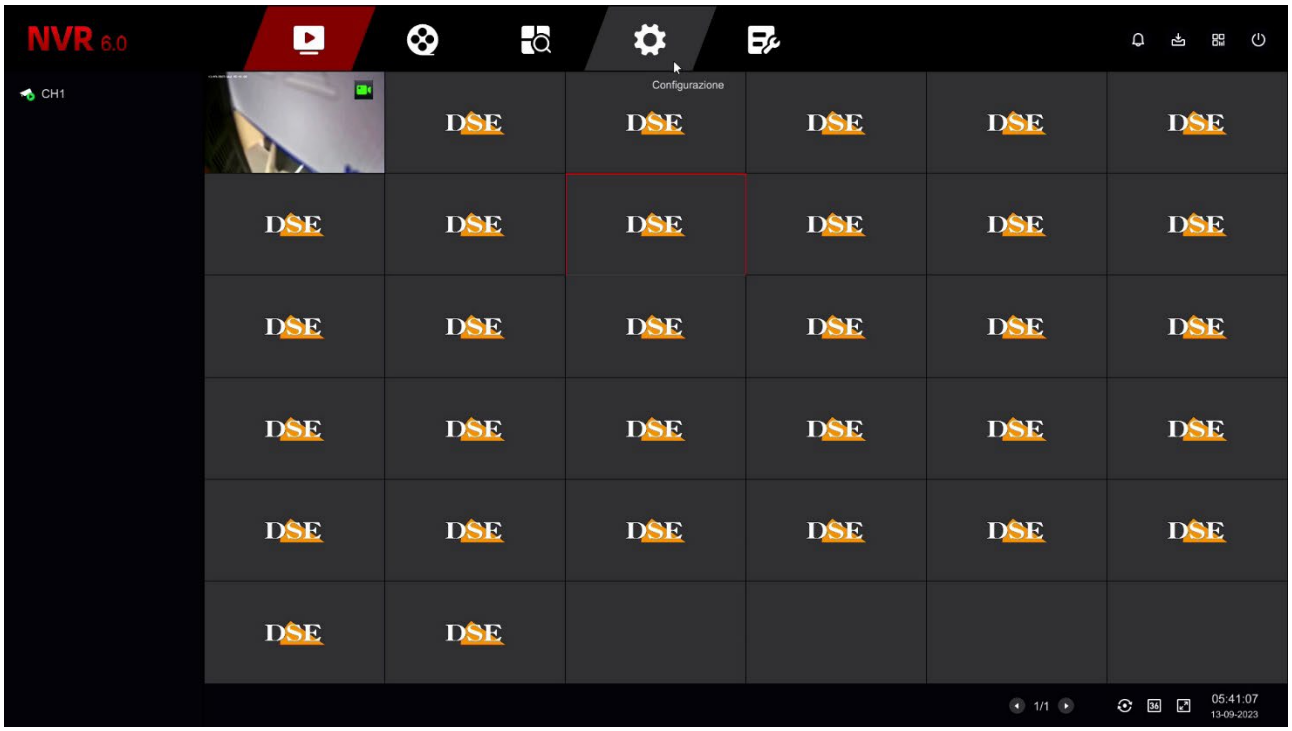
RK and RKK SERIES

DVR and NVR



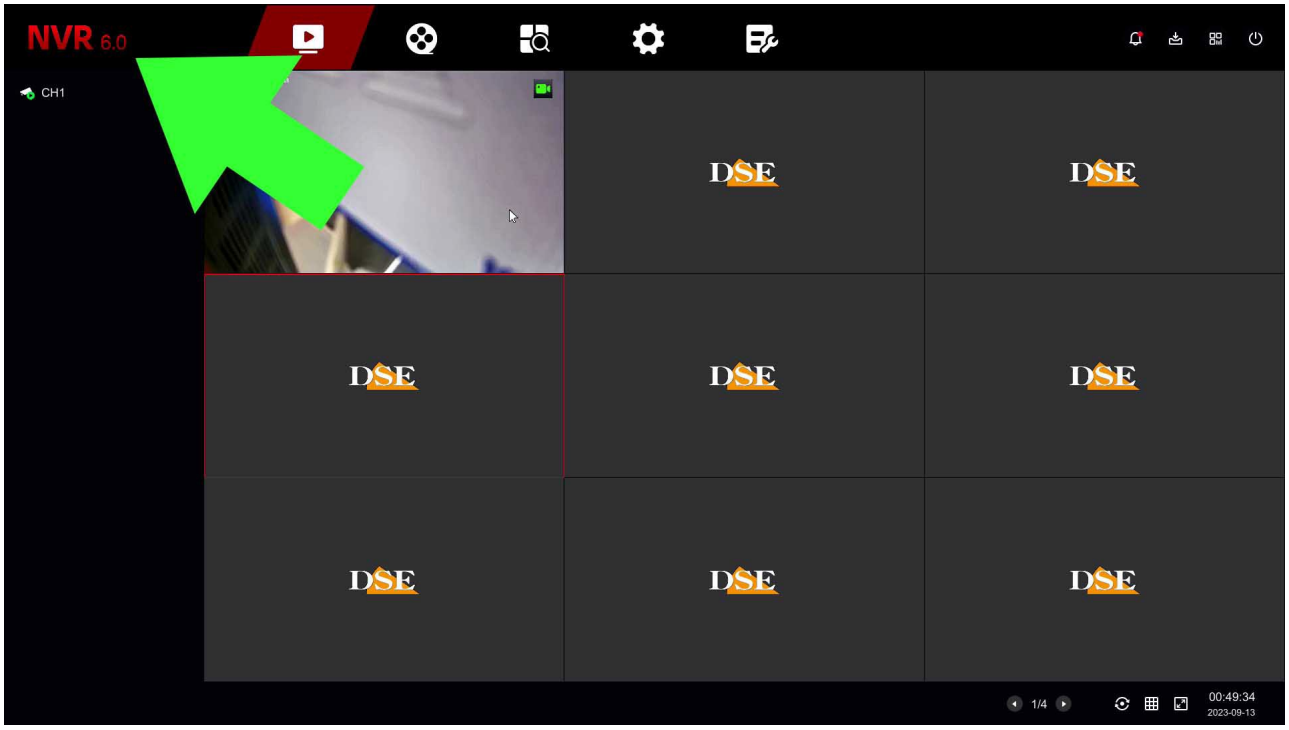
Configuration manual - Menu 6.0

How to configure all system operating options

Contents of the manual

This manual explains in detail all the configuration options for make the best use of our RK Series DVRs/NVRs. For using normal live viewing functions and playback, for hardware installation and for connecting cameras download the installation manual .

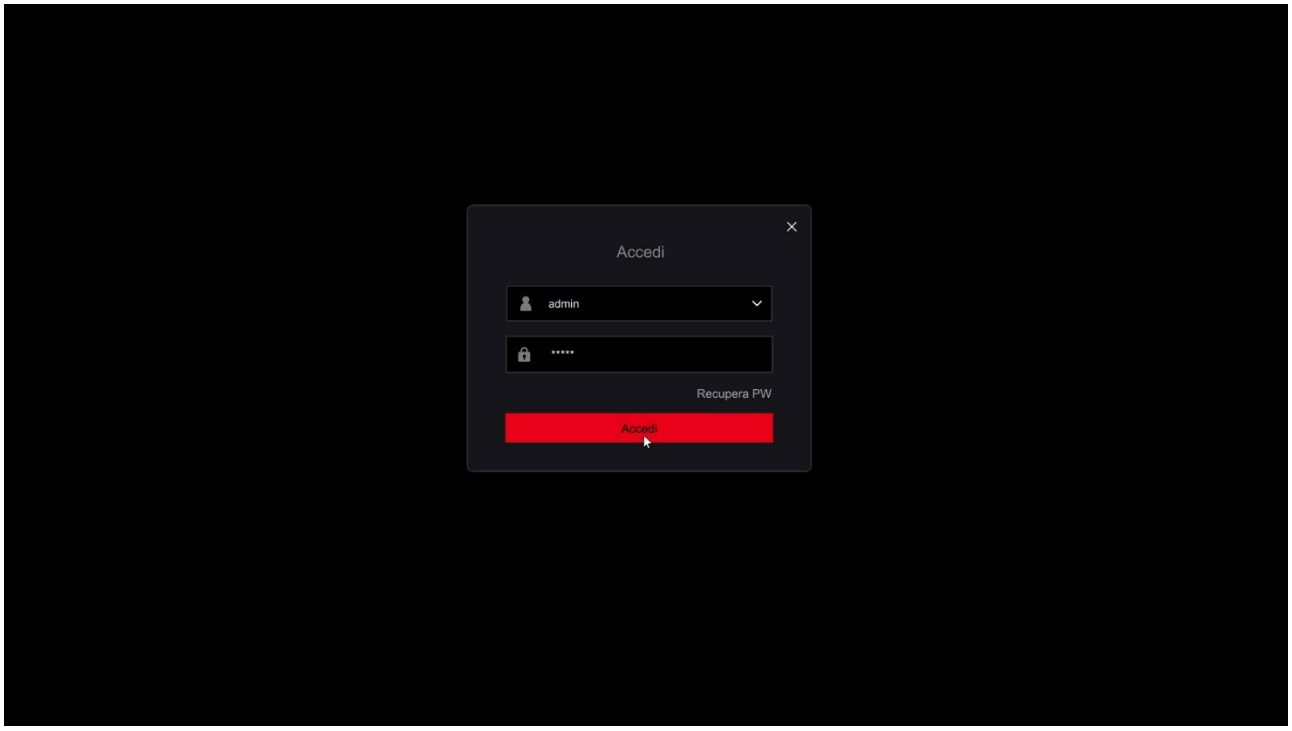
This manual refers to the NVRs with Version 6.0 graphical interface that you see below



If your NVR/DVR has our interface 5.0 or earlier, you can download the specific manual for your version, or you can continue reading this manual considering that you will find in the your screen the same options, just with different graphics.

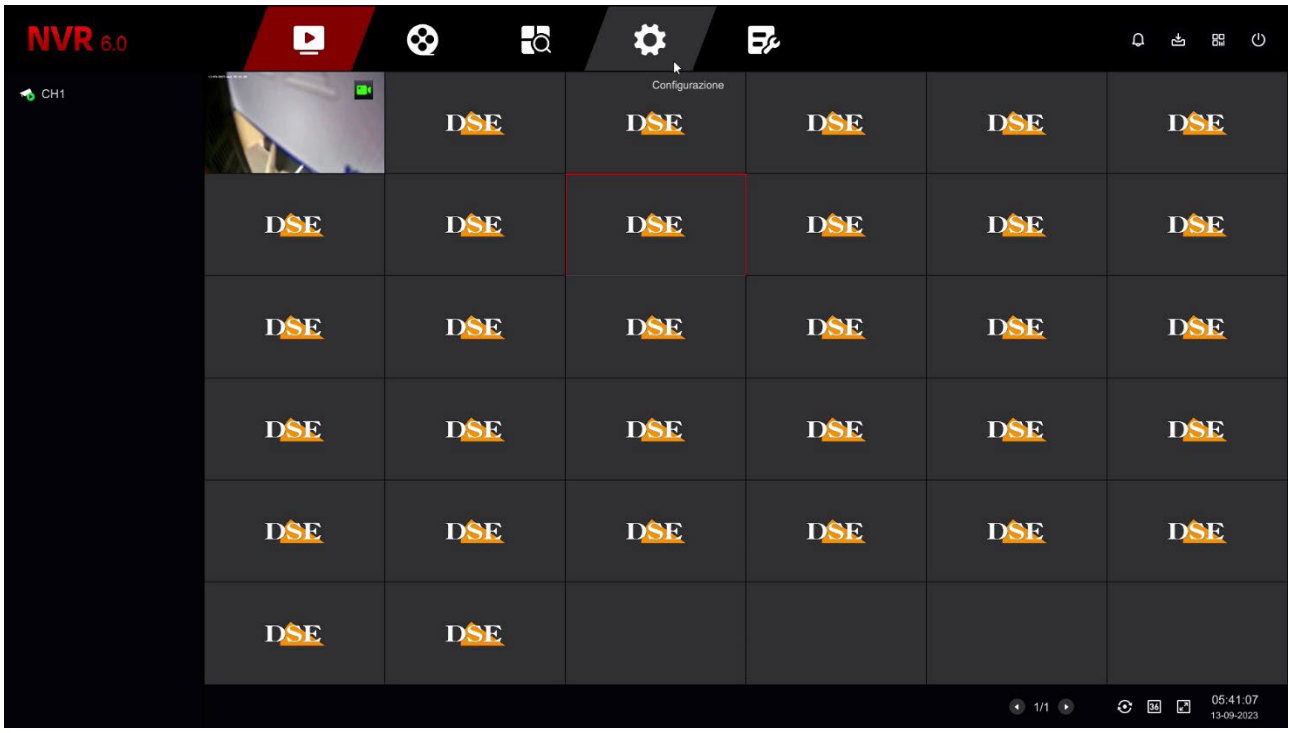
Access the control menu

The installation manual explains how to install and use the basic, live features
and playback, of our RK Series NVRs and DVRs.
If you haven't mounted your system yet and you don't yet see the cameras on the monitor, it's a good idea
return to the installation manual and follow the instructions. If you have installed the e
you are able to move the mouse around the screen, you can continue reading this
manual and learn all the advanced features of your CCTV system.
In this manual we start from the login window in which to enter the username and password for
access.



The factory access data for the RK Series NVRs and DVRs are:
USERNAME: admin
PASSWORD: 12345

To access the configuration menu you must right-click on the screen


NVR 6.0
CH1
Configurazione
1/1
05:41:07
13-09-2023

Navigation bar

At the top of the monitor there is a navigation bar to browse the different control environments of the device.

LIVE PLAYBACK MAINTENANCE CONFIGURATION SEARCH

The first 3 environments LIVE, PLAYBACK and SEARCH, for viewing and playback, are explained in installation manual .

This manual explains the CONFIGURATION and MAINTENANCE pages

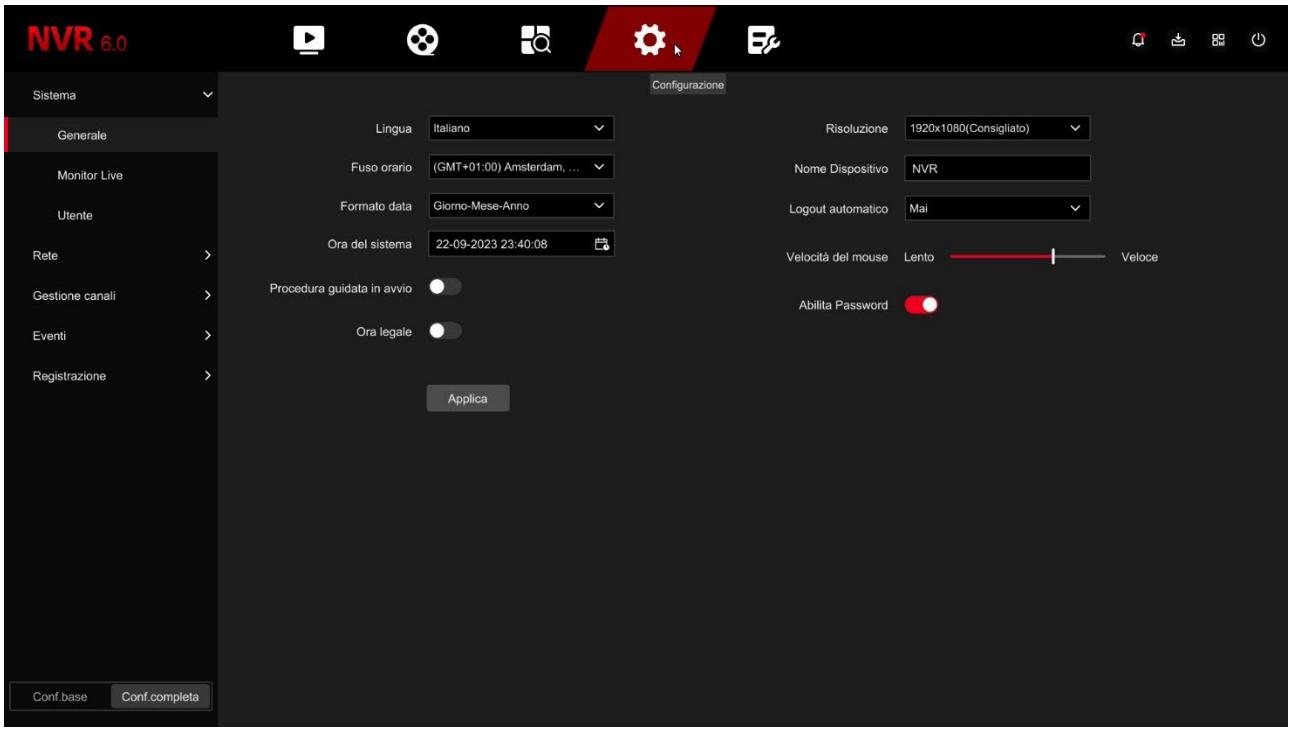
In addition to the main navigation bar there are buttons at the top right

1 2 3 4

1 – Opens the popup window listing the latest alarm events, divided into Anomalies, Alarms normal and Intelligent Alarms
2 – Opens the backup window where you can see the progress of saving videos to memory external
3 – Shows the QR code that identifies the device and is used to load it into our app
4 – The power off button allows you to log out (a new login will be required),
turn off the device and restart it.

CONFIGURATION | SYSTEM

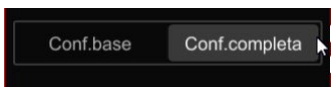
Click the CONFIGURATION button to open the page containing the configurable options of the your NVR/DVR



BASIC AND COMPLETE CONFIGURATION

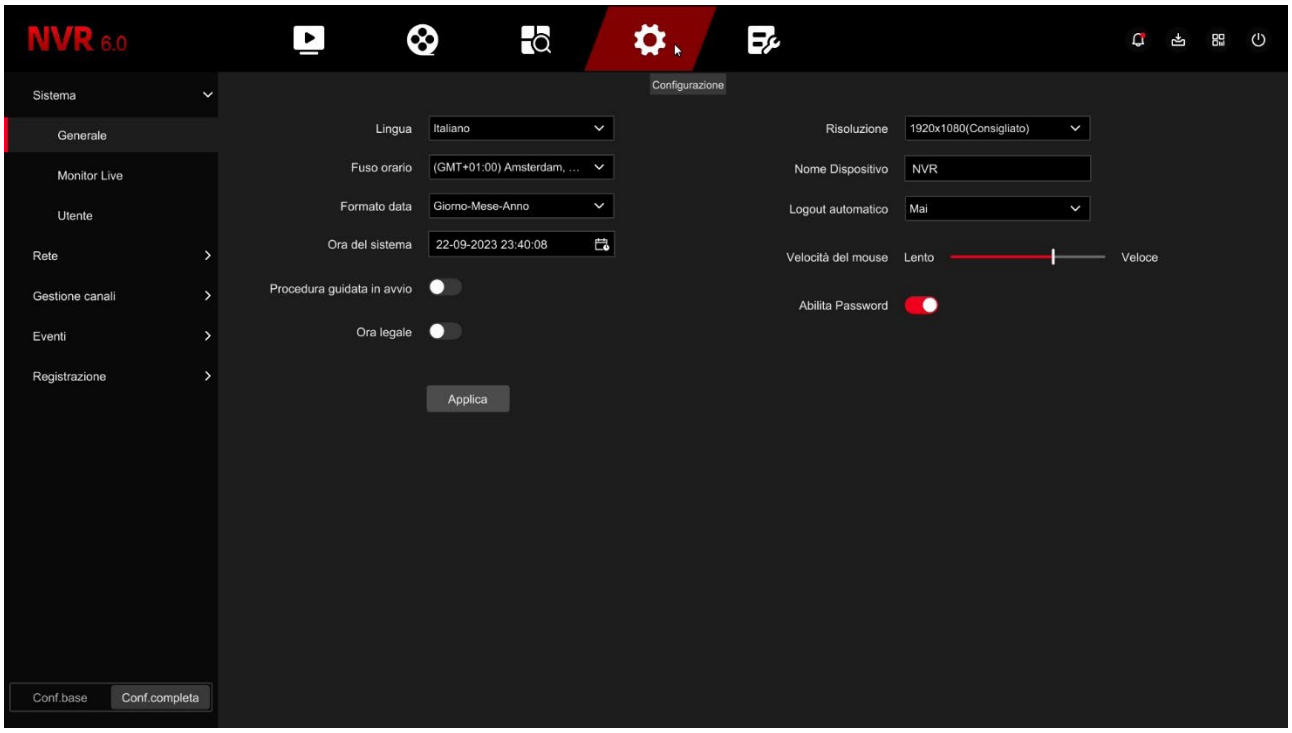
In the bottom left corner you can select whether to see the basic configuration or the advanced configuration. The basic configuration shows the most used options, so you can find them more easily. The complete configuration includes all options.

In this manual we activate the FULL CONFIGURATION to describe all the items of configuration



SYSTEM | GENERAL

On this page, the first of the SYSTEM section, some general options are set device



LANGUAGE – The factory language is Italian, but you can choose another from the dozens available

TIME ZONE – Choose the time zone of your area which in Italy is GMT+1

DATE FORMAT – Choose the format to indicate date and time, normally Day/Month/Year

SYSTEM TIME – Shows the system date and time which you can manually change

STARTUP WIZARD – After completing the installation of the NVR/DVR it is convenient for you disable the wizard when starting the video recorder by unchecking it
option. The wizard is explained in the installation manual.

DAYLIGHT TIME – You can have the NVR automatically adjust to daylight saving time. This setting may vary from country to country. In Italy, you must set the WEEKLY type and duration 60 minutes, starting at 2am on the last Sunday of March and ending at 3am on the last Sunday of October.

RESOLUTION – Here you set the resolution of the video outputs for the monitor. Don't set one too high resolution that your monitor does not support. The resolution most commonly supported by the monitors is the factory 1920x1080 one.

DEVICE NAME – You can assign a name to your DVR/NVR to easily identify it.

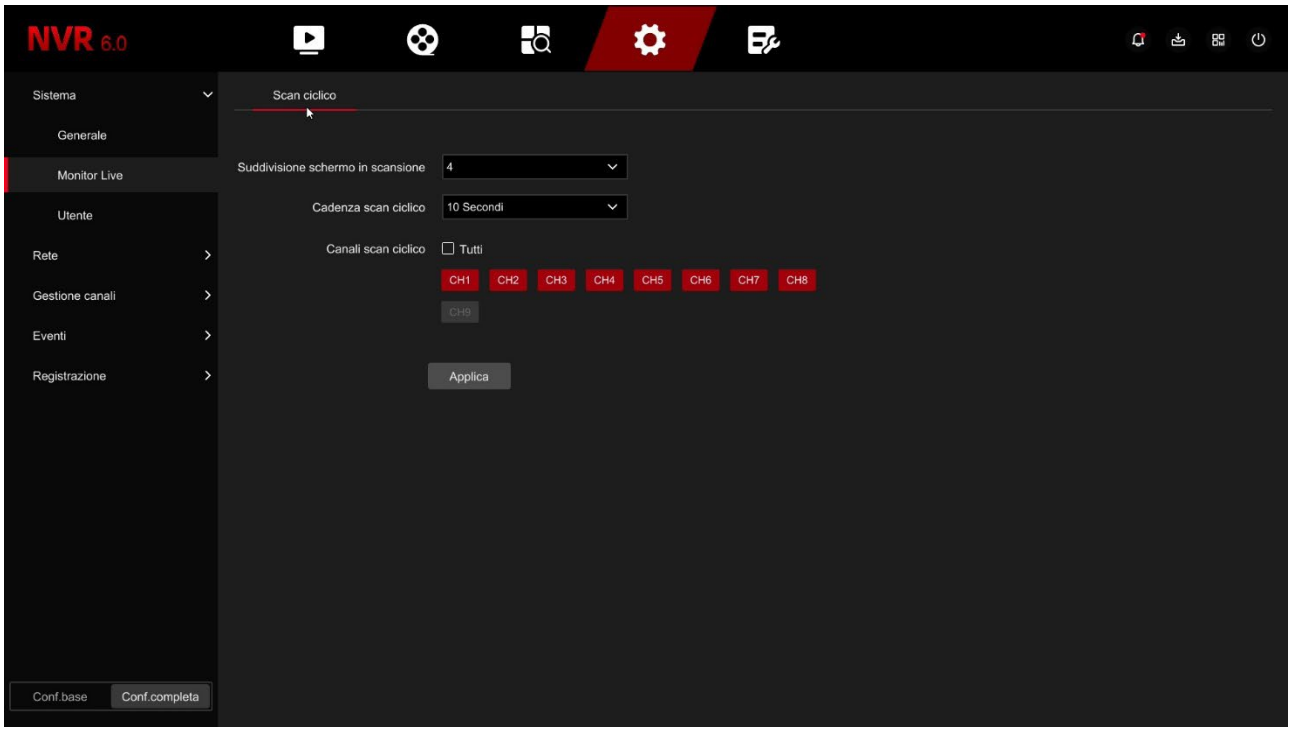
AUTOMATIC LOGOUT – Defines after how many minutes of operator inactivity the system will require a new login to access the NVR.

MOUSE SPEED – Adjust the mouse speed of the DVR/NVR

ENABLE PASSWORD – Normally access to the NVR control is protected by a password. If you use the NVR locally, among known people, you can disable password control. Disable the Password checking is never recommended if your device has access to the Internet.

SYSTEM | LIVE MONITOR | CYCLIC SCAN

Here you can configure the cyclic scanning of cameras on the monitor. Cyclic scanning is possible activate and suspend with one button in the live window.



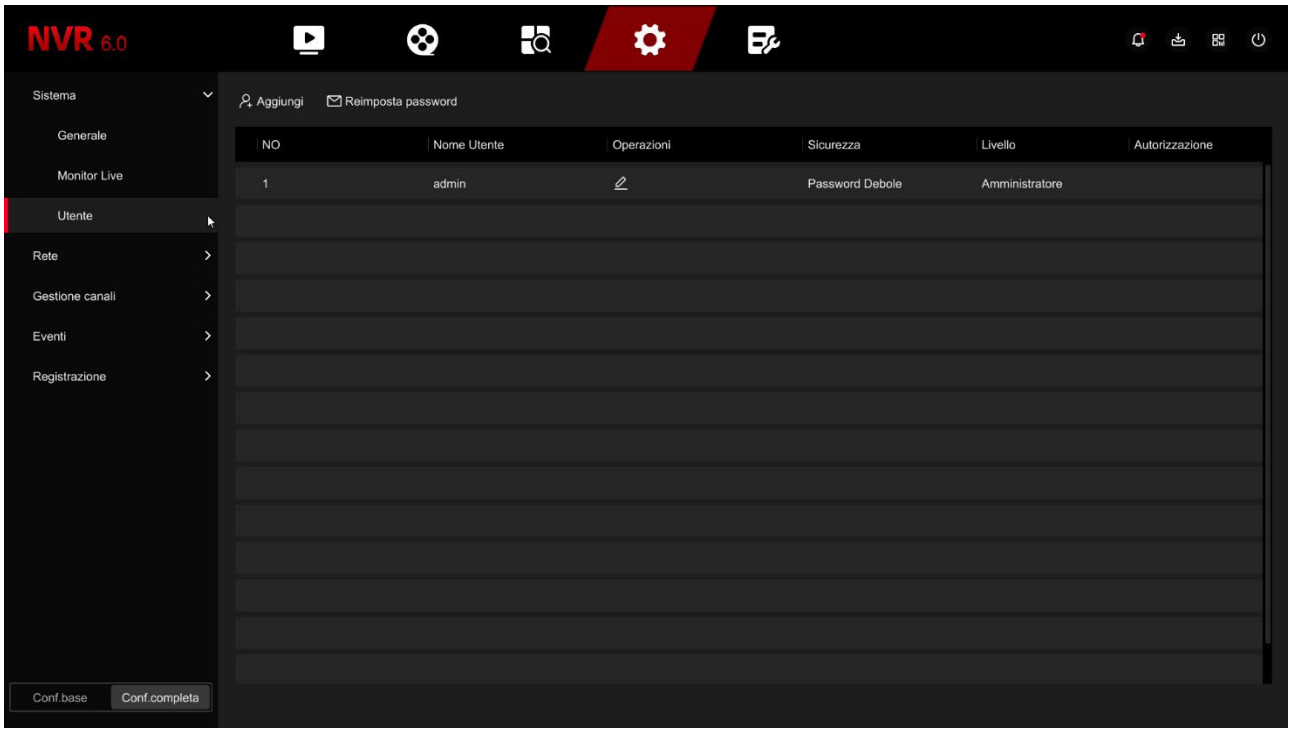
SCREEN SPLIT IN SCAN – Normally cyclic scanning is carried out by taking a full screen one camera at a time. To get this feature you need to set this parameter to 1. If you have many cameras you may also want to cycle the multivisions by 4 or 9 cameras at a time.

