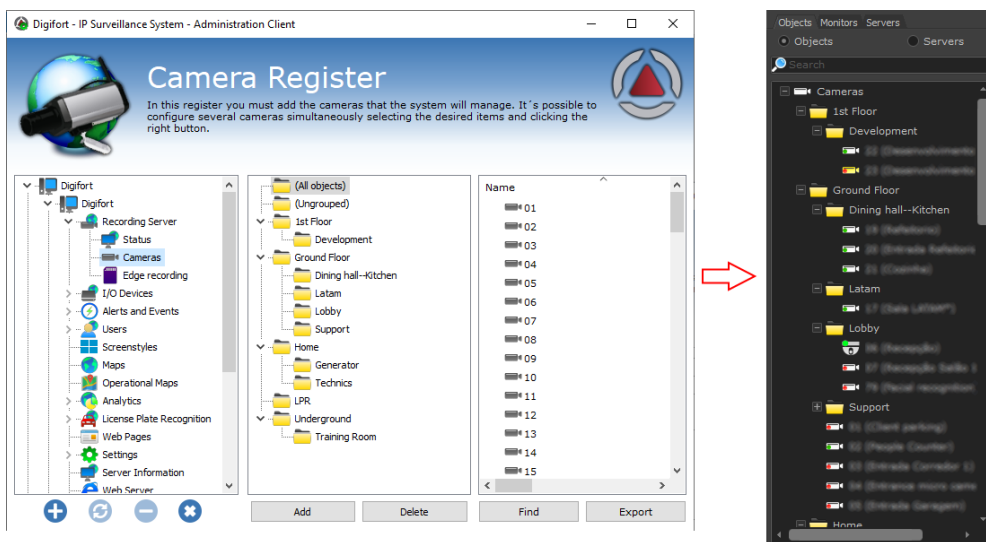
When clicking on the **Add** button, the system will ask for the name of the group to be created and then the group will be available in the list

Once the group has been created, to add one or more cameras to the group, simply select the desired camera(s) and drag it to the group. It is also possible to create subgroups, to do this, select the parent group and click the **Add** button or right-click and select **New Group**. You can also move groups and place them within subgroups using drag and drop.



Once the groups have been created the system will only list cameras belonging to the selected group.

Example of operation with the Surveillance Client:



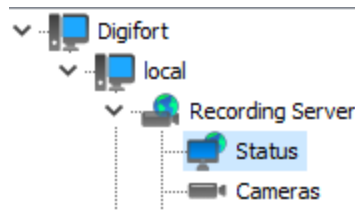
### +Tip

Camera Groups can be synchronized between servers using the Master / Slave function.

## 6.5 Monitoring Recording Server Status

In this area of the system you can check the general status of all cameras registered in the system.

To access this function, select the Status item within Recording Server in the Settings Menu, as illustrated in the figure below:



The status screen allows the selection of custom columns with new information to be displayed in the list (By right-clicking on the list header) and ordering by any column in the list and it is also possible to export the current data to a .CSV file.

This screen has a list of cameras with information about each camera and a dashboard next to the list, with information summarized for all cameras.

With the Camera Groups feature, when selecting a group (or multiple groups), the records will be filtered to display only cameras from the selected groups.

**Left Sidebar:**

- (All objects)
- (Ungrouped)
- Teste

**Central Table:**

Name	Working	Description	Activated
Camera 40	Yes	Camera 40	Yes
Cam 01	No	Cam 01	Yes
Cam 02	No	Cam 02	Yes
Cam 03	No	Cam 03	Yes
Cam 04	No	Cam 04	Yes
Cam 05	No	Cam 05	Yes
Cam 06	No	Cam 06	Yes

10 Disabled camera(s) for lack of license. Click for more information.

**Right Sidebar Dashboard:**

- 226** Total
- 7** Activated
- 219** Deactivated
- 1** Working
- 6** Not Working
- 7** Configured to Record
- 1** Writing to Disk
- 29** Total FPS
- 29** Recorded FPS
- 0** Highest recording buffer
- 9.78 mbits/s** Total received data rate
- 1.22 MB/s** Total recording rate

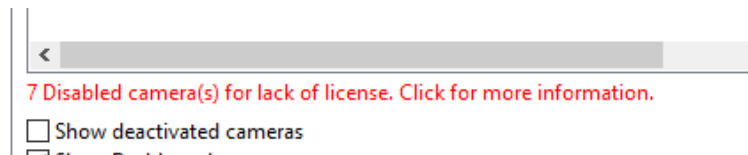
**Buttons:** Search, Export

Details:

- **Total:** Total number of cameras registered on the server.
- **Activated:** Number of activated cameras.

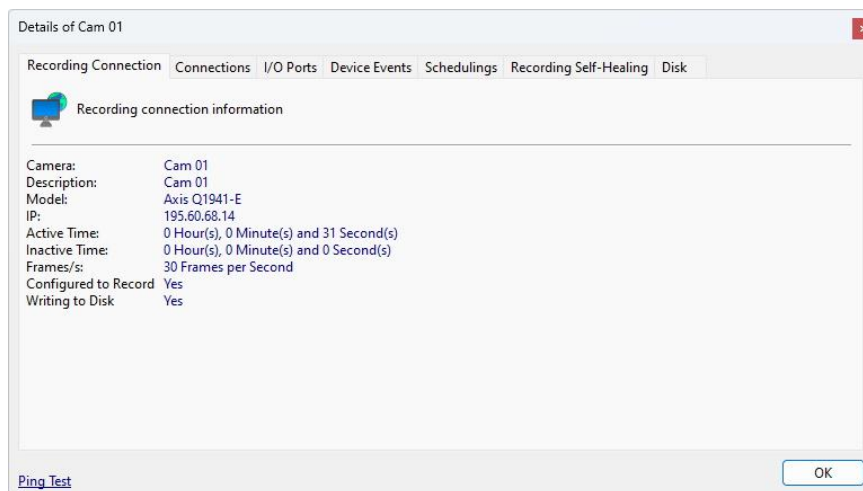
- **Deactivated:** Number of cameras disabled.
- **Working:** Number of cameras in operation.
- **Not Working:** Number of cameras currently out of operation.
- **Configured to Record:** Number of cameras that are configured to record.
- **Writing to Disk:** Number of cameras that are currently writing to disk. This value may vary if cameras are recording by event or movement.
- **Total FPS:** Total number of Frames per Second being transmitted to the server.
- **Recorded FPS:** Number of Frames per Second being recorded on the server.
- **Larger recording buffer:** The longest recording buffer time among server cameras.
- **Total received data rate:** Amount of data received by the server over the network.
- **Total recording rate:** Amount of data being written to disks per second.
- **Disks:** A summary of free and occupied disk space on each disk in use (Each disk will have an item on the dashboard).

The system may also display a warning regarding objects deactivated due to a lack of available licenses:



## 6.5.1 Individual Camera Details

You can view additional camera details by simply double-clicking the camera item in the status list.

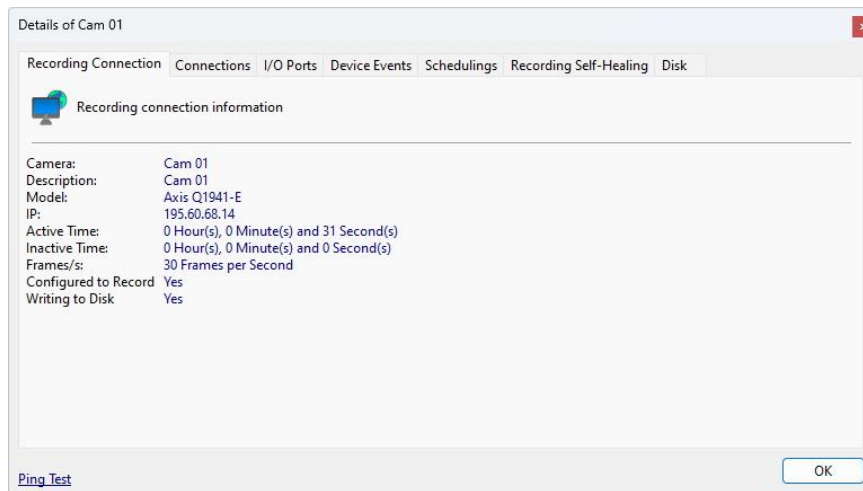


The above screen will be displayed with detailed camera information.

- **Ping Test:** Opens a window with the camera ping test.

### 6.5.1.1 Recording Connection

This screen provides us with detailed information about the connection used with the camera for recording images, as illustrated in the figure below:



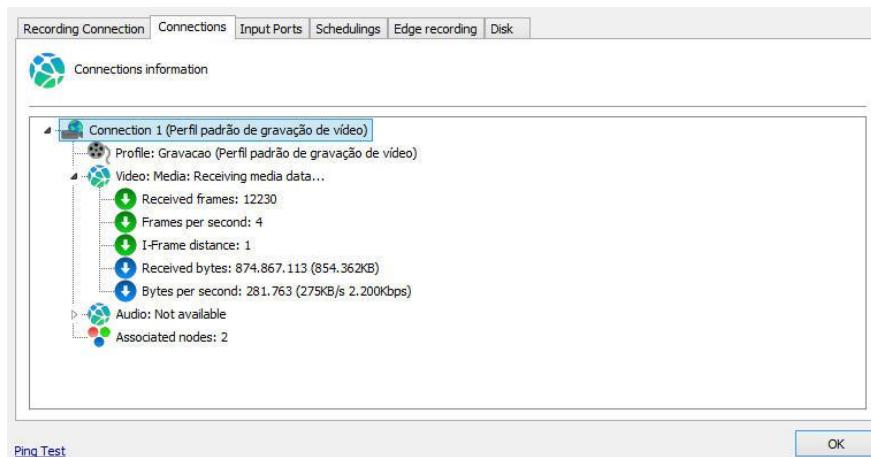
- **Camera:** Name of the registered camera.
- **Description:** Description of the registered camera.
- **Model:** Model of the registered camera.
- **IP:** IP address of the camera.
- **Active Time:** Time of camera activity since activation or parameter change.
- **Inactive Time:** Camera downtime. If the camera is out of order, this is the total time it has been out of order. Reactivating or changing the object's settings will reset this value. This value will be reset when the camera starts working again.
- **Frame/s:** Frames per second being received from the camera.
- **Configured to Record:** Indicates whether the camera is set to record
- **Writing to Disk:** Indicates whether the camera is currently recording to disk (Varies during recording by motion or event).

#### 6.5.1.2 Connections

This screen gives us information about all connections made with the camera for video recording and viewing.

The connections are displayed in a list in tree format, that is, with items, showing the type of connection, and sub-items, showing the details of the connection.

To access this feature, click on the **Connections** tab, as shown in the figure below:.



- **Profile:** Media profile associated with the connection. To learn what a media profile is see [Media profiles](#)
- **Frames Received:** Frames received from the camera with this connection since its activation or parameter change.
- **Frames Per Second:** Frames per second being received in real time.
- **I-Frame Distance:** Shows the number of frames between received I-Frames.
- **Bytes Received:** Bytes received from the camera with this connection since its activation or parameter change.
- **Bytes per Second:** Bytes per second being received in real time,
- **Associated Nodes:** Number of resources using this connection. In this case, this connection is being used only for recording images, showing the value 1. If the camera is also being monitored through the Relay Server through this connection, the value 2 will be shown. The value of nodes will increase according to the number of client connections opened viewing this camera.

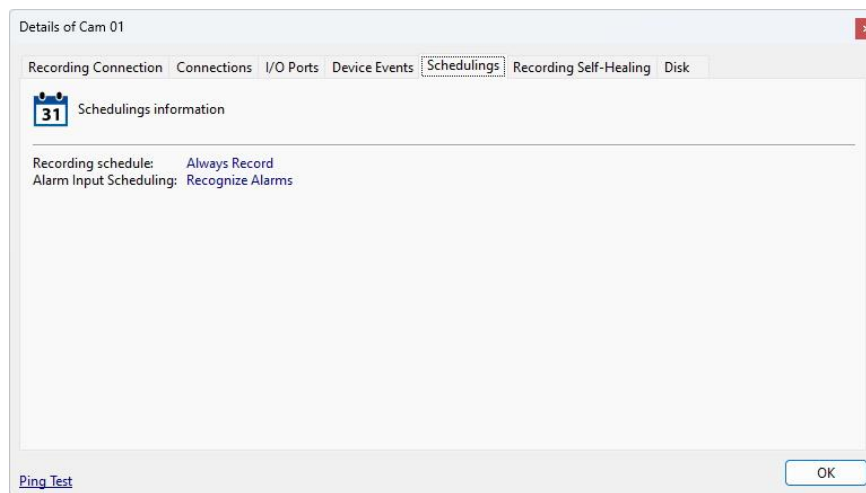
### 6.5.1.3 Schedulings

This screen provides us with information about the current recording type, whether they are continuous recording, motion recording or not recording.

The type of recording is defined in the camera register. To learn how to define the type of recording see [Recording](#).

To access this feature, click on the **Schedulings** tab, as shown in the figure below:



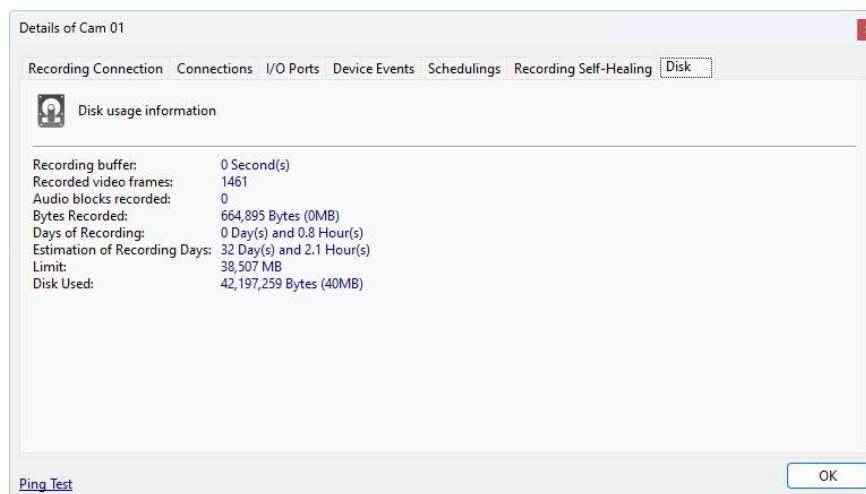


- **Recording Scheduling:** Indicates the current state of the recording schedule.
- **Alarm Input Scheduling:** Indicates the current status of I/O system event scheduling

#### 6.5.1.4 Disk

This screen provides us with information about the camera's disk space usage.

To access this feature, click on the **Disk** tab as shown in the figure below:



- **Recording Buffer:** Current size of the Recording Buffer. A high value (above 5 seconds) may mean disk performance problems.
- **Recorded Video Frames:** Total number of video frames recorded since activation or parameter change.
- **Recorded Audio Blocks:** Total number of audio blocks recorded since activation or parameter change.
- **Bytes Recorded:** Recorded bytes of the camera since its activation or parameter changes.
- **Recording Days:** Number of days stored on disk.
- **Estimated Recording Days:** Approximate estimate of recording days based on current allocated disk space for the camera.
- **Limit:** Limit allocated for recording camera footage.

- **Disk Used:** Disk space used by camera footage.

# Chapter



VII

## 7 Alerts and Events

The system offers a series of alerts and alarms that help monitor the normal operation of a set of cameras and the server itself. These alerts are configured by the system administrator, according to the individual needs of each solution, and can be modified at any time as a new need arises.

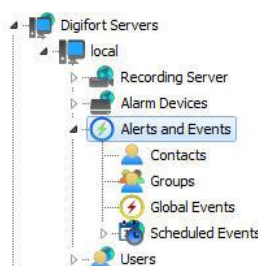
The alerts and events functions allow the system to send e-mails or SMS messages to a list of users previously registered in the system every time an event programmed by the administrator occurs. An event can be, among others, a communication failure between the camera and the server, a data recording failure, a motion alert, or an alert associated with an external electrical device. All alerts are also recorded in a log file for later consultation and analysis.

Alerts and alarms are activated immediately after they are configured, with no need to stop the system for a configuration to take effect. An alert can be made for the entire system or for a specific camera.

Monitoring these alerts is the responsibility of the person the administrator has delegated control to. The lack of interest in verifying the anomalies detected and reported by the system is considered a serious failure, which could compromise security as a whole.

### 7.1 How to Access Alerts and Events

To access alerts and events, click on the Alerts and Events item in the Settings Menu, as shown in the figure below:



#### 7.1.1 How To Configure Contacts

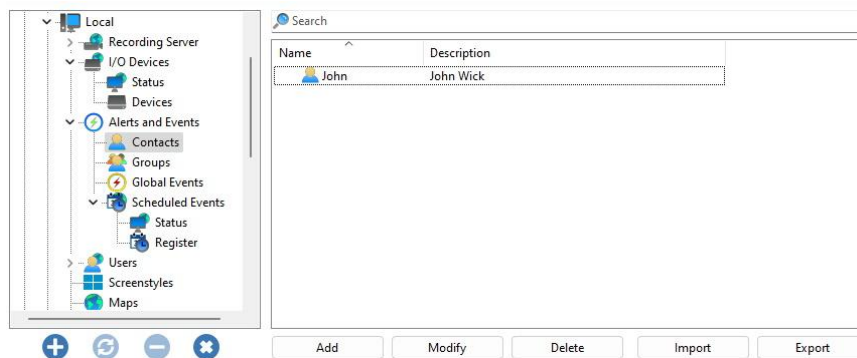
Contacts are system entities who are responsible for receiving system alert emails. In other words, contacts are people registered in the system with information such as name, phone number and e-mail. And with this information, the system is able to alert them.

Contacts and contact groups are used for event action notification via email, SMS or Push Notification.

The system does not send emails or alerts to just one contact, but to groups of contacts.

To access the contact register, click on the **Contacts** item.

Once this is done, the contact register will be displayed on the right, as shown in the figure below:



To add a contact, click on the **Add** button. To change a contact select it and click on the **Modify** button. To delete a contact, select it and click on the **Delete** button.

#### 7.1.1.1 How To Add A Contact

After clicking on the **Add** button, as explained in the previous topic, the screen for adding contacts will be displayed, as illustrated in the figure below:

- **Contact:** Internal name of the contact. This name must be unique and cannot be changed after saving, as this information is for internal use by the system.
- **Contact Name:** Contact's full name.
- **Contact Description:** A brief description of the contact aiming at easy identification. This field can contain the contact's role in the company, for example.
- **Address:** Address of the contact.
- **Phone:** Contact phone.
- **Company:** Contact company.
- **Email:** Contact email. It is to this email that the system will send the notifications configured by the administrator.
- **Format message for SMS:** Sends the notification to a cell phone in SMS format instead of sending it by email. In this case, the cell phone e-mail must be specified in the "E-mail" field.

- **Mobile device ID for Push Notification:** This ID will be used in the configuration of events with the action for sending push notification, the ID can be found directly in the **Mobile Client** application.

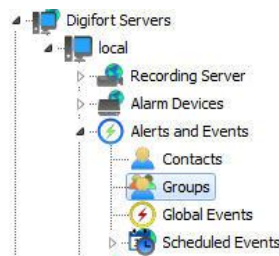
### +Note

Sending SMS messages is a service external to the system and is the responsibility of the cell phone operator that will receive the message. Check the availability of this service with your carrier.

