Digifort Explorer Manual
Administration Client
Version 7.3.0.0
Rev. A

© 2002 - 2020 by Digifort, all rights reserved

Index

Part I Welcome to Digifort Explorer Manual 8

1 Screen Shots ... 8
2 For whom this manual is intended ... 8
3 How to use this manual ... 8
4 Prerequisites ... 8

Part II Digifort Services Administrator 11

1 How to execute the Digifort Services Administrator ... 11
2 How to initiate the Digifort Server service ... 12
3 How to stop the Digifort Server service ... 13

Part III Basic functions of the Administration Client 15

1 How to execute the Administration Client ... 15
- Add Server ... 15
- Modify Server ... 15
- Delete Server ... 16
- Disconnect from server ... 16
- About Digifort ... 16
- How to configure the servers to be administrated ... 16

2 How to connect a management server ... 17

Part IV Licensing Digifort 21

1 How to configure the licenses ... 21
- How to add a license ... 23
- How to send data for registration ... 24
- How to install licenses via Online Licenses ... 26
- How to install licenses via license files ... 26
- Enabling a temporary license ... 27

Part V Registering Digifort 30

1 How to register Digifort ... 30
2 Registering Digifort Online ... 32
3 Registering Digifort Offline ... 33

Part VI Recording Server 36

1 How to add a camera ... 36
- Camera ... 37
  - General ... 37
  - Lenses ... 42
  - Motion Detection ... 45
    - Use motion detection via software ... 45

© 2002 - 2020 by Digifort, all rights reserved

Auto desativar detecção de movimento durante o PTZ //OLD: Auto deactivate motion detection during PTZ ... 49
Use motion detection by external notification ... 49
Configuration ... 50
Digifort configuration ... 50
Camera configuration ... 51
Notification type ... 54
Notification of Start and End ... 54
Notificação Instantânea ... 54
Testing the configuration ... 55
Motion end detection interval ... 55
Audio ... 56
Streaming ... 56
Media profiles ... 57
How the Media Profiles save network bandwidth ... 58
How to add Media Profiles ... 59
How to visualize the functioning of the configured media profile ... 59
Calculator for disk space usage ... 60
Audio ... 64
Recording ... 65
Buffer de Snapshot ... 66
Live View ... 67
How to configure the visualization of the camera ... 67
This camera will be accessed by the client via relay server ... 67
Private IP address ... 67
Private IP port ... 68
Public IP address ... 68
Public IP port ... 68
User and Password ... 68
Connection timeout (in MS) ... 68
Media profile ... 68
Media profile for access via mobile ... 69
Recording ... 69
Type of recording ... 70
Recording Cycle ... 70
Rights ... 70
Users ... 71
PTZ ... 71
Configurations ... 71
Activate the PTZ control for this camera ... 72
Use the device's PTZ features ... 72
Use the device's COM port for the system to carry out PTZ functions directly ... 72
Use of PTZ ... 73
Agendamento de Operação ... 73
Presets ... 74
How to configure the Presets Control ... 74
How to create a preset ... 76
Events ... 78
Communication ... 78
Communication failure event ... 78
Connection restoration event ... 79
Devices failure report ... 79
Recording failure ... 80

© 2002 - 2020 by Digifort, all rights reserved

Event Variables ... 80
How to configure the alarm actions ... 84
Send an e-mail message to a group of persons in the case of an alarm ... 86
Sound an alarm in the Surveillance Client ... 88
Send instant message to the operator of the computer ... 89
Enable or disable system objects ... 89
Camera management functions ... 90
Activate camera ... 91
Disactivate camera ... 91
Duplicate camera ... 91
Connection ... 91
Configuração PTZ em massa ... 92
Type of recording ... 92
Relay ... 93
Multiple Camera Recording Directory Change ... 93
Media Profiles ... 94
Media Profiles ... 94
Mobile viewing media profile ... 95
Viewing media profile ... 95
Recording media profile ... 95
Grant Rights ... 95
Deny Rights ... 95
Delete Cameras ... 95
Locating and registering cameras automatically ... 96
Registration of one device only ... 99
Registration of various devices ... 99
Importar objetos de outros servidores ... 101
Multichannel device registration ... 102
Registering a DVR ... 103
2 Camera Groups ... 107
3 Column Organization ... 111
4 Exporting Data from the Recording Server ... 112
5 Monitoring recording server status ... 113
Monitorando o status de câmeras individualmente ... 115
Conexão de Gravação ... 115
Conexões ... 116
Disco ... 117
Exportação de dados na tela de Status ... 118
Part VII Alerts and Events 120
1 How to access the Alerts and Events ... 120
How to configure the contacts ... 120
How to configure the contact groups ... 121
Part VIII User administration 124
1 Administrating users ... 124
Monitoring user activity ... 125
2 Adding, modifying and excluding users ... 126
User data ... 127
Force use of Strong Password ... 129
Weak Password Alert ... 130

© 2002 - 2020 by Digifort, all rights reserved

2-Factor Authentication ... 130
User rights ... 131
Video Search and Playback ... 132
Surveillance Views ... 132
System Cameras ... 132
Alarm Devices ... 133
Alarms ... 133
System Users ... 133
Alerts and Events ... 133
Server ... 133
Surveillance Client Features ... 134
Groups Inquiry ... 134
Rights Inquiry ... 135
User general observations field ... 135
3 User administration functions ... 136
Reset password ... 137
Login schedule ... 137
Login options ... 137
Block account ... 138
Unblock account ... 138
Account expiration ... 138
Rights ... 138
Give rights ... 138
Deny rights ... 138
Features ... 138
Policies ... 138
4 Adding, altering and excluding Groups ... 138
Group rights ... 141
Surveillance Client Features ... 141
Rights Inquiry ... 142
Part IX Configurations 144
1 Global Configurations ... 144
General Configurations ... 144
Recordings ... 145
Multicast ... 146
Backup ... 148
Restoring backups of Digifort ... 149
Database ... 150
STMP Configurations ... 151
Disk Limits ... 152
Network Units ... 153
How to add a network unit ... 154
2 Server health monitoring event ... 156
Part X Server Information 158
1 Disk Usage ... 159
2 Monitoring by graphics ... 160
Part XI Web Server 162
1 How to access the configurations of the Web Server ... 162

© 2002 - 2020 by Digifort, all rights reserved

Part XII Servidor RTSP 164

1 Status ... 164
2 Configurations ... 166

Part XIII System Logs 168

1 How to access the system logs ... 168
2 How to visualize the event logs ... 170
3 How to configure the event logs ... 171
Activate system logs ... 172
Delete logs older than X days ... 172
Event log options ... 172
Failure in communication with the devices ... 173
Failure in recording ... 173
How to visualize the event logs ... 173
4 Audit ... 173
How to access Audit ... 173
Viewing the Logs ... 174

Part XIV Automatic Client update 177

Part XV Maintaining the Database 181

1 Backup ... 181
2 Restore ... 182
3 Maintenance ... 182

Part XVI Digifort Mobile Camera 185

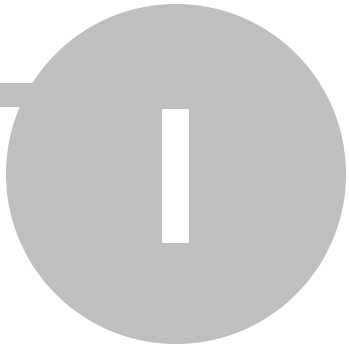
1 Registering the Mobile Camera Server ... 185
2 Configuring the Mobile Camera Server ... 187
Configurations ... 187
Status ... 188
Mobile devices ... 190
3 Configuring the application ... 192
4 Registering the camera ... 197

Part XVII Centralized server list 202

Index 0

© 2002 - 2020 by Digifort, all rights reserved

Chapter



1 Welcome to Digifort Explorer Manual



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

1.1 Screen Shots

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

1.2 For whom this manual is intended

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

1.3 How to use this manual

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

Important:

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

1.4 Prerequisites

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

© 2002 - 2020 by Digifort, all rights reserved

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter



2 Digifort Services Administrator

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

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

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

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

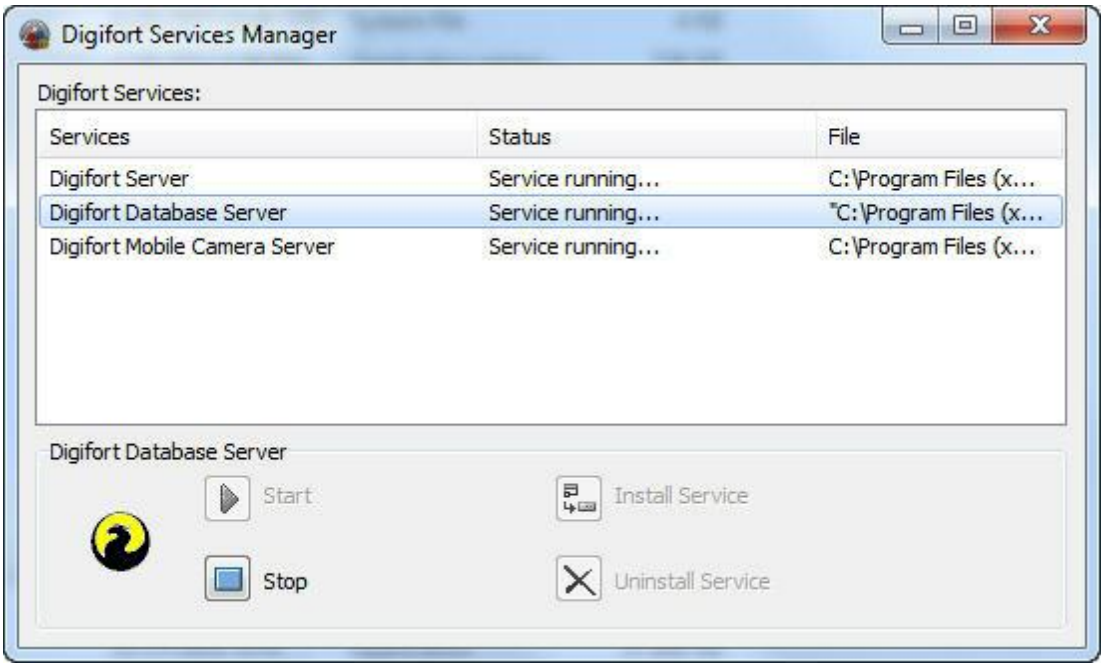
Note

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

2.1 How to execute the Digifort Services Administrator

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

© 2002 - 2020 by Digifort, all rights reserved



The Services Administrator offers the following functions:

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

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

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

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

2.2 How to initiate the Digifort Server service

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

1. Select the service “Digifort Server”

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

© 2002 - 2020 by Digifort, all rights reserved

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

Note

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

2.3 How to stop the Digifort Server service

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

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter



3 Basic functions of the Administration Client

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

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

3.1 How to execute the Administration Client

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



The Administration Client offers the following initial configurations:



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

3.1.1 Add Server



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

3.1.2 Modify Server



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

© 2002 - 2020 by Digifort, all rights reserved

3.1.3 Delete Server



Delete Server: Delete selected server.

3.1.4 Disconnect from server



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

3.1.5 About Digifort

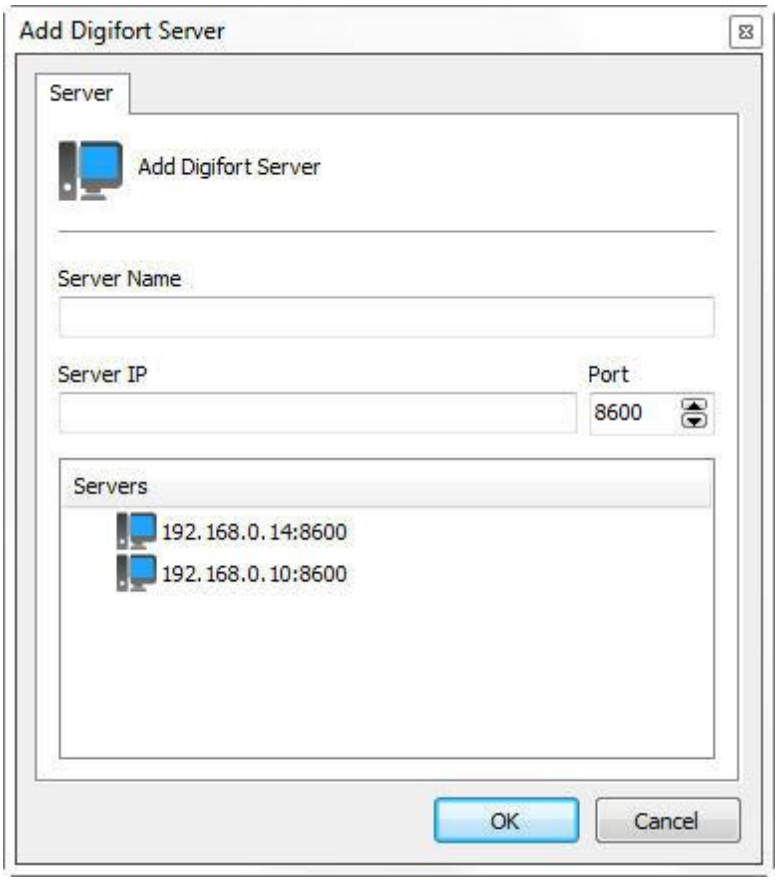


About: Show information about current Digifort version.

3.1.6 How to configure the servers to be administrated

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

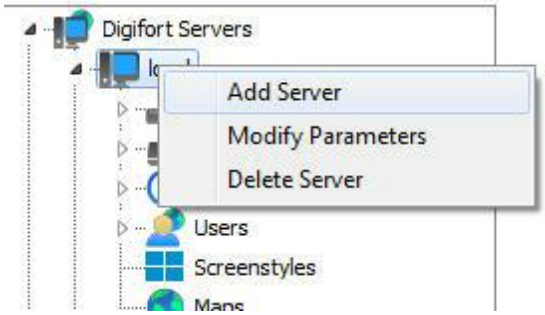
To add a server, click on the **Add** Server button, opening the server registration screen, as shown in the picture below



© 2002 - 2020 by Digifort, all rights reserved

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

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



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

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

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

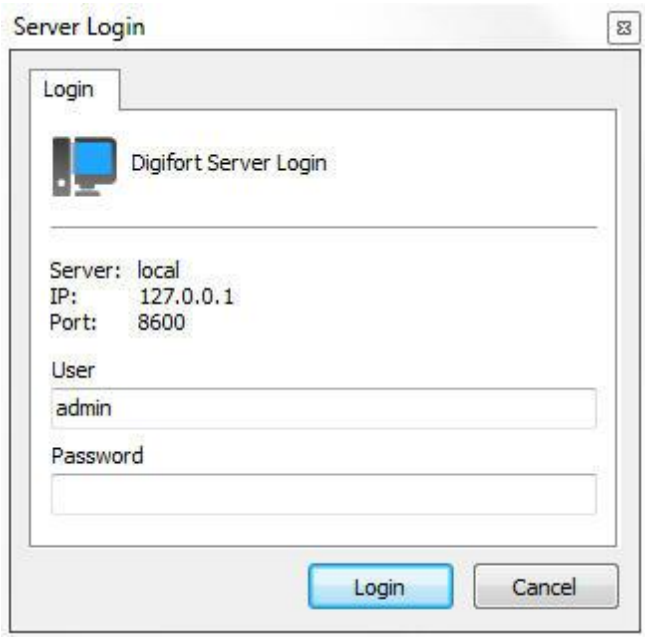
Tip

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

3.2 How to connect a management server

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

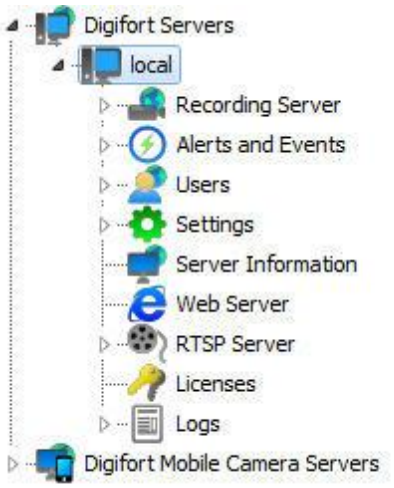
© 2002 - 2020 by Digifort, all rights reserved



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

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

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



Note

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

© 2002 - 2020 by Digifort, all rights reserved

the system.

© 2002 - 2020 by Digifort, all rights reserved

Chapter IV

4 Licensing Digifort

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

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

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

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

Tip

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

Important

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

4.1 How to configure the licenses

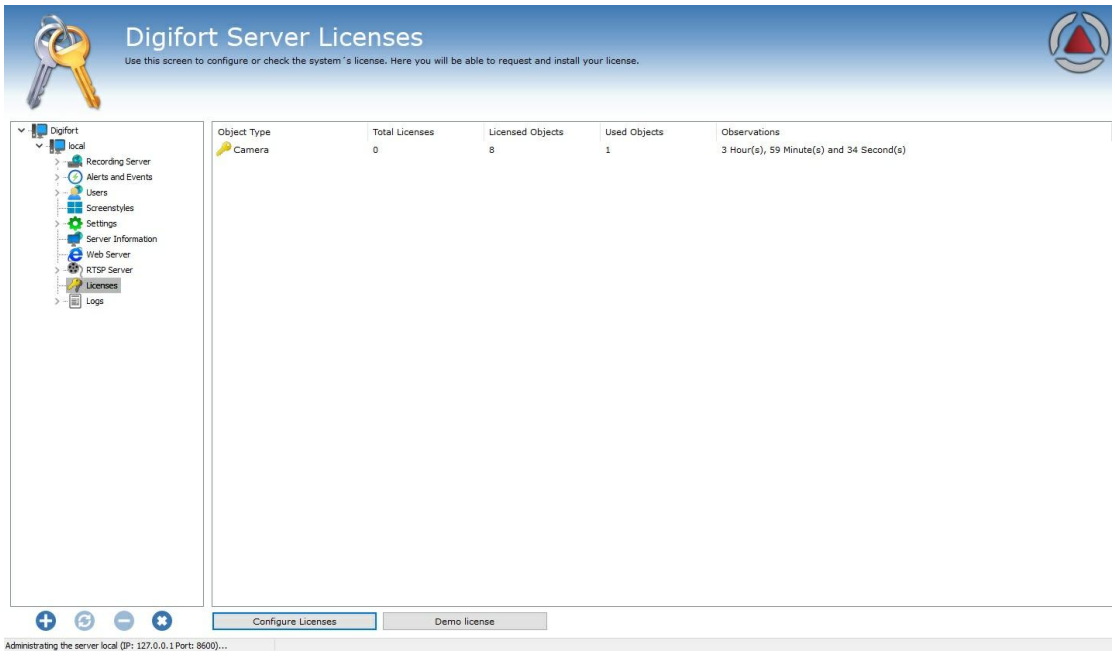
Before you start your server, check if the Hardkey that is sold together with the software is correctly connected to your machine.

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



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

© 2002 - 2020 by Digifort, all rights reserved



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

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

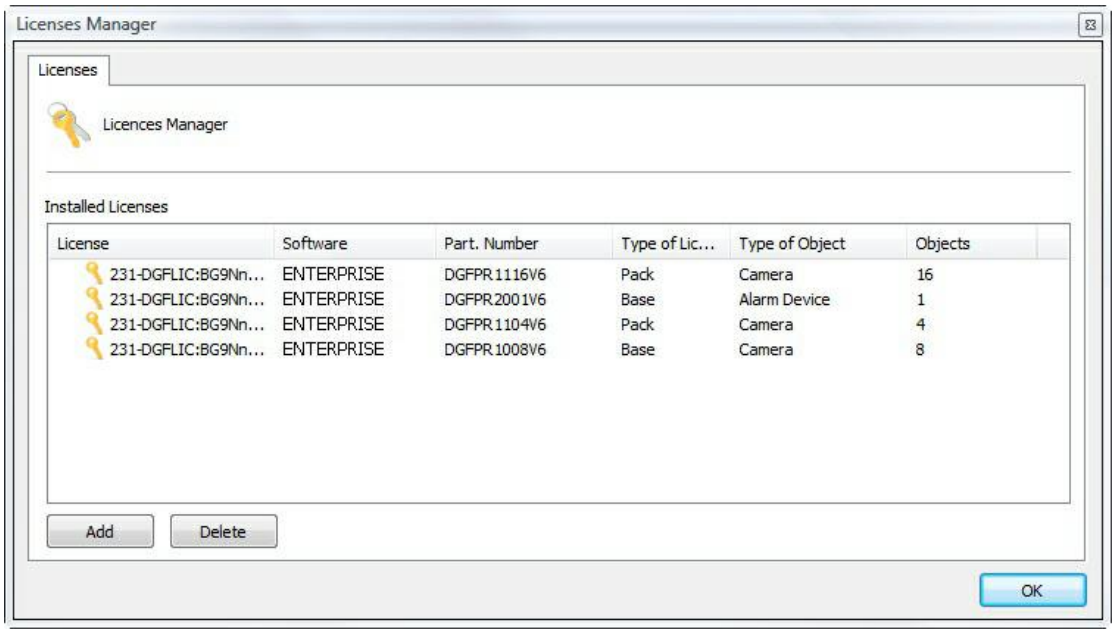
Types of licenses:

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

To learn more about licensing, see your dealer.

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

© 2002 - 2020 by Digifort, all rights reserved



In this screen, all licenses installed on the server are displayed. To add a license, click on the **Add** button and to remove a license, select the desired license and click on the **Remove** button.

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

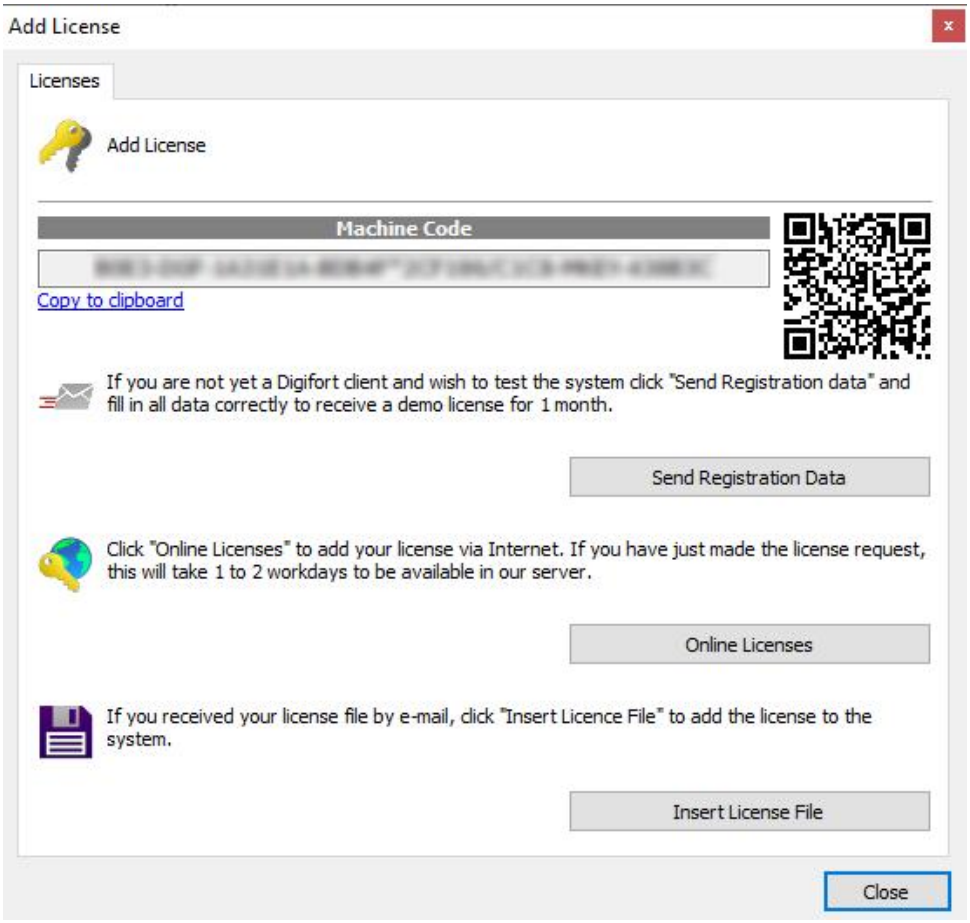
Note

If the base license is removed, the pack licenses will not be loaded and will automatically disappear from the screen. Pack licenses are only loaded if the base license is installed.

4.1.1 How to add a license

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

© 2002 - 2020 by Digifort, all rights reserved



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

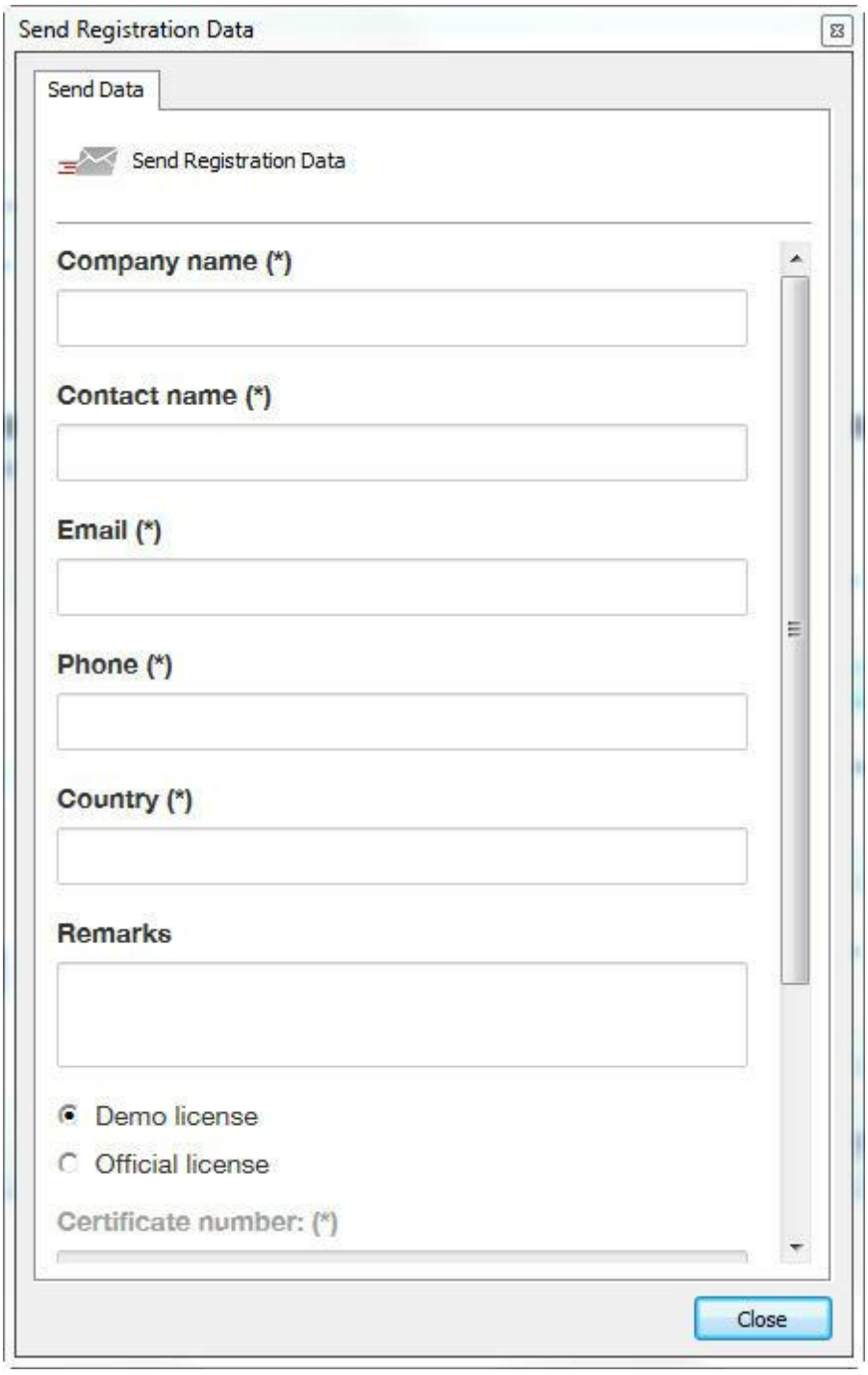
4.1.2 How to send data for registration

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

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

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

© 2002 - 2020 by Digifort, all rights reserved



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

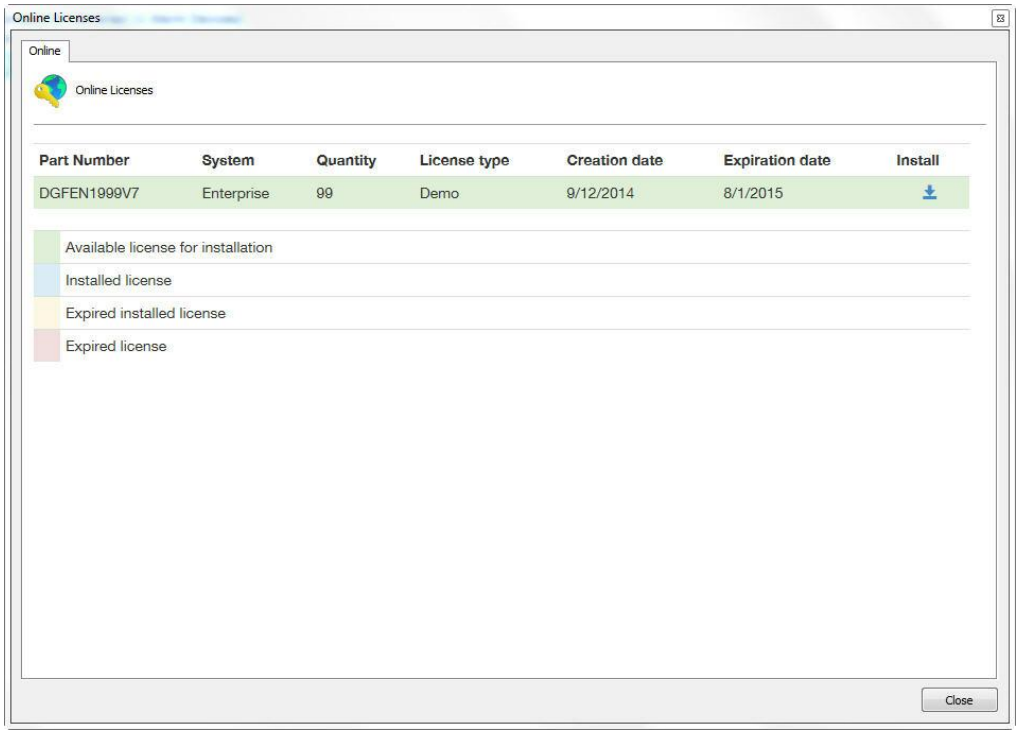
These instructions are also described in the following pages of this manual.

© 2002 - 2020 by Digifort, all rights reserved

4.1.3 How to install licenses via Online Licenses

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

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



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

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

4.1.4 How to install licenses via license files

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

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

© 2002 - 2020 by Digifort, all rights reserved

files.

Observation

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

4.1.5 Enabling a temporary license

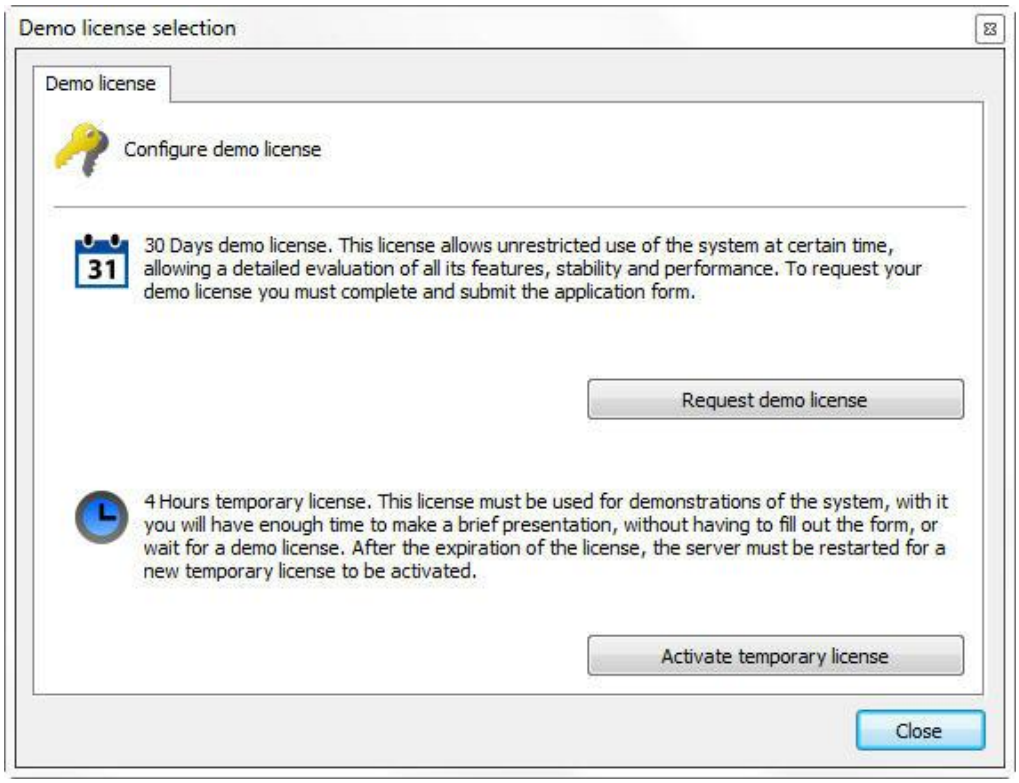
The temporary license feature was created to enable the software demo. Once the temporary license is activated, the software will work for two hours.

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

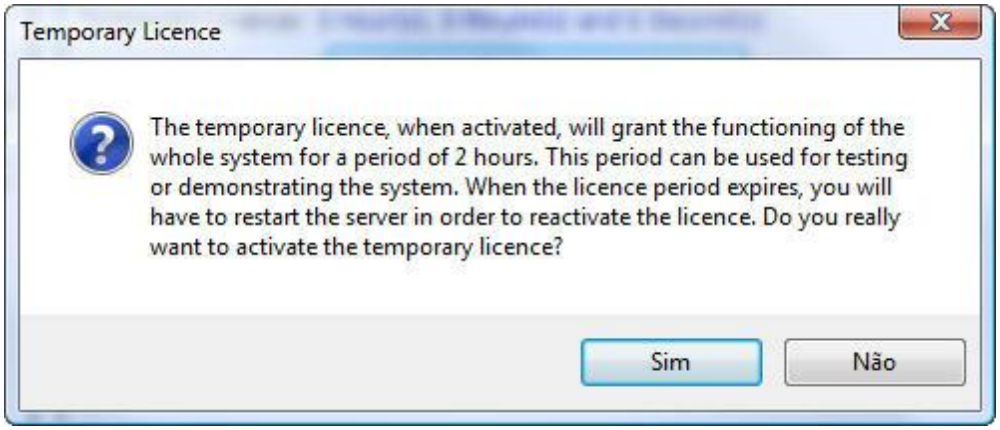


Then click on Activate temporary license as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



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



© 2002 - 2020 by Digifort, all rights reserved

Chapter V

5 Registering Digifort

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

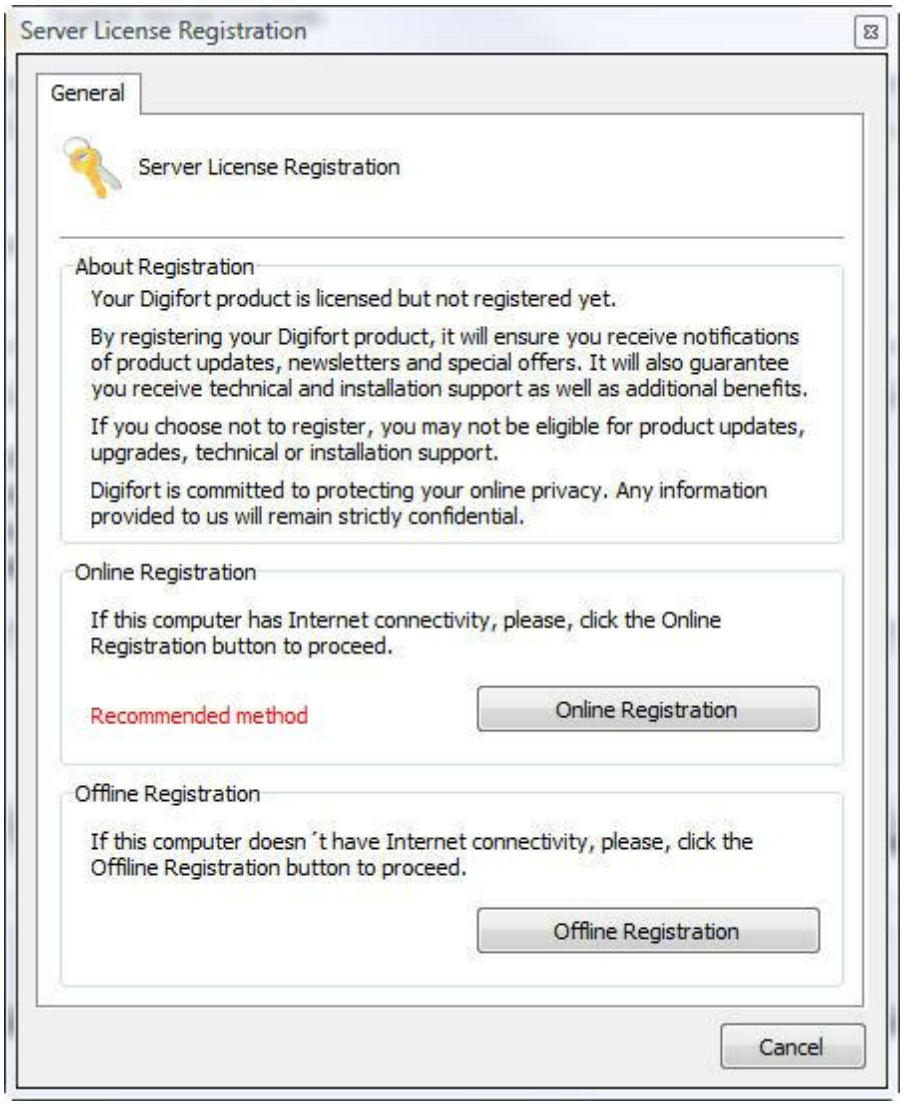
If you decide not to register, you will not be eligible for updates, upgrades, technical support or installation support.

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

5.1 How to register Digifort

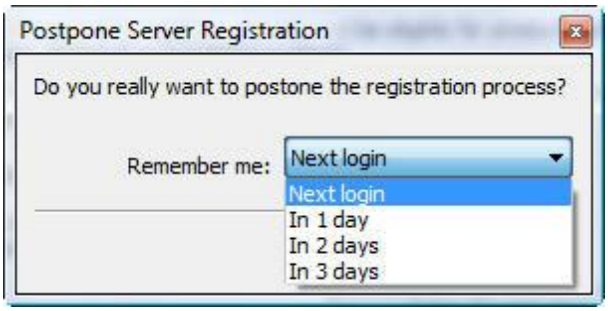
After inserting your usage license, the software's registration window will automatically be displayed, as shown in the figure below. To understand how to install licenses in Digifort, see Licensing Digifort.

© 2002 - 2020 by Digifort, all rights reserved



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

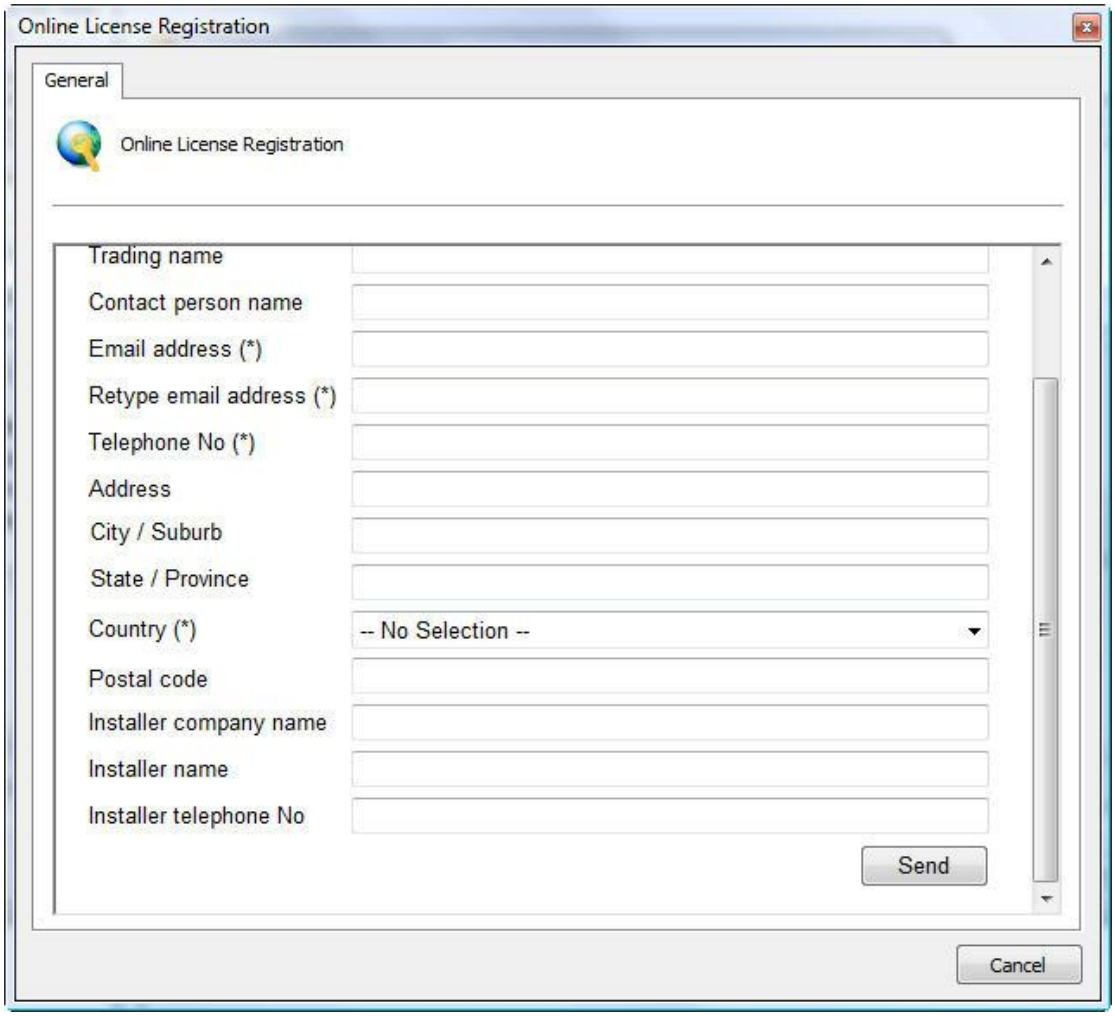
If you wish to register later, close this window and select the desired option, as shown below:



© 2002 - 2020 by Digifort, all rights reserved

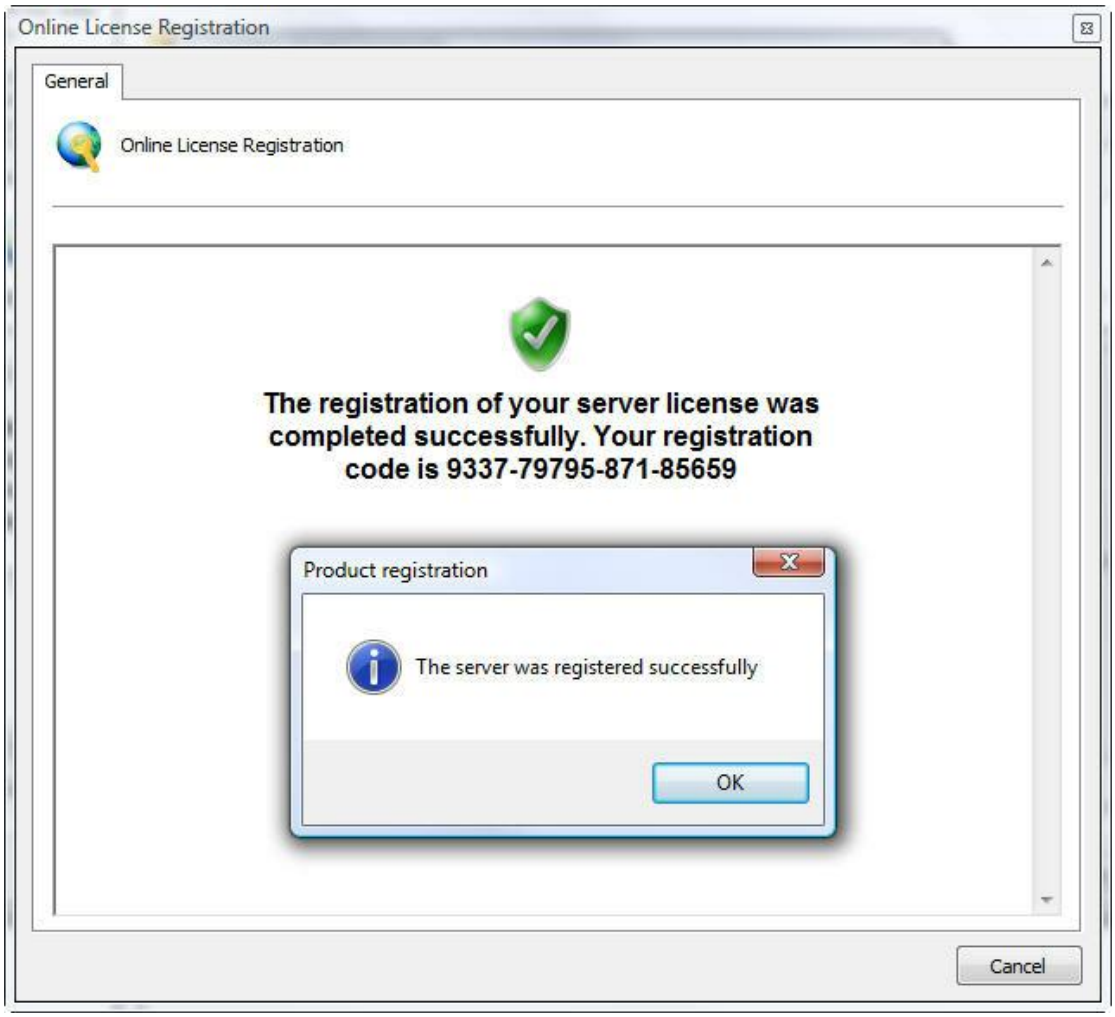
5.2 Registering Digifort Online

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



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

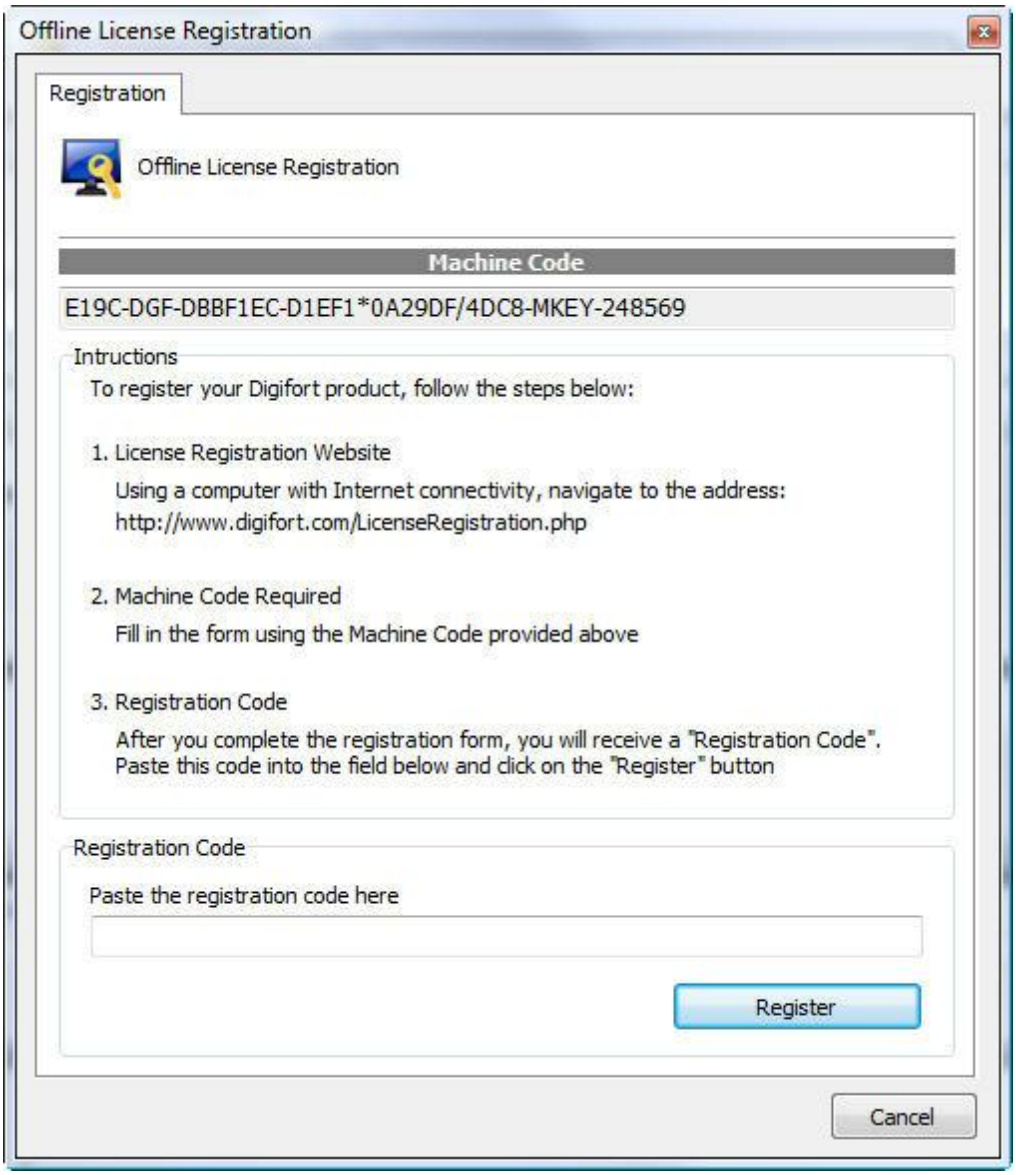
© 2002 - 2020 by Digifort, all rights reserved



