Digifort Enterprise Manual
Administration Client
Version 7.4.1
Rev. A

© 2002 - 2024 by Digifort. All rights reserved.

Index

Part I Welcome to Digifort Enterprise Manual 13

1 Screen Shots ... 14
2 Who is this manual intended for? ... 14
3 How to Use this Manual ... 14
4 Prerequisites ... 14

Part II Service Manager 15

1 How To Run The Services Manager ... 16
2 How To Start Services ... 17
3 How To Stop Services ... 17

Part III Basic Features of the Administration Client 18

1 How to run the Administration Client ... 19
Interface ... 20
2 How to Configure the Servers to be Managed ... 20
3 How to Connect to a Server for Management ... 22
4 Multiple Object Configuration ... 23
5 Duplicate Objects ... 24
6 Extra Columns on Registration Screens ... 24
7 Export Data to CSV ... 25
8 Import Objects from Other Servers ... 26
9 Shortcuts to Registration Lists ... 27

Part IV Licensing 28

1 How to Configure Licenses ... 29
How to add a License ... 31
How to Send Registration Data ... 31
How to install licenses through Online Licenses ... 32
How to Install Licenses from License Files ... 33
Activating a Temporary License ... 33
Requesting a Demo license ... 35

Part V Registering the software 37

1 How to register the software ... 38
2 Registering the software Online ... 39
3 Registering the software Offline ... 40

Part VI Recording Server 41

1 How to Add a Camera ... 42

© 2002 - 2024 by Digifort. All rights reserved.

Camera **43**
General 43
Lenses 45
Panomorph Lenses 46
Fisheye Lenses 47
Motion Detection 47
Use Motion Detection by Software 47
Auto disable motion detection during PTZ 50
Use motion detection by device 51
Use motion detection by external notification 51
End detection interval and motion duration 51
Audio 52
Image Filters 53
Streaming **53**
Media Profiles 53
How to add Media Profiles 54
How to view the functioning of the configured media profile 56
Disk space usage calculator 56
Audio 59
Recording 59
Automatic Recording Profile Switching 60
Create Bookmark on Profile Switching 61
Snapshot Buffer 62
Live View 62
Switch media profile on camera selection 63
Recording **64**
Settings 64
Recording Type 64
How to configure the recording schedule 64
Recording Cycle 69
Image Buffer 69
Self-Healing 69
Metadata 71
Archiving 72
Operation and tips 73
Rights **74**
Users 74
PTZ **74**
Settings 74
PTZ Usage 75
PTZ Lock 76
Operation Scheduling 76
Presets 77
How to create a preset 78
PTZ Patrol 78
How to add a PTZ Patrol scheme 79
How to configure schedules of PTZ Patrol Schemes 82
Auxiliary 82
Joystick 83
Menu Control 85
Visual Joystick 86
I/O **86**
How to add input events 86
How to add output actions 89

© 2002 - 2024 by Digifort. All rights reserved.

How to configure event scheduling ... 90
Virtual I/O ... 91
Events ... 94
Communication ... 94
Communication Failure Event ... 94
Connection restore event ... 94
Device failure report ... 94
Recording Failure Event ... 95
Motion Detection ... 95
How to configure motion detection event ... 96
Audio Detection ... 96
Manual Events ... 97
Device Events ... 98
Event Variables ... 99
Privacy ... 101
Privacy Mask ... 101
Privacy Mode ... 103
Advanced ... 104
Object Links ... 104
Advanced Device Settings ... 108
Operational Map ... 110
Multi-Channel Device Registration ... 110
Import Cameras From Other Servers ... 113
Finding and Registering Cameras Automatically ... 113
Single Camera Registration ... 115
Multiple Camera Registration ... 115
2 How to Delete a Camera ... 116
3 How to Change Parameters for Multiple Cameras Simultaneously ... 117
Recording Directory ... 118
Add, Modify or Delete Media Profiles ... 118
Grant and Deny User Rights ... 119
4 Camera Groups ... 120
5 Monitoring Recording Server Status ... 122
Individual Camera Details ... 123
Recording Connection ... 124
Connections ... 125
I/O Ports ... 125
Device Events ... 126
Schedulings ... 126
Recording Self-Healing ... 127
Disk ... 128
6 Edge Recording ... 128
Activity Log ... 129
Part VII I/O Devices 131
1 How to access the register of I/O Devices ... 132
How to add an I/O Device ... 132
General ... 133
IO Control ... 133
Events ... 134
Communication Failure Event ... 135
Communication Restore Event ... 135

© 2002 - 2024 by Digifort. All rights reserved.

Scheduling ... 135
How to Change Parameters for Multiple Devices Simultaneously ... 136
2 Status ... 136
Individual Device Details ... 136
General ... 137
I/O Ports ... 137
Scheduling ... 138
3 I/O driver for testing hosts ... 138

Part VIII Alerts and Events 140

1 How to Access Alerts and Events ... 141
How To Configure Contacts ... 141
How To Add A Contact ... 142
How To Set Up Contact Groups ... 143
How To Add A Contact Group ... 143
Global Events ... 144
How To Access The Global Events register ... 144
How To Add A Global Event ... 145
General ... 146
Rights ... 146
Scheduled Events ... 147
Registering Scheduled Events ... 147
Adding Scheduled Events ... 148
Scheduling Types ... 149
Once ... 149
Daily ... 150
Weekly ... 150
Monthly ... 151
2 How to configure event actions ... 151
Send an email to a group of people when an alarm occurs ... 153
Display images from cameras on the operator screen ... 154
View a looped recorded video on the operator screen ... 155
Display snapshots of cameras from the moment of the event on the operator's screen ... 156
Play an alarm sound in the Surveillance Client ... 156
Send instant message to operator ... 157
Request written acknowledgement from users ... 158
Send Objects to Virtual Matrix ... 158
Send single objects ... 159
Send views ... 160
Send push notification to mobile devices with Digifort Mobile Client installed ... 160
Send Audio Clip to Device ... 161
Call camera presets ... 162
Trigger alarm output actions scripts ... 163
Trigger Global Events ... 164
Activate or Deactivate system objects ... 165
Send an HTTP request ... 166
Create Bookmark ... 167
Download recordings from devices that support edge recording ... 168
Create Timer Events ... 169

Part IX User Management 172

1 Adding, Changing, and Deleting Users ... 173

© 2002 - 2024 by Digifort. All rights reserved.

User Account Info ... **175**
2 Factor Authentication ... 176
Login IPs ... 177
Adding an Access IP Range ... 177
User Rights ... **178**
Video Playback and Search ... 178
Live Audio ... 179
Surveillance Views ... 179
System Cameras ... 179
IO Devices ... 179
Alarms ... 179
Virtual Matrix ... 179
System Users ... 179
Alerts and Events ... 179
Global Events ... 179
Scheduled Events ... 180
Maps ... 180
Operational Maps ... 180
Analytics ... 180
Plate Recognition ... 180
Web Pages ... 180
Screen Layouts ... 180
Server ... 180
Report Authentication ... 180
Bookmarks ... 181
Recording Protection ... 181
Surveillance Client Features ... **181**
Centralized Surveillance Client Configuration ... 182
Policies ... **184**
Ownership Identification ... **185**
Web Customization ... 185
Watermark ... 186
General User Remarks ... **186**
Groups View ... **187**
Rights View ... **187**
2 Monitoring User Activities ... **188**
3 How To Change Parameters For Multiple Users Simultaneously ... **189**
4 Adding, Changing, and Deleting Groups ... **190**
Group Rights ... **192**
Surveillance Client Features ... **192**
Policies ... **192**
Rights View ... **193**
5 Options ... **193**
Security ... **193**
Force use of strong password ... 193
OTP ... 194
Active Directory ... **194**
6 Active Directory Integration ... **195**
Part X Layouts Management **197**
1 How To Access Layouts Management ... **198**
How To Add A Layout ... **198**

© 2002 - 2024 by Digifort. All rights reserved.

Part XI BioPass 201

1 How to install BioPass on your computer ... 202
2 How to set up BioPass ... 202

Part XII Maps 207

1 Map Registration ... 208
- Adding Images ... 209
- Google Maps Integration ... 210
- Adding Texts ... 214
- Adding Cameras ... 214
  - Camera Field of View ... 216
  - Adding Presets ... 218
- Adding Input Events, Output Actions, and I/O Ports ... 218
  - Adding Events Or I/O Ports ... 218
  - Adding Output Actions ... 220
- Adding Global And Manual Events ... 220
- Map Link ... 221
- Checking For Invalid Objects In Maps ... 222
- Alignment Grid ... 223
- Map Editor Tips ... 223
  - How To Select Multiple Objects ... 223
  - How To Delete Objects ... 224
  - Move objects with precision ... 224
- Icon for Operational Map ... 224
- Object Status ... 225
- Rights ... 225

2 How To Change Parameters For Multiple Maps Simultaneously ... 226

Part XIII Operational Map 228

1 Registering Operational Maps ... 229
- Rights ... 231
- How To Change Parameters For Multiple Maps Simultaneously ... 232

2 Custom Objects ... 232
- Linked Operational Maps ... 233
- Rights ... 234
- How To Change Parameters Of Multiple Objects Simultaneously ... 235
- Working Example ... 235

Part XIV Analytics 237

1 Server Analytics ... 238
- Understanding Distributed Processing ... 238
- How To Start The Analytics Server Service ... 239
- How To Configure The Servers To Be Managed ... 240
- How to Connect to a Server for Management ... 241
- Licensing Analytics Server ... 242
  - How To Configure Analytics Licenses ... 243
- Analytics Server Status ... 244
  - Monitoring ... 245
- Analytics Server Settings ... 246

© 2002 - 2024 by Digifort. All rights reserved.

Adding an Analytics Configuration 247
Options 248
Events 248
Communication Failure 249
Communication Restore 249
Rights 249
How To Configure Basic Analytics 250
Foreign Objects 252
Removed Objects 254
Face Detection 255
How To Configure Advanced Analytics 256
Scene Calibration 259
Object Classification 261
How To Configure Analytics Rules 263
Presence 263
Enter 263
Exit 264
Appear 265
Disappear 266
Direction Filter 266
Speed Filter 267
Tailgating 268
Stopped 269
Loitering 270
Abandoned and Removed Objects 271
How to configure the Count line rule 272
Counters 273
Camera Tampering 276
Advanced Options 276
How To Configure Professional Analytics 278
Object Trackers 280
How to configure Pro Analytics rules 281
Basic Rules (Inputs) 282
Abandoned Object 282
Appear 283
Direction 283
Directional Crossing 284
Disappear 285
Loitering 285
Enter 286
Exit 286
Presence 286
Stopped 287
Tailgating 287
Counting Line 288
Fall 289
Hands Up 289
Fight 290
Filters 290
Speed 290
Object Types 291
Colors 292
Retrigger 292
Conditional 293

© 2002 - 2024 by Digifort. All rights reserved.

Continuous ... 293
Previous ... 293
Logical Condition ... 294
Repeatedly ... 294
Counters ... 295
Scene Calibration ... 298
Object Classification ... 301
Camera Tampering ... 303
Advanced Options ... 303
How To Change Parameters For Multiple Analytics Simultaneously ... 306
General Options ... 306
2 Edge Analytics ... 307

Part XV Plate Recognition 309

1 LPR on Server ... 310
Understanding Distributed Processing ... 310
How To Start The LPR Server Service ... 311
How To Configure The Servers To Be Managed ... 312
How To Connect To A Server For Management ... 313
Licensing The LPR Server ... 314
How To License The LPR Server ... 314
How To License Carmen Engine ... 315
How To License Neural Labs Engine ... 315
How To Extract The .c2v File To Request The License ... 315
How To Apply The .v2c File To License The Engine ... 317
LPR Server Status ... 318
Monitoring ... 319
Sessions ... 320
LPR Server Settings ... 320
API Keys ... 322
Adding an LPR Configuration ... 323
Engine Settings ... 324
Sensor ... 324
Image ... 325
Attributes ... 326
Options ... 327
Surrounding Cameras ... 328
Rights ... 328
Events ... 329
Communication Failure ... 330
Communication Restore ... 330
How To Change Multiple LPR Parameters Simultaneously ... 330
General Options ... 331
Checking the Status of LPR Configurations ... 332
General ... 332
Configurations ... 332
LPR Bridge ... 334
2 Edge LPR ... 334
3 License Plates ... 335
Registration Expiration ... 337
4 Configuring LPR lists ... 338
Masks ... 339

© 2002 - 2024 by Digifort. All rights reserved.

5 Events ... 340
Conditions ... 342
6 LPR Zones ... 343
Processing ... 344
Options ... 345
LPR zone events ... 346
Occupancy ... 346
Rights ... 347
LPR Zone Groups ... 348
7 Plate Category Groups ... 349
8 Integrations ... 351

Part XVI Web Pages 353

1 Web Page Registration ... 354
Rights ... 356
2 How to change parameters for multiple web pages simultaneously ... 357

Part XVII Settings 358

1 System ... 359
General ... 359
Recordings ... 360
Recording Encryption ... 360
Advanced ... 360
Recording Protection ... 361
Master / Slave ... 361
Multicast ... 362
Backup ... 363
Backup Structure ... 363
Restoring Backups ... 364
Settings ... 364
Folders ... 364
Database ... 365
Database ... 365
SMTP ... 366
Disk Limits ... 367
Network Units ... 368
SNMP ... 369
Google Maps ... 370
Protocols ... 370
2 Server Events ... 371
3 Failover ... 372
Multiple Servers ... 376
How to change parameters for multiple monitors simultaneously ... 377
4 IP Filters ... 377
IP Filter Registration ... 377
How to add authorized IPs ... 378
How to add rogue IPs ... 378
5 Report Authentication ... 379

© 2002 - 2024 by Digifort. All rights reserved.

Part XVIII Server Information 381

1 Disk Usage ... 383
2 Master / Slave ... 383
3 Failover ... 383
4 Monitoring ... 384

Part XIX Web Server 385

1 Settings ... 386
2 FIle Server ... 386

Part XX RTSP Server 388

1 Settings ... 389
2 Status ... 389

Part XXI Logs 392

1 System Logs ... 393
How To Configure System Logs ... 393
How To View System Logs ... 393
2 Event Logs ... 394
How To Configure Event Logs ... 394
How To View Event Logs ... 395
3 Audit ... 395

Part XXII SSL Certificates 398

1 How to Generate a Self-Signed Certificate ... 399
2 Converting Certificates to PFX Format ... 401

Part XXIII Clients auto-update 403

Part XXIV Database Maintenance 406

1 Backup ... 407
2 Restore ... 407
3 Maintenance ... 408

Part XXV Centralized Server List 409

Part XXVI Mobile Camera 412

1 How to start the Mobile Camera Server service ... 413
2 How to configure the servers to be managed ... 414
3 Configuring the Mobile Camera server ... 415
Mobile Devices ... 415
Settings ... 416
Status ... 417

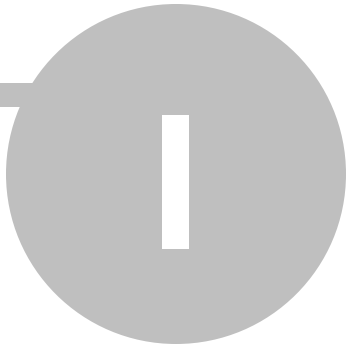
© 2002 - 2024 by Digifort. All rights reserved.

4 Configuring the Application 418
5 Registering the Camera on the VMS Server 421

Index 0

© 2002 - 2024 by Digifort. All rights reserved.

Chapter



1 Welcome to Digifort Enterprise Manual

This User Manual and Technical References provide all the information necessary to effectively implement and use all the basic and advanced features found in the Digifort System Administration Client.Enterprise.
This manual is constantly updated and does not describe the functionality of the Beta and DEV versions of the system.

1.1 Screen Shots

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

1.2 Who is this manual intended for?

This manual is intended for administrators of the system.

1.3 How to Use this Manual

This manual is structured into chapters, topics and subtopics.

Important:

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

1.4 Prerequisites

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

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

2 Service Manager

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

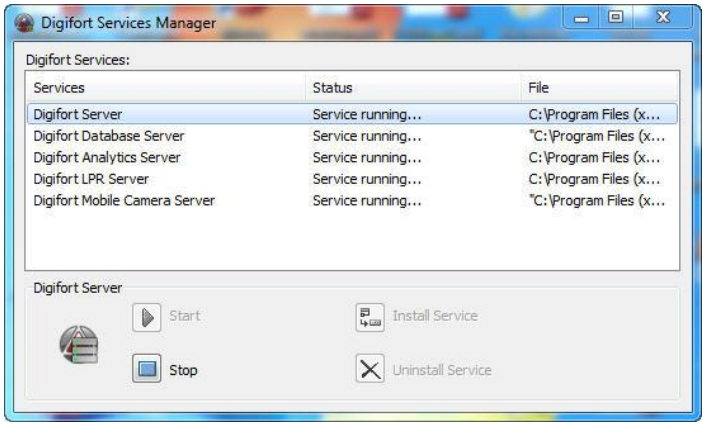
In the client-server platform, all information is stored on a central server responsible for its management. In the case of the Digifort System, the server is the component responsible for, among other functions, keeping the recordings generated by the images provided by the cameras, managing disk space,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

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

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

2.1 How To Run The Services Manager

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



The Service Manager provides the following functionality:

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

For the system to function, the following services must be in operation:
"**Digifort Server**" responsible for managing recordings and communicating with clients.
"**Digifort Database Server**" responsible for managing the system database.

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

© 2002 - 2024 by Digifort. All rights reserved.

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

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

2.2 How To Start Services

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

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

Note

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

2.3 How To Stop Services

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

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

3 Basic Features of the Administration Client

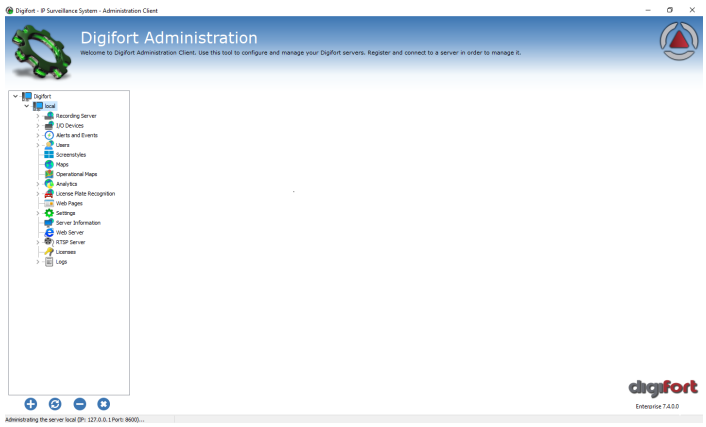
The Administration Client is the system module responsible for configuring the server. In this module you can, among other functions, register cameras, program alarms, check the server status and define the users who will have access to the system, among other administrative activities.

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

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

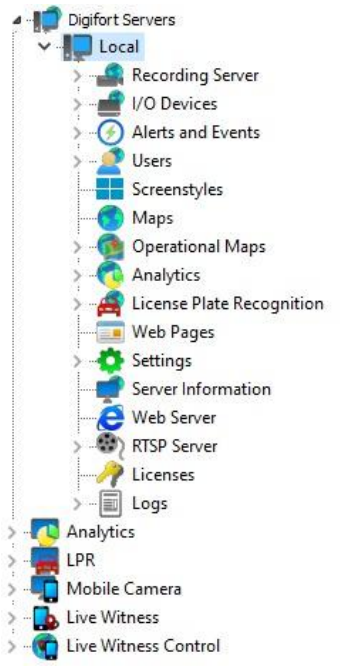
3.1 How to run the Administration Client

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



The Administration Client provides the following initial settings:

© 2002 - 2024 by Digifort. All rights reserved.



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

3.1.1 Interface

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

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

Delete Server: Deletes selected server.

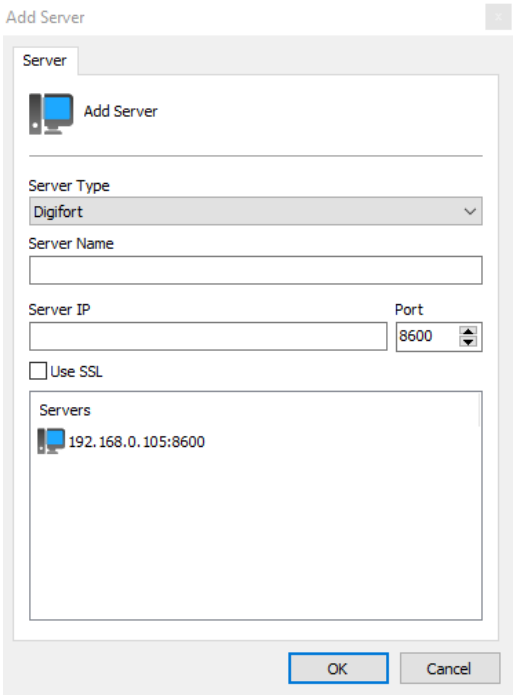
Disconnect from server: Terminates connection and management of the selected server. To disconnect from a server, select it in the Settings Menu and then click this button.

About: Displays system version information

3.2 How to Configure the Servers to be Managed

The first step to be carried out when configuring a server is to add it to the list of servers to be managed by the Administration Client.
To add a server, click on the **Add Server** button, opening the server registration screen, as shown below:

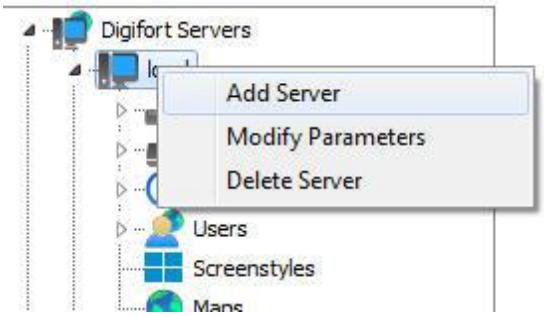
© 2002 - 2024 by Digifort. All rights reserved.



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

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

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



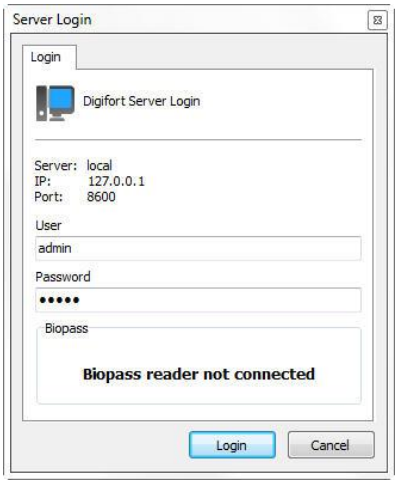
© 2002 - 2024 by Digifort. All rights reserved.

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

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

3.3 How to Connect to a Server for Management

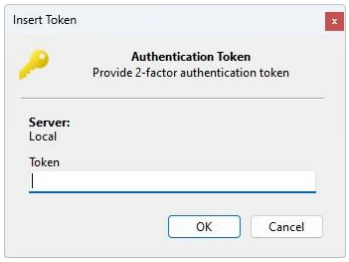
After adding the server, locate it in the Settings Menu and double-click on it or click on the arrow to the left of the server icon. Once this is done, a username and password will be required to access the server settings, as shown in the figure below:



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

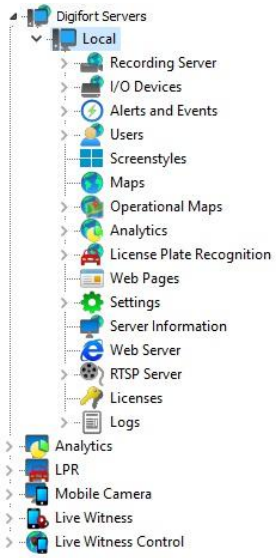
Enter the user name and password to access the server. If this is the first access to the system, inform the user equal to admin and a blank password.

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



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

© 2002 - 2024 by Digifort. All rights reserved.

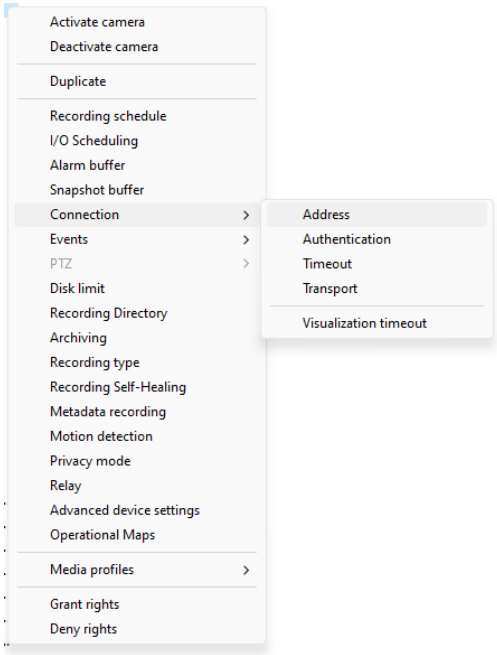


Note

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

3.4 Multiple Object Configuration

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



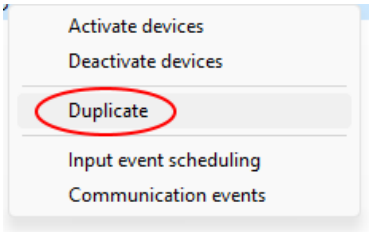
© 2002 - 2024 by Digifort. All rights reserved.

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

3.5 Duplicate Objects

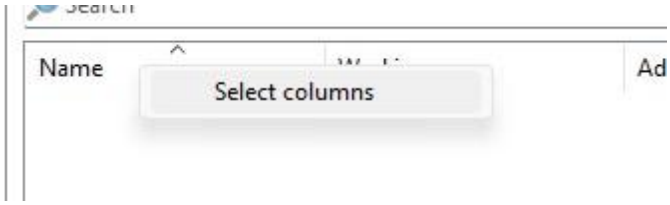
All of the system's main object registration screens allow duplication of objects, creating a new registration with the same information, just adding "-Copy" to the end of the name, allowing the creation of "templates" of already pre-configured objects and facilitating server administration.

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



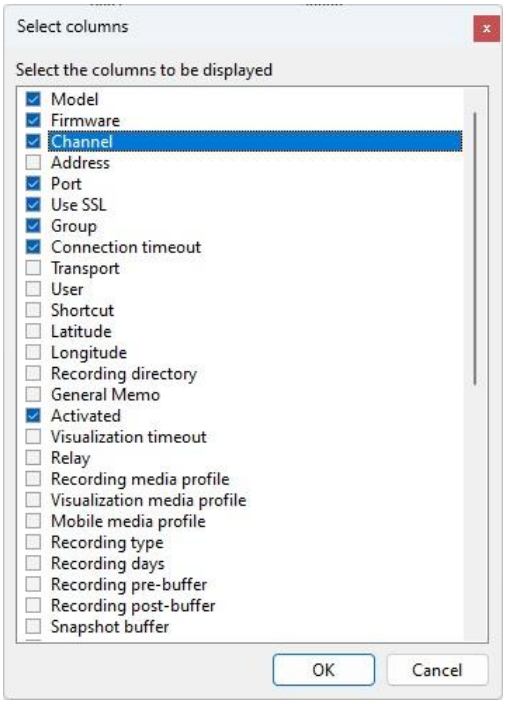
3.6 Extra Columns on Registration Screens

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



A screen with the available columns will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



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

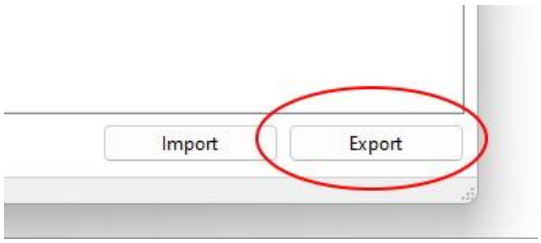
Port	Connection timeout	Use SSL	Recording Self-Healing	Metadata recording	Metadata type	Archiving days	Activated	Transport
8631	30000	Inactive	Inactive	Inactive		0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Inactive	Analytics	0	No	Auto
8601	30000	Inactive	Active (Failover Server)	Active	Motion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

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

You can sort the list by clicking on a column.

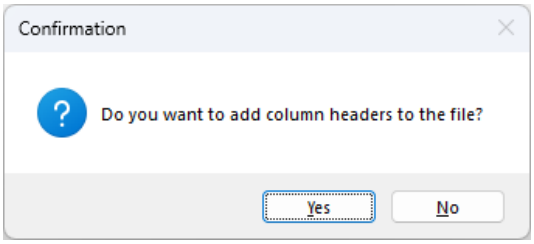
3.7 Export Data to CSV

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



© 2002 - 2024 by Digifort. All rights reserved.

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



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

Note

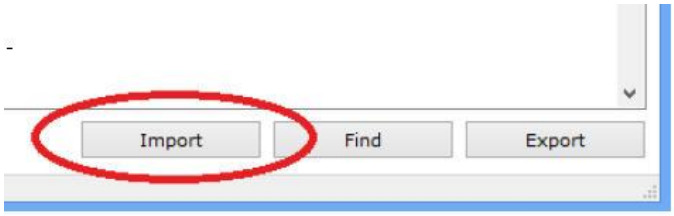
The exported data is informative only, contains only the information on screen and cannot be used to import the objects again on the same or another server. To import objects from another server, see the Object Import feature

3.8 Import Objects from Other Servers

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

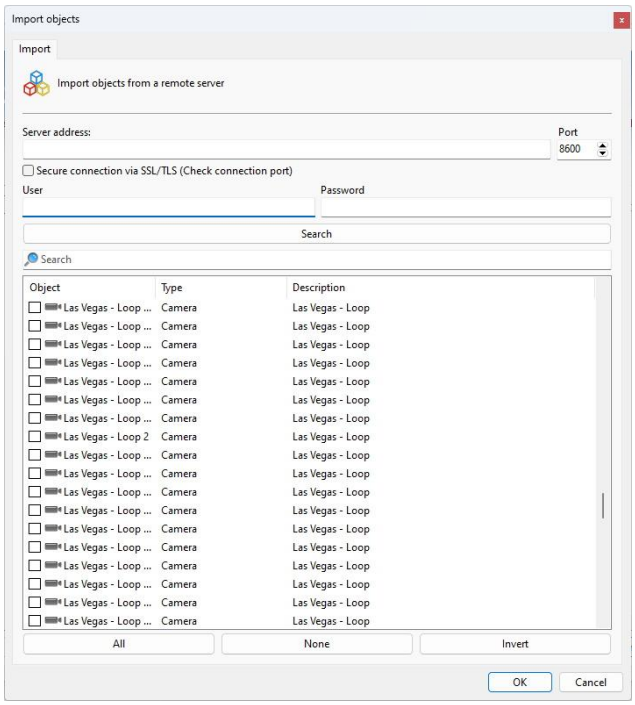
The system allows the import of any object such as Cameras, I/O Devices, Users, Analytics Settings, LPR, among others.

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



The object import screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



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

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

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

3.9 Shortcuts to Registration Lists

All system object lists have the following shortcuts:

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter IV

4 Licensing

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

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

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

There are two methods of licensing, online licensing and offline licensing.
Licensing carried out over the internet is the safest and recommended, but if your server cannot access the internet, use licensing through license files.

Tip

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

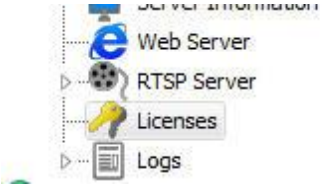
Important

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

4.1 How to Configure Licenses

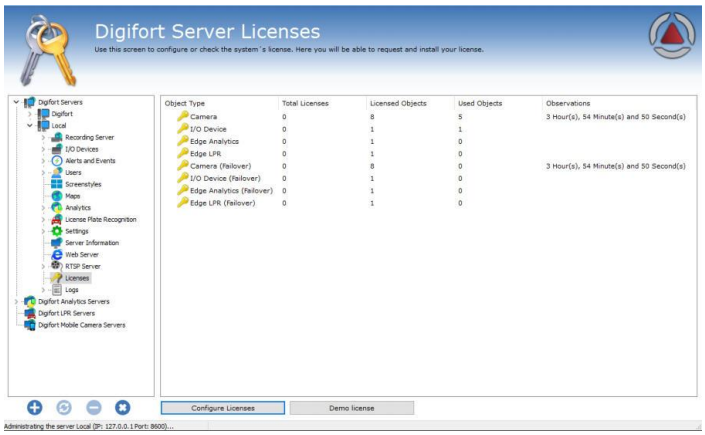
Before starting your server, make sure the HardKey (USB Dongle) that is sold together with the software is connected to your machine correctly.

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



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

© 2002 - 2024 by Digifort. All rights reserved.



From this screen we can get the following information:

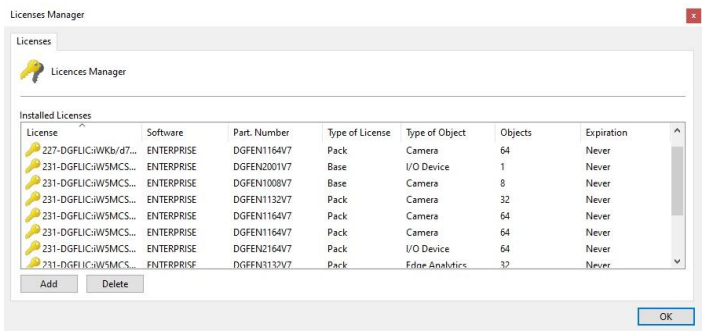
- **Total licenses:** Number of licenses installed on the server for a certain type of object.
- **Licensed objects:** Number of licensed objects for the object type.
- **Objects Used:** How many objects are currently using the licenses.
- **Observations:** Important license notes (If available) such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

License types:

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

To learn more about licensing, consult your reseller.

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



© 2002 - 2024 by Digifort. All rights reserved.

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

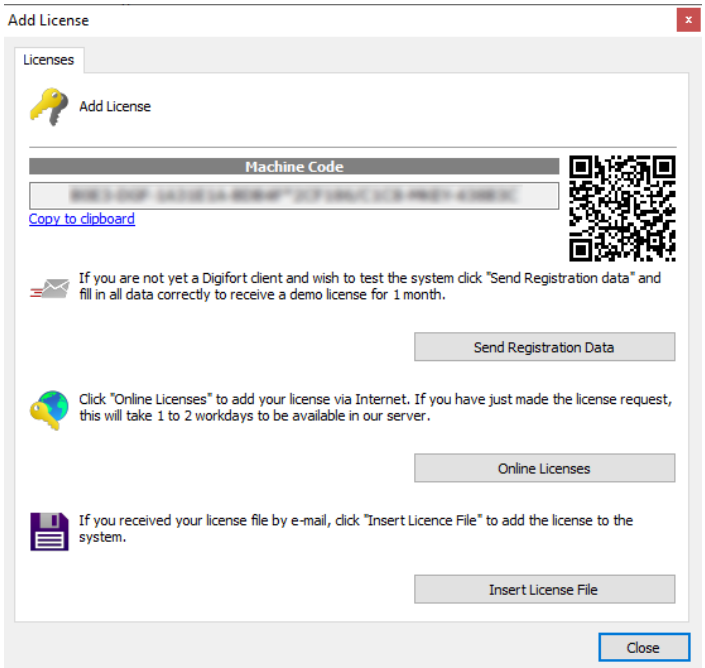
At the end of the settings, click on the **OK** button to close this screen.

Notes

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

4.1.1 How to add a License

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



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

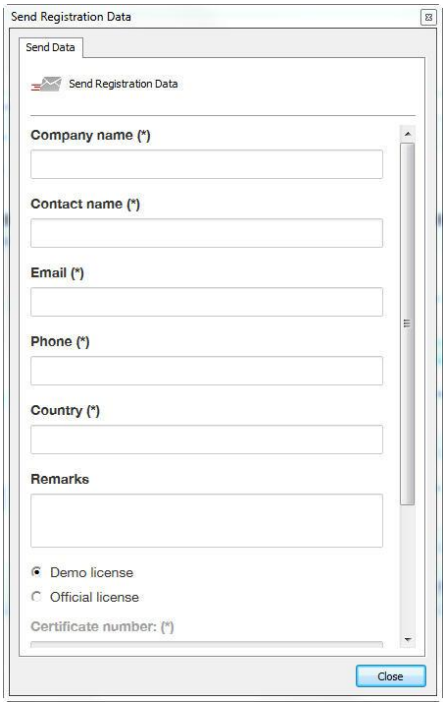
4.1.2 How to Send Registration Data

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

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

© 2002 - 2024 by Digifort. All rights reserved.

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



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

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

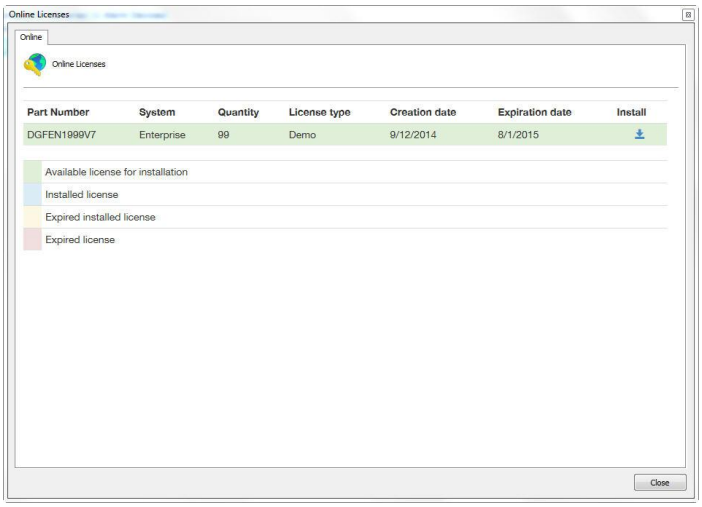
These instructions will also be described on the next pages of this manual.

4.1.3 How to install licenses through Online Licenses

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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

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

4.1.4 How to Install Licenses from License Files

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

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

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

Note

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

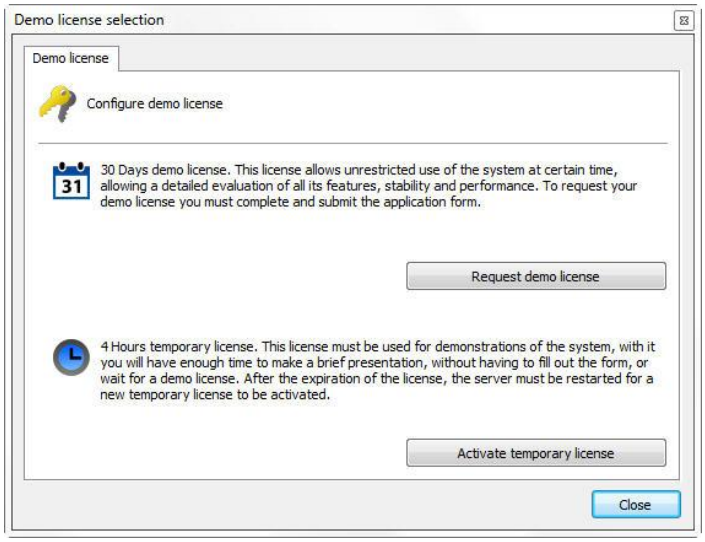
4.1.5 Activating a Temporary License

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

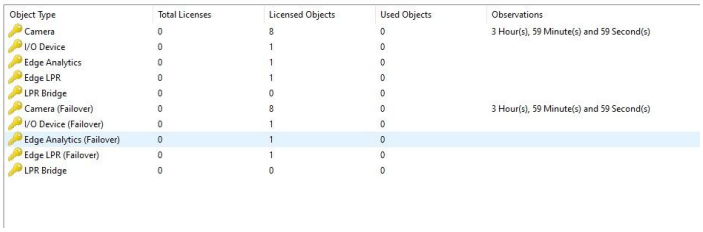
To activate the Temporary License, click on the **Demo License** button as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

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



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



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

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

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

And it's respective Failover Licenses.

Note

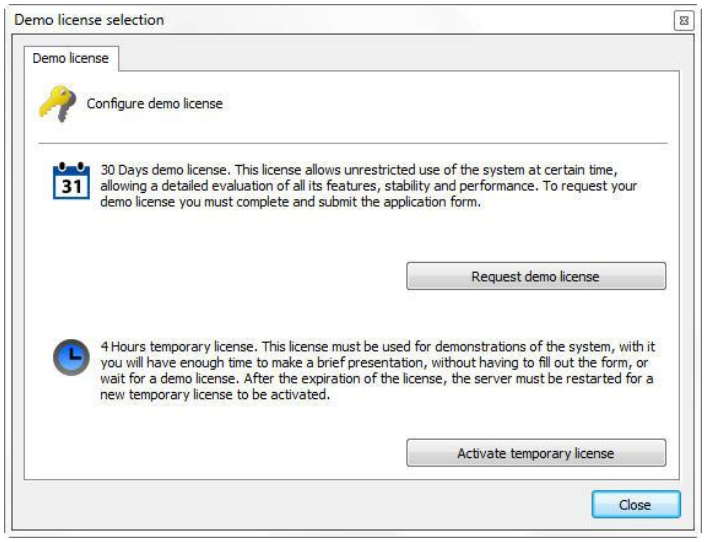
The temporary license is a free non feature-restricted license (only time-restricted), which means you can use an unlimited number of times. Once the period of 4 hours is expired, just simply stop the server service and start it again.

© 2002 - 2024 by Digifort. All rights reserved.

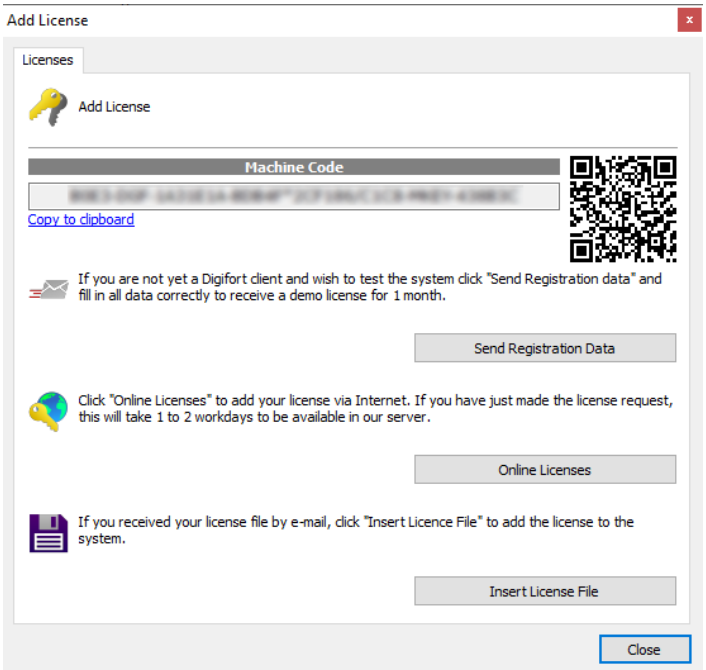
4.1.6 Requesting a Demo license

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

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



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



© 2002 - 2024 by Digifort. All rights reserved.

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter V

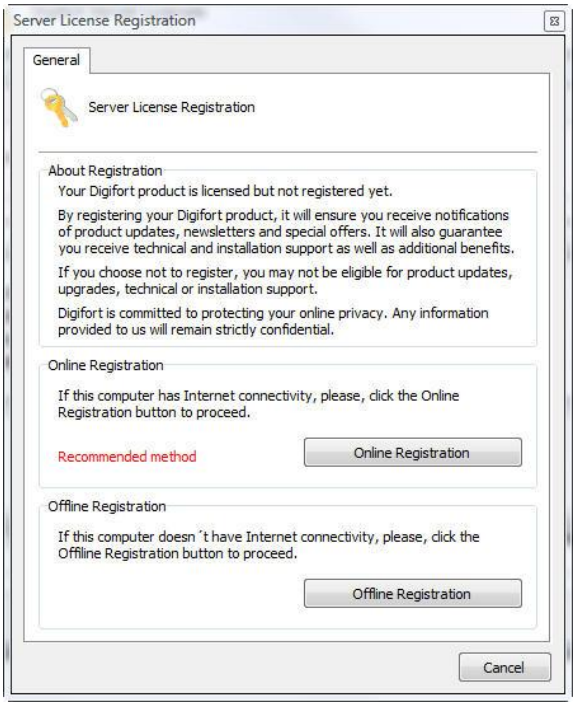
5 Registering the software

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

If you choose not to register, you may not be eligible for updates, upgrades, technical or installation support.
By registering the software, you will receive a registration code that, for security purposes, will also be stored in our licensing center. If you use a hard key and it is necessary to format the server or reinstall the server, our licensing center will identify your server and automatically register it again.

5.1 How to register the software

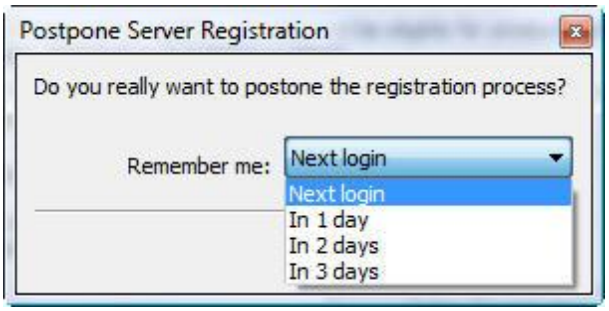
After inserting your official software license, the software registration window will be automatically displayed, as shown in the figure below. To learn how to install licenses, see Licensing



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

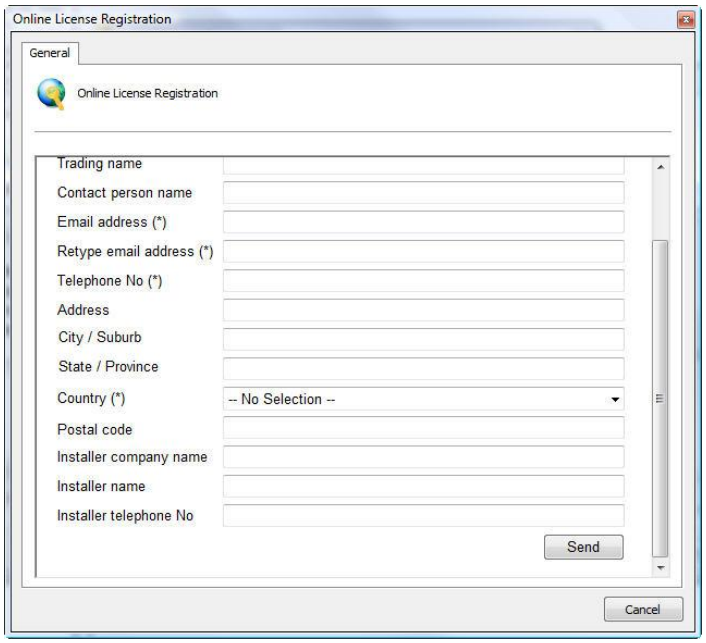
If you want to register later, close this window and select the desired option, as shown in the image below:

© 2002 - 2024 by Digifort. All rights reserved.



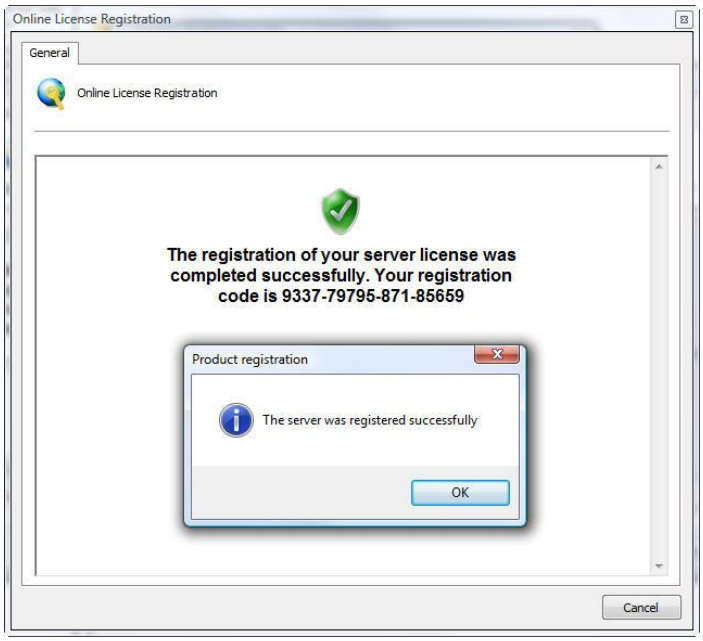
5.2 Registering the software Online

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



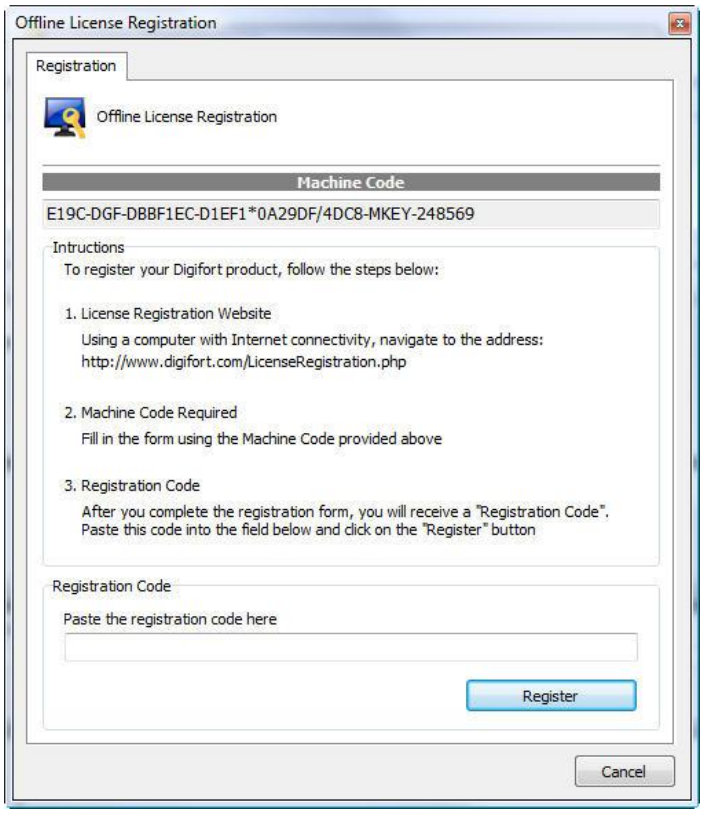
Fill in all fields and click Submit. The registration confirmation screen will be displayed along with your registration code, as shown in the figure below.

© 2002 - 2024 by Digifort. All rights reserved.



5.3 Registering the software Offline

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



© 2002 - 2024 by Digifort. All rights reserved.

Chapter VI

6 Recording Server

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

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

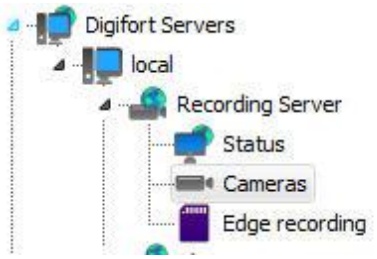
The system operates with the main brands of digital cameras on the market and accepts analog cameras as long as they are connected through the video-server device. These cameras can be located on the same site as the server or they can be remote, connected through some network connection. The main camera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

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

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

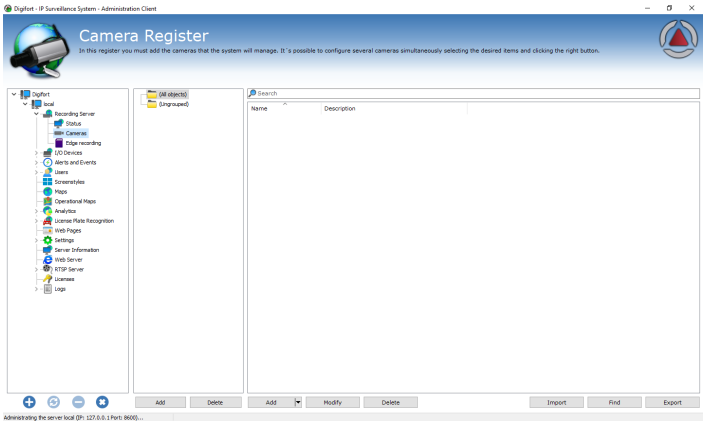
6.1 How to Add a Camera

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



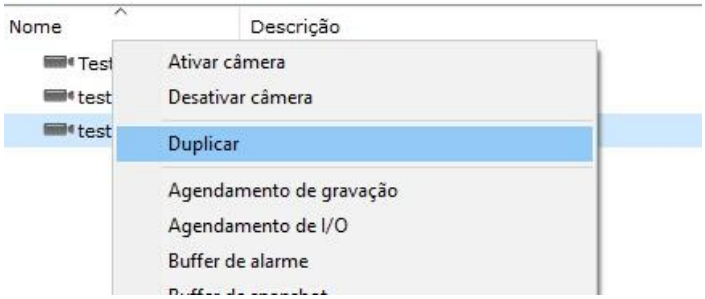
Once this is done, the registration of cameras will be executed, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



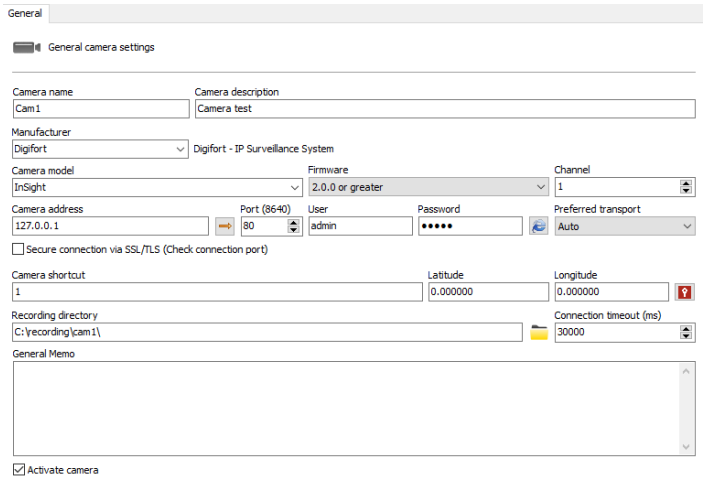
To add a camera, click **Add**. To change or remove a camera, select the desired camera and click on the corresponding button.

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



6.1.1 Camera

6.1.1.1 General



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

© 2002 - 2024 by Digifort. All rights reserved.

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

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

- **Preferred Transport:** Select the preferred transport method among Auto, UDP and TCP.
  - **Auto** - Transport used will generally be TCP, unless during device integration performance was not satisfactory, then transport will be done via UDP
  - **TCP** - Transport will be done by TCP when possible
  - **UDP** - Transport will be done via UDP when possible

➢ This option is a transport preference and not mandatory, that is, even if you specifically configure TCP or UDP, the system will not necessarily follow the configuration, as the device's media driver must support the desired protocol.

- **Connection via SSL/TLS:** If the camera has support to secure connection, check the box to activate the SSL communication method between the camera and the Server, it is important to check the port for such communication. If the camera does not have the feature, this option will appear as inaccessible.
- **Camera shortcut:** Type a shortcut for the camera so that in the Surveillance Client this camera can be quickly shown on the screen through this shortcut.
- **Latitude and Longitude:** Both options are used to mark the positioning of a camera on a map, this feature serves several purposes, such as tracing vehicle routes using an LPR server (for more information about the feature, check the Surveillance Client User Manual).
- **Connection timeout (in ms):** This parameter is used by the system when the connection with the camera is lost in some way. The server will attempt to re-establish the connection after the configured time. To convert this value to seconds, simply divide the value by 1000. By default, this parameter is set to 30000ms (30 seconds).
- **Directory for recording:** The system makes it possible to record cameras distributed on several disks, for that, select the directory for recording images of the camera to be inserted. It is possible to record on network drives, that is, on disks of other computers on the network. To learn how to use this feature see Network Units.
- **General Notes:** If necessary, use the field to add additional information about the camera.
- **Activate Camera:** Indicates whether the system should activate this camera

© 2002 - 2024 by Digifort. All rights reserved.

Note

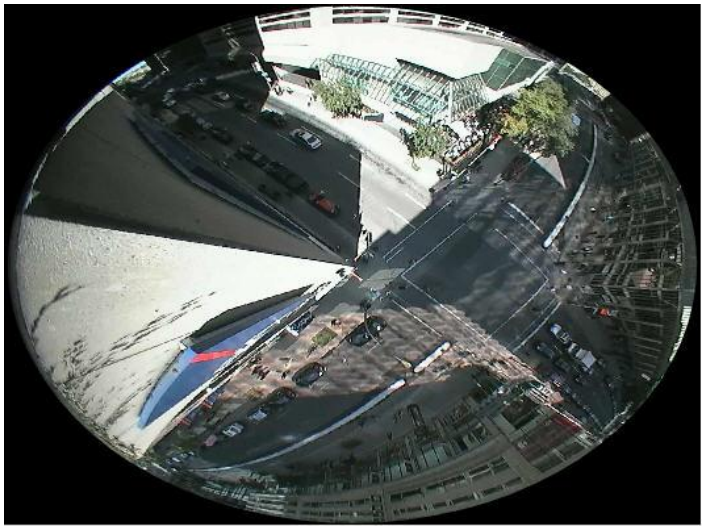
The server is responsible for managing the structure of directories used for camera recording, therefore, no file in its database must be manually deleted, and the camera recording directory cannot be created by methods external to the server, such as For example, Windows Explorer.

6.1.1.2 Lenses

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

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

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



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

© 2002 - 2024 by Digifort. All rights reserved.

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

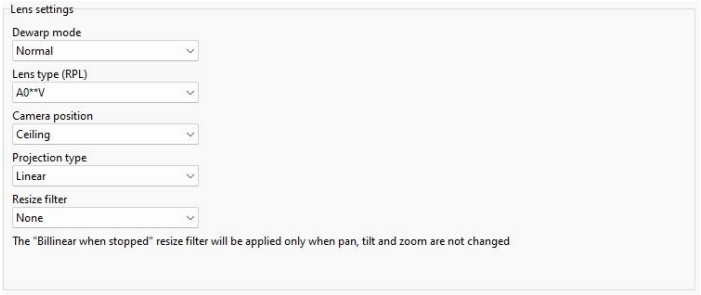
To learn how to use this feature live, see the Surveillance Client manual.

See the Administration Client settings in the screen below**:**

Lens used: Select the type of lens to be used

6.1.1.2.1 Panomorph Lenses

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



- **Dewarp Mode**: Select dewarp mode for higher quality or higher rendering performance
- **Lens type:** Select the panomorph lens type
- **Camera position:** Select the position where the camera is installed. Wall, Ceiling, Ground.
- **Projection Type:** Scene projection type
- **Resize Filter:** The resizing filter may improve image quality, but reduce performance:

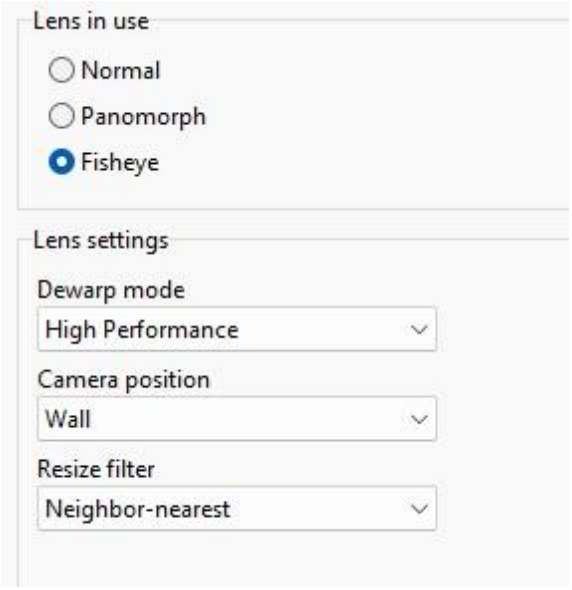
© 2002 - 2024 by Digifort. All rights reserved.

- **None:** No resizing filter (Best performance)
- **Bilinear:** Bilinear resizing for greater visual quality
- **Bilinear when stopped:** Bilinear resize filter will be applied only when camera is still (During PTZ it will be disabled)

6.1.1.2.2 Fisheye Lenses

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

Fisheye lens setup example:



Nota

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

6.1.1.3 Motion Detection

6.1.1.3.1 Use Motion Detection by Softw are

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

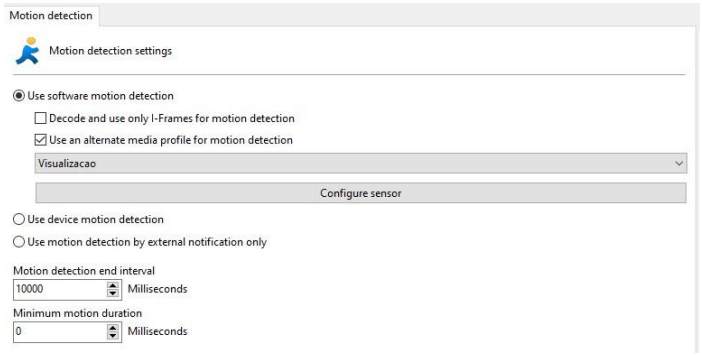
We must bear in mind that motion detection via software will always increase the processing of the image recording server. This happens because for each camera in which motion detection is activated, the server has to decode an entire chain of frames and from this chain only 2 frames are compared. An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

To reduce processing on the server, an option was developed that allows performing motion detection on a lower resolution media profile. In this way, images can be recorded in high resolution and motion

© 2002 - 2024 by Digifort. All rights reserved.

detection in low resolution. The lower the resolution used for motion detection, the less processing used. It is recommended to get good detection at minimum CIF resolution. As for the frames per second, only 3 frames per second are recommended, because in a sequence of 30 frames only 2 frames would be analyzed.

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



To learn how to create media profiles see the chapter Media Profiles

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

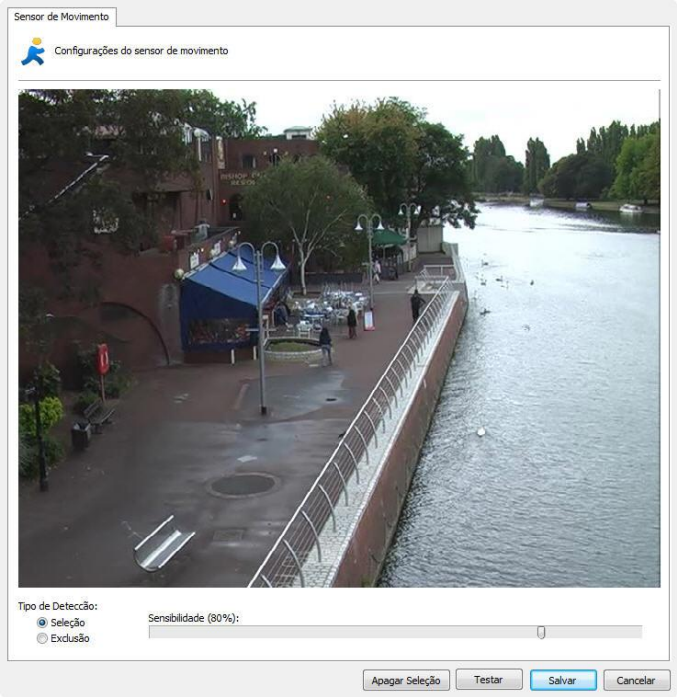
The **Motion Sensor** consists of a tool that allows the user to define areas of the image that will be sensitive or not sensitive to movement.

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

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

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

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.

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

6.1.1.3.1.1 Auto disable motion detection during PTZ

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

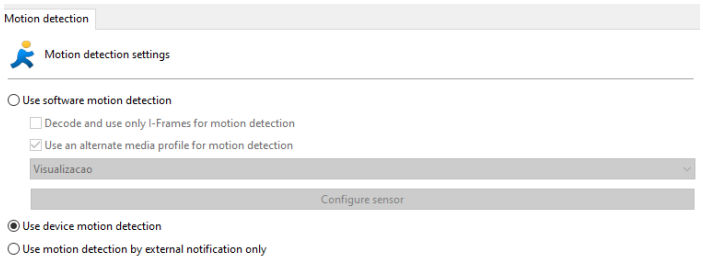
© 2002 - 2024 by Digifort. All rights reserved.

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

6.1.1.3.2 Use motion detection by device

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

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



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

Note

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

6.1.1.3.3 Use motion detection by external notification

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

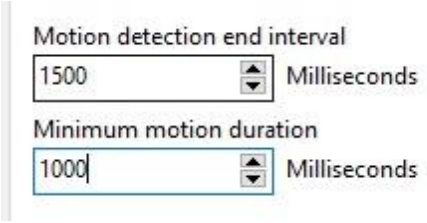
If your device has not been integrated with support for motion detection, you can use this option that allows motion notification through the server's HTTP API.

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

6.1.1.3.4 End detection interval and motion duration

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

© 2002 - 2024 by Digifort. All rights reserved.



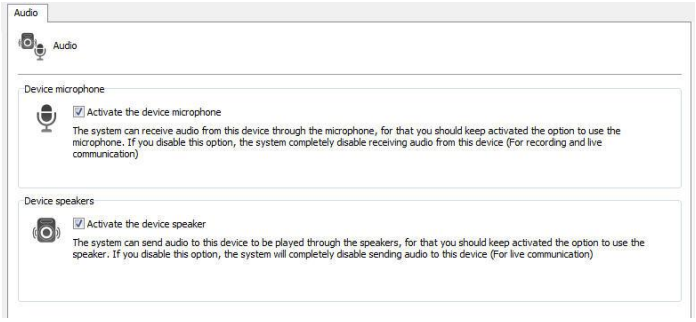
- **Motion Detection End Interval:** Configure the time that the system will continue to consider that the camera has motion, even after the motion ends. This is an important system fine-tuning option, especially if the **motion detection via device** option is selected, as the camera does not send frequent continuous notification of motion detection, there is a time interval between notifications, which can cause so that the system understands that the camera is no longer detecting movement, even though it is detecting movement. The default value of 1500 milliseconds is optimized for software detection.

- **Minimum Motion Duration:** This value is used to determine the start of motion detection. For the system to consider that movement has occurred in the camera, there must be uninterrupted movement for at least X milliseconds, thus preventing image artifacts from triggering the motion sensor, reducing false alarms.

6.1.1.4 Audio

The system allows the use of a camera's audio features.
You can listen and record the audio that the camera's microphone picks up or send the audio to your speakers.

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



On the screen above the following features are available:

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

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

© 2002 - 2024 by Digifort. All rights reserved.

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

6.1.1.5 Image Filters

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

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

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

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

6.1.2 Streaming

6.1.2.1 Media Profiles

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

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

© 2002 - 2024 by Digifort. All rights reserved.

define that we want to visualize the camera at ten frames per second with a resolution of 640x480 and low image compression.

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

- **Video Compression:** Video compression to be used when recording the images on disk. The system currently supports **Motion JPEG**, **MPEG4, MxPEG, H263**, **H264** and **H265** formats.
- **Image resolution**: Image resolution that will be used in the profile. When selecting the camera model, this list of resolutions automatically starts showing only the resolutions supported by the camera. A very high image resolution will consume a lot of disk space and network bandwidth, but the image will have a higher quality where it is possible to recognize more details in the image, such as a person's face. A very small image resolution will consume little disk space and network bandwidth, but the image will have a lower quality, providing little detail. This parameter must be configured as needed. The system has a disk space consumption calculator that will help you better configure image resolution and frames per second. To learn how to use system calculator, see Disk Space Usage Calculator
- **Image quality:** The images coming from the cameras go through a compression process. The higher the image compression level, the less quality this image will have, and the lower the image compression level, the more quality.
- **Frames per second:** Frames per second to be recorded. A higher frames per second rate will consume more network bandwidth and disk space, but will give smoother motion. A lower rate of frames per second will consume little network bandwidth and disk space, but the movement will be more robotic. It is proven that from three to seven frames per second it is already possible to recognize all the movements of a person. In some cases, the camera may not be able to send the configured amount of frames per second, especially with high frame rates per second. This is due to several factors such as internal network malfunction, number of connections made to the camera and camera processing power.

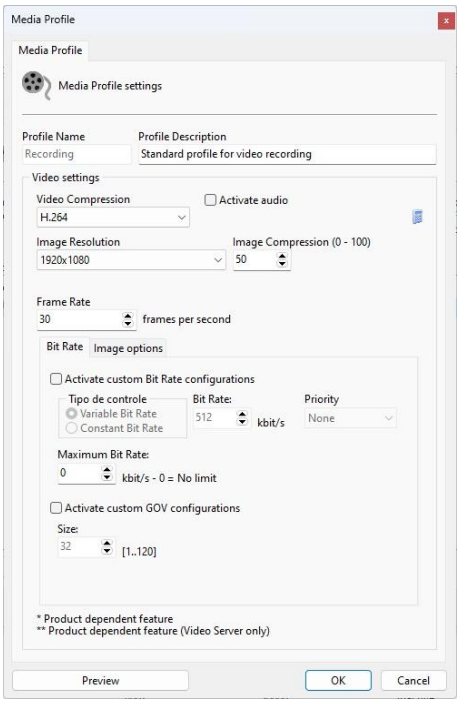
Some specific parameters of each equipment, among others, we can exemplify the insertion of texts in the image, image rotation, color levels, etc.

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

6.1.2.1.1 How to add Media Profiles

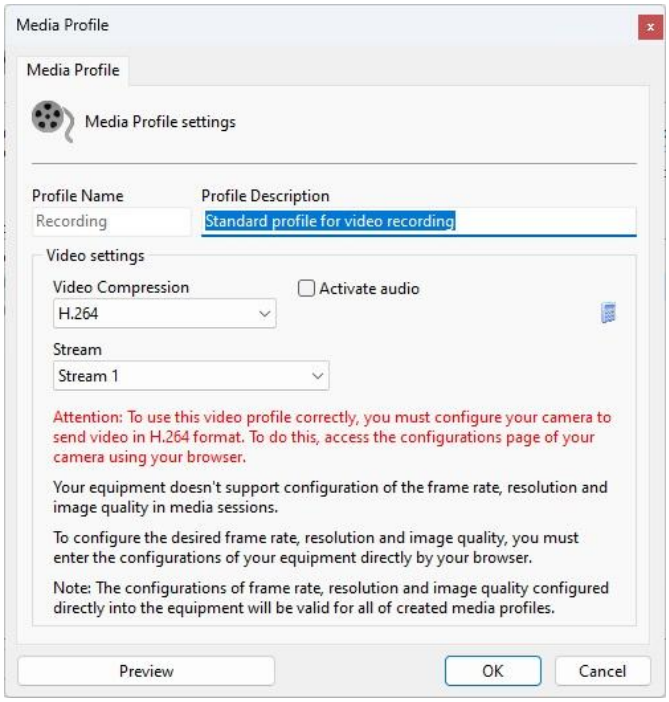
To add a media profile, click **Add**, and the media profile addition screen will be executed as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



It is important to note that this screen may vary from camera to camera, as each one has its own set of configuration parameters.
In the example above, the selected camera supports different types of settings such as Resolution, Compression, Frame Rate, among others.

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



© 2002 - 2024 by Digifort. All rights reserved.

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

6.1.2.1.2 How to view the functioning of the configured media profile

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

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

This screen also contains the following information:

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

Note

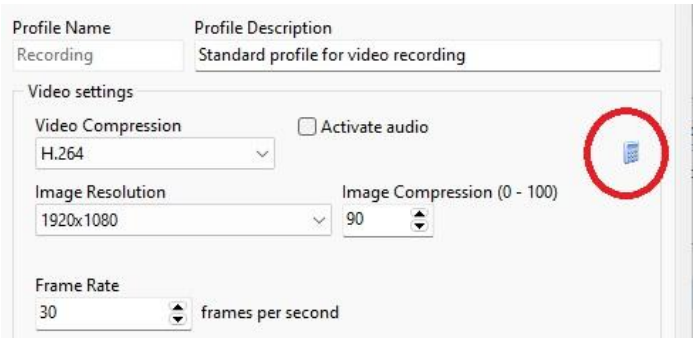
All information contained in the image is updated every second.

6.1.2.1.3 Disk space usage calculator

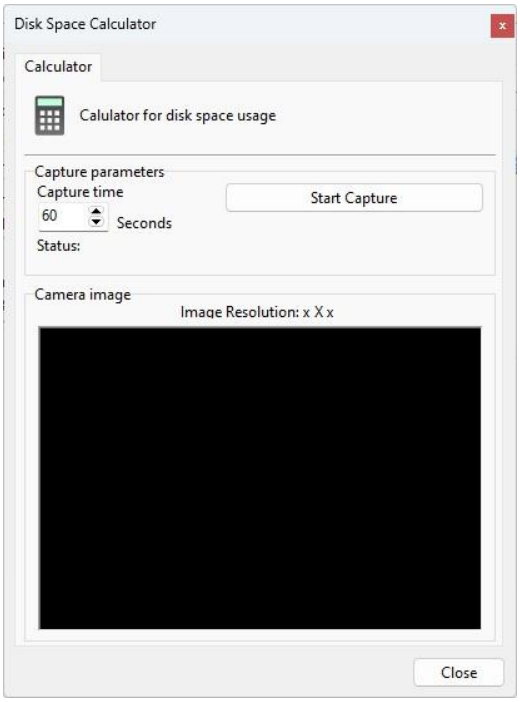
The system has a very useful tool to help dimensioning the disk space to be reserved for each camera, which is the disk space usage calculator. To access this feature, click on the button identified by a “calculator” on the media profiles configuration screen, as shown in the figure below:

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

© 2002 - 2024 by Digifort. All rights reserved.



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



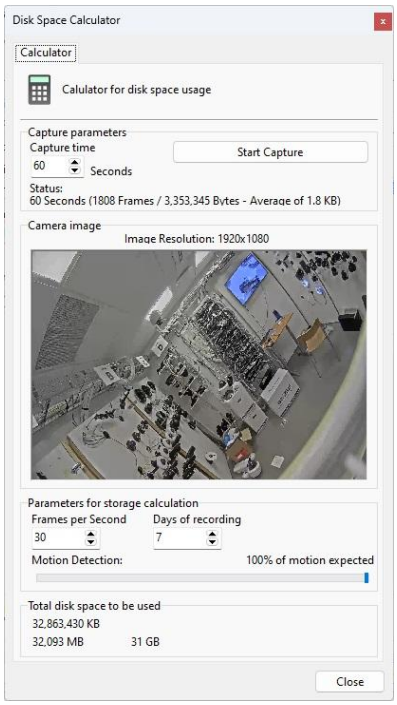
To calculate the disk space required for camera recording, the calculator captures an original temporary video from the camera with the image quality and resolution parameters, configured in the media profile being edited, and the capture time, entered on this screen. Based on the received video, a calculation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

For compressions such as **MPEG-4, MxPEG, H.263, H.264 and H.265** the recommended capture time is **60 seconds**.
For **Motion JPEG**, the recommended capture time is **5 seconds**.

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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

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

Important

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

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

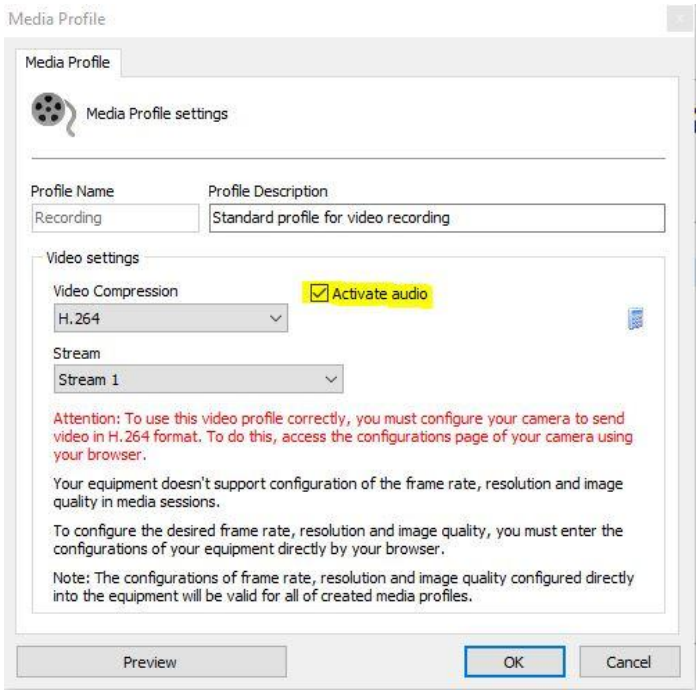
- **Recording days:** Enter the number of days to be stored for this camera. The higher this value, the more disk space used.
- **Frames per second:** Enter the number of frames per second to be used by the camera recording.
- **Motion Detection:** Enter the percentage of movement expected at the camera's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

© 2002 - 2024 by Digifort. All rights reserved.

6.1.2.1.4 Audio

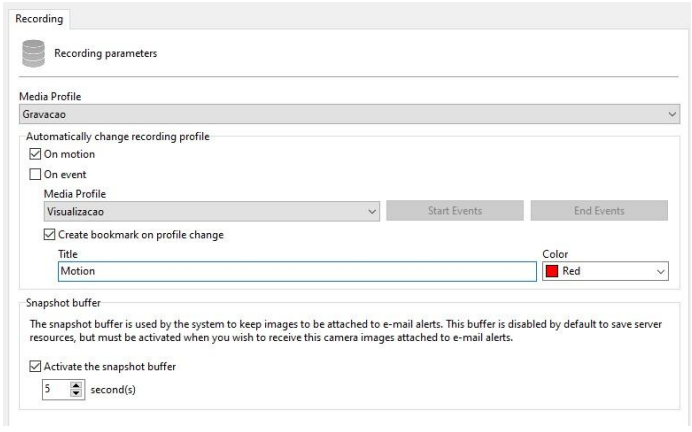
If your camera supports audio, you can select the "Activate audio" option so that the system requests audio for the desired profile.

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



6.1.2.2 Recording

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

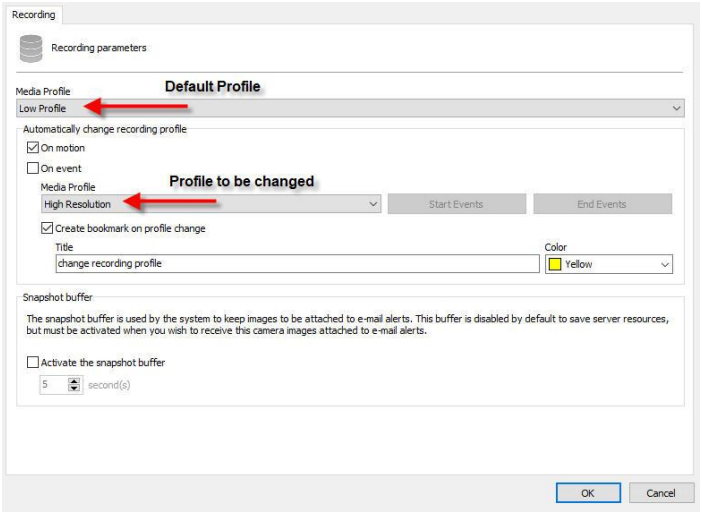


- **Media Profile:** Choose the default media profile that will be used by the software to record images.

© 2002 - 2024 by Digifort. All rights reserved.

6.1.2.2.1 Automatic Recording Profile Switching

Using the multi-streaming system, the recording profile can be changed dynamically upon motion or by event, which allows the system to be configured to record continuously with a standard profile and when there is motion or event the profile will be automatically changed to another profile (For example, with higher resolution and frame rate). This configuration allows greater flexibility for those who want to save on image storage.



To configure profile switching for movement, select the **On Motion** option and select the profile that the system should record during movement.

To configure profile switching per event, select the **On Event** option, select the profile that the system will record during the event and select the start and end events. When a start event is triggered, the system will switch the recording to the selected profile and when an end event is triggered, the system will return the recording to the default recording profile.

It is possible to select any event available in system (I/O, Global Events, Analytics, etc.) for the profile switch.

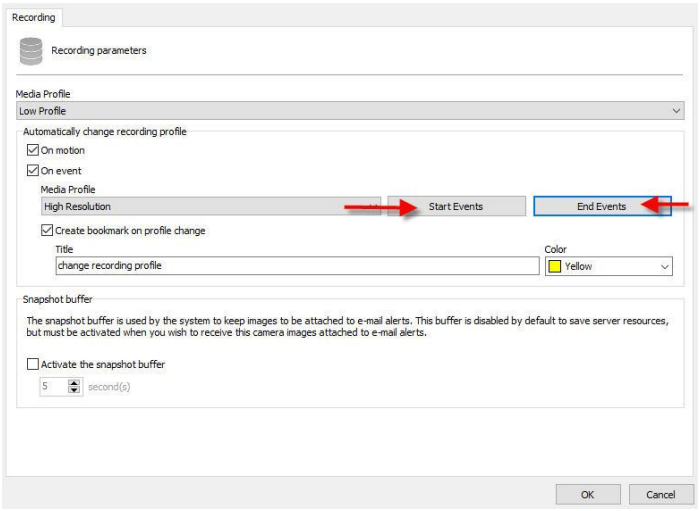
Important

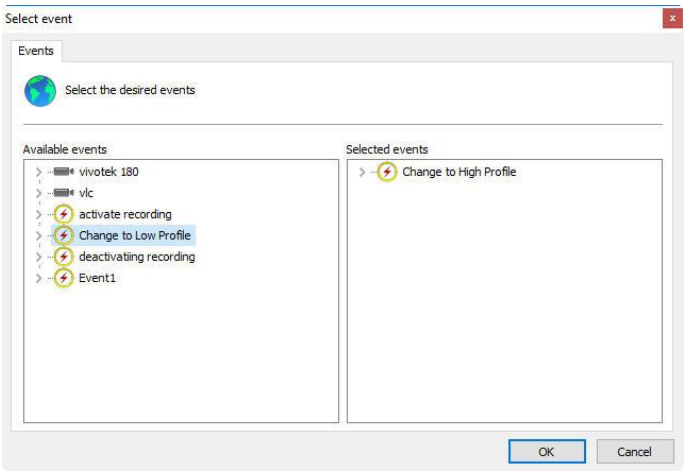
You should always choose start and end events. If an end event is not selected, the system may constantly record with the event profile and never return recording to the default profile.

Tip

If you are using an event that does not have an end (For example, a global event), you can create a timer in the actions of this event (Which will fire X seconds after the event has been triggered) and use this timer as an end event

© 2002 - 2024 by Digifort. All rights reserved.



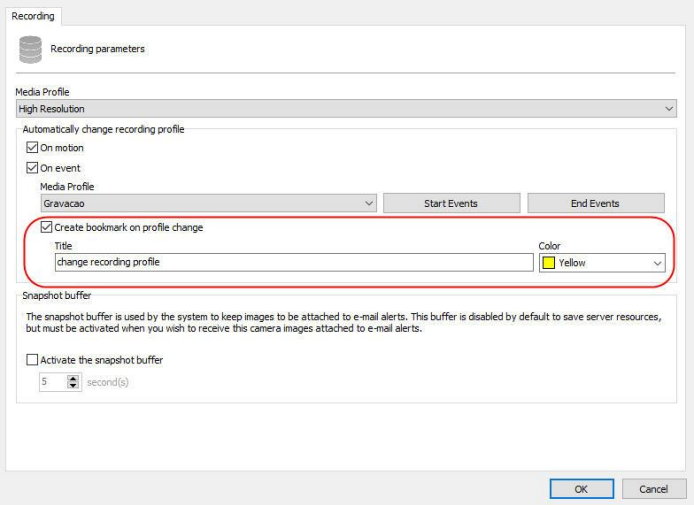


6.1.2.2.1.1 Create Bookmark on Profile Switching

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

Every time the system changes the profile, there will be a Bookmark on the recording, making it easier to search for events.

© 2002 - 2024 by Digifort. All rights reserved.



To activate this function, click **Create bookmark when changing profile**.

Choose a title for the Bookmark and a color.

6.1.2.2.2 Snapshot Buffer

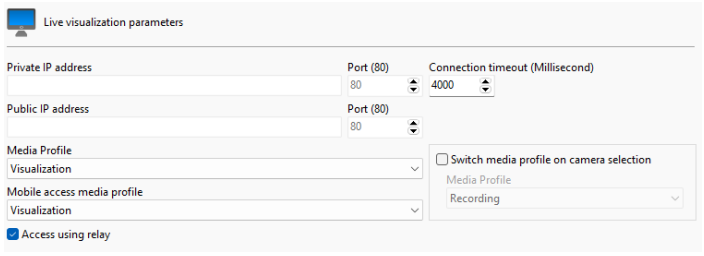
The Image Buffer is used when you want to send still images from the cameras via email or popup when an alarm occurs.
In case your edition supports the map feature, the system can display the image preview in the camera status on the map (See the Surveillance Client manual).

By default this option is disabled to save server resources.

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

6.1.2.3 Live View

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



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

The parameters to be configured are described below.

© 2002 - 2024 by Digifort. All rights reserved.

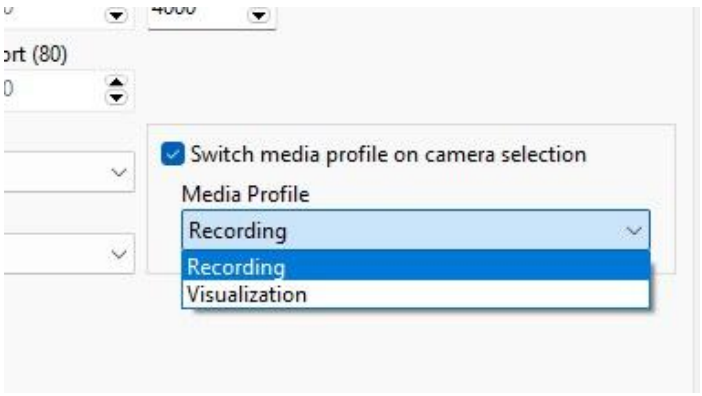
- **Access via Relay:** When using this option (Selected by default), the client will receive images from the cameras through the system server instead of connecting directly to the camera. This is the recommended connection method as it allows greater security of the solution (As the cameras can be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

6.1.2.3.1 Switch media profile on camera selection

The system has the option of switching between media profiles for live view in your Surveillance Client with one click.

This option serves to optimize processing in your Client, enabling, for example, the use of a lower resolution media profile for standard mosaic viewing (With multiple cameras on screen) and a high definition profile that can be accessed through the camera selection in the Client (by clicking on the image) when the user wants to see more details of the image.

To activate this option, select "Change profile on camera selection", and select the media profile you want to be displayed when the camera is selected in the Client.

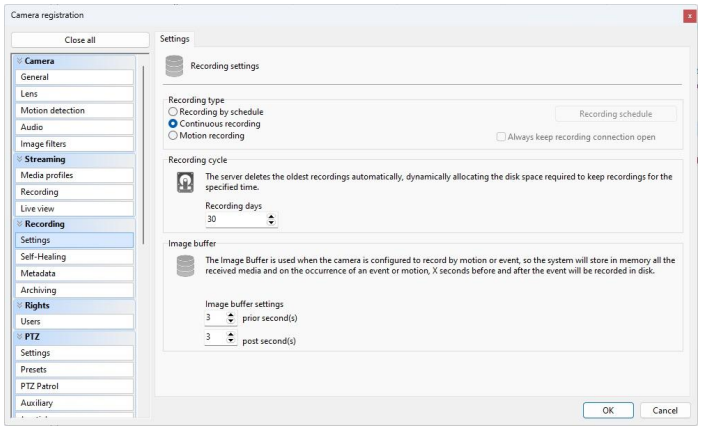


© 2002 - 2024 by Digifort. All rights reserved.

6.1.3 Recording

6.1.3.1 Settings

On this screen you can configure the recording options:



6.1.3.1.1 Recording Type

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

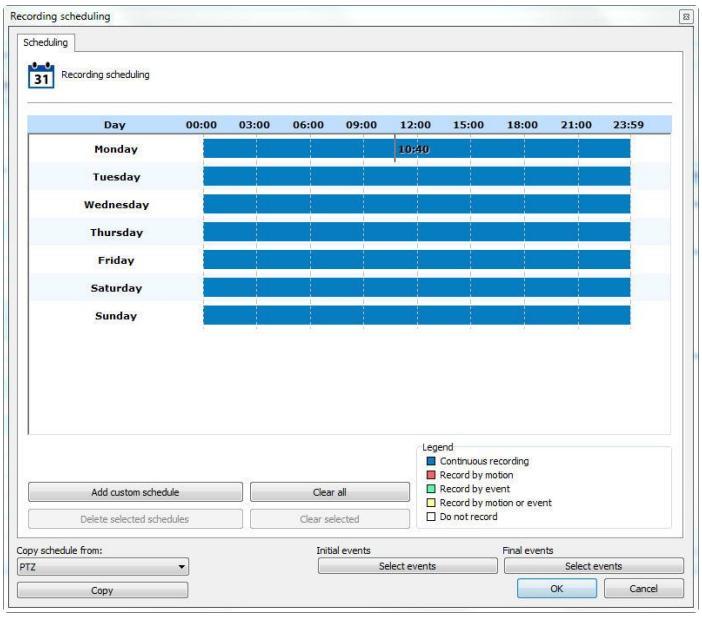
- **Always keep recording connection open:** Keep the camera recording stream always streaming in case of event recording. This way the recording pre-buffer will work normally. This option is also required to send audio to cameras via the Monitoring Client or through the send audio to cameras event action.

6.1.3.1.1.1 How to configure the recording schedule

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

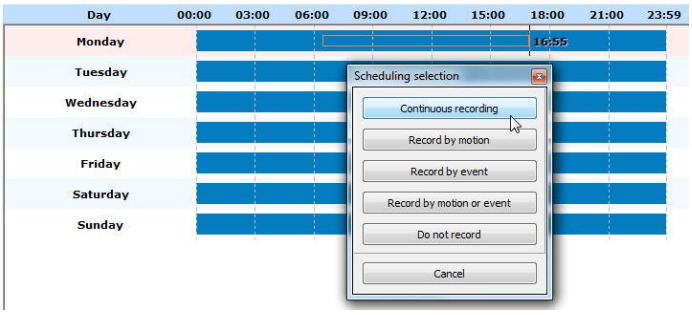
The scheduling screen below will open:

© 2002 - 2024 by Digifort. All rights reserved.



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

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

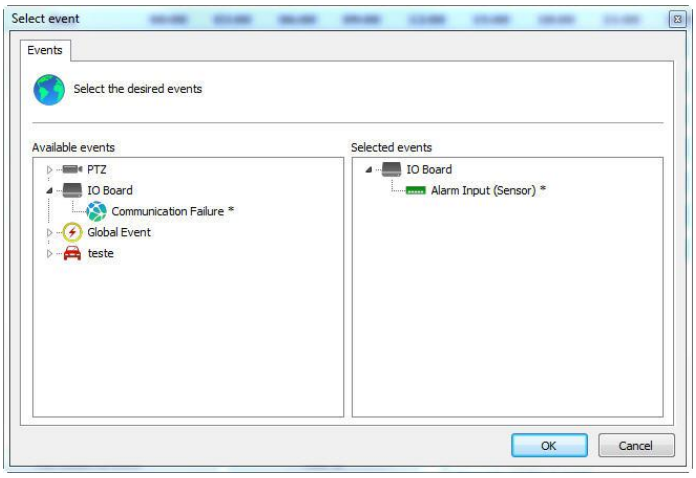


You can select multiple days to apply a setting to all at the same time Just click on the desired days of the week.
In the figure below, the first three were selected:

© 2002 - 2024 by Digifort. All rights reserved.

Scheduling options are:

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



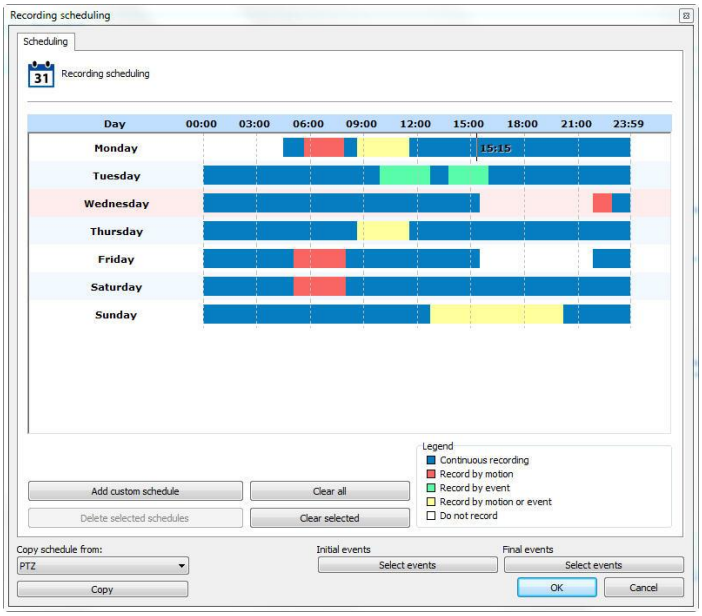
This screen presents two lists, the list of available events and the list of selected events.

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

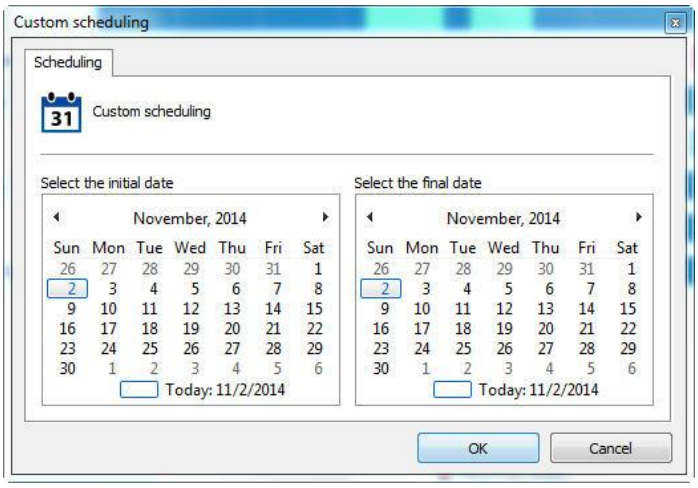
© 2002 - 2024 by Digifort. All rights reserved.

The events that have the "*" symbol next to them are the events that will actually occur, that is, suppose we have chained timer events, in this case it is not all the events that will occur, but the one with the symbol " *" next to. Timer events are events that occur at a certain user-defined time to trigger another event. To learn about timer events see Timer Events.
To select an event, select it from the list of available events and drag it to the list of selected events. To remove an event, follow the same process in reverse.

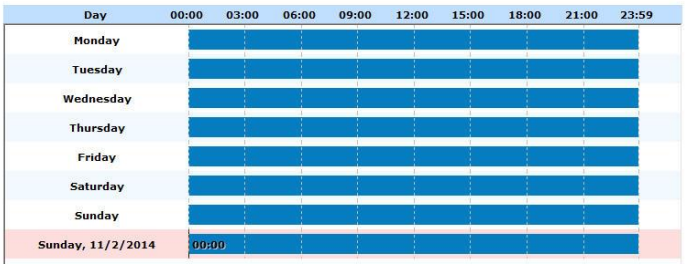
In the image below, we have different types of appointments on different days:



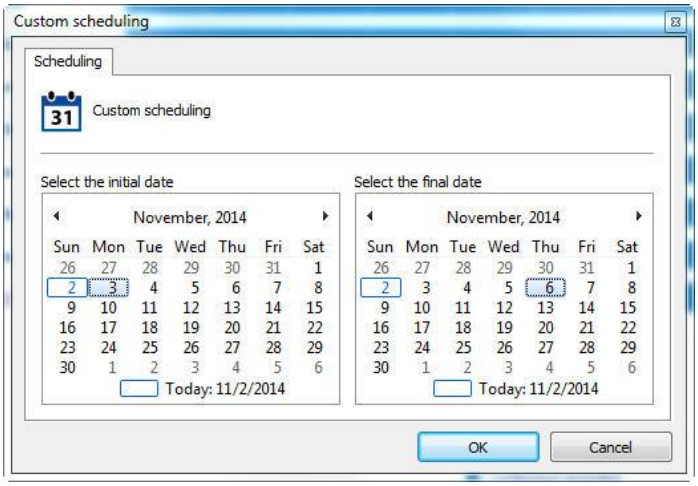
The scheduling screen allows scheduling to be made for a specific day of the year, such as a holiday or a special event.
To add a custom schedule, click the Add custom schedule button.
It is possible to choose a single day as shown in the images below:

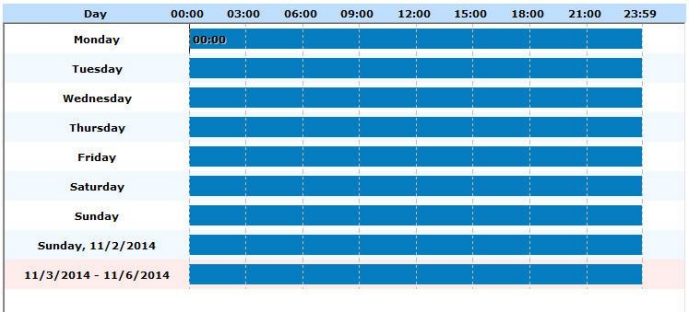


© 2002 - 2024 by Digifort. All rights reserved.



Or add a range:



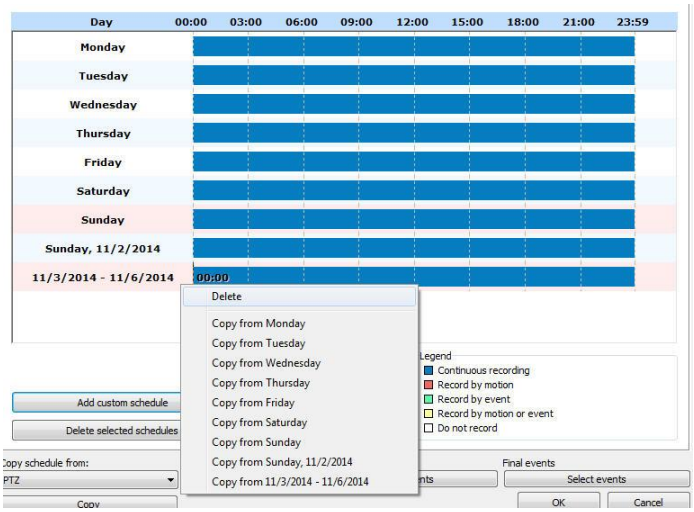


Note

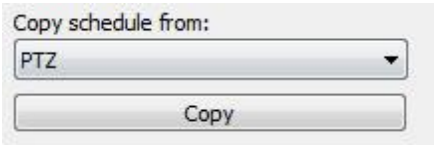
Custom schedules will have priority over regular schedules. For example: In a custom schedule that is scheduled on a Monday, it will override the settings already made for Monday on that specific day.

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

© 2002 - 2024 by Digifort. All rights reserved.



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



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

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

6.1.3.1.2 Recording Cycle

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

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

6.1.3.1.3 Image Buffer

The Image Buffer is used when the camera is configured to record by motion detection or event, so the system will store the received images in memory, and in the event of a movement or event, X seconds before and after the movement/event will also be recorded on disk.

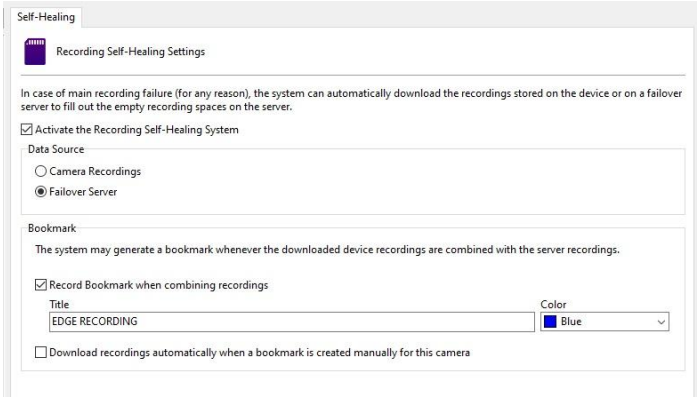
By default, the initial value for this setting is three seconds before and three seconds after. The greater the number of seconds configured, the greater the memory used by the server to store the images.

6.1.3.2 Self-Healing

Self-Healing allows that in cases of loss of connection with the camera, the server can download the image recorded in the camera's SD / HD and then merge the downloaded images with the main recording.

To enable Self-Healing, click **Activate the Recording Self-Healing System**

© 2002 - 2024 by Digifort. All rights reserved.