CYCLIC SCAN RATE – Here you set the duration of each 5 scan on the screen seconds to 5 minutes

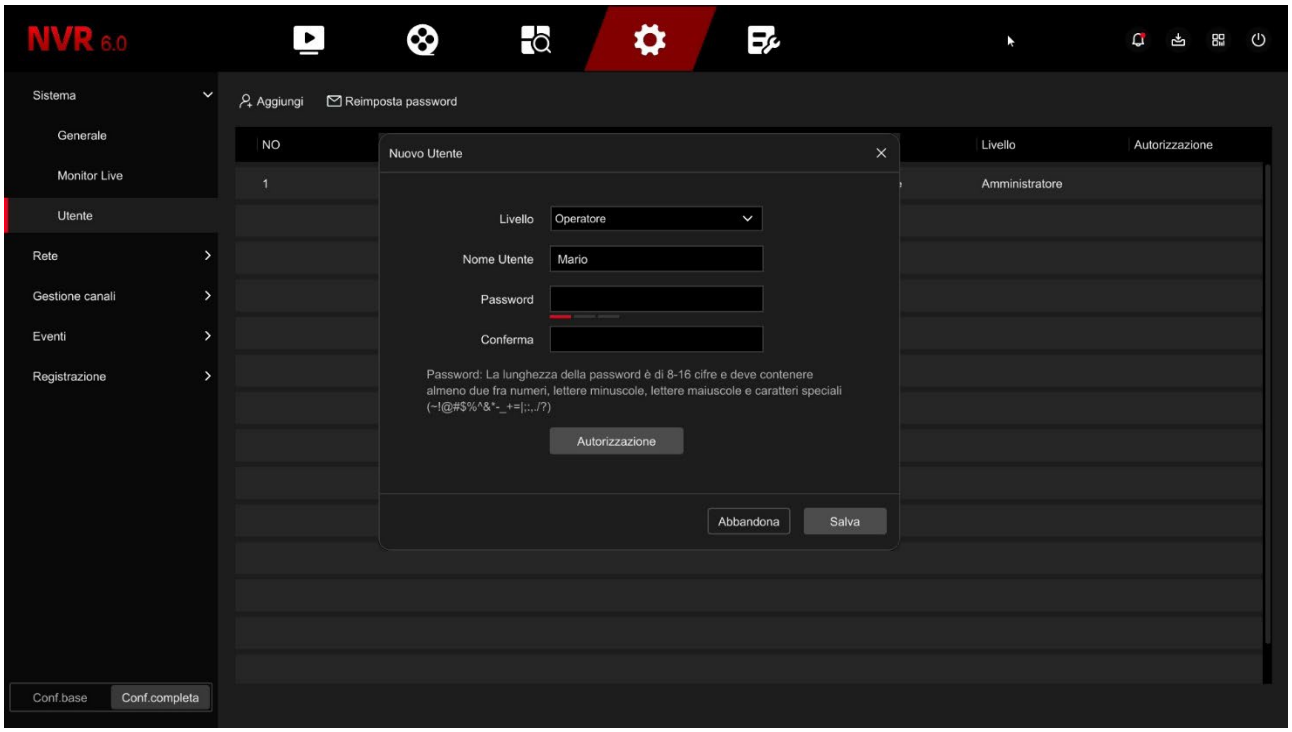
CYCLIC SCAN CHANNELS – You can set which channels to include in the scan, possibly excluding some.

SYSTEM | USER

Here the administrator can enter other users who will have access to the device, each with your access level



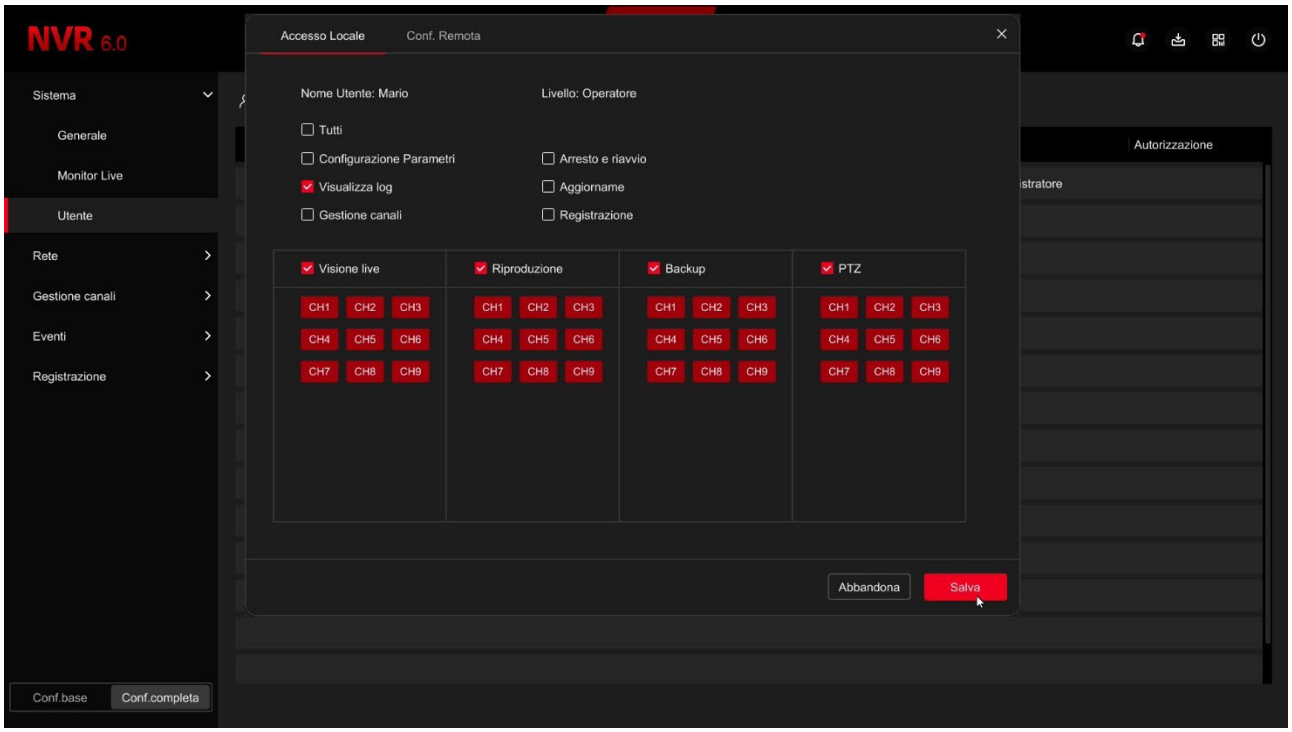
RESET PASSWORD – The first button allows you to enter the email address that will be used for possible future recovery of the forgotten password.
ADMIN USER – The administrator user is already present in the list and cannot be deleted. With the edit button you can change the administrator password. You can enter a new one password of at least 8 characters with at least one letter and one number and also set a sign unlocking, as is done on mobile phones.
ADD – Press to add a new user



LEVEL - There are two pre-configured permission levels that you can choose when creating the user: Operator User (access to all operations except configuration) and User Normal (access to viewing and playback only), but after creating the new user you can customize the access level as desired, for example allowing access only to certain cameras.

USERNAME/PASSWORD – Enter the credentials of the new user

AUTHORIZATION – By pressing this button you can enable and disable access to the various functions that you want to guarantee to the new user.

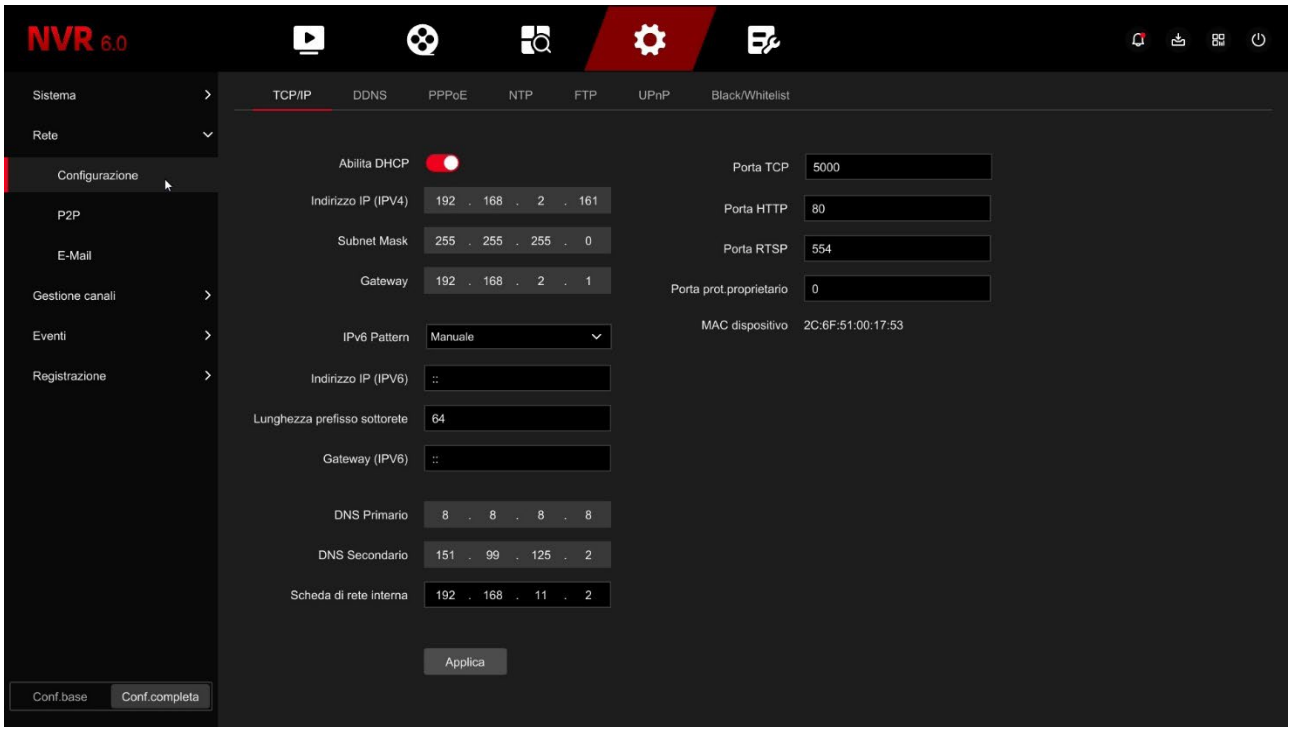

NVR 6.0
Sistema
Generale
Monitor Live
Utente
Rete
Gestione canali
Eventi
Registrazione
Conf.base
Conf.completa
Accesso Locale
Conf. Remota
Nome Utente: Mario
Livello: Operatore
Tutti
Configurazione Parametri
Visualizza log
Gestione canali
Arresto e riavvio
Aggiorname
Registrazione
Visione live
Riproduzione
Backup
PTZ
CH1
CH2
CH3
CH4
CH5
CH6
CH7
CH8
CH9
Abbandona
Salva
Autorizzazione

CONFIGURATION | NET

Click the button**CONFIGURATION then NETWORK**to open the network port settings

NETWORK | CONFIGURATION | TCP/IP

In this section you can enter the NVR network data.

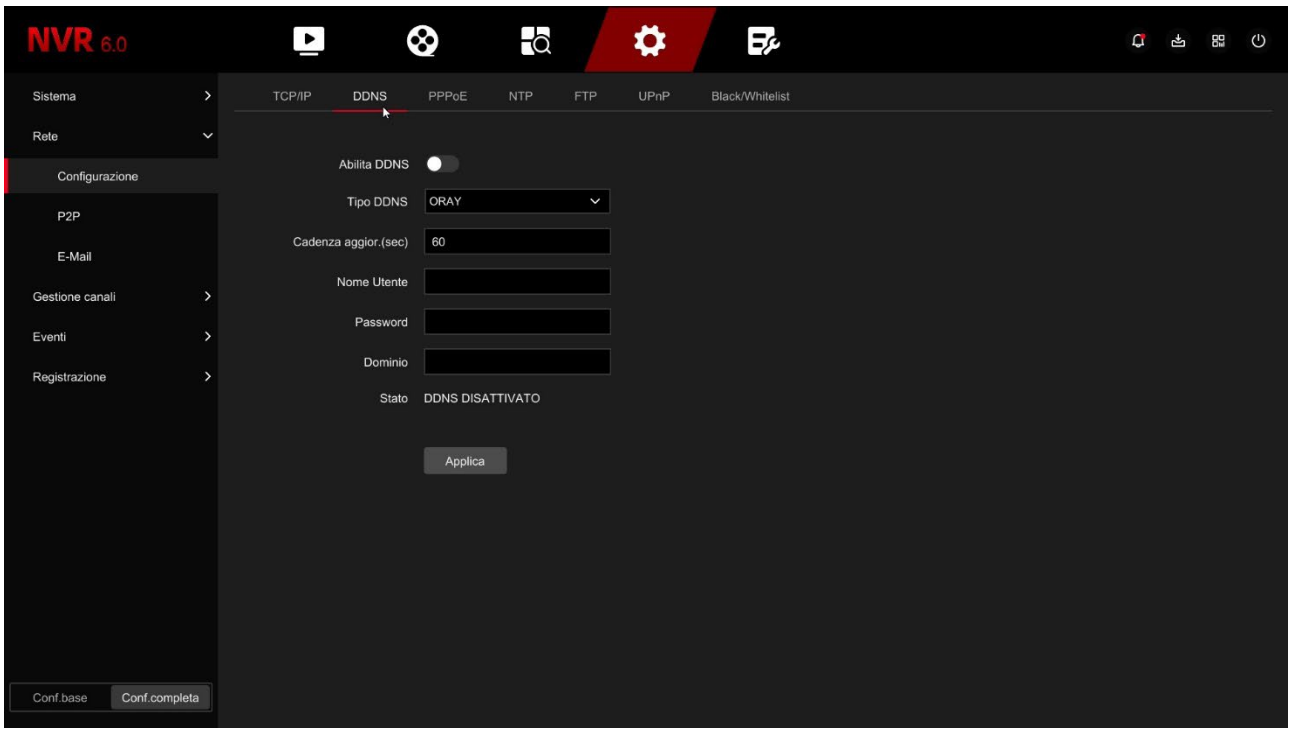


NETWORK ADDRESSES – IP address, Subnet mask, Gateway and primary and secondary DNS are the addresses that allow your DVR/NVR to communicate with the network. The easiest thing is to maintain the factory setting with DHCP enabled so that the device configures itself automatically on the network. To use this function, the DVR/NVR must be connected to a network with a router or other equipment that acts as a DHCP server.
If for some reason you have to enter the parameters manually, read up carefully before doing so because inserting incorrect parameters can make the system unreachable from the outside.
Remember that all devices on your network must have IP addresses with the first 3 numbers the same e the same subnet mask (usually 255.255.255.0). The gateway is usually the address of the router, the network number 1 (for example 192.168.1.1). DNS is important for the DVR/NVR to work browse the Internet and connect to external hosts, such as our P2P server or your SMTP provider to send emails. If you don't know your provider's DNS, use Google's 8.8.8.8.
Below is the other data in this window

IP INTERNAL NETWORK CARD – If you have purchased an NVR with built-in POE ports you can find it here the starting address that will be assigned to the cameras connected to the NVR ports. From Our POE NVRs use the class 192.168.11... for the internal network and it is advisable not to modify it.
In this window there are also the communication ports used by the camera which are not you should never change unless a specific need actually requires it.

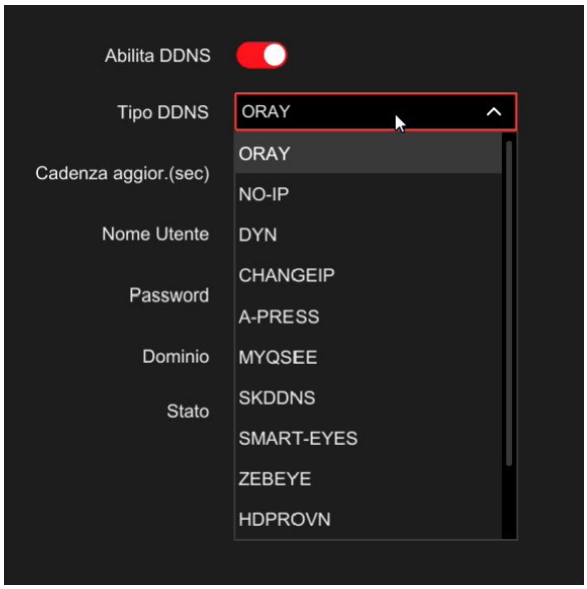
PORTS – The ports used by the NVR/DVR for network communication are indicated here in the use of TCP, HTTP (ONVIF), RTSP protocols. Our private protocol, used by the app and from the IoVedo.RK software, it uses port 6000 by default. It is advisable never to modify these communication ports.
DEVICE MAC – Unique device identifier

NETWORK | CONFIGURATION | DDNS
In this section you can enter the connection data to a DDNS server.



DDNS servers are services offered via the Internet that allow you to reach a variable IP as if it were static.
With our DVR/NVR you don't need these services because the P2P cloud server we offer free of charge performs this function very well. However VCRs support it different DDNS services and you can set the connection data in this folder if you intend to use them.

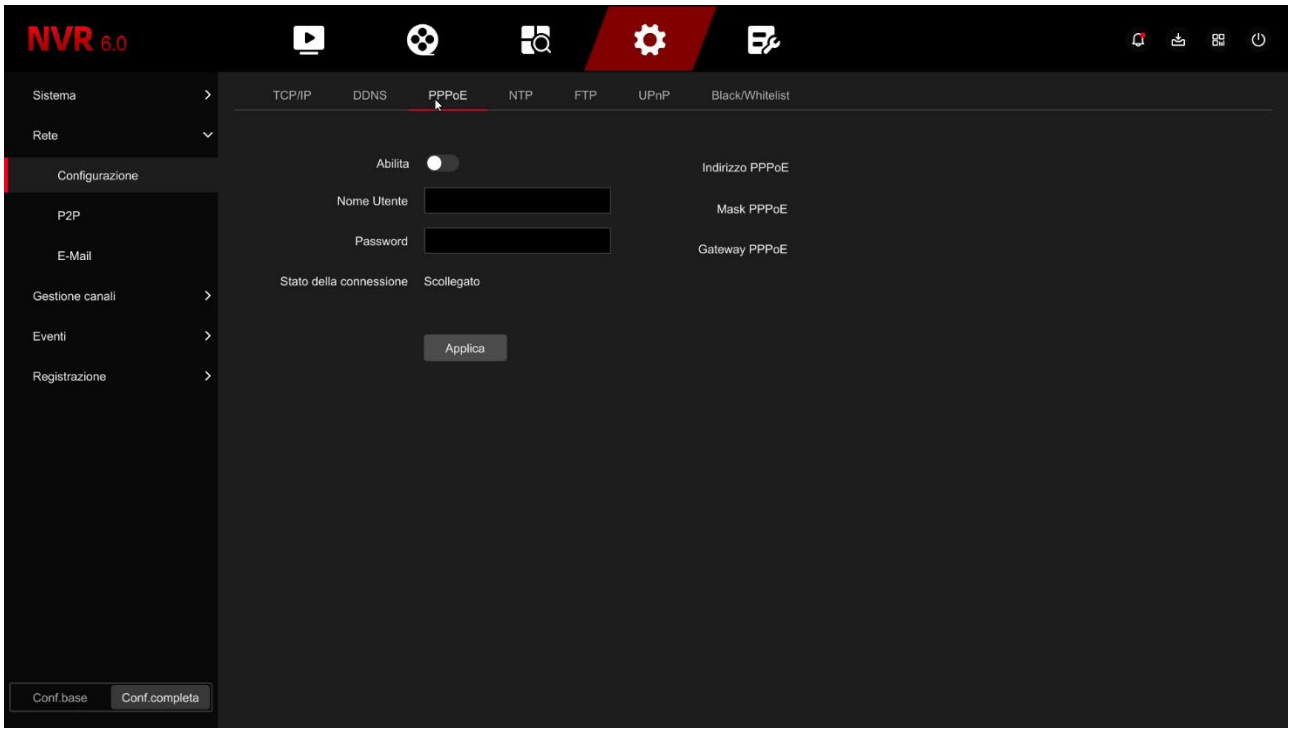
Remember that if you use a DDNS service, instead of our P2P cloud you will need to map appropriately the ports in the router to be able to communicate with the DVR/NVR.



Typically, the data required to connect to a DDNS server is the domain name and credentials and are assigned by the DDNS provider when subscribing to the service.
You can also set a refresh interval that indicates how often the DVR/NVR should perform will communicate its connection data to the server.

NETWORK | CONFIGURATION | PPPOE

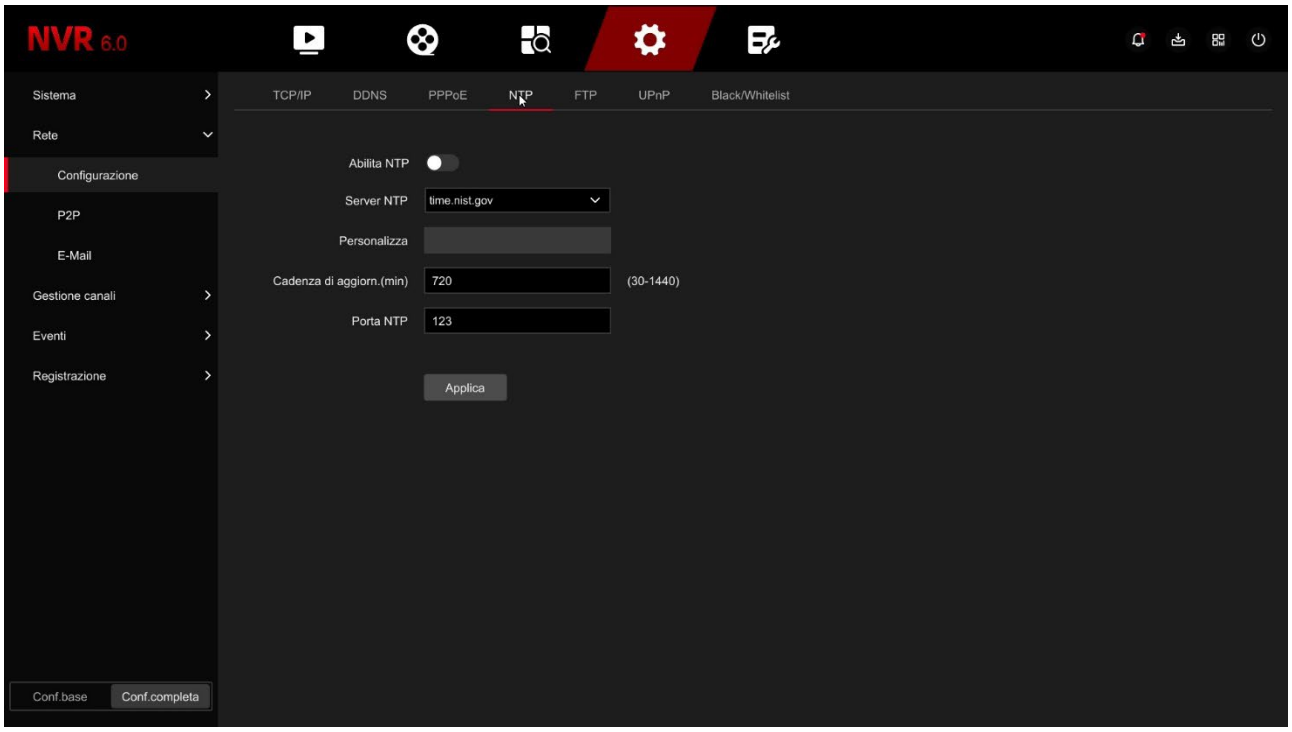
NVR/DVR can be connected directly to an ADSL modem to connect to the Internet by making a call (dial-up) and entering your credentials.



Normally you will not need this page because today it is preferred to use routers for Internet access and this protocol is not necessary

NETWORK | CONFIGURATION | NTP

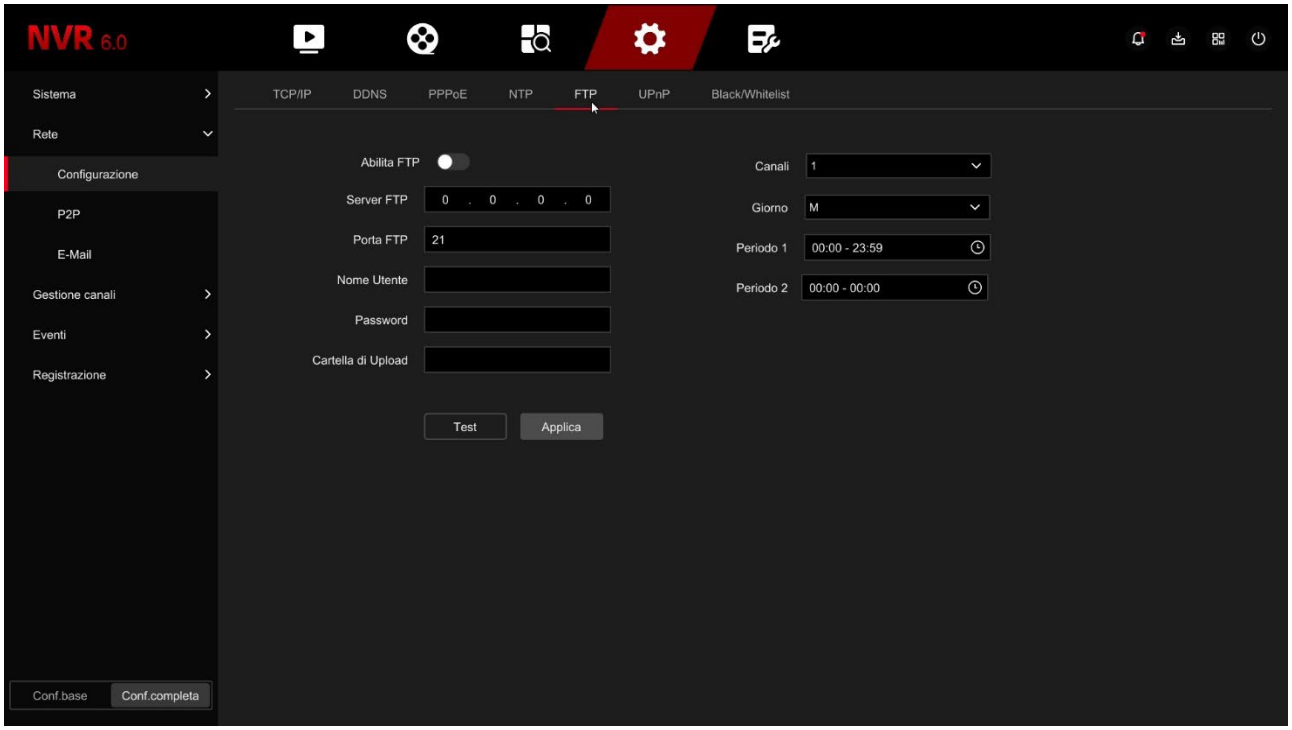
The NTP protocol is used to automatically synchronize the time of the NVR via the Internet



If you enable NTP protocol management, the NVR will synchronize the time via the Internet with an NTP server.
SERVER - You will find the most popular free servers for time synchronization listed. You can too insert a custom one.
CADENCE – Set the frequency of synchronization with the server in minutes.
NTP PORT – NTP servers normally use port 123

NETWORK | CONFIGURATION | FTP

The DVR/NVR can send photos in case of intrusion or alarm to a network FTP server. It's a useful function if you have a web space where you can secure salient images.



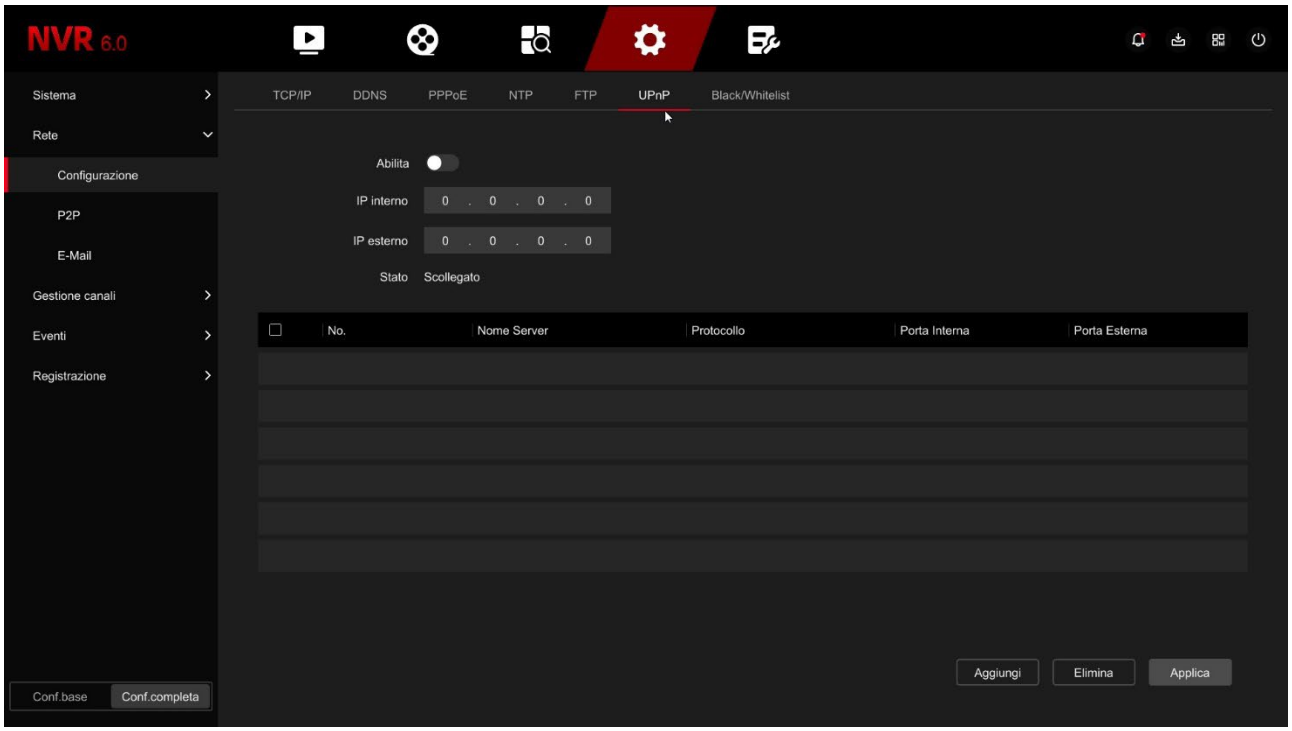
FTP SERVER/PORT – These are the main data of your FTP space
USERNAME/PASSWORD – Access credentials to your FTP space
UPLOAD FOLDER – Write the name of the folder where the files are stored on the FTP server
CHANNELS/DAY/PERIOD 1-2 – You can enable sending files only in certain time slots depending on of the day of the week. You can set different rules for each channel.
TEST – Before saving, press this button to verify that the FTP server is reachable with the parameters you entered.