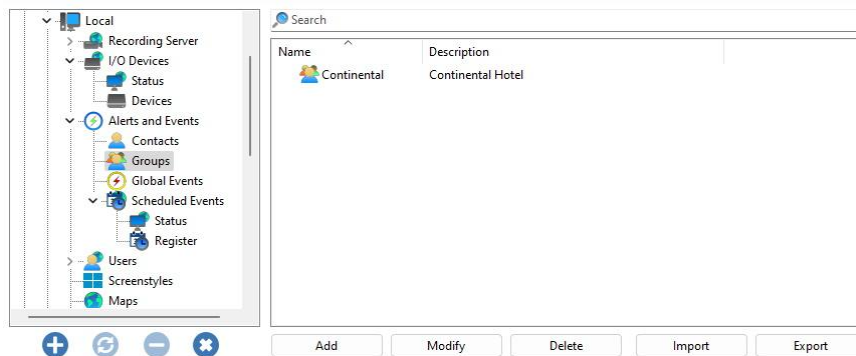
## 7.1.2 How To Set Up Contact Groups

Creating groups of contacts is necessary as the system does not send notification emails to just one contact, but to a group of contacts.

To access the registration of groups of contacts, click on the item Groups, as shown in the figure below:



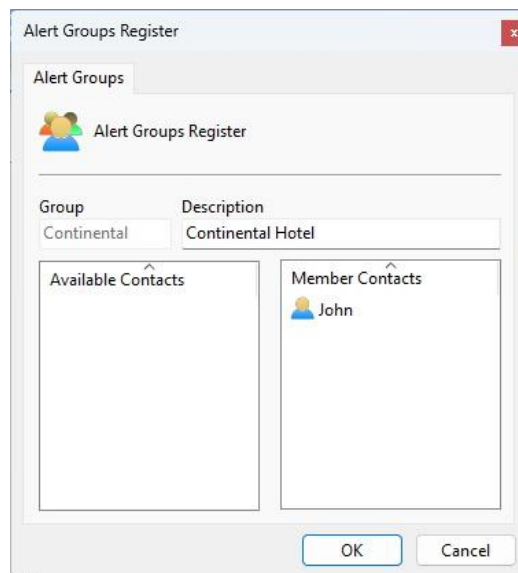
Once this is done, the group registration will be displayed on the right, as shown in the figure below:



To add a contact group, click on the **Add** button. To change a contact group, select it and click on the **Change** button. To delete a contact group, select it and click **Delete**.

### 7.1.2.1 How To Add A Contact Group

After clicking on the **Add** button, as explained in the previous topic, the screen for adding contact groups will be displayed, as illustrated in the figure below



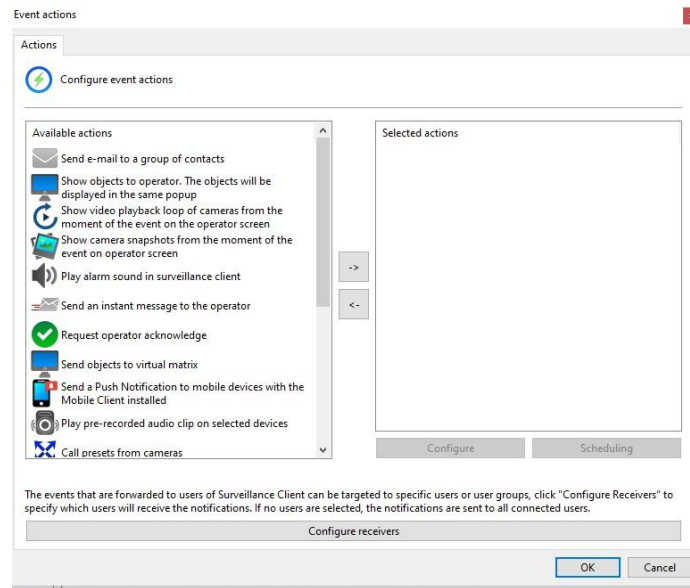
- **Group:** Name of the contact group. Once saved, this name cannot be changed, as it will be used internally by the system.
- **Description:** Description of the contact group.
- **Available Contacts:** List of all contacts registered in the system.
- **Member Contacts:** List of contacts belonging to the group.

To **add** contacts to the group, select the desired contact from the list of available contacts and drag it to the list of belonging contacts.

To **remove** a contact from the group, select the desired contact from the list of belonging contacts and drag it to the list of available users.

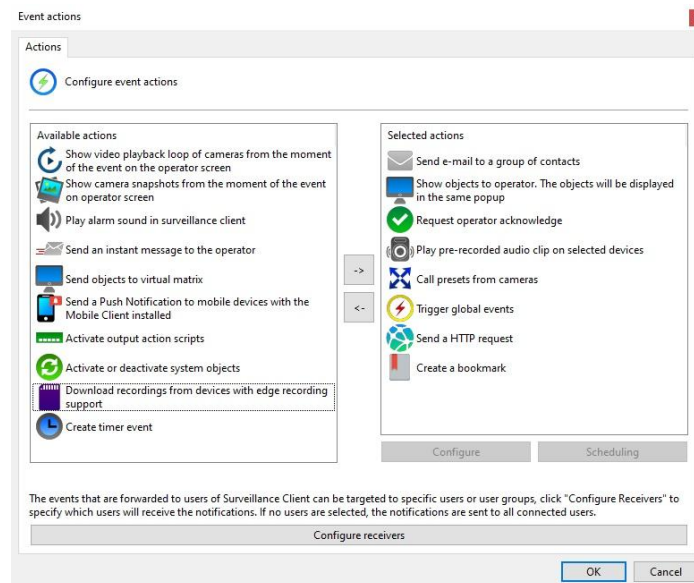
## 7.2 How to configure event actions

Several events require the configuration of event actions. To access these settings, click on Event Actions corresponding to the configuration performed. By clicking this button, the alarm configuration screen will be displayed as shown in the figure below:



Depending on your system edition, each event action has its own individual schedule so you can configure what times and days of the week events can occur.

To enable any of the events, simply click and drag the **Selected Actions** to the list on the right, as shown in the image below:



To configure an action, select the desired action in the list on the right (Selected Actions) and click the **Configure** button or double-click on the desired action.

To schedule when an action will be performed, select the desired action from the list on the right (Selected Actions) and click the **Schedule** button. The event action scheduling screen works like the previously discussed recording scheduling screen, with the difference that the selection options will only



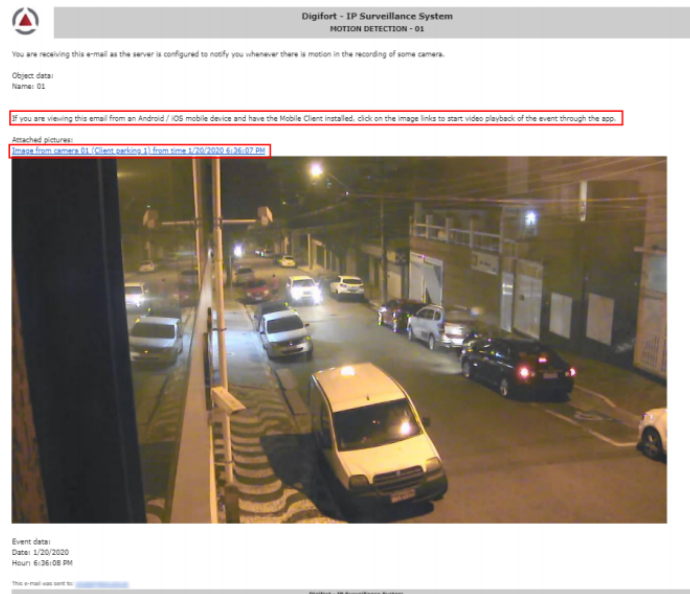
be to Enable or Disable the action. To learn how to configure the schedule, see [How to configure the recording schedule](#)

## 7.2.1 Send an email to a group of people when an alarm occurs

Sends a notification email to an alert group when an event occurs.

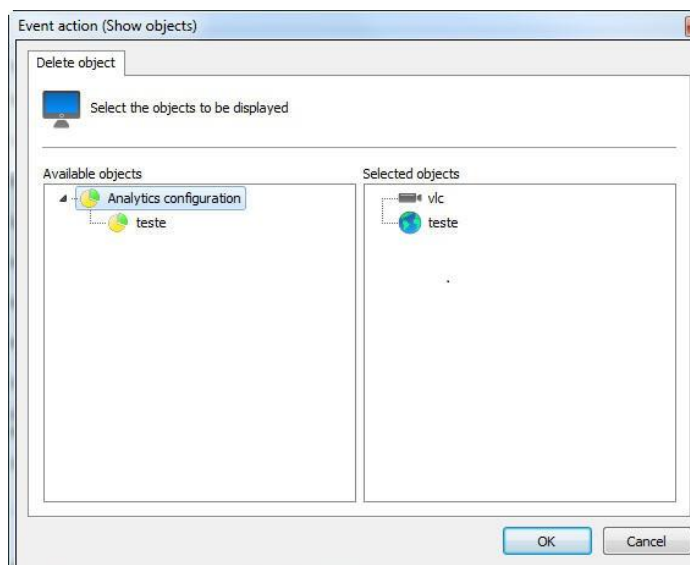
- **Alert group:** Select the alert group that will receive event notification via email.
- **Message:** Configure the message that will be sent in the body of the email.
- **Include images from cameras:** It is possible that in any event, an image from one or more Cameras/Analytics is attached to the email sent. Just drag the desired object to the Selected Objects list. In the case of analytics, the image will be rendered along with the metadata. See the chapter Metadata.
- **Number of Images:** Allows you to attach multiple images of an event when sending emails. The interval between the number of images will be 1 second.
- **Include link for Playback of the event:** It is possible to attach a script file that, when executed, will open the Surveillance Client and reproduce the video of the cameras whose images were selected to be sent in the e-mail. This feature will only work with the Desktop Surveillance Client. If the email is opened on a mobile device such as Apple or Android, the script file will not work
- **Use this server record:** Fill in the server data where the camera image that will be attached to the email is located. With this option, when running the email script, the Surveillance Client will automatically connect with the pre-configured data for this option. If this option is not checked, after the script is activated, the playback will only be opened after the user connects to the correct server.
- **Use standard SMS message:** If the contact the system is sending the email to is configured as an SMS contact, the system will format the email to be sent with a short description to be sent via SMS via some service of Email-to-SMS. By selecting this option, the SMS message will be a standard system message and will not include the personalized message from the **Message** field.
- **Use Standardized SMS message:** With this option, when sending an SMS, the system will replace the standard short SMS text with the text entered in the **Message** field. Check the maximum message size with your Email-to-SMS service provider.

Alert emails that include camera footage will now include a "DeepLink" in the body of the email, where if the email is being viewed via an Android or iOS mobile device it will allow video playback of the event (When press the link) through the Mobile Client (If installed).



## 7.2.2 Display images from cameras on the operator screen

Displays system objects on the operator's screen in the Surveillance Client in a popup. You can select multiple objects of different types. If more than one object is selected, an automatic view will be created. To learn about views see the Surveillance Client manual.



To select the objects to be displayed on the operator screen, select the desired objects from the list of available objects and drag them to the list of selected objects.

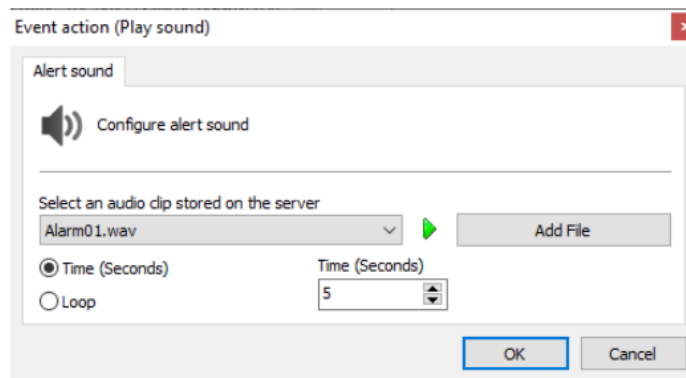
To remove objects to be displayed on the operator screen, select the desired objects from the list of selected objects and drag them to the list of available objects. You can also remove objects from the list of selected objects by double-clicking the desired object.

### 7.2.3 Play an alarm sound in the Surveillance Client

This action will play an alarm sound on the Surveillance Client alerting the operator of the event that has occurred.

The system also allows the use of customized alert sound files to be played on the Surveillance Client.

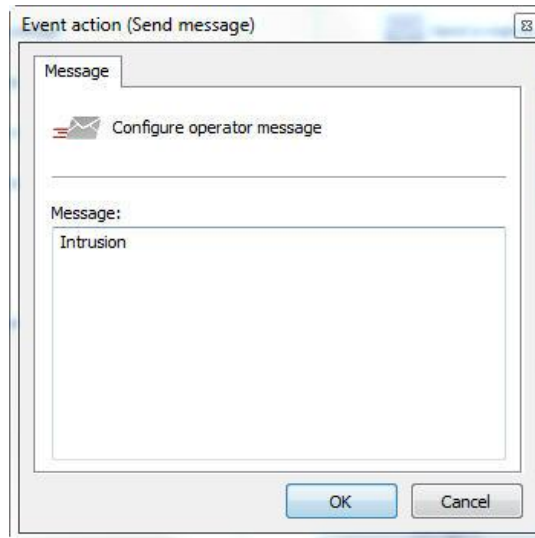
Select the desired alert sound and execution time in the Surveillance Client. To test the selected sound, click the **Play** button. You can select system default alarm sounds, or add your custom alarm sound (.WAV files only)



- **Selected File:** Sound file to be played on the Surveillance Client
- **Play button:** Test alarm sound file locally
- **Add File:** Adds a custom audio file. Only files in .WAV format are supported. The file will be saved on the server and you can reuse this file for other events.
- **Reproduction Type:** Select between Time (Seconds) or Loop. For Time, the audio will play for X seconds specified in the Time field. For Loop, the audio will play for X number of times specified in the Loop field
- **Time or Loop:** Indicates the number of seconds or number of loops to play the audio file in the Surveillance Client

### 7.2.4 Send instant message to operator

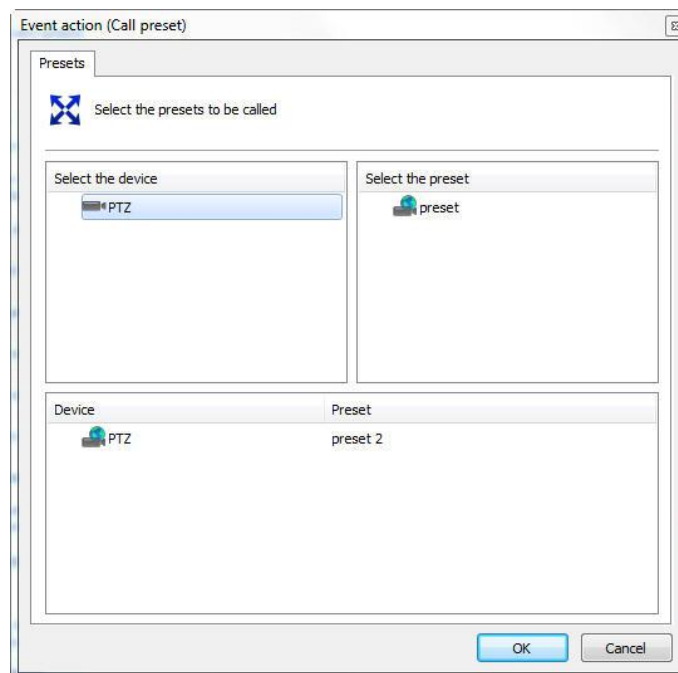
Sends an instant message to the operator with information defined by the administrator. These messages may contain instructions on the procedure to be carried out by the operator to solve the problem, for example.



On this screen, configure the message to be displayed on the Surveillance Client popup to the operator.

### 7.2.5 Call camera presets

This action will call camera presets when the event occurs. To learn what presets are, see [How to set up Control Presets](#).



On this screen, select the desired camera, then select the preset you want to activate and then drag it to the list below, as shown in the figure above.

You can choose presets for several cameras and the system will position all cameras simultaneously, but you must select only 1 preset per camera.

# Chapter



## 8 User Management

A security system only really works if it has functionalities and administration capable of making it reliable to vulnerabilities and technical problems during its operation.

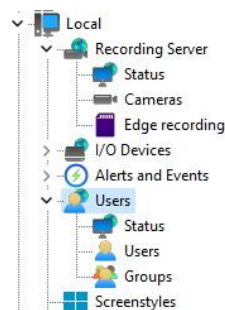
Creating users is very important for good organization and security of the system.

The system administrator must define a set of users who will be responsible for monitoring and correcting events related to the operation of the Digifort System. These users will eventually be activated automatically by the system, being notified about the conditions and anomalies that occur and that were defined by the organization as subject to verification. An abnormal situation would be a camera that stopped working, or a safe room that warned about someone's undue entry, for example.

These users must be extremely trusted by the company, as a security solution only works with reliable equipment and people.

The system user manager is divided into three parts, Status, where user activity on the server can be monitored, Users, where system users can be included, changed and deleted, and Groups, where user groups can be included, modified and deleted. This way, the user will be able to access their profile in any monitoring environment.

To access the user management area, locate the Users item in the Settings Menu of the server to be managed and double-click it. The item will expand showing the Status and Users options, as shown in the figure below:

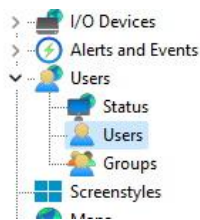


### +Tip

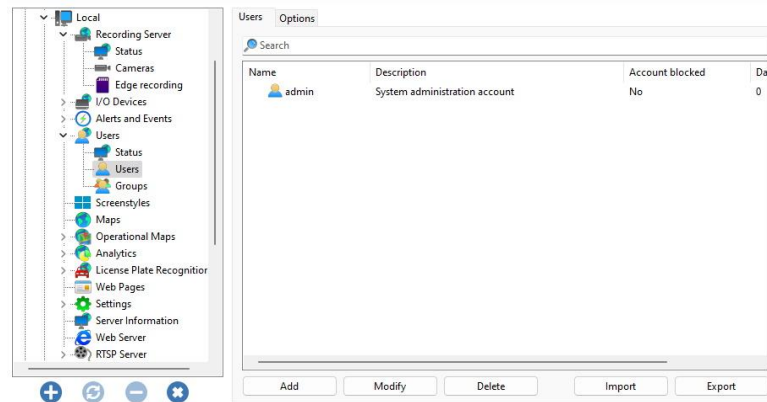
To facilitate management of multiple servers, the Administration Client will reuse login credentials for all servers. If you successfully log in to one server, when connecting to another server, these same credentials will be used automatically, facilitating the administration process as it will not be necessary to enter login credentials for all servers. An exception is if 2-factor authentication is enabled, then you will need to provide the 2-factor key at each login.

### 8.1 Adding, Changing, and Deleting Users

To access user management, locate the Users item within the Users item in the Server Settings Menu, as shown in the figure below:



Once this is done, the user management screen will open on the right side as shown in the figure below:



By clicking on the **Add** button, the user editing screen will be opened. Let's start by entering the user's data, then the rights and finally the client's resources.

To change an already registered user, select it and click on **Modify**, and change the data as explained in the following pages.

To remove a user, select the desired user and click on the **Remove** button.