5.3 Registering Digifort Offline

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

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

Chapter VI

6 Recording Server

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

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

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

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

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

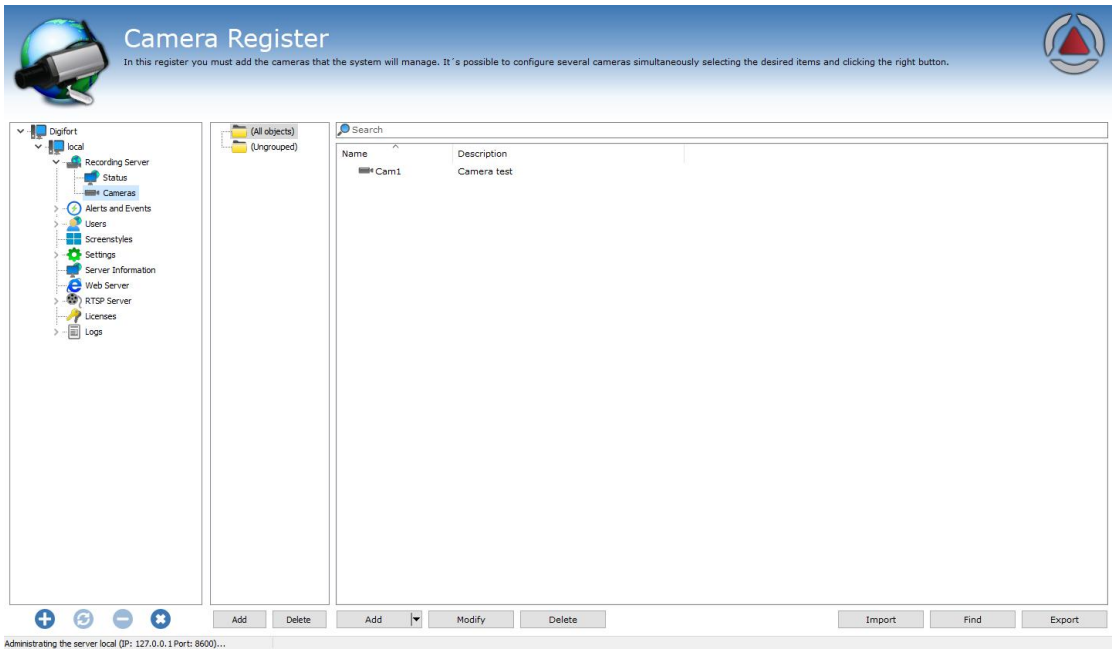
6.1 How to add a camera

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



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

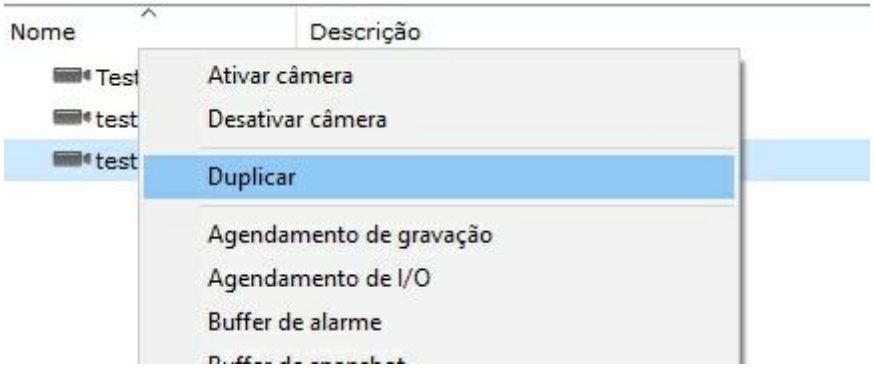
© 2002 - 2020 by Digifort, all rights reserved



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

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

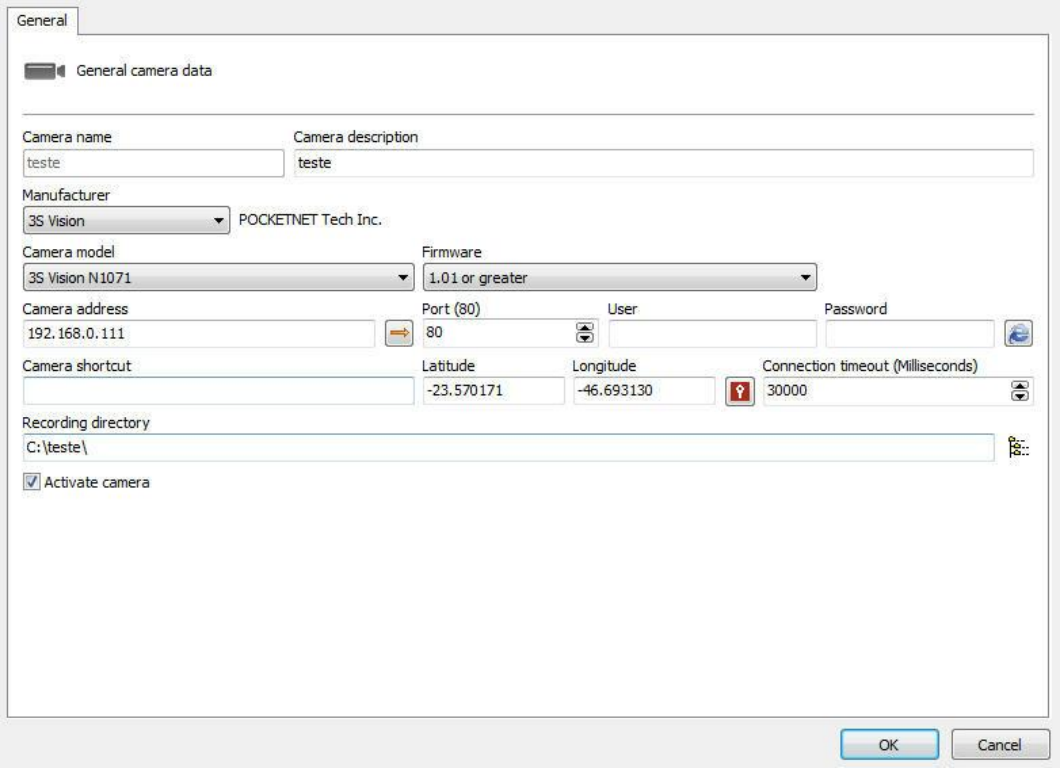
Tip: After adding a camera to the server, the administrator will be able to duplicate it, if necessary, by right-clicking on your registration and clicking on **Duplicate**



6.1.1 Camera

6.1.1.1 General

© 2002 - 2020 by Digifort, all rights reserved



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

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

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

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

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

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

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

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

© 2002 - 2020 by Digifort, all rights reserved

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

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

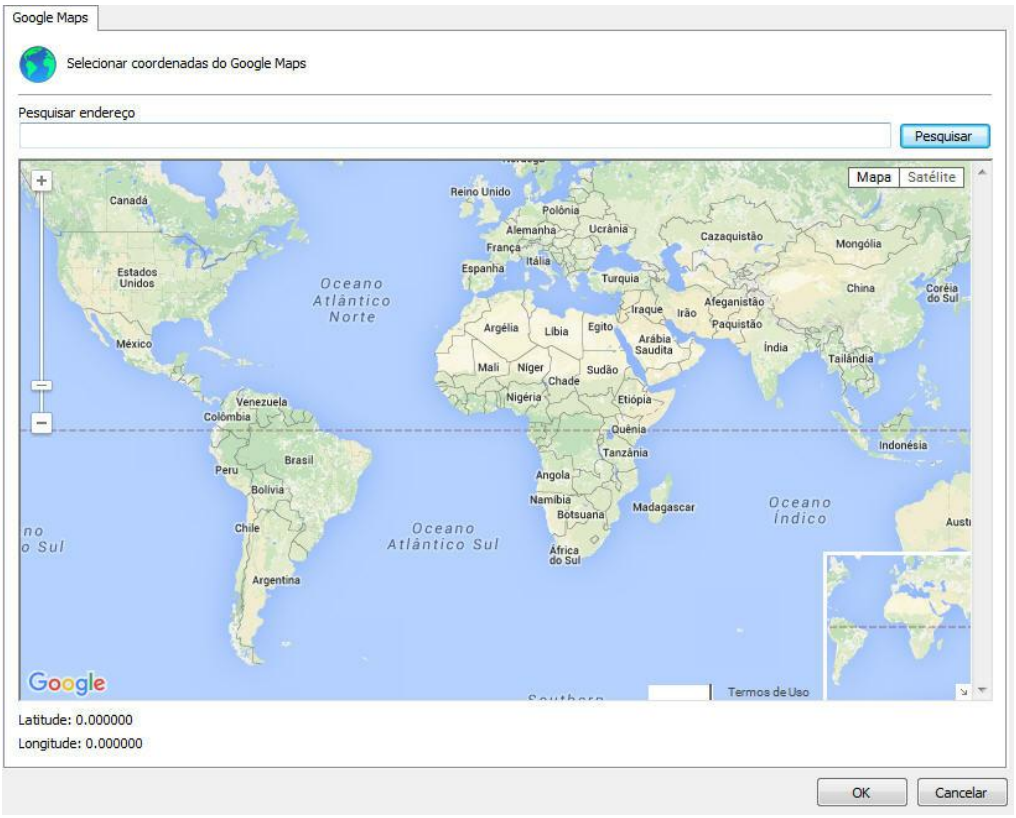
        - **Auto** - The transport used will usually be TCP, unless during the integration of the device the performance was not satisfactory, in that case transport will be done by UDP.
        - **TCP** - Transport will be done by TCP whenever possible.
        - **UDP** - Transport will be done by UDP whenever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

    - **Connection via SSL/TLS**: If the camera has a secure connection, check the box to activate the communication method using SSL between the camera and the server; it is important to check the port for such communication. If the camera does not have the feature, this option will appear as inaccessible.

- **Camera shortcut**: Choose a shortcut to the camera so that this camera can be quickly displayed on the surveillance client screen through this shortcut.

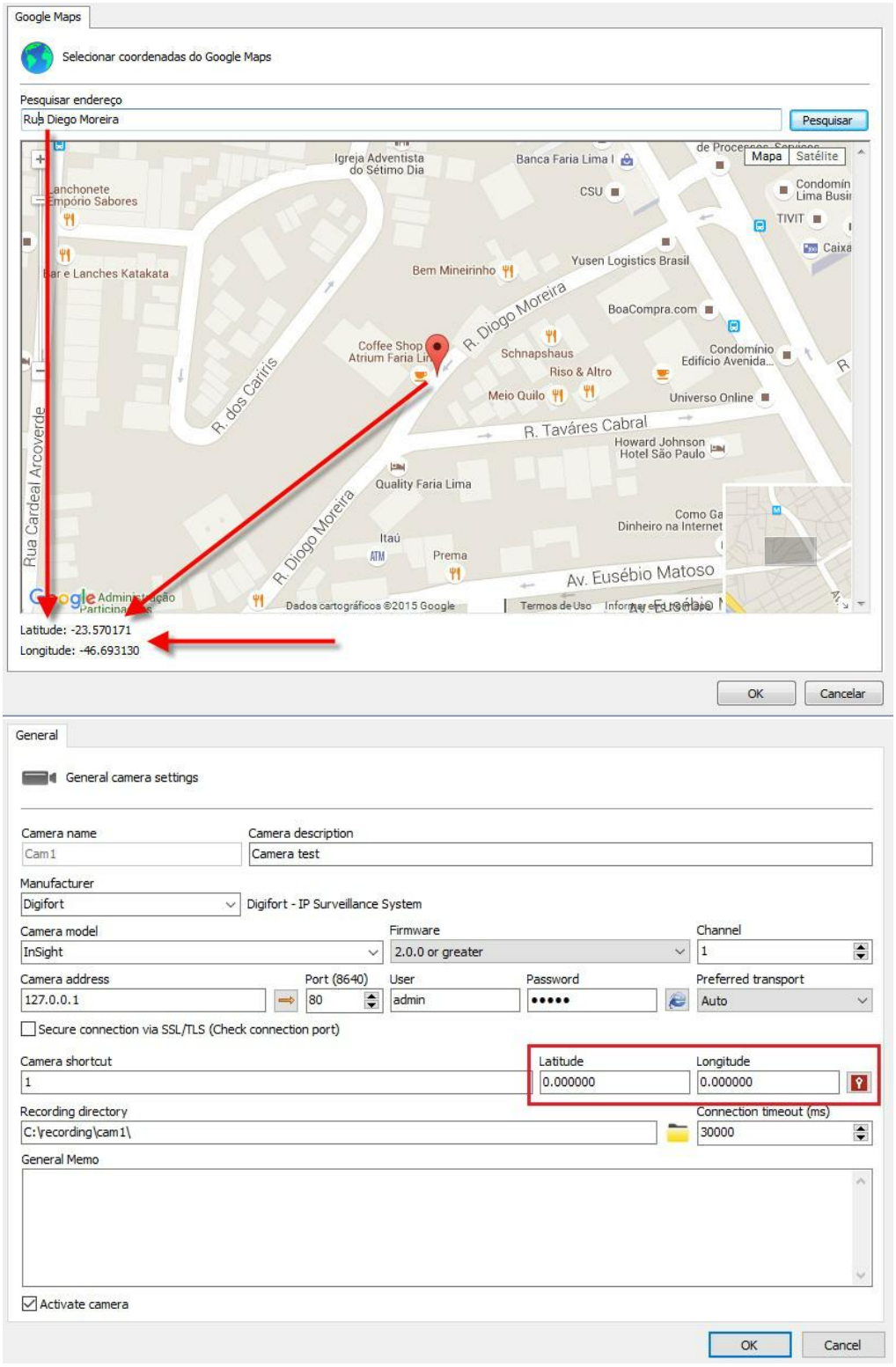
- **Latitude and Longitude**: Fill in longitude and latitude data of the location where the camera has been installed. This option can be used to create maps for easy positioning of the camera.
- **Select Google Maps coordinates**: Facilitates filling the Latitude and Longitude fields with automatic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

© 2002 - 2020 by Digifort, all rights reserved



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

© 2002 - 2020 by Digifort, all rights reserved



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

© 2002 - 2020 by Digifort, all rights reserved

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

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

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

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

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

Attention

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

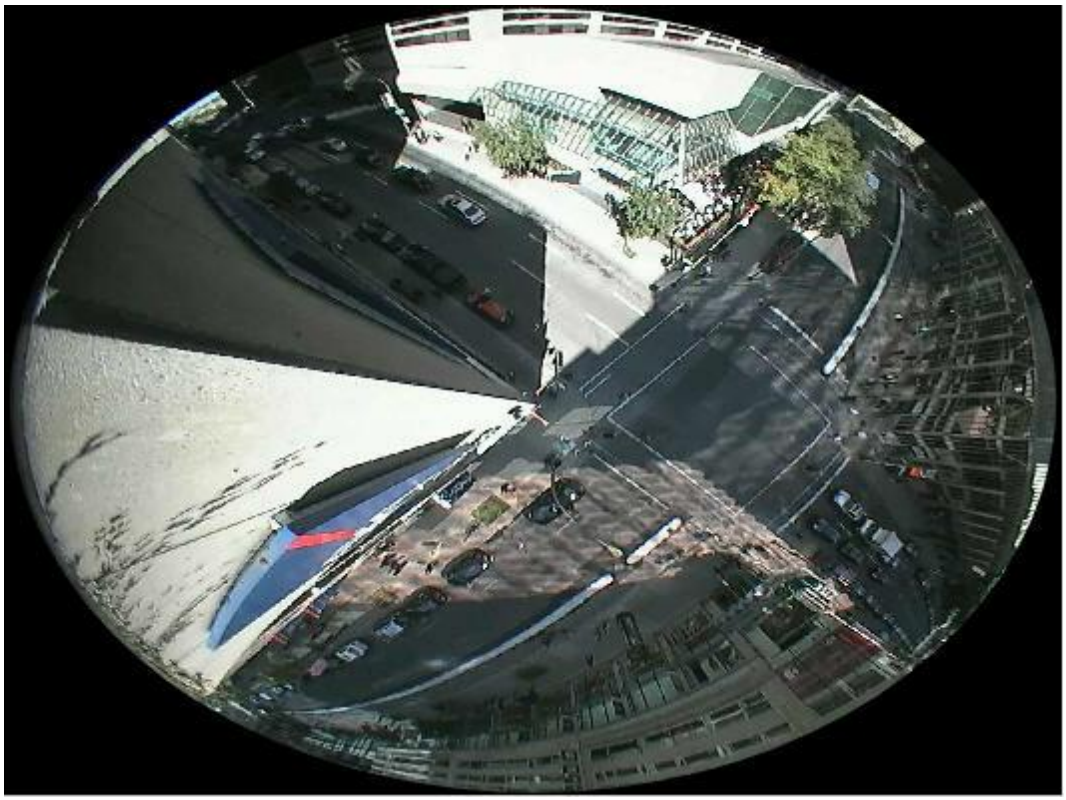
6.1.1.2 Lenses

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

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

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

© 2002 - 2020 by Digifort, all rights reserved



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

© 2002 - 2020 by Digifort, all rights reserved



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



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

Panamorph lens settings

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.1.3 Motion Detection

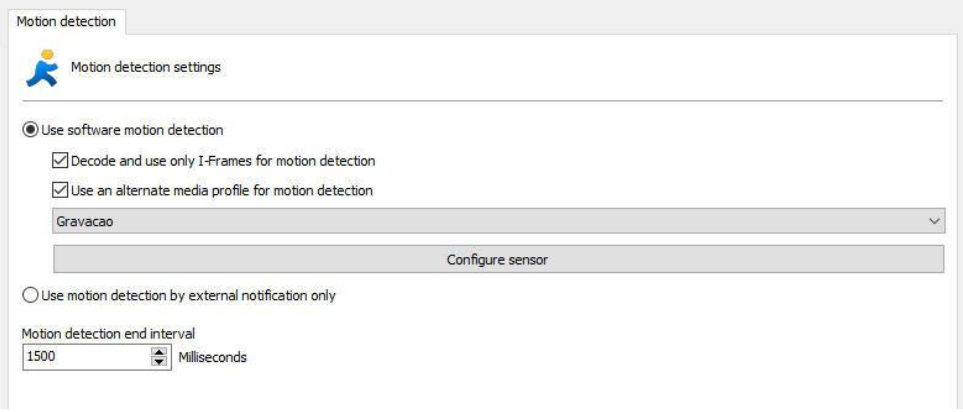
6.1.1.3.1 Use motion detection via softw are

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

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

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

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



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

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

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

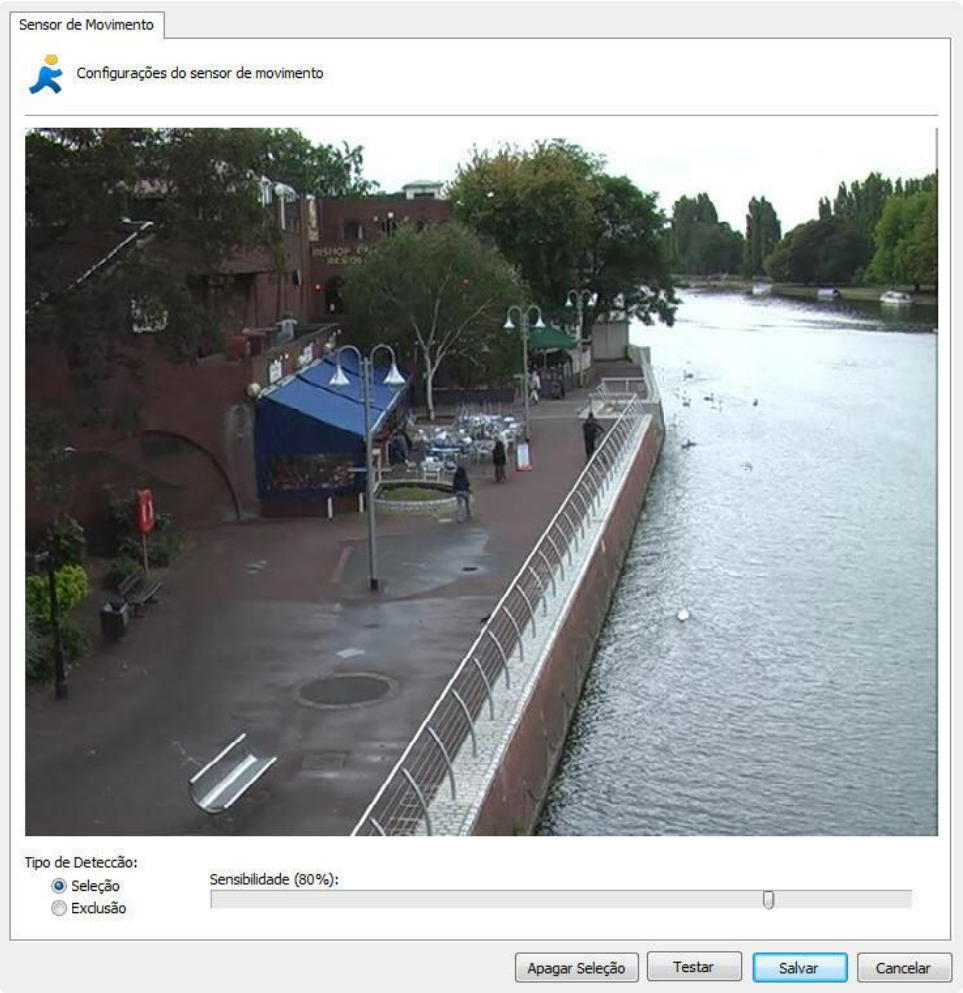
© 2002 - 2020 by Digifort, all rights reserved

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

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

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

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



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

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

© 2002 - 2020 by Digifort, all rights reserved

the process.

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

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

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

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



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

© 2002 - 2020 by Digifort, all rights reserved



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

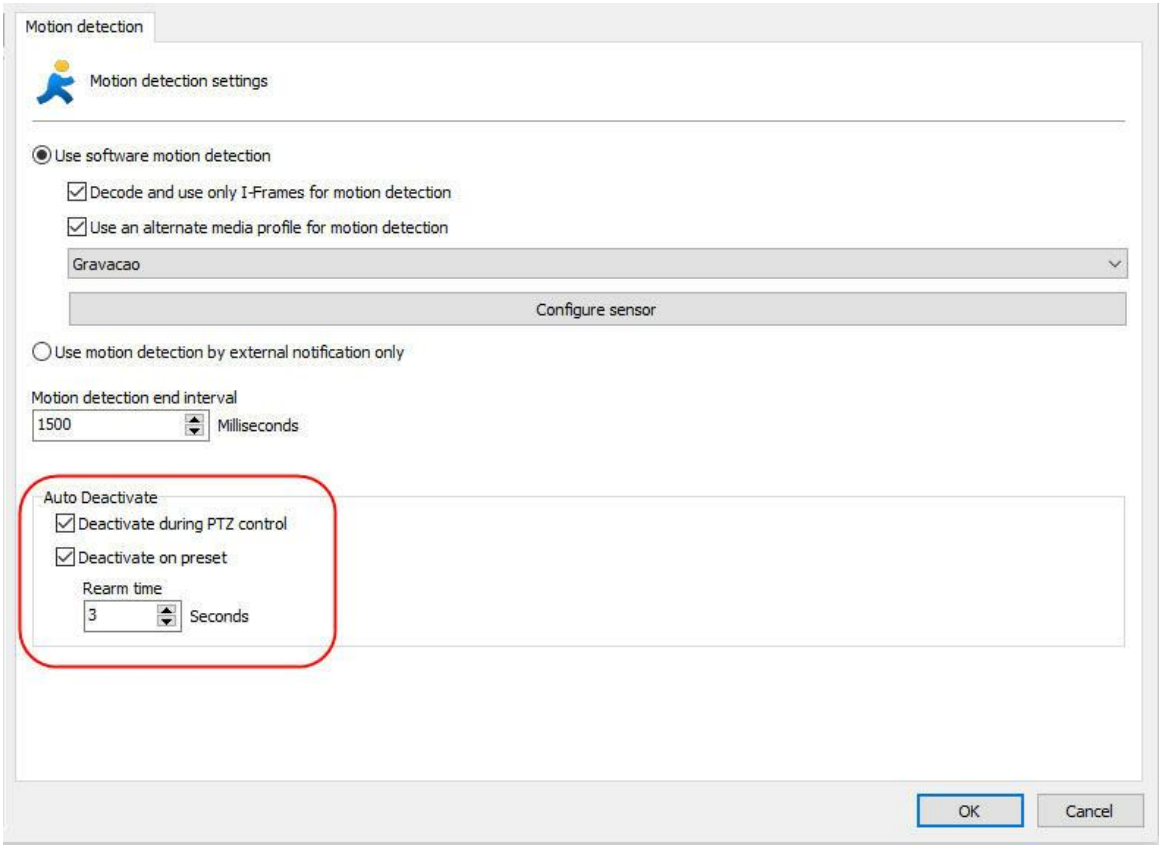
The motion sensor settings are very important to save disk space used by the camera. If on the camera tab you chose the recording method by motion detection, it is recommended to adjust the sensor as needed.

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

© 2002 - 2020 by Digifort, all rights reserved

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

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



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

6.1.1.3.2 Use motion detection by external notification

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

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

© 2002 - 2020 by Digifort, all rights reserved

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

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

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

6.1.1.3.2.1 Configuration

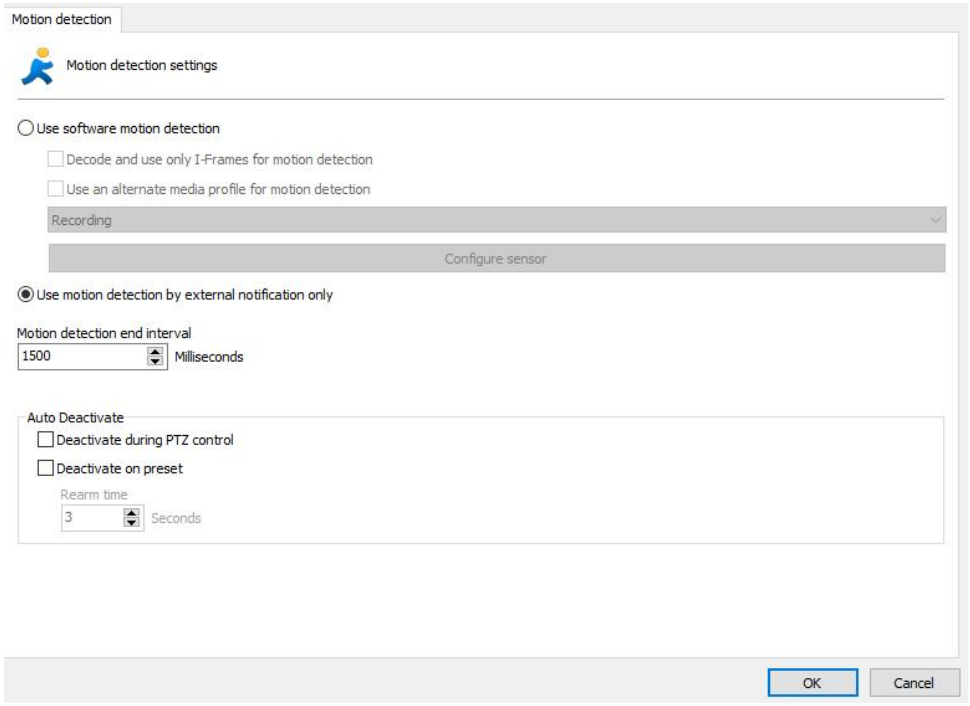
It is very simple to configure movement detection via the hardware. Only two steps are necessary to configure the Digifort to receive notifications by HTTP:

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

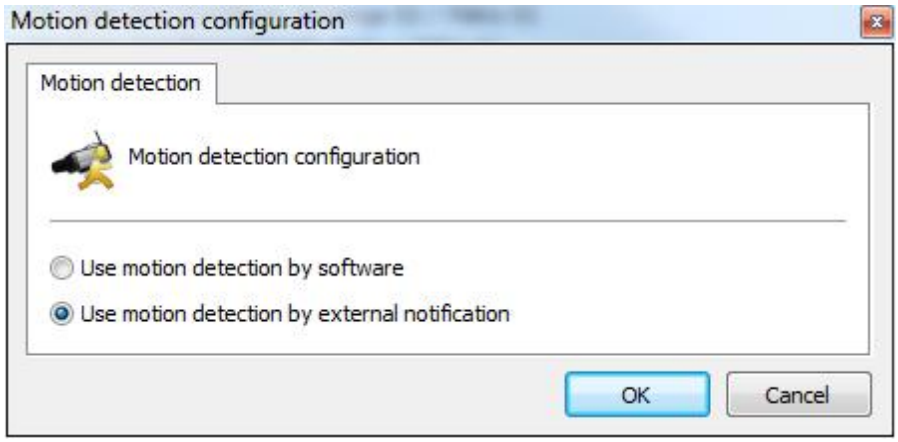
The only configuration made at the Digifort is to select the option "Use motion detection by external notification" in the "Motion Detection" tab of the cameras that will be using movement detection via hardware.

.

© 2002 - 2020 by Digifort, all rights reserved



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



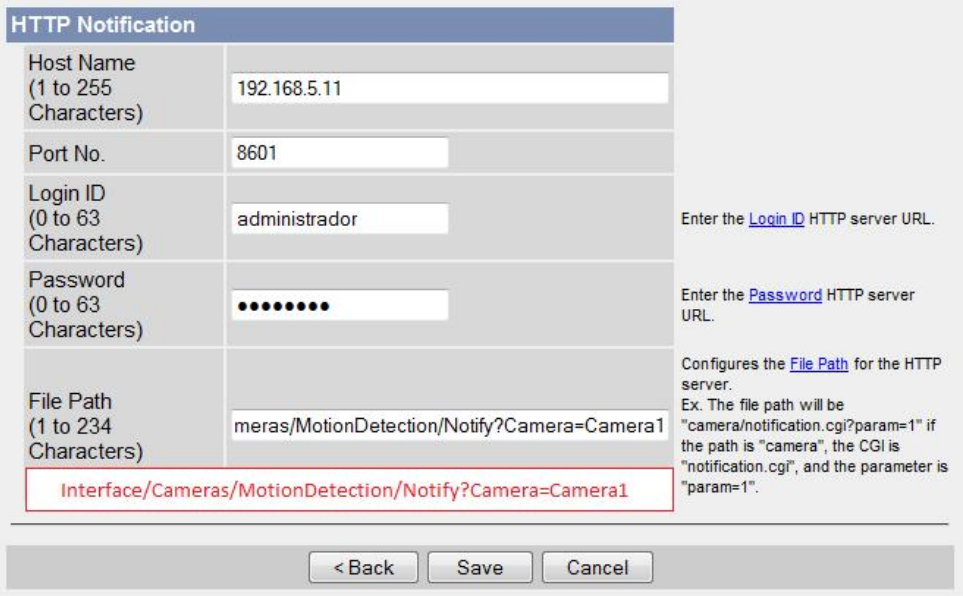
The camera configuration may be the more complex part of the process as each manufacturer implements the HTTP notification resource differently.

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

© 2002 - 2020 by Digifort, all rights reserved

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

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

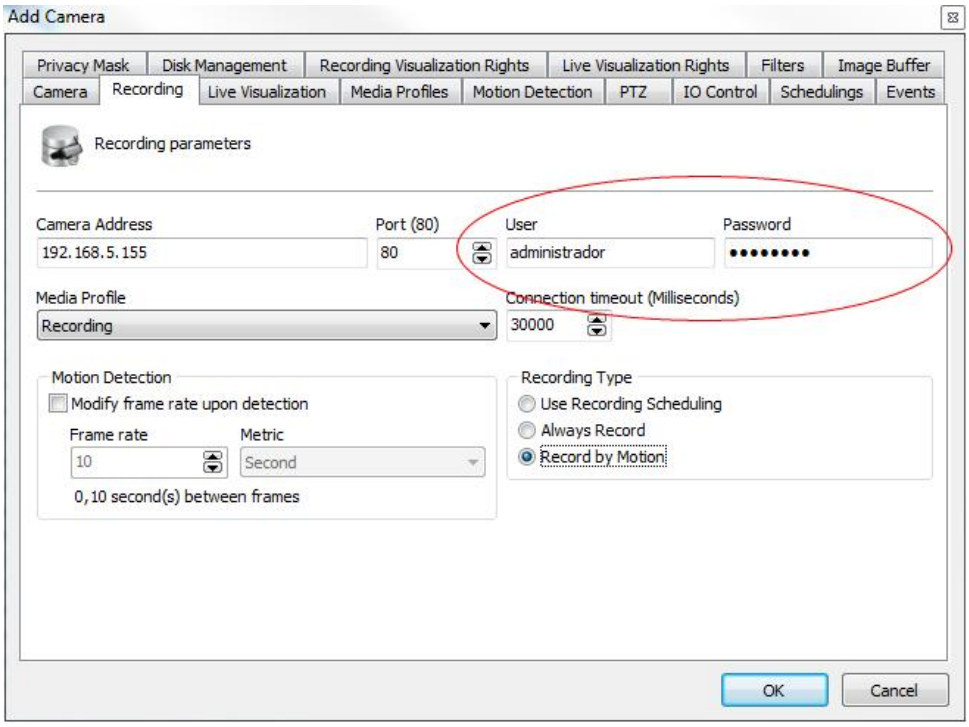


In this picture, the following notification parametres are configured:

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

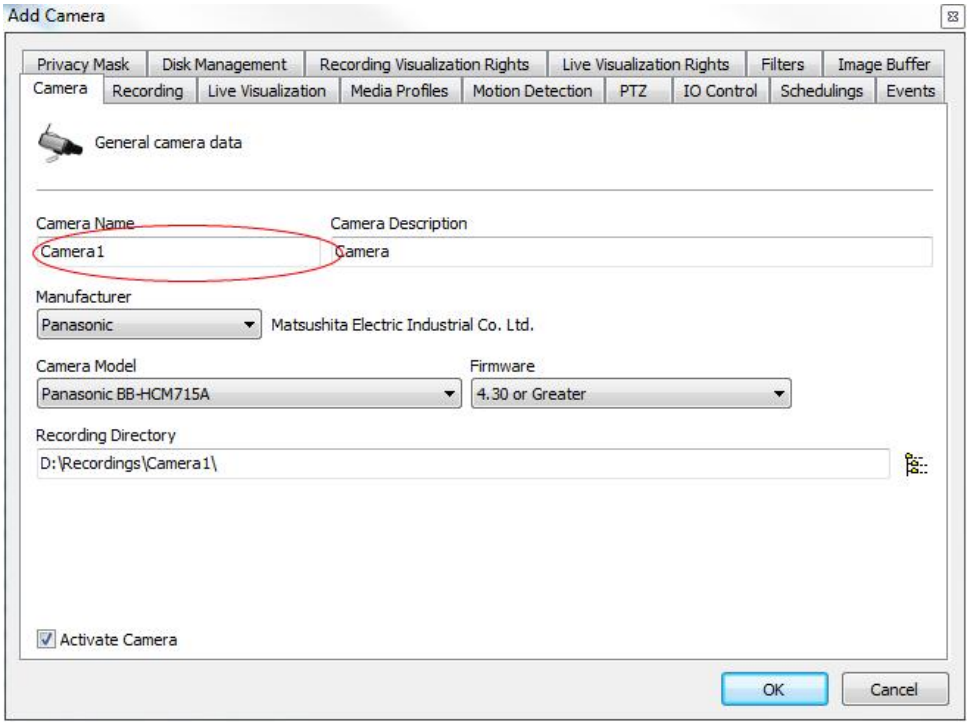
The credentials to access the API Digifort, must coincide with the data supplied when registering the camera in the system. See the picture below:

© 2002 - 2020 by Digifort, all rights reserved



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

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



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

© 2002 - 2020 by Digifort, all rights reserved

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

Examplo:
Camera name: Camera 1

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

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

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

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

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

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

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

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

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

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

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

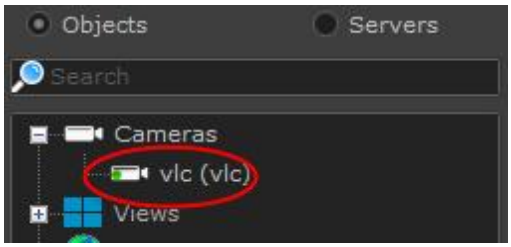
```
/Interface/Cameras/MotionDetection/Notify?Camera=Camera1
```

© 2002 - 2020 by Digifort, all rights reserved

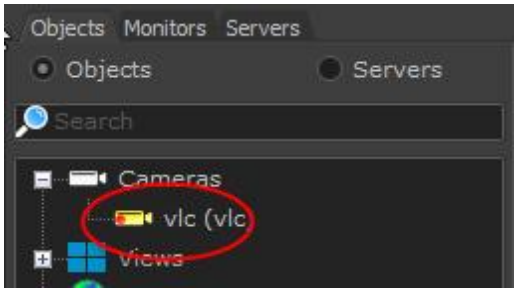
Important: When the system receives this type of notification it will record the imag post buffers added up are complete (3 seconds pattern for each buffer, which can be "Image Buffer" tab for the camera configurations in the Digifort). If your camera allow notification interval, use the same value (in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

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

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



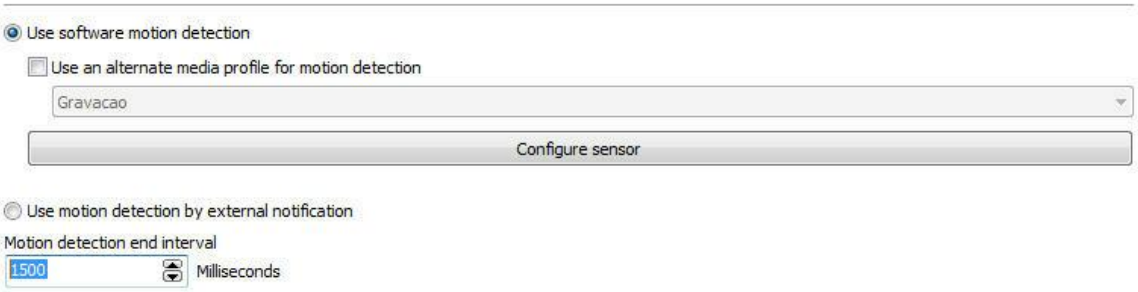
Create movement in the camera and watch if the camera icon changes to yellow as shown below. This icon indicates movement in the camera.



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

6.1.1.3.3 Motion end detection interval

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



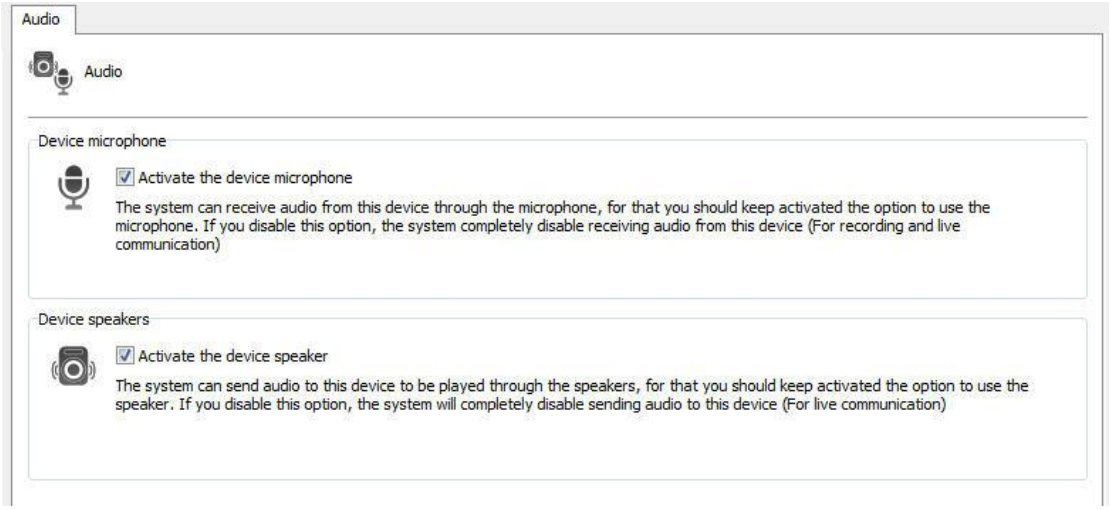
© 2002 - 2020 by Digifort, all rights reserved

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

6.1.1.4 Audio

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

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



In the screen above the following features are available:

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

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

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

6.1.2 Streaming

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.1 Media profiles

A media profile consists of a set or individual parameters of each camera such as image resolution, frames per second and image quality, that are associated with Recording and Live Visualization.
For better understanding, let's take the following situation: A recording profile could be created, that will be associated to the camera recording event. In this profile we could define that we want to record five frames per second, with a resolution of 320x240 and with high image compression. A visualization profile could also be created, that will be associated to visualization of the camera. In this profile we could define that we want to visualize the camera at ten frames per second with a resolution of 640x480 and low image compression.

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

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

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

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

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

© 2002 - 2020 by Digifort, all rights reserved

due to various factors, such as the bad functioning of the internal network, the number of connections made to the camera and the processing power of the camera.

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

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

6.1.2.1.1 How the Media Profiles save network bandwidth

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

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

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

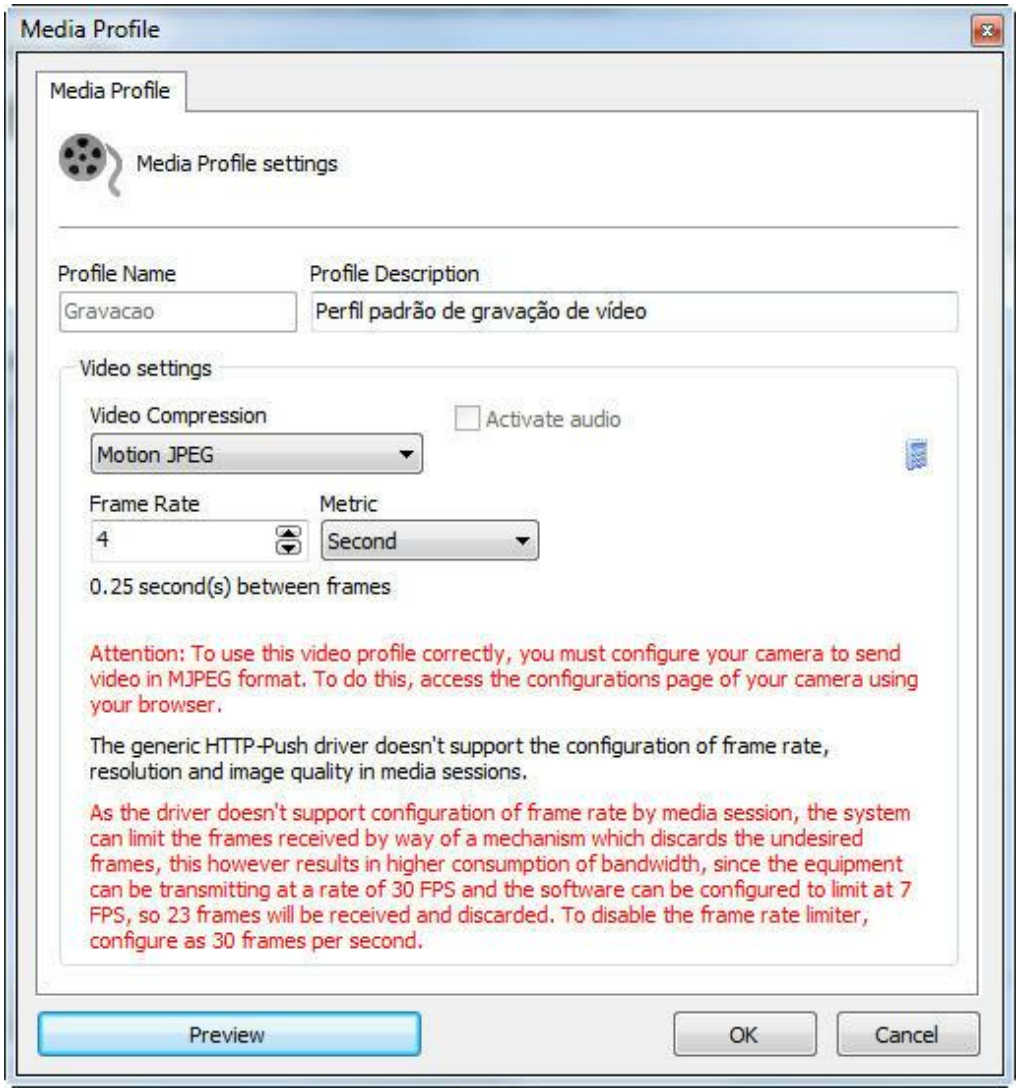
Obs: Digifort operates with any resolution supplied by the camera, whether it is low or high resolution (HD) and with any commercially available compression formats (Motion JPEG, MPEG4 and H264).

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.1.1.1 How to add Media Profiles

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



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

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

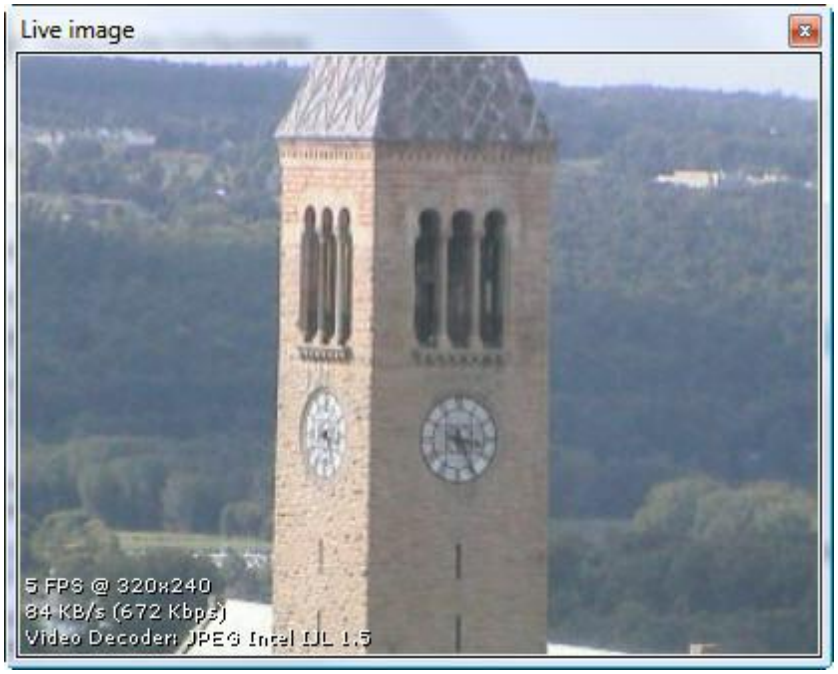
6.1.2.1.1.2 How to visualize the functioning of the configured media profile

To visualize the results of the configurations of the parameters of the media profile being edited, click on the Preview button, opening a screen with the live image of the camera,

© 2002 - 2020 by Digifort, all rights reserved

as shown in the picture below:

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



In this screen, the following configurations are informed:

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

Observation

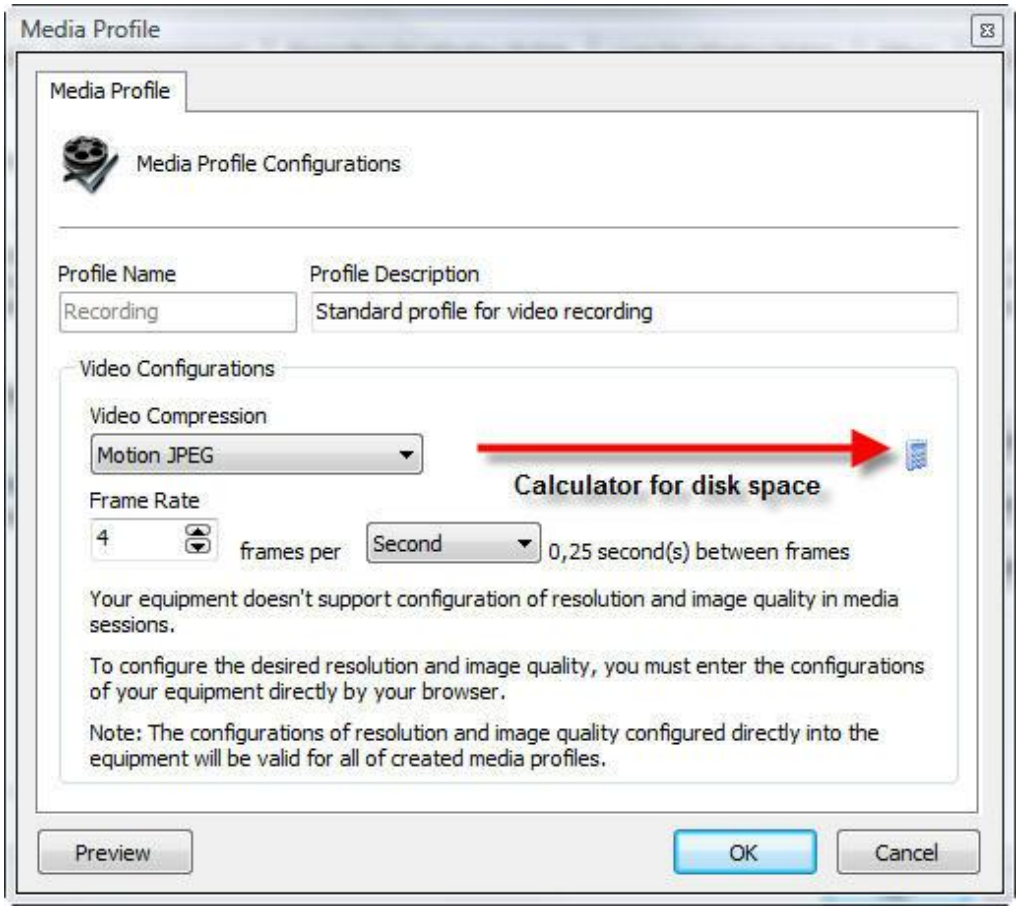
All information contained in the image is updated every second.

