Digifort Enterprise Manual
Administration Client
Version 7.3.0.0
Rev. A

© 2002 - 2020 by Digifort, all rights reserved

Index

Part I Welcome to Digifort Enterprise Manual 13

1 Screen Shots ... 13
2 For whom this manual is intended ... 13
3 How to use this manual ... 13
4 Prerequisites ... 13

Part II Digifort Services Administrator 16

1 How to execute the Digifort Services Administrator ... 16
2 How to initiate the Digifort Server service ... 17
3 How to stop the Digifort Server service ... 18

Part III Basic functions of the Administration Client 20

1 How to execute the Administration Client ... 20
- Add Server ... 21
- Modify Server ... 21
- Delete Server ... 21
- Disconnect from server ... 21
- About Digifort ... 21
- How to configure the servers to be administrated ... 22

2 How to connect a management server ... 23

Part IV Licensing Digifort 27

1 How to configure the licenses ... 27
- How to add a license ... 29
- How to send data for registration ... 30
- How to install licenses via Online Licenses ... 32
- How to install licenses via license files ... 32
- Enabling a temporary license ... 33

Part V Registering Digifort 36

1 How to register Digifort ... 36
2 Registering Digifort Online ... 38
3 Registering Digifort Offline ... 39

Part VI Recording Server 42

1 How to add a camera ... 42
- Camera ... 43
  - General ... 43
  - Lenses ... 48
  - Motion Detection ... 51
    - Use motion detection via software ... 51

© 2002 - 2020 by Digifort, all rights reserved

Auto desativar detecção de movimento durante o PTZ //OLD: Auto deactivate motion detection during PTZ ... 55
Use motion detection by external notification ... 55
Configuration ... 56
Digifort configuration ... 56
Camera configuration ... 57
Notification type ... 60
Notification of Start and End ... 60
Notificação Instantânea ... 60
Testing the configuration ... 61
Motion end detection interval ... 61
Audio ... 62
Image Filters ... 62
Streaming ... 63
Media profiles ... 63
How the Media Profiles save network bandwidth ... 65
How to add Media Profiles ... 65
How to visualize the functioning of the configured media profile ... 66
Calculator for disk space usage ... 67
Audio ... 71
Recording ... 72
Automatically change recording profile ... 73
Create Bookmark on Profile Change ... 76
Buffer de Snapshot ... 77
Live View ... 77
How to configure the visualization of the camera ... 78
This camera will be accessed by the client via relay server ... 78
Private IP address ... 78
Private IP port ... 78
Public IP address ... 79
Public IP port ... 79
User and Password ... 79
Connection timeout (in MS) ... 79
Media profile ... 79
Selection of camera in the client ... 79
Media profile for access via mobile ... 80
Recording ... 80
Type of recording ... 81
How to configure the scheduling of recording ... 81
Recording Cycle ... 87
How to configure the Image Buffer ... 88
Metadata ... 88
Archiving ... 90
How to configure the archiving ... 90
Edge Recording ... 91
Rights ... 93
Users ... 93
PTZ ... 94
Configurations ... 94
Activate the PTZ control for this camera ... 95
Use the device's PTZ features ... 95
Use the device's COM port for the system to carry out PTZ functions directly ... 95
Select the PTZ protocol ... 96

© 2002 - 2020 by Digifort, all rights reserved

Camera ID (RS-485) ... 96
COM port of video server ... 96
Use of PTZ ... 96
PTZ Lock ... 96
Agendamento de Operação ... 97
Presets ... 98
How to configure the Presets Control ... 98
How to create a preset ... 100
PTZ Patrol ... 101
How to configure PTZ Patrol ... 101
How to add a PTZ Patrol scheme ... 103
How to configure the scheduling of PTZ Patrol schemes ... 104
Auxiliary ... 105
Joystick ... 106
How to configure the Joystick ... 106
Menu Control ... 108
How to remotely configure analogical cameras ... 108
Visual joystick ... 109
I/O ... 110
How to add input events ... 110
How to add output events ... 113
How to configure the scheduling of events ... 115
Virtual I/O ... 116
Events ... 119
Communication ... 120
Communication failure event ... 120
Connection restoration event ... 121
Devices failure report ... 121
Recording failure ... 121
Motion Detection ... 122
How to configure the motion detection event ... 123
Audio detection ... 123
Manual Events ... 124
Device Events ... 126
Event Variables ... 127
Privacy ... 130
Privacy mode ... 130
Privacy Mask ... 132
Advanced ... 134
Object links ... 134
Advanced Camera Settings ... 139
Operational Map ... 142
How to configure the alarm actions ... 143
Send an e-mail message to a group of persons in the case of an alarm ... 145
Display camera images in the screen of the operator ... 147
Sound an alarm in the Surveillance Client ... 148
Display camera snapshots on the operator's screen at the time of the event ... 149
Send Audio Clip ... 150
Send instant message to the operator of the computer ... 151
Request written confirmation from users ... 152
Activate camera presets ... 153
Activate action scripts of alarm outputs ... 153
Enable or disable system objects ... 154

© 2002 - 2020 by Digifort, all rights reserved

Create Bookmark ... 155
Download device recordings with edge recording support ... 157
Send a HTTP Request ... 158
Create timer events ... 160
Camera management functions ... 161
Activate camera ... 162
Disactivate camera ... 162
Duplicate camera ... 162
Recording scheduling ... 162
Events scheduling ... 163
Alarm buffer ... 163
Snapshot Buffer ... 163
Connection ... 163
Events ... 163
Configuração PTZ em massa ... 163
Disk limit ... 164
Type of recording ... 164
Edge Recording ... 165
Metadata Recording ... 165
Motion Detection ... 165
Privacy Mode ... 165
Relay ... 165
Multiple Camera Recording Directory Change ... 165
Media Profiles ... 166
Media Profiles ... 166
Motion detection media profile ... 167
Mobile viewing media profile ... 168
Viewing media profile ... 168
Recording media profile ... 168
Grant Rights ... 168
Deny Rights ... 168
Delete Cameras ... 168
Locating and registering cameras automatically ... 169
Registration of one device only ... 172
Registration of various devices ... 172
Importar objetos de outros servidores ... 174
Multichannel device registration ... 175
Registering a DVR ... 176
2 Camera Groups ... 180
3 Column Organization ... 184
4 Exporting Data from the Recording Server ... 185
5 Monitoring recording server status ... 186
Monitorando o status de câmeras individualmente ... 188
Conexão de Gravação ... 188
Conexões ... 189
Portas de Entrada ... 190
Agendamentos ... 191
Gravação em Borda ... 192
Disco ... 192
Exportação de dados na tela de Status ... 193
6 Edge Recording ... 194

© 2002 - 2020 by Digifort, all rights reserved

Part VII Alarm Devices 198

1 How to access the alarm devices register ... 198

How to add an alarm device ... 199

Main data ... 199

I/O Control ... 201

Events ... 201

Scheduling ... 202

Management functions of the Alarm Devices ... 203

2 Status ... 204

3 I/O Driver for PING ... 205

Part VIII Alerts and Events 209

1 How to access the Alerts and Events ... 209

How to configure the contacts ... 209

How to add a contact ... 211

How to configure the contact groups ... 212

How to add a contact group ... 213

Global Events ... 213

How to access the Global Events Register ... 214

How to add a global event ... 215

Main data ... 216

Rights ... 216

Sheduled Events ... 218

Registering Sheduled Event ... 218

Adding Sheduled Event ... 219

Types of Scheduling ... 220

Only once ... 221

Daily ... 222

Weekly ... 222

Monthly ... 223

Part IX User administration 226

1 Administrating users ... 226

Monitoring user activity ... 227

2 Adding, modifying and excluding users ... 228

User data ... 229

Force use of Strong Password ... 231

Weak Password Alert ... 232

2-Factor Authentication ... 232

Login IPs ... 233

Adding a range of access IPs ... 234

Login hours ... 235

Biopass ... 235

User rights ... 235

Video Search and Playback ... 236

Live Audio ... 236

Surveillance Views ... 237

System Cameras ... 237

Alarm Devices ... 237

Alarms ... 237

© 2002 - 2020 by Digifort, all rights reserved

Virtual Matrix ... 237
System Users ... 237
Alerts and Events ... 238
Global Events ... 238
Scheduled Events ... 238
Maps ... 238
Operational Maps ... 238
Analytics ... 238
Plate Recognition ... 238
Web Pages ... 239
Screen styles ... 239
Server ... 239
Report Authentication ... 239
Bookmark ... 239
Record Protection ... 239
Surveillance Client Features ... 240
Centralized Surveillance Client Configuration ... 240
Policies ... 244
Property ID ... 245
Web personalization ... 246
Water mark ... 247
Groups Inquiry ... 247
Rights Inquiry ... 248
User general observations field ... 248
3 User administration functions ... 249
Reset password ... 250
Login IPs ... 250
Login options ... 250
Block account ... 251
Unblock account ... 251
Account Type ... 251
Account expiration ... 251
Rights ... 251
Give rights ... 251
Deny rights ... 251
Features ... 251
Policies ... 251
Web customization ... 251
4 Adding, altering and excluding Groups ... 252
Group rights ... 255
Surveillance Client Features ... 255
PTZ ... 256
Rights Inquiry ... 256
5 Integration with the Active Directory ... 256
Part X Screenstyle Administration 261
1 How to access the screenstyle administration ... 261
How to add a screenstyle ... 262
Part XI BioPass 266
1 How to install BioPass on your computer ... 266

© 2002 - 2020 by Digifort, all rights reserved

2 How to configure the BioPass ... 266

Part XII Maps 276

1 Registration of Maps ... 276

Adding Images ... 278
Google Maps integration ... 279
Adding Texts ... 286
Adding Cameras ... 286
Field of View of Cameras ... 288
Adding Functions to the Alarm Board ... 291
Monitoring global and manual events ... 294
Status de objetos ... 295
Monitoring ... 296
Map Links ... 296
Check invalid objects on maps ... 298
Maps / Alignment grid ... 299
Operational Map Icon ... 300

Part XIII Operational Map 303

Part XIV Analytics 309

1 Licensing the Digifort Analytics ... 309

Understanding the distributed processing ... 310
How to start the Analytics Server ... 312
Analytics server status ... 312
How to configure the servers to be managed ... 313
How to connect a management server ... 315
How to configure the analytics licenses ... 316

2 Analytics Server Configurations ... 318

Adding an analytics configuration ... 320
How to configure the Basic Analytics ... 326
How to configure the Foreign Objects module ... 330
How to configure the Missing Objects module ... 332
How to configure the Face Detection module ... 334
How to configure the Advanced Analytics ... 335
How to calibrate the analytics ... 340
How to classify objects ... 344
How to configure the Analytics' Rules ... 346
How to configure the Presence rule ... 346
How to configure the Entry rule ... 347
How to configure the Exit rule ... 348
How to configure the Appear rule ... 349
How to configure the Disappear rule ... 350
How to configure the Direction Filter rule ... 351
How to configure the Speed Filter rule ... 353
How to configure the rule of Tailgating ... 354
How to configure the Stopped rule ... 355
How to configure the Loitering rule ... 356
How to configure the rule of abandoned objects ... 357
How to configure the rule removed objects ... 359
How to configure the rule counting line ... 361
How to configure the counters ... 363

© 2002 - 2020 by Digifort, all rights reserved

How to configure the Camera Tampering ... 368
The Analytics Advanced Options ... 369

Part XV License Plate Recognition 373

1 How to create a License Plate Recognition Server ... 373
How to configure your LPR server ... 374
Status do Servidor de LPR ... 376
Monitoring ... 377
2 Licensing the LPR ... 378
How to license the LPR Server ... 379
How to license the Carmen engine ... 382
How to license the Neuro Labs Engine ... 383
3 How to configure the License Plate recognition ... 383
Configuring Carmen Engine / Neuro Labs / OpenALPR ... 390
Plates ... 393
Record Expiration ... 396
Verifying the LPR Status ... 397
Configuring the LPR lists ... 401
Masks ... 404
Importing plates with lists ... 406
Events ... 406
Conditions for Triggering Events ... 410
Evento de Falha e Restauração ... 411
Plate category groups ... 412

Part XVI Páginas Web 415

Part XVII Configurations 419

1 Global Configurations ... 419
General Configurations ... 419
Recordings ... 420
Record protection ... 421
Recording encryption ... 421
Master / Slave ... 421
Sharing Plate Data between Master/Slave ... 422
Multicast ... 422
Backup ... 424
Restoring backups of Digifort ... 425
Database ... 426
STMP Configurations ... 427
Disk Limits ... 428
Network Units ... 429
How to add a network unit ... 430
SNMP ... 432
2 Server health monitoring event ... 433
3 Failover ... 433
Failover - Multiple servers ... 440
4 IP Filters ... 441
How to access IP Filters ... 441
How to add authorized IPs ... 443
How to add unauthorized IPs ... 443

© 2002 - 2020 by Digifort, all rights reserved

5 Report authentication ... 444

Part XVIII Server Information 448

1 Disk Usage ... 449
2 Master / Slave ... 450
3 Failover ... 450
4 Monitoring by graphics ... 451

Part XIX Web Server 453

1 How to access the configurations of the Web Server ... 453

Part XX Servidor RTSP 455

1 Status ... 455
2 Configurations ... 457

Part XXI System Logs 459

1 How to access the system logs ... 459
2 How to visualize the event logs ... 461
3 How to configure the event logs ... 462
Activate system logs ... 464
Delete logs older than X days ... 464
Event log options ... 464
Failure in communication with the devices ... 464
Alarm inputs ... 465
Failure in recording ... 465
Motion detection ... 465
Manual events ... 465
Timer events ... 465
Programmed events ... 465
Global events ... 465
Eventos de analítico ... 465
LPR events ... 465
Save Configurations button ... 465
How to visualize the event logs ... 465
4 Audit ... 466
How to access Audit ... 466
Viewing the Logs ... 467

Part XXII Automatic Client update 469

Part XXIII Maintaining the Database 473

1 Backup ... 473
2 Restore ... 474
3 Maintenance ... 474

Part XXIV Digifort Mobile Camera 477

© 2002 - 2020 by Digifort, all rights reserved

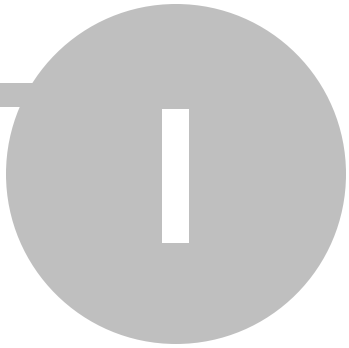
1 Registering the Mobile Camera Server ... 477
2 Configuring the Mobile Camera Server ... 479
Configurations ... 479
Status ... 480
Mobile devices ... 482
3 Configuring the application ... 484
4 Registering the camera ... 489

Part XXV Centralized server list 494

Index 0

© 2002 - 2020 by Digifort, all rights reserved

Chapter



1 Welcome to Digifort Enterprise Manual



This User Manual and Technical References provides all of the information needed to effectively implement and use all of the basic and advanced features found in the Digifort EnterpriseSystem Administration Client.
This manual is constantly updated and does not include the features for Digifort's Beta versions. Information about the use of audio will be included in the next version of this manual.

1.1 Screen Shots

The screen shots contained in this manual may not be identical to the interface that you will see using the Software. Some differences may appear, with no impairment in use of this manual. This is due to the fact that frequent updates and the inclusion of new features are carried out with the purpose of continuous improvement of the system.

1.2 For whom this manual is intended

This manual is directed toward Digifort System administrators who are responsible for the complete configuration of the Digifort Server.

1.3 How to use this manual

This manual is structured into chapters, topics and sub-topics.

Important:

- If your version is not the Enterprise, some features may present limitations. To know the limitations of your version check the Feature Matrix table on the www.digifort.com site.
- The screenshots in this manual are originally taken from the Enterprise version. For this reason, some features may present differences in the screenshot from the version you are using. We are constantly updating this manual and improving its content.

1.4 Prerequisites

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

© 2002 - 2020 by Digifort, all rights reserved

- Use of computers and their peripherals equipment.
- Use of the Microsoft Windows operating system.
- Knowledge of client-server architecture.
- Knowledge of computer network architecture.

© 2002 - 2020 by Digifort, all rights reserved

Chapter



2 Digifort Services Administrator

The Digifort System is a software developed around the client-server platform, making use of all the features and benefits that this platform offers.

In the client-server platform, all of the information is stored in the central server responsible for its administration. In the case of the Digifort System, the server is the component responsible for (among other functions) maintaining the recordings generated by the images supplied by cameras, administrating disk space, alerting the operators and administrators about system abnormalities and making information available to the clients.

The Digifort Server is an application that runs as a Windows system service, therefore, it is executed automatically when Windows is initiated, without need for user intervention.

The Services Administrator is the software responsible for the control of its execution, displaying information about the state of working and offering service installation and initialization controls.

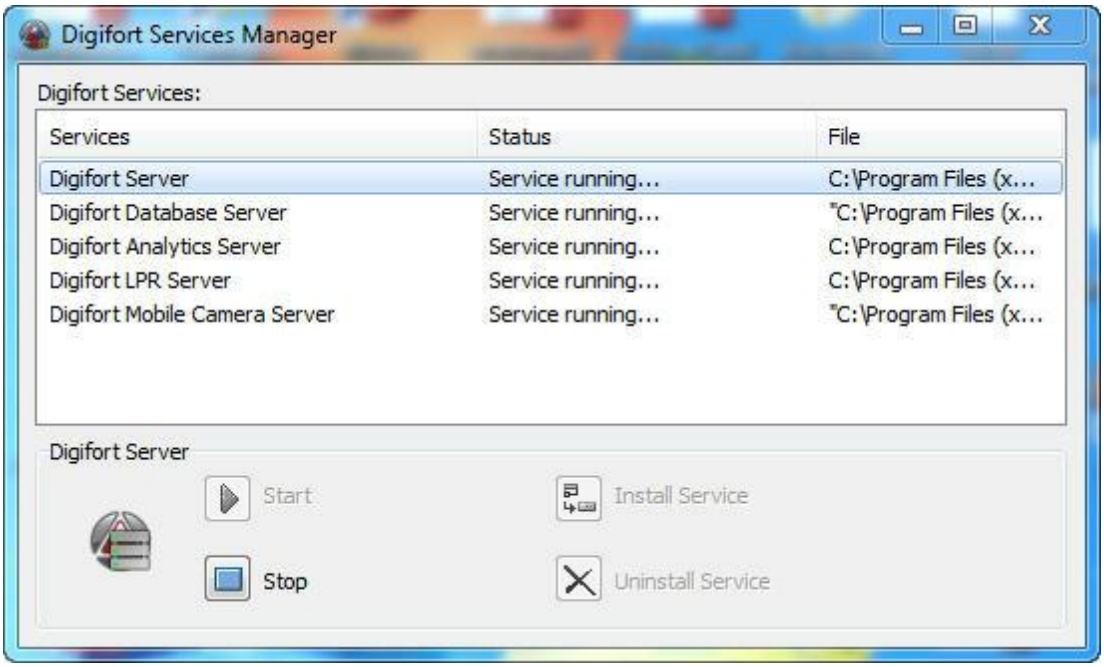
Note

As this is a Windows service, Digifort enables you to use its various features, such as the Active directory, the Explorer file management system (DHCP, UpnP), TCP/IP communication systems, video control systems, etc

2.1 How to execute the Digifort Services Administrator

To execute the Services Administrator, locate the Digifort Enterprise 7.3.0.0 Server icon on your Desktop, or, in Start->Programs->Digifort Enterprise 7.3.0.0 ->Server->Server and execute it. The Services Administrator will be started opening the screen shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



The Services Administrator offers the following functions:

- **Digifort Services:** Displays the list of available services that can be manipulated.
- **Initiate:** Initiates the selected service. Available only if the service is installed and stopped.
- **Stop:** Stops the selected service. Available only if the service is installed and initiated.
- **Install Service:** Installs the selected service. Available only if the service is not installed.
- **Uninstall Service**: Uninstalls the selected service. Available only if the service is installed and stopped

For the operation of the following services must be Digifort in operation:
Digifort Server responsible for managing the recording and communicating with customers.
Digifort Database Server responsible for managing Digifort database.

The **"Digifort Analytics Server"** must be running in a network device so that video analysis modules can run. (Standard, Professional e Enterprise)
The **"Digifort LPR Server"** must be running in a network device so that LPR modules can run. (Standard, Professional e Enterprise)

The **"Digifort Mobile Camera Server"** must be running so that the Digifort Mobile Camera module can run.

2.2 How to initiate the Digifort Server service

To initiate the Digifort Server service, first it must be installed. Carry out the following steps to correctly initiate the service:

1. Select the service “Digifort Server”

2. Click on **Install Service**, a confirmation screen will be shown, informing that the service was successfully installed.

© 2002 - 2020 by Digifort, all rights reserved

3. Click on **Initiate** and wait while the server is initiated. The process of initialization terminates when the message “Service functioning...” appears on the status bar.

Note

If the server was stopped for some reason and initiated again, the initialization process can be slow, since a check-out has to be carried out in all of the existing recordings, creating a disk structure map.

2.3 How to stop the Digifort Server service

At any moment, the execution of the Digifort Server service can be interrupted. When this is done, the server will no longer execute any function such as, for example, the administration of alarms and recording of the cameras.

The process of stopping the Digifort Server is quite simple, just clicking on the Stop button. When the service is successfully stopped, the “Service stopped...” should appear on the status bar.

© 2002 - 2020 by Digifort, all rights reserved

Chapter



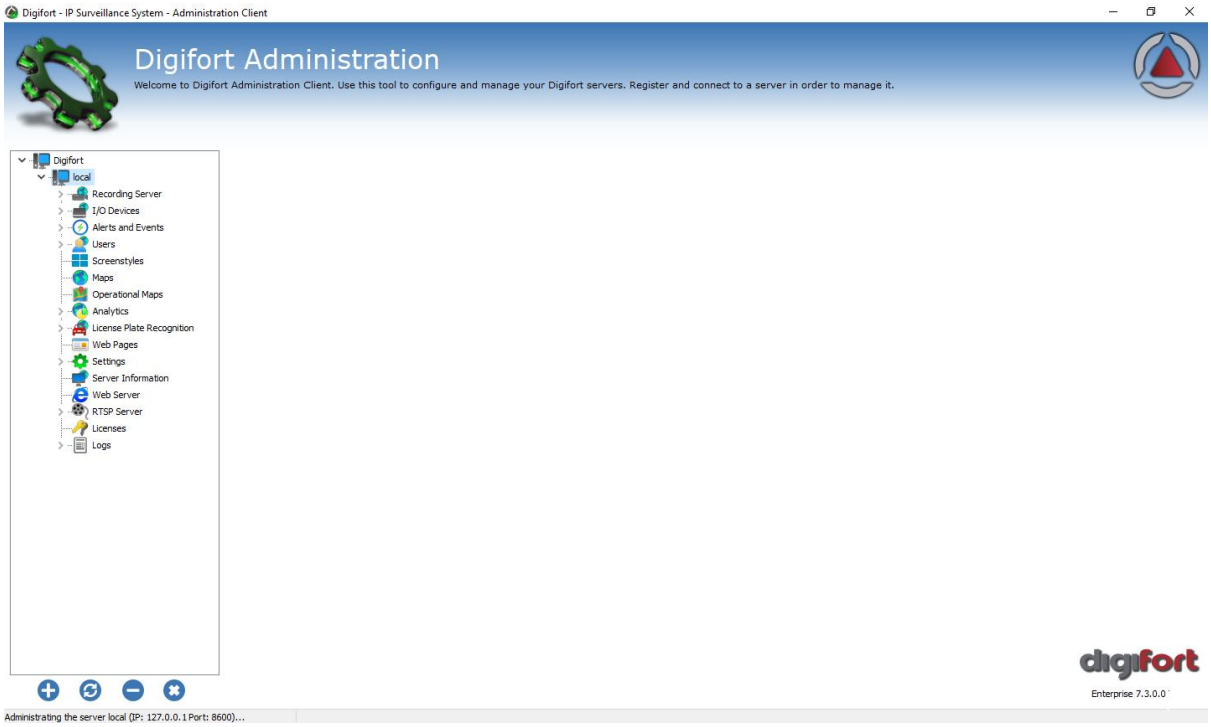
3 Basic functions of the Administration Client

The Administration Client is the system module of Digifort that is responsible for the server configuration. In this module you will be able, among other things, to register the cameras, set alarms, check the status of the server and set the users who will have access to the system.

The Administration Client can manage unlimited servers simultaneously, simply by registering the desired servers. There is no limit to the number of customers and the number of cameras to be monitored, depending only on the storage capacity and server processing.

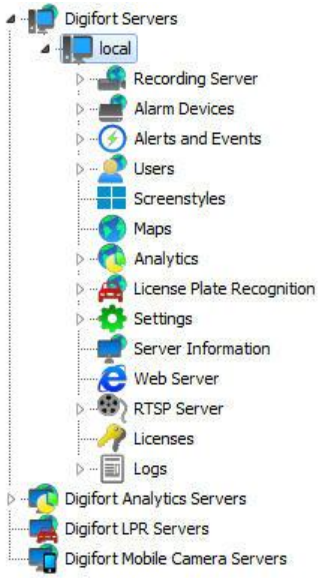
3.1 How to execute the Administration Client

To access the Administration client, locate the icon Digifort Enterprise 7.3.0.0 administration client on your Desktop or on
Start Menu->Programs->Digifort->Administration Client and run it. The Administration Client will start as shown in the figure below:



The Administration Client offers the following initial configurations:

© 2002 - 2020 by Digifort, all rights reserved



Configurations Menu: This menu displays the configurations available for the selected server. The configurations are shown in tree format that is, with items and sub-items. To access some server configuration, click on the desired menu. The configurations related to the selected item will be displayed in the reserved area at the right of the item.

3.1.1 Add Server



Add Server: Starts the inclusion of a server. Use this button to add servers that are administered by the Administration Client. To learn how to include servers see How to configure the servers to be administrated

3.1.2 Modify Server



Modify Server: With the server selected, this option shows the server settings configuration.

3.1.3 Delete Server



Delete Server: Delete selected server.

3.1.4 Disconnect from server



Disconnect from server: Terminates the connection and administration of the selected server. To disconnect from a server, select it in the Configurations Menu and click on this button

3.1.5 About Digifort



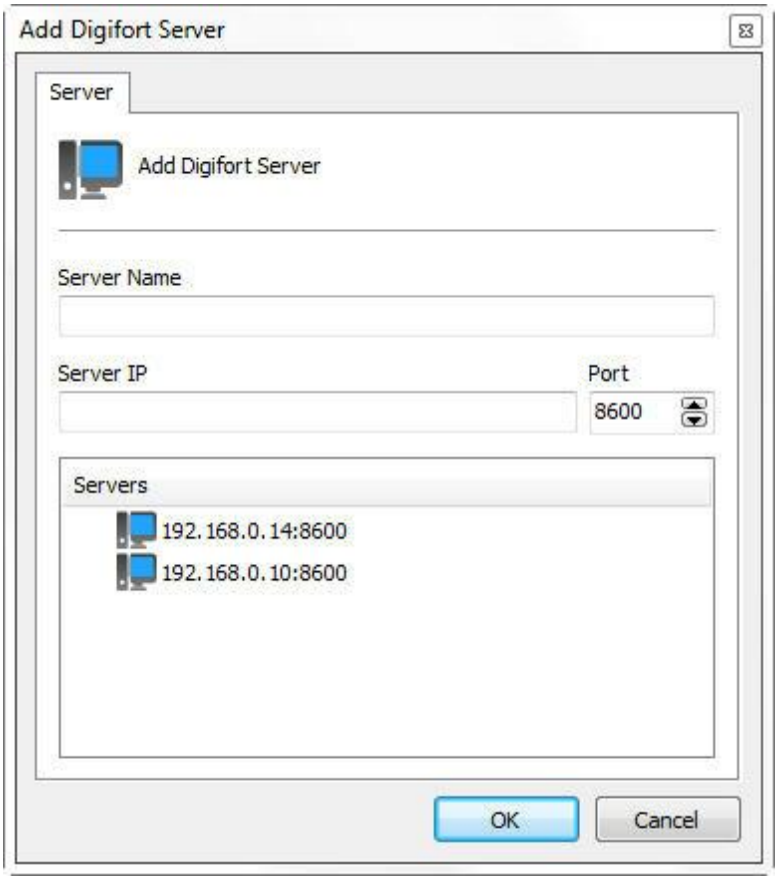
About: Show information about current Digifort version.

© 2002 - 2020 by Digifort, all rights reserved

3.1.6 How to configure the servers to be administrated

The first step to be done in the configuration of a server is to add it to the list of servers to be administrated by the Administration Client.

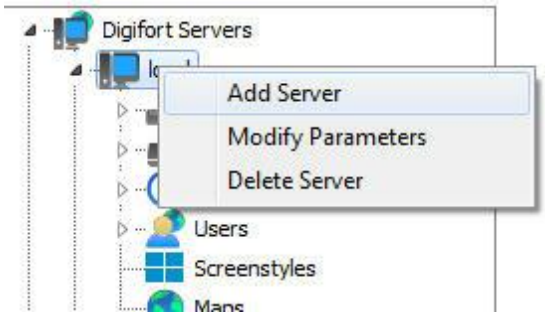
To add a server, click on the **Add** Server button, opening the server registration screen, as shown in the picture below



- **Server Name**: Enter the name of the server to be added. After confirmation of the data, the name of the server cannot be changed..
- **Server IP:** Enter the IP of the server to be administrated.
- **Port:** Enter the communication port of the server. As a standard, the port is 8600. The communication port of the server cannot be changed, this configuration should only be changed if accessing the server located in remote places, for example, Internet.
- **Servers**: This list will contain all of the Digifort servers that the Administration Client found in the network. Upon clicking on one of the servers, the IP and Port fields (described above) will be filled in automatically, leaving only the Server Name field to be entered to complete the registration.

After correctly informing all data, click **OK**.
After inclusion of the server, it will be displayed in the Configuration Menu as shown in the picture below

© 2002 - 2020 by Digifort, all rights reserved



To change the parameters of a server already saved, click on the right button over the desired server and then click on Modify Parameters. In the screen that opens, modify the data as necessary and click on **OK**.

To exclude a server, click on the right button over the desired server and then click on Exclude Server. Click on Yes on the confirmation message that appears.

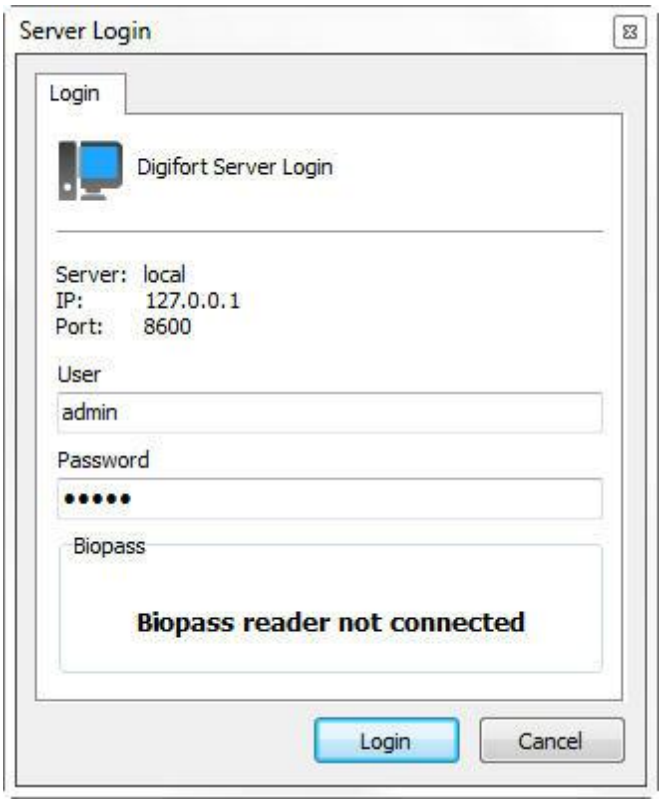
Tip: If the Digifort Server is being executed on the same computer as the Administration Client, the Loopback IP, identified by 127.0.0.1 may be informed.

Tip
If the Digifort Server is being executed on the same computer as the Administration Client, the Loopback IP, identified by 127.0.0.1 may be informed.

3.2 How to connect a management server

After adding the server, locate in it in the Configurations Menu and double-click on it. Once this is done, you will be asked to provide a username and password to access the server configurations as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

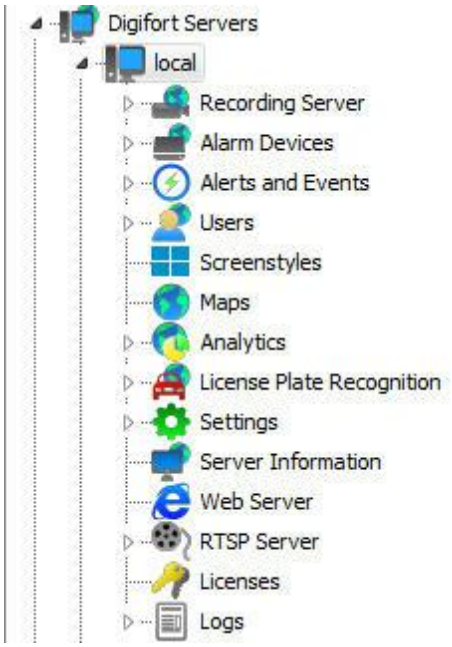


- Username**:** Access username.
- Password**:** Password for access.

Enter your username and password to access the server. If this is the first time you are accessing the system, insert the same username as the admin and leave the password blank.

Once you have filled in the access information, click on OK. If the authentication for access is successful, the Configurations Menu opens showing the configurations available for the server, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



Note

The admin user is the only user that cannot be removed from the system and has every right of access. For security purposes, a password must be given to stop unauthorized people accessing the system.

© 2002 - 2020 by Digifort, all rights reserved

Chapter IV

4 Licensing Digifort

To unlock the system and some features, it is necessary to perform the licensing of the software.

There are many types of licenses and license packages. For more information, contact your resale.

The licenses only work on the server for which the registration request was made. This is because each server generates a different password and the licenses are generated based on this password, making them unique.

There are two licensing methods for Digifort - the licensing performed via the internet and the one via license files.
The licensing performed via the internet is the safest and recommended, but if your server does not feature internet access, use the licensing via license files.

Tip

As Digifort works on the Client-Server platform, the registration request does not have to be made by the server itself, i.e., any other computer on the network can perform this request via the Administration Client.

Important

If the recording server is formatted, a new password is generated by the server. Thus, a new registration request must be made

4.1 How to configure the licenses

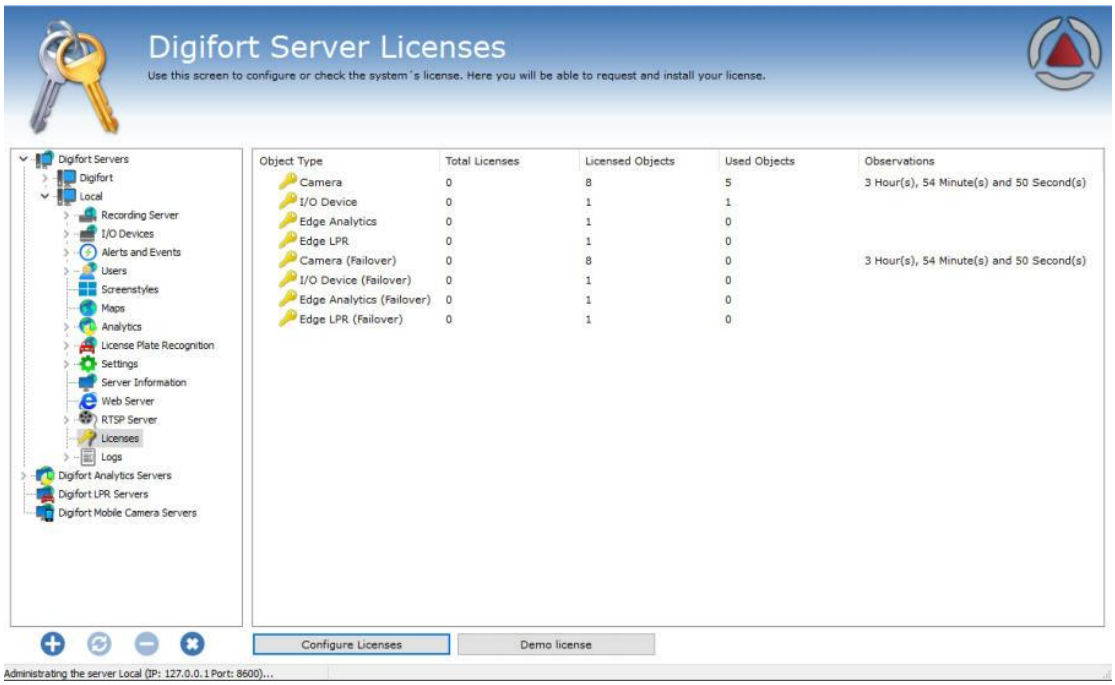
Before you start your server, check if the Hardkey that is sold together with the software is correctly connected to your machine.

To begin licensing Digifort, after logging into the server, locate the Licenses item in the **Server's Settings Menu**, as shown in figure below:



Once this is done, information on the present status of Digifort licensing will be displayed on the right side, as illustrated in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



From this screen, it is possible to retrieve the following information:

- **Total licenses**: Number of licenses installed on the server of a particular type of object.
- **Licensed objects**: Number of licensed objects for the type of object.
- **Used Objects:** How many objects are using the licenses at this time.

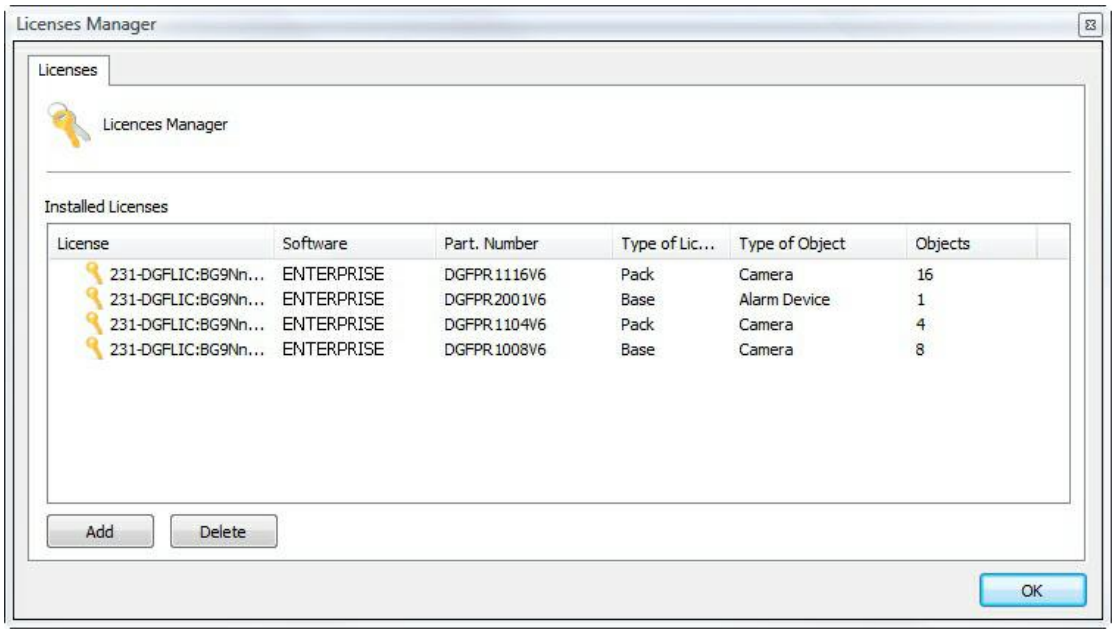
Types of licenses:

- **Camera**: License to release camera recording.
- **I/O Device:** License for the use of I/O boards.
- **Edge Analytics**: License to use bundled analytics.
- **Edge LPR**: License to use bundled LPR.
- **Camera Failover**: Allows the use of the Failover feature for a given number of cameras.
- **I/O Devices (Failover**): Allows the use of the Failover feature for a given number of I/O devices.
- **Edge Analytics (Failover**): Allows the use of the Failover feature for a given number of edge analytics.
- **Edge LPR (Failover**): Allows the use of the Failover feature for a given number of edge LPR.

To learn more about licensing, see your dealer.

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

© 2002 - 2020 by Digifort, all rights reserved



In this screen, all licenses installed on the server are displayed. 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 settings, click on the **OK** button to close this screen.

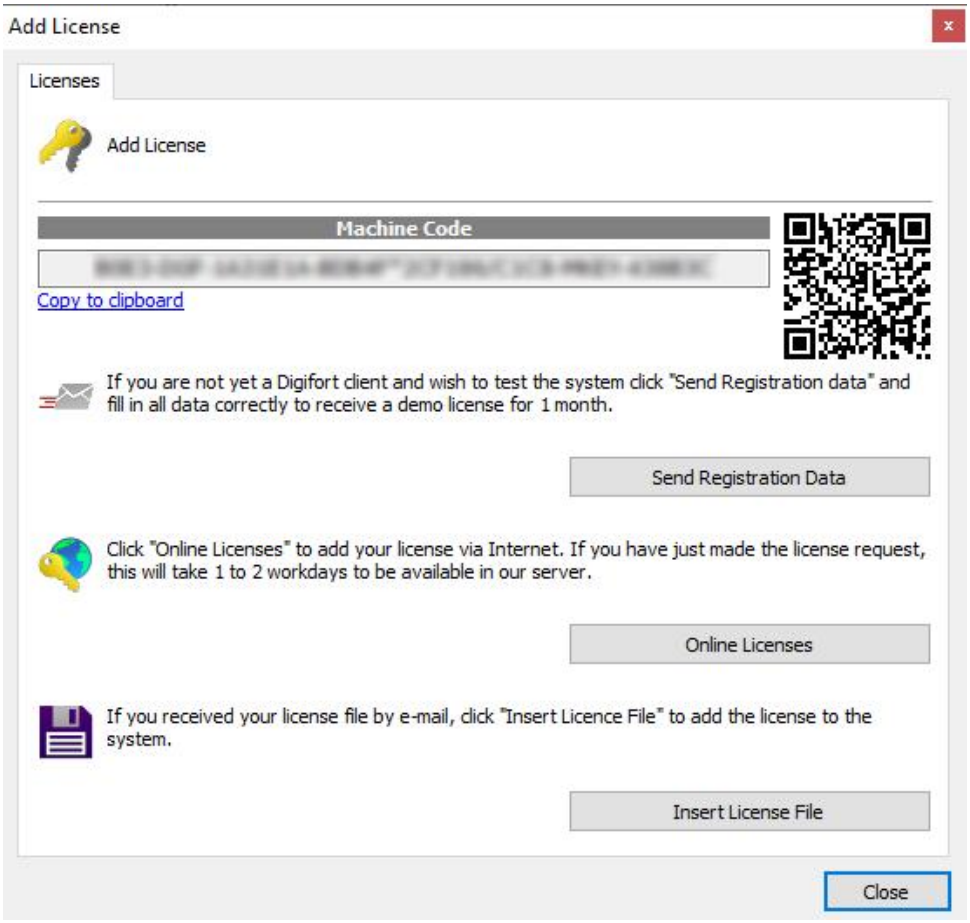
Note

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:

© 2002 - 2020 by Digifort, all rights reserved



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

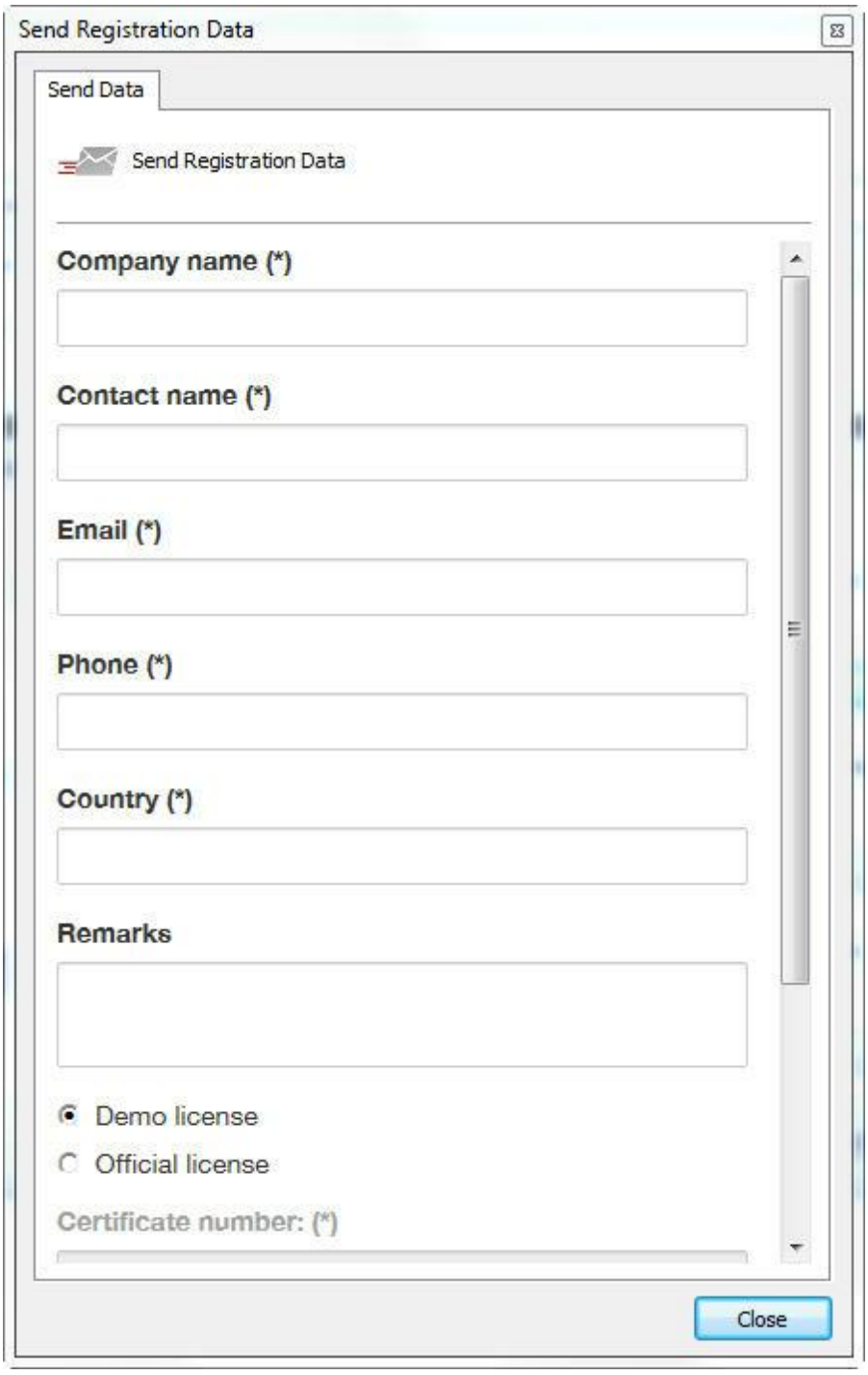
4.1.2 How to send data for registration

The first phase in licensing Digifort is the sending of data for registration. This process consists of filling out the user's data which will be sent together with the counter password of the server to the Licensing Center.

With this data at hand, the Licensing Center will generate the requested licenses and a confirmation will be sent to the supplied e-mail address.

To start the process of sending registration data, click on **Send data for Registration**. This action will open a form to be filled out with the client's data, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



After correctly filling in the fields, click on the **Send** button. Your license will be generated in at most two weekdays. When your license is finished, you will receive a confirmation letter by e-mail with all of the instructions for installing the license.

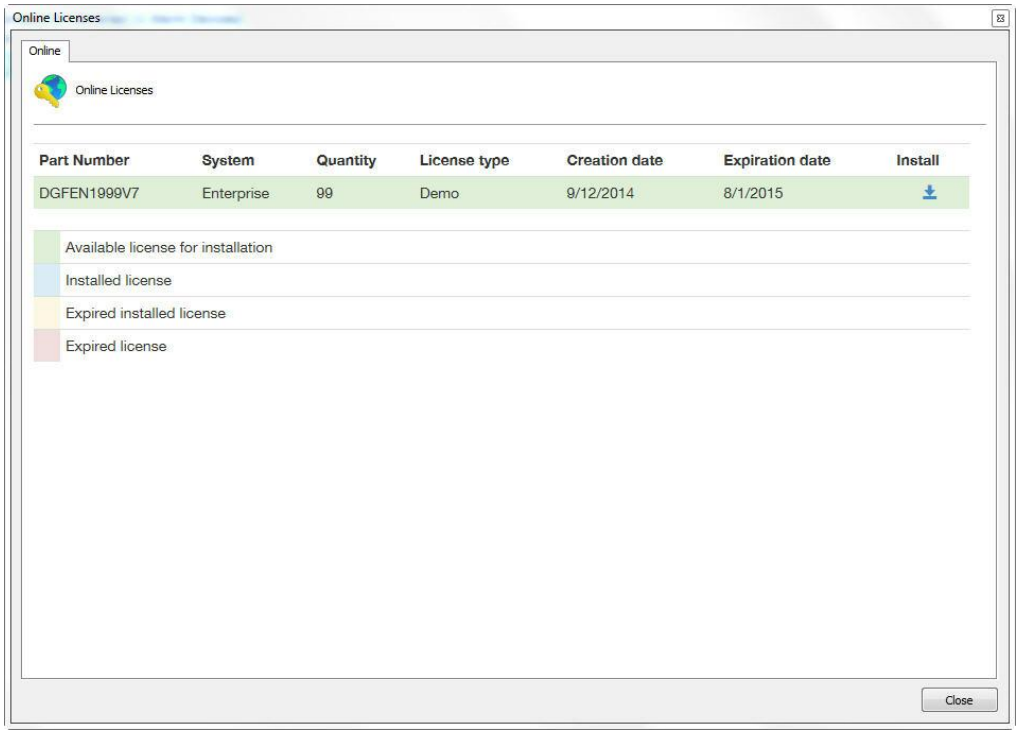
These instructions are also described in the following pages of this manual.

© 2002 - 2020 by Digifort, all rights reserved

4.1.3 How to install licenses via Online Licenses

Licensing via Online Licenses is the safest and most practical way to license Digifort.

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



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

After installation of the licenses, click on the **Close** button.

4.1.4 How to install licenses via license files

In case your server has no access to Internet, you must use licensing via license files. To carry out this process, copy the counter password of your server and send it via e-mail to Digifort. Your license will be generated using this counter password. Soon afterwards, the license files will be sent to your e-mail address.

To install the license files in the Digifort Server, copy them to the server or to some network unit that it has access to and click on Insert License File. A window should open requesting the location of the license files.
Locate the files and open first the base license file and afterwards all of the pack license

© 2002 - 2020 by Digifort, all rights reserved

files.

Observation

Some errors can occur using this licensing method. This is due to the fact that the licensing process is being carried out by means outside of the realm of Digifort. The most common errors are: sending of an incorrect counter password and corruption of the license files sent by e-mail. For this reason, try to use the Online Licensing method.

4.1.5 Enabling a temporary license

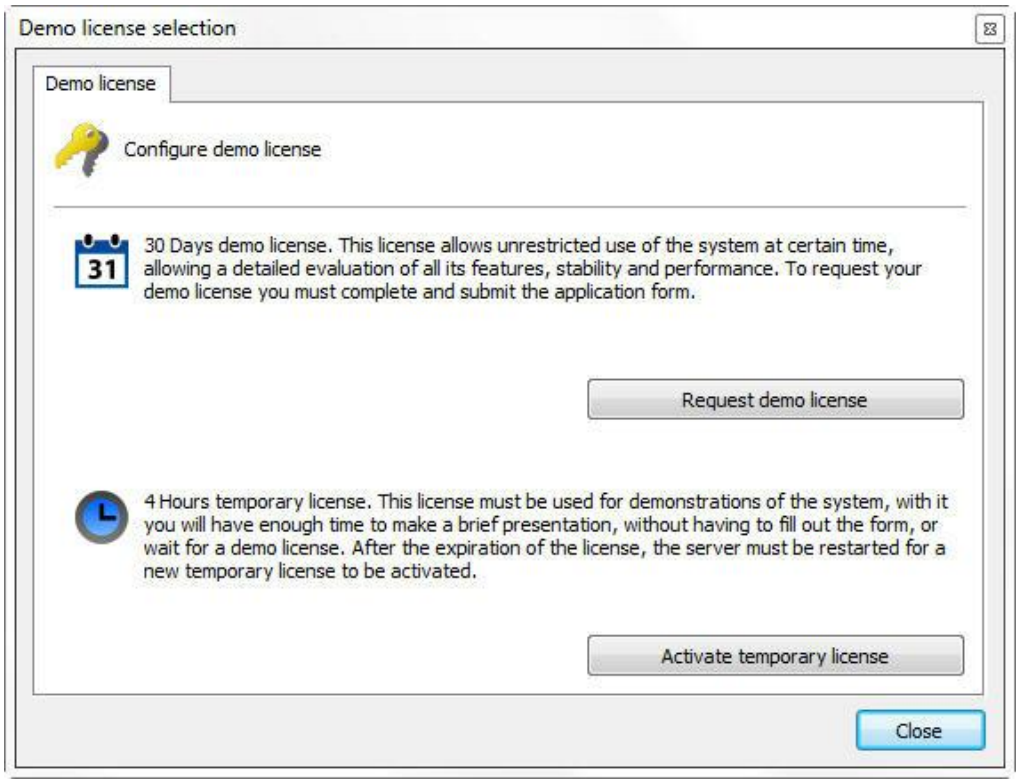
The temporary license feature was created to enable the software demo. Once the temporary license is activated, the software will work for two hours.

To activate the temporary license click on the Demo License button as shown in the Picture below:

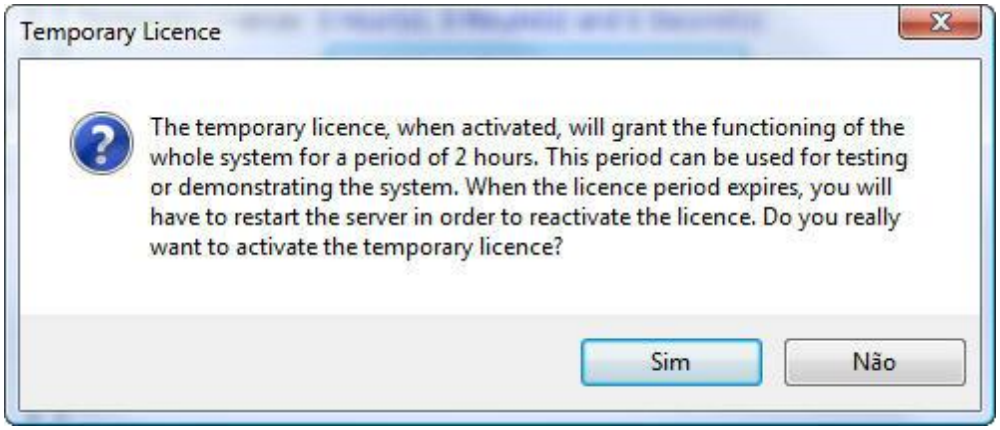


Then click on Activate temporary license as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



You will see the window shown below; click on yes to install the license.



© 2002 - 2020 by Digifort, all rights reserved

Chapter V

5 Registering Digifort

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

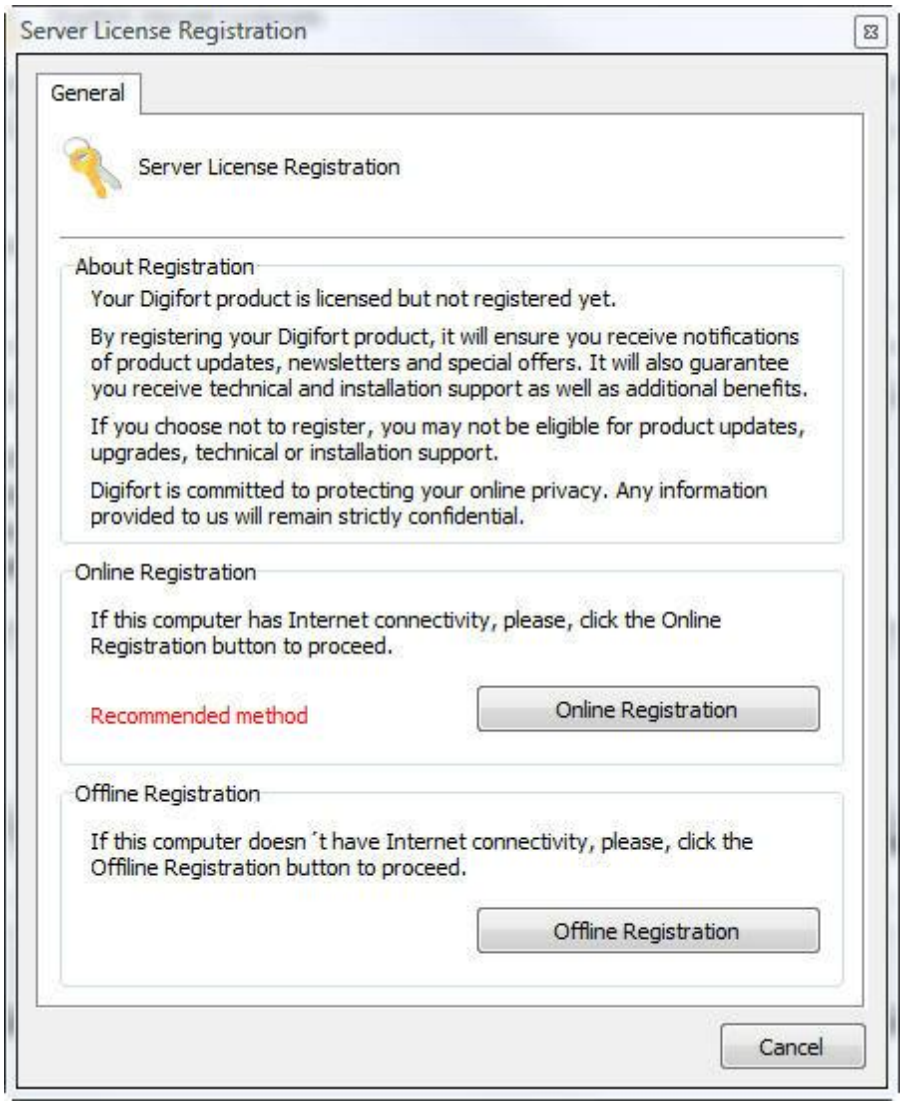
If you decide not to register, you will not be eligible for updates, upgrades, technical support or installation support.

Registering Digifort, you will receive a registration code which, for security reasons, will also be stored in our licensing center. If you use a hard key and it becomes necessary to format the Server or reinstall Digifort, out licensing Center will identify your server and will automatically register it again.

5.1 How to register Digifort

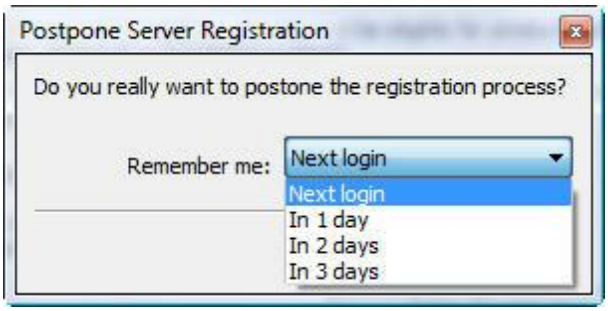
After inserting your usage license, the software's registration window will automatically be displayed, as shown in the figure below. To understand how to install licenses in Digifort, see Licensing Digifort.

© 2002 - 2020 by Digifort, all rights reserved



Registration of Digifort can be done in two ways, Online and Offline. The Online method is recommended, but can be used only when the computer which is executing the Administration Client is connected to Internet. The Offline method must be used when the computer has no access to Internet.

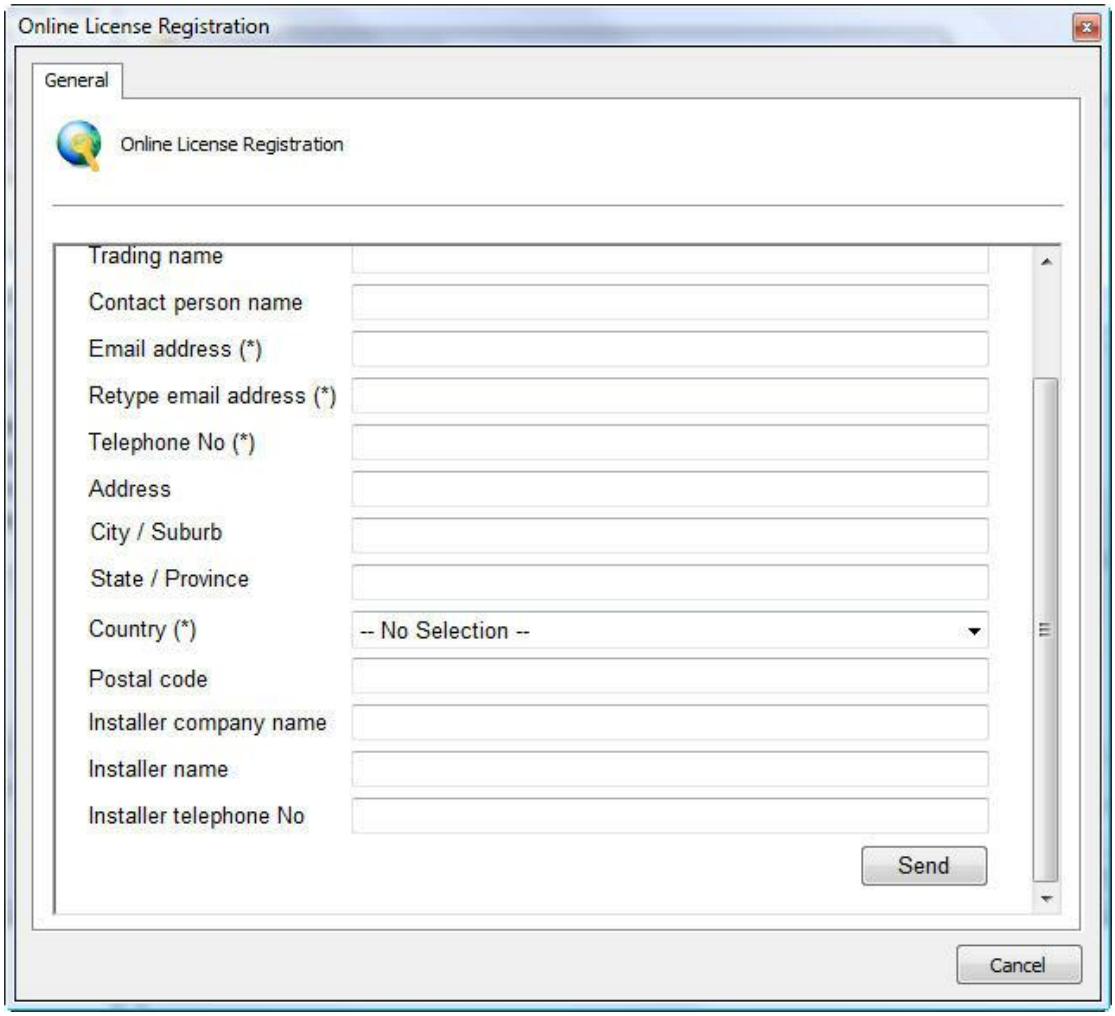
If you wish to register later, close this window and select the desired option, as shown below:



© 2002 - 2020 by Digifort, all rights reserved

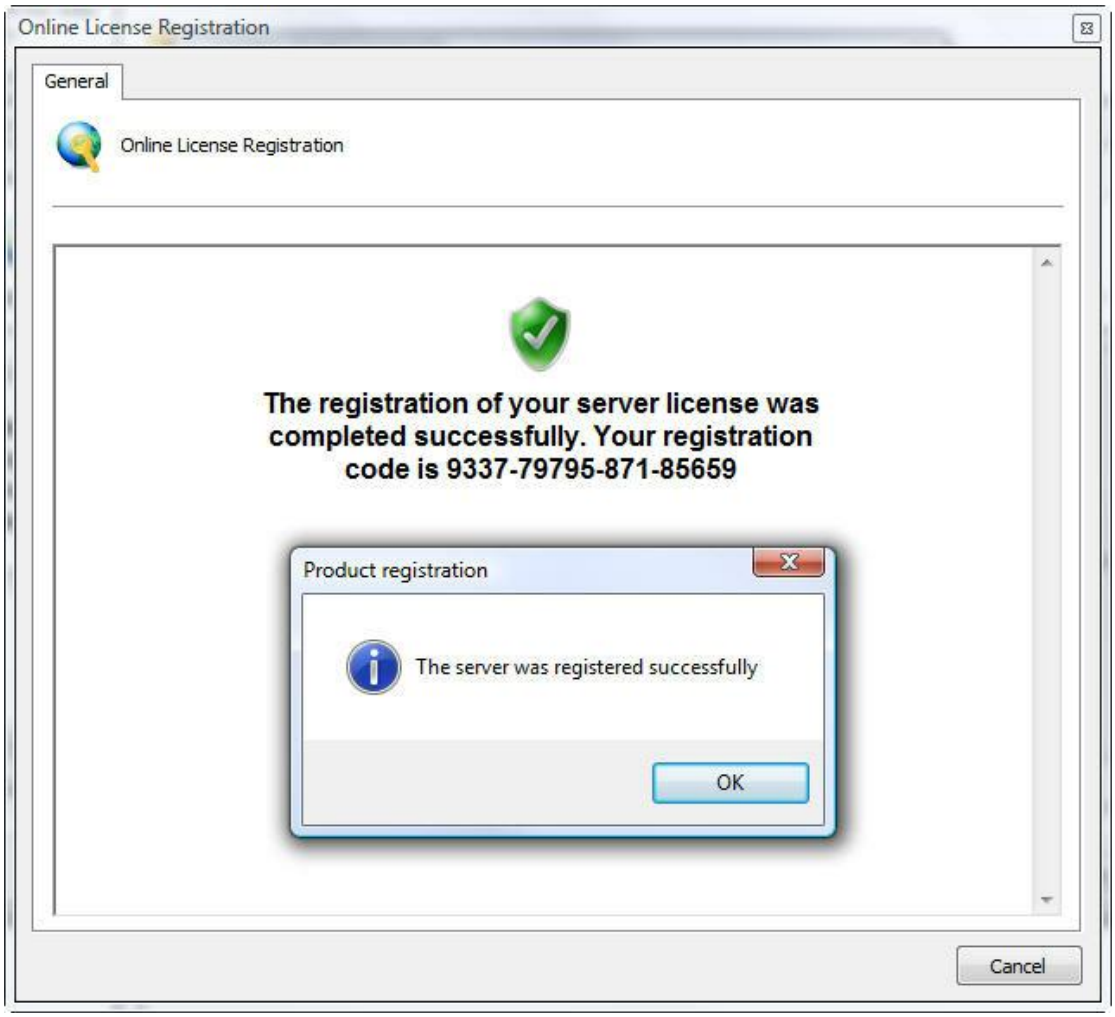
5.2 Registering Digifort Online

To register Digifort online, click on the Register Online Button. A screen will be displayed with the form to be filled out, as shown in the figure below:



Fill in all of the fields and click on Send. A registration confirmation screen will be displayed, together with your registration code, as shown in the figure below

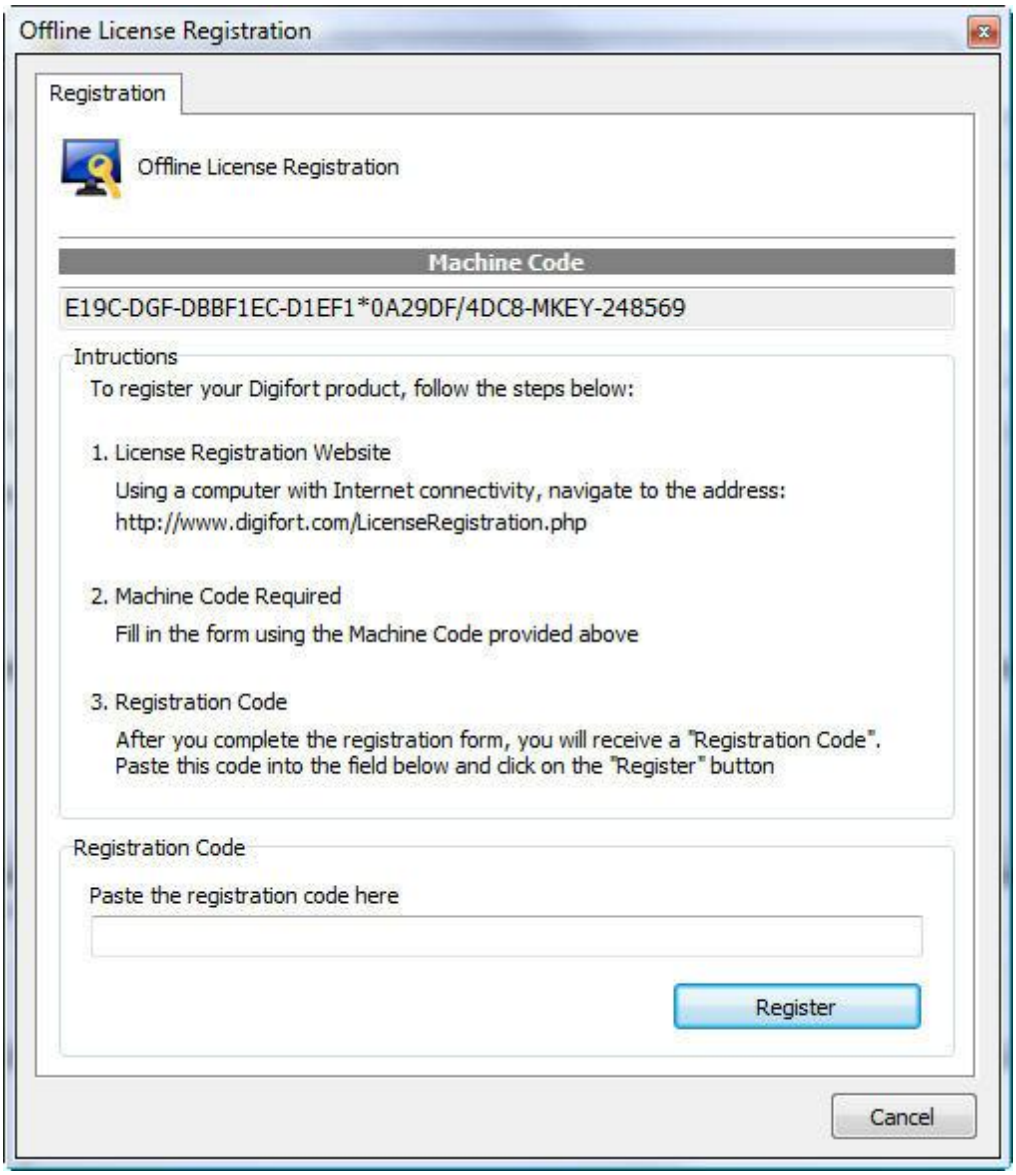
© 2002 - 2020 by Digifort, all rights reserved



5.3 Registering Digifort Offline

To register Digifort offline, click on the **Register Offline** button. A screen will be displayed with instructions on how to register Digifort. Follow the instructions shown in the screen and click on **Register**.

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter VI

6 Recording Server

This chapter is dedicated to the Recording Server of the Digifort System. It is in this module that the cameras are registered and their functioning is monitored.

The Recording Server is divided into two modules, the Camera module where the cameras are registered, and the Status module where the functioning of the cameras is monitored.

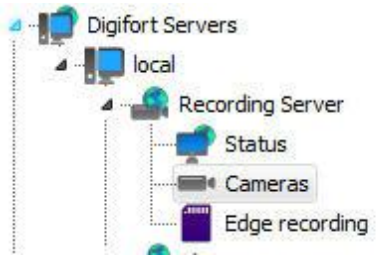
The Digifort System works with the main brands of digital cameras in the market and accepts analogical cameras as long as they are connected by way of a video-server device. These cameras can be located at the same site where the server is or can be remotely connected by way of some network connection. The main attributes of the configuration of the cameras, such as image resolution, number of frames per second and visualization rights are configured in the Digifort System and automatically applied to the cameras, regardless of location and without stopping the recording of the other cameras.

Performing tasks such as recording, video playback, system settings, query events, live monitoring, location of images are possible so that a task does not generate reflections in another.

The Register of Cameras is one of the most critical parts of the system, since a bad configuration can lead to the malfunctioning of the system. Therefore, careful planning must be done beforehand, collecting data such as the number of cameras, desired number of frames per second, days of storage, available disk space, etc.

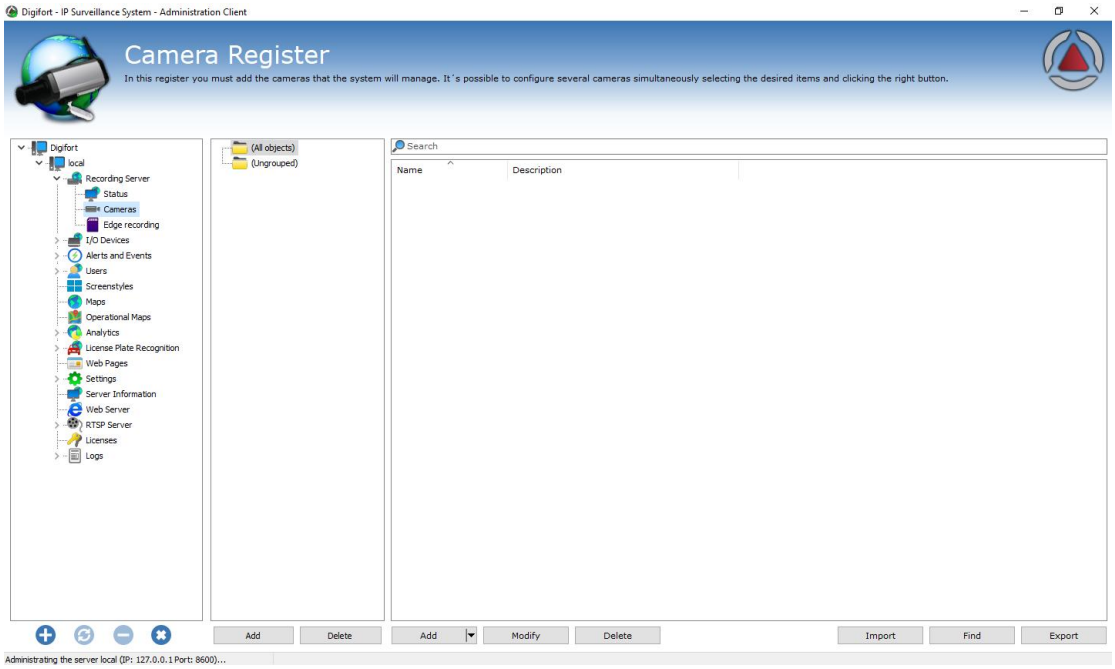
6.1 How to add a camera

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



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

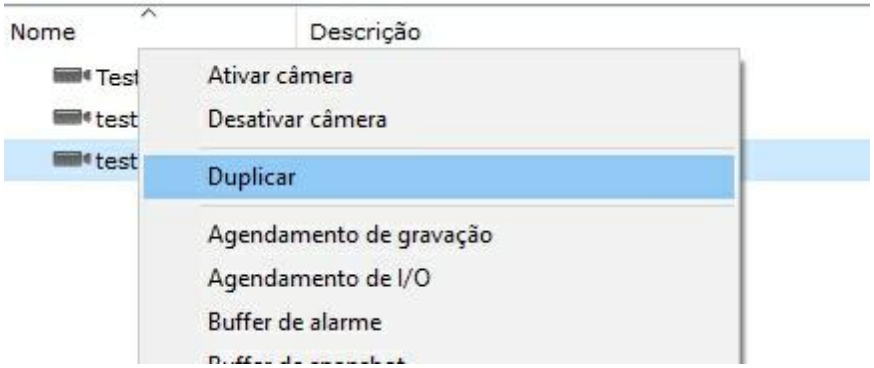
© 2002 - 2020 by Digifort, all rights reserved



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

Para adicionar uma câmera clique em **Adicionar**. Para alterar ou remover uma câmera, selecione a câmera desejada e clique sobre o botão correspondente.

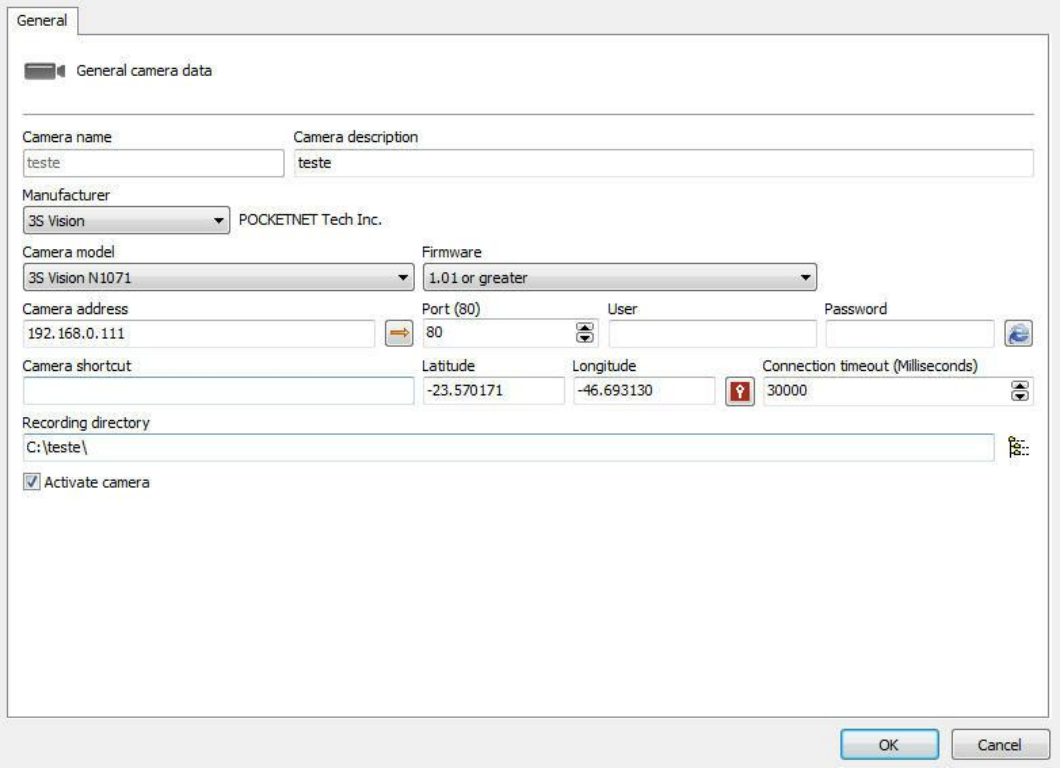
Tip: After adding a camera to the server, the administrator will be able to duplicate it, if necessary, by right-clicking on your registration and clicking on **Duplicate**



6.1.1 Camera

6.1.1.1 General

© 2002 - 2020 by Digifort, all rights reserved



- **Camera Name**: Enter a name for the camera. This name will be used as an internal reference of the system. Therefore, once saved it cannot be modified.

- **Description of the camera**: Enter a short description for the camera to aid in its identification. In the Surveillance Client it is this description that will help to identify each camera.

- **Manufacturer:** Select the manufacturer of the camera to be inserted..

- **Model of the camera:** Select the model of the camera to be inserted.

- **Firmware**: Select the version of the firmware of the camera to be inserted. As default, upon selecting the model of the camera, the last version of the firmware is automatically selected. In most cases, the choice of the most recent firmware allows the camera to work perfectly in all of its modes.

- **Camera Address**: The IP or DNS address of the camera. The IP address to be used should have already been internally configured in the camera.

There is support for IPV4 and IPV6 upon registration. When using a literal IPv6 address in the system, it must be placed between brackets ("[" and "]").
For example [2001:db8:85a3:8d3:1319:8a2e:370]. If the address is literal IPv4 or DNS, the address must not contain brackets.

- **Arrow button**: Opens the Windows Command Prompt with the ping command configured with the camera IP.
- **Port**: Camera communication port. Most cameras on the market connect through port 80. The port to be used must be internally configured on camera in advance.

© 2002 - 2020 by Digifort, all rights reserved

- **Username and Password:** Enter the user that Digifort will use to authenticate the camera. Check your camera's manual to find out the default user and how to add more users. Enter the password that Digifort will use to authenticate the camera. Check your camera's manual to find out the default password and how to change it.
- **Important**: It is recommended that you inform the camera user and password in the proper fields, because some cameras features depend on such information for a prior authentication and execution of the requested command. The user to be entered must be the camera administrator user. To obtain this information please check your camera's user manual.

    - **Preferred Transport:** It selects the preferred means of transport among Auto, UDP, and TCP.

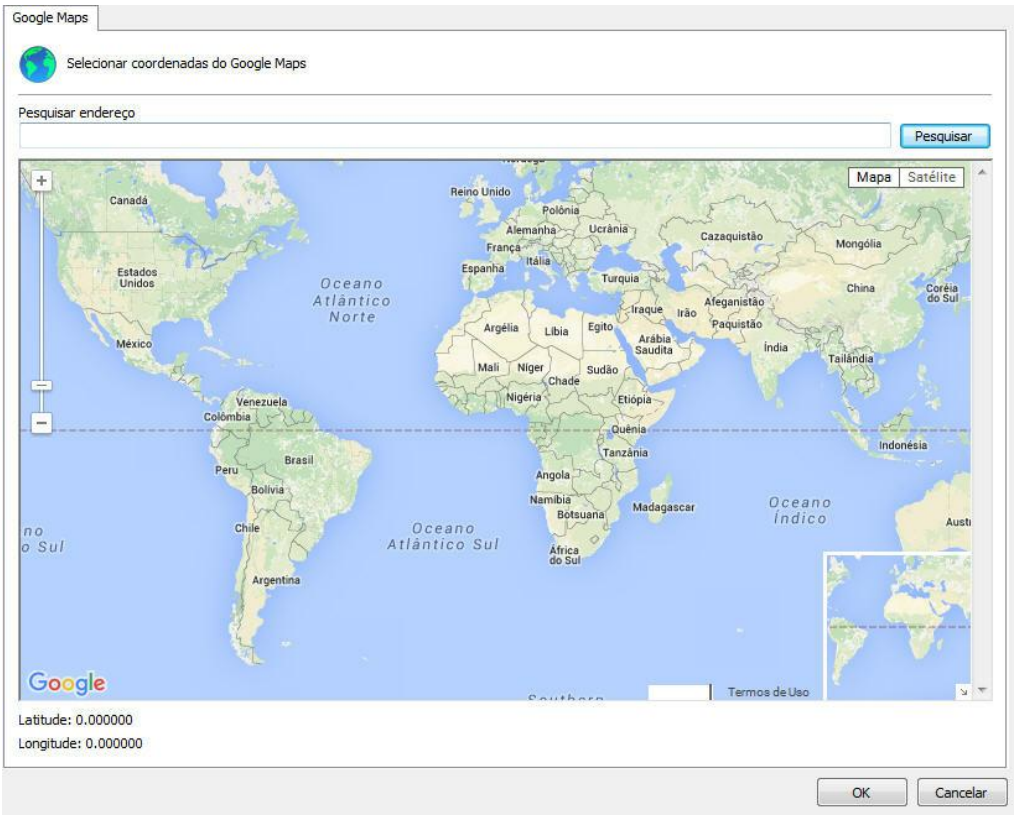
        - **Auto** - The transport used will usually be TCP, unless during the integration of the device the performance was not satisfactory, in that case transport will be done by UDP.
        - **TCP** - Transport will be done by TCP whenever possible.
        - **UDP** - Transport will be done by UDP whenever possible.
            - This option is a transport preference and not mandatory, i.e., even when specifically configuring either in TCP or UDP, the system will not necessarily follow the configuration as the device's media driver must support the desired protocol.

    - **Connection via SSL/TLS**: If the camera has a secure connection, check the box to activate the communication method using SSL 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**: Choose a shortcut to the camera so that this camera can be quickly displayed on the surveillance client screen through this shortcut.

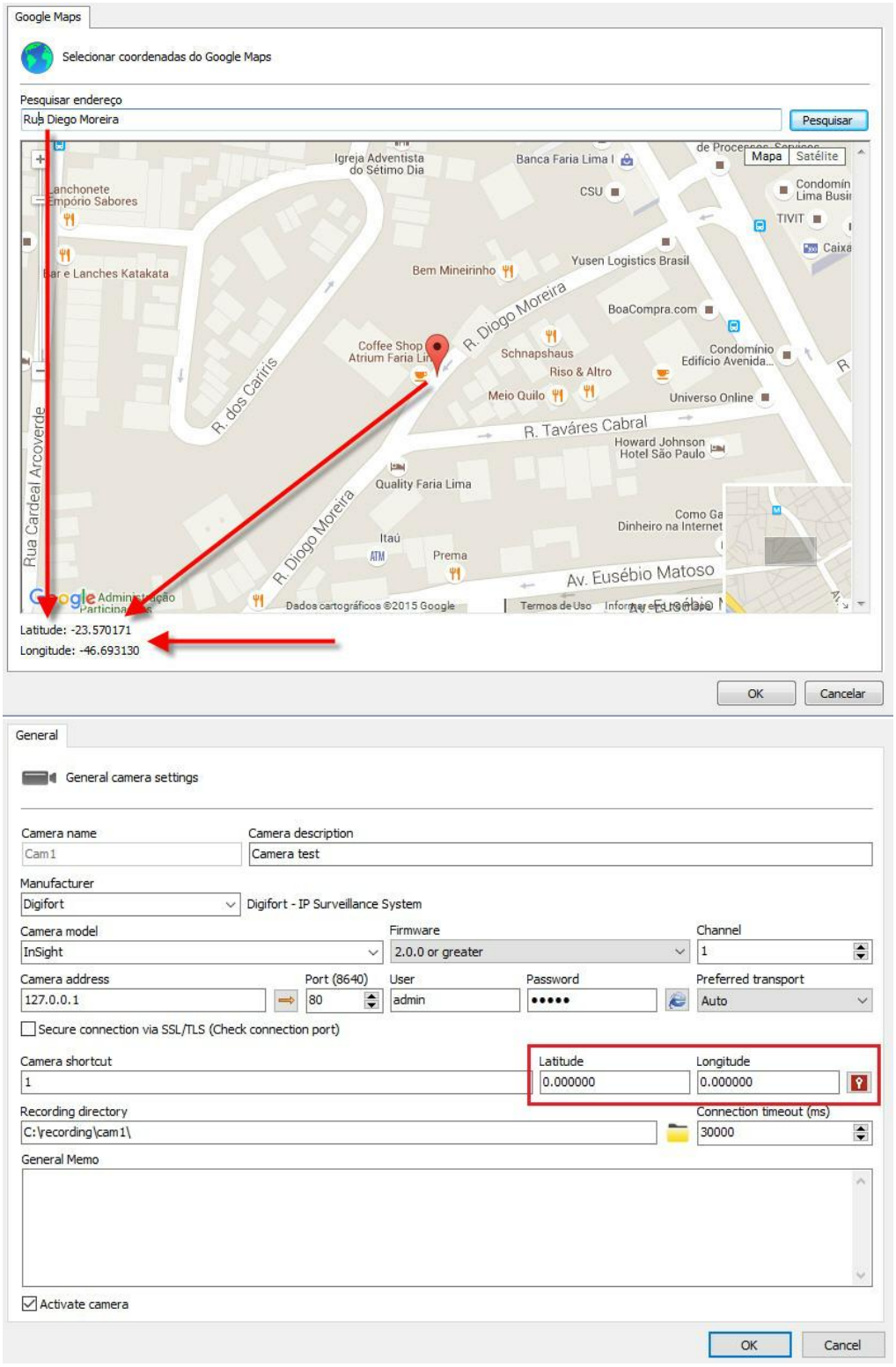
- **Latitude and Longitude**: Fill in longitude and latitude data of the location where the camera has been installed. This option can be used to create maps for easy positioning of the camera.
- **Select Google Maps coordinates**: Facilitates filling the Latitude and Longitude fields with automatic selection in Google Maps. By clicking this icon  the following screen will open:

© 2002 - 2020 by Digifort, all rights reserved



Simply select the desired position and the Latitude and Longitude fields will be filled in automatically.

© 2002 - 2020 by Digifort, all rights reserved



- **Connection timeout (in ms):** This parameter is used by the system when the connection with the camera is lost somehow. Then every X milliseconds the system will attempt to reestablish the connection, in which X is the specified value. To convert

© 2002 - 2020 by Digifort, all rights reserved

this value to seconds simply divide the value by 1000. By default this parameter is configured to 4000 ms (4 seconds).

- **Video port**: If the device to be inserted it a video-server, select the number of the port on which the camera is found. This field will only visible for video-servers with more than one port.

- **Recording directory** Digifort allows camera recording to be distributed among several disks. For this purpose, select the recording directory for images of the camera to be inserted. It's possible to record in network units, that is, in the disks of other computers in the network. To learn how to use this feature, see Network Units.

    - **General Observations**: If necessary, use the field to add additional information about the camera.

- **Activate camera**: Indicates whether the system must record the images received from the camera.

Attention

Digifort is responsible for administrating the structure of directories used in camera recording. Therefore, no file of its database should be excluded manually, and the camera recording directory may not be created by any means other than Digifort such as, for example, Windows Explorer.

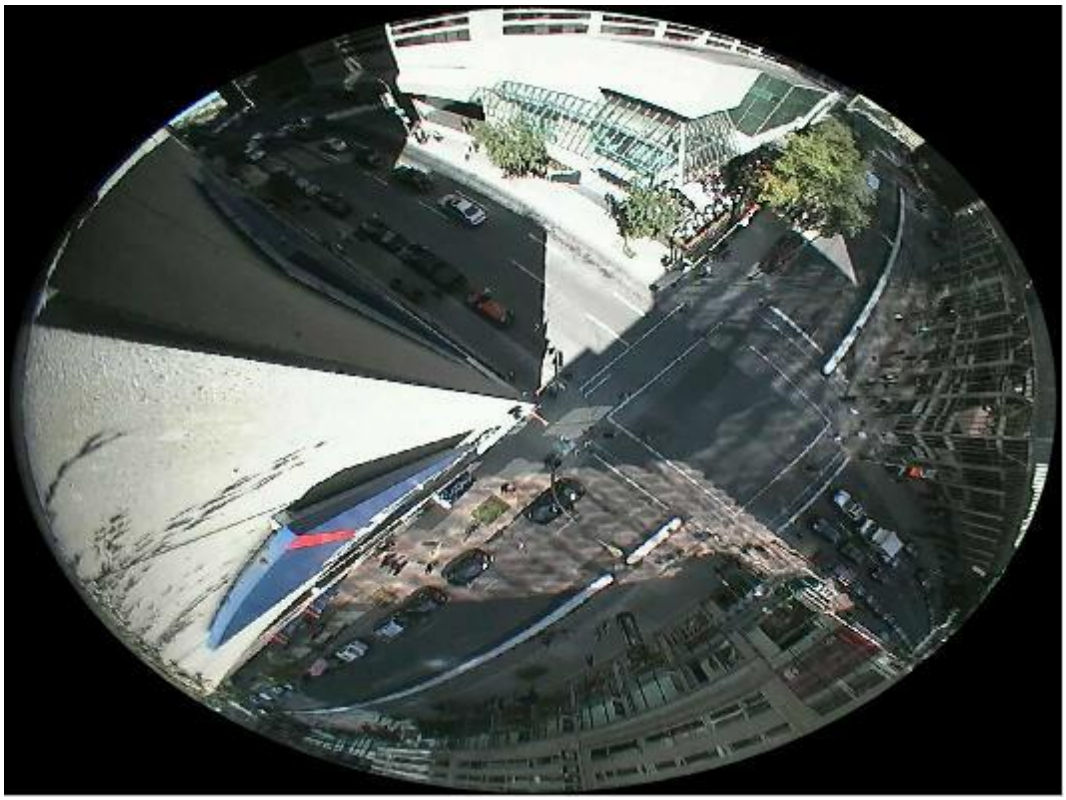
6.1.1.2 Lenses

Digifort allows the use of two types of integrated camera lenses: **normal** and **panamorphic**.

The standard Normal lenses are those that most cameras employ, ie with an opening that does not create a large image distortion.

Panamorphic lenses use an opening angle that focuses on a full 360 degrees. In this case, the image looks oval and distorted. See the image below:

© 2002 - 2020 by Digifort, all rights reserved



With this integration, Digifort makes what is called "dewarping", ie removes the distortion and you can see the image normally. This type of lens works very well with mega-pixel cameras, because with only one camera it is possible to focus all angles of a room and split the image as if it were from multiple cameras. See the example below:

© 2002 - 2020 by Digifort, all rights reserved



NOTE: Panamorphic lenses do not function as "fish eye" lenses, i.e. a fish eye camera should be integrated according to its manufacturer. The advantage of Panamorph lens is that it can be used in any camera with 1/3 sensor.
To learn how to use this feature live, see the monitoring client's manual.
See administration client settings in the screen below:



- **Lens used:** Select the type of lens being used

Panamorph lens settings

- **Lens Type:** Select the model of Panamorph lens being used.
- **Position the camera:** Select the location that the camera is installed: Wall, Ceiling, Ground

© 2002 - 2020 by Digifort, all rights reserved

6.1.1.3 Motion Detection

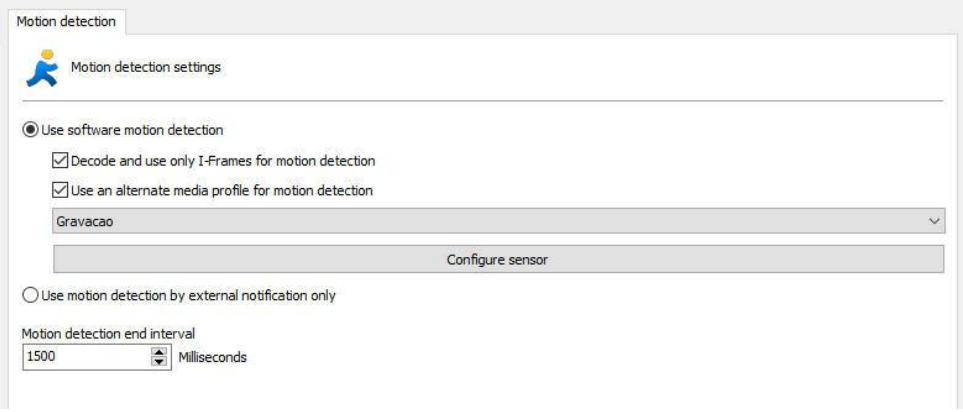
6.1.1.3.1 Use motion detection via softw are

When motion detection via Digifort is used, some care must be taken in respect to server processing and even the identification of areas of interest in the image for detection.

One must bear in mind that motion detection via software will always increase processing on the image recording server. This takes place as for each camera in which motion detection is activated, Digifort must decode an entire chain of frames and only 2 frames are compared from this chain.
An example of a CPU increase: the decoding of an entire chain of frames every second from a megapixel camera using H264 compression.

To reduce processing on the Digifort server, when configured to perform motion detection in the cameras, an option was developed to allow motion detection to be performed in a lower resolution media profile. Thus, image recording may be performed in high resolution and motion detection in low resolution. The lower the resolution used for motion detection the lower processing used.
The use of the CIF minimum resolution is recommended to achieve a good detection. In the matter of frames per second, only 3 frames per second is recommended, as in a 30-frame sequence, only 2 frames would be analyzed.

To selected a media profile for motion detection, select the **use of an alternative media profile for motion detection** and select the desired media profile, as shown in the figure below.



To learn how to use media profiles, refer to the Media Profiles chapter

Another option that helps decrease image processing is to **use only I-Frames to detect motion.** This option must provide a significant reduction in CPU usage by the server, but we recommend the use of 2 I-Frames per second for improved motion detection performance. Simply enable the option as shown in the image above **(Decode and use only I-Frames for motion detection).**

Motion Sensor consists of a tool that enables the user to define areas on the

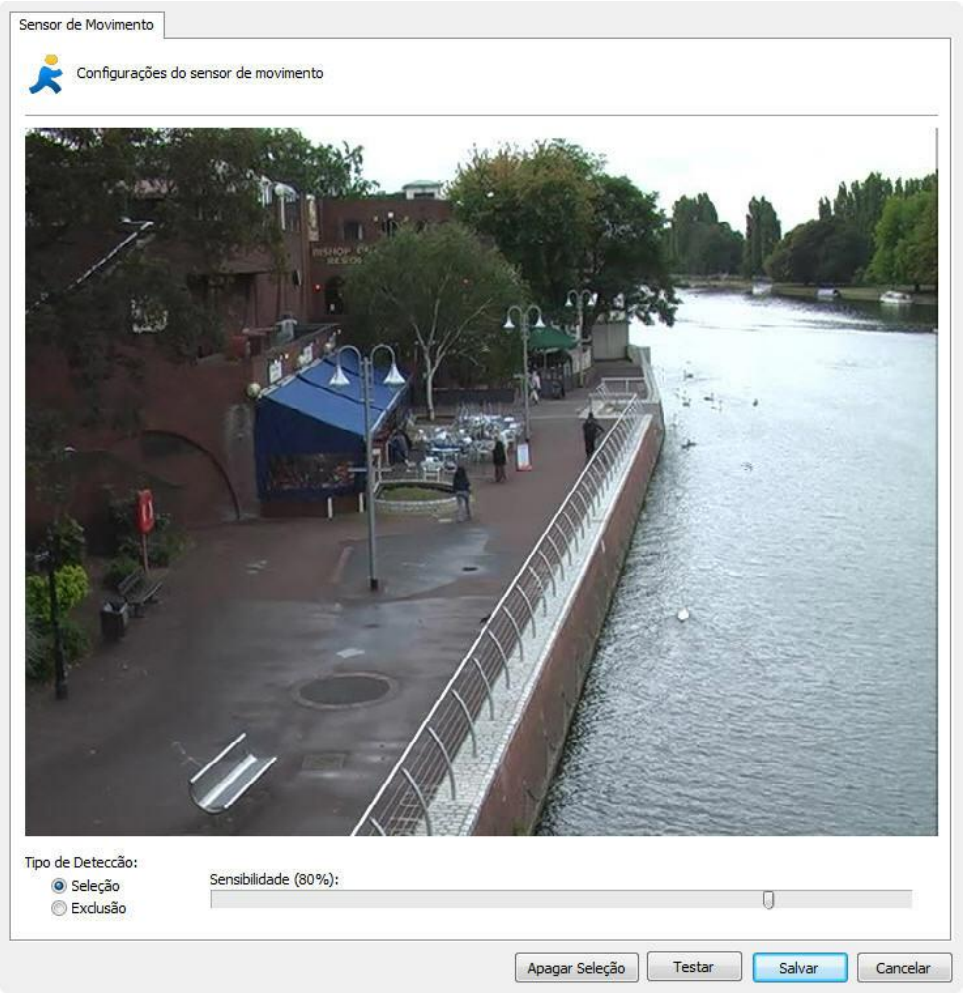
© 2002 - 2020 by Digifort, all rights reserved

image which will be sensitive or non-sensitive to motion.

The motion sensor settings are very important to save disk space used by the camera. If on the camera tab you chose to detect motion using the recording method, it is recommended to adjust the sensor as needed.

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

To configure the motion sensor, click on the **Configure Sensor** button.
By clicking on this button, the motion sensor settings window will open with a real image of the camera, as shown in the figure below:



On this screen, you can select the areas that are sensitive to motion or areas that are not sensitive to motion.

To select areas that will be sensitive to motion, select the type of detection and click on the image by dragging the mouse to form a square selection. To select areas which will not be sensitive to motion, select the **Deletion** button, repeating

© 2002 - 2020 by Digifort, all rights reserved

the process.

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

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

Once this is done, click on the **Test** button to view the operation of the selected motion detection.
For performance reasons, Digifort analyzes camera images at two frames per second, i.e., it is not necessary to perform motion detection on all frames, whereas an image is analyzed at every 500ms. With this standard, any motion is detected.

The figure below shows the operation of the motion sensor with motion-sensitive areas selected:



The figure below shows the operation of the motion sensor with non-motion-sensitive areas selected:

© 2002 - 2020 by Digifort, all rights reserved



The **Motion Sensor** consists of a tool that enables the user to define areas of the image which will be sensitive or non-sensitive to motion.

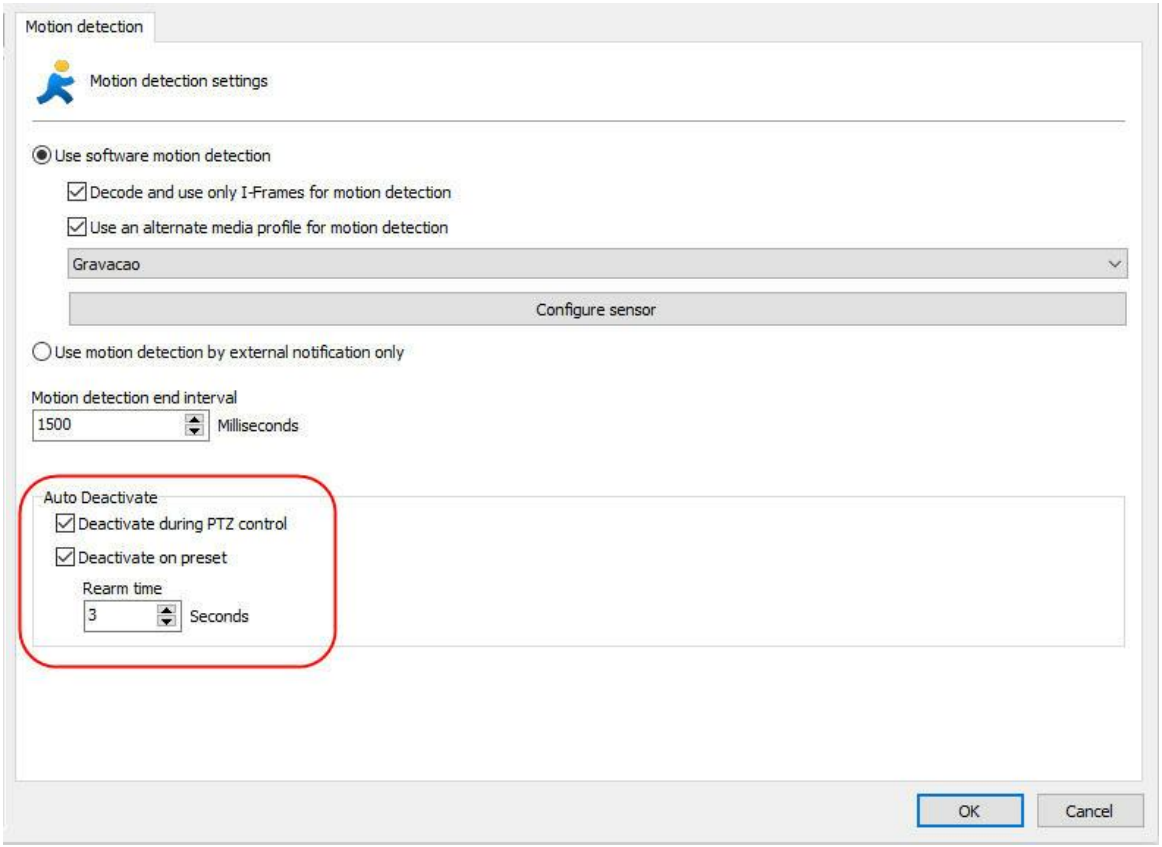
The motion sensor settings are very important to save disk space used by the camera. If on the camera tab you chose the recording method by motion detection, it is recommended to adjust the sensor as needed.

By default, if the sensor is not configured, the entire image will be sensitive to motion.

© 2002 - 2020 by Digifort, all rights reserved

6.1.1.3.1.1 Auto desativar detecção de movimento durante o PTZ //OLD: Auto deactivate motion detection during PTZ

The system allows motion detection on the server to be temporarily deactivated if the camera's PTZ is in use or during preset changes. This option should provide greater performance for the image processing server.



- **Deactivate during PTZ control**:It deactivates motion detection during PTZ control.
- **Deactivate on preset**: It deactivates motion detection when a preset is activated.
- **Rearm Time:** It sets the time to rearm motion detection after being deactivated by the previous options. In the case of PTZ usage, rearm will be counted from the moment PTZ stops being used. The preset option, on the other hand, will count from the moment the preset command is sent.

6.1.1.3.2 Use motion detection by external notification

Movement detection via external notification is an option that allows any type of equipment or software to activate movement detection of a camera registered in the Digifort system. Movement detection via external notification is mostly used via the camera hardware and video servers.

With the evolution of encoders and IP cameras, many resources are now part of the equipment so that they may make better use of their processing capacity, providing better solutions and decentralizing the image server processing activity.

© 2002 - 2020 by Digifort, all rights reserved

Movement detection is a simple resource that has been included in equipment thanks to this development. The main aim of processing movement detection directly by the equipment (Camera / Encoder) is to lighten the server processing activity as it needs to decode and analyze the images received. This may require a lot of processing by the CPU and, also, another advantage of processing movement via the hardware is that is can make the analysis using the original images (before compressing) which may ensure a better result because compressing the image may add artifacts (noise), which interfere with the analysis of movement.

There are two configurations that must be made to activate this option: **Setting up at the Digifort and camera configuration**

It is recommended that the document Using Hardware Motion Detection.pdf, as well as the following instructions, are read for better understanding of the subject

6.1.1.3.2.1 Configuration

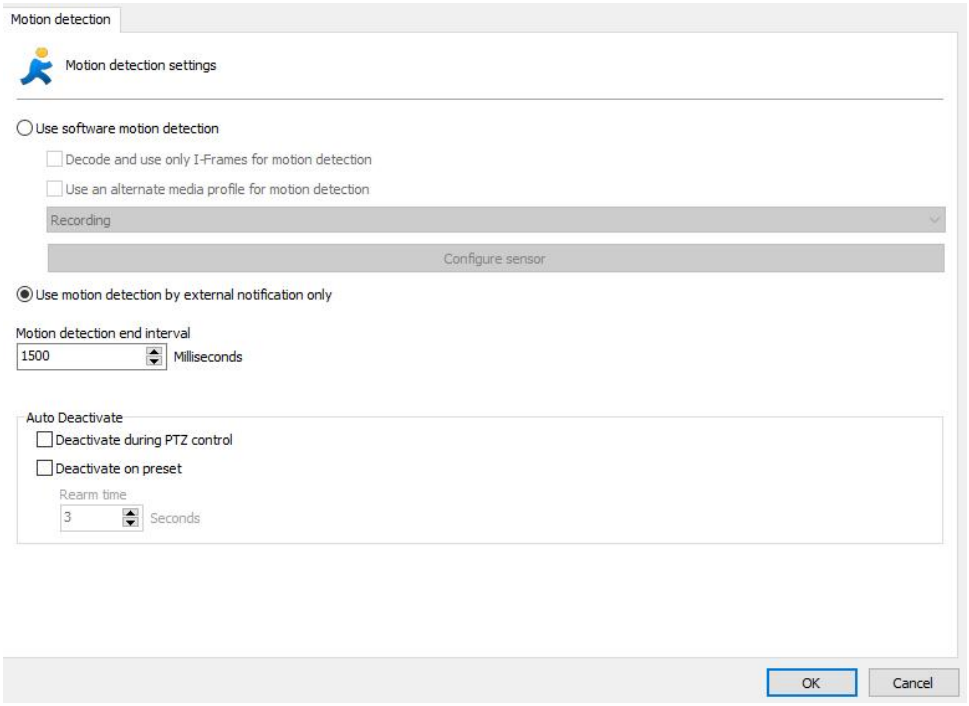
It is very simple to configure movement detection via the hardware. Only two steps are necessary to configure the Digifort to receive notifications by HTTP:

1. Configure the cameras in the Digifort server
2. Configure the cameras to inform the Digifort

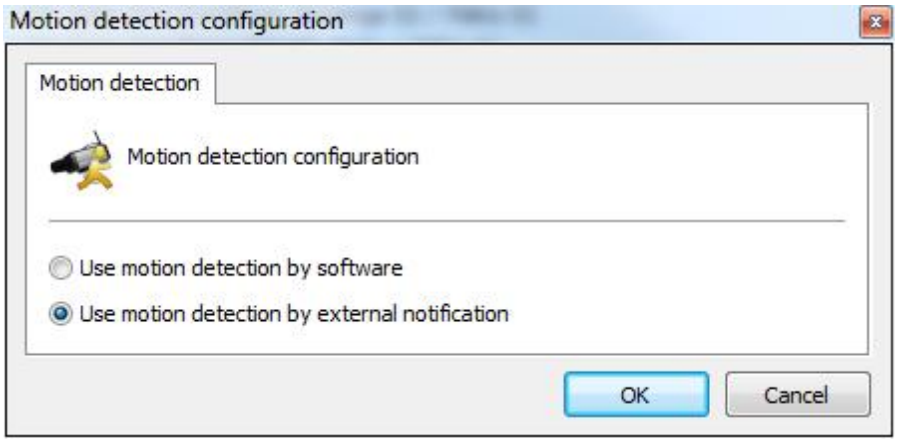
The only configuration made at the Digifort is to select the option "Use motion detection by external notification" in the "Motion Detection" tab of the cameras that will be using movement detection via hardware.

.

© 2002 - 2020 by Digifort, all rights reserved



You may also configure this option for several cameras simultaneously by selecting all the cameras chosen and clicking on the option “Motion Detection” in the popup menu accessed by clicking the righ-hand button on the mouse.



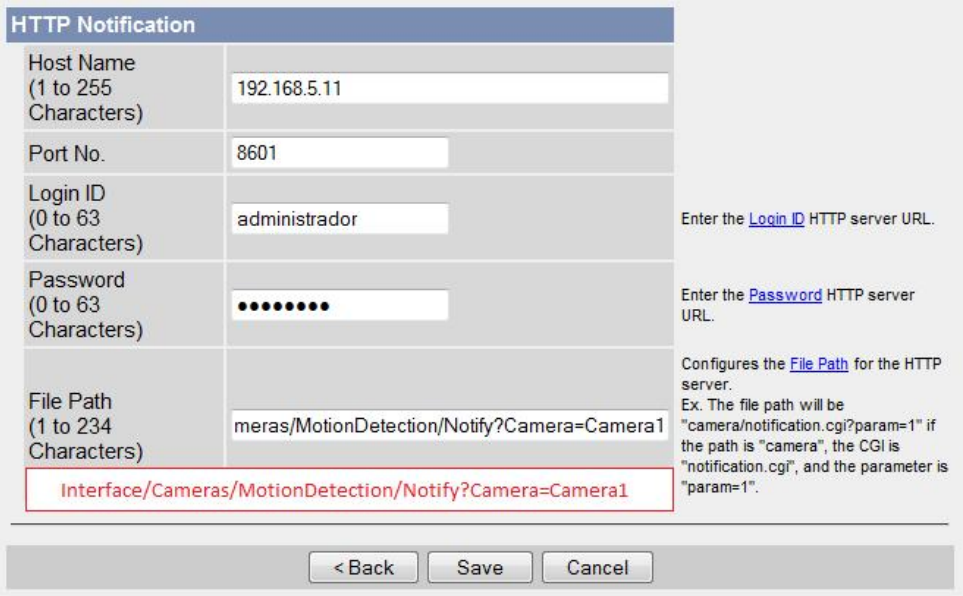
The camera configuration may be the more complex part of the process as each manufacturer implements the HTTP notification resource differently.

In this document, we will be describing the basic configuration procedure for a camera with movement notification by HTTP.

© 2002 - 2020 by Digifort, all rights reserved

Tip: Check if there is an document available for configuring a camera by a specific manufacturer.

As configuring a movement notification by http will vary considerably according to different manufacturers, an example of a general model is shown below

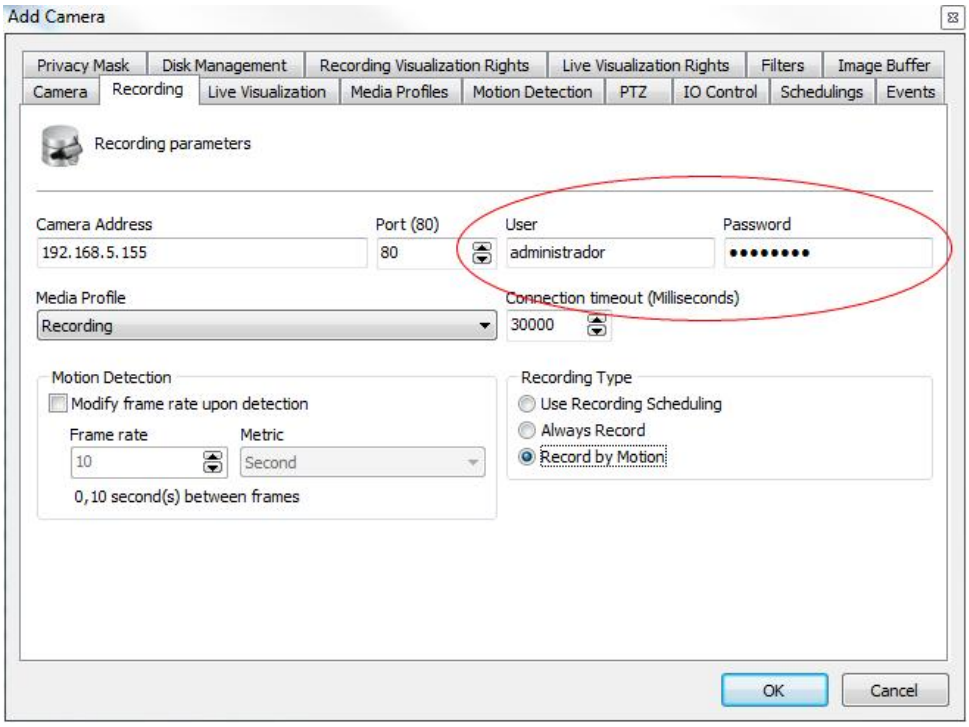


In this picture, the following notification parametres are configured:

Server: 192.168.5.11. This is the Digifort server address that will be notified
Port: 8601. This is Digifort's API HTTP port
User: administrator. This is the user used to access the camera and is the same user configured for the Digifort camera
Password: **********. This password is used to access the camera and must be the same password used to configure the Digifort camera
Parametres: These are the API notification parametres for movement detection at the Digifort

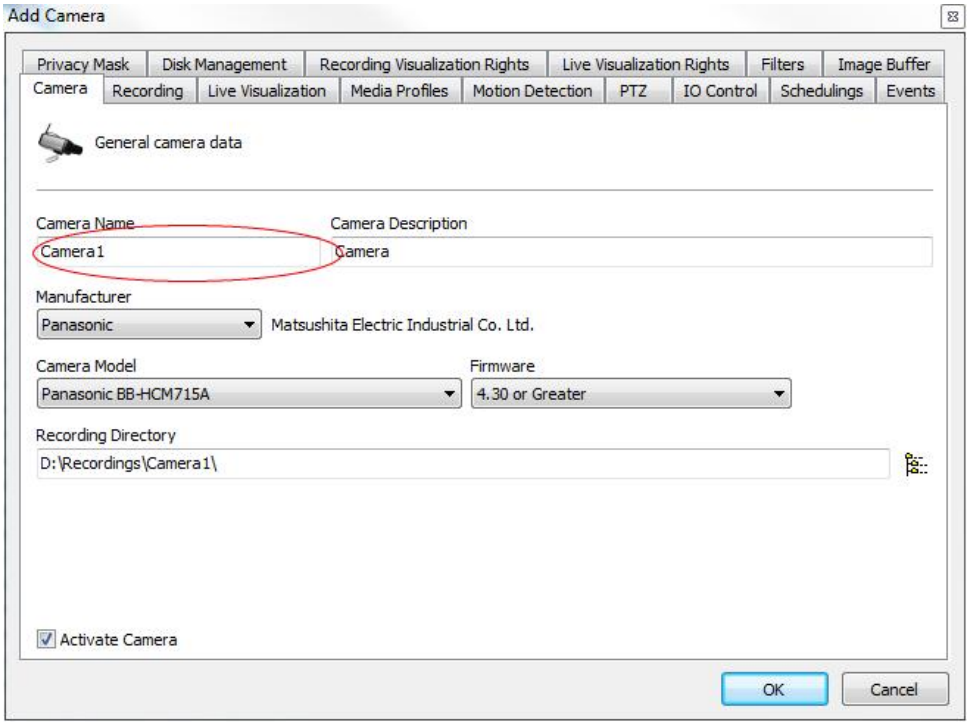
The credentials to access the API Digifort, must coincide with the data supplied when registering the camera in the system. See the picture below:

© 2002 - 2020 by Digifort, all rights reserved



The parameter `Camera` in the API's `Notify` command must be filled in with the same exact name as the camera supplied in the Digifort

```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1
```



If there is a space in the camera name, replace that space with the characters %

© 2002 - 2020 by Digifort, all rights reserved

20; this is because there can't be any spaces in the parametres of an HTTP GET request and the %20 characters represent a space.

Examplo:
Camera name: Camera 1

```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera%201
```

Cameras work with two types of movement detection notifications: **Start/End** and **Instant**.

Start/End: Cameras working with this type of notification (such as the Axis cameras) will send a request as soon as movement starts and another request as soon as it finishes.

Instant: Most camera models work with this type of notification. In this type, the camera will send a notification as soon as movement begins and subsequent notification while the movement continues.

Some cameras indicate the start and end of the movement. For the cameras that works like this, there should generally be two configurations made to the camera.

For this type of notification, the Motion parametre must be used:

To notify the start of the movement
```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1&Motion=Start
```

To notify the end of the movement
```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1&Motion=End
```

Note: If you configure only the notification for the start of movement and do not confi for the end of movement, the camera will start when it detects movement but will not

Most camera models work with this type of notification. In this type, the camera will send a notification as soon as movement begins and subsequent notification while the movement continues.
This is the standard operation of the API. The `Motion` parametre of the `Notify` command can include the `Instant` option, or you can choose to omit this parametre as the `Instant` value will be used as standard.

```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1&Motion=Insta
```

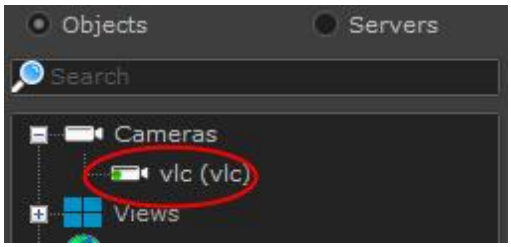
```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1
```

© 2002 - 2020 by Digifort, all rights reserved

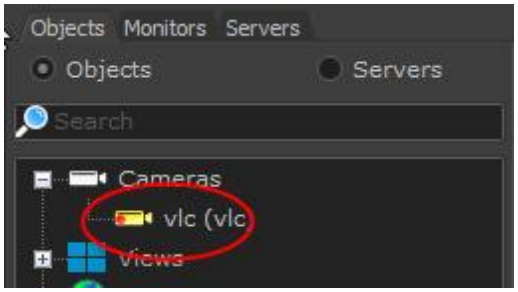
Important: When the system receives this type of notification it will record the imag post buffers added up are complete (3 seconds pattern for each buffer, which can be "Image Buffer" tab for the camera configurations in the Digifort). If your camera allow notification interval, use the same value (in seconds) of the post alarm buffer. If your have the option to configure the notification interval, increase the post-alarm buffer va tested do not take longer than 5 seconds to send the notification again).

To test if the configuration of the movement detection notification is working, open the monitoring client and check the camera status in the list of objects.

The camera's normal icon is grey with a small green circle. This icon indicates no movement in the camera.



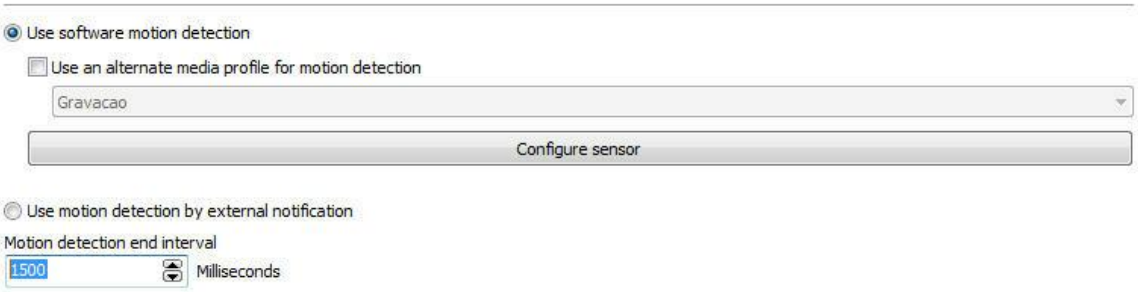
Create movement in the camera and watch if the camera icon changes to yellow as shown below. This icon indicates movement in the camera.



If there are no changes to the icon, check the configurations and try again.

6.1.1.3.3 Motion end detection interval

This option allows Digifort to record for X configured minutes after the motion ends.



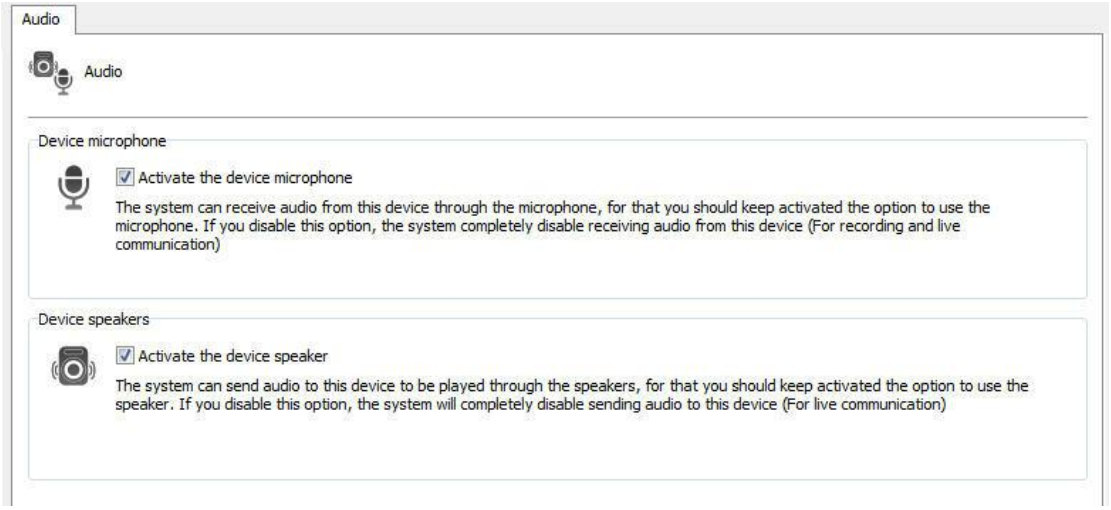
© 2002 - 2020 by Digifort, all rights reserved

In the above image, Digifort will stop recording after 1500 milliseconds after the motion ends, until the next one starts.

6.1.1.4 Audio

Digifort allows the use of the audio features of a camera.
You can listen and record audio captured by the camera's microphone or send the audio to your speakers.

With this feature, the operator can hear and communicate remotely via a microphone connected to the monitoring client. To learn how to use the audio in the monitoring client see your manual.



In the screen above the following features are available:

- **Enable the device's microphone**: Enable this option if you want to hear what the audio camera is capturing. When you enable this feature, the audio will be recorded automatically synchronized with the video camera.
- **Enable the loudspeaker device**: Enable this option if you want to send audio to the speakers of the camera

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

Audio formats supported: PCM, G.711, G.726 and AAC

6.1.1.5 Image Filters

Digifort is equipped with a set of effects that can be applied to the image so

© 2002 - 2020 by Digifort, all rights reserved

that cameras that have an impaired image can be improved.

This set of effects is only applied during the camera's visualization in the Surveillance Client, that is, the camera's original image is stored in the server.

To access this feature, click on the Effects tab, as shown in the picture below:



- **Red**: Adjusts the level of the color red in the image.
- **Blue**: Adjusts the level of the color blue in the image.
- **Green**: Adjusts the level of the color green in the image.
- **Contrast**: Adjusts the level of contrast in the image.
- **Brightness**: Adjusts the level of brightness in the image.
- **Color level**: Adjusts the level of color in the image.
- **Zero button**: Returns the above mentioned values to their initial positions.
- **Preview button**: Opens the video of the camera with the applied configurations.
- **Emboss**: Leaves the image in gray tones to highlight relief.
- **Flip**: Inverts the image horizontally. Recommended when the camera is installed in an inverted position.
- **Flop**: Inverts the image vertically. Recommended when the camera is installed in an inverted position.
- **Grayscale**: Leaves the image in gray tones.
- **Blur**: Applies a blurring effect to the image. Adjust the intensity level of the filter using the slide bar alongside.
- **Gaussian Blur**: Applies a Gaussian blurring effect to the image. Adjust the intensity level of the filter using the slide bar alongside.
- **Sharpen**: Applies a border highlight effect to the image.

6.1.2 Streaming

6.1.2.1 Media profiles

A media profile consists of a set or individual parameters of each camera such as image resolution, frames per second and image quality, that are associated with Recording and Live Visualization.
For better understanding, let's take the following situation: A recording profile could be created, that will be associated to the camera recording event. In this profile we could

© 2002 - 2020 by Digifort, all rights reserved

define that we want to record five frames per second, with a resolution of 320x240 and with high image compression. A visualization profile could also be created, that will be associated to visualization of the camera. In this profile we could define that we want to visualize the camera at ten frames per second with a resolution of 640x480 and low image compression.

As default, upon registering a new camera, two pre-defined media profiles are created, one for recording and one for visualization. The pre-configured parameters of each profile are only those parameters in common to all devices. The Media Profiles of most cameras and video-servers have parameters in common and individual parameters of each piece of equipment. The common parameters are:

- **Video compression**: The video compression to be used in recording images in disk. At present, Digifort supports the Motion JPEG and Wavelet formats..

- **Image resolution**: The image resolution that will be used in the profile. Upon selecting the model of the camera, this resolution list will automatically display only the resolutions supported by that camera. A very high image resolution will use up much disk space and bandwidth in your network, but the image will have a superior quality in which we will be able to recognize more detail in the image, such as, for example, the face of a person. A very low image resolution will use up little disk space and bandwidth in your network, but the image will have an inferior quality, giving few details. This parameter should be well configured according to your needs. Digifort has a calculator for disk space use that will help you to better configure the image resolution and frames per second. To learn how to use the Digifort calculator, see Calculator for disk space usage.

- **Image quality**: The images coming from the cameras go through a compression process. The higher the image compression level, the less quality the image will have, and the lower the image compression level, the more quality the image will have. Digifort offers five quality levels ranging from High (low compression) and Low (high compression). After various laboratory tests we recommend the Medium quality, as it offers an excellent image quality and low network traffic and low disk space usage.

- **Frames per second**: The number of frames per second to be recorded. A greater frames-per-second rate will use up more bandwidth in your network and more disk space, but will offer smoother movement. A lower rate of frames per second will use up less bandwidth in your network and less disk space, but the movement will be jerkier. It has been scientifically proven that at three to seven frames per second, it is possible to recognize all movements of a person. In some cases, it might not be possible for the camera to send the configured number of frames per second, especially at high frames-per-second rates. This is due to various factors, such as the bad functioning of the internal network, the number of connections made to the camera and the processing power of the camera.

As parameters specific to an individual piece of equipment, we can cite insertion of text into the image, image rotation, color levels, etc.

Some cameras may not support the adjustment of common parameters, such as, for example, the frame rate and the image quality. In these cases, adjustments must be made directly in the camera using its own interface.

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.1.1 How the Media Profiles save network bandwidth

The media profiles also help to save network bandwidth. To explain this concept, first we will define two media profiles, described below:

"Recording" Media Profile	
Parameter	**Value**
Video compression	Motion JPEG
Image resolution	640x480
Image quality	Medium
Frame rate	4 fps

"Visualization" Media Profile	
Parameter	**Value**
Video compression	Motion JPEG
Image resolution	640x480
Image quality	Média
Frame rate	30 fps

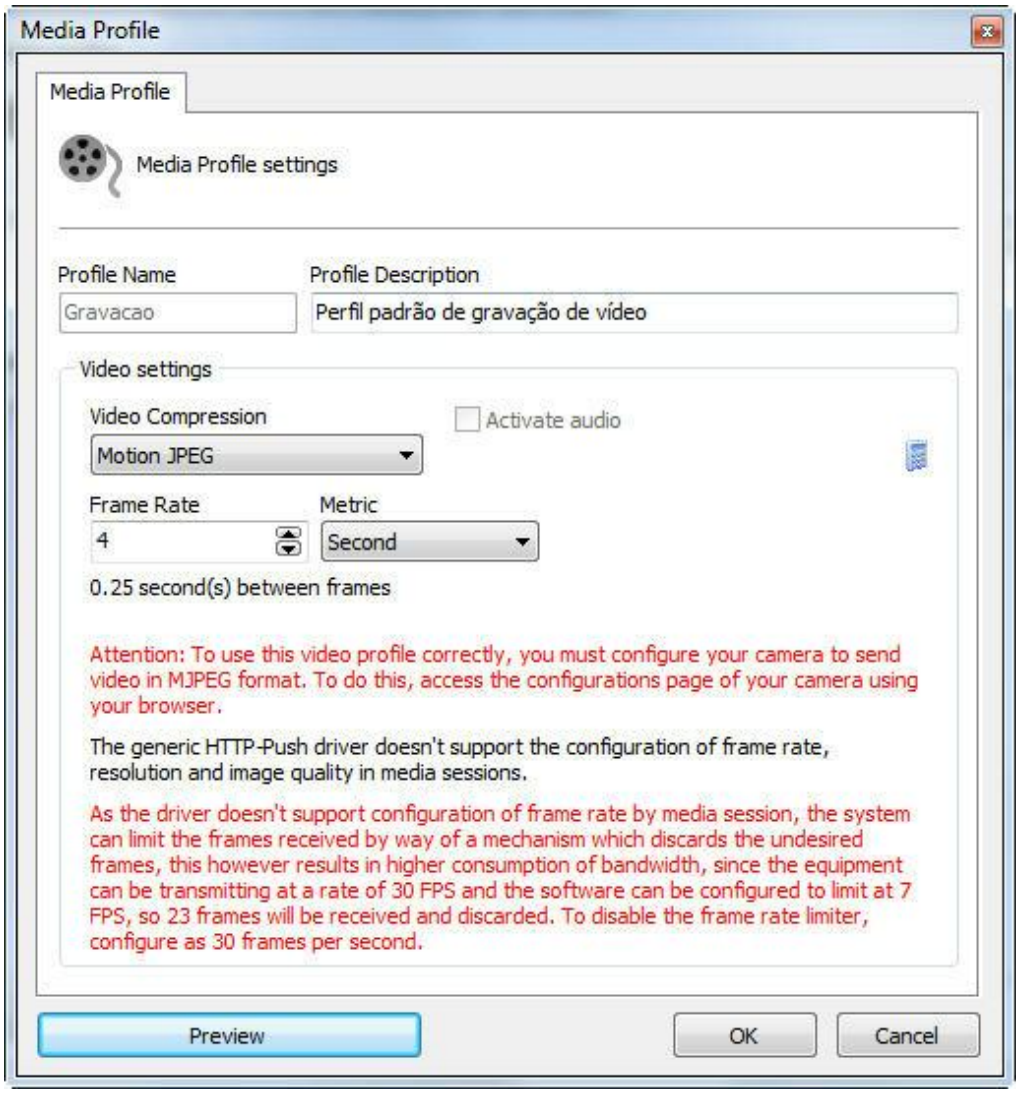
Obs: Digifort operates with any resolution supplied by the camera, whether it is low or high resolution (HD) and with any commercially available compression formats (Motion JPEG, MPEG4 and H264).

As we can see in the two examples of Media Profiles, all of the parameters of the "Recording" profile are the same as those of the "Visualization" profile, except the Frame rate. With this type of configuration, where only the frame rate is different, Digifort save bandwidth in this way: Let's suppose that the server is recording the images generated normally by the
camera with the associated "Recording" profile. In this case, it will be receiving only four frames per second. In a certain moment, the user wants to visualize this same camera in the Surveillance Client at a frame rate of 30 frames per second. At this moment, Digifort recognizes that the configurations are the same, with only the visualization frame rate being higher than the recording frame rate. Instead of the server making a new connection to the camera to receive the desired 30 frames per second, it closes the present connection and opens a new connection receiving the 30 frames per second, applying a frames speed filter on the recording profile, limiting its velocity to 4 frames per second. This way, only one connection is maintained with the camera receiving only 30 frames per second instead of two connections receiving a total of 34 frames per second.

6.1.2.1.1.1 How to add Media Profiles

To add a media profile, click on **Add**, and the media profile adding screen will be displayed as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



It's important to point out that this screen can vary from camera to camera, since each one has its own set of configuration parameters.

In the example above, the selected camera doesn't support adjustment of image resolution and quality.

6.1.2.1.1.2 How to visualize the functioning of the configured media profile

To visualize the results of the configurations of the parameters of the media profile being edited, click on the Preview button, opening a screen with the live image of the camera, as shown in the picture below:

This function will only work if the camera's connection address was previously informed.

© 2002 - 2020 by Digifort, all rights reserved



In this screen, the following configurations are informed:

- **Received frames per second:** Informs the number of frames per second received.
- **Image size**: Informs the size of the received image in KB/s and in Kbps. These values help in the dimensioning of the disk space and network bandwidth that this camera occupies..
- **Decoder codec**: The codec used for decoding the image. Digifort uses various decoding codecs. When the camera is added, the codec that has the best performance based on the received image is automatically identified.

Observation

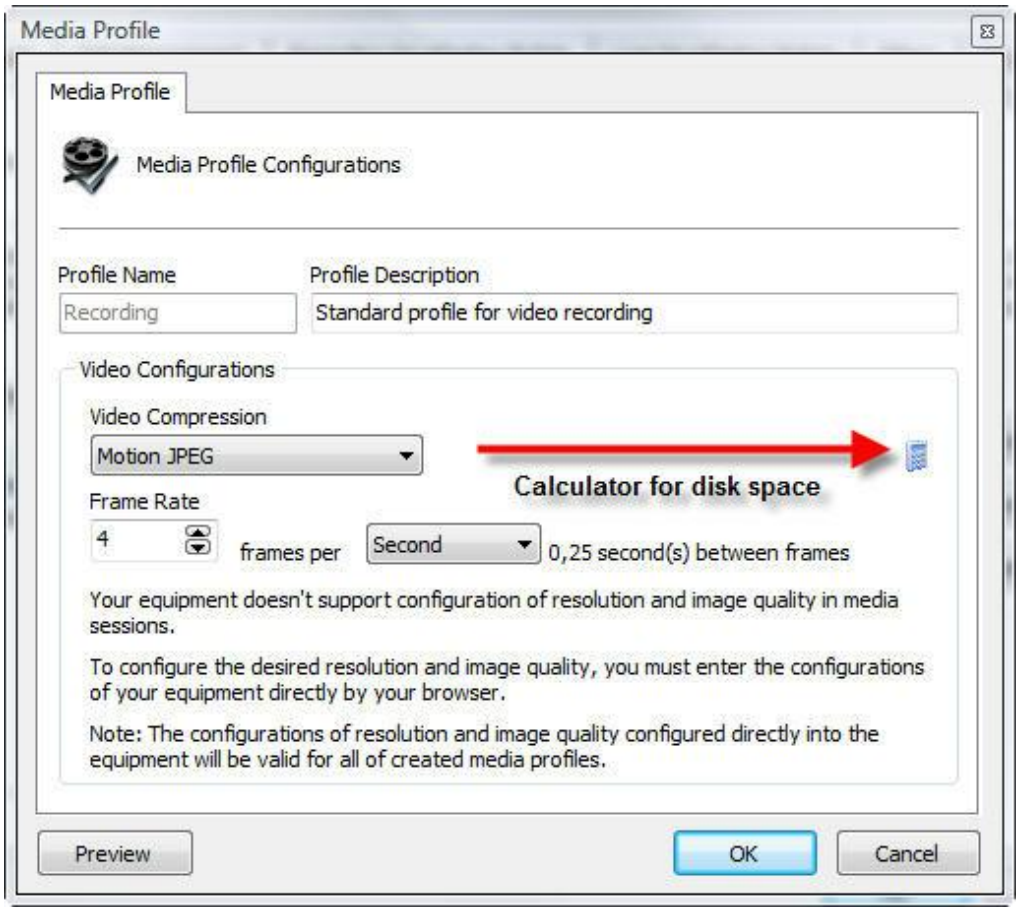
All information contained in the image is updated every second.

6.1.2.1.1.3 Calculator for disk space usage

Digifort has a very useful tool to aid in the dimensioning of disk space to be reserved for each camera: the disk space usage calculator. To access this feature, click on the button identified by a “calculator”, on the media profile configuration screen, as shown in the picture below:

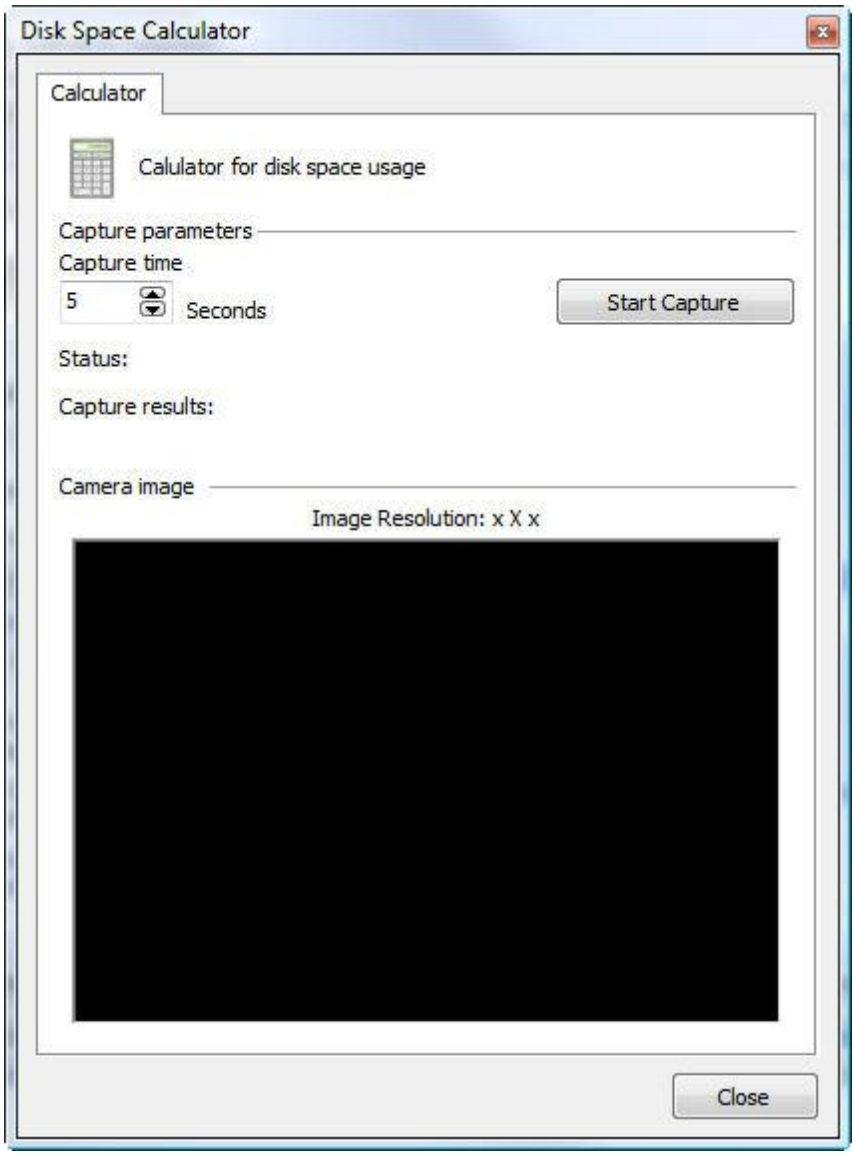
This function will only work if the camera’s connection address was previously informed.

© 2002 - 2020 by Digifort, all rights reserved



Clicking on this button, the disk space calculator will be executed as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

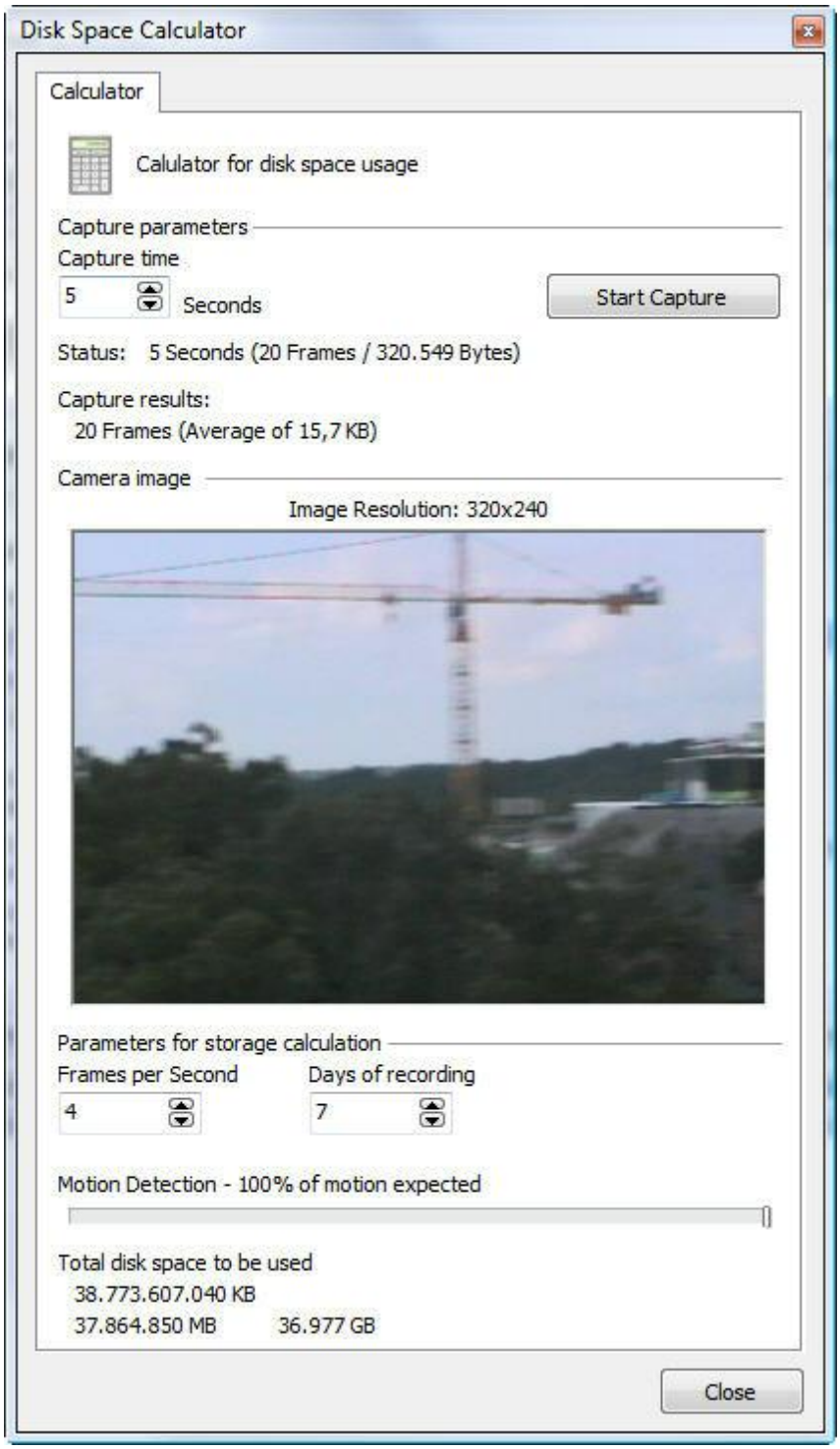


To calculate the disk space necessary for the recording of the camera, the calculator captures an original temporary video from the camera with the parameters of image quality and resolution configured in the media profile being edited and the capture time informed in this screen. Based on the video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

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

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

© 2002 - 2020 by Digifort, all rights reserved



After the end of the analysis of the captured video, the calculator fills the maximum frames-per-second value that the camera is able to send, that is, if the media profile was configured for recording at 30 frames per second, but the camera is only able to send 12 frames, this value will be 12. Modify the values of frames per second, days of recording and estimation of the motion detection to get an estimation of the

© 2002 - 2020 by Digifort, all rights reserved

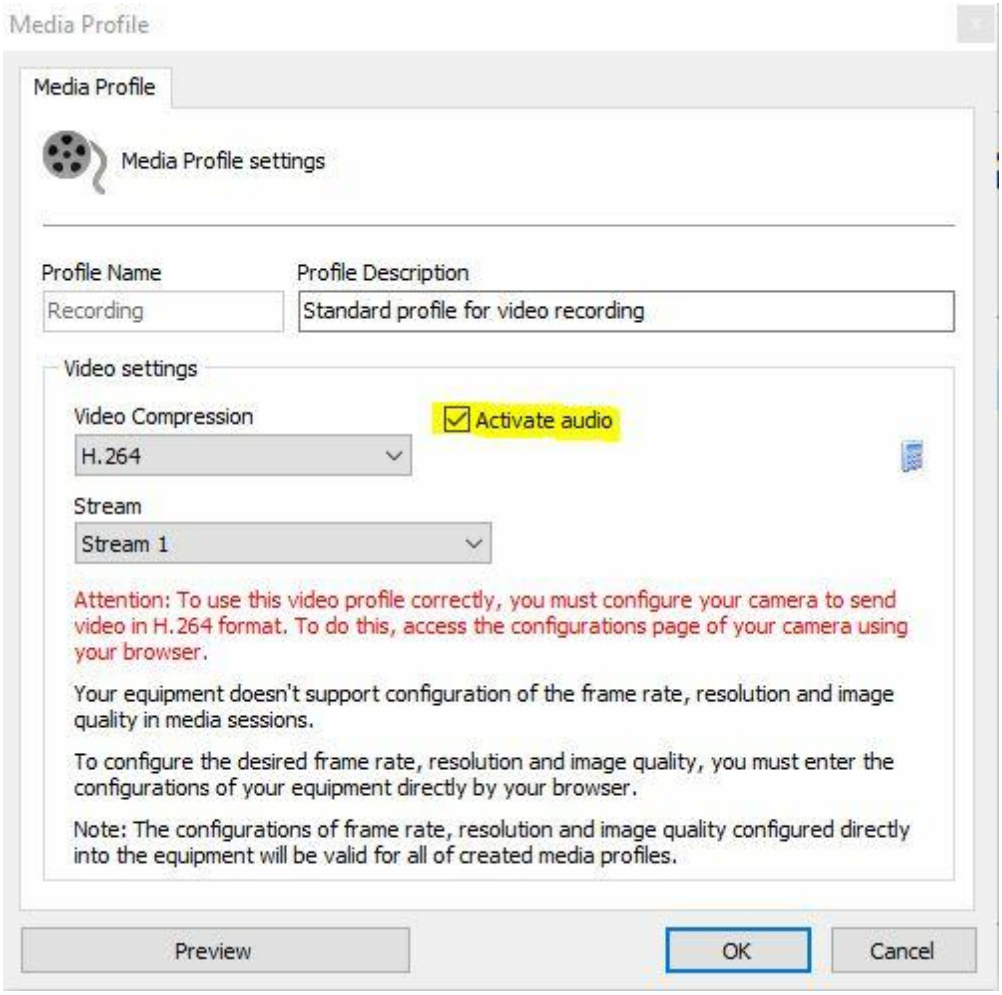
occupation of disk space to be used by the camera. Below are descriptions of how each parameter of the space calculator works.

- **Days of recording:** Informs the number of days to be stored for this camera. The greater this value is, the more disk space is used.
- **Frames per second:** Informs the number of frames per second to be used in recording of the camera.
- **Motion detection:** Informs the percentage of motion expected at the location of the camera in a day. For example, if the normal operation of a camera doesn't detect motion at night, then we slide this control, adjusting its value to 50%.
- **Total of disk to be used:** Informs the disk space necessary for storing the images generated by the camera with the parameters configured in the media profile being edited, the number of storage days and the percentage of motion configured.
- **Calculate size:** Click on this button to recalculate the disk space necessary for storage of the images of this camera with a new image.

6.1.2.2 Audio

If your camera has audio support, you can select the media profile you want to play:

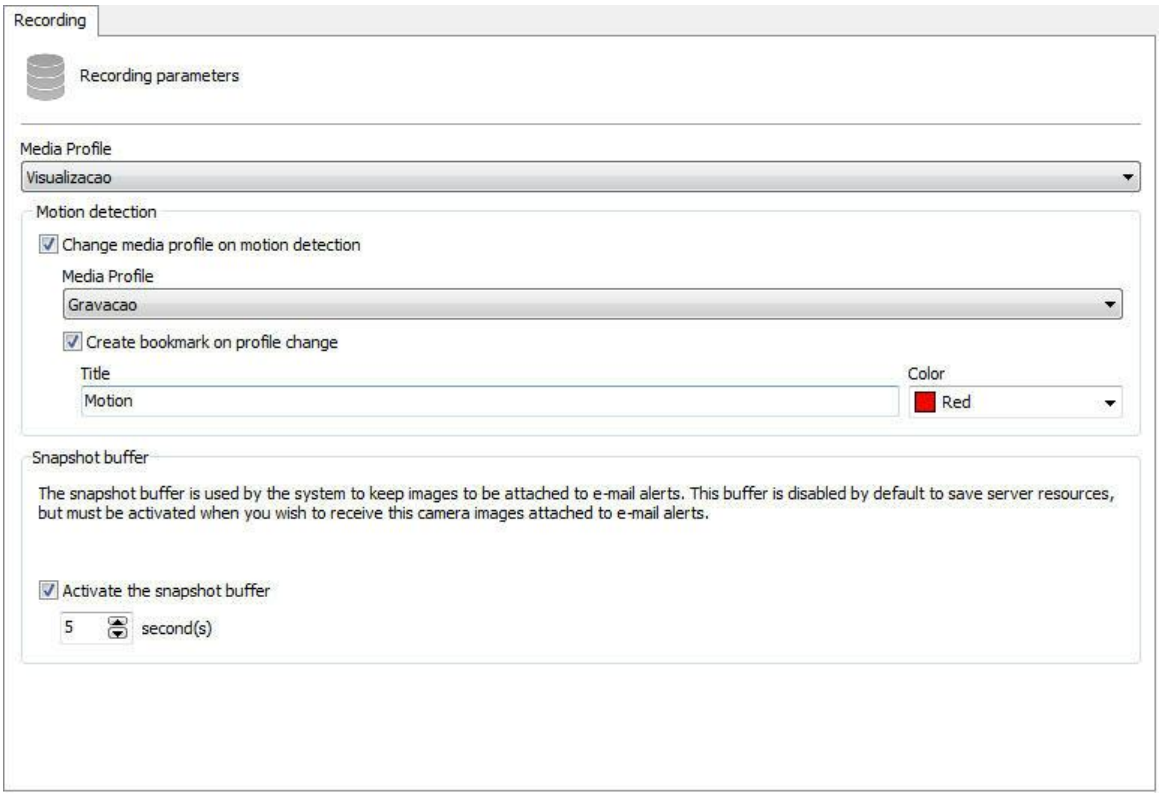
© 2002 - 2020 by Digifort, all rights reserved



6.1.2.3 Recording

On this screen, you can configure the camera recording stream on Digifort.

© 2002 - 2020 by Digifort, all rights reserved



The previous screen has the following features:

- **Profile Media**: Choose the media profile that will be used by the software when recording images.

Motion Detection

- **Change the media profile in the media detection**: Changes the current recording profile for what is selected in sequence. This option can be used in the following situation: you desire, for example, to record images continuously at 3 frames per second and when motion is detected the recording will change to 30 frames per second.

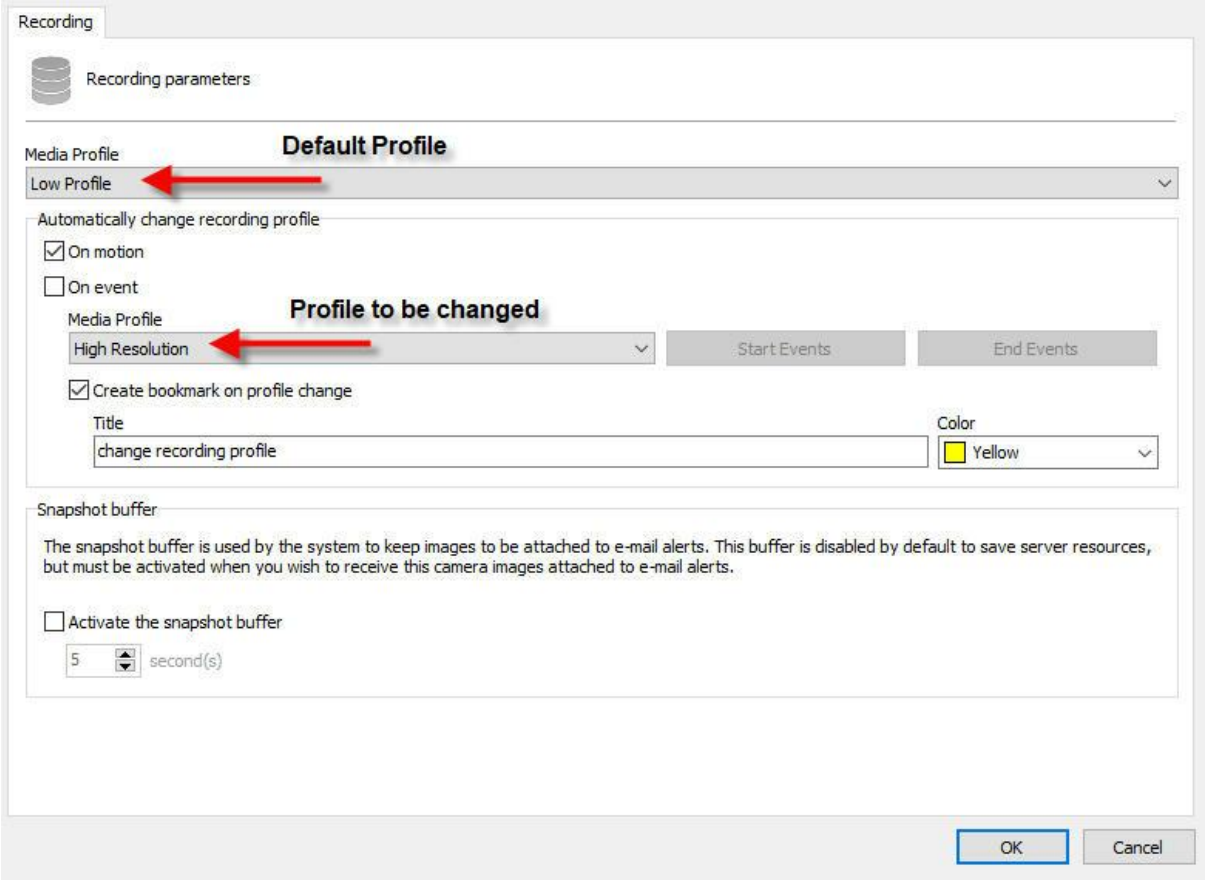
6.1.2.3.1 Automatically change recording profile

The profile that is used for recording on Digifort may be changed in real time.
One of the available features is to change the recording profile when motion is detected.

Example of operation:

If a camera has two profiles, one with the higher resolution and the other with a lower resolution, the system may be configured to record continuously in the lower profile and when motion is detected, the profile will be automatically changed to the higher one. This configuration allows greater flexibility for those who want to save on image storage.

© 2002 - 2020 by Digifort, all rights reserved

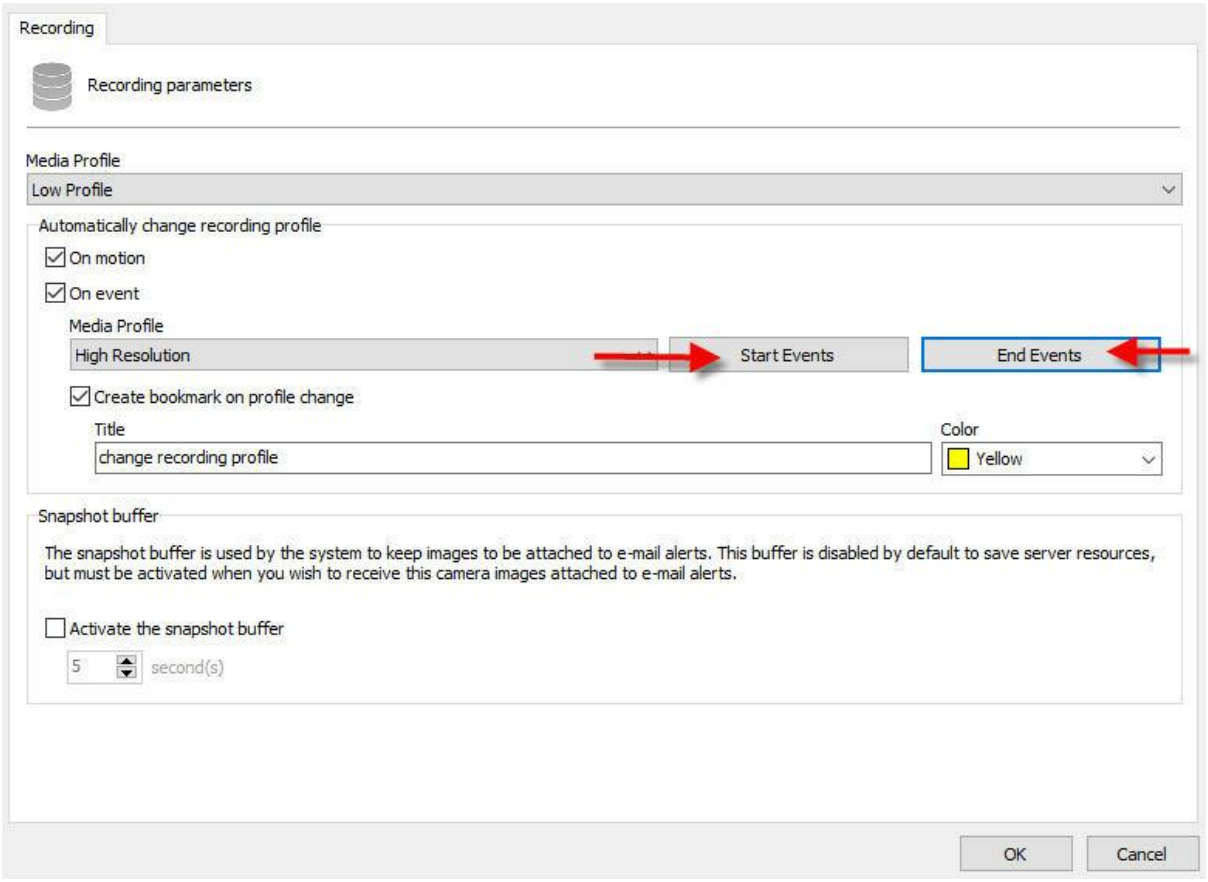


The above image shows the configuration for the motion detection event (On Motion)

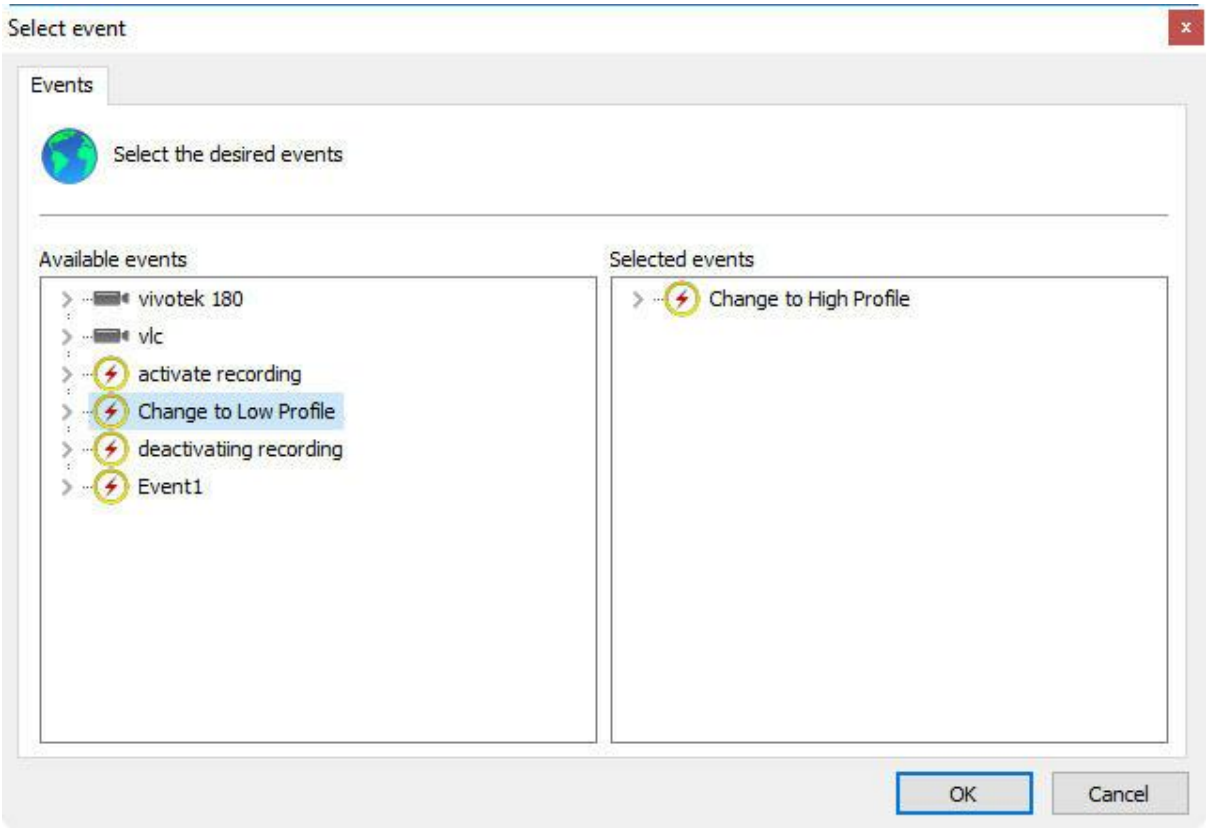
Another interesting option to change the recording profile in real time is the option **per Event (On Event**). It is possible to select any available event on Digifort (I/O, Global Events, Analytics, etc.) to begin the profile change and to finish the profile change.

