PRO

MANUAL
ELKRON-ONE

ELKRON PRO
The key to security

Contents

Part I – GENERAL **4**

INTRODUCTION TO ELKRON-ONE **5**
ADJUSTING Elkron-ONE FOR YOUR DISPLAY 7
LOGIN 7
WORK AREAS 8
PASSWORD RENEWAL 9
SWITCH USERS WITHOUT LOGGING OUT 10
USER DISCONNECTED 10
LOGOUT 11
SYSTEM NOTIFICATIONS 12
INTERNAL MESSAGES 12
STORAGE USAGE 13
CONNECTED USERS 13
SERVER CONNECTION 14
ABOUT ELKRON-ONE 14
ONLINE HELP 15

INTERFACE MANAGEMENT **16**

Part II – OPERATOR **17**

RESOURCE AREA AND TREE VIEW **18**
MANAGING DEVICE NOTES IN THE TREE VIEW 21
DEVICE INTEROPERABILITY 25
REMOTE COMMANDS 28
MULTIPLE MEDIA VIEWER 31
CONFIGURED LAYOUTS 32
VIEWING LIVE VIDEO 35
VIEWING RECORDED VIDEO 39
MOTION DETECTION 39
PLAYBACK TIMELINE 42
CONTINUOUS PTZ AND JOYSTICK 43
AUDIBLE ALARM 43
VIDEO BROWSER 45

OPERATIONAL CONTROL **49**

EVENT MANAGEMENT **52**
ACKNOWLEDGING AN ALARM 53
VIEWING ALARM ATTACHMENTS 57
VIEWING ALARM DETAILS 57
CLOSE EVENT AND SEND TO DAILY REPORT 61

CONFIGURING ALARM VIEWS **67**

SEARCHING AND EXPORTING DATA **69**
SEARCH RESULT REPORTS 80
PRINTING DATA 81
EXPORTING DATA 82

FLOOR PLANS **95**

SITES **96**

VOIP MODULE **97**

Part III ADMINISTRATION **104**

DEVICE MANAGEMENT **105**

CONTROL PANELS **114**

SCHEDULES **116**

DVR MANAGEMENT **117**

EVENTS – ACTIONS **120**

USER ACCOUNTS **123**
USER MANAGEMENT 123

LOG MANAGEMENT **127**

FLOOR PLAN AND SITE MANAGEMENT **129**

ACTIVE VIDEO SURVEILLANCE **133**

CLIENT SETTINGS **138**

INACTIVITY TIMEOUT **142**

EVENT CONFIGURATION **144**

WEB ADMIN **146**

USER PERMISSIONS **155**

Part I – GENERAL

INTRODUCTION TO ELKRON-ONE

Elkron-ONE is an application for managing integrated surveillance systems.

Through a simple user interface, Elkron-ONE provides full management of video streams and alarms from devices distributed across multiple locations. In particular, Elkron-ONE allows you to:

- record and archive video streams, then search for and view them;
- view live video streams from devices;
- configure each camera with precise operating parameters for recording mode and image quality;
- configure user accounts to restrict access to specific software features to authorised users only;
- control camera pan, tilt and zoom, and manage preset positions;
- organise data into reports;
- print and export data.

Elkron-ONE uses a multi-tier application architecture comprising:

- a client module installed on operators' workstations;
- an application logic module that forms an integral part of the Elkron-ONE server system;
- an optimised data access module.

This manual is divided into three main parts:

- Part I: General, describing the basic ways of using the system.
- Part II: specifically for the Operator;
- Part III: specifically for the Administrator.

The document includes illustrations that guide users through the steps required to use the system's functions.

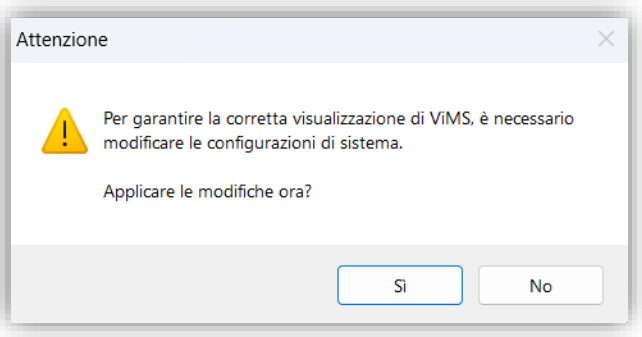
Network requirements

The table lists the requirements for configuring the Elkron-ONE client's network connection.

FUNCTION	PROTOCOL	PORT(S)	CLIENT TO SERVER	SERVER TO CLIENT
Server connection	TCP	80	Yes	
NTP (system time synchronisation)	UDP	123	Yes	Yes
Live video streaming (DVR recordings)	TCP	80. 443,8880, 55080, (16280)	Yes	
Real-time messages to clients	TCP	16447		Yes
SSH	TCP	22, 2222	Yes	
FTP	TCP	21	Yes	

ADJUSTING Elkron-ONE FOR YOUR DISPLAY

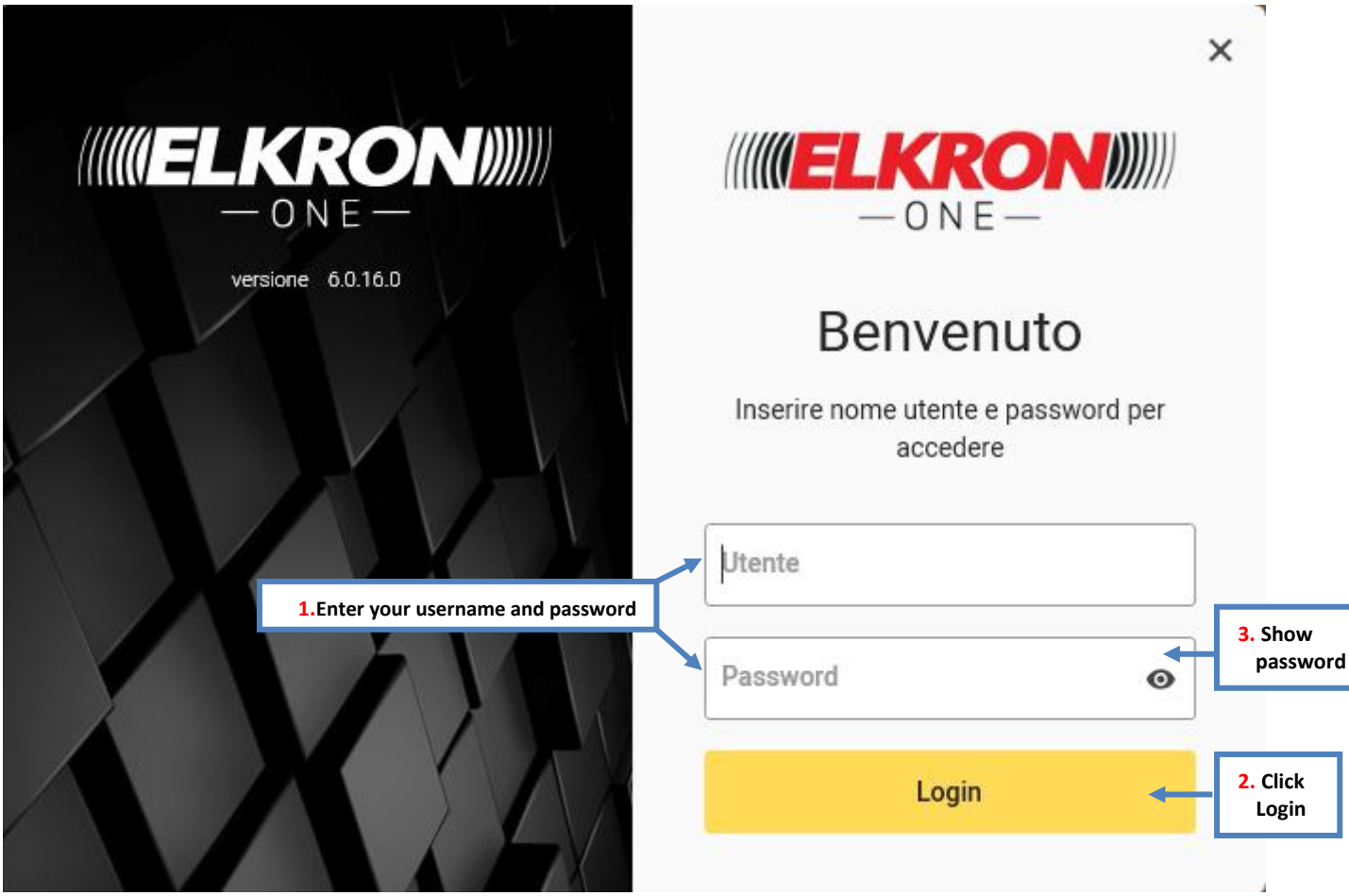
When Elkron-ONE starts for the first time, the following pop-up appears if the screen size and DPI settings are unsuitable for the application.



Click *Sì* (Yes) to change the settings and ensure that the Elkron-ONE platform is displayed correctly.

LOGIN

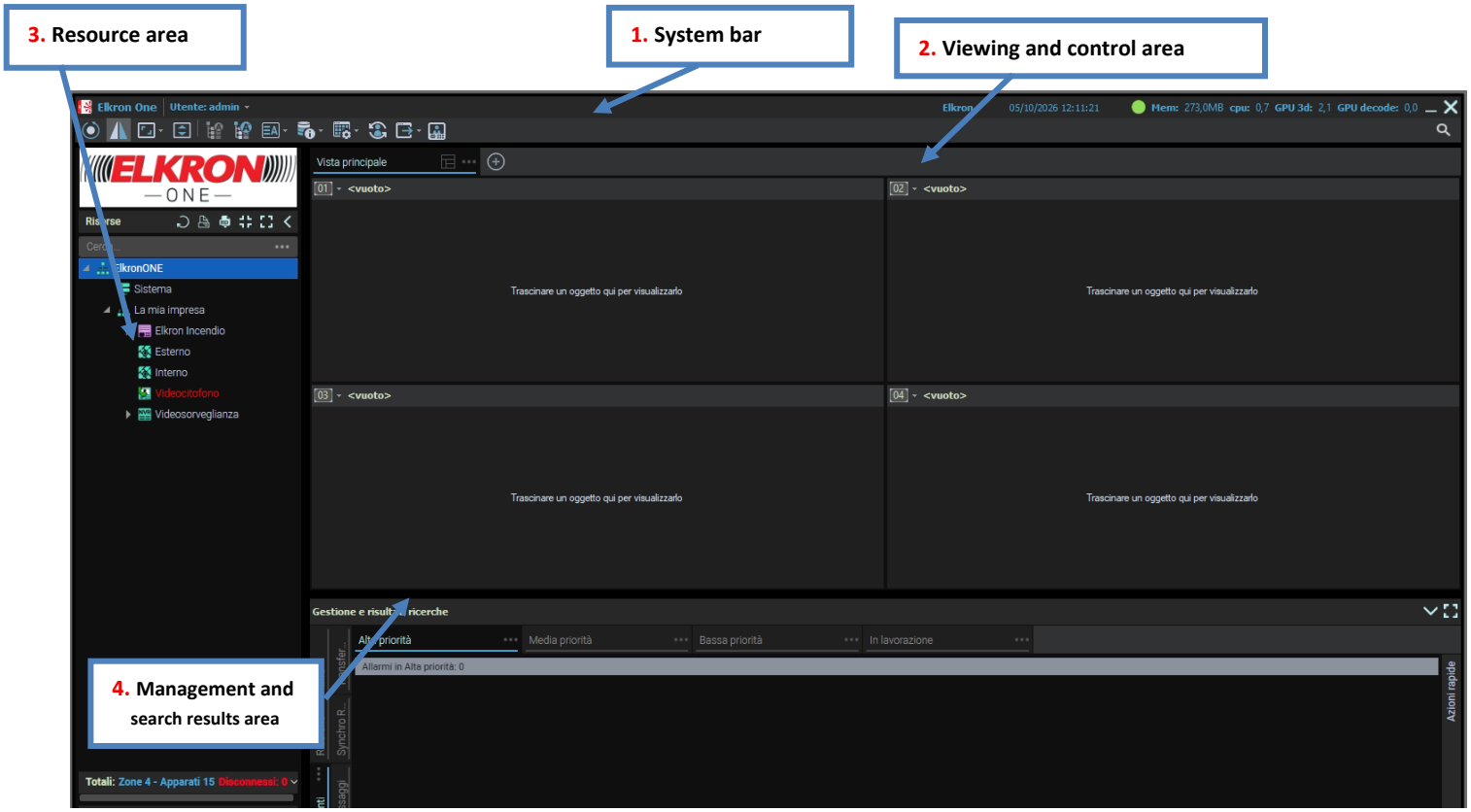
To access the system, enter your login credentials.



An incorrect username and/or password is reported during login.

WORK AREAS

Elkron-ONE is organised into functional areas for day-to-day operation:



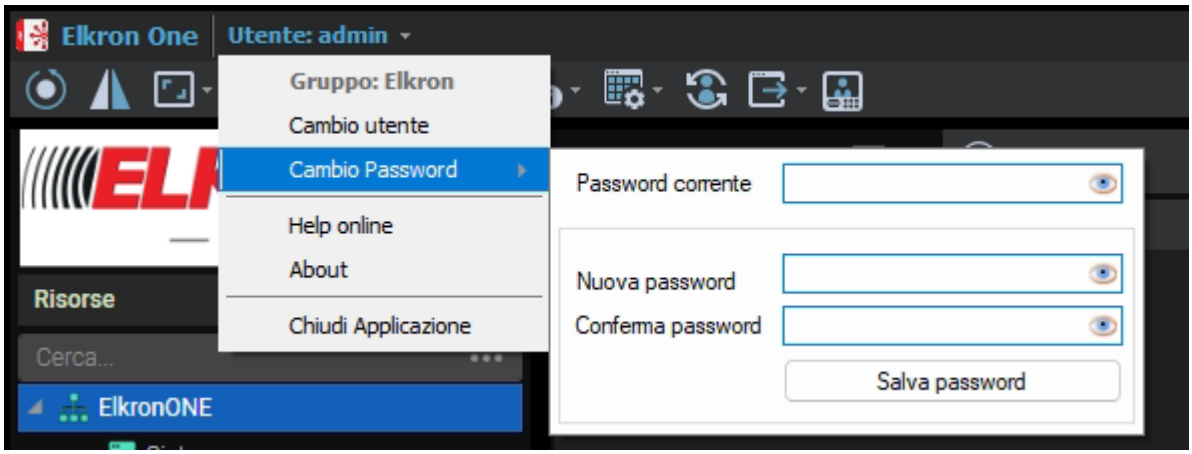
1. **RESOURCE AREA:** displays the system resources in a tree view and provides quick access to device operations.

2. **SYSTEM BAR:** provides commands for managing the layout, viewing system information, accessing administration functions and searching archived data.

3. **VIEWING AND CONTROL AREA:** displays data using the selected number and type of viewers.

4. **MANAGEMENT AND SEARCH RESULTS AREA:** includes alarm management and access to database search results.

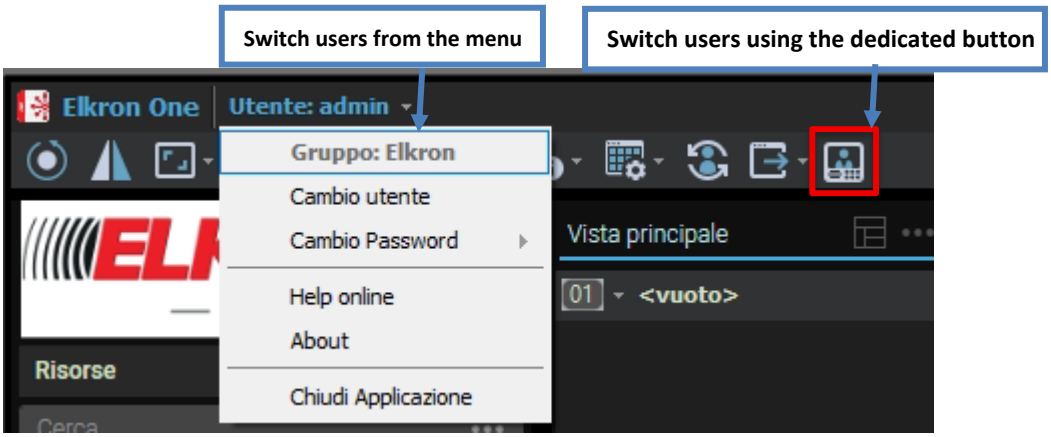
If password expiry is enabled, a pop-up appears at each login during the ten days before expiry, informing the operator how much time remains before the password expires. The image shows how to change the password:



Note: Password expiry and the password validity period can be configured on the Elkron-ONE **AdminWeb** page.

SWITCH USERS WITHOUT LOGGING OUT

The image shows two ways to switch users without logging out:



In both cases, the login window appears so that the new credentials can be entered.

After the new login, the client updates to reflect the new user's permissions. The alarm queue remains active.

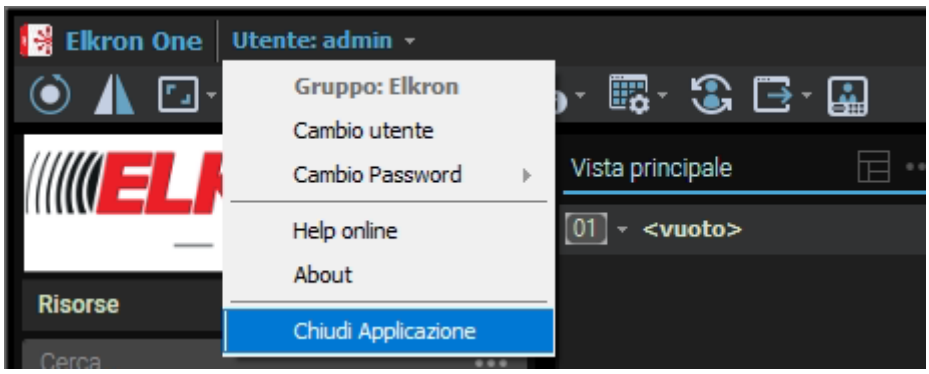
USER DISCONNECTED

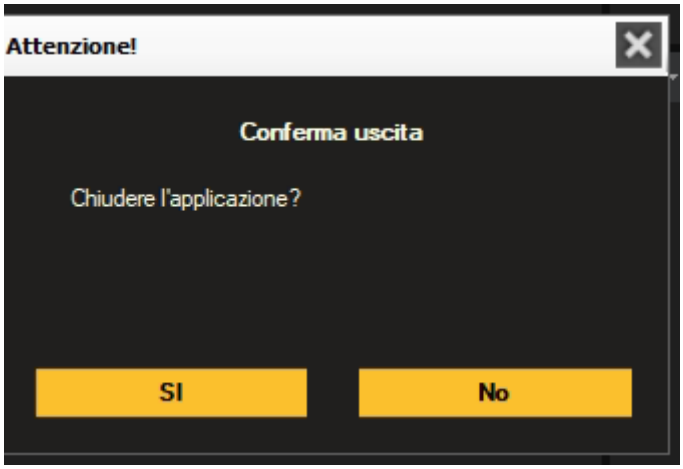
A working session may be interrupted in the following cases:

- another user logs into the system using the credentials currently in use;
- the current user's permissions for specific functions are changed (enabled or disabled);
- the current user account is changed or deactivated;
- a second login is made from the same client.