6.1.2.1.1.3 Calculator for disk space usage

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

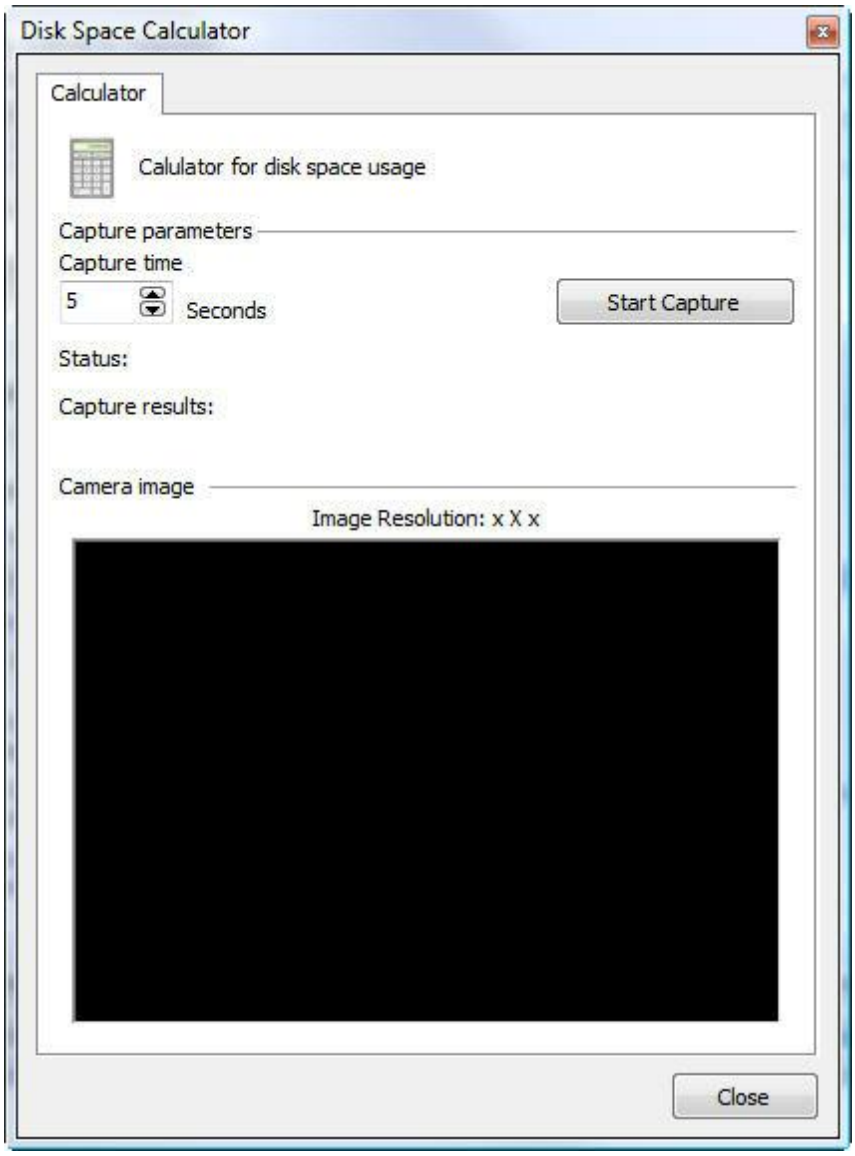
© 2002 - 2020 by Digifort, all rights reserved

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



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

© 2002 - 2020 by Digifort, all rights reserved

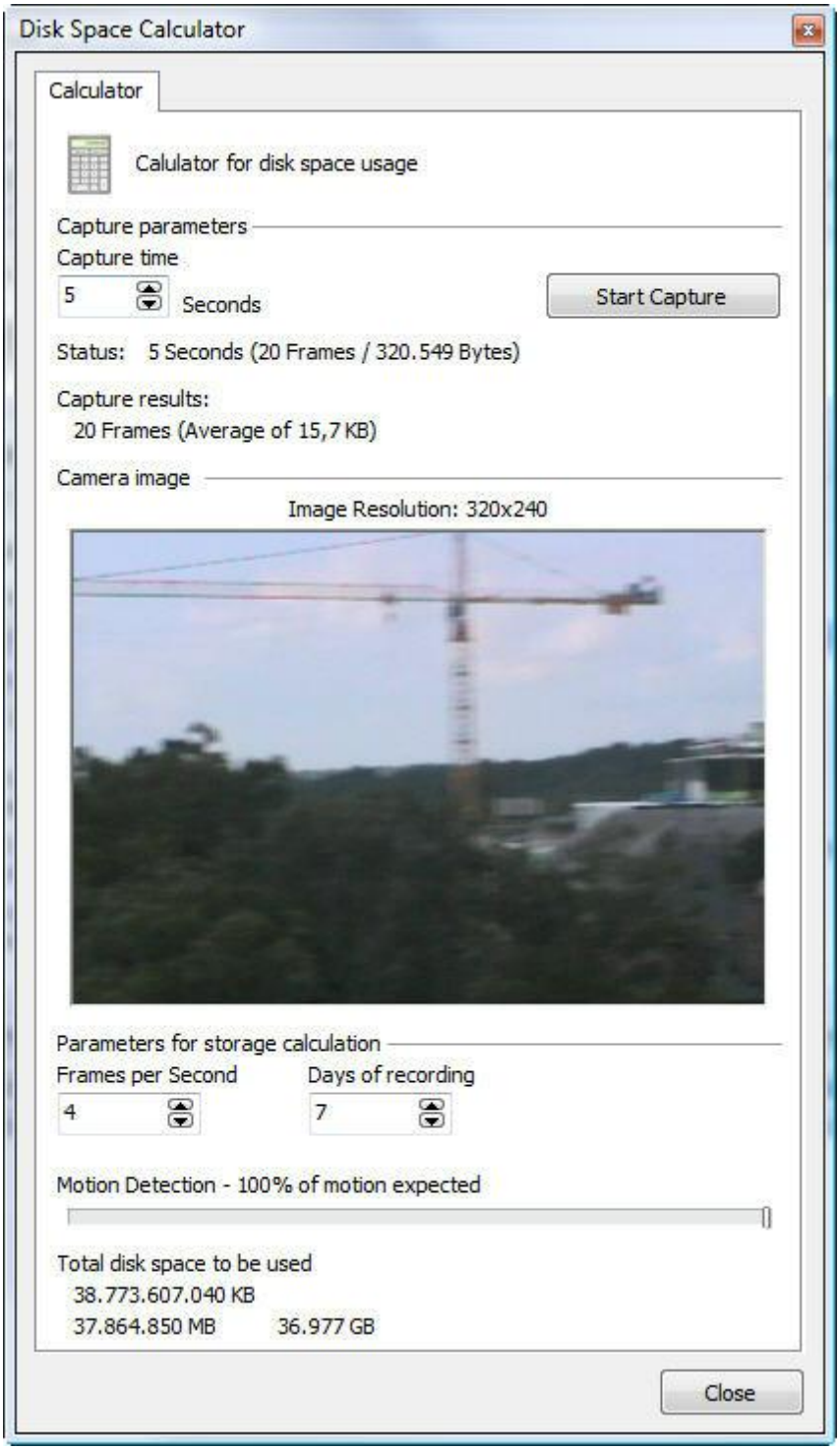


To calculate the disk space necessary for the recording of the camera, the calculator captures an original temporary video from the camera with the parameters of image quality and resolution configured in the media profile being edited and the capture time informed in this screen. Based on the video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

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

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

© 2002 - 2020 by Digifort, all rights reserved



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

© 2002 - 2020 by Digifort, all rights reserved

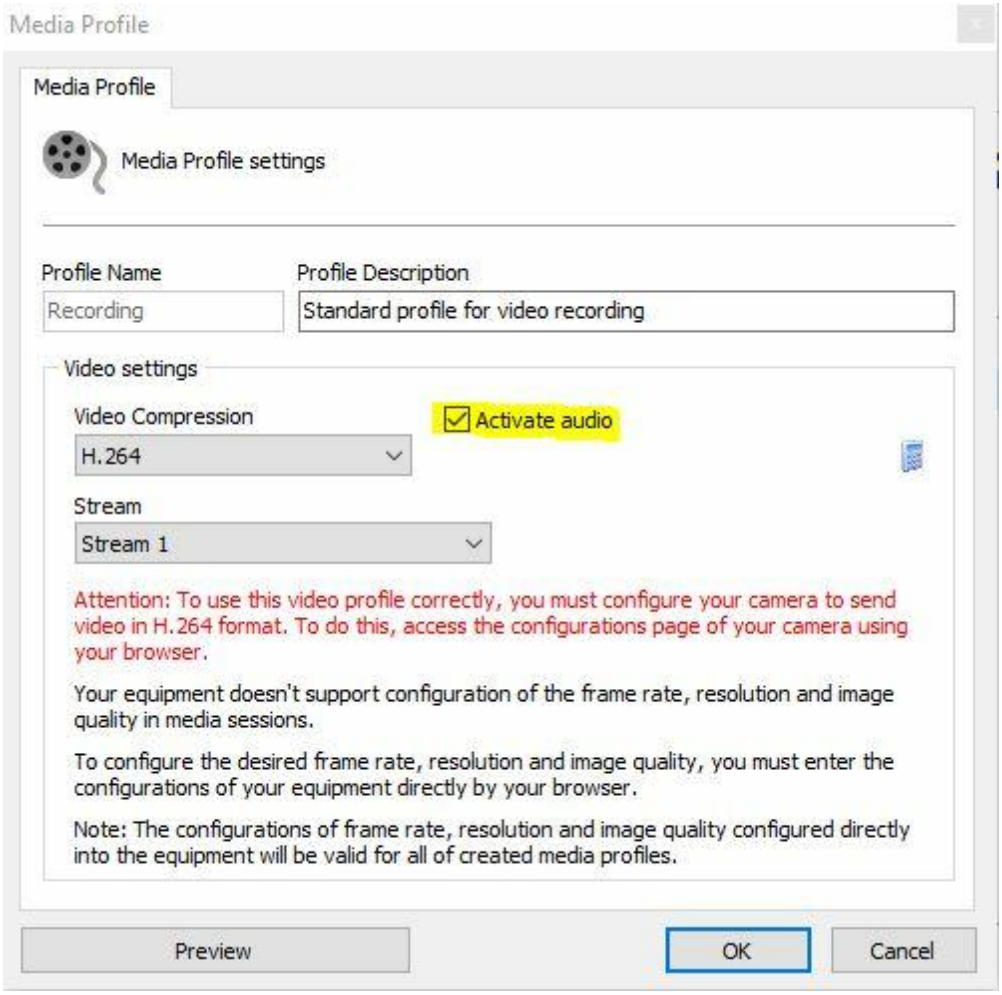
occupation of disk space to be used by the camera. Below are descriptions of how each parameter of the space calculator works.

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

6.1.2.2 Audio

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

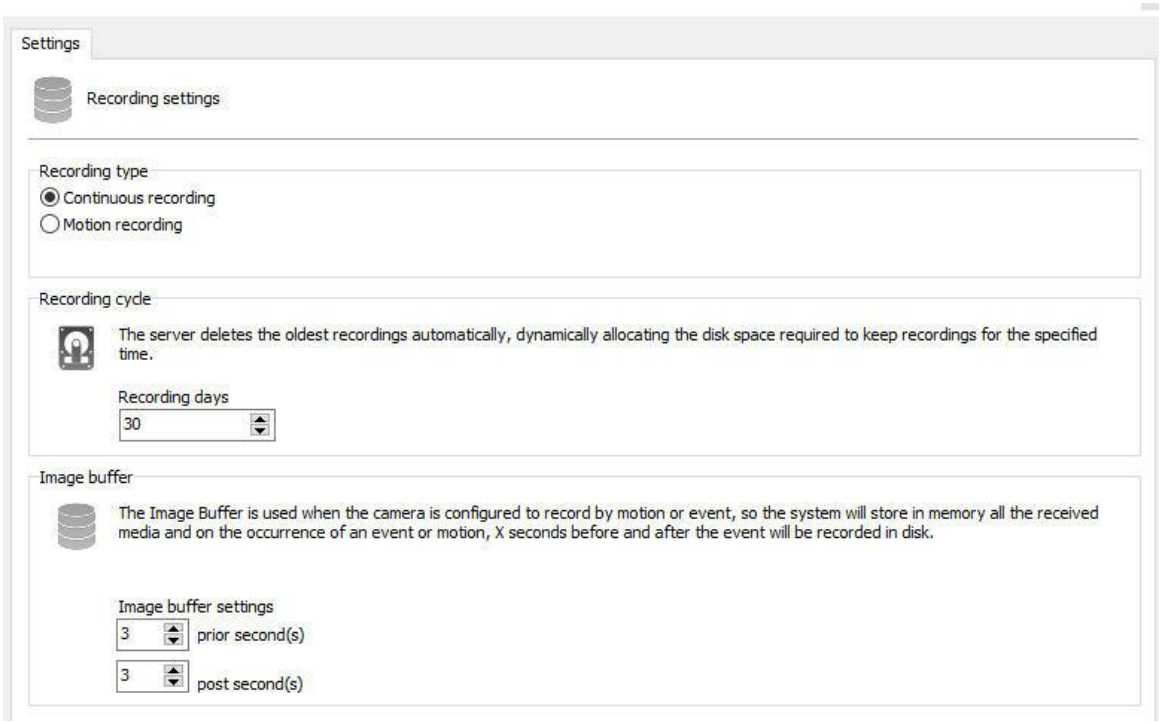
© 2002 - 2020 by Digifort, all rights reserved



6.1.2.3 Recording

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

© 2002 - 2020 by Digifort, all rights reserved



The previous screen has the following features:

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

Motion Detection

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

6.1.2.3.1 Buffer de Snapshot

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

By default this option is disabled to save server resources.

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

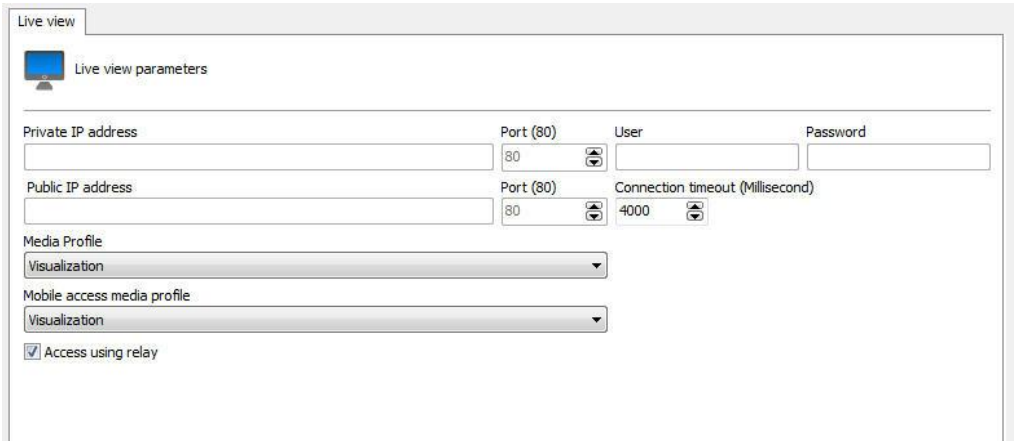
© 2002 - 2020 by Digifort, all rights reserved

6.1.2.4 Live View

6.1.2.4.1 How to configure the visualization of the camera

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

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



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

The parameters to be configured are described below.

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

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

6.1.2.4.1.2 Private IP address

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.4.1.3 Private IP port

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

6.1.2.4.1.4 Public IP address

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

6.1.2.4.1.5 Public IP port

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

6.1.2.4.1.6 User and Password

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

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

Important

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

6.1.2.4.1.7 Connection timeout (in MS)

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

6.1.2.4.1.8 Media profile

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.2.4.1.9 Media profile for access via mobile

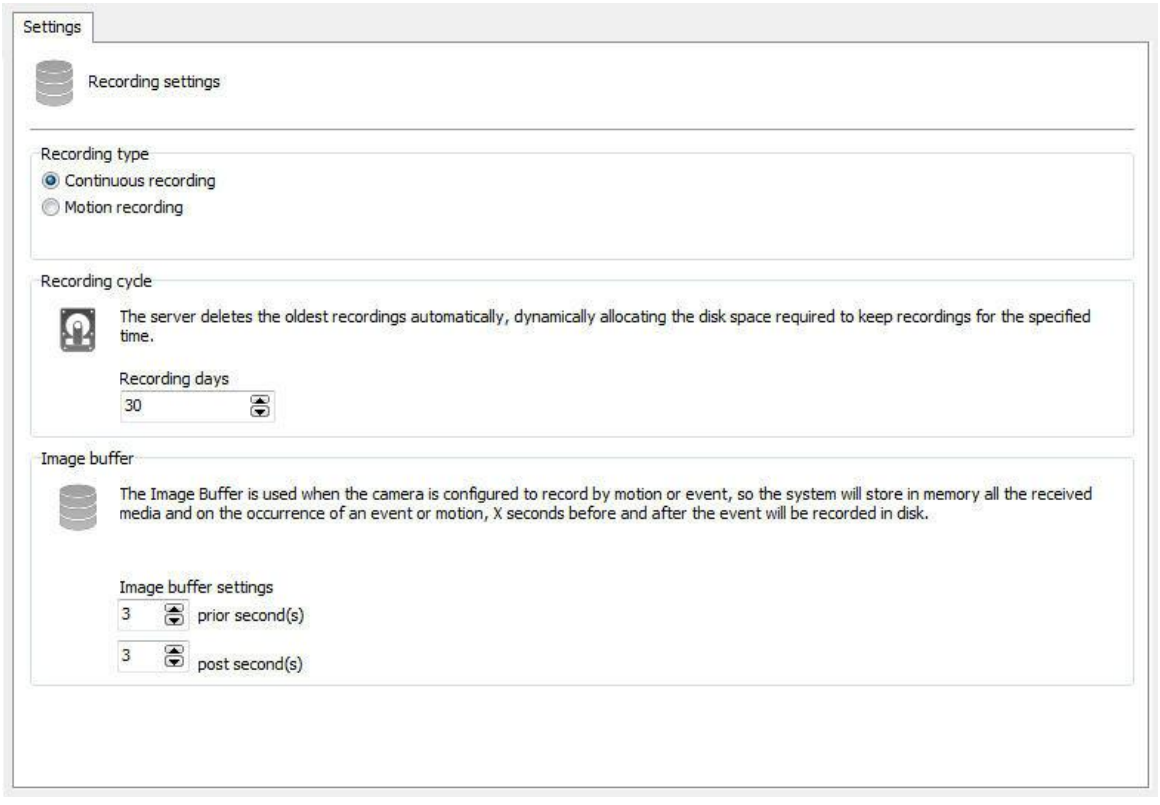
The system allows the use of a differential media profile for viewing via mobile devices.

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

To learn more about Media Profile check Media Profiles

6.1.3 Recording

The next screen has the recording settings of the camera:



© 2002 - 2020 by Digifort, all rights reserved

6.1.3.1 Type of recording

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

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

6.1.3.2 Recording Cycle

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

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

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

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

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

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

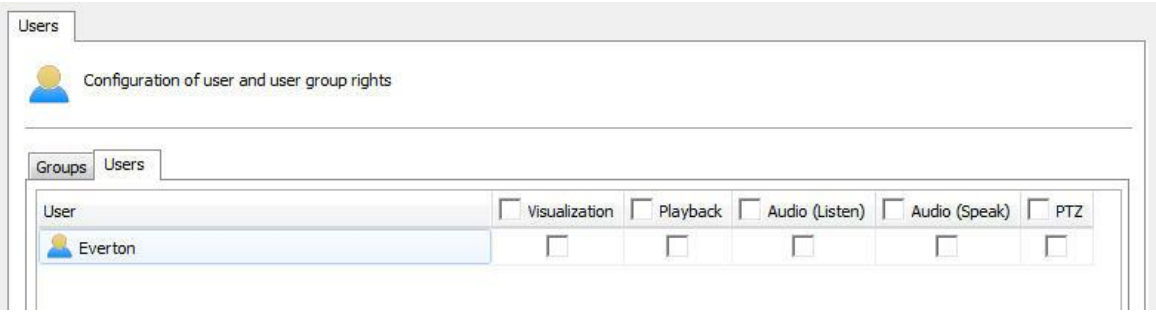
6.1.4 Rights

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.4.1 Users

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



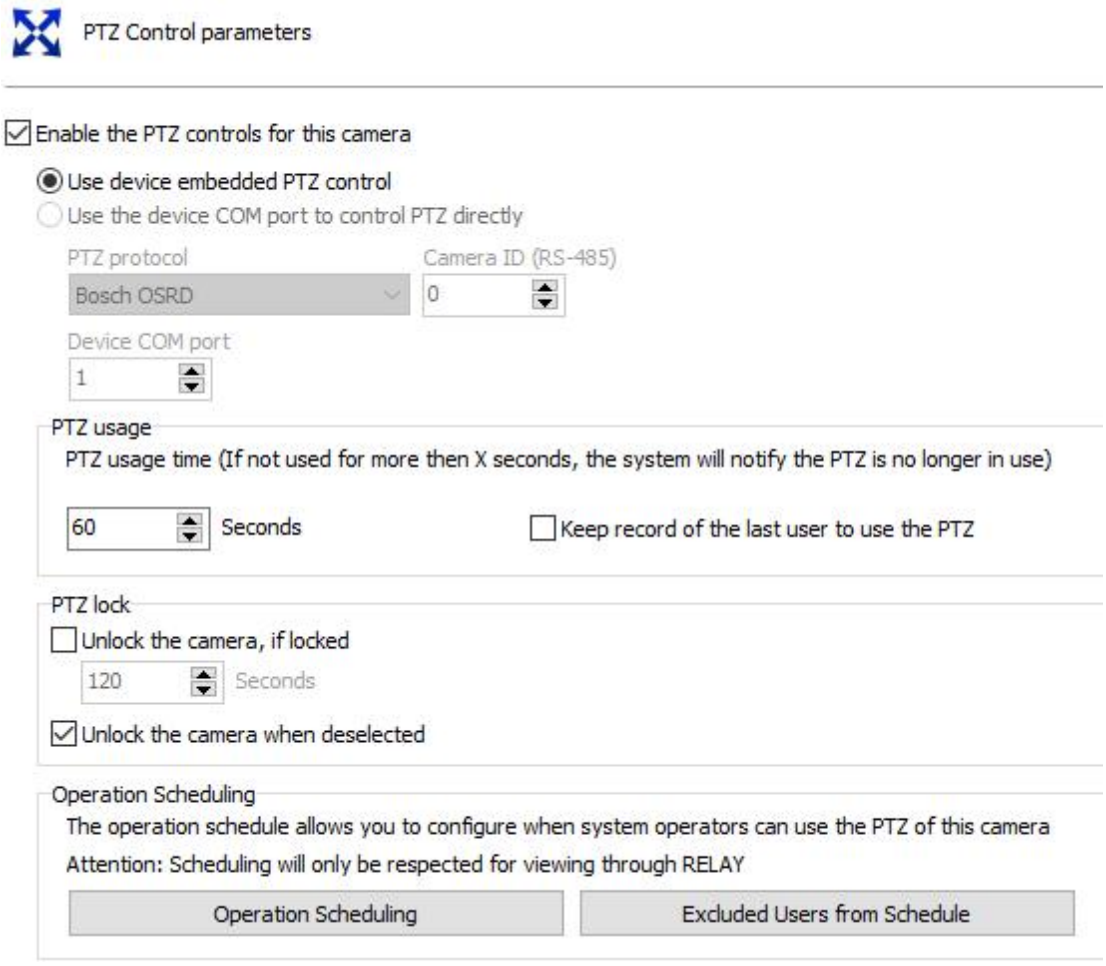
- **Preview:** Check this option if the user can see the camera in live mode in Surveillance Client.
- **Playback:** Select this option if the user will be able to view the recorded images.
- **Audio (Listen):** Select this option if the user can hear the audio captured by the camera.
- **Audio (Talking):**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

6.1.5 PTZ

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

6.1.5.1 Configurations

© 2002 - 2020 by Digifort, all rights reserved



The settings screen offers the following features

6.1.5.1.1 Activate the PTZ control for this camera

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

6.1.5.1.2 Use the device's PTZ features

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

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

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.5.1.4 Use of PTZ

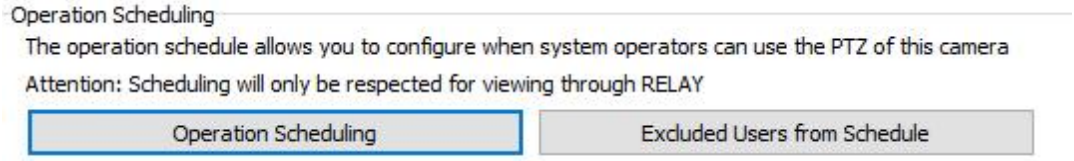
By using the PTZ monitoring client the system shows all other users who are in control right now.
In this option you can configure **X seconds** which the system will understand that the PTZ is no longer in use if it is not moved by the operator.

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

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



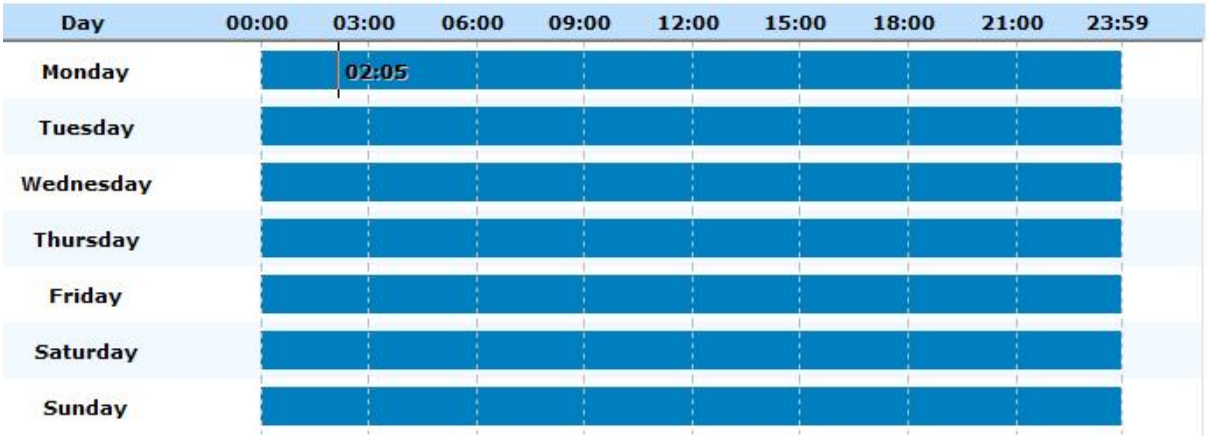
6.1.5.1.5 Agendamento de Operação



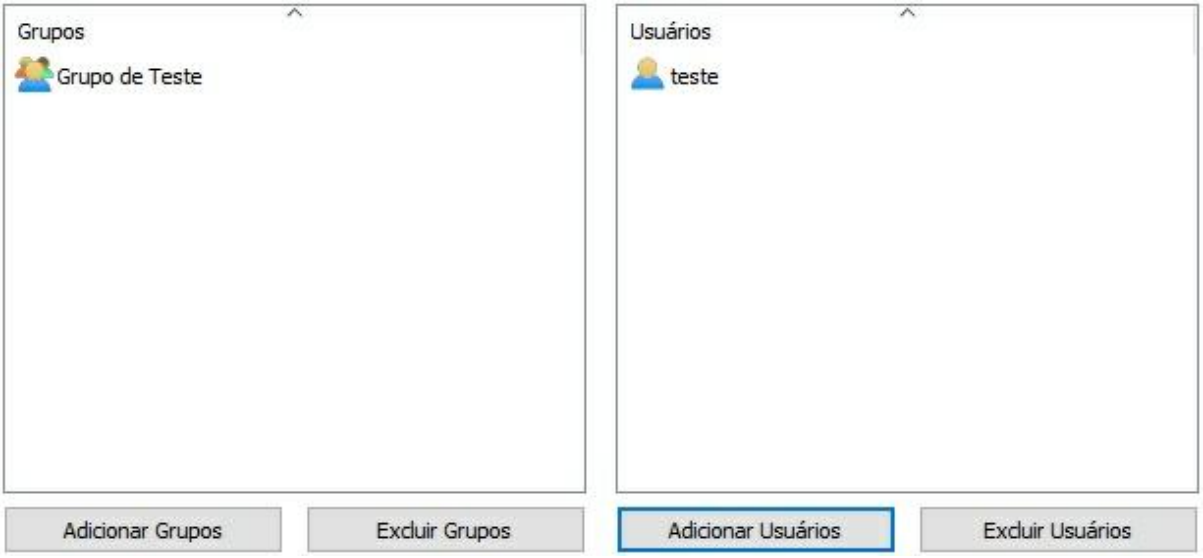
The Operation Schedule allows you to configure when the system operators will be able to use the PTZ of this camera.

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

© 2002 - 2020 by Digifort, all rights reserved



- **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 the Operation Schedule, the camera must be configured for viewing through the Relay Server.

6.1.5.2 Presets

6.1.5.2.1 How to configure the Presets Control

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

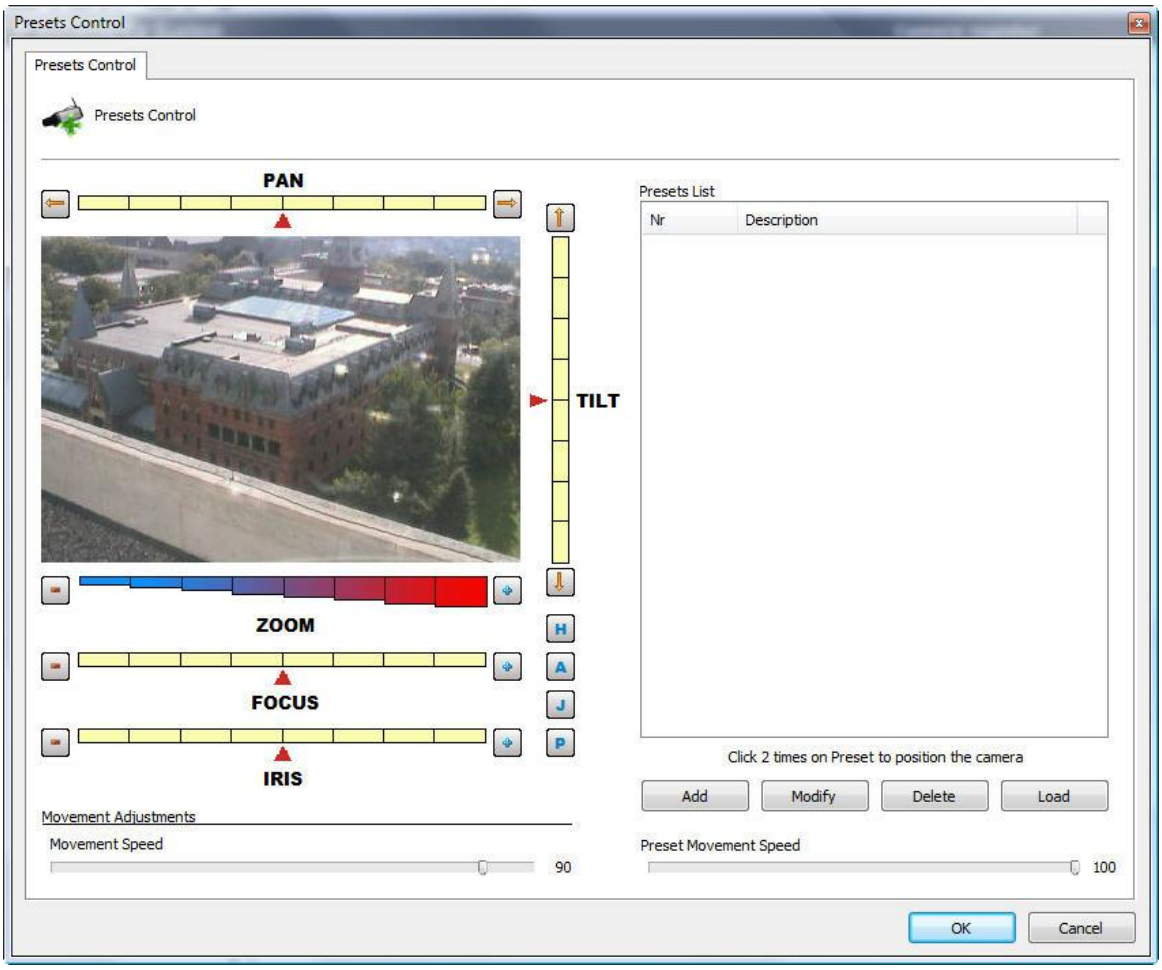
Each model of camera supports a certain number of presets. The role of Digifort is to maintain an internal positions list created by the user referring to the list of internal presets of the camera, that is, the position 1, created by the user, is associated to internal position 1 of the camera, for

© 2002 - 2020 by Digifort, all rights reserved

example. When the user adds a preset, the two positions are linked.

The presets will be available for use in the Surveillance Client. Consult the Surveillance Client to learn how to call up the configured preset.

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



- **PAN bar**: Moves the camera to the left and to the right
- **TILT bar**: Moves the camera up and down
- **ZOOM bar**: Moves the camera's zoom in and out.
- **Focus bar**: Adjusts the camera's focus, in case this isn't done automatically.
- **Iris bar**: Adjusts the camera's iris, in case this isn't done automatically.
- **Home button**: This configuration is located on the button identified by an "H". Clicking on this button causes the camera to be positioned in its initial factory-determined position.
- **Advanced PTZ button**: This configuration is located on the button identified by an "A". Clicking on this button causes the advanced PTZ controls to be displayed. To learn how to use this feature, see Advanced PTZ.
- **Visual Joystick button**: This configuration is located on the button identified by a "J". Clicking on this button causes the visual joystick to be displayed over the allowing you to control its movement by mouse. To learn how to use this feature, see page Visual Joystick.
- **Movement adjustments**:
  - **PTZ by bar**:Define in what way the new camera positioning will be obtained. This

© 2002 - 2020 by Digifort, all rights reserved

configuration can have one of two values:

- **Absolute PTZ**: The new positioning commands of the camera will be absolute, that is, relative to the Home position..
- **Relative PTZ**: The new positioning commands of the camera will be relative to the present position
  - **Movement speed:** Movement speed of the camera while its position is being adjusted. This value is expressed as a percentage and its default value is 90% of the maximum speed of the camera.
- **Presets list:** This list contains all of the presets registered for this camera. To position the camera in a preset, double-click on the preset.
- **Add button:** Memorizes the present position of the camera. To learn how to use this feature, see How to create a preset
- **Modify button:** Modifies the selected preset..
- **Exclude button**: Excludes the selected preset.
- **Download button**: Loads the configured camera presets directly to the camera.
- **Preset movement speed**: Specifies the movement speed of the camera from one preset to another. This value is expressed as a percentage and its default value is 100% of the maximum speed.
- **Custom Home Position:** Allows you to customize the home position of mobile cameras. Many cameras do not have / support the home position, so for cameras that do not support this option, the administrator can now configure a camera preset as home.

Important

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

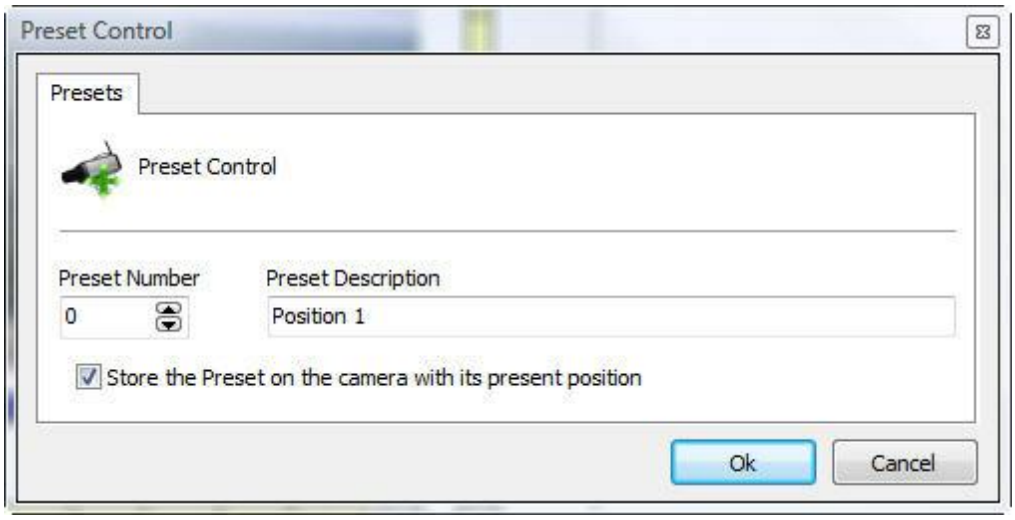
Tip

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

6.1.5.2.2 How to create a preset

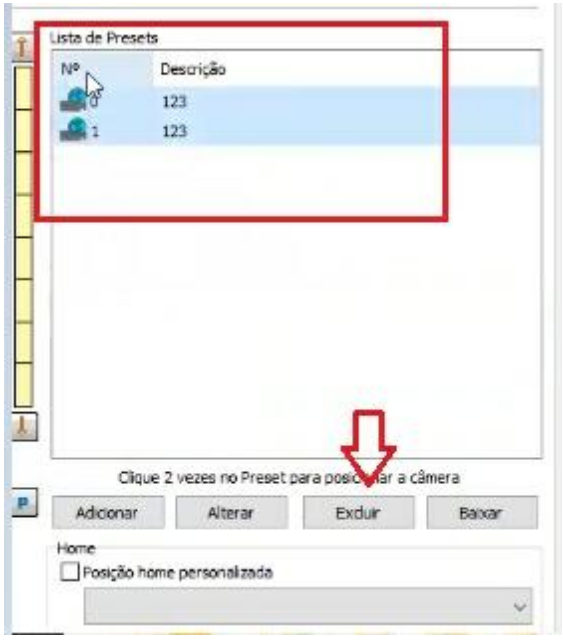
The process of creation of presets is quite easy, simply positioning the camera with the controls presented in the previous topic and clicking on Add, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



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

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



© 2002 - 2020 by Digifort, all rights reserved

6.1.6 Events

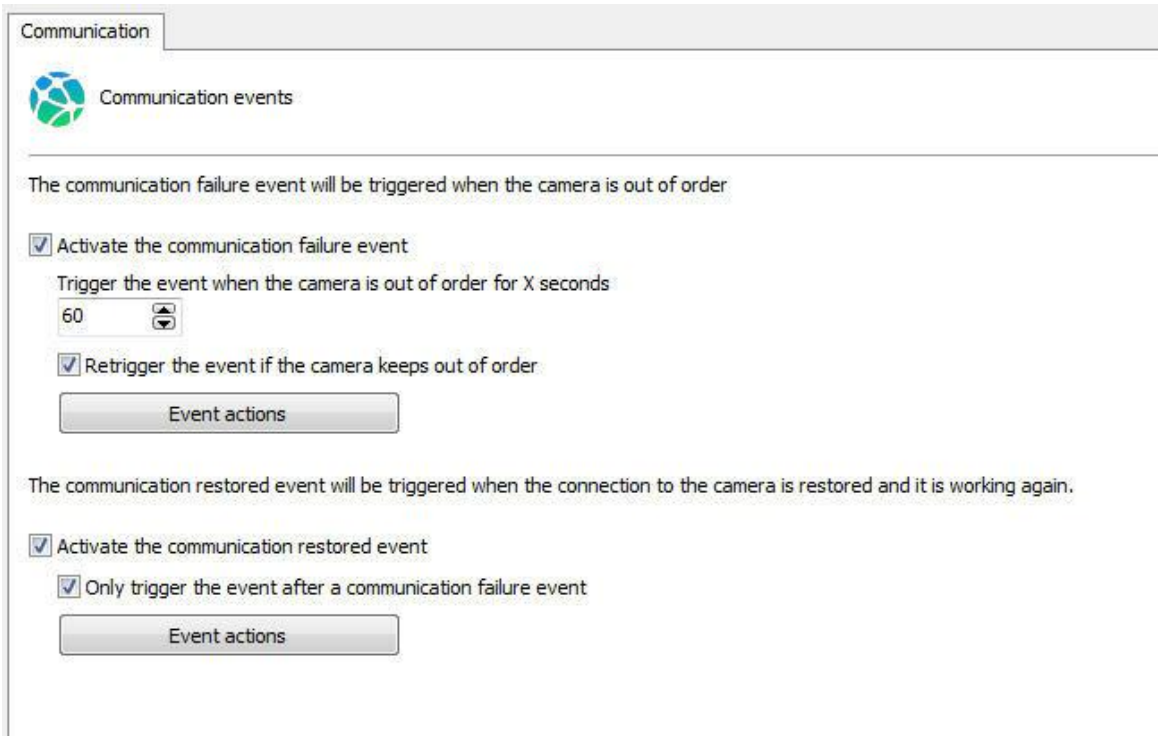
During the operation of the camera in the Digifort System, various events occur in the camera. These events can be communication failures or alarm recognition events, for example.

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

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

6.1.6.1 Communication

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

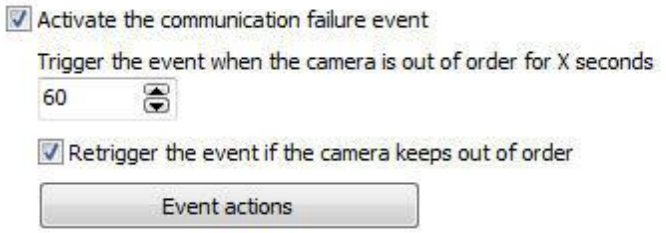


6.1.6.1.1 Communication failure event

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

© 2002 - 2020 by Digifort, all rights reserved

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

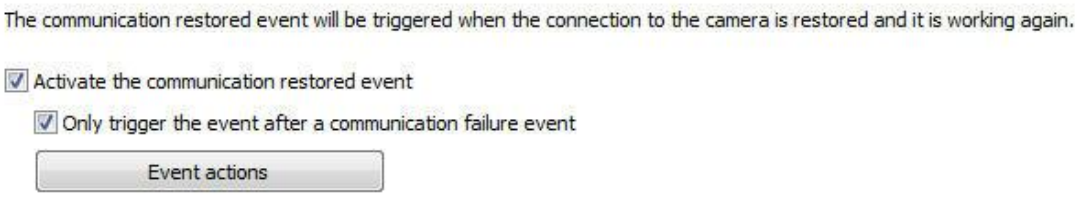


To learn how to set the alarm actions see How to set the alarm

6.1.6.1.2 Connection restoration event

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

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



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

6.1.6.1.3 Devices failure report

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.6.2 Recording failure

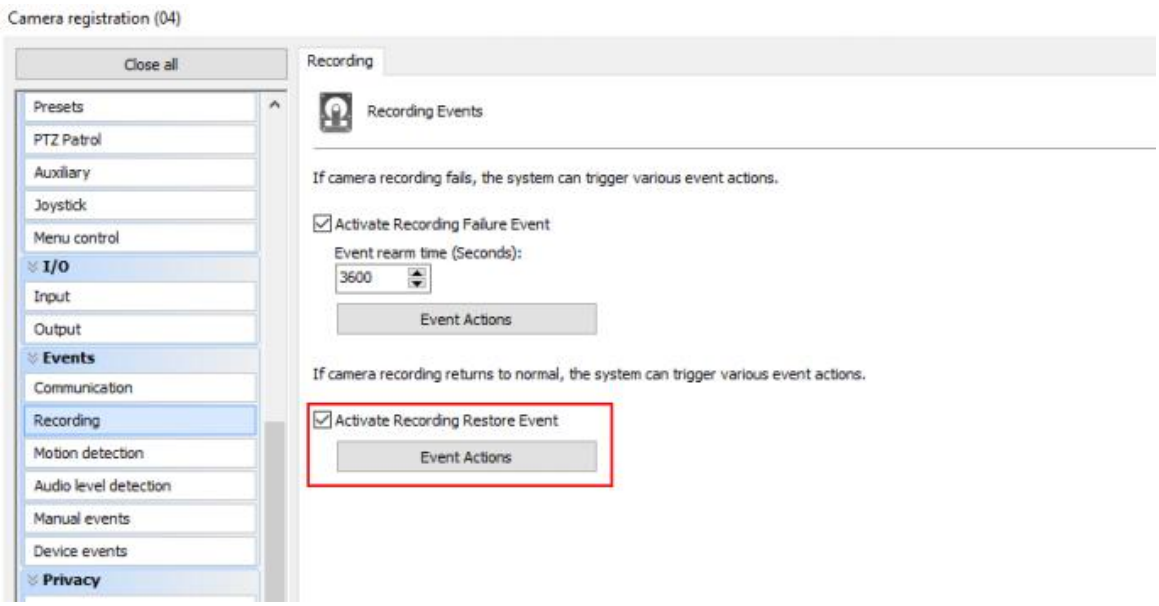


To configure the recording failure event, select the Activate recording failure event option.

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

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

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



6.1.6.3 Event Variables

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

© 2002 - 2020 by Digifort, all rights reserved

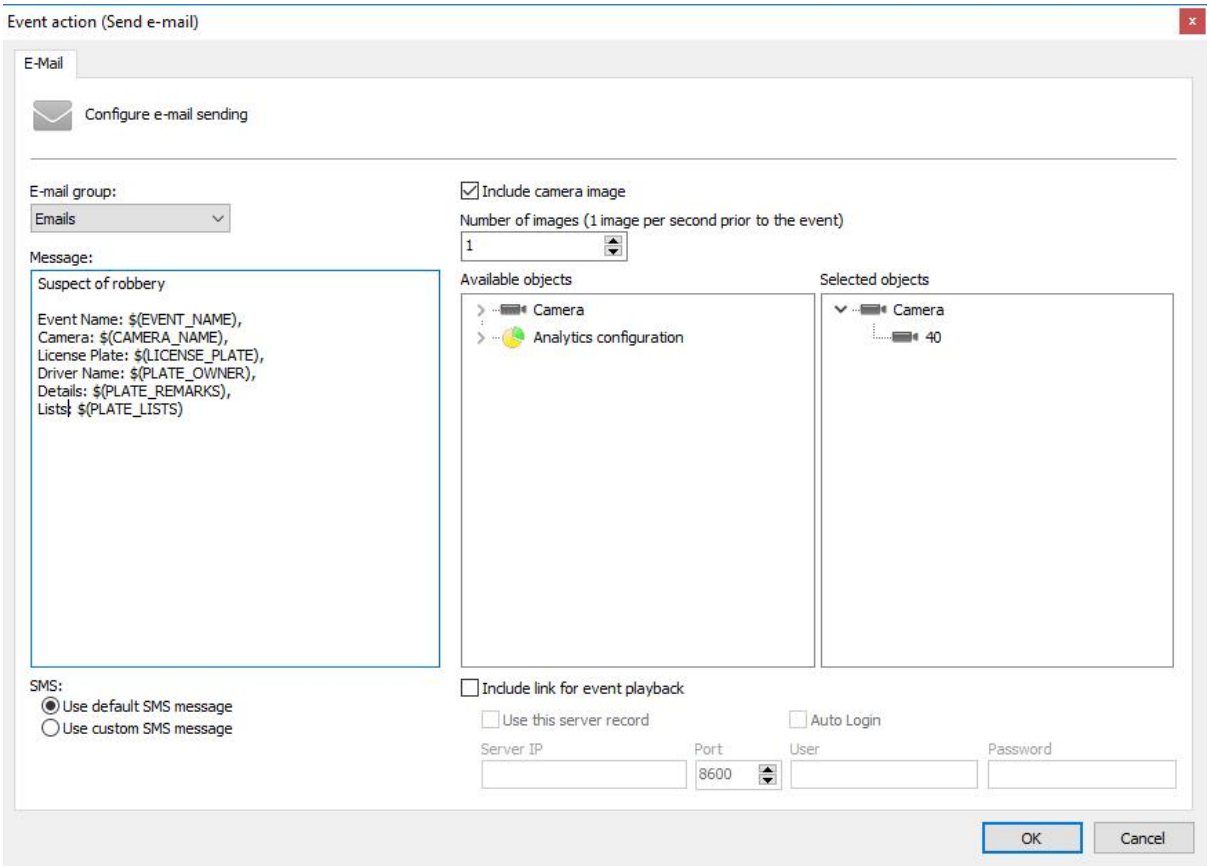
The Event Variable value can be accessed through the variable name reference, using a variable name identifier: $(VARIABLE_NAME)

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

The following event actions support the use of variables:

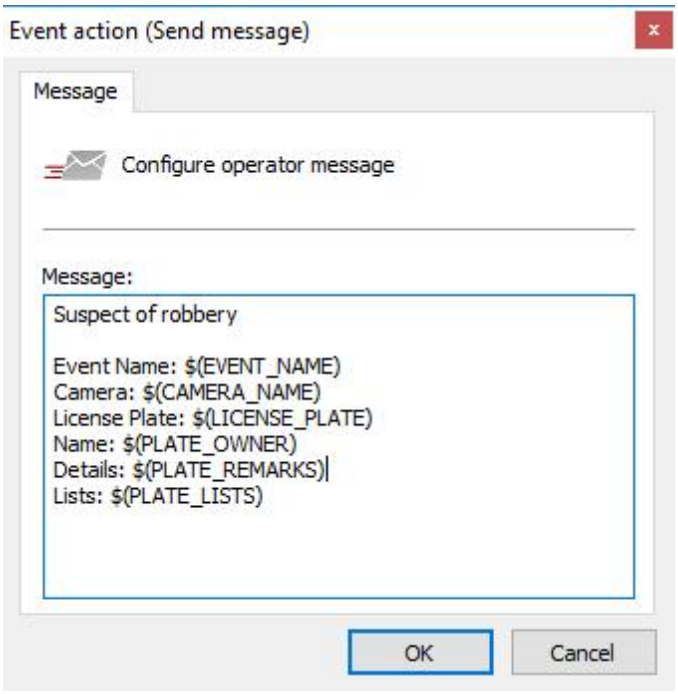
- Send e-mail
- Send message to the Operator
- Send HTTP request
- Create Bookmark

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



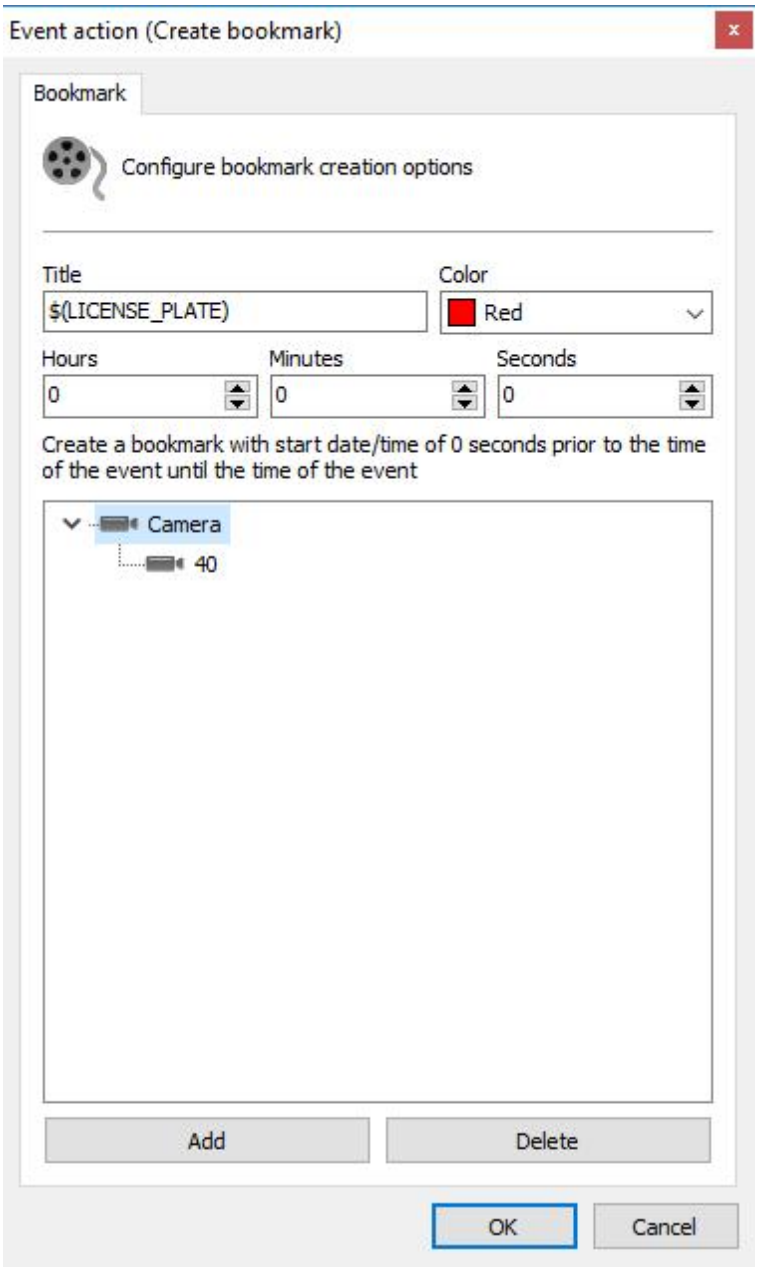
The same can be configured for messages sent to system operators, adding valuable information on the alarm pop-up:

© 2002 - 2020 by Digifort, all rights reserved



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

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

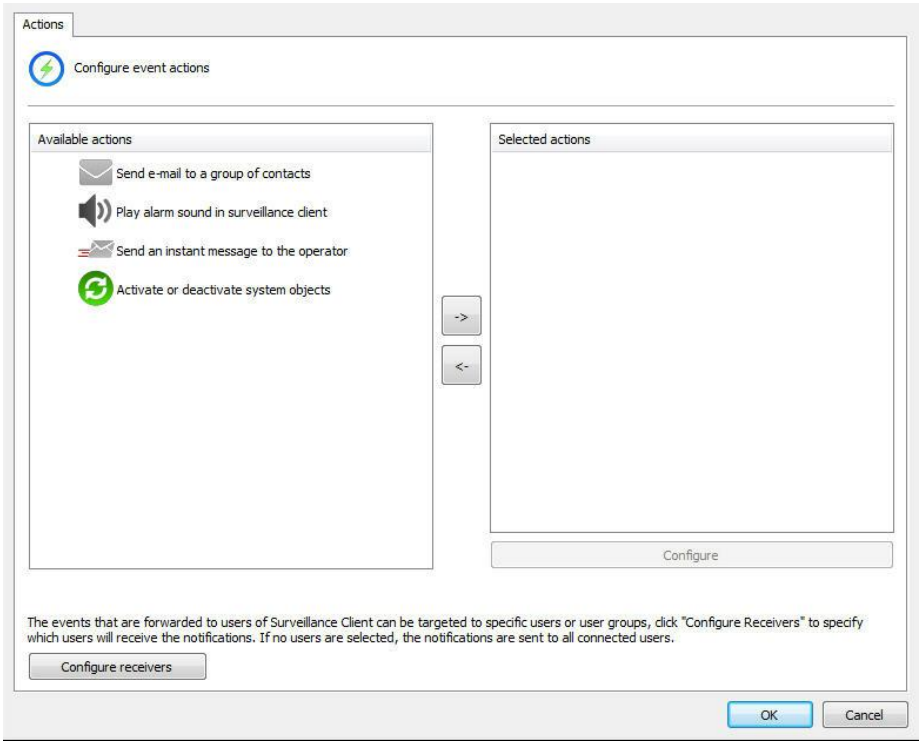


To receive the complete documentation with all system event variables, please contact our support team.