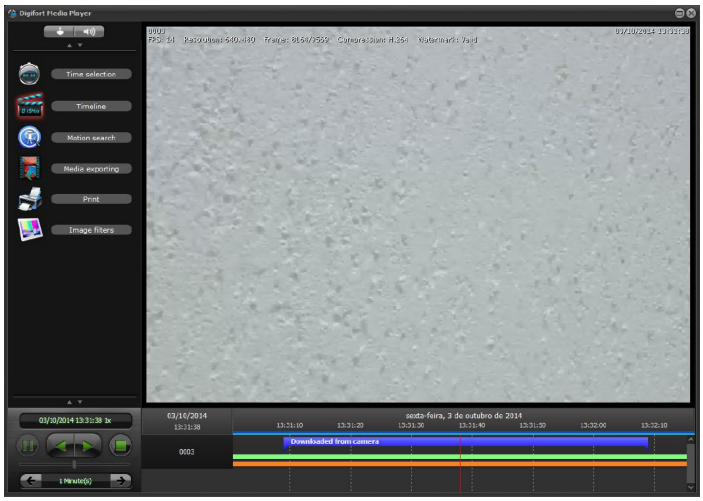


The system allows downloading recordings from the camera's SD/HD or a failover server

- **Camera Recordings:** Select this option to configure the system to download recordings directly from the camera's SD Card/HD in case of connection or environmental failure.
- **Failover Server:** Select this option to configure the system to download recordings from a Failover Server. In this mode, if the main server goes offline for any reason, it will download the recordings stored on the Failover Server and merge it with the main recordings when it returns to normal operation. For this option to work correctly, the copy of this camera (With the same name) on the Failover Server must be activated in the Failover event of the Failover monitor.

- **Create Bookmark when combining recordings:** Select this option to automatically create a bookmark when the system finishes the process of downloading and merging the videos with the main recording on the server. Create a title for the bookmark and choose a color.

The result in the Surveillance Client will be this:



- **Download recordings automatically when a bookmark is manually created for this camera:** Select this option to instruct the system to always download videos when a bookmark is manually created for this camera by the Surveillance Client operator. This is a feature that can be used in deployments that only have edge recording (for example using NVRs), however, in the event of an event where the operator can create a bookmark, the system can then download these most important images and maintain a copy on the main server.

© 2002 - 2024 by Digifort. All rights reserved.

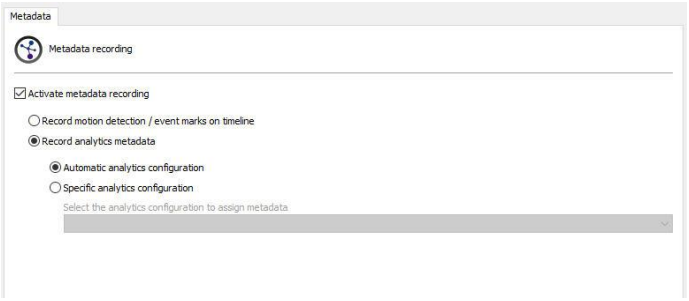
Observation

The combination of the downloaded video with the main video from the server will only occur one hour and thirty minutes after downloading the camera file.

6.1.3.3 Metadata

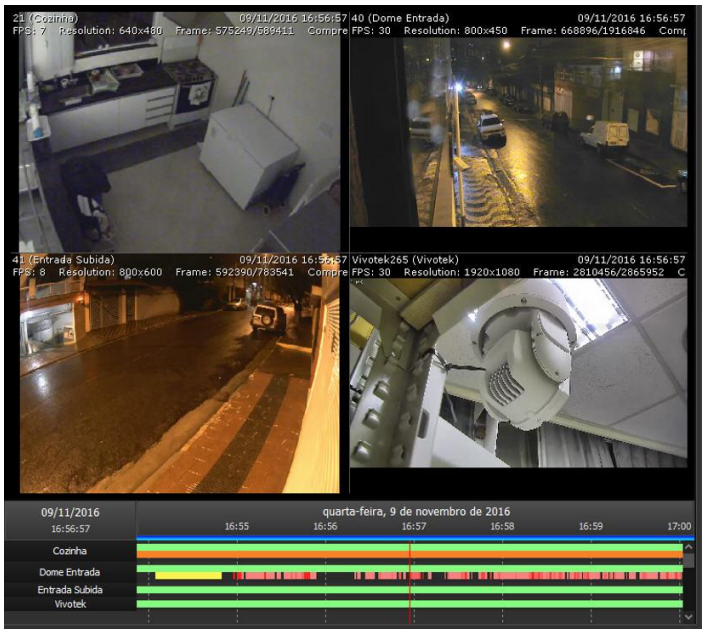
The system allows the recording and playback of metadata along with camera images.
Metadata is additional information that will be available along with the camera video recording. Analytics metadata, motion detection, and event recording are currently supported.

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



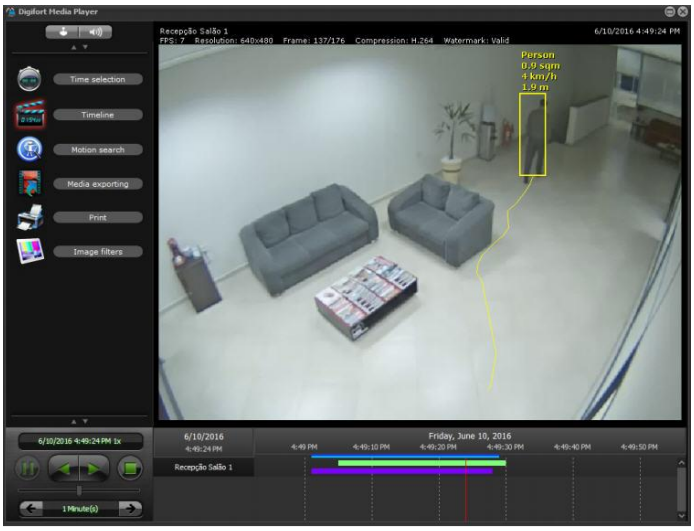
- **Record motion detection / events remarks on timeline**: If the system is detecting motion in the camera, the motion metadata will be presented in the media playback as a red bar with lighter or darker colors to inform the amount of movement at that moment. If recording events are triggered, a yellow bar will be recorded, informing you that that video session was recorded by event.

Once configured, it will be possible to check the metadata together with the recording of images in the Surveillance Client as shown in the image below:



© 2002 - 2024 by Digifort. All rights reserved.

- **Record Analytics Metadata**: The system allows the recording of analytics metadata automatically, where the system will record the first analytics configuration that is in operation associated with the camera. This allows recording analytics metadata for PTZ cameras with different analytics configurations in different presets. You can also manually select which analytics should be associated with this camera from the list. Once activated, it will be possible to check 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.

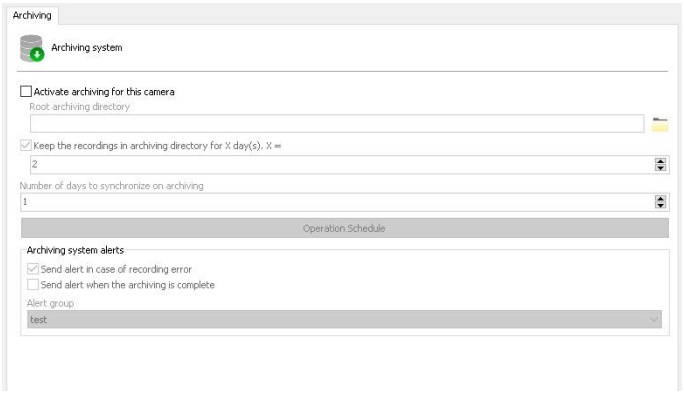
To learn more about Video Playback, see the Surveillance Client manual.

6.1.3.4 Archiving

The system allows recordings from a camera to be sent to another disk or computer on the network in order to make backups on tapes or other backup devices, as well as in the cloud.

In this configuration, you can specify the number of days that recordings should be kept on the disk or network computer.

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



- **Enable archiving for this camera:** Enable media archiving for this camera.

© 2002 - 2024 by Digifort. All rights reserved.

- **Archive Root Directory:** Enter the directory where archiving will be performed. This directory must be the same for all cameras as the system will create subdirectories for each archived day and for each camera automatically.
- **Keep recordings in the archive directory for X days:** Enter the number of days that camera images should be kept within the archiving directory. Exactly the last X specified days will be kept. Previous days will be deleted. NOTE: The system does not manage free space in archive directories, so make sure you have enough free space to store all the backup days defined here, otherwise archiving new images will fail due to lack of free space .
- **Number of days to synchronize on archiving:** Specify the number of previous recording days that the archive will synchronize during processing.
- **Operation Schedule:** Allows you to configure an operation schedule to determine when archiving can operate. The archiving system still remains an ongoing process, but will only operate during the scheduling period.
- **Send alert in case of recording failure:** If any error occurs during archiving an email notification can be sent. To do so, check this option and select the desired alert group.
- **Send alert when the archiving is complete:** Sends the selected alert group a notification email when archiving is successfully completed.

6.1.3.4.1 Operation and tips

The archiving process is the continuous process, that is, every 10 minutes, the system will check if the images from the previous days (According to the number of days selected for synchronization) that are located in the recording folder are archived and synchronized in the archive folder, if the system finds that any files are missing, it will copy these files again. This continuous process allows the system to continue an archiving operation even if the system has stopped for any reason (such as a network outage). If you delete a file from the archive folder that is still within the synchronization period, it will be copied again by the archiver.

In standard normal operation, when the clock changes to the next day, the system will begin copying recordings from the previous day(s) to the archive folder. If the server stops during the process, it will restart again as soon as the server is back up and running.

The archive root folder structure will contain a subfolder for each day of recording (with the date as the folder name) and within this day folder, you will find subfolders for each camera that was archived that day.

The archiving process is linear, that is, the system will copy data from only 1 camera at a time so as not to overload the main recording disk with excessive reads.

You can configure the archiving process to only work at certain times or days, thus allowing complex configurations such as, instead of archiving every day (the previous day), you could configure the system to synchronize only during the weekend. To do this, you must configure the operation schedule to occur only during the weekend (For example Saturday and Sunday) and configure the number of days for synchronization to 7, so when the process starts, it will synchronize the last 7 days of recording during the archiving process, in this case you also need to configure the number of days to keep in the archive folder with a minimum of 7 days.

The archive folder can typically be located on another computer on the network, or it can also be directed to a virtual cloud folder (It is possible, for example, to map drives in Azure Cloud via SMB).

The Surveillance Client also allows playback of videos recorded in the archive folder through the archive playback function. If you want to use this function, it will not be possible to use Glacial cloud storages due to excessive data reading time, which can take hours.

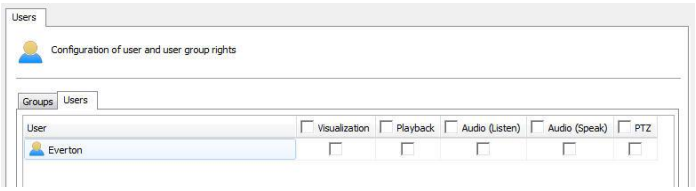
© 2002 - 2024 by Digifort. All rights reserved.

6.1.4 Rights

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

6.1.4.1 Users

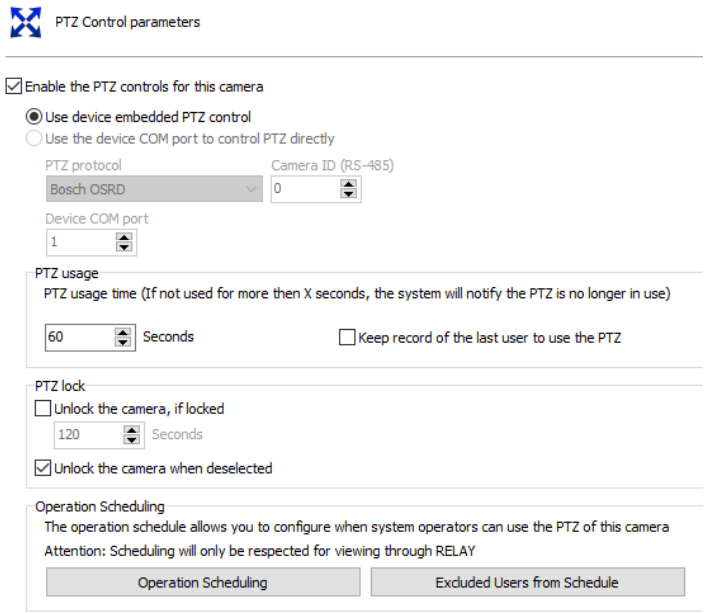
System Users and Groups will be listed automatically and may have 5 rights:



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

6.1.5 PTZ

6.1.5.1 Settings



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

- **Enable PTZ controls for this camera:** Enable this option (Enabled by default) to provide PTZ control for Surveillance Client users. If this option is disabled, operators will not have access to the camera's PTZ and the camera icon in the Surveillance Client will be displayed as a fixed camera.

© 2002 - 2024 by Digifort. All rights reserved.

- **Use the device's embedded PTZ control:** Select this option only if the camera being registered is an IP camera. In this case, the system will send PTZ commands directly to the camera. In this mode, the system will send PTZ control commands using the equipment's native protocol. If you are using an analog PTZ camera (connected via RS-485 for example) on a video server, DVR or NVR, by checking this option the system will send the commands in the device protocol (video server, NVR, DVR...) and the device should translate these commands to the camera protocol (For example Pelco-D), however some devices do not support this type of control and only have a pass-through option through the serial port, in these cases, you must choose the option **Use the device's COM port to control PTZ directly**.

- **Use the device's COM port for PTZ control directly:** By checking this option (If available), the system will send native commands in the chosen PTZ protocol (For example Pelco-D) through the connected equipment, using the pass-through commands of the device. Use this option only if the device to which the analog camera is connected does not have the ability to natively control the cameras.

- **PTZ Protocol:** Select which PTZ protocol your analog camera is configured for (Only for direct pass-through control)

- **Camera ID (RS-485):** Enter the ID of your analog camera (Configured in the camera)

- Device COM Port: Select the COM port number of the network device (Video server, DVR, NVR) if the device has more than 1 port

6.1.5.1.1 PTZ Usage

When using PTZ on the Surveillance Client, the system shows all other users who is currently in control of the camera.
In this option you can configure **X seconds** after which the system will understand that the PTZ is no longer in use if it is not moved by the operator.

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

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

© 2002 - 2024 by Digifort. All rights reserved.

6.1.5.1.2 PTZ Lock

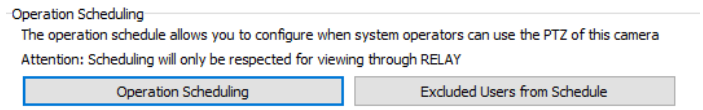
PTZ lock is a feature that allows the user to block the use of a camera's PTZ through user priority levels.

When a user locks the PTZ, only that user will have control over the camera. Other users who attempt to operate will not have access to the control as it is blocked for exclusive use by the operator who initiated the blocking, however, a user with a higher priority than him will be able to take control of the lock (The users' priority level can be configured through user or user group policies).

PTZ lock options include:

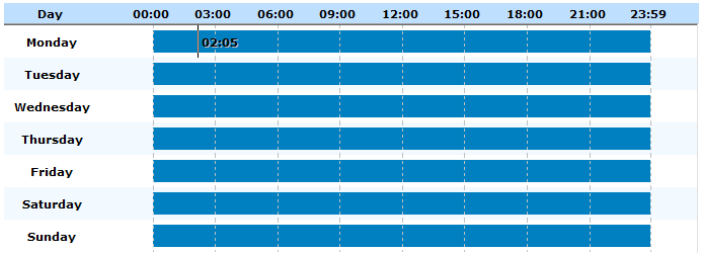
- **Unlock the camera, if blocked in X seconds:** If PTZ is blocked by a user, this option sets a time in seconds for it to be automatically unlocked, if the user has not already done so.
- **Unlock camera when deselected:** Unlocks the PTZ of the locked camera in the Surveillance Client when it is deselected.

6.1.5.1.3 Operation Scheduling

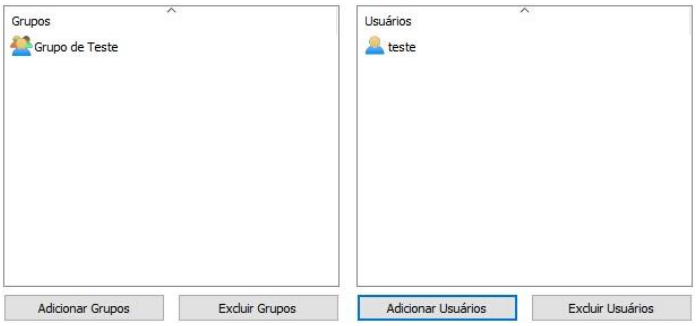


The Operation Scheduling allows configuring when system operators will be able to use the PTZ of this camera.

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



- **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:



Note

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

© 2002 - 2024 by Digifort. All rights reserved.

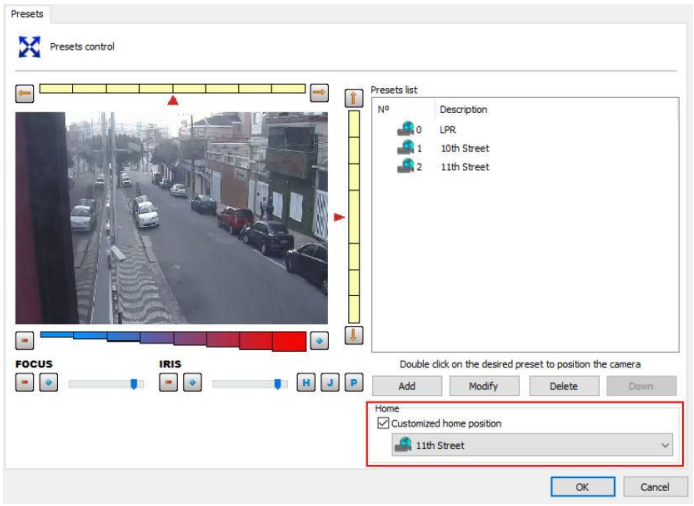
6.1.5.2 Presets

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

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

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

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



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

© 2002 - 2024 by Digifort. All rights reserved.

Important

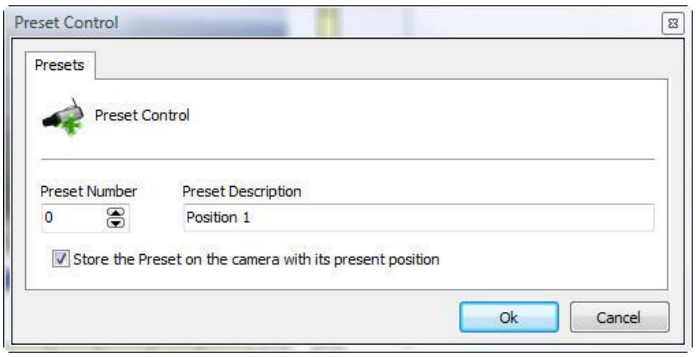
The preset list only displays the list of presets belonging to the camera. All presets created by the system are saved in the camera itself. The system associates the list item with the camera preset using its number.

Tip

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

6.1.5.2.1 How to create a preset

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



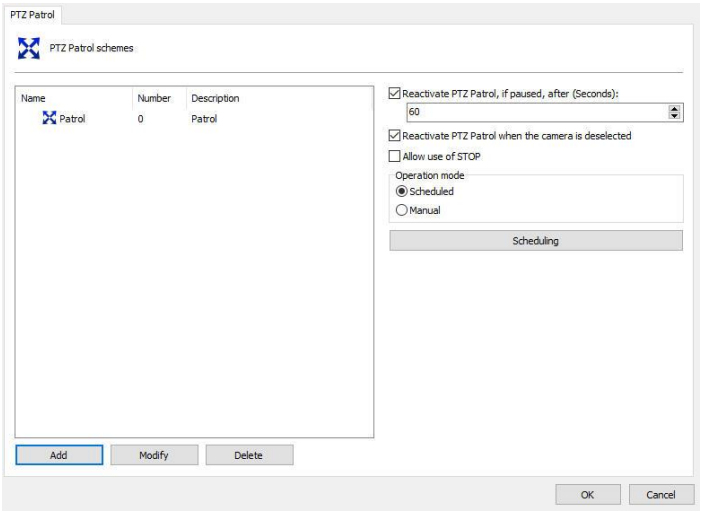
- **Preset Number:** Preset number that the system will associate with the camera's internal preset list.
- **Preset Description:** A description of the preset being added. This name will be displayed to the user in the Surveillance Client.
- **Save the preset to the camera with its current positions**: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

6.1.5.3 PTZ Patrol

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

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

© 2002 - 2024 by Digifort. All rights reserved.



- **Scheme List:** List of PTZ Patrol schemes created for the selected camera.
- **Add button:** Add a new PTZ Patrol scheme.
- **Change button:** Changes the selected scheme.
- **Delete button:** Deletes the selected scheme.
- **Reactivate PTZ Patrol if paused after (seconds):** Reactivates PTZ Patrol in the specified time if it is paused in the Surveillance Client.
- **Allow the use of STOP**: This option allows the Surveillance Client operator to definitively stop a PTZ Surveillance. If the patrol is stopped, the system will not reactivate it automatically as automatic reactivation will work only if the patrol is paused. This option can be used as an emergency way where the operator needs to stop the patrol operation of a camera and keep it fixed in one position for a long time. By changing the automatic operation of PTZ Surveillance, the administrator has the option of enabling or disabling this option, with the default value being disabled.

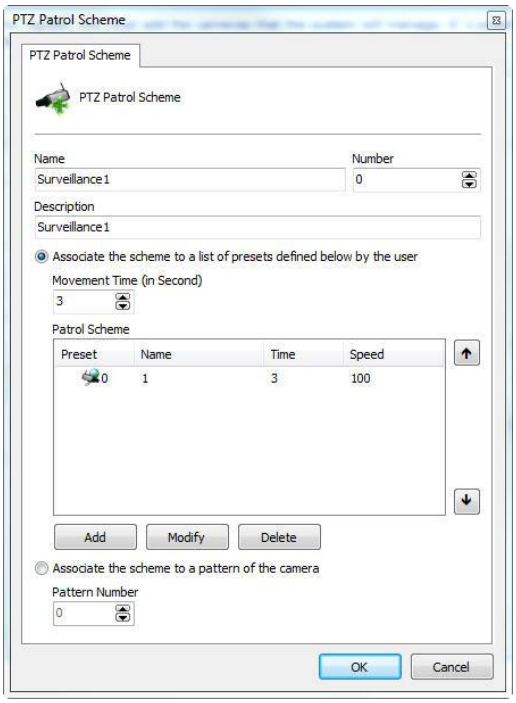
- **Operation mode (Operation mode):**
  - **Scheduled:** Allows scheduling of PTZ Patrol. In this mode, other patrol schemes for the same camera cannot be activated manually and the whole operation will be automatic.
  - **Manual:** For PTZ Patrol to start working on the camera, it must be manually activated in the Surveillance Client.

- **Scheduling button:** Defines times and days of the week that the PTZ Patrol schemes will work.

6.1.5.3.1 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:

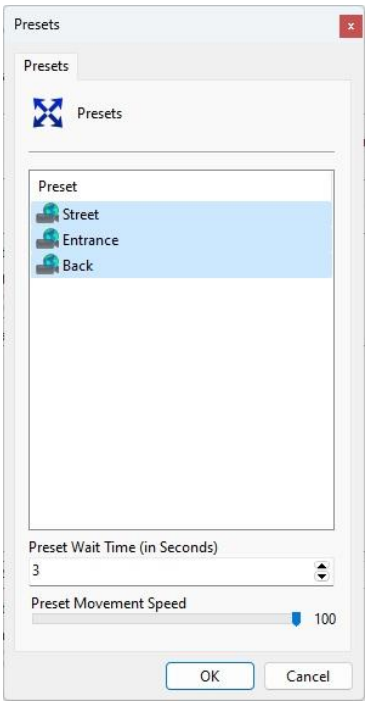
© 2002 - 2024 by Digifort. All rights reserved.



- **Schema name:** Enter an identification name for the PTZ Patrol to be created.
- **Number:** This number is used to start PTZ Patrol through the PTZ Keyboard controller.
- **Schema description:** Enter a brief description of the PTZ Patrol to be created.
- **Associate the scheme with the list of presets defined below by the user:** Allows the user to create the list of presets in which the camera will assume its positions during PTZ Patrol.
  - **Movement time:** Global waiting time for switching between presets. This time will be added to the individual waiting time of each preset.
  - **Preset list:** List of presets added by the user.
  - **Add Button:** Adds a preset to the scheme to be created.
  - **Change button:** Changes the selected preset.
  - **Delete button:** Deletes the selected preset.
- **Associate the scheme with a camera pattern:** Select this option if PTZ Patrol is configured directly on the camera. To learn how to use this feature, consult your camera manual.
  - **Pattern number:** Pattern number configured on the camera.

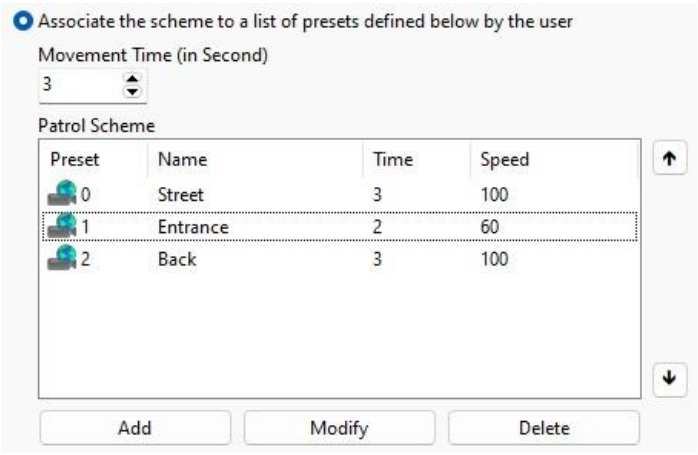
The default operation for most cameras is to use the preset list, so the system will constantly send preset commands to the cameras. To add the desired presets, click the Add button:

© 2002 - 2024 by Digifort. All rights reserved.



On this screen you must select the presets that you want to be part of the patrol scheme and you can define a waiting time for each preset, as well as the movement speed:

- **Wait time:** Set the time (In seconds) that the system will keep the camera in the preset before moving to the next preset.
- **Preset Movement Speed:** Some cameras allow you to specify a movement speed when calling the preset, so if you decrease this value (Represented as a percentage), the camera can move faster or slower for a given preset.



You can set independent speed and hold time values for each preset.

To change the preset order, simply select the desired preset from the list and click on the up and down arrows located on the right side of the list.

© 2002 - 2024 by Digifort. All rights reserved.

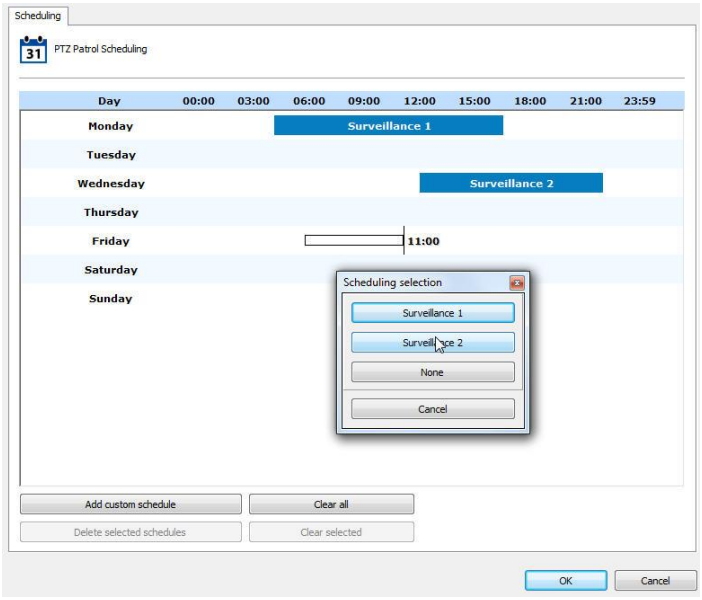
Tip

During patrol operation, the system will send the preset positioning command to the camera and wait for the preset time + the specified global time, that is, if you set a global time of 3 seconds and an individual time of 3 seconds to a preset, then the system will wait 6 seconds before sending the command to move to the next preset.

6.1.5.3.2 How to configure schedules of PTZ Patrol Schemes

After registering all PTZ Patrol schemes, it is necessary to define the times and days of the week when these schemes will come into effect.

To configure the schedule, click on the Schedule button, as illustrated in the figure below



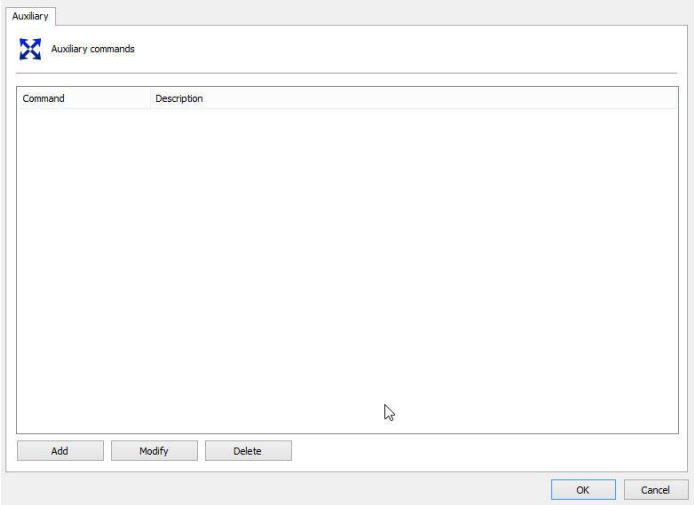
The operation of this screen is identical to the screen specified in the topic How to Configure the Recording Schedule, with the difference that the previously registered PTZ Patrol schemes must be chosen.

The system will load the desired scheme at the specified times and if there is no scheme scheduled then the camera will not move.

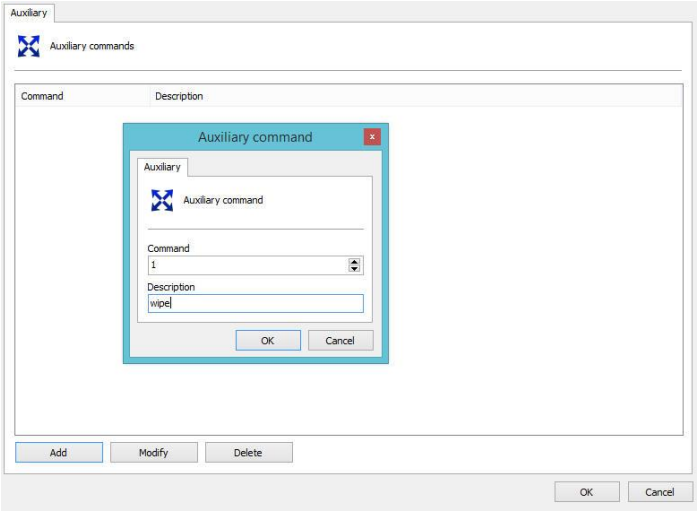
6.1.5.4 Auxiliary

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

© 2002 - 2024 by Digifort. All rights reserved.



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



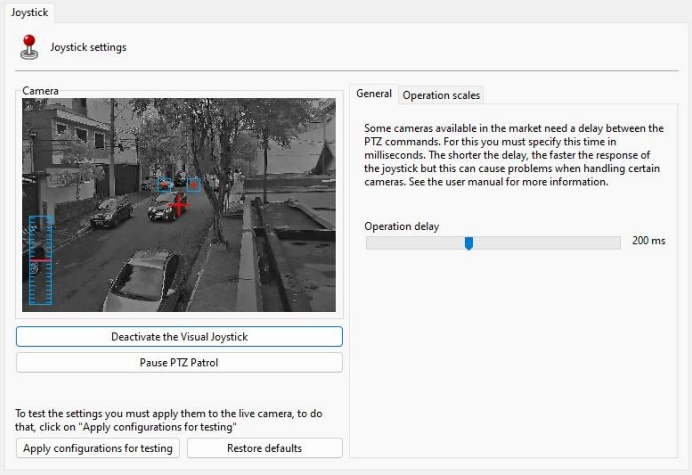
6.1.5.5 Joystick

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.



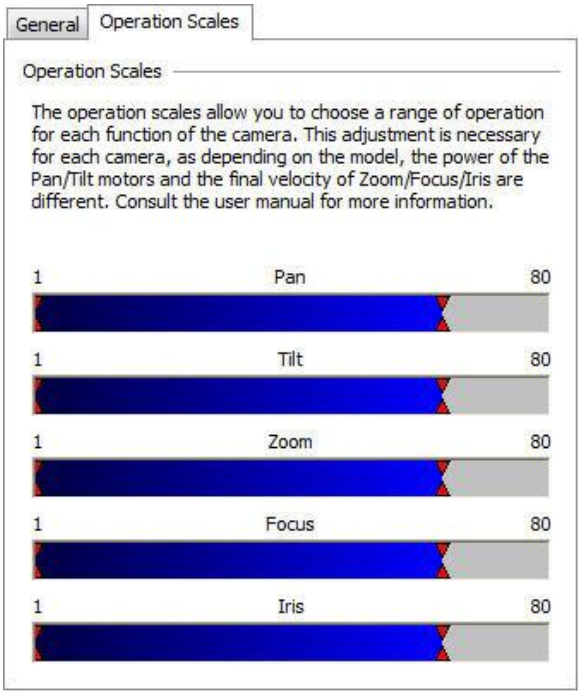
- **Activate / Deactivate the Visual Joystick:** Enable or disables the visual joystick. To learn what the visual joystick is and how it works, see Visual Joystick.
- **Pause PTZ Patrol:** Pauses current PTZ Patrol to allow PTZ control.
- **Apply settings for testing:** Apply the settings made only for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

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

6.1.5.6 Menu Control

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

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

- **Open Menu button:** Opens the camera settings menu.
- **Close Menu button:** Closes the camera settings menu.
- **Navigation Buttons:** Navigates through the camera settings menu. Click on the central button to enter a configuration.

© 2002 - 2024 by Digifort. All rights reserved.

- **Enable Visual Joystick Button:** Enables the visual joystick

6.1.5.7 Visual Joystick

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

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

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

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

The movement and zoom sensitivity can be adjusted in the operating scale settings on the page How to configure the Joystick

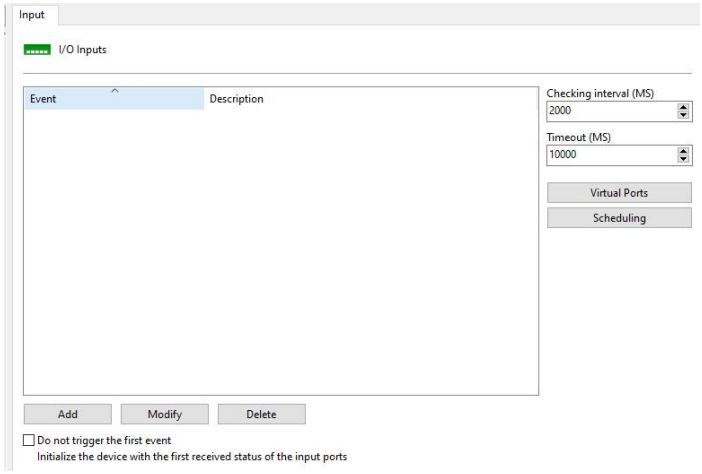
6.1.6 I/O

The system has the ability to control the alarm inputs and outputs of cameras that provide this feature.

6.1.6.1 How to add input events

An I/O input can be, for example, a motion sensor or panic button.

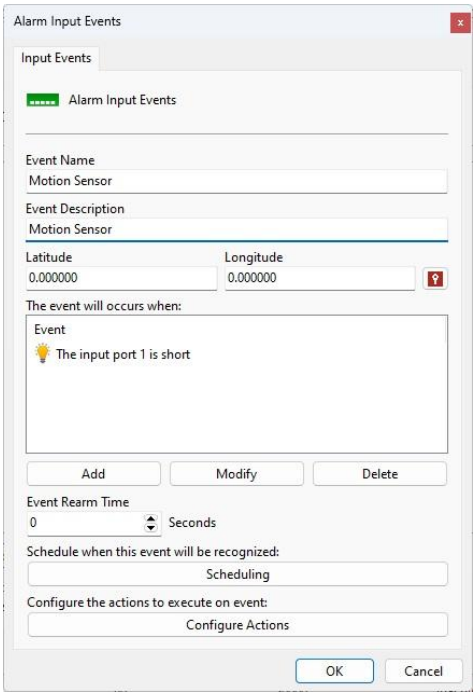
© 2002 - 2024 by Digifort. All rights reserved.



- **Checking interval (ms)**: Interval at which the system will communicate with the camera to recognize an input event, for example, a presence sensor.
- **Timeout (ms):** Interval at which the system will attempt a new connection with the camera if the current connection is lost.
- **Do not fire the first event:** When selecting this option, the system will ignore the initial status of the I/O port, so that triggering will only begin at the first status change. This option is particularly useful to prevent the system from generating events at server startup or when a camera is saved (If the conditions of any input event are satisfied).

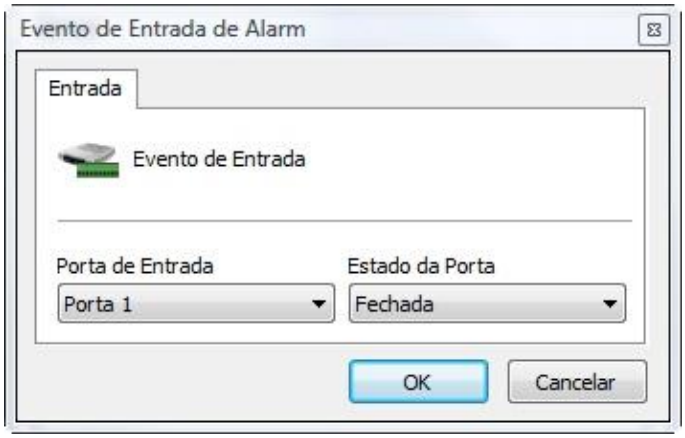
To add an input event, click **Add**. To change an input event, click **Modify**. To delete an input event, click **Delete**. All of these buttons refer to input events, located right below their list.

By clicking **Add**, the following screen will be displayed:



© 2002 - 2024 by Digifort. All rights reserved.

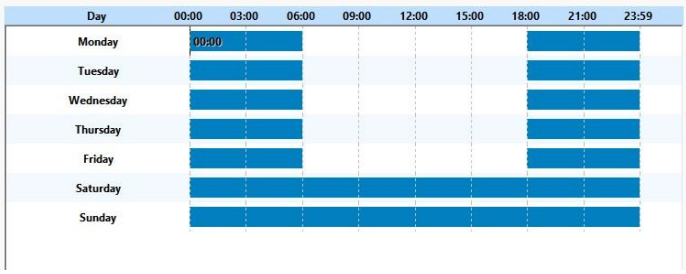
- **Event name:** Camera input event name.
- **Description for this event**: Camera input event description.
- **Latitude / Longitude**: You can define a geographic position where the sensor is located. This position can be used in Operational Maps and in event search to show where the event was triggered.
- **The event will occur when**: Complete this list according to your needs. In the example above, it was configured so that the event is only generated when port 1 of the camera's alarm input is activated. Combinations can be created such as port 1 activated, 2 activated and 3 deactivated. To add an event, click the Add button. To change and delete, click on the corresponding buttons. When clicking on the add button the following screen will be displayed:



On this screen select the gateway and its state for the event being configured to occur.

- **Event Rearm Time:** Define a time for the system to reset this event after a trigger. For example, if you configure the event with a reset of 60 seconds and this event is recognized again before 60 seconds, then the system will ignore this new trigger.

- **Scheduling:** Allows the operation schedule of this alarm.



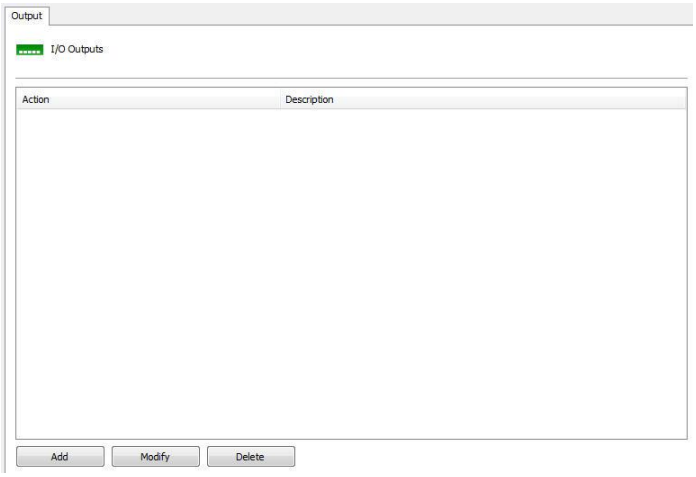
The operation of this schedule is identical to the screen specified in the topic How to Configure the Recording Schedule with the difference that the I/O operation must be chosen between Activate or Deactivate.
In the example above, this event will only be recognized between 00:00 and 06:00 and 18:00 until 00:00 on weekdays and during the whole period throughout the weekend.

- **Configure Actions button**: Click this button to configure the actions that the system will take when this event occurs. To learn how to configure actions, see How to configure alarm actions.

© 2002 - 2024 by Digifort. All rights reserved.

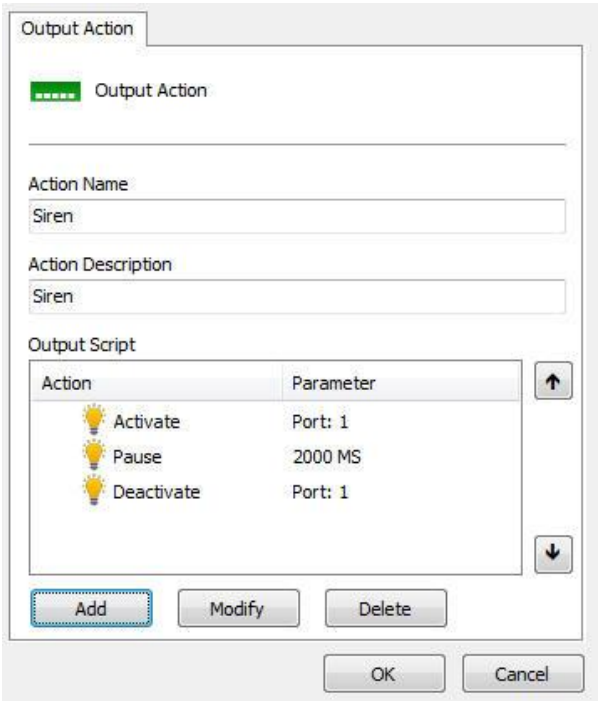
6.1.6.2 How to add output actions

Camera's output actions are configured in the form of a script, that is, a set of parameters that are executed in the order defined by the user.



To add an exit action, click **Add**. To change an exit action, click **Modify**. To delete an exit action, click **Delete**. All these buttons refer to output actions, located right below their list.

Clicking on add, the following screen will be displayed:



- **Action name:** Enter the name of the output action
- **Description for this action:** Enter the description for this output action.
- **Output Script:** Displays the list of parameters that will be executed in this action. The figure above illustrates the triggering of a siren as follows:

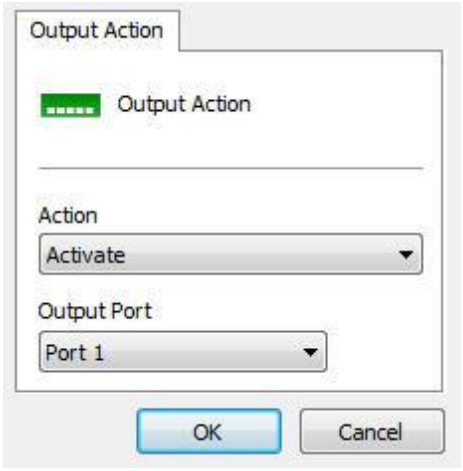
© 2002 - 2024 by Digifort. All rights reserved.

1. Turn on the siren
2. Keeps the siren on for 2 seconds (2000 ms)
3. Turn off the siren

You can move items in the list using the up and down arrow buttons located on the right side of the action list.

To add an output action click **Add**. To change or delete click on the corresponding button.

When clicking **Add** the following screen will be displayed:



The available actions are:
- **Activate:** Ativa uma porta de saída do dispositivo.
- **Pause:** Waits X milliseconds to trigger the next action in the script.
- **Deactivate:** Disables a device output port.
- **Invert:** Inverts the state of a device port.

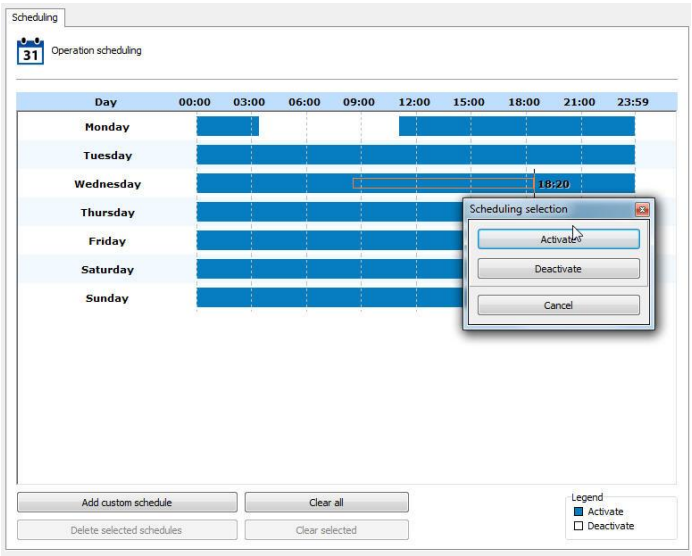
On this screen select the action and the action parameters such as which port it will act on.

6.1.6.3 How to configure event scheduling

The system has a global alarm input schedule, which defines the operation of all alarm input events, where no incoming alarm will be acknowledged during the period that is disabled in the schedule (In this mode, the system will not communicate with the device to get I/O status).

To configure the event schedule, click on the **Scheduling**, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



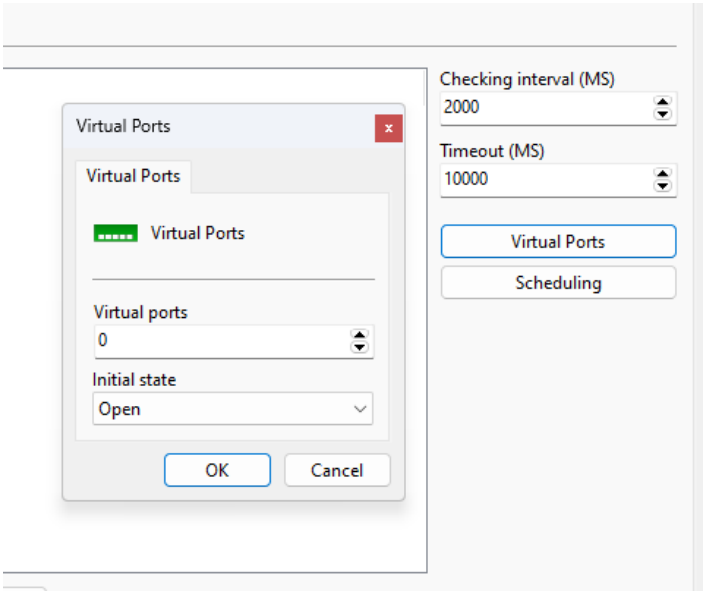
The operation of this screen is identical to the screen specified in the topic How to Configure the Recording Schedule, except for the types of actions:

- **Activate:** Enables alarm input event recognition from this camera at the specified times and days of the week. This configuration is represented by the blue color.
- **Deactivate**: Disable alarm input event recognition from this camera at the specified times and days of the week. This option is represented by the color white.

6.1.6.4 Virtual I/O

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

Virtual I/O ports can be defined for I/O Devices or Camera I/O:



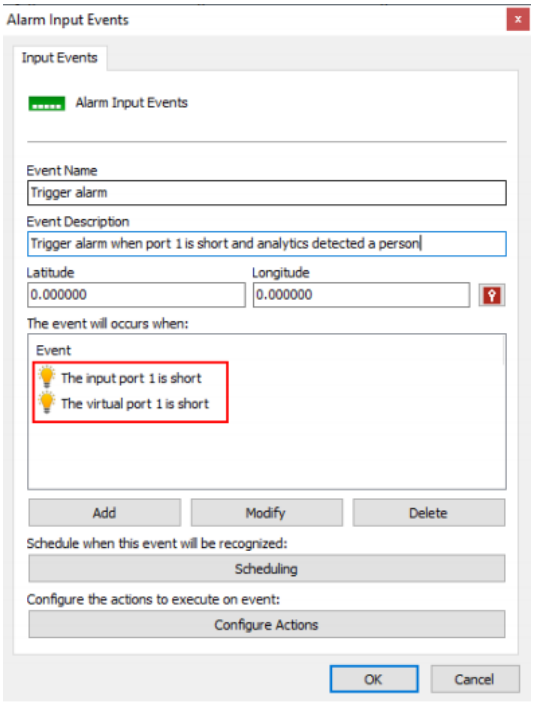
- **Virtual Ports:** Set the number of virtual ports for this device

© 2002 - 2024 by Digifort. All rights reserved.

- **Initial State:** Set the initial state of this device's virtual ports

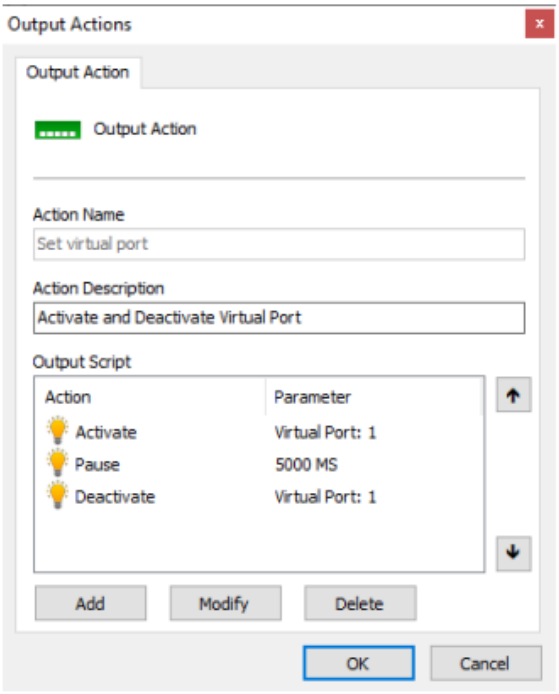
With virtual I/O it is possible to combine one or more physical alarm inputs with one or more virtual I/O ports, with this it is possible to define, for example, that for an event to occur it is necessary that the alarm input be activated (through of the physical input) and a software event occurs (for example an analytics, or an LPR event) and changes the status of the virtual port.

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

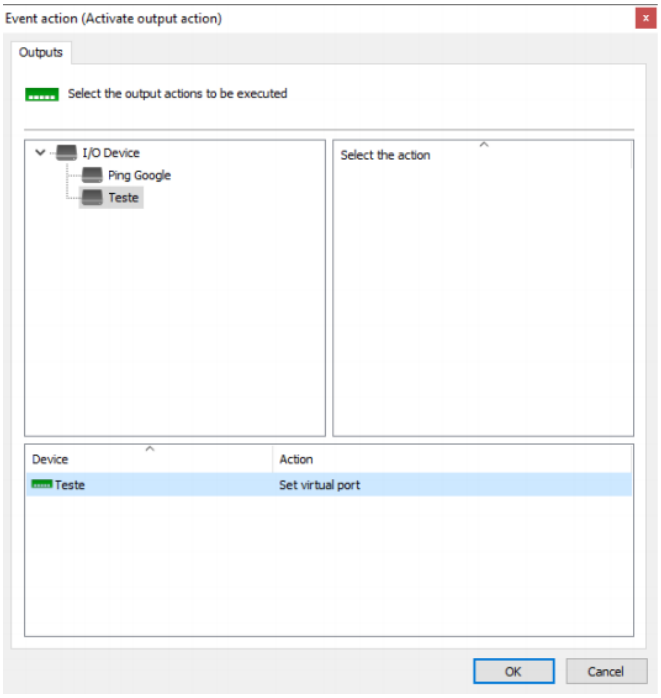


To activate the virtual port, you need to create an exit script that activates the port:

© 2002 - 2024 by Digifort. All rights reserved.



And this script can be called by any system event, such as an analytics presence detection (Or even via API):



Virtual I/O is an excellent tool that can be used to create complex automation and alarm scenarios by combining logical and physical events. As it is a complex feature, if you have difficulty configuring it, contact our support team and we will help you succeed.

© 2002 - 2024 by Digifort. All rights reserved.

6.1.7 Events

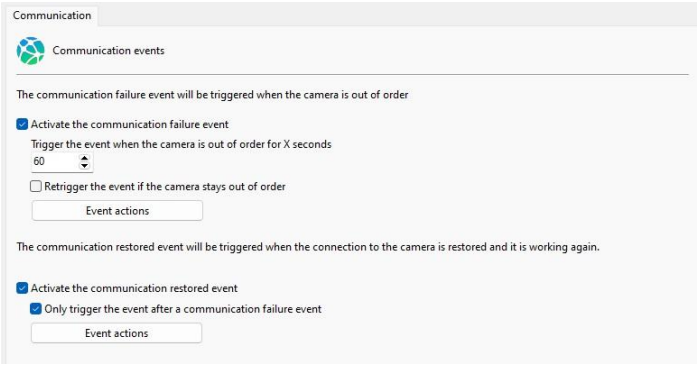
During camera operation in the system, several events occur with it. These events can be communication failures or alarm input events, for example.

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

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

6.1.7.1 Communication

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



6.1.7.1.1 Communication Failure Event

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

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

To learn how to configure event actions see How to configure event actions

6.1.7.1.2 Connection restore event

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

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

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

6.1.7.1.3 Device failure report

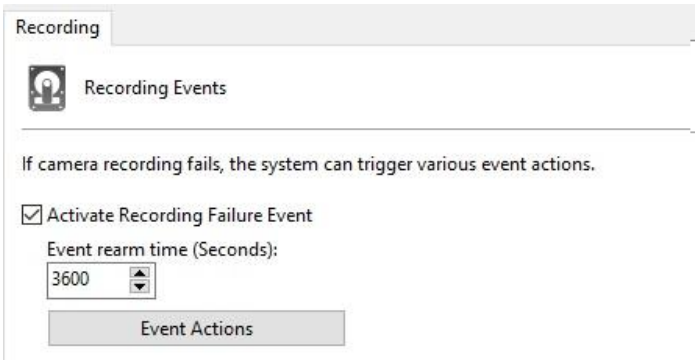
The Device Failure Report will list all failures and communication recovery with devices in the system, also providing the total failure time for each device.

© 2002 - 2024 by Digifort. All rights reserved.

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

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

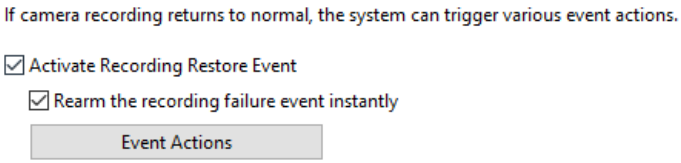
6.1.7.2 Recording Failure Event



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

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

To learn how to configure event actions see How to configure event actions



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

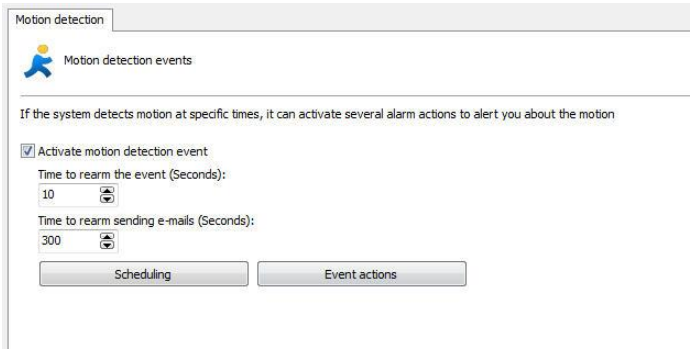
- **Activate Recording Restore Event:** Activates the recording restore event
- **Rearm the Recording Failure Event Instantly:** With this option enabled, the Recording Failure Event will reset instantly (Instead of waiting for the previously set reset time) when the Recording Restore Event occurs after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

6.1.7.3 Motion Detection

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

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

© 2002 - 2024 by Digifort. All rights reserved.



6.1.7.3.1 How to configure motion detection event

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

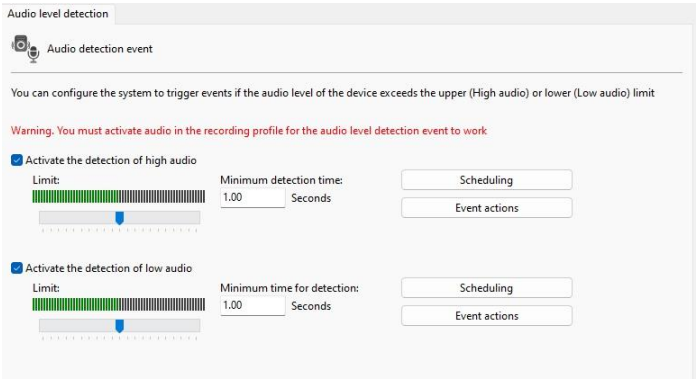
- **Activate Motion Detection Event:** Activates the motion detection event.
- **Event rearm time:** Specify the value in seconds that the system will recognize new events after an event has occurred.
- **Time to rearm sending emails:** Specify the time interval in which the system will send another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

Note

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

6.1.7.4 Audio Detection

The audio detection event allows events to be triggered in two situations if the volume is above or below a specified threshold for a specified time:



© 2002 - 2024 by Digifort. All rights reserved.

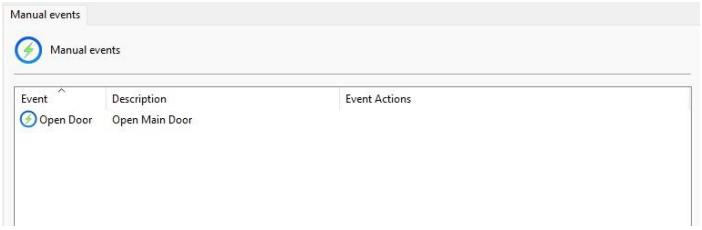
The screen offers the following features:

- **Enable Loud Sound detection:**
  - Position the cursor on the desired audio level that will trigger the event. Configure the time that the configured high audio volume must be sustained for the trigger to happen.
  - Configure Event Scheduling. To know about scheduling see the chapter How to configure the recording schedule
  - Configure the desired actions for the event. To know more about events see the chapter How to configure event actions

- **Enable Low Sound detection:**
  - Position the cursor on the desired audio level that will trigger the event. Configure the time that the configured low audio volume must be sustained for the trigger to happen.
  - Configure Event Scheduling. To know about scheduling see the chapter How to configure the recording schedule
  - Configure the desired actions for the event. To know more about events see the chapter How to configure event actions

6.1.7.5 Manual Events

It is possible to create specific events within the cameras that can be triggered by operators manually by right-clicking on the live camera.

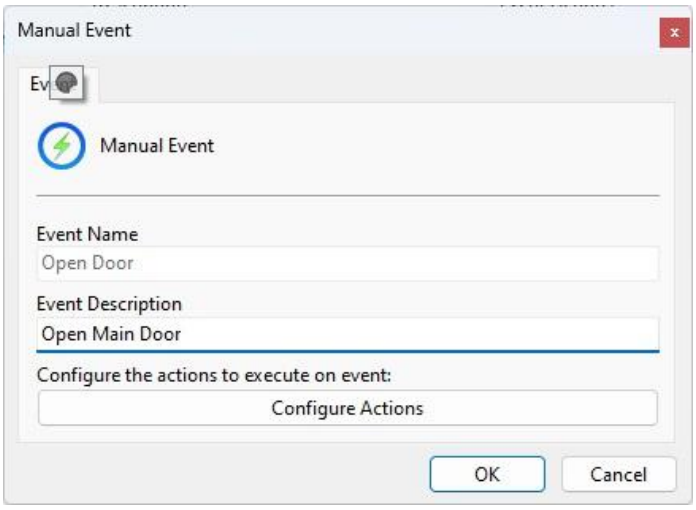


On this screen, the manual events that can be triggered by the operator in the Surveillance Client must be registered. In the example of the figure above, an event is registered that opens a door.

To learn how to trigger manual events through the Surveillance Client, consult its manual.

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

© 2002 - 2024 by Digifort. All rights reserved.



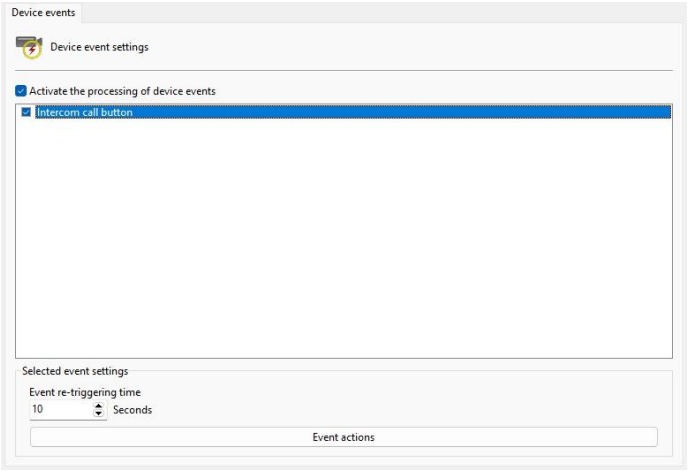
On this screen, provide the name and description of the event and finally click on **Configure Actions** to configure which actions the system will take when the operator triggers this event. To learn how to configure the actions that this manual event will execute, see How to configure event actions

6.1.7.6 Device Events

Some devices have events that don't fit into any of the system's predefined categories, so we created this architecture to be able to support different types of camera events.

For example, built-in Intercomm devices will provide the event "Intercomm call button" that will be triggered when someone presses the bell on the equipment, and you can configure event actions associated with these custom events.

If the camera has any extra event, it will appear in the configuration window, devices have different types of events such as Disk Failure, Video Loss, etc.
In the example below, the doorphone call event is available to be triggered on a Videointercom:



As in any other system event, you can configure the time for re-triggering and the actions that must be taken if the event is triggered, to see more about the actions navigate to How to configure event actions.

© 2002 - 2024 by Digifort. All rights reserved.

6.1.7.7 Event Variables

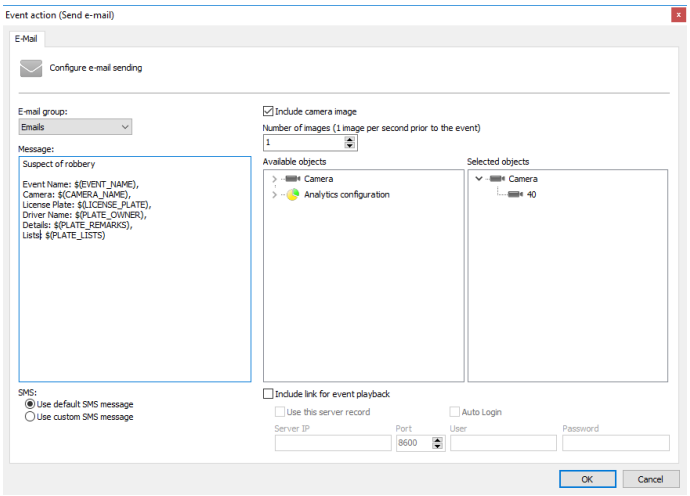
The Event Variables feature allows the use of dynamic variable values within event actions.

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

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

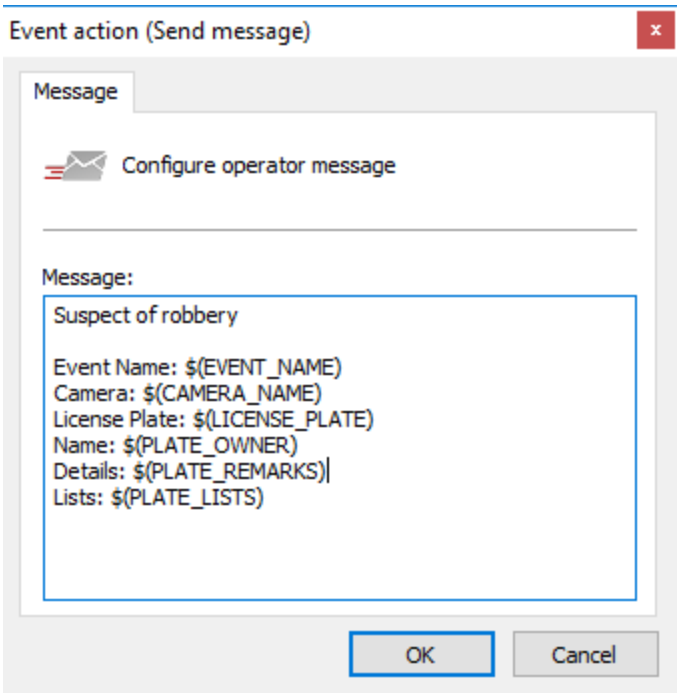
- The following event actions support the use of variables:
- Send Email
- Send Message to Operator
- Send a Push Notification
- Send HTTP Request
- Create Bookmark

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

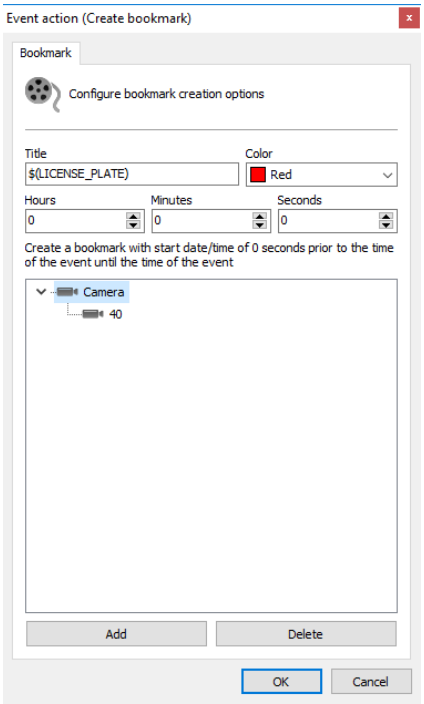


The same can be configured for messages sent to system operators, adding precious information in the alarm popup:

© 2002 - 2024 by Digifort. All rights reserved.



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



© 2002 - 2024 by Digifort. All rights reserved.

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

6.1.8 Privacy

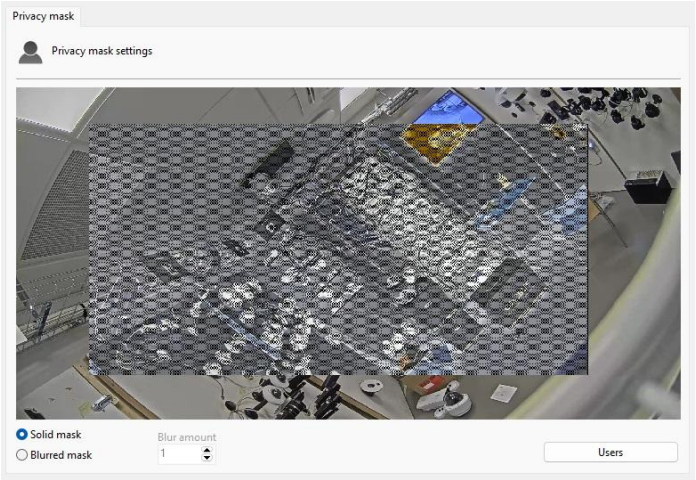
6.1.8.1 Privacy Mask

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

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

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

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

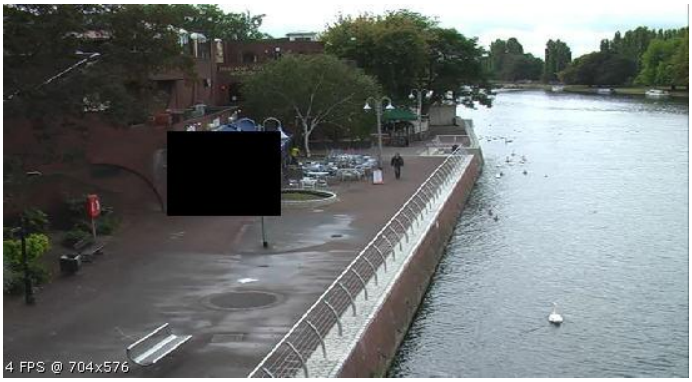


To add a privacy mask, click with the left mouse button on the image and drag it forming a rectangle. To remove a selected area, right-click a rectangle encompassing the entire area of the mask to be removed,

© 2002 - 2024 by Digifort. All rights reserved.

or right-click on the image and select **Erase Areas** to delete all created masks. By clicking on the Users button, it is possible to define which users or groups of users will be affected by the mask.

You can select two types of privacy mask: **Solid** or **Blurred**.
Solid will generate a completely black mask. The effect of the opaque mask is shown in the figure below:

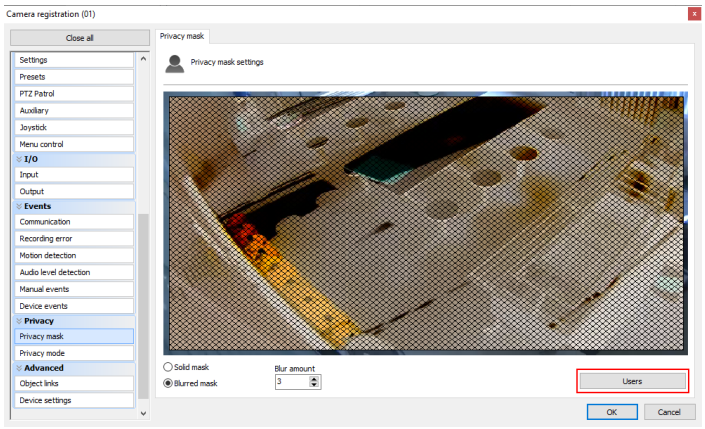


The **Blurred** mask can generate a mask with levels of transparency that can be configured within a scale of 1 to 10. The image below shows the application of the blurred mask:

Another usage example:

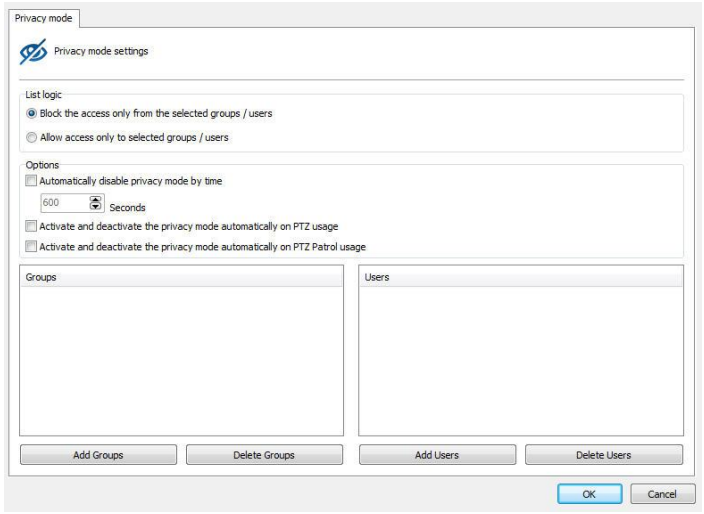
Privacy Mask can be conditionally applied to specific users / user groups.

© 2002 - 2024 by Digifort. All rights reserved.



6.1.8.2 Privacy Mode

The privacy mode allows the determination of a list of users who will lose access to a camera's image when a user activates the privacy mode via the Surveillance Client. This feature can be very useful when the cameras of an installation are available externally, with this, the operator can temporarily block external access to the camera whenever he wants.



The privacy mode screen has the following functionality:

- **Block access only from selected groups/users:** In this mode, all selected users and groups will lose access to camera image when privacy mode is triggered.
- **Only allow access to groups; selected users:** In this mode, everyone will lose access to camera image except selected users and groups when privacy mode is triggered.

- **Automatically deactivate the privacy mode by time:** Automatically deactivates the privacy mode after X configured seconds.
- **Activate and Deactivate the pricacy mode automatically on PTZ usage:** This option will activate the privacy mode when an operator moves the camera (PTZ) and will automatically deactivate when the operator finishes the use of PTZ controls.

© 2002 - 2024 by Digifort. All rights reserved.

- **Activate and deactivate the privacy mode automatically on PTZ Patrol:** This option will activate the privacy mode automatically when PTZ Patrol is paused and disable the privacy mode when PTZ Patrol is reactivated.

- **Add groups:** Add groups of users to privacy mode.
- **Delete groups:** Delete groups of users in privacy mode.
- **Add users (Add users):** Add users to privacy mode.
- **Delete users (Delete users):** Deletes users in privacy mode.

Nota

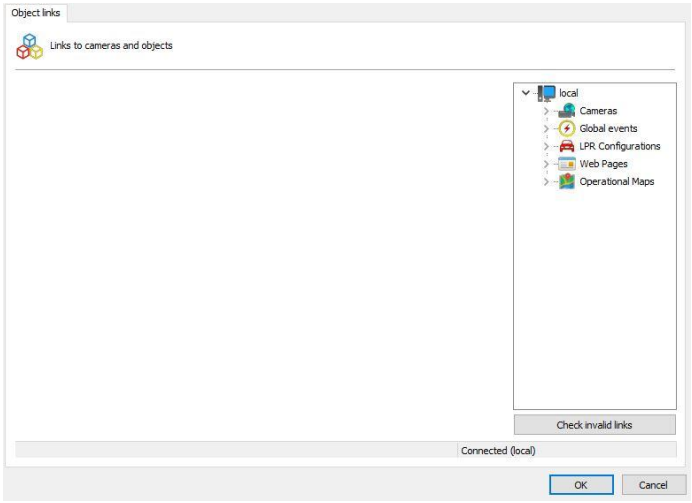
The user must have rights to activate privacy mode. To learn how to grant user rights, see the User Rights chapter

6.1.9 Advanced

6.1.9.1 Object Links

The Object Link feature allows the creation of clickable objects on the camera image itself, which, when activated, lead to other objects in the system or trigger events.

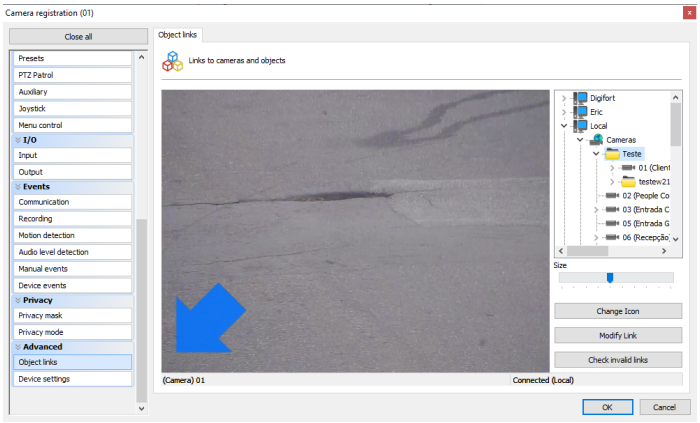
They allow the creation of virtual links between different cameras and also the creation of superimposed event triggers on the camera images.



The available objects can be from any servers that are connected in the administration client, making it possible to make a link between servers.

Setting up the links is very easy. The link editor is located within the "Object Links" option in the camera register. To create a link, just drag and drop the desired object from the list of objects and the link type selection option will be displayed (zone or icon).

© 2002 - 2024 by Digifort. All rights reserved.

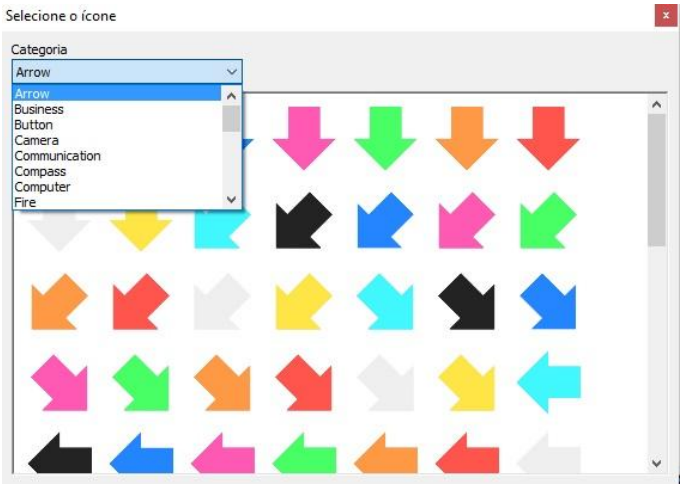


Zone: the system will create an area that can be defined by the user by dragging the points (using a double click on the border the system will create another point) to form the desired area.

Once the zone is selected the select color and change link buttons will be available:

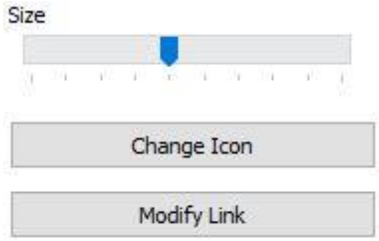
If the operator selects the option to change link, just click on the new object and the system will make the new object the target of the link.

Icon: the system will then ask the user which icon to place:

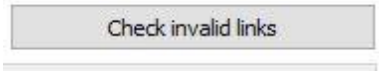


© 2002 - 2024 by Digifort. All rights reserved.

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



The system also allows the verification of invalid links, in case an object is deleted or loses connection with other servers. To do this just click on the check for invalid links button.



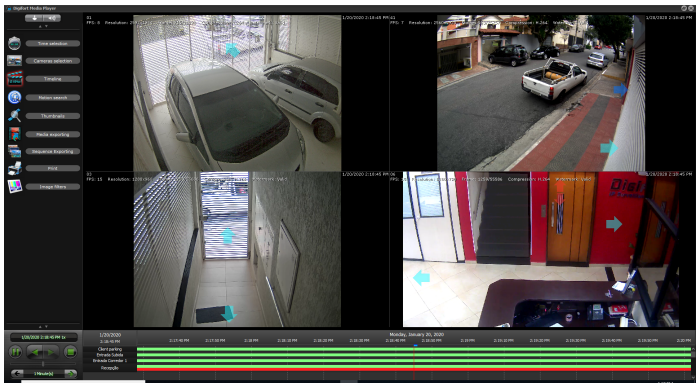
The image below shows an example of using object links. Each camera in live view has a link to other cameras in the image. When clicking on the link (represented here by semi-transparent arrows), the associated camera will be loaded, allowing quick navigation between cameras, for example, when following a person who is moving between cameras.

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

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

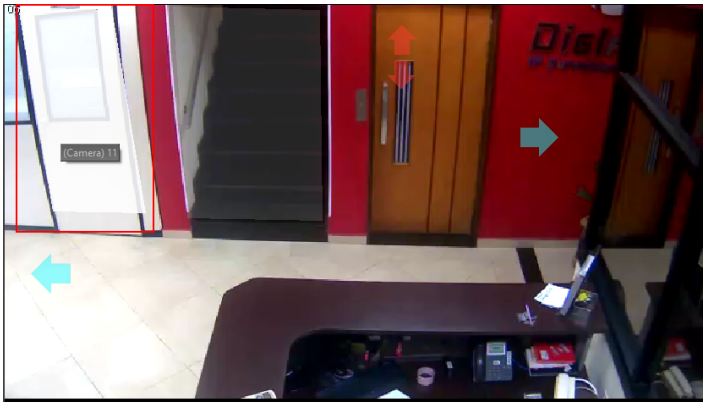
In the Video Player, only links to cameras will be displayed.

© 2002 - 2024 by Digifort. All rights reserved.



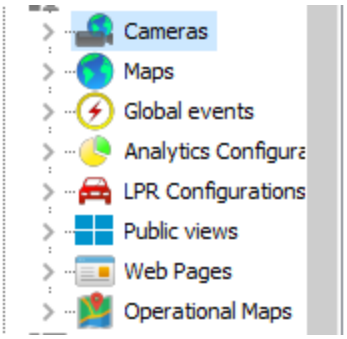
A zone is represented through a semi-transparent polygon in the image, which can be added for example in the contour of a door or gate, providing a visual representation that if the operator clicks on this gate, he will be able to see the image of the camera that is on the other side, or you can also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

The image below shows a white zone, which is associated with a door, when clicking on the door, the camera from inside the room will be displayed.



Links can also be in the form of icons superimposed on the image. When creating an icon link, an editor will appear with several categories of icons that can be chosen to best represent the associated action.

Links can be configured for any visual object in the system, any event (Global and Manual), camera presets and public views, providing great flexibility to the resource:



© 2002 - 2024 by Digifort. All rights reserved.

Consult the Surveillance Client manual to check different settings for optimizing the use of object links.

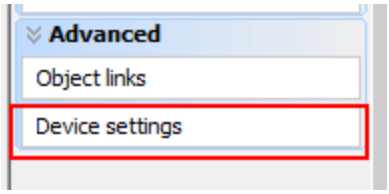
6.1.9.2 Advanced Device Settings

With the Advanced Device Settings option, you will be able to configure parameters (generally streaming parameters) of the cameras and apply the configurations to multiple cameras simultaneously.

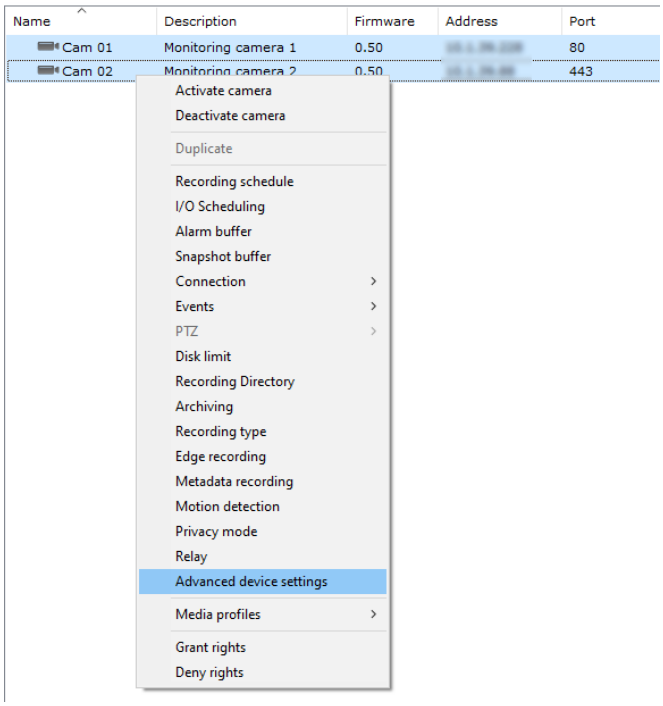
The vast majority of manufacturers do not allow dynamic image streaming, which allows the VMS to request images in a certain configuration (Resolution, Frame Rate, Bitrate, etc.) dynamically, that is, these settings are fixed in the camera and the VMS can only request a preconfigured stream.
To facilitate camera configuration, we have developed an advanced configuration feature, where the system can manipulate these fixed camera configurations through the Administration Client interface, without having to open the browser and configure the cameras manually.

The best thing about this feature is that you can still apply the desired changes (such as resolution, bitrate, codec, etc.) to several cameras at the same time (as long as they are from the same manufacturer and have the same configuration driver).

Device Settings can be accessed through the "Device Settings" menu on the camera registration (for individual change):



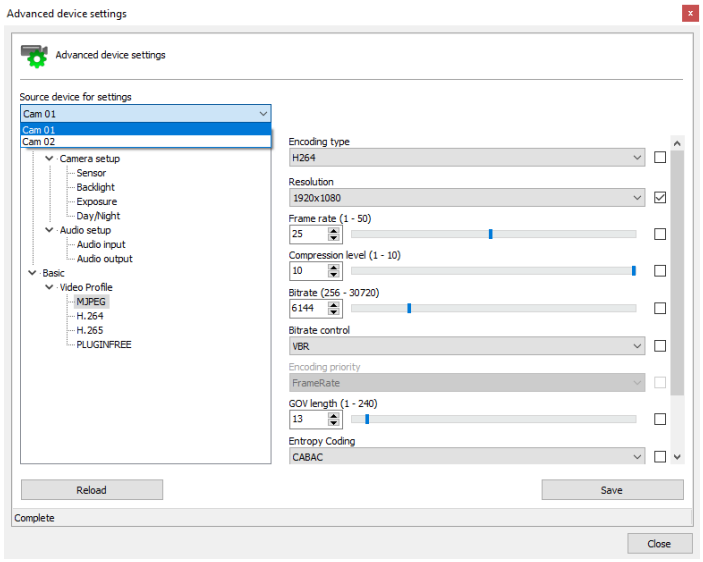
Or it can still be accessed through the selection of multiple cameras and the option "Advanced Device settings" with the right mouse button click on the selected cameras:



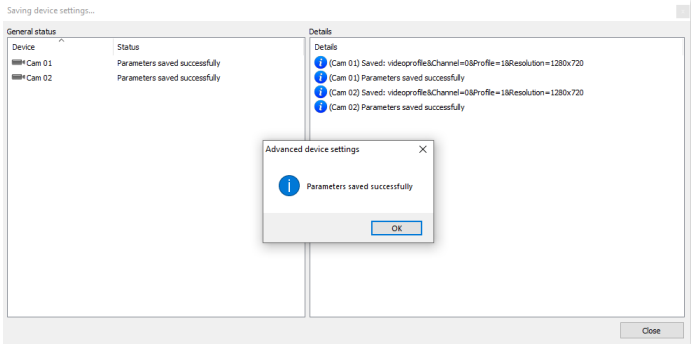
© 2002 - 2024 by Digifort. All rights reserved.

Camera settings will be downloaded (Only image, audio and streaming settings can be configured) and you can change the desired parameters.

In the upper combo you can choose a reference camera (from which the system will download the settings and display) and when saving the settings, the system will only save the changed parameters (which are identified through the selected checkbox next to the changed option) :

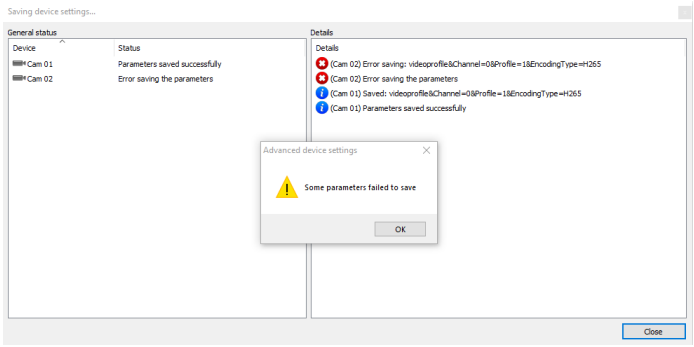


The system will then save the changed parameters for all cameras:



If any configuration fails to be saved, the system will inform you through an error message, however it will try to save all changed configurations. A setting may fail to be changed if the camera does not support the parameter (When a parameter is being recorded from multiple cameras at the same time):

© 2002 - 2024 by Digifort. All rights reserved.



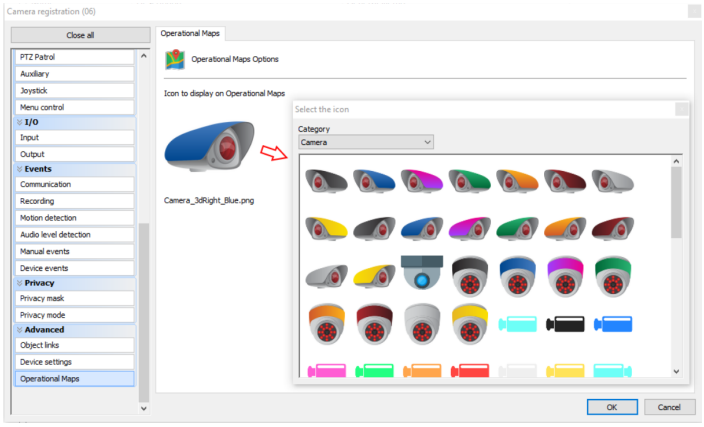
Dica

You can select all cameras that have the same configuration driver as the selected camera through the shortcut **CTRL + S**, thus being able to change all of them simultaneously.

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 chapter Operational Maps .

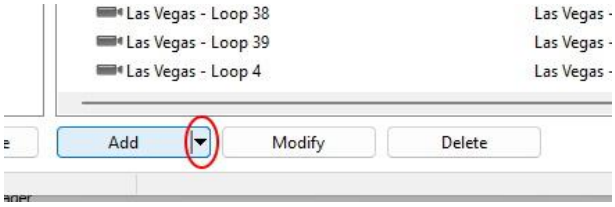
Just click on the camera image and choose the new image as shown in the image below:



6.1.10 Multi-Channel Device Registration

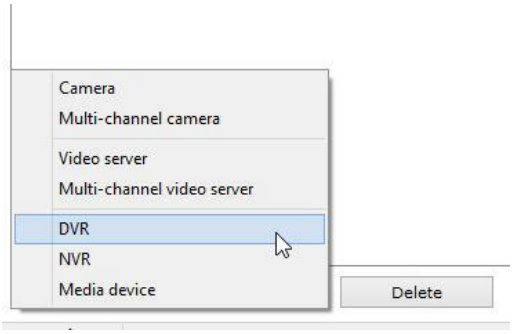
The system enables easy registration for multi-channel devices such as: DVRs, NVRs, Video Servers, Cameras with multi-lenses, etc.
This option allows all channels on a device to be registered at once.

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



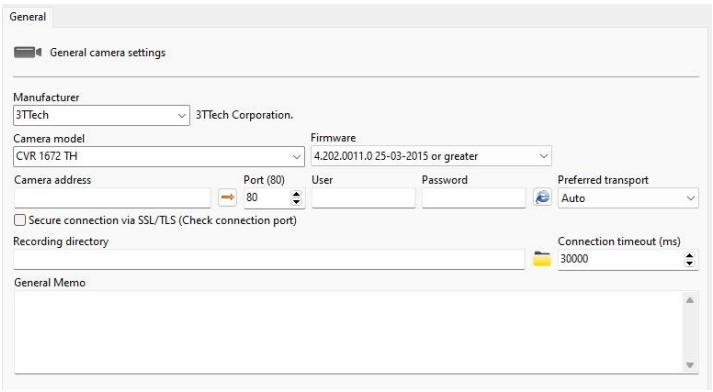
© 2002 - 2024 by Digifort. All rights reserved.

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



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

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

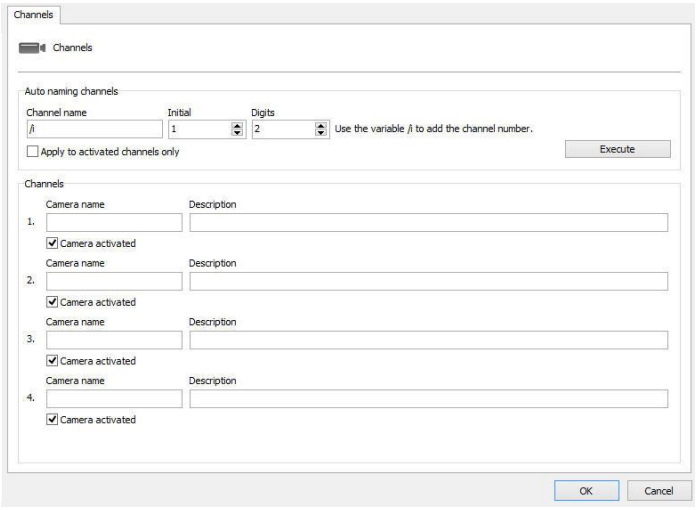


On this screen, the basic information of the equipment must be filled in, as already discussed in the General topic of camera registration

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

The following screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.

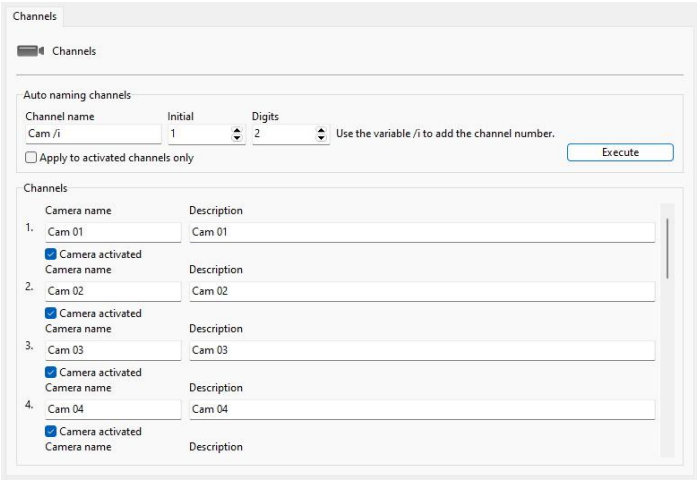


The following options will be available:

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

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

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



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

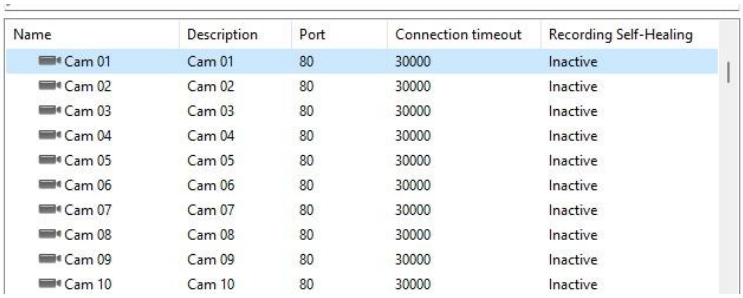
Note

The device name cannot be changed after registration.

© 2002 - 2024 by Digifort. All rights reserved.

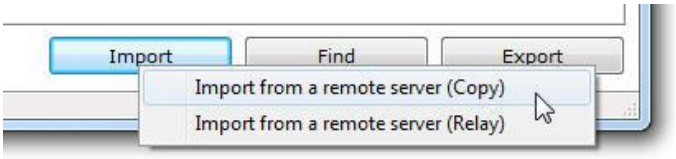
Recording folders will be created with the chosen names for the channels within the chosen root folder.

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



6.1.11 Import Cameras From Other Servers

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



Import cameras from a remote server (copy): When the import is made as a copy, the settings will come exactly as from the imported server. An important example is the recording unit: if on the source server the cameras are recording in the E: directory and on the current server this unit does not exist, the camera will not record.

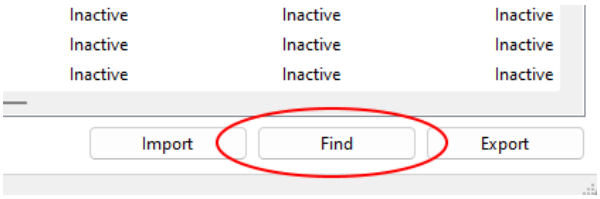
Import cameras from a remote server (relay): When the import is done as a relay, the current server will register the cameras with the Digifort RTSP Server driver, which in this case will fetch the images from the source server.

See the Object Import topic for more information on how to import objects.

6.1.12 Finding and Registering Cameras Automatically

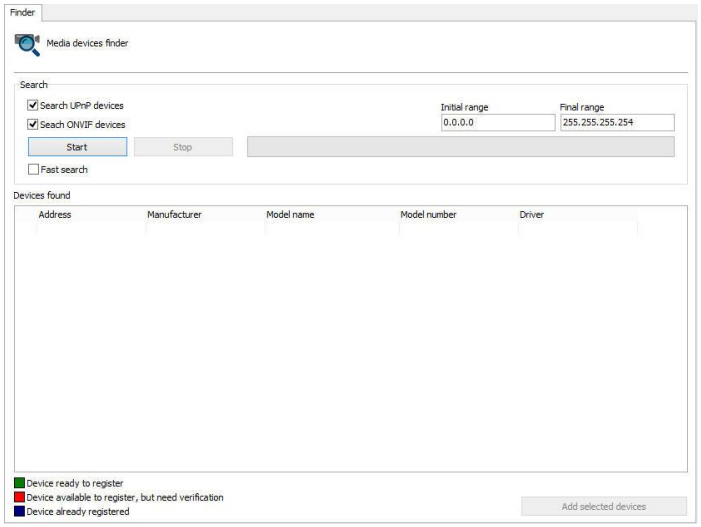
The system has the option for cameras that support the UPnP and ONVIF protocols to be located and registered automatically.

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



© 2002 - 2024 by Digifort. All rights reserved.

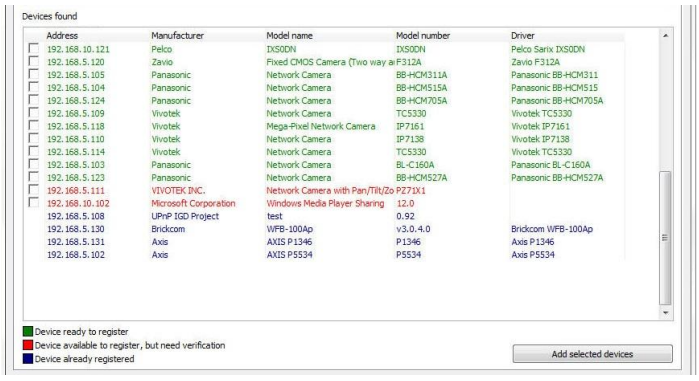
The following screen will be displayed:



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

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

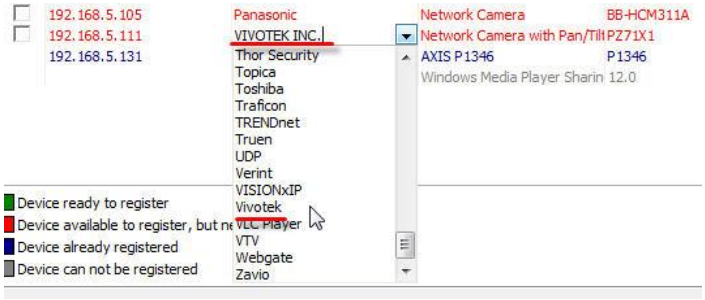
To start the search, click **Start** and the message **Wait, locating devices (wait, location devices)** will appear while the equipment is being located. Once found, the equipment will be listed as shown in the figure below:



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

© 2002 - 2024 by Digifort. All rights reserved.

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



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

There are two ways to register the equipment found.

6.1.12.1 Single Camera Registration

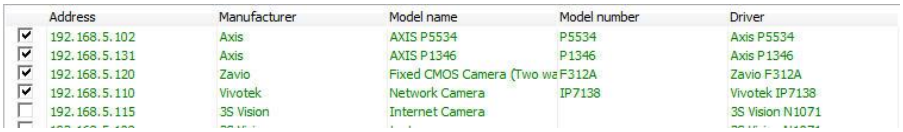
Select a device using the selection box as shown in the figure below:

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

6.1.12.2 Multiple Camera Registration

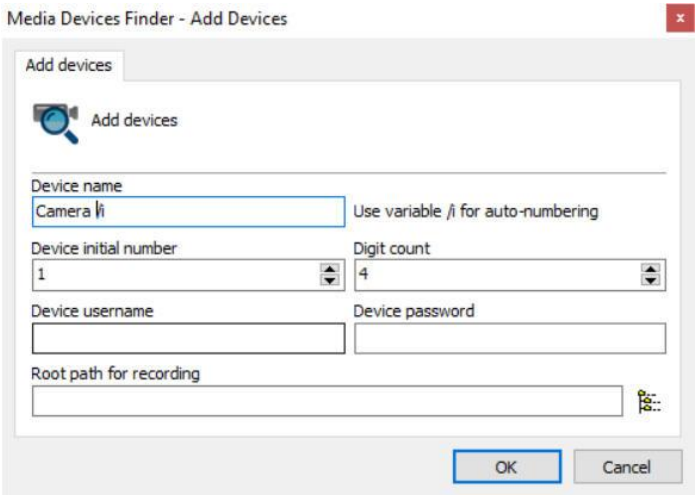
This feature can register several cameras at the same time with sequential numbers. To start, select several devices using the selection box as shown in the figure below:



Address	Manufacturer	Model name	Model number	Driver
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 equipment, click the **Add Selected Equipment** button and the following screen will appear:

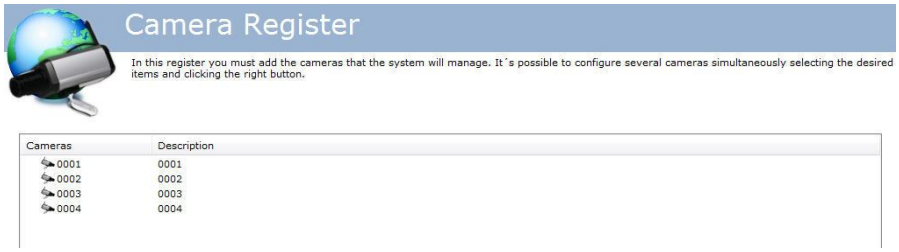
© 2002 - 2024 by Digifort. All rights reserved.