LOGOUT

In addition to using the X in the top-right corner of the application, the images show how to log out and close Elkron-ONE:

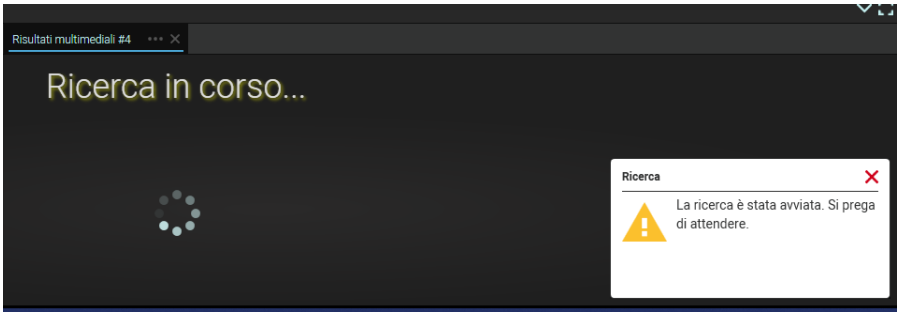




Elkron-ONE provides several ways to report the outcome or status of user operations, provide system information and indicate the status of data usage or connected users.

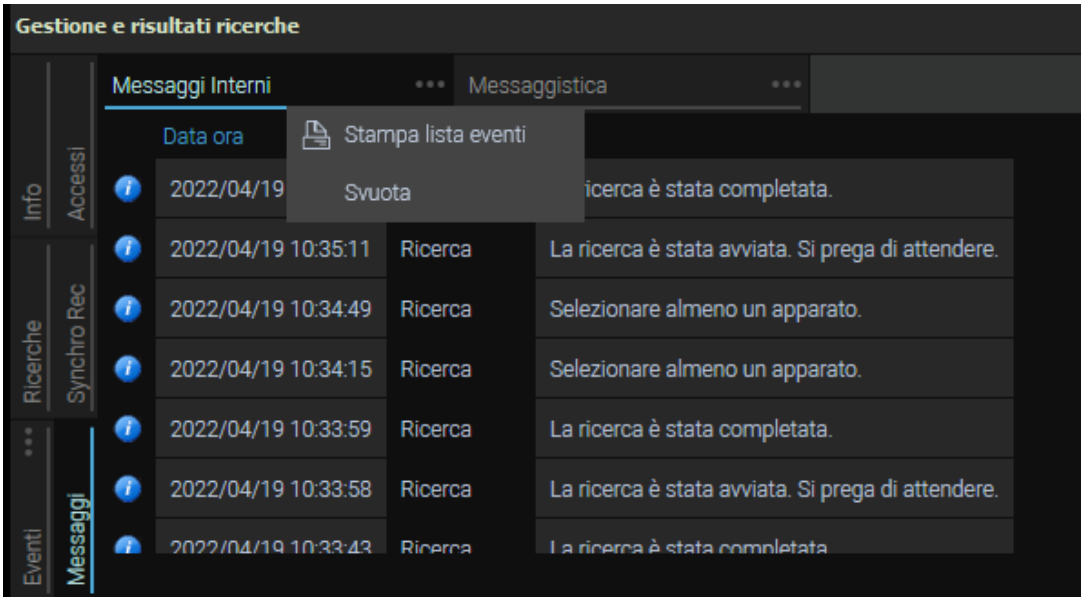
SYSTEM NOTIFICATIONS

In response to user actions, the bottom-right corner of the system displays temporary panels:



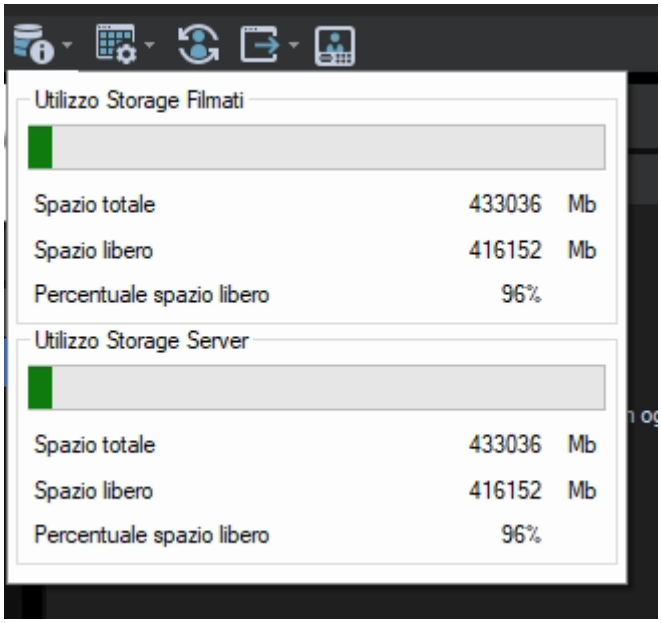
INTERNAL MESSAGES

A dedicated area in Elkron-ONE stores all notifications from the current working session for consultation:



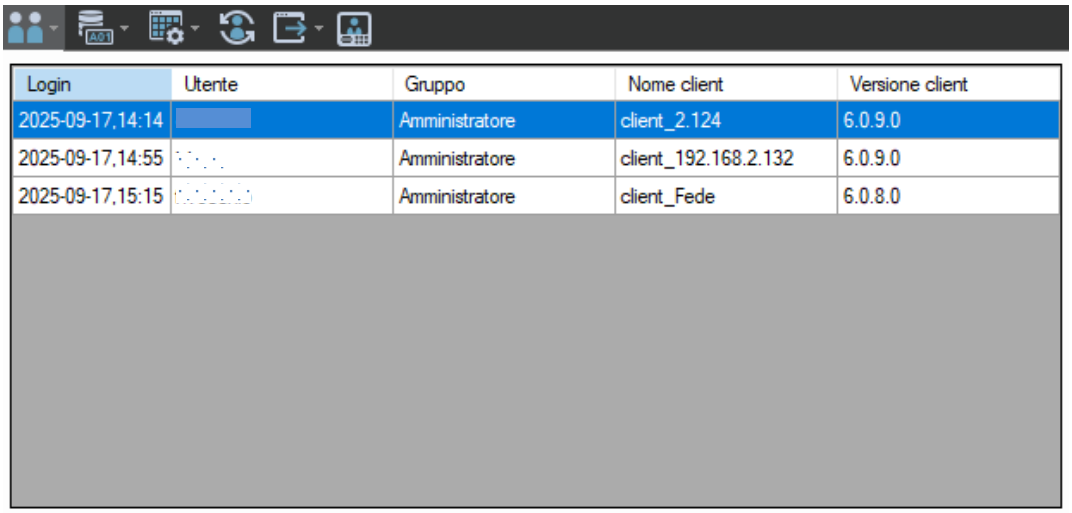
STORAGE USAGE

If the available system storage falls below the configured threshold, data is deleted from the system:

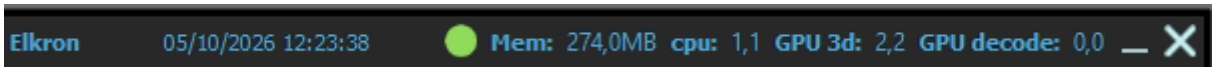


CONNECTED USERS

The image shows how to display the users currently logged into the system.

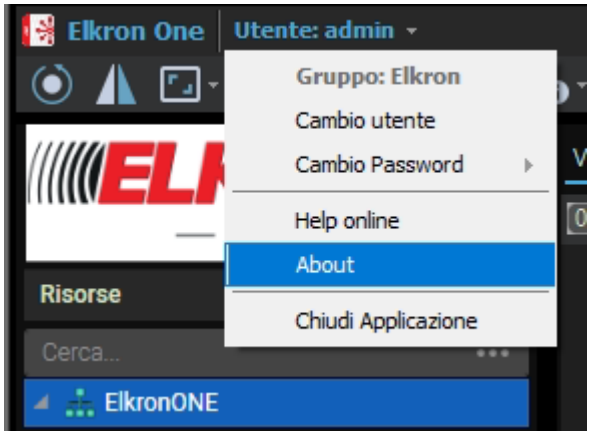


SERVER CONNECTION



- **green:** connection to the server established;
- **orange:** connection error;
- **red:** server unreachable.

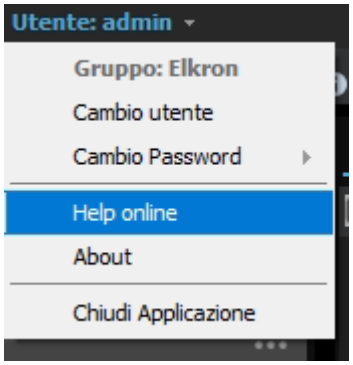
ABOUT ELKRON-ONE





ONLINE HELP

The image shows how to access the Elkron-ONE user manual in PDF format:



Note: If the manual is not up to date, clear the cache of the web browser in use.

INTERFACE MANAGEMENT

To make work easier, users can change some Elkron-ONE interface settings, particularly to optimise the display of the work areas. In order:

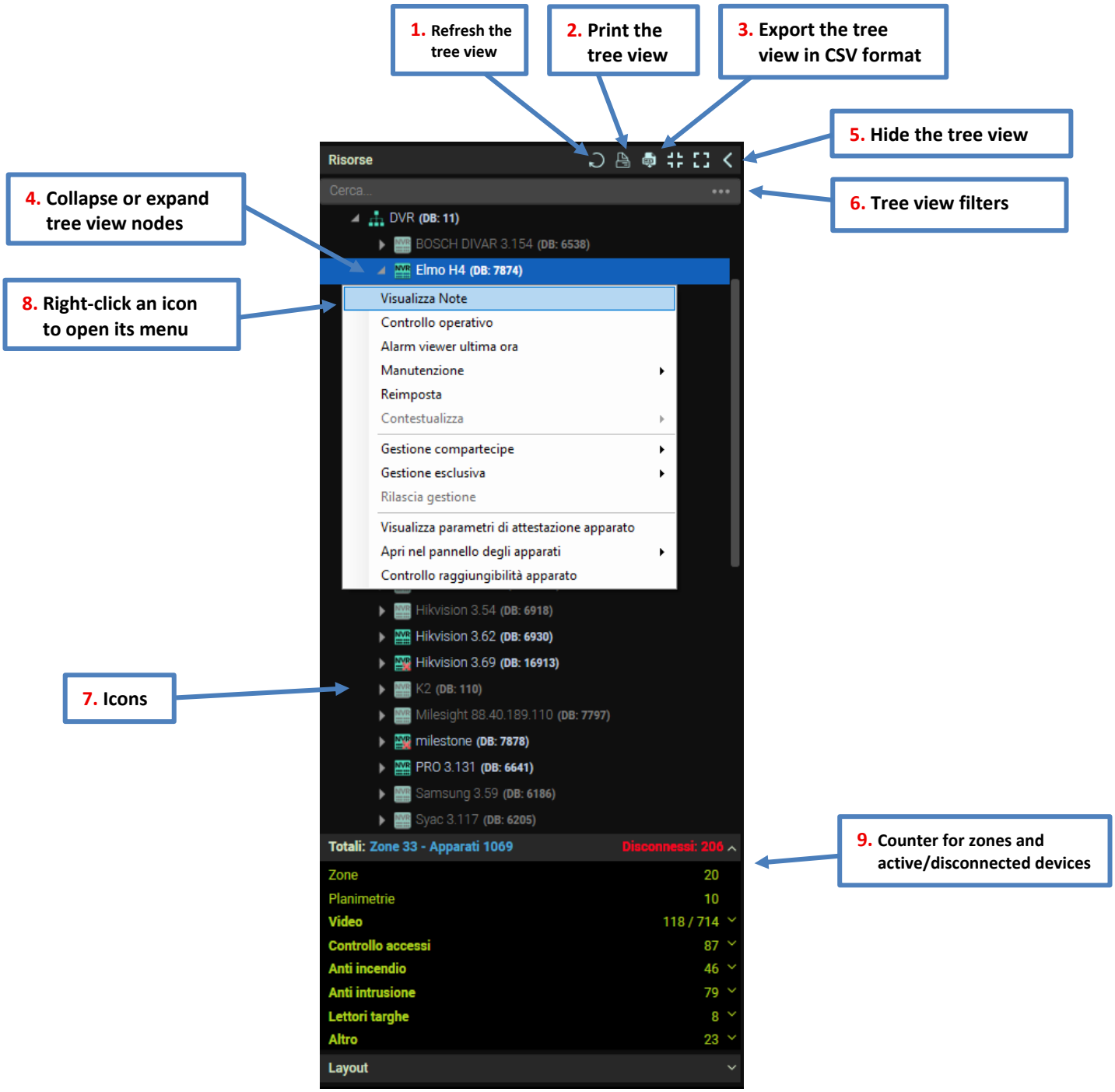


1.  Restore the default layout after interface changes;
2.  Right-to-left layout: position the resource area on the left or right of the page;
3.  Aspect Ratio options: Original, Extended, 16/9 or 4/3;
4.  Matrix mode;
5.  Change the font used for device names in viewers;
6.  Increase/decrease the font size across all tree views;
7.  Storage usage;
8.  Show the administration panel;
9.  Switch users;
10.  Go to the video import/export tools;
11.  Open the VoIP module to call other VoIP devices/clients;

Part II – OPERATOR

RESOURCE AREA AND TREE VIEW

The resources connected to Elkron-ONE are displayed in a hierarchical tree view. Its root node identifies the installation site. Levels and sublevels branch from this node to represent the zones and subzones containing the devices and resources managed by Elkron-ONE. The image shows the actions available for adjusting the resource display in the tree view and performing certain management operations. Search filters help locate resources quickly in large tree views. A counter also shows the total number of zones and devices and a detailed count for each resource type:



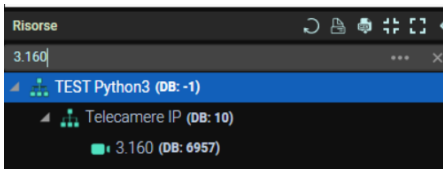
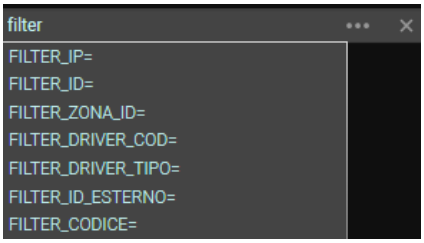
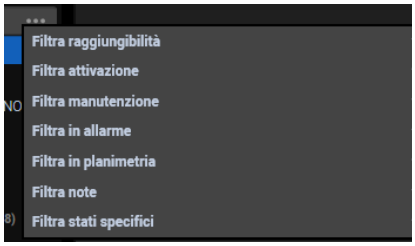
Icons

Each device has a specific icon that updates when its status changes. The icon appearance indicates the device's operating status:

DEVICE ICON	STATUS
	Device **unreachable**
	Device **disabled**
	Device under **maintenance**
	Device **being viewed**
	Device **not recording**

Tree view filters

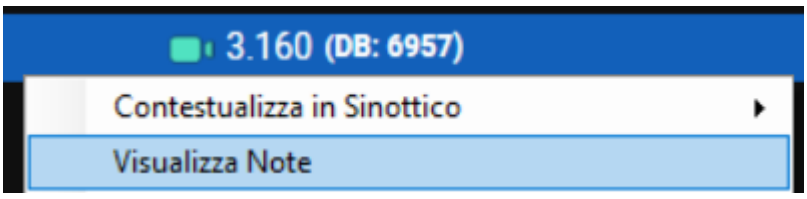
The tree view offers several types of filter to display only devices that meet specific criteria. The zone and device counters update to match the filters. Multiple filters can also be combined using the **AND** operator.

TEXT FILTER	ADVANCED FILTER	STATUS FILTER
		
Quickly find a device in a large tree view. Entering text displays the matching resources and the tree view levels containing them. The search updates immediately as each letter is entered.	The advanced ***filter*** is activated by starting to type filter in the text box. **FILTER_IP:** searches for devices by IP address; **FILTER_ID:** filters by device ID and returns only devices with the exact ID entered; **FILTER_DRIVER_COD:** filters for devices whose driver has the code entered in the filter; **FILTER_DRIVER_TIPO:** searches for devices whose driver name contains the string entered in the filter. For example, searching for “SAM” returns devices with a “SAMSUNG” driver; **FILTER_ID_ESTERNO:** this filter searches the Device ID, used for example in access control. It also matches substrings: for example, searching for a Device ID of “I010” returns devices with IDs “I010a”, “I010b”, etc.; **FILTER_CODICE:** filters for devices with the exact code entered in the filter. **FILTER_ZONA_ID:** filters by zone ID and returns the zone and the devices it contains.	The status filter displays only devices in the selected states in the tree view. **REACHABILITY:** filters for devices that can or cannot be reached by the Elkron-ONE server. **ACTIVATION:** filters for active or inactive devices. **MAINTENANCE:** filters for devices that are or are not under maintenance. **ALARM:** filters for devices in an alarm state. **FLOOR PLAN:** filters for devices that are or are not on a floor plan. **NOTES:** filters for devices with highlighted notes, notes currently valid or valid in the future, or notes containing the text entered. **SPECIFIC STATES:** filters for devices in the states selected by the user. The available states depend on the control system type: intrusion alarm control panels, fire alarm control panels or access control.