## 8.1.1 User Account Info

The first step when adding a user is to enter their main data, they are:

- **User:** User name, this must be entered when logging in to any module in the system. Once saved, it cannot be changed.
- **Password:** User password. (Register or modify the user password). When the user is being modified, leave this field blank. If you want to change your password, simply fill in the new password.
- **Confirm:** Re-enter the user password
- **User Description:** A brief description about the user, with the purpose of helping to identify them in the system.
- **Login Times:** Allows you to schedule when the user can access the system. When you click this button, a scheduling screen will be displayed. All scheduling screens in the system have the same scheduling system. To learn how to work with scheduling, check the [How to configure recording schedule](#) topic.
- **Login IPs:** Allows you to restrict user access to certain IPs on the network, providing an extra layer of security against unauthorized access. Check the Login IPs topic for more information.
- **Block user due to invalid login:** If activated, the system will block the account of the user who logs in with the wrong password for more than X configurable attempts.
- **User type:**
  - **Native User:** Native user of the system. Native user password is set in the system
    - **The user cannot change the password:** By checking this option, the user can never change their password, leaving it up to the system administrator to carry out this action.
    - **Force password change on next login:** By checking this option, the user will be required to change their password the next time they access the system via Desktop Client.
  - **Active Directory User:** If your edition supports integration with Active Directory, this user will be linked to the AD login. The username must be the same as that registered in AD.
    - **Domain:** Enter the domain name where this user is registered.
- **User Account Options:**
  - **Blocked account:** By checking this option, the user will not be able to authenticate to the system.



- **Account expiration:** In this parameter, a date can be defined on which the user account will expire. If the user's account expires, he will not be able to authenticate to the system. To reactivate an expired account, select **Never** or change the expiration date to a later date.
  - **Never:** The user account never expires.
  - **Expires in:** The user account expires on the specified date.
- **Authentication:**
  - **Authentication Method:** Select authentication method
    - **Username and password:** User authentication will be done purely by username and password
    - **Biopass:** Authentication will be done using the biometrics reader (This product has been discontinued). Biometrics only works on Desktop clients. To learn about this feature see the BioPass chapter.
    - **Username and password or Biopass:** The user can choose between providing username and password or biometrics (This product has been discontinued). Biometrics only works on Desktop clients.
    - **Username and password and Biopass:** The user must provide username and password and biometrics (This product has been discontinued). Biometrics only works on Desktop clients.
  - **OTP (One-time Password):** Enables the use of 2-factor authentication. For more details, see the [2-factor authentication](#) topic.
    - **Key:** Sets the 2-factor authentication key.

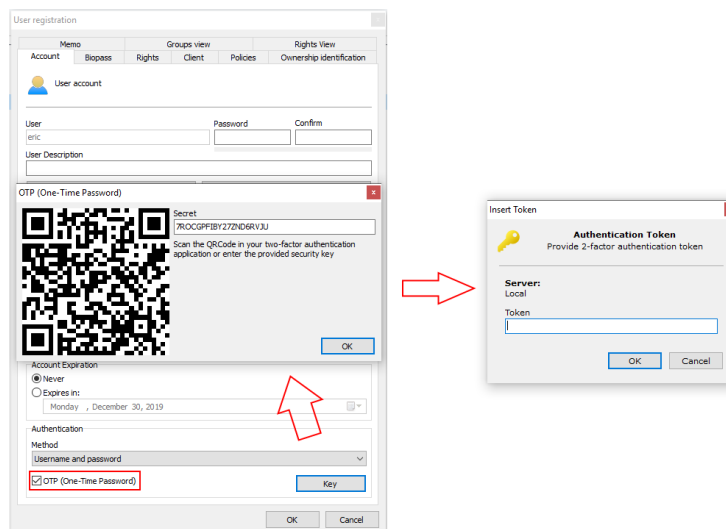
#### +Tip

The password can be registered blank and the user on their first access to the system can register their password using the **Force password change on the next login** option.

### 8.1.1.1 2 Factor Authentication

For greater security, the system allows the use of 2-factor authentication using the **TOTP** algorithm (Time-based One-Time Password algorithm).

The user can use any 2FA application compatible with this algorithm (Ex: Google Authenticator).



To enable 2-factor authentication, check the **OTP (One-time Password)** option and click the **Key** button.

The system will generate a QR Code that must be scanned in your 2-factor authentication app. Consult your authentication app's manual to learn how to register a key. Each user will have a different authentication key.

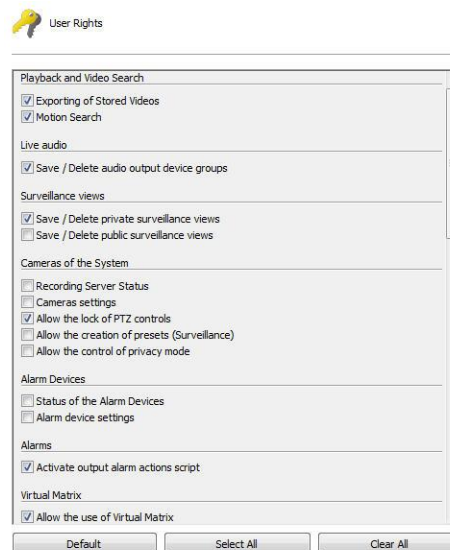
When the user logs into the system through a Desktop Client, an extra authentication window will be displayed, asking the user for the code that is being displayed in the authentication app.

### Note

For greater security, once the authentication key is generated, it can no longer be accessed using the **Key** button. If you click the **Key** button again, a warning window will appear and a new key will be created.

## 8.1.2 User Rights

After filling in the main user data, access rights must be configured. By default, rights are configured for a monitoring user profile, that is, only live monitoring and video playback operations can be carried out on the system.



### 8.1.2.1 Video Playback and Search

- **Export of stored videos:** Allows the user to export previously recorded videos for backup or viewing on another workstation. To learn how to export videos, see the Surveillance Client manual.
- **Motion Search:** Allows the user to perform motion search on stored videos. Motion Search assists in searching for claims in a scene. To learn about the Motion Search, consult the Surveillance Client manual.

### 8.1.2.2 Live Audio

- **Save / Delete audio output device groups:** Allows you to save or delete audio output groups in the Surveillance Client.

### 8.1.2.3 Surveillance Views

- **Save/Delete private views:** Allows the user to save or delete views that will only be available for their account.

- **Save/Delete public views:** Allows the user to save or delete public views, which will be available to all users of the system.

#### 8.1.2.4 System Cameras

- **Recording Server Status:** Allows the user to check the general status of the system and the individual status of each camera, obtaining information such as disk space used, frames per second received, up time, etc. See more at [Recording Server](#).
- **Camera Settings:** Allows the user to configure the cameras to be managed by the system.
- **Allow Blocking PTZ Controls:** Allows the user to block camera movement by priority.
- **Allow the Creation of Presets:** Allows the user to save presets via the Surveillance Client.
- **Allow the Control of Privacy Mode:** If your edition supports Privacy Mode, allows the user to activate the privacy mode of a camera, if configured.

#### 8.1.2.5 Alarms

- **Activate alarm output scripts:** Allows the operator to trigger alarm output scripts directly through the Synoptic Map.

#### 8.1.2.6 System Users

- **User activity on the server:** Allows the user to monitor user activity on the server. To learn how to use this feature see [Monitoring user activities](#)
- **User registration:** Allows the user to access the user registration.

#### 8.1.2.7 Alerts and Events

- **Alert Contact Register:** Allows the user to access the alert contact register. Contacts must be registered to receive notifications about anomalies in the system or the occurrence of claims. See more at [Alerts and Events](#).
- **Allow Activation of Manual Events:** Allows the user to activate manual events registered in the camera object.
- **Viewing Event Logs:** Allows the user to view event logs.

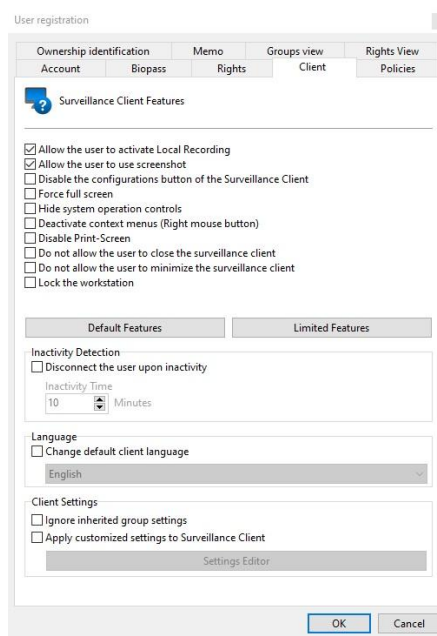
#### 8.1.2.8 Server

- **Server Settings:** Allows the user to change global system settings, such as server connection limits, disk recording limits, etc. See more at [Server Configurations](#).
- **Server Monitoring:** Allows the user to monitor the displayed information about the server. See more at [Server Information](#).
- **Visualization of Server Logs:** Allows the user to access server log settings. See more at [System Logs](#).

### 8.1.3 Surveillance Client Features

Configuring the Surveillance Client features is very important for the security of a site. This feature provides tools that affect the person monitoring the cameras, causing other factors to interfere with the operator's attention.

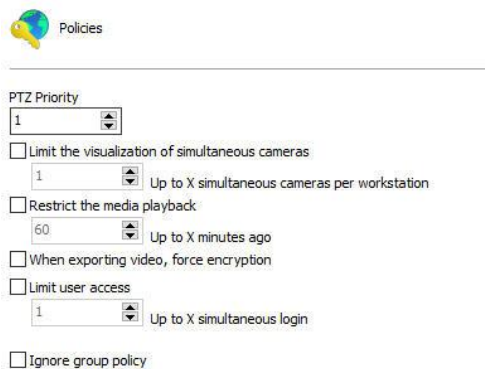
To access these tools, click the Client Resources tab.



- **Allow user to activate Local Recording:** Allows the user to activate local emergency recording on the Surveillance Client. To learn about local recording see the Surveillance client manual.
- **Allow the user to use the screenshot:** Permission for the user to use the system's screenshot feature.
- **Disable Surveillance Client Settings Button:** Prevents the user from accessing the Surveillance Client settings. To learn about the Surveillance Client settings, consult it's manual.
- **Force full screen:** Force the user to use the Surveillance Client in full screen.
- **Hide system operation controls:** This option will make the Surveillance Client operate in "full screen" mode, that is, the camera visualization matrix will be expanded and the user will not have access to any operation controls, being restricted to the camera view screen only.
- **Disable context menus:** This option will disable the use of menus accessible via the right mouse button, further blocking operator access to the system.
- **Disable Print-Screen:** Disables the print-screen key.
- **Do not allow the user to close the Surveillance Client:** Prevents the user from closing the Surveillance Client.
- **Do not allow the user to minimize the Surveillance Client:** Prevents the user from minimizing the Surveillance Client, keeping it tied to the system.
- **Lock workstation:** Locks the user's workstation, disallowing the use of shortcuts such as CTRL + ALT + DEL, ALT + TAB, and any other command that may terminate the Surveillance Client.
- **Inactivity Detection:**
  - **Disconnect User Due to Inactivity:** This function, when activated, will disconnect a user from the Surveillance Client if they are inactive for longer than the configured limit.
  - **Inactivity Time:** Configure the inactivity time (in minutes) for disconnection.
- **Language:**
  - **Change client language automatically per user:** The client language (Administration, Monitoring and Web) can be dynamically changed for each user logged into the system, overwriting the computer's language option. Click on the option Change the default system language and then choose the desired language for the user in the box.
- **Client Settings:**
  - **Ignore Inherited Group Settings:** In the centralized Surveillance Client configuration function, this option will ignore custom settings inherited by user groups.

- **Apply Customized Settings to Surveillance Client:** Defines settings for the Surveillance Client when this user logs in.

### 8.1.4 Policies



Policies

PTZ Priority  
1

☐ Limit the visualization of simultaneous cameras  
1 Up to X simultaneous cameras per workstation

☐ Restrict the media playback  
60 Up to X minutes ago

☐ When exporting video, force encryption

☐ Limit user access  
1 Up to X simultaneous login

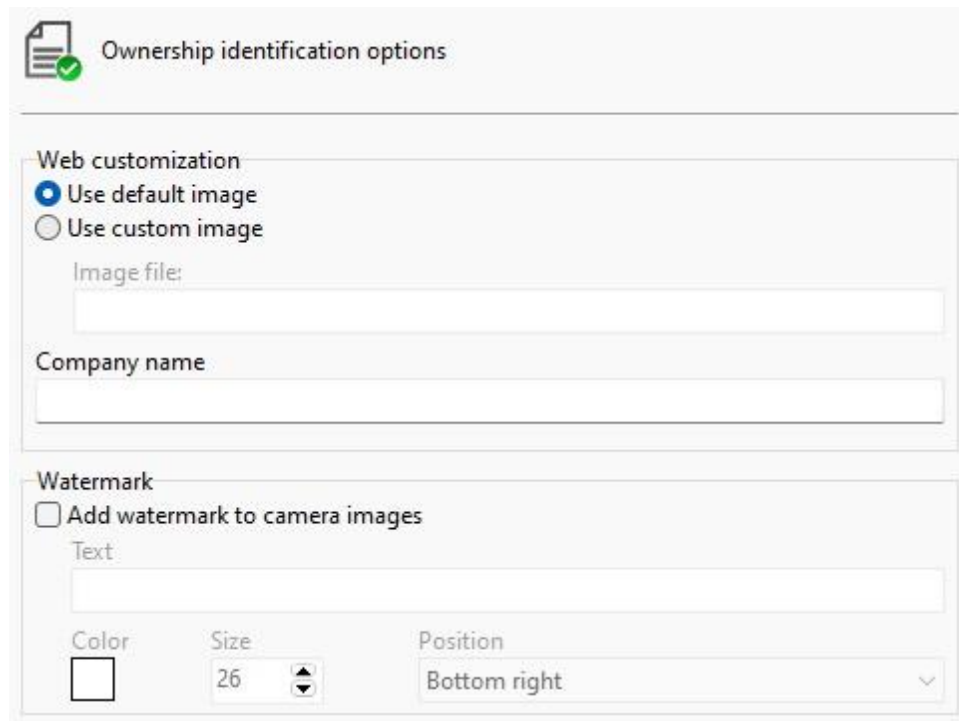
☐ Ignore group policy

This screen allows the following settings:

- **PTZ Priority:** This option aims to prioritize a user in locking camera PTZ controls for exclusive use. The priority with value 1 is the highest of all, therefore, no user with equal or lower priority will be able to unlock the PTZ while that user is using it. Now let's imagine a user with priority 3, this user will lose control of the PTZ to the one who has a higher priority, in this case 1 or 2, but no user at the same or lower level (3,4,5,6...) will be able to take PTZ control while using it. To learn more, see the PTZ Lock topic.
- **Limit the visualization of simultaneous cameras:** Restricts the number of cameras that the user can visualize simultaneously in the Surveillance Client.
- **Restrict the media playback:** Limits the user to only playback X configurable seconds of video prior to the current server date.
- **Force export with encryption:** Allows you to force encryption on all video exports. This option can be configured per user or user group. For more information about export with encryption, see the Surveillance Client manual. When this option is active, only the native export format will be available to the operator.
- **Limit user access:** Limits the number of simultaneous logins for this user through Desktop clients.
- **Ignore group policies:** The user with this option checked will not have a user group policy overridden by that of his user.

### 8.1.5 Ownership Identification

These settings allow customizing the user interaction page when the system is accessed through an internet browser and the image that is seen or reproduced by users in the Surveillance Client.



The image shows a dialog box titled "Ownership identification options" with a document icon and a green checkmark. It contains two main sections: "Web customization" and "Watermark".

**Web customization**

- ☒ Use default image
- ☐ Use custom image
- Image file:
- Company name:

**Watermark**

- ☐ Add watermark to camera images
- Text:
- Color:
- Size:  (with up/down arrows)
- Position:  (with a dropdown arrow)

#### 8.1.5.1 Web Customization

This feature can be used to customize the user interaction page showing the company logo, for example.

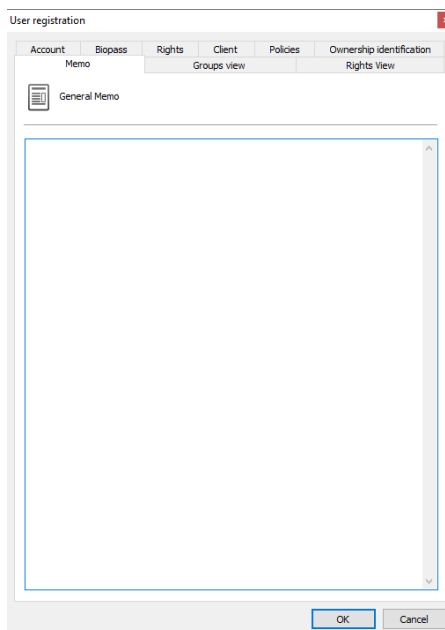
A different web personalization can be created for each user, just specify these parameters properly in the registration of each user.

- **Use default image:** Displays the system logo on the user interaction page.
- **Use custom image:** Enables the path to the image field, allowing you to locate an image on your computer that will be used on the user interaction page, replacing the standard system logo.
- **Company Name:** Enter the company name to display on the user interaction page.

#### 8.1.6 General User Remarks

This field is free text and can be used to store any information pertinent to the user.

The field can also be displayed in the user list via extended columns and exported along with the user list export.



### 8.1.7 Groups View

Allows viewing in which groups this user is registered.



### 8.1.8 Rights View

This screen allows viewing the rights granted to the user, such as the right to view and reproduce cameras and maps.



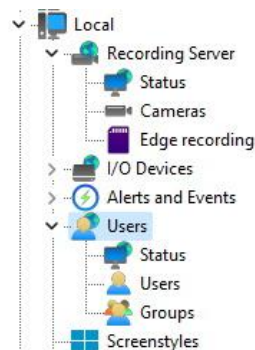
This screen offers the following features:

- **Right Type:** Lists the types of rights granted to the user.
- **Objects:** Lists the objects related to the granted right.

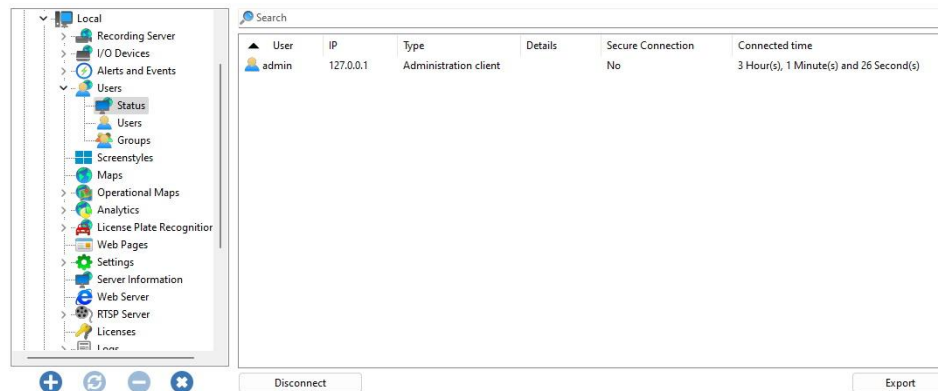
## 8.2 Monitoring User Activities

This feature is very important for server security, as the activities of users logged into the system can be monitored here. If the user is taking any inappropriate action, he may be disconnected or blocked.

To access this feature, locate the **Status** item within the **Users** item in the Server Settings Menu, as shown in the figure below:



Once this is done, the user activity monitoring screen on the system will open on the right side, as illustrated in the figure below:

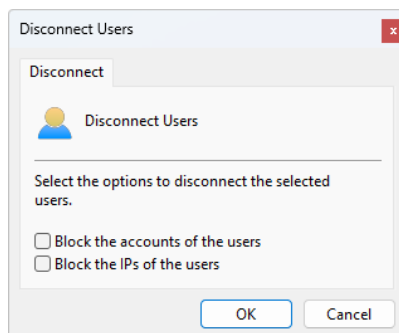


This list displays all users currently logged in, displaying information such as user name, IP address, type of access to the server and connection time.