Simply select the option **On Event** and choose the events as on the images below:

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

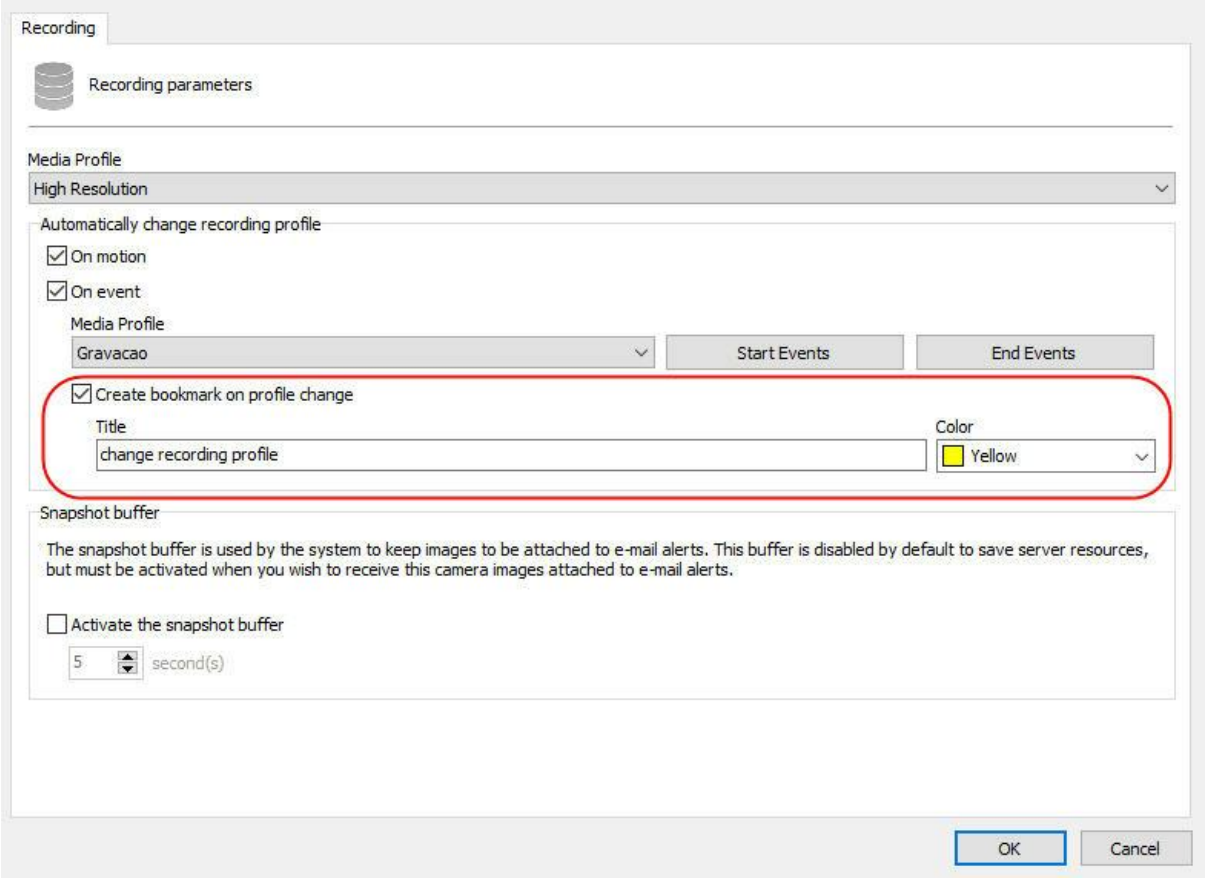


6.1.2.3.2 Create Bookmark on Profile Change

If the recording profile is changed on motion detection, the system may create a Bookmark on the video. To learn more about Bookmarks, see the Surveillance Client manual.

All movements in which the system detected motion and changed the profile, there will be a Bookmark on the recording, thus easing the search for events.

© 2002 - 2020 by Digifort, all rights reserved



To activate this feature, click on **Create Bookmark on Profile Change**.
Choose a title and a color for the Bookmark.

6.1.2.3.3 Buffer de Snapshot

The Image Buffer is used when you want to send still images from the cameras via email if an alert is triggered.
In case your version supports the maps feature, Digifort may display the image preview on the camera status on a map (check the surveillance client manual).

By default this option is disabled to save server resources.

- **Activate image buffer**: If you activate the image buffer, the server will hold the images in memory for X seconds so they can be sent by e-mail. If there are many cameras linked to an alarm, it is advisable to increase the number of seconds since it takes time to attach the images to the e-mail.

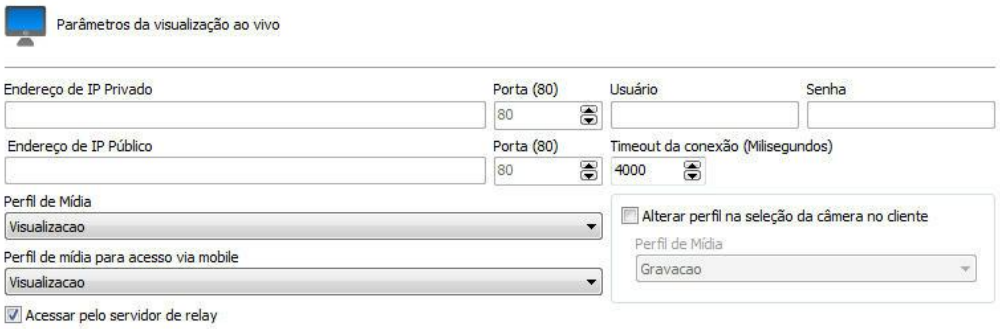
6.1.2.4 Live View

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.4.1 How to configure the visualization of the camera

After registering the media profiles to be used, it's necessary to associate them to the events of recording and visualization of the camera.

To access this configuration, click on the Visualization tab, as shown in the picture below:



The configuration carried out here will be applied to the Surveillance Client, which will use this information to capture the image from the cameras and show on the screen.

The parameters to be configured are described below.

6.1.2.4.1.1 This camera will be accessed by the client via relay server

With this option marked, the server will send the client, images that are being recorded in real time using the media profile associated in the Recording tab. With this option marked, no additional configuration is necessary.é necessária.

6.1.2.4.1.2 Private IP address

In case access to the camera via relay server is not used, inform the IP address of the camera's local network.

6.1.2.4.1.3 Private IP port

Informs the communication port with the camera of your internal network. a porta de comunicação com a câmera de sua rede interna.

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.4.1.4 Public IP address

Digifort also offers the possibility of making a connection with the camera via external network, such as Internet, for example. Fill in the Internet IP address. For this option to work, your router must be configured to supply access to the camera externally.

6.1.2.4.1.5 Public IP port

Informs the communication port with the camera via external network. com a câmera através da rede externa.

6.1.2.4.1.6 User and Password

User: Informs the user that Digifort will use to carry out authentication on the camera. Consult the manual of your camera to identify the default user and how to add more users.

Password: Informs the password that Digifort will use to carry out authentication on the camera. Consult the manual of your camera to identify the default password and how to modify it.

Important

it's recommended that you inform the user and the password of the camera in the correct fields, as some camera features depend on this information for previous authentication and execution of the requested command. The user to be supplied must be the administrator user of the camera. To get this information, consult the user manual of your camera.

6.1.2.4.1.7 Connection timeout (in MS)

This parameter is used by the system when the connection with the camera is somehow lost. Then, every X milliseconds the system will try to re-establish the connection, where X is the specified value. To convert this value to seconds, simply divide this value by 1000. By default, this parameter is already configured at 4000ms (4 seconds).

6.1.2.4.1.8 Media profile

Select the media profile to be used for visualization of the camera. This option will only be available if this camera will be accessed by the client via relay server is unmarked.

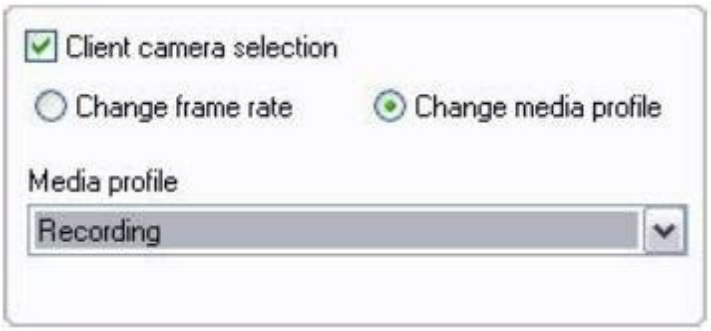
6.1.2.4.1.9 Selection of camera in the client

Selection of camera in the client: These configurations are applied in the Surveillance Client and work in the following way: when this camera is selected, its frame rate is changed according to the configurations specified here. For example, when a camera being monitored at 4 frames per second is selected, the frame rate is changed to 10 frames per second.

© 2002 - 2020 by Digifort, all rights reserved

- **Modify the frame rate upon detection**: Activates this feature.
- **Frame rate**: Specify the desired value.

Otherwise, you can configure this feature to change the camera media profile, according to the picture below:



To learn more about Media profile see Media profile

6.1.2.4.1.10 Media profile for access via mobile

The system allows the use of a differential media profile for viewing via mobile devices.

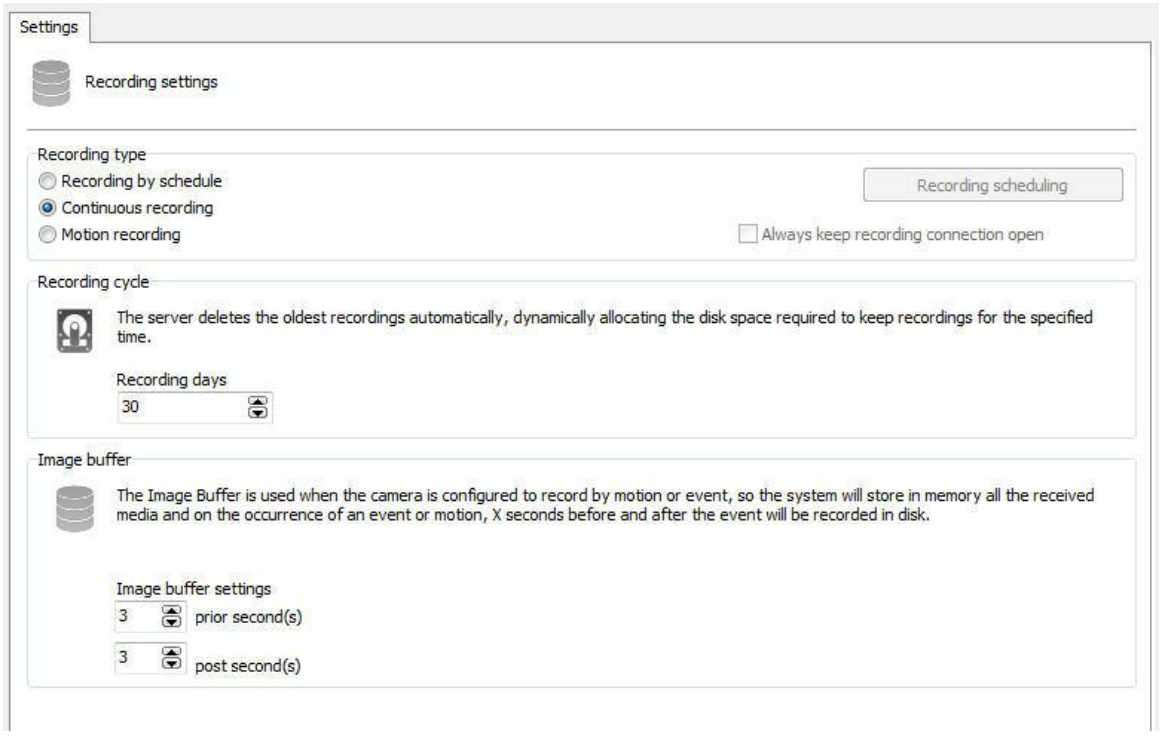
The access via mobile devices generates a processing load on the server since the system needs to transcode the video before sending it to the device. If the camera is set to record megapixel images, the transcoding process can be cumbersome, generating an unwanted processing load to the server. This new option allows the administrator to select a lower-resolution media profile to perform the transcoding, leading into a lower processor use.

To learn more about Media Profile check Media Profiles

6.1.3 Recording

The next screen has the recording settings of the camera:

© 2002 - 2020 by Digifort, all rights reserved



6.1.3.1 Type of recording

Digifort Enterprise offers three types of recording: continuous recording (always record), recording by motion detection, and recording by scheduling. Continuous recording will record to disk all images received by the camera. Recording by motion detection will record images only when there is motion. Recording by scheduling permits the configuring of recording times in which the camera will always record, record by motion detection, or not record. In most cases, recording by motion detection or event is the most appropriate, as it drastically reduces disk space used. To learn more about recording by motion detection see How to configure the Motion Sensor.

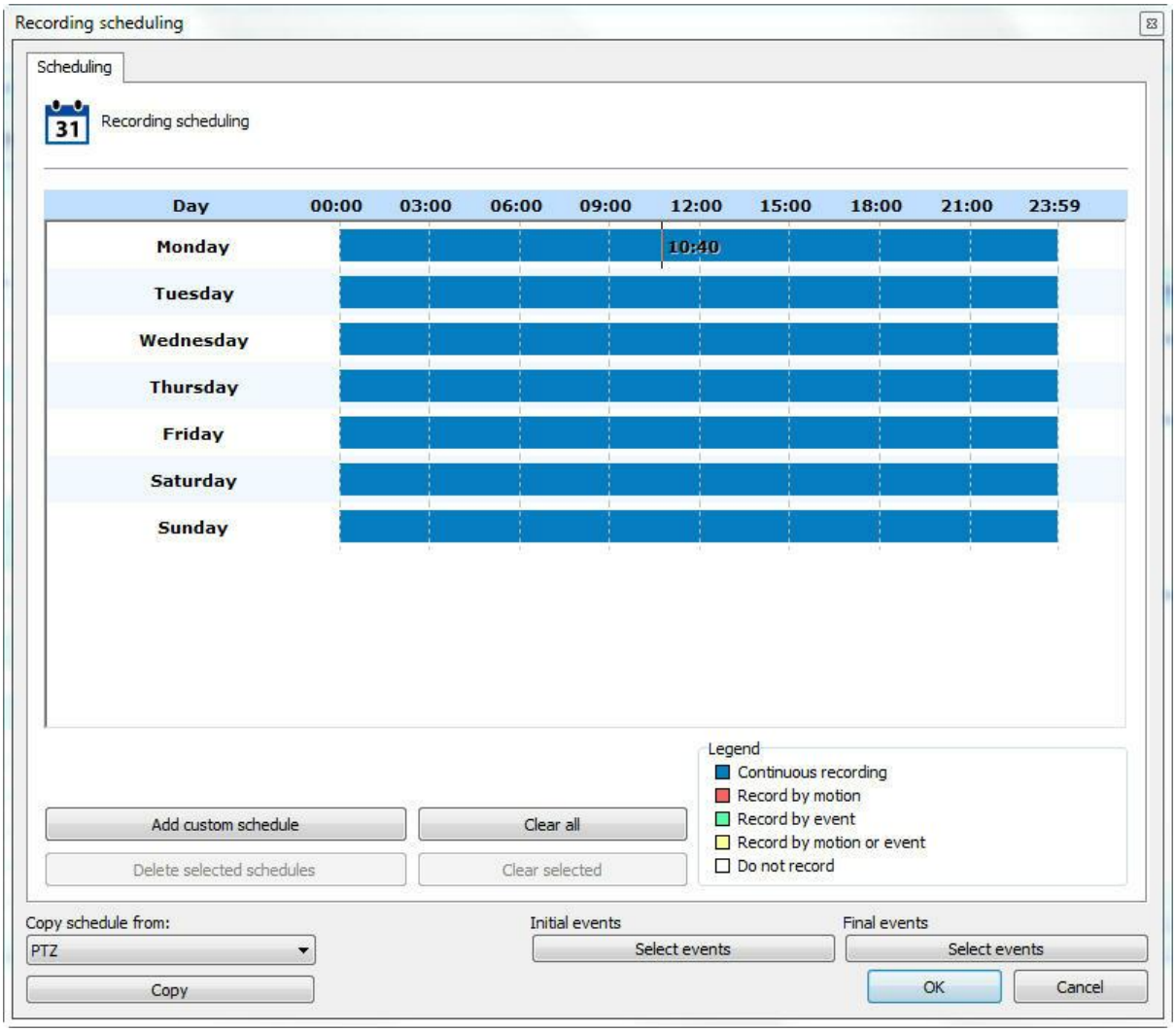
• **Always keep the recording connection open**: Maintains the camera recording stream always transmitting in case of recording by events. Thus the prerecording buffer works normally.

6.1.3.1.1 How to configure the scheduling of recording

To configure the schedule of recording click on the Schedule of recording button.

© 2002 - 2020 by Digifort, all rights reserved

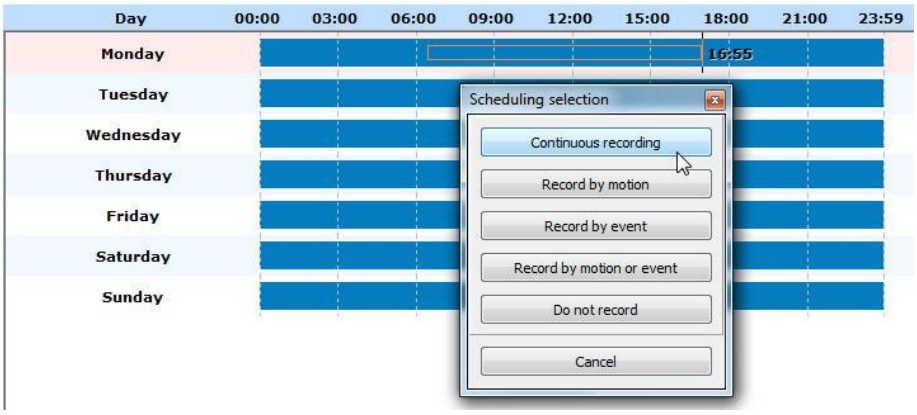
The scheduling screen below will open:



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

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

© 2002 - 2020 by Digifort, all rights reserved



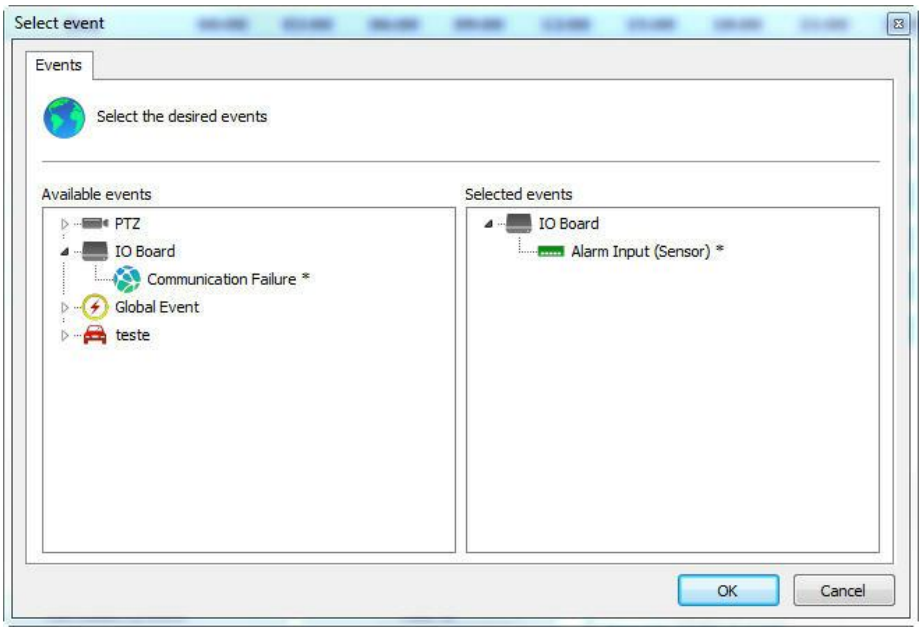
You can select multiple days to apply a configuration to all at the same time. Simply click on the days of the week you want.
In the picture below the first three ones were selected:



The options for scheduling are:

- **Always record**: Activates the continuous recording from the camera during specified time. This option is represented in blue.
- **Record by motion:** Activates the recording by motion in the camera during the specified time. This option is represented in red.
- **Record by event**: Activates the recording by event in the camera during the specified time. This option is represented in green.
- **Motion and event**: Activates the recording by motion detection and by detection of camera events. This option is represented in yellow.
- **No recording**: Disables the camera recording during the specified time. This option is represented in white.
- **Cancel**: Cancels the creation of scheduling during the specified time.
- **Select Initial and End Events button**: If the schedule type is configured to record by event, click on this button to configure the event that starts or ends the recording of camera images in the server. When you click on this button, the following screen appears:

© 2002 - 2020 by Digifort, all rights reserved



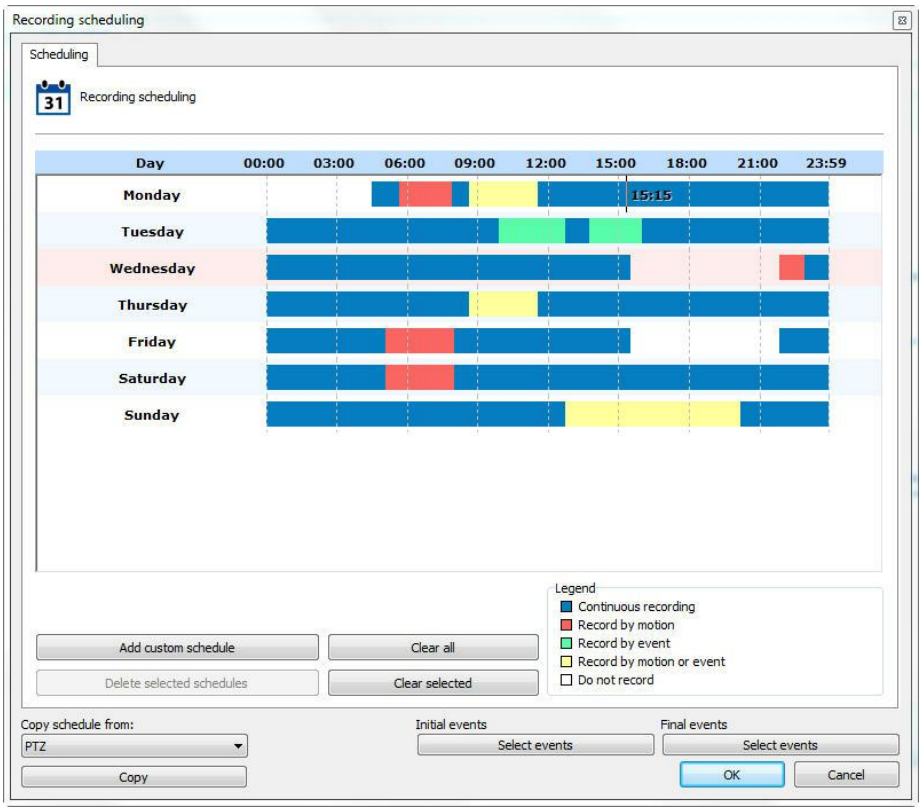
This screen presents two lists, the list of available events and the list of selected events.

The available events list displays the list of all cameras and alarm devices registered in the system, and the selected events list displays all events that are added by the user so that the event occurs.

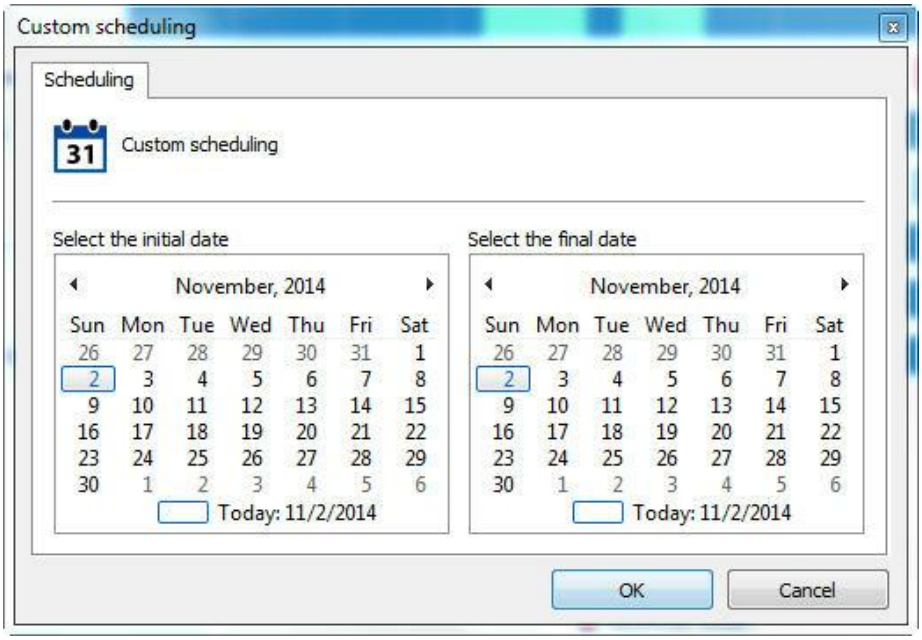
The events that have an "*" beside are the events that will in fact occur, that is, supposing we have timer-linked events, in this case not all the events will occur, but only those that have an "*" beside. Timer events are those that occur in a given user-defined time to trigger another event. To learn about timer events check Timer events.
To select an event, select it in the list of available events and drag it to the list of selected events. To remove an event do the same reverse process.

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

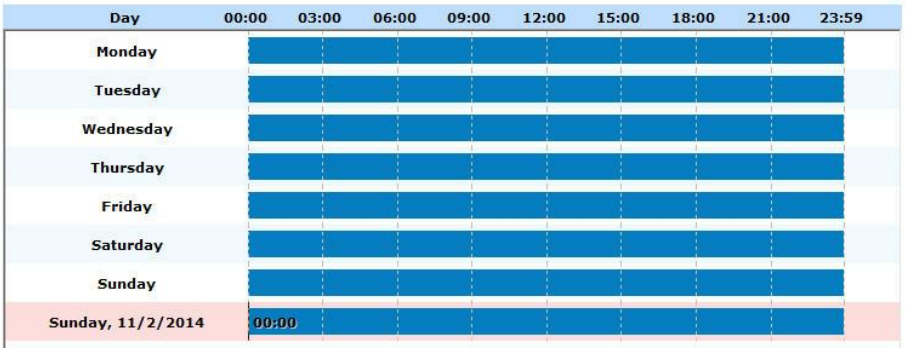
© 2002 - 2020 by Digifort, all rights reserved



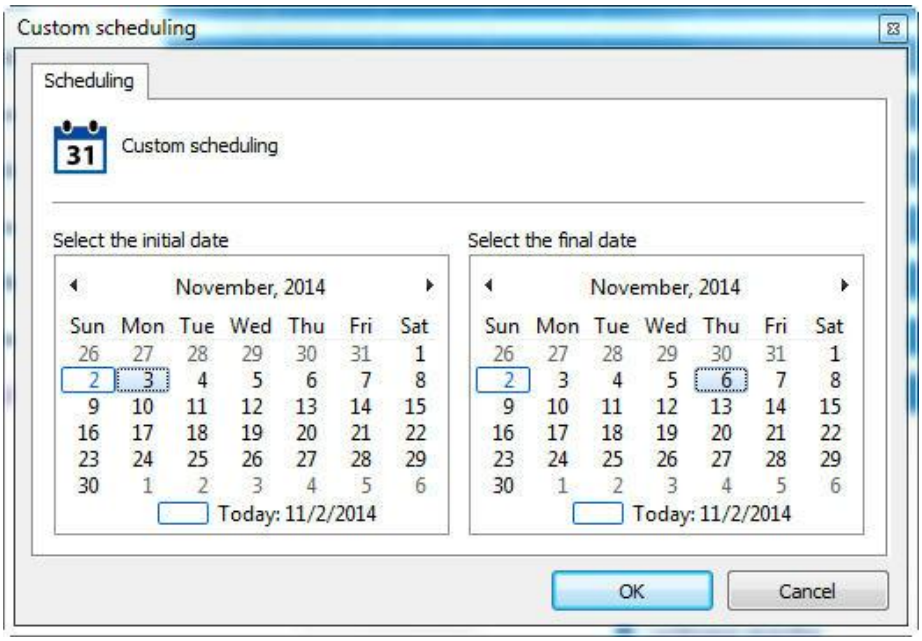
The schedules screen allows a schedule to be made for a specific day of the year, such as a holiday or a special event.
To add a custom schedule, click on the button Add custom schedule. You can choose a single day as shown in the images below:

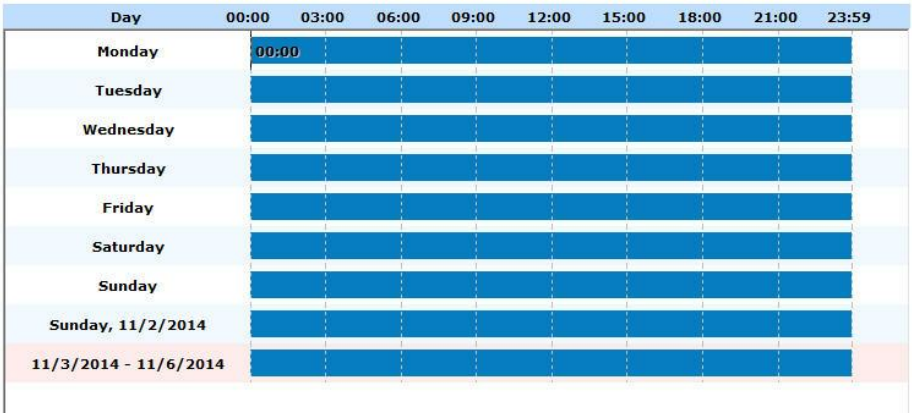


© 2002 - 2020 by Digifort, all rights reserved



Or add a range:

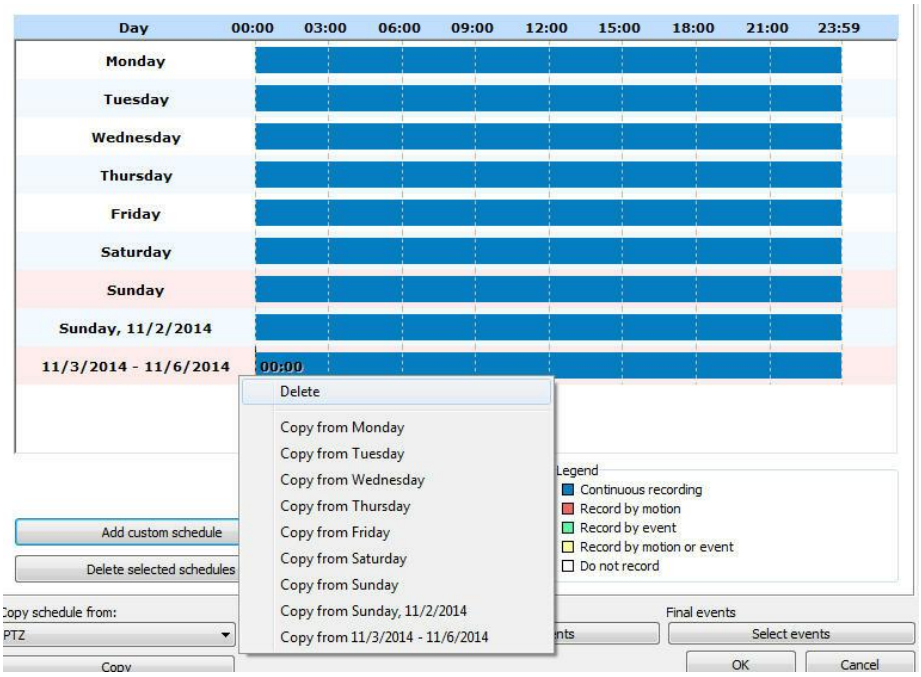




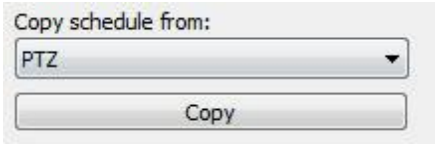
Note: Customized schedules have priority over the normal schedules. For example: In a customized schedule that is set on a Monday, you will overwrite the settings already made for Monday in that specific day.

© 2002 - 2020 by Digifort, all rights reserved

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



You can also copy the scheduling of another object of the system. Simply select it and click on Copy:



6.1.3.2 Recording Cycle

Set this option the number of days Digifort keep the camera recordings on the disc.

Recording by limit of days keeps the camera images stored in disk during only the specified absolute number of days.

For a better understanding of this type of configuration, let's suppose we have these two situations:

1.The recording mode of the camera is configured for continuous recording (always record) and the limit of days of recording is configured for seven days. With this configuration, seven days of images are stored in disk, and when the eighth day comes, the oldest recording (first day) will be deleted.

© 2002 - 2020 by Digifort, all rights reserved

2.The recording mode of the camera is configured for recording by motion detection and the limit of days of recording is configured for seven days. Supposing that, of these seven days, only four had motion, then only four days of images are stored in disk, and when the eighth day comes, the oldest recording will be deleted.

As we can observe by the situations described, we must be very careful with this configuration, since if the camera is recording by motion detection, it's not always recording in disk the specified number of days, since there was no motion on some days, the images of these days are not recorded. This is due to the fact that the configured number of consecutive days will be recorded.

6.1.3.3 How to configure the Image Buffer

The Image Buffer is used when the camera is set to record by motion detection. This way, the system holds in memory the images received, and in case of motion detection, X seconds before and after the motion are also recorded in disk. To learn how to configure motion detection recording check How to configure the Motion Sensor.

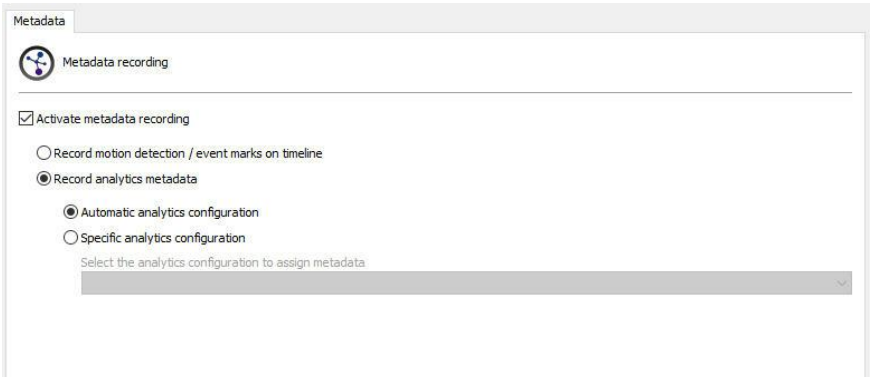
By default, the initial value of this setting is three seconds prior and three seconds after. The greater the number of seconds configured, the greater the processing used by Digifort to store the images.

6.1.3.4 Metadata

Digifort allows metadata recording and playback together with images from the cameras.
Metadata is additional information that will remain available together with the video recording from the cameras. Metadata from analytics, motion detection, and recording by event are supported at this time.

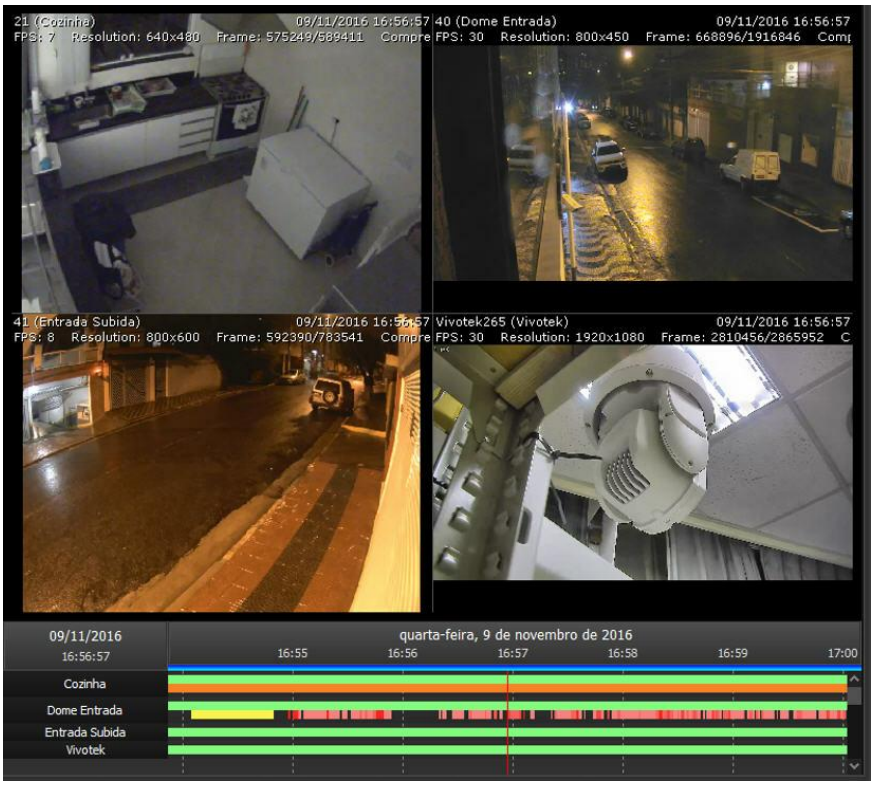
In the Administration Client, it is possible to enable or disable metadata recording and to select its origin. Simply click on "**Activate metadata recording**" and select the desired option, as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved



- **Record motion detection events and recording by event**: Whenever a motion detection event takes place, it will be presented in the media playback as a red bar (to enable motion detection events, see the [the Motion Detection chapter](#)).

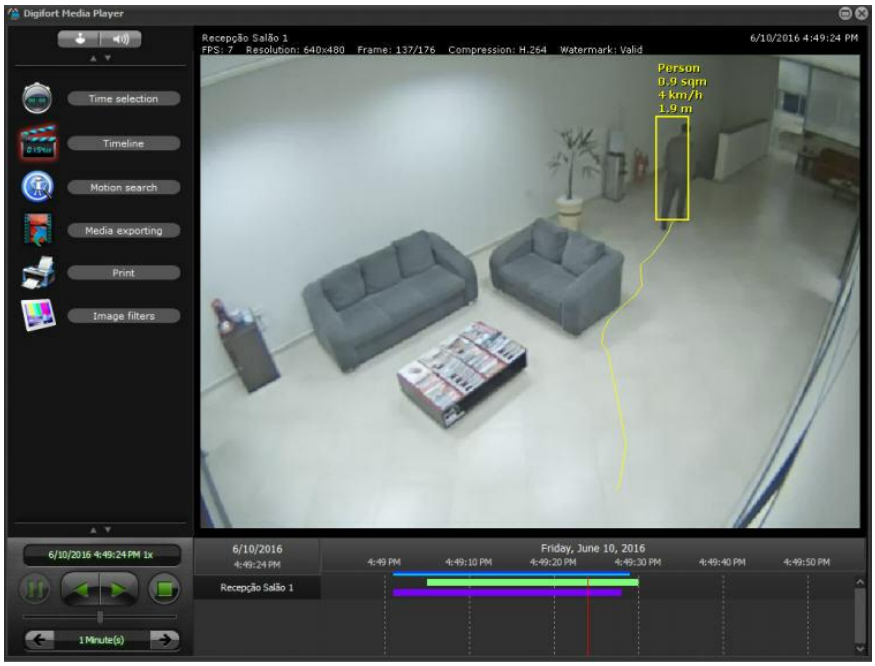
Whenever a recording starts because of an event, it will be marked with a yellow bar in the surveillance (to learn about recording by event, see the [Recording Type chapter)](#).
When configured, it will be possible to verify the metadata together with the recording of the images in the Surveillance Client, as shown in the image below:



- **Record Analytics Metadata**: The system allows the recording of analytics metadata automatically, wherein the system will record the first analytics configuration that is in operation associated to the camera.

© 2002 - 2020 by Digifort, all rights reserved

This allows the recording of analytics metadata for mobile cameras with different analytics configuration in different presets. It is also possible to select manually which analytics will be associated to this camera from the list. When enabled, it will be possible to verify the metadata together with the recording of images in the Surveillance Client, as shown in the image below:



To learn how to configure analytics, see the Analytics chapter.

To learn more, see the Digifort Surveillance Client manual.

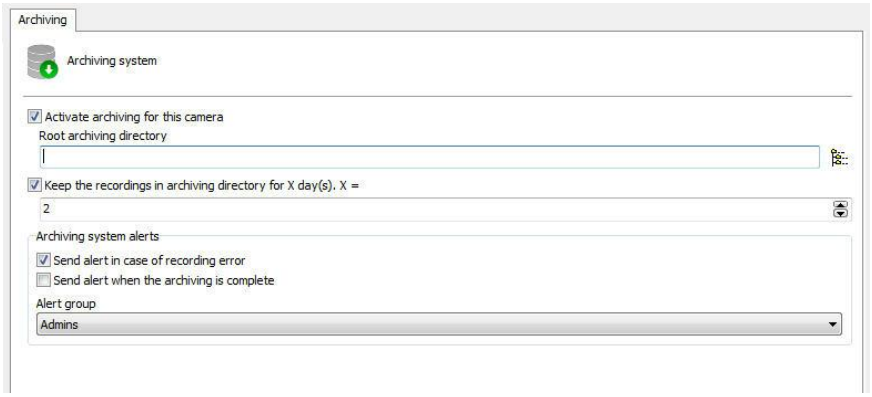
6.1.3.5 Archiving

6.1.3.5.1 How to configure the archiving

Digifort makes it possible for the recordings of a camera to be sent to a different disk or computer in the network, aimed at executing backups in tape or other backup device.
In this configuration, the number of days in which the recordings must be kept in disk or the specified computer of the network can be specified.

To access this feature, click on **Configurations of Archiving**, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



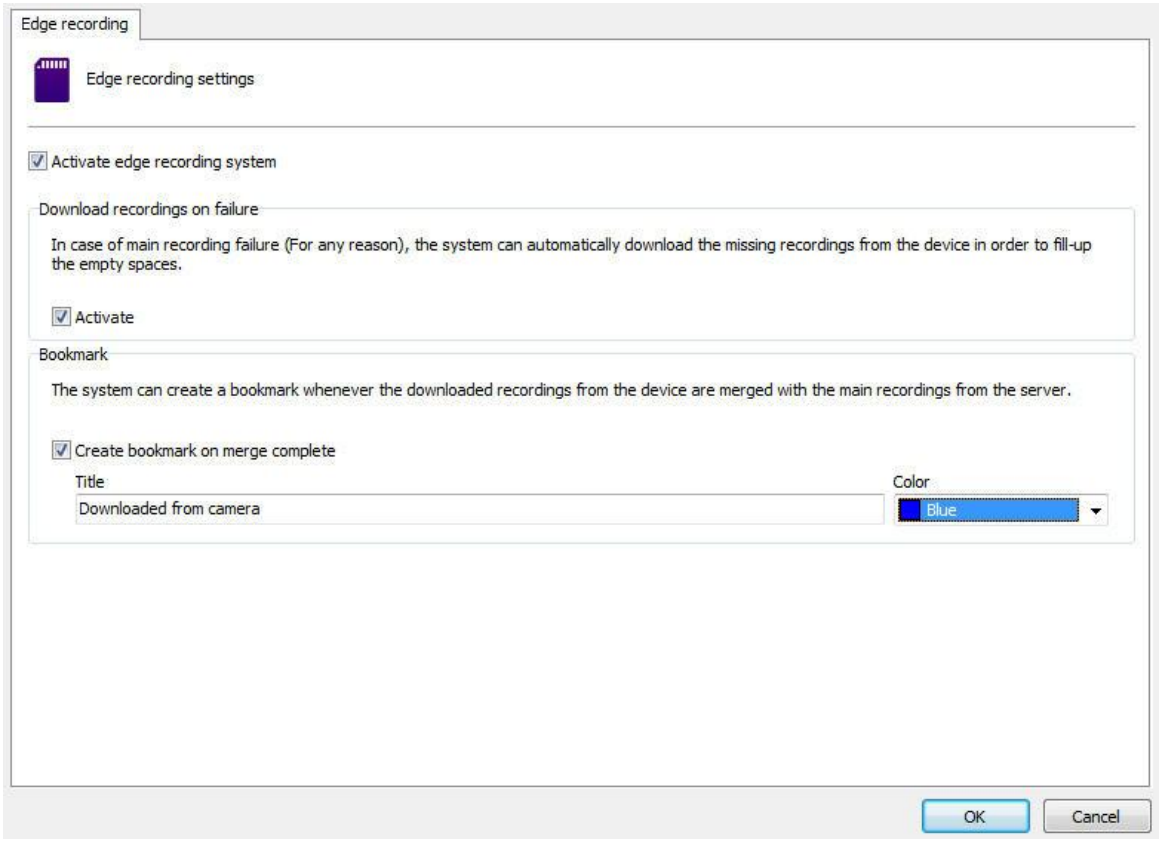
- **Activate the archiving for this camera**: Activates the archiving for the camera being edited.
- **Root Directory of archiving**: Enter the directory in which the archiving will be done.
- **Keep the recordings in the archiving directory for X days**: Enter the number of days the images of the cameras shall be maintained. Exactly the specified last X days will be kept. Previous days will be eliminated.
- **Number of days to synchronize during archiving:** allows the configuration of an operation schedule, to determine when the archiving will be able to work. The archiving system is still a continuous process, however it will only work during the scheduling period. In addition, it is now also possible to configure how many days of recordings that the archive will copy during its processing (Previously the archive only copied the previous day).
- **Operation Scheduling:** Select the days and times that Archiving will work or will be disabled.
- **Agendamento de Operação:** Seleciona os dias e horários que o Arquivamento irá funcionar ou irá ficar desativado.
- **Send alert in case of recording failure**: If some error occurs during the archiving, an e-mail notification can be sent. For this purpose, mark this option and select the desired alert group.
- **Send alert when the system finishes the archiving**: Sends an e-mail notification to the selected alert group when the archiving is successfully completed.

6.1.3.6 Edge Recording

The Edge recording allows, in case of camera connection loss, Digifort to download the image recorded on the camera SD and then attach it to the main recording.

If your camera supports it, click on Activate Edge Recording:

© 2002 - 2020 by Digifort, all rights reserved



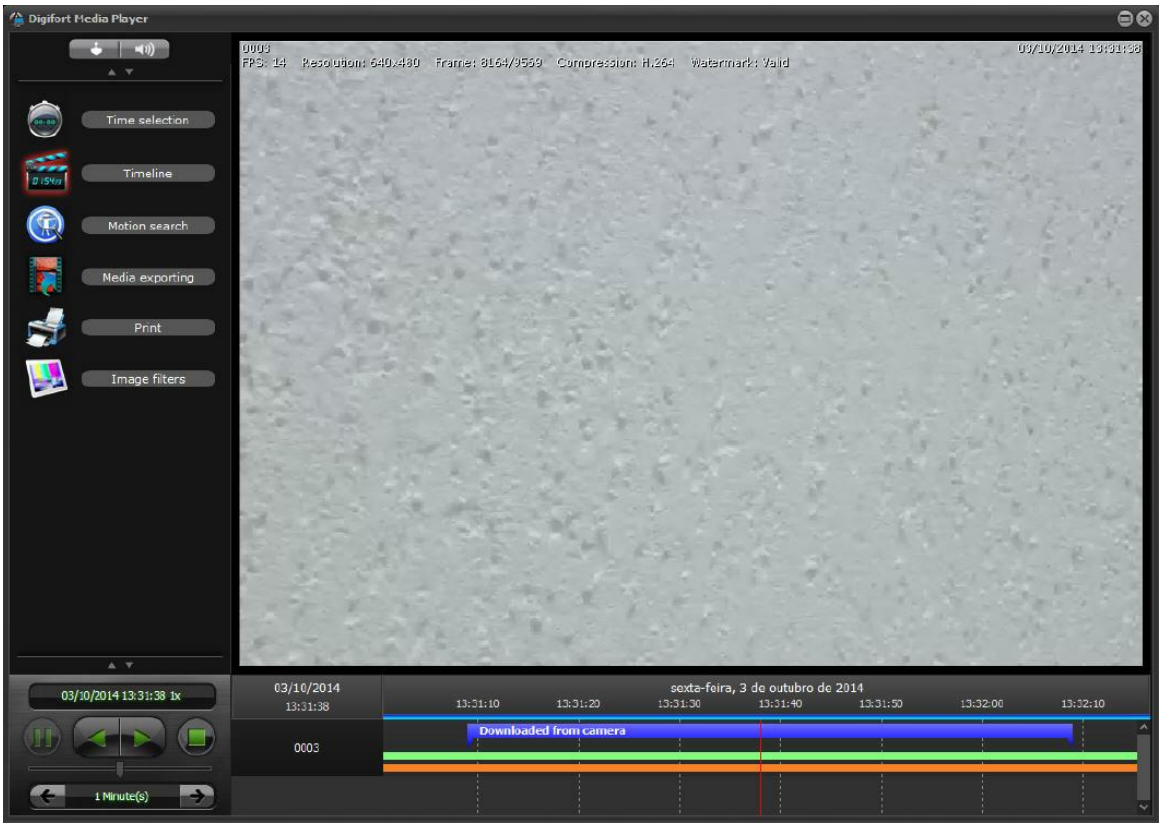
To activate the image download in case of a failure, simply click on Activate as shown above.

You can also create a bookmark when the system has finished the process of downloading and joining the videos with the Digifort main recording.
To do this, simply check the **Create Bookmark when combining recordings option.**

Create a bookmark title and choose a color.

The result on the Surveillance client is this:

© 2002 - 2020 by Digifort, all rights reserved



NOTE: The combination of the video downloaded with the Digifort main video only occurs one hour and thirty minutes after downloading the file from the camera.

To learn more about bookmark check the Surveillance Client manual.

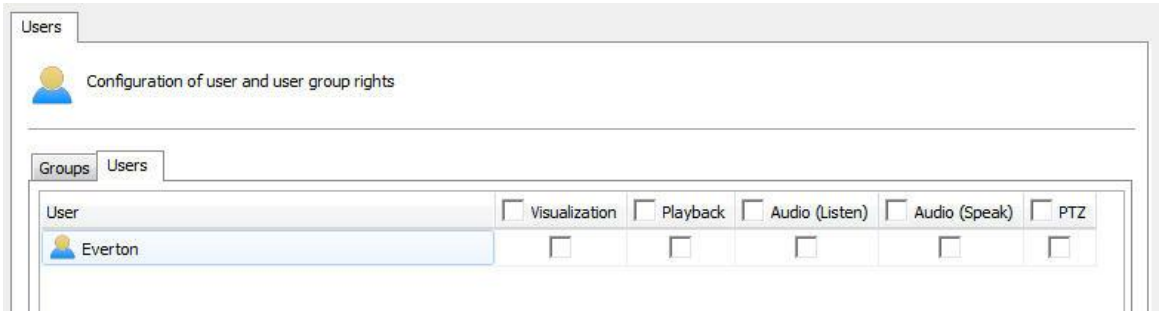
6.1.4 Rights

This area of registration of cameras is reserved for the definition of user rights on the camera.

6.1.4.1 Users

Users and Groups from the system will be automatically listed and may have 5 rights:

© 2002 - 2020 by Digifort, all rights reserved



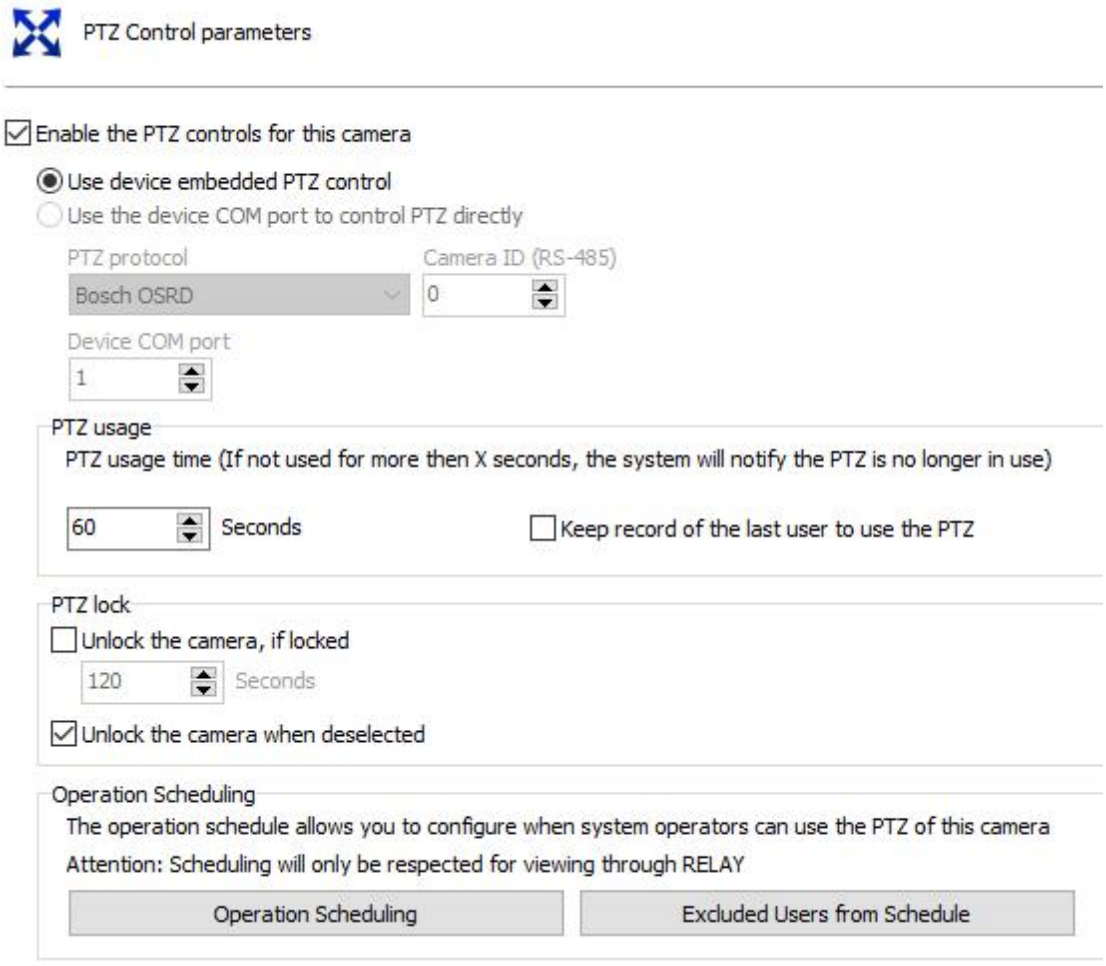
- **Preview:** Check this option if the user can see the camera in live mode in Surveillance Client.
- **Playback:** Select this option if the user will be able to view the recorded images.
- **Audio (Listen):** Select this option if the user can hear the audio captured by the camera.
- **Audio (Talking):** Select this option if you can talk through the speaker of the camera.
- **PTZ:** Select this option if the user will have control over the PTZ camera.

6.1.5 PTZ

PTZ settings allow you to specify the parameters of moving mobile cameras.

6.1.5.1 Configurations

© 2002 - 2020 by Digifort, all rights reserved



The settings screen offers the following features

6.1.5.1.1 Activate the PTZ control for this camera

Activates the PTZ controls for this camera. If this option in unmarked, movement for this camera will not be available.

6.1.5.1.2 Use the device's PTZ features

Mark this option only if the camera being registered is an IP camera. In this case, Digifort will send the PTZ commands directly to the camera. para a câmera.

6.1.5.1.3 Use the device's COM port for the system to carry out PTZ functions directly

Mark this option only if the camera being registered is an analogical camera converted by a video server. In this case, Digifort will send the PTZ commands to the video-server, and then passed on to the camera. para a câmera.

© 2002 - 2020 by Digifort, all rights reserved

6.1.5.1.3.1 Select the PTZ protocol

In case the camera being registered is analogical, select the communication protocol that the video server will use for sending the PTZ commands to the camera.

6.1.5.1.3.2 Camera ID (RS-485)

In case the camera being registered is analogical, select the camera ID that the video server will use for sending the PTZ commands to the camera.

6.1.5.1.3.3 COM port of video server

Select the communication port of the video server with the camera. Generally video servers use the COM 2 port.

6.1.5.1.4 Use of PTZ

By using the PTZ monitoring client the system shows all other users who are in control right now.
In this option you can configure **X seconds** which the system will understand that the PTZ is no longer in use if it is not moved by the operator.

Keeping track of the last user to use the PTZ : The system allows you to view , in the monitoring client, the last user record that moved a camera through PTZ controls.

The PTZ controls use icon in monitoring customer will be semi -transparent , indicating that there is no one using the controls and will inform the user name and the IP of the station used to move the camera when you hold the mouse pointer on the icon :



6.1.5.1.5 PTZ Lock

The PTZ locking system allows the user to lock a camera's PTZ use by setting user priority levels. To learn about PTZ priority, refer to the chapter User Management

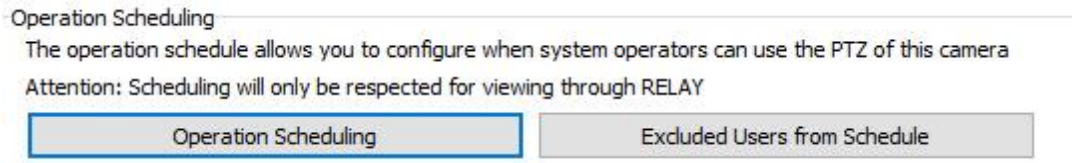
The PTZ locking options include:
- **Unlocking the camera if locked in X seconds:** If a user locks the PTZ,

© 2002 - 2020 by Digifort, all rights reserved

this option allows to set a time in seconds where it is automatically unlocked.

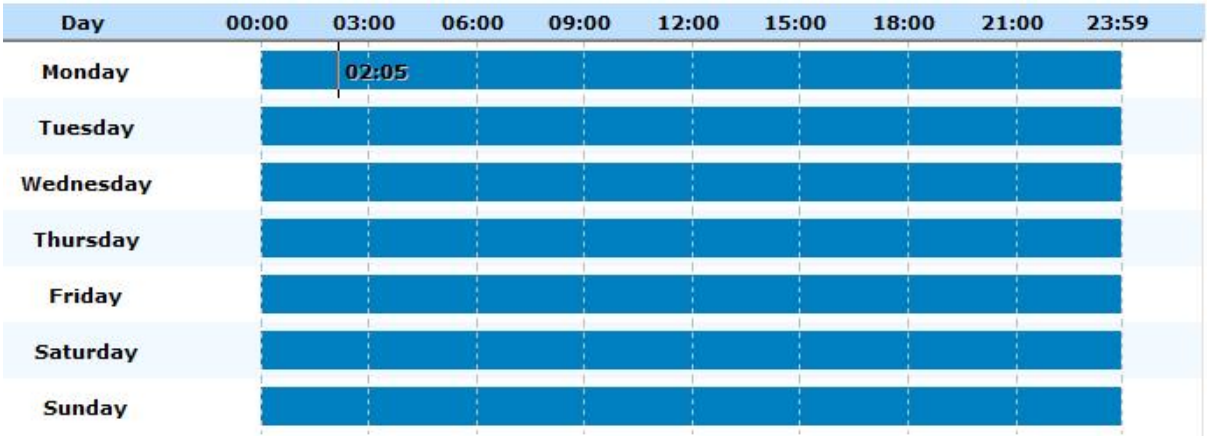
- **Unlocking a camera when not selected**: Unlocks the PTZ of the monitoring client's locked camera if it is not selected.

6.1.5.1.6 Agendamento de Operação



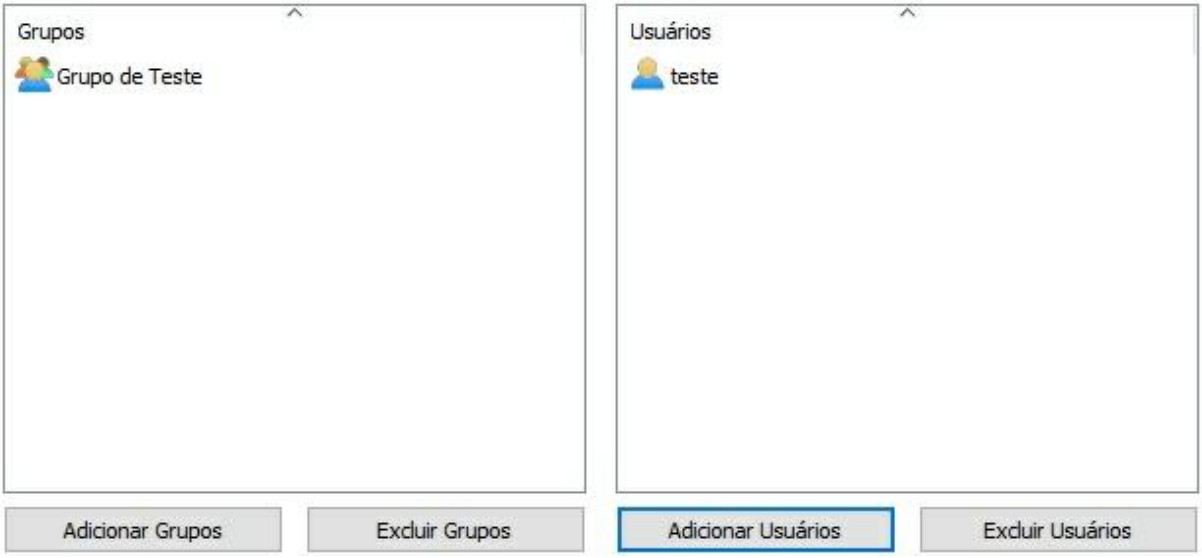
The Operation Schedule allows you to configure when the system operators will be able to use the PTZ of this camera.

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



- **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:

© 2002 - 2020 by Digifort, all rights reserved



Note: To use the Operation Schedule, the camera must be configured for viewing through the Relay Server.

6.1.5.2 Presets

6.1.5.2.1 How to configure the Presets Control

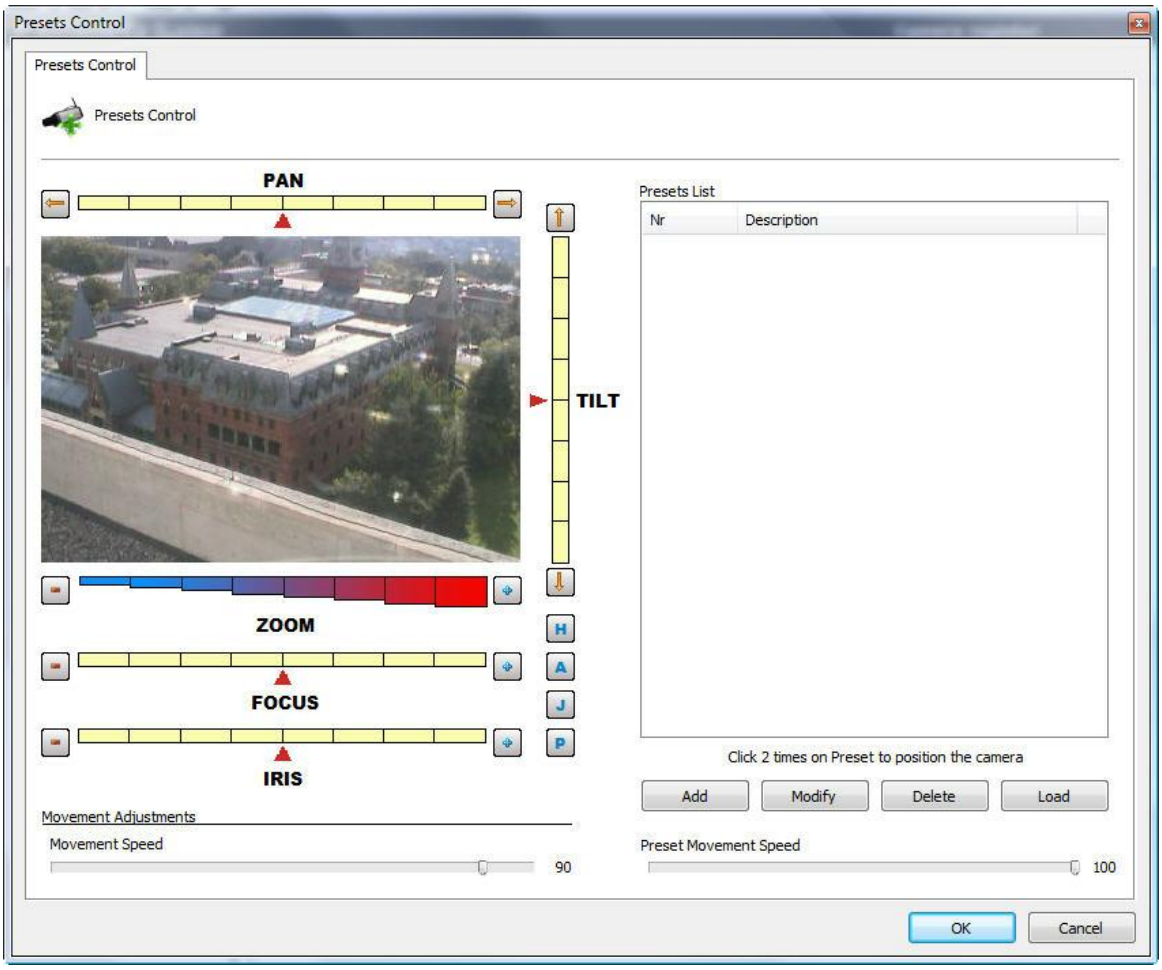
Presets are memorized positions of a movable camera. With this feature, we can memorize positions, and at any moment rapidly send the focus of the camera to the desired position.

Each model of camera supports a certain number of presets. The role of Digifort is to maintain an internal positions list created by the user referring to the list of internal presets of the camera, that is, the position 1, created by the user, is associated to 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 to learn how to call up the configured preset.

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

© 2002 - 2020 by Digifort, all rights reserved



- **PAN bar**: Moves the camera to the left and to the right
- **TILT bar**: Moves the camera up and down
- **ZOOM bar**: Moves the camera's zoom in and out.
- **Focus bar**: Adjusts the camera's focus, in case this isn't done automatically.
- **Iris bar**: Adjusts the camera's iris, in case this isn't done automatically.
- **Home button**: This configuration is located on the button identified by an "H". Clicking on this button causes the camera to be positioned in its initial factory-determined position.
- **Advanced PTZ button**: This configuration is located on the button identified by an "A". Clicking on this button causes the advanced PTZ controls to be displayed. To learn how to use this feature, see Advanced PTZ.
- **Visual Joystick button**: This configuration is located on the button identified by a "J". Clicking on this button causes the visual joystick to be displayed over the allowing you to control its movement by mouse. To learn how to use this feature, see page Visual Joystick.
- **Movement adjustments**:
  - **PTZ by bar**:Define in what way the new camera positioning will be obtained. This configuration can have one of two values:
    - **Absolute PTZ**: The new positioning commands of the camera will be absolute, that is, relative to the Home position..
    - **Relative PTZ**: The new positioning commands of the camera will be relative to the present position
  - **Movement speed:** Movement speed of the camera while its position is being adjusted. This value is expressed as a percentage and its default value is 90% of the maximum speed of the

© 2002 - 2020 by Digifort, all rights reserved

camera.

- **Presets list:** This list contains all of the presets registered for this camera. To position the camera in a preset, double-click on the preset.
- **Add button:** Memorizes the present position of the camera. To learn how to use this feature, see How to create a preset
- **Modify button:** Modifies the selected preset..
- **Exclude button**: Excludes the selected preset.
- **Download button**: Loads the configured camera presets directly to the camera.
- **Preset movement speed**: Specifies the movement speed of the camera from one preset to another. This value is expressed as a percentage and its default value is 100% of the maximum speed.
- **Custom Home Position:** Allows you to customize the home position of mobile cameras. Many cameras do not have / support the home position, so for cameras that do not support this option, the administrator can now configure a camera preset as home.

Important

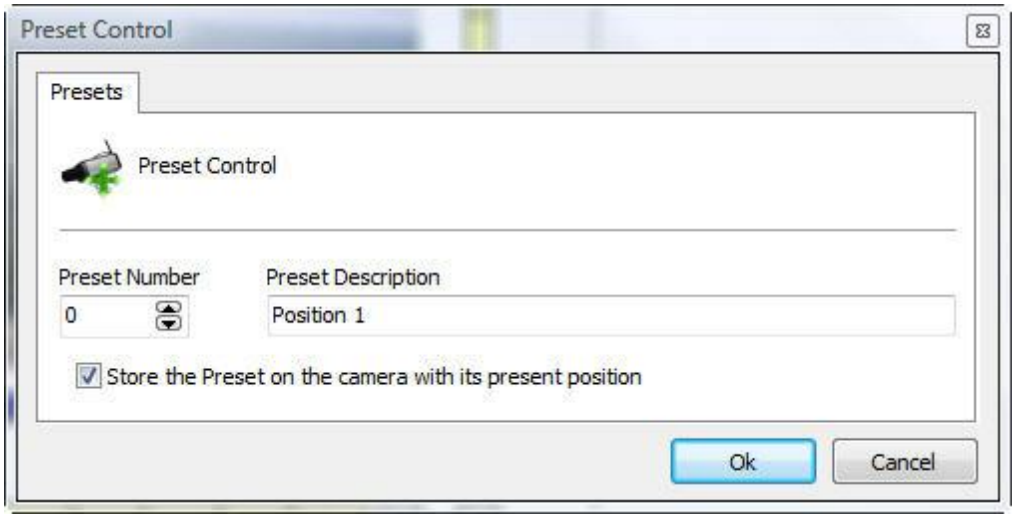
The presets list shows only a list of presets belonging to the camera. All presets created by Digifort are saved in the camera itself. Digifort associates the item of the list with the preset of the camera by way of its number.

Tip

it's possible to position the camera merely by clicking on the image in the place in which you wish to centralize it or use a table joystick.

6.1.5.2.2 How to create a preset

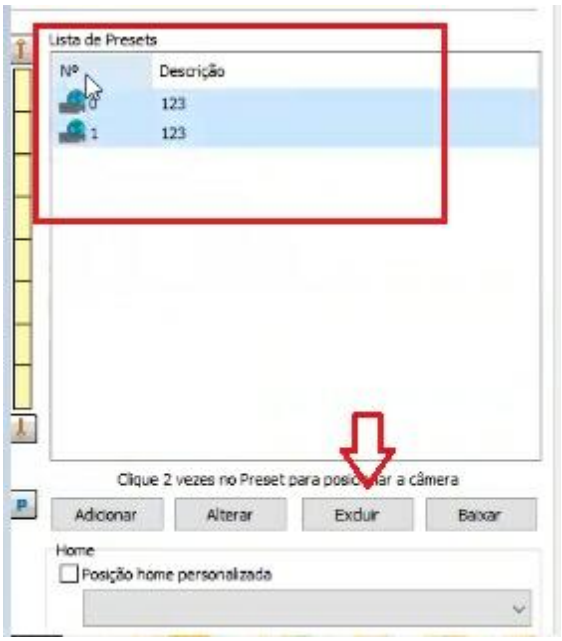
The process of creation of presets is quite easy, simply positioning the camera with the controls presented in the previous topic and clicking on Add, as shown in the picture below:



© 2002 - 2020 by Digifort, all rights reserved

- **Preset number:** The number of the preset that Digifort will associate with the camera's internal presets list.
- **Description of the preset:** A description of the preset being added. This name will be displayed to the user in the Surveillance Client.
- **Record the preset in the camera with its present position:** With this option marked, Digifort will substitute the position of the camera of the informed preset number. In the example of the picture above, the position of the camera will be saved in the preset number zero of the camera. With this option unmarked, Digifort will only associate the description of the preset with the present position of the camera of preset zero.

Note: To delete all presets simultaneously, just select them and click delete:



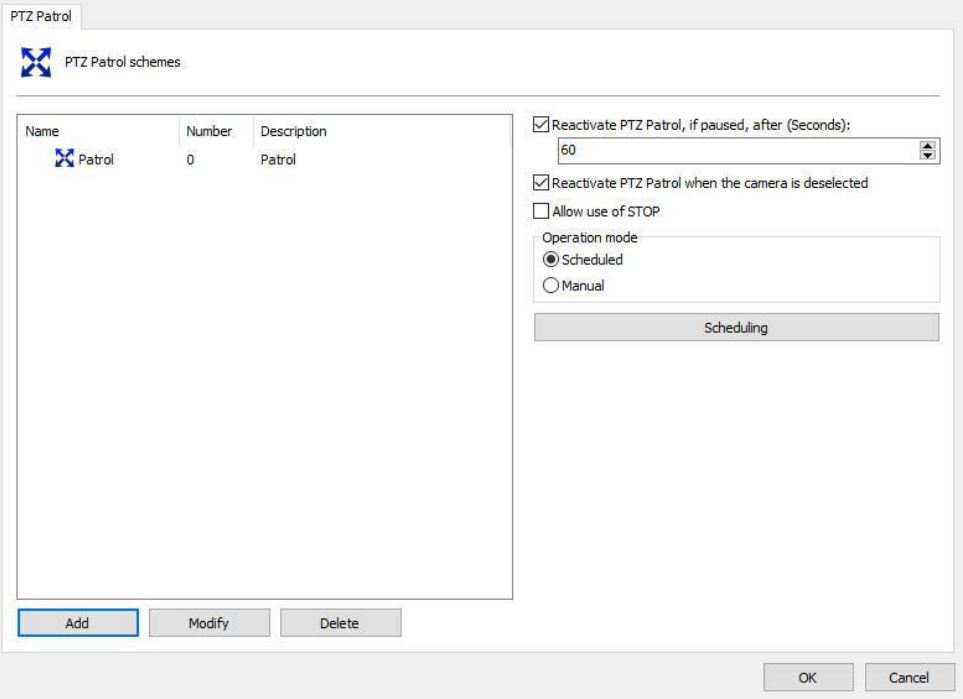
6.1.5.3 PTZ Patrol

6.1.5.3.1 How to configure PTZ Patrol

PTZ Patrol is a feature available in Digifort where it's possible to make the camera pass through the presets previously registered in the system.

To access this feature, click on **PTZ Patrol**, opening the screen below:

© 2002 - 2020 by Digifort, all rights reserved



- **Scheme list:** List of PTZ patrol schemes created for the selected camera.
- **Add button**: Adds a new PTZ patrol scheme
- **Modify button:** Modifies the selected scheme.
- **Exclude button:** Excludes the selected scheme
- **Reactivate PTZ patrol, if paused, after (seconds):** Reactivates the PTZ patrol in the specified time if it was paused in the Surveillance Client.
- **Allow use of STOP:** The system now has a new option that allows the Surveillance Client operator to stop definitely a PTZ patrol. If the patrol is stopped, the system will not automatically reactivate it because automatic reactivation will only work if patrol is paused. This option can be used as an emergency mode where the operator has to stop the patrol operation of a camera and keep it fixed in a position for a long time. By changing the automatic operation of PTZ Patrol, the administrator has the option to activate or deactivate this option. The default value is deactivated.



Pause and stop options in the monitoring client. For more information refer to the surveillance client manual.

Operation modes:

- **Scheduled:** Allows scheduling of surveillance PTZ. In this mode other surveillance camera for the same can not be atividas manually.
- **Manual:** For PTZ surveillance camera in operation in its activation is necessary

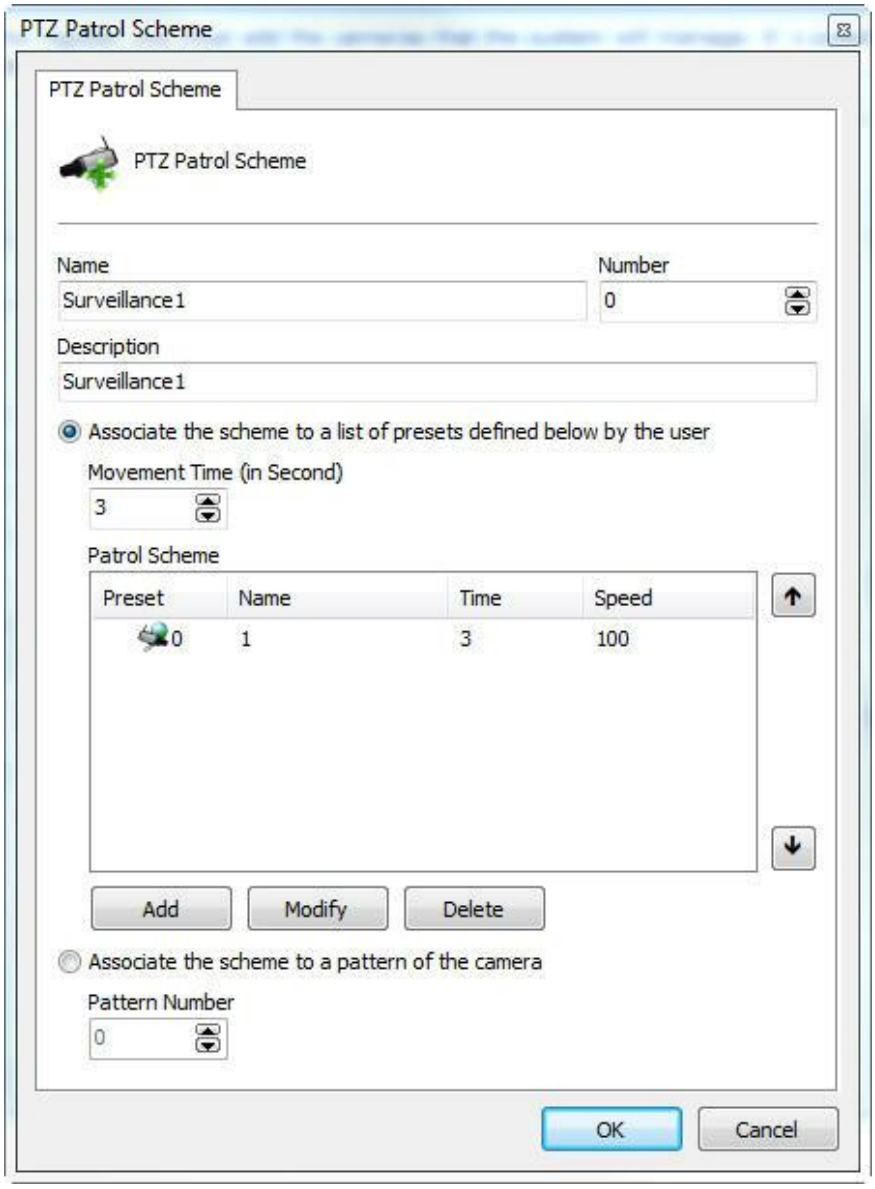
© 2002 - 2020 by Digifort, all rights reserved

on account of manual monitoring Digifort.

- **Scheduling button**: Defines times of day and days of the week in which the PTZ schemes will work. To learn how to use this feature, see : Defines times of day and days of the week in which the PTZ schemes will work. To learn how to use this feature, see [How to configure the scheduling of PTZ Patrol schemes]

6.1.5.3.1.1 How to add a PTZ Patrol scheme

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



- **Name of the scheme:** Inform the identification name of the PTZ patrol to

© 2002 - 2020 by Digifort, all rights reserved

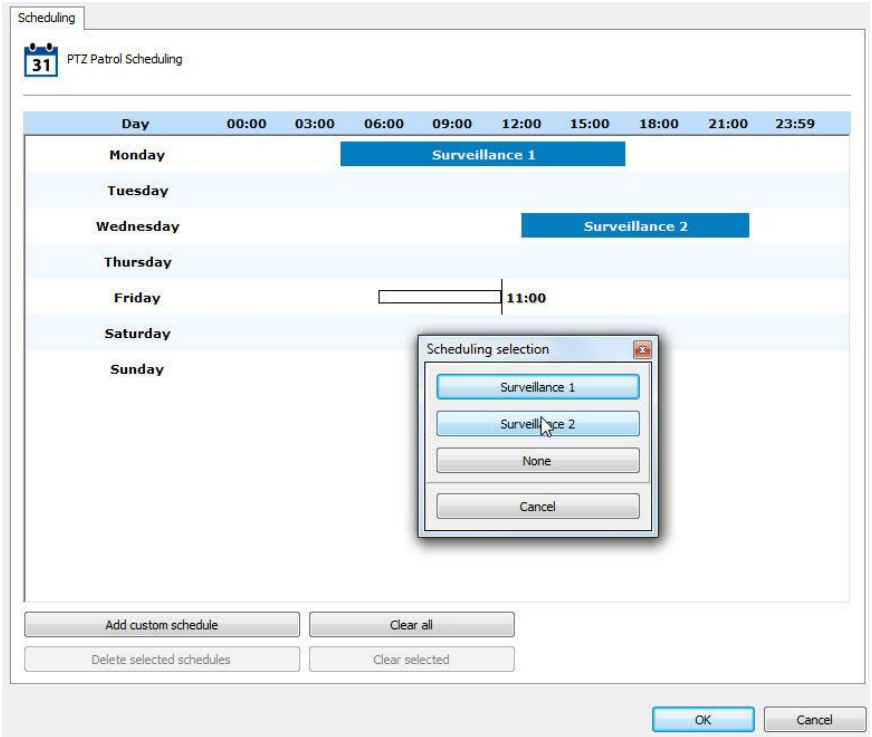
be created.

- **Description of the scheme**: Inform a short description of the PTZ patrol to be created.
- **Associate the scheme with the list of presets defined below by user:** Allows the user to create the list of presets in which the camera will position itself during PTZ patrol.
  - **o Movement time:** Inform the average movement time of the camera from one position to another.
  - **o Patrol scheme:** List of presets added by the user.
  - **o Add button:** Adds a preset to the scheme to be created.
  - **o Modify button:** Modifies the selected preset.
  - **o Exclude button:** Excludes the selected preset.
- **Associate the scheme to a camera pattern:** Select this option if the Recording Server PTZ patrol is configured directly in the camera. To learn how to use this feature, consult the manual of your camera.

o Pattern number: Number of the pattern configured in the camera.

6.1.5.3.1.2 How to configure the scheduling of PTZ Patrol schemes

After registering all of the PTZ patrol schemes, it's necessary to define the hours and days of the week in which these schemes will enter into effect.



In the example in the figure above, the following schedule was configured:

- **00:00 to 06:00:** The Tour scheme will take effect.

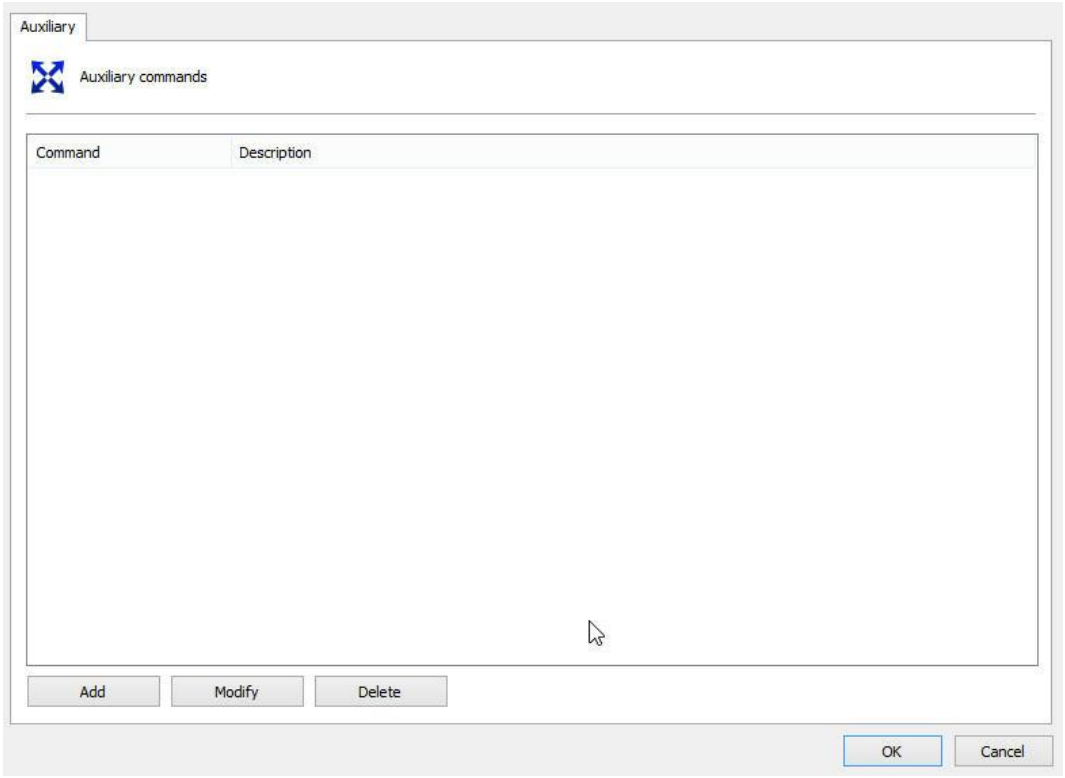
© 2002 - 2020 by Digifort, all rights reserved

- **06:01 to 12:00**: No scheme will take effect, at this point the camera will be immobile.
- **12:01 to 18:00**: The Surveillance scheme will take effect.
- **6:01 pm to 9:00 pm**: No scheme will go into effect, at this point the camera will be immobile.
- **21:01 to 23:59**: In this time range, a new scheme is being configured.

The functioning of this screen is identical to the one on the screen specified in the topic How to configure the scheduling of recording with the difference that the PTZ surveillance schemes previously registered should be chosen.

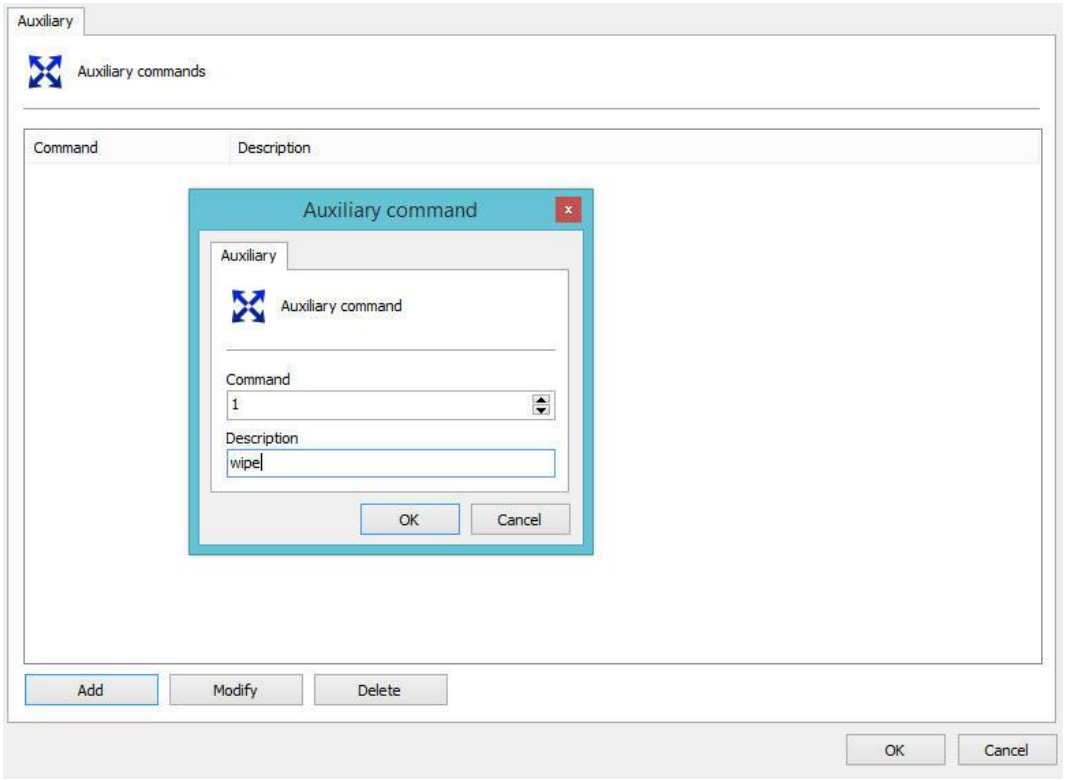
6.1.5.4 Auxiliary

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



Just click on **Add**, enter the ID related to the command, and type the desired name.

© 2002 - 2020 by Digifort, all rights reserved



6.1.5.5 Joystick

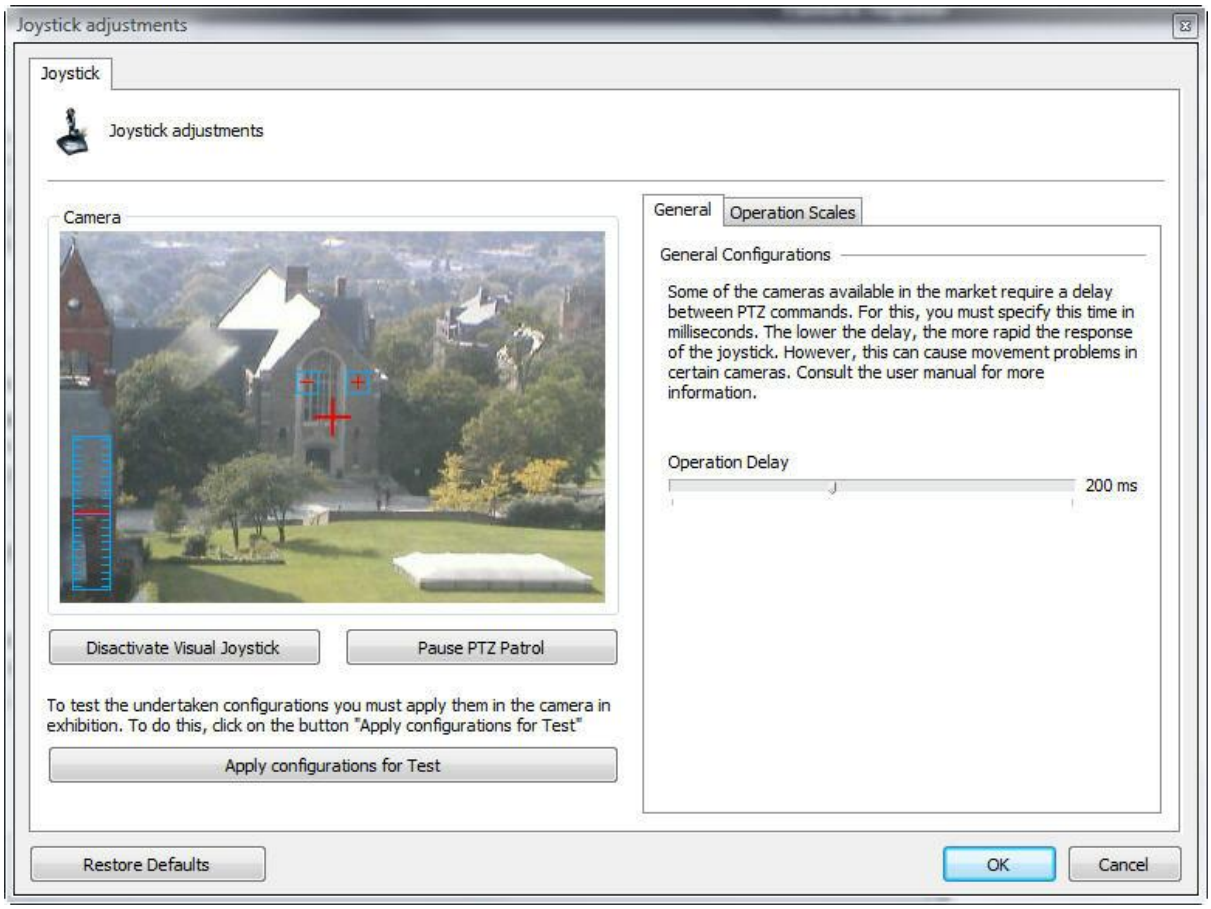
6.1.5.5.1 How to configure the Joystick

The joystick configurations allow its adjustment, aimed at customizing the operating method according to the user's taste.

These configurations involve parameters such as the sensitivity of the joystick and delay of operation.

To access this configuration, click on the **Joystick Configurations** button, located in the PTZ configurations of the camera, opening the screen below:

© 2002 - 2020 by Digifort, all rights reserved



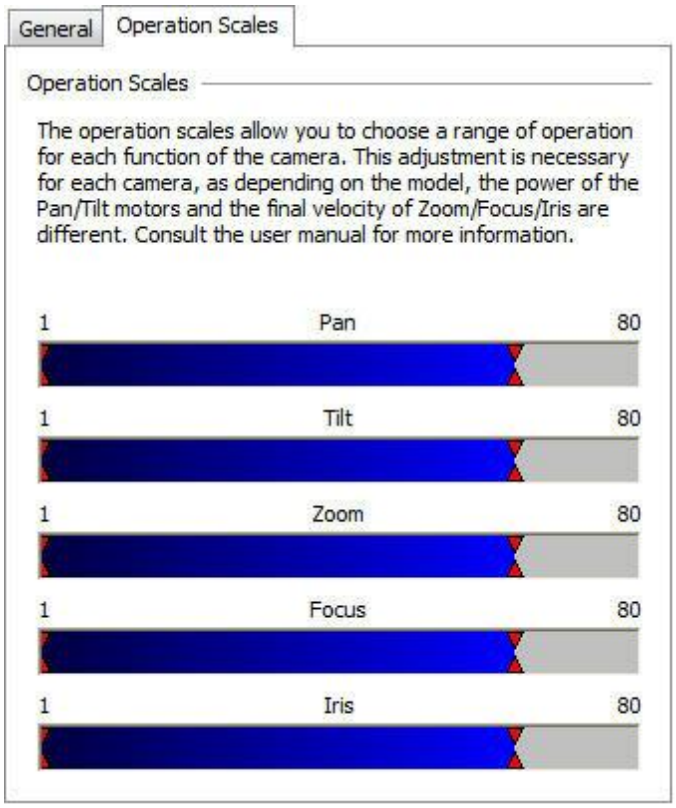
- **Disactivate the visual joystick**: Disactivates the visual joystick. To learn how the visual joystick works, see Visual Joystick.
- **Apply configurations for test**: Applies the prepared configurations only for test. The tests of camera movement with the prepared adjustments should be done on the camera image in the configuration screen itself.
- **Restore Defaults button**: Restores the default configurations of the joystick adjustments.
- **General tab**: Allows access to the configurations of delay of operation.
- **Operation Scales tab:** Allows access to the configurations of the operation scales, defining the sensitivity for the joystick.

The delay of operation is the system's wait time for the command to be sent to the camera. The default of this configuration is 200ms, that is, moving the joystick to the left and holding it in this position for 200ms, the command will be sent to the camera, for example.

The operation scales allow you to choose an operation range for each function of the camera. All of the values are expressed in percentages.

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

© 2002 - 2020 by Digifort, all rights reserved



These configurations are applied to the force of the motors. 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 speed of the camera will be 80% of its maximum speed. It's also possible to specify a minimum movement speed, that is, if you hold the joystick only a few centimeters to the left, the speed of the camera will be 5% of the minimum speed of the camera.

6.1.5.6 Menu Control

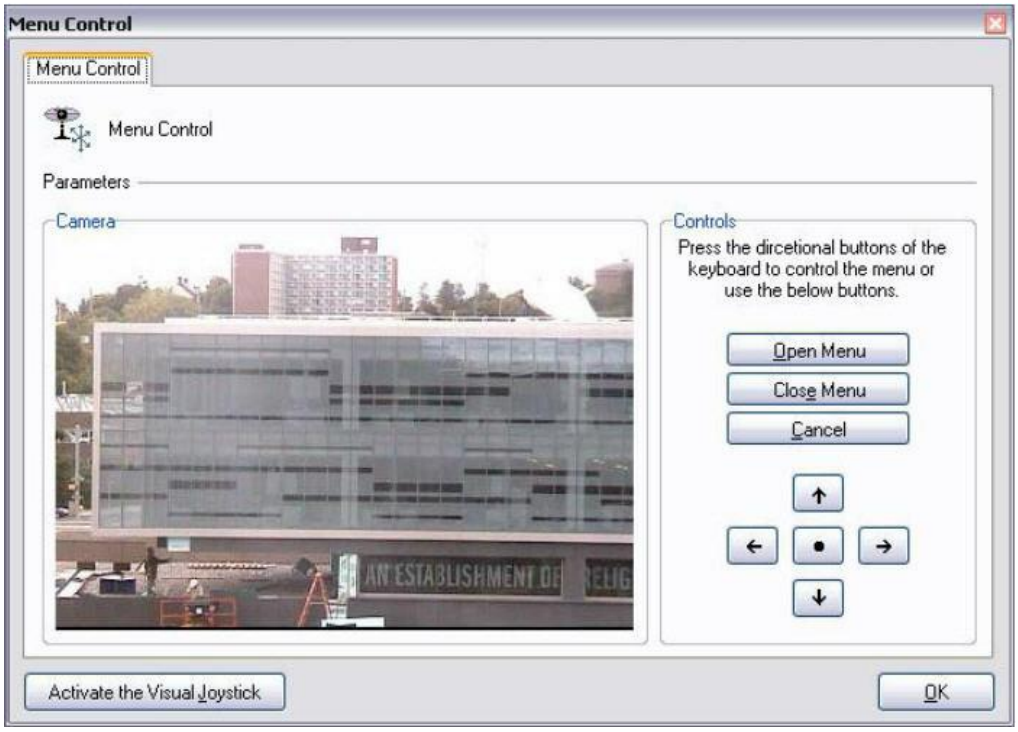
Opens the analog camera configuration screens, allowing the remote configuration of their function such as its ID, for example. To learn how to use this feature, see How to remotely configure analogical cameras

6.1.5.6.1 How to remotely configure analogical cameras

Digifort allows the remote configuration of analogical cameras. This configuration is very useful when we have a camera of difficult access and it's necessary to execute its configuration.

To access this configuration, click on the Open Menu Control button, located in the PTZ configurations of the camera, opening the screen below:

© 2002 - 2020 by Digifort, all rights reserved



- **Open Menu button**: Opens the configurations menu of the camera.
- **Close Menu button:** Closes the configurations menu of the camera.
- **Navigation button:** Navigates through the configurations menu of the camera. Click on the central button to enter in a configuration.
- **Activate the Visual Joystick button**: Activates the visual joystick. To learn how the visual joystick works, see Visual Joystick

6.1.5.6.1.1 Visual joystick

The visual joystick is a tool that simulates the functions of a table joystick. Upon activating the visual joystick over a camera, it will have the appearance of the picture below:

© 2002 - 2020 by Digifort, all rights reserved



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

To carry out zoom operation, use the wheel of the mouse, turning it to front, the image will be brought closer, and to the back pushes the image away. The speed of the zoom can also be controlled and visualized by the control at the left side of the image. The closer the red mark is to the center, the faster the zoom, and vice-versa.

The sensitivity of movement and zoom can be adjusted in the operation scales configurations on page How to configure the Joystick

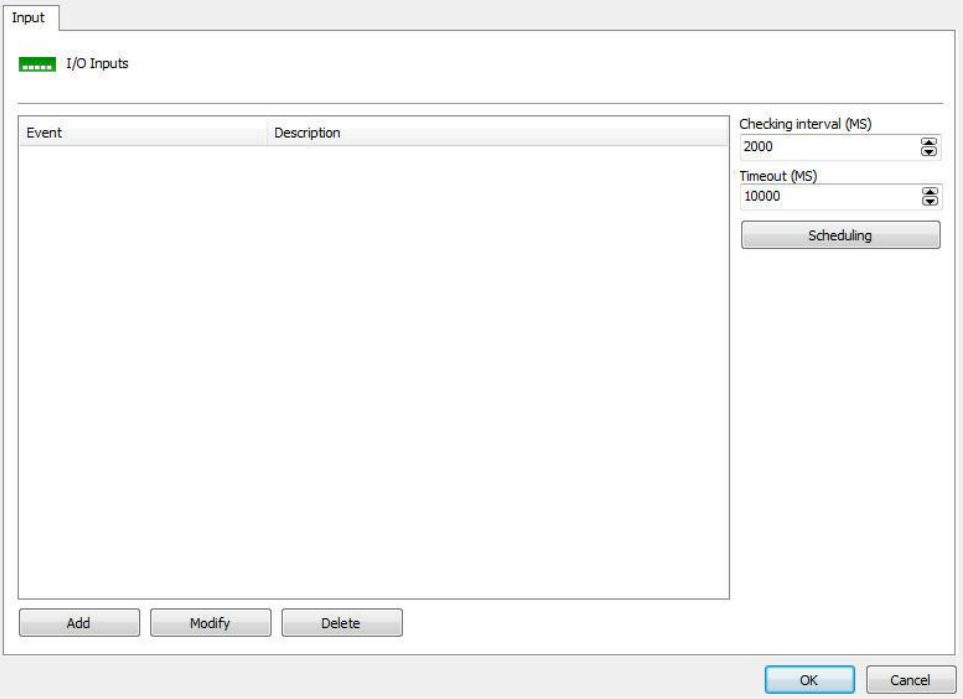
6.1.6 I/O

Digifort is able to control the alarm inputs and outputs of cameras that have this feature.

An I/O input could be, for example, a presence sensor, and an I/O output could be, for example, a siren or an electric lock.

6.1.6.1 How to add input events

© 2002 - 2020 by Digifort, all rights reserved



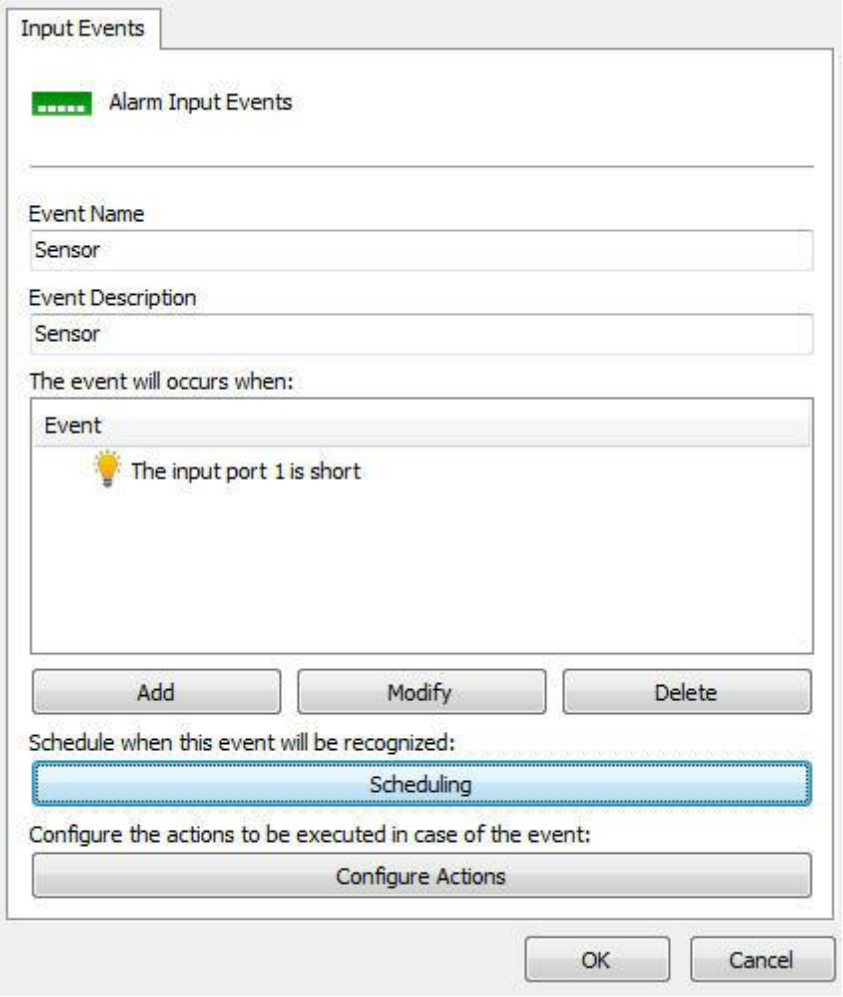
- **Checking interval (ms):** range that Digifort communicate with the camera for recognizing a specific input event, for example, a presence sensor.
- **Timeout (ms):** Interval in Digifort to attempt a new connection to the camera if the current connection is lost.

To add an input event, click on **Add**. To modify and input event, click on **Modify**.

To exclude and input event, click on Exclude. All of these buttons refer to the input events located right below its list.

After clicking on **Add**, the following screen will be displayed:

© 2002 - 2020 by Digifort, all rights reserved



- **Event name:** Name of the camera input event.
- **Description of this event:** Description of the camera input event.
- **The event will occur when:** Fill in the list according to your needs. In the example above, the configuration is for the event to be generated only when port 1 of the camera alarm input is activated. Combinations can be created, such as port 1 activated, 2 activated and 3 disactivated. To add an event click on the **Add** button. To modify and exclude, click on the corresponding buttons. After clicking on the **Add** button, the following screen will be displayed:

© 2002 - 2020 by Digifort, all rights reserved



In this screen, select the input port and its state for which the event being configured occurs.

- **Configure Actions button:** Click on this button to configure the actions that Digifort will execute when this event happens. To learn how to configure the actions, see How to configure the alarm actions.

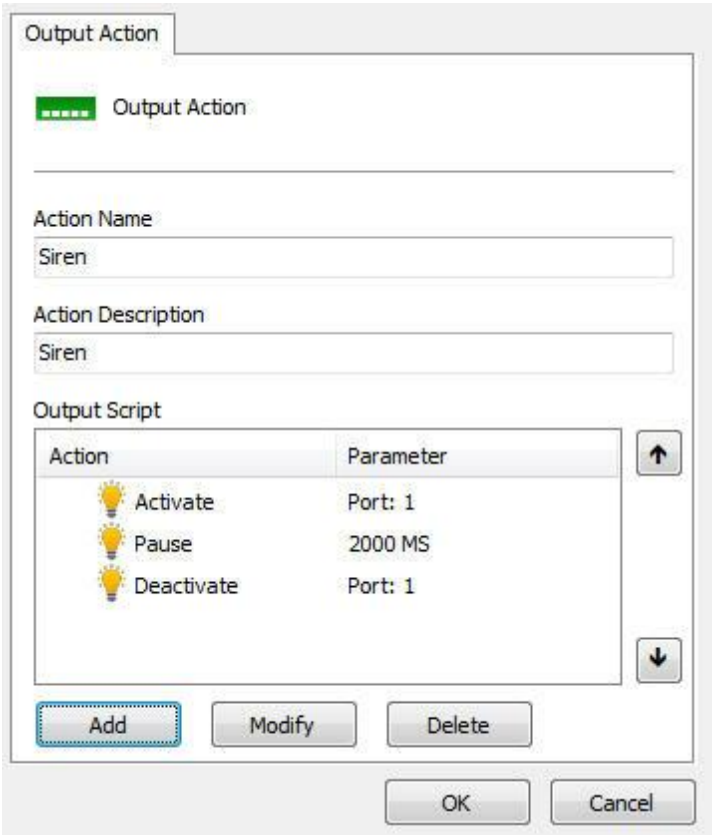
6.1.6.2 How to add output events

Cameras out actions are set in script, that is, a set of parameters executed in the order established by the user.

To add an out event, click on Add. To alter an out event, click on **Alter**. To exclude na out event, click on **Exclude**. All these buttons refer to out events located immediately below your list.

The following screen is shown when you click on Add:

© 2002 - 2020 by Digifort, all rights reserved



- **Name of action:** Type the name of the out action
- **Description for this action**: Type the description for this out action.
- **Out Script**: Shows the list of parametres executed in this event. The picture above shows an example of a siren set off as follows:

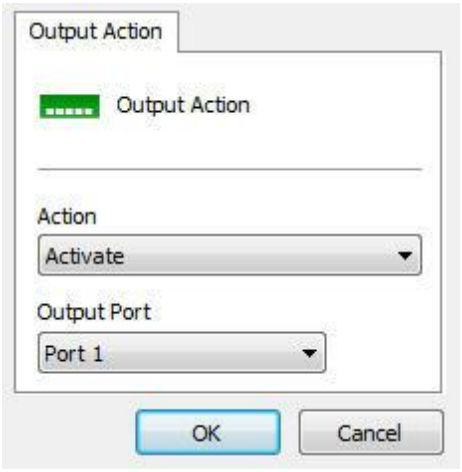
1. Siren turned on
2. Keeps siren turned on for 50 seconds (50000 ms)
3. Turns siren off

Available elements include:
- **Active**: Ativates a commbox outlet.
- **Pause**: Waits X milliseconds to execute the next action in the script.
- **Desactivate**: Deactivates a commbox outlet.
- **Invert**: Inverts the status of a Digifort port.

To add an out action click on **Add**. To alter or exclude click on the corresponding button.

The following screen is shown when clicking on **Add**:

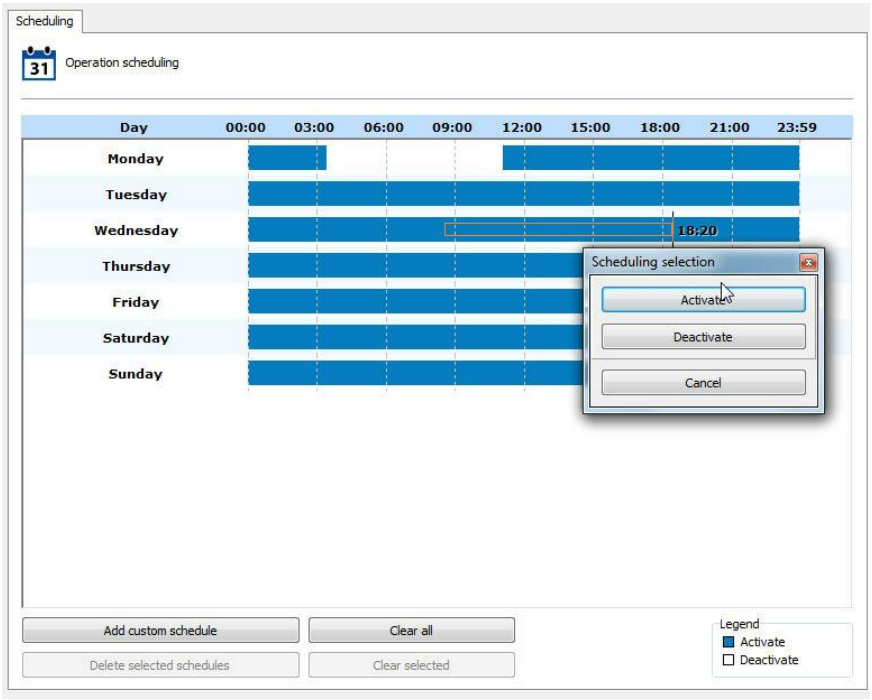
© 2002 - 2020 by Digifort, all rights reserved



In this screen select the action and the port where this action will be executed.

6.1.6.3 How to configure the scheduling of events

To configure the scheduling of events, click on the Open Scheduling of Events button, as shown in the picture below:



The functioning of this screen is identical to the screen specified in the previous topic, except for the types of schedulings:

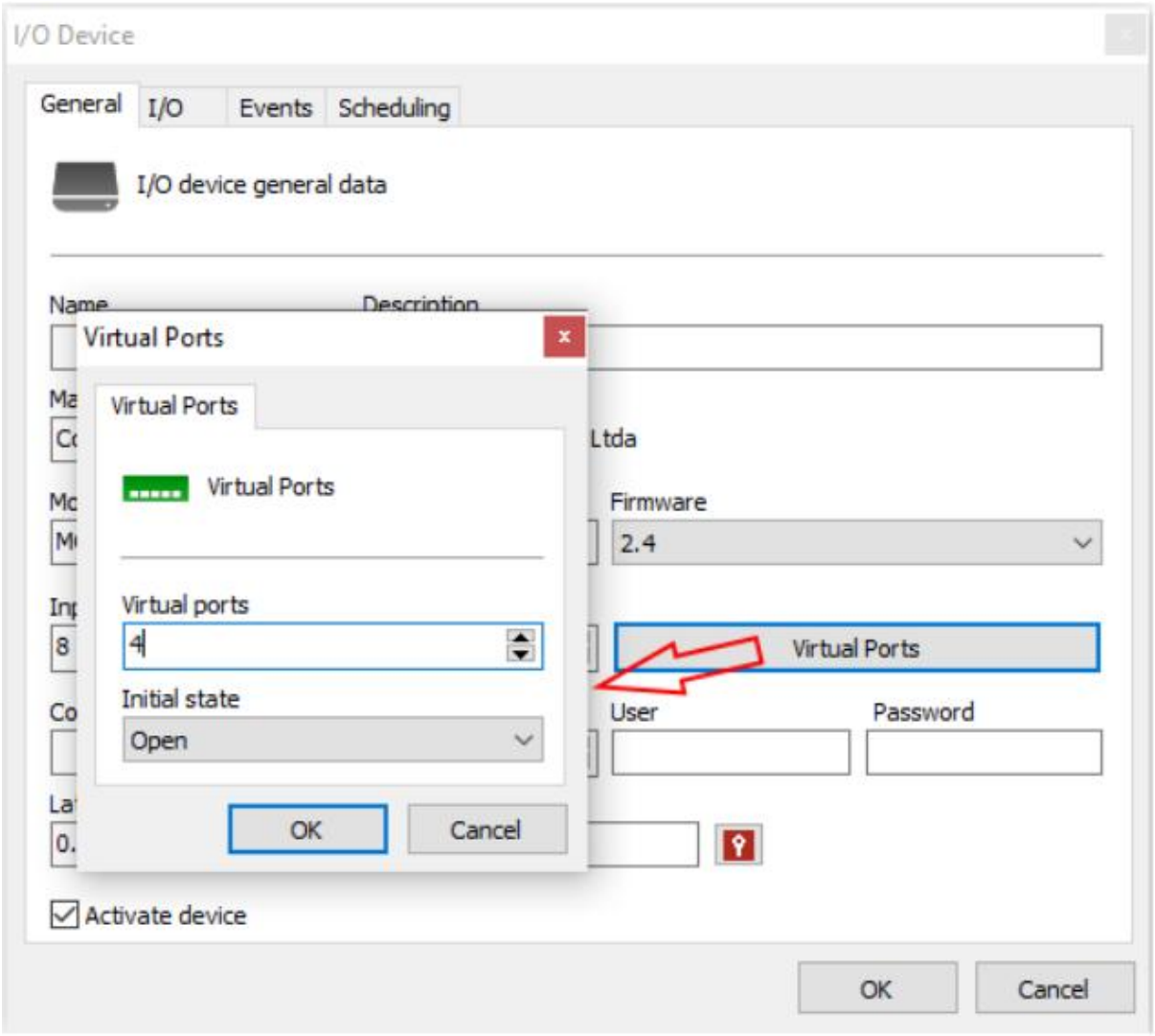
© 2002 - 2020 by Digifort, all rights reserved

- **Activate**: Activates the recognition of events of this camera in the specified hours and days of the week. This option is represented by blue.
- **Disactivate**: Disactivates the recognition of events of this camera in the specified hours and days of the week. This option is represented by white.

6.1.6.4 Virtual I/O

The new virtual I/O port feature can be used for advanced integrations between physical I/O inputs and software events.

Virtual I/O Ports can be defined for I/O Devices or I/O of Cameras:

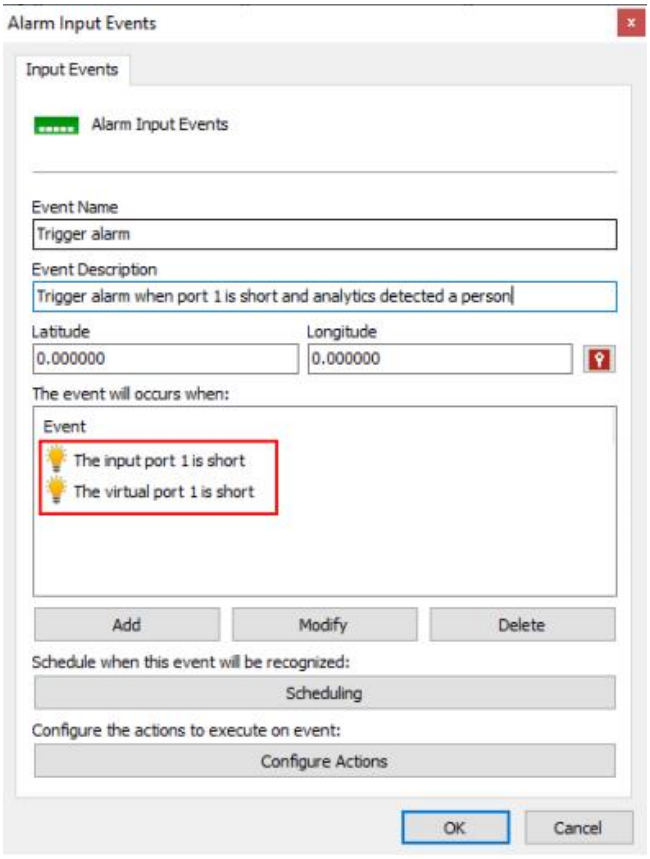


With virtual I/O, you can combine one or more physical alarm inputs with one or more virtual I/O ports. This makes it possible to define, for example, that for an event to take place it is necessary for the alarm

© 2002 - 2020 by Digifort, all rights reserved

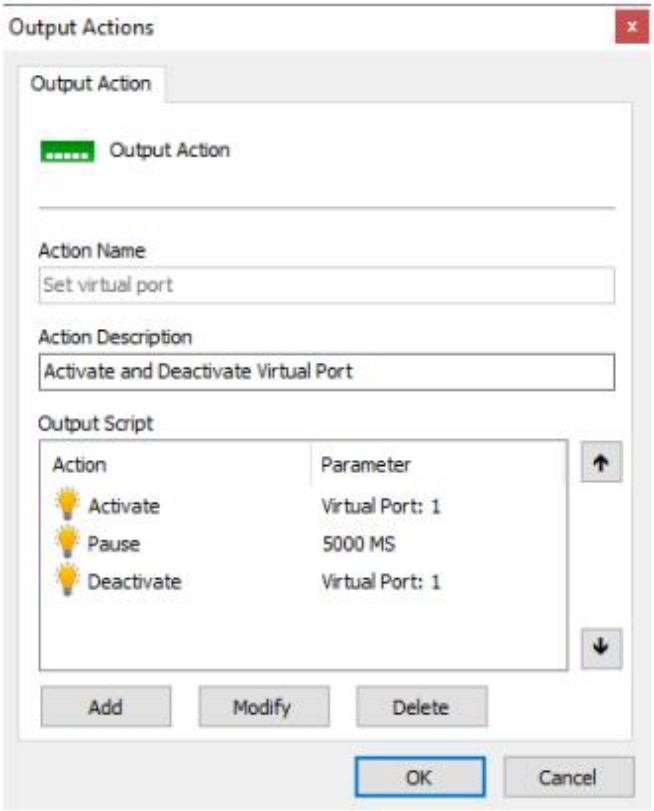
input to be triggered (through the physical input) and a software event to take place (an analytics, for example, or an LPR event) and the virtual door's status be changed.

In the example below, we are specifying that the "Trigger alarm" input event will take place when the device's port 1 is closed and the virtual port 1 is closed. The device's port 1 will be closed through a dry contact (e.g., connected to a door, a motion sensor, a temperature sensor, etc.) and virtual port 1 will be activated through analytics.



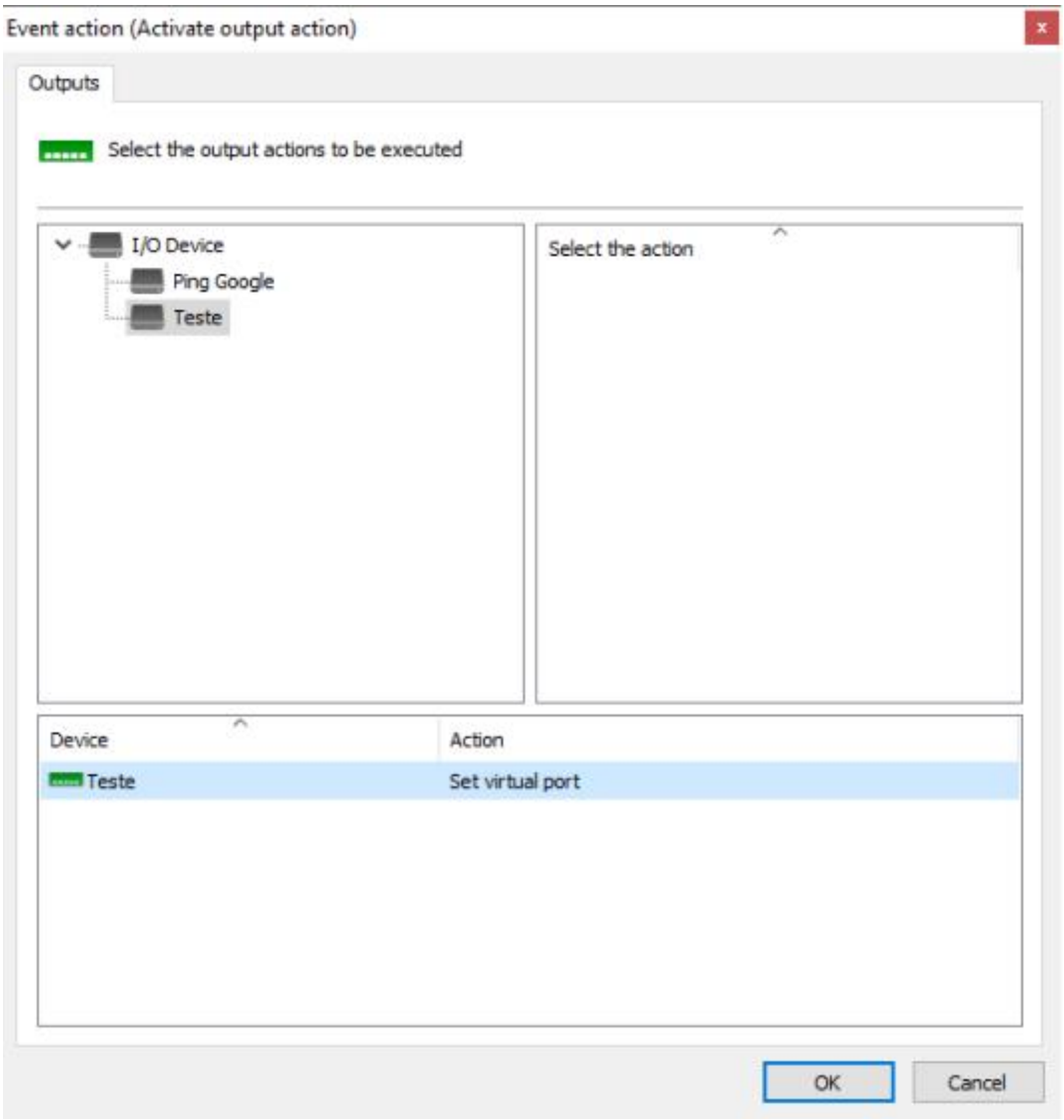
To activate the virtual port, you need to create an output script which activates the port:

© 2002 - 2020 by Digifort, all rights reserved



And this script can be called by any system event, such as, for example, an analytics presence detection:

© 2002 - 2020 by Digifort, all rights reserved



The Virtual I/O is an excellent tool that can be explored to create complex automation and alarm scenarios, combining logical and physical events. Since it is a complex feature, if you face difficulties setting it up, please contact our support team and we will help you succeed.

6.1.7 Events

During the operation of the camera in the Digifort System, various events occur in the camera. These events can be communication failures or alarm recognition events, for example.

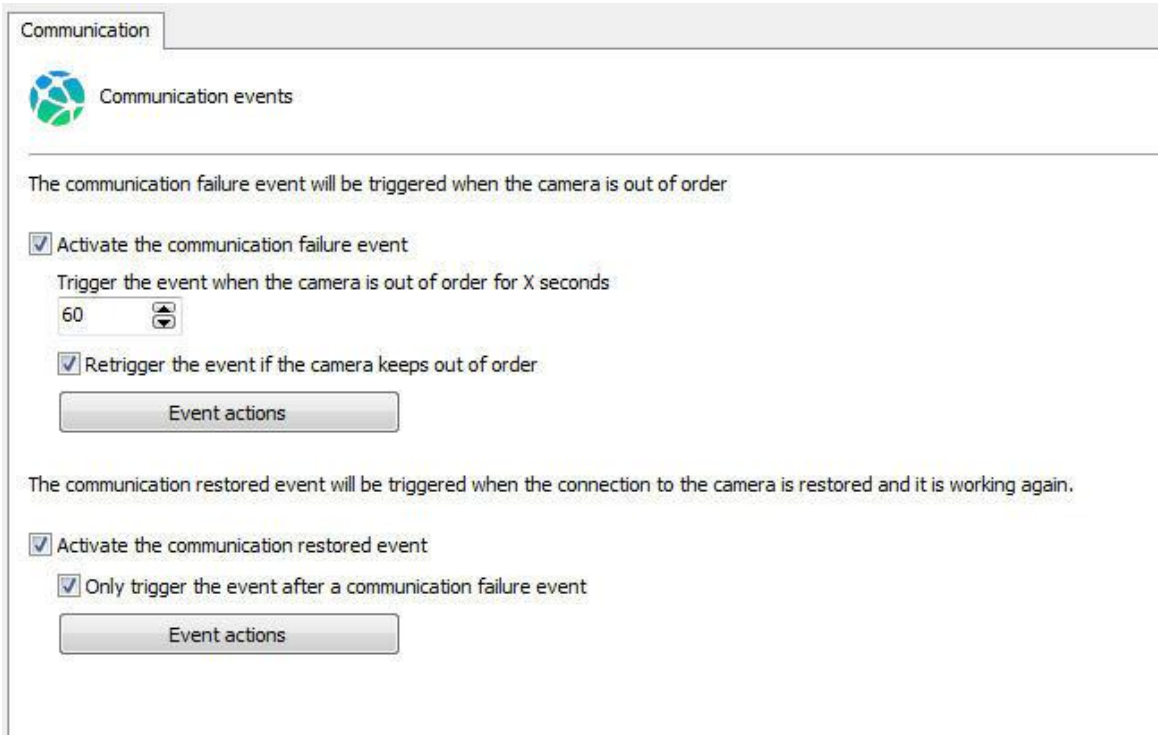
By configuring the events of the camera, it's possible to specify a set of actions that Digifort will undertake when a determined event occurs.

Digifort Enterprise offers control over automatic events, that is, events that occur without user intervention, and manual events, which are events generated based on intervention of the user.

© 2002 - 2020 by Digifort, all rights reserved

6.1.7.1 Communication

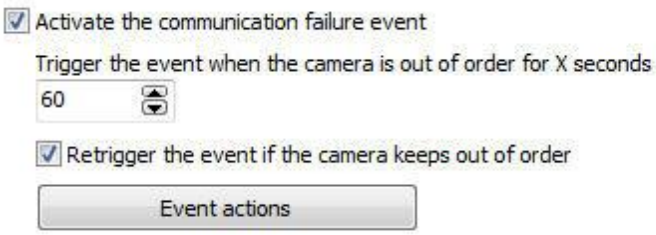
Digifort can generate an alert when a camera is **out of order.**



6.1.7.1.1 Communication failure event

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

The system also allows the event to continue triggering every X seconds while the device is off-line; if the option is disabled, the system will generate the event only once.



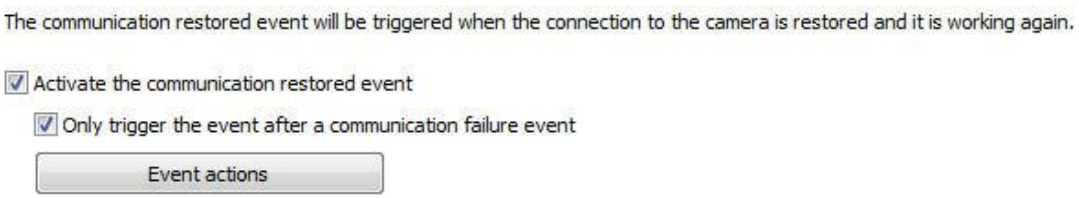
© 2002 - 2020 by Digifort, all rights reserved

To learn how to set the alarm actions see How to set the alarm

6.1.7.1.2 Connection restoration event

The connection restoration event is to generate an event when the device starts do run again in the system.

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



To learn how to set the alarm actions, see How to set the alarm actions

6.1.7.1.3 Devices failure report

The devices failure report will list all faults and communication recovery with the system devices, also providing the failure total time period for each device.
This report uses the communication recovery event to list and calculate fails; therefore, this event must be enabled for all devices.
To learn about generating the report, see the Surveillance Client manual.

6.1.7.2 Recording failure



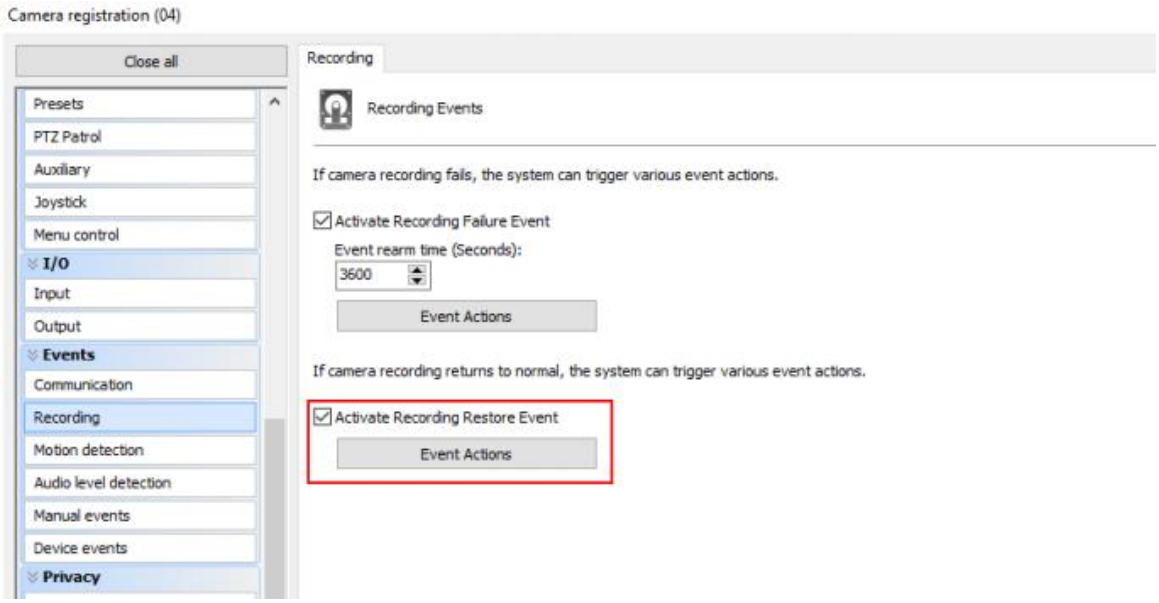
To configure the recording failure event, select the Activate recording failure event option.

To learn how to configure alarm actions, see How to configure alarm actions .

© 2002 - 2020 by Digifort, all rights reserved

The “Recording Re-establishment” event can be triggered when the camera successfully resumes recording after a Recording Failure.

To activate, simply click on **Activate Recording Re-establishment Event** as shown in the image below.

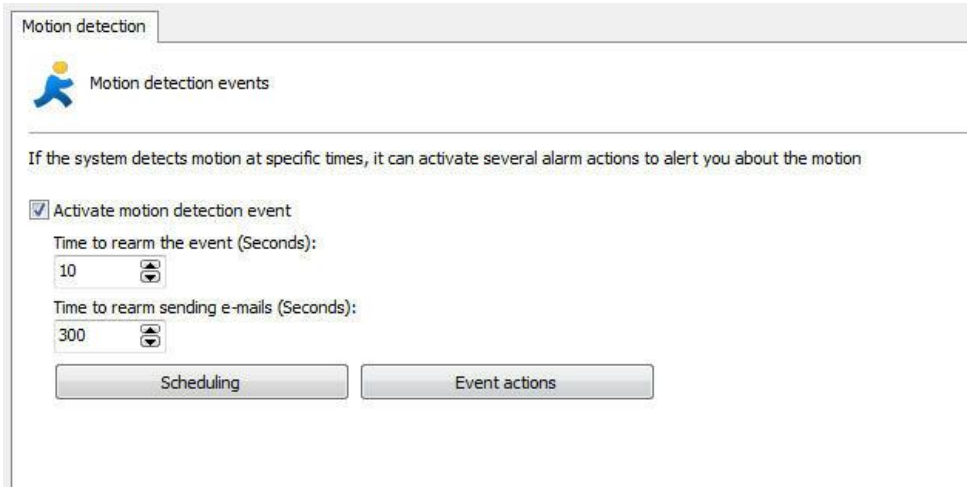


6.1.7.3 Motion Detection

Motion detection can be utilized in Digifort to start a recording or even trigger an alarm.
The configuration of this detection can be done in two ways which are explained in the following topics

The following options are displayed in the Motion detection tab:

© 2002 - 2020 by Digifort, all rights reserved



6.1.7.3.1 How to configure the motion detection event

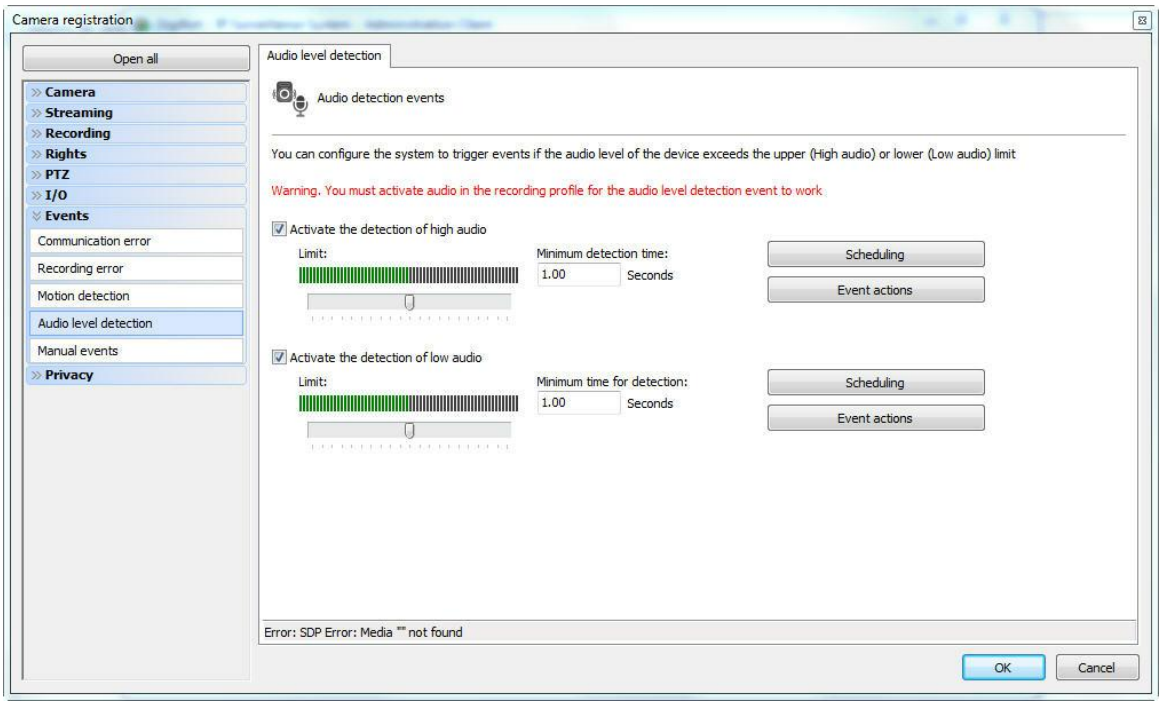
To configure the communications failure event, mark the option Activate motion detection event.
The configuration of this event involves the following parameters:

- **Activate motion detection event**: Activates the motion detection event.
- **Rearming time of the event**: Specify the value in seconds in which Digifort will recognize new motions after a motion has occurs.
- **If sending e-mail, include photos**: Include the photo in which there was motion if sending notification e-mail.
- **Rearming time of the sending of e-mail**: Specify the time interval in which Digifort will send another e-mail message in case the motion event still is recognized.
- **Alarm Actions button:** Click on this button to define the actions that Digifort will execute when the event of motion detection was detected. To learn how to configure the alarm actions, see How to configure the alarm actions
- **Scheduling**: Click on this button to define the times of days and days of the week in which Digifort is to recognize motion events. If this configuration is not done, the motion events will be recognized 24 hours per day and 7 days per week. To learn how to configure the scheduling, see How to configure the scheduling of recording

6.1.7.4 Audio detection

The event audio detection allows triggering events in two situations: if the level is above or below a specified limit for a given time:

© 2002 - 2020 by Digifort, all rights reserved



The screen offers the following features:

Enable loud sound detection:

- Position the cursor at the desired audio level that triggers the event. Configure the time that the configured audio level takes to trigger the event.
- Configure the event scheduling. To know more about scheduling check the How to configure the scheduling of recording chapter.
- Configure the desired event actions. To learn more about events check the How to configure the alarm actions chapter

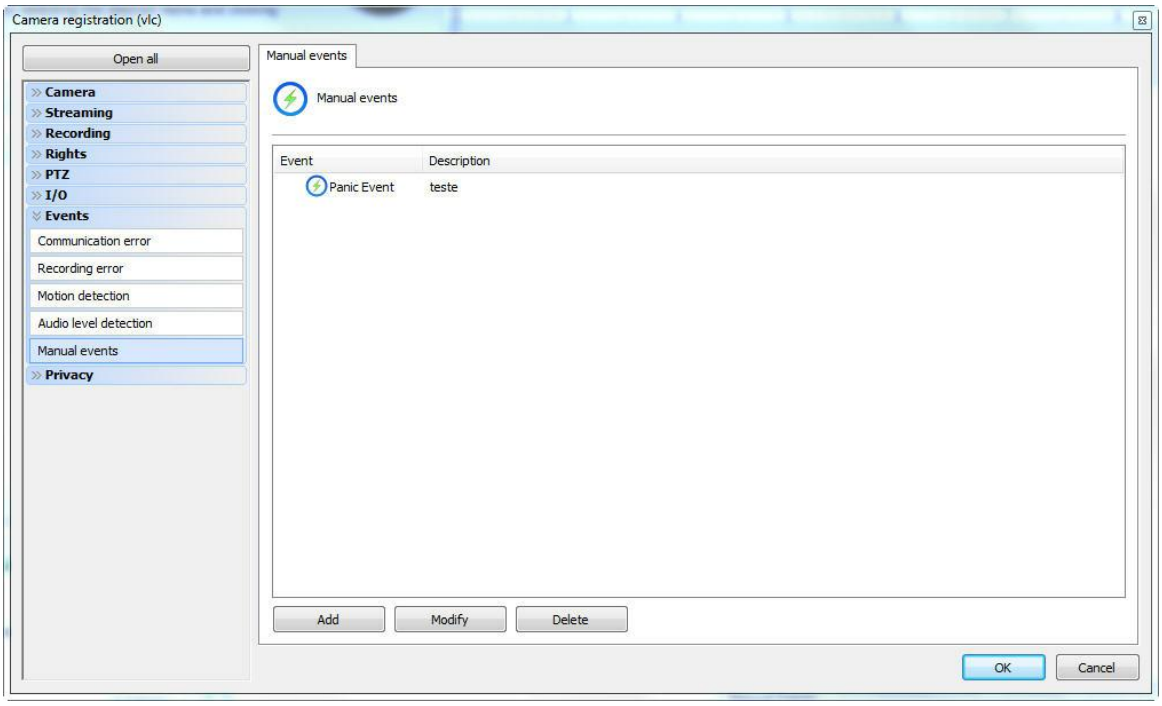
Enable detection of Low Sound:

- Position the cursor at the desired audio level that triggers the event. Configure the time that the configured audio level takes to trigger the event.
- Configure the event scheduling. To know more about scheduling check the How to configure the scheduling of recording chapter.
- Configure the desired event actions. To learn more about events check the Como configurar as ações de alarme chapter.

6.1.7.5 Manual Events

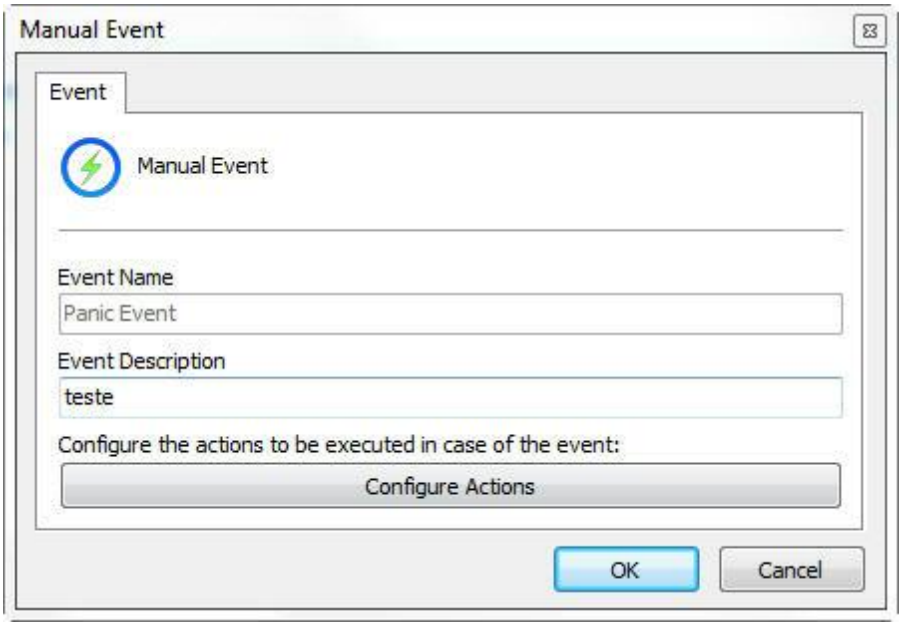
You can create specific events within the cameras that can be triggered manually by operators.

© 2002 - 2020 by Digifort, all rights reserved



On this screen must be registered manuals events that may be triggered by the operator in the Monitoring Client. In the example above is registered an event that opens a door.
To learn to enable the manual events through the Monitoring Client, see your manual.

To add a manual event, click on the **Add** button, opening the screen below. To change and delete, click on the corresponding button



In this screen enter the name and description of the event and finally click on **Configure Actions**.
To learn how to configure the actions that this manual event will run see How to configure the alarm

© 2002 - 2020 by Digifort, all rights reserved

actions

6.1.7.6 Device Events

Some cameras have internal events that can be triggered through your Surveillance Client.
These are Device Events.

Some devices have events that do not fall into any preset system category, so this architecture was created to provide support to different types of camera events.

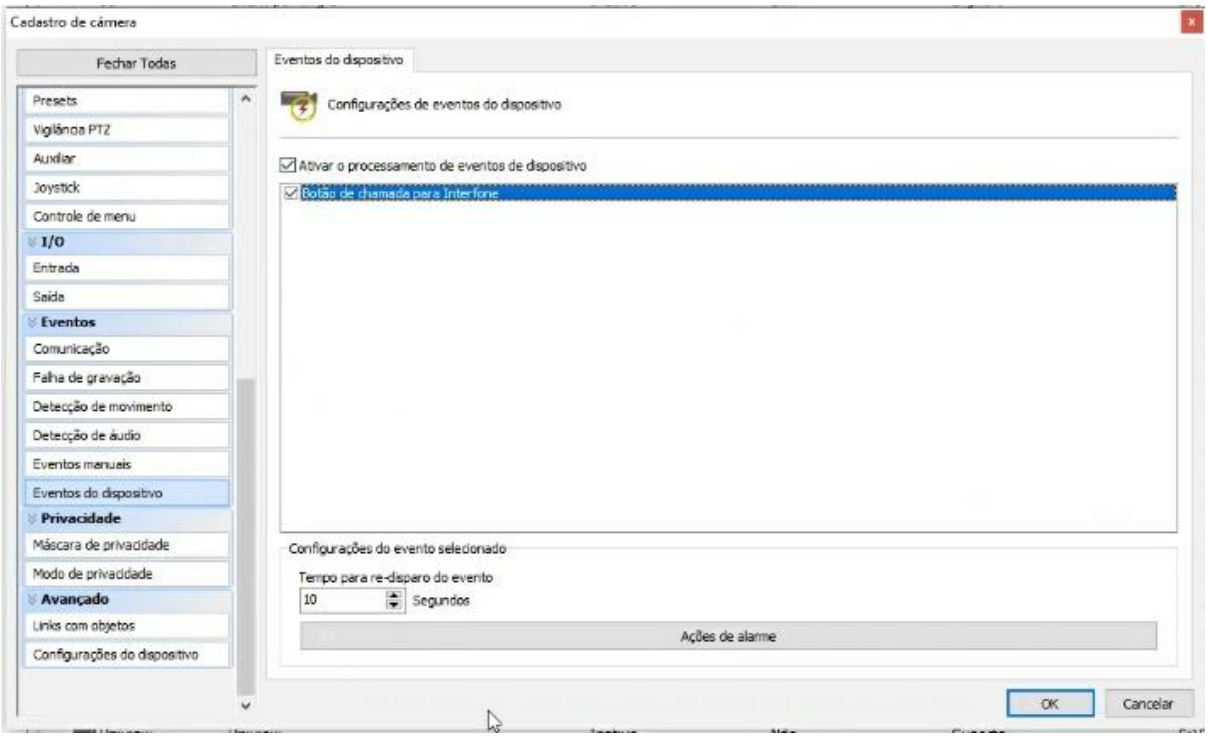
For example, integrated Intercomm devices will provide the “Intercomm call button” event that will be triggered when someone pushes the equipment’s bell. For these custom events, you will be able to configure event actions associated with them.

To find them, go to you Recording Server, Cameras, and open the registration of the camera of interest.
In the registration, navigate to the Events column and select Device Events:



If the camera has some HTTP event, it will appear in the configuration window. Devices have several types of events, such as Disk Failure, Motion Detection, etc.
In the example below, the intercom call event is available to be triggered in a Video doorman:

© 2002 - 2020 by Digifort, all rights reserved



As with any other Digifort event, you can configure the re-triggering time and the actions that should be taken if the event is triggered. To read more about actions, navigate to How to Configure Alarm Actions.

6.1.7.7 Event Variables

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

The Event Variable value can be accessed through the variable name reference, using a variable name identifier: $(VARIABLE_NAME)

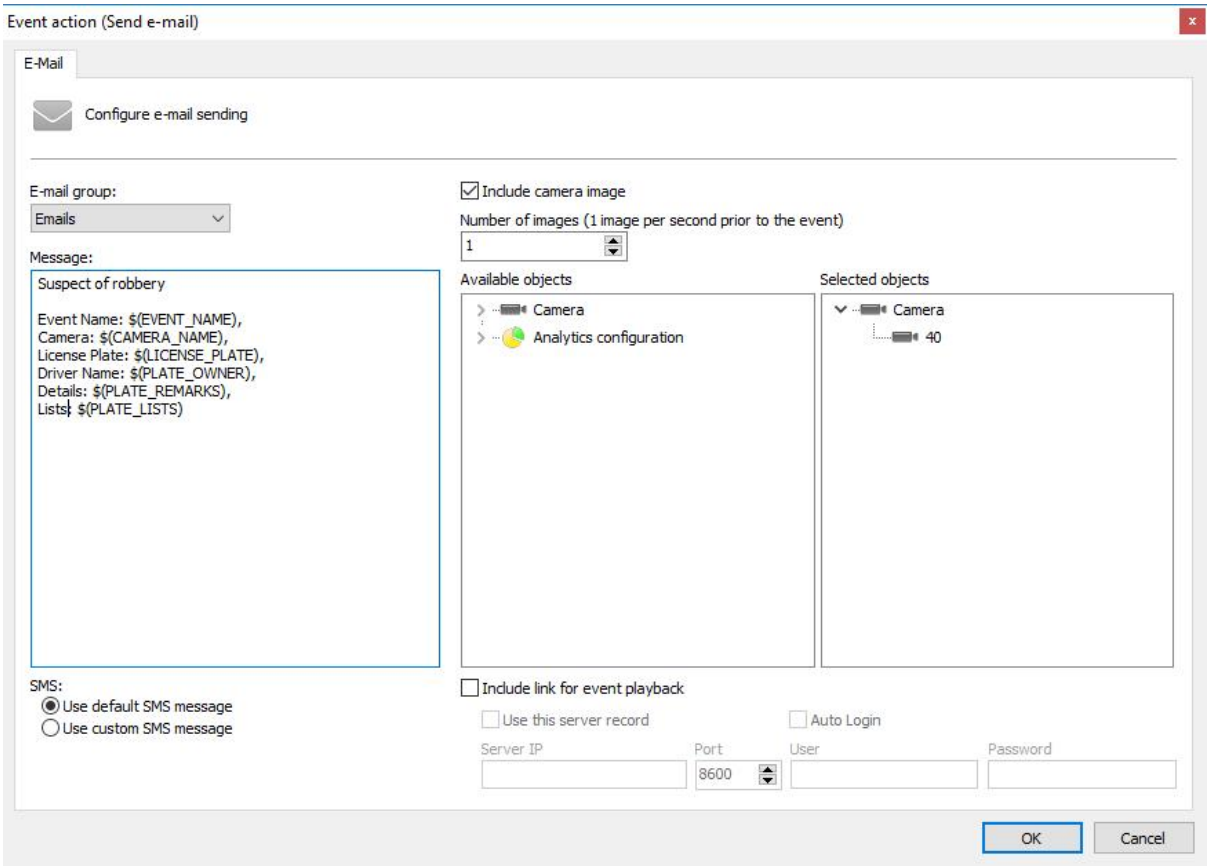
Each system event introduces different types of variables whose values can be used in event actions.

The following event actions support the use of variables:

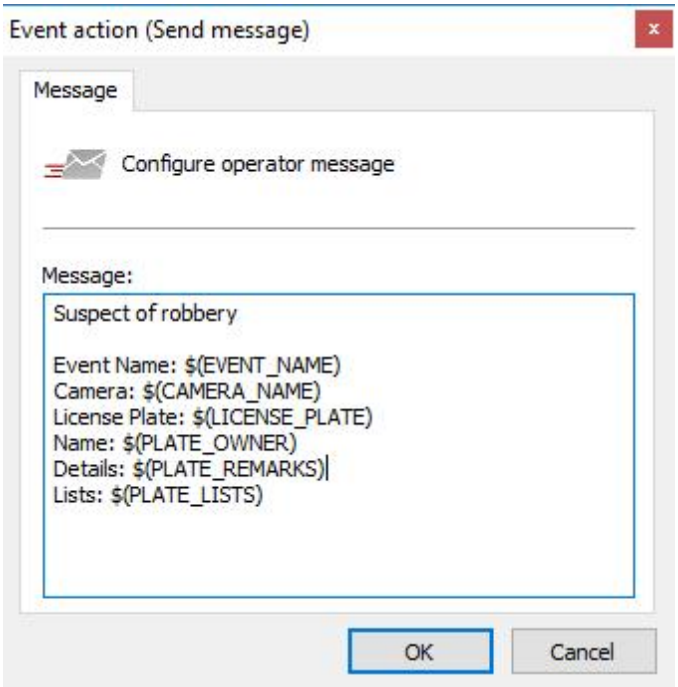
- Send e-mail
- Send message to the Operator
- Send HTTP request
- Create Bookmark

In the example below, an e-mail will be automatically sent with specific data relative to the LPR event, including license plate number and driver's name if the recognized plate is flagged as stolen:

© 2002 - 2020 by Digifort, all rights reserved

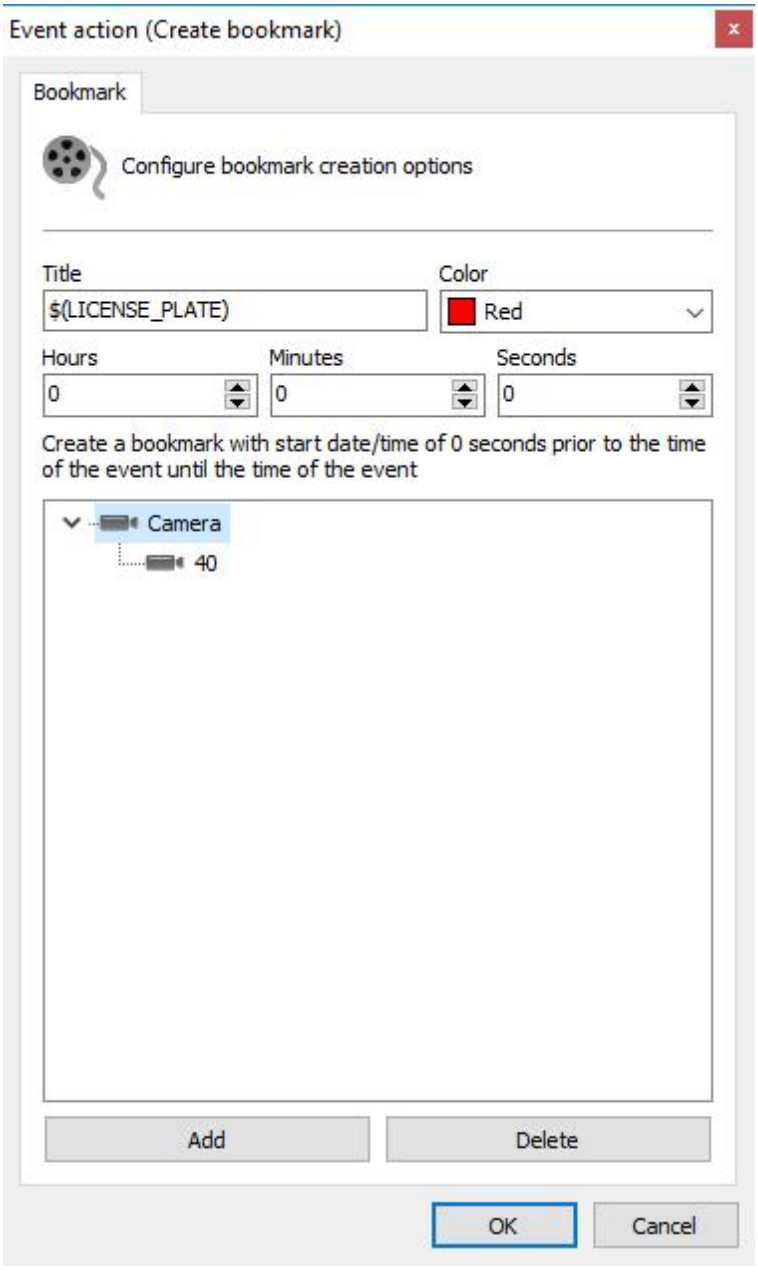


The same can be configured for messages sent to system operators, adding valuable information on the alarm pop-up:



© 2002 - 2020 by Digifort, all rights reserved

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



© 2002 - 2020 by Digifort, all rights reserved



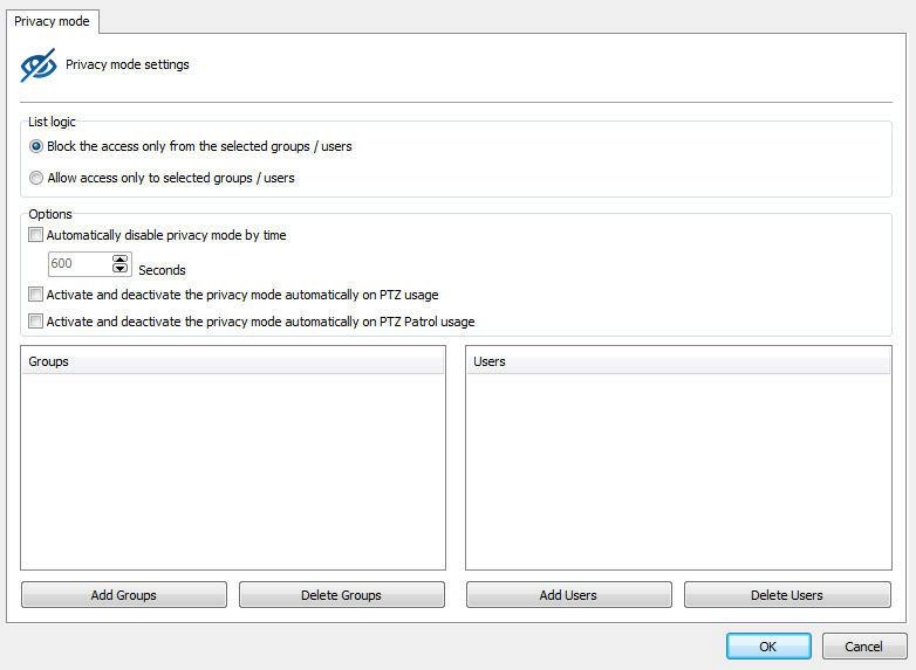
To receive the complete documentation with all system event variables, please contact our support team.

6.1.8 Privacy

6.1.8.1 Privacy mode

Privacy mode allows the administrator to determine a list of users who will lose access to the image of a camera when a user activates the customer privacy mode tracking. This feature can be very useful when the cameras of an installation are available externally, with this, the operator may temporarily block external access to the camera at any time.

© 2002 - 2020 by Digifort, all rights reserved



The privacy mode screen has the following features:

- **Block access only from selected groups/users**: In this mode, all of the selected groups and users will lose access to the camera's image when privacy mode is triggered.
- **Allow access only from selected groups/users**: In this mode, all will lose access to the camera's image, except the selected users and groups when the privacy mode is triggered.

Options

- **Automatically deactivate the privacy mode after**: Disables the privacy mode after X seconds configured.
- **Activate and deactivate the privacy mode automatically on PTZ usage** : This option will enable the privacy mode when an operator moves the camera (PTZ) and will automatically deactivate when the operator ends the use of the PTZ controls.
- **Automatically activate and deactivate the privacy mode during the PTZ surveillance**: This option will automatically enable the privacy mode when the PTZ surveillance is paused and disable the privacy mode when the PTZ surveillance is reactivated.

- **Add groups**: Adds the groups of users to the privacy mode.
- **Delete groups:** Deletes the user groups to the privacy mode.
-
- **Add users**: Adds users to the privacy mode.
- **Delete users**: Deletes users to the privacy mode.

OBS: It is required that the user have rights to enable privacy mode. To learn how to grant rights to the user, see the chapter **User Rights**

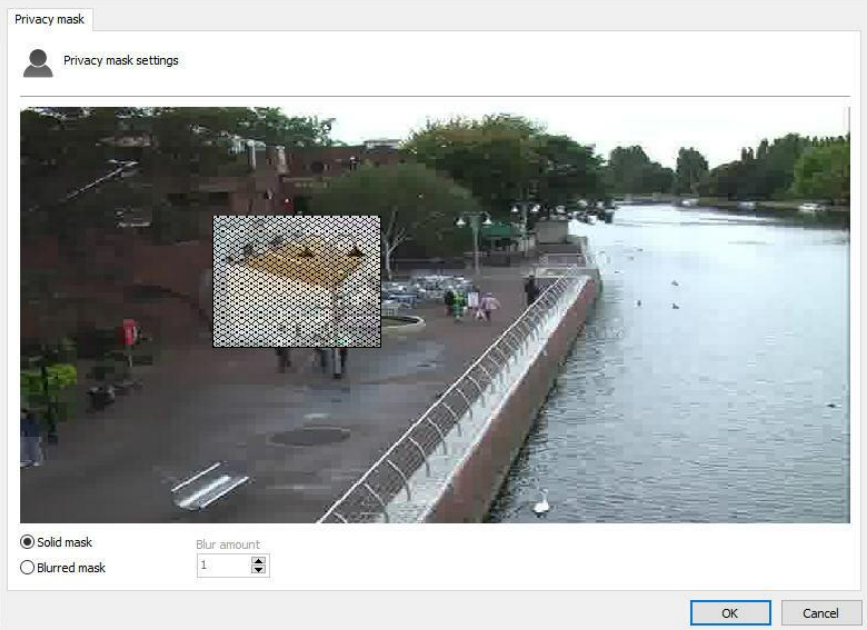
© 2002 - 2020 by Digifort, all rights reserved

6.1.8.2 Privacy Mask

Privacy Mask is a tool that allows hiding areas of the image that cannot be viewed by the operator.

It is important to emphasize that the privacy mask is not recorded on the server, but on the contrary, the original image is recorded and when the image is displayed on the screen, the privacy mask is applied.

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



To add a privacy mask, left-click on the image and drag the mouse, drawing a rectangle. To remove a selected area, make a rectangle with the right mouse button encompassing the entire area of the mask to be removed, or click on **Delete Selection** to delete all created masks.

Two types of privacy masks can be selected: opaque or blurry.
The opaque mask will generate an entirely black mask.
The effect from the opaque mask is shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



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



Another example of use:



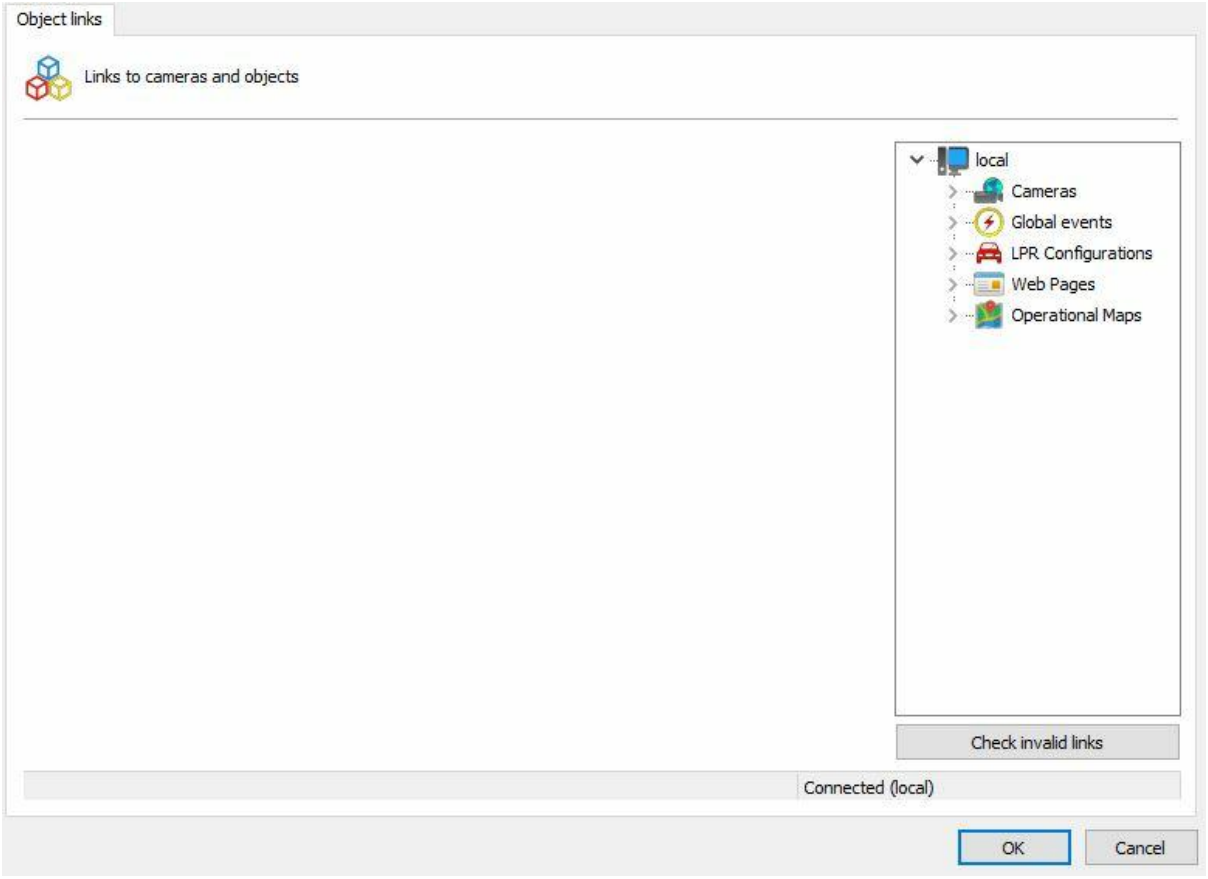
© 2002 - 2020 by Digifort, all rights reserved

6.1.9 Advanced

This registration area is for advanced options.