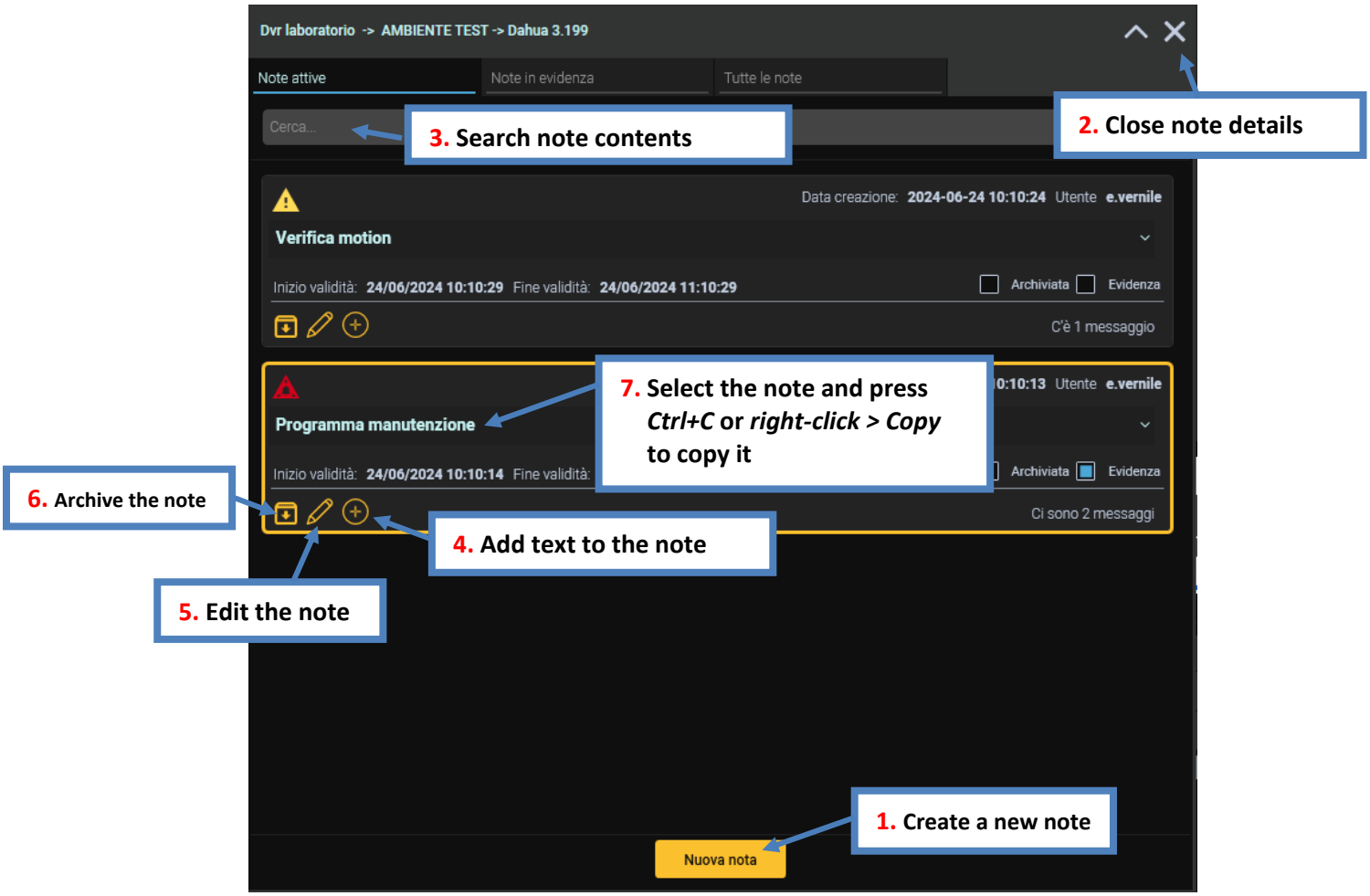
MANAGING DEVICE NOTES IN THE TREE VIEW

Elkron-ONE includes a module for managing notes on resources in the tree view. This function can help users follow operating procedures by sharing device information or highlighting alerts on specific resources in the tree view.

Users can attach notes to devices and zones, view or edit existing notes, highlight particularly important notes and add information to existing notes.
Right-click a zone or device in the tree view and select **Visualizza Note (View Notes):**



The note management panel opens:



Each note shows the username and its validity start and end dates. It can contain several text messages, including messages added by different users. Only the user who created the note can edit or archive it.

Notes can be archived to indicate that they are no longer valid. If the archived note was the only note attached to a device, the icon indicating the presence of notes disappears from the tree view.

Specific icons next to the resource icon in the tree view indicate the presence of notes.

 The note is currently active because today's date falls between its validity start and end dates.

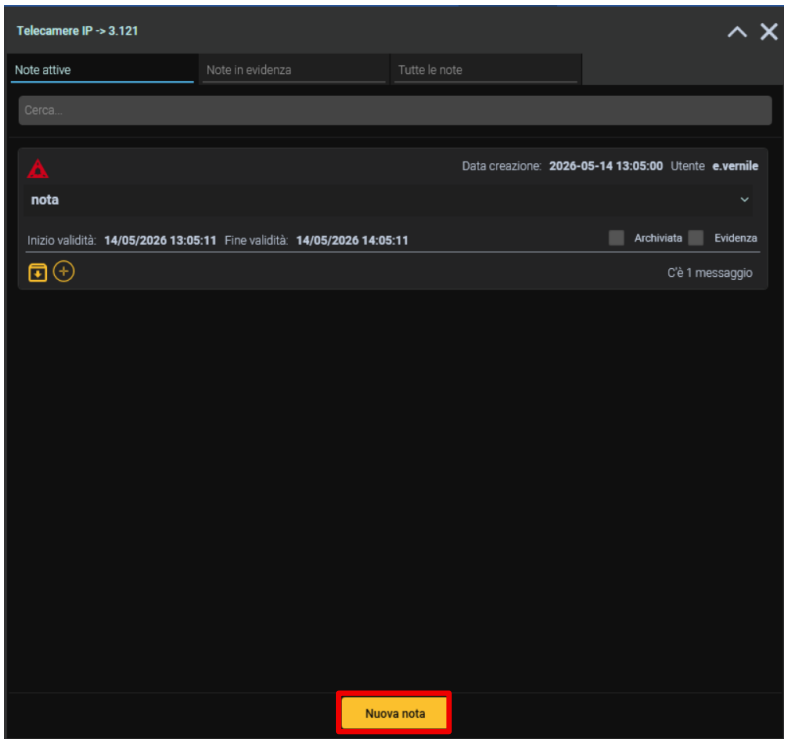
 The note will become active in the future because its validity start date is later than its creation date.

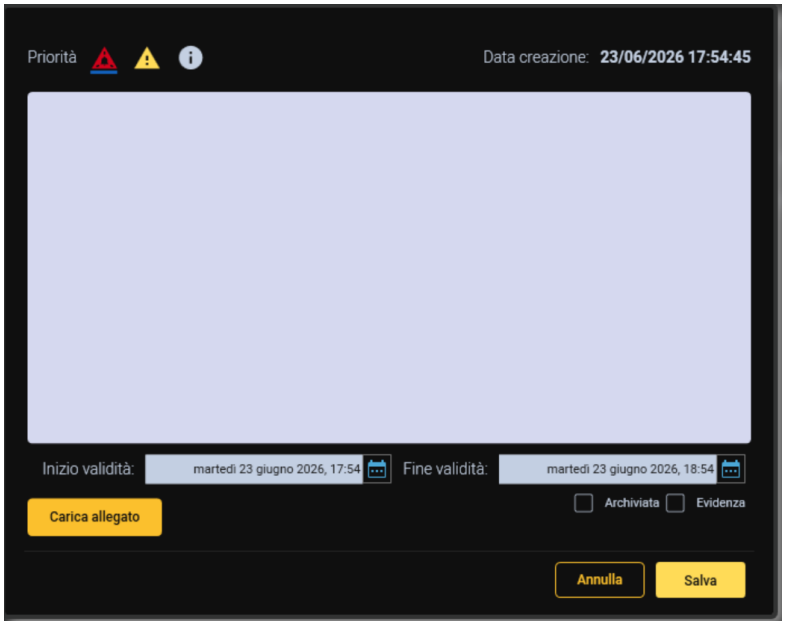
 The note appears at the top of the list because it has been highlighted.

> **Note:** If a note is highlighted, its icon remains in the tree view until the note is archived, even after it expires.

Adding a note to a resource in the tree view

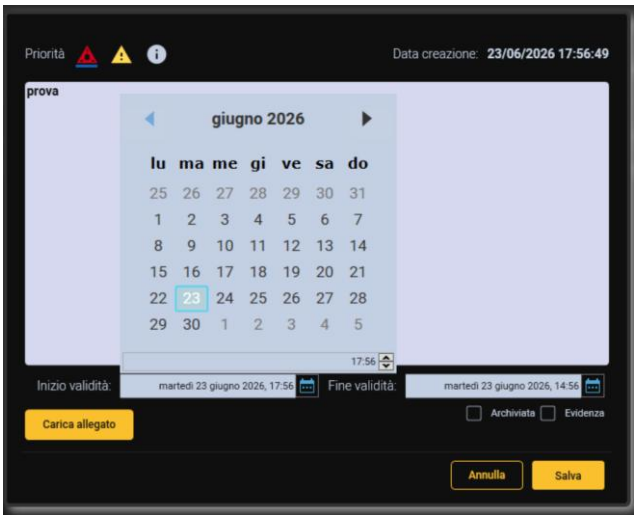
The image shows how to create a note for a device or zone:





To enter the note's validity start and end dates, select the value to change and overwrite it using the keyboard, 21/10/2019 11:50:50

or use the calendar:

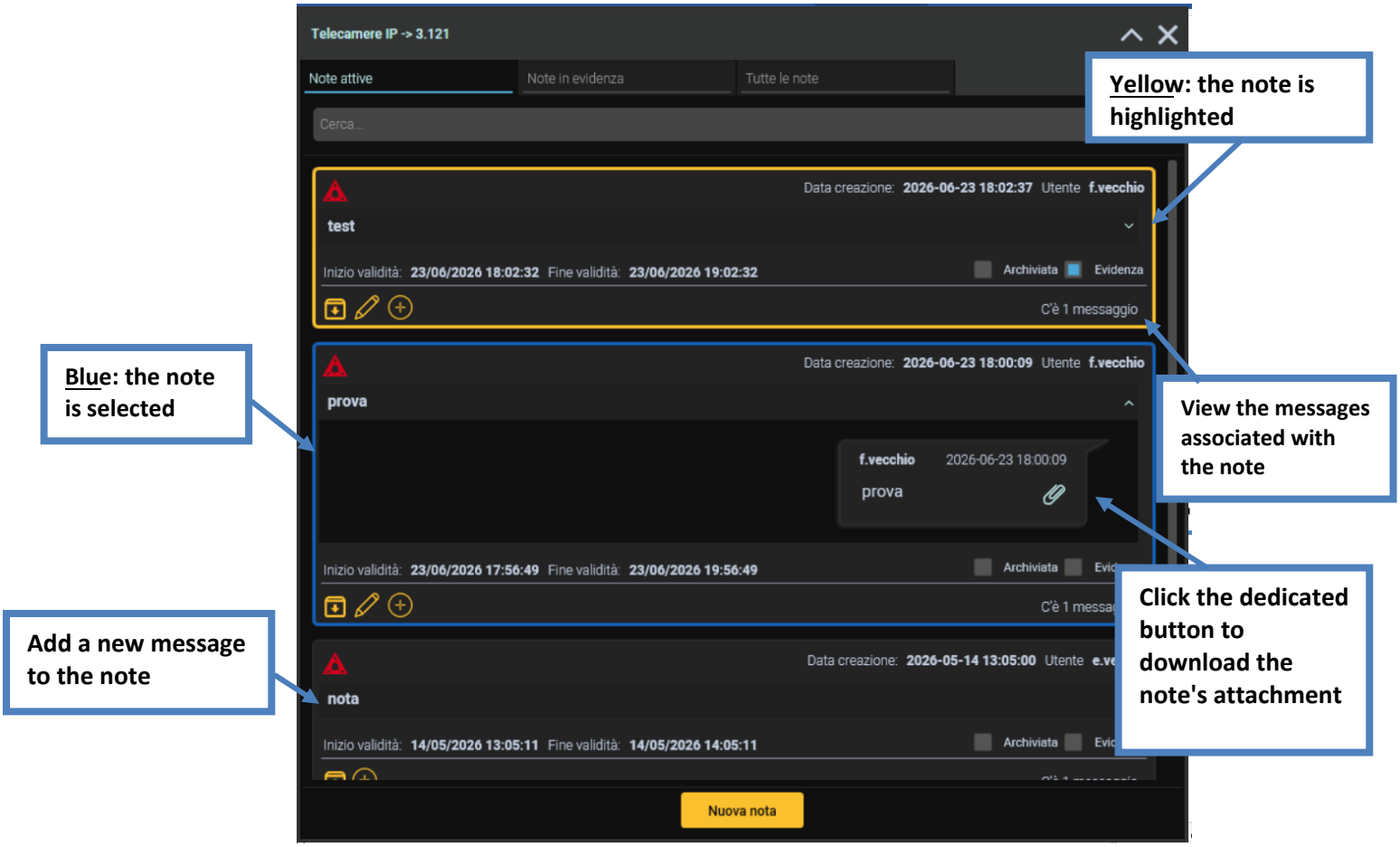


A pop-up alerts the user to any errors in the selected dates.

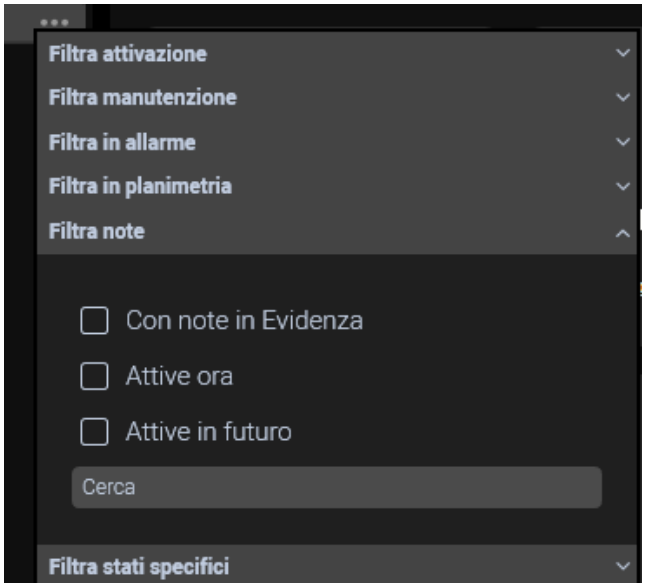
For example, if the validity end date is earlier than the validity start date:



The following image shows how to interpret notes created for a device:



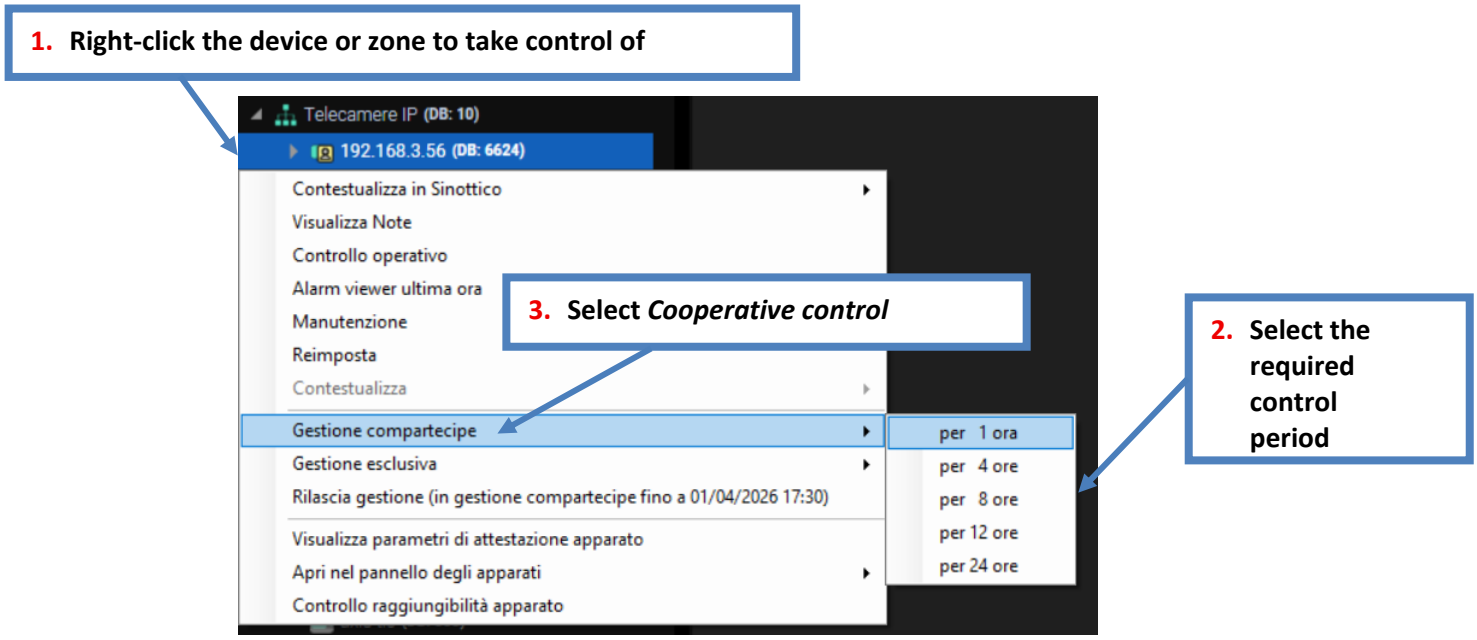
The tree view filter includes a specific search by note type:



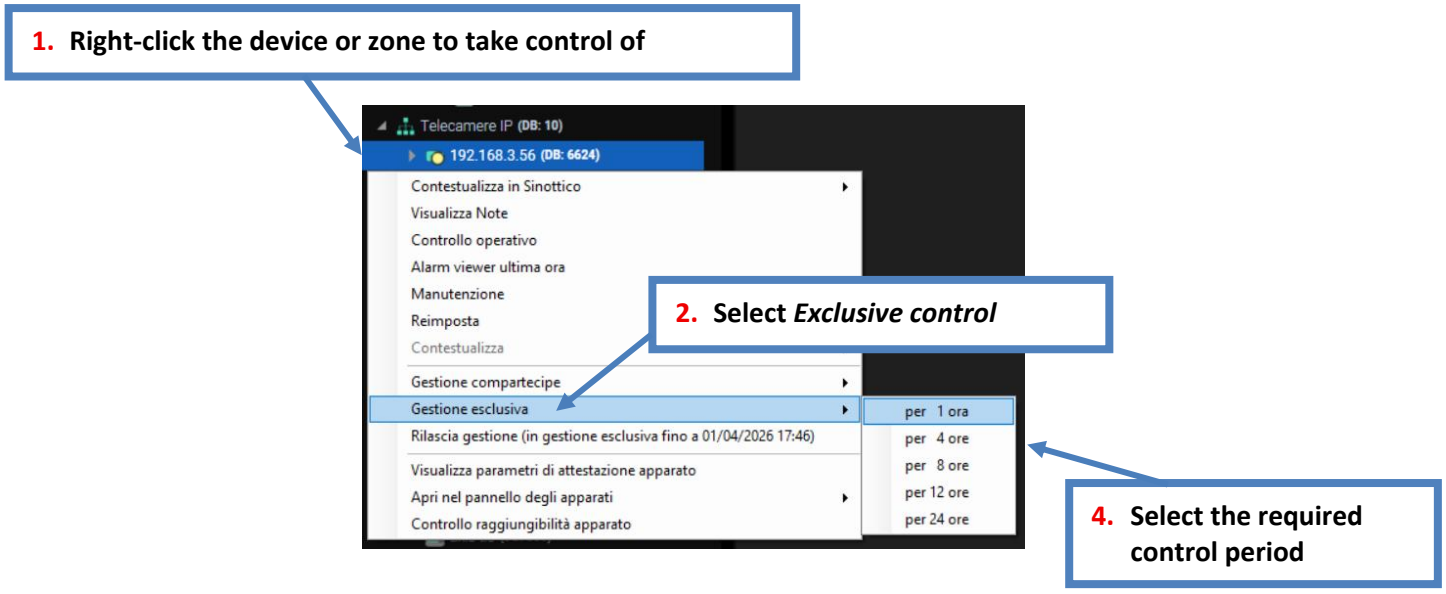
DEVICE INTEROPERABILITY

Elkron-ONE provides advanced functions for shared management of one or more devices by several users, or exclusive management by a single user.