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

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

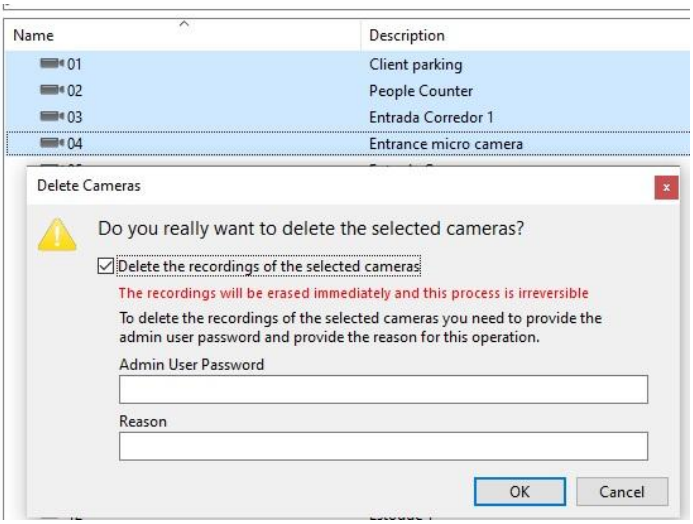
After registering the various cameras, their respective status will automatically change to **BLUE (Camera already registered)**. This way, the cameras were successfully registered as shown in the image below:



6.2 How to Delete a Camera

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

© 2002 - 2024 by Digifort. All rights reserved.

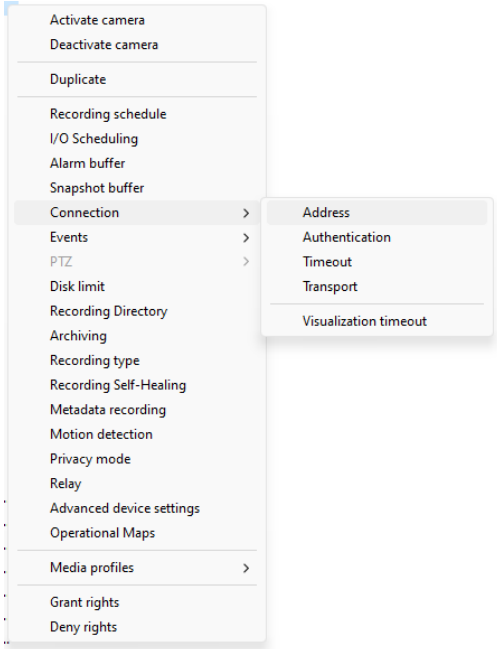


- **Delete recordings from selected cameras:** With this option checked, the system will delete recordings from the cameras that are being deleted. For security reasons, the **Admin** user password must be provided for this process.
  - **Admin User Password:** Provide the **Admin** user password to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

6.3 How to Change Parameters for Multiple Cameras Simultaneously

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

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



© 2002 - 2024 by Digifort. All rights reserved.

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

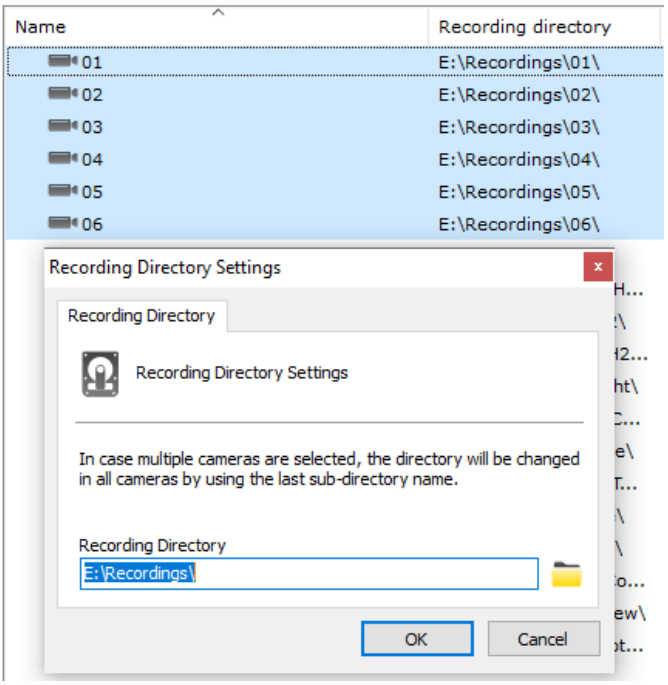
6.3.1 Recording Directory

Allows changing the recording root directory of multiple cameras simultaneously.

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

Important

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



6.3.2 Add, Modify or Delete Media Profiles

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

Tip

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

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

© 2002 - 2024 by Digifort. All rights reserved.

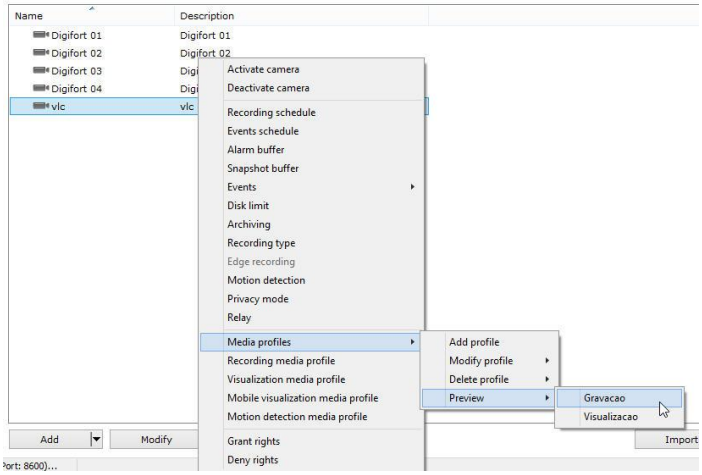
Camera 1
View Profile
Recording Profile
Mobile Profile

Camera 2
Recording Profile

Let's analyze the following hypotheses separately:

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

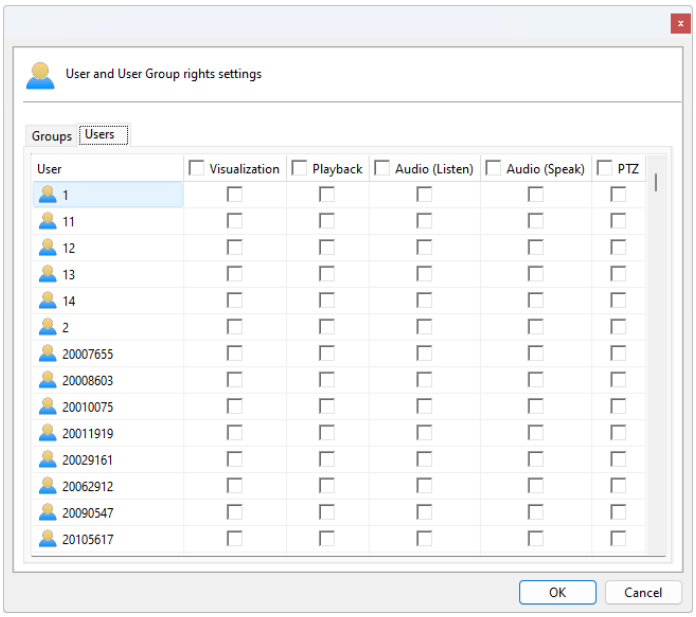
- You can also see the camera image from the list by clicking on Preview:



6.3.3 Grant and Deny User Rights

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

© 2002 - 2024 by Digifort. All rights reserved.



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

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

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

6.4 Camera Groups

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

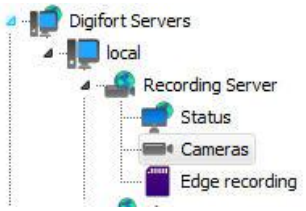
In the Surveillance Client, the groups will be part of the object list and the cameras belonging to the groups will be added below them.

The Surveillance Client offers great flexibility to work with groups:

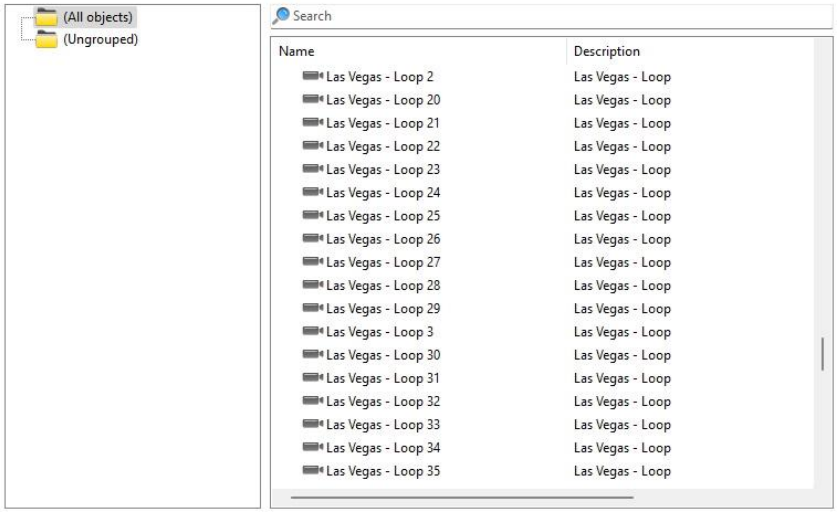
- You can drag and drop a group onto the screen and the cameras in that group will be added to the monitoring.
- To add the group's cameras and all cameras from all subgroups to the screen, simply press and hold the Shift button while dragging and dropping the desired group.
- You can drag and drop a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

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

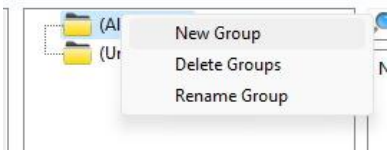
© 2002 - 2024 by Digifort. All rights reserved.



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



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



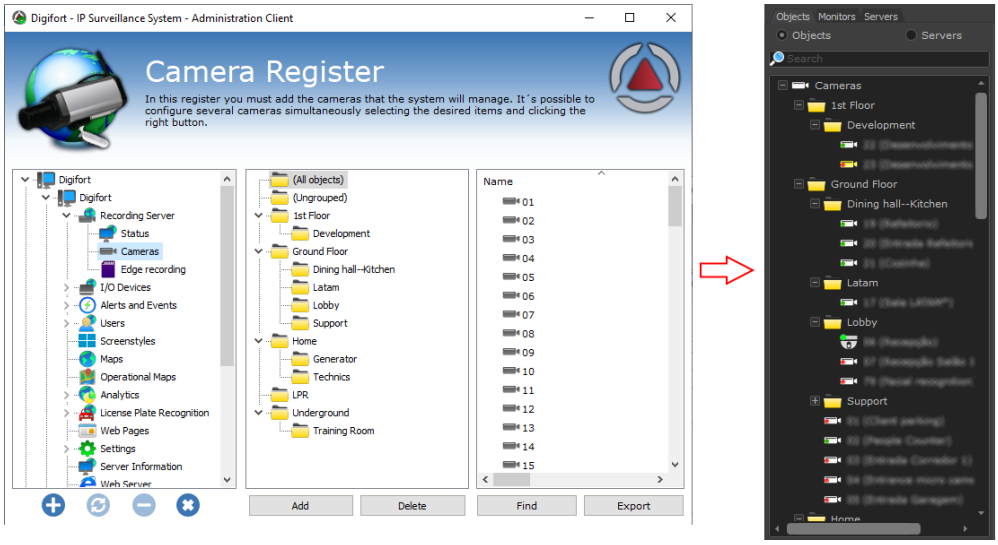
When clicking on the **Add** button, the system will ask for the name of the group to be created and then the group will be available in the list

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

© 2002 - 2024 by Digifort. All rights reserved.

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

Example of operation with the Surveillance Client:



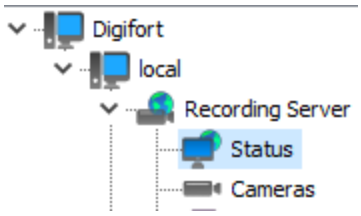
Tip

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

6.5 Monitoring Recording Server Status

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

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

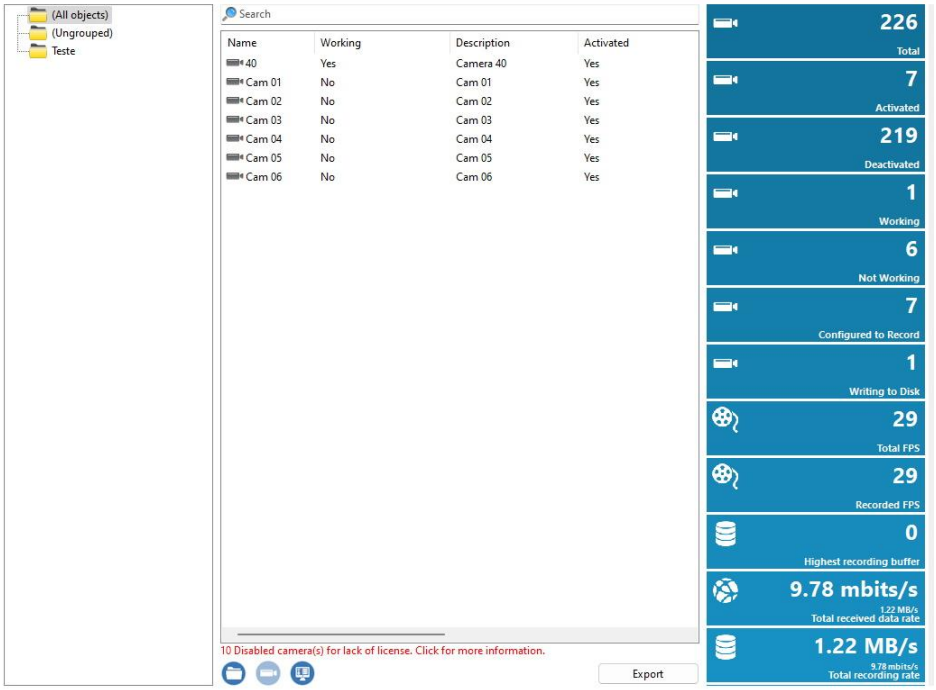


The status screen allows the selection of custom columns with new information to be displayed in the list (By right-clicking on the list header) and ordering by any column in the list and it is also possible to export the current data to a .CSV file.

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

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

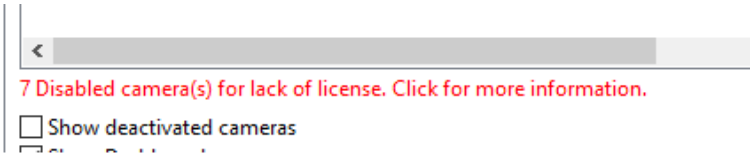
© 2002 - 2024 by Digifort. All rights reserved.



Details:

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

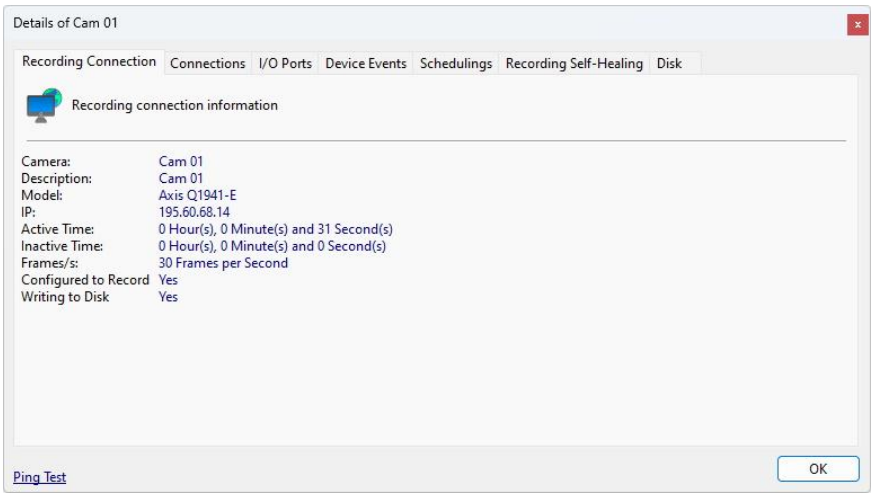
The system may also display a warning regarding objects deactivated due to a lack of available licenses:



6.5.1 Individual Camera Details

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

© 2002 - 2024 by Digifort. All rights reserved.

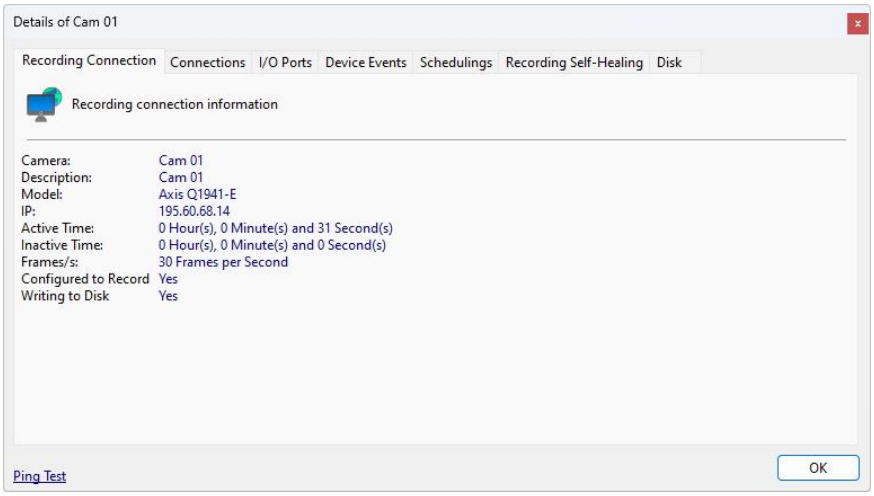


The above screen will be displayed with detailed camera information.

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

6.5.1.1 Recording Connection

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



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

© 2002 - 2024 by Digifort. All rights reserved.

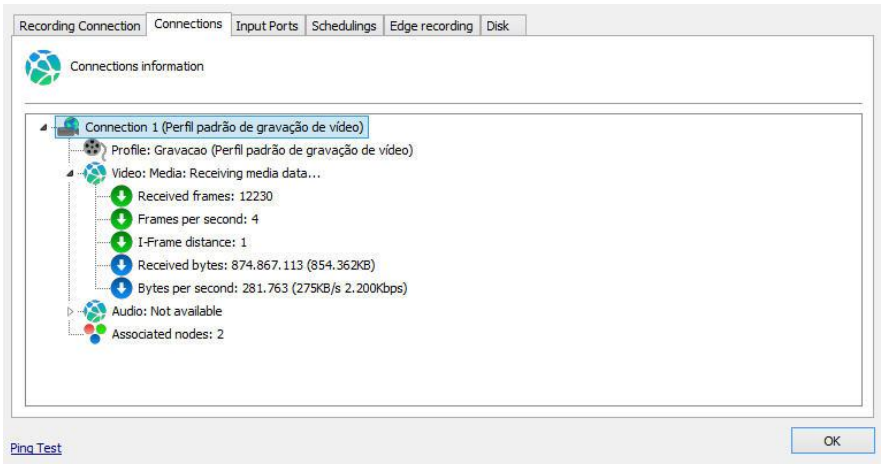
- **Writing to Disk:** Indicates whether the camera is currently recording to disk (Varies during recording by motion or event).

6.5.1.2 Connections

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

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

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

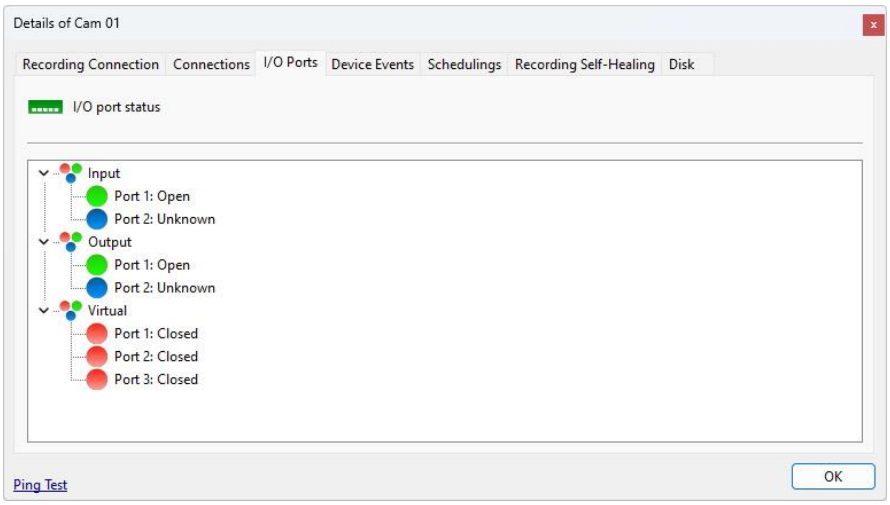


- **Profile:** Media profile associated with the connection. To learn what a media profile is see Media profiles
- **Frames Received:** Frames received from the camera with this connection since its activation or parameter change.
- **Frames Per Second:** Frames per second being received in real time.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

6.5.1.3 I/O Ports

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

© 2002 - 2024 by Digifort. All rights reserved.



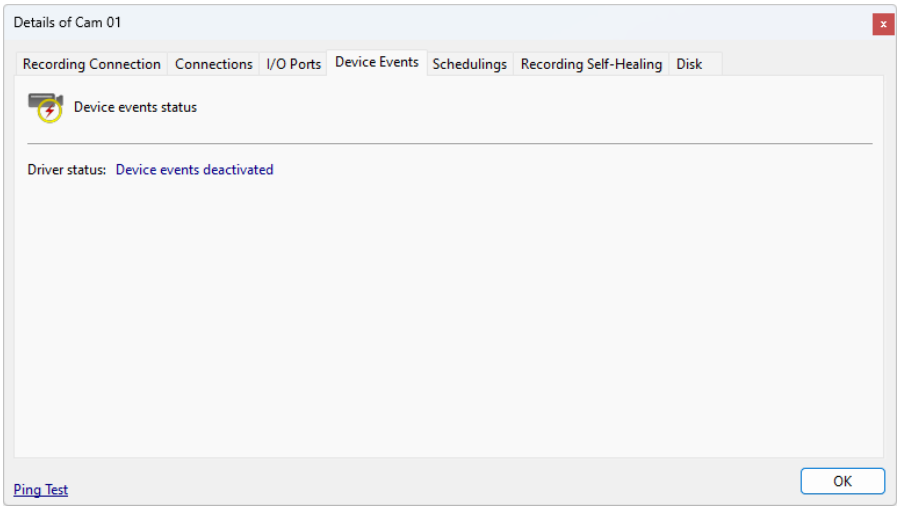
Each port will be represented by 3 statuses:

- **Green:** Port open
- **Red:** Port Closed
- **Blue:** Unrecognized state

To learn how to configure alarms, see the chapter I/O.

6.5.1.4 Device Events

This screen provides information about the device event driver.



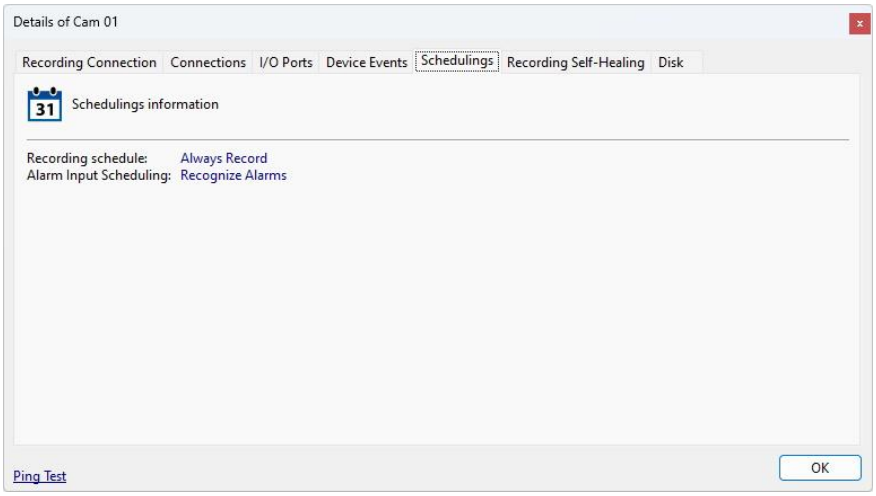
6.5.1.5 Schedulings

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

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

© 2002 - 2024 by Digifort. All rights reserved.

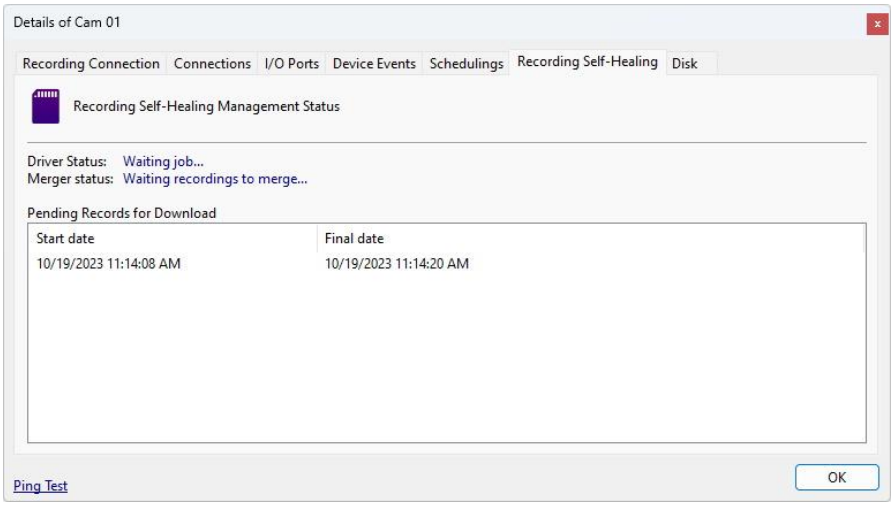
To access this feature, click on the **Schedulings** tab, as shown in the figure below:



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

6.5.1.6 Recording Self-Healing

On this screen, you can follow the Recording Self-Healing progress statuses



During the self-healing process, you can see the following statuses:

- **Downloading recordings:** Downloading recordings from the desired camera
- **Download of recordings completed**: Completed downloading videos from camera
- **Combining recordings:** Combining the downloaded recordings with the main recordings
- **Engravings merged successfully**: End of self-healing process

In the List of Pending Records for Download you can check all created self-healing records that have not yet been processed. You can delete records by clicking on the item and pressing the **Delete** button on the keyboard.

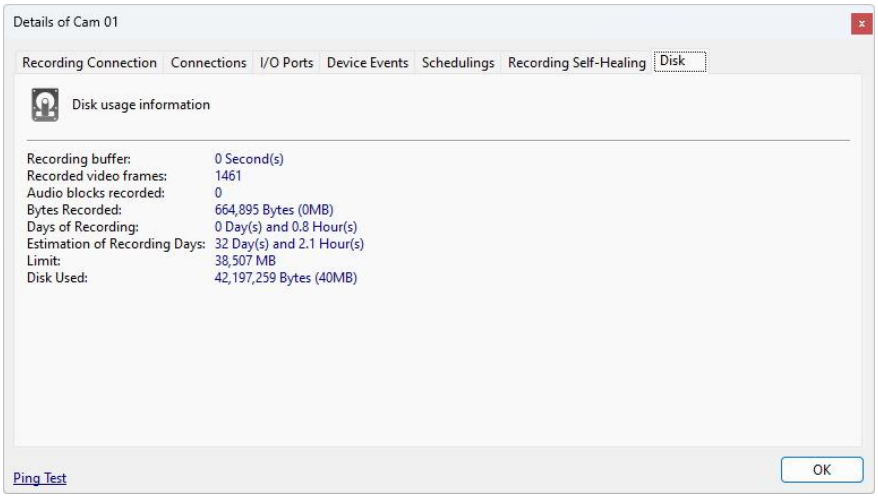
To learn more about self-healing, see the Self-Healing chapter

© 2002 - 2024 by Digifort. All rights reserved.

6.5.1.7 Disk

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

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

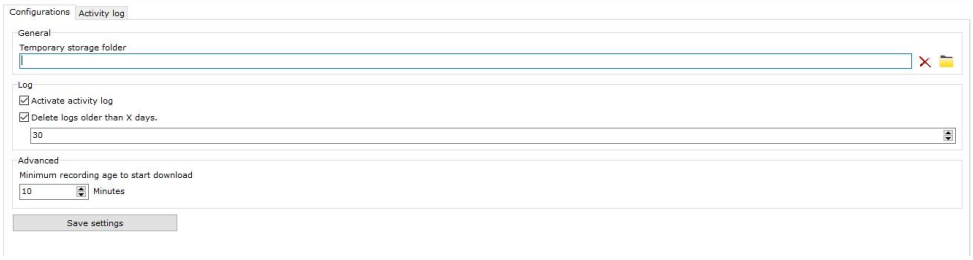


- **Recording Buffer:** Current size of the Recording Buffer. A high value (above 5 seconds) may mean disk performance problems.
- **Recorded Video Frames:** Total number of video frames recorded since activation or parameter change.
- **Recorded Audio Blocks:** Total number of audio blocks recorded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

6.6 Edge Recording

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

© 2002 - 2024 by Digifort. All rights reserved.

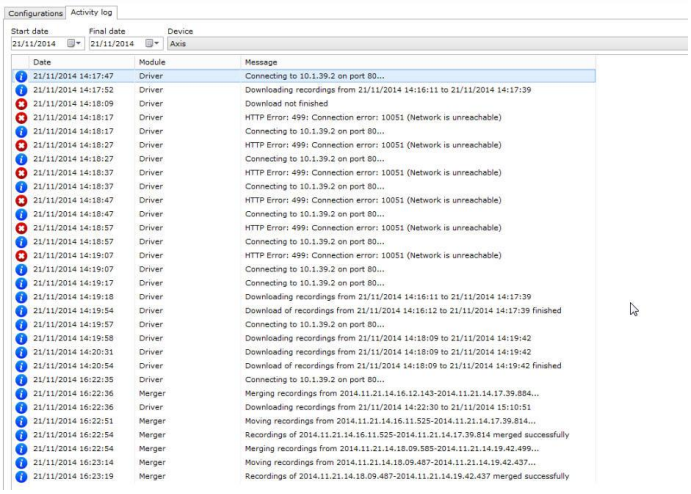


In the **Settings** tab we have the following options:

- **Temporary Storage Folder:** Choose a directory where the recordings downloaded from the cameras will remain until they are combined with the main recordings
- **Activate Activity Log:** Enables logging that records Edge Recording activities
- **Delete Logs Older Than X days**: Deletes edge recording logs older than configurable X days.
- **Minimum Download Time:** The system will wait until the end time of this recording is at least X minutes to start the download, so that the system gives enough time for the camera to close the recording file.

6.6.1 Activity Log

In the **Activity Log** tab, we can search for records related to edge recording actions:

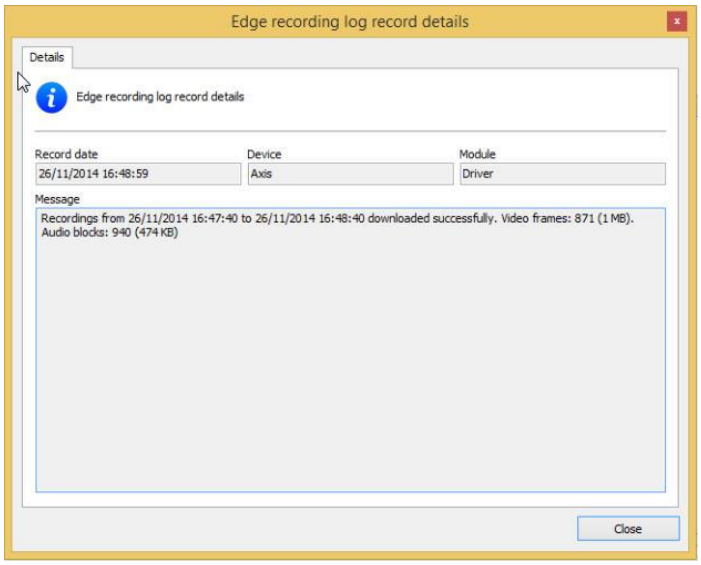


On this screen it is possible to view logs of:

- **Server connections with the camera.**
- **Connection errors.**
- **Recording download process.**
- **Completed recording download process.**
- **Combining recordings started.**
- **Combination completed successfully.**

It is possible to see the detail of a record with a double click:

© 2002 - 2024 by Digifort. All rights reserved.



To learn more about edge recording see chapter Self-Healing

© 2002 - 2024 by Digifort. All rights reserved.

Chapter VII

7 I/O Devices

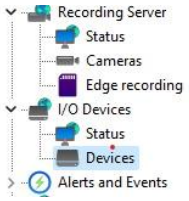
The system allows the management of external I/O devices. These devices are usually network-controlled alarm boards and, like some cameras, have alarm inputs and outputs that can be monitored through the system.

I/O devices are usually installed in places where there are no cameras or the installed cameras do not have alarm input and output ports.

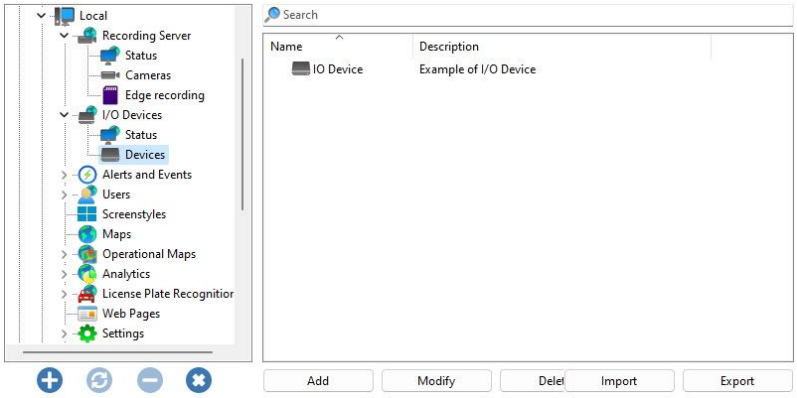
They can be used for the automation of an environment, attaching sensors and panic buttons to their entrance doors, among other devices, and sirens, electric locks and lamps to their exit doors, among other devices.

7.1 How to access the register of I/O Devices

To access the I/O Devices register, click on the **Devices** item within **I/O Devices**, as shown in the figure below:



Once this is done, the register of I/O Devices will be displayed on the right, as shown in the figure below:

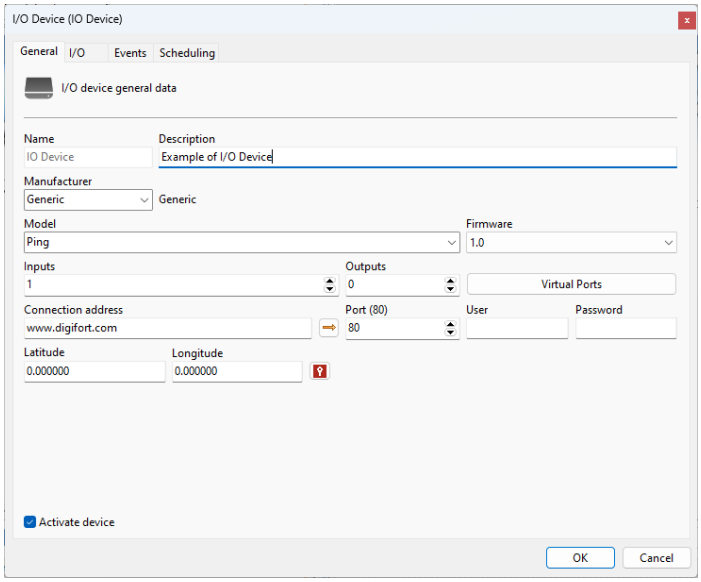


7.1.1 How to add an I/O Device

To add an I/O Device, click **Add**. To change or delete, select the desired I/O Device and click on the corresponding button.

© 2002 - 2024 by Digifort. All rights reserved.

7.1.1.1 General



- **Name:** I/O Device identification name. After the device is included in the system, the name cannot be changed, as it will be for internal use by the system.
- **Device Description:** Brief description of the I/O Device.
- **Manufacturer:** Select the I/O Device manufacturer.
- **Device Model:** Select the device model.
- **Firmware:** Select the supported firmware version.
- **Inputs:** Select the number of alarm input ports the device has.
- **Outputs:** Select the number of alarm output ports the device has.
- **Virtual Ports:** Allows configuration of virtual ports for this device.
- **Connection Address:** Enter the IP connection to the I/O Device.
- **Arrow**: Initiates ping command to the device.
- **Port:** Enter the port to connect to the I/O Device. The default port used for integration will be displayed in parentheses.
- **User:** Enter the I/O Device authentication user.
- **Password:** Enter the I/O Device authentication password.
- **Latitude and Longitude:** Coordinates of where the I/O Device is located.
- **Activate Device:** Enables or disables the I/O Device.

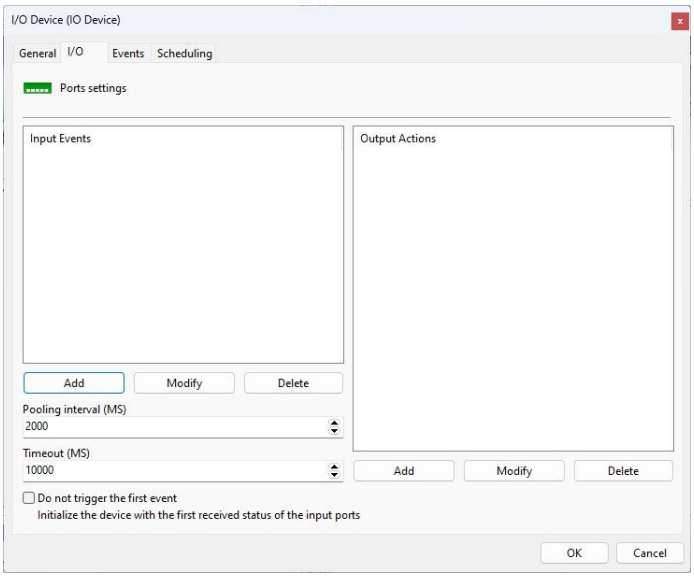
Important

To find out the IP and connection port, username and password, consult the I/O Device instruction manual.

7.1.1.2 IO Control

It is in this area that the operation of the I/O device will be configured. To access these settings, click on the **I/O** tab, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

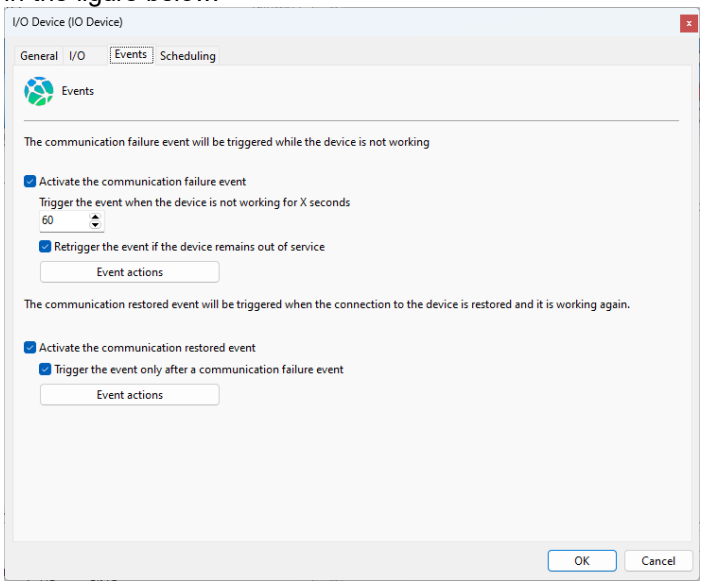


The settings for Input Events and Output Actions are exactly the same as those for camera registration. See the topic How to configure camera I/O for details on how to configure the I/O of I/O devices

7.1.1.3 Events

As with cameras, Digifort also controls the operating state of I/O Devices, providing notification functions in case the equipment stops working for some reason.

Digifort can notify the administrator of communication failures with the I/O Device, which can be caused by a lack of energy in the place or signs of vandalism, for example. To access this feature, click on the Events tab, as shown in the figure below:



If you want to activate this notification, check the option Activate communication failure event and define the time for checking. This time defines the interval in which Digifort will check if there is connectivity with the device. Finally, click on Alarm Actions to define a set of actions that Digifort will take when this event occurs. To learn how to configure alarm actions see How to Configure IO Events

© 2002 - 2024 by Digifort. All rights reserved.

7.1.1.3.1 Communication Failure Event

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

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

To learn how to configure event actions see How to configure event actions

7.1.1.3.2 Communication Restore Event

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

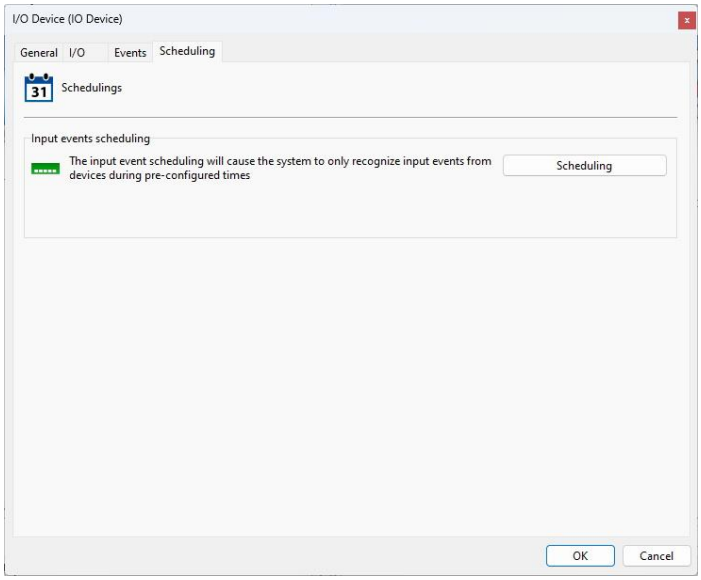
The system also allows events to only be triggered if a **communication failure event** for the same object has been triggered previously..

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

7.1.1.4 Scheduling

Scheduling makes it possible to configure times and days of the week in which events received by I/O Devices are processed. For example, a rule can be defined that events will only be processed during the night.

To access this resource, click on the **Scheduling** tab, as illustrated in the figure below:



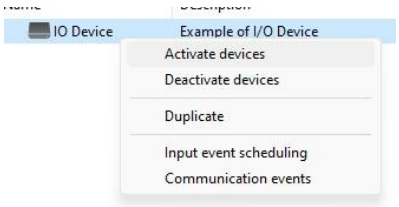
To configure the schedule, click the **Scheduling** button. The scheduling configuration is standard for all system scheduling screens, for further instructions, check the topic How to configure the recording schedule

© 2002 - 2024 by Digifort. All rights reserved.

7.1.2 How to Change Parameters for Multiple Devices Simultaneously

As already explained in the Multiple Object Configuration topic, the system allows the basic configurations common on all selected devices to be applied simultaneously.

To use this feature, select the desired devices and right-click, as shown in the figure below:

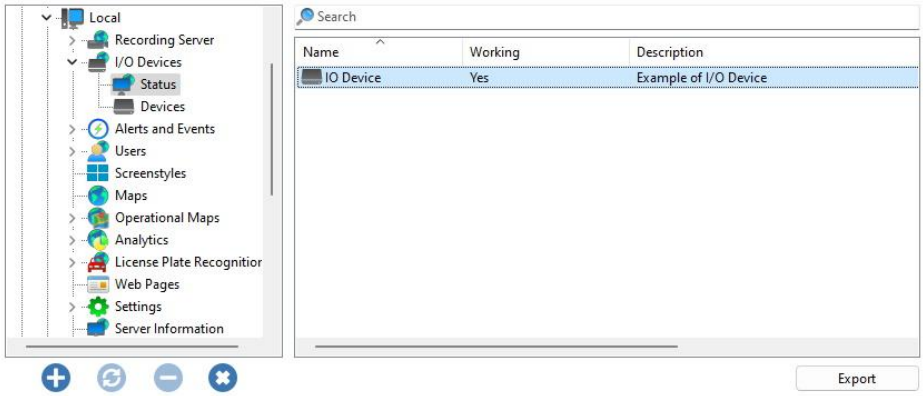


- **Activate Devices:** Activates selected devices, allowing their alarms to be managed.
- **Deactivate Devices:** Disables selected devices.
- **Duplicate:** Duplicates the registration of the selected device.
- **Input Event Scheduling:** Configures input event scheduling for selected devices. To learn how to use this feature, see I/O Control
- **Communication Events:** Configures communication events for selected devices. To learn how to use this feature, see Events.

7.2 Status

In the Status option you can check if the I/O Devices are working, Port Status and Scheduling.

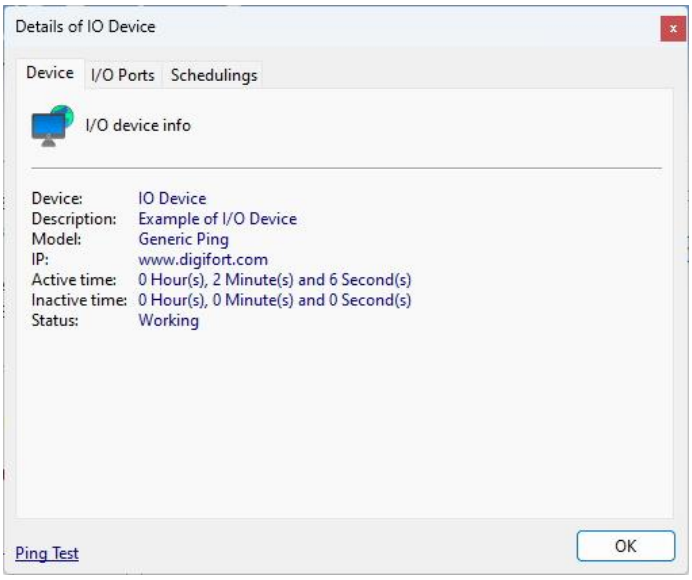
In the image below it is possible to identify which devices are working and not working:



7.2.1 Individual Device Details

To obtain more details about a device, simply double-click on the desired device and the following screen will appear:

© 2002 - 2024 by Digifort. All rights reserved.



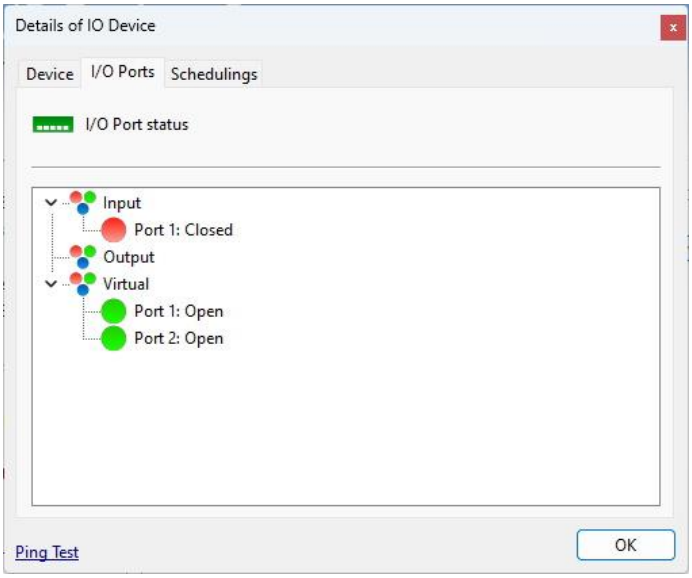
- **Ping Test**: Opens a window with the camera ping test.

7.2.1.1 General

- **Device**: Name of the selected device.
- **Description**: Device description
- **Model**: Device model
- **IP:** Device IP address
- **Active Time:** Device uptime since activation or parameter changes.
- **Inactive Time**: Device downtime. If the device is out of order, this is the total time it is out of order. Reactivating or changing the object's settings will reset this value. This value will be reset when the device returns to operation.
- **Status:** Indicates whether the equipment is working.

7.2.1.2 I/O Ports

This screen shows the alarm ports (input, output and virtual) of the I/O Device and their respective status



© 2002 - 2024 by Digifort. All rights reserved.

Each port will be represented by 3 statuses:

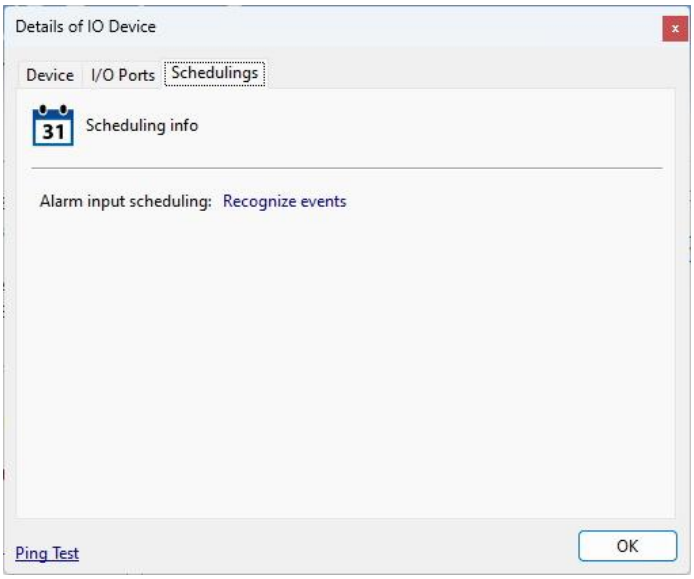
- **Green:** Port open
- **Red:** Port closed
- **Blue:** Unrecognized state

To learn how to configure alarms, see the I/O chapter.

7.2.1.3 Scheduling

This screen provides us with information about the current schedule type. The type of scheduling is defined by Event Scheduling. To learn how to define event scheduling, see the Event Scheduling topic.

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



- **Alarm Input Scheduling:** Provides the current status of the alarm input schedule

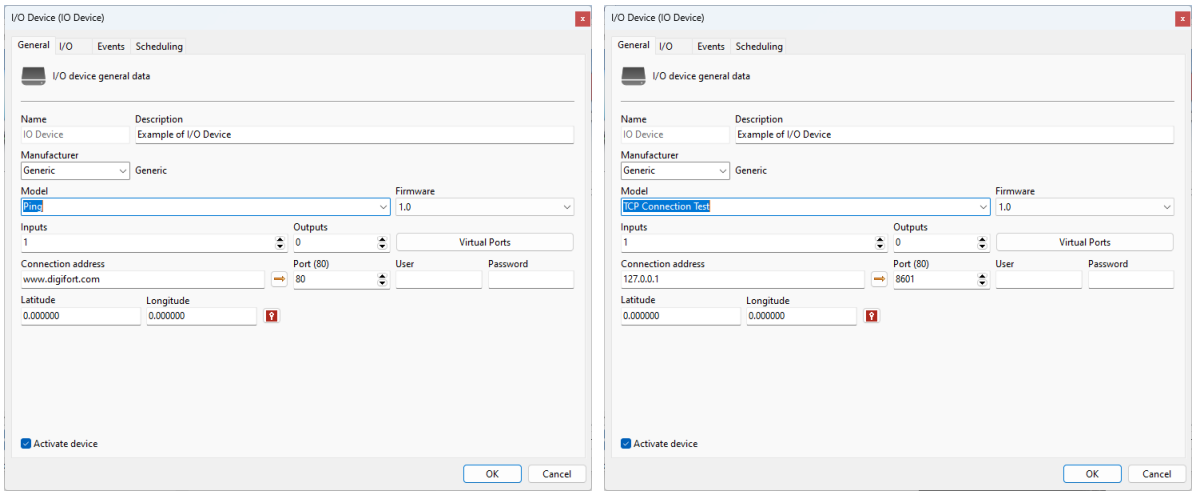
7.3 I/O driver for testing hosts

The system has a special "I/O Device" driver for monitoring hosts via **ping** or **TCP connection**.

Using the **Generic Ping** or **Generic TCP Connection Test** model in the I/O Devices register, it is possible to monitor any IP or host (for equipment monitoring, for example) and configure alarms and events when the host becomes offline. It is also possible to add the status of hosts to a Synoptic Map.

- The **Generic Ping** driver will use the ICMP protocol to test whether the host is up and running. This method is useful for testing any type of generic IP address.
- The **Generic TCP Connection Test** driver will test a host TCP port (specified in the settings). The system will constantly open and close connections to this port in order to check if it is accessible. This method is useful for testing not only whether a host is reachable, but whether a service the host is providing is reachable.

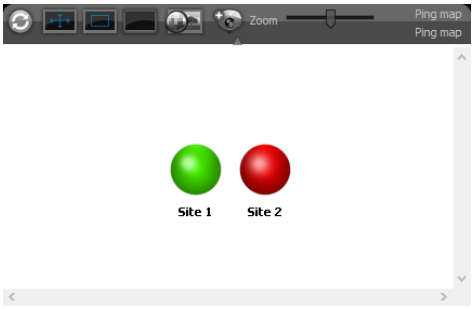
© 2002 - 2024 by Digifort. All rights reserved.



The driver has 1 input port, and this port will reflect the ping status. If the port is **closed**, the host is working, if the port is **open**, the host is not accessible.

The host out of order alarm can be configured through the Alarm Input Events (Using Port 1) or also through the Communication Failure and Communication Restoration events in the "I/O Device" Registration

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



© 2002 - 2024 by Digifort. All rights reserved.

Chapter VIII

8 Alerts and Events

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

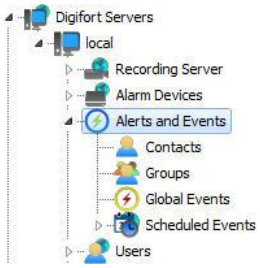
The alerts and events functions allow the system to send e-mails or SMS messages to a list of users previously registered in the system every time an event programmed by the administrator occurs. An event can be, among others, a communication failure between the camera and the server, a data recording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

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

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

8.1 How to Access Alerts and Events

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



8.1.1 How To Configure Contacts

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

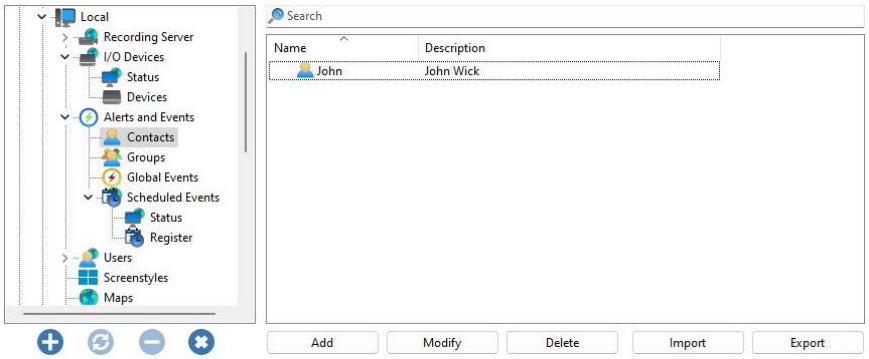
Contacts and contact groups are used for event action notification via email, SMS or Push Notification.

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

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

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

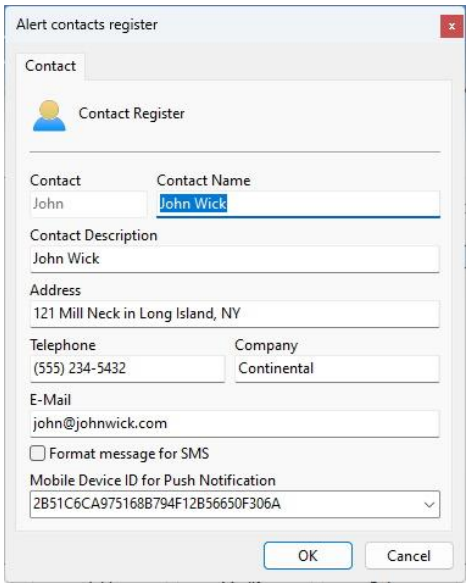
© 2002 - 2024 by Digifort. All rights reserved.



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

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 illustrated in the figure below:



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

© 2002 - 2024 by Digifort. All rights reserved.

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

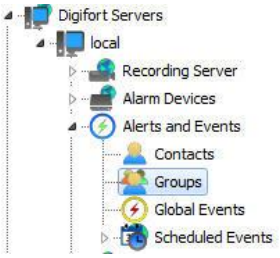
Note

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

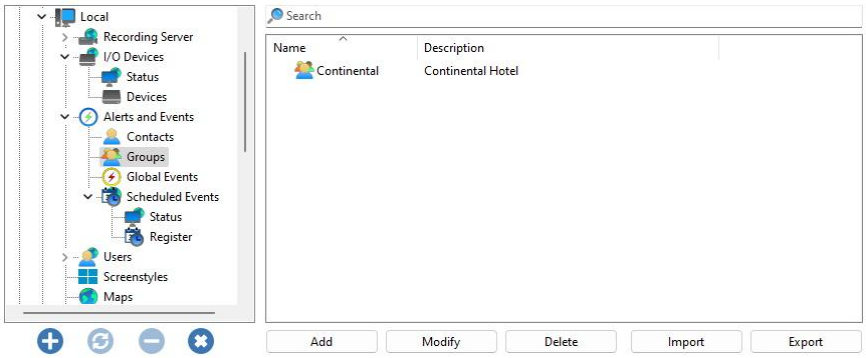
8.1.2 How To Set Up Contact Groups

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

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



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

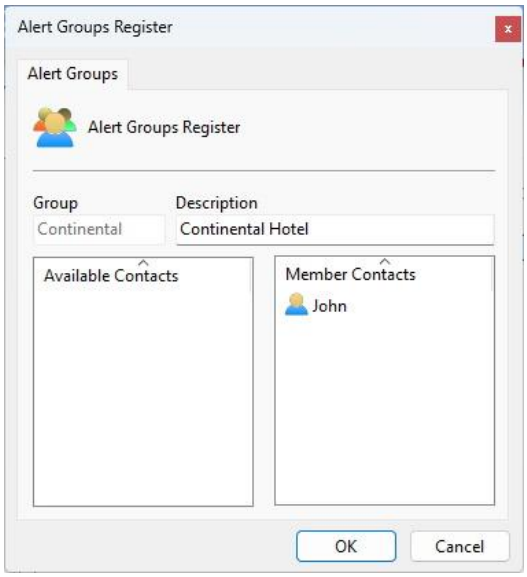


To add a contact group, click on the **Add** button. To change a contact group, select it and click on the **Change** button. To delete a contact group, select it and click **Delete**.

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 illustrated in the figure below

© 2002 - 2024 by Digifort. All rights reserved.



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

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

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

8.1.3 Global Events

Global events are powerful alarming and systems integration tools. Like any other event, global events can be used to trigger pre-programmed actions in the system, as well as enable or disable camera recording.

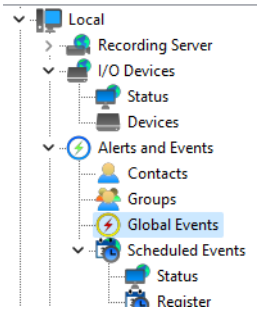
Global events can be triggered by users through the Surveillance Client or by external systems, thus allowing any application to activate an event in the system.

This chapter will only cover how to configure global events. For information on how to trigger a global event through an external application, consult the global events API.

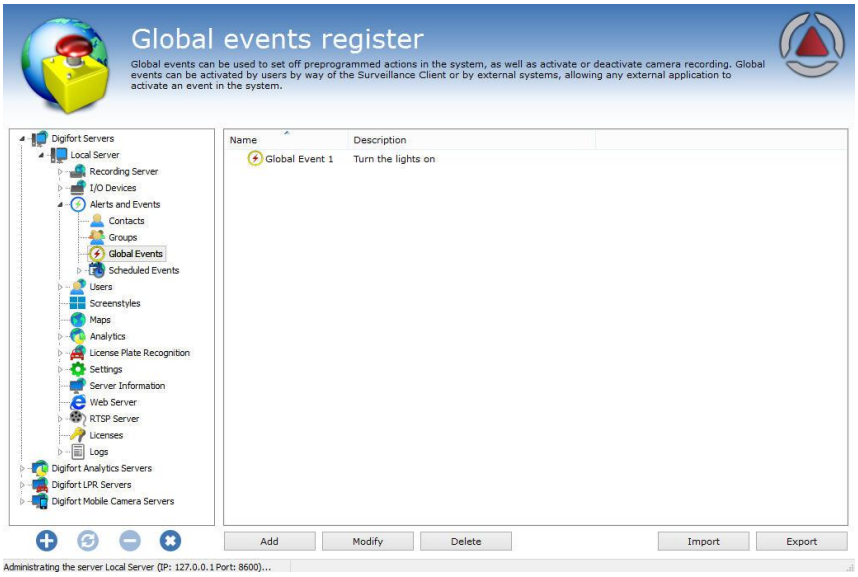
8.1.3.1 How To Access The Global Events register

To access the Global Events register, click on the Global Events item, as shown in the figure on the side.

© 2002 - 2024 by Digifort. All rights reserved.



Once this is done, the register of Global Events will be displayed on the right, as shown in the figure below.

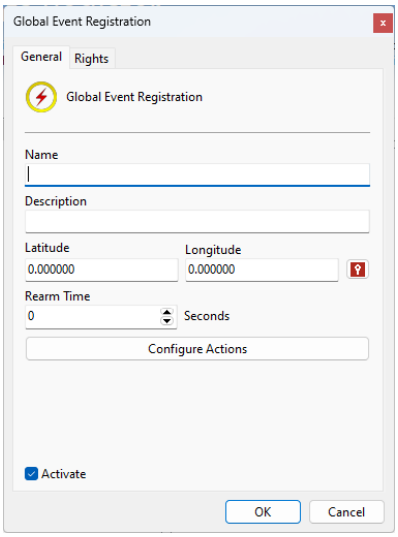


To add a global event, click **Add**. To change or delete, select the desired global event and click on the corresponding button.

8.1.3.2 How To Add A Global Event

By clicking on the **Add** button, as explained in the previous topic, the screen for adding global events will be displayed, as illustrated in the figure below.

© 2002 - 2024 by Digifort. All rights reserved.



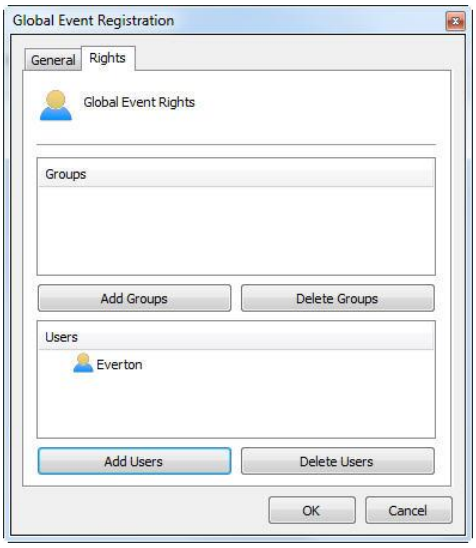
8.1.3.2.1 General

- **Name**: Global event identification name. The global event name will be used to trigger the event in the system.
- **Description**: Brief description of the global event.
- **Latitude and longitude:** Coordinates used to identify the location of the event on geo-referenced maps.
- **Rearm Time:** How many seconds the system should wait to process a new activation of the global event.
- **Activate**: Enables or disables the global event for use.

To configure the global event actions, click on the **Configure Actions** button. How action configuration works is described in the chapter How to configure event actions

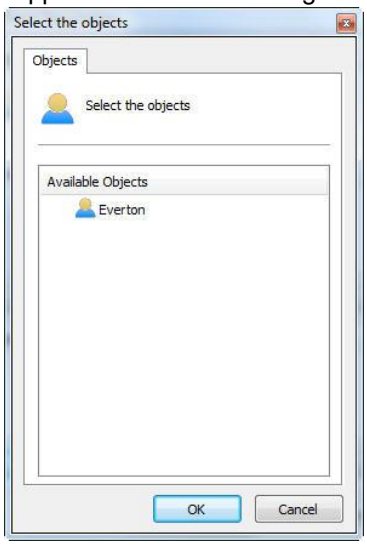
8.1.3.2.2 Rights

Global events may have access restricted to some system users. To assign user rights, click on the Rights tab, as shown in the image below:



© 2002 - 2024 by Digifort. All rights reserved.

To grant access rights to the desired users/groups, just click on Add Groups/Users and select them from the list of Groups/Users that will appear as shown in the figure.



Select Available User and click **OK**. The same rule applies to the group list.

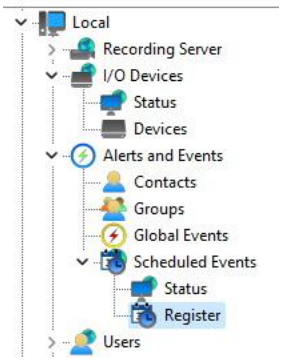
8.1.4 Scheduled Events

Scheduled events allow the user to create scheduled actions to perform some function on the system at specific dates and times.

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

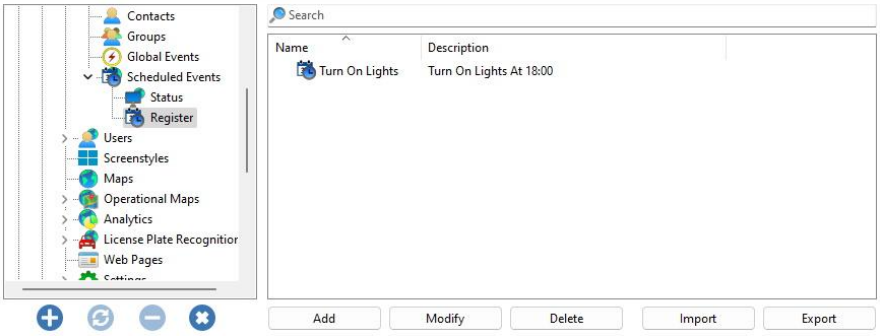
8.1.4.1 Registering Scheduled Events

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



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

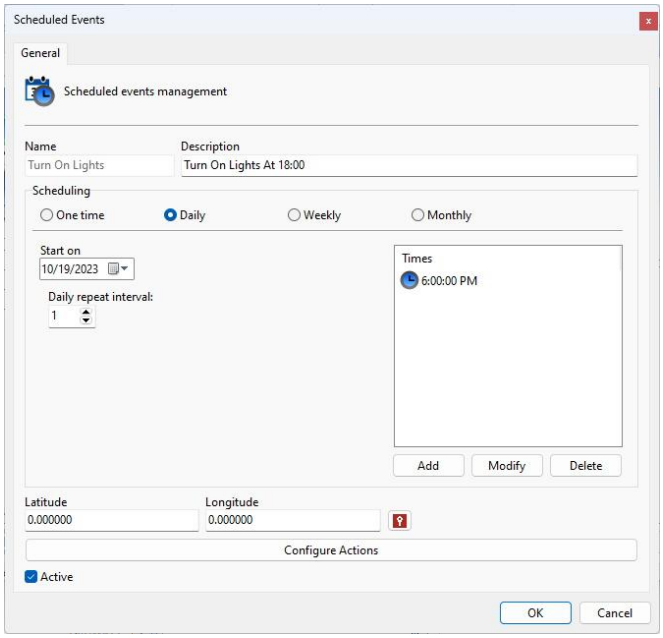
© 2002 - 2024 by Digifort. All rights reserved.



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

8.1.4.1.1 Adding Scheduled Events

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



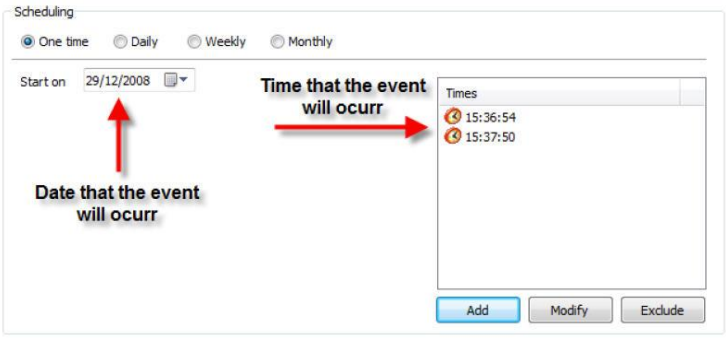
This screen provides the following configurations:

- **Name:** Enter the desired name for the event. This name will be the key for recognition in the system.
- **Description:** Desired description for the event to be registered.
- **Scheduling:** Type of scheduling to be done. The event can be activated only once, daily, weekly and monthly. Scheduling types will be explained later.
- **Times:** Screen where one or more times will be added for the event to be activated.
- **Latitude and Longitude:** Coordinates used to identify the location of the event on geo-referenced maps.
- **Configure Actions**: Click this button to configure the actions that the system will take when this event happens. To learn how to configure actions see How to configure event actions
- **Active:** Activates or deactivates the event.

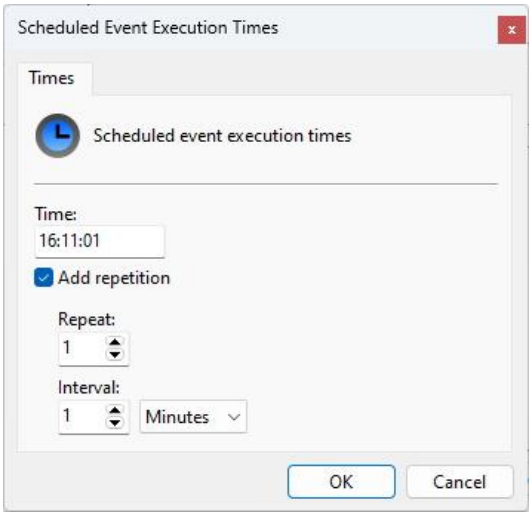
© 2002 - 2024 by Digifort. All rights reserved.

8.1.4.1.1.1 Scheduling Types

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



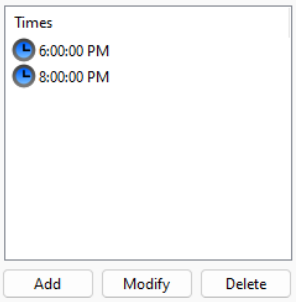
First select the date on which the event should take place, then click on Add in the timetable window and the following screen will be displayed:



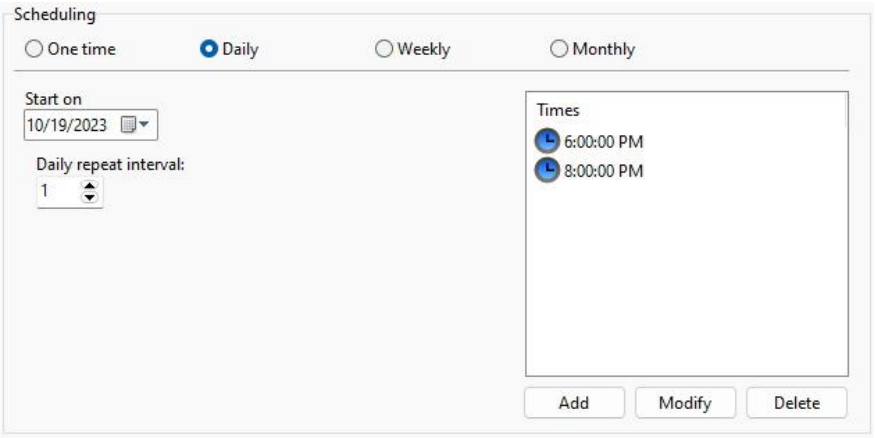
In this window, select the desired time for the execution of the event, if necessary, the event can be repeated every X minutes.

The time will appear on the screen as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



In this option the same previous configurations are presented except for the field shown in the figure below:

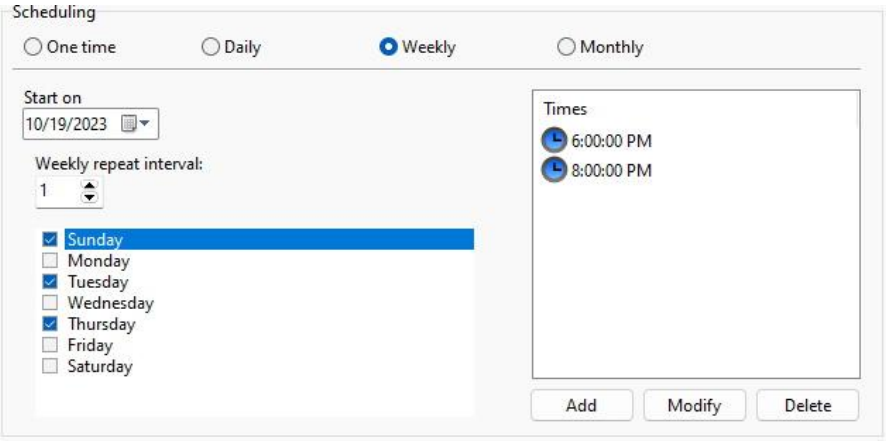


This field allows the event to occur every day (as shown in the figure) or every two days, every three days and so on, depending on the configured number.

- **Start on:** Event start date
- **Daily Repeat Interval:** Enter the interval between days that will trigger the event

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

The weekly scheduling options are shown in the figure below:



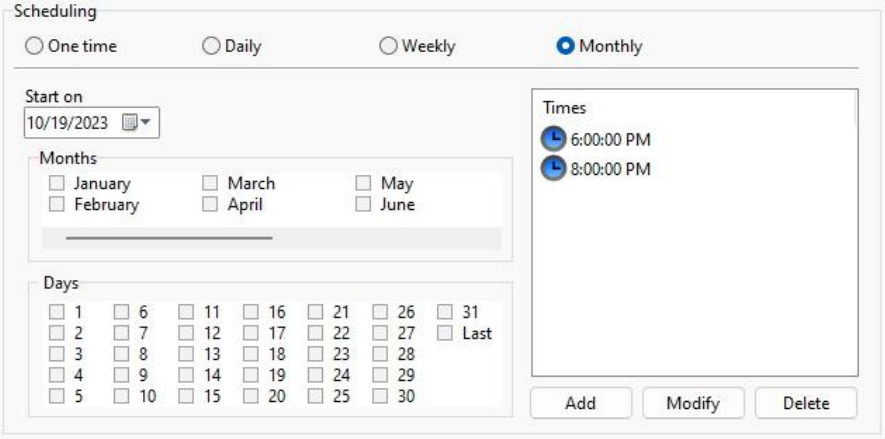
© 2002 - 2024 by Digifort. All rights reserved.

This screen provides the following functionality:

- **Start on:** Event start date. In the case of weekly scheduling, the software will adopt the current week as the initial one, that is, the next week will start on the next Sunday.
- **Weekly Repeat Interval:** Repeats the event every X configured number of weeks (every two weeks, every three weeks, etc.) on the desired days. Just tick the days that the event should occur.
- **Days Of The Week:** Select the days of the week on which the event will occur.
- **Times:** Add the times that the event should take place.

In the monthly settings it is possible to choose the desired months and days for a certain event to occur.

The month registration screen is shown in the figure below:



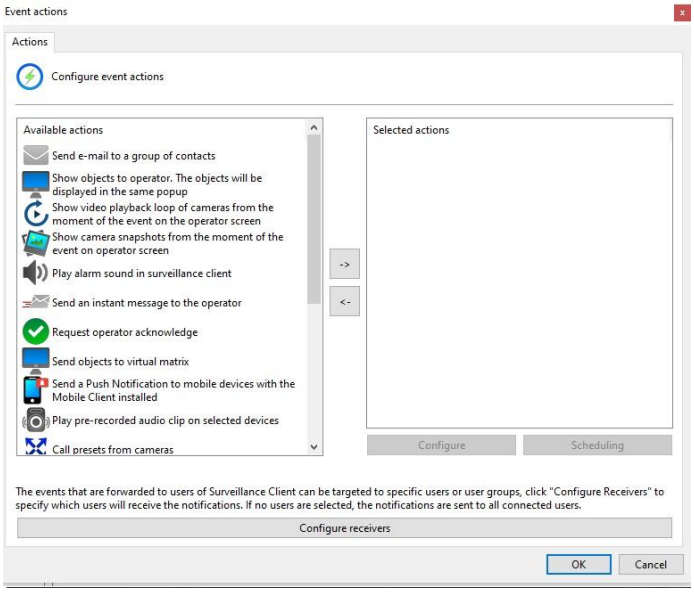
This screen provides the following functionality:

- **Start on:** Event start date. Select the desired date for the start of events.
- **Months:** Select the desired months in which the events will occur.
- **Days:** Select the desired days on which the event will take place.
- **Times:** Add the times that the event should take place.

8.2 How to configure event actions

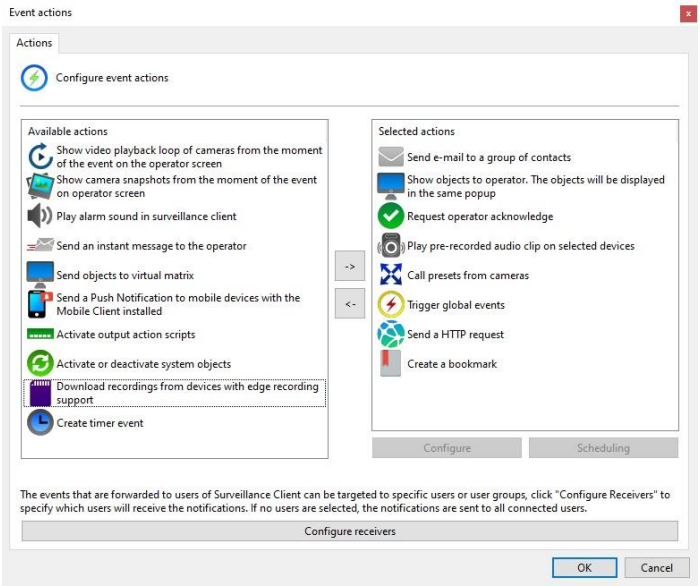
Several events require the configuration of event actions. To access these settings, click on Event Actions corresponding to the configuration performed. By clicking this button, the alarm configuration screen will be displayed as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



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

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



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

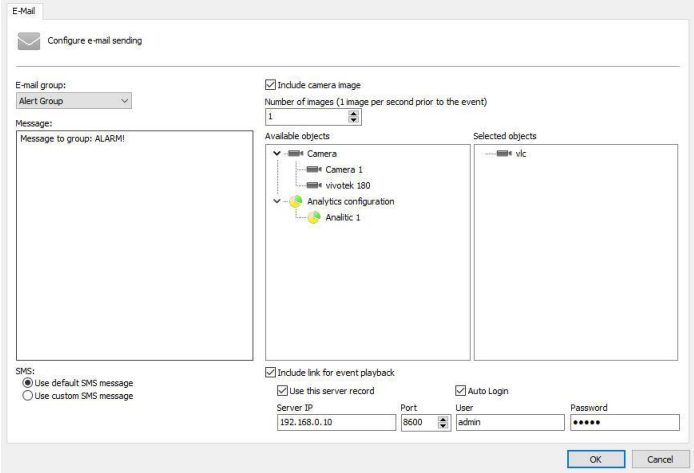
To schedule when an action will be performed, select the desired action from the list on the right (Selected Actions) and click the **Schedule** button. The event action scheduling screen works like the previously discussed recording scheduling screen, with the difference that the selection options will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

© 2002 - 2024 by Digifort. All rights reserved.

be to Enable or Disable the action. To learn how to configure the schedule, see How to configure the recording schedule

8.2.1 Send an email to a group of people when an alarm occurs

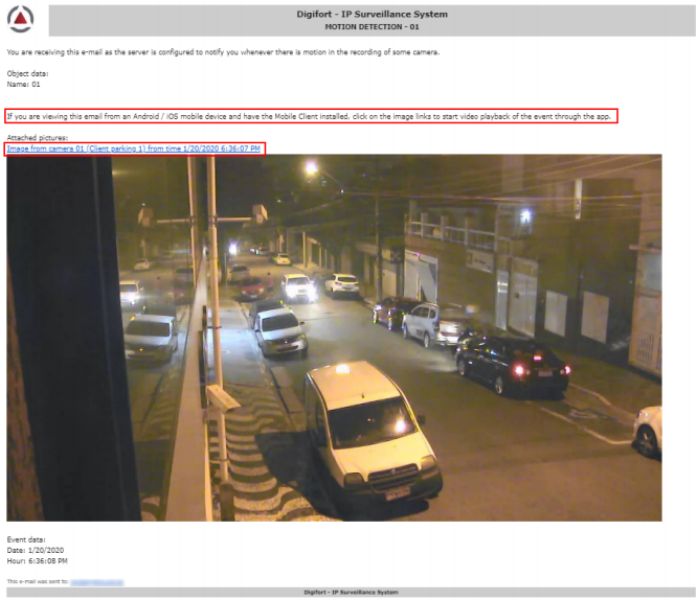
Sends a notification email to an alert group when an event occurs.



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

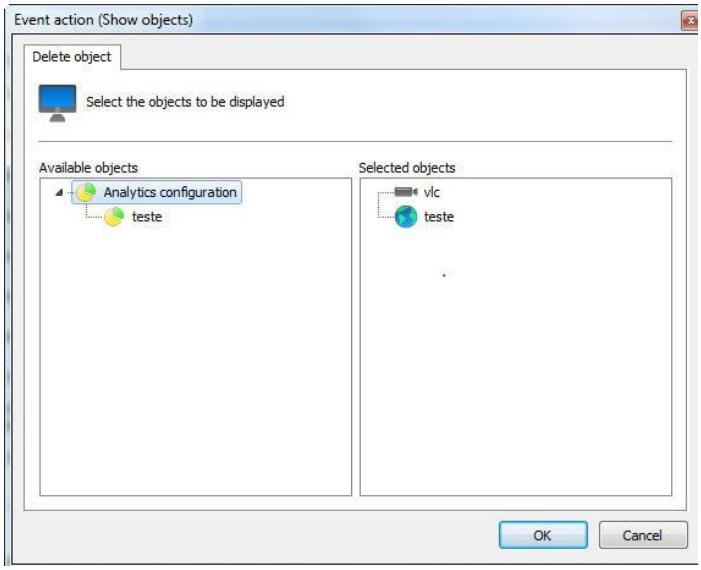
© 2002 - 2024 by Digifort. All rights reserved.

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



8.2.2 Display images from cameras on the operator screen

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



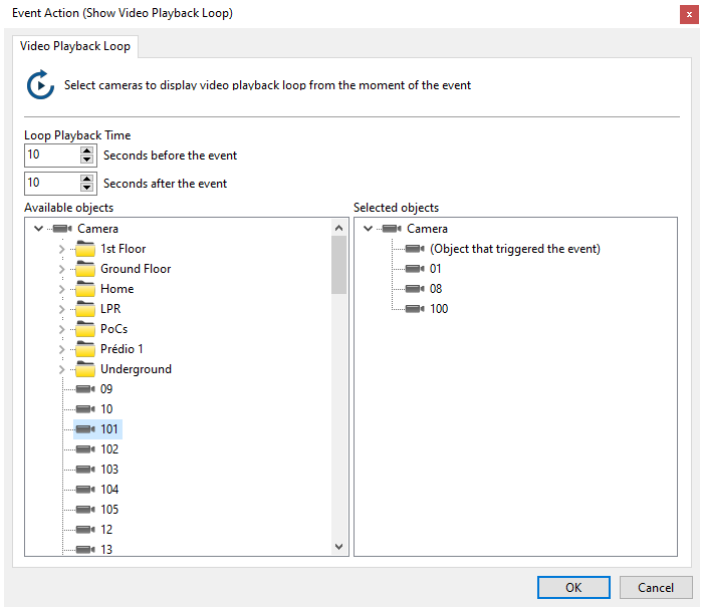
To select the objects to be displayed on the operator screen, select the desired objects from the list of available objects and drag them to the list of selected objects.

© 2002 - 2024 by Digifort. All rights reserved.

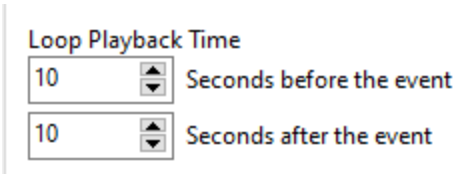
To remove objects to be displayed on the operator screen, select the desired objects from the list of selected objects and drag them to the list of available objects. You can also remove objects from the list of selected objects by double-clicking the desired object.

8.2.3 View a looped recorded video on the operator screen

Displays recorded video in a loop over a predetermined period from any camera in the system on the operator's screen in the Surveillance Client in a popup. You can select multiple cameras, and if more than one camera is selected, an automatic view will be created. To learn about views see the Surveillance Client manual.



To select how much pre and post alarm recording time should be displayed, simply select in the fields on the top left side of the screen:



In the example above, the system will display a 20-second loop of video, from 10 seconds before the event occurs to 10 seconds after the event triggers.

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

To remove cameras from being displayed on the operator screen, select the desired cameras from the selected cameras list and drag them to the available cameras list.

© 2002 - 2024 by Digifort. All rights reserved.

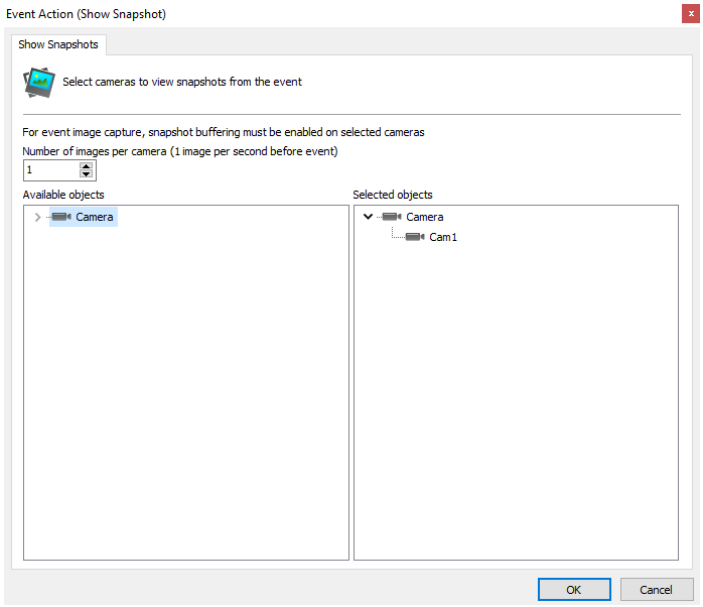
8.2.4 Display snapshots of cameras from the moment of the event on the operator's screen

Displays a snapshot of the moment of the event from any camera in the system on the operator's screen in the Surveillance Client in a popup. You can choose multiple cameras, and if more than one camera is selected, an automatic view will be created. To learn about views see the Monitoring Client manual.

You will also be able to choose snapshots of Analytics Configurations. Analytics snapshots will contain the rendered metadata along with the camera image.

Important

For this feature to work, you must enable Snapshot Buffer for the selected cameras



You can choose multiple snapshots of the same objects (1 snapshot per second before the event). To select the number of snapshots per camera (how many seconds prior to the event 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 objects to be displayed on the operator screen, select the desired objects from the list of available objects and drag them to the list of selected objects.

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

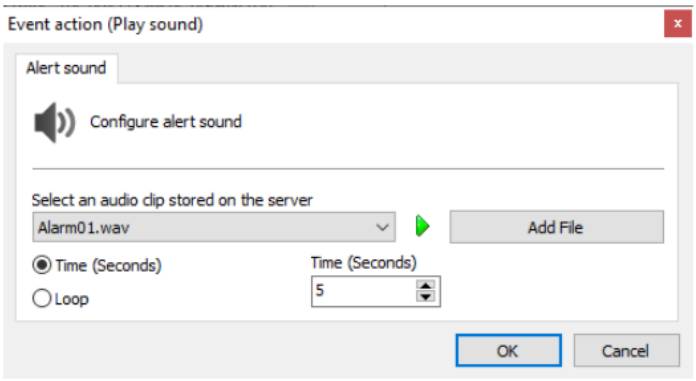
8.2.5 Play an alarm sound in the Surveillance Client

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

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

© 2002 - 2024 by Digifort. All rights reserved.

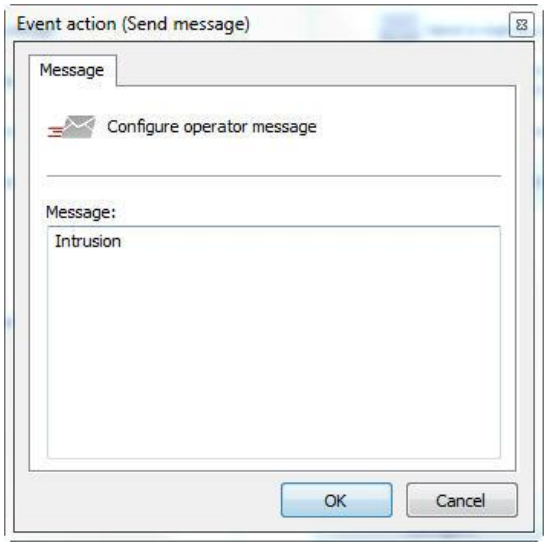
Select the desired alert sound and execution time in the Surveillance Client. To test the selected sound, click the **Play** button. You can select system default alarm sounds, or add your custom alarm sound (.WAV files only)



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

8.2.6 Send instant message to operator

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

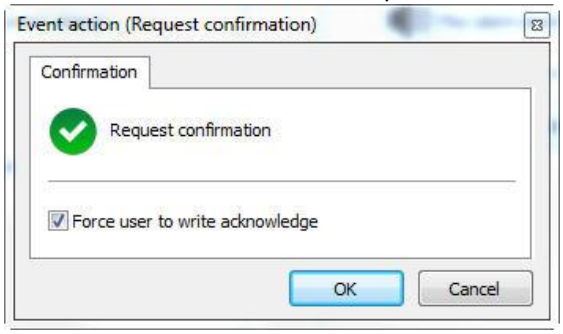


On this screen, configure the message to be displayed on the Surveillance Client popup to the operator.

© 2002 - 2024 by Digifort. All rights reserved.

8.2.7 Request written acknowledgement from users

Requests written confirmation from users. This confirmation must be written by the Surveillance Client operator directly in the alarm popup. These confirmations may contain information about the procedure that the operator performed when an event occurred, for example.

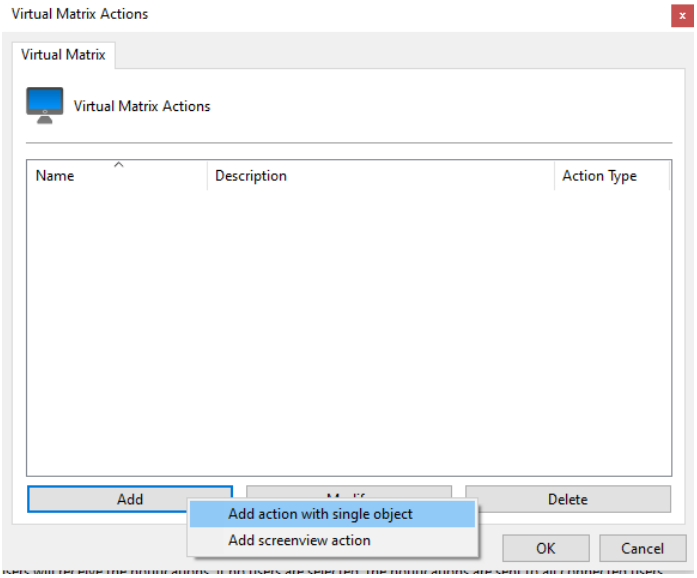


If you want the operator to be required to write the confirmation, select this option. If this option is active, the operator will not be able to close the alarm popup without writing something in the confirmation field.

8.2.8 Send Objects to Virtual Matrix

Displays objects on screen for the operator, sending via the Virtual Matrix feature (for more information on Virtual Matrix, see the Surveillance Client manual) instead of the alarm popup.

You can choose between sending a single object or sending a pre-configured view to the Virtual Matrix:



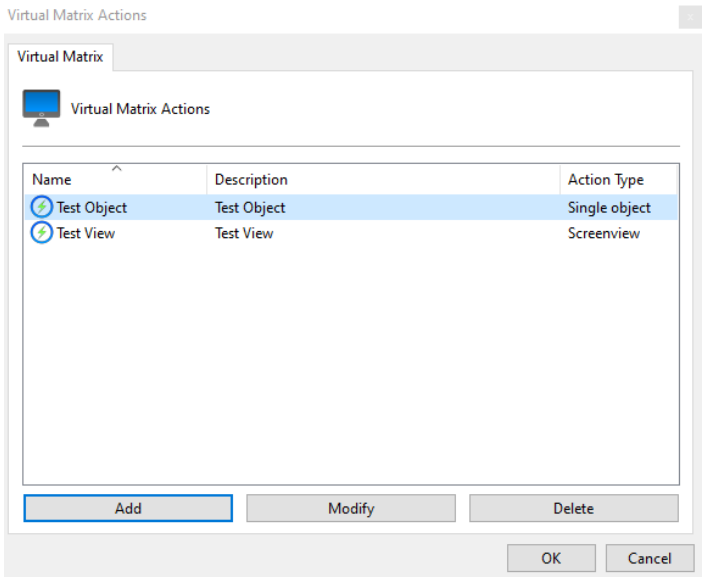
Click the **Add** button and select between **Add action with single object** or **Add screenview action**.

To change registered actions, select the action and click **Modify**.

To delete registered actions, select the desired action and click **Delete**.

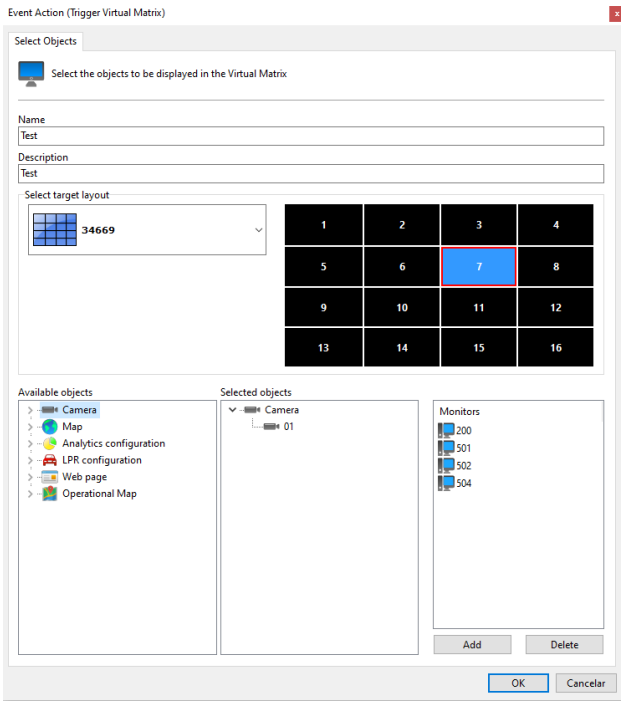
You will be able to configure multiple Virtual Matrix actions (Including different types):

© 2002 - 2024 by Digifort. All rights reserved.



8.2.8.1 Send single objects

In the action for single objects, it is possible to select the layout to be used and in which position of the layout the object will appear, check out the image below:



In the example above we will have camera 01 being sent using layout 34669 in position 7 for monitors 200, 501, 502 and 504.

- **Name:** Specify a name for this action
- **Description:** Specify a description for this action

© 2002 - 2024 by Digifort. All rights reserved.

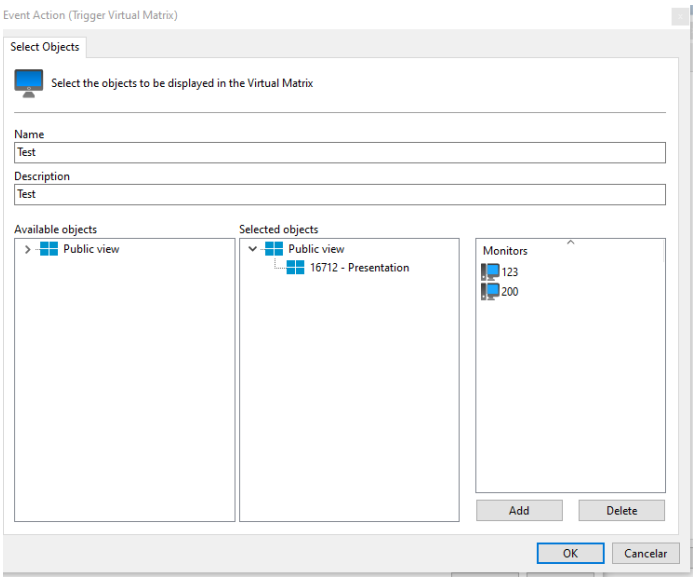
- **Layout:** Specify the desired tile layout. After selecting the desired layout, select the tile where you want the object to be displayed. If the layout is the same as the one already loaded on the target monitors, the Surveillance Client will not remove the current objects and will only replace the desired object in the selected tile.
- **Available objects:** List of available objects to select for sending to the Virtual Matrix
- **Selected Object:** Drag 1 object from the list of available objects to the selected object list to specify which object will be sent to the Virtual Matrix. Only 1 object can be selected
- **Monitors:** List of Virtual Matrix monitors to which the system will send the selected object. Click the **Add** button to add monitors or the **Delete** button to delete selected monitors.

8.2.8.2 Send views

When sending views, you can choose 1 pre-configured **public view** to be displayed on the Virtual Matrix monitors:

Note

This feature only works with public views.



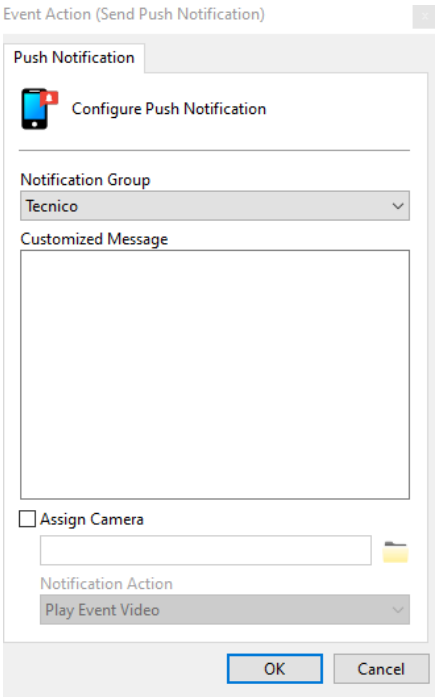
In the example above, the Presentation view, from layout 16712, will be displayed on monitors 123 and 200.

- **Name:** Specify a name for this action
- **Description:** Specify a description for this action
- **Available objects:** List of public views to select to send to the Virtual Matrix
- **Selected Object:** Drag 1 public view from the list of available objects to the selected object list to specify which view will be sent to the Virtual Matrix. Only 1 view can be selected
- **Monitors:** List of Virtual Matrix monitors to which the system will send the selected view. Click the **Add** button to add monitors or the **Delete** button to delete selected monitors.

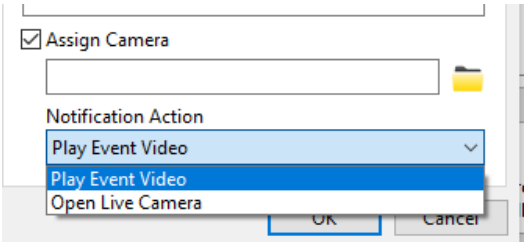
8.2.9 Send push notification to mobile devices with Digifort Mobile Client installed

Sends a push notification with the configured information to mobile devices pre-registered in the system using the Mobile Client. To register a mobile device, you must first associate it with a contact.

© 2002 - 2024 by Digifort. All rights reserved.



- **Notification Group:** Select the alert group to send the push notification
- **Custom Message:** You will be able to provide a personalized message that will appear in the push message on the mobile device
- **Associate Camera:** You can associate a camera with this action. When a user clicks on the push message and a camera is associated, the Mobile Client will open and perform the chosen action
- **Notification Action:** When a camera is associated with the action, you can choose between **Play Event Video** or **Open Live Camera** when the user presses the notification:
  - **Play Event Video:** When the user taps the notification, Mobile Client will open the video playback from the selected camera from the time this event was triggered
  - **Open Live Camera:** When the user taps the notification, Mobile Client will open the live video from the selected camera. This option is especially useful when you are using cameras for Intercom, for example.



8.2.10 Send Audio Clip to Device

Sends an Audio Clip to a device or a list of available devices.