- **User:** Logged in user name
- **IP:** User station IP
- **Type:** User connection type
- **Details:** Extra connection details. In case of a live video or video playback connection, the name of the camera being viewed will be displayed
- **Secure Connection:** Indicates whether the user connection is secure (via SSL/TLS)
- **Connection Time:** Total connection time for this user



To disconnect a user, select the selected user and click the **Disconnect** button and the following screen will be displayed:



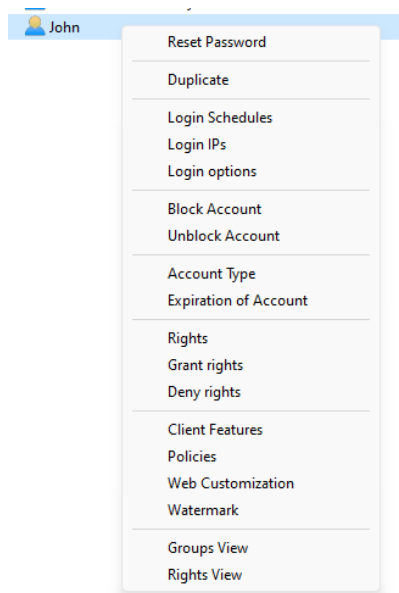
- **Block Users Account:** With this option checked, all disconnected users will also have their account blocked.
- **Block Users IP:** With this option checked, all disconnected users will also have their connection IP blocked using the IP Filter feature.

#### Note

Every camera being viewed by the user will generate a new connection, therefore an operator's monitoring station can have multiple connections, depending on the number of cameras being viewed or reproduced.

## 8.3 How To Change Parameters For Multiple Users Simultaneously

The system's User Manager provides quick access to the most common user settings that can be changed for multiple users simultaneously. In the user registration, select the desired users and right-click. A menu will open as shown in the figure below:



Most of the options you can change are self-explanatory and you can consult the [User Registration](#) topic to learn more about each option.

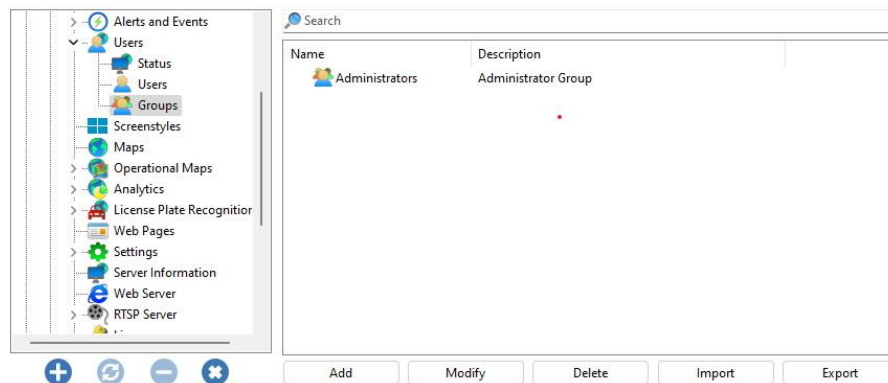
## 8.4 Adding, Changing, and Deleting Groups

To access group management, locate the **Groups** item within the **Users** item in the Server Settings Menu, as illustrated in the figure below:



The groups option was created to facilitate the management of users in the system.

Once this is done, the **Group management** screen will open on the right side as shown in the figure below:



By clicking on the **Add** button, the group editing screen will be opened. Let's start by inserting a group, then the rights and finally the resources .

To change an already registered group, select it and click on **Change**, and change the data as explained in the following pages.

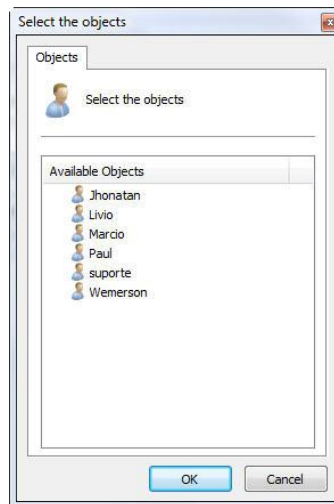
To remove a group, select the desired group and click on the **Remove** button.

The screenshot shows a 'Add group' dialog box with the following fields and controls:

- Group:** A text field containing 'Administrators'.
- Group Description:** A text field containing 'Administrator Group'.
- Login times:** A button.
- Login IPs:** A button.
- Group Users:** A list box containing one user, 'John'.
- Buttons:** 'Add', 'Delete', 'OK', and 'Cancel' at the bottom.

The first step when adding a group is to enter its main data, they are:

- **Group:** User group name. Once saved, it cannot be changed.
- **Group Description:** A brief description of the group, with the purpose of helping to identify it in the system.
- **Login Times:** Allows you to schedule when a user in the group can access the system. When you click this button, a scheduling screen will be displayed. All scheduling screens in the system have the same scheduling system. To learn how to work with scheduling, check the [How to configure recording schedule](#) topic. If a user is in multiple groups, he will have access to the system if any group provides login permission, that is, the schedule of all groups (as well as the user's individual schedule) will be added together.
- **Login IPs:** To learn about this feature see Login IPs. If a user is in multiple groups, he will have access to the system if any group provides login permission by IP, that is, the IP restriction of all groups (as well as the individual user restriction) will be added together.
- **Group Users:** List of users belonging to this group. To add a user to the group, simply click on the **Add** button and a window will open to choose the user as shown in the figure. To delete a user from the group, simply select it from the list and click the **Delete** button.



### 8.4.1 Group Rights

After filling in the main user data, access rights must be configured. By default, rights are configured for a monitoring user profile, that is, only live monitoring and video playback operations can be carried out on the system.

The rights settings for the group are the same as the user rights settings. To learn how to configure group rights see [User Rights](#)

#### +Note

The effective rights of users will be the user's individual rights plus all group rights to which the user belongs to

### 8.4.2 Surveillance Client Features

Configuring the Surveillance Client features is very important for the security of a site. This feature provides tools that affect the person monitoring the cameras, causing other factors to interfere with the operator's attention.

The Surveillance Client Features setting for the group is the same as the Surveillance Client Features setting for the user. To learn how to configure Group Surveillance Client Features see [Surveillance Client Features](#).

#### +Note

The effective features of users will be the user's individual features added to the resources of the groups to which the user belongs.

- The effective **Inactivity Time** value will be the lesser of all groups or the individual user value.

### 8.4.3 Policies

The Policies setting for the group is the same as the User Policies setting. To learn how to configure group Policies, see the [User Policies](#) topic.

#### +Note

The effective user policies will be the combination of the individual user policies and the group policies. The result of the combination will always be the most restrictive, that is, if a group introduces a greater

### +Note

restriction, this greater restriction will take precedence.

## 8.4.4 Rights View

This screen allows you to view the group's effective rights over objects, such as the right to view and reproduce cameras and maps.

The Rights View screen for the group is the same as the User Rights View screen. To learn about group Rights Inquiry see [User Rights View](#).

## 8.5 Options

To access user options, click on the **Options** tab on the **User Registration** screen:

The screenshot shows the 'Options' tab of the 'User Registration' screen. It is divided into two main sections: 'Security' and 'Active Directory'.  
Under 'Security':  
- There is a checkbox 'Force the use of strong passwords for users' which is unchecked.  
- There is a checked checkbox 'Force user to change weak password at next login'.  
- There is an unchecked checkbox 'Do not request an OTP (One-Time Password) again for same user / station for X hours'. Below this checkbox is a spinner box showing '24' and the text 'Hours'.  
Under 'Active Directory':  
- There is an unchecked checkbox 'Keep imported Active Directory users synchronized'.  
- Below this are three text input fields: 'User for domain authentication', 'Password for domain authentication', and 'Synchronization Interval'.  
- The 'Synchronization Interval' field has a spinner box showing '3' and the text 'Hours'.  
At the bottom of the form is a 'Save settings' button.

### 8.5.1 Security

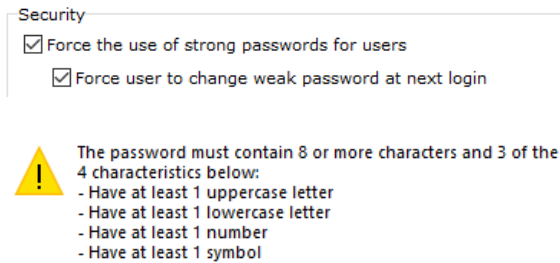
#### 8.5.1.1 Force use of strong password

The system allows users to use a strong password. A strong password must contain at least 8 characters and 3 of the 4 characteristics below:

- Contain at least 1 lowercase character
- Contain at least 1 uppercase character
- Contain at least 1 number
- Contain at least 1 symbol

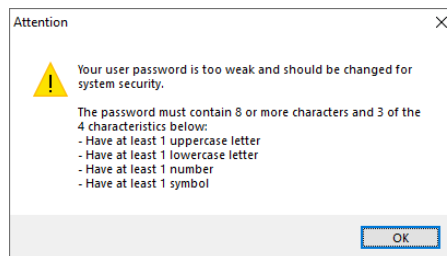
When activating the option to force the use of a strong password, new users can only be registered with a strong password. The system also allows you to force the change of a weak password (If the user is currently using a weak password) on the user's next login through the Surveillance Client or Administration Client.

The use of a strong password only applies to native system users and not to LDAP/Active Directory users, where the strong password requirement must be applied directly on the domain controller.



- **Force user to change weak password on next login:** If you already have users registered before activating the option to use a strong password, you can activate this option to force users with a weak password to change their password the next time they log in through a Desktop client (Surveillance or Administration).

The system will issue a weak password alert when the user accesses the server through the Administration Client with a password that does not meet the minimum security levels.



#### 8.5.1.2 OTP

- **Do not request OTP again for the same user/station for X hours:** With this option active, the system will not ask for a new OTP (For 2-factor authentication) if the user is logging in from the same station.
  - **Hours:** Number of hours to request OTP again

# Chapter



IX

## 9 Layouts Management

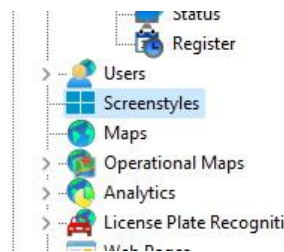
Layouts are groupings of cameras in a certain format and order that are used by the Surveillance Client to display the cameras on the screen.

In addition to pre-defined layouts, the system allows the creation of new types of layout, aiming to personalize the system according to the user's taste.

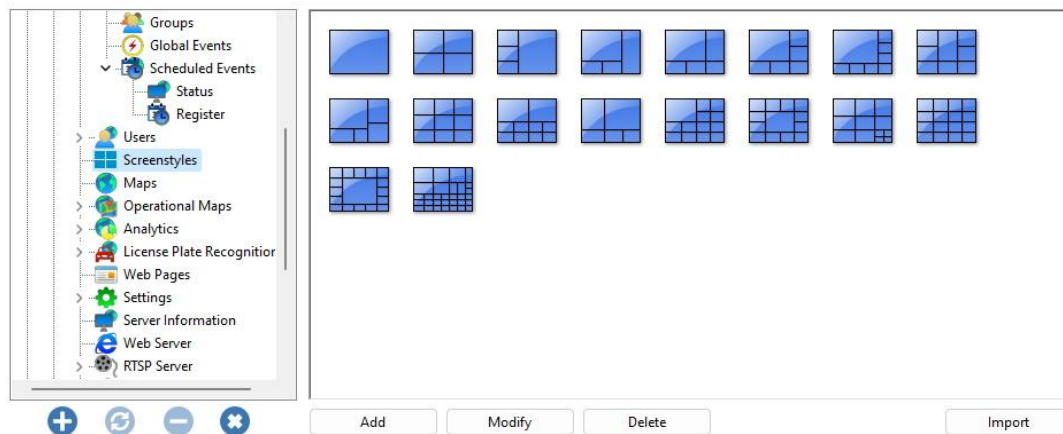
In the Administration Client, it is only possible to manage layouts, that is, create, modify or delete them. To learn how to add cameras to tiles, see the Surveillance Client manual.

### 9.1 How To Access Layouts Management

To access layout management, locate the Layouts item in the Settings Menu, as shown in the figure below:



Once this is done, the layout registration will be displayed on the right, as shown in the figure below:



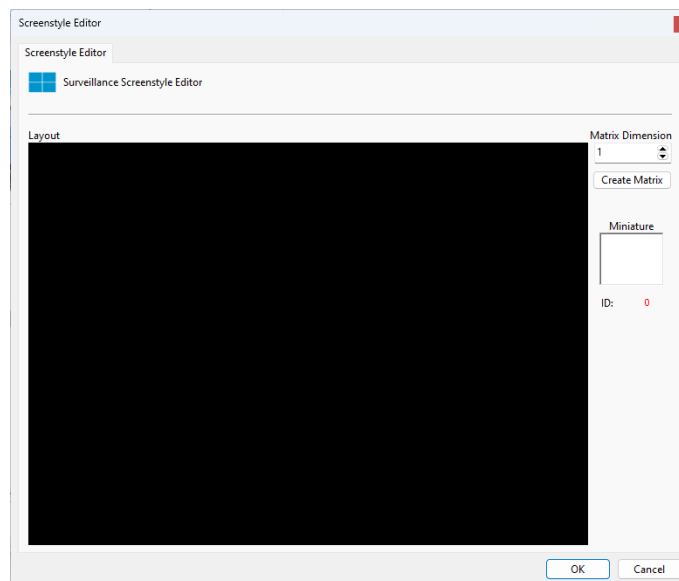
The system provides some pre-defined layouts that cannot be changed or deleted.

To add a new layout, click **Add**. To change or delete a layout, select it and click on the corresponding button.

#### 9.1.1 How To Add A Layout

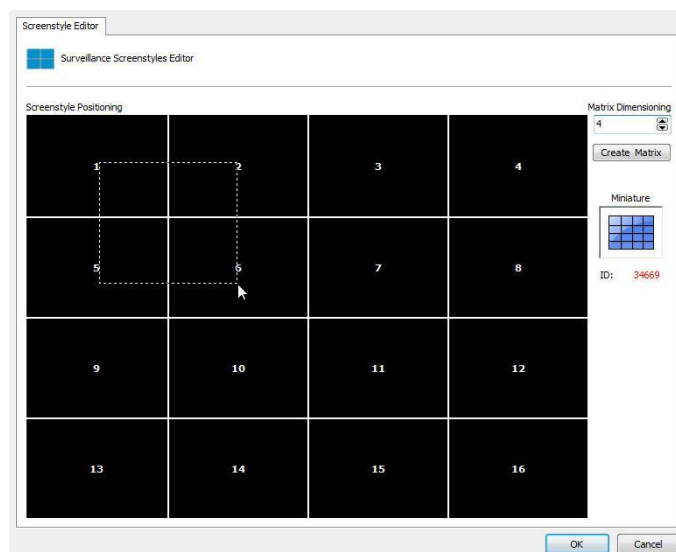
After clicking **Add**, as explained in the previous topic, the following screen will be displayed:





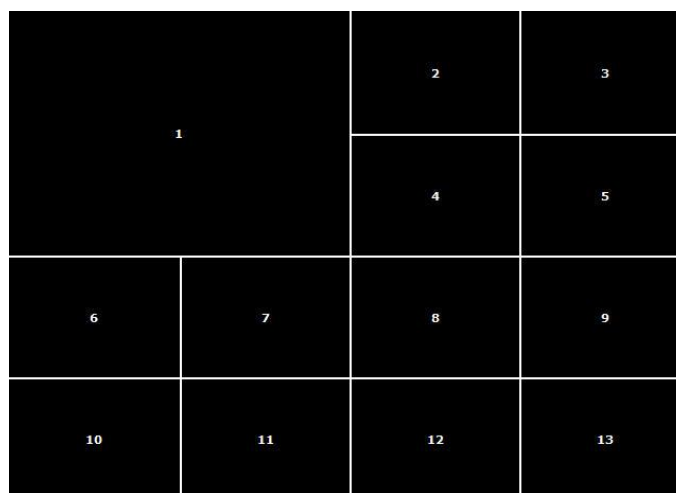
- **Matrix Dimension:** Choose the dimension of the matrix to be created. The value is NxN.

Select the matrix dimension and click the **Create Matrix** button



In the image above we created a 4x4 matrix, making it possible to add 16 cameras to the screen.

After creating the matrix, it is possible to join tiles by clicking with the left mouse button and dragging it, aiming to obtain a larger viewing area, in the example above we are joining tiles 1, 2, 5 and 6, forming the layout shown in the image below:



With the union of these four tiles we obtain space for the allocation of 13 cameras, one of which will be four times larger.

It is possible to join as many tiles as necessary as long as the final area is a rectangle.  
To undo a join, repeat the same process with the right mouse button.

After creating the layout, it will be available in the Surveillance Client. To learn how to use it, consult the Surveillance Client manual.

# Chapter



## 10 Settings

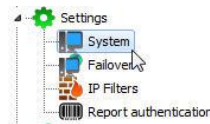
### 10.1 System

This area of the system is reserved for adjusting global server settings.

Global settings are parameters that, once configured, will affect the entire operation of the system.

#### 10.1.1 General

To access this area, click on the Settings item in the Settings Menu, as shown in the figure below:



Once this is done, the general system settings screen will open on the right side, as shown in the figure below:

 A screenshot of the 'General' system settings screen. The screen has a tabbed interface with tabs for 'General', 'Recordings', 'Master / Slave', 'Multicast', 'Backup', 'Database', 'SMTP settings', 'Disk Limits', 'Network Units', 'SNMP', and 'Google Maps'. The 'General' tab is active. It contains several input fields and checkboxes:
 

- 'Company name' with an empty text box.
- A checkbox labeled 'Send periodic e-mail with server report' which is currently unchecked.
- 'E-mail sending interval (In minutes):' with a text box containing '120'.
- 'E-mail group:' with a greyed-out text box.
- 'TCP port for server communication:' with a text box containing '8600'.
- A checkbox labeled 'Secure communication via SSL' which is currently unchecked.
- '8400' is shown below the SSL checkbox.
- A 'Save settings' button at the bottom.

- **Company name:** Company name will be used in video exports to facilitate operation in the monitoring client.
- **Send periodic email with server report:** Sends a periodic email to the specified alert group a server report at a specified time interval. This report contains information such as user access to the system and recording status.
  - **Interval:** Specify the email sending interval.
  - **Email Group:** Specify the contact group to send the reports.
- **Server communication TCP port:** Communication port on which the Surveillance Client and the Administration Client will communicate with the server. When changing this configuration, the communication port of the Administration Client and Surveillance Client server registration must be changed. To learn how to perform this configuration in the Administration Client, see [How to configure the servers to be managed](#). To learn how to change the port on the Surveillance Client, consult its manual.
- **Secure communication via SSL:** Communication port where the Surveillance Client and Administration Client will communicate with the server via SSL. To use SSL you must provide SSL certificates. See the [SSL Certificates](#) topic for more information.

After adjusting the settings, click on the **Save Settings** button so that no changes are lost.

## 10.1.2 Recordings

In this tab it is possible to configure some advanced options related to recording images.

Percentage of free space that the system must maintain when performing the recordings

2%

☐ Manage used disk space by deactivated cameras

☐ Use files cache for quick server startup

Recording Encryption

☐ Activate Recording Encryption

Method

AES 128 bit

Key

Advanced

☐ Record the pre-alarm buffer in full when an event occurs

Recording Protection

Storage Directory of Protected Recordings

Save Settings

- **Percentage of free space that the system must maintain when recording:** Enter the percentage of disk space you want to keep free here. For example, if a 1TB hard drive is used, with a free space percentage of 2%, 20GB would not be used by the system for recordings, remaining free for use, however if these 20GB are used for other purposes, then the system will free up plus 20GB, that is, you will always keep 2% of the disk free. This limit is also applied in "Disk Limits". To learn how to create a disk limit, see [Disk Limits](#)
- **Manage Disk Usage of Disabled Cameras:** The recording system has the option to manage disk space used by deactivated cameras. If this option is not checked and the camera is disabled, its recordings would not be deleted during recording recycling. With this option activated, all deactivated cameras will also enter the recording recycling process and their recordings will be deleted according to the configured time. This option is important for Failover servers (where cameras are generally always disabled) and compliance with GDPR data protection laws that define the maximum retention period for images.
- **Use file caching for fast server startup:** In systems where the number of recording days is very high, restarting the server service can take a long time. This option allows the server to start up much faster by maintaining a map of recordings previously used before the system stopped. It is not recommended to use this option if you have problems with power outages on your server or storage, as the file cache may become out of date and cause recording problems.