6.1.7 How to configure the alarm actions

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

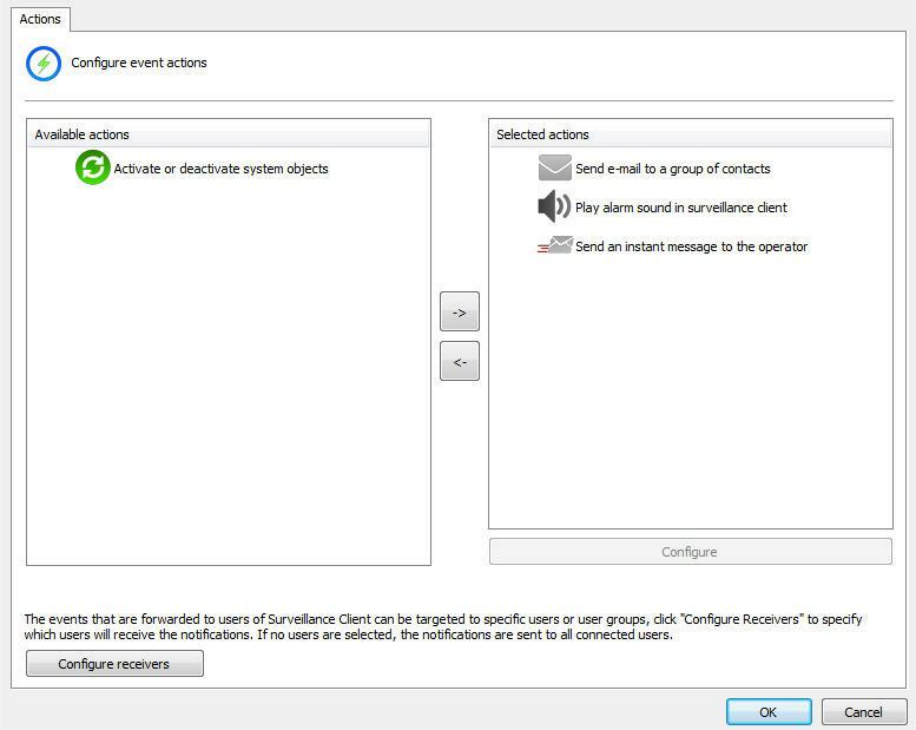
© 2002 - 2020 by Digifort, all rights reserved



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

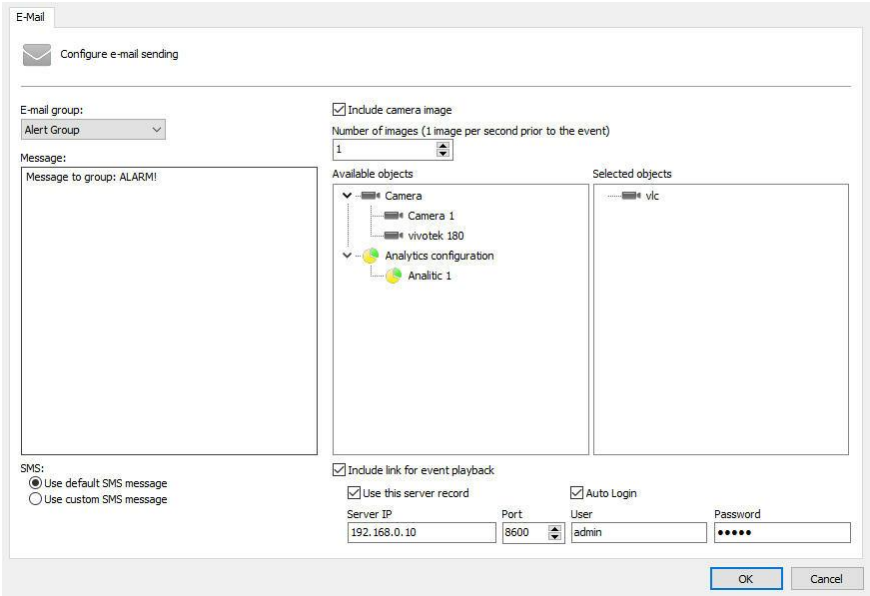
To enable any of the events just click and drag it to the list on the right **Selected Actions** as shown below:

© 2002 - 2020 by Digifort, all rights reserved



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

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



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

© 2002 - 2020 by Digifort, all rights reserved

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

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

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

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

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

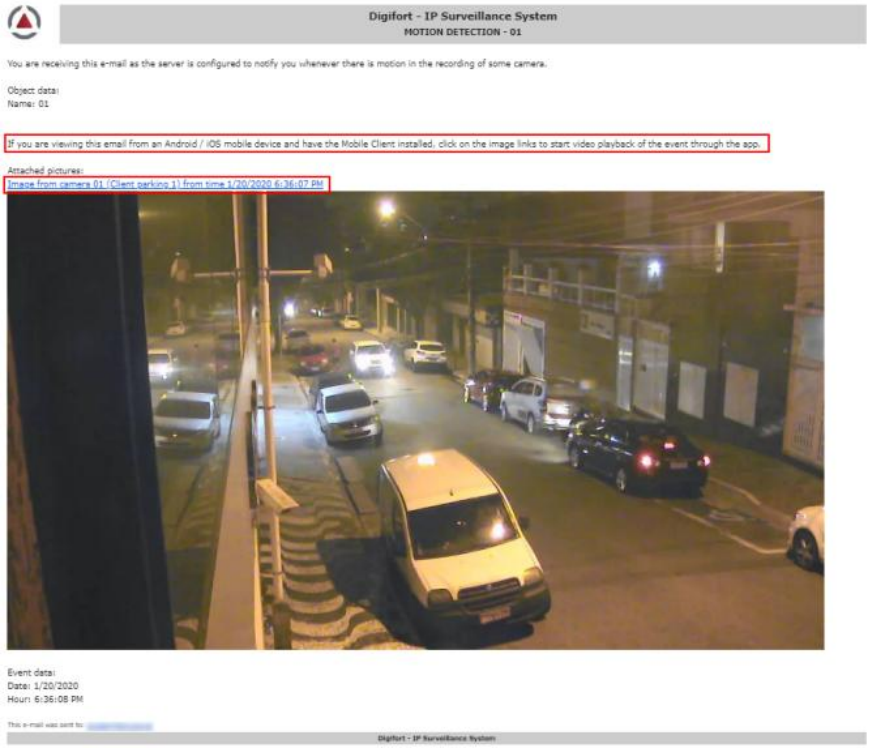
- **Use this server record**: Fill in with data from the server where the camera image that will be attached to the e-mail is located. With this option, upon running the e-mail script, the surveillance client will auto connect with the pre-configured data from this option. If this option is not selected,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

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

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

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

© 2002 - 2020 by Digifort, all rights reserved



6.1.7.2 Sound an alarm in the Surveillance Client

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



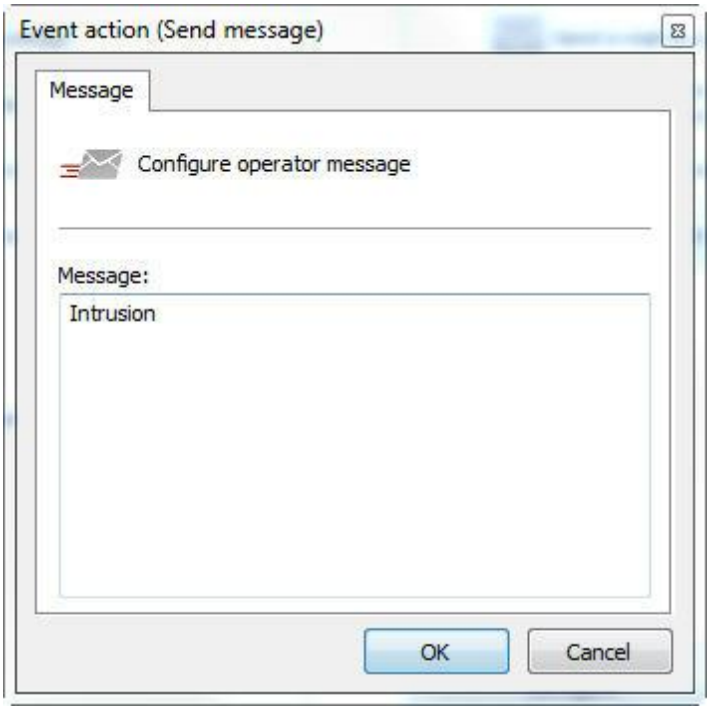
Select the desired alert sound and execution time in the Surveillance

© 2002 - 2020 by Digifort, all rights reserved

Client. To test the selected sound, click on the **Play** button.

6.1.7.3 Send instant message to the operator of the computer

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



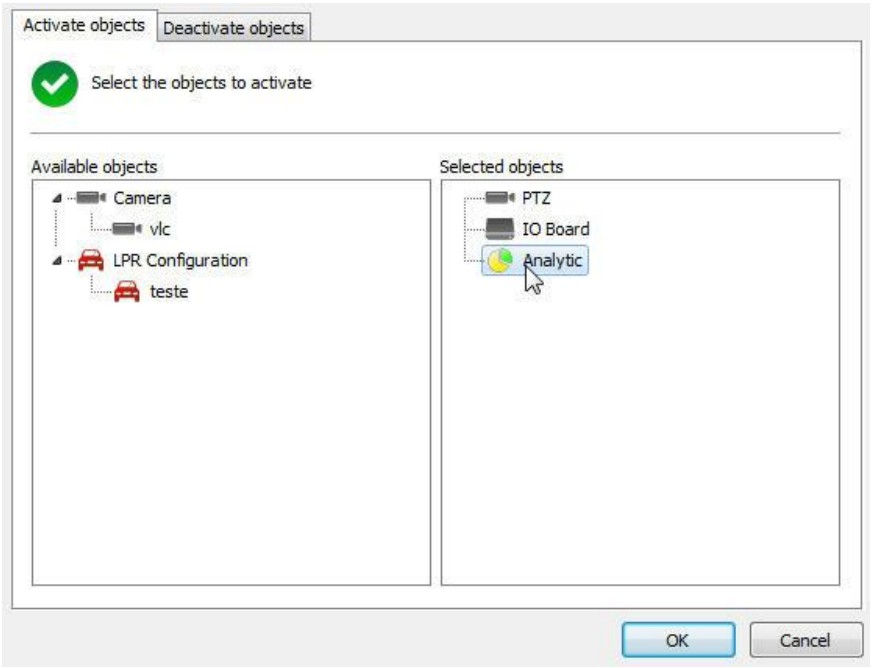
In this screen, configure the message to be displayed to the operator on the Surveillance Client.

6.1.7.4 Enable or disable system objects

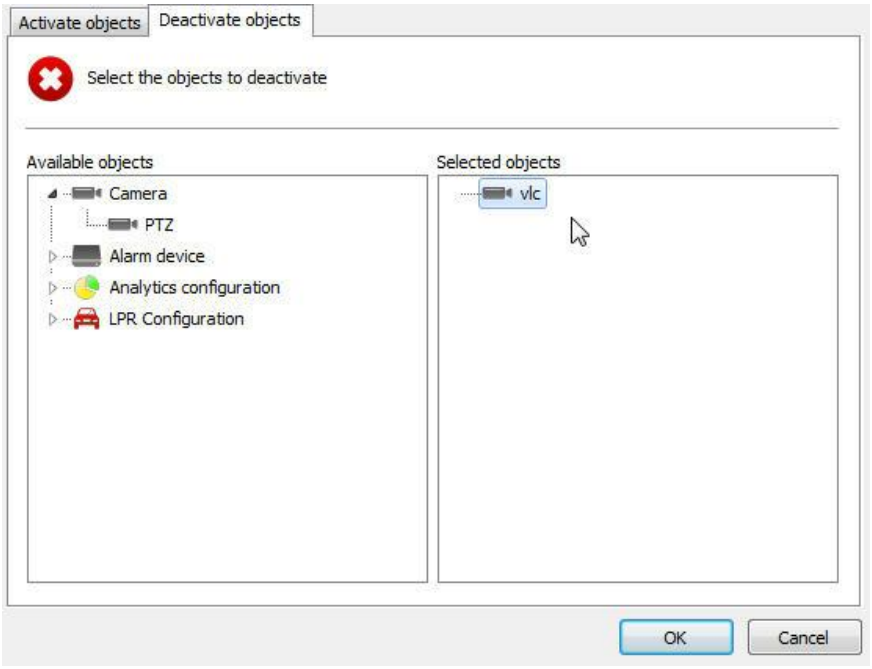
With this event, it is possible to enable and/or disable system objects. The objects that can be enabled or disabled using this action are Cameras, Alarm Devices, Maps, LPR Settings, and Analytics Configurations.

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

© 2002 - 2020 by Digifort, all rights reserved



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

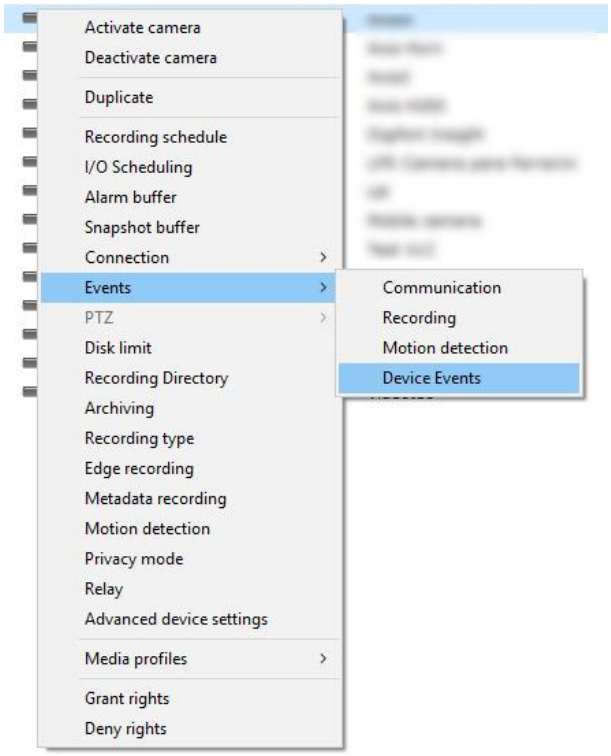


6.1.8 Camera management functions

Digifort allows the basic configurations in common with all cameras to be applied in batch.

© 2002 - 2020 by Digifort, all rights reserved

Select the desired cameras and click on the right button, opening the Options Menu, as shown in the picture below:



The options menu offers the following functions:

6.1.8.1 Activate camera

Activates the recording of the selected cameras

6.1.8.2 Disactivate camera

Disactivates the recording of the selected cameras

6.1.8.3 Duplicate camera

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

6.1.8.4 Connection

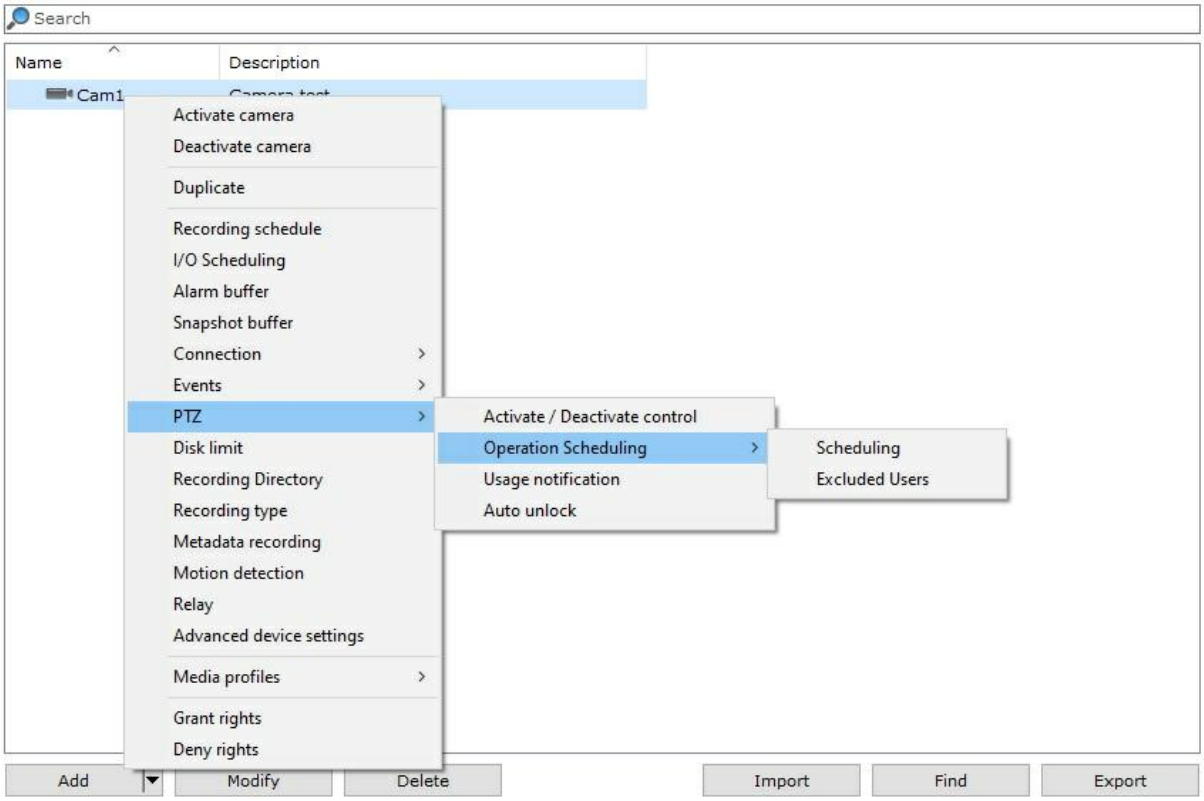
Allows changing Address, Authentication, Timeout and Visualization Timeout

© 2002 - 2020 by Digifort, all rights reserved

settings. To learn how to configure this feature, see How to add a camera.

6.1.8.5 Configuração PTZ em massa

To perform bulk PTZ configuration, follow the image below:



In your Administration Client, navigate to the Cameras section.

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

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

6.1.8.6 Type of recording

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

© 2002 - 2020 by Digifort, all rights reserved

6.1.8.7 Relay

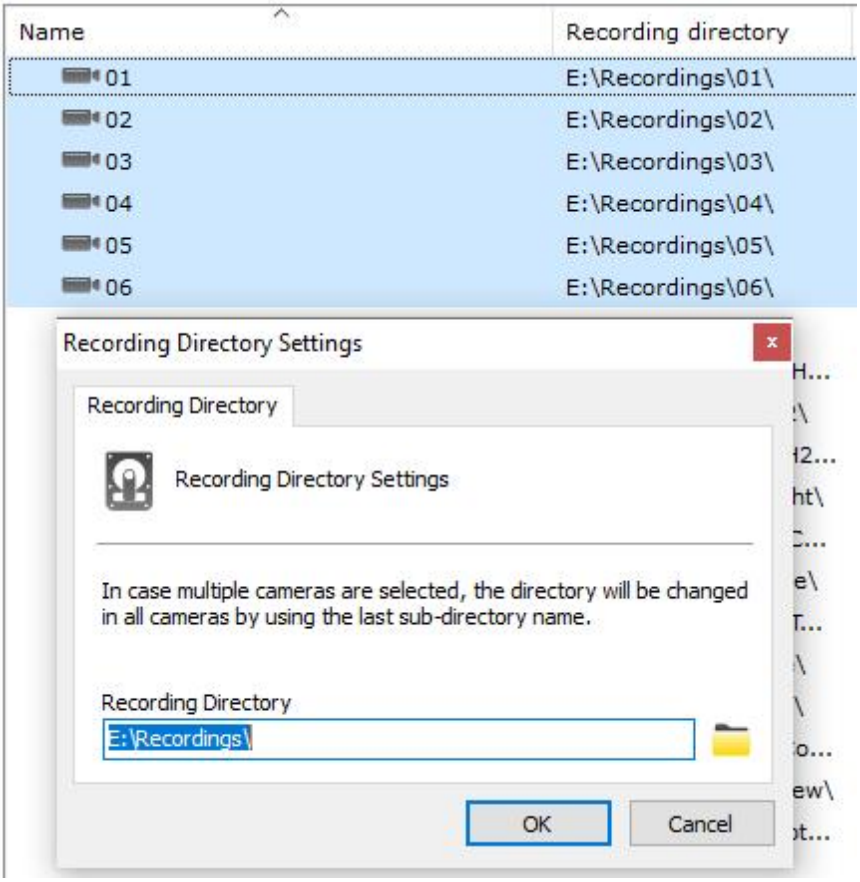
Activate Relay for the selected cameras. To learn how to config this feature see How to configure the visualization of the camera

6.1.8.8 Multiple Camera Recording Directory Change

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

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

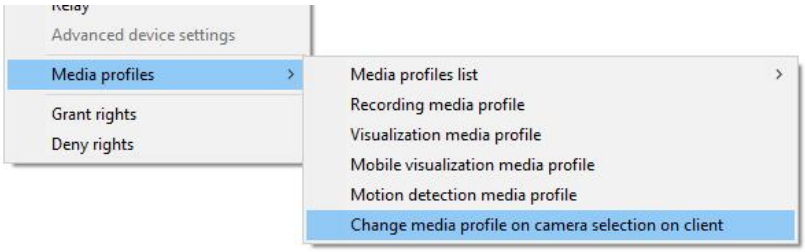
It is important to emphasize that changing the directory will not move the recordings from the old directories to the new ones. This procedure must be done manually, with the server service stopped.



© 2002 - 2020 by Digifort, all rights reserved

6.1.8.9 Media Profiles

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



6.1.8.10 Media Profiles

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

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

Camera 1
Viewing Profile
Recording profile
Mobile Profile

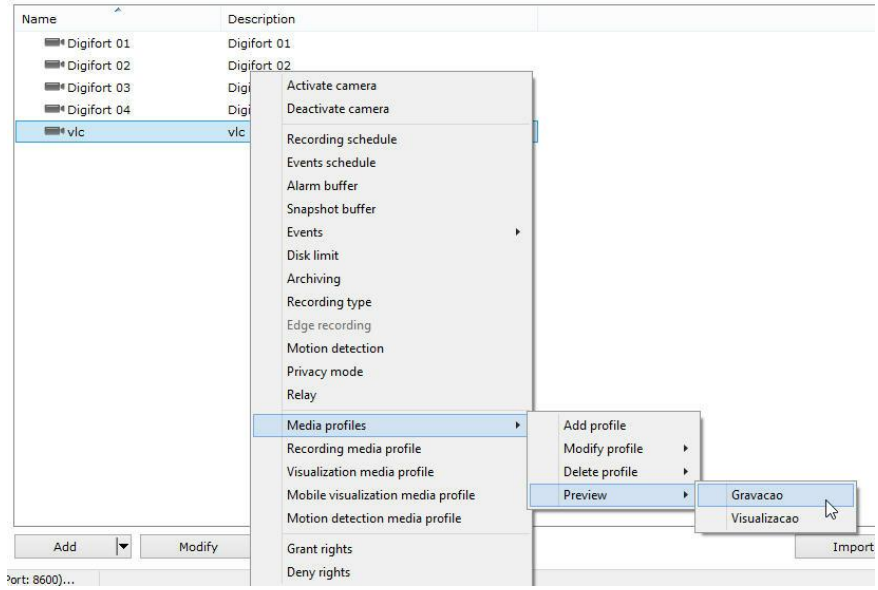
Camera 2
Recording profile

Let us analyze the following hypothesis individually:

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

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

© 2002 - 2020 by Digifort, all rights reserved



6.1.8.10.1 Mobile view ing media profile

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

6.1.8.10.2 View ing media profile

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

6.1.8.10.3 Recording media profile

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

6.1.8.11 Grant Rights

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

6.1.8.12 Deny Rights

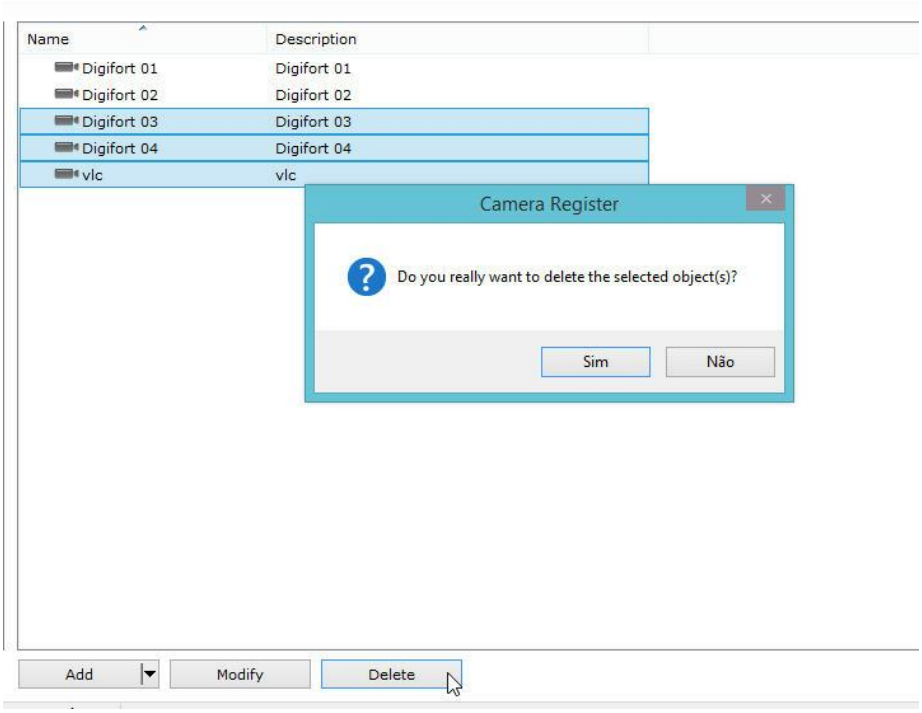
Denies user rights on devices. To learn more, see Rights .

6.1.8.13 Delete Cameras

To delete registered devices, simply select one or more devices and click the

© 2002 - 2020 by Digifort, all rights reserved

Delete button.



6.1.9 Locating and registering cameras automatically

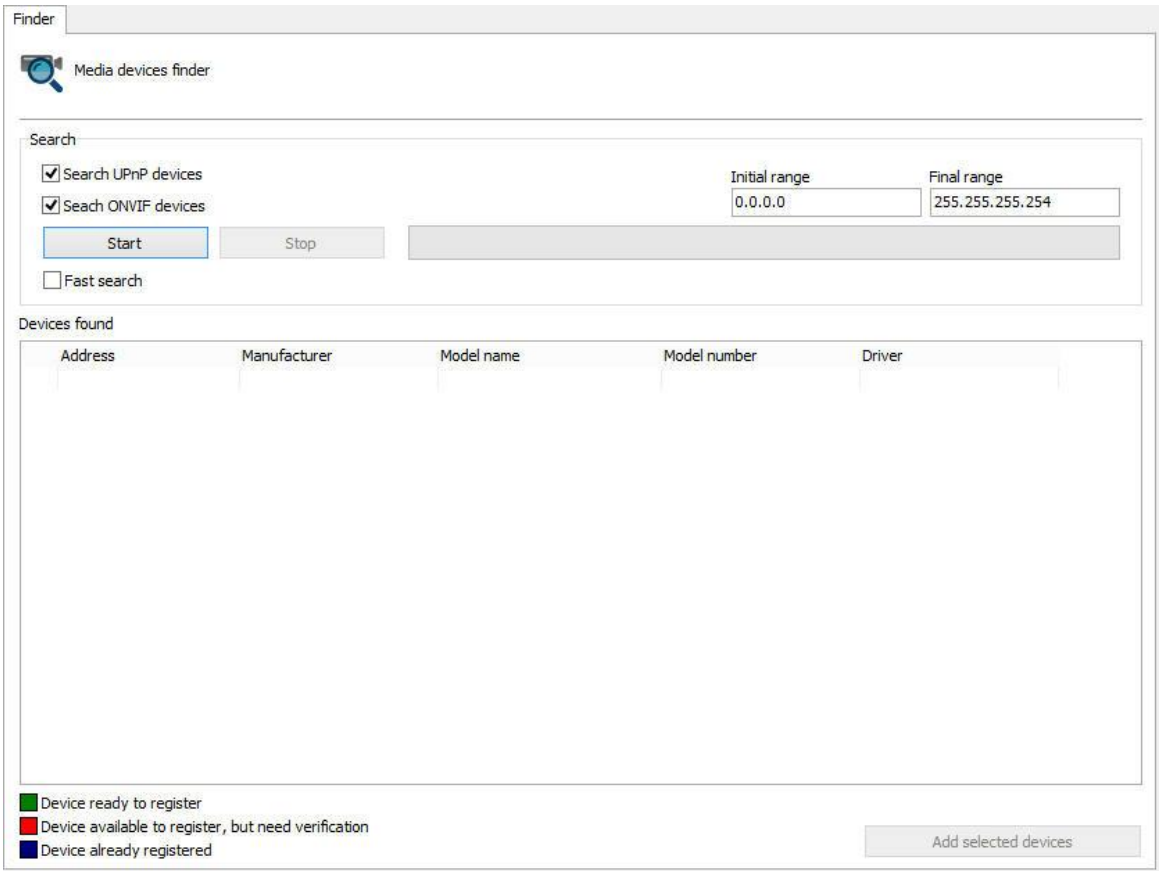
Digifort features the option of automatically locating and registering in the system those cameras with UPnP and ONVIF support.
Find out how this feature works below:

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



The following screen will be displayed:

© 2002 - 2020 by Digifort, all rights reserved

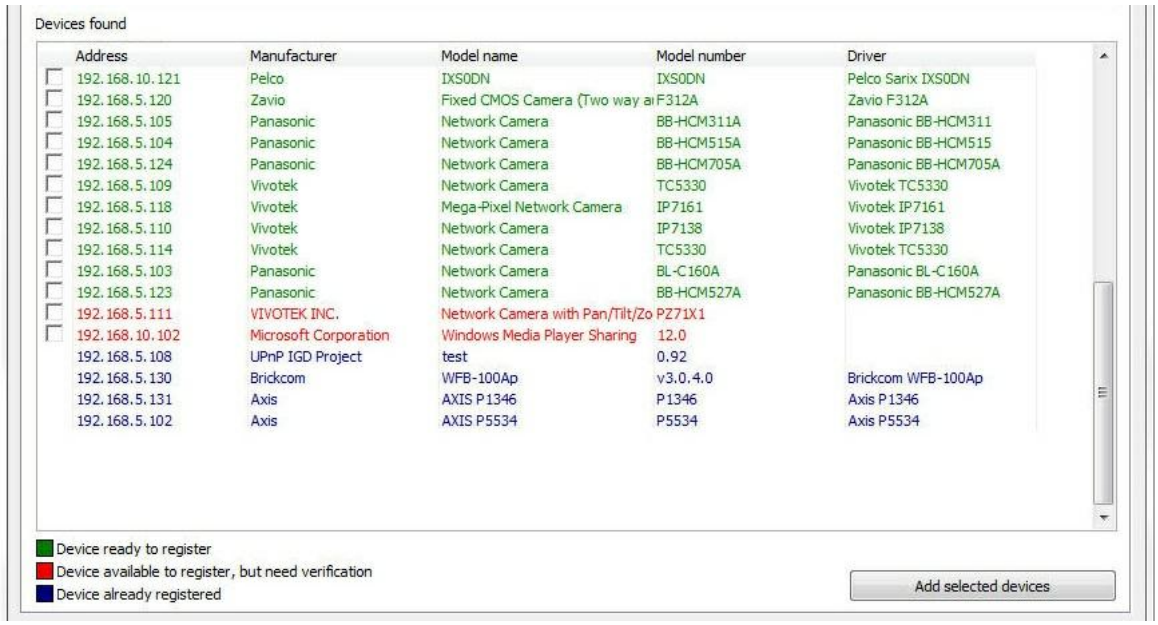


Equipment search is done on this screen. There are two types of search:

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

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

© 2002 - 2020 by Digifort, all rights reserved

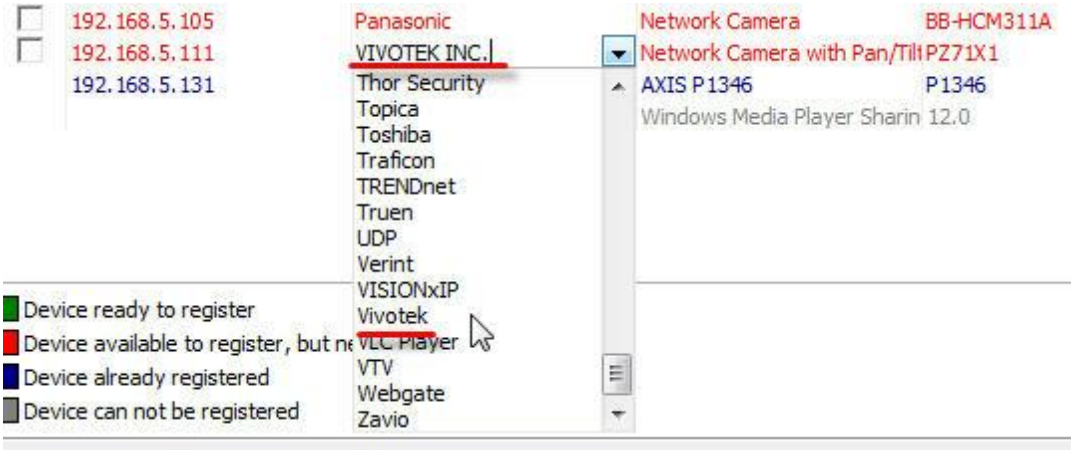


Three types of equipment can be found according to the caption in the bottom left corner of the screen:

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

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

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



- **Blue - (Device already registered**): These are equipment thathave already

© 2002 - 2020 by Digifort, all rights reserved

been registered on Digifort.

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

There are two ways to register the equipment found.

6.1.9.1 Registration of one device only

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

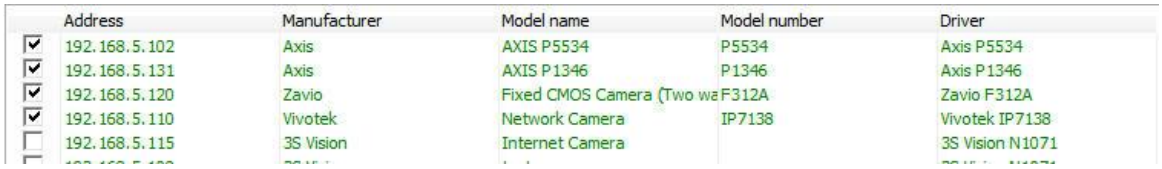


	Address	Manufacturer	Model name	Model number	Driver
☑	192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
☐	192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138

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

6.1.9.2 Registration of various devices

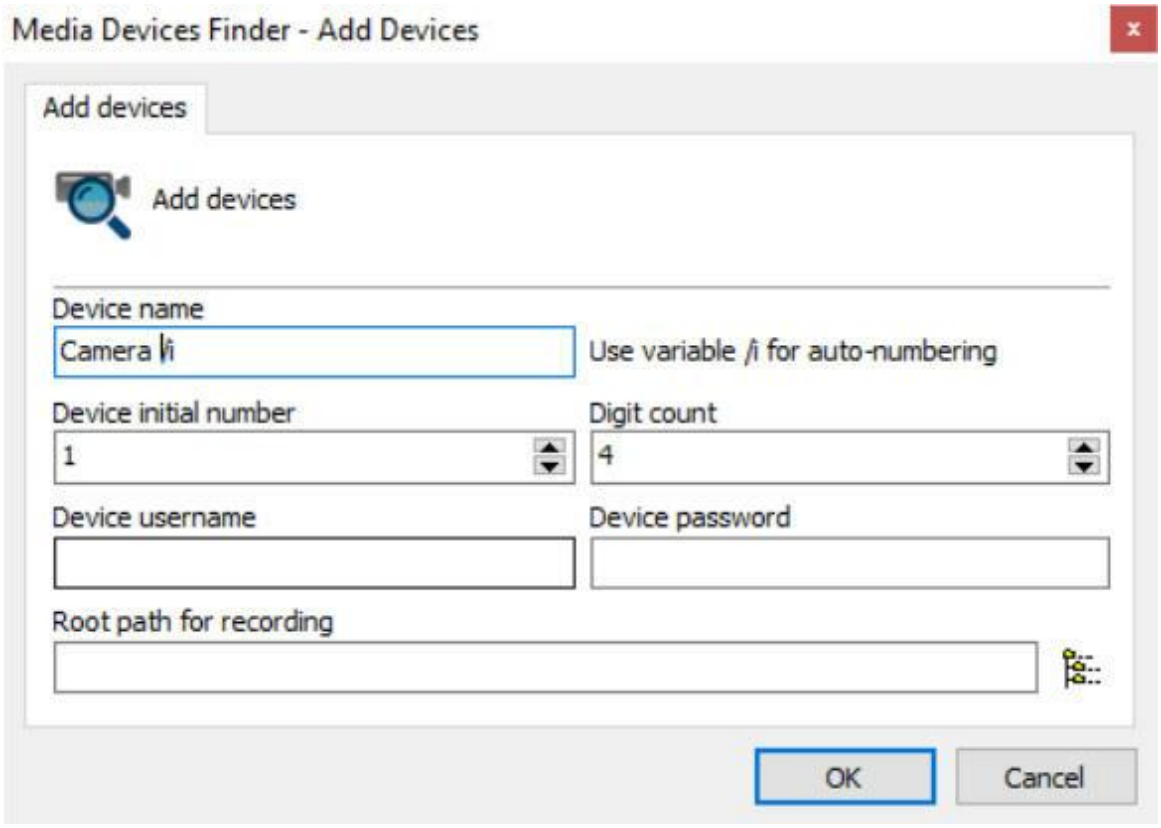
This feature can register multiple cameras simultaneously with sequential numbers. To begin, select several devices from the selection box as shown below:



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

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

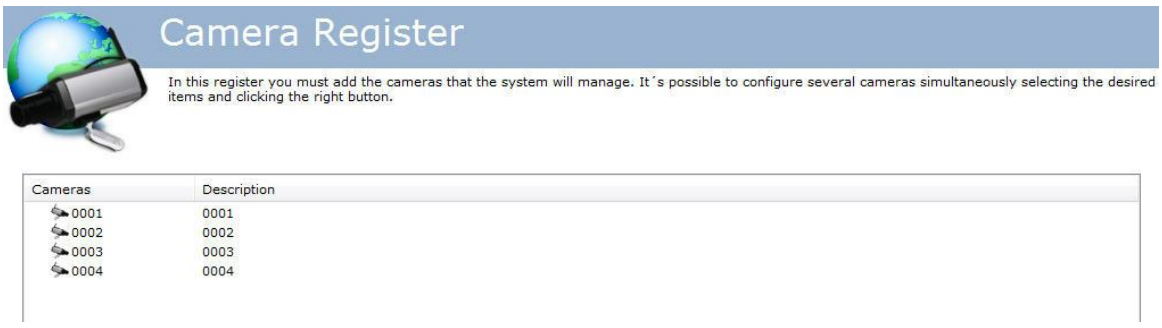
© 2002 - 2020 by Digifort, all rights reserved



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

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

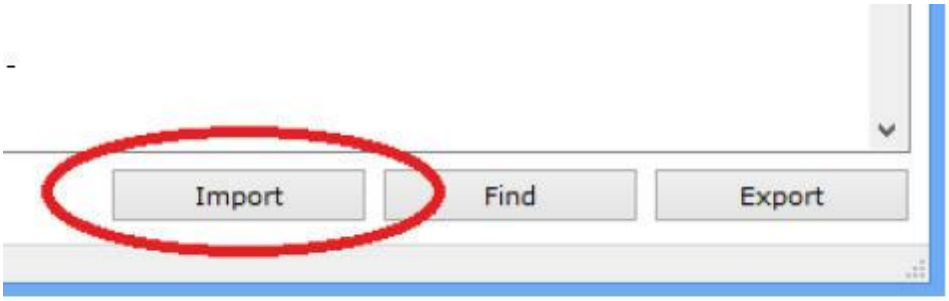
After registering various cameras, their status will change automatically to **BLUE (Camera already registered)**. This shows the cameras have been registered successfully as shown below:



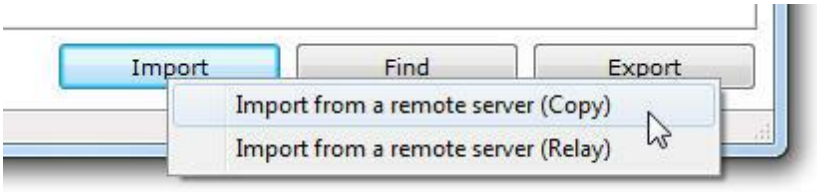
© 2002 - 2020 by Digifort, all rights reserved

6.1.10 Importar objetos de outros servidores

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



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



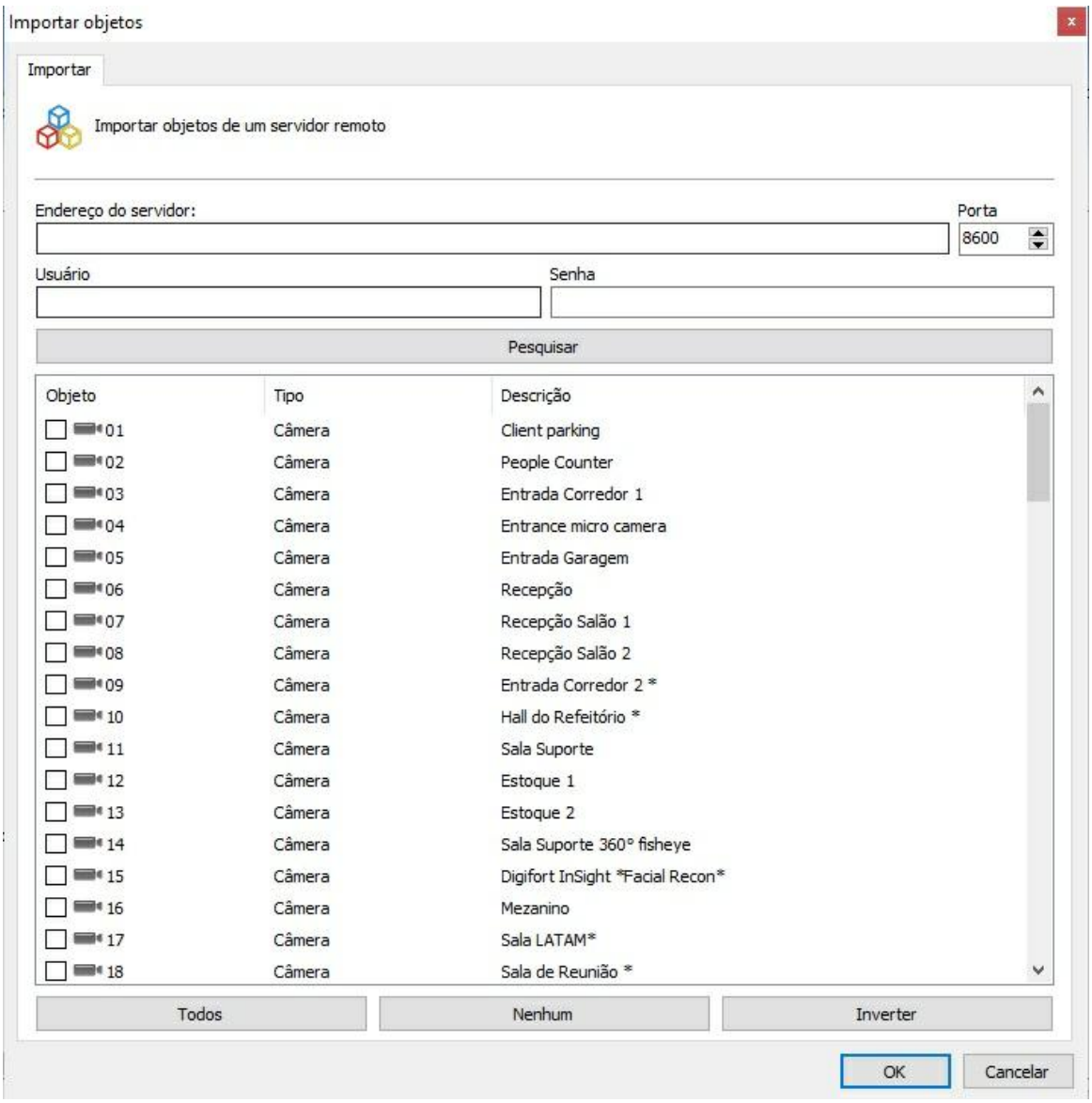
Import cameras from a remote server (copy): When the import is done as a copy, the settings will be imported just as they are on the imported server. An important example is the recording unit: if on the source server the cameraswere recording on the E: directory and in the current server this unit does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

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

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

© 2002 - 2020 by Digifort, all rights reserved

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



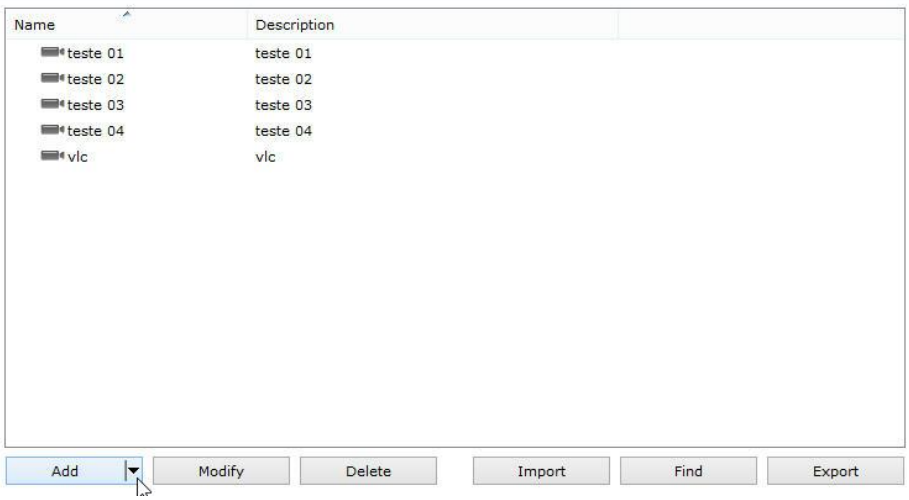
Select the desired objects and click on **OK**.

6.1.11 Multichannel device registration

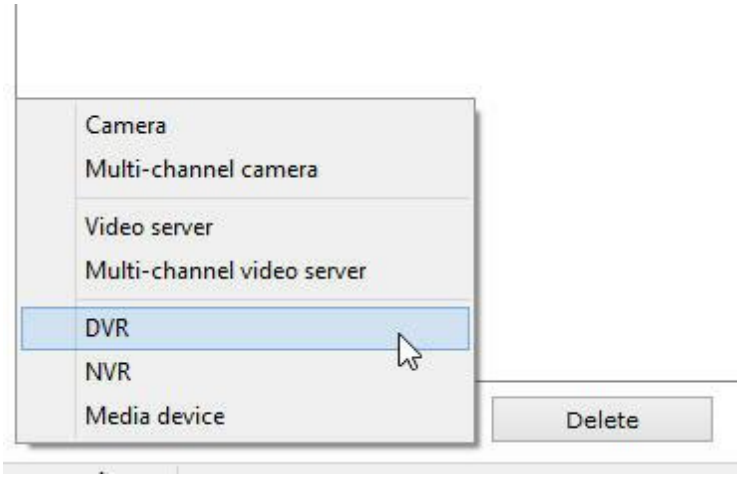
Digifort enables the registration of multichannel devices to be easily done, such as DVRs, NVRs, Video Servers, Multi-lens Cameras, etc.
For example, this option allows all channels on a DVR to be registered at once.