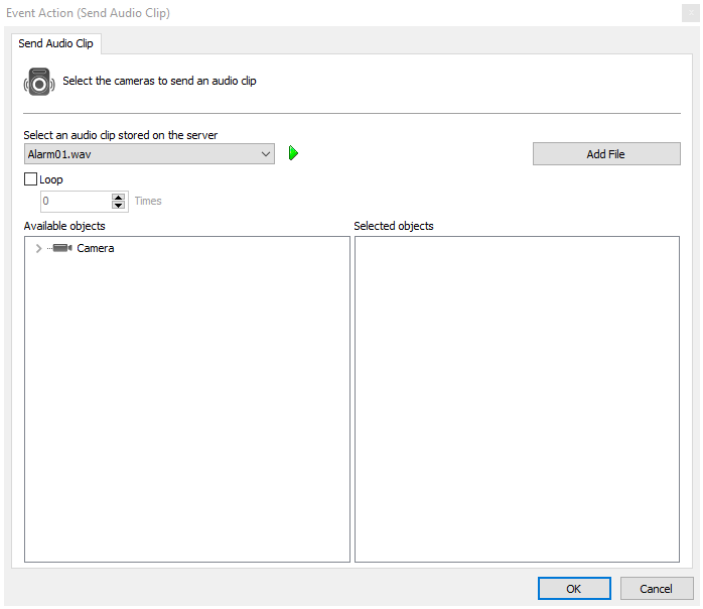
The system also allows the use of personalized alert sound files to be played on the device

Select the desired alert sound and click the **Play** button to test the file locally. You can select system default alarm sounds, or add your custom alarm sound (.WAV files only)

© 2002 - 2024 by Digifort. All rights reserved.

Important

- Custom audio files must be in .WAV format, with a frequency of 8hz, 16bits and Mono
- If the camera is configured to record by event, the option to **always keep the recording connection open** must be selected, otherwise audio will only be sent if the camera is currently recording. For more information about this option, see the Recording Type topic.

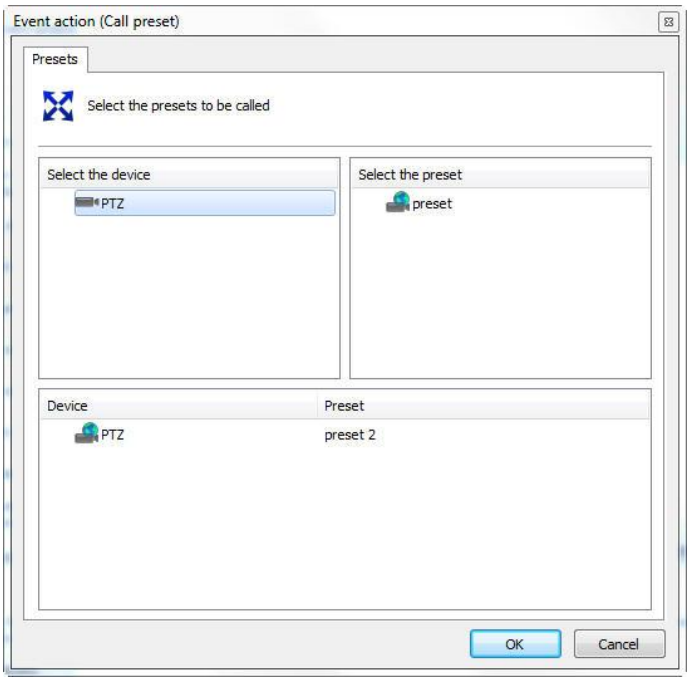


- **Select Audio File:** Select an audio file to be sent to the device.
- **Play button:** Test the audio file locally
- **Add File:** Click this button to add a custom audio file. The audio file will be saved on the server and will be available for other events.
- **Loop:** Select this option to play the audio in a loop
  - **Times:** Select the number of loops to play
- **Available Objects:** List of available devices to select. Drag the desired devices to the Selected Objects list
- **Selected Objects:** List of devices to which the system will send audio

8.2.11 Call camera presets

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

© 2002 - 2024 by Digifort. All rights reserved.



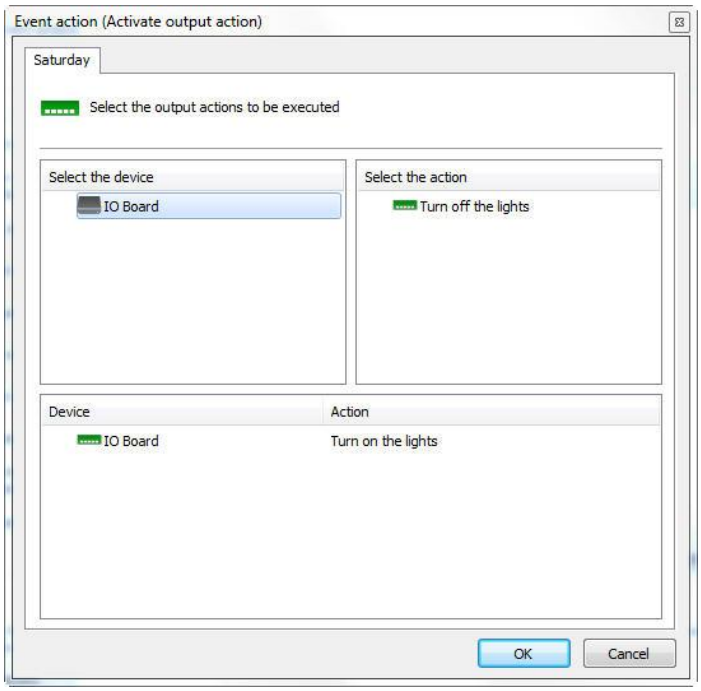
On this screen, select the desired camera, then select the preset you want to activate and then drag it to the list below, as shown in the figure above.

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

8.2.12 Trigger alarm output actions scripts

This action allows the system to trigger alarm output action scripts, for example, triggering a siren, upon the occurrence of an event. To learn how to configure alarm output action scripts see How to add output events.

© 2002 - 2024 by Digifort. All rights reserved.

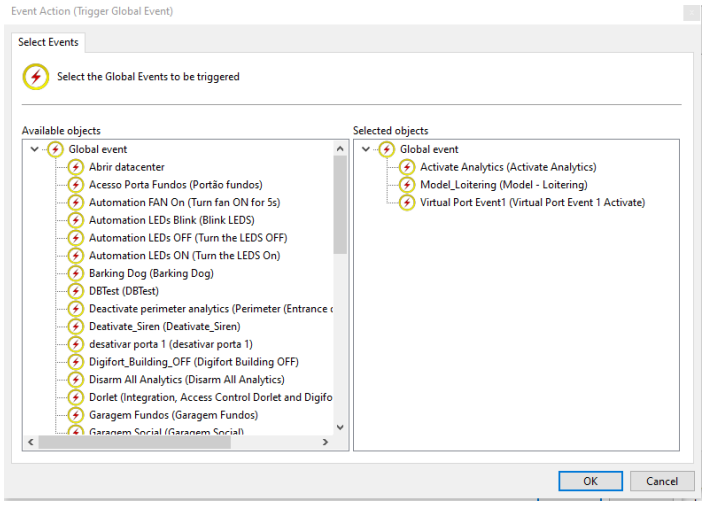


On this screen select the camera or I/O Device that contains the alarm output action script you want to activate. Then select the event and drag it to the list below, as shown in the figure above.

You can output actions from several devices and the system will call all actions simultaneously, but you must choose only 1 action per device.

8.2.13 Trigger Global Events

Trigger a Global Event when the event is fired, and can also fire multiple global events:



In the example above the action will trigger the events "Activate Analytics", "Model_Loitering" and "Virtual Port Event1".

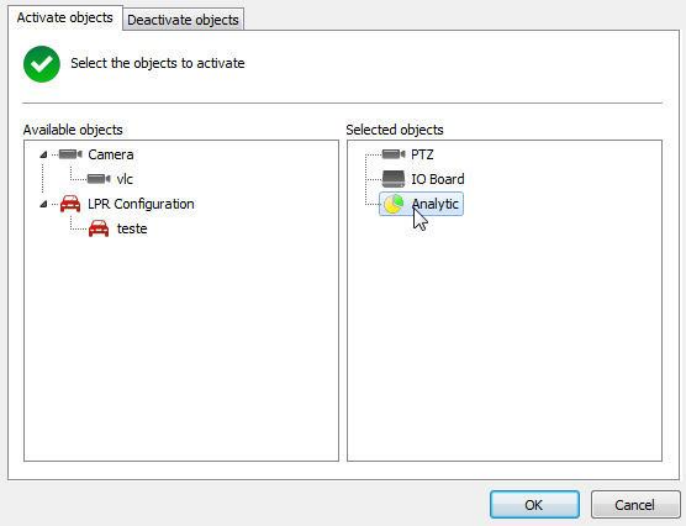
© 2002 - 2024 by Digifort. All rights reserved.

8.2.14 Activate or Deactivate system objects

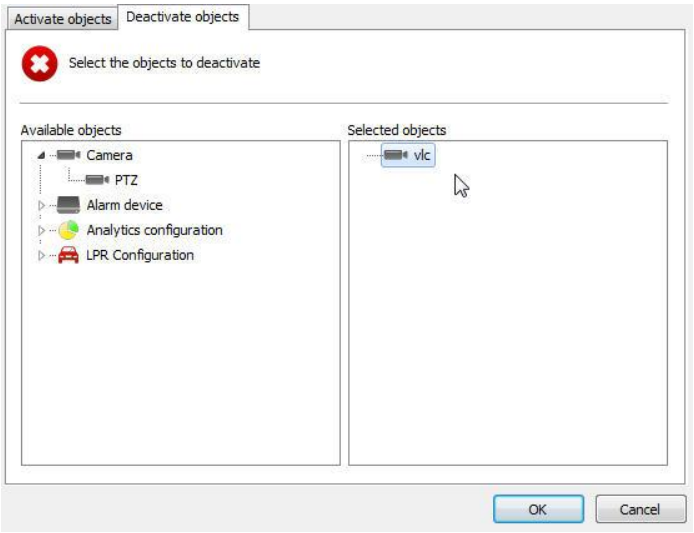
With this action it is possible to activate and/or deactivate system objects.

Any object that has activation control can be activated or deactivated through this action. You can activate or deactivate multiple objects at the same time.

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



To deactivate objects, simply go to the **Deactivate Objects** tab and click and drag the desired objects to the **Selected Objects** list on the right, as shown in the image below:



Note

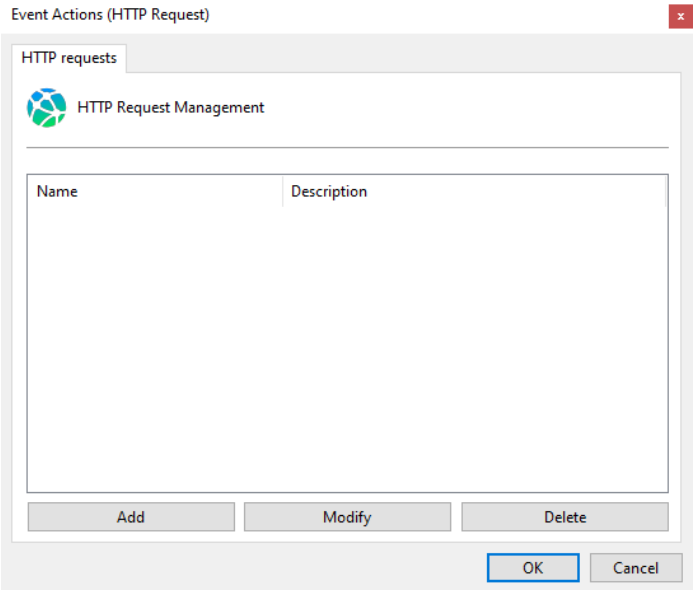
The server will first perform the **Deactivate Objects** action and then the **Activate Objects** option

© 2002 - 2024 by Digifort. All rights reserved.

8.2.15 Send an HTTP request

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

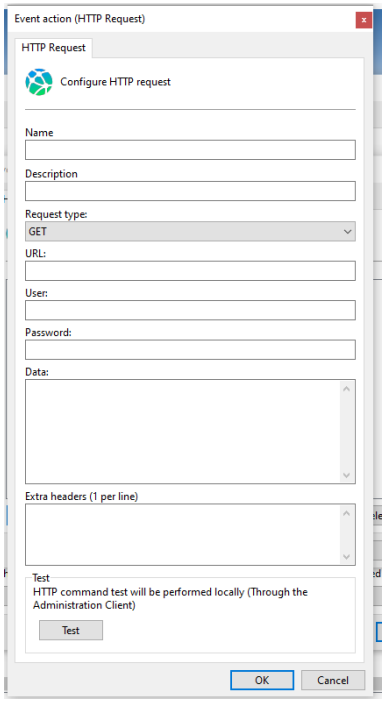
This resource requires a minimum knowledge of web programming to better understand how it works.



Here it is possible to register several HTTP actions that will be triggered simultaneously.

Click the **Add** button to add a new HTTP call.
Click on the **Modify** button to change previously registered HTTP calls
Click the **Delete** button to delete previously registered HTTP calls

© 2002 - 2024 by Digifort. All rights reserved.



This screen has the following settings:

- **Name:** Name of the request.
- **Description:** Description of the request.
- **Type of Request (Request type):** Type of request to be made.
- **URL**: HTTP URL for the request
- **User:** User for command authentication.
- **Password:** Password for command authentication.
- **Data:** When the **POST, PUT** or **PATCH** request type is selected the field for the data will be available. This is the data to be sent in the HTTP request.
- **Extra Headers:** Allows the configuration of extra headers that may be necessary for the request. You must enter the header in the format **HEADER: VALUE**
- **Test:** Allows you to test the HTTP action by sending the command configured above. The test will be carried out through the Administration Client, therefore the Administration Client must have access to the specified HTTP server.

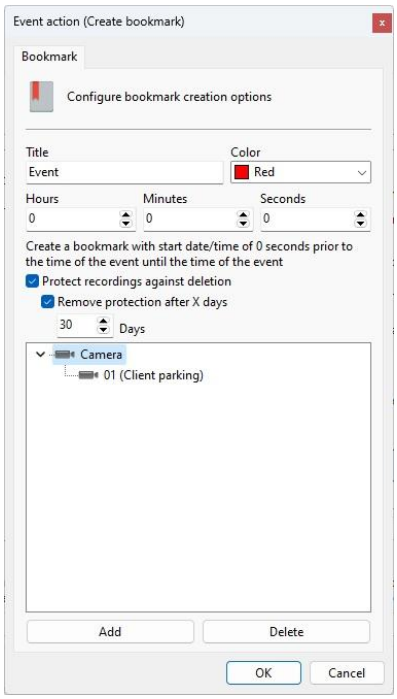
Tip

HTTPS commands via the HTTPS:// URL are also supported

8.2.16 Create Bookmark

This action allows the system to create a bookmark whenever a certain event occurs, easily identifying them in the recordings.

© 2002 - 2024 by Digifort. All rights reserved.



On the configuration screen, the following options are available:

- **Title:** Title that will be used for the Bookmark
- **Color:** Color used by the bookmark
- **Hours, Minutes and Seconds:** Select the duration of the bookmark. This way the bookmark will have a start and an end marking. The bookmark start time will be the selected time before the event occurred and will end at the time the event was triggered. If the configuration is left to zero, a simple bookmark will be created.
- **Protect recordings against deletion**: If your edition has the Recording Protection feature, this option will create a Recording Protection record for the bookmark's time, protecting the period of video marked by the bookmark against deletion.
  - **Remove protection after X days**: Configures the system to delete the created protection automatically after X configured days.
- **Camera:** Select one or more cameras where this bookmark should be created.
- **Add Button**: Add a camera to the camera list to create the bookmark
- **Delete Button**: Remove the selected camera from the list

To learn more about Bookmark, consult the Surveillance Client manual.

Tip

To create a bookmark with an end date after the event, instead of creating the bookmark action directly in the event, first create a **Timer** event that will fire X seconds after the event and then configure the bookmark in the Timer event, thus the end time of the bookmark will coincide with the timer trigger time.

8.2.17 Download recordings from devices that support edge recording

The edge recording system allows the system to download recordings upon the occurrence of any system event, enabling various operations such as:

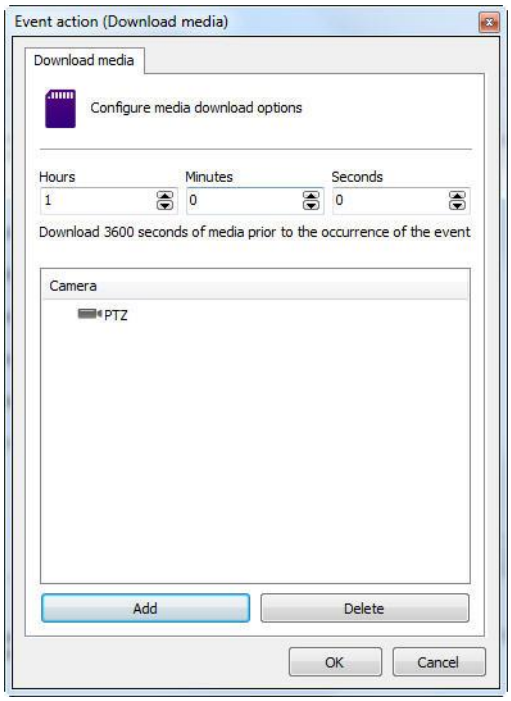
- Download recordings using scheduled event, creating a scenario where camera recordings can be downloaded daily, at a scheduled time.

© 2002 - 2024 by Digifort. All rights reserved.

- Download recordings with different resolution in the event of any event.

To configure this event simply select the desired time period to download and combine the camera recording with the server recording.

In the image below, the event will fetch 1 hour of recording **prior** to event from the "**PTZ**" camera:



- **Hours, Minutes and Seconds:** Select the duration of the downloaded video. The video will be downloaded at the specified time in the period before the event occurred. For example, if the event occurred at 15:00:00, and you set it to download 1 hour, then the system will download the video from 14:00:00 until 15:00:00.
- **Camera**: Select one or more cameras to download the video.
- **Add Button**: Add a camera to the camera list to download video
- **Delete Button**: Remove the selected camera from the list

Important

Any downloaded recordings that are combined will overwrite any existing recordings if they are at the same time.

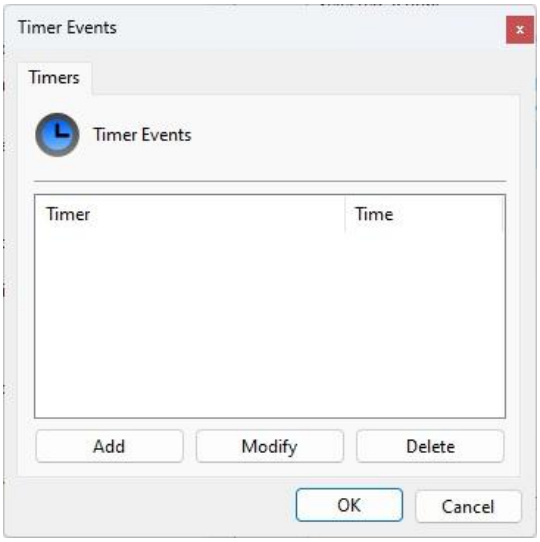
Tip

To download videos with an end date after the event, instead of creating the video download action directly in the event, first create a Timer event that will fire X seconds after the event and then configure the action in the Timer Event, so the end time of the downloaded video will coincide with the timer trigger time.

8.2.18 Create Timer Events

Timer events are events that fire after an event, after the specified time. It is possible, for example, when recognizing motion in a camera, trigger a siren exactly at the time of the event and, through a timer event, position a camera in a certain position five seconds later.

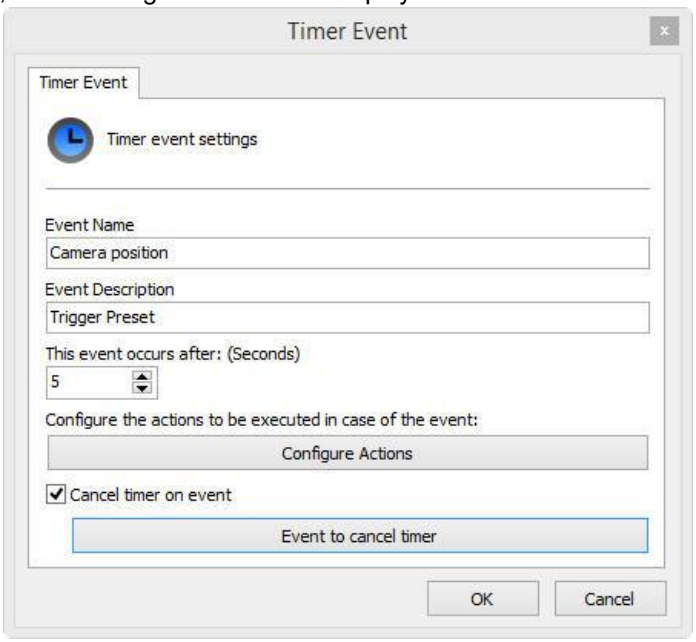
© 2002 - 2024 by Digifort. All rights reserved.



The system allows you to create multiple timer events in this action.

Click **Add** to create a new timer event
Click **Modify** to modify an existing timer event
Click **Delete** to delete a timer event

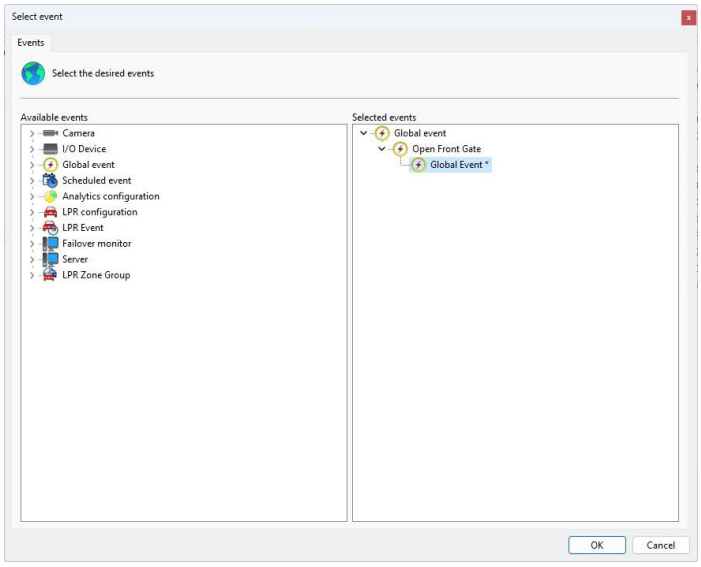
When adding an event, the following screen will be displayed:



- **Event Name:** Enter a name for the timer event
- **Description of the event:** Enter a description for this timer event
- **This event occurs after (Seconds):** Select the time, after the parent event fires, at which the timer event will fire.
- **Configure Actions:** Select the actions for this event. To learn how to configure event actions see How to configure event actions.

© 2002 - 2024 by Digifort. All rights reserved.

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



If the selected event occurs before the timer event is triggered, it will cancel its execution. This option is very useful for, for example, operations like "Door Open for a Long Time" where the system must trigger an event if a door is left open for a long time. To create this type of hypothetical scenario, simply create a timer event when the door is opened, in this timer event you can configure, for example, to trigger a siren after 60 seconds, but you select the event when the door is closed to cancel this timer, that is, the timer will only be triggered if the door is open for more than 60 seconds as it will be canceled if the door is closed.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter IX

9 User Management

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

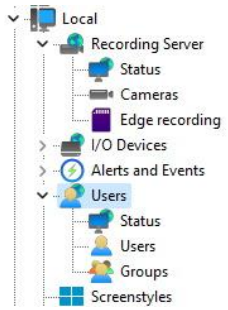
Creating users is very important for good organization and security of the system.

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

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

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

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



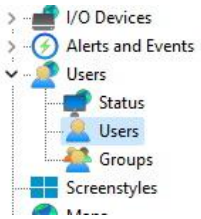
Tip

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

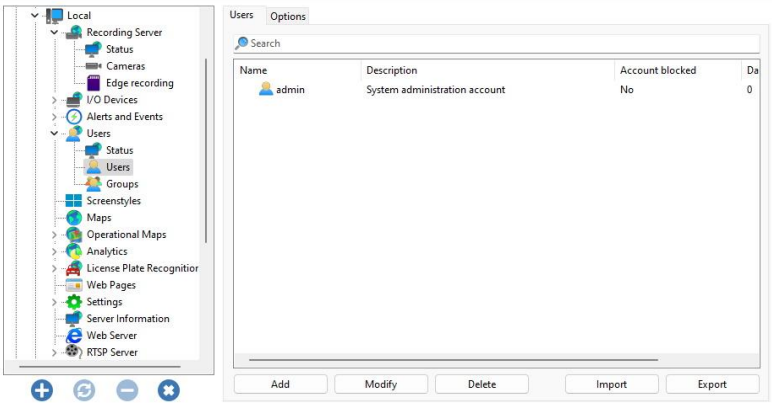
9.1 Adding, Changing, and Deleting Users

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

© 2002 - 2024 by Digifort. All rights reserved.



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

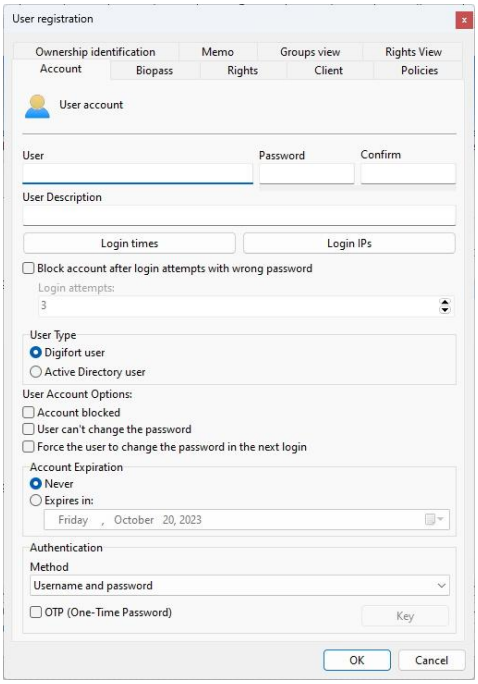


By clicking on the **Add** button, the user editing screen will be opened. Let's start by entering the user's data, then the rights and finally the client's resources.

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

© 2002 - 2024 by Digifort. All rights reserved.

9.1.1 User Account Info



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

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

© 2002 - 2024 by Digifort. All rights reserved.

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

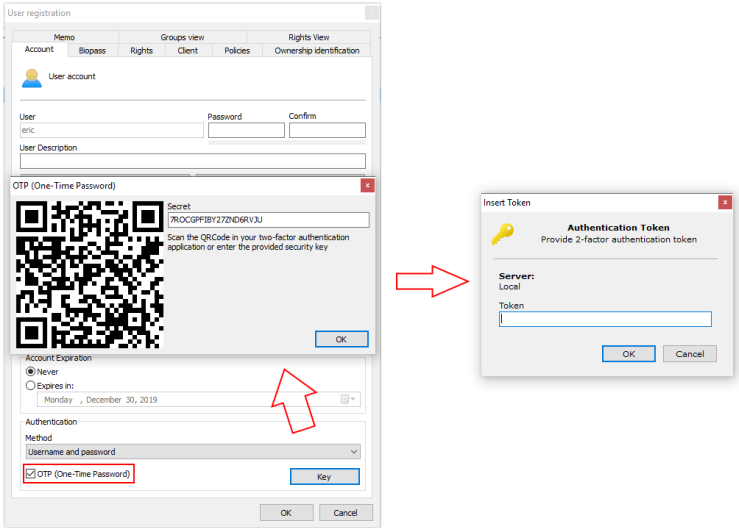
Tip

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

9.1.1.1 2 Factor Authentication

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

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



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

© 2002 - 2024 by Digifort. All rights reserved.

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

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

Note

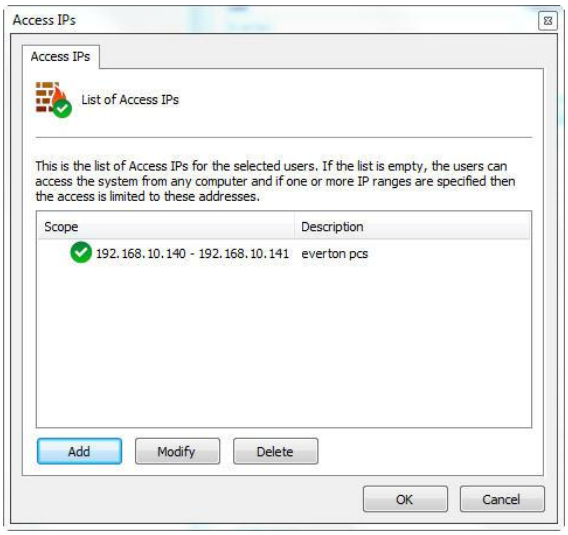
For greater security, once the authentication key is generated, it can no longer be accessed using the **Key** button. If you click the **Key** button again, a warning window will appear and a new key will be created.

9.1.1.2 Login IPs

The configuration of the Login IPs is very important for the security of the system, because in this configuration the range of IPs that the user can use for his authentication in the system can be registered.

For greater security, except in specific cases, it is recommended that you register your workstation user's IP, preventing them from accessing the system from other locations, such as your home.
If this configuration is not done, the user will be able to authenticate from any workstation.

To access this feature, click on the Login IPs button located on the User tab, opening the Login IPs register, as shown in the figure below:



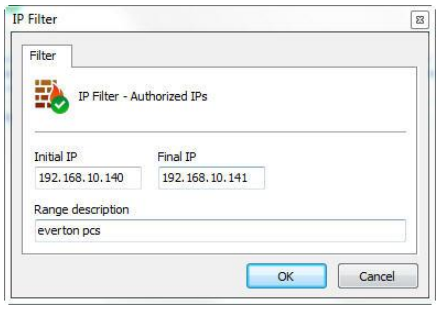
In the figure, a configuration is being exemplified where the user can authenticate in the system from the IPs within the range **192.168.5.2 to 192.168.5.4**.

To add a range of access IPs click on **Add**. To change a range of access IPs select it and click on **Change**. To delete a range of access IPs, select it and click **Delete**.

9.1.1.2.1 Adding an Access IP Range

To add a range of Access IPs, click **Add** and the editing screen will be displayed, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

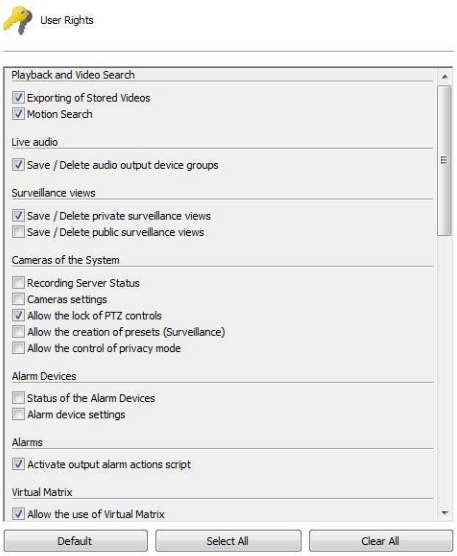


Enter the Initial IP and Final IP of the range and finally enter a description for the scope to be added. If you want to add a single IP, fill in the **Initial IP** and **Final IP** fields with the same value.

- **Initial IP:** Enter the starting IP of the IP scope (IPv4 only)
- **Final IP:** Enter the final IP of the IP scope (IPv4 only)
- **Description:** Enter a description for easy identification

9.1.2 User Rights

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



9.1.2.1 Video Playback and Search

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

© 2002 - 2024 by Digifort. All rights reserved.

9.1.2.2 Live Audio

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

9.1.2.3 Surveillance Views

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

9.1.2.4 System Cameras

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

9.1.2.5 IO Devices

- **Status of I/O Devices:** Allows the user to access the status of I/O Devices.
- **I/O Device Settings:** Allows the user to access I/O Device registration. See more at IO Devices.

9.1.2.6 Alarms

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

9.1.2.7 Virtual Matrix

- **Allow the use of virtual matrix:** Allows the user to send objects to the virtual matrix.
- **Allow joining the virtual matrix:** Allows the user to register their monitors to be part of the virtual matrix.

9.1.2.8 System Users

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

9.1.2.9 Alerts and Events

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

9.1.2.10 Global Events

- **Global Events Register:** Allows the registration of global events. See more at Global Events.
- **Global Events Triggering:** Allows the user to trigger global events.

© 2002 - 2024 by Digifort. All rights reserved.

9.1.2.11 Scheduled Events

- **Scheduled Events Register:** Allows the user to register scheduled events. See more at Scheduled Events.
- **Scheduled Events Status:** Allows the user to consult the status of scheduled events.

9.1.2.12 Maps

- **Maps Register:** Allows the registration of maps. See more at Maps.

9.1.2.13 Operational Maps

- **Operational Maps Registration:** Allows the registration of Operational maps. See more at Operational Maps.

9.1.2.14 Analytics

- **Analytics Configurations Registration:** Allows the registration of analytic configurations. See more at Analytics.
- **Analytics Configurations Status:** Allows viewing the status of the registered configuration.
- **Analytics Search and Reporting:** Allows the user to search and report on analytics events.

9.1.2.15 Plate Recognition

- **LPR Configuration Status:** Allows you to view the LPR Configuration Status. See more at Plate Recognition.
- **Configuration and Registration:** Allows the Registration of LPR configurations.
- **Allow Registration from Surveillance:** Allows the registration of plates in the LPR list via the Surveillance Client.
- **Allow Modification of Recognized Plates:** Allows the Surveillance Client operator to change the value of recognized plates through Live LPR control.
- **LPR Search and Reporting:** Allows searching and reporting of LPR events.

9.1.2.16 Web Pages

- **Web Pages Registration:** Allows the registration of Web Pages. See more at Web Pages.

9.1.2.17 Screen Layouts

- **Screen Layouts**: Allows the creation of new screen layouts for monitoring.

9.1.2.18 Server

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

9.1.2.19 Report Authentication

- **Visualization of Authenticated Reports:** Allows the user to search authenticated reports in the Surveillance Client. See more at Report authentication.

© 2002 - 2024 by Digifort. All rights reserved.

9.1.2.20 Bookmarks

- **Insert Bookmarks:** Allows the user to create bookmarks in the Surveillance Client.
- **Delete Bookmarks:** Allows the user to delete bookmarks, even if he was not the creator of the bookmark in question.
- **Bookmarks Visualization:** Allows the user to search and visualize the bookmarks created in the Surveillance Client.

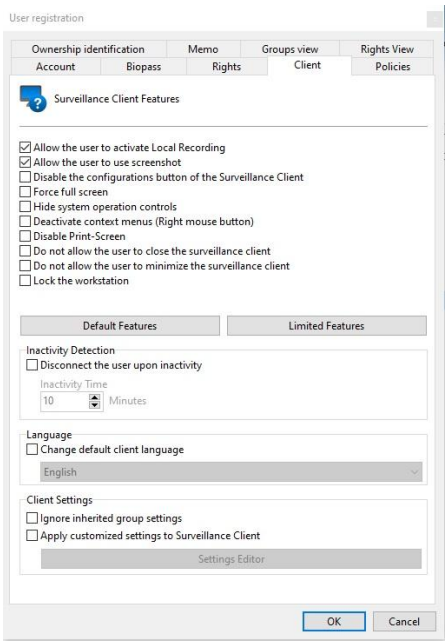
9.1.2.21 Recording Protection

- **Protect Recordings Against Deletion:** Allows the user to protect recordings. Look Recording Protection.
- **Delete Recording Protections:** Allows the user to delete existing recording protections. Look Recording Protection.
- **View Recording Protection Records:** Allows the user to view reports of created, existing and deleted protections. Look Recording Protection.

9.1.3 Surveillance Client Features

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

To access these tools, click the Client Resources tab.



- **Allow user to activate Local Recording:** Allows the user to activate local emergency recording on the Surveillance Client. To learn about local recording see the Surveillance client manual.
- **Allow the user to use the screenshot:** Permission for the user to use the system's screenshot feature.
- **Disable Surveillance Client Settings Button:** Prevents the user from accessing the Surveillance Client settings. To learn about the Surveillance Client settings, consult it's manual.
- **Force full screen:** Force the user to use the Surveillance Client in full screen.

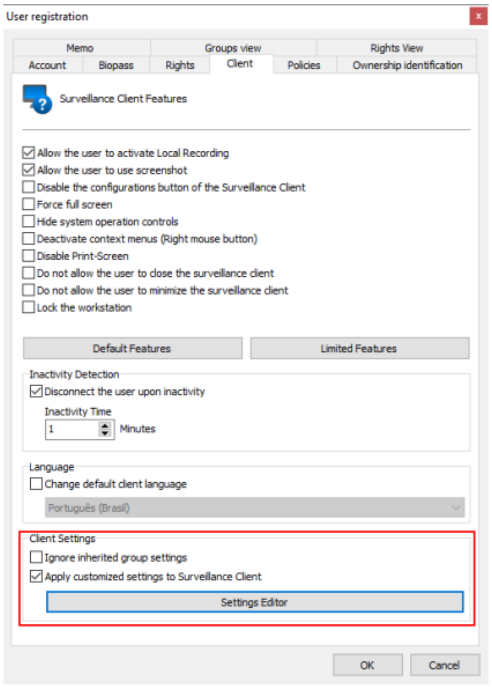
© 2002 - 2024 by Digifort. All rights reserved.

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

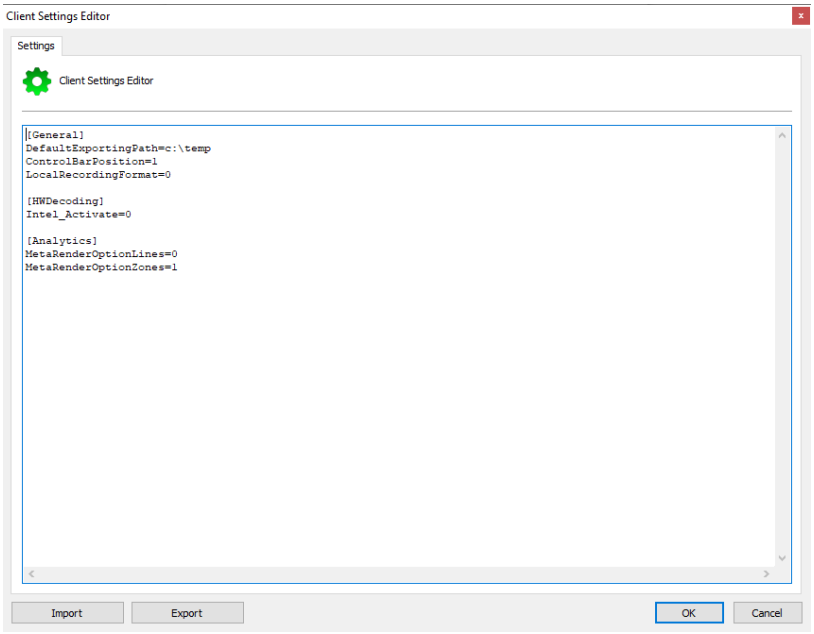
9.1.3.1 Centralized Surveillance Client Configuration

It is possible to apply customized (or all) configurations in the Surveillance Client according to user login. Settings are adjusted per user and per user group.
When registering a user, or registering a group of users, select the Client Settings option:

© 2002 - 2024 by Digifort. All rights reserved.



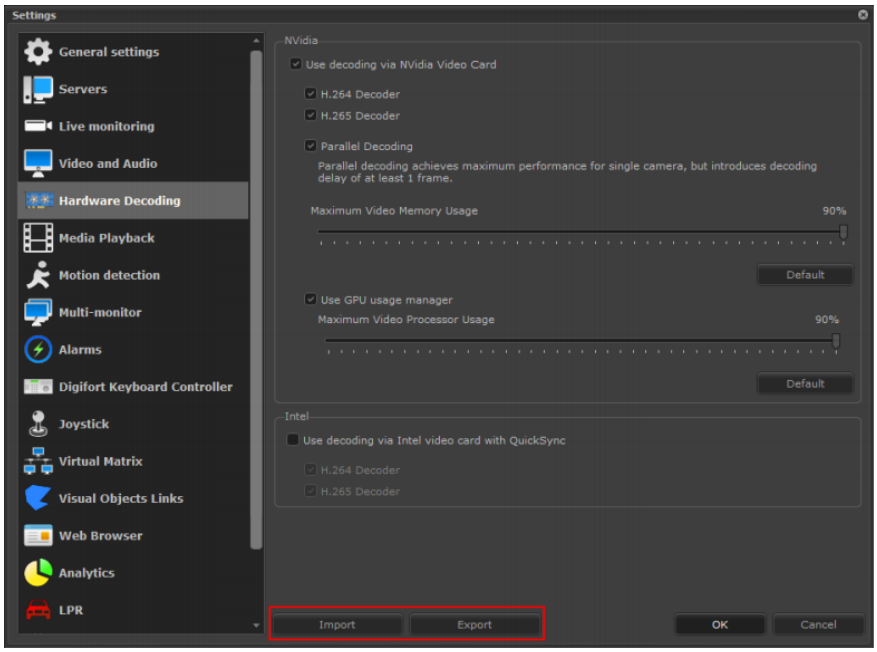
The editor allows adjusting the settings and values that will be applied in the Surveillance Client when the user logs into the server.
The values follow the .INI file format:



This is a way to centrally force default configurations for multiple Surveillance Clients, facilitating the distribution and configurations of workstations, since their options can be changed in the user's profile.

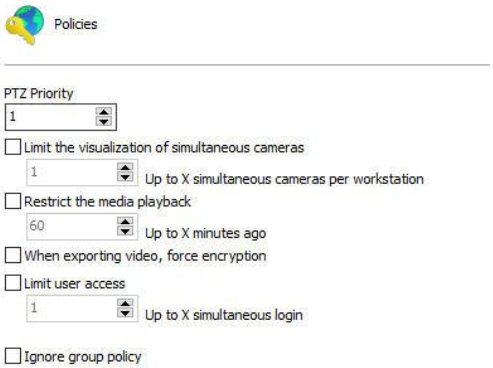
Configuration values can be exported through the Surveillance Client configuration export screen:

© 2002 - 2024 by Digifort. All rights reserved.



You will be able to change any configuration value and apply it to the client through this editor. Use a configuration file exported from the Surveillance Client as a reference for configuration values to be added to the editor.

9.1.4 Policies



This screen allows the following settings:

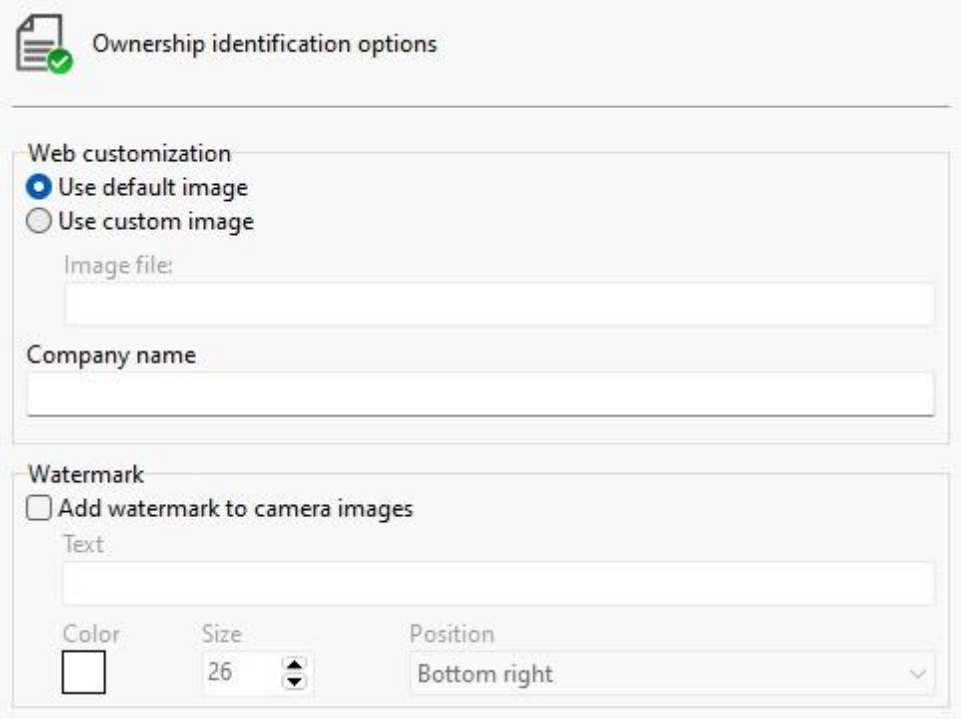
- **PTZ Priority:** This option aims to prioritize a user in locking camera PTZ controls for exclusive use. The priority with value 1 is the highest of all, therefore, no user with equal or lower priority will be able to unlock the PTZ while that user is using it. Now let's imagine a user with priority 3, this user will lose control of the PTZ to the one who has a higher priority, in this case 1 or 2, but no user at the same or lower level (3,4,5,6...) will be able to take PTZ control while using it. To learn more, see the PTZ Lock topic.
- **Limit the visualization of simultaneous cameras:** Restricts the number of cameras that the user can visualize simultaneously in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.

- **Restrict the media playback:** Limits the user to only playback X configurable seconds of video prior to the current server date.
- **Force export with encryption:** Allows you to force encryption on all video exports. This option can be configured per user or user group. For more information about export with encryption, see the Surveillance Client manual. When this option is active, only the native export format will be available to the operator.
- **Limit user access:** Limits the number of simultaneous logins for this user through Desktop clients.
- **Ignore group policies:** The user with this option checked will not have a user group policy overridden by that of his user.

9.1.5 Ownership Identification

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



9.1.5.1 Web Customization

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.

9.1.5.2 Watermark

This resource makes it possible to create a watermark on top of the image that is viewed and reproduced by the user. This watermark is intended to identify the owner of images when system images are provided to external users. This watermark will also be present when exporting images.

To add a watermark to the video, click on **Add watermark to camera images**. The following options will be available:

- **Text:** Text to be inserted as a watermark.
- **Color**: Color of the text inserted as a watermark.
- **Size:** Font size of the text inserted as a watermark.
- **Position**: Position on the image where the watermark will appear.

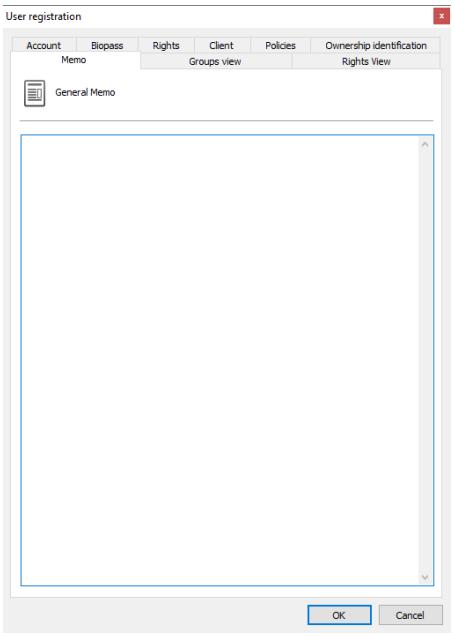
Below is an example of a watermark in an image in the Surveillance Client:

9.1.6 General User Remarks

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

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

© 2002 - 2024 by Digifort. All rights reserved.



9.1.7 Groups View

Allows viewing in which groups this user is registered.

9.1.8 Rights View

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

This screen offers the following features:

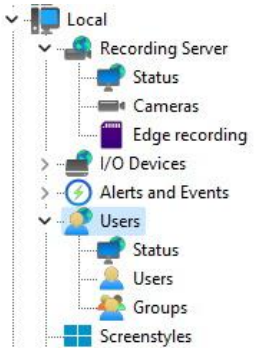
© 2002 - 2024 by Digifort. All rights reserved.

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

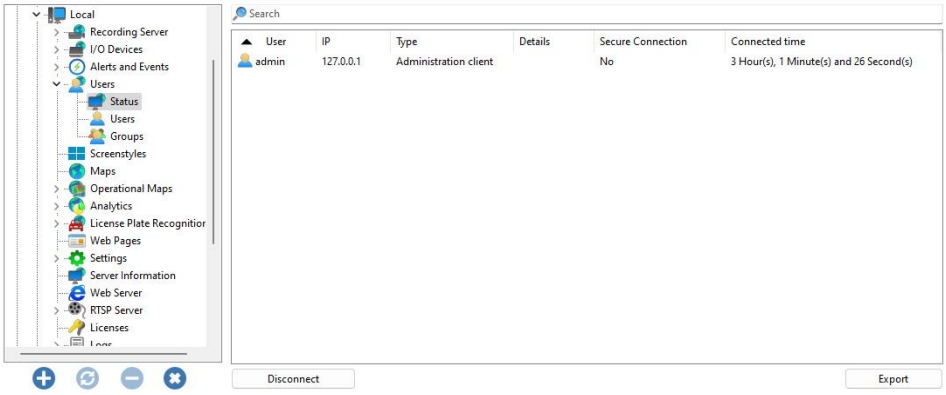
9.2 Monitoring User Activities

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

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



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

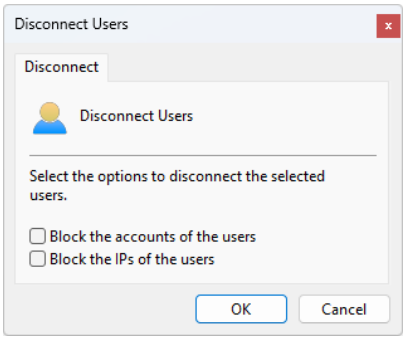


This list displays all users currently logged in, displaying information such as user name, IP address, type of access to the server and connection time.

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

© 2002 - 2024 by Digifort. All rights reserved.

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



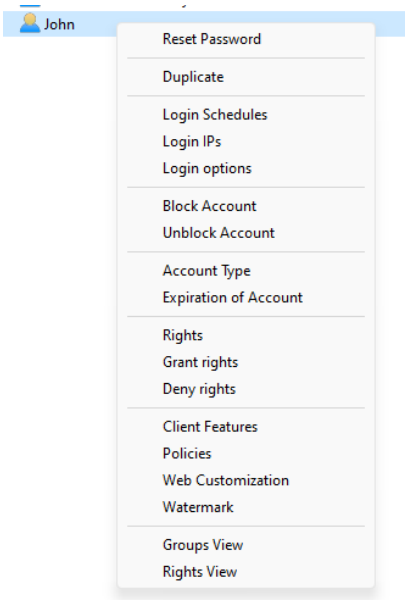
- **Block Users Account:** With this option checked, all disconnected users will also have their account blocked.
- **Block Users IP:** With this option checked, all disconnected users will also have their connection IP blocked using the IP Filter feature.

Note

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

9.3 How To Change Parameters For Multiple Users Simultaneously

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

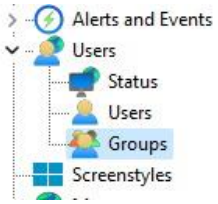


Most of the options you can change are self-explanatory and you can consult the User Registration topic to learn more about each option.

© 2002 - 2024 by Digifort. All rights reserved.

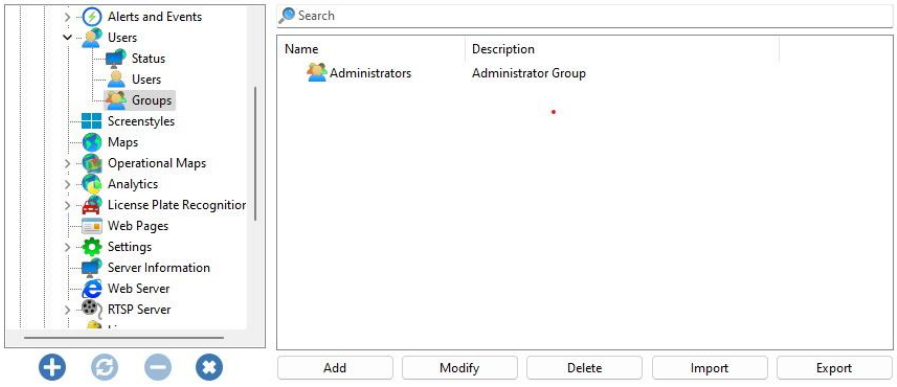
9.4 Adding, Changing, and Deleting Groups

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



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

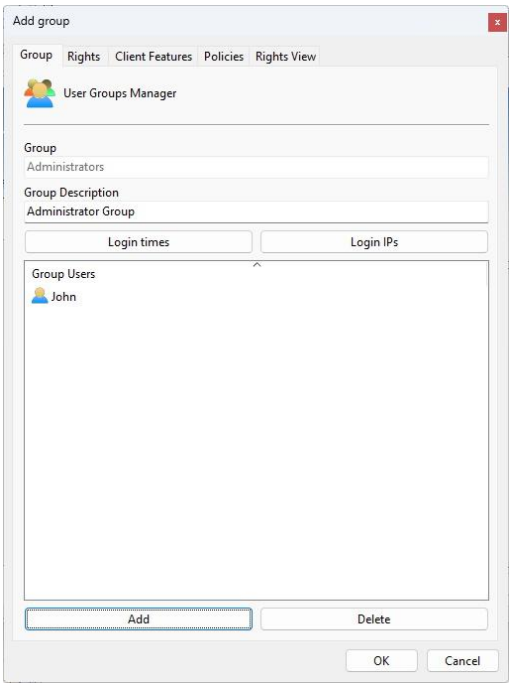
Once this is done, the **Group management** screen will open on the right side as shown in the figure below:



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

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

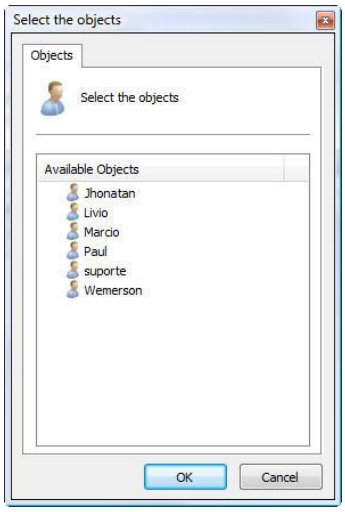
© 2002 - 2024 by Digifort. All rights reserved.



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

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

© 2002 - 2024 by Digifort. All rights reserved.



9.4.1 Group Rights

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

The rights settings for the group are the same as the user rights settings. To learn how to configure group rights see User Rights

Note

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

9.4.2 Surveillance Client Features

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

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

Note

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

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

9.4.3 Policies

The Policies setting for the group is the same as the User Policies setting. To learn how to configure group Policies, see the User Policies topic.

Note

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

© 2002 - 2024 by Digifort. All rights reserved.

Note

restriction, this greater restriction will take precedence.

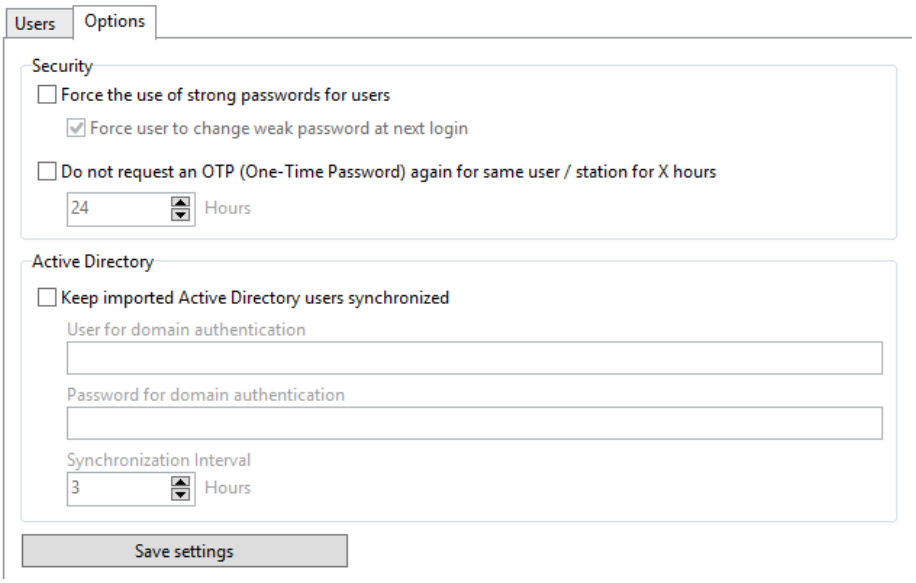
9.4.4 Rights View

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

The Rights View screen for the group is the same as the User Rights View screen. To learn about group Rights Inquiry see User Rights View.

9.5 Options

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



9.5.1 Security

9.5.1.1 Force use of strong password

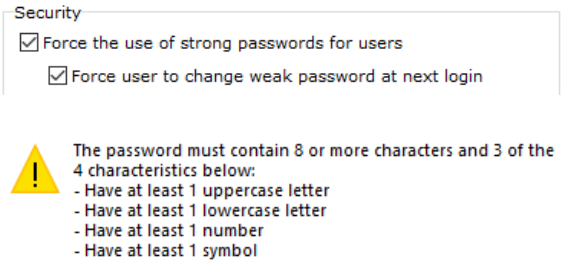
The system allows users to use a strong password. A strong password must contain at least 8 characters and 3 of the 4 characteristics below:

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

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

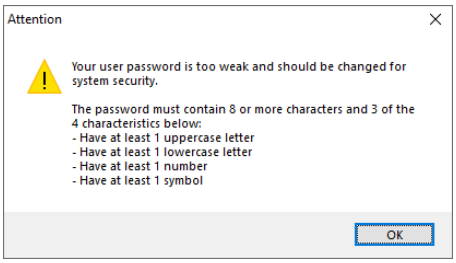
The use of a strong password only applies to native system users and not to LDAP/Active Directory users, where the strong password requirement must be applied directly on the domain controller.

© 2002 - 2024 by Digifort. All rights reserved.



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

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

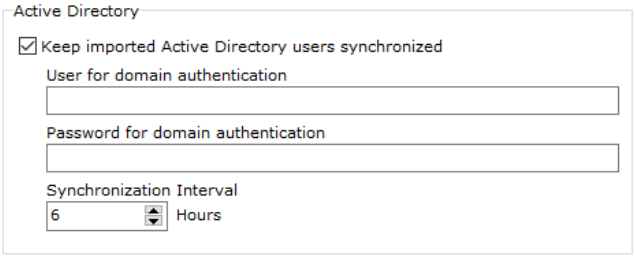


9.5.1.2 OTP

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

9.5.2 Active Directory

When integrating with Active Directory, the server allows you to keep users imported from AD synchronized with the domain, that is, if the user is deleted from the domain, he will also be deleted from the system.



- **Keep users imported from Active Directory synchronized**
  - **User for domain authentication:** Specify a domain user with the right to query the user list
  - **Password for domain authentication:** Specifies the domain user password
  - **Sync Interval:** Time for users to synchronize (In hours)

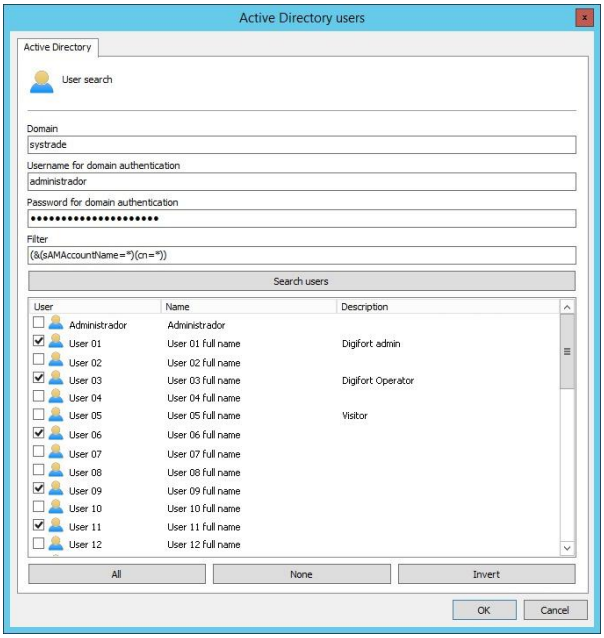
© 2002 - 2024 by Digifort. All rights reserved.

9.6 Active Directory Integration

Active Directory is a set of objects located on the domain server, which contains all the information that allows users to control access to the network. It records user names and passwords, their access permissions to files, printers and other network resources, disk quotas, computers and times that each user can use, etc.

Interaction with Active Directory allows network users from the domain in which the system server is located to be imported and incorporated as system users.

There are 2 ways to do this integration, the first is by importing users directly from Active Directory. To do this, go to **Users** and click on **Import from Active Directory** as shown in the image below:

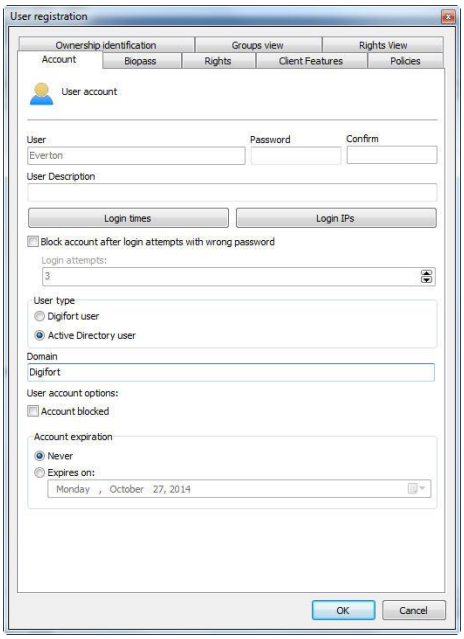


- **Domain:** Enter the network domain.
- **User for domain authentication:** User to authenticate to the domain with the right to list users.
- **Password for domain authentication:** Domain user password.
- **Filter**: Search filters allow you to define criteria and provide more efficient searches. To learn about the LDAP filter visit the Microsoft page: https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx

After filling in the fields, click **Search Users** and all users registered in the domain will be listed. To add the desired users to the system, simply select them and click **OK**.

A user belonging to the domain has the following configuration screen:

© 2002 - 2024 by Digifort. All rights reserved.



All username and password options are blocked because authentication is done in the domain and no longer natively in the system, that is, the account lock, Biopass and Account expiration options will no longer be available.

The second way of integration is to create a user or change an existing native one. To do this, change the **User Type** field to **Active Directory User**. For correct operation, the user name and domain must be filled in correctly according to the users registered in the current Domain.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

10 Layouts Management

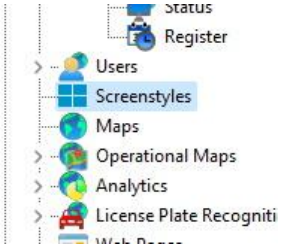
Layouts are groupings of cameras in a certain format and order that are used by the Surveillance Client to display the cameras on the screen.

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

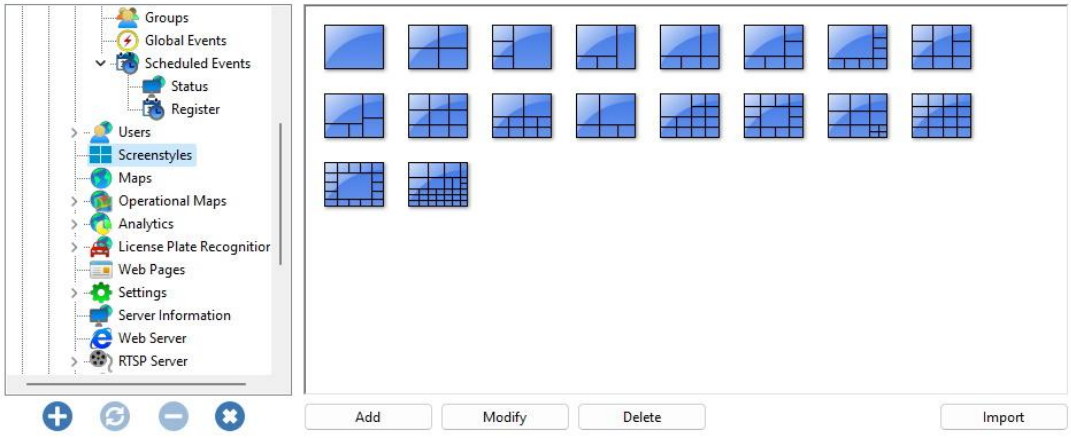
In the Administration Client, it is only possible to manage layouts, that is, create, modify or delete them. To learn how to add cameras to tiles, see the Surveillance Client manual.

10.1 How To Access Layouts Management

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



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



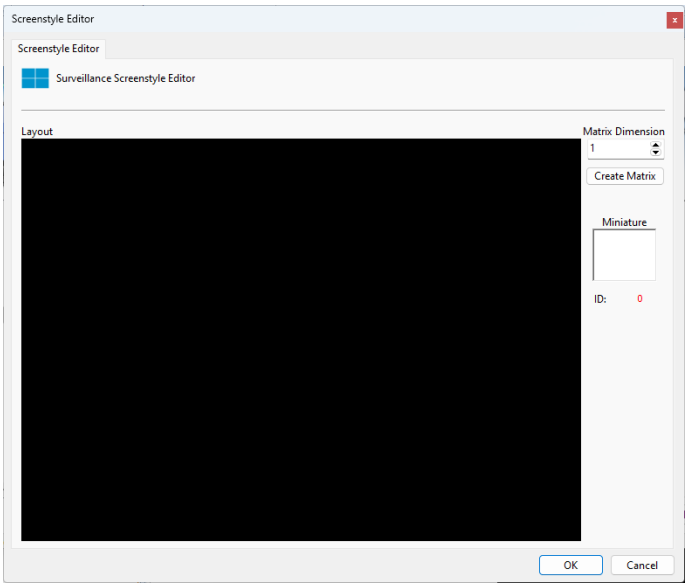
The system provides some pre-defined layouts that cannot be changed or deleted.

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

10.1.1 How To Add A Layout

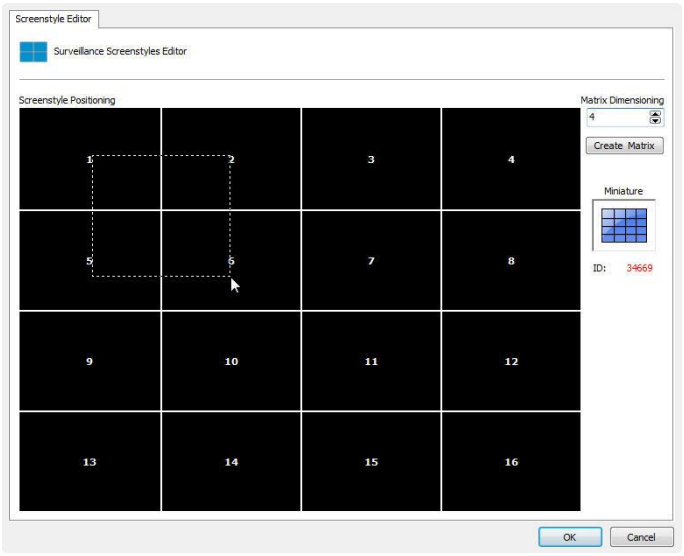
After clicking **Add**, as explained in the previous topic, the following screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



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

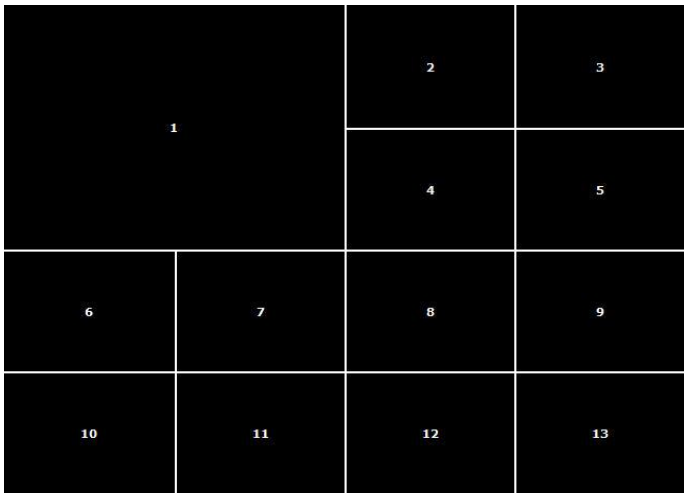
Select the matrix dimension and click the **Create Matrix** button



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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

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

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XI

11 BioPass

BioPass is a system biometric authentication product. In order to increase the security of users who authenticate themselves in the system, it is possible to require authentication via biometrics.

This is a depreciated product and is no longer sold.

11.1 How to install BioPass on your computer

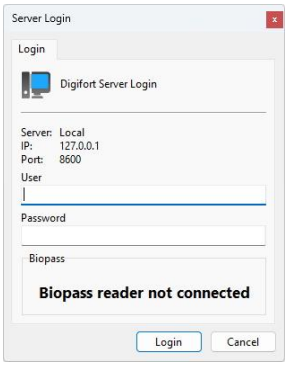
After installing the system version, BioPass Digital Reader drivers will be available for the operating system to install.

With the system already installed, connect the Biopass reader to your machine, and you will see the following message from the Operating System.

After the message, you will be able to configure BioPass on the system.

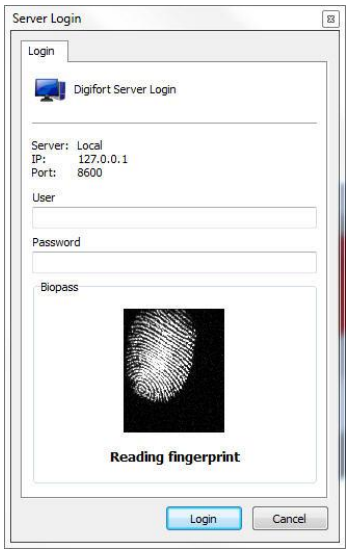
11.2 How to set up BioPass

If your reader is not recognized, or is not plugged in, **the message Biopass reader is not connected** appears as shown in the image below:



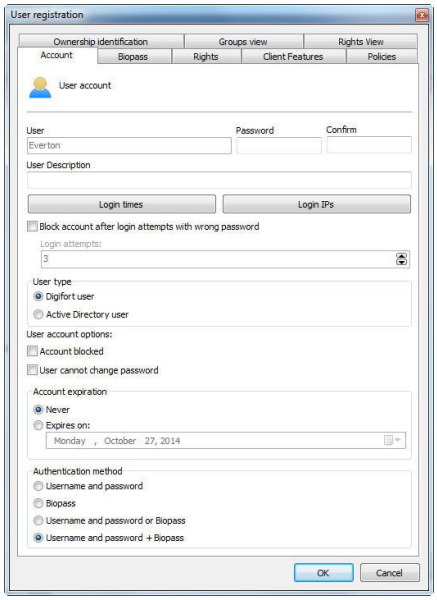
With the Reader already plugged in and recognized by the operating system, you must now open the Administration Client and login to your server.
You will notice that the Login screen now has a differential, as shown in the following image:

© 2002 - 2024 by Digifort. All rights reserved.



An area for viewing the fingerprint appears on the screen, but there is still no fingerprint registered, so login must be performed using a username and password.
Now to configure the fingerprints we must go to the **Users Registration.**

Once this is done, we will create a user to configure the Biometric Reader. (See the chapter User Management to learn about system users):



Enter a username, password, and description for the New User. In the “Authentication Method” area we have four options:

- **User and password:** Default system authentication
- **Biopass:** Only a fingerprint is required.
- **User and password or Biopass (User and password + Biopass):** Login can be performed with user and password or Biopass. (Not recommended unless using the web server is required as it does not have BioPass functionality).

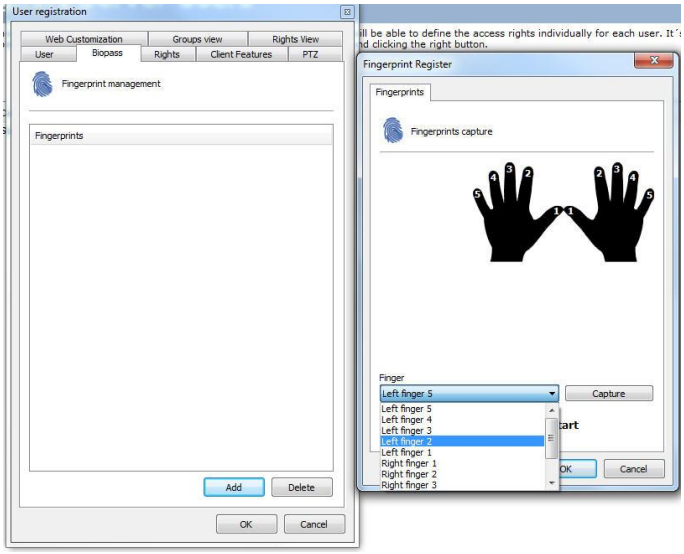
© 2002 - 2024 by Digifort. All rights reserved.

- **User and password + Biopass (User and password + Biopass):** Requires username and password + Biopass to login.

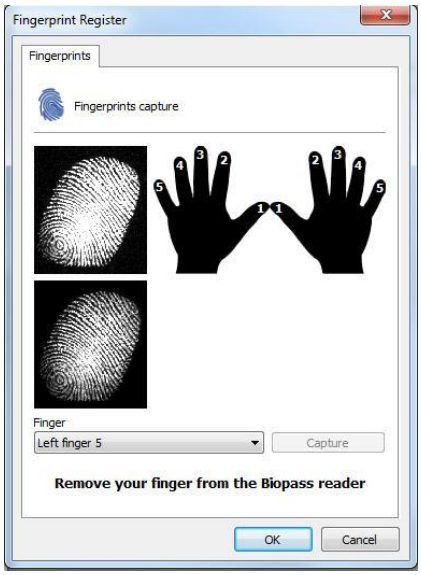
In this area you will select the way the user will be able to login to the system, in this case the option
- **User and Password + Biopass.**

It should be taken into account that, for greater security, the **User and Password + Biopass** option is the most recommended, as this will force the user to use his username and password and still use biometric authentication.

Once this part is configured, now we must open the "**BioPass"** tab, as in the following figure:



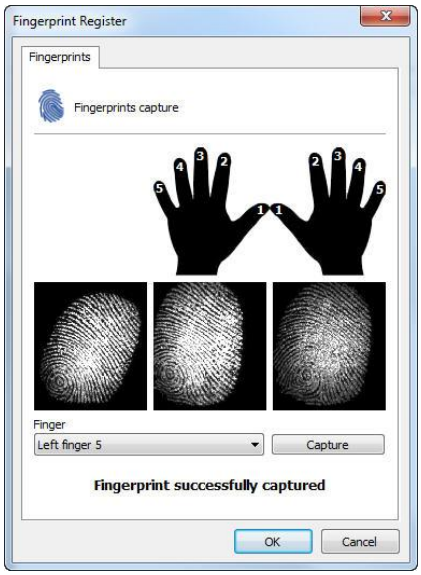
Click on **Add**, after that the screen on the right will be shown to you, where you will select the finger that you want to capture the fingerprint (To facilitate the choice of the finger to be captured, you can also click on the the numbers in the drawing of the hands). Chosen the finger now click on **Capture:**



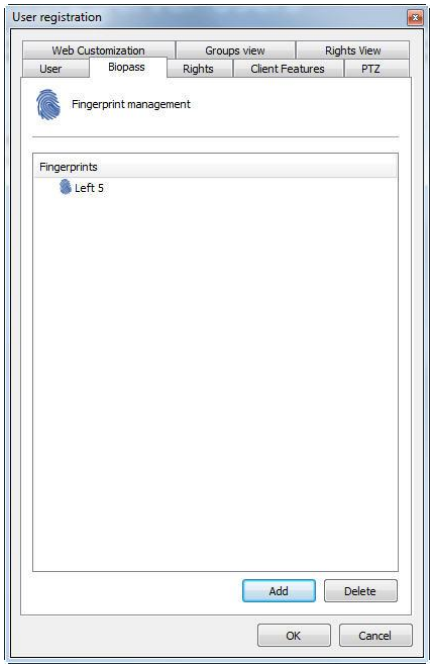
© 2002 - 2024 by Digifort. All rights reserved.

The screen has undergone a small change, where instructions for configuring the Fingerprints will appear. The software will ask you to take three fingerprint captures from the same finger. The finger must be placed and removed from the Biopass when the message **Remove your finger from the Biopass reader appears.**

After completing the capture, the **Fingerprint successfuly captured** message will be shown:



After that, click on **"OK"** to save the configuration applied to this finger and the screen of captured fingerprints will be shown as in the image below:



It is recommended that more than one finger be captured, just to be on the safe side.

© 2002 - 2024 by Digifort. All rights reserved.

From that moment on, login can be done via BioPass both in the Administration Client and in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.

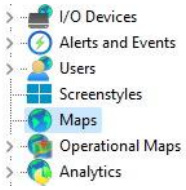
Chapter XII

12 Maps

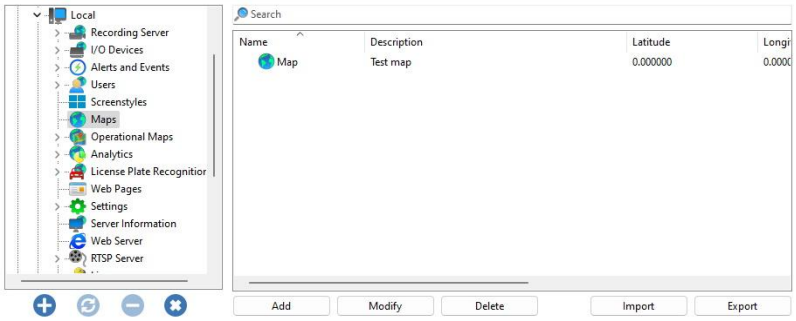
The system brings as added value a synoptic map, which makes it possible to fully monitor an industrial plant, a building, etc. With the map, there is a better visualization and control of the location, allowing, in addition to viewing the cameras, triggering alarms.

12.1 Map Registration

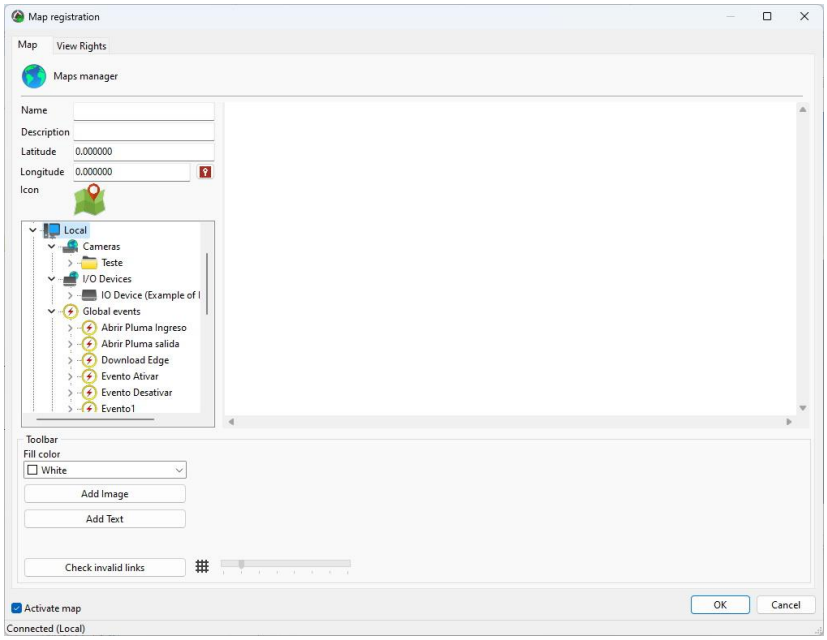
To register a map, click on the Maps item in the Settings Menu, as shown in the figure below:



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



Click **Add** to open the Map settings screen as shown below:



© 2002 - 2024 by Digifort. All rights reserved.

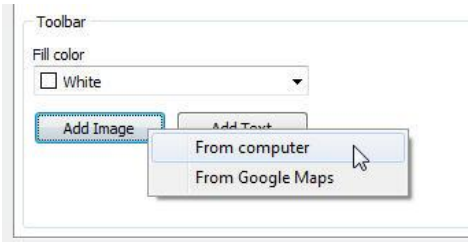
To change an already registered map, select it and click **Modify**, and change the data as explained on the following pages.
To remove a map, select the desired map and click the **Remove** button.

This screen allows objects from different servers to be present on the same map. You can connect to one or more servers from the list located on the right side of the screen. Look How to Connect to a Server for Management.The servers present in the list will be the same ones that are registered in **Servers** in the Administration client's main list.

- **Name:** Provide a name for the map. Once saved, the name cannot be changed.
- **Description:** Provide a description for the map for easy identification in the system.
- **Latitude and longitude:** Georeferenced position of the map item, for identification and access through **Operational Maps**.
- **Activate Map:** Enables or disables this map object.

12.1.1 Adding Images

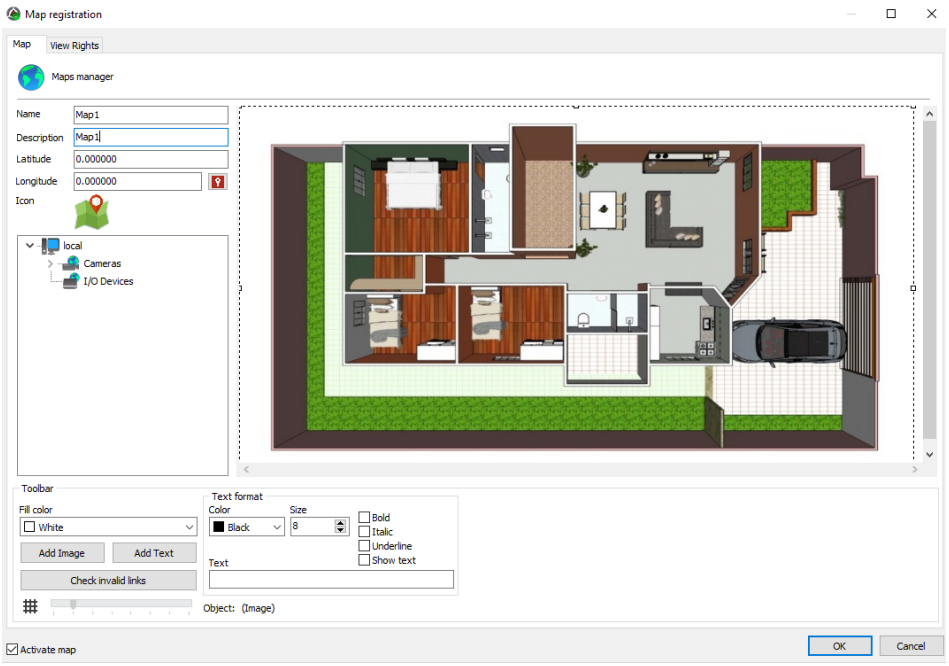
Click on add image to locate the desired figure for your map and choose From computer as shown in the image below:



The system supports ***.jpg, *.jpeg, *.bmp, *.wmf, *.png and *.gif** images.

After choosing the image, it will be displayed in the center of the screen as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

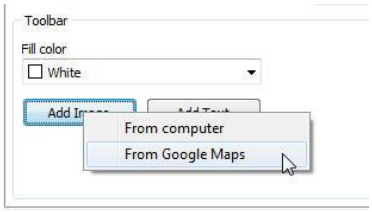


You will now be able to resize and position the image on the map using the resize controls displayed around the image when selected.

12.1.2 Google Maps Integration

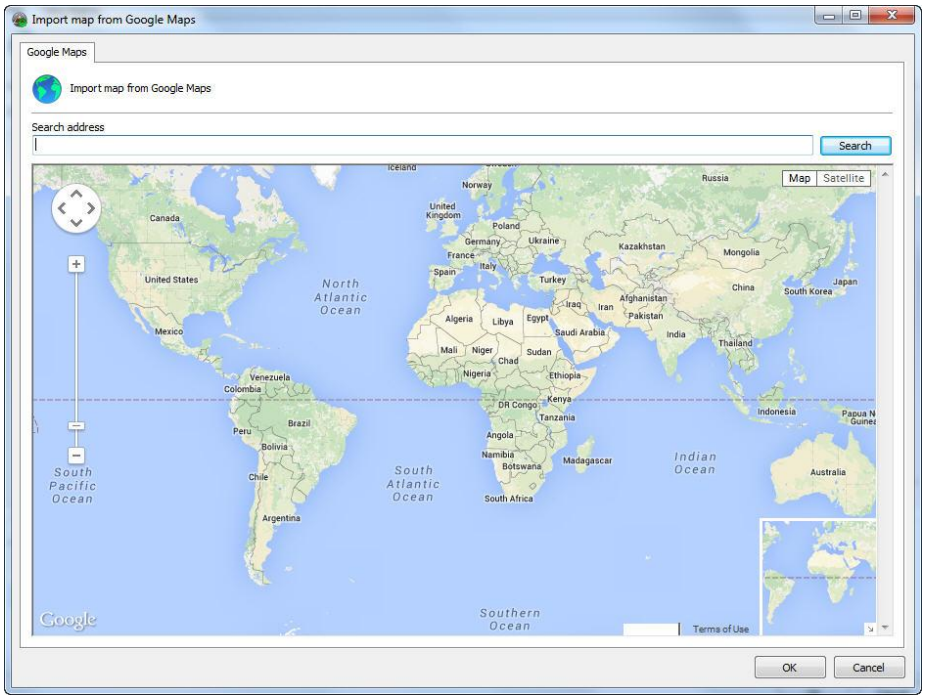
For ease, the map screen allows a photo to be taken directly from Google Maps.

Click on **Add Image** and then on **From Google Maps** as shown in the image below:

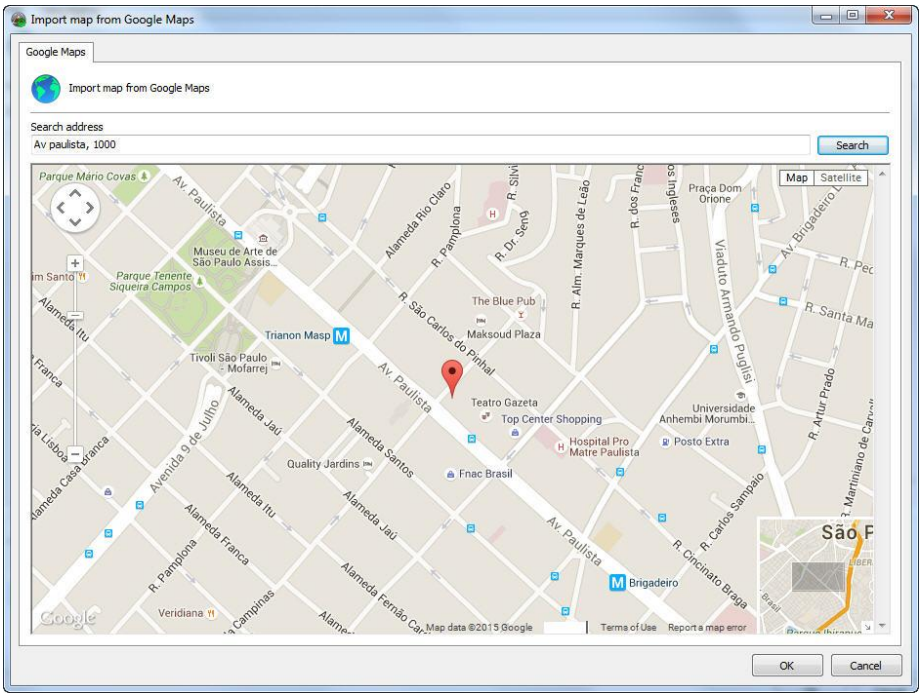


A screen will open with Google maps. **Note:** This feature requires an internet connection.

© 2002 - 2024 by Digifort. All rights reserved.

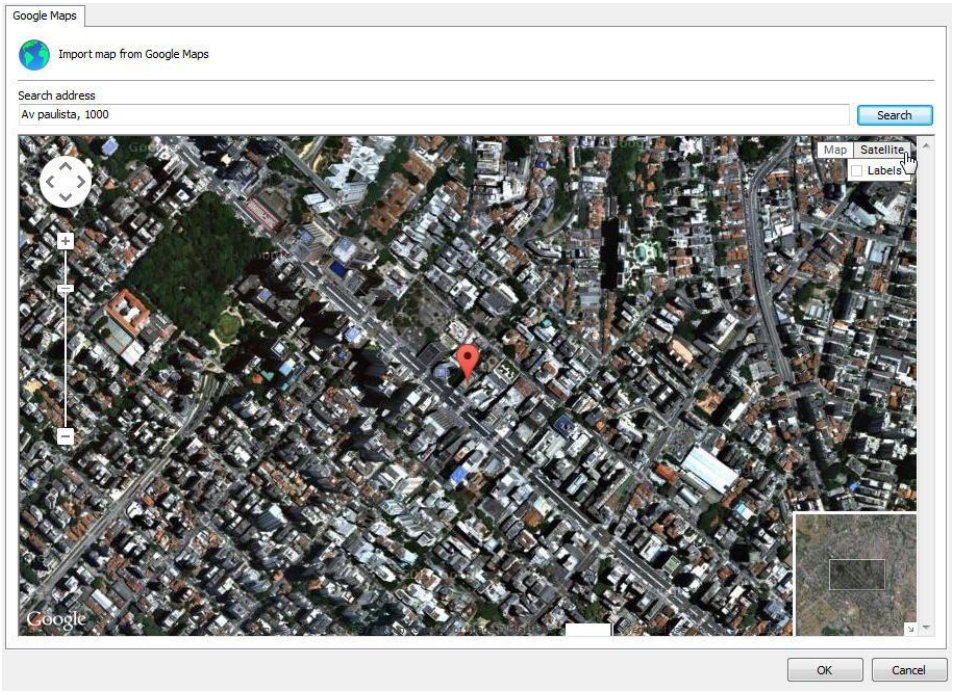


Navigation can be done with the mouse or an address can be typed directly into the **Search Address** field:



Through the address, the system will consult the map on Google Maps, which allows both the visualization of maps and satellite photos:

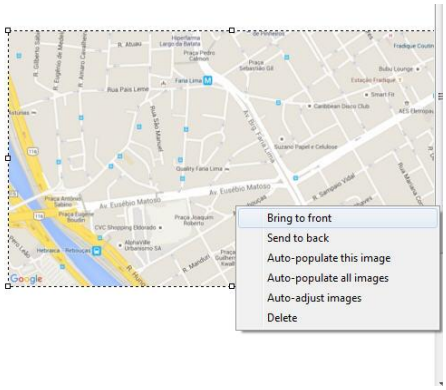
© 2002 - 2024 by Digifort. All rights reserved.



After choosing the desired position, just click OK and the current position will be used as the background image for your map.

You can place more than one image on the map, just click on **Add Image** and then on **From Google Maps** again. With this option it is possible to create larger maps composed of several Google images. The system allows self-adjustment of images based on their location to facilitate their organization and merging.

When right-clicking on an image, the following options will be available:



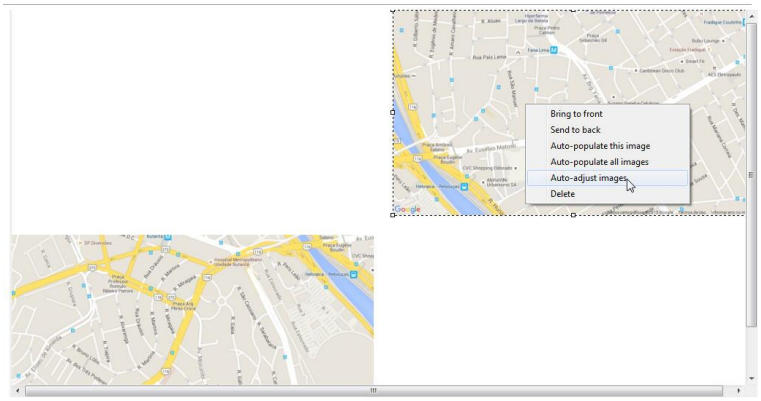
- **Bring to Front:** Positions the selected image above other images on the map.
- **Bring to Back:** Positions the selected image below other images on the map.
- **Auto-populate this image:** From the longitude and latitude configuration registered in the objects, the system will automatically position the objects in the selected image that have the same coordinates. See the chapter How to add a camera to learn how to register the coordinates of the cameras.
- **Auto-populate all images**: Based on the configuration of longitude and latitude registered in the objects, the system will automatically position the objects in all images on Google Maps that have the

© 2002 - 2024 by Digifort. All rights reserved.

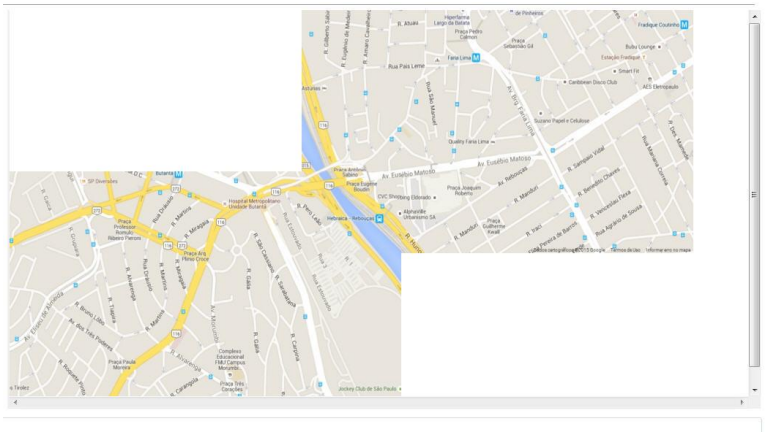
same coordinates. see the chapter How to add a camera to learn how to register the coordinates of the cameras.

- **Auto-Adjust images**: This option allows Digifort to auto-organize Google images based on their coordinates, thus facilitating this work to be done manually in cases where more than one image is needed to create a larger map. See the examples:

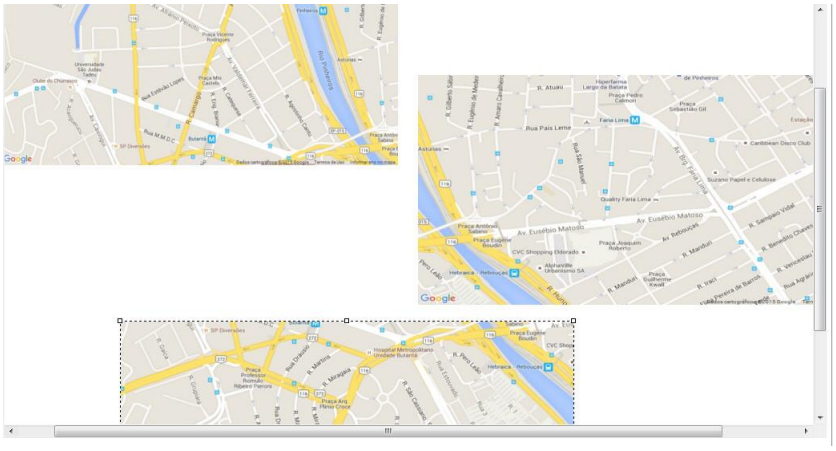
Two separate images:



After the auto-adjust command:

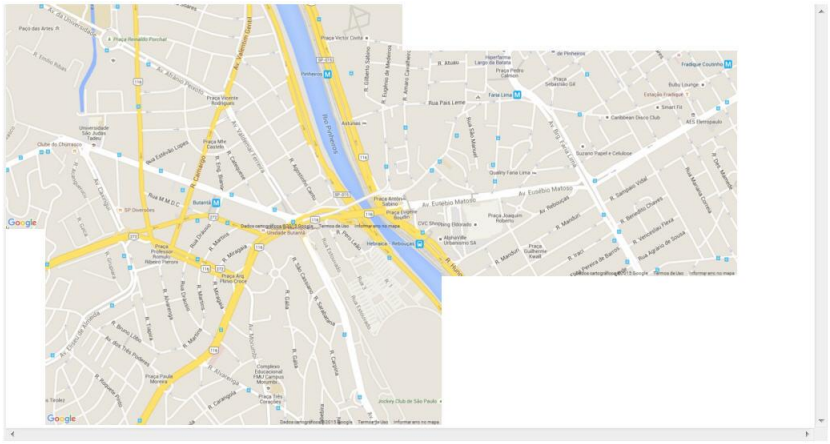


3 separate images:



© 2002 - 2024 by Digifort. All rights reserved.

After the auto-adjust command:



Note

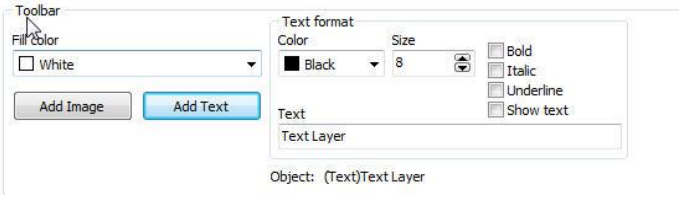
Auto-Adjust takes into account the size of the selected image, so the other images will be resized based on the selected image.

12.1.3 Adding Texts

In the button **Add** text, legends can be added to the map. Once created, you can edit its text and its font. Just select it and change the Text Formatting properties found at the bottom of the screen.

These options are valid for any map text object:

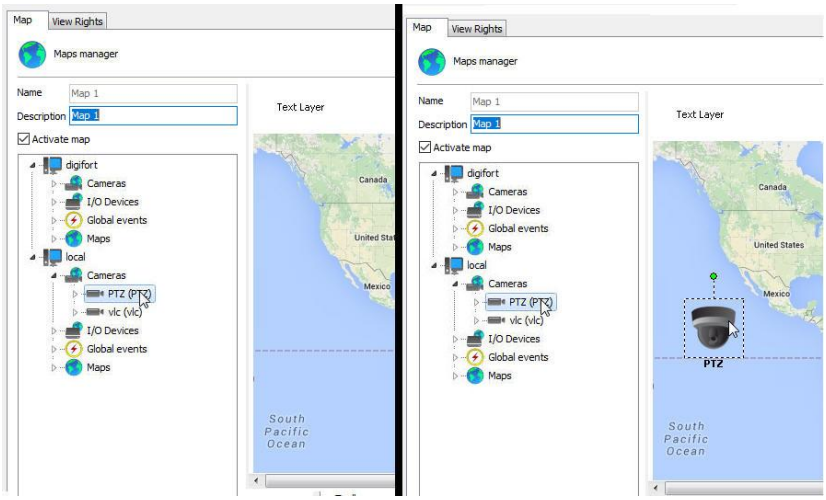
- **Color:** Changes the text color.
- **Size:** Changes the text size.
- **Text:** Changes the subtitle text.
- **Bold:** Makes the text bold.
- **Italics:** Makes the text italicized
- **Underline:** Underlines the text.
- **Show Text:** Show text or not in an object.



12.1.4 Adding Cameras

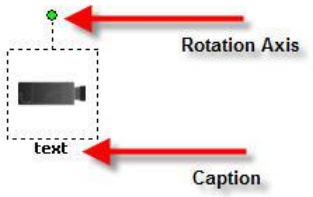
To position the objects on the map, just drag them from the list positioned on the left of the screen, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



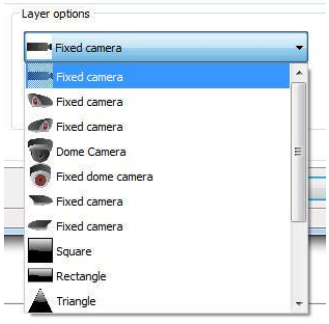
From the list of cameras located on the left, drag the desired camera onto the map. It will take the form of a camera on the map as shown in the figure below:

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.

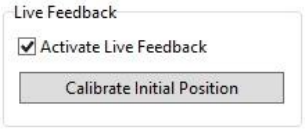
It is possible to change the camera icon, select it and in the Layer Options menu choose the desired icon as shown in the figure below:



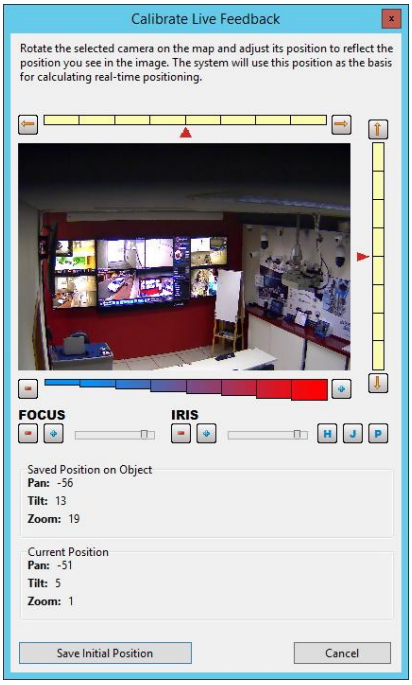
There is also an option to change the size and color of the icons. In the layer's Options menu, locate the **Size** and **Color** boxes shown in the figure and change the values by clicking on them.