After adjusting the settings, click on the **Save Settings** button so that no changes are lost.

### 10.1.2.1 Recording Encryption

This option will encrypt the recording data stored on the server itself, which can be AES 128 bits or 256 bits.

- **Activate Recording Encryption:** Enables recording with encryption (This option will increase server CPU usage).
  - **Method:** Select encryption method: AES 128bit or AES 256bit
  - **Key:** Provide the encryption key. Once the key is configured, **it cannot be changed**. This happens because if the key is changed, old recordings become impossible to read.

### 10.1.2.2 Advanced

- **Record the full pre-alarm buffer in full when an event occurs:** The option to write the pre-alarm buffer will cause the system to immediately write the pre-alarm buffer (instead of waiting for the queue), making it possible to send Playback Loop Event Actions at the time of occurrence of the alarm. If this option is disabled (Default), the system will write the pre-alarm buffer as new frames are received, not

generating a spike in disk write data, but some features such as the Playback Loop Event Action can be compromised as the images may not have yet been written to the disk. With the option enabled, the system will write the entire buffer to the disk as soon as the event or movement occurs, which will generate a spike in data recording that can cause performance problems with the storage.

### 10.1.3 Multicast

This option allows the server to send videos to Surveillance Clients via Multicast communication.

Multicast is the delivery of information to multiple recipients simultaneously using the most efficient strategy where messages only pass through a link once and are only duplicated when the link to the recipients splits in two directions.

In the case of VMS, the use of Multicast is only recommended when several Surveillance Clients monitor the same cameras at the same time in the same local network. Otherwise there may be a high rate of information traffic causing problems on the network.

Below is the multicast options configuration screen:

- **Activate media distribution by Multicast:** Enables video streaming to be sent via multicast.
- **Multicast Address:** Considering the IPv4 IP naming architecture and best practices, it is known that the IP range reserved for multicasting is: 224.0.0.0 to 239.255.255.255. For this reason, as standard, we adopted the IP 255.5.10.1 which can be modified at any time.
- **Multicast TTL:** Allows you to change the TTL of the multicast packet. Configuration required for some brands of switches.
- **Source Network:** Select the source network for multicast transmission.
- **Use SRTP Encryption:** When the Surveillance Client connects to the server using SSL/TLS, the multicast media transmission to the client (if configured for multicast video transmission) will also be encrypted using the SRTP protocol.
- **Forcing the use of Multicast:** When the Multicast option is enabled, the Surveillance Client will not necessarily use it, as there is an option on the Surveillance Client that allows the choice of Multicast or Unicast (See the Surveillance Client manual). When the **Force the use of Multicast** option is activated, the server ignores the Surveillance Client settings and thus they will use sending images via Multicast.
- **Save Settings:** Saves the current settings

### 10.1.4 Backup

The system allows the backup if its settings and database.

- **Activate The Backup Of System Configurations:** Select to enable automatic backup of system registration files, folders, and settings.
- **Activate The Backup of Database:** Click to activate automatic backup of the system database that contains analytics records, LPR, general events, logs, audit, etc.
  - **Backup Directory:** Choose the directory where the backup files will be stored. If a directory is not specified, the system will perform the backup in a subfolder named **Backup** within the server installation folder.
  - **Delete backup files older than X days:** Configure the number of days that backup files will be kept in the backup directory.
- **Save Settings:** Saves the chosen settings.
- **Manual Backup**
  - **Backup Of System Settings:** When you click on this option, the system will back up the registration files and folders to the selected backup directory.
  - **Start Database Backup:** When you click this option, the system will back up the database files to the backup directory.

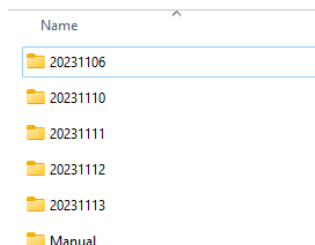
#### +Note

The system does not perform backups of recorded videos. Use the Archiving function for long-term image storage.

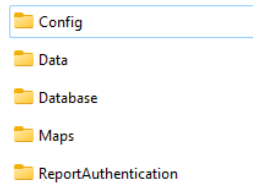
#### 10.1.4.1 Backup Structure

The system will perform a security backup of settings, folders and database using the following structure:

- A **Server** subfolder will be created within the backup folder.
- In the **Server** subfolder, a folder for each day will be created, as well as a **Manual** subfolder that will contain manual backups:



- Within each day's folder, a subfolder will be saved for each system component:




- **Config:** Contains system configuration files.
  - **Data:** Contains the **Data** subfolder that is found in the server installation folder and contains data that is too large to be written to the OS registry.
  - **Database:** Contains the backup of the database files.
  - **Maps:** Contains the binary files with images stored for the **Synoptic Maps**.
  - **ReportAuthentication:** Contains the authentication files for **Authenticated Reports**.
- The **Manual** subfolder will contain a subfolder with date and time for each manual backup performed where the folder structure listed above will be found, with the backups performed.

### 10.1.4.2 Restoring Backups

#### 10.1.4.2.1 Settings

To restore a system settings backup, follow these steps:

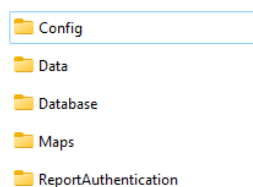
1. With the server service stopped, open the registry editor (regedit.exe) and delete the main folder with all system settings: HKEY\_LOCAL\_MACHINE\SOFTWARE\Digifort.
2. In the file explorer, locate the folder with the desired backup and double-click on the registry file to import the settings:

Name	Date modified	Type	Size
 Backup_Config_20231106	11/6/2023 11:25 AM	Registration Entries	4,229 KB

3. A registry editor confirmation message will be displayed asking if you want to continue with the operation, click **Yes** and wait until the confirmation message is displayed.
4. Restart the server service and the settings are now restored.

#### 10.1.4.2.2 Folders

The system backs up some settings folders that must be restored:



- **Data:** To restore the **Data** folder, copy and replace the corresponding folder in the server installation folder.
- **Maps:** To restore the **Maps** folder, copy and replace the corresponding folder in the server installation folder.
- **ReportAuthentication:** To restore the Authenticated Reports files, copy the contents of this folder to the **ReportAuthentication** folder in the server root or to the folder configured to store authenticated



reports. To learn more about the storage folder for authenticated reports, see the Report Authentication topic.

#### 10.1.4.2.3 Database

To restore the database, you will need to use the database maintenance tool (DatabaseMaintenance.exe) found in the server installation folder:



In this tool, click on **Restore** and follow the steps:

1. Select the desired backup file (\*.ddb) by clicking the button with 3 dots (...).
2. Select a temporary file, where the database will be rewritten. Name the file DIGIFORTDB.FDB
3. Click **Start Restore**.
4. Wait for the backup restore process. This process may take anywhere from a few minutes to a few hours, depending on the size of the database file.
5. Stop the system server service (If it is not already stopped) with the Service Manager.
6. Replace the DIGIFORTDB.FDB file in the server installation folder with the newly restored file.
7. Start the system server process again.

### 10.1.5 Database

The system has a database to store different types of records such as: analytical event records, LPR event records, events, audit, logs, among others.

The database settings screen configures maintenance options, as well as performs database maintenance tasks:

- **Recompute Indexes:** This option will start the re-computation of the database indexes, in order to increase performance during record queries. This task must be performed periodically.
- **Purge Old Search Filters:** This option will cause old search indexes (which are no longer referenced in the database) to be effectively deleted. This task must be performed periodically.
- **Automatic Maintenance Scheduling:**
  - **Recompute Indexes:** Check this option for the system to perform the index recomputation task during scheduled maintenance.
  - **Purge Old Search Filters:** Check this option for the system to perform the task of purging old search filters during scheduled maintenance.
  - **Scheduling:** Select the maintenance task frequency.
    - **Weekly:** When selecting the **Weekly** option, the days of the week will be displayed. Select the days of the week to perform scheduled database maintenance.
    - **Monthly:** When selecting the **Monthly** option, the days of the month will be displayed. Select the days of the month to perform scheduled database maintenance.
- **Save Settings:** Stores the chosen settings.

### 10.1.6 SMTP

SMTP settings are used by the system to send notification emails to users. The actions for sending e-mails can be due to communication failures with the cameras, for example, and must be previously configured by the administrator.

To access this feature, click on the SMTP Settings tab, as shown in the figure below:

Servidor SMTP:  25

Nome para HELO:

☐ Meu servidor requer autenticação por usuário e senha

Usuário:

Senha:

☐ Utilizar autenticação segura por SSL

De (Nome):

De (E-Mail):

Personalização do e-mail

Logo (55x55)  Titulo

☐ Remover imagem de logo do e-mail

Grupo para E-Mail de Teste:

Enviar e-mail de Teste

Salvar Configurações

- **SMTP Server:** SMTP server address to be used for sending e-mails. This parameter can be an IP, if your company has its own SMTP server, for example, or a DNS if you use third-party SMTP servers.
- **My server requires username and password authentication:** If your SMTP server requires a username and password for authentication when sending e-mails, check this option. By checking this option, the User and Password fields will be enabled and must be filled in.
  - **User:** User for authentication when sending e-mails.
  - **Password:** Password for authentication when sending e-mails.
  - **Use SSL authentication:** Select this option to securely connect to the SMTP server.
- **From:** Sender's email address. Inform in this field the e-mail of the system administrator, for example.
- **Email Customization:** Allows customization of the company's logo and name when sending event emails. Just choose the desired logo image and change the title on the side.
- **Remove logo image from e-mail:** Allows sending e-mails without the logo.
- **Group for test email:** Select an alert group to send a test email for the specified settings. This alert group must be previously configured. To learn how to configure groups of alerts see [How to set up contact groups](#).
- **Send Test Email:** Sends a test email to the selected group. You need to save the settings before sending the test email.
- **Save Settings:** Saves the settings. If not pressed all settings will not be saved after exiting this screen.

### 10.1.7 Disk Limits

In this area of the system you can set disk limits on all your recording drives. The system will divide the specified limit between the cameras configured to record on these units.

To access this feature, click on the Disk Limits tab within the Settings item in the Settings Menu, as shown in the figure below:

Disk Unit	Recording Limit
D: [DATA]\	200,000 MB

Add Modify Delete Export

To add a disk limit, click on the **Add** button.



Select the desired disk drive and provide the number of megabytes of the limit you want to enforce. At the end of the configuration, click on the **OK** button.

To change a limit, select it and click the **Modify** button.

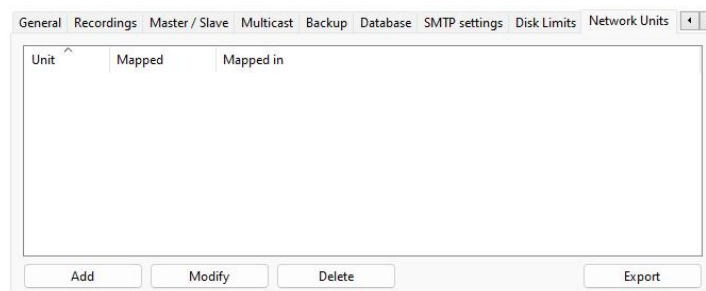
To remove a disk limit, select it and click on the **Delete** button.

### 10.1.8 Network Units

The system makes it possible to perform camera recordings not only on local disks. It is also possible to define network units in which the server can record the images from the cameras.

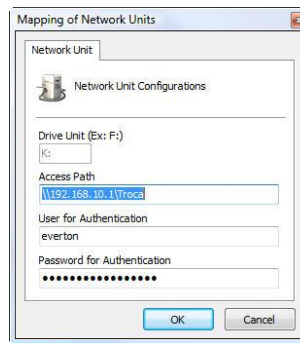
Mapping network drives may be necessary because the user account that runs the system server (Local System Account) is not a regular user account, and does not have network drives mapped by default.

To access this feature, click on the **Network Units** tab, as shown in the figure below:



To add a new network drive, click **Add**. To change or delete a network drive, select it and click on the corresponding button.

After clicking **Add**, as explained in the previous topic, the following screen will be displayed:

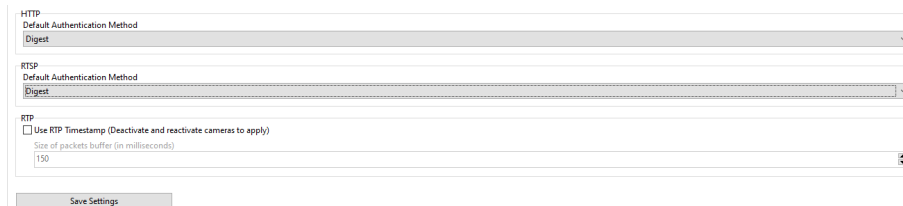


- **Drive Letter:** Specify a letter identifying the drive to be mapped.
- **Access path:** Specify the full path of the remote computer folder you want to map.
- **User for authentication:** Windows network user who has access to the folder.
- **Password for authentication:** Windows network password that has access to the folder.

After registering the network unit, a status message will be displayed when registering the units. If the drive is mapped successfully, a success message will be displayed, otherwise an Operating System error message will be displayed. Consult the Operating System manual for more information about the error message displayed.

### 10.1.9 Protocols

This tab allows you to configure advanced protocol options used by the system. When selecting this tab we get the following screen:



- **Standard HTTP authentication method:** Here we can select between **Digest** (more secure) or **Basic** methods. The system always determines, according to the HTTP driver of the devices, which authentication method will be used, however the first attempt will be made with the protocol selected here. By default, the recommendation is to keep it in the **Digest** method, as it is safer and does not expose data in this first attempt.
- **Default RTSP authentication method:** Here we can select between **Digest** (more secure) or **Basic** methods. The system always determines, according to the devices' RTSP driver, which authentication method will be used, however the first attempt will be made with the protocol selected here. By default, the recommendation is to keep it in the **Digest** method, as it is safer and does not expose data in this first attempt.
- **Use RTP timestamp:** When selecting this option, the system will use the RTP timestamp instead of the operating system timestamp for its operations. This option will only work for cameras that work with the RTSP protocol and can help smooth the video stream for cameras with low connection quality (For example via the internet), but will introduce a small latency (Configurable). To apply this setting you need to deactivate and reactivate your cameras.
  - **Packet Buffer Size:** Determines the buffer size for RTP packets. The larger the buffer, the greater the latency of the images, but the better the smoothing of the video stream, especially for low quality connections.

## 10.2 Server Events

The system allows the configuration of server health monitoring events. With these events it is possible to monitor the system's CPU and memory usage and trigger events in the event of an abnormality.

CPU monitoring will monitor the global CPU of the server (and not just the system server process). It is possible to configure a usage limit and a timeout, where if the global CPU usage goes above the configured limit for the specified time, then the event will be triggered. A restore to normal (Below Threshold) event can be triggered when CPU usage returns below the threshold.

RAM monitoring will only monitor memory usage by the system server process (Server.exe). It is possible to configure a limit for memory usage by the server, where if the usage goes above the configured limit, then the event will be generated. A restore to normal (Below Threshold) event can be triggered when RAM usage returns below the threshold.

The screenshot shows the 'Hardware' configuration window. It contains two main sections: 'CPU Events' and 'RAM Events'. Each section has checkboxes to activate specific events, input fields for thresholds and timeouts, and buttons to configure actions.

**CPU Events**

- ☒ Activate event of global CPU usage limit
  - Percentage of CPU usage to trigger the event: 80
  - Time of CPU usage over the limit to trigger the event (Seconds): 10
  - Event rearm time (Seconds): 60
  - Configure the actions to execute on event: Event Actions
- ☒ Activate event of return to normal CPU usage
  - Configure the actions to execute on event: Event Actions

**RAM Events**

- ☒ Activate event of server memory usage limit
  - RAM Memory usage limit (MB) to trigger the event: 3000
  - Configure the actions to execute on event: Event Actions
- ☒ Activate event of return to normal memory usage
  - Configure the actions to execute on event: Event Actions

At the bottom of the window is a 'Save Settings' button.

- **CPU Events:**

- **Activate Global CPU Usage Limit Event:** Trigger an event when CPU usage remains above a configured threshold for a long time.
  - **CPU Usage Percentage to trigger the event:** Enter the threshold value that will be used to trigger the event if CPU usage remains above this value.
  - **CPU usage time above limit:** Enter the value (In seconds) for the event to trigger if the CPU is above the configured limit for more than this configured time.
  - **Event Rearm Time:** Rearm time, where the system will wait the configured time before triggering a new event (If CPU usage still remains high)
  - **Event Actions:** Desired event actions when this event is triggered. To learn more about alarm actions see chapter [How to configure event actions](#).
- **Activate Return to Normal CPU Usage Event:** Trigger an event when CPU usage normalizes below the configured threshold.
  - **Event Actions:** Desired event actions when this event is triggered. To learn more about alarm actions see chapter [How to configure event actions](#).

- **Memory Events:**

- **Activate Memory Usage Limit Event (By server process only, not global):** Triggers an event when memory usage by the VMS server service is above a configured threshold.
  - **Memory Usage Limit (In MB) to Trigger the Event:** Specify the limit in Megabytes of memory usage of the VMS server process to trigger the event.
  - **Event Actions:** Desired event actions when this event is triggered. To learn more about alarm actions see chapter [How to configure event actions](#).
- **Activate Return to Normal Memory Usage Event:** Trigger an event when memory usage normalizes below the configured threshold.
  - **Event Actions:** Desired event actions when this event is triggered. To learn more about alarm actions see chapter [How to configure event actions](#).

# Chapter



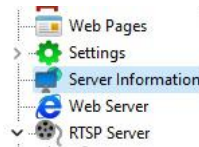
XI



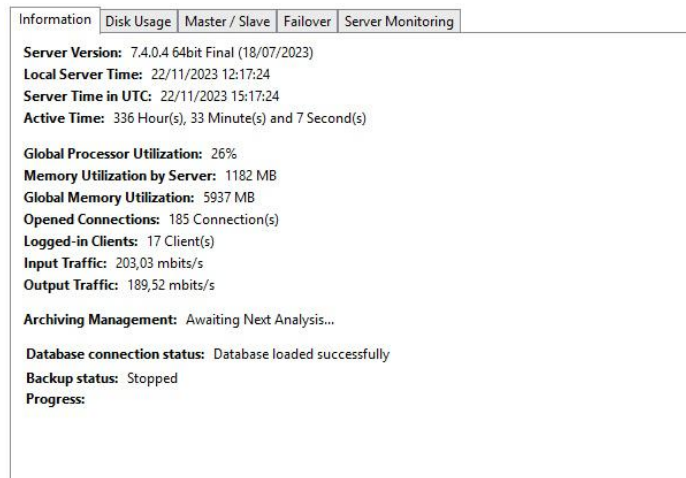
## 11 Server Information

In this area of the system you can monitor how the server is performing, retrieving data such as processor usage, memory, network traffic, etc.