6.1.9.1 Object links

Object links allows the administrator to create clickables on camera images which, when these links are activated, lead to other system objects or trigger events.
They allow the creation of virtual links between different cameras and the creation of overlaid event triggers on camera images.

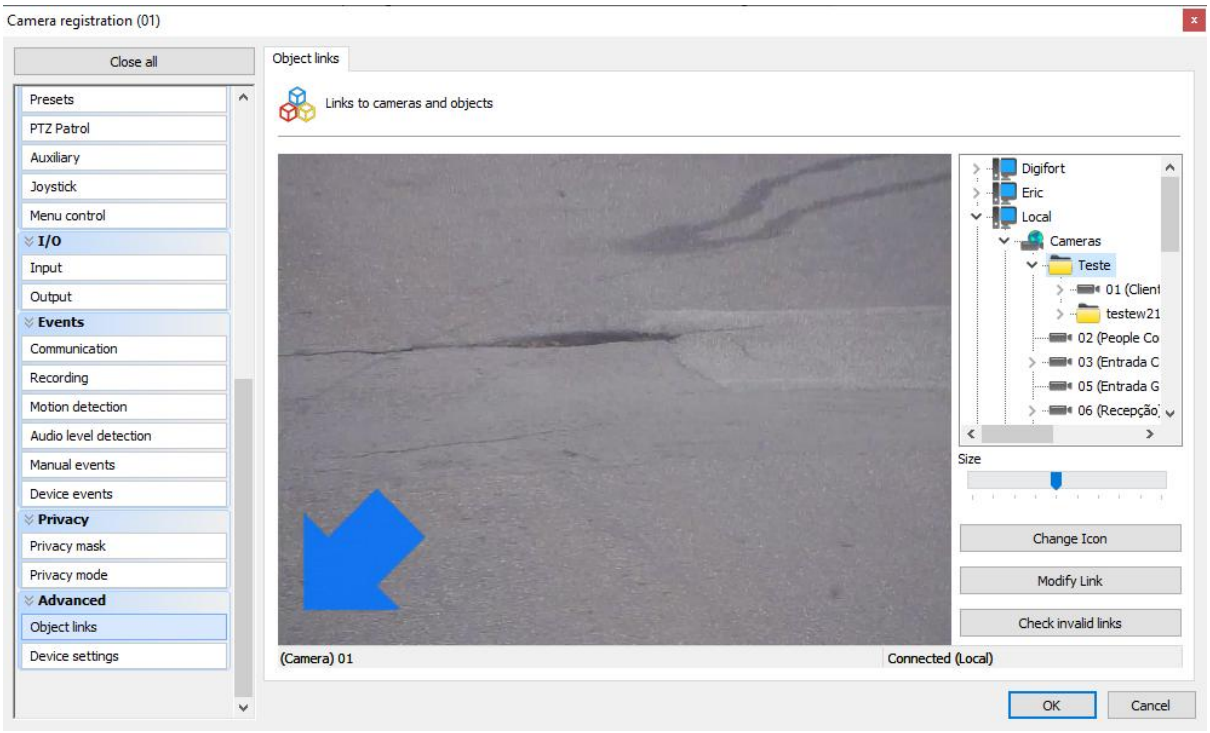


The available objects can be from any server connected to the Administration Client, thus allowing the possibility of linking servers.

Link configuration is very simple. The links editor can be found within the “Object Links” option in camera registration. To create a link, simply drag and drop the desired object from the objects list and the link type selection option will be displayed (zone or icon).

© 2002 - 2020 by Digifort, all rights reserved





Zone: the system will create an area that can be defined by the user by dragging points (double-clicking on the border will prompt the system to create another point) to form the desired area.

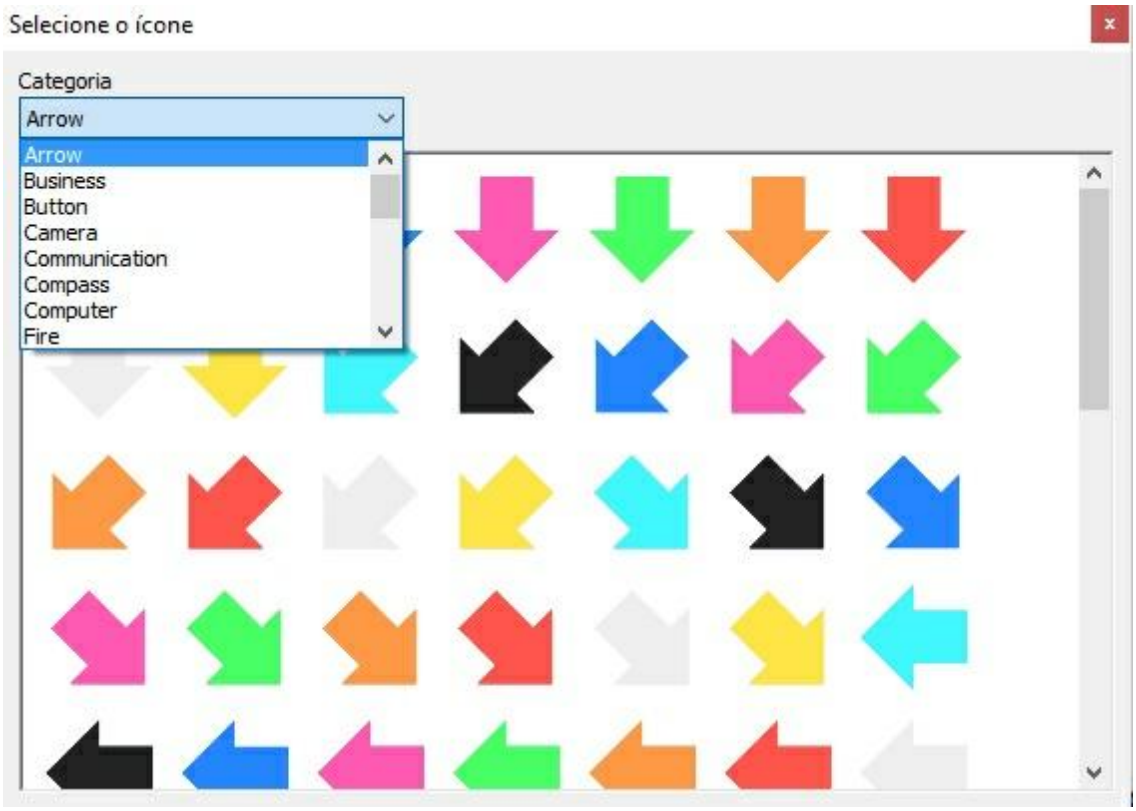
Once the zone has been selected, the color selection and change link buttons will become available:



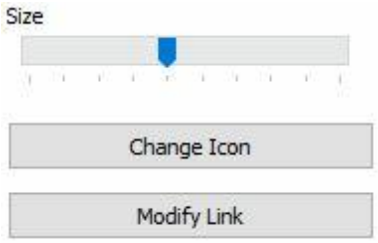
If the operator selects the change link option, simply click on the new object and the system will cause the new object to become the link's destination.

© 2002 - 2020 by Digifort, all rights reserved

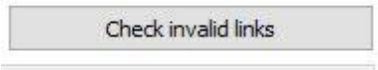
Icon: the system will then ask the user to inform which icon is to be used:



Digifort has an extensive library of available icons and all the user needs to do is choose the best one for each situation. Once the icon is selected, the system will allow the user to change size, icon, or link:



The system also allows the verification of invalid links in case any object is deleted or loses connection with other servers. To do this, simply click on the **Check Invalid Links** button.

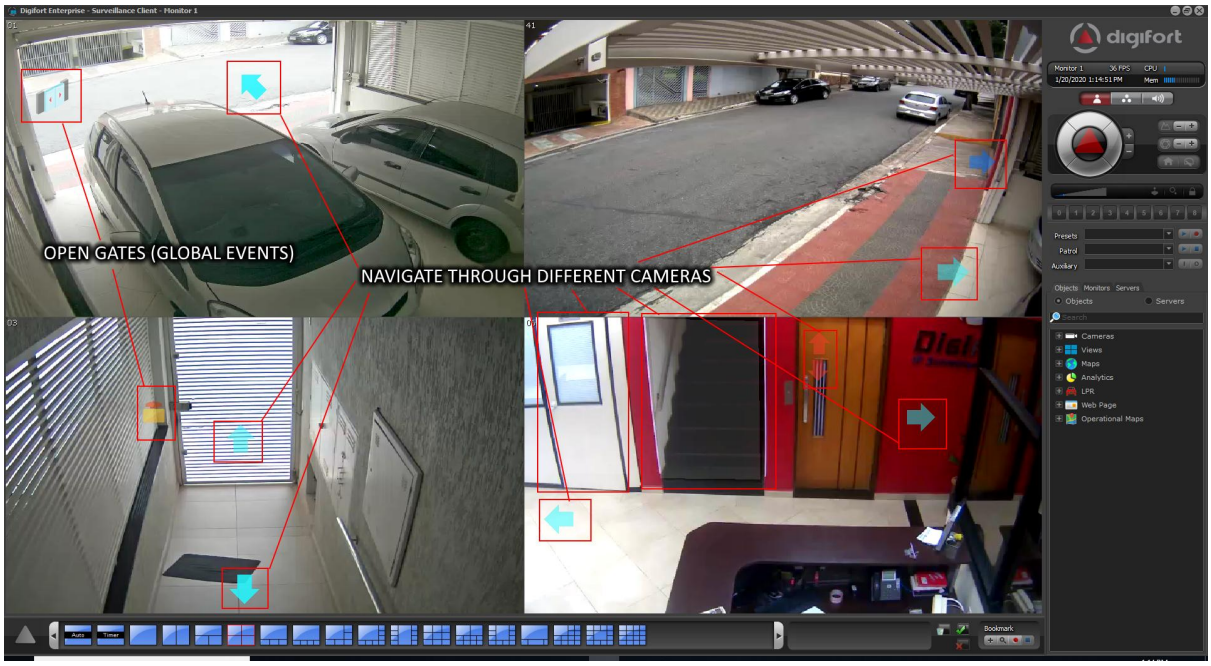


The image below shows an example of the use of object links. Each camera on display has a link to other cameras on the image. By clicking on the link (represented here by semi-transparent arrows), the

© 2002 - 2020 by Digifort, all rights reserved

associated camera will be loaded, allowing quick navigation between cameras, such as, for example, when following a person who is moving between cameras.

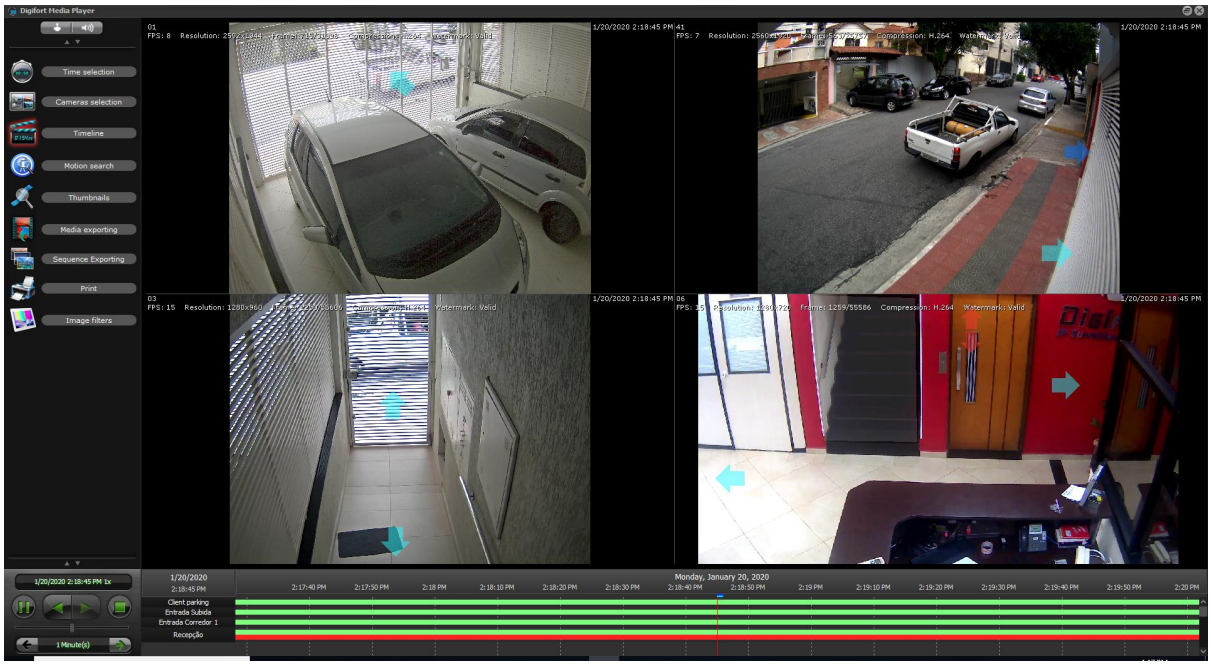
You can also associate events (and several other types of objects) on the images, such as, for example, Global Events that can be used to trigger I/O outputs to open doors and gates. On the image below, cameras 01 and 03 have buttons to physically open the gates.



Object links can also be used during video playback, thus becoming an indispensable tool for analyzing recorded incidents.

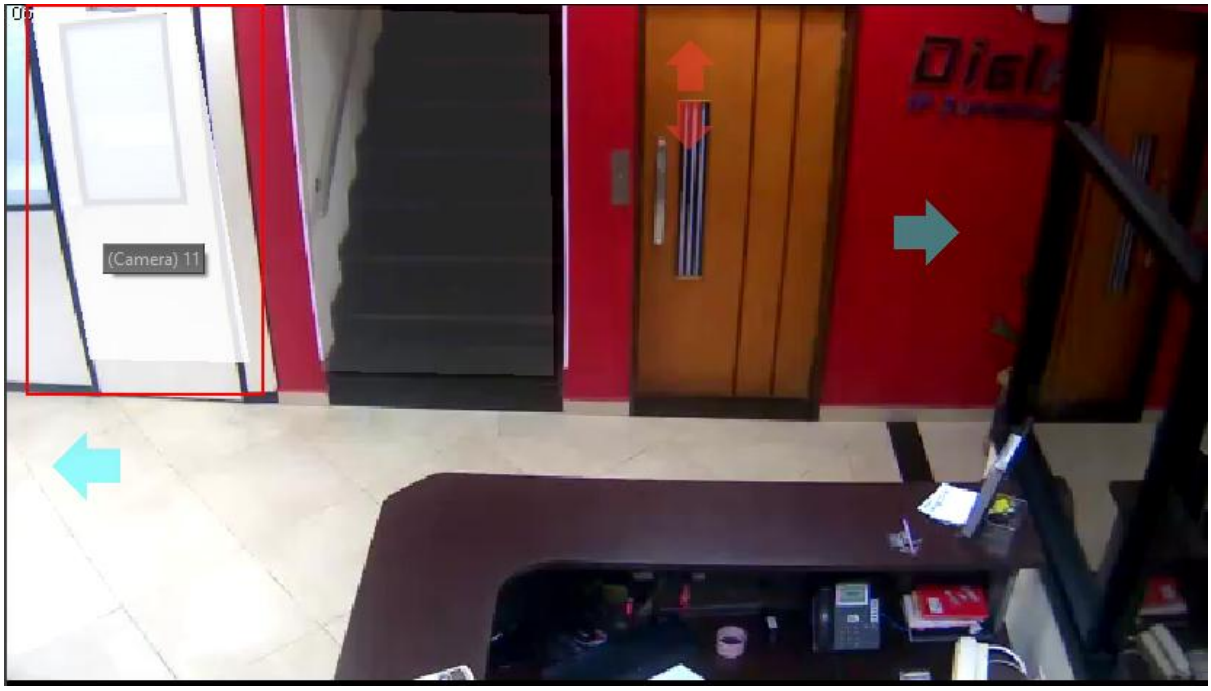
In the Media Player, only links to cameras will be displayed.

© 2002 - 2020 by Digifort, all rights reserved



A zone is represented by a semi-transparent polygon in the image, which can be added, for example, to the outline of a door or gate, thus providing a visual representation that if the operator clicks on this gate, he will be able to see the image of the camera that is on the other side, or also to open it.

The image below shows a white-colored zone, which is associated with a door that, by clicking on it, will display the camera inside the room.

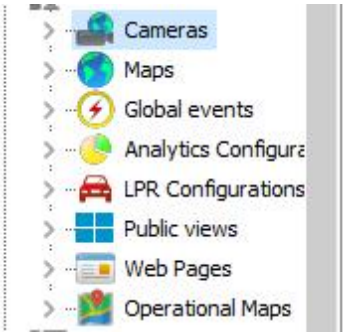


The links can also have the shape of superimposed icons on the image. When creating a link with an

© 2002 - 2020 by Digifort, all rights reserved

icon, an editor will be displayed with various icon categories that can be chosen to better represent the associated action.

The links can be configured for any system visual object, any event (Global and Manual), camera presets, and public mosaics, providing great flexibility to the feature:



See the Surveillance Client manual to check the different settings to optimize the use of object links.

To see this new feature in action, visit the videos available on our YouTube channel: http://www.youtube.com/DigifortChannel
https://www.youtube.com/playlist?list=PLFIhAF6oQd_qjUWb9Ri7XV955EhxweWgf

6.1.9.2 Advanced Camera Settings

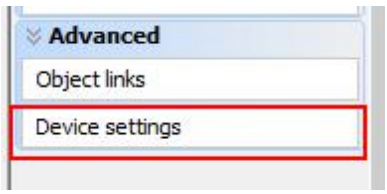
With the Advanced Camera Settings option, you can configure camera parameters (usually streaming parameters) and apply settings to multiple cameras simultaneously.

Most manufacturers do not allow the dynamic streaming of images, which allows the VMS to dynamically request images in a particular configuration (Resolution, Frame Rate, Bitrate, etc.), i.e., these settings are fixed in the camera and the VMS can only request a preconfigured stream.

To facilitate camera configuration, we have developed an advanced settings feature, whereby the system can manipulate these fixed camera settings through the Administration Client's interface without the need to open the browser and configure the cameras manually.

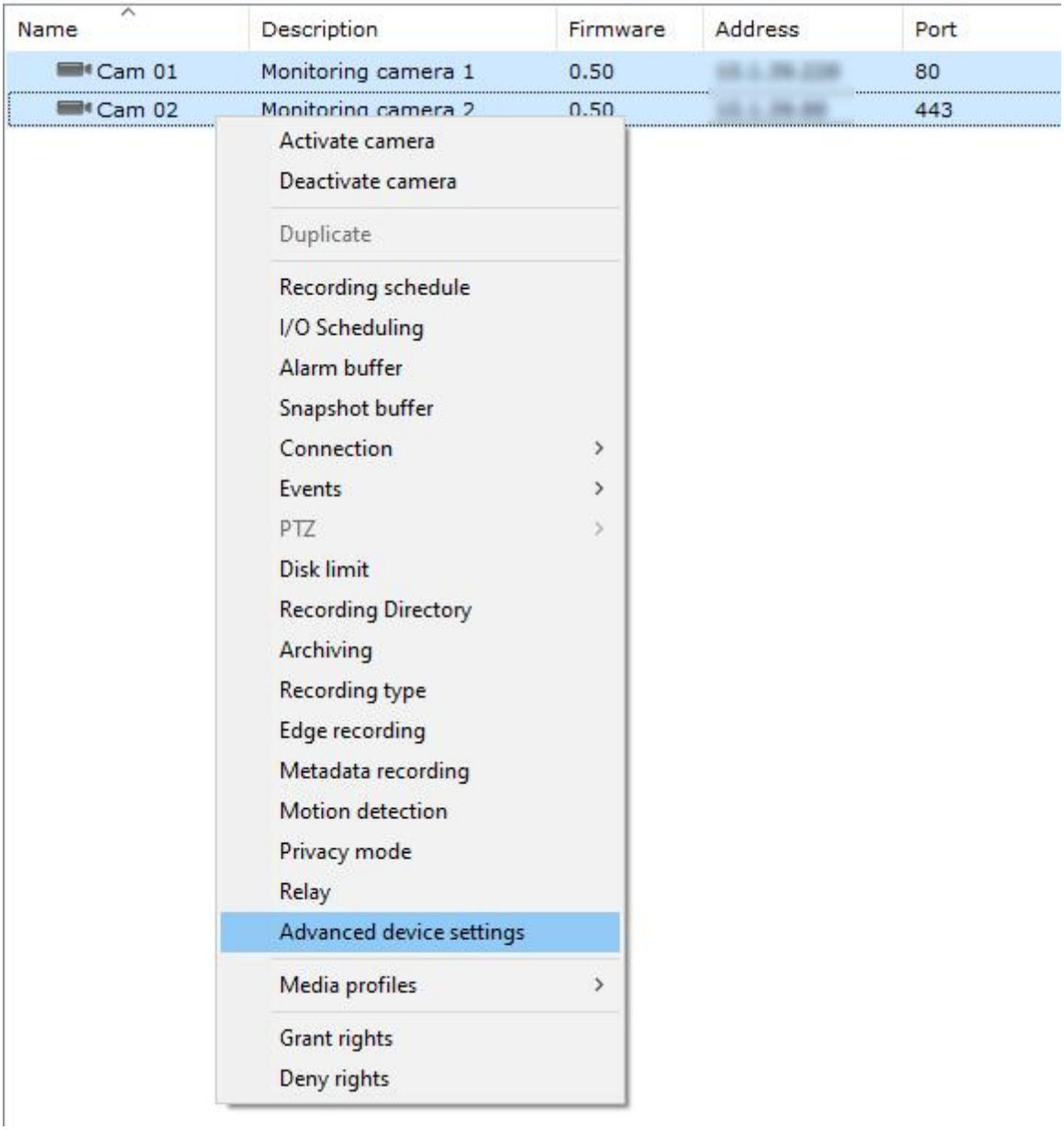
The best of this feature is that it further allows the application of the desired changes (such as, for example, Bitrate, Codec, etc.) to several cameras simultaneously (provided they are from the same manufacturer and have the same configuration driver).

The advanced settings can be accessed through the "Device Settings" menu under camera registration (for individual change):



Alternatively, they can be accessed by selecting multiple cameras and the "Advanced Settings" option by right-clicking on the selected cameras:

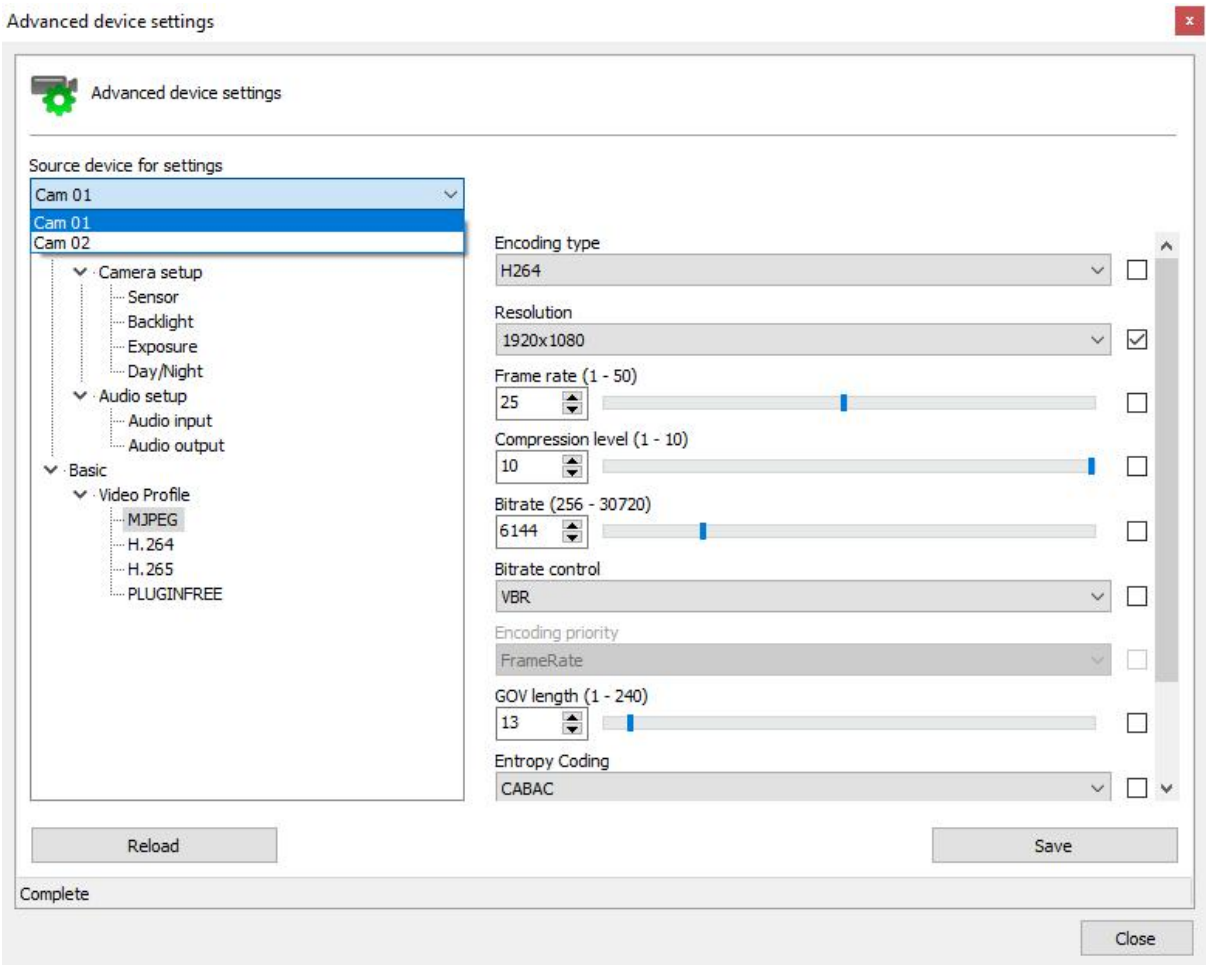
© 2002 - 2020 by Digifort, all rights reserved



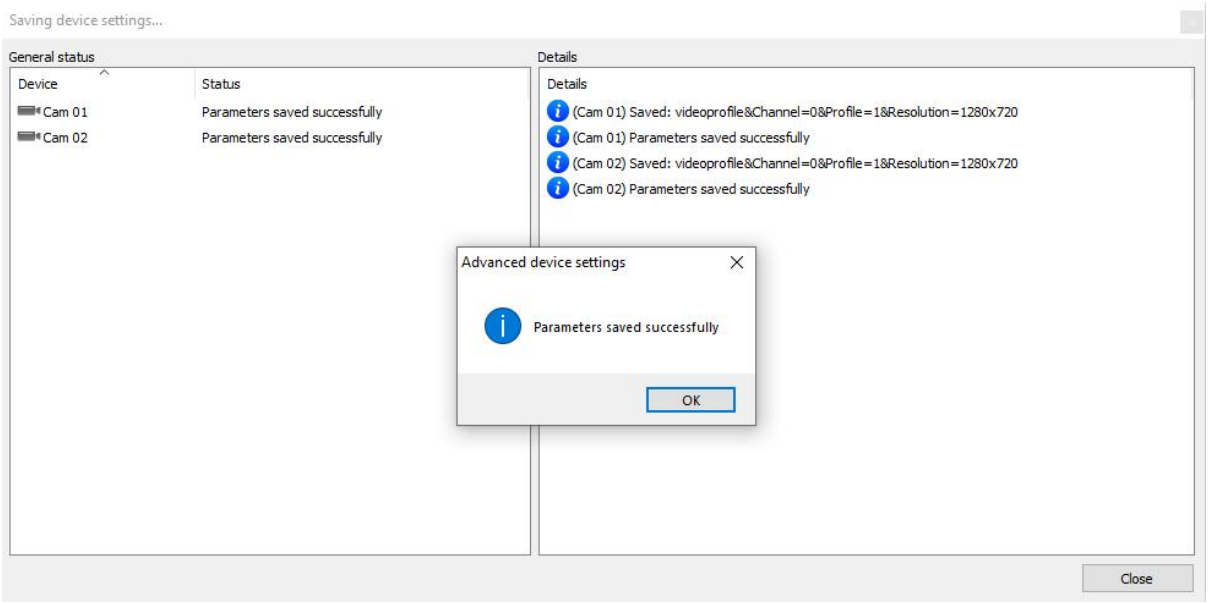
The camera settings will be downloaded (only image, audio, and streaming settings can be configured) and you will be able to change the desired parameters.

In the top combo, you can choose a reference camera (from which the system will download the settings and display them). Upon saving the settings, the system will only save the parameters that have been changed (which are identified through the selected checkbox beside the changed option):

© 2002 - 2020 by Digifort, all rights reserved

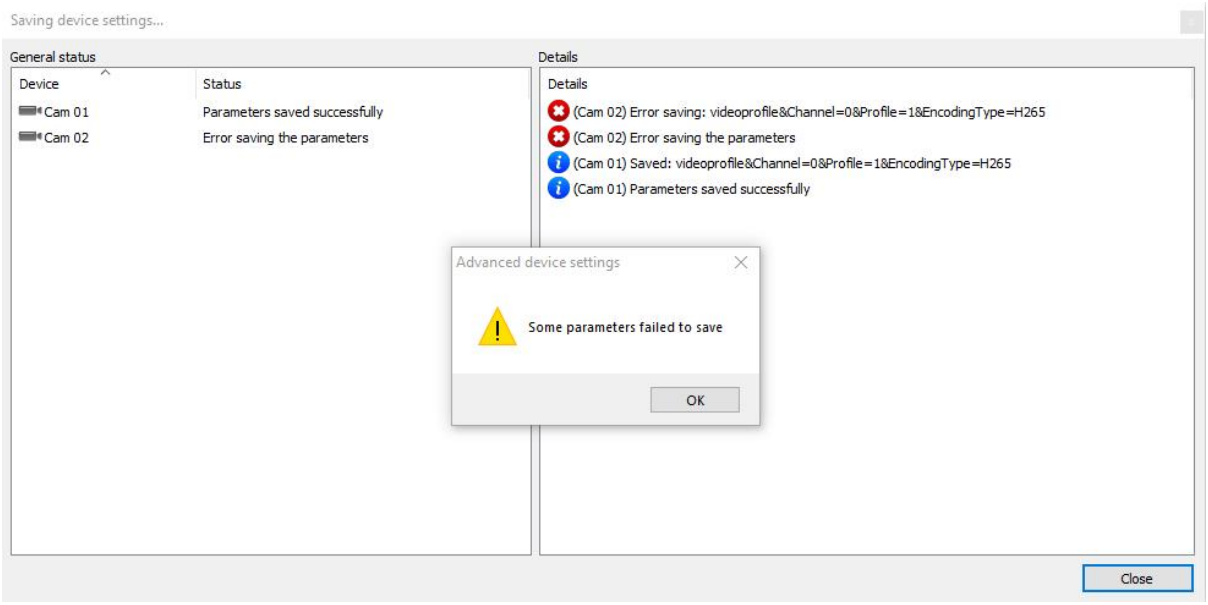


The system will then save the changed parameters for all cameras:



© 2002 - 2020 by Digifort, all rights reserved

If any settings fail upon saving, the system will inform this through an error message, but it will attempt to save all changed settings. A setting may fail upon being changed if the camera does not support the parameter (when a parameter is being recorded on multiple cameras at the same time):



- **Tip**: You can select all cameras that have the same configuration driver as the selected camera through the CTRL + S shortcut, allowing all of them to be changed simultaneously.

To see this new feature in action, visit the videos available on our YouTube channel: http://www.youtube.com/DigifortChannel

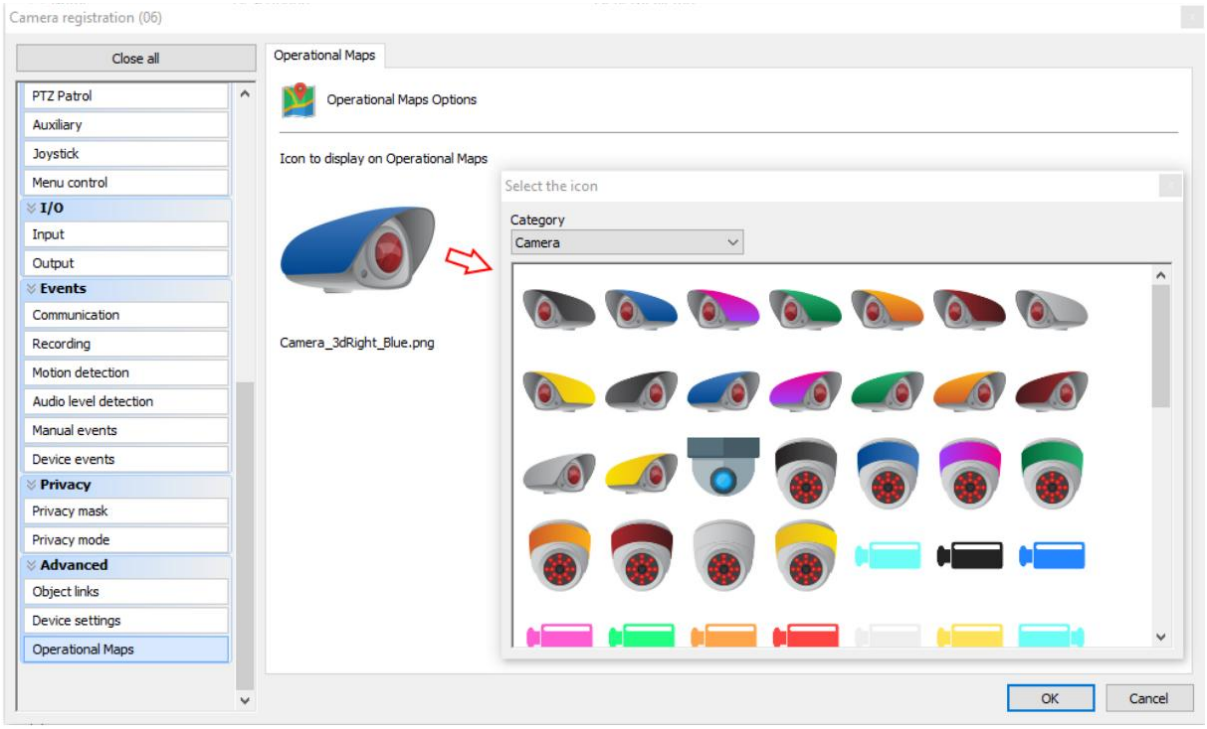
https://www.youtube.com/watch?v=tNCTZjVaBXg

6.1.9.3 Operational Map

On this screen you can choose the icon that will represent your camera on the Operational Map. To learn more, see the Operational Map chapter.

Just click on the **camera image** and choose the new image as shown in the image below:

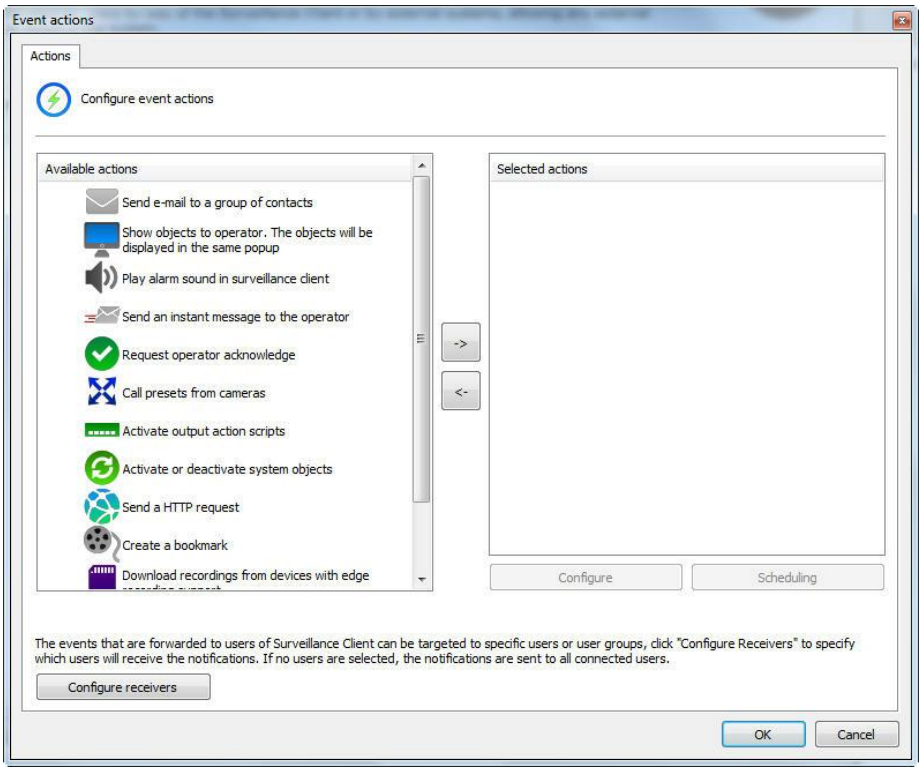
© 2002 - 2020 by Digifort, all rights reserved



6.1.10 How to configure the alarm actions

Various events require the configuration of alarm actions. To access these configurations, click on the Alarm Actions corresponding to the executed configuration. After clicking on this button the screen of alarms configuration will be displayed, as shown in the picture below:

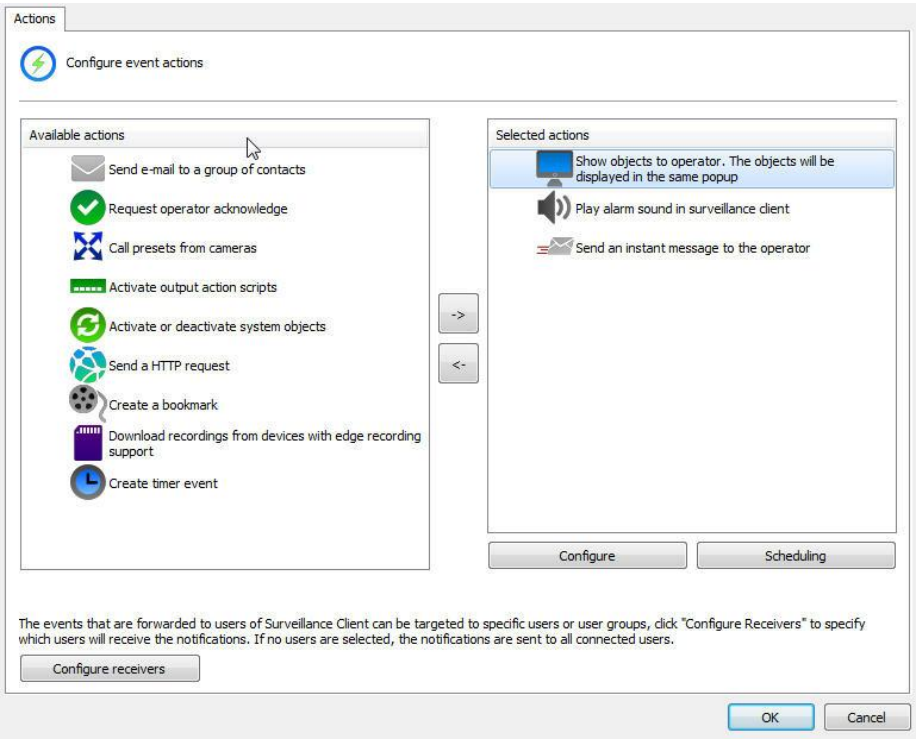
© 2002 - 2020 by Digifort, all rights reserved



Each alarm action has its own individual schedule so that you can configure which times and days of the week the events can occur.

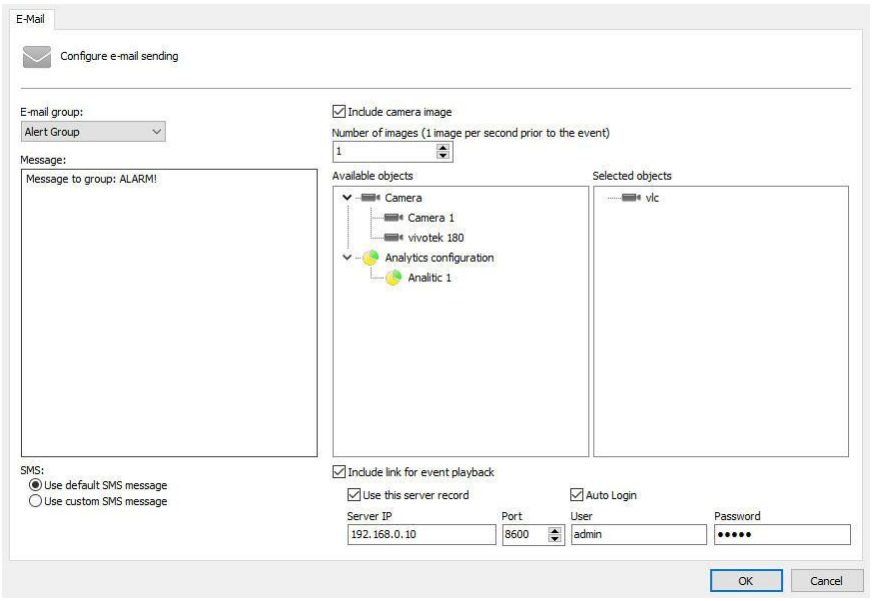
To enable any of the events just click and drag it to the list on the right **Selected Actions** as shown below:

© 2002 - 2020 by Digifort, all rights reserved



6.1.10.1 Send an e-mail message to a group of persons in the case of an alarm

It sends a notification e-mail to the selected alert group. If this action is to be applied in the occurrence of the selected event, select this option and click on **Configure E-mail**, opening the settings screen of the e-mail to be sent, as shown in the figure below:



- **Alert group**: Selects the alert group that will receive the alarm notification e-mail.

© 2002 - 2020 by Digifort, all rights reserved

- **Message**: Configures the message that will be sent in the body of the e-mail.

- **Add image from cameras**: It is possible to attach an image from one or more Cameras/Analytics to the e-mail sent in the event of an alarm. Simply drag the desired object to the **Selected Objects** list.

For analytics, the image will be sent together with the metadata.
See the Metadata chapter.

- **Number of images**: It allows you to attach multiple images of an event when sending e-mails. The interval between the quantities of images will be 1 second.

- **Include link for event Playback**: It is possible to attach a script file that, when executed, will open the Surveillance Client and playback the video from those cameras whose images were selected to be sent in the e-mail. This feature will only work with the desktop version of the Surveillance Client. If the e-mail is opened in a mobile device, such as Apple or Android, the script file will not work.

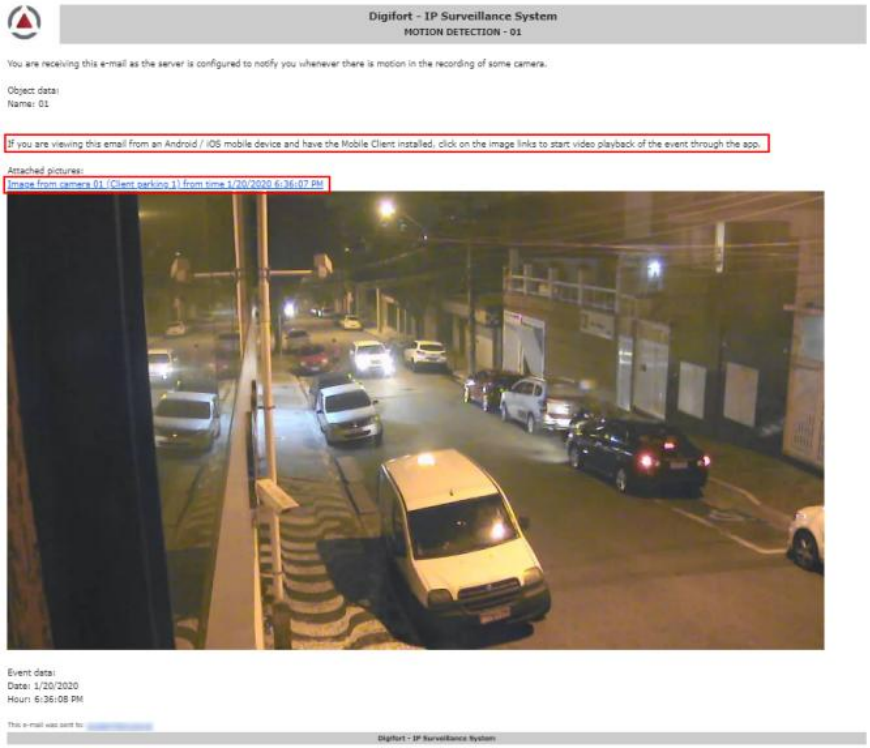
- **Use this server record**: Fill in with data from the server where the camera image that will be attached to the e-mail is located. With this option, upon running the e-mail script, the surveillance client will auto connect with the pre-configured data from this option. If this option is not selected, after the script is deployed, playback will only open after the user connects to the correct server.

- **Use Default SMS message**: In the event a SMS is sent, Digifort sends a standard message to the user.

- **Use Standard SMS message**: In the event a SMS is sent, Digifort will send the text that the user typed in the **Message** field with a limit of 140 characters.

The alert e-mails that include camera images will not include a “DeepLink” in the body of the e-mail, where, if the e-mail is being viewed through an Android or iOS device, the playback of the event’s video will be allowed (upon clicking on the link) through the Mobile Client (if installed).

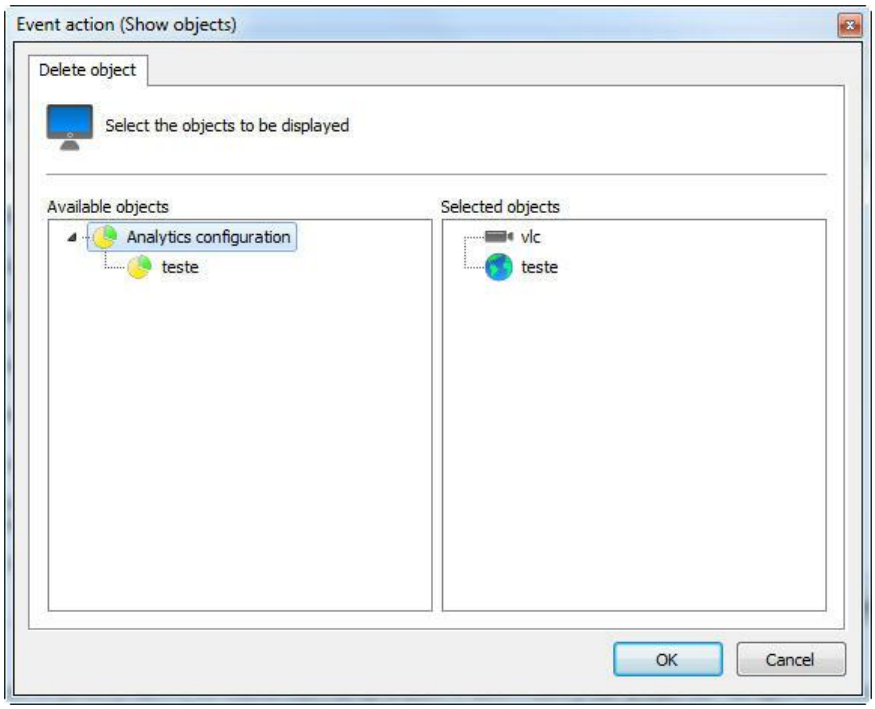
© 2002 - 2020 by Digifort, all rights reserved



6.1.10.2 Display camera images in the screen of the operator

Displays images from any camera of the system in the screen of the operator of the Surveillance Client in a pop-up. The number of cameras that can be displayed in a pop-up is unlimited, that is if more than one camera is selected, an automatic view will be created. To learn about surveillance views, see the manual of the Surveillance Client. If you wish to execute this action in case of the selected event, mark this option and click on Select Cameras, opening the configuration screen of cameras to be displayed on the screen, as shown in picture below:

© 2002 - 2020 by Digifort, all rights reserved



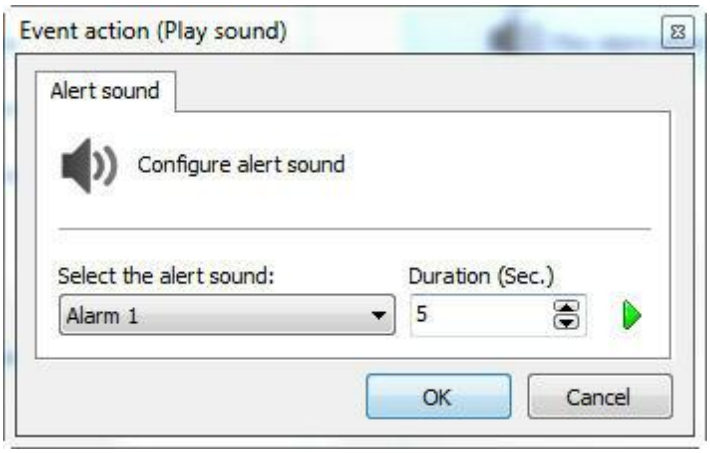
To select the cameras to be displayed on the operator's screen, select the desired cameras in the list of available cameras and drag them to the list of selected cameras.

To remove the cameras to be displayed on the operator's screen, select the desired cameras in the list of selected and drag them to the list of available cameras.

6.1.10.3 Sound an alarm in the Surveillance Client

Sounds an alarm in the Surveillance Client, alerting the operator to the event that occurred. If you wish to execute this action, in case of the selected event, mark this option and click on Select Sound, opening the configuration screen of the sound to be executed in the Surveillance Client, as shown in picture below:

© 2002 - 2020 by Digifort, all rights reserved

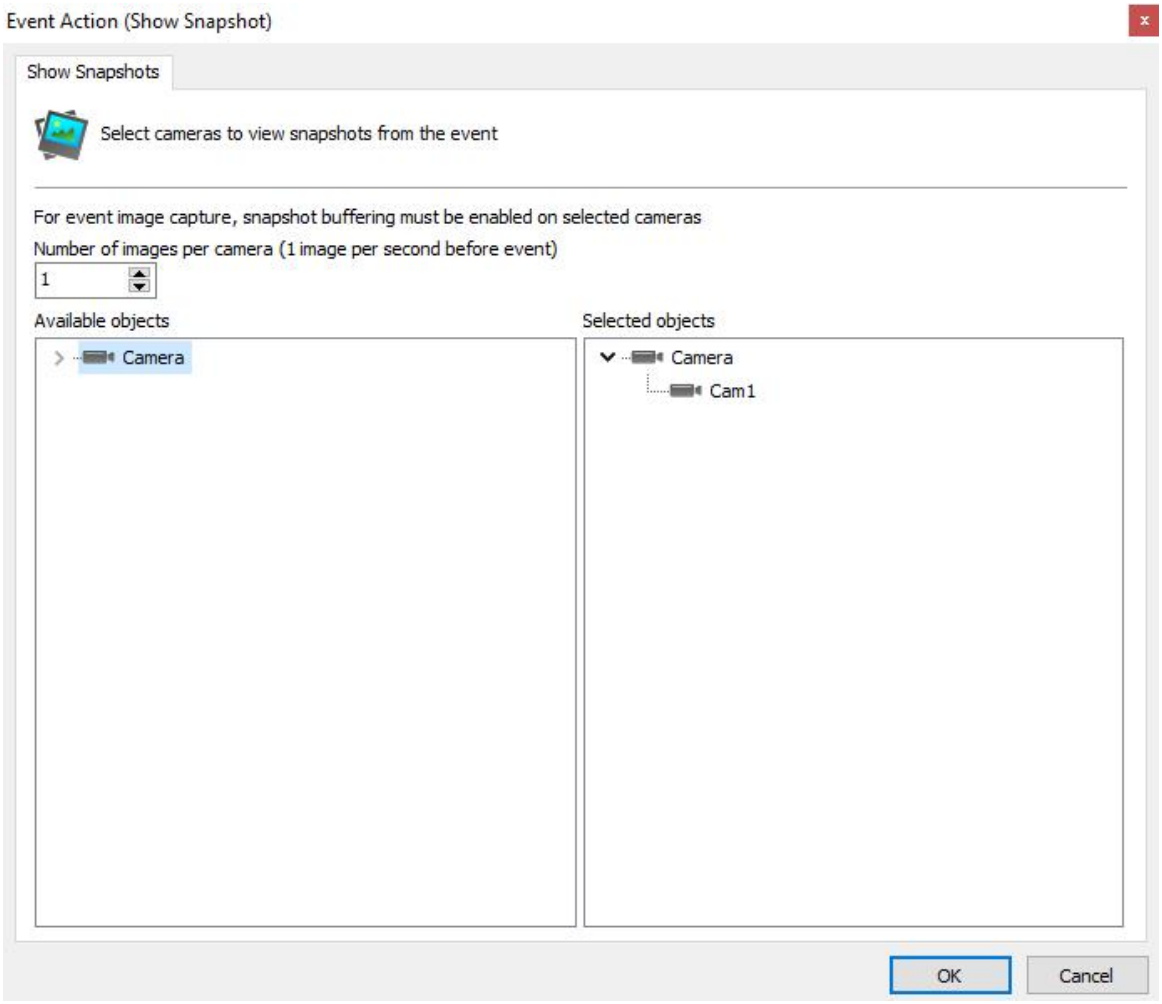


Select the desired alert sound and execution time in the Surveillance Client. To test the selected sound, click on the **Play** button.

6.1.10.4 Display camera snapshots on the operator's screen at the time of the event

It displays a snapshot via pop-up at the time of the event from any system camera on the operator's screen in the Surveillance Client. The number of cameras that can be displayed in the pop-up is limited, i.e., if more than a camera is selected, an automatic mosaic will be created. To learn about surveillance mosaics, see the Surveillance Client manual. If you want to perform this action at the time of the selected event, check this option and click on Select Cameras, thus opening the settings screen of the cameras to be displayed on the screen, as illustrated in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



To select the number of images per camera (how many seconds prior to the event they will be displayed on the screen), change the number according to the desired quantity. The maximum number of images per event is equal to the camera's snapshot buffer...

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

To remove the cameras to be displayed on the operator's screen, select the desired cameras in the list of selected cameras and drag them to the list of available cameras.

6.1.10.5 Send Audio Clip

It sends an audio clip to a device or to a list of available devices.

The audio clips can be selected from a list of already-available .wav files by clicking on Select an Audio Clip stored on the server. To test the audio, simply click on the green play button beside the list.

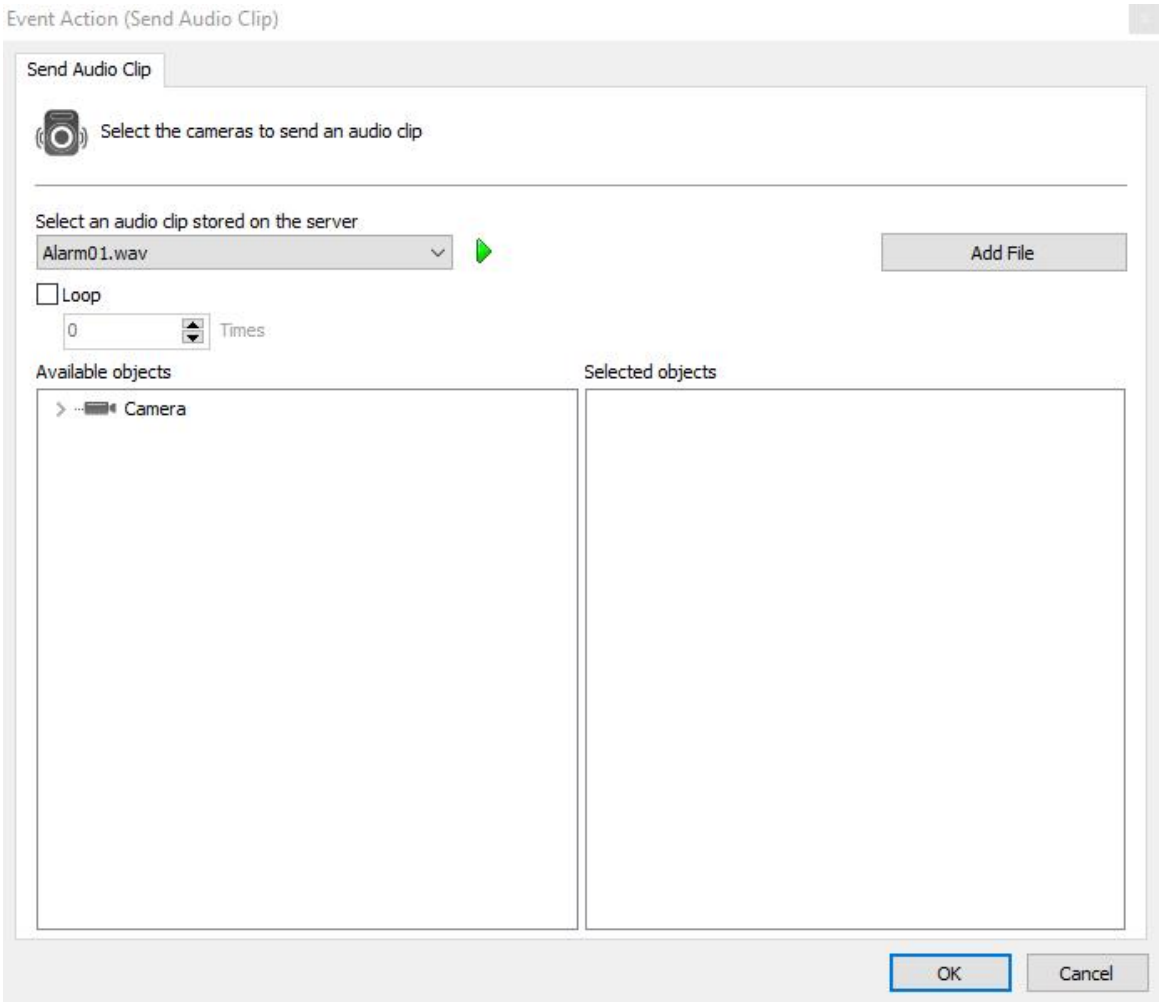
You can also send your own audios to the server to use them on your devices. To do so, simply

© 2002 - 2020 by Digifort, all rights reserved

click on Add File and select the desired file.

Important: For the device to be able to reproduce such audio, the latter must have a frequency of 8KHz, to be 16bits and Mono.

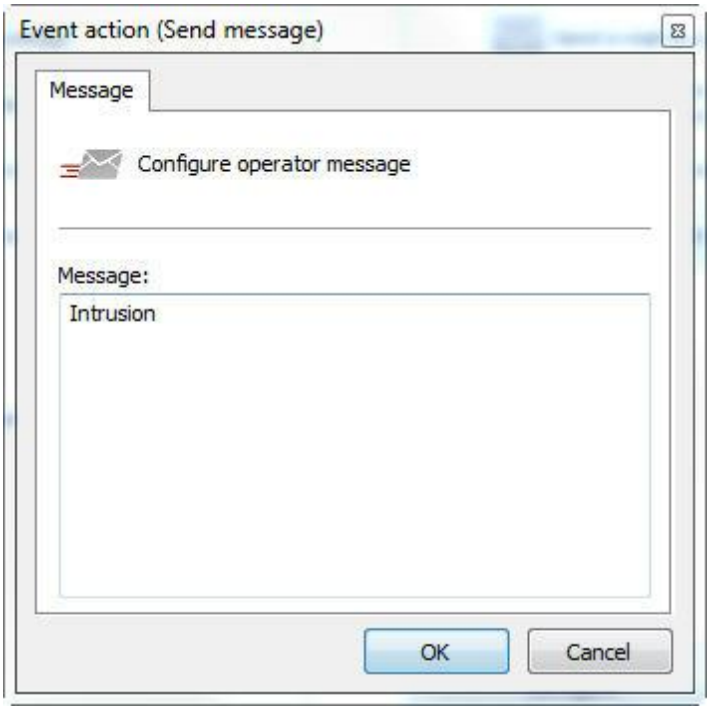
The **Loop** button determines how often the device will trigger such an audio in loop. Select the number of times in the box below.



6.1.10.6 Send instant message to the operator of the computer

Send an instant message to the operator with information defined by the administrator. These messages can contain instructions of the procedure to be executed by the operator for solution of the problem, for example. If you wish to execute this action in case of the selected event, mark this option and click on Configure Message, opening the configuration screen of the message to be displayed on the Surveillance Client, as shown in picture below:

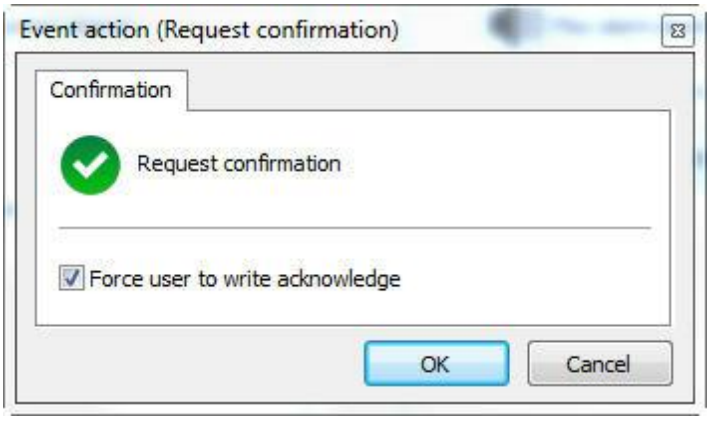
© 2002 - 2020 by Digifort, all rights reserved



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

6.1.10.7 Request written confirmation from users

Requests a written confirmation from the users. This confirmation will be displayed to the operator in the Surveillance Client. These confirmations can contain information about the procedure that the operator executed in the case of an event. If you wish to execute this action in case of the selected event, mark this option and click on Configure Confirmation, opening the screen for configuration of the confirmation to be displayed on the Surveillance Client, as shown in picture below:

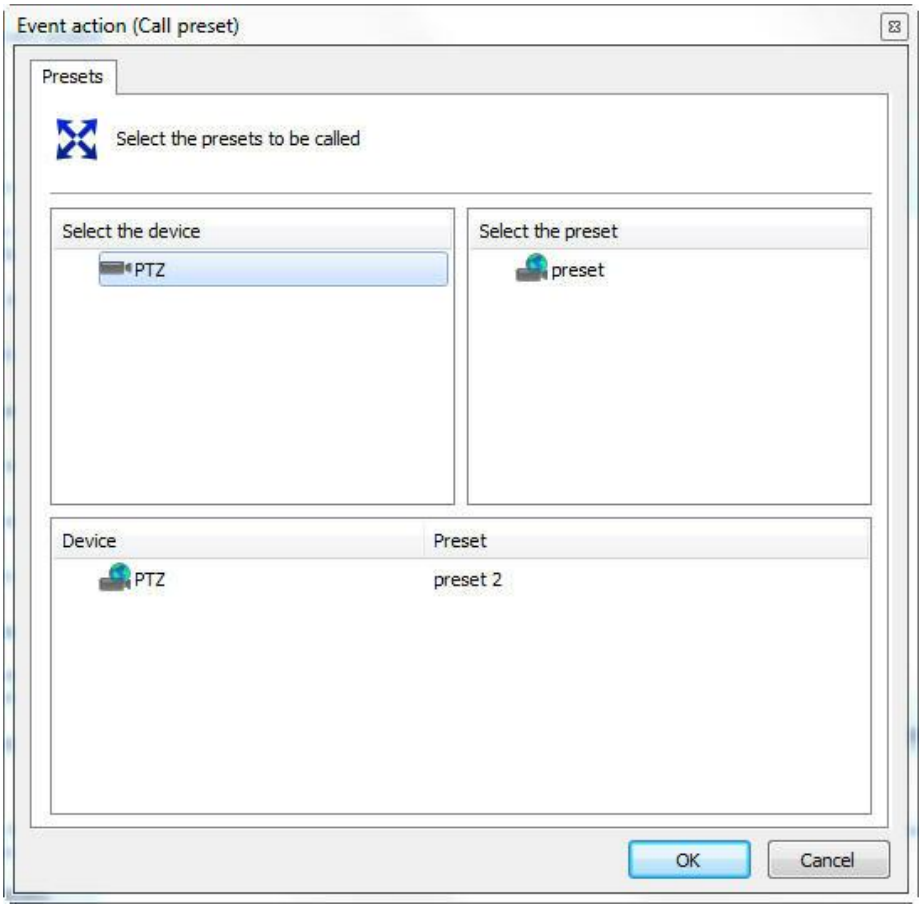


If you wish to oblige the operator to write a confirmation, mark this option..

© 2002 - 2020 by Digifort, all rights reserved

6.1.10.8 Activate camera presets

Activates camera presets when an event occurs, that is, when this event occurs, some cameras can be configured to position themselves in a pre-defined position. To learn how make presets see How to configure the Presets Controls.If you wish to execute this action in case of the selected event, mark this option and click on Configure Presets, as shown in picture below:

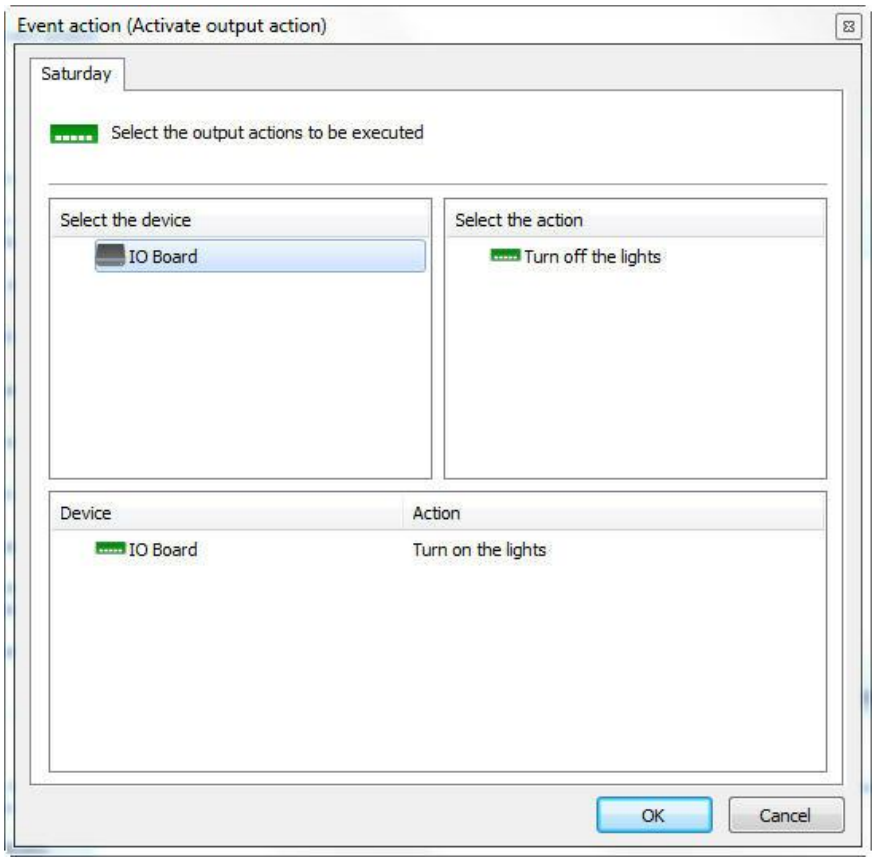


In this screen, select the desired camera, select the preset that you wish to activate, and then drag it to the list below, as shown in the picture below:

6.1.10.9 Activate action scripts of alarm outputs

When an event occurs, this option lets Digifort activate action scripts of alarm outputs, such as, for example, setting off a siren. To learn how to configure scripts of alarm outputs, see How to add output events. If you wish to execute this action in the case of the selected event, mark this option and click on Configure Actions, as shown in picture below:

© 2002 - 2020 by Digifort, all rights reserved



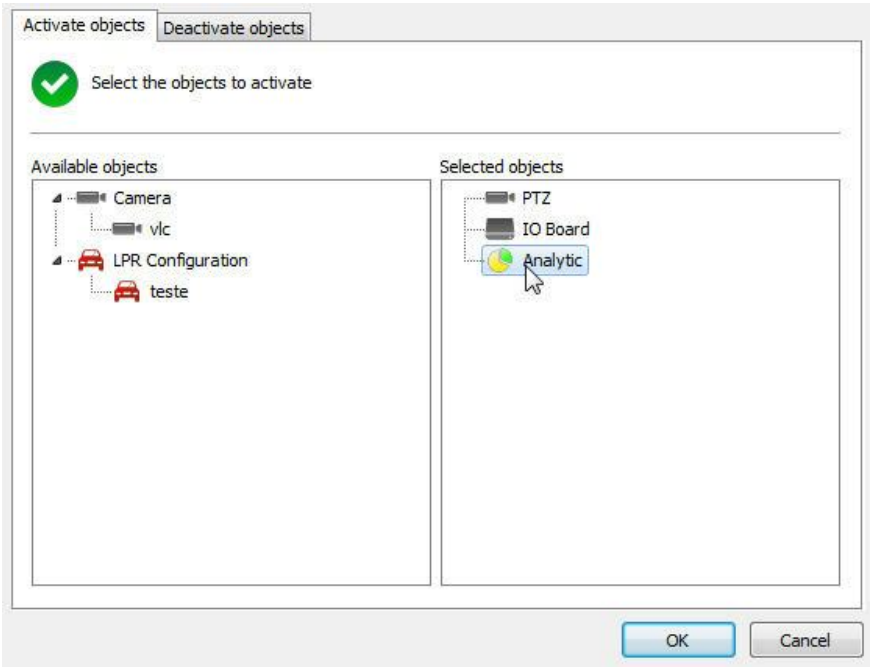
In this screen, select the camera or alarm device which contains the script of actions of the alarm output that you want to activate. Following this, select the event and drag it to the list below, as shown in the picture below:

6.1.10.10 Enable or disable system objects

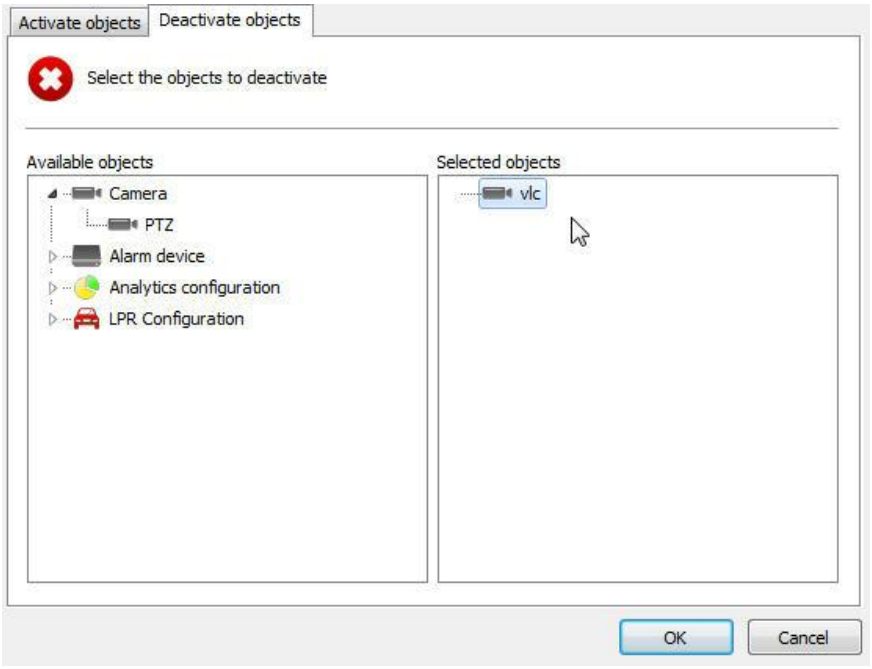
With this event, it is possible to enable and/or disable system objects. The objects that can be enabled or disabled using this action are Cameras, Alarm Devices, Maps, LPR Settings, and Analytics Configurations.

To enable an object, simply go to the **Activate Objects tab** and click and drag the desired object to the **Selected Objects list** on the right, as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved



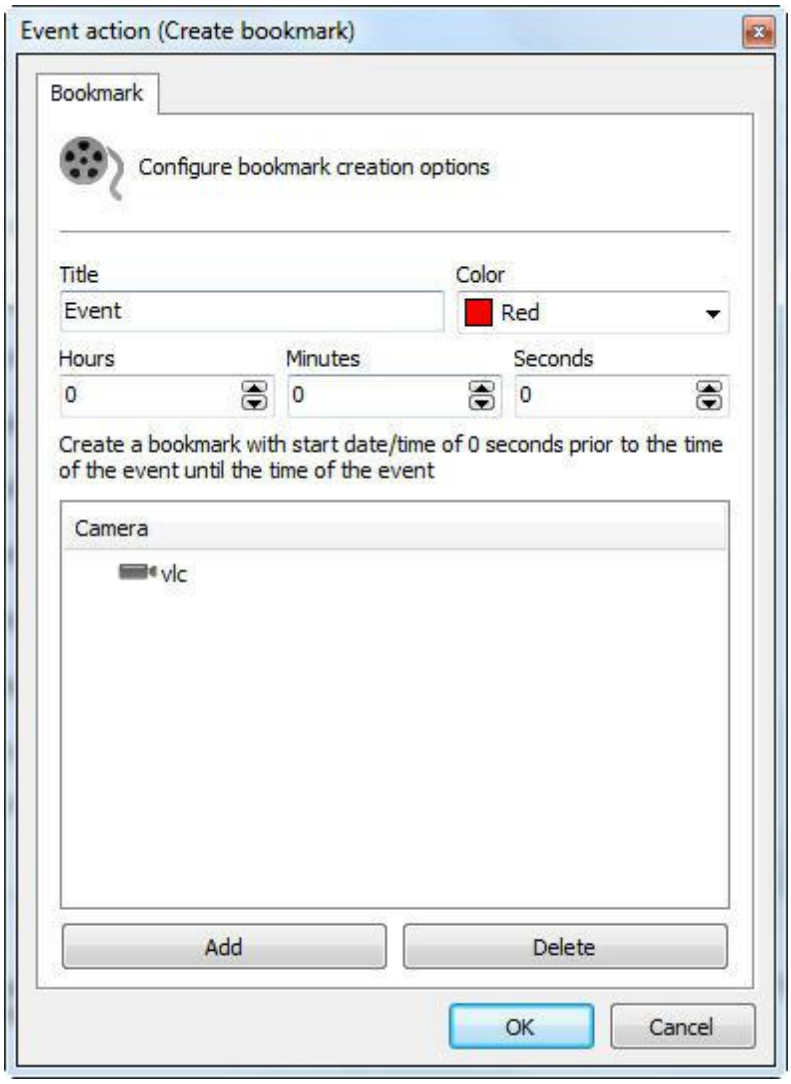
To disable an object, simply go to the **Disable Objects** tab and click and drag the desired object to the Selected Objects list on the right, as shown in the image below:



6.1.10.11 Create Bookmark

This event allows the system to create a bookmark whenever certain event occurs, easily identifying it on the recordings.

© 2002 - 2020 by Digifort, all rights reserved



In the configuration screen, the following options are available:

- **Title**: The title that is used for the Bookmark
- **Color**: Color used for the bookmark
- **Hours, Minutes and Seconds**: From the event time, select the bookmark duration. This way, the bookmark has a beginning and an end.
- With no setting, a punctual bookmark is created.
- **Camera**: Select one or more cameras in which this bookmark is created.

To learn more about Bookmark, check the Surveillance client manual.

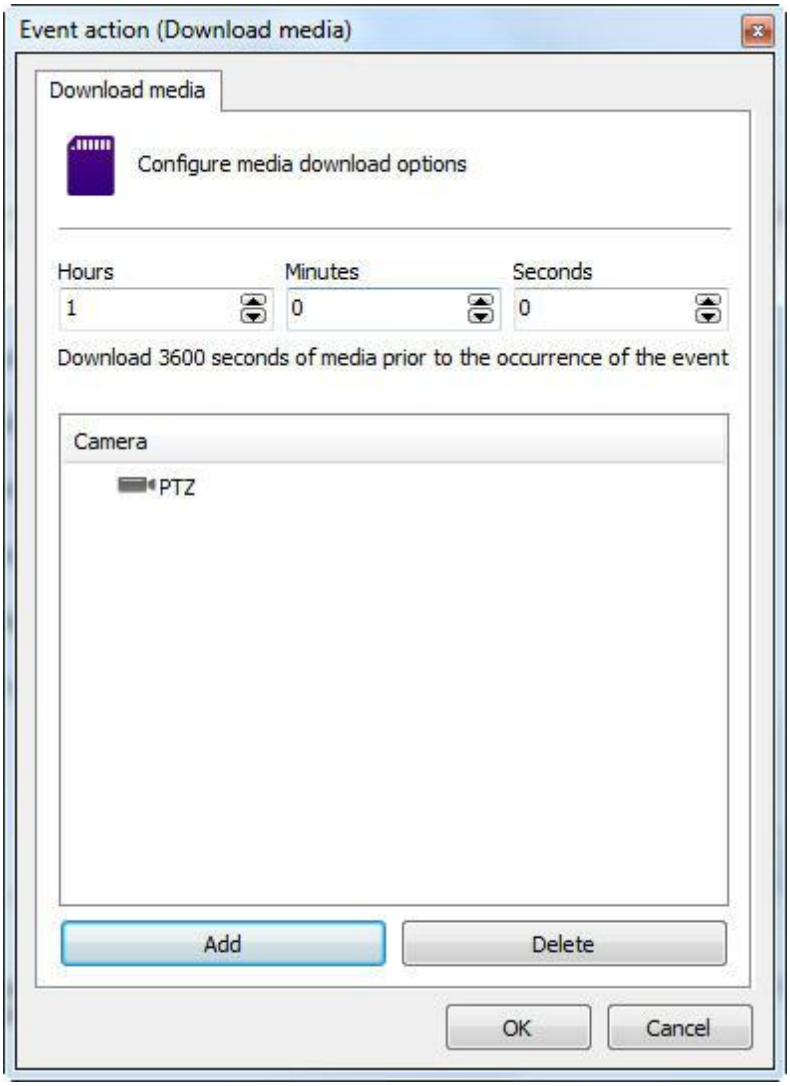
© 2002 - 2020 by Digifort, all rights reserved

6.1.10.12 Download device recordings with edge recording support

The edge storage system also allows you to download recordings when any system event occurs, allowing several operations such as:

- Download recordings using a scheduled event, creating a scenario in which the camera recordings can be downloaded daily, at a scheduled time
- Download recordings with different resolution when an event occurs

To configure this event, simply select the desired period of time to match the camera recording to the Digifort recording.
In the image below, the event will get 1 hour of recording **previously** to the event triggering on the "**PTZ**" camera:



© 2002 - 2020 by Digifort, all rights reserved

Note: Every combined downloaded recording overwrites any existing recording if they are at the same time.

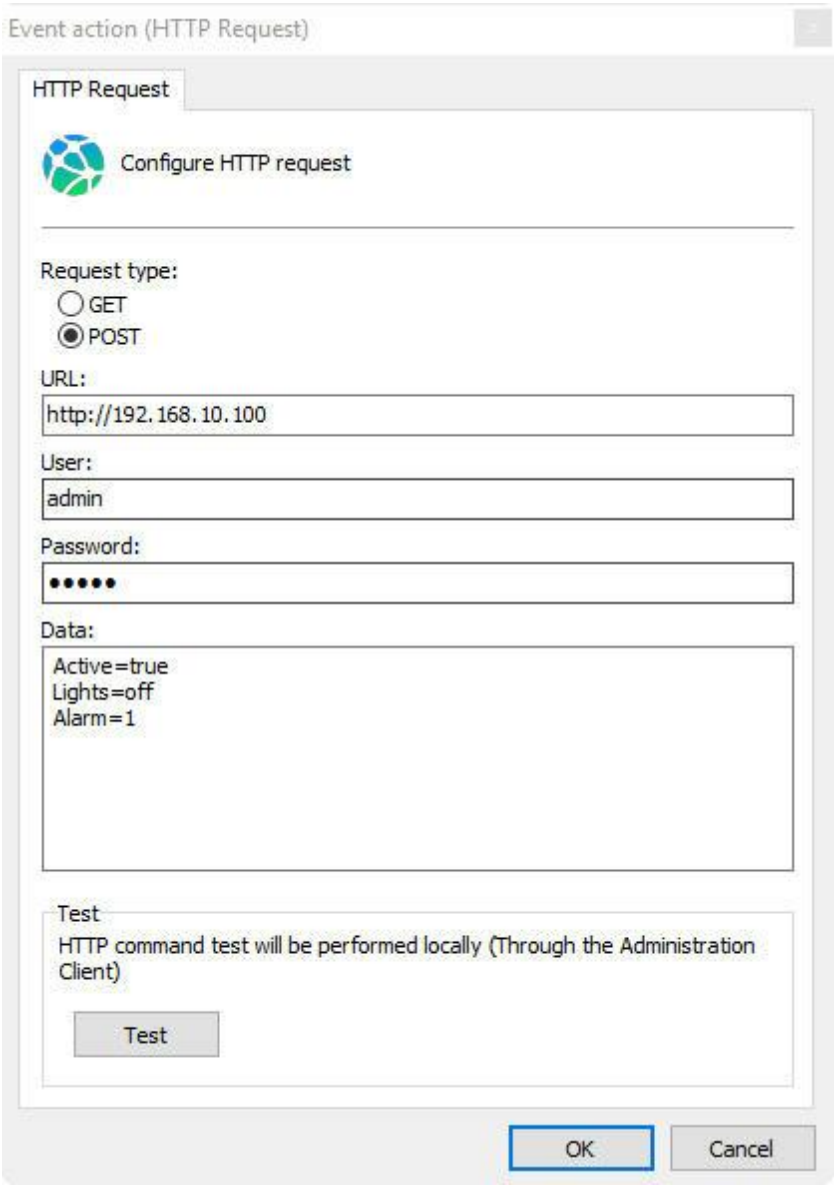
6.1.10.13 Send a HTTP Request

The HTTP request aims to create a channel of communication between Digifort and external software. This action allows integration of Digifort with any hardware or software that can process HTTP commands, for example: cameras, access control software, etc.

This feature requires a minimum knowledge of web programming for better understanding of its operation.

To start setup click "**Configure request".** And the following screen appears:

© 2002 - 2020 by Digifort, all rights reserved



This screen has the following settings:

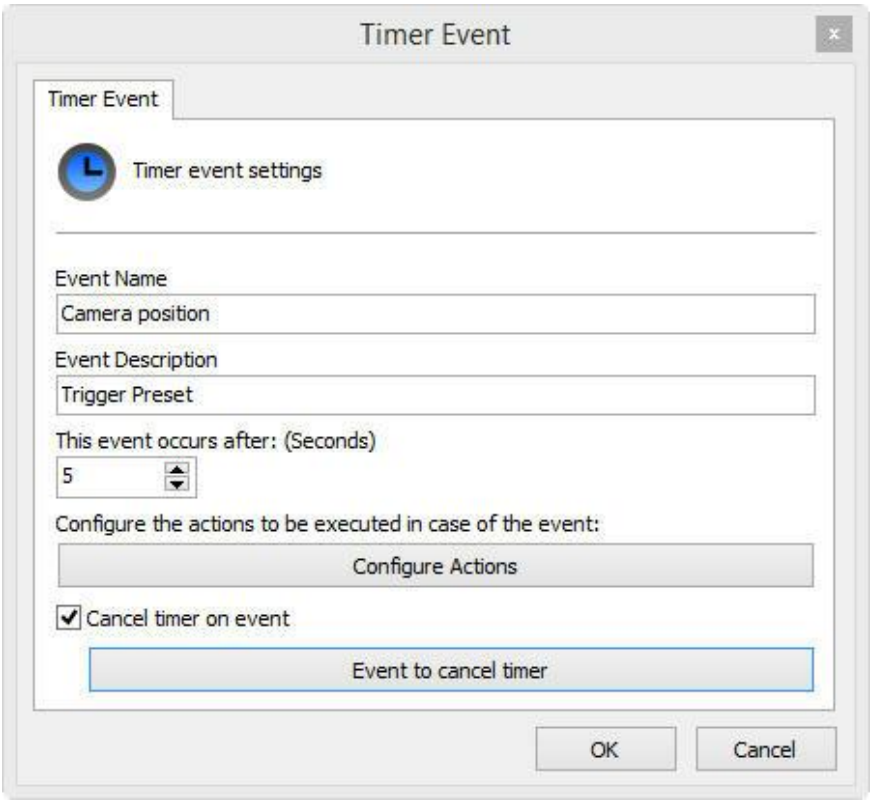
- **Request type**: Request: GET, where all parameters are in the URL.
- **Username:** User authentication command.
- **Password:** password for authentication command.
- **Data:** when the request: POST is selected the field for data becomes available.
- **Test**: It allows you to test HTTP action by sending the command configured above.

HTTPS commands are also supported.

© 2002 - 2020 by Digifort, all rights reserved

6.1.10.14 Create timer events

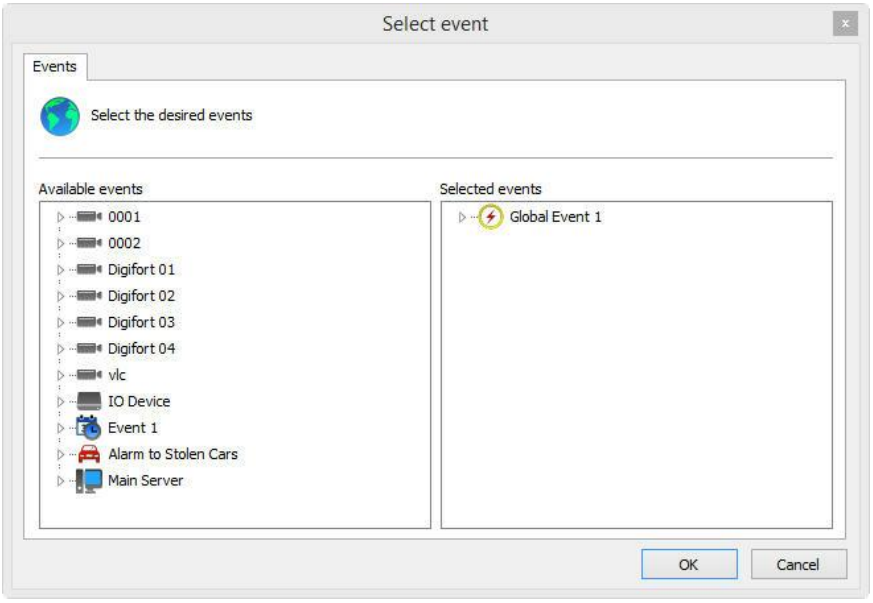
Timer events are events that trigger other events after a configured time. It is possible, for example, to detect motion in any camera, trigger a siren precisely at the time of the event, and, through an event timer, position a camera in a given position five seconds later. If this action is to be applied in the occurrence of the selected event, select this option and click on **Configure Actions**, as shown in the figure below:



In this screen, enter the name of the event, its description, and set how many seconds after the main event it is to take place. At last, click on **Configure Actions** to configure the actions that this event will perform. To learn how to configure alarm actions, see How to configure alarm actions..

Cancel timer event. It is possible to cancel a timer event in the occurrence of another event, which can be selected by clicking on **Event to cancel Timer**. Simply select the desired event as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved

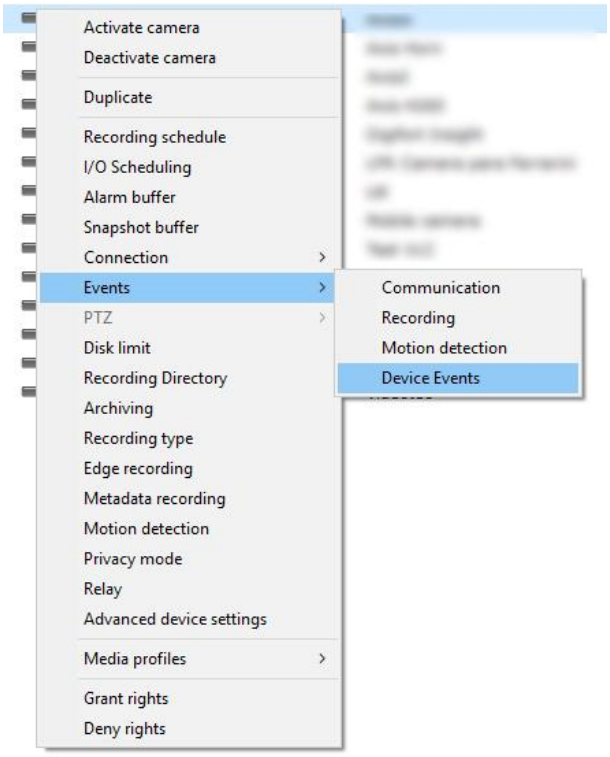


If the selected event takes place before the timer event is triggered, it will abort its execution.

6.1.11 Camera management functions

Digifort allows the basic configurations in common with all cameras to be applied in batch.
Select the desired cameras and click on the right button, opening the Options Menu, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



The options menu offers the following functions:

6.1.11.1 Activate camera

Activates the recording of the selected cameras

6.1.11.2 Disactivate camera

Disactivates the recording of the selected cameras

6.1.11.3 Duplicate camera

Duplicates the registration of the camera, creating a new registration with the same information, just adding "-Copy" to the end of the name and also creating a new folder as a recording directory (also with the suffix "-Copy"), allowing the creation of "templates" of cameras already pre-configured and facilitating server administration

6.1.11.4 Recording scheduling

Configures the scheduling of recording of the selected cameras. To learn how to use this feature, see How to configure the scheduling of recording.

© 2002 - 2020 by Digifort, all rights reserved

6.1.11.5 Events scheduling

Configures the scheduling of events of the selected cameras. To learn how to use this feature, see How to configure the scheduling of recording.

6.1.11.6 Alarm buffer

Modifies the configurations of the image buffer. To learn how to use this feature, see How to configure the Image Buffer.

6.1.11.7 Snapshot Buffer

Changes Snapshot buffer settings. To learn how to use this feature, see Snapshot Buffer.

6.1.11.8 Connection

Allows changing Address, Authentication, Timeout and Visualization Timeout settings. To learn how to configure this feature, see How to add a camera.

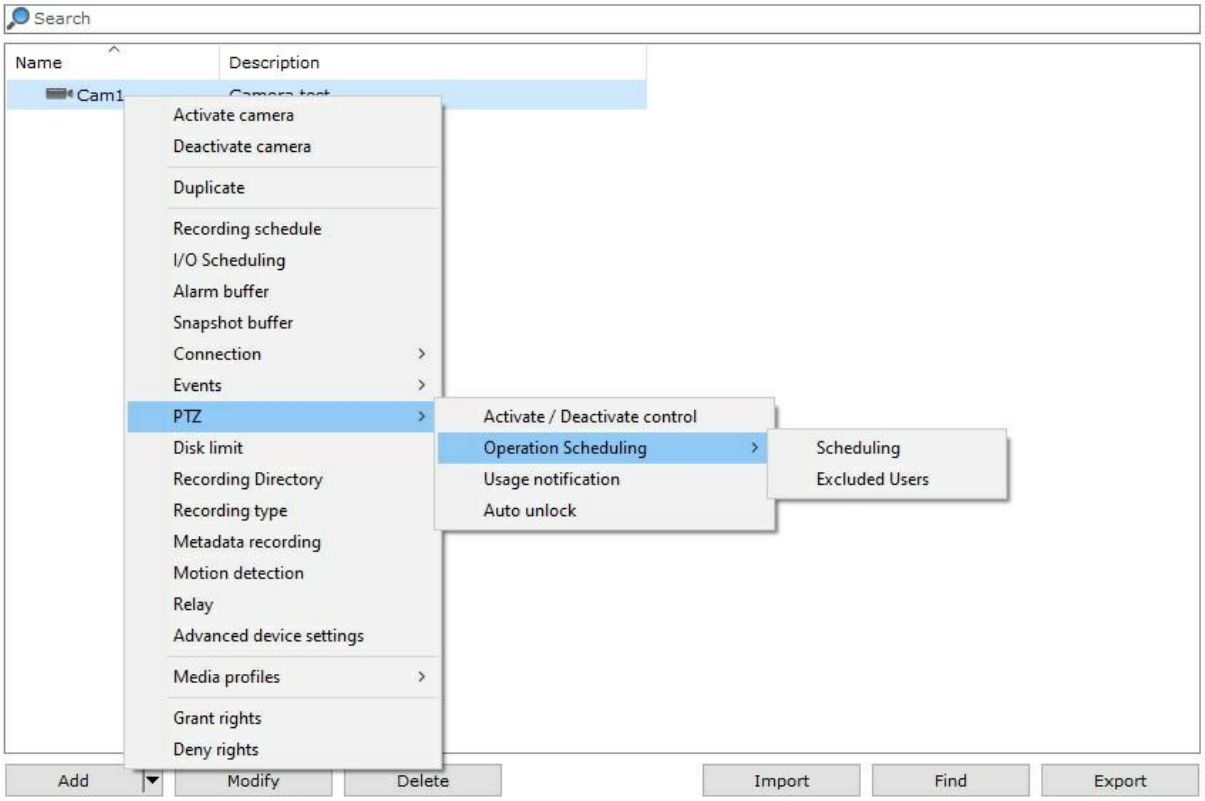
6.1.11.9 Events

Configures events from selected cameras. To learn how to use this feature, see Events

6.1.11.10 Configuração PTZ em massa

To perform bulk PTZ configuration, follow the image below:

© 2002 - 2020 by Digifort, all rights reserved



In your Administration Client, navigate to the Cameras section.

By right-clicking on a camera having the PTZ function, as shown in the image above, the following bulk configuration options will be available:

- **Activate/Deactivate Control**: It allows the administrator to activate or deactivate the camera's PTZ controls.
- **Operation Scheduling**: It allows you to schedule when PTZ controls can be activated and checks which users are excluded from configuration limitations.
- **Use Notification**: It allows you to choose whether the administrator will be notified when PTZ is used.
- **Automatic Release**: It allows the user to release PTZ.

6.1.11.11 Disk limit

Modifies the configurations of the disk limit of the selected cameras. To learn how to use this feature, see Disk Limits

6.1.11.12 Type of recording

Modifies the type of recording of the selected cameras. To learn how to use this feature, see Recording

© 2002 - 2020 by Digifort, all rights reserved

6.1.11.13 Edge Recording

Changes edge recording settings. To learn how to configure this feature, see Edge Recording

6.1.11.14 Metadata Recording

Changes metadata recording settings. To learn how to configure this feature, see Metadata.

6.1.11.15 Motion Detection

Changes motion detection settings. To learn how to configure this feature, see Motion Detection.

6.1.11.16 Privacy Mode

Changes privacy mode settings. To learn how to use this feature, see Privacy Mode

6.1.11.17 Relay

Activate Relay for the selected cameras. To learn how to config this feature see How to configure the visualization of the camera

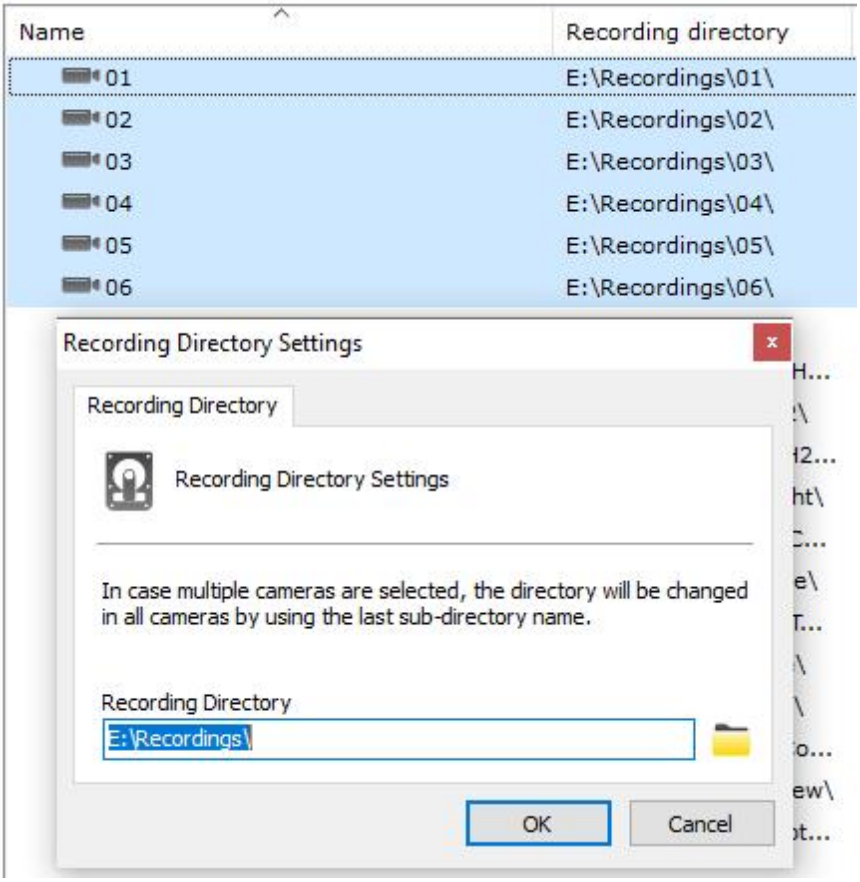
6.1.11.18 Multiple Camera Recording Directory Change

The Administration Client now allows you to change the recording root directory of multiple cameras simultaneously. To change the recording directory, simply select the cameras, right-click on the camera list and select “Recording Directory” in the context menu pop-up.

The system allows you to define a “Root” directory which will be used as basis for all cameras. The name of the last subdirectory (usually the camera’s name) will be kept. For example, if the camera is currently being recorded in “E:\Recordings\01” and you wish to change to “E:\NewRecordings”, the system will change the directory of this specific camera to “E:\NewRecordings\01” and thus successively for all selected cameras.

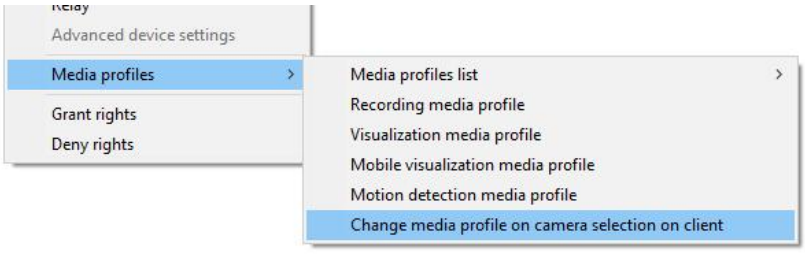
It is important to emphasize that changing the directory will not move the recordings from the old directories to the new ones. This procedure must be done manually, with the server service stopped.

© 2002 - 2020 by Digifort, all rights reserved



6.1.11.19 Media Profiles

Change the video profile when selecting the camera in the Monitoring Client:



6.1.11.20 Media Profiles

Add, Change or Delete Media Profiles on multiple cameras simultaneously, as long as they feature the same media options.
To select the cameras with the same media profile, select a desired camera and press **Ctrl + M**. If there are cameras with the same media profile as the selected camera, it will be automatically selected.

Let us exemplify how logic works in the event of multiple profile selection. In the example, two cameras with the following settings will be used:

© 2002 - 2020 by Digifort, all rights reserved

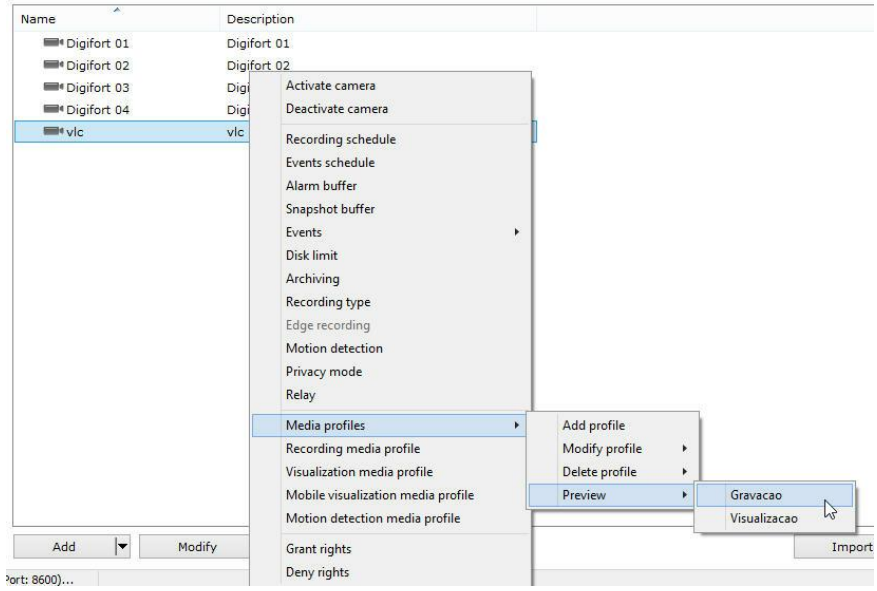
Camera 1
Viewing Profile
Recording profile
Mobile Profile

Camera 2
Recording profile

Let us analyze the following hypothesis individually:

- In the event that a **Viewing Profile** is **Added**, this profile will only be included **at Camera 2** and the current profile at **Camera 1** will be **changed** according to the new configuration;
- In the event a **Viewing Profile** is changed, the change will only be done at **Camera 1**;
- In the event a **Recording Profile** is changed, the changes will be done on both Cameras;
- In the event a **Mobile Profile** is deleted, it will only take effect at Camera 1;
- In the event a **Recording Profile** is deleted, both cameras will have their profiles deleted;

It is also possible to view the image from the camera through the list by clicking on Preview:



6.1.11.20.1 Motion detection media profile

Changes motion detection media profile settings. To learn how to configure this feature, see Motion Detection. .

© 2002 - 2020 by Digifort, all rights reserved

6.1.11.20.2 Mobile viewing media profile

Changes mobile viewing media profile settings. To learn how to configure this feature, see Media Profile for Mobile Access..

6.1.11.20.3 Viewing media profile

Altera as configurações do perfil de mídia de visualização. Para aprender a configurar este recurso veja Media Profiles.

6.1.11.20.4 Recording media profile

Changes recording media profile settings. To learn how to configure this feature, see Media Profiles.

6.1.11.21 Grant Rights

Grants user rights on devices. To learn more, see Rights .

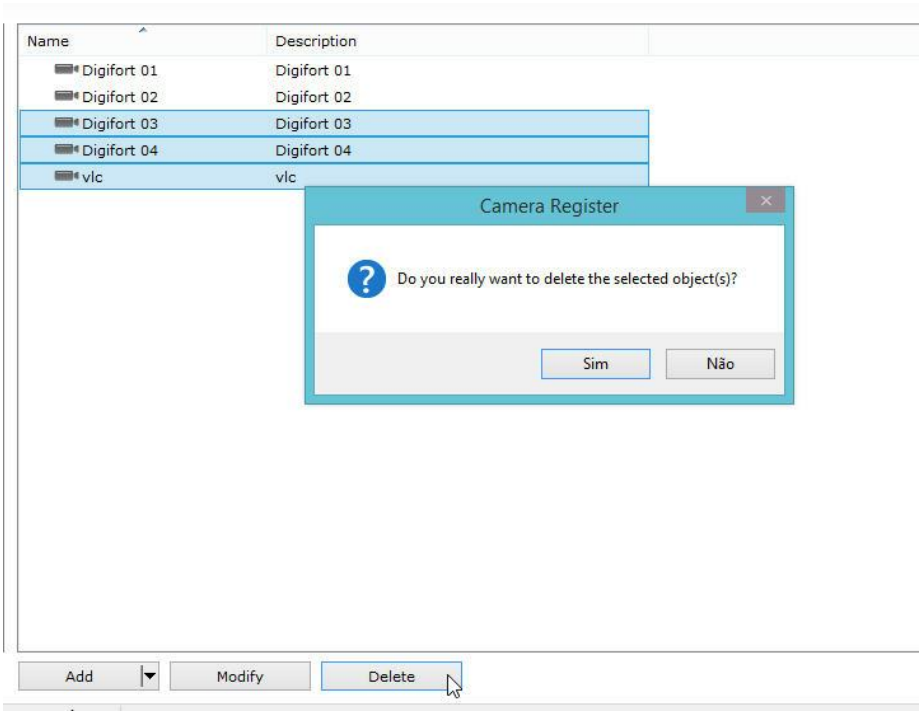
6.1.11.22 Deny Rights

Denies user rights on devices. To learn more, see Rights .

6.1.11.23 Delete Cameras

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

© 2002 - 2020 by Digifort, all rights reserved

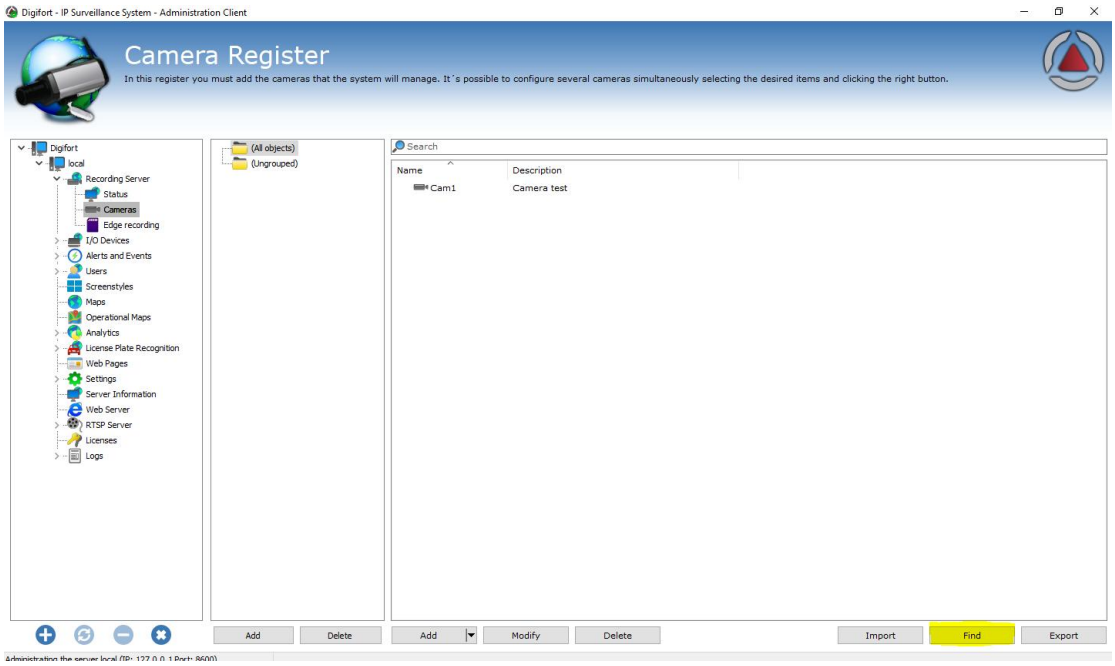


6.1.12 Locating and registering cameras automatically

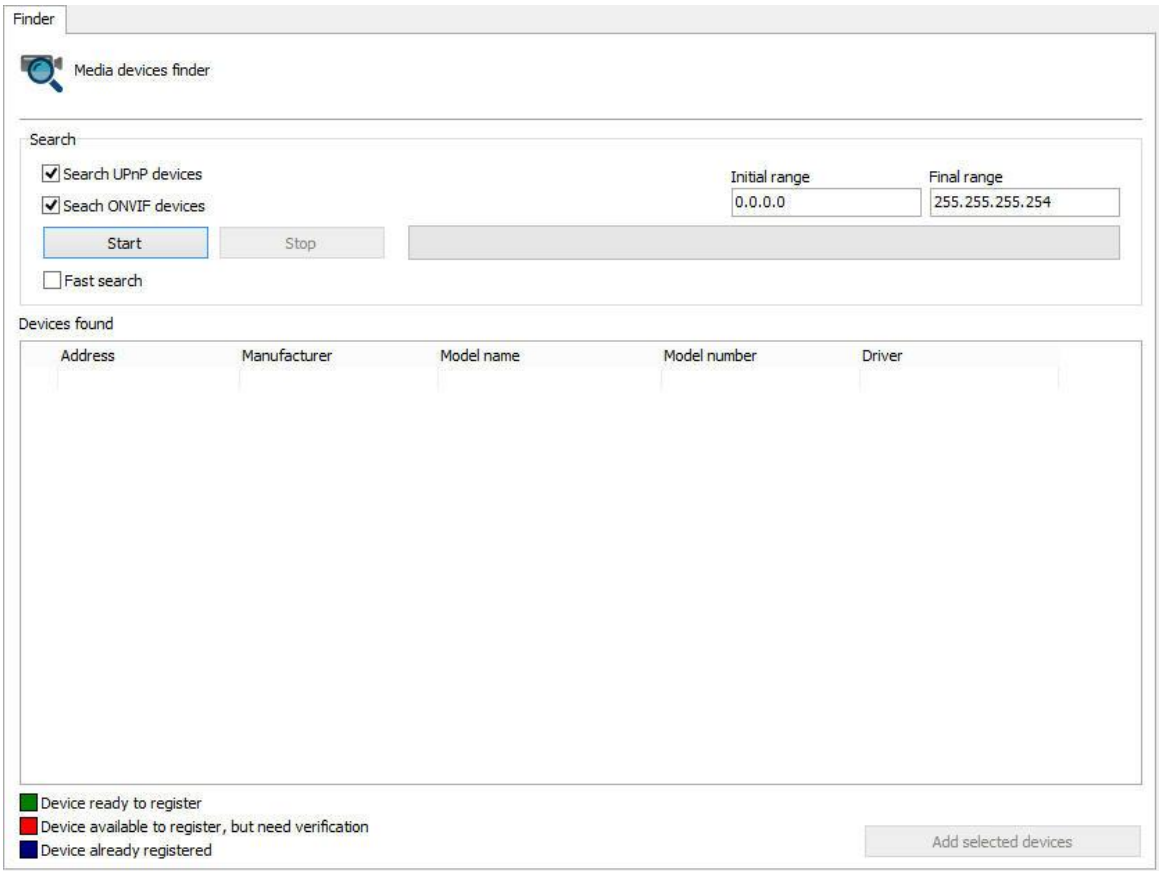
Digifort features the option of automatically locating and registering in the system those cameras with UPnP and ONVIF support.
Find out how this feature works below:

In the camera registration screen, click on the **Find** button, as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved



The following screen will be displayed:

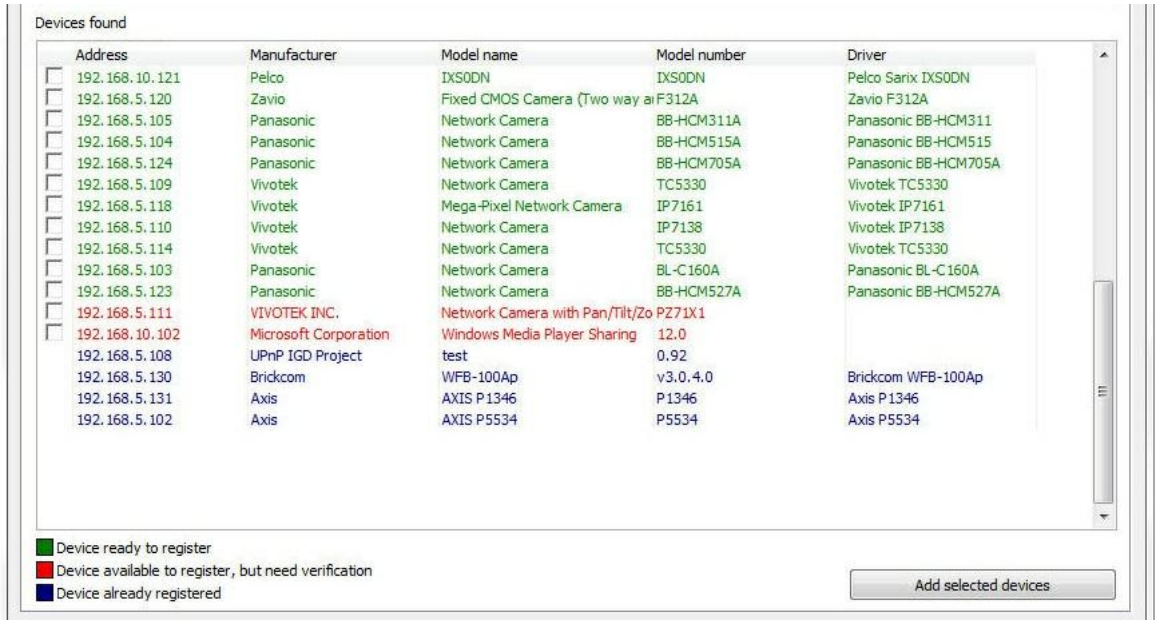


Equipment search is done on this screen. There are two types of search:

© 2002 - 2020 by Digifort, all rights reserved

- **Normal**: The normal search for UPnP equipment takes an average of 40 seconds to find the equipment. This happens because, in addition to finding the equipment that have replied to a request, this search looks for UPnP broadcast packages on the network, causing the search to find more devices.
- **Quick search**: The quick search for UPnP equipment takes an average of 15 seconds to find the equipment. This search only finds those devices that have replied to the UPnP request done by Digifort. To enable quick search, simply click the **Quick Search** check box;
- **Initial Range and Final Range**: Limits the search between the set IP range.

To start the search, click on **Start** and the message "**Wait, Finding Equipment**" will be displayed while the equipment is being located.
Once found, the equipment will be listed as shown in the figure below:



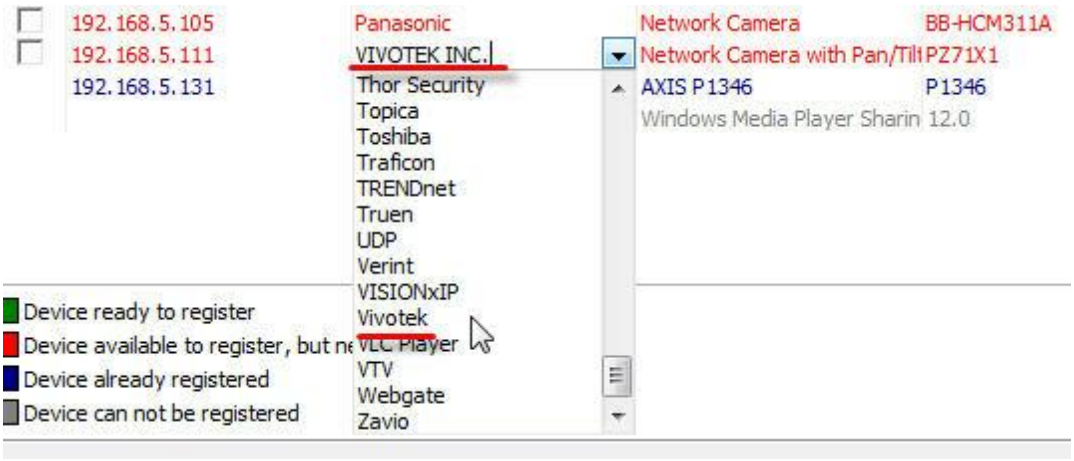
Three types of equipment can be found according to the caption in the bottom left corner of the screen:

- **Green - (Device ready to register):** These are the cameras found whose manufacturers and models have already been approved on Digifort.
  This camera equipment is ready to be added to Digifort.

- **Red - (Device available to register):** These are equipment that have not been found in the database of equipment approved on Digifort. This may take place either because the equipment is not actually approved or if the manufacturer/ driver is written differently from what is registered on Digifort.

If the name is incorrect, it can be corrected on the same screen through a check box, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



- **Blue - (Device already registered**): These are equipment thathave already been registered on Digifort.

- **Gray - (Device cannot be registered):** In this case, the equipment or program found has not returned any IP address and it cannot be automatically added.

There are two ways to register the equipment found.

6.1.12.1 Registration of one device only

- **Registration of one device only:** Select a product over the box as shown below:

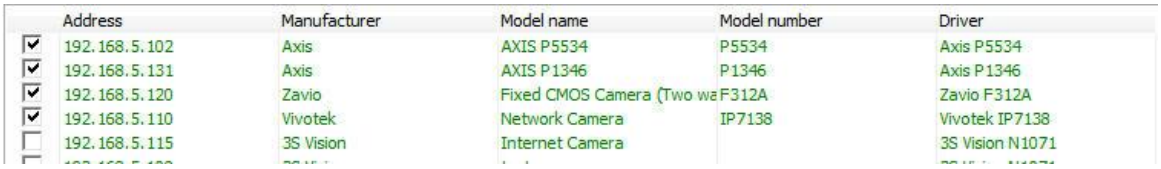


Address	Manufacturer	Model name	Model number	Driver
192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138

After selecting the device, click the **Add selected devices** and the camera registration screen is displayed with **Manufacturer**, **Camera model, IP** and **Port** fields already filled. Thus we will only have to fill out name, description, recording directory, and password of the camera.

6.1.12.2 Registration of various devices

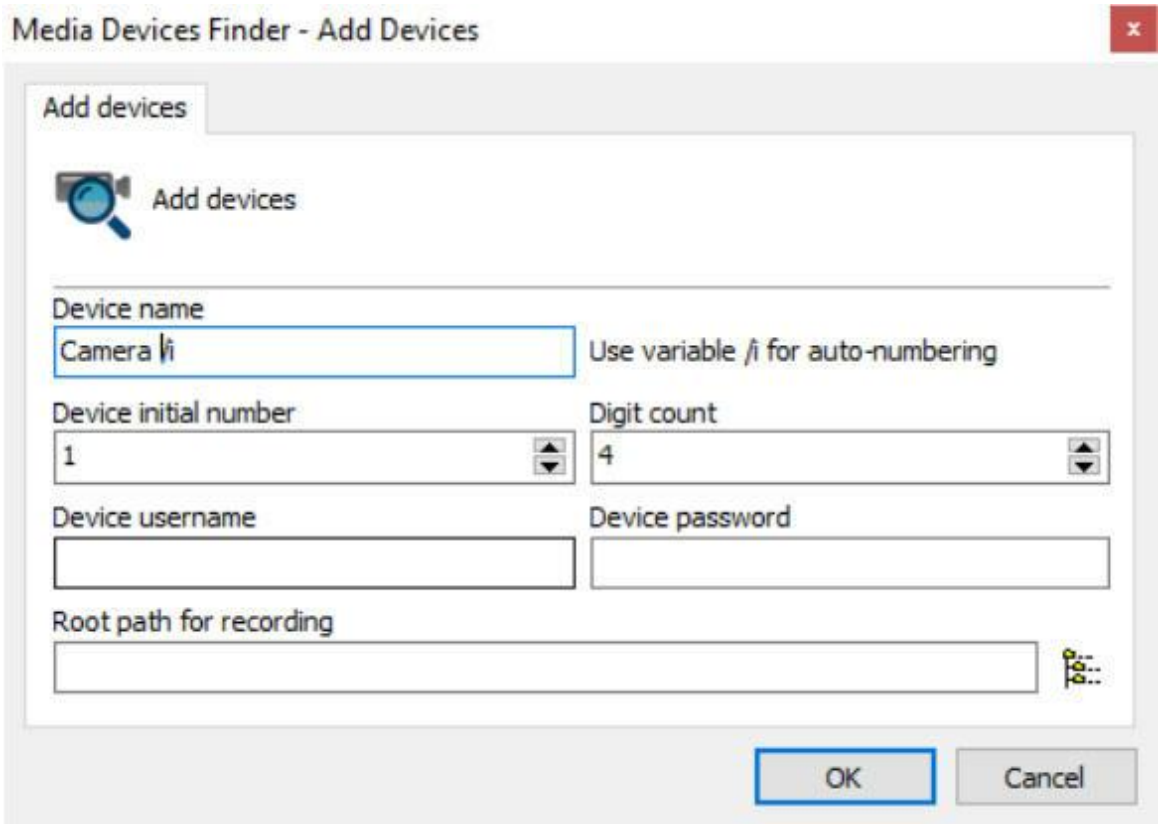
This feature can register multiple cameras simultaneously with sequential numbers. To begin, select several devices from the selection box as shown below:



Address	Manufacturer	Model name	Model number	Driver
192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
192.168.5.131	Axis	AXIS P1346	P1346	Axis P1346
192.168.5.120	Zavio	Fixed CMOS Camera (Two wa	F312A	Zavio F312A
192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138
192.168.5.115	3S Vision	Internet Camera		3S Vision N1071

After selecting the device, click the Add selected devices and the following screen appears:

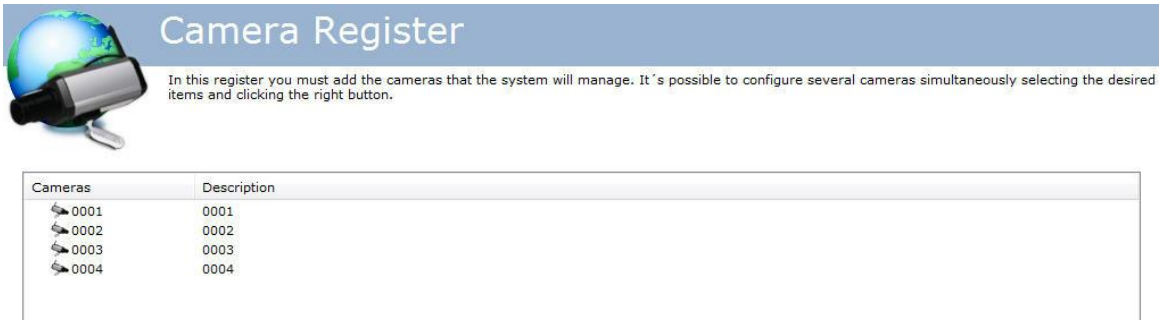
© 2002 - 2020 by Digifort, all rights reserved



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

- **Device name**: It allows you to name one or more cameras. To add the number after the initial name, simply insert the "/i" at the end.
- **Device initial number:** The name of the cameras will be recorded in the form of a sequence of numbers. This field will set the starting number from which to begin counting.
- **Digit count**: number of spaces you want. E.g.: If the counting starts with number 1 and number of decimal places is 4 then the name of the first camera registered will be 0001.
- **Device username**: User name used for Digifort to authenticate the devices.
- **Device password**: Password used for Digifort to authenticate the devices.
- **Root path for recording:** Enter a directory where Digifort will create a folder for each camera to store your recordings. This folder will have the same camera name (E.g.: 0001, 0002, etc.).

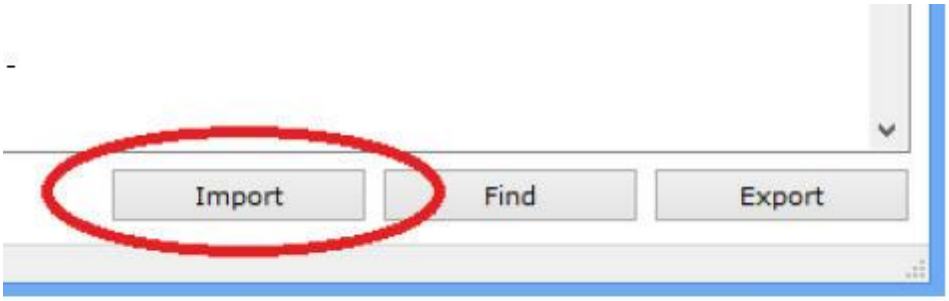
After registering various cameras, their status will change automatically to **BLUE (Camera already registered)**. This shows the cameras have been registered successfully as shown below:



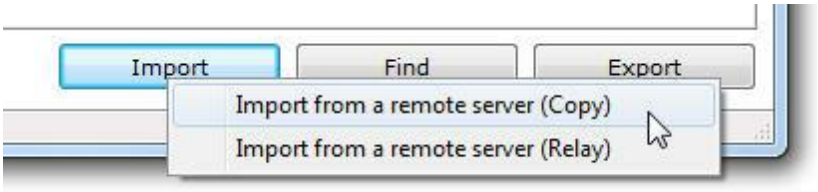
© 2002 - 2020 by Digifort, all rights reserved

6.1.13 Importar objetos de outros servidores

Importing objects from a remote server is a tool that will help manage large Digifort installations.
This new tool allows the system administrator to import objects from other Digifort servers, streamlining the configuration of a new server.
The system allows the import of any object, as well as Cameras, Alarm Devices, Users, Analytics Settings, and LPR.
Every configuration screen that allows the import of objects now features an **"Import"** button.



In the case of importing cameras, there are two options as shown in the figure below:



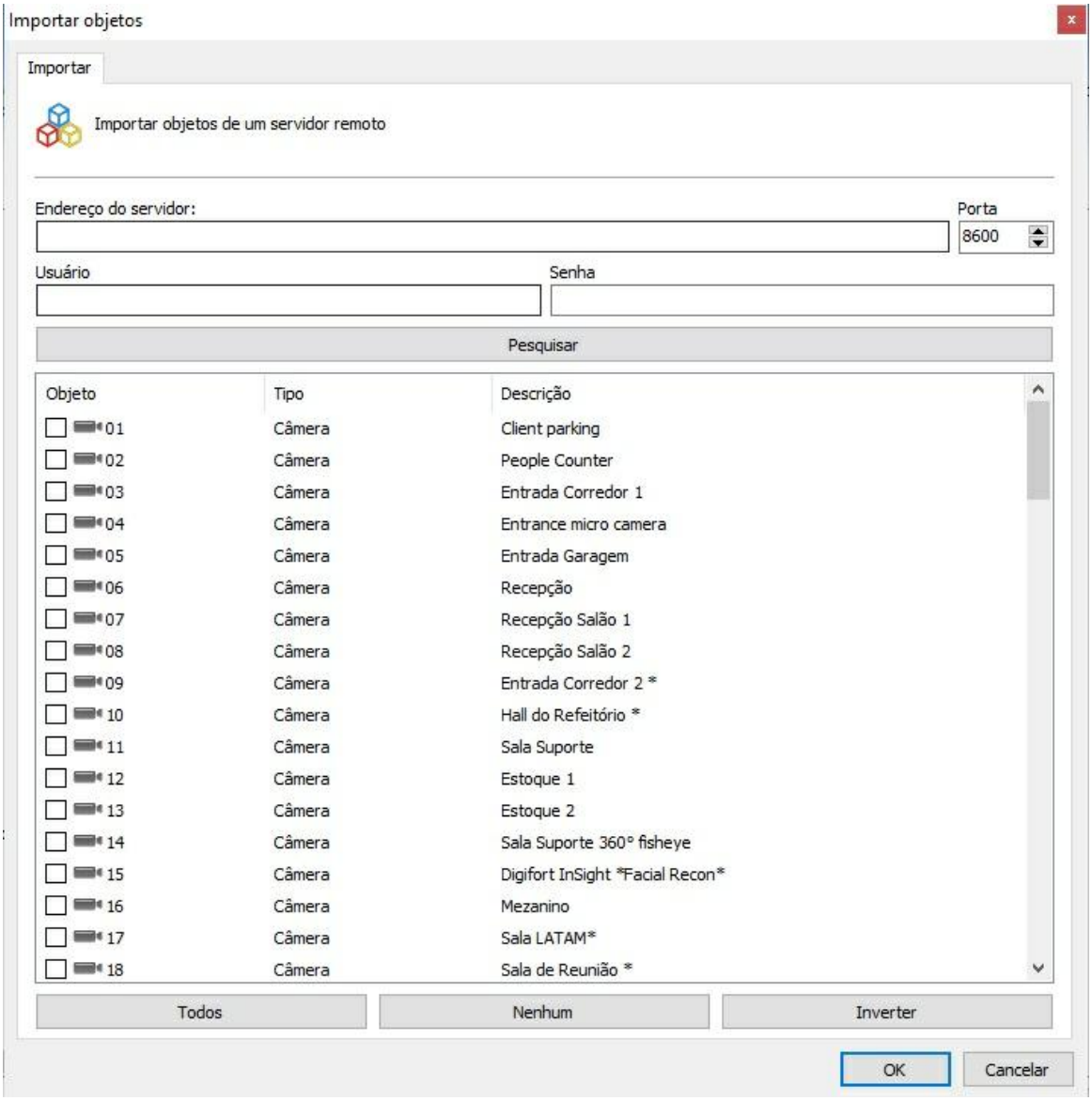
Import cameras from a remote server (copy): When the import is done as a copy, the settings will be imported just as they are on the imported server. An important example is the recording unit: if on the source server the cameraswere recording on the E: directory and in the current server this unit does not exist, the cameras 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 using the Digifort RTSP Server driver, in which case it will fetch the images from the source server.

To import, simply enter the **source server IP,** the Digifort **communication port** and a Digifort **username and password**. The objects that will be loaded will be those that the user holds

© 2002 - 2020 by Digifort, all rights reserved

management rights for that type of object.
Click on **Search** and the objects will be displayed in a list as shown in the image below:



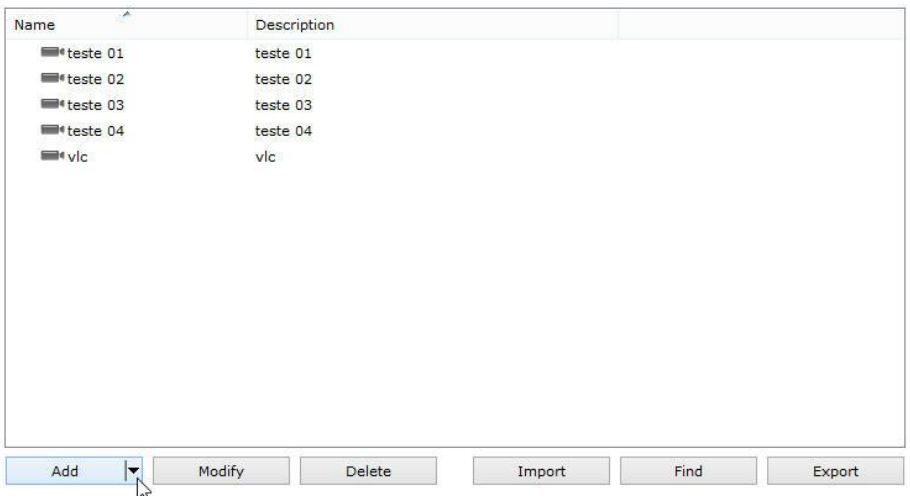
Select the desired objects and click on **OK**.

6.1.14 Multichannel device registration

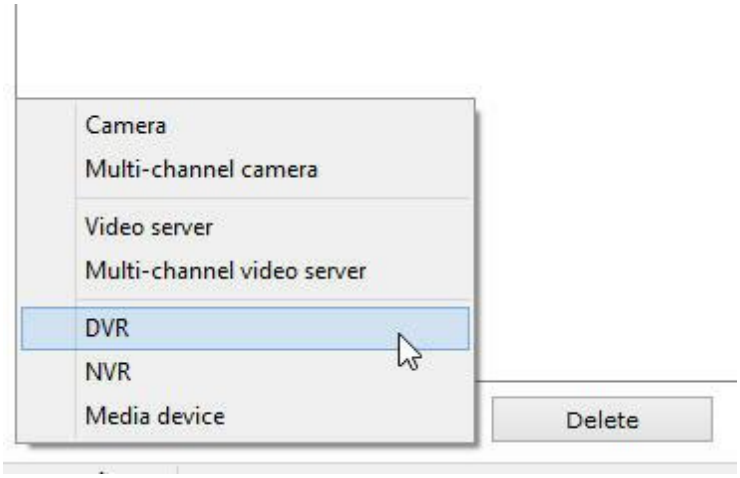
Digifort enables the registration of multichannel devices to be easily done, such as DVRs, NVRs, Video Servers, Multi-lens Cameras, etc.
For example, this option allows all channels on a DVR to be registered at once.

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

© 2002 - 2020 by Digifort, all rights reserved



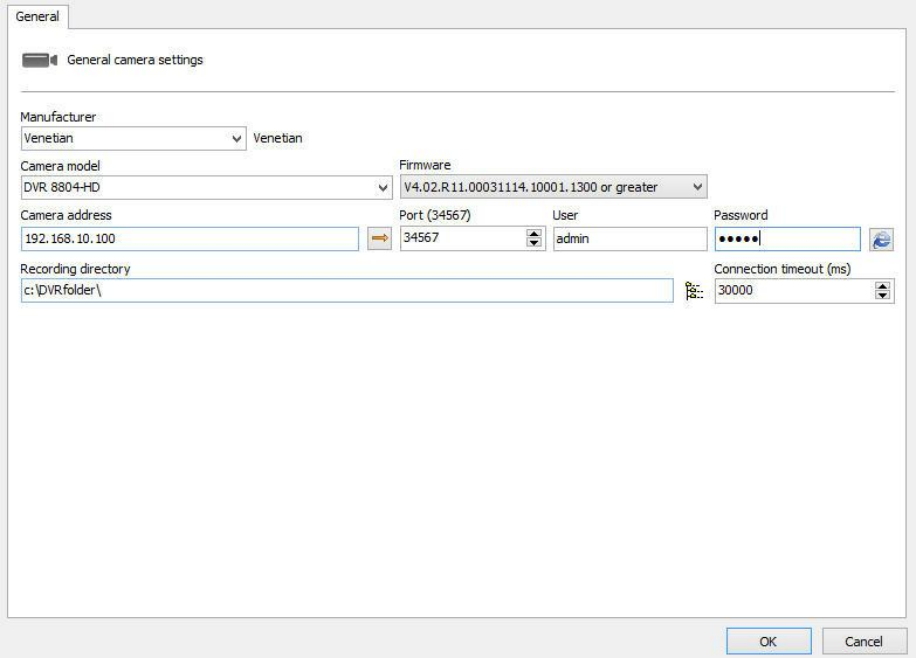
The options for those supported devices that can be registered are shown as in the image below:



6.1.14.1 Registering a DVR

To illustrate, a 4-channel DVR will be registered.
After clicking on **Add ->DVR**, the general information screen will be displayed as in the image below:

© 2002 - 2020 by Digifort, all rights reserved



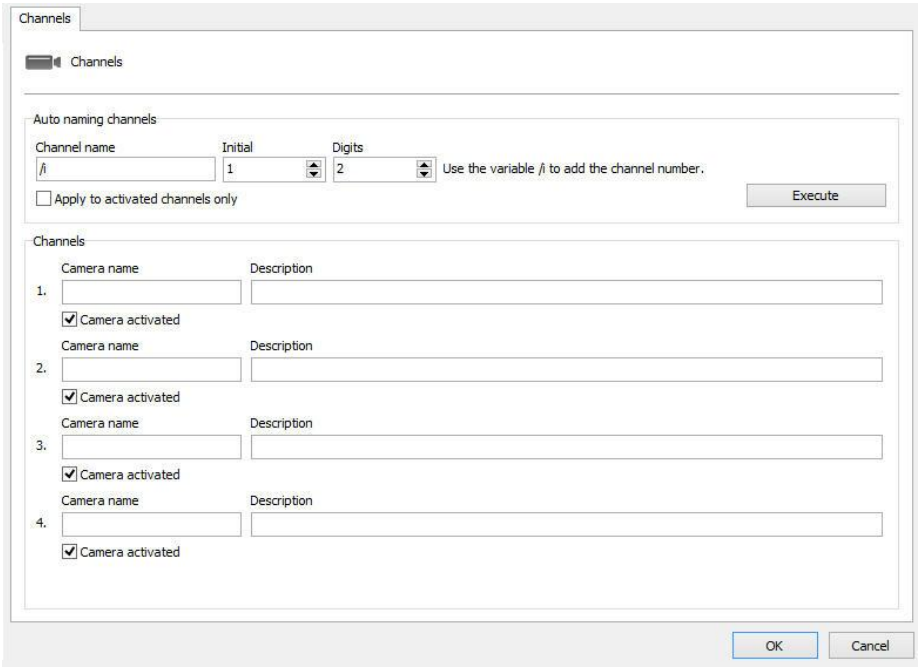
Basic information on the equipment must be filled in.**Manufacturer, Model, IP, Communications port, Username, Password, and the Directory where the recordings will be stored.**

After filling the data in, as illustrated in the previous image, click on the **Channel** option located on the side menu, as shown below:



The following screen will be displayed:

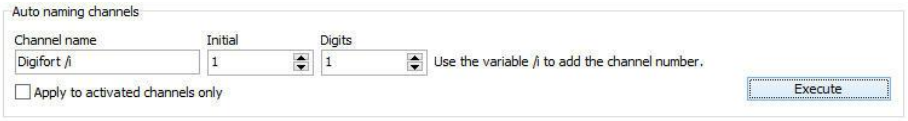
© 2002 - 2020 by Digifort, all rights reserved



The following options are available:

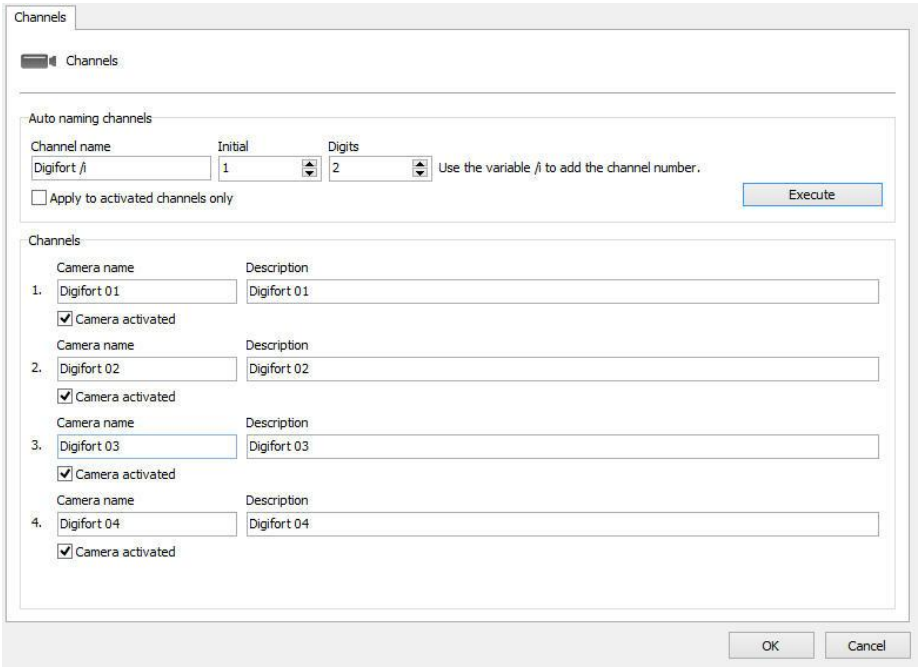
- **Auto naming Channels**: Allows a naming standard to be applied on all channels of the device.
- **Channel Name**: Desired name followed by a number (feature /i).
- **Initial**: Starting number that will be applied to the channels.
- **Digits**: Number of digits that are required for naming.
- **Apply only to activated channels**: Applies a naming sequence only to those channels activated at the bottom of the screen.
- **Execute**: Applies the standard to all channels.

Example: To register a DVR with the naming standard: Digifort 1, Digifort 2, Digifort 3, etc., the following configuration will be carried out:



To register a DVR with the naming standard: Digifort 01, Digifort 02, Digifort 03, etc., the following configuration will be carried out:

© 2002 - 2020 by Digifort, all rights reserved

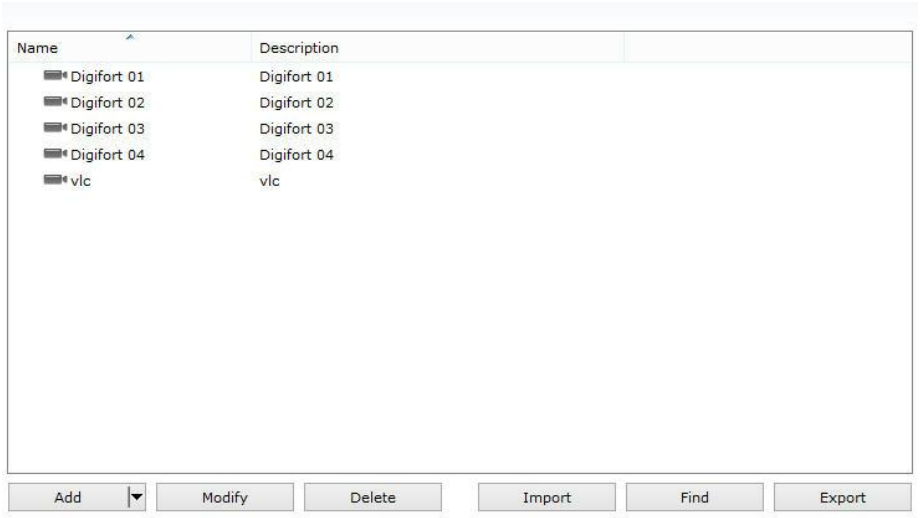


In the **Channels** area, it is possible to check/modify the name applied.
It is important to remember that each channel is registered as an independent device, thereby consuming 1 recording license per registration.

NOTE: The device name cannot be changed after registration.

The recording folders will be created with the names chosen for the channels within the selected root folder.

To finish registration, simply click on **OK** and all DVR channels will be simultaneously included.



© 2002 - 2020 by Digifort, all rights reserved

6.2 Camera Groups

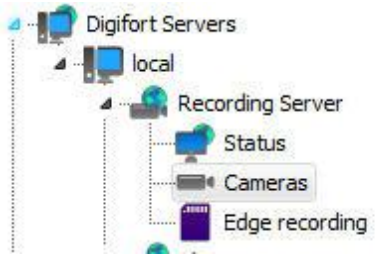
The system allows the creation of Camera Groups for improved organization of objects.

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

The Surveillance Client offers great flexibility towards working with groups:

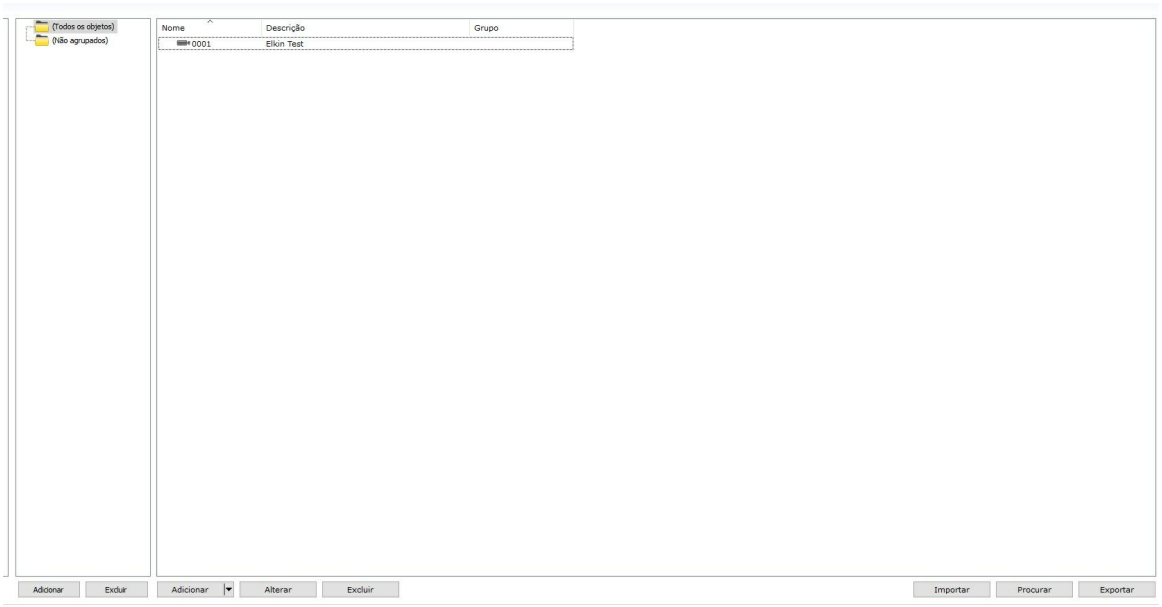
- You can drag and drop a group on the screen, and cameras from that group will be added to the surveillance.
- To add cameras from the group and all cameras from all subgroups, simply press and hold the Shift key while dragging and dropping the desired group.
- You can drag and drop a group onto the media player to playback the cameras from that group. To add cameras from subgroups, simply press and hold the Shift key while dragging and dropping.
- By right-clicking on the group, you can play all cameras from the group and, if desired, the cameras from all subgroups as well.
- By right-clicking on the group, you can send all cameras from the group to the virtual matrix and, if desired, the cameras from all subgroups as well.

To create camera groups, access **Camera Registration**, locate the Recording Server icon and then click on the Cameras icon, as illustrated in the figure below:



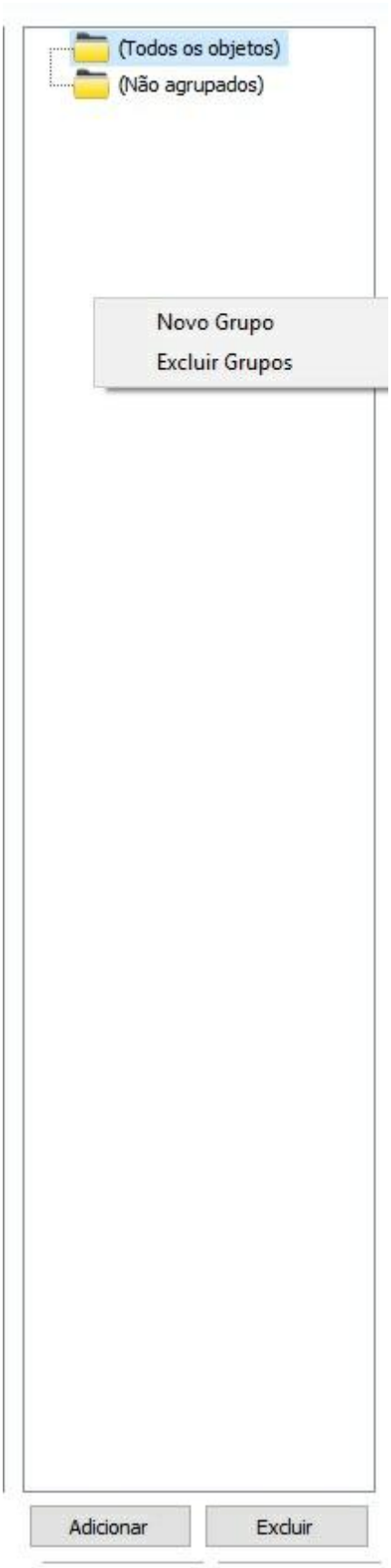
Once this is done, camera registration will be displayed, as illustrated in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



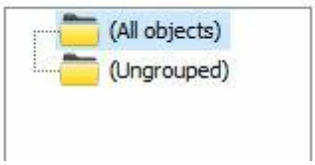
To add a group, click on the Add button in the groups section, on the left, or right-click on the group zone as shown in the image below.

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

By clicking on the Add button, the system will request you to inform the name of the group to be created and then the group will become available on the list.

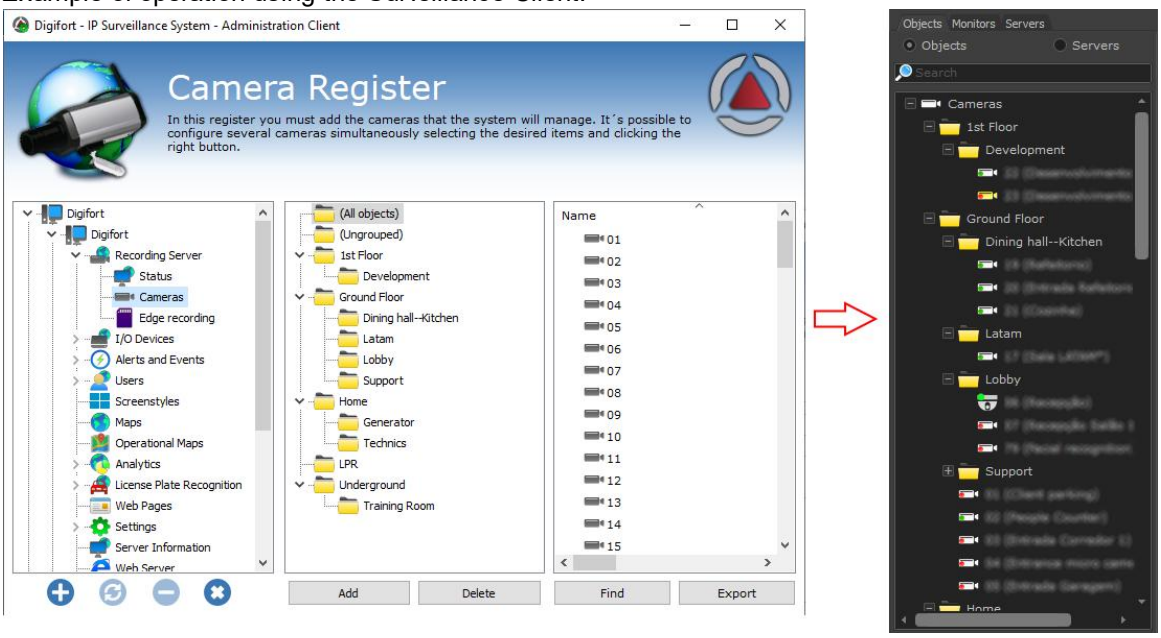


Once the group has been created, to add one or more cameras to the group, simply click on the desired camera(s) and drag it/them to the group. You can also create subgroups by simply creating a new group with the larger group selected or then drag all desired groups into a larger group:



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

Example of operation using the Surveillance Client:



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

To see this new feature in action, visit the videos available on our YouTube channel: http://www.

© 2002 - 2020 by Digifort, all rights reserved

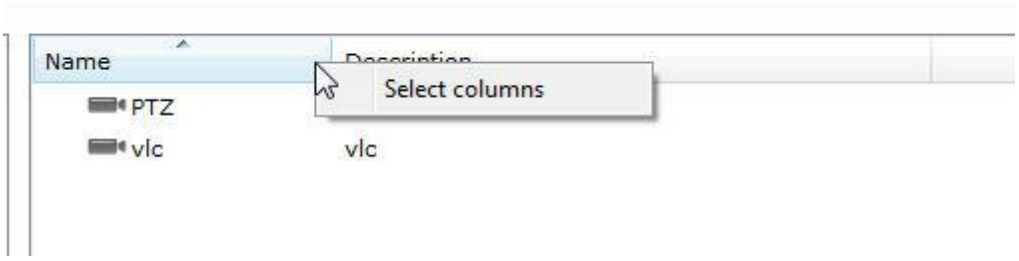
youtube.com/DigifortChannel

https://www.youtube.com/watch?v=IaNEKPyzdL0&list=PLFIhAF6oQd_rJjV3wEWHB8f0ZuzruvrOS

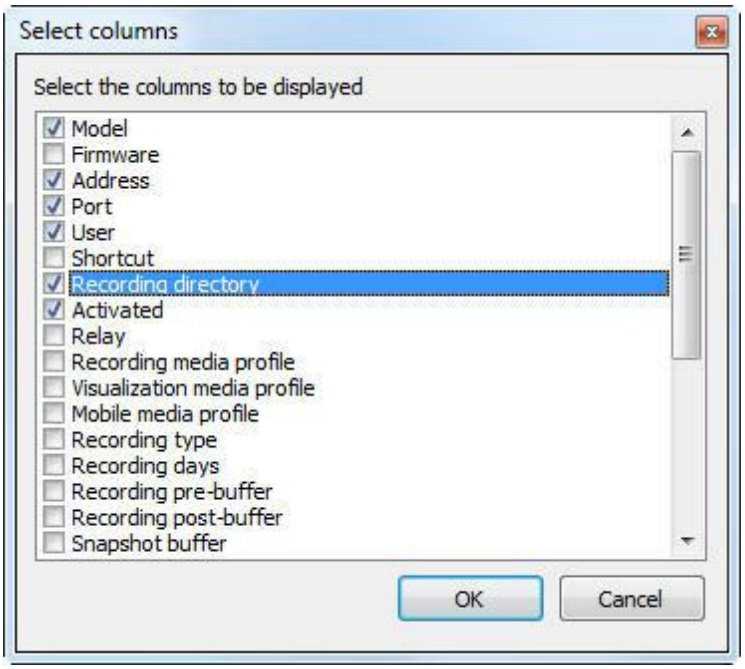
6.3 Column Organization

The Administration client now has a great tool that assists the object administration and configuration in the server. The extended columns are implemented in all registration screens that have information that can be displayed in a list.

In the camera registration, for example, the user can select which columns should be displayed. To do that, click with the **right button on the columns**, and then click on **Select columns** as shown below:

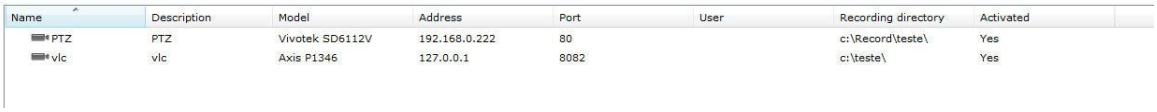


The following screen will appear with the available columns options:



Select the columns you want, and then click on **OK**. They are displayed on the main screen:

© 2002 - 2020 by Digifort, all rights reserved



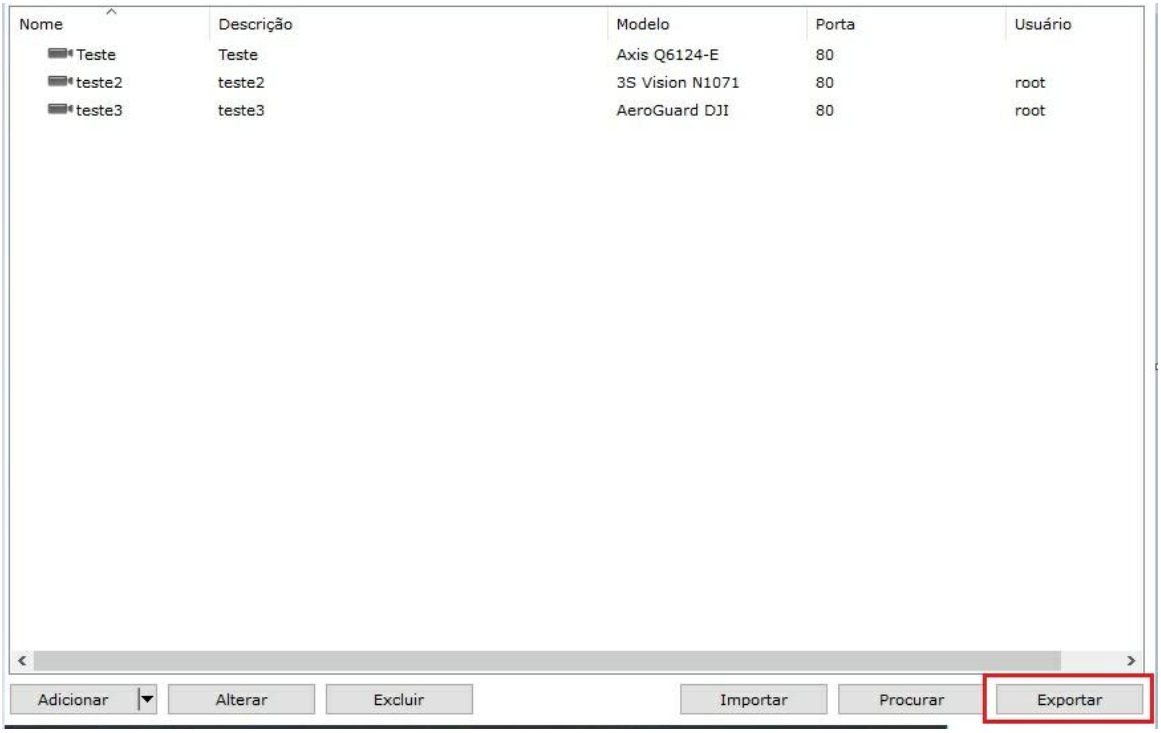
Name	Description	Model	Address	Port	User	Recording directory	Activated
PTZ	PTZ	Vivotek SD6112V	192.168.0.222	80		c:\Record\teste\	Yes
vlc	vlc	Axis P1346	127.0.0.1	8082		c:\teste\	Yes

If you want, the information displayed can be exported to a .csv file. Simply click on **Export** on the lower-right corner of the main screen.

6.4 Exporting Data from the Recording Server

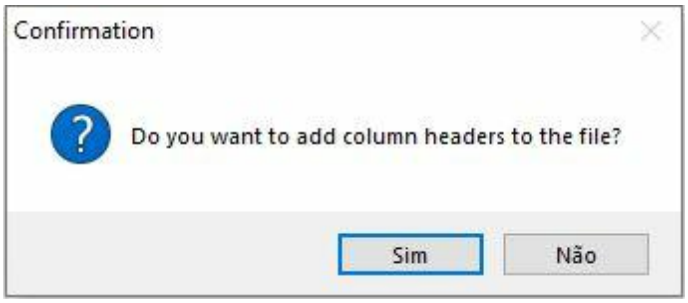
The Digifort Administration Client can export in the .CSV format, which contains a summary of the recording server.Such information can be used for various purposes, such as reports and controls.

To do it, navigate to your Recording Server, on the Cameras tab, click on Export on the lower right corner:



Set a path to save the file and then the following window should appear:

© 2002 - 2020 by Digifort, all rights reserved



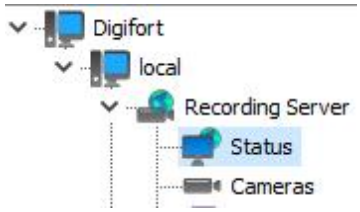
This window requests the confirmation to export the columns being displayed in your Recording Server. In the above example, the Name, Description, Model, Port, and User columns will be exported, as follows:

	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						

6.5 Monitoring recording server status

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

To access this feature, select the item Status within the 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 sorting by any column of the list. In addition, you can export the current data in a .CSV file.

The camera status screen design has been redesigned to provide more information. The screen is now single (it does not have the General and Status tabs) and it features a powerful dashboard with an excellent status summary.

The new dashboard in the right corner of the screen replaces the previous design in which 2 tabs were necessary (General and Details), and it features all

© 2002 - 2020 by Digifort, all rights reserved

the information that was previously displayed on the “General” tab.

A new information relative to the number of recording cameras was added to the dashboard.
This number will account for all cameras configured to record (Continuous, By Motion or By Event) that are currently in operation. The camera will be accounted for in this same value even if it is not currently recording to disk (as when configured to record by motion or event).

A new recording rate information per disk drive was also added to the dashboard. The system will now inform the recording rate (in MB/s and Mbits/s) of each disk drive and this will make it possible to check in detail bandwidth usage for each one.
With the new Camera Groups feature, upon selecting a group (or multiple groups), logs will be filtered to display only the selected camera groups.



Details:

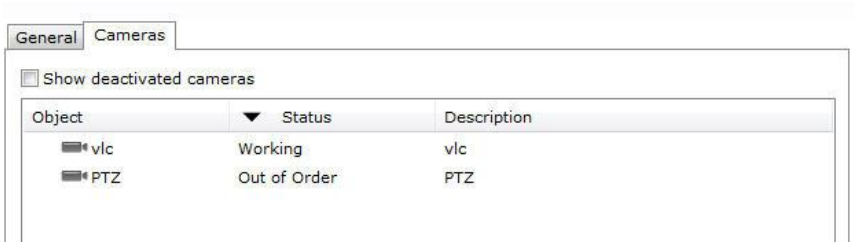
- **Total**: Total number of cameras registered on the server.
- **Activated**: Number of activated cameras.
- **Deactivated**: Number of deactivated cameras.
- **In operation**: Number of cameras in operation.
- **Recording**: Number of cameras that are recording.
- **Total FPS:** Total number of frames per second being transmitted to the server.
- **FPS Recorded:** Number of frames per second being recorded on the server.
- **Largest recording buffer**: The largest buffer time between server cameras.
- **Total rate of received data**: Amount of data received by the server over the network.
- **Total recording rate:** Amount of data being recorded per second on the disks.
- **E**: A summary of free and occupied disk space (in this case, E: drive).

© 2002 - 2020 by Digifort, all rights reserved

6.5.1 Monitorando o status de câmeras individualmente

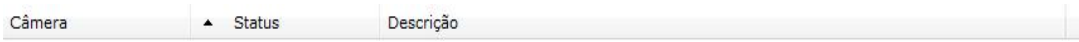
In this area of the system you can check the individual status of each camera, obtaining information such as its operating status, IP address, uptime, used disk space, etc.

To access this feature, click on the Cameras tab under the **Recording Server Status** item, as shown in the figure below:



On this screen, all the cameras registered and active in the system will appear and inform us about their functioning status. If the status is "In operation" the camera is functioning normally and if the status is "Out of operation" some communication problem with the camera is occurring, check the electrical and logic network.