© 2002 - 2024 by Digifort. All rights reserved.

In addition, it is possible to configure live feedback on PTZ cameras. Live Feedback will provide the current position of the camera on the map by rotating the camera icon to where the camera is currently facing. In the Live Feedback menu select the option to enable live feedback and calibrate your starting position.



When clicking on the calibrate initial position button, the following window will open:



On this screen, position the camera to match the current position of the camera icon on the map and click **Save Initial Position**.

12.1.4.1 Camera Field of View

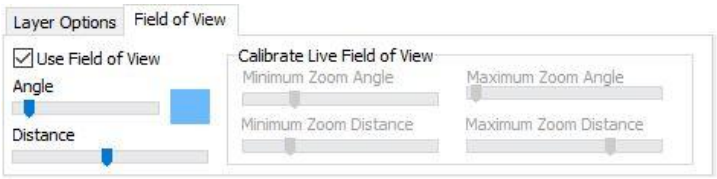
The synoptic map system now allows the display of a visual representation of a field of view of the cameras. You can configure the field of view for any camera on the synoptic map.

Note

The field of view feature is only available for Synoptic Maps and is not available for Operational Maps.

Select the **Field of View** tab and adjust the values accordingly:

© 2002 - 2024 by Digifort. All rights reserved.

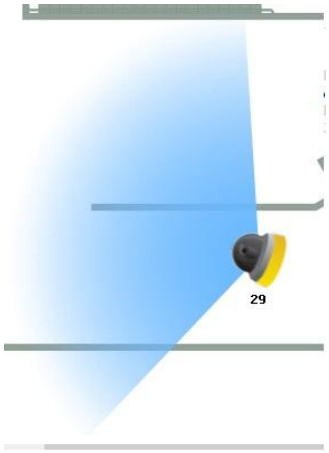


- **Angle:** The greater the opening angle, the "wider" the field of view will be.
- **Distance:** The greater the configured distance, the longer the mark on the map.
- **Color:** By clicking on the blue square it is possible to choose another color for marking the field of view.

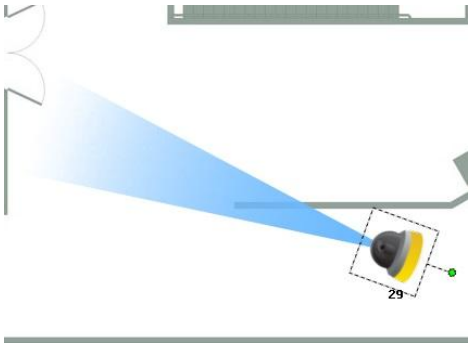
Within the field of view calibration we have the options (Only for PTZ cameras with this feature integrated):

- **Minimum Zoom Angle:** Specify the camera's field of view when the zoom is as small as possible.
- **Minimum Zoom Distance:** Specify how far you can see with the camera at its minimum zoom.
- **Maximum Zoom Angle:** Specify the camera's field of view when zoomed in as far as possible.
- **Maximum Zoom Distance:** Specify how far you can see with the camera at its maximum zoom.

Below is an example of a camera with maximum and minimum zoom:



Camera with minimum zoom, having a greater field of view and shorter distance.



Camera with maximum zoom, having a smaller field of view and greater distance.

The field of view is not required to be re-saved when calibrating the home position, as the home position is independent of the field of view.

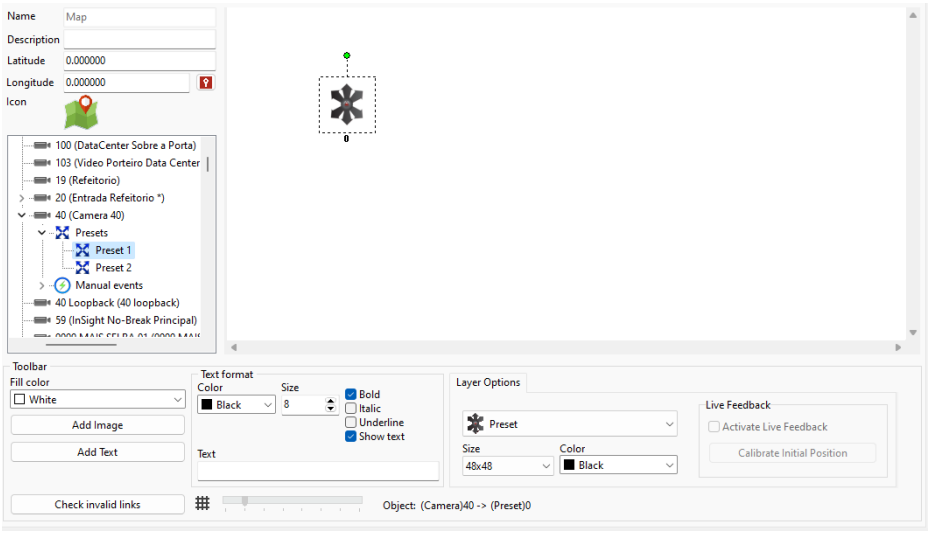
© 2002 - 2024 by Digifort. All rights reserved.

The live feedback feature will only be available for cameras that have built-in PTZ driver. Check the models with integrated PTZ on our website.

12.1.4.2 Adding Presets

If your PTZ camera has presets registered, you can drag the preset icons on the map, allowing the operator to position the camera in the preset quickly, just by clicking on the preset icon.

To add camera presets to the map, drag the desired preset icon inside the camera:



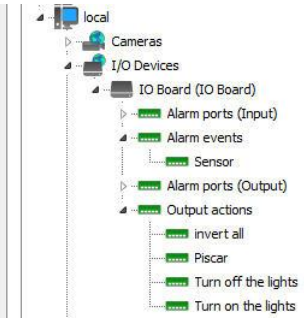
- **Image:** Select an image to represent the preset icon on the map
- **Size:** Select image size
- **Color:** Select icon color

12.1.5 Adding Input Events, Output Actions, and I/O Ports

The system allows you to create icons with visual representations of alarm input event status, alarm input and output port status, virtual port status and buttons for alarm output actions from Cameras or I/O Devices. The icons for alarm input events or alarm input ports will represent the current state of the event or input port (whether it is open or closed). The alarm output actions icons. To learn more about I/O, see the topic on Camera I/O.

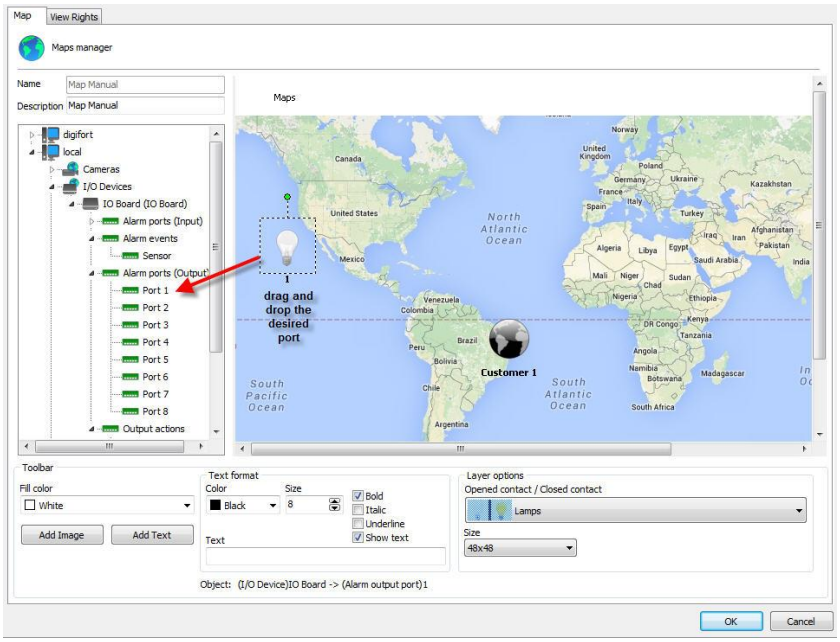
12.1.5.1 Adding Events Or I/O Ports

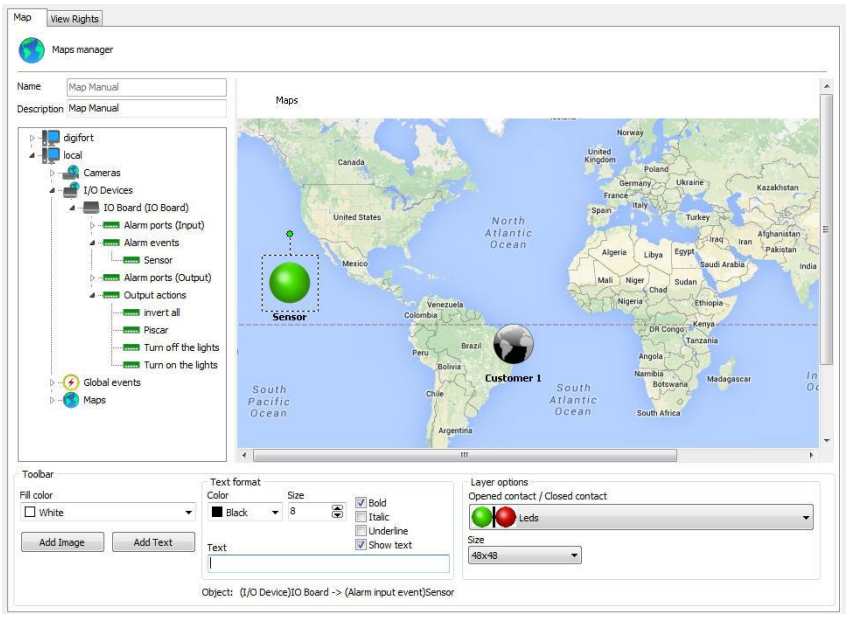
To add events or I/O port status to the map, simply drag them from the list positioned on the left of the screen as shown in the figure below.



© 2002 - 2024 by Digifort. All rights reserved.

You can drag the available objects within Cameras or I/O Devices. In the figure above we have the objects of an I/O Device.





The event icon and its size can be changed just like the camera icons. Just select the desired object and go to the Layer Options as shown in the figure below:

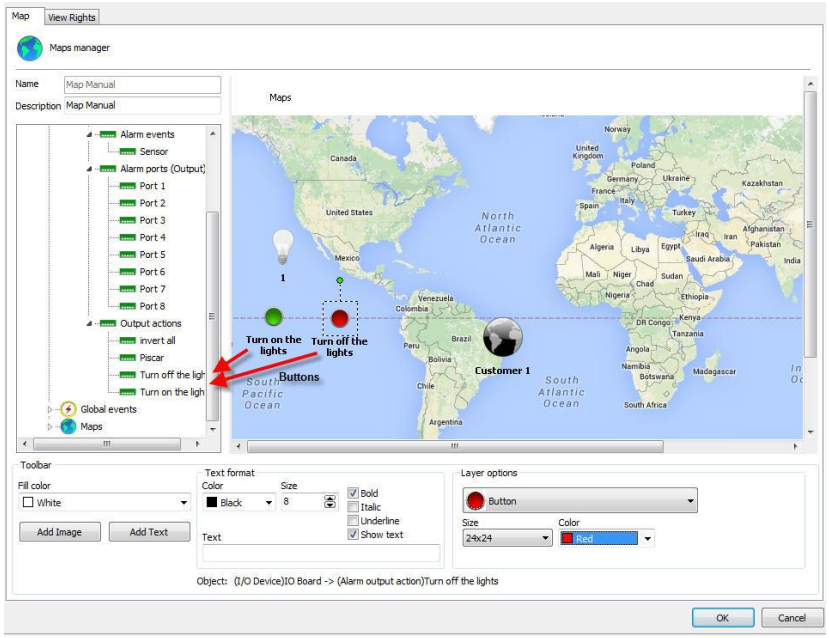
© 2002 - 2024 by Digifort. All rights reserved.

- **Image:** Select the appropriate image to represent the event or port on the map. The objects have two images to represent the different states of the event or port. The image on the left will represent the object when the port is open. The image on the right will represent the object when the port is closed. For input events, the image on the left will represent the object when the event is not occurring, and when the event occurs, the icon will flash, switching between the two images until the operator confirms the alarm by double-clicking on the map object in the Surveillance Client.
- **Size:** Select icon size

12.1.5.2 Adding Output Actions

The output action buttons are intended to activate or deactivate an alarm output in the system.

Drag the desired output action icons onto the map:



- **Image:** Select an image to represent the exit action icon on the map
- **Size:** Select image size
- **Color:** Select icon color

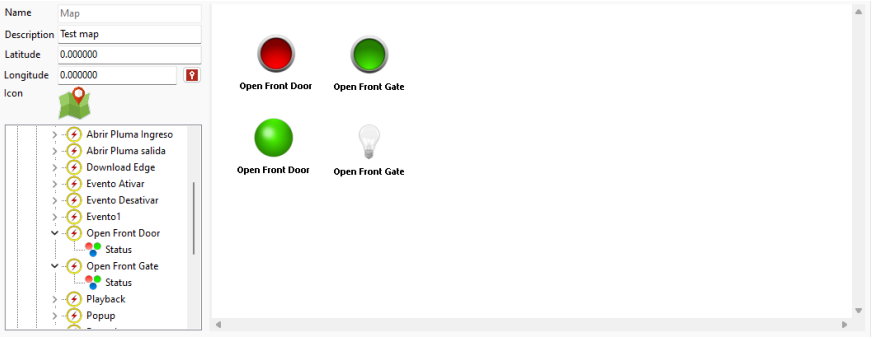
In the Surveillance Client, if the operator has the right to activate alarm outputs, he can click on the corresponding icon on the map and the action will be executed.

12.1.6 Adding Global And Manual Events

The system allows you to create icons with visual representation for Global and Manual Events (Registered in Cameras). You can add actions for the operator to activate the event, and you can also add event status icons.

To add Global or Manual Events, drag the corresponding icons from the list (Manual events are found inside camera objects):

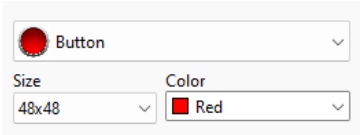
© 2002 - 2024 by Digifort. All rights reserved.



If you drag the main event icon, the icon on the map will be an action button for the Surveillance Client operator that they can click to trigger the event.

You can also drag the event status, to do this simply select the **Status** icon located within the corresponding event.

Event objects have the following properties:



- **Image:** Select an image to represent the event icon on the map
- **Size:** Select image size
- **Color:** Select icon color

Status objects have the following properties:

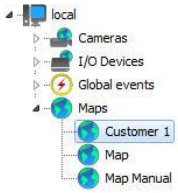
- **Image:** Select the appropriate image to represent the event on the map. The image on the left will represent the object when the event is not occurring, and when the event occurs, the icon will flash, switching between the two images until the operator confirms the alarm by double-clicking on the map object in the Monitoring Client.
- **Size:** Select icon size

12.1.7 Map Link

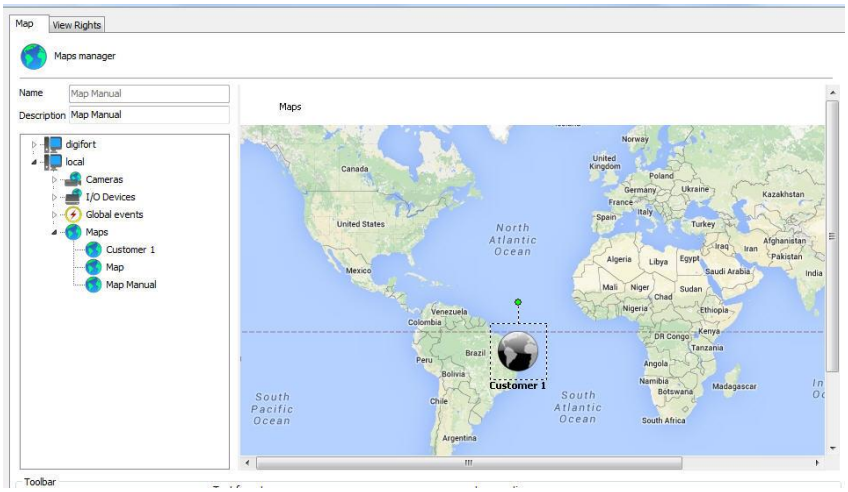
The map link is a feature to improve map management. Within a created map you can create links to other maps (Synoptic or Operational), thus facilitating navigation between them.

To create links you need to have two or more maps registered, when there is more than one map registered in addition to the one being used, they will appear in the list of maps as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



Click and drag the object to the map as shown below:



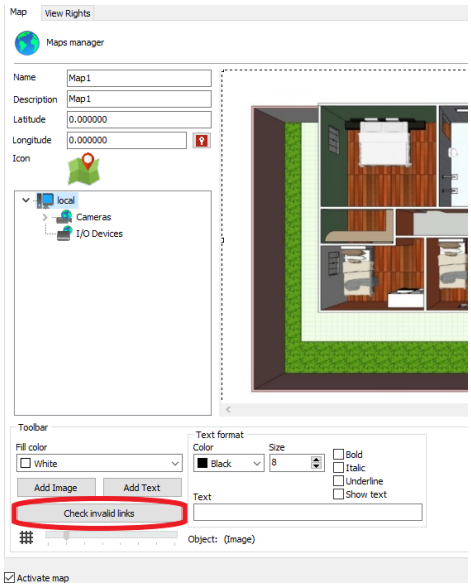
When opening the map in the Surveillance Client, the icon on the screen will call the next map when clicked.

12.1.8 Checking For Invalid Objects In Maps

The map editing tool in the Administration Client lets you check if there are any invalid links in the map and tries to find an object with the same name on another server to fix the link.

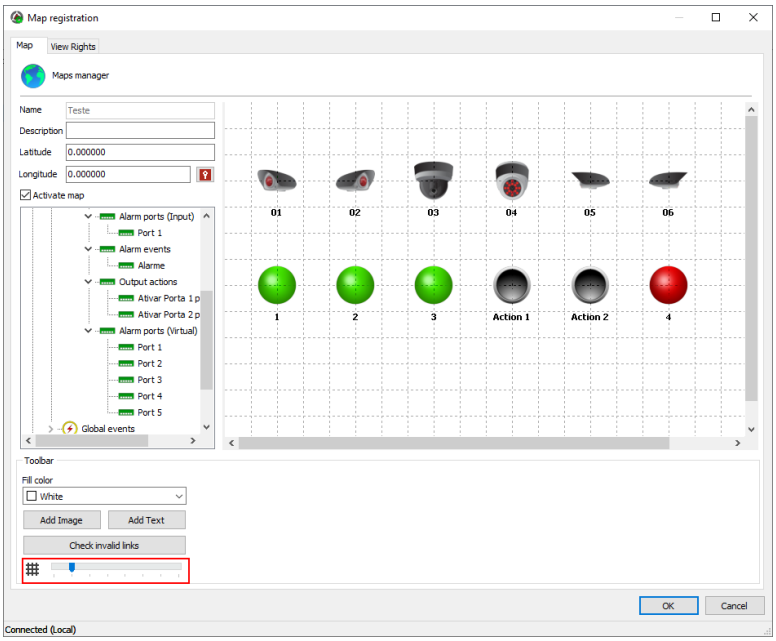
Object links in maps can be broken when an object is removed or also in case the server machine code changes, in which case link checking can fix all invalid links without the need to position all objects again.

© 2002 - 2024 by Digifort. All rights reserved.



12.1.9 Alignment Grid

The map creation tool also has an alignment grid for better map design. The grid will only be displayed in the editor and can be adjusted by moving the slider denoted in the picture below:



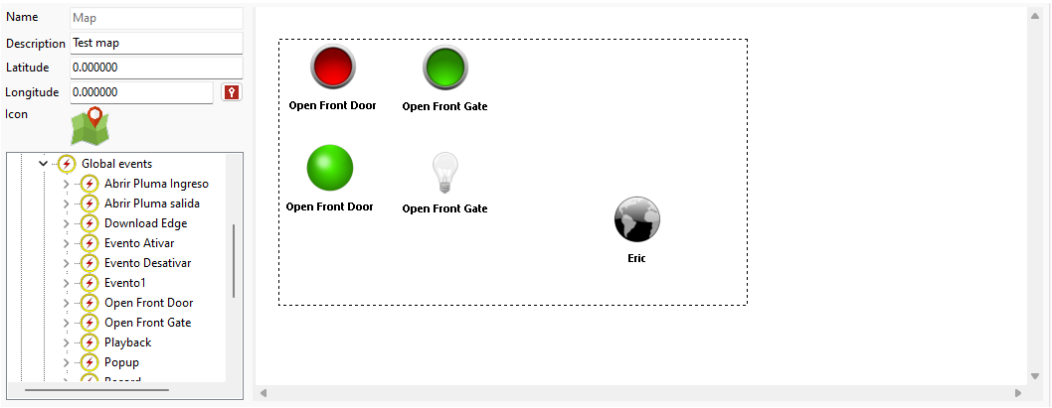
With the grid active, you can now drag objects and they will "stick" to the intersections of the lines.

12.1.10 Map Editor Tips

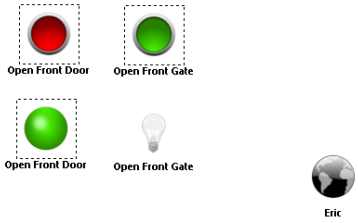
12.1.10.1 How To Select Multiple Objects

In the map editor, you can select multiple objects at the same time to move or delete. To select objects, simply click and drag with the right mouse button, and a selection rectangle will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



You can also select multiple objects individually. To do this, hold down the **Ctrl** or **Shift** key on your keyboard while clicking on the objects to select:



12.1.10.2 How To Delete Objects

To delete objects in the map editor, simply select the desired objects and press the **Delete** button on the keyboard. You also have the option to right-click and select the **Delete** option.

12.1.10.3 Move objects with precision

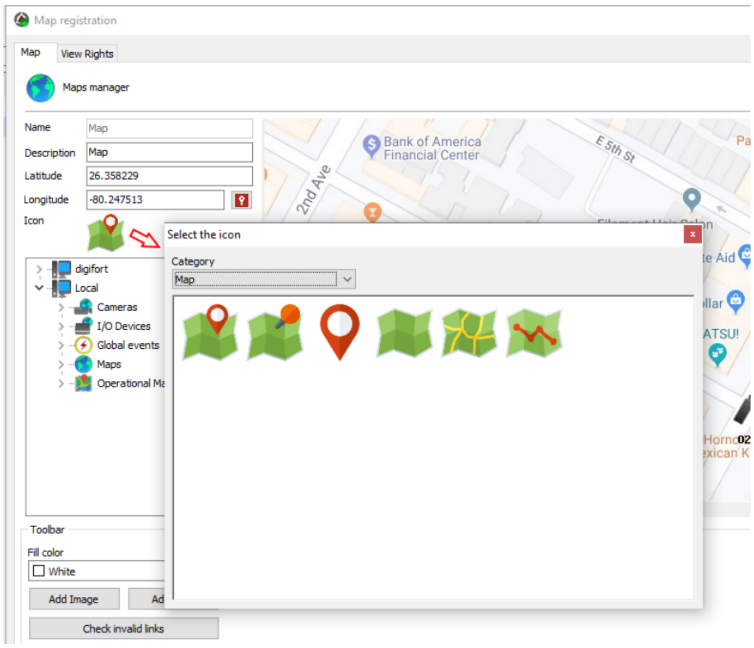
The map editor allows you to move objects pixel by pixel for greater precision when creating the map. To move objects with 1 pixel precision, select the desired objects and press the directional arrows on the keyboard while holding down the CTRL key.

12.1.11 Icon for Operational Map

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

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

© 2002 - 2024 by Digifort. All rights reserved.



12.1.12 Object Status

The device status identifier in synoptic maps will reflect the current recording state in the Surveillance Client's live map component.

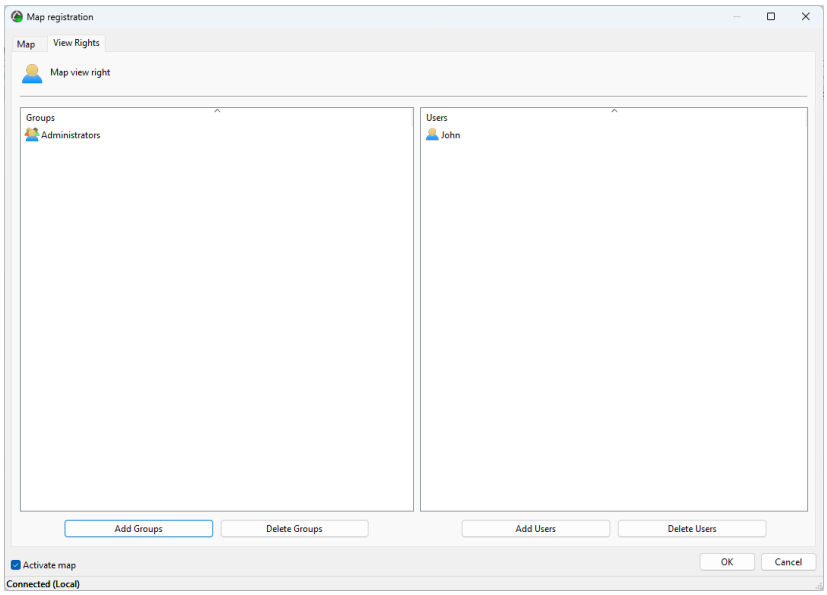
- Identifies that the device is working and currently writing to disk.
- Identifies that the device is working but is not currently writing to disk
- Identifies that the device is out of order

The absence of a state identifier indicates that the device is disabled.

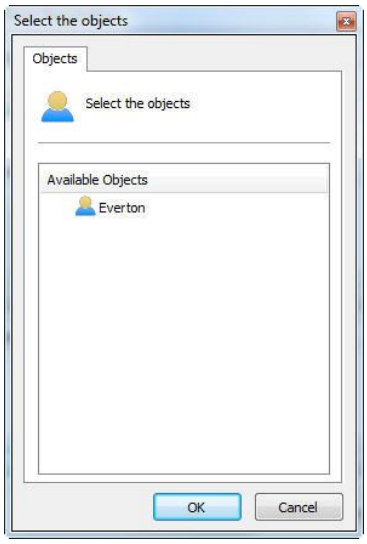
12.1.13 Rights

On the **Viewing Rights** tab you can define the list of users and user groups that will have the right to view this map in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

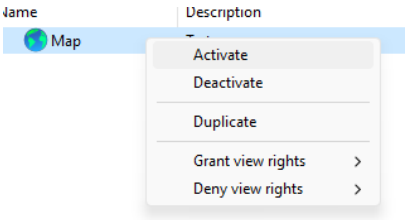


Select the available User and click **OK**. The same rule applies to the group list.

12.2 How To Change Parameters For Multiple Maps Simultaneously

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

© 2002 - 2024 by Digifort. All rights reserved.



Most of the options you can change are self-explanatory and you can consult the Map Registration topic to learn more about each option.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XIII

13 Operational Map

Operational maps have advanced applications within servers with several cameras, monitoring different points, for example, in a city.
This is a feature that, through integration with Google Maps, allows the creation of navigation maps and event maps.

The **navigation maps** provide an overview with the geo-positioning of all cameras in the system (which have geo-positioning activated) and will allow access to these cameras through icons referenced on the map. If the Monitoring Client is connected to multiple servers, the operational map will focus and display 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 offers a detailed view of the locations where events are occurring and allows the operator to access cameras close to an event, thereby accelerating response to the event.

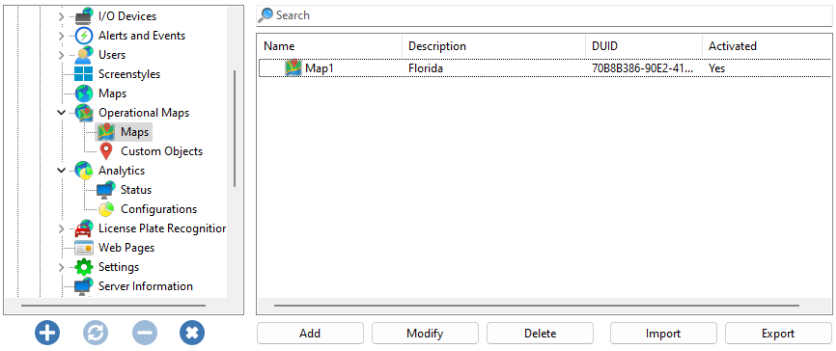
Maps can be registered and configured to automatically display a region of the globe when placed on the screen, thus allowing the creation of maps for different regions.

Event maps can also be configured to filter and display events from just a few categories and events can also be filtered by geo-location, meaning only events from a specific region will be populated on the map.

13.1 Registering Operational Maps

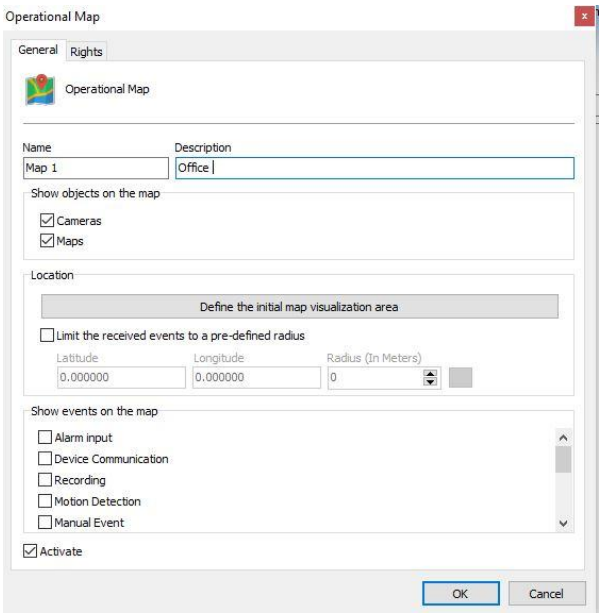
To add **Operational Maps**, in your Administration Client, search for the **Operational Maps** item and click on **Maps**:

The Operational Map Registration screen will be displayed:



Click **Add** to add a new map.

© 2002 - 2024 by Digifort. All rights reserved.

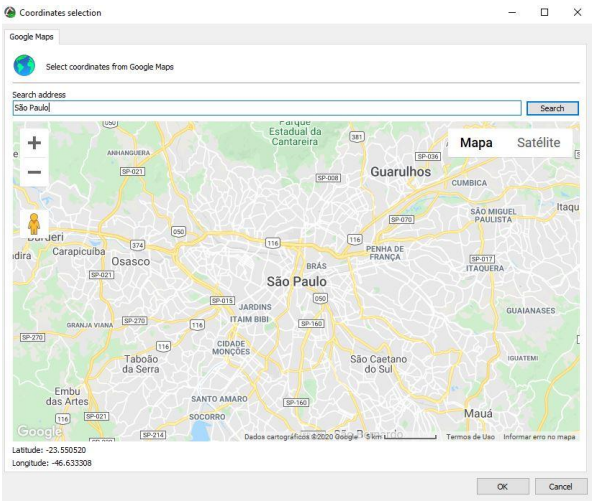


To change an already registered map, select it and click **Modify**, and change the data as explained on the following pages.
To remove a map, select the desired map and click the **Remove** button.

- **Name:** Name of your Operational Map.
- **Description:** Description of your Operational Map.
- **Show Objects on the Map:** Select which objects should appear on the map, between Cameras and Internal Synoptic Maps.

Location

- **Define the intial map visualization area:** Defines the starting point for displaying the map on the screen, e.g.:



On this map screen you must adjust the map to your starting position. The position where you leave it will be loaded into the Surveillance Client when the operator puts this map on screen.

© 2002 - 2024 by Digifort. All rights reserved.

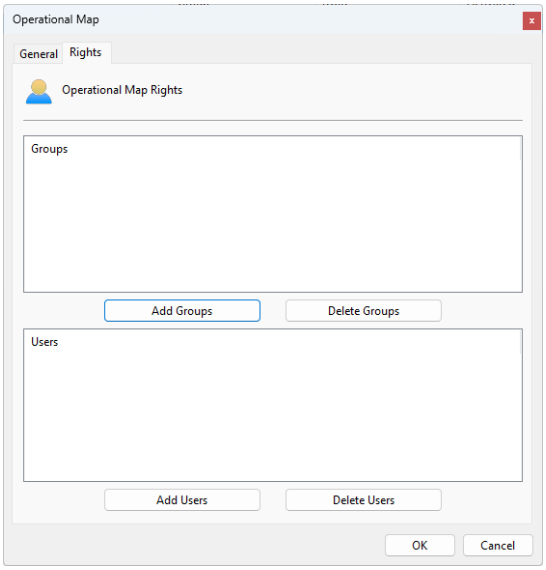
- **Limit the received events to a pre-defined Radius:** Determines an area of the map, in Latitude, Longitude and Radius, where events triggered by the system will only be displayed on the map if they are within the defined radius.
- **View Events on the Map:** Filter to determine what type of event will be displayed on the map.

Important

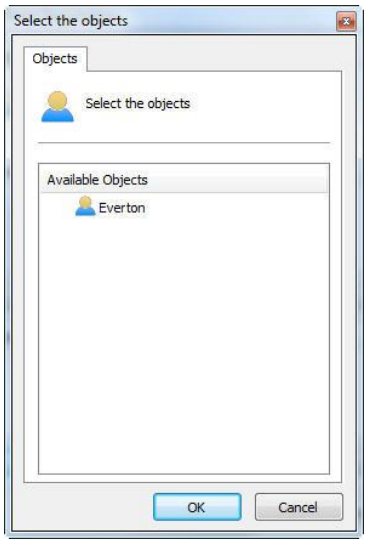
You must configure Google Maps integration in Server Settings. See the Google Maps Configuration topic for more information.

13.1.1 Rights

On the **Rights** tab you can define the list of users and user groups that will have the right to view this map in the Monitoring Client.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

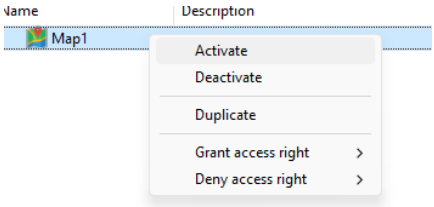


© 2002 - 2024 by Digifort. All rights reserved.

Select the available User and click **OK**. The same rule applies to the group list.

13.1.2 How To Change Parameters For Multiple Maps Simultaneously

The system's operational map manager provides quick access to the most common settings that can be changed for multiple operational maps simultaneously. In the operational maps register, select the desired maps and right-click. A menu will open as shown in the figure below:



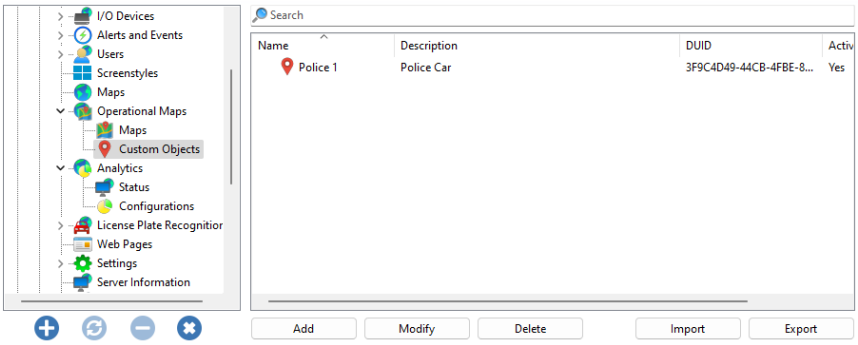
Most options you can change are self-explanatory and you can consult the Operational Maps Registration topic to learn more about each option.

13.2 Custom Objects

The system allows the creation of custom operational map objects. These are objects that will be displayed on the desired operational maps and can be associated with an object that will be displayed if the operator clicks on the custom object icon. The position of custom objects can be updated via API for integration with third-party systems. See the API manual to learn how to dynamically update the position of custom objects.

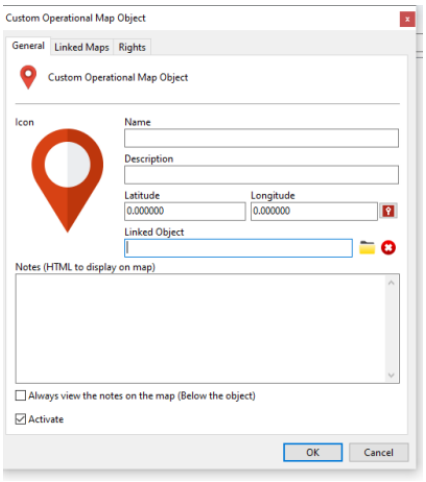
To add **Custom Objects** to **Operational Maps**, in your Administration Client, search for the **Operational Maps** item and click on **Custom Objects**:

The Custom Object Registration screen will be displayed:



Click **Add** to add a new **Custom Object**:

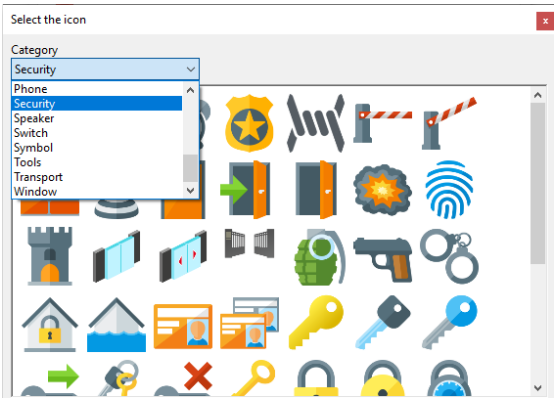
© 2002 - 2024 by Digifort. All rights reserved.



To modify an already registered object, select it and click **Modify**, and change the data as explained on the following pages.
To remove an object, select the desired object and click the **Remove** button.

- **Name:** Object name.
- **Description:** Description of the object for easy identification in the system.
- **Latitude and Longitude:** Geo-referenced coordinates of the object.
- **Linked Object:** Object to be associated with this icon on the map.
  - **Select Button:** Selects the associated object. A screen will be displayed for selecting an object in the system.
  - **Clear Button:** Removes association with object.
- **Notes (HTML to be displayed on the map):** Observations and notes in HTML format that can be displayed on the map
- **Always view the notes on the map (Below the object):** If activated, this option will make the notes always visible, regardless of whether the operator has the mouse under the object
- **Activate:** Activate or deactivate the object

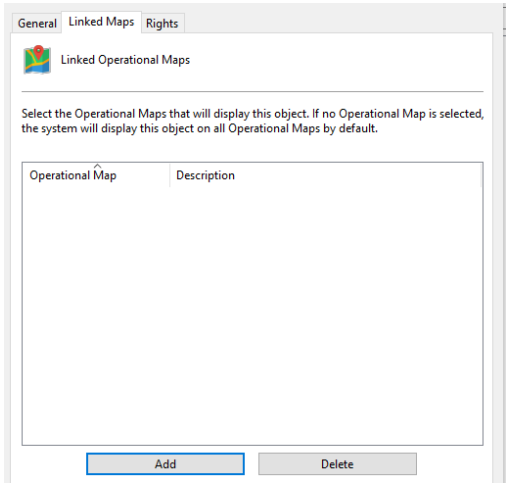
To select the icon for this object, simply click on the icon image (by default the red pointer) and select the desired icon:



13.2.1 Linked Operational Maps

The **Linked Maps** tab allows you to select which maps will have this object associated with it, that is, this object will only be displayed on the maps selected in this list:

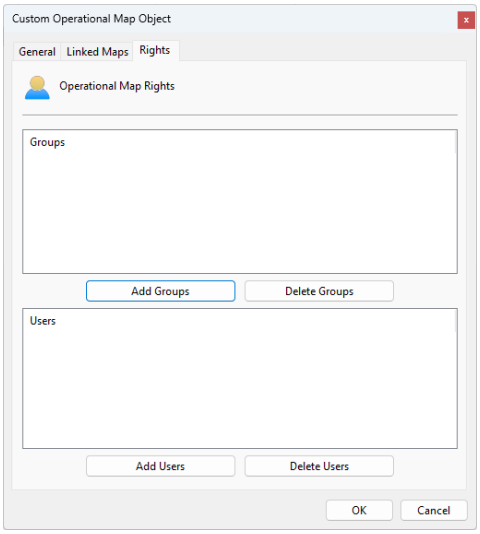
© 2002 - 2024 by Digifort. All rights reserved.



Click **Add** to select maps and **Delete** to delete links to operational maps.

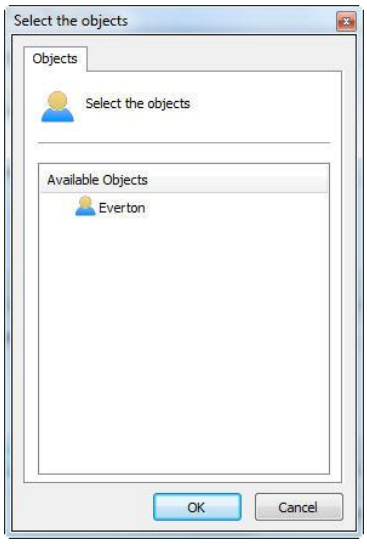
13.2.2 Rights

On the **Rights** tab you can define the list of users and user groups that will have the right to see this object in Operational Maps.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

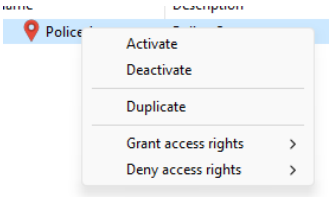
© 2002 - 2024 by Digifort. All rights reserved.



Select the available User and click **OK**. The same rule applies to the group list.

13.2.3 How To Change Parameters Of Multiple Objects Simultaneously

The system's custom object manager provides quick access to the most common settings that can be changed for multiple custom objects simultaneously. In the custom object register, select the desired objects and right-click. A menu will open as shown in the figure below:



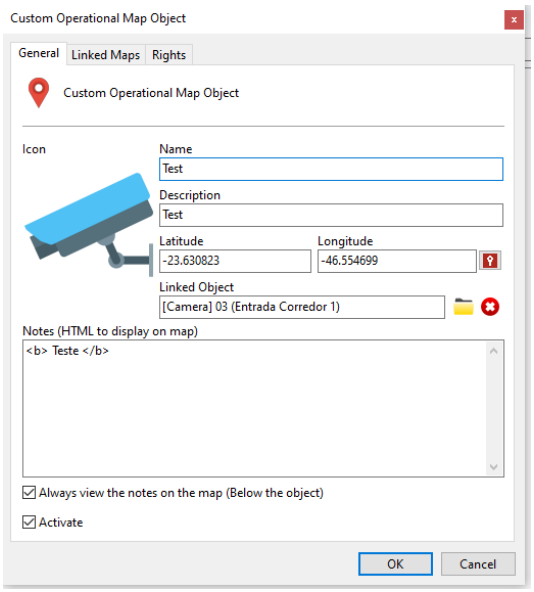
Most of the options you can change are self-explanatory and you can consult the Custom Object Registration topic to learn more about each option.

13.2.4 Working Example

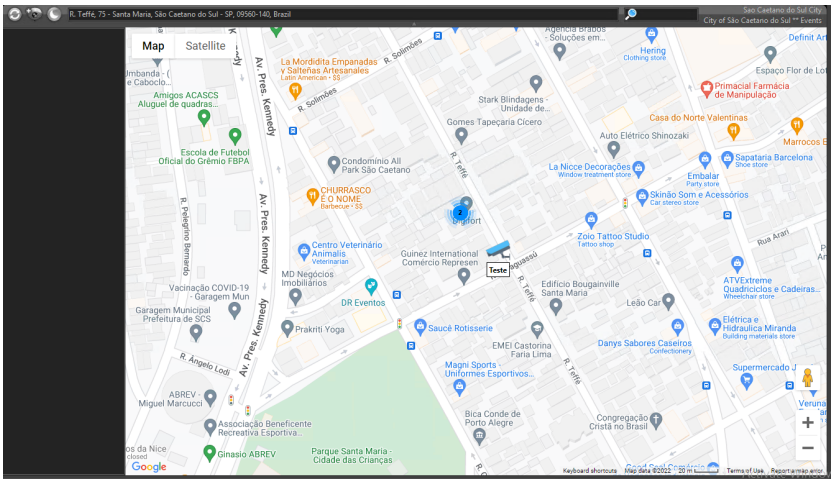
Below we can see how a Custom Object works.

Registered Object:

© 2002 - 2024 by Digifort. All rights reserved.



In this example we will have a camera with the name **Test** associated with camera 03 on the server with the "test" notes in bold being displayed on the map:



If the Surveillance Client operator clicks on this object, camera 03 will be opened.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XIV

14 Analytics

Analytics is a set of tools that processes camera images in an intelligent way. This processing includes object counting, flow control, objects left and removed, face detection and others that we will see in detail below. This system is capable of detecting the moment when there is a violation of pre-defined rules and triggering alarms in order to attract the attention of the operator.

Analytics can complement monitoring in a variety of ways such as triggering alarms, archiving events, and generating reports.

Analytics is considered an additional module as it is not included in the camera server license.

The system supports server-side or edge analytics processing. In the case of server-based analytics, camera images will be processed by the system's analytics module, on servers dedicated to image processing. In edge analytics, the cameras themselves already process the images and only send metadata and events to the system.

Analytics has its own server/service for image processing, which can be installed on the same machine where the cameras are recorded or on another computer designed just for this service (most recommended). Learn more about distributed processing in the chapter Understanding distributed processing.

14.1 Server Analytics

14.1.1 Understanding Distributed Processing

Video analysis in terms of processing is more demanding than recording/viewing a camera. Thinking about flexibility, the system has an innovative processing architecture which is the distributed processing architecture.

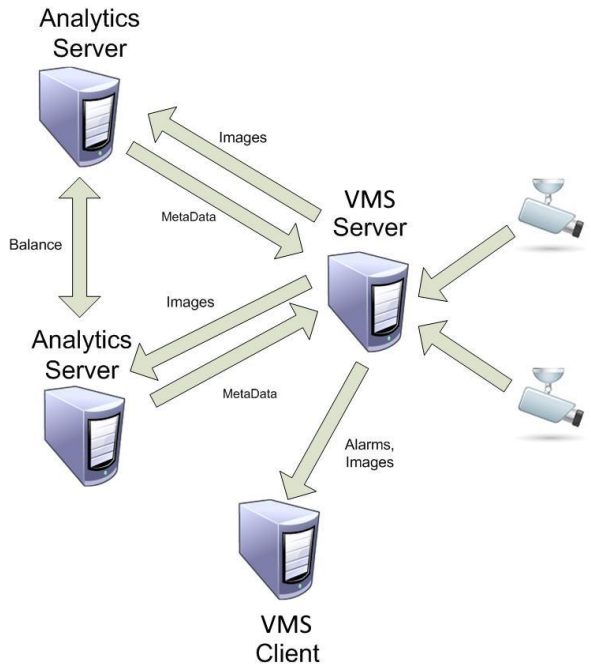
The system allows the analytics processing of cameras that are recorded on the camera server to be done on one or more computers that have the Analytics Server module. The great advantage is that with this flexibility the recording server is not overloaded and does not need to be a "super-machine".

The analytical server automatically checks the computers with less processing and performs a "load balancing", that is, it distributes the processing of video analyzes in order to leave all computers with the least possible processing, as long as all servers have sufficient licenses.

What determines the amount of analytics that can run on the same server is the processing capacity of this server. The larger the processor, the greater the possibility of running several cameras at the same time and several analytics on the same camera. The system processes analytics on fixed and mobile IP cameras and on fixed and mobile analog cameras, as long as these are converted through encoders or DVRs integrated into the system.

See the diagram below:

© 2002 - 2024 by Digifort. All rights reserved.



In the diagram above, the **VMS Server** records the images from the cameras and sends them to the **Analytics Servers** which in turn carry out the analyzes and return the metadata (information about the alarms that are generated, position of objects and areas of alarms). Between the **Analytics Servers** there is load balancing, if configured for that. When the metadata is returned to the **VMS Server**, it sends the metadata and alarms to the **VMS Client** (Surveillance Clients).

14.1.2 How To Start The Analytics Server Service

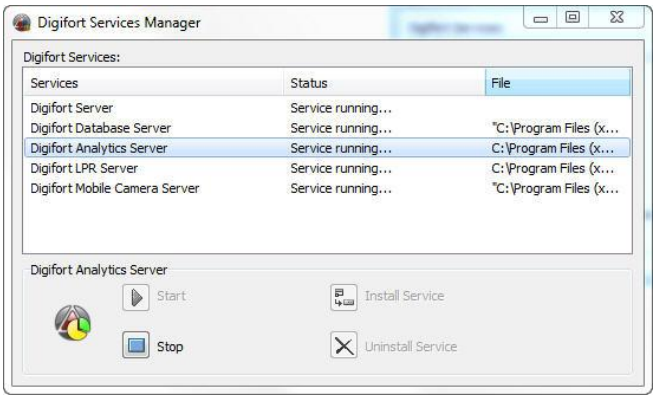
To start the Analytics Server service, it must first be installed, follow the steps below to correctly start the service using the Service Manager:

1. Select the **Analytics Server** service.

2. Click **Install Service**, a confirmation window will be displayed to select the service architecture (32 or 64 bits), informing you that the service was installed successfully.

3. Click **Start** and wait while the server starts. The initialization process ends when the message “Service running...” appears in the status bar.

© 2002 - 2024 by Digifort. All rights reserved.



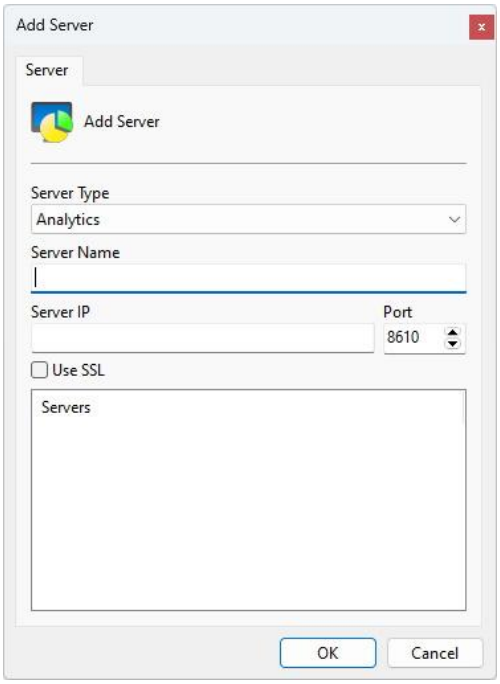
Important

- The **Basic Analytics** Module requires the 32-bit version of the Analytics Server
- The **Advanced Analytics** Module requires the 32-bit version of the Analytics Server
- The **Professional Analytics** Module requires the 64-bit version of the Analytics Server

14.1.3 How To Configure The Servers To Be Managed

The first step to be taken when configuring 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 **Analytics Servers** tree and then on the **Add Server** button, opening the server registration screen, as shown below:



- **Server Name:** Enter the name of the server to be added. After confirming the data, the server name cannot be changed.
- **Server IP:** Enter the IP of the server to be managed.
- **Port:** Type the communication port with the server. By default the port is 8610 or 8410 for secure connection with SSL/TLS.

© 2002 - 2024 by Digifort. All rights reserved.

- **Use SSL:** Use secure connection with SSL/TLS. Don't forget to specify the SSL/TLS connection port.
- **Servers:** In this list, all the Analytics servers that the administration client found on the network will be available. By clicking on one of the servers, the IP and Port field described above will be automatically filled in, leaving only the Server Name field to complete the registration.

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

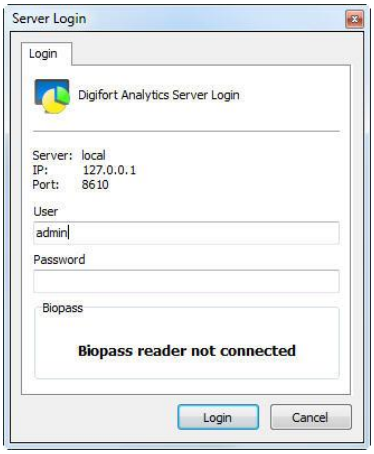
After adding the server, it will be shown in the Settings Menu as shown in the figure below:

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

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

14.1.4 How to Connect to a Server for Management

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

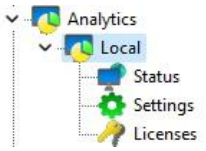


- **User:** Login user.
- **Password:** Access password.

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

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

© 2002 - 2024 by Digifort. All rights reserved.



14.1.5 Licensing Analytics Server

The Analytics server license works like the camera server, there is a "Base License" for the server and "Engine Licenses" for each camera.

The Base License of Analytics module includes **Basic Analytics** which contains the following modules: **Left Objects, Removed Objects and Face Detection** which can be used in as many cameras as desired**.**

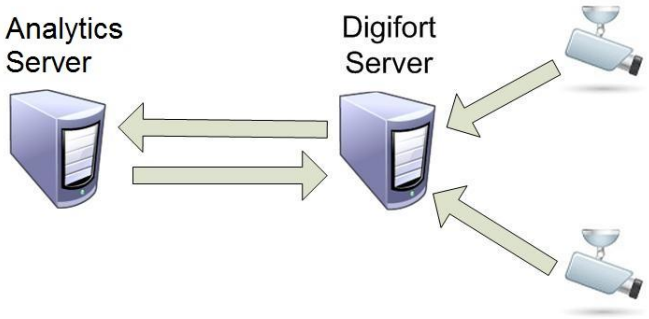
Engine Licenses contain the license for the **Advanced Analytics** which has the following modules available: **Presence, Enter, Exit, Appear, Disappear, Stationary, Loitering, Direction Filter, Speed Filter, Camera tampering and Shaking Cancellation**. There is also a license for **Professional Analytics** which is a more powerful engine, using Deep Learning and processing via GPU for filters and more complex scenarios, having the following modules available: **Abandoned object, appear , color filter, continuous filter, counter, line count, deep learning, direction, disappear, enter, exit, logic rules, loitering, object, presence, previous, speed, stationary object, tailgating, among others.**

The **Professional** module requires the use of GPU and 64-bit analytics service architecture. Consult our technical support for server sizing for this module at support@digifort.com.

Important

- **The Basic Analytics engine is already deprecated and is no longer supported or developed, being maintained only for compatibility.**
- **The Advanced Analytics engine is already deprecated and is no longer under development, being maintained only for compatibility.**

The following diagram shows the licensing of two cameras with video analysis together with the VMS server:



In the figure above, the distribution of licenses would look like this:

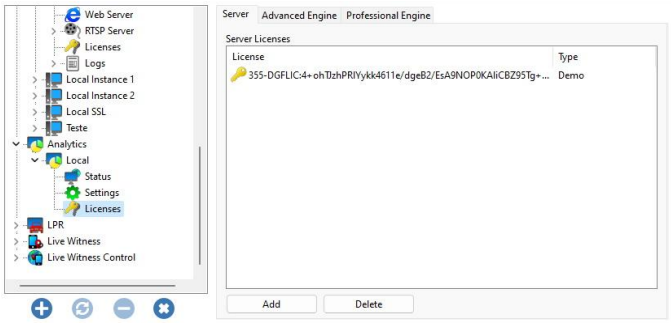
- **Analytics Server:** 1 analytics base license + 1 engine license for 2 cameras.
- **VMS Server:** 1 Base license (The base license of the Enterprise edition already have 8 licenses available for recording, if the number added exceeds the number of base licenses, "pack licenses") must be added.

© 2002 - 2024 by Digifort. All rights reserved.

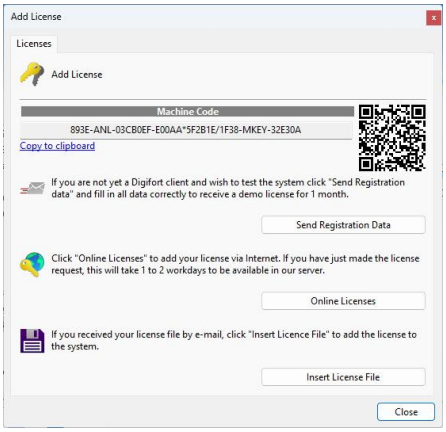
14.1.5.1 How To Configure Analytics Licenses

As previously mentioned, the Analytics will work with 2 types of license: the Base License (Basic) and the Pack License (Advanced or Professional).

The first step to license analytics is to add the base license (Basic). After connected, go to licenses as shown in the figure below:

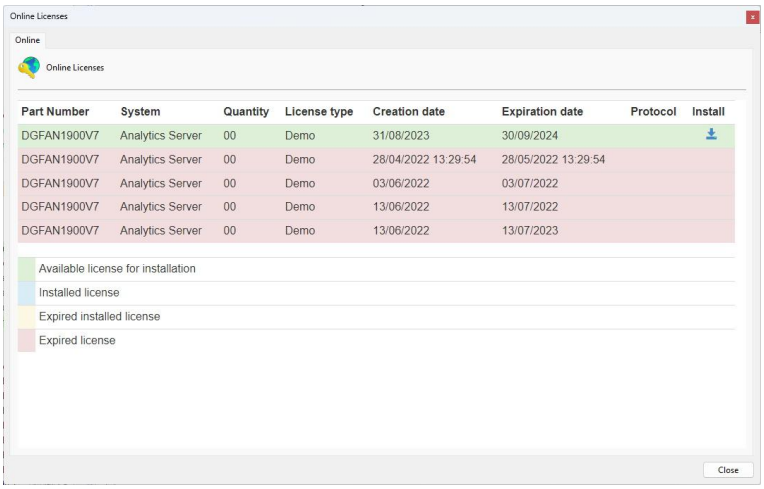


To add a license, click **Add**, and the following screen will be displayed:

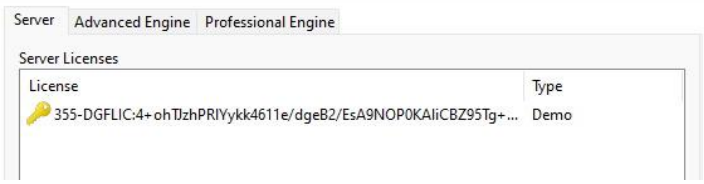


The process for adding licenses is the same as for VMS and is described in the chapter How to configure licenses .
On the online licenses screen, the license description should appear as **Analytics Server** as shown in the figure below:

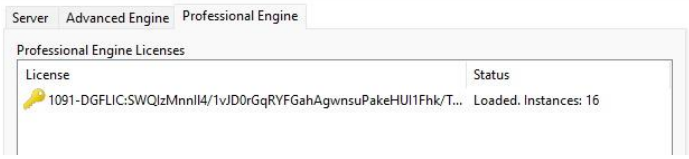
© 2002 - 2024 by Digifort. All rights reserved.



Click the button available in the install column of the corresponding license to install. After adding a license, it will be available as shown in the figure below:



The **Advanced Analytics and Professional Analytics** license works the same way and it is possible to view how many licenses are available in the status field, as shown in the figure below:



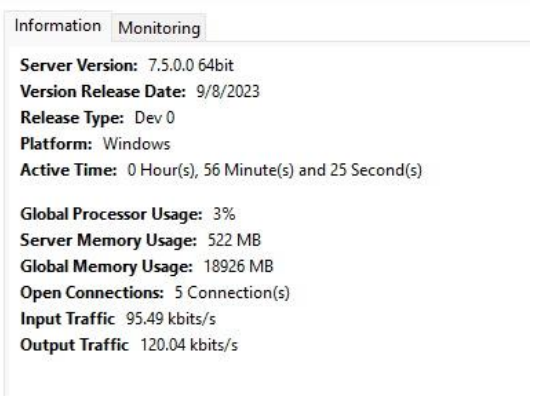
14.1.6 Analytics Server Status

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

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

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

© 2002 - 2024 by Digifort. All rights reserved.

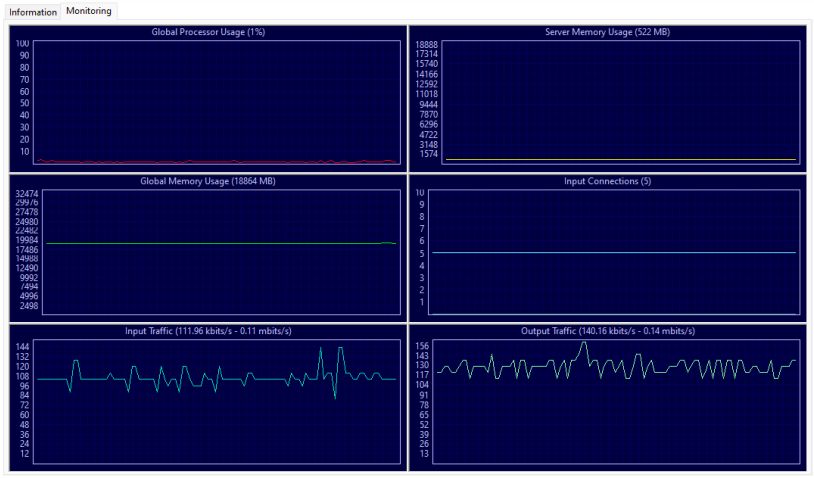


- **Server Version:** Displays the Analytics Server version.
- **Release Date:** Displays the release date of this server version.
- **Release Type:** Displays the release type of this server version.
- **Platform:** Displays the platform of this server version.

- **Global Processor Usage:** Displays the global CPU usage of the server where the analytics process is running. This value represents the total usage by all Operating System processes and not just the Analytics Server.
- **Server Memory Usage:** Displays the memory usage of the Analytics Server process only.
- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Open Connections:** Number of open connections with the Analytics Server.
- **Input Traffic:** Total data being sent to the Analytics Server by the VMS Servers for processing.
- **Output Traffic:** Total data being sent from the Analytics Server to the VMS Servers.

14.1.6.1 Monitoring

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



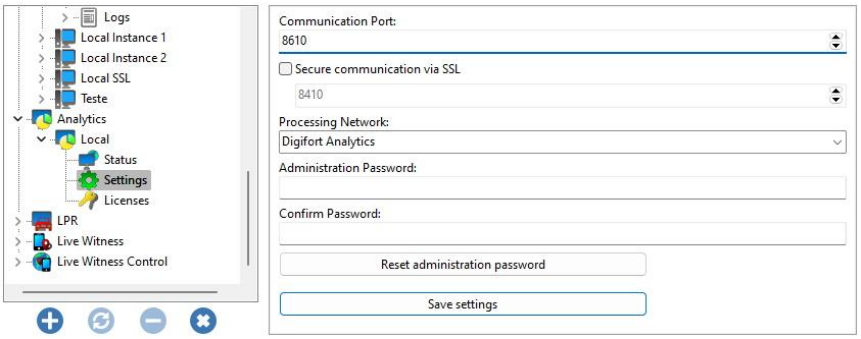
- **Global Processor Usage:** Displays the global CPU usage of the server where the analytics process is running. This value represents the total usage by all Operating System processes and not just the Analytics Server.
- **Server Memory Usage:** Displays the memory usage of the Analytics Server process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

© 2002 - 2024 by Digifort. All rights reserved.

- **Open Connections:** Number of open connections with the Analytics Server.
- **Input Traffic:** Total data being sent to the Analytics Server by the VMS Servers for processing.
- **Output Traffic:** Total data being sent from the Analytics Server to the VMS Servers.

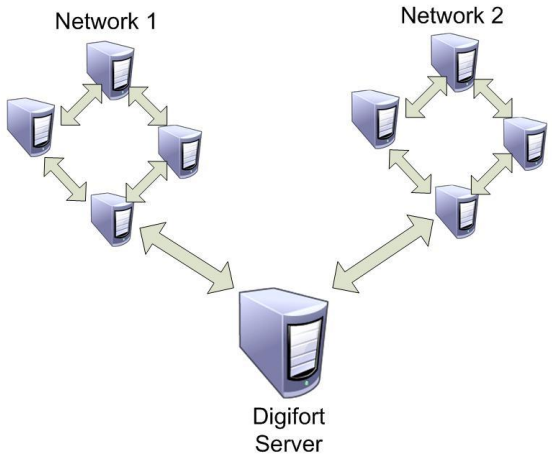
14.1.7 Analytics Server Settings

To access the analytics server settings, click on **Settings** as shown in the image below:



- **Communication Port:** Communication port with the analytics server. It is only recommended to change if this is already being used on the computer in question.
- **Secure Connection via SSL:** Enables secure connection to the server via SSL/TLS. To use SSL you must provide SSL certificates. See the SSL Certificates topic for more information.
  - **Port:** Specify the secure communication port

- **Processing Network:** Name of the distributed network in which this server will load balance. When more than one server has the same **"Processing Network"** name, processing will be balanced between them. To understand better, see the diagram below:



In the image above, the **VMS Server** sends images from the cameras to two different **Processing Networks**. This way, each group of computers balances the load only between the **Analytics Servers** that have the same network name.

- **Administration Password:** Password to access the analytics server. Fill in this field to change the current password.
- **Confirm Password:** Retype the password from the field above.

© 2002 - 2024 by Digifort. All rights reserved.

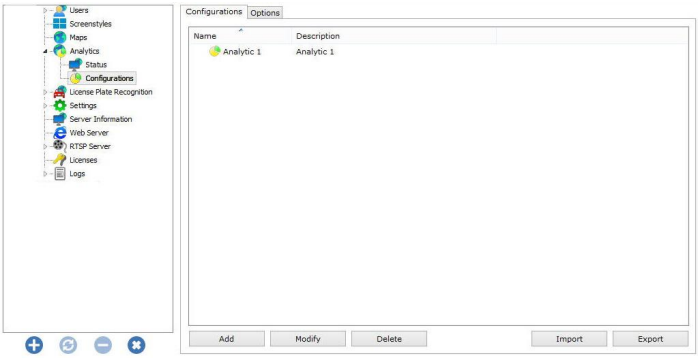
- **Reset Administration Password:** Returns the blank password.
- **Save Settings:** Saves the changes made on this screen.

14.1.8 Adding an Analytics Configuration

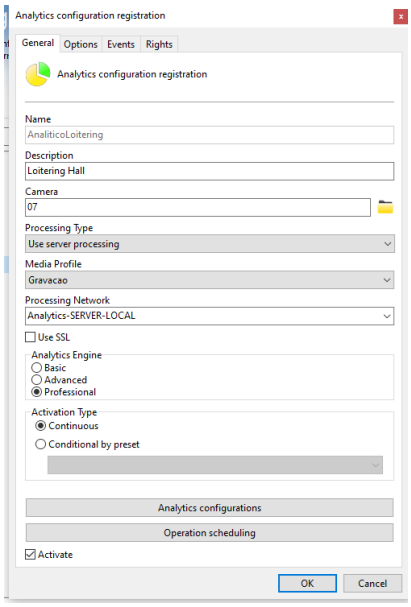
Analytics Configurations are objects created on the VMS server to perform image analysis. Each Analytics Configuration is associated with a camera and has options for processing images from this camera. You can create multiple Analytics Configurations for the same camera, each with its own independent options.

This topic will discuss how the configurations of system's **Basic, Advanced and Professional** analytics are made.

After correctly licensing the **Analytics Server**, you must add the **Analytics Configurations** to the **VMS Server**. To do this, connect to the VMS Server and open the **Configurations** item within **Analytics**.



The **Configurations** tab allows you to add a new **Analytics Configuration**. To do so, click on the **Add** button to start configuring the analytics. The following screen will be displayed:



To change an already registered configuration, select it and click **Modify**, and change the data as explained on the following pages.
To remove a configuration, select the desired configuration and click the **Remove** button.

© 2002 - 2024 by Digifort. All rights reserved.

- **Name**: Name of the desired analytics, for example: AnalyticsLoitering
- **Description:** Description of the analytics record, for example: Loitering Hall
- **Camera**: In this selecion box, all cameras registered on the VMS server will be available. The analytics rules defined will be valid for the camera that is configured in this selection box. To learn how to register cameras, see the chapter How to add a camera.
- **Processing Type**: Allows images to be processed in engines available locally at Analytics Server or on third-party servers. This option opens up the range of Analytic integrations and allows the future expansion of the Analytics base system for powerful integrations with third-party systems.
- **Media profile:** Select the media profile that is desired for analysis. It is recommended to use images with a size of 640x480. Video analytics does not interfere with the quality/performance of the video that is streamed and recorded.
- **Processing network:** In this field, all **"Processing networks"** (analytics servers) active on the network will be available. Choose a network on which this configuration will be processed. It is possible to specify the server for processing by its IP, use the following format **"IP:<server_ip>"** or **"IP:<server_ip>:<port>"** in the field. Example: **IP:192.168.0.10** or **IP:192.168.0.10:8610**.
- **Use SSL:** Select this option to securely connect to the Analytics Server for this configuration.
- **Analytics Engine:** Choose the engine that will analyze the images, already discussed in previous topics.
- **Activation type**
  - **Continuous**: Processes the image from a camera continuously.
  - **Conditional By Preset:** Activate the Analytics Configuration conditionally by preset, so you could define a preset so that this configuration is only active when the camera is positioned in the specified preset.
- **Analytics Configurations:** Opens the chosen engine configuration screen.
- **Operation Scheduling:** Allows you to schedule the operating hours of this Analytics Configuration.
- **Activate:** Activates or deactivates the analytics configuration.

14.1.8.1 Options

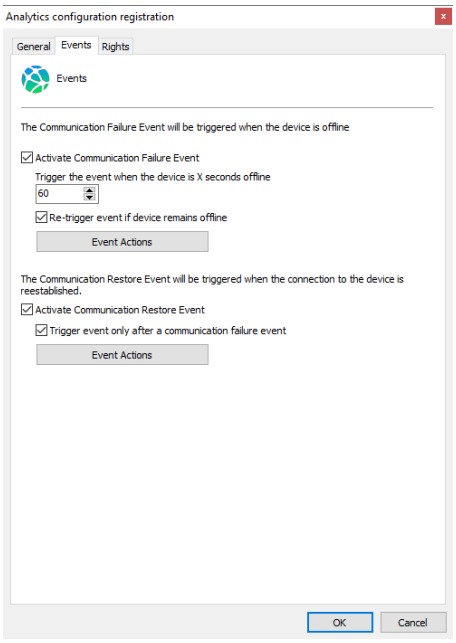
In the options tab, we can configure a delay for drawing the analytics metadata in the monitoring client. When using third party analytics it is possible that there is a delay between the image and the metadata which can be corrected with this feature.

- **Metadata Offset:** Defines the image delay time for metadata rendering in the Surveillance Client (In Milliseconds). Use this option if metadata is being displayed late.

14.1.8.2 Events

In the events tab, it is possible to configure the Communication Failure or Communication Restore events for the Analytics Configuration, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



14.1.8.2.1 Communication Failure

The **Communication Failure** event consists of checking how long the configuration has been out of operation, therefore the system will only generate the communication failure event if the configuration remains out of operation for more than X seconds.

The system still allows the event to continue firing every X seconds while the configuration is not working, if the option is disabled the system will generate the event only once.

To learn how to configure event actions see How To Configure Event Actions.

14.1.8.2.2 Communication Restore

The **Communication Restore** event consists of generating an event when the configuration returns to work in the system.

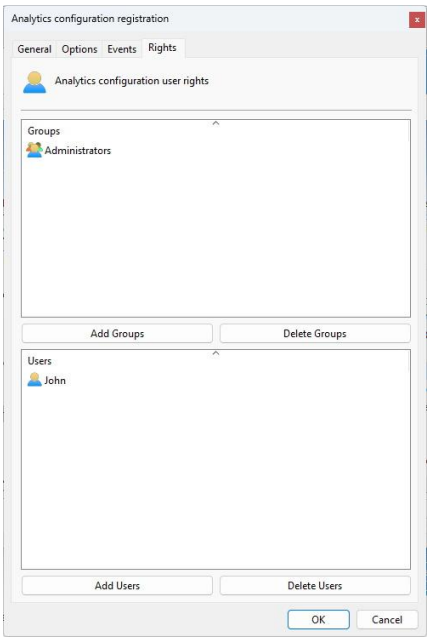
The system also allows events to only be triggered if a **Communication Failure** event for the same object has been triggered previously.

To learn how to configure event actions see How To Configure Event Actions.

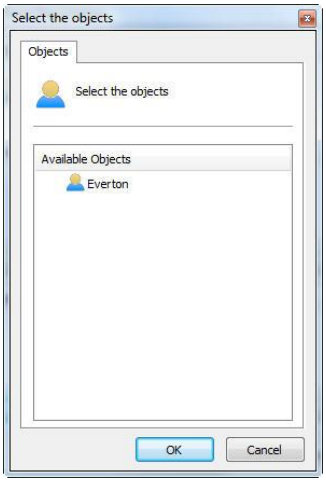
14.1.8.3 Rights

On the **Rights** tab you can define the list of users and user groups that will have the right to view this configuration in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

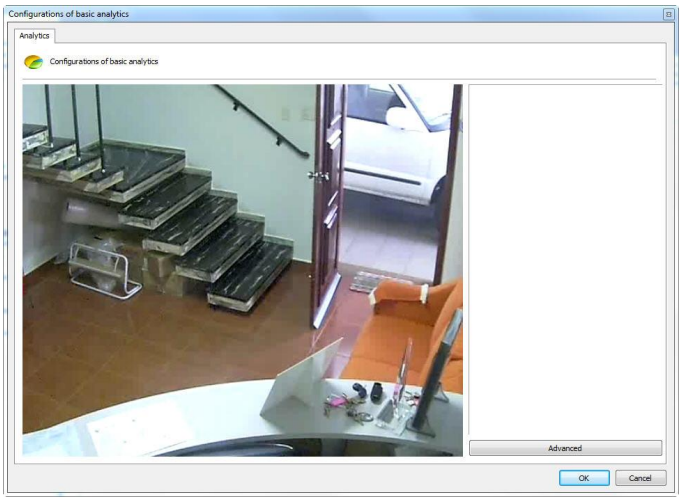


Select the available User and click **OK**. The same rule applies to the group list.

14.1.8.4 How To Configure Basic Analytics

If the Basic engine is chosen on the analytics registration screen, the following screen will appear:

© 2002 - 2024 by Digifort. All rights reserved.

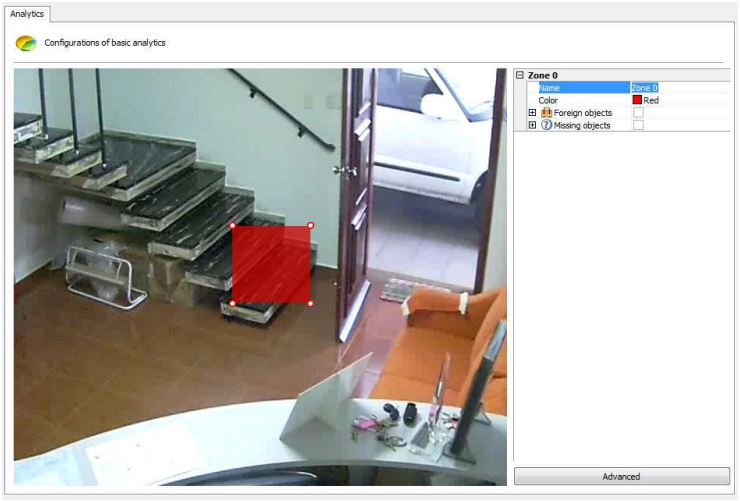


The image that will appear will be related to the camera and the media profile selected on the analytics registration screen.

This screen has the following functionalities when the right button is activated:

- **Create zone:** Creates a zone where the analysis module will be defined.
- **Delete:** Deletes a selected zone.

Create a zone and click on it as shown in the figure below:

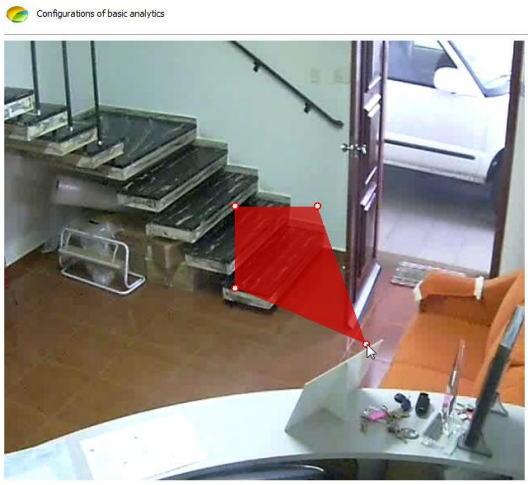


You will notice that a zone options menu will open in the right column of the screen. The following options will be available:

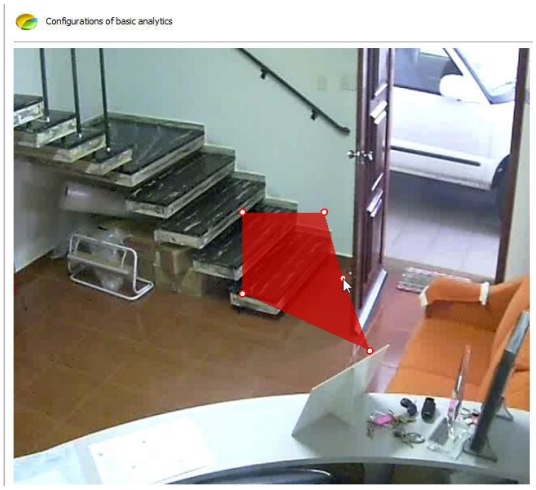
© 2002 - 2024 by Digifort. All rights reserved.

- **Name:** Name for the created zone. It is important that this name is well thought out as it will be possible to generate reports from this name.
- **Color:** Changes the color of the selected zone.
- **Foreign Objects**: Foreign objects analysis module. This module will be discussed in the chapter How to configure the Foreign Objects module
- **Missing Objects:** Missing objects analysis module. This module will be discussed in the chapter How to configure the Removed Objects module

It is possible to move the zone points by clicking on the circles as in the figure below:



And add points by double clicking near the edge of the zone as below:



The maximum possible points per zone is 20.

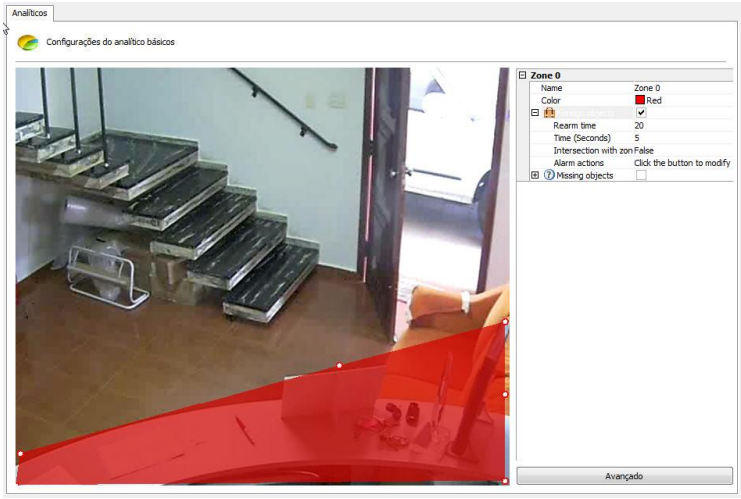
14.1.8.4.1 Foreign Objects

The Left Objects module can generate alerts when an object is left in a specific area of the image or when something in the scene is changed. Example: A suitcase left on the floor, a key that appears on top of a table. From these events it is possible to recover the video, generate alarms and reports.

© 2002 - 2024 by Digifort. All rights reserved.

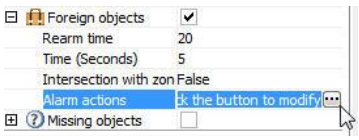
The analytical modules were made to help with monitoring and are not completely accurate, for example: the left objects module can trigger alarms with changes in lighting, projected shadows, etc., generating what is called a false alarm.

In our example, a detection zone was created for the table as shown in the figure below:



Opening the left side options of **Foreign Objects** we have the following functionalities:

- **Foreign Objects**: Check this option to activate Foreign Objects in this zone.
- **Rearm time:** Rearm time for the alarm to be activated again in the Surveillance Client (if configured).
- **Intersection with the zone:** If **false**, only objects that have their center inside the zone will be fired. If **true**, any object intersecting the zone can trigger the alarm.
- **Time:** Time in seconds that the object must remain stationary in the zone for the alarm to be triggered. Long times are not recommended in places with a lot of movement.
- **Alarm Actions**: Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure event actions .

Here is an example where the alarm was triggered in the previously configured situation:

© 2002 - 2024 by Digifort. All rights reserved.

Every time an alarm is triggered the scenario is automatically relearned.

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

Note

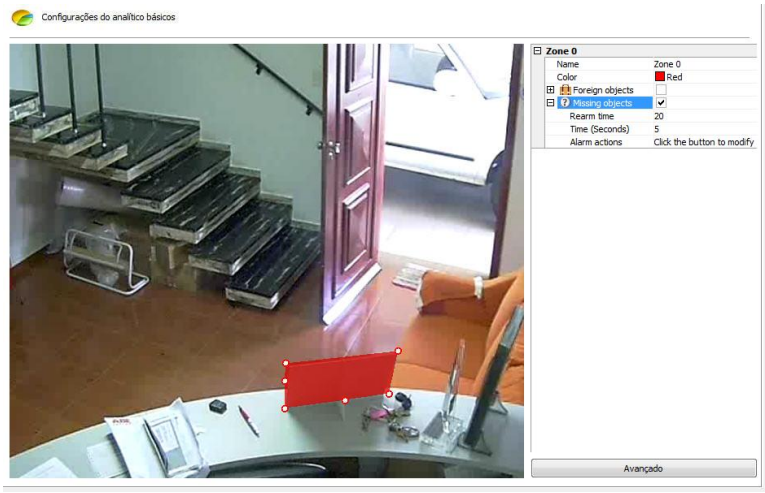
The left objects module will trigger alarms on any change of scenery, that is, both when objects are removed or when they are left. The difference between this module and the removed objects module is that this module looks for objects within a zone, while the removed objects demarcate the zone exactly around the object in question.

14.1.8.4.2 Removed Objects

The **Removed Objects** module can generate alerts when a demarcated object is removed from the scene. Example: A painting, valuables, etc. From these events it is possible to recover the video, generate alarms and reports.

The analytical modules were made with the intention of helping the monitoring and are not totally accurate, for example: the removed objects module can trigger alarms with changes in lighting, projected shadows, etc., generating what is called a false alarm.

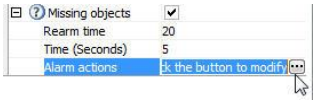
In our example, a detection zone was created on an object on the table as shown in the figure below:



As can be seen in the Removed Objects the zone must be made around a specific object as opposed to the objects left.

Opening the side options of **Missing Objects**, we have the following features:

- **Missing Objects**: Check this option to activate Missing Objects in this zone.
- **Rearm time:** Rearm time for the alarm to be activated again in the monitoring client (if configured).
- **Time:** Time in seconds that the object must remain stationary in the zone for the alarm to be triggered. Long times are not recommended in places with a lot of movement.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



© 2002 - 2024 by Digifort. All rights reserved.

On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions .

Here is an example where the alarm was triggered in the previously configured situation:

Every time an alarm is triggered the scenario is automatically relearned.

To learn how to generate reports, consult the Surveillance client manual.

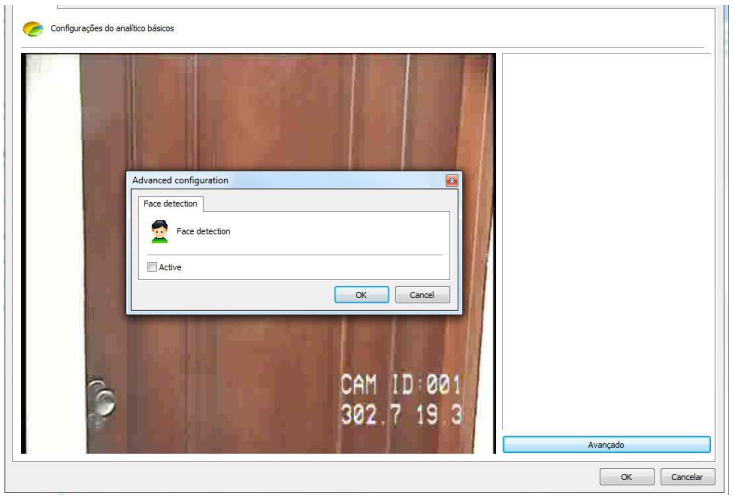
14.1.8.4.3 Face Detection

The Face Detection module aims to capture the faces that pass through a certain camera and file them in a database.

For best use, this module needs the camera to focus on a certain area in which a person's face has around 20% to 70% of the image area. Here's an example below:

On the analytics configuration screen, click the Advanced button and Activate on face detection.

© 2002 - 2024 by Digifort. All rights reserved.

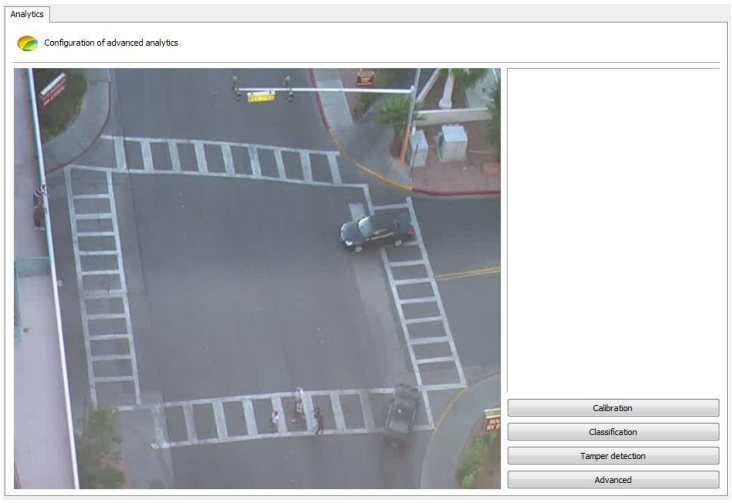


Here is an example where the faces were captured in the previously configured situation:

To learn how to generate reports and consult the captured faces, see the surveillance client manual.

14.1.8.5 How To Configure Advanced Analytics

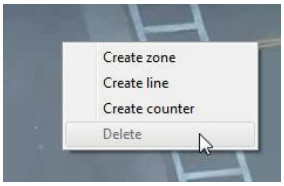
If the Advanced engine is chosen on the analytics registration screen, the following screen will appear:



© 2002 - 2024 by Digifort. All rights reserved.

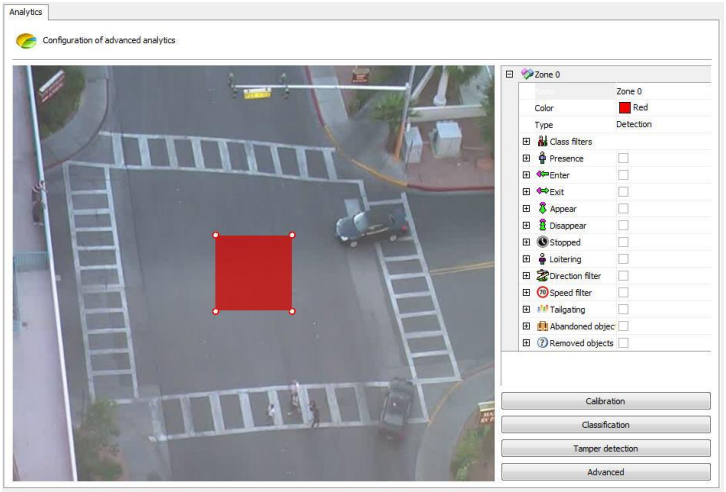
The image that will appear will be related to the camera and the media profile selected on the analytics registration screen. The camera must be registered and activated on the server for the image to appear.

This screen has the following functionalities when the direct button is activated:



- **Create Zone:** Creates a zone where the analysis module (Rule) will be defined.
- **Create Line:** Creates a line where the analysis module (Rule) will be defined.
- **Create Counter:** Creates a counter that will be associated with an analysis module (rule).
- **Delete:** Deletes a selected zone/line/counter.

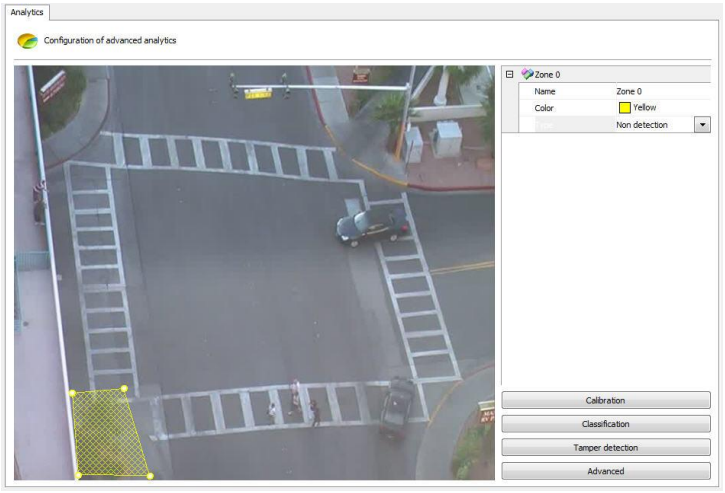
Create a zone/line and click on it as shown in the figure below:



You will notice that a zone options menu will open in the right column of the screen. The following options will be available:

- **Name:** Name for the created zone. It is important that this name is well thought out as it will be possible to generate reports from this name.
- **Color:** Changes the color of the selected zone/line.
- **Type:** There are two zone types: Detection and Non-detection.
  - The **detection zone** is the standard zone where analytical modules are applied.
  - The **non-detection zone** is used to remove unwanted image areas such as trees, rivers, etc. The figure below illustrates a **non-detection** area:

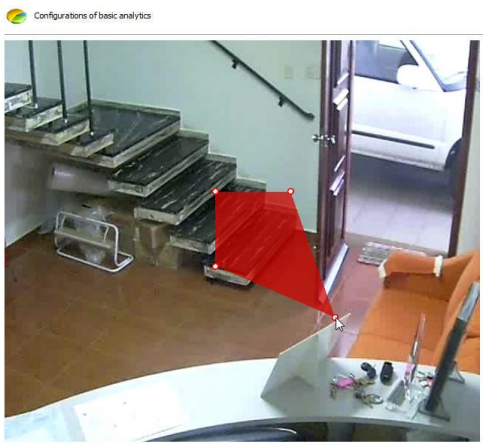
© 2002 - 2024 by Digifort. All rights reserved.



- **Class filters:** Determines which object should be included/excluded from detection in the selected area. Learn more about this feature in the chapter How to sort objects

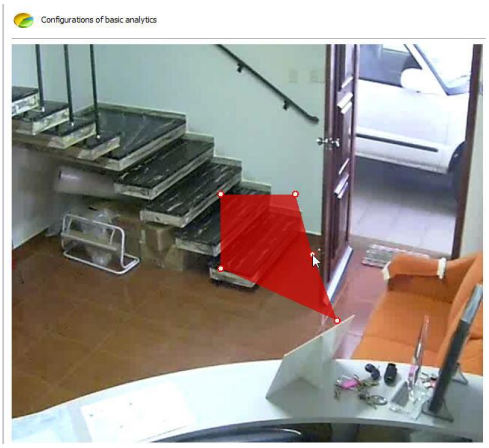
The list will contain a series of analysis filters that can be activated for the selected zone. To learn about filters, see the topic on How to Configure Analytics Rules.

It is possible to move the zone points by clicking on the circles as in the figure below:



And add points by double clicking near the edge of the zone as below:

© 2002 - 2024 by Digifort. All rights reserved.



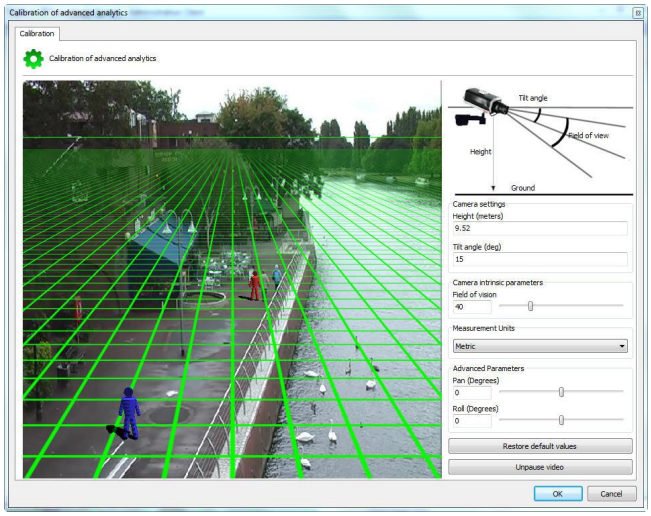
The maximum possible points per zone is 20.
These same rules apply to lines.

14.1.8.5.1 Scene Calibration

Advanced analytics requires some calibration settings for it to work properly.

The first configuration is the calibration of distances, it is necessary to get alarms like speed and to classify objects like cars, people, groups of people and so on.

To start, on the analytics configuration screen, click on **Calibration**. The following screen will be displayed:



On this screen, the configured camera image will appear along with a 3D Grid.

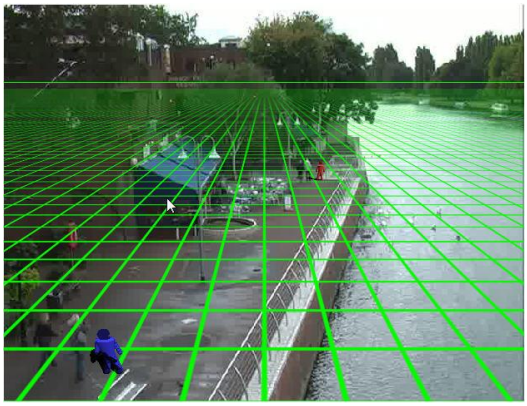
If no command is activated, some messages will appear on the screen with information on how to operate the grid:

- Measure or estimate the height of the camera above the ground.
- Use the middle mouse button to adjust the camera height
- Click and drag the grid to change the vertical angle of the camera
- Click and drag the 3D people to compare the size with the people in the image.

© 2002 - 2024 by Digifort. All rights reserved.

- Each grid square equals 2 square meters.

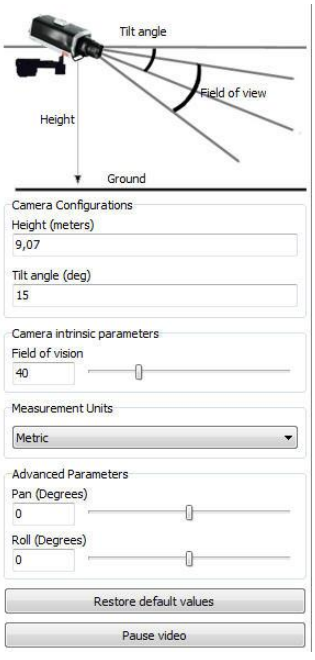
To facilitate configuration, first move the grid trying to position the Horizon line compatible with the image as shown in the figure below:



In the configuration above you can see the horizon line, the grid compatible with the image and the 3D puppets with the approximate size of the people in the image.

Ready! The grid is already configured.

In case you have precise values of the positioning of the camera in the place, the menu on the right side also helps in configuring the grid:



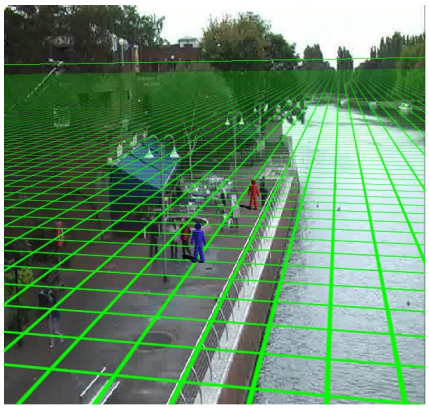
The menu has the following features:

- **Height:** Height in meters that the camera is in relation to the ground.
- **Tilt Anle:** Vertical angle of the camera.
- **Field of view:** Camera's field of view.

© 2002 - 2024 by Digifort. All rights reserved.

These values, when changed, automatically adjust the positioning of the Grid.

- **Units of Measure**: You can change the measurement type from **Metric** to **Imperial** in the **Unit of Measure** field.
- **Advanced Parameters**: Use the parameters below for a finer adjustment of the grid as in the figure below.



  - **Pan (Degrees):** Rotates the grid on the Y axis of the Cartesian plane.
  - **Roll (Degrees):** Rotates the grid on the Z axis of the Cartesian plane.

- **Restore Default Values:** Restores the initial grid positioning values.
- **Pause video:** Allows you to pause the camera video for grid adjustment

With the grid configured correctly, we will be able to classify the objects being detected. See the next chapter to learn how to classify objects.

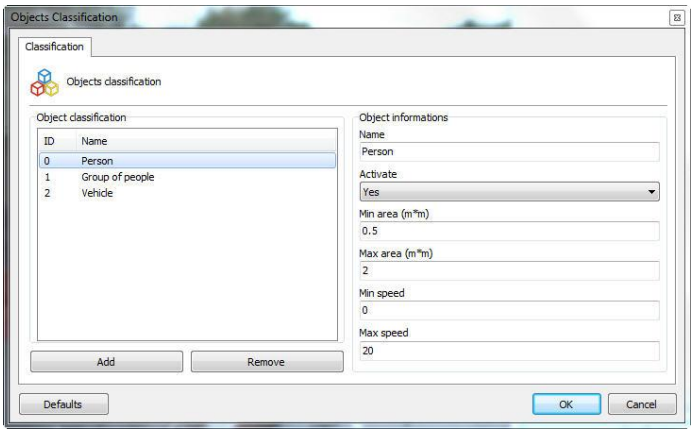
14.1.8.5.2 Object Classification

The analytics uses the object classification table to determine the type of object recognized by the object tracker, based on its size and speed and with this, the object class can be used to filter detections for objects such as cars, people, groups of people, animals, etc. Example: An area can trigger alarms only when people move around or only when cars are stopped.

After **Calibration** has been done correctly it is possible to create object classifications.

To start, on the analytics configuration screen, click on **Classification**. The following screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



Initially the system will have the standard objects registered, namely: **People, Group of People and Vehicles**. To register a new object, click **Add** and fill in the fields. The image above shows what a **Person** classification would look like when registering.

The fields that must be filled in are described below:

- **Name:** Name of the classification to be added.
- **Active:** Sorting can be turned off at any time by changing the checkbox to **no**.
- **Minimum Area:** The minimum area that the object must have to be recognized within this classification.
- **Maximum Area:** The maximum area that the object must have to be recognized within this classification.
- **Minimum Speed:** The minimum speed that the object must be at to be recognized within this classification.
- **Maximum speed:** The maximum speed that the object must be at to be recognized within this classification.

To remove a classification, just select it from the list and click **Remove**.

Here is the result of this classification in the monitoring:

To learn how to view the live analytics functionalities, consult the Surveillance Client manual.

© 2002 - 2024 by Digifort. All rights reserved.

14.1.8.5.3 How To Configure Analytics Rules

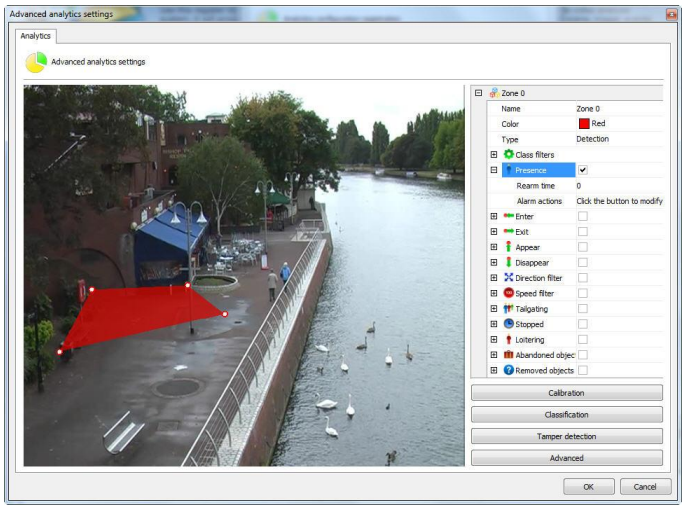
Each analytics analysis module (Enter, Stopped, Presence, etc...) is considered a rule, which in turn is applied to a zone.

Next, we will see how to configure all the analytical rules and their alarms in zones for different situations.

14.1.8.5.3.1 Presence

The **Presence** rule can trigger alarms if it detects any objects within a certain area.