To access this feature, click on the **Server Information** item in the Settings Menu, as shown in the figure below:



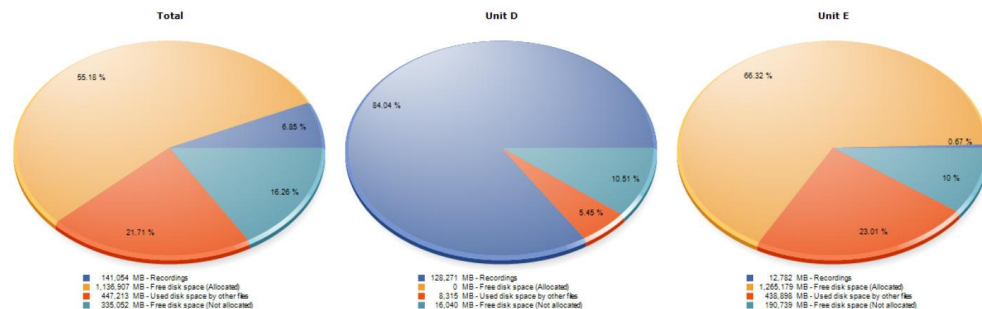
Once this is done, the server information window will open on the right side, as shown in the figure below:



- **Server Version:** Displays the server version.
- **Local Server Time:** Displays the server's local time.
- **Server Time in UTC:** Displays the server time adjusted to UTC.
- **Active Time:** Displays the time that the server service has been active.
- **Global Processor Usage:** Displays the global CPU usage of the server where the server process is running. This value represents the total usage by all Operating System processes and not just the VMS Server.
- **Server Memory Usage:** Displays the memory usage of the VMS Server process only.
- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Open Connections:** Number of open connections with the VMS Server.
- **Logged in Clients:** Number of individual clients connected to the server.
- **Input Traffic:** Total data being received by the VMS server (Device Traffic).
- **Output Traffic:** Total data being sent by the VMS server (To clients).
- **Archiving Management:** Displays the current state of the archiving system.
- **Database Connection Status:** Displays the current status of the Database connection.
- **Backup Status:** Informs whether the database backup is running.
- **Progress:** Displays the database backup progress.

## 11.1 Disk Usage

The server disk usage tab generates a graph for each disk unit managed by the server and an overall graph (Total):



- The dark blue color in the graph represents the percentage of recorded data.
- The yellow color represents the percentage of free disk space allocated for recording.
- The orange color represents the percentage of space used by other files not related to image recording.
- The light blue color represents the percentage of disk space not allocated for recordings by the system. This space can be changed, see the chapter: [General Settings](#).

In the example above, the first graph is the sum of the other two units used by the system (Unit D and Unit E);

## 11.2 Monitoring

On this screen you will be able to monitor the use of server resources via graphs, as shown in the image below:



- **Global Processor Usage:** Displays the global CPU usage of the server where the server process is running. This value represents the total usage by all Operating System processes and not just the VMS Server.
- **Server Memory Usage:** Displays the memory usage of the VMS Server process only.

- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Connections:** This graph has 2 lines, the blue line represents the number of open connections with the server and the green line represents the number of connected clients.
- **Input Traffic:** Total data being received by the VMS server (Device Traffic).
- **Output Traffic:** Total data being sent by the VMS server (To clients).

# Chapter



XII

## 12 Web Server

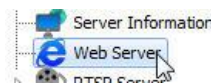
The system has an embedded web server, which is used to distribute files necessary for automatic client updates (in server version upgrades), distribution of general files and also has an interface for monitoring and video playback via Internet Explorer.

### + Note

For live monitoring and video playback, the Embedded Web Server works only with ActiveX plugins in Internet Explorer and is kept on the system for backwards compatibility reasons only. For a better experience with greater compatibility, use the system's HTML5 Web Server, installed separately.

### 12.1 Settings

To access the Web Server settings, click on **Web Server**, located in the **Settings Menu**, as illustrated in the figure below:



Once this is done, the Web Server settings will be displayed on the right, as shown in the figure below:






A screenshot of the Web Server settings form. It contains two sections. The first section has a checked checkbox 'Activate web server' and a checked checkbox 'Activate HTTP (No encryption)'. Below these is a text field 'Server port:' with the value '7001' and a small icon to its right. The second section has an unchecked checkbox 'Activate HTTPS (SSL)'. Below it is a text field 'Server port:' with the value '443' and a small icon to its right. At the bottom is a blue button labeled 'Save settings'.

- **Activate the web server:** Activates the Web server allowing users to connect to the server through a web browser.
- **Server port:** Port used to access the server. This port can be changed and must be configured on your router for external access.
- **Enable HTTPS (SSL):** Enable HTTPS support on the web server. To use SSL you must provide SSL certificates. See the [SSL Certificates](#) topic for more information.
- **Server Port:** Configure the access port via HTTPS.

### 12.2 File Server


The Web Server can also work as a file server. You can use this feature to for example provide a centralized client server list script file (See the topic on [Centralized server list](#) for more information) or provide any file you want.

To use this feature, just create a folder named **public** inside the **http** folder in the server installation directory:

Name	Date modified	Type	Size
 imagens	5/25/2021 4:41 PM	File folder	
 public	6/23/2023 5:53 PM	File folder	
 SSLCert	8/10/2020 12:23 PM	File	7 KB
 SSLKey	8/10/2020 12:23 PM	File	2 KB
 SSLRootCert	8/10/2020 12:23 PM	File	7 KB

All files and subfolders within the **public** folder will be accessible through the Web Browser (or third-party systems) via the URL **http://<IP>:<PORT>/public**

For example, a servers script file **servers.dssf** can be accessed through the URL **http://<IP>:<PORT>/public/servers.dssf**

Name	Date modified	Type	Size
 servers.dssf	11/22/2023 1:32 PM	DSSF File	1 KB

# Chapter



XIII

## 13 RTSP Server

The RTSP server can be used to provide media to any player that supports the RTSP protocol, and can also be used to send media to broadcast servers such as Wowza and integrate with third-party systems.

The RTSP server supports media in the following formats:

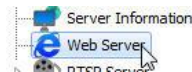
- **Video:** H.265, H.264, MPEG-4 and Motion JPEG
- **Audio:** PCM, G.711, G.726 and AAC

To receive live video on RTSP clients, use the syntaxes below:

- **Live Video with Standard Profile:** `rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<CAMERA_NAME>`
- **Live Video with Specific Profile:** `rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<CAMERA_NAME>&Profile=Custom&CustomProfile=<PROFILE_NAME>`

### 13.1 Settings

To access the RTSP Server settings, expand the **RTSP Server** icon, located in the **Settings Menu** and select the **Settings** icon as shown in the figure below:



The settings screen below will be displayed:

 A screenshot of the RTSP Server settings window. It contains the following elements:
 

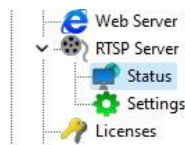
- A checked checkbox labeled 'Activate RTSP server'.
- A 'Server Port' label followed by a text box containing '554' and a spin button.
- A checked checkbox labeled 'RTSPS'.
- An 'RTSPS Port' label followed by a text box containing '322' and a spin button.
- An unchecked checkbox labeled 'Limit connection time'.
- Below the 'Limit connection time' checkbox, a text box containing '300' and a spin button, followed by the text 'Seconds per connection'.
- A 'Save settings' button at the bottom.

- **Activate the RTSP server:** Enables or disables the RTSP Server.
  - **Server Port:** Port used to access the RTSP Server. The default RTSP port is 554.
  - **RTSPS:** Enables or disables RTSPS (RTSP over SSL).
    - **RTSPS Port:** Connection port for RTSPS. The default RTSPS port is 322.
- **Connection Time Limit:** Option to configure a maximum time limit for which each connection can remain open.
- **Save Settings:** Saves the options configured on the screen.

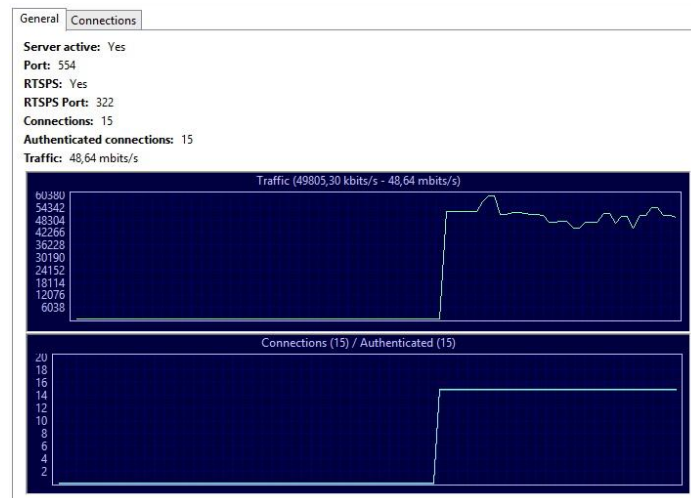
### 13.2 Status

To access the RTSP Server status, expand the **RTSP Server** item, and click on **Status**, located in the **Settings Menu**, as illustrated in the figure below:





Once this is done, the screen below will be displayed with two tabs, **General** and **Connections**:



The **General** tab will provide the following information:
















- **Server Active:** Indicates whether the RTSP server is active.
- **Port:** Indicates the port on which the server is running.
- **RTSPS:** Indicates whether the RTSPS option is enabled.
- **RTSPS Port:** Indicates the port configured for RTSPS.
- **Connections:** Indicates the number of connections to the RTSP server.
- **Authenticated Connections:** Indicates the number of authenticated connections to the RTSP server.
- **Traffic:** Displays the network bandwidth used in real time.
- **Traffic Graph:** Displays the RTSP Server traffic history.
- **Connection Graph:** Displays the history of connections to the server. This graph has 2 lines, one line showing the number of open connections and the other line showing the number of effectively authenticated connections.

The **Connections** tab will display details about the currently open connections to the RTSP server:

General

Connections

Search

User	IP	Camera	Transport	Traffic	Connection time
 user	192.168.1.100	60	TCP	11,28 kbits/s	68 Hour(s), 0 Minute(s) and 39 Second(s)
 user	192.168.1.100	48	TCP	992,32 kbits/s	67 Hour(s), 58 Minute(s) and 51 Second(s)
 user	192.168.1.100	79	TCP	3,24 mbits/s	67 Hour(s), 53 Minute(s) and 4 Second(s)
 user	192.168.1.100	03	TCP	3,09 mbits/s	10 Hour(s), 55 Minute(s) and 1 Second(s)
 user	192.168.1.100	03	TCP	3,09 mbits/s	9 Hour(s), 18 Minute(s) and 8 Second(s)
 user	192.168.1.100	52	TCP	1,58 mbits/s	9 Hour(s), 18 Minute(s) and 8 Second(s)
 user	192.168.1.100	79	TCP	3,24 mbits/s	9 Hour(s), 18 Minute(s) and 8 Second(s)
 user	192.168.1.100	41	TCP	1,71 mbits/s	9 Hour(s), 18 Minute(s) and 8 Second(s)
 user	192.168.1.100	02	TCP	832,87 kbits/s	6 Hour(s), 38 Minute(s) and 28 Second(s)
 user	192.168.1.100	79	TCP	3,24 mbits/s	6 Hour(s), 38 Minute(s) and 28 Second(s)
 user	192.168.1.100	11	TCP	5,26 mbits/s	6 Hour(s), 38 Minute(s) and 28 Second(s)
 user	192.168.1.100	02	TCP	13,41 kbits/s	6 Hour(s), 38 Minute(s) and 28 Second(s)
 user	192.168.1.100	11	TCP	69,00 kbits/s	6 Hour(s), 37 Minute(s) and 24 Second(s)
 user	192.168.1.100	51	TCP	3,55 mbits/s	1 Hour(s), 18 Minute(s) and 52 Second(s)
 user	192.168.1.100	51	TCP	17,00 mbits/s	0 Hour(s), 0 Minute(s) and 11 Second(s)

Disconnect

Export

- **User:** Name of the logged in user.
- **IP:** IP of the logged in user.
- **Camera:** Camera the user is viewing.
- **Transport:** Transport mode used (TCP or UDP).
- **Traffic:** Bandwidth used by the connection.
- **Connection Time:** Total time the connection is open.
- **Disconnect:** Disconnects selected connections.

# Chapter

XIV

## 14 Logs

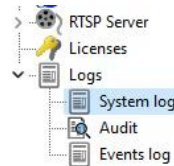
Logs are very important tools for an environment involving a security system such as Digifort, as they record all events and user actions that occur in the system.

### 14.1 System Logs

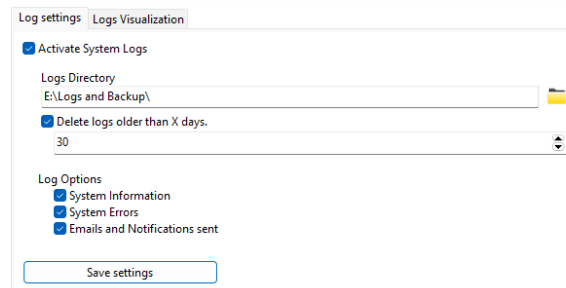
System logs record server-specific events, such as when the server was started or stopped, recording recycling information, deleted files, server errors, emails sent, among others. System logs are recorded in text files in the configured folder.

#### 14.1.1 How To Configure System Logs

To access the system log settings, expand the **Logs** item, located in the **Settings Menu**, and click on the **System Logs** item as shown in the figure below:



Once this is done, the log settings will be displayed on the right, as shown in the figure below:

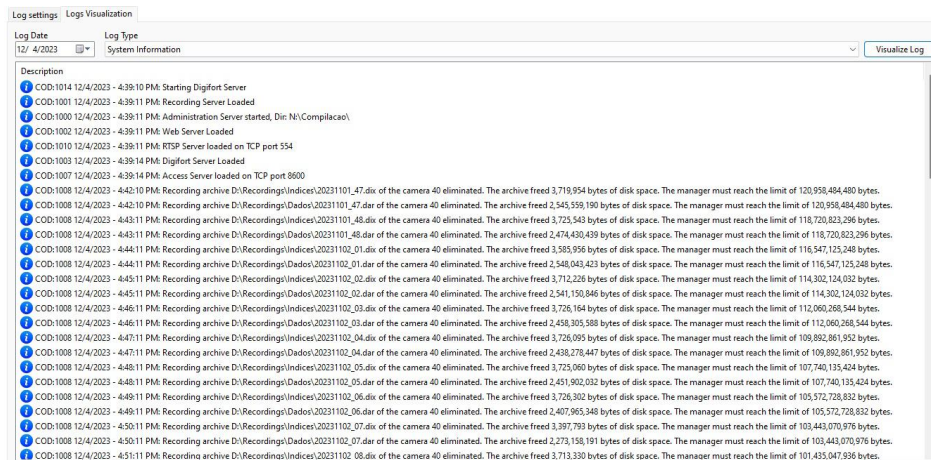


- **Activate system logs:** Enables or disables system logs.
- **Log Directory:** Select the directory where alert and event logs will be saved.
- **Delete logs older than X days:** Deletes old logs, specified by the number of days entered.
- **Event log options:**
  - **System information:** This log records information about system operation, such as, for example, the time the server was loaded, terminated.
  - **System errors:** This log records information about system errors such as the incorrect functioning of some system functionality.
  - **E-mails and Notifications sent:** This log records information about emails and push notifications sent by the system, for example, emails about camera recording and communication failures.
- **Save Settings:** Saves system logs settings.

#### 14.1.2 How To View System Logs

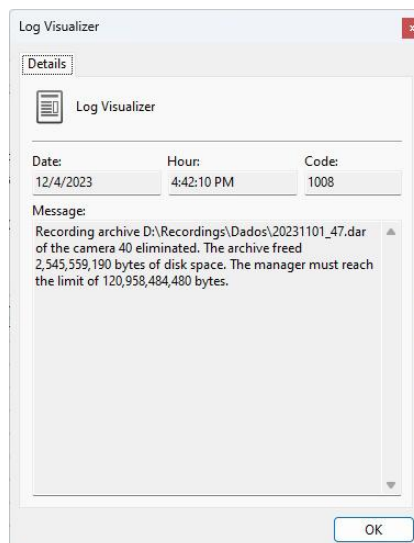
The visualization of the logs is a tool to help the administrator in the analysis of a problem, presenting a more friendly and productive interface compared to a simple text file.

To view the event logs, click on the **Logs Visualization** tab, as shown in the figure below:



To view a log, select the date, type and click on the **View Log** button. Thus the list of log records will be populated.

Double-clicking on an item in the log will display a screen with detailed information about the record, as shown in the figure below:



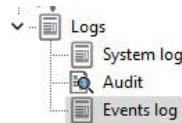
## 14.2 Event Logs

Event logs record events that occur on the server, such as device events, global events, motion detection, among others. Unlike system logs, event logs are recorded in the server database to provide detailed query and reporting through the Surveillance Client.

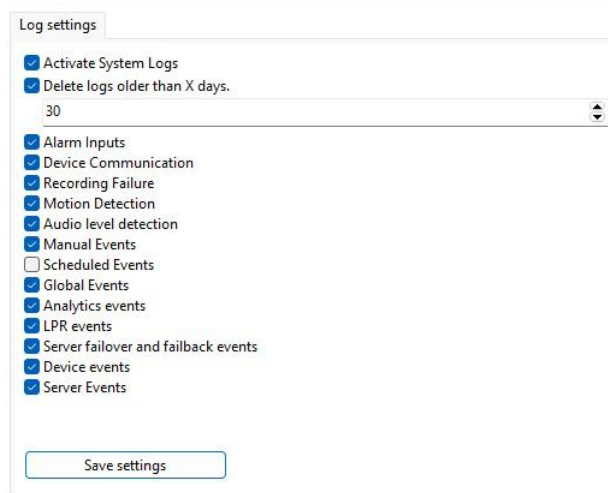
### 14.2.1 How To Configure Event Logs

Configuring system event logs allows several categories of events to be recorded in your database. These events can be listed and used to search for any pertinent recordings in the surveillance client.

To access the event log configuration, expand the **Logs** item, located within the **Settings Menu** and click on the **Event Log** item:



Once this is done, the alert and event log configuration screen will be displayed on the right, as shown in the figure below:



- **Activate system logs:** Enables or disables system logs.
- **Delete logs older than X days:** Deletes old logs, specified by the number of days entered.

The system will provide a list of types of events to be registered. Select all event types that you want to keep recorded in the log.

- **Save Settings:** Saves the current settings on screen.

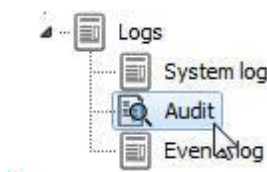
## 14.2.2 How To View Event Logs

Event Logs are viewed within the Surveillance Client. To learn how to view event logs, see the Surveillance Client manual.

## 14.3 Audit

The Audit feature aims to record all user actions on the system and connections to the server.

To access the event log configuration, expand the **Logs** item, located within the **Settings Menu** and click on the **Audit** item:



Once this is done, the **Audit Log** will be displayed on the screen on the right:

Start date and time	Final date and time	Category	Keyword					
11/ 1/2023	12/ 5/2023	All						
00:00:00	23:59:59		<input checked="" type="checkbox"/> Search by exact keyword					
Date	User	IP	Event	Object	Object name	Category	Complement	
11/6/2023 1:17:54 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Live view via relay	
11/6/2023 1:17:55 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Live view via relay	
11/6/2023 1:17:55 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Administration Client	
11/6/2023 1:17:55 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Audio	
11/6/2023 1:22:30 PM	admin	127.0.0.1	Logout	Server	2	Connections to the server	Connection time: 0 Hour	
12/1/2023 4:32:18 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Audio	
11/6/2023 11:20:40 AM	admin	127.0.0.1	Login	Server	0	Connections to the server	Administration client	
11/6/2023 1:39:21 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Live view via relay	
11/6/2023 1:39:21 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Administration Client	
11/6/2023 1:52:36 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Live view via relay	
11/6/2023 1:52:36 PM	admin	127.0.0.1	Viewed	Camera	40	User action	Administration Client	
11/6/2023 3:00:01 PM	admin	127.0.0.1	Login	Server	0	Connections to the server	Administration client	
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	01	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	06	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	100	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	103	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	19	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	20	User action		
12/1/2023 4:32:18 PM	admin	127.0.0.1	Started controlling	Camera PTZ	40	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	40	User action	General.Activate: True ->	
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 04	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 05	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 06	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 07	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 08	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 09	User action		
11/6/2023 3:00:08 PM	admin	127.0.0.1	Modified	Camera	IBCloud Native 10	User action		

The audit system maintains two categories of information in the database: **User actions in the system** and **Connections with the server**.