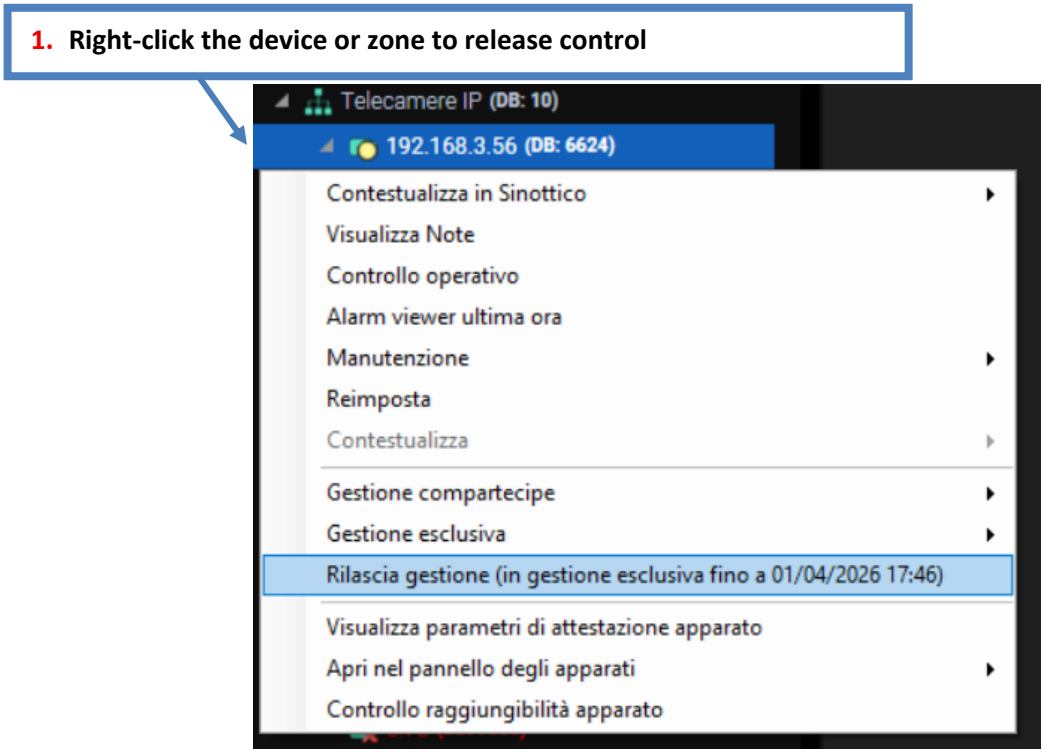
- The image below shows how to take **cooperative control** of a device or zone from the tree view:



- The image below shows how to take **exclusive control** of a device or zone from the tree view:



- The image below shows how to **release** shared or exclusive control of a device or zone from the tree view:



The table describes the possible interoperability states and the icon for each state:

STATUS	DESCRIPTION	ICON
Cooperative control (for all groups)	The device is freely available and can therefore be controlled and used by any user, regardless of their group.	
***Exclusive* control** (for the assigned group)	Data acquired from the device can be viewed and managed by the user who took control of it or another user in the same group.	
Cooperative control (for other groups)	Data acquired from the device can be viewed but cannot be managed because a user in another group has taken control of it. The group is identified in the corresponding tooltip.	
Exclusive control (for other groups)	Data acquired from the device can be neither viewed nor managed because a user in another group has taken control of it. The group is identified in the corresponding tooltip.	

The effects of shared and exclusive control vary according to the type of device on which control has been activated.

Specifically:

- **Cooperative control:**
  - For encoders, PTZ commands and access to recordings for the entire period during which control is active are restricted to users in the group that activated it. Recordings from this period are also automatically protected from deletion for a configurable period.

- **Exclusive control:**
  - For encoders, in addition to the cooperative-control restrictions above, users outside the group that activated control are denied access to live video and event reception. o For control panels, event reception and remote commands are restricted to

    users in the group that activated control.

Permissions for managing interoperability work as follows:

- Main tree view
  - A non-administrator user without the *"Allow taking/releasing device control"* permission and without the *"Force taking/releasing device control"* permission cannot manage interoperability. Right-clicking any device or zone in the tree view does not show interoperability options in the context menu; o A non-administrator user with the *"Allow taking/releasing device control"* permission but without the *"Force taking/releasing device control"* permission can manage interoperability for devices or zones that are not under control or are controlled by the user's own group. Right-clicking a device or zone controlled by another group shows disabled interoperability options in the context menu; o A non-administrator user with both the *"Allow taking/releasing device control"* permission and the *"Force taking/releasing device control"* permission has unrestricted control, like an administrator.
- Device Management
  - A non-administrator user without the *"Allow taking/releasing device control"* permission cannot see the interoperability-related "Diritti di utilizzo" (Usage rights) tab in Device Management.

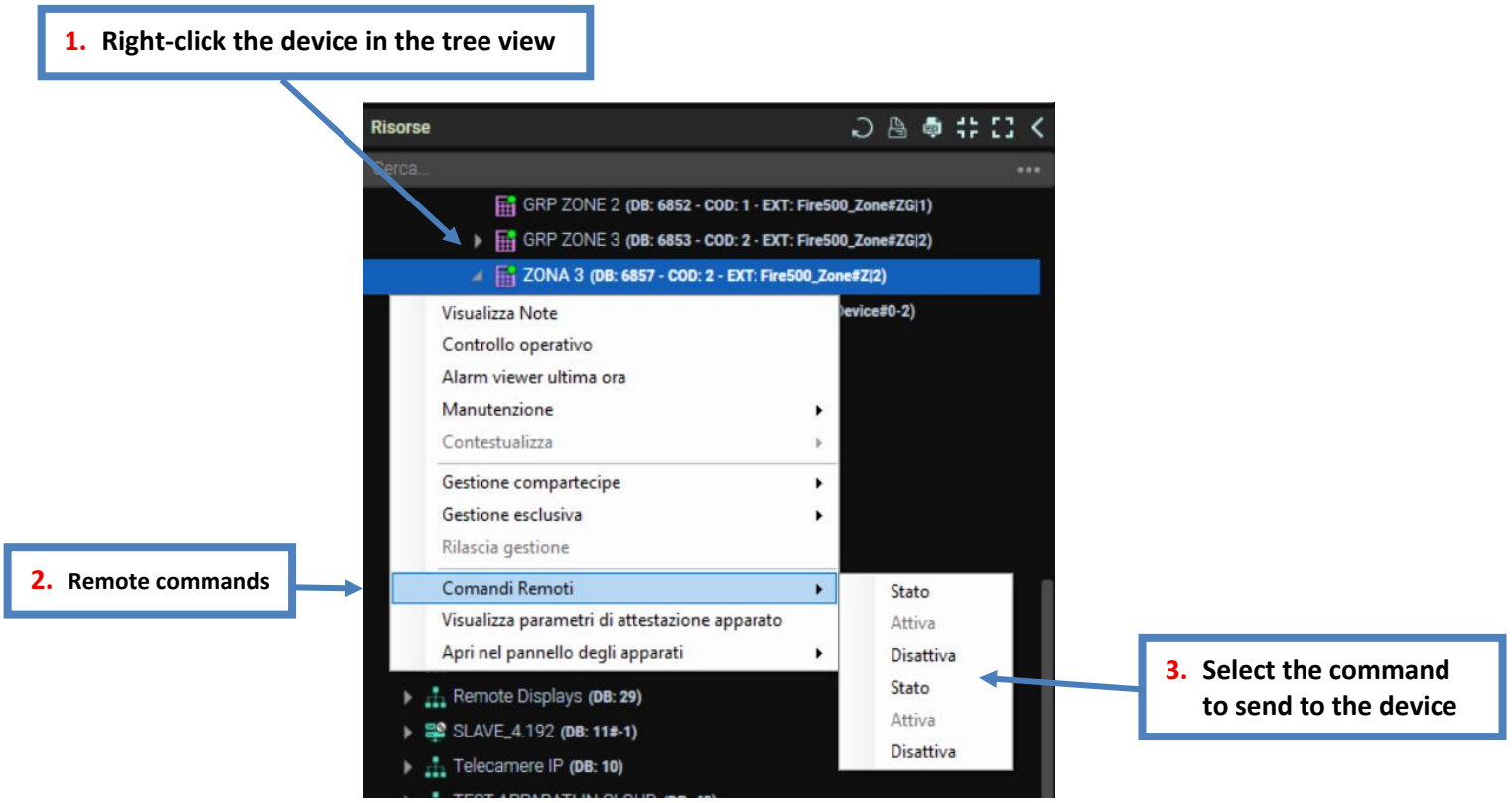
Note: The permissions of users in the administrator group are unaffected. Their access to video streams, PTZ control and interaction with control panels is therefore never blocked.
Administrators also always see the *Exclusive control* and *Cooperative control* icons in yellow.

Enabling *"Force taking/releasing device control"* automatically enables *"Allow taking/releasing device control"* when the settings are saved. The reverse does not apply.

For further information on taking or releasing control of a device from the Events/Actions tab instead of the tree view, see the relevant section of this manual.

REMOTE COMMANDS

Elkron-ONE allows certain operations on access control, intrusion alarm and fire alarm systems to be performed directly from the system. These operations are normally performed on the device itself. The image shows how to send commands to the device.



The following commands are generally available on most control panels. Device types supporting particular functions are indicated in brackets.

Intrusion alarm systems

Area commands

- **Status:** forces an area status request
- **Arm / Disarm:** arms / disarms the alarm system for the area
- **Abort:** cancels the arming command just sent (Galaxy)
- **Part Set:** arms the system, omitting open zones (Galaxy)
- **Force Set:** immediately arms the system, omitting open zones (Galaxy, ATS8400)
- **System Reset:** resets the control panel memories and outputs (Galaxy, ATS8400)
- **Reset memories:** resets the alarm memory (ENET)
- **Omit / Un-omit:** puts the area into / out of service (ENET)

Zone commands

- **Status:** forces a zone status request
- **Omit / Un-omit:** omits / reinstates the zone
- **Reset:** resets the alarm memory for the zone (ENET, ATS8400)

Output commands

- **Status:** forces an output status request
- **Activate / Deactivate:** activates / deactivates the output contact
- **Omit / Un-omit:** puts the output into / out of service (ENET)

Function commands

- **Execute:** executes the function on the control panel (ENET)

Fire alarm systems

Control panel commands

- **General ACK:** resets the alarm memory
- **Silence/Reset Outputs:** silences alarms and resets the outputs
- **General Reset:** resets the outputs and alarm memory

Detector commands

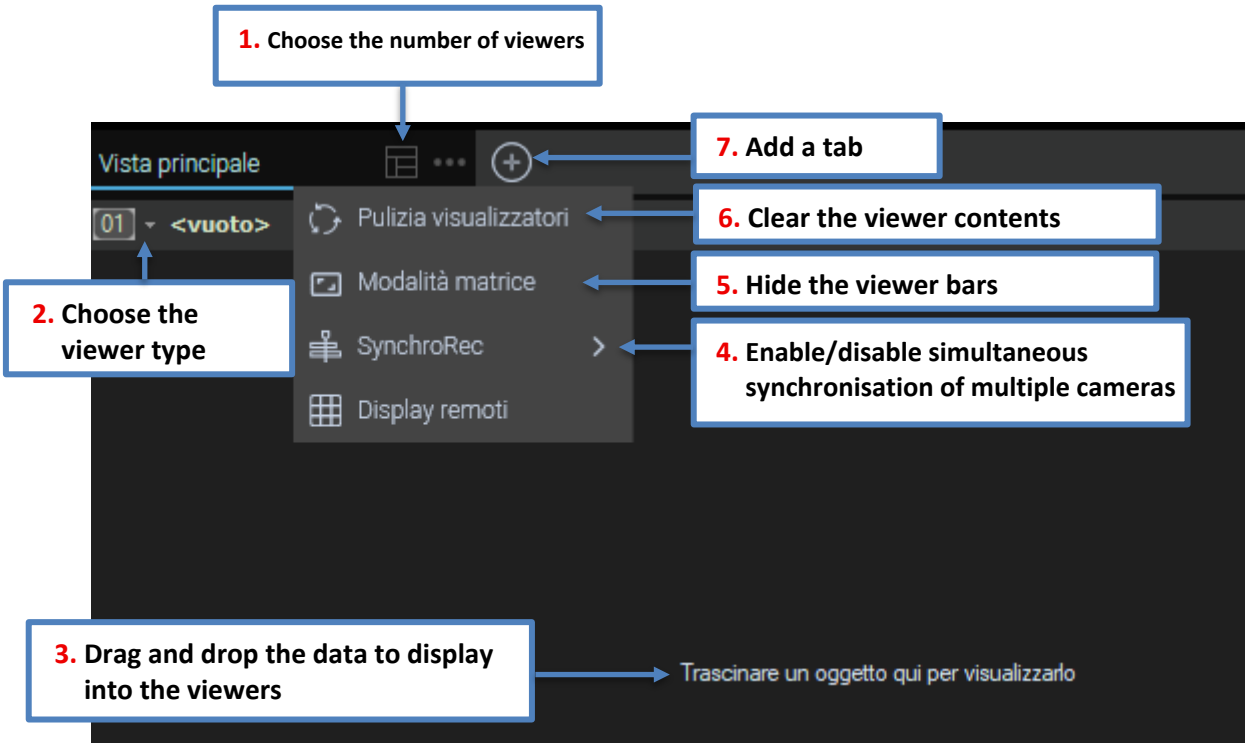
- **Status:** forces a detector status request
- **Omit / Un-omit:** omits / reinstates the detector

Zone commands

- **Status:** forces a zone status request
- **Omit / Un-omit:** omits / reinstates the zone

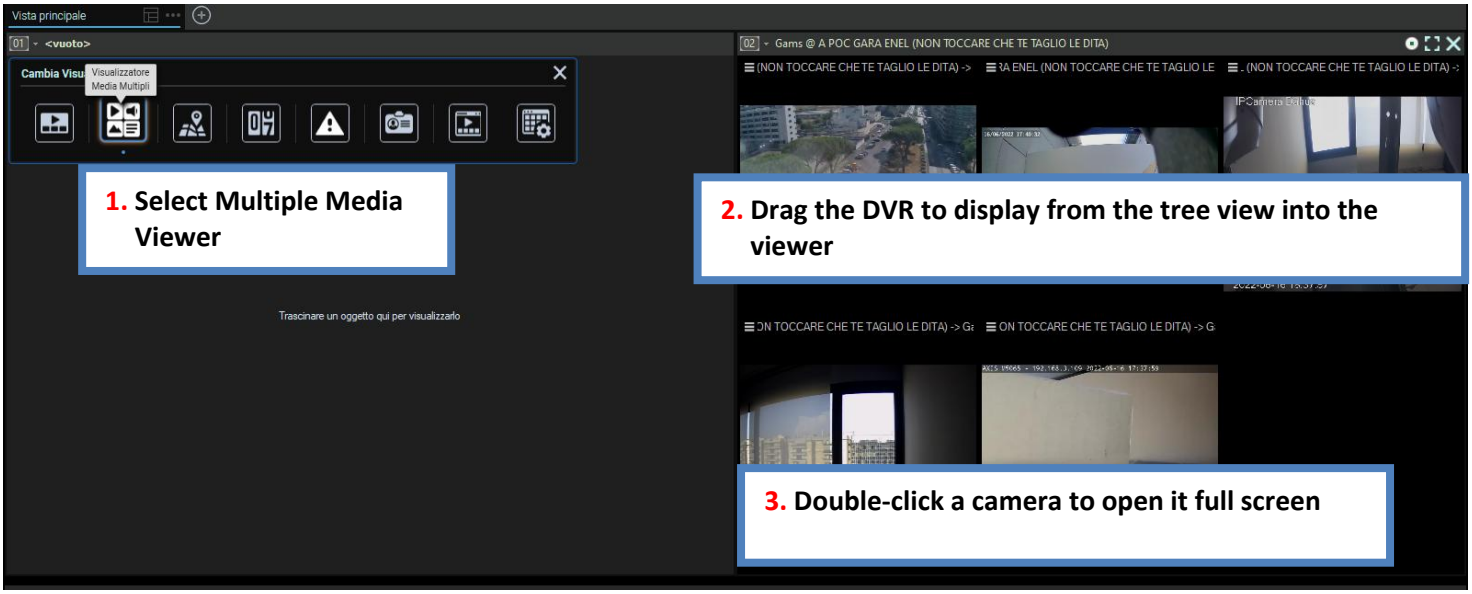
VIEWING AND CONTROL

The viewing and control area allows full monitoring of data. By default, the area has four viewers. The image shows the actions available to the user.



MULTIPLE MEDIA VIEWER

The image shows how to display up to twenty DVR channels in the same viewer.

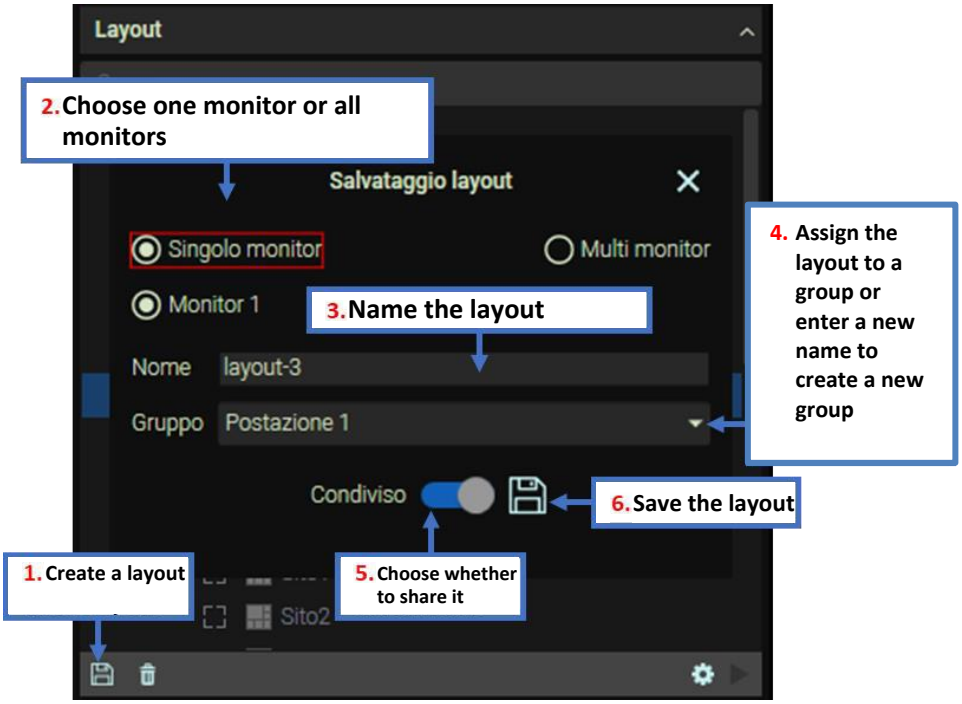


CONFIGURED LAYOUTS

Elkron-ONE allows viewing layouts to be configured, saved and quickly recalled when required. Users can choose the number and type of viewers and the data to display in them.