NETWORK | CONFIGURATION | UPNP

If you have a static IP address on the Internet, you can also decide not to use our server cloud to connect via the web and connect directly via the Internet to the IP address of your router. In this case you must map the router ports so that the ports used by the

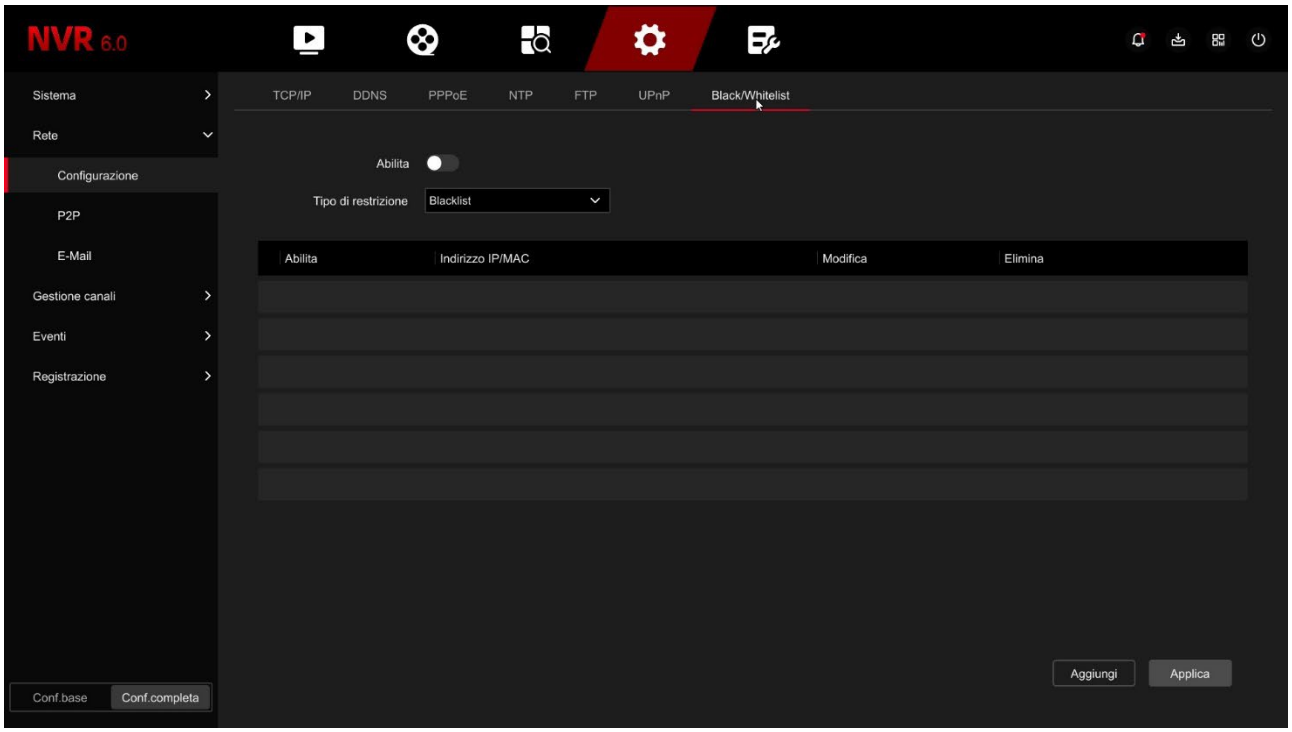
DVR/NVR (factory 80,5000,554,6000) are transferred from the Internet side to your DVR/NVR on the internal network.

It would be a good idea to do the mapping manually in the router configuration. However if your router accepts upnp mapping you can also enable it in the NVR so it runs automatically.



NETWORK | CONFIGURATION | BLACK/WHITELIST

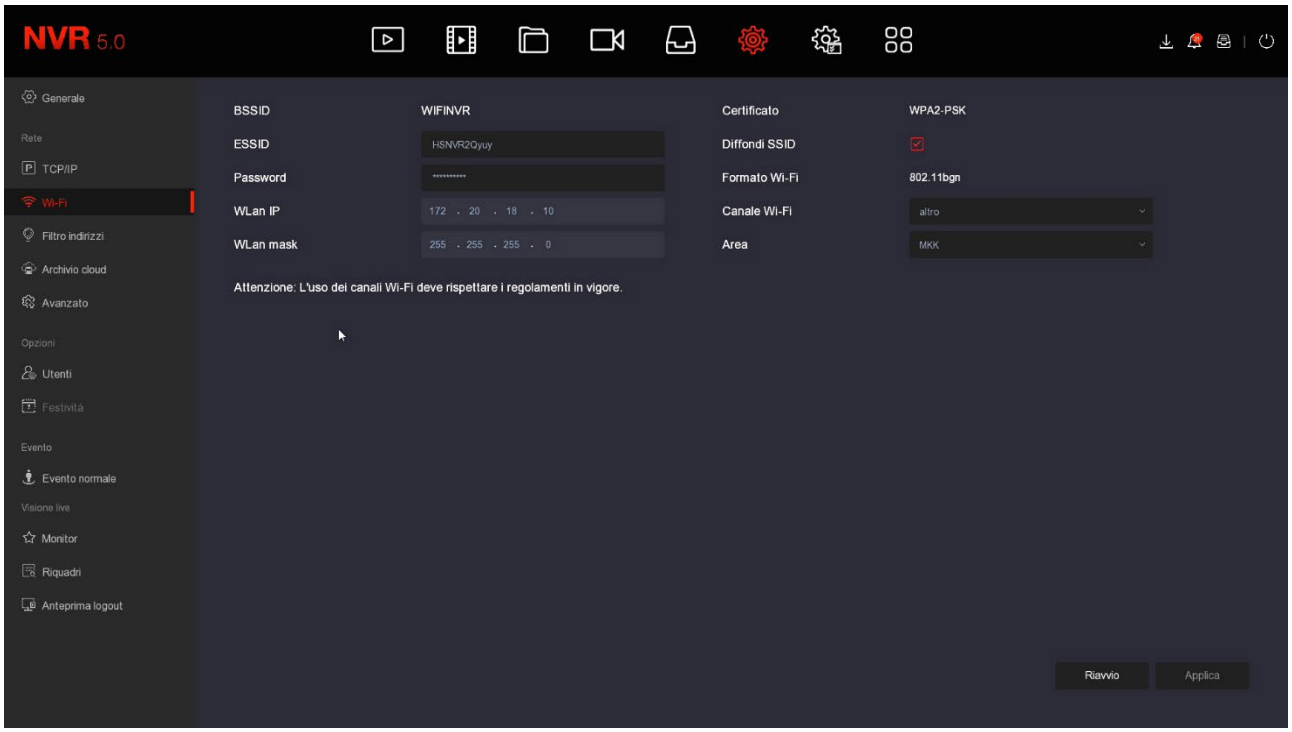
On this page you can allow or prevent remote connection to your DVR/NVR based on to the IP address or Mac Address of the client making the connection. It is useful for narrowing down the possibility of remote access to authorized IPs only.



If you use the BLACKLIST mode you can then add all the IP addresses or MAC addresses to which you do not you want to grant access to the system. If you use the WHITELIST mode you can insert the IP addresses or MAC addresses to which access is allowed, while all others will be excluded.

WIFI

This section is only present in NVRs with built-in wifi and controls the generated wifi network from the NVR.



BSSID/ESSID – It is the name that distinguishes the wifi network generated by the NVR

PASSWORD – It is the access password to connect to the NVR's WiFi network. From the factory "lspassword"

WLAN IP/MASK – Indicates the address class and subnet mask used by the NVR's WiFi network

CERTIFICATE – It is the security coding used by the NVR's wifi network

SPREAD SSID – If you disable this option the NVR's wifi network will not be visible in the search of wifi networks.

WIFI FORMAT – Indicates the WiFi technology of the NVR's WiFi network

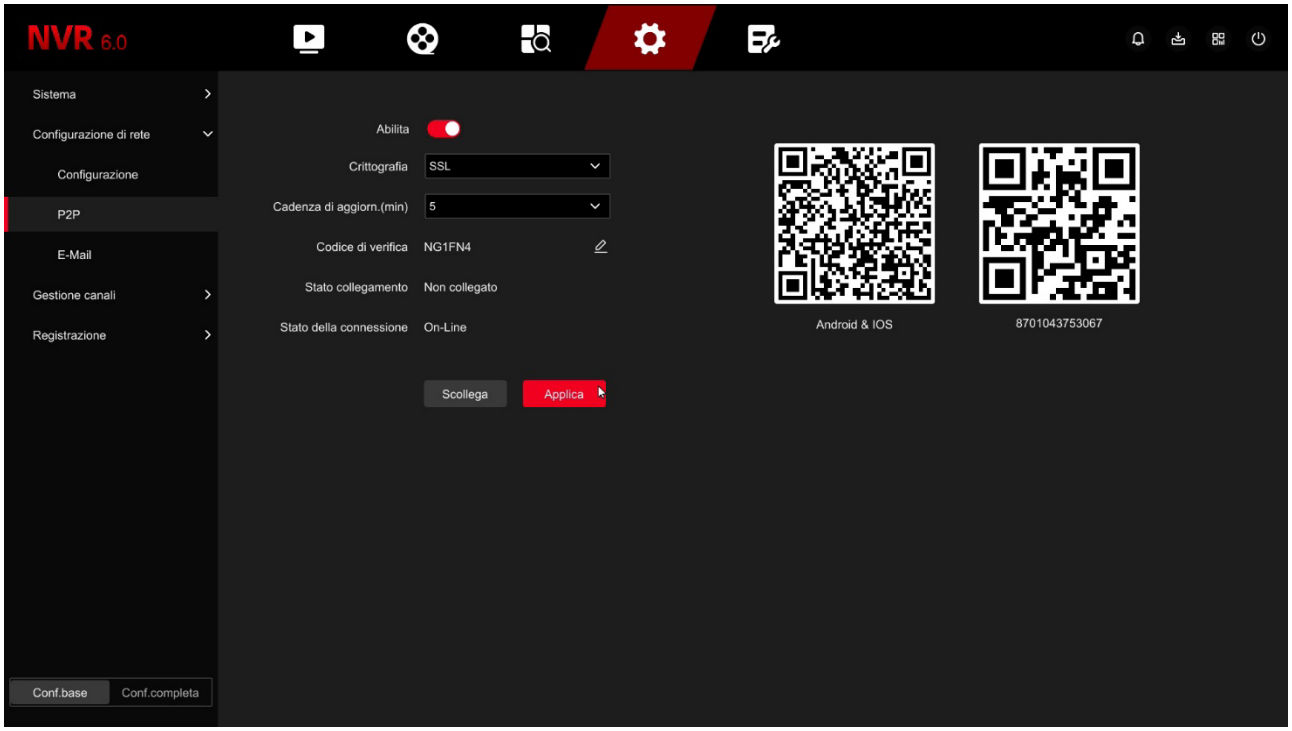
WIFI CHANNEL – Here you set the WiFi channel to use for communication with the cameras. From the factory it is best to keep the factory automatic option. However, it is possible to force it communication on a specific channel from 1 to 13. Setting a specific WiFi channel can help to avoid frequencies disturbed by the presence of other devices. If you are having problems with occasional disconnection of WiFi cameras, you can try setting different channels in this box.

AREA – Defines the WiFi standard to use. If you want the NVR's wifi network to be visible and usable by other European devices you must set EU.

NETWORK | P2P

This is a very important window because it contains the data for connecting to our server P2P cloud that allows you quick access via web with PCs and mobile phones. In the access manual remote you will find the explanation of how it works and explanations on how to use our app

IoVedo.RK



ENABLE P2P – You must enable P2P if you want to easily use the web connection with ours app and our software. If for privacy reasons you prefer that your DVR/NVR not connect to the cloud server, you can disable this function, but to connect via the web you will need an IP static on the Internet and configure your router manually.

ENCRYPTION – It is advisable to maintain the factory SSL encryption

UPDATE RATE – This is the waiting interval between sending a push notification to the app IoVedo.RK and the next. It is advisable to maintain a delay of 5 or 10 minutes to avoid receive too many notifications and to avoid exhausting the maximum number of 100 notifications/day per channel expected.

VERIFICATION CODE is the captcha code used to upload the device to our site IoVedo.RK app. If you do not enter anything in this box, the captcha code to use in the app will be the factory one that you find on the product label. If you want you can customize the code captcha of 6 letters/numbers by typing it in this box. If you want the appliance can be added to the app without requiring the captcha, enter the code ABCDEF in this box.

LINK STATUS - shows if the device has already been linked to an account on the app IoVedo.RK. If the device is linked to an account, you can unlink it with the UNLINK for button re-pair it to a different account.

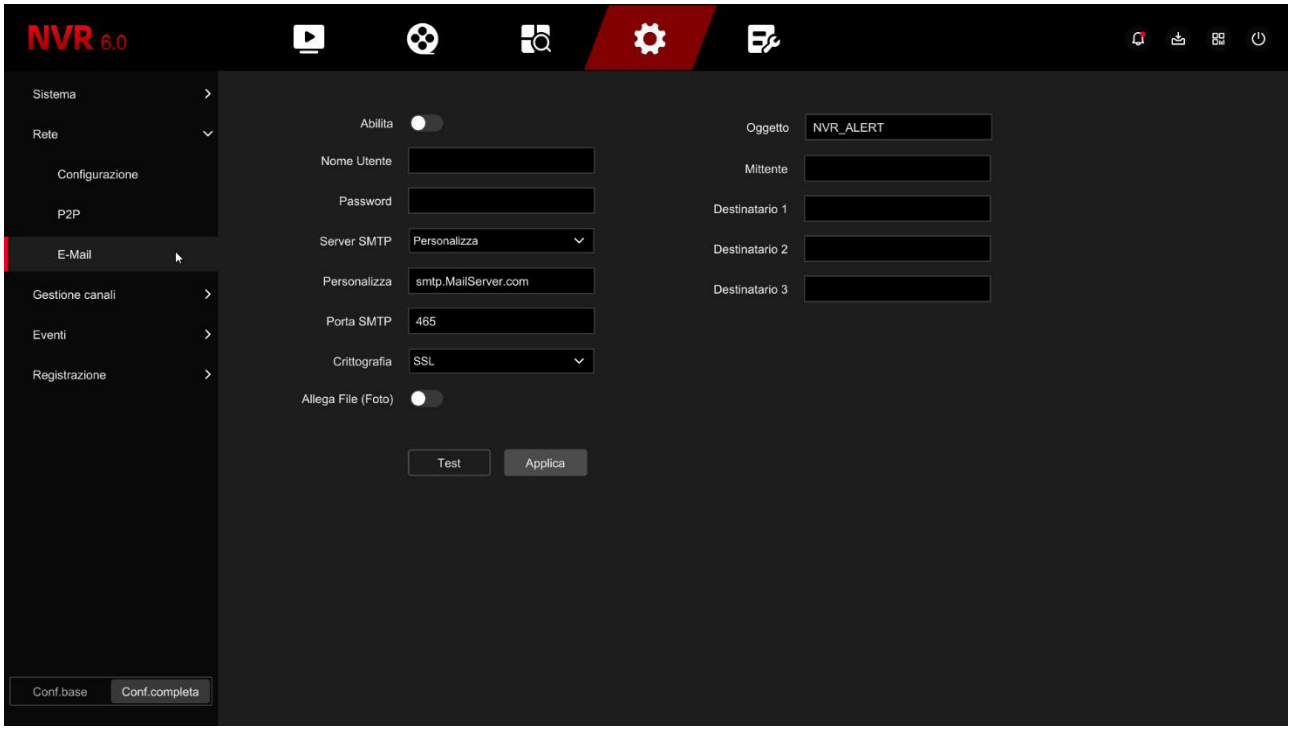
CONNECTION STATUS – shows the connection status to the P2P server.Connected, It means the system is connected to our P2P server successfully.Disconnect indicate instead you can't connect remotely to the cloud because the NVR doesn't see the Internet.

Always check the status of your cloud connection before trying to connect via the Internet.
If the server is offline, the most likely thing is that the network settings of the DVR/NVR are incorrect
are correct. Then enable the DHCP function in the network settings and restart the device, in
so that the DVR/NVR automatically receives the correct settings from your router. Then
double check in this section if the P2P server is connected.
QR CODE – The first QR code on the left can be scanned with your mobile phone to download the APP
IoVedo.RK for iOS or for Android. The second QR code is instead used in the app configuration
to quickly load the DVR/NVR serial number. This serial number consists of
13 numbers and identify your DVR/NVR in our cloud server. It is also written under the QR Code,
if you need to enter it manually. The QR code is also shown on the label
self-adhesive under the video recorder and on the packaging.
UNLINK - If your device is linked to an app account that is not yours, for example del
previous owner, you can disconnect it with the UNCONNECT button to be able to recharge it in yours
account.

IPEYE is not used

NETWORK | E-MAIL

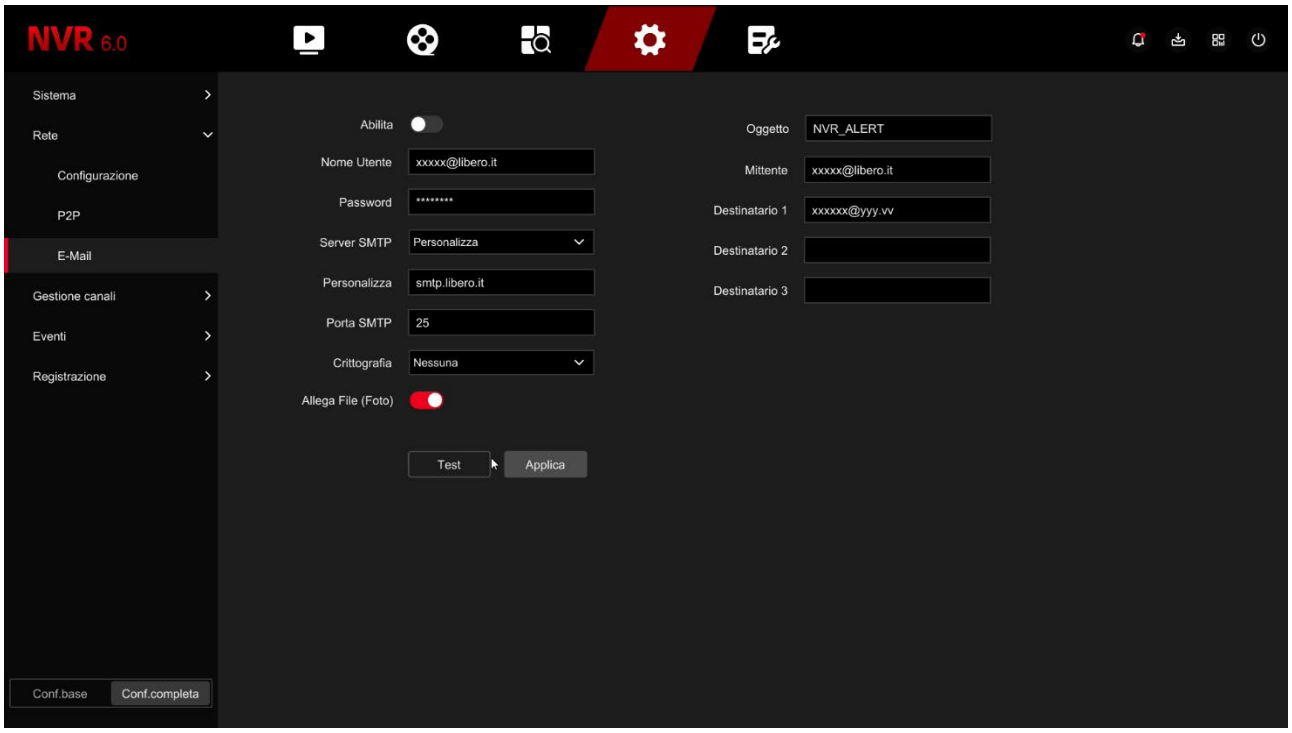
In this section you can enter the data necessary to have your NVR/DVR send messages
email in case of alarm. You must consult your email provider to find out which data
enter in order to communicate correctly with the SMTP outgoing mail server.



USERNAME/PASSWORD – These are your login credentials, to be used if your provider requires authentication on the SMTP server
SMTP SERVER/SMTP PORT – These are the main data to be able to communicate with your SMTP server for sending e-mail and the provider of your e-mail account must provide them to you.
ENCRYPTION – Several providers use encryptions in the SMTP protocol. It is essential to insert here is the encryption used by your provider (SSL or TLS). Note that mail providers often have of different access methods, with different settings based on the encryption used.
ATTACH FILE – If you want to attach the photo to the alarm email, enable this option.
SUBJECT – Type the subject you want to appear in the alarm email
SENDER – Enter the name and email address you want to appear as the sender of the email.
alarm sent by the DVR/NVR
RECIPIENTS – You can enter here the recipients to whom the email will be sent in the event of an alarm. You can enter up to 3 recipients.
TEST – Before saving, do a test send with this TEST button.

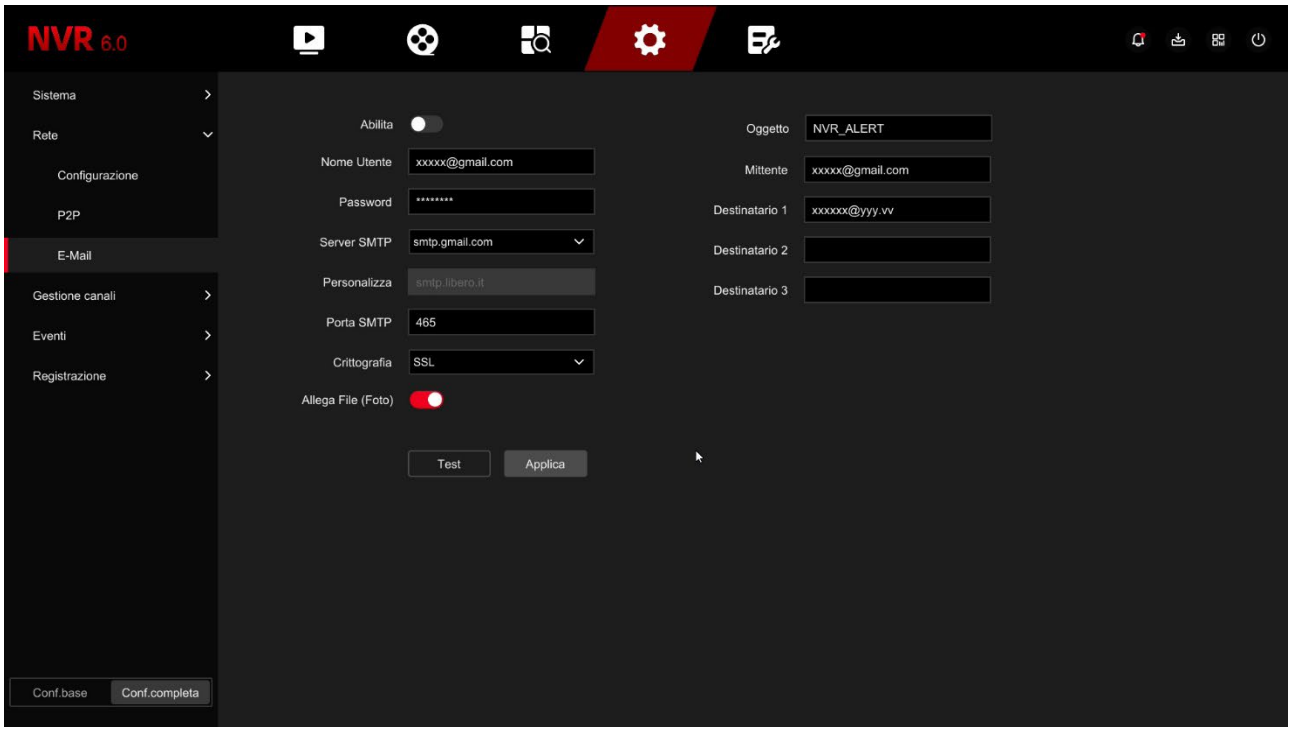
If the test fails, do not contact our support thinking that the device is not working.
Remember that sending emails depends only to a small extent on the NVR and largely on the your smtp provider. It's important to use the correct parameters for your provider and sometimes you even have to set up features in your inbox settings to allow sending
emails from devices considered unsafe.

Below is an example of an effective configuration that you can achieve by creating a free account on**LIBERO.IT**and using their SMTP server without encryption on port 25.

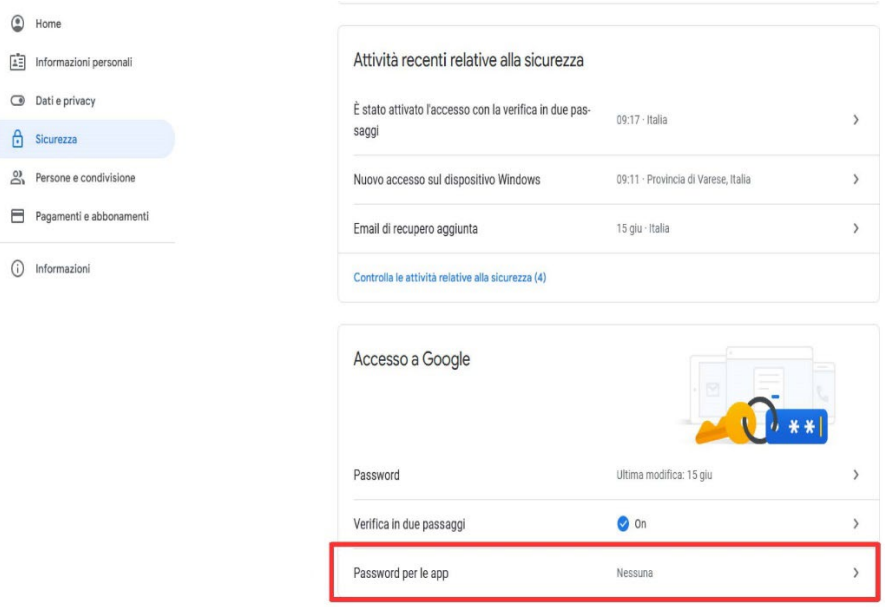


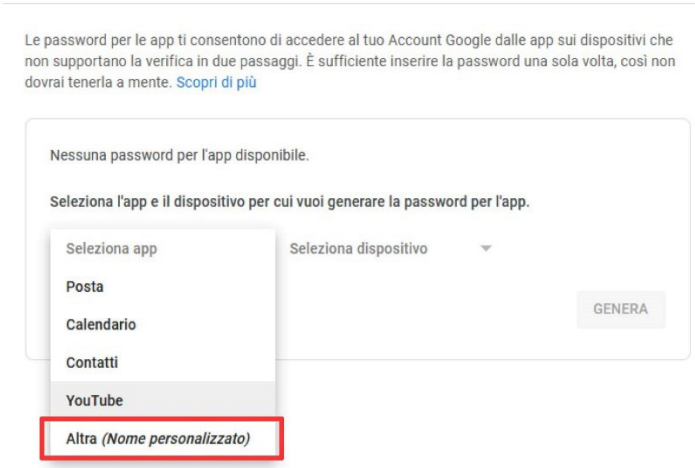
The widespread provider**GMAIL**It can be used to send emails from automatic devices such as NVRs and DVR, but requires a more complex procedure to bypass double authentication than NVRs they cannot perform.