The list can be ordered by the name of the cameras, their status or their description. To do this, just click on the desired topic. An arrow will indicate which topic is being listed and whether it is in ascending or descending order as shown in the figure



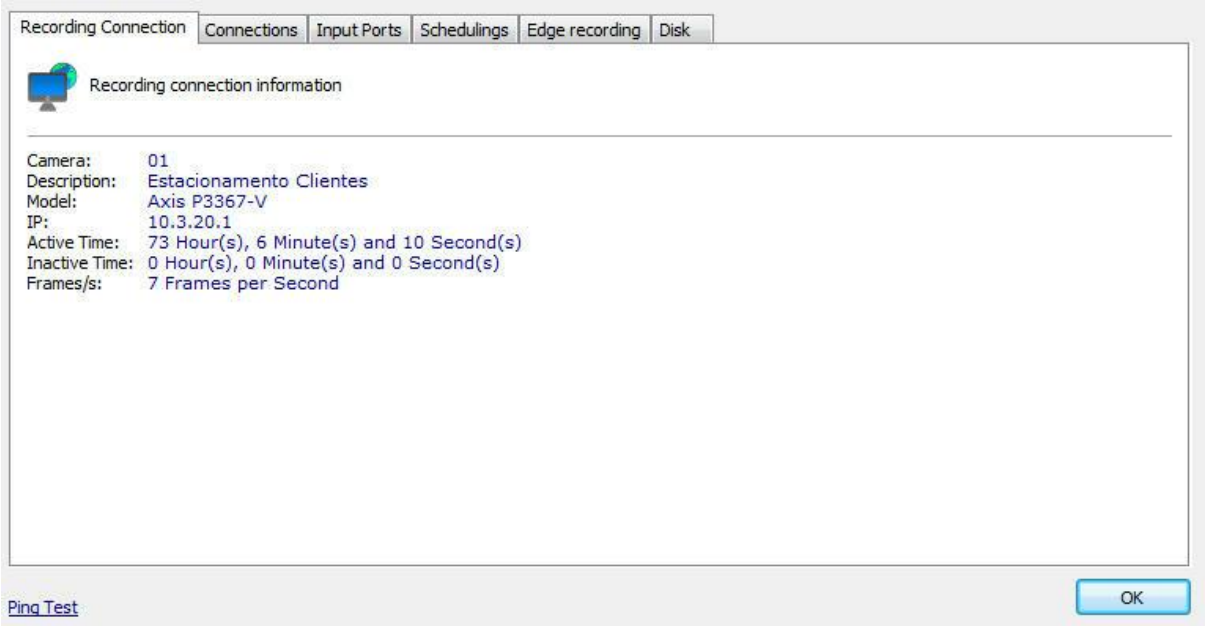
To view the details of the operation of each camera, double-click on the desired camera. Details will be described in the following topics.

- **Shows the deactivated cameras:** Check this option to see the cameras that are deactivated in the camera register;

6.5.1.1 Conexão de Gravação

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

© 2002 - 2020 by Digifort, all rights reserved



- **Camera**: Name of the registered camera.
- **Description**: Description of the registered camera.
- **Model**: Registered camera model.
- **IP**: IP address of the camera.
- **Active time**: Time of activity of the camera since its activation or change of parameters.
- **Idle time**: Camera idle time.
- **Photos received**: Photos received from the camera since its activation or changing parameters.
- **Bytes received**: Number of bytes received from the camera since its activation or changing parameters.
- **Frame / s**: Frames per second being received from the camera.
- **Ping Test**: Opens a window with the ping test for the camera.

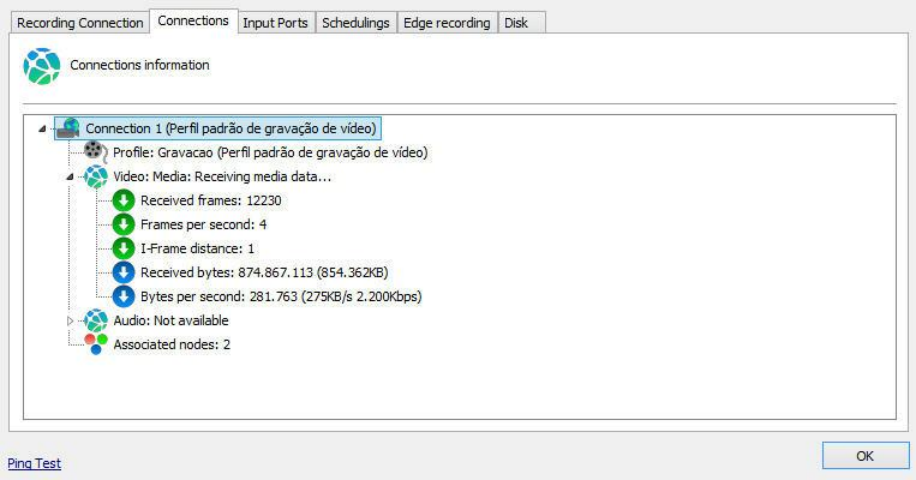
6.5.1.2 Conexões

This screen provides information about all connections made to the camera for recording and viewing video.

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

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

© 2002 - 2020 by Digifort, all rights reserved



- **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 changing parameters.
- **Frames per Second**: Frames per second being received in real time.
- **I-Frame Distance**: Shows the number of frames between the frames I received.
- **Bytes Rec**eived: Bytes received from the camera with this connection since its activation or changing parameters.
- **Bytes per Second**: Bytes per second being received in real time,
- **Associated Nodes:** Number of resources that are using this connection. In this case this connection is being used only for recording the images, showing the value 1. If the camera is also being monitored through the Relay Server through this connection, the value 2 would be shown.

6.5.1.3 Portas de Entrada

This screen shows us the alarm ports (input, output and virtual), the camera and their respective Status

© 2002 - 2020 by Digifort, all rights reserved



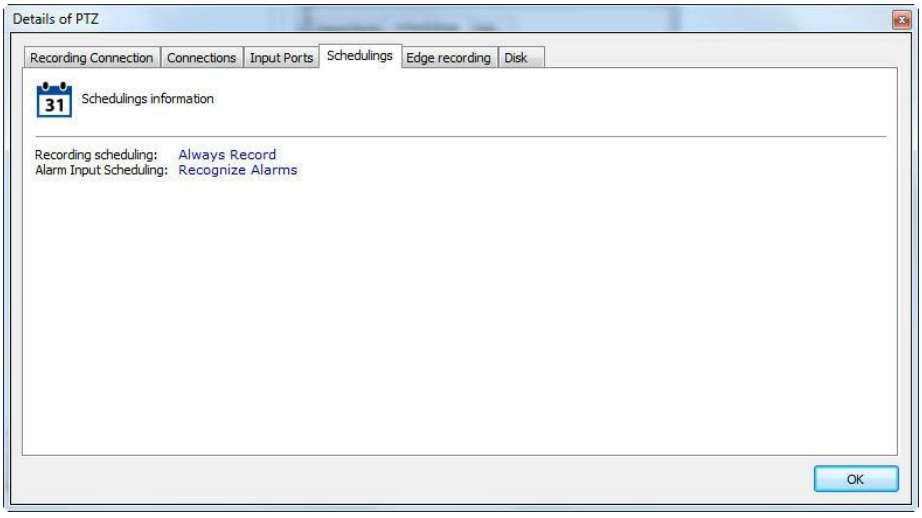
To learn how to configure arming see the chapter How to configure the alarm actions

6.5.1.4 Agendamentos

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

The recording type is defined in the camera register. To learn how to define the type of recording, see Recordings..

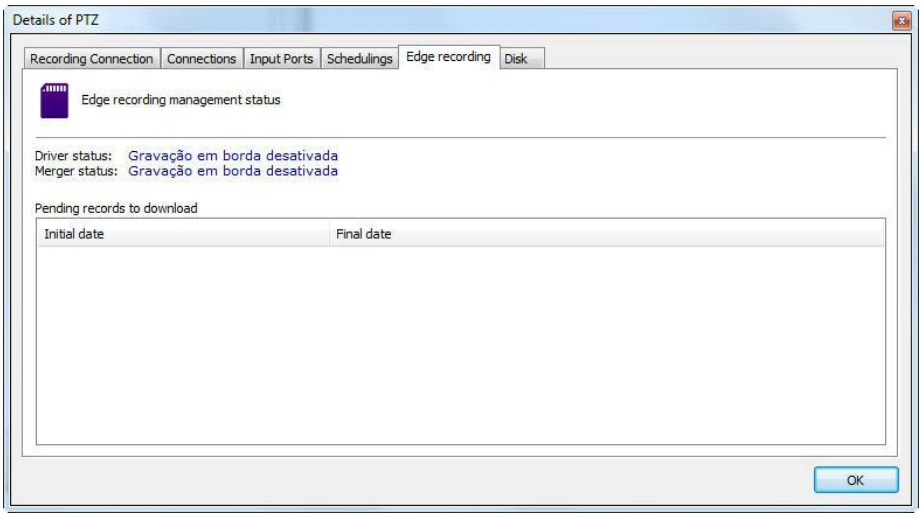
To access this resource, click on the Schedules tab, as shown in the figure below:



© 2002 - 2020 by Digifort, all rights reserved

6.5.1.5 Gravação em Borda

On this screen it is possible to follow the **Status** of the progress of the Edge Recording



During the edge recording process you can see the following status:

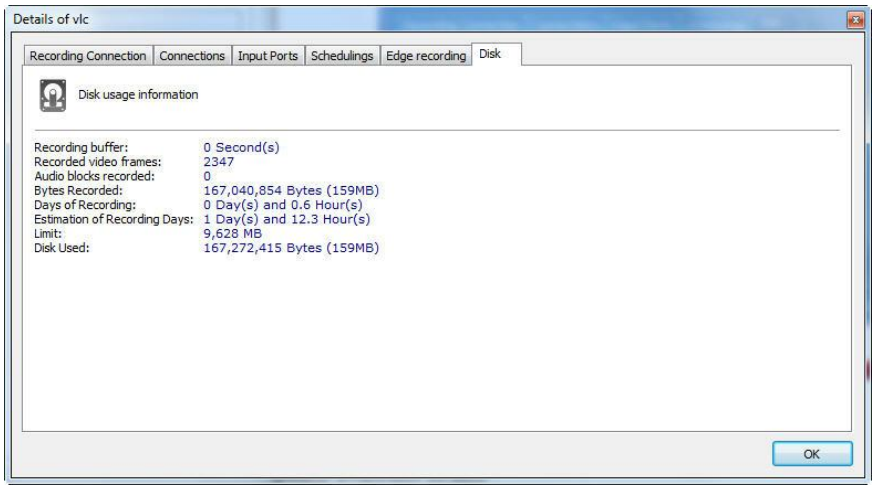
Downloading recordings: Downloading recordings from the desired camera
Recordings download complete: Downloading videos from camera completed
Combining recordings: Combining downloaded recordings with Digifort's main recording
Recordings successfully combined: End of the edge recording process

To learn more about edge recording see the chapter Edge Storage - Edge Recording

6.5.1.6 Disco

This screen provides us with information about disk space usage by the camera.
To access this resource, click on the Disk tab as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



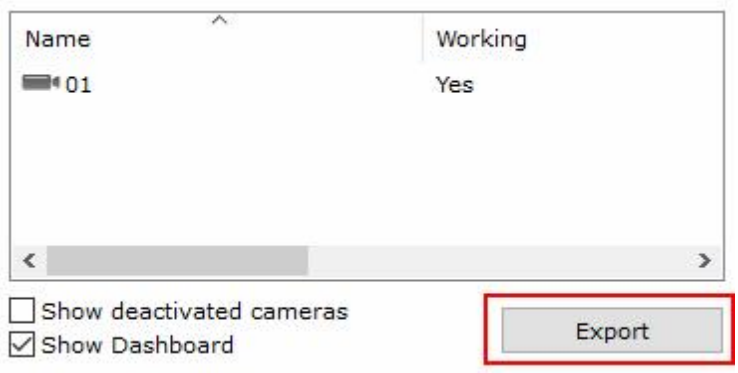
To better understand all of these items read the topic on Disk Management on the Recording Recording Cycle

- **Recorded photos**: Recorded photos from the camera since its activation or changing parameters.
- **Recorded bytes**: Recorded bytes of the camera since its activation or parameter change.
- **Recording hours**: Recording hours stored on disk.
- **Estimated recording hours**: Estimated approximate recording hours.
- **Recording days**: Recording days stored on disk.
- **Estimated recording days**: Approximate estimated recording days.
- **Limit**: Limit allocated for recording images from the camera.
- **Disk used:** Disk space used by camera images.

6.5.1.7 Exportação de dados na tela de Status

The Administration Client object status screens now allow you to export the data to a .CSV file.

All status screens now have a button labeled "Export" and the data will be exported including all selected columns.



Screens with export button support:

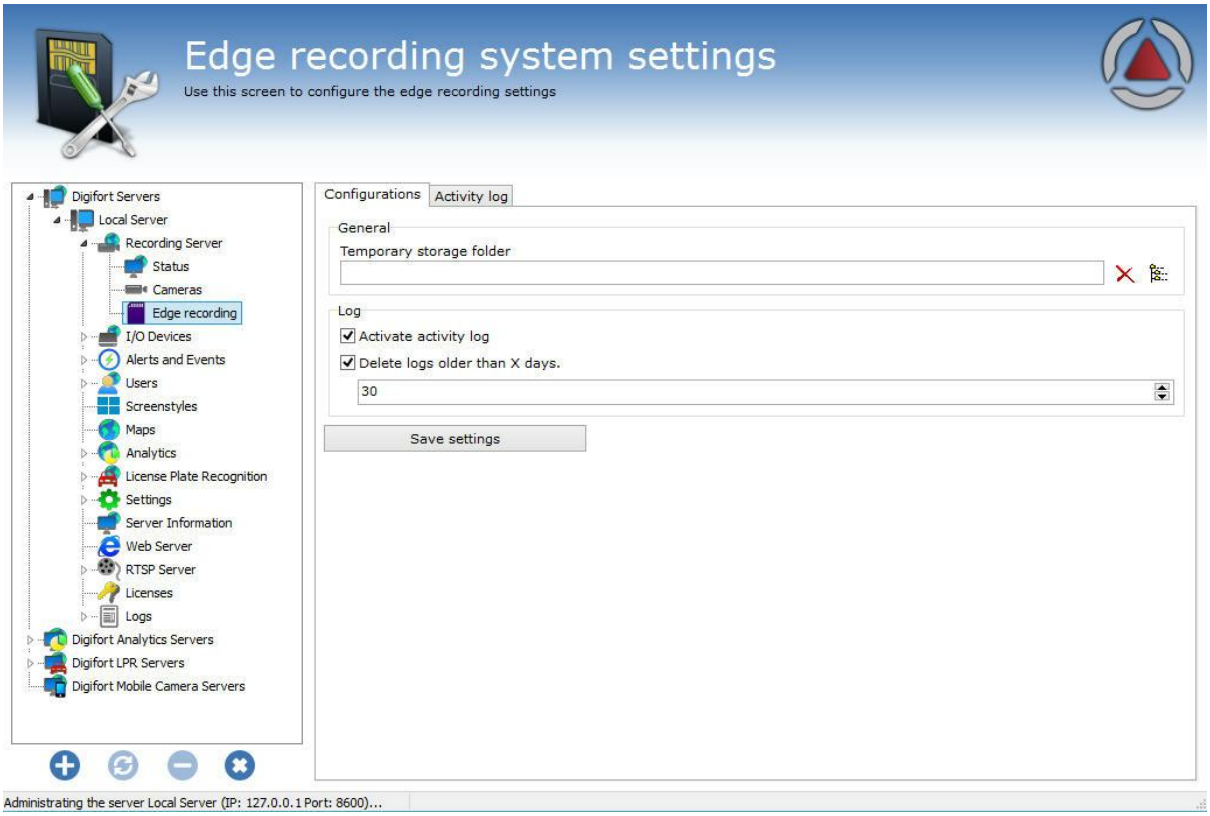
© 2002 - 2020 by Digifort, all rights reserved

- Camera Status
- I / O Device Status
- Analytics Settings Status
- Status of LPR Settings
- Failover status
- Master / Slave connections
- Status of Scheduled Events
- User Connection Status
- Status of RTSP Connections
- Edge Recording Log

6.6 Edge Recording

To access the edge recording general settings, click on **Edge Recording** as shown in the image below:



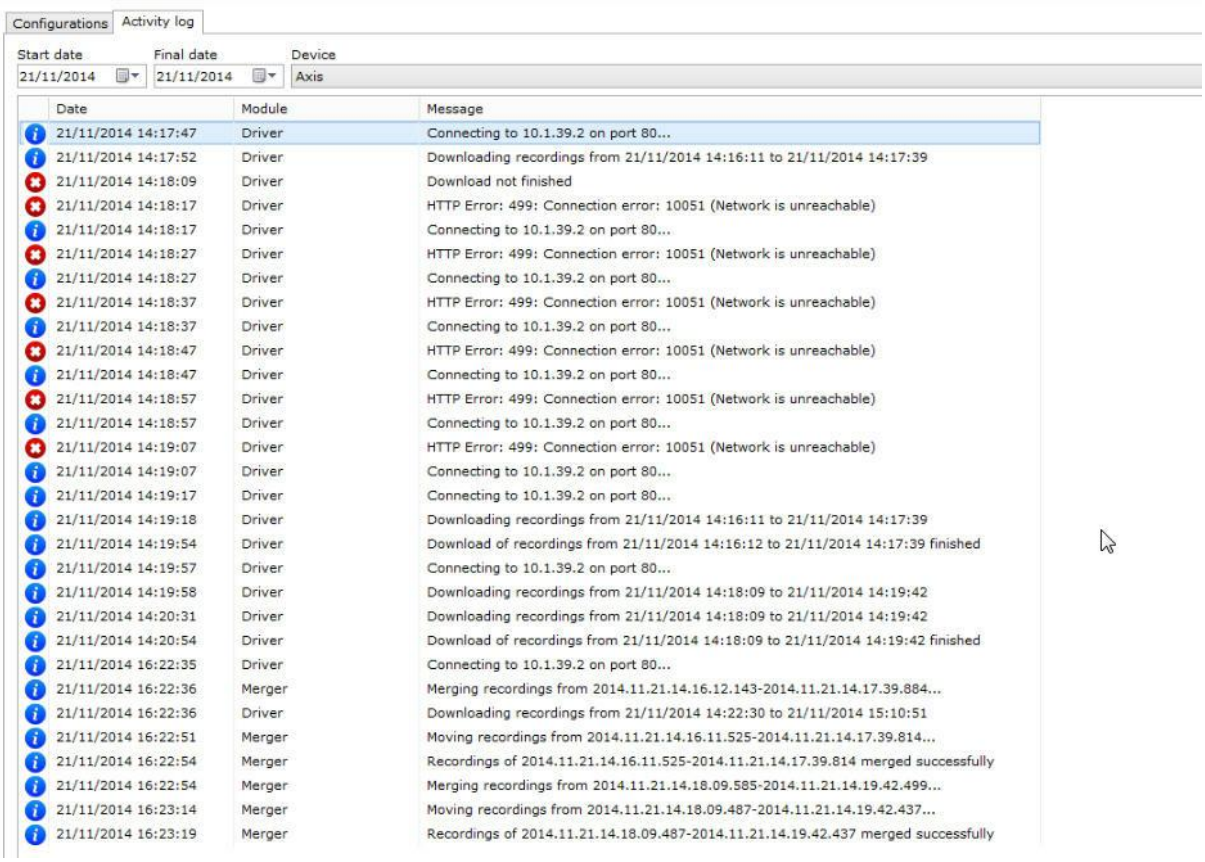


© 2002 - 2020 by Digifort, all rights reserved

On the **Settings** tab there are the following options:

- **Temporary storage directory**: Choose a directory where the recordings downloaded from the cameras stay until combined with the Digifort main recording
- **Enable activity logging**: Activates the log that records the edge recording activities
- **Delete logs older than X days**: Deletes the edge recording logs older than X configurable days.

In the Activity Log, you can search for the records related to the edge recording actions:

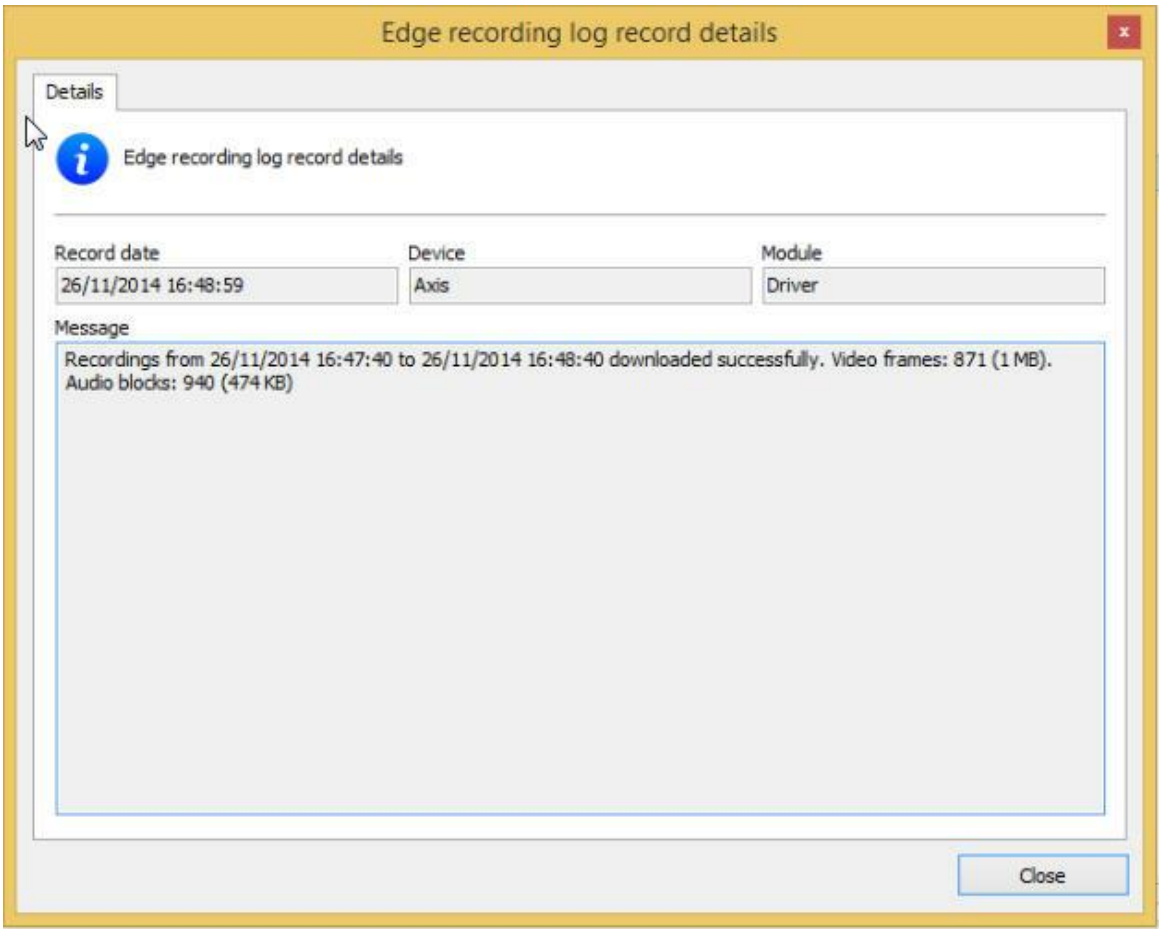


On this screen you can filter logs of:

- **Server connections with the camera.**
- **Connection errors.**
- **Recordings download process.**
- **Recordings download process completed.**
- **Recording combination started.**
- **Combination successfully completed**.

You can see the details of a record by double clicking:

© 2002 - 2020 by Digifort, all rights reserved



To learn more about edge recording check the Edge Recording chapter.

© 2002 - 2020 by Digifort, all rights reserved

Chapter VII

7 Alarm Devices

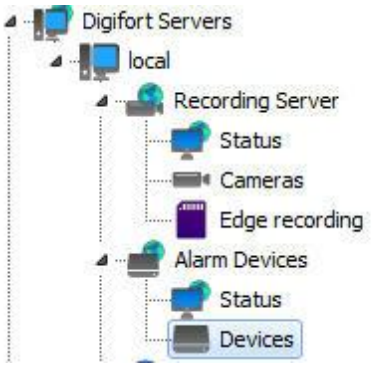
The Digifort System allows the management of external alarm devices. Normally, these devices are alarm boards controlled by the network, as are some cameras, and have alarm inputs and outputs that can be monitored by Digifort.

Normally, the alarm devices are installed in places that don't have alarms or the cameras that are installed don't have ports for alarm input and output.

They can be used in automation of an area. Sensors and panic buttons, among other things, can be attached to their input ports. Sirens, electrical locks and lights, among other things, can be attached to their output ports.

7.1 How to access the alarm devices register

To access the alarm devices register, click on the Devices item in Alarm Devices, as shown in the picture below:



Once this is done, the alarm devices register will be shown on the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



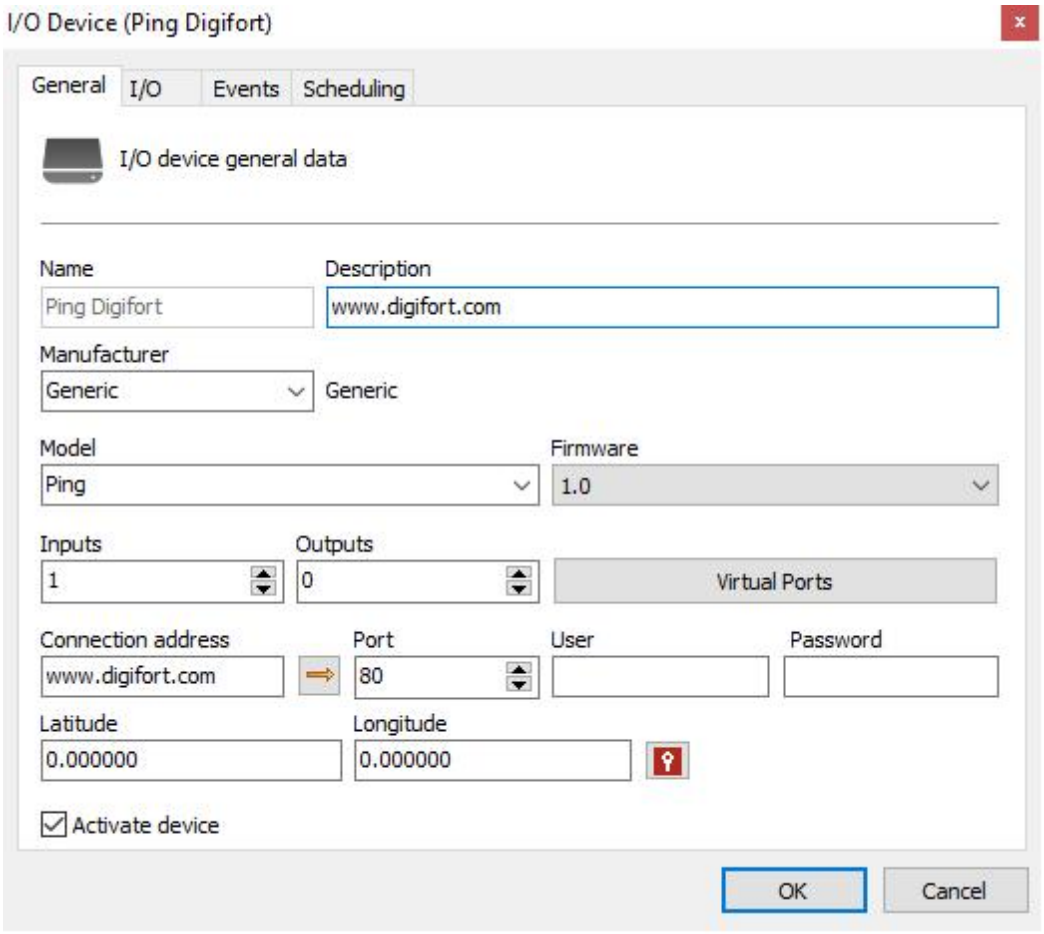
To add an alarm device, click on **Add**. To modify or exclude select the desired alarm device and click on the corresponding button.

7.1.1 How to add an alarm device

After clicking on the **Add** button, as explained in the previous topic, the screen for adding alarm devices will be shown, as shown in the picture below

7.1.1.1 Main data

© 2002 - 2020 by Digifort, all rights reserved



- **Name**: Identification name of the alarm device. After inclusion of the device in the system, the name cannot be modified, as it will be used internally by the system.
- **Description of the device**: Brief description of the alarm device.
- **Manufacturer**: Select the manufacturer of the alarm device.
- **Model of the device**: Select the model of the alarm device.
- **I/O expansion board**: If your device has a port expansion board, select it from this list.
- **Alarm inputs**: Select the number of alarm input ports the device has.
- **Alarm outputs**: Select the number of alarm output ports the device has.
- **Connection IP**: Enter the IP of the connection with the alarm device.
- **Arrow**: Starts the ping command to the device.
- **Connection port**: Enter the port of the connection with the alarm device.
- **User**: Enter the user of the access to the alarm device.
- **Password**: Enter the password of the access to the alarm device.

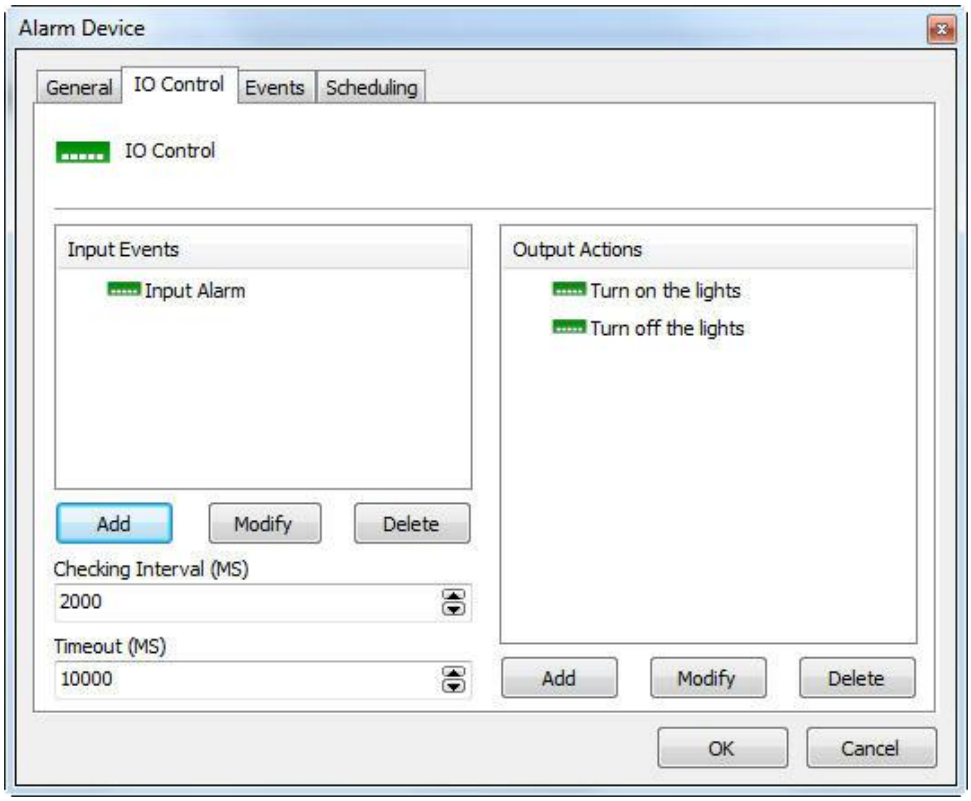
Important

To find out the IP and port of the connection, and the user and password of access, consult the alarm device's instructions manual.

© 2002 - 2020 by Digifort, all rights reserved

7.1.1.2 I/O Control

In this area the alarm device will be configured. To access these configurations, click on the I/O Control tab, as shown in the picture below:



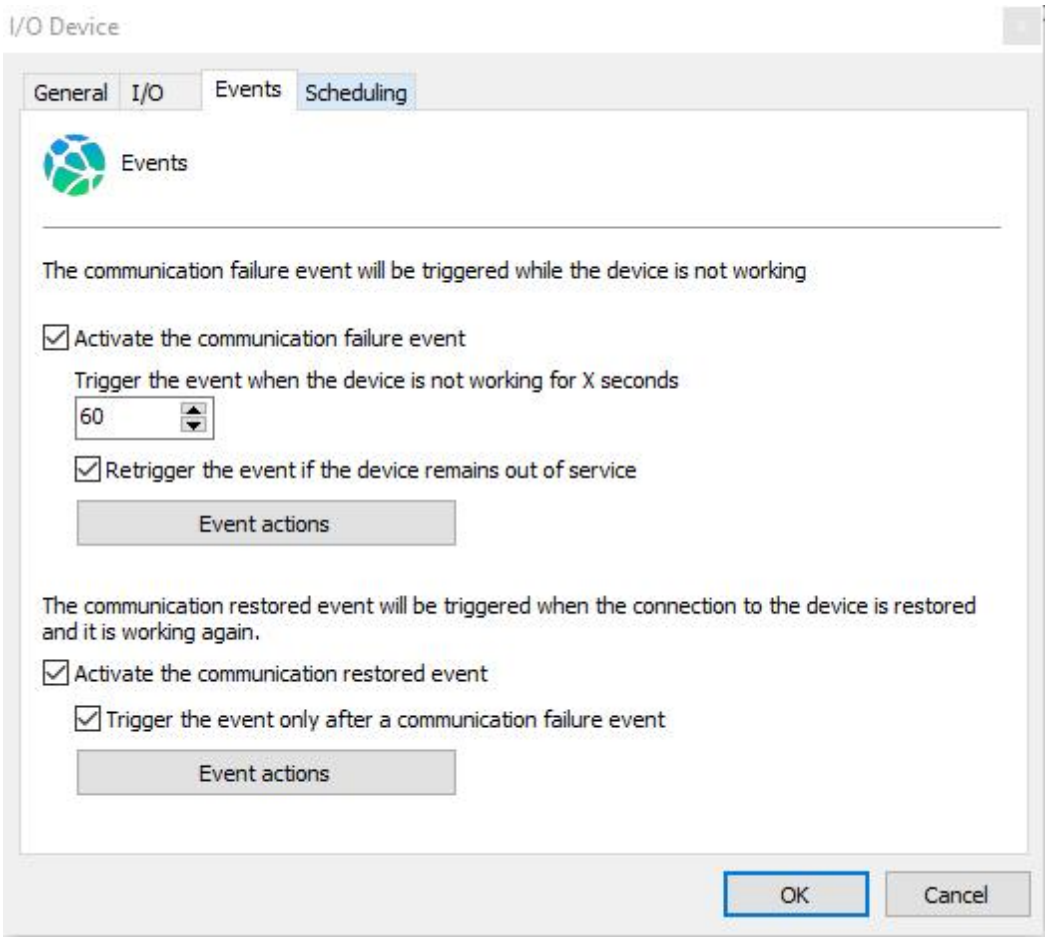
To learn how to use this screen, see **How to configure the I/O**

7.1.1.3 Events

As in the case of cameras, Digifort can also monitor the working state of the alarm devices, offering notification functions, in case the equipment stops functioning for any reason.

Digifort can inform the administrator of failures in communication with the alarm device that can be caused by lack of power at the site, or signs of vandalism, for example. To access this feature, click on the **Events** tab, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



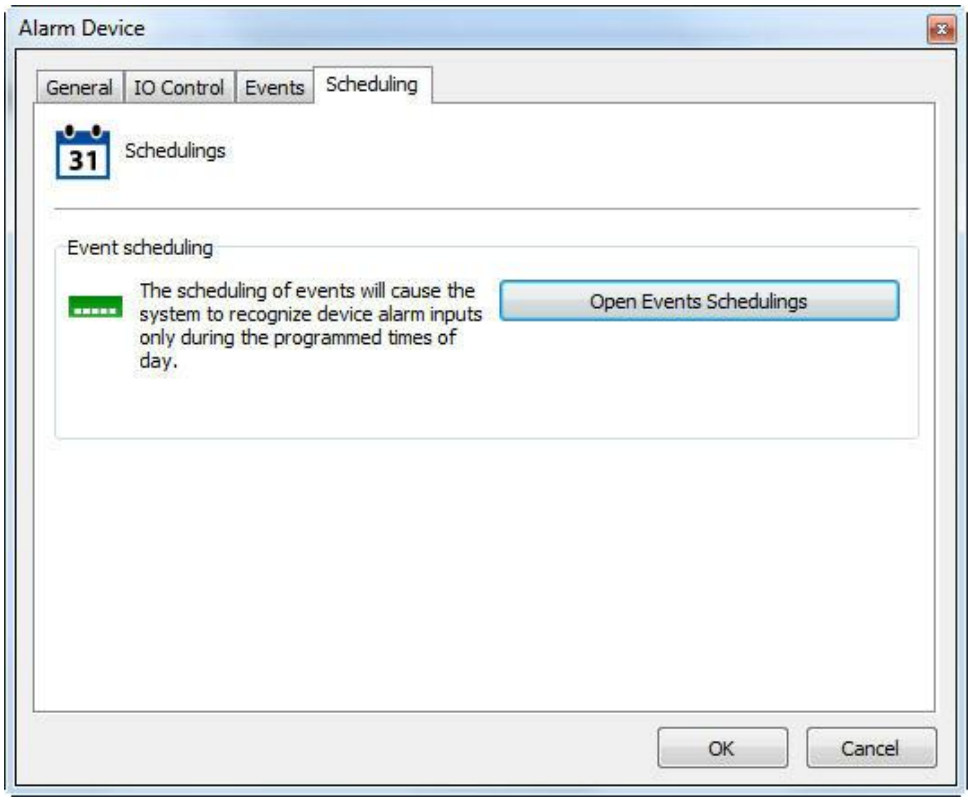
If you wish to activate this notification, mark the option Activate communications failure event and define the time for checking. This time defines the interval after which Digifort verifies if there is connection with the device. For this, click on Alarm Actions to define the set of actions that Digifort will carry out when this event occurs. To learn how to configure the alarm action, see How to configure the alarm actions

7.1.1.4 Scheduling

Scheduling makes it possible for the administrator to configure the times of day and days of the week in which the events received by the alarm devices are to be processed. For example, a rule can be defined that the events will only be processed at night.

To access this feature, click on the Scheduling tab, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

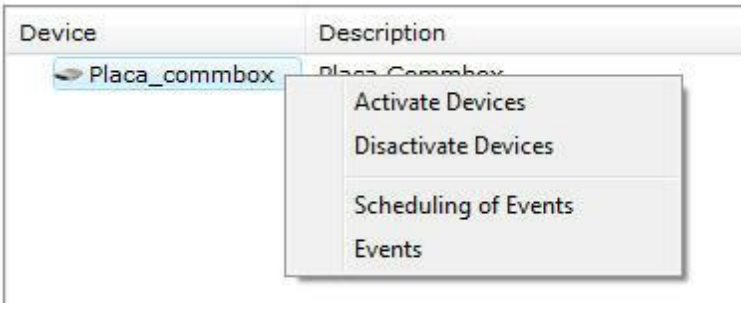


To configure the scheduling, click on Open Scheduling of Events and follow the instruction on page How to configure the scheduling of recording

7.1.2 Management functions of the Alarm Devices

Digifort offers the principal configurations of alarm devices that can be accessed based on its register, thus making it possible to configure several devices simultaneously.

To use this feature, select the desired devices and click on the right button of the mouse, as shown in the picture below:



- **Activate devices**: Activates the selected devices, causing the alarms to be administrated.
- **Disactivate devices**: Disactivates the selected devices.
- **Scheduling of events**: Configures the scheduling of events of the selected device. To learn how to use this feature, see Events.

© 2002 - 2020 by Digifort, all rights reserved

- **Events**: Configures the events of the selected devices. To learn how to use this feature, see I/O Control

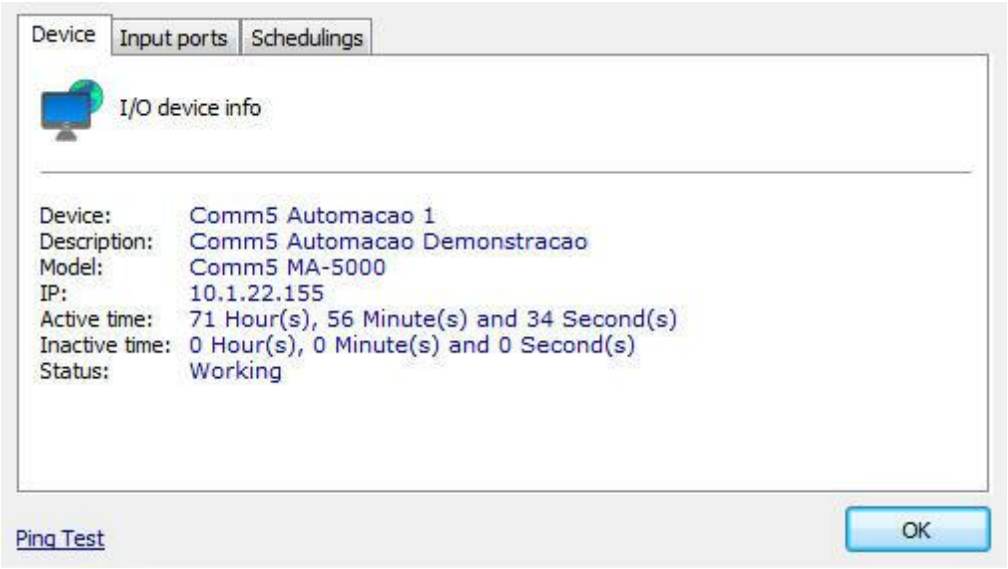
7.2 Status

In the Status option you can check if the alarm devices are in operation, the ports Status and Scheduling.

In the image below it is possible to identify which devices are in operation and out of operation:

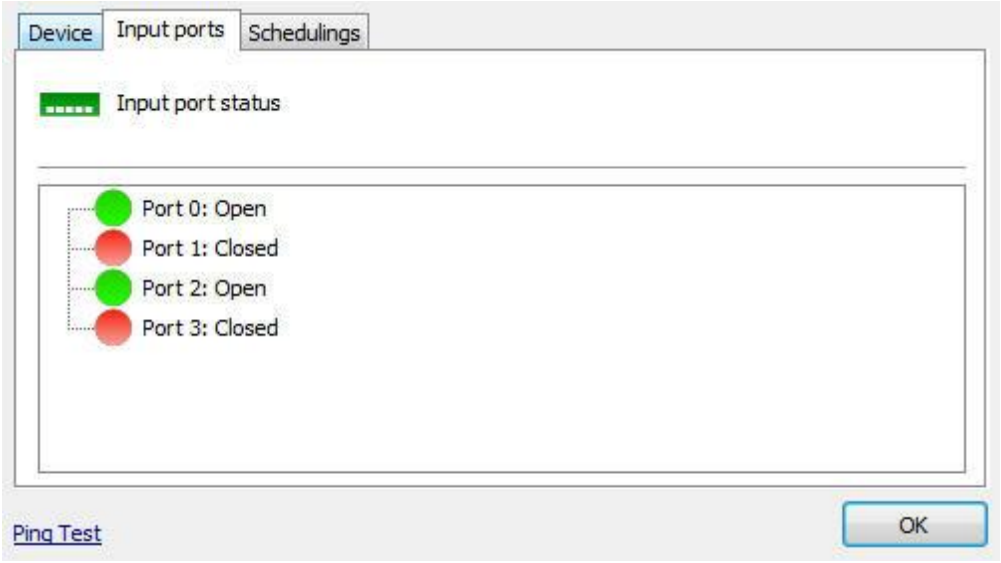


For more details, just double click on the desired device and the following screen will appear:

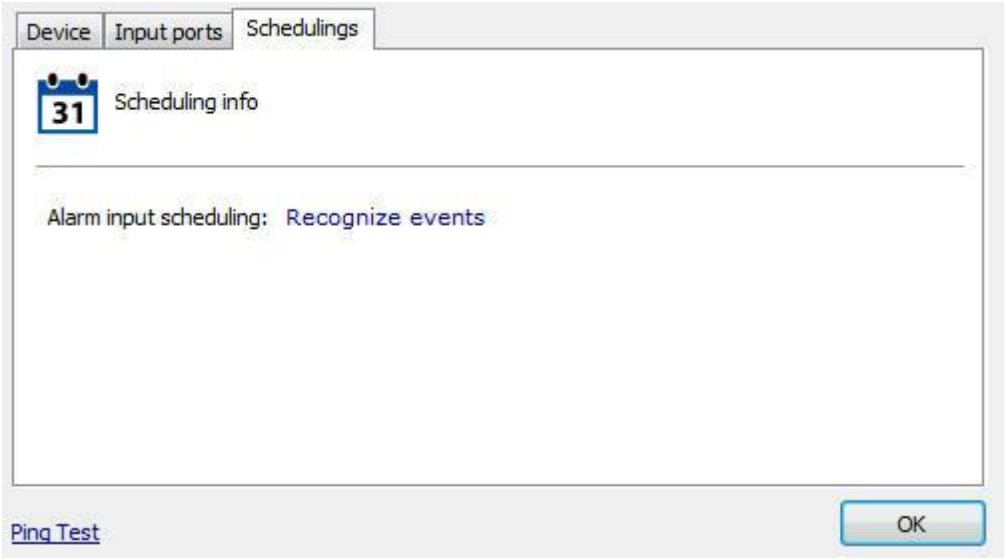


The first Device tab provides us with the following information about the equipment registration, uptime and downtime. The screen also has a ping command to test the equipment connectivity on the network.

© 2002 - 2020 by Digifort, all rights reserved



In the **Input ports** tab it is possible to test in real time the device input port status.



In the **Scheduling tab** there will be information from appointments made to this device;

7.3 I/O Driver for PING

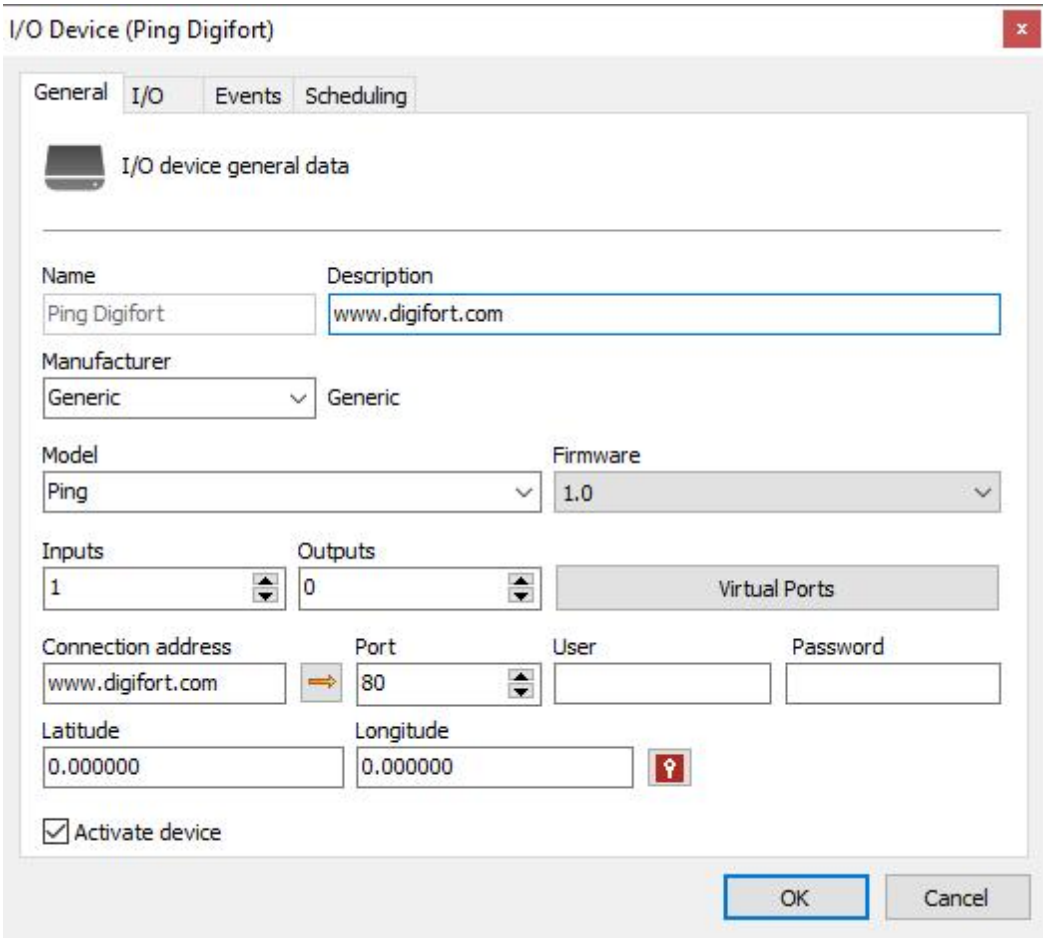
An “I/O Device” driver was created for monitoring hosts through PING.

© 2002 - 2020 by Digifort, all rights reserved

Through the “Generic Ping” model in the registration of I/O Devices, you can monitor any IP or host (for equipment monitoring, for example) and configure alarms and events at the time that the host goes offline. You can also add the status of hosts to a Synoptic Map.

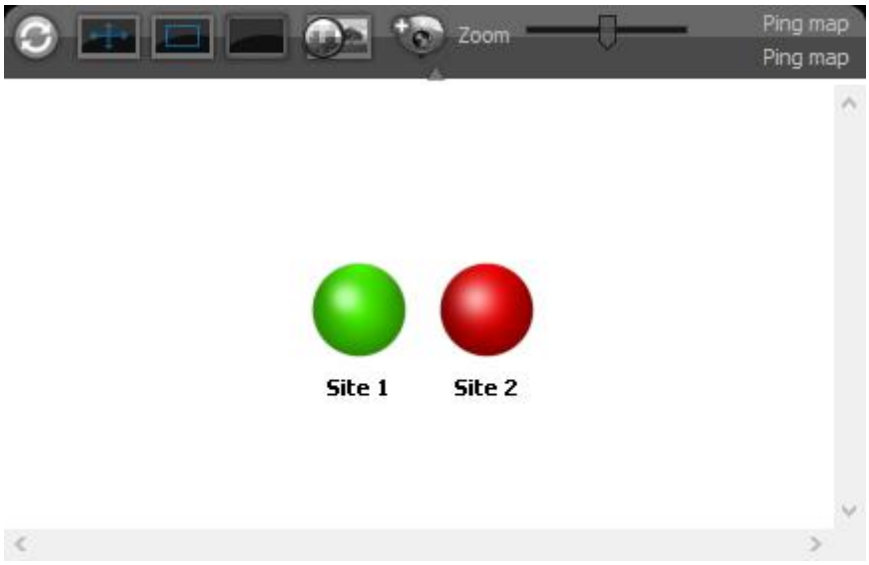
The driver has 1 input port and this port will reflect the status of the ping.
If the port is CLOSED, the host is operating, if the port if OPEN, the host is not accessible.

The non-operational host alarm can be configured through Alarm Input Events (using port 1) or also through Communication Failure and Communication Restoration in the Registration of “I/O Device”.



The image below illustrates a simple use in the Synoptic Map to display the status of multiple hosts, in this case Site 1 is accessible and Site 2 is not accessible.

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter VIII

8 Alerts and Events

The Digifort System offers a series of alerts and alarms that can help to monitor the normal operation of a set of cameras and the server itself. These alerts are configured by the system's administrator, according to the individual needs of each solution, and can be modified at any moment whenever a new need appears.

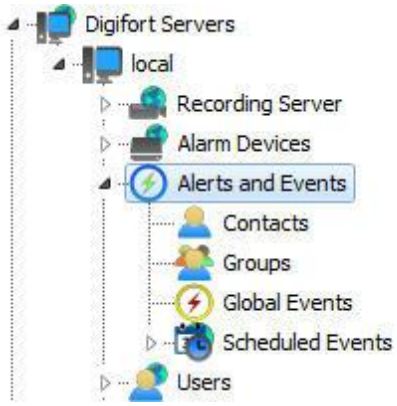
The functions of alerts and events allows Digifort to send e-mail or SMS messages to a list of users that was previously registered in the system each time some event Programmed by the administrator occurs. An event can be, among others, a failure in the communication of the camera with the server, a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

The alerts and alarms are activated immediately following their configuration, making it unnecessary to paralyze the system to accomplish a configuration. An alert can be made for the entire system or for a specific camera.
The monitoring of these alerts is the responsibility of the person to whom the administrator delegated the control.

The lack of interest in checking up on abnormalities detected and informed by the system is considered a serious failure, putting security as a whole at risk.

8.1 How to access the Alerts and Events

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



This area of the system is divided into three parts, the contacts register, the contact groups register and the log configuration.

8.1.1 How to configure the contacts

Contacts are system units that are responsible for alert e-mail messages from the system. In other words, contacts are people who are registered in the system with information such as name, telephone and e-mail address. By way of this information, Digifort is able to

© 2002 - 2020 by Digifort, all rights reserved

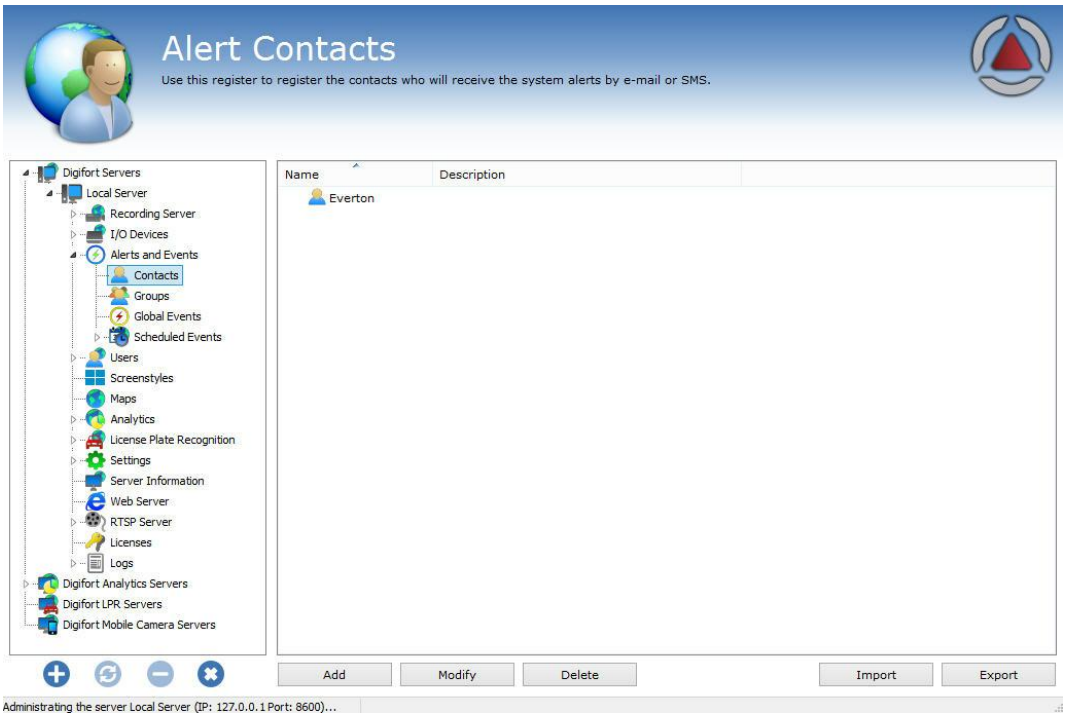
contact them.

Digifort sends e-mail messages not only to a contact, but also to groups of contacts.

To access the contacts register, click on the item Contacts, as shown in the picture below:



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

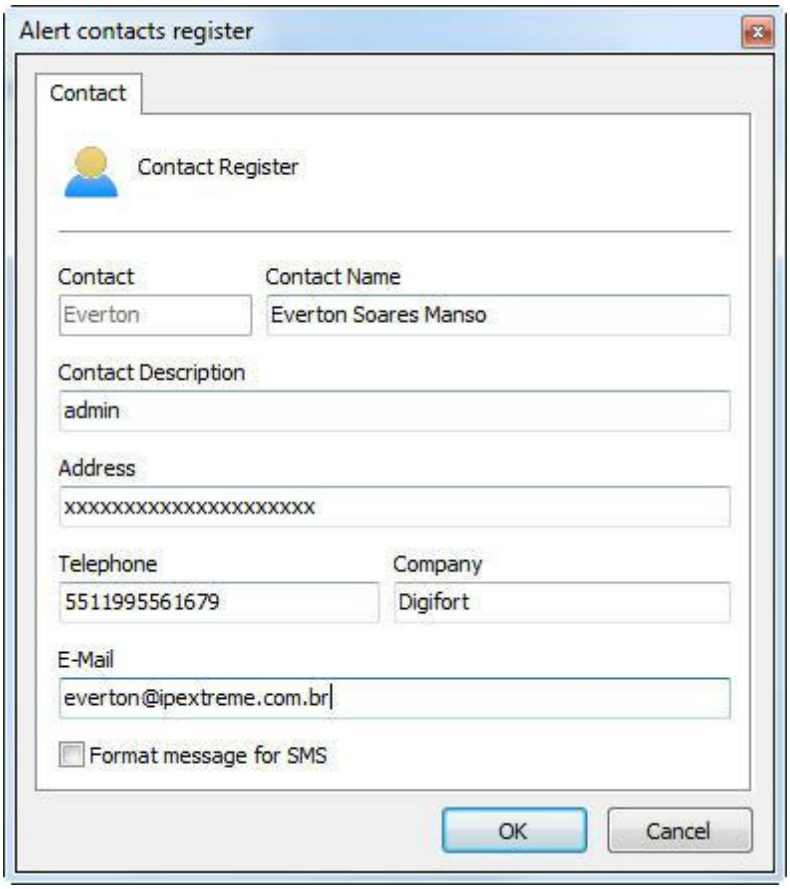


To add a contact, click on the **Add** button. To modify a contact, select it and click on the **Modify** button. To exclude a contact, select it and click on the **Exclude** button.

© 2002 - 2020 by Digifort, all rights reserved

8.1.1.1 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 shown in the picture below:



- **Contact**: Internal name of the contact. This name must be unique and cannot be modified once saved, as this information in used internally by the system.
- **Name of the contact**: Complete name of the contact.
- **Description of the contact**: A brief description of the contact for the purpose of its easy identification. This field may contain, for example, the function of the person in the company.
- **Address**: Address of the contact.
- **Telephone**: Telephone of the contact.
- **Company**: Company of the contact.
- **E-mail**: E-mail address of the contact. It is to this address that Digifort will send the notifications configured by the administrator.
- · **Format message for SMS**: Sends the notification to cell phone in SMS format instead of by e-mail. In this case the e-mail address of the cell phone must be specified in the field “E-mail”.

Important

The sending of SMS messages is a service out of the realm of Digifort and is

© 2002 - 2020 by Digifort, all rights reserved

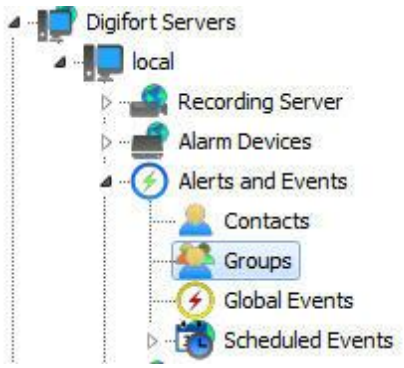
Important

therefore the responsibility of the operator of the cell phone who will receive the message. Verify the availability of this service with your operator.

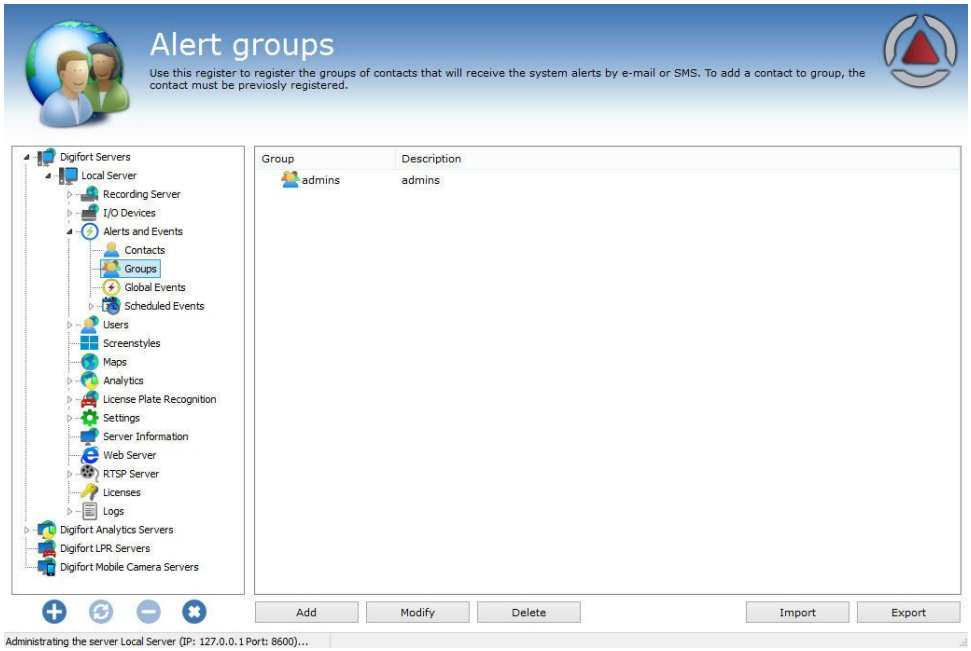
8.1.2 How to configure the contact groups

The creation of contact groups is necessary, since Digifort sends e-mail notifications not only to a contact, but also to a group of contacts.

To access the contact groups register, click on the item Groups, as shown in the picture below:



Once this is done, the group register will be displayed at the right, as shown in the picture below:



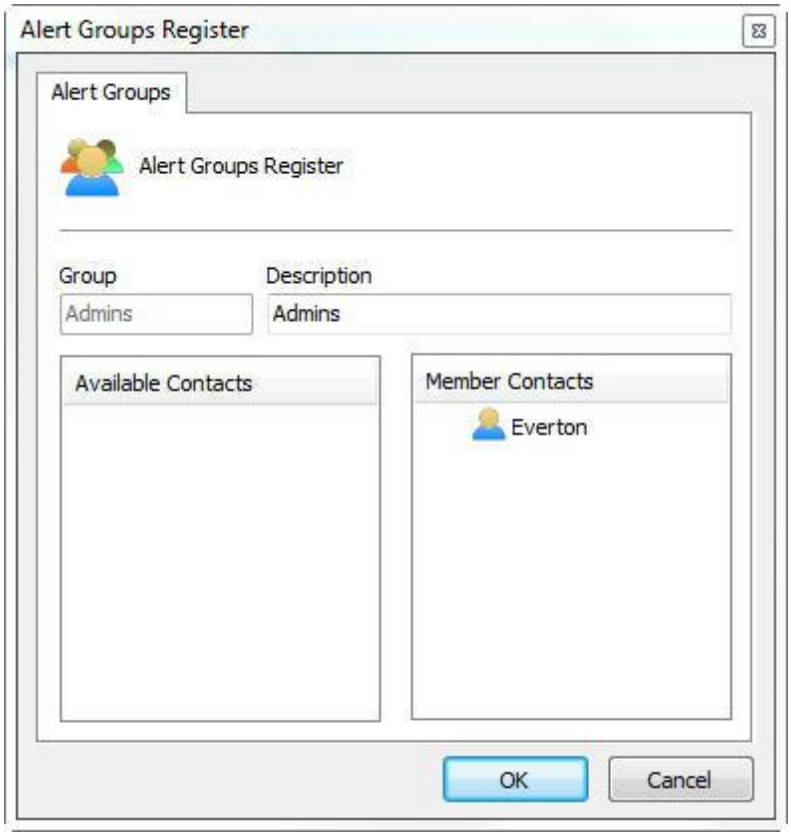
To add a contact group, click on the **Add** button. To modify a contact group, select

© 2002 - 2020 by Digifort, all rights reserved

it and click on the **Modify** button. To exclude a contact group, select it and click on **Exclude**.

8.1.2.1 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 shown in the picture below:



- **Group**: Name of the contact group. Once saved, this name cannot be modified, 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 all contacts who are members of the group.

To add contacts to the group, select the desired contact in the list of available contacts and drag it to the list of member contacts.

To remove a contact from the group, select the desired contact in the list of member contacts and drag it to the list of available contacts.

8.1.3 Global Events

Global events are powerful alarm and system integration tools. Like any other event, global events can be used to set off preprogrammed system actions, as well as activate and deactivate the

© 2002 - 2020 by Digifort, all rights reserved

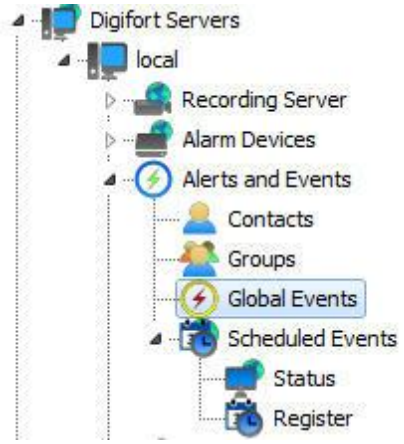
recording of cameras.

Global events can be activated by users by way of the Surveillance Client or by external system, thus allowing any other application to activate an event in Digifort.

This chapter will cover only the configuration of global events. For information on how to activate a global event by way of an external applicatio, consult the API of global events.

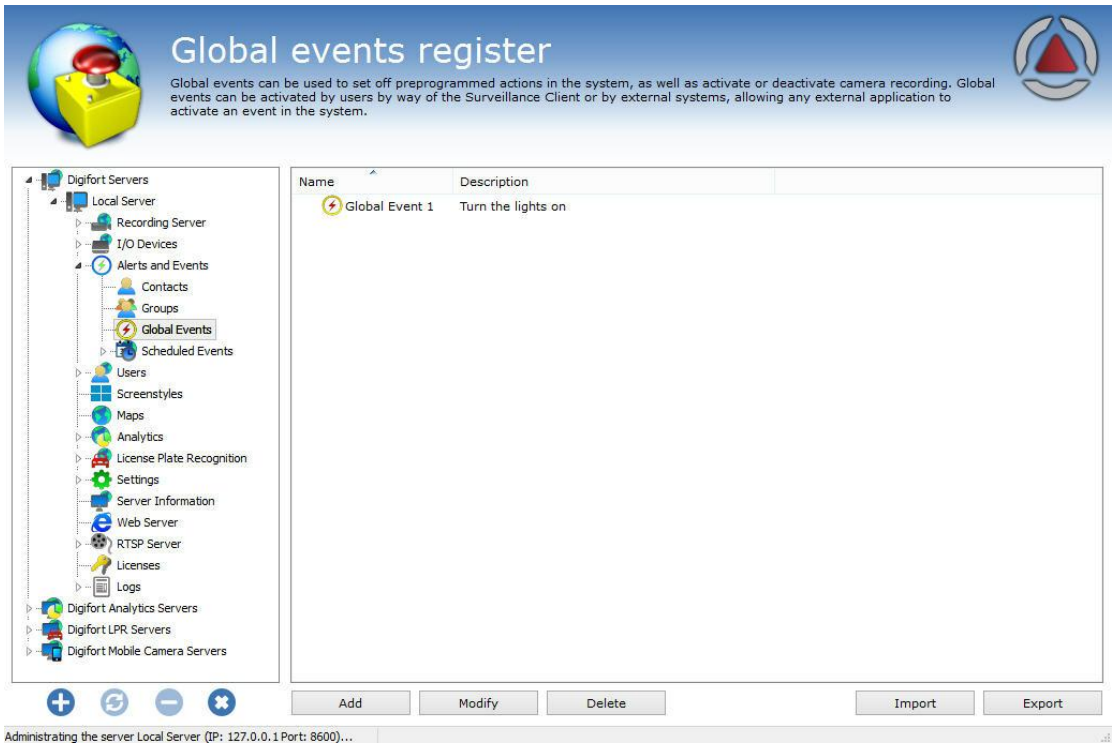
8.1.3.1 How to access the Global Events Register

To access the Global Events Register, click on the item Global Events, as shown in the figure bellow.



Once this is done, the alarm devices register will be displayed at the right, as shown in the figure below.

© 2002 - 2020 by Digifort, all rights reserved

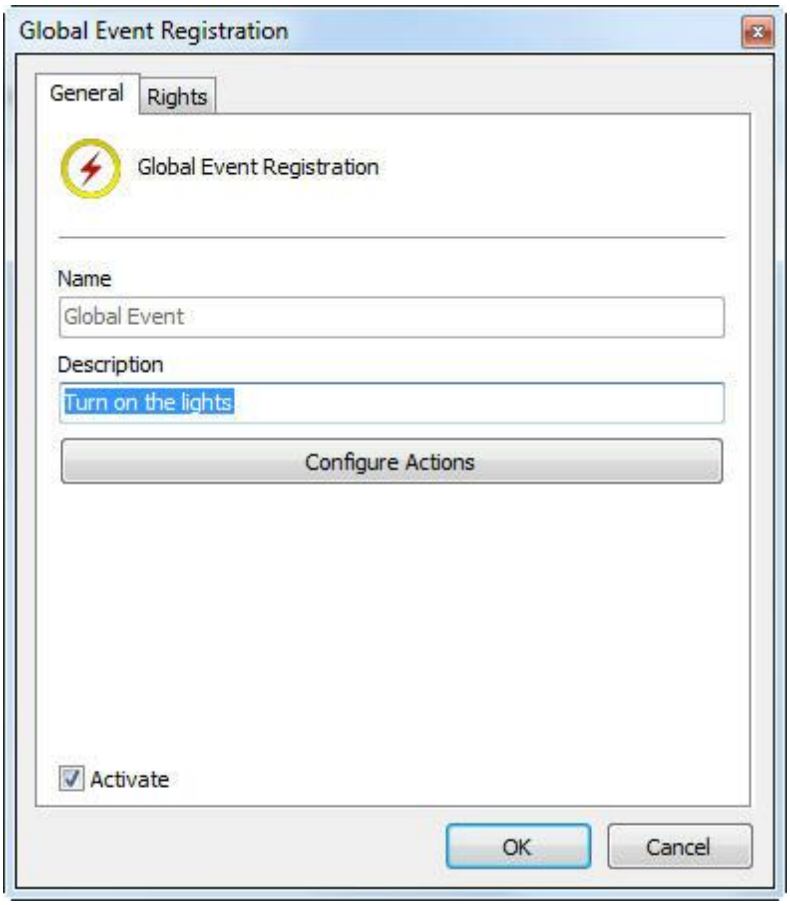


To add a global event, click on **Add**. To modify or exclude, select the desired global event and click on the correspondig button.

8.1.3.2 How to add a global event

Once the Add button is clicked, as explained in the topic above, the screen for adding global events will be displayed, as shown in the figure below.

© 2002 - 2020 by Digifort, all rights reserved



8.1.3.2.1 Main data

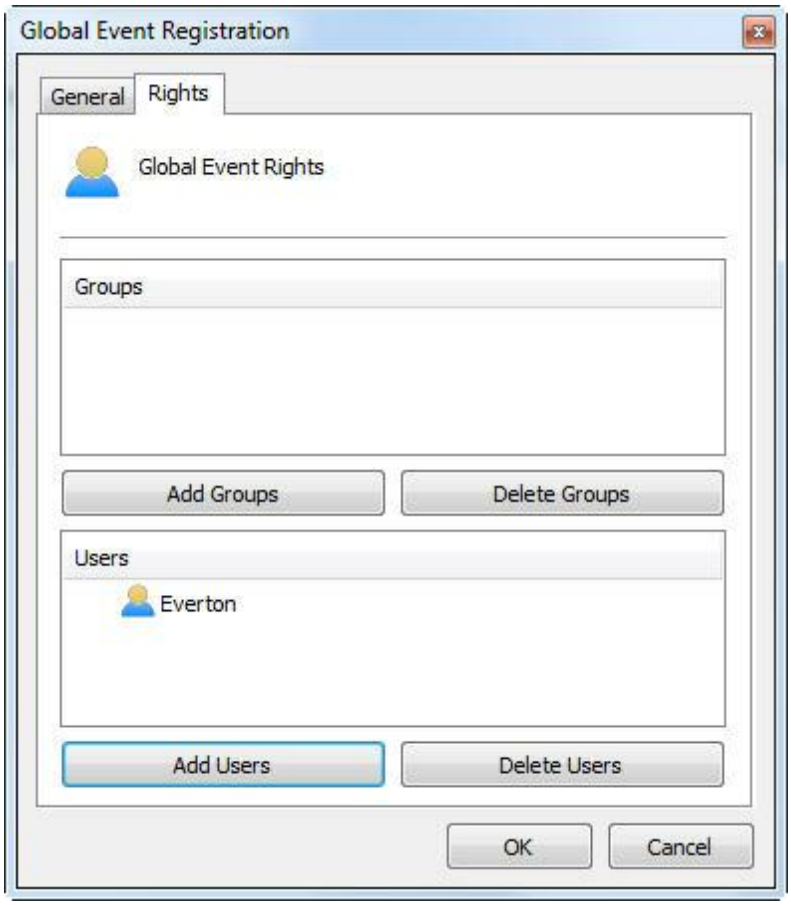
- **Name**: Identification name of the global event. The name of the global event will be used to set off the event in Digifort. After inclusion of the event in the system, the name cannot be modified, as it will be for internal use of the system.
- **Description**: Short description of the global event.
- **Activate**: Enables or disables the global event for use.

To configure the actions of the global event, click on the Configure Actions button. The operational mode of the configuration of the actions is described in Chapter How to configure the alarm actions

8.1.3.2.2 Rights

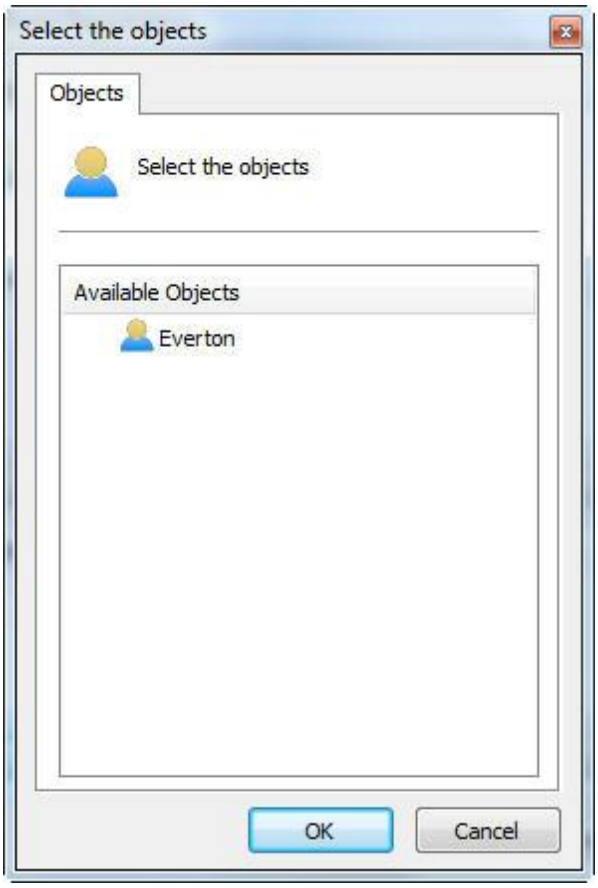
Global events can have access restricted to some users of the system. To attribute user rights, click on the **Rights** tab, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



To conceed the right of access to the desired users/groups, simply click on the **Add Grupos/Users** button and select them in the list of **Groups/Users** which will appear as the figure shows.

© 2002 - 2020 by Digifort, all rights reserved



Select the available User and click on **OK**. The same rule applies to the list of groups.

8.1.4 Sheduled Events

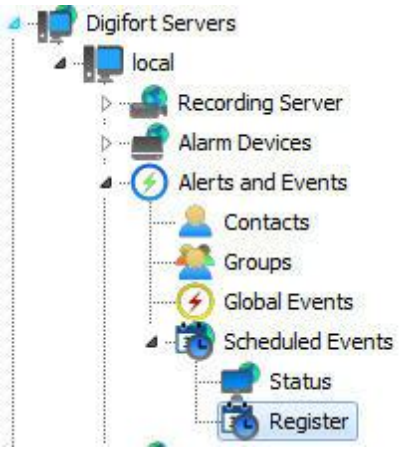
Sheduled events allow the user to create scheduled actions for executing some system function at specified dates and times.

This feature is very useful for automating and easing routine tasks such as turning on lights, opening doors and controlling the activation of any kind of equipment at the Sheduled time.

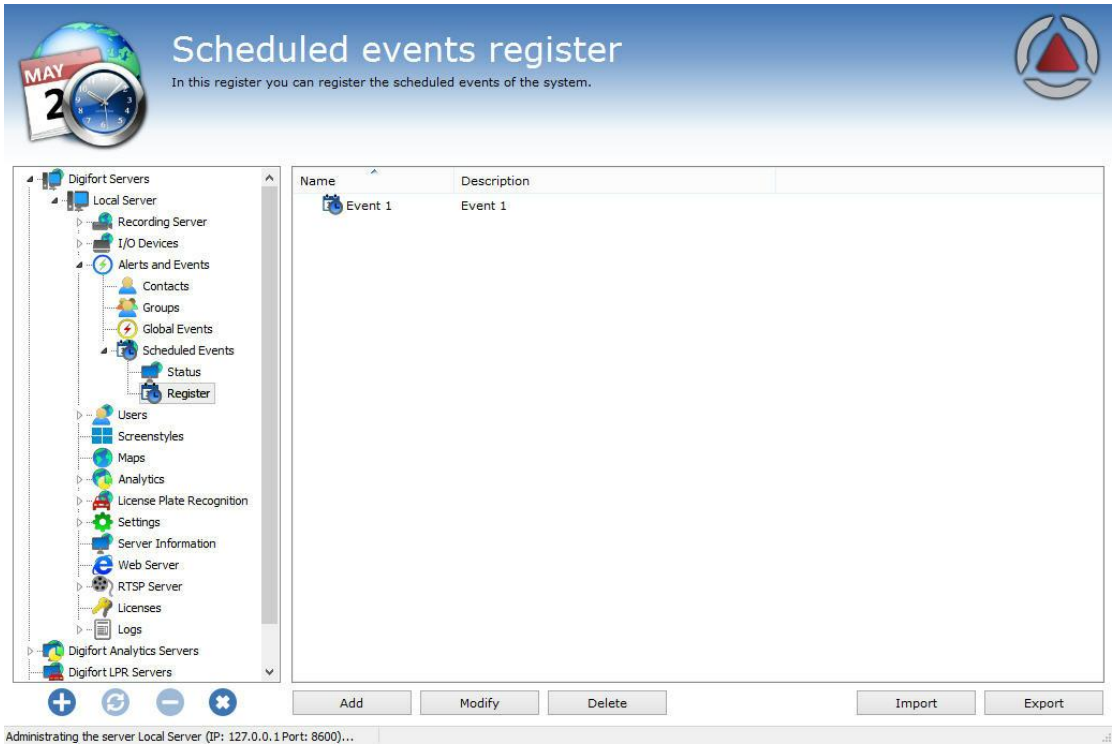
8.1.4.1 Registering Sheduled Event

To access this area, click on the Register tab in the Menu of Sheduled Events, as shown in Figure bellow:

© 2002 - 2020 by Digifort, all rights reserved



Once this is done, the general system configuration screen will open up at the right, as shown in Figure bellow:



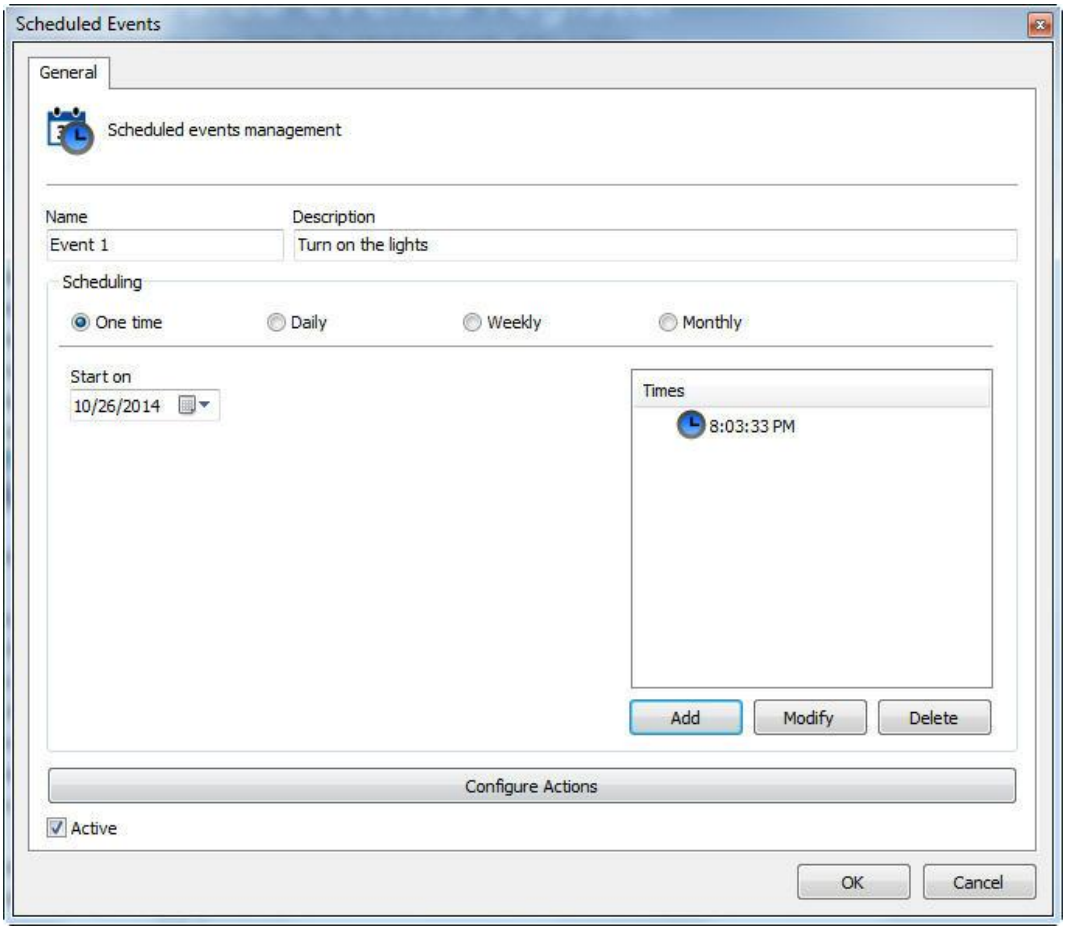
To add a Sheduled Event, click on **Add**. To modify or delete a Sheduled Event, select the desired camera and click on the corresponding button.

8.1.4.1.1 Adding Sheduled Event

Após clicar em **Adicionar** a tela de cadastro de eventos será aberta como demonstra a figura abaixo:

© 2002 - 2020 by Digifort, all rights reserved

After clicking on **Add**, the event registration screen will open up as shown in the figure below:



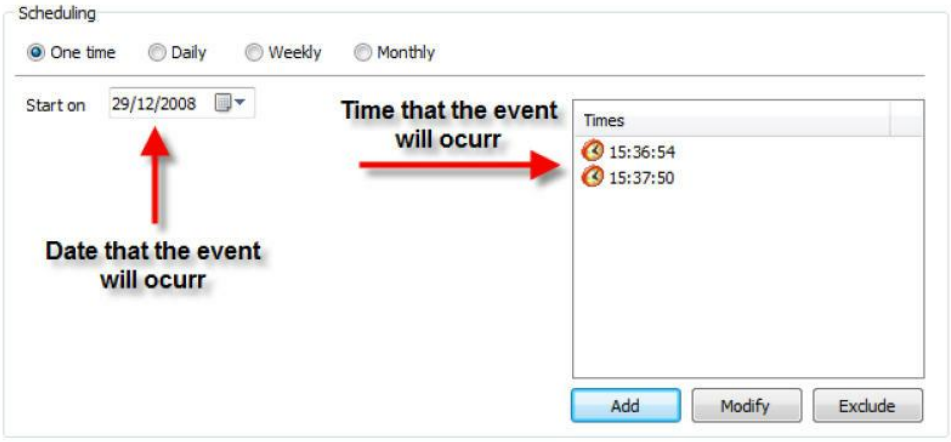
This screen offers the following function:

- **Name**: Enter the desired name for the event. This name will be the key for recognition in the system.
- **Description**: The desired description for the event to be registered.
- **Scheduling**: The type of scheduling to be made. The event can be activated only once, daily, weekly or monthly. The types of scheduling will be explained further on.
- **Times**: Screen in which one or more times of day can be added for the event to be activated.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions
- **Active**: Active or de-Active the event.

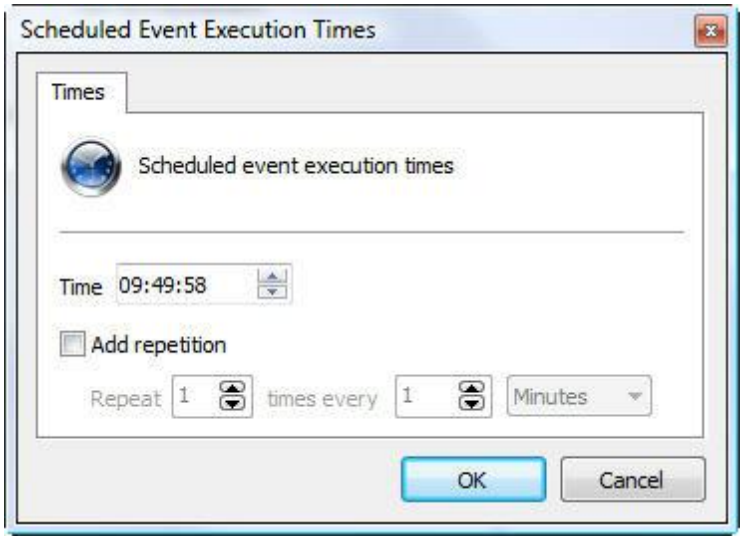
8.1.4.1.1.1 Types of Scheduling

© 2002 - 2020 by Digifort, all rights reserved

In this option, only the options for the date and time of the execution of the event will be configured as shown by the figure below:



First, select the date on which the event shall occur, followed by clicking on Add in the times window and the following screen will be displayed:



In this window, select the desired time of day for execution of the event. If necessary, the repetition of the event every X minutes can be added.

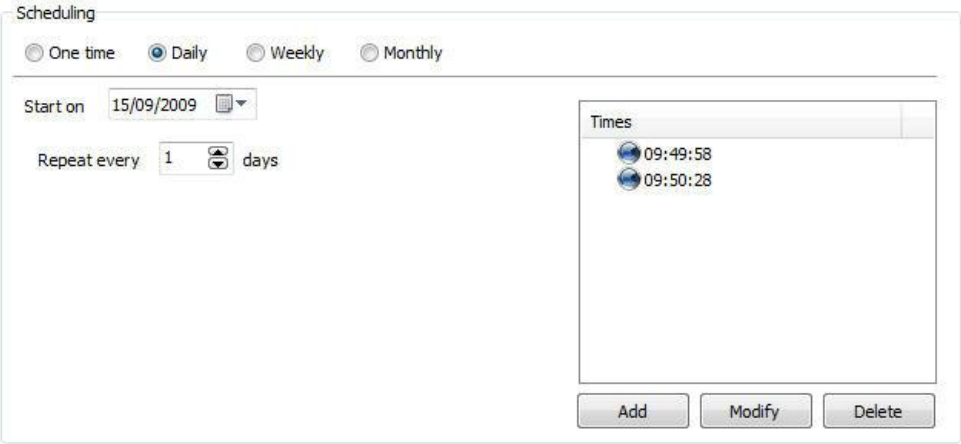
The time of day will remain in the screen as shown by the Figure below:

© 2002 - 2020 by Digifort, all rights reserved



NOTE: As many times of day can be added as necessary by simply repeating the process.

In this option, the same setting as before are presented with exection of the field shown in the figure below:

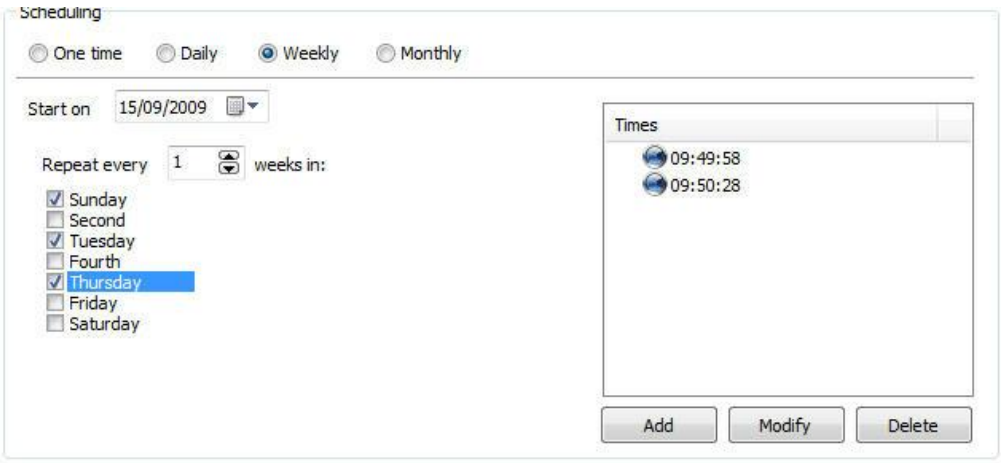


This field allow the event to occur every day (as the figure shows) or every other day, every third day, and so on, depending on the number configured.

The Weekly scheduling allow the event to be repeated every X weeks, at the defined times and on the desired days of the week.

The options of weekly sceduling are shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



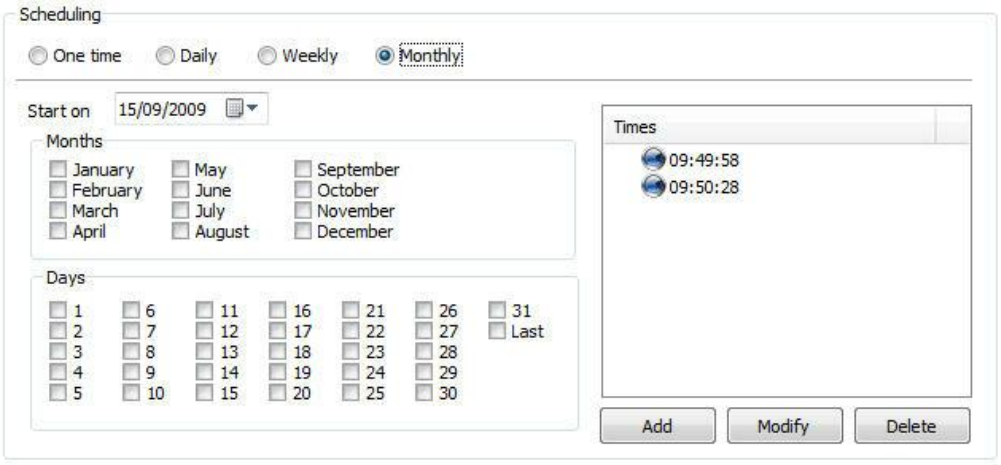
This screen offers the following functions:

- **Start on**: Starting date of the event. In the case of weekly scheduling, the software will assume the current week as the beginning, that is, the following week will start on the next Sunday.
- **Repeat every X weeks on**: Repeat the event every X weeks (every other week, every three weeks, etc.) on the desired days. Just click on the days on which the event shall occur.
- **Times**: Add the times of day on which the event shall occur.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions

In the monthly configuration it's possible to choose the desired months and days for the determined event to occur.

The months registration screen is shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



This screen offers the following functions:

- **Start on**: Starting date of the event. Select the desired date for beginning of the events.
- **Months**: Select the desired months during which the events shall occur.
- **Days**: Select the desired days on which the events shall occur.
- **Times**: Add the times of day at which the events shall occur.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions

© 2002 - 2020 by Digifort, all rights reserved

Chapter IX

9 User administration

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

The creation of users is very important for the good organization and security of the Digifort Server.

The system's administrator must define a set of users who are responsible for the monitoring and correction of events related to the operation of the Digifort System. With time, these users are automatically notified by the system regarding the conditions and abnormalities that occur and that were defined by the organization as worthy of checking out. An abnormal situation would be a camera that stopped working, or a vault that alerted about someone's undue entry, for example.

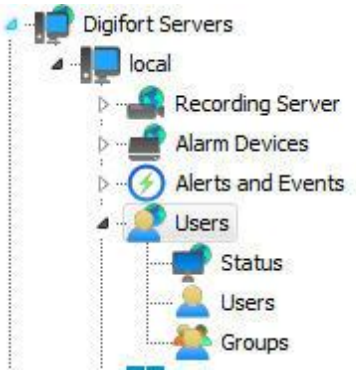
These users must be of the utmost trust to the company, as a security solution only works with trustworthy equipment and personnel.

The Digifort user manager is divided into two parts, Status, where the activity of users on the server and Users can be monitored, where users can be added, changed and deleted from the system. In this way, the user will be able to access his profile in any monitoring environment.

NOTE: To facilitate the management of multiple servers, the Administration Client will now reuse login credentials for all servers. If the login is successful on 1 server, when connecting to another server, these same credentials will be used automatically, facilitating the administration process since it will not be necessary to enter the 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.

9.1 Administrating users

To access the area of user administration, locate the **Users** item in the Configuration Menu of the server to be administrated and give a double-click. The item will be expanded, showing the Status and Users options, as shown in the picture below:

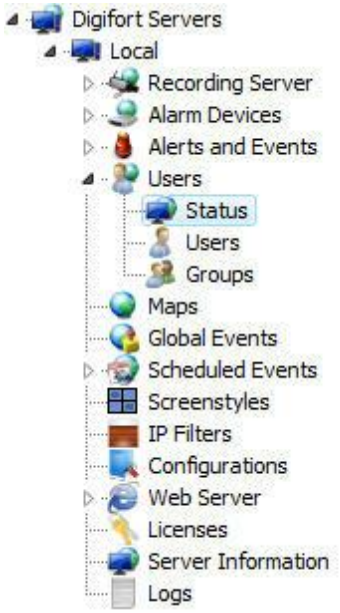


© 2002 - 2020 by Digifort, all rights reserved

9.1.1 Monitoring user activity

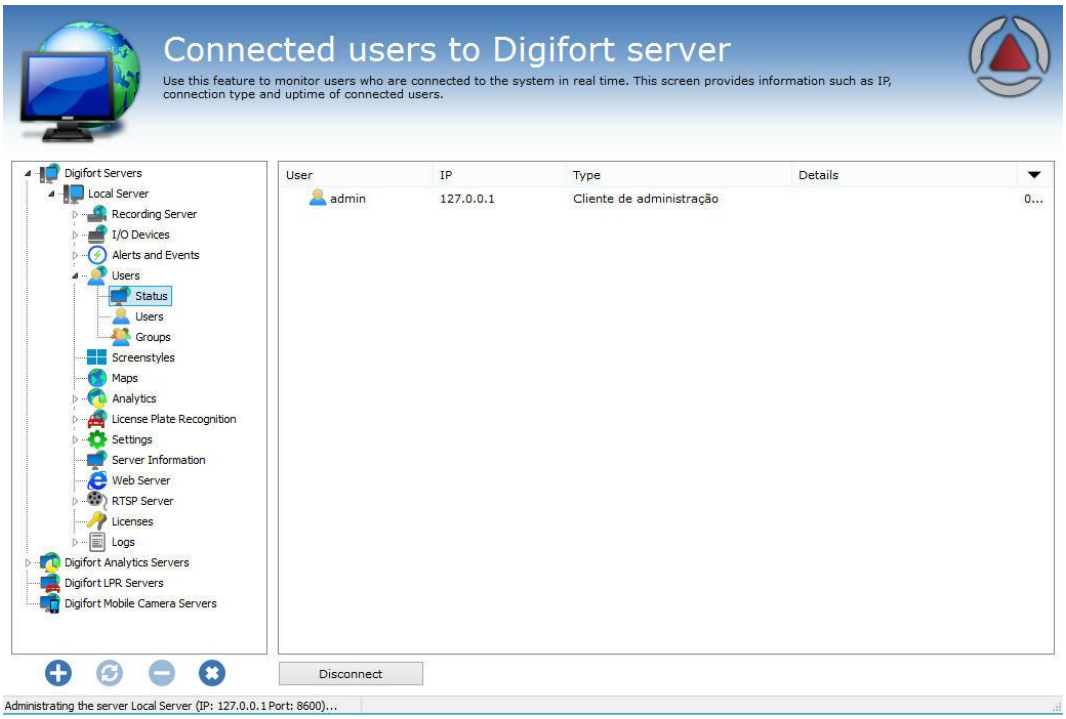
This feature is very important for the security of the server, since logged-in users' activity is monitored here. If the user is taking an undue action, he can be disconnected or blocked.

To access this feature, locate the Status item in the Users item in the Configurations Menu of the server, as shown in the picture below:



Once this is done, the system user activity screen will be opened on the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

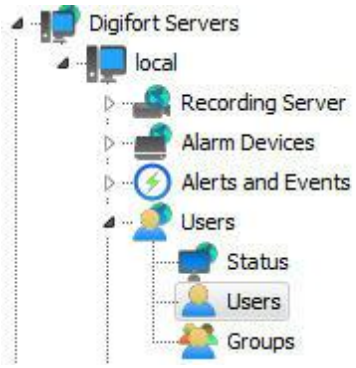


All presently logged-in users of the system are displayed, showing information such as user name, IP address, server access type, and connection time.

To disconnect a user, select the user and click on the **Disconnect** button.

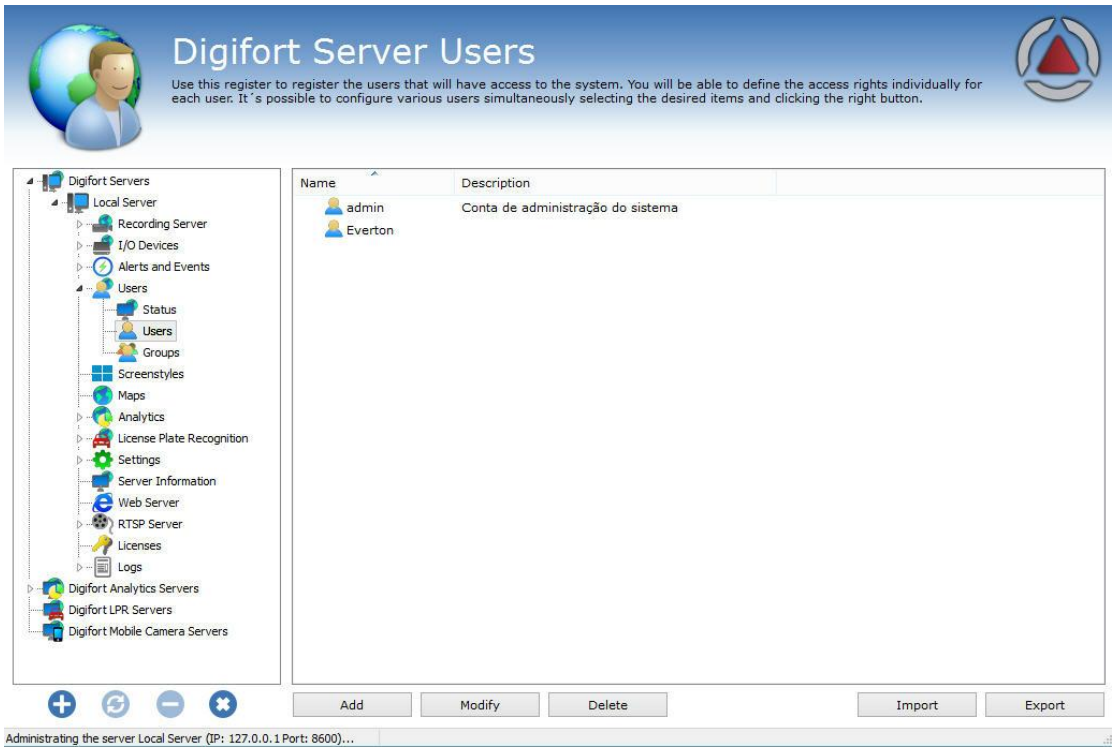
9.2 Adding, modifying and excluding users

To access the user administration, locate the Users item in the Configurations Menu of the server, as shown in the picture below:



Once this is done, the user administration screen will be opened on the right side, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



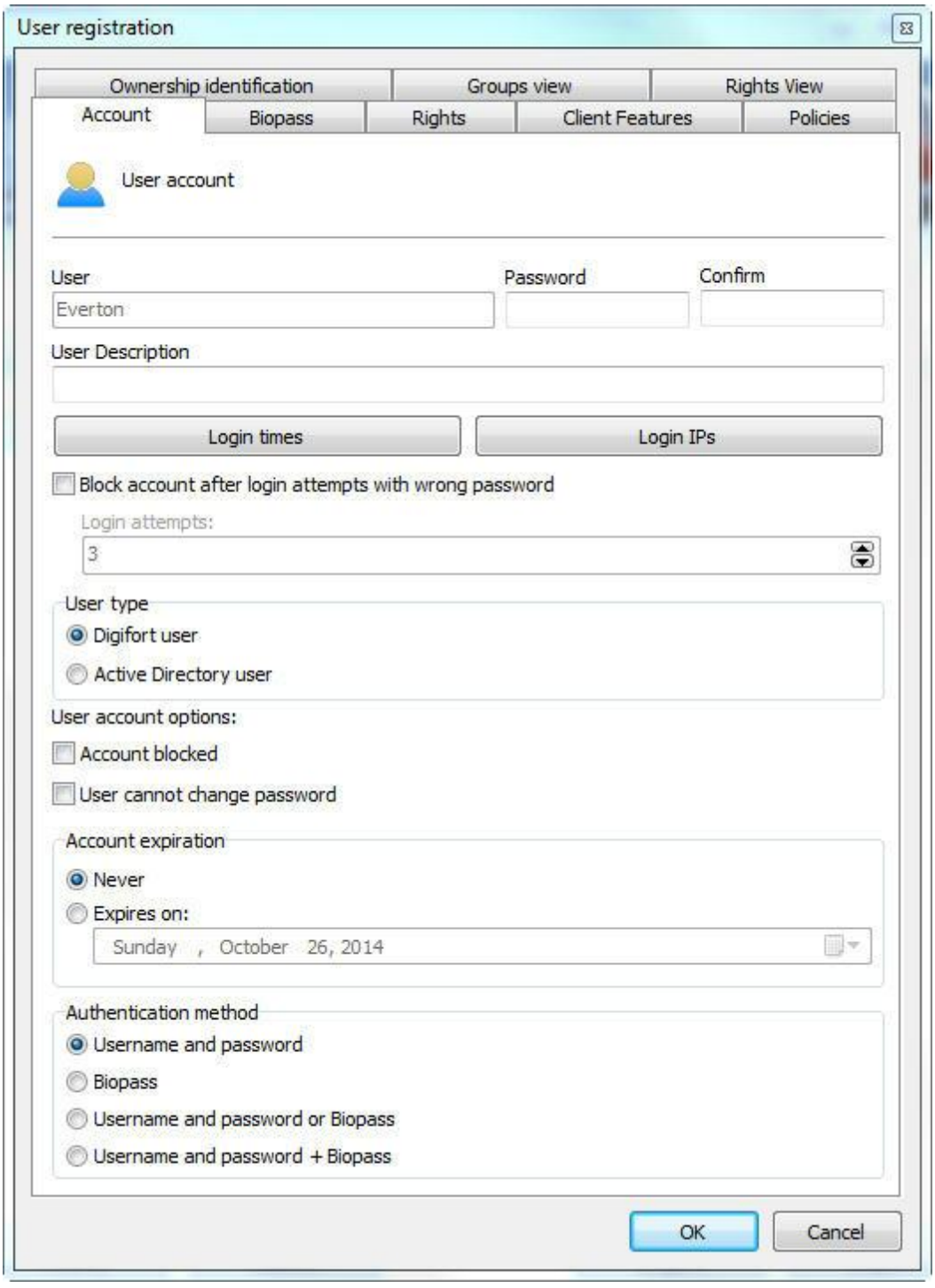
After clicking on the **Add** button, the users editing screen will be opened. Let's start by inserting the user's data, followed by the rights and, lastly, the client features.

To modify a previously registered user, select it and click on **Modify**, and alter the data as explained on the following pages.

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

9.2.1 User data

© 2002 - 2020 by Digifort, all rights reserved



The first step is to add a User is inform their primary data, they are:

- **User**: Name of the user. This must be informed at login in any module of the Digifort System. After being saved it cannot be modified.
- **Password**: The user's password.
- **Confirm**: Enter the user's password again.
- **Description of the user:** A brief description of the user, for aiding in his identification in

© 2002 - 2020 by Digifort, all rights reserved

the system.

- **Block user by invalid login:** If enabled, the system will block the account of the user who logs in with the wrong password for more than X attempts that are configurable
- **User account options**:
  - **The user cannot change the password**: With this option marked, the user can never change his password, leaving this up to the system administrator.
  - **This user will receive alerts**: With this option marked, the user will receive the configured alerts when some event occurs.
  - **Account blocked**: With this option marked, the user will not be able to authenticate himself in the system.

- **Expiration of the account:** In this parameter you can define a date upon which the user account will expire. If the user account expires, he will not be able to authenticate himself in the system. To reactivate an expired account, mark the option Never or change the expiration to a later one.
  - **Never**: The user account never expires.
  - **Expires on:** The user account expires on the specified date.

Tip

The password can be left blank when registering and the user will be able to register his password during his first access to the system.

9.2.1.1 Force use of Strong Password

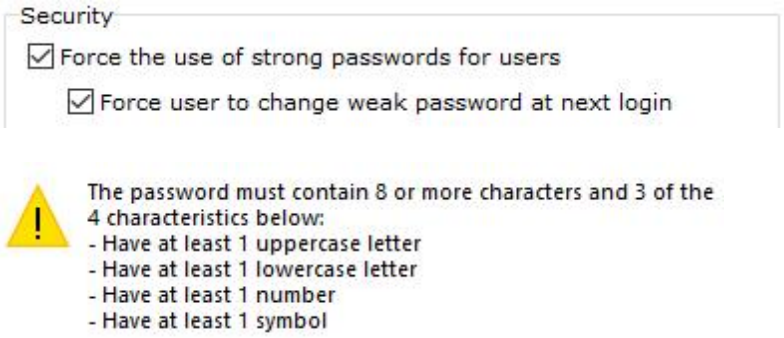
The system allows the obligation of using a strong password by part of the users. A strong password must contain at least 8 characters and have 3 of the 4 characteristics below:

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

Upon activating the option to force the use of 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) the next time the user logs in through the Surveillance Client or the AdministrationClient.

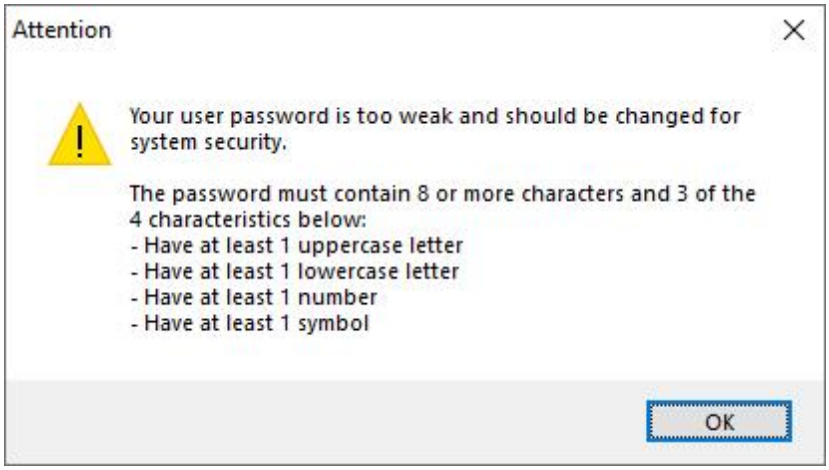
The use of a strong password applies only to native users of the system and not to LDAP/Active Directory users, where the strong password requirement must be applied directly at the domain controller.

© 2002 - 2020 by Digifort, all rights reserved



9.2.1.1.1 Weak Password Alert

Digifort will issue a weak password alert when the user accesses the server through the Administration Client using a password that does not fulfill minimum security levels.

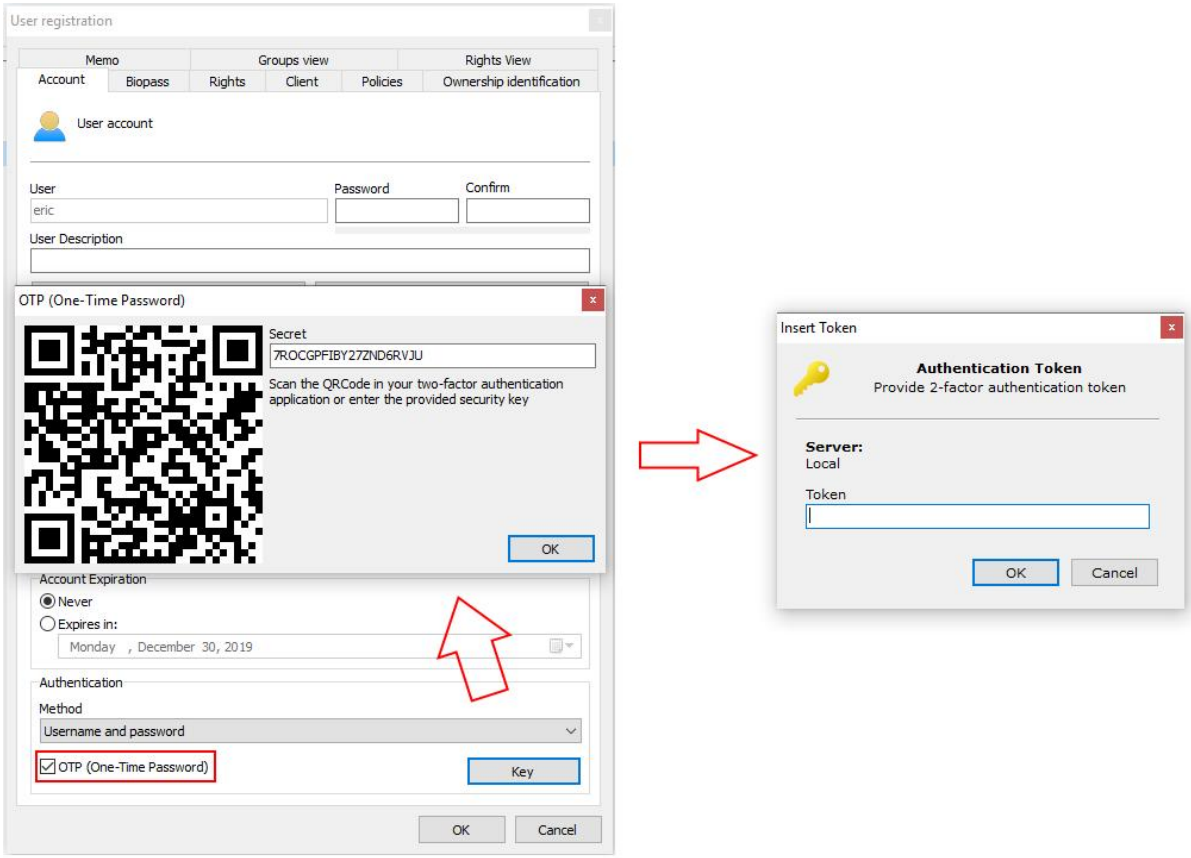


9.2.1.2 2-Factor Authentication

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

The user can use any 2FA application compatible with this algorithm (e.g., Google Authenticator).

© 2002 - 2020 by Digifort, all rights reserved



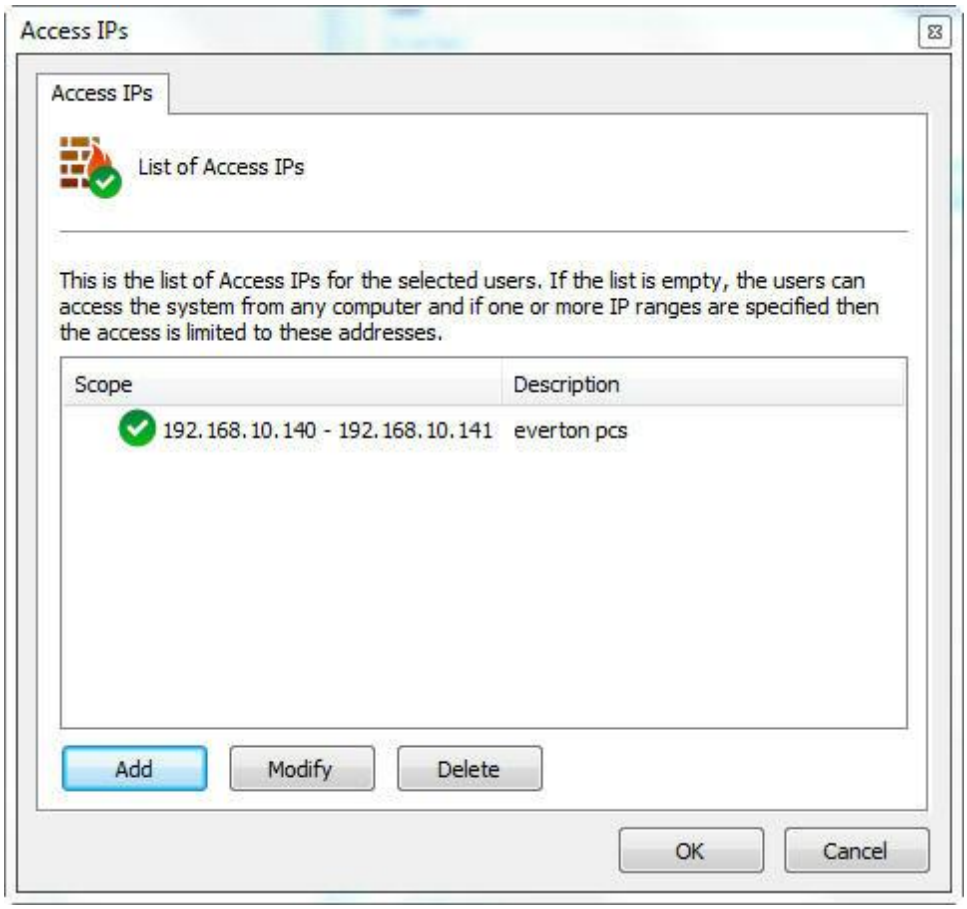
9.2.1.3 Login IPs

The configuration of Login IPs is very important for the security of the Digifort Server, as it is in this configuration that we register the range of IPs that a user can use for his authentication in the system.

For greater security, except in specified cases, it is recommended that the IP of the workstation of the user is registered, blocking access to the system from other locations like, for example, his home.
If this configuration is not done, the user will be able to authenticate at any workstation.

To access this feature, click on the **Login IPs** button, located in the User tab, opening the Login IPs register, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



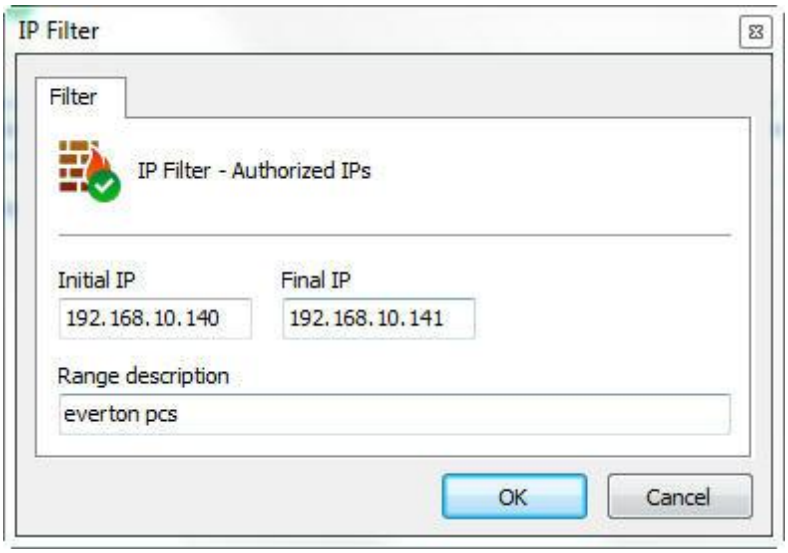
This picture examples a configuration where the user will be able to authenticate himself in the system, using IPs within the range from 192.168.5.2 to 192.168.5.4.

To add an access IP range, click on **Add**. To modify a range of access IPs, select it and click on **Modify**. To exclude a range of access IPs, select it and click on **Exclude**.

9.2.1.3.1 Adding a range of access IPs

To add a range of access IPs, click on Add and the editing screen will be displayed, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



Enter the initial IP and final IP of the range and, lastly, enter a description for the range to be added.

If you wish to add only one IP, fill in the initial IP field and the final IP field with the same value

9.2.1.4 Login hours

the Digifort server are the login hours, with which it's possible to define the times of day that users can have access to the system.

To access this feature, click on Login Hours, opening the scheduling screen. The function of this screen is specified on page How to configure the scheduling of recording

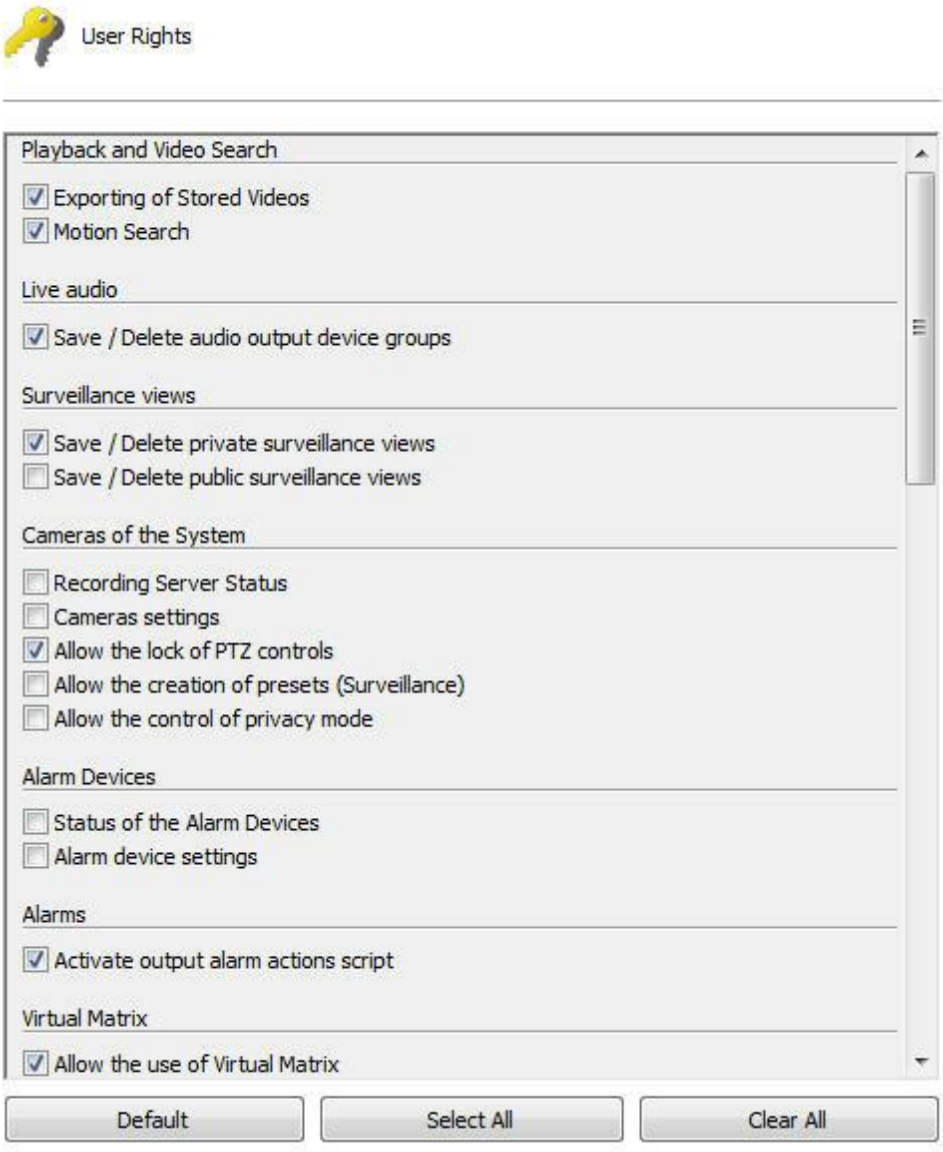
9.2.2 Biopass

To learn about this resource, refer to chapter: BioPass

9.2.3 User rights

After completing the user primary data, user access rights must be configured. By default rights are configured for a surveillance user profile, that is, it can only perform live surveillance operations and video playback in the system.

© 2002 - 2020 by Digifort, all rights reserved



9.2.3.1 Video Search and Playback

- **Export stored videos**: Allows the user to export videos previously recorded for backup, or to view them on another workstation. To learn how to export videos, check the Surveillance Client manual.
- **Advanced search**: Allows the user to perform advanced searches in stored videos. Advanced Search helps searching for incidents on a scene. To learn about Advanced Search, check the Surveillance Client manual.

9.2.3.2 Live Audio

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

© 2002 - 2020 by Digifort, all rights reserved

in the surveillance client.

9.2.3.3 Surveillance Views

- **Save / Delete private surveillance views**: Allows the user to save or delete the surveillance views regarding their account.
- **Save / Delete public surveillance views:** Allows the user to save or delete the surveillance views regarding all users connected to the Digifort server.

9.2.3.4 System Cameras

- **Recording Server Status**: Allows the user to check the overall system status and the individual status of each camera, obtaining information such as disk space used, received frames per second, uptime, etc. See more at Recording Server.
- **Camera Configuration**: Allows the user to configure the cameras to be managed by the system.
- **Allow blocking of PTZ controls**: Allows the user to block the camera movement by priority.
- **Allow the creation of presets (Surveillance)**: Allows the user to save presets via surveillance client.
- **Allow the control of privacy mode:** Allows the user to activate the privacy mode of a camera, if configured.

9.2.3.5 Alarm Devices

- **Alarm Devices Settings**: Allows the user to access the alarm devices settings. See more at Alarm Devices..
- **Alarm Devices Status**: Allows the user to access the monitoring of alarm devices status.

9.2.3.6 Alarms

- **Activate alarm output scripts**: Allows the operator to trigger the alarm outputs. See more at Alarm Devices..

9.2.3.7 Virtual Matrix

- **Allow the use of virtual matrix:** Allows the user to utilize the virtual matrix feature.
- **Allow joining the virtual matrix:** Allows the user to register their monitors to be part of the virtual matrix.

9.2.3.8 System Users

- **Users' activities on the server**: Allows the user to monitor users' activity on the server. To learn how to use this feature, check Monitoring users' activities

© 2002 - 2020 by Digifort, all rights reserved

- **Users' Registration**: Allows the user to access the users' directory.

9.2.3.9 Alerts and Events

- **Alert contacts registration:** Allows the user to access the alert contacts registration. The contacts must be registered to receive notifications about anomalies in the system or occurrence of incidents. See more at Alerts and Events..
- **Alert logs view**: Allows the user to view the alert logs.
- **Allow manual events activation**: Allows the user to activate the manual events such as a siren through Digifort.

9.2.3.10 Global Events

- **Global Events Register**: Allows the global events registration. See more at Global Events..
- **Global Events Triggering**: Allows the user to trigger the global events.

9.2.3.11 Scheduled Events

- **Scheduled Events Register**: Allows the user to register scheduled events. See more at Scheduled Events..
- **Scheduled Events Status**: Allows the user to check the scheduled events status.

9.2.3.12 Maps

- **Maps register**: Allows the registration of maps. See more at Maps.

9.2.3.13 Operational Maps

- **Operational Maps registration**: It allows the registration of Operational maps. See more in Operational Maps.

9.2.3.14 Analytics

- **Analytics Configurations Registration**: Allows the registration of analytics settings. See more at Analytics.
- **Analytics Configurations Status**: Allows viewing the registered configuration status.
- **Analytics search and reporting:** Allows the user to search and generate reports of analytics events.

9.2.3.15 Plate Recognition

- **LPR Configuration status:** Allows viewing the LPR configuration status. See more at Plate Recognition..

© 2002 - 2020 by Digifort, all rights reserved

- **Configuration and registration**: Allows the registration of LPR configuration.
- **Allow plate's inclusion in surveillance**: Allows plates registration in the LPR list via surveillance client.
- **LPR search and reporting**: Allows searching and generating LPR events reports.

9.2.3.16 Web Pages

- **Web Pages Registration**: Allows the registration of Web Pages. See more at Web Pages.

9.2.3.17 Screen styles

- **Surveillance screen styles**: Allows the user to create their own surveillance screen styles.

9.2.3.18 Server

- **Server Configuration**: Allows the user to change the system global settings, such as limit of connections to the server, disk recording limits, etc.
- **Server monitoring:** Allows the user to monitor the displayed information about the server. See more at Server Information..
- **Server logs view**: Allows the user to access the server logs configuration. See more at System Logs..

9.2.3.19 Report Authentication

- **Visualization of Authenticated reports**: Allows the user to search for the authenticated reports on the surveillance client. See more at Report authentication.

9.2.3.20 Bookmark

- **Insert Bookmarks:** Allows the user to create bookmarks on the surveillance client.
- **Bookmarks View**: Allows the user to search for and view the generated bookmarks on the surveillance client.
- **Delete Bookmarks**: Allows the user to delete bookmarks, even if he was not the creator of the bookmark in question

9.2.3.21 Record Protection

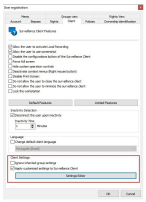
- **Protect recordings against exclusions**: Allows the user to protect recordings. See Write Protection
- **Delete recording protections**: Allows the user to delete existing recording protections. See Write Protection
- **View reports of protected recordings** : Allows the user to view the reports of the protections that were created, existing and deleted. See Write Protection

© 2002 - 2020 by Digifort, all rights reserved

9.2.4 Surveillance Client Features

The configuration of the Surveillance Client Features is very important for the security of a site. This feature provides tools that affect the person who monitors the cameras, causing other factors to interfere with the operator's attention.

To access these tools, click on the **Client Features tab**.

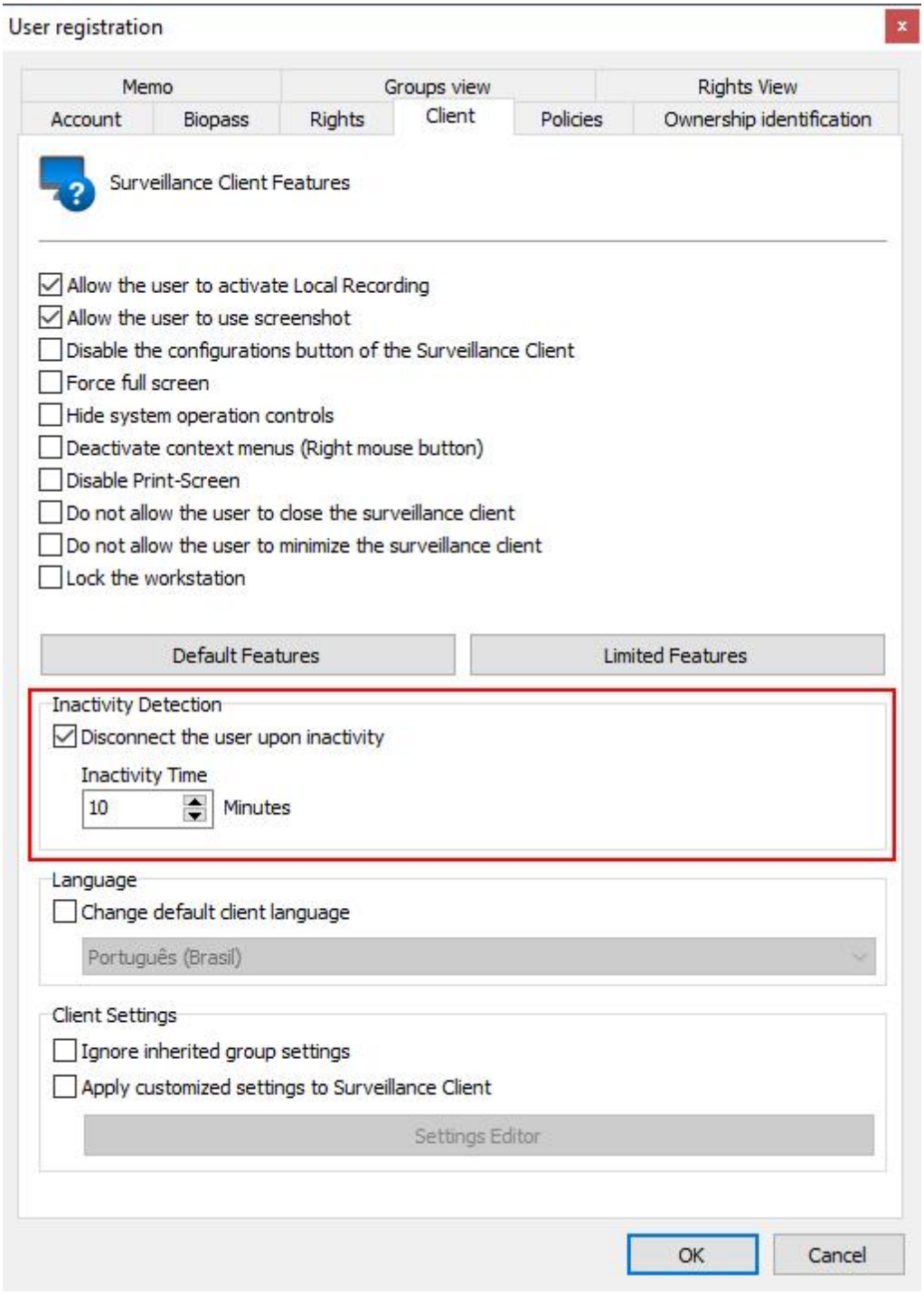


- **Allow the user to enable Local Recording:** To learn about local recording, see the Surveillance Client manual.
- **Allow the user to use screenshots:** Permission for the user to use the screenshot feature from Digifort.
- **Disable the Surveillance Client's settings button**: Prevents the user from accessing the Surveillance Client's settings. To learn about the Surveillance Client's settings, see the Surveillance Client manual.
- **Force full screen:** Forces the user to use Digifort in full screen.
- **Hide system operation controls:** This option will cause the Surveillance Client to run in "full screen" mode, in other words, the camera-viewing matrix will be expanded and the user will not have access to any operation control, being restricted to the camera-viewing screen.
- **Disable context menus:** This option will disable the use of accessible menus through the right mouse button, further blocking the 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, maintaining it locked to the system.
- **Lock Workstation**: Locks the user's workstation, not allowing the use of shortcuts, such as CTRL + ALT + DEL, ALT + TAB, and any other command that can close the Surveillance Client.
- **Automatically change client language per user**: The clients (Administration, Surveillance and Web) language can be dynamically changed for each user logged into the system, overwriting the computer's language option. Click on the option Charge default system language and then select the desired language for the user in the box.

9.2.4.1 Centralized Surveillance Client Configuration

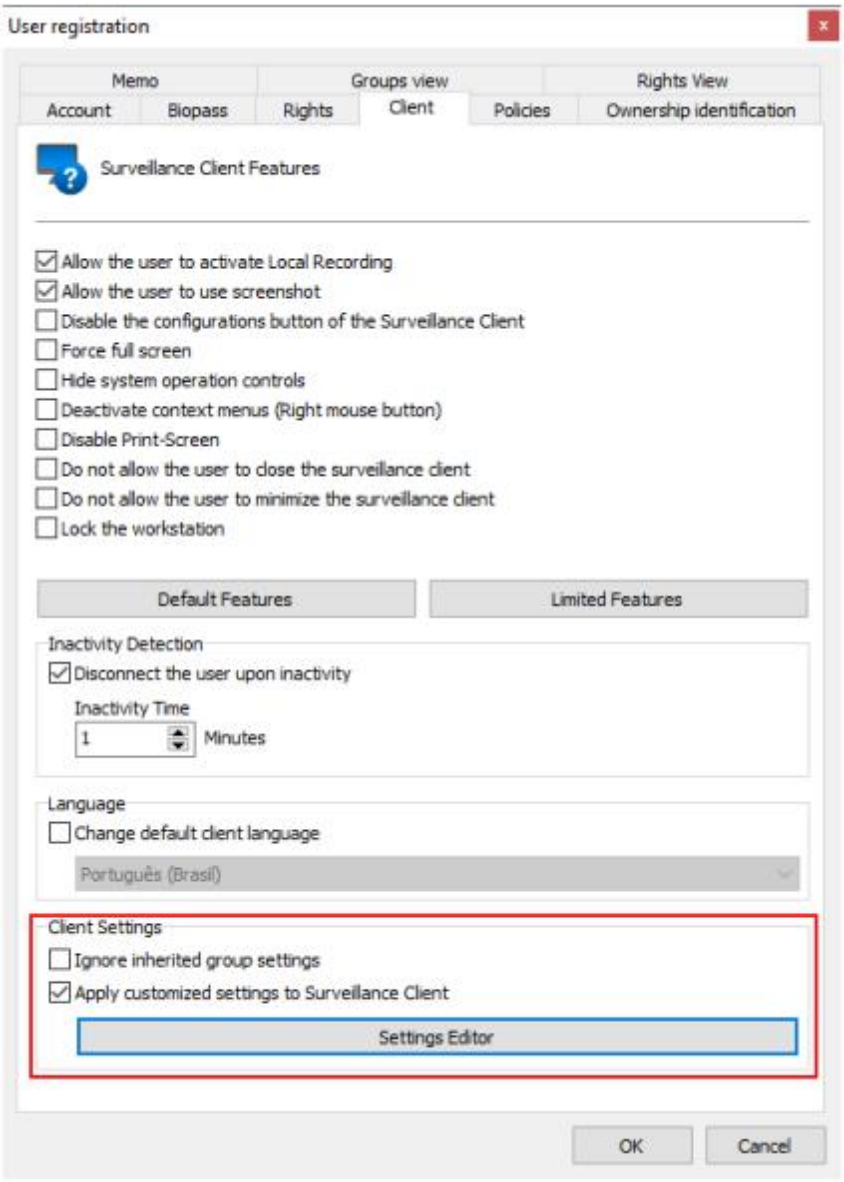
The system also configures a disconnection time due to inactivity for users / user groups.
This feature, when activated, will disconnect the user from the Surveillance Client if the user remains inactive for longer than the specified time limit.

© 2002 - 2020 by Digifort, all rights reserved



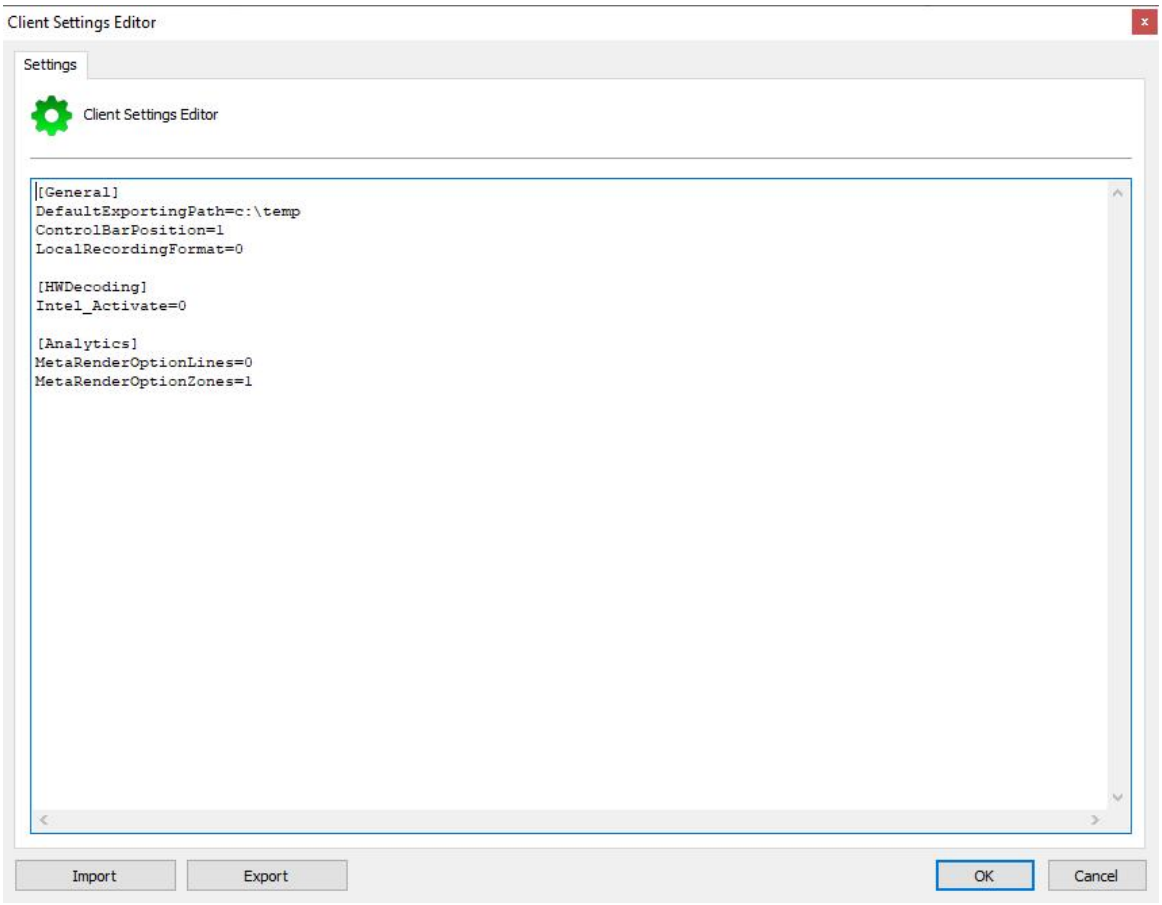
You can apply custom settings (or all settings) in the Surveillance Client according to user login. The settings are adjusted by the user and user groups.
During user or user groups registration, a new Client Settings option will be displayed:

© 2002 - 2020 by Digifort, all rights reserved



The editor allows you to adjust the settings and values to be applied in the Surveillance Client when the user logs on the server.The values follow the INI file format:

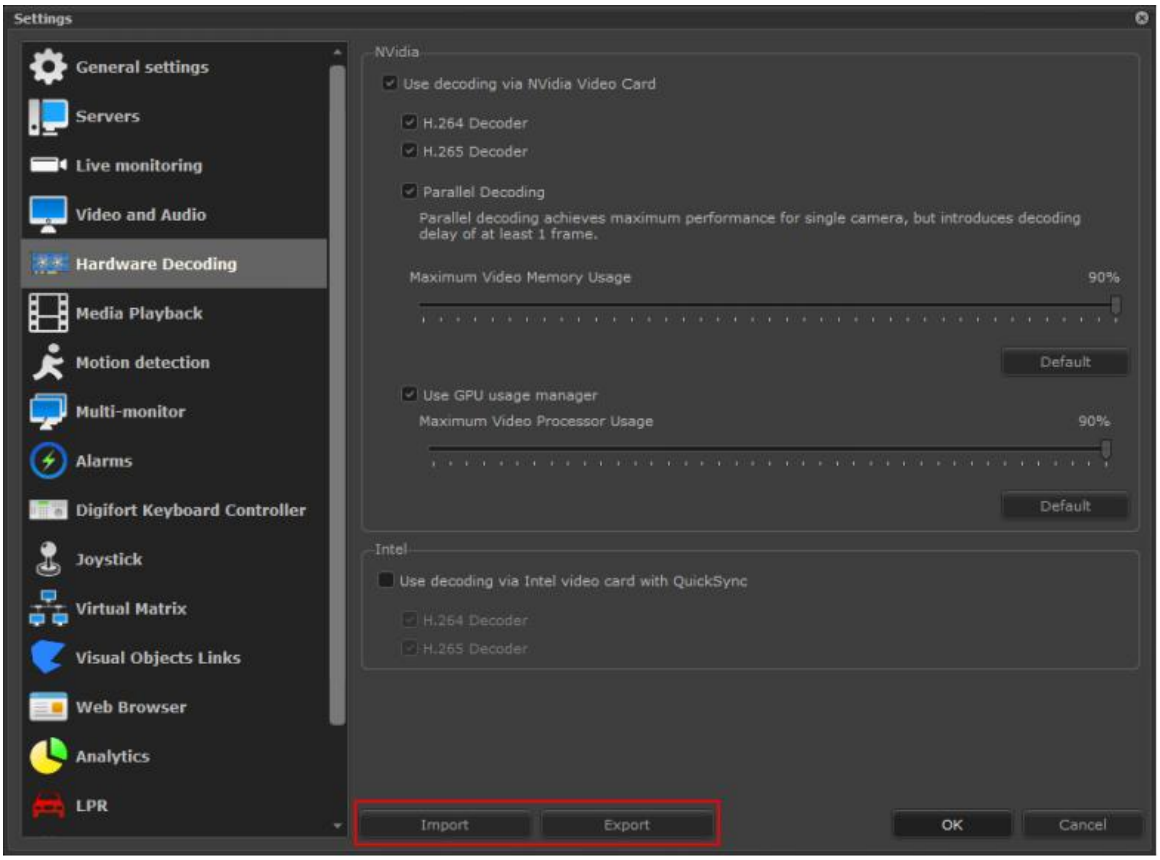
© 2002 - 2020 by Digifort, all rights reserved



This is a way to force default settings for multiple Surveillance Clients in a centralized manner, thus facilitating workstation distribution and configuration, as their options can be changed in the user profile.

The settings values can be exported through the Surveillance Client's settings export screen:

© 2002 - 2020 by Digifort, all rights reserved

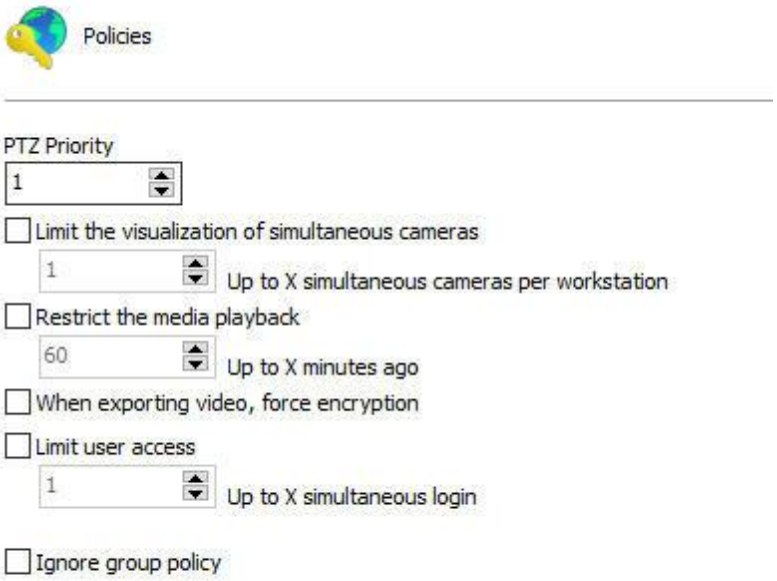


You can change any setting value and apply it to the client through this editor. It uses a settings file exported from the Surveillance Client as settings reference values to be added to the editor.

9.2.5 Policies

These settings enable you to define some policies related to Digifort and the user.

© 2002 - 2020 by Digifort, all rights reserved



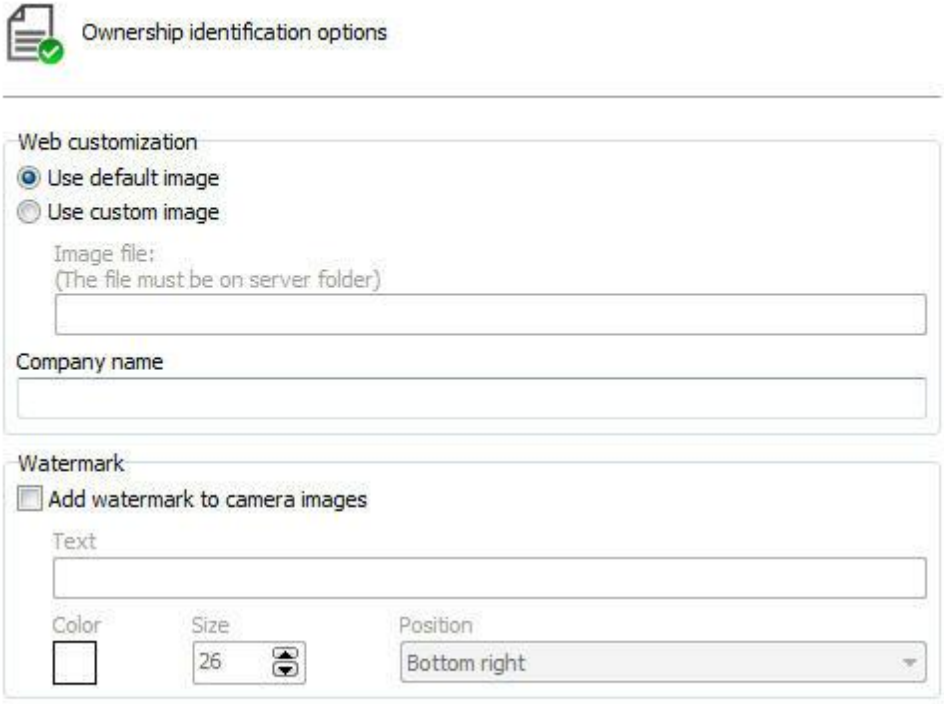
This screen allows the following settings:

- **PTZ Priority**: This option aims to prioritize a user in the use of the cameras PTZ. The priority with value 1 is the highest of all, therefore, no user with equal or lower priority may unlock the PTZ while this user is using it. Now let us imagine a user with priority 3. That user will lose control of the PTZ to the one who has a higher priority, in this case 1 or 2, but no user on the same level or lower (3, 4, 5, 6...) can take control of PTZ while he is using it.
- **Limit the visualization of simultaneous cameras**: Restricts the number of cameras that the user can simultaneously view on the Digifort surveillance client.
- **Restrict the media playback**: Limits the user to only view X configurable seconds of video from before the current date from the server on the surveillance client.
- **Force encrypted exporting**: Allows you to force the use of encryption on every video export. This option can be configured per user or user group. For more information about encrypted exporting, see the Surveillance Client manual.
- **Limit user access**: Limits the user to stay logged into the system from up to X simultaneous logins.
- **Ignore group policies**: The user with this option set does not have a group policy superimposed by the one of from his user.

9.2.6 Property ID

These settings enable you to customize the page of user interaction when the Digifort is accessed through an internet browser and the image that is seen or reproduced by users in monitoring client.

© 2002 - 2020 by Digifort, all rights reserved



9.2.6.1 Web personalization

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

Can be created a different web customization for each user, simply specify these parameters properly on registration of each user.

© 2002 - 2020 by Digifort, all rights reserved

To access these settings click on the tab Web Customization, as illustrated in the figure below: To access this feature, click the Privacy tab, as shown in the figure below:

- **Use default image:** Displays the logo of Digifort on interaction with the user.
- **Use custom image:** Enables the field path to the image allowing to locate an image on your computer that will be used on the user interaction page, replacing the Digifort logo.
- **Company name:** Type the company name for the view in the user interaction page

9.2.6.2 Water mark

This feature lets you can create a watermark over the image that is viewed and reproduced by the user. This water mark aims to identify the owner of the images when the images of the system are provided to external users. This watermark will also be present in the export of images.

To insert a watermark in the video click "Add watermark on the images from the cameras". The following options are available:

- **Text**: Text to be inserted as watermark.
- **Color**: Color of inserted text as watermark.
- **Size**: Font size of the inserted text as watermark.
- **Position**: Position the image where the watermark will appear.

Below is an example of watermark in an image on the client tracking:



9.2.7 Groups Inquiry

Allows viewing of the groups in which the user is registered.

© 2002 - 2020 by Digifort, all rights reserved



9.2.8 Rights Inquiry

This screen allows viewing of the rights given to the user, such as, for example, the right to view and playback cameras and maps.



This screen offers the following functions:

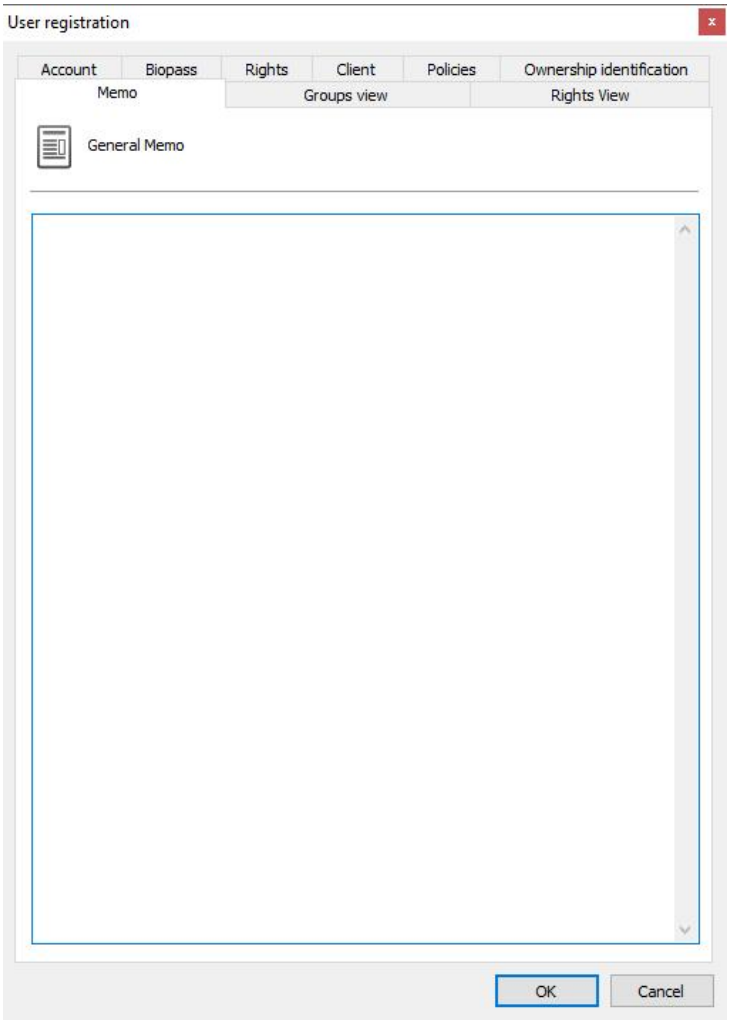
- **Type of right**: List of the types of rights given to the user.
- **Objects:** List of the objects related to the given right

9.2.9 User general observations field

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

The field can also be displayed in the users list through extended columns and exported together with the users list export..

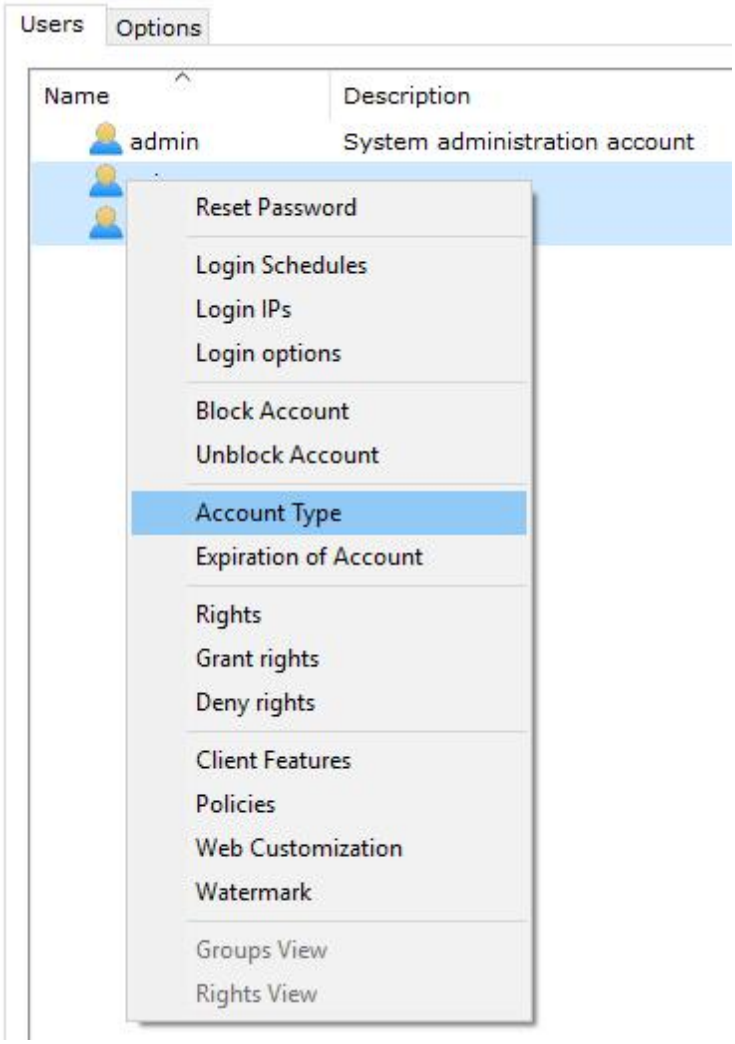
© 2002 - 2020 by Digifort, all rights reserved



9.3 User administration functions

The Digifort's User Administrator offers rapid access to the most common user configurations. In the user register, select the desired user and click on the right button. A menu will be opened, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



9.3.1 Reset password

Resets the password of the selected user, leaving it blank. For security reasons, this option will be available selecting one user at a time.

9.3.2 Login IPs

Opens the configurations of user login IPs. This configuration allows you to define from which IPs a user can authenticate himself in the system. To learn how to use this feature, see Login IPs

9.3.3 Login options

Opens account lockout settings after a certain number of failed attempts.

© 2002 - 2020 by Digifort, all rights reserved

9.3.4 Block account

Blocks the account of selected users, making them unable to authenticate in the system. com que eles não consigam autenticação no sistema.

9.3.5 Unblock account

Unblocks the account of selected users, making them able to use the system again.

9.3.6 Account Type

It allows changing the type of account (Digifort or Active Directory) of the selected users.

9.3.7 Account expiration

Defines an expiration date for the accounts of the selected users. After the expiration date, the user can no longer authenticate himself in the system..

9.3.8 Rights

Opens the user rights screen. To learn about user rights, see Login hours

9.3.9 Give rights

Opens the user rights screen giving the selected rights. If no right is selected, but some user has it, the rights defined here will be added. somados.

9.3.10 Deny rights

Opens the user rights screen denying the selected rights.

9.3.11 Features

Opens the features screen of the Surveillance Client. To learn about this feature, see Surveillance Client Features.

9.3.12 Policies

Opens the Policies screen. To learn about this feature, see Policies.

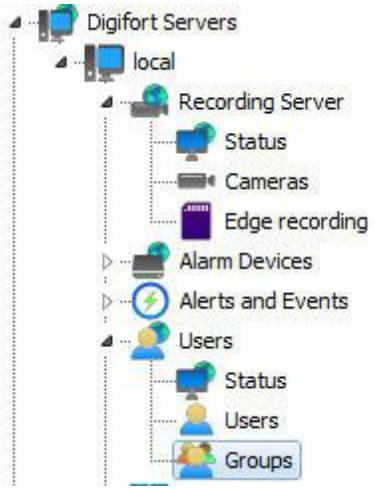
9.3.13 Web customization

Opens the screen for configuration of the user's web customization. To learn how to use this feature, see Web Customization

© 2002 - 2020 by Digifort, all rights reserved

9.4 Adding, altering and excluding Groups

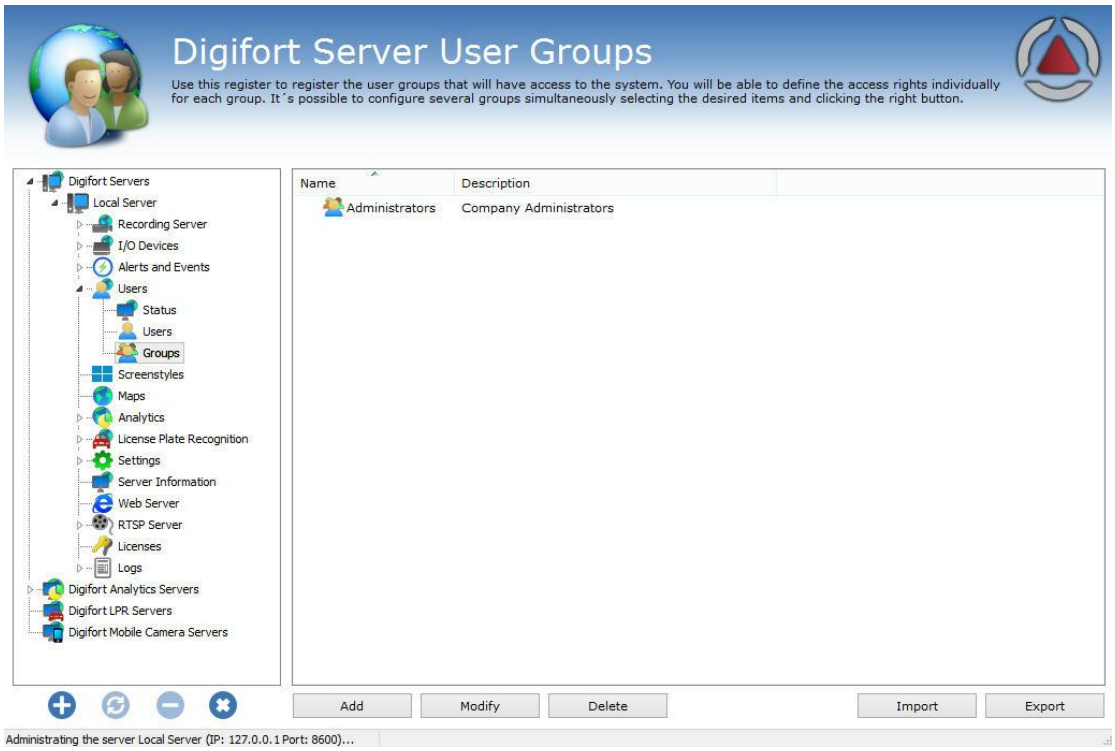
To access the group management feature, locate Groups in User in the server's Configurations menu as shown in the picture below:



The 'Groups' option was created to facilitate user management within the system.

Once this is done, the Groups management screen will open on the right as illustrated in the picture below:

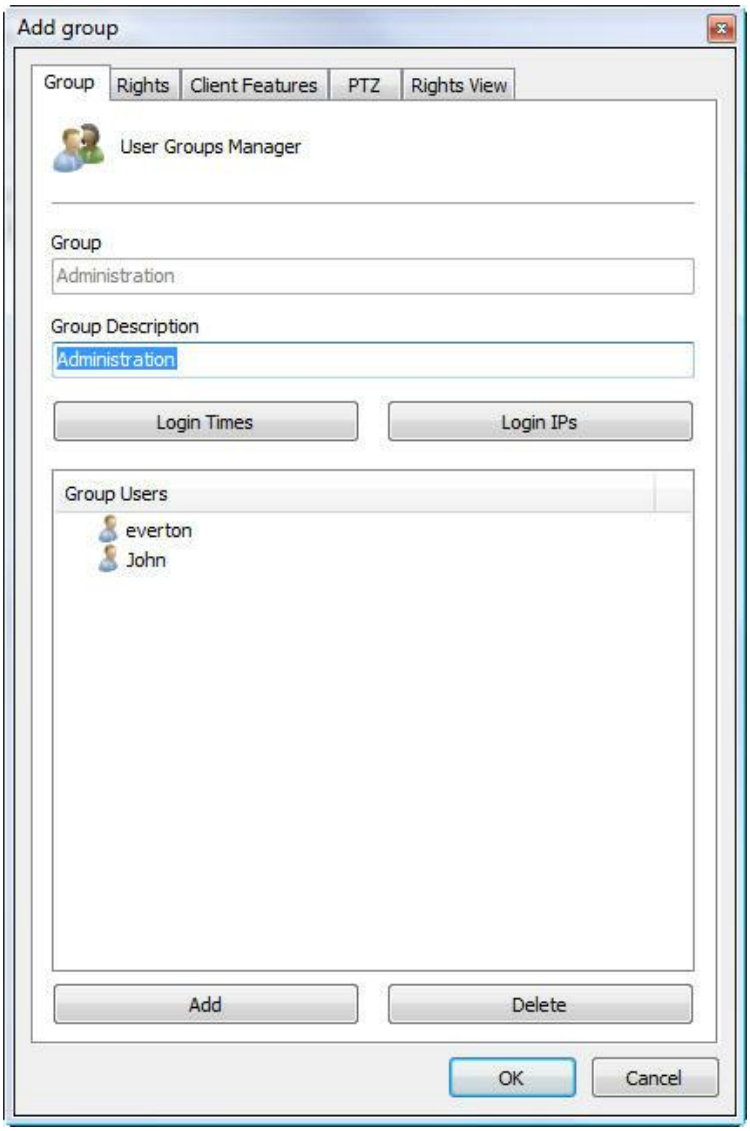
© 2002 - 2020 by Digifort, all rights reserved



By clicking on the Add button, the group edition screen will open up. Let's start by introducing a group, moving on to the entitlements and then the features.

To change an already registered user, select it and click on Change and then change the data as explained throughout the manual.
To remove a user, select the user you wish to remove and click on the Remove button.

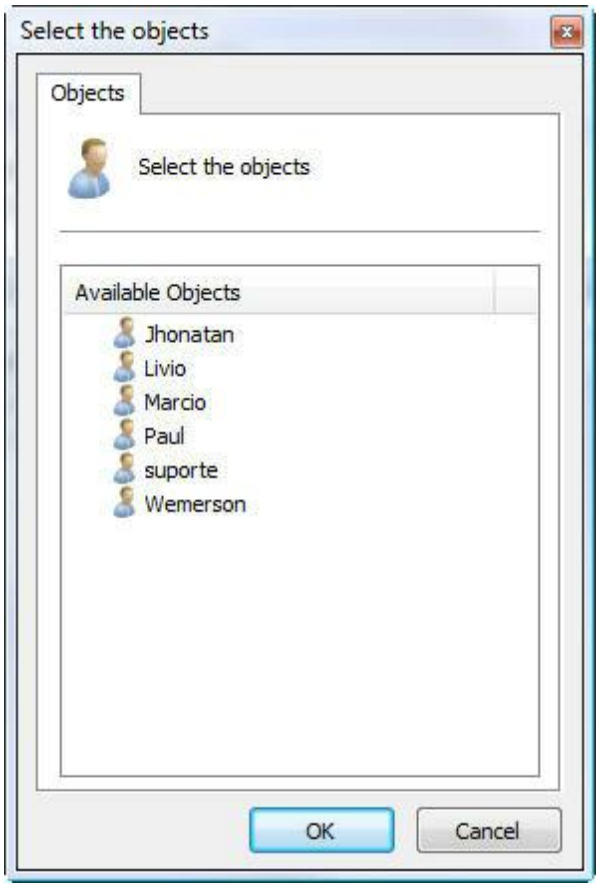
© 2002 - 2020 by Digifort, all rights reserved



When adding a group, the first step is to indicate its main data, i.e.:

- Group: Username, which must be indicated when logging in to any module of the Digifort System. Once saved it cannot be altered.
- Group description: A brief description of the user to help identify him in the system.
- Login times**:** To learn about this feature refer to Login Times
- Login IPs: To learn about this feature refer to Login IPs
- Group Users: List of users in the group. To add a user to the group, simply click on **Add** and a window will open so that you may select the user to be added as shown in the picture. To remove a user, simply select it from the list and click on the **Remove** button.

© 2002 - 2020 by Digifort, all rights reserved



9.4.1 Group rights

After filling in the main user data, the access rights must be configured. As default, the rights are configured for a surveillance user profile, that is, the user will only be able to carry out the system operations of live surveillance and video playback.