Creating a new layout

To create a new layout, first set up the work area with the required viewers. Then follow the steps in the image below to save it.

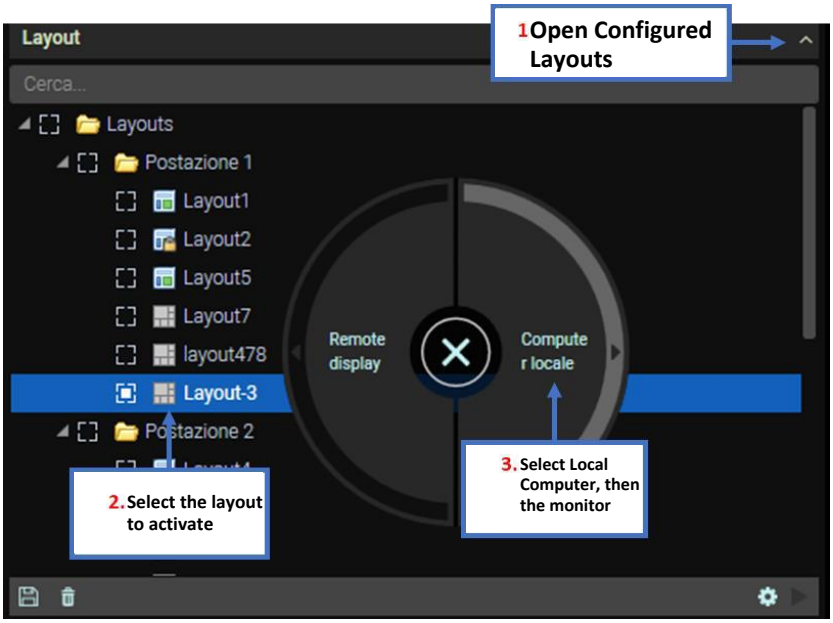


Shared layouts can be recalled by all users. Non-shared layouts can be recalled only by the user who created them.

Saving a layout with an existing name overwrites the previously configured layout.

Activating a layout

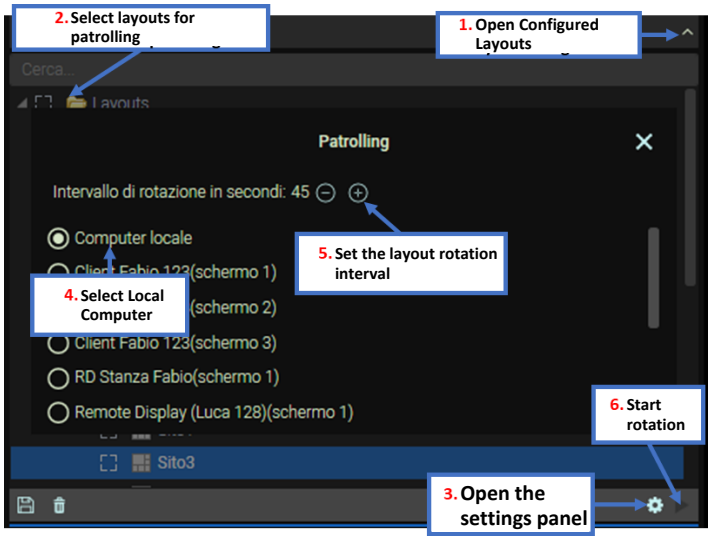
When using a single monitor, simply double-click the layout:

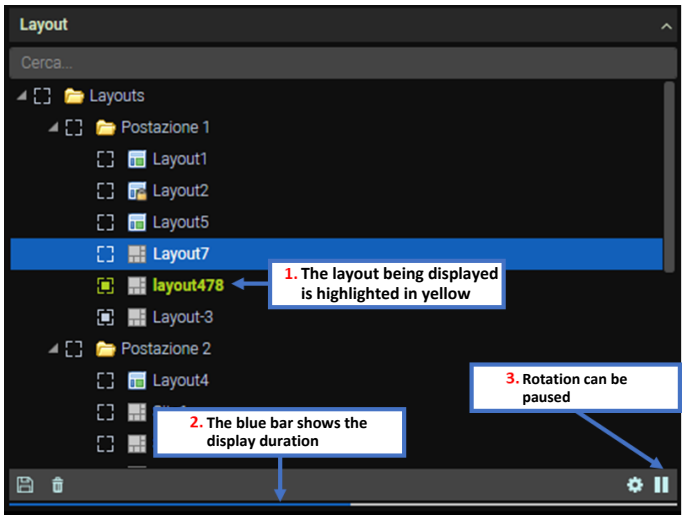


The icons in the table identify the layout type.

	Layout configured for a single monitor
	Layout configured for multiple monitors
	Non-shared layout

Activating a layout sequence

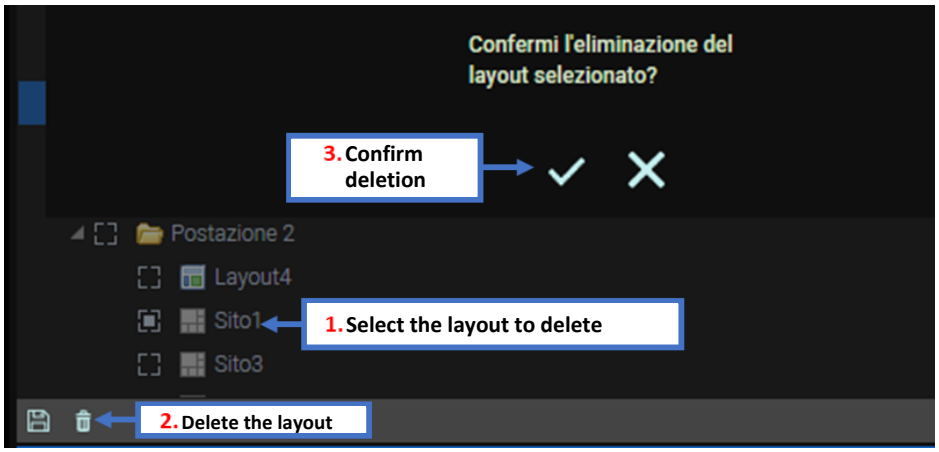




The images show how to activate layout patrolling to display multiple layouts in sequence, switching after a preset interval.

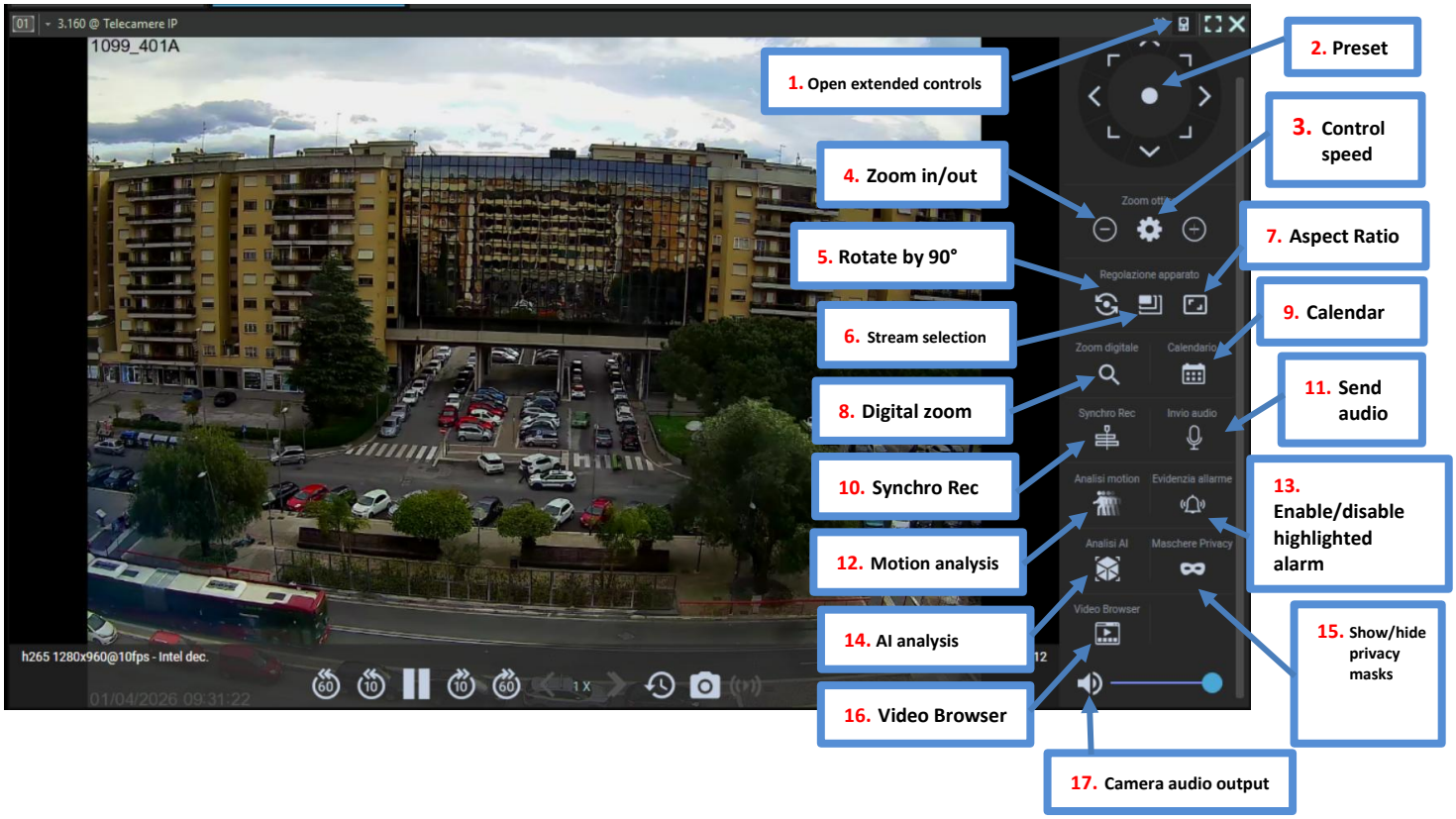
Deleting a layout

Users can delete only layouts they created. Administrators can also delete layouts created by other users, provided they are shared:



VIEWING LIVE VIDEO

Video surveillance devices, including IP cameras/encoders and DVRs/NVRs, are integrated into the Elkron-ONE platform for full operation and remote control through device and multimedia stream management. Drag a device from the tree view into a viewer and use the commands shown in the image to manage the video stream.



1. PTZ SPEED: adjusts the pan, tilt and zoom movement speed.

2. ZOOM: zooms in and out on the scene.

3. ROTATION: rotates the displayed video by 90°.

4. STREAM SELECTION: three live stream viewing options are available:

- **Automatic:** when this option is enabled, the stream configured on the device is displayed.
- **Main Stream:** displays the primary stream, overriding the device configuration. Disable **Automatic** to select the main stream.
- **Sub Stream:** displays the secondary stream, overriding the device configuration.
- **Sub Stream 2:** displays the tertiary stream, overriding the device configuration. Disable **Automatic** to select sub stream 2.

Note: Stream types are defined in the Camera Configuration area.

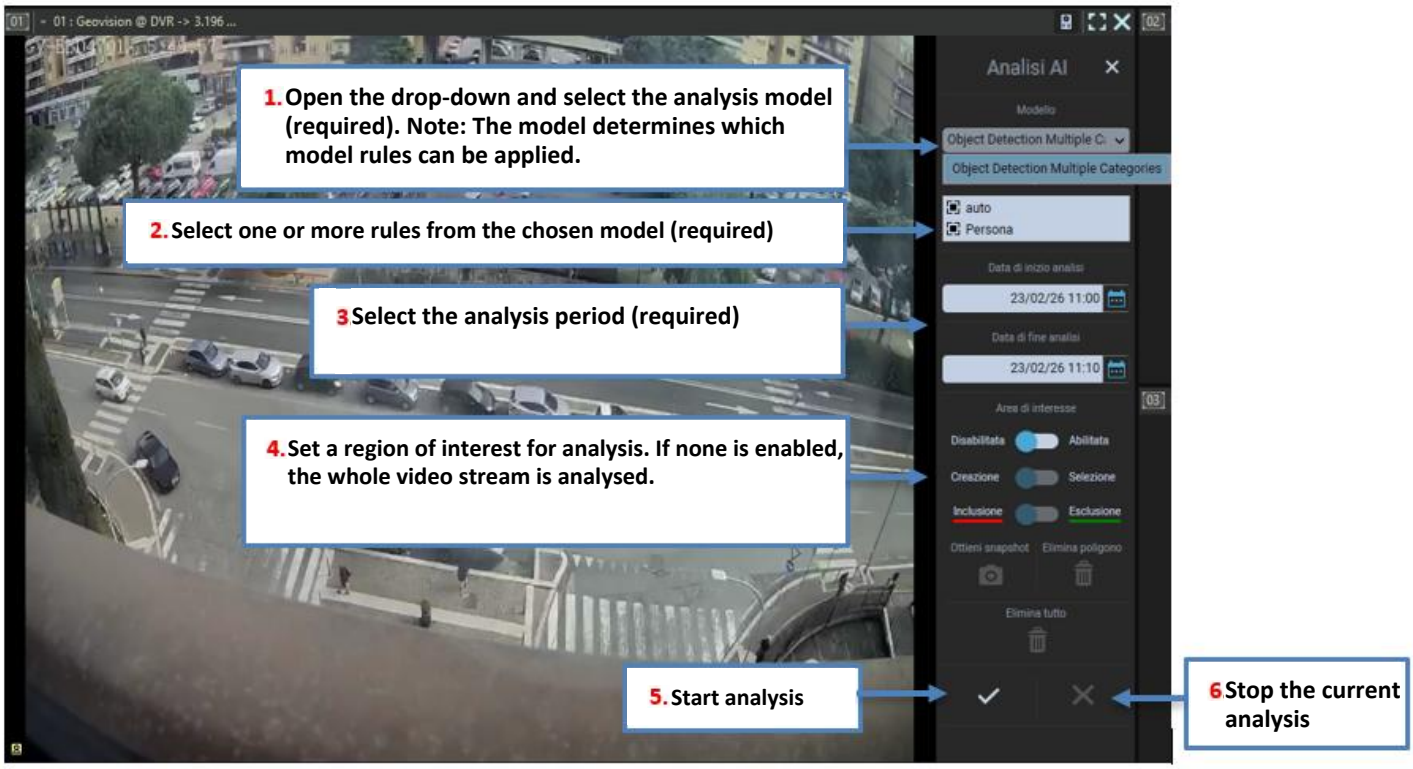
Basic Configuration tab.

5. **ASPECT RATIO:** four aspect ratio options are available:
   - **Original:** displays the video using the aspect ratio configured on the device.
   - **Extended:** forces the video to fill the entire viewer, overriding the device configuration.
   - **16/9:** displays the video with a 16/9 aspect ratio, overriding the device configuration.
   - **4/3:** displays the video with a 4/3 aspect ratio, overriding the device configuration.
6. **DIGITAL ZOOM:** adjusts digital zoom using the mouse wheel.
7. **CALENDAR:** selects the date and time to search in recordings.
8. **SYNCHRO REC:** navigates recordings from all selected cameras simultaneously.
9. **SEND AUDIO:** if supported by the device, audio received from the camera can be enabled for live or recorded video. If supported, audio can also be sent to the camera using the *Send Audio* button (see Operational Control).
10. **MOTION ANALYSIS:** identifies motion events in the scene captured during video recording.
11. **HIGHLIGHTED ALARM:** enables or disables highlighted alarm mode.
12. **AI ANALYSIS:** configures and starts advanced AI analysis of recordings. For details, see the following *"AI analysis"* section.
13. **PRIVACY MASK:** shows or hides privacy masks created in Elkron-ONE (see the Privacy masks section) on the camera's video stream.
14. **VIDEO BROWSER:** opens the camera directly in Video Browser search mode.
15. **AUDIO:** if the recording contains an audio stream, the volume control is also available.

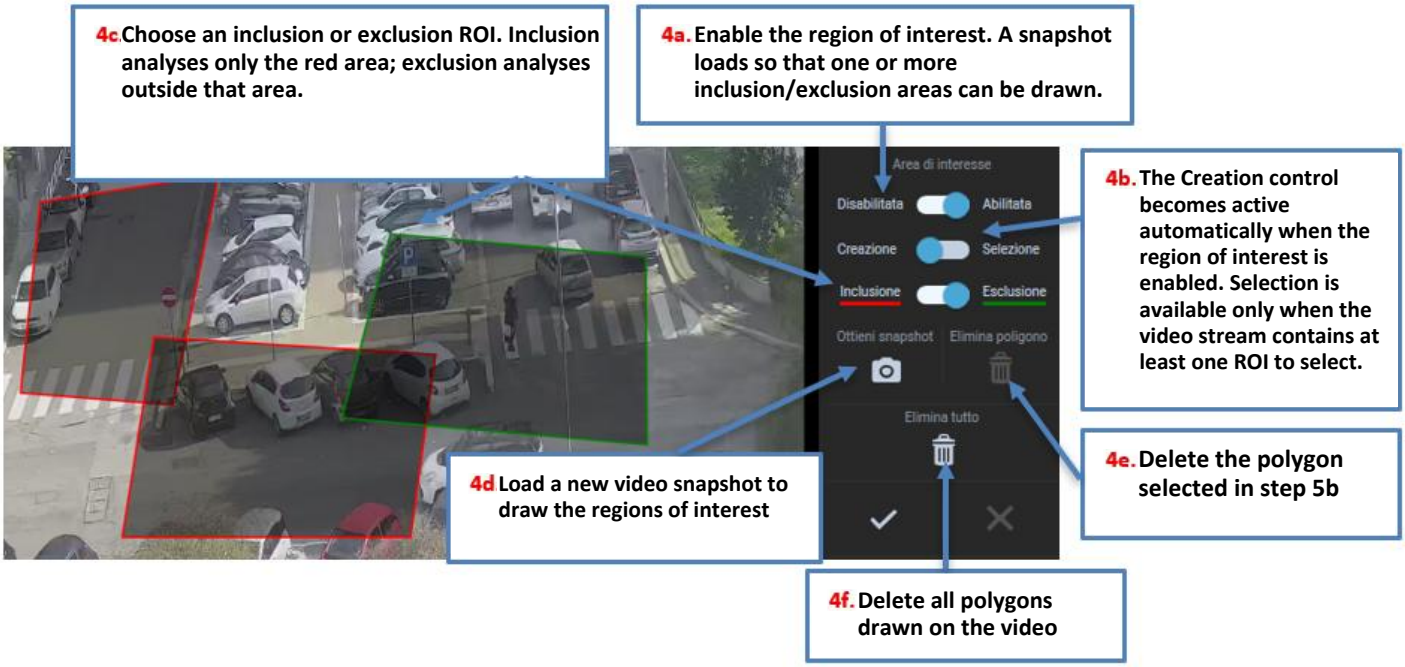
AI analysis

While viewing a video stream in Elkron-ONE, the operator may want to locate specific events quickly, such as people, vehicles or both passing through the scene. To do this, select *"Analisi AI"* (AI Analysis) in the extended controls. This analyses recordings around the event of interest using the Magic Box device integrated into Elkron-ONE. This function detects more sophisticated events than the existing Elkron-ONE analysis tools, such as motion analysis, providing the operator with more detailed, higher-quality results. Analysis covers the entire scene or one or more regions of interest (ROIs) drawn by the operator.