Let's configure a presence alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



With the zone selected, select the **Presence** rule. The options for this rule are as follows:

- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions**: Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

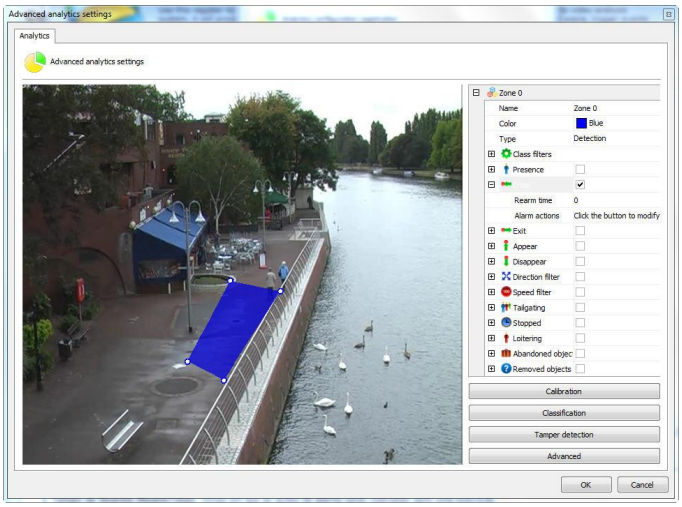
On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.2 Enter

The **Enter** rule can trigger alarms if it detects an object entering a certain area.

Let's set up an **Enter** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:

© 2002 - 2024 by Digifort. All rights reserved.



With the zone selected, select the **Enter** rule. The options for this rule are as follows:

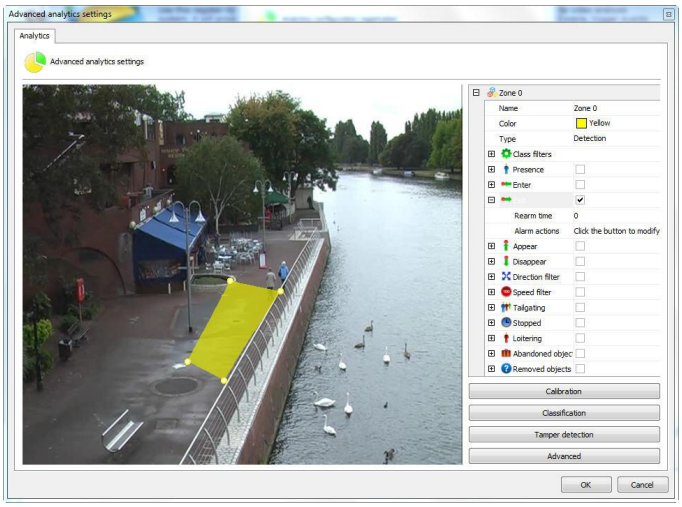
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.3 Exit

The **Exit** rule can trigger alarms if it detects any objects exiting a certain area.

Let's configure an **Exit** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



© 2002 - 2024 by Digifort. All rights reserved.

With the zone selected select the **Exit** rule. The options for this rule are as follows:

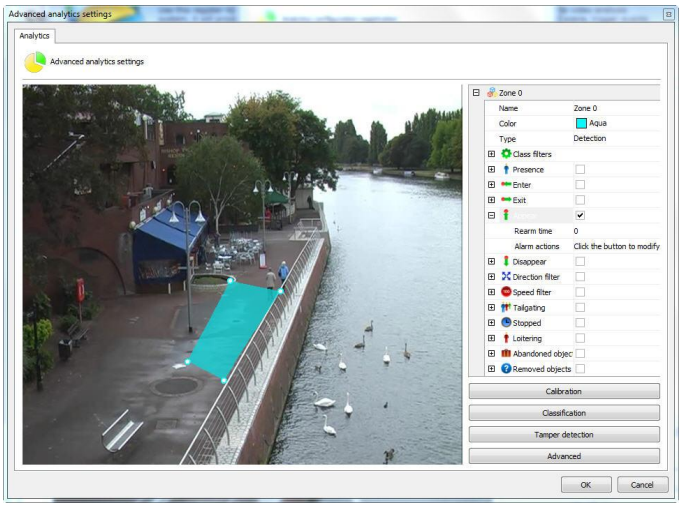
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions**: Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.4 Appear

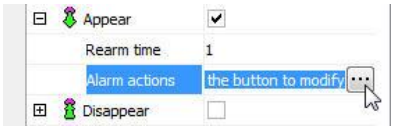
The **Appear** rule can trigger alarms if it detects any objects appear in a certain area.

Let's set up an **Appear** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



With the zone selected select the **Appear** rule. The options for this rule are as follows:

- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



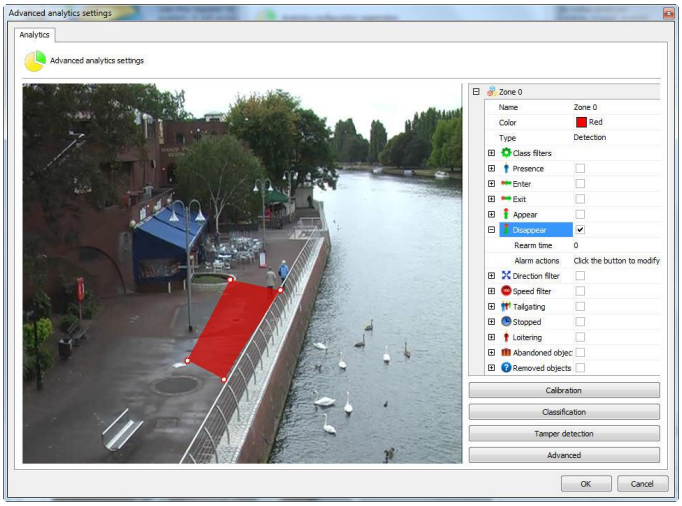
On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

© 2002 - 2024 by Digifort. All rights reserved.

14.1.8.5.3.5 Disappear

The **Disappear** rule can trigger alarms if any object disappears in a certain area.

Let's set up a **Disappear** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



With the zone selected select the **Disappear** rule. The options for this rule are as follows:

- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

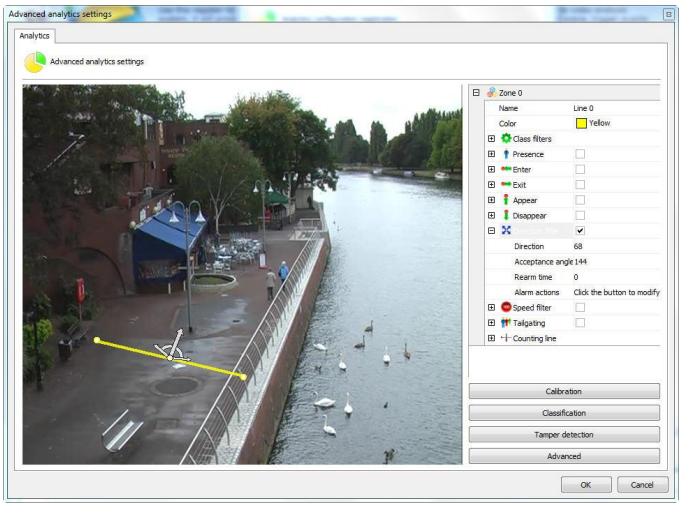
On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.6 Direction Filter

The **Direction Filter** rule can trigger alarms if it detects objects in configured directions.

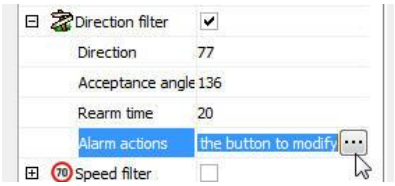
Let's configure a **Direction Filter** alarm from a line. In the figure below, a line was created in the previously calibrated image:

© 2002 - 2024 by Digifort. All rights reserved.



With the line selected select the **Direction Filter** rule. The options for this rule are as follows:

- **Direction:** Direction in angle that the object must travel for the alarm to be activated. You can configure the direction by clicking and moving the large (direction) arrow.
- **Acceptable angle:** The acceptance angle is a "slack" from the main angle, that is, an object will not pass at exactly 90 degrees (it will pass at 100, 80, 70), so the greater the acceptance angle the easier it will be to trigger the alarm. You can configure the acceptance angle by clicking and moving one of the smaller arrows.
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



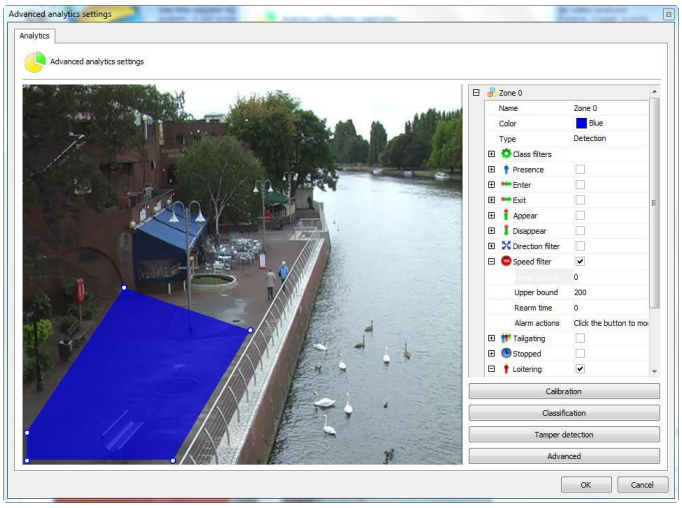
On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.7 Speed Filter

The **Speed Filter** rule can trigger alarms if it detects objects at configured speeds.

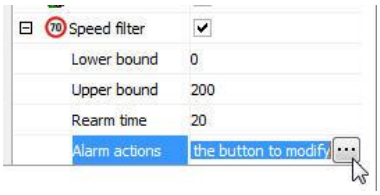
Let's configure a **Speed Filter** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:

© 2002 - 2024 by Digifort. All rights reserved.



With the zone selected select the **Speed Ffilter** rule. The options for this rule are as follows:

- **Minimum and Maximum Speed:** Set the minimum and maximum speed values. The event will be triggered if the object's speed is between the minimum and maximum values.
- **RearmTime:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

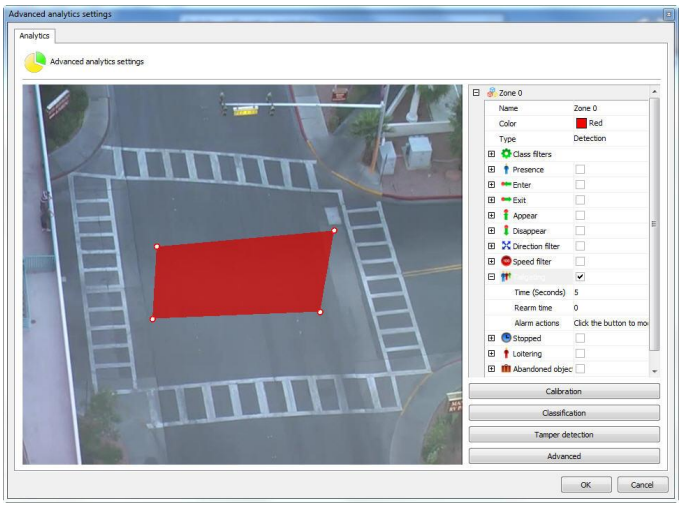


On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

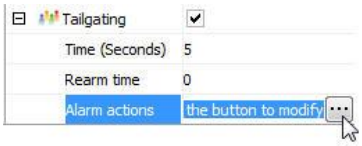
14.1.8.5.3.8 Tailgating

The **Tailgating** rule can trigger an alarm when a second object passes a certain area after the first object, within a configurable period of time. We can exemplify an alarm when a car that passes along with another when a toll gate is lifted.

© 2002 - 2024 by Digifort. All rights reserved.



- **Time:** Time in seconds between objects entering an area. If after an object enters the area, a second object enters with a time shorter than the configured one, an alarm will be triggered.
- **RearmTime:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

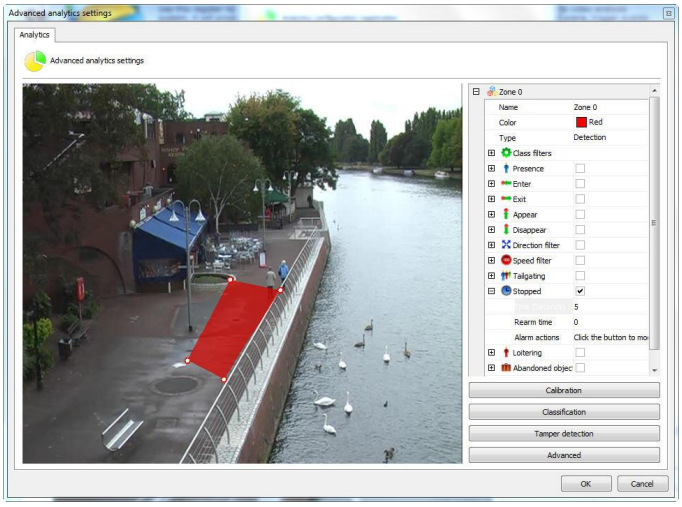


On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.9 Stopped

The **Stopped** rule can trigger alarms if it detects a stationary object in a certain area.

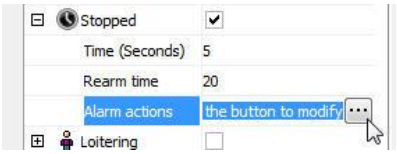
Let's configure a **Stopped** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



© 2002 - 2024 by Digifort. All rights reserved.

With the zone selected select the **Stopped** rule. The options for this rule are as follows:

- **Time:** Time the object has to stay still to trigger the alarm.
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:

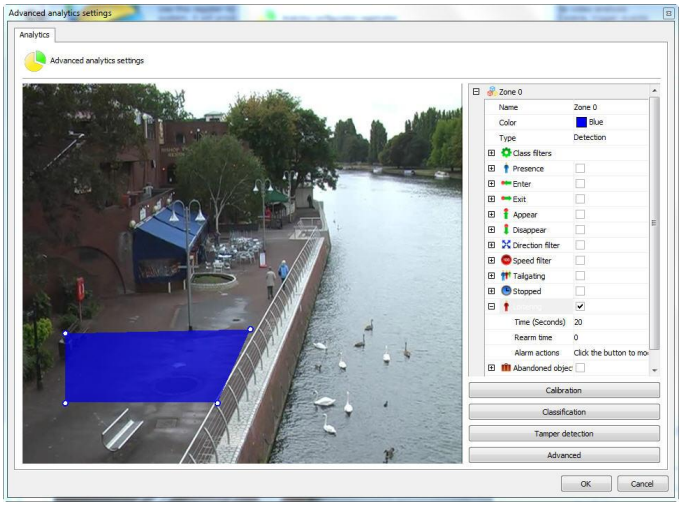


On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.10 Loitering

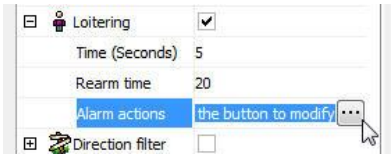
The **Loitering** rule can trigger alarms if it detects an object transiting in a certain area for a certain time.

Let's configure a **Loitering** alarm from a zone. In the figure below, a zone was created in the previously calibrated image:



With the zone selected select the **Loitering** rule. The options for this rule are as follows:

- **Time:** Time the object has to stay still to trigger the alarm.
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



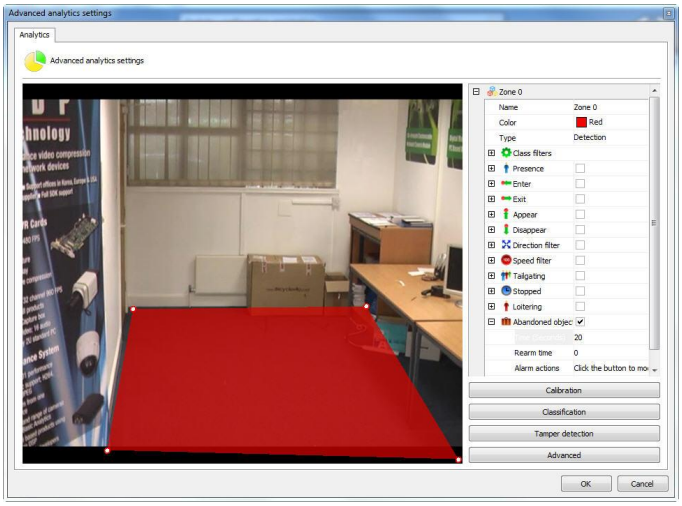
© 2002 - 2024 by Digifort. All rights reserved.

On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.3.11 Abandoned and Removed Objects

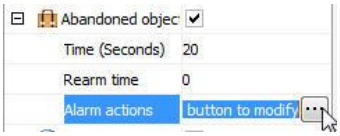
The **Abandoned or Removed Objects** rules can generate alerts when an object is left in a specific area of the image or when something in the scene is changed. Example: A suitcase left on the floor, a key that appears on top of a table, a box removed from a shelf. From these events it is possible to recover the video, generate alarms and reports.

In our example, a detection zone was created in the figure below:



Opening the left side options **Abandoned or Removed Objects** the options for this rule are as follows:

- **Time:** Time in seconds that the object must remain stationary in the zone for the alarm to be triggered. Long times are not recommended in places with a lot of movement.
- **Rearm Time:** Time in which the alarm actions will be reactivated after an execution.
- **Alarm Actions:** Click on the alarm actions line and then on the button with 3 dots as shown in the figure below:



On the alarms screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions .

Here is an example where the alarm was triggered in the previously configured situation:

© 2002 - 2024 by Digifort. All rights reserved.

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

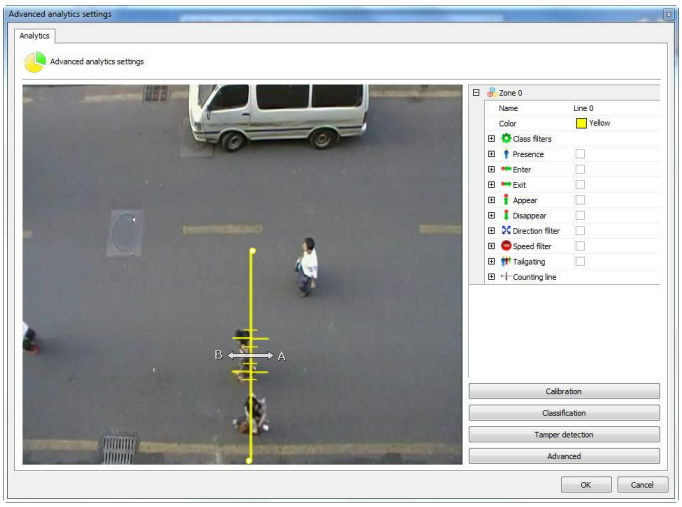
Note

The abandoned or removed objects module will trigger alarms on any change of scenery, that is, both when objects are removed or when they are abandoned.

14.1.8.5.3.12 How to configure the Count line rule

The **Counting Line** has the purpose of counting the objects that pass in the image, more specifically people or vehicles. The **Counting Line** rule can only be applied to lines and not zones.

Let's configure the count line from an ordinary line. In the figure below, a line was created in the previously calibrated image:



The count line offers the following configuration options:

- **Direction A:** Specifies that there will be counting for the A side of the line
- **Direction B:** Specifies that there will be counting for the B side of the line
- **Calibration:** Calibration of the size of the object to be counted. This calibration can be done directly through the line. In the case of the figure above, crossing the counting line there are 6 more lines, where the largest refer to the size of the object to be contacted, that is, the gap between these two largest straight lines would be the size of a person's shoulders, and the smaller lines would be an acceptance limit. Note that for this count to work well, the camera must be well above the objects, in the case of people, the head and shoulders must be more visible in the image. Below is an example of proper camera and counting line positioning:

© 2002 - 2024 by Digifort. All rights reserved.

The red arrow in the image demonstrates where the count line is located.

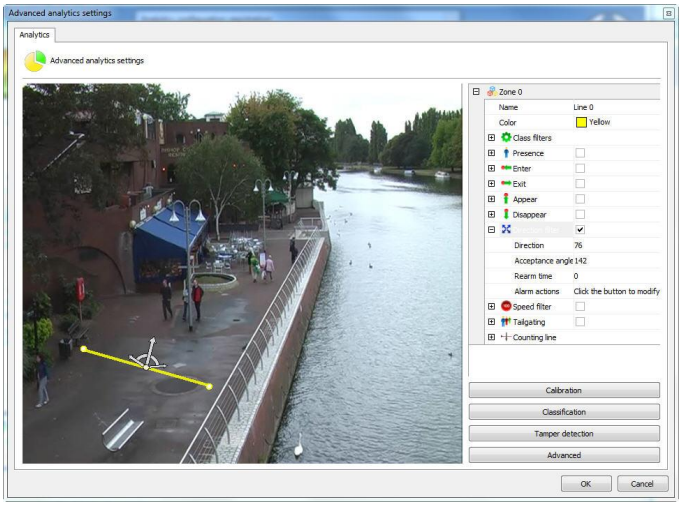
- **Shadow filter:** If there is shadow interference in the place, this filter can help to minimize the effect.

14.1.8.5.4 Counters

Counters are visual objects that allow, in real time, when monitoring images, to know the count of events that are happening.

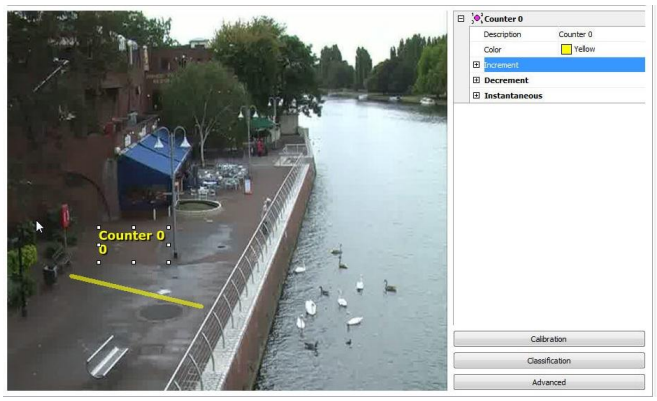
Counters are Incremented or Decremented by configured events. Let's see some examples.

In the image below a Direction Filter rule has been configured.



What we are going to do is configure a counter so that for each object that activates this event automatically, the counter will increment. To do this, right-click on the screen and create a counter as in the image below:

© 2002 - 2024 by Digifort. All rights reserved.

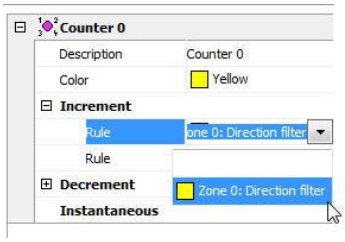


In the menu on the right some options are available:

- **Increment:** Increments the counter according to available rules.
- **Decrement:** Decrements the counter according to available rules.
- **Instantaneous:** Returns the momentary value of the rules that are triggered.

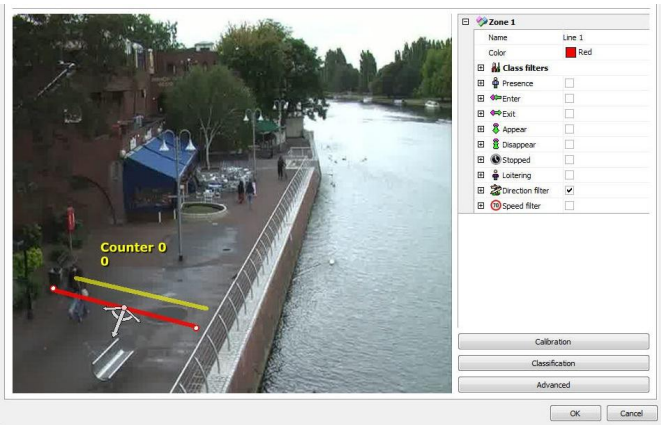
For better learning we will illustrate how to use the resources above.

Initially we will just increment the counter with the direction rule we created. To do so, open the **Increment** option and in **Rule** select which type of rule you want to increment (In this case we only configured the **Direction Filter**, so it is the only one available).



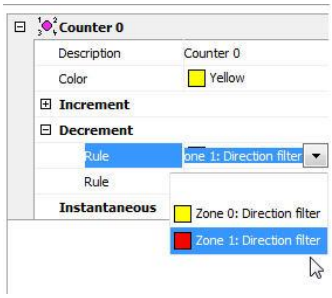
After selecting the rule you will notice that another **Rule** field will appear, with it another rule could be applied to also increment the counter. You can select multiple rules to increment or decrement the counter.

Now we will create another rule of **Direction Filter** as shown in the figure below:



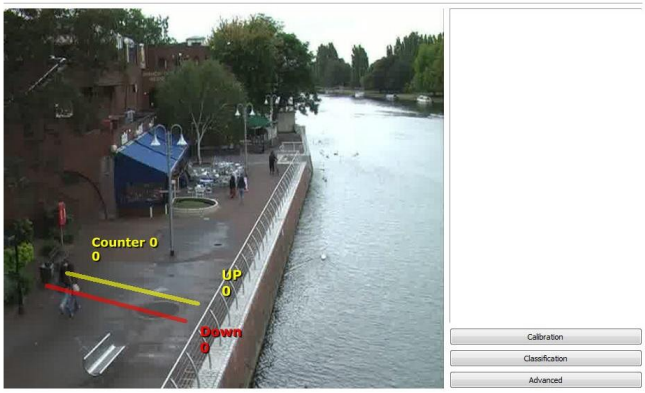
© 2002 - 2024 by Digifort. All rights reserved.

With this Rule we will decrement the counter already created.
Select it and in Decrease choose the rule of the second Zone as shown in the figure below:

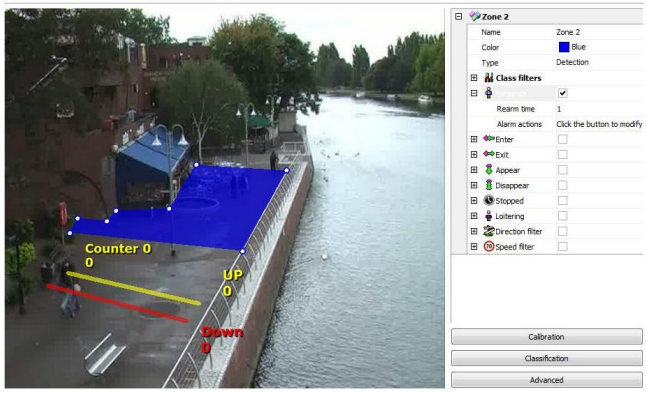


With this configuration the Counter will **increment** when people walk up and **decrement** when people walk down.

There could still be a counter for each line as shown in the figure below:

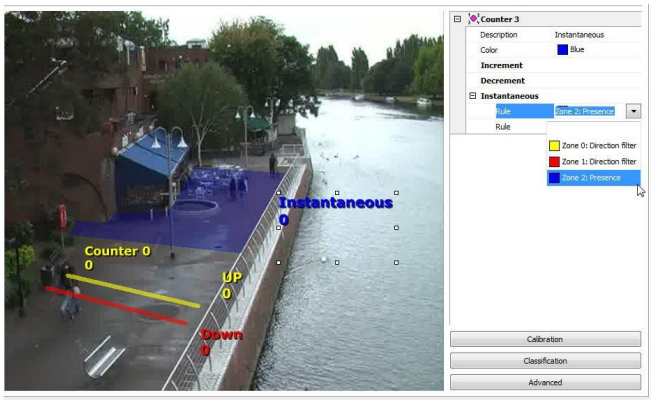


To test the instantaneous counter, we will create a presence detection area as shown in the image below:



Now a counter will be created that will show the value of how many presence rules are activated within that area, in other words, return how many objects are present at the exact moment within the area. The image below shows this configuration:

© 2002 - 2024 by Digifort. All rights reserved.

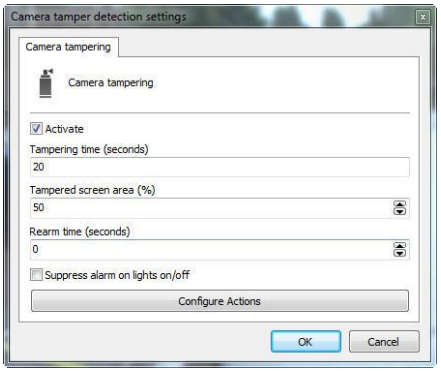


You can configure up to 40 counters per analytics configuration.
The size of the counters can be adjusted by selecting and dragging the squares around them.

14.1.8.5.5 Camera Tampering

The **Camera Tampering** module may trigger alarms if something obstructs the camera's image, for example: changing the camera's position, blocking the lens, placing an object to block the view of an area.

To configure the camera obstruction module, click the **Advanced** button on the Analytics Configuration screen as shown in the image below:



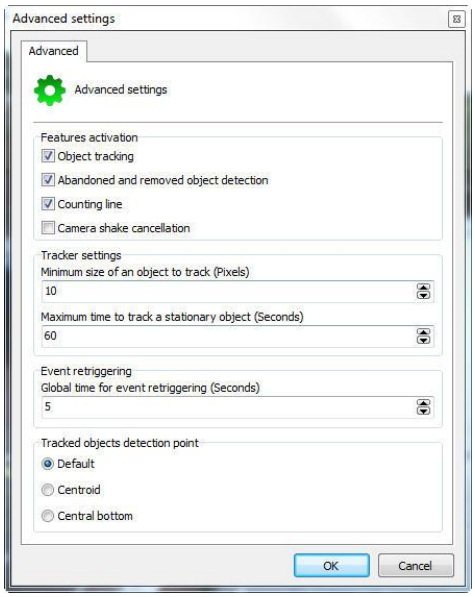
This screen has the following features:

- **Activate:** Enables or disables the operation of the camera tampering module.
- **Tampering Time:** Time in seconds that the camera must be obstructed for the alarm to be triggered.
- **Tampered Screen Area:** Percentage of the image that must be obstructed for the alarm to be triggered.
- **Rearm Time:** Waiting time for another alarm to be triggered.
- **Suppress alarm on lights on/off**: Does not trigger the alarm when turning on and off the ambient light.
- **Configure alarm actions:** On the alarm screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

14.1.8.5.6 Advanced Options

The advanced options contain some general functionality which will be covered below.

© 2002 - 2024 by Digifort. All rights reserved.



This screen has the following features:

- **Object tracking:** Activates the object tracking module. Deactivate this option in case of using only the count line modules or abandoned/withdrawn objects.
- **Abandoned and removed object detection:** Activates the abandoned and removed object module. Disable this option if you are not going to use it.
- **Counting line:** Activates the counting line module. Disable this option if you are not going to use it.
- **Canceling camera shake (Camera shake cancellation):** This module aims to assist in image analysis in cameras that may shake for various reasons where they are fixed. With the module enabled, image analysis will run much better and the chances of errors will decrease. This option will not generate a shake-cancelled camera image, this is just an internal option.

- **Tracker Settings**
  - **Minimum size of object to track (Pixels):** Set the minimum size of pixel to be considered a trackable object by video analytics.
  - **Maximum time to track a stationary object (Seconds):** Maximum time in which a stationary object will be tracked, after which the object will be incorporated into the learned scenario.

- **Event Re-Triggerring**: Configures a global time for the re-trigger of analytics events in the current configuration.
- **Tracked Objects Detection Point:** The rules are activated from this point, which must have its position configured according to the scene.
  - **Default:** The default point will be centered below the object
  - **Centroid:** The point will be the center of the object
  - **Central Bottom:** The point will be centered below the object

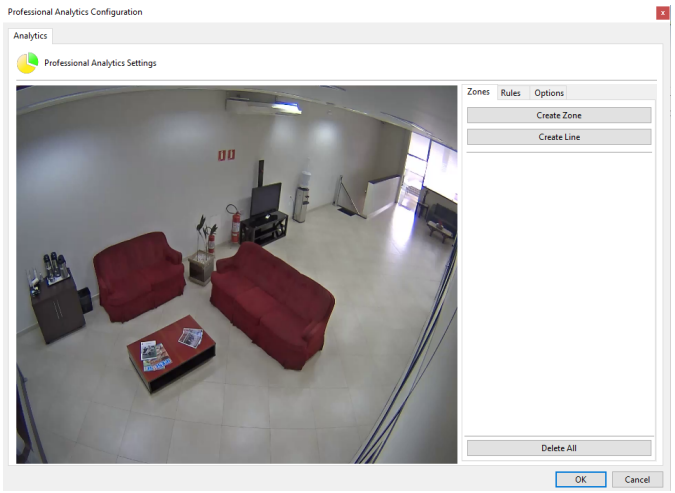
© 2002 - 2024 by Digifort. All rights reserved.

Centroid

Central Bottom

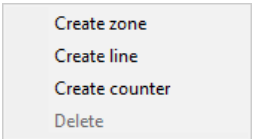
14.1.8.6 How To Configure Professional Analytics

If the **Professional** engine is selected, the following screen will appear:



The image that will appear will be related to the camera and the media profile selected on the analytics registration screen. The camera must be registered and activated on the server for the image to appear.

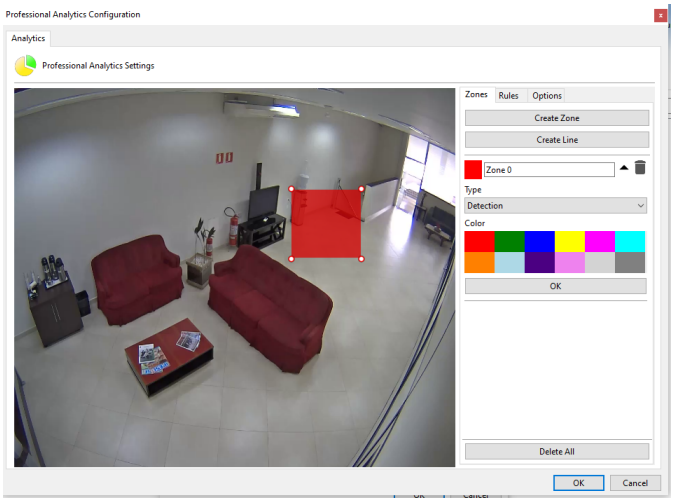
This screen has the following functionalities when the direct button is activated:



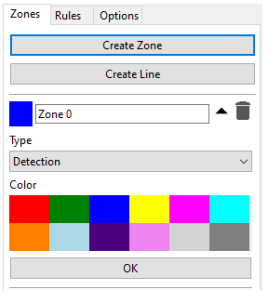
- **Create Zone:** Creates a zone where the analysis module (Rule) will be defined.
- **Create Line:** Creates a line where the analysis module (Rule) will be defined.
- **Create Counter:** Creates a counter that will be associated with an analysis module (rule).
- **Delete:** Deletes a selected zone/line/counter.

© 2002 - 2024 by Digifort. All rights reserved.

Create a zone/line and click on it as shown in the figure below:



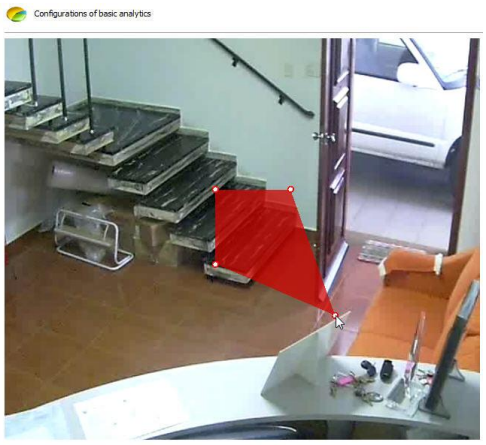
When selecting the object, some options will appear on the right side:



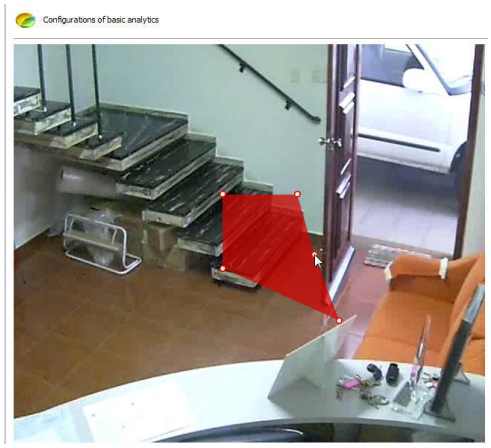
- **Name:** Name for the created zone. It is important that this name is well thought out as it will be possible to generate reports from this name.
- **Color:** Changes the color of the selected zone/line.
- **Type: There are two zone types:** Detection and Non-detection.
  - The **detection zone** is the standard zone where analytics modules are applied.
  - The **non-detection zone** is used to remove unwanted image areas such as trees, rivers, etc. from the analysis.

It is possible to move the zone points by clicking on the circles as in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



And add points by double clicking near the edge of the zone as below:

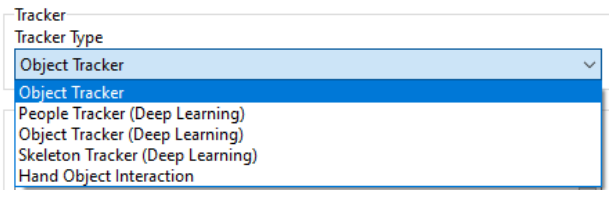


The maximum possible points per zone is 20.
These same rules apply to lines.

14.1.8.6.1 Object Trackers

Professional Analytics has several types of Object Trackers. The Object Tracker is the core component of the analytics solution and is the one that recognizes the objects in the scene, determines their speed, size, direction... Each Object Tracker has different techniques for analyzing a scene and identifying objects. Once objects are identified and classified, rules can be applied to these objects in order to trigger alarms. Each type of tracker is capable of recognizing different types of objects and features.

The configuration of which tracker to use is in Advanced Options of the Analytics Configuration:



- **Object Tracker:** This is the standard object tracker. This tracker uses only CPU (Does not use GPU) and uses the movement to differentiate the background and foreground objects in the scene, together

© 2002 - 2024 by Digifort. All rights reserved.

with the calibration grid and object classification options to recognize and classify objects. As only motion is used to detect an object, the tracker itself is not recognizing an object by the way it looks, instead an object's classification is defined through the use of its estimated size and speed (which are determined by correct calibration of the 3d grid).

- **Object Tracker (Deep Learning):** This object tracker utilizes appearance based neural networks, trained on millions of images, to locate and recognize similar objects in a scene. As a result, the motion of a tracked object and its estimated speed and size are not required to determine the object's classification. The use of appearance based deep learning models generally provides more accurate and diverse object detection in a scene and tends to have lower levels of false alarms due to their resiliency to environmental effects such as lighting changes or extreme weather. This tracker is the most suitable tracker for general analytics use cases if you have a compatible GPU on the analytics server, however it is not recommended for use with thermal cameras, where the standard Object Tracker is the most recommended for this case. Due to the nature of deep learning and specifically neural networks this type or processing is done on GPU.

- **People Tracker (Deep Learning):** This tracker is suitable for processing scenes with people, and just like the Deep Learning Object Tracker, it also uses pre-trained neural networks to recognize people. In this case the People Tracker's Deep Learning models are specifically trained and optimized to only detect people and help identify human behavior.

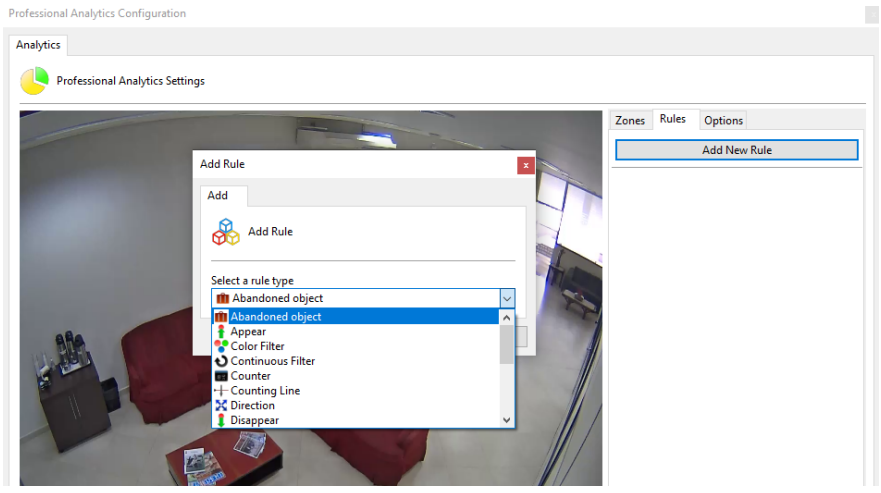
- **Skeleton Tracker (Deep Learning):** This tracker is suitable for tracking people in situations where the camera's field of view is relatively close. The Skeleton Tracker is based on Pose Estimation technology, providing the location of the person in the camera's field of view, as well as additional data such as body parts that are used for advanced pose recognition rules.

- **Hand Object Interaction Tracker:** The Hand Object Interaction tracker was developed to detect hands and the objects they hold. This tracker requires a top-down, relatively close field of view to detect optimally. This tracker requires an additional **Behavior** license.

Some rules are only available to a certain type of tracker, such as the Fall rule (Fallen People) can only be used with the People Tracker (Deep Learning) and Skeleton Tracker (Deep Learning). Select the ideal tracker for your type of scenario.

14.1.8.6.2 How to configure Pro Analytics rules

In the "Rules" tab, it is possible to create a new rule and, when clicking on the add button, the popup for selecting the type of rule will be displayed as shown in the image below:



© 2002 - 2024 by Digifort. All rights reserved.

Here it is possible to combine several filters, inputs and conditions to create complex rules (such as secondary triggers, conditionals, etc.) that can be verified in the configuration of each filter where it is applicable.

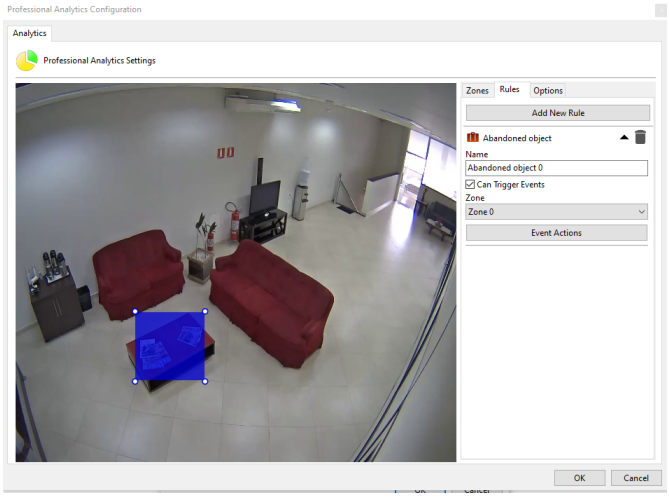
Rules can be of three types:

- **Basic Rules (Inputs)**: These are rules that can be configured so that they trigger by themselves or as a condition for another rule. Basic rules always require a zone associated with them, and may require additional parameters.
- **Filters:** A filter does not trigger an event by itself and requires a basic rule, another filter, or conditional rule as input for triggering events.
- **Conditional:** Conditional rules are similar to filters, in the sense that they do not trigger by themselves, always needing another rule to compose the trigger.

14.1.8.6.2.1 Basic Rules (Inputs)

The **Abandoned Objects** rule can generate alerts when an object is left in a specific area of the image or when something in the scene is changed. Example: A suitcase left on the floor, a key that appears on top of a table. From these events it is possible to recover the video, generate alarms and reports.

In our example, a detection zone was created in the figure below:



Opening the side options of Abandoned Objects we have the following functionalities:

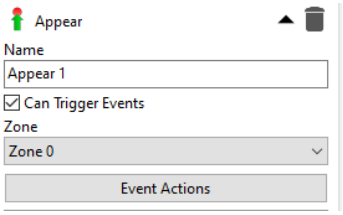
- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

Here is an example where the alarm was triggered in the previously configured situation:

© 2002 - 2024 by Digifort. All rights reserved.

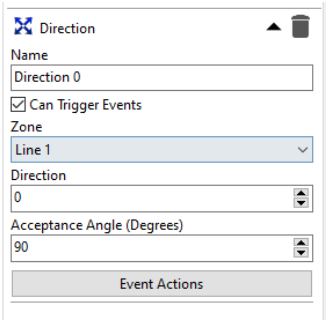
To learn how to generate reports, consult the Surveillance Client manual.

The **Appear** rule will be triggered when an object appears already inside the zone (like coming out of a door, or from the background of the image, etc). When selecting this option we have the following configuration options on the right side:



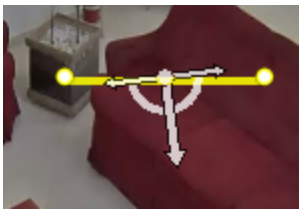
- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Direction** rule will be triggered when an object is moving in a certain direction over a zone. When selecting this option we will have the following settings in the panel on the right side:



- **Name:** Name of the filter;
- **Can trigger events:** Mark this filter with the possibility of triggering events;
- **Zone:** Zone to which this filter is associated;
- **Direction**: Direction of movement (in degrees). The direction can be configured with the help of the graphical interface, simply clicking and dragging the larger arrow:

© 2002 - 2024 by Digifort. All rights reserved.



- **Acceptance Angle:** Movement acceptance angle (for diagonal movements) in degrees. This angle can be configured with the help of the graphical interface, simply clicking and dragging on the smaller indicators:

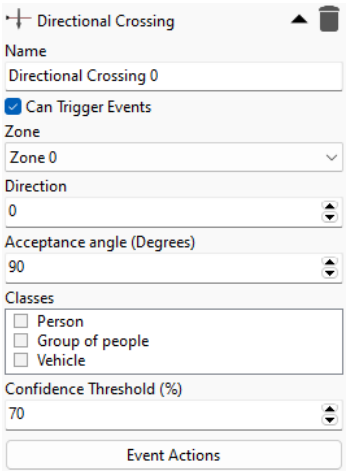
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Directional Crossing** rule will trigger when an object is moving in a certain direction over a zone. This rule differs from the **Direction** rule because it was designed to reduce false alarms, common in cases of simple line crossing. The **Directional Crossing** rule is designed for use with a zone rather than a line and adds a series of additional checks to an object as it enters and leaves that zone.

For an object to trigger the **Directional Crossing** rule it must:

- Enter the zone by traveling in a direction that is within the acceptance angle.
- Be classified as one of the specified object classes.
- Exit this zone by traveling in a direction that is within the acceptance angle.

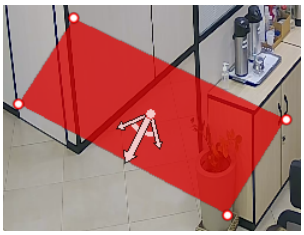
When selecting this rule we will have the following settings in the right-hand panel:



- **Name:** Filter name.
- **Can trigger events:** Mark this filter with the possibility of triggering events;
- **Zone:** Zone to which this filter is associated;
- **Direction**: Direction of movement (in degrees). The direction can be configured with the help of the graphical interface, simply clicking and dragging the larger arrow:

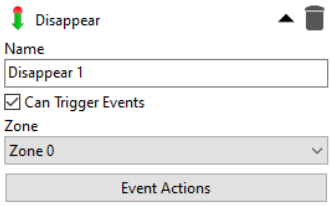
© 2002 - 2024 by Digifort. All rights reserved.

- **Acceptance Angle:** Movement acceptance angle (for diagonal movements) in degrees. This angle can be configured with the help of the graphical interface, simply clicking and dragging on the smaller indicators:



- **Classes**: Which classes will be considered for triggering the event. Object classes will be displayed according to the **Object Tracker type** selected in Advanced Options. Each tracker type will present a different list of supported object types.
- **Confidence Threshold (In percentage):** Specify the minimum confidence for object class recognition (For Deep Learning type trackers).
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about event actions see chapter How to configure event actions.

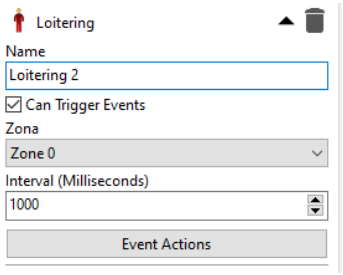
The **Disappear** rule will be triggered when an object disappears from the zone. When selecting this option, you have the following options:



- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

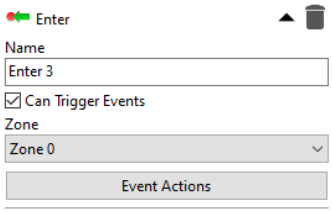
The **Loitering** rule will be triggered when a certain object remains transiting the area for longer than the configured time. When selecting this option, the following settings appear on the right side panel:

© 2002 - 2024 by Digifort. All rights reserved.



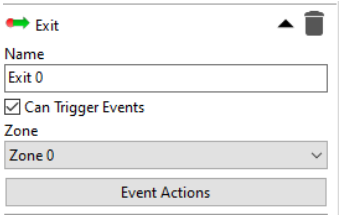
- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Interval (milliseconds):** Time interval that the object must remain in the zone to trigger the event.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Enter** rule will be triggered when an object enters the zone. When selecting this rule the following options are displayed:



- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Exit** rule will be triggered when an object leaves the selected zone. When choosing this rule, the following options are displayed on the right side panel:

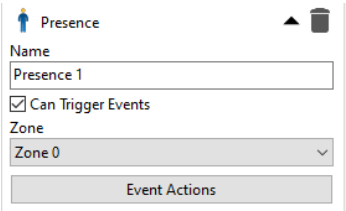


- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Presence** rule will be triggered when an object is detected within the zone, either coming from outside (entering) or appearing within the zone. When selecting the presence rule, the following options

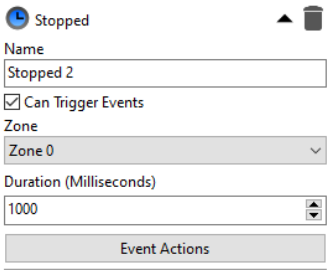
© 2002 - 2024 by Digifort. All rights reserved.

will be displayed:



- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

The **Stopped** rule will be triggered when an object has been stopped in a zone for a specified time. When selecting this rule we have the following options in the right-hand panel:



- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Duration (milliseconds):** Time interval that the object must remain stationary in the zone to trigger the event.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

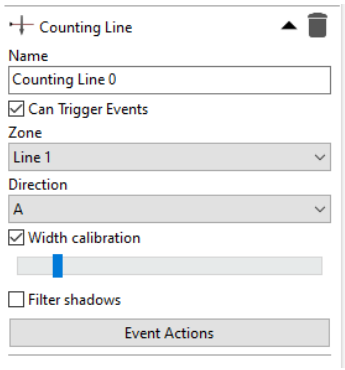
The **Tailgating** rule will be triggered when a second object passes a certain area after the first object, within a configurable period of time. We can exemplify an alarm when a car passes along with another when a toll gate rises. When selecting the tailgating option the following options are displayed:

- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.

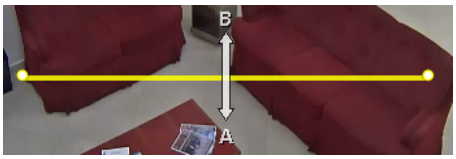
© 2002 - 2024 by Digifort. All rights reserved.

- **Duration (milliseconds):** Time interval between objects entering an area. If after an object enters the area, a second object enters with a time shorter than that configured, the event will be triggered.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

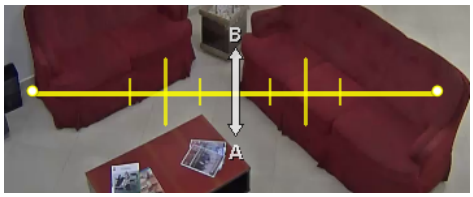
The **Counting Line** rule will be triggered when an object is detected crossing a line, and can be used to count objects. The selected zone type must necessarily be of the line type. When selecting the counting line we have some options for calibration and configuration:



- **Name:** Name of the filter;
- **Can trigger events:** Mark this filter with the possibility of triggering events;
- **Zone:** Zone to which this filter is associated;
- **Direction:** Direction in which the object must cross the line. Select between A, B or A/B. The visual interface indicates the direction:



- **Width Calibration:** Width of objects to be captured. When activating this option, the system will display a visual indication of the width to be considered, giving the operator the possibility to use the slider for the best adjustment:



Larger bars indicate the average size of the object, while smaller bars indicate the minimum and maximum to be considered by the system.

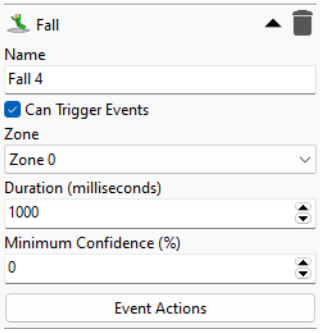
- **Shadow filter:** Activates or deactivates the shadow filter, thus avoiding double counts due to the excess of the object.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

© 2002 - 2024 by Digifort. All rights reserved.

Important

This rule is only available for the **People Tracker (Deep Learning)** and **Skeleton Tracker (Deep Learning)**

The **Fall** rule will be triggered when a person is detected fallen in the input zone. When selecting the fall rule, the following options will be displayed:



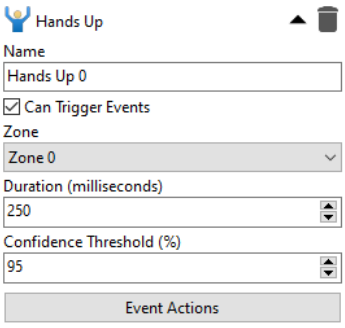
- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Minimum Confidence (In percentage):** Specify the minimum detection confidence.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

Important

This rule requires an additional **Behavior** license

The **Hands Up** rule detects when an object classified as a Person, by the **Skeleton Tracker (Deep Learning)**, has its hands raised.

When the **Hands Up** rule is added to a channel configuration, the **Hands Up** detection algorithm starts running in the background on any detected person. The classification is based on the metadata of the skeleton keypoints generated by the **Skeleton Tracker (Deep Learning)**. Currently this rule is only available when using the **Skeleton Tracker (Deep Learning)**. When selecting the drop rule the following options will be displayed:



- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Zone**: Zone to which this filter is associated.
- **Duration:** Period of time in which the person must have their hands up for the rule to be triggered.

© 2002 - 2024 by Digifort. All rights reserved.

- **Confidence Threshold (In percentage):** Specify the minimum detection confidence.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about event actions see chapter How to configure event actions.

Important

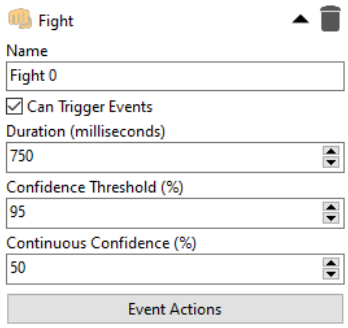
This rule requires an additional **Behavior** license

The **Fight** rule that is triggered when fighting behavior is detected in the field of view for longer than the specified duration.

Note

This rule does not require a zone and runs independently of the tracker. Enabling this algorithm by adding this rule will impact channel capacity as the algorithm runs in addition to the selected tracker.

When selecting the drop rule the following options will be displayed:

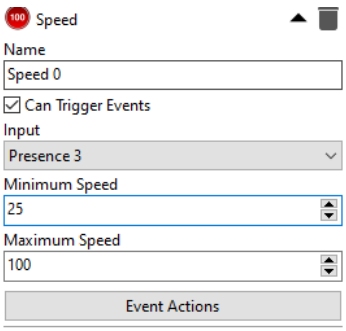


- **Name:** Name of the filter.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Duration:** Detection time period for the rule to be triggered.
- **Confidence Threshold (In percentage):** Specify the minimum detection confidence before the fight is detected.
- **Continuous Confidence (In percentage):** Specify the minimum continuous confidence required for the specified duration.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about event actions see chapter How to configure event actions.

14.1.8.6.2.2 Filters

The **Speed Filter** will be triggered when an object, which triggered an input rule, is traveling between a minimum and maximum speed. For this filter to generate an event, the channel must have been calibrated. When selecting the speed filter, the following options will be available in the right-hand panel:

© 2002 - 2024 by Digifort. All rights reserved.



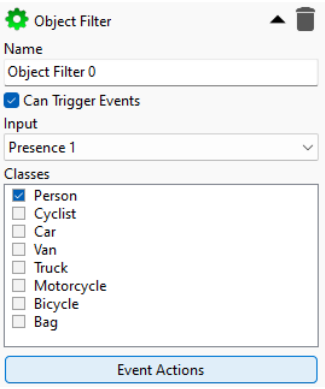
- **Name:** Filter name.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Input:** Input rule for this filter.
- **Minimum and Maximum Speed:** Set the minimum and maximum speed values. The event will be triggered if the object's speed is between the minimum and maximum values.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

In the example above we have the filter named "Speed 0" triggering events for objects detected within the "Presence 3" rule that are between 25 and 100 km/h (or mph, depending on the calibrated measurement unit). Objects detected below 25km/h or above 100km/h will be disregarded.

Tip

If this filter is triggered, both it and the input rule will trigger events. For example, if a **Presence** rule was used as an input rule for this filter, then you will have this input rule and also the **Speed Filter** triggered (If the conditions of this filter have been met). You can disable the input rule triggering events by deselecting the **Can Trigger Events** option in the input rule settings, so only **Speed Filter** events will be triggered.

The **Object Filter** is used to give more assertiveness to the rules created, so we can have an area where the triggering of a rule only happens for objects of interest (triggering for people but not for vehicles or other objects, etc.). When selecting the object filter we have the following options:



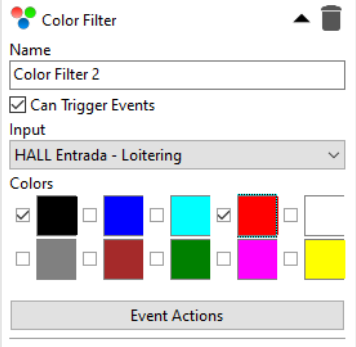
- **Name:** Filter name.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Input:** Input rule for this filter.
- **Classes**: Which classes will be considered for triggering the event. Object classes will be displayed according to the **Object Tracker type** selected in Advanced Options. Each tracker type will present a different list of supported object types.

© 2002 - 2024 by Digifort. All rights reserved.

- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

In this example we will have a trigger if the "Presence 1" rule is triggered by a person. If it is a vehicle or other type of object, no action will be taken.

The **Color Filter** will be triggered when an object, which triggered an input rule, has at least 5% of any selected color. When selecting this filter we have the options below:

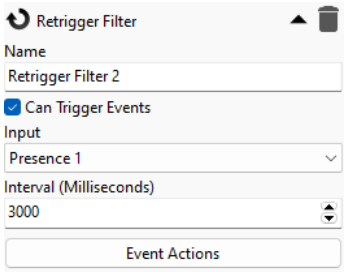


- **Name:** Filter name.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Input:** Input rule for this filter.
- **Colors:** Select object colors that can trigger this event. This is an OR list, which means the event will trigger if the object has any of the selected colors.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

In the example above we will have a trigger if an object with black or red colors (or both) is detected in the rule "HALL Entrance - Loitering".

The **Retrigger Filter** acts as an event passthrough, which only generates an event if the input has not previously been triggered within the defined interval.

Typically, the **Retrigger Filter** would be applied at the end of a rule combination to avoid sending duplicate alarms. This provides more granular control than the **Event Retrigger Time** option. The events produced by the **Retrigger Filter** will have the event type of the inbound rule. When selecting this filter we have the options below:



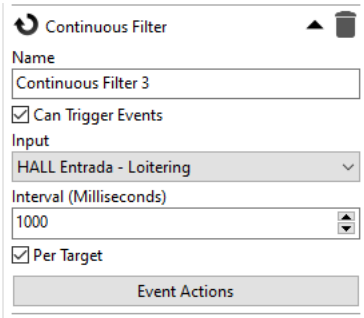
- **Name:** Filter name.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Input:** Input rule for this filter.
- **Interval (milliseconds):** Period in which the input event cannot generate another event.

© 2002 - 2024 by Digifort. All rights reserved.

- **Event Actions**: Desired event actions when this rule is triggered. To learn more about event actions see chapter How to configure event actions.

14.1.8.6.2.3 Conditional

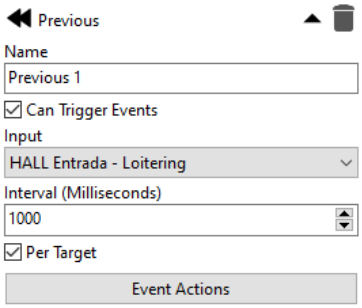
The **Continuous** conditional rule will be triggered only if an input rule remains "alarmed" for a certain period of time. When selecting this condition we have the following options:



- **Name:** Filter name.
- **Can Trigger Events:** Check this option if this rule can trigger events.
- **Input:** Input rule for this filter.
- **Interval (milliseconds):** How long the input rule must remain alarmed for it to trigger.
- **Per Target:** If this option is checked, the system will trigger an independent event for each object.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

In the example above, the condition will take the configured actions if an object triggers the loitering event of watering "HALL Entrance - Loitering" continuously for at least one second. If a second object is in the zone simultaneously and triggers loitering for a second, the rule will be triggered again.

The **Previous** conditional rule is used to generate complex scenarios and will be triggered when a certain rule occurred previously within a certain period of time. This rule is useful when combined with some other conditional rule such as the **Logical Filter And**, where for example, it could be triggered if a Presence rule was triggered but before the Presence rule, a Loitering rule was triggered 1 second before . When selecting this condition the following options are available:

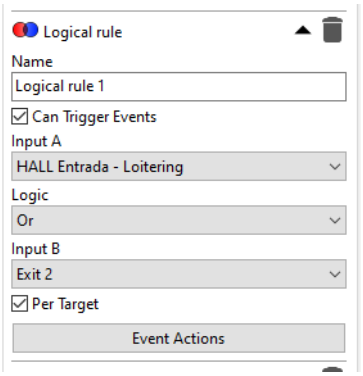


- **Name:** Condition name;
- **Can trigger events:** Check this condition with the possibility of triggering events;
- **Input:** Rule where you want to apply this filter;
- **Interval (milliseconds):** Interval from the previous rule trigger.
- **Per Target:** If this option is checked, the system will trigger an independent event for each object.

© 2002 - 2024 by Digifort. All rights reserved.

- **Event Actions:** Desired alarm actions when analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

The **Logical Condition** rule allows you to combine rules to form even more complex filters and conditions, allowing the use of analytics for complex scenarios where it is necessary to configure different actions for each type of scenario. When selecting this option we have the following settings available on the panel:



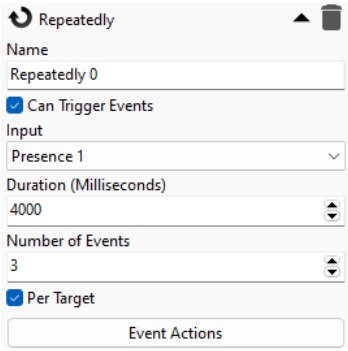
- **Name:** Condition name;
- **Can trigger events:** Check this condition with the possibility of triggering events;
- **Input A:** First rule where you want to apply this filter;
- **Logic:** Type of logic to be used (OR, AND or NOT);
- **Input B:** Second rule where you want to apply this filter;
- **Per Target:** If this option is checked, the system will trigger an independent event for each object.
- **Event Actions:** Desired alarm actions when analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

The available logics are the following:

OR: This option will cause the condition to be triggered if rule A **OR** rule B has been triggered.
AND: This option will cause the condition to be triggered only when **BOTH** configured rules are triggered.
NOT: This option will cause the condition to be triggered when rule A is **NOT** triggered.

The **Repeatedly** rule is a logical operator that fires when an input rule is triggered a certain number of times within a defined period. The duration period is a time window calculated from each input event. For example, with a Repeatedly rule configured to generate an event when the input fires three times in eight seconds and this input rule fires four times in eight seconds, the Repeatedly rule will fire after the third input rule fires and again after the fourth. This is because the first three triggers (events 1-3) fired within an 8-second window, in addition, the second set (events 2-4) also occurred within its own 8-second window. When selecting this option we have the following settings available on the panel:

© 2002 - 2024 by Digifort. All rights reserved.



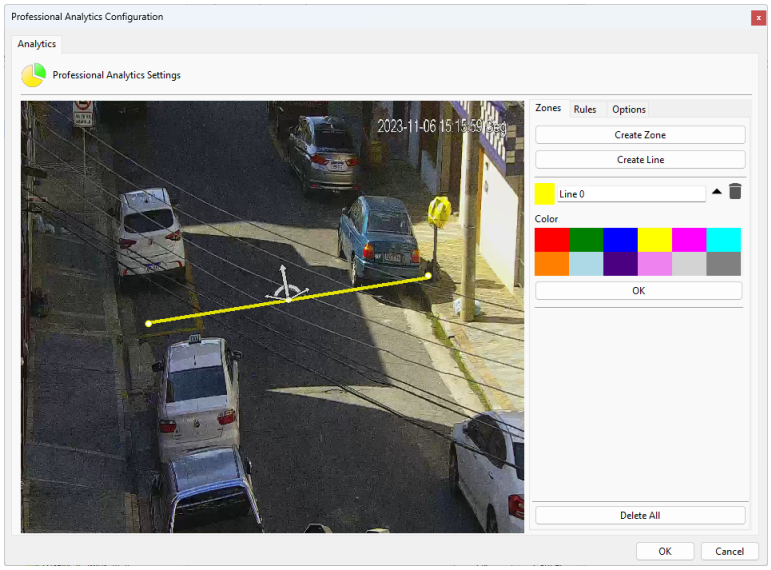
- **Name:** Condition name;
- **Can trigger events:** Check this condition with the possibility of triggering events;
- **Input:** Rule where you want to apply this filter;
- **Duration (milliseconds):** Time in which the configured number of events must occur for triggering.
- **Number of Events:** Number of events required to trigger the rule.
- **Per Target:** If this option is checked, the system will trigger an independent event for each object.
- **Event Actions**: Desired event actions when this rule is triggered. To learn more about event actions see chapter How to configure event actions.

14.1.8.6.3 Counters

Counters are visual objects that allow, in real time, when monitoring images, to know the count of events that are happening.

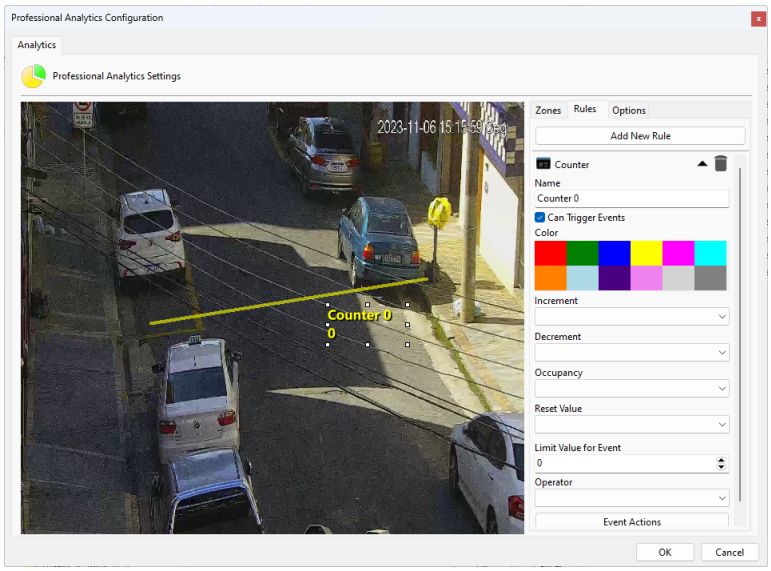
Counters are incremented or decremented by triggered rules and can trigger events when the value satisfies the conditional rule.

To configure a counter, you first need to give it one or more input rules. In the example below, we have a **Direction** rule that we will use to increase the counter value when vehicles trigger this rule:



To create the counter, right-click on the image and select the **Create Counter** option:

© 2002 - 2024 by Digifort. All rights reserved.

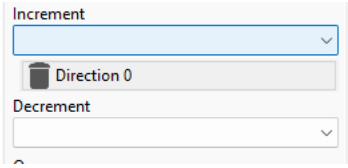


When the counter is created, it will be selected and in the right menu some options are available:

- **Name:** Counter name.
- **Can trigger events:** Check this condition with the possibility of triggering events;
- **Color:** Color of the counter to be displayed on the screen.
- **Increment:** Which rule(s) will increment the counter when triggered.
- **Decrement:** Which rule(s) will decrement the counter when triggered.
- **Occupation:** Which rule(s) will be part of the occupancy condition, which will display the count of rules currently alarmed.
- **Reset Value:** Which rule(s) will reset the counter value to 0.
- **Limit Value For Event:** What value should the counter reach for the triggering of actions to occur.
- **Operator (none, >, <, >=, <=, ==, !=):** Which operator will be taken into account with the limit value (for example: selecting the ">" operator for triggers above a certain limit value or the "!=" operator for when it is different from the selected limit value, etc.).
- **Event Actions:** Desired alarm actions when analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

For better learning, we will illustrate how to use the resources above.

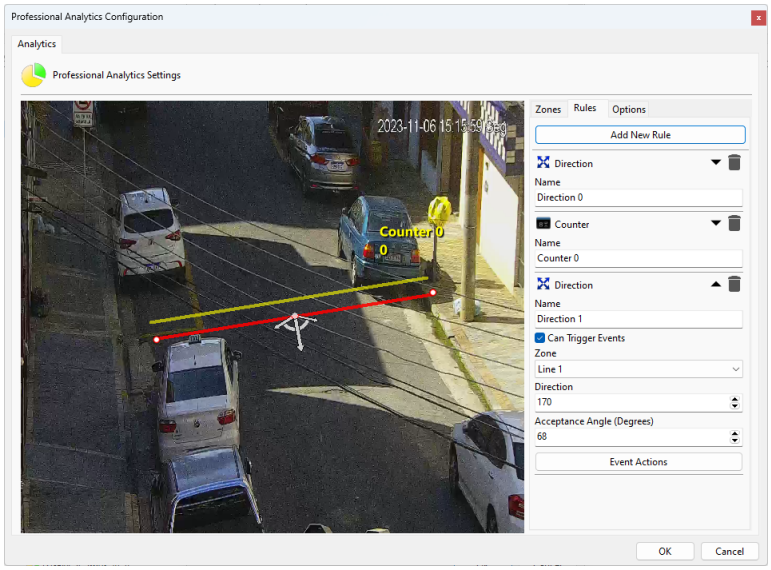
Initially we will just increment the counter with the direction rule we created. To do this, open the **Increment** option and in **Rule** select which type of rule you want to increment (In this case we only configured the **Direction Filter (Direction 0)** so it is the only one available).



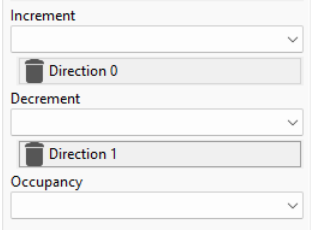
After selecting the rule you will notice that it will be added to a list below the selection control. You can add multiple rules to increment, decrement or display occupancy in the counter. To remove a rule, simply click on it (The control is a button).

Now we will create another **Direction Filter** rule as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

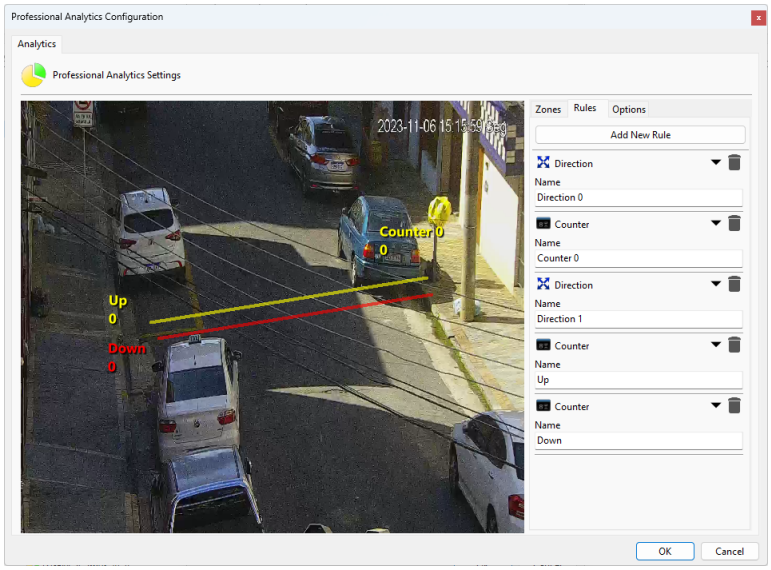


With this Rule we will **decrement** the counter already created.
Select it and in **Decrement** choose the second Zone rule as shown in the figure below:



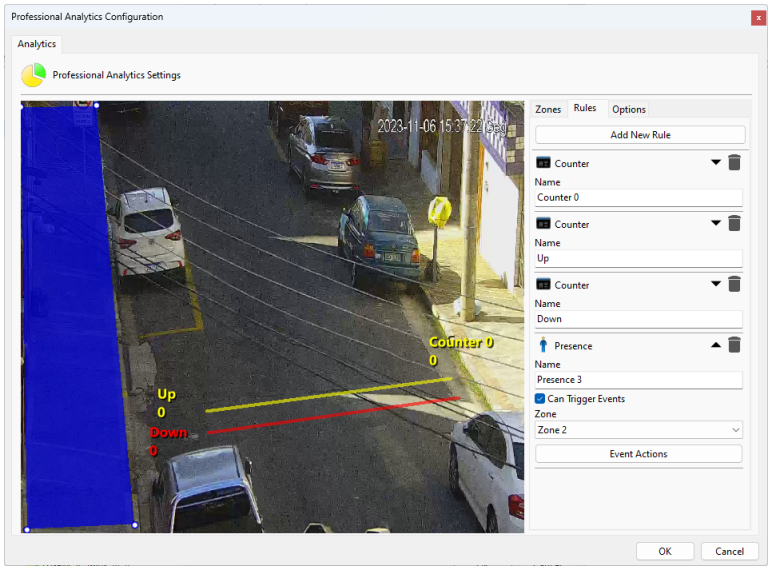
With this configuration, the Counter will **increase** when vehicles are traveling upwards and **decrease** when vehicles are traveling downwards.

There could still be a counter for each line as shown in the figure below:

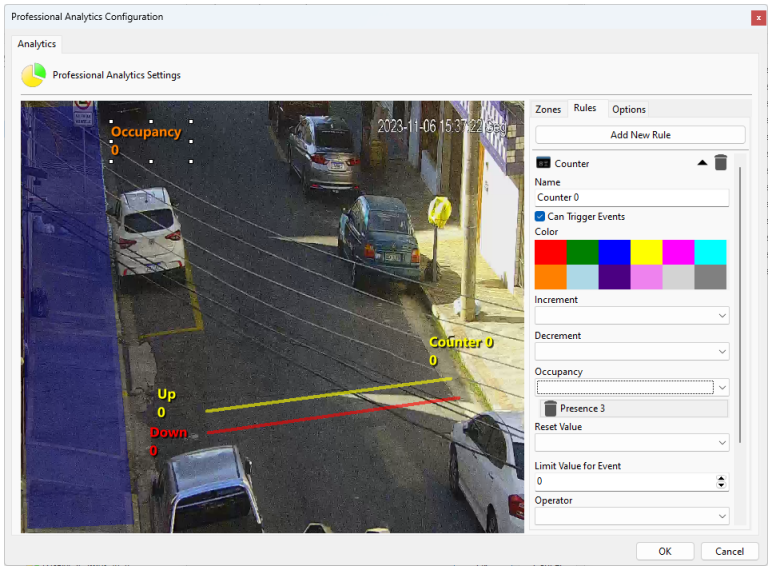


© 2002 - 2024 by Digifort. All rights reserved.

To test the **occupancy** counter we will create a presence detection area as shown in the image below:



Now a counter will be created that will show the value of how many presence rules are activated within that area, in other words, return how many objects are present at the exact moment within the area. The image below shows this configuration:



You can configure up to 40 counters per analytics configuration.
The size of the counter can be adjusted by selecting and dragging the squares around it.

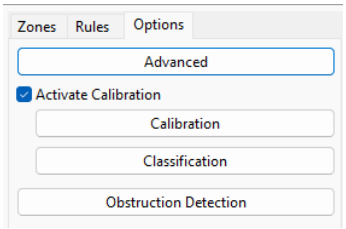
14.1.8.6.4 Scene Calibration

Professional analytics requires some calibration settings for it to work properly.

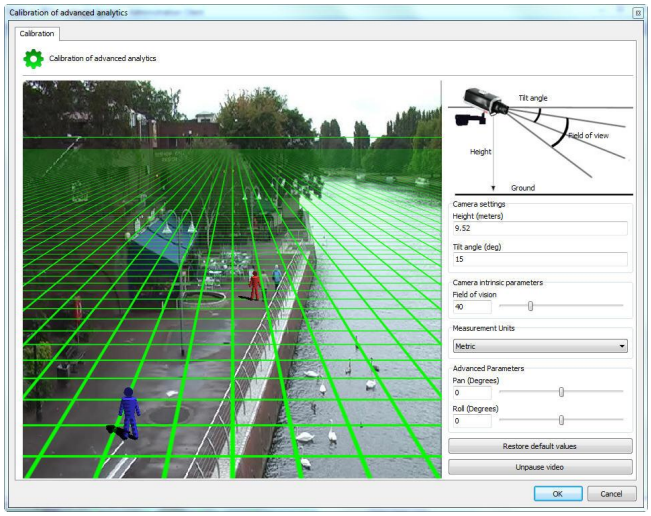
The first configuration is the calibration of distances, it is necessary to get alarms like speed and to classify objects like cars, people, groups of people and so on.

© 2002 - 2024 by Digifort. All rights reserved.

To start, on the analytics configuration screen, click on **Calibration:**



The following screen will be displayed:



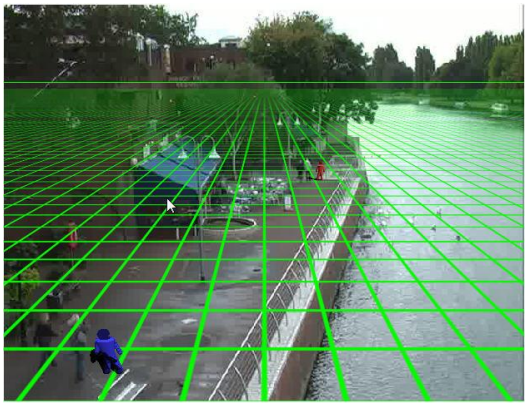
On this screen, the configured camera image will appear along with a 3D Grid.

If no command is activated, some messages will appear on the screen with information on how to operate the grid:

- Measure or estimate the height of the camera above the ground.
- Use the middle mouse button to adjust the camera height
- Click and drag the grid to change the vertical angle of the camera
- Click and drag the 3D people to compare the size with the people in the image.
- Each grid square equals 2 square meters.

To facilitate configuration, first move the grid trying to position the Horizon line compatible with the image as shown in the figure below:

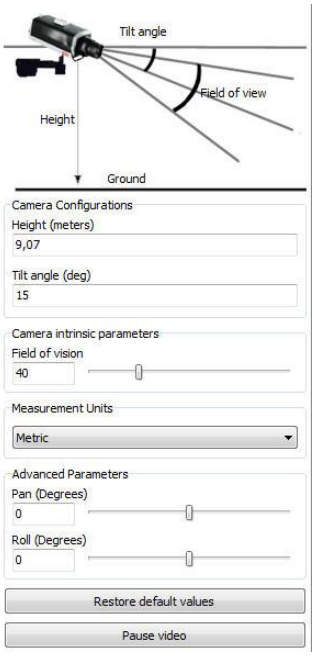
© 2002 - 2024 by Digifort. All rights reserved.



In the configuration above you can see the horizon line, the grid compatible with the image and the 3D puppets with the approximate size of the people in the image.

Ready! The grid is already configured.

In case you have precise values of the positioning of the camera in the place, the menu on the right side also helps in configuring the grid:



The menu has the following features:

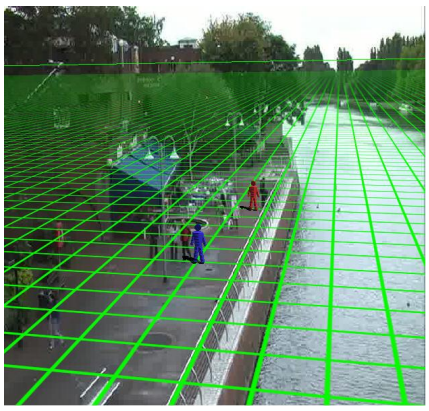
- **Height:** Height in meters that the camera is in relation to the ground.
- **Tilt Anle:** Vertical angle of the camera.
- **Field of view:** Camera's field of view.

These values, when changed, automatically adjust the positioning of the Grid.

- **Units of Measure**: You can change the measurement type from **Metric** to **Imperial** in the **Unit of Measure** field.

© 2002 - 2024 by Digifort. All rights reserved.

- **Advanced Parameters**: Use the parameters below for a finer adjustment of the grid as in the figure below.



  - **Pan (Degrees):** Rotates the grid on the Y axis of the Cartesian plane.
  - **Roll (Degrees):** Rotates the grid on the Z axis of the Cartesian plane.

- **Restore Default Values:** Restores the initial grid positioning values.
- **Pause video:** Allows you to pause the camera video for grid adjustment

With the grid configured correctly, we will be able to classify the objects being detected. See the next chapter to learn how to classify objects.

14.1.8.6.5 Object Classification

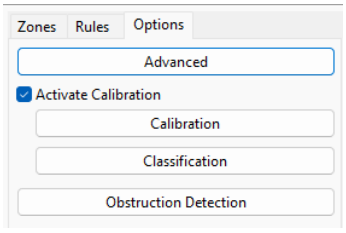
Important

The classification list is only necessary for using the standard Object Tracker (No Deep Learning)

The analytics uses the object classification table to determine the type of object recognized by the object tracker, based on its size and speed and with this, the object class can be used to filter detections for objects such as cars, people, groups of people, animals, etc. Example: An area can trigger alarms only when people move around or only when cars are stopped.

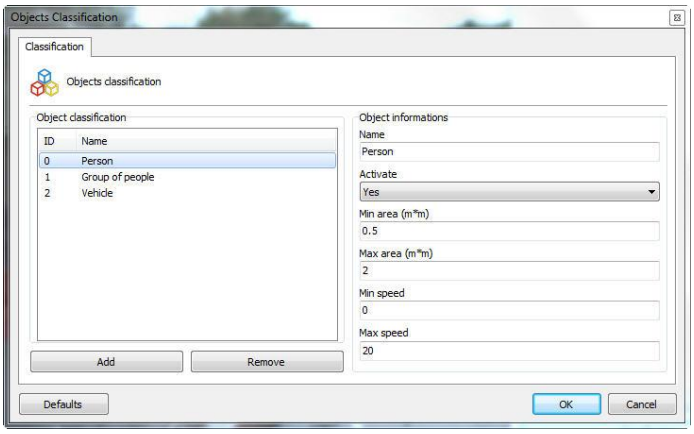
After **Calibration** has been done correctly it is possible to create object classifications.

To start, on the analytics configuration screen, click on **Classification:**



The following screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



Initially the system will have the standard objects registered, namely: **People, Group of People and Vehicles**. To register a new object, click **Add** and fill in the fields. The image above shows what a **Person** classification would look like when registering.

The fields that must be filled in are described below:

- **Name:** Name of the classification to be added.
- **Active:** Sorting can be turned off at any time by changing the checkbox to **no**.
- **Minimum Area:** The minimum area that the object must have to be recognized within this classification.
- **Maximum Area:** The maximum area that the object must have to be recognized within this classification.
- **Minimum Speed:** The minimum speed that the object must be at to be recognized within this classification.
- **Maximum speed:** The maximum speed that the object must be at to be recognized within this classification.

To remove a classification, just select it from the list and click **Remove**.

Here is the result of this classification in the monitoring:

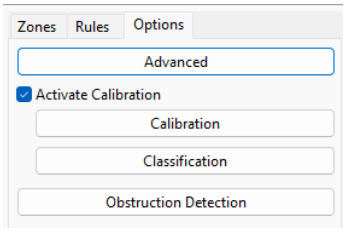
To learn how to view the live analytics functionalities, consult the Surveillance Client manual.

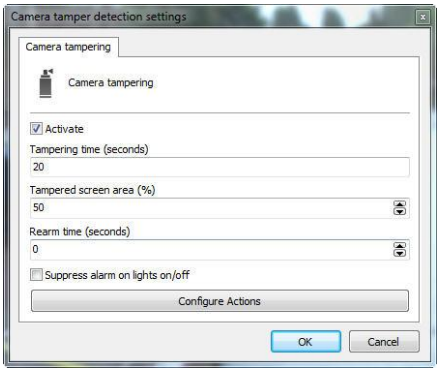
© 2002 - 2024 by Digifort. All rights reserved.

14.1.8.6.6 Camera Tampering

The **Camera Tampering** module may trigger alarms if something obstructs the camera's image, for example: changing the camera's position, blocking the lens, placing an object to block the view of an area.

To configure the camera obstruction module, click the **Obstruction Detection** button on the Analytics Configuration screen as shown in the image below:



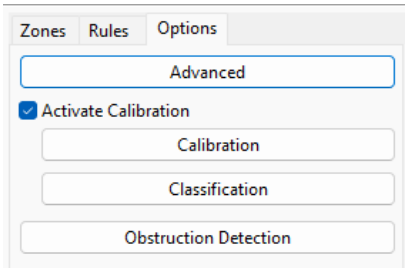


This screen has the following features:

- **Activate:** Enables or disables the operation of the camera tampering module.
- **Tampering Time:** Time in seconds that the camera must be obstructed for the alarm to be triggered.
- **Tampered Screen Area:** Percentage of the image that must be obstructed for the alarm to be triggered.
- **Rearm Time:** Waiting time for another alarm to be triggered.
- **Suppress alarm on lights on/off**: Does not trigger the alarm when turning on and off the ambient light.
- **Configure alarm actions:** On the alarm screen, configure the desired actions when the analytics trigger events. To learn more about alarm actions see chapter How to configure alarm actions.

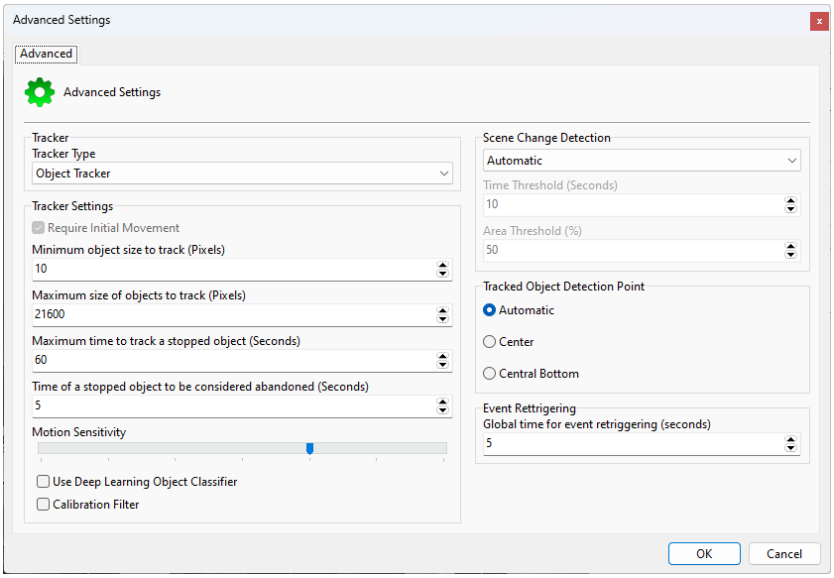
14.1.8.6.7 Advanced Options

When selecting the options tab, we have the following screen:



© 2002 - 2024 by Digifort. All rights reserved.

When clicking on **advanced options** the following screen will appear:



Within this screen, it is possible to make several fine adjustments and configurations necessary for the operation of the engine:

- **Tracker selection:** In this menu it is possible to select the type of engine to be used. Having as an option Object Tracker (where the engine learns the scenario and analyzes the pixels to determine objects/background of the scene) and People Tracker (Deep Learning) / Object Tracker (Deep Learning) which are exclusive to professional analytics. These trackers will use deep learning technology to analyze the data and when starting the following message will be displayed on the Surveillance Client:

This indicates that the engine is initializing the analytical models compatible with the GPU used on the server (it is necessary to install the drivers CUDA in the server). This process can take up to 60 minutes per model and can vary depending on the GPU, once the initialization process has finished the message will disappear and will not be needed unless the GPU is changed or driver updated.

- **Tracker Options:** Tracker options will vary based on the type of tracker selected. Getting disabled when not applicable for the selected tracker. The options are:
  - **Initial movement required:** Check this option so that the system waits for the initial movement to track objects. This option is only available for the Deep Learning Object Tracker and is necessary to recognize only moving objects because due to the nature of Deep Learning, it will recognize stationary objects (For example a parked car) and this option is necessary to recognize only the objects that have their first movement detected.
  - **Minimum object size for tracking (pixels):** Minimum size, in pixels, for the system to consider the object.
  - **Maximum object size for tracking (pixels):** Maximum size, in pixels, for the system to consider the object.
  - **Maximum time to track stationary objects (seconds):** Time in seconds that the system will wait to consider an object as part of the environment.

© 2002 - 2024 by Digifort. All rights reserved.

- **Time for a stationary object to be considered abandoned (seconds):** Time in seconds that the system must wait to consider a stationary object as abandoned.
- **Motion Sensitivity:** Motion sensitivity setting so that the system considers it as an object rather than as part of the environment.
- **Use Deep Learning Object Classifier:** Check this option to have object classification derived from deep learning instead of object crawler
- **Calibration Filter:** The Calibration Filter is a tool that prevents objects that are too large or too small from being tracked and causing false alarms. This tool also improves situations where a large amount of motion is detected in the Object Tracker caused by lighting changes, or a Deep Learning Tracker recognizing very large or very small features as valid objects. An object is defined as large or small based on the metadata produced when Calibration is enabled. When the Calibration Filter is activated, an object is only valid when it meets all of the criteria below:
  - Object Height larger than 0.5m
  - Object Height shorter than 6m
  - Object Area larger than 0.5m²
  - Object Area smaller than 50m²

- **Scene change detection:** This option is used for the standard Object Tracker to recognize that a scene has changed significantly and must be relearned.
  - **Disabled:** Scene change detection will be disabled.
  - **Automatic:** This is the most recommended option and will automatically recognize when a scene changes significantly.
  - **Manual:** Uses manually determined scene change parameters
    - **Time limit (seconds)**: Time limit to trigger the learning of a new scene.
    - **Area limit (%):** What percentage of the image must be changed for the system to learn the scene again.
  - **Adaptive:** The system will automatically adapt to changes in the scene. This option is recommended for use with thermal cameras.

- **Tracked Objects Detection Point:** The rules are activated from this point, which must have its position configured according to the scene.
  - **Default:** The default point will be centered below the object
  - **Centroid:** The point will be the center of the object
  - **Central Bottom:** The point will be centered below the object

Centroid

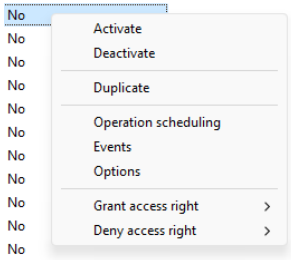
Central Bottom

© 2002 - 2024 by Digifort. All rights reserved.

- **Event redisplay time (seconds):** This option allows the configuration of a global timer for retriggering events of the same object and rule.

14.1.8.7 How To Change Parameters For Multiple Analytics Simultaneously

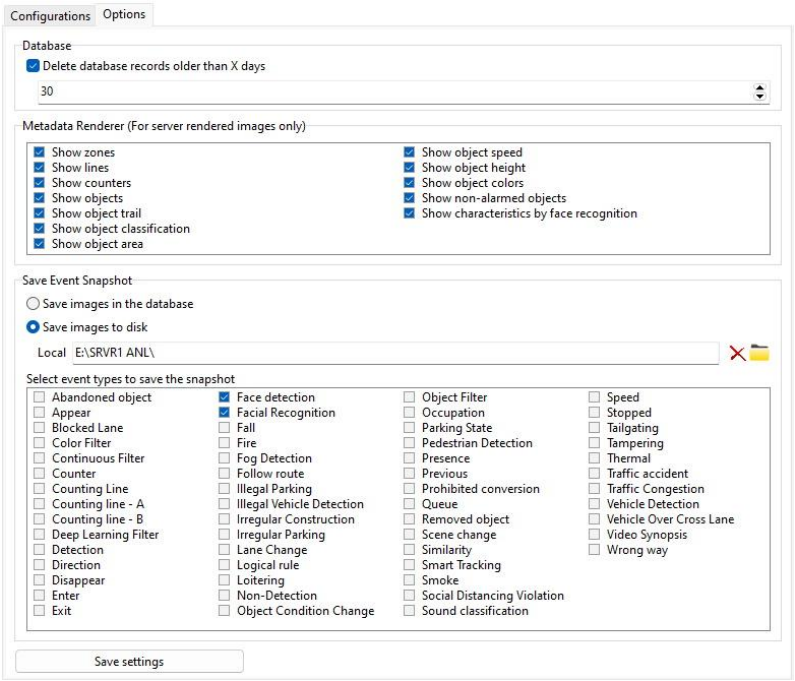
The system analytics configuration manager provides quick access to the most common settings that can be changed for multiple analytics simultaneously. In the analytics configurations register, select the desired analytics and right-click. A menu will open as shown in the figure below:



Most of the options you can change are self-explanatory and you can consult the Analytics Configuration Registration topic to learn more about each option.

14.1.9 General Options

In the **Options** tab, we will have several general options applied to all Analytics Configurations:



- **Delete Old Database Records Older Than X Days:** Enable this option to have the system automatically delete old analytics event records
  - **Days:** Select the number of days to keep records

- **Metadata Renderer:** When the server needs to send images from cameras (For example a snapshot for a snapshot event action or an email with the analytics image), it needs to render the metadata

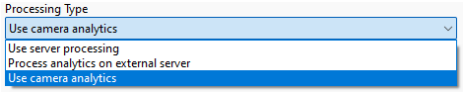
© 2002 - 2024 by Digifort. All rights reserved.

received from the camera into the image. This option allows you to specify which data will be rendered in the image.

- **Save Event Snapshots:**
  - **Save Images To The Database:** The images of the analytics events will be saved in the Database. This option is not recommended as it may inflate the size of the database file and decrease its performance.
  - **Save Images To Disk:** Analytics event images will be saved directly to a folder on disk.
  - **Select Event Types To Save Snapshots:** This list contains all analytics event types supported by the system. Select the analytics event types you want to have event images saved for. By default only Facial Recognition and Face Detection will be activated.

14.2 Edge Analytics

The system allows the use of analytics embedded in cameras or analytics from third-party analytics providers instead of processing on the system's local analytics server. To use this option you must select the Analytics Configuration Processing Type:



As Analytics Configurations have been discussed previously, to learn how to add an Analytics Configuration, see the Adding an Analytics Configuration topic.

- **Process Analytics on External Server:** Select this option to use integration with third-party image analysis software (and servers). If this option is selected, the configuration screen below will be displayed:

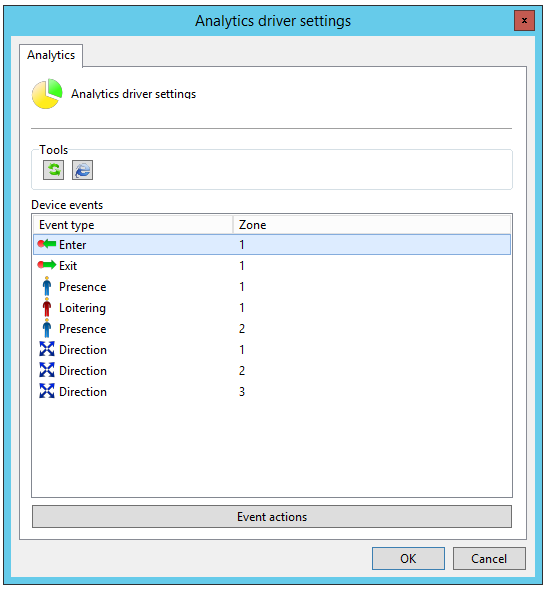
  - **Type:** Select the external server type (Supported Software).
  - **Version:** Select the supported version of the external server.
  - **Server Address:** Enter the external server address.
  - **Port:** Enter the communication port of the external server.
  - **Use SSL:** Select for secure communication with the server (If it supports it).
  - **User:** User for authentication on the server.
  - **Password:** Password for authentication on the server.
  - **ID:** String with camera ID or additional server parameters. See the external server integration technical document for more information.

- **Use Camera Analytics:** If the selected camera has embedded analytics and this is supported by the system, this option will be available. Select this option to use the camera's built-in analytics.

© 2002 - 2024 by Digifort. All rights reserved.

In both options, the analytics configuration will be done externally to the system (Directly on the camera or directly on the external server being integrated) and the system will only receive metadata and events from the device.

Click **Analytics Settings** to open event binding:



On this screen you will have the list of events configured on the external device. To associate event actions, select the desired event and click **Event Actions**.

- **Event Actions**: Desired event actions when this rule is triggered. To learn more about alarm actions see chapter How to configure event actions.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XV

15 Plate Recognition

LPR is a set of services that processes images from cameras to automatically read vehicle license plates. The system has several tools to work with results such as searches, reports, alarms, automation, among others.

LPR is considered an additional module as it is not included in the camera server license.

The system supports server-side or edge-side LPR processing. In the case of LPR on a server, the camera images will be processed by the system's LPR module, on servers dedicated to image processing, whereas in LPR on edge, the cameras themselves already process the images and only send metadata and results of reading for the system.

The system's LPR module has its own server/service for image processing, which can be installed on the same machine where the cameras are recorded or on another computer designed just for this service (more recommended). Learn more about distributed processing in the chapter Understanding distributed processing.

15.1 LPR on Server

15.1.1 Understanding Distributed Processing

Video analysis for LPR in terms of processing is more demanding than recording/viewing from a camera. Thinking about flexibility, the system has an innovative processing architecture, which is the distributed processing architecture.

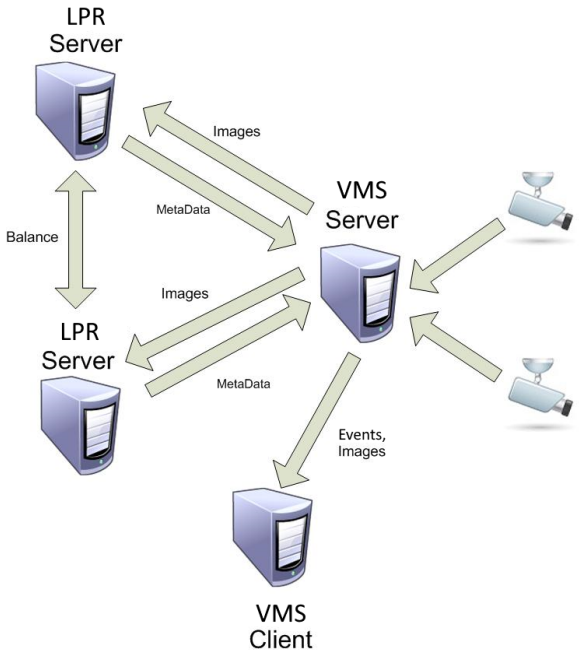
The system allows LPR processing of cameras that are recorded on the camera server to be done on one or more computers that have the LPR Server module. The big advantage is that with this flexibility the recording server is not overloaded and does not need to be a "super-machine".

The LPR server automatically checks the computers with the lowest processing power and performs "load balancing", that is, it distributes the processing of video analysis in order to leave all computers with the lowest possible processing capacity, as long as all servers have sufficient licenses.

What determines the number of LPRs that can run on the same server is the processing capacity of this server. The larger the processor, the greater the possibility of running multiple cameras at the same time. The system processes LPR in fixed and PTZ IP cameras and in fixed and PTZ analog cameras, as long as these are converted through encoders or DVRs integrated into the system.

See the diagram below:

© 2002 - 2024 by Digifort. All rights reserved.



In the diagram above, the **VMS Server** records images from the cameras and sends them to the **LPR Servers**, which in turn perform the analyzes and return the metadata (information on recognized license plates and vehicles). Between the **LPR Servers** there is load balancing, if configured for this. When the metadata returns to the **VMS Server**, it sends the metadata and events to the **VMS Clients** (Surveillance Clients).

15.1.2 How To Start The LPR Server Service

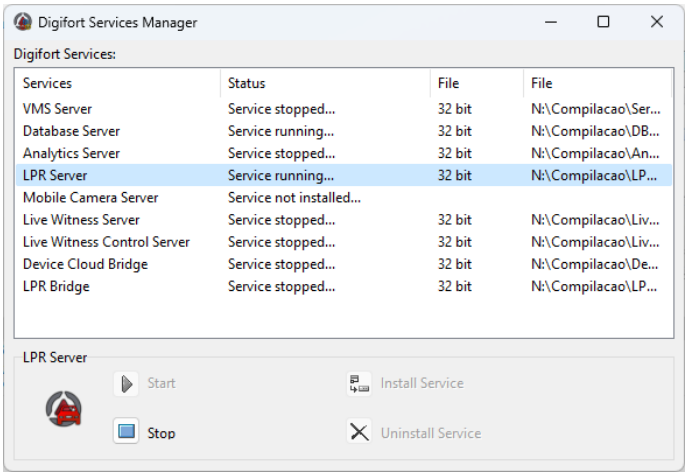
To start the LPR Server service, it must first be installed, follow the steps below to correctly start the service using the Service Manager:

1. Select the **LPR Server** service.

2. Click **Install Service**, a confirmation window will be displayed to select the service architecture (32 or 64 bits), informing you that the service was installed successfully.

3. Click **Start** and wait while the server starts. The initialization process ends when the message “Service running...” appears in the status bar.

© 2002 - 2024 by Digifort. All rights reserved.

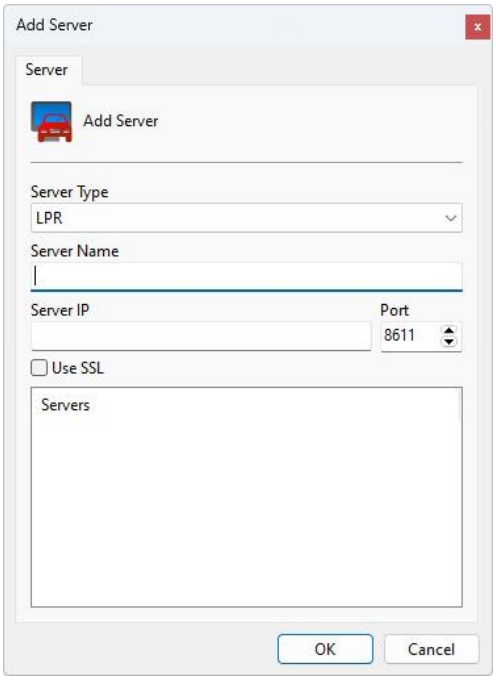


Important

Some engines only work in 64bit

15.1.3 How To Configure The Servers To Be Managed

The first step to be taken when configuring an LPR server is to add it to the list of servers to be managed by the Administration Client.
To add a server, click on the **LPR Servers** tree and then on the **Add Server** button, opening the server registration screen, as illustrated below:



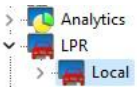
- **Server Name:** Enter the name of the server to be added. After confirming the data, the server name cannot be changed.
- **Server IP**: Enter the IP of the server to be managed.
- **Port:** Enter the communication port with the server. By default the port is 8611 or 8411 for secure connection with SSL/TLS
- **Use SSL:** Use secure connection with SSL/TLS. Don't forget to specify the SSL/TLS connection port.

© 2002 - 2024 by Digifort. All rights reserved.

- **Servers:** All LPR servers that the administration client found on the network will be available in this list. By clicking on one of the servers, the **IP** and **Port** field described above will be automatically filled in, and all that remains is to fill in the **Server Name** field to register.

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

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

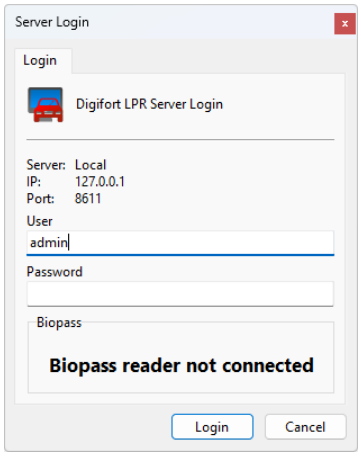


To change the parameters of an already saved server, right-click on the desired server and then click on **Change Parameters**. In the window that opens, change the data as necessary and click **OK**.

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

15.1.4 How To Connect To A Server For Management

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

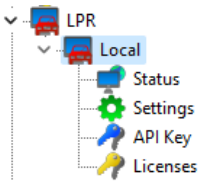


- **User:** Access user.
- **Password:** Access password.

Enter your username and password to access the server. If this is your first access to the system, enter the username **admin** and a blank password.

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

© 2002 - 2024 by Digifort. All rights reserved.



15.1.5 Licensing The LPR Server

The LPR server license works like the camera server, there is a "Base License" for the server and "Engine Licenses" for the engines.

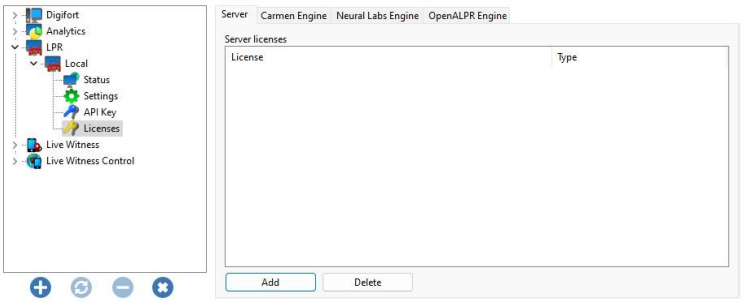
The LPR Base License is required to use the LPR server service.

Engine Licenses are necessary for the use of third-party engines and are generally installed using each engine manufacturer's own methods.

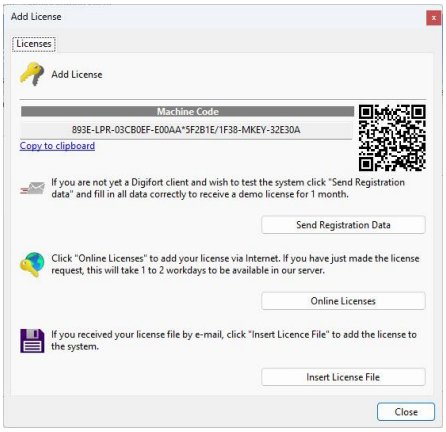
15.1.5.1 How To License The LPR Server

As previously stated, LPR will work with 2 types of license: the Base License and Engine Licenses.

The first step to licensing LPR is to add **Base Licenses**. Once connected, go to licenses as shown in the figure below:



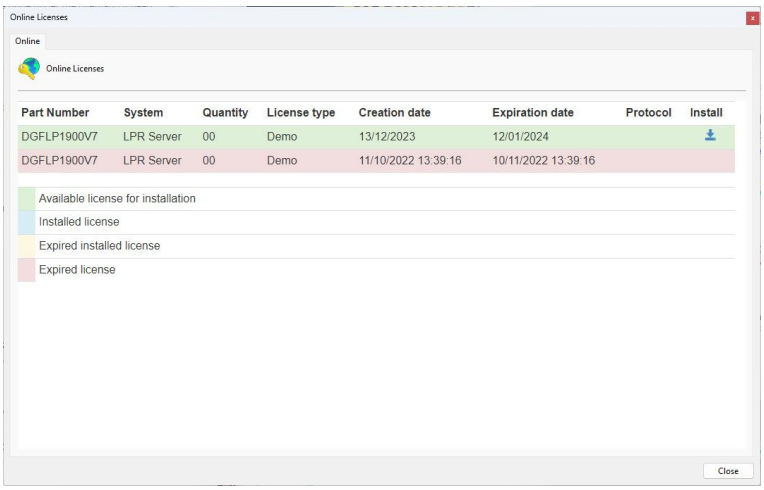
To add a license, click **Add**, and the following screen will be displayed:



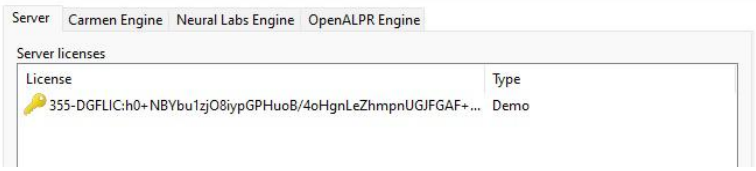
The process for adding licenses is the same as for VMS and is described in the chapter How to configure licenses.

© 2002 - 2024 by Digifort. All rights reserved.

On the online license screen, the license description should appear as **LPR Server** as shown in the figure below:



Click the button available in the install column of the corresponding license to install. After adding a license it will be available as shown in the figure below:



15.1.5.1.1 How To License Carmen Engine

To license **Carmen Engine**, simply have the engine Hardkey plugged in and the licenses are automatically recognized, as shown in the following image:

15.1.5.1.2 How To License Neural Labs Engine

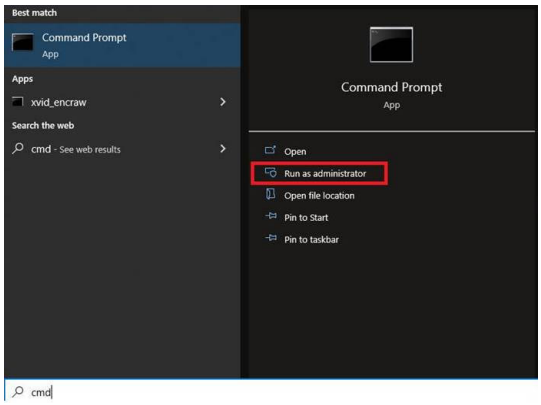
Neural Labs licensing is necessarily done offline, through .c2v and .v2c files. First you must generate the .c2v file that will contain server information, this file will be sent to Neural Labs, which will generate a .v2c license file that will be applied to the engine.

See the following topics for how to generate the .c2v request file and how to install the .v2c license file.

15.1.5.1.2.1 How To Extract The .c2v File To Request The License

Open **Command Prompt** with administrator rights (The process must be done with administrator rights, otherwise the generated file will be invalid):

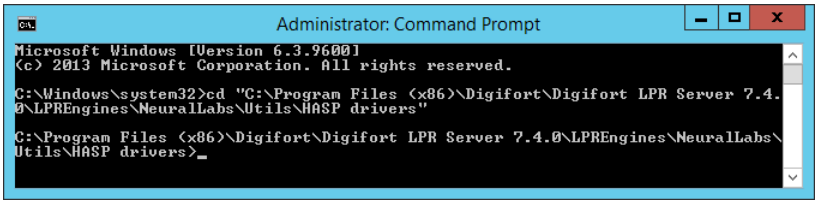
© 2002 - 2024 by Digifort. All rights reserved.



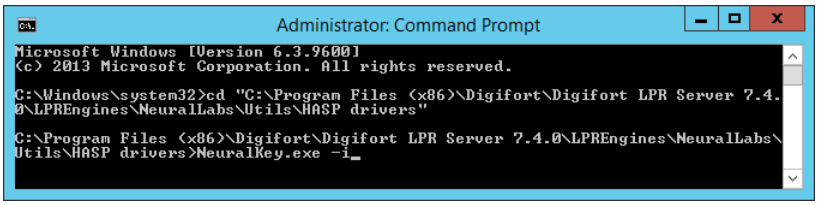
Go to the "neuralkey.exe" executable directory in the command prompt. "neuralkey.exe" is located within the "LPREngines\NeuralLabs\Utils\HASP drivers" subfolders that are located within the LPR server installation folder.

Writing the command cd <directory>, it usually looks similar to this:

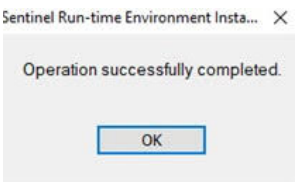
```
cd "C:\Program Files (x86)\Digifort\Digifort LPR Server 7.4.0\LPREngines\NeuralLabs\Utils\HASP dri
```



Now run the command `"Neuralkey.exe -i"`.

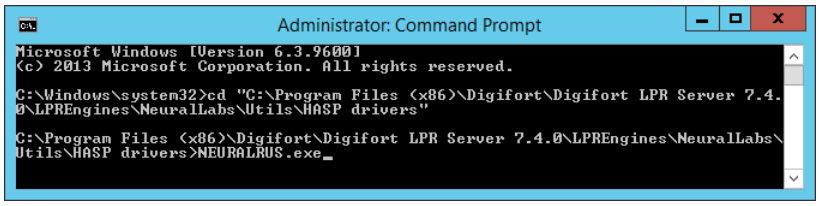


Wait for it to load and this message should appear:



Once this is done, open the "NEURALRUS.exe" application, which is located in the same directory:

© 2002 - 2024 by Digifort. All rights reserved.



The following application will be displayed:

In this same tab, if it is the first request, select the second option **Installation of new protection key** and then click on **Collect Information** and a **.c2v** file will be generated.

Save the c2v extension file and send it to our support team, along with the following completed questionnaire:

1. Project name or reference
2. Name of end or reference customer

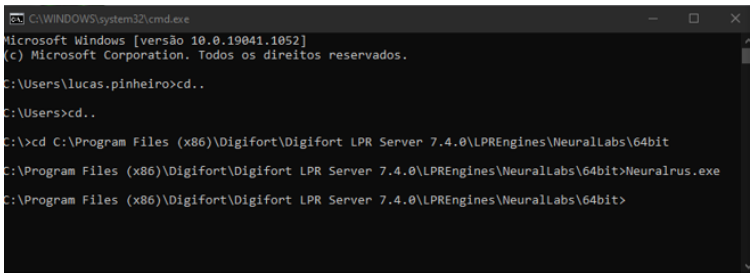
If this is a demo license request, please answer the following additional questions:

3. Countries - Target
4. Number of Cameras involved in this project
5. Number of Cores to License
6. Demo Time: 30 or 60 days
7. Will this be a demo extension (Yes / No)

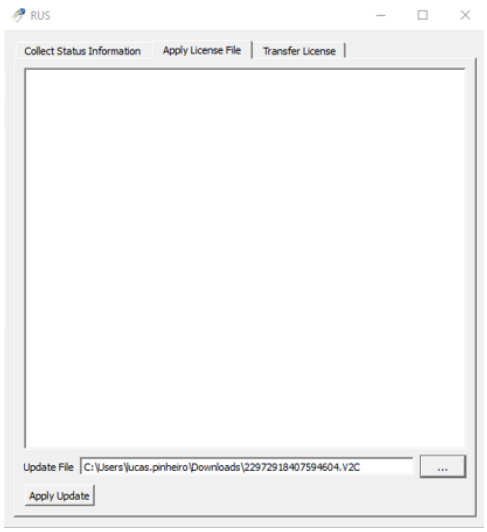
15.1.5.1.2.2 How To Apply The .v2c File To License The Engine

Para ativar o arquivo de licença Neural Labs, abra a aplicação **Neuralrus.exe** através do **Prompt de Comando** como administrador. O "Neuralrus.exe" está localizado dentro das subpastas "LPREngines\NeuralLabs\Utils\HASP drivers" que se encontram dentro da pasta de instalação do servidor de LPR:

© 2002 - 2024 by Digifort. All rights reserved.



No aplicativo que irá abrir, acesse a aba **Apply License File**, em Update File aponte o diretório com o arquivo de licença .v2c e clique em **Apply Update:**

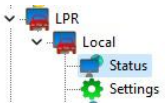


Restart the LPR server service, access the server through the Administration Client, enter the **Licenses** tab, and click on the **Neural Labs** tab. If the license was installed successfully, you will see the number of licensed cores. If the number of licensed cores is 0, then an error occurred while loading the license, in which case you should contact support.

15.1.6 LPR Server Status

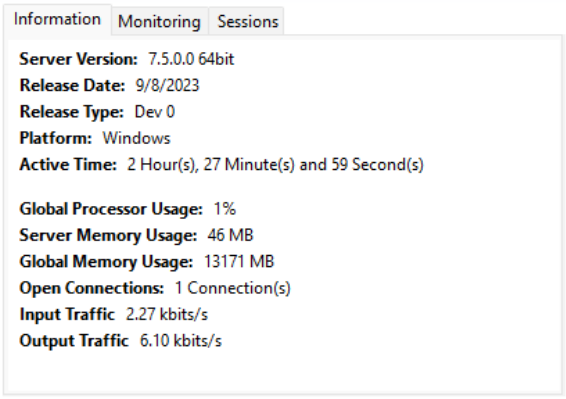
In this area of the system you can monitor how the server is performing, retrieving data such as processor usage, memory, network traffic, etc.

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



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

© 2002 - 2024 by Digifort. All rights reserved.

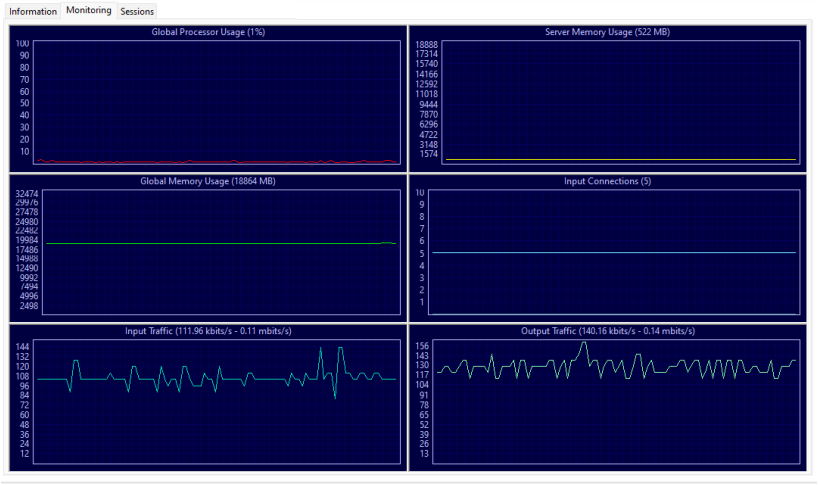


- **Server Version:** Displays the LPR Server version.
- **Release Date:** Displays the release date of this server version.
- **Release Type:** Displays the release type of this server version.
- **Platform:** Displays the platform of this server version.

- **Global Processor Usage:** Displays the global CPU usage of the server where the LPR process is running. This value represents the total usage by all Operating System processes and not just the LPR Server.
- **Server Memory Usage:** Displays the memory usage of the LPR Server process only.
- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Open Connections:** Number of open connections with the LPR Server.
- **Input Traffic:** Total data being sent to the LPR Server by the VMS Servers for processing.
- **Output Traffic:** Total data being sent from the LPR Server to the VMS Servers.

15.1.6.1 Monitoring

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



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

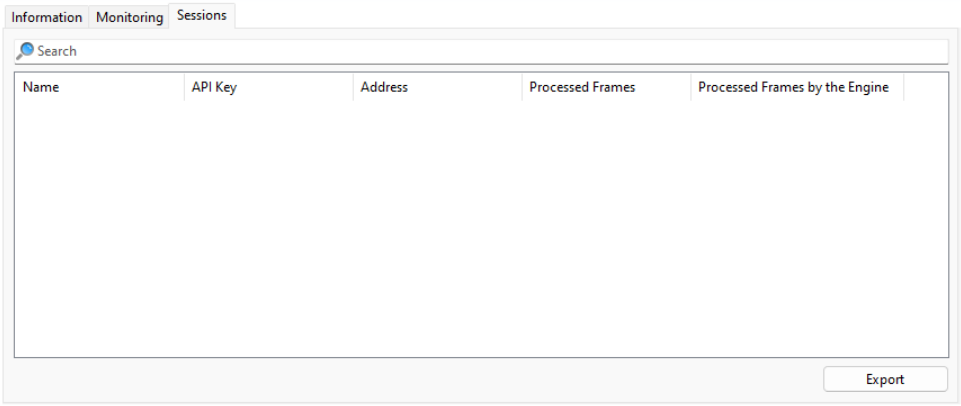
© 2002 - 2024 by Digifort. All rights reserved.

- **Open Connections:** Number of open connections with the LPR Server.
- **Input Traffic:** Total data being sent to the LPR Server by the VMS Servers for processing.
- **Output Traffic:** Total data being sent from the LPR Server to the VMS Servers.

15.1.6.2 Sessions

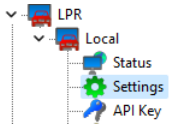
In the sessions tab you can check all LPR sessions currently running on the LPR Server. This screen will bring detailed information about the sessions such as the VMS server address, number of frames being processed, resolution, engine used, among other information.

Like other status and registration screens, this screen also has columns with extra information that can be added by right-clicking on the name of the columns in the list.

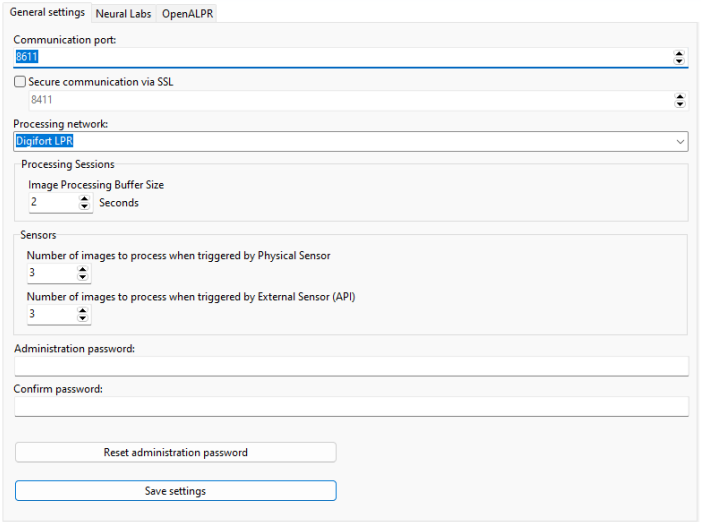


15.1.7 LPR Server Settings

To access the LPR server settings, click on Settings as shown in the image below:



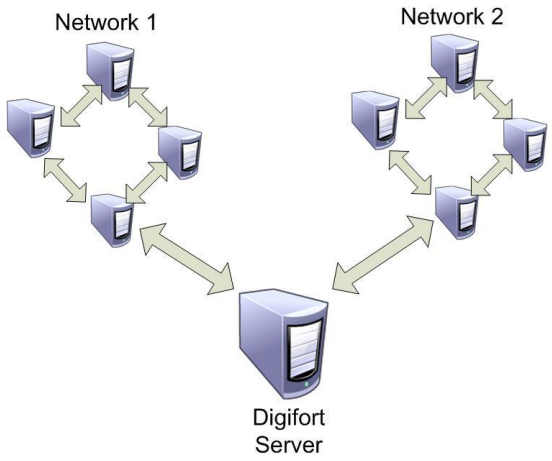
The settings screen will be displayed:



© 2002 - 2024 by Digifort. All rights reserved.

- **Communication Port:** Communication port with the LPR server. It is only recommended to change if this is already being used on the computer in question.
- **Secure Connection via SSL:** Enables secure connection to the server via SSL/TLS. To use SSL you must provide SSL certificates. See the SSL Certificates topic for more information.
  - **Port:** Specify the secure communication port

- **Processing Network:** Name of the distributed network in which this server will load balance. When more than one server has the same "Processing Network" name, processing will be balanced between them. To understand better, see the diagram below:



In the image above, the **VMS Server** sends images from the cameras to two different **Processing Networks**. This way, each group of computers balances the load only between **LPR Servers** that have the same network name.

- **Image Processing Buffer Size:** Specify a maximum size for the image buffer (no seconds) that is used to temporarily store images for processing. During peaks of high CPU usage, the system will use this buffer to prevent images from being lost due to lack of processing capacity, however if this buffer is very large and processing is heavily overloaded, the response latency will be greater (from according to buffer size).

- **Sensors:** Image processing settings when sensors (physical or API) are used.
  - **Number of images to process when triggered by physical sensor:** Choose the number of images that the system should process when a physical sensor (Associated Event in LPR Configuration) is triggered.
  - **Number of images to process when triggered by external sensor (API):** Choose the number of images that the system should process when an external sensor (API call for integration with third-party systems) is triggered.

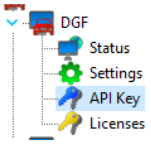
- **Administration Password:** Password to access the LPR server. Fill in this field to change the current password.
- **Confirm password:** Retype the password from the field above.
- **Reset Administration Password:** Returns the blank password.
- **Save settings:** Saves the changes made on this screen.

© 2002 - 2024 by Digifort. All rights reserved.

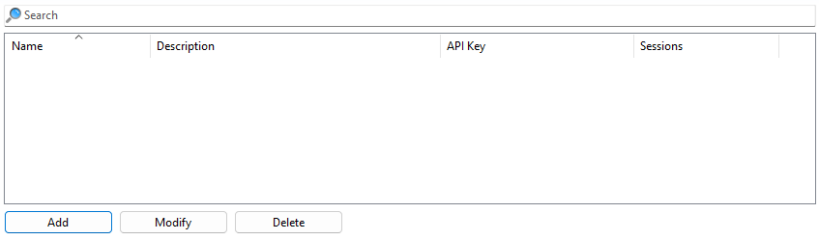
15.1.8 API Keys

The system allows the configuration of API Keys for the LPR Server, thus allowing VMS servers that are external to the LPR environment to use this server to perform image processing. This allows the system administrator to have more control in this type of scenario, being able to limit which engine can be used, the number of connections for each key, in addition to providing greater access security because when an API key is created , connections for processing on this server will only be accepted upon presentation of the key in the LPR Configurations.

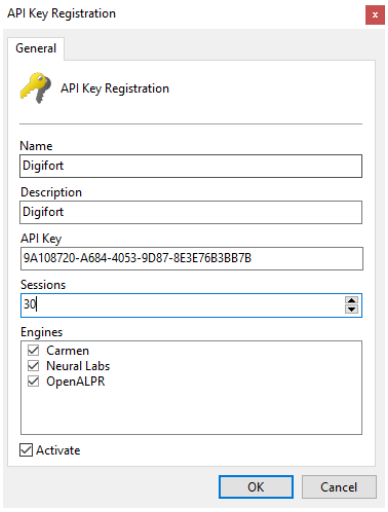
To add an API key, simply select the configuration in the LPR server menu:



The API key registration screen will be displayed:



When selecting this option, simply click the **Add** button to configure the desired key:



To change an already registered key, select it and click **Modify**, and change the data as explained on the following pages.
To remove a key, select the desired key and click the **Delete** button.

- **Nome:** Key name.
- **Description:** Key description.
- **API Key:** The automatically generated key that must be added in the LPR configuration.

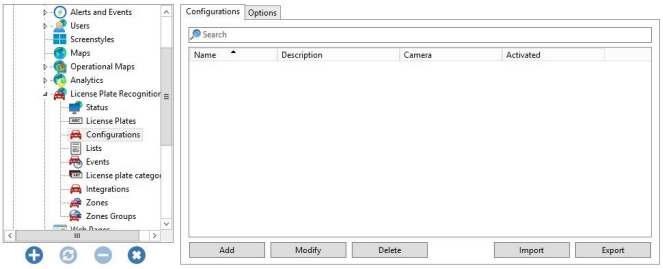
© 2002 - 2024 by Digifort. All rights reserved.

- **Sessions:** Number of configurations this key supports.
- **Engines:** Which engines can this key use?
- **Activate:** Enables or disables the API key.s

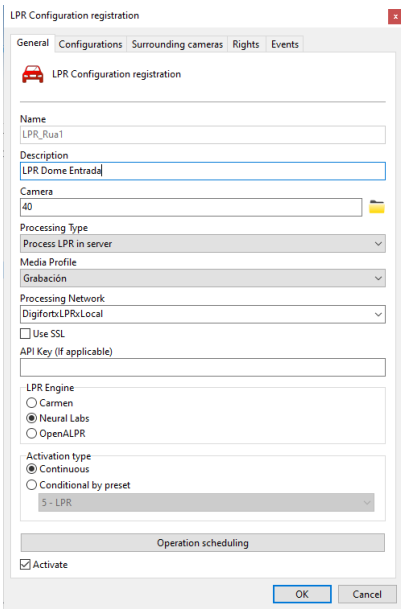
15.1.9 Adding an LPR Configuration

LPR Configurations are objects created on the VMS server to perform license plate recognition. Each LPR Configuration is associated with a camera and has options for processing images from this camera. You can create multiple LPR settings for the same camera, each with its own independent options.

After correctly licensing the LPR Server, you must add the **LPR Configurations** to the **VMS Server**. To do this, connect to the VMS Server and open the **Configurations** item within **License Plate Recognition**.



The **Settings** tab allows you to add a new **LPR Configuration**. To do this, click the **Add** button to start the LPR Configuration registration. The following screen will be displayed:



To change an already registered configuration, select it and click **Modify**, and change the data as explained on the following pages.
To remove a configuration, select the desired configuration and click the **Delete** button.

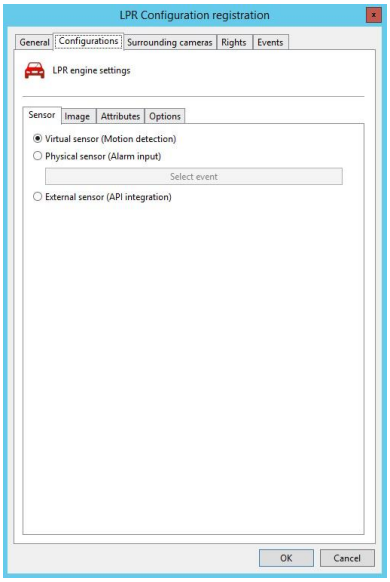
- **Name:** Desired LPR name
- **Description:** Description of the LPR registration for easy identification in the system.

© 2002 - 2024 by Digifort. All rights reserved.

- **Camera:** In this selection box, all cameras registered on the server will be available. License plate recognition will be done with images from the camera configured in this check box. To learn how to register cameras, see the chapter How to add a camera.
- **Processing Type**: Allows images to be processed in engines available locally on the LPR Server or on third-party servers. This option opens up the range of LPR integrations and allows future expansion of the system's base LPR system for powerful integrations with third-party systems.
- **Media Profile:** Select the media profile that is desired for analysis. Video analisis does not interfere with the quality/performance of the video that is transmitted and recorded.
- **Processing Network:** In this field, all **"Processing networks"** (LPR servers) active on the network will be available. Choose a network on which this configuration will be processed. It is possible to specify the server for processing by its IP, use the following format **"IP:<server_ip>"** or **"IP:<server_ip>:<port>"** in the field. Example: **IP:192.168.0.10** or **IP:192.168.0.10:8611**.
- **Use SSL:** Select this option to securely connect to the LPR Server for this configuration.
- **API Key:** This field must be filled in with the server's API key, if used.
- **LPR engine:** Choose the engine that will analyze the images.
- **Activation Type**
  - **Continuous**: Processes the image from a camera continuously.
  - **Conditional by Preset:** Activate the LPR Configuration conditionally by preset, so you could define a preset so that this setting is only active when the camera is positioned in the specified preset.
- **Operation Scheduling:** Allows you to schedule the operating hours of this LPR Configuration.
- **Activate:** Enables or disables the LPR configuration.

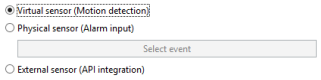
15.1.9.1 Engine Settings

After configuring the **General** options, click on the **Settings** tab to adjust parameters and options for the selected engine.



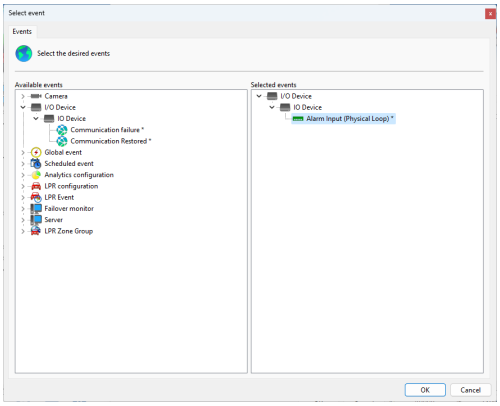
15.1.9.1.1 Sensor

Allows you to configure the type of sensor that will be used to detect the presence of a vehicle in the image and trigger license plate recognition.



© 2002 - 2024 by Digifort. All rights reserved.

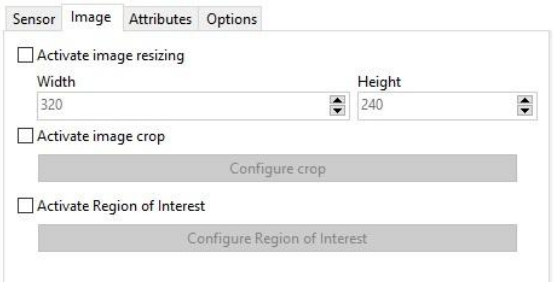
- **Virtual Sensor (Motion Detection):** Select this option (Default) to use motion detection to initiate license plate recognition.
- **Physical Sensor (Alarm Input):** Select this option to use a physical sensor through an alarm input, or any other system event to initiate license plate recognition.
  - **Select Event:** When the physical sensor option is selected, you must choose which events will initiate license plate recognition. Click this button and the event selection screen will be displayed, select the desired events available in the left column and drag and drop with the left mouse button in the right column:



- **External Sensor (Integration via API):** Select this option to use API integration to start license plate recognition. This option will generally be used in conjunction with integrated third-party systems.

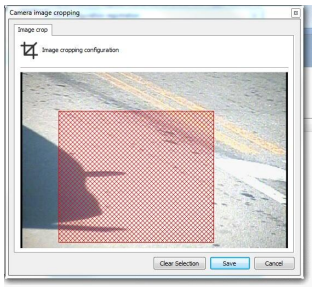
15.1.9.1.2 Image

Allows you to configure image pre-processing options.



- **Activate Image Resizing:** This option aims to modify the size of the image captured by the camera in order to save processing.
- **Activate Image Crop:** If this option is used, the system will crop the image according to the selection made, therefore, the resolution of the image sent to the engine will be lower than the original image, covering only the area of the selected image.
  - **Configure Crop:** Click this button to open the editor and select the cropping area. On the editor screen, click the left mouse button and drag over the desired area:

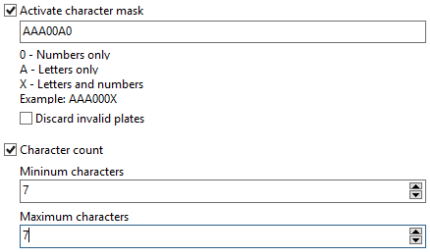
© 2002 - 2024 by Digifort. All rights reserved.



- **Activate Region of Interest:** This option (if the engine supports it) will instruct the engine to recognize license plates only in the selected region, however, unlike the crop option, the original image is used.
  - **Configure Region of Interest:** Click this button to open the editor and select the cropping area. On the editor screen, click with the left mouse button and drag over the desired area, as shown in the previous figure.

15.1.9.1.3 Attributes

Allows you to configure options with plate attribute filters:



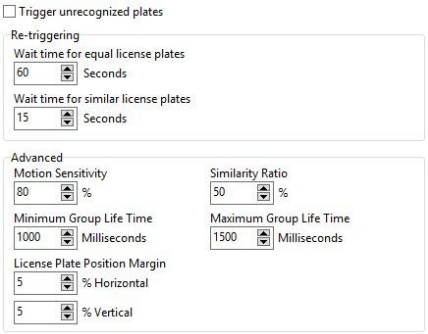
- **Enable Character Mask:** This option allows you to have more advanced control over what the software will identify on a board. The character **0** identifies only numbers, the **A** only letters and the **X** letters and numbers. If, for example, the desired plate capture standard is EGV1234 then the best filter to configure is AAA000.
  - **Discard invalid plates:** If this option is selected, the system will discard cards that do not satisfy the mask. If this option is disabled, the system will attempt to replace invalid characters.

- **Plate character count:** This option aims to configure a **Minimum** and **Maximum** number of characters to be identified by recognition, therefore, if a plate with fewer or more characters is recognized, it will be discarded from the results.

© 2002 - 2024 by Digifort. All rights reserved.

15.1.9.1.4 Options

Provides advanced processing options.



- **Triggering unrecognized plates:** This option only works for the physical or external sensor. If a license plate is not recognized after the sensor is triggered, the system will generate a record without a license plate.
- **Retriggering:** Provides options for retriggering control of cards that are recognized multiple times in a short period of time
  - **Waiting time for re-triggering of identical plates:** If the same plate is recognized in less than X seconds (configured) since its last capture, the system will ignore it and will not generate a new record.
  - **Waiting time for re-triggering similar plates:** If a very similar plate is recognized in less than X seconds (configured) since the last capture of the similar plate, the system will ignore it and will not generate a new record, avoiding false positives in the reading.
- **Advanced:** Advanced processing options.
  - **Motion Sensitivity:** How much movement the system must detect for it to take a reading. The **higher** this value, the **less** movement will be required for the trigger.
  - **Similarity Ratio:** How similar the plate must be (in %) for the system to consider the same reading as possible. For example, when several readings are made in sequence, the system evaluates the similarity between them and if they are within the configured %, it considers it a possible reading error, waiting for the closing time of the similarity group to display the best reading made.
  - **Minimum Group Lifetime:** Every recognized plate will create a temporary group that will contain all recognition records for this plate. Plates with very high similarity (previously configured) will be added to the same group as they may have been the result of an engine reading failure, different plates or those with low similarity will create their own groups. This option will determine the minimum lifetime of the group, that is, when a new plate is recognized, the group will be created and maintained for at least X milliseconds (configured), awaiting new readings in order to group the results into just one record and provide the record with better reading quality as a result. For example, if the LPR server is processing 30 frames per second from this camera, a group with a lifetime of at least 1 second will potentially contain 30 recognition records for the same license plate (1 for each frame if the license plate has been recognized in all frames), so it is possible to determine the best reading to offer the most accurate result. As this is a minimum value for the life of the group, the result will only be displayed after closing the group, that is, if this configured value is too high, you may experience latency in the recognition response, where, for example, a group configured with minimum lifetime of 5 seconds (5,000 milliseconds) will have a latency of at least 5 seconds between the vehicle passing through the image and the response with the reading result. The group will remain open for the specified time even if the system is no longer recognizing the plate in this group and as explained, this will be the minimum response latency time (Not counting the LPR Bridge processing time for integrations with external systems).
  - **Maximum Group Lifetime:** This value determines the maximum time that a group can remain open waiting for new readings from a plate to determine the best reading for the result. While the

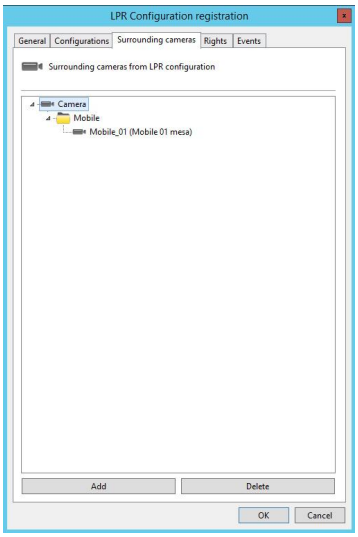
© 2002 - 2024 by Digifort. All rights reserved.

minimum group time determines the minimum time that the group will be open waiting for readings from a card, the maximum value will be used if the card continues to be read after the minimum time, that is, if you keep a very high maximum value and the plate is no longer present in the image after the minimum time, the group will be closed, however, if after the minimum time the plate still remains in the scene, the group will continue to be open, receiving new records, until the maximum configured time is reached , where the result will be presented regardless of whether the card is still in the scene, therefore, this will be the maximum latency time of the reading response (Not counting the LPR Bridge processing time for integrations with external systems).

- **License Plate Position Margin:** Determines a border (in %) around the image where if a plate recognized within this border will be discarded from the result. This configuration is necessary to avoid partial plate captures, where part of the plate may still be outside the image.

15.1.9.2 Surrounding Cameras

In the **Surrounding Cameras** tab, you can enter the cameras that are close to the main camera for LPR. With this, the user will be able to have results and reports containing the images from the surrounding cameras when the license plate was captured, along with the image from the main camera.



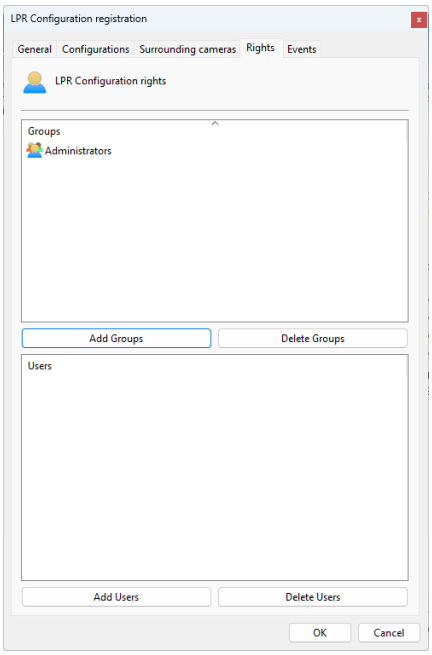
Click **Add** to associate the desired cameras and the standard object selection screen will be displayed, select the desired cameras and click OK.

Click **Delete** to delete associated cameras.

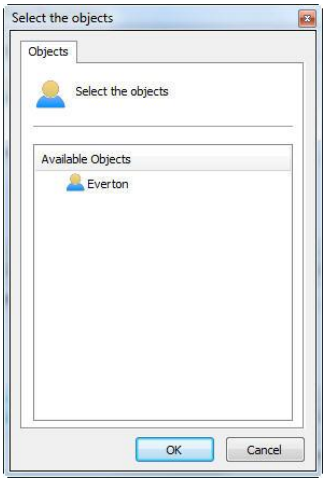
15.1.9.3 Rights

On the **Rights** tab you can define the list of users and user groups that will have the right to view this configuration in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

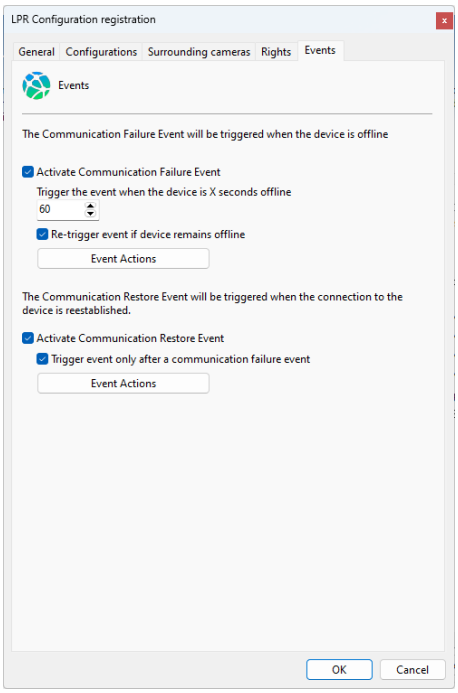


Select the available User and click **OK**. The same rule applies to the group list.

15.1.9.4 Events

In the events tab, it is possible to configure the Communication Failure or Communication Restoration events for the LPR Configuration, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.



15.1.9.4.1 Communication Failure

The **Communication Failure** event consists of checking how long the configuration has been out of operation, therefore the system will only generate the communication failure event if the configuration remains out of operation for more than X seconds.

The system still allows the event to continue firing every X seconds while the configuration is not working, if the option is disabled the system will generate the event only once.

To learn how to configure event actions see How to configure event actions.

15.1.9.4.2 Communication Restore

The **Communication Restore** event consists of generating an event when the configuration starts working again on the system.

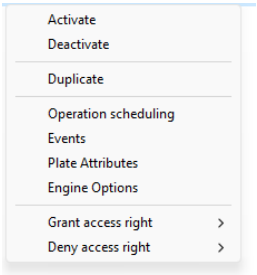
The system also allows events to only be triggered if a **Communication Failure** event for the same object has been triggered previously.

To learn how to configure event actions see How to configure event actions.

15.1.9.5 How To Change Multiple LPR Parameters Simultaneously

The system's LPR configuration manager provides quick access to the most common settings that can be changed for multiple configurations simultaneously. In the LPR settings register, select the desired settings and right-click. A menu will open as shown in the figure below:

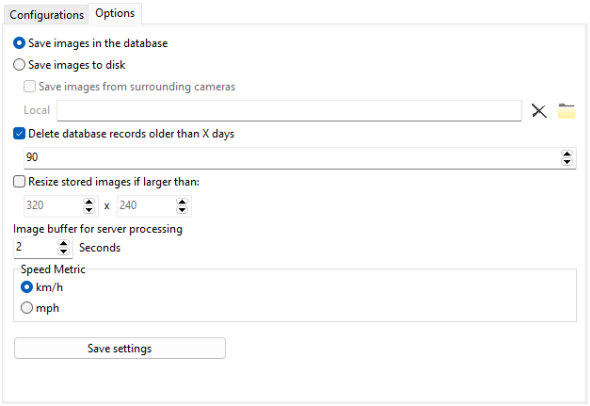
© 2002 - 2024 by Digifort. All rights reserved.



Most of the options you can change are self-explanatory and you can refer to the LPR Configurations Registration topic to learn more about each option.

15.1.10 General Options

In the **Options** tab we will have several general options applied to all LPR Settings:



- **Save images to the database:** LPR saves the images of recognized license plates on the server. With this option, the images will be kept in the system database (Not recommended for environments with many records as it will overload the database file).
- **Save images to disk:** Images associated with LPR records will be stored in a configured folder on disk (Recommended).
  - **Save images from surrounding cameras:** Select this option to also store images from surrounding cameras on disk.
    - By default, images from surrounding cameras are consulted in the camera recordings, however, in some cases it is necessary to keep these records for 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 the database.

- **Delete LPR records older than X days**: Deletes LPR records that have been stored for more than the configured X days.
- **Resize stored images if larger than**: Record images are stored in the original captured resolution by default, however, to save disk space (If the original image is of high resolution), you can activate this option and the system will resize the images to a maximum resolution. Activating this option will not resize images already recorded from previous records and will only affect new records.
- **Image buffer size for server processing:** Allows you to configure the image buffer size for processing. This buffer is used when the LPR Server is overloaded (which can occur when image recognition from several cameras is activated simultaneously), then the system will temporarily store the images in memory (before discarding) for a few seconds in order to wait the LPR Server responds to image processing. A high buffer value can improve processing and recognition results as otherwise

© 2002 - 2024 by Digifort. All rights reserved.

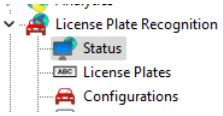
the images would be discarded if the LPR Server was overloaded, however, it could also increase the recognition response time.

- **Speed Metric**: Some cameras can return the speed at which the vehicle passed the camera along with the license plate. In these cases, you must choose which speed metric the system will use: **km/h** or **mph**.

15.1.11 Checking the Status of LPR Configurations

In this area of the system you can monitor the status of LPR Configurations with detailed information about their current operation.

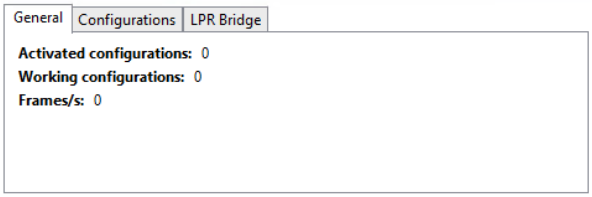
To access this feature, open the **LPR Configurations** item in the **Settings Menu** and click on the **Status** item, as shown in the figure below:



This screen is made up of 3 tabs: **General**, **Settings** and **LPR Bridge**.

15.1.11.1 General

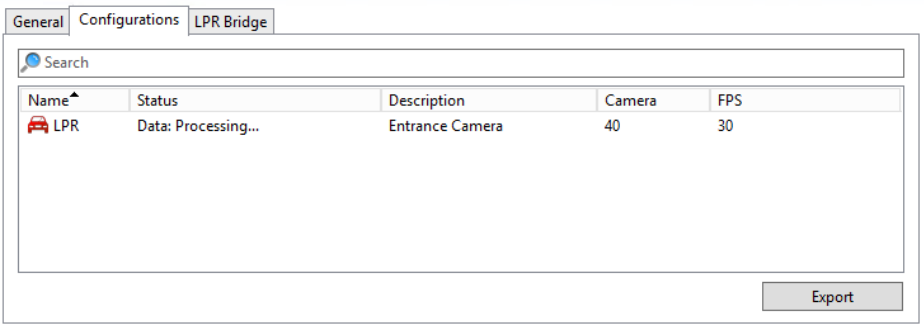
The **General** tab will provide a summary of the currently active settings.



- **Active Configurations:** LPR Configurations currently active.
- **Working Configurations:** Working LPR Configurations.
- **Frames/s:** Number of frames processed.

15.1.11.2 Configurations

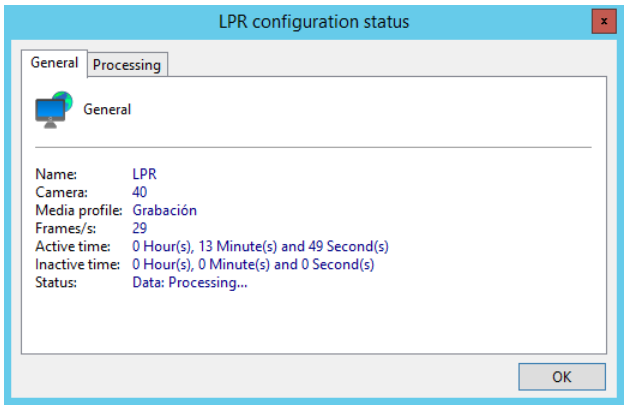
The **Configurations** tab provides details about active configurations.



In this list you can check the current status of the activated settings and you can add columns with extra information by right-clicking on a column and selecting the **Select Columns** option.

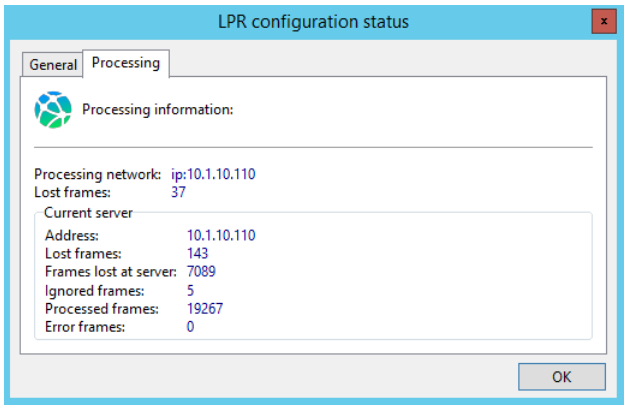
By double-clicking on a setting, you will have detailed information about how it works:

© 2002 - 2024 by Digifort. All rights reserved.



In the **General** tab you will have general configuration information:

- **Name:** Active configuration name
- **Camera:** Name of the camera that the engine is processing.
- **Media Profile:** Media Profile used in processing.
- **Frames/s:** Number of frames received from the camera.
- **Active Time:** Time the configurations has been active to date.
- **Idle Time:** Time the configuration has been inactive so far.
- **Status:** Active configuration status.



In the **Processing** tab you will have information about processing:

- **Processing Network:** Processing network name
- **Lost Frames:** Frames lost on the server. This is the total number of frames that were received from the camera but were not sent to the LPR server due to a connection error or LPR server unavailability.

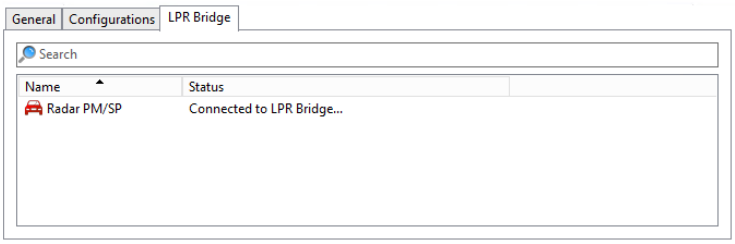
Current server: Provides information about the current session with the LPR Server.

- **Address:** Address of the LPR Server where the configuration is being processed.
- **Lost frames:** Number of frames that were received from the camera but were not sent to this LPR Server due to server overload.
- **Frames lost on the server:** Frames that were sent to the LPR Server but discarded on the server due to processing errors or LPR Server overload.
- **Ignored Frames:** Number of frames dropped on the server before opening a session (Frames used to start the LPR session).
- **Frames processed:** Total Frames Processed.
- **Frames with errors:** Total frames that were not processed due to errors on the LPR Server.

© 2002 - 2024 by Digifort. All rights reserved.

15.1.11.3 LPR Bridge

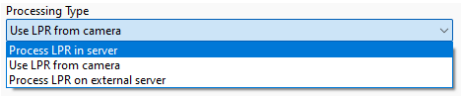
The LPR Bridge tab will display the status of active LPR Bridge Services. LPR Bridge is software used to integrate the LPR system with third-party systems or databases. To learn how to configure the LPR Bridge, consult its manual.



On this screen you will have a list of currently configured and active services and their status.

15.2 Edge LPR

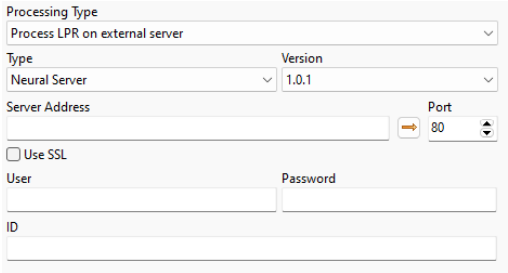
The system allows the use of LPR embedded in cameras or LPR being processed on third-party servers instead of processing on the system's local LPR server. To use this option you must select the LPR Configuration Processing Type:



As LPR Configurations have already been discussed previously, to learn how to add an LPR Configuration, see the topic Adding an LPR Configuration.

- **Use LPR on Camera:** If the selected camera has built-in LPR and it is supported by the system, this option will be available. Select this option to use the camera's built-in LPR.

- **Process on External LPR Server:** Select this option to use integration with third-party LPR software (and servers). If this option is selected, the configuration screen below will be displayed:



  - **Type:** Select the external server type (Supported Software).
  - **Version:** Select the compatible version of the external server.
  - **Server address:** Enter the external server address.
  - **Port:** Enter the communication port of the external server.
  - **Use SSL:** Select for secure communication with the server (If it supports it).
  - **User:** User for server authentication.
  - **Password:** Password for server authentication.

© 2002 - 2024 by Digifort. All rights reserved.

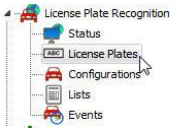
- **ID:** String with camera ID or additional server parameters. See the external server integration technical document for more information.

In both options, the configuration of the LPR will be done externally to the system (Directly on the camera or directly on the external server being integrated) and the system will only receive metadata and events from the device, therefore the **Engine Settings** tab will not be available.

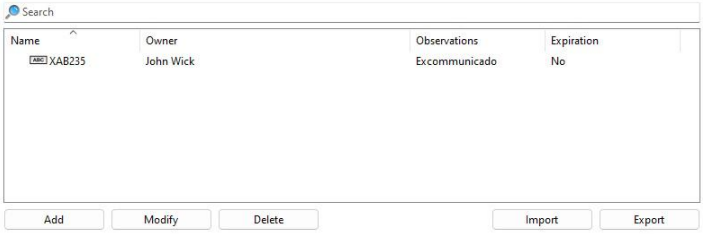
15.3 License Plates

The system has a built-in license plate registry that can be used to identify pre-registered vehicles and drivers, as well as being added to license plate lists to be used in LPR events, which in turn can trigger actions such as automatically opening a gate when a certain license plate is recognized or even trigger an alarm if a stolen vehicle is recognized.

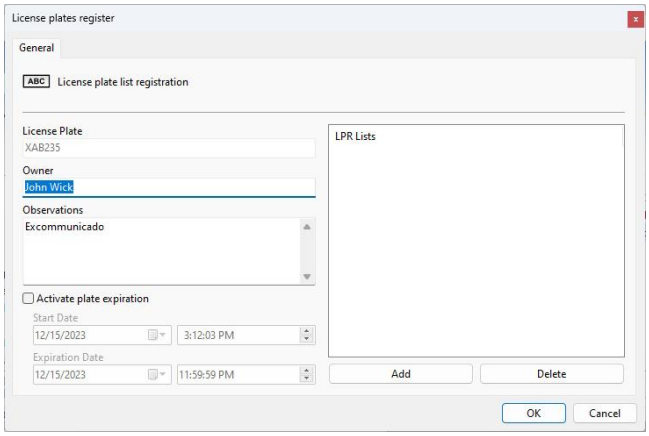
To access the license plate registration, open the **License Plate Recognition** item in the **Settings Menu** and click on the **License Plates** item as shown in the image below:



The registration screen below will be displayed:



To register a plate, simply click on the **Add** button and the registration screen will be displayed:



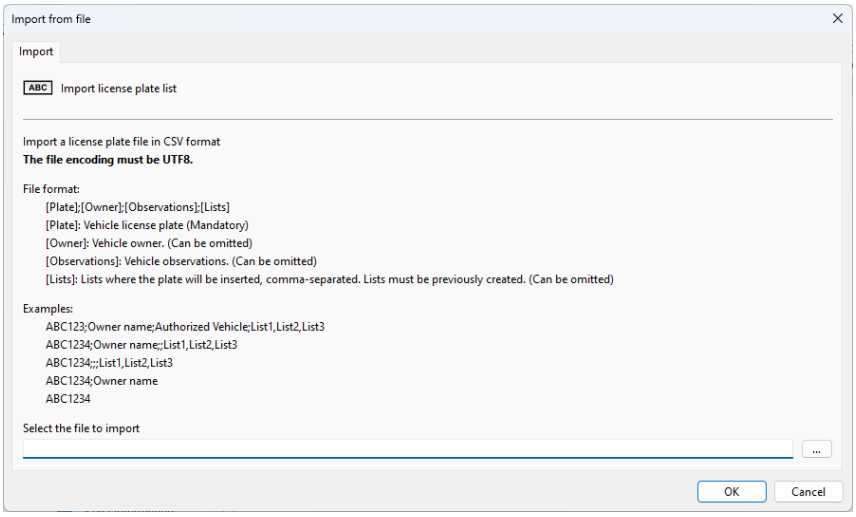
To change an already registered license plate, select it and click **Modify**, and change the data as explained on the following pages.
To remove a plate, select the desired configuration and click the **Delete** button.

© 2002 - 2024 by Digifort. All rights reserved.

- **Plate**: Plate number.
- **Owner**: Information about the owner (Non-Mandatory Field).
- **Observations**: Notes on the plate.
- **Activate plate expiration:** Allows you to choose the registration validity period for this card, which can be used as parameters in LPR events, where it is possible to configure that an event will only be triggered if the recognized card is within the validity period.
- **List**: Select the lists this card belongs to. See about lists in the next topic of this manual.
  - **Add:** Open the list selection screen
  - **Delete:** Remove selected lists

On the main registration screen, it is also possible to import and export plates in files with a .csv extension. Just click **Import / Export**.

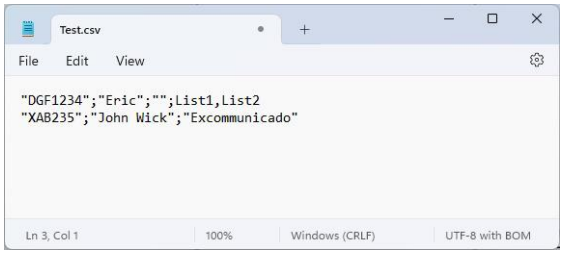
Importing boards from CSV files requires a specific format:



Important

The file must be in CSV format with a semicolon as the delimiter ";" of columns. The column delimiter for lists (last column in the file) will be the comma ",".

Below is an example of the file format for importing 2 boards:



In the example above, see that the first **DGF1234** board has no observations, but the field is still delimited, and this record is part of the lists **List1** and **List2** (separated by a comma). On the second plate **XAB235**, the observations field is filled in and this record is not part of any list.

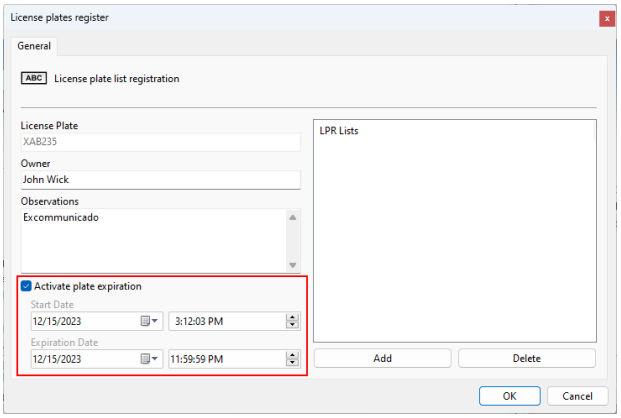
© 2002 - 2024 by Digifort. All rights reserved.

15.3.1 Registration Expiration

It is possible to set an expiration date for plates registered in the LPR system.

The expiration of plates is used through LPR Events and is very useful for scenarios where, for example, an expired plate cannot open a gate associated with the event, therefore it is possible to create temporary plates that will have access to the location.

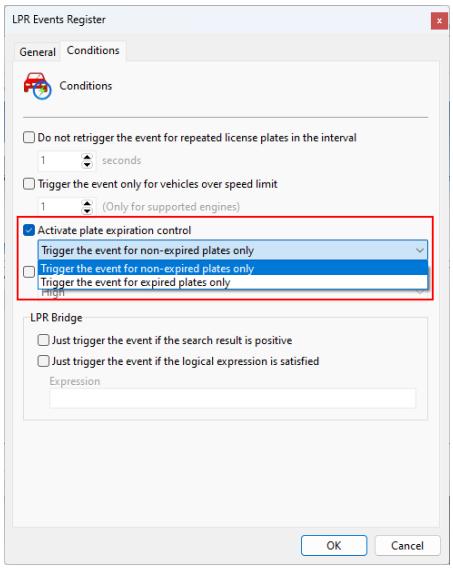
It is possible to define a start date (When the license plate will be valid) and an expiration date through the license plate registration:



LPR events can be conditioned to fire using plate expiration control.

You can configure an LPR Event to fire only if:

- **The recognized license plate is not expired:** This option is useful for creating access control to a location, where the system will only automatically open a gate for license plates that are not expired.
- **The recognized license plate is expired:** This option is useful for creating alarm events if a vehicle with an expired license plate is recognized, in this case, the operator can receive an alarm popup to inform about the condition of the vehicle.



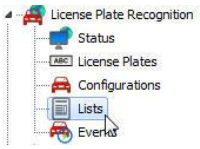
© 2002 - 2024 by Digifort. All rights reserved.

To learn more about events see the LPR Events topic.

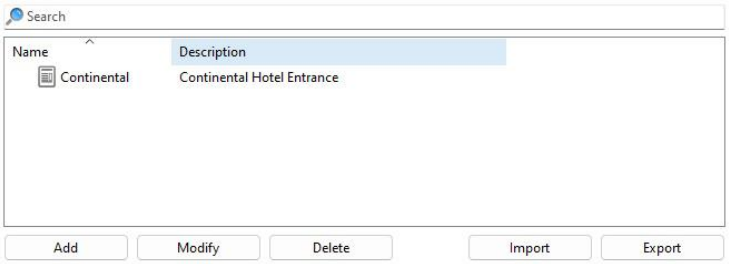
15.4 Configuring LPR lists

Plate lists allow the categorization of registered plates, as well as being used to trigger conditional events, for example, a plate can be inserted in a list that will give the vehicle access to entrance 1 and also in another list that will give access to the entrance 2 of a company. Each of the lists can relate to different events in the system. Lists can also be used to trigger alarms (such as popups, triggering I/Os, push notifications, etc.) functioning, for example, as a black list, where the operator can receive an alert when a specific vehicle is recognized.

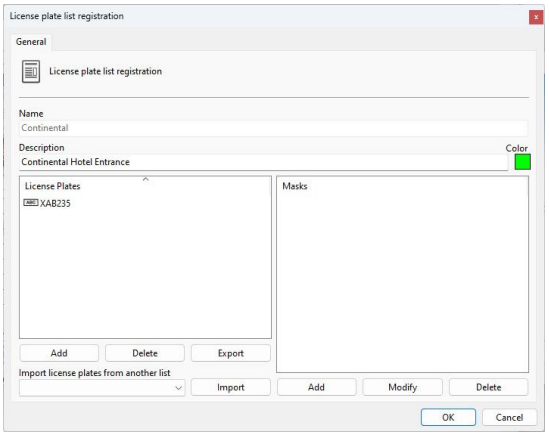
To access the license plate registration, open the **License Plate Recognition** item in the **Settings Menu** and click on the **Lists** item as shown in the image below:



The registration screen below will be displayed:



To register a list, simply click on the **Add** button and the registration screen will be displayed:



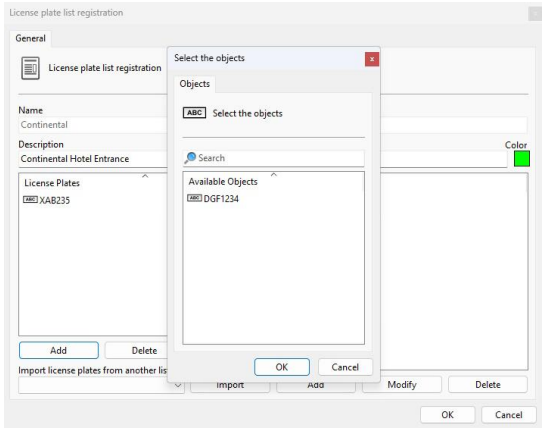
To change an already registered list, select it and click **Modify**, and change the data as explained on the following pages.
To remove a list, select the desired configuration and click the **Delete** button.

- **Name:** Name given to the list. Example: Gate 1, Unauthorized Vehicles.
- **Description:** Desired description of the list for better identification in the system.

© 2002 - 2024 by Digifort. All rights reserved.

- **Color:** Color that will be associated with this list. This color will be visually displayed in the Surveillance Client when a plate from the list is recognized.
- **Plates:** Plates associated with this list. These plates are added from the registration of plates already created. See the previous topic of this manual.
- **Masks**: The purpose of the masks is to consider all plates that satisfy the mask syntax as part of the list, at the time of recognition. See examples in the next topic.
- **Import plates from another list**: To facilitate registration, it is possible to import license plates already registered in another list. To do this, select the source list and click **Import**.

To add a plate to the list, simply click on **Add** and a window will appear with the available plates that have been pre-registered:



Select the desired cards and click **OK**.

It is also possible to delete plates from the list using the **Delete** button or export them to a text file. To export, simply click **Export** and select the directory to save the text file.

15.4.1 Masks

The purpose of the masks is to consider all plates that satisfy the mask syntax as part of the list, at the time of recognition, even if they are not registered in the system:

- The mask consists of character literals, sets, and wildcards.
- Each literal character must match a single character in the string. Comparison of literal characters is **case-insensitive**.
- Each set begins with an opening bracket ([) and ends with a closing bracket (]). Between the brackets are the elements of the set. Each element is a literal character or range.
- Ranges are specified using a start value, a hyphen (-), and an end value. Do not use spaces or commas to separate the elements of the set.
- A set must match a single character in the string.
- Characters match the set if it is the same as some literal character in the set, or if it is in one of the ranges in the set.
- A character is in a range if it matches the start value, end value, or is in between the two values.
- If the first character after the opening bracket of a set is an exclamation mark (!), then the set will match any character that is not in the set (Negation).
- Wildcards are asterisks (*) or question marks (?). An asterisk matches any number of characters and any character. A question mark matches any single character.

Examples:

© 2002 - 2024 by Digifort. All rights reserved.

Mask: ABC*
Result: Returns all records that begin with ABC
Examples: ABCD, ABC123, ABCXYZ

Mask: ABC*123
Result: Returns all records that start with ABC and end with 123
Examples: ABCD123, ABC123, ABCXYZ123

Mask: ABC?123
Result: Returns all records that start with ABC, have any character and end with 123
Examples: ABCD123, ABCX123, ABCY123

Mask: ABC??23
Result: Returns all records that start with ABC, have any two characters and end with 23
Examples: ABCD123, ABCXR23, ABCY923

Mask: ABC[XYZ]123
Result: Returns all records that start with ABC, have a character from the set (X, Y or Z) and end with 123
Examples: ABCX123, ABCY123, ABCZ123

Máscara: ABC[!XYZ]123
Result: Returns all records that begin with ABC, have a character outside the set (other than X, Y or Z) and end with 123
Examples: ABCD123, ABCE123, ABCF123

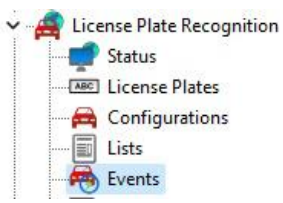
Mask: ABC[D-G1-3]
Result: Returns all records that start with ABC and have a character from the sets (D to G) or (1 to 3)
Examples: ABCD, ABC3, ABCF

Mask: ABC[D-G1-3]??[!ABC1-3]XYZ*
Result: Returns all records that begin with ABC, have a character from the sets (D to G) or (1 to 3), have any two characters, have a character outside the set (other than ABC and outside the range 1 to 3), have the literal characters XYZ and end with any character string
Examples: ABCD12UXYZ, ABC2Y1UXYZ12345: ABC*

15.5 Events

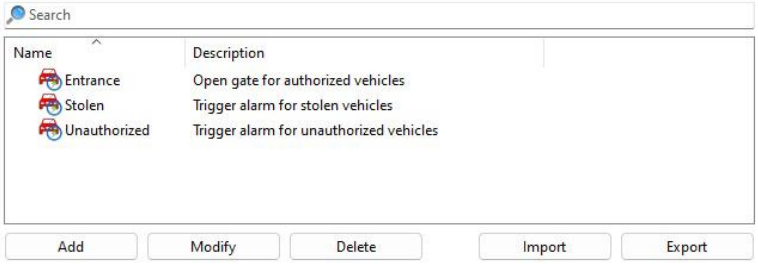
The system allows the creation of events that can be triggered when a specific plate is recognized in the system. These events allow you to create complex alarm or automation scenarios.

To access the event registration, open the **License Plate Recognition** item in the **Settings Menu** and click on the **Events** item as shown in the image below:

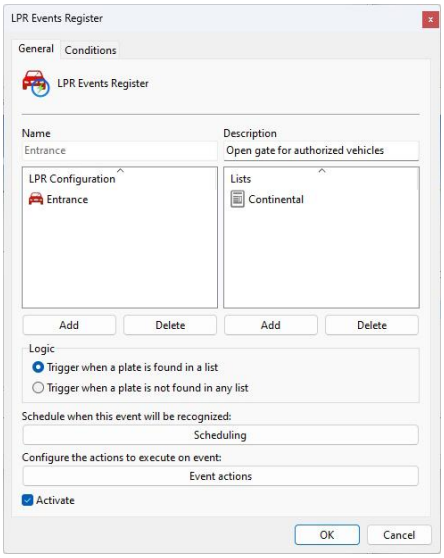


The registration screen below will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



To create a new Event click **Add**. The following screen will be displayed:



To change an event already registered, select it and click **Modify**, and change the data as explained on the following pages.
To remove an event, select the desired event and click the **Delete** button.

On this screen we must associate the license plate lists that we want to trigger an event, such as **Stolen Cars** and associate them with one or more LPR configurations. When a recognized plate in one of the associated configurations meets the event conditions, then this event will be triggered.

- **LPR Configurations:** List of configurations associated with this event. Only plates read from these configurations will be used in the event.
- **Lists:** Lists of plates associated with this event. For the event to be triggered, the plate must belong to one or more associated lists, or belong to none, depending on the configuration of the event logic.
- **Logic:** Specifies the logic for using lists for this event.
  - **Trigger when a plate is found in a list:** Fires the event only if the plate recognized by one of the associated LPR configurations belongs to at least one associated list.
  - **Trigger when a card is not found in a list:** Fires the event only if the plate recognized by one of the associated LPR configurations does not belong to any associated list.
- **Scheduling:** Allows you to schedule when this event can be triggered. When you click this button, the system's default scheduling screen will be displayed. The functionalities of this screen have already been discussed in previous topics in the manual.
- **Event Actions:** Desired event actions when this event is fired. To learn more about event actions, see the chapter How to configure event actions.

© 2002 - 2024 by Digifort. All rights reserved.

- **Activate:** Activates or deactivates this event.

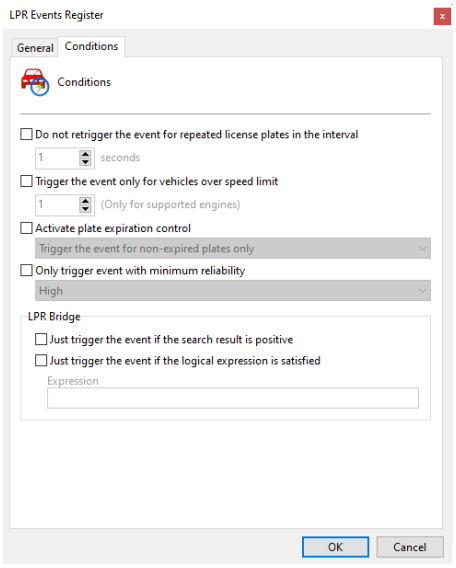
15.5.1 Conditions

LPR Events support multiple trigger conditions.

Using trigger conditions it is possible to restrict when an LPR event will be triggered, offering great configuration flexibility.

Important

The conditions selected on this screen are aggregated, that is, all selected conditions must be satisfied for the event to be triggered.



- **Do not retrigger the event for repeated license plates in the interval:** This option prevents the system from triggering the LPR event if the same plate is recognized within a configured time interval.
- **Trigger the event only for vehicles above speed limit:** This option will cause the event to only be triggered if the vehicle is traveling above the defined speed. This condition will only work for cameras or engines that support speed detection.
- **Activate plate expiration control:** This option allows triggering the event to be conditioned on the expiration of the plates.
  - **The recognized license plate is not expired:** Triggers the event only if the recognized plate is not expired.
  - **The recognized license plate is expired:** Triggers the event only if the recognized plate is expired.
- **Only trigger event with minimum reliability:** This option prevents the system from triggering the LPR event if the license plate recognition result does not reach a minimum level of reliability.

- **Integration via LPR Bridge:** Allows you to condition the triggering of the event according to the response from the LPR Bridge. To learn more about this module, see the topic on Integrations with LPR.
  - **Only trigger the event if the search result is positive:** This option prevents the system from triggering the event if the external system does not return results when searching for the plate, and can be used to consult lists in external databases, for example.
  - **Only trigger the event if the logical expression is satisfied:** This option allows a logical expression to be entered so that the system only filters for events that return this expression. An

© 2002 - 2024 by Digifort. All rights reserved.

example would be the expression `incident_type = "OWNER WANTED"` where the system would only trigger the event if the "incident_type" field has the value "OWNER WANTED". You can use the name of the fields returned by LPR Bridge and compare their values with logical expressions. Supported operators:

- `+`
- `-`
- `/`
- `*`
- `=`
- `>=`
- `<=`
- `%` (mod)
- `IN` (Value in an array of values. Array is supported with [])
- `AND`
- `OR`
- `XOR`
- `NOT`
- `LIKE`

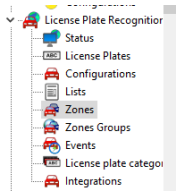
15.6 LPR Zones

The system allows the creation of **LPR Zones** that can be used for more advanced concepts such as occupancy rate of premises monitored by the system. A zone has **Entry** and **Exit** LPR Configurations. Vehicles recognized by the configurations associated with the zone entry will be added within the zone, as well as vehicles recognized by the zone exit configurations will be removed from the zone.

The LPR Zone object in the Surveillance Client will display the number of vehicles within the zone, as well as the number of entries and exits for the day, average occupancy rate and the list of all vehicles currently within the zone:

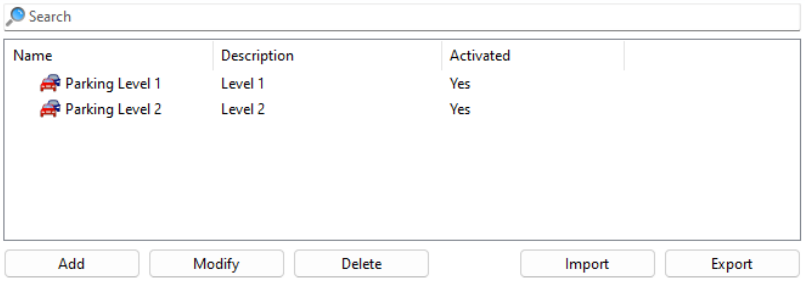
The system also has reports and searches for entry and exit records in zones. For more information on the operation of this feature, see the Surveillance Client manual.

To access the Zones register, open the **License Plate Recognition** item in the **Settings Menu** and click on the **Zones** item as shown in the image below:

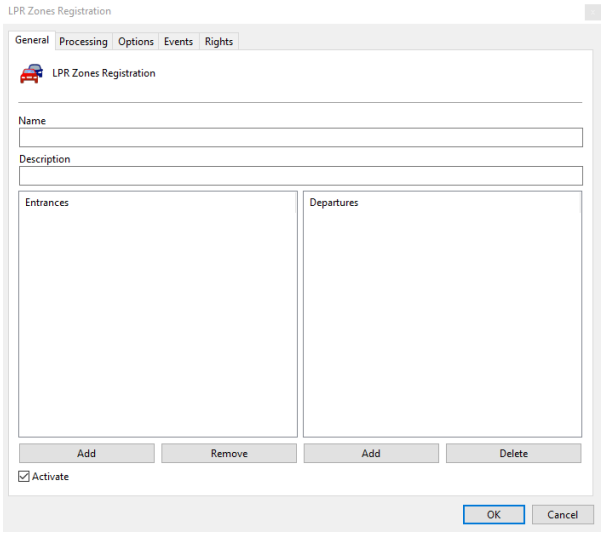


Once selected, the system will display the zone registration screen:

© 2002 - 2024 by Digifort. All rights reserved.



When clicking on the **Add** button, the system will display the following screen:



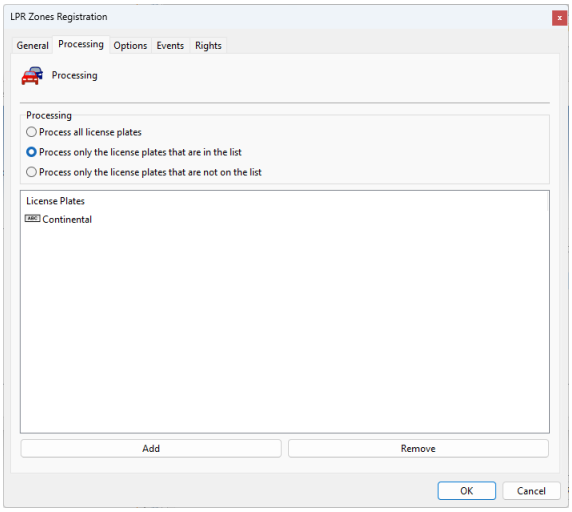
To change an already registered zone, select it and click **Modify**, and change the data as explained on the following pages.
To remove a zone, select the desired configuration and click the **Delete** button.

- **Name:** Name of the Zone to be added.
- **Description:** Description of the Zone to be added.
- **Entrances:** LPR Configurations that should be considered as inputs (increase in the number of vehicles within the zone).
- **Departures:** LPR Configurations that should be considered as exits (reduce the number of vehicles within that zone),
- **Activated:** Determines whether this Zone will be activated.

15.6.1 Processing

You can configure LPR zones to only consider plates that satisfy the configured processing logic.
Navigating to the **Processing** tab, the system will have the following screen:

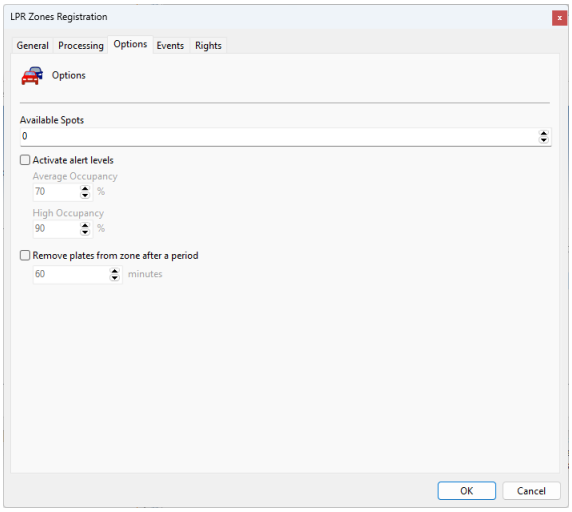
© 2002 - 2024 by Digifort. All rights reserved.



- **Process all license plates**: This option will make the system consider all captured license plates.
- **Process only license plates belonging to the lists**: This option will make the system only consider plates that are in one of the selected lists.
- **Process only license plates that do not belong to the lists**: This option will cause the system to ignore plates belonging to the selected lists.

15.6.2 Options

When selecting the **Options** tab we get the following screen:



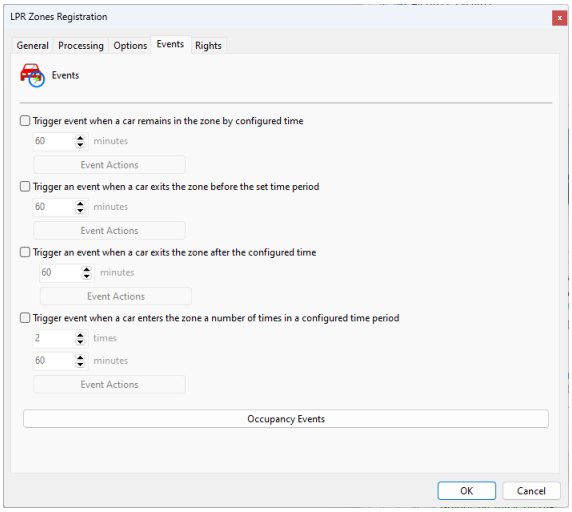
- **Available Spots**: The total number of spots available in a given zone. This number is only used for the visual representation of the vehicle count in the area through visual alerts, where low occupancy will be displayed in green, medium occupancy in yellow and high occupancy in red (Defined through the alert levels below).
- **Alert Levels**: This option will cause the system to consider values such as average occupancy (making the indicator on the Surveillance Client yellow) and high occupancy (making the indicator on the Surveillance Client red), also being used to activate LPR zone events.

© 2002 - 2024 by Digifort. All rights reserved.

- **Remove plates from the zone after a certain period**: This option will cause the system to automatically remove license plates from this zone after X minutes of entry, even without this vehicle being recognized in the exit configurations.

15.6.3 LPR zone events

The LPR Zones system has events that can be triggered according to the conditions of entry or exit of a vehicle:

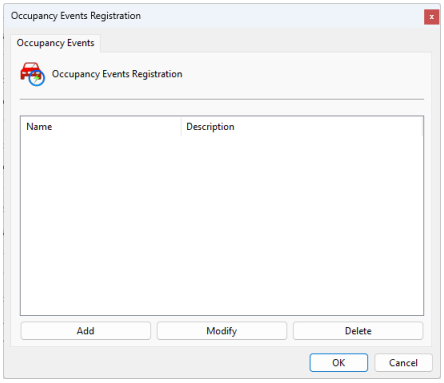


- **Trigger event when a vehicle remains in the zone for the configured time**: This option will trigger the configured actions if a license plate is captured at the input and is not captured at the output after the defined X minutes.
- **Trigger event when a vehicle leaves the zone before the configured time:** This option will trigger the configured actions if a license plate is captured at the input and is captured at the output before the defined X minutes.
- **Trigger event when a vehicle leaves the zone after the configured time**: This option will trigger the configured actions if a license plate is captured at the output after X minutes of capturing the input.
- **Trigger event when a vehicle enters the zone X times in Y minutes:** This option will trigger event actions when a vehicle enters and leaves the zone many times in a short period of time. In the example above, the event would be triggered if the same license plate was recognized entering the zone twice in less than 60 minutes.
- **Event Actions:** Desired alarm actions when the event is triggered. To learn more about event actions, see the chapter How to configure event actions.

15.6.3.1 Occupancy

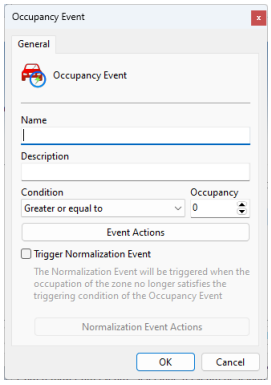
This option allows the configuration of occupancy events (based on the number of vehicles within the zone). When clicking on the Occupancy Events button, the event registration screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



You can define multiple events (For different occupancy conditions).

To create a new Event click **Add**. The following screen will be displayed:



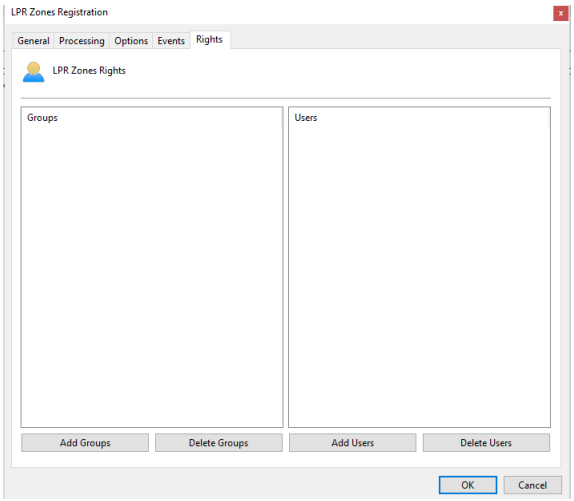
To change an event already registered, select it and click **Modify**, and change the data as explained on the following pages.
To remove an event, select the desired event and click the **Delete** button.

- **Name:** Name of the occupancy event.
- **Description:** Description of the occupancy event.
- **Condition:** Condition for triggering the event. Conditions can be **equal**, **different**, **less**, **less than or equal**, **greater** and **greater than or equal**.
- **Occupancy:** Occupancy to be considered in the condition.
- **Event Actions:** Desired event actions when this event is fired. To learn more about event actions, see the chapter How to configure event actions.
- **Trigger normalization event:** The normalization event is triggered when the zone occupancy returns to the "normal" state, that is, to the opposite condition than that configured to trigger the event. The normalization event is used so that the operation is notified of the normalization of zone occupancy.

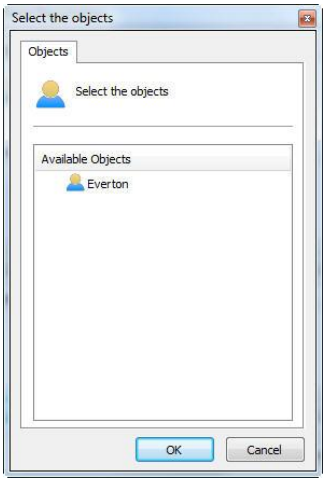
15.6.4 Rights

On the **Rights** tab you can define the list of users and user groups that will have the right to view this zone in the Surveillance Client.

© 2002 - 2024 by Digifort. All rights reserved.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

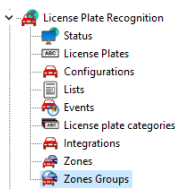


Select the available User and click **OK**. The same rule applies to the group list.

15.6.5 LPR Zone Groups

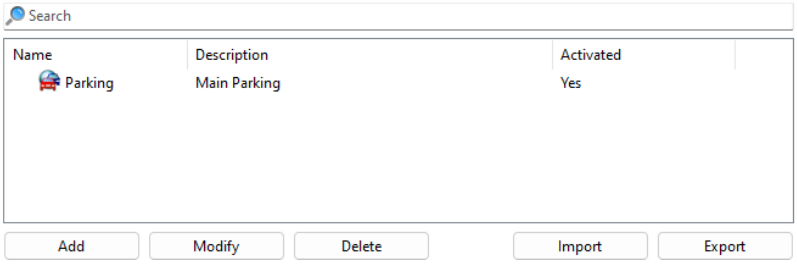
The system allows you to group LPR zones so that the **total** occupancy of these zones is considered for triggering events and displaying them in the Surveillance Client.

To access the Zone Groups register, open the **License Plate Recognition** item in the **Settings Menu** and click on the **Zone Groups** item as shown in the image below:

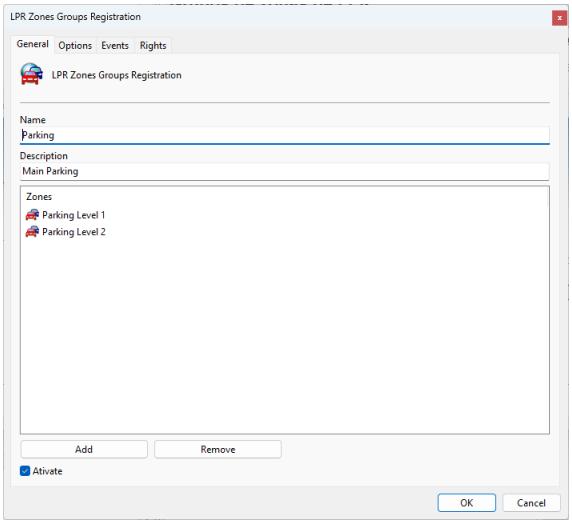


Once selected, the system will display the screen with the **Zone Group** registration:

© 2002 - 2024 by Digifort. All rights reserved.



When clicking on the **Add** button, the system will display the following screen:



To change an already registered zone group, select it and click **Modify**, and change the data as explained on the following pages.
To remove a zone group, select the desired group and click the **Delete** button.

- **Name:** Name of the Zone Group to be added.
- **Description:** Description of the Zone Group to be added.
- **Zones:** List of Zones that are part of this group.
- **Activated:** Determines whether this group will be activated.

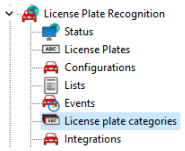
The settings for options, events and rights will be the same as for the LPR Zones already discussed in previous topics.

15.7 Plate Category Groups

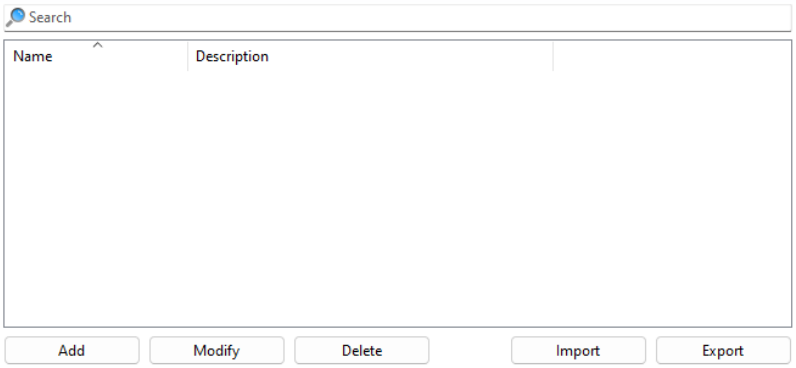
The plate categories feature is currently used exclusively with the ARH Carmen engine. This engine is capable of differentiating the type of license plate (for example, cars, taxis, motorcycles, etc.) through a category code (ID), however this ID is not user-friendly, so it is possible to register a label where the system will replace the ID received by the library by the label provided in this registration.

To access the integration settings, open the **License Plate Recognition** item in the **Settings Menu** and click on the **License Plate Categories** item as shown in the image below:

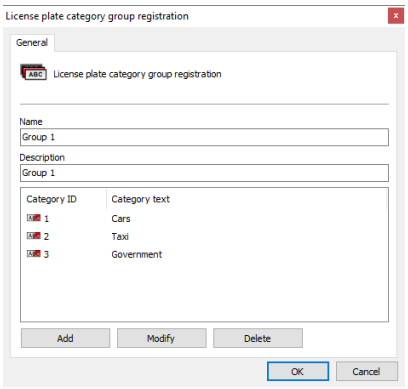
© 2002 - 2024 by Digifort. All rights reserved.



Once selected, the system will display the group registration screen:



When clicking on the **Add** button, the system will display the following screen:

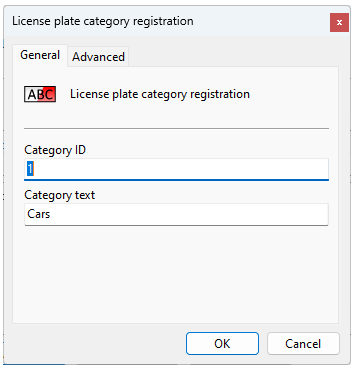


To change an already registered group, select it and click **Modify**, and change the data as explained on the following pages.
To remove a group, select the desired group and click the **Delete** button.

- **Name:** Group's name.
- **Description:** Group description.
- **Category List:** List of registered categories.

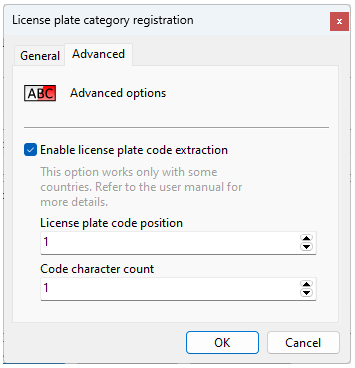
Click the **Add** button to create a new category label.

© 2002 - 2024 by Digifort. All rights reserved.



- **Category ID:** ID provided by the Carmen engine (This ID can be found in the details of the license plate recognition result in the Surveillance Client).
- **Category Text:** Provide the text that will replace the ID in the Surveillance Client

Advanced:



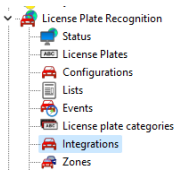
- **Enable Plate Code Extraction:** Allows the system to extract a special identification code from the plate (This feature is only available for certain Middle Eastern countries).
  - **Plate Code Position:** Specify the position of the plate code character.
  - **Character Count:** Specify how many characters are part of the license plate code.

15.8 Integrations

The system allows integration with various third-party systems or external databases to query and send data to these systems. This integration is done through the **LPR Bridge** module and requires a license for each camera/service set that will send the data.

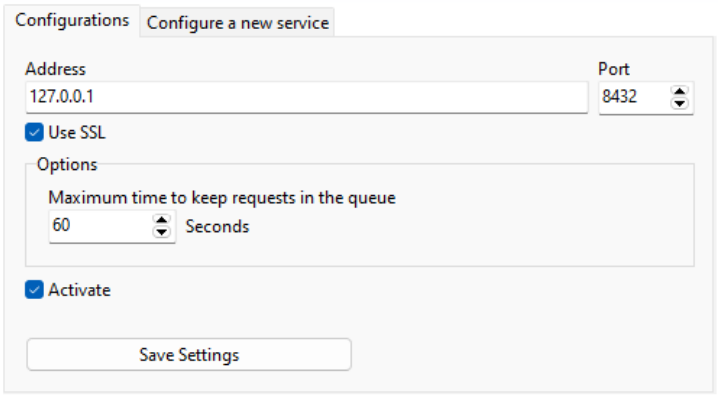
The LPR Bridge module must be running on some server on the network, preferably on the same VMS server. LPR Bridge licenses are configured on the VMS server.

To access the integration settings, open the **License Plate Recognition** item in the **Settings Menu** and click on the **Integrations** item as shown in the image below:



© 2002 - 2024 by Digifort. All rights reserved.

The LPR Bridge integration configuration screen will be displayed:



- **Address:** Address of the server where the LPR Bridge service is installed.
- **Port:** Port on which the LPR Bridge service is configured.
- **Use SSL:** Check this option if the system uses SSL.
- **Maximum time to keep requests in the queue:** Time that the system must wait for a response before discarding that request.
- **Activate:** Activates or deactivates the integration.

For more information on how to configure each of the available services, see the LPR Bridge manual.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XVI

16 Web Pages

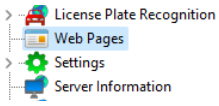
Through **Web Page** objects, registered through the Administration Client, it is possible to add pre-configured links to web pages or web systems that can be accessed by system operators, as well as an integrated browser for the Surveillance Client operator to use if necessary. necessary.

Examples of using the integrated browser:

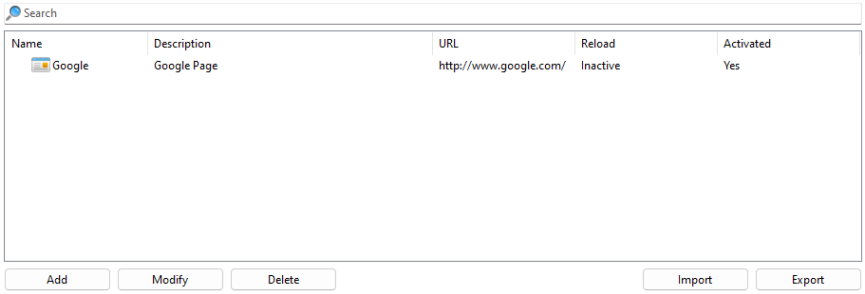
- Integrate third-party web systems into the same camera management interface. Systems such as access controls, alarm controls, face recognition, among others can now be opened and operated through the Surveillance Client
- Display dashboards on a video wall or at operator stations
- Access pre-defined websites
- Free navigation

16.1 Web Page Registration

To register a Web Page, click on the **Web Pages** item in the Settings Menu, as shown in the figure below:

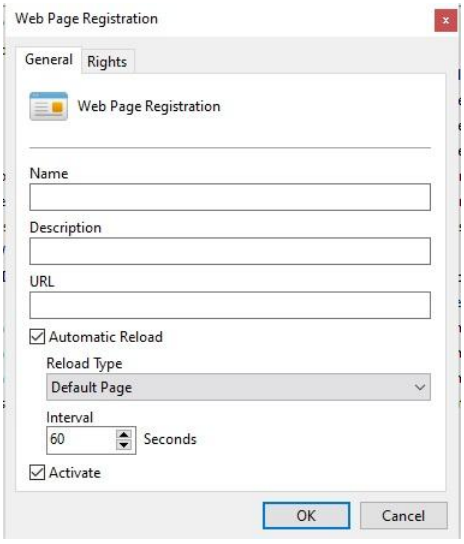


Once this is done, the system Web Pages registration screen will open on the right side, as shown in the figure below:



Click **Add** to open the Web Pages settings screen as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

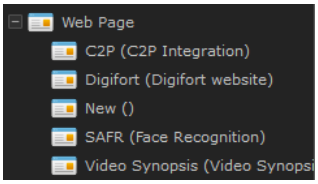


- **Name:** Name of the web page
- **Description:** Provide a description for the object for easy identification in the system.
- **URL:** Link to the page that will open in the Surveillance Client. Note: if the URL form is left blank, the user can enter the website address within the Surveillance Client,
  Ex.:

- **Automatic Reload:** This option will make the system automatically update the page every X seconds. Also allowing the option to reload the default page (registered in this option) or reload the page the user is currently on.
  - **Reload Type:**
    - **Default Page:** Reloads the default page specified in the URL.
    - **Current Page:** Reloads the current page the user is currently browsing.

- **Activate:** Activate the web page.

In the Surveillance Client, the operator will have access to the web pages to which he or she is entitled through the list of objects:



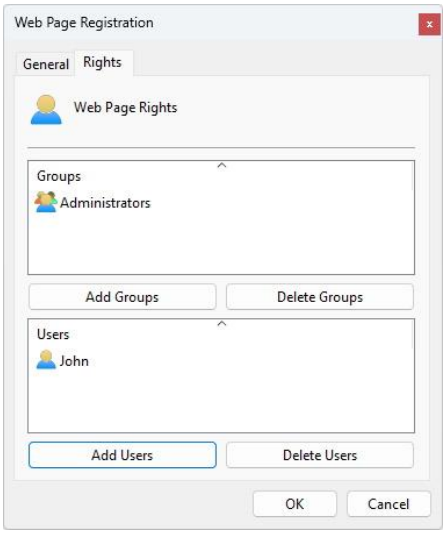
The browser associated with the pre-registered pages will not provide the address bar, preventing the operator from accessing any other website or page other than the specified page, however, it is possible to free up the address bar for free navigation by creating a page object web with a blank address, in this case, when the operator places this object on the screen, the browser will provide the address bar for navigation.

© 2002 - 2024 by Digifort. All rights reserved.

We use the Chromium browser by default, which is already embedded in the Surveillance Client, however it is possible to use Internet Explorer 11 or native Windows Edge by changing the browser option in the Surveillance Client options.

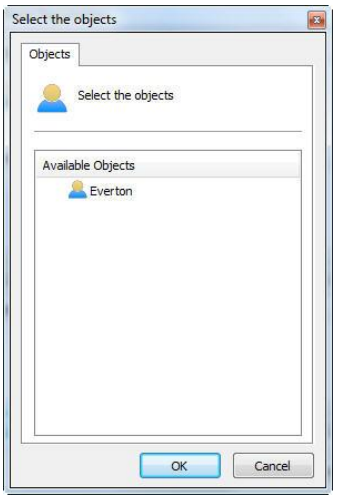
16.1.1 Rights

In the **Rights** tab you can define the list of users and user groups that will have the right to view this Web Page in the Surveillance Client.



To grant access rights to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** that will appear as shown in the figure.

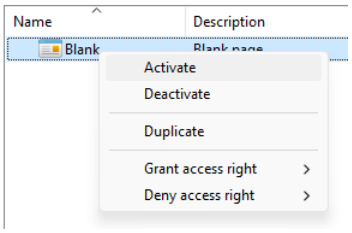
© 2002 - 2024 by Digifort. All rights reserved.



Select the available User and click **OK**. The same rule applies to the group list.

16.2 How to change parameters for multiple web pages simultaneously

The system's web page manager provides quick access to the most common settings that can be changed for multiple pages simultaneously. In the web page registry, select the desired objects and right-click. A menu will open as shown in the figure below:



Most of the options you can change are self-explanatory and you can consult the Web Page Registration topic to learn more about each option.

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XVII

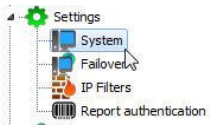
17 Settings

17.1 System

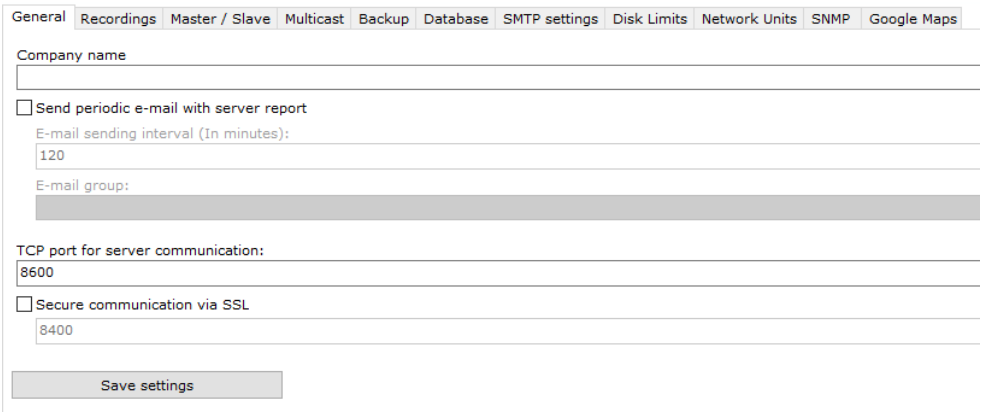
This area of the system is reserved for adjusting global server settings.
Global settings are parameters that, once configured, will affect the entire operation of the system.

17.1.1 General

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



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



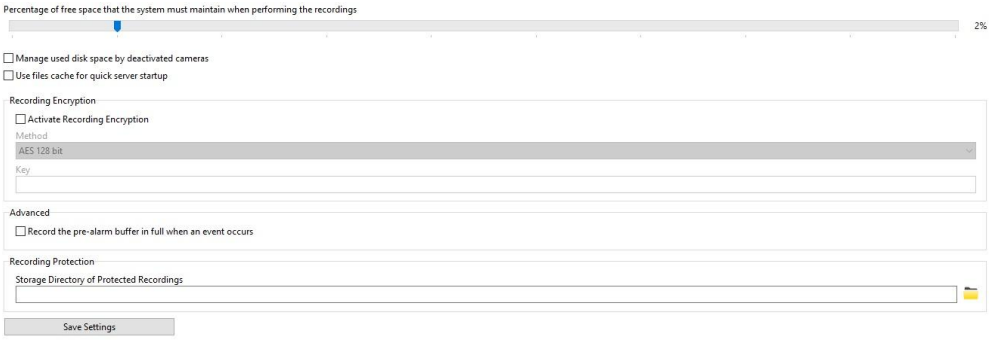
- **Company name:** Company name will be used in video exports to facilitate operation in the monitoring client.
- **Send periodic email with server report:** Sends a periodic email to the specified alert group a server report at a specified time interval. This report contains information such as user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

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

© 2002 - 2024 by Digifort. All rights reserved.

17.1.2 Recordings

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



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

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

17.1.2.1 Recording Encryption

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

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

17.1.2.2 Advanced

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

© 2002 - 2024 by Digifort. All rights reserved.

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

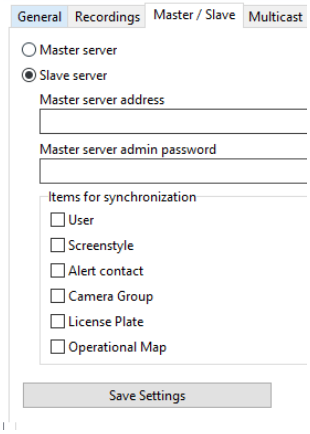
17.1.2.3 Recording Protection

Enter the location for storing protected recordings. This location will be where recordings will be saved that will not be deleted as recycling is achieved. To learn more, consult the Surveillance Client manual

17.1.3 Master / Slave

The Master / Slave option allows sharing of objects that are common between recording servers.

By default the server will always be **Master**. To configure it as a **Slave**, simply select the slave option and fill in the following fields as shown in the figure below. The **Slave** server will import all selected objects from a **Master** server.



- **Master server address:** IP address or dns of the master server.
- **Master server admin user password**: Admin user password to access the server.
- **Items for Synchronization**
  - **Users:** Shares the user base between servers.
  - **Layouts:** Shares screen layouts between servers.
  - **Alert Contacts:** Shares alert contacts between servers.
  - **Camera Groups:** Share camera groups between servers.
  - **License Plates:** Shares license plate registration, license plate lists and license plate categories between servers.
  - **Operational Maps:** Shares the operational map registry between servers.

For the settings to take effect, click **Save Settings**, you will notice that all information has been exported successfully.

Note

In general, objects shared between the master server and slaves can only be changed on the master server. The registration of these objects on slave servers will be blocked.

When the LPR synchronization option between Master / Slave is activated, the Plate Registration, List Registration and Plate Category Registration will be shared between the servers.

© 2002 - 2024 by Digifort. All rights reserved.

Note

Generally, object registration is only allowed on the Master server, however, in the case of LPR it is possible to register plates through the Surveillance Client, connected to a Slave server only, and the Slave server will share the data with the Master and the Master will forward the data to other Slave servers.

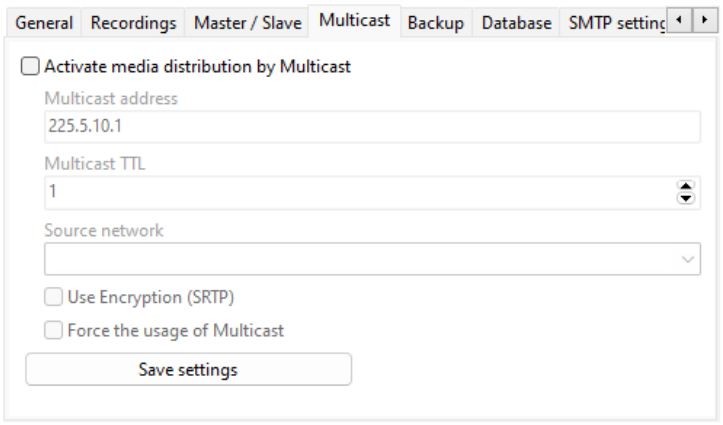
17.1.4 Multicast

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

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

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

Below is the multicast options configuration screen:

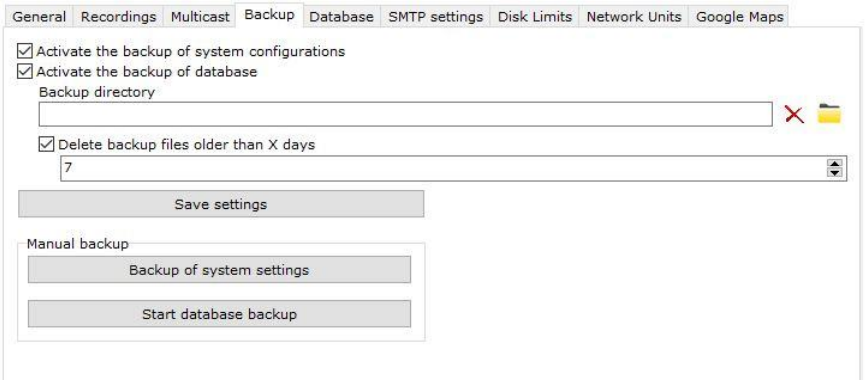


- **Activate media distribution by Multicast:** Enables video streaming to be sent via multicast.
- **Multicast Address**: Considering the IPv4 IP naming architecture and best practices, it is known that the IP range reserved for multicasting is: 224.0.0.0 to 239.255.255.255. For this reason, as standard,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

© 2002 - 2024 by Digifort. All rights reserved.

17.1.5 Backup

The system allows the backup if its settings and database.



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

- **Save Settings:** Saves the chosen settings.

- **Manual Backup**
  - **Backup Of System Settings:** When you click on this option, the system will back up the registration files and folders to the selected backup directory.
  - **Start Database Backup:** When you click this option, the system will back up the database files to the backup directory.

Note

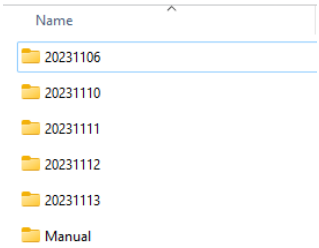
The system does not perform backups of recorded videos. Use the Archiving function for long-term image storage.

17.1.5.1 Backup Structure

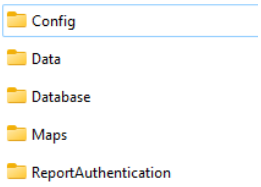
The system will perform a security backup of settings, folders and database using the following structure:

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

© 2002 - 2024 by Digifort. All rights reserved.



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



  - **Config:** Contains system configuration files.
  - **Data:** Contains the **Data** subfolder that is found in the server installation folder and contains data that is too large to be written to the OS registry.
  - **Database:** Contains the backup of the database files.
  - **Maps:** Contains the binary files with images stored for the **Synoptic Maps**.
  - **ReportAuthentication:** Contains the authentication files for **Authenticated Reports**.

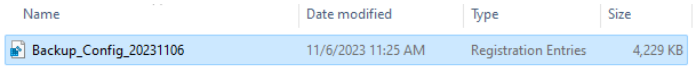
- The **Manual** subfolder will contain a subfolder with date and time for each manual backup performed where the folder structure listed above will be found, with the backups performed.

17.1.5.2 Restoring Backups

17.1.5.2.1 Settings

To restore a system settings backup, follow these steps:

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

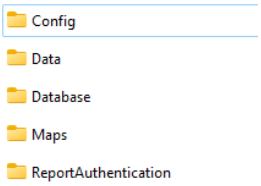


3. A registry editor confirmation message will be displayed asking if you want to continue with the operation, click **Yes** and wait until the confirmation message is displayed.
4. Restart the server service and the settings are now restored.

17.1.5.2.2 Folders

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

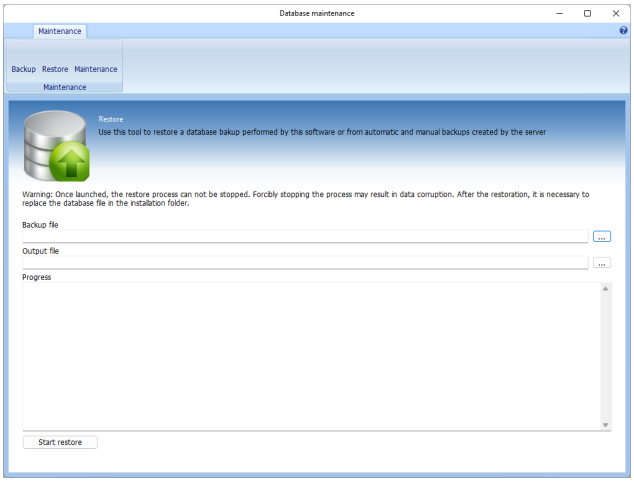
© 2002 - 2024 by Digifort. All rights reserved.



- **Data:** To restore the **Data** folder, copy and replace the corresponding folder in the server installation folder.
- **Maps:** To restore the **Maps** folder, copy and replace the corresponding folder in the server installation folder.
- **ReportAuthentication:** To restore the Authenticated Reports files, copy the contents of this folder to the **ReportAuthentication** folder in the server root or to the folder configured to store authenticated reports. To learn more about the storage folder for authenticated reports, see the Report Authentication topic.

17.1.5.2.3 Database

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



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

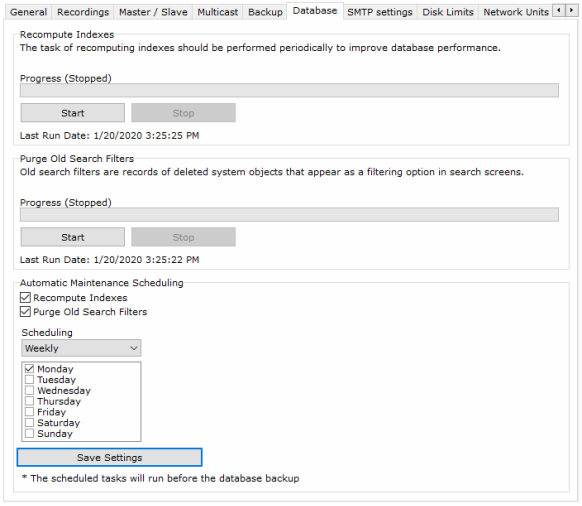
1. Select the desired backup file (*.ddb) by clicking the button with 3 dots (...).
2. Select a temporary file, where the database will be rewritten. Name the file DIGIFORTDB.FDB
3. Click **Start Restore**.
4. Wait for the backup restore process. This process may take anywhere from a few minutes to a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

17.1.6 Database

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

© 2002 - 2024 by Digifort. All rights reserved.

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



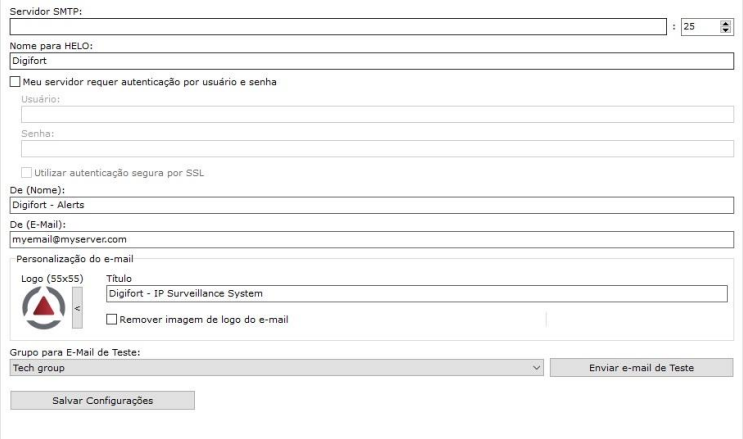
- **Recompute Indexes:** This option will start the re-computation of the database indexes, in order to increase performance during record queries. This task must be performed periodically.
- **Purge Old Search Filters:** This option will cause old search indexes (which are no longer referenced in the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

17.1.7 SMTP

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

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

© 2002 - 2024 by Digifort. All rights reserved.

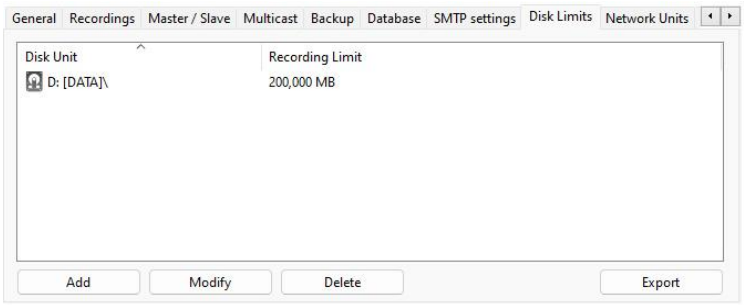


- **SMTP Server:** SMTP server address to be used for sending e-mails. This parameter can be an IP, if your company has its own SMTP server, for example, or a DNS if you use third-party SMTP servers.
- **My server requires username and password authentication:** If your SMTP server requires a username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

17.1.8 Disk Limits

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

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



© 2002 - 2024 by Digifort. All rights reserved.

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

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

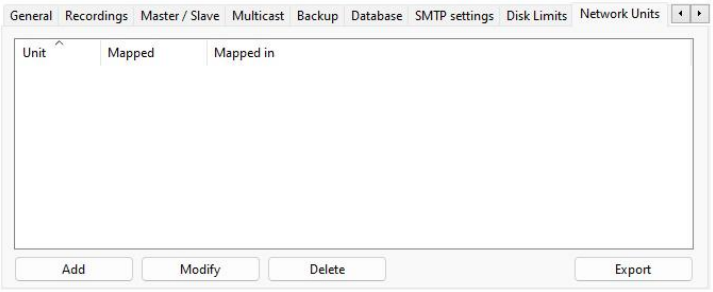
To change a limit, select it and click the **Modify** button.
To remove a disk limit, select it and click on the **Delete** button.

17.1.9 Network Units

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

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

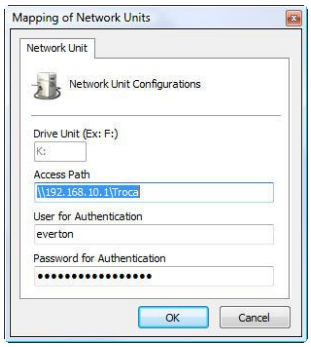
To access this feature, click on the **Network Units** tab, as shown in the figure below:



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

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

© 2002 - 2024 by Digifort. All rights reserved.



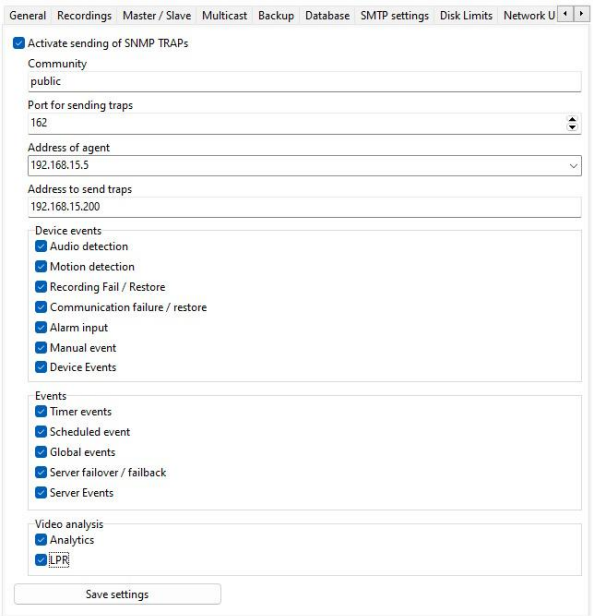
- **Drive Letter:** Specify a letter identifying the drive to be mapped.
- **Access path:** Specify the full path of the remote computer folder you want to map.
- **User for authentication:** Windows network user who has access to the folder.
- **Password for authentication:** Windows network password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

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

17.1.10 SNMP

Simple Network Management Protocol (SNMP), is a standard protocol for managing devices on IP networks.
Some equipment and software can use this protocol to receive and send alarms.

The system allows the sending of TRAPs to notify the occurrence of a system event through the SNMP protocol. The SNMP screen on the system has the following options:



© 2002 - 2024 by Digifort. All rights reserved.

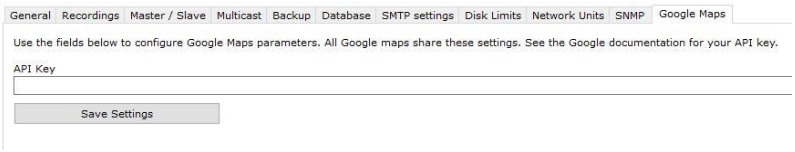
- **Community:** Public is the default setting for sending SNMP notifications in read-only mode.
- **Port for sending traps:** Select the port for sending traps;
- **Agent Address:** Select the network where the trap will be sent.
- **Address to send traps:** Select the address to send traps.
- **Device events:** Select the desired device related events to send traps.
- **Events:** Select the desired events for sending traps.
- **Analytics:** Select the desired analytics events to send traps.
- **Save settings:** Saves screen settings.

Note

To import the system's SNMP information bases, simply use the **Digifort-MIB.mib** file located in the software installation root.

17.1.11 Google Maps

To use system resources that use Google Maps (such as Operational Maps, Event Maps, LPR Maps, among others), you must specify an API key for Google Maps.



- **API Key:** Fill in this field with your Google Maps JavaScript API key.
- **Save Settings:** Saves screen settings.

Refer to Google's documentation to learn how to create a new API key.

The Google Maps API Key must be of type JavaScript.

Tip

Don't forget to create / associate the billing account on Google Cloud, otherwise the created key will not work.

17.1.12 Protocols

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

- **Standard HTTP authentication method:** Here we can select between **Digest** (more secure) or **Basic** methods. The system always determines, according to the HTTP driver of the devices, which authentication method will be used, however the first attempt will be made with the protocol selected here. By default, the recommendation is to keep it in the **Digest** method, as it is safer and does not expose data in this first attempt.

© 2002 - 2024 by Digifort. All rights reserved.

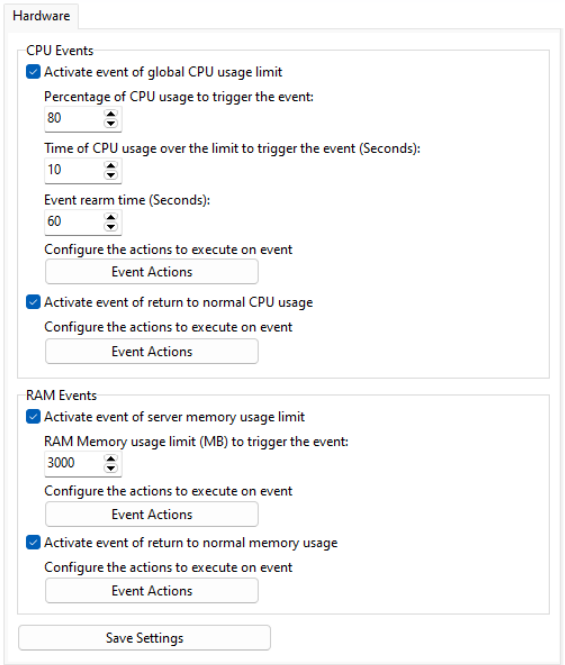
- **Default RTSP authentication method:** Here we can select between **Digest** (more secure) or **Basic** methods. The system always determines, according to the devices' RTSP driver, which authentication method will be used, however the first attempt will be made with the protocol selected here. By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

17.2 Server Events

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

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

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



- **CPU Events:**

© 2002 - 2024 by Digifort. All rights reserved.

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

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

17.3 Failover

The system's servers can be configured to work as Failover, that is, if one server stops working, another will take over the operation of desired objects (and previously imported from the main server).

On the server that will act as Failover, you must register objects called **Failover Monitors**. The Failover Monitors will monitor the activity of the desired servers and when a communication failure with any of these servers occurs, the Failover Monitor will trigger the **Failover** event that can be used to activate objects imported from the main server on the Failover server, objects such as cameras, analytics, LPR, among others, can be imported and activated during Failover. When communication is reestablished, the Failover Monitor will trigger the **Failback** event, where event actions must be configured to disable objects activated during Failover. If your version of the system has the Auto-Healing feature, the main server can automatically download recordings from the Failover server for the period that the main server was down. To learn how to configure this feature, see the Auto-Healing topic. Camera cure.

To exemplify the Failover server configuration, let's assume a scenario of a company that has two servers, **Server A** with 4 cameras and **Server B** as Failover. If **Server A** stops working, **Server B** must start recording 1 camera out of the 4 cameras on the first.

First, we must import the camera we want to fail over on **Server B** and leave it disabled. To learn more, see the topic Import objects from other servers.

Tip

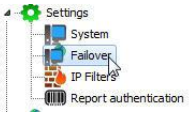
You will be able to import any type of objects from the main server to the Failover server and activate / deactivate these objects during main server failure. This is necessary because if the main server is down,

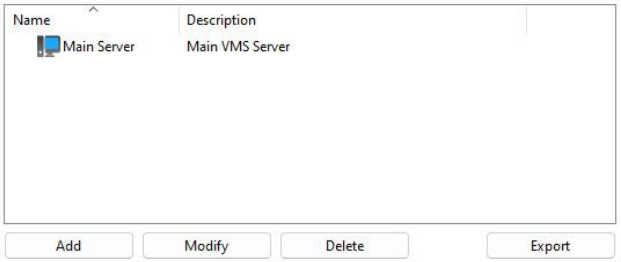
© 2002 - 2024 by Digifort. All rights reserved.

Tip

the Surveillance Clients will not have access to the objects on this server but only to the objects on the Failover server.

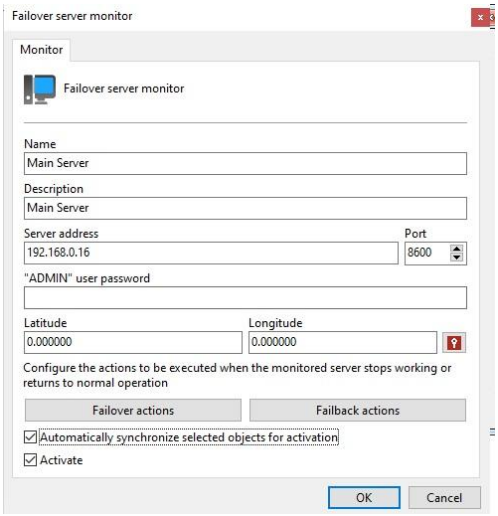
Now access the **Server B** Failover option as shown in the image below:





On **Server B** we will register **Server A**. This way, if **Server A** goes down we can start recording the camera on **Server B**.

To add the Server, click **Add** and the following screen will be displayed:



To change an already registered monitor, select it and click **Modify**, and change the data as explained below.
To remove a monitor, select the desired object and click the **Delete** button.

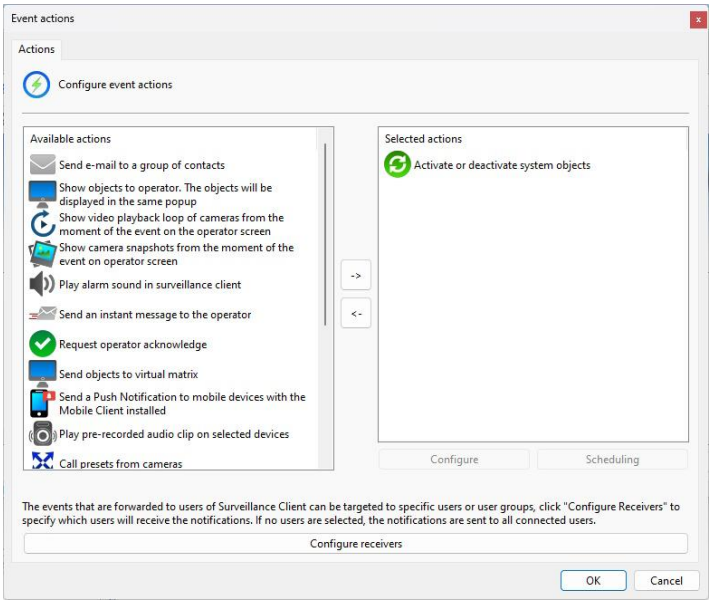
- **Name**: Failover Monitor Name
- **Description**: Description of the Failover Monitor for this server
- **Server address**: Server IP to be monitored
- **Port:** Main connection port to the server.
- **Admin user password**: Password for the admin user of the server to be monitored.
- **Latitude / Longitude:** Coordinates of where this server is located.

© 2002 - 2024 by Digifort. All rights reserved.

- **Failover Actions:** Desired event actions when the Failover event is triggered. To learn more about event actions, see the chapter How to configure event actions.
- **Failback Actions:** Desired event actions when the Failback event is triggered. To learn more about event actions, see the chapter How to configure event actions.
- **Sync selected objects for activation automatically:** This option will cause the system to automatically update the objects selected in the **Activate Objects** action of the **Failover** event, so if the object is changed on the main server (for example, the IP of a camera), these changes will be applied to the registration of this camera on the Failover Server.
- **Activate**: Enables or Disables this Failover Monitor.

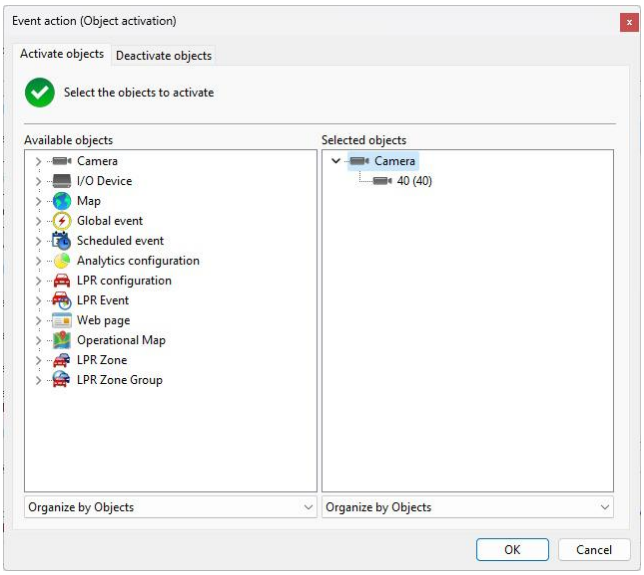
Now we must create the actions that we want to execute when the Failover situation is detected by the system.
To do this, click **Failover Actions**:

The main action in the Failover situation is to **activate the objects** that we want to start working on **Server B**. Let's give an example with the operation of a camera, but keep in mind that the same theory can be applied to objects such as I/O Devices, analytics, LPR, among others.



Drag the **Activate or Deactivate System Objects** option to the right list to activate this event action and double-click to configure.

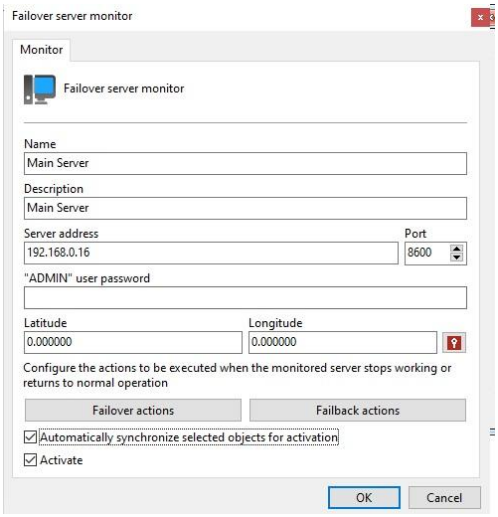
© 2002 - 2024 by Digifort. All rights reserved.



Now configure the camera you want to activate when **Server A** stops working by dragging to the right as shown in the image above.

According to the scenario proposed here, as soon as **Server A** stops working, **Server B** will activate camera "**40**" and start recording.

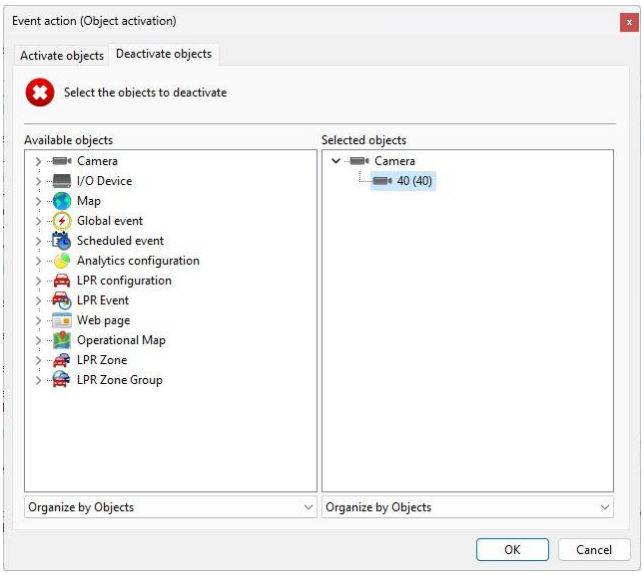
Now we will return to the Failover registration screen:



To complete the process, we must configure an action for when **Server A** comes back up and running. Click **Failback Actions** to continue.

In our example, we will now disable the camera on the **Failover** server as **Server A** is already working again. Once **Failback** is detected, camera "40" will be disabled on **Server B** as shown in the image below:

© 2002 - 2024 by Digifort. All rights reserved.

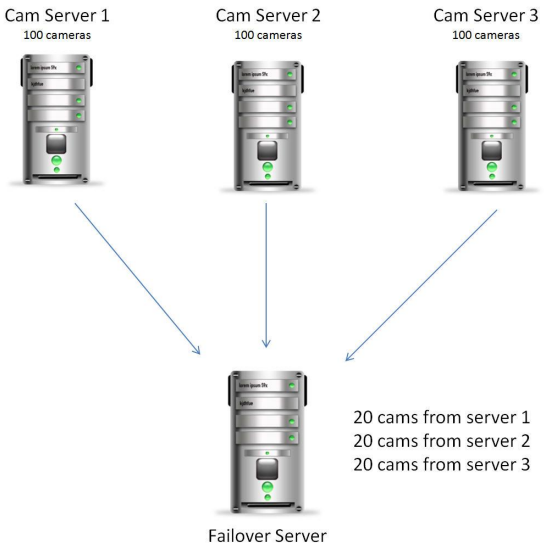


With the server configuration now complete, you will need to configure the Survellance Clients. All servers (Main and Failover) must be registered in the Survellance Client and it must be connected to all servers so that the automatic exchange between the main and failover server objects can occur. In the Survellance Client you also need to activate the Failover Operation option in the server registration. For more information, see the Survellance Client manual.

17.3.1 Multiple Servers

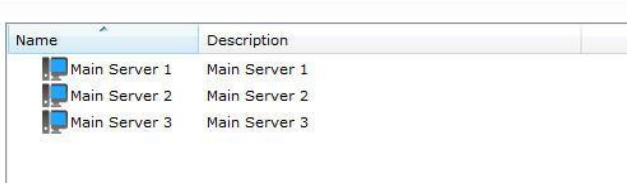
The failover system is extremely flexible, allowing 1-1, 1-N and N-N configuration through the registration of multiple Failover Monitors.

Below is a second example where the Failover server is programmed to start recording 20 cameras from each main server.



In this case, 20 main cameras were imported from each server and then configured the 3 monitors for **failover** as shown in the image below:

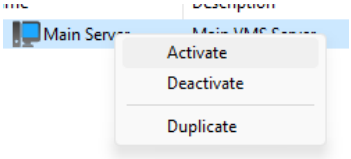
© 2002 - 2024 by Digifort. All rights reserved.



In the example above, this Failover server will have 60 registered cameras (20 cameras being imported from each VMS server) and each Failover Monitor must be configured to activate the respective cameras on their servers when the failure occurs and deactivate them when the server comes back up, as described in the previous topic.

17.3.2 How to change parameters for multiple monitors simultaneously

The system's Failover Monitor manager provides quick access to the most common settings that can be changed for multiple objects simultaneously. In the Failover Monitors register, select the desired objects and right-click. A menu will open as shown in the figure below:



Most of the options you can change are self-explanatory and you can consult the Failover Monitor Registration topic to learn more about each option.

17.4 IP Filters

As another means of security, the system provides another very important tool for the security of the server, which are IP filters.

These filters work like a firewall, blocking unwanted connections to the server.

IP filters can add IPs that will and will not have access to the system.

When a user tries to connect to the server through a blocked IP, his connection will not be allowed, disconnecting him and registering this action in the log.

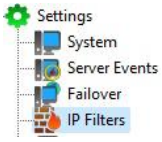
If this configuration is not done, all IPs are allowed to access the server.

Note

The IP Filter feature only works with IPv4

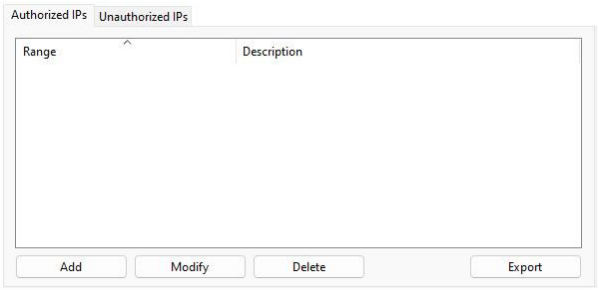
17.4.1 IP Filter Registration

To access IP filters, locate the IP Filters item in the Settings Menu, as shown in the figure below:



© 2002 - 2024 by Digifort. All rights reserved.

Once this is done, the **IP filter** register will be displayed on the right, as shown in the figure below.



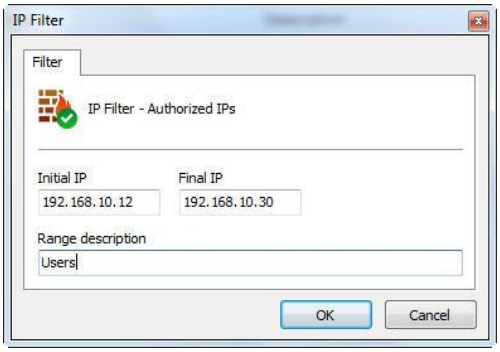
This configuration is divided into two parts: authorized IPs and unauthorized IPs. Authorized IPs have privileges over unauthorized ones, that is, if a certain authorized IP is in the range of unauthorized IPs, it will be allowed.

In the examples given in the next chapters, we will block all IPs and only allow monitoring stations in the range from 192.168.10.12 to 192.168.10.30.

To add authorized IPs click **Add**. To change or delete authorized IPs, select it and click on the corresponding button.

17.4.1.1 How to add authorized IPs

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

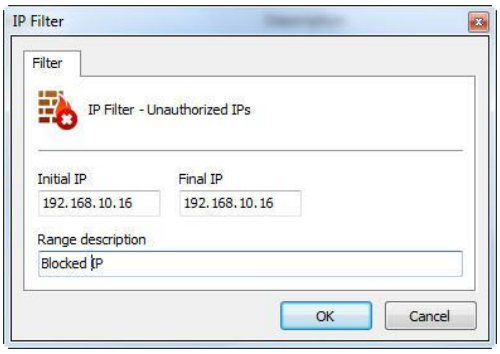


- **Initial IP:** Initial IP of the range to be configured.
- **Final IP:** Final IP of the range to be configured.
- **Range Description:** Identification name of the range to be configured.

17.4.1.2 How to add rogue IPs

To add unauthorized IPs, click on the Unauthorized IPs tab and then click Add, opening the screen below:

© 2002 - 2024 by Digifort. All rights reserved.



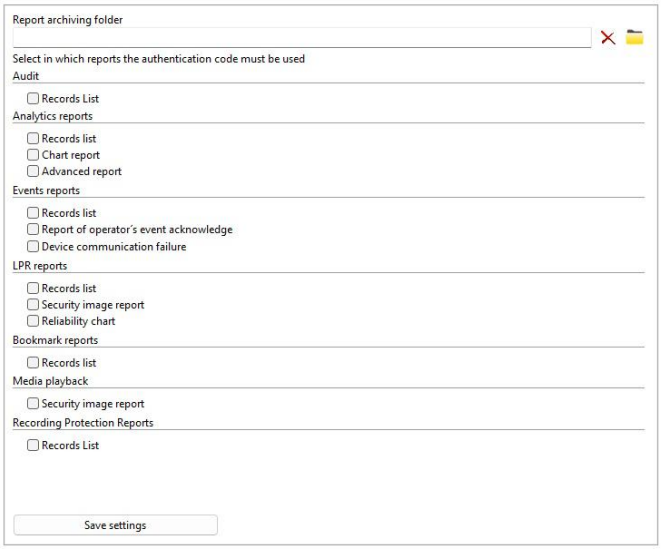
- **Initial IP:** Initial IP of the range to be configured.
- **Final IP:** Final IP of the range to be configured.
- **Range Description:** Identification name of the range to be configured.

17.5 Report Authentication

The **authenticated reports** option aims to generate reports in the system with a unique identification of authenticity. In this way, the reports generated by the software will contain a unique number along with a barcode, thus allowing subsequent search and access to the original report generated by the software.

Reports often need to be generated, whether from event logs, LPR, analytics, or even a printout of an image from video playback. Later, if the user wishes to check a report issued by the system, simply request the report using its barcode and the system will generate it again with the originally saved data, making it possible to compare it with an already printed report in order to confirm its authenticity.

To activate this feature, click on **Report authentication** as in the image below:



© 2002 - 2024 by Digifort. All rights reserved.

On this screen we have the following functionalities:

- **Report Archiving Directory:** Choose a directory where the system will store authenticated reports. If not filled in, the reports will go to the "**ReportAuthentication**" folder in the server installation folder.
- **Select in which reports the authentication code must be used:** This section will display all system reports that support authentication, select the reports you want to be authenticated when printing.
- **Save Settings:** Save the options chosen on this screen.

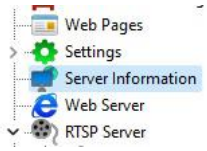
To learn how to generate and search authenticated reports, see the Surveillance Client manual.

© 2002 - 2024 by Digifort. All rights reserved.

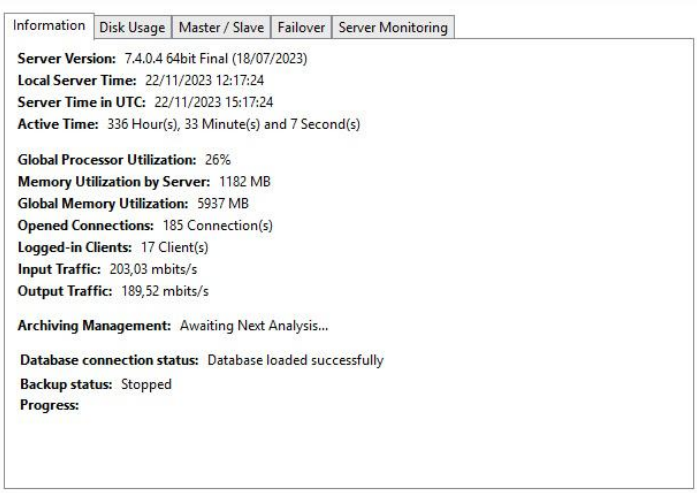
Chapter XVII

18 Server Information

In this area of the system you can monitor how the server is performing, retrieving data such as processor usage, memory, network traffic, etc.
To access this feature, click on the **Server Information** item in the Settings Menu, as shown in the figure below:



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



- **Server Version:** Displays the server version.
- **Local Server Time:** Displays the server's local time.
- **Server Time in UTC:** Displays the server time adjusted to UTC.
- **Active Time:** Displays the time that the server service has been active.

- **Global Processor Usage:** Displays the global CPU usage of the server where the server process is running. This value represents the total usage by all Operating System processes and not just the VMS Server.
- **Server Memory Usage:** Displays the memory usage of the VMS Server process only.
- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Open Connections:** Number of open connections with the VMS Server.
- **Logged in Clients:** Number of individual clients connected to the server.
- **Input Traffic:** Total data being received by the VMS server (Device Traffic).
- **Output Traffic:** Total data being sent by the VMS server (To clients).

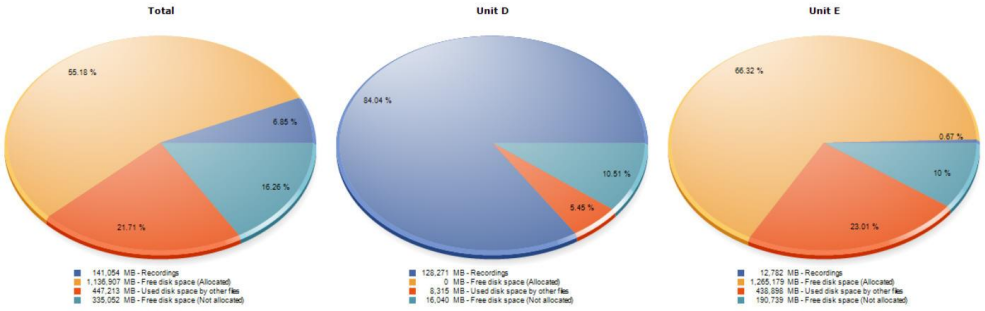
- **Archiving Management:** Displays the current state of the archiving system.

- **Database Connection Status:** Displays the current status of the Database connection.
- **Backup Status:** Informs whether the database backup is running.
- **Progress:** Displays the database backup progress.

© 2002 - 2024 by Digifort. All rights reserved.

18.1 Disk Usage

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

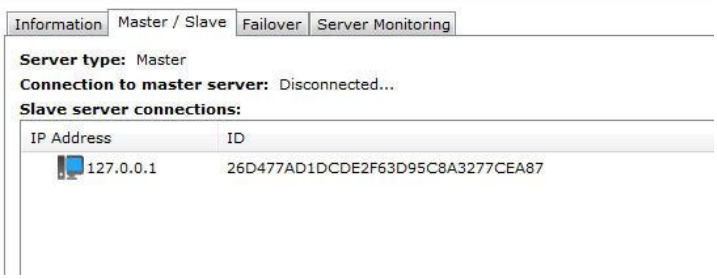


- The dark blue color in the graph represents the percentage of recorded data.
- The yellow color represents the percentage of free disk space allocated for recording.
- The orange color represents the percentage of space used by other files not related to image recording.
- The light blue color represents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

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

18.2 Master / Slave

Shows the status of Master / Slave servers and their connections. To learn more about master / slave servers see the Master / Slave chapter

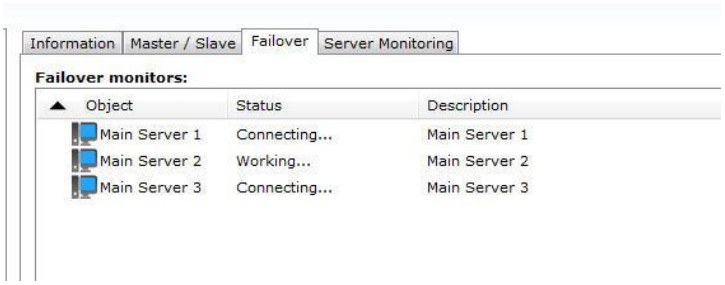


- **Server Type:** Identifies whether this server is a Master or Slave server
- **Connection To The Master Server:** If this is a slave server, the connection status with the master server will be displayed here
- **Slave Server Connections:** If this is a master server, the list of slave server connections to this server will be displayed here.

18.3 Failover

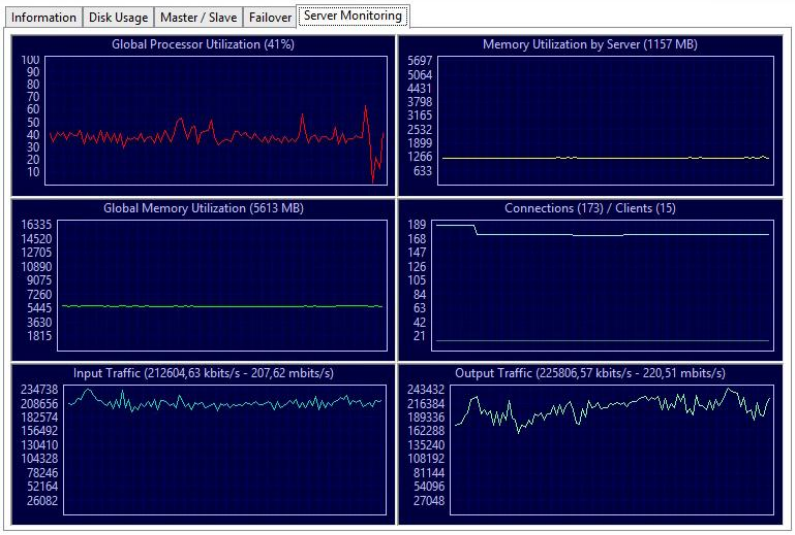
Shows the Status of servers being monitored by the Failover feature. To learn more about Failover see the chapter: Failover

© 2002 - 2024 by Digifort. All rights reserved.



18.4 Monitoring

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



- **Global Processor Usage:** Displays the global CPU usage of the server where the server process is running. This value represents the total usage by all Operating System processes and not just the VMS Server.
- **Server Memory Usage:** Displays the memory usage of the VMS Server process only.
- **Global Memory Usage:** Displays the total memory usage by all Operating System processes.
- **Connections:** This graph has 2 lines, the blue line represents the number of open connections with the server and the green line represents the number of connected clients.
- **Input Traffic:** Total data being received by the VMS server (Device Traffic).
- **Output Traffic:** Total data being sent by the VMS server (To clients).

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XIX

19 Web Server

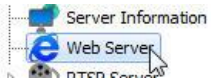
The system has an embedded web server, which is used to distribute files necessary for automatic client updates (in server version upgrades), distribution of general files and also has an interface for monitoring and video playback via Internet Explorer.

Note

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

19.1 Settings

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



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

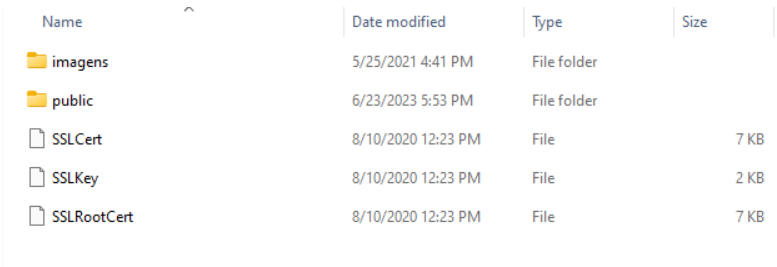
- **Activate the web server:** Activates the Web server allowing users to connect to the server through a web browser.
- **Server port**: Port used to access the server. This port can be changed and must be configured on your router for external access.
- **Enable HTTPS (SSL):** Enable HTTPS support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

19.2 FIle Server

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

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

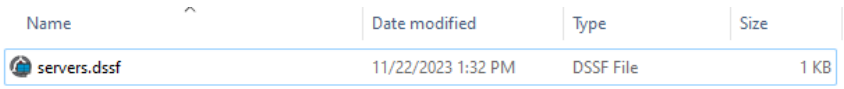
© 2002 - 2024 by Digifort. All rights reserved.



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

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

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



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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

20 RTSP Server

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

The RTSP server supports media in the following formats:

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

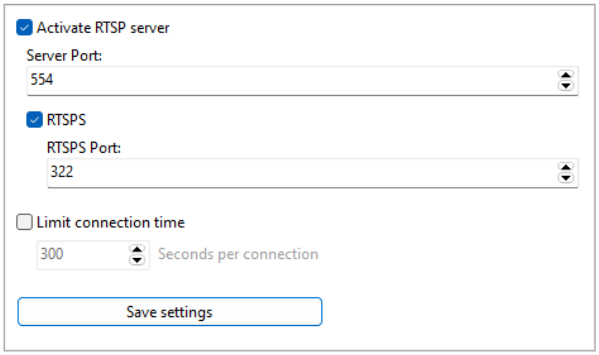
To receive live video on RTSP clients, use the syntaxes below:

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

20.1 Settings

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

The settings screen below will be displayed:

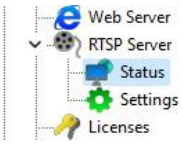


- **Activate the RTSP server:** Enables or disables the RTSP Server.
  - **Server Port**: Port used to access the RTSP Server. The default RTSP port is 554.
  - **RTSPS:** Enables or disables RTSPS (RTSP over SSL).
    - **RTSPS Port:** Connection port for RTSPS. The default RTSPS port is 322.
- **Connection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

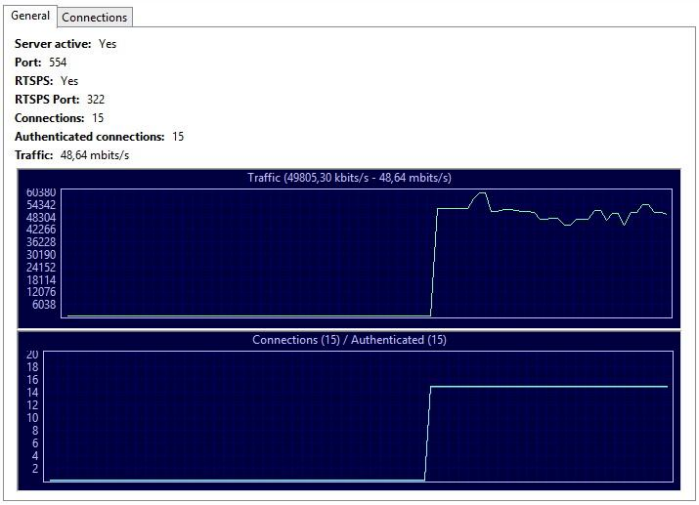
20.2 Status

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

© 2002 - 2024 by Digifort. All rights reserved.



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

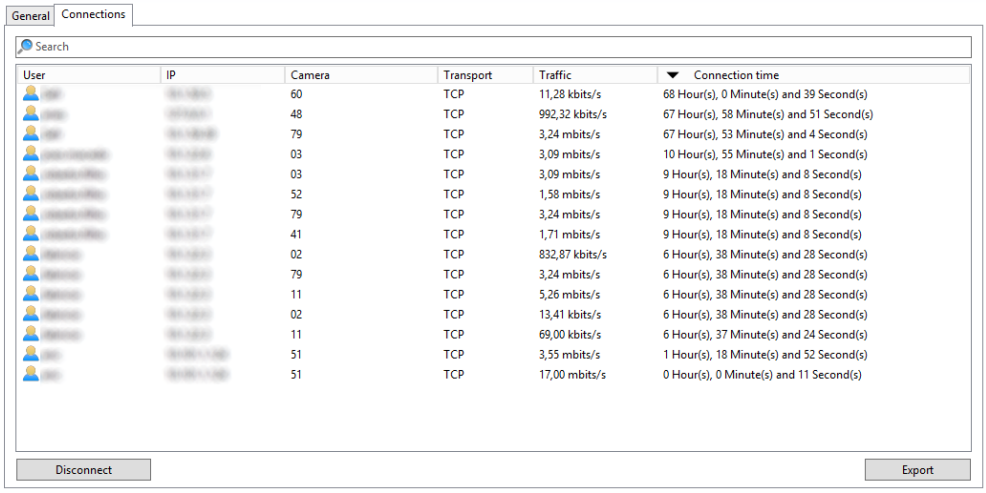


The **General** tab will provide the following information:

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

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

© 2002 - 2024 by Digifort. All rights reserved.



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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

21 Logs

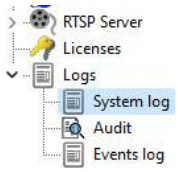
Logs are very important tools for an environment involving a security system such as Digifort, as they record all events and user actions that occur in the system.

21.1 System Logs

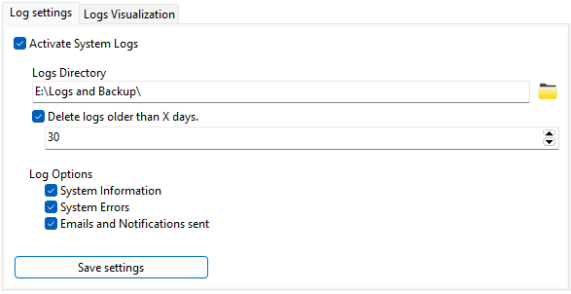
System logs record server-specific events, such as when the server was started or stopped, recording recycling information, deleted files, server errors, emails sent, among others. System logs are recorded in text files in the configured folder.

21.1.1 How To Configure System Logs

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



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



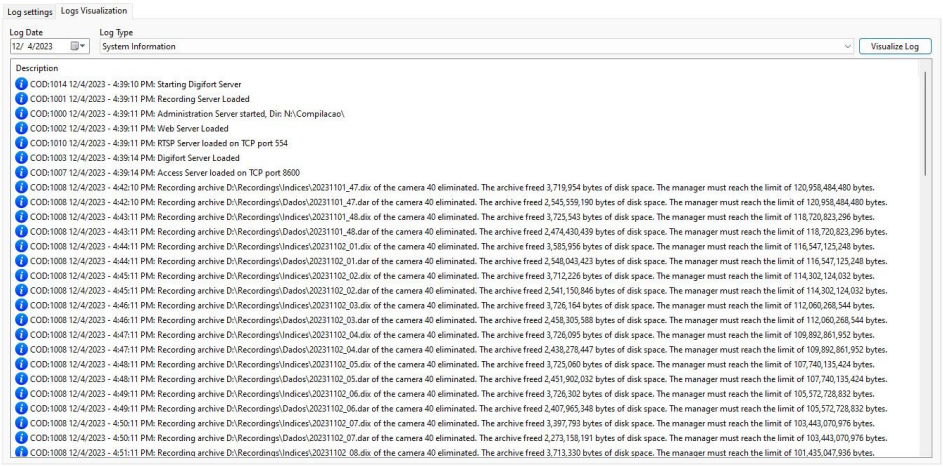
- **Activate system logs:** Enables or disables system logs.
- **Log Directory:** Select the directory where alert and event logs will be saved.
- **Delete logs older than X days:** Deletes old logs, specified by the number of days entered.
- **Event log options:**
  - **System information:** This log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

21.1.2 How To View System Logs

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

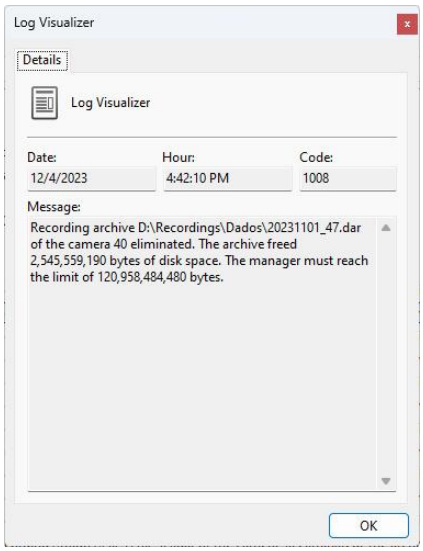
© 2002 - 2024 by Digifort. All rights reserved.

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



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

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



21.2 Event Logs

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

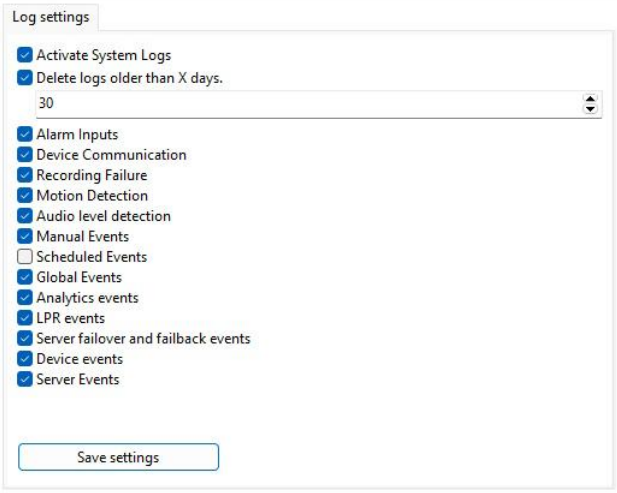
21.2.1 How To Configure Event Logs

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

© 2002 - 2024 by Digifort. All rights reserved.

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

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



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

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

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

21.2.2 How To View Event Logs

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

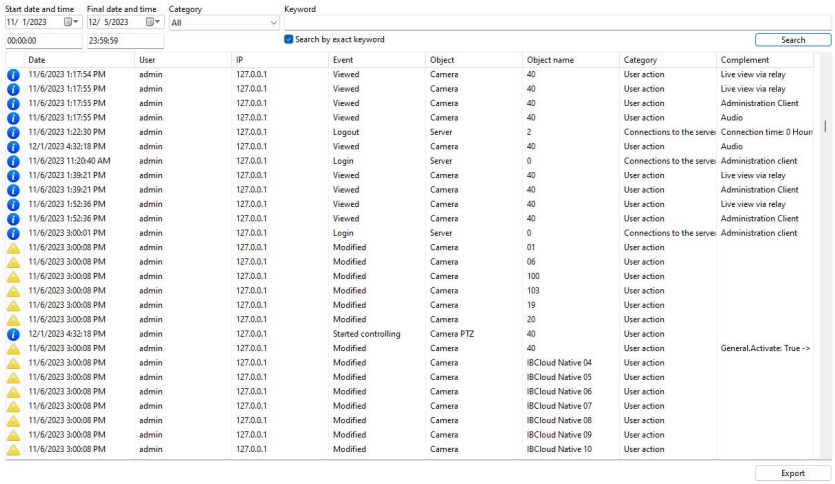
21.3 Audit

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

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

© 2002 - 2024 by Digifort. All rights reserved.

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

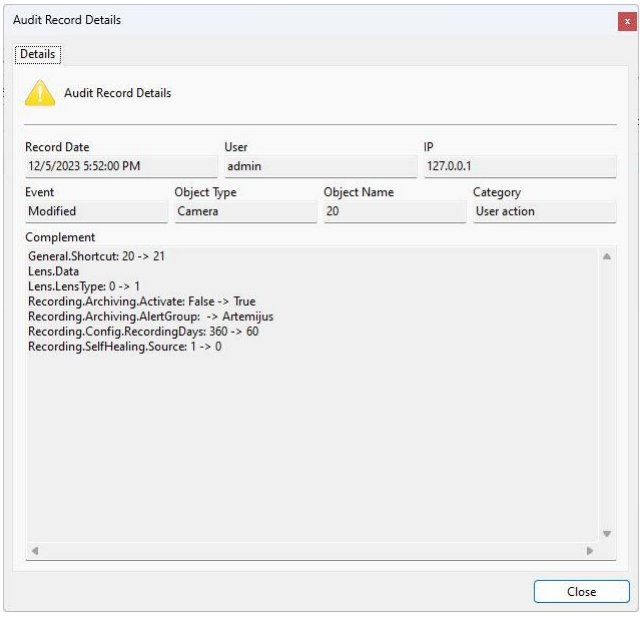


The audit system maintains two categories of information in the database: **User actions in the system** and **Connections with the server**.

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

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

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



© 2002 - 2024 by Digifort. All rights reserved.

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

© 2002 - 2024 by Digifort. All rights reserved.

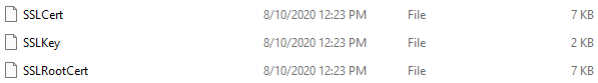
Chapter XXII

22 SSL Certificates

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

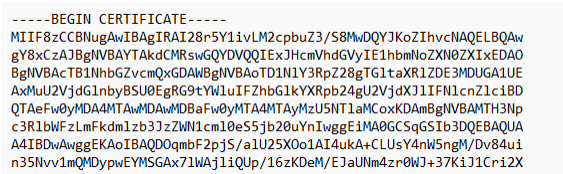
The system provides a standard, self-signed certificate, which must be replaced with your certificate.

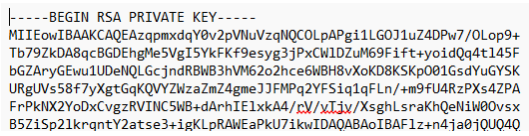
The certificate files are located in the **HTTP** subfolder in the case of the VMS Server, or in the installation root folder in the case of the other services (Analytics, LPRI, Mobile Camera, Live Witness, etc...).



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

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





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

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

22.1 How to Generate a Self-Signed Certificate

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

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

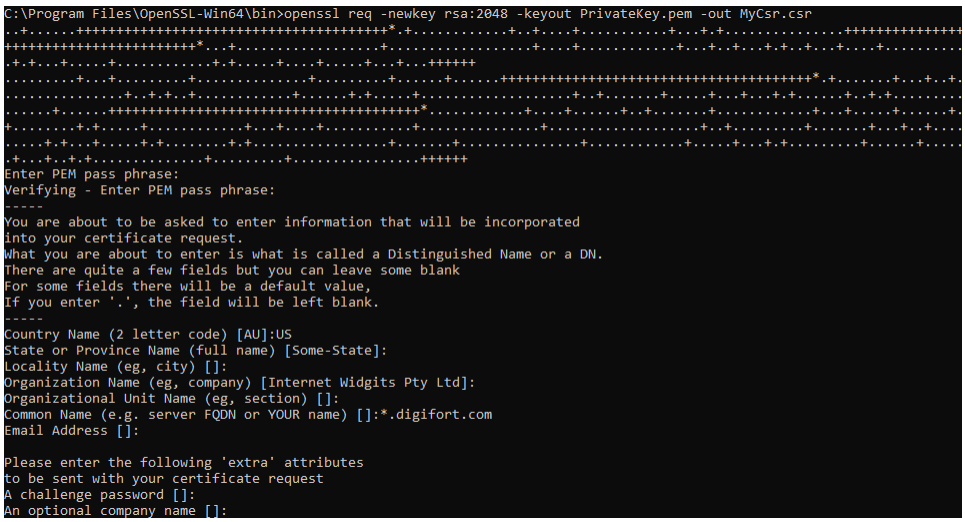
1. Generate a Certificate Signing Request (CSR) along with the private key.

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

© 2002 - 2024 by Digifort. All rights reserved.

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

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



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

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

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

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

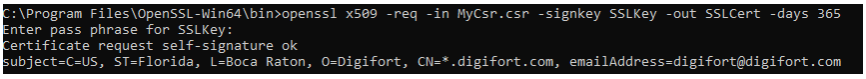
2. Generating the Self-Signed Certificate

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

© 2002 - 2024 by Digifort. All rights reserved.

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

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



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

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

3. Root certificate

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

```
copy SSLCert SSLRootCert
```

4. Private Key

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

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

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

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

22.2 Converting Certificates to PFX Format

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

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

1. Extract the private key

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

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

© 2002 - 2024 by Digifort. All rights reserved.

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

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

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

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

2. Extract the certificate

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

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

3. Root certificate

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

```
copy SSLCert SSLRootCert
```

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

© 2002 - 2024 by Digifort. All rights reserved.

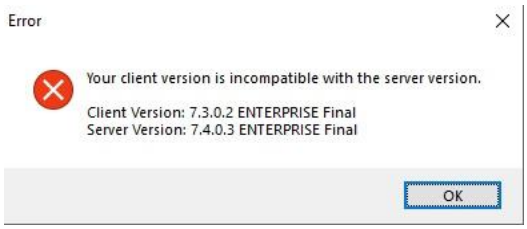
Chapter

23 Clients auto-update

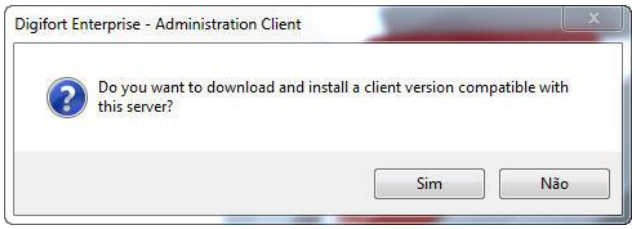
In a server version update, the system enables automatic updating of Administration and Monitoring Clients.

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

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

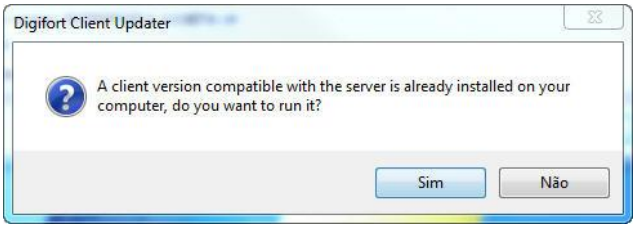


When clicking **OK** a dialog box will appear with the following question: **Do you want to download and install a client version compatible with this server?**



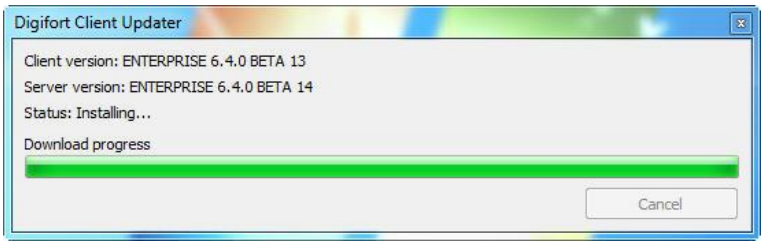
By clicking on **No** the dialog box will close and nothing will happen. If you click **Yes**, the system will automatically install the compatible client versions on the computer.

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

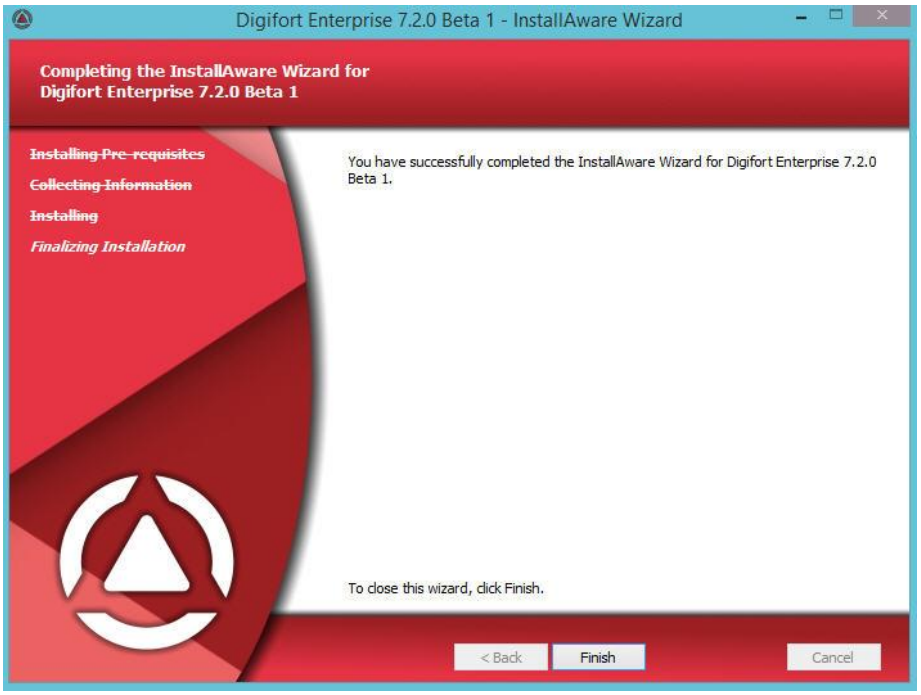


If you click **Yes** the client will run. Otherwise the client installation will continue. Clients installation will be downloaded from the server through the tool displayed below:

© 2002 - 2024 by Digifort. All rights reserved.



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



Note

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

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter

24 Database Maintenance

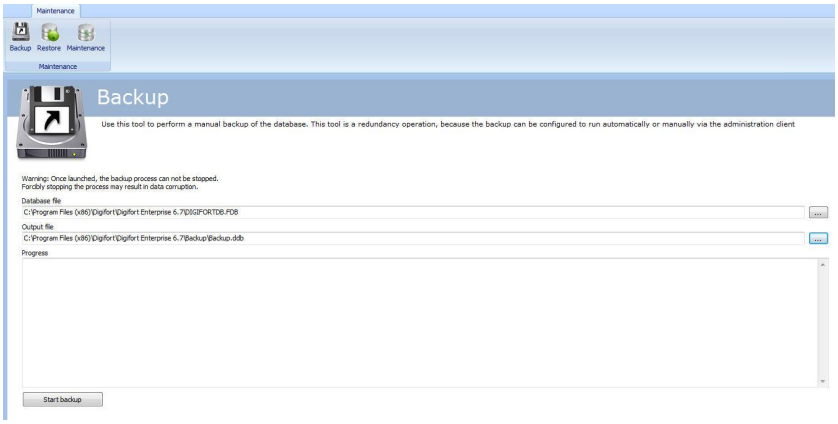
Through the database maintenance application you will be able to:

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

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

24.1 Backup

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



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

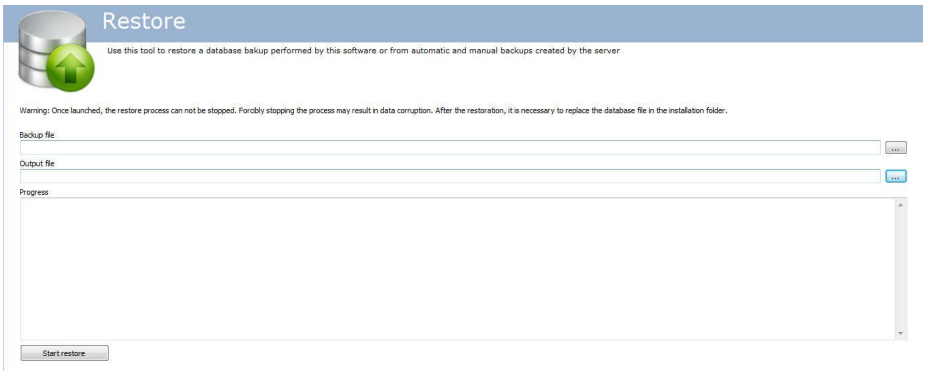
Database backup is saved in **.ddb** format and the current database format is **.FDB**. Thus, the only way to restore the backup is using this same software.

24.2 Restore

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

The following screen will be displayed:

© 2002 - 2024 by Digifort. All rights reserved.



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

24.3 Maintenance

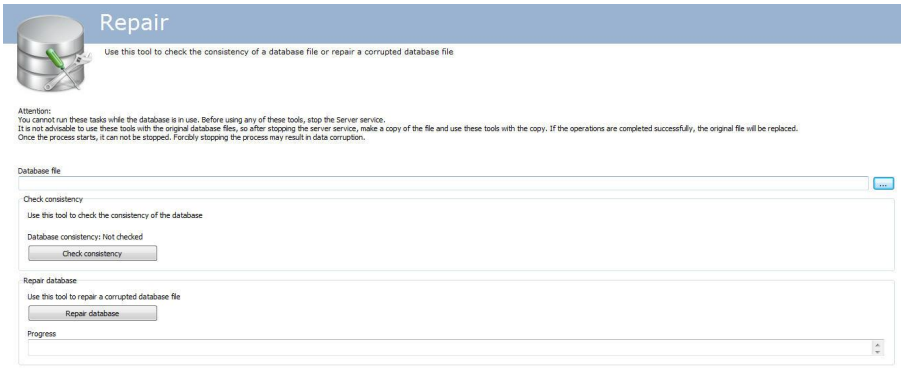
Use this option to check database consistency or fix database corruption issues.

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

Note

To perform maintenance, stop all system services.

The following screen will be displayed:



The screen has the following features:

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

© 2002 - 2024 by Digifort. All rights reserved.

Chapter XXV

25 Centralized Server List

In large installations with multiple monitoring stations and servers, registering and managing (adding or removing) servers in the Surveillance Client can be an extremely time-consuming task. To facilitate the management of these server records in the Surveillance Clients, it is possible to create a single list with the registration of all servers and when opening the Surveillance Client, it will download this list and register these servers locally (Only for the session current) automatically, so if you need to add a server, remove a server or even change the connection parameters of a server, you can do it once in the configuration file and all Surveillance Clients will be updated automatically the next time once they are started.

The registration of servers must be done in a script file with **.dssf** extension in **XML** format.

File syntax:

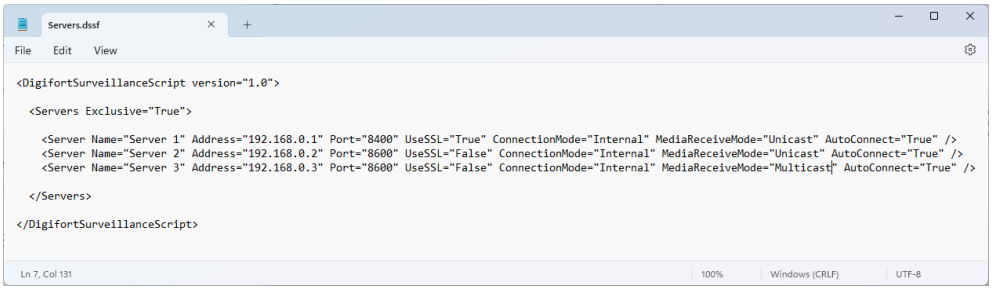
```
<DigifortSurveillanceScript version="1.0">
  <Servers Exclusive="True">

    <Server Name="SERVER_NAME_1" Address="SERVER_ADDRESS" Port="SERVER_PORT"
     UseSSL="True|False" ConnectionMode="Internal|External"
     MediaReceiveMode="Unicast|Multicast" AutoConnect="True|False" />

    <Server Name="SERVER_NAME_2" Address="SERVER_ADDRESS" Port="SERVER_PORT"
     UseSSL="True|False" ConnectionMode="Internal|External"
     MediaReceiveMode="Unicast|Multicast" AutoConnect="True|False" />

  </Servers>
</DigifortSurveillanceScript>
```

You can add as many servers as you want to this list, just by creating more records. See an example file below:



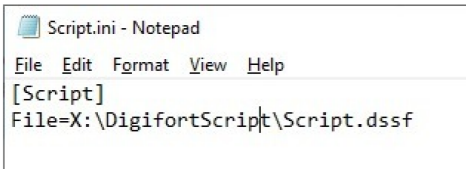
- **Name:** Provide a name for the server.
- **Address:** Provide the server address.
- **Port:** Provide the communication port. 8600 is the default port for normal connection and 8400 is the default port for SSL/TLS connection.
- **UseSSL:**
  - **True:** Enable the use of SSL/TLS (Don't forget to provide the SSL port, 8400).
  - **False:** Uses connection without SSL/TLS (Don't forget to provide the default port, 8600).
- **ConnectionMode:** Provide connection mode:
  - **Internal:** Select **Internal** if the Surveillance Client is running on a local network, or if the cameras are configured to transmit via Relay (Default).
  - **External:** Select **External** if the Surveillance Client is running outside the server's local network and the cameras are configured for direct transmission (No Relay).

© 2002 - 2024 by Digifort. All rights reserved.

- **MediaReceiveMode:** Select between **Unicast** and **Multicast** for the default media transmission mode.
- **AutoConnect:**
  - **True:** Select **True** for the Surveillance Client to automatically connect to this server when opened.
  - **False:** Select **False** so that the Surveillance Client does not connect to this server automatically when opening. The user must manually connect (by double-clicking on the server) to each server.

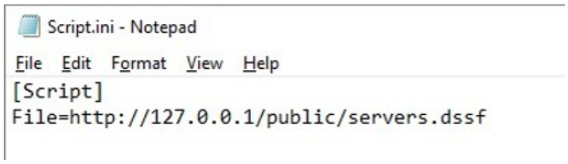
With the server registration file complete, you must now place it in a location where Surveillance Clients have access. You can use 2 options for this:

Shared Folder:
You can place the server registration file in a shared folder on the network, as long as all Monitoring Clients have access to this file. To instruct the Surveillance Client to download this file over the network, you must create a file called **Script.ini** and place this file within the client installation folder:



In this Script.ini file you will specify the path to the server registration file, as shown above.

Web Server:
You can place the server registration file on a Web Server, as long as all Surveillance Clients have access to this server. To instruct the Surveillance Client to download this file over the network, you must create a file called **Script.ini** and place this file within the client installation folder:



In the example above, the V Client will download the server registration file from the URL http://127.0.0.1/public/servers.dssf

You can use the File Server feature of the system's own embedded Web Server to provide the server registration file. See the Web Server File Server topic

© 2002 - 2024 by Digifort. All rights reserved.

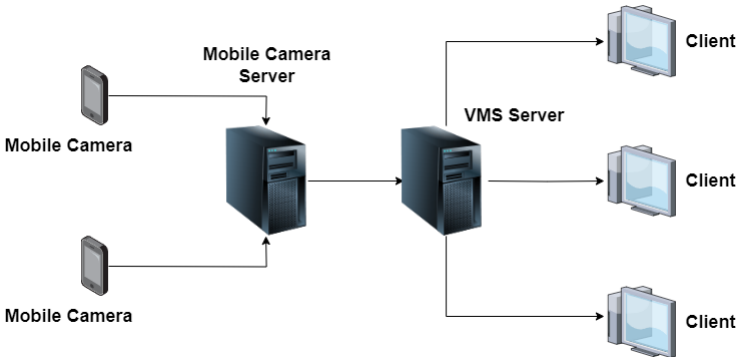
Chapter

26 Mobile Camera

Mobile Camera is an application that can be installed on cell phones and tablets running IOS (Apple) and Android (Google).

With this application you can turn your cell phone into a mobile remote camera and transmit live video to your VMS server via wireless or 3g/4g/etc connectivity.

In order for the VMS server to receive images from the Mobile Camera application, it needs an intermediary service (which can be running on the same VMS server or on a separate server), called Mobile Camera Server:



The Mobile Camera application, installed on the smartphone or tablet, will connect to the Mobile Camera Server and send the video. The Mobile Camera Server service will in turn forward the images to the VMS server, which will consider each cell phone as a camera registered in the system.

Each mobile device will be independently registered and identified on the VMS server and a camera license will be required for each device.

On the next topics you will see how to configure the Mobile Camera server, as well as how to register the camera on the VMS server to retrieve the images from the Mobile Camera server.

26.1 How to start the Mobile Camera Server service

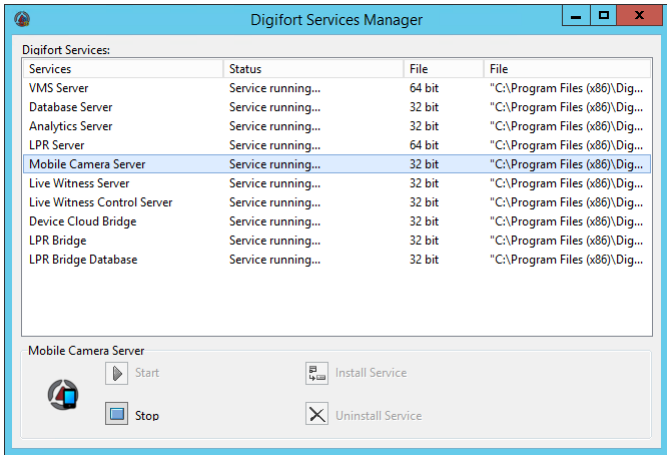
To start the Mobile Camera Server service, it must first be installed, follow the steps below to start the service correctly using the Service Manager:

1. Select the **Mobile Camera Server** service .

2. Click on **Install Service**.

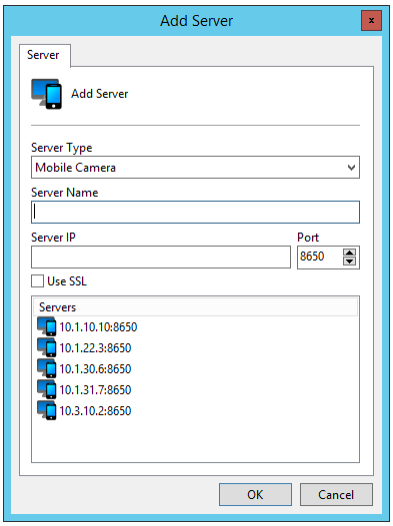
3. Click **Start** and wait for the server to start. The start-up process ends when the message "Service running..." appears in the status bar.

© 2002 - 2024 by Digifort. All rights reserved.



26.2 How to configure the servers to be managed

The first step in configuring a Mobile Camera server is to add it to the list of servers to be managed by the Administration Client.
To add a server, click on the **Mobile Camera Servers** tree and then on the **Add Server** button, opening the server registration screen, as shown below:

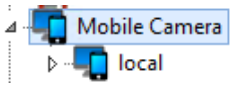


- **Server Name:** Enter the name of the server to be added. Once the data has been confirmed, the server name cannot be changed.
- **Server IP**: Enter the IP of the server to be managed.
- **Port:** Enter the port used to communicate with the server. By default the port is 8650 or 8450 for secure connection with SSL/TLS
- **Use SSL:** Use secure connection with SSL/TLS. Don't forget to specify the SSL/TLS connection port.
- **Servers:** This list shows all the Mobile Camera servers that the administration client has found on the network. By clicking on one of the servers, the **IP** and **Port** fields described above will be automatically filled in, and all that remains is to fill in the **Server Name** field to complete the registration.

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

Once the server has been added, it will be displayed in the **Settings** Menu, as shown in the figure below:

© 2002 - 2024 by Digifort. All rights reserved.

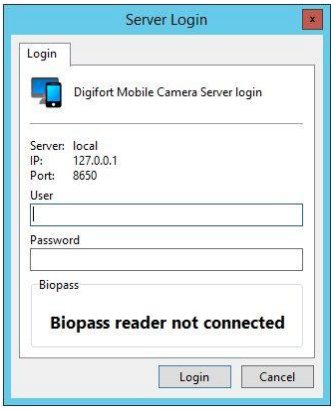


To change the parameters of an already saved server, right-click on the desired server and then click on **Change Parameters**. In the window that opens, change the data as necessary and click **OK**.

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

26.3 Configuring the Mobile Camera server

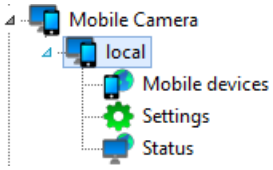
After adding the server, locate it in the Settings Menu and double-click on it. Once this is done, a user name and password will be required to access the server's settings, as shown in the figure below:



- **User:** Access user.
- **Password:** Access password.

Enter the username and password for accessing the server. If this is your first access to the system, enter the username admin and a blank password.

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

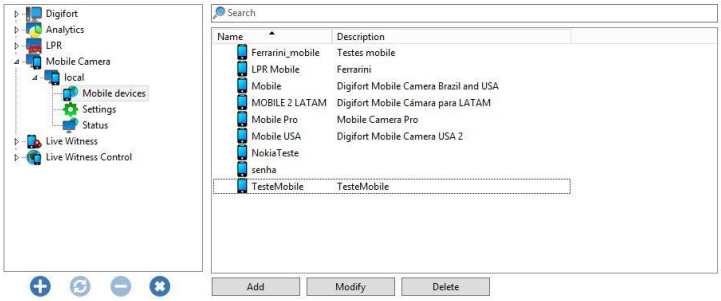


26.3.1 Mobile Devices

Every mobile device (iOS or Android cell phone or tablet) must be identified and connected to the Mobile Camera server. To do this, you must register the device on the server and give it a unique name. In the Mobile Camera app, you must use this name in your settings, thus linking the mobile device to the Mobile Camera server.

To register the devices on the server, click on the **Mobile Devices** option as in the image below:

© 2002 - 2024 by Digifort. All rights reserved.



To add a mobile device ,click **Add**. To change or delete, select the device you want and click on the corresponding button.

The registration screen will appear:

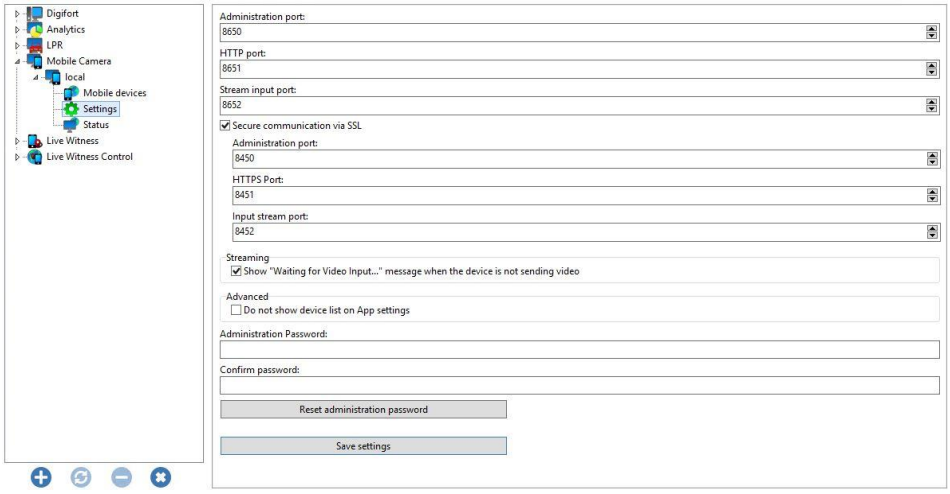
- **Name**: Enter a unique identifier for this device (This name must also be used in the app installed on this device).
- **Description**: Enter a description for this device, for easy identification and organization in the system.
- **Password**: Enter a security password for this device. You must set the same password in the app. This password is required to prevent any other device from connecting to your server.
- **Activate**: Activates or deactivates this device.

Click **OK** to register the device. Repeat this process for all the desired mobile devices.

26.3.2 Settings

To access the server settings, click on **Settings** as in the image below:

© 2002 - 2024 by Digifort. All rights reserved.



- **Admin Port**: Port used by the system to configure the Mobile Camera server.
- **HTTP Port**: HTTP port used for communication. The Mobile Camera app must be able to access this port.
- **Stream Input Port**: Port used to receive the video stream. The Mobile Camera app must be able to access this port.
- **Secure communication via SSL**: Activates secure communication via SSL / TLS channel for video transmission.
  - **Administration port**: Secure port used by the system to configure the Mobile Camera server.
  - **HTTPS Port**: HTTPS port used for communication. The Mobile Camera app must be able to access this port.
  - **Stream Incoming Port**: Secure port used to receive the video stream. The Mobile Camera app must be able to access this port.

- **Display message "Waiting for incoming video...":** With this option activated, when the camera is not sending video, Mobile Camera will generate a periodic video stream, with the message "Waiting for incoming video..." to be displayed in the Surveillance Client, thus informing the system operator that the video is not yet being transmitted.

- **Not displaying the list of devices in the app configuration**: The Mobile Camera app will list all the devices registered on the Mobile Camera server, which may not be desirable in some cases. Check this option to not display the device list in the app. In this case, the app operator will need to specify the device name manually.

- **Administration password: Administration** password for the Mobile Camera server.
- **Confirm password**: Confirm the password for registration.

- **Reset admin password**: Resets the admin user's admin password (Blank).
- **Save settings**: Saves the changed settings.

Important

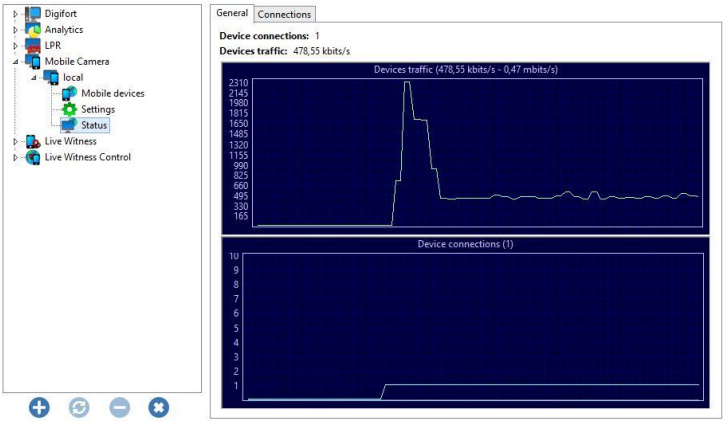
The ports must be cleared on the firewall of the network and servers involved for the system to function correctly.

26.3.3 Status

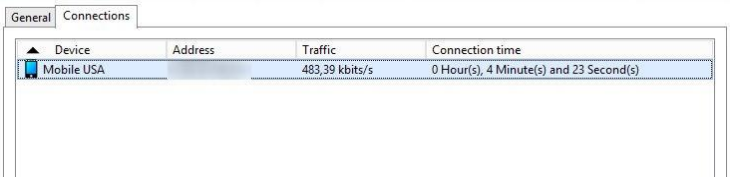
In Status we can view important information such as bandwidth consumed and connected devices.

© 2002 - 2024 by Digifort. All rights reserved.

To access it, click on **Status** as shown in the image below:



- **General**: The general tab will display graphs and general consumption information.
  - **Device Connections**: Number of device connections.
  - **Device Traffic**: Total bandwidth used by all connected devices.
  - **Traffic Graph**: Displays a continuous historical graph of the bandwidth consumption of connected devices.
  - **Connections Graph**: Displays a continuous historical graph of the number of connected devices.



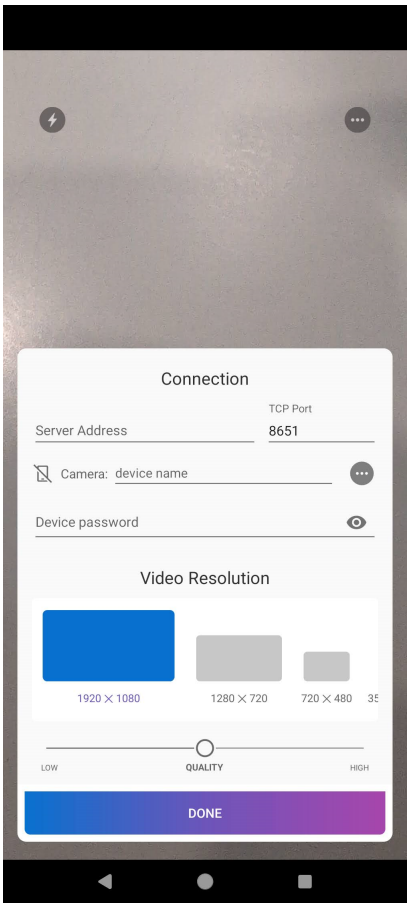
- **Connections**: The connections tab will display a list of all connected devices.
  - **Device**: Identification of the connected device.
  - **Address**: IP address of the device.
  - **Traffic**: Current bandwidth usage.
  - **Connection Time**: Total video transmission time.

26.4 Configuring the Application

First download the **Digifort Mobile Camera Pro** app from Google Play or Apple Store and install it on your mobile device.

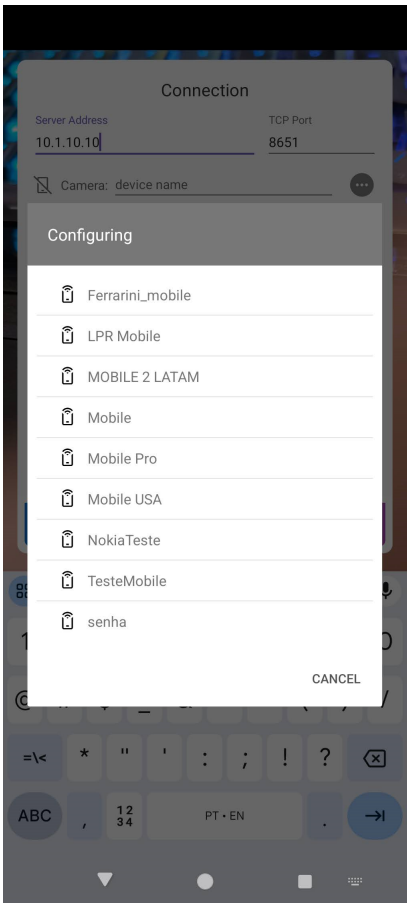
When you open the app for the first time, provide all the requested rights and the settings screen will appear:

© 2002 - 2024 by Digifort. All rights reserved.



- **Server Address**: Provide the IP or DNS of the Mobile Camera server.
- **Port**: Provide the HTTP Port of the Mobile Camera server.
- **Camera**: Click the "..." button to select a camera. If the Mobile Camera Server is configured not to display the list of devices, enter the name of the device registered with the Mobile Camera Server manually.

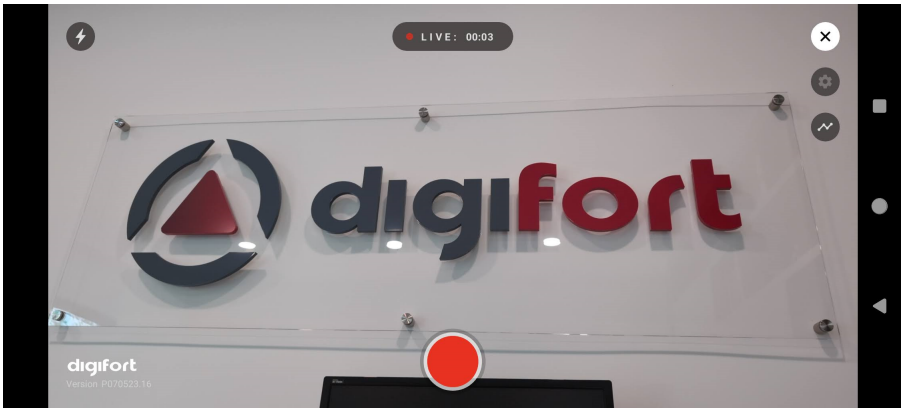
© 2002 - 2024 by Digifort. All rights reserved.



- **Password**: If a password was provided when registering the device with the Mobile Camera Server, enter the same password in this field.
- **Video Resolution**: Select the video resolution for streaming.
- **Quality**: Select the compression quality for the stream. Lower quality will use less bandwidth, making it ideal for internet transmissions.

Once the settings have been made, press the **DONE** button to return to the main screen.

On the main screen, press the bottom center button to start streaming video:



© 2002 - 2024 by Digifort. All rights reserved.

The image captured by the mobile device is sent to the Mobile Camera Server.

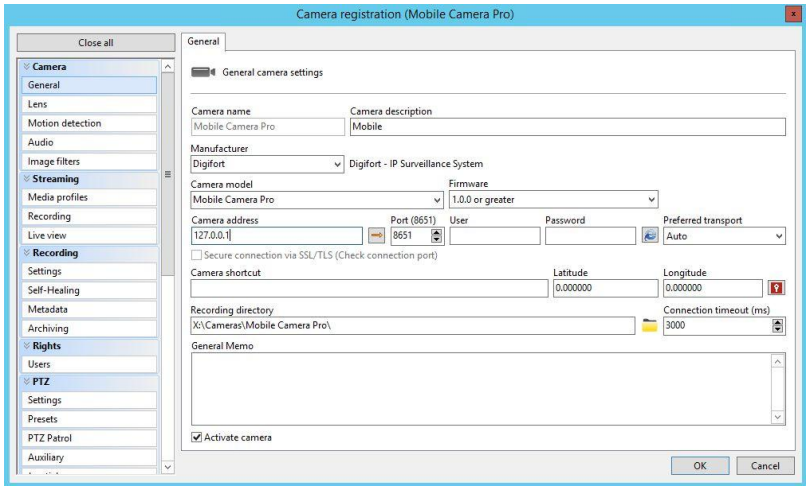
In the **top-left** corner, you have the option to **turn on the device's flashlight** if supported.
In the **top right** corner, there is a button to open the settings and details of the video stream**.**

If you want to stop the video stream, just press the streaming button (red button)**.**

26.5 Registering the Camera on the VMS Server

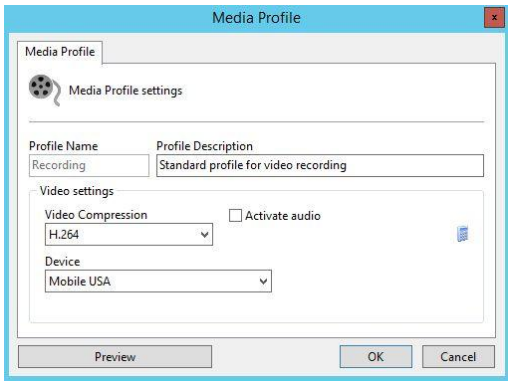
The last step is to register the cameras on the VMS server.

On the recording server, open the camera register and click **Add**. If you have any questions about registering cameras, see the chapter How to add a camera.



1. Enter the **Name** and **Description** that identifies your mobile device.
2. Under Manufacturer, choose **Digifort**.
3. Under Camera model, choose **Mobile Camera Pro**.
4. Under Camera address, choose the **IP** address of your Mobile Camera Server. See Configuring the Mobile Camera server.
5. If you haven't changed it, the default port for communication with the Mobile Camera Server is 8651.
6. Choose a directory for recording.

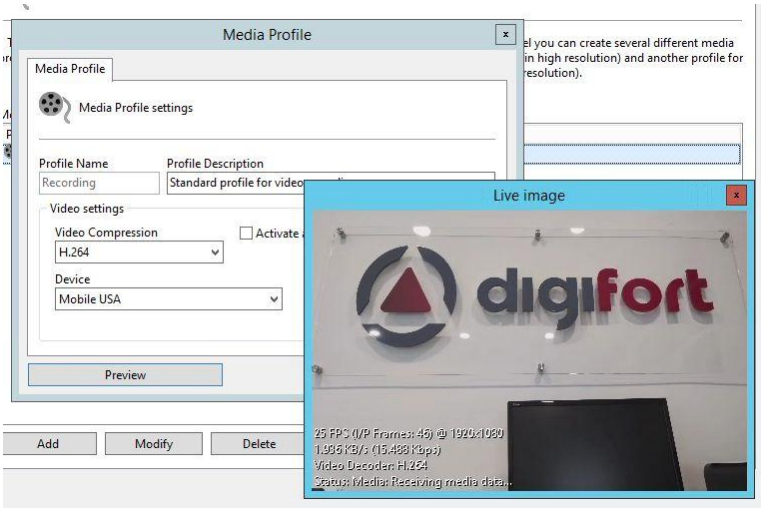
Now click on **Media Profiles** and double-click on the **Recording** profile:



© 2002 - 2024 by Digifort. All rights reserved.

1. The transmission supported by Mobile Camera Pro is H.264. Select H.264 compression
2. In the Device option, choose the device registered on the Mobile Camera Server that identifies the mobile device you want to register.

Click Preview to see the image being transmitted:



© 2002 - 2024 by Digifort. All rights reserved.