As configurações de direitos para o grupo é igual a configuração de direitos de usuário.

9.4.2 Surveillance Client Features

The configuration of the features of the Surveillance Client is very important for the security of a site. This feature offers tools that affect the person who monitors the cameras, causing other factors to impair the attention of the operator.

The configuration of the Resources of the Surveillance Client for the group is the same as the configuration of the Resources of the Surveillance Client of the user. To learn how to configure the Resources of the Surveillance Client of the group see Surveillance Client Features.

© 2002 - 2020 by Digifort, all rights reserved

9.4.3 PTZ

These configurations allow the definition of a priority to the group of or PTZ control of the cameras.

The configuration of the PTZ for the group is the same as the configuration of the PTZ of the user. To learn how to configure the PTZ of the group see PTZ

9.4.4 Rights Inquiry

This screen allows the viewing of the rights given to the group, such as, for examplo, the right of viewing and playback of cameras and maps.

The configuration of the Rights Inquiry for the group is the same as the configuration of the Rights Inquiry of the user. To learn how to configure the Rights Inquiry of the group see Rights Inquiry

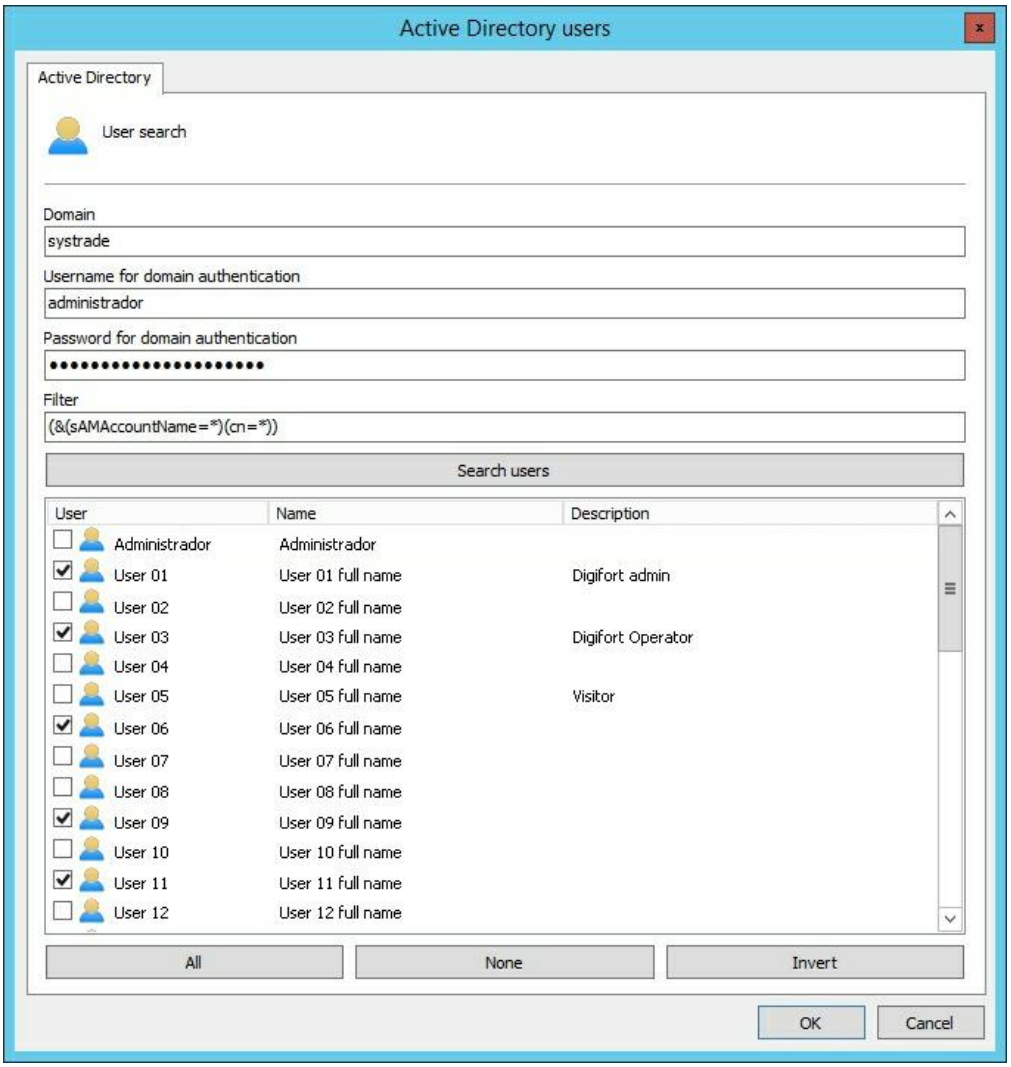
9.5 Integration with the Active Directory

The **Active Directory** is a set of archives located in the domain server which holds all the information needed to control user access to the network. The usernames and passwords are registered in the Active Directory, including authorizations to access archives, printers and other network features, the disk quotas, computers and times each user can use, etc.

Interaction with the Active Directory means that network users of the Digifort server domain can be imported and integrated as Digifort users.

There are 2 ways in which to integrate them: the first is to import the users directly from the Active Directory. To do so, in Users click on **Import** from **Active Directory** as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



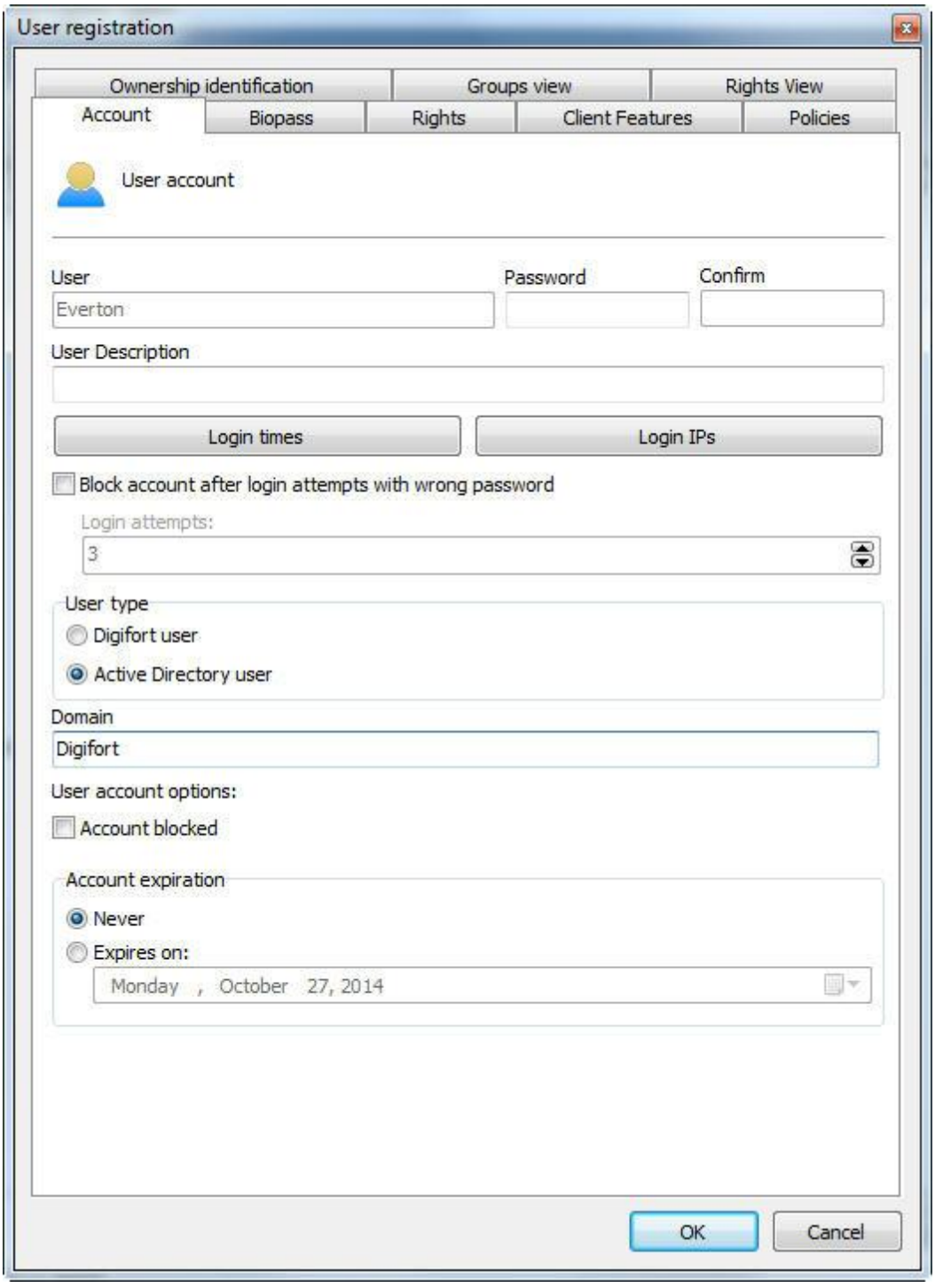
This screen has the following functionalities:

Domain: Type the network domain.
Username for domain authentication: Username to be authenticated in the domain.
Password for domain authentication: Domain user password.
Filter: Filters allow you to define criteria and provide more efficient searches. To learn about the LDPA filter visit the microsoft page: https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx

After filling in each field, click on **Search Users** and all users registered in the domain will be listed. To add users to Digifort simply select them and click on OK.

A user belonging to the domain has the following configuration screen:

© 2002 - 2020 by Digifort, all rights reserved



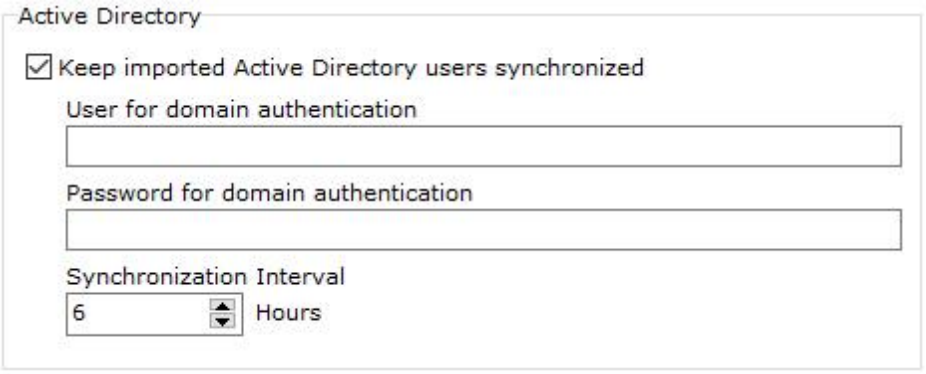
All the username and password options are blocked because the authentication is made in the domain and no longer in Digifort, so the block account options, Biopass and account Expiry will no longer be available.

It is possible to change a user already found in Digifort to a network user, simply change the "User Type" field. To function properly, the username and the domain must be filled in correctly

© 2002 - 2020 by Digifort, all rights reserved

according to the users registered in the current Domain.

The server allows users imported from Active Directory to be kept in sync with the domain, that is, if the user is deleted from the domain, it will also be deleted from the system.



© 2002 - 2020 by Digifort, all rights reserved

Chapter



10 Screenstyle Administration

Screenstyles are groupings of cameras in a determined format and order that are used by the Surveillance Client to exhibit the cameras in the screen.

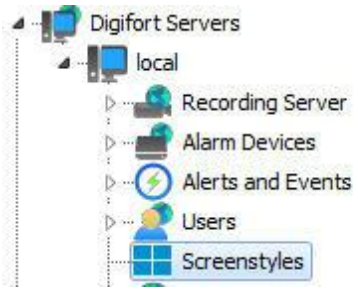
In addition to pre-defined screenstyles, Digifort Enterprise allows for the creation of new types of screenstyles, aimed at customization of the system according to the user's taste.

In the Administration Client, it's possible to administer the screenstyles, that is, their creation, modification or exclusion. To learn how to add cameras to the screenstyles, consult the manual of the Surveillance Client. Cliente de Monitoramento.

Note: To know the limitations of your version of Digifort see the feature matrix on our Website: http://www.digifort.com.br/feature-matrix

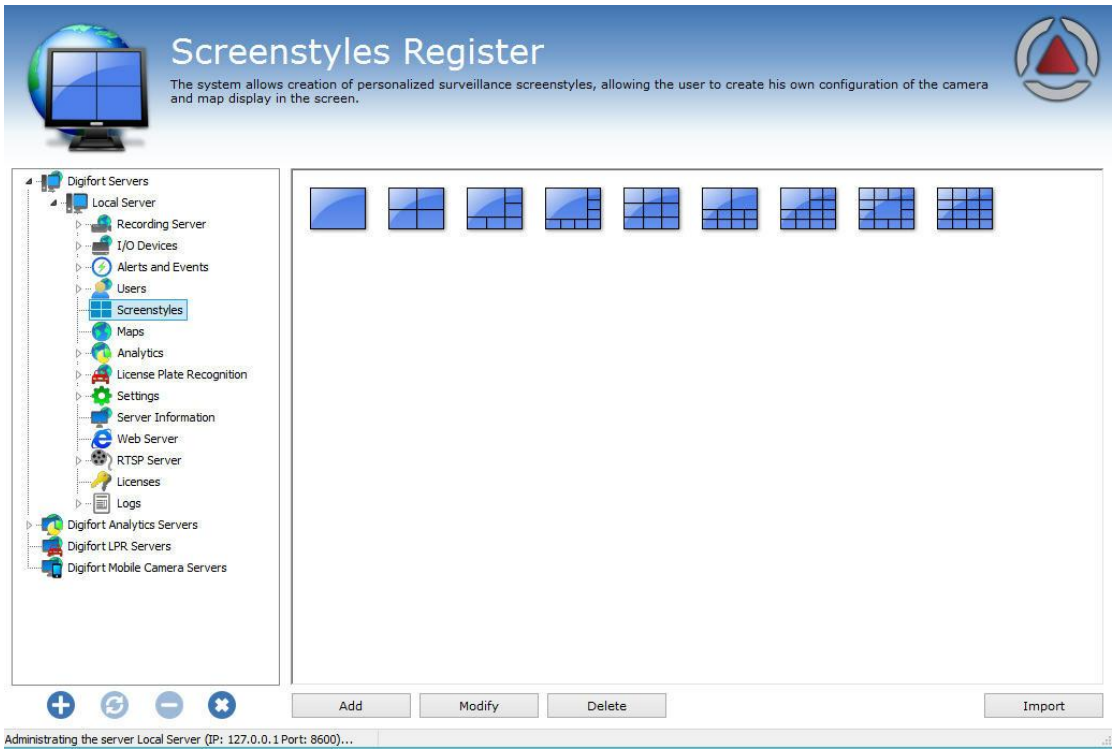
10.1 How to access the screenstyle administration

To access the screenstyle administration, locate the item Screenstyles in the Configurations Menu, as shown in the picture below:



Once this is done, the screenstyles register will be displayed at the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

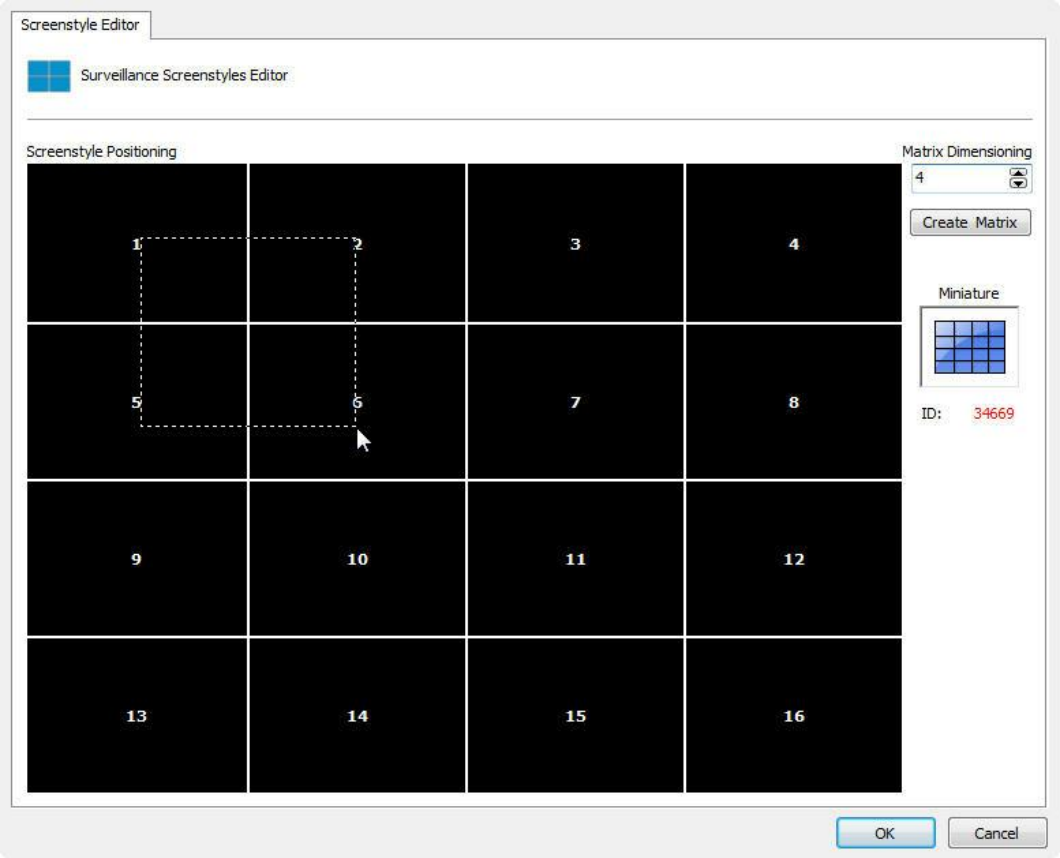


Digifort Enterprise offers six pre-defined screenstyles that cannot be modified or excluded. To add a screenstyle, click on Add. To modify or exclude a screenstyle, select it and click on the corresponding button.

10.1.1 How to add a screenstyle

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

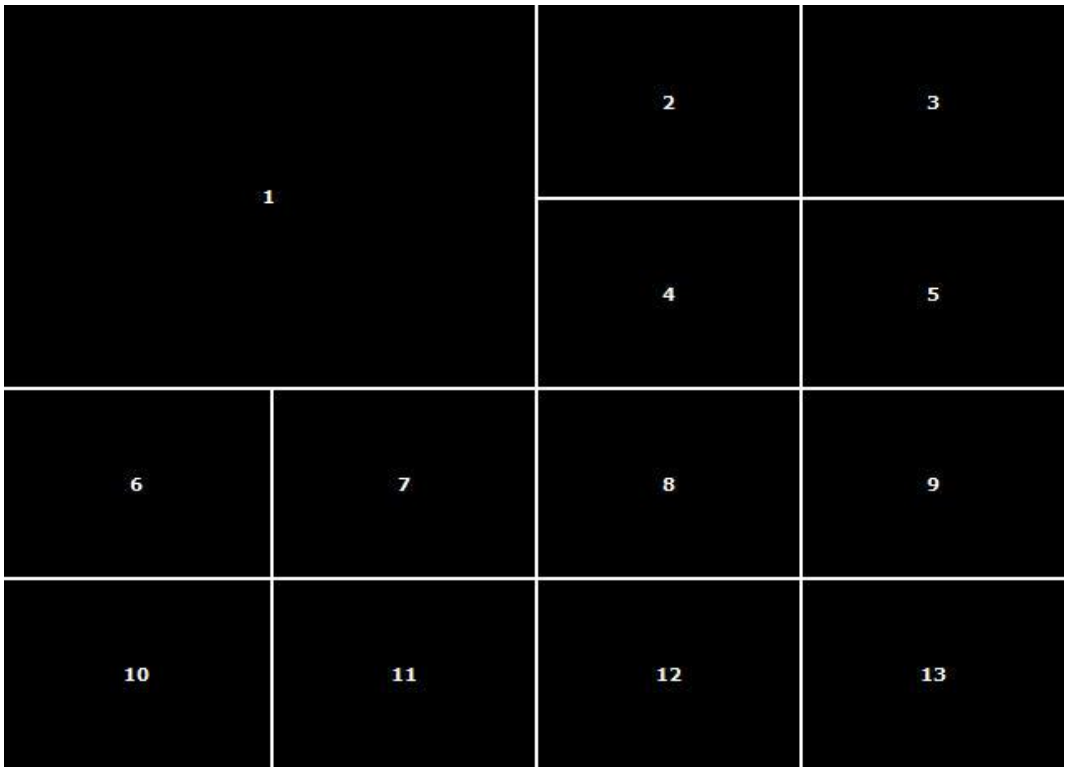
© 2002 - 2020 by Digifort, all rights reserved



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

After creating the matrix, it's possible to join the quadrants, clicking on the left button of the mouse and dragging it, with the purpose of having a larger visualization area. In the example above, we are joining the quadrants 1, 2, 5 and 6, forming the screenstyle presented in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



By joining these four quadrants we obtain space for allocation of 13 cameras, with one of them having double the size.

It's possible to join as many quadrants as necessary as long as the final area is a rectangle.
To undo this joining, repeat the process with the right button of the mouse.

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter XI

11 BioPass

BioPass is an authentication product via Digifort's biometry. To increase the security of users who have been authenticated in the system, it is possible to enforce a biometric authentication.

11.1 How to install BioPass on your computer

After installing the Digifort 7.3.0.0 Enterprise, , the drivers of the BioPass Digital Reader will be available to be installed by the operational system.
With the 7.3.0.0 Enterprise already installed, connect the BioPass reader to your computer and the following message will show up on the Operative System:

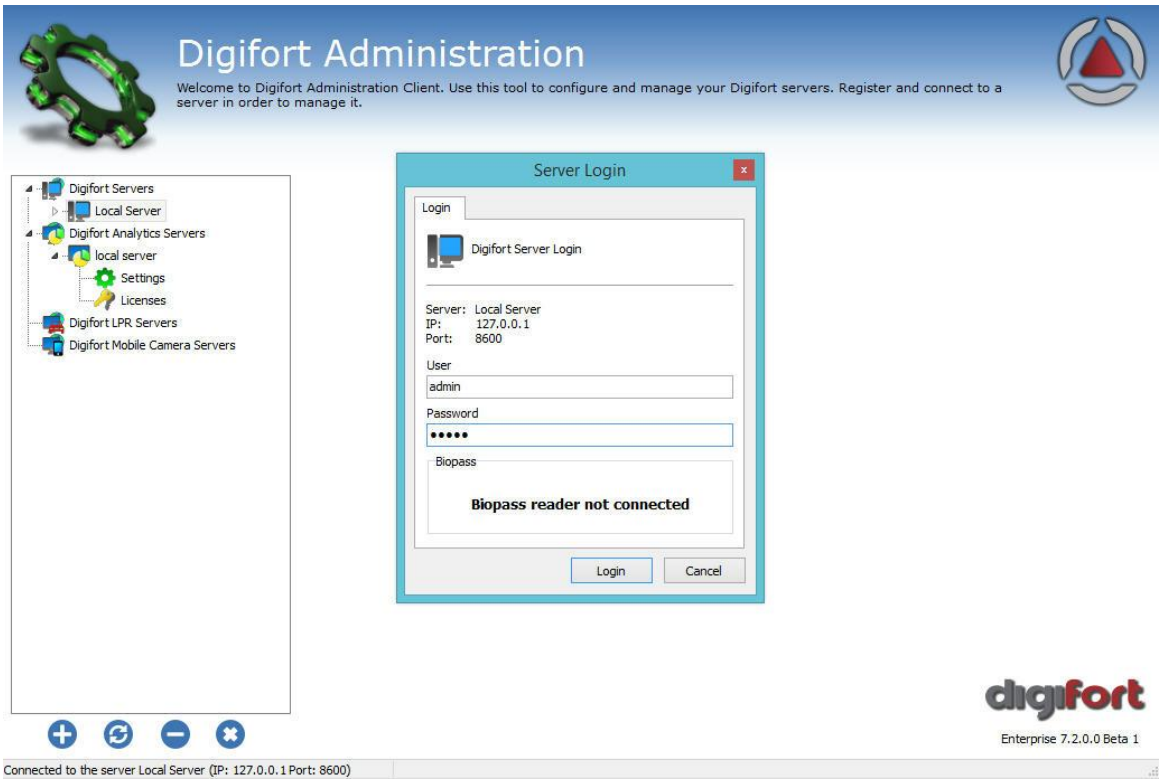


Once this message is shown, you can configure the BioPass in Digifort.

11.2 How to configure the BioPass

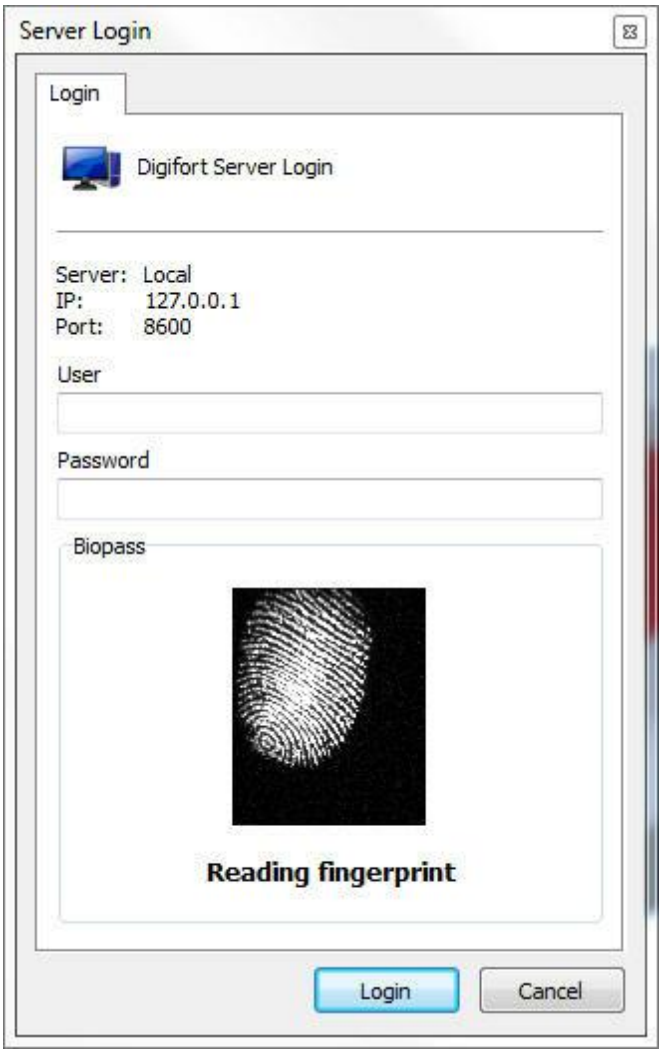
If the reader is not recognized or is not plugged in, the message **Biopass reader not connected** will show up as in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



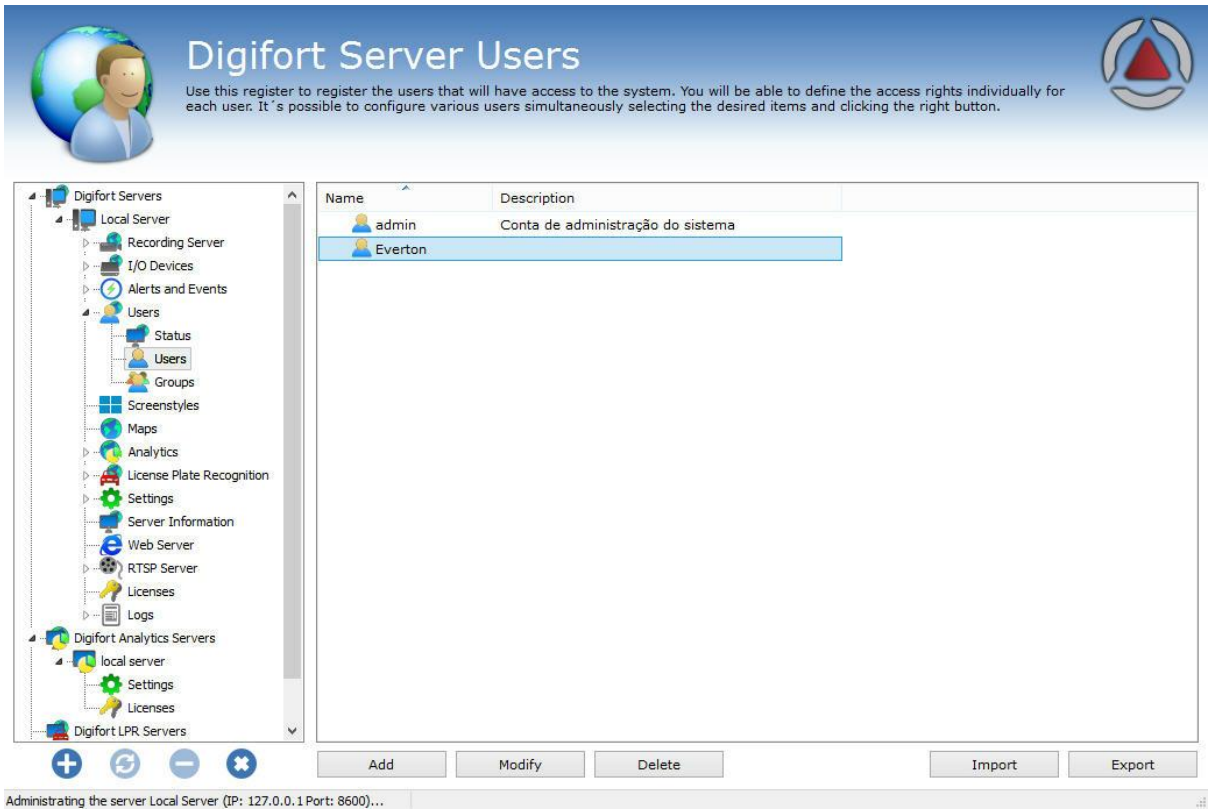
Once the reader is plugged in and recognized by the operative system, open Digifort's Administration Client and Log into your server.
Note that the Login screen now has a differential as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



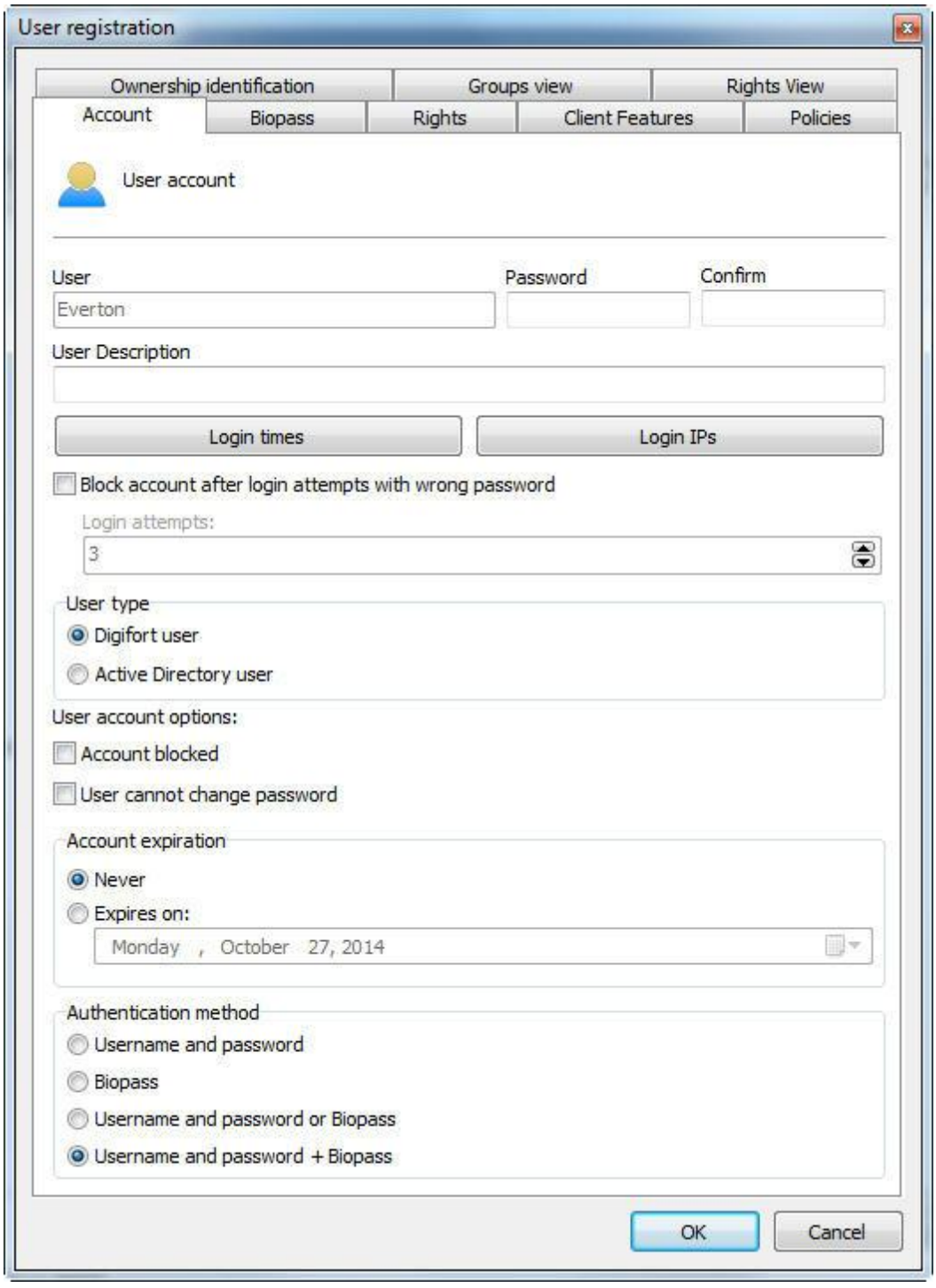
There is a finger print view on the screen but no finger print has yet been registered, so the Login must be made with the username and password.
Now, to configure the finger prints go to "**Users"** as shown in the following picture:

© 2002 - 2020 by Digifort, all rights reserved



Now, create a user to configure the Biometric Reader. (See User Management to learn about the system's users):

© 2002 - 2020 by Digifort, all rights reserved



Insert a username, a password and a description for the New User. In the field "**Authentication Method**" there are four options:

- Username and password: System's standard authentication.
- **Biopass:** Only asks for the finger print authentication
- **Username and password or BioPass**: The login can be made with the username and password

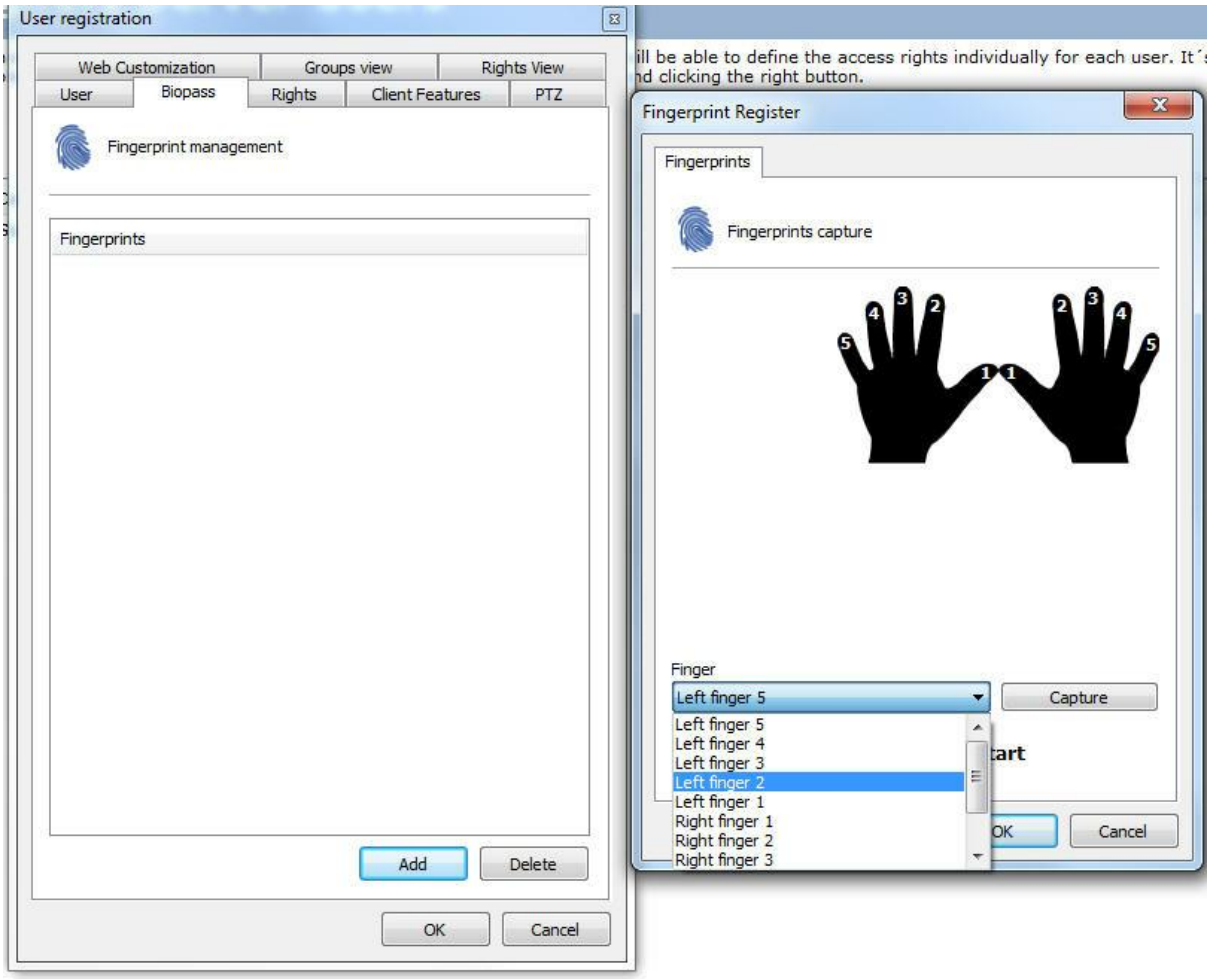
© 2002 - 2020 by Digifort, all rights reserved

or BioPass. (Not recommended unless you need to use the web server as it does not have the BioPass functionality).

- Username and password + Biopass: Needs username and password + Biopass for login.

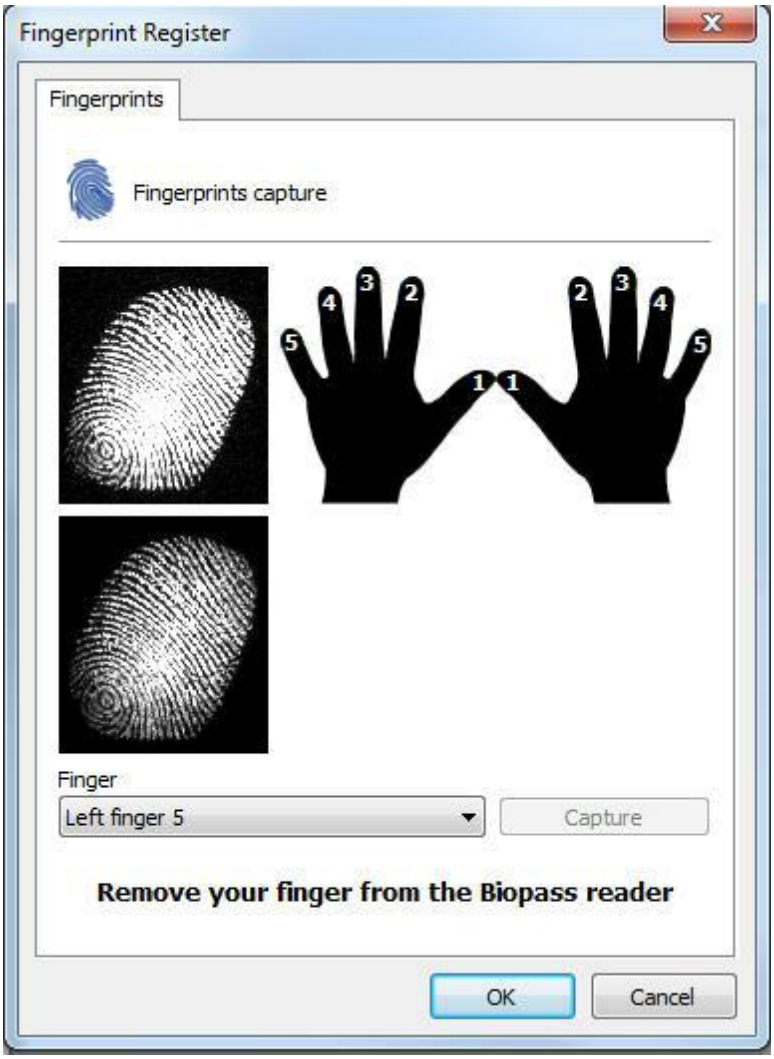
Here the user selects how he will log into the system, in this case **"Username and Password + Biopass".**

Remember that the option "User and Password + Biopass" is the most recommended in terms of security as it will force the user to use his username and password and also use the biometric authentication.
Now this part has been configured, we can open the **"BioPass"** tab as shown in the following picture:



Click on "**Add"** and, on the screen on the right select the finger you will be using for the digital print (you can also click on the number on the 'hand' picture). Once you have decided which print to use click on "Capture"

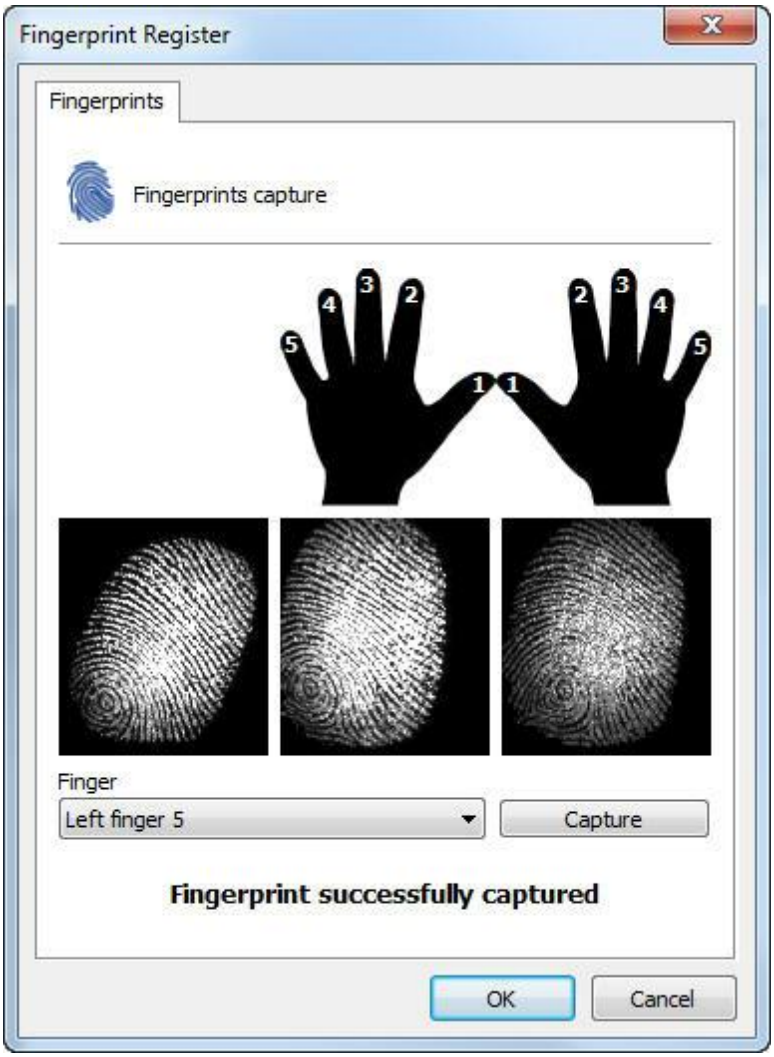
© 2002 - 2020 by Digifort, all rights reserved



A minor change has occurred on the screen and you should now see the instructions to configure the Digital authentication.
The software will ask you to capture three digital prints of the same finger. Place your finger on the BioPass and remove it when the message **Remove your finger from the BioPass** reader is shown.

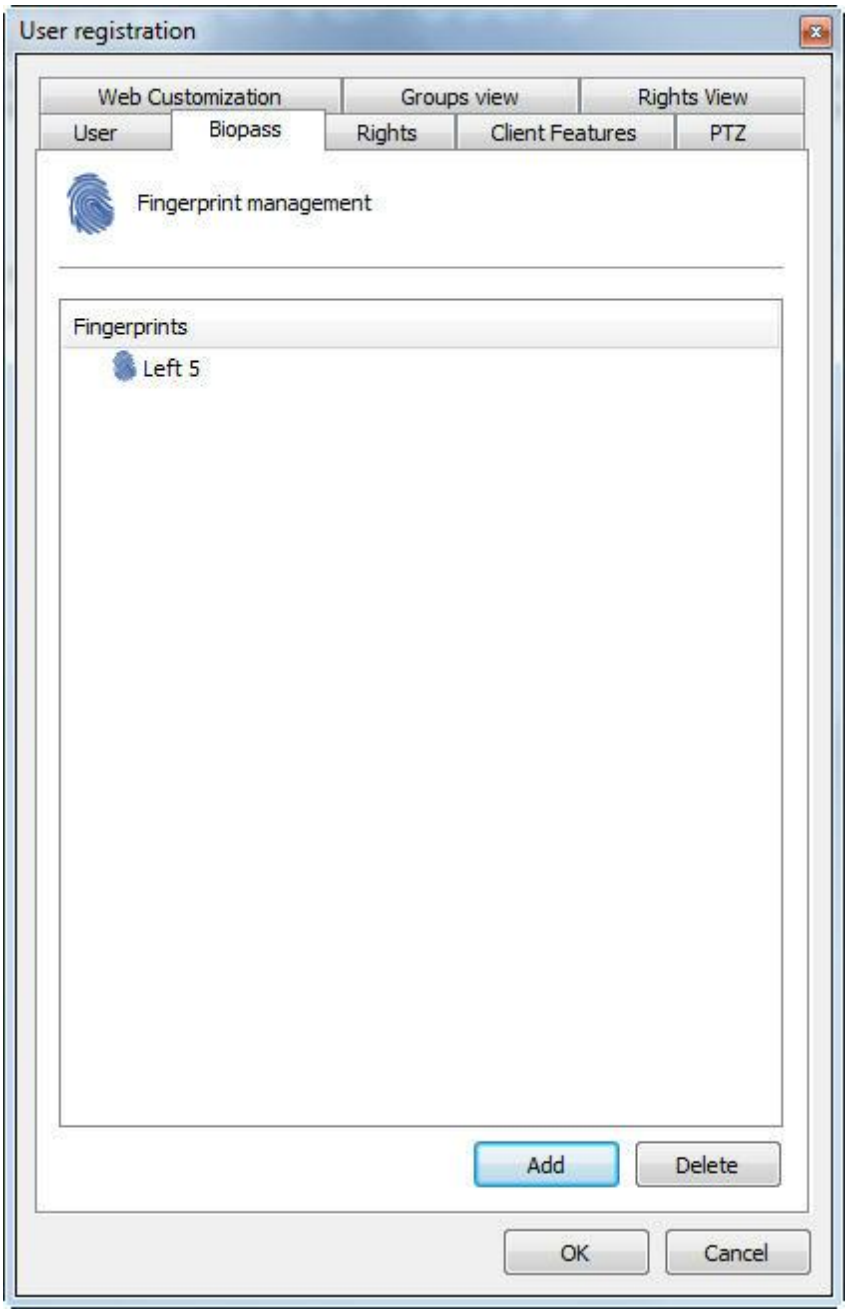
Once the print has been captured, you should receive the message **Digital print captured successfully:**

© 2002 - 2020 by Digifort, all rights reserved



When finished, click on “OK” to save the configuration applied to that print and you will see a screen with the captured finger prints as in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



For security purposes, it is recommended that you capture more than one finger.
From now on, the login can be made via BioPass both in the Administration Client as well as the Surveillance Client.

© 2002 - 2020 by Digifort, all rights reserved

Chapter XII

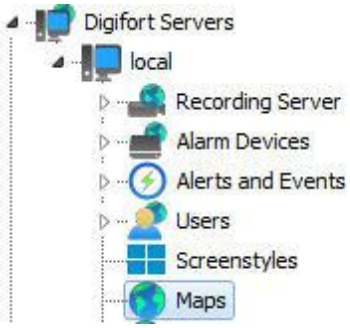
12 Maps

The Digifort software brings another built-in feature – a synoptic map, which makes the complete surveillance of an industrial plant, a building, etc., possible. With the map there is better viewing and control of the site, making the viewing of cameras as well as activation of alarms possible.

NOTE: To conheçer limitations of these resources for your version of Digifort see the matrix of resources on our website: **http://www.digifort.com.br/feature-matrix**

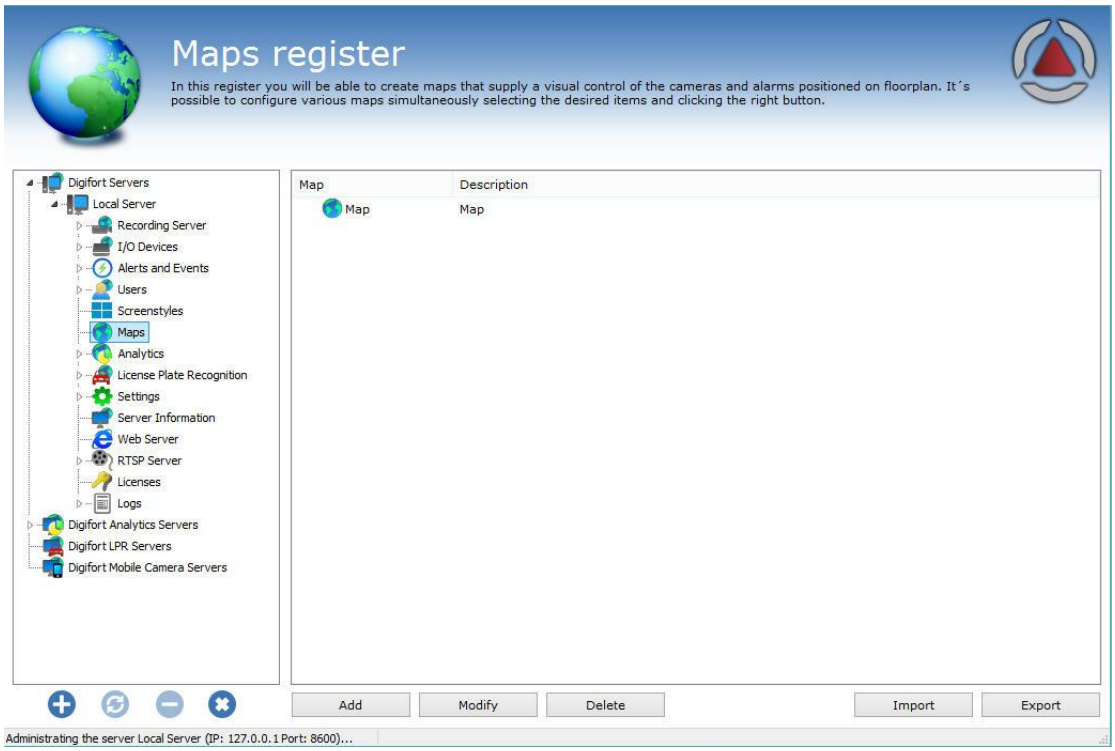
12.1 Registration of Maps

To register a map, click on the item Maps in the Settings Menu, as shown in the figure below:

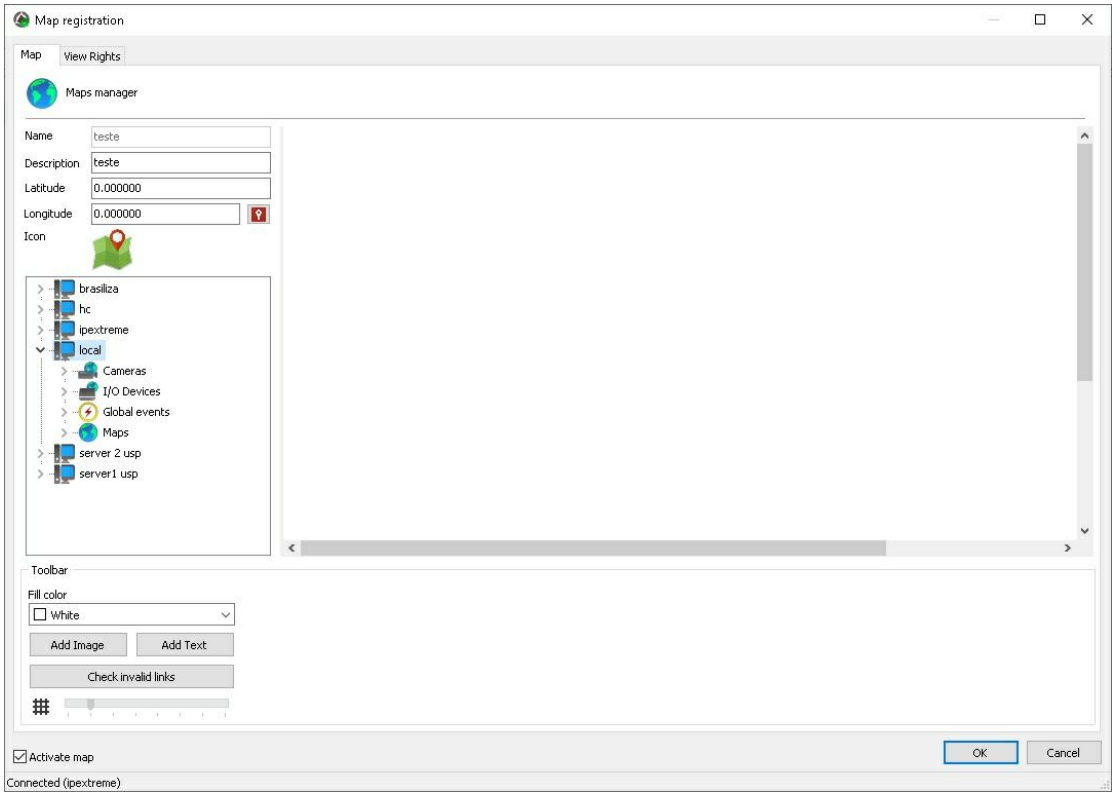


After that, the system maps registration screen on the right side will open, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



Click **Add** to open the Map settings screen, as shown below:



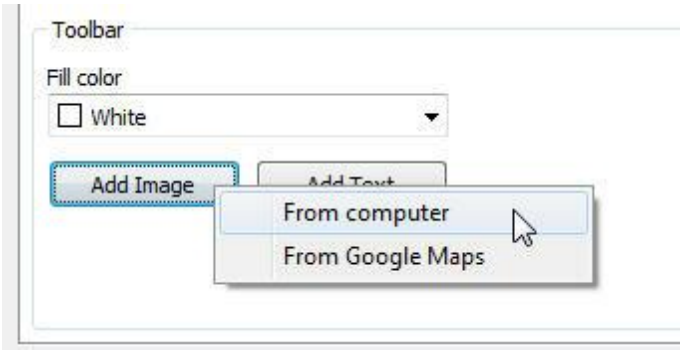
© 2002 - 2020 by Digifort, all rights reserved

This screen allows objects of different servers to be present on the same map. You can connect to one or more servers on the list on the right of the screen. See How to connect to a server to manage. The servers on the list are the same ones that are registered in Digifort Servers on the main Administration client list.

Start by informing a **Name** and a **Description** for your map.
Make sure that the **Activate Map** option is checked for your map.

12.1.1 Adding Images

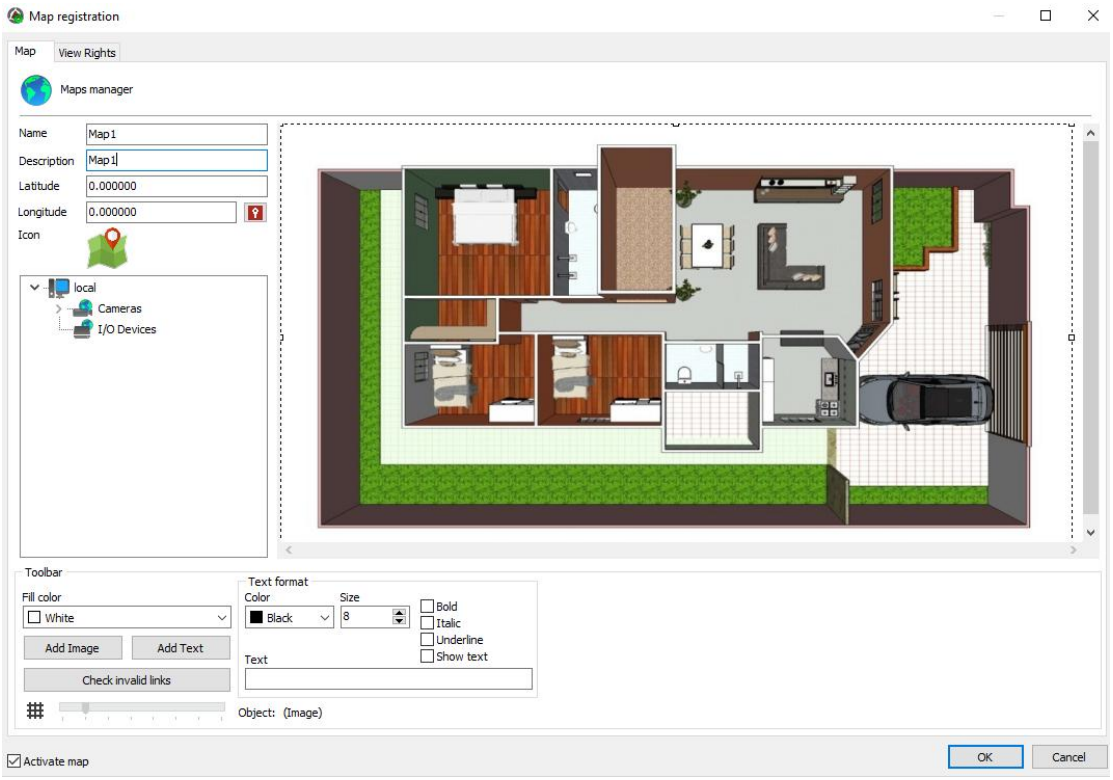
Click **Add Image** to locate the desired picture to your map and choose **From computer**, as shown in the picture below:



The system supports images in the formats *.jpg, *.jpeg, *.bmp, *.wmf, *.png and *.gif.

After choosing the image, it appears on the center screen, as shown in the figure below:

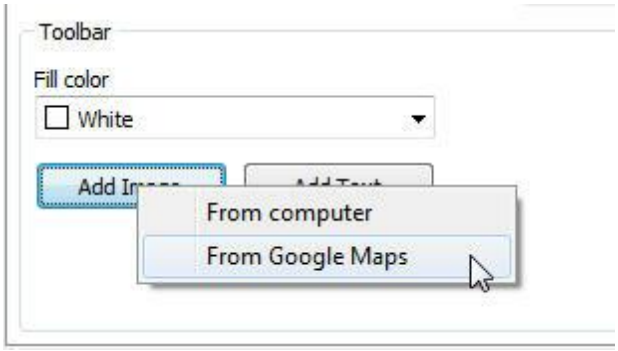
© 2002 - 2020 by Digifort, all rights reserved



12.1.2 Google Maps integration

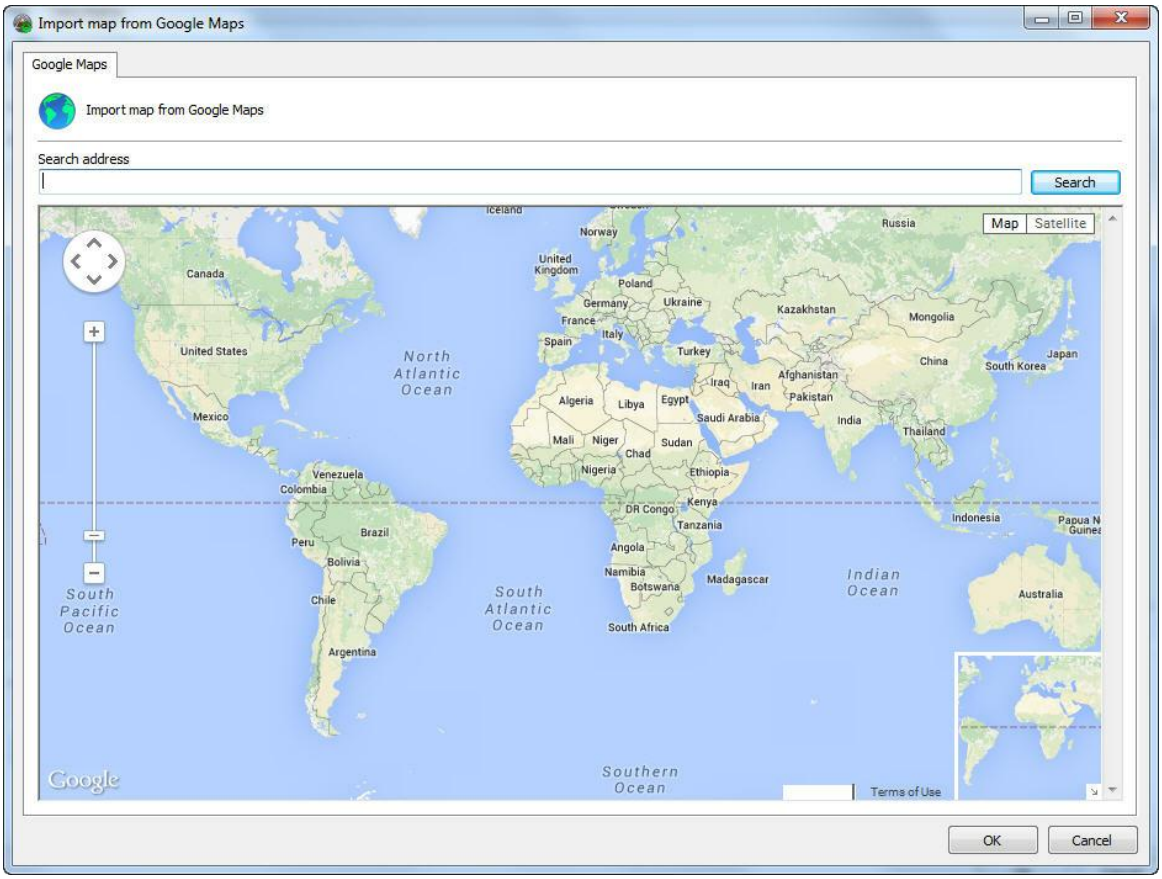
For ease, the Maps screen allows a photo to be taken directly from Google Maps.

Click **Add Image** and then later click **From Google Maps**, as shown in the image below:



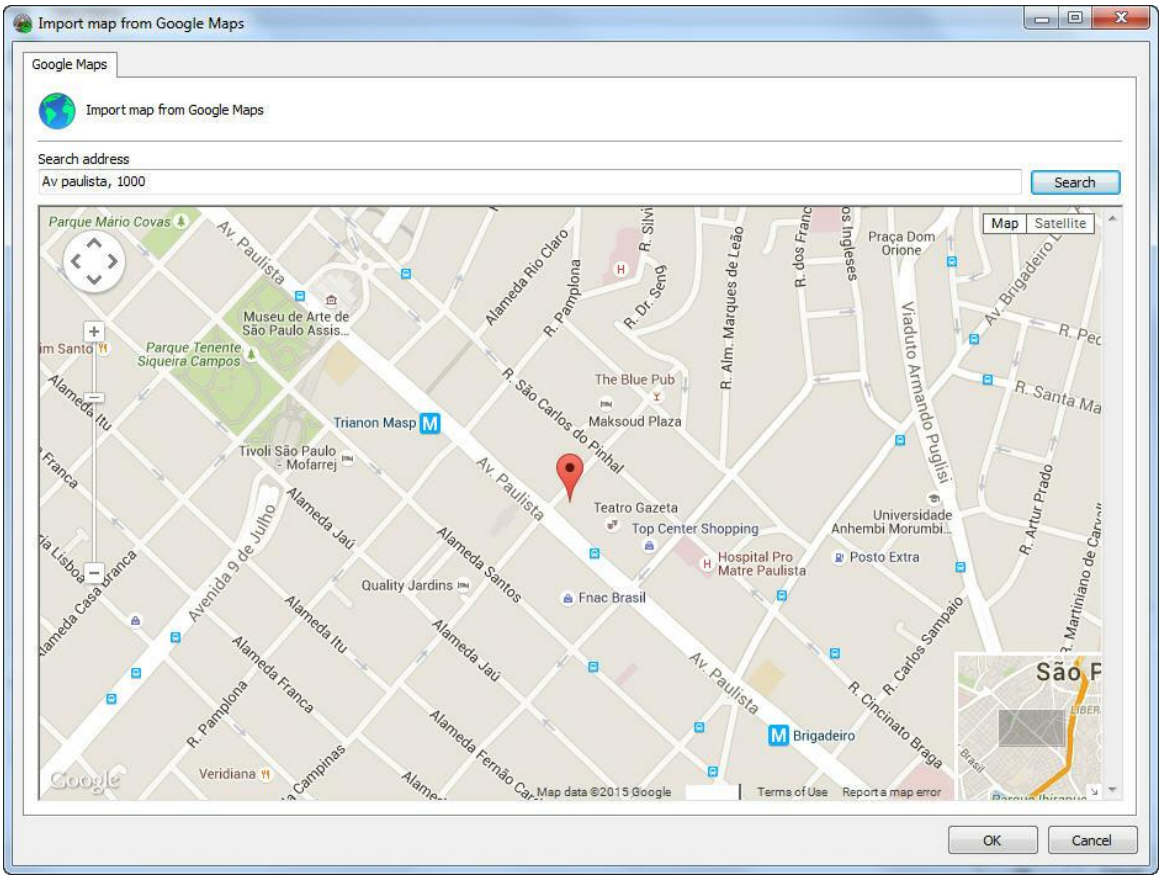
A screen will open with Google maps. **Note**: This feature requires an Internet connection.

© 2002 - 2020 by Digifort, all rights reserved



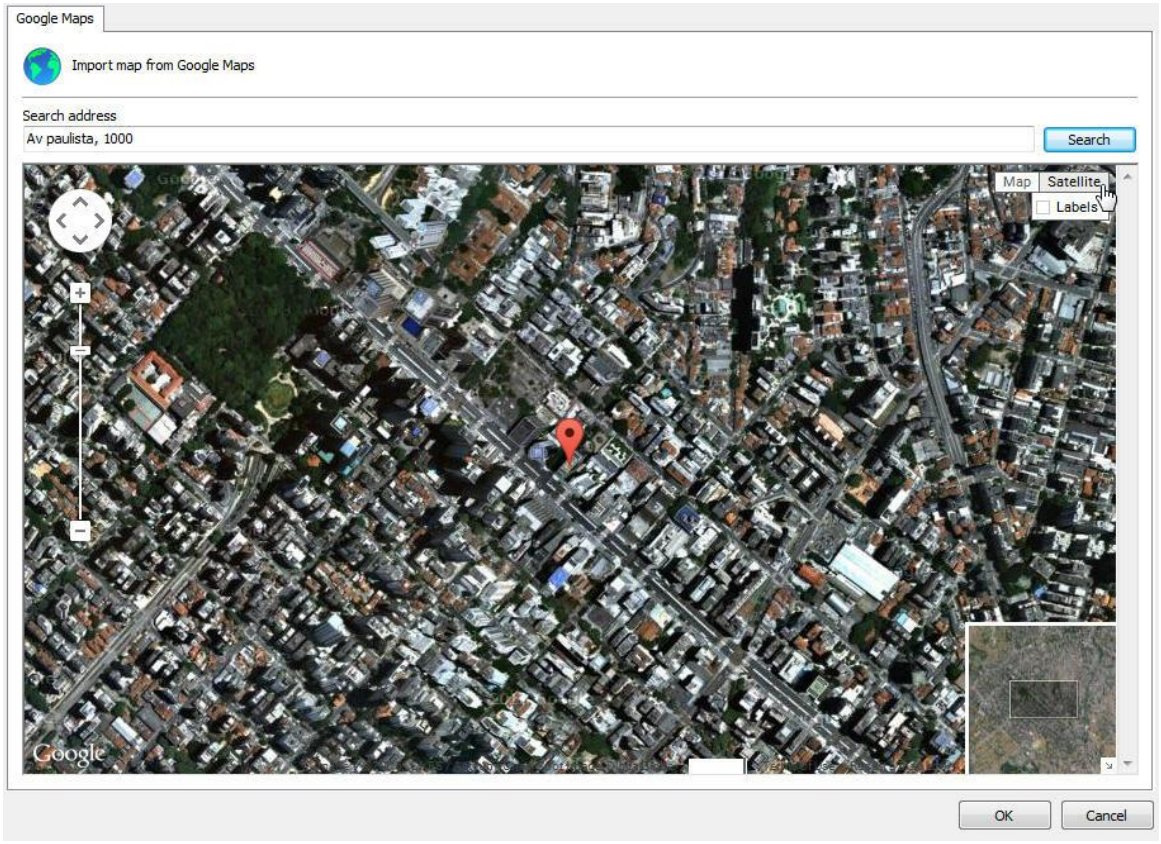
The navigation can be done with the mouse or an address can be entered directly in the **Search Address** field:

© 2002 - 2020 by Digifort, all rights reserved



By the address, the system will query the map on Google Maps, which allows both the map display as satellite photos:

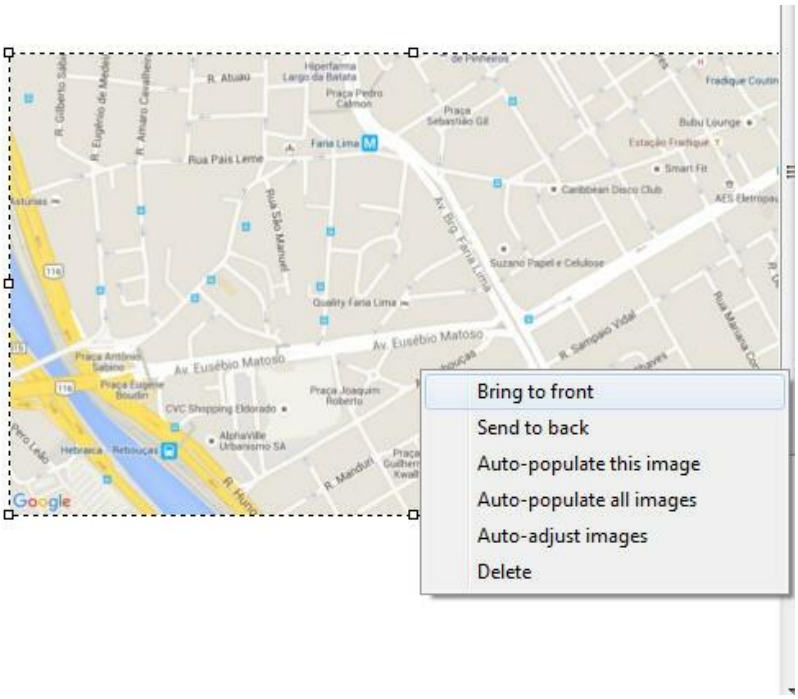
© 2002 - 2020 by Digifort, all rights reserved



When choosing the desired position, simply click **OK** and the current location will be used as a background image for your map.

You can add more than one image to the map, by simply clicking **Add Image** followed by **Do Google Maps** again. This option enables the creation of larger maps composed of multiple Google images. Digifort allows self-adjusting images based on your location to facilitate the organization and image merging.
By right clicking on top of an image the following options are available:

© 2002 - 2020 by Digifort, all rights reserved



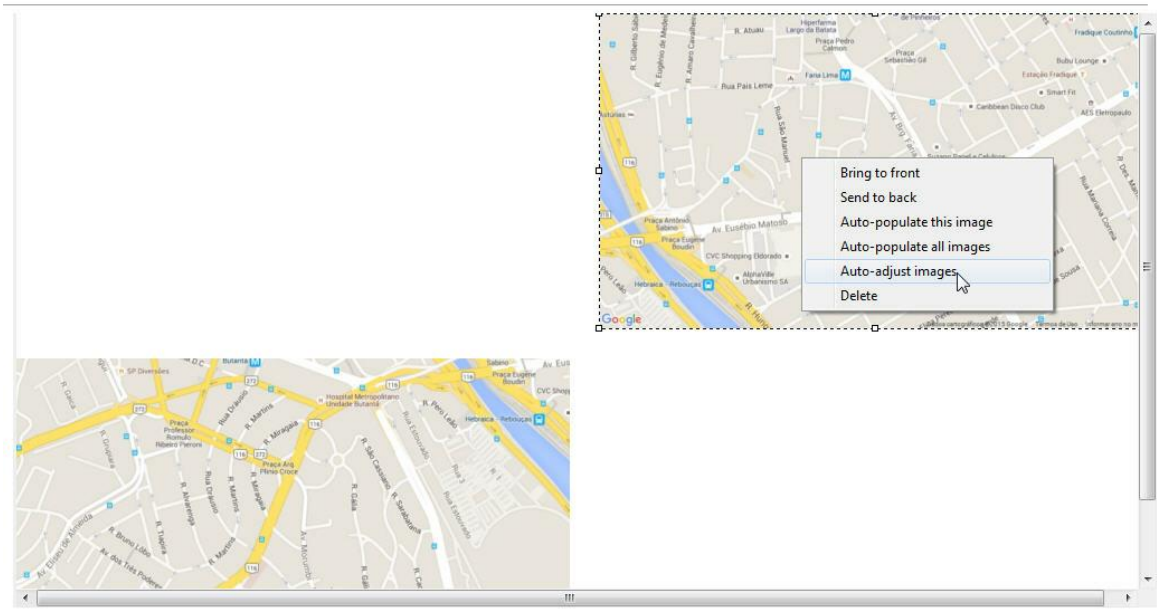
- **Bring Forward:** Move the selected image over the other pictures on the map..
- **Bring back:** Move the selected picture under the other images on the map.
- **Auto-populate this image**: From the longitude and latitude configuration registered in cameras, Digifort will automatically position the cameras in the selected image that has the same coordinates. See section Adding a camera to learn how to register cameras coordinates.

- **Auto-populate all pictures:** From the longitude and latitude configuration registered in cameras, Digifort will automatically position the cameras in all Google Maps images that has the same coordinates. See section Adding a camera to learn how to register cameras coordinates.

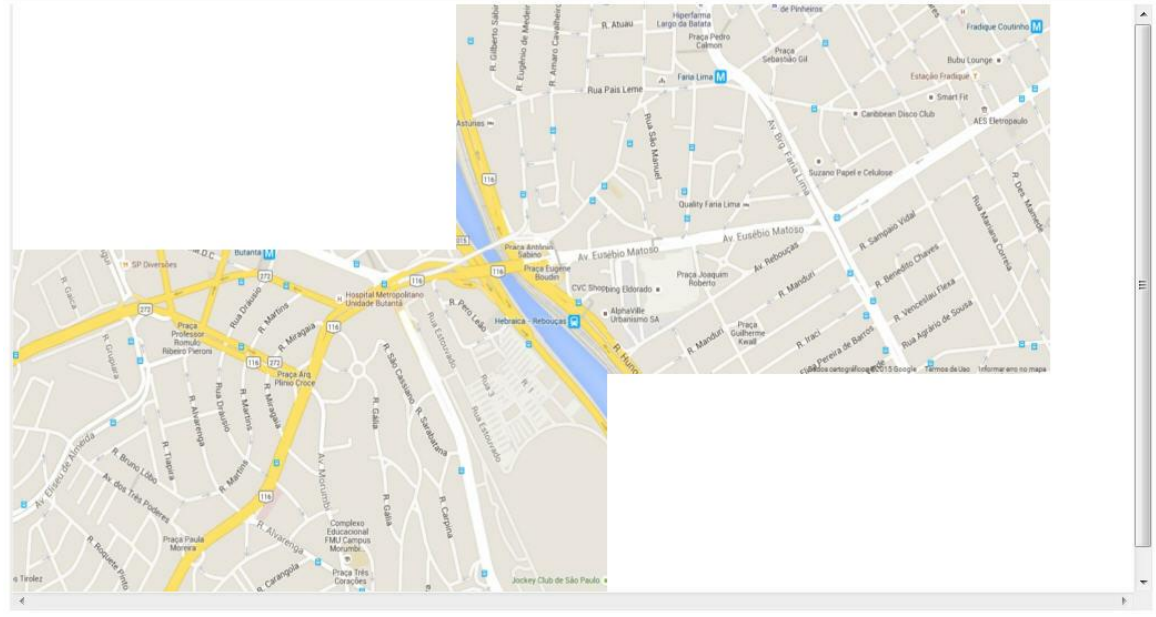
- **Self-Adjusting images**: This option allows Digifort to self-organize images from Google based on its coordinates, thus facilitating this work to be done manually when more than one image is needed to create a larger map. See examples:

Two separate images:

© 2002 - 2020 by Digifort, all rights reserved

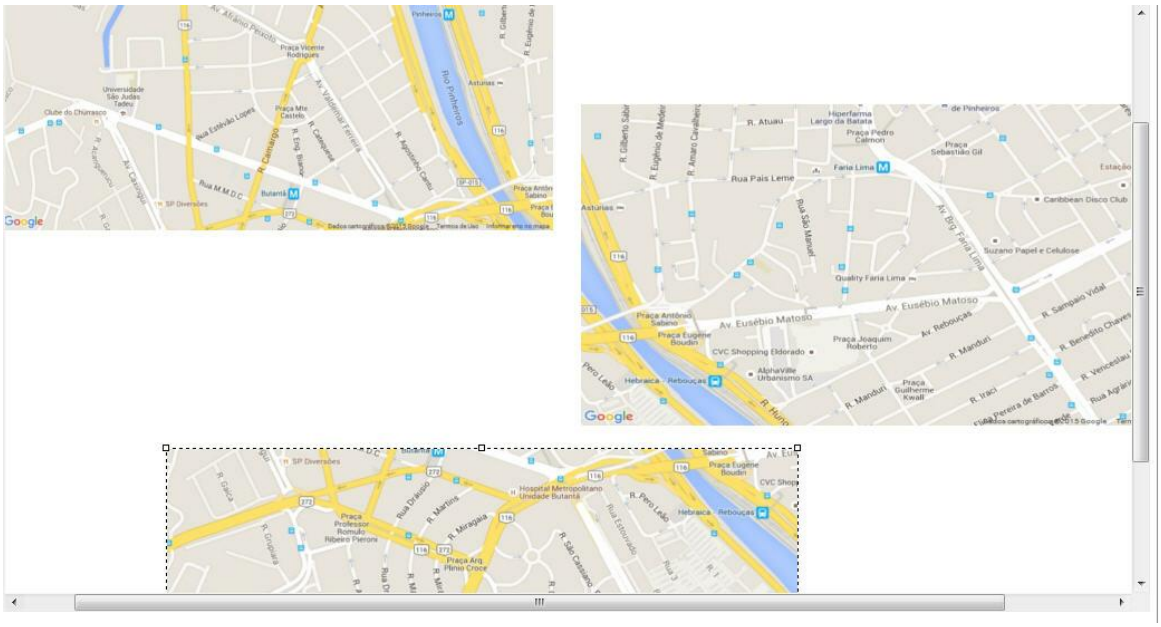


After the self-adjust command:

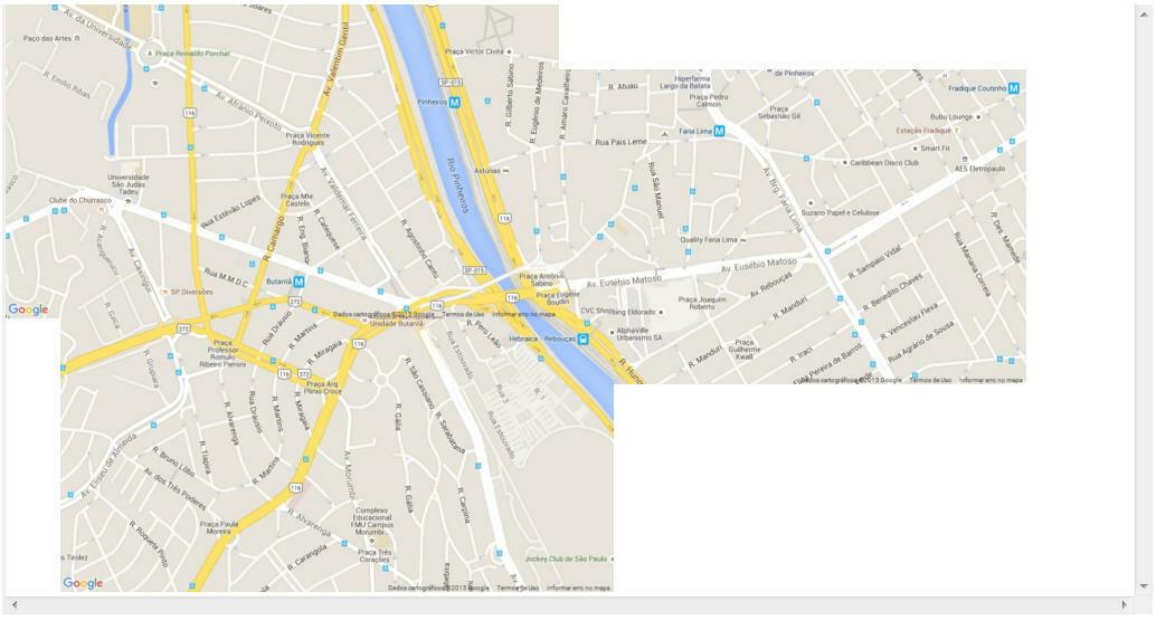


3 separate images:

© 2002 - 2020 by Digifort, all rights reserved



After the self-adjust command:



NOTE: The auto-tuning takes into account the size of selected image, therefore the remaining images will be resized based on the selected image.

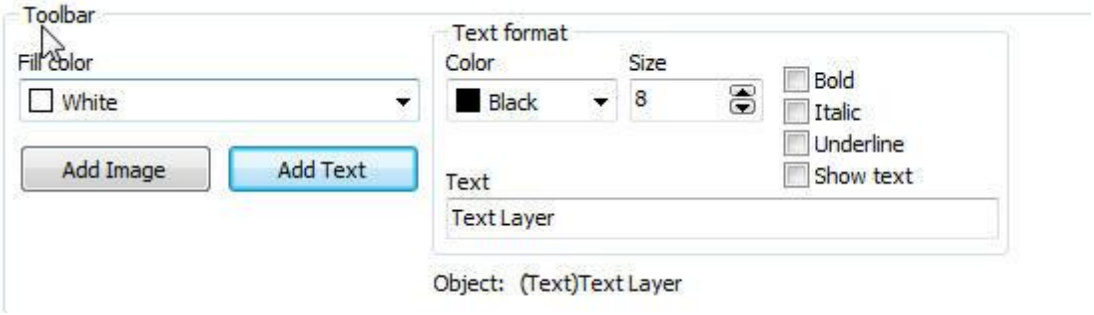
© 2002 - 2020 by Digifort, all rights reserved

12.1.3 Adding Texts

In the **Add Text** button, subtitles can be added to the map. Once created, you can edit your text and its font. Just select it and change the text formatting properties found in the bottom of the screen.

These options are valid for any map text object:

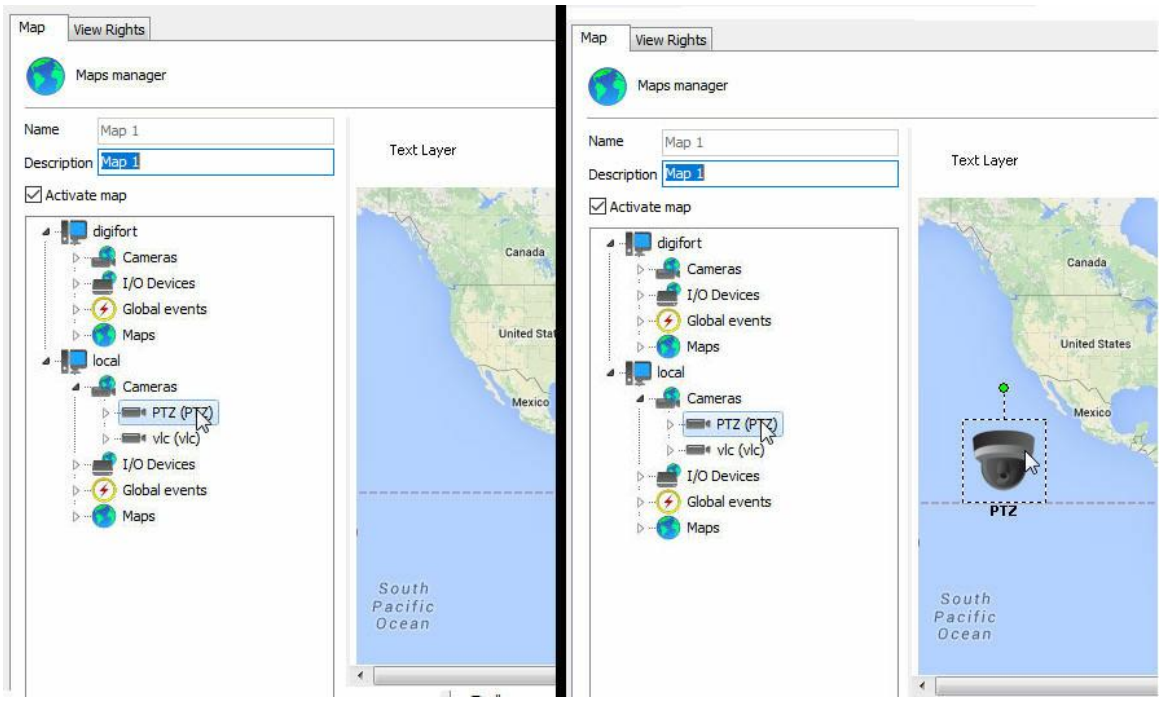
- **Color**: It changes the text color.
- **Size**: It changes the text size.
- **Text**: It changes the caption text.
- **Bold**: It turns the text bold.
- **Italics**: It turns the text italics.
- **Underlined**: It underlines the text.
- **Show Text**: It shows text or not in an object.



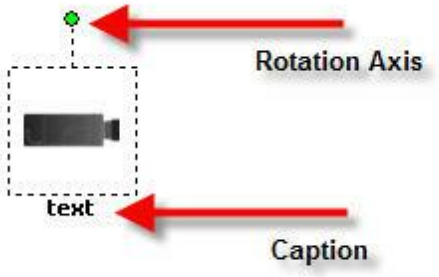
12.1.4 Adding Cameras

To position objects on the map, just drag them from the positioned list on the left of the screen, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



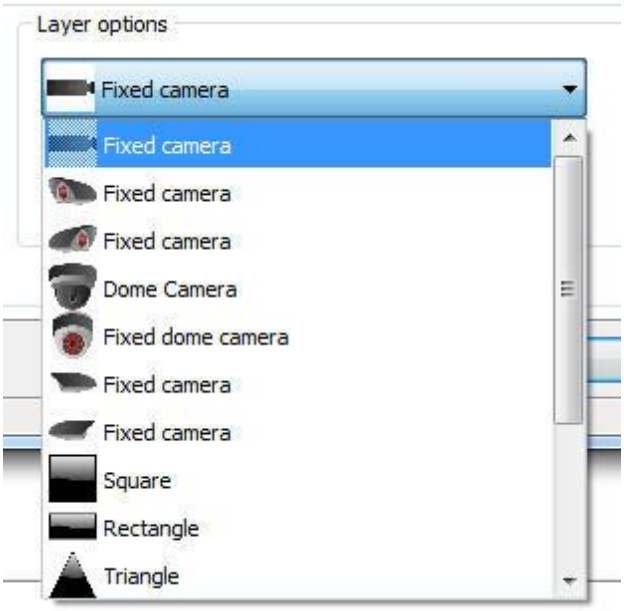
On the list of cameras located on the left, drag the desired camera to the map. It will take the shape of a camera on the map, as shown below:
To move it on the map, just click on its icon and drag it to the desired location.



The camera can be rotated by the rotation axis shown in the figure, just click on it and move the mouse cursor.

You can change the camera icon; select it and on the Options menu of the layer choose the desired icon, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



There is also the option of changing the icons size and color. In the Options menu of the layer, locate the **Size** and **Color** boxes shown in the figure and change the values by clicking on them.



12.1.4.1 Field of View of Cameras

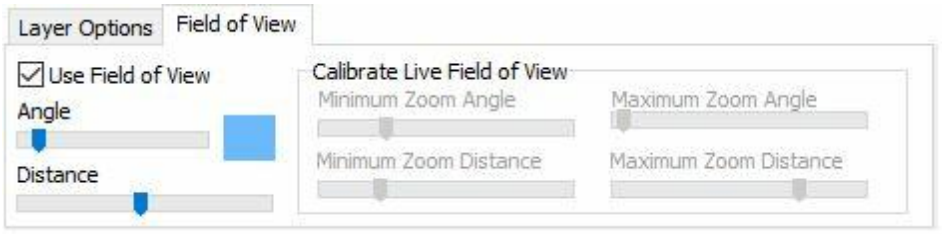
The synoptic map system now allows the display of the visual representation of the camera's field of view.
You can configure the field of view for any camera on the synoptic map.

The field of view feature is only available for Synoptic Maps and it is not available for Operational Maps.

Use the buttons to position the camera according to its desired starting position and then point the icon on the map according to the camera's starting position and click on the "**Save Starting Position**" button.

Furthermore, you can calibrate the camera's field of view. Simply select the "Field of View" tab and adjust the values accordingly:

© 2002 - 2020 by Digifort, all rights reserved



The available options are:

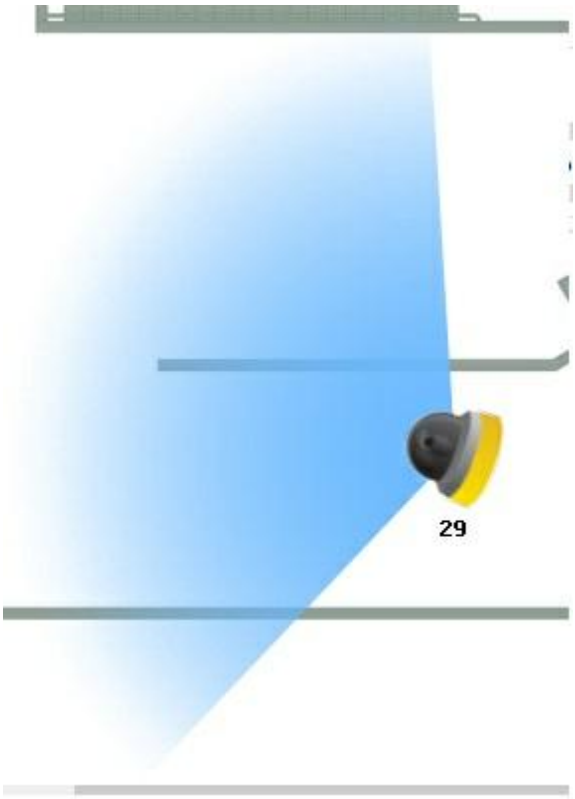
- **Angle**: the larger the opening angle, the “wider” the field of view.
- **Distance**: the greater the configured distance, the longer the marking on the map.
- **Color**: by clicking on the blue square, you can choose another color for marking the field of view.

Within the calibration of the field of view, we have the options:

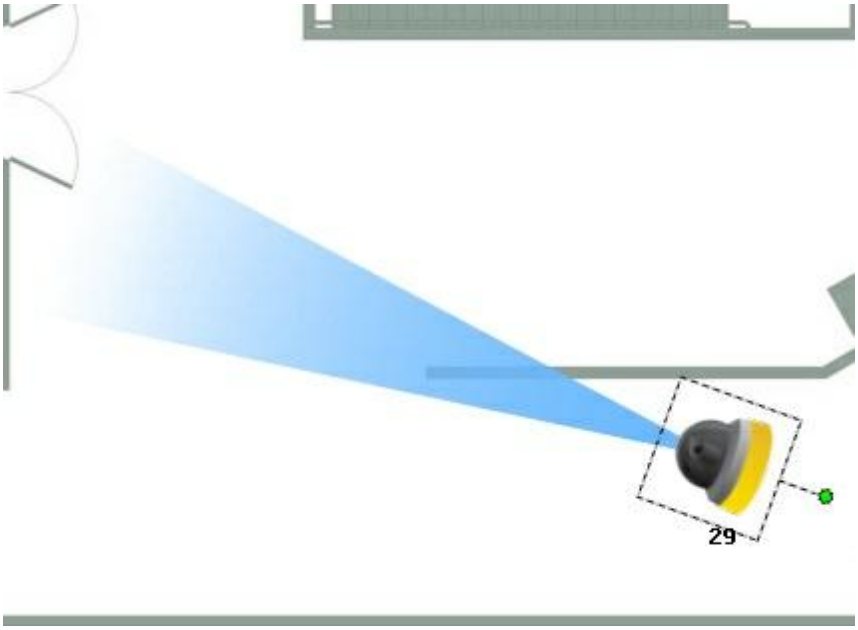
- **Angle with minimum zoom**: which is the camera’s field of view when the zoom is as low as possible.
- **Distance with minimum zoom**: it is how far it is possible to see with the camera in its minimum zoom.
- **Angle with maximum zoom**: which is the camera’s field of view when the zoom is as high as possible.
- **Distance with maximum zoom**: it is how far it is possible to see with the camera in its maximum zoom.

An example of a camera with a maximum and a minimum zoom is below:

© 2002 - 2020 by Digifort, all rights reserved



Camera with minimum zoom, having a wider field of view and shorter distance.



Camera with maximum zoom, having a narrower field of view and greater distance.

It is not necessary to save the field of view again after calibrating the starting position, as the starting position is independent of the field of view.

© 2002 - 2020 by Digifort, all rights reserved

The live feedback feature is only available for cameras having the integrated PTZ driver. Check the models having integrated PTZ on the Digifort site.

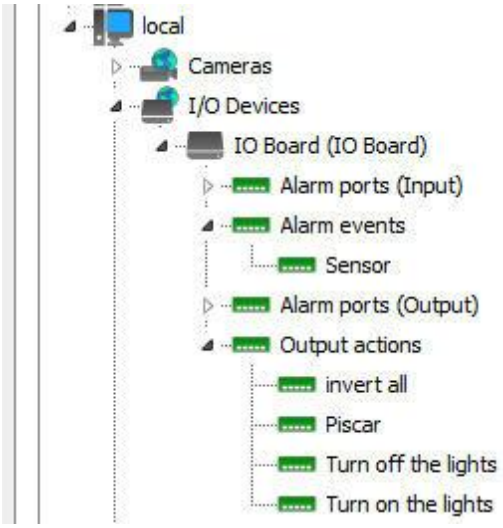
To see this new feature in action, visit the videos available on our YouTube channel: http://www.youtube.com/DigifortChannel

https://www.youtube.com/watch?v=pEwgc12a8zE&list=PLFlhAF6oQd_rJjV3wEWHB8f0ZuzruvrOS

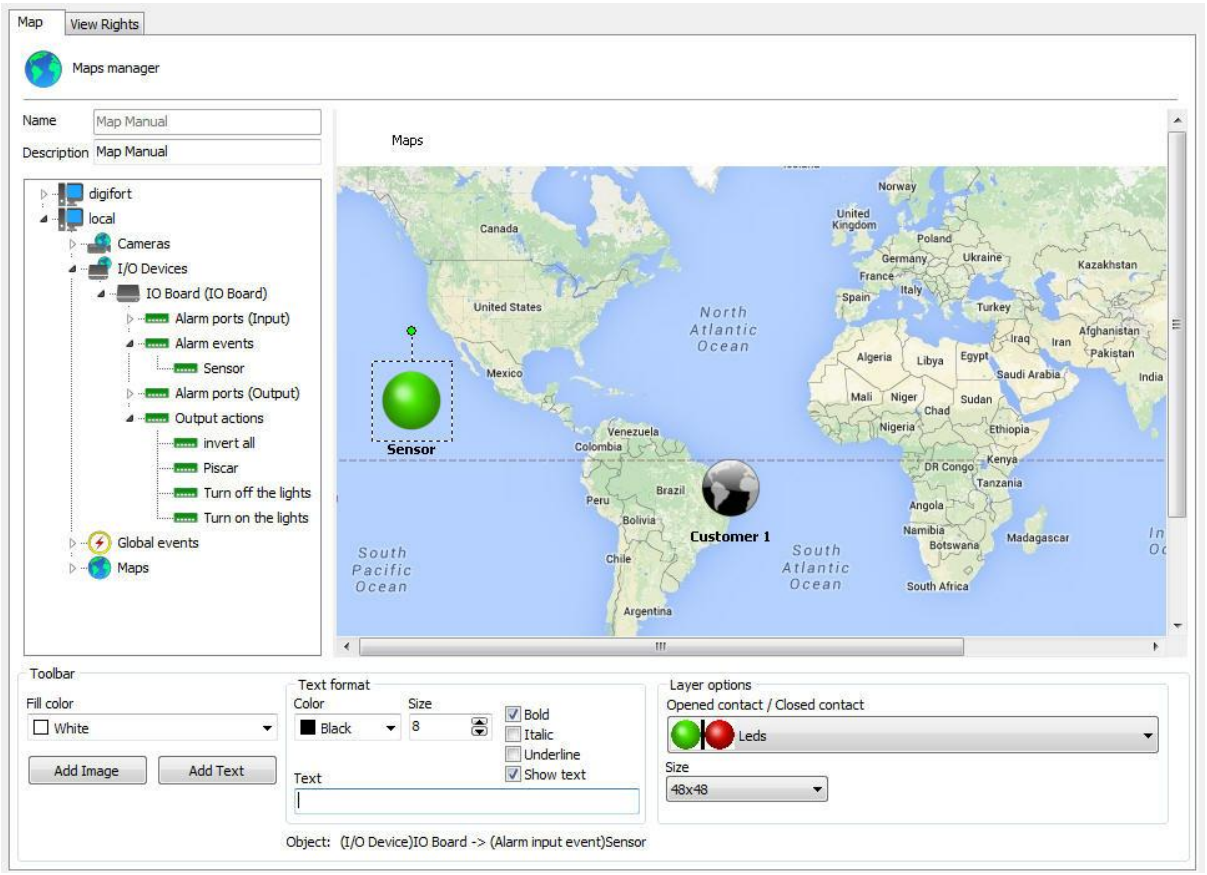
12.1.5 Adding Functions to the Alarm Board

With the events already configured on the alarm board, it's possible to add them for rapid access by way of the map. To learn how to configure events of the board, see How to configure the I/O.

To add the events simply drag them from the list at the right of the screen to the map as shown in Figures bellow:



© 2002 - 2020 by Digifort, all rights reserved



The icon of events and their respective sizes can be changed as well as those of cameras. Simply select the desired object and go to Layer options as figure bellow:



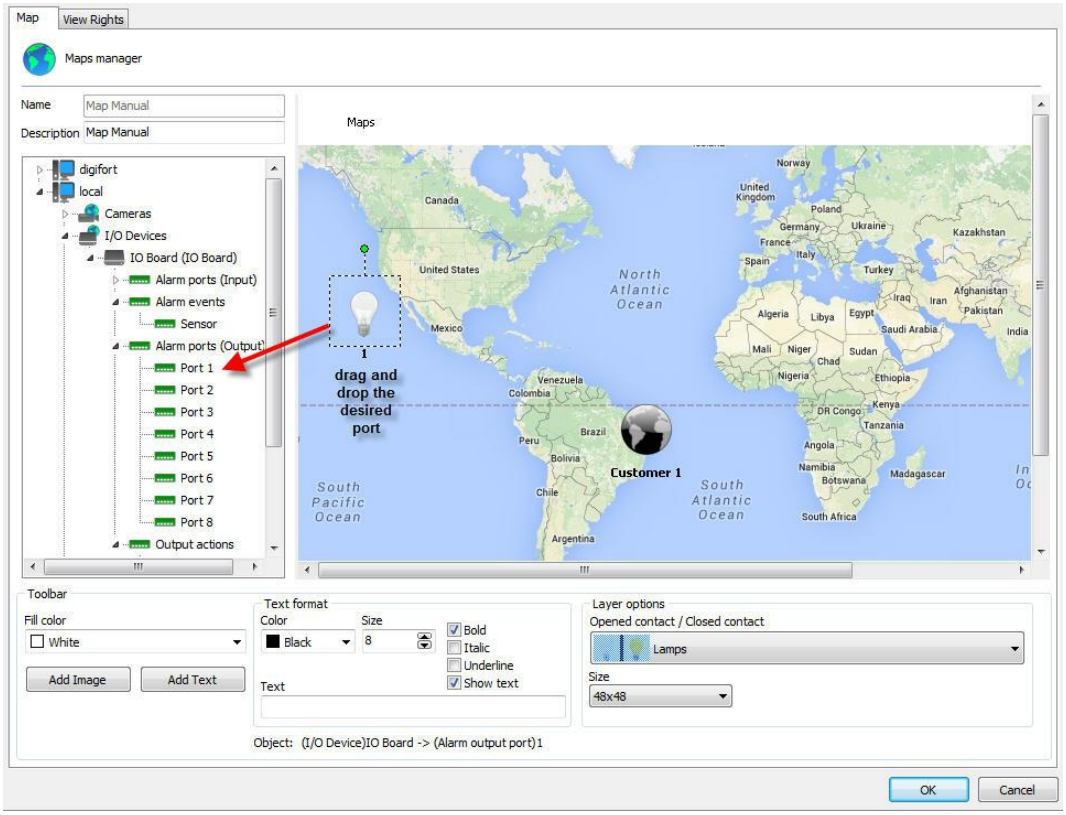
In the case of the figure 8.10, every time someone passes thought the outer fence, Digifort will be alerted and will inform the operator according to the pre-Programmed events. To learn about preProgrammed events, consult How to configure the I/O..

Let's now add an event with buttons. The buttons have the purpose of activating or disactivating an alarm board output via Digifort. To learn how to make events with buttons, consult How to configure the alarm actions

First, drag the port to the map on which the device will be activated is found as shown in

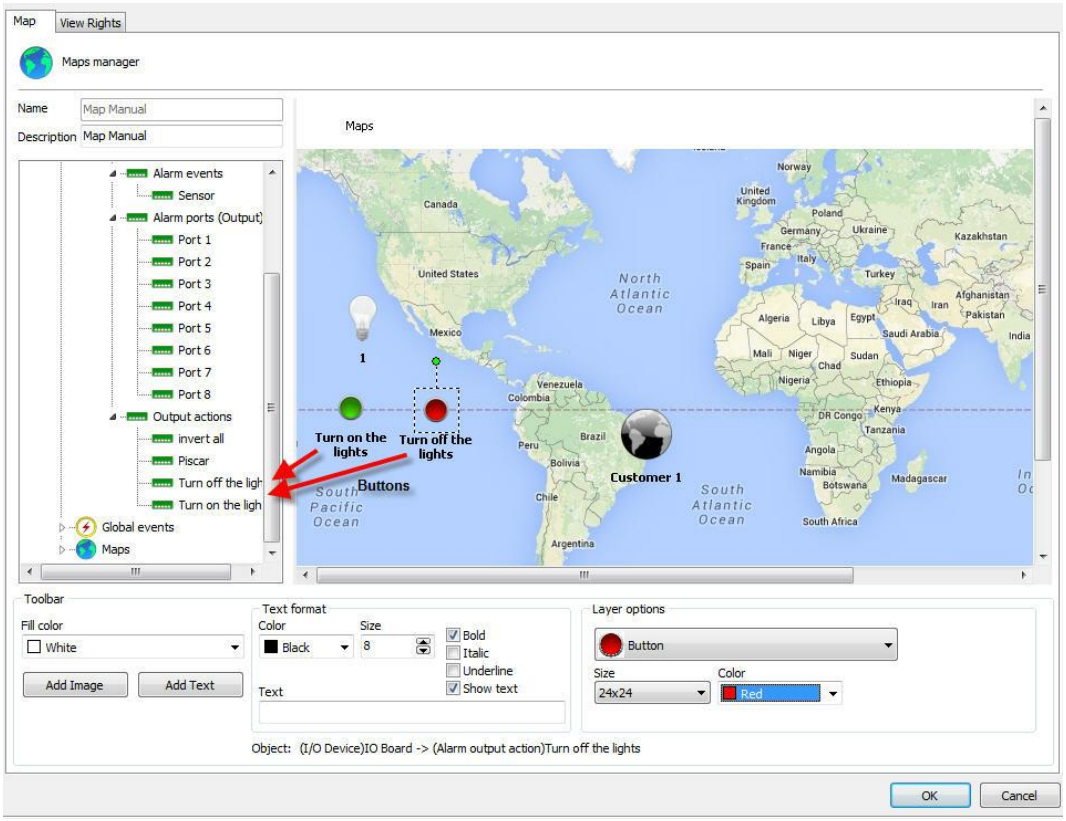
© 2002 - 2020 by Digifort, all rights reserved

Figure bellow:



Now drag the Pre-Programmed buttons to the chosen port as shown in Figure bellow:

© 2002 - 2020 by Digifort, all rights reserved

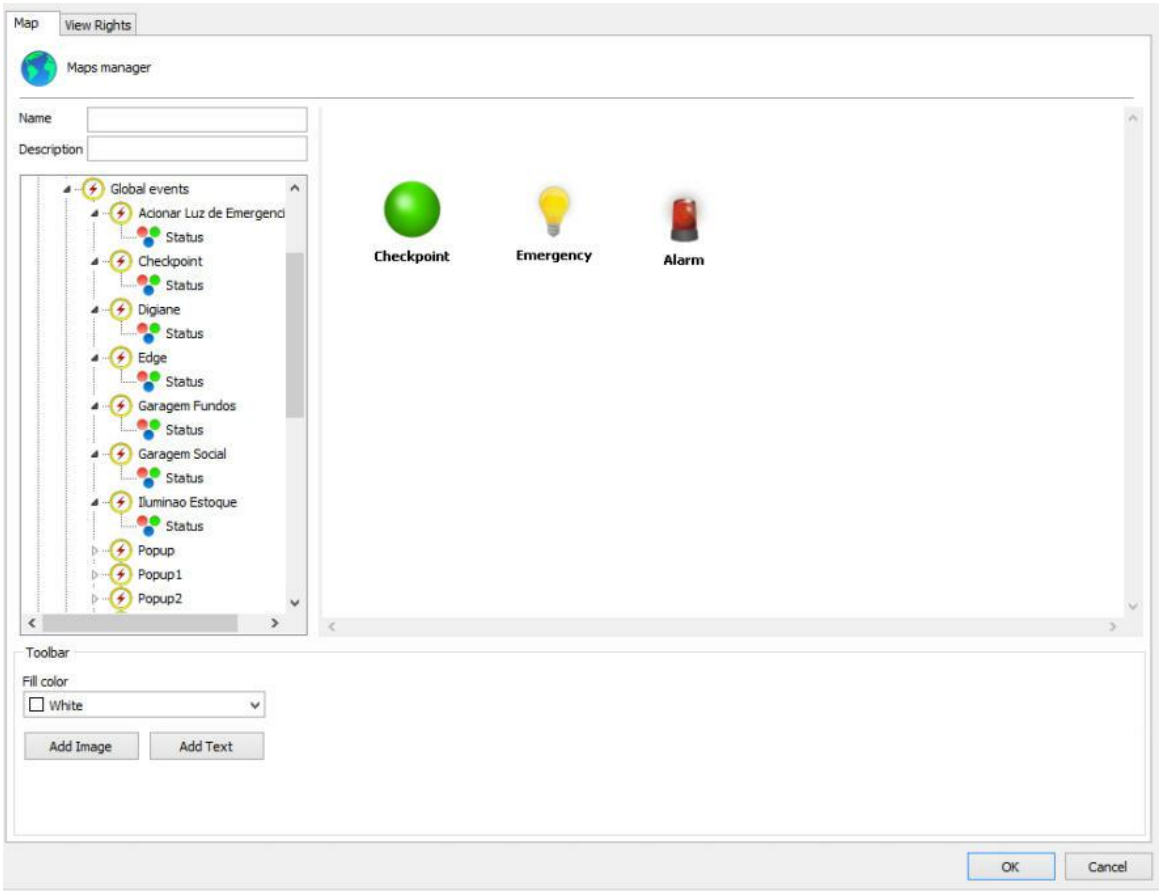


Done! When the map is opened in the Surveillance Client, the alarms will be ready to be activated by the map. To learn how to use the maps in the Surveillance Client, consult its manual.

12.1.6 Monitoring global and manual events

The map system allows real-time display of the Global Events and Manual Events status. With this feature, when a Global Event or Manual Event associated with the map are triggered, the alarm icon will be animated in the Surveillance Client, notifying the operator about the event:

© 2002 - 2020 by Digifort, all rights reserved



To see the events status in the Surveillance Client, simply drag the global/manual event Status object to the map, as in the previous image;

12.1.7 Status de objetos

The device status identifier in the synoptic maps has now been changed to reflect the current recording state.



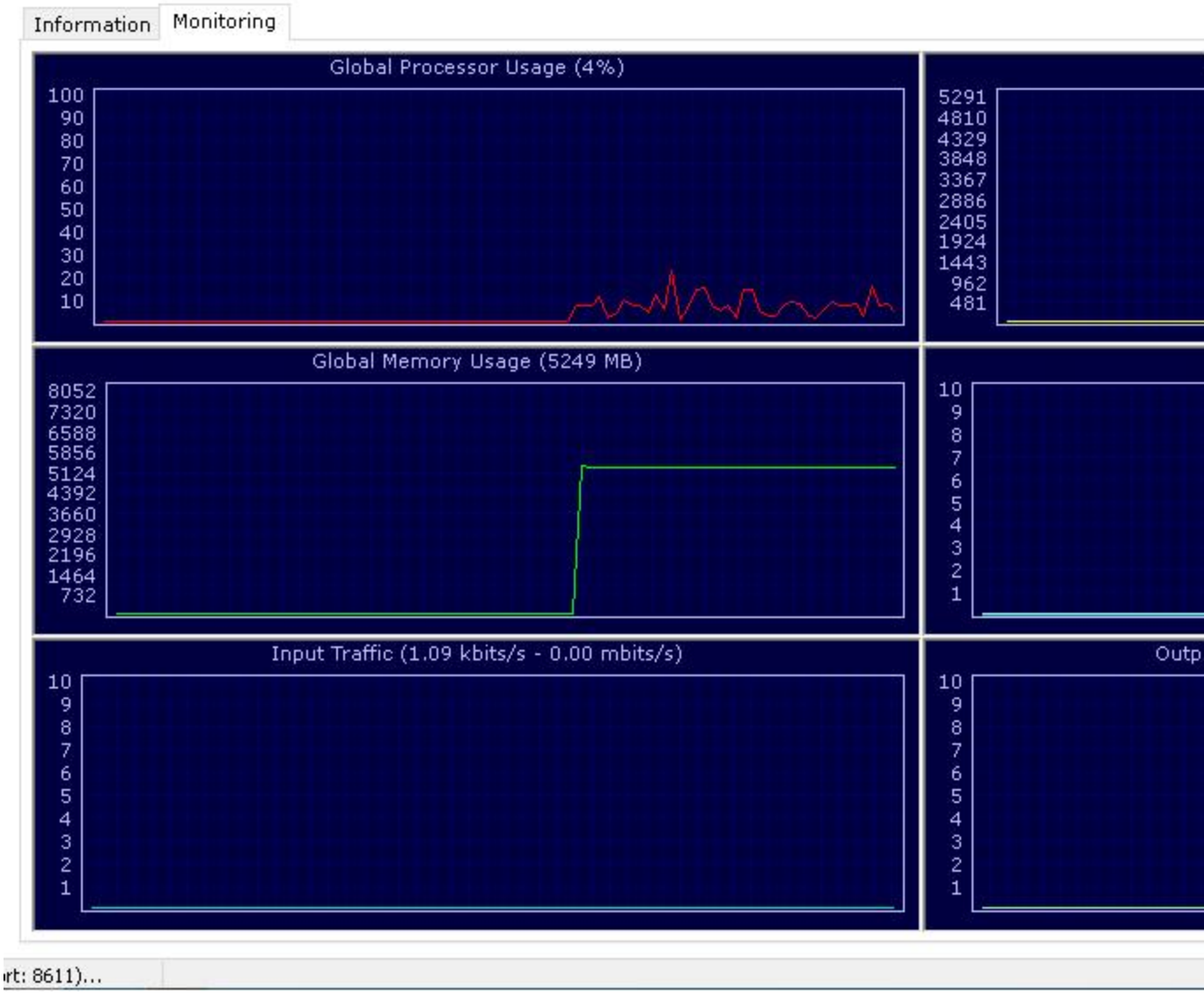
- Identifies that the device is working and is currently writing to disk
- Identifies that the device is working but is not currently writing to disk
- Identifies that the device is out of order

The absence of a status identifier indicates that the device is disabled.

© 2002 - 2020 by Digifort, all rights reserved

12.1.7.1 Monitoring

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

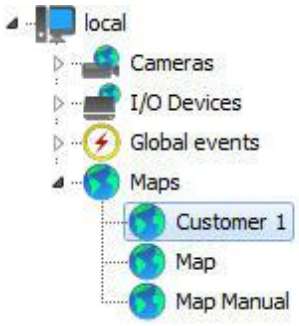


12.1.8 Map Links

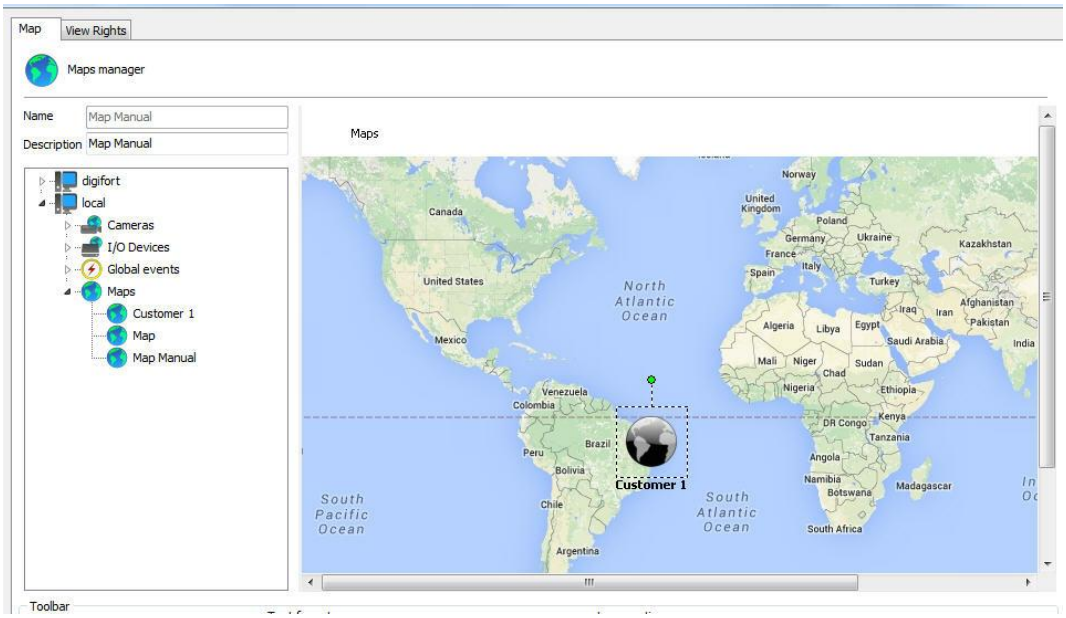
The link to maps is a resource for improving the maps management. Within a map created, you can create links to other maps, thus facilitating navigation among them.

To create links, you must have registered two or more maps; when there are more than one registered map, in addition to the one being used, they will appear in the maps list, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



Click and drag the object to the map, as shown below:



And that is it! When you open the map in the Surveillance Client, the icon on the screen already calls the next map.

Do not forget to put a link on the map that is called to go back to the main map, as shown in the figure below:

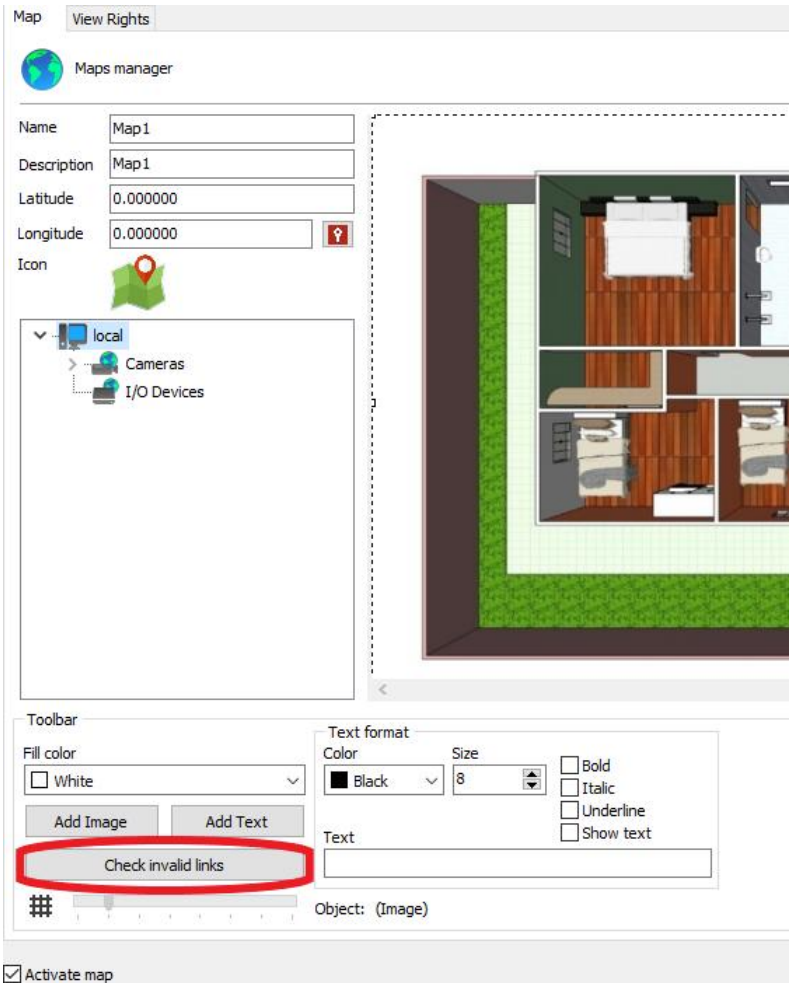
© 2002 - 2020 by Digifort, all rights reserved



12.1.9 Check invalid objects on maps

The map editing tool in the Administration Client allows you to check for invalid links on the map and tries to locate an object with the same name on another server to correct the link.
Links to objects on maps can be broken if the server password changes, in which case, checking links can correct all invalid links without having to position all objects again.

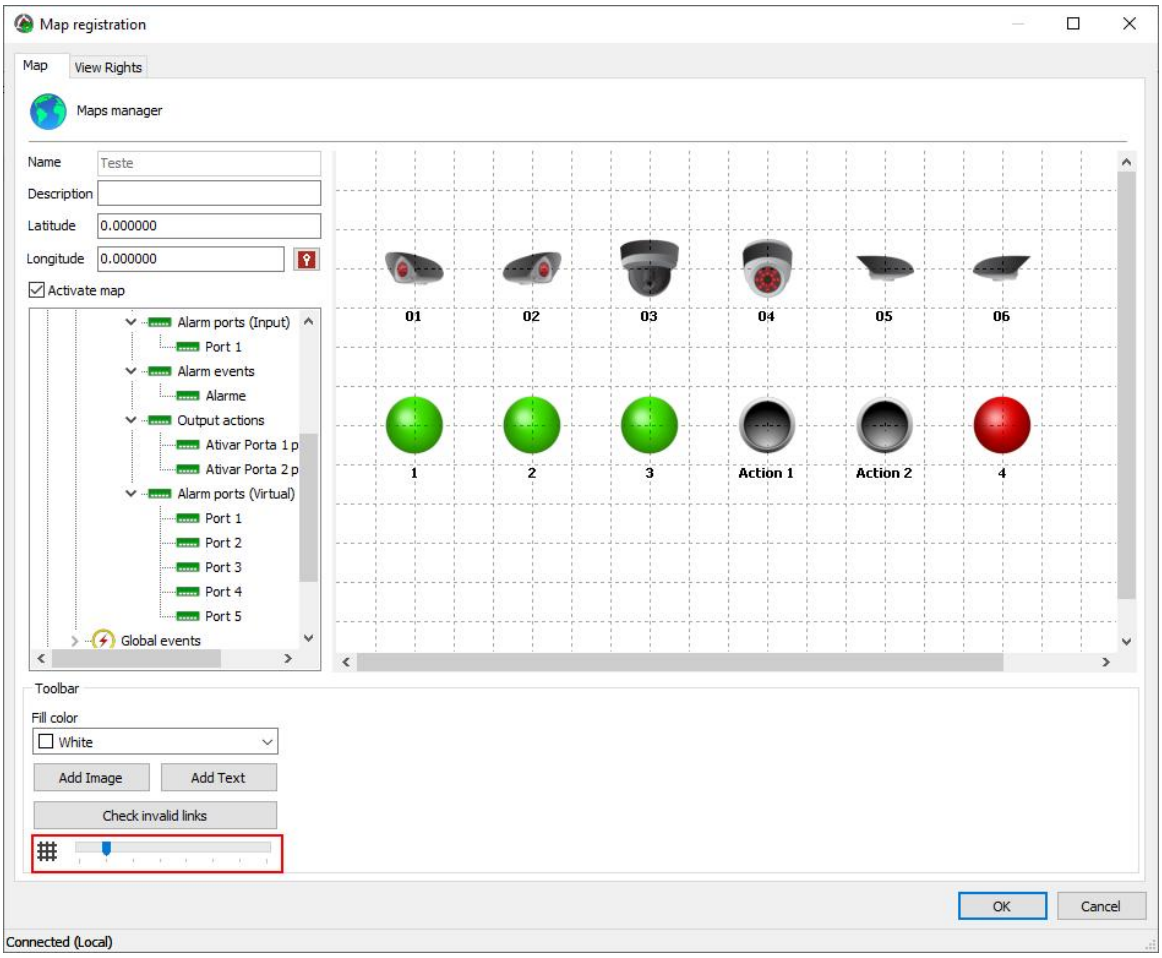
© 2002 - 2020 by Digifort, all rights reserved



12.1.10 Maps / Alignment grid

The maps creation tool also has an alignment grid for improved map design. The grid will only be displayed in the editor and can be adjusted by moving the slider denoted in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

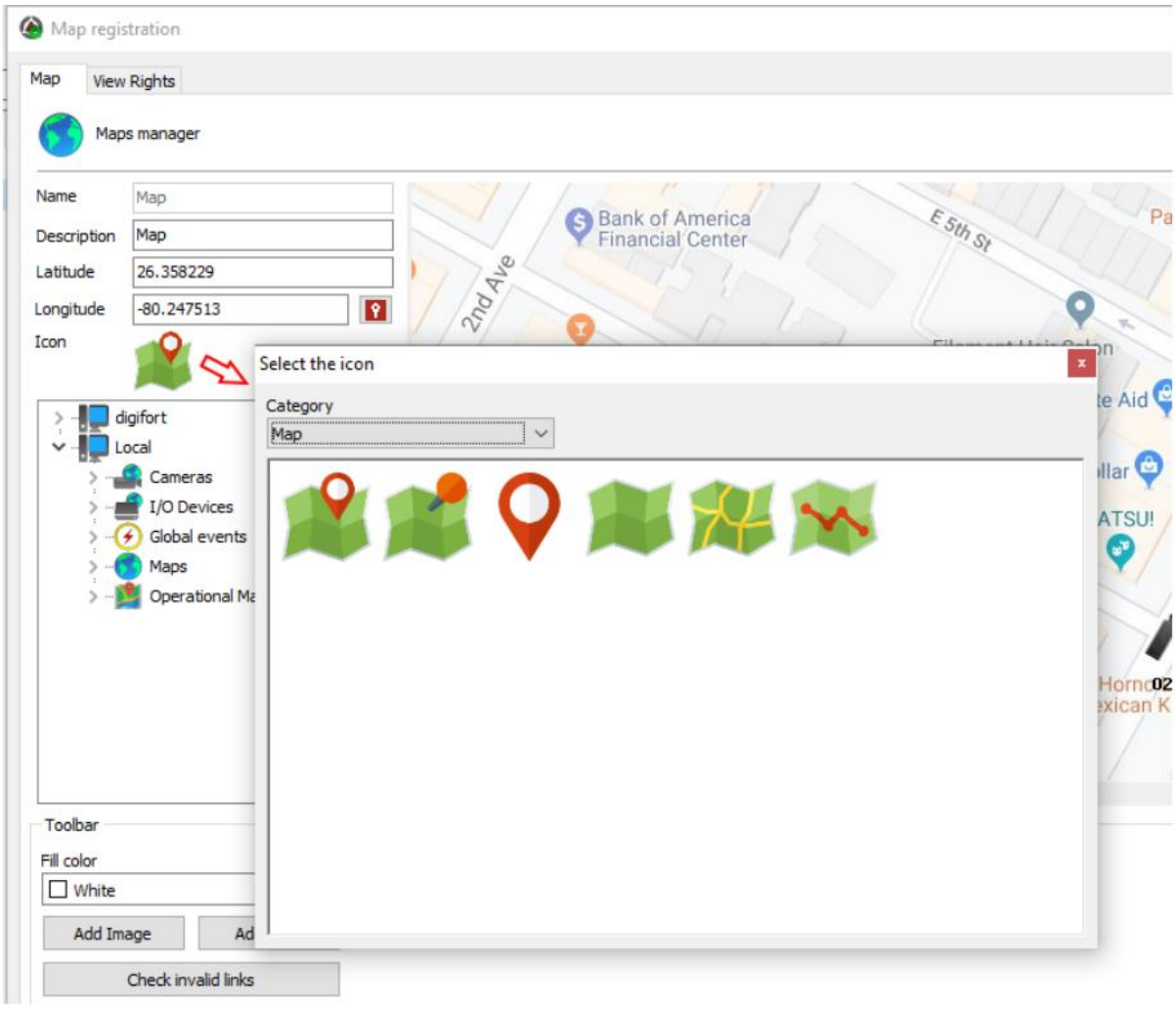


12.1.11 Operational Map Icon

On this screen it is possible to choose the icon that will represent your map within the Operational Map. To learn more, see the Operational Map chapter.

Just click on the camera image and choose the new image as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter XIII

13 Operational Map

The operational map features advanced applications within servers with multiple cameras, monitoring several areas, e.g., in a city.

This is a feature that, through the integration with Google Maps, allows the creation of navigation maps and event maps.

Navigation maps provide an overview using the geo-positioning of all system cameras (which have geo-positioning activated) and will allow access to these cameras through icons referenced on the map.
If the Surveillance Client is connected to multiple servers, the operational map will focus on and display the objects from all servers automatically.

Event maps provide, in real time, the position of the event (if it is geo-referenced) on the map when it occurs, creating a powerful visualization and navigation interface that provides a detailed view of the locations where the events are occurring, allowing the operator to access the cameras near the event, thus speeding up the response to the event.

The maps can be registered and configured to display a region of the globe automatically when placed on screen, thus allowing the creation of maps for different regions.

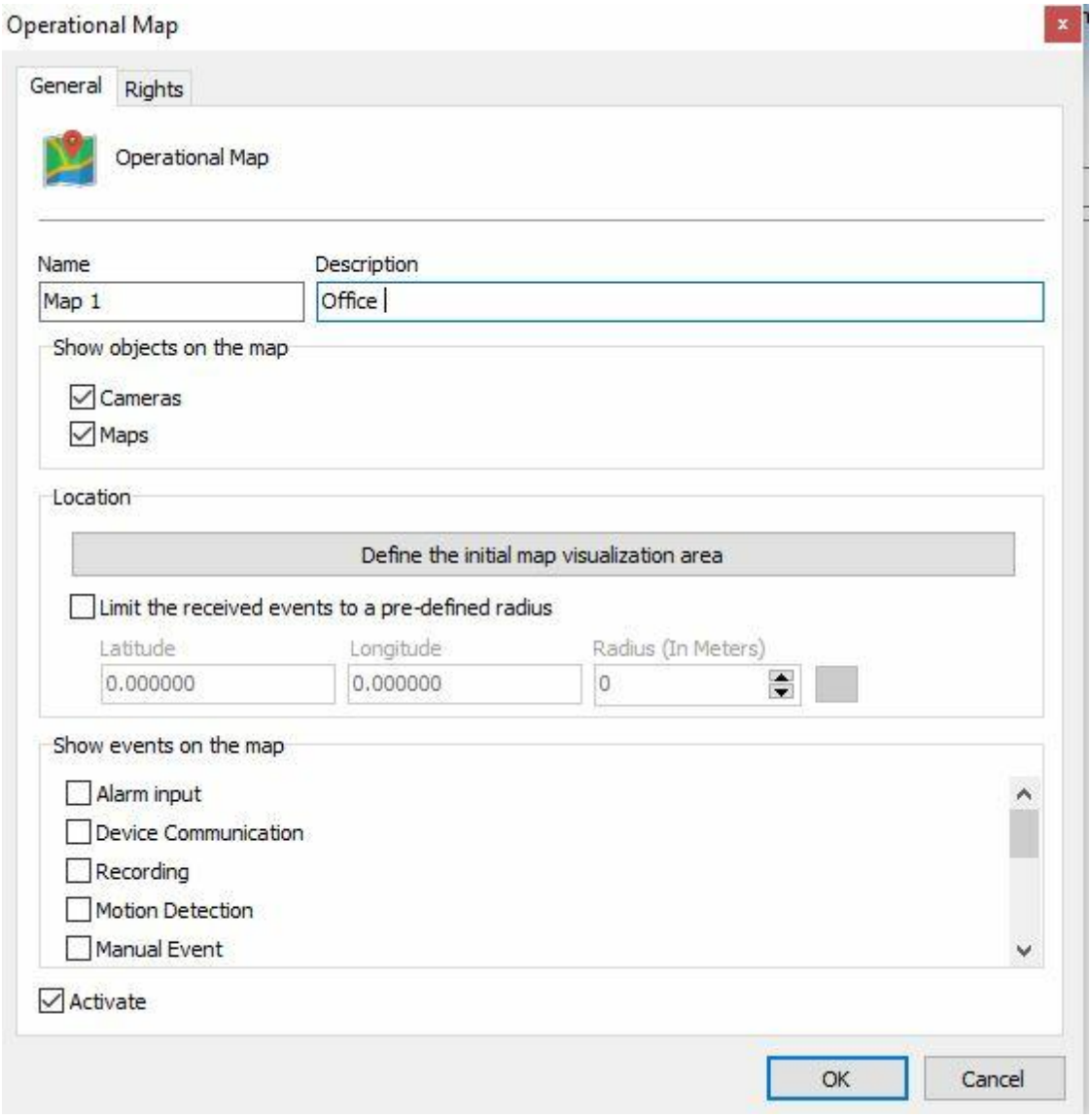
Event maps can also be configured to filter and display events only from some categories. Events can also be filtered by geo-location, i.e., only events from a specific region will be populated on the map.

To add Operational Maps to your Administration Client, search for the tab in your Digifort server:



© 2002 - 2020 by Digifort, all rights reserved

By clicking on Add, the following window should appear:

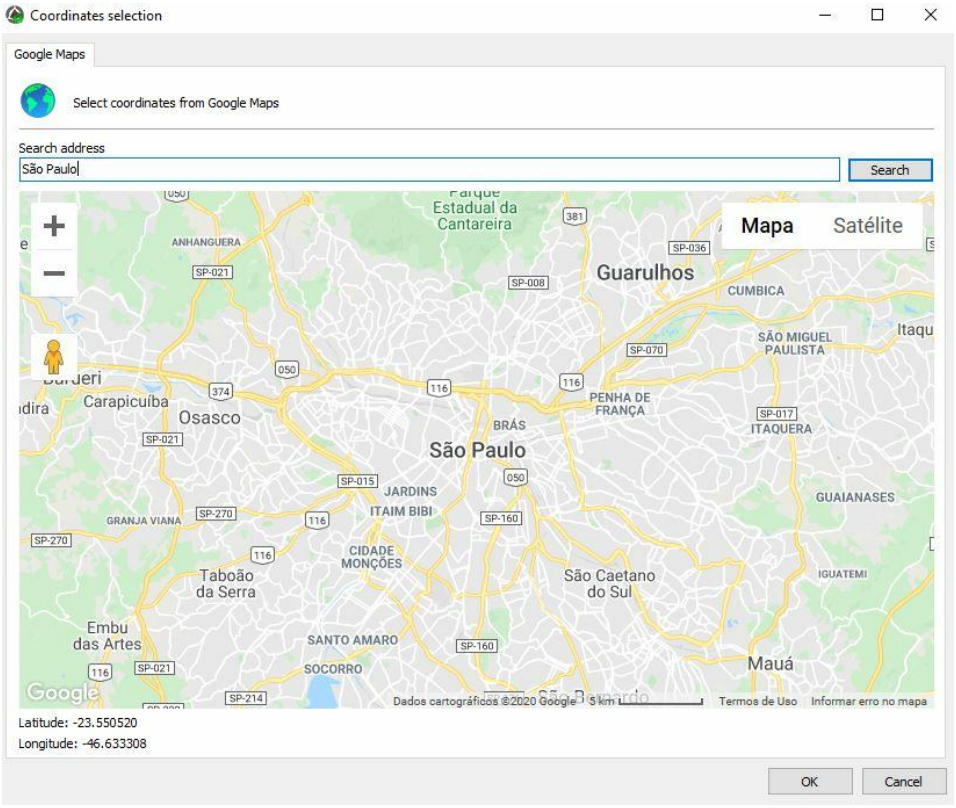


- **Name**: Name of your Operational Map.
- **Description**: Description of your Operational Map.
- **Display Objects on the Map:** It selects which objects should appear on the map, among Cameras and Internal Synoptic Maps.

Location

- It defines **the map's viewing area**: It defines the starting point for map display on the screen, e.g.:

© 2002 - 2020 by Digifort, all rights reserved

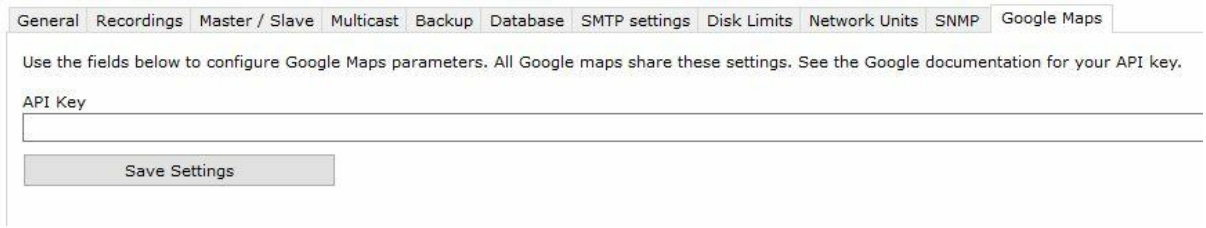


- **It limits the receipt of Events in a preset Radius**: It determines which area of the map, in Latitude, Longitude, and Radius, can trigger events on the Digifort Server.
- **Display Events on the Map:** It defines which events will be displayed on your operational map, among them:

  - Alarm input
  - Communication with devices
  - Recording failure
  - Motion detection
  - Manual event
  - Scheduled event
  - Global event
  - Analytics
  - Plate reading
  - Audio level detection
  - Server failover
  - Device events

To configure Google Map's parameters, navigate to the Settings tab in your Administration Client, and under System, search for the Google Maps tab.
The following settings will be displayed:

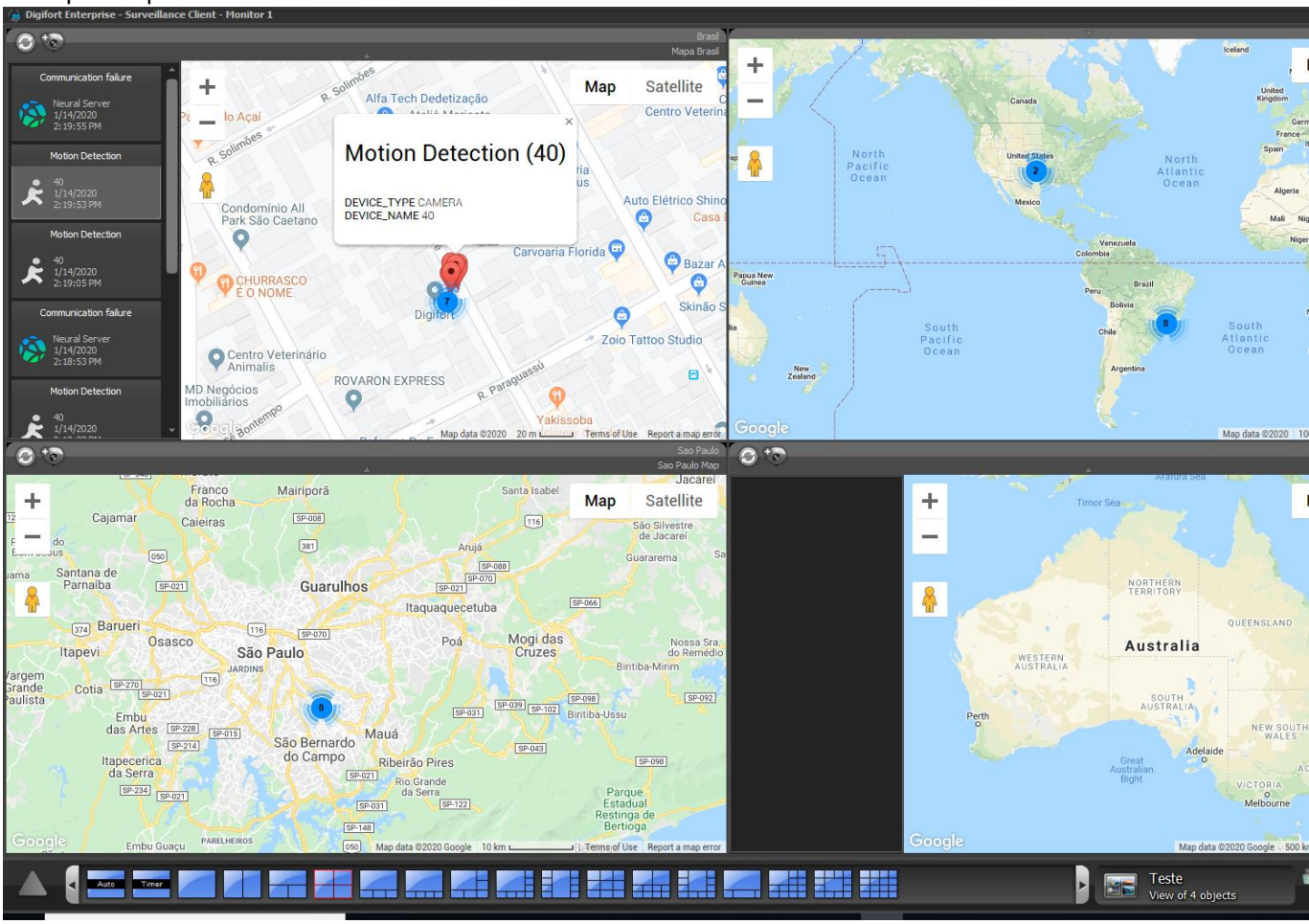
© 2002 - 2020 by Digifort, all rights reserved



To use Google Maps on your Digifort system, the system administrator must take the following steps to have access to an API Key:

- Visit the Google Developers site;
- Within this site, click on the 'Obtain a Key' option;
- Log in using your Gmail account's username and password;
- Create or select a project;
- Click on Continue to activate the API;
- Access the 'Credentials' option, create a Credential, and choose the 'Browser Key' option;
- Enter an API name;
- Create a key and copy the code.

Example of operation:



© 2002 - 2020 by Digifort, all rights reserved

To see this new feature in action, visit the videos available on our YouTube channel: http://www.youtube.com/DigifortChannel

https://www.youtube.com/playlist?list=PLFlhAF6oQd_op7kOm-gULjQj-JSK0qGDE

© 2002 - 2020 by Digifort, all rights reserved

Chapter XIV

14 Analytics

The analytics is a set of tools that intelligently processes the cameras' images. This process includes object count, flow control, missing and foreign objects, face detection and others shown in more detail below.

The analytics can complement surveillance in several ways, such as by triggering alerts, filing events and generating reports.

The Digifort analytics is considered an extra module as it is not included in the license of the Digifort cameras' server.

The Digifort Analytics has a server/own service for processing images and which can be installed on the same computer in which the camera images are recorded or in another computer used only for this purpose (recommended). Learn more about distributed processing in the chapter Understanding distributed processing.

14.1 Licensing the Digifort Analytics

How does the architecture for the Digifort Analytics work?

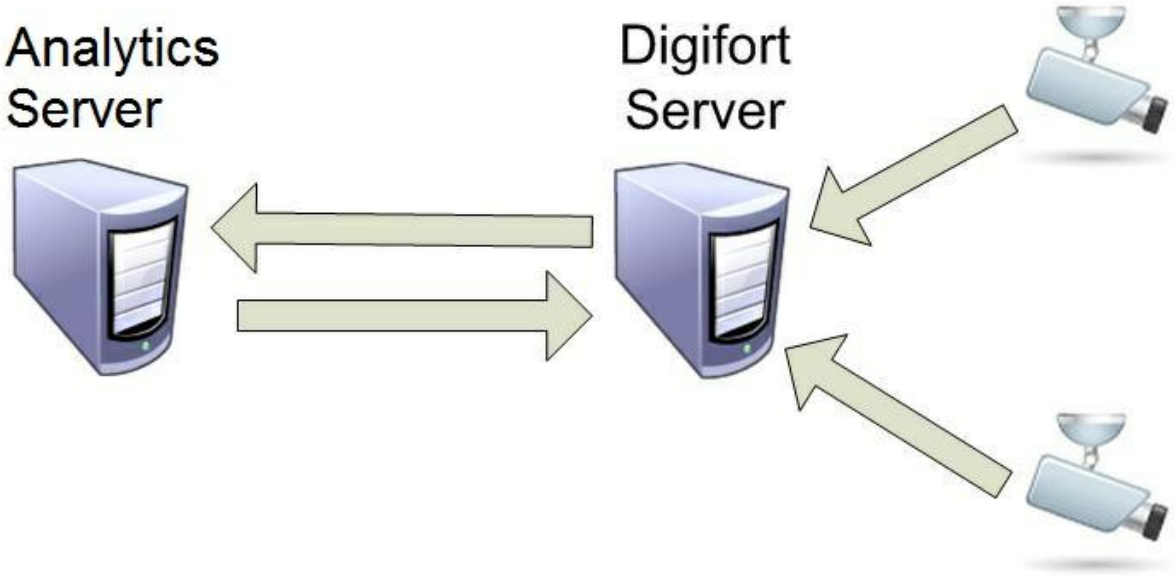
The license for the Analytics server works like the server for the Digifort cameras. There is a "base license" for the server and "additional licenses" for each camera.

The Digifort Analytics' base license includes the "Basic Analytics" which has the following modules: **Foreign Objects, Missing Objects and Face Detection** which can be used in as many cameras as needed.

The licenses for cameras (better known as "license pack") include de license for the **Advanced Analytics** which has the following modules available: **Presence, Entry, Exit, Disappear, Motionless, Loitering, Direction Filter, Speed Filter, Camera Tampering, and Cancel Shaking.**

The following diagram shows the licensing of two cameras with video analysis (**Basic** and **Advanced**) together with the Digifort server:

© 2002 - 2020 by Digifort, all rights reserved



In the picture above, the license distribution would be as follows:

- Analytics Server**: 1 licença base de analítico + 1 licença pack para 2 câmeras.**
- Digifort Server**:** 1 Base license (the version's base license Enterprise already includes <% BASE_LICENSE%> licenses available for recording; if the number of cameras added surpasses the number of base licenses, license packs should be added).

14.1.1 Understanding the distributed processing

In terms of processing, video analysis is heavier than recording/viewing from a camera. With flexibility in mind, Digifort developed an innovative processing architecture – the distributed processing architecture.

Digifort allows the cameras' analytical processing recorded on the Digifort server to be carried out on one or more computers that include the Analytical Server. The major advantage is that with such flexibility the recording server does not become overloaded and does not need to be a "super machine".

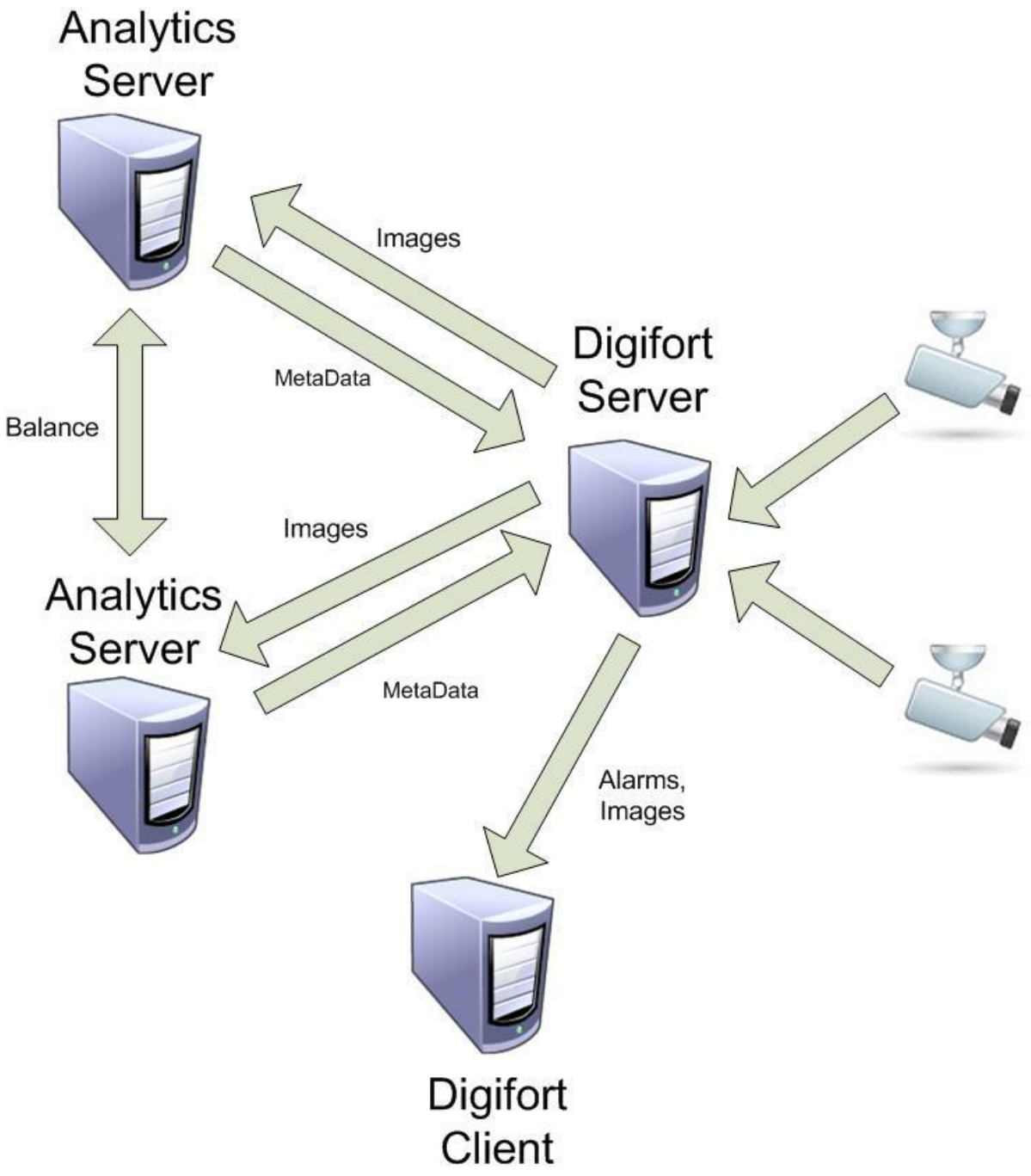
The analytical server automatically checks the computers with smaller processing capacity and

© 2002 - 2020 by Digifort, all rights reserved

"counterbalances the load", in other words, it distributes the processing of the video analyses so that all computers are left with as little processing as possible.

Remember that each computer with distributed processing is licensed with the Digifort Analytics base license.

Look at the diagram below:



© 2002 - 2020 by Digifort, all rights reserved

In the diagram above, the "**Digifort Server**" records the cameras' images and sends them to the "**Analytics Servers**" which, in turn, carry out their analyses and return the metadata (information on the alerts generated, object positioning and alert areas). The load counterbalance is among the "Analytics Servers" if it has been configured to do so. When the metadata return to the Digifort Server, it sends them and the alerts to the "**Digifort Clients**" (Surveillance Clients).

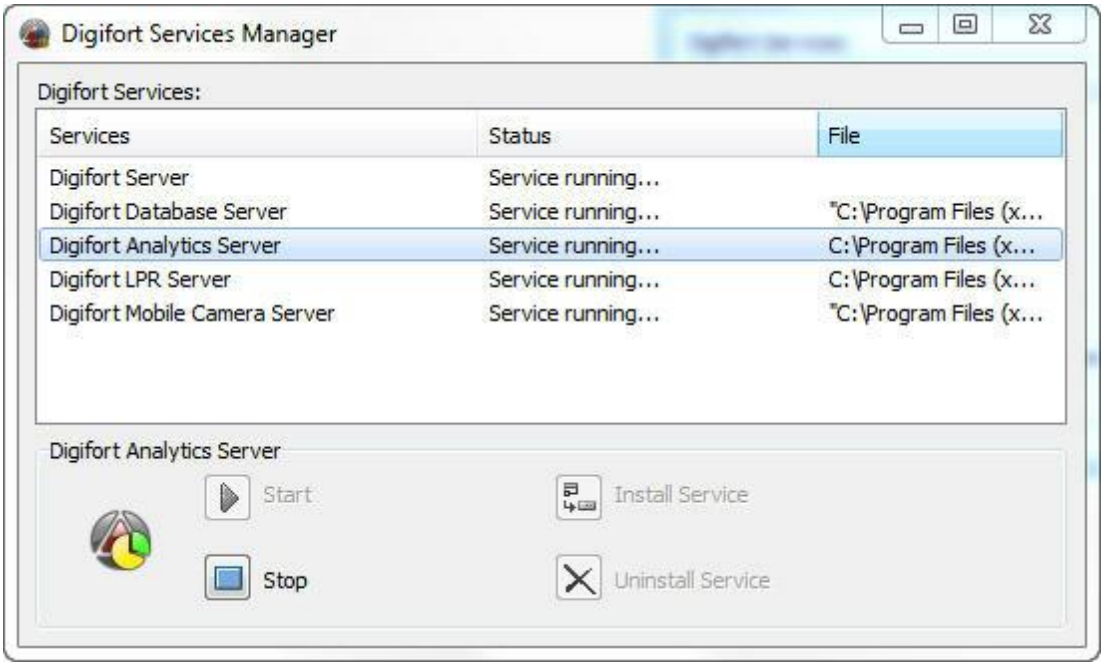
14.1.2 How to start the Analytics Server

To start the Digifort Analytics Server it must first be installed. Follow these steps to start the service correctly:

1. Select the "Digifort Analytics Server" service.

2. Click on Install Service. A confirmation screen will open indicating the service has been successfully installed.

3. Click on Start and wait while the server initializes. The start process ends when the message "Service in operation..." shows on the status bar.



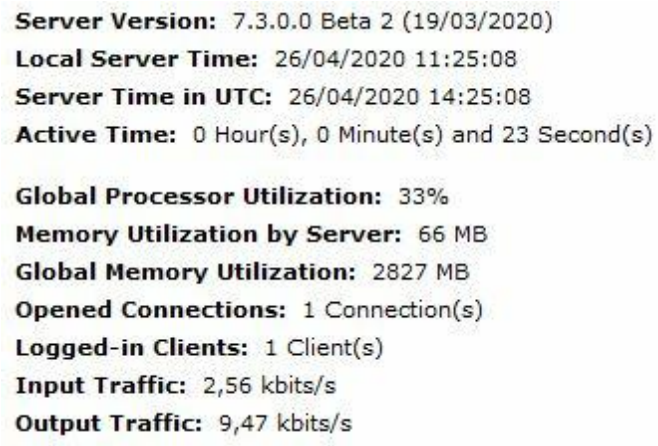
14.1.3 Analytics server status

In this area of the system you can monitor how the server is performing, recovering data such as processor usage, memory, network traffic, etc.
To access this resource, click on the Server Information item in the Settings Menu, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



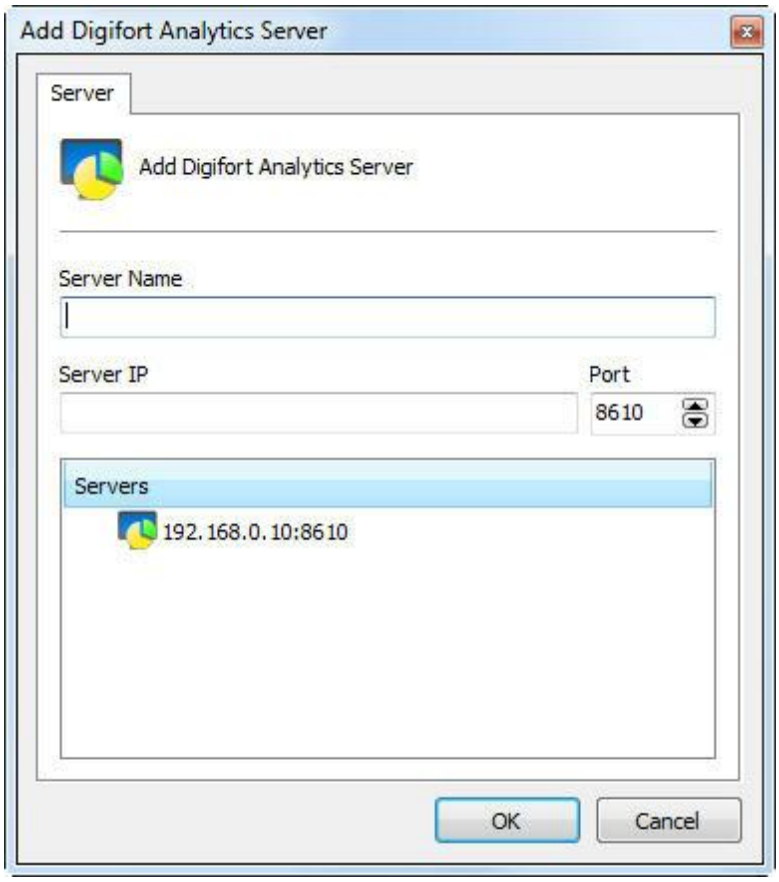
That done, the server information window will open on the right side, as shown in the figure below:



14.1.4 How to configure the servers to be managed

The first step to configure an analytics server is to add it to the list of servers to be managed by the Administration Client.
To add a server, click on the **Digifort Analytics Servers** diagram and then on the **Add Server** button, and the screen with the server registration will open as shown below:

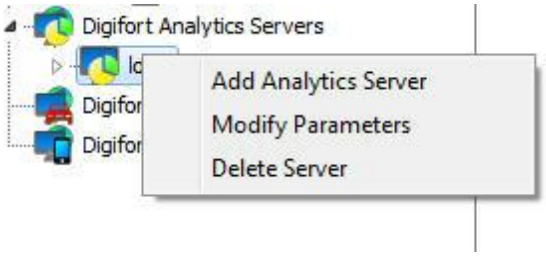
© 2002 - 2020 by Digifort, all rights reserved



- **Server Name**: Type the name of the server to be added. Once the data has been confirmed, the server name cannot be altered.
- **Server IP**: Type the name of the server to be managed.
- **Port**: Type the communication port with the server. By default, the port is 8610. The communication port with the server cannot be altered. This configuration should only be altered if you are accessing a remotely located server, such as the Internet, for example.
- **Servers**: This list comprises all the Analytics servers found on the network by the administration client. By clicking on one of the servers, the IP and **Port** described above are automatically filled in and all you have to do is fill in the **Server Name** to register.

Once you have provided all the correct data, click on **OK**.

When it has been included in the server, it will come up on the **Configurations** Menu as shown in the picture below:



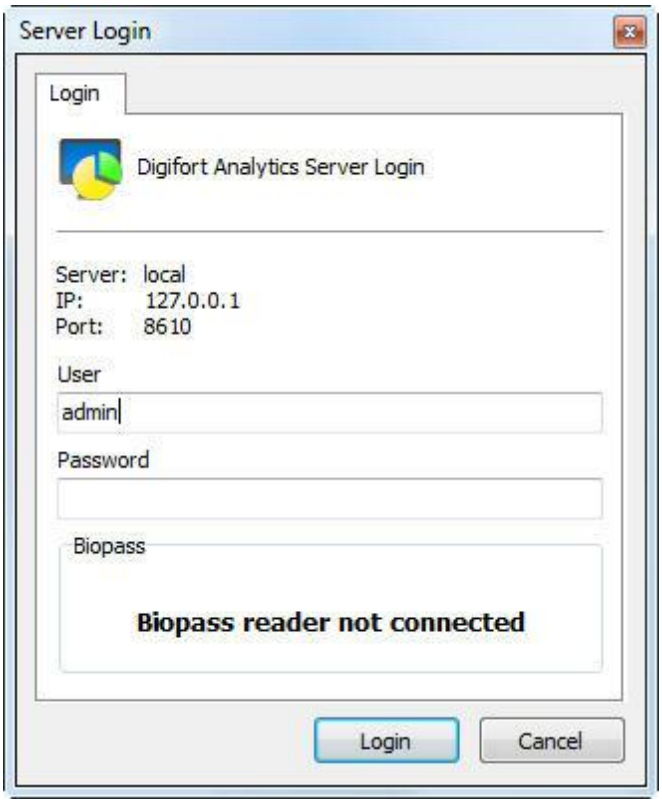
© 2002 - 2020 by Digifort, all rights reserved

To change the parameters of a server previously saved, click with the right-hand button of the mouse on the server chosen and click on Change Parameters. Change the data as necessary on the window that opens and click on **OK**.

To remove a server, click with the right-hand button of the mouse on the server chosen and then click on **Remove Server**. On the confirmation message that shows up click on **Yes**.

14.1.5 How to connect a management server

After adding the server, locate in it in the Configurations Menu and double-click on it. Once this is done, you will be asked to provide a username and password to access the server configurations as shown in the picture below:

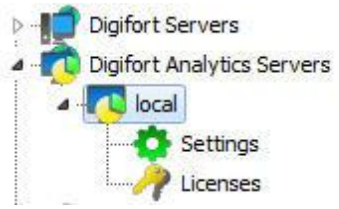


- **Username:** Access username.
- **Password:** Password for access.

Enter your username and password to access the server or the biometrics. If this is the first time you are accessing the system, insert the same username as the admin and leave the password blank.

Once you have filled in the access information, click on **OK**. If the authentication for access is successful, the Configurations Menu opens showing the configurations available for the server, as shown in the picture below:

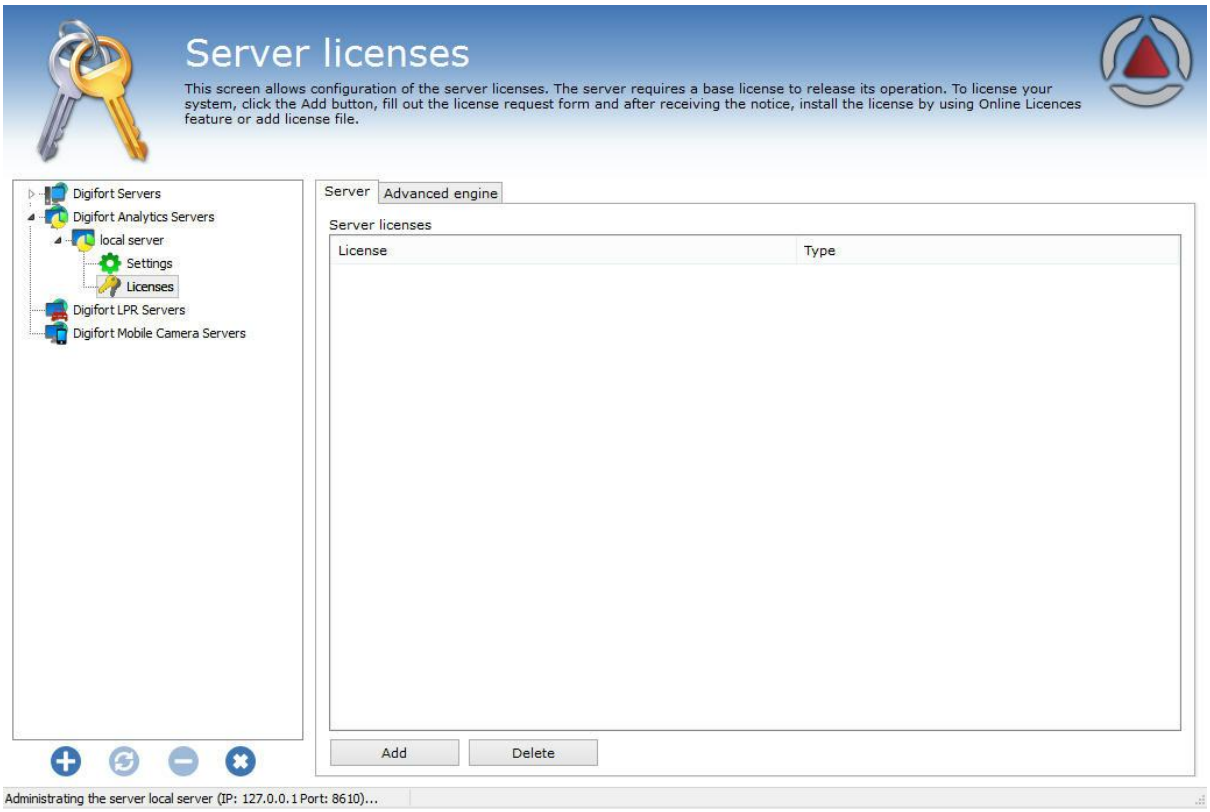
© 2002 - 2020 by Digifort, all rights reserved



14.1.6 How to configure the analytics licenses

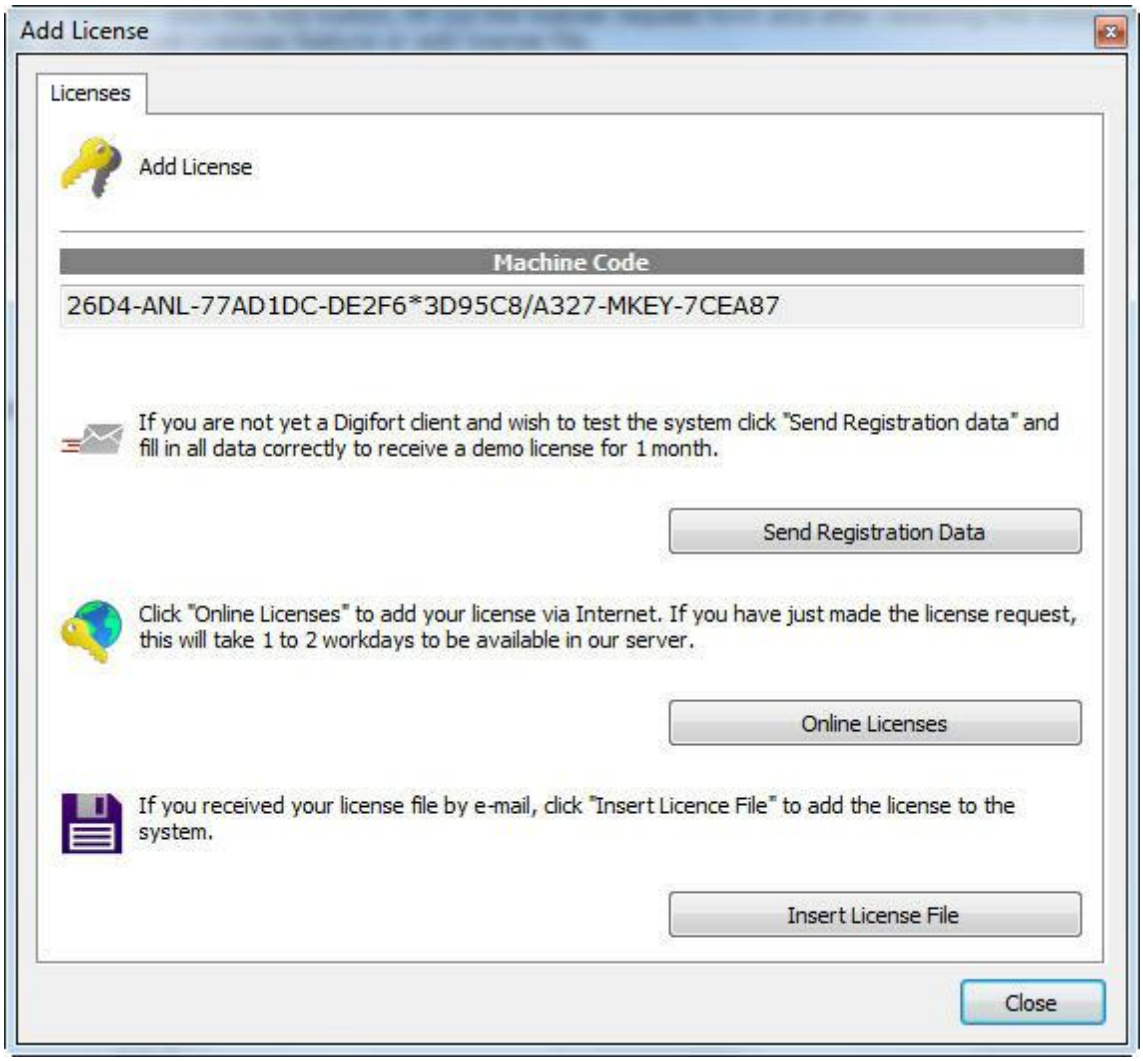
As said before, the Analytics works with two types of licenses: the Base License (**Basic**) and the License Pack (**Advanced**).