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

© 2002 - 2020 by Digifort, all rights reserved



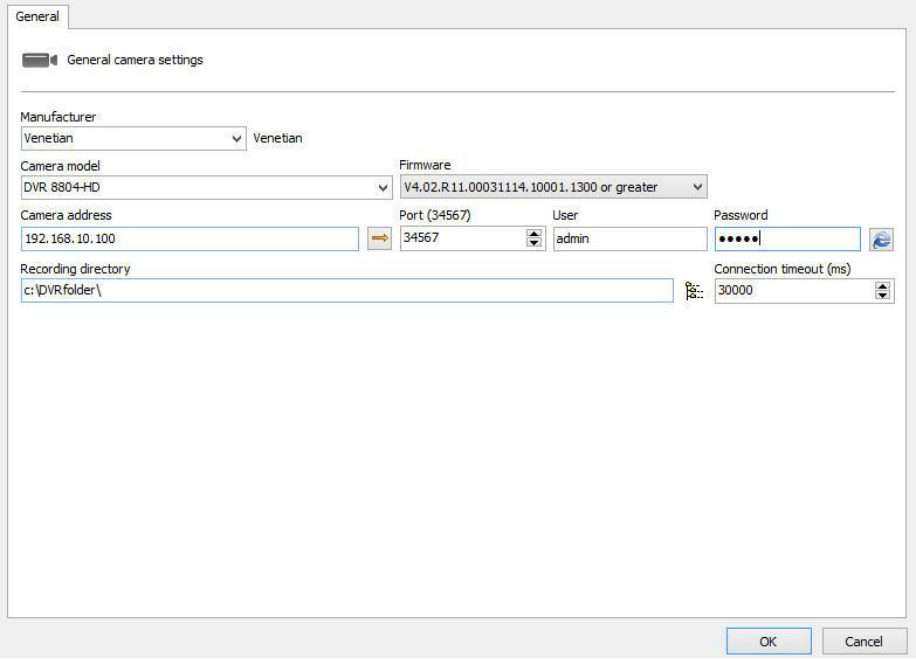
The options for those supported devices that can be registered are shown as in the image below:



6.1.11.1 Registering a DVR

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

© 2002 - 2020 by Digifort, all rights reserved



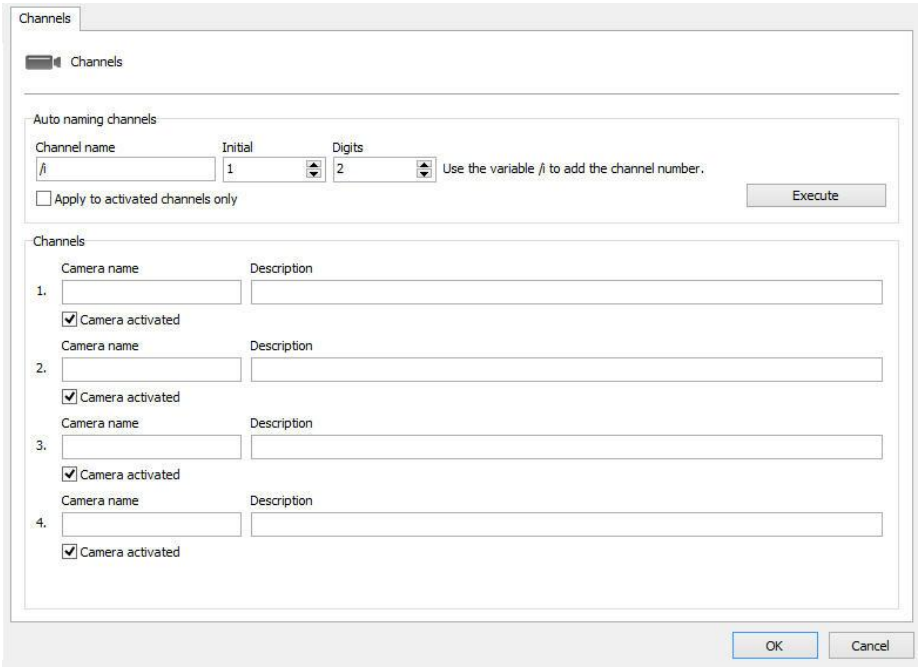
Basic information on the equipment must be filled in.**Manufacturer, Model, IP, Communications port, Username, Password, and the Directory where the recordings will be stored.**

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



The following screen will be displayed:

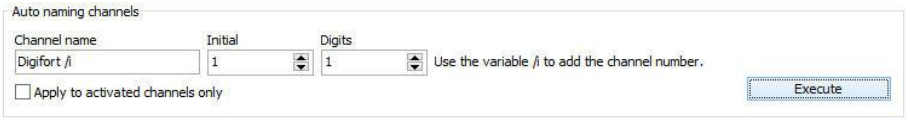
© 2002 - 2020 by Digifort, all rights reserved



The following options are available:

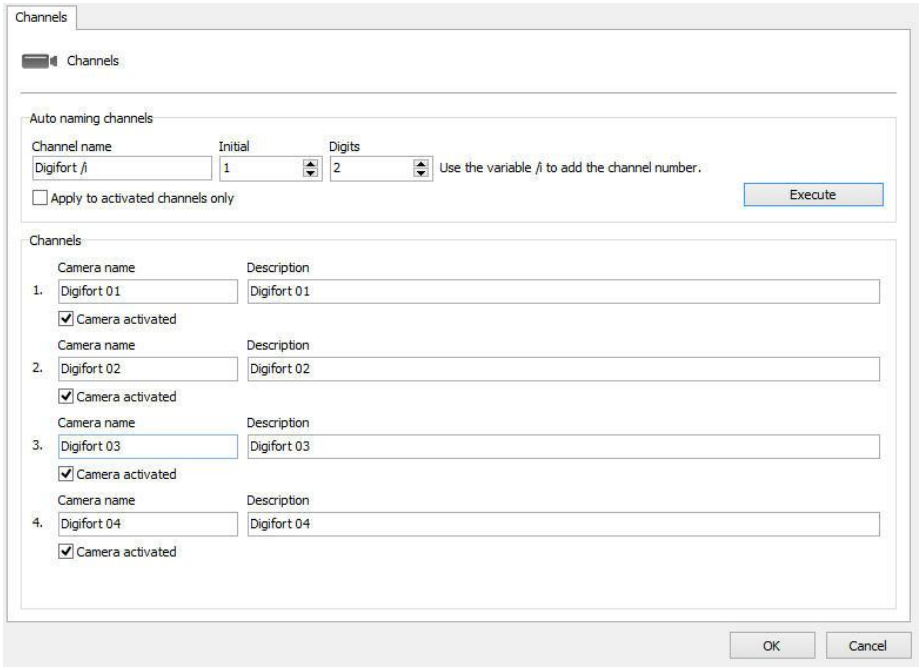
- **Auto naming Channels**: Allows a naming standard to be applied on all channels of the device.
- **Channel Name**: Desired name followed by a number (feature /i).
- **Initial**: Starting number that will be applied to the channels.
- **Digits**: Number of digits that are required for naming.
- **Apply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

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



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

© 2002 - 2020 by Digifort, all rights reserved

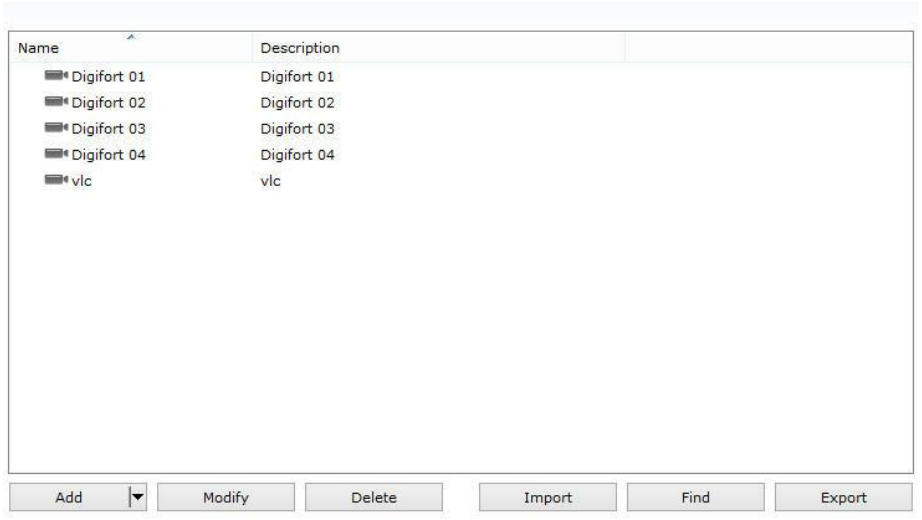


In the **Channels** area, it is possible to check/modify the name applied.
It is important to remember that each channel is registered as an independent device, thereby consuming 1 recording license per registration.

NOTE: The device name cannot be changed after registration.

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

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



© 2002 - 2020 by Digifort, all rights reserved

6.2 Camera Groups

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

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

The Surveillance Client offers great flexibility towards working with groups:

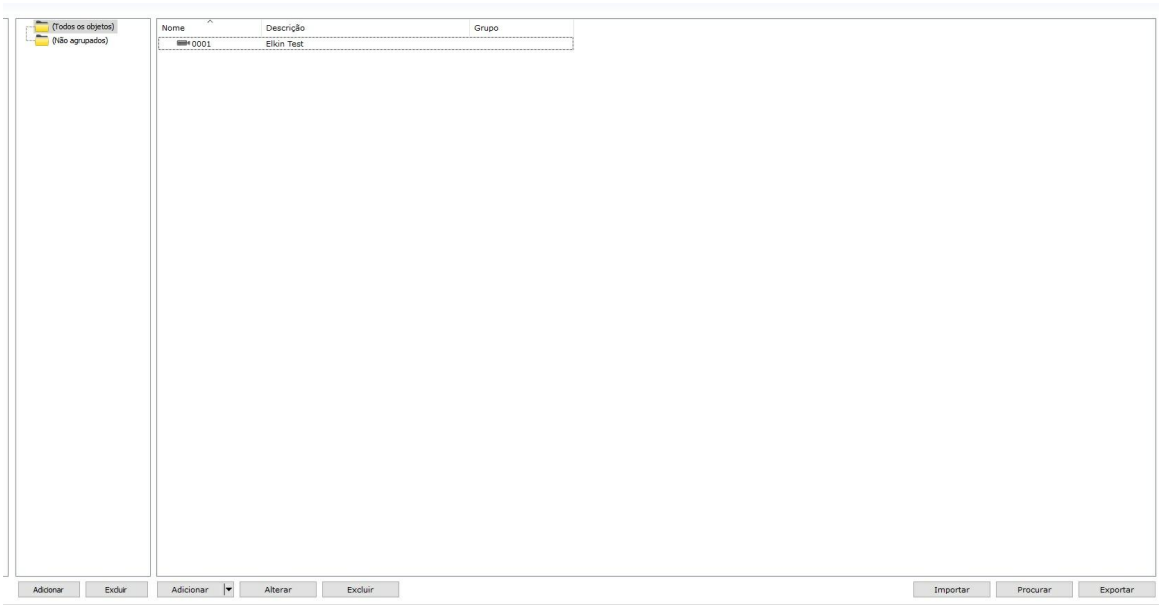
- You can drag and drop a group on the screen, and cameras from that group will be added to the surveillance.
- To add cameras from the group and all cameras from all subgroups, simply press and hold the Shift key while dragging and dropping the desired group.
- You can drag and drop a group onto the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

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



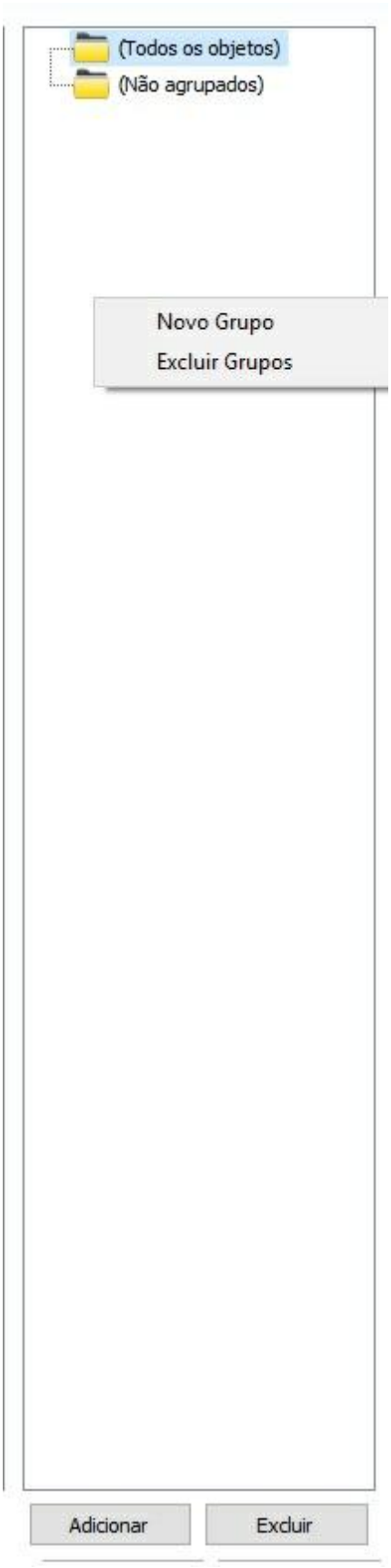
Once this is done, camera registration will be displayed, as illustrated in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



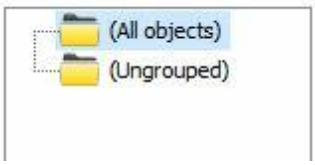
To add a group, click on the Add button in the groups section, on the left, or right-click on the group zone as shown in the image below.

© 2002 - 2020 by Digifort, all rights reserved



© 2002 - 2020 by Digifort, all rights reserved

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

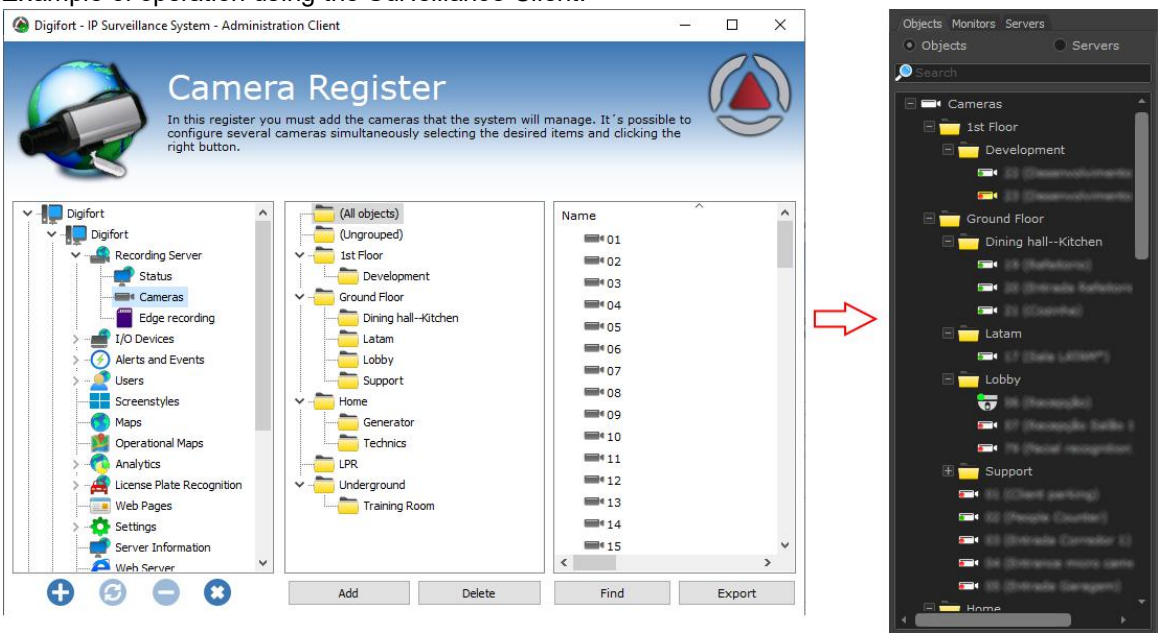


Once the group has been created, to add one or more cameras to the group, simply click on the desired camera(s) and drag it/them to the group. You can also create subgroups by simply creating a new group with the larger group selected or then drag all desired groups into a larger group:



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

Example of operation using the Surveillance Client:



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

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

© 2002 - 2020 by Digifort, all rights reserved

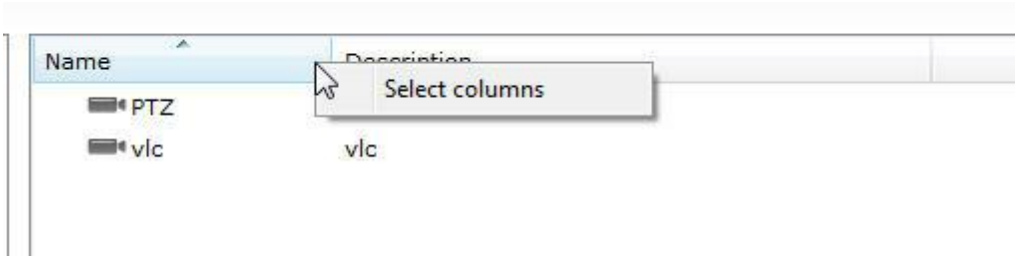
youtube.com/DigifortChannel

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

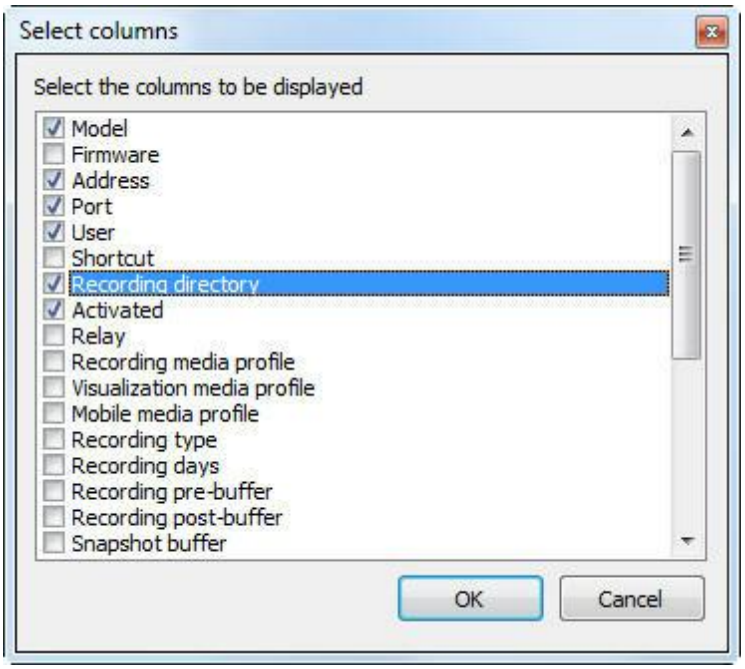
6.3 Column Organization

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

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

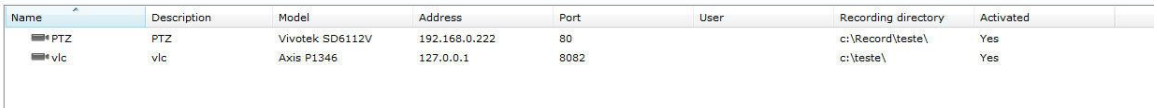


The following screen will appear with the available columns options:



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

© 2002 - 2020 by Digifort, all rights reserved



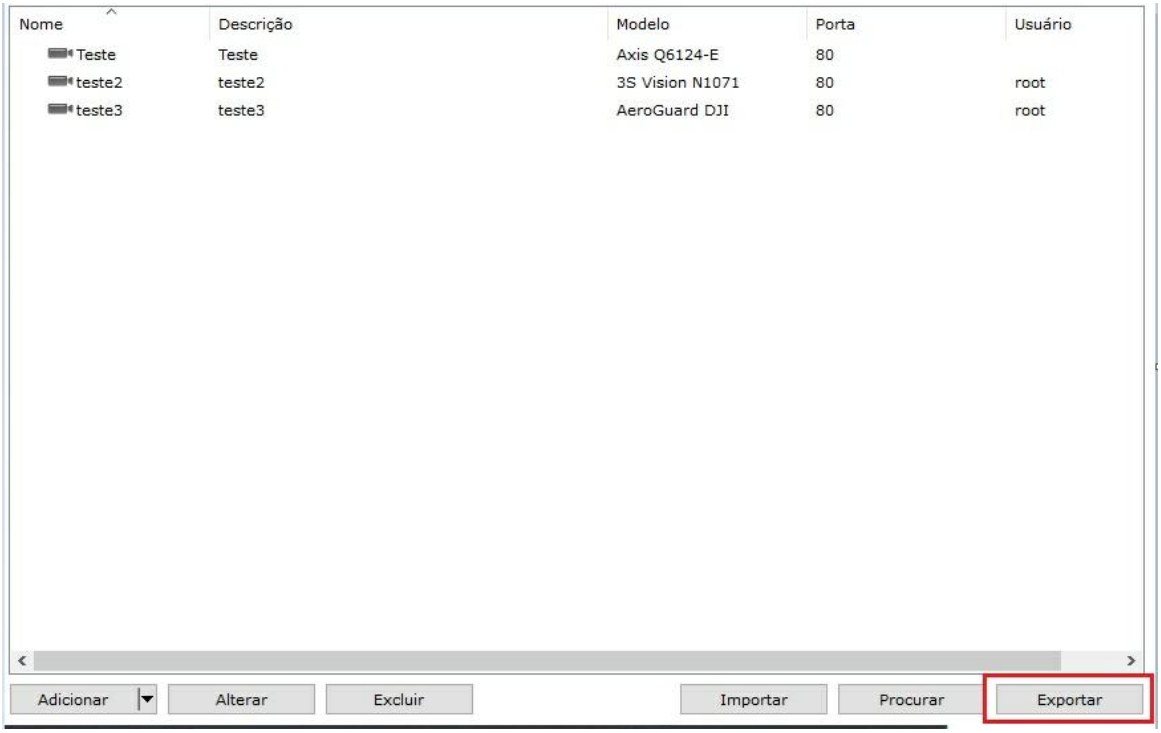
Name	Description	Model	Address	Port	User	Recording directory	Activated
PTZ	PTZ	Vivotek SD6112V	192.168.0.222	80		c:\Record\teste\	Yes
vlc	vlc	Axis P1346	127.0.0.1	8082		c:\teste\	Yes

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

6.4 Exporting Data from the Recording Server

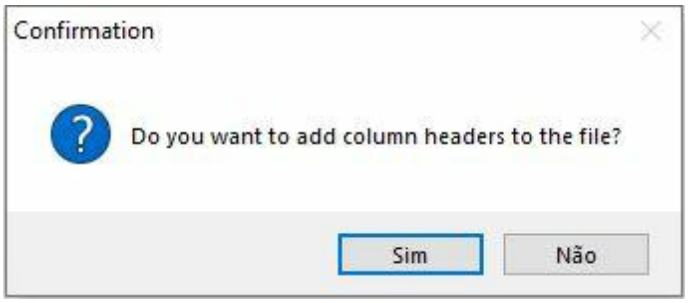
The Digifort Administration Client can export in the .CSV format, which contains a summary of the recording server.Such information can be used for various purposes, such as reports and controls.

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



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

© 2002 - 2020 by Digifort, all rights reserved



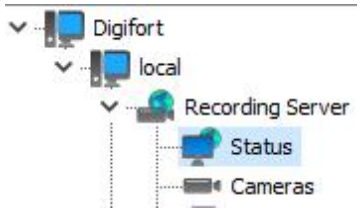
This window requests the confirmation to export the columns being displayed in your Recording Server. In the above example, the Name, Description, Model, Port, and User columns will be exported, as follows:

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

6.5 Monitoring recording server status

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

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



The status screen allows the selection of custom columns with new information to be displayed in the list (by right-clicking on the list header) and sorting by any column of the list. In addition, you can export the current data in a .CSV file.

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

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

© 2002 - 2020 by Digifort, all rights reserved

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

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

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



Details:

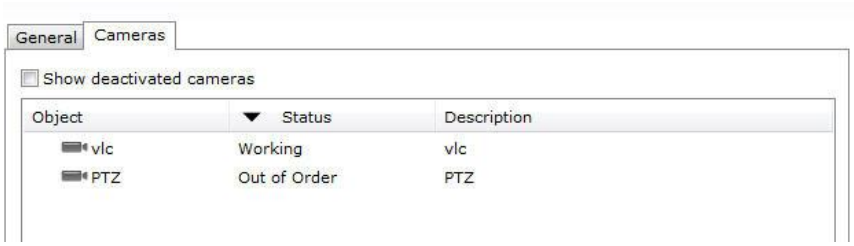
- **Total**: Total number of cameras registered on the server.
- **Activated**: Number of activated cameras.
- **Deactivated**: Number of deactivated cameras.
- **In operation**: Number of cameras in operation.
- **Recording**: Number of cameras that are recording.
- **Total FPS:** Total number of frames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

© 2002 - 2020 by Digifort, all rights reserved

6.5.1 Monitorando o status de câmeras individualmente

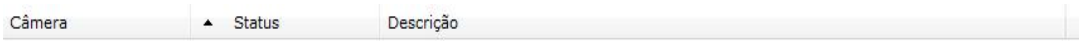
In this area of the system you can check the individual status of each camera, obtaining information such as its operating status, IP address, uptime, used disk space, etc.

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



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

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



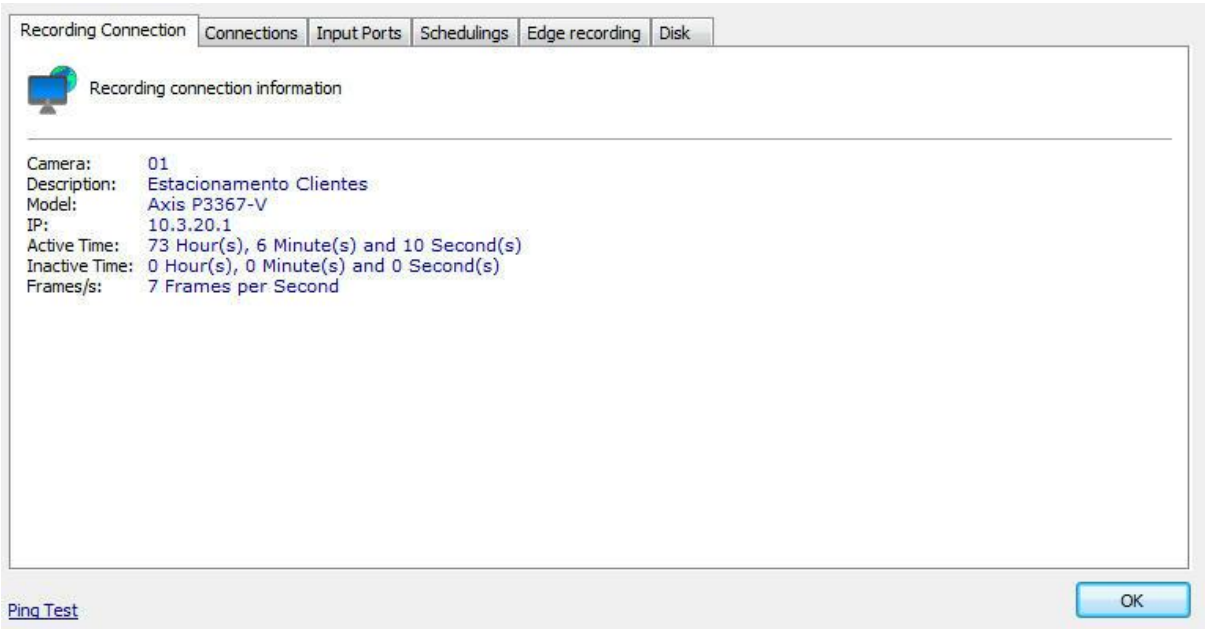
To view the details of the operation of each camera, double-click on the desired camera. Details will be described in the following topics.

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

6.5.1.1 Conexão de Gravação

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

© 2002 - 2020 by Digifort, all rights reserved



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

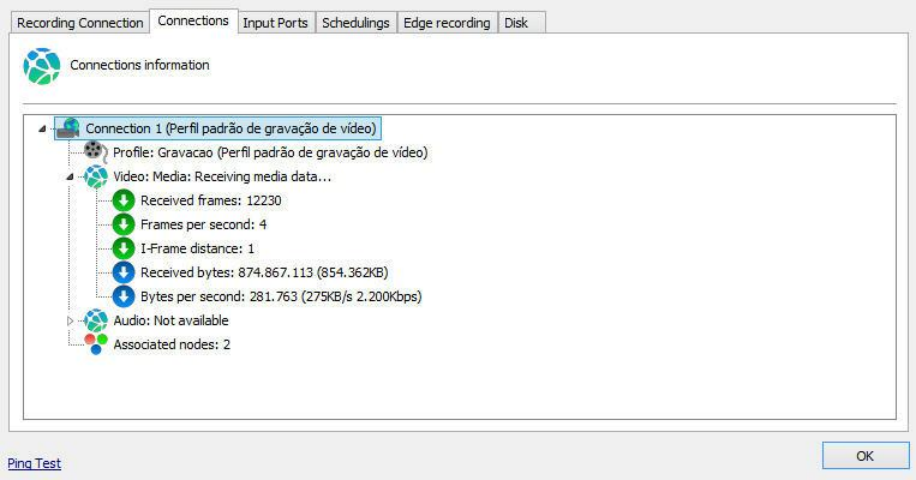
6.5.1.2 Conexões

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

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

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

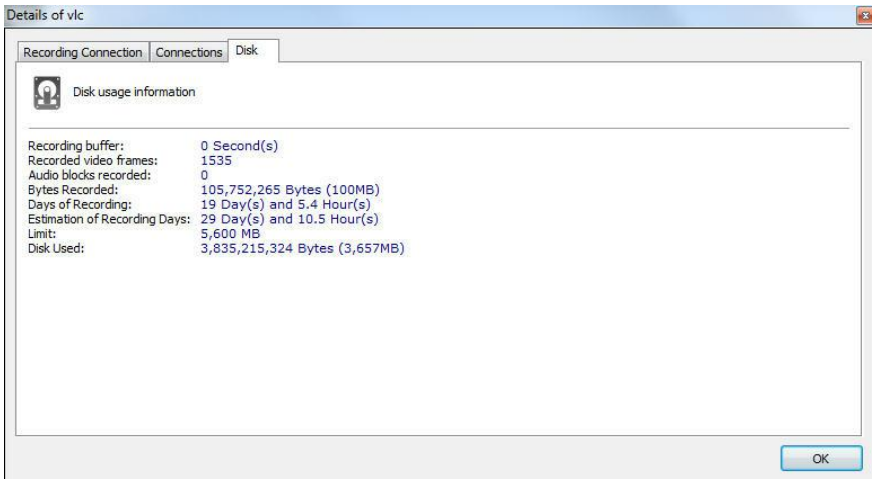
© 2002 - 2020 by Digifort, all rights reserved



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

6.5.1.3 Disco

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



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

© 2002 - 2020 by Digifort, all rights reserved

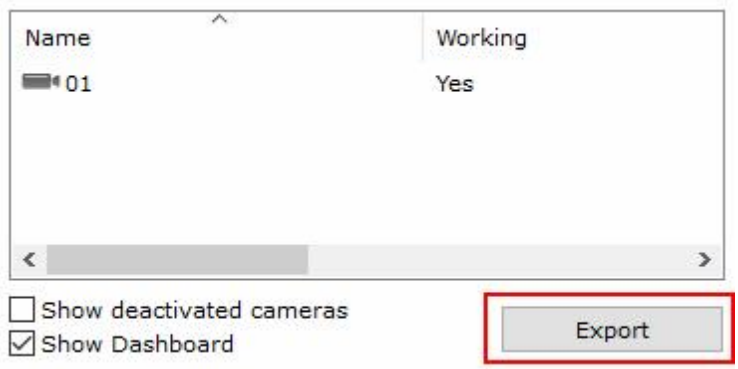
on the Recording Recording Cycle

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

6.5.1.4 Exportação de dados na tela de Status

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

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



Screens with export button support:

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter VII

7 Alerts and Events

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

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

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

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

7.1 How to access the Alerts and Events

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



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

7.1.1 How to configure the contacts

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

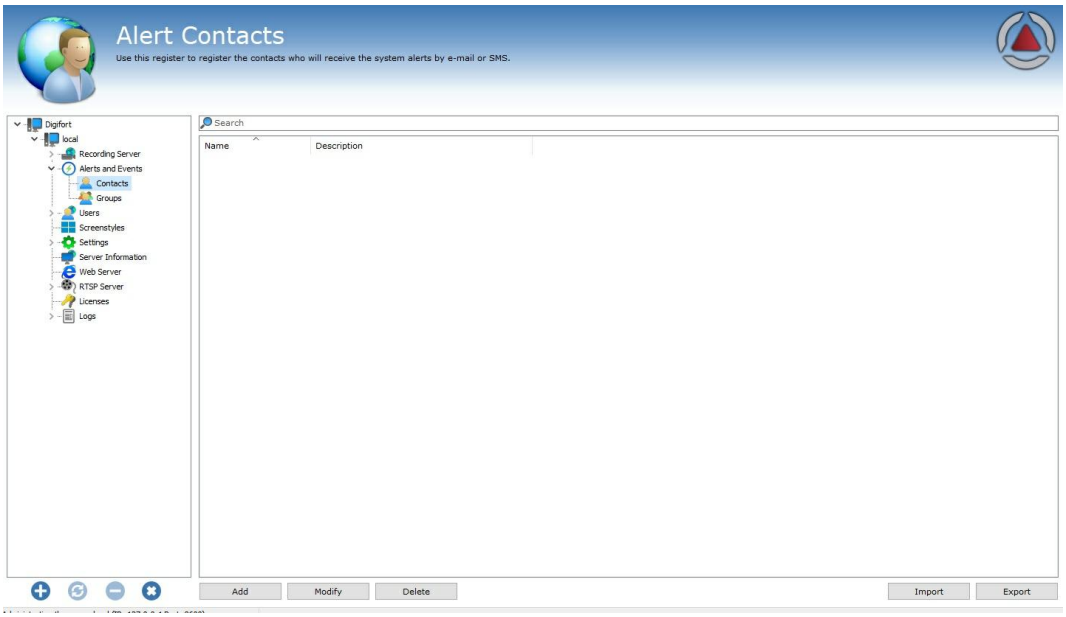
Digifort sends e-mail messages not only to a contact, but also to groups of contacts.

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

© 2002 - 2020 by Digifort, all rights reserved



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



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

7.1.2 How to configure the contact groups

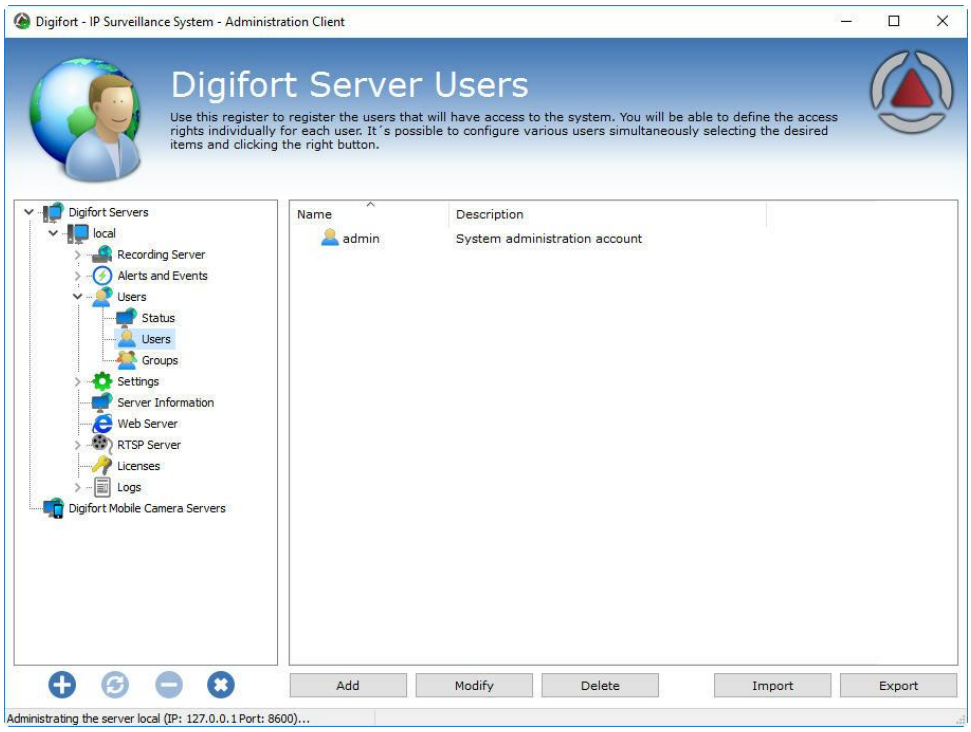
The creation of contact groups is necessary, since Digifort sends e-mail notifications not only to a contact, but also to a group of contacts.

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

© 2002 - 2020 by Digifort, all rights reserved



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



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

© 2002 - 2020 by Digifort, all rights reserved

Chapter VIII

8 User administration

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

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

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

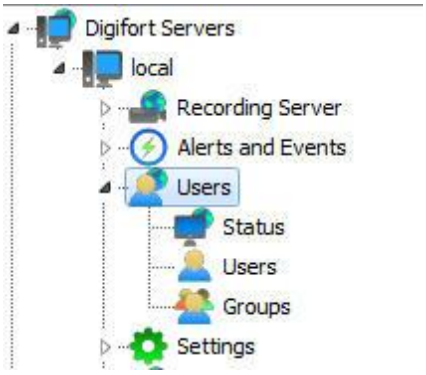
These users must be of the utmost trust to the company, as a security solution only works with trustworthy equipment and personnel.

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

NOTE: To facilitate the management of multiple servers, the Administration Client will now reuse login credentials for all servers. If the login is successful on 1 server, when connecting to another server, these same credentials will be used automatically, facilitating the administration process since it will not be necessary to enter the login credentials for all servers. An exception is if 2-factor authentication is enabled, then you will need to provide the 2-factor key at each login.

8.1 Administrating users

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

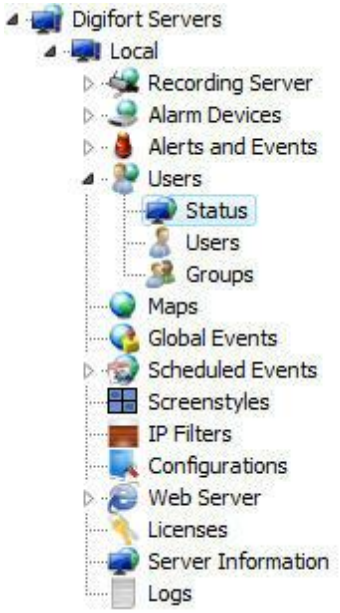


© 2002 - 2020 by Digifort, all rights reserved

8.1.1 Monitoring user activity

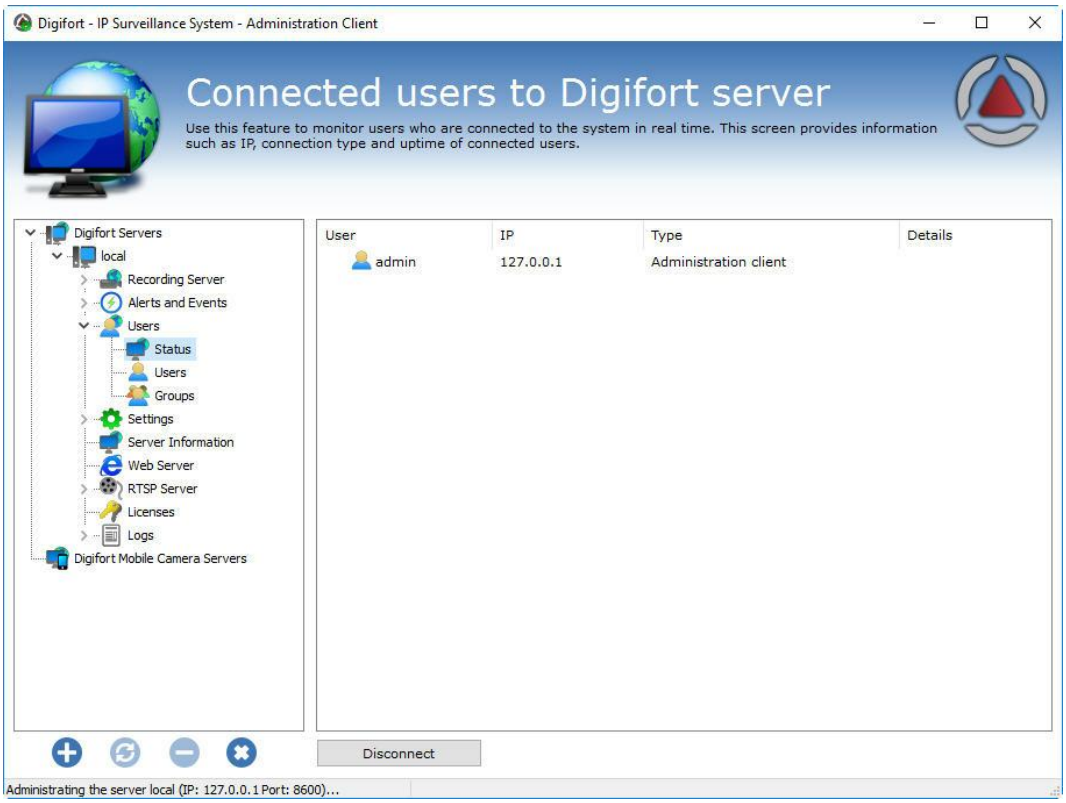
This feature is very important for the security of the server, since logged-in users' activity is monitored here. If the user is taking an undue action, he can be disconnected or blocked.

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



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

© 2002 - 2020 by Digifort, all rights reserved

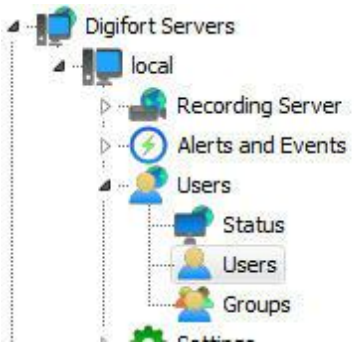


All presently logged-in users of the system are displayed, showing information such as user name, IP address, server access type, and connection time.

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

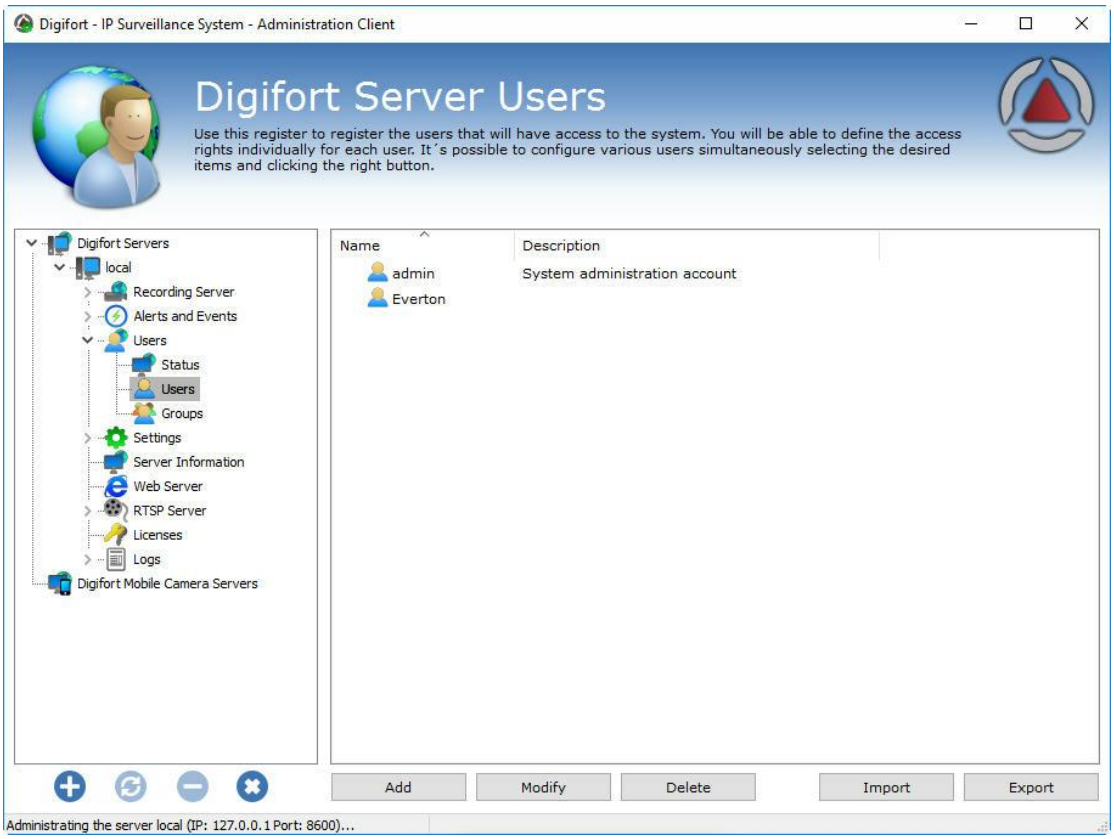
8.2 Adding, modifying and excluding users

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



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

© 2002 - 2020 by Digifort, all rights reserved



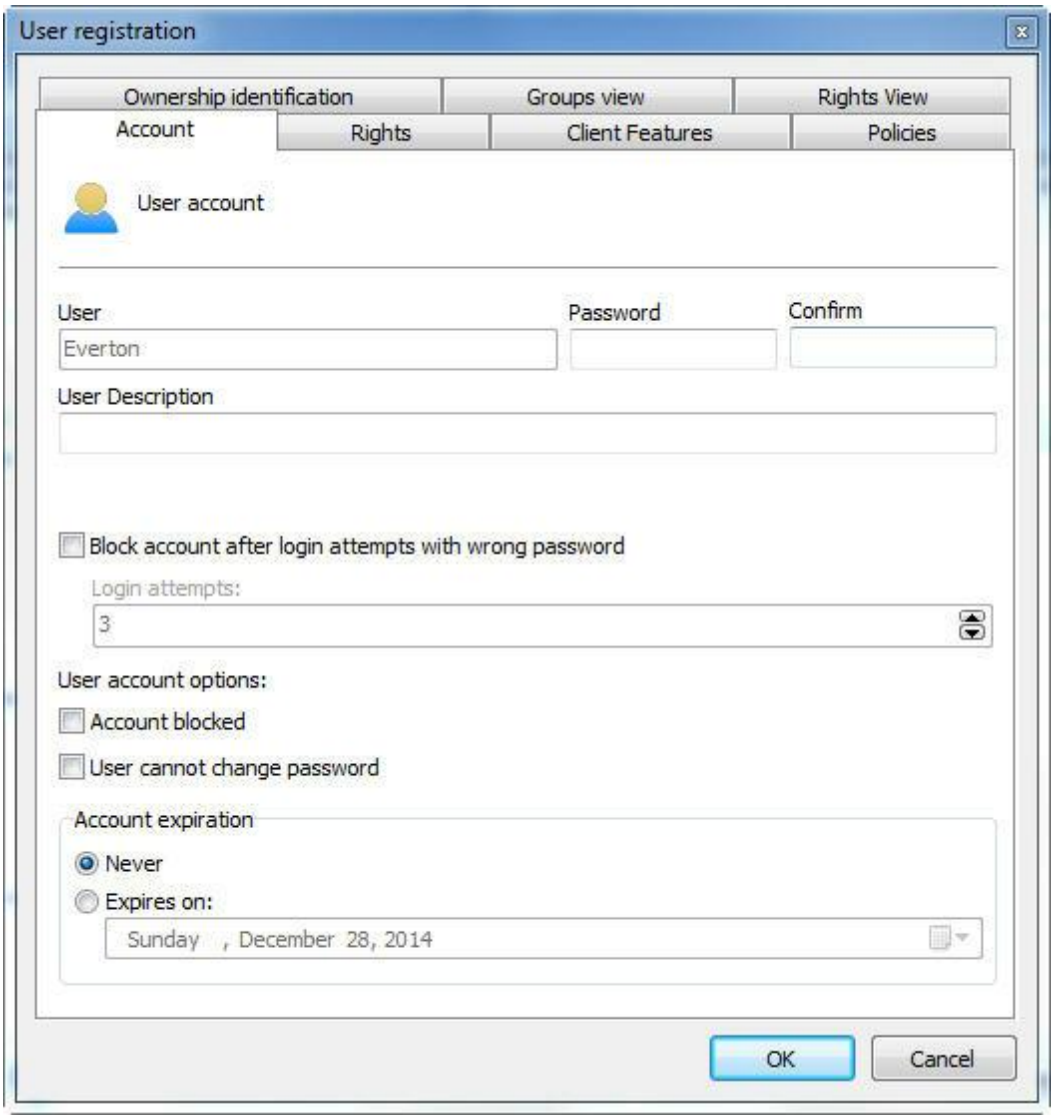
After clicking on the **Add** button, the users editing screen will be opened. Let's start by inserting the user's data, followed by the rights and, lastly, the client features.

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

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

8.2.1 User data

© 2002 - 2020 by Digifort, all rights reserved



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

- **User**: Name of the user. This must be informed at login in any module of the Digifort System. After being saved it cannot be modified.
- **Password**: The user's password.
- **Confirm**: Enter the user's password again.
- **Description of the user:** A brief description of the user, for aiding in his identification in the system.
- **Block user by invalid login:** If enabled, the system will block the account of the user who logs in with the wrong password for more than X attempts that are configurable
- **User account options**:
  - **The user cannot change the password**: With this option marked, the user can never change his password, leaving this up to the system administrator.
  - **This user will receive alerts**: With this option marked, the user will receive the configured alerts when some event occurs.
  - **Account blocked**: With this option marked, the user will not be able to authenticate himself in the system.

© 2002 - 2020 by Digifort, all rights reserved

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

Tip

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

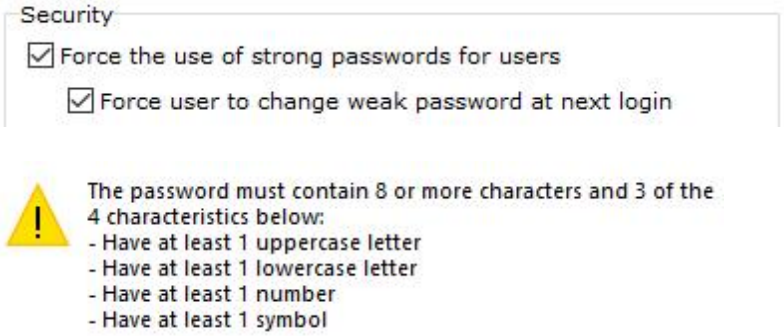
8.2.1.1 Force use of Strong Password

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

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

Upon activating the option to force the use of strong password, new users can only be registered with a strong password. The system also allows you to force the change of a weak password (if the user is currently using a weak password) the next time the user logs in through the Surveillance Client or the AdministrationClient.

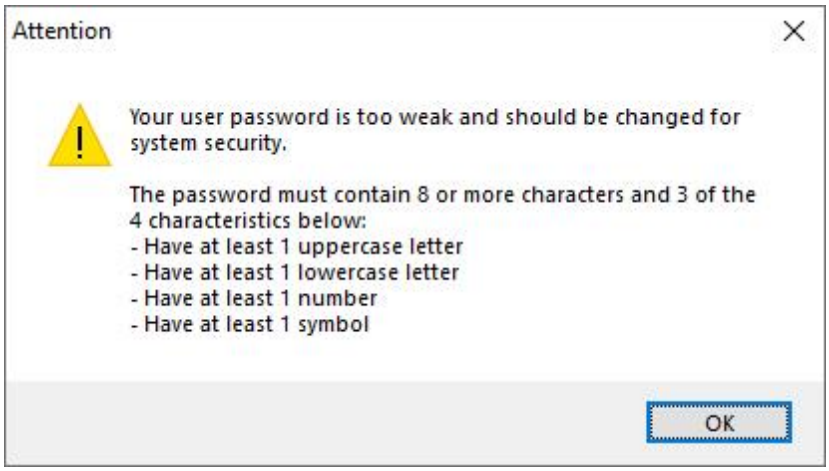
The use of a strong password applies only to native users of the system and not to LDAP/Active Directory users, where the strong password requirement must be applied directly at the domain controller.