Follow these steps to start the analysis:

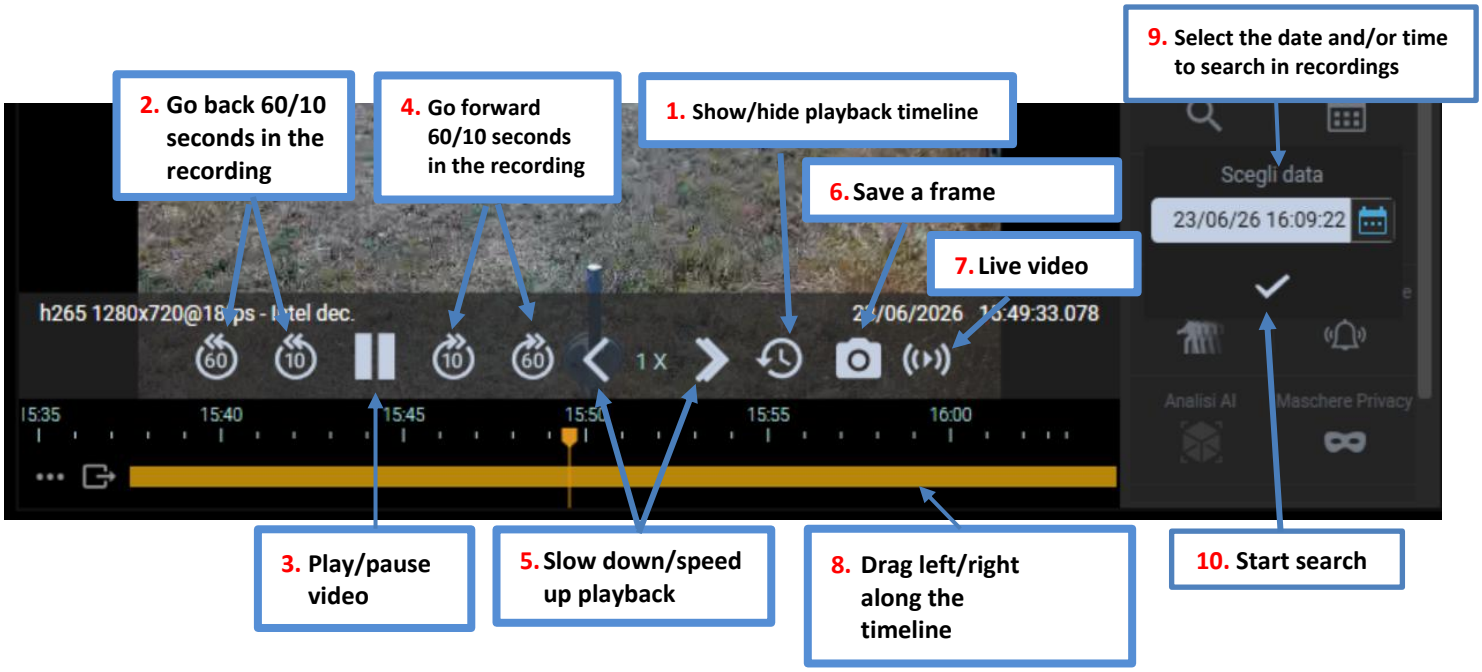


Configuring regions of interest (ROIs)



Note: The analysis models to be selected must already be loaded on the Magic Box.

VIEWING RECORDED VIDEO

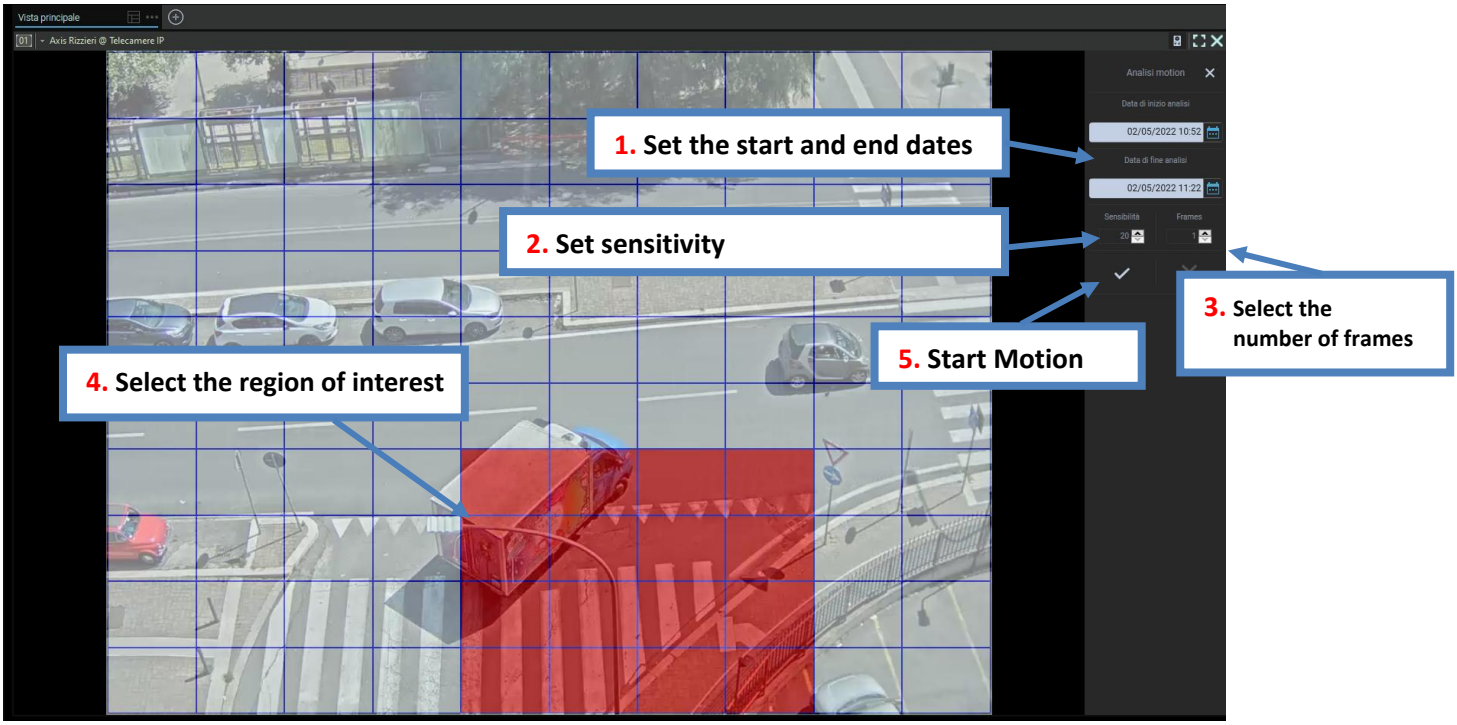


6. **SAVE A FRAME:** exports a snapshot of the displayed video to the local computer. A system notification informs the user of the path where the image was saved.

7. **VIEW RECORDINGS:** plays recordings from a past date set by the user, or allows direct navigation using the playback timeline (no. 8). Playing recordings enables the additional controls shown in the image.

MOTION DETECTION

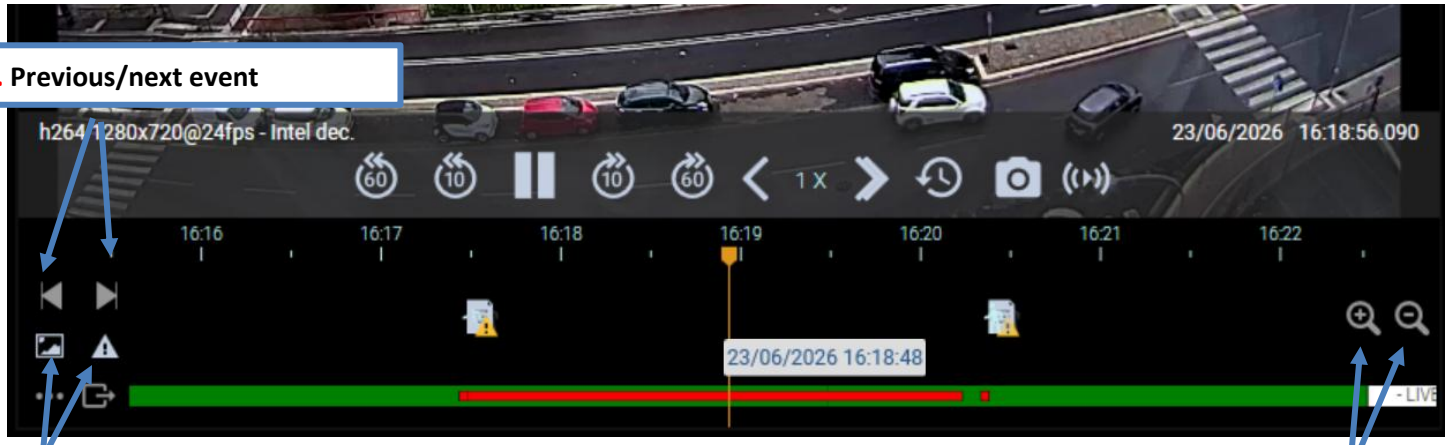
Motion Detection continuously monitors the entire scene or selected areas to identify motion events captured during video recording. Movement is detected by comparing video frames over time and/or against a reference background image:



2. **Sensitivity:** determines how significant a change must be to trigger a motion event. Select a value between 20 and 99.
    - The higher the sensitivity, the better the motion detector can recognise small objects. Motion alarms will then be triggered by the slightest movement.
    - The lower the sensitivity, the more significant the movement must be to generate a motion event.

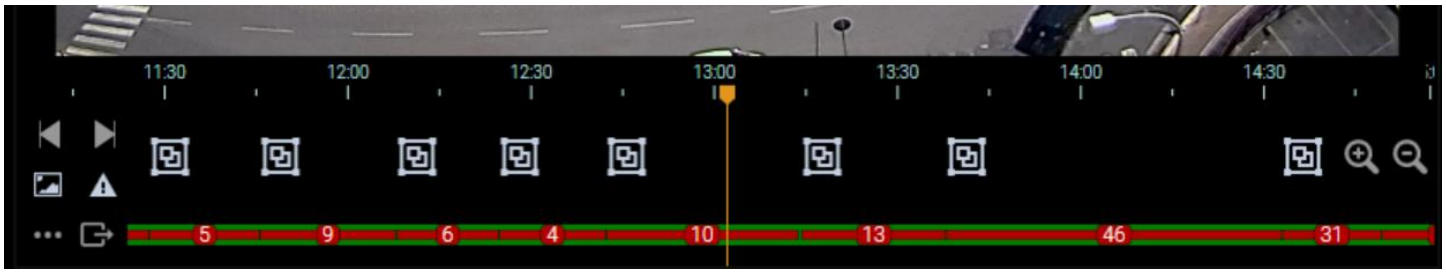
3. **Frames:** the number of consecutive frames showing a significant scene change that triggers an event. Select a value between 1 and 10.
    a. Setting the value to 1 reports any movement. b. Values greater than 1 are more suitable for avoiding false positives.

4. **Start Motion:** analyses movement while also searching for multimedia files. The process can be stopped at any time using the red x.
    When analysis is complete, detected motion events are highlighted in red on the timeline. The image shows how to use the controls to view events in the recordings.



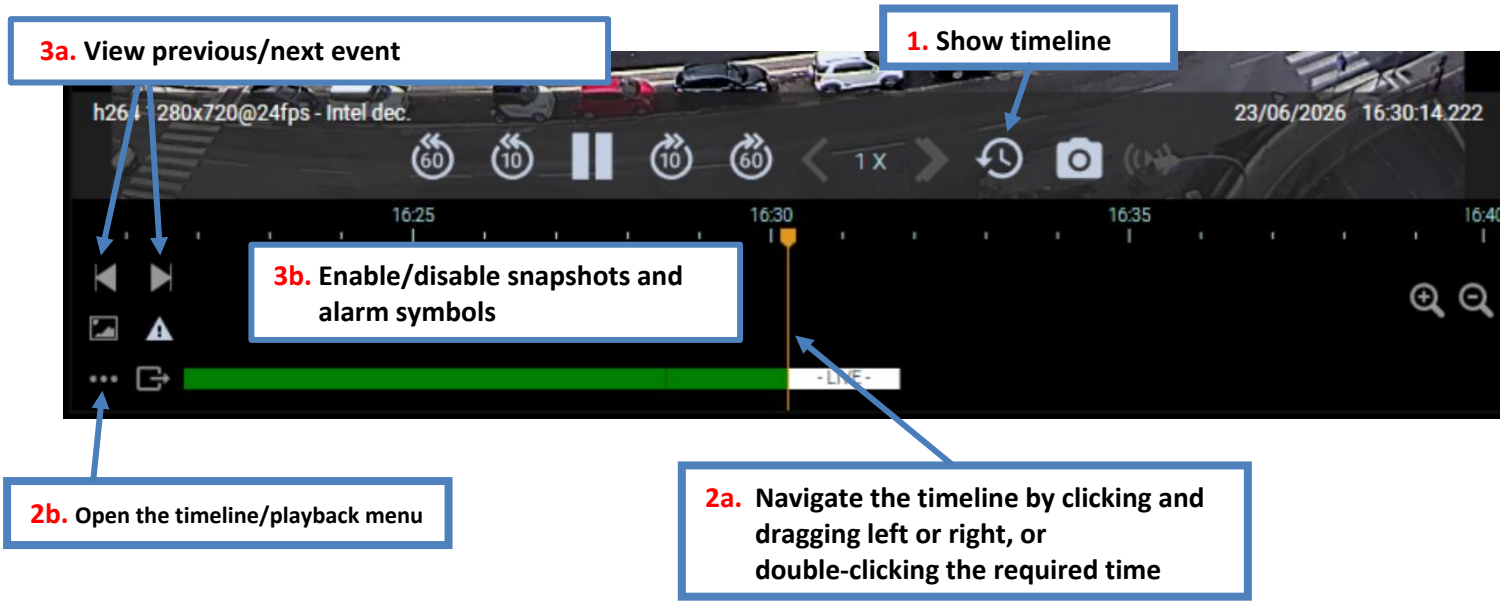
The timeline lets you navigate through the recording to view different recorded motion events or return to live video.

Zooming out on the playback timeline groups events together instead of displaying them individually, as shown above. Each group is identified by the number of alarms it contains and highlighted by the icon .



PLAYBACK TIMELINE

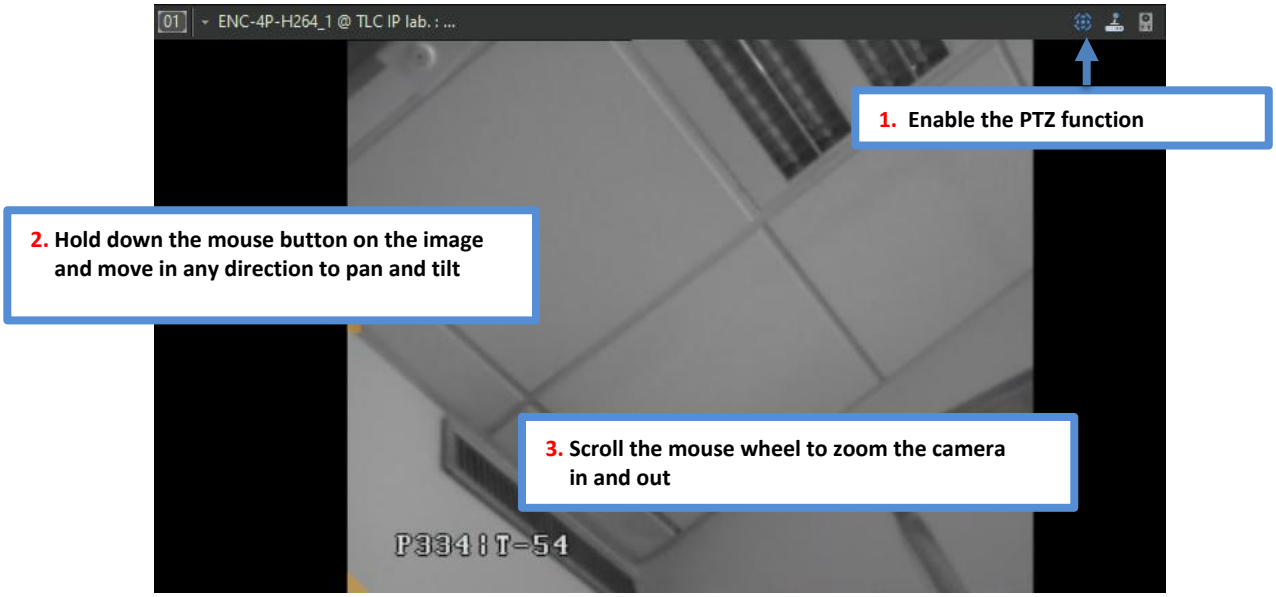
The image shows how to use the playback timeline to view live and recorded camera video:



CONTINUOUS PTZ AND JOYSTICK

Continuous PTZ

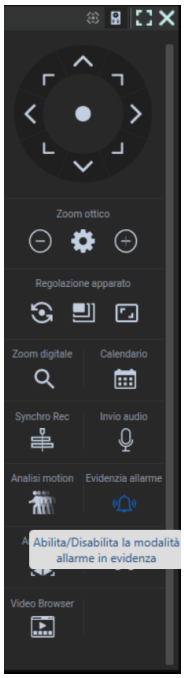
Continuous PTZ allows IP cameras to be panned and tilted through 360° directly from the viewer using only the mouse. When enabled, its icon is highlighted in blue .



To exit Continuous PTZ mode, click its icon again.

AUDIBLE ALARM

The image shows how to enable an audible alert when an alarm is detected on the device being viewed. This function is disabled by default:



CAMERA SYNCHRONISATION

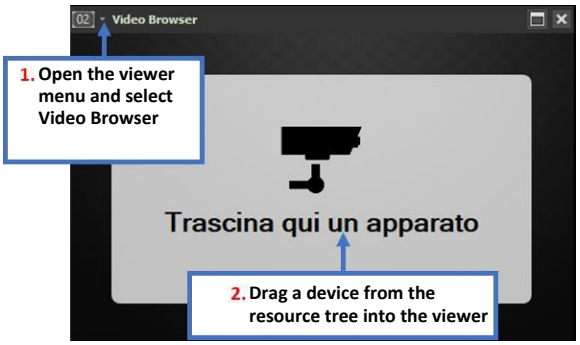
Elkron-ONE can synchronise playback from several cameras simultaneously, whether they belong to a DVR or are IP cameras. This allows an event to be analysed by viewing the scene captured by multiple cameras at the same time.