The first step to license the analytics is to add the base license (**Basic**). Once connected, go to the licenses field as shown below:



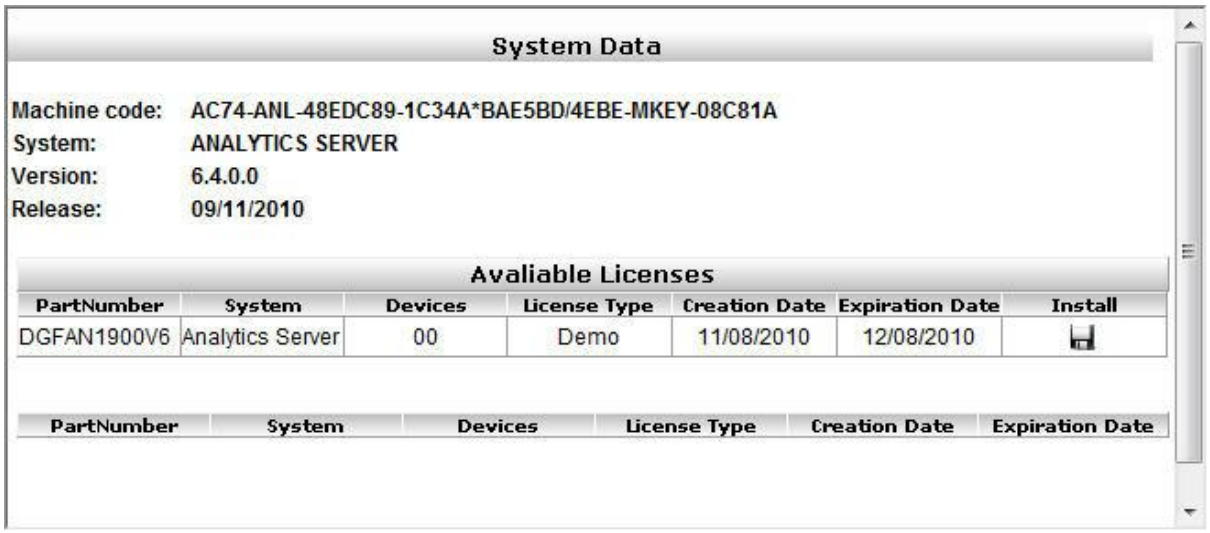
To add a license, click on Add and the following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved



The procedure to add licenses is the same as for Digifort and is described in the chapter How to configure licenses .
On the online license screen the description should be "**Analytics Server**" as shown in the picture below:

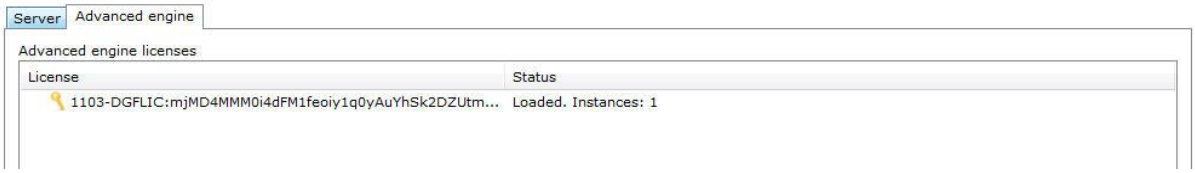
© 2002 - 2020 by Digifort, all rights reserved



Once a license has been added it becomes available as shown in the picture below:



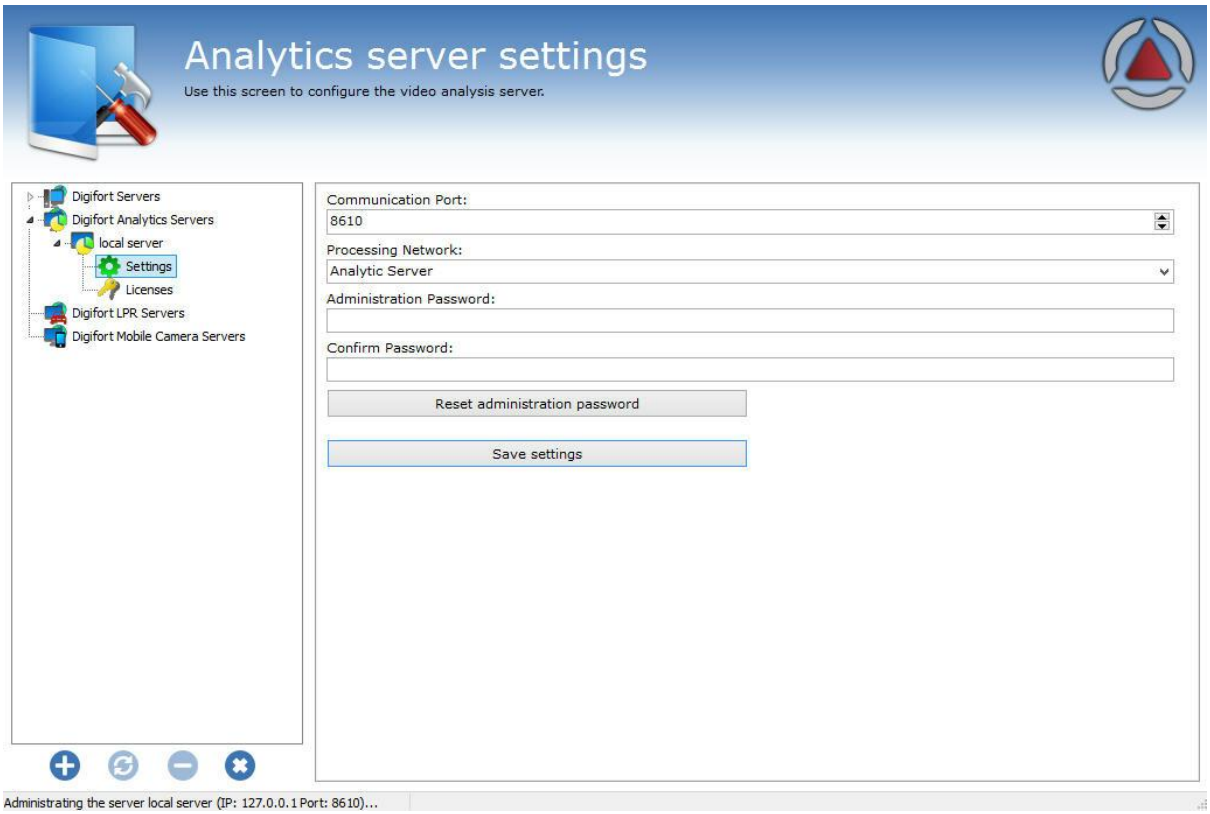
The **Advanced** analytics license works in the same way and in the status field you can see how many licenses are available, as shown in the picture below:



14.2 Analytics Server Configurations

To access the analytics server configurations, click on Configurations as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

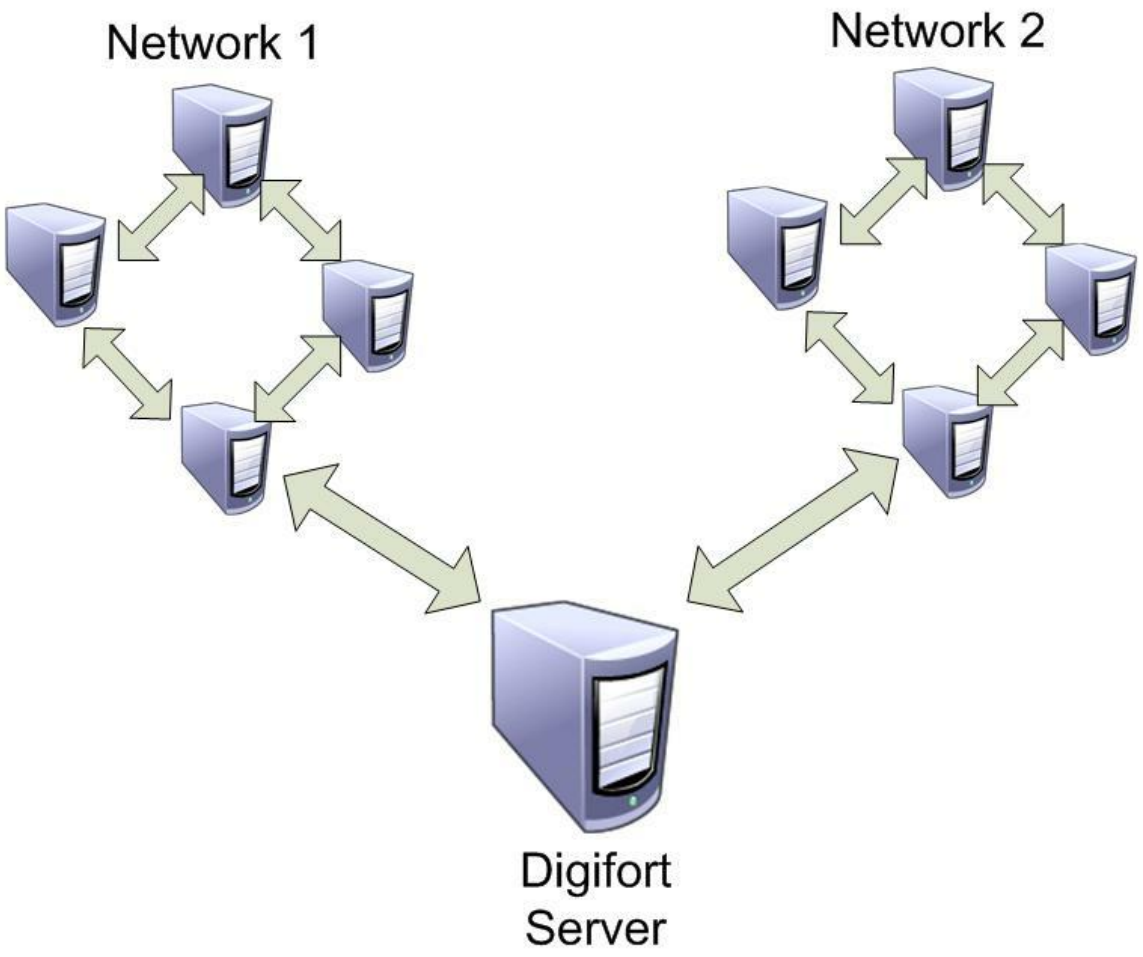


This screen has the following functionalities:

Communication Port: Communication port with the analytics server. It should only be changed if it is already being used on the computer in question.

Processing Network: Name of the distributed network where the server will counter balance the load. When more than one server has the same "Processing Network" name there will be a processing counterbalance among them. Look at the diagram below to get a better idea:

© 2002 - 2020 by Digifort, all rights reserved



In the picture above, the "**Digifort Server**" sends the images of the cameras to two different " **Processing networks**". This way, each set of computers only counterbalances the load among the **Analytics Servers** with the same network name.

Administration Password: Password to access the analytics server. Fill in this field to change the current password.

Confirm Password: Type the password again.

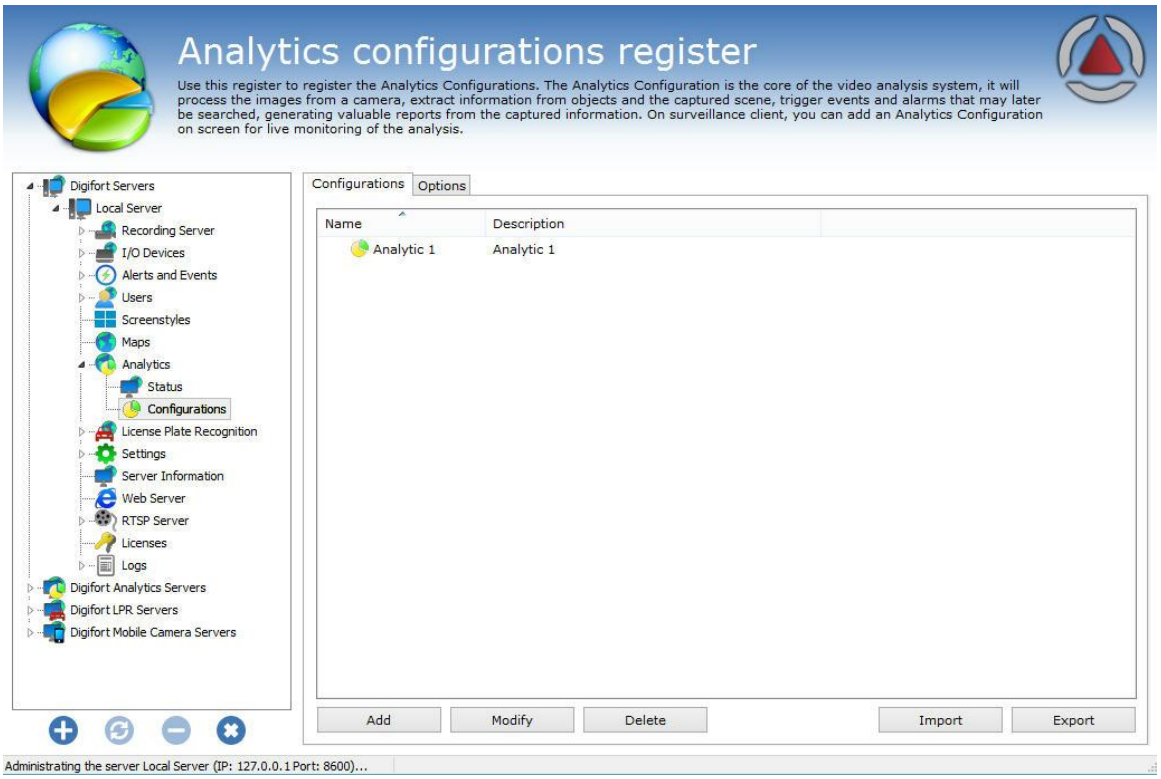
Reset administration password: Blank password is retrieved.

Save configurations: Saves changes made on the screen.

14.2.1 Adding an analytics configuration

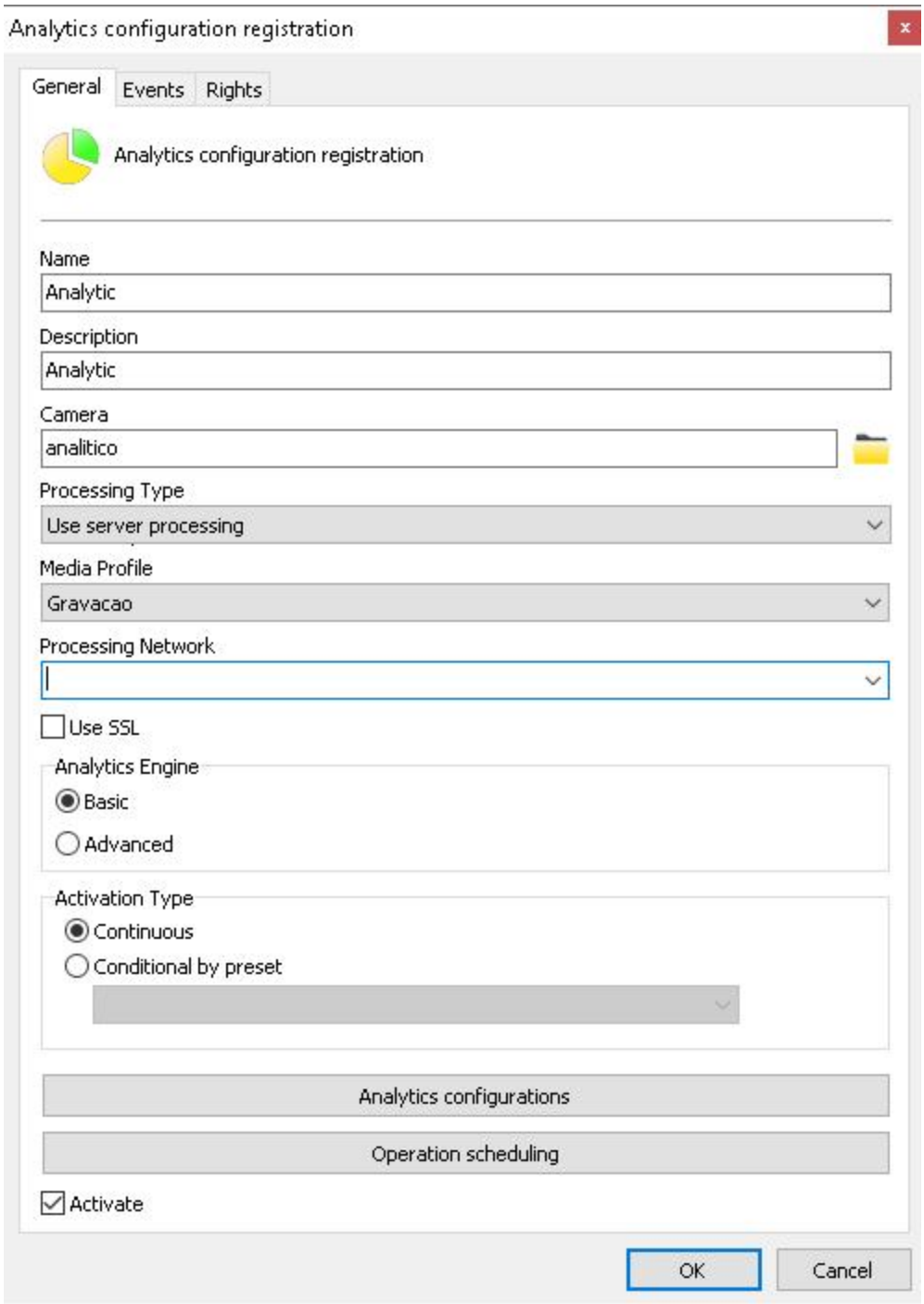
This topic will address how Digifort's **Basic** and **Advanced** analytics settings are done.
After properly licensing the analytics server, go to **Analytics Settings** as shown in the image below.

© 2002 - 2020 by Digifort, all rights reserved



The **Settings** tab allows you to add a new analytics setting.
To do this, click on the **Add** button to start the analytics settings. The following screen will be displayed:

© 2002 - 2020 by Digifort, all rights reserved



This screen provides the following features:

- **Name**: The name of the desired analytics, for example: **Digifort 1**
- **Description**: Description of the analytics registration, for example: **Vehicle count from Avenue 1.**

© 2002 - 2020 by Digifort, all rights reserved

- **Camera**: All cameras registered on the Digifort server will be available in this check box. The analytics rules defined will apply to the camera that is configured in this check box. To learn how to register cameras, see the 'How to add a camera' chapter.

- **Processing Type**: Allows images to be processed in engines available locally at Digifort or on third party servers. This option opens the range of Analytical integrations and allows the future expansion of the Digifort Analytical base system for powerful integrations with third-party systems.
  - The following servers are currently supported:
    - Axis Perimeter Defender
    - IPXAnalytics (IP Extreme)
    - SAFR
    - VCA Server
    - VideoSynopses

- **Media Profile**: It selects the media profile that is desired for analysis. The analytics always analyzes images in a 320x240 or 352x240 resolution, so it is recommended for the camera to have at least these values or higher. Video analysis does not interfere in the quality/performance of the video that is transmitted and recorded.

- **Processing Network**: All processing networks (analytics servers) active on the network will be available in this field. It selects a network in which this configuration will be processed. You can specify the processing server by its IP. To do so, use the following format in the field: **"IP:server IP**". Example: **IP:192.168.0.10.**

- **Analytics Engine**: It chooses the engine that will analyze the images. There are two engines on Digifort for image processing: Basic Analytics and Advanced Analytics.
  - The **Basic Analytics** has the following analysis modules: **Objects left, objects removed and Face Detection**.
  - The **Advanced Analytics** has the following analysis modules: **Presence, Enter, Leave, Appear, Disappear, Stationary, Loitering, Directional Filter, Speed Filter, Camera tampering and Trepidation canceling.**

- **Activation Type**
  - **Continuous**: It processes the image from a camera continuously.
  - **Conditional per preset**: The system now allows you to activate an analytics configuration conditionally by preset. Thus, you can define a preset to activate the analytics configuration and this configuration will only work when the camera is on the configured preset.

- **Analytics configuration**: It opens the configuration screen of the chosen engine.

Operation Scheduling: It allows you to schedule the analytics' operation time.

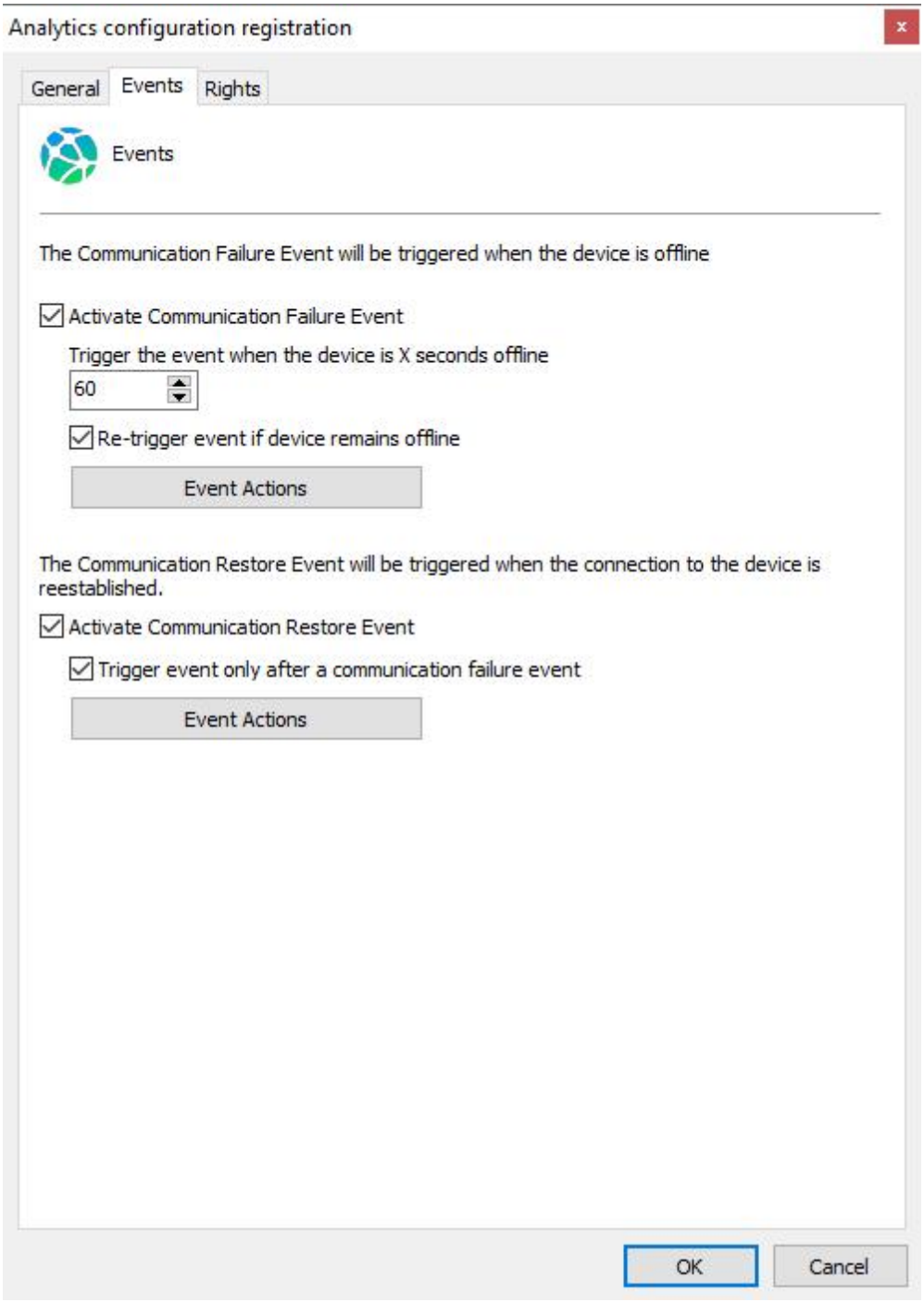
Activate: It activates or deactivates the analytics settings.

Note

When an Advanced analytics configuration is active, a license will be used.

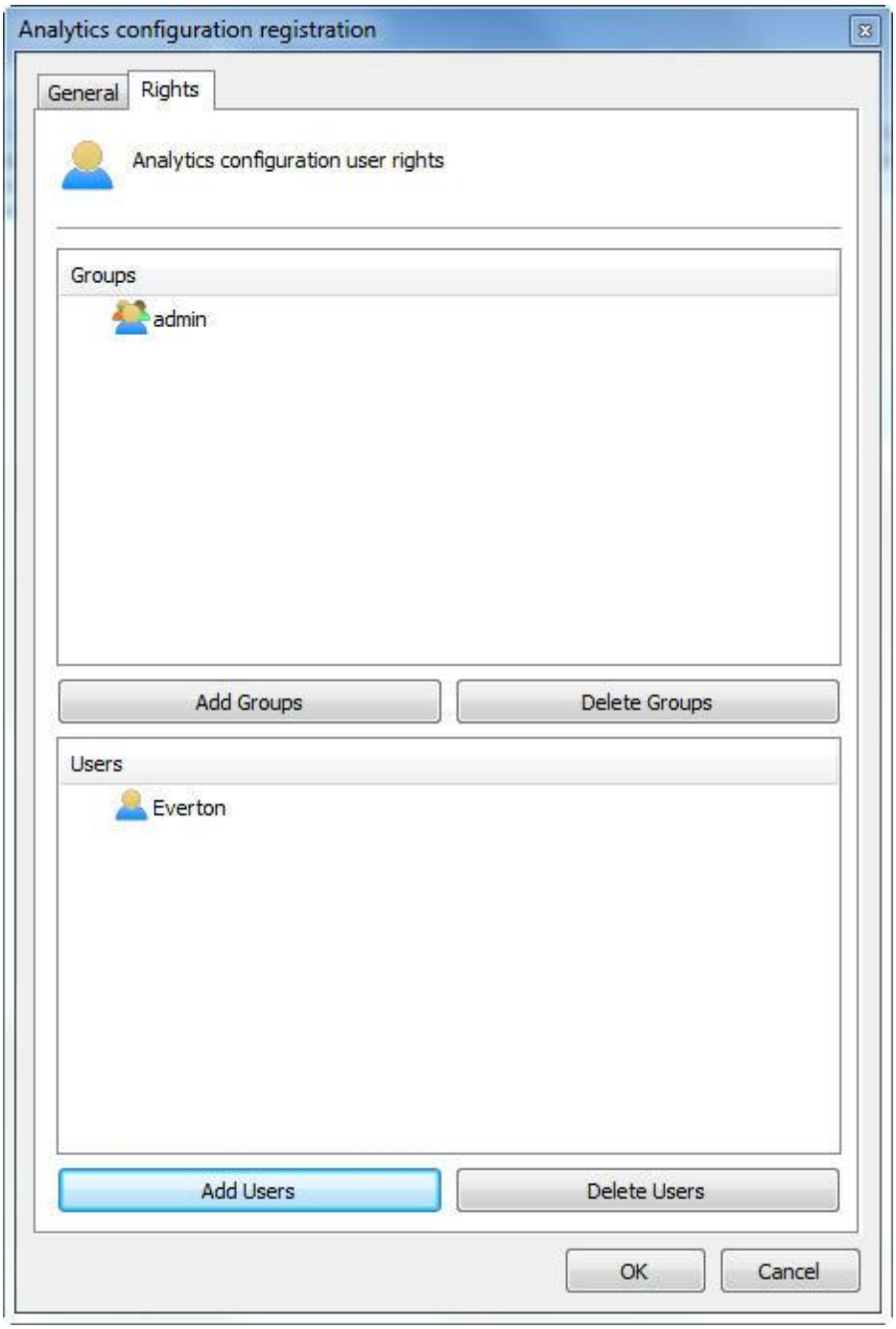
On the events tab, you can configure the communication failure or communication restoration events for the analytics configuration, as per the figure below:

© 2002 - 2020 by Digifort, all rights reserved



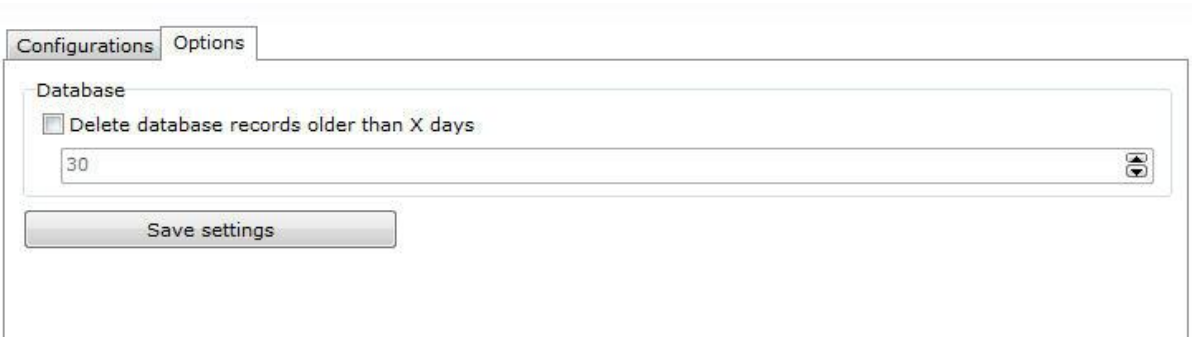
On the events tab, you can configure the communication failure or communication restoration events for the analytics configuration, as per the figure below:

© 2002 - 2020 by Digifort, all rights reserved



To learn about users and user groups, see the 'User Management' . chapter.
On the Options tab, you can set the number of days in which records of analytics events will be kept on the Digifort database.

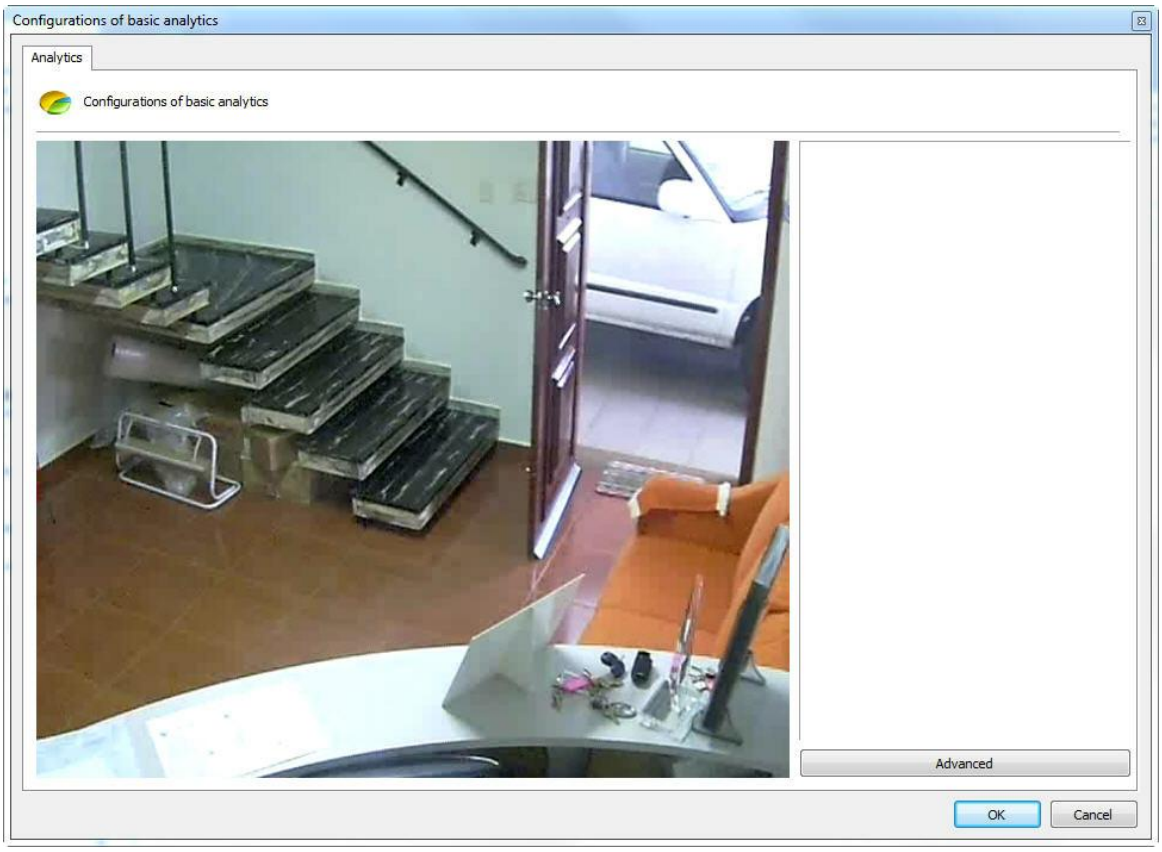
© 2002 - 2020 by Digifort, all rights reserved



14.2.1.1 How to configure the Basic Analytics

If the **Basic** engine is chosen in the analytics register screen, the following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved



The image that appears is related to the camera and the media profile selected in the register screen of the analytics.

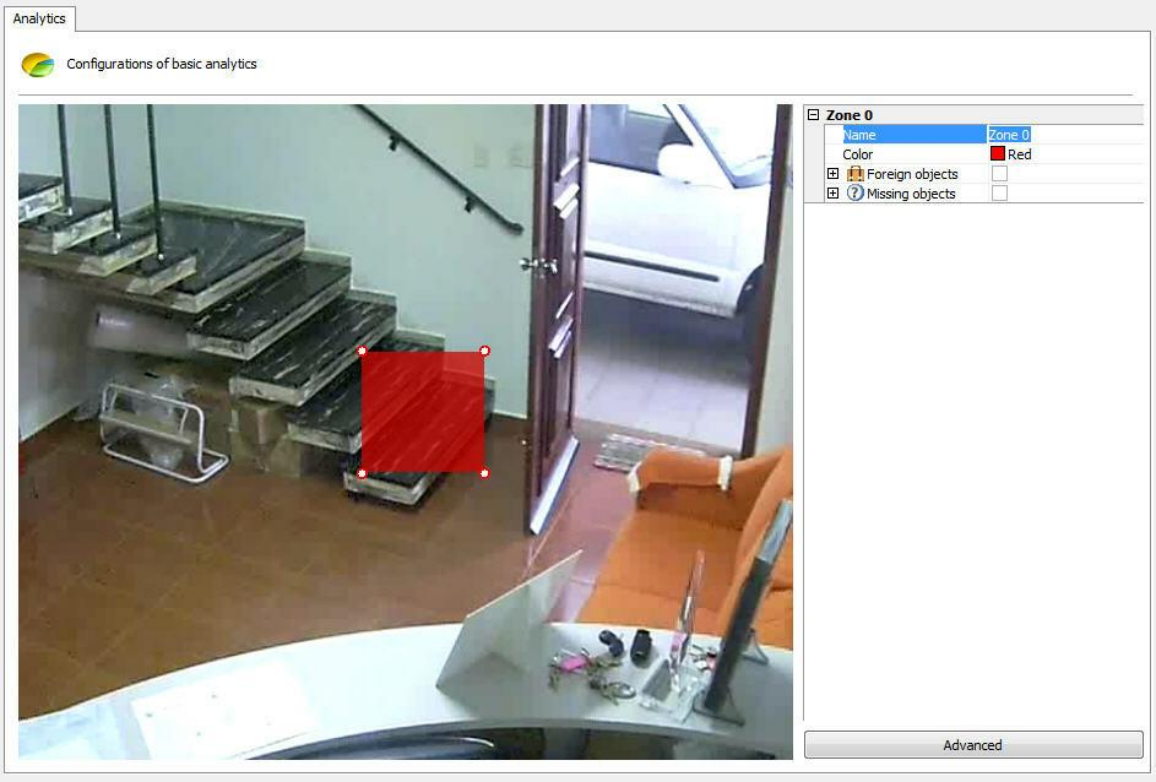
This screen has the following functionalities when the right-hand button is activated:



- **Create zone**: Creates a zone where the analysis module is defined.
- **Delete**: Deletes a selected zone.

Create a zone and click on it as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



An options menu of the area will open on the screen's right-hand column. The following options will be available:

- **Name**: Name for the area created. It is important to consider what name will be given as it will be possible to create reports using that name.
- **Colour**: Changes the colour of the area selected.
- **Foreign Objects**: Module that analyzes the objects left. This module will be described in chapter Foreign Objects
- **Missing Objects:** Module that analyzes the objects removed. This module will be described in chapter Missing Objects

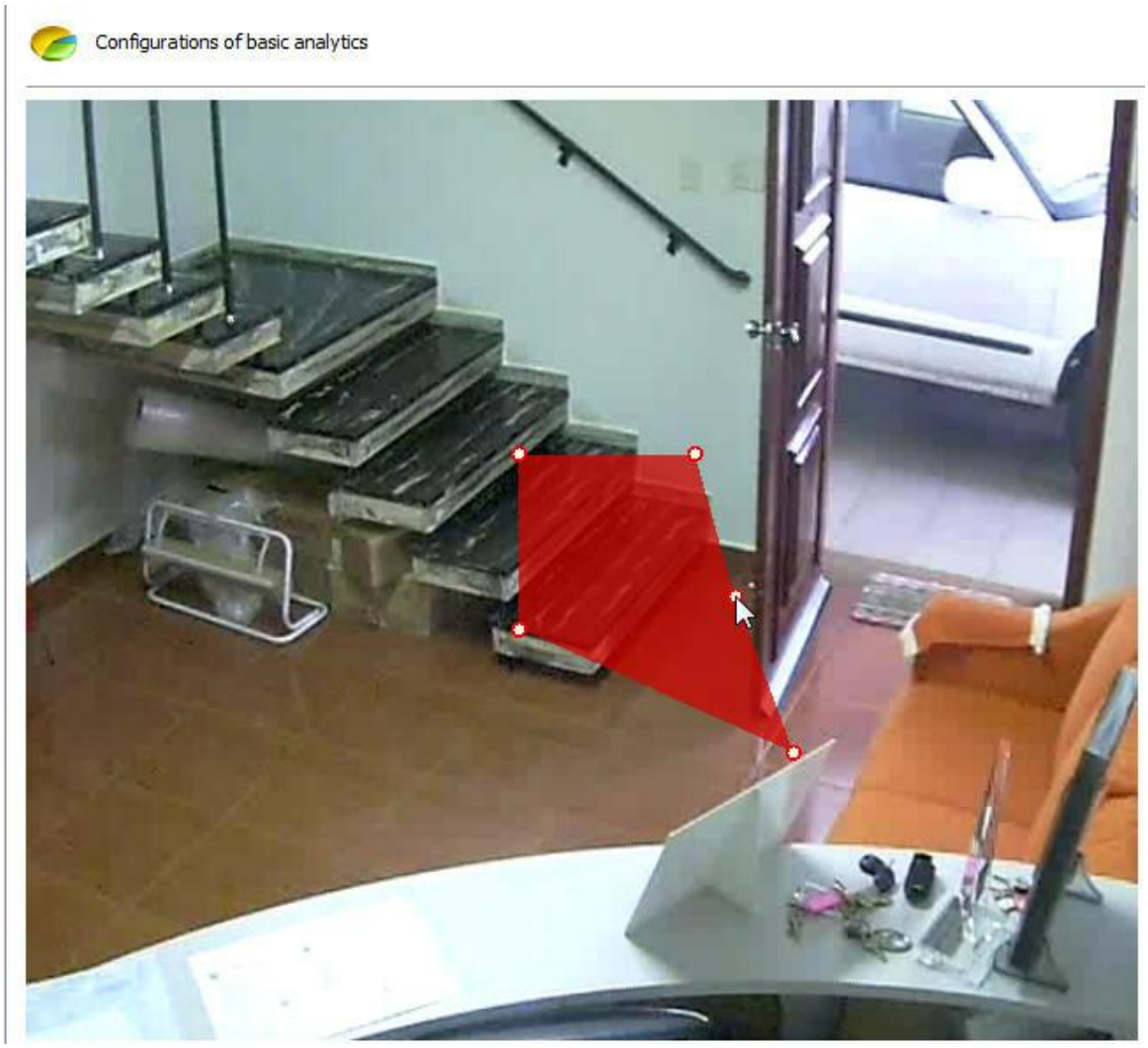
You can move the points in the area by clicking on the circles, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



And add points with a double-click near the area's edge as shown below:

© 2002 - 2020 by Digifort, all rights reserved



20 is the maximum number of points per area.

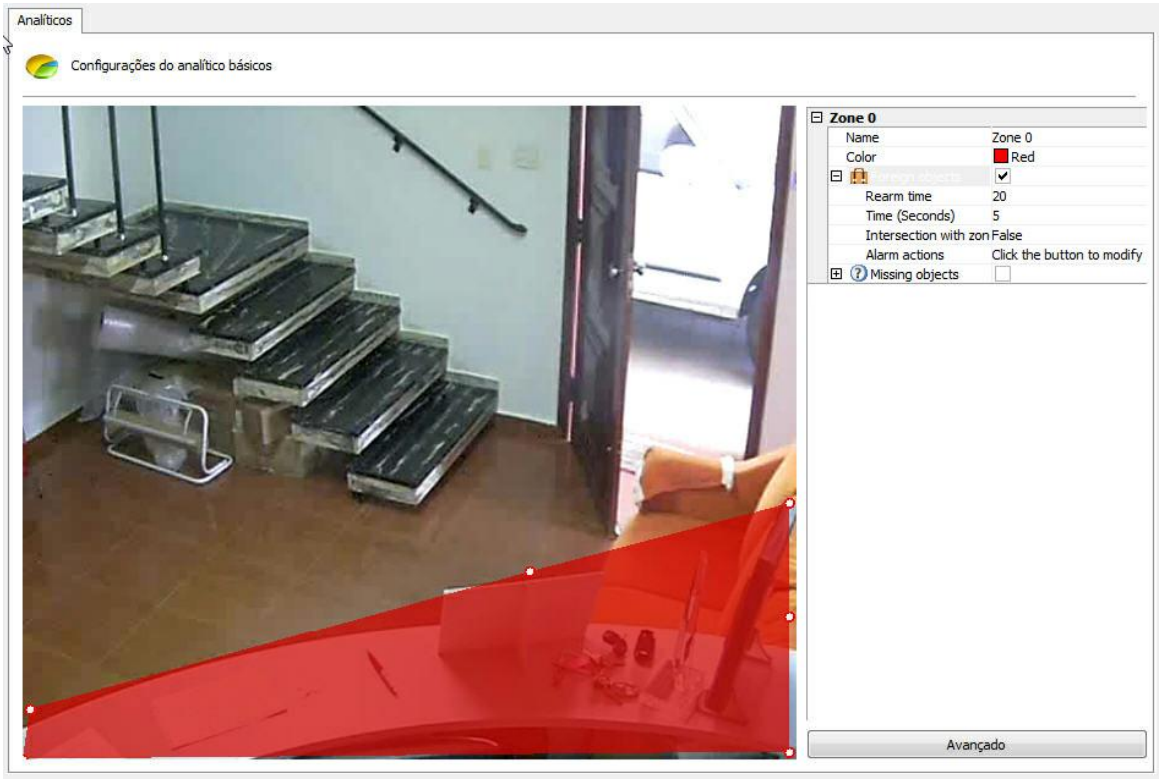
14.2.1.1.1 How to configure the Foreign Objects module

The **Foreign Objects** module can generate alerts when an object is left in a specific area of the image or when something in the scene changes. Example: A bag left on the floor; a key found on a table. The video can be recovered from these events, and alerts and reports generated.

The analytics modules were designed to help surveillance and are not 100% precise. For example: the foreign objects module can create alerts if there are changes to the lighting, projected shadows, etc. and this creates the so-called false alarm.

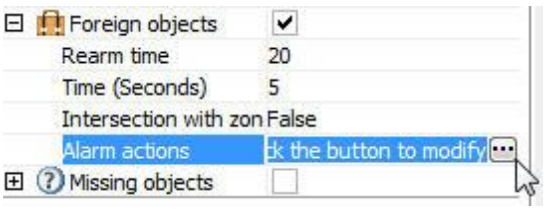
In our example, we created a detection area for the table as in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



By opening the side options in **Foreign Objects**, the following functionalities are available:

- **Foreign Objects:** Tick this option to activate the Foreign Objects in this area.
- **Rearm time**: Rearm time for the alert to be activated again in the surveillance client (if configured).
- **Intersection with the area**: If false it will only be triggered if there are objects with their centre within the zone. If true, any object intersecting with the area can trigger the alert.
- **Time**: Time in seconds the object must remain unmoving in the area to trigger the alert. Long periods are not recommended for areas where there is a lot of movement.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

The following is an example of when the alert was triggered in the situation previously configured:

© 2002 - 2020 by Digifort, all rights reserved



Whenever an alert is triggered the scene is automatically captured.
To learn how to generate reports, refer to the Surveillance Client manual.

Nota

The Foreign Objects module will trigger alerts if there is any change in the scene, in other words, whenever objects are left or removed. The difference between this module and the Missing Objects one is that this one looks for objects within an area, whereas the Foreign Objects module outlines the area exactly around the object in question.

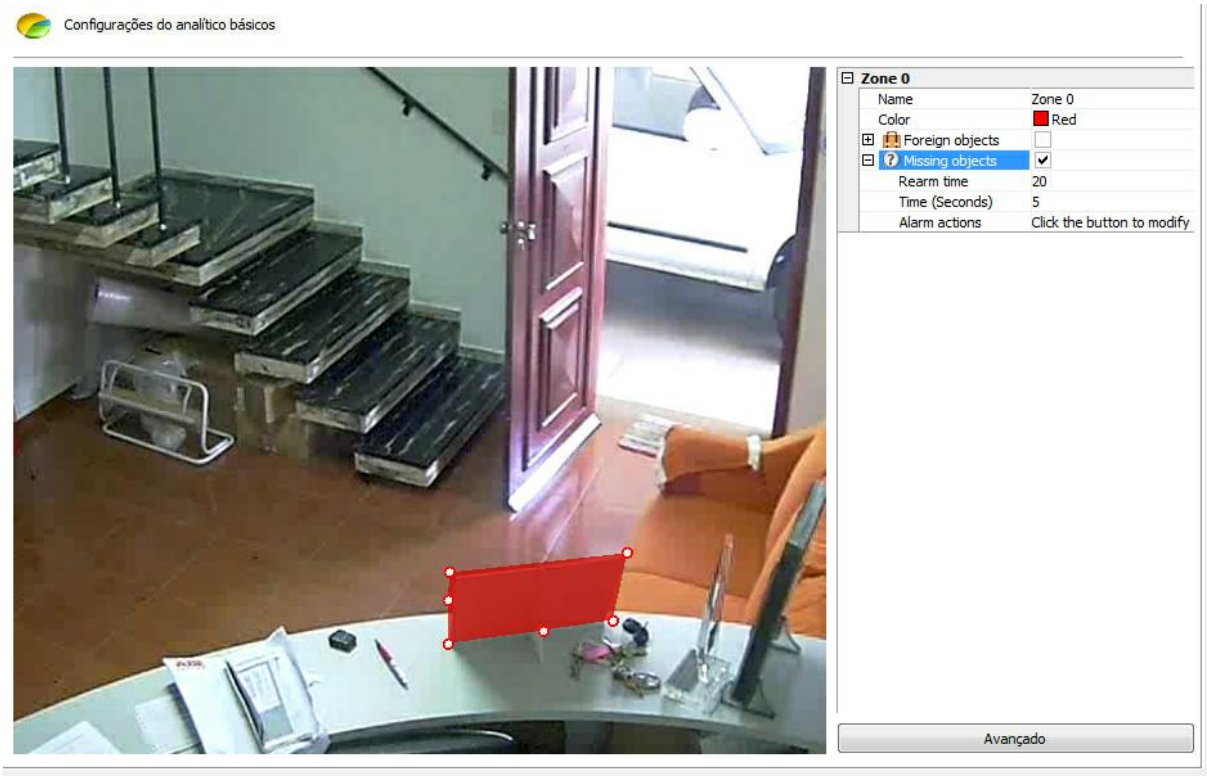
14.2.1.1.2 How to configure the Missing Objects module

The **Missing Objects** module can generate alerts when a delimited object is removed from the scene. Example: A picture, a valuable object, etc. The video can be recovered from these events, and alerts and reports generated.

The analytics modules were designed to help surveillance and are not one 100% precise. For example: the missing objects module can create alerts if there are changes to the lighting, projected shadows, etc. and this creates the so-called false alarm.

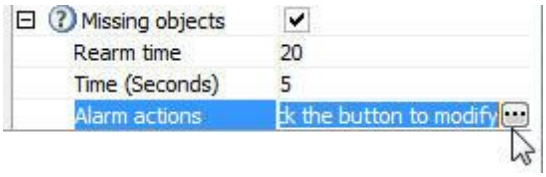
In our example, we created a detection area for an object on the table as in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



As you can see in the Missing Objects, the zone must be delimited around a specific object, contrary to the Foreign Objects.
By opening the side options in **Missing Objects**, the following functionalities are available:

- **Missing Objects:** Tick this option to activate the Foreign Objects in this area.
- **Rearm time**: Rearm time for the alert to be activated again in the surveillance client (if configured).
- **Time**: Time in seconds the object must remain unmoving in the area to trigger the alert. Long periods are not recommended for areas where there is a lot of movement.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

The following is an example of when the alert was triggered in the situation previously configured:

© 2002 - 2020 by Digifort, all rights reserved



Whenever an alert is triggered the scene is automatically captured.
To learn how to generate reports, refer to the Surveillance Client manual.

14.2.1.1.3 How to configure the Face Detection module

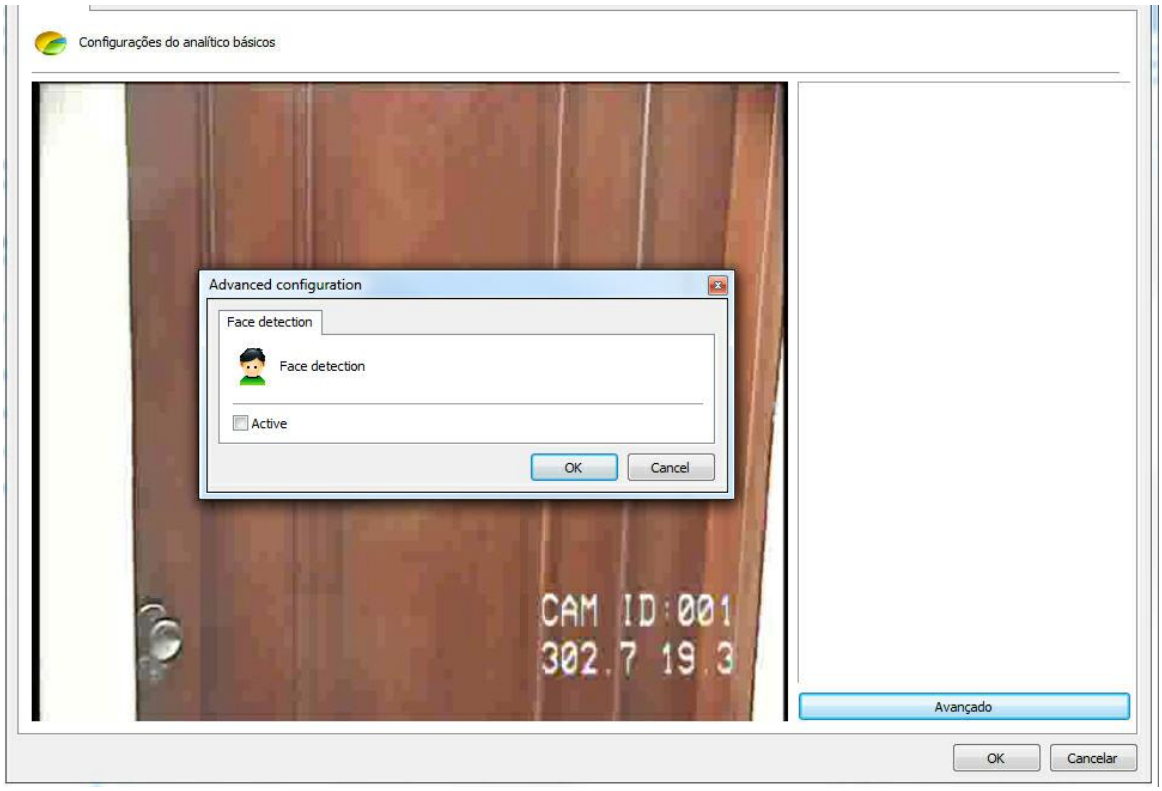
The aim of the **Face Detection** module is to capture the faces that pass by a certain camera and store them in a database.

For best results, the camera must focus a certain area so that the person's face occupies about 20% to 70% of the area of the image. Here is an example:

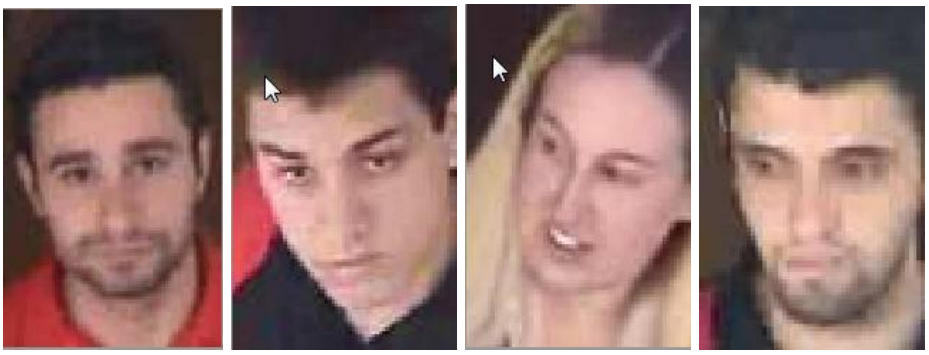


In the analytics configuration screen, click on the **Advanced** button and on **Activate** on face detection.

© 2002 - 2020 by Digifort, all rights reserved



The following is an example where the faces were captured in the situation previously configured:

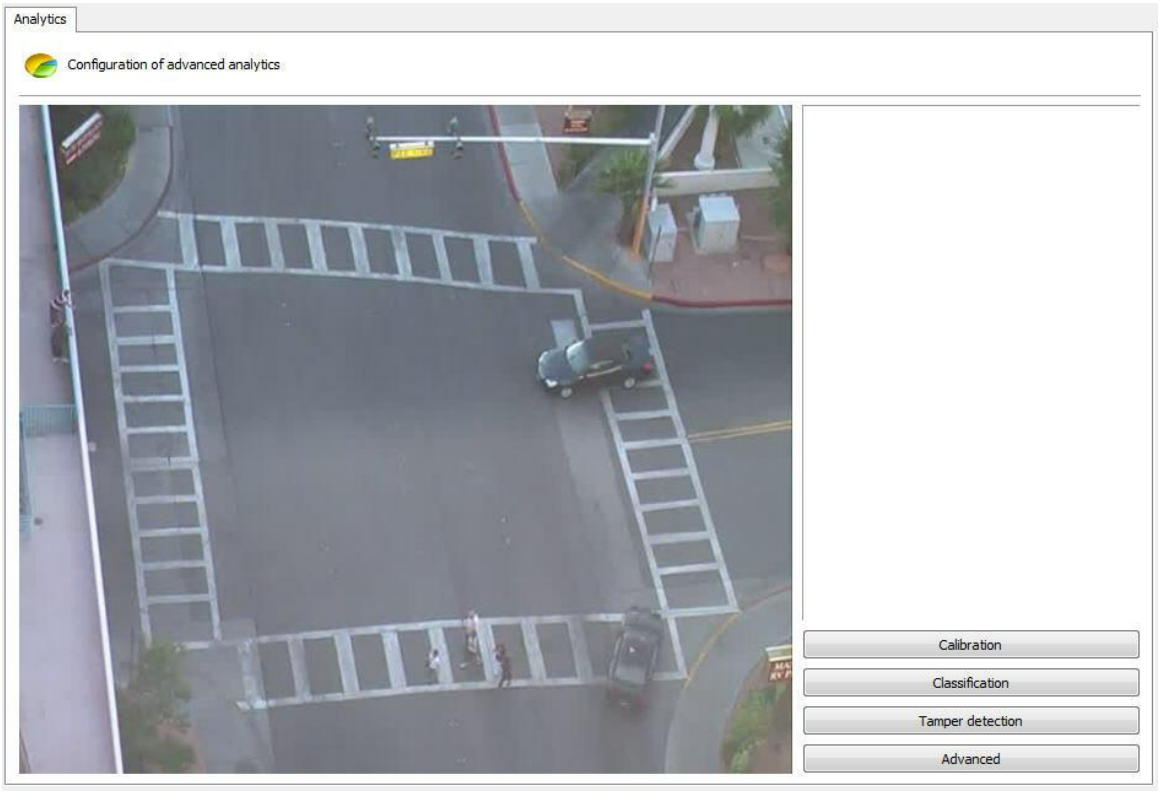


To learn how to generate reports and look up the faces captured, refer to the Surveillance Client manual.

14.2.1.2 How to configure the Advanced Analytics

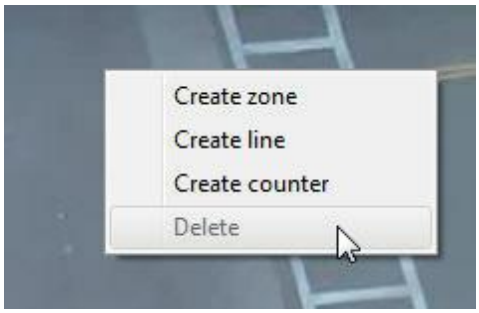
If the **Advanced** engine is chosen in the analytics register screen, the following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved



The image that appears is related to the camera and the media profile selected in the register screen of the analytics.

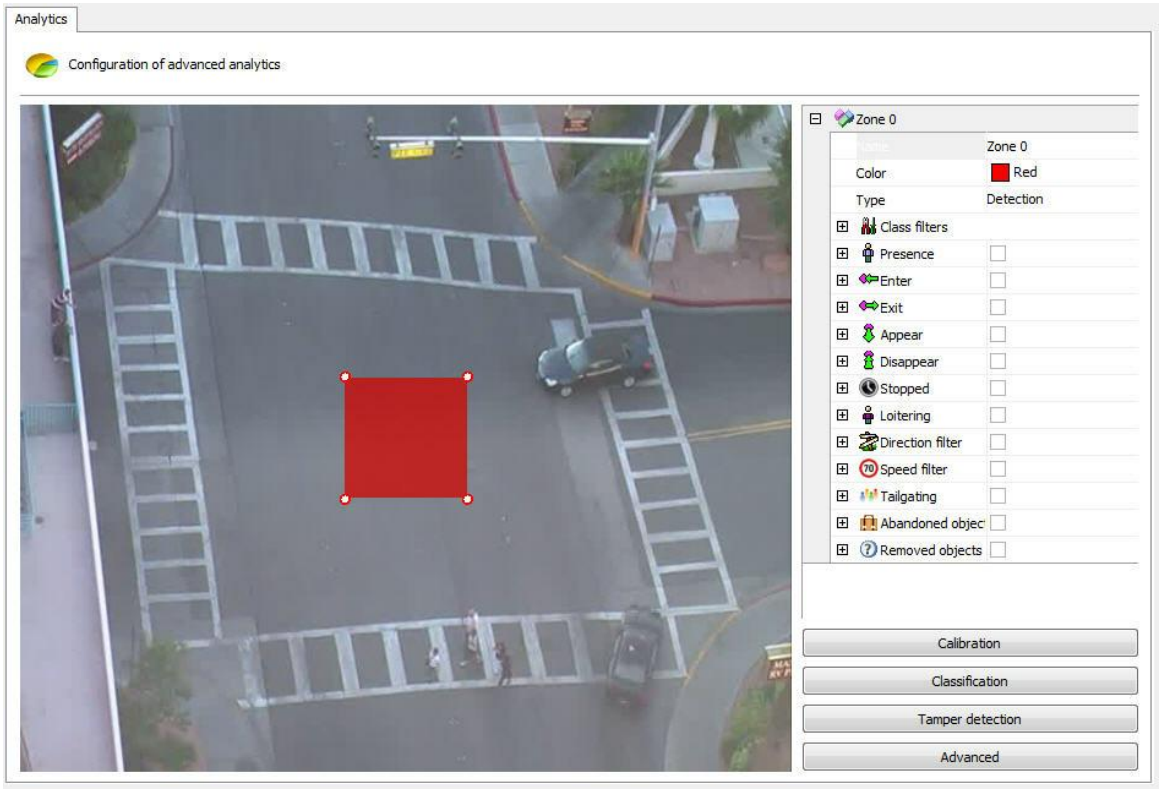
This screen has the following functionalities when the right-hand button is activated:



- **Create zone**: Creates a zone where the analysis module is defined (Rules).
- **Create line:** Creates a line where the analysis module is defined (Rule).
- **Create counter**: Creates a counter which will be associated to an analysis module (rule).
- **Delete**: Deletes a selected area/line/counter.

Create an area/line and click on it as shown in the picture below:

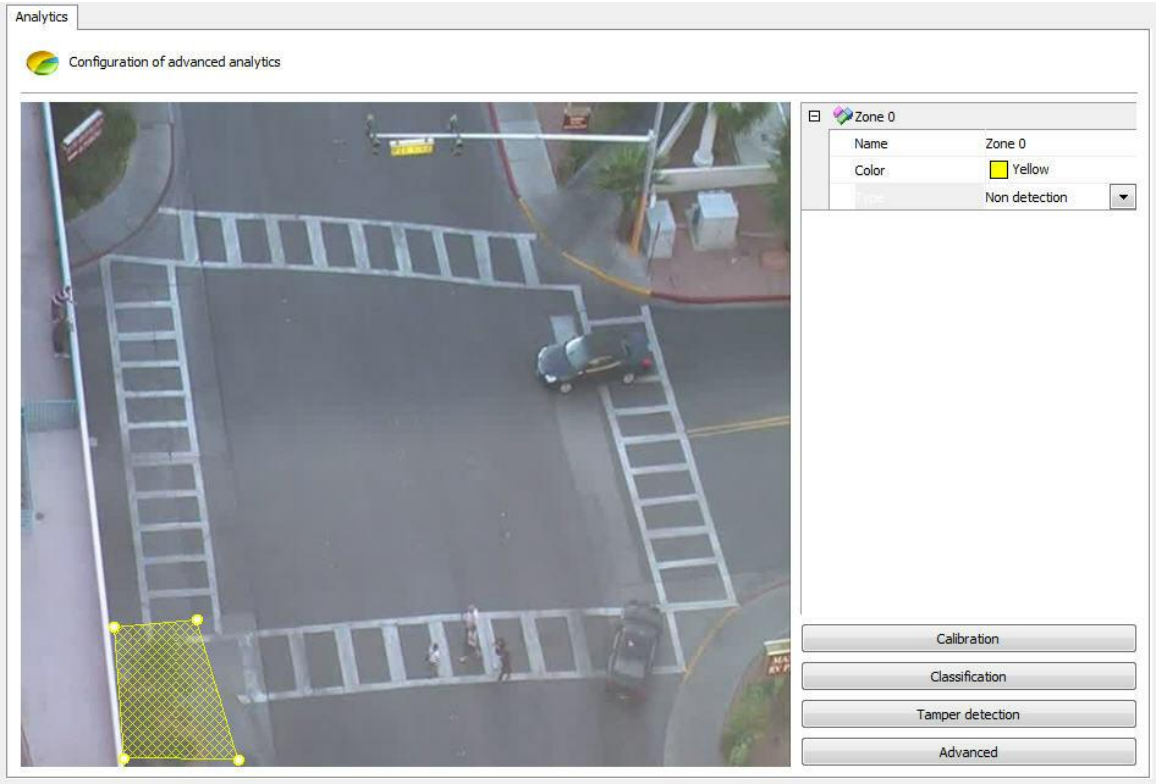
© 2002 - 2020 by Digifort, all rights reserved



An options menu of the area will open on the screen's right-hand column. The following options will be available:

- **Name**: Name for the area created. It is important to consider what name will be given as it will be possible to create reports using that name.
- **Colour**: Changes the colour of the area/line selected.
- **Type**: There are two area types: **Detection** and Non-detection.
  - The **detection** area is the standard area where the analytical modules are applied.
  - The non-detection area is used to remove unwanted areas from the image, such as trees, rivers, etc. The picture below illustrates a non-detection area:

© 2002 - 2020 by Digifort, all rights reserved



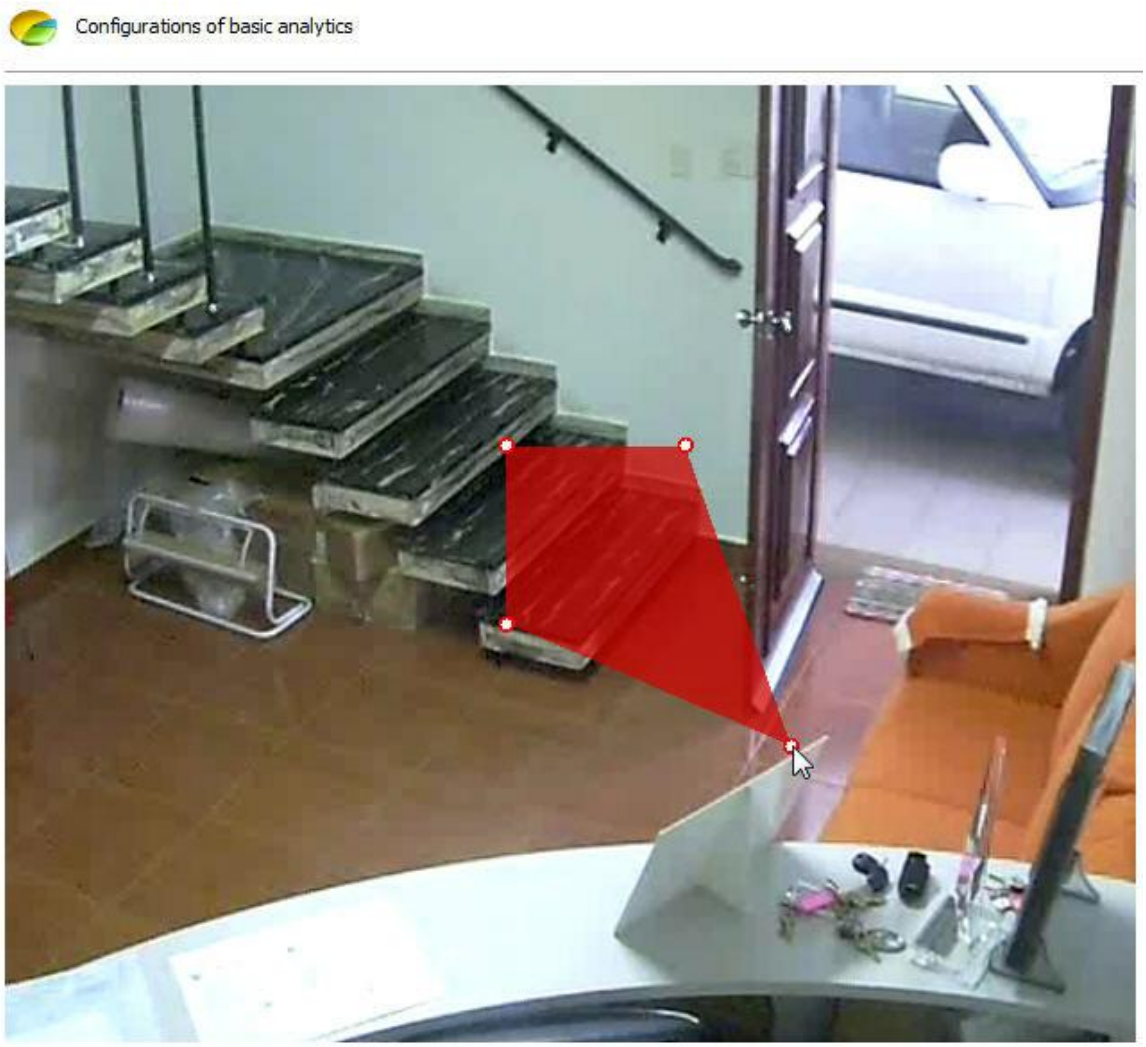
- **Object filters**: Determines the object that should be included in /excluded from the detection in the selected area. Learn more about this feature in chapter How to classify objects
- **Presence**: The module that detects the presence of an object within the selected area (person, cars, animals, etc). This module is described in chapter How to configure the Presence rule
- **Entry**: Module that detects when an object enters the selected area. This module is described in chapter How to configure the Entry rule
- **Exit**: Module that detects when an object exits the selected area. This module is described in chapter How to configure the Exit rule
- **Appear**: Module that detects when an object appears in the selected area. This module is described in chapter How to configure the Appear rule
- **Disappear**: Module that detects when an object disappears from the selected area. This module is described in chapter How to configure the Disappear rule
- **Stopped**: Module that detects when an object is unmoving within the selected area for more than a certain length of time. This module is described in chapter How to configure the Stopped rule
- **Loitering**: Module that detects when an object is moving within the selected area for more than a certain length of time. This module is described in chapter How to configure the Loitering rule
- **Direction Filter:** This module detects when an object is going through a wrong way. This module is described in chapter How to configure the Direction Filter rule
- **Speed Filter:** Module that triggers alerts when the speed of the object is between the configured maximum and minimum speeds. This module is described in chapter How to configure the Speed Filter rule
- **Count Line**: Allows people count from one line. This module will be covered in chapter Configuring the rule count line
- **Tailgating**: Module that detects when a second object passes in a given area within a

© 2002 - 2020 by Digifort, all rights reserved

configurable amount of time between the first object that previously went through the same area. This module will be covered in chapter Configuring the Tailgating rule

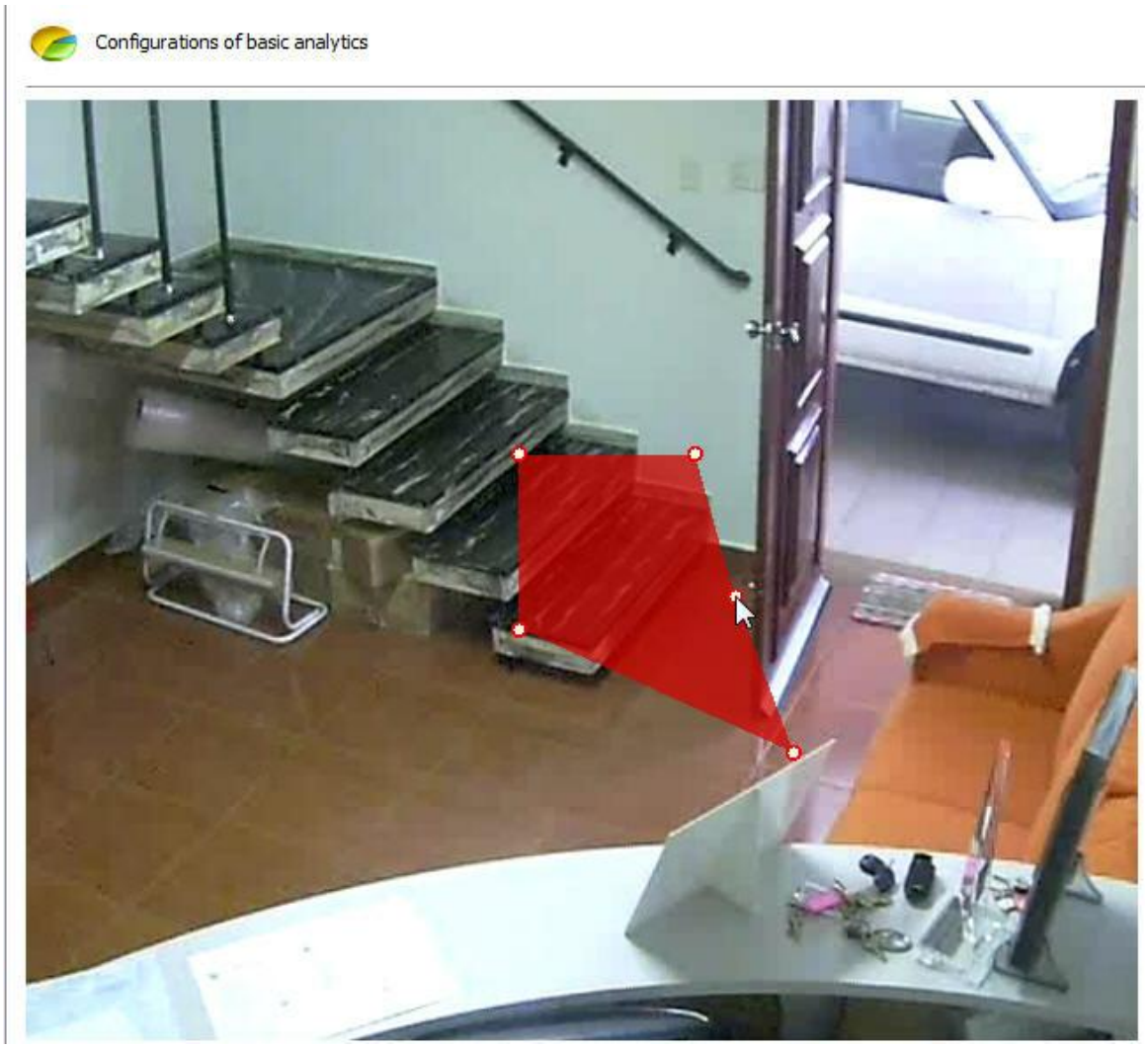
- **Abandoned objects**: analysis module of abandoned objects. This module will be covered in the chapter Configuring the rule of abandoned objetcs
- **Removed Objects**: Removed objects Analysis module. This module will be covered in chapter configuring the rule removed objects Configuring the rule removed objects

You can move the points in the area by clicking on the circles, as shown in the picture below:



And add points with a double-click near the area's edge as shown below:

© 2002 - 2020 by Digifort, all rights reserved



20 is the maximum number of points per area.
These same rules apply to lines.

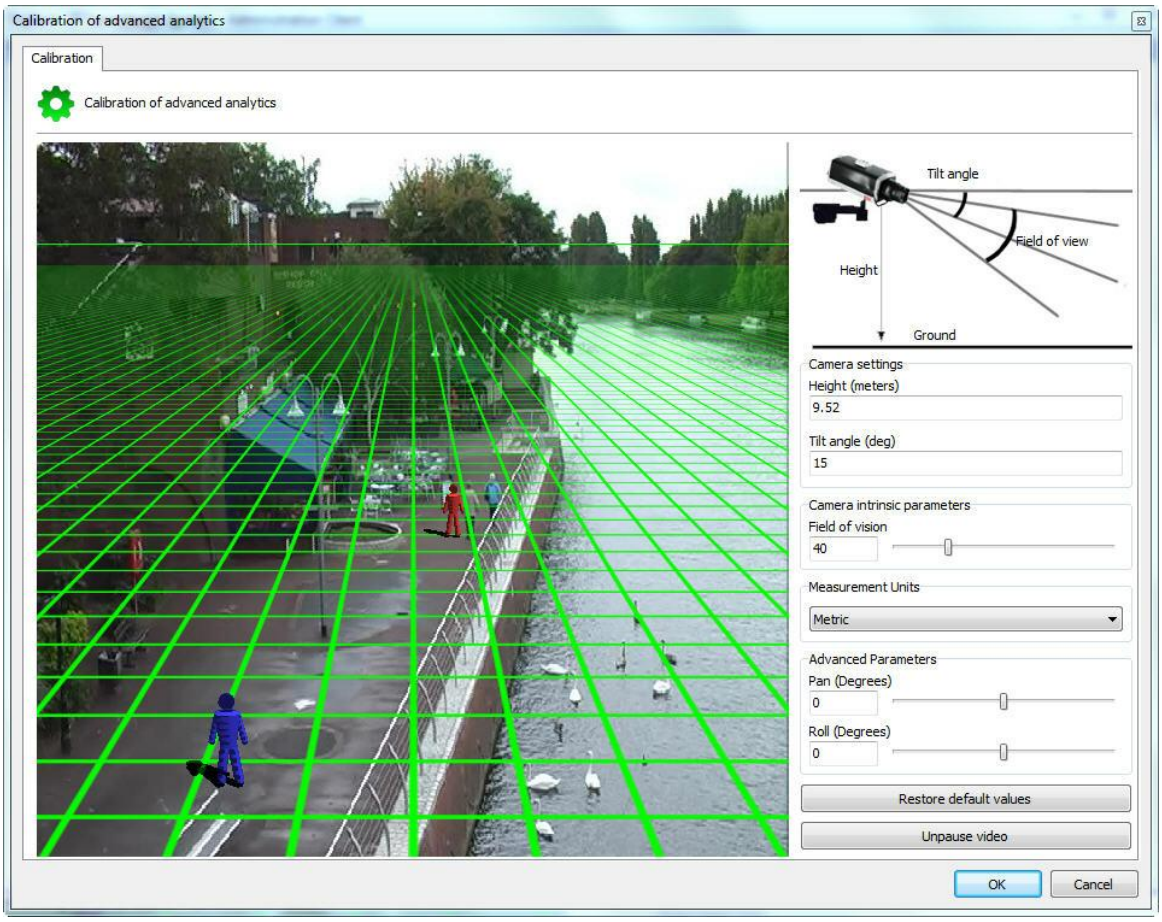
14.2.1.2.1 How to calibrate the analytics

The advanced analytics need to include calibration configurations so that it may operate suitably.

The first configuration is to calibrate the distances needed to get speed alerts and to classify objects such as cars, people, a group of people, etc.

To begin with, in the analytics configuration screen click on **Calibration**. The following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved



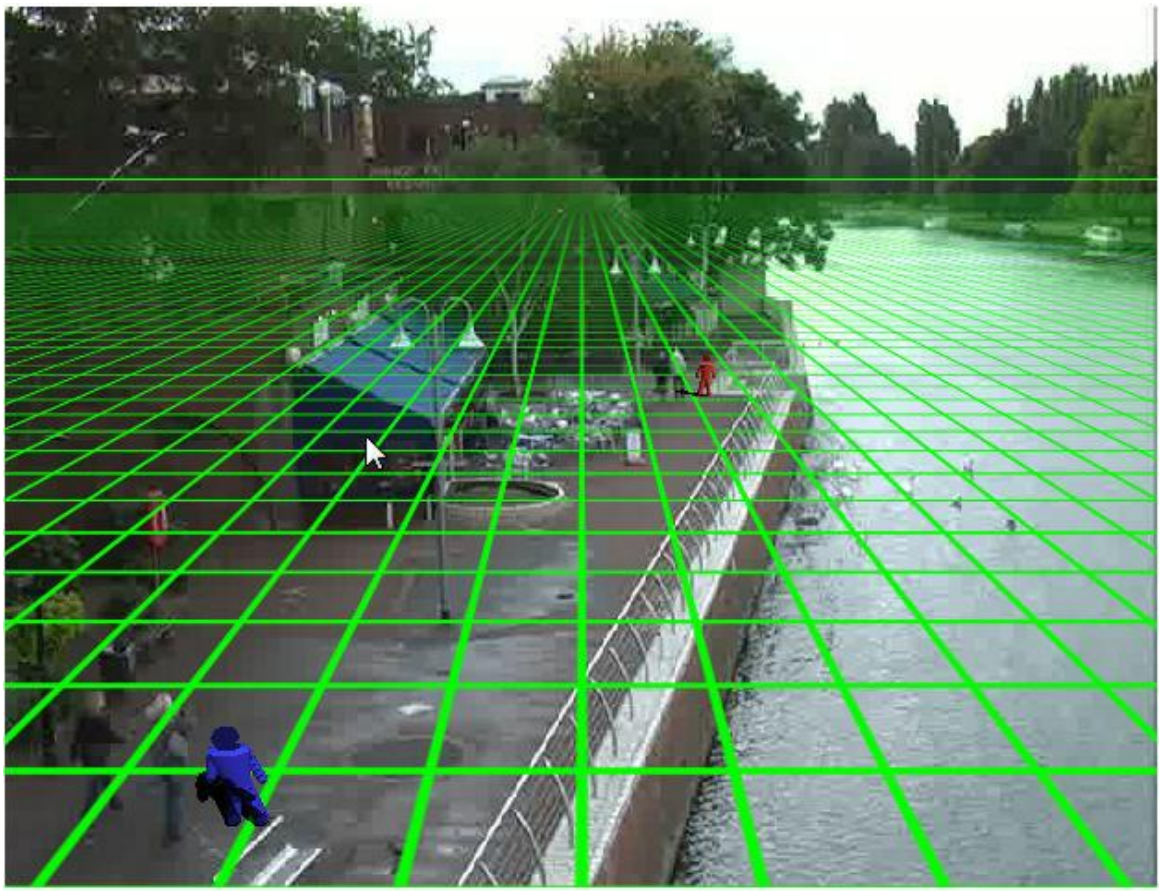
The image of the configured camera will appear in this screen as well as a 3DGrid.

If no command is activated, messages will appear on screen indicating how to operate the grid:

- Measure or estimate the distance between the camera and the ground.
- Use the wheel on the mouse to regulate the height of the camera.
- Click and drag the grid to change the vertical angle of the camera.
- Click and drag the 3D people to compare with the people on the image.
- Each square on the grid is equivalent to 2x2 metres.

For easier configuration, first move the grid so that the horizon line is compatible with the image, as shown in the picture below:

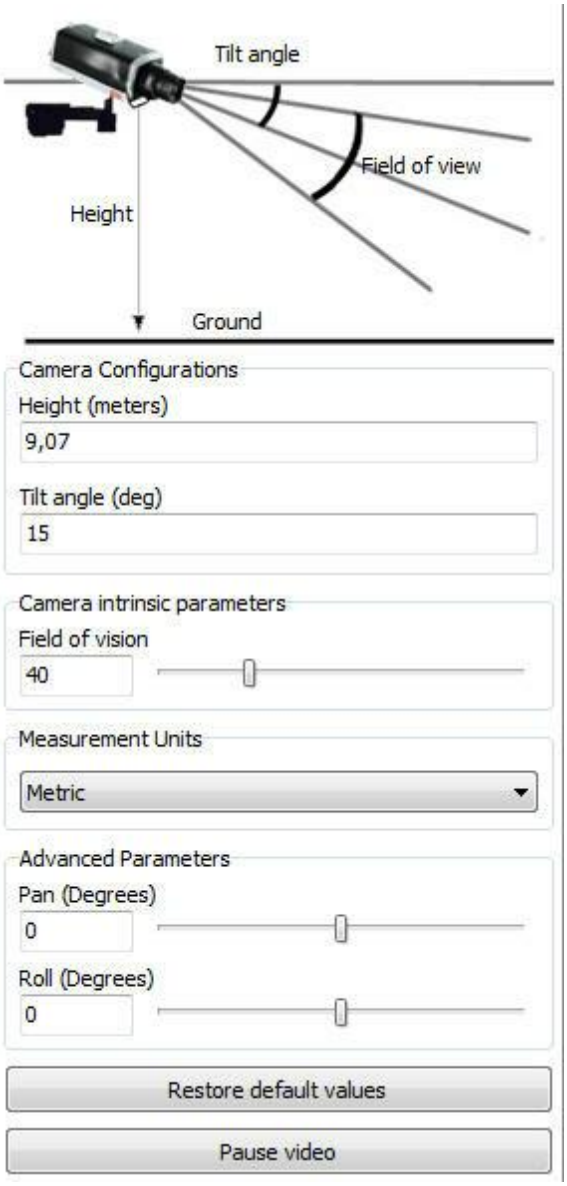
© 2002 - 2020 by Digifort, all rights reserved



In the configuration above you can see the line of the horizon on the grid compatible with the image, and the 3D figure with an approximate size to that of the people in the image.

Done! The grid is configured.
If you have precise measurements of the camera's position on site, the menu on the right can also help you configure the grid:

© 2002 - 2020 by Digifort, all rights reserved



The menu has the following features:

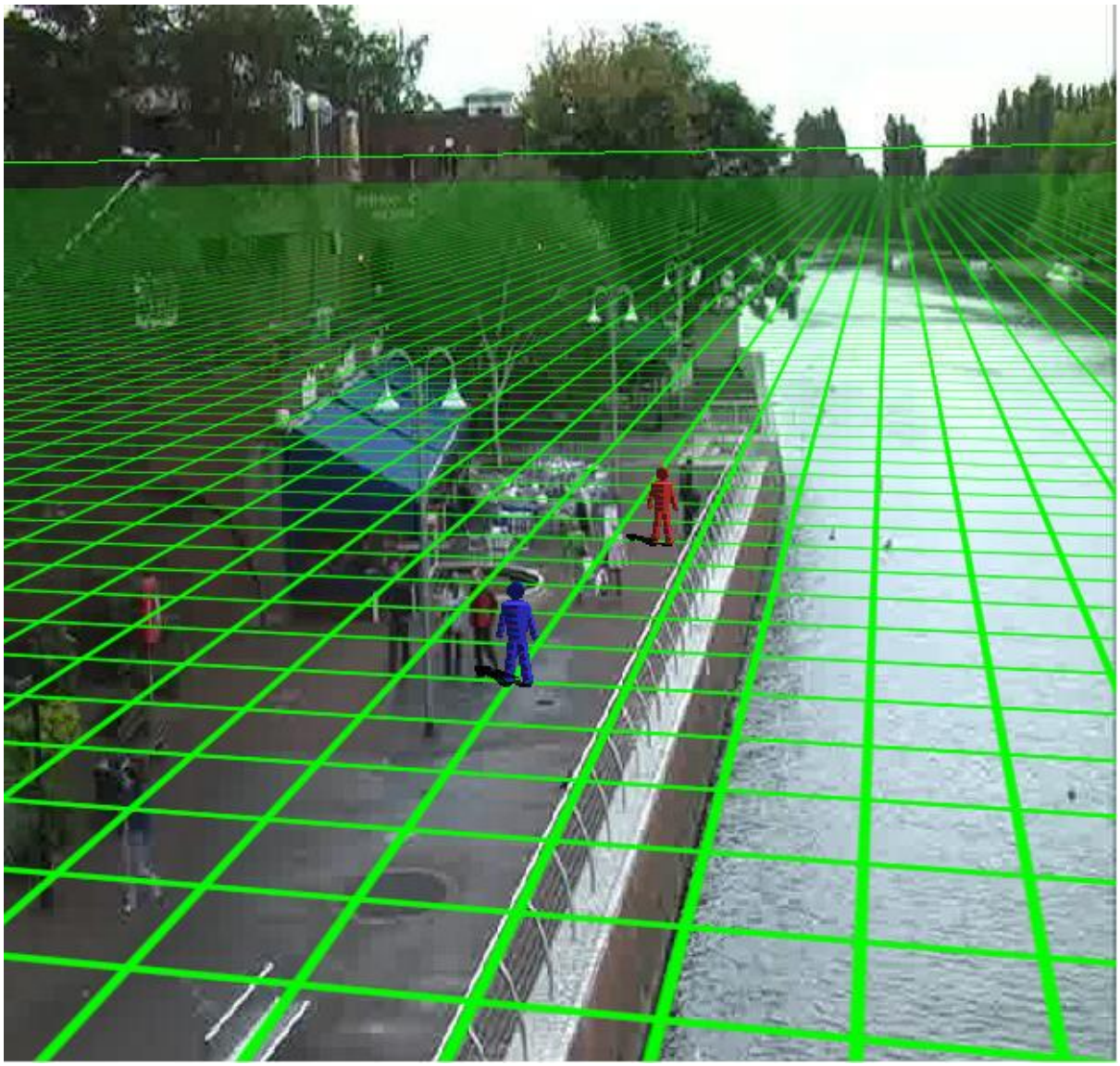
- **Height**: Height in meters that the camera is in relation to the ground.
- **Tilt Angle:** Vertical angle of the camera.
- **Field of vision:** Field of vision of the camera.

These values are changed automatically regulates the placement of the Grid.

- **Units of measurement** It is possible to change the type of measurement to meters in Imperial measurement unit field.

Advanced Parameters: Use the parameters below to a thinner adjustment of grid as in the figure below.

© 2002 - 2020 by Digifort, all rights reserved



- **Pan (Degrees):** Rotate the grid on the Y axis of the Cartesian plane.
- **Roll (Degrees):** Rotate the grid on the Z axis of the Cartesian plane.

Restore default values: Restores the original values of the positioning grid.
Pause video: Allows the video to be paused from the camera to adjust the grid

With the grid correctly configured we can sort the objects to be detected, for example: People from 2 to 3 meters of height walking at a speed from 1km to 8km. See the next chapter to learn how to sort the objects

14.2.1.2.2 How to classify objects

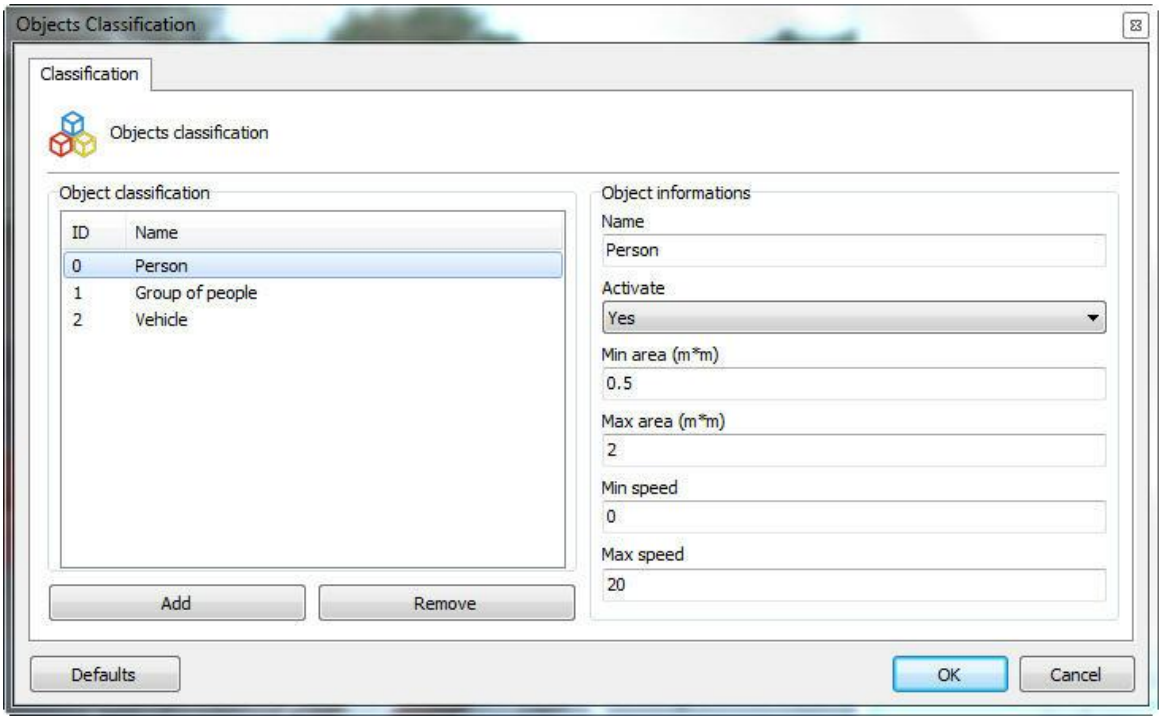
The advanced analytics stores what type of objects triggered the alerts and filters them, for example,

© 2002 - 2020 by Digifort, all rights reserved

by cars, people, groups of people, animals, etc. Example: An area can trigger alerts only when there are people circulating or only when cars are motionless.

When the **Calibration** has been made correctly, you can create object classifications.

To begin with, in the analytics configuration screen click on Classification. The following screen will show up:



At first, there won't be any objects registered. To register an object, fill in the fields and click on Add. The picture above shows what the registration for "person" would be like.

The fields to be filled in are described below:

Name: Name of the classification to be added.
Activate: The classification can be deactivated at any given time; simply change the selection box to No.
Min. area: The minimum area the object must have to be recognized within that classification.
Max. area: The maximum area the object must have to be recognized within that classification.
Min. area: The minimum area the object must have to be recognized within that classification.
Max. area: The maximum area the object must have to be recognized within that classification.

To remove any classification, simply select it on the list and click on **Remove**.
Segue o resultado dessa classificação no monitoramento:

© 2002 - 2020 by Digifort, all rights reserved



To learn how to view the analytics' functionalities live, refer to the surveillance client.

14.2.1.2.3 How to configure the Analytics' Rules

Each analytics analysis module (Entry, Motionless, Presence) is considered a rule which, in turn, is applied to an area.

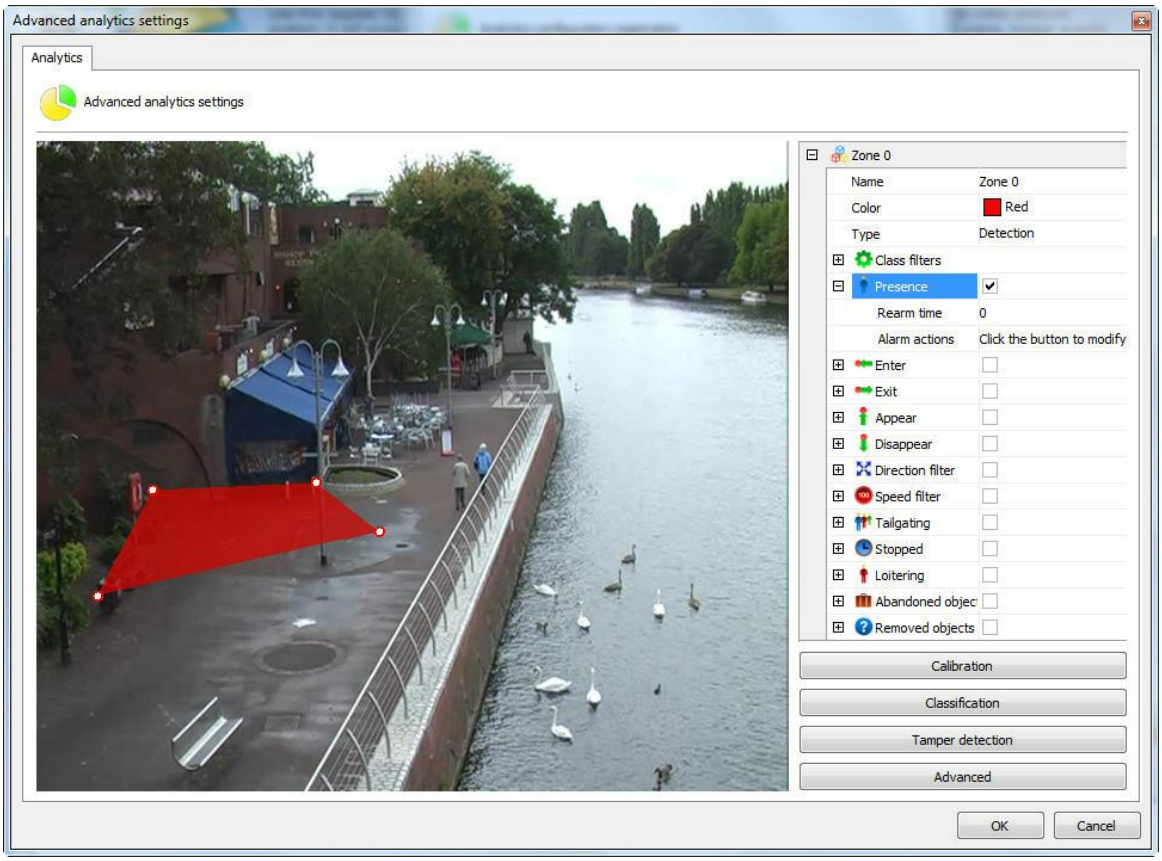
We will now see how to configure all the analytics rules and alerts in areas for different situations.

14.2.1.2.3.1 How to configure the Presence rule

The Presence rule can trigger an alert if it detects an object within a certain area.

Let's configure a presence alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on Presence. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:

In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

Note

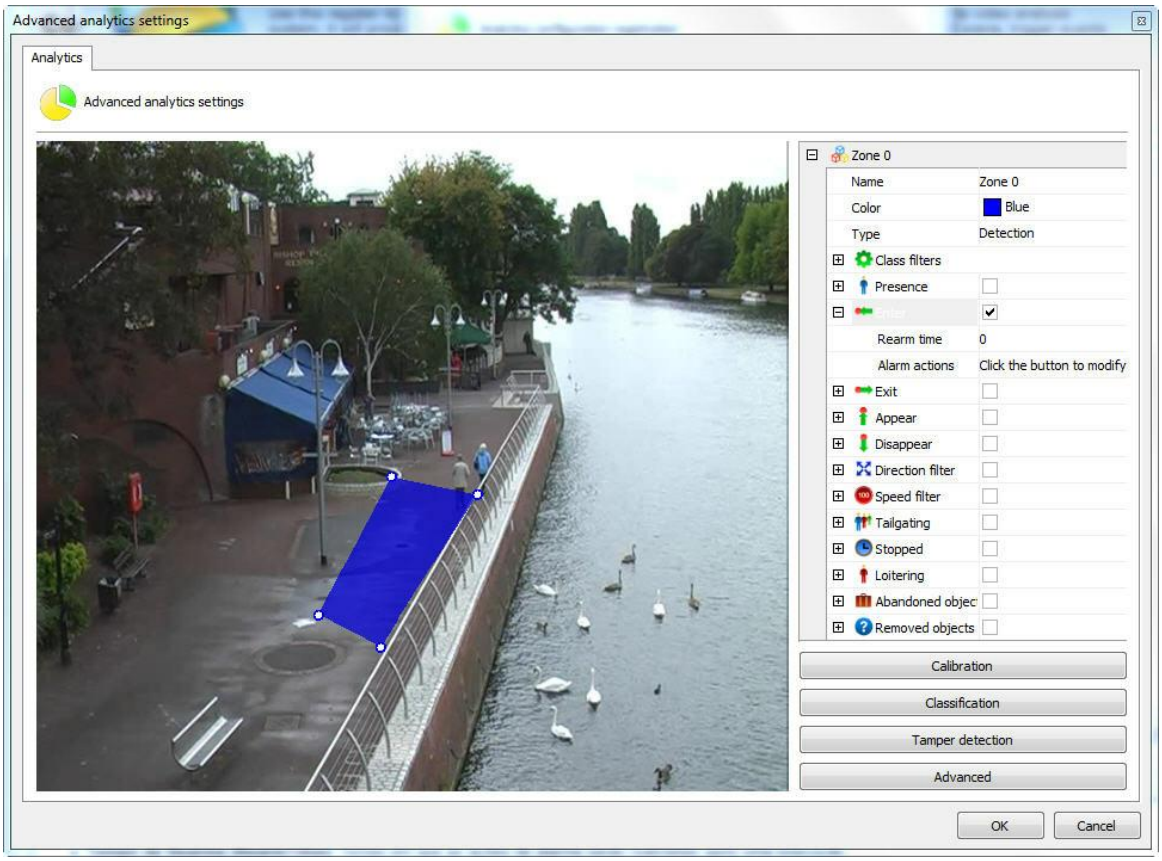
The presence rule indicates the number of objects detected within its area. The detected object can, for example, be 4 people standing close together and in that case the count info is 1 not 4.

14.2.1.2.3.2 How to configure the Entry rule

The **Enter** rule can trigger an alert if it detects an object entering a certain area.

Let's configure an **Enter** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on **Enter**. The options for this rule are the following:

- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



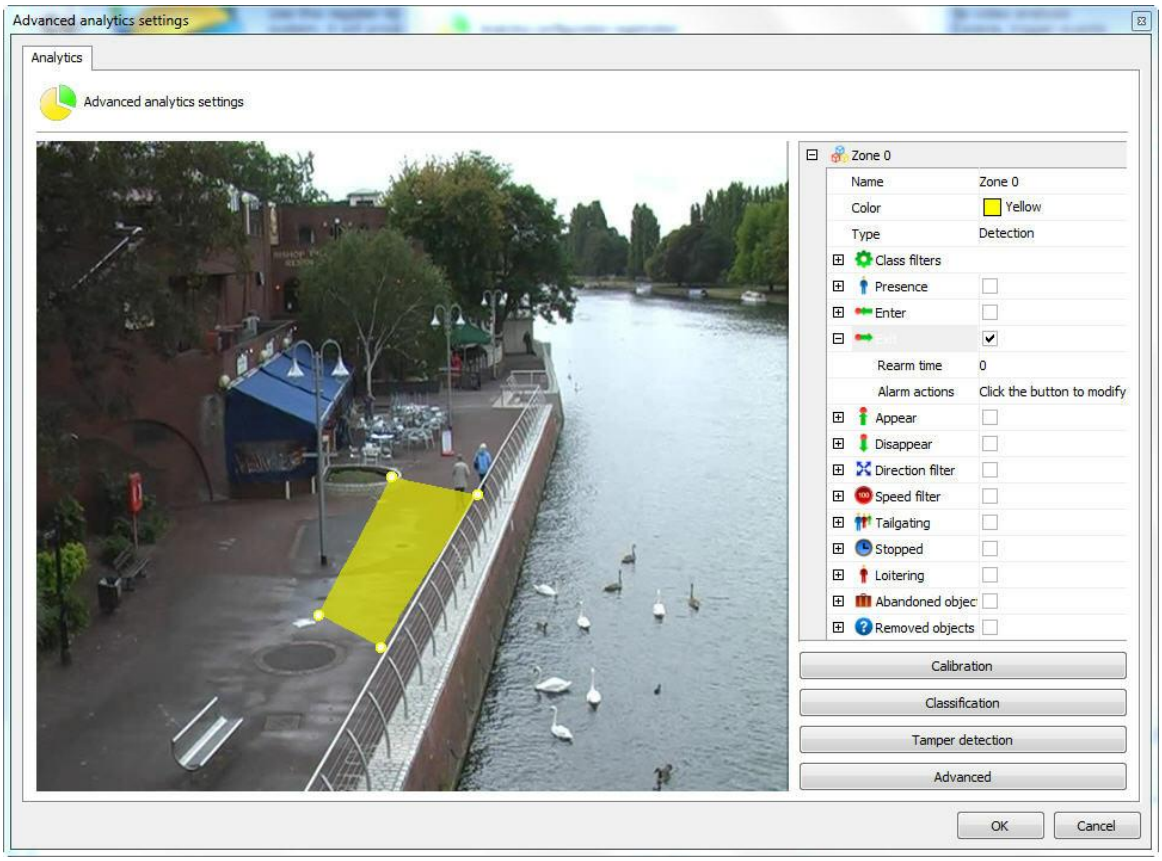
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

14.2.1.2.3.3 How to configure the Exit rule

The **Exit** rule can trigger an alert if it detects an object leaving a certain area.

Let's configure an **Exit** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on Exit. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions:** Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



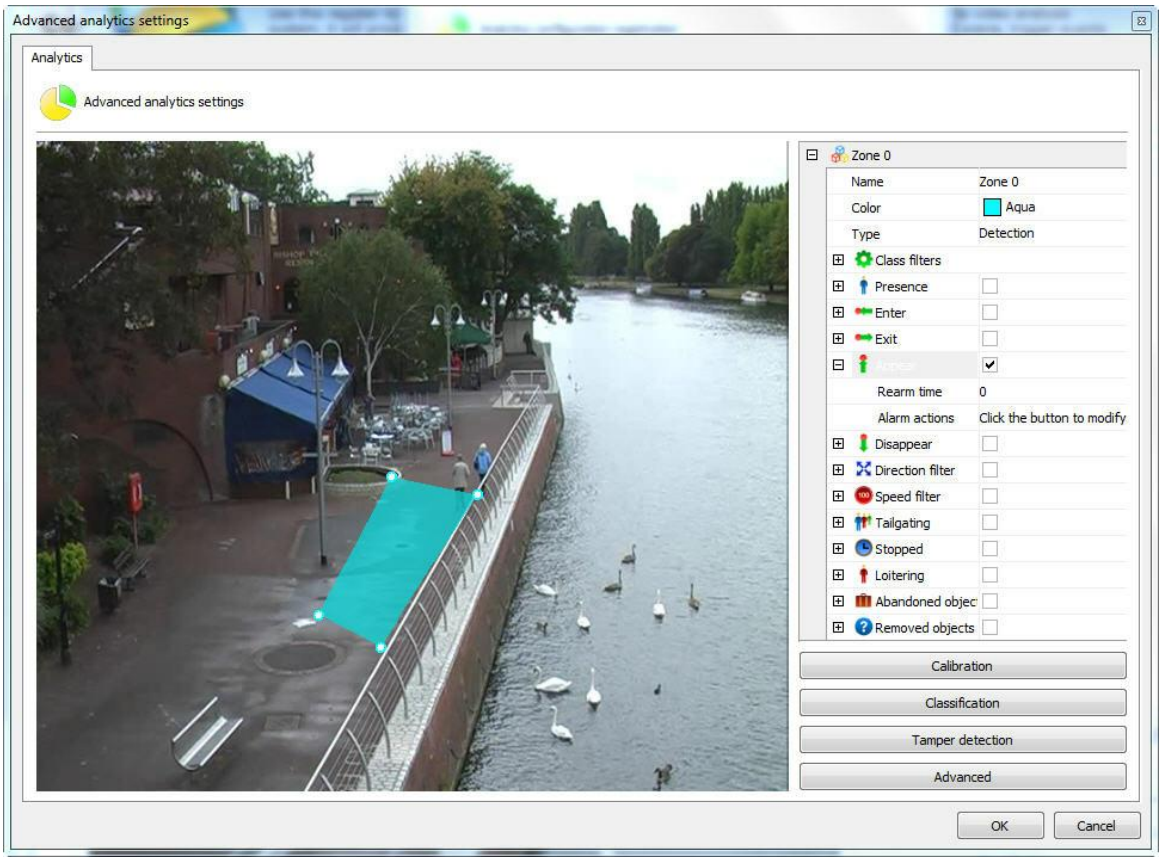
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

14.2.1.2.3.4 How to configure the Appear rule

The **Appear** rule can trigger an alert if it detects an object appearing in a certain area.

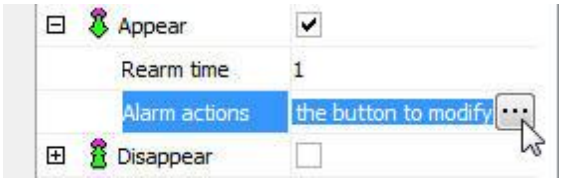
Let's configure an **Appear** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on **Appear**. The options for this rule are the following:

- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



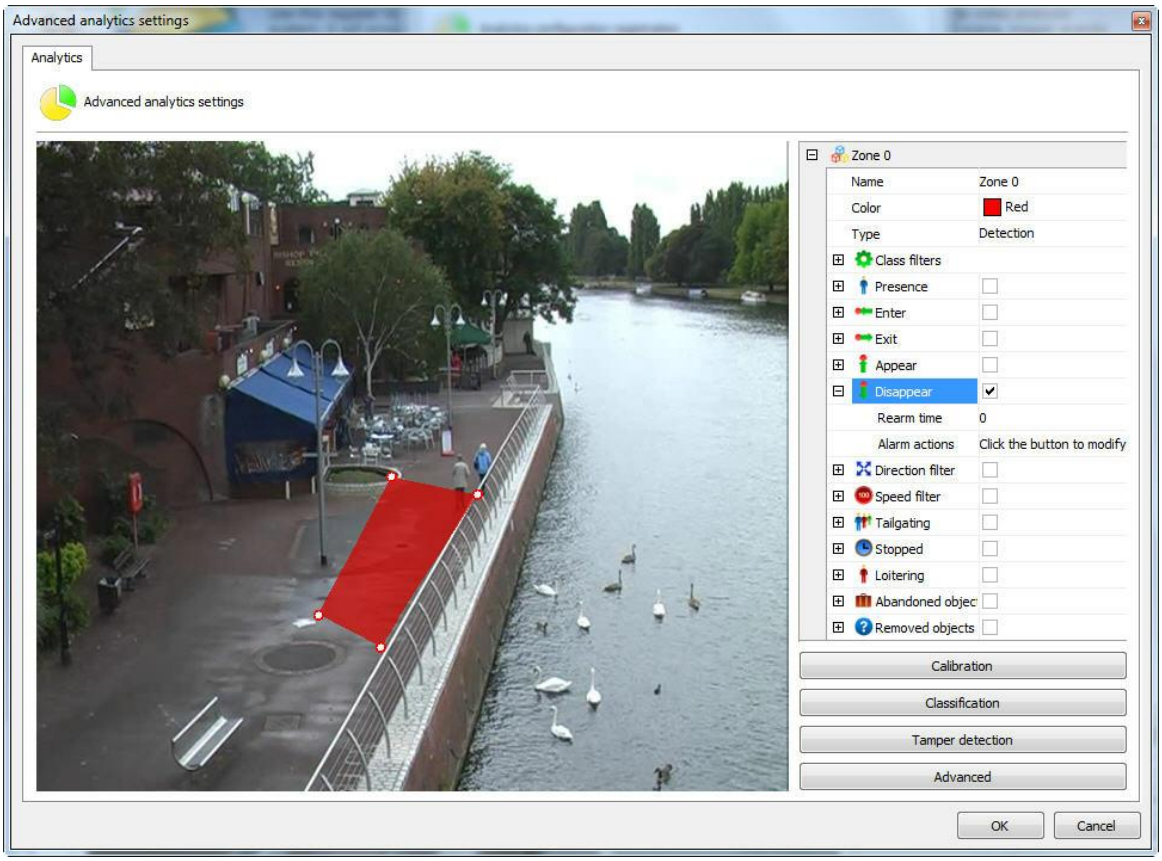
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

14.2.1.2.3.5 How to configure the Disappear rule

The **Disappear** rule can trigger an alert if it detects an object disappearing from a certain area.

Let's configure a **Disappear** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on **Disappear**. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



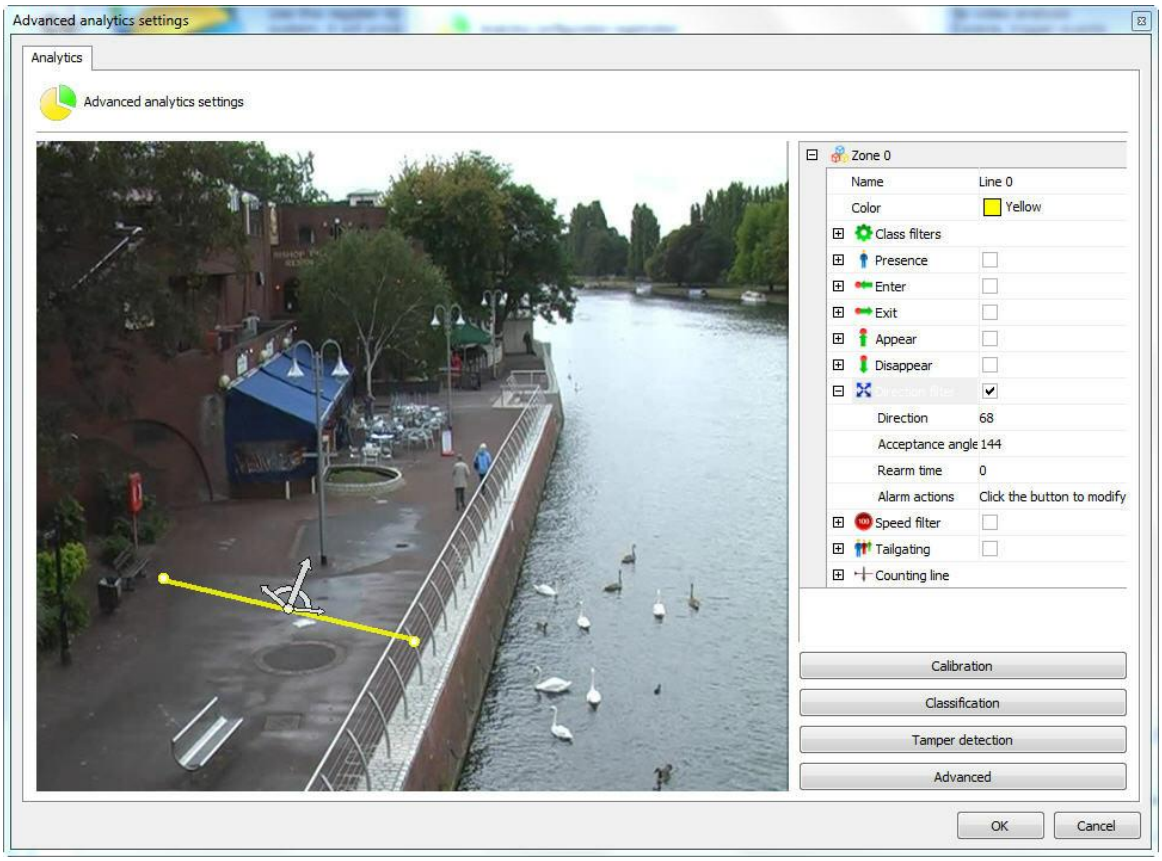
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

14.2.1.2.3.6 How to configure the Direction Filter rule

The **Direction Filter** rule can trigger alerts if it detects objects in configured directions.

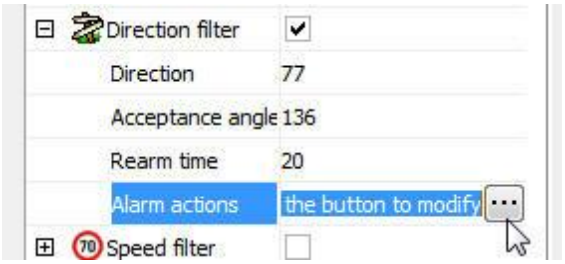
Let's configure a **Direction Filter** alert from a line. A line has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the line selected, click on the **Direction filter** rule. The options for this rule are the following:

- **Direction**: Direction within an angle in which the object must move along to trigger the alert.
- **Acceptable angle**: The acceptable angle is a slight difference from the main angle, that is, the object will not go past at exactly 90 degrees (it will pass at 100, 80, 70) so, the wider the acceptable angle, the easier it is for the alert to set off.
- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



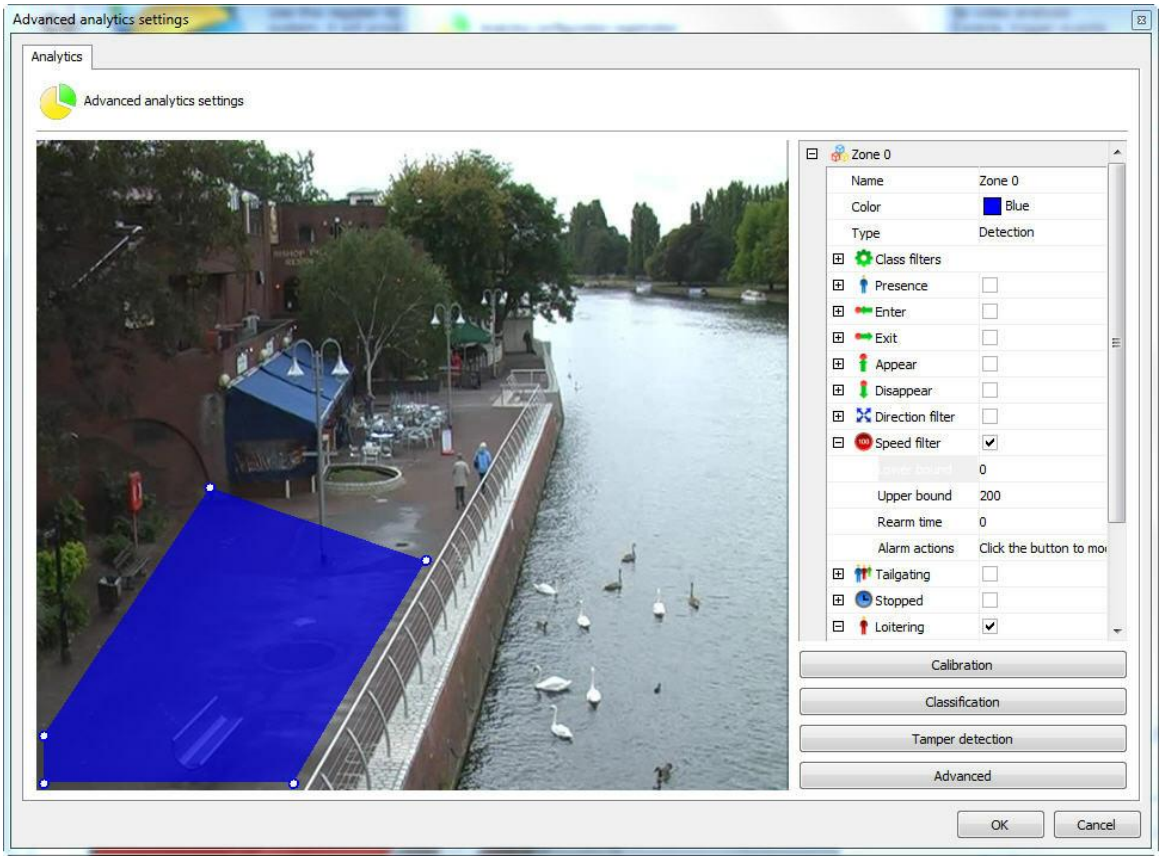
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

© 2002 - 2020 by Digifort, all rights reserved

14.2.1.2.3.7 How to configure the Speed Filter rule

The **Speed Filter** rule can trigger alerts if it detects objects at configured speeds.

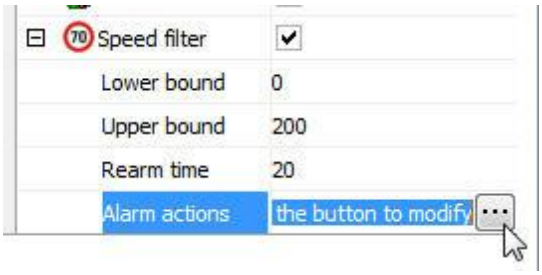
Let's configure a **Speed Filter** alert from an area. An area has been created in the previously calibrated image:



With the area selected, click on the **Speed filter** rule. The options for this rule are the following:

- **Minimum Speed**: The minimum speed that the object must be moving to trigger the alert for that rule.
- **Maximum Speed:** The maximum speed that the object must be moving to trigger the alert for that rule.
- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:

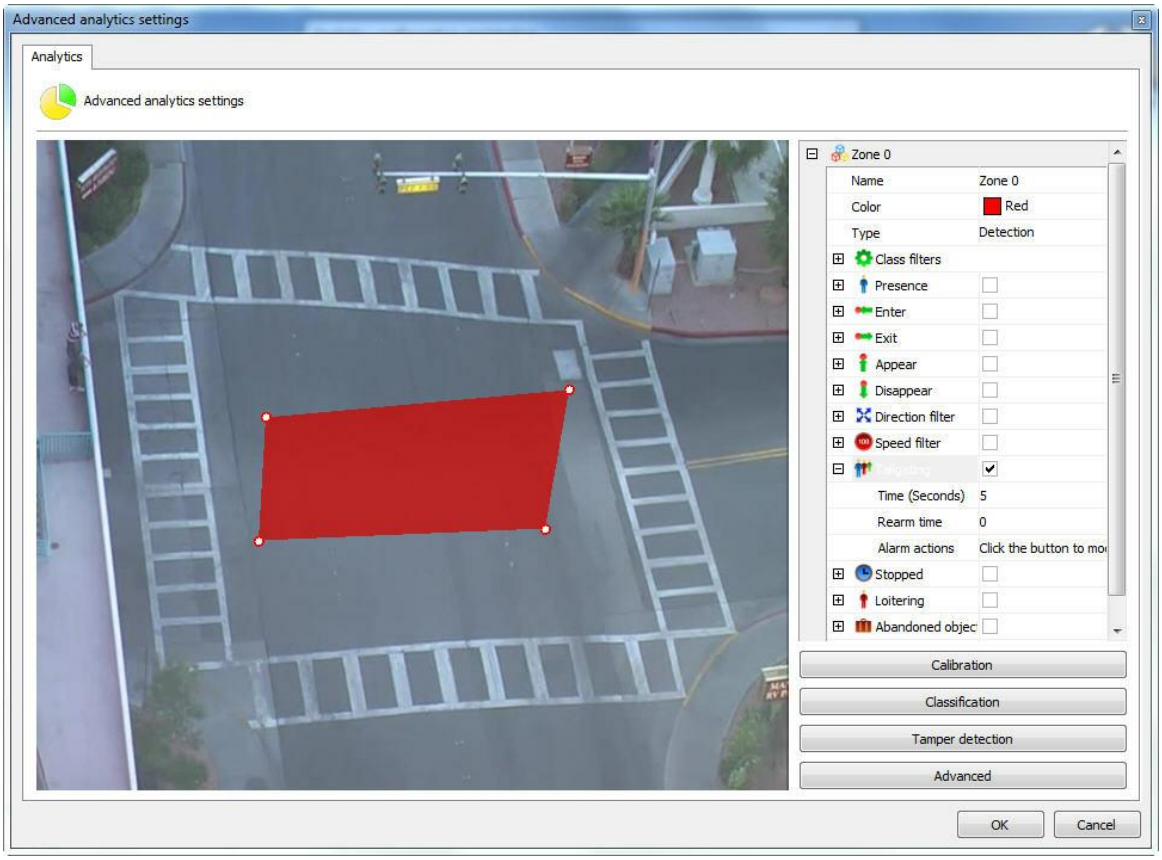
© 2002 - 2020 by Digifort, all rights reserved



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

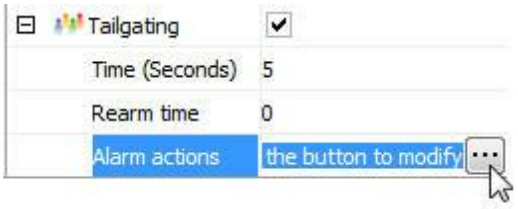
14.2.1.2.3.8 How to configure the rule of Tailgating

Tailgating rule can trigger an alarm when a second object passes in a given area within a configurable amount of time between the first object that previously went through the same area. We can exemplify an alarm when a car that goes along with another when one recalls toll rises.



- **Time**: Time in seconds between entry of objects in an area. If after the entry of an object in the area, a second object enter the time less than the configured, an alarm is triggered.
- **RearmTime:** Time alarm actions will be reactivated after a run.
- **Alarm actions**: Click on the line of alarm actions and soon after the button has 3 points as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved

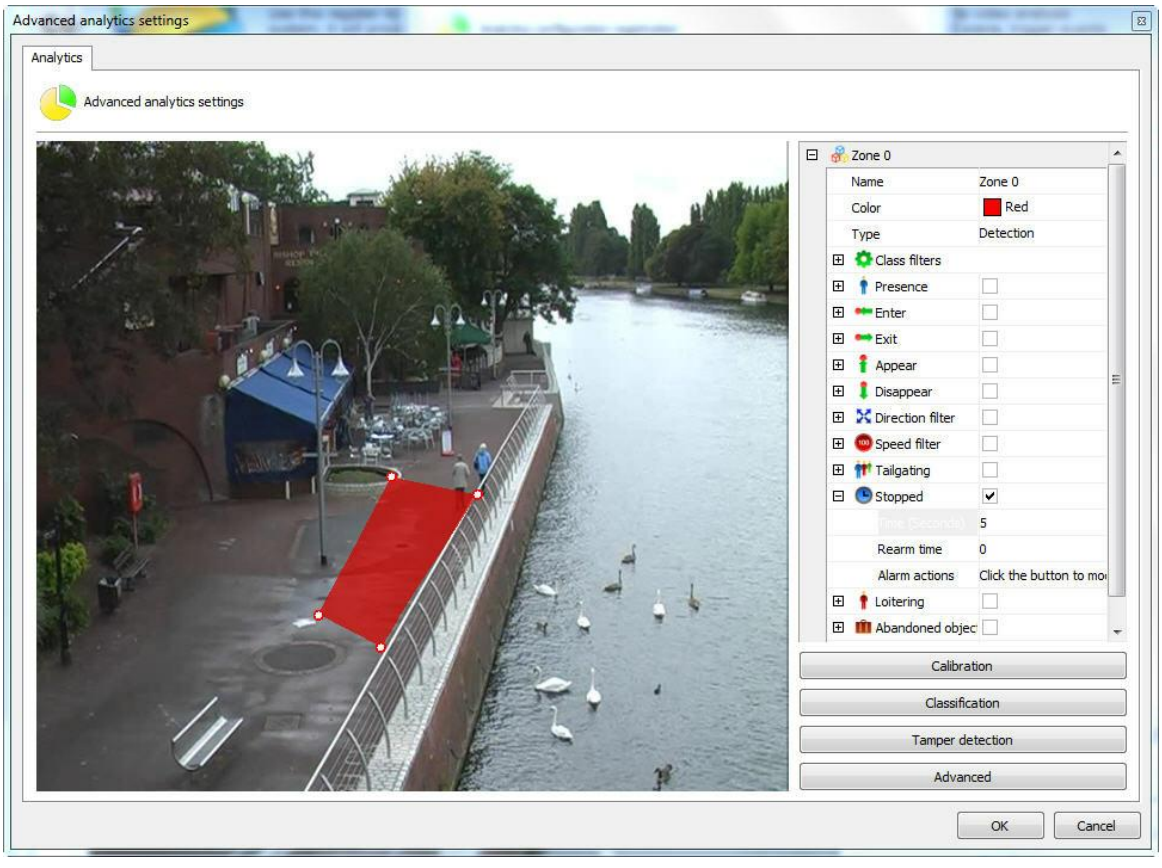


Configure alarms screen desired actions when the contents firing the events. To learn more about the actions of an alarm see chapter[How to configure alarm actions](#).

14.2.1.2.3.9 How to configure the Stopped rule

The **Stopped** rule can trigger an alert if it detects a motionless object in a certain area.

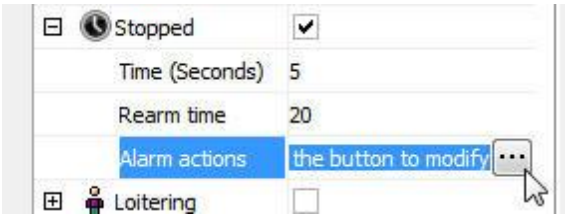
Let's configure a **Stopped** alert for a certain area. An area has been created in the previously calibrated image:



With the area selected, click on Motionless. The options for this rule are the following:

© 2002 - 2020 by Digifort, all rights reserved

- **Time**: Time the object has to remain motionless to trigger the alert.
- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions:** Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



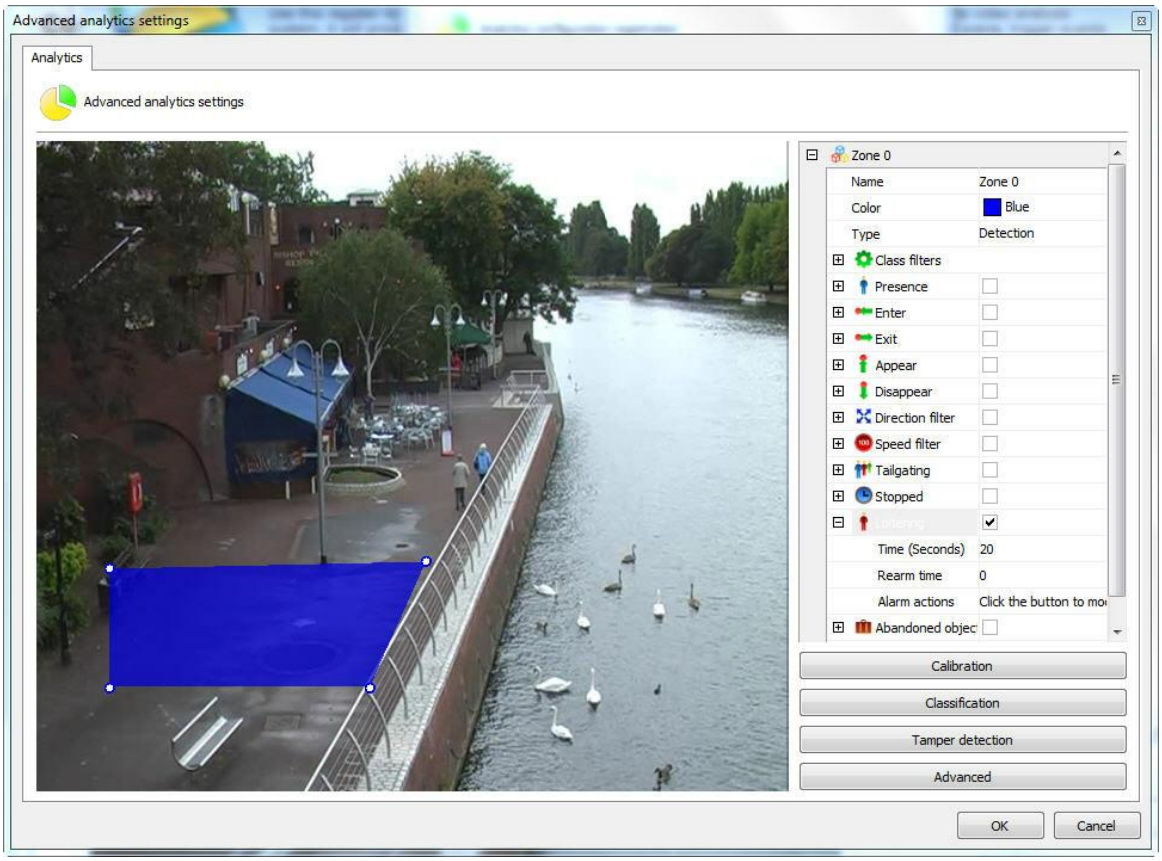
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

14.2.1.2.3.10 How to configure the Loitering rule

The **Loitering** rule can trigger an alert if it detects an object moving in a certain area for a certain amount of time.

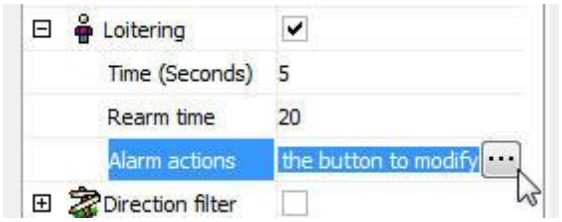
Let's configure a **Loitering** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



With the area selected, click on **Loitering**. The options for this rule are the following:

- **Time**: Time the object has to remain motionless to trigger the alert.
- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

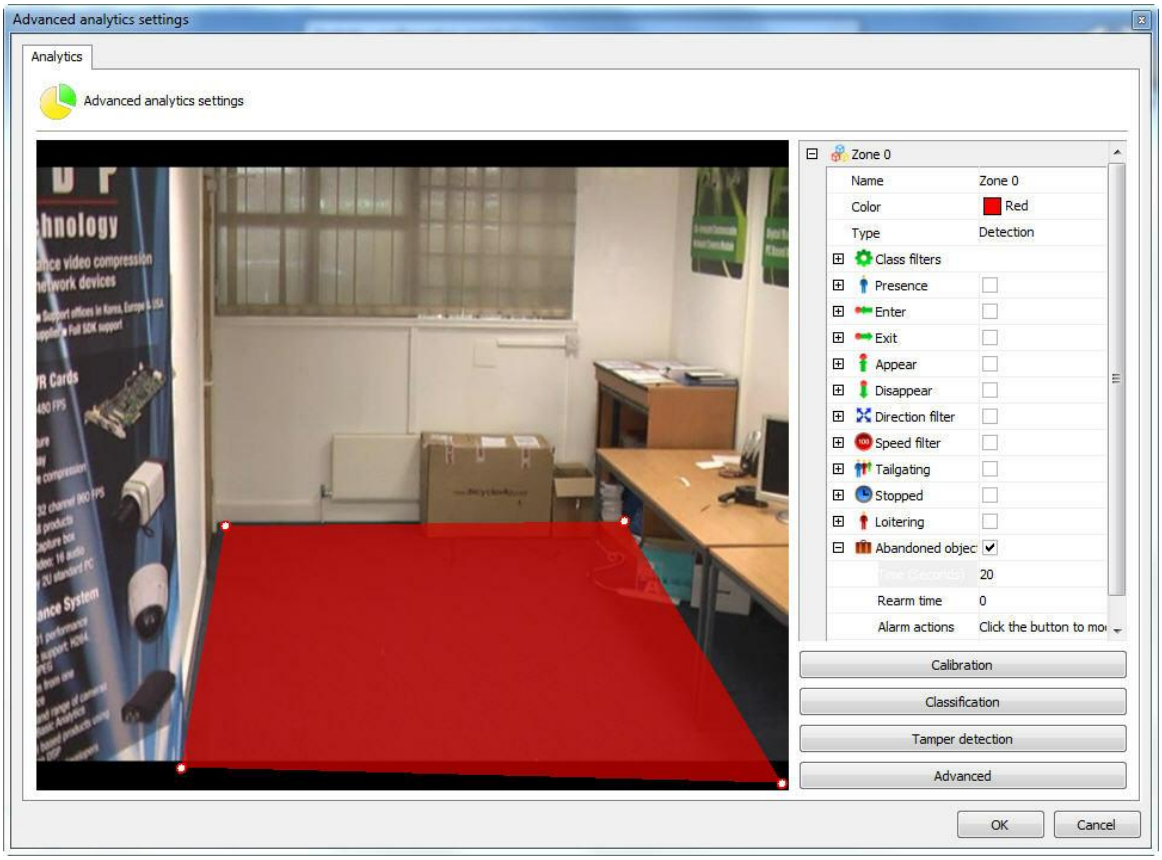
14.2.1.2.3.11 How to configure the rule of abandoned objects

The object module Left can generate alerts when an object is left in some area specifies the image or when something in the scene is changed. Example: A suitcase left in the ground, a key that

© 2002 - 2020 by Digifort, all rights reserved

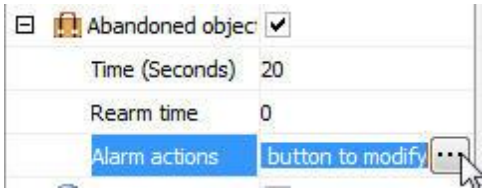
appears on top of a table. From these events it is possible to retrieve the video, generate alarms and reports.

In our example was created a detection area in the figure below:



Opening the options side of **Abandoned objetcts** have the following features:

- **Abandoned objetcts:** Tick this option to activate the objects Left in this area.
- **Rearm time:** Reset time for which the alarm will be activated again in monitoring client (if configured).
- **Time**: Time in seconds that the object must remain stationary in the zone to which the alarm is triggered. It is not recommended in places with a lot of movement.
- **Alarm Actions**: Click on the line of alarm actions and soon after the button has 3 points as shown in the figure below:



Configure alarms screen desired actions when the contents firing the events. To learn more about the actions of an alarm see chapter How to configure alarm actions.

© 2002 - 2020 by Digifort, all rights reserved

Here is an example where the alarm was triggered in the situation previously configured:



To learn how to generate the reports, consult our customer tracking

Note

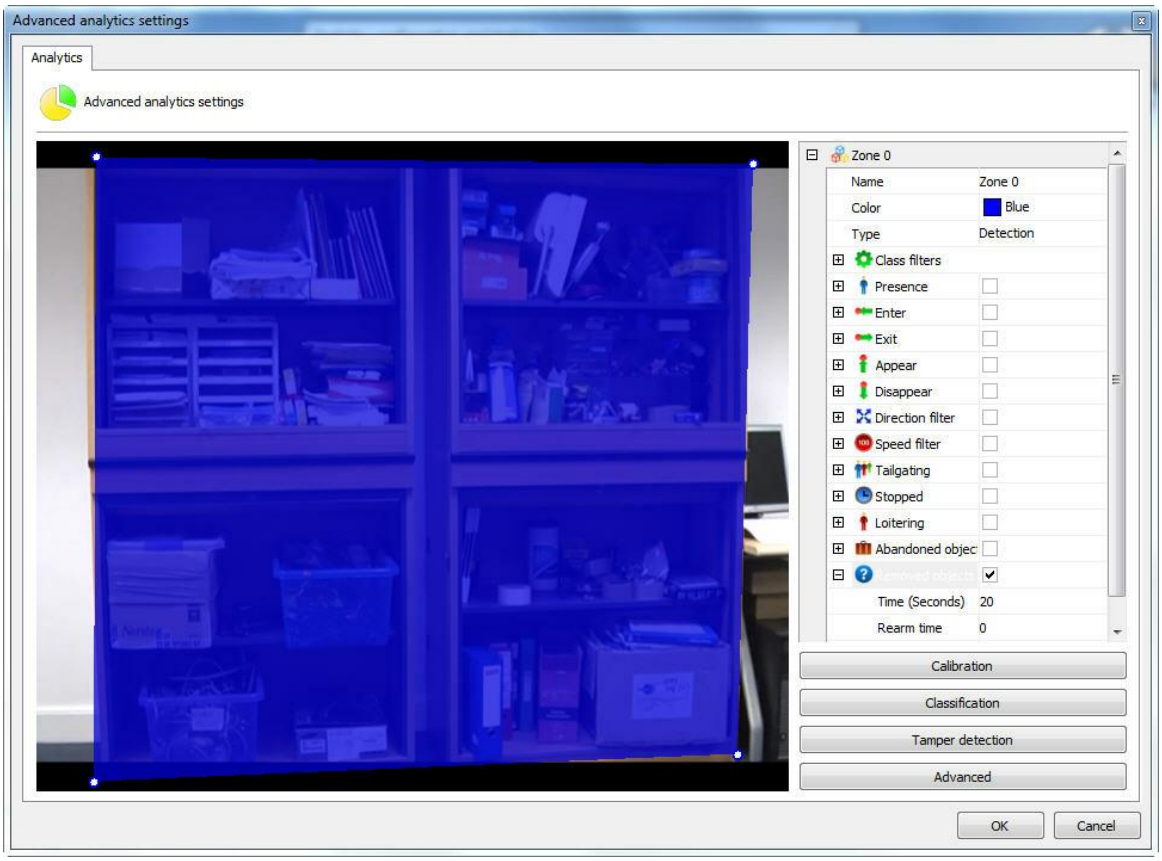
The module will trigger alarms objects left in any change of scenario, i.e. when both objects are removed or when they are left.

14.2.1.2.3.12 How to configure the rule removed objects

Remove Objects module can generate alerts when a marquee object is removed from the scene. Example: A framework, value object, etc. From these events it is possible to retrieve the video, generate alarms and reports.

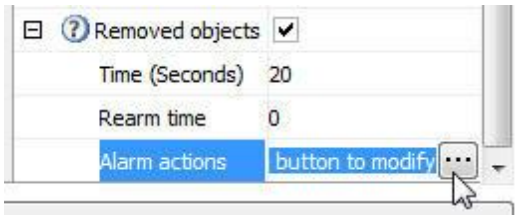
In our example was created a detection area in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



Opening the options side of Objects left (Foreign Objects) have the following features:

- **Abandoned Objects:** Tick this option to activate the objects Left in this area.
- **Rearm time**: Reset time for which the alarm will be activated again in monitoring client (if configured).
- **Time**: Time in seconds that the object must remain stationary in the zone to which the alarm is triggered. It is not recommended in places with a lot of times great movement.
- **Alarm Actions:** Click the row of alarm actions and soon after the button has 3 points as shown in the figure below:



Configure alarms screen desired actions when the contents firing the events. To learn more about the actions of an alarm see chapter how to configure alarm actions.

Here is an example where the alarm was triggered in the situation previously configured:

© 2002 - 2020 by Digifort, all rights reserved



To learn how to generate the reports, consult our customer tracking.

Nota

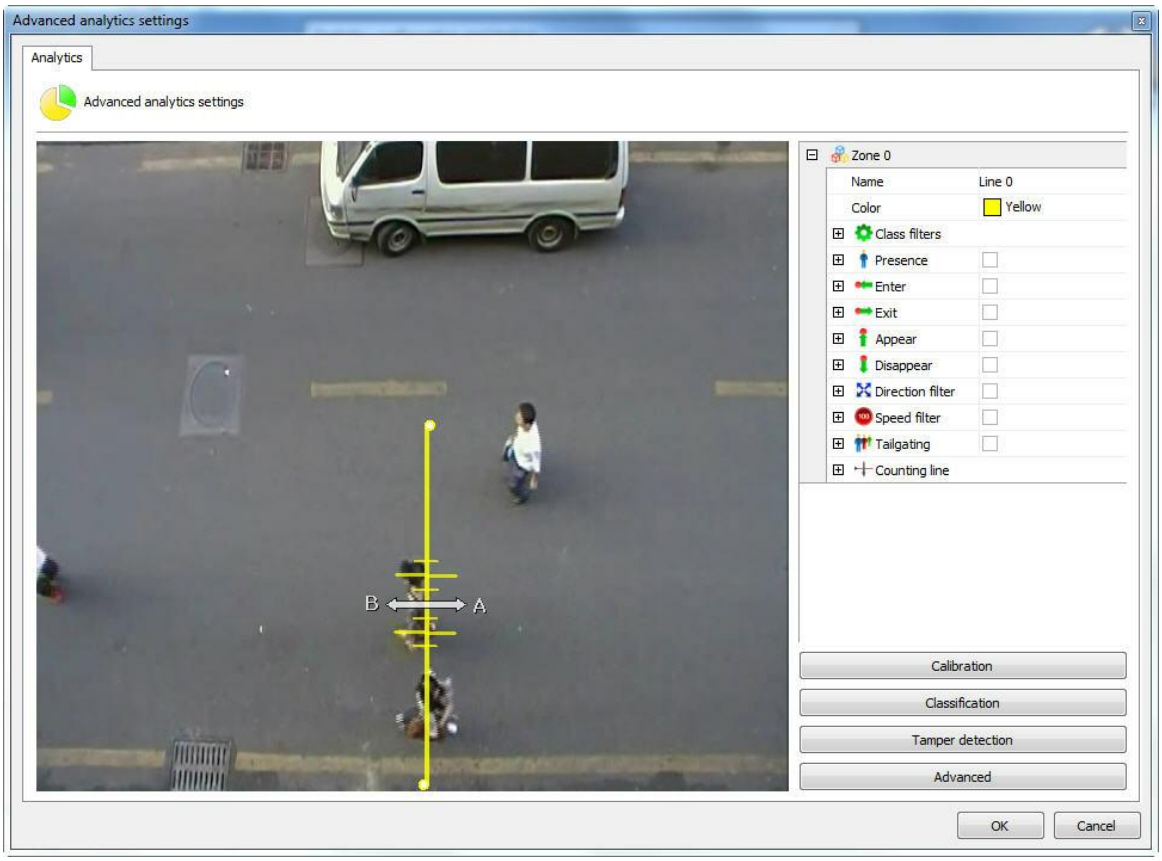
The module will trigger alarms objects left in any change of scenario, i.e. When both objects are removed or when left.

14.2.1.2.3.13 How to configure the rule counting line

The **counting line** is meant to count the objects that are in the picture, more specifically people.

Let's configure the count line from a common line. In the picture below was created a row in the calibrated image:

© 2002 - 2020 by Digifort, all rights reserved



A linha de contagem oferece as seguintes opções de configuração:

- **Direction A**: Specifies that there will be count for the left side of the row
- **Direction B**: Specifies that there will be count for the right side of the row
- **Calibration**: Calibration of the size of the object to be contact. This calibration may be made directly by the line. In the case of the figure above, crossing the line count exists red straight 6, where the major refers to the size of the object to be contact, i.e. the larger straight will between these two would be the size of a person's shoulders. Note that in order for this to work well the camera count should stay well above the objects, in the case of individuals, the head and shoulders should be more visible in the image. Below is an example of proper positioning and camera: count line

© 2002 - 2020 by Digifort, all rights reserved



E

The red arrow in the image shows where the line count.

- **Shadow filter:** If there is interference from the shadows on the spot, this filter can help minimize the effect.

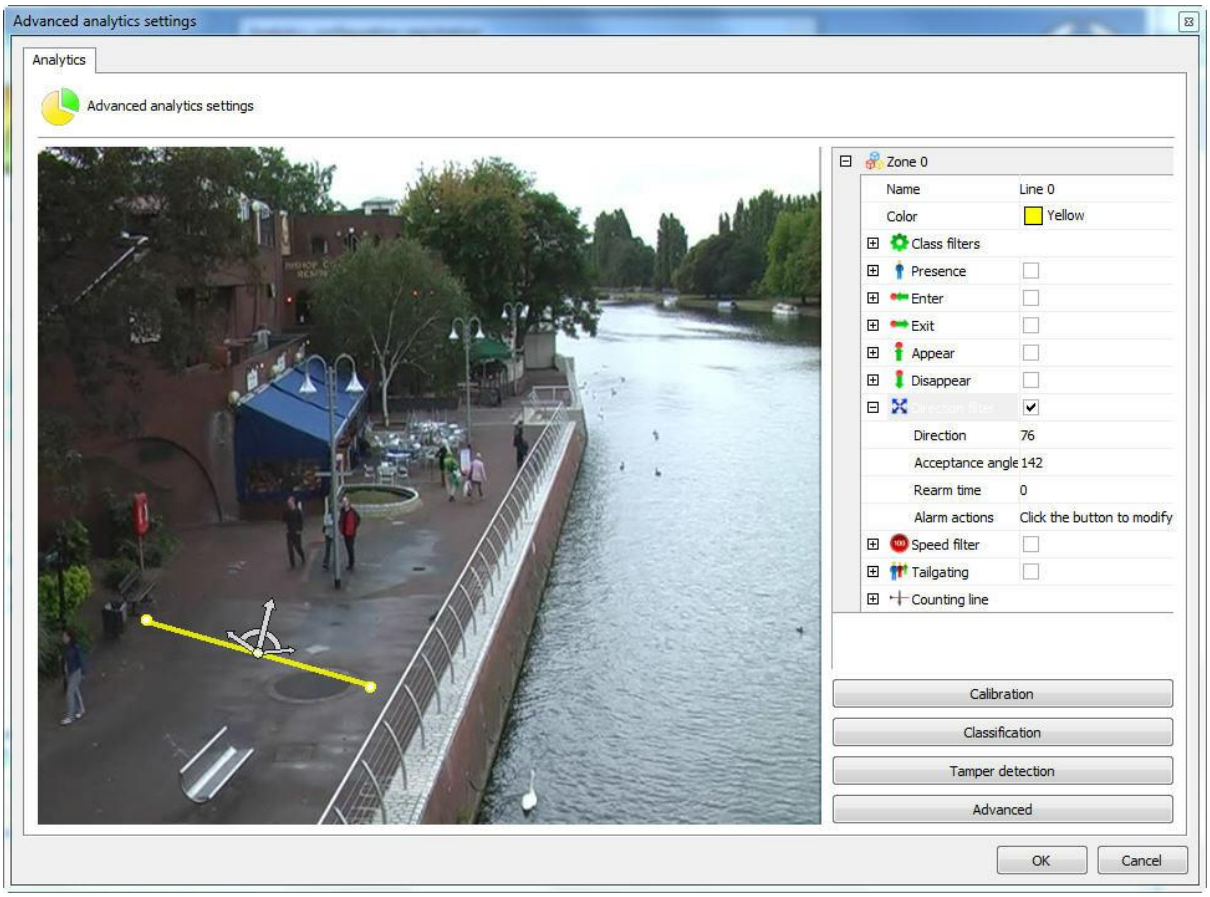
14.2.1.2.4 How to configure the counters

The counters have visual objects that in real time allow to get information on the events taking place in the image surveillance.

Counters are Incremented or Decremented by configured events. Let's see some examples.

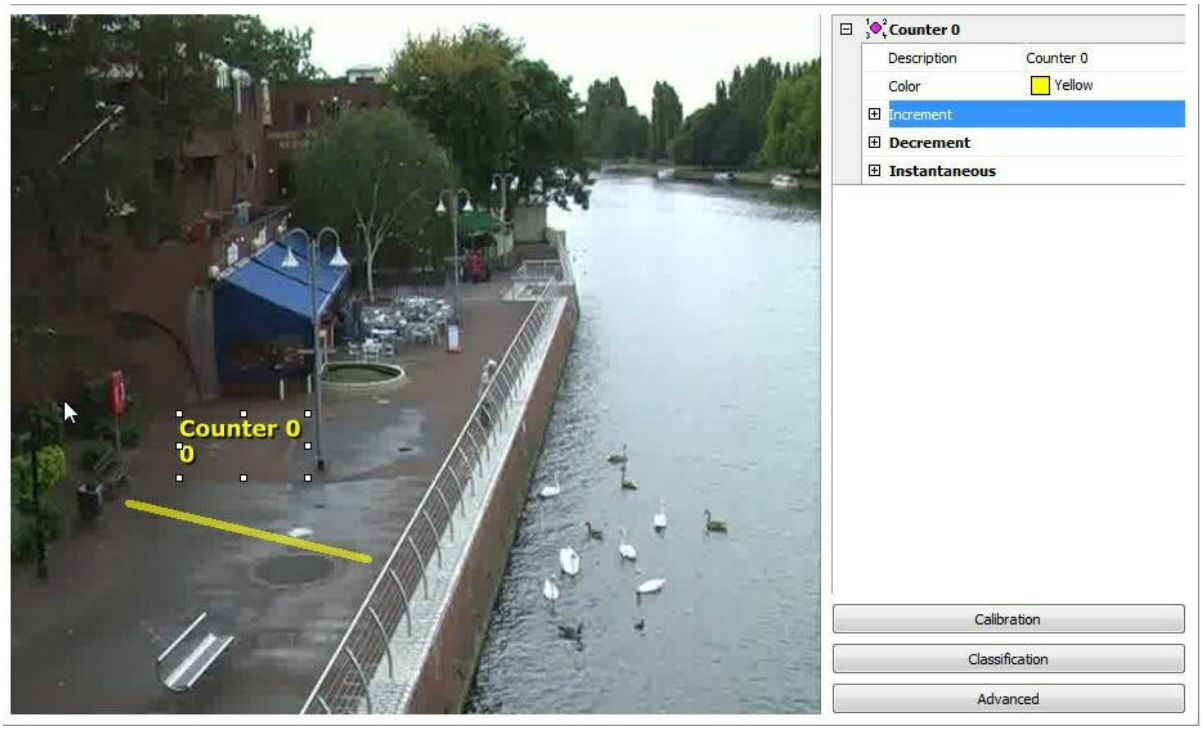
In the picture below a Direction Filter rule has been configured.

© 2002 - 2020 by Digifort, all rights reserved



We will configure a counter so that each object that activates this event will automatically be incremented by a counter. To do that, click with the right-hand button of the mouse on the screen and create a counter like the picture below:

© 2002 - 2020 by Digifort, all rights reserved



Some options are available in the menu on the right:

- **Increment:** Increments the counter according to the rules available.
- **Decrement:** Decrements the counter according to the rules available.
- **Instantaneous:** Returns the current value of the rules that are activated.

To understand better, let's see how to use the features above.

At first we will only increment the counter with direction rule that we created. To do that, open the **Increment** option and in Rule select the type of rule that you want to increment (in this case we only configured the Direction Filter, so it is the only one available).



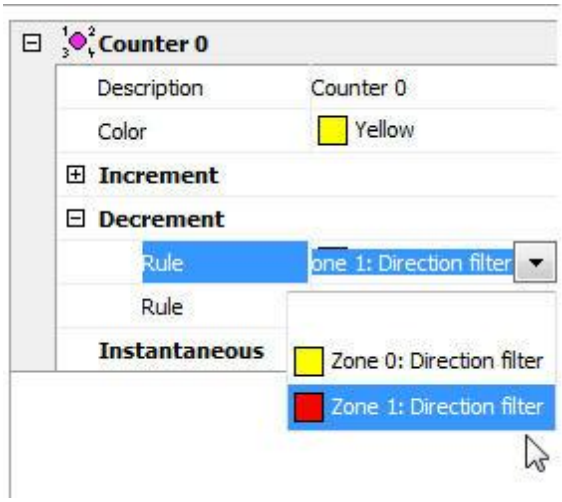
When you select the rule you'll see that another **Rule** field will open and it could be used to apply another rule to increment the counter.

© 2002 - 2020 by Digifort, all rights reserved

Now we'll create another **Direction Filter** field as shown in the picture below:



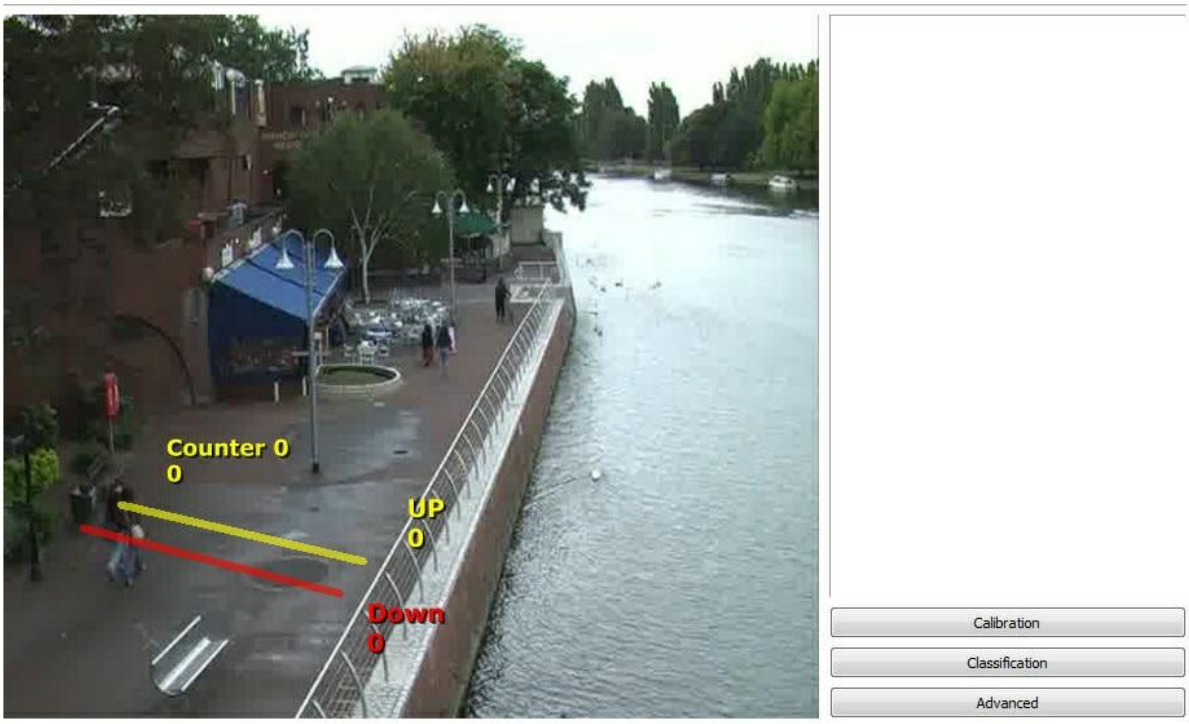
With that rule we'll **decrement** the counter already created.
Select it and in Decrement choose the rule of the second area as shown in the picture below:



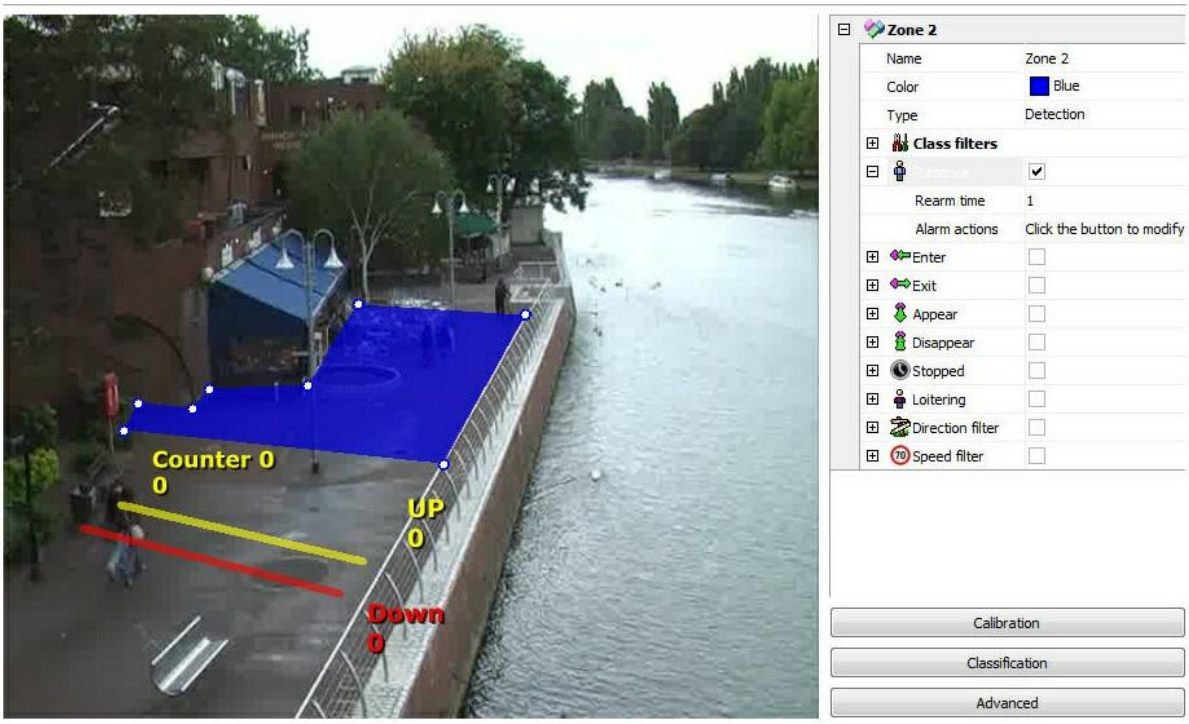
With this configuration, the Counter will **increment** when people walk up and **decrement** when people walk down.