Just like the Event Log, Audit logs are recorded in the database for better consultation and details.

- **Start and End Date and Time:** Select the start and end date and time for consulting audit records
- **Category:** Select the audit category to filter the records
- **Keyword:** Enter a keyword to search audit logs. The system will search for this word in all details of the records, such as object names, username, IP and complement.
  - **Search by Exact Keyword:** Select this option for the system to make the comparison using exactly the keyword entered (For example, a username). Disabling this option will potentially provide more results, but the search will be slower.

Some audit records (such as object changes) will record additional details (such as what was changed). Double click on a record to open the screen with more details:

Audit Record Details

Details

Audit Record Details

Record Date	User	IP
12/5/2023 5:52:00 PM	admin	127.0.0.1

Event	Object Type	Object Name	Category
Modified	Camera	20	User action

Complement

General.Shortcut: 20 -> 21  
 Lens.Data  
 Lens.LensType: 0 -> 1  
 Recording.Archiving.Activate: False -> True  
 Recording.Archiving.AlertGroup: -> Artemijus  
 Recording.Config.RecordingDays: 360 -> 60  
 Recording.SelfHealing.Source: 1 -> 0

Close

The Surveillance Client also provides an audit viewer, but it is more powerful than the one found in the Administration Client. The Surveillance Client's audit search tool works on multiple servers simultaneously and has more filters and features. For more information, see the Surveillance Client manual.



# Chapter



XV

## 15 SSL Certificates

For the system to provide access to the server via SSL / TLS, the use of SSL certificates is required.

The system provides a standard, self-signed certificate, which must be replaced with your certificate.

The certificate files are located in the **HTTP** subfolder in the case of the VMS Server, or in the installation root folder in the case of the other services (Analytics, LPRI, Mobile Camera, Live Witness, etc...).

SSLCert	8/10/2020 12:23 PM	File	7 KB
SSLKey	8/10/2020 12:23 PM	File	2 KB
SSLRootCert	8/10/2020 12:23 PM	File	7 KB

- **SSLCert**: Certificate file in PEM format.
- **SSLKey**: Private key file in PEM format, without encryption.
- **SSLRootCert**: Root certificate file in PEM format.

The system only supports files in PEM format. To check whether a certificate file is in PEM format, open the file in Notepad:

```
-----BEGIN CERTIFICATE-----
MIIF8zCCBNugAwIBAgIRAI28r5Y1ivLM2cpbuZ3/S8MwDQYJKoZIhvcNAQELBQAw
gY8xCzAJBgNVBAYTAkdCMRswGQYDVQQIEzJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
BgNVBAcTB1NhbGZvcmlkLWUuIFZhbG1kYXRpb24gTG1taXR1ZDE3MDUGA1UE
AxMuU2VjdG1nb3B5SU0EgRG9tYwluIFZhbG1kYXRpb24gTG1taXR1ZDE3MDUGA1UE
QTAeFw0yMDA4MTAwMDAwMDAwFw0yMTA4MTAyMTU5NTIaMCoxKDAwBgNVBAMTH3Np
c3R1bWZlLnFkdmlzb3JzZW51cm10eS5jb20uYnIwggE1MA0GCSCqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDQ0qmbF2pJ5/a1U25X0o1AI4ukA+CLUsY4nW5ngM/Dv84u1
n35Nvv1mQMDypwEYMSGAx71WAj1iQUip/16zKDeM/EJaUnm4zr0WJ+37K1J1Cr-i2X
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzqpmxdqY0v2pVluVzqNQCOPAPgi1LGOJ1uZ4DPw7/OLop9+
Tb79ZkDA8qcBGDEhgmE5VgISykFKf9esy3jPxCwIDZuM69F1ft+yo1dQq4t145F
bGZArYGEWu1UDeNQLGcJndRBWB3hVM62o2hce6WBH8vXoKD8KSKp001GsdYuGYSK
URgUVs58F7yXgtGqKQVYZwzaZmZ4gmeJJFMPq2YFSiq1qFLn/+m9FU4RzPXs4ZPA
FrPkNX2YoDcvgzRVINC5WB+dArhIE1xkA4/rV/yTjv/XsghLsraKhQeNiW0vsvx
B5ZiSp2lkrqntY2atse3+igKLPRAWEaPkU71kwIDAQABAoIBAF1z+n4ja0j0UQ04Q
```

The certificate file should contain the text **-----BEGIN CERTIFICATE-----**

The private key file should contain the text **-----BEGIN RSA PRIVATE KEY-----** or corresponding to the format of your key.

- Replace the **SSLKey** file with your private key file. The private key file is generated when you request a new certificate.
- Replace the **SSLCert** file with your certificate file.
- If you don't have a root certificate, just copy the **SSLCert** file to **SSLRootCert**.

### 15.1 How to Generate a Self-Signed Certificate

To generate a self-signed certificate, we recommend using the OpenSSL library.

Install OpenSSL on your server. You can download binary files from this address:  
<https://wiki.openssl.org/index.php/Binaries>

#### 1. Generate a Certificate Signing Request (CSR) along with the private key.

First, you must generate a CSR. The example below will generate a CSR and a private key in 2048-bit RSA format.

```
openssl req -newkey rsa:2048 -keyout PrivateKey.pem -out MyCsr.csr
```

- **openssl**: Command to run OpenSSL.
- **-req**: New certificate signing request (CSR).
- **-newkey rsa:2048**: Specifies that a new private key should be created, with a 2048-bit RSA algorithm. If you prefer a 4096-bit key, you can change this number to 4096.
- **-keyout PrivateKey.pem**: Specifies the name of the output file (PrivateKey.pem), which will be in PEM format, encrypted.
- **-out MyCsr.csr**: Specifies the certificate signing request (CSR) file.

[illegible]

When you press **Enter**, you will be presented with a series of questions.

1. First create and verify the password for the file. **Remember this password as you will need it again to access your private key.**
2. Now you have to enter the information that should be included in your CSR. This information is also known as the **Distinguished Name**, or **DN**. The **Common Name** field is required by SSL.com when submitting your CSR, but the others are optional. If you want to ignore an optional item, just type enter when it appears:
3. The **Country Name** (optional) uses a two-letter [country code](#).
4. The **Locality Name** field (optional) is for your city or town.
5. The **Organization Name** field (optional) is for the name of your company or organization.
6. The **Common Name** field (required) is used for the [FQDN \(Fully Qualified Domain Name\)](#) of the website that this certificate will protect.
7. E-mail address (optional).
8. The Challenge Password field is optional and can also be ignored.

Once this process is complete, you will be returned to a command prompt. You will not receive any notification that the CSR has been successfully created.

You should now have the PrivateKey.pem and MyCSR.csr files.

## 2. Generating the Self-Signed Certificate

You can now generate the self-signed certificate using the CSR and the private key. You will also specify the validity period of the certificate:

```
openssl x509 -req -in MyCsr.csr -signkey PrivateKey.pem -out
SSLCert -days 365
```

- **openssl**: Command to run OpenSSL.
- **x509**: Public standard format for certificates.
- **-req**: Indicates that you are creating a certificate from a CSR.
- **-in MyCsr.csr**: Specifies the CSR file created in the previous step.
- **-signkey PrivateKey.pem**: Specifies the private key file created in the previous step.
- **-out SSLCert**: Indicates the certificate output file (SSLCert).
- **-days 365**: Indicates the validity of the certificate.

```
C:\Program Files\OpenSSL-Win64\bin>openssl x509 -req -in MyCsr.csr -signkey SSLKey -out SSLCert -days 365
Enter pass phrase for SSLKey:
Certificate request self-signature ok
subject=C=US, ST=Florida, L=Boca Raton, O=Digifort, CN=*.digifort.com, emailAddress=digifort@digifort.com
```

Press **Enter**, you will be required to enter the password for the private key file created in the previous step.

If the process completes successfully, you will now have the SSLCert file.

### 3. Root certificate

The generated certificate will also be used as the root certificate, so copy the SSLCert file to SSLRootCert

```
copy SSLCert SSLRootCert
```

### 4. Private Key

Now we'll generate the SSLKey file, to do this use the following command:

```
openssl rsa -in PrivateKey.pem -out SSLKey
```

Press **Enter**, you will be required to enter the password for the private key file created in the previous step.

Now you have the **SSLCert**, **SSLRootCert** and **SSLKey** files, copy these files and replace them in the system installation folder to load the certificates and restart the services.

## 15.2 Converting Certificates to PFX Format

The system only supports files in PEM format. If you have your certificate or private key in another format, you must first convert the file to PEM format.

The PFX file is a package that contains the private key and the certificate, encrypted within the same file. To extract the private key and certificate, follow these steps:

### 1. Extract the private key

The first step is to extract the private key from the certificate file:

```
openssl pkcs12 -in certificate.pfx -nocerts -out PrivateKey.pem
```

When you press **Enter**, provide the export password for the pfx file and also provide a new password for the private key file.

Now we'll generate the SSLKey file (assuming the key is RSA), using the following command:

```
openssl rsa -in PrivateKey.pem -out SSLKey
```

Press **Enter** to supply the password for the private key file created in the previous step.

## 2. Extract the certificate

The second step is to extract the certificate from the file:

```
openssl pkcs12 -in certificate.pfx -clcerts -nokeys -out SSLCert
```

## 3. Root certificate

The generated certificate will also be used as the root certificate, so copy the SSLCert file to SSLRootCert

```
copy SSLCert SSLRootCert
```

Now you have the **SSLCert**, **SSLRootCert** and **SSLKey** files, copy these files and replace them in the system installation folder to load the certificates and restart the services.

# Chapter



XVI

## 16 Clients auto-update

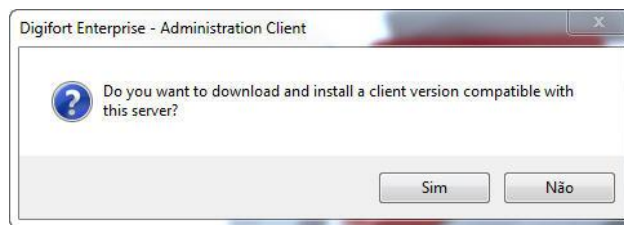
In a server version update, the system enables automatic updating of Administration and Monitoring Clients.

This feature consists of checking whether the versions of the server the client is trying to connect to are the same, if the versions are different, the system will offer automatic updating, which will download the client installation directly from the server and update them. at the local station.

When logging into the system, whether in the Administration or Surveillance client, if the versions are not compatible (example: 6.4 with 6.5) the following message will appear: **Your client version is incompatible with the server version.** as shown in the image below:

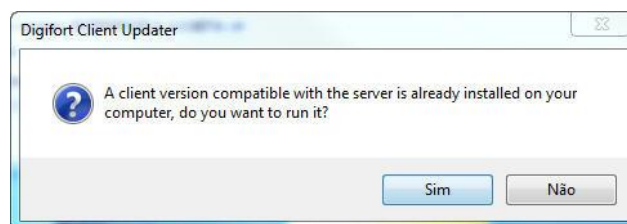


When clicking **OK** a dialog box will appear with the following question: **Do you want to download and install a client version compatible with this server?**

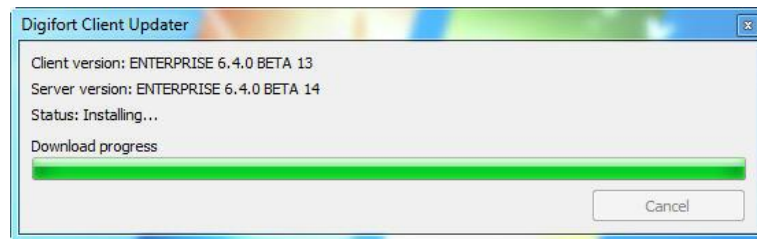


By clicking on **No** the dialog box will close and nothing will happen. If you click **Yes**, the system will automatically install the compatible client versions on the computer.

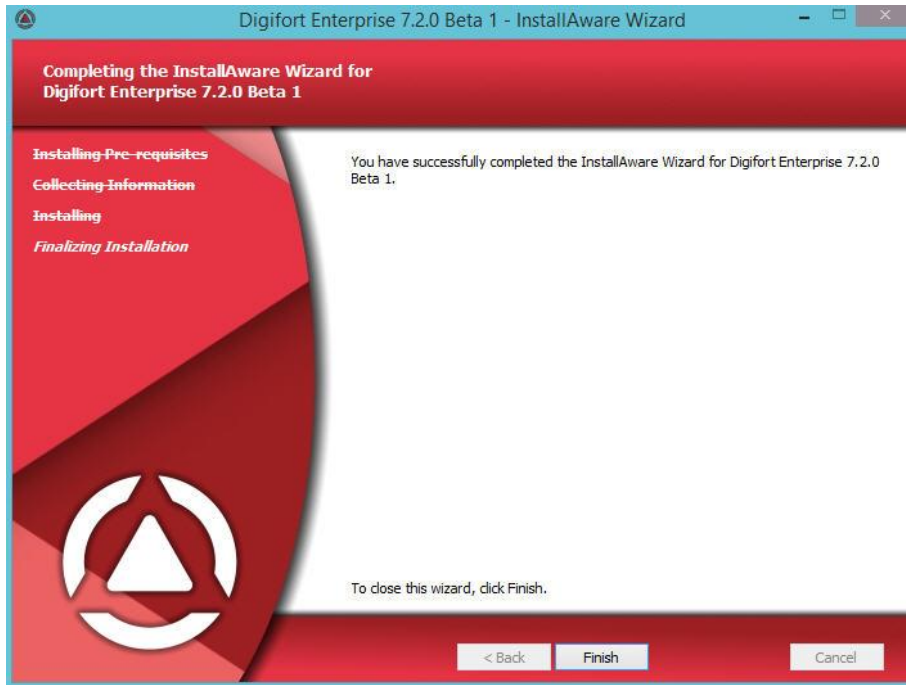
If there is a digifort version compatible on your machine, the following message will appear: **A version compatible with the server is already installed on your computer, do you want to run it?**



If you click **Yes** the client will run. Otherwise the client installation will continue. Clients installation will be downloaded from the server through the tool displayed below:



The installer will be displayed, proceed with the installation normally and at the end click **Finish**:



#### Note

The user performing the installation must have rights to install programs on the Operating System

After installation the compatible client will be ready to connect to the required server.



# Chapter



## 17 Database Maintenance

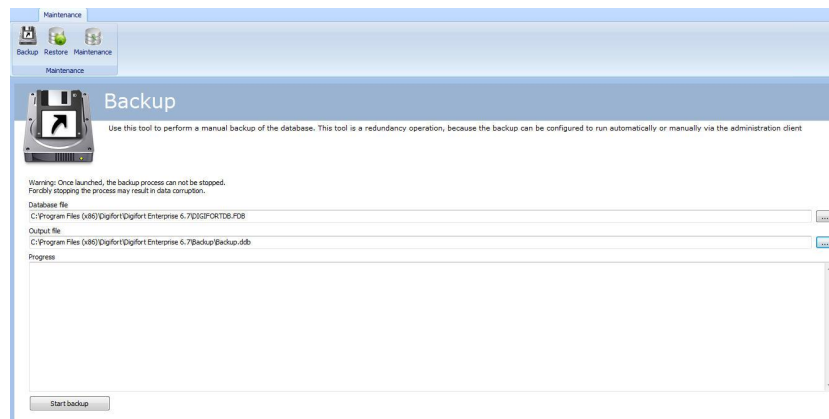
Through the database maintenance application you will be able to:

- **Back up the system database**
- **Restore a system database backup**
- **Repair a corrupted database file**

This software is a piece of software located in the root directory of the system installation. Its name is: **DatabaseMaintenance.exe**

### 17.1 Backup

The first available option is the Backup option, in which it is possible to back up the Digifort database.



First choose the database that the backup will be made, then choose the name and directory where the backup will be and finally click on Start Backup.

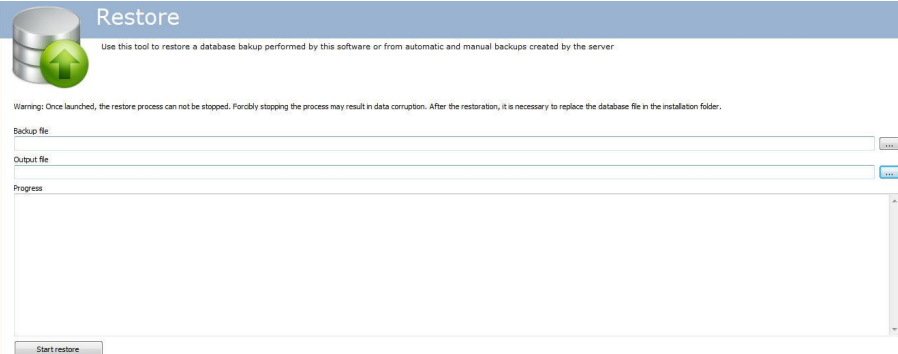
Database backup is saved in **.ddb** format and the current database format is **.FDB**. Thus, the only way to restore the backup is using this same software.

### 17.2 Restore

To start a restoration click on the Restore button shown in the image below:



The following screen will be displayed:



**Restore**  
Use this tool to restore a database backup performed by this software or from automatic and manual backups created by the server.

Warning: Once launched, the restore process can not be stopped. Forcibly stopping the process may result in data corruption. After the restoration, it is necessary to replace the database file in the installation folder.

Backup file:

Output file:

Progress:

- **Backup File:** Select the file to be restored with **.ddp** extension
- **Output file:** Select the file where the restoration will be done. Once done, replace the file in digifort's root folder with the name: DIGIFORTDB.FDB
- **Start Restore:** Click to start restoring the database.

## 17.3 Maintenance

Use this option to check database consistency or fix database corruption issues.

To execute this function, click on the **Maintenance** button indicated in the image below:



### + Note

To perform maintenance, stop all system services.

The following screen will be displayed:



**Repair**  
Use this tool to check the consistency of a database file or repair a corrupted database file.

Attention:  
You cannot run these tasks while the database is in use. Before using any of these tools, stop the Server service.  
It is not advisable to use these tools with the original database files, so after stopping the server service, make a copy of the file and use these tools with the copy. If the operations are completed successfully, the original file will be replaced.  
Once the process starts, it can not be stopped. Forcibly stopping the process may result in data corruption.

Database file:

Check consistency  
Use this tool to check the consistency of the database

Database consistency: Not checked

Repair database  
Use this tool to repair a corrupted database file

Progress:

The screen has the following features:

- **Database File:** Select the file you want to maintain.
- **Check Consistency:** Click to check if your database is corrupted.
- **Repair Database:** Click if the database is corrupted as pointed out by the consistency test.

# Chapter



## 18 Centralized Server List

In large installations with multiple monitoring stations and servers, registering and managing (adding or removing) servers in the Surveillance Client can be an extremely time-consuming task. To facilitate the management of these server records in the Surveillance Clients, it is possible to create a single list with the registration of all servers and when opening the Surveillance Client, it will download this list and register these servers locally (Only for the session current) automatically, so if you need to add a server, remove a server or even change the connection parameters of a server, you can do it once in the configuration file and all Surveillance Clients will be updated automatically the next time once they are started.