© 2002 - 2020 by Digifort, all rights reserved

8.2.1.1.1 Weak Password Alert

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

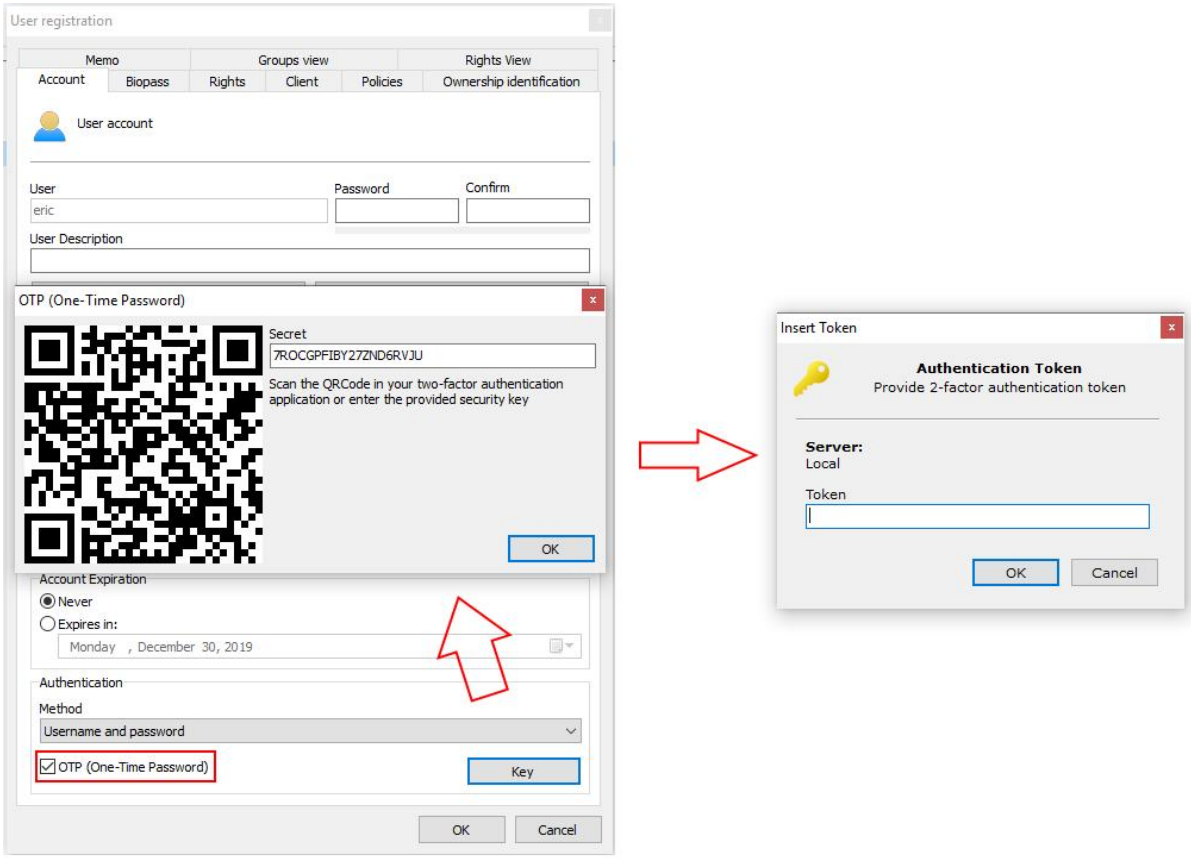


8.2.1.2 2-Factor Authentication

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

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

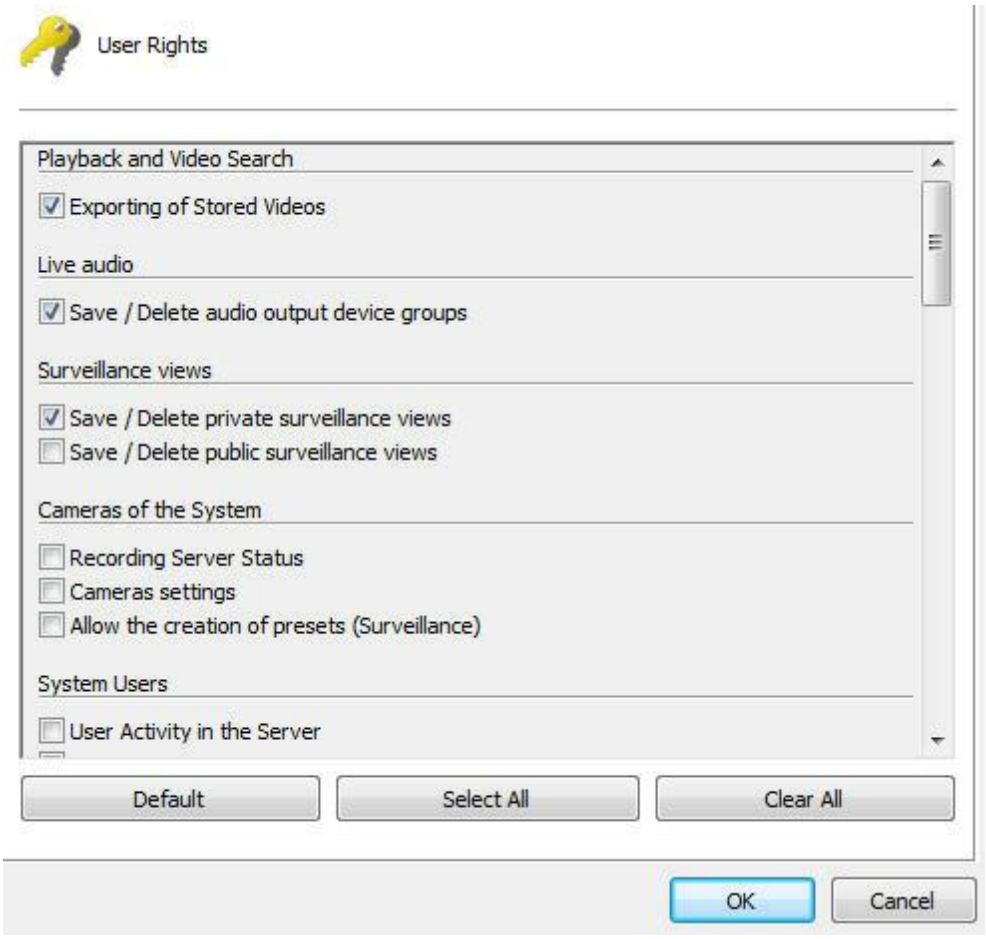
© 2002 - 2020 by Digifort, all rights reserved



8.2.2 User rights

After completing the user primary data, user access rights must be configured. By default rights are configured for a surveillance user profile, that is, it can only perform live surveillance operations and video playback in the system.

© 2002 - 2020 by Digifort, all rights reserved



8.2.2.1 Video Search and Playback

- **Export stored videos**: Allows the user to export videos previously recorded for backup, or to view them on another workstation. To learn how to export videos, check the Surveillance Client manual.
- **Advanced search**: Allows the user to perform advanced searches in stored videos. Advanced Search helps searching for incidents on a scene. To learn about Advanced Search, check the Surveillance Client manual.

8.2.2.2 Surveillance Views

- **Save / Delete private surveillance views**: Allows the user to save or delete the surveillance views regarding their account.
- **Save / Delete public surveillance views:** Allows the user to save or delete the surveillance views regarding all users connected to the Digifort server.

8.2.2.3 System Cameras

- **Recording Server Status**: Allows the user to check the overall system status and the

© 2002 - 2020 by Digifort, all rights reserved

individual status of each camera, obtaining information such as disk space used, received frames per second, uptime, etc. See more at Recording Server.
- **Camera Configuration**: Allows the user to configure the cameras to be managed by the system.
- **Allow blocking of PTZ controls**: Allows the user to block the camera movement by priority.
- **Allow the creation of presets (Surveillance)**: Allows the user to save presets via surveillance client.
- **Allow the control of privacy mode:** Allows the user to activate the privacy mode of a camera, if configured.

8.2.2.4 Alarm Devices

- **Alarm Devices Settings**: Allows the user to access the alarm devices settings. See more at Alarm Devices..
- **Alarm Devices Status**: Allows the user to access the monitoring of alarm devices status.

8.2.2.5 Alarms

- **Activate alarm output scripts**: Allows the operator to trigger the alarm outputs. See more at Alarm Devices..

8.2.2.6 System Users

- **Users' activities on the server**: Allows the user to monitor users' activity on the server. To learn how to use this feature, check Monitoring users' activities
- **Users' Registration**: Allows the user to access the users' directory.

8.2.2.7 Alerts and Events

- **Alert contacts registration:** Allows the user to access the alert contacts registration. The contacts must be registered to receive notifications about anomalies in the system or occurrence of incidents. See more at Alerts and Events..
- **Alert logs view**: Allows the user to view the alert logs.
- **Allow manual events activation**: Allows the user to activate the manual events such as a siren through Digifort.

8.2.2.8 Server

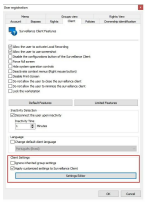
- **Server Configuration**: Allows the user to change the system global settings, such as limit of connections to the server, disk recording limits, etc.
- **Server monitoring:** Allows the user to monitor the displayed information about the server. See more at Server Information..
- **Server logs view**: Allows the user to access the server logs configuration. See more at System Logs..

© 2002 - 2020 by Digifort, all rights reserved

8.2.3 Surveillance Client Features

The configuration of the Surveillance Client Features is very important for the security of a site. This feature provides tools that affect the person who monitors the cameras, causing other factors to interfere with the operator's attention.

To access these tools, click on the **Client Features tab**.



- **Allow the user to enable Local Recording:** To learn about local recording, see the Surveillance Client manual.
- **Allow the user to use screenshots:** Permission for the user to use the screenshot feature from Digifort.
- **Disable the Surveillance Client's settings button**: Prevents the user from accessing the Surveillance Client's settings. To learn about the Surveillance Client's settings, see the Surveillance Client manual.
- **Force full screen:** Forces the user to use Digifort in full screen.
- **Hide system operation controls:** This option will cause the Surveillance Client to run in "full screen" mode, in other words, the camera-viewing matrix will be expanded and the user will not have access to any operation control, being restricted to the camera-viewing screen.
- **Disable context menus:** This option will disable the use of accessible menus through the right mouse button, further blocking the operator access to the system.
- **Disable Print-Screen:** Disables the print-screen key.
- **Do not allow the user to close the Surveillance Client**: Prevents the user from closing the Surveillance Client.
- **Do not allow the user to minimize the Surveillance Client:** Prevents the user from minimizing the Surveillance Client, maintaining it locked to the system.
- **Lock Workstation**: Locks the user's workstation, not allowing the use of shortcuts, such as CTRL + ALT + DEL, ALT + TAB, and any other command that can close the Surveillance Client.
- **Automatically change client language per user**: The clients (Administration, Surveillance and Web) language can be dynamically changed for each user logged into the system, overwriting the computer's language option. Click on the option Charge default system language and then select the desired language for the user in the box.

8.2.4 Groups Inquiry

Allows viewing of the groups in which the user is registered.

© 2002 - 2020 by Digifort, all rights reserved



8.2.5 Rights Inquiry

This screen allows viewing of the rights given to the user, such as, for example, the right to view and playback cameras and maps.



This screen offers the following functions:

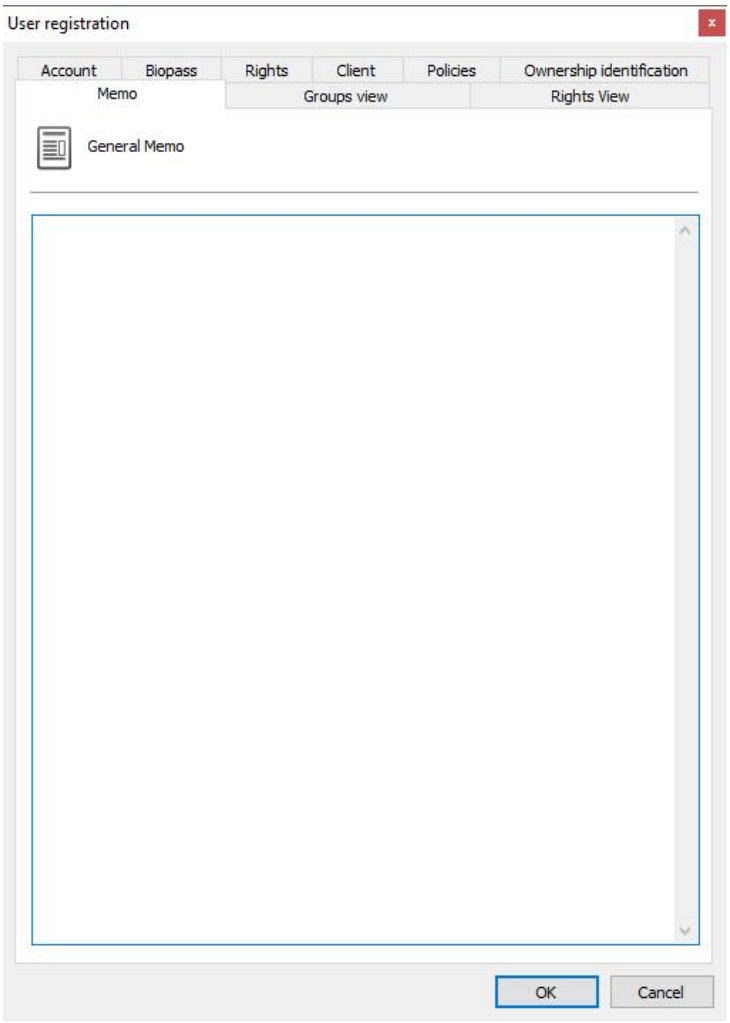
- **Type of right**: List of the types of rights given to the user.
- **Objects:** List of the objects related to the given right

8.2.6 User general observations field

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

The field can also be displayed in the users list through extended columns and exported together with the users list export..

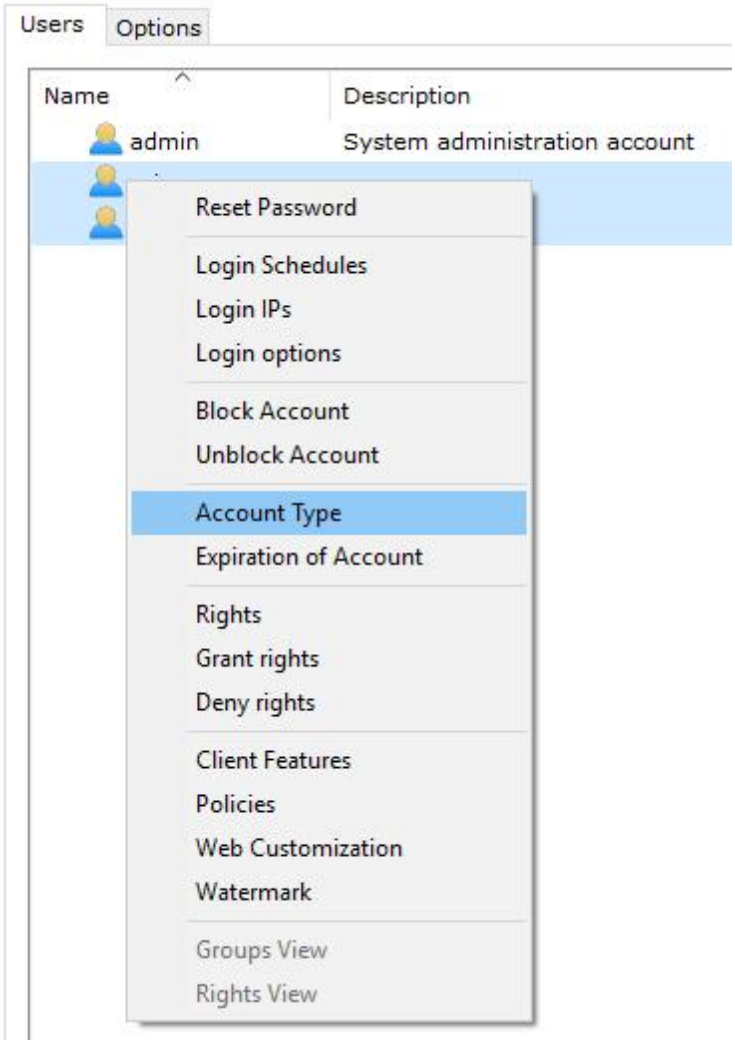
© 2002 - 2020 by Digifort, all rights reserved



8.3 User administration functions

The Digifort's User Administrator offers rapid access to the most common user configurations. In the user register, select the desired user and click on the right button. A menu will be opened, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



8.3.1 Reset password

Resets the password of the selected user, leaving it blank. For security reasons, this option will be available selecting one user at a time.

8.3.2 Login schedule

Opens the user login scheduling settings. This setting allows you to define from what time the user can authenticate in the system. To learn how to use this feature see login times

8.3.3 Login options

Opens account lockout settings after a certain number of failed attempts.

© 2002 - 2020 by Digifort, all rights reserved

8.3.4 Block account

Blocks the account of selected users, making them unable to authenticate in the system. com que eles não consigam autenticação no sistema.

8.3.5 Unblock account

Unblocks the account of selected users, making them able to use the system again.

8.3.6 Account expiration

Defines an expiration date for the accounts of the selected users. After the expiration date, the user can no longer authenticate himself in the system..

8.3.7 Rights

Opens the user rights screen. To learn about user rights, see Login hours

8.3.8 Give rights

Opens the user rights screen giving the selected rights. If no right is selected, but some user has it, the rights defined here will be added. somados.

8.3.9 Deny rights

Opens the user rights screen denying the selected rights.

8.3.10 Features

Opens the features screen of the Surveillance Client. To learn about this feature, see Surveillance Client Features.

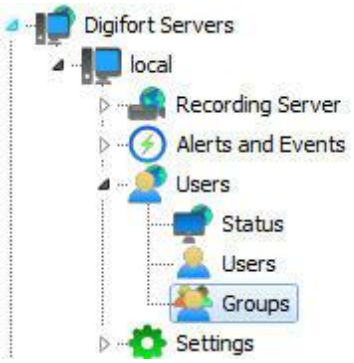
8.3.11 Policies

Opens the Policies screen. To learn about this feature, see Policies.

8.4 Adding, altering and excluding Groups

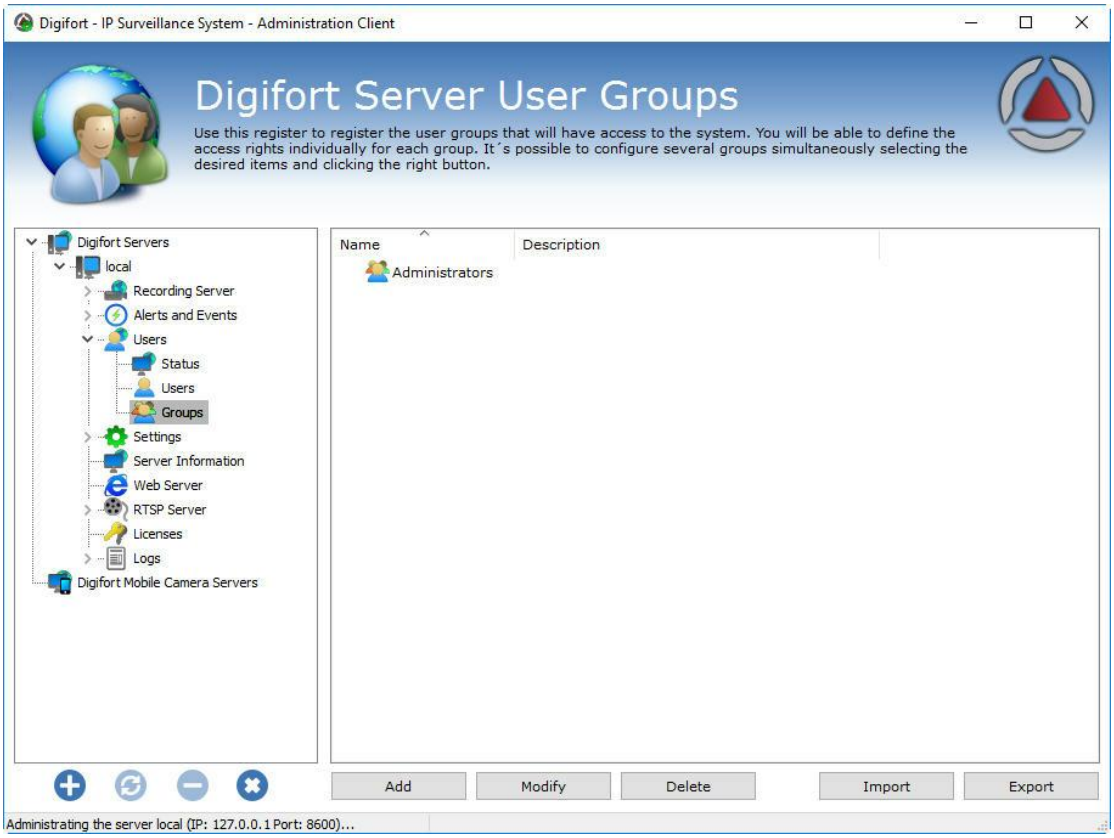
To access the group management feature, locate Groups in User in the server's Configurations menu as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



The ‘Groups’ option was created to facilitate user management within the system.

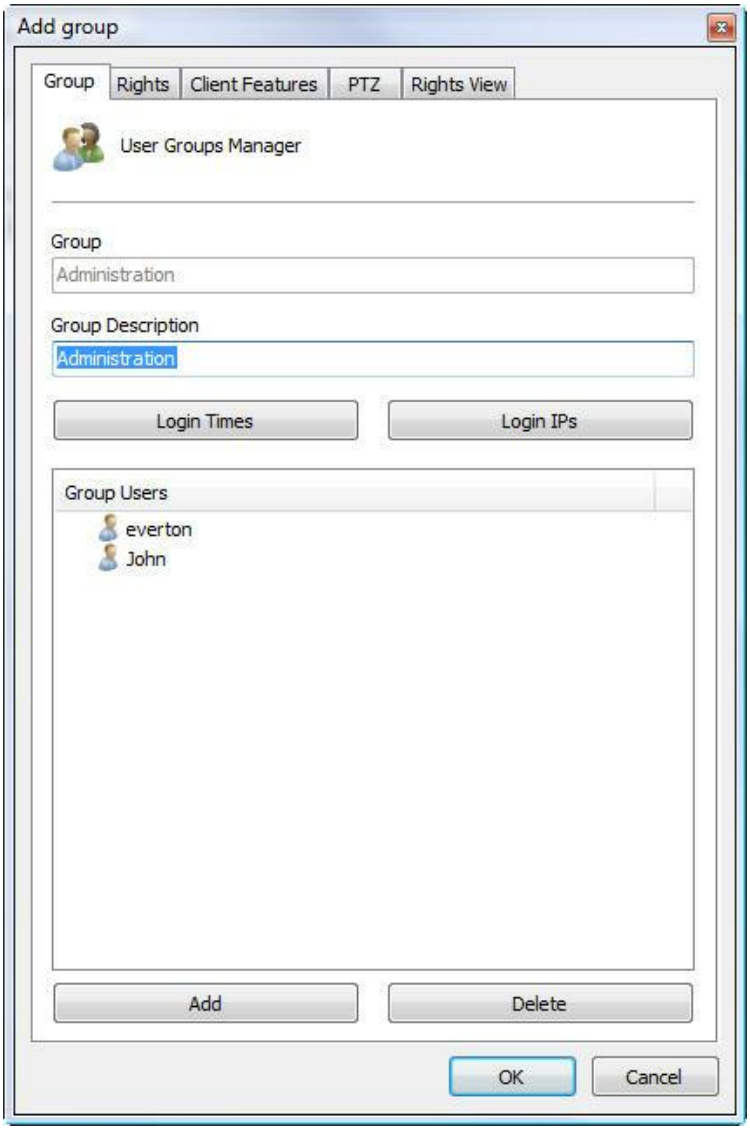
Once this is done, the Groups management screen will open on the right as illustrated in the picture below:



By clicking on the Add button, the group edition screen will open up. Let’s start by introducing a group, moving on to the entitlements and then the features.

To change an already registered user, select it and click on Change and then change the data as explained throughout the manual.
To remove a user, select the user you wish to remove and click on the Remove button.

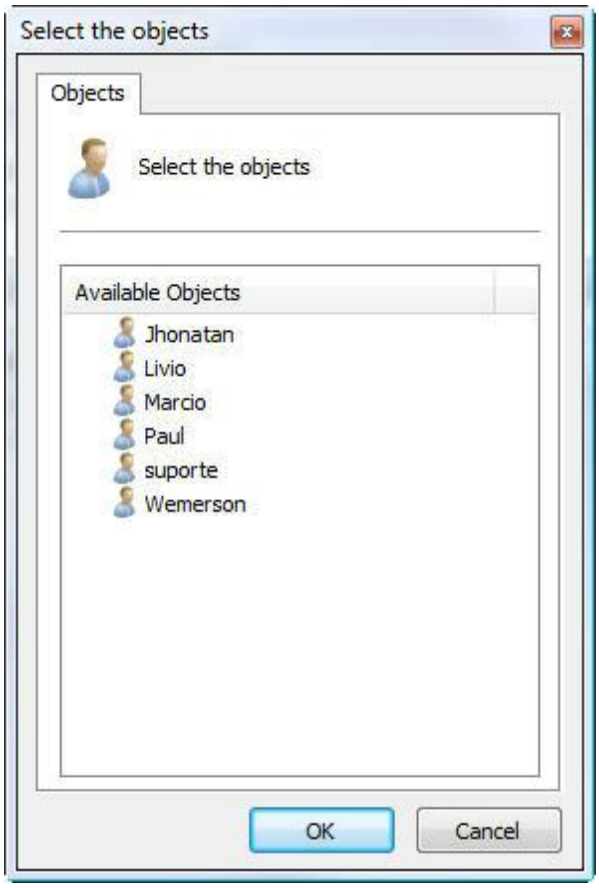
© 2002 - 2020 by Digifort, all rights reserved



When adding a group, the first step is to indicate its main data, i.e.:

- Group: Username, which must be indicated when logging in to any module of the Digifort System. Once saved it cannot be altered.
- Group description: A brief description of the user to help identify him in the system.
- Login times**:** To learn about this feature refer to Login Times
- Login IPs: To learn about this feature refer to Login IPs
- Group Users: List of users in the group. To add a user to the group, simply click on **Add** and a window will open so that you may select the user to be added as shown in the picture. To remove a user, simply select it from the list and click on the **Remove** button.

© 2002 - 2020 by Digifort, all rights reserved



8.4.1 Group rights

After filling in the main user data, the access rights must be configured. As default, the rights are configured for a surveillance user profile, that is, the user will only be able to carry out the system operations of live surveillance and video playback.

As configurações de direitos para o grupo é igual a configuração de direitos de usuário.

8.4.2 Surveillance Client Features

The configuration of the features of the Surveillance Client is very important for the security of a site. This feature offers tools that affect the person who monitors the cameras, causing other factors to impair the attention of the operator.

The configuration of the Resources of the Surveillance Client for the group is the same as the configuration of the Resources of the Surveillance Client of the user. To learn how to configure the Resources of the Surveillance Client of the group see Surveillance Client Features.

© 2002 - 2020 by Digifort, all rights reserved

8.4.3 Rights Inquiry

This screen allows the viewing of the rights given to the group, such as, for examplo, the right of viewing and playback of cameras and maps.

The configuration of the Rights Inquiry for the group is the same as the configuration of the Rights Inquiry of the user. To learn how to configure the Rights Inquiry of the group see Rights Inquiry

© 2002 - 2020 by Digifort, all rights reserved

Chapter IX

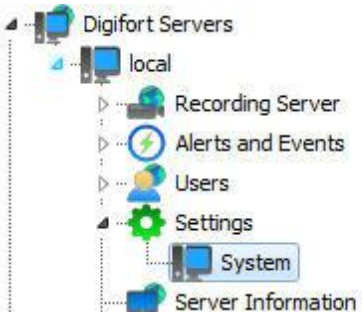
9 Configurations

9.1 Global Configurations

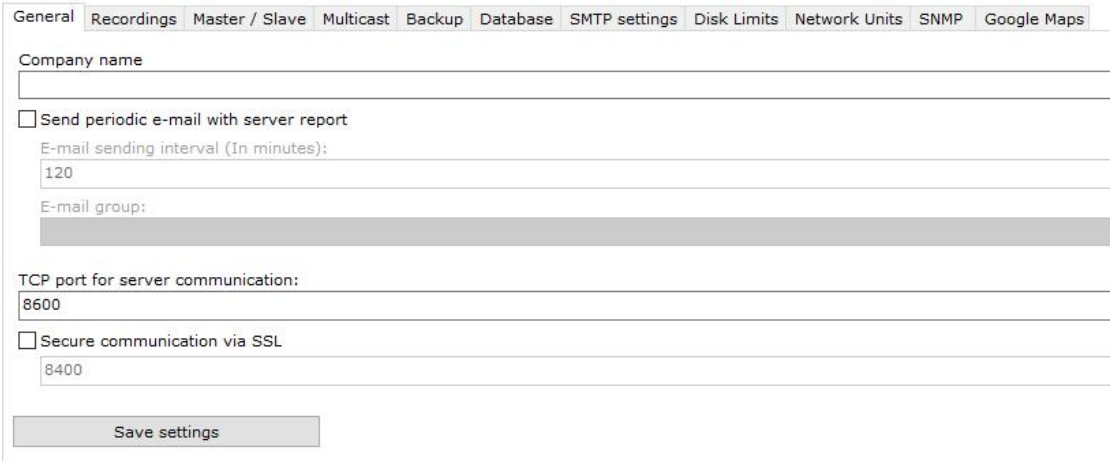
Esta área do sistema é reservada para o ajuste das configurações globais do servidor.
As configurações globais são parâmetros que depois de configurados afetarão todo o funcionamento do sistema.

9.1.1 General Configurations

To access this area, click on the Configurations item in the Configurations Menu, as illustrated in the figure below:



Once this is done, the general system configurations screen opens on the right, as illustrated in the figure below:



- **Company name**: The company name is used when you export a video in order to facilitate the surveillance client operation.
    - **Send periodic e-mail with server report:** Sends e-mail with a server report periodically to the specified alert group in the specified time interval. This report contains information such as user accesses to the system and recording status.

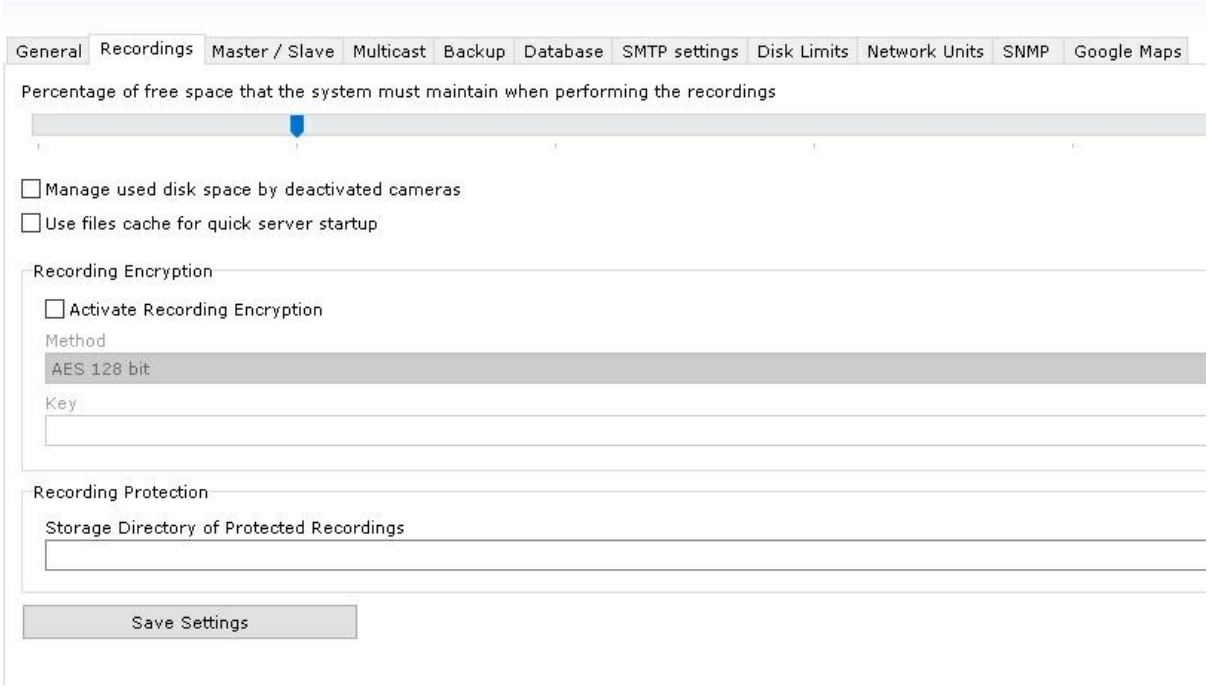
© 2002 - 2020 by Digifort, all rights reserved

- **TCP communication port with the server:** Communication port by which the Surveillance Client and the Administration Client will communicate with the server. After modifying this configuration, it's necessary to modify the communication port of the server register of the Administration Client and the Surveillance Client. To learn how to carry out this configuration in the Surveillance Client, see How to configure the servers to be administrated. To learn how to modify the port in the Surveillance Client, consult its manual..
- **Secure communication via SSL:** Communication port where the Monitoring Client and the Administration Client will communicate with the server via SSL.

After adjusting the configurations, click on the Save Configurations button so that no modification is lost.

9.1.2 Recordings

On this tab, you can configure some advanced options related to image recording.



- **Percentage of free space that the system must maintain when performing recordings**: Enter here the percentage of disk space you want to reserve for other applications external to Digifort. For example, in case an 80GB hard drive is used, with a free disk space percentage of 2%, 16GB would not be used by Digifort for recordings, being directed to other software, such as the operating system. This limit is also applied to "Disk Limits". To learn how to create a disk limit, see 'Disk Limits'.

- **Use file cache for quick server startup**: In systems where the number of days of recording is very high, the act of restarting the Digifort service can take a long time: 30, 40 60 min. This option makes Digifort able to start up much faster keeping a map of the recordings used previously before the system stopped. It is not recommended to use this option if you have problems with power failures on your server, as this can corrupt the recordings on the system.

© 2002 - 2020 by Digifort, all rights reserved

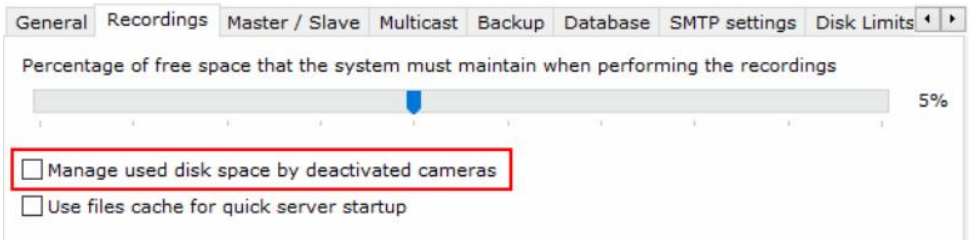
After adjusting the settings, click on the **Save Settings** button so that no change is lost.

Após o ajuste nas configurações clique sobre o botão **Salvar Configurações** para que nenhuma alteração ser perdida.

Important

The percentage of free disk space reserves a disk space for applications external to Digifort. By default, it is set to 2%. If there is a lot of disk space available for recordings, this percentage may be too high.

NOTE: The recording system has the option of managing the disk space used by deactivated cameras. Previously, if the camera was deactivated, its recordings were not deleted during recording recycling. With this option activated, all deactivated cameras will also enter recording recycling and their recordings will be deleted according to the set time. This option is important for Failover servers (where cameras are usually always deactivated) and compliance with protection laws for GDPR and LGPD data, which define themaximum retention period for images.

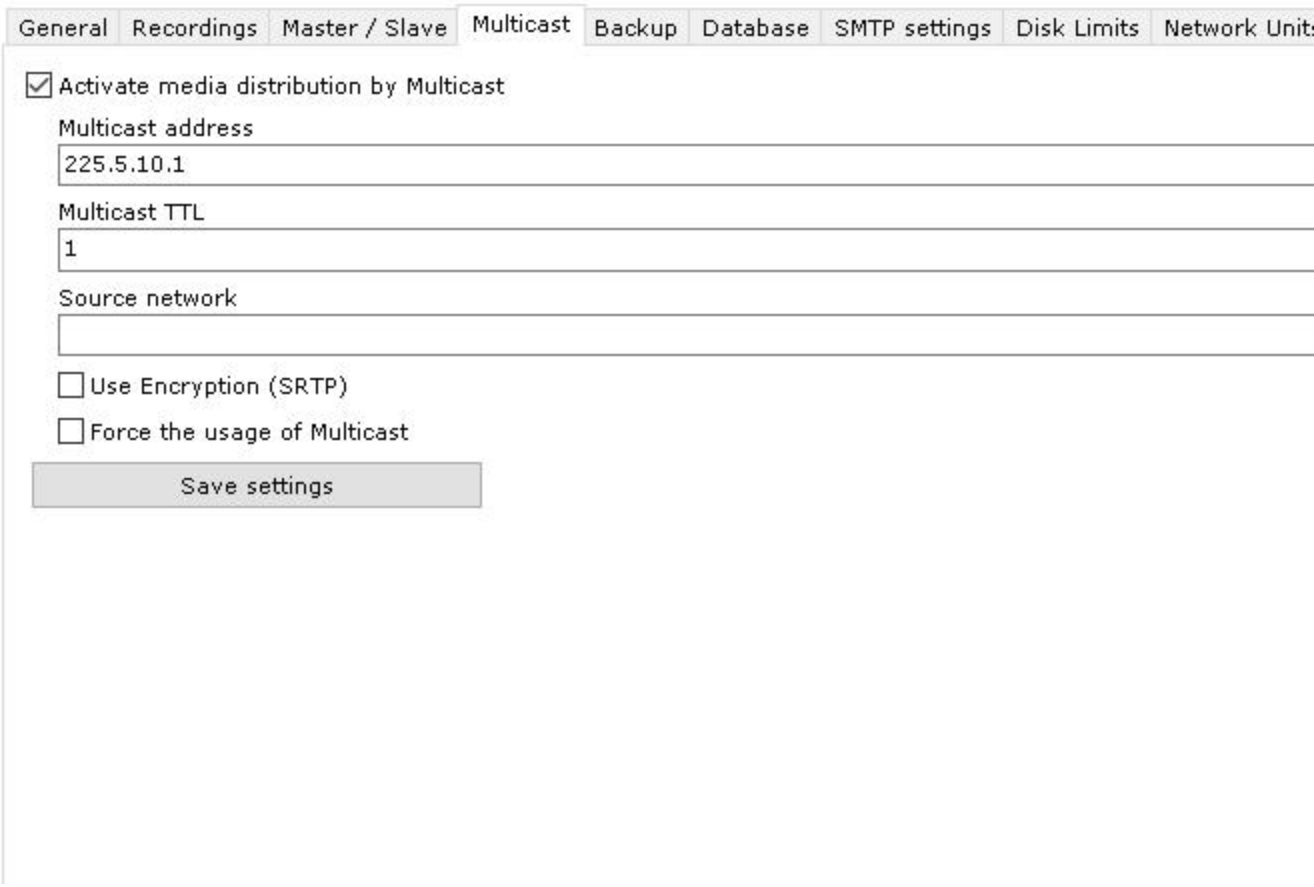


9.1.3 Multicast

Essa opção permite que o servidor Digifort envie os vídeos aos Clientes de Monitoramento via comunicação Multicast.
Multicast é a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções.
No caso do Digifort, é apenas recomendado o uso de Multicast na seguinte situação: Vários clientes de monitoramento que monitoram as mesmas câmeras na tela. Caso contrário pode haver um alto indice de tráfego de informação causando problemas na rede.lado

Segue abaixo a tela de configuração das opções multicast:

© 2002 - 2020 by Digifort, all rights reserved



Essa tela possuí as seguintes configurações:

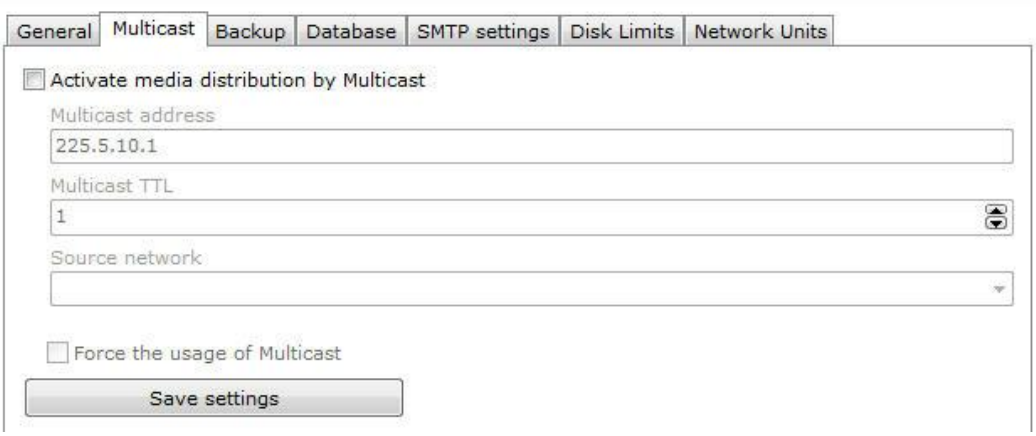
- **Ativar a distribuição de vídeo via Multicast (Activate media distribution by Multicast):** Habilita o envio de fluxo de vídeo via multicast..
- **Endereço do Multicast (Multicast address):** Considerando a arquitetura IPv4 de nomenclatura IP e as melhores práticas, é conhecido que o range de IP reservado para a prática do multicast é: 224.0.0.0 até 239.255.255.255. Por esse motivo, como padrão o Digifort adotou o IP 255.5.10.1 que pode ser modificado a qualquer momento.
- **Multicast TTL:** Permite mudar o TTL do pacote multicast. Configuração necessárias para algumas marcas de switchs.
- **Rede de origem:** Selecione a rede de origem para a transmissão do multicast.
- **Forçar o uso do Multicast (Force the usage of multicast):** Quanto a opção Multicast é habilitada, não necessáriamente o cliente de Monitoramento Digifort irá utilizá-la, pois existe uma opção por parte do cliente de monitoramento que permite a escolha do Multicast ou Unicast (Veja o manual do cliente de monitoramento). Quando a opção **Forçar o uso do Multicast** é ativada, o Servidor Digifort ignora as configurações do cliente de Monitoramento e dessa maneira eles usarão o envio de imagens via Multicast.
- **Usar Criptografia SRTP:** Quando o Cliente de Monitoramento conectar no servidor utilizando SSL/TLS, a transmissão de mídia por multicast para o client (Caso esteja configurado para transmissão de vídeo em multicast) também será criptografada utilizando o protocolo SRTP.
- **Salvar configurações (Save Configurations):** Salva as configurações desejadas.

----------OLD_TEXT----------

© 2002 - 2020 by Digifort, all rights reserved

This option allows the Digifort server to send the videos to the Monitoring Clients via Multicast communication.
Multicast delivers information to several end receivers at the same time using the most efficient strategy where messages only go through a link once and are only duplicated when the link to the end receiver is split in two directions.
In the case of Digifort, the Multicast is only recommended in the following situation: Several monitoring clients monitoring the same cameras on screen. Otherwise there may be increased movement of information causing problems to the network.

The configuration screen of the multicast options is shown below:



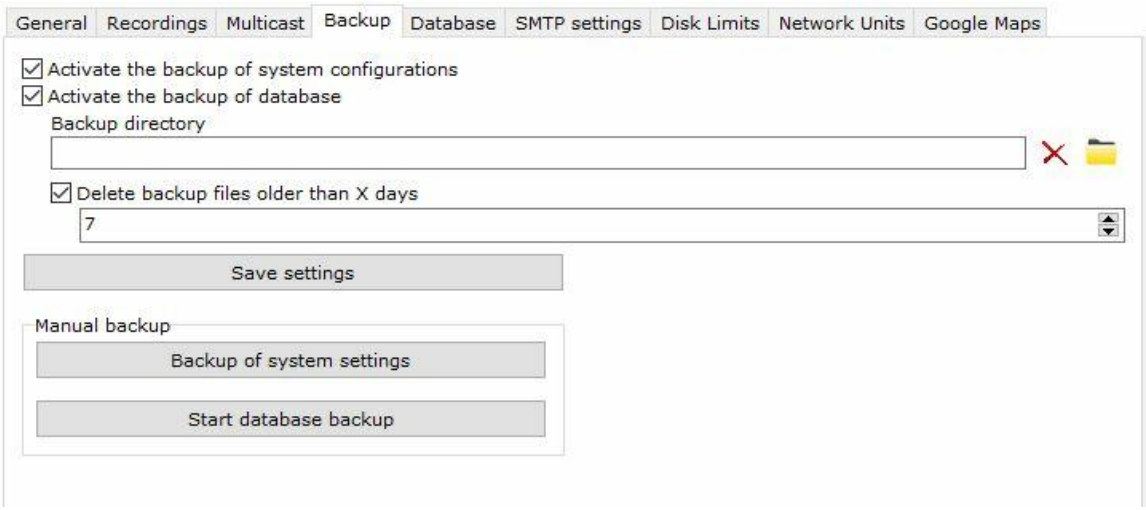
This screen has the following settings:

- **Activate media distribution via Multicast**: Enables the sending of video stream via Multicast.
- **Multicast address**: Considering the IPv4 architecture of IP nomenclature, as well as best practices, it is known that the reserved IP range for multicast is: 224.0.0.0 to 239.255.255.255. For this reason, Digifort adopted IP 255.5.10.1 as default, which can be modified at any time.
- **Multicast TTL**: It allows you to change the TTL of the multicast packet. Required settings for some brands of switches.
- **Source network**: It selects the source network for multicast transmission.
- **Force the usage of Multicast**: When the Multicast option is enabled, the Surveillance Client will not necessarily use it, as there is an option on the Surveillance Client to allow the choice of Multicast or Unicast (see the Surveillance Client manual). When the Force the usage of Multicast option is activated, the Digifort server ignores the Surveillance Client's settings and images will be sent via Multicast.
- **Use SRTP Encryption**: When the Surveillance Client connects to the server using SSL/TLS, media transmission to the client via multicast (in case it is configured for video transmission in multicast) will also be encrypted using the SRTP protocol.
- **Save Settings**: It saves the desired settings.

9.1.4 Backup

Backup options in this tab are related to Digifort database.

© 2002 - 2020 by Digifort, all rights reserved



This screen has the following features:

- **Activate the backup of system configurations:** Select to enable the automatic backup of log files containing the settings of system registers Digifort.
- **Active the backup of database**: Click to activate the automatic backup of the database that contains the analytical events Digifort events of LPR, General events, logs, etc.
- **Backup directory**: Choose the directory where the backup files will be stored.
- **Delete backup files older than X days**: Configure the number of days on which the backup files are kept in the chosen directory.
- **Save configurations**: Saves the settings you choose.

Manual backup

- **Start database backup**: Clicking this option the Digifort backs of the log files in the directory selected in the option Digifort above.
- **Start database backup:** Clicking this option the Digifort will backup database files in the directory selected in the option above.

9.1.4.1 Restoring backups of Digifort

To restore system settings, settings made in the registers and, just run the file Digifort of record you want with the service "Digifort Server stopped.

To restore the database, replace in the installation folder on the server DIGIFORTDB "file.FDB "by the desired file with the same name and with the services "**Digifort Database Server** " and " **Digifort Server**"stopped.

To learn about services see chapter How to run Digifort Services Manager

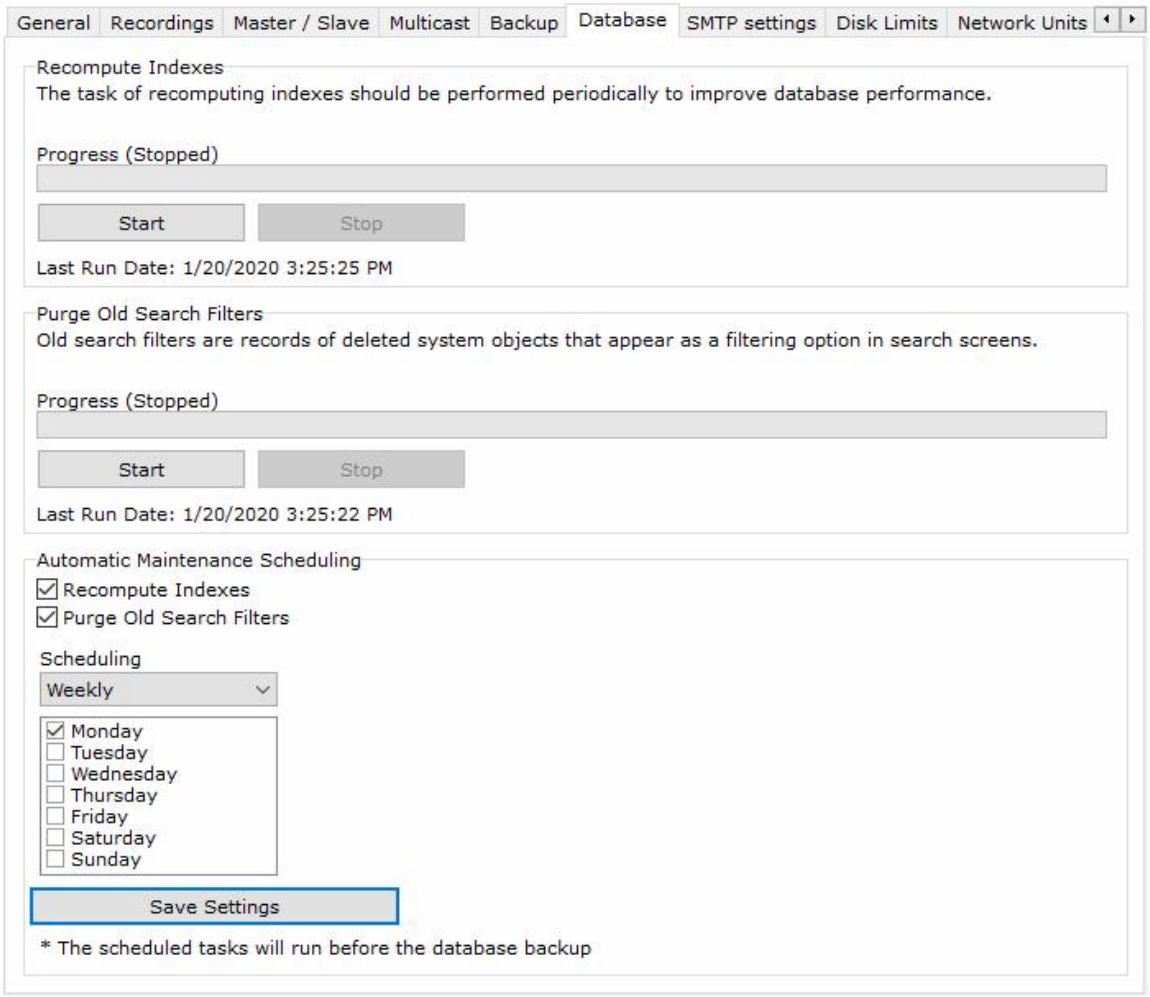
© 2002 - 2020 by Digifort, all rights reserved

9.1.5 Database

The Digifort has a database to store different types of records as: analytical event logs, event logs, system logs and LPR.