There could still be a counter for each line as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

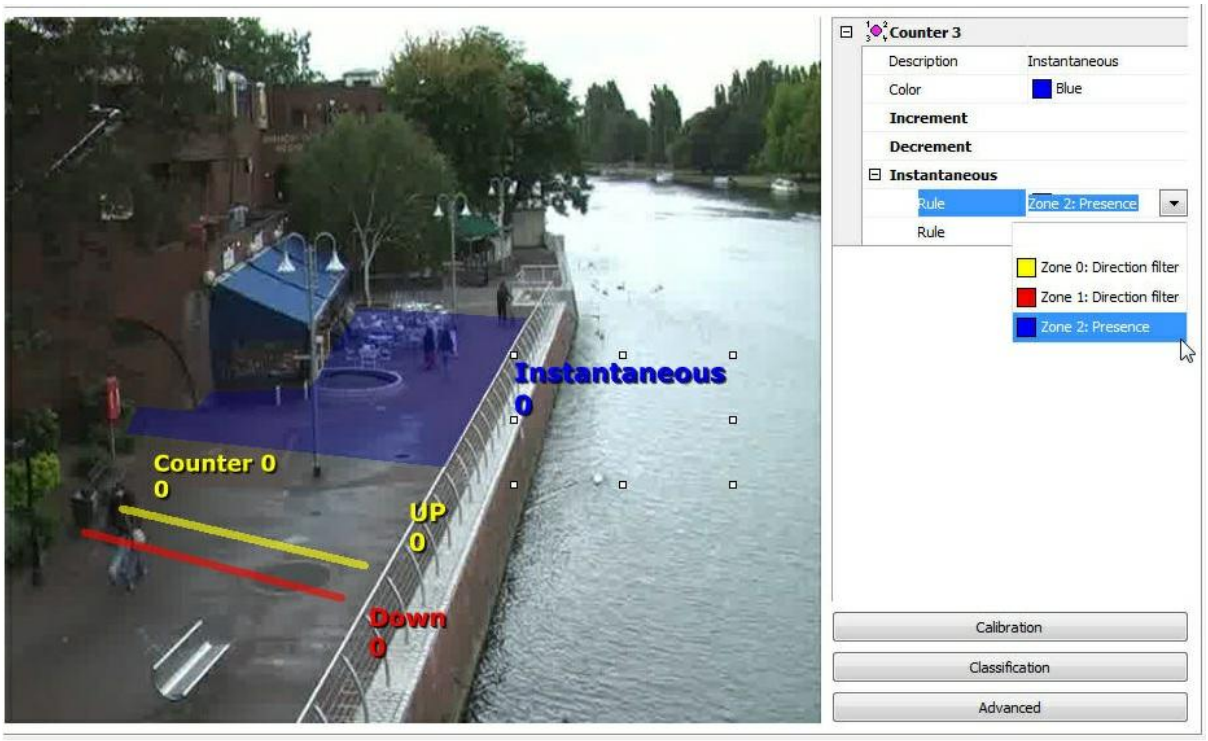


To test the instant counter we will create a presence detection area as shown in the picture below:



Now a counter will be created to show the value of the presence rules activated within this area, in other words, it will give the number of objects present at the exact time within the area. The picture below shows that configuration:

© 2002 - 2020 by Digifort, all rights reserved



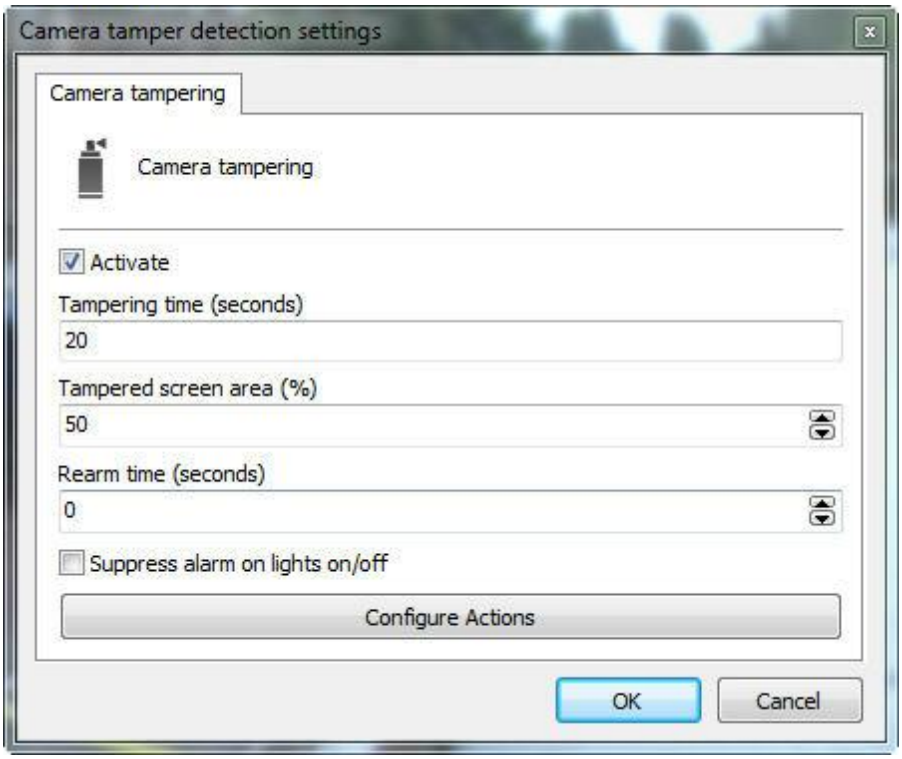
You can configure up to 40 counters per analytic configuration.
The counter size can be adjusted when selected and by dragging the squares around it.

14.2.1.2.5 How to configure the Camera Tampering

The Tampered Camera module can trigger alerts if there is something obstructing the camera, such as: the camera's position is altered, the lenses are fixed, an object is placed to block the view of a certain area.

To configure the tampered camera module click on the s button on the analytics configuration screen as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



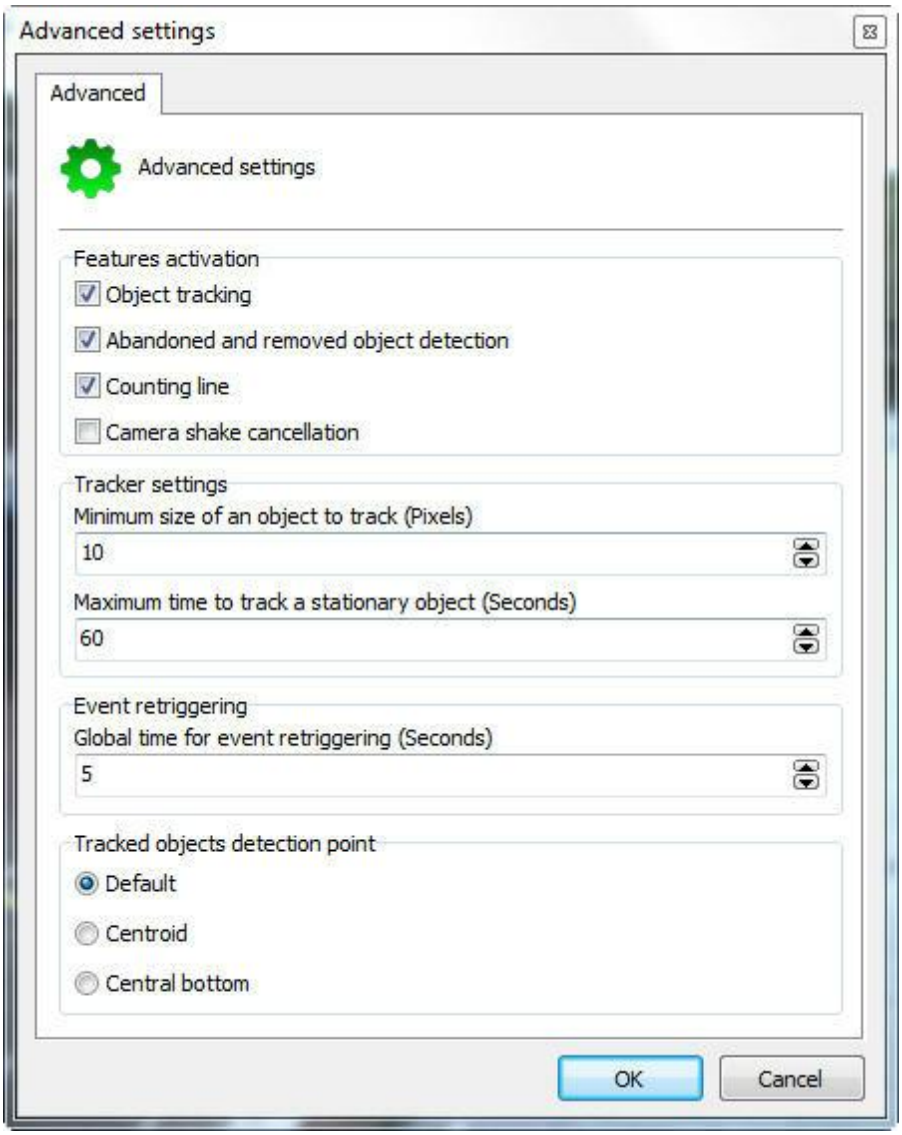
This screen has the following functionalities:

- **Activate**: Activates or deactivates the camera tampering module.
- **Tampering Time**: Time in seconds that the camera has to be obstructed to trigger the alert.
- **Tampered screen area**: Percentage of the image on the screen that must be obstructed to trigger the alert.
- **Rearm time:** Period before another alert is triggered.
- **Suppress alert on lights on/off**: The alert is not triggered if lights are switched on/off in the selected environment.
- **Configure alert actions:** In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

14.2.1.2.6 The Analytics Advanced Options

Advanced options contains some general functions that are discussed below.

© 2002 - 2020 by Digifort, all rights reserved



This screen has the following features:

• **Tracking Object:** Activates the object tracking module. Disable this option if you use only the line modules or abandoned objects count/withdrawn.
• **Abandoned and removed object detection:** Activates the object module abandoned and withdrawn. Disable this option if you do not use it.
• **Counting line:** Activates the count line module. Disable this option if you do not use it.
• **Camera shake cancellation:** This module aims to assist in the analysis of image in cameras that can swing for several reasons which are fixed. With the module activated, image analysis will be much better and the chances of errors decreases.

Tracker configuration
Minimum size of object to track (Pixels): Configure the minimum size of the pixel to be considered an object to track by video analysis.
Maximum time to track the stationary object (Seconds): Maximum time in which a stationary

© 2002 - 2020 by Digifort, all rights reserved

object is tracked after this time the object is embedded in the learned scenario.

Event retriggering: Sets an overall time for the analytical event re -trigger in the current configuration.

Tracked objects detection point: Define the point of object detection.

© 2002 - 2020 by Digifort, all rights reserved

Chapter XV

15 License Plate Recognition

The LPR server is a module different from the Digifort server, as well as the Digifort Analytics.

The LPR and Analytics servers are installed along with the Digifort server, however, licenses are purchased separately.

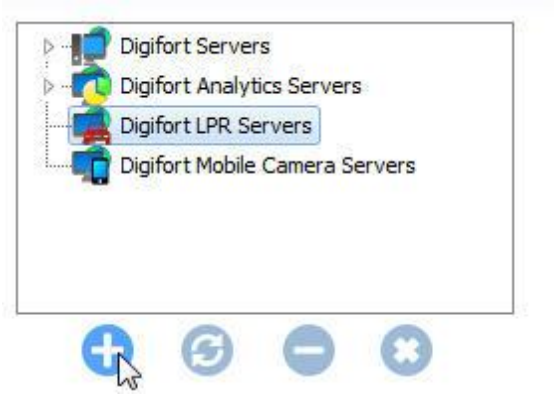
The LPR works with two different Engines: iPTS and Carmen. In addition to the basic license, which must be purchased so that they may work with Digifort, both Engines work from a Hardkey, as well as the Digifort base.

Carmen is an international engine and works with an unlimited number of cameras. Its only limit is your computer's hardware.
iPTS is an engine specially developed for Turkey plates;

Recording in the database is limited only to disk storage capacity of the equipment used and the server has FailOver function, since if a server fails, another one is automatically triggered.

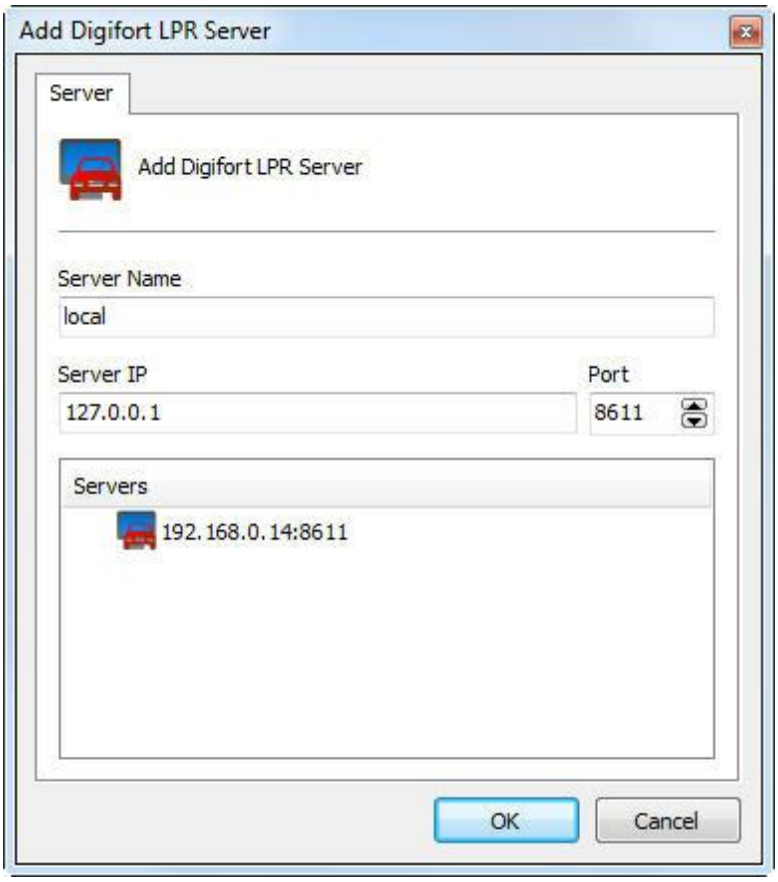
15.1 How to create a License Plate Recognition Server

To start using the LPR module, you must first create a Digifort LPR Server.
In the Administration Client, select the **Digifort LPR Servers** option and click on “Add server”, as in the picture below.



Select the “Digifort LPR Servers” option and click on the button **Add Server** on the top left-hand corner of the screen.
The following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved

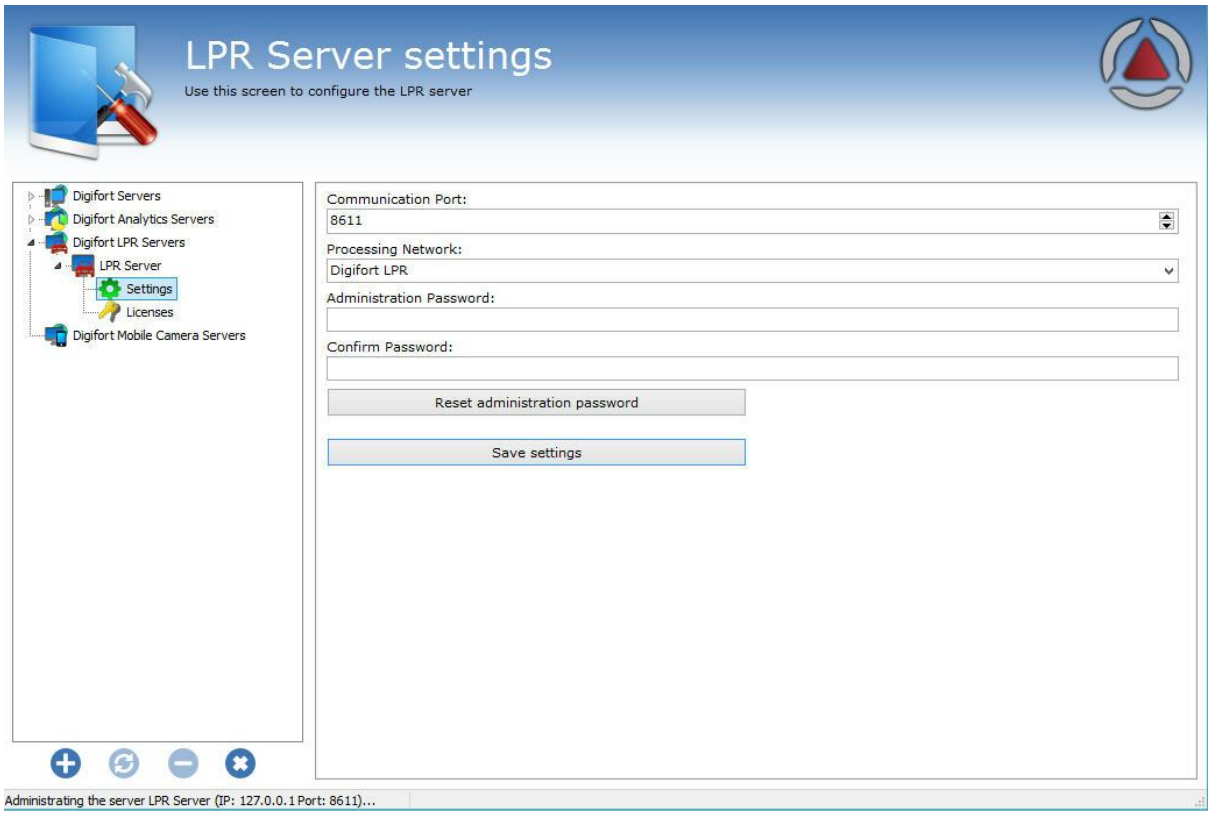


In this screen you have to define a name and an IP where the LPR Server is active. When you've done this, click on **"OK"**.

15.1.1 How to configure your LPR server

As configurações do servidor LPR são bem simples como mostra a imagem abaixo:

© 2002 - 2020 by Digifort, all rights reserved

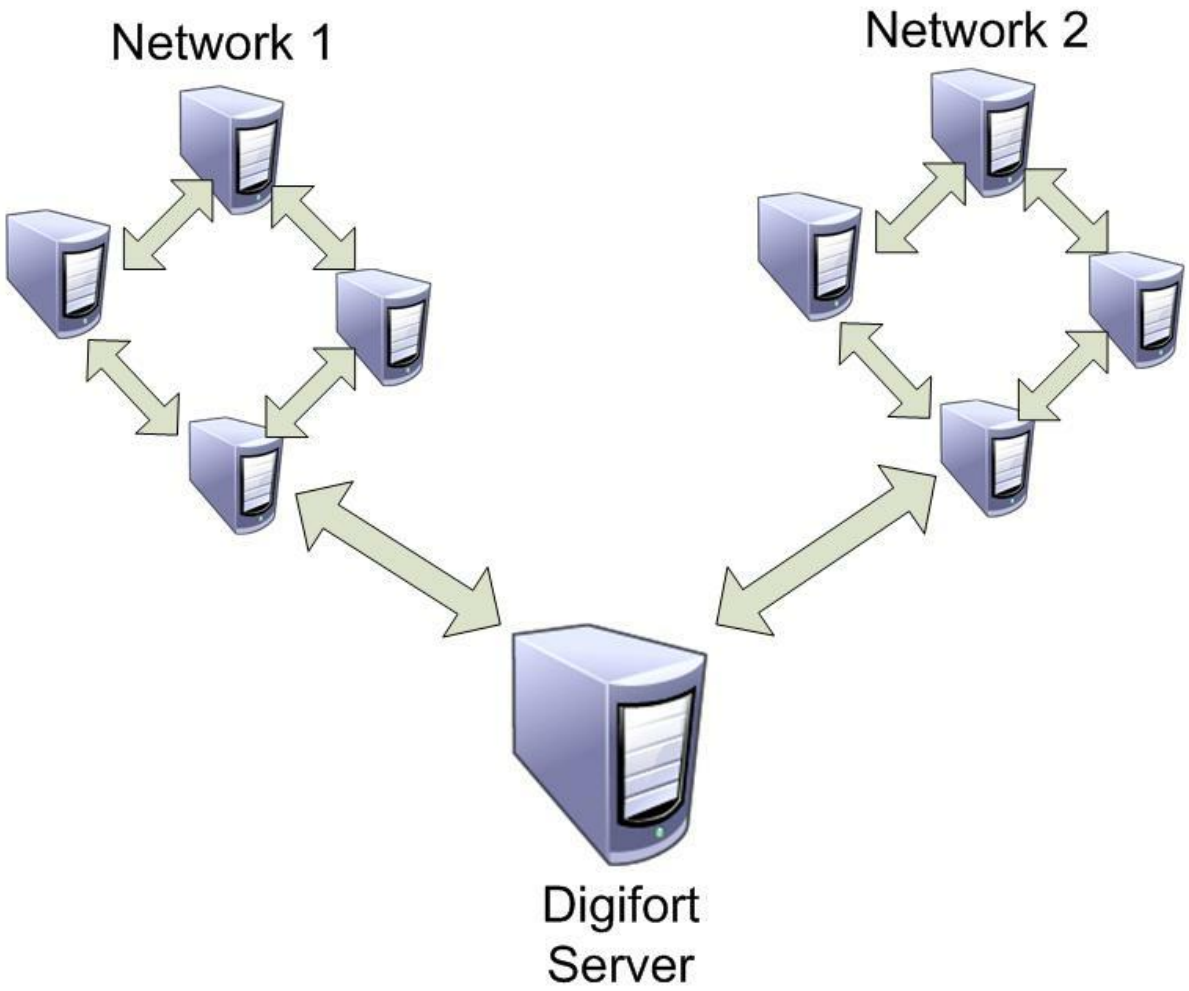


The only configurations to be applied are:

- **Communication Port:** Communication port to the analytics server. It is recommended that you change this only if another program is already using it.

- **Processing Network:** Name of the distributed network where the server will counterbalance the load. When more than one server has the same "Processing Network" name there will be a processing counterbalance among them. Look at the diagram below to get a better idea:

© 2002 - 2020 by Digifort, all rights reserved



In the picture above, the **"Digifort Server"** sends the images of the cameras to two different " **Processing networks**". This way, each set of computers only balances the load among the **LPR Servers** with the same network name.

- **Administration Password**: Password to access the analytics server. Fill in this field to change the current password.
- **Confirm Password**: Type the password again.
- **Save configurations**: Saves changes made on the screen.

The default port is 8611, but it can also be edited.
The processing network can have any name chosen by the user who can also create an authentication password.

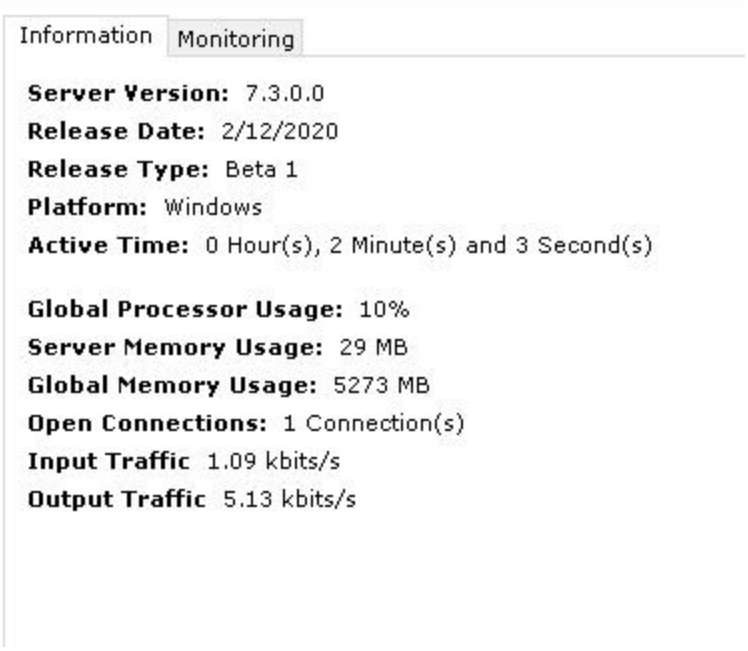
15.1.2 Status do Servidor de LPR

n this area of the system you can monitor how the server is performing, recovering data such as processor usage, memory, network traffic, etc.
To access this resource, click on the Server Information item in the Settings Menu, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



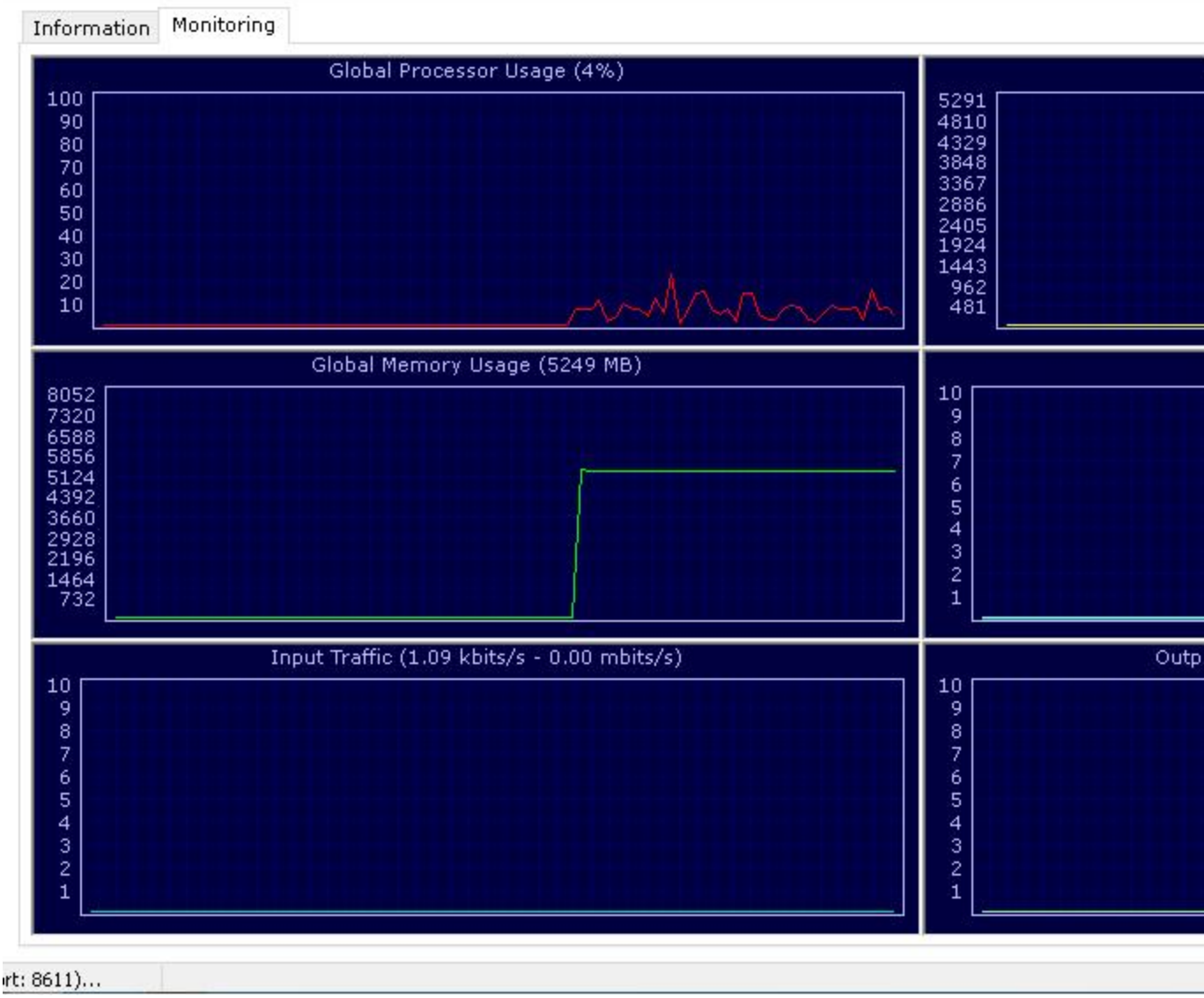
That done, the server information window will open on the right side, as shown in the figure below:



15.1.2.1 Monitoring

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

© 2002 - 2020 by Digifort, all rights reserved



15.2 Licensing the LPR

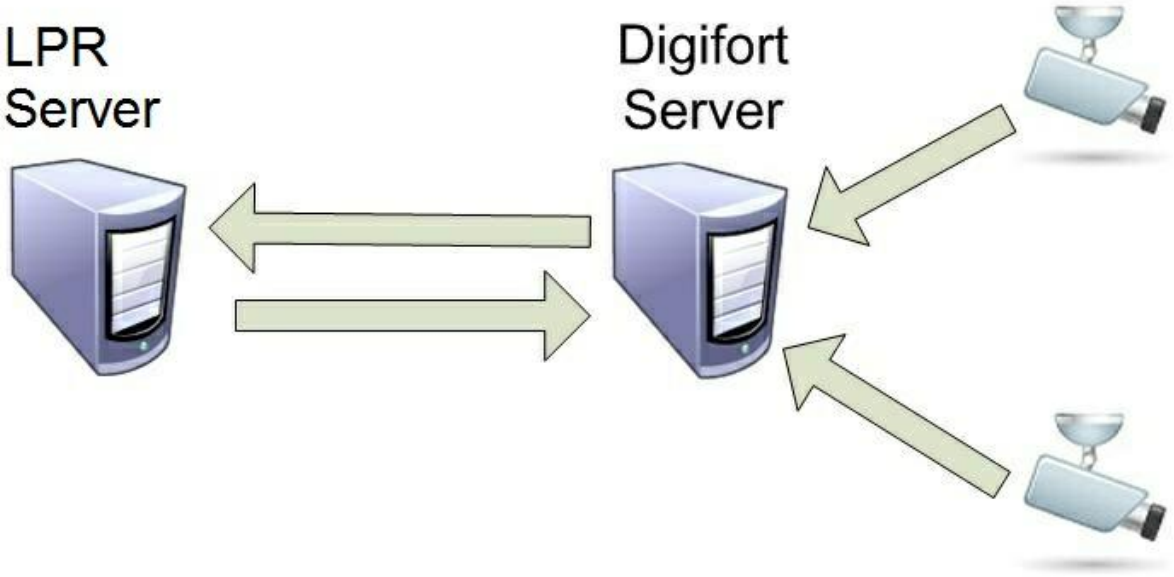
How does the architecture for the Digifort LPR work?

The license for the LPR server works like the server for the Digifort cameras, there is a “base license” for the server and other licenses for the LPR.

There are three types of licensing, **Neural Labs, OpenALPR** and **Carmem** engine.

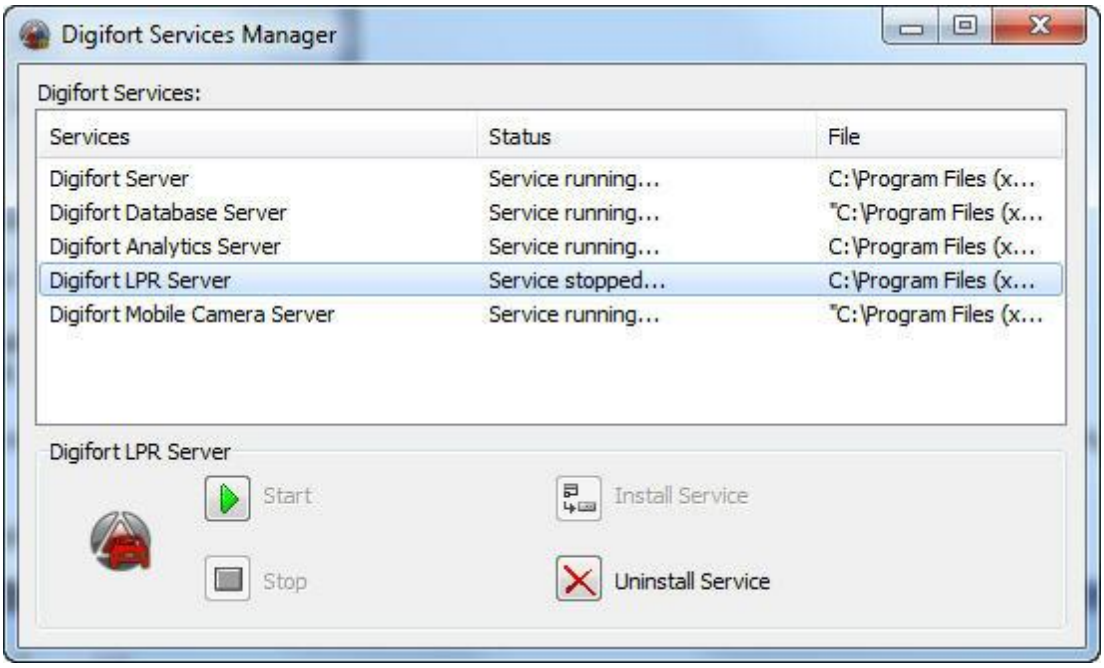
The **Carmen** engine is licensed via Hardkey which licenses a Core of the processor. This way the engine will process as many LPR as possible according to the Core processing capacity.

© 2002 - 2020 by Digifort, all rights reserved



15.2.1 How to license the LPR Server

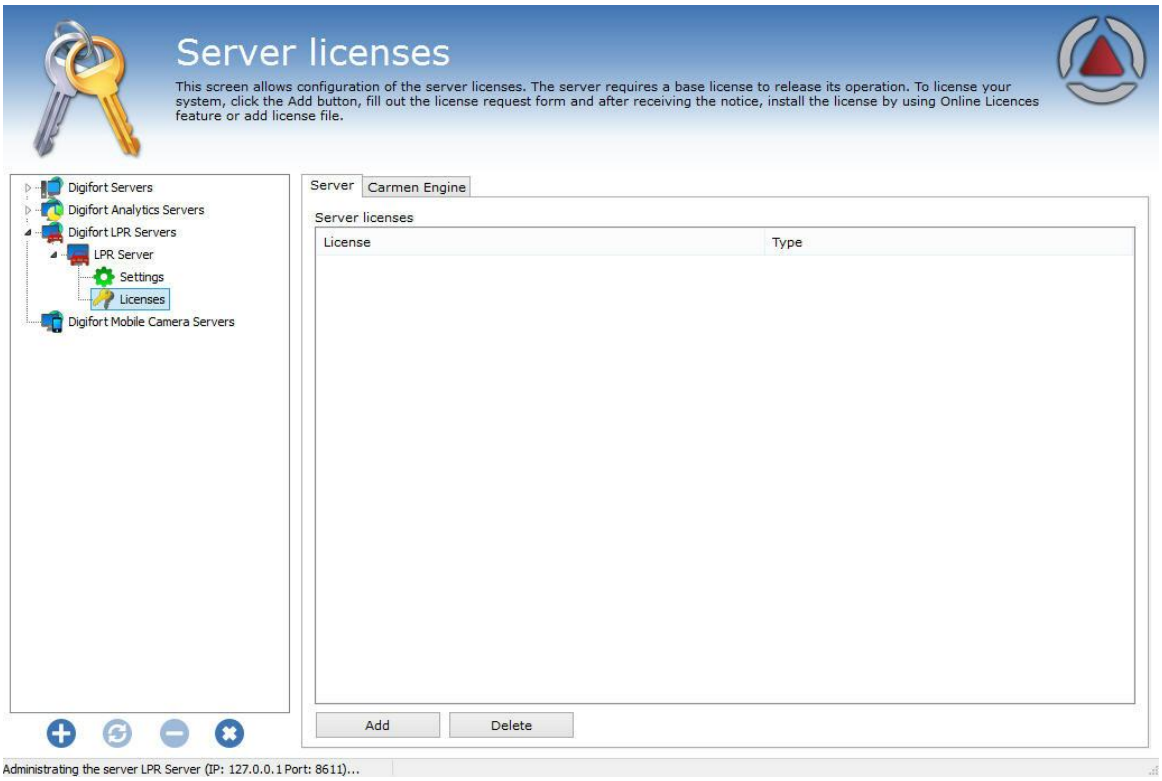
Once you have created the LPR server, you have to license it. As an example, we'll use the Carmen license to begin with.
First of all, for Digifort to recognize the Hardkey in the computer, you must stop all server activity as shown in the picture below:



© 2002 - 2020 by Digifort, all rights reserved

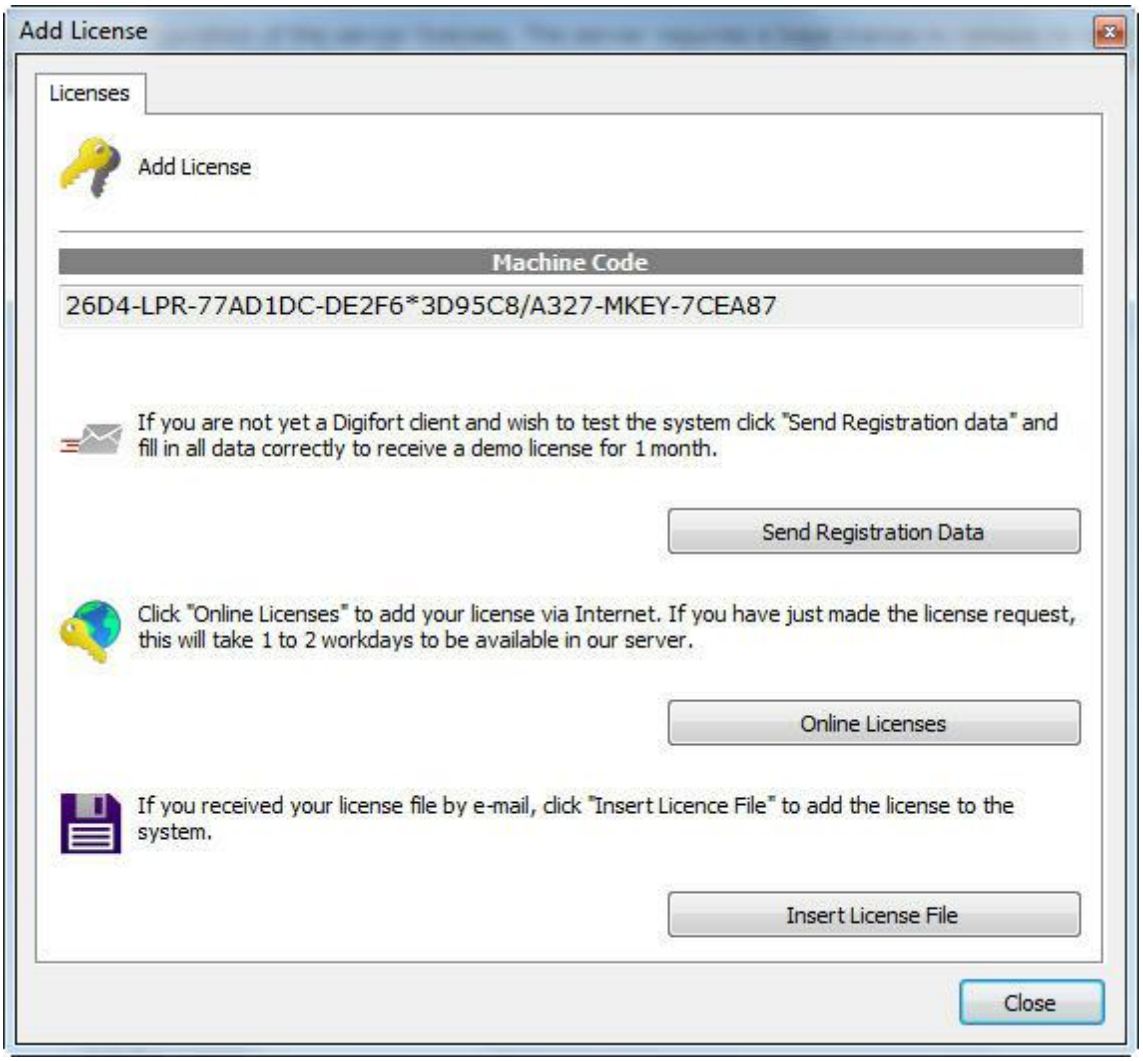
The Digifort Server and Digifort LPR Servers must be stopped. Now that the services have been stopped, you can connect the Hardkey to the computer and only then start the services again.

Now you can log into your LPR server and click on the “Licenses” option as shown in the picture below:



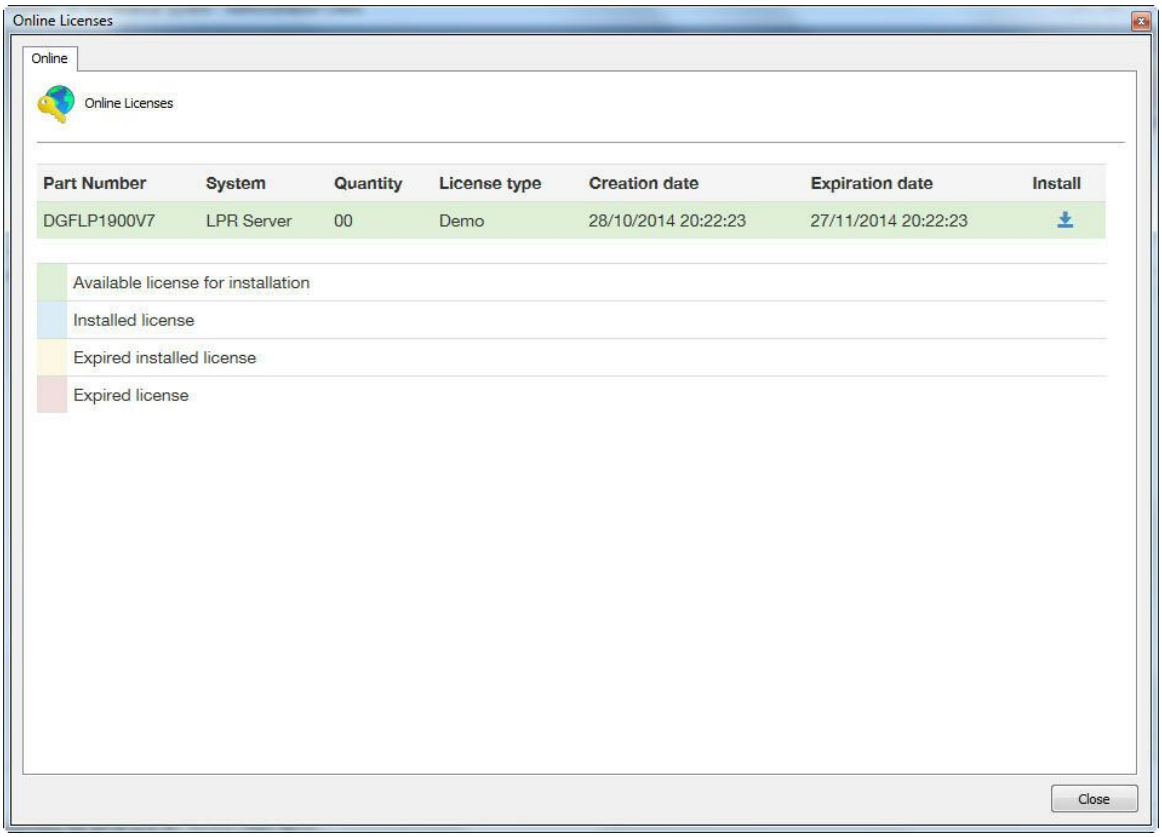
The base for the LPR to function will be installed in that Server tab.
The license is carried out on the Internet with the client information and a protocol number received by the client.
To install the base license, click on “Add” and the following screen will show up:

© 2002 - 2020 by Digifort, all rights reserved

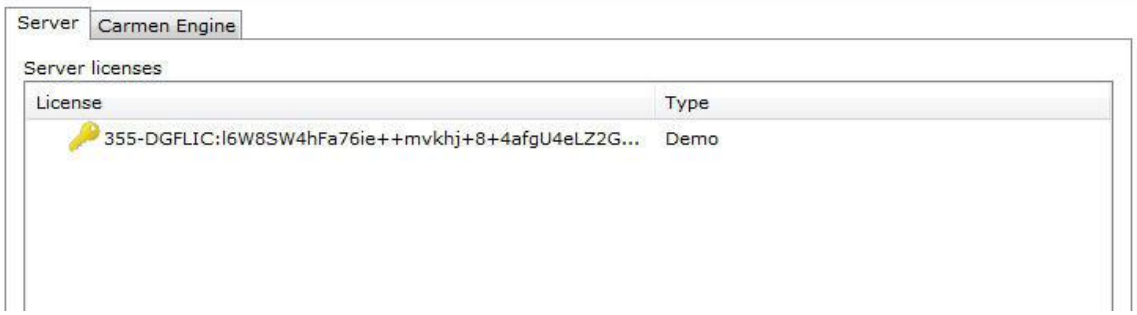


The licensing process is the same as for Digifort.
On the online license screen the description should be "LPR Server" as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



Once a license has been added it becomes available as shown in the picture below:



Now, let's configure the Engines.

15.2.1.1 How to license the Carmen engine

All the **Carmen** engine needs is that the Hardkey be plugged in and all the licenses are automatically recognized, as shown in the following picture:

© 2002 - 2020 by Digifort, all rights reserved



Pronto agora seu LPR com o **Engine Carmen** já está licenciado.

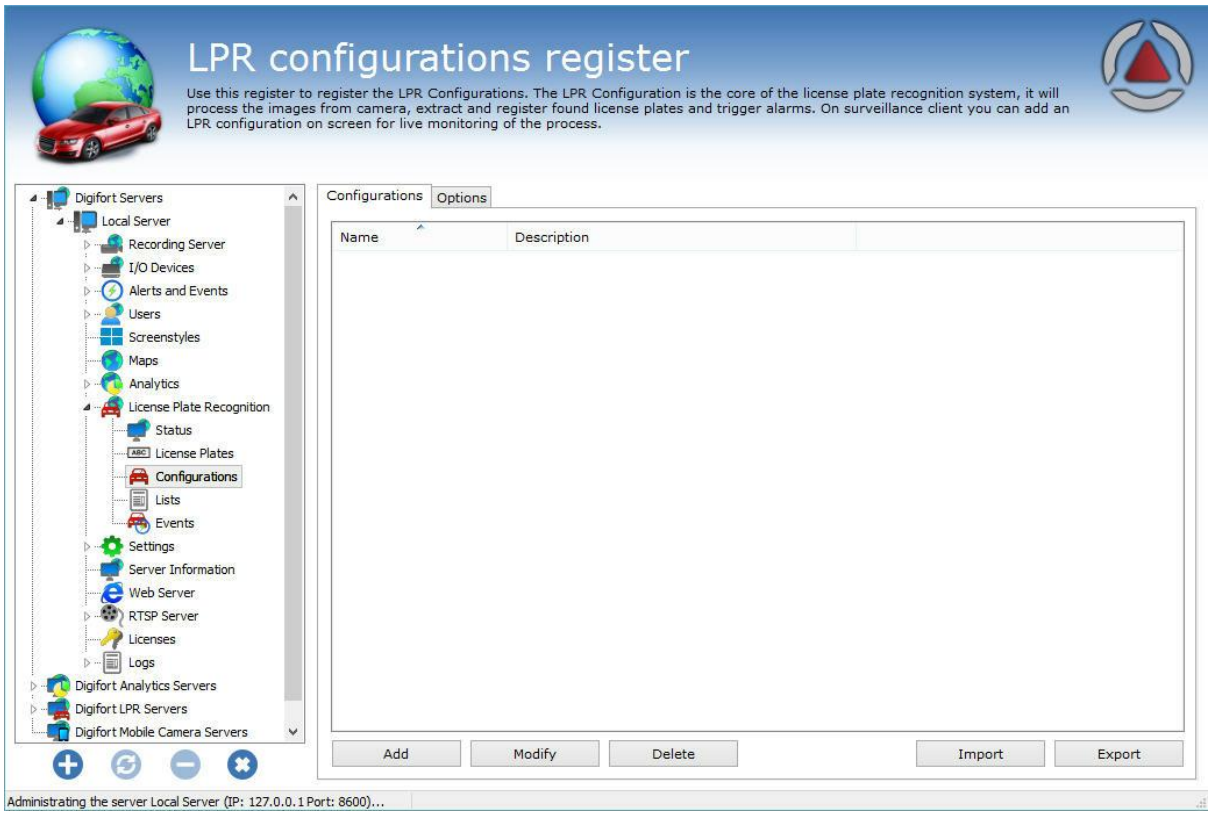
15.2.1.2 How to license the Neuro Labs Engine

Check with your dealer the purchase and installation process of Neuro Labs licenses.

15.3 How to configure the License Plate recognition

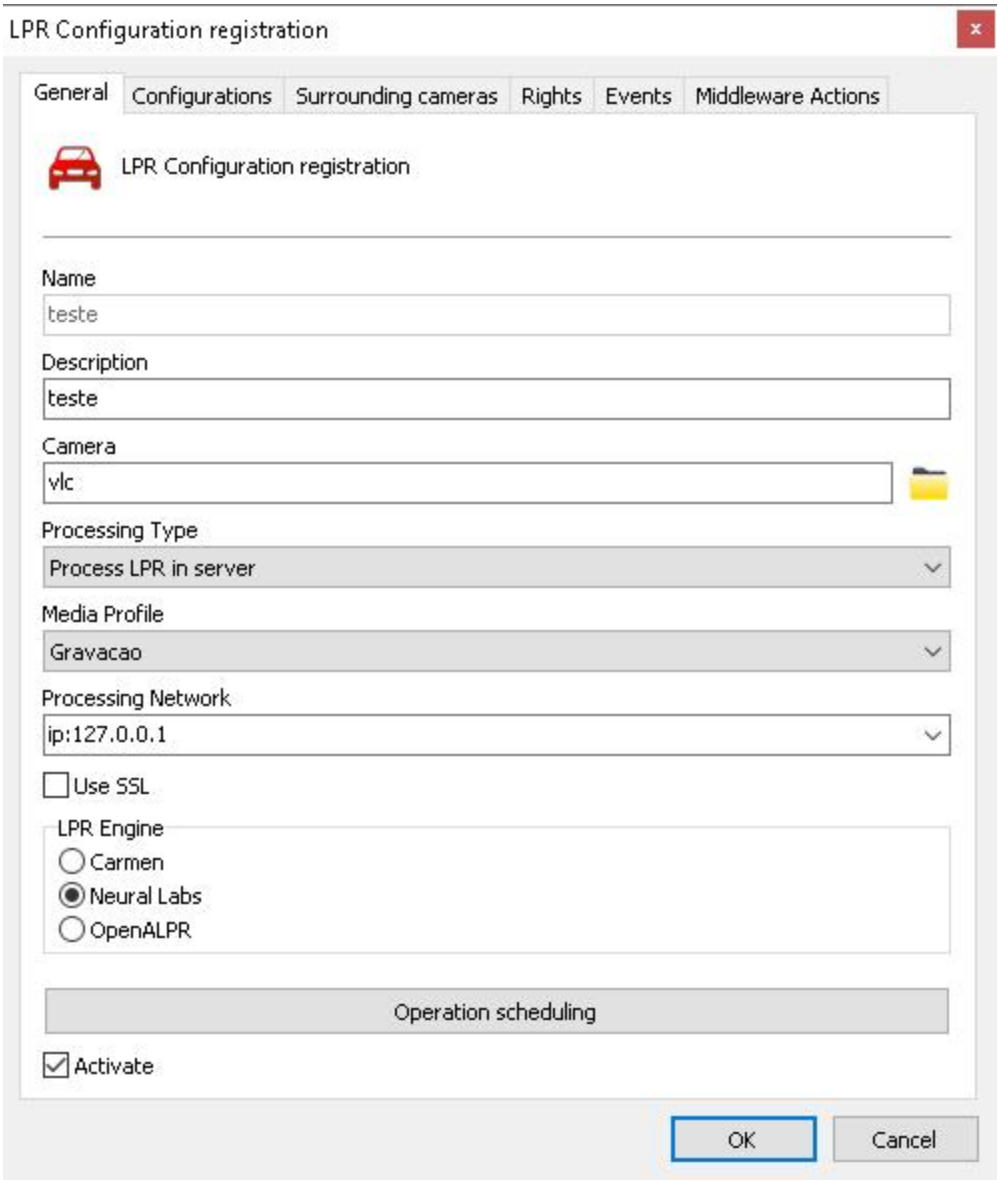
To configure plate recognition with the Carmen engine, we must first log into the Digifort server and access the **Settings** option under **Plate Recognition**, as shown in the following image:

© 2002 - 2020 by Digifort, all rights reserved



The **Settings** tab allows you to add a new analytics setting. For this, click on the **Add** button to start LPR settings. The following screen will be displayed:

© 2002 - 2020 by Digifort, all rights reserved



This screen provides the following features:

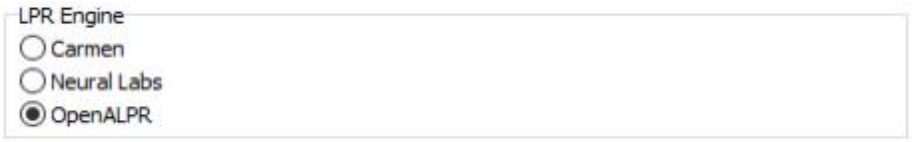
- **Name**: Desired LPR name, for example: Digifort 1
- **Description**: Description of the analytics registration, for example: Plate recognition from Avenue 1.
- **Camera**: All cameras registered on the Digifort server will be available in this check box.
  To learn how to register cameras, see the [How to add a camera' chapter.] chapter.
- **Processing Type**: It allows images to be processed locally in the available engines on Digifort or on third-party servers. This option opens the range of LPR integrations and allows for future expansion of Digifort's LPR base system for powerful integrations with third-party systems.
  - The following servers are currently supported:
    - **Neural Server**

© 2002 - 2020 by Digifort, all rights reserved

- **Media Profile**: It selects the media profile that is desired for analysis. The analytics always analyzes images in a 320x240 or 352x240 resolution, so it is recommended for the camera to have at least these values or higher.

- **Processing Network**: All processing networks (LPR servers) active on the network will be available in this field. It selects a network in which this configuration will be processed. You can specify the processing server by its IP. To do so, use the following format in the field: “IP:server IP”. Example: IP:192.168.0.10.

- **LPR Engine**: It chooses the engine that will analyze the images. There are three image processing engines on Digifort: Carmen, Neural Labs, and OpenALPR.
  Choose the engine that was acquired to perform the settings.



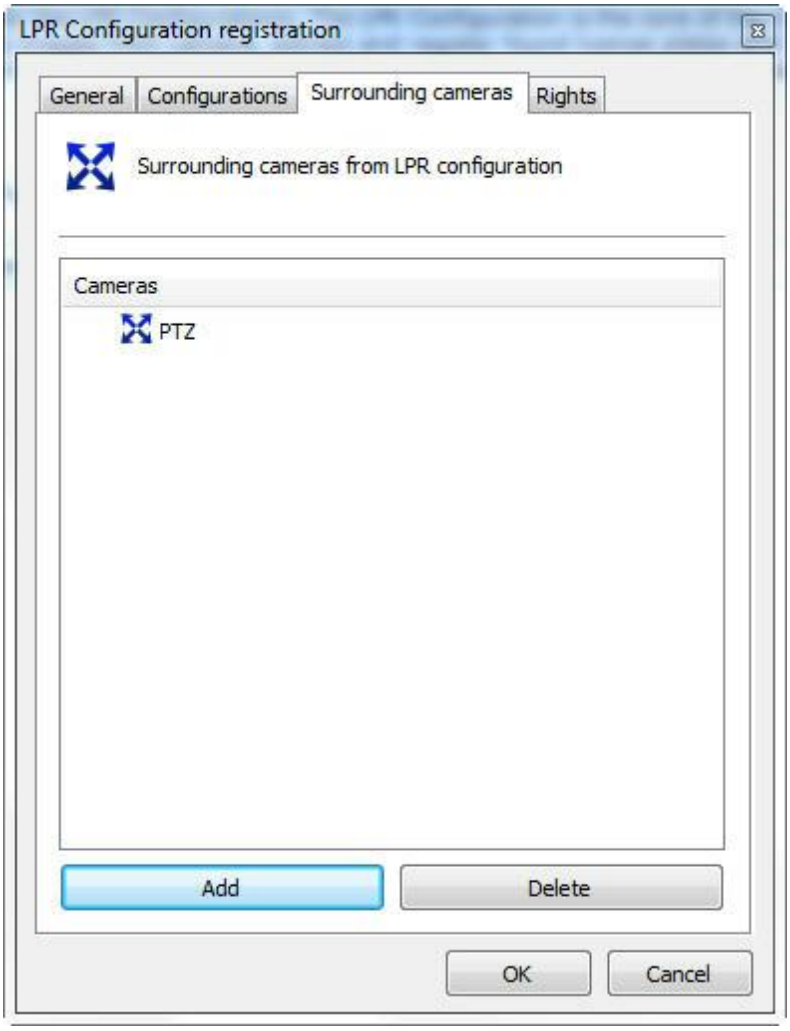
- **Use LPR from camera**: The LPR system now supports the edge operating mode, thus allowing total integration of autonomous LPR cameras that feature on-board recognition algorithm. A new (Edge LPR) license is required for each LPR configuration using edge processing. See your reseller for more details.

- **Operation Scheduling**: It allows you to schedule the LPR’s hours of operation.

- **Activate**: It activates or deactivates the analytics settings.

On the Surrounding Cameras tab, you can inform the cameras that are connected to the main camera for LPR. Thus, the user can be provided with reports containing images from surrounding cameras together with the image from the main camera.

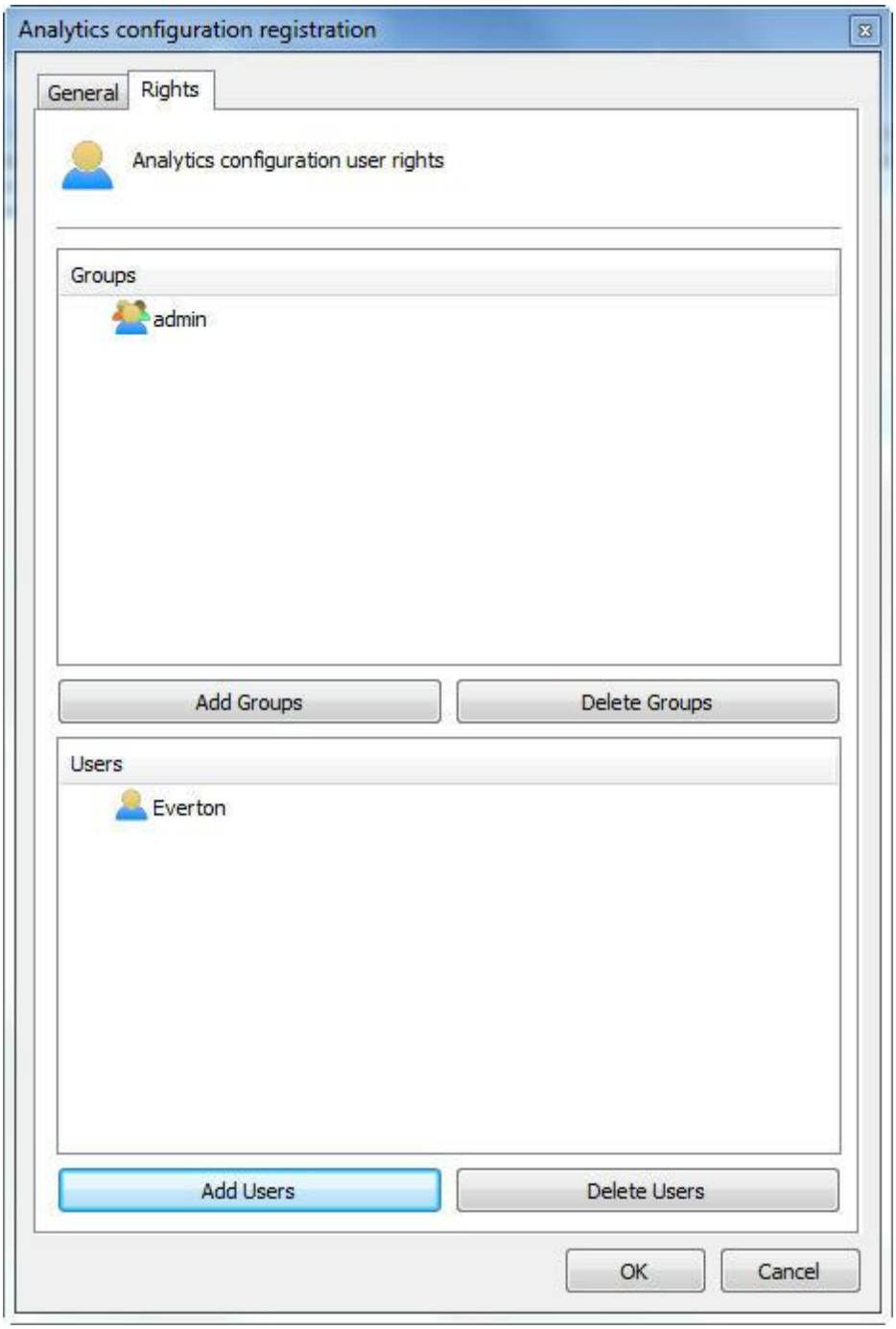
© 2002 - 2020 by Digifort, all rights reserved



Simply click on add and select the desired surrounding camera.

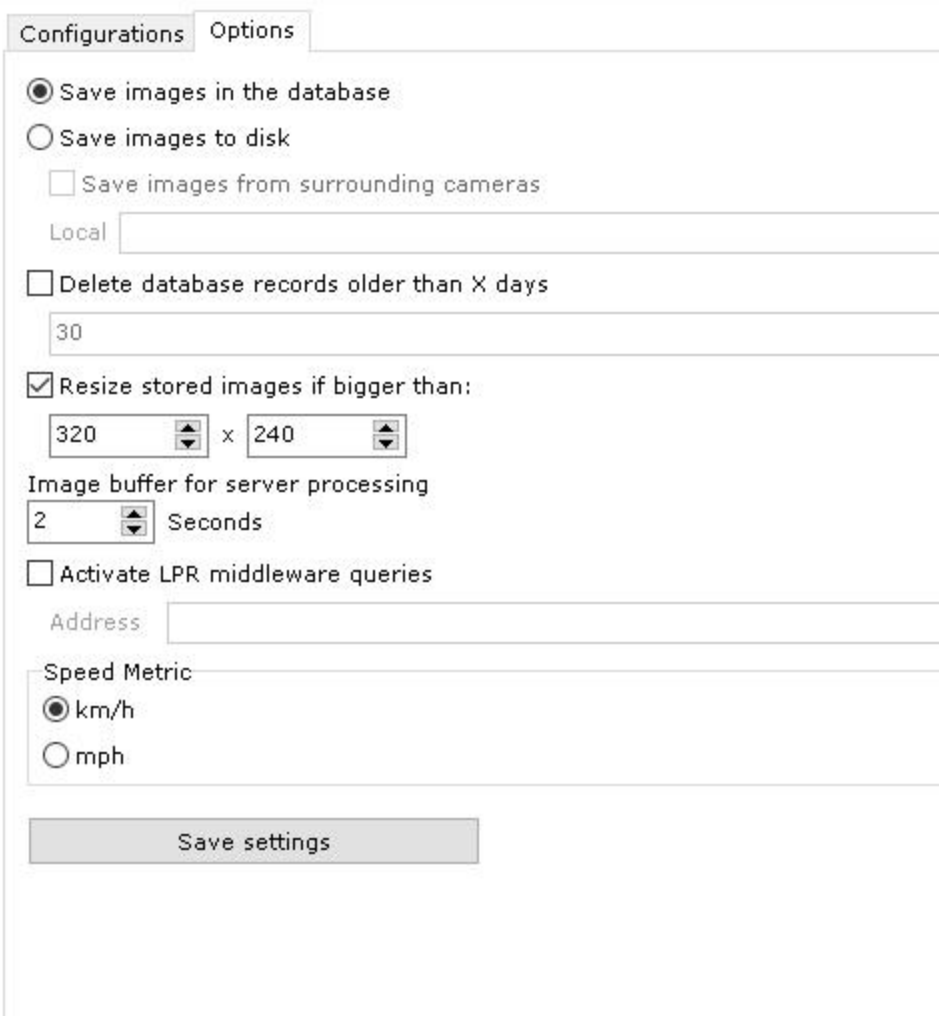
On the Rights tab, you can configure the rights of which users who will be granted permission to view this configuration. See the figure below:

© 2002 - 2020 by Digifort, all rights reserved



To learn about users and user groups, see the ‘User Management’ . chapter.

© 2002 - 2020 by Digifort, all rights reserved



On the **Options** tab, we have the following options:

- **Save images in the database**: LPR saves the images of recognized plates on the server. With this option, the images will be kept in Digifort's database.
    - The LPR system allows you to store images from surrounding cameras associated with LPR settings.
        - By default, images from surrounding cameras are queried in camera recordings, but, in some cases, it is necessary to keep these records longer and, in this case, the images can be saved together with the recognition image.
        - This option is only available when images are saved to disk instead of in the database.
- **Save images to disk**: LPR saves the images of recognized plates on the server. With this option, the images will be kept directly on the server's disk.
- **Delete LPR records older than X days**: It deletes LPR records that have been stored for more than X configured days.

© 2002 - 2020 by Digifort, all rights reserved

- **Resize stored images if larger than**: By default, images are stored in 320x240. However, if a camera with a higher resolution is used, you can save the image with a higher resolution by simply changing the resolution settings on this screen.

- **Image buffer size settings**: It allows you to set image buffer for processing. This buffer is used when the LPR Server is overloaded (which can happen when image recognition from several cameras is activated simultaneously). Therefore, the system will temporarily store the images on memory (before discarding them) for a few seconds to await the LPR Server reply to image processing. A high buffer value can improve processing as well as recognition results as images would be previously discarded if the LPR Server was overloaded, but it can also increase recognition response time.

- **Activate LPR middleware query**: Address to connect to a software that will make queries in a third-party database. See Digifort for more information on integrations.

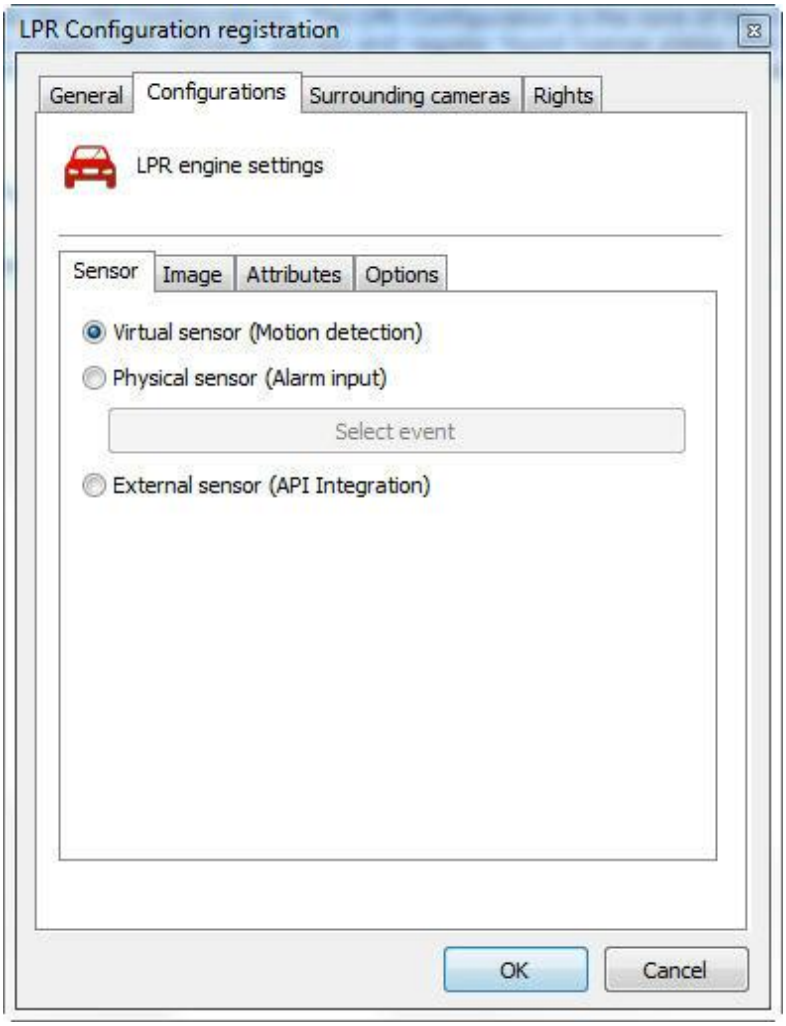
- **Speed Metric**: Some cameras can return the speed at which the vehicle passed by the camera together with the plate. In such cases, you must choose which speed metric Digifort will use: km/h or mph.

NOTE:
The LPR Server now has a 64bit version.
The OpenALPR engine works only in the 64bit version.This version is still experimental.
Use only if you are using the OpenALPR engine or if the LPR server's service is consuming more than 3GB of memory.

15.3.1 Configuring Carmen Engine / Neuro Labs / OpenALPR

After configuring the **General** options, click on the **Settings** tab.

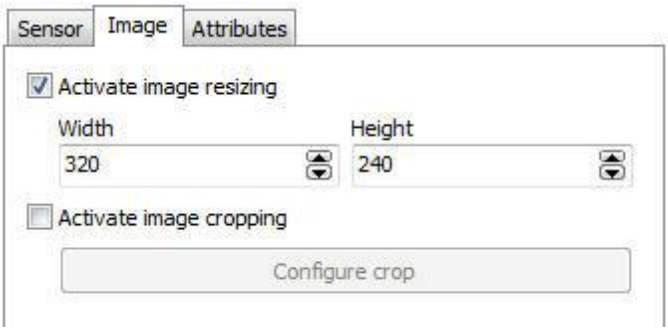
© 2002 - 2020 by Digifort, all rights reserved



There are three configurations to be done on this tab:

- **Sensor**: The sensor will be the one that will trigger the camera for it to capture the plate. It can be triggered both by a **Physical Sensor**, as an Infrared barrier, and a **Virtual Sensor**, which will use motion detection to trigger the LPR.

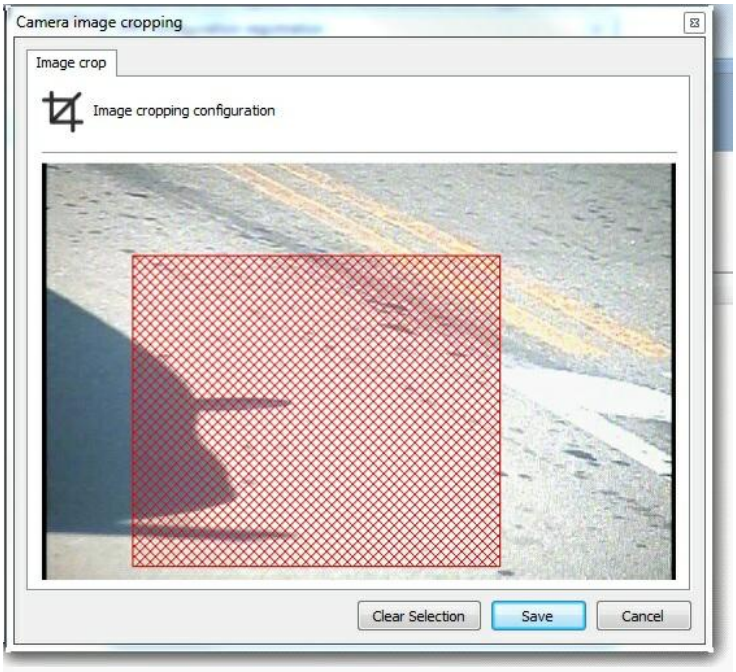
- **Image**: On the **Image** tab, the following options are available:



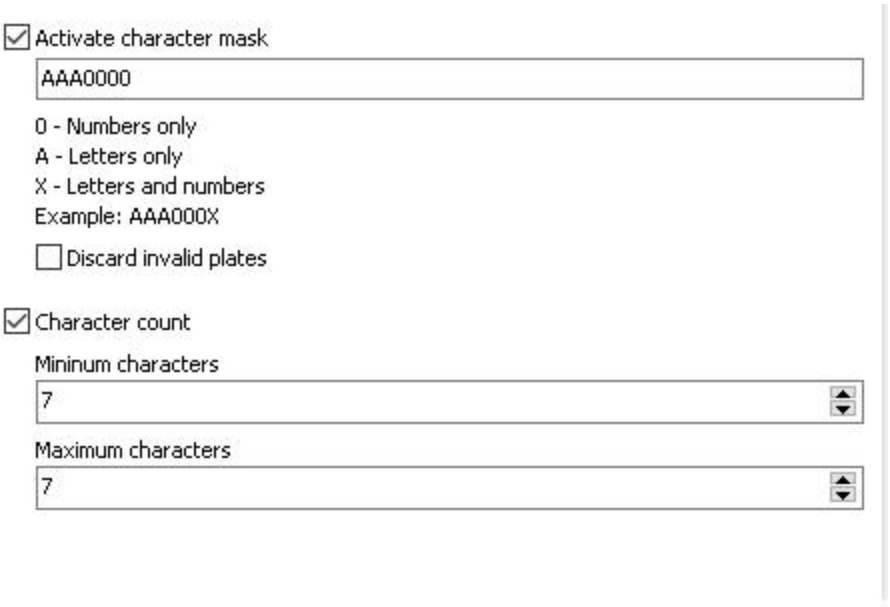
Now we have:

© 2002 - 2020 by Digifort, all rights reserved

- **Activate image resizing**: This option aims at changing the size of the photo captured by the camera to save processing.
- **Activate image cropping:** This option aims at selecting a specific area where the engine will look for plates to be captured. This option is useful where there is a megapixel camera



- **Attributes**: See the available options below:



- **Activate character mask**: This option allows you to have a more advanced control over what the software will identify on a plate. The character 0 identifies only numbers, the A only letters, and X

© 2002 - 2020 by Digifort, all rights reserved

letters and numbers. If, for example, the desired plate's capture pattern is EGV - 1234, then the best filter to be configured is AAA000.

- **Character mask** configuration allows the option of discarding invalid records, i.e., those that do not follow the character mask.Up to version 7.2.1, the system attempted to change numeric values to letters, or vice versa.

- **License plate character count**: This option aims at configuring the Minimum and Maximum number of characters to be identified by the recognition. This is useful because in many countries the number of characters is different.

- **Options**: See the available options below:



- **Triggers unrecognized plates**: If a plate is not recognized, Digifort will store the failure record. Therefore, you can identify problems and even generate statistics.

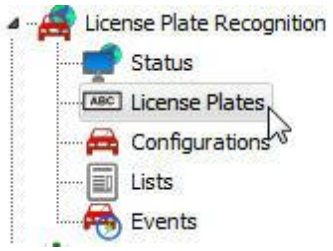
- **Plate re-triggering**: Select this option not to recognize repeated plates in the interval of X seconds. If the option is not checked, Digifort will ignore repeated plates in sequence.

15.3.2 Plates

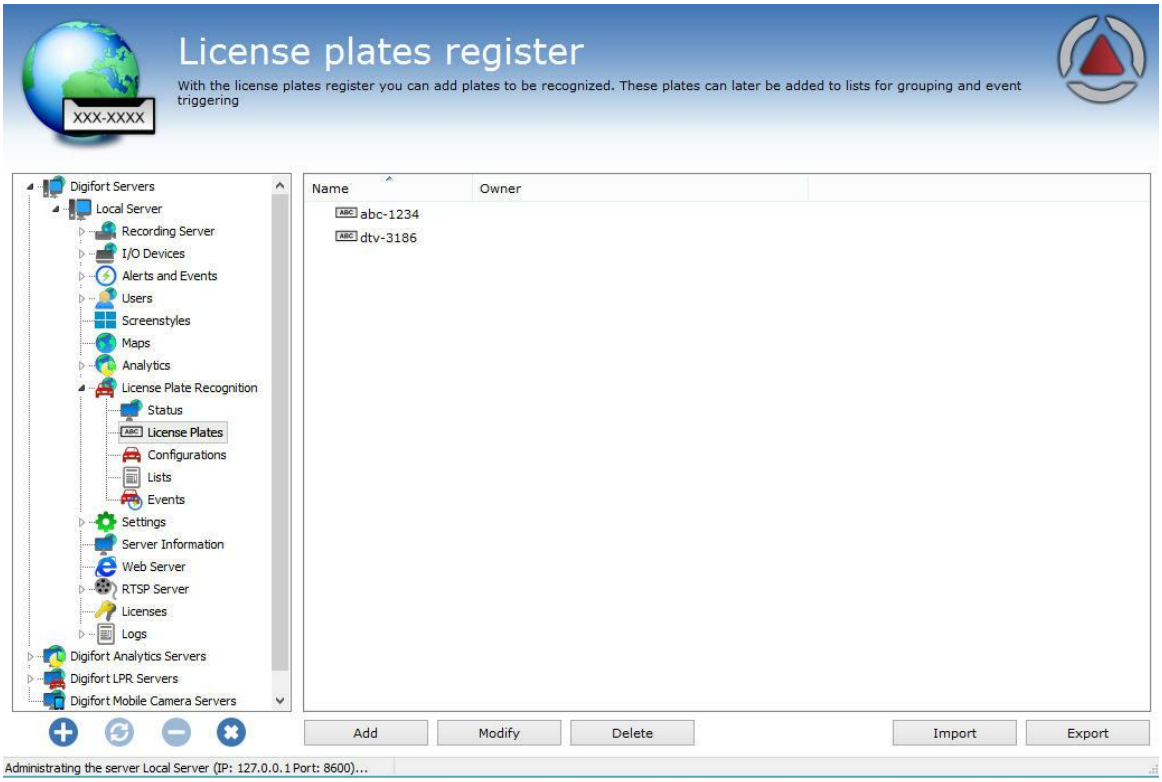
As well as the Capture and Identification of vehicle license plates in Digifort, the LPR can also create a number of alerts when an already registered license is recognized.

To access the plates directory click on the **Plates** item as shown below:

© 2002 - 2020 by Digifort, all rights reserved

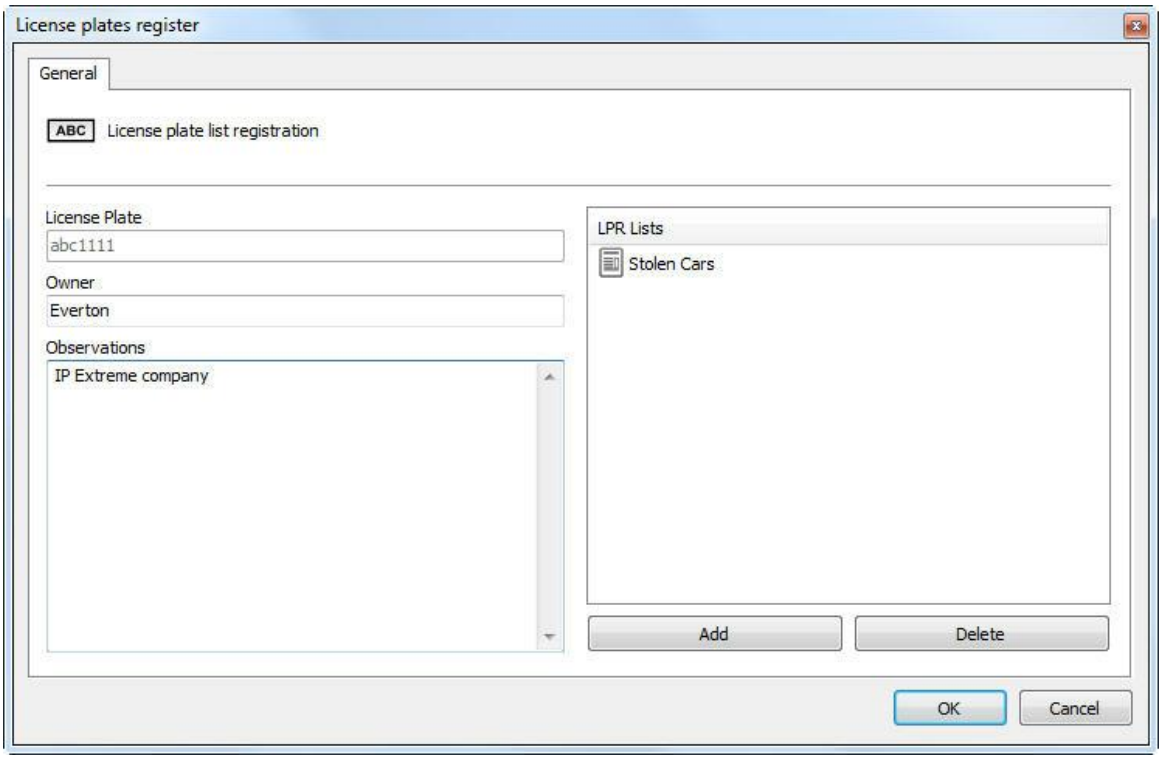


On this screen you must register the plates for which you want to trigger an alert action as a pop-up or even release an access using alert devices.



To register a plate, simply click on **Add**.

© 2002 - 2020 by Digifort, all rights reserved



The registration screen displays the following fields:

- **Plate**: Register the plate to be detected
- **Owner**: Information about the owner (non-mandatory field).
- **Observations**: Observations on the plate;
- **List**: The plate must belong to one or more lists. Learn about lists in the next topic of this manual.

On the main screen you can also import and export plates in files with .csv extension. Simply click on import/export.

Here is an example of exporting 3 plates:

	A	B	C
1	abc1111;Everton;"IP Extreme company"		
2	HJI6978;Francisco;		
3	JHY7896;Eric;"Digifort Company"		
4			
5			
6			
7			
8			

To import plates to Digifort, they should follow the pattern of the image above:

Plate; Owner of the Vehicle; "Observations"

© 2002 - 2020 by Digifort, all rights reserved

Plate; Owner of the Vehicle; "Observations"
Plate; Owner of the Vehicle; "Observations"
... Etc.

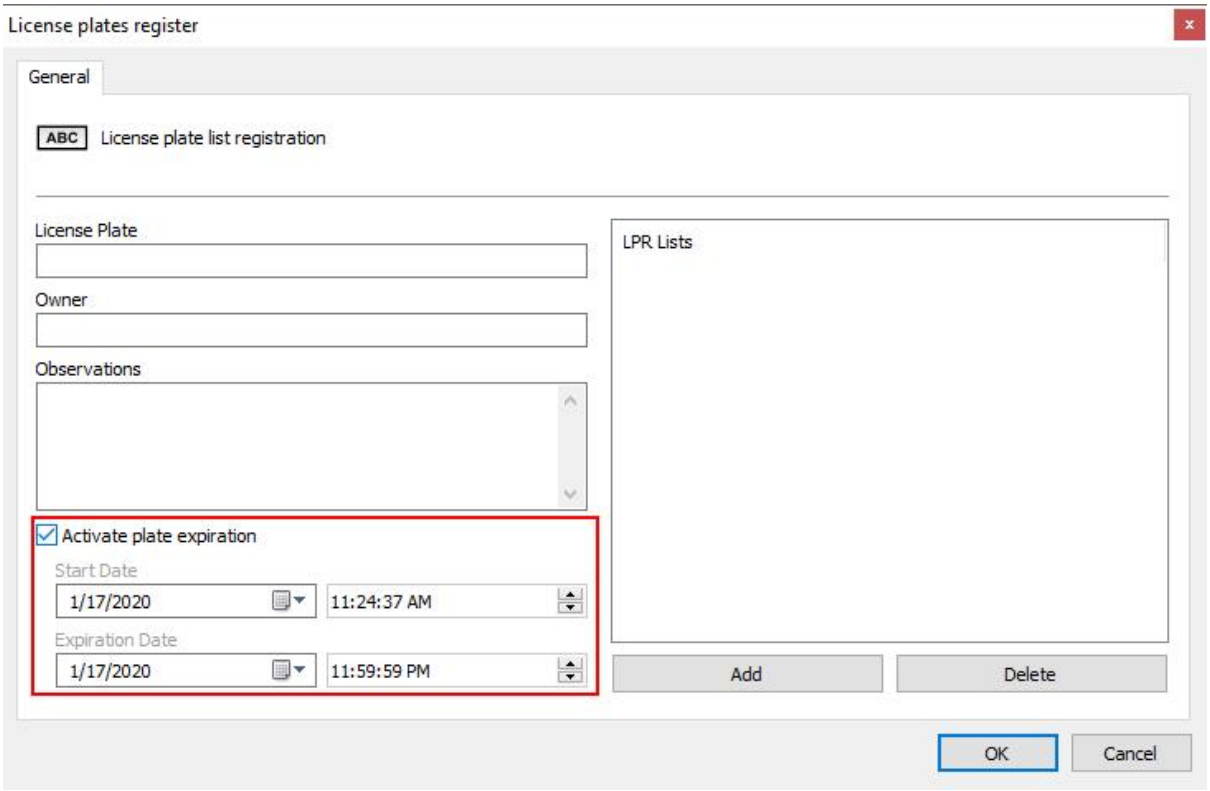
To exclude one or more cards registered at the same time, just select them and click **Delete**;

15.3.2.1 Record Expiration

It is possible to set an expiration date for plates registered in the LPR system.

Plate expiration is used through LPR Events and it is very useful for scenarios where, for example, an expired plate cannot open a gate associated with the event, so it is possible to create temporary plates which will be granted access to the site.

You can set a start date (when the plate will become valid) and an expiration date through plate registration:



LPR events can be conditioned to be triggered using the plate expiration control.

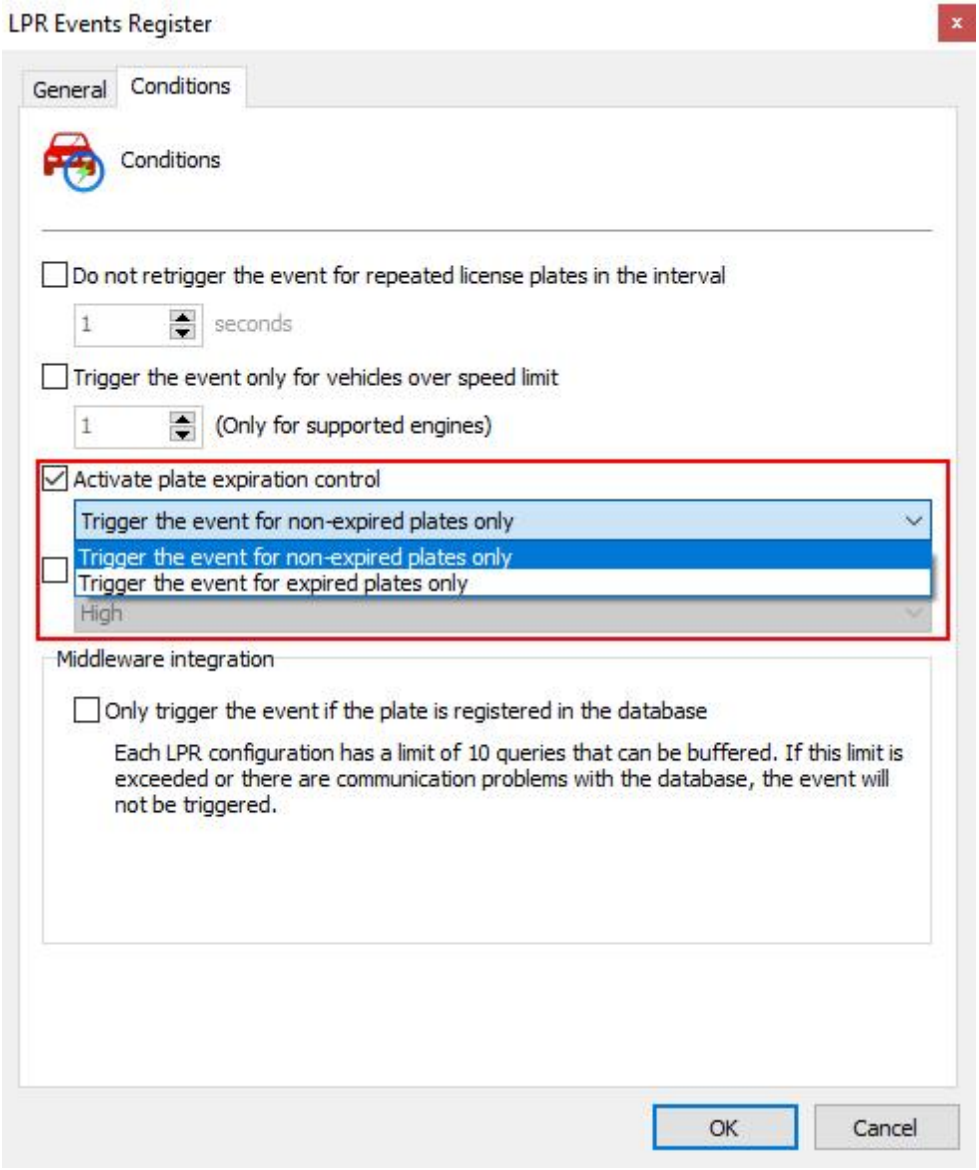
You can configure an LPR event to trigger only if:

- The recognized plate is not expired - this option is useful to create a control for accessing a location, where the system will only open a gate automatically for plates that are not expired.

- The recognized plate is expired - this option is useful to create alarm events if a vehicle with

© 2002 - 2020 by Digifort, all rights reserved

an expired plate is recognized, in this case, the operator can receive an alarm pop-up informing about the vehicle's status. para criar eventos de alarme caso um veículo com a placa expirada seja reconhecido, neste caso, o operador pode receber um popup de alarme para informar sobre a condição do veículo.

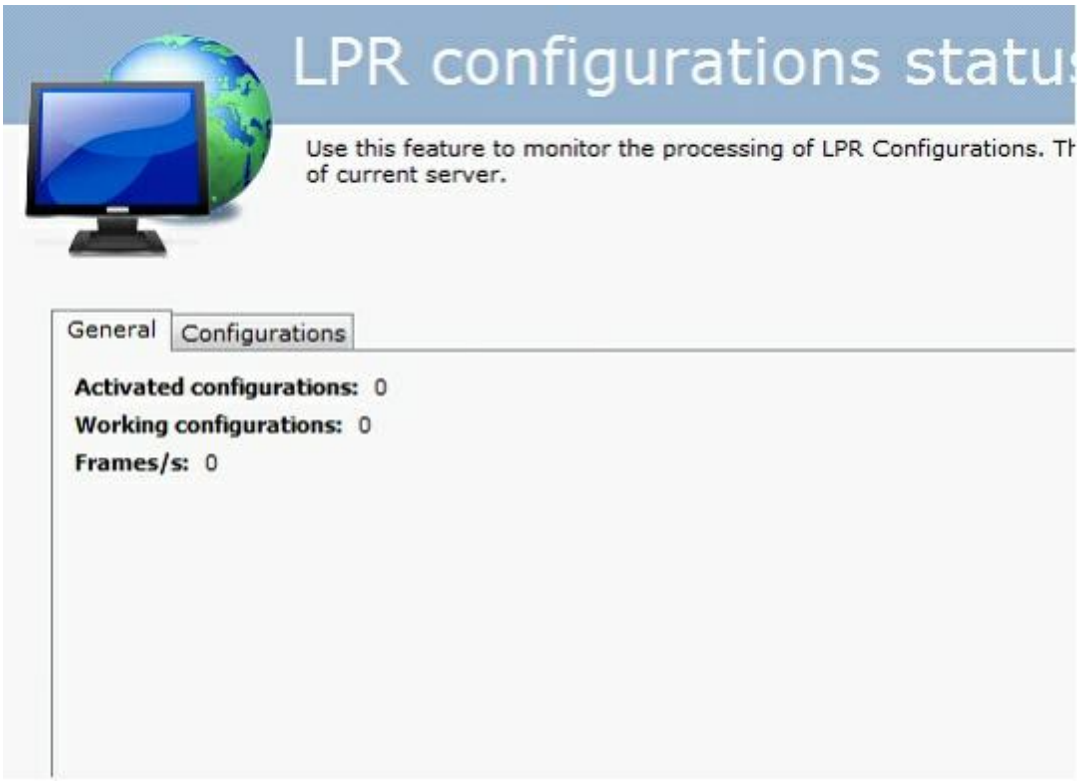


15.3.3 Verifying the LPR Status

The Status option will give you all the information on LPR configurations, such as: number of active LPR configurations, number of active LPR configurations, among other functions shown below.

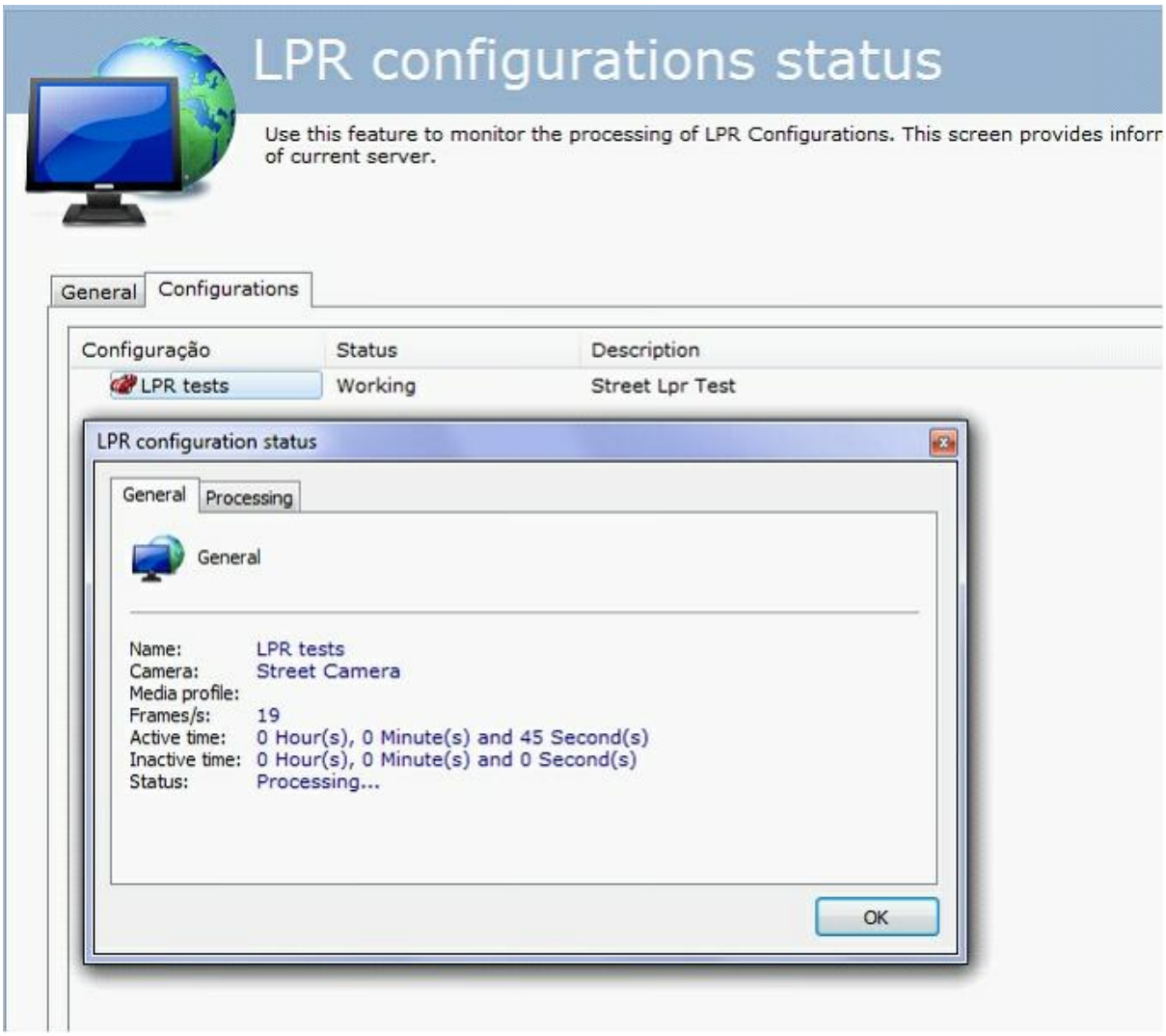
With the **Status** option you can check different information regarding the configurations made as shown in the following pictures:

© 2002 - 2020 by Digifort, all rights reserved



- **Active Configurations**: LPR configurations active at the time.
- **Working Configurations**: Working LPR configurations.
- **Frames**: Number of frames processed.

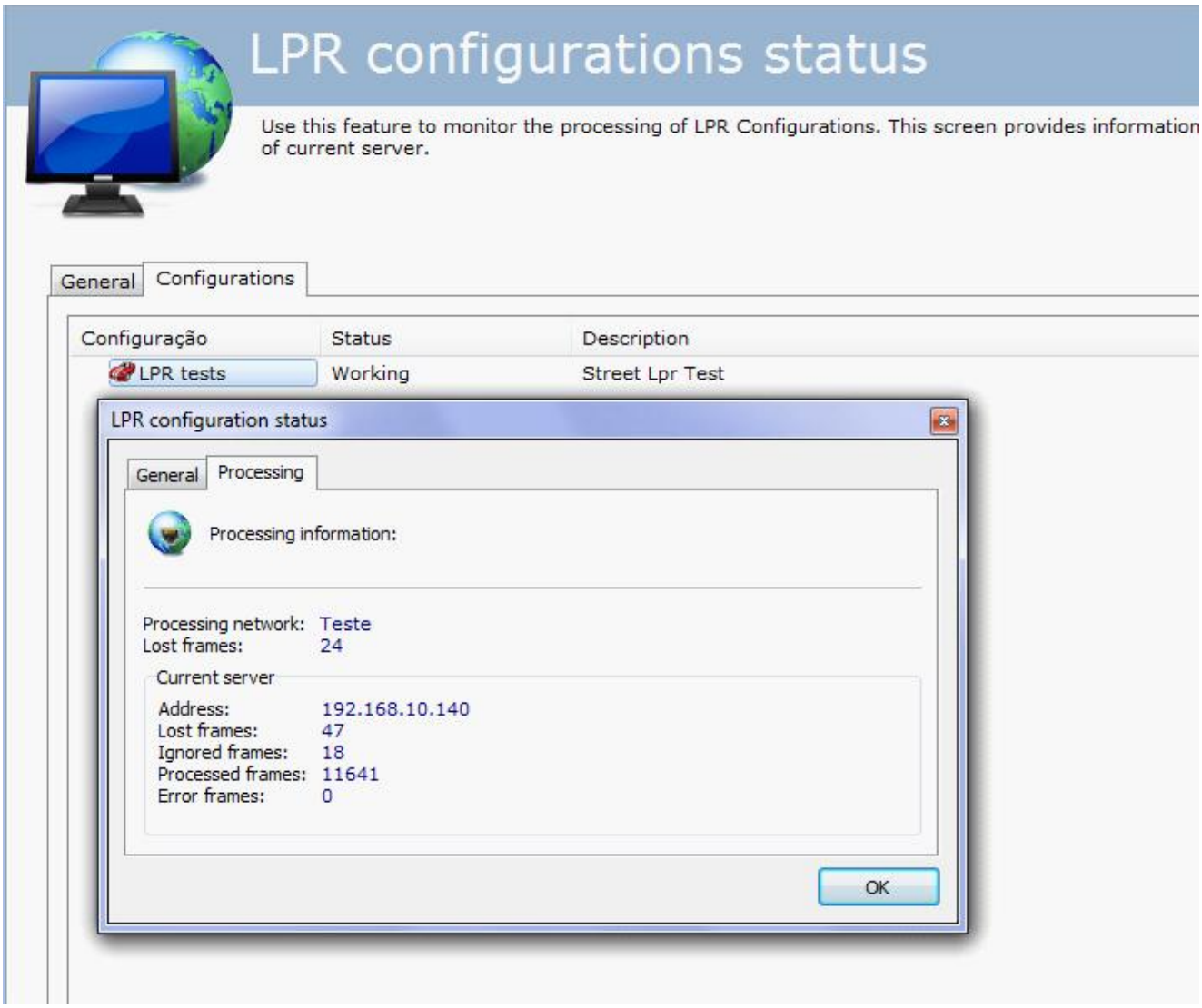
© 2002 - 2020 by Digifort, all rights reserved



In the **General** tab you'll have information such as:

- **Name**: Name of the active configuration
- **Camera**: Name of the camera being processed by the engine.
- **Media profile**: Media profile used for processing.
- **Frames**: Number of frames processed.
- **Active Time**: Time the configuration has been active up to that point.
- **Inactive Time**: Time the configuration has been inactive to that point.
- **Status**: Status of the active configuration.

© 2002 - 2020 by Digifort, all rights reserved



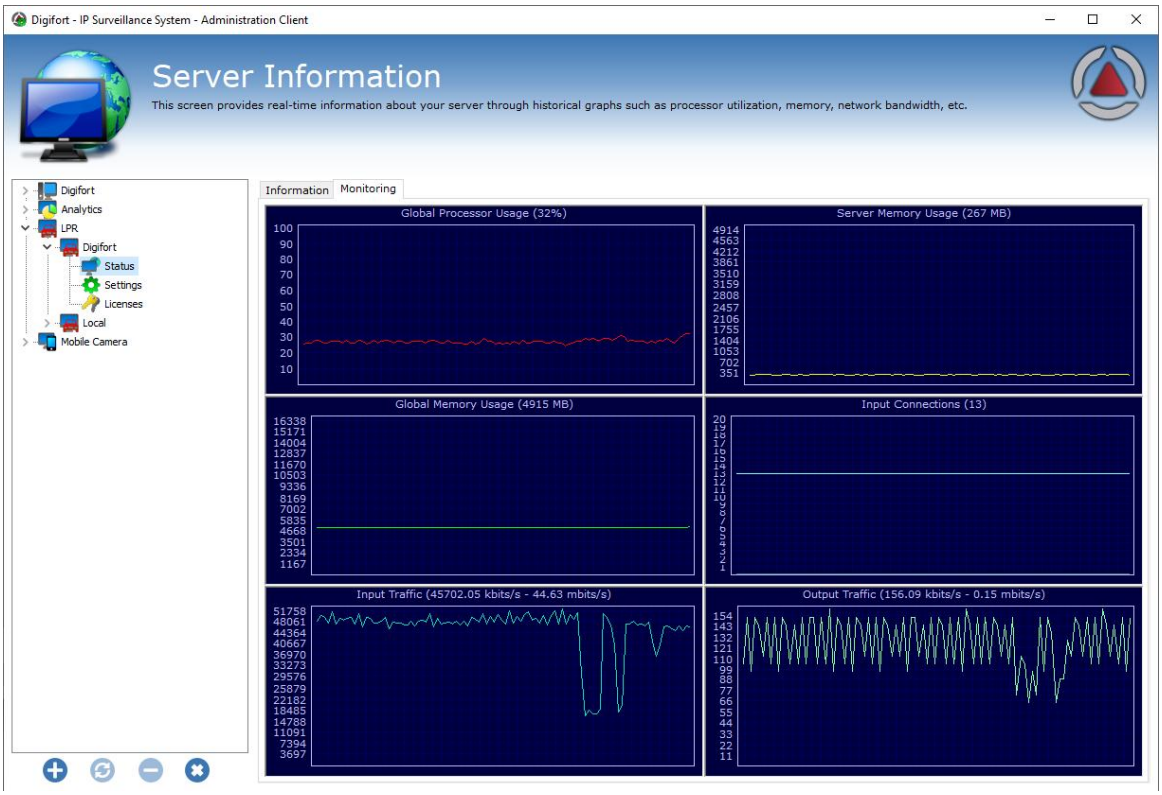
- **Processing Network:** Name of the processing network that is processing the current configuration.
- **Lost Frames:** Frames perdidos na análise no Servidor.

Current server:

- **Address**: Address where the configuration is being processed.
- **Ignored Frames**: Frames ignored by the server.
- **Processed Frames**: Total frames processed.
- **Error frames**: Frames that reached the server with errors.

LPR also offers a status monitoring option with graphics:

© 2002 - 2020 by Digifort, all rights reserved

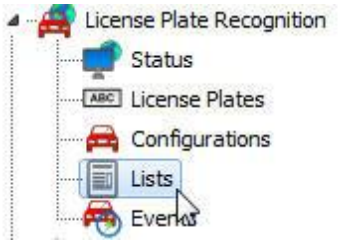


15.3.4 Configuring the LPR lists

To create an alert action in the plate recognition, you must first create lists that contain the registered plates.

The lists allow a better control of alerts and events. For example: a plate can be inserted in a list that gives the car access to gatehouse 1 and also in another list which gives access to gatehouse 2 in a company. Each of the lists can relate to different events in Digifort.

To register the list click on **Lists** as in the image below:

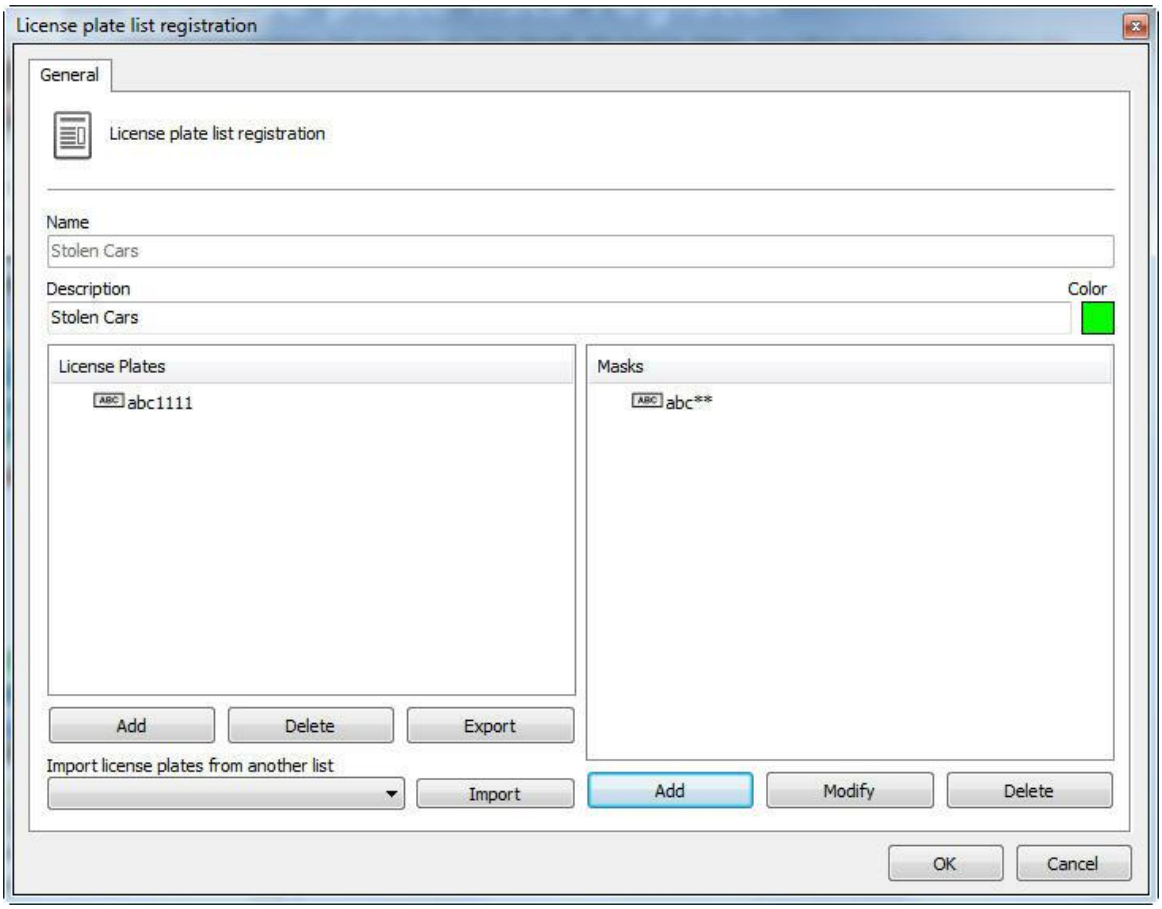


© 2002 - 2020 by Digifort, all rights reserved



To create a new list click on **Add**

© 2002 - 2020 by Digifort, all rights reserved

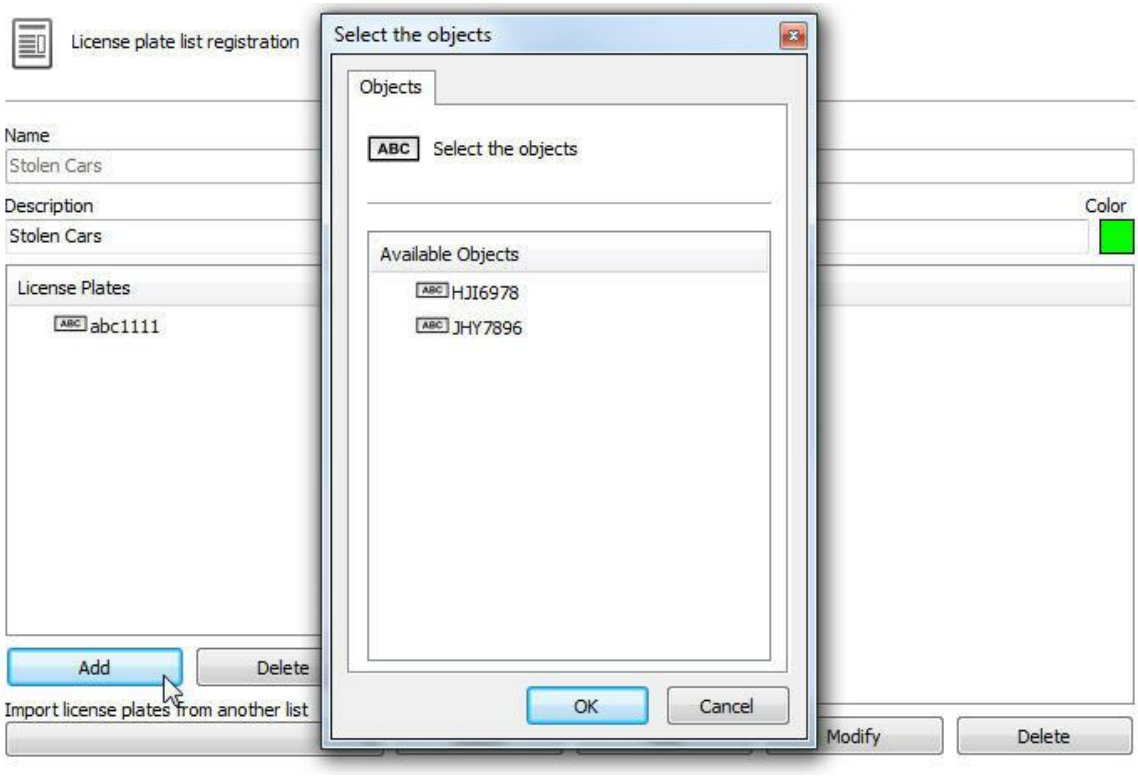


On this screen, click on Add. After clicking, the plates registration screen is displayed, where you have the fill in the fields:

- **Name**: The list name. Example: Gateway 1 list, City 2 list.
- **Description**: Desired list description. Example: Stolen cars, allowed cars, etc.
- **Color**: Color associated with this list. This color is visually displayed on the surveillance client when the list triggers an alert.
- **License Plates**: List of plates that can trigger the alerts. These plates are added from the plate register already done. Check the previous topic on this manual.
- **Masks**: The masks have the purpose of considering, at the recognition time, only some parts of the plate to trigger events in Digifort. Check examples in the next topic.
- **Import plates from another list**: To facilitate registration, you can import the plates already registered in another list.

To add a plate on the list, simply click on **Add** and a window opens to show the available plates that were pre-registered:

© 2002 - 2020 by Digifort, all rights reserved



Select the plates you want, and then click on **OK**.

It is also possible to **Delete** the plates in the list **export them** to a text file. To export, simply click on **Export** and select the directory to save the text file.

You can import plates from any type of text document. Simply click on the **Import** button and select a text document that has the plates. In this document, the plates must be organized in different lines.

To delete the plates from the list, simply select one or more plates and click on the **Delete button**.

15.3.4.1 Masks

The masks have the purpose of considering, at the recognition time, only some parts of the plate to trigger events in Digifort. The mask added is applied to all plates registered in the list.

The mask compares the results with the specified mask parameter, keeping only the valid results.
The mask consists of literal characters, sets and wildcards values.
Each literal character must match a single character in the string. The literal character comparison is case-insensitive.
Each set begins with opening bracket ([) and ends with closing bracket (]). Between the brackets are the elements of the set. Each element is a literal character or an interval.
Intervals are specified by an initial value, a hyphen (-), and a final value. Do not use spaces or commas to separate the set elements. A set must correspond to a single
character in the string. The characters correspond to the set if it is the same character as any literal character from the set, or if it is in one of the intervals of the set. A character is in an interval if it

© 2002 - 2020 by Digifort, all rights reserved

matches the initial value, final value, or if it is between the two values. If the first character after the opening bracket of a set is an exclamation point (!), then the set matches any character that is not in the set (negative).

Asterisks (*) or question marks (?) are the wildcards. An asterisk matches any number of characters, and any character. A question mark matches any simple character.

Examples:

Match any character that is not in the set (negative).
Asterisks (*) or question marks (?) are the wildcards. An asterisk matches any number of characters and any character. A question mark matches any simple character.

Examples:

Mask: ABC*
Result: Gets all records that start with ABC.
Examples: ABCD, ABC123, ABCXYZ

Mask: ABC*123
Result: Gets all records that start with ABC and end with 123
Examples: ABCD123, ABC123, ABCXYZ123

Mask: ABC?123
Result: Gets all records that start with ABC, have a character and end with 123
Examples: ABCD123, ABCX123, ABCY123

Mask: ABC??23
Result: Gets all records that start with ABC, have any two characters and end with 23
Examples: ABCD123, ABCXR23, ABCY923

Mask: ABC[XYZ]123
Result: Gets all records that start with ABC, have a character from the set (X, Y or Z) and end with 123
Examples: ABCX123, ABCY123, ABCZ123

Mask: ABC[!XYZ]123
Result: Gets all records that start with ABC, have a character outside the set (other than X, Y or Z) and end with 123
Examples: ABCD123, ABCE123, ABCF123

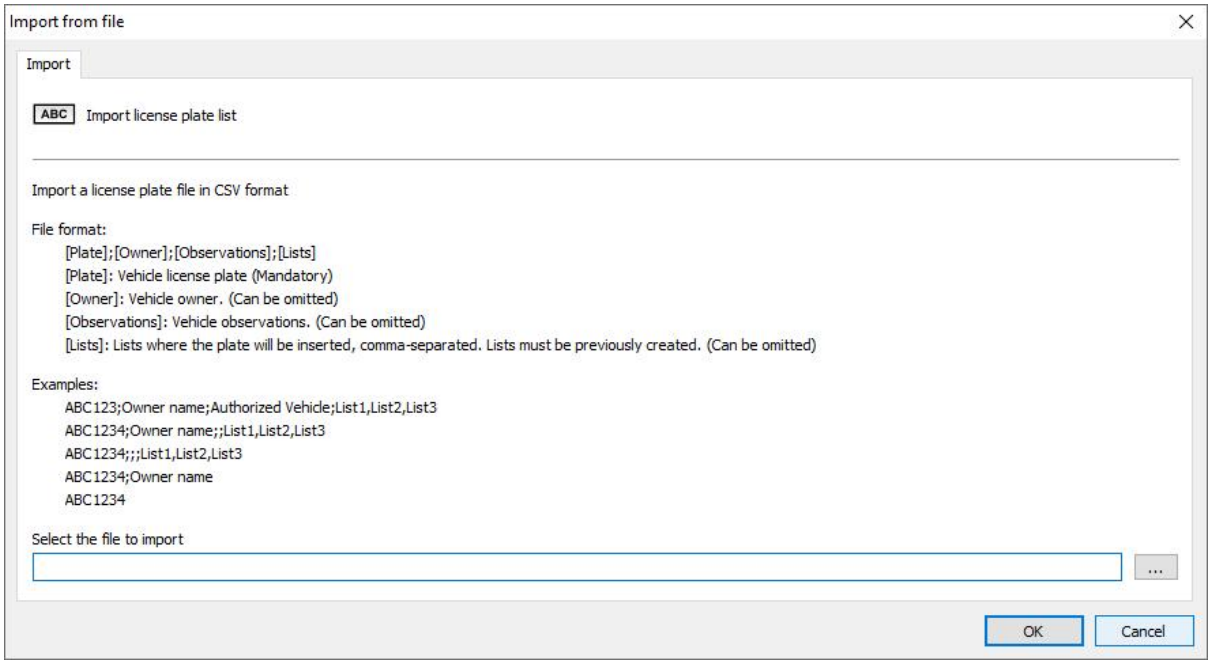
Mask: ABC[D-G1-3]
Result: Gets all records that start with ABC and have a character from the set (D to G) or (1 to 3)
Examples: ABCD, ABC3, ABCF

Mask: ABC[D-G1-3]??[!ABC1-3]XYZ*
Result: Gets all records that start with ABC, have a character from the set (D to G) or (1 to 3), have any two characters, have a character outside the set (other than ABC and outside the interval from 1 to 3), have the literal characters XYZ and end with any character string.
Examples: ABCD12UXYZ, ABC2Y1UXYZ12345: ABC*

© 2002 - 2020 by Digifort, all rights reserved

15.3.4.2 Importing plates with lists

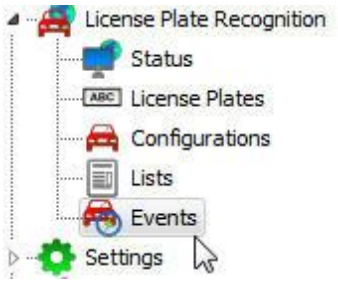
The plate list importer allows you to specify which lists the plate belongs to.



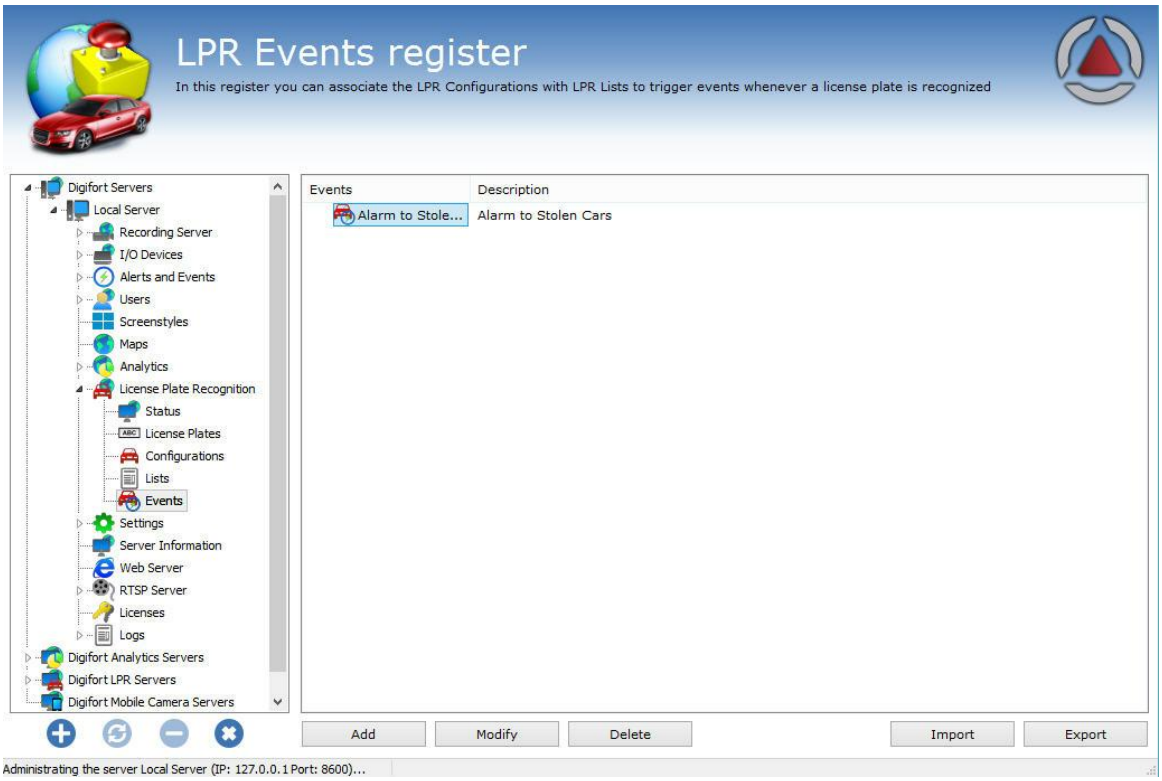
15.3.5 Events

On the LPR event screen, you can associate a list of plates to a specific camera and generate events in Digifort.

To access this function, click on **Events** as the image below:

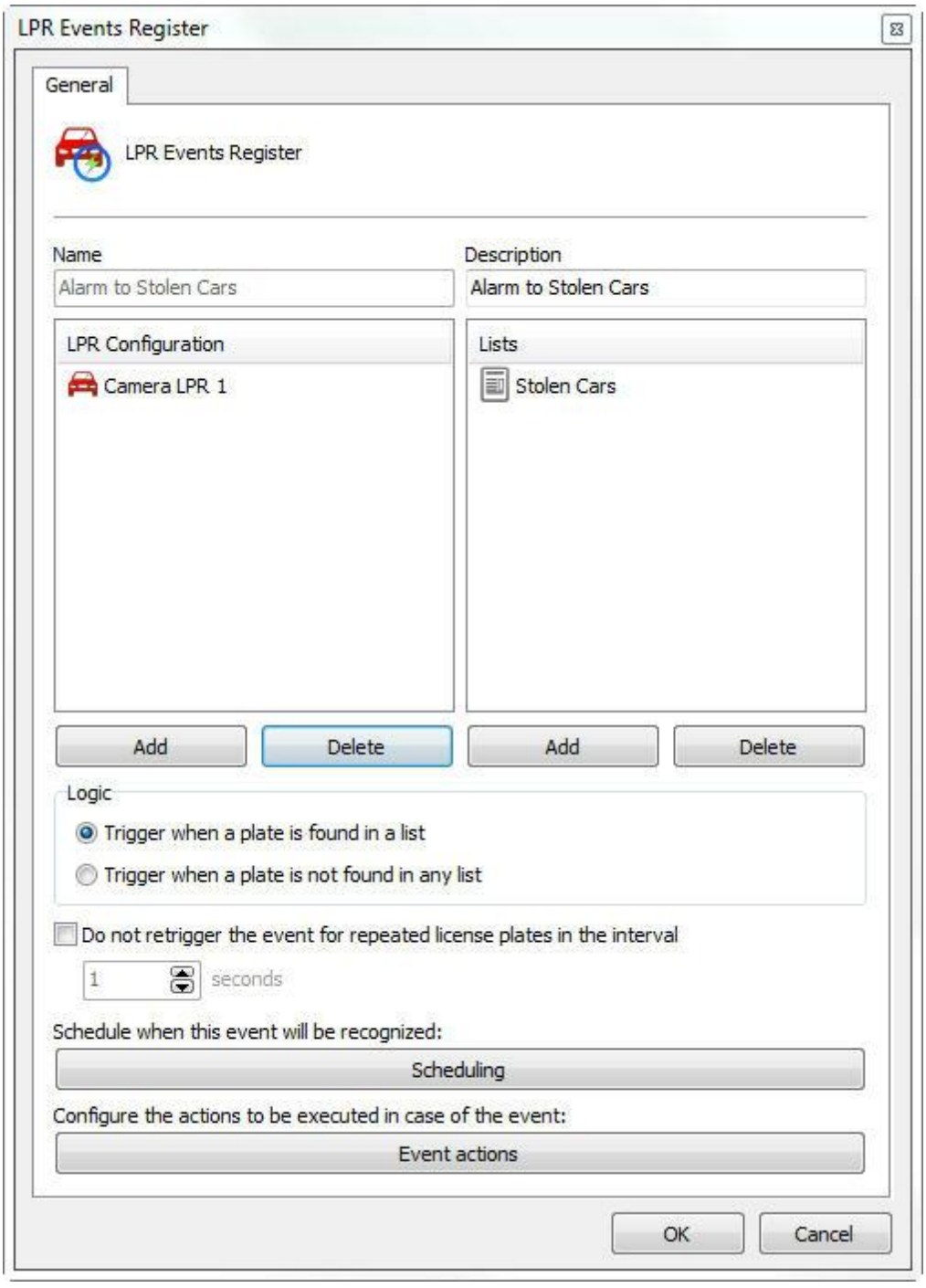


© 2002 - 2020 by Digifort, all rights reserved



To create a new event, click on **Add**. The following screen appears:

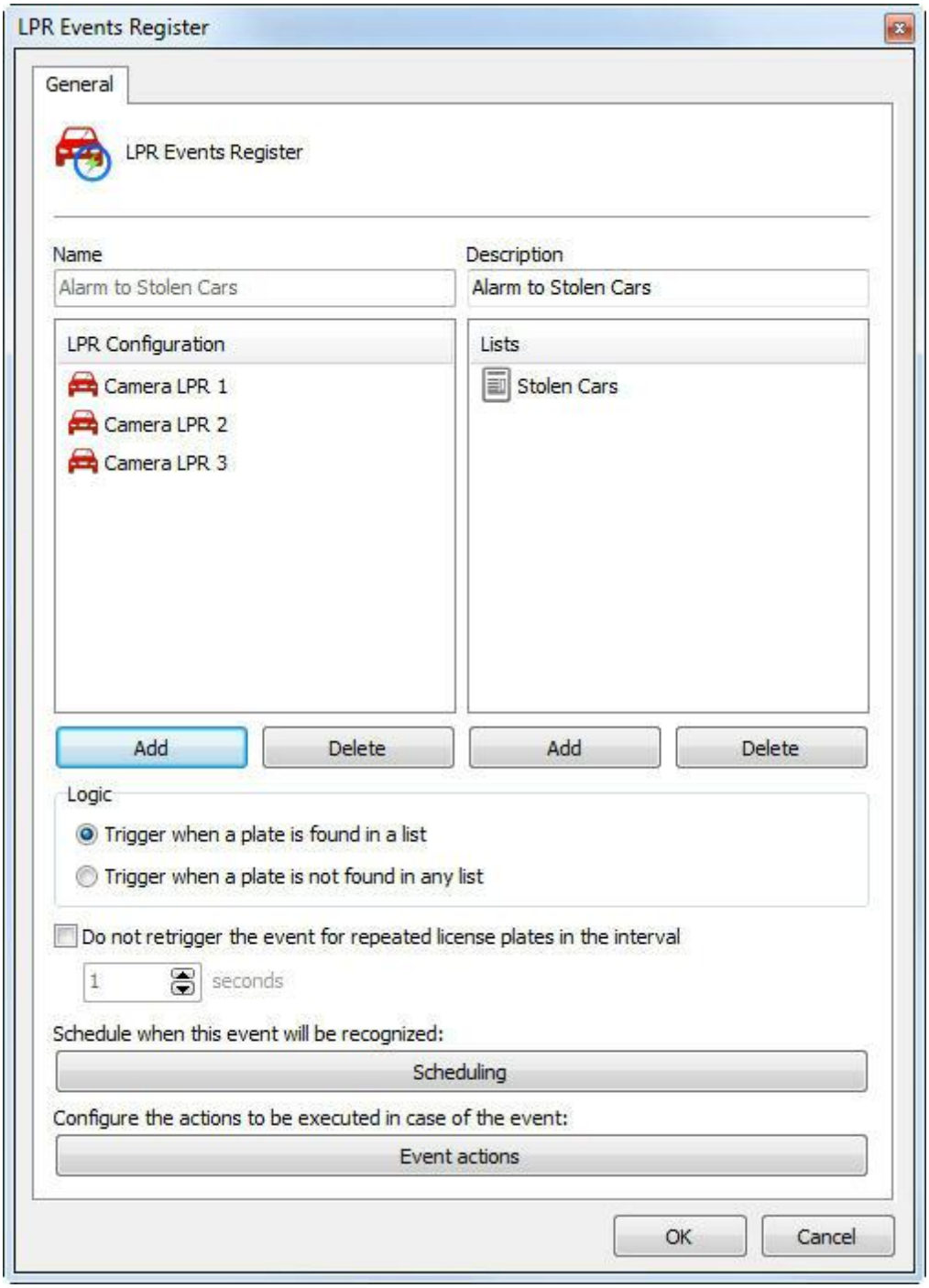
© 2002 - 2020 by Digifort, all rights reserved



On this screen, you must associate the lists of plates that will trigger an event, such as Stolen Cars, and associate one or more LPR settings.
The configuration from the picture above shows that, if any plate in the **Stolen Cars** list is recognized by the "**LPR Camera 1**" setting, an event is generated.

In the image below, there is the following example:

© 2002 - 2020 by Digifort, all rights reserved



The same happens if any plate from the Stolen Cars list is recognized by "**LPR Camera 1**", "**LPR Camera 2**" or "LPR Camera 3". An event is generated. Or vice versa.

Logic: The LPR allows events to be triggered when a card is found in one of the selected lists or when not found.

© 2002 - 2020 by Digifort, all rights reserved

- **Trigger when a card is found on a list:** It triggers the events set, in the case of the recognized card belonging to some of the selected lists.
- **Trigger when a card is found on a list**:It triggers the events set, in the case of a recognized card not belonging to any of the selected lists.

- **Do not trigger the event for repeated plates in the interval of seconds**: This option allows the user to select a minimum time for the event to be repeated for repeated plates.
- **Trigger the event only for vehicles above a speed**: This option will cause the event to be triggered only if the vehicle is above a certain speed (km / h).

15.3.5.1 Conditions for Triggering Events

LPR events support multiple trigger conditions.
Using trigger conditions, you can restrict when an LPR event will be triggered, offering great configuration flexibility.

Conditions:

- Not re-trigger the event for repeated plates in an interval - this option prevents the system from triggering the LPR event if the same plate is recognized in a set time interval.

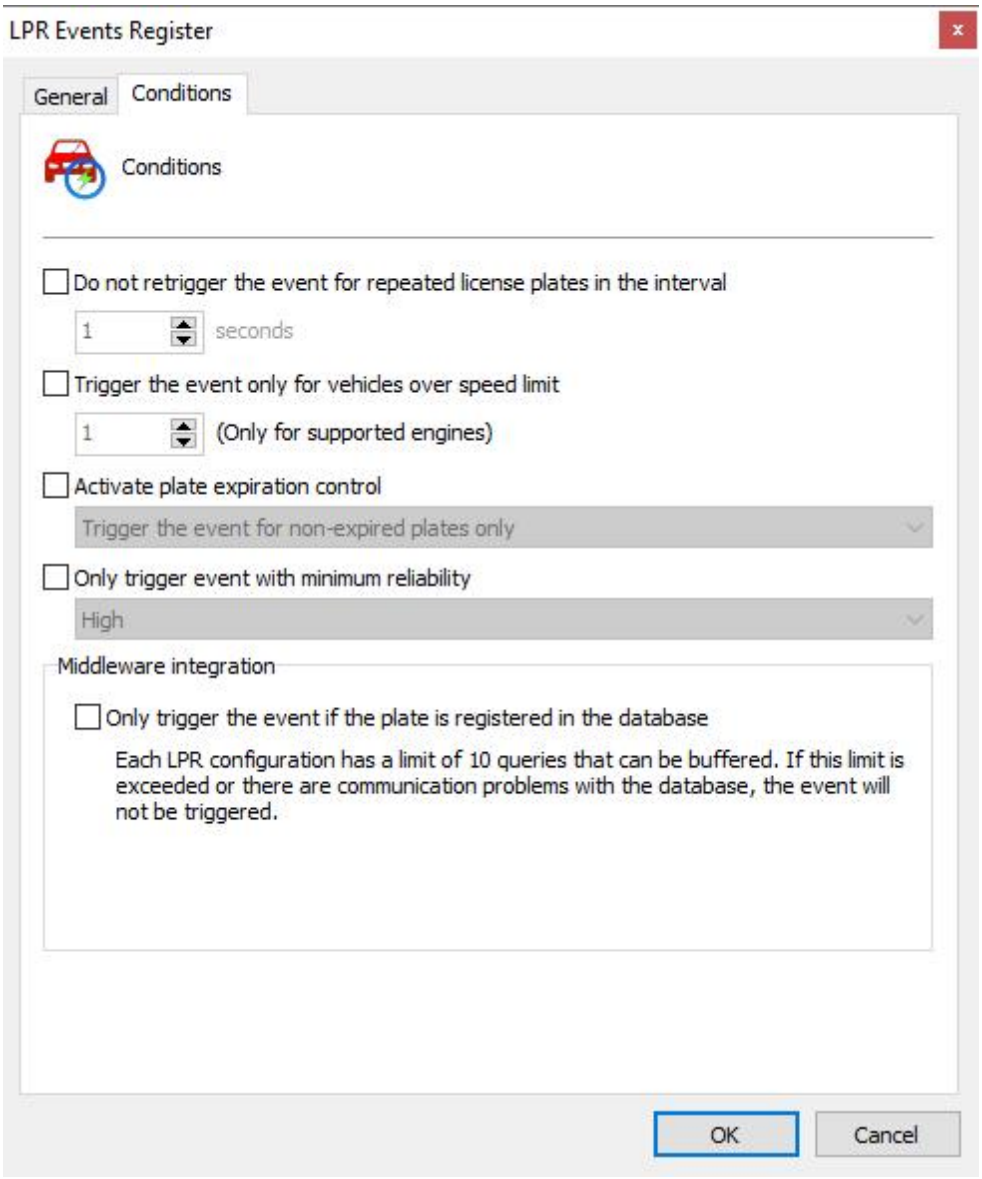
- It triggers the event only if the vehicle is above the set speed.

- Plate expiration control - this option allows to condition event triggering to plate expiration.

- Trigger the event only with minimum reliability - this option prevents the system from triggering the LPR event if the plate recognition result does not reach a minimum level of reliability.

- (Middleware) It triggers only if the plate is registered in a database - this option allows the event to check whether the plate is registered in an external database (through the use of LPR Middleware for integration with external databases) and conditions, it triggers only if the plate is found on the database.

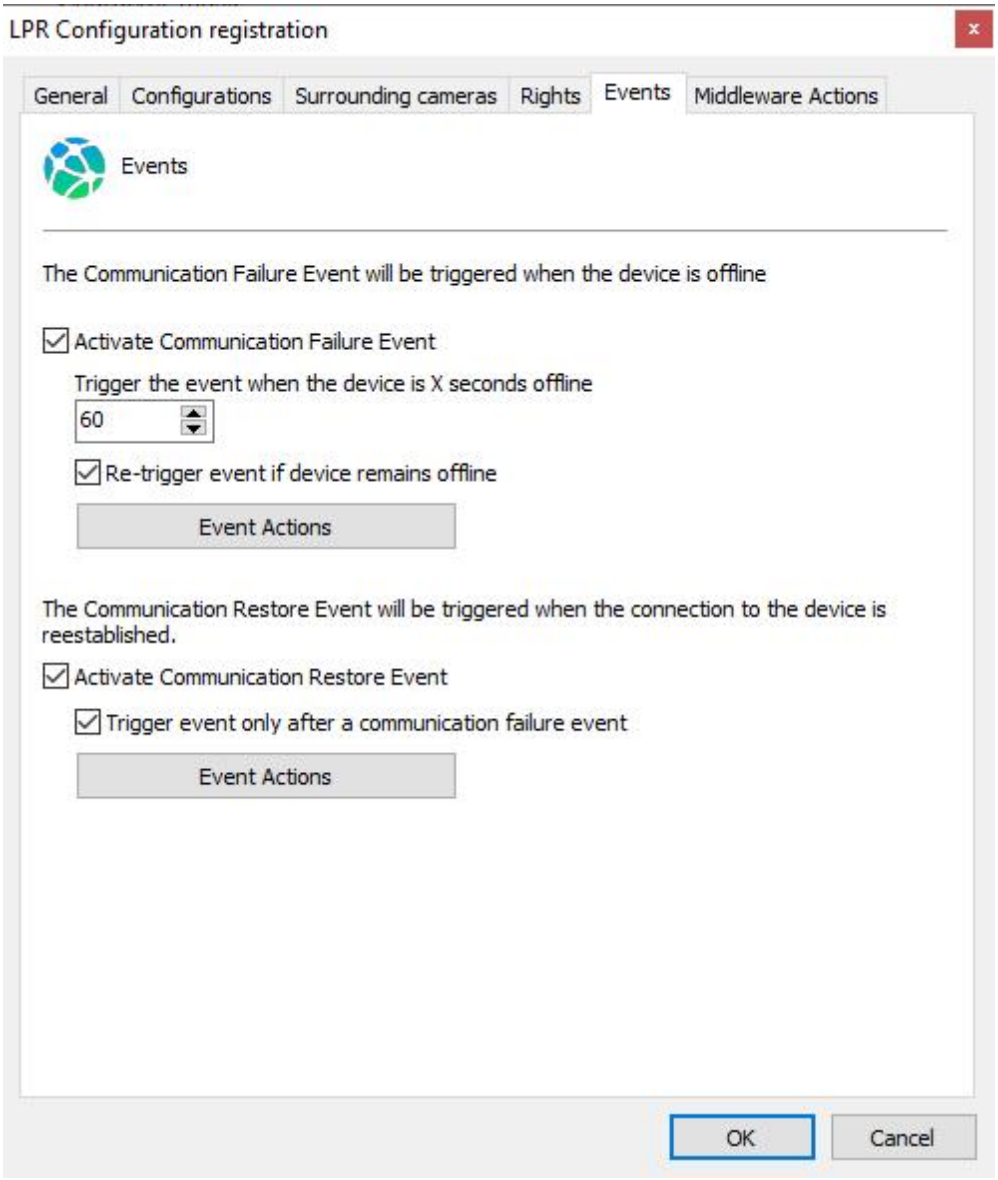
© 2002 - 2020 by Digifort, all rights reserved



15.3.5.2 Evento de Falha e Restauração

The LPR event configurations have Communication Failure and Communication Restore events. This feature works exactly as explained in the Communication chapter

© 2002 - 2020 by Digifort, all rights reserved

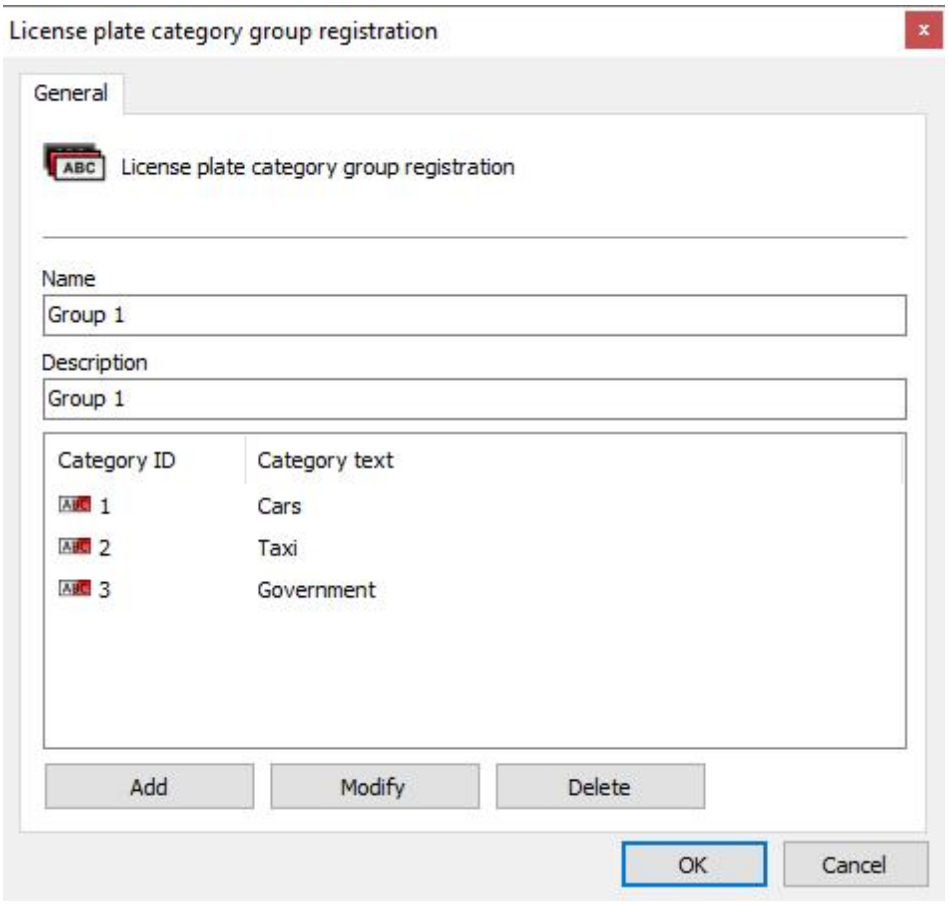


15.3.6 Plate category groups

The plate category groups feature uses a plate categorization feature of the ARH Carmen engine that is able to differentiate the type of plate (for example, cars, taxi, motorbikes...) through a category code that is provided by the engine.

This feature was specifically developed for countries in the Middle East where license plate categorization is important to identify the type of vehicle, but it should work for other countries if the LPR engine supports license plate categorization

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter XVI

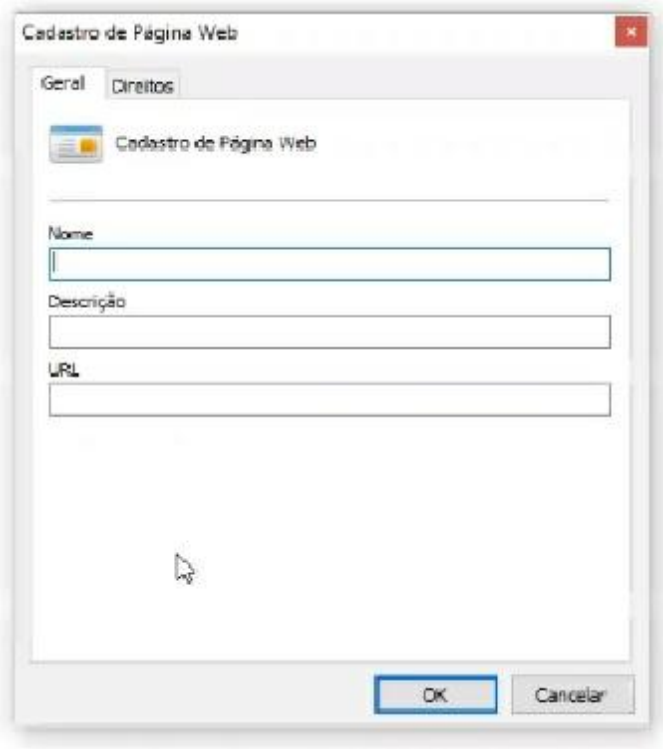
16 Páginas Web

Register and configure the Web pages that will appear in your system objects, in the Surveillance Client.

Through the new “Web Page” objects, registered through the Administration Client, you can add preconfigured links for web pages or web systems that can be accessed by system operators.

Examples of integrated browser use:

- Integrate third-party web systems on the same camera management interface. Systems such as access control, alarm control, face recognition, among others, now can be opened and operated through the Surveillance Client.
- Display dashboards on a video wall or on operator stations.
- Access predefined sites.
- Free browsing.



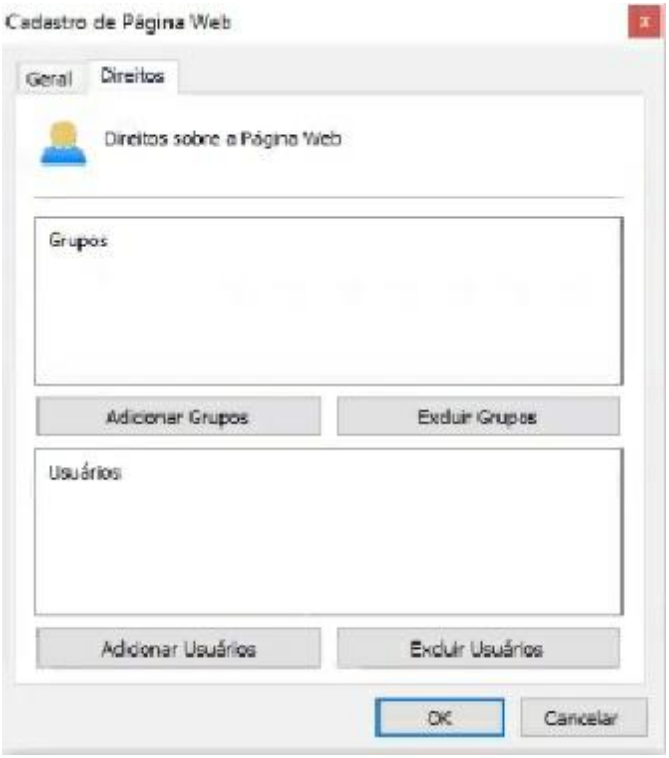
- Name: Name that the registration will display on the Surveillance Client.
- Description: Description that the registration will display on the Surveillance Client.
- URL: Link to the page that will be opened on the Surveillance Client.
  Note: if the URL is left blank, the user may enter the site address within the Surveillance Client, e.g.:

ex.:

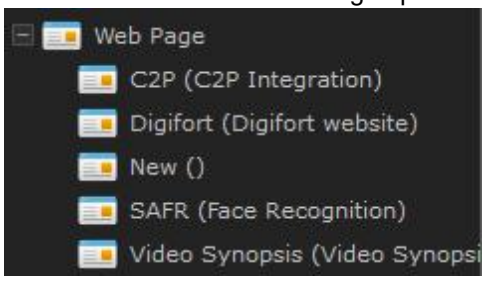


© 2002 - 2020 by Digifort, all rights reserved

Defina quais usuários e grupos de usuário terão o direito de ver/navegar na página cadastrada.



Defines which users and user groups will have the right to view/browse on the registered page.



The browser associated with the pre-registered pages will not provide the address bar, thus preventing the operator from accessing any site or page other than the specified page, but it is possible to release the address bar for free browsing by creating a web page object with a blank address. In this case, when the operator enters this object on screen, the browser will provide the address bar for browsing.

We use the Chromium browser by default, which is already embedded in the Surveillance Client, but you can use Internet Explorer 11 native to Windows by editing the browser option in the Surveillance Client options.

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter XVII

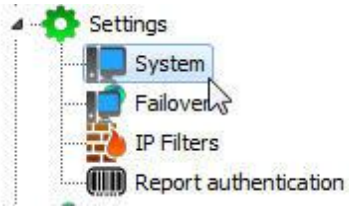
17 Configurations

17.1 Global Configurations

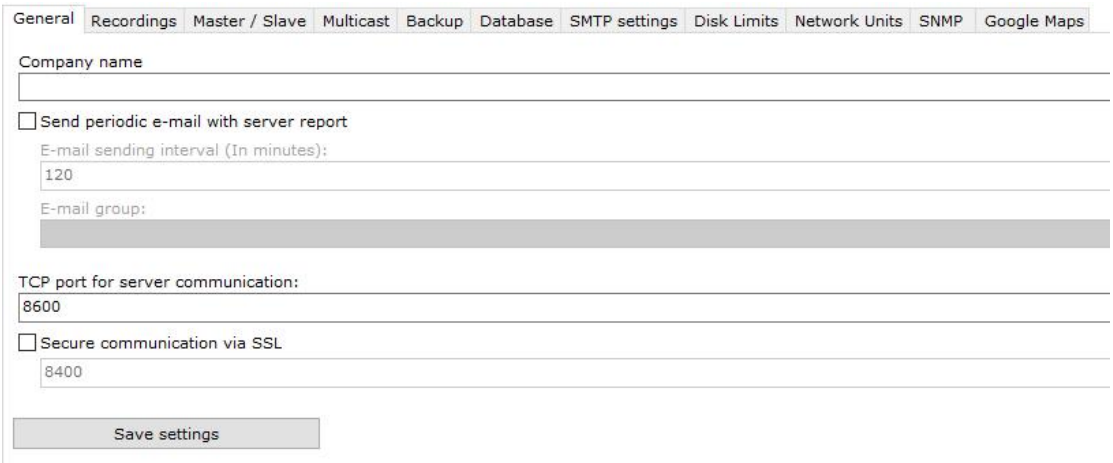
Esta área do sistema é reservada para o ajuste das configurações globais do servidor.
As configurações globais são parâmetros que depois de configurados afetarão todo o funcionamento do sistema.

17.1.1 General Configurations

To access this area, click on the Configurations item in the Configurations Menu, as illustrated in the figure below:



Once this is done, the general system configurations screen opens on the right, as illustrated in the figure below:



- **Company name**: The company name is used when you export a video in order to facilitate the surveillance client operation.
    - **Send periodic e-mail with server report:** Sends e-mail with a server report periodically to the specified alert group in the specified time interval. This report contains information such as user accesses to the system and recording status.
    - **TCP communication port with the server:** Communication port by which the Surveillance Client and the Administration Client will communicate with the server. After modifying this configuration, it's necessary to modify the communication port of the server register of the

© 2002 - 2020 by Digifort, all rights reserved

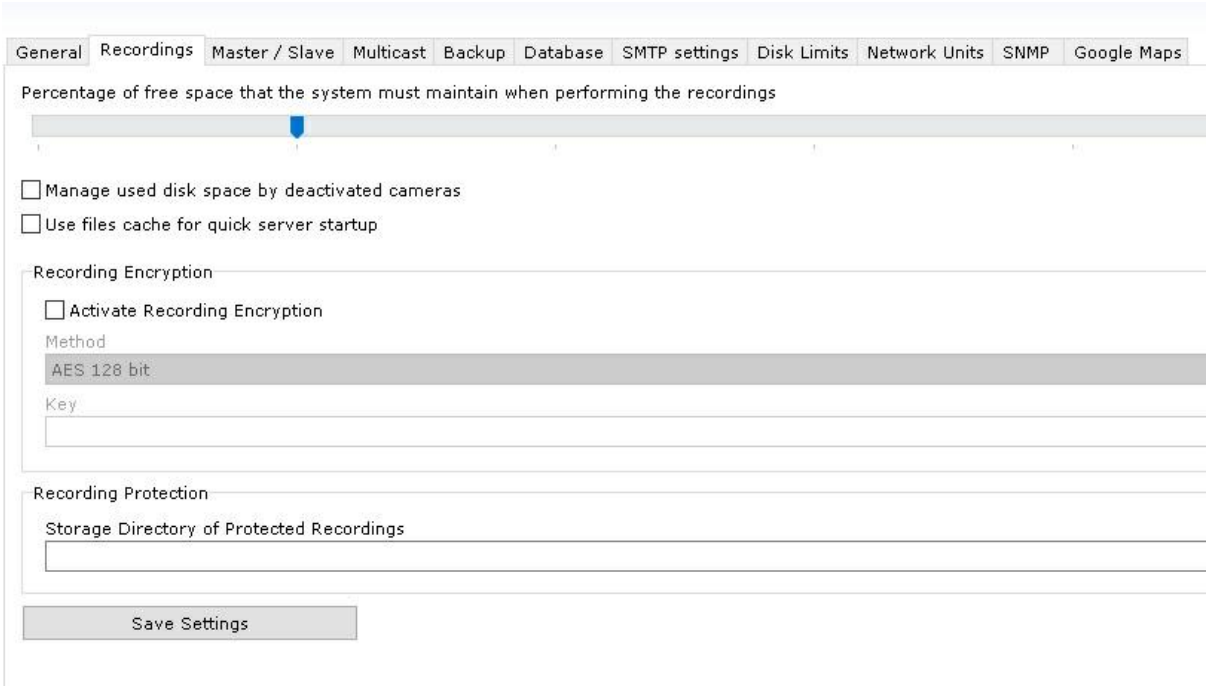
Administration Client and the Surveillance Client. To learn how to carry out this configuration in the Surveillance Client, see How to configure the servers to be administrated. To learn how to modify the port in the Surveillance Client, consult its manual..

- **Secure communication via SSL:** Communication port where the Monitoring Client and the Administration Client will communicate with the server via SSL.

After adjusting the configurations, click on the Save Configurations button so that no modification is lost.

17.1.2 Recordings

On this tab, you can configure some advanced options related to image recording.



- **Percentage of free space that the system must maintain when performing recordings**: Enter here the percentage of disk space you want to reserve for other applications external to Digifort. For example, in case an 80GB hard drive is used, with a free disk space percentage of 2%, 16GB would not be used by Digifort for recordings, being directed to other software, such as the operating system. This limit is also applied to "Disk Limits". To learn how to create a disk limit, see 'Disk Limits'.

- **Use file cache for quick server startup**: In systems where the number of days of recording is very high, the act of restarting the Digifort service can take a long time: 30, 40 60 min. This option makes Digifort able to start up much faster keeping a map of the recordings used previously before the system stopped. It is not recommended to use this option if you have problems with power failures on your server, as this can corrupt the recordings on the system.

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

Após o ajuste nas configurações clique sobre o botão **Salvar Configurações** para que nenhuma

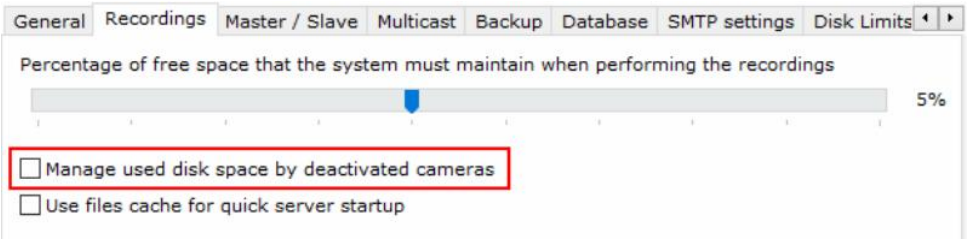
© 2002 - 2020 by Digifort, all rights reserved

alteração ser perdida.

Important

The percentage of free disk space reserves a disk space for applications external to Digifort. By default, it is set to 2%. If there is a lot of disk space available for recordings, this percentage may be too high.

NOTE: The recording system has the option of managing the disk space used by deactivated cameras. Previously, if the camera was deactivated, its recordings were not deleted during recording recycling. With this option activated, all deactivated cameras will also enter recording recycling and their recordings will be deleted according to the set time. This option is important for Failover servers (where cameras are usually always deactivated) and compliance with protection laws for GDPR and LGPD data, which define themaximum retention period for images.



17.1.2.1 Record protection

Inform the storage location of the protected recordings. This location will be where the recordings will be saved and will not be deleted as recycling is reached. For more information see the monitoring client manual

17.1.2.2 Recording encryption

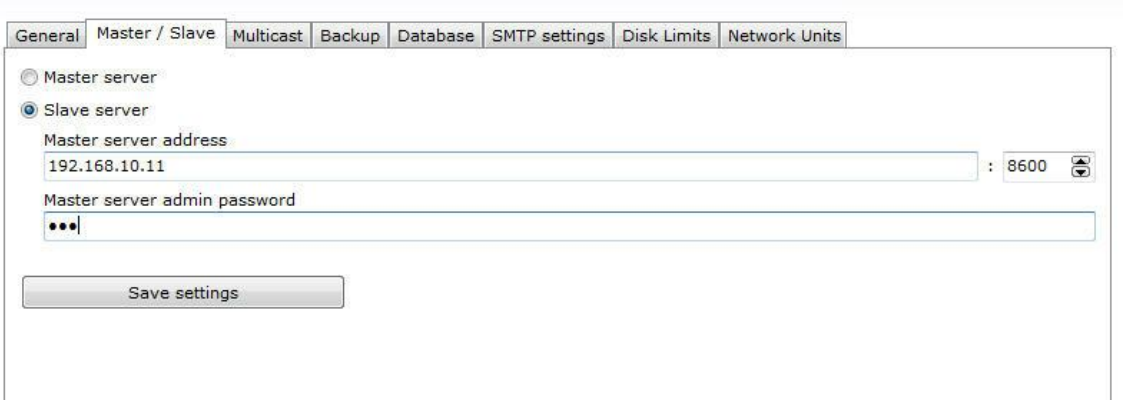
This option will encrypt recording data stored on the server itself, using either AES 128-bit or 256-bit encryption. Once the key is configured, it cannot be changed. This is because if the key is changed, the old recordings would become impossible to be read.

17.1.3 Master / Slave

The master / slave option was developed in case there is more than one server with Digifort that needs to share user information, user groups, contacts, contact groups, and screen styles.

The server by default is always **Master**. To be configured as **Slave** simply select the ‘slave' option and fill in the fields as indicated below: The **Slave** server will import all the **Master** server configurations.

© 2002 - 2020 by Digifort, all rights reserved



The screen has the following functionalities:

- **Master server address:** The master server's IP address or server DNS from where the user information, user groups, contacts, contact groups and alerts will be replicated.
- **Password of the master server's admin user**: Password of the admin user for server access.

In the items for synchronization, it is possible to select which items the slave server will inherit from the master.

For the settings to take effect click on **Save Settings**, you will notice that all the information has been exported successfully.

For more information on how to use the Master / Slave system with plate recognition, navigate to the LPR configuration tab

17.1.3.1 Sharing Plate Data between Master/Slave

When the LPR synchronization option between Master / Slave is activated, Plate Registration, List Registration, and Plate Category Registration will be shared between the servers.

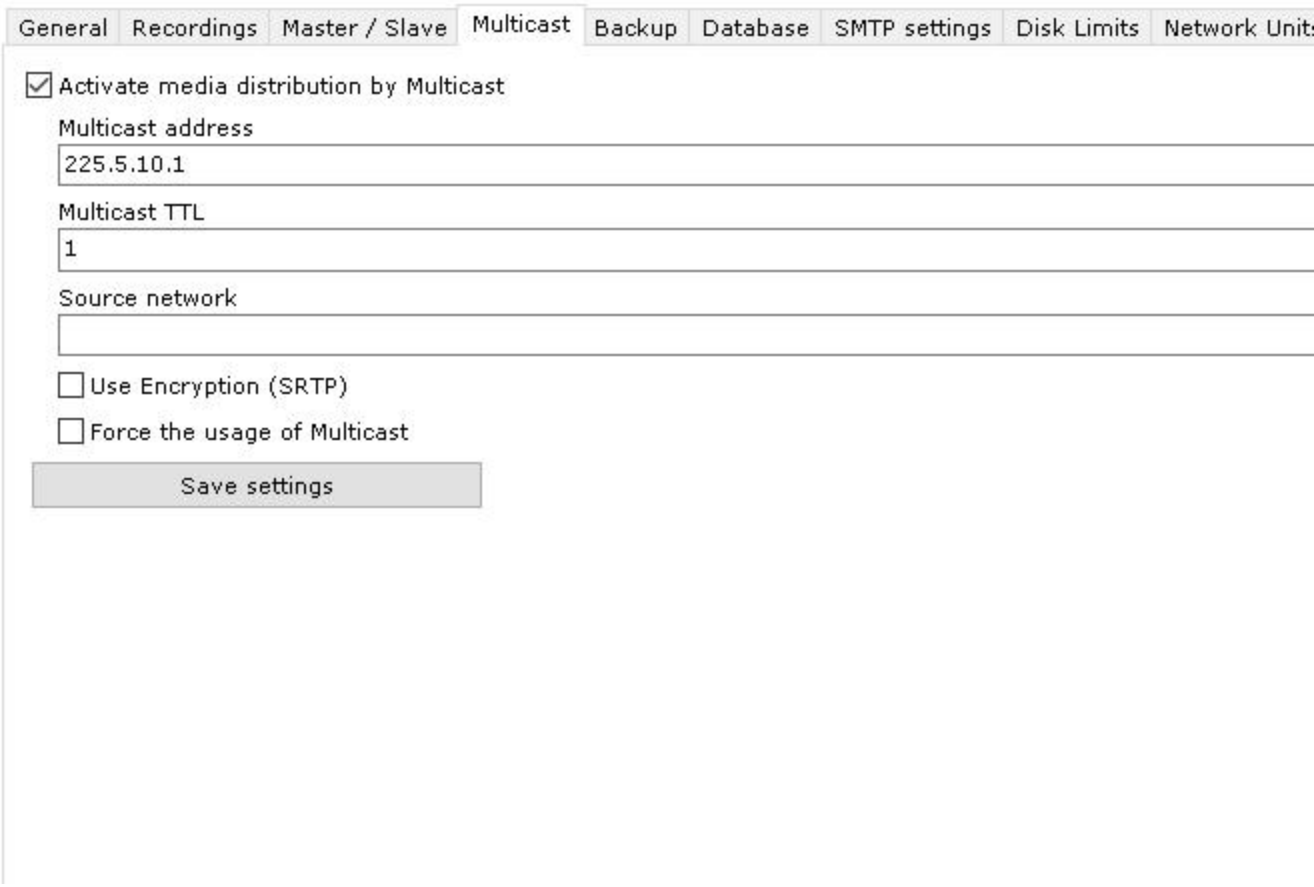
Generally, object registration is only allowed on the Master server, however, in the case of LPR, you can register plates through the Surveillance Client, connected to a Slave server only, and theSlave server will share the data with the Master, and the Master will forward the data to the other Slave servers.

17.1.4 Multicast

Essa opção permite que o servidor Digifort envie os vídeos aos Clientes de Monitoramento via comunicação Multicast.
Multicast é a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções.
No caso do Digifort, é apenas recomendado o uso de Multicast na seguinte situação: Vários clientes de monitoramento que monitoram as mesmas câmeras na tela. Caso contrário pode haver um alto indice de tráfego de informação causando problemas na rede.lado

Segue abaixo a tela de configuração das opções multicast:

© 2002 - 2020 by Digifort, all rights reserved



Essa tela possuí as seguintes configurações:

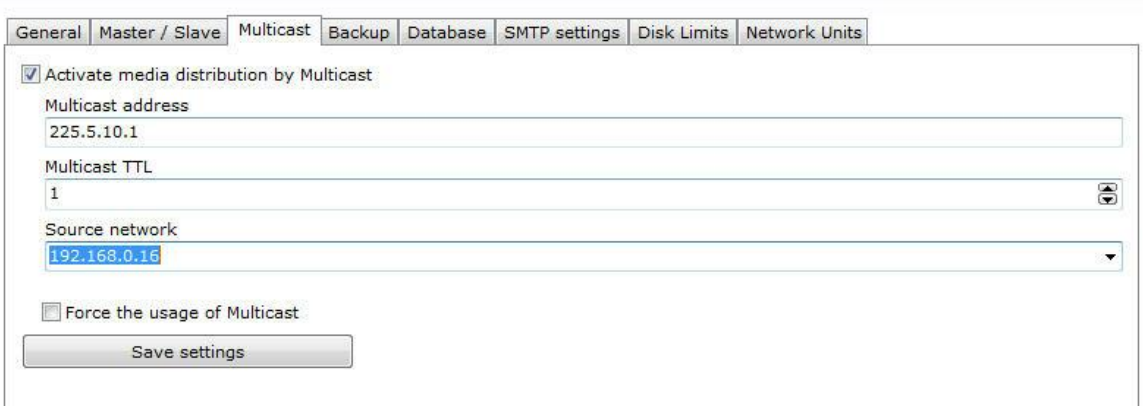
- **Ativar a distribuição de vídeo via Multicast (Activate media distribution by Multicast):** Habilita o envio de fluxo de vídeo via multicast..
- **Endereço do Multicast (Multicast address):** Considerando a arquitetura IPv4 de nomenclatura IP e as melhores práticas, é conhecido que o range de IP reservado para a prática do multicast é: 224.0.0.0 até 239.255.255.255. Por esse motivo, como padrão o Digifort adotou o IP 255.5.10.1 que pode ser modificado a qualquer momento.
- **Multicast TTL:** Permite mudar o TTL do pacote multicast. Configuração necessárias para algumas marcas de switchs.
- **Rede de origem:** Selecione a rede de origem para a transmissão do multicast.
- **Forçar o uso do Multicast (Force the usage of multicast):** Quanto a opção Multicast é habilitada, não necessáriamente o cliente de Monitoramento Digifort irá utilizá-la, pois existe uma opção por parte do cliente de monitoramento que permite a escolha do Multicast ou Unicast (Veja o manual do cliente de monitoramento). Quando a opção **Forçar o uso do Multicast** é ativada, o Servidor Digifort ignora as configurações do cliente de Monitoramento e dessa maneira eles usarão o envio de imagens via Multicast.
- **Usar Criptografia SRTP:** Quando o Cliente de Monitoramento conectar no servidor utilizando SSL/TLS, a transmissão de mídia por multicast para o client (Caso esteja configurado para transmissão de vídeo em multicast) também será criptografada utilizando o protocolo SRTP.
- **Salvar configurações (Save Configurations):** Salva as configurações desejadas.

----------OLD_TEXT----------

© 2002 - 2020 by Digifort, all rights reserved

This option allows the Digifort server to send the videos to the Monitoring Clients via Multicast communication.
Multicast delivers information to several end receivers at the same time using the most efficient strategy where messages only go through a link once and are only duplicated when the link to the end receiver is split in two directions.
In the case of Digifort, the Multicast is only recommended in the following situation: Several monitoring clients monitoring the same cameras on screen. Otherwise there may be increased movement of information causing problems to the network.