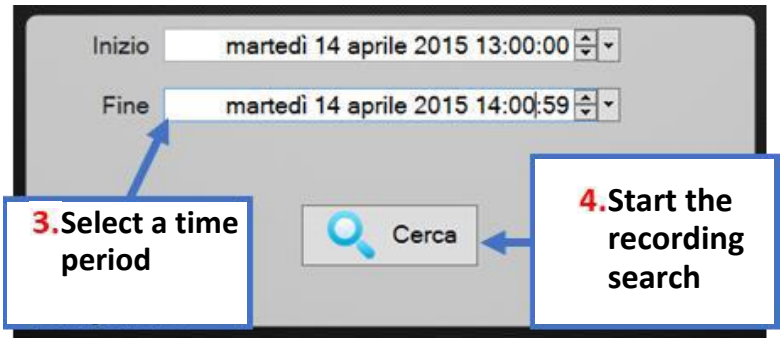


The operator can drag the timeline with the mouse to focus on a specific moment in the synchronised cameras' recordings. Motion events are shown in red.

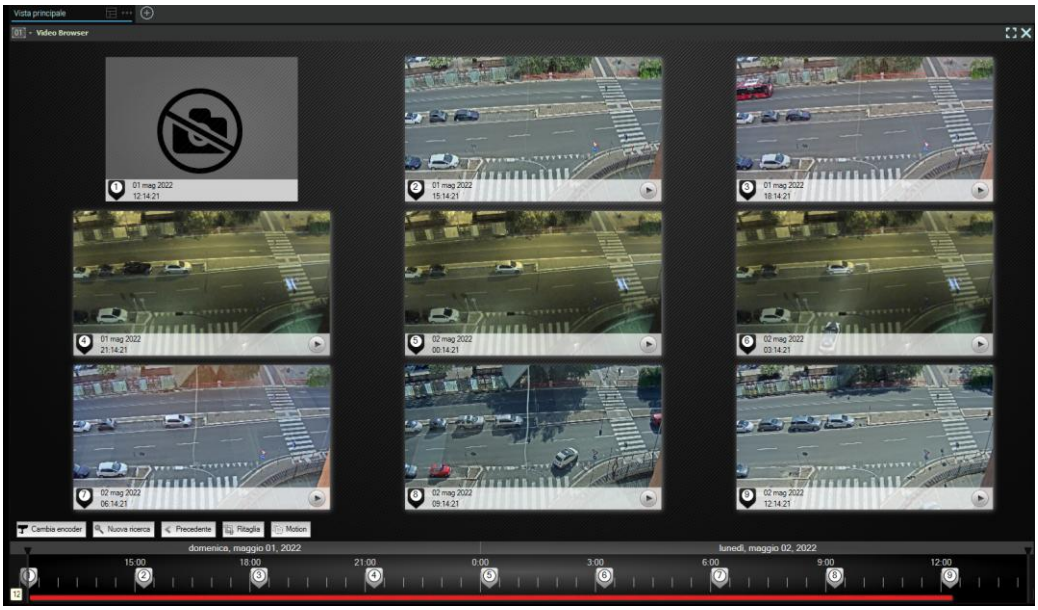
VIDEO BROWSER

Video Browser lets you focus on specific sections of camera footage, examining and comparing individual frames captured at successive moments within a user-defined period. The following images show how to select footage for analysis.





The selected period is divided into eight equal time segments. The nine frames at their boundaries are displayed and numbered chronologically.



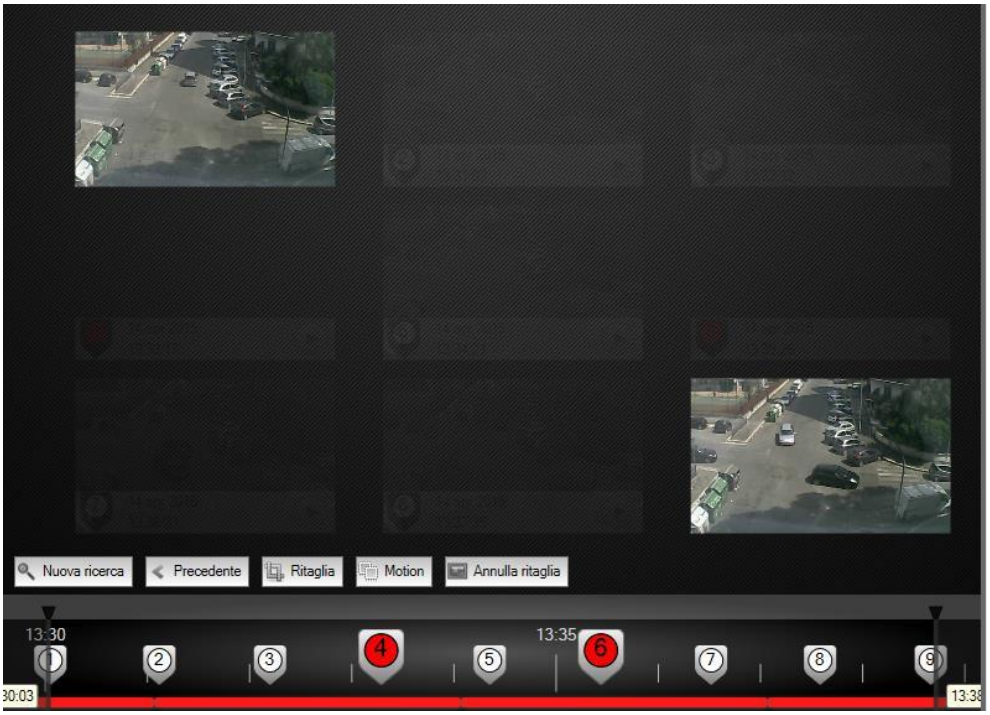
The image shows the video stream availability notifications.



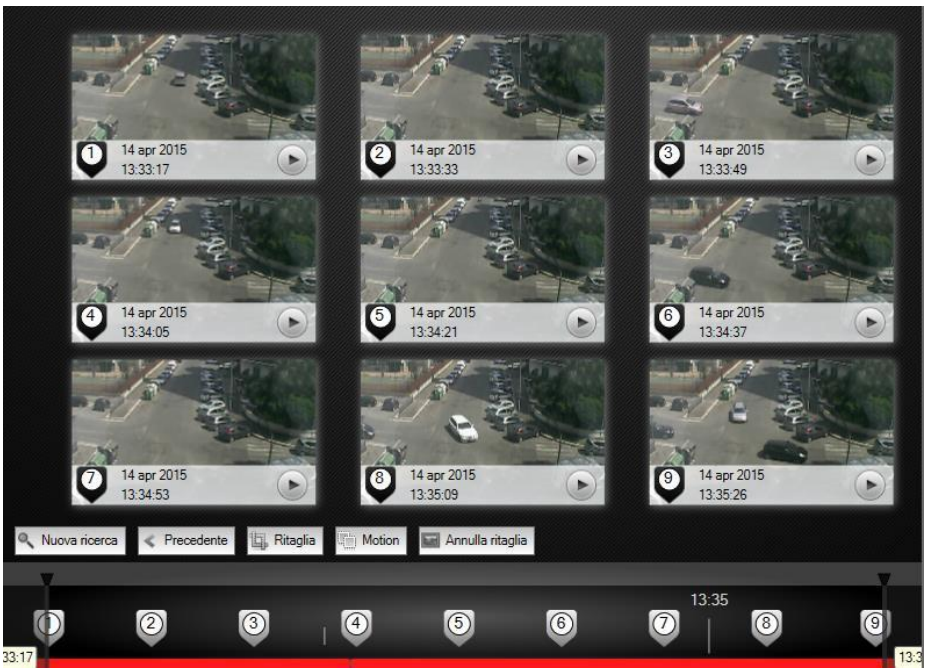
The **Play** button on each frame starts previewing the recording from that frame onwards. The selected frame is also marked in yellow on the timeline.



The selected time interval can be subdivided further to locate the event of interest more precisely, down to a minimum of one second per frame. Select two of the nine available frames to mark the start and end of the recording section to subdivide. Click the two frames to select them; they are highlighted in red. The same operation can be performed on the timeline.



In the example, the focus is on two minutes of recording, from 13:33:17 to 13:35:26.



The following operations are available:

- **Change encoder:** switches to another device for analysis.
- **New search:** starts a new search by dragging a device from the tree view.
- **Previous:** retrieves and displays the previous time interval.
- **Cancel request:** stops the current search, for example if it is taking too long.

- **Crop:** enables digital zoom to select a specific video area. Drag from any of the four corners to select the area, then confirm with OK or cancel to abandon zooming. Once set, the zoom applies to all frames.



With zoom enabled, all frames show only the selected detail throughout the sequence.

- **Cancel crop:** disables zoom.
- **Motion:** compares frames and highlights in green the areas where a change or movement was recorded.

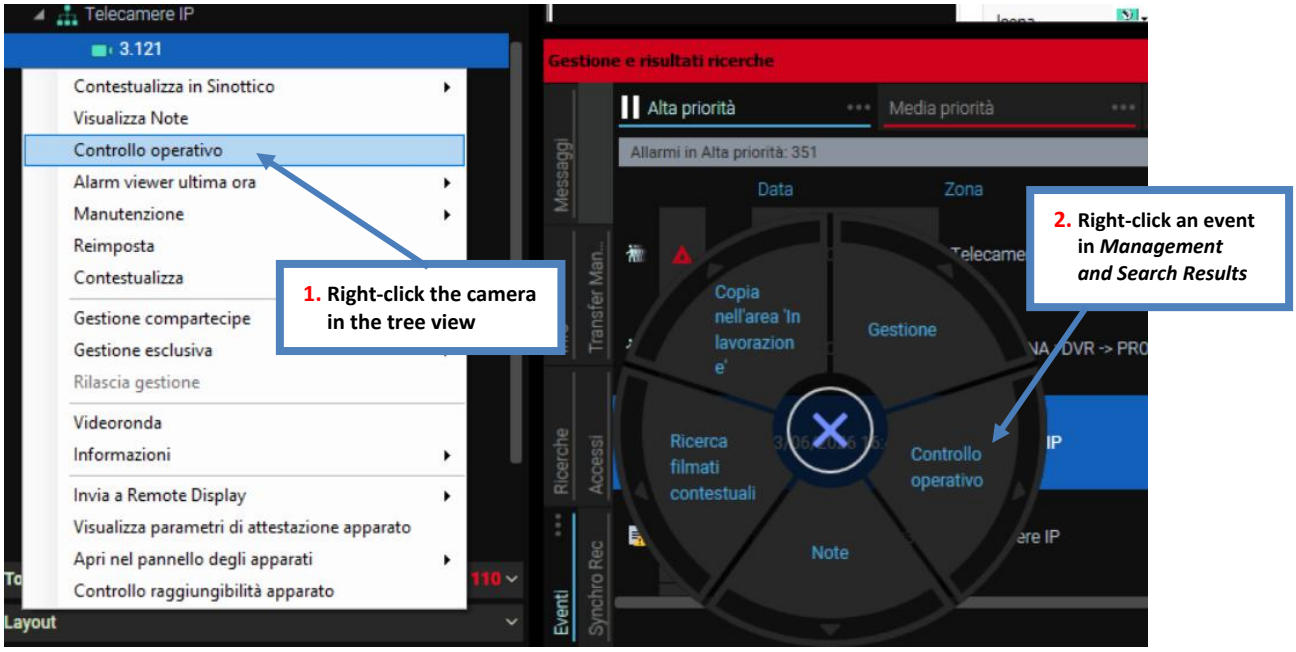


- **Download recording:** saves the selected recording locally so that it can be analysed in detail at any time.
- **Quick recording export:** quickly exports footage in MKV or MP4 format, with or without privacy masks. The *Export Video* button opens the dedicated section, as shown below.



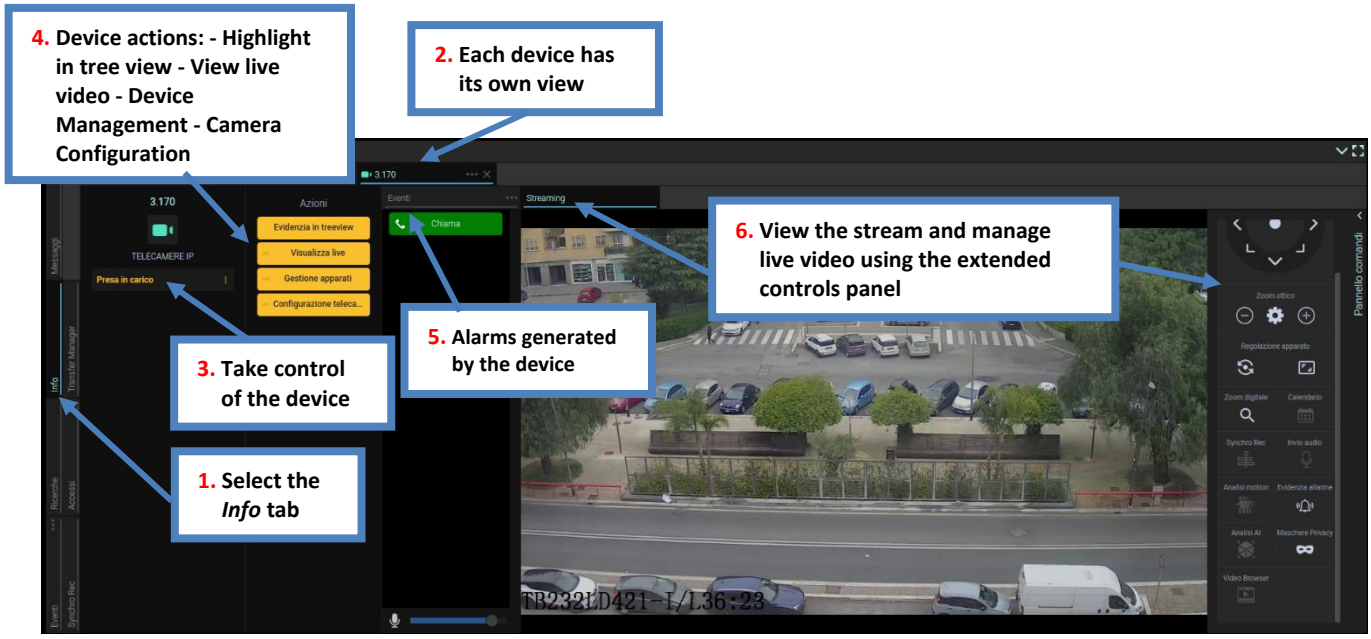
OPERATIONAL CONTROL

Elkron-ONE includes a module for operational control of devices from a single area. This provides a focused overview and management of one or more devices and their alarms. The image shows how to activate Operational Control.



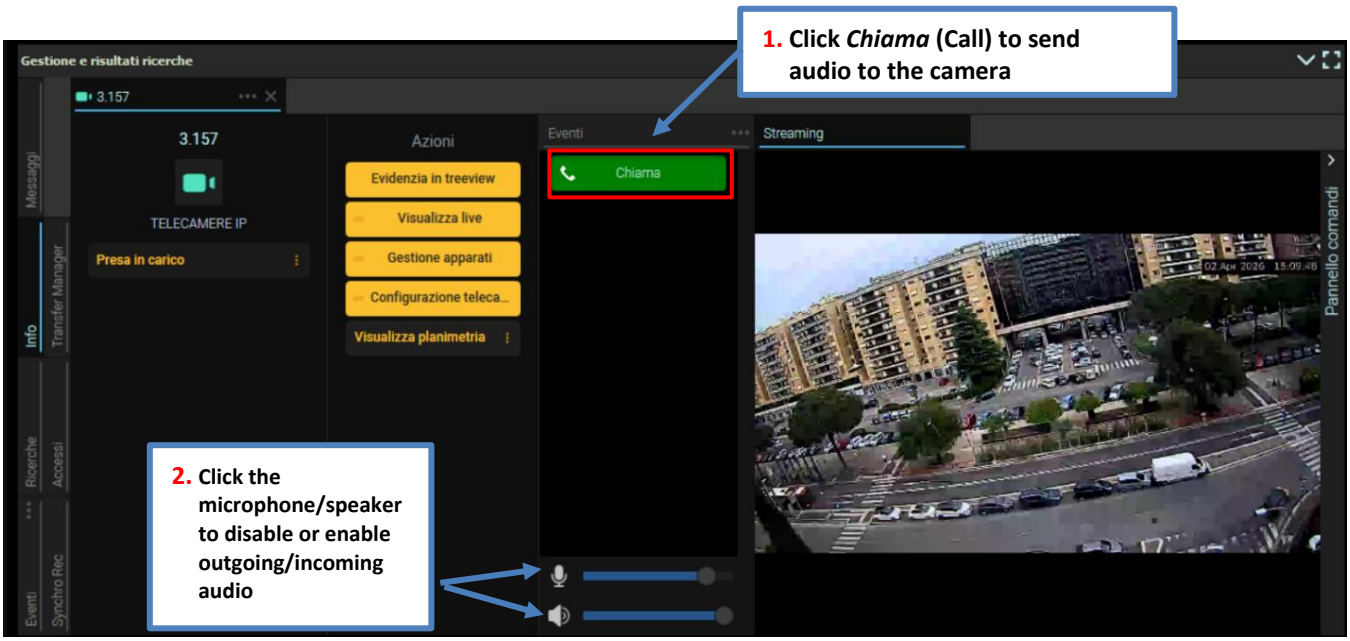
A tab opens automatically for each device. The available operations and information depend on the device type. The image shows operational control of a camera.

The operator can check the device status, take control of it, highlight it in the tree view, view live video, configure operating parameters, view and manage associated alarms and consult information attached to the device.

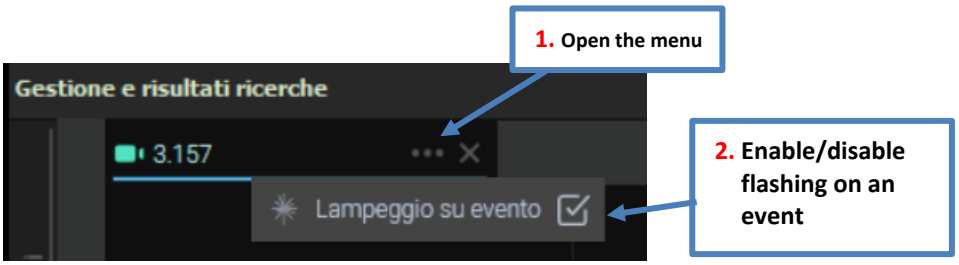


Operational Control also supports incoming and outgoing audio communication for ONVIF cameras that provide this function.