The configuration screen of the database allows the user to start a maintenance in order to enhance the performance of access to data by Digifort. Click **Start** to start the database maintenance process.

It is also possible to set up a database maintenance schedule, so that the task is automated.

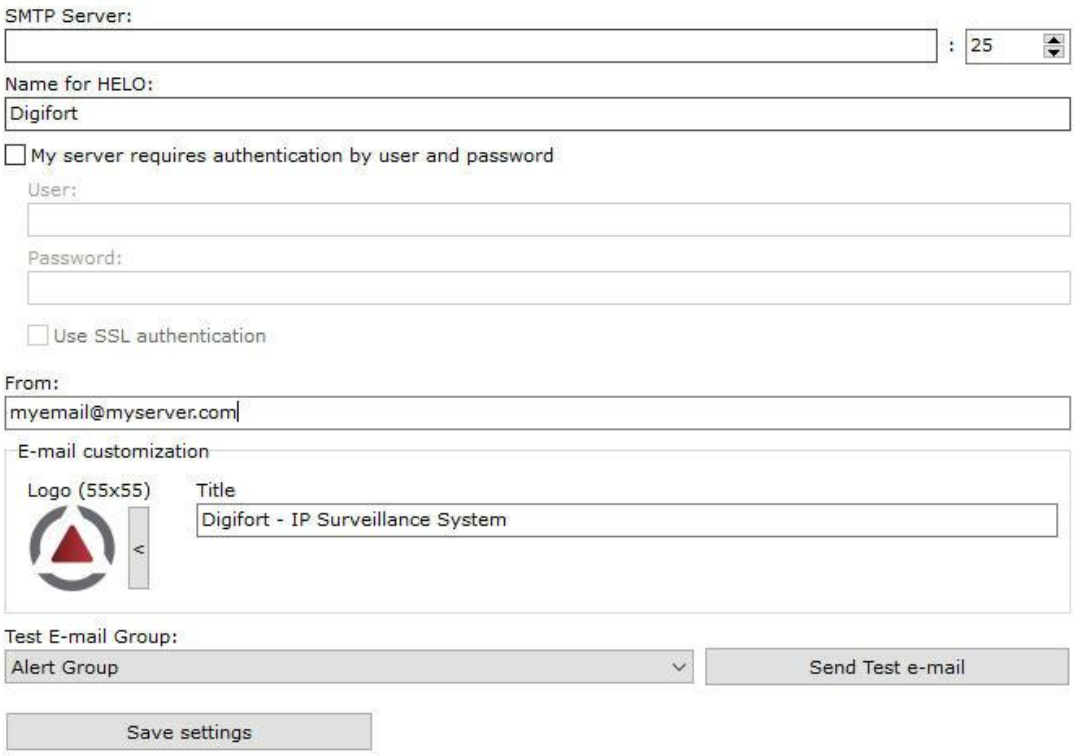


© 2002 - 2020 by Digifort, all rights reserved

9.1.6 STMP Configurations

The STMP configurations are used by Digifort t send notification e-mail to users. The actions for sending e-mail could be failures in communication with the cameras, for example, and must be previously configured by the administrator.

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



- **STMP Server SMTP**: Address of the SMTP server to be used for the sending of e-mail. This parameter can be an IP, if there is an STMP server in your company, for example, or a DNS if third-party STMP servers are used.
- **My server needs authentication by user and password:** If your SMTP server needs a user and password for authentication for sending of e-mail, mark this option. When this option is marked, the User and Password fields will be activated and must be filled in.
  - **User:** User for authentication in the sending of e-mail messages.
  - **Password**: Password for authentication in the sending of e-mail messages.
  - **Use SSL authentication :** With SSL, authentication is performed by an exchange of certificates. These certificates are used to authenticate on some servers to increase the level of security.
- **From:** Sender's e-mail address. In this field, enter the e-mail address of the system administrator, for example.
- **E-mail customization:** Allows customization of the logo and name of the company when sending e-mails of events. Simply choose the desired logo image and change the title next to it.
- **Group for test e-mail**: Select an alert group for the sending of a test e-mail message for the

© 2002 - 2020 by Digifort, all rights reserved

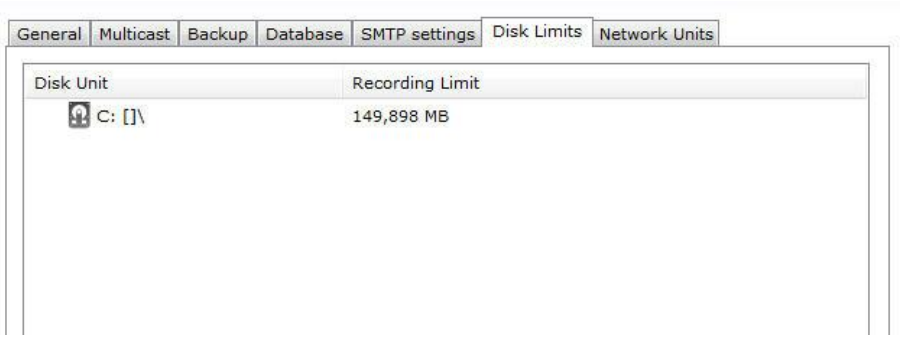
specified configurations. This alert group must have been previously configured. To learn how to do this configuration see How to configure the contact groups

- **Save Configurations button:** Saves the configurations. If not pressed, no configurations will be saved after leaving this screen.

9.1.7 Disk Limits

In this area of the system you can define disk limits in all of your units, if you wish to maintain a cushion of free disk space.

To access this feature, click on the Disk Limits tab in the Configurations item of the Configurations Menu, as shown in the picture below:



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

© 2002 - 2020 by Digifort, all rights reserved



Select the desired disk unit and enter the number of megabytes of limit that you wish to impose.
At the end of the configuration, click on the **OK** button.

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

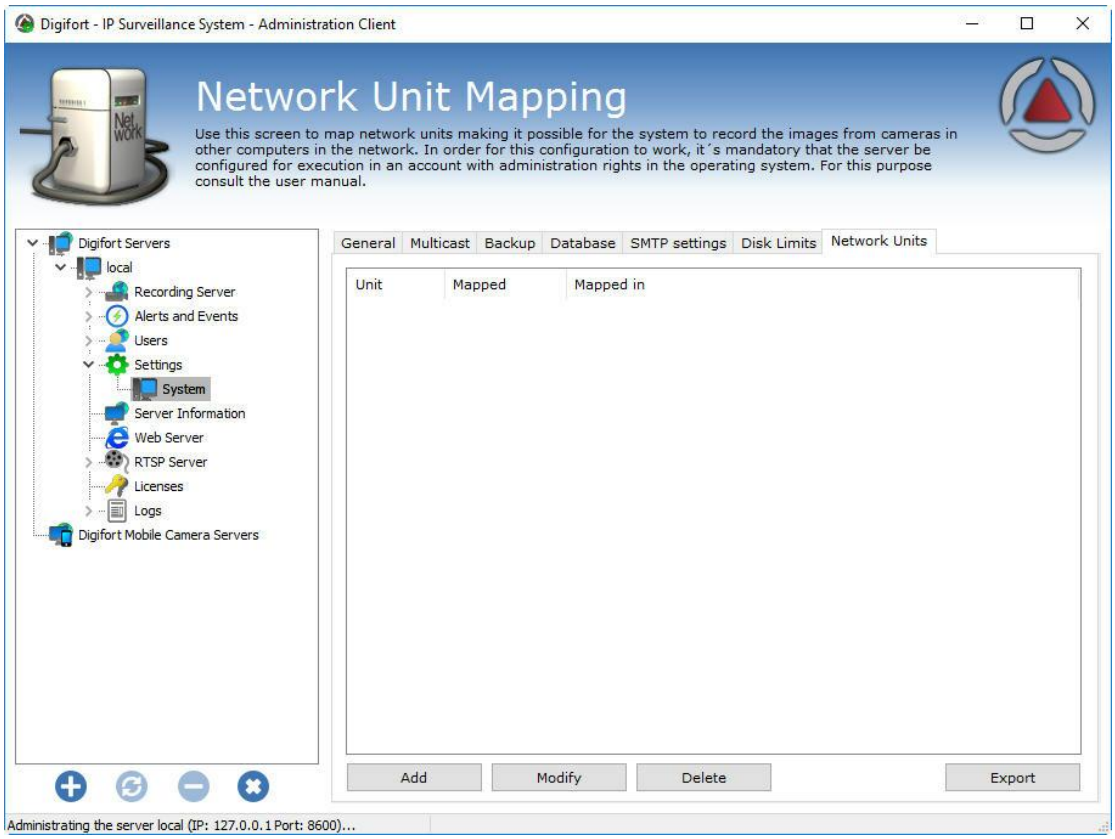
9.1.8 Network Units

Digifort Explorer makes it possible to carry out recording of cameras not only in local disks. It's also possible to define network units in which Digifort can record the images from cameras.

Digifort's mapping of network units is different from that of Windows, and must, therefore, be defined by Digifort itself.

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

© 2002 - 2020 by Digifort, all rights reserved

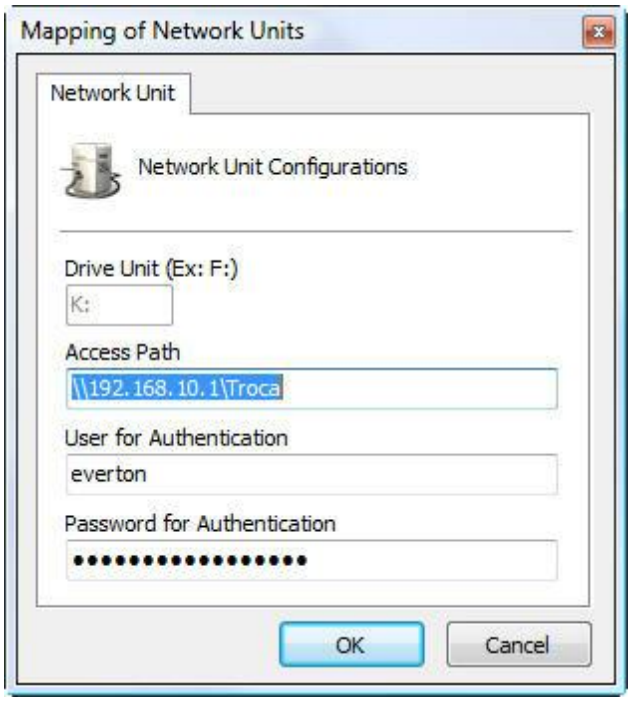


To add a new network unit, click on **Add**. To modify or exclude a network unit, select it and click on the corresponding button.

9.1.8.1 How to add a network unit

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

© 2002 - 2020 by Digifort, all rights reserved



- **Unit letter**: Specify the identification letter of the unit to be mapped.
- **Access path**: Specify the complete folder path of the unit to be mapped.
- **User for authentication**: User of the Windows network who has access to the folder.
- **Password for authentication**: Password of the Windows network who has access to the folder.

© 2002 - 2020 by Digifort, all rights reserved

9.2 Server health monitoring event

The system allows the configuration of server health monitoring events. With these events, you can monitor the usage of CPU and System Memory, and trigger events in case of abnormality.

CPU monitoring will monitor the server's global CPU (and not only the system's server process).
You can configure a usage limit and a time limit, whereby, if the global CPU usage remains above the set limit by the specified time, the event will then be generated. A condition restoration event (below the limit) can usually be triggered when CPU usage returns below the limit.

RAM monitoring will only monitor memory usage by the system's server process (server.exe).
You can configure a memory usage limit by the server, whereby, if the usage remains above the configured limit, the event will then be generated. A normal condition restoration event (below the limit) can be triggered when CPU usage returns below the limit.



© 2002 - 2020 by Digifort, all rights reserved

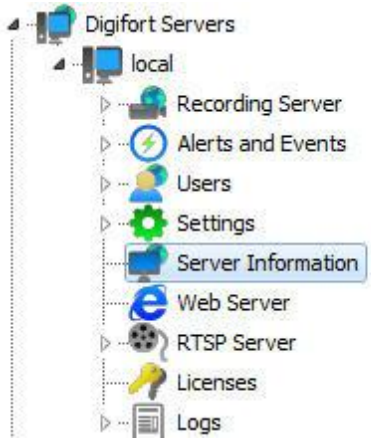
Chapter



10 Server Information

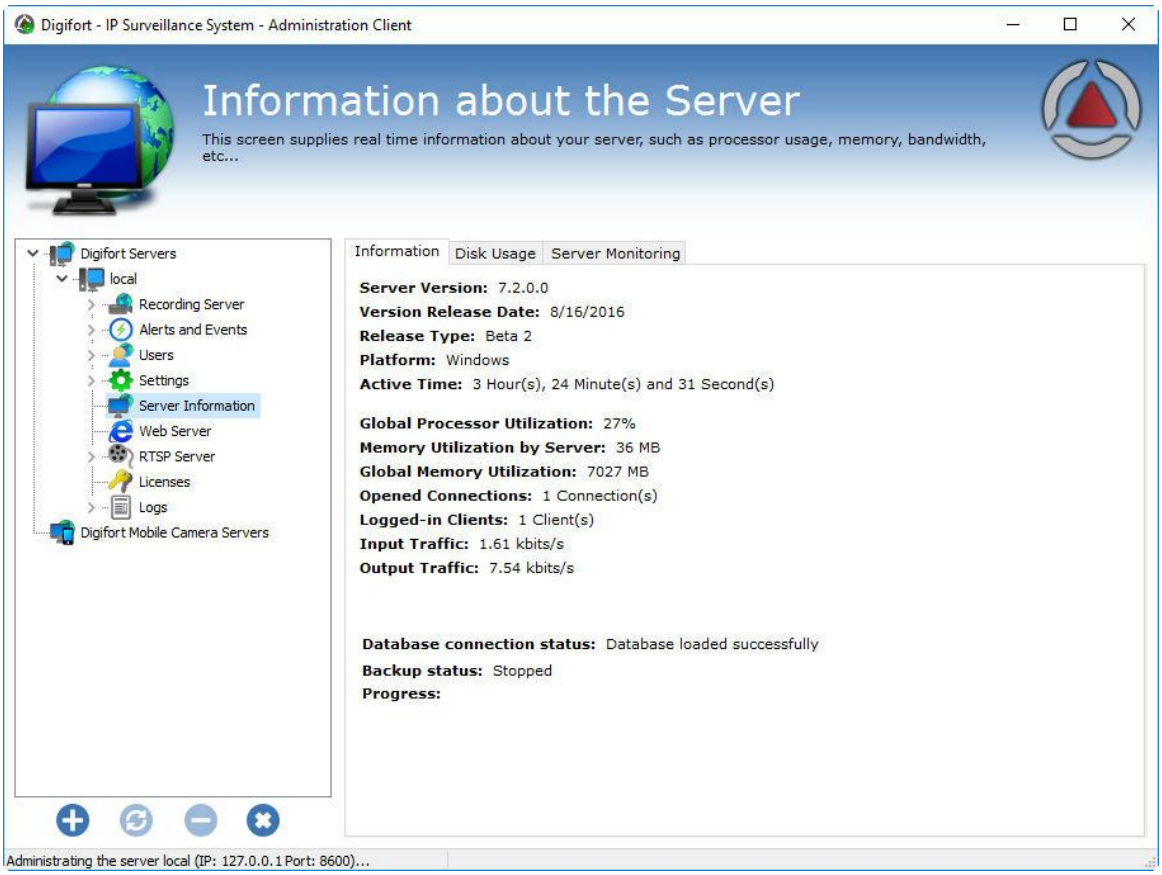
In this area of the system you will be able to accompany the performance of the server, receiving data such as processor and memory utilization, network traffic, etc.

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



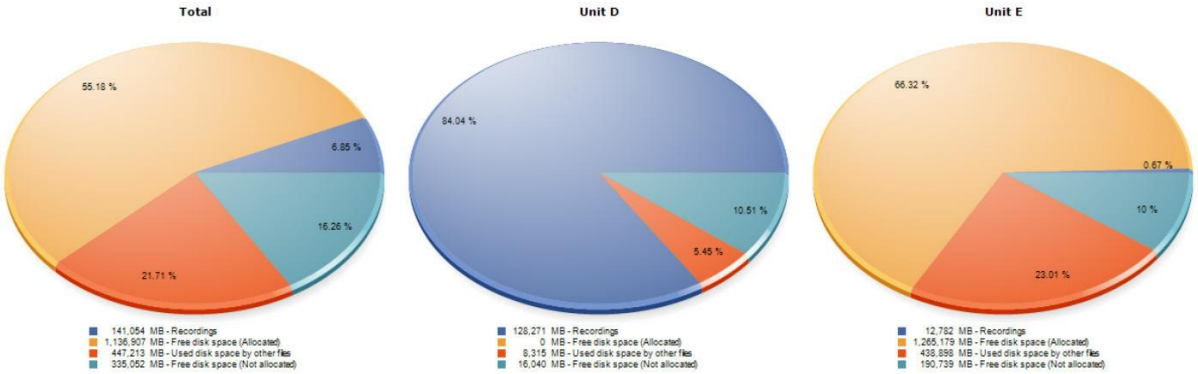
Once this is done, a window will be opened on the right side with server information, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



10.1 Disk Usage

The server disk usage tab generates a chart for each drive managed by the server and a general chart (Total):



The dark blue color on the chart represents the percentage of recordings occupied on a disk.

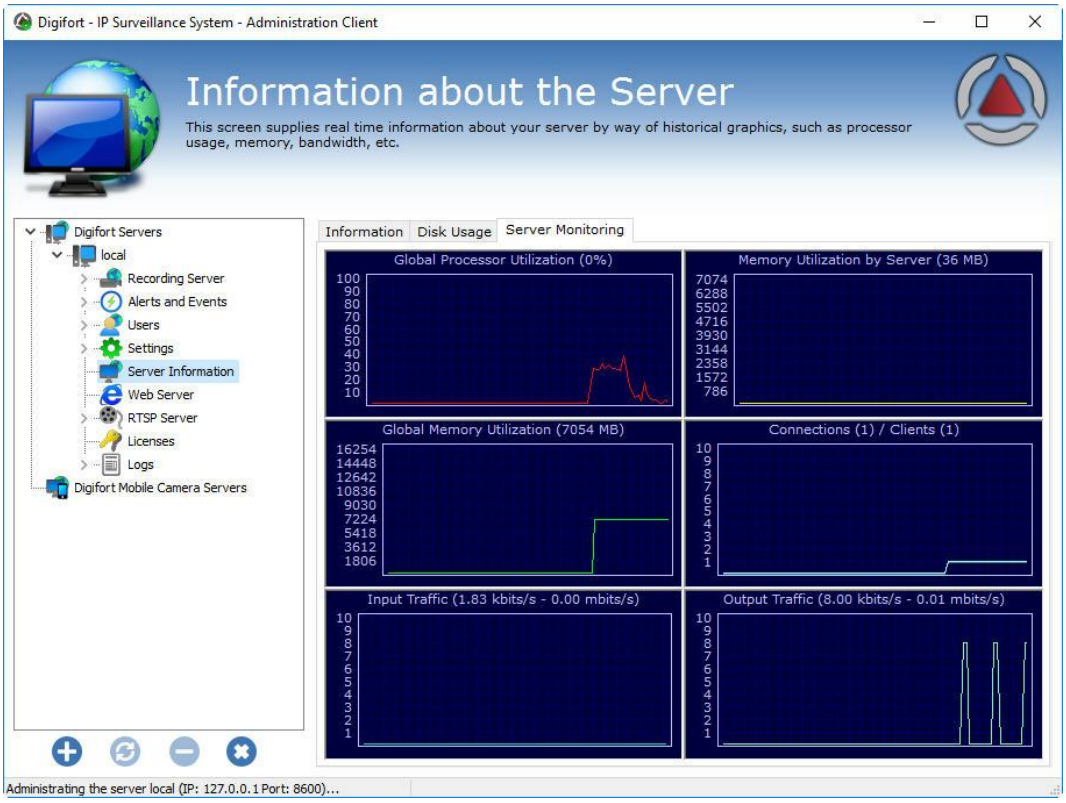
© 2002 - 2020 by Digifort, all rights reserved

The yellow color represents the percentage of free disk space.
The orange color represents the percentage of space used by other files non-related to image recording.
The light blue color represents the percentage of unallocated disk space for recordings by Digifort. This space can be changed; see chapter: General Settings.

In the example above, the first chart is the sum of the other two drives used by Digifort (drive D and drive E);

10.2 Monitoring by graphics

Digifort offers an interesting feature that makes it possible to monitor the resources used by the server in real time by way of graphics updated every second. To access this configuration, click on the **Monitoring** tab, as shown in the picture below:



© 2002 - 2020 by Digifort, all rights reserved

Chapter XI

11 Web Server

Digifort is equipped with a Web server, by means of which, users can visualize cameras and play videos back locally or via Internet with the use of an Internet navigator.

It's important to point out that, for access to the Digifort Server via Internet, it's necessary to configure your router with the purpose of redirecting the server connection by way of an Internet IP and a port.

To carry out the connection via Internet, Digifort requires two communication ports, the port 8600 and another configurable port.

11.1 How to access the configurations of the Web Server

To access the configurations of the Web Server, click on the item **Web Server**, and click on **Configurations**, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configurations of the Web Server will be displayed at right, as shown in the picture below:



- **Activate the Web server**: Activates the Web server Web allowing users to connect to the server by way on an Internet navigator.
- **Server port:** The port used for access to the server. This port can be modified and must be configured in your router for external access. Digifort uses a different one internally, because the port 8600
- **Enable HTTPS (SSL):** Enable HTTPS support on the web server.
- **Server Port**: Configure the access port via HTTPS.

© 2002 - 2020 by Digifort, all rights reserved

Chapter XII

12 Servidor RTSP

The RTSP server can be used to provide media to any player that supports RTSP, and can also be used to send media to broadcast servers like Wowza and make third party systems integrations with Digifort.

To illustrate, let's take the case of a client who wants to provide the image of a Digifort camera on his web site. In that case, he could use the API website and request a stream or a snapshot in MJPEG. However, if this site had a large volume of access, MJPEG could become unfeasible because of its size. The RTSP server generates flow of the following formats:

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

Then to add the image to a site just add a player that can receive a stream in RTSP with the following command line:

Syntax: rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<name of the camera registered on digifort>

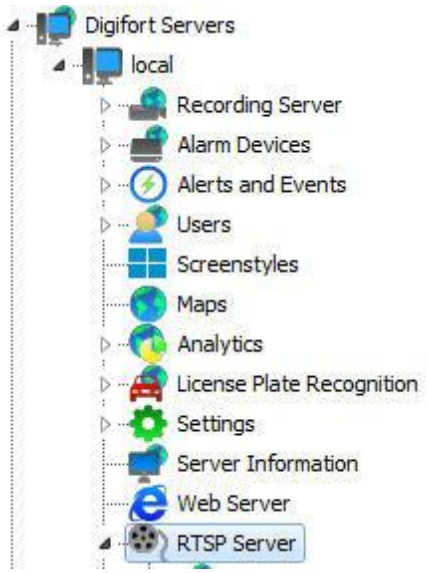
The command will bring up the recording profile image. You can choose the profile by adding the following command:

Syntax: rtsp://<server_address>:<rtsp port>/Interface/Cameras/Media?Camera=<name of the camera registered on digifort>&Profile=<profile name>

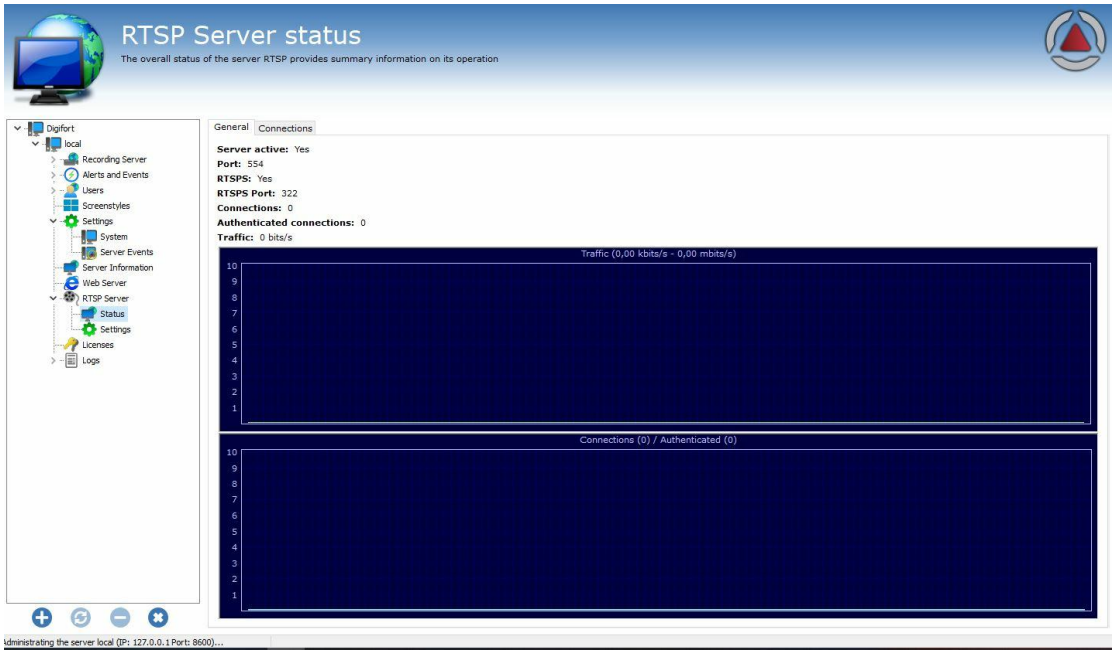
12.1 Status

To access the settings for the RTSP Server, expand the Web Server item, and click on Settings, located in the Settings Menu, as shown in the figure below:

© 2002 - 2020 by Digifort, all rights reserved



That done, these Status settings will be displayed on the right, as illustrated in the figure below:

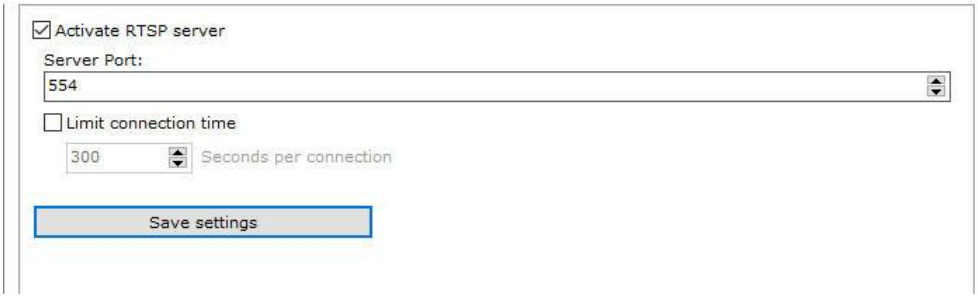


This screen provides the following information:

- **Active server:** Indicates if the RTSP server is active.
- **Port**: Indicates the port on which the server is running.
- **Connections**: Indicates the number of connections to the RTSP server.
- **Authenticated connections**: Indicates the number of authenticated connections to the RTSP server.
- **Traffic**: Displays the bandwidth used in real time.

© 2002 - 2020 by Digifort, all rights reserved

12.2 Configurations



The settings screen of the RTSP server allows the following settings:

- **Enable the Web server**: Enables Web server allowing users to connect to the server via a web browser.
- **Server port**: Port used to access the server. This port can be changed and must be configured on your router for external access. Digifort internally uses another because the 8600 serves the communication of the server with the clients.
- **RTSP port**: Port used to access the server via RTSPS, if activated.
- **Limit connection time**: Option to configure a time limit in which each connection can remain open.

© 2002 - 2020 by Digifort, all rights reserved

Chapter XIII

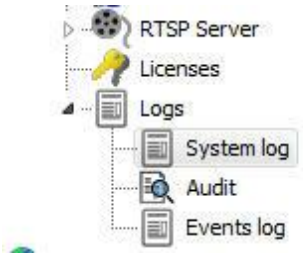
13 System Logs

The logs are very important tools for an environment that involves a security system such as Digifort, as it is in these logs that all events are registered, as well as user actions that occur in the system.

This chapter of the manual will cover the system logs, that is, those in which server events are registered, as opposed to the logs of alerts and events, where events related to external devices are registered. To better understand what alert and event logs are, see How to access the Alerts and Events

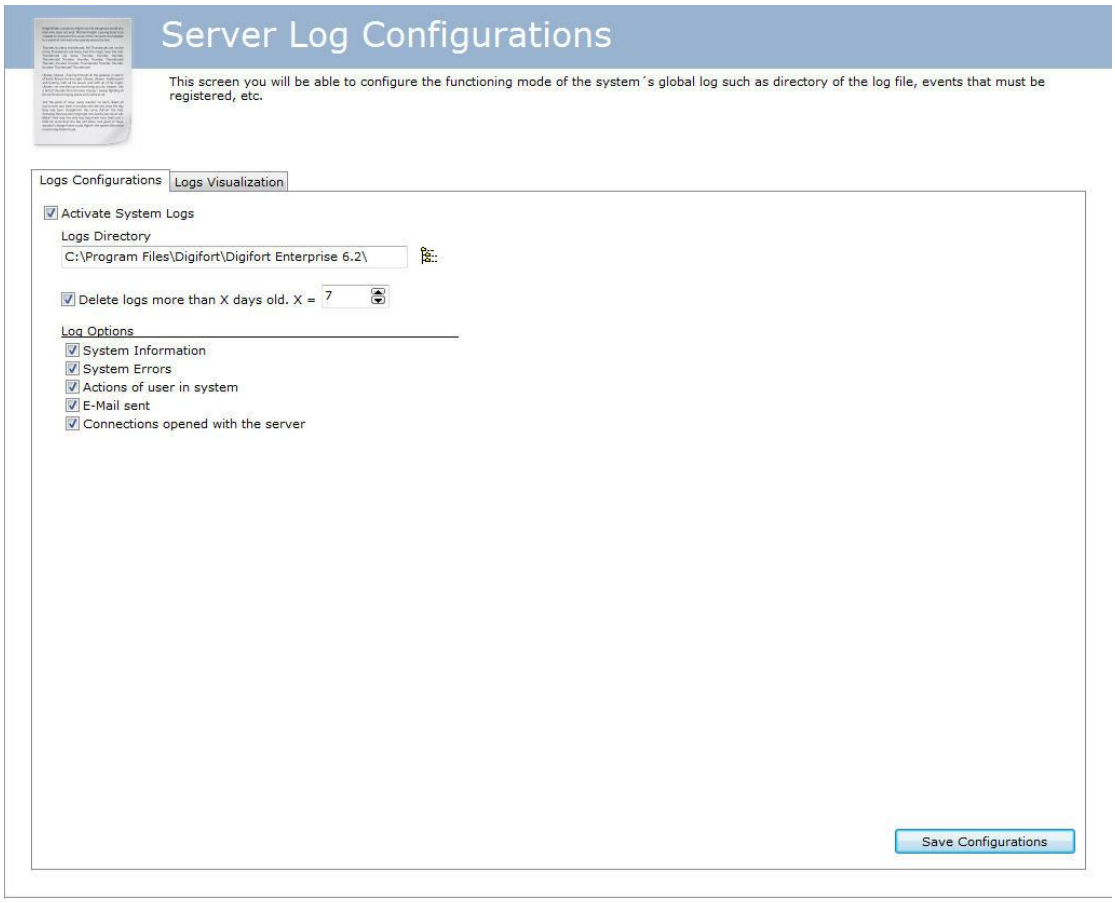
13.1 How to access the system logs

To access the system logs, click on the Logs item, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configuration of logs will be displayed on the right, as shown in the picture below:

© 2002 - 2020 by Digifort, all rights reserved



- **Activate system logs**: Activates the alert and event logs of Digifort.
- · **Log directory**: Select the directory in which the alert and event logs will be saved.
- · **Eliminate logs more than X days old**: Eliminates the old logs, specified by the informed number of days.

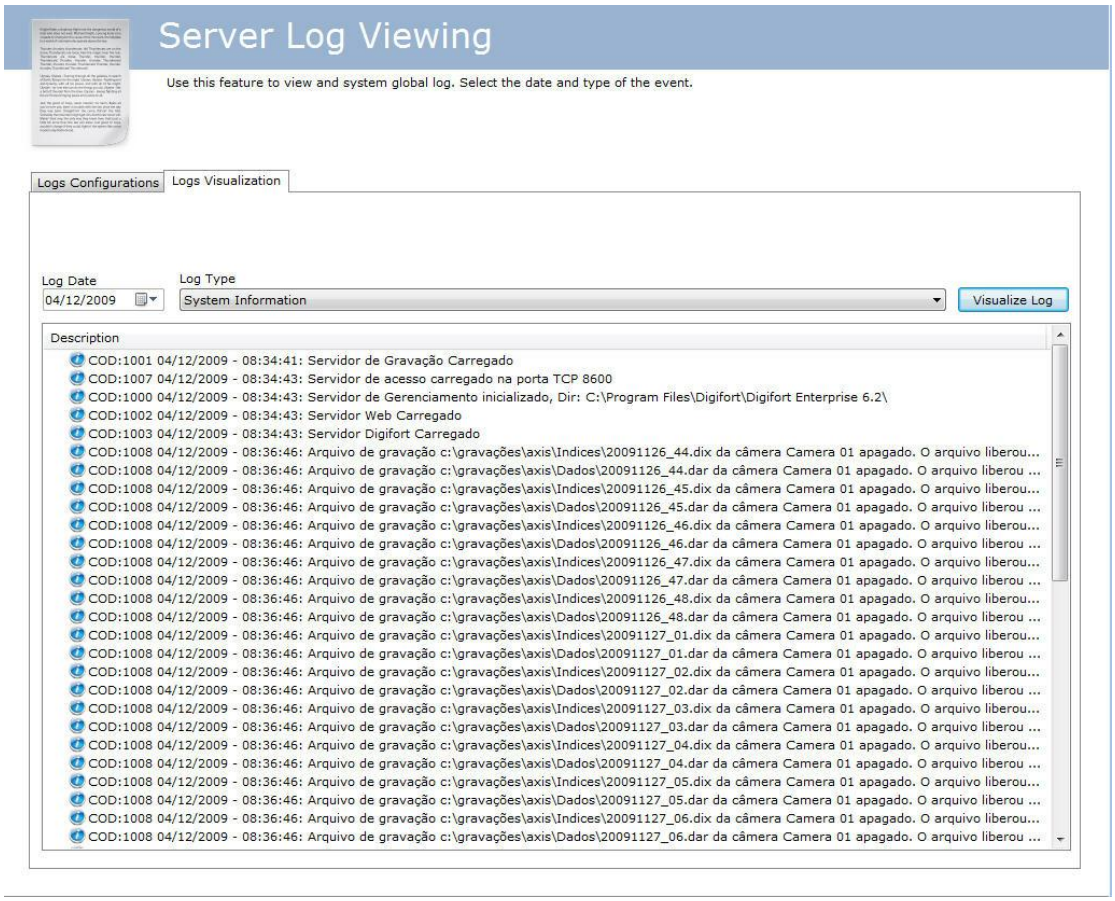
- **Options of the event log:**
  - **System informat**ion: This log contains information about system functioning like, for example, the time at which the server was loaded, terminated.
  - **System errors**: This log contains information about system errors such as the incorrect execution of some system function. This log rarely receives data.
  - **System user actions:** This log contains information about system user actions like, for example, the visualization of some camera and modification of configurations.
  - **E-mail sent:** This log contains information about the e-mail messages sent by Digifort like, for example, e-mail messages about failures in recording or communication of cameras.
  - **Open connections with the server:** This log contains information about the user connection with the server, showing information such as access time and IP.
- **Save Configurations button:** Saves the configurations of system logs.

© 2002 - 2020 by Digifort, all rights reserved

13.2 How to visualize the event logs

The visualization of logs is an auxiliary tool for the administrator when analyzing a log, presenting a friendlier and more productive interface compared to a simple text file.

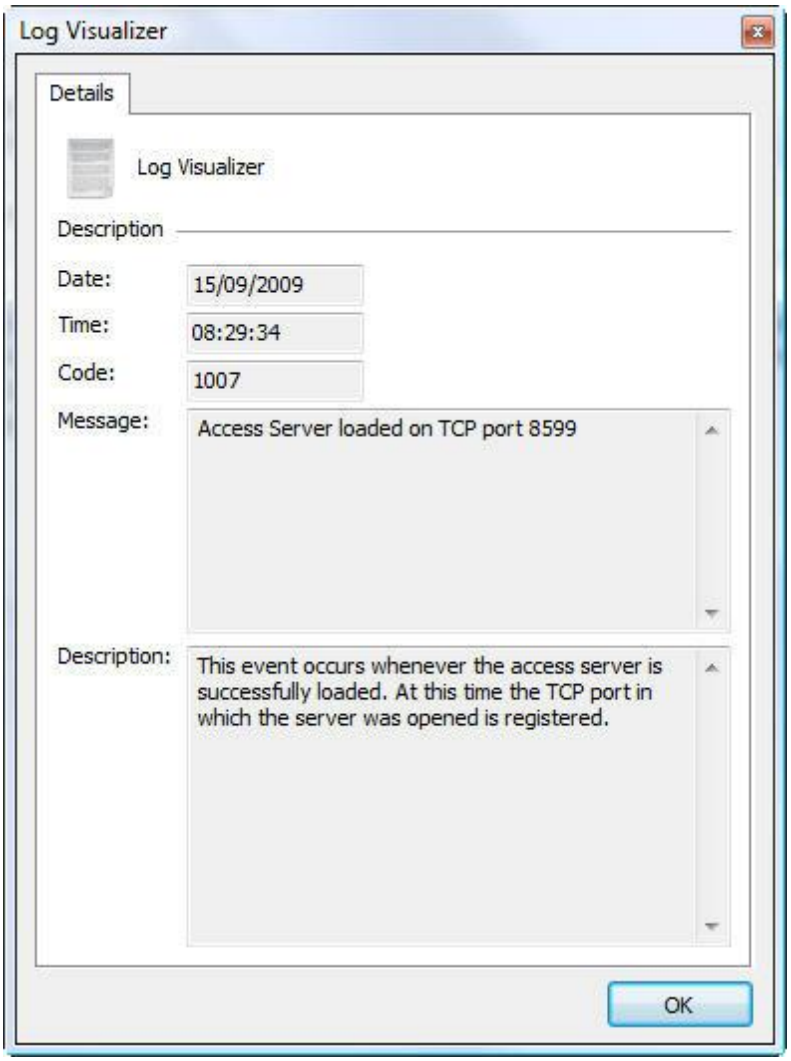
To visualize the event logs, click on the **Log visualization** tab, as shown in the picture below:



To visualize a log, select the date and type, then click on the Visualize Log button. This way the list of log registers will be filled.

Upon double-clicking on some log item, a screen will be displayed with details about the occurrence, as shown in the picture below:

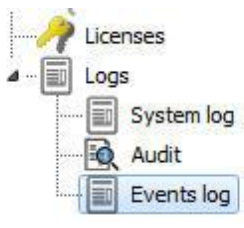
© 2002 - 2020 by Digifort, all rights reserved



13.3 How to configure the event logs

The Digifort's log configuration allows to register several event categories in its database. Those events can be listed and used to look for a pertinent recording in the monitoring client.

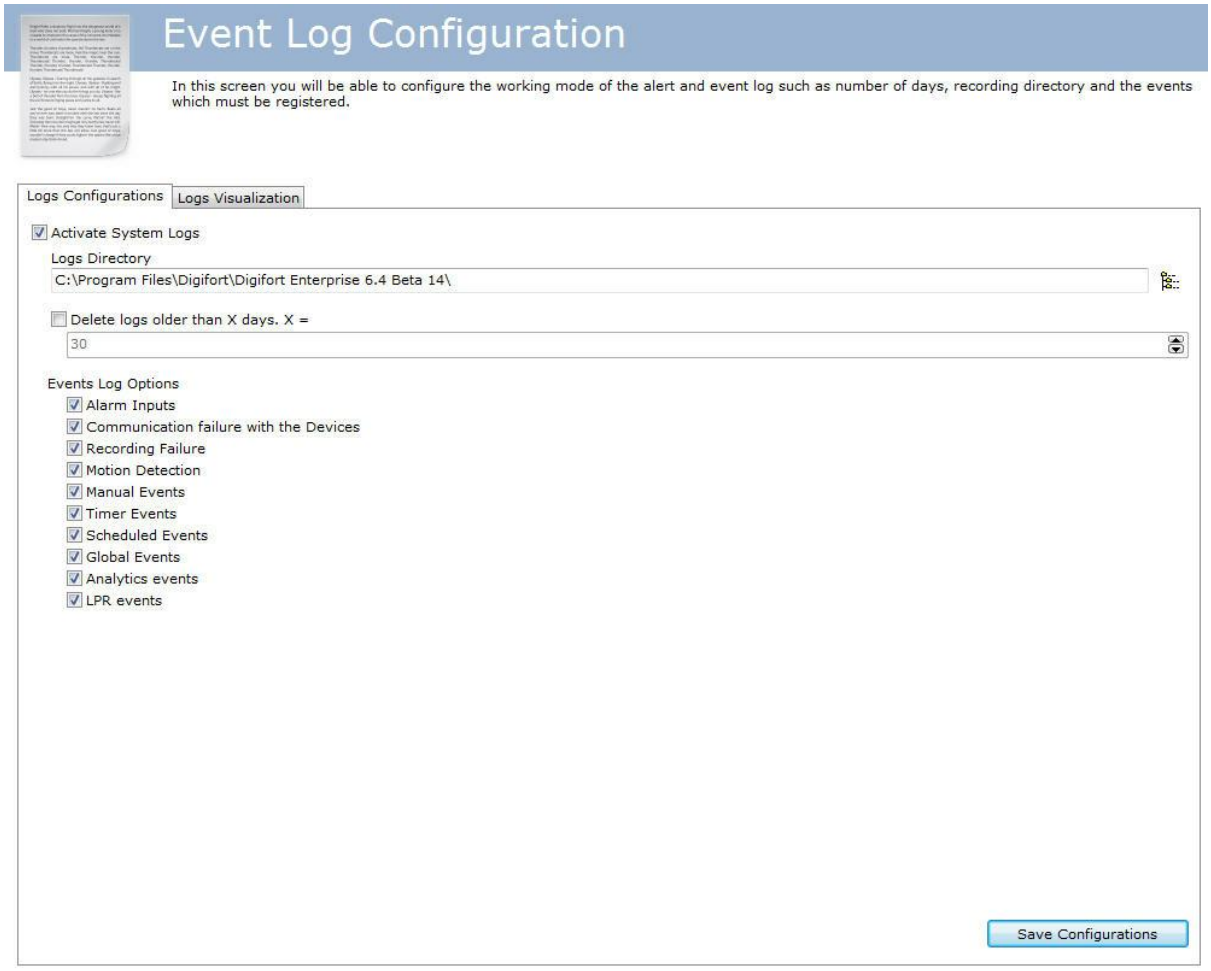
To access this feature, click on the item Logs, as shown in the picture below:



Once this is done, the screen for configuration of alert and event logs will be

© 2002 - 2020 by Digifort, all rights reserved

displayed at the right, as shown in the picture below:



13.3.1 Activate system logs

Activates Digifort's alert and event logs.

13.3.2 Delete logs older than X days

Delete the logs in the database that have been in the server for more than X days.

13.3.3 Event log options

© 2002 - 2020 by Digifort, all rights reserved

13.3.3.1 Failure in communication with the devices

Logs the failures of communication with the cameras

13.3.3.2 Failure in recording

Logs the failures in recording in disk of images coming from the cameras.

13.3.4 How to visualize the event logs

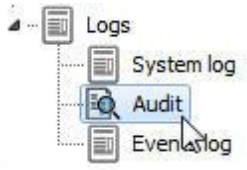
To learn how to view the event logs refer to the Surveillance client manual

13.4 Audit

The aim of the Digifort Audit is to record all the occurrences related to the users in the system and connections to the server.

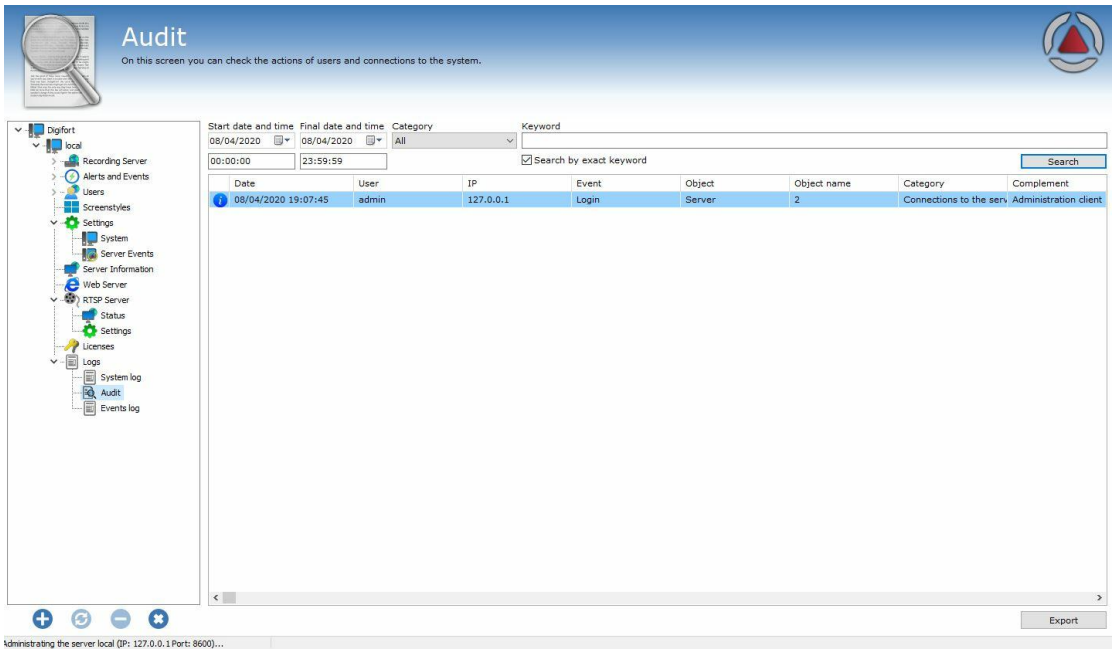
13.4.1 How to access Audit

To access the Audit screen, click on the item **Audit**, located in the Configurations menu as shown in the picture below:



Once this has been done, the **Audit** configurations will show up on the right as shown below:

© 2002 - 2020 by Digifort, all rights reserved



When open, the screen will show all the records on the current date.

13.4.2 Viewing the Logs

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

The following **user actions** are recorded by Digifort audit:

- **Locked and Unlocked**: Users or groups.
- **Reset**: User or group passwords.
- **Added**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Changed**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Deleted**: System settings, such as Equipment, IP filter, screen style, license, users, etc.
- **Created**: A recording directory.
- **Enabled and Disabled**: System settings (cameras, analytics, LPR, alarm boards, etc.)
- **Started**: Search by motion and video playback
- **Granted rights and Denied rights**: User viewing or recording
- **Viewed**: Cameras on the system.
- **Logged**: On the administration, surveillance or web client
- **Media Playback**: The start and the end date of user's media playback.

The following **Server Connections** are recorded by Digifort audit:

- **Connected**: Displays user connections to the server.
- **Disconnected**: Displays user disconnections from the server.

© 2002 - 2020 by Digifort, all rights reserved

Searching the audit system allows the records to be filtered by Date, Category and keywords. Searching with keyboard will only find records by the fields: user, IP, complement, and the object's name.
It is possible to select the **Search by Exact Word** option to speed up the search.

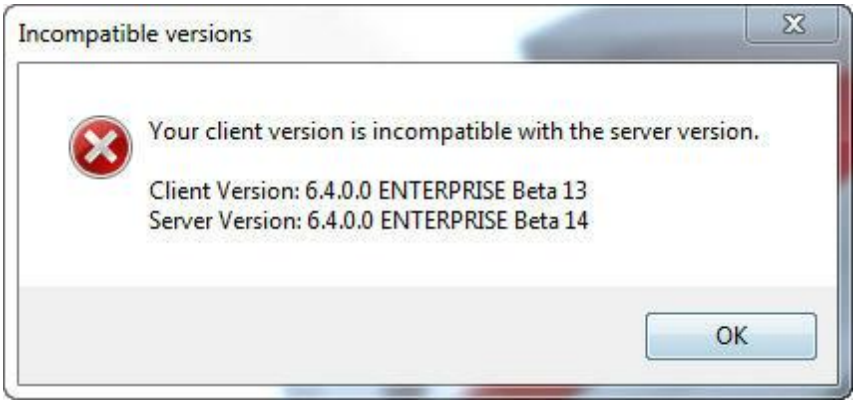
© 2002 - 2020 by Digifort, all rights reserved

Chapter XIV

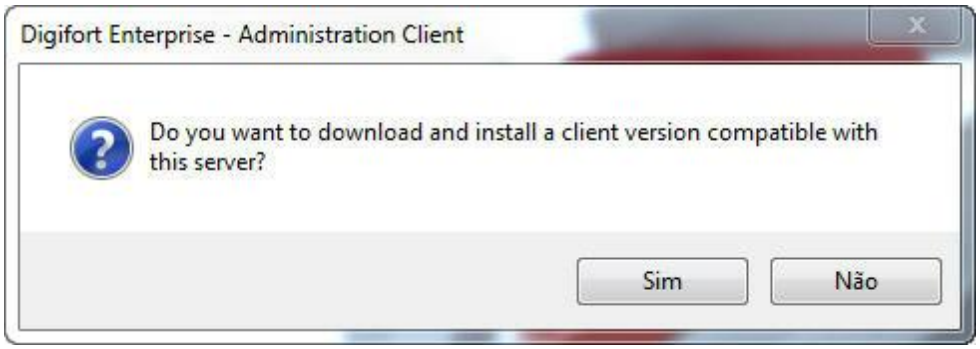
14 Automatic Client update

With swiftness and speed in mind, Digifort created a new feature that will be available in all the post-6.4 versions: the automatic update of the Surveillance and Administration Clients.
The feature will check if the server versions to which the client is trying to connect are the same.