The configuration screen of the multicast options is shown below:



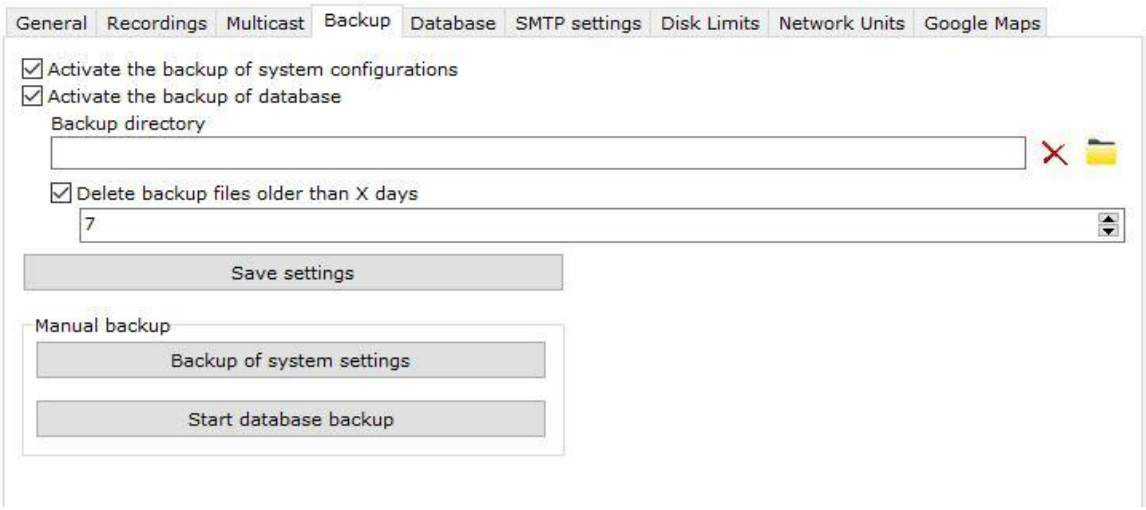
This screen has the following settings:

- **Activate media distribution via Multicast**: Enables the sending of video stream via Multicast.
- **Multicast address**: Considering the IPv4 architecture of IP nomenclature, as well as best practices, it is known that the reserved IP range for multicast is: 224.0.0.0 to 239.255.255.255. For this reason, Digifort adopted IP 255.5.10.1 as default, which can be modified at any time.
- **Multicast TTL**: It allows you to change the TTL of the multicast packet. Required settings for some brands of switches.
- **Source network**: It selects the source network for multicast transmission.
- **Force the usage 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 to allow the choice of Multicast or Unicast (see the Surveillance Client manual). When the Force the usage of Multicast option is activated, the Digifort server ignores the Surveillance Client's settings and images will be sent via Multicast.
- **Use SRTP Encryption**: When the Surveillance Client connects to the server using SSL/TLS, media transmission to the client via multicast (in case it is configured for video transmission in multicast) will also be encrypted using the SRTP protocol.
- **Save Settings**: It saves the desired settings.

17.1.5 Backup

Backup options in this tab are related to Digifort database.

© 2002 - 2020 by Digifort, all rights reserved



This screen has the following features:

- **Activate the backup of system configurations:** Select to enable the automatic backup of log files containing the settings of system registers Digifort.
- **Active the backup of database**: Click to activate the automatic backup of the database that contains the analytical events Digifort events of LPR, General events, logs, etc.
- **Backup directory**: Choose the directory where the backup files will be stored.
- **Delete backup files older than X days**: Configure the number of days on which the backup files are kept in the chosen directory.
- **Save configurations**: Saves the settings you choose.

Manual backup

- **Start database backup**: Clicking this option the Digifort backs of the log files in the directory selected in the option Digifort above.
- **Start database backup:** Clicking this option the Digifort will backup database files in the directory selected in the option above.

17.1.5.1 Restoring backups of Digifort

To restore system settings, settings made in the registers and, just run the file Digifort of record you want with the service "Digifort Server stopped.

To restore the database, replace in the installation folder on the server DIGIFORTDB "file.FDB "by the desired file with the same name and with the services "**Digifort Database Server** " and " **Digifort Server**"stopped.

To learn about services see chapter How to run Digifort Services Manager

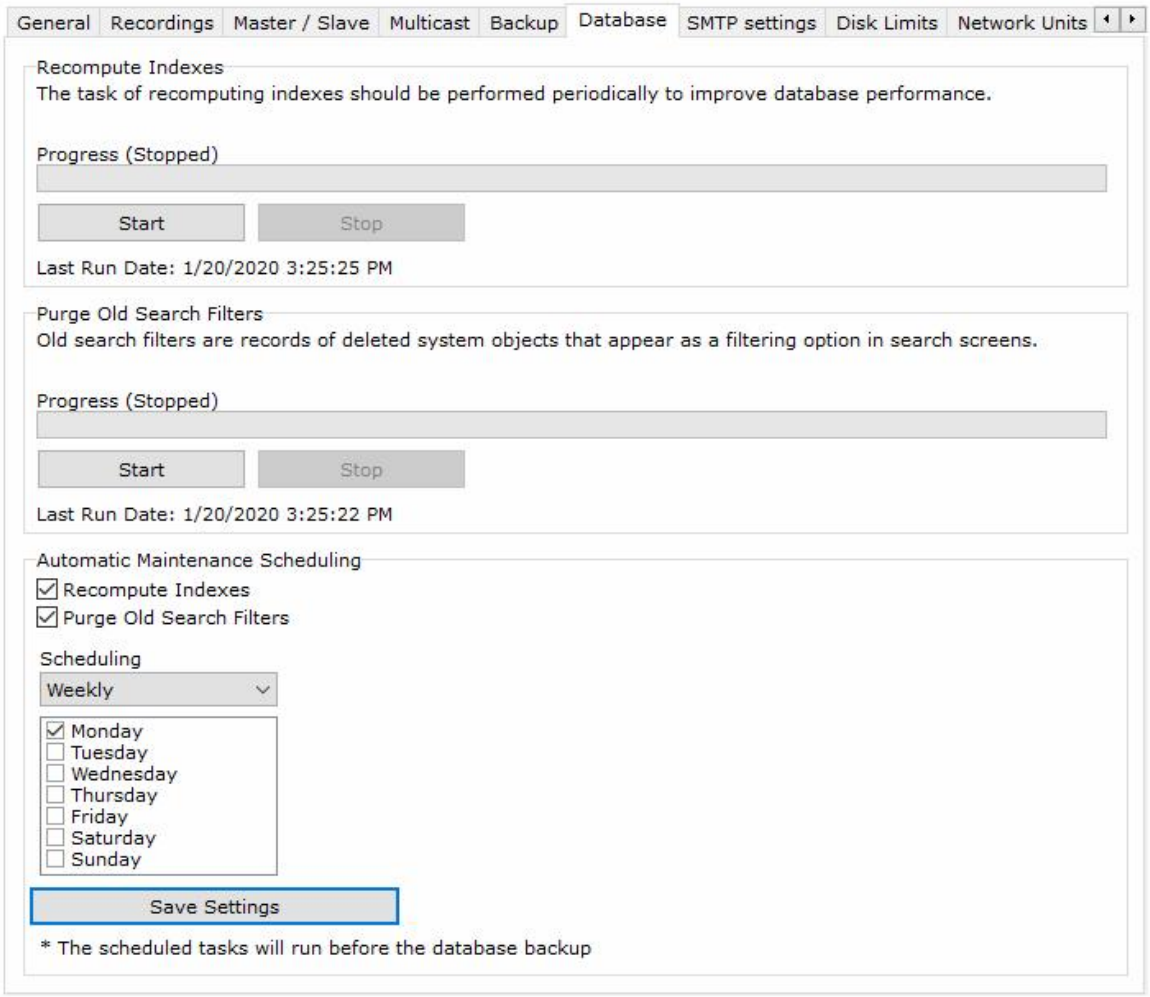
© 2002 - 2020 by Digifort, all rights reserved

17.1.6 Database

The Digifort has a database to store different types of records as: analytical event logs, event logs, system logs and LPR.

The configuration screen of the database allows the user to start a maintenance in order to enhance the performance of access to data by Digifort. Click **Start** to start the database maintenance process.

It is also possible to set up a database maintenance schedule, so that the task is automated.

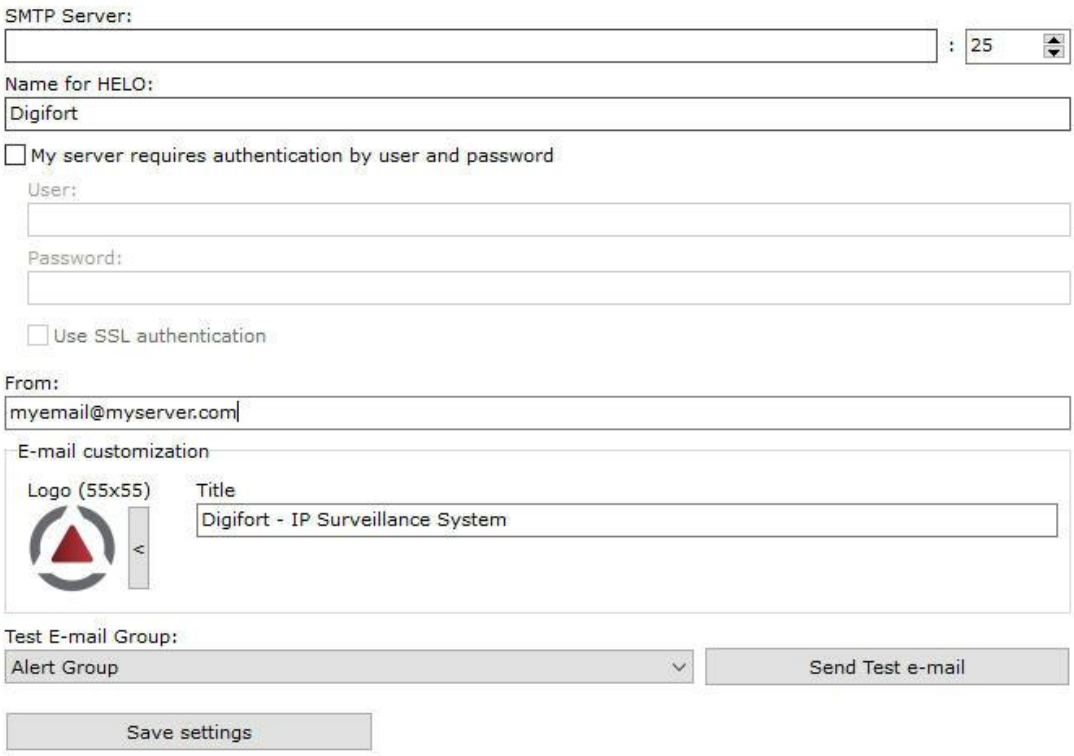


© 2002 - 2020 by Digifort, all rights reserved

17.1.7 STMP Configurations

The STMP configurations are used by Digifort t send notification e-mail to users. The actions for sending e-mail could be failures in communication with the cameras, for example, and must be previously configured by the administrator.

To access this feature, click on the **STMP Configurations** tab, as shown in the picture below:



- **STMP Server SMTP**: Address of the SMTP server to be used for the sending of e-mail. This parameter can be an IP, if there is an STMP server in your company, for example, or a DNS if third-party STMP servers are used.
- **My server needs authentication by user and password:** If your SMTP server needs a user and password for authentication for sending of e-mail, mark this option. When this option is marked, the User and Password fields will be activated and must be filled in.
  - **User:** User for authentication in the sending of e-mail messages.
  - **Password**: Password for authentication in the sending of e-mail messages.
  - **Use SSL authentication :** With SSL, authentication is performed by an exchange of certificates. These certificates are used to authenticate on some servers to increase the level of security.
- **From:** Sender's e-mail address. In this field, enter the e-mail address of the system administrator, for example.
- **E-mail customization:** Allows customization of the logo and name of the company when sending e-mails of events. Simply choose the desired logo image and change the title next to it.
- **Group for test e-mail**: Select an alert group for the sending of a test e-mail message for the

© 2002 - 2020 by Digifort, all rights reserved

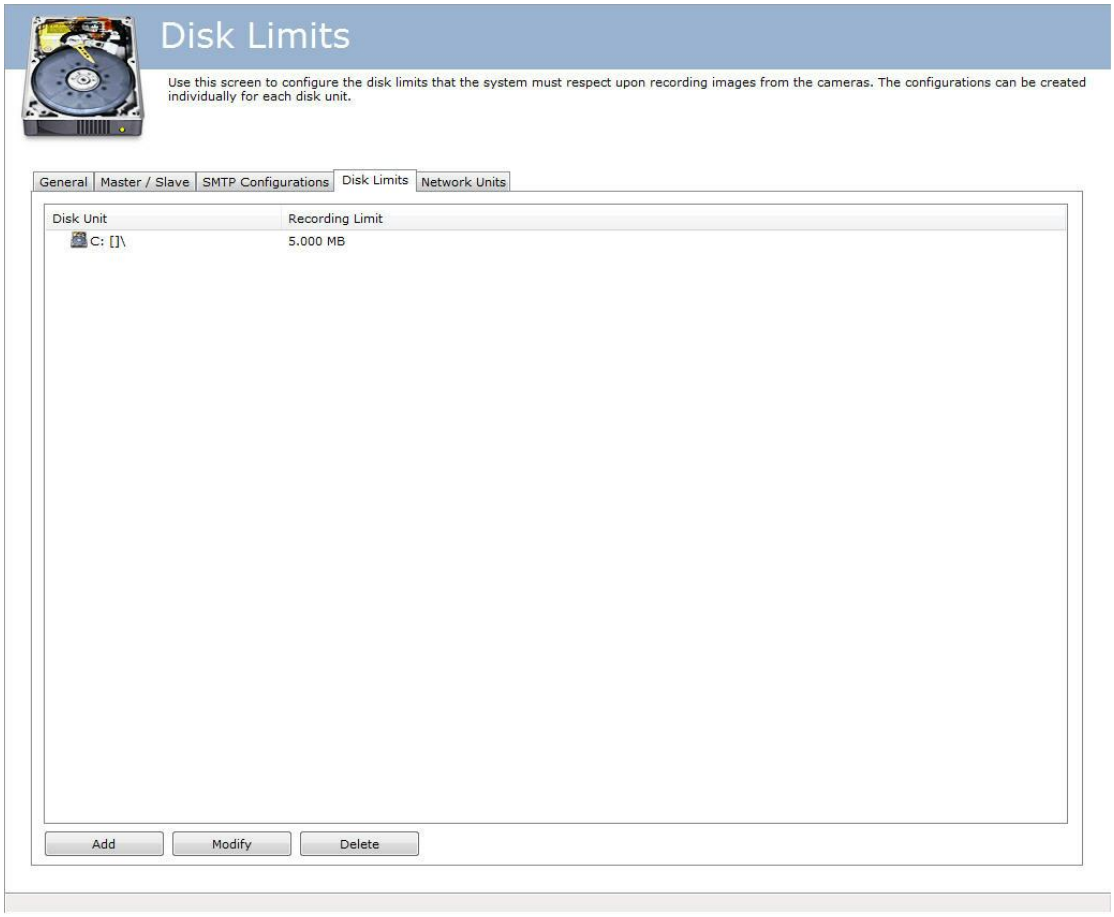
specified configurations. This alert group must have been previously configured. To learn how to do this configuration see How to configure the contact groups

- **Save Configurations button:** Saves the configurations. If not pressed, no configurations will be saved after leaving this screen.

17.1.8 Disk Limits

In this area of the system you can define disk limits in all of your units, if you wish to maintain a cushion of free disk space.

To access this feature, click on the Disk Limits tab in the Configurations item of the Configurations Menu, as shown in the picture below:



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

© 2002 - 2020 by Digifort, all rights reserved



Select the desired disk unit and enter the number of megabytes of limit that you wish to impose.
At the end of the configuration, click on the **OK** button.

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

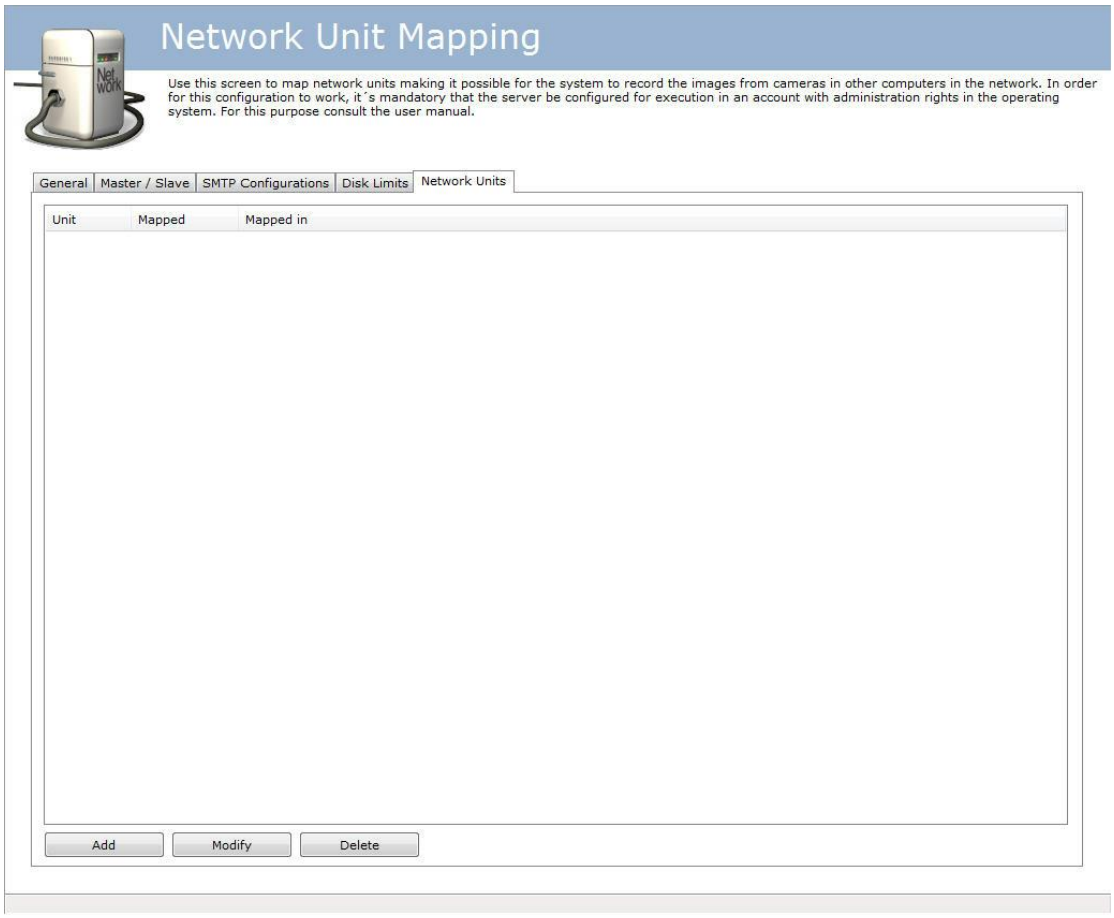
17.1.9 Network Units

Digifort Enterprise makes it possible to carry out recording of cameras not only in local disks. It's also possible to define network units in which Digifort can record the images from cameras.

Digifort's mapping of network units is different from that of Windows, and must, therefore, be defined by Digifort itself.

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

© 2002 - 2020 by Digifort, all rights reserved

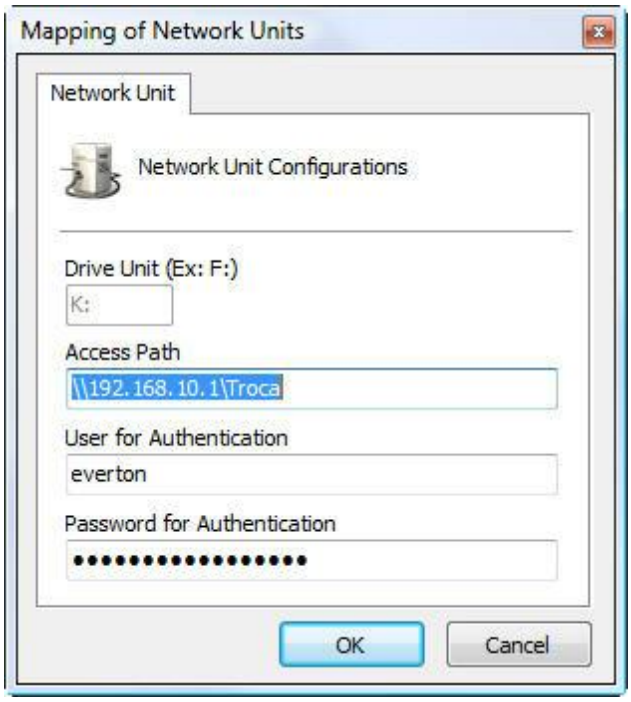


To add a new network unit, click on **Add**. To modify or exclude a network unit, select it and click on the corresponding button.

17.1.9.1 How to add a network unit

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

© 2002 - 2020 by Digifort, all rights reserved



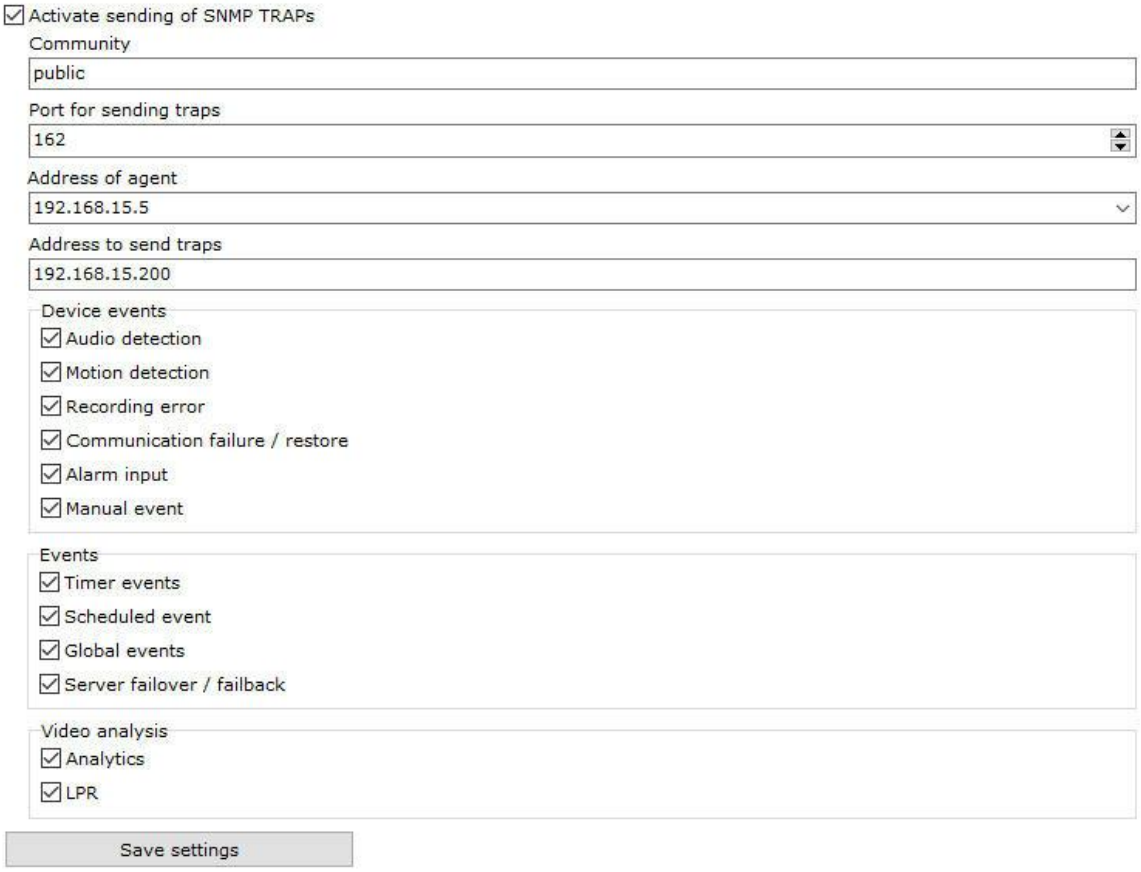
- **Unit letter**: Specify the identification letter of the unit to be mapped.
- **Access path**: Specify the complete folder path of the unit to be mapped.
- **User for authentication**: User of the Windows network who has access to the folder.
- **Password for authentication**: Password of the Windows network who has access to the folder.

© 2002 - 2020 by Digifort, all rights reserved

17.1.10 SNMP

Simple Network Management Protocol (SNMP) is an "Internet standard protocol for managing devices on IP networks".
Some equipment and software can use this protocol to send and receive alarms.

The system allows the sending of TRAPs to notify the occurrence of a system event through the SNMP protocol. The Digifort SNMP screen has the following options:



- **Community**: Public is the default setting for sending SNMP notifications in read-only mode.
- **Port for sending traps**: Selects the port for sending traps.
- **Agent Address**: Selects the network in which the trap will be sent.
- **Address for sending traps**: Selects the address for sending traps.
- **Device events:** Selects the events related to the devices you want to send traps. Available events are audio detection, motion detection, recording error, communication failure and restoration, alarm input, and manual events.
- **Events**: Selects the desired events for sending traps. Available events are Time events, Scheduled events, Global events, and Failover and Failback events.
- **Analytics/LPR**: Selects the desired analytics events for sending traps. Analytics and LPR events are available.
- **Save settings**: Saves screen settings.

NOTE: To import the Digifort SNMP information bases simply use the **Digifort-MIB.mib** file located

© 2002 - 2020 by Digifort, all rights reserved

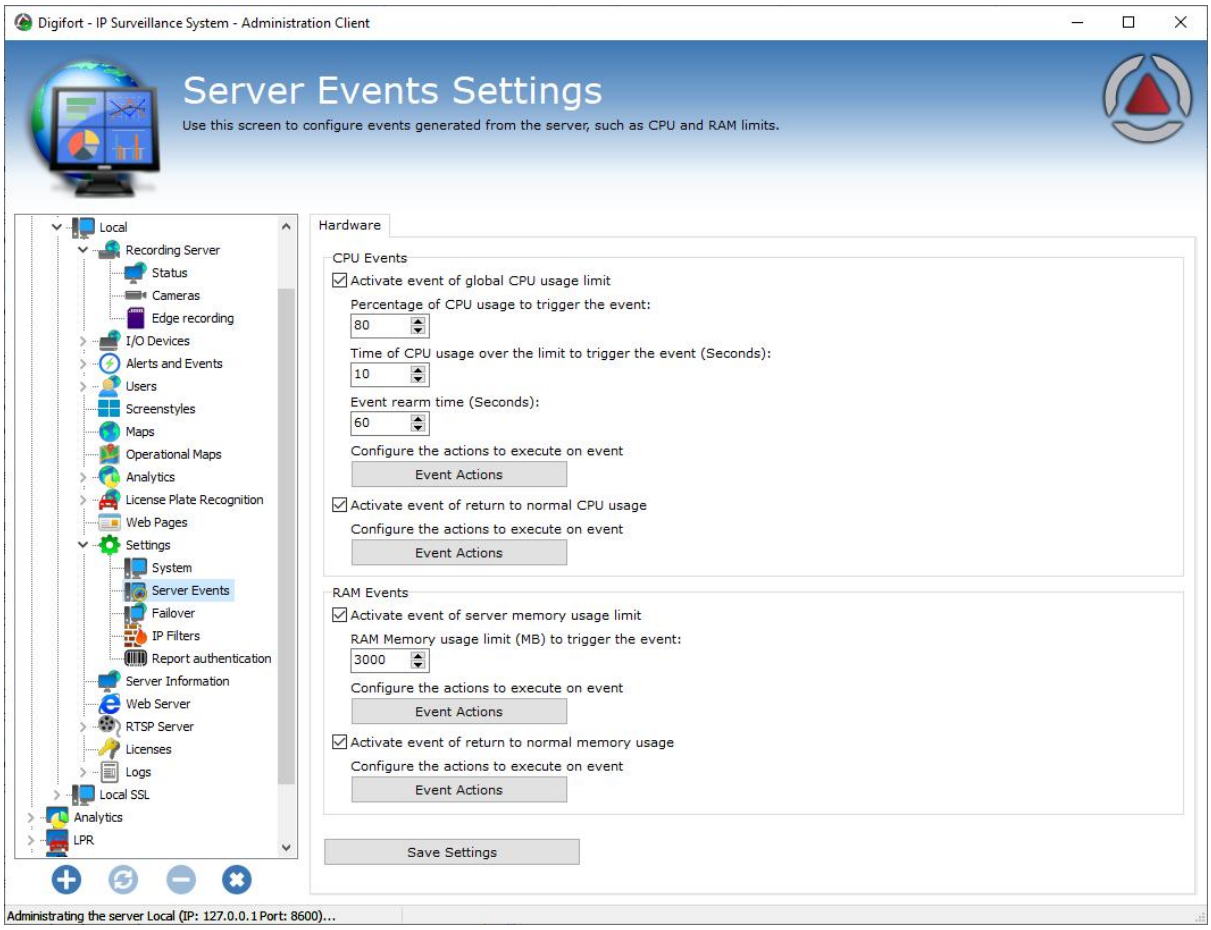
in the root of the software installation.

17.2 Server health monitoring event

The system allows the configuration of server health monitoring events. With these events, you can monitor the usage of CPU and System Memory, and trigger events in case of abnormality.

CPU monitoring will monitor the server's global CPU (and not only the system's server process). You can configure a usage limit and a time limit, whereby, if the global CPU usage remains above the set limit by the specified time, the event will then be generated. A condition restoration event (below the limit) can usually be triggered when CPU usage returns below the limit.

RAM monitoring will only monitor memory usage by the system's server process (server.exe). You can configure a memory usage limit by the server, whereby, if the usage remains above the configured limit, the event will then be generated. A normal condition restoration event (below the limit) can be triggered when CPU usage returns below the limit.



17.3 Failover

Digifort servers can be configured to function as Failover, that is, if a server stops working another

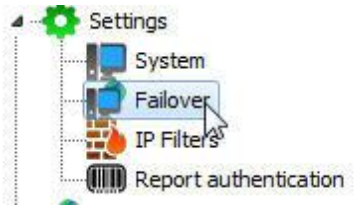
© 2002 - 2020 by Digifort, all rights reserved

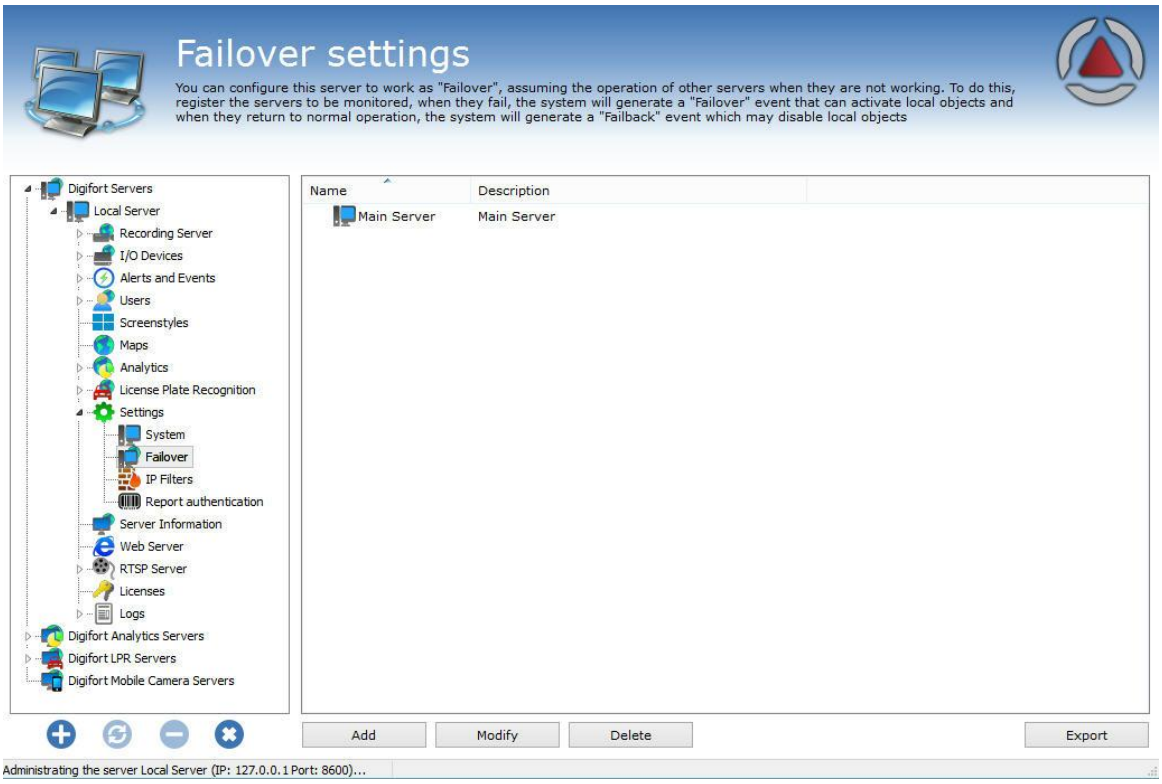
one will take over.

For explanatory purposes, let's assume a scenario of a company that has two Digifort servers, **Server A** with 4 cameras and **Server B** as FailOver. If **Server A** stops working, **Server B** will start recording with 1 out of the 4 cameras from **Server A.**

First you must register the camera that you wish to execute FailOver in **Server B** and leave it disabled. To learn how to register a camera check the How to add a camera chapter.
Note: Digifort allows you to import cameras from other servers. To learn how to do this, check the Import objects from other server's topic.

Now access the Failover option from **Server B** as shown in the image below:

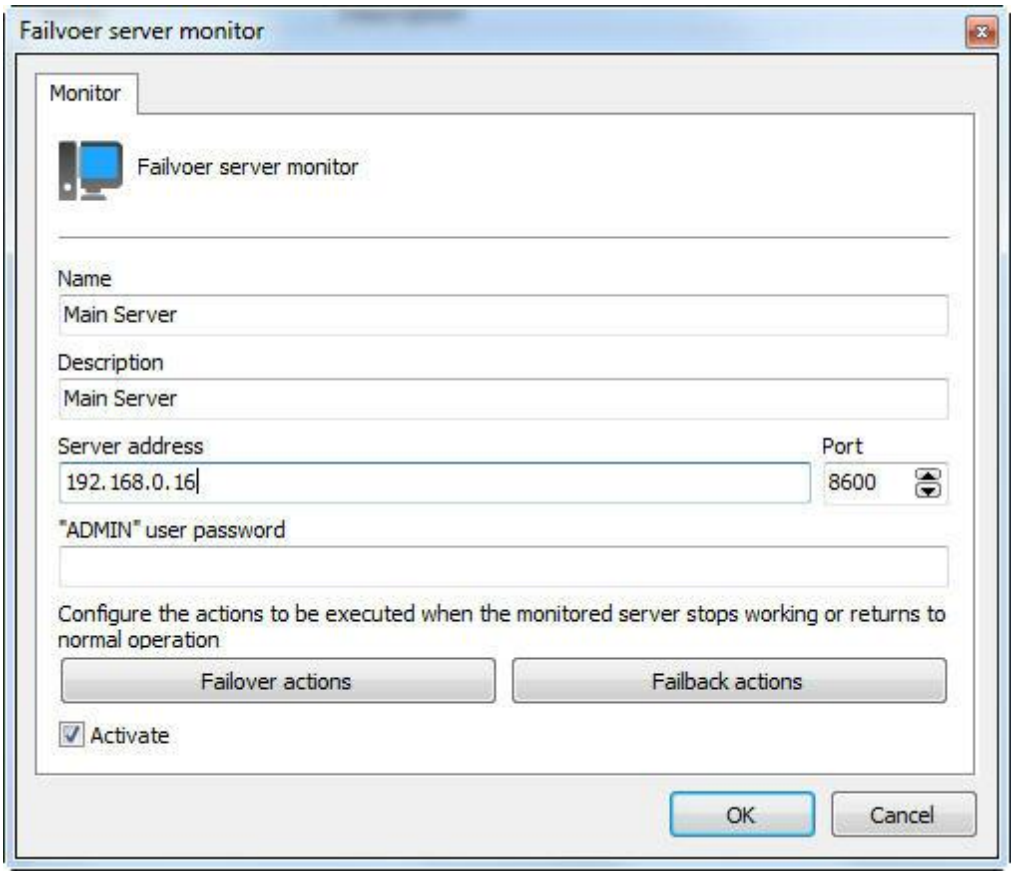




We will register **Server A** on **Server B**. This way, if Server A stops working, we can start recording from the camera on **Server B**.

To add the server click on **Add** and the following screen appears:

© 2002 - 2020 by Digifort, all rights reserved



On this screen we need to fill:

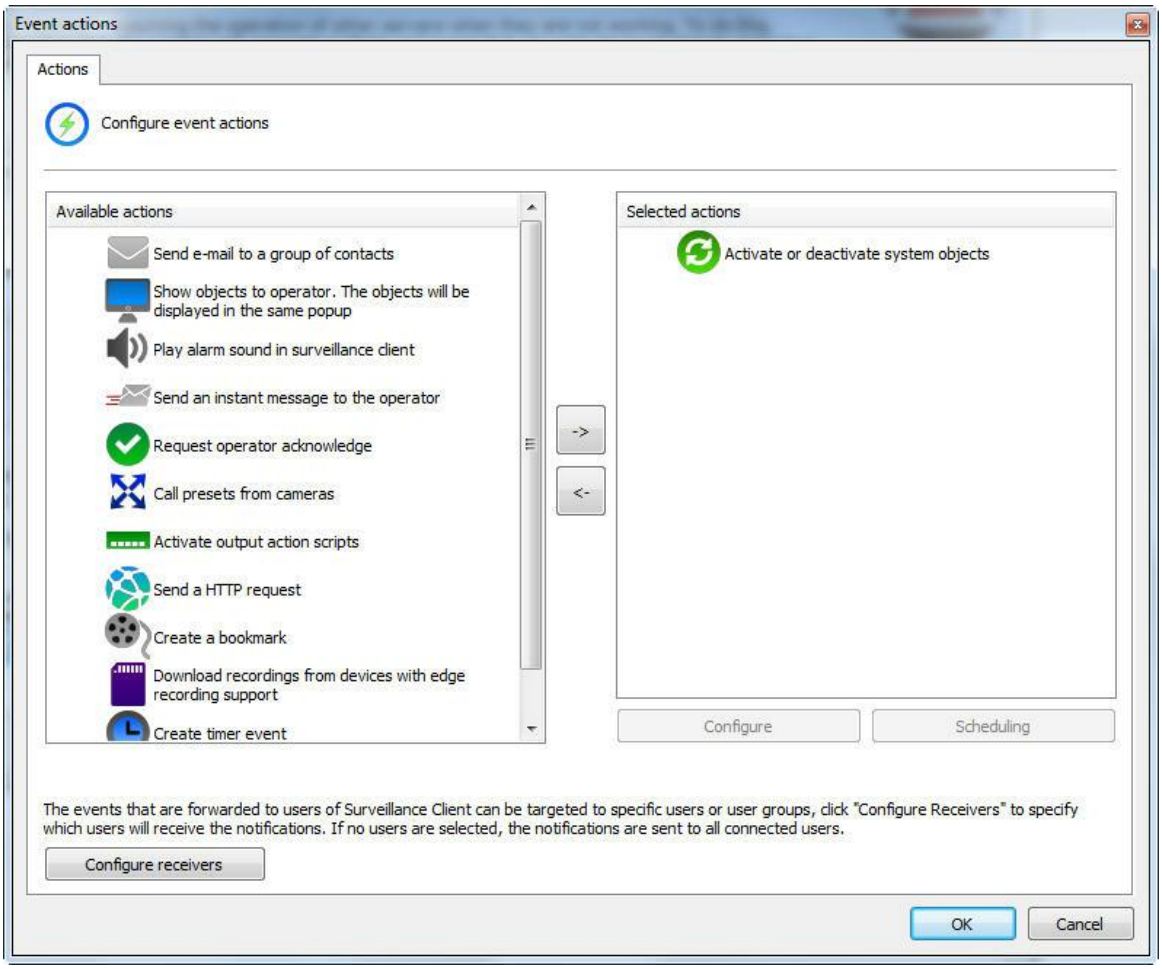
- **Name**: Name of the main server
- **Description**: Description of the main server
- **Server address**: Server IP to be monitored
- **Admin user password**: Admin user password from the server to be monitored.

Now we must create the actions we want to perform when the Failover situation is detected by Digifort.
To do this, click on Failover Actions:

The main action on Failover situation is to **Activate the objects** that will start working on **Server B**. Let's exemplify with a camera operation, but keep in mind that the same theory can be applied to objects as alarm devices, analytics and LPR.

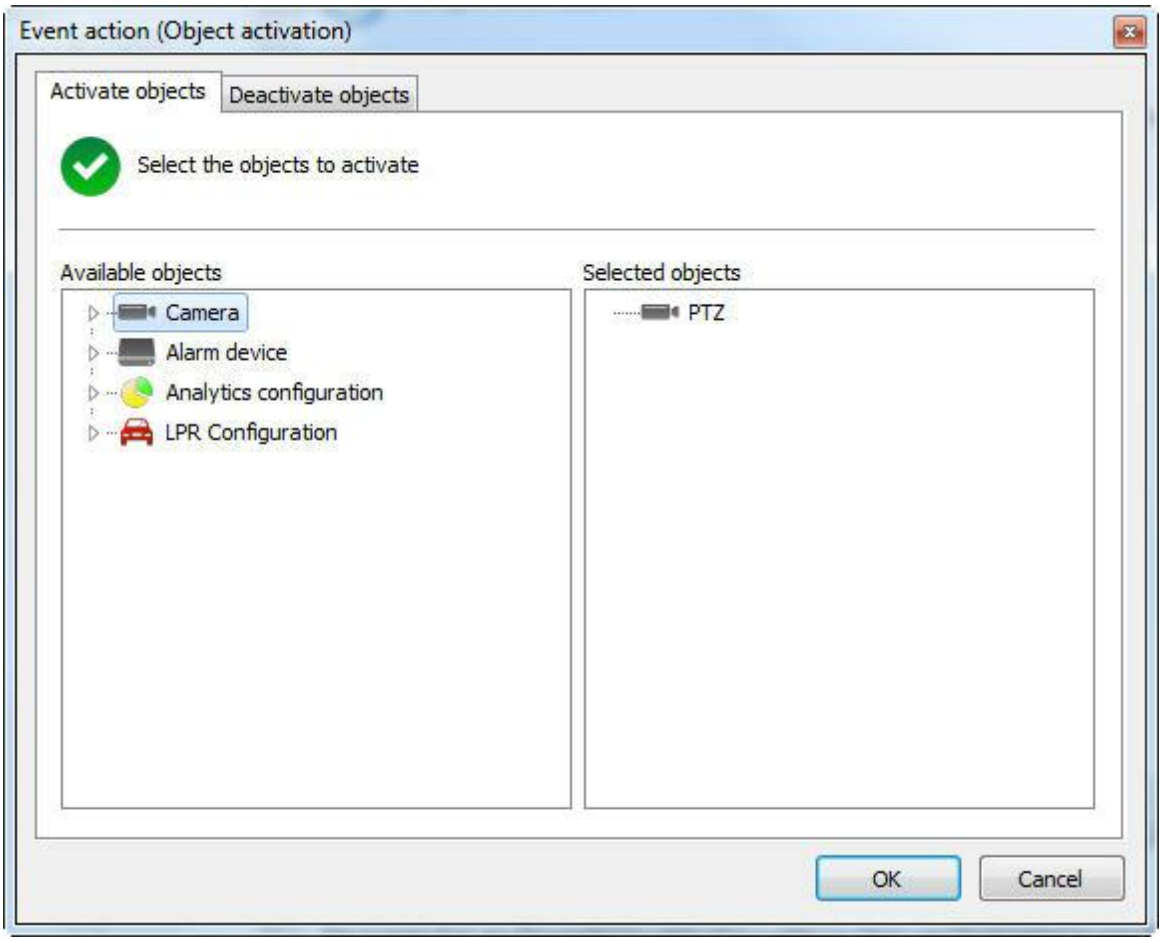
To learn about alarm actions, check the How to configure alarm actions

© 2002 - 2020 by Digifort, all rights reserved



Now drag the object to **enable or disable Objects** in the list on the right. Now you can configure the camera that you want to activate when **Server A** stops working. Simply drag it to the right:

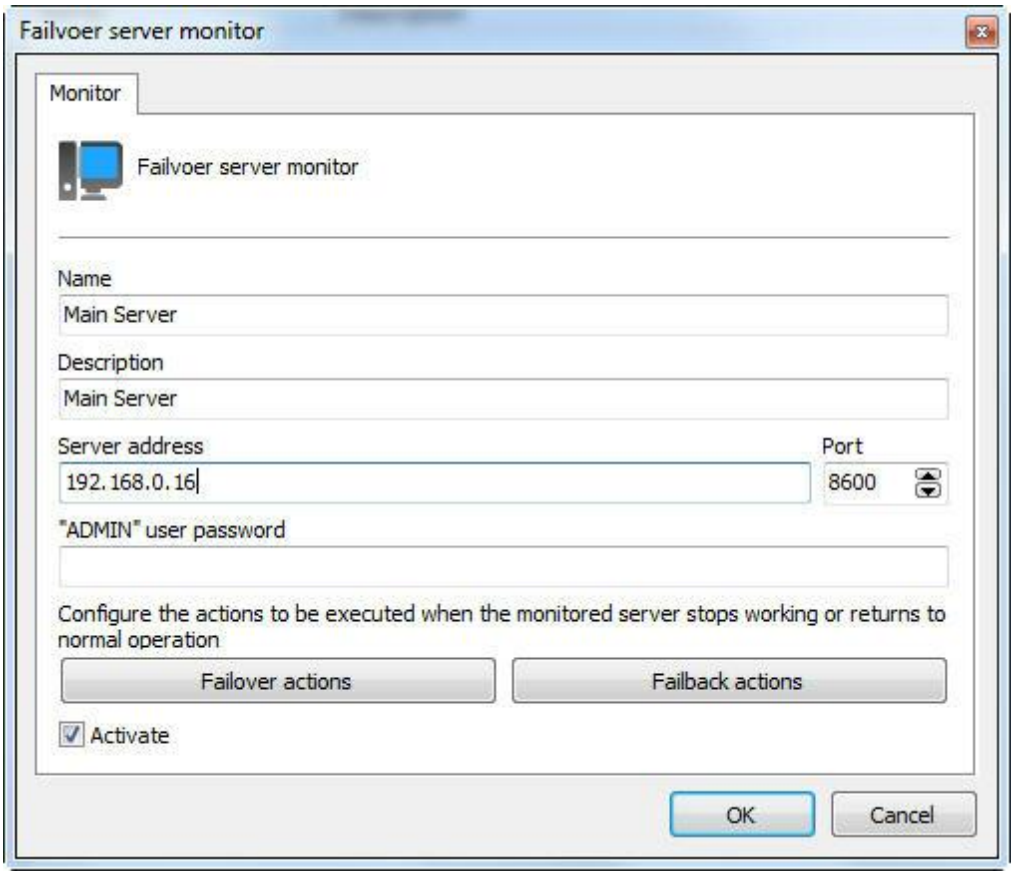
© 2002 - 2020 by Digifort, all rights reserved



Done! According to the scenario proposed here, when **Server A** shuts down, **Server B** will activate the "**PTZ**" camera and start recording.

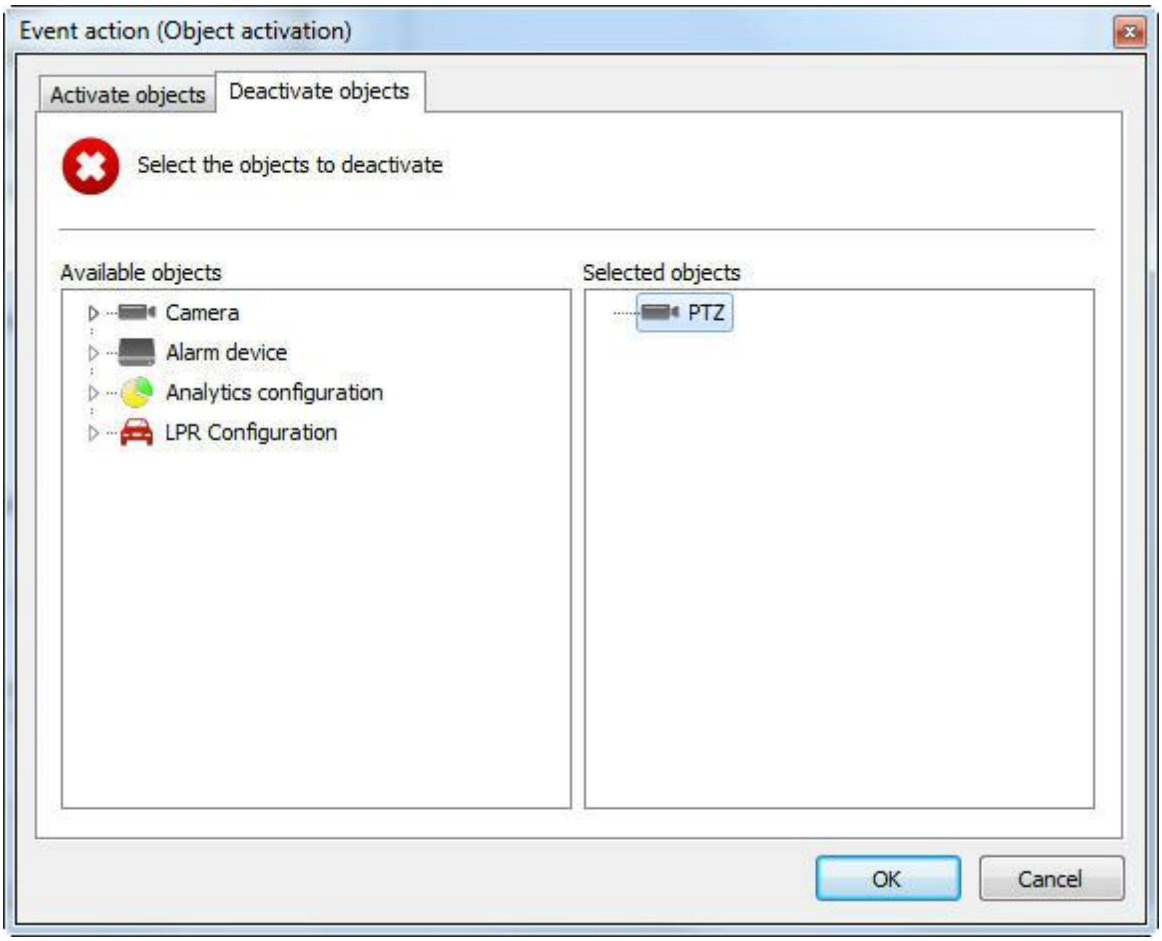
Now let's return to the Failover registration screen:

© 2002 - 2020 by Digifort, all rights reserved



To finish the process, you can configure an action to be applied when **Server A** is back into operation. Simply click on **Failback Actions**.
In our example, we will now disable the **Failover** server camera because **Server A** is running again. Once **Failback** is detected, the "PTZ" camera is disabled on **Server B** as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved



In this example, the software licensing is like this:

4 camera licenses on server A.
1 camera license to the Failover server.

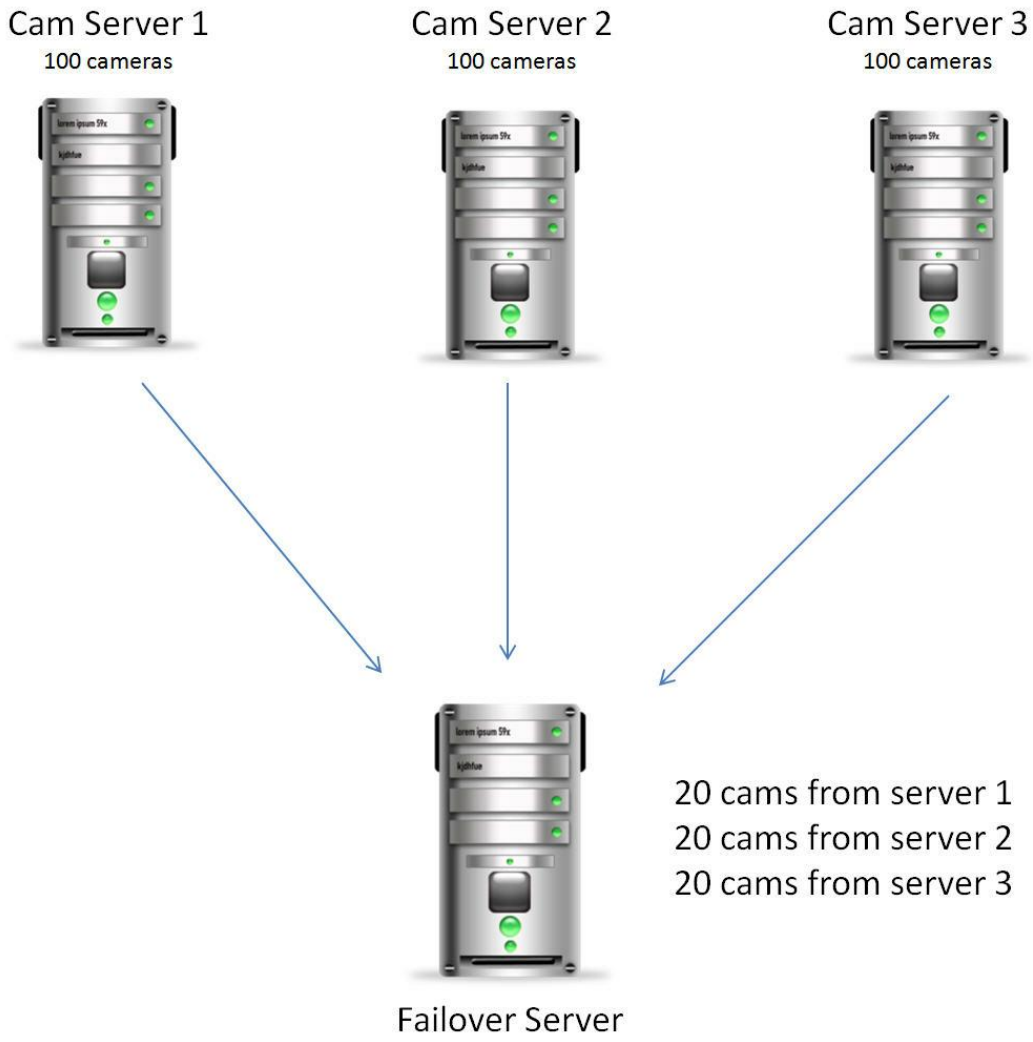
Check your reseller for license sale.

© 2002 - 2020 by Digifort, all rights reserved

17.3.1 Failover - Multiple servers

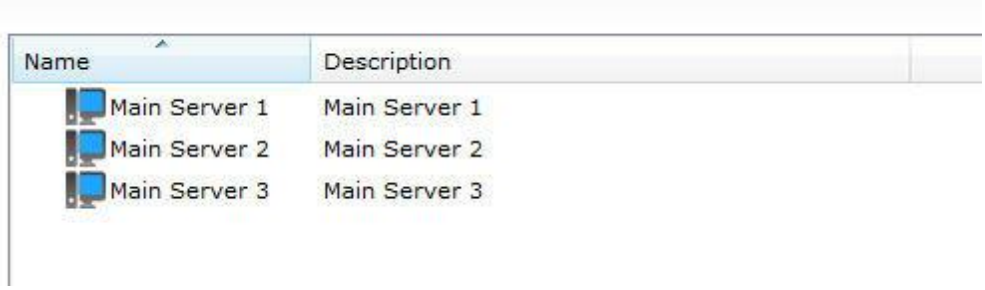
In the previous topic, we had an example of the Failover **resource** for 1 server.

Below, there is a second example, in which the Failover server is scheduled to begin recording 20 cameras from each main server.



In this case, 20 main cameras were registered for each server and then the 3 servers were configured for failover, as shown below:

© 2002 - 2020 by Digifort, all rights reserved



In this example, the software licensing is like this:

1st option:
300 camera licenses including all main servers.
60 camera licenses to the Failover server, whereas the 3 servers can stop working at the same time.

2nd option:
300 camera licenses including all main servers.
20 camera licenses to the Failover server, whereas only one server would be out of service at a given time.

Check your reseller for license sale.

17.4 IP Filters

As one more means of security, Digifort offers another tool which is extremely important for the security of the Digifort server – the IP filters.

These filters act like a firewall, blocking unwanted connections to the server.
IPs that will or will not have access to the systems can be added to the IP filters.

When a user tries to connect to the server by way of a blocked IP address, its connection will not be permitted, disconnecting it and registering the action in the log.

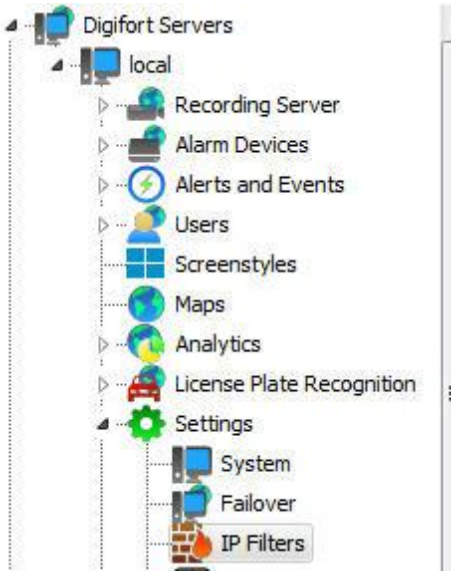
If this configuration is not done, all IPs are free to access the server.

17.4.1 How to access IP Filters

To access the IP filters, locate the item IP Filters in the Configurations Menu, as shown in the

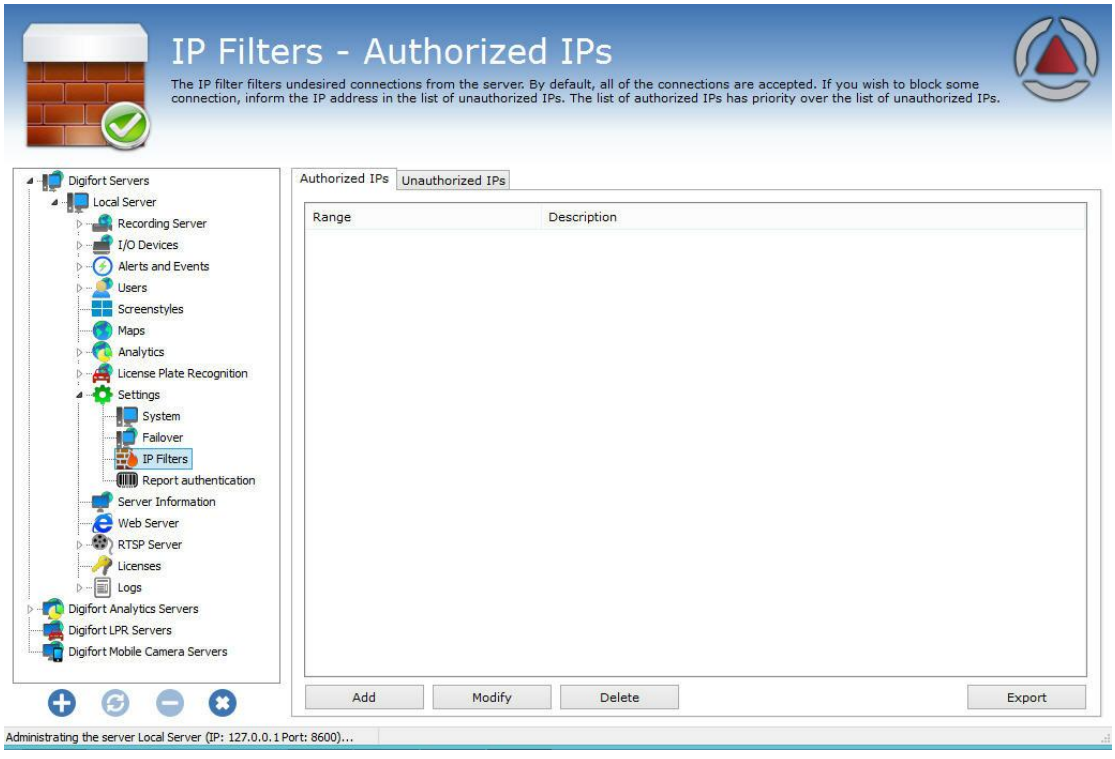
© 2002 - 2020 by Digifort, all rights reserved

picture below:



Once this is done, the IP filters register will be displayed at the right, as shown in the picture below:
This configuration is divided into two parts: authorized IPs and unauthorized IPs. The authorized IPs are more privileged than the unauthorized ones, that is, if a given authorized IP is in the range of unauthorized IPs, it will be permitted.

In the examples given below, we will block all IPs and free only the surveillance stations:



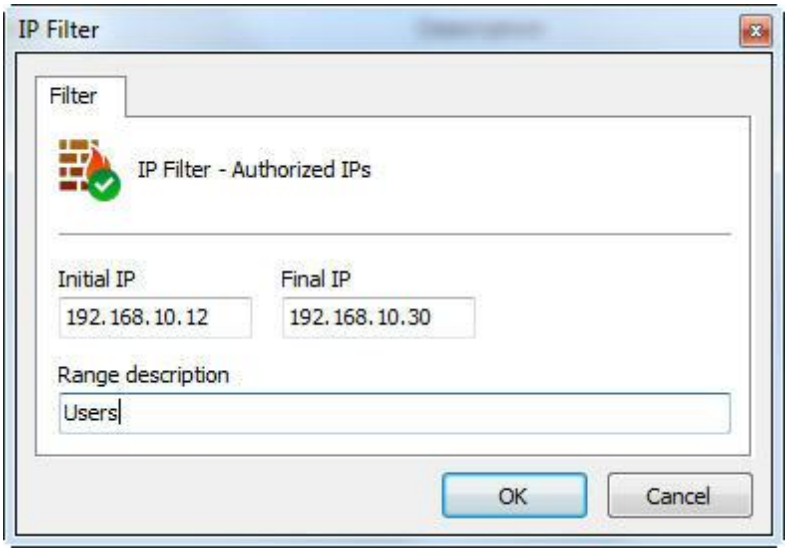
© 2002 - 2020 by Digifort, all rights reserved

In the example in the picture above the IPs in the range from 192.168.10.12 to 192.168.10.30 are free for access to the server.

To add authorized IPs, click on **Add**. To modify or exclude authorized IPs, select it and click on the corresponding button.

17.4.1.1 How to add authorized IPs

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

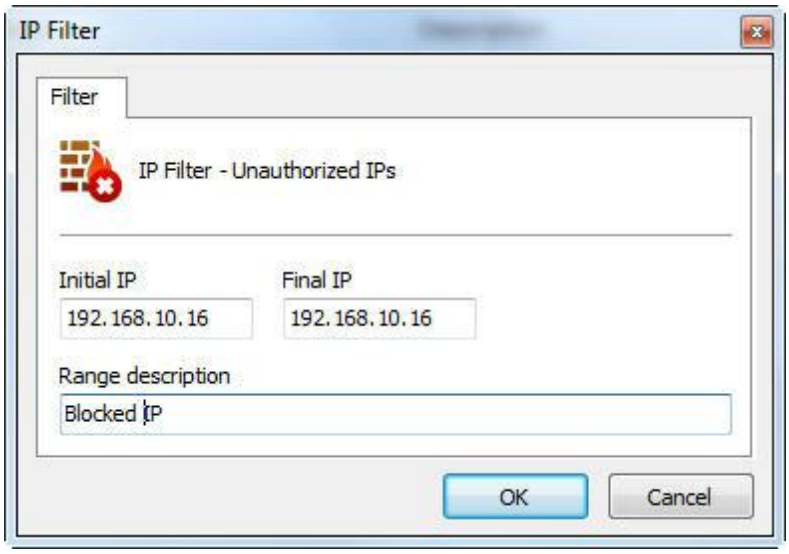


- **Initial IP**: initial IP of the range to be configured.
- **Final IP**: final IP of the range to be configured.
- **Description of the range**: Identification name of the range to be configured.

17.4.1.2 How to add unauthorized IPs

To add unauthorized IPs, click on the Unauthorized IPs tab and then click on Add, opening the screen below:

© 2002 - 2020 by Digifort, all rights reserved



- **Initial IP**: initial IP of the range to be configured.
- **Final IP**: final IP of the range to be configured.
- **Description of the range**: Identification name of the range to be configured.

17.5 Report authentication

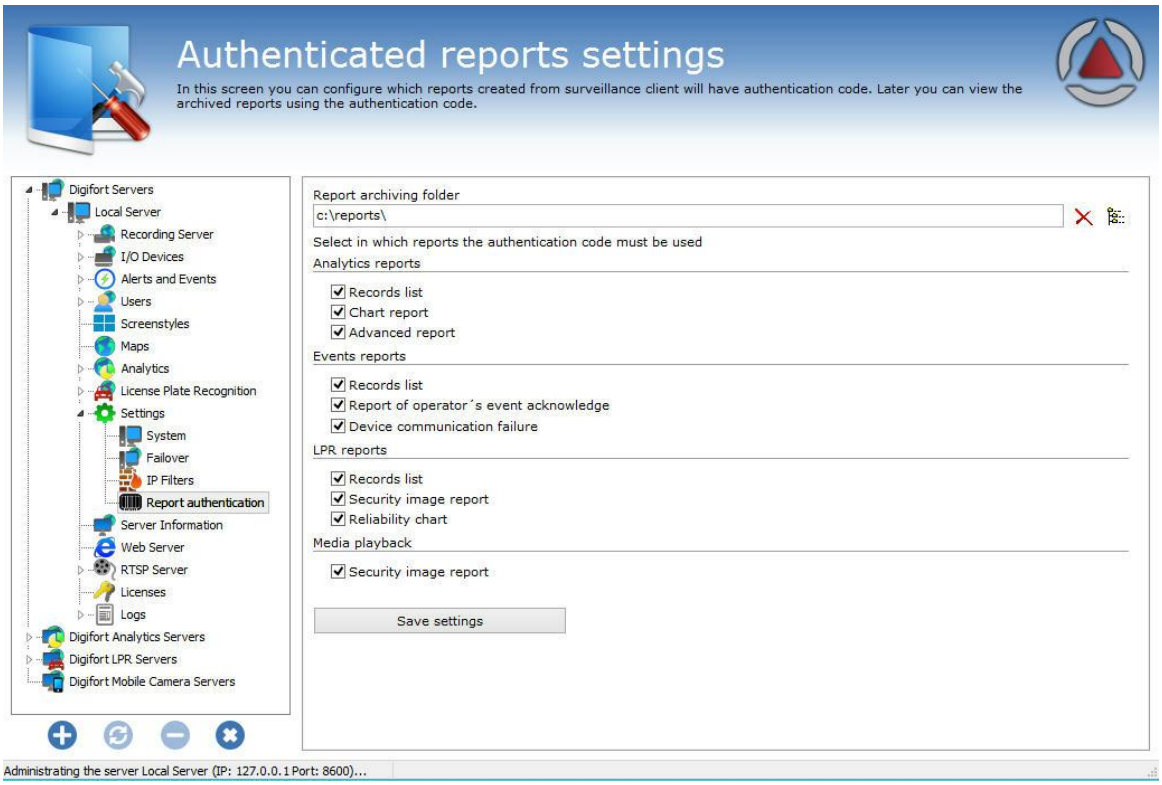
The **authenticated reports** option generates reports in the system with a unique authenticity identification. This way, the software generated reports contain a unique number along with bar codes, which allow the subsequent search and access to the original software-generated report.

Reports often need to be generated, from event, LPR or analytics records or even a video playback image print. If you want to subsequently check a system-generated report, simply request the report using its bar code and the system will generate it again with the originally saved data, making it possible to compare it to a printed report to confirm its authenticity.

To enable this feature, click on **Report Authentication** as in the image below:



© 2002 - 2020 by Digifort, all rights reserved



On this screen there are the following features:

Report archive directory: Choose a directory where Digifort will store the authenticated reports. If not filled, the reports will go to the "Report Authentication" folder in the Digifort installation folder.

Select the reports to receive the authenticity code: The reports that may have the authenticity code are:

- **Analytics**:
  - Records List
  - Graphic Report
  - Advanced Report

- **Event report**:
  - Records List
  - Operator Response Report

- **LPR Report**:
  - Records List
  - Security image print
  - Reliability chart
  -

- **Media Player**:
  - Security image print

After selecting the reports, click on **Save settings**

© 2002 - 2020 by Digifort, all rights reserved

To learn how to generate and search for the authenticated reports, check the Surveillance Client Manual

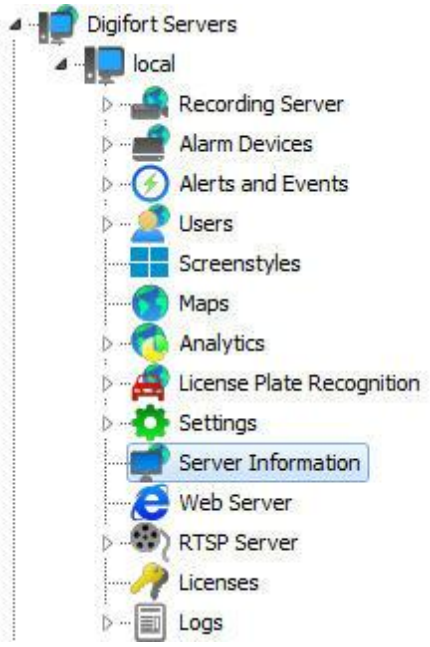
© 2002 - 2020 by Digifort, all rights reserved

Chapter XVII

18 Server Information

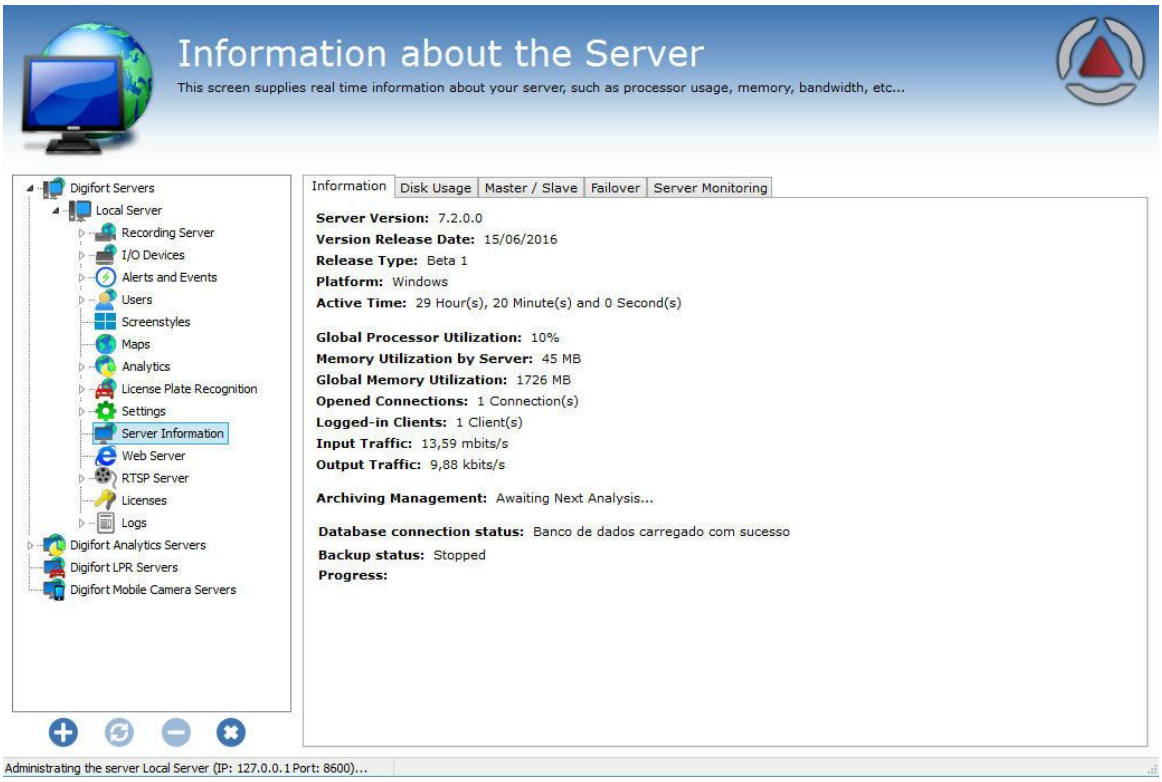
In this area of the system you will be able to accompany the performance of the server, receiving data such as processor and memory utilization, network traffic, etc.

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



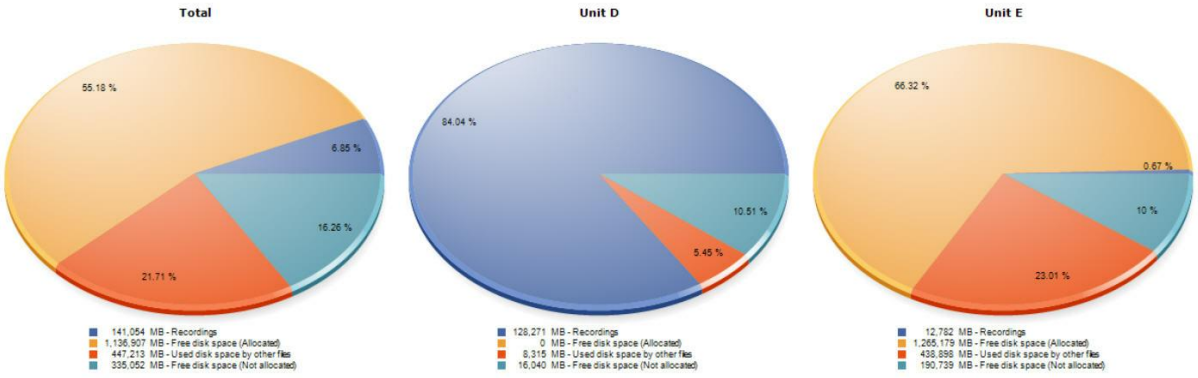
Once this is done, a window will be opened on the right side with server information, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



18.1 Disk Usage

The server disk usage tab generates a chart for each drive managed by the server and a general chart (Total):



The dark blue color on the chart represents the percentage of recordings occupied on a disk.
The yellow color represents the percentage of free disk space.
The orange color represents the percentage of space used by other files non-related to image recording.

© 2002 - 2020 by Digifort, all rights reserved

The light blue color represents the percentage of unallocated disk space for recordings by Digifort. This space can be changed; see chapter: General Settings.

In the example above, the first chart is the sum of the other two drives used by Digifort (drive D and drive E);

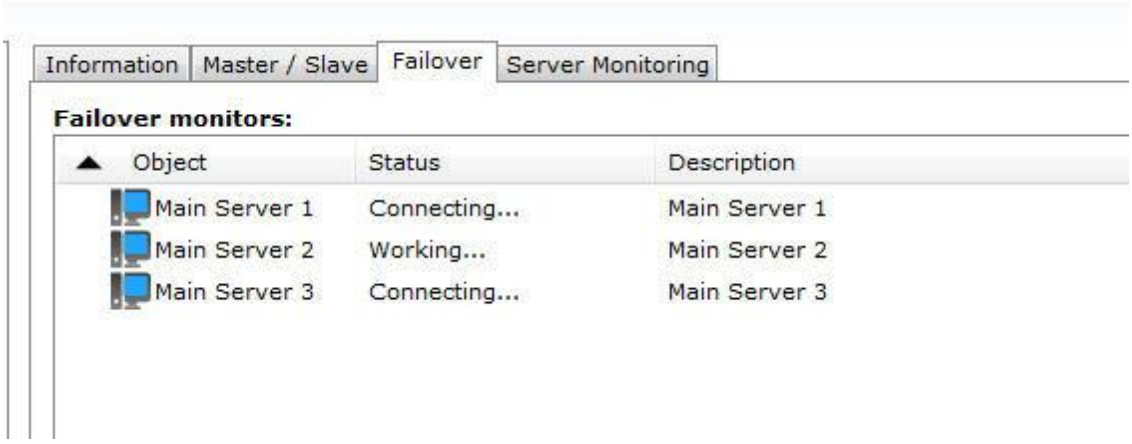
18.2 Master / Slave

Shows the Master / Slave Servers status and their connections. To learn more about master / slave servers, check the Master / Slave chapter,



18.3 Failover

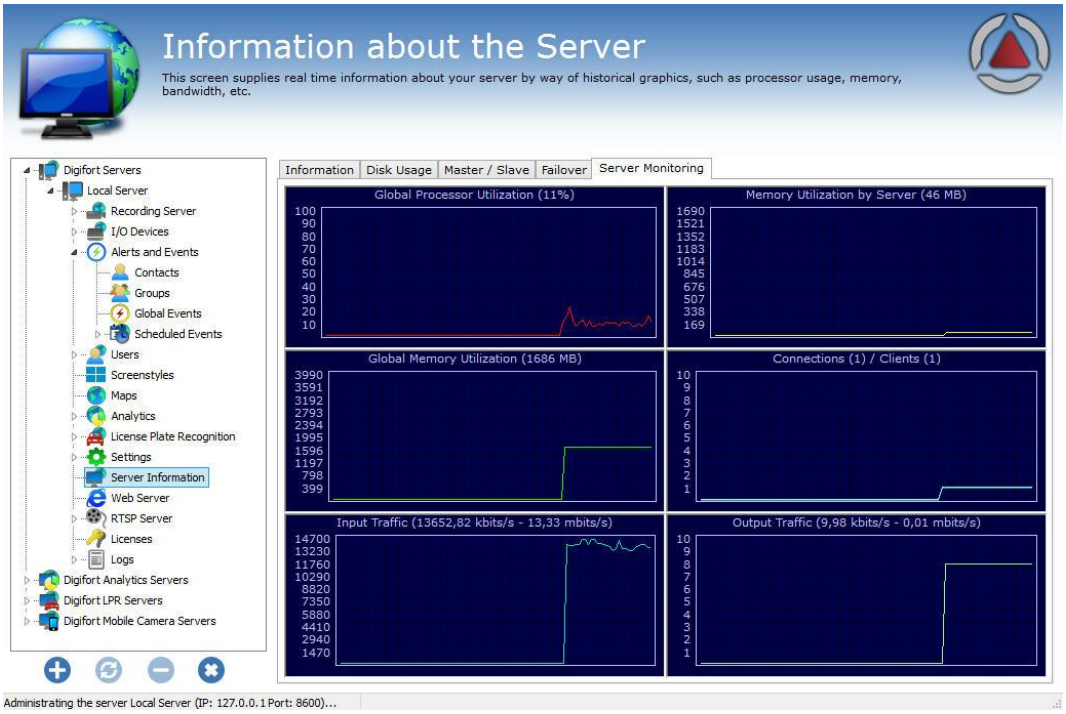
Shows the Status of the servers being monitored by the Failover feature. To learn more about Failover, check the Failover chapter.



© 2002 - 2020 by Digifort, all rights reserved

18.4 Monitoring by graphics

Digifort offers an interesting feature that makes it possible to monitor the resources used by the server in real time by way of graphics updated every second. To access this configuration, click on the **Monitoring** tab, as shown in the picture below:



© 2002 - 2020 by Digifort, all rights reserved

Chapter



19 Web Server

Digifort is equipped with a Web server, by means of which, users can visualize cameras and play videos back locally or via Internet with the use of an Internet navigator.

It's important to point out that, for access to the Digifort Server via Internet, it's necessary to configure your router with the purpose of redirecting the server connection by way of an Internet IP and a port.

To carry out the connection via Internet, Digifort requires two communication ports, the port 8600 and another configurable port.

19.1 How to access the configurations of the Web Server

To access the configurations of the Web Server, click on the item **Web Server**, and click on **Configurations**, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configurations of the Web Server will be displayed at right, as shown in the picture below:



- **Activate the Web server**: Activates the Web server Web allowing users to connect to the server by way on an Internet navigator.
- **Server port:** The port used for access to the server. This port can be modified and must be configured in your router for external access. Digifort uses a different one internally, because the port 8600
- **Enable HTTPS (SSL):** Enable HTTPS support on the web server.
- **Server Port**: Configure the access port via HTTPS.

© 2002 - 2020 by Digifort, all rights reserved

Chapter



20 Servidor RTSP

The RTSP server can be used to provide media to any player that supports RTSP, and can also be used to send media to broadcast servers like Wowza and make third party systems integrations with Digifort.

To illustrate, let's take the case of a client who wants to provide the image of a Digifort camera on his web site. In that case, he could use the API website and request a stream or a snapshot in MJPEG. However, if this site had a large volume of access, MJPEG could become unfeasible because of its size. The RTSP server generates flow of the following formats:

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

Then to add the image to a site just add a player that can receive a stream in RTSP with the following command line:

Syntax: rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<name of the camera registered on digifort>

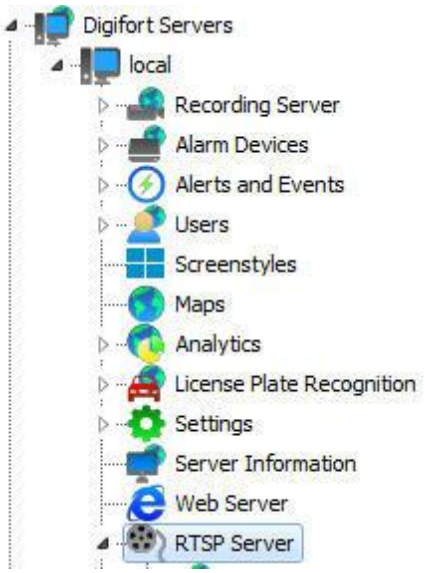
The command will bring up the recording profile image. You can choose the profile by adding the following command:

Syntax: rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<name of the camera registered on digifort>&Profile=<profile name>

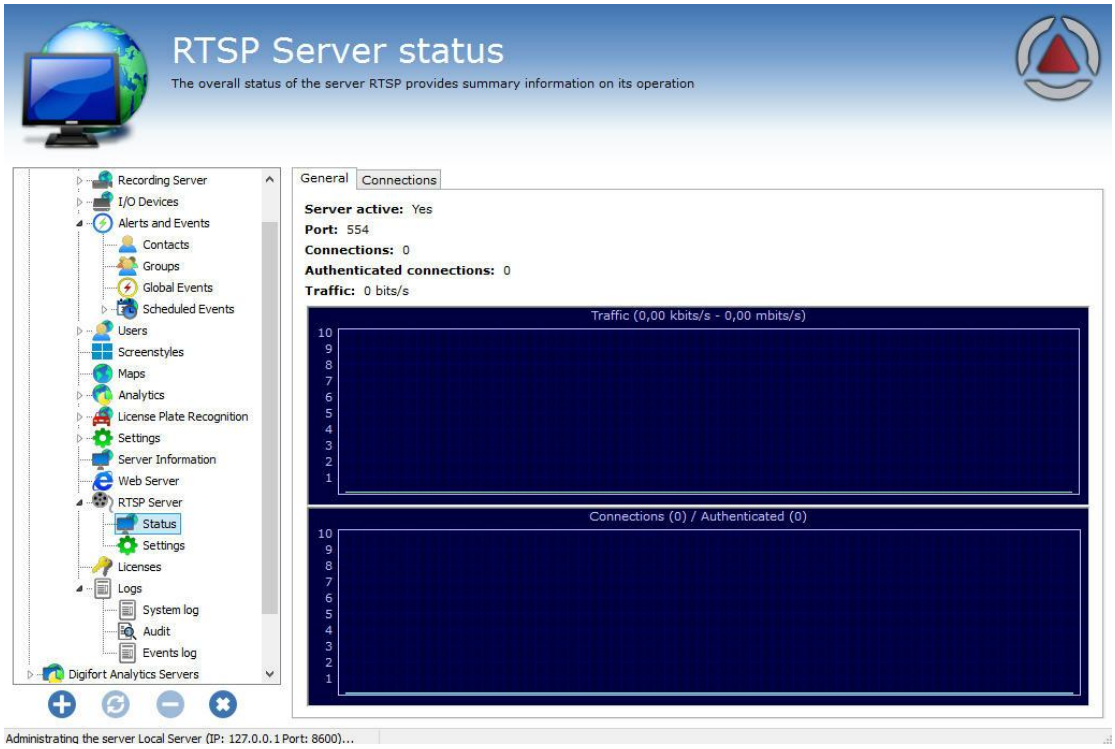
20.1 Status

To access the settings for the RTSP Server, expand the Web Server item, and click on Settings, located in the Settings Menu, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



That done, these Status settings will be displayed on the right, as illustrated in the figure below:

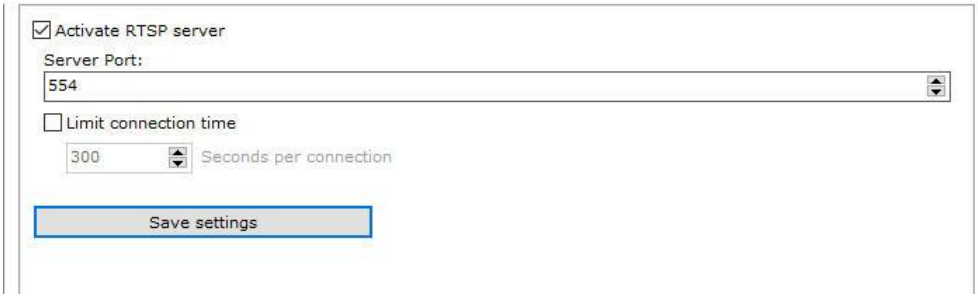


This screen provides the following information:

- **Active server:** Indicates if the RTSP server is active.
- **Port**: Indicates the port on which the server is running.
- **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 bandwidth used in real time.

© 2002 - 2020 by Digifort, all rights reserved

20.2 Configurations



The settings screen of the RTSP server allows the following settings:

- **Enable the Web server**: Enables Web server allowing users to connect to the server via 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. Digifort internally uses another because the 8600 serves the communication of the server with the clients.
- **RTSP port**: Port used to access the server via RTSPS, if activated.
- **Limit connection time**: Option to configure a time limit in which each connection can remain open.

© 2002 - 2020 by Digifort, all rights reserved

Chapter



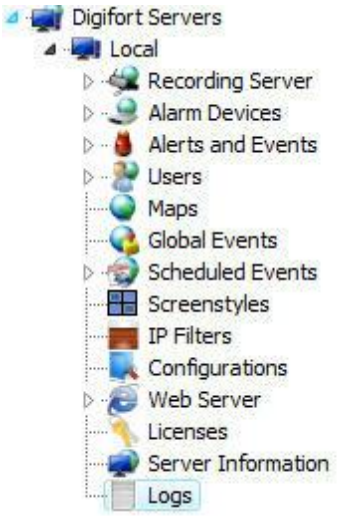
21 System Logs

The logs are very important tools for an environment that involves a security system such as Digifort, as it is in these logs that all events are registered, as well as user actions that occur in the system.

This chapter of the manual will cover the system logs, that is, those in which server events are registered, as opposed to the logs of alerts and events, where events related to external devices are registered. To better understand what alert and event logs are, see How to access the Alerts and Events

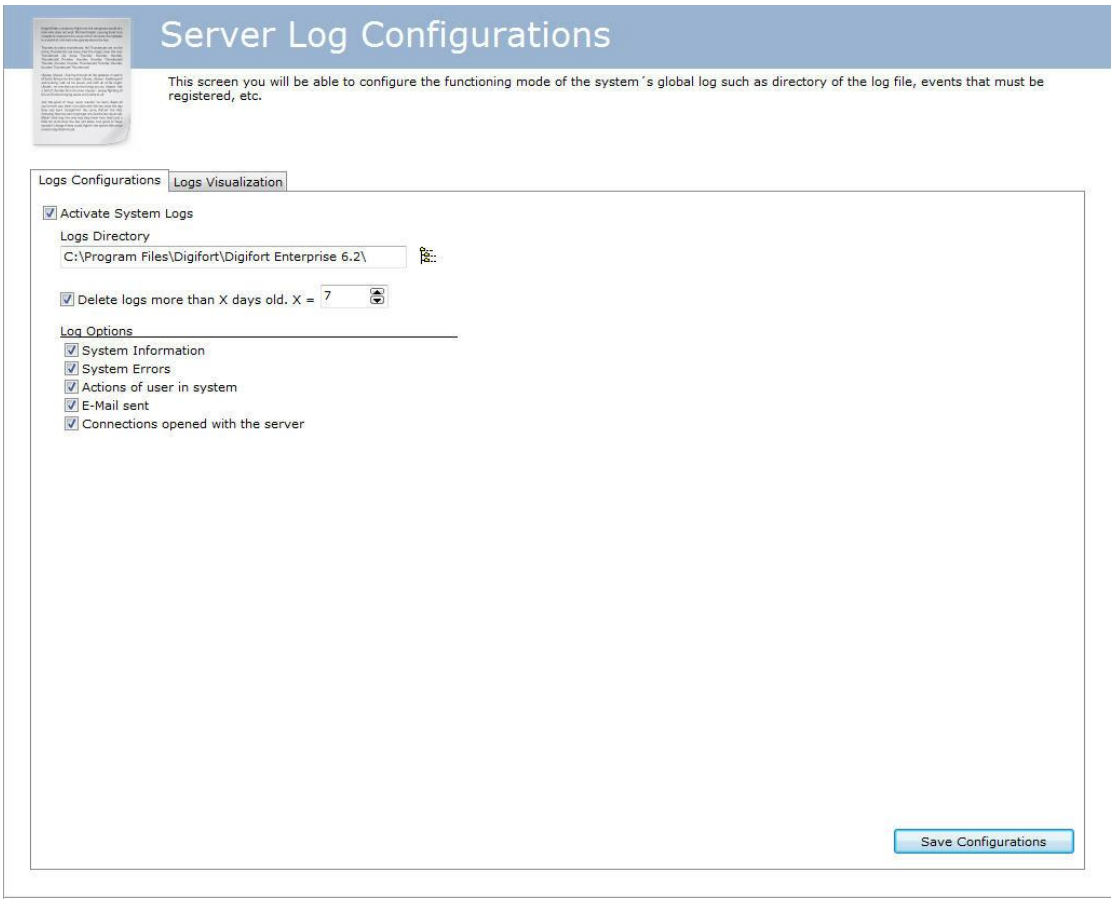
21.1 How to access the system logs

To access the system logs, click on the Logs item, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configuration of logs will be displayed on the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



- **Activate system logs**: Activates the alert and event logs of Digifort.
- · **Log directory**: Select the directory in which the alert and event logs will be saved.
- · **Eliminate logs more than X days old**: Eliminates the old logs, specified by the informed number of days.

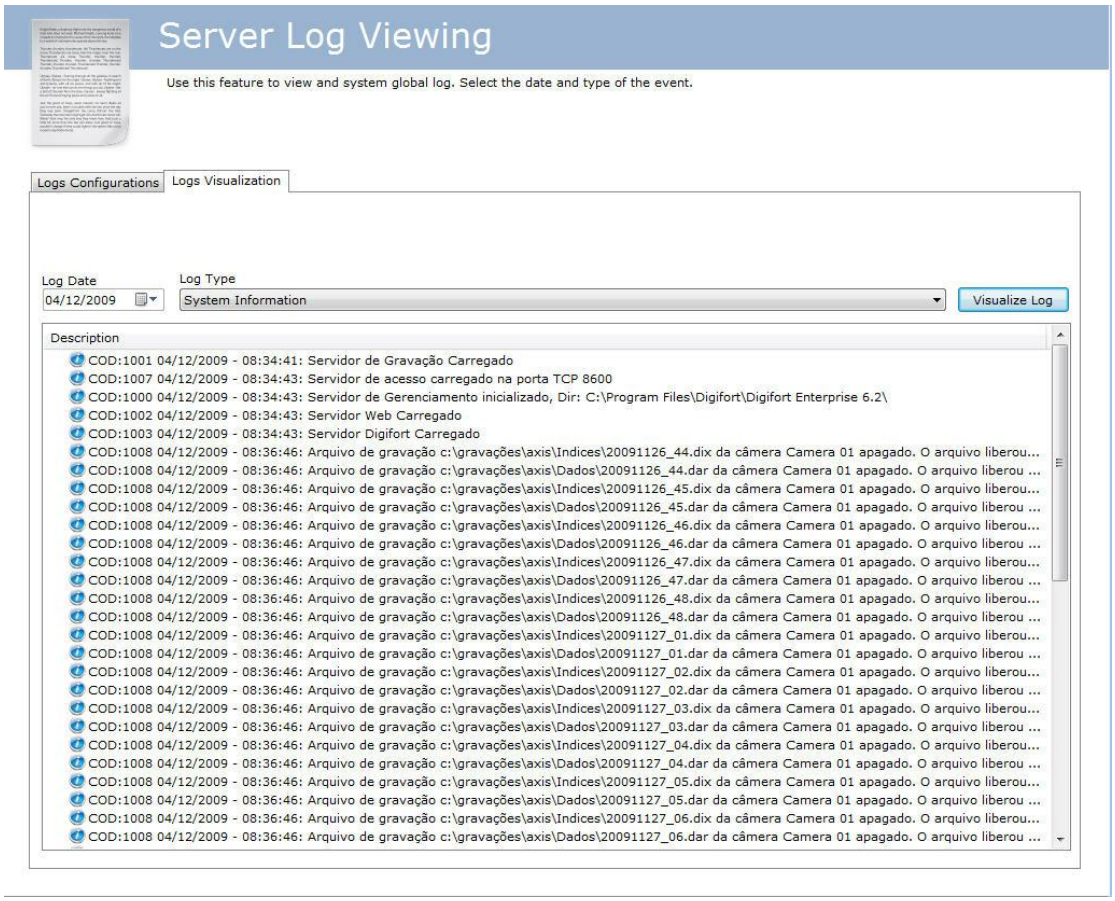
- **Options of the event log:**
  - **System informat**ion: This log contains information about system functioning like, for example, the time at which the server was loaded, terminated.
  - **System errors**: This log contains information about system errors such as the incorrect execution of some system function. This log rarely receives data.
  - **System user actions:** This log contains information about system user actions like, for example, the visualization of some camera and modification of configurations.
  - **E-mail sent:** This log contains information about the e-mail messages sent by Digifort like, for example, e-mail messages about failures in recording or communication of cameras.
  - **Open connections with the server:** This log contains information about the user connection with the server, showing information such as access time and IP.
- **Save Configurations button:** Saves the configurations of system logs.

© 2002 - 2020 by Digifort, all rights reserved

21.2 How to visualize the event logs

The visualization of logs is an auxiliary tool for the administrator when analyzing a log, presenting a friendlier and more productive interface compared to a simple text file.

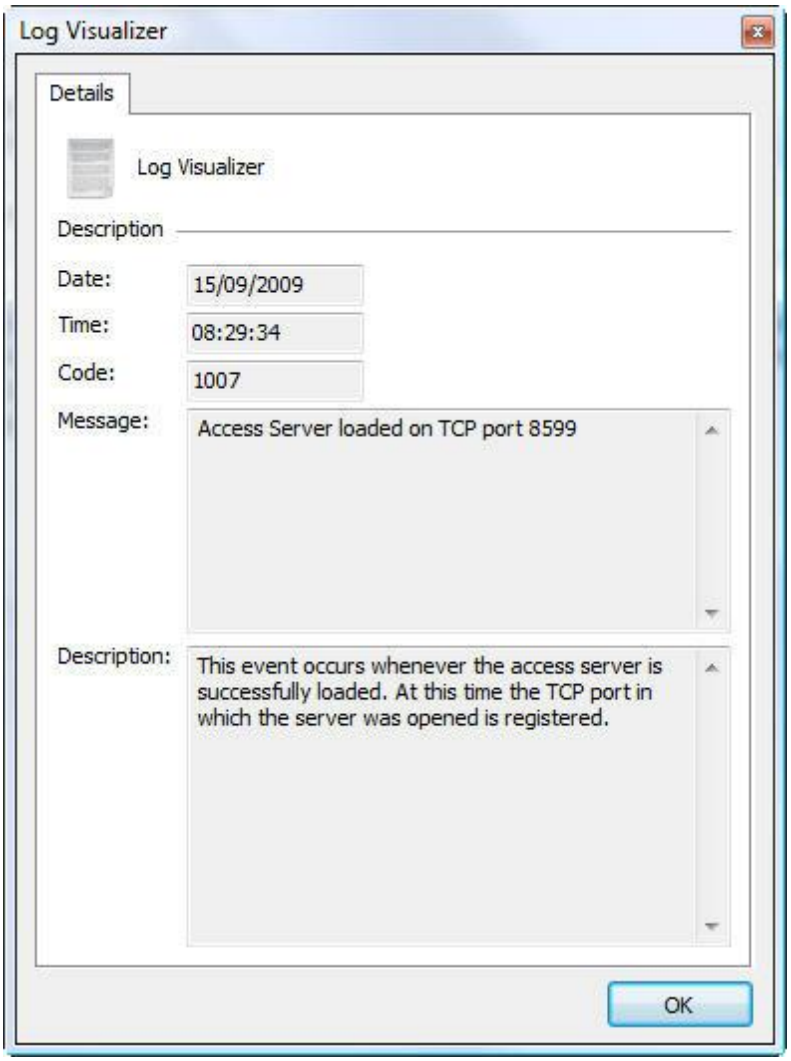
To visualize the event logs, click on the **Log visualization** tab, as shown in the picture below:



To visualize a log, select the date and type, then click on the Visualize Log button. This way the list of log registers will be filled.

Upon double-clicking on some log item, a screen will be displayed with details about the occurrence, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved

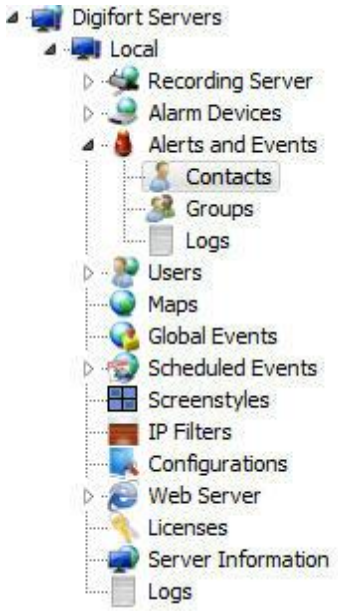


21.3 How to configure the event logs

The Digifort's log configuration allows to register several event categories in its database. Those events can be listed and used to look for a pertinent recording in the monitoring client.

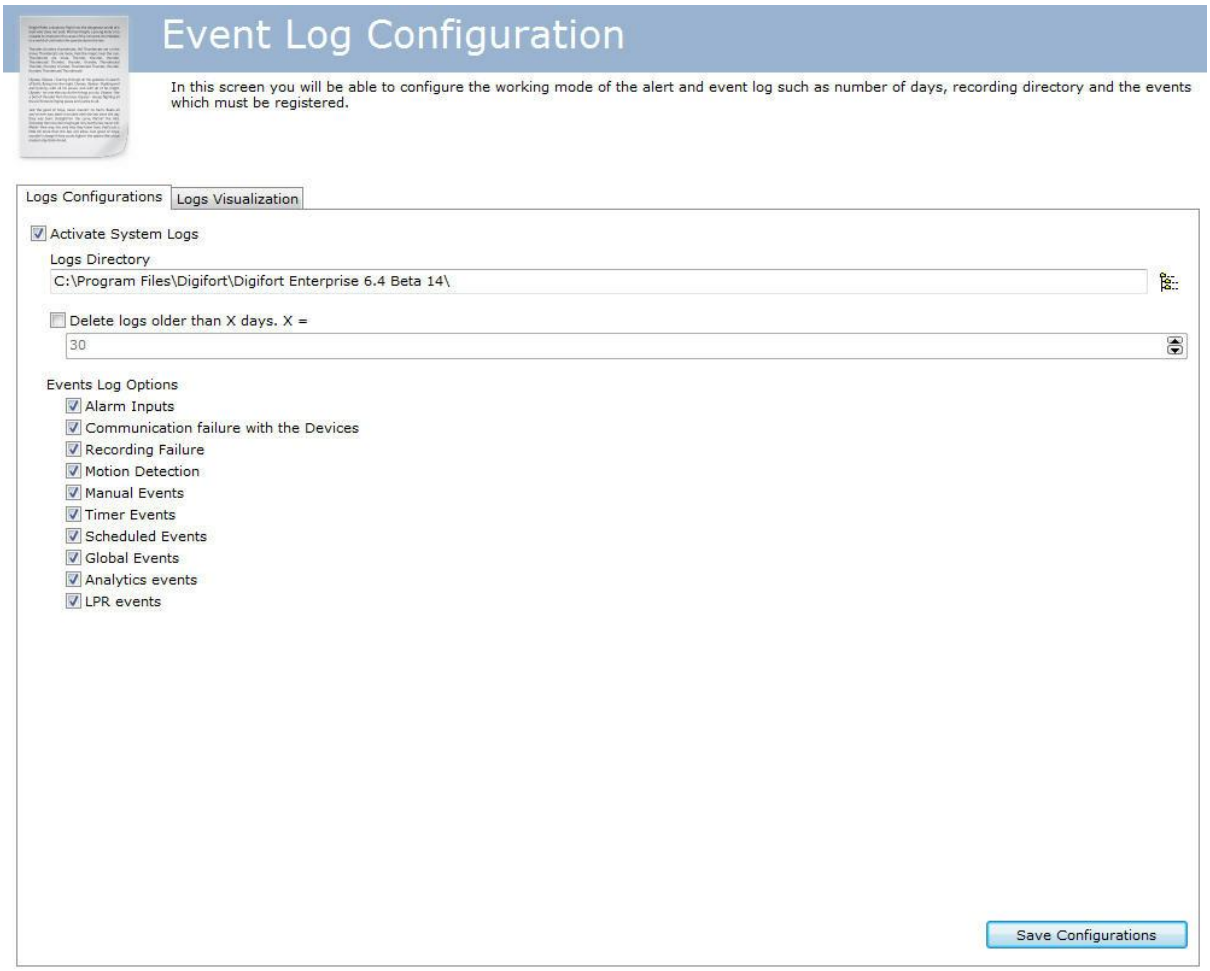
To access this feature, click on the item Logs, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



Once this is done, the screen for configuration of alert and event logs will be displayed at the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



21.3.1 Activate system logs

Activates Digifort's alert and event logs.

21.3.2 Delete logs older than X days

Delete the logs in the database that have been in the server for more than X days.

21.3.3 Event log options

21.3.3.1 Failure in communication with the devices

Logs the failures of communication with the cameras

© 2002 - 2020 by Digifort, all rights reserved

21.3.3.2 Alarm inputs

Logs the occurrences of alarm inputs of some device such as the detection of motion in the presence sensor.

21.3.3.3 Failure in recording

Logs the failures in recording in disk of images coming from the cameras.

21.3.3.4 Motion detection

Logs the occurrences of motion detection in some camera.

21.3.3.5 Manual events

Logs the occurrences of manual events set off by the operator such as, for example, the opening of an electrical lock

21.3.3.6 Timer events

Logs the occurrences of timer events.

21.3.3.7 Programmed events

Registers the occurrence of programmed events in the log.

21.3.3.8 Global events

Registers the occurrence of global events in the log.

21.3.3.9 Eventos de analítico

Registers the occurrence of analytics events in the log.

21.3.3.10 LPR events

Registra no log as ocorrências os eventos de LPR

21.3.4 Save Configurations button

Saves the configurations specified here.

21.3.5 How to visualize the event logs

To learn how to view the event logs refer to the Surveillance client manual

© 2002 - 2020 by Digifort, all rights reserved

21.4 Audit

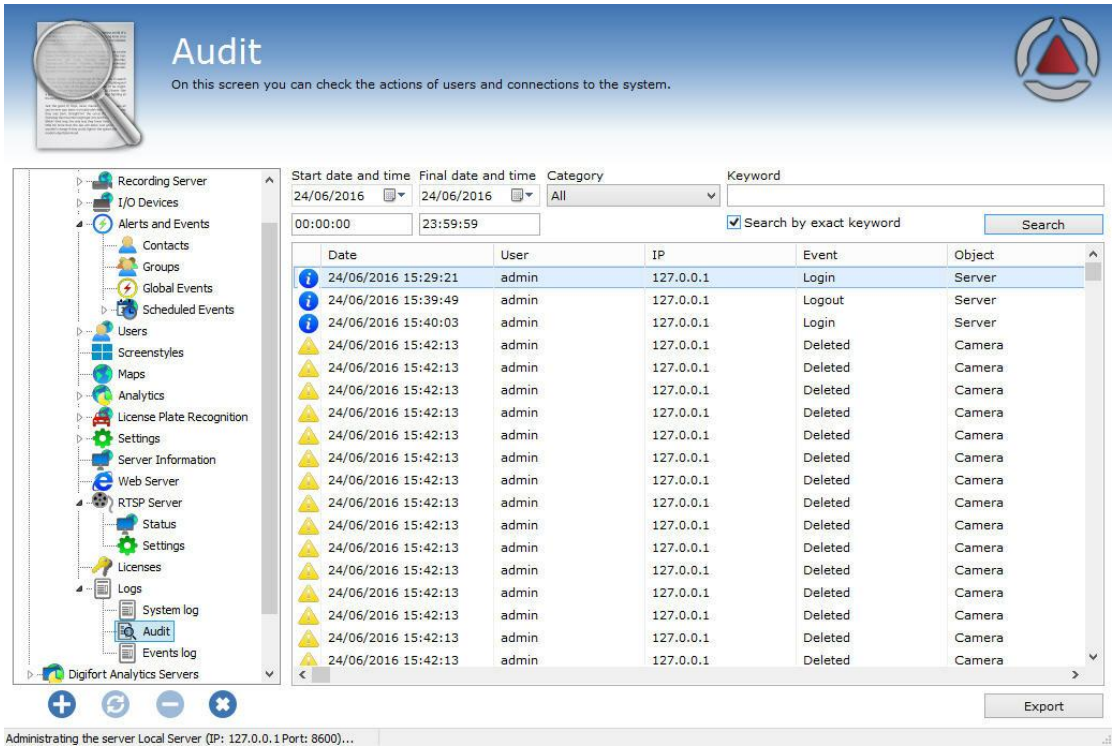
The aim of the Digifort Audit is to record all the occurrences related to the users in the system and connections to the server.

21.4.1 How to access Audit

To access the Audit screen, click on the item **Audit**, located in the Configurations menu as shown in the picture below:



Once this has been done, the **Audit** configurations will show up on the right as shown below:



When open, the screen will show all the records on the current date.

© 2002 - 2020 by Digifort, all rights reserved

21.4.2 Viewing the Logs

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

The following **user actions** are recorded by Digifort audit:

- **Locked and Unlocked**: Users or groups.
- **Reset**: User or group passwords.
- **Added**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Changed**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Deleted**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Created**: A recording directory.
- **Enabled and Disabled**: System settings (cameras, analytics, LPR, alarm boards, etc.)
- **Started**: Search by motion and video playback
- **Granted rights and Denied rights**: User viewing or recording
- **Viewed**: Cameras on the system.
- **Logged**: On the administration, surveillance or web client
- **Media Playback**: The start and the end date of user's media playback.

The following **Server Connections** are recorded by Digifort audit:

- **Connected**: Displays user connections to the server.
- **Disconnected**: Displays user disconnections from the server.

Searching the audit system allows the records to be filtered by Date, Category and keywords. Searching with keyboard will only find records by the fields: user, IP, complement, and the object's name.
It is possible to select the **Search by Exact Word** option to speed up the search.

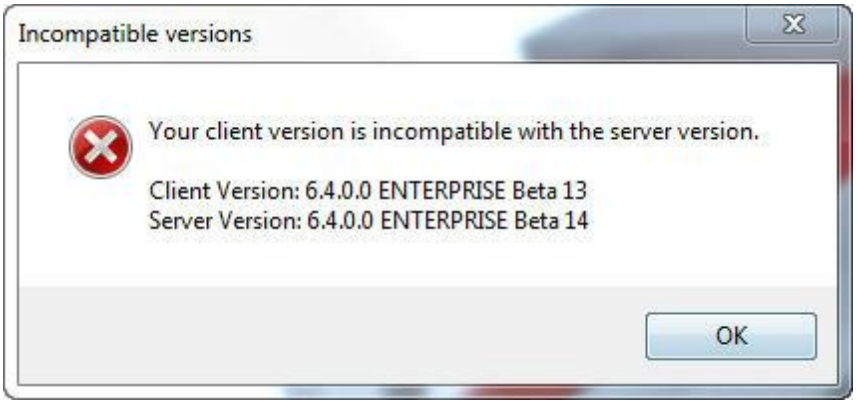
© 2002 - 2020 by Digifort, all rights reserved

Chapter XXII

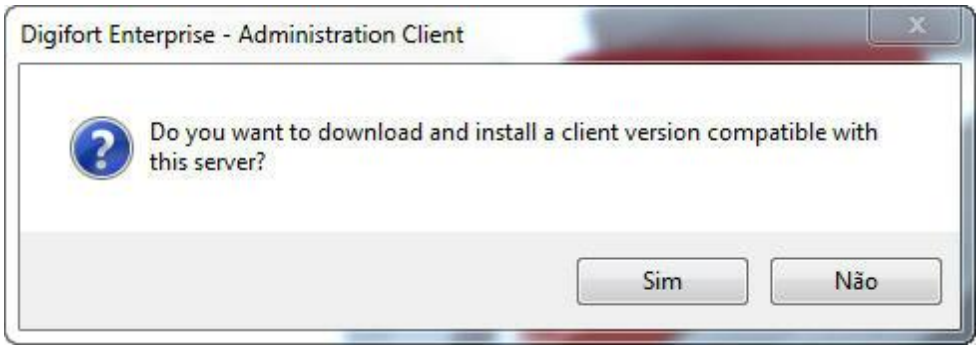
22 Automatic Client update

With swiftness and speed in mind, Digifort created a new feature that will be available in all the post-6.4 versions: the automatic update of the Surveillance and Administration Clients.
The feature will check if the server versions to which the client is trying to connect are the same.

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



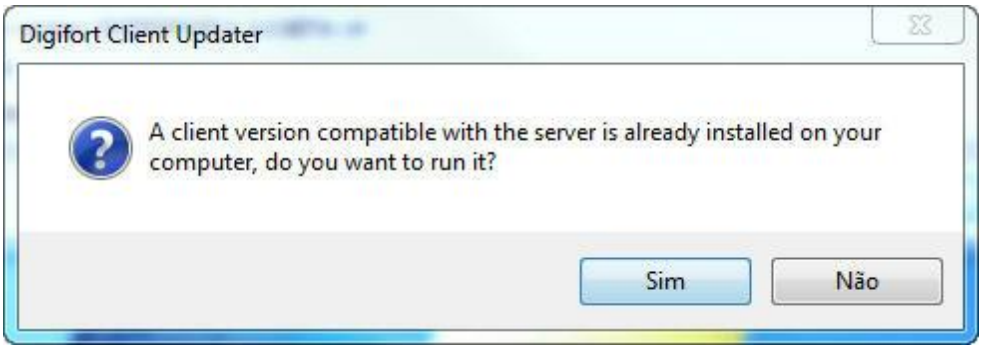
By clicking on **OK** a dialogue box will open with the following question: **Do you wish to download and install a client version compatible with this server?**



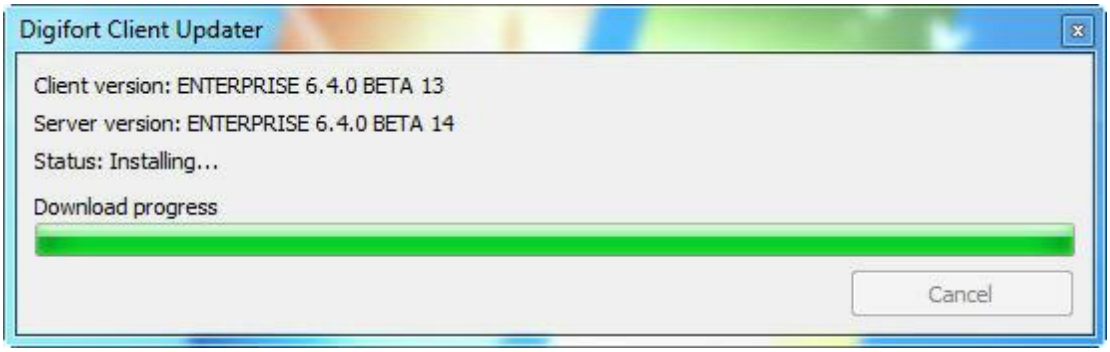
If you click on **No** the dialogue box closes and nothing happens. If you click on **Yes**, Digifort automatically installs the compatible client versions on the computer.

If the Digifort version on your computer is compatible, you will get the following message: **A compatible version is already installed on your computer; do you wish to execute it?**

© 2002 - 2020 by Digifort, all rights reserved

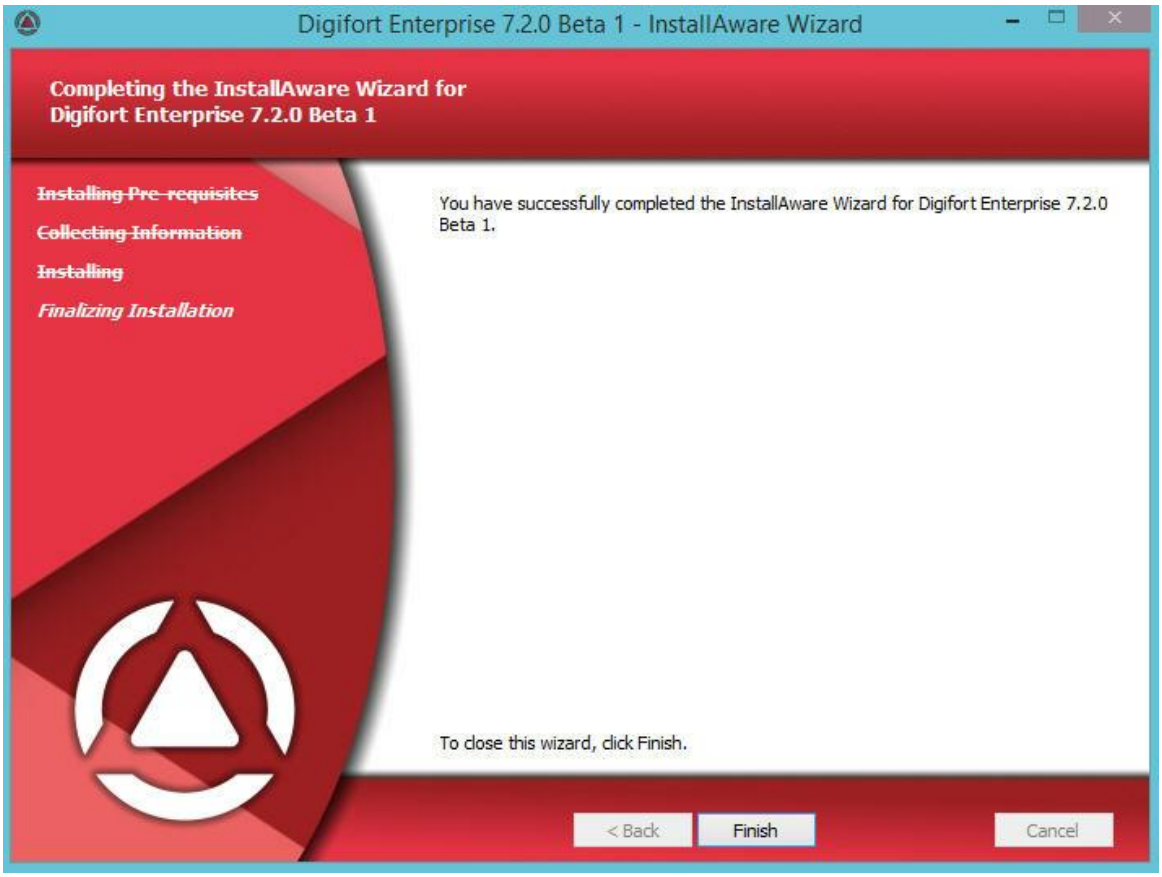


If you click on **Yes** the client will execute. Otherwise, the client installation will continue:



Continue the installation as normal and at the end click on **Finish**:

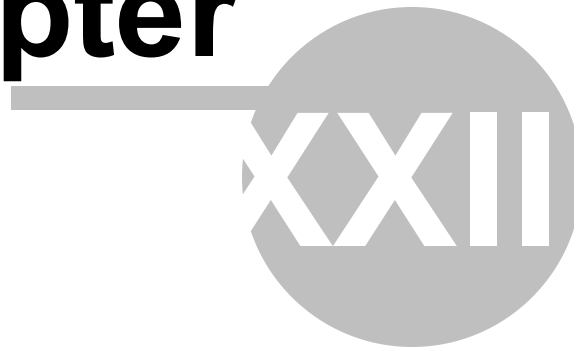
© 2002 - 2020 by Digifort, all rights reserved



Once installed, the compatible client is ready to connect to the requested server.

© 2002 - 2020 by Digifort, all rights reserved

Chapter



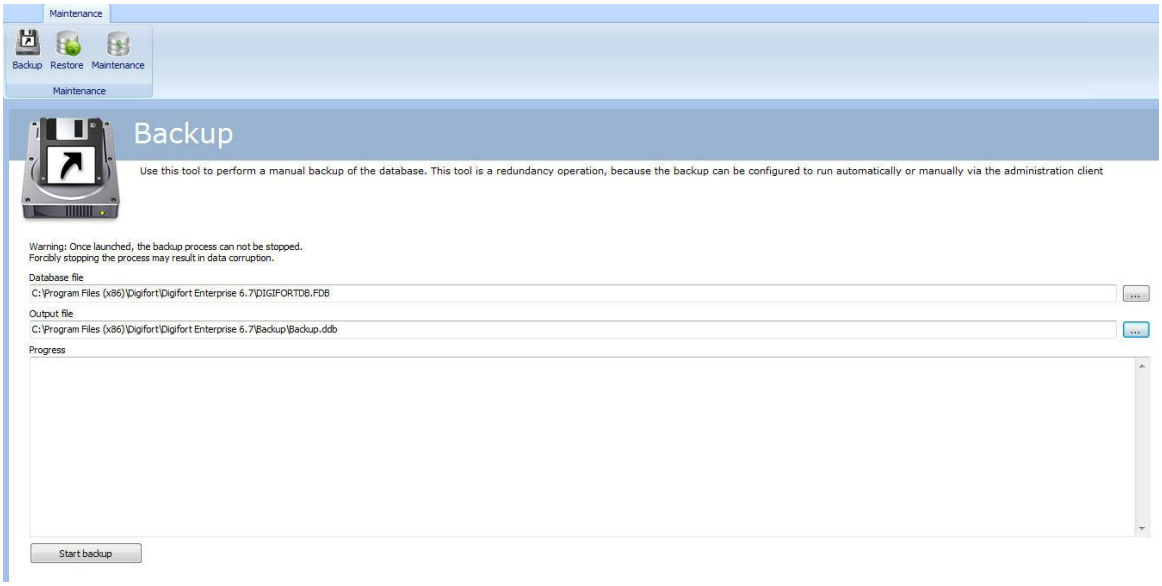
23 Maintaining the Database

We created new software for maintaining the database. Through it you can:

- **Make a backup of the database system**
- **Restore a backup of the database system**
- **Repair a corrupted database file**

This software is located in the root installation directory of Digifort. Its name is: DatabaseMaintenance.exe

Open the program as Administrator, and the following screen appears:



23.1 Backup

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

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

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

© 2002 - 2020 by Digifort, all rights reserved

23.2 Restore

After doing some backup, the only way to restore it is by this software.
To initiate a restore, click on the **Restore** button displayed in the image below:



The following screen appears:



- **Backup File:** Select the file to be restored with .**ddp**
- **Output File:** Select the file where the restore will be. Once that is done, replace the file in the root folder of Digifort with the name: **DIGIFORTDB.FDB**
- **Start Restore:** Click to start restoring the database.

23.3 Maintenance

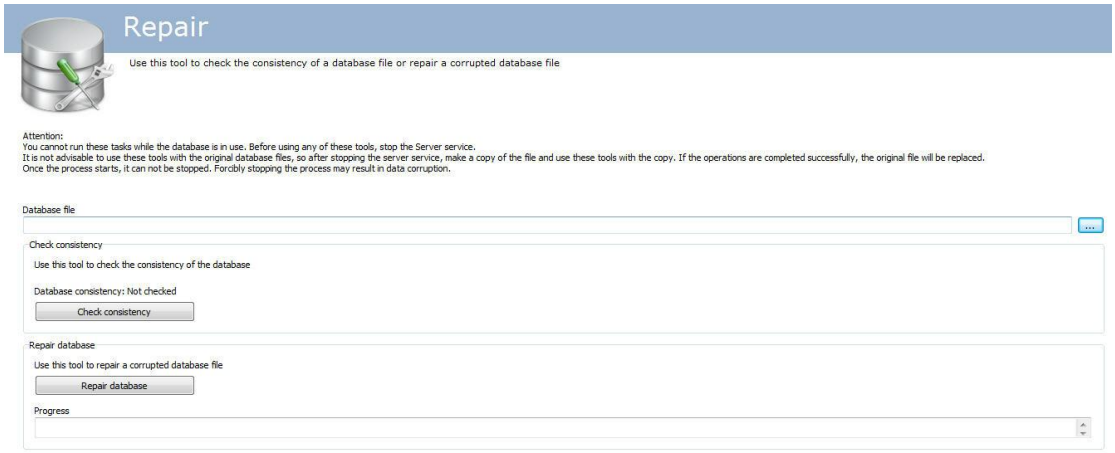
Use this option to check the consistency of the database or fix corrupt database problems.
To perform this function, click on the **Restore** button shown in the picture below:



NOTE: To perform maintenance, stop all Digifort services.

© 2002 - 2020 by Digifort, all rights reserved

The following screen appears:



The screen has the following features:

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter



24 Digifort Mobile Camera

The Digifort Mobile Camera is an application that can be installed on mobile phones and tablets with IOS (Apple) and Android (Google).

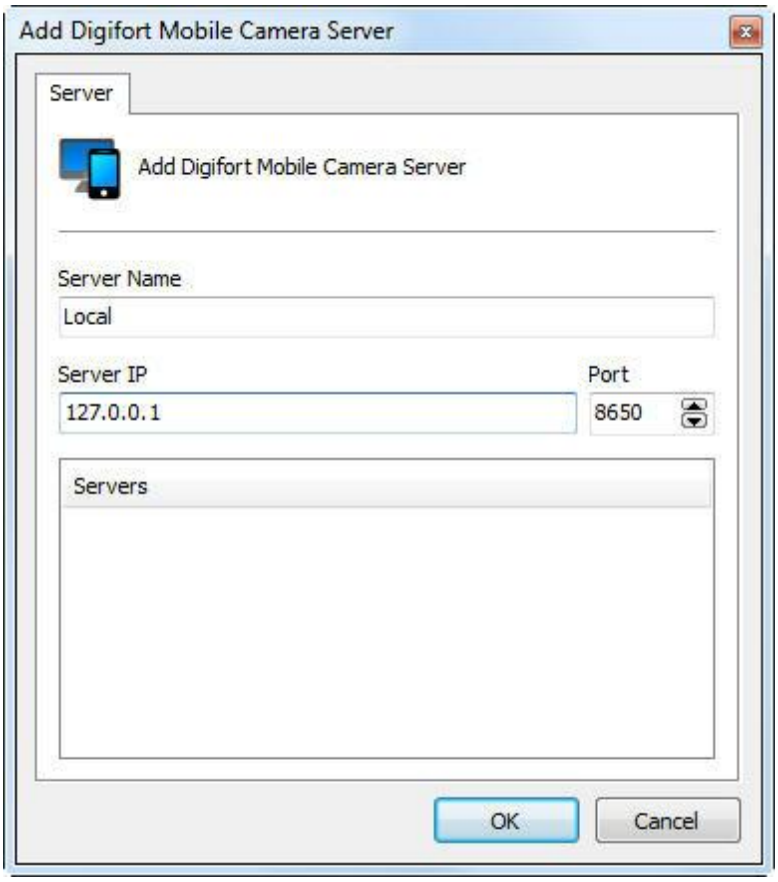
With this application you can turn your phone into a mobile remote camera and transmit a live video to your Digifort server via wireless or 3g / 4g connectivity, etc.

24.1 Registering the Mobile Camera Server

The first step to be done on the Mobile Camera configuration is to add and configure the server that will receive the application video streams.
To add a server click on the **Digifort Mobile Camera Servers** tree and then on the button **Add Server**, which opens the server registration screen, as illustrated in the image below:



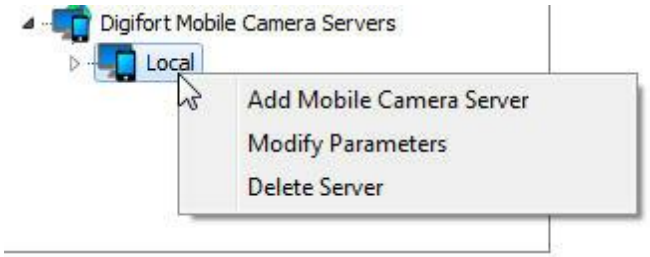
© 2002 - 2020 by Digifort, all rights reserved



- **Server Name**: Type the name of the server to be added. After data confirmation, the server name cannot be changed.
- **Server IP**: Enter the IP of the server to be managed.
- **Port**: Enter the communication port with the server. By default the port is 8650.
- **Servers**: In this list, all servers in the Mobile Camera that the Administration client can find on the network are available. Clicking on one of the servers, the IP and Port fields described above are automatically filled in. You only have to fill in the server name field to register.

After informing all data correctly click on **OK**.

After the server inclusion, it appears in the **Configuration Menu** as shown in the figure below:



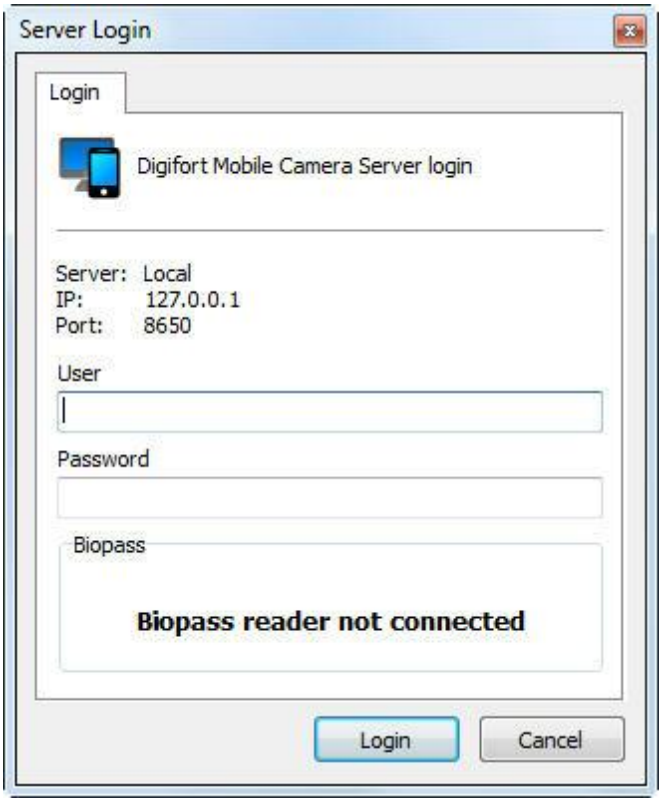
To change the settings of a server already saved, right-click on the server you want, and then click on Change parameters. In the window that opens, change the data as required and click on **OK**.

© 2002 - 2020 by Digifort, all rights reserved

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

24.2 Configuring the Mobile Camera Server

To configure the server, double-click on the registered server and the login screen appears:



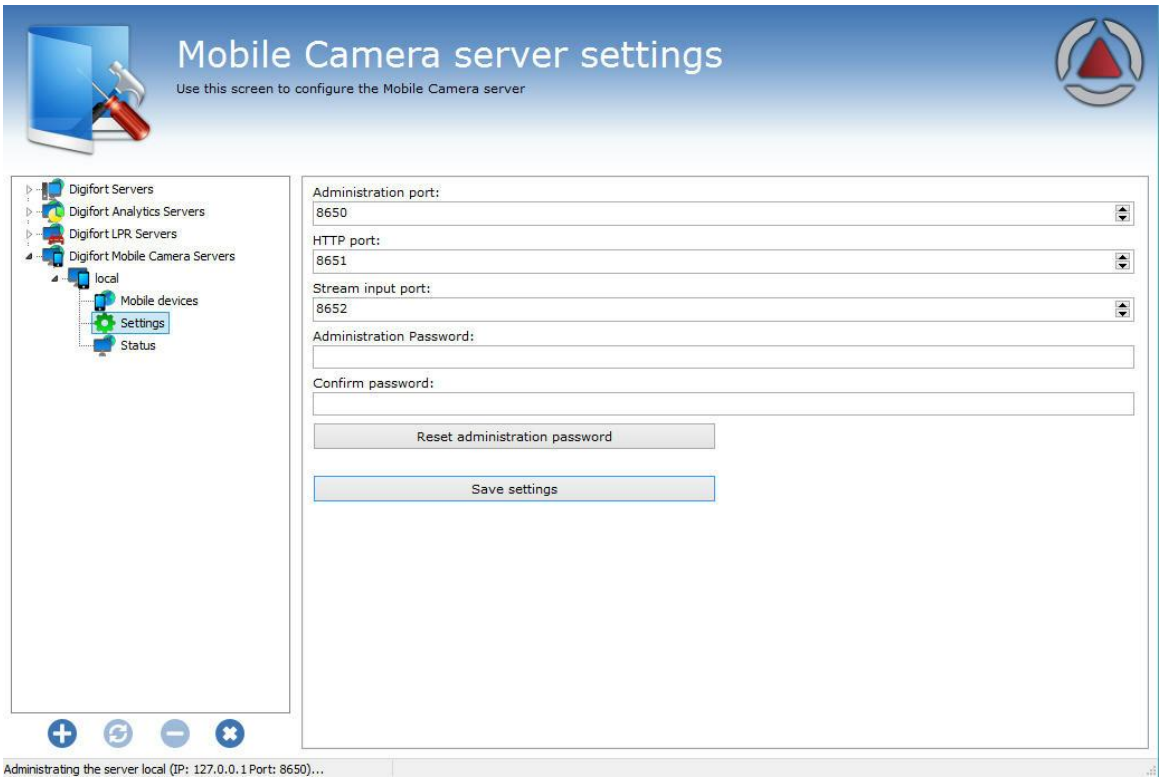
The default username is **admin** and the password is blank.

24.2.1 Configurations

To access the server configurations, click on **Configurations** as in the image below:



© 2002 - 2020 by Digifort, all rights reserved



This screen provides the following features:

- **Administration port**: Port used by Digifort to configure the Digifort Mobile Camera server.
- **HTTP Port**: http port used for communication.
- **Stream input port**: Port used to receive the video stream;
- **Administration password**: Administration password of the Digifort Mobile Camera server.
- **Confirm password**: Confirm the password to register.

- **Admin password reset**: redefines default password, that is, blank.
- **Save Configuration**: Saves the changed configuration.

Note: It is important to remember that these ports must be released on the firewall and network of computers involved.

24.2.2 Status

In **status** you can check important information such as consumed bandwidth and connected devices.

To access click on **Status** as shown below:

© 2002 - 2020 by Digifort, all rights reserved



In the **General** tab, there are two charts:



The first one shows the **total bandwidth consumption** and the second one shows the amount of **devices attached** to the server.

In the **connections tab**, there is the list of connected devices, IP, bandwidth consumption and the total time connected to the server:

© 2002 - 2020 by Digifort, all rights reserved



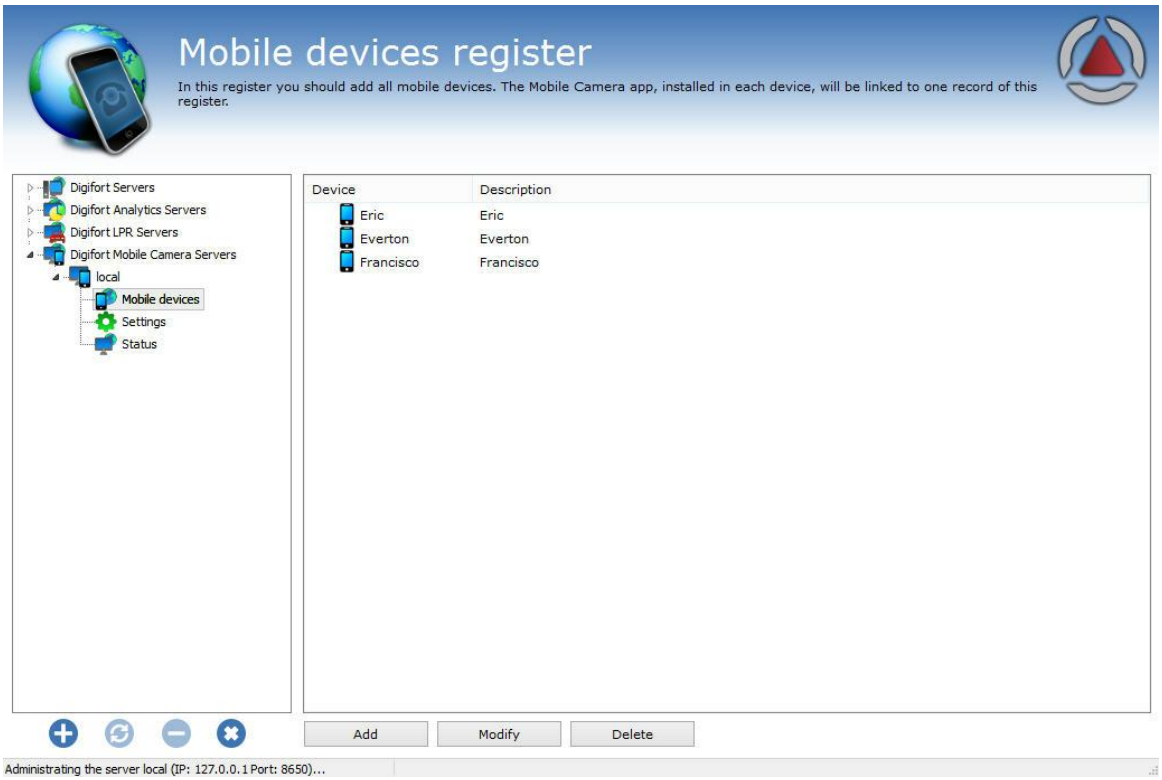
24.2.3 Mobile devices

You need to register the devices that will send the images to Digifort.
Click on **mobile devices** as in the image below:



The following Register screen appears:

© 2002 - 2020 by Digifort, all rights reserved

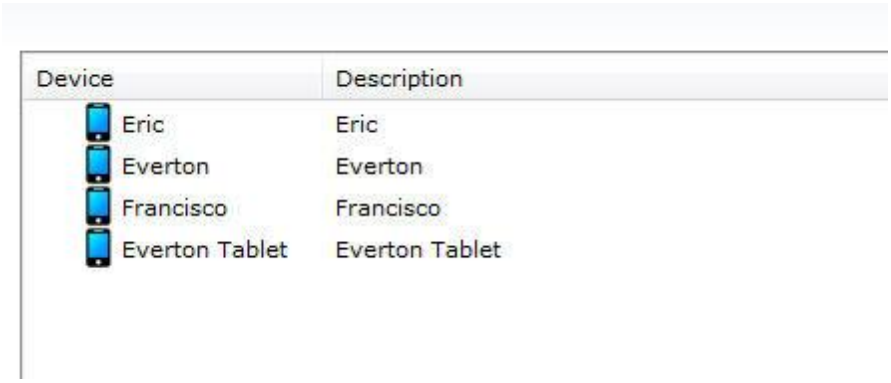


Add a **unique name** to associate the mobile device to the Software. To do this, click on Add. The following screen appears:



Enter the device name and click on OK. The device will be registered in the list:

© 2002 - 2020 by Digifort, all rights reserved



24.3 Configuring the application

First of all, download the **Digifort Mobile Camera** application on Google Play or AppleStore and install it on your mobile device.

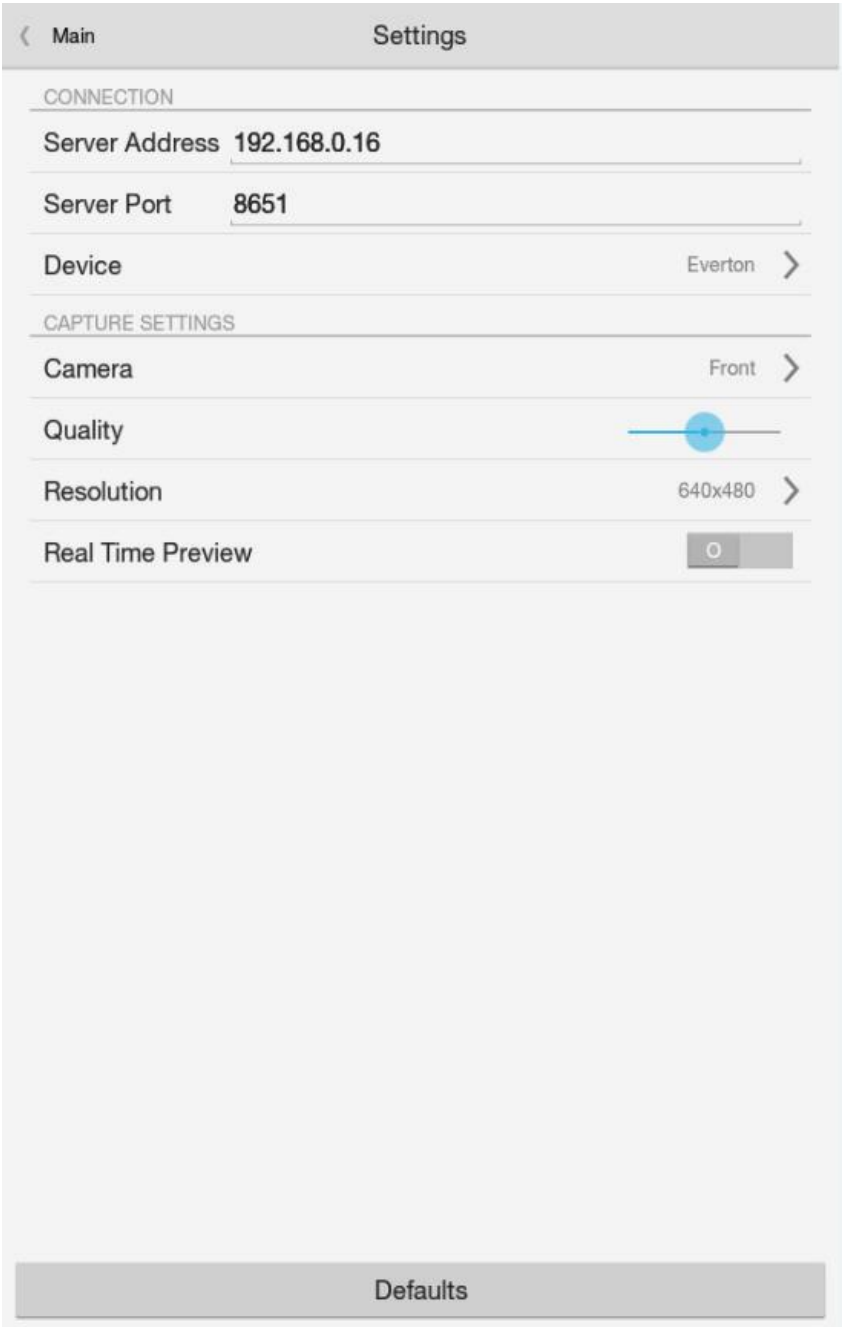
When you open the application, the following screen appears:

© 2002 - 2020 by Digifort, all rights reserved



First, click on the gear on the top right corner, and the following configuration screen appears:

© 2002 - 2020 by Digifort, all rights reserved



In the configuration screen, register the **Server IP** where the **mobile device** is registered, as explained in the previous topic.

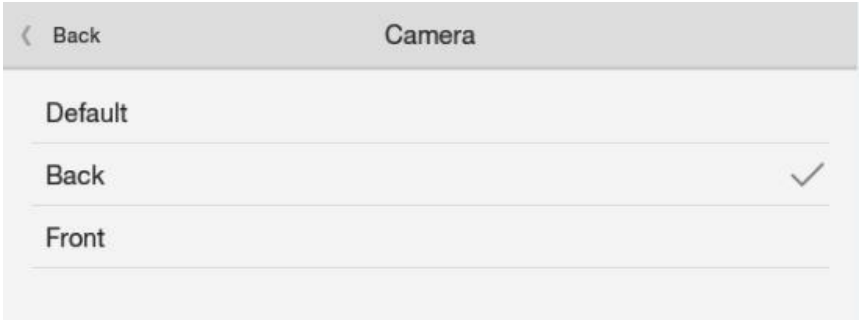
- **The server port** is the same from the previous topic.
- **Device**: click on this option and the devices registered in Digifort appear in a list:

© 2002 - 2020 by Digifort, all rights reserved



Select the desired device.

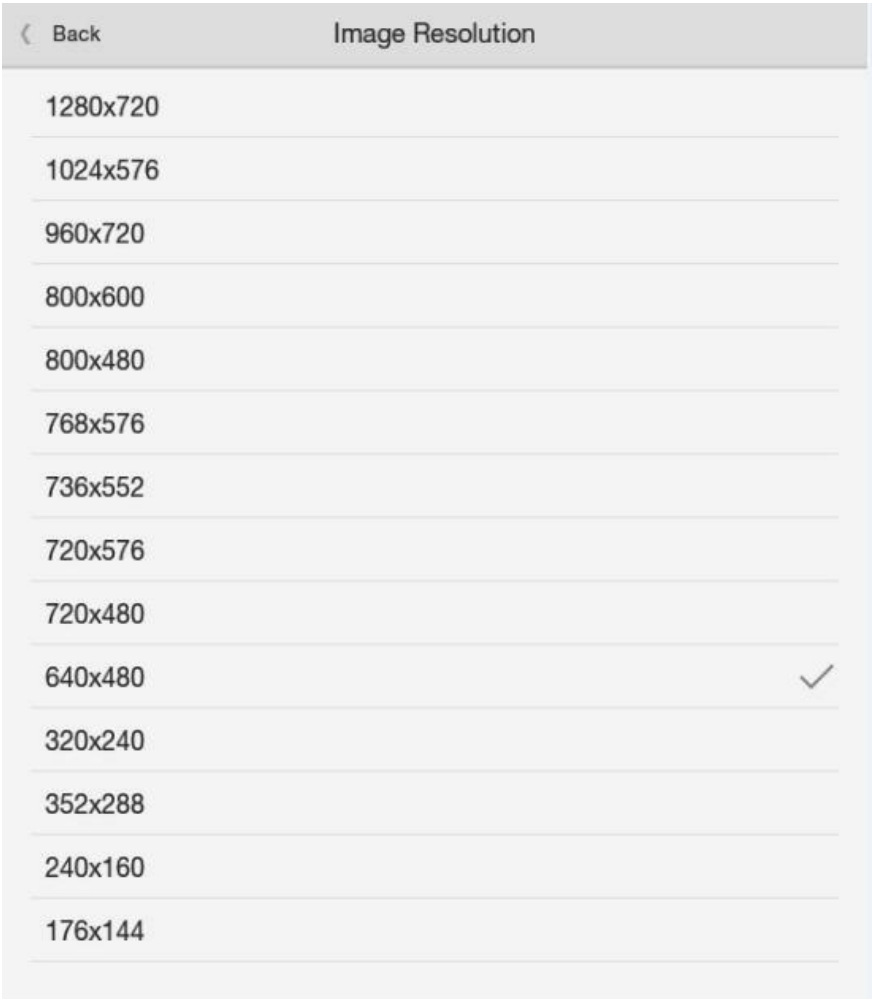
Camera: If your device has a front or rear camera, you can select it in this option.



Quality: Select the streaming quality of the images.

Resolution: Click on this option to choose the resolution for image streaming;

© 2002 - 2020 by Digifort, all rights reserved



Real Time Preview: If the option is not enabled, the video stream appearing on your device screen is sent to the system. In case of slow streaming, you can have a defective image.

After the **settings**, go back to the home screen and click on **Start Streaming**

© 2002 - 2020 by Digifort, all rights reserved



The image captured by the mobile device is sent to the server.

On the **top left** corner, there is the option to **turn on your device flashlight** if supported.
On the **lower left** corner, there is the detail of video streaming: **Frames per second and bandwidth used**.

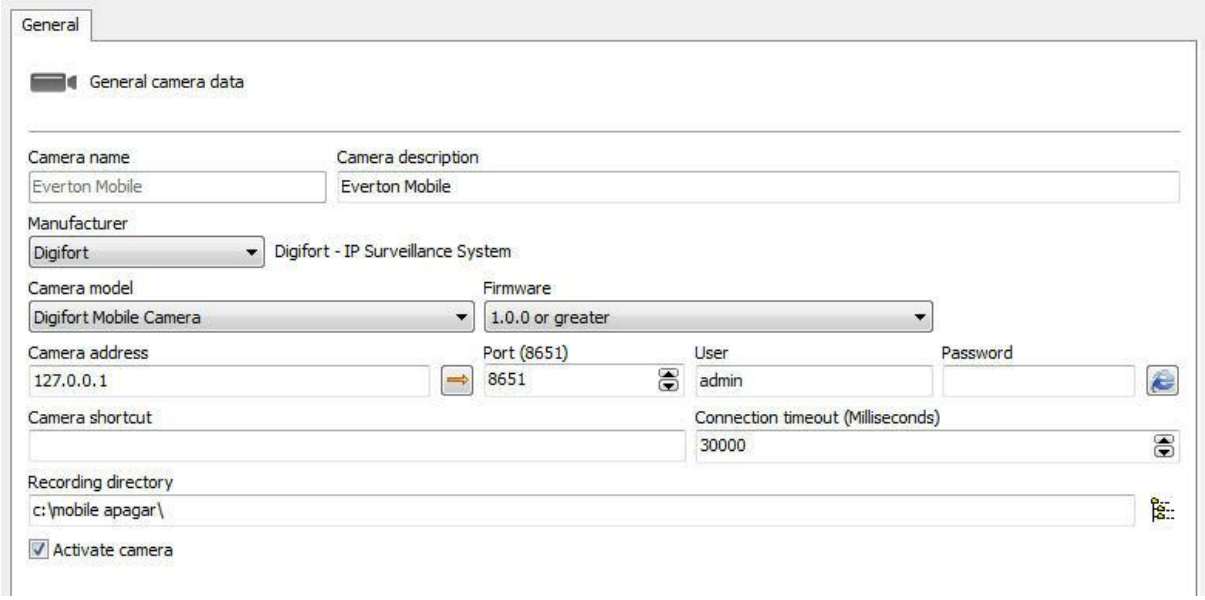
If you want to interrupt the video streaming, simply click on **Stop Streaming**.

24.4 Registering the camera

The last step is to register the Mobile Camera to record in Digifort.

Open the recording server and click on **Add**. If you have any questions on camera registration, check Recording Server

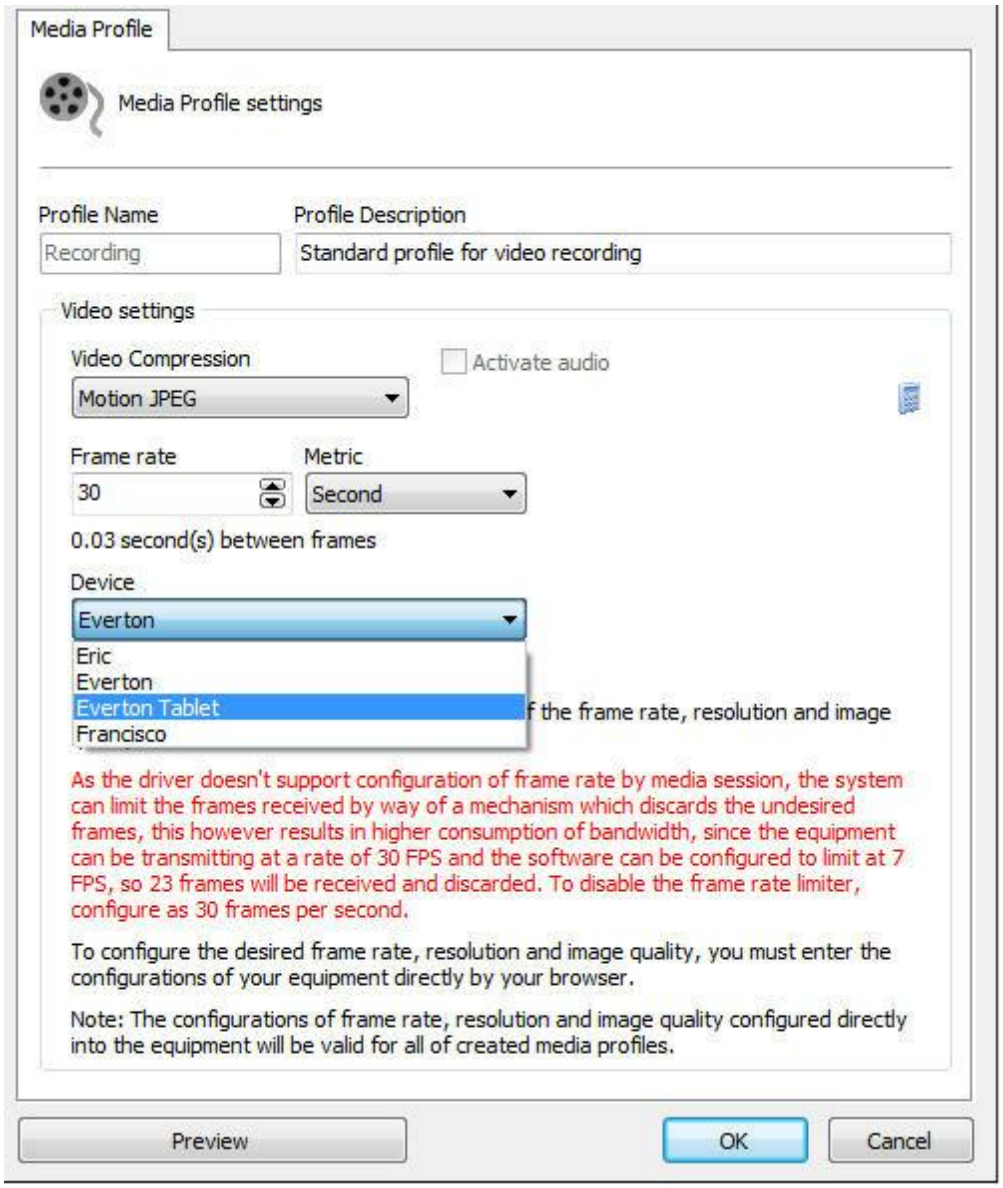
© 2002 - 2020 by Digifort, all rights reserved



On this screen, type the **Name** and description to identify your camera.
In **Manufacturer**, choose Digifort.
In **camera model** choose Digifort Mobile Camera.
In **Camera Address**, choose your server IP from the Digifort Mobile Camera server. Check Configuring the Mobile
If it has not been changed, the default communication port of the Digifort Mobile Camera is **8651**.
In User and Password, enter the Digifort Mobile Camera server user.
And finally, choose a directory for recording;

Now click on **Media Profiles** and double click on the recording profile:

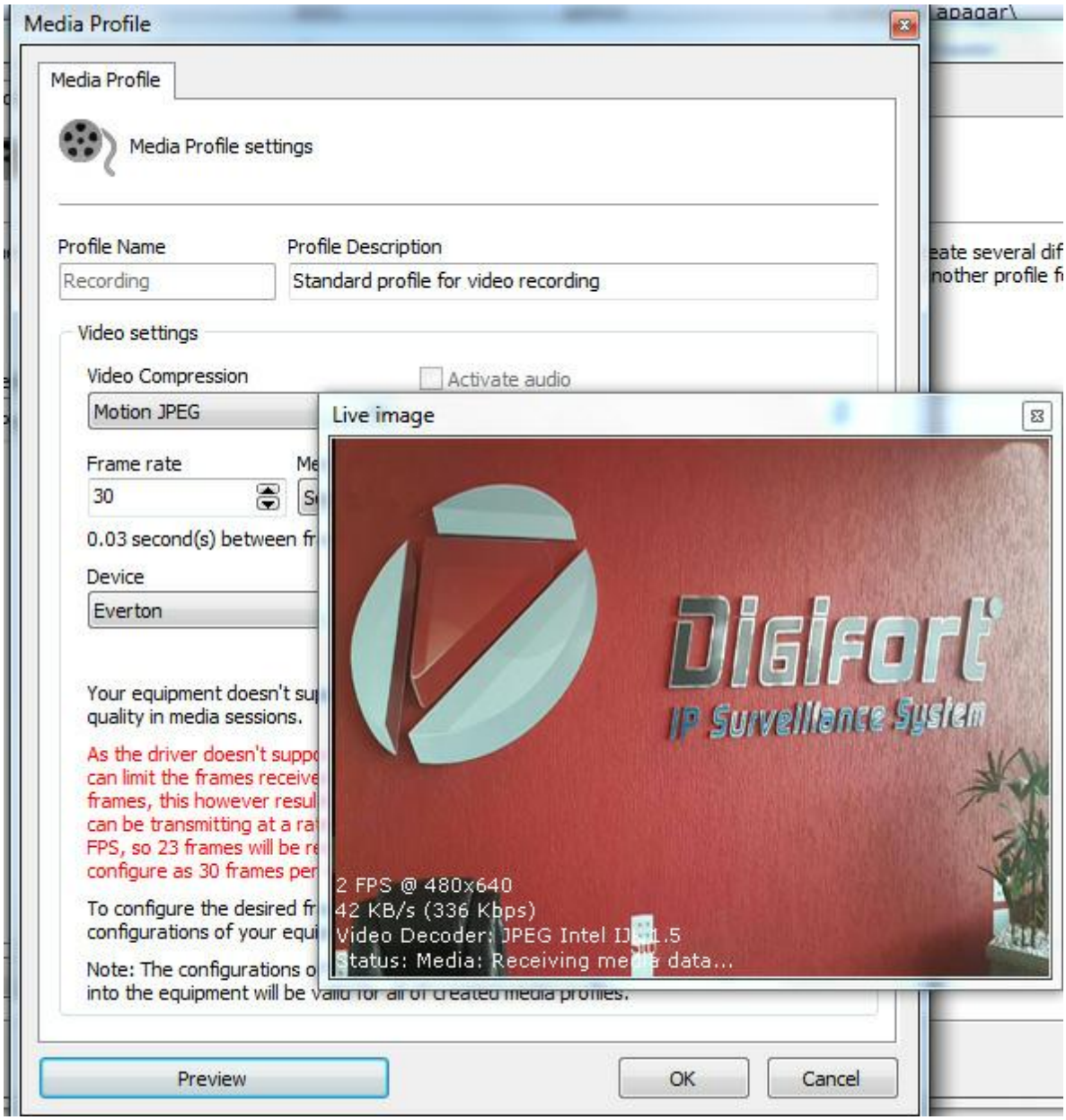
© 2002 - 2020 by Digifort, all rights reserved



The Digifort streaming is made in **JPEG Motion**. Choose the desired frames per second rate.

Now on the **Device** option, choose the device that is receiving the **Stream**.
Click on **Preview** to view the image being streamed:

© 2002 - 2020 by Digifort, all rights reserved



Done, Digifort is ready to record the images received.
Note that the resolution of the image to be recorded must be configured in the Device, as shown in the Configuring the application topic

© 2002 - 2020 by Digifort, all rights reserved

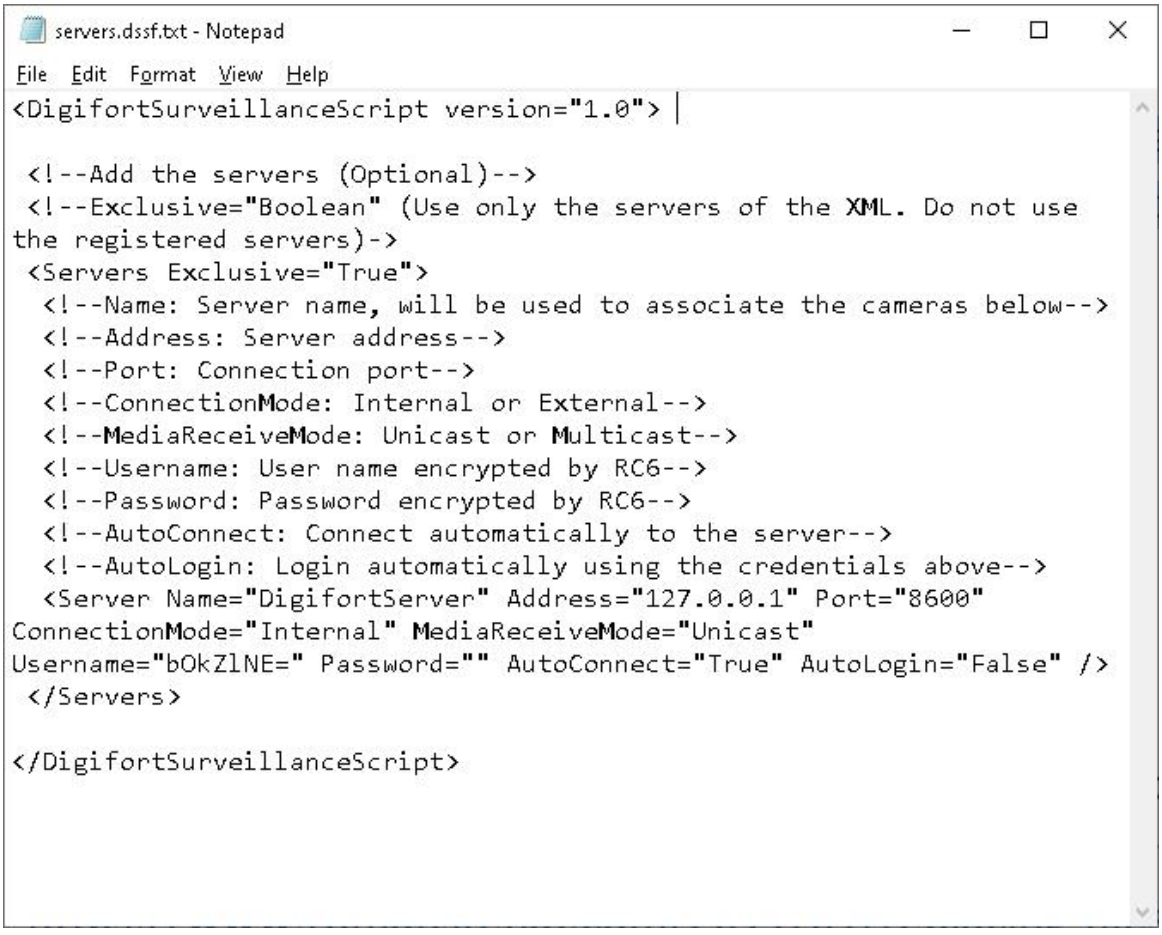
Chapter XXV

25 Centralized server list

Attention, this feature is intended for advanced users of the system.

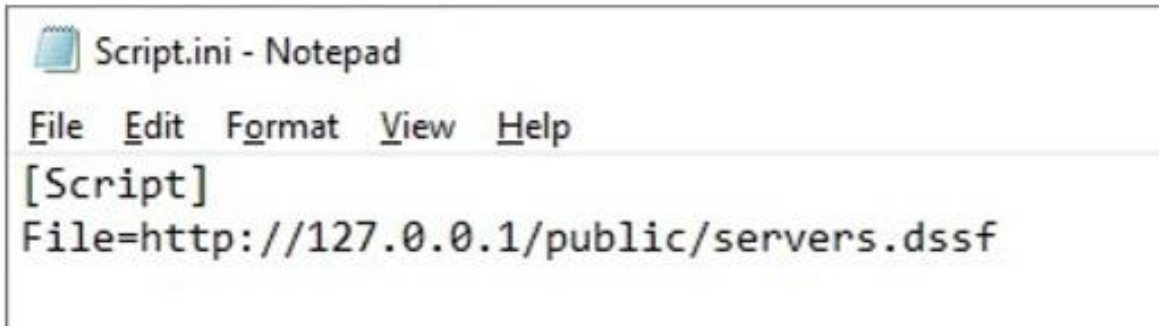
It is possible to have your Monitoring clients access Digifort servers listed in a file that is hosted on the eu network on a web server.
The idea behind this feature is that you do not have to manually register the servers to be connected to the Monitoring client manually.

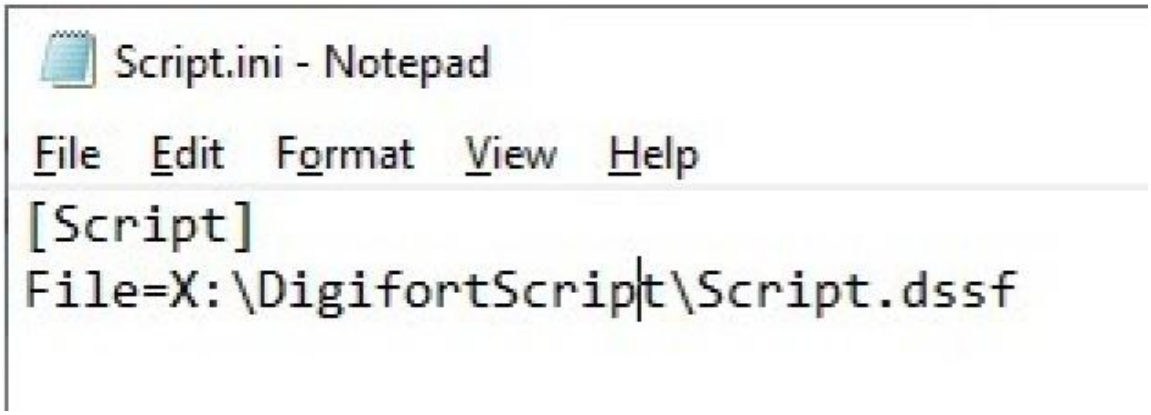
To do this, you will need to create a file with the extension .dssf. Within this file there will be an xml structure with the information of the server to be accessed:



After that create a Script.ini file in your Digifort installation folder (Ex: C:\Program Files (x86) \Digifort\Digifort <your version>)
with the path to the Dssf file as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved





Now whenever you start the monitoring client it will look for the servers contained in the dssf file.

© 2002 - 2020 by Digifort, all rights reserved