Here is the gmail configuration on the NVR side



To be able to use gmail it is not enough to set up the NVR, you also need to access the security settings of your gmail account and generate a so-called PASSWORD FOR APP





Once you have the special app password you will need to use it in the NVR's email panel

ADVISE

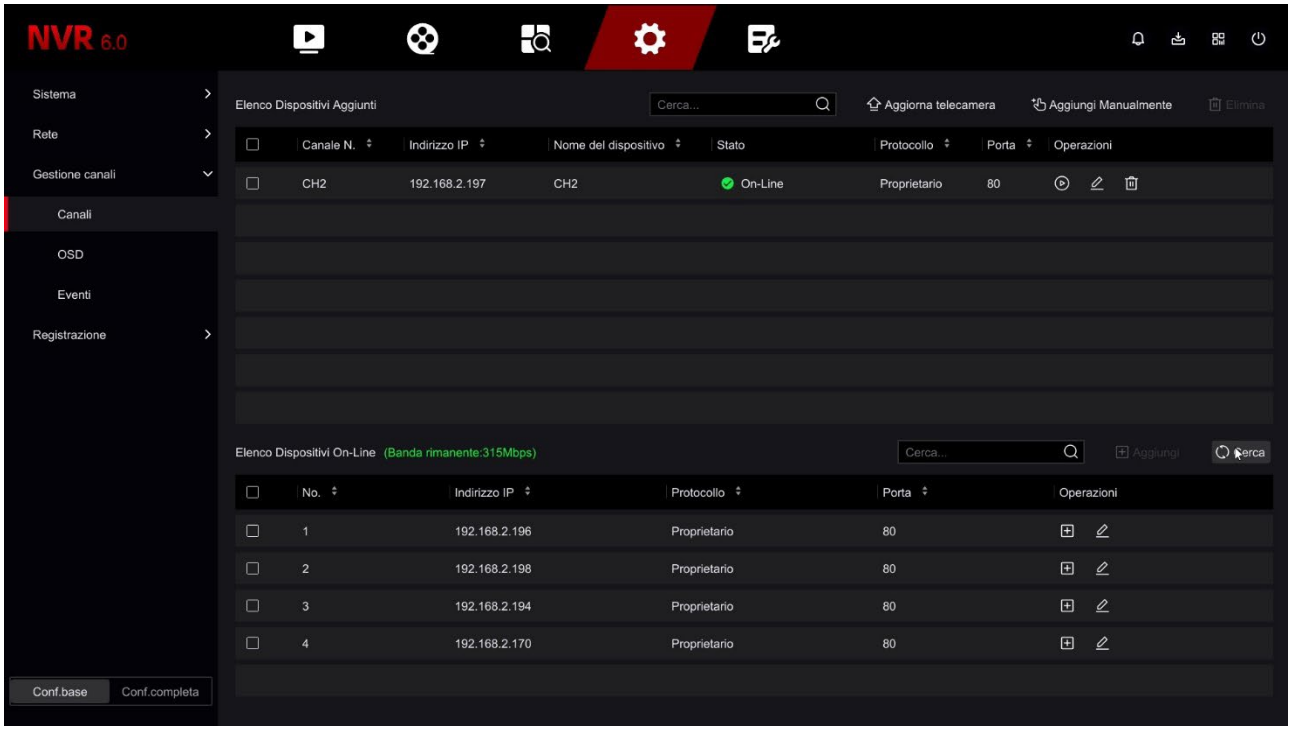
If you can't find success with your regular smtp provider, don't go crazy trying to correct settings for that provider. You can try other free accounts online, such as libero.it or email.it. You don't necessarily have to use their POP3 mailbox to receive emails, but you can limit yourself to only use SMTP for sending.

CONFIGURATION | CHANNELS

Click the CONFIGURATION button then CHANNEL MANAGEMENT to configure the cameras

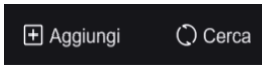
CHANNELS

In this section you can upload IP cameras and configure channels

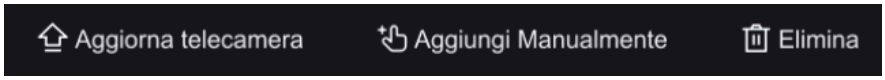


In this section you can add IP cameras to your NVR/DVR.

ATTENTION: The procedure for**adding IP cameras to your video recorder is explained in the installation manual**and use the SEARCH button to activate the search for network cameras that appear in the lower table, and the ADD button, to connect the camera to the NVR. See details in the installation manual.



This manual describes the other commands in the section

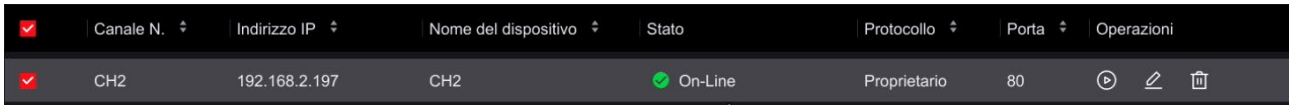


UPDATE CAMERA – With this button you can update the firmware of one or more cameras with a DSE update file that must be copied to a connected USB stick

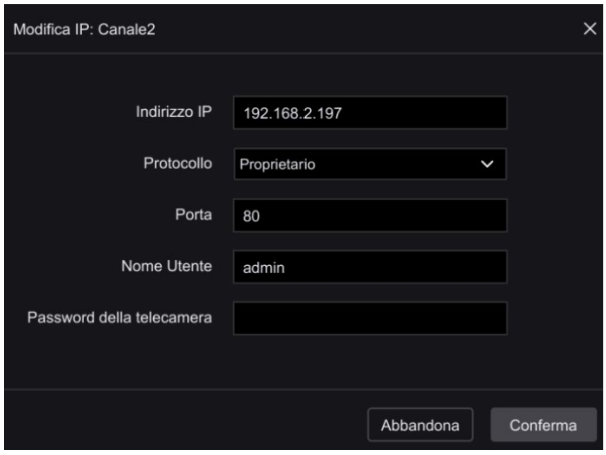
to the NVR.

ADD MANUALLY – Allows you to enter the data of a new camera manually
when it is not possible to use the network search function, for example to connect a
camera connected to another network or via the web.
DELETE – Delete the selected cameras, freeing the corresponding channels

The channel table includes various indications and commands



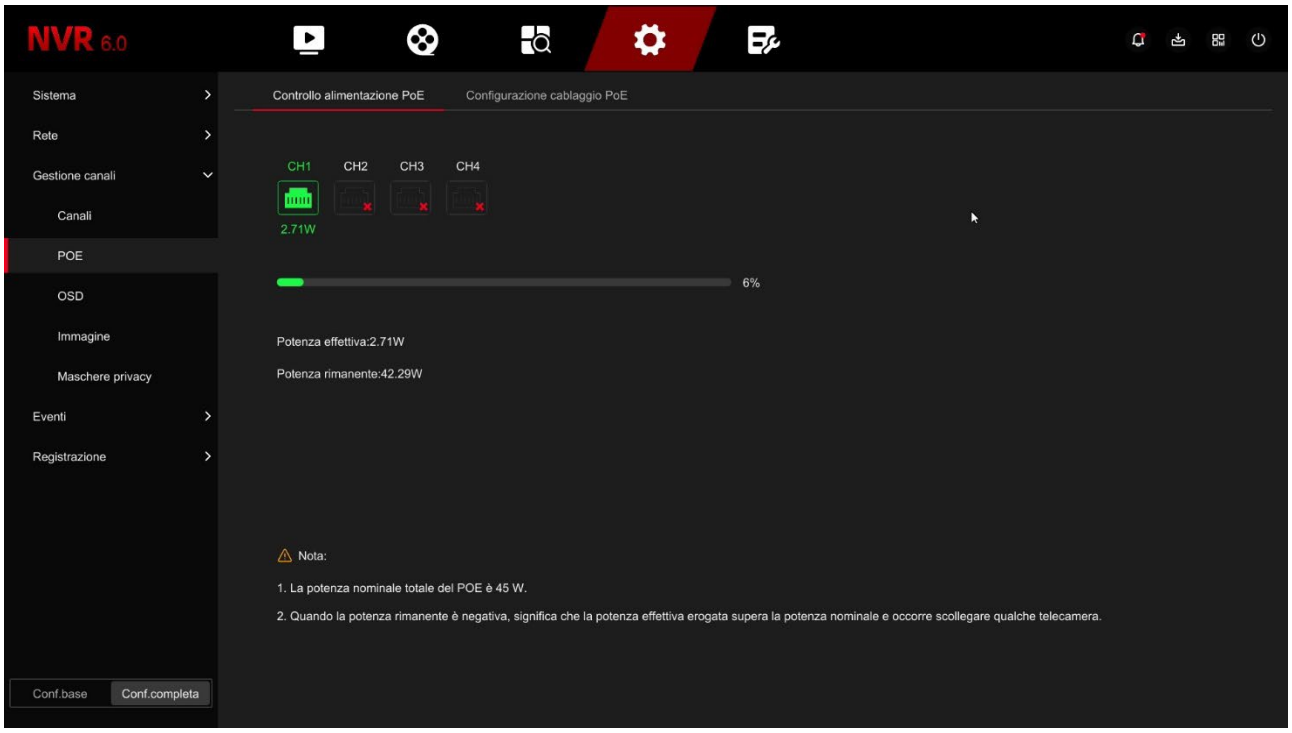
CHANNEL/ADDRESS/NAME – Data of the channel and the connected camera
STATUS – Shows a yellow triangle if the connection is not in progress or a green dot if it is
camera is connected.
PROTOCOL – Indicates the protocol used to communicate with the camera. It is normally used
the Proprietary protocol with our cameras and the Onvif protocol for other cameras
brand.
PORT – Indicates the communication port used to communicate with the camera
PLAY ICON – Shows the camera video in a preview pane
EDIT ICON – You can manually edit the camera connection data



DELETE ICON – Delete the camera and free the channel

POE | POE POWER CONTROL

This section is only available in NVRs with integrated POE ports.



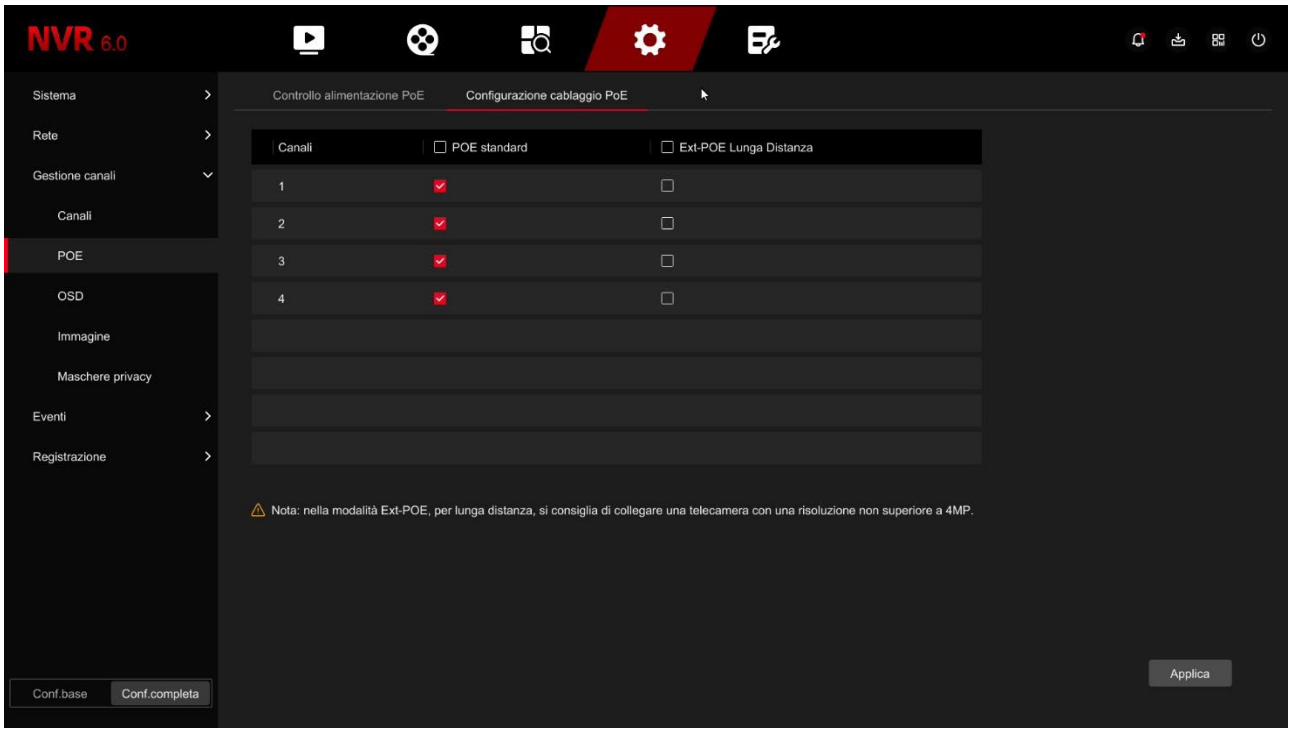
Shows the status of the ports which are colored green if the camera is connected with the indication of the power absorbed by each camera and the total power delivered and residual of the NVR

POE | POE WIRING CONFIGURATION

This section is only available in NVRs with integrated POE ports.

This section allows you to permanently connect the physical inputs of the POE ports, located on the back of the NVR, to channels 1-4, 1-8 or 1-16 of the NVR. NVRs with POE ports have this connection active at the factory so that port 1 is reserved for channel 1, port 2 for channel 2 and etc.

In this factory configuration, for example, the NVR has 4 POE ports. Channels 1 to 4 are matched to the NVR ports so any external cameras will be inserted from the 5 in. channel after you.

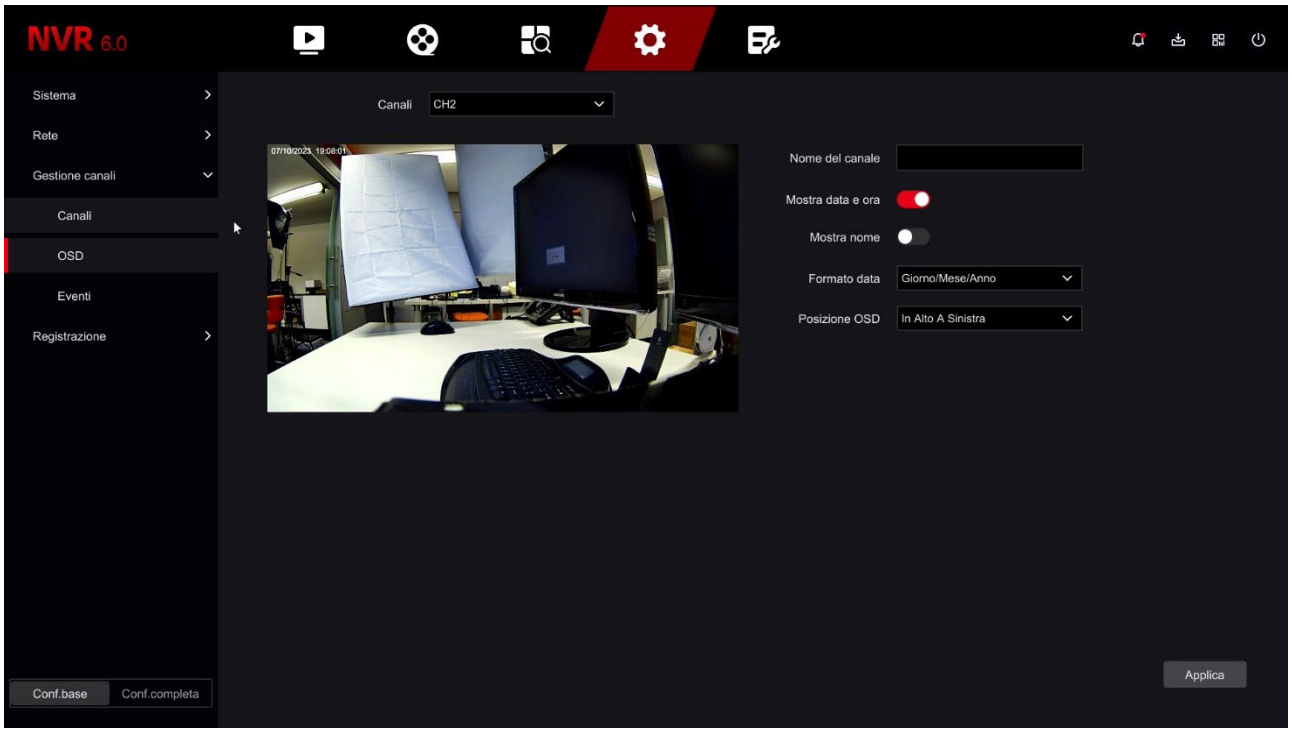


If you connect the cameras only to the NVR ports you can maintain this factory setting.
If instead you connect some cameras to the POE ports of the NVR and others externally on the network, then You should disconnect the POE ports that you don't use in order to have these channels available for external cameras. For example, if you uncheck POE on channels 3 and 4, POE ports 3 and 4 will not connect. they will no longer be able to use. Channels 1 and 2 will remain reserved for POE ports 1 and 2 while any external cameras will be placed starting from channel 3

This page also allows you to choose the type of POE cabling to use for the cameras connected to the POE ports
STANDARD POE – Enables standard POE power on the port which allows cabling up to 100 m. with maximum bandwidth 100MB
EXTENDED POE LONG DISTANCE – Enables Extended POE power on the port allows wiring up to 250 m. with maximum bandwidth 10MB. Use this option only for cameras with long cabling, exceeding 100 metres.

OSD

In this section you can define the screen overlays for each camera.
This is a feature you can useonly with analog cameras orwith ours RK Series IP cameras connected with PRIVATE protocol (not Onvif) . With other IP cameras you have to set the overlays directly in the camera's internal menu.



You can overlay the date and time (SHOW DATE AND TIME), choosing the date format, and also the camera name (SHOW NAME), which you type in the box at the top CHANNEL NAME.

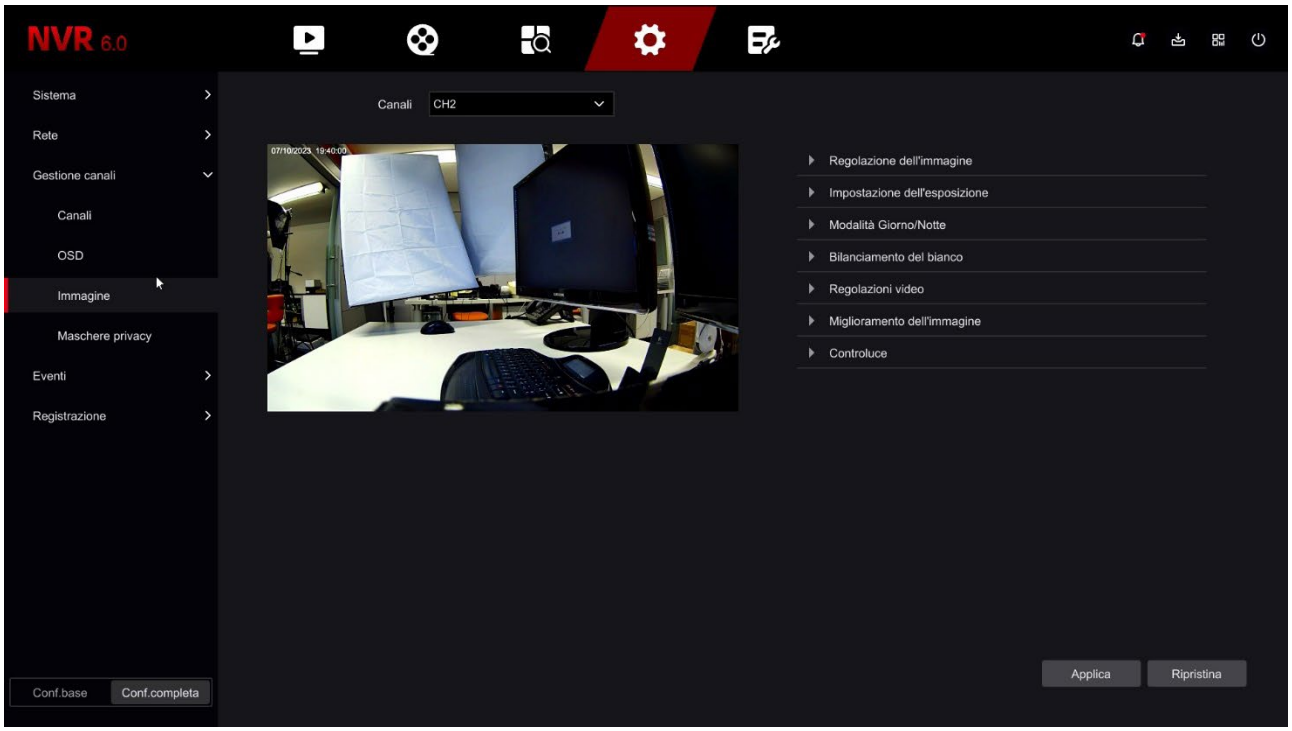
The position of the overlay can be chosen in different positions on the screen (OSD POSITION).

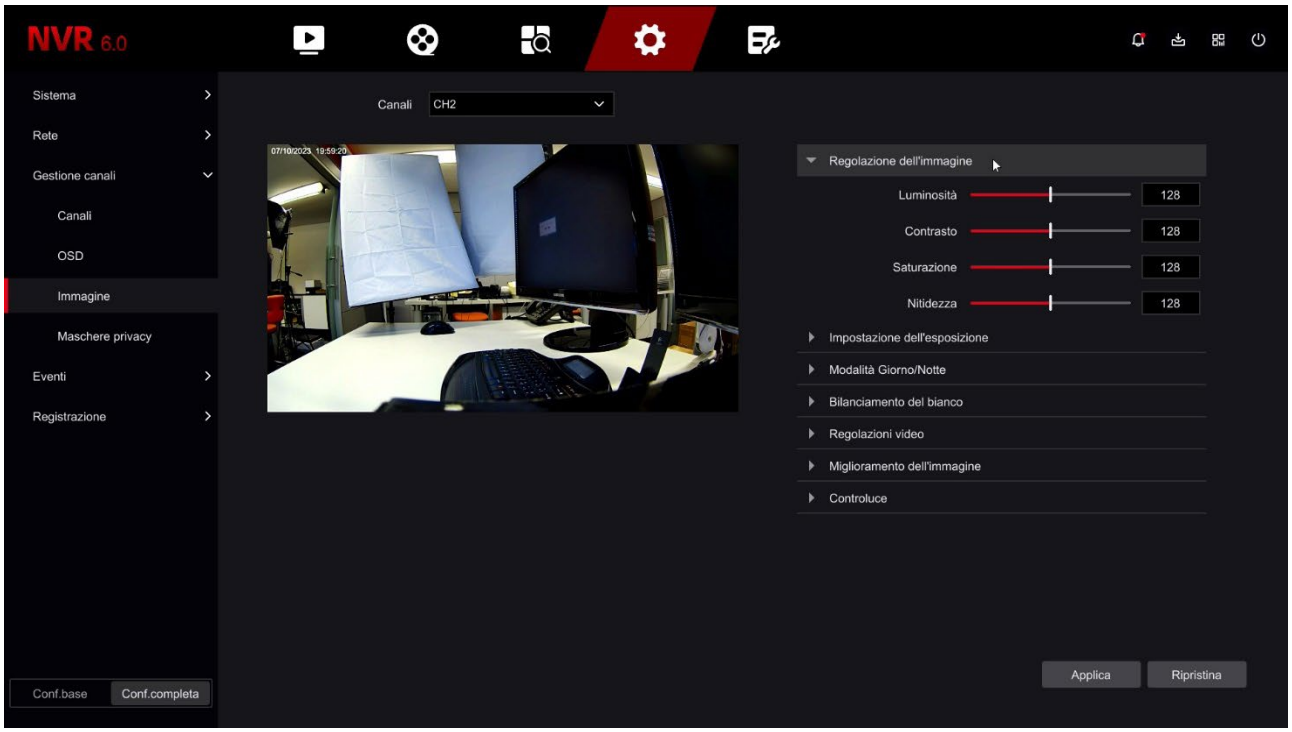
IMAGE

In this section you can adjust the cameras image parameters to compensate

less than perfect environmental situations. First choose the channel on which to operate in the box above, then act on the adjustments by checking the effects of your changes directly in the preview.

If you connect one of our RK series cameras via the private protocol you can adjust all the internal image options of the camera, while with different IP cameras or with cameras analogue you can only adjust the basic parameters

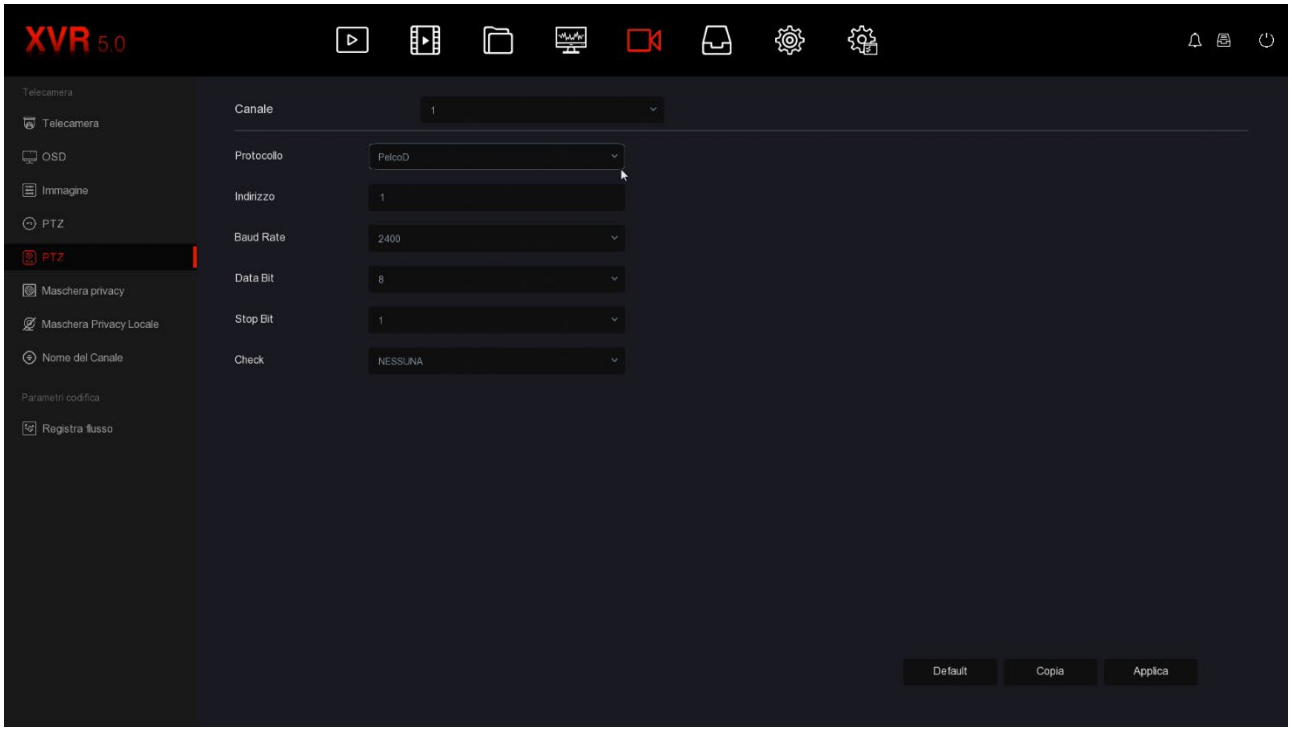




The settings available in this menu depend on the camera model. For the detailed explanation of all the adjustments refer to the configuration manual of the camera.

PTZ

In this section you can set the communication protocol to use for the command analog motorized cameras. It is a section that you only find in our DVRs with BNC inputs because it is only relevant for analog PTZ cameras and does not concern IP cameras.



You can choose PelcoD, PelcoP, UTC protocol

PelcoD – It is used for all DSE motorized cameras that are controlled via the door RS485 serial port on the back of the DVR. Address, Baudrate, Data Bit, Stop Bit and Parity Check must be the same as those set in the camera. The most common baud rate values are 2400 e 4800 baud. Each camera has its own address which generally starts from the number 1 which is factory set in the cameras.

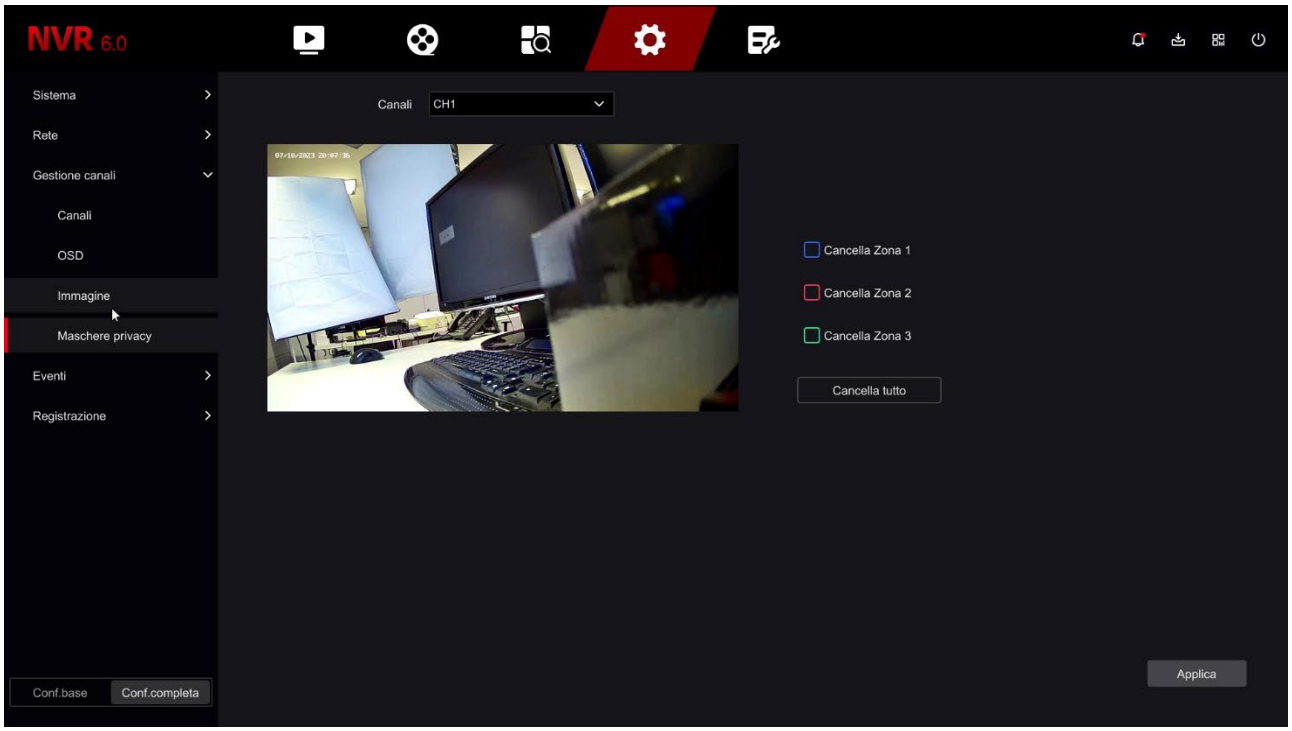
PelcoP – Another variant of the PelcoD, to be used with cameras from other manufacturers

UTC - The UTC protocol is used to control the latest analog cameras which, thanks to this protocol, they are able to receive commands along the video cable, without the need for additional control pair. It is the protocol enabled by default on all analog channels, with which you can control the cameras OSD menu, motorized zoom and even movements of motorized cameras that support this protocol. With the UTC protocol you don't have to set any communication parameters.

PRIVACY MASKS

In this window you can draw up to 3 masking areas in the image with the mouse darken areas to protect privacy. Typically this function is used to darken areas outside the property.

This is a feature you can useonly with analog cameras orwith ours RK Series IP cameras connected with PRIVATE protocol (not Onvif) . With other IP cameras you need to set privacy masks directly in the camera settings.

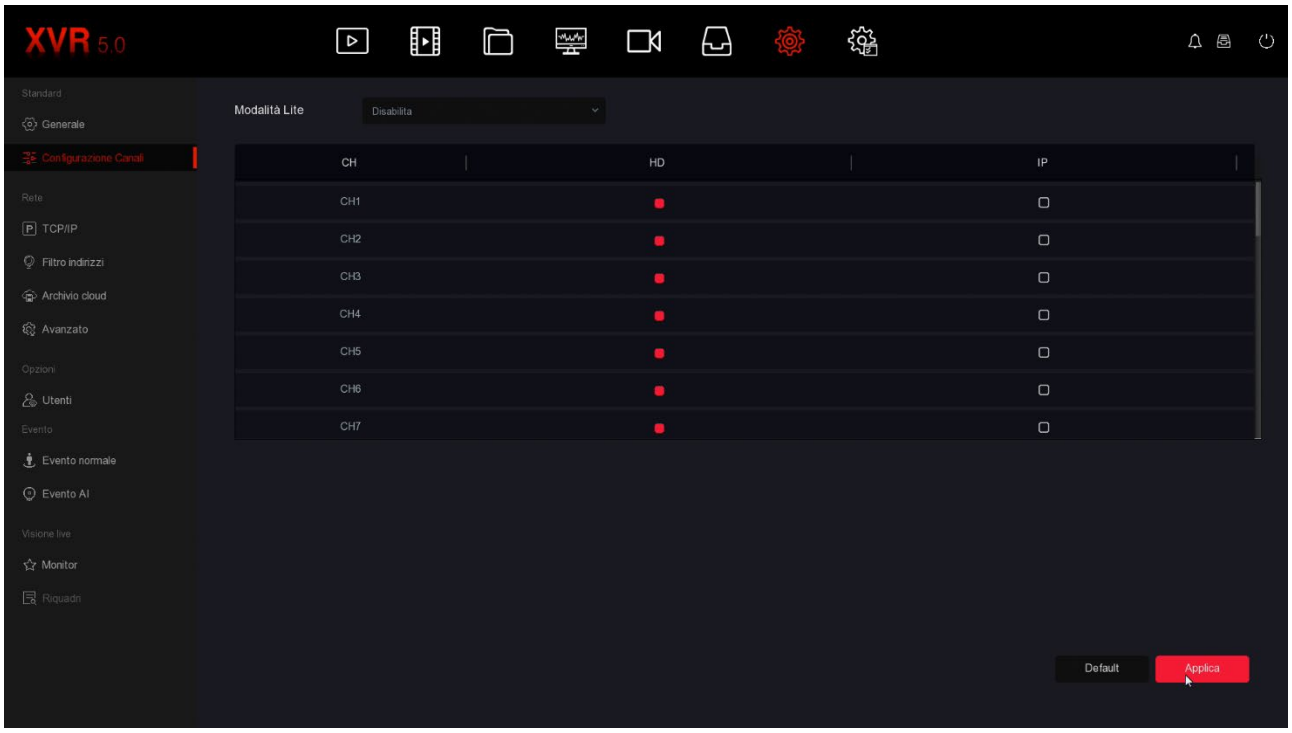


Choose the channel to operate on in the top box and then draw the mask directly on the preview. You can define up to 3 rectangular privacy masks. If you are not satisfied use i DELETE commands.

In some analog DVRs you can insert two different types of masks: the standard masks and the local masks. Local masks are masks that only appear in live viewing while the recording is not masked.

CHANNEL CONFIGURATION

This section is only present in DVRs with BNC inputs that can manage both cameras analogue and IP.



The DVRs in this range are supplied from the factory with all analogue channels enabled so as to be able to use all the rear BNC inputs.

In this window you can decide to disable one or more analog inputs to enable some IP inputs. If you uncheck an analog input you will automatically see a certain one activated number of IP channels.

If you disable an analog channel (HD) the related BNC will be deactivated.

Normally you can disable BNC inputs in pairs.

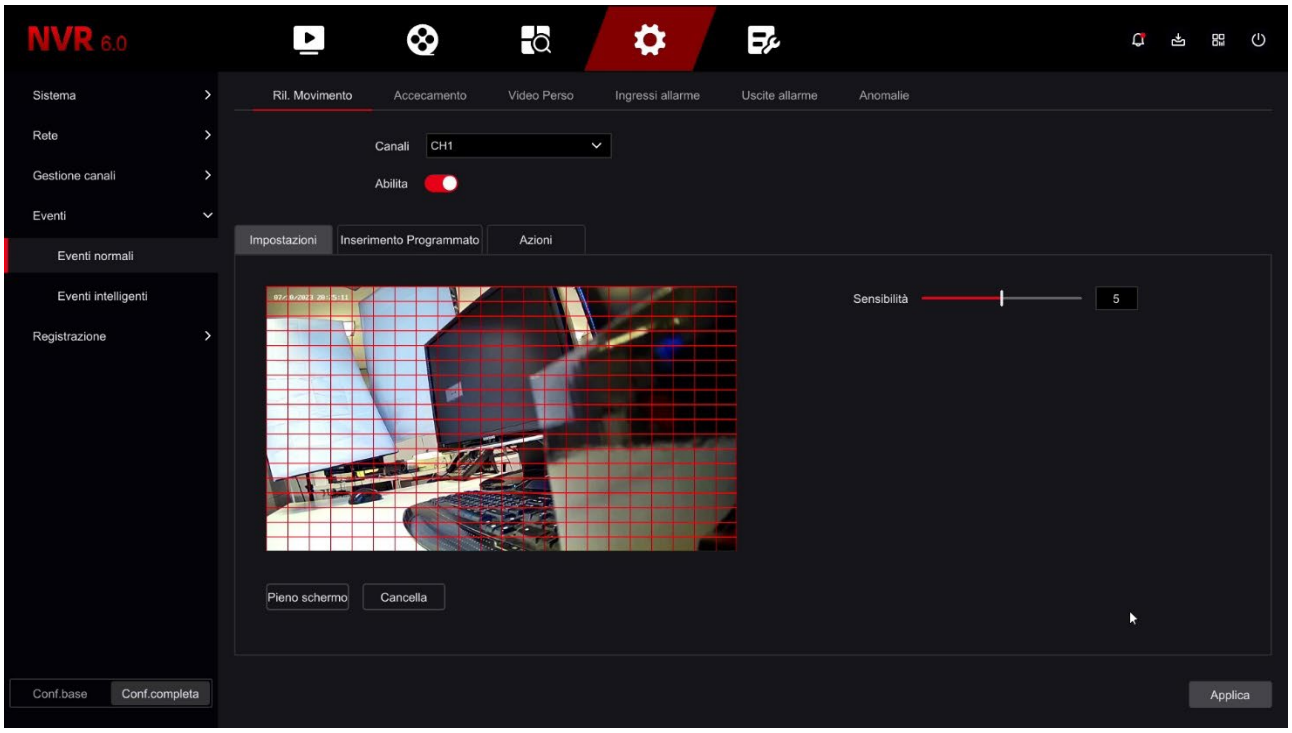
LITE MODE – You can enable lite mode if you want to increase the frame rate slightly of the footage, both live and recorded, reducing the resolution a little. Usually this option is not convenient, but can be interesting if you shoot moving targets fast to increase the fluidity of the video.

CONFIGURATION | EVENTS

Click the CONFIGURATION button then EVENTS to configure the camera detections.
Note that in analog DVRs intrusion detections are made by the DVR while in
IP cameras the detections reside in the camera and when you configure the detections in the NVR
these will simply transfer them to the cameras. In this section EVENTS are configured only
the rules of the surveys while how and when to record is defined in the next section:
REGISTRATION

NORMAL EVENTS | MOVEMENT DETECTION

In this section you can activate the motion detection function, also called: motion detection.



Motion detection is a very useful function that allows the DVR/NVR to record only when an intrusion occurs, thus saving a lot of disk space.

It also allows you to send push and email notifications. If you use motion detection, in addition to obtain a much higher storage capacity, you will also have greater ease in consult the video history because you will see at a glance the moments in which errors occurred significant events and you won't have to scroll through long periods of empty environments, as happens with the continuous recording.

The use of motion detection is generally advisable, but it also has disadvantages. You can not use motion if the subjects remain still for a long time (in motion detection the recording would stop) or in framing situations where motion detection is not possible can be regulated effectively. You also have to consider that if you record in motion you might lose recordings where the subject is very far from the camera or in a corner of the frame.

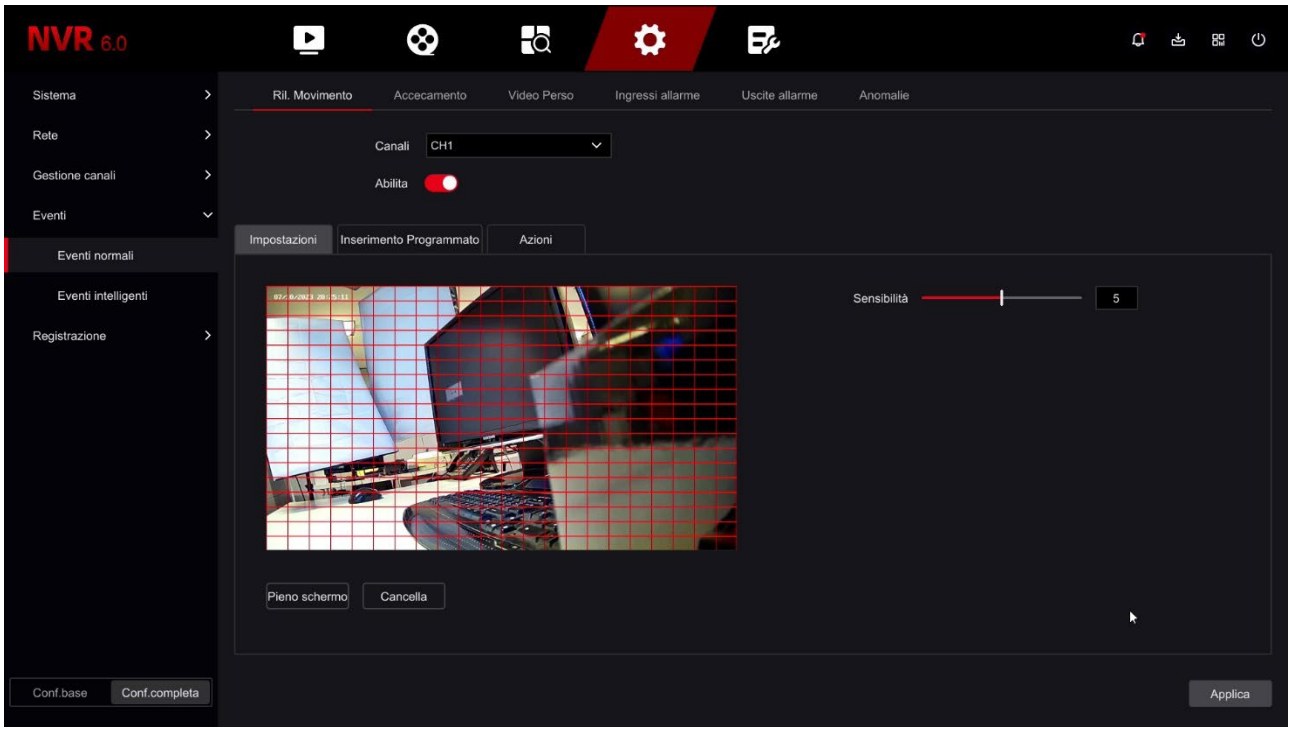
Motion detection is not considered intelligent detection because it senses any type of image modification, regardless of what generates it.

Also remember that to have the most effective detection possible you will have to carry out several tests to find the right compromise between high sensitivity and false detections.

UNDERSTANDING MOTION ADJUSTMENTS IN IP CAMERAS

In analogue cameras all motion detection functions are carried out by the DVR. In IP cameras, however, no. In IP cameras the detection function is performed by the camera, while the NVR only carries out the alarm actions resulting from the detection. It follows that When you configure motion detection from the NVR, the detection settings, such as enabling, the area and sensitivity are sent to the camera to be put into practice. Our NVR can send these adjustments only to our RK Series cameras, connected with private protocol. With cameras from other manufacturers, the NVR may not be able to control these parameters (Area, Sensitivity and Enablement) remotely and in this case**you will have to set these functions in the camera menu, connecting with the browser**directly to camera.

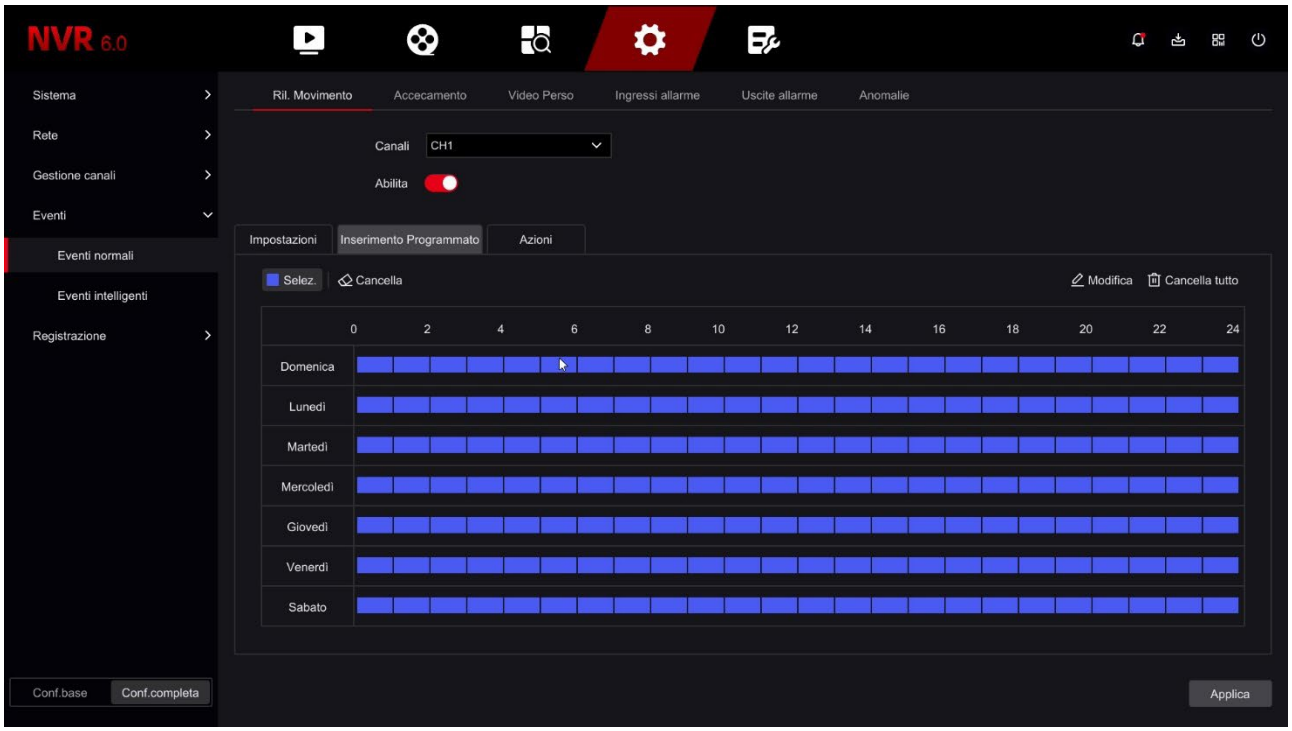
Now let's see how motion detection is configured, option by option.
Remember that in this EVENTS section you can only adjust the detection options, while **you must set how and when to register in the REGISTRATION section**.



CHANNEL – You can activate motion detection differently for each camera. You do be careful not to underestimate this box, because each channel has a schedule different, soyou have to individually configure all channels one by one.
ENABLE – Check this option if you want to use motion detection on the selected channel. Note that you should not enable motion detection on a camera where you plan to enable intelligent detection functions. If after some tests you have the impression that this

motion adjustment is not effective is because your camera requires you to perform it directly in the camera menu and not through the 'NVR.
You have 3 configuration tabs available.

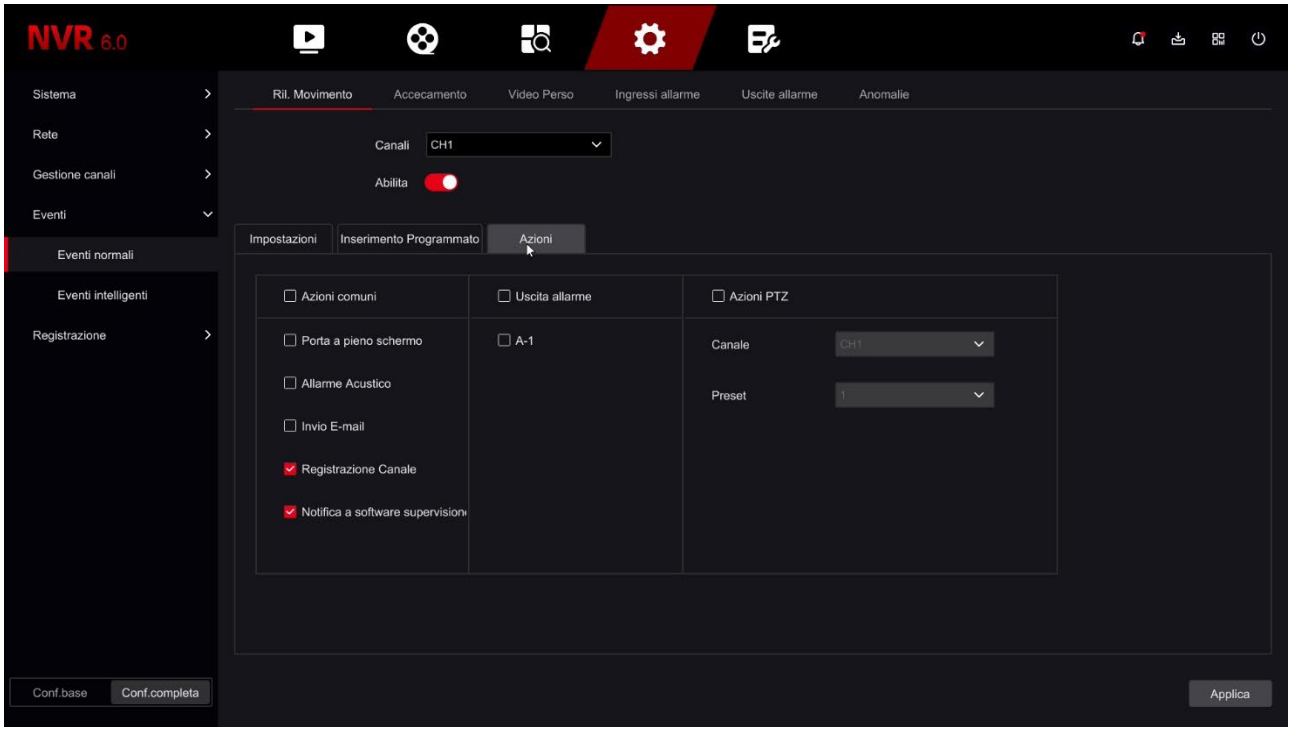
AREA SETTINGS – You can define in which area of the field of view the detection takes place movement. Areas not covered by the red grid will be ignored for detection purposes. For selecting the detection area colors the image boxes with the mouse. If you want the detection occurs on the entire image, select FULL SCREEN or color all the frames dragging the mouse. Depending on the type of DVR/NVR the active area can also be shown as colored gray instead of the red grid. If after some tests you have the impression that this adjustment is not effective is because your camera requires you to configure the detection directly in the camera menu and not through the 'NVR.
SENSITIVITY – You can choose a sensitivity value to exclude, as far as possible, false messages detections due to small movements. Remember that however you can set the sensitivity, you will never be able to completely exclude the probability of false interventions due to multiple factors such as changes in ambient brightness, insects, heavy rain etc.. If after some tests you have the impression that this adjustment is not effective is because your camera requires it you run it directly in the camera menu and not through the 'NVR.
SCHEDULED INSERT – For each day of the week you can define time slots enable if you want motion detection to be active only in certain periods.



Color by dragging the mouse the time slots in which you want the detection to be active. From

In the factory the detection is always active so the table is completely coloured.

ACTIONS – These are the actions that the NVR/DVR will perform following a detection



GO TO FULL SCREEN – You can automatically bring the camera to full screen case of alarm.

ACOUSTIC ALARM - You can activate the internal buzzer of the DVR/NVR at each motion detection. AND' a convenient function to have a local sound alert. We recommend enabling this function while adjusting the motion function, so you can hear if the alarm goes off when you move in front of the camera.

SEND EMAIL – You can send an email in case of detection. For the email to start successfully you must check that the motion triggers properly (check if the little red man appears in the superimposition) and that the SMTP network settings are correct (use the test button in the email section)

CHANNEL RECORDING – You can choose to start recording following detection of the movement. Or you can use motion just to launch alerts and record in continuous.

NOTIFICATION TO SUPERVISION SOFTWARE – Sends event notification to external software

ALARM OUTPUT – If your DVR/NVR has alarm output, you can choose to activate the output following the detection.

PTZ ACTIONS – If you have motorized cameras in your system you can call back automatically preset a camera so that the camera positions itself automatically to a predefined position.

DETECTION TEST

To verify that your motion settings are effective you need to perform walk tests while moving within the field of vision, as an intruder might do. It is ideal to have a collaborator for do these tests more comfortably.

When the motion is triggered you must see the little red man icon that appears overlayed in the live image. If you have programmed motion recording, you also need to see it light up the green video camera icon.

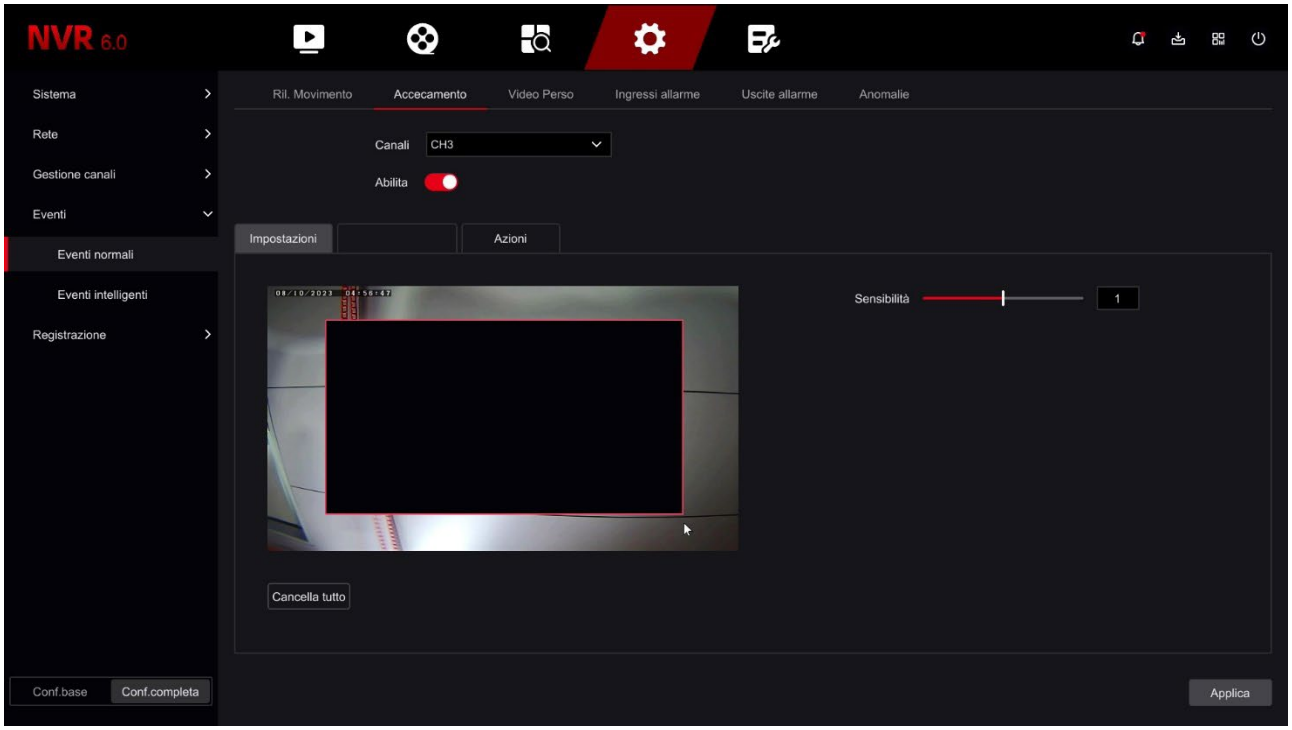
Channel recording

Motion detection alarm channel

If during the test you see that the little red man does not appear during an intrusion you must check the motion detection options described above. If instead the little red man appears, but not the green camera is because recording in the event of a motion alarm is not programmed, then check the table in the REGISTRATION section.

NORMAL EVENTS | BLINDING

In this section you can set the anti-blinding function which is used to generate an alarm if a camera produces a black image because it is covered by malicious people. Not all models of cameras support this function.



ENABLE – Enables detection

SETTINGS – Trace with the mouse the portion of the image on which to activate the detection

SENSITIVITY – Set the sensitivity if the camera supports it

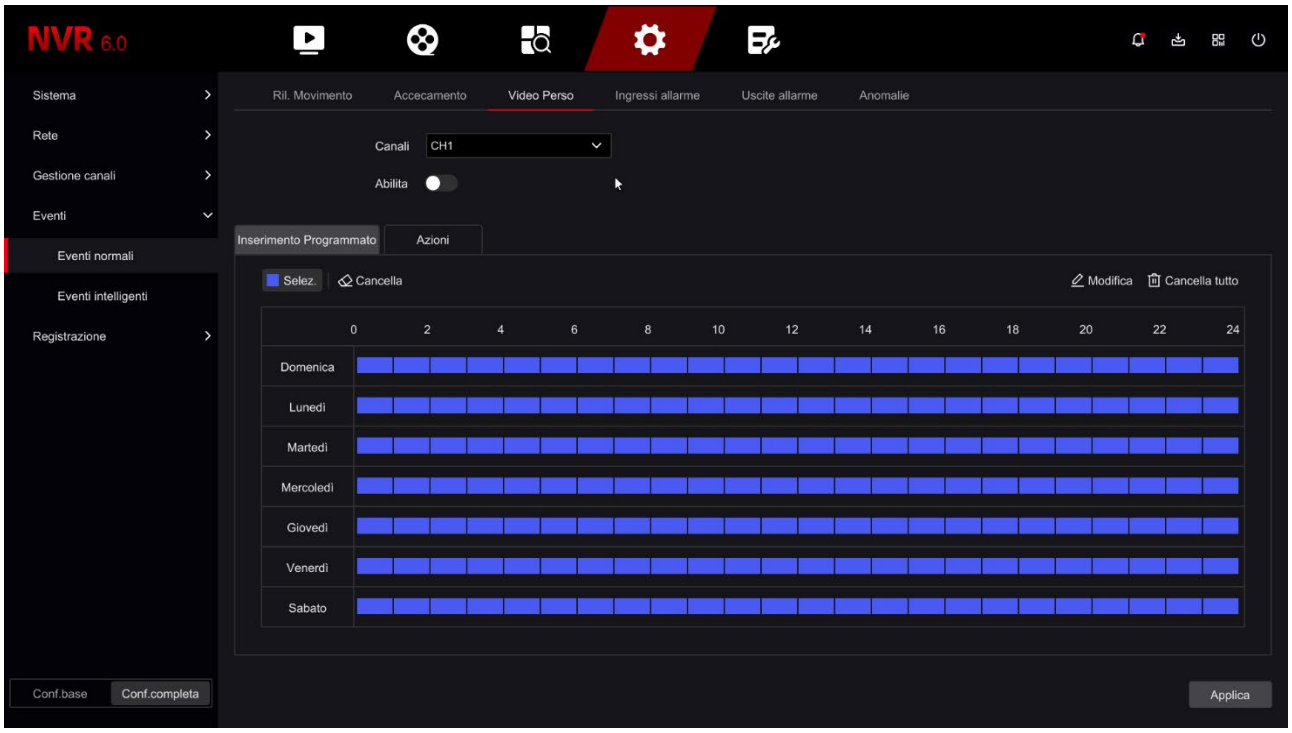
SCHEDULED ARMING – Colors the time slots in which to enable the detection

ACTIONS – In case of detection you can enable the alarm actions already described for the detection of movement: Full screen, Audible alarm, Email sending, Alarm output, Preset recall of cameras

NORMAL EVENTS | LOST VIDEO

In this section you can activate alarm actions in case of loss of a video signal

it may be caused by a fault or sabotage.



ENABLE – Enables detection

SCHEDULED ARMING – Colors the time slots in which to enable the detection

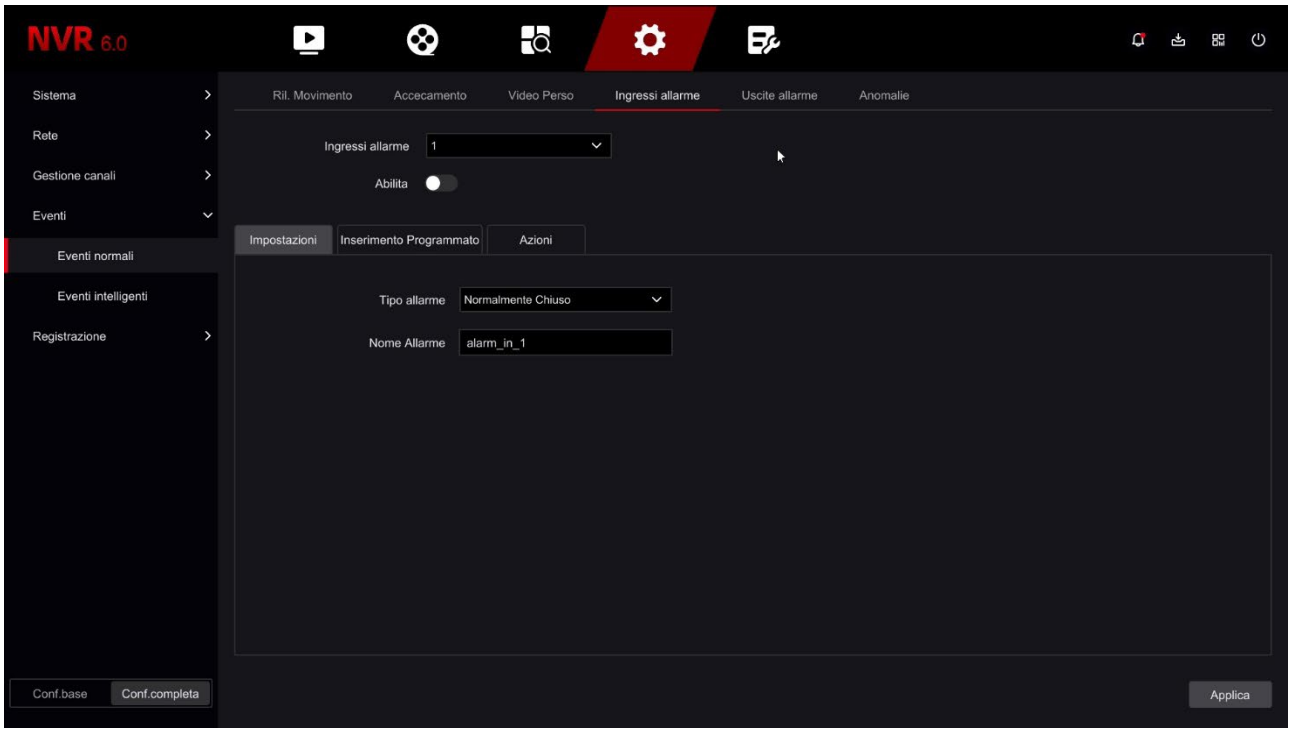
ACTIONS – In case of detection you can enable the alarm actions already described for the detection

of movement: Full screen, Audible alarm, Email sending, Alarm output, Preset recall

of cameras

NORMAL EVENTS | ALARM INPUTS

If your DVR/NVR has alarm inputs here you can configure their operation



ALARM INPUT – Each input on the terminal block has its own programming

ENABLE – Enables the selected alarm input

ALARM TYPE - You can choose NO operation (Normally open, alarm on closing)

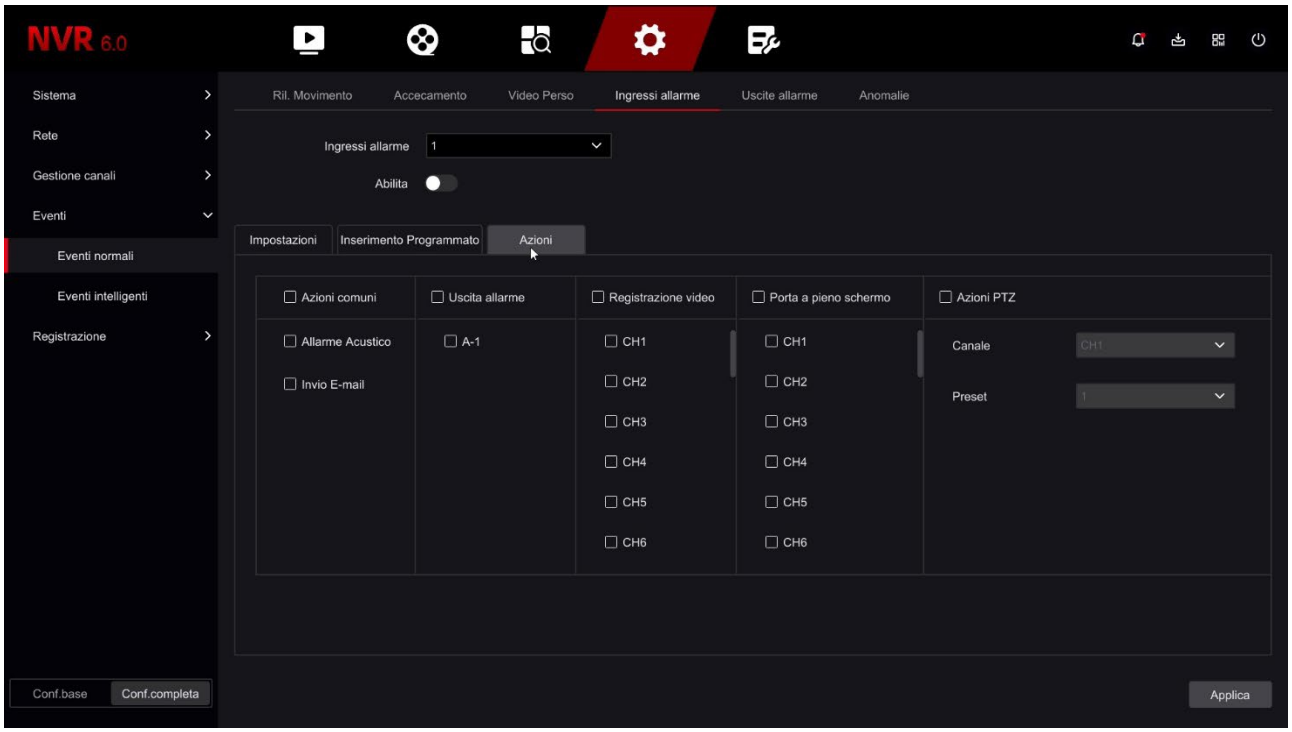
or NC (Normally closed, alarm on opening)

ALARM NAME – You can edit a name that identifies the function of the input

SCHEDULED ARMING – Colors the time slots in which to enable the detection

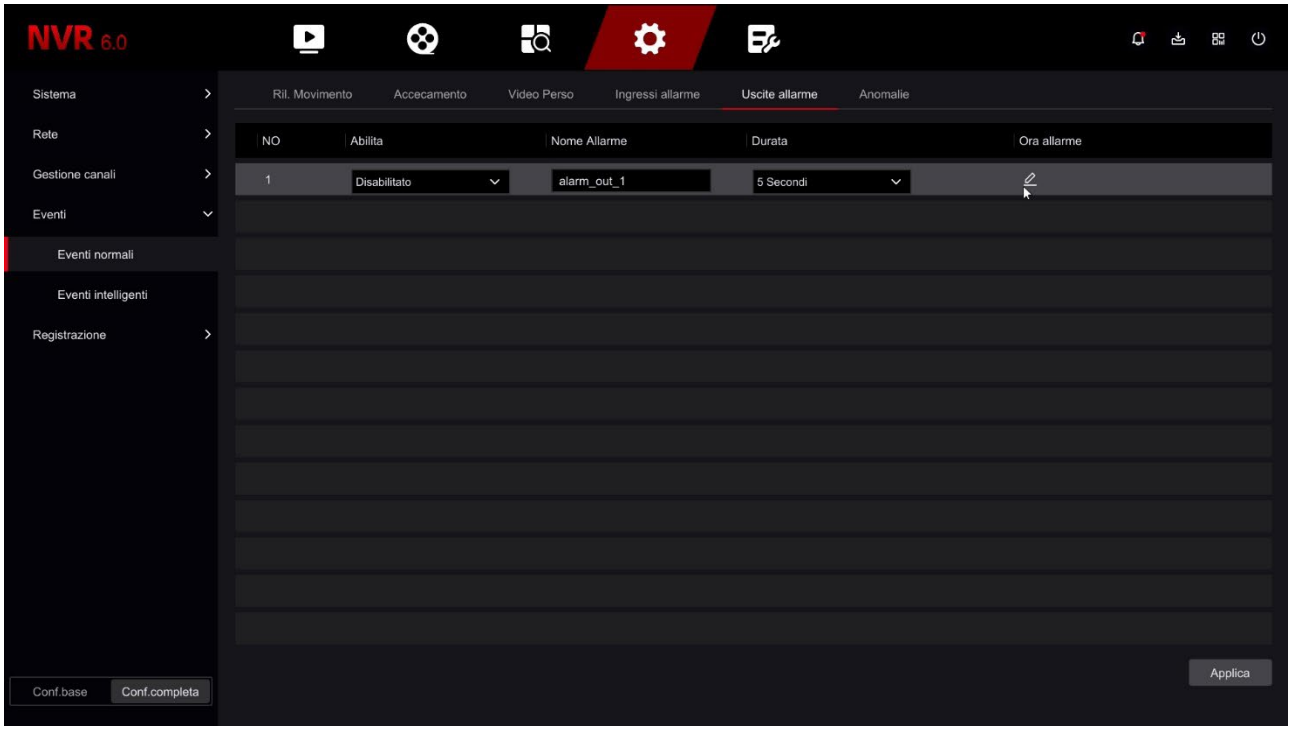
ACTIONS – In case of detection you can enable the alarm actions already described for the detection of movement: Acoustic alarm, Send email, Alarm output, Recall camera presets.

You can also define which cameras to bring to full screen and record.



NORMAL EVENTS | ALARM OUTPUTS

If your DVR/NVR has alarm outputs you can configure them here



ENABLE – Enables the selected alarm output

ALARM NAME – For each output on the terminal board you can edit an identifying name

DURATION – You can define how long the output remains active in the event of an alarm (from 5 sec to 10 min)

ALARM TIME - Colors the time bands in which to enable the alarm output

NORMAL EVENTS | ANOMALIES

In this section you can enable a report in case of anomalous events such as:

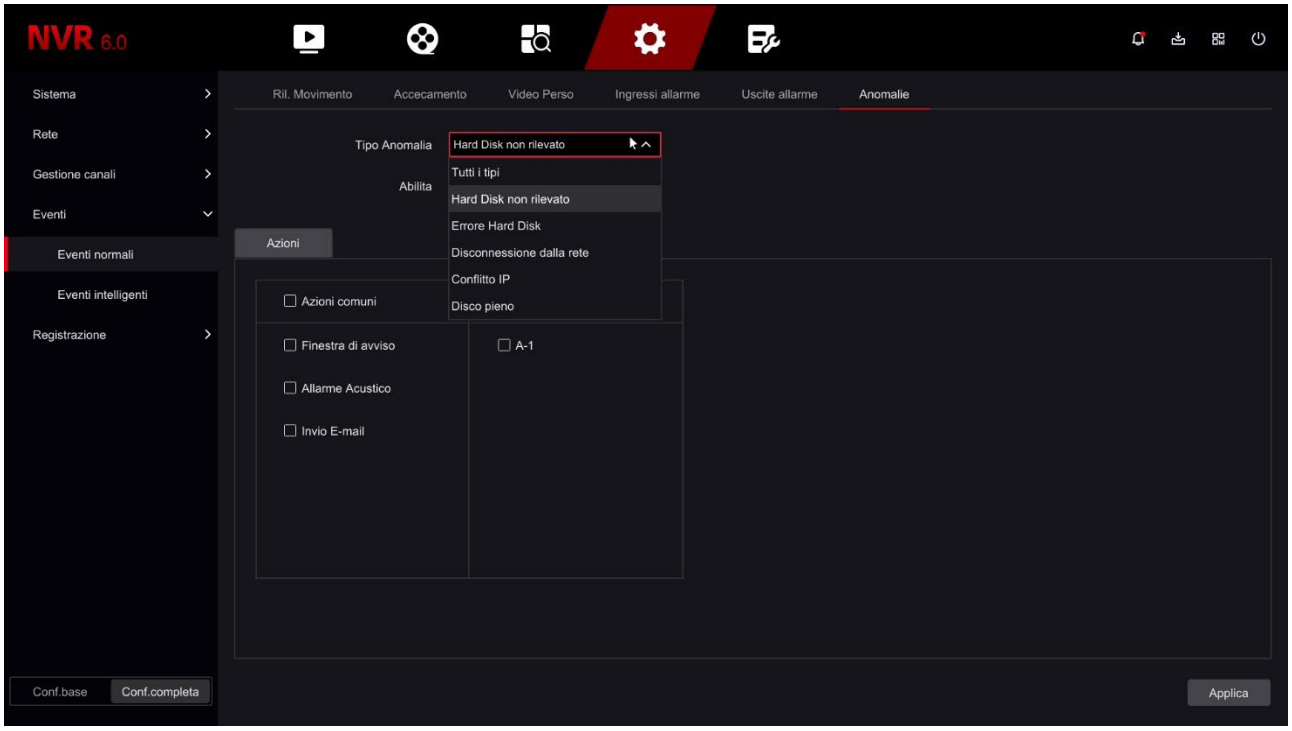
Disk not present

Disk writing errors

Network disconnected

IP conflict on the network

Disk full



For each anomalous event you can enable a message on the monitor, the sending of an email, the sound of the internal buzzer and activation of outputs.

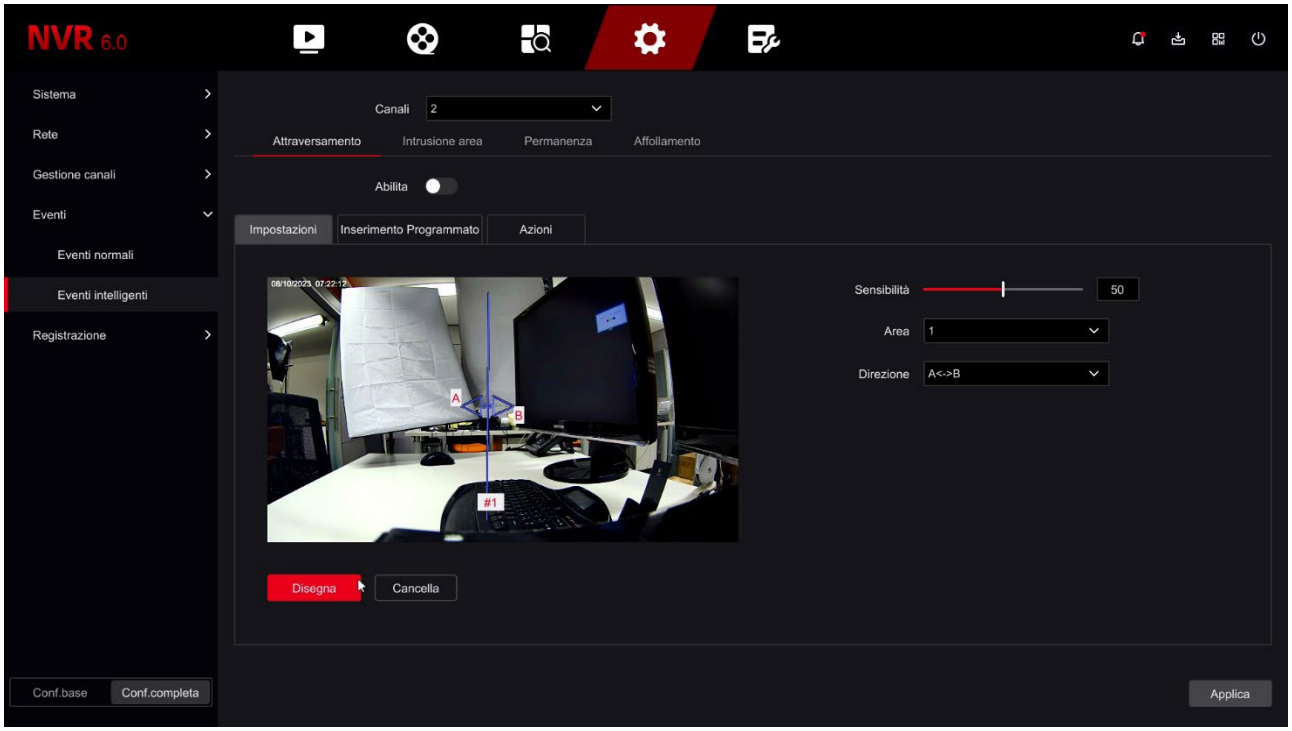
INTELLIGENT EVENTS | CROSSING

If you have connected one of our RK cameras with intelligent detection to your NVR line crossing here you can set the detection parameters.

Line crossing allows you to detect the crossing of a virtual line by a person.

Note that the adjustments for these intelligent functions reside in the camera. The NVR gives you allows you to set the configuration and send it to the camera. Refer to the manual

RK Series camera setup for more details on these features.

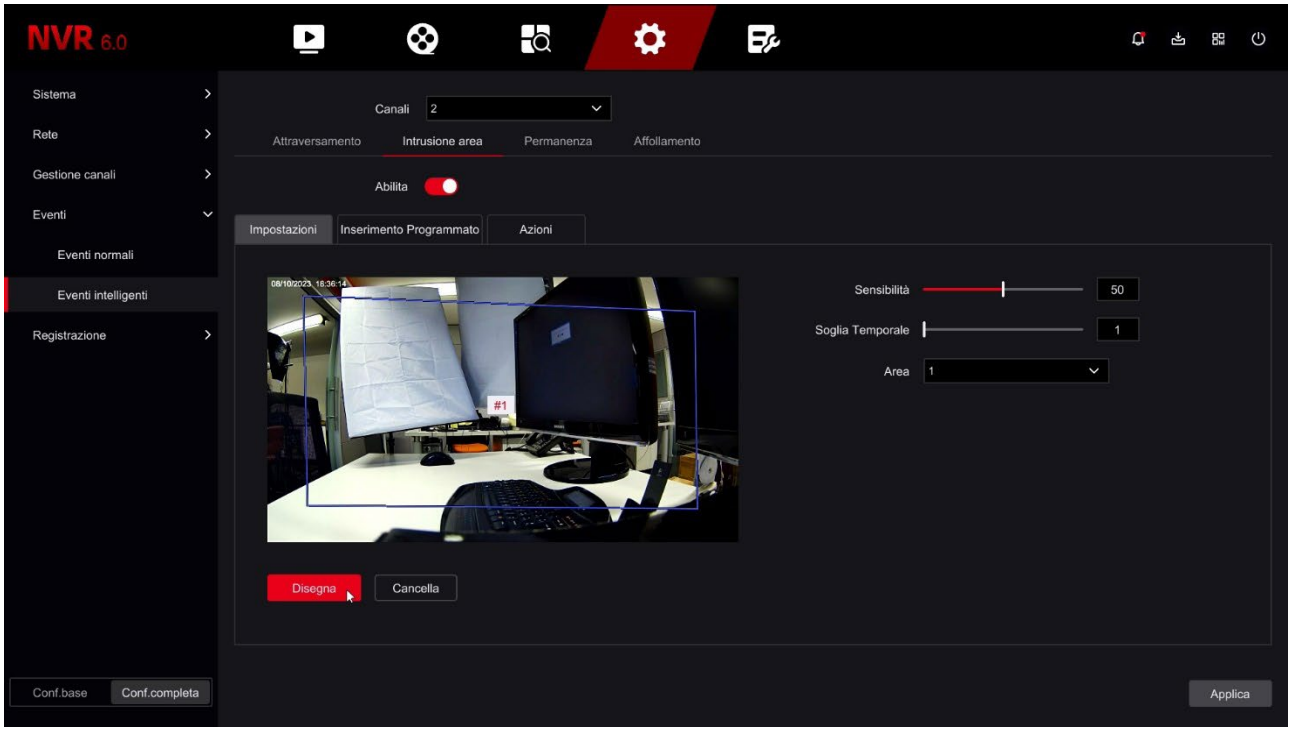


CHANNELS – You can set intelligent functions only for cameras that support them.
DRAW/END DRAWING – Click to draw the crossing line with the mouse
on the live image
SENSITIVITY – Adjusts the detection sensitivity
AREA – You can draw up to 4 virtual crossing lines
DIRECTION – You can define whether to detect crossings in one direction only or in both
directions.
SCHEDULED ARMING – Colors the time slots in which to enable the detection
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

INTELLIGENT EVENTS | AREA INTRUSION

If you have connected one of our RK cameras with intelligent detection to your NVR
human here you can set the detection parameters. Almost all of our cameras
today they have human detection.
Human intrusion detection in an area is distinguished from motion detection
we have already described how it exclusively detects people, ignoring movements
other nature. If you use this detection you should disable motion detection
normal, which you find among normal events.
Note that the adjustments for these intelligent functions reside in the camera. The NVR gives you

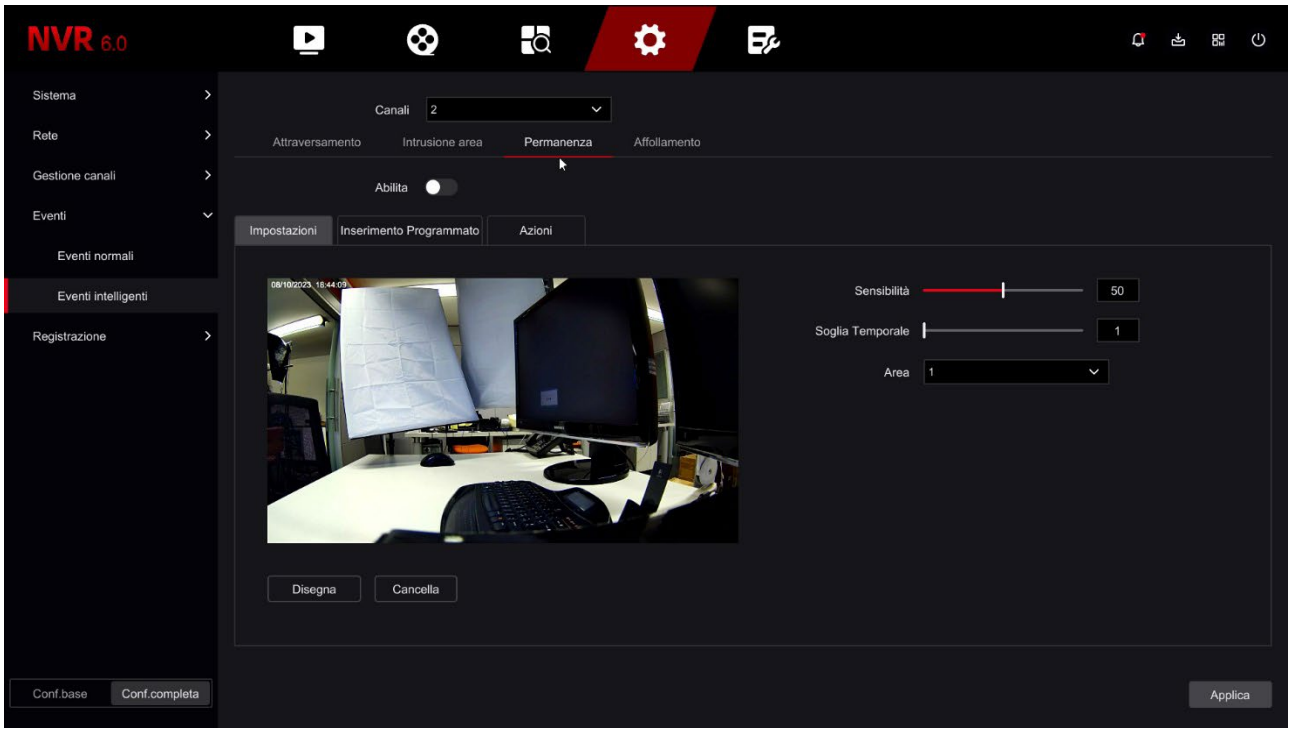
allows you to set the configuration and send it to the camera. Refer to the manual
RK Series camera setup for more details on these features.



CHANNELS – You can set intelligent functions only for cameras that support them.
DRAW/END DRAWING – Click to trace the area in which to survey with the mouse
the intrusion
SENSITIVITY – Adjusts the detection sensitivity
TIME THRESHOLD – You can define a delay between detection and the start of the alarm.
AREA – You can trace up to 4 detection areas
SCHEDULED ARMING – Colors the time slots in which to enable the detection
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

INTELLIGENT EVENTS | STAY

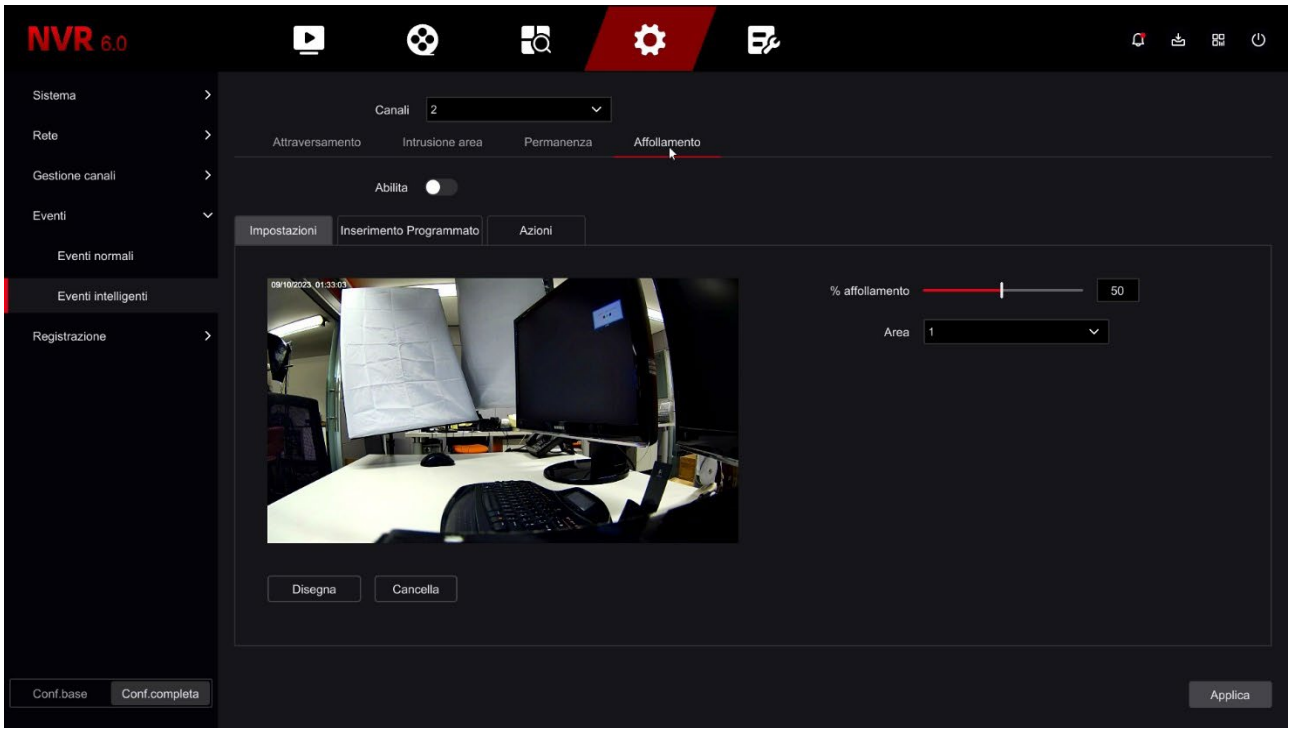
If you have connected one of our RK cameras with intelligent permanence detection to your NVR here you can set the detection parameters.
Human permanence detection is used to generate an alarm if a person remains in one certain area for longer than permitted.
Note that the adjustments for these intelligent functions reside in the camera. The NVR gives you allows you to set the configuration and send it to the camera. Refer to the manual
RK Series camera setup for more details on these features.



CHANNELS – You can set intelligent functions only for cameras that support them.
DRAW/END DRAWING – Click to trace with the mouse the area in which to detect the
stay
SENSITIVITY – Adjusts the detection sensitivity
TIME THRESHOLD – You can define how long a person can stay inside
of the defined area without generating the alarm.
AREA – You can trace up to 4 detection areas
SCHEDULED ARMING – Colors the time slots in which to enable the detection
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

INTELLIGENT EVENTS | CROWDING

If you have connected one of our RK cameras with intelligent crowding detection to your NVR here you can set the detection parameters.
Human crowding detection is used to generate an alarm if crowding occurs in a certain area crowded with a greater number of people than allowed.
Note that the adjustments for these intelligent functions reside in the camera. The NVR gives you allows you to set the configuration and send it to the camera. Refer to the manual
RK Series camera setup for more details on these features.



CHANNELS – You can set intelligent functions only for cameras that support them.

DRAW/END DRAWING – Click to trace the area in which to survey with the mouse the crowding

% CROWDING – Adjusts the amount of people in the area needed to trigger the alarm.

AREA – You can trace up to 4 detection areas

SCHEDULED ARMING – Colors the time slots in which to enable the detection

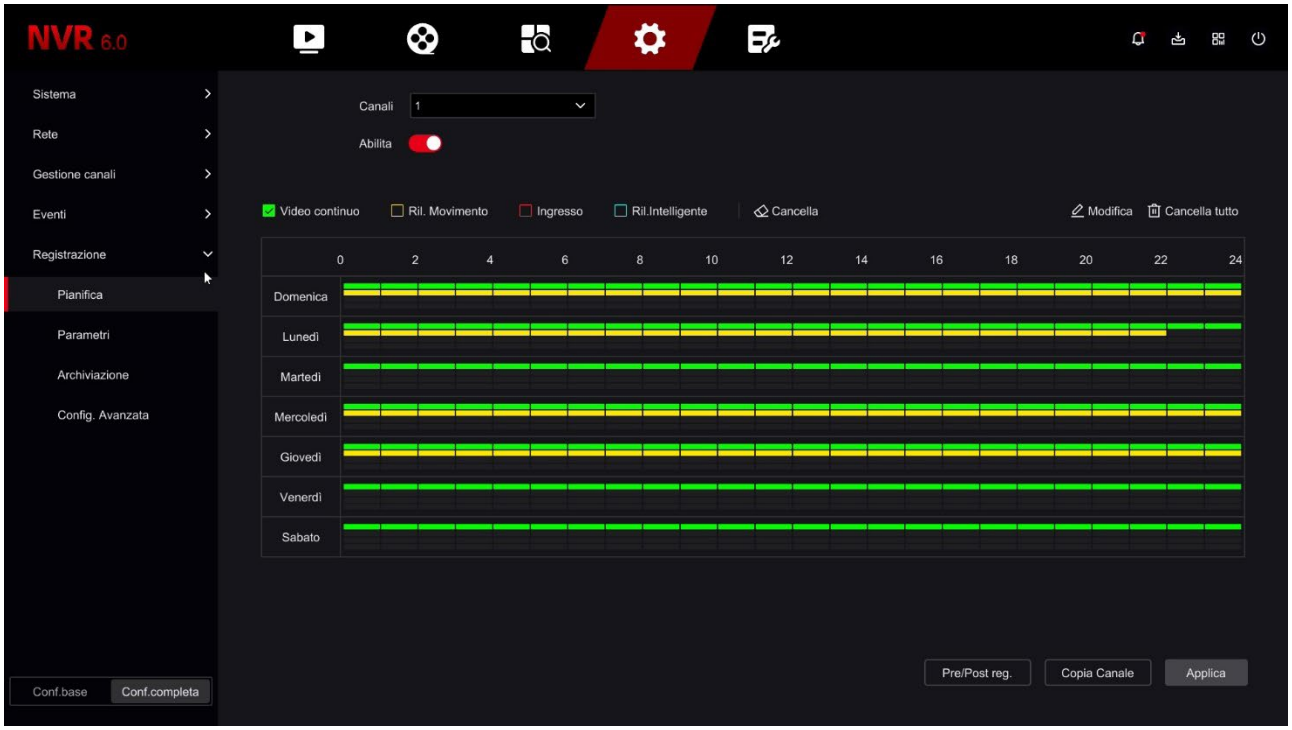
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

CONFIG.| REGISTRATION

Click the CONFIGURATION button and then choose REGISTRATION to open the page you need allows you to control the Hard Disk and recording rules.

PLAN

On this page you define how to record the cameras depending on the time and day of the week



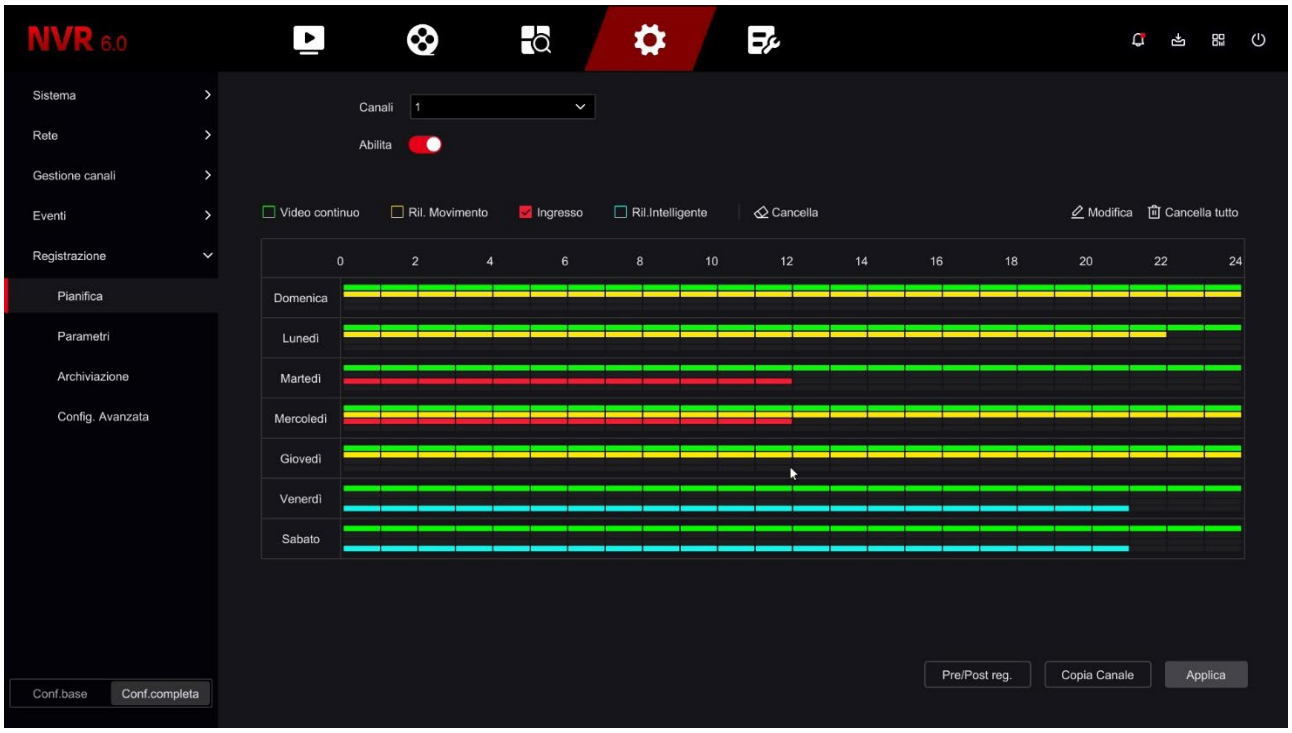
The first thing you need to do is choose the channel to configure at the top. Each camera has its own programming so you have to configure them one by one. If you want to configure all channels in the in the same way you can configure channel 1 and then use the COPY CHANNEL button.

Choose the channel to configure above and then color the green or yellow bands in the calendar with the mouse weekly. The green bands indicate continuous recording, the yellow bands indicate the recording only in case of motion detection (motion detection).

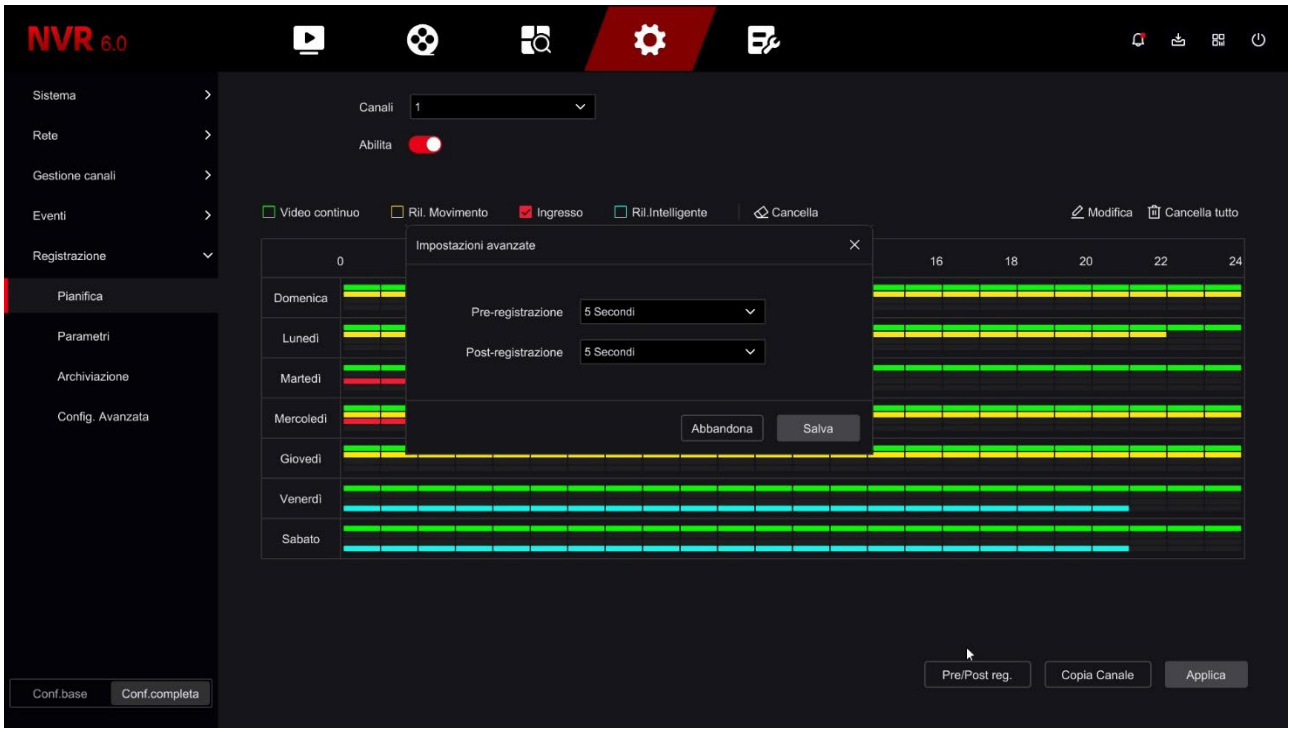
To color the table, choose the green or yellow color at the top, then drag the mouse directly onto it calendar.

If your DVR/NVR has alarm inputs for external contacts, in addition to the yellow and green colors you can also color the table RED (recording from alarm input). If you use ours RK Series IP cameras with intelligent human detection, you can also color the table BLUE (intelligent recording).

You can set up several types of recording at the same time so it is advisable
Always keep the green continuous recording active to ensure you never lose
no image.

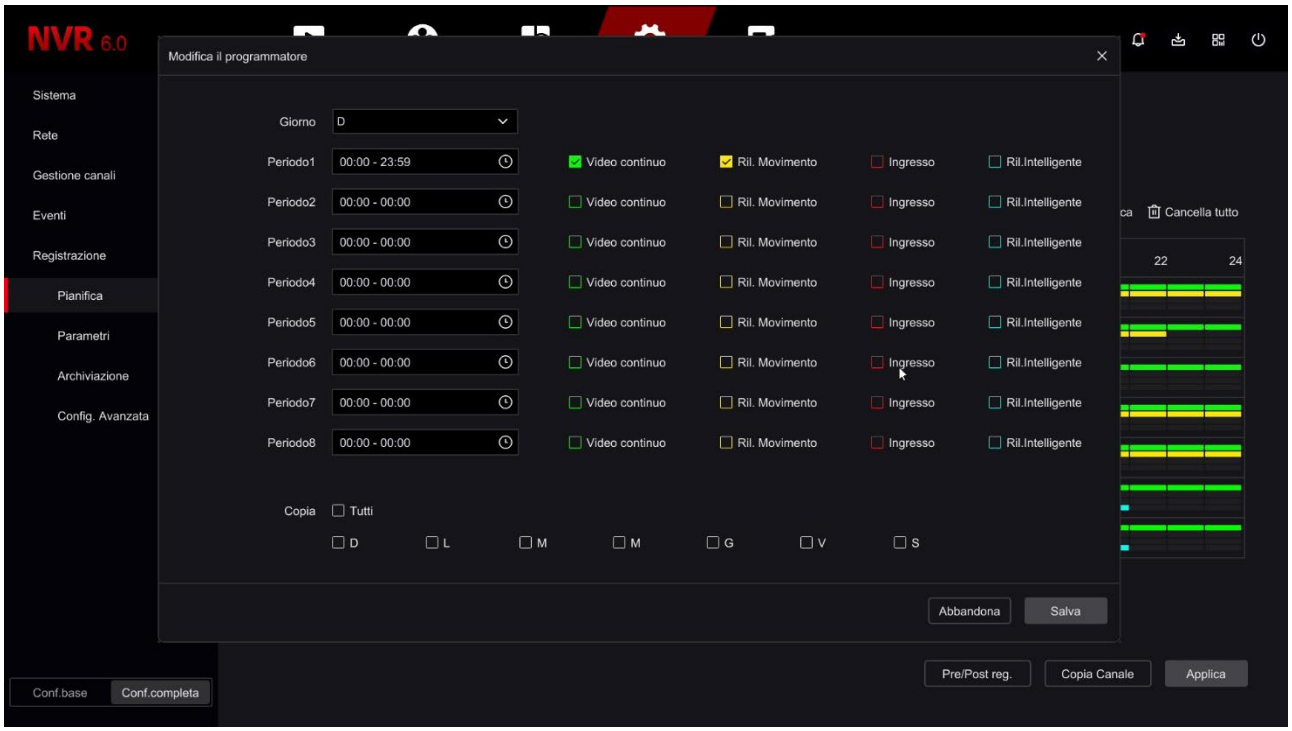


The PRE/POST REC button. allows you to set the pre-registration period, which allows you to record a certain period before the survey, and the post-registration period i.e. the recording duration following the event.



With the EDIT button you have another way to schedule recordings.

You can set each day's time slots manually instead of tracking them with the mouse.



REGISTRATION VERIFICATION

To make sure you have set the registration table correctly, check

the live image of the cameras. If the recording is in progress you must see the overlay
the green camera icon.

Channel recording

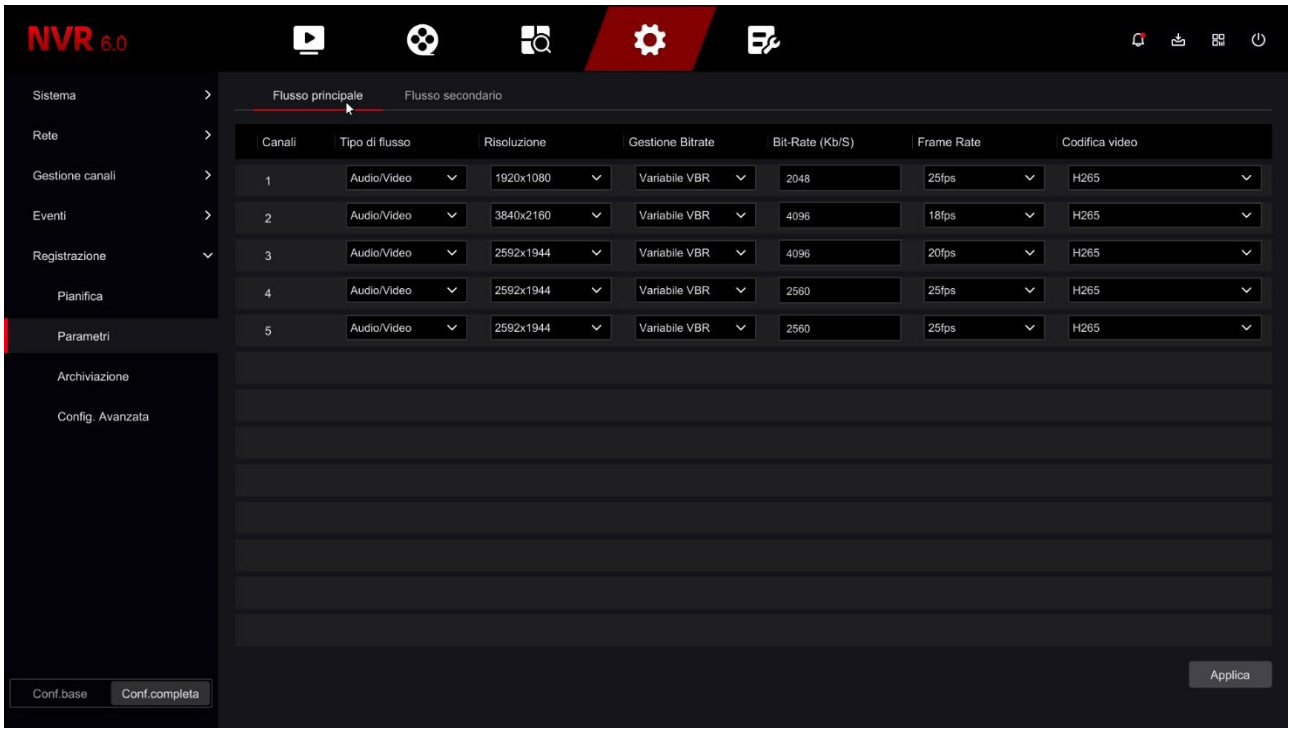
If the channel does not record even though you have set the table well, check the HARD section
DISK because there may be problems on the hard disk on which the files are stored
recordings.

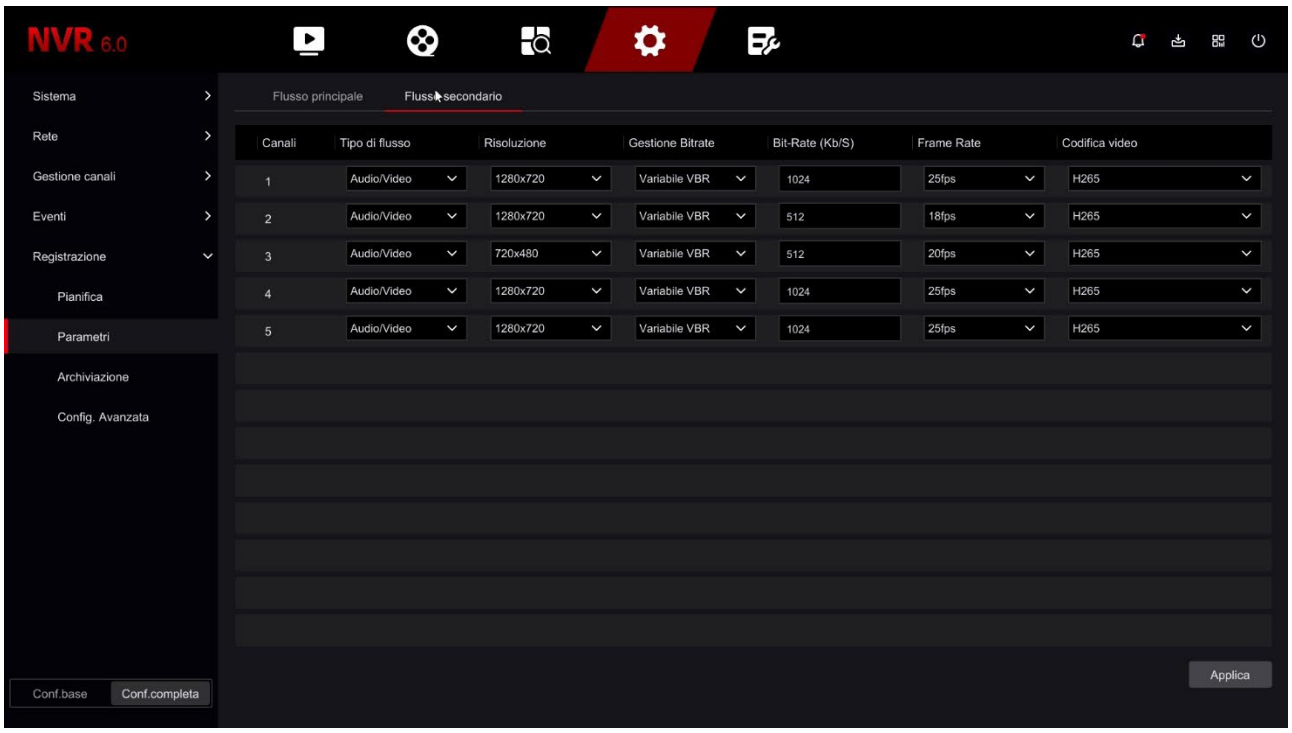
PARAMETERS | MAIN FLOW / SECONDARY FLOW

In these windows you set the main and secondary video streams of the cameras.
Each camera can generate two video streams: the main stream and the stream
secondary (substream). The main video stream is the one at the highest resolution
It is used in full screen viewing and recording. Secondary streaming, or sub
stream is the lightest one that is used when viewing many screen cameras and so on
Internet.
This section consists of two tabs: one for the main streaming and one for the secondary.
Each channel has its own configuration.

IN IP CAMERAS video streaming adjustment is done in the settings
camera, not via the NVR. This is because the NVR does not process the video arriving from the
camera, but just receives it. However, our NVRs allow you to adjust the streaming
of our RK series IP cameras by configuring the options which are then sent to the
camera. You will find two separate configuration pages for the two video streams.
If you have not connected RK series IP cameras, these pages are not effective.

IN ANALOG AND AHD CAMERAS video streaming adjustment is done in the DVR
as it is the DVR that digitizes the analog signal. On this page you can
set the DVR video encoding parameters for each channel.



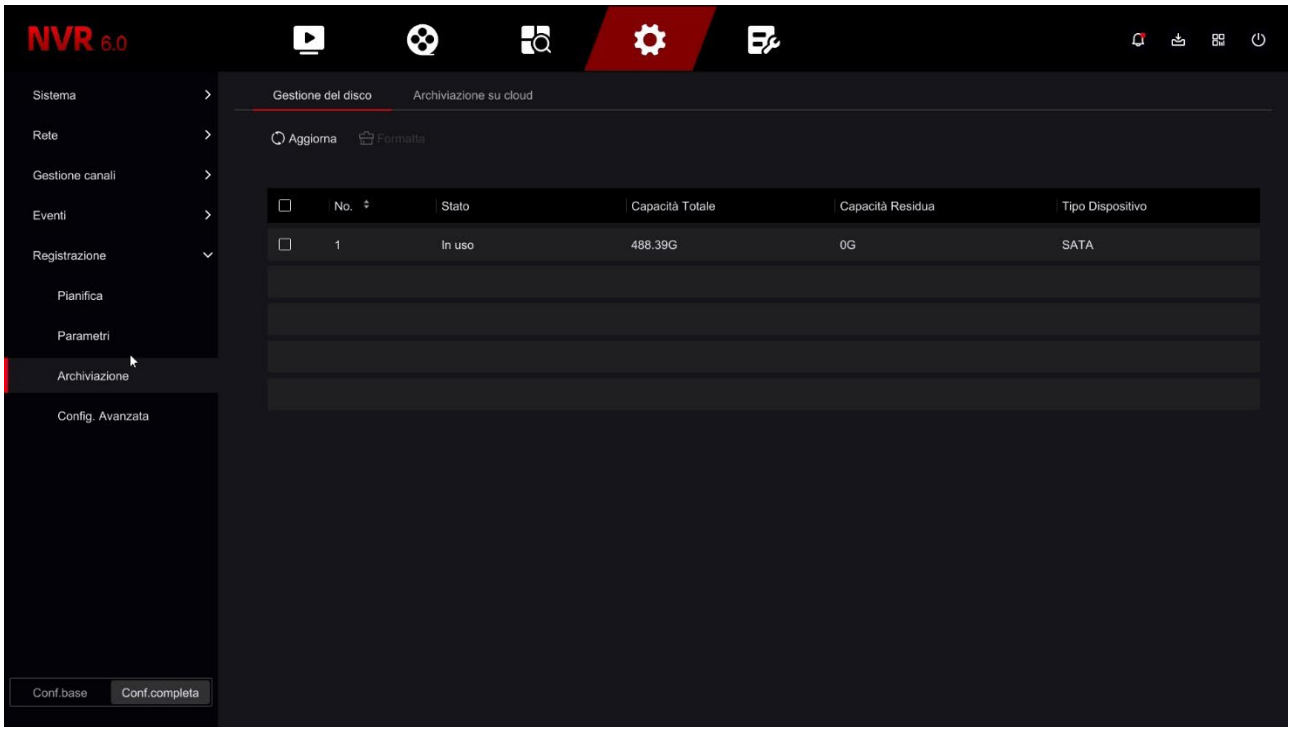


In this manual we do not explain in detail the meaning of the adjustment items
video streaming from IP cameras. You can find this information in the camera manual.
STREAM TYPE – You can choose Video or, if the camera allows it, Audio/Video
RESOLUTION – The resolution of the video stream
BITRATE MANAGER – You can choose CBR (constant band) or VBR (variable band) management

constant quality)
BITRATE – Sets the maximum bandwidth (Kb/s) that the camera will occupy
FRAME RATE – The number of frames/second that you set to the highest value or possible reduce to limit the space occupied on the disk at the expense of less fluidity of the images movement.
VIDEO ENCODING – Choose H265, the most up-to-date format, for maximum efficiency compression or H264 if the camera does not support H265 – With our RK cameras you can enable further improvement in H265+ or H264+ compression which reduce bandwidth consumption further.

STORAGE | DISK MANAGEMENT

In this tab you control the memory drives (internal or USB)

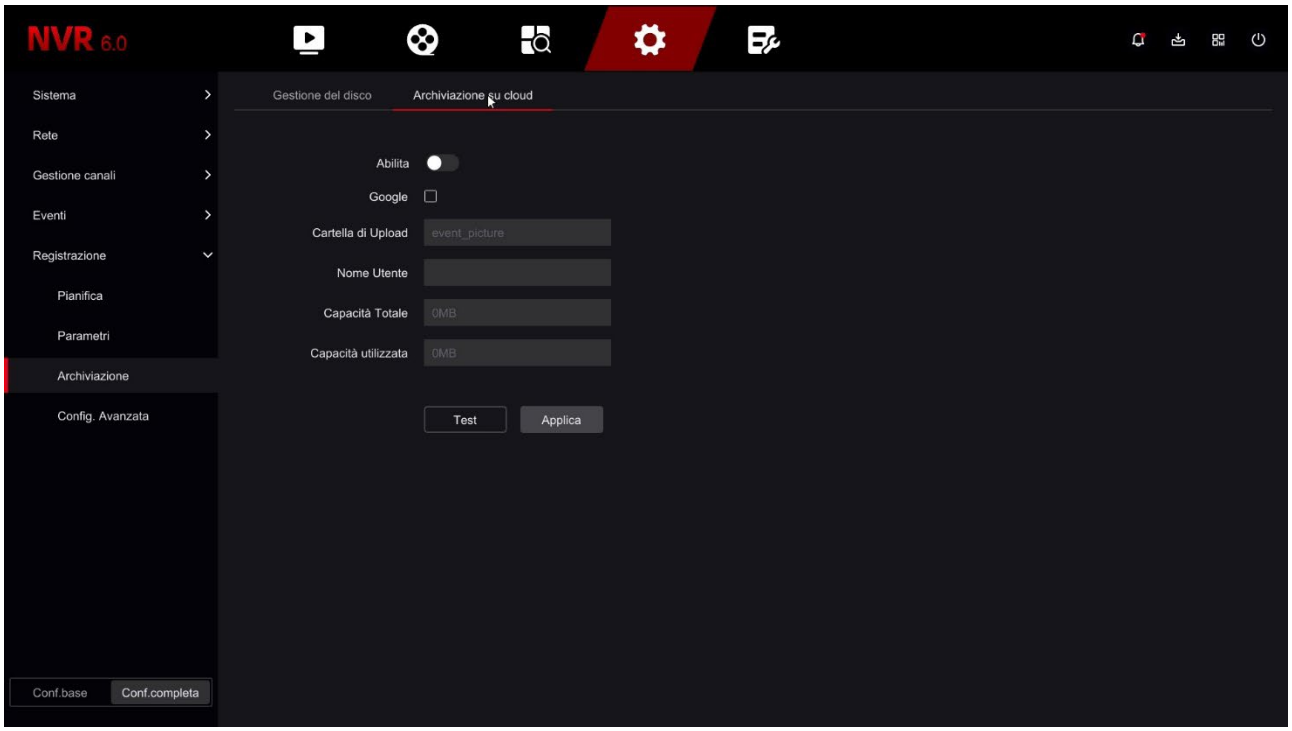


On this page you can check the status of the internal hard disk of the DVR/NVR and find out the total and residual capacity. With the FORMAT button you can proceed to format the disk with the deletion of all data. When the DVR/NVR detects a new disk it prompts automatically formats at startup so you generally don't need to go into this window to make it usable. However, this window can be used to check the status of the disk and to do a forced formatting if you want to delete all the recordings.
If your hard disk is working well, in this window you should see it indicated as IN USE with correct indication of maximum and residual capacity

STORAGE | CLOUD STORAGE

The RK Series NVR/DVRs allow you to save images recorded in the event of an alarm on a server CLOUD storage via the Internet. Google cloud service is supported. In this case, yes These are services similar to our P2P Cloud to facilitate connection, but rather archive spaces web that you can purchase from Google to store data online.

Note that continuous recordings cannot be saved to the cloud, only images afterwards to alarm (motion, alarm input etc.)



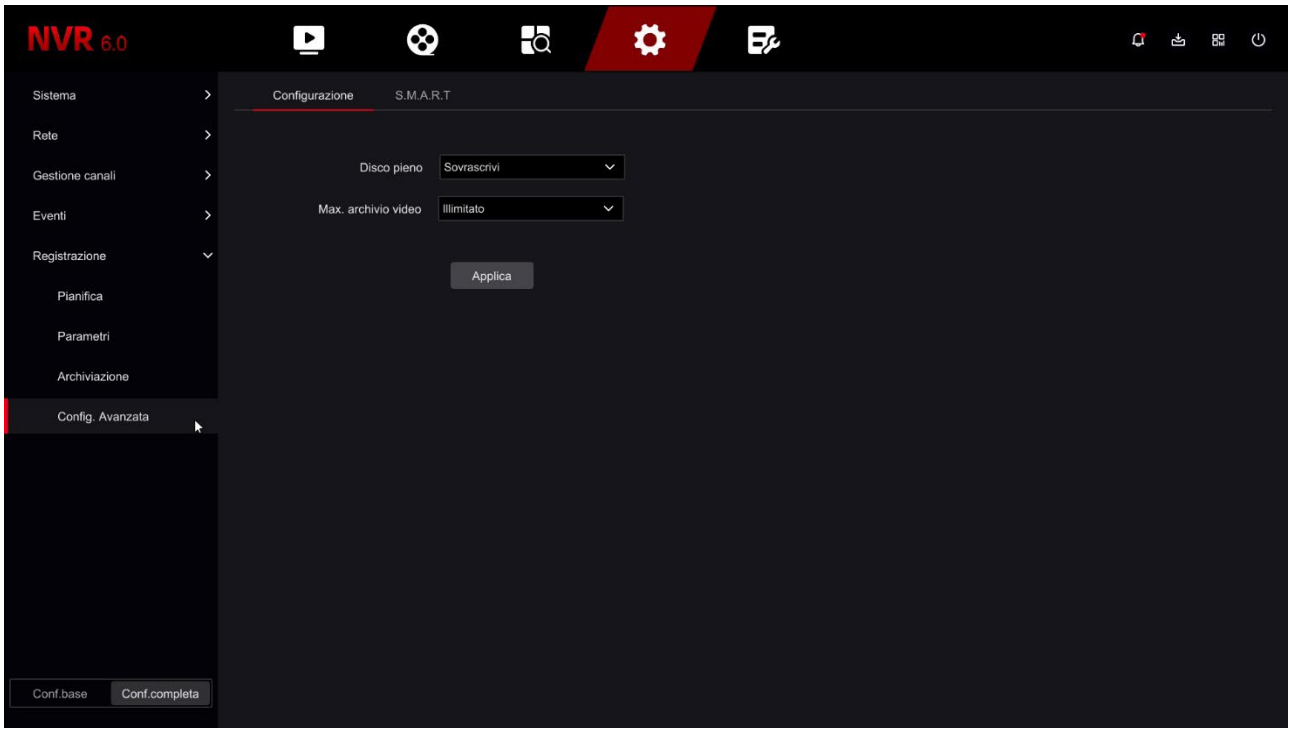
Before completing this table you must obviously subscribe to Google Cloud and have access credentials. You also need to create a folder in your cloud space where to save your files.

On this page you must enter your Google Cloud login details. After entering the required data use the TEST button to verify that they are correct.

Once connected, the available and occupied space on the server will be indicated.

ADVANCED CONFIGURATION | CONFIGURATION

On this page there are some additional settings related to video archiving

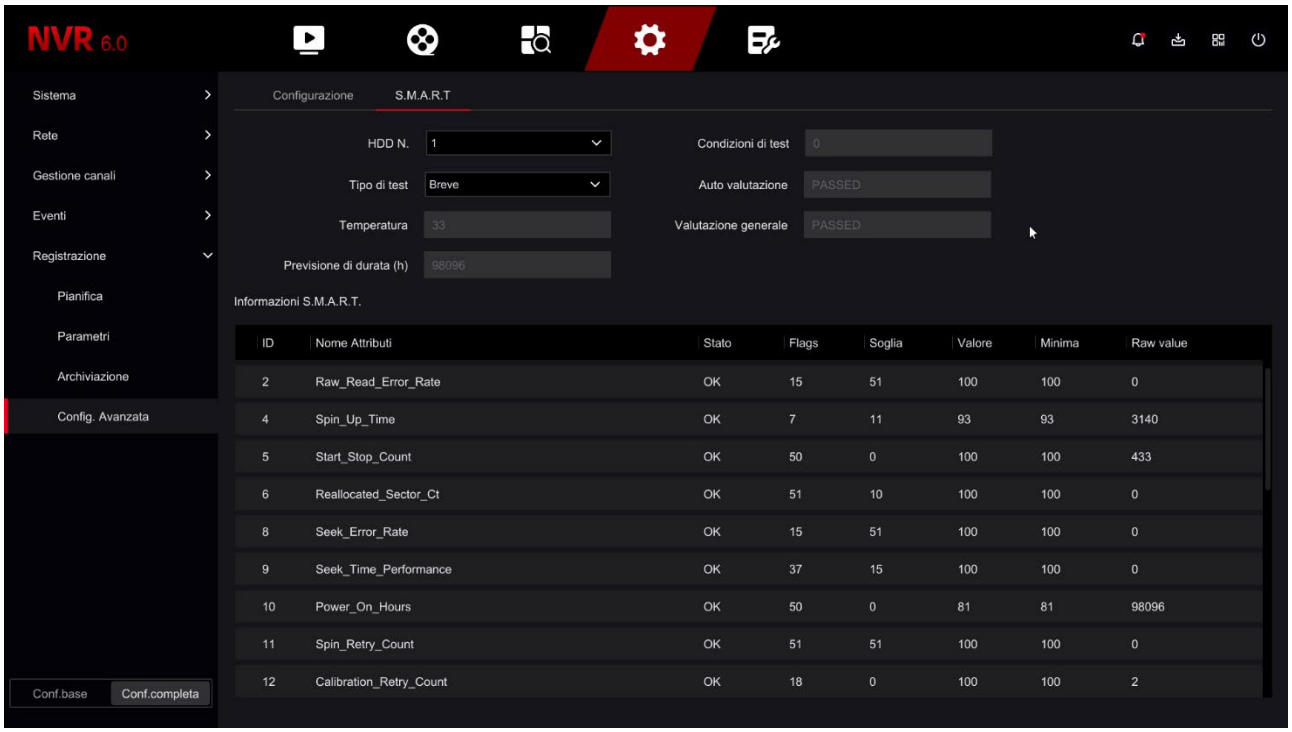


DISK FULL – If you choose Overwrite the NVR will overwrite the oldest files once it runs out disk space. If you choose Don't overwrite recording stops when it runs out of space on disk.

MAX. VIDEO ARCHIVE – You can limit the video archive to a certain number of days to accommodate to regulations relating to privacy.

ADVANCED CONFIGURATION | SMART

On this page, a disk test is performed to evaluate its health

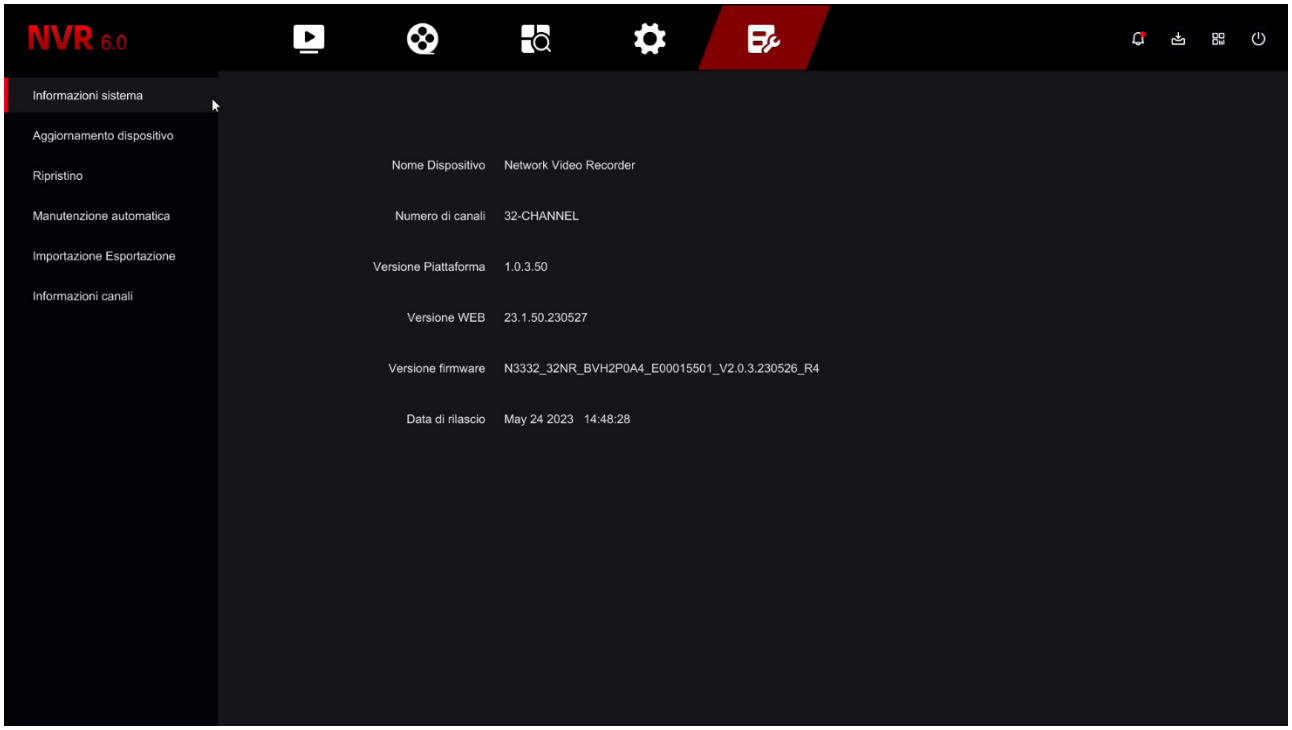

NVR 6.0
Sistema
Rete
Gestione canali
Eventi
Registrazione
Pianifica
Parametri
Archiviazione
Config. Avanzata
Conf.base
Conf.completa
Configurazione
S.M.A.R.T
HDD N. 1
Tipo di test Breve
Temperatura 33
Previsione di durata (h) 98096
Condizioni di test 0
Auto valutazione PASSED
Valutazione generale PASSED
Informazioni S.M.A.R.T.
ID Nome Attributi Stato Flags Soglia Valore Minima Raw value
2 Raw_Read_Error_Rate OK 15 51 100 100 0
4 Spin_Up_Time OK 7 11 93 93 3140
5 Start_Stop_Count OK 50 0 100 100 433
6 Reallocated_Sector_Ct OK 51 10 100 100 0
8 Seek_Error_Rate OK 15 51 100 100 0
9 Seek_Time_Performance OK 37 15 100 100 0
10 Power_On_Hours OK 50 0 81 81 98096
11 Spin_Retry_Count OK 51 51 100 100 0
12 Calibration_Retry_Count OK 18 0 100 100 2

MAINTENANCE

In the maintenance section there are various operations for maintaining the system.

SYSTEM INFORMATION

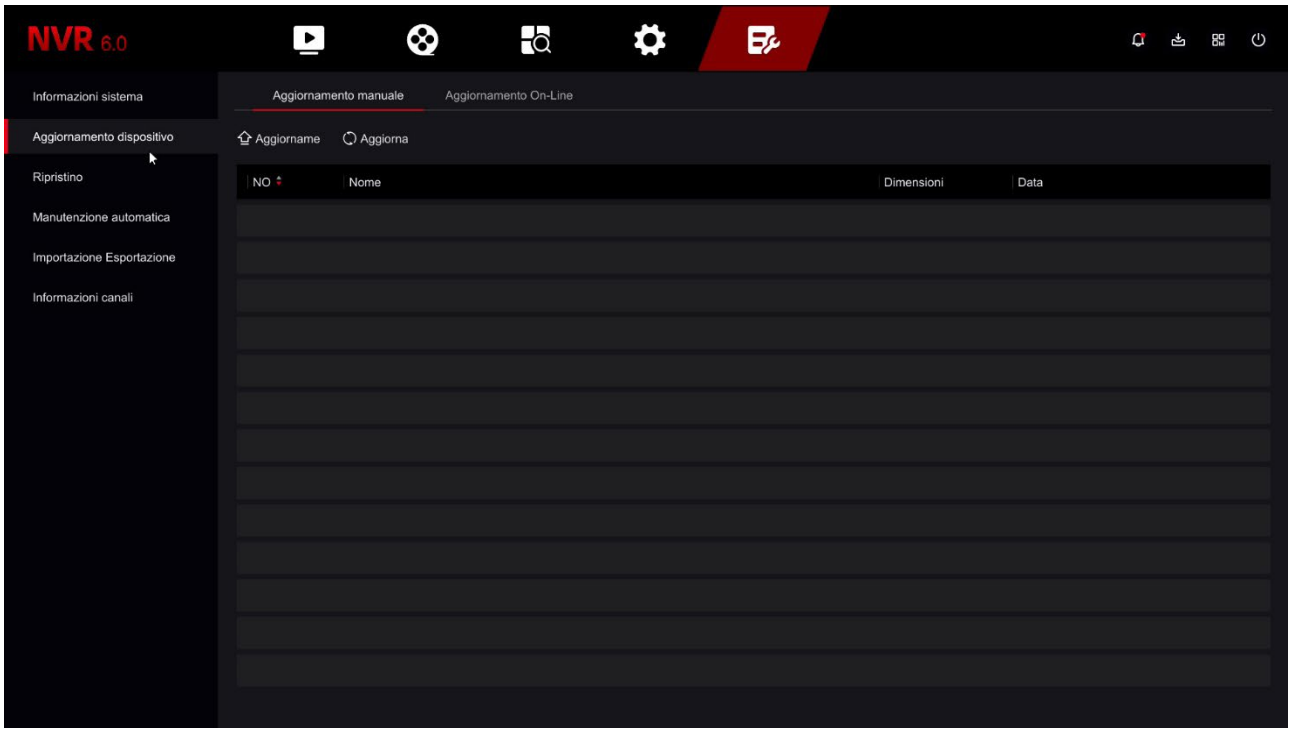
On this page there is information about the video recorder with the firmware version it is the internal software of the device



DEVICE UPDATE | MANUAL UPDATE

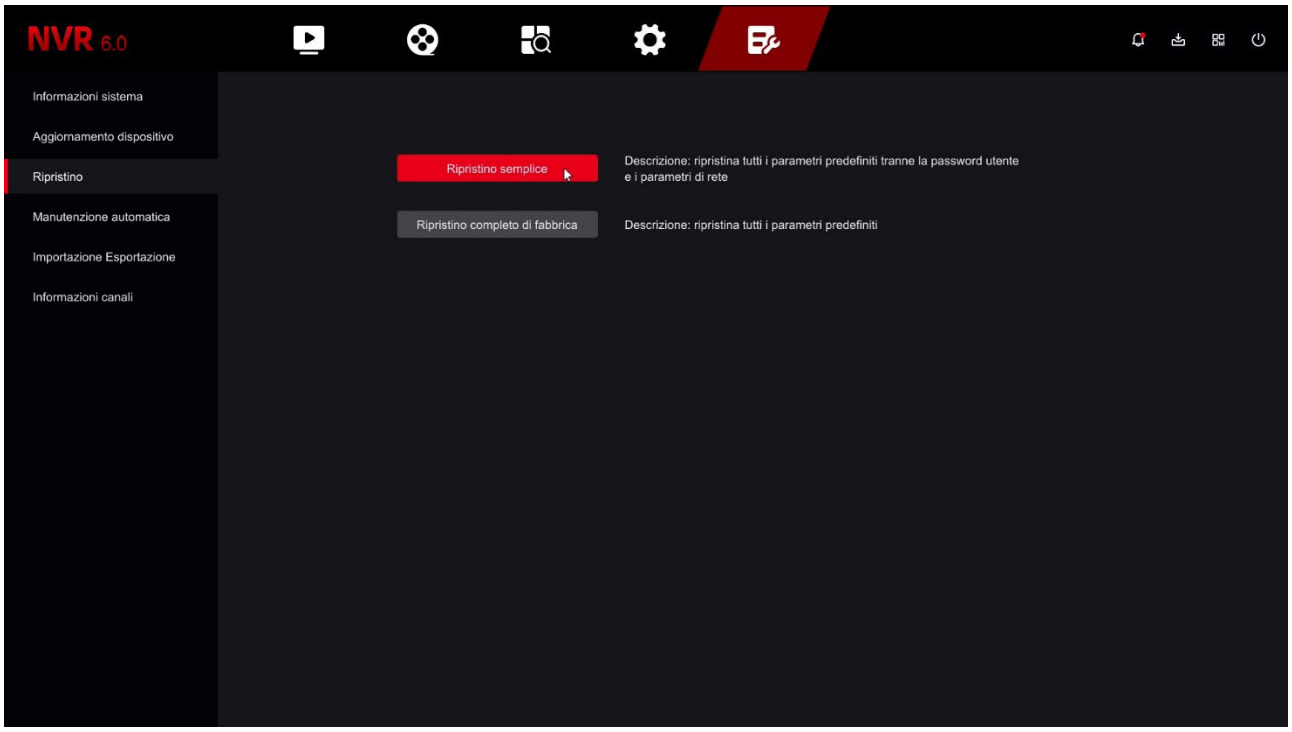
On this page you can update the device's firmware if you have received a update from our customer service. The file must be copied onto a USB stick and then inserted into the NVR/DVR. By inserting the USB stick the file is detected and listed in the table. To start update, choose the file and press UPDATE.

The UPDATE button searches for the update file again.



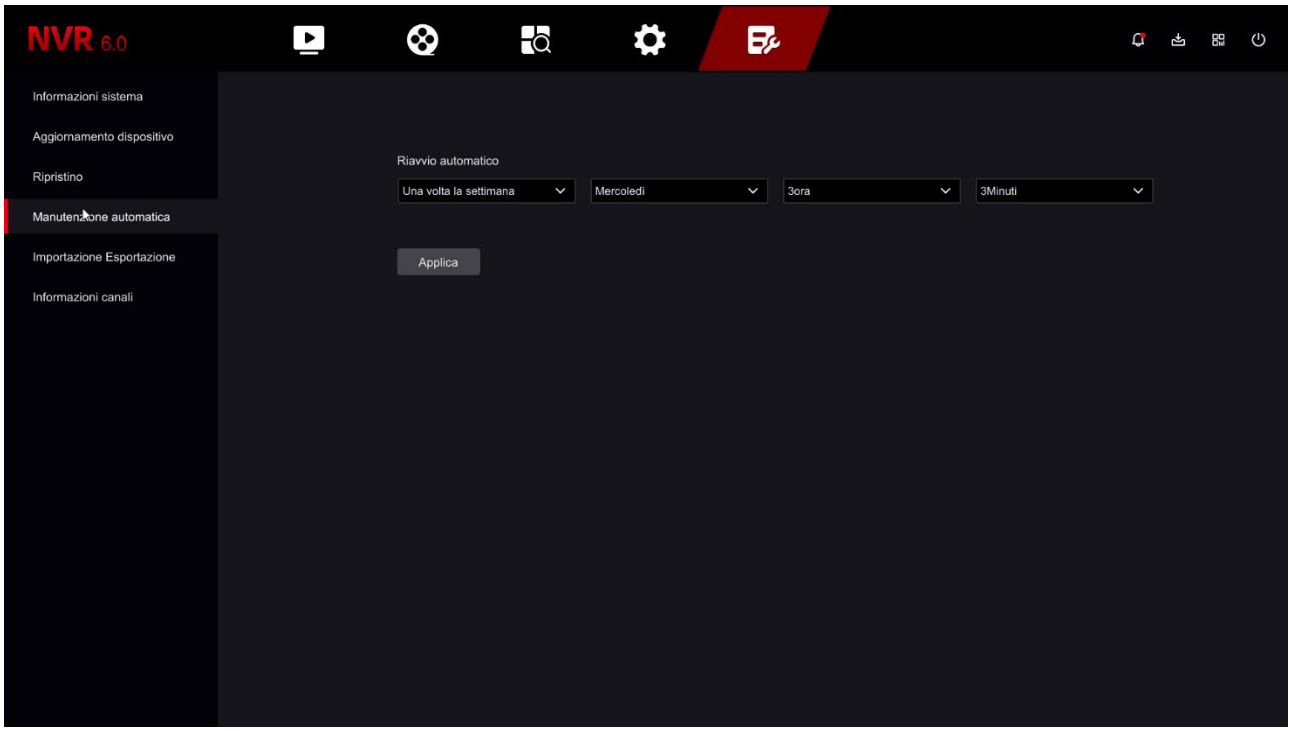
RESTORATION

On this page you can restore the device's factory parameters. You can choose between complete restore of all parameters and simple restore that preserves credentials login and network settings.



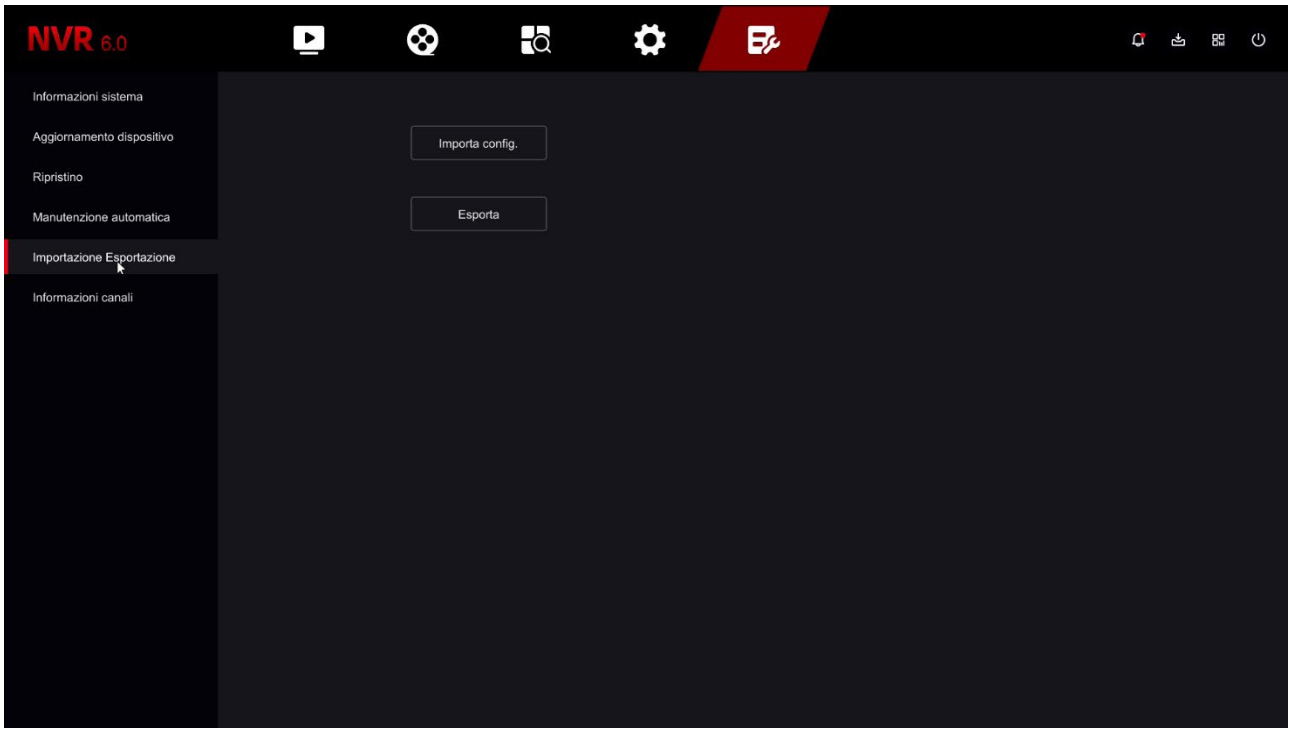
AUTOMATIC MAINTENANCE

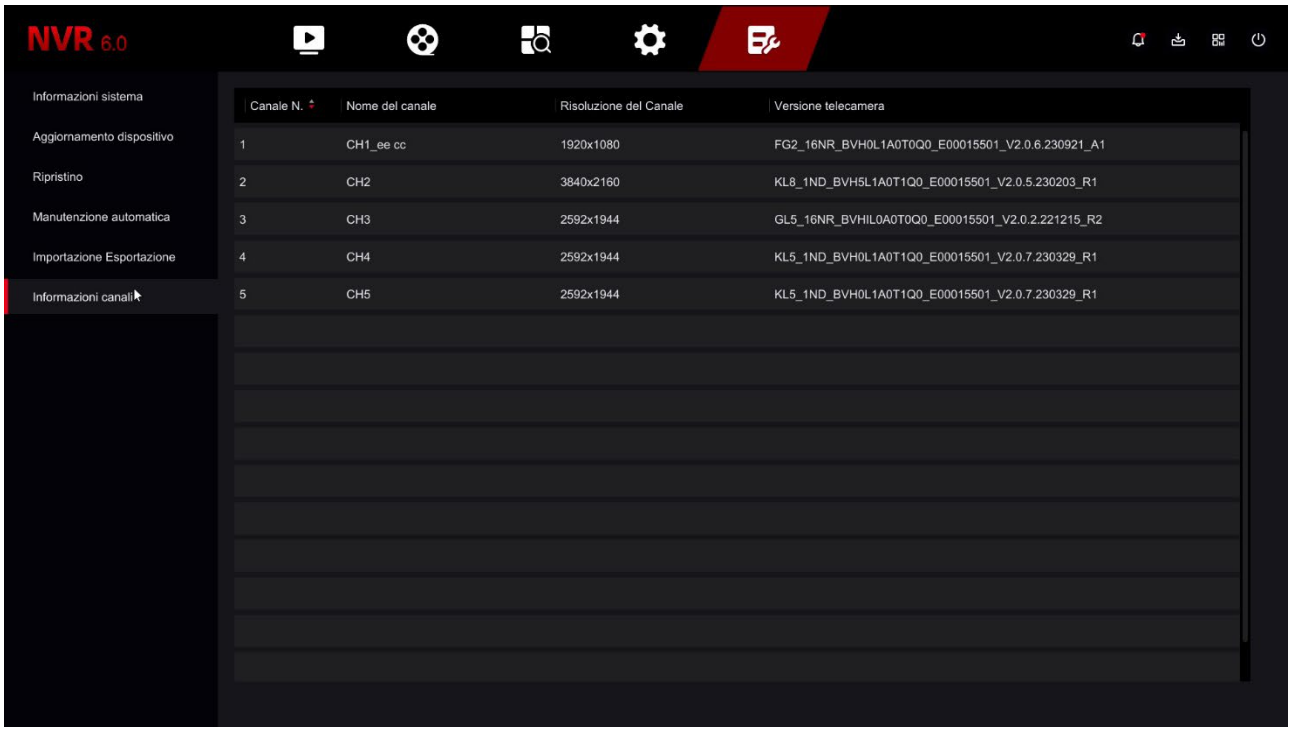
On this page you can set the automatic restart of the DVR/NVR which is set at the factory once a week



IMPORT / EXPORT

On this page you can export the entire DVR/NVR configuration to a file or import one previously exported configuration. It is a useful function for saving the configuration performed in case of failure.



CHANNEL INFORMATION

On this page you can check information on the cameras connected to the different channels with the video resolution and camera firmware version