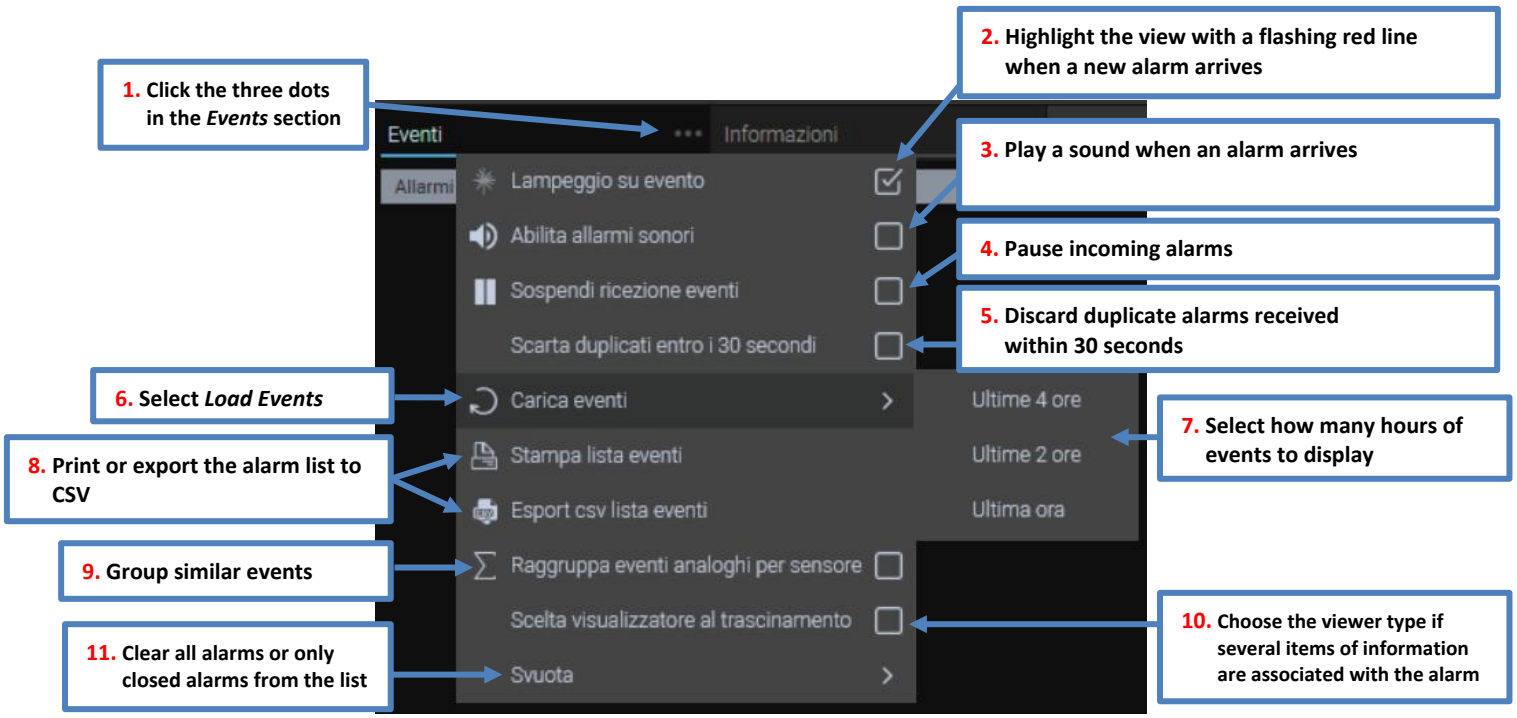
The following operations are available on the Streaming tab:



Finally, the event list is available in Operational Control. The foreground device tab is marked with a blue horizontal line. Alarm reception can be highlighted with a red horizontal line, as follows:



The image below shows the actions available on the event list.

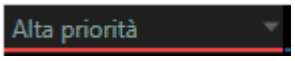


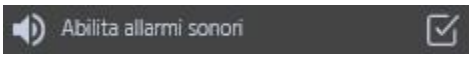
EVENT MANAGEMENT

Elkron-ONE generates an alarm whenever a device detects a critical event. Advanced alarm event management functions allow the operator to monitor device reports. Alarms include the acquisition date, the originating device, the report type and any additional information. Alarms are grouped into themed tabs, configurable in **Event View Configuration.**

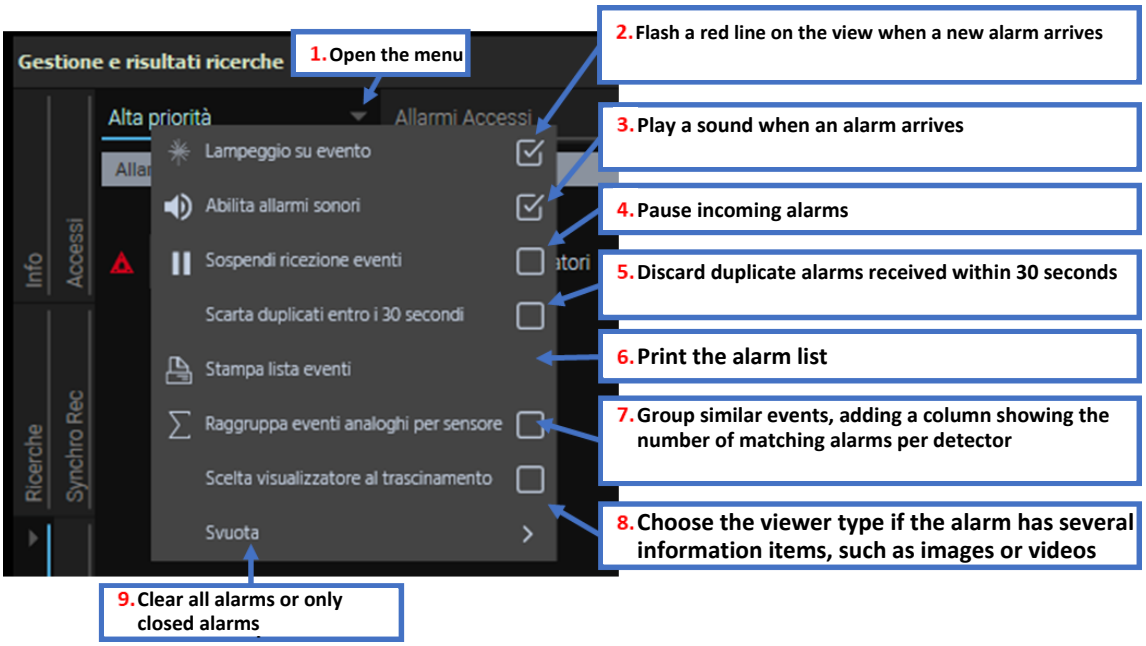


Several types of alert notify the user of new critical events to review:

- **Red line** on the tab 

- **Audible alert:** disabled by default. 

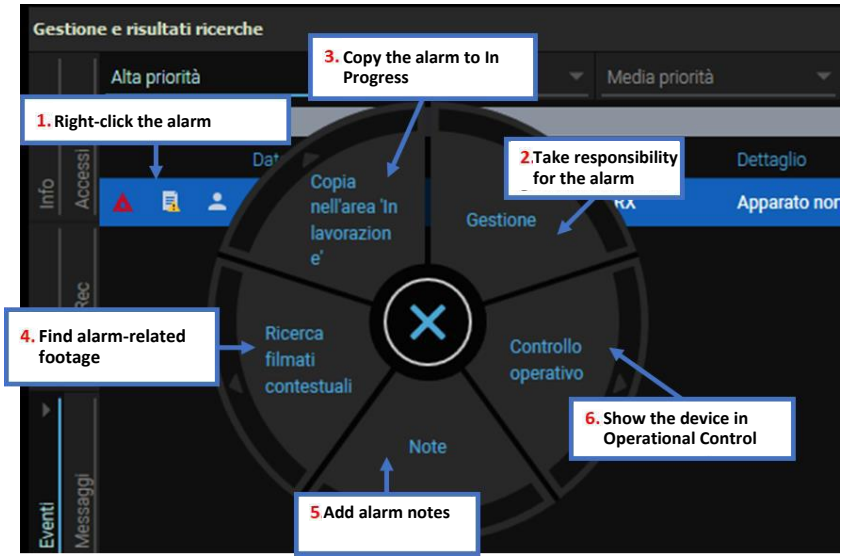
- **Flashing red bar.** If the *Management and Search Results* area has been minimised, the bar flashes red to indicate the presence of alarms.



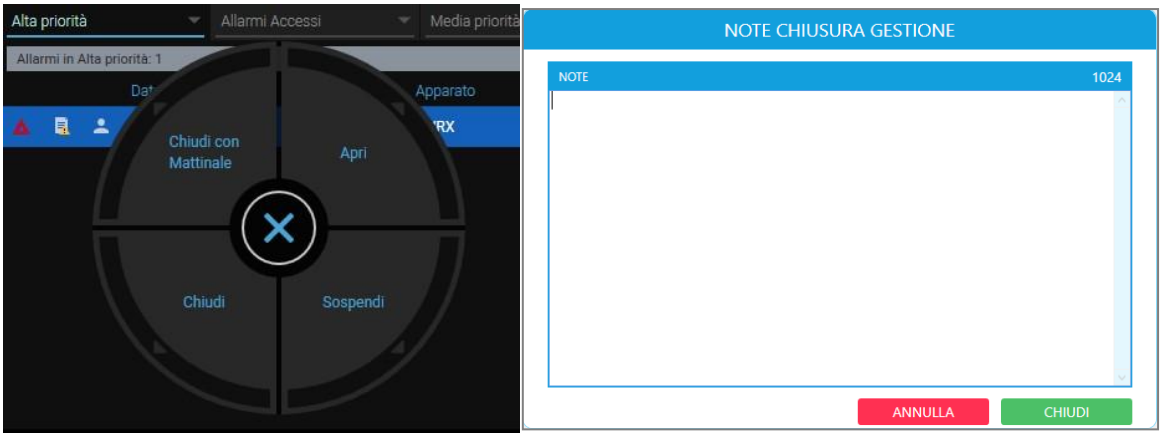
Note: If flashing is disabled for all tabs, the results management bar provides no visual notification of new events when minimised.

ACKNOWLEDGING AN ALARM

The image shows the operations available for an individual alarm.



2. Alarm management: the available actions are taking responsibility for the alarm, suspending it or closing its management. Closing alarm management requires notes to be entered.



The alarm queue shows each alarm's management status and the user who handled it:

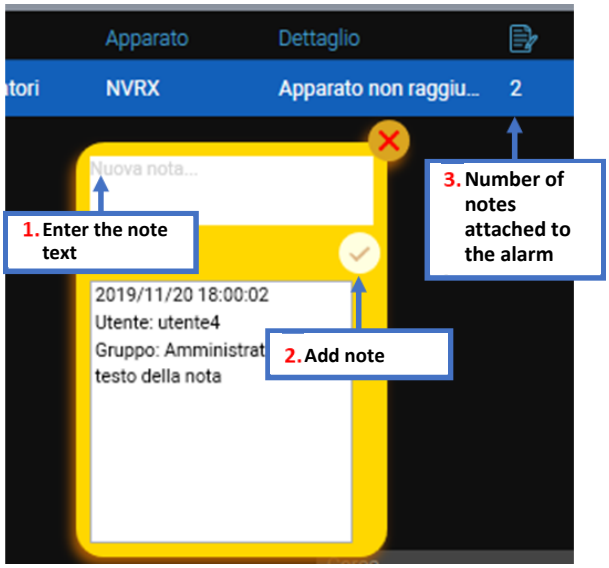


3. Copy to the In Progress area: manages the alarm independently of incoming real-time events. The image shows how to clear the In Progress area after handling the alarm.

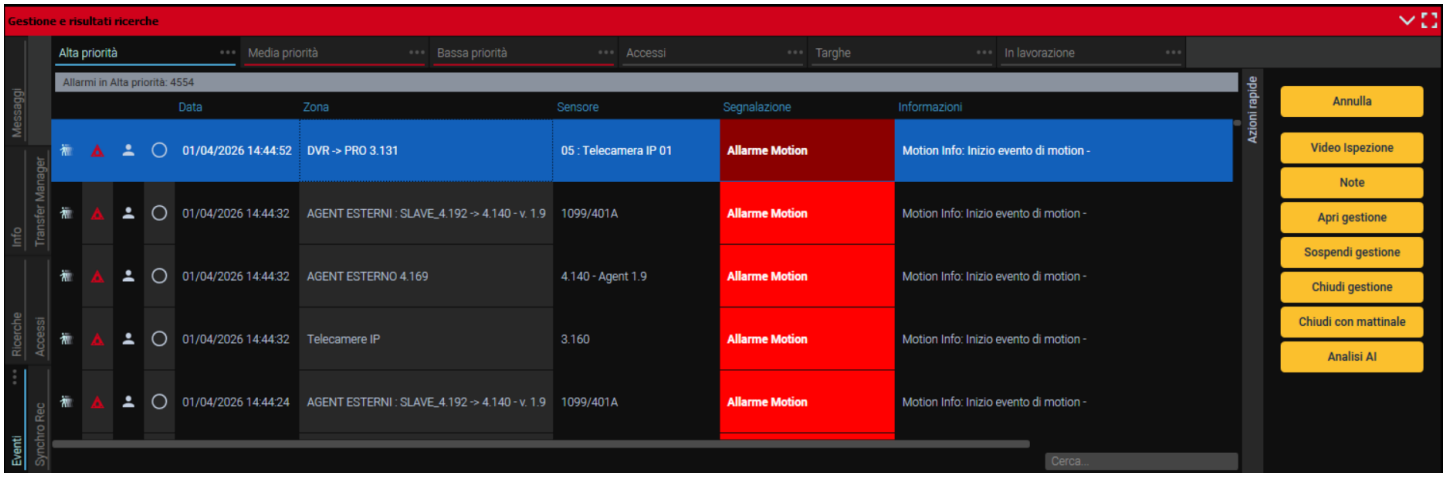


4. Search for alarm-related footage: retrieves all video recordings containing the alarm.

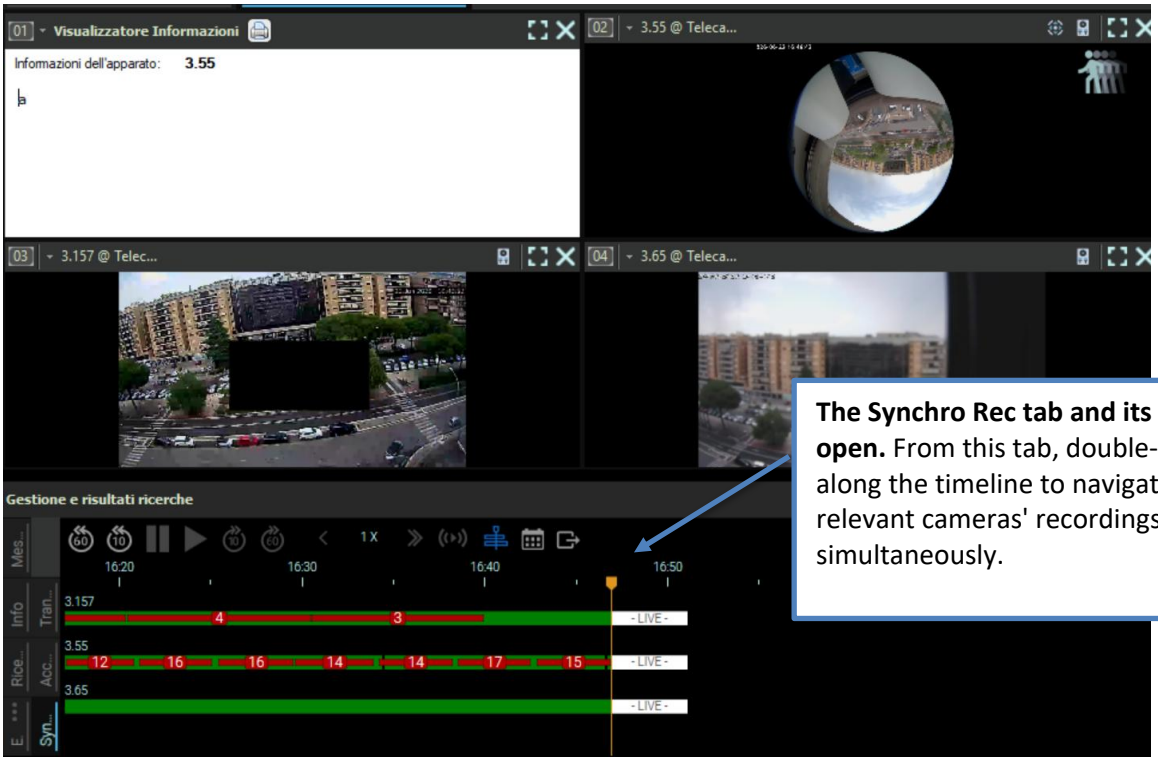
5. Notes: the image shows how to add notes to the alarm:



The same functions are available in a quick menu of yellow buttons on the right, which opens when an alarm is clicked:



The *quick actions* also include **Video Inspection,** which opens a layout in a new view containing video players showing recordings from the relevant cameras at the time of the event, the corresponding floor plan and any device information. The system also automatically opens the Synchro Rec tab and synchronises each camera's playback timeline near the event time, identified by a red tag (see the following image).



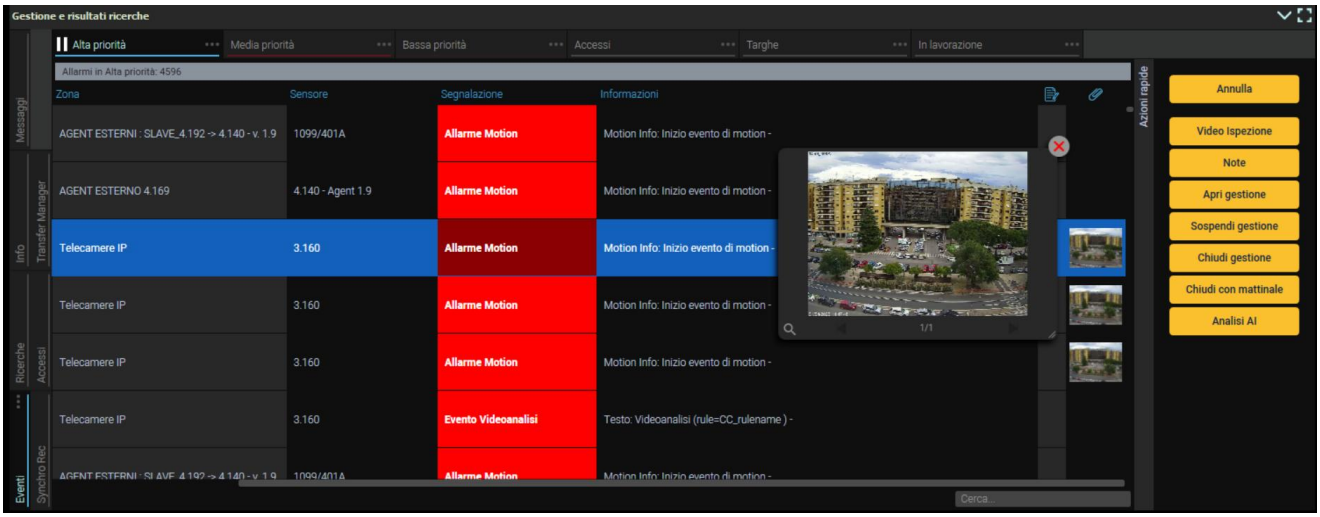
The Synchro Rec tab and its Event tag open. From this tab, double-click or pan along the timeline to navigate all relevant cameras' recordings simultaneously.

Users without general permission to access recordings can be granted limited use of this function by enabling the following permission in the Users section of the administration panel. They can then access recordings only for the