The registration of servers must be done in a script file with **.dssf** extension in **XML** format.

File syntax:

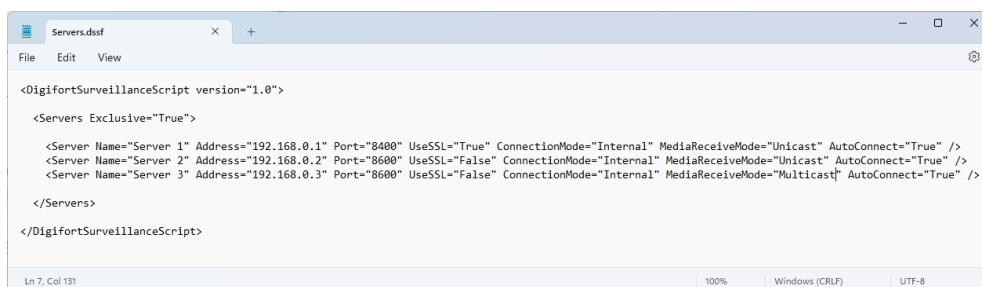
```
<DigifortSurveillanceScript version="1.0">
  <Servers Exclusive="True">

    <Server Name="SERVER_NAME_1" Address="SERVER_ADDRESS" Port="SERVER_PORT"
      UseSSL="True|False" ConnectionMode="Internal|External"
      MediaReceiveMode="Unicast|Multicast" AutoConnect="True|False" />

    <Server Name="SERVER_NAME_2" Address="SERVER_ADDRESS" Port="SERVER_PORT"
      UseSSL="True|False" ConnectionMode="Internal|External"
      MediaReceiveMode="Unicast|Multicast" AutoConnect="True|False" />

  </Servers>
</DigifortSurveillanceScript>
```

You can add as many servers as you want to this list, just by creating more records. See an example file below:



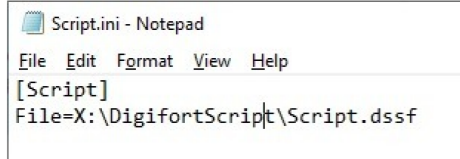
- **Name:** Provide a name for the server.
- **Address:** Provide the server address.
- **Port:** Provide the communication port. 8600 is the default port for normal connection and 8400 is the default port for SSL/TLS connection.
- **UseSSL:**
  - **True:** Enable the use of SSL/TLS (Don't forget to provide the SSL port, 8400).
  - **False:** Uses connection without SSL/TLS (Don't forget to provide the default port, 8600).
- **ConnectionMode:** Provide connection mode:
  - **Internal:** Select **Internal** if the Surveillance Client is running on a local network, or if the cameras are configured to transmit via Relay (Default).
  - **External:** Select **External** if the Surveillance Client is running outside the server's local network and the cameras are configured for direct transmission (No Relay).

- **MediaReceiveMode:** Select between **Unicast** and **Multicast** for the default media transmission mode.
- **AutoConnect:**
  - **True:** Select **True** for the Surveillance Client to automatically connect to this server when opened.
  - **False:** Select **False** so that the Surveillance Client does not connect to this server automatically when opening. The user must manually connect (by double-clicking on the server) to each server.

With the server registration file complete, you must now place it in a location where Surveillance Clients have access. You can use 2 options for this:

#### Shared Folder:

You can place the server registration file in a shared folder on the network, as long as all Monitoring Clients have access to this file. To instruct the Surveillance Client to download this file over the network, you must create a file called **Script.ini** and place this file within the client installation folder:



```
Script.ini - Notepad
File Edit Format View Help
[Script]
File=X:\DigifortScript\Script.dssf
```

In this Script.ini file you will specify the path to the server registration file, as shown above.

#### Web Server:

You can place the server registration file on a Web Server, as long as all Surveillance Clients have access to this server. To instruct the Surveillance Client to download this file over the network, you must create a file called **Script.ini** and place this file within the client installation folder:



```
Script.ini - Notepad
File Edit Format View Help
[Script]
File=http://127.0.0.1/public/servers.dssf
```

In the example above, the V Client will download the server registration file from the URL <http://127.0.0.1/public/servers.dssf>

You can use the File Server feature of the system's own embedded Web Server to provide the server registration file. See the Web Server [File Server](#) topic

# Chapter



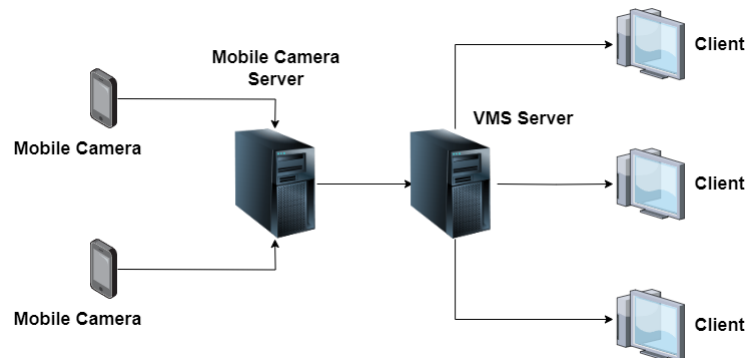
XIX

## 19 Mobile Camera

Mobile Camera is an application that can be installed on cell phones and tablets running IOS (Apple) and Android (Google).

With this application you can turn your cell phone into a mobile remote camera and transmit live video to your VMS server via wireless or 3g/4g/etc connectivity.

In order for the VMS server to receive images from the Mobile Camera application, it needs an intermediary service (which can be running on the same VMS server or on a separate server), called Mobile Camera Server:



The Mobile Camera application, installed on the smartphone or tablet, will connect to the Mobile Camera Server and send the video. The Mobile Camera Server service will in turn forward the images to the VMS server, which will consider each cell phone as a camera registered in the system.

Each mobile device will be independently registered and identified on the VMS server and a camera license will be required for each device.

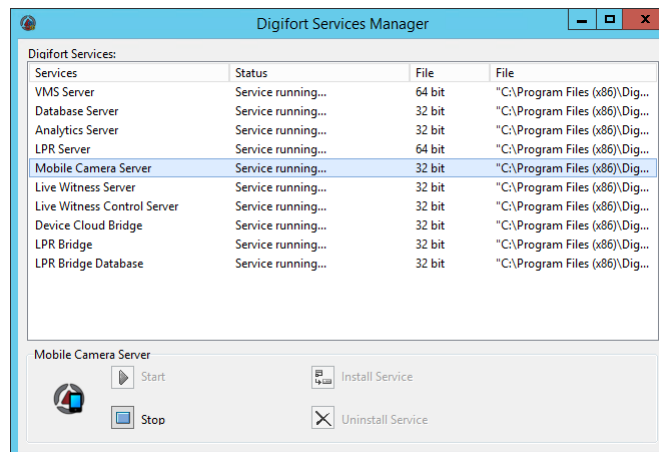
On the next topics you will see how to configure the Mobile Camera server, as well as how to register the camera on the VMS server to retrieve the images from the Mobile Camera server.

### 19.1 How to start the Mobile Camera Server service

To start the Mobile Camera Server service, it must first be installed, follow the steps below to start the service correctly using the Service Manager:

1. Select the **Mobile Camera Server** service .
2. Click on **Install Service**.
3. Click **Start** and wait for the server to start. The start-up process ends when the message "Service running..." appears in the status bar.

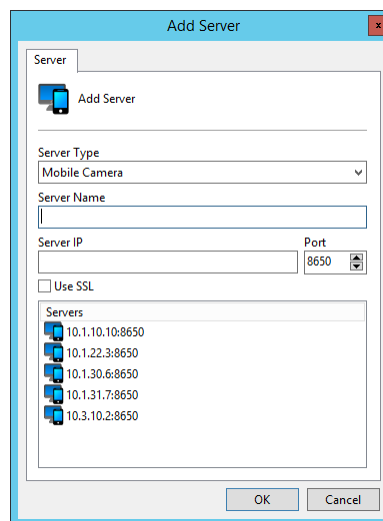




## 19.2 How to configure the servers to be managed

The first step in configuring a Mobile Camera server is to add it to the list of servers to be managed by the Administration Client.

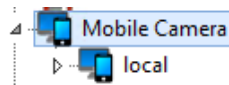
To add a server, click on the **Mobile Camera Servers** tree and then on the **Add Server** button, opening the server registration screen, as shown below:



- **Server Name:** Enter the name of the server to be added. Once the data has been confirmed, the server name cannot be changed.
- **Server IP:** Enter the IP of the server to be managed.
- **Port:** Enter the port used to communicate with the server. By default the port is 8650 or 8450 for secure connection with SSL/TLS
- **Use SSL:** Use secure connection with SSL/TLS. Don't forget to specify the SSL/TLS connection port.
- **Servers:** This list shows all the Mobile Camera servers that the administration client has found on the network. By clicking on one of the servers, the **IP** and **Port** fields described above will be automatically filled in, and all that remains is to fill in the **Server Name** field to complete the registration.

After entering all the data correctly, click **OK**.

Once the server has been added, it will be displayed in the **Settings** Menu, as shown in the figure below:

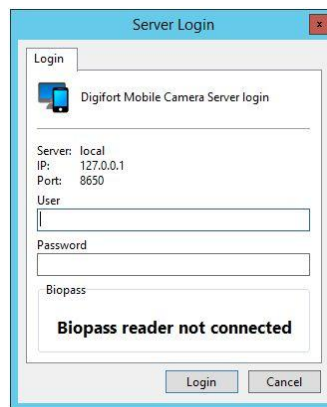


To change the parameters of an already saved server, right-click on the desired server and then click on **Change Parameters**. In the window that opens, change the data as necessary and click **OK**.

To delete a server, right-click on the desired server and then click **Delete Server**. In the confirmation message that appears, click **Yes**.

## 19.3 Configuring the Mobile Camera server

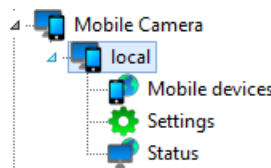
After adding the server, locate it in the Settings Menu and double-click on it. Once this is done, a user name and password will be required to access the server's settings, as shown in the figure below:



- **User:** Access user.
- **Password:** Access password.

Enter the username and password for accessing the server. If this is your first access to the system, enter the username admin and a blank password.

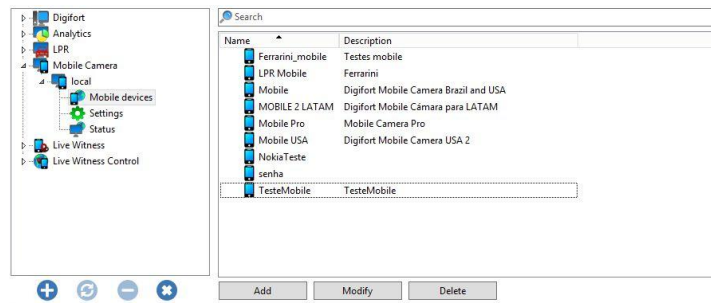
After filling in the access data, click **OK**. If access authentication is successfully completed, the **Settings Menu** will expand, showing the settings available for the server, as illustrated in the figure below:



### 19.3.1 Mobile Devices

Every mobile device (iOS or Android cell phone or tablet) must be identified and connected to the Mobile Camera server. To do this, you must register the device on the server and give it a unique name. In the Mobile Camera app, you must use this name in your settings, thus linking the mobile device to the Mobile Camera server.

To register the devices on the server, click on the **Mobile Devices** option as in the image below:



To add a mobile device ,click **Add**. To change or delete, select the device you want and click on the corresponding button.

The registration screen will appear:



- **Name:** Enter a unique identifier for this device (This name must also be used in the app installed on this device).
- **Description:** Enter a description for this device, for easy identification and organization in the system.
- **Password:** Enter a security password for this device. You must set the same password in the app. This password is required to prevent any other device from connecting to your server.
- **Activate:** Activates or deactivates this device.

Click **OK** to register the device. Repeat this process for all the desired mobile devices.

### 19.3.2 Settings

To access the server settings, click on **Settings** as in the image below:

- **Admin Port:** Port used by the system to configure the Mobile Camera server.
- **HTTP Port:** HTTP port used for communication. The Mobile Camera app must be able to access this port.
- **Stream Input Port:** Port used to receive the video stream. The Mobile Camera app must be able to access this port.
- **Secure communication via SSL:** Activates secure communication via SSL / TLS channel for video transmission.
  - **Administration port:** Secure port used by the system to configure the Mobile Camera server.
  - **HTTPS Port:** HTTPS port used for communication. The Mobile Camera app must be able to access this port.
  - **Stream Incoming Port:** Secure port used to receive the video stream. The Mobile Camera app must be able to access this port.
- **Display message "Waiting for incoming video...":** With this option activated, when the camera is not sending video, Mobile Camera will generate a periodic video stream, with the message "Waiting for incoming video..." to be displayed in the Surveillance Client, thus informing the system operator that the video is not yet being transmitted.
- **Not displaying the list of devices in the app configuration:** The Mobile Camera app will list all the devices registered on the Mobile Camera server, which may not be desirable in some cases. Check this option to not display the device list in the app. In this case, the app operator will need to specify the device name manually.
- **Administration password:** Administration password for the Mobile Camera server.
- **Confirm password:** Confirm the password for registration.
- **Reset admin password:** Resets the admin user's admin password (Blank).
- **Save settings:** Saves the changed settings.

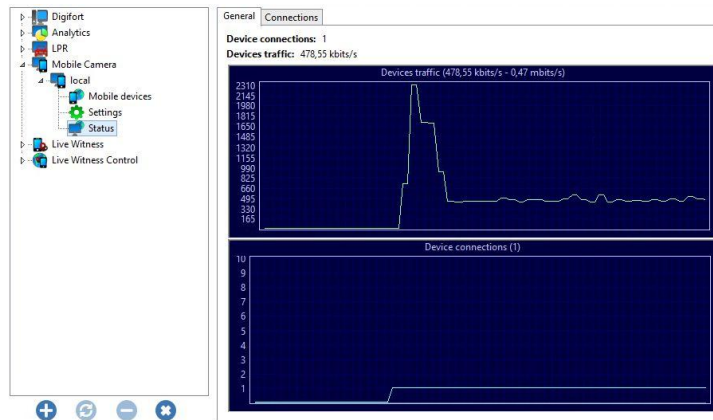
### + Important

The ports must be cleared on the firewall of the network and servers involved for the system to function correctly.

## 19.3.3 Status

In Status we can view important information such as bandwidth consumed and connected devices.

To access it, click on **Status** as shown in the image below:



- **General:** The general tab will display graphs and general consumption information.
  - **Device Connections:** Number of device connections.
  - **Device Traffic:** Total bandwidth used by all connected devices.
  - **Traffic Graph:** Displays a continuous historical graph of the bandwidth consumption of connected devices.
  - **Connections Graph:** Displays a continuous historical graph of the number of connected devices.

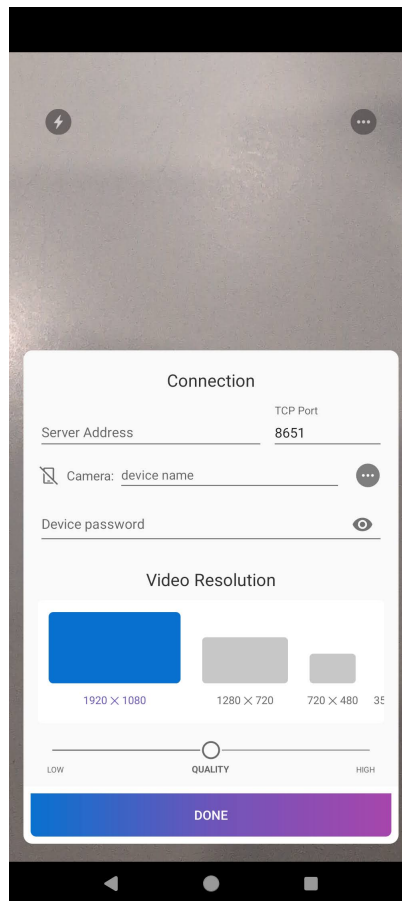
Device	Address	Traffic	Connection time
Mobile USA		483.39 kbits/s	0 Hour(s), 4 Minute(s) and 23 Second(s)

- **Connections:** The connections tab will display a list of all connected devices.
  - **Device:** Identification of the connected device.
  - **Address:** IP address of the device.
  - **Traffic:** Current bandwidth usage.
  - **Connection Time:** Total video transmission time.

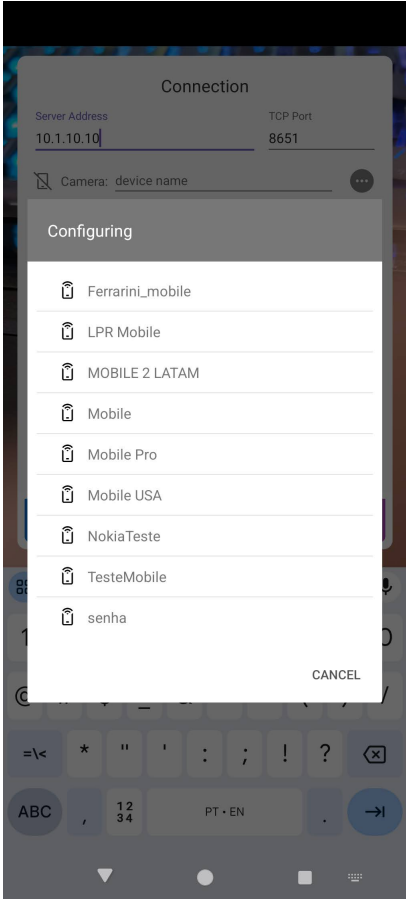
## 19.4 Configuring the Application

First download the **Digifort Mobile Camera Pro** app from Google Play or Apple Store and install it on your mobile device.

When you open the app for the first time, provide all the requested rights and the settings screen will appear:



- **Server Address:** Provide the IP or DNS of the Mobile Camera server.
- **Port:** Provide the HTTP Port of the Mobile Camera server.
- **Camera:** Click the "... " button to select a camera. If the Mobile Camera Server is configured not to display the list of devices, enter the name of the device registered with the Mobile Camera Server manually.



- **Password:** If a password was provided when registering the device with the Mobile Camera Server, enter the same password in this field.
- **Video Resolution:** Select the video resolution for streaming.
- **Quality:** Select the compression quality for the stream. Lower quality will use less bandwidth, making it ideal for internet transmissions.

Once the settings have been made, press the **DONE** button to return to the main screen.

On the main screen, press the bottom center button to start streaming video:



The image captured by the mobile device is sent to the Mobile Camera Server.

In the **top-left** corner, you have the option to **turn on the device's flashlight** if supported.  
In the **top right** corner, there is a button to open the settings and details of the video stream.

If you want to stop the video stream, just press the streaming button (red button).

## 19.5 Registering the Camera on the VMS Server

The last step is to register the cameras on the VMS server.

On the recording server, open the camera register and click **Add**. If you have any questions about registering cameras, see the chapter [How to add a camera](#).

1. Enter the **Name** and **Description** that identifies your mobile device.
2. Under Manufacturer, choose **Digifort**.
3. Under Camera model, choose **Mobile Camera Pro**.
4. Under Camera address, choose the **IP** address of your Mobile Camera Server. See [Configuring the Mobile Camera server](#).
5. If you haven't changed it, the default port for communication with the Mobile Camera Server is 8651.
6. Choose a directory for recording.

Now click on **Media Profiles** and double-click on the **Recording** profile:



1. The transmission supported by Mobile Camera Pro is H.264. Select H.264 compression
2. In the Device option, choose the device registered on the Mobile Camera Server that identifies the mobile device you want to register.

Click Preview to see the image being transmitted:

