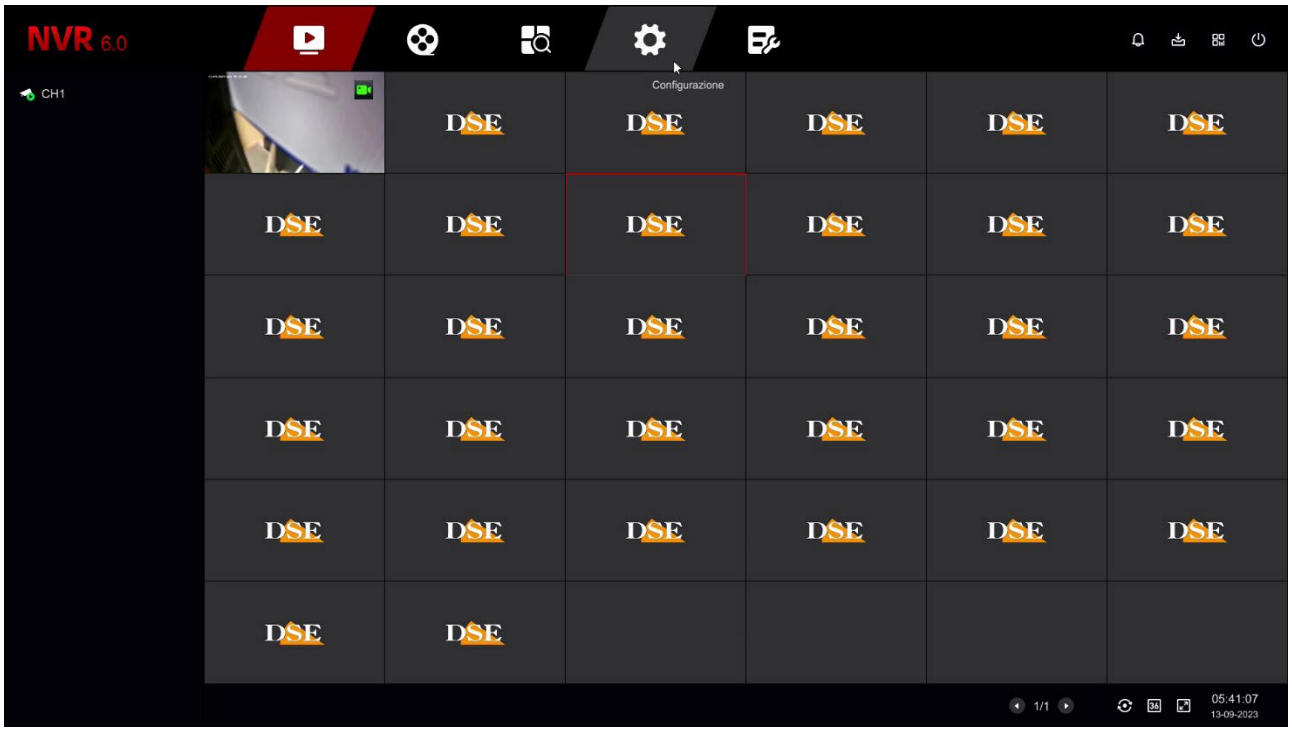
RK and RKK SERIES

DVR and NVR



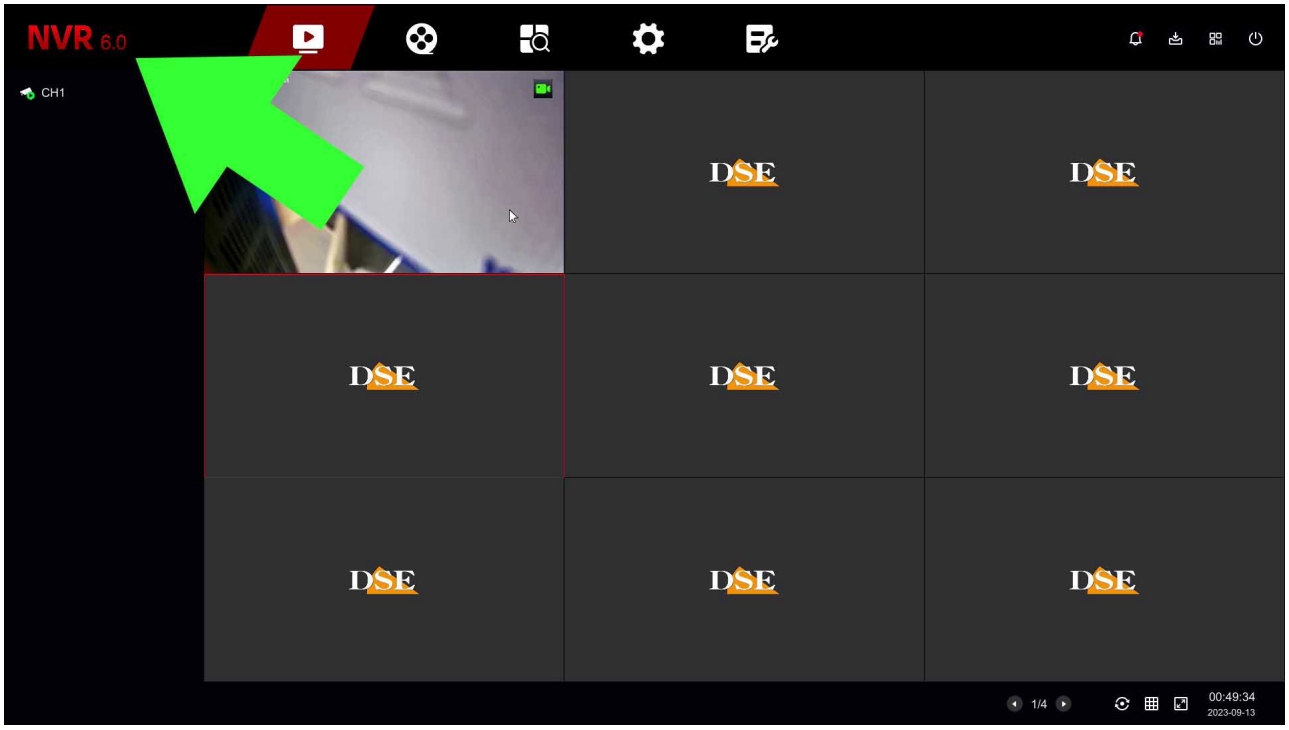
Setup Manual - Menu 6.0

How to configure all system operation options

Contents of the manual

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

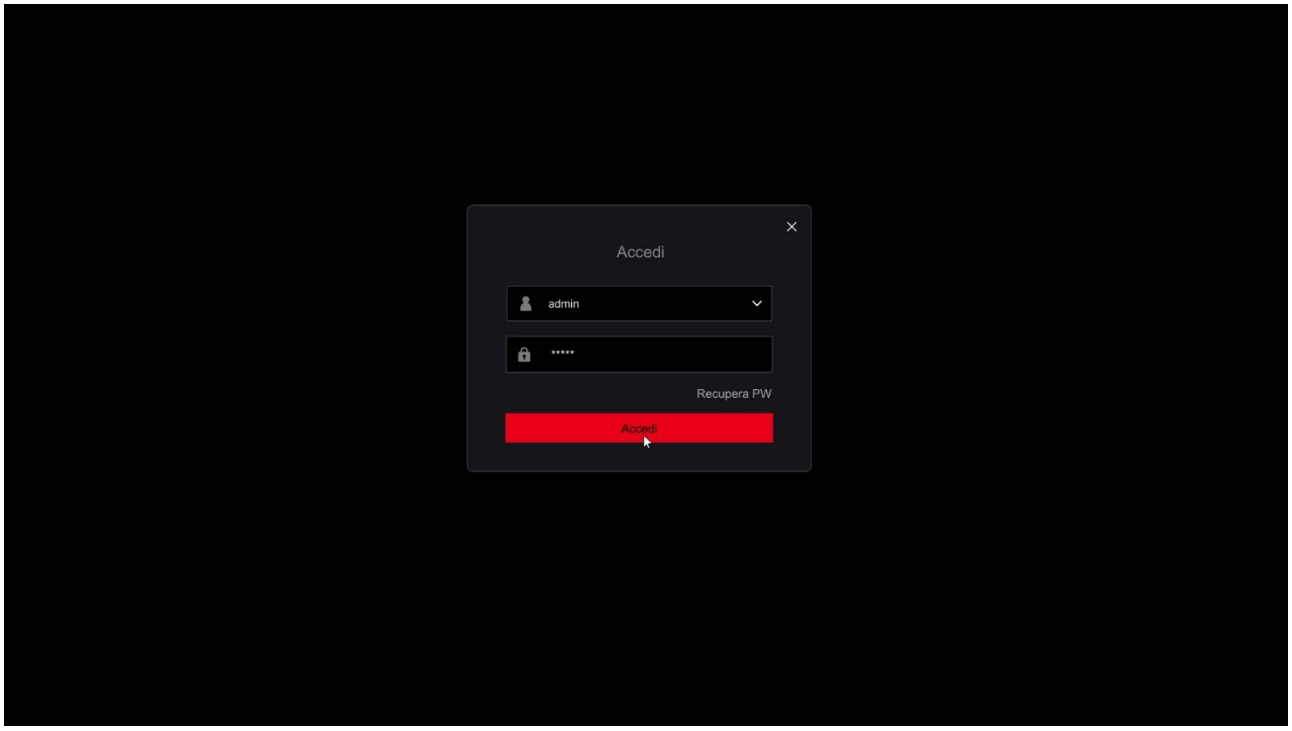
This manual refers to the NVRs with GUI Version 6.0 that you see below



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.

Accessing 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 installed your system yet and you don't see the cameras on your monitor yet, you should take the installation manual and follow the instructions. If you have installed the system and you are able to move the mouse on 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 where you enter your username and password to access.



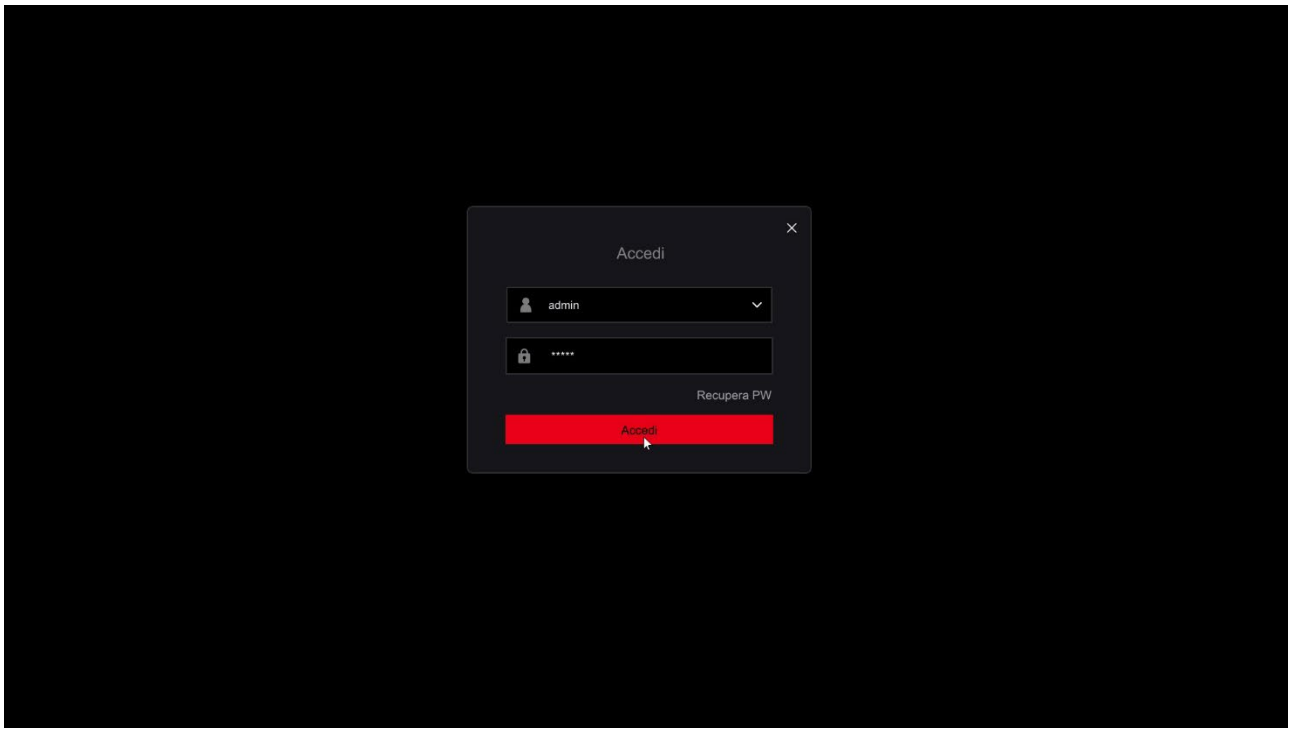
The factory login data for RK Series NVRs and DVRs are:

USER: admin
PASSWORD: 123456

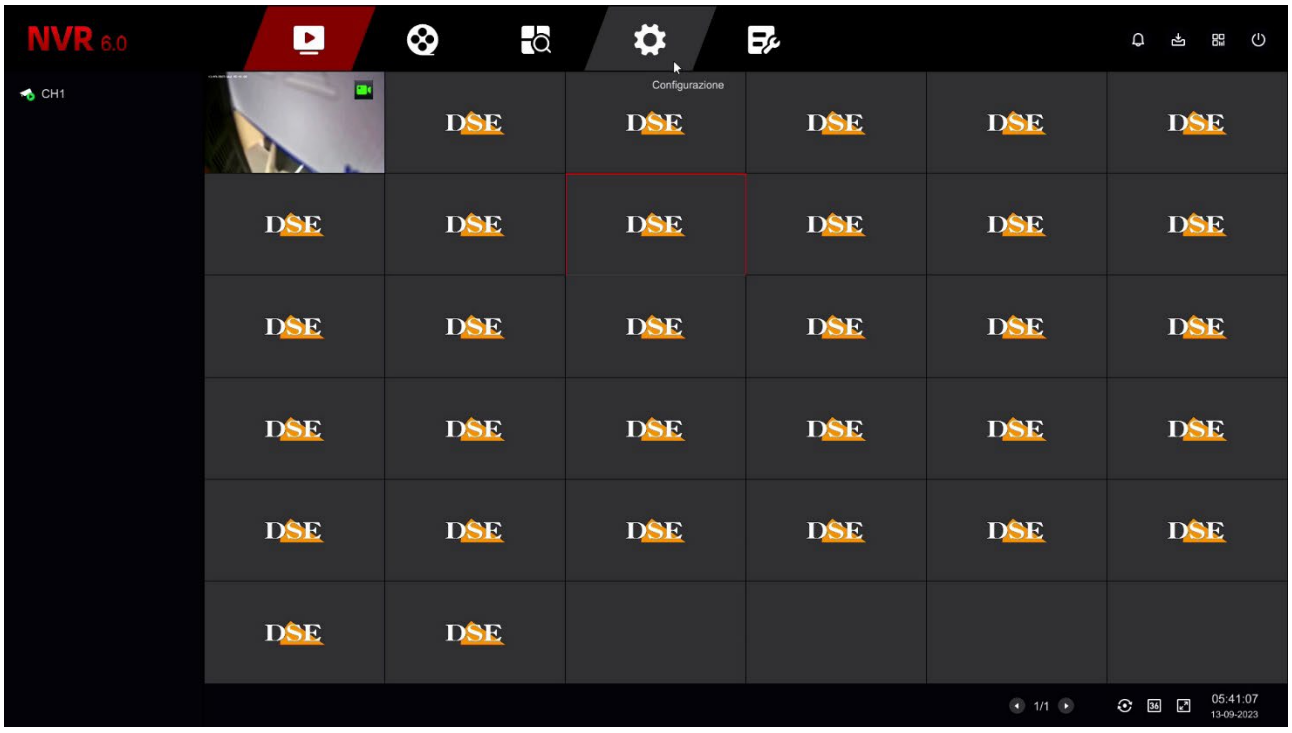
Then press LOGIN.

Some firmware, prior to 2025, use password

USER: admin
PASSWORD: 12345



To access the configuration menu you have to right-click on the screen



Navigation bar

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

LIVE PLAYBACK SEARCH CONFIGURATION MAINTENANCE

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

This manual explains the CONFIGURATION and MAINTENANCE pages

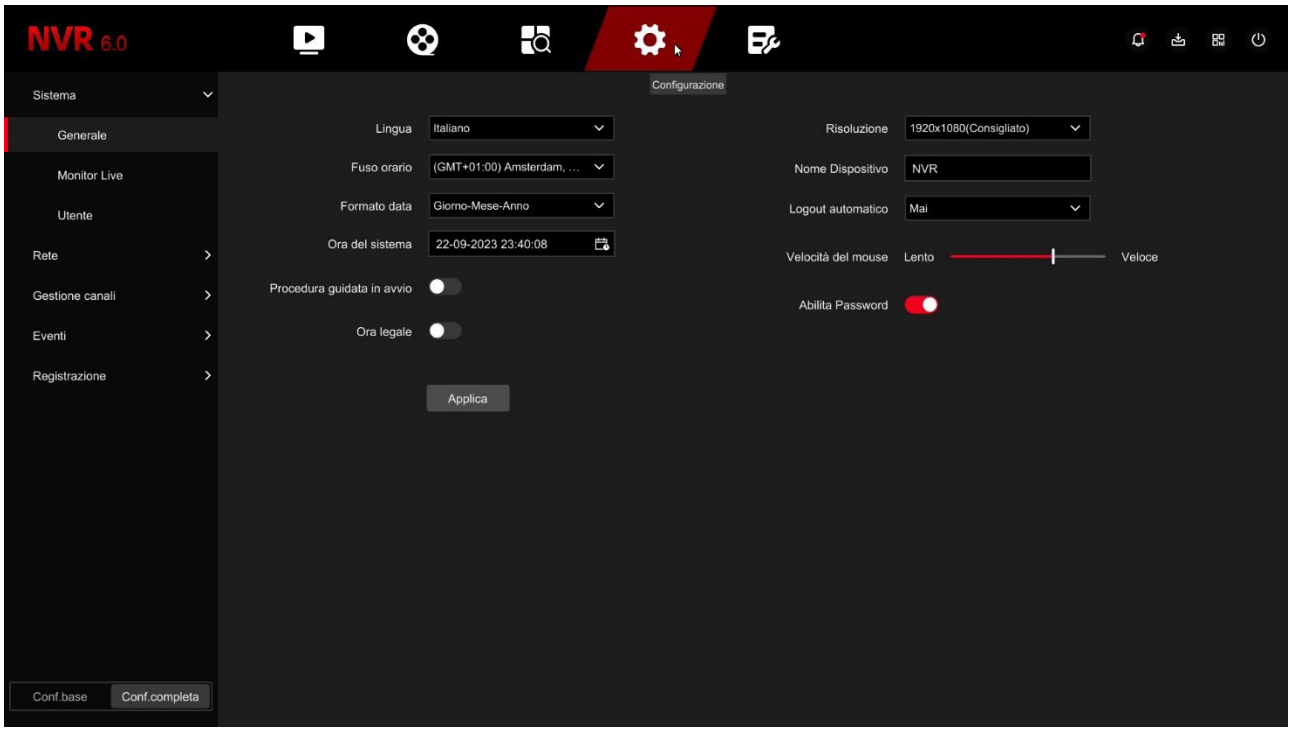
In addition to the main navigation bar, there are buttons at the top right

1 2 3 4

1 – Opens the popup window that lists the latest alarm events, divided into Anomalies, Alarms Normal and Smart 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 shutdown button allows you to log out (you will be required to log in again), turn off the device and restart it.

CONFIGURATION | SYSTEM

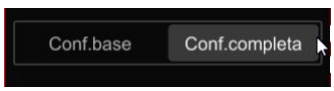
Click the CONFIGURATION button to open the page containing the configurable options of the your NVR/DVR



BASIC AND COMPLETE CONFIGURATION

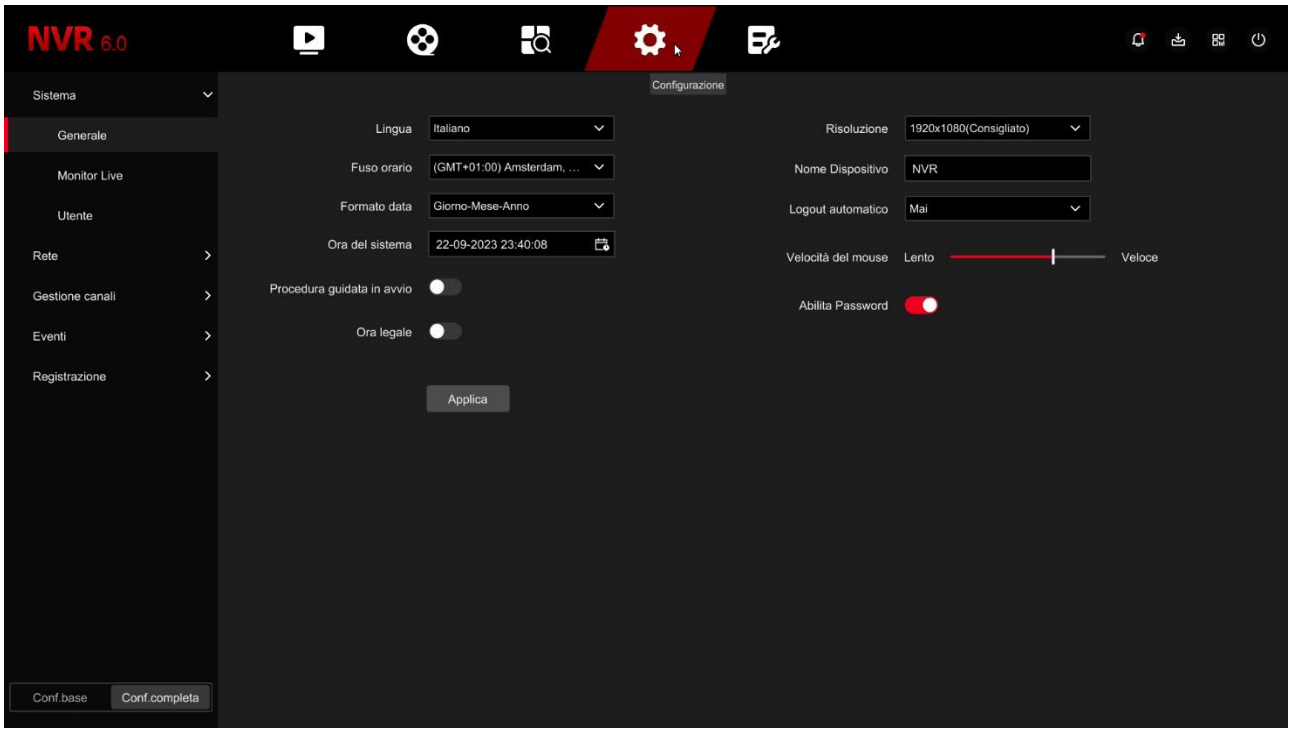
In the lower left corner you can select whether to see the basic configuration or the advanced configuration. The basic configuration shows the most used options, to find them more easily easily. The complete setup includes all options.

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



SYSTEM | GENERAL

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



LANGUAGE – The default 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 – Displays the system date and time which you can change manually

START-UP WIZARD – After completing the installation of the NVR/DVR, you should disable the wizard when starting the video recorder by unchecking it option. The wizard is explained in the installation manual.

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

RESOLUTION – Here you set the resolution of the video outputs for the monitor. Do not set a resolution too high that your monitor does not support. The most common resolution supported by the monitors is the factory 1920x1080.

DEVICE NAME – You can assign a name to your DVR/NVR for easy identification.

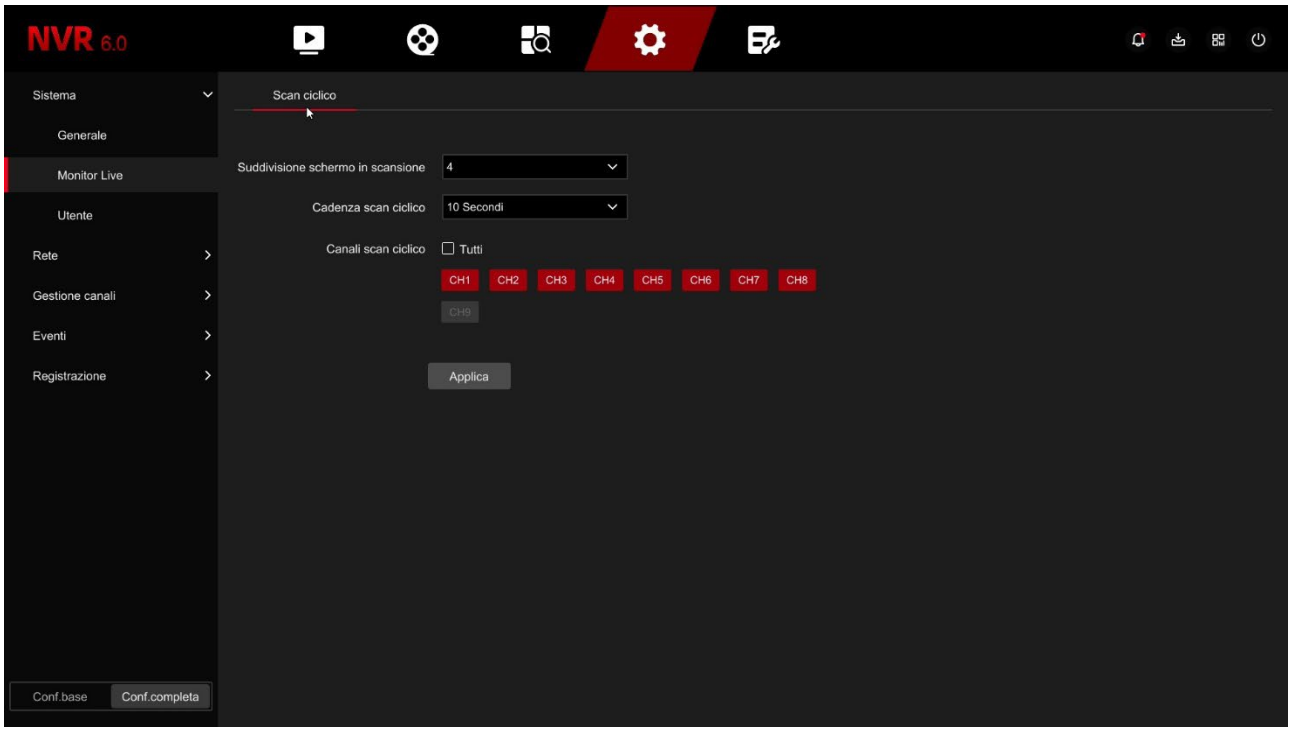
AUTOMATIC LOGOUT – Defines after how many minutes of operator inactivity the system will require a new login to access the NVR.

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

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

SYSTEM | LIVE MONITOR | CYCLIC SCAN

Here you can configure the cyclic scan of the cameras on the monitor. The cyclic scan can be activate and pause with a button in the live window.



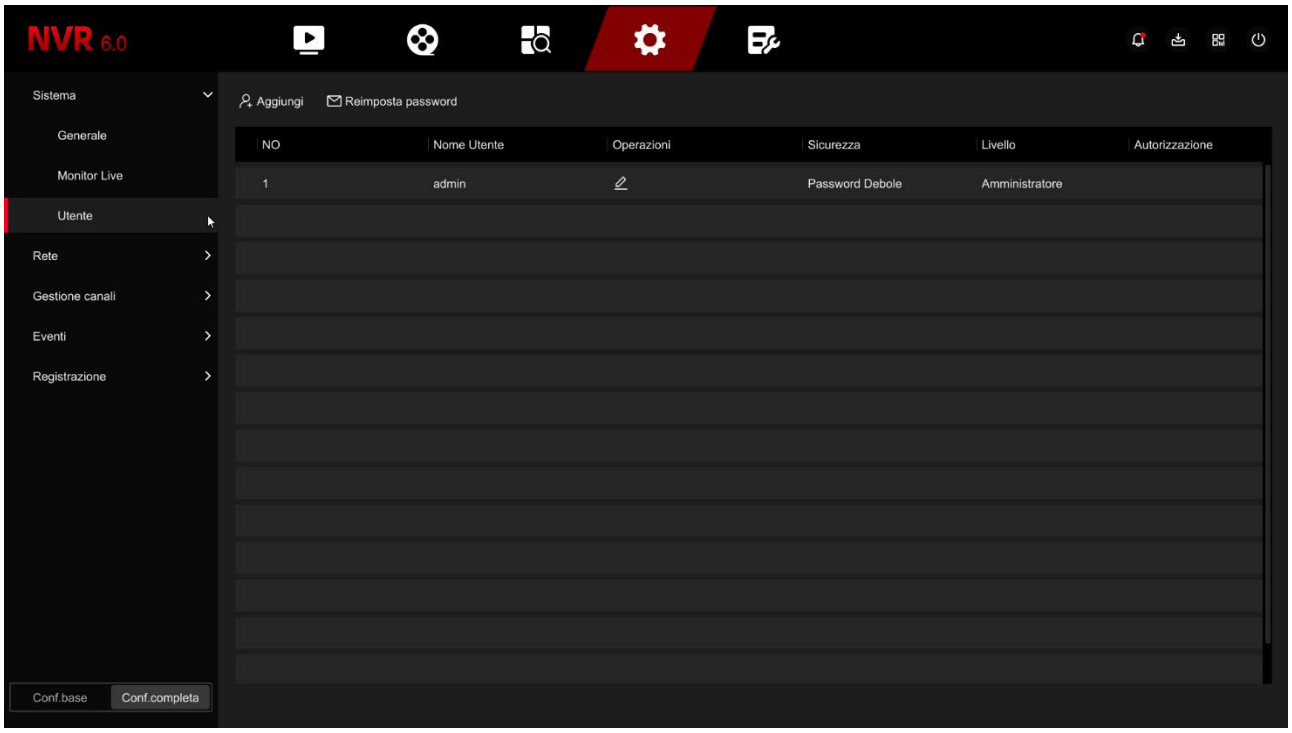
SCREEN DIVISION IN SCANNING – Normally the cyclic scanning is performed by bringing to full screen one camera at a time. To get this feature you need to set this parameter to 1. If you have many cameras you may also want to cycle the multivisions by 4 or 9 cameras at a time.

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

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

SYSTEM | USER

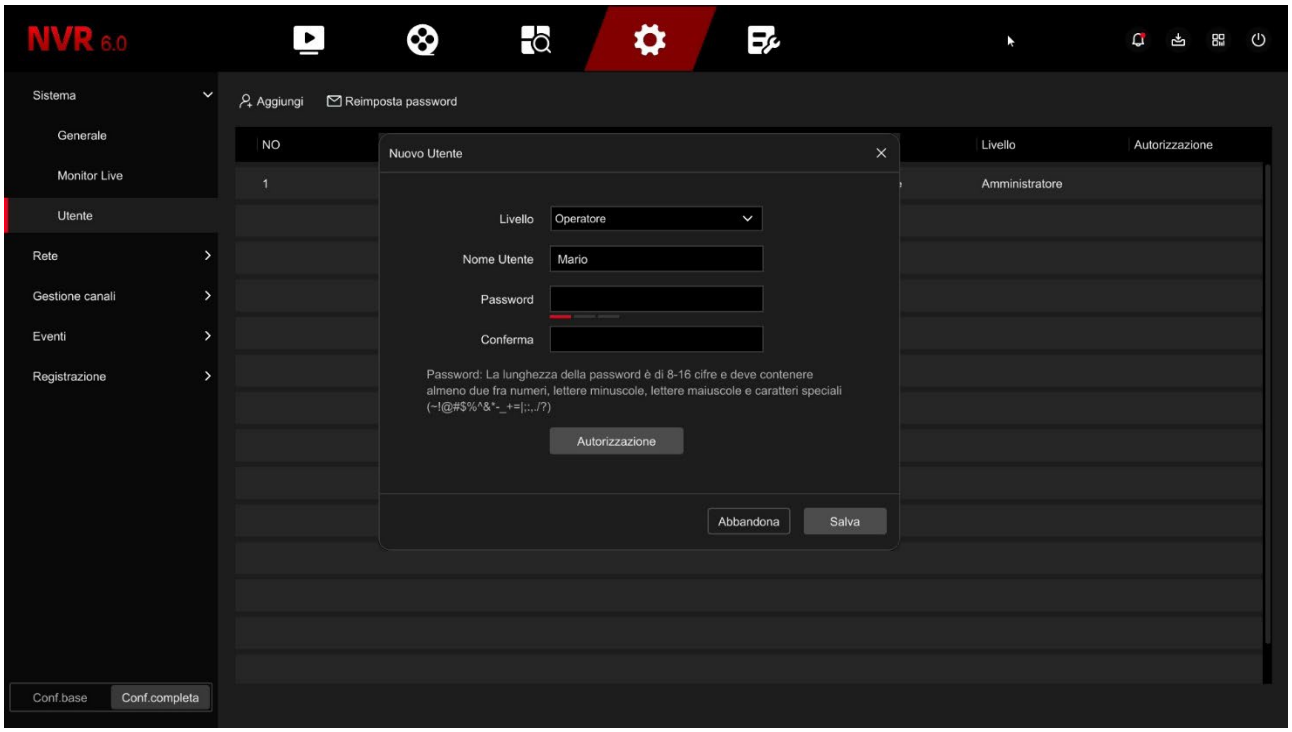
Here the administrator can enter other users who will have access to the device, each with your own access level



RESET PASSWORD – The first button allows you to enter the email address that will be used for a possible future recovery of the forgotten password. It is advisable to enter this email address because this way you can recover the NVR password using the IoVedo.RK app, even without the NVR being connected to the network or loaded into the app.

ADMIN USER – The administrator user is already 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, like you do on cell phones.

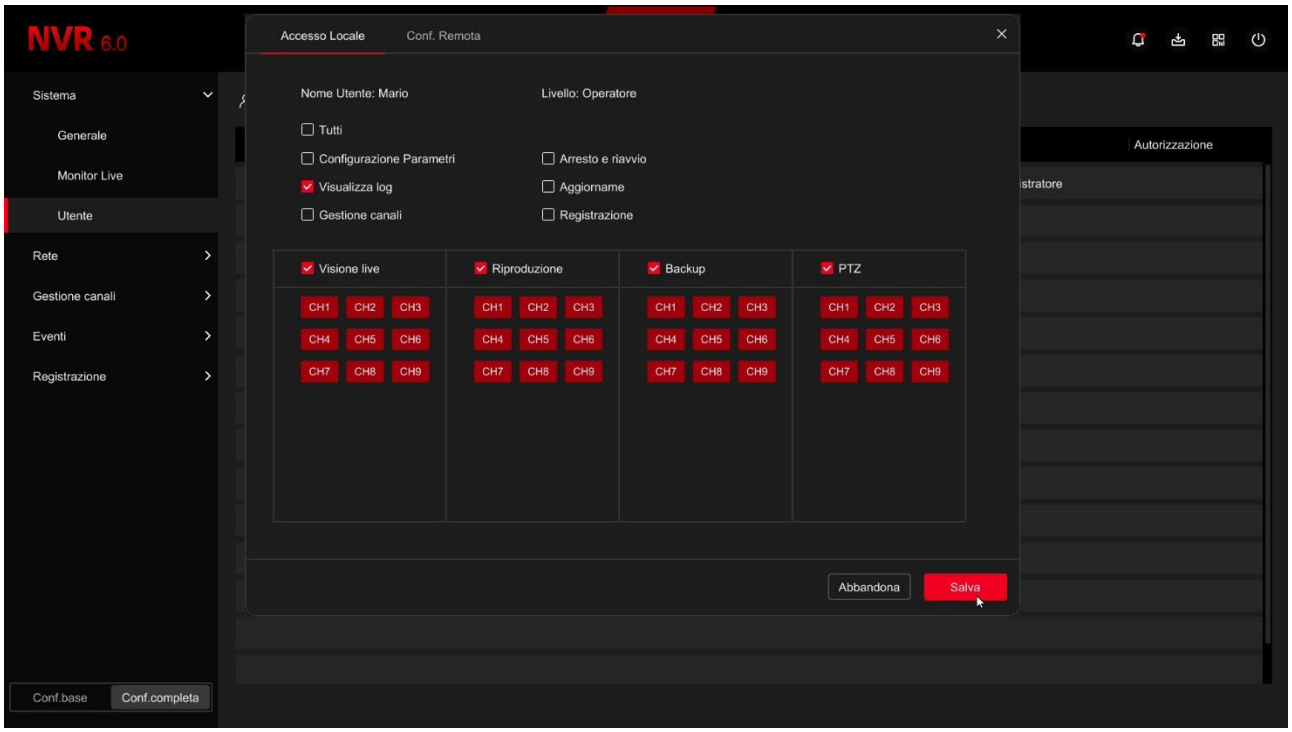
ADD – Press to add a new user



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 you like, for example by 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 features you want to provide to the new user.

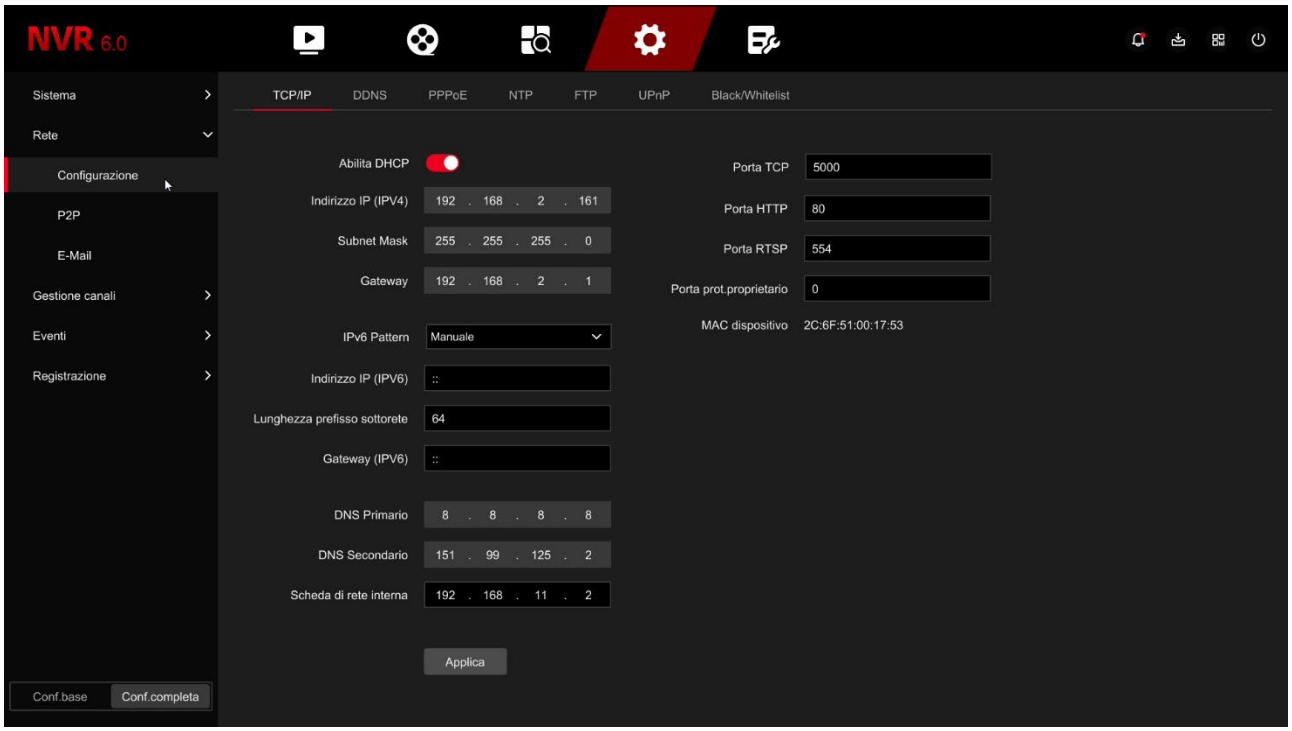

NVR 6.0
Sistema
Generale
Monitor Live
Utente
Rete
Gestione canali
Eventi
Registrazione
Conf.base
Conf.completa
Accesso Locale
Conf. Remota
Nome Utente: Mario
Livello: Operatore
Tutti
Configurazione Parametri
Visualizza log
Gestione canali
Arresto e riavvio
Aggiorname
Registrazione
Visione live
Riproduzione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

CONFIGURATION | NETWORK

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

NETWORK | CONFIGURATION | TCP/IP

In this section you can enter the network data of the NVR.

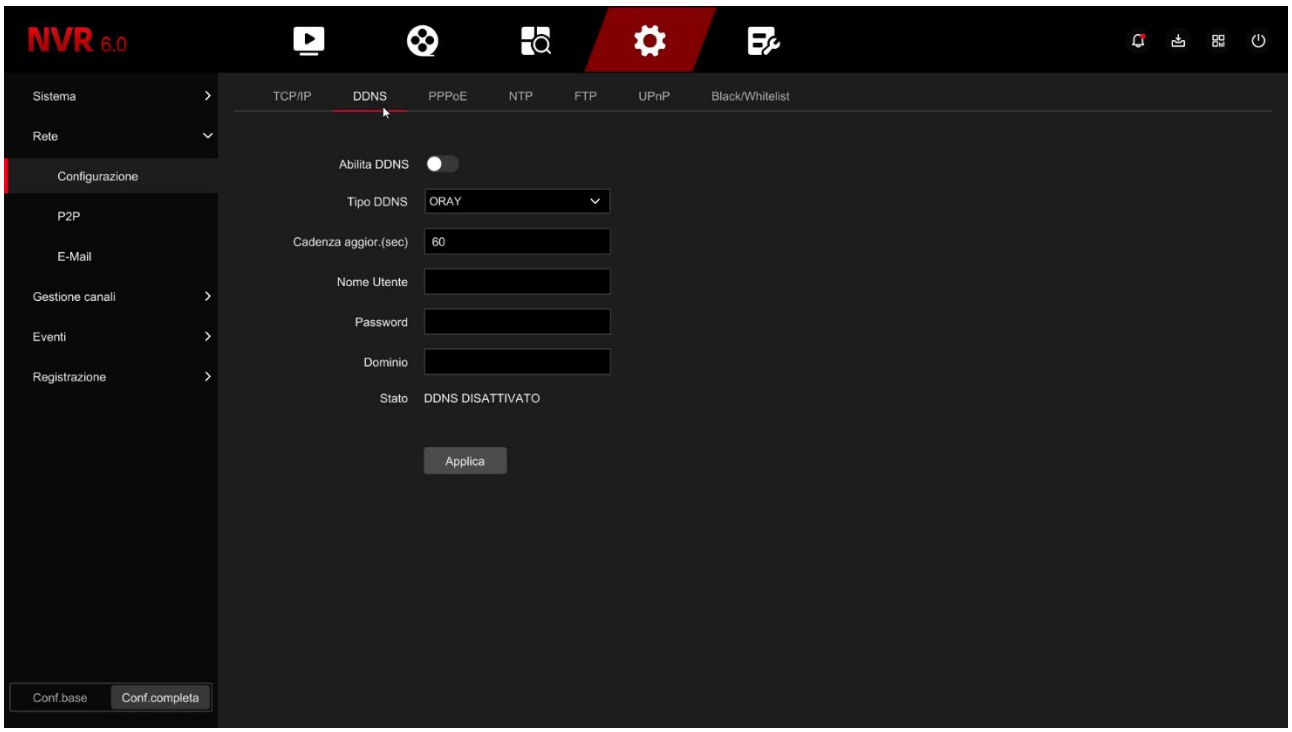


NETWORK ADDRESSES – IP address, Subnet mask, Gateway and primary and secondary DNS are the addresses that allow your DVR/NVR to communicate with the network. The easiest thing is to keep the factory setting with DHCP enabled so that the device configures itself automatically on the network. To use this 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 need to enter the parameters manually, do your research before doing so. because entering 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 being the same and the same subnet mask (usually 255.255.255.0). The gateway is usually the router address, the number 1 of the network (for example 192.168.1.1). DNS is important for the DVR/NVR to be able to 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 present in this window

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

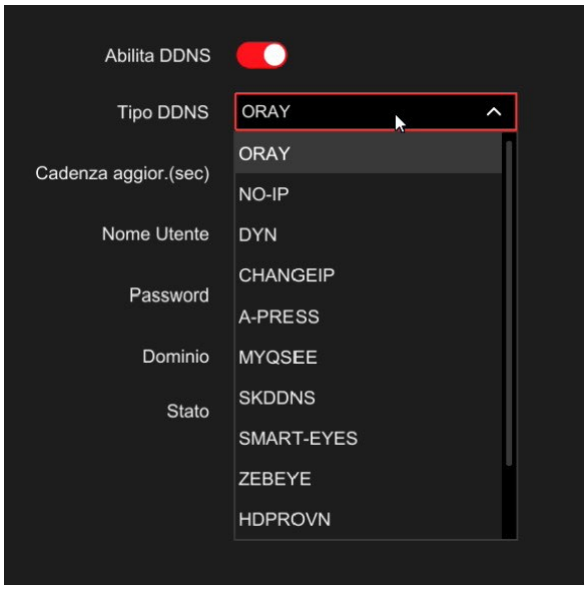
PORTS – Here are the ports used by the NVR/DVR for network communication.
in the use of TCP, HTTP (ONVIF), RTSP protocols. Our private protocol, used by the app and from the IoVedo.RK software, it uses port 6000 by default. It is advisable never to change it these communication ports.
MAC DEVICE – Unique 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 it does this function very well. However, video recorders support different DDNS services and you can set the connection data in this folder, if you intend to use them.

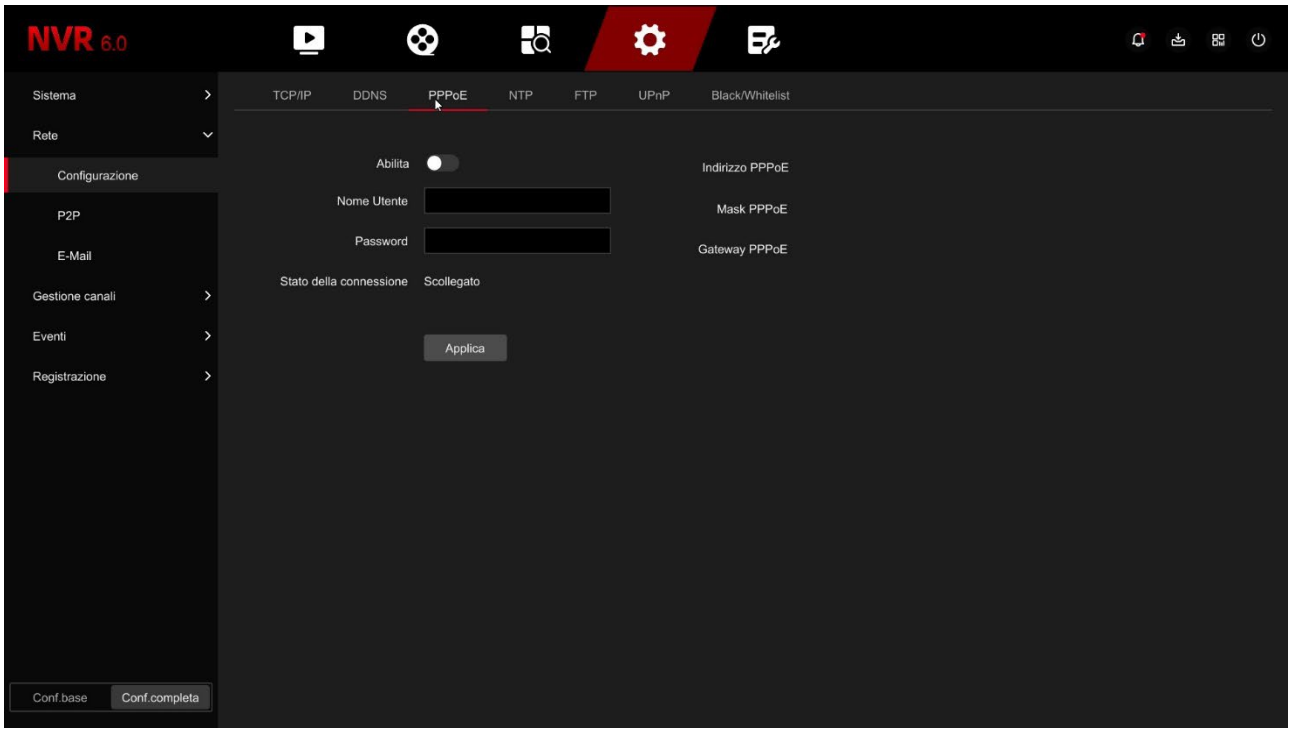
Remember that if you use a DDNS service, instead of our P2P cloud you will have to map properly configure the ports in the router to be able to communicate with the DVR/NVR.



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

NETWORK | CONFIGURATION | PPPOE

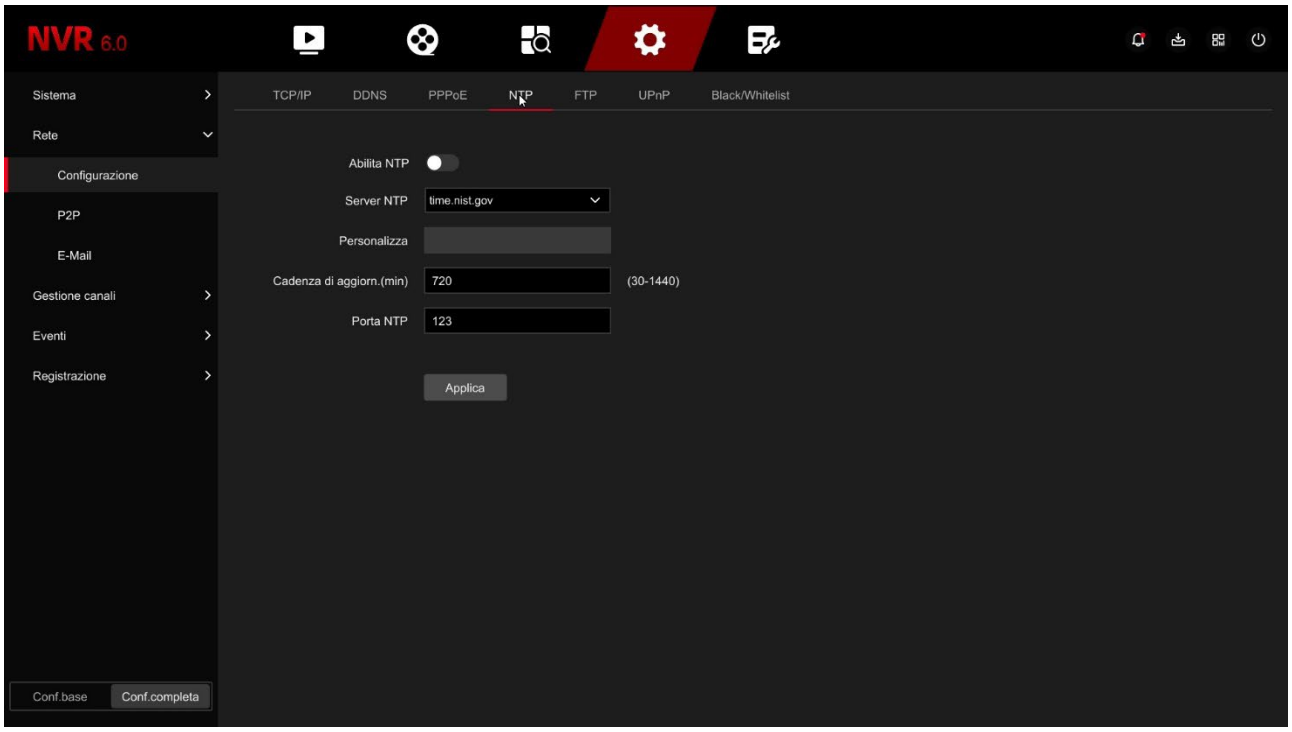
NVR/DVR can be connected directly to an ADSL modem to connect to the Internet by making a call (dial-up) and entering the credentials.



Normally you won't need this page because nowadays it's preferable to use routers for Internet access and this protocol is not necessary

NETWORK | CONFIGURATION | NTP

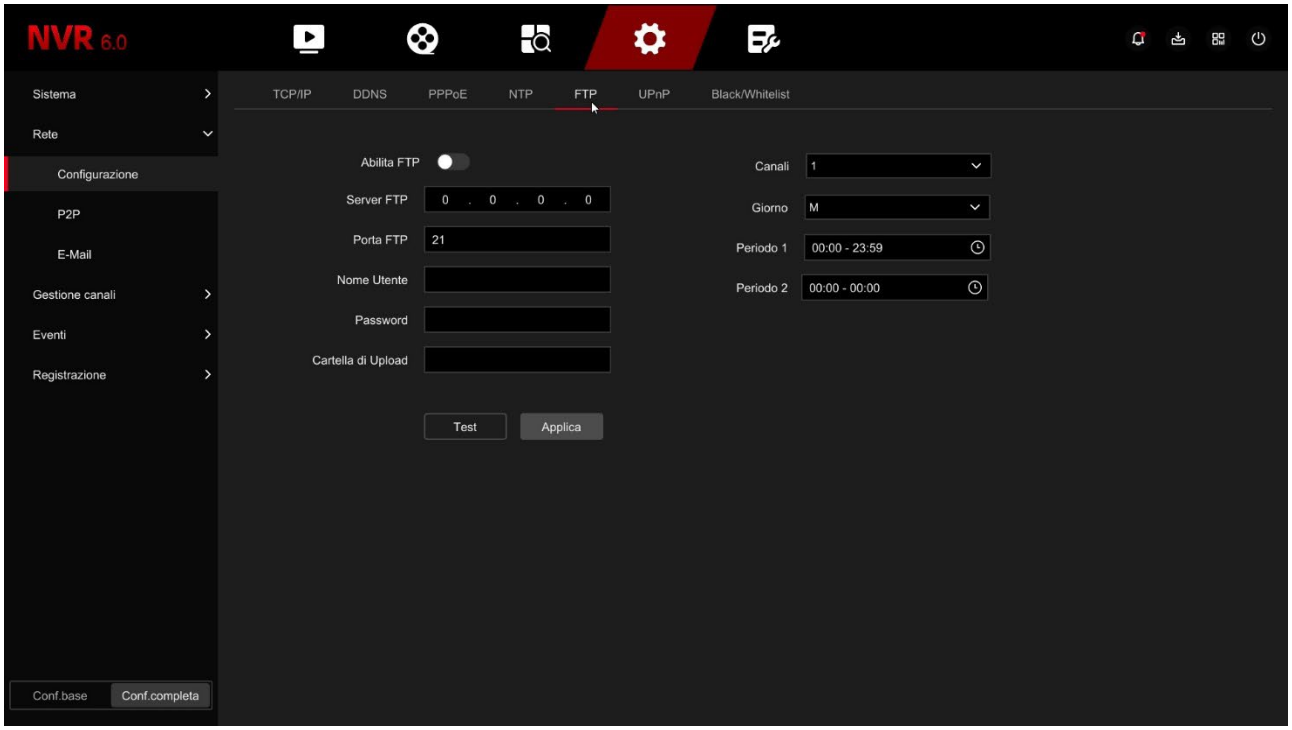
The NTP protocol is used to automatically synchronize the NVR time via the Internet.



If you enable NTP protocol management, the NVR will synchronize the time via the Internet with an NTP server.
SERVER - Listed are the most popular free servers for time synchronization. You can also 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 is a useful feature if you have a web space where you can store important images.



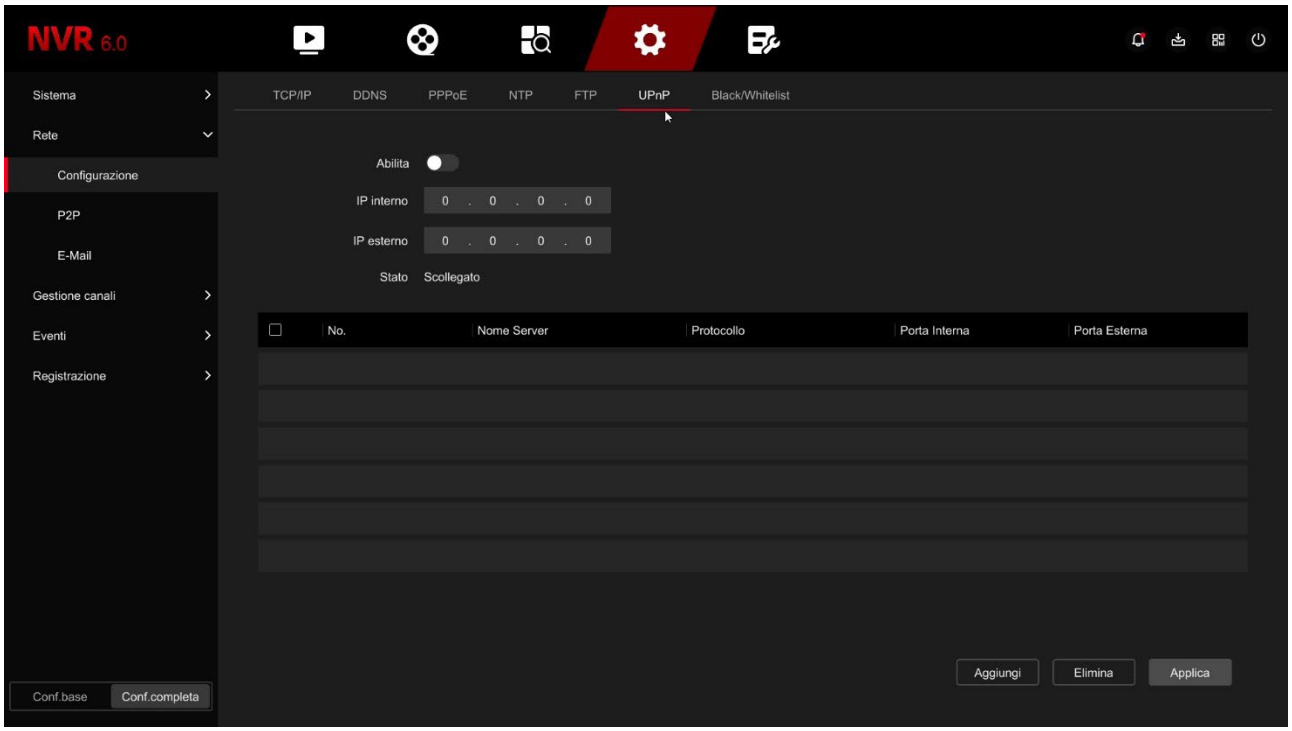
FTP SERVER/PORT – These are the main data of your FTP space
USERNAME/PASSWORD – Access credentials to your FTP space
UPLOAD FOLDER – Enter the name of the folder where to store the files on the FTP server
CHANNELS/DAY/PERIOD 1-2 – You can enable sending files only in certain time slots depending on of 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 need to map the router ports so that the ports used by the

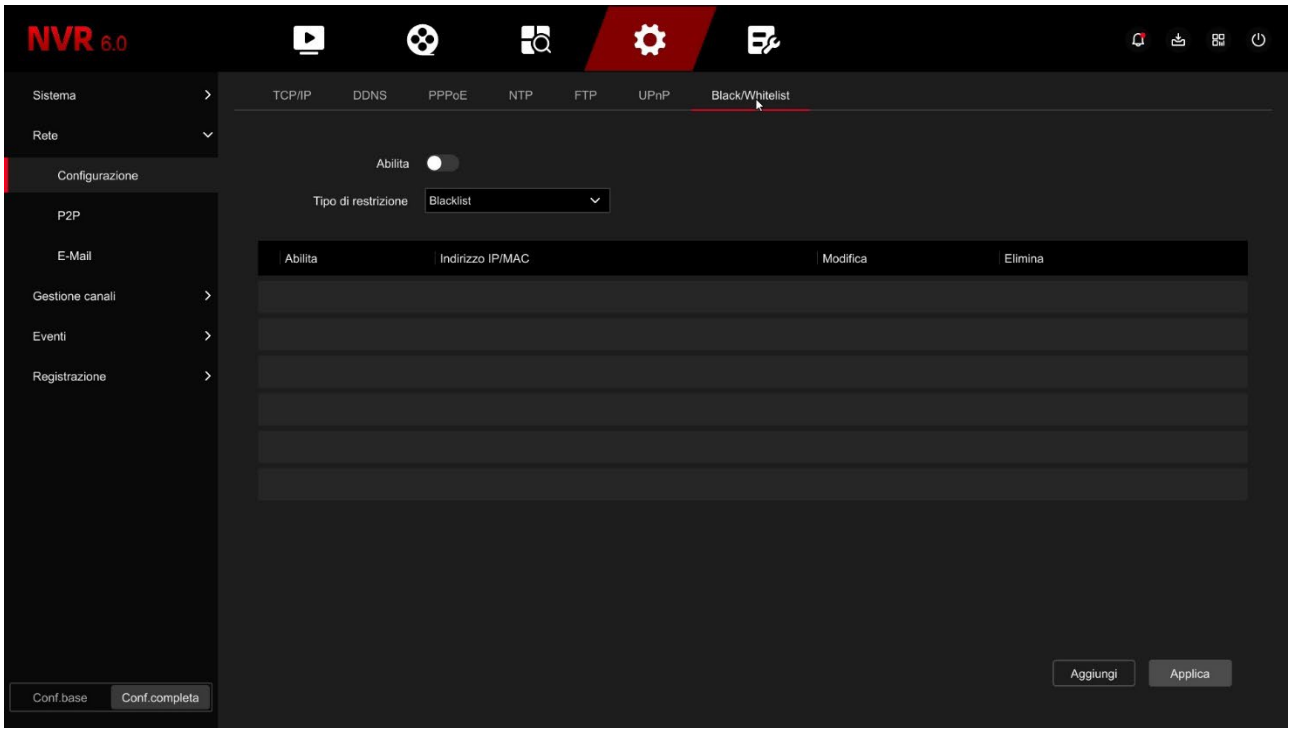
DVR/NVR (factory 80,5000,554,6000) are transferred from the Internet side to your DVR/NVR on the internal network.

It would be best 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 that it is done automatically.



NETWORK | CONFIGURATION | BLACK/WHITELIST

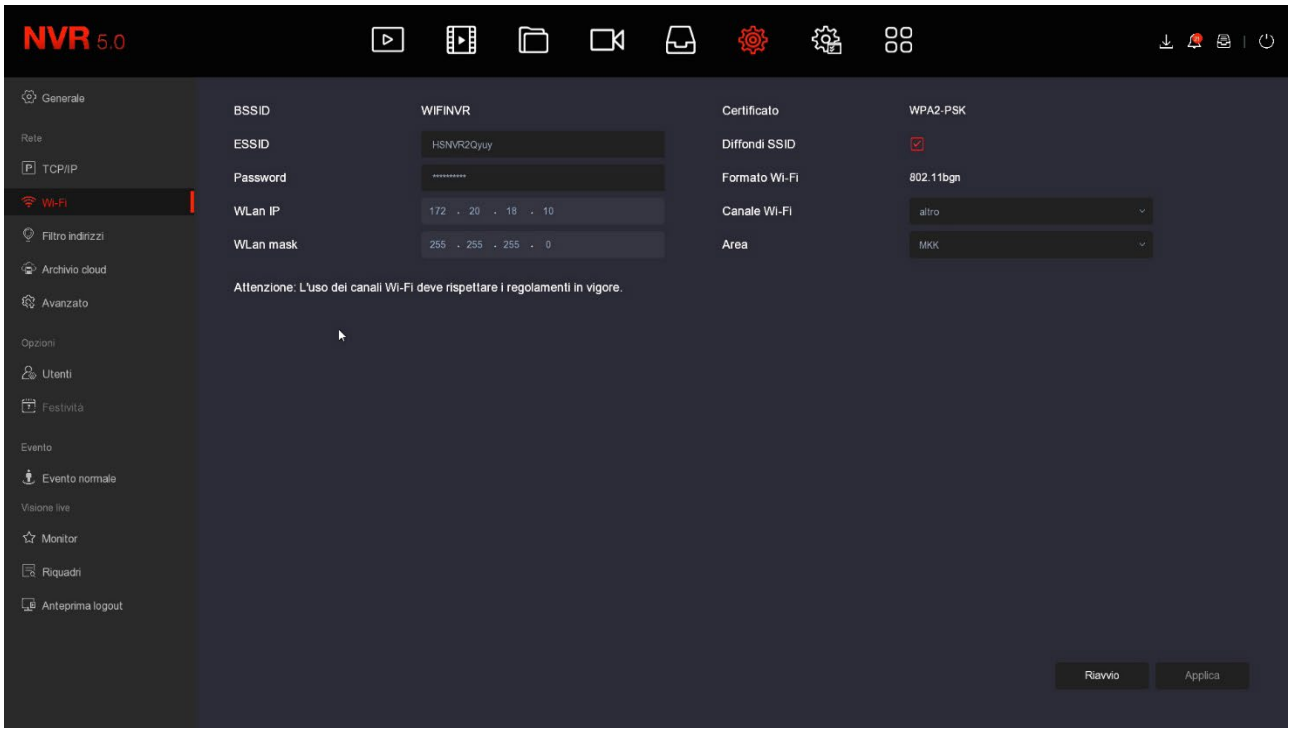
On this page you can allow or deny remote connection to your DVR/NVR based on to the IP address or Mac Address of the client making the connection. It is useful for restricting the possibility of remote access to authorized IPs only.



If you use the BLACKLIST mode you can then add all the IP addresses or MAC addresses that 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 that are allowed access, 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 – This is the name that distinguishes the wifi network generated by the NVR

PASSWORD – This is the access password to connect to the NVR WiFi network. Default "lspassword"

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

CERTIFICATE – This is the security encryption used by the NVR's wifi network

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

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

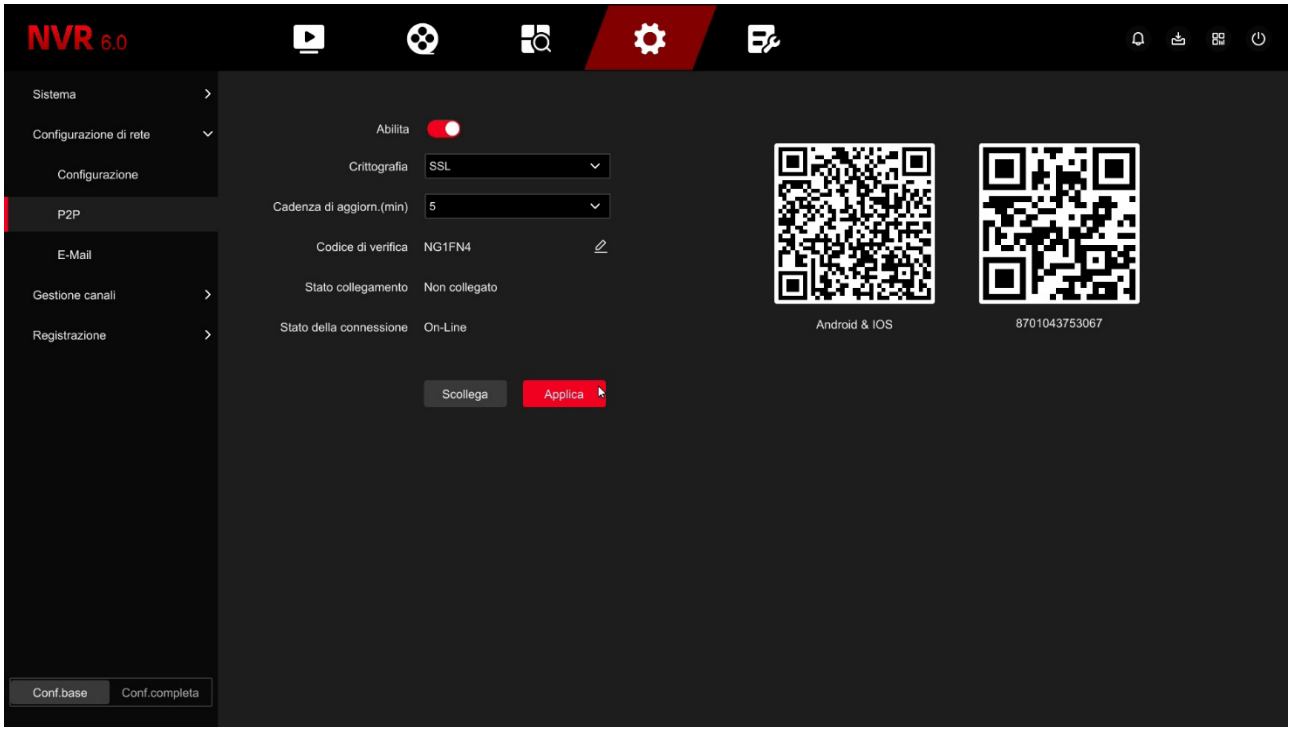
WIFI CHANNEL – Here you set the WiFi channel to use for communication with the cameras. By default, it is best to keep the automatic factory option. However, it is possible to force the communication on a specific channel from 1 to 13. Setting a specific WiFi channel can help to avoid frequencies disturbed by the presence of other devices. If you encounter 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 PC and mobile phones. In the access manual remotely you will find the explanation of the operation and the explanations on how to use our app

ISee.RK



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

ENCRYPTION – It is recommended to keep the factory SSL encryption

UPDATE CADENCE – This is the waiting interval between sending a push notification to the app IoVedo.RK and the next one. It is advisable to keep a delay of 5 or 10 minutes to avoid receive too many notifications and not to exhaust the maximum number of 100 notifications/day per channel expected.

VERIFICATION CODE is the captcha code that is needed to be able to load the device into our app IoVedo.RK. 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 device to be able to added to the app without requiring the captcha enter the code ABCDEF in this box.

CONNECTION STATUS - shows if the device has already been connected to an account on the app IoVedo.RK. If the device is linked to an account, you can disconnect it with the UNCONNECT button to re-pair it to a different account.

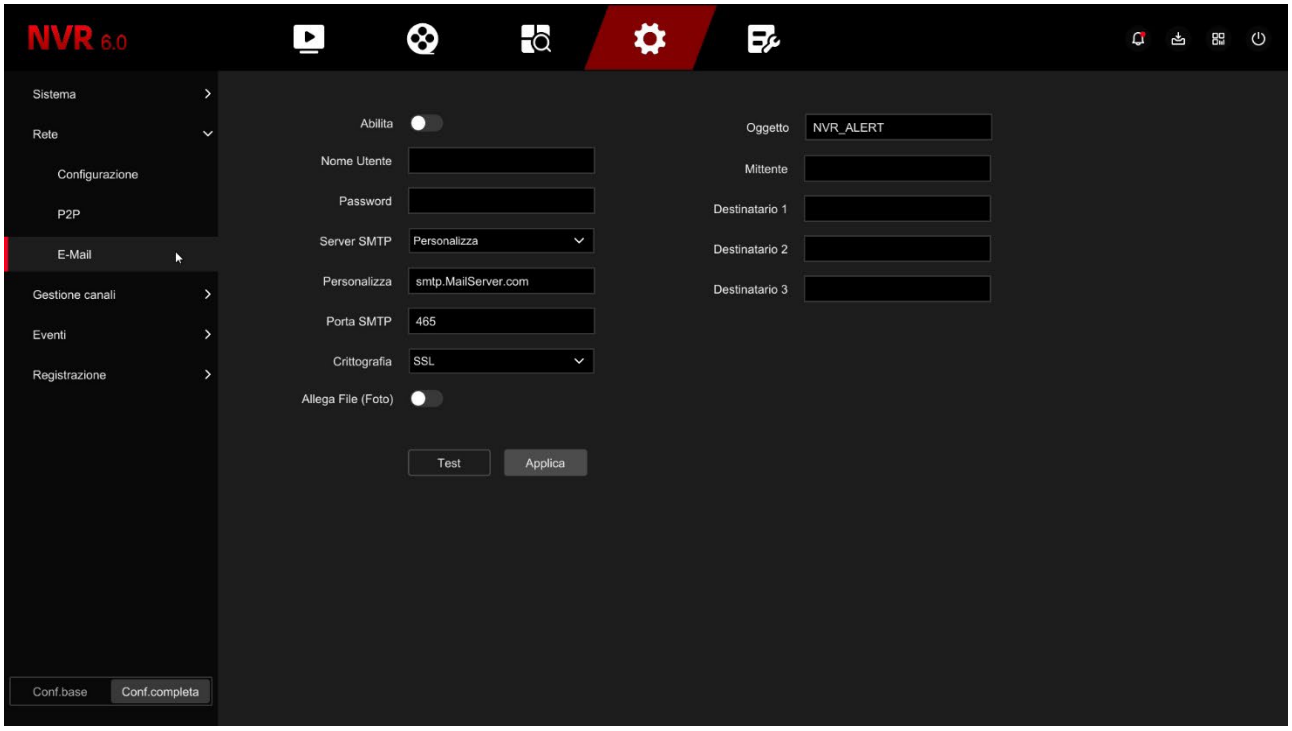
CONNECTION STATUS – shows the connection status to the P2P server.Connected, It means that the system is connected to our P2P server successfully.Not connected indicates instead you can't connect remotely to the cloud because the NVR doesn't see the Internet network.

Always check the status of your cloud connection before attempting to connect via the Internet. If the server is offline, it is most likely that the DVR/NVR network settings are not are correct. Then enable the DHCP function in the network settings and reboot the device, in so that the DVR/NVR automatically receives the correct settings from your router. Then Please check in this section if the P2P server is connected.
QR CODE – The first QR code on the left can be framed with your mobile phone to download the APP IoVedo.RK for iOS or Android. The second QR code is used instead in the app configuration to quickly load the serial number of the DVR/NVR. This serial number is composed 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 VCR and on the packaging.
UNCONNECT - If your device is linked to an app account that is not yours, such as your previous owner, you can disconnect it with the DISCONNECT button to be able to recharge it in your account.

IPEYE is not used

NETWORK | EMAIL

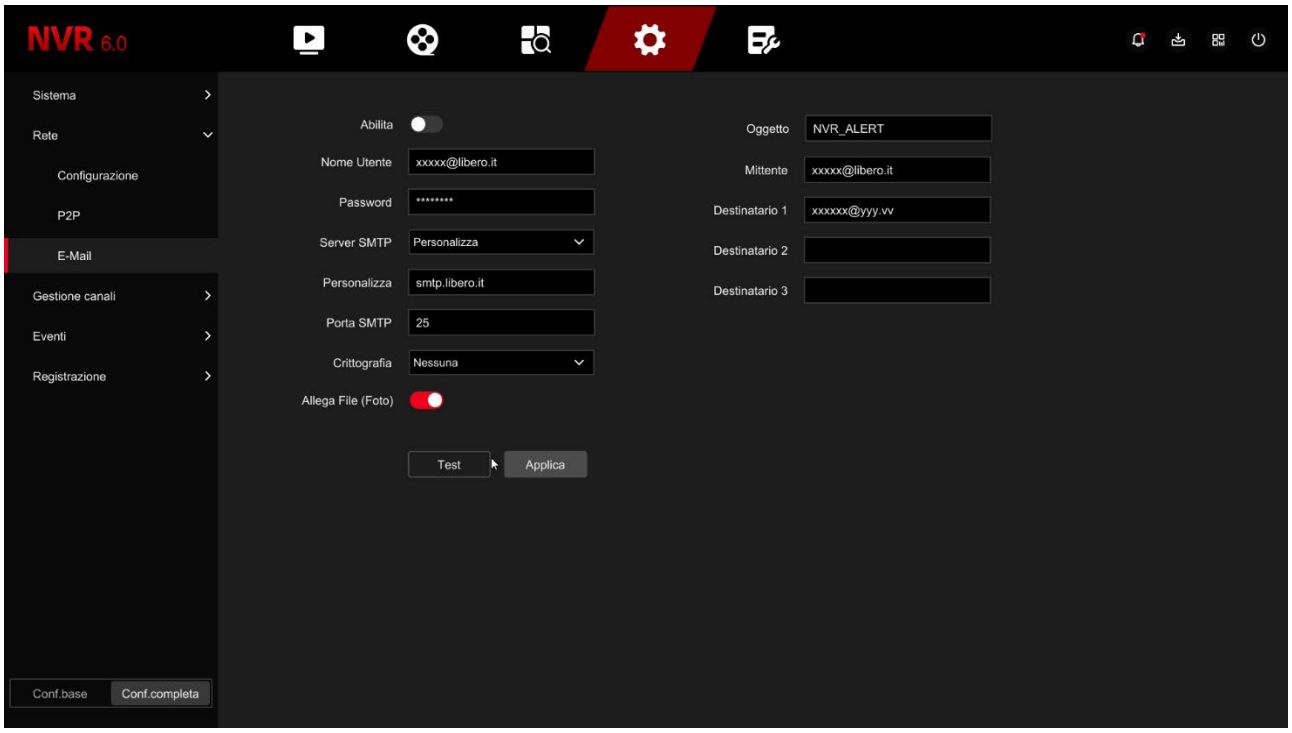
In this section you can enter the necessary data to make your NVR/DVR send email in case of alarm. You should consult your email provider to find out what data enter to communicate correctly with the SMTP outgoing mail server.



USERNAME/PASSWORD – These are your login credentials, to be used if your provider requires SMTP server authentication
SMTP SERVER/SMTP PORT – These are the main data needed to communicate with your SMTP server. for sending emails and your email account provider must provide them to you.
ENCRYPTION – Several providers use encryption in the SMTP protocol. It is essential to enter here is the encryption used by your provider (SSL or TLS). Note that mail providers often have of different access modes, 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 – Enter 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 from DVR/NVR
RECIPIENTS – You can enter here the recipients to whom the email will be sent in case of an alarm. You can enter up to 3 recipients.
TEST – Before saving, do a test send with this TEST button.

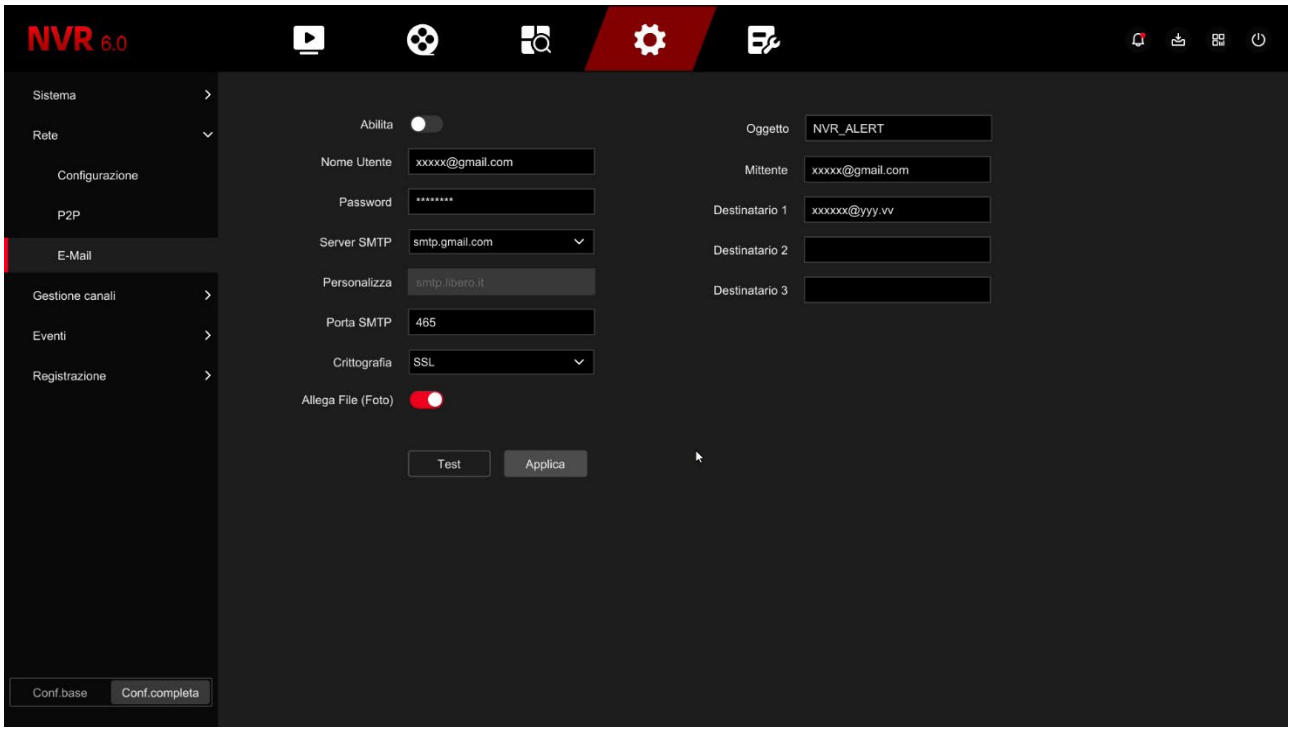
If the test fails, do not contact our support thinking that the device is not working.
Remember that sending emails depends only to a small extent on the NVR and to a large extent on the your smtp provider. It is important to use the correct parameters for your provider and sometimes you also need to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

Here below is an example of an effective configuration that you can create by creating a free account on**FREE.IT**and using their unencrypted SMTP server on port 25.

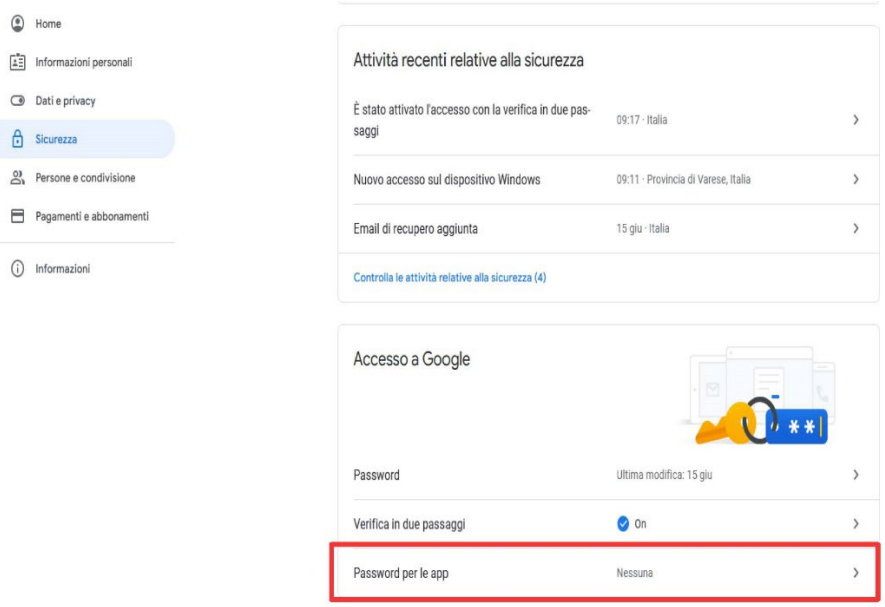


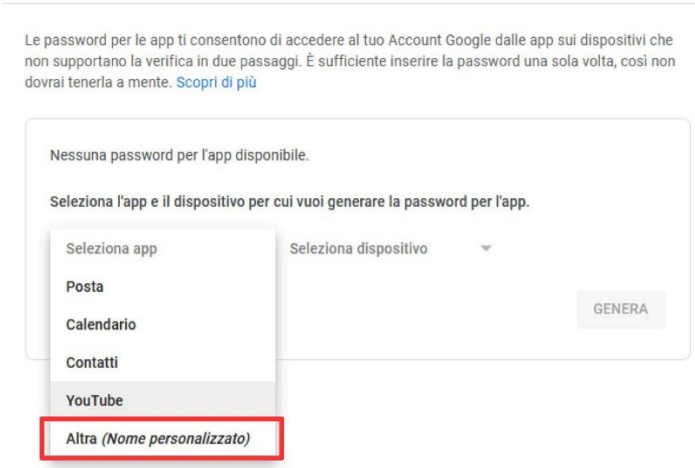
The widespread provider**GMAIL**It can be used to send emails from automatic devices such as NVR and DVR, but requires a more complex procedure to bypass the double authentication that NVRs they cannot carry out.

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 mailbox and generate a so-called PASSWORD FOR THE APP





Once you have obtained the special password for the apps you will need to use it in the NVR email panel

ADVISE

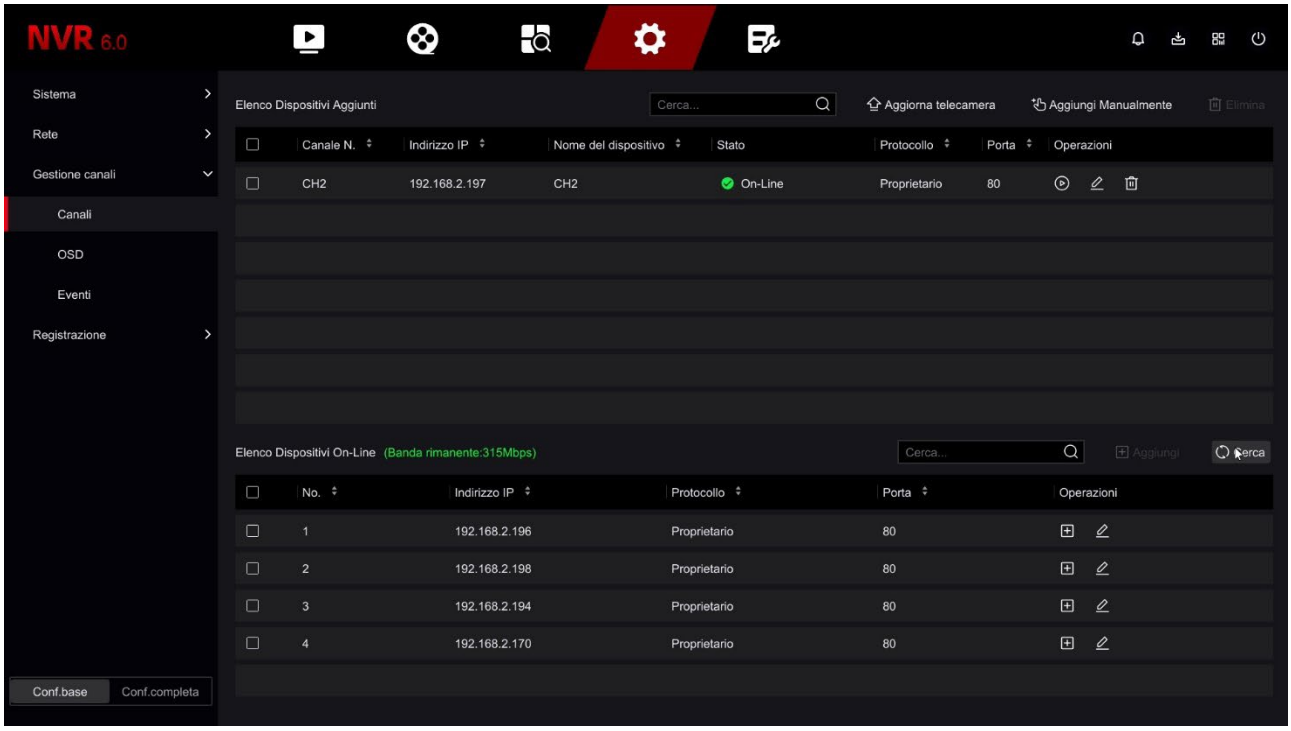
If you can't get success with your usual SMTP provider, don't go crazy looking for correct settings for that provider. You can try other free accounts on the net, like libero.it or email.it. You don't necessarily have to use their POP3 mailbox to receive emails, but you can limit yourself to use only SMTP for sending.

CONFIGURATION | CHANNELS

Click the CONFIGURATION button then CHANNEL MANAGEMENT to configure the cameras

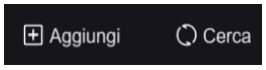
CHANNELS

In this section you can upload IP cameras and configure channels

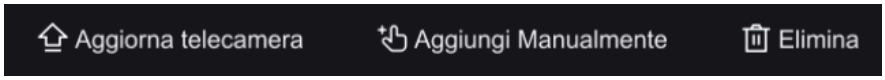


In this section you can add IP cameras to your NVR/DVR.

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



This manual describes the other commands in the section



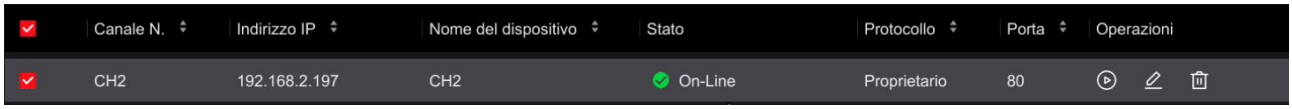
UPDATE CAMERA – With this button you can update the firmware of one or more cameras. cameras with a DSE update file that needs to be copied to a connected USB stick

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 – Deletes 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

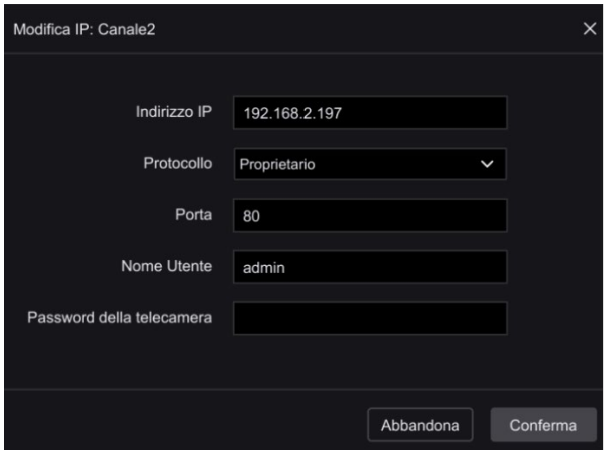
STATUS – Shows a yellow triangle if the connection is not in progress or a green dot if the camera is connected.

PROTOCOL – Indicates the protocol used to communicate with the camera. Normally, it is 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

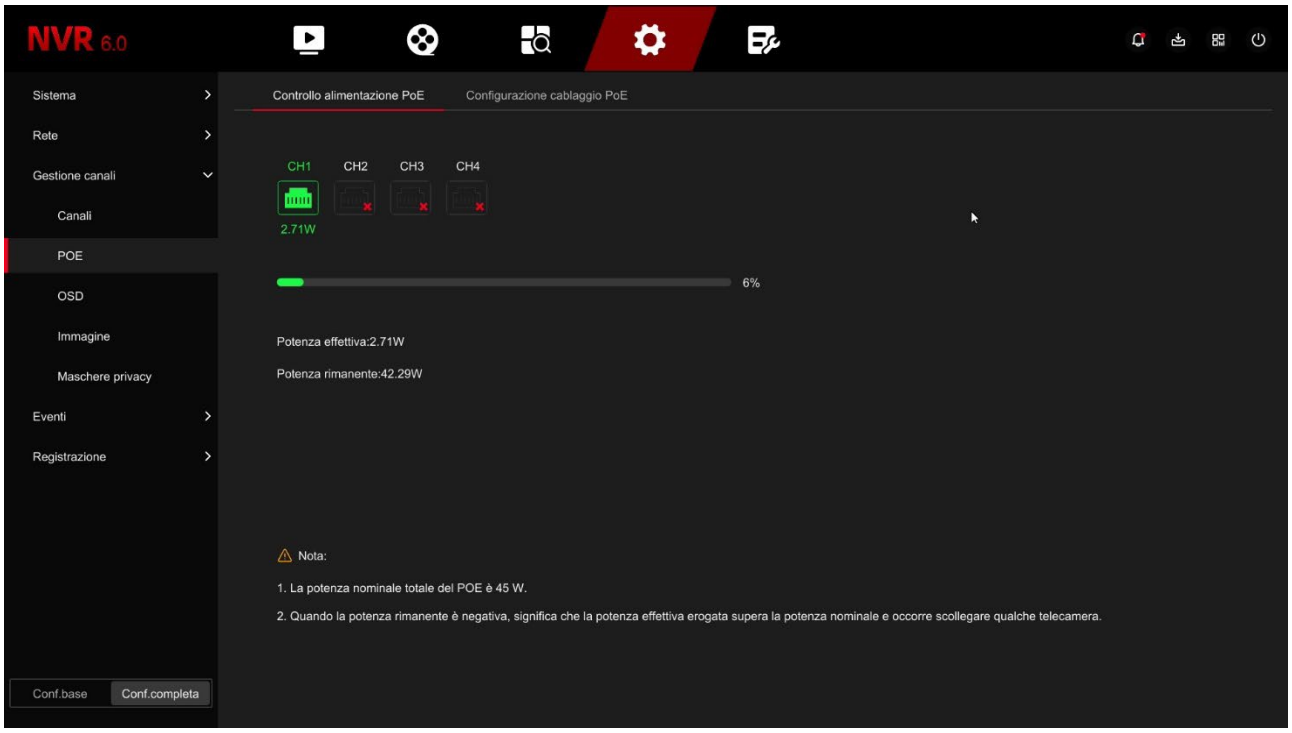
EDIT ICON – You can manually edit the camera connection data



DELETE ICON – Deletes the camera and frees the channel

POE | POE POWER CONTROL

This section is only available in NVRs with built-in POE ports.



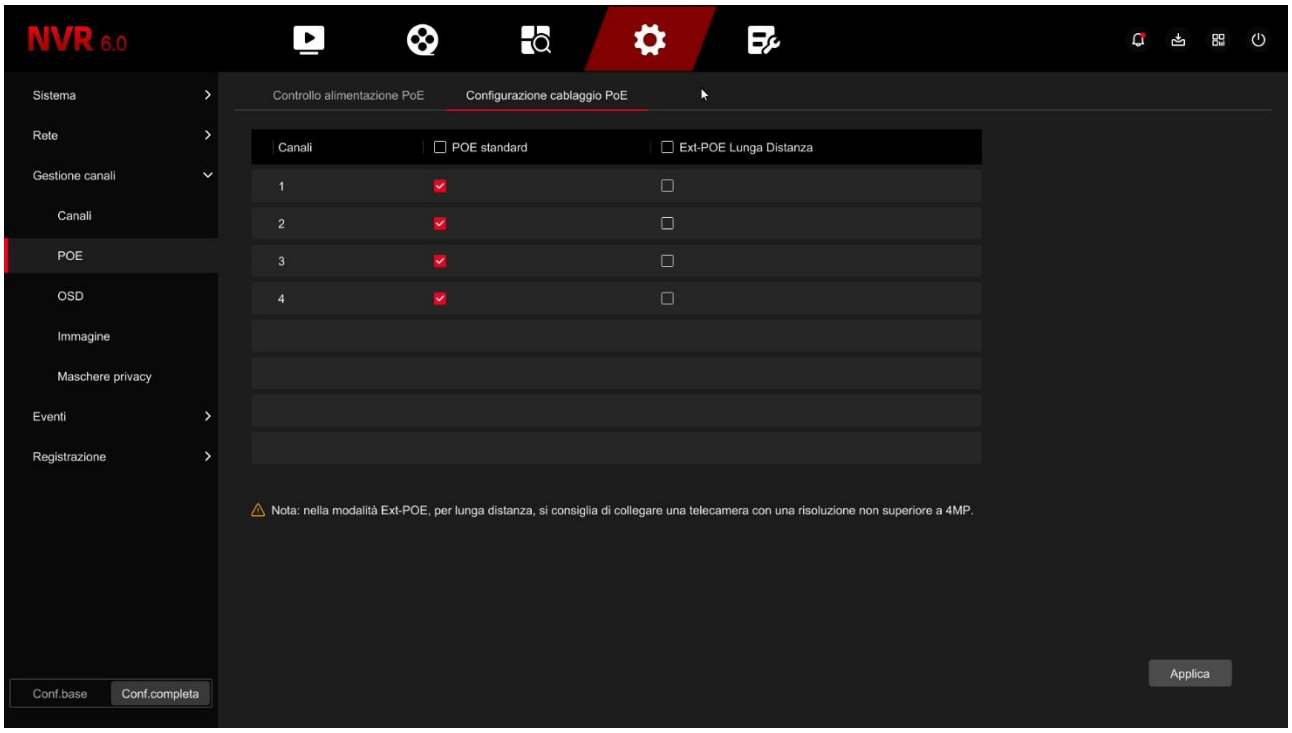
Shows the status of the ports which are colored green if the camera is connected with the indication of the power absorbed by each camera and the total power supplied and residual of the NVR

POE | POE CABLING CONFIGURATION

This section is only available in NVRs with built-in 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 factory enabled so that port 1 is reserved for channel 1, port 2 for channel 2, and and so on.

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 channel 5 in after you.

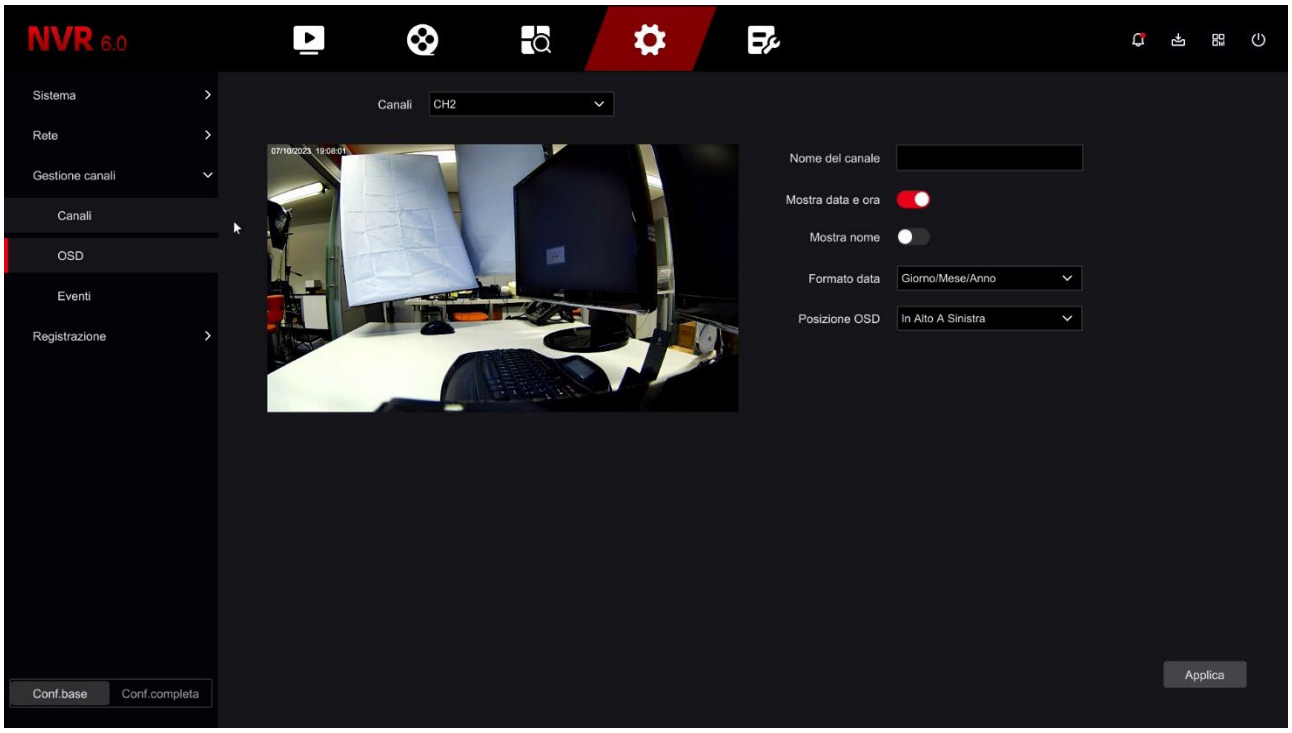


If you connect cameras only to the NVR ports you can keep this factory setting.
If you connect some cameras to the POE ports of the NVR and others externally on the network, then you should disconnect the poe ports that you are not using so that you have these channels available for the external cameras. For example, if you uncheck POE on channels 3 and 4, POE ports 3 and 4 will not be 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 installed starting from channel 3

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

OSD

In this section you can define 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 need to set the overlays directly in the camera's internal menu.



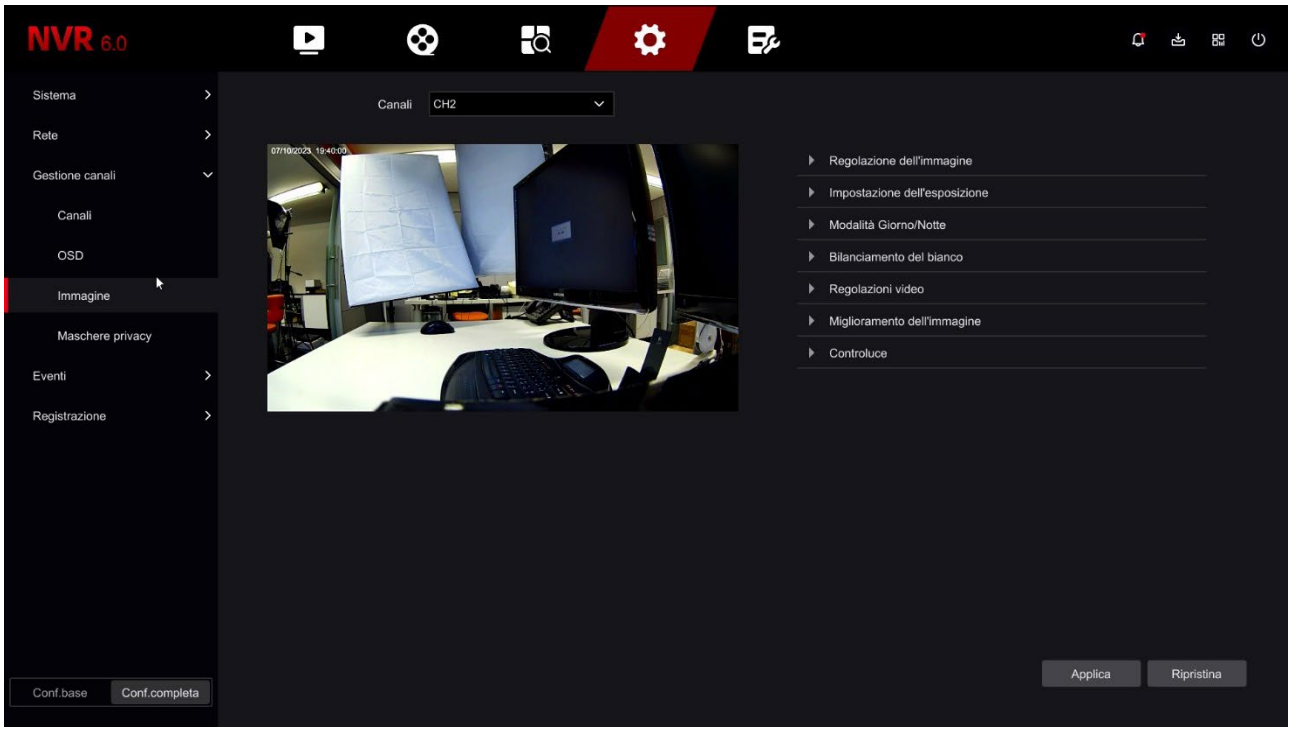
You can display the date and time as an overlay (SHOW DATE AND TIME) by choosing the date format, and also the name of the camera (SHOW NAME), which you type in the box CHANNEL NAME at the top.

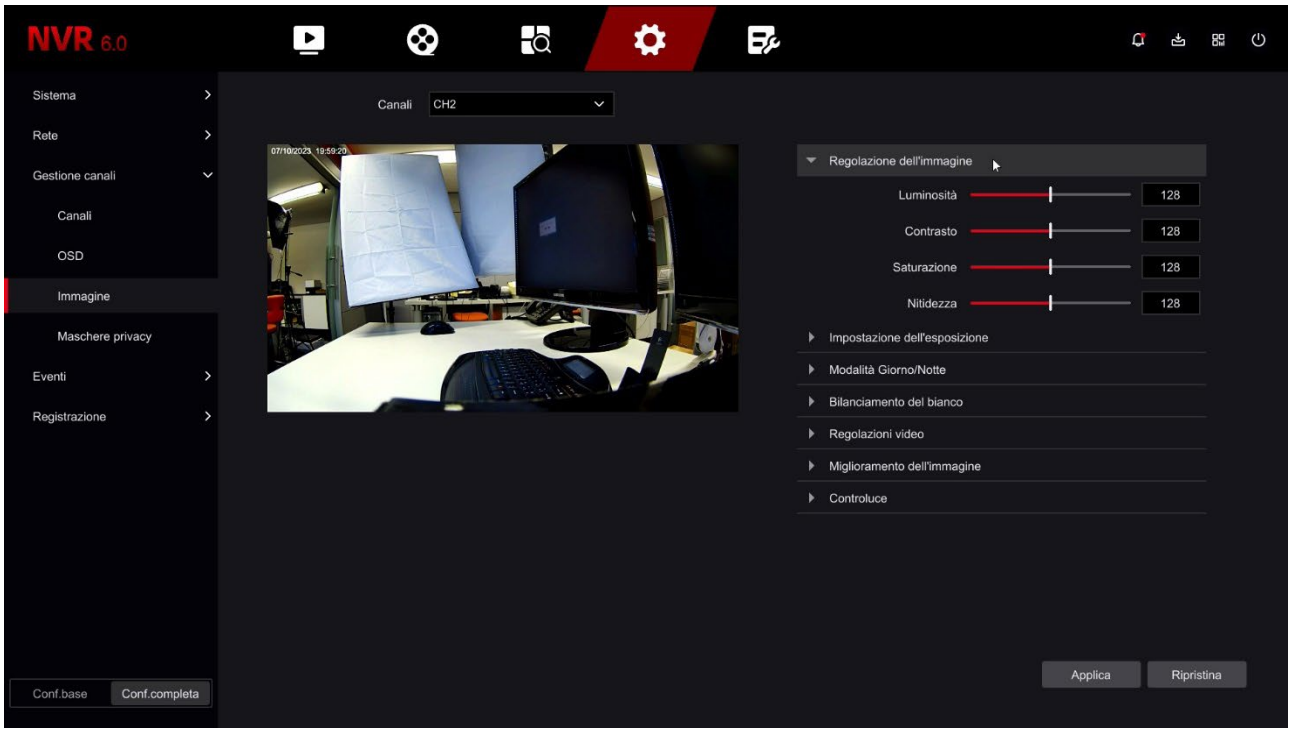
The position of the overlay can be chosen in different positions on the screen (OSD POSITION).

IMAGE

In this section you can adjust the image parameters of the cameras to compensate non-perfect environmental situations. First choose the channel to operate on in the box above, then act on 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 camera image options, while with different IP cameras or with cameras analog you can only adjust the basic parameters

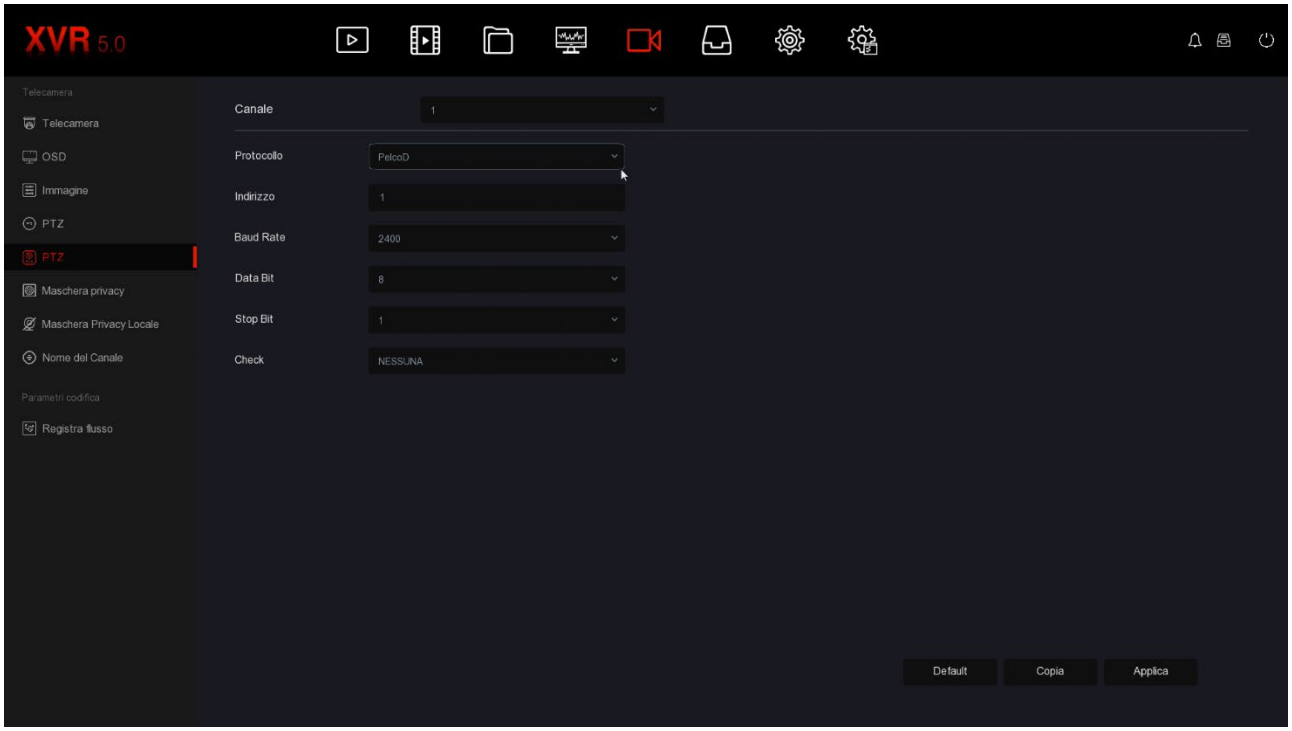




The settings available in this menu depend on the camera model. For the detailed explanation of all settings please refer to the setup manual camera.

PTZ

In this section you can set the communication protocol to use for the command of the analog motorized cameras. This is a section that you can 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

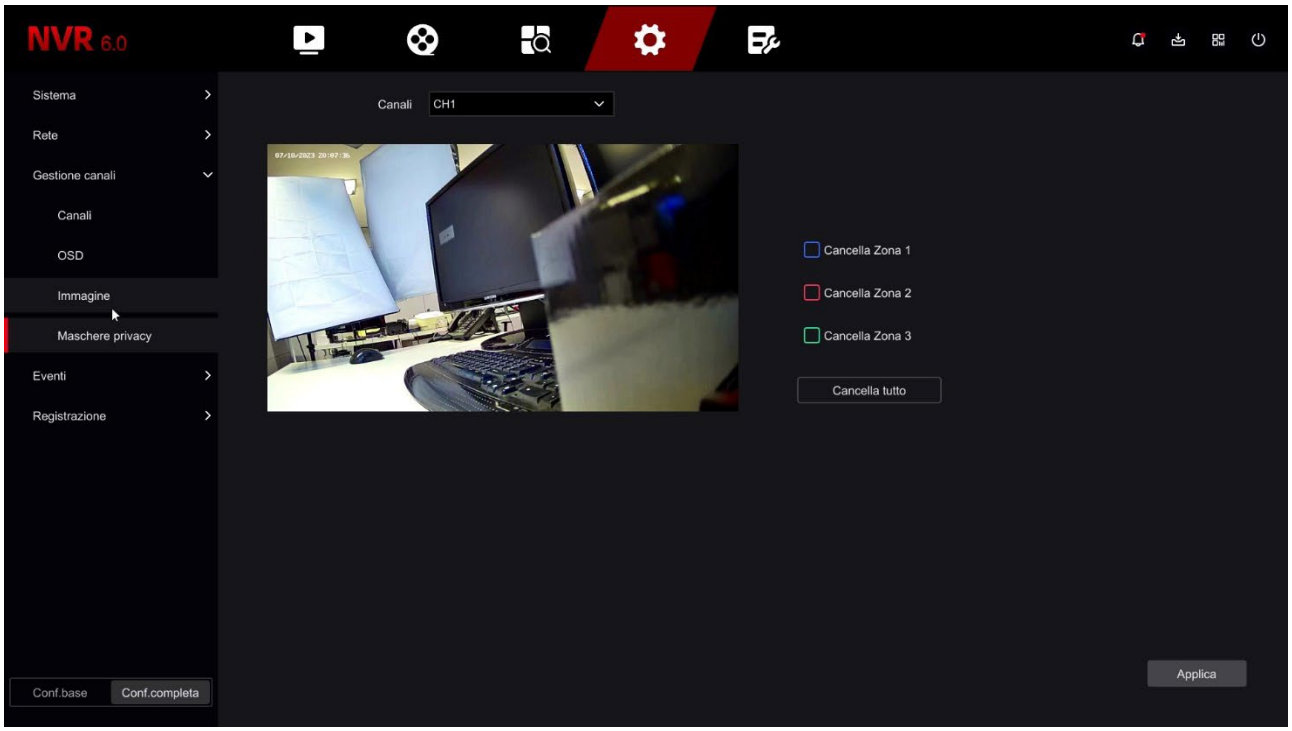
PelcoD – It is used for all DSE motorized cameras that are controlled via the door RS485 serial port on the back of the DVR. Address, Baudrate, Data Bit, Stop bit and Parity Check must be the same as those set in the camera. The most common baudrate values are 2400 and 4800 baud. Each camera has its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

PelcoP – Another variant of the PelcoD, for use with cameras from other manufacturers

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

PRIVACY MASKS

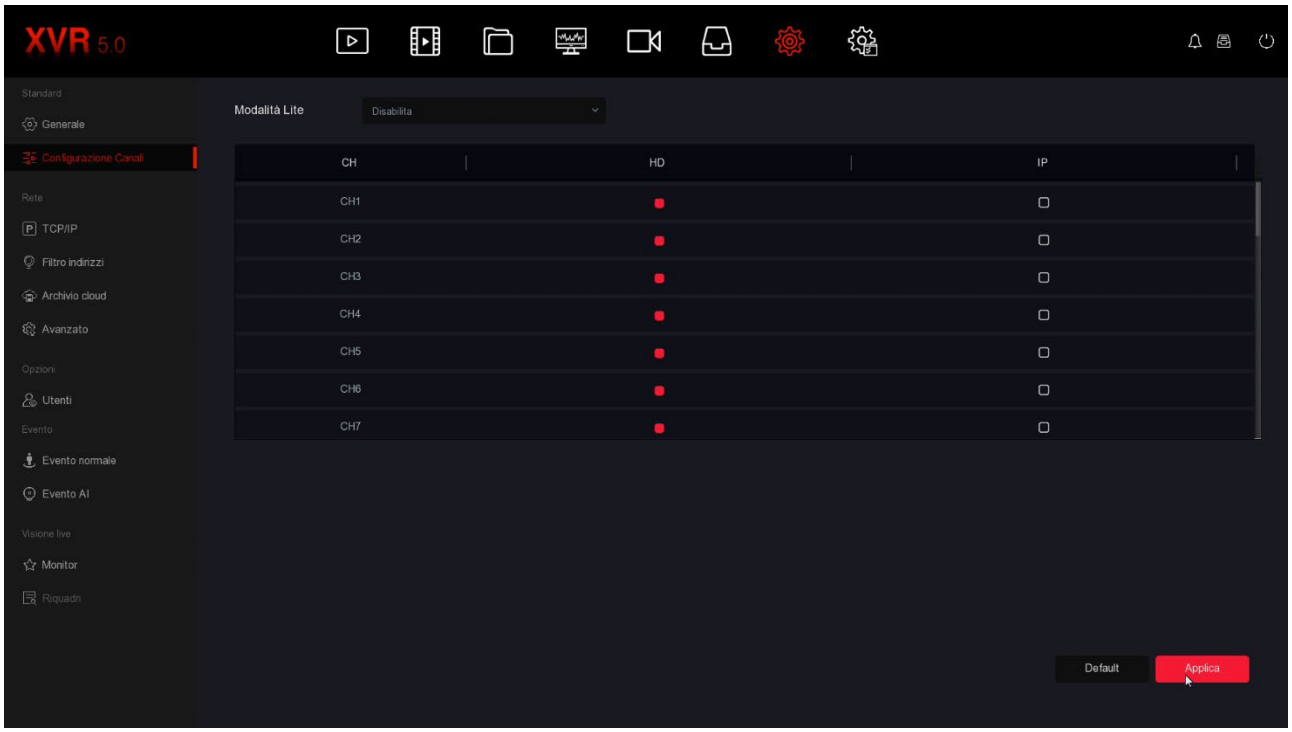
In this window you can draw up to 3 masking areas in the image with the mouse.
black out areas to protect privacy. Typically this function is used to black out areas
outside the property.
This is a feature you can useonly with analog cameras orwith ours
RK Series IP cameras connected with PRIVATE protocol (not Onvif) . With other IP cameras
You need to set privacy masks directly in the camera settings.



Choose the channel you want 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 the
DELETE commands.
In some analog DVRs you can insert two different types of masks: standard masks and
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
analog and IP.



DVRs in this range are factory-supplied with all analogue channels enabled so that 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 number of IP channels.

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

Normally you can disable the BNC inputs in pairs.

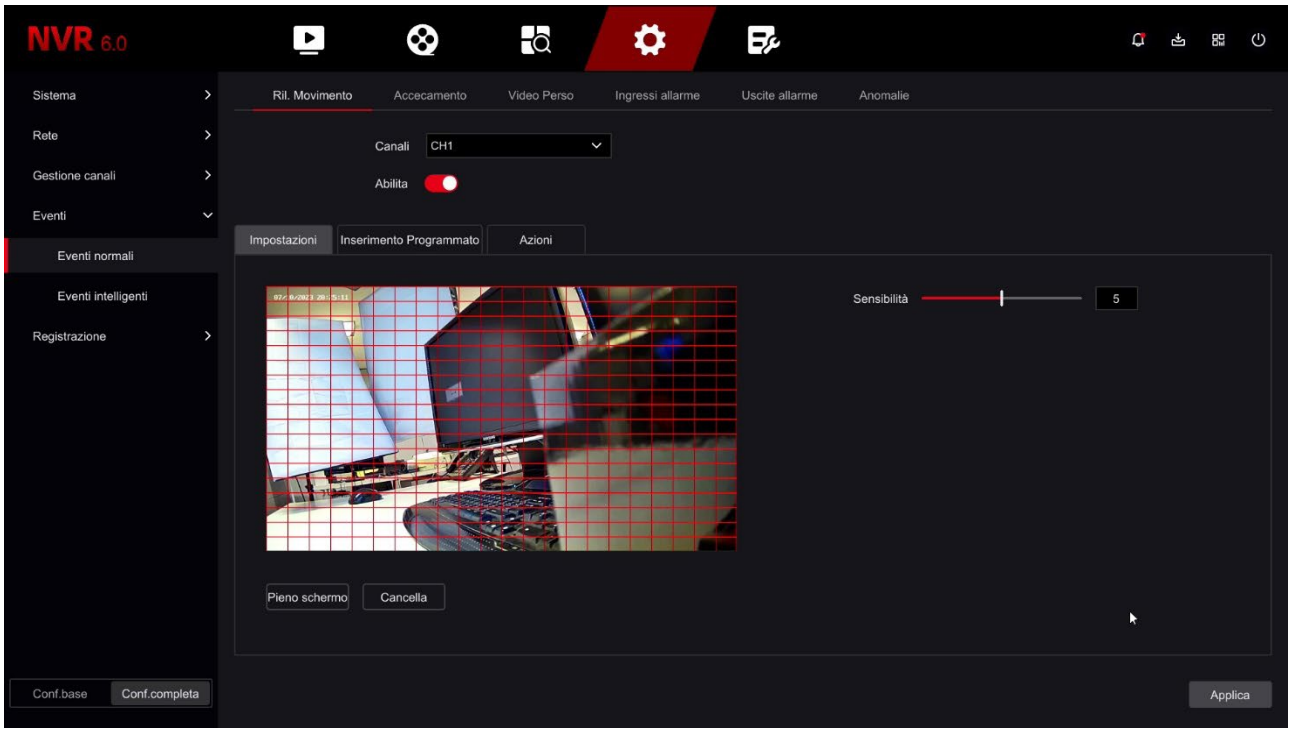
LITE MODE – You can enable lite mode if you want to slightly increase the frame rate of the shots, both live and recorded, reducing the resolution a little. Usually this option is not convenient, but it can be interesting if you shoot moving targets fast to increase the smoothness of the video.

CONFIGURATION | EVENTS

Click the CONFIGURATION button then EVENTS to configure the camera detections.
Note that in analog DVRs intrusion detections are performed by the DVR while in
IP cameras the detections reside in the camera and when you configure the detections in the NVR
these will do nothing more than transfer them to the cameras. In this EVENTS section you only configure
the rules of the surveys while how and when to record is defined in the next section:
REGISTRATION

NORMAL EVENTS | MOTION DETECTION

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



Motion detection is a very useful feature 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 get 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 events 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 cannot 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 you can adjust it effectively. You also have to consider that if you record in motion you could lose recordings where the subject is very far from the camera or in a corner of the shot.

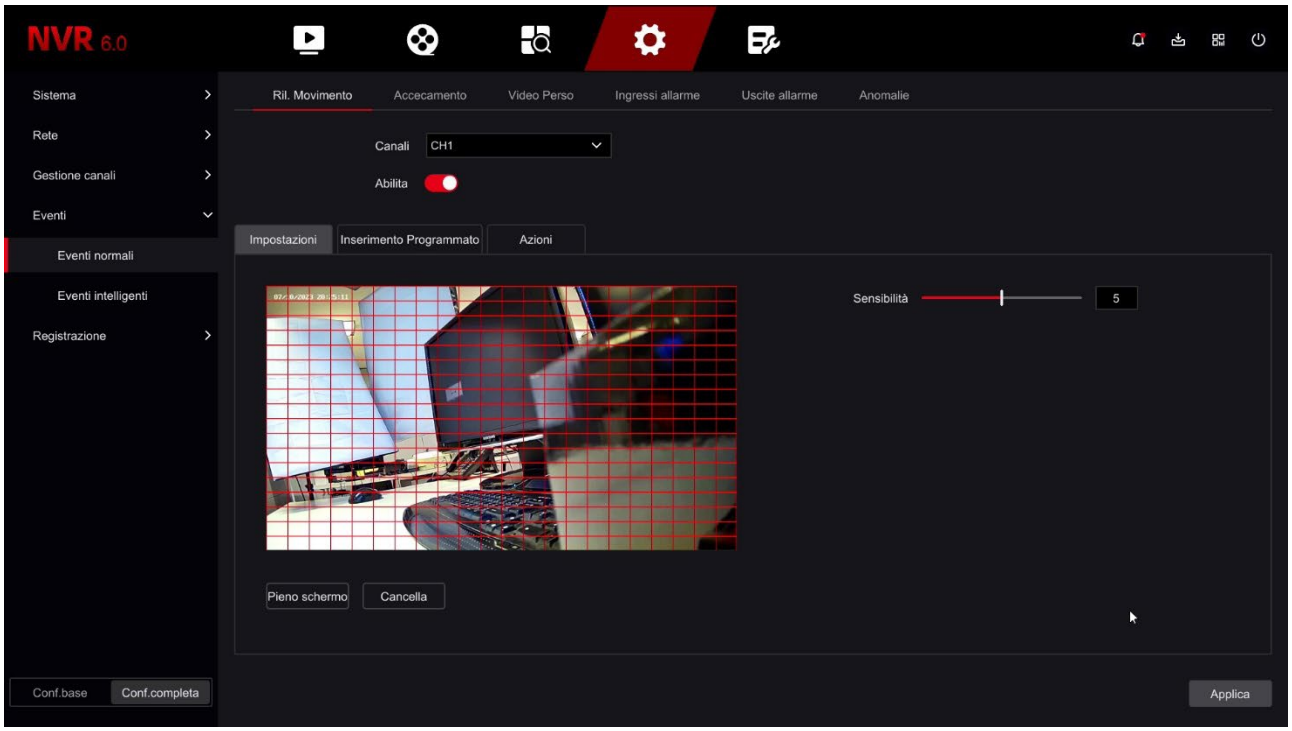
Motion detection is not considered intelligent detection because it detects any type of image editing, regardless of what generates it.

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 analog cameras all motion detection functions are performed by the DVR. In IP cameras, on the other hand, do not. In IP cameras, the detection function is performed by the camera, while the NVR only performs alarm actions following the detection. It follows that When you set up motion detection from the NVR, the detection settings, such as enable, the area and sensitivity are sent to the camera for action. Our NVRs can only send these adjustments 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 Enable) remotely and in this case**you will need to set these functions in the camera menu, by connecting with the browser**directly to the camera.

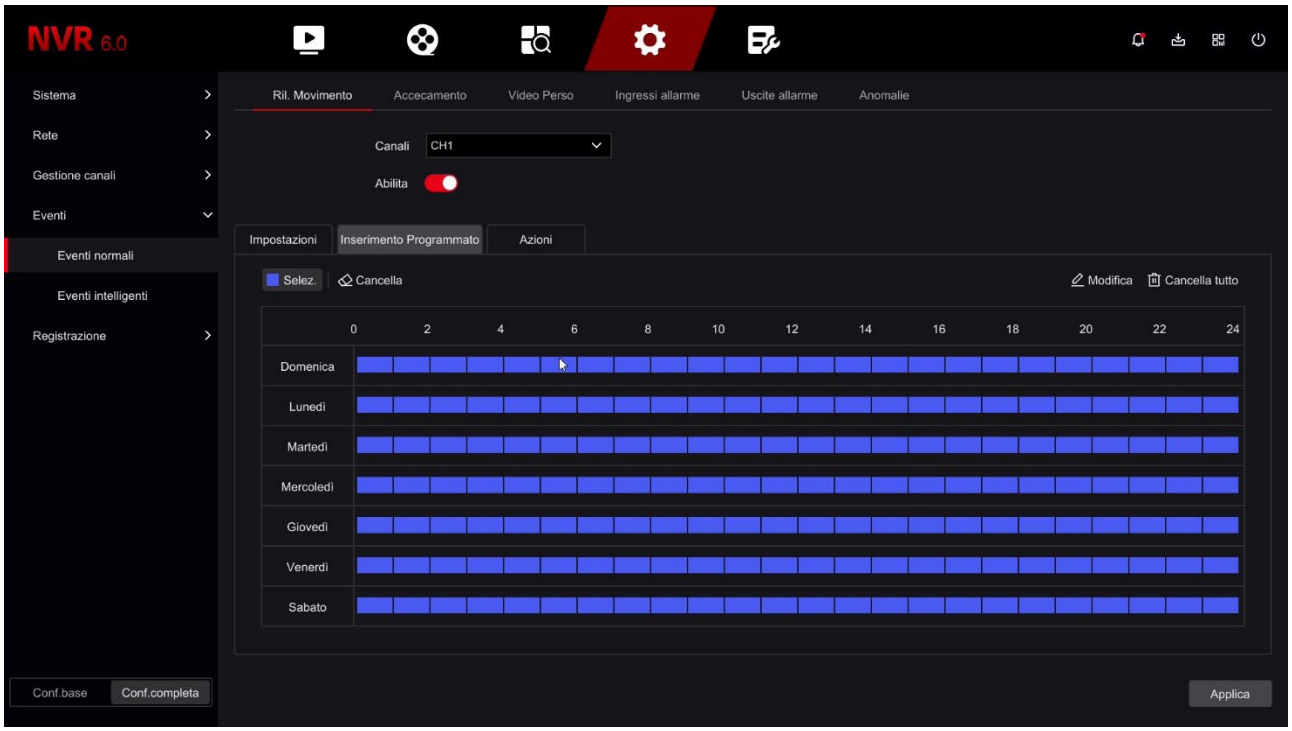
Now let's see how to configure motion detection, option by option.
Remember that in this EVENTS section you can only adjust the detection options, while **how and when to record you have to set it in the REGISTRATION section**.



CHANNEL – You can activate motion detection differently for each camera. 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 smart detection features. If after some tests you feel that this

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

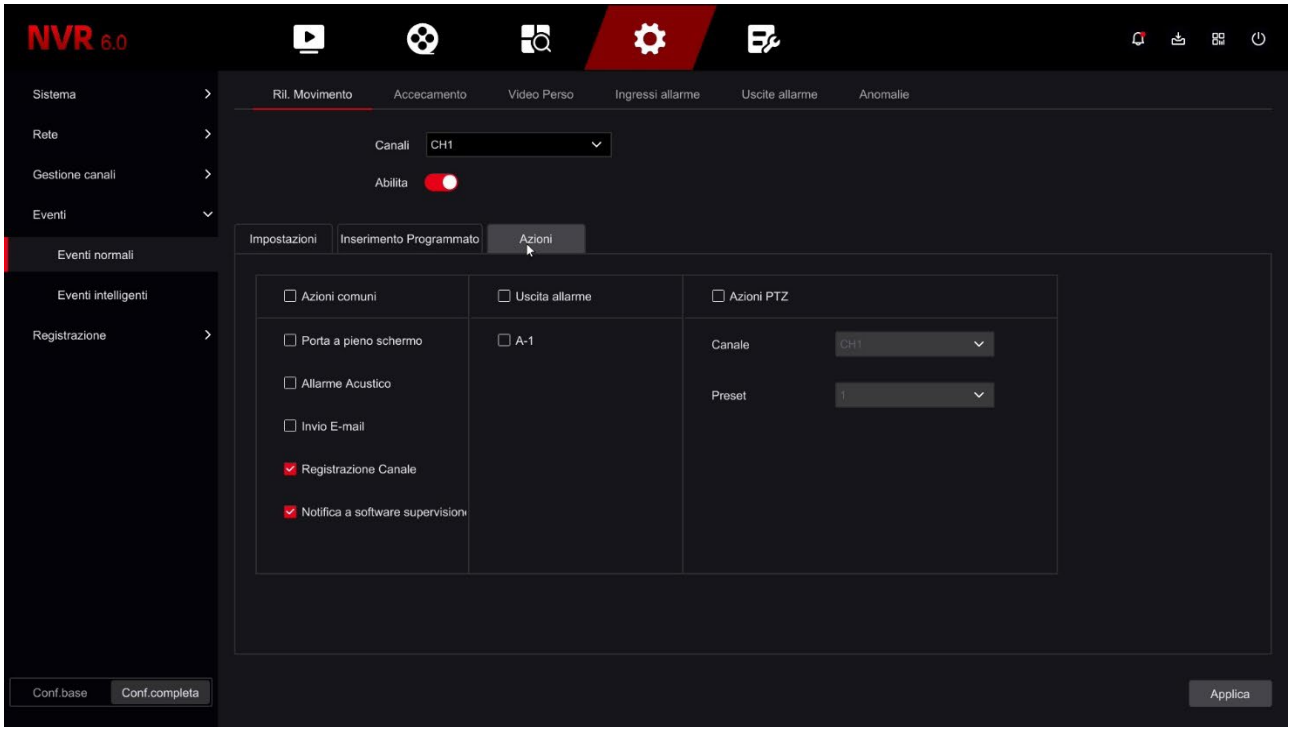
AREA SETTINGS – You can define in which area of the field of vision the detection takes place. movement. Areas not covered by the red grid will be ignored for detection purposes. For select the detection area color the image boxes with the mouse. If you want the detection occurs on the entire image, select FULL SCREEN or color all the boxes by dragging the mouse. Depending on the DVR/NVR type the active area may also be shown as colored in gray instead of with the red grid. If after some tests you have the impression that This setting is not effective because your camera requires you to configure the detection directly in the camera menu and not through 'NVR.
SENSITIVITY – You can choose a sensitivity value to exclude, as far as possible, false detections due to small movements. Remember that no matter how much you can set the sensitivity, you can never completely exclude the possibility 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 ineffective is because your camera requires that you do it directly in the camera menu and not through 'NVR.
SCHEDULED ENTRY – You can define time slots for each day of the week enable if you want motion detection to be active only during certain periods.



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

Factory detection is always active so the table is completely colored.

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



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

AUDIBLE ALARM – You can activate the internal buzzer of the DVR/NVR at every motion detection. It is a convenient feature to have a local sound alert. We recommend that you enable 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 be sent successfully you must check that the motion triggers properly (check if the red man appears in overlay) and that the SMTP network settings are correct (use the test button in the email section)

CHANNEL RECORDING – You can choose to start recording after detection of motion. Or you can use motion only to send alerts and record in continuous.

NOTIFICATION TO SUPERVISION SOFTWARE – Send 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 up automatically preset a camera so that the camera positions itself automatically in a predefined position.

DETECTION TEST

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

When the motion is triggered you should see the red man icon appearing in overlay in the live image. If you have scheduled motion recording, you should also see it light up the green camera icon.

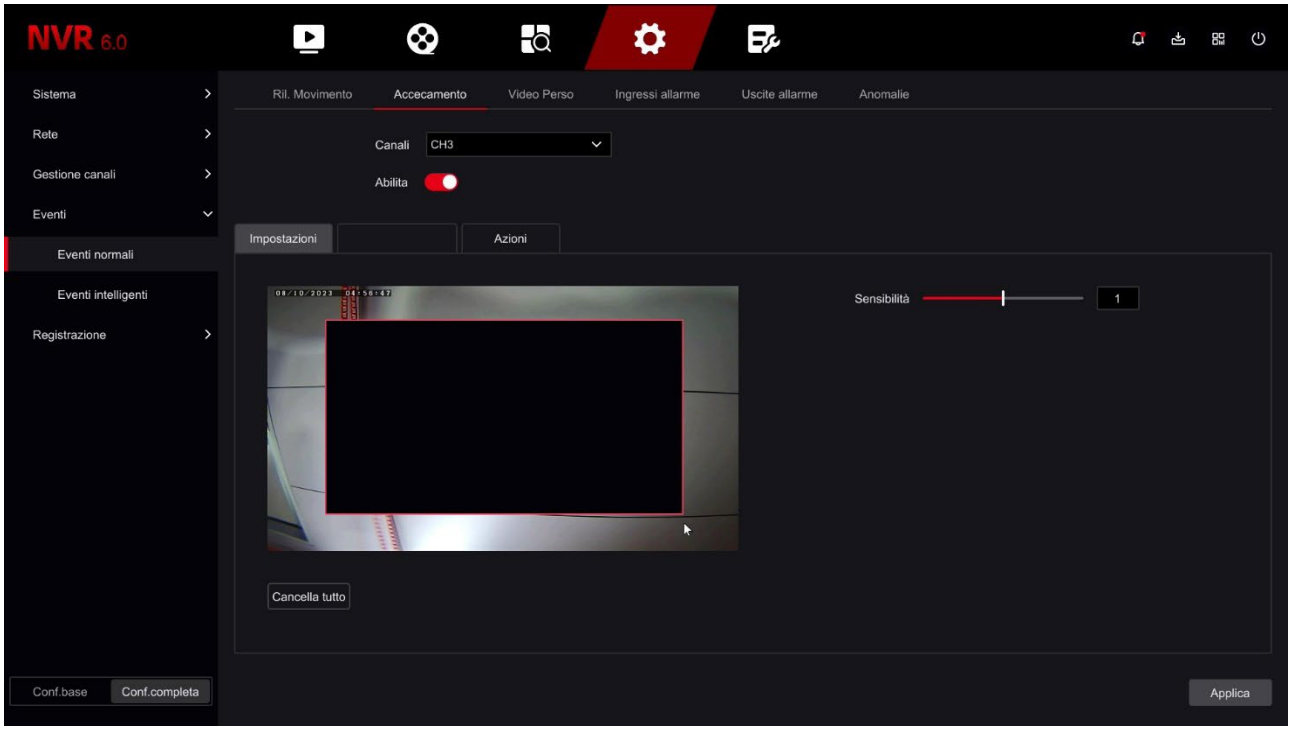
Channel recording

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 the little red man appears, but not the green camera is because it is not programmed to record in case of motion alarm, 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 gives a black image because it is covered by intruders. Not all models of cameras support this function.



ENABLE – Enable detection

SETTINGS – Use the mouse to trace the portion of the image on which to activate the detection

SENSITIVITY – Set the sensitivity if the camera supports it

SCHEDULED INSERT – Color the time slots in which to enable detection

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

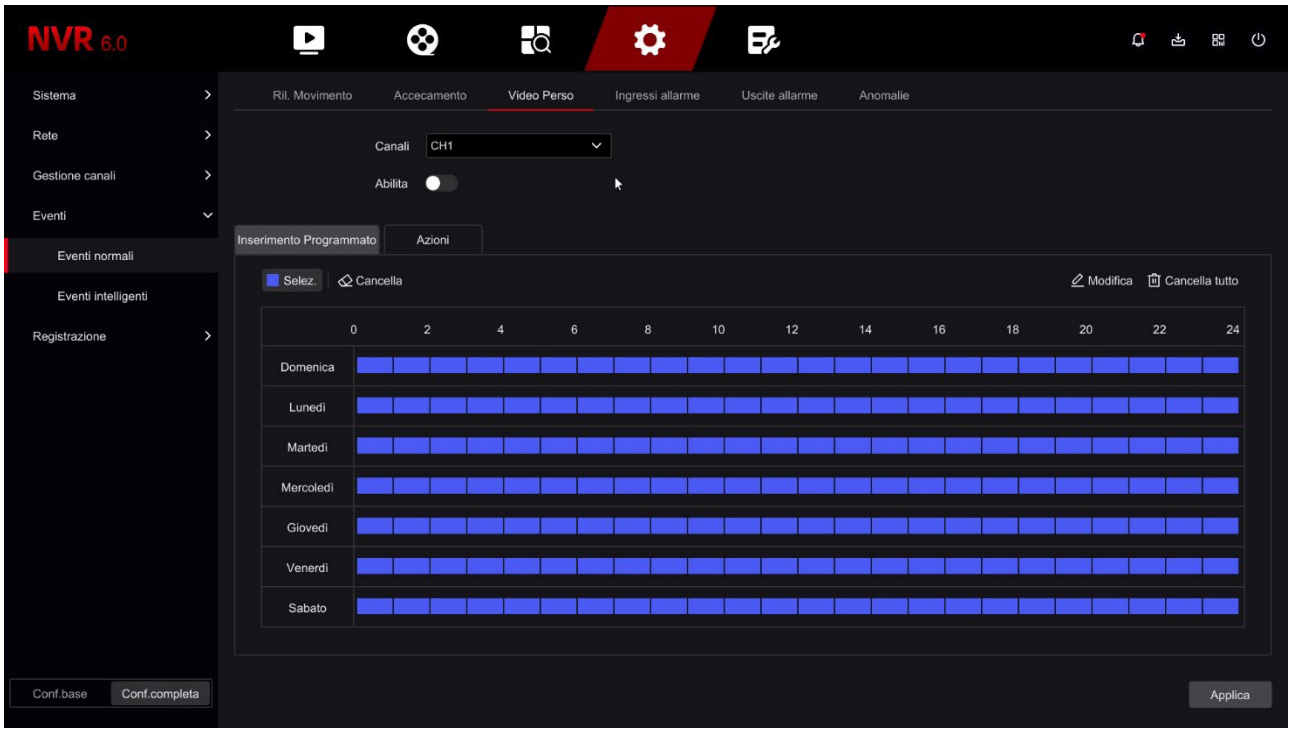
Motion: Full screen, Beep alarm, Send email, Alarm output, Preset recall

of cameras

NORMAL EVENTS | LOST VIDEO

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

It can be caused by a fault or sabotage.



ENABLE – Enable detection

SCHEDULED INSERT – Color the time slots in which to enable detection

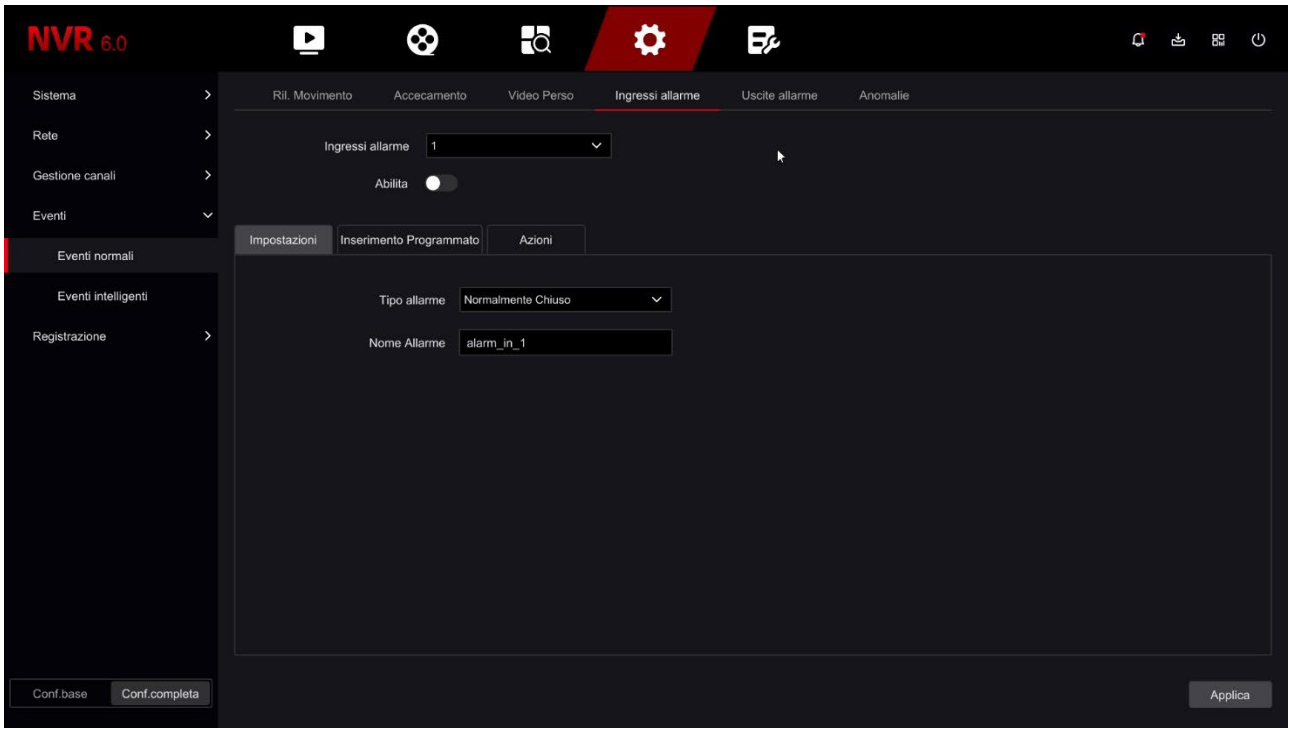
ACTIONS – In case of detection you can enable the alarm actions already described for the detection

Motion: Full screen, Beep alarm, Send email, Alarm output, Preset recall

of cameras

NORMAL EVENTS | ALARM INPUTS

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



ALARM INPUT – Each input in 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)

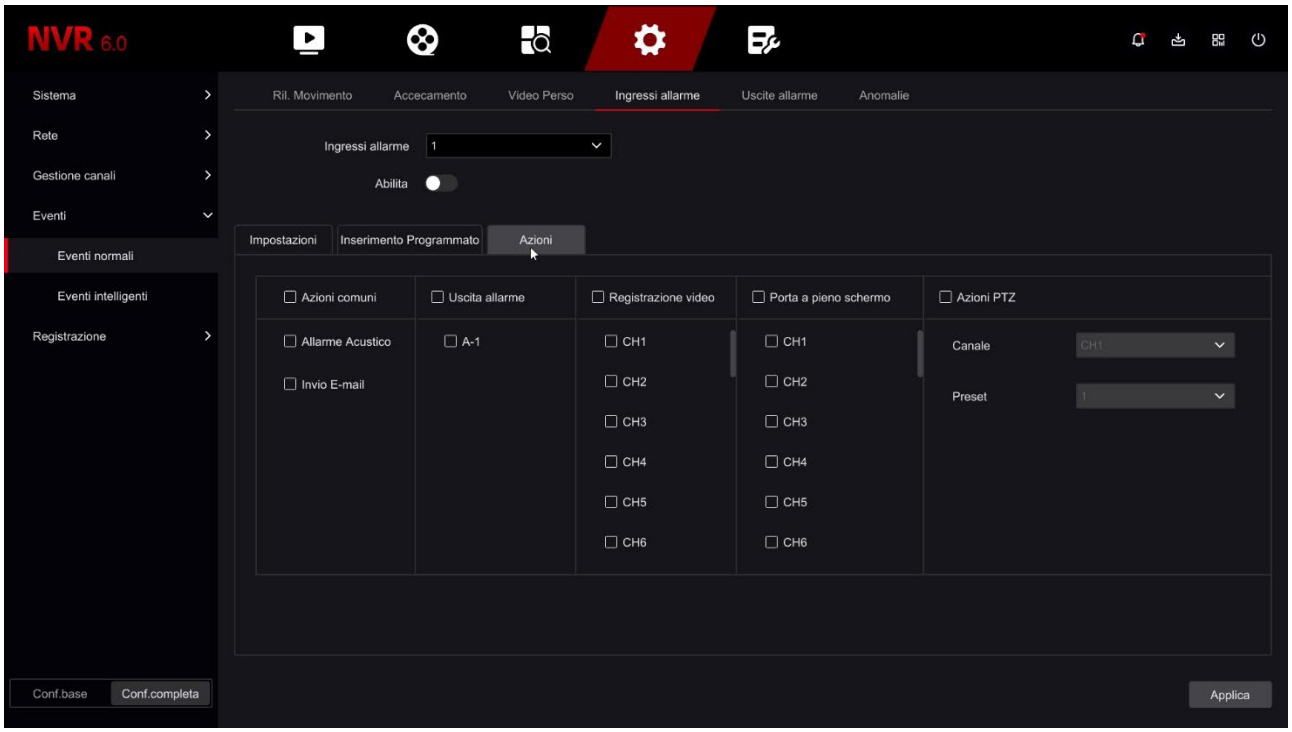
or NC (Normally closed, alarm on opening)

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

SCHEDULED INSERT – Color the time slots in which to enable detection

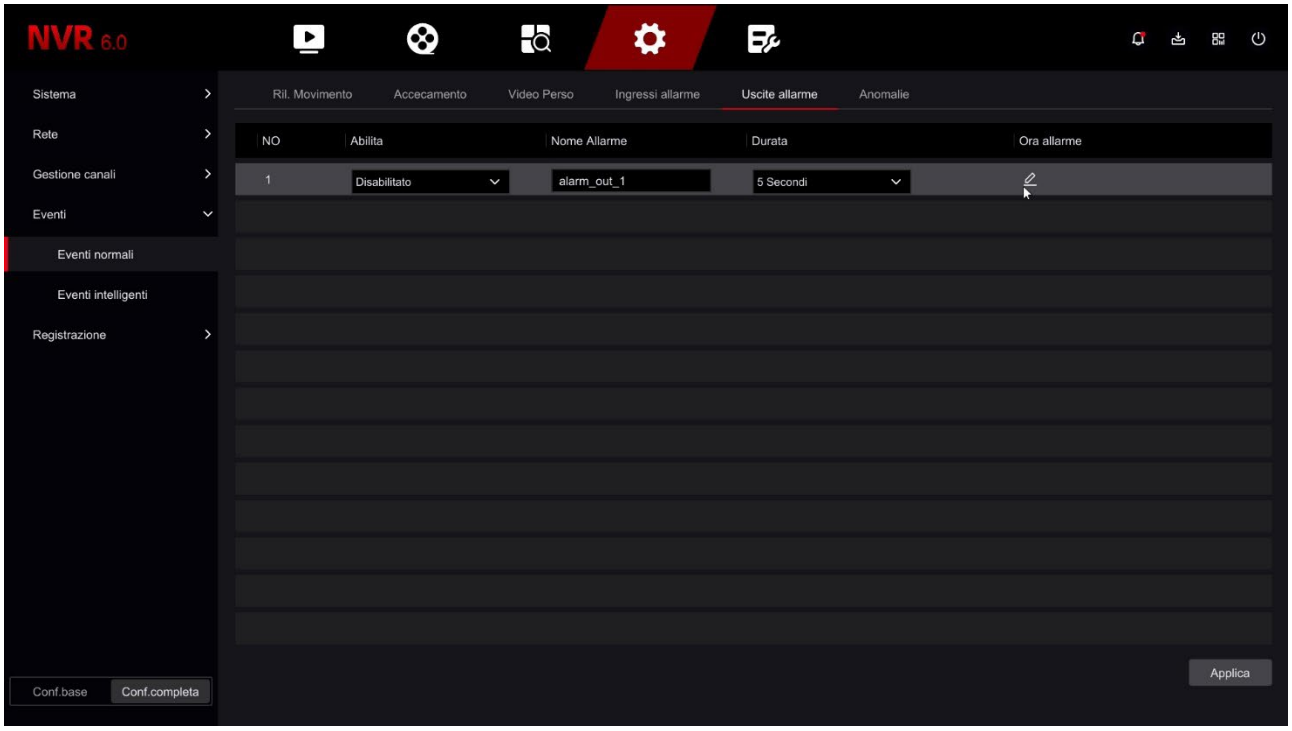
ACTIONS – In case of detection you can enable the alarm actions already described for the detection of motion: Audible alarm, Send email, Alarm output, Call camera presets.

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 in the terminal block you can edit an identification name

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

ALARM TIME - Color the time slots in which to enable the alarm output

NORMAL EVENTS | ANOMALIES

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

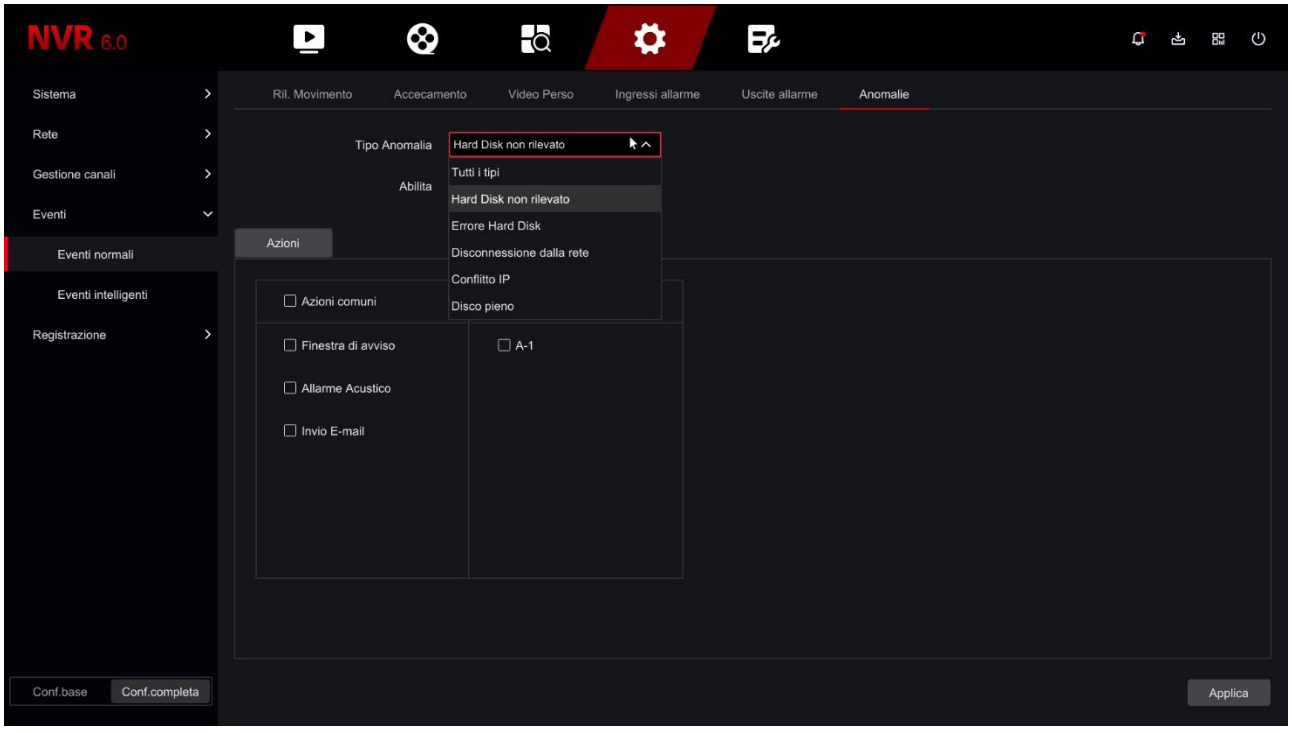
Disk not present

Disk writing errors

Network disconnected

IP conflict on network

Disk full

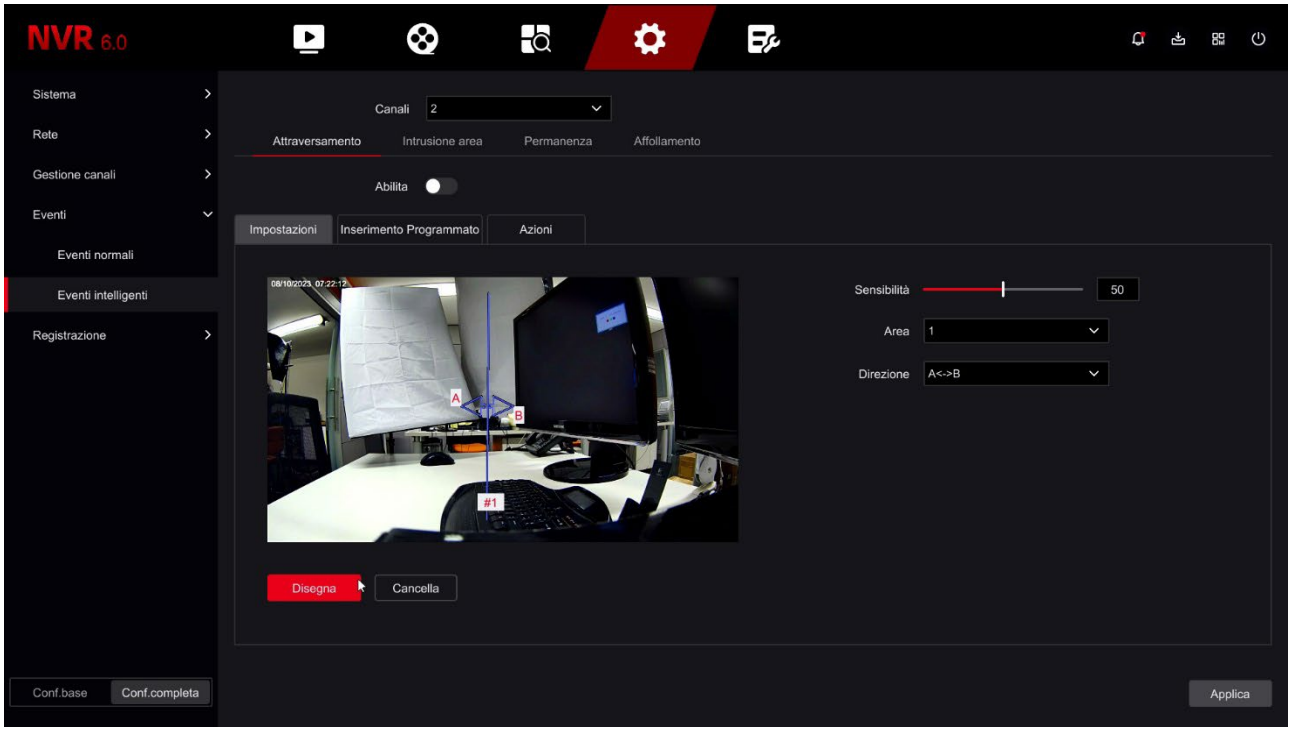


For each abnormal event you can enable a message on the monitor, sending an email, the sound of the internal buzzer and output activation.

SMART 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 settings for these smart functions reside in the camera. The NVR will
allows you to set the configuration and send it to the camera. Please refer to the manual

RK Series Camera Setup for more details on these features.

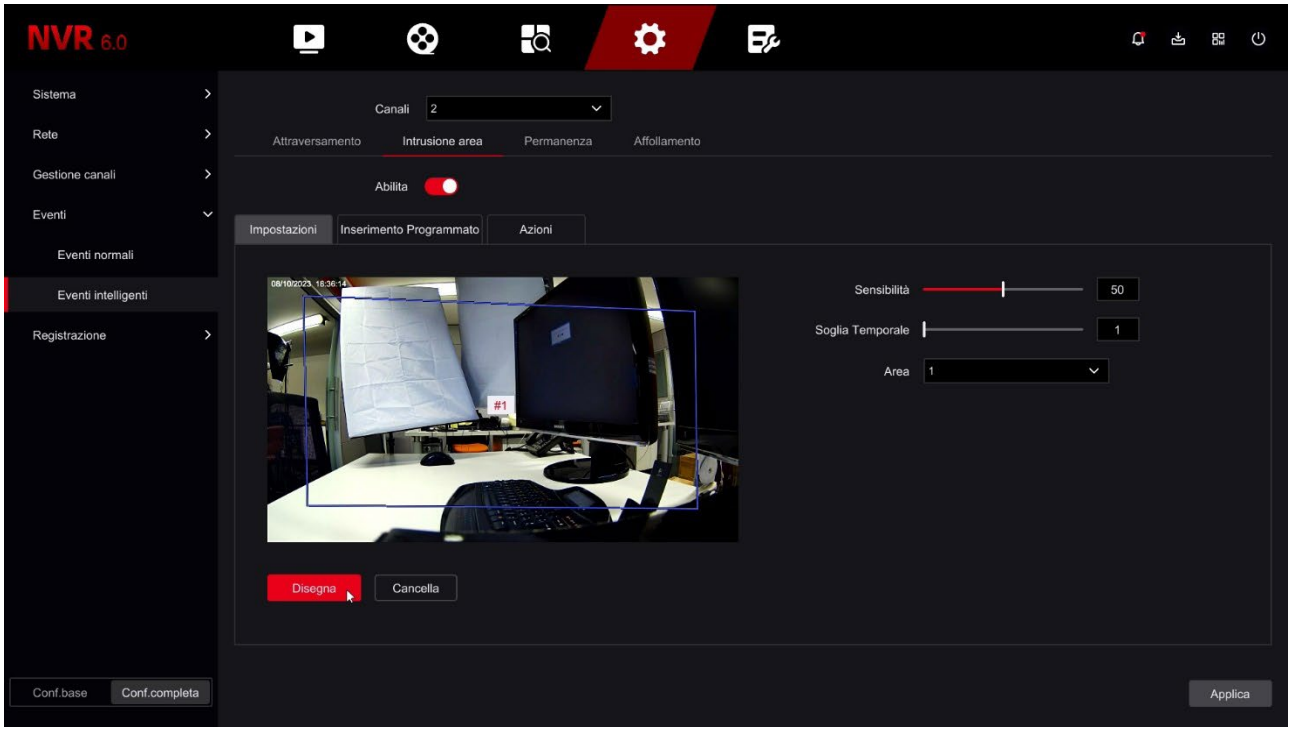


CHANNELS – You can set smart functions only for cameras that support them.
DRAW/FINISH DRAWING – Click to draw the crossing line with the mouse
on the live image
SENSITIVITY – Adjusts the sensitivity of the detection
AREA – You can draw up to 4 virtual crossing lines
DIRECTION – You can define whether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

SMART 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 have human detection.
Human intrusion detection in an area is distinct from motion detection which
we have already described how it detects only people, ignoring movements of
other nature. If you use this detection you should disable motion detection
normal, which you find among normal events.
Note that the settings for these smart functions reside in the camera. The NVR will

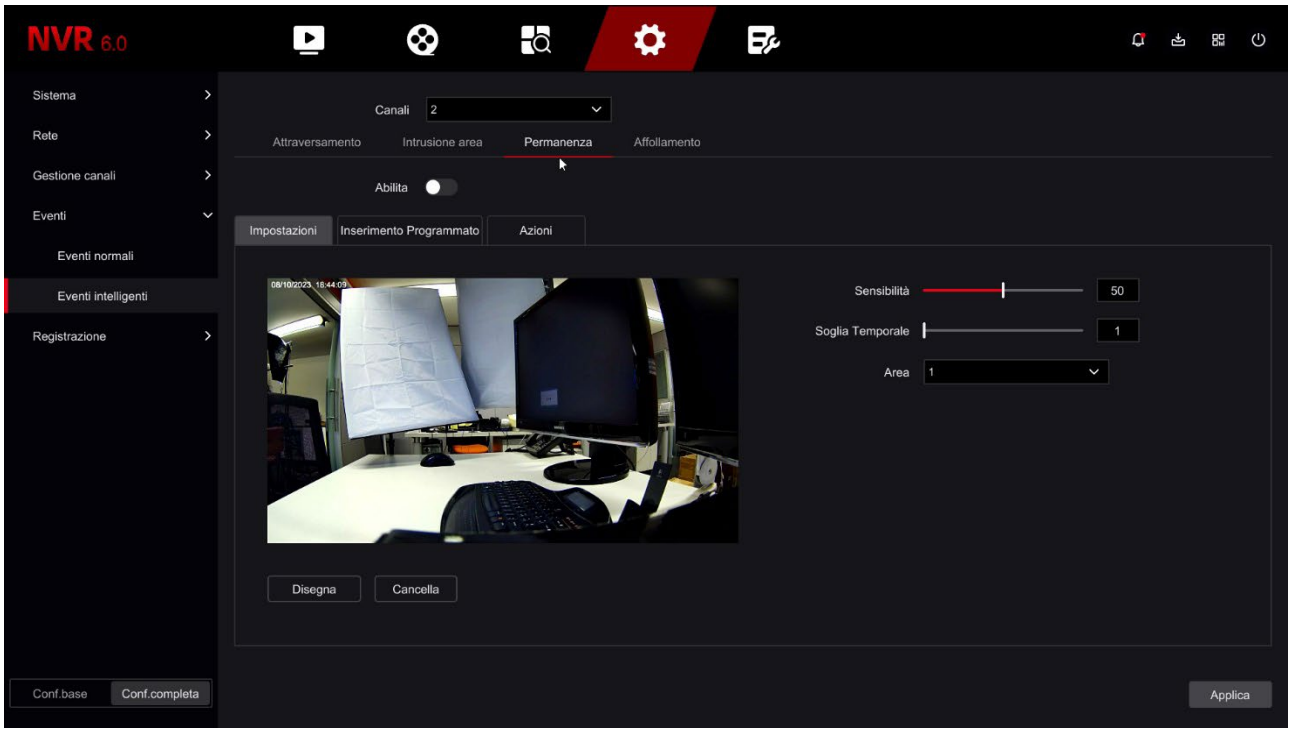
allows you to set the configuration and send it to the camera. Please refer to the manual
RK Series Camera Setup for more details on these features.



CHANNELS – You can set smart functions only for cameras that support them.
DRAW/FINISH DRAWING – Click to trace with the mouse the area in which to detect
the intrusion
SENSITIVITY – Adjusts the sensitivity of the detection
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 INSERT – Color the time slots in which to enable detection
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

SMART EVENTS | STAY

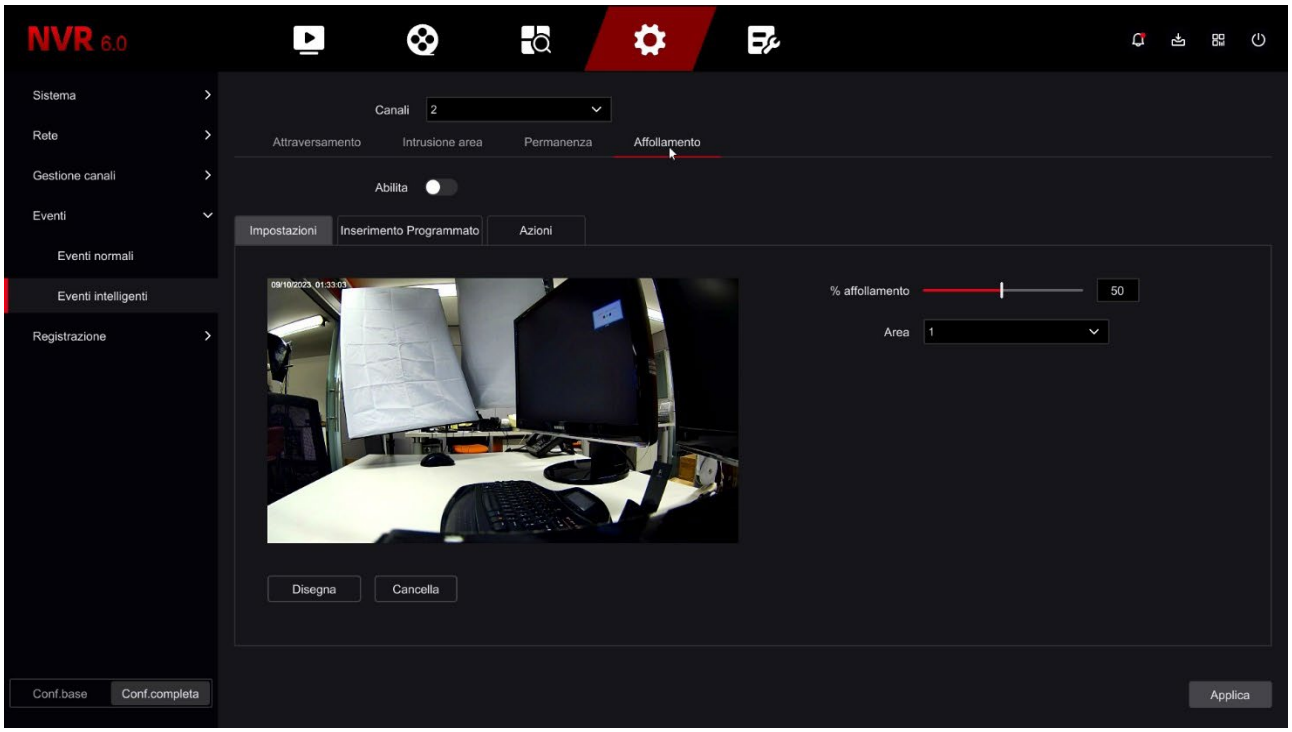
If you have connected one of our RK cameras with intelligent presence detection to your NVR
Here you can set the detection parameters.
Human presence detection is used to generate an alarm if a person remains in a
certain area for longer than permitted.
Note that the settings for these smart functions reside in the camera. The NVR will
allows you to set the configuration and send it to the camera. Please refer to the manual
RK Series Camera Setup for more details on these features.



CHANNELS – You can set smart functions only for cameras that support them.
DRAW/FINISH DRAWING – Click to trace with the mouse the area in which to detect the
stay
SENSITIVITY – Adjusts the sensitivity of the detection
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 INSERT – Color the time slots in which to enable detection
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

SMART EVENTS | CROWDING

If you have connected one of our RK cameras with intelligent crowd detection to your NVR
Here you can set the detection parameters.
Human crowding detection is used to generate an alarm if there is crowding in a certain area.
crowds more people than permitted.
Note that the settings for these smart functions reside in the camera. The NVR will
allows you to set the configuration and send it to the camera. Please refer to the manual
RK Series Camera Setup for more details on these features.



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

DRAW/FINISH DRAWING – Click to trace with the mouse the area in which to detect the crowding

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

AREA – You can trace up to 4 detection areas

SCHEDULED INSERT – Color the time slots in which to enable detection

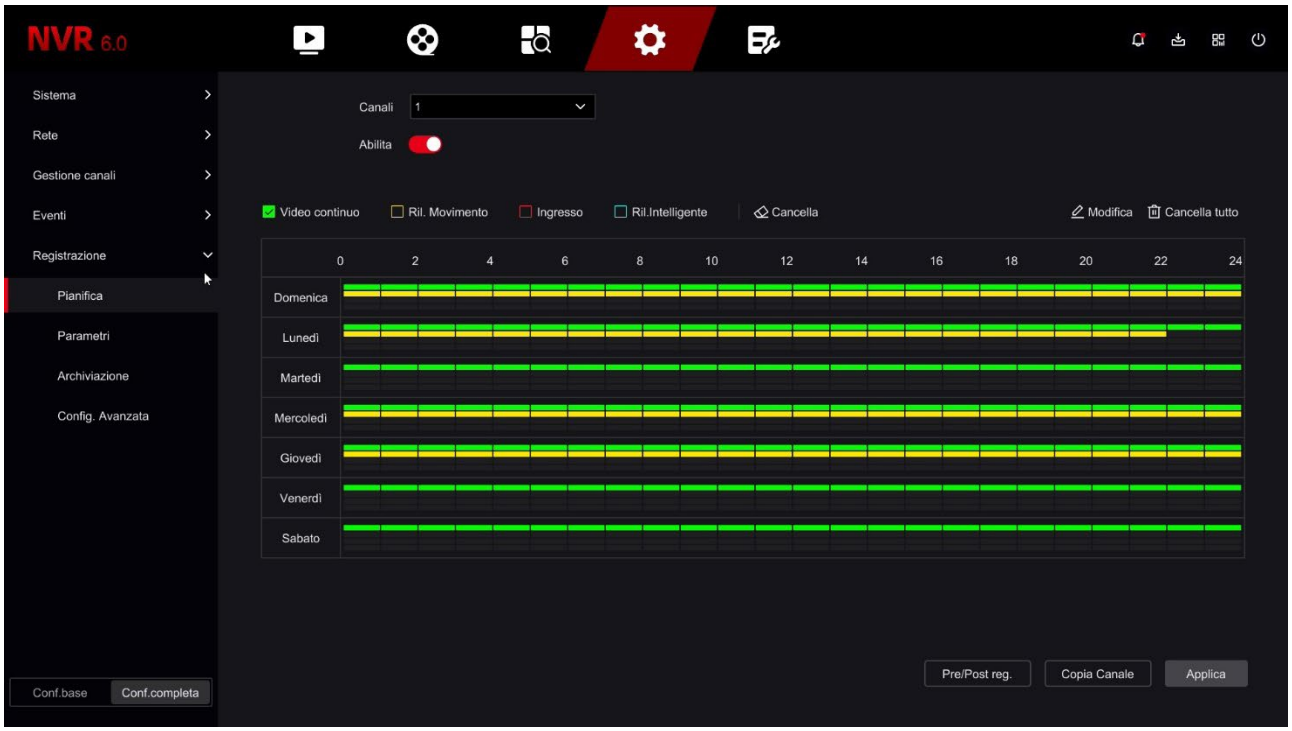
ACTIONS – In case of detection you can enable the same alarm actions already described above for the motion detection.

CONFIG. | REGISTRATION

Click the CONFIGURATION button and then choose REGISTRATION to open the page that will 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



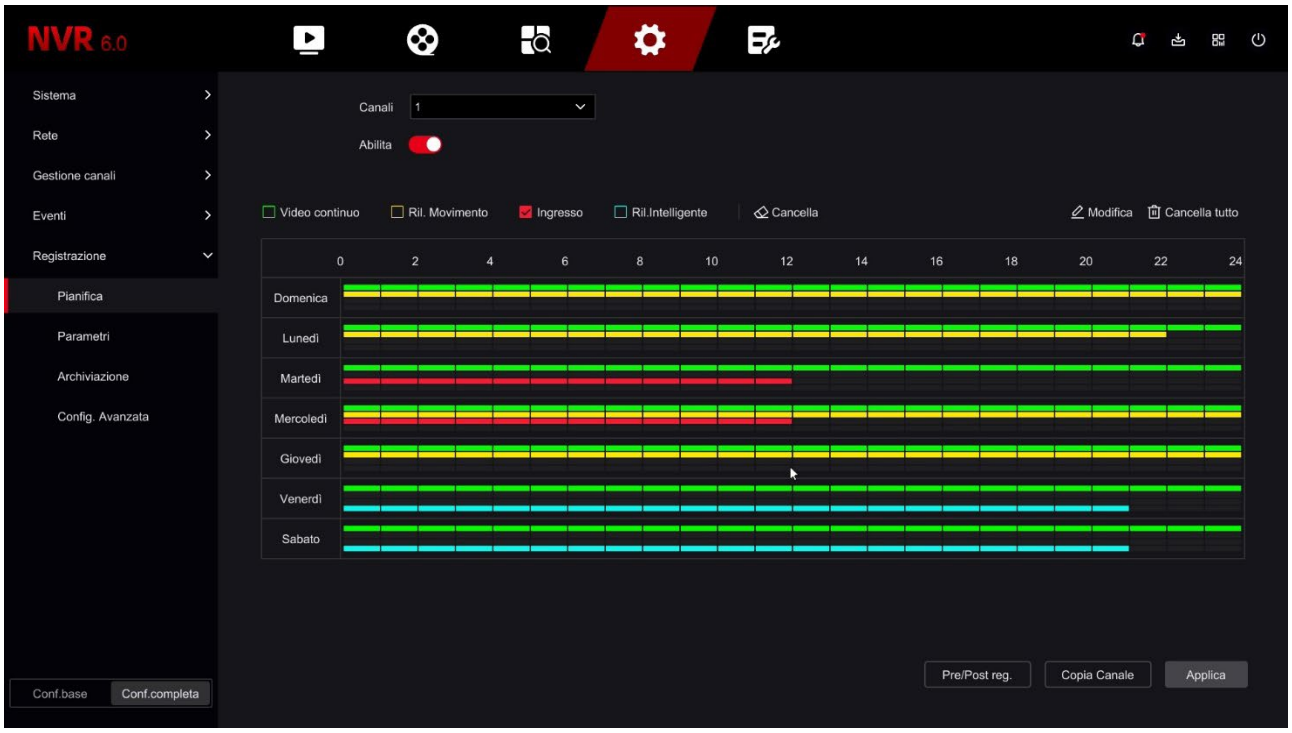
The first thing you need to do is choose the channel you want to configure at the top. Each camera has its own programming so you have to configure them one by one. If you want to configure all the channels in the you can similarly configure channel 1 and then use the COPY CHANNEL button.

Select the channel to configure at the top and then color the green or yellow bands in the calendar with the mouse weekly. Green bands indicate continuous recording, yellow bands indicate recording only when motion detection is detected.

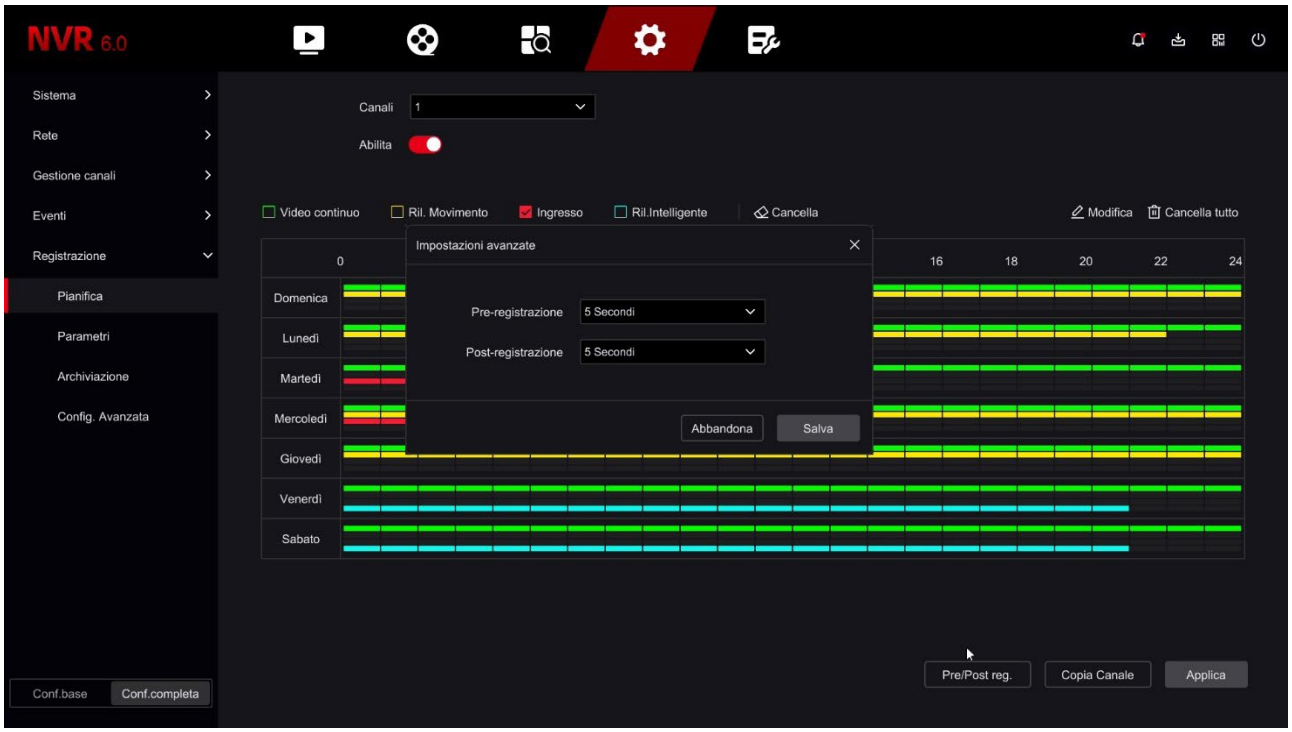
To color the table, choose the green or yellow color at the top, then drag the mouse directly onto the calendar.

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 our RK Series IP cameras with intelligent human detection, you can also color the table BLUE (smart recording).

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

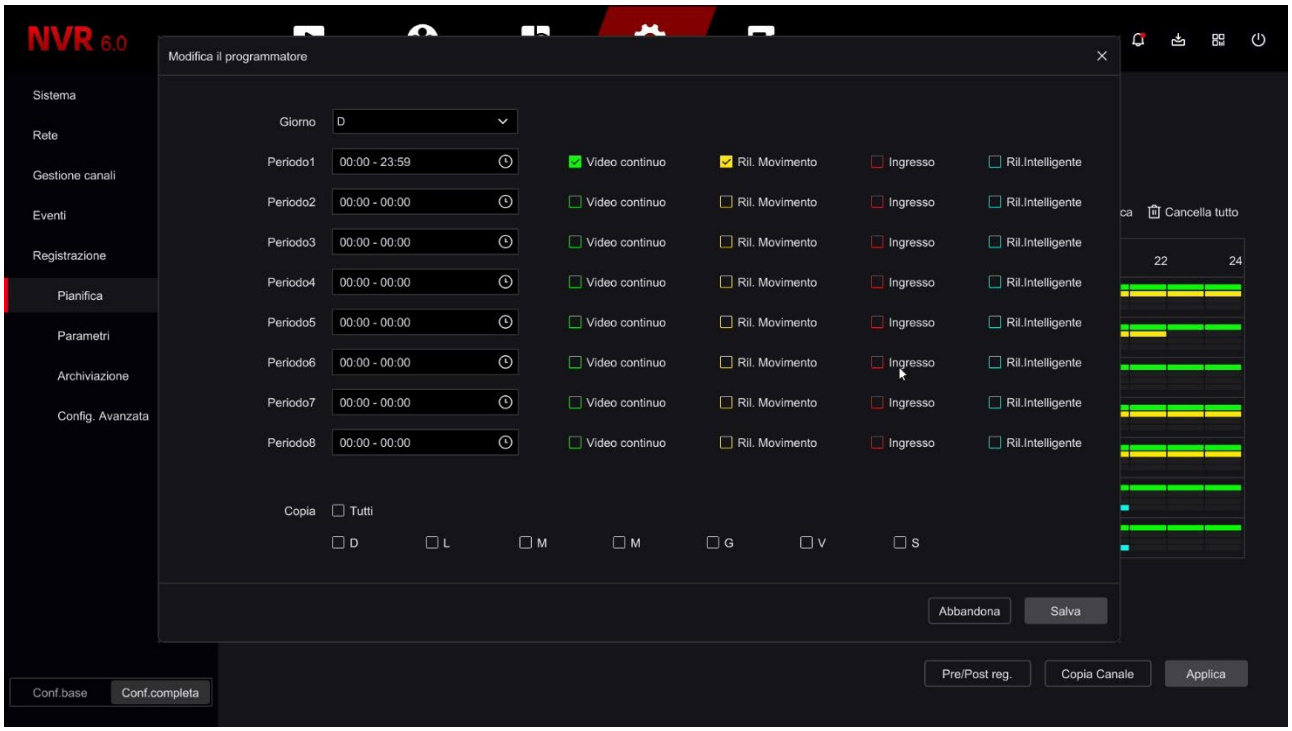


The PRE/POST REG. button allows you to set the pre-recording period, which allows you to record a certain period before the detection, and the post-recording period i.e. the duration of recording following the event.



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

You can set the time slots for each day manually instead of drawing them with the mouse.



REGISTRATION VERIFICATION

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

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

 Channel recording

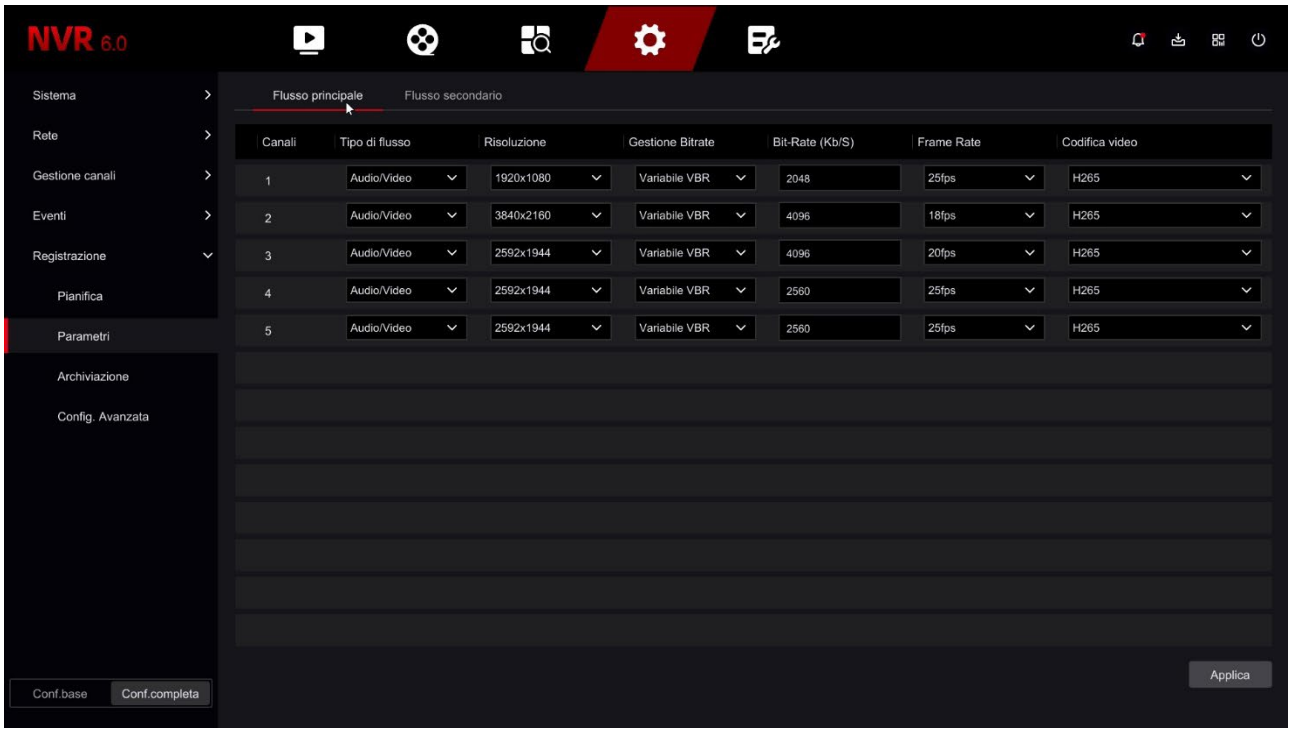
If the channel does not record even though you have set the table correctly, check the HARD section
DISK because there may be problems with the hard disk on which the data is stored.
recordings.

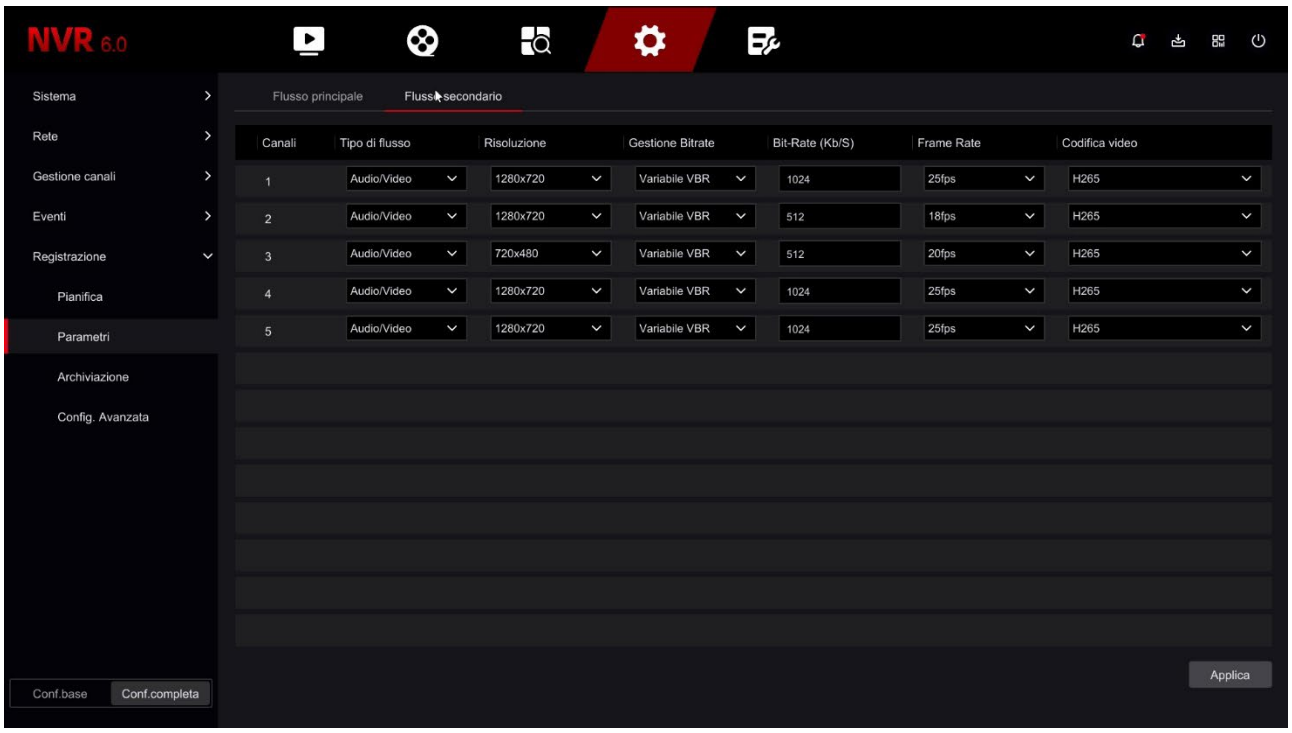
PARAMETERS | MAIN FLOW / SECONDARY FLOW

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

IN IP CAMERAS Video streaming adjustment is done in the settings
camera, not through the NVR. This is because the NVR does not process the incoming video from the
camera, but it only 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 ANALOGUE AND AHD CAMERAS Video streaming adjustment is done in the DVR
as it is the DVR that performs the digitalization of the analog signal. On this page you can
Set DVR video encoding parameters for each channel.





In this manual we do not explain in detail the meaning of the adjustment items of the IP camera video streaming. You can find this information in the camera manual.

FLOW 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 bandwidth) or VBR (variable bandwidth) management

consistent quality)

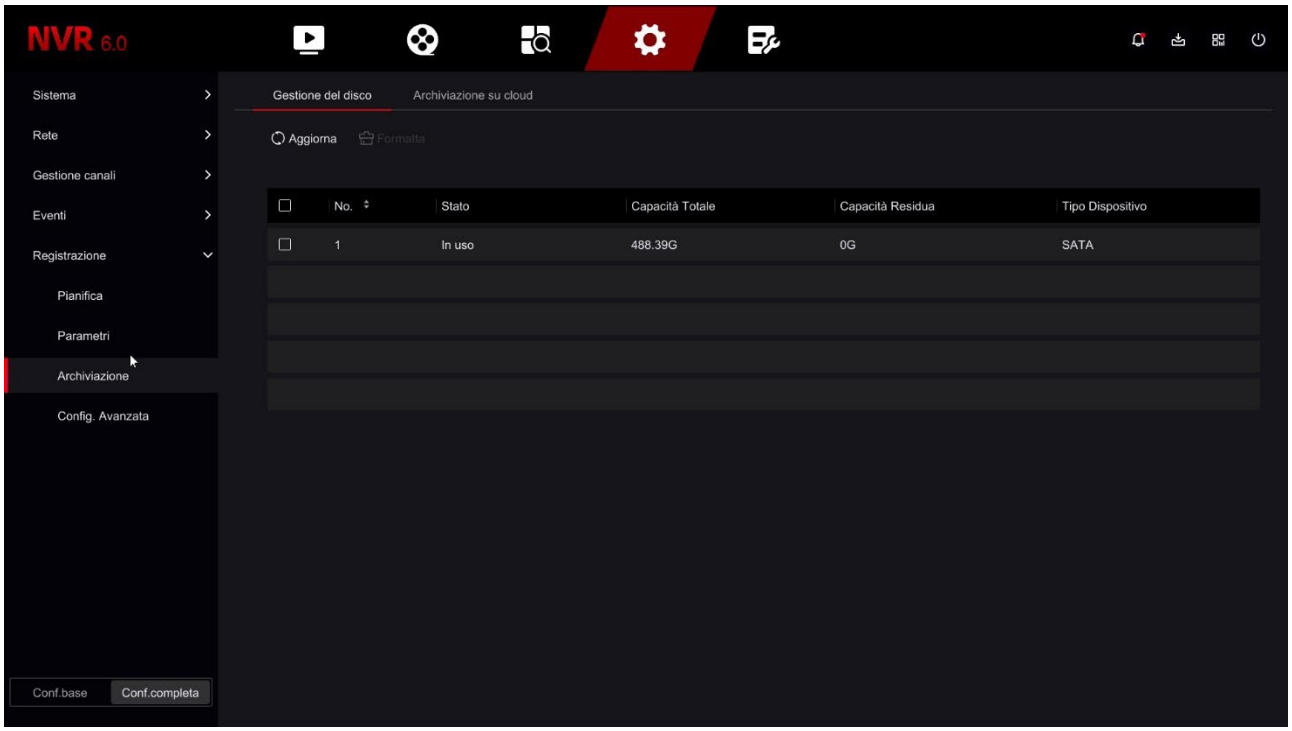
BITRATE – Sets the maximum bandwidth (Kb/s) that the camera will occupy

FRAME RATE – The number of frames/second which you set to the highest value or you can reduce to limit the space occupied on disk at the expense of a lesser fluidity of the images in movement.

VIDEO CODING – Choose H265, the most up-to-date format, for maximum video 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 further bandwidth consumption.

STORAGE | DISK MANAGEMENT

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



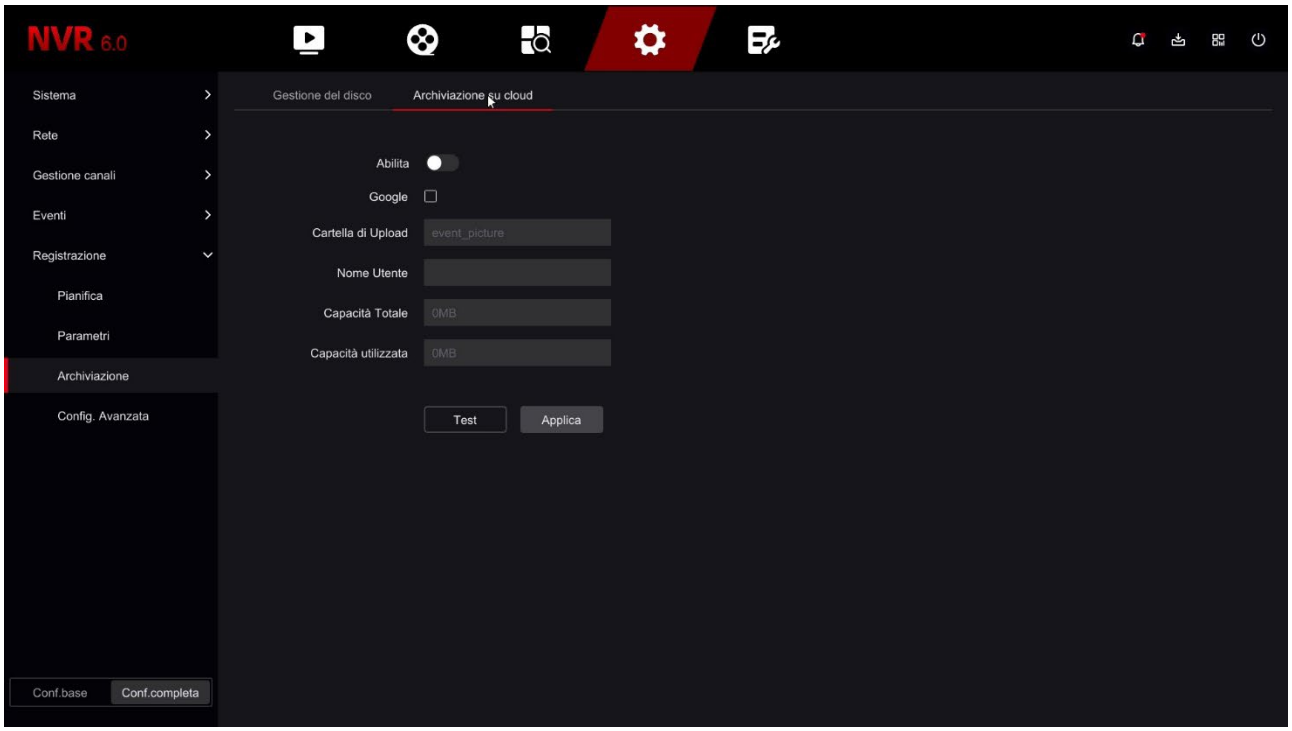
In this page you can check the status of the DVR/NVR internal hard disk and know the total and residual capacity. With the FORMAT button you can proceed to format the disk with all data erased. When the DVR/NVR detects a new disk it requires automatically formatting at startup so you usually don't need to enter this window to make it usable. However, this window can be used to check the status of the disk and to do a forced format if you want to erase all 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/DVR allows you to save recorded images in the event of an alarm on a server CLOUD storage via the Internet. Google cloud service is supported. In this case, you do not These are services similar to our P2P Cloud to facilitate connection, but rather storage spaces web that you can purchase from Google to store data online.

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



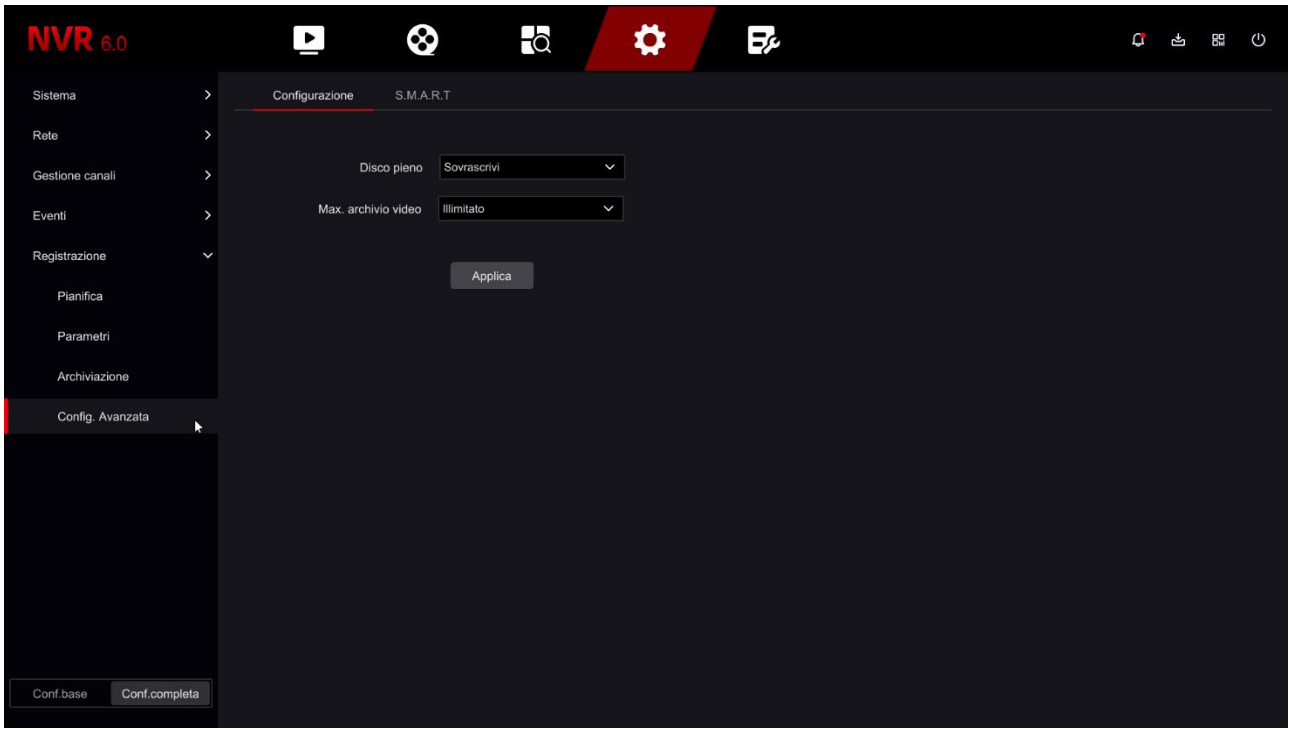
Before completing this table you must obviously subscribe to Google Cloud and have access credentials. You also need to create a folder in your cloud space where to save your files.

On this page you need to enter your Google Cloud login details. After entering the required data use the TEST button to check if 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 storage

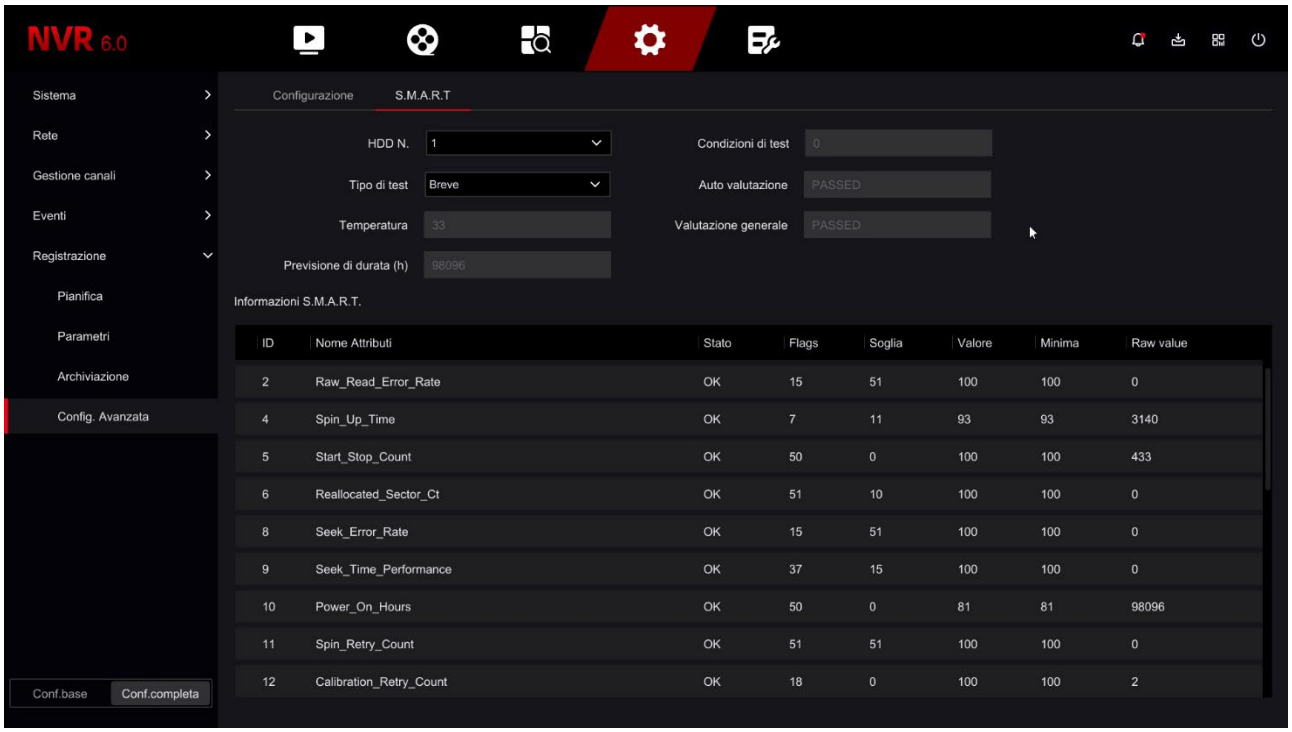


DISK FULL – If you choose Overwrite the NVR will overwrite the oldest files once the disk is full. disk space. If you choose Do not overwrite, recording stops when the space runs out on disk.

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

ADVANCED CONFIGURATION | SMART

This page runs a disk test that evaluates the health of the disk.

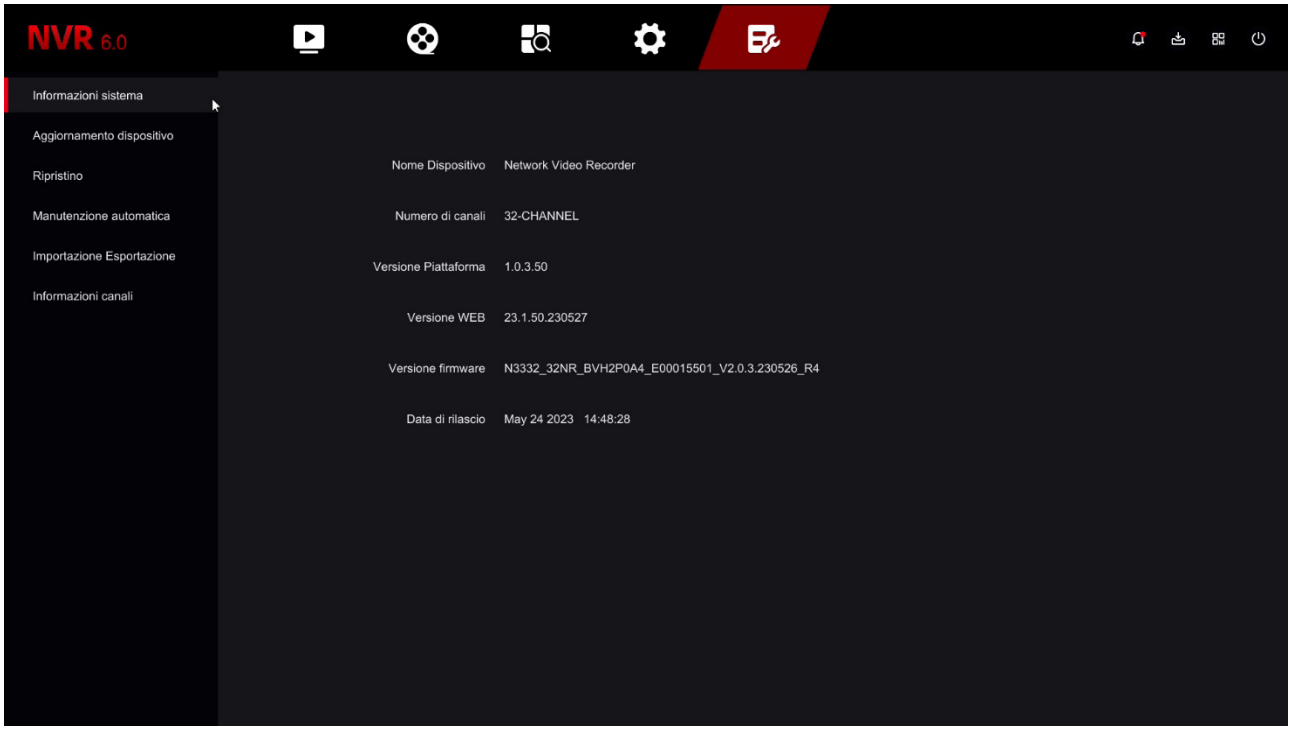

NVR 6.0
Sistema
Rete
Gestione canali
Eventi
Registrazione
Pianifica
Parametri
Archiviazione
Config. Avanzata
Conf.base
Conf.completa
Configurazione
S.M.A.R.T
HDD N. 1
Tipo di test Breve
Temperatura 33
Previsione di durata (h) 98096
Condizioni di test 0
Auto valutazione PASSED
Valutazione generale PASSED
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 system maintenance.

SYSTEM INFORMATION

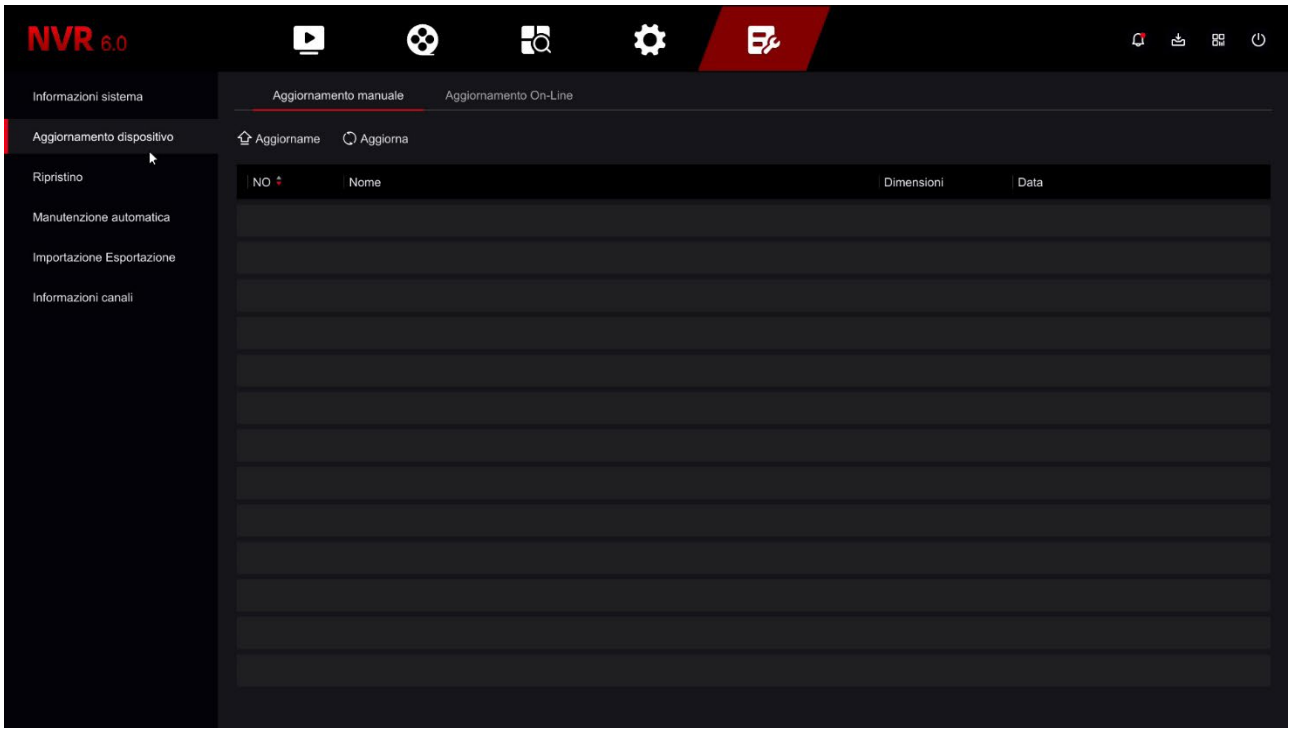
On this page you will find information about your video recorder with the firmware version it is the internal software of the device



DEVICE UPDATE | MANUAL UPDATE

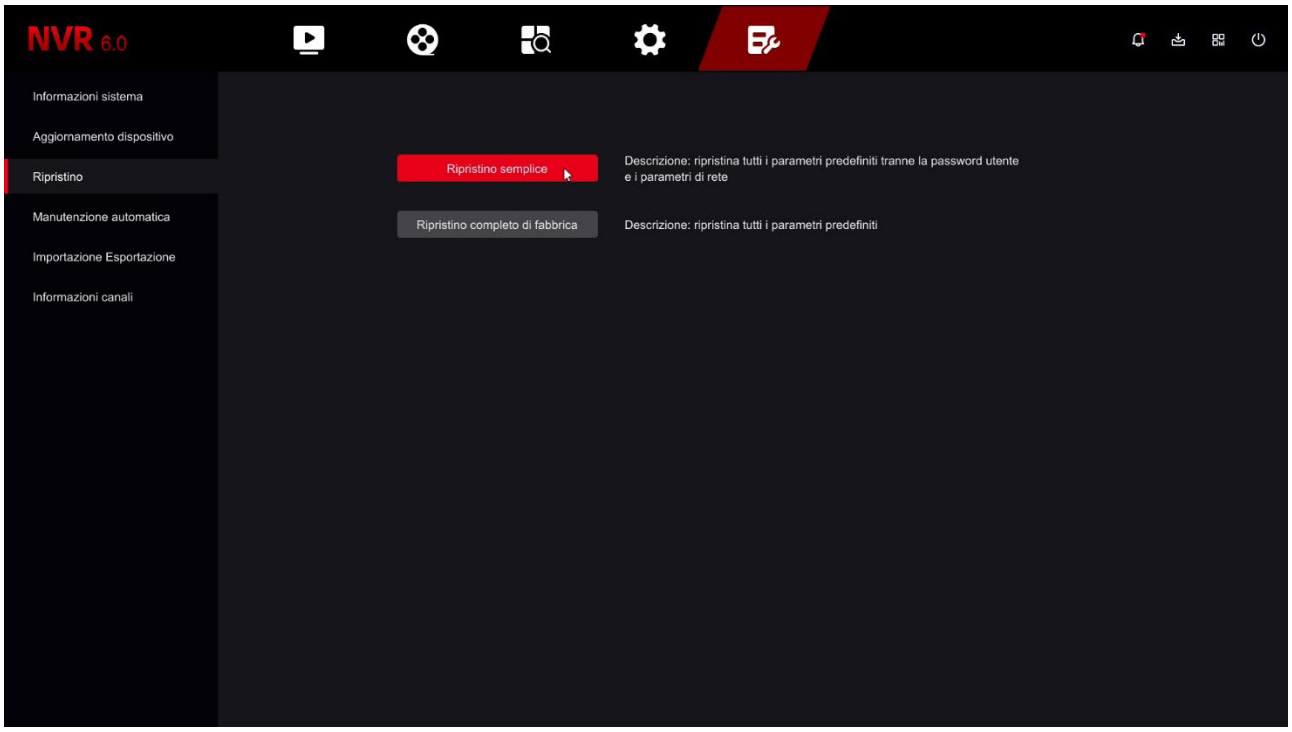
On this page you can update the firmware of your device if you have received a firmware file. update from our customer service. The file must be copied to a USB stick then inserted into the NVR/DVR. By inserting the USB stick the file is detected and listed in the table. To start the update, choose the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

The UPDATE button searches again for the update file.



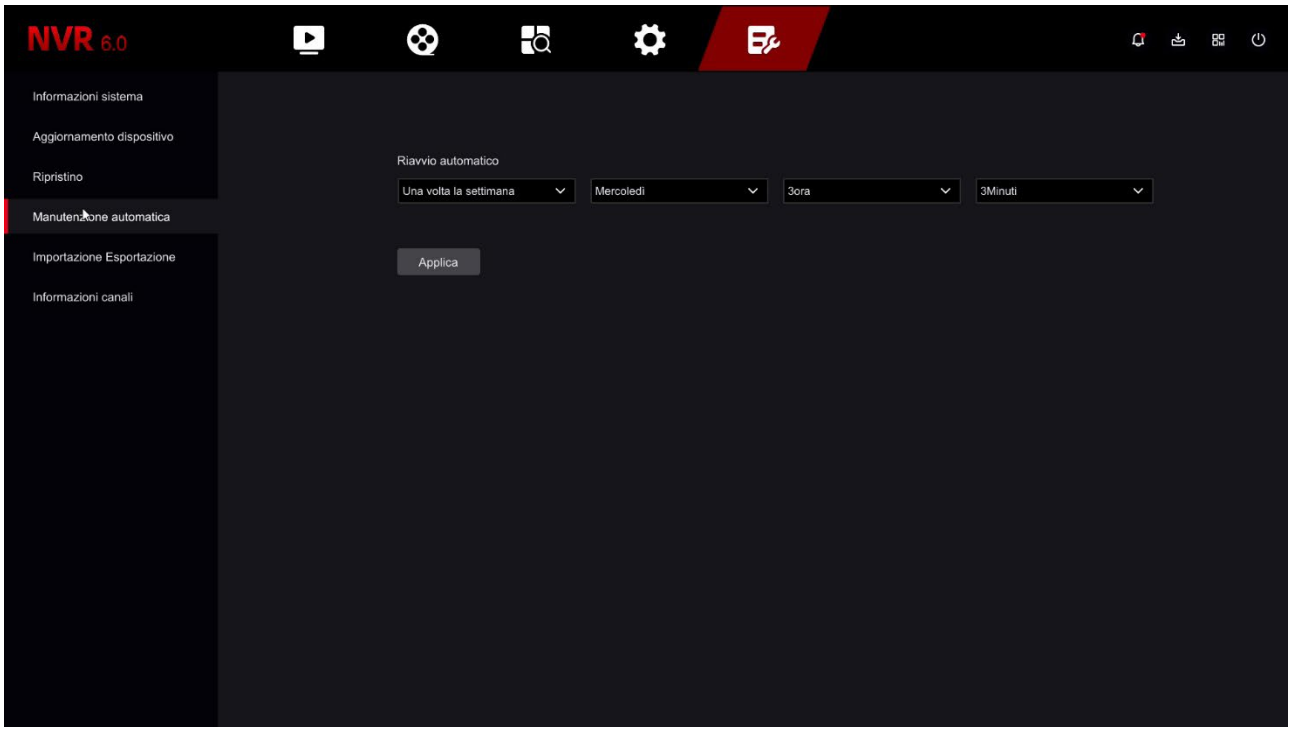
RESTORATION

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



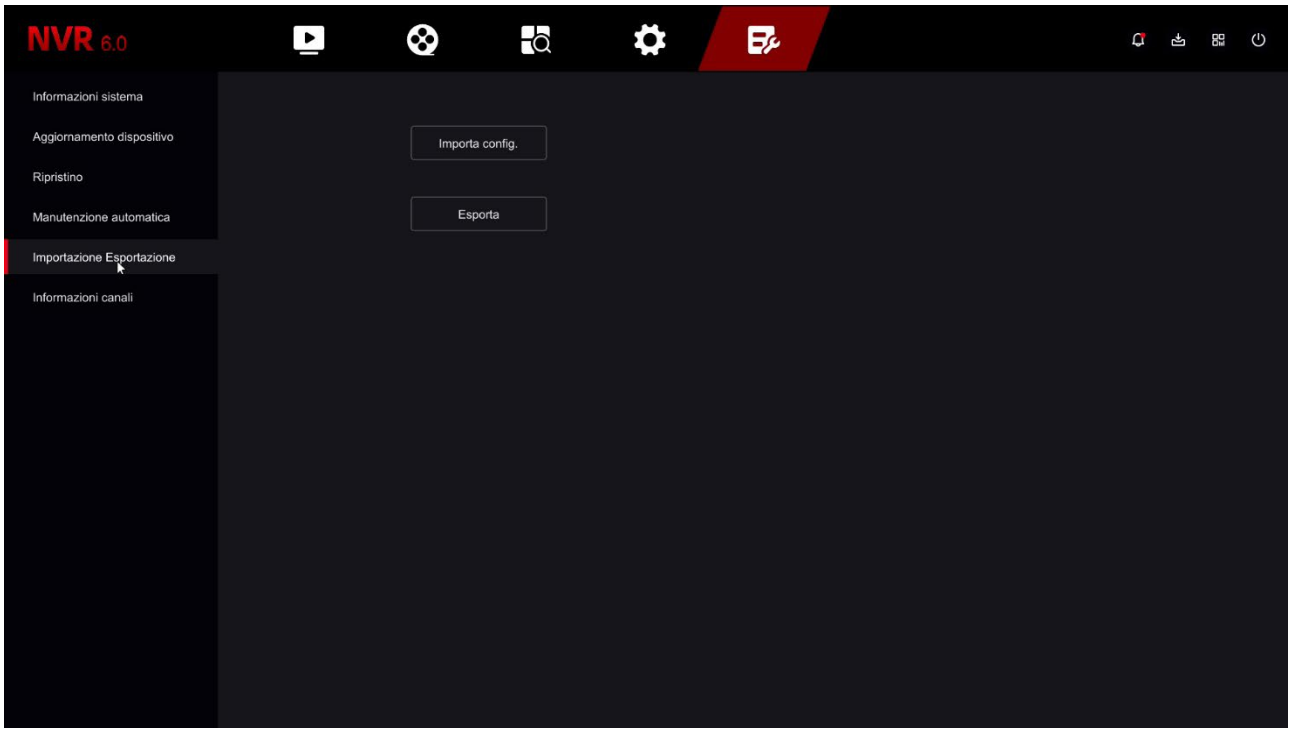
AUTOMATIC MAINTENANCE

In this page you can set the automatic reboot of the DVR/NVR which is set by default once a week



IMPORT / EXPORT

On this page you can export the entire DVR/NVR configuration to a file or import a previously exported configuration. This is a useful feature to save the configuration performed in case of failure.



CHANNEL INFORMATION

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