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



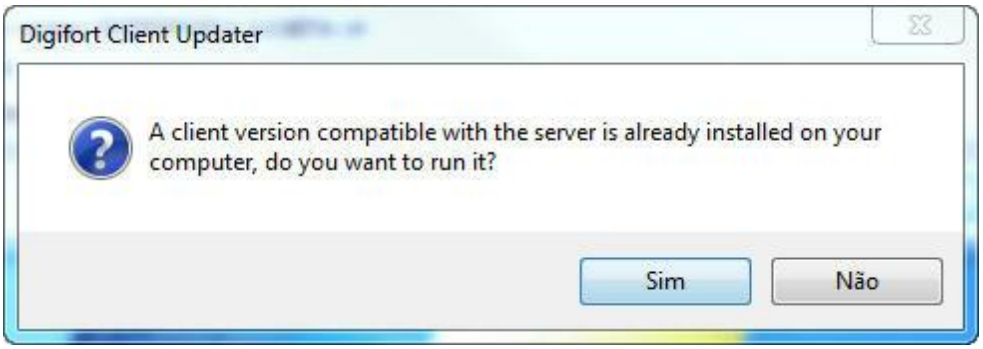
By clicking on **OK** a dialogue box will open with the following question: **Do you wish to download and install a client version compatible with this server?**



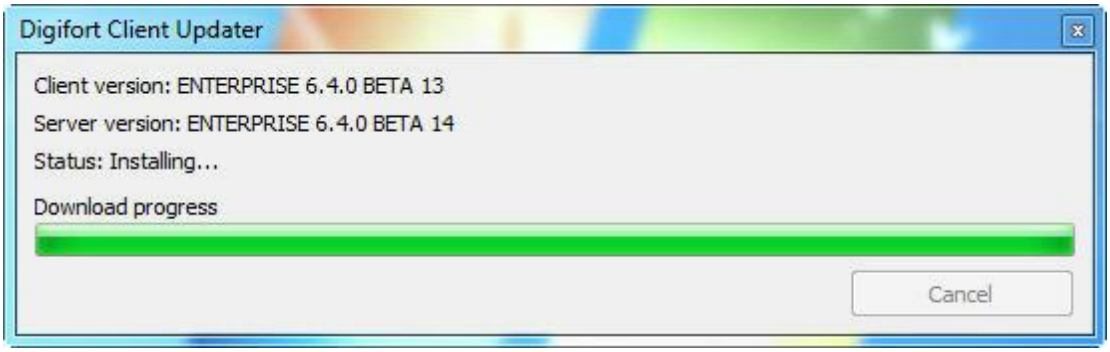
If you click on **No** the dialogue box closes and nothing happens. If you click on **Yes**, Digifort automatically installs the compatible client versions on the computer.

If the Digifort version on your computer is compatible, you will get the following message: **A compatible version is already installed on your computer; do you wish to execute it?**

© 2002 - 2020 by Digifort, all rights reserved

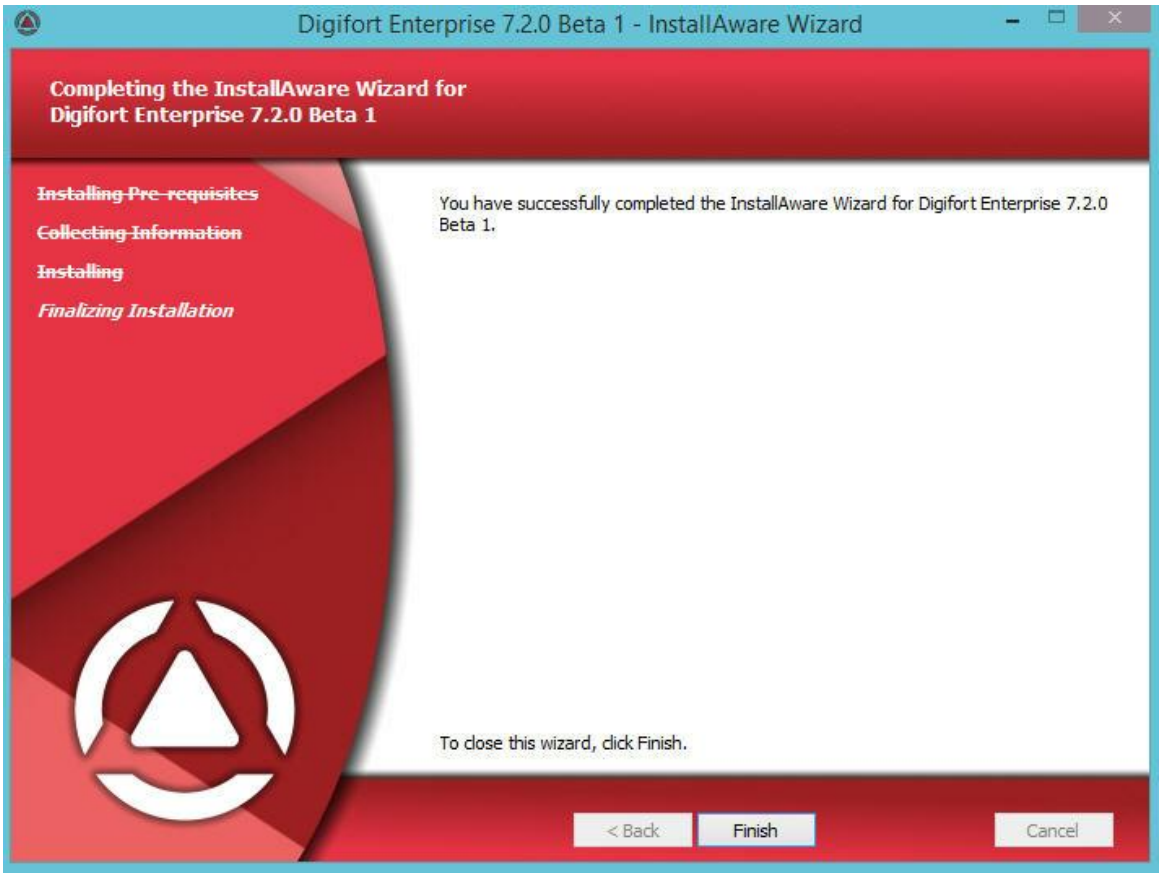


If you click on **Yes** the client will execute. Otherwise, the client installation will continue:



Continue the installation as normal and at the end click on **Finish**:

© 2002 - 2020 by Digifort, all rights reserved



Once installed, the compatible client is ready to connect to the requested server.

© 2002 - 2020 by Digifort, all rights reserved

Chapter XV

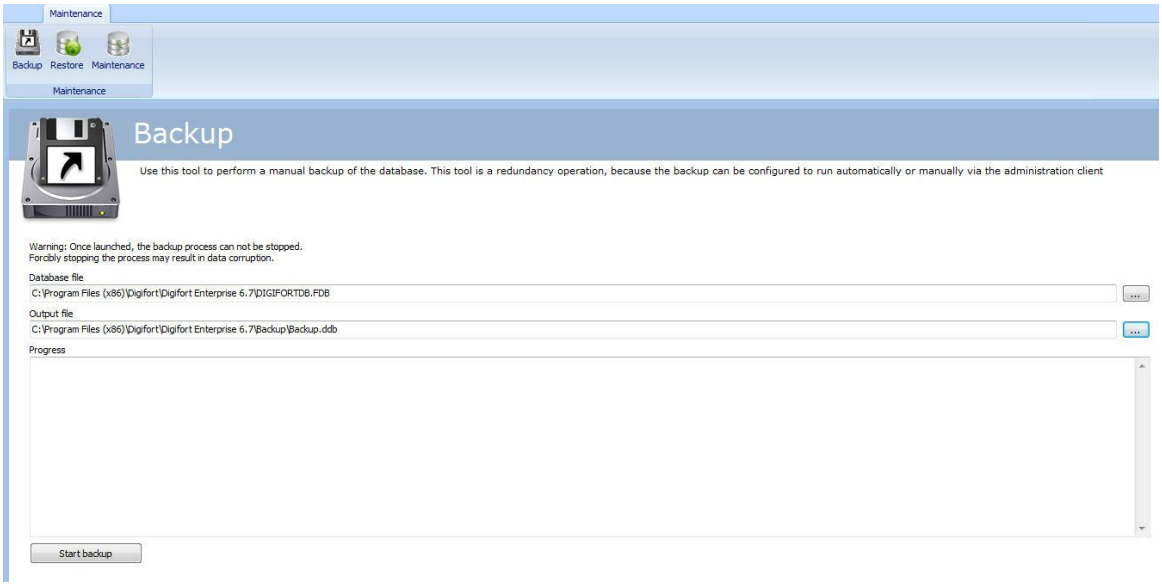
15 Maintaining the Database

We created new software for maintaining the database. Through it you can:

- **Make a backup of the database system**
- **Restore a backup of the database system**
- **Repair a corrupted database file**

This software is located in the root installation directory of Digifort. Its name is: DatabaseMaintenance.exe

Open the program as Administrator, and the following screen appears:



15.1 Backup

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

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

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

© 2002 - 2020 by Digifort, all rights reserved

15.2 Restore

After doing some backup, the only way to restore it is by this software.
To initiate a restore, click on the **Restore** button displayed in the image below:



The following screen appears:



- **Backup File:** Select the file to be restored with .**ddp**
- **Output File:** Select the file where the restore will be. Once that is done, replace the file in the root folder of Digifort with the name: **DIGIFORTDB.FDB**
- **Start Restore:** Click to start restoring the database.

15.3 Maintenance

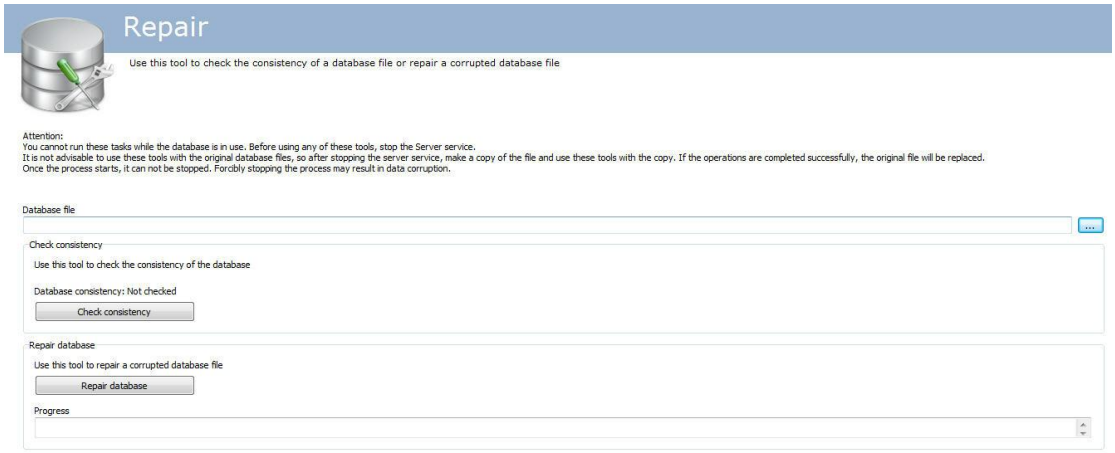
Use this option to check the consistency of the database or fix corrupt database problems.
To perform this function, click on the **Restore** button shown in the picture below:



NOTE: To perform maintenance, stop all Digifort services.

© 2002 - 2020 by Digifort, all rights reserved

The following screen appears:



The screen has the following features:

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

© 2002 - 2020 by Digifort, all rights reserved

Chapter XVI

16 Digifort Mobile Camera

The Digifort Mobile Camera is an application that can be installed on mobile phones and tablets with IOS (Apple) and Android (Google).

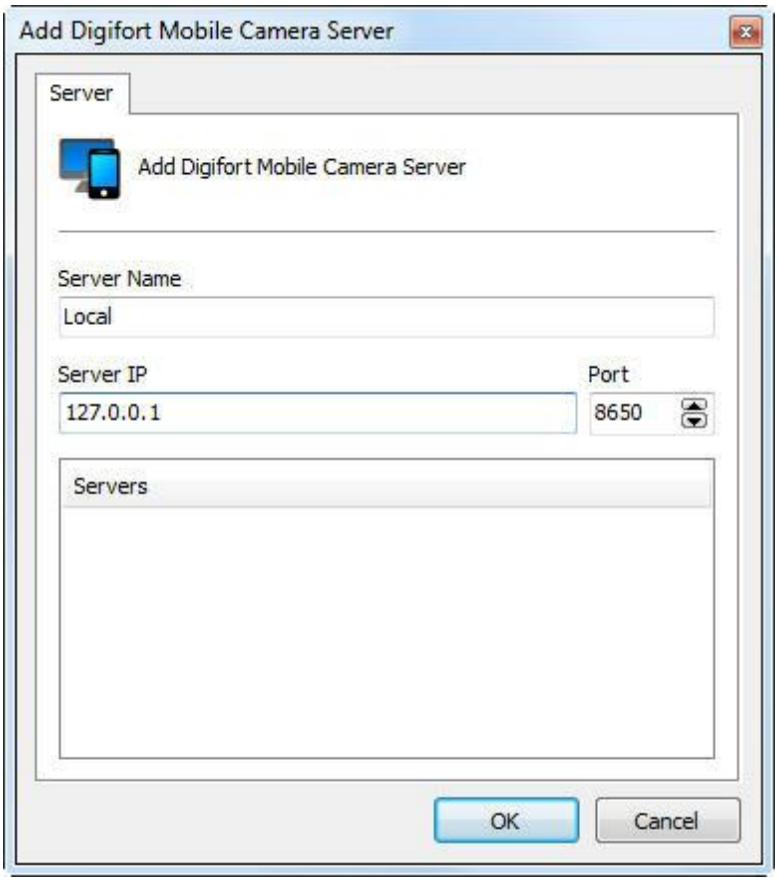
With this application you can turn your phone into a mobile remote camera and transmit a live video to your Digifort server via wireless or 3g / 4g connectivity, etc.

16.1 Registering the Mobile Camera Server

The first step to be done on the Mobile Camera configuration is to add and configure the server that will receive the application video streams.
To add a server click on the **Digifort Mobile Camera Servers** tree and then on the button **Add Server**, which opens the server registration screen, as illustrated in the image below:



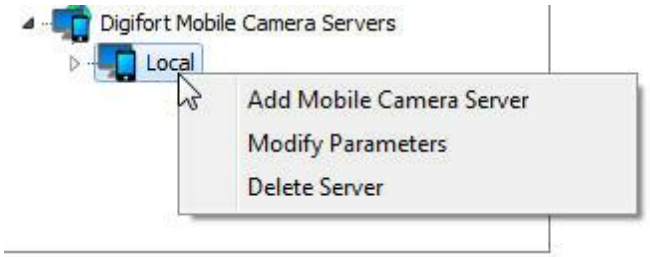
© 2002 - 2020 by Digifort, all rights reserved



- **Server Name**: Type the name of the server to be added. After data confirmation, the server name cannot be changed.
- **Server IP**: Enter the IP of the server to be managed.
- **Port**: Enter the communication port with the server. By default the port is 8650.
- **Servers**: In this list, all servers in the Mobile Camera that the Administration client can find on the network are available. Clicking on one of the servers, the IP and Port fields described above are automatically filled in. You only have to fill in the server name field to register.

After informing all data correctly click on **OK**.

After the server inclusion, it appears in the **Configuration Menu** as shown in the figure below:



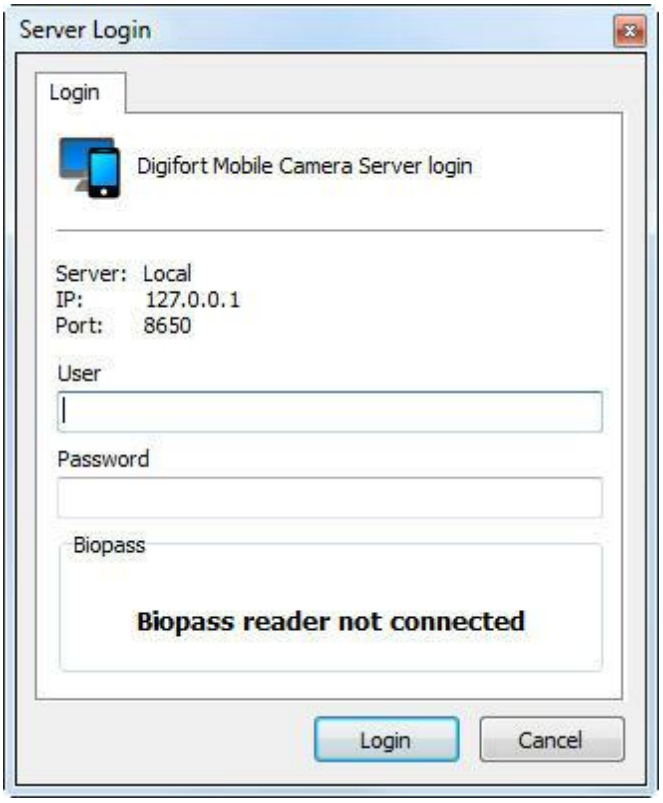
To change the settings of a server already saved, right-click on the server you want, and then click on Change parameters. In the window that opens, change the data as required and click on **OK**.

© 2002 - 2020 by Digifort, all rights reserved

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

16.2 Configuring the Mobile Camera Server

To configure the server, double-click on the registered server and the login screen appears:



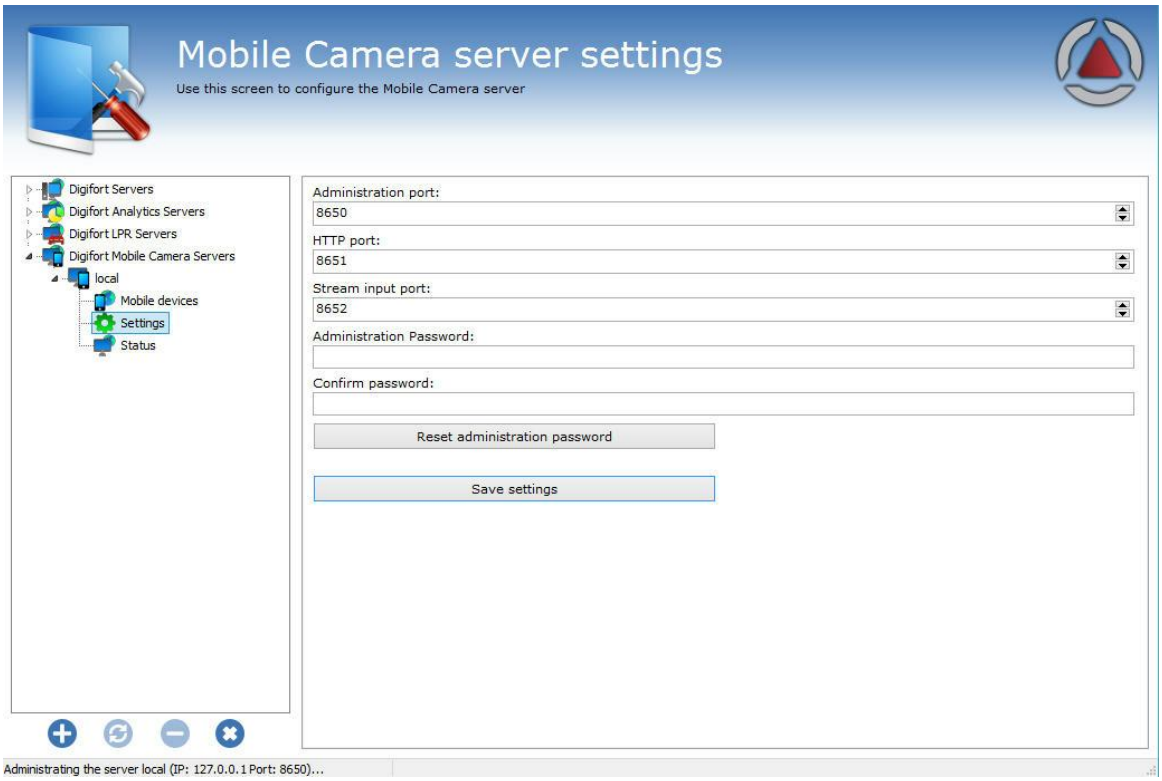
The default username is **admin** and the password is blank.

16.2.1 Configurations

To access the server configurations, click on **Configurations** as in the image below:



© 2002 - 2020 by Digifort, all rights reserved



This screen provides the following features:

- **Administration port**: Port used by Digifort to configure the Digifort Mobile Camera server.
- **HTTP Port**: http port used for communication.
- **Stream input port**: Port used to receive the video stream;
- **Administration password**: Administration password of the Digifort Mobile Camera server.
- **Confirm password**: Confirm the password to register.

- **Admin password reset**: redefines default password, that is, blank.
- **Save Configuration**: Saves the changed configuration.

Note: It is important to remember that these ports must be released on the firewall and network of computers involved.

16.2.2 Status

In **status** you can check important information such as consumed bandwidth and connected devices.

To access click on **Status** as shown below:

© 2002 - 2020 by Digifort, all rights reserved



In the **General** tab, there are two charts:



The first one shows the **total bandwidth consumption** and the second one shows the amount of **devices attached** to the server.

In the **connections tab**, there is the list of connected devices, IP, bandwidth consumption and the total time connected to the server:

© 2002 - 2020 by Digifort, all rights reserved



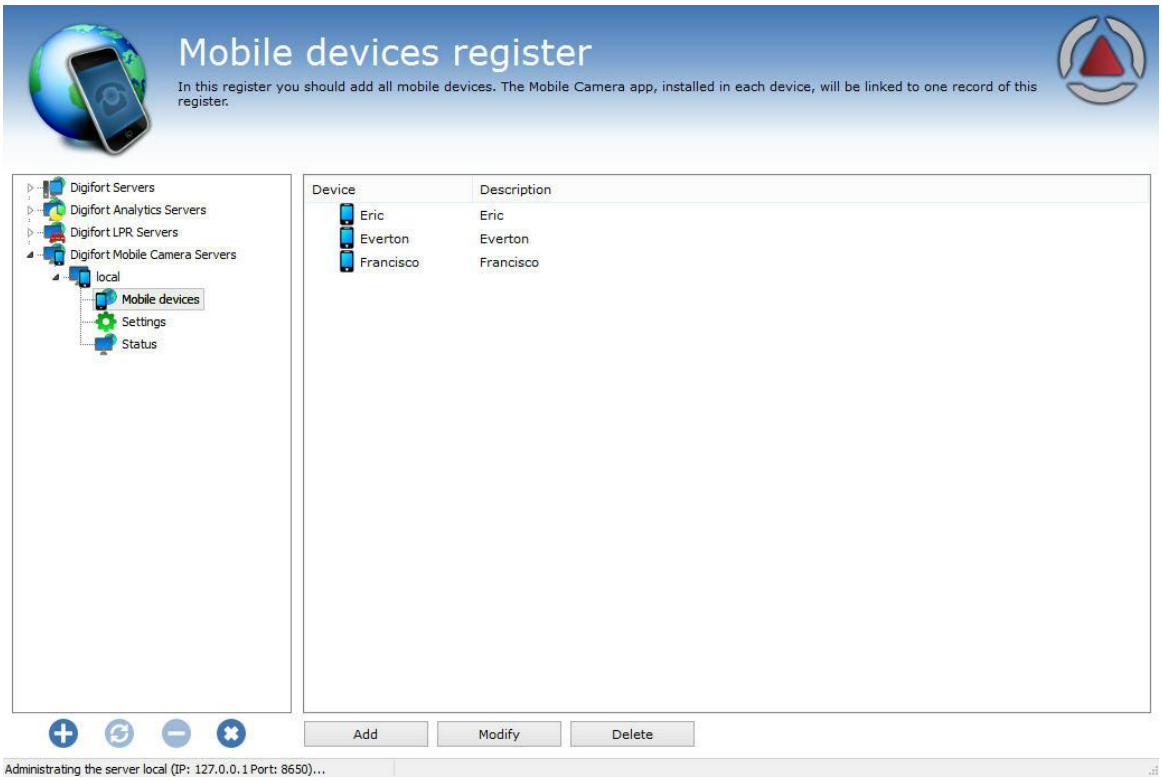
16.2.3 Mobile devices

You need to register the devices that will send the images to Digifort.
Click on **mobile devices** as in the image below:



The following Register screen appears:

© 2002 - 2020 by Digifort, all rights reserved

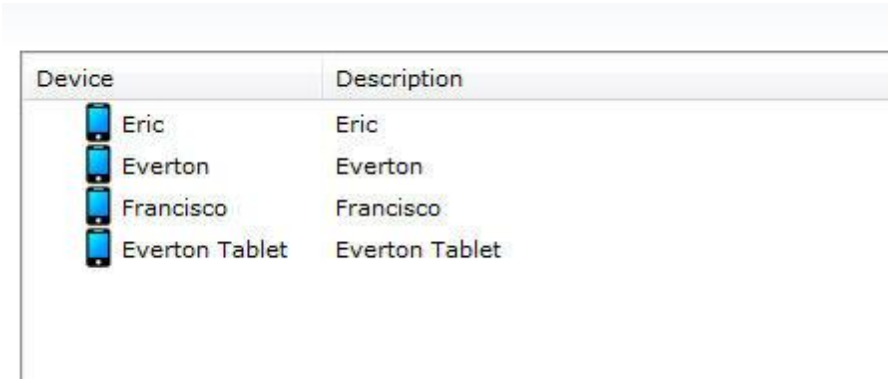


Add a **unique name** to associate the mobile device to the Software. To do this, click on Add. The following screen appears:



Enter the device name and click on OK. The device will be registered in the list:

© 2002 - 2020 by Digifort, all rights reserved



16.3 Configuring the application

First of all, download the **Digifort Mobile Camera** application on Google Play or AppleStore and install it on your mobile device.

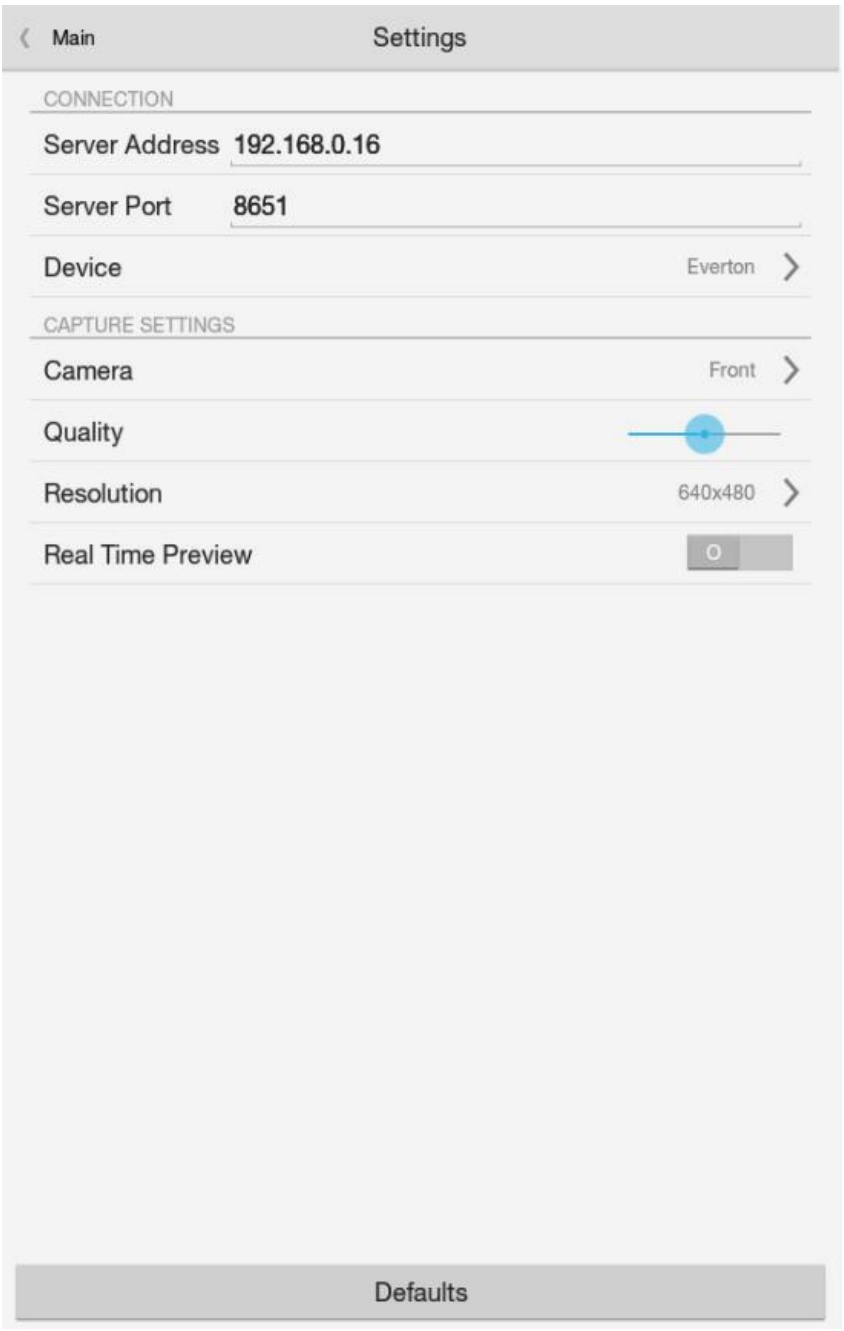
When you open the application, the following screen appears:

© 2002 - 2020 by Digifort, all rights reserved



First, click on the gear on the top right corner, and the following configuration screen appears:

© 2002 - 2020 by Digifort, all rights reserved



In the configuration screen, register the **Server IP** where the **mobile device** is registered, as explained in the previous topic.

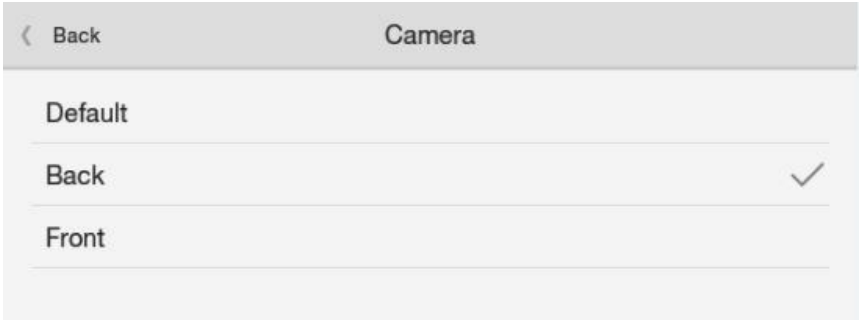
- **The server port** is the same from the previous topic.
- **Device**: click on this option and the devices registered in Digifort appear in a list:

© 2002 - 2020 by Digifort, all rights reserved



Select the desired device.

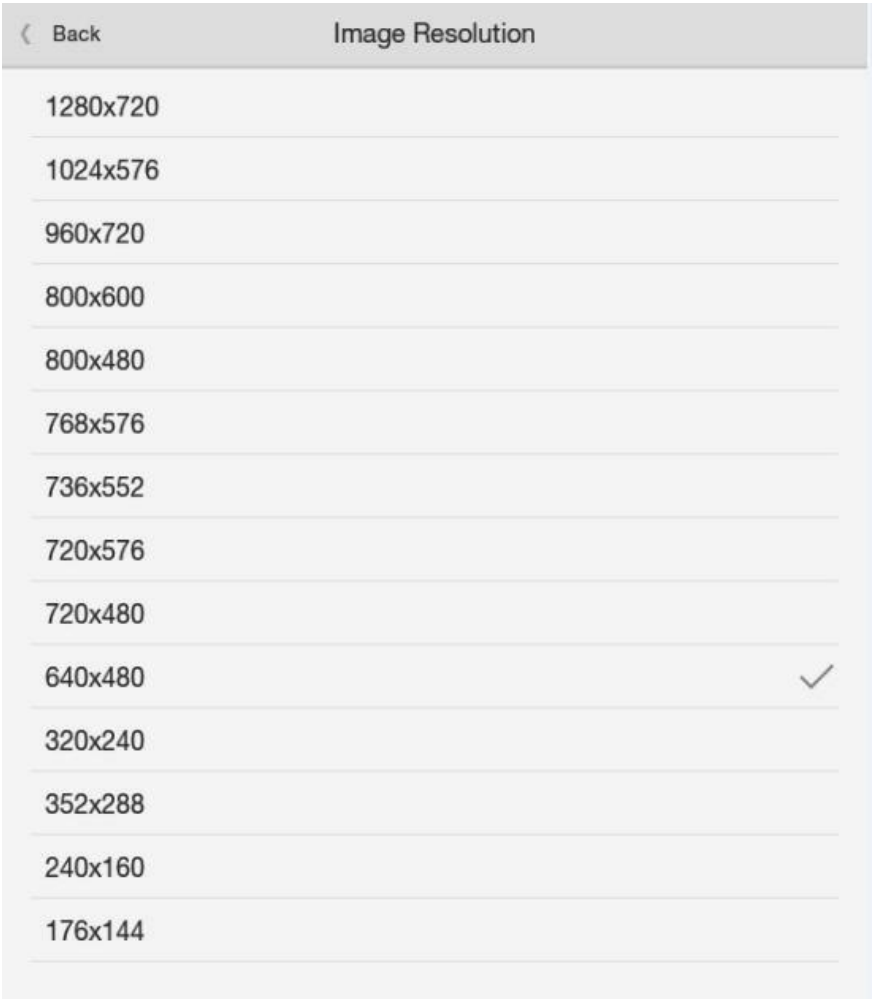
Camera: If your device has a front or rear camera, you can select it in this option.



Quality: Select the streaming quality of the images.

Resolution: Click on this option to choose the resolution for image streaming;

© 2002 - 2020 by Digifort, all rights reserved



Real Time Preview: If the option is not enabled, the video stream appearing on your device screen is sent to the system. In case of slow streaming, you can have a defective image.

After the **settings**, go back to the home screen and click on **Start Streaming**

© 2002 - 2020 by Digifort, all rights reserved



The image captured by the mobile device is sent to the server.

On the **top left** corner, there is the option to **turn on your device flashlight** if supported.
On the **lower left** corner, there is the detail of video streaming: **Frames per second and bandwidth used**.

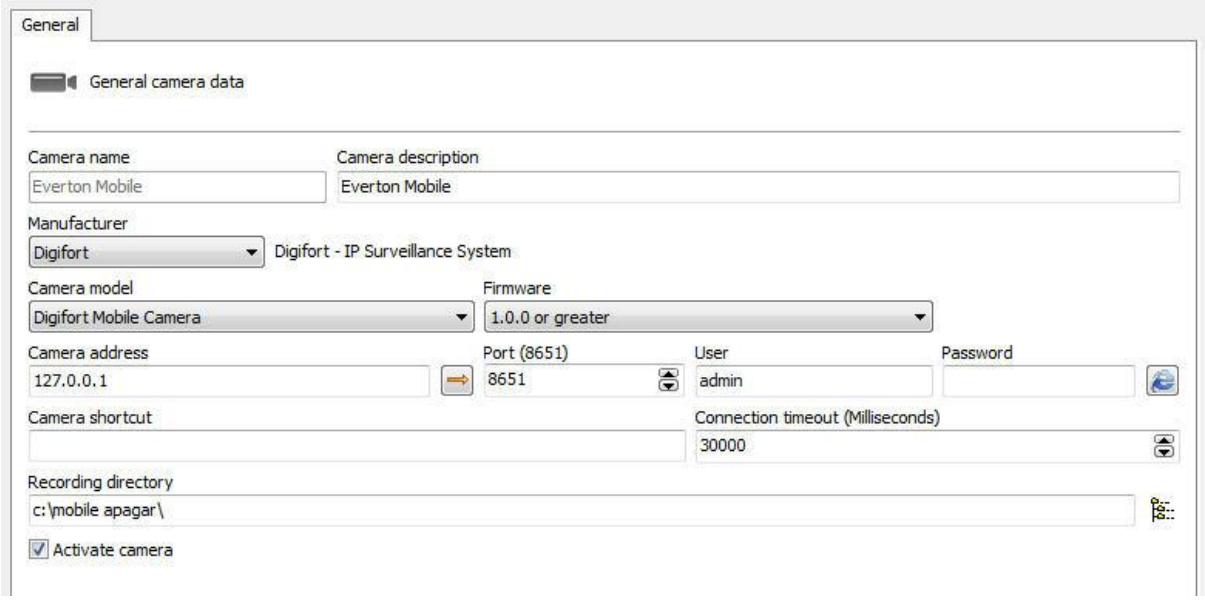
If you want to interrupt the video streaming, simply click on **Stop Streaming**.

16.4 Registering the camera

The last step is to register the Mobile Camera to record in Digifort.

Open the recording server and click on **Add**. If you have any questions on camera registration, check Recording Server

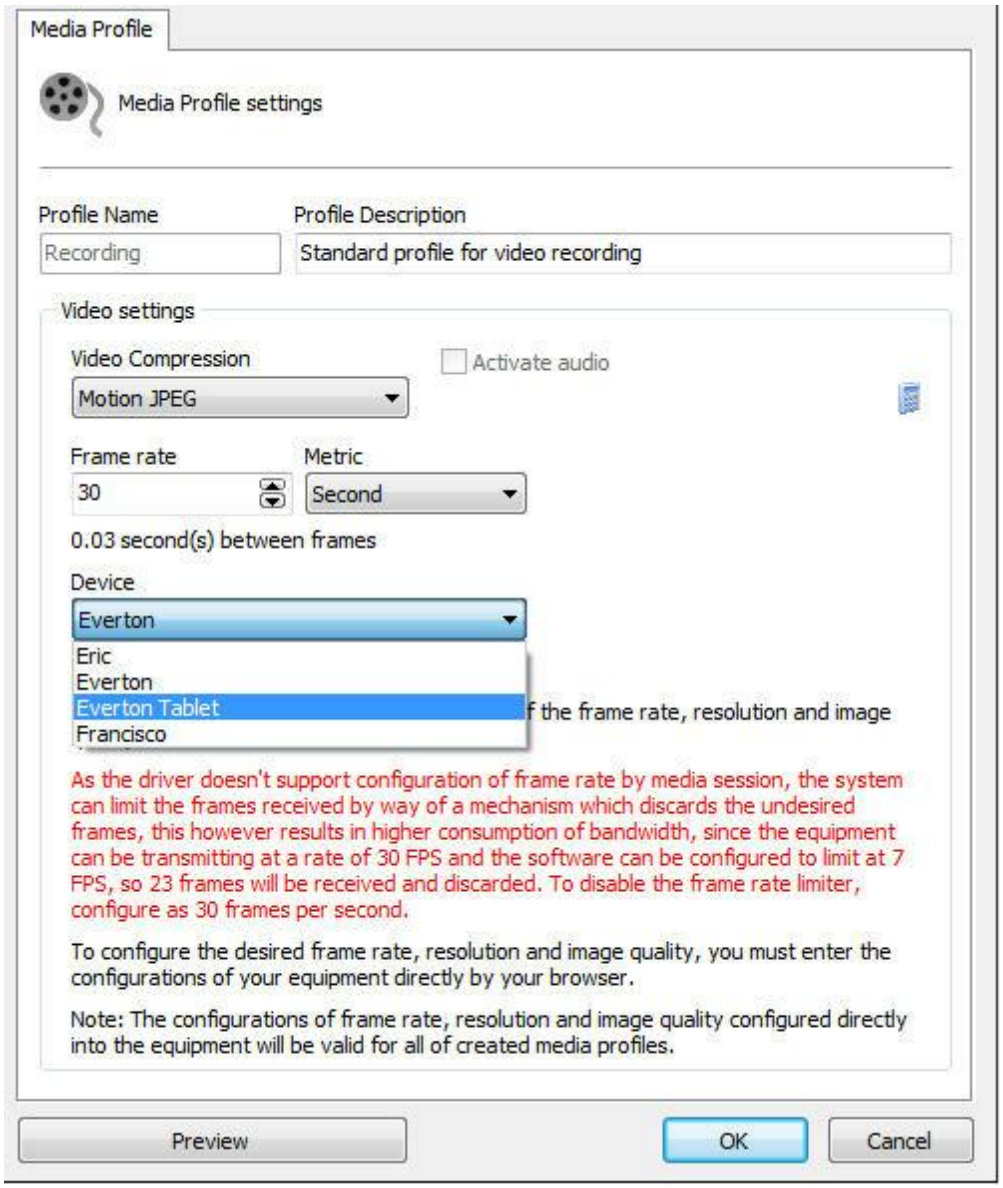
© 2002 - 2020 by Digifort, all rights reserved



On this screen, type the **Name** and description to identify your camera.
In **Manufacturer**, choose Digifort.
In **camera model** choose Digifort Mobile Camera.
In **Camera Address**, choose your server IP from the Digifort Mobile Camera server. Check Configuring the Mobile
If it has not been changed, the default communication port of the Digifort Mobile Camera is **8651**.
In User and Password, enter the Digifort Mobile Camera server user.
And finally, choose a directory for recording;

Now click on **Media Profiles** and double click on the recording profile:

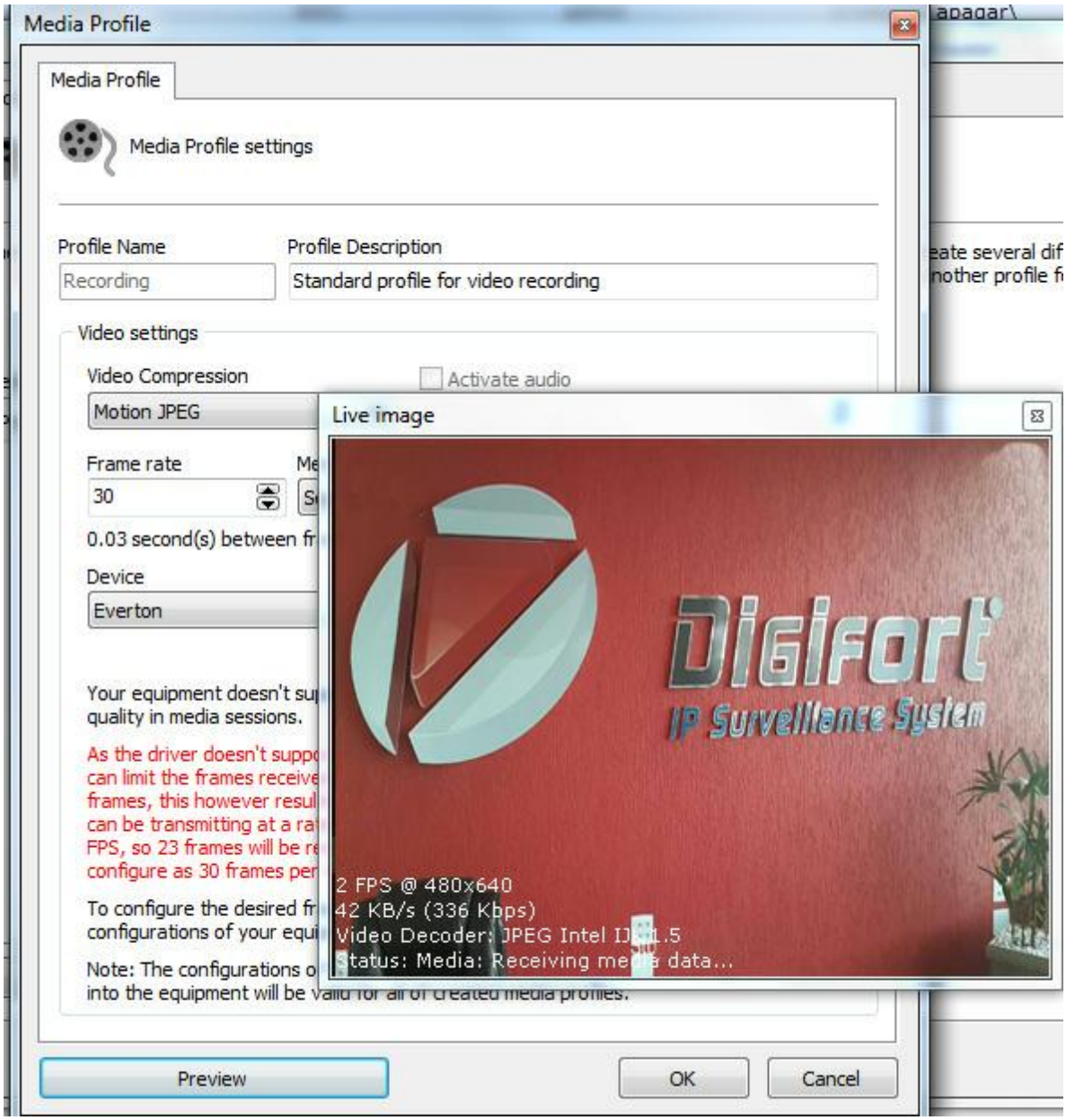
© 2002 - 2020 by Digifort, all rights reserved



The Digifort streaming is made in **JPEG Motion**. Choose the desired frames per second rate.

Now on the **Device** option, choose the device that is receiving the **Stream**.
Click on **Preview** to view the image being streamed:

© 2002 - 2020 by Digifort, all rights reserved



Done, Digifort is ready to record the images received.
Note that the resolution of the image to be recorded must be configured in the Device, as shown in the Configuring the application topic

© 2002 - 2020 by Digifort, all rights reserved

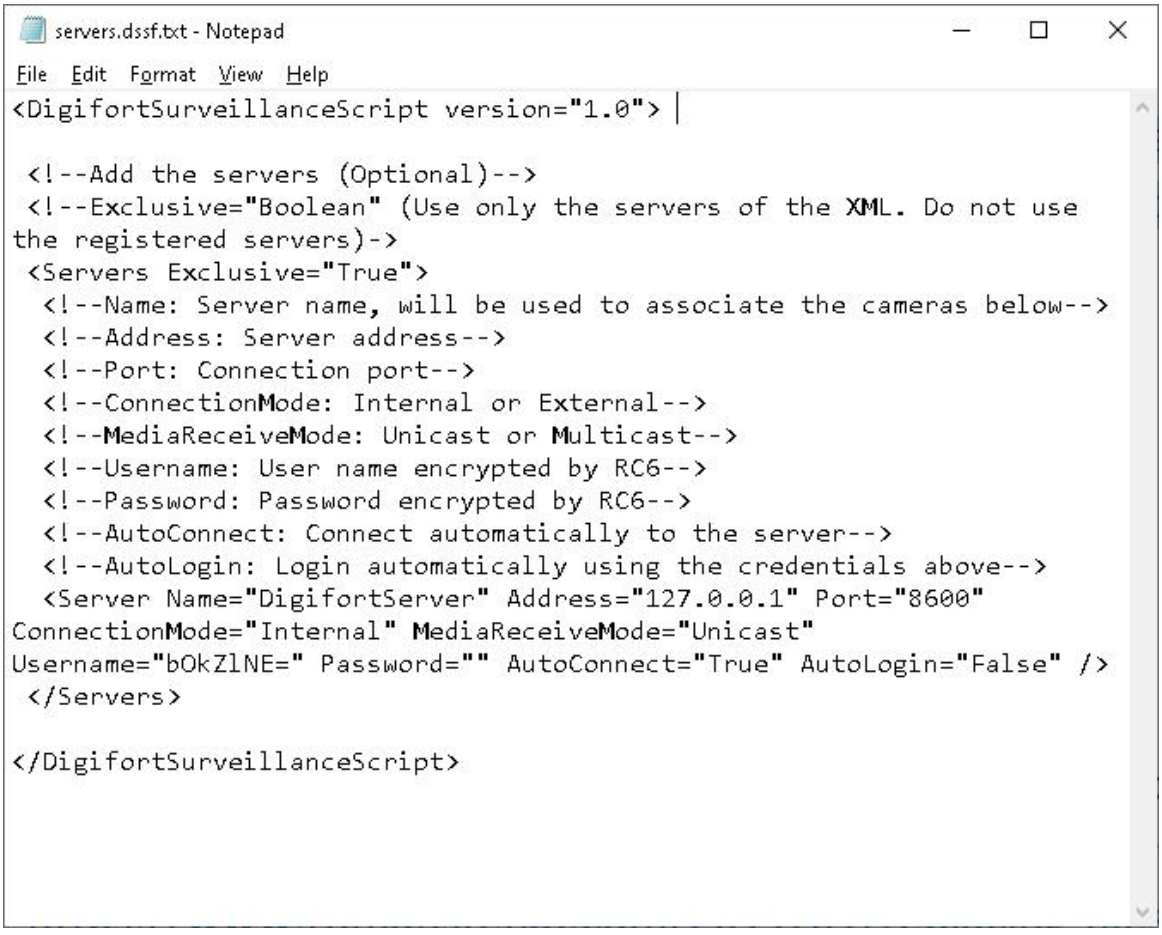
Chapter XVII

17 Centralized server list

Attention, this feature is intended for advanced users of the system.

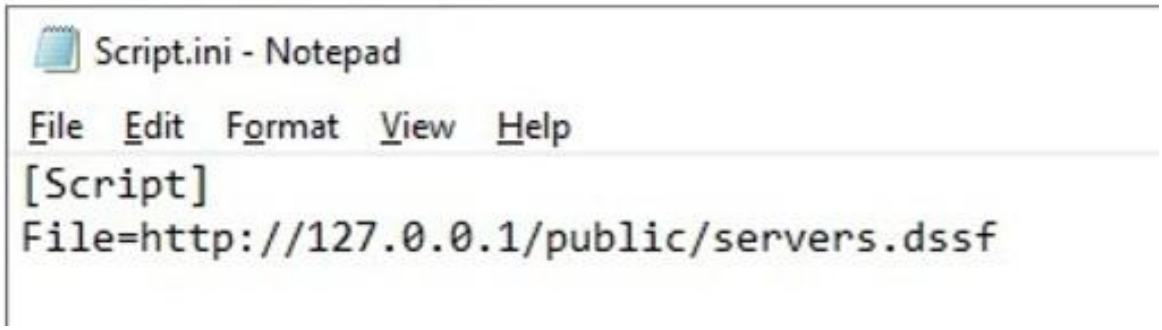
It is possible to have your Monitoring clients access Digifort servers listed in a file that is hosted on the eu network on a web server.
The idea behind this feature is that you do not have to manually register the servers to be connected to the Monitoring client manually.

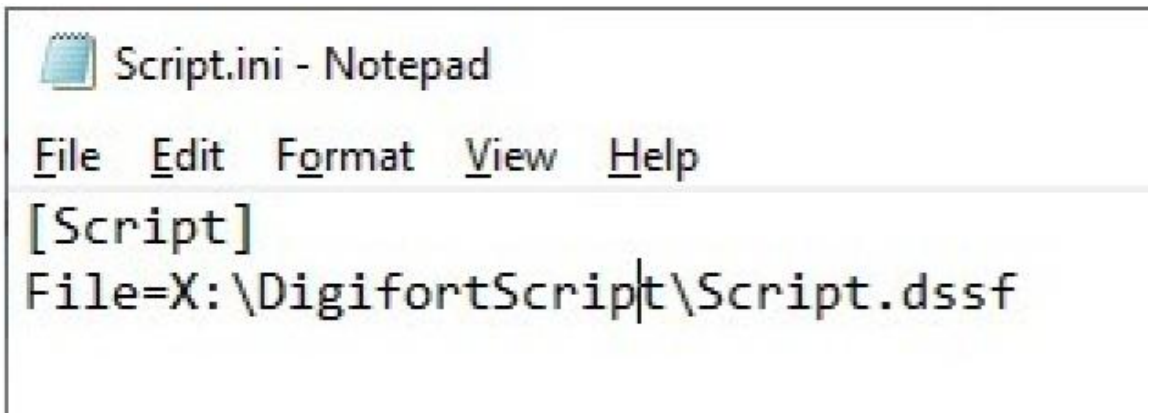
To do this, you will need to create a file with the extension .dssf. Within this file there will be an xml structure with the information of the server to be accessed:



After that create a Script.ini file in your Digifort installation folder (Ex: C:\Program Files (x86) \Digifort\Digifort <your version>)
with the path to the Dssf file as shown in the image below:

© 2002 - 2020 by Digifort, all rights reserved





Now whenever you start the monitoring client it will look for the servers contained in the dssf file.

© 2002 - 2020 by Digifort, all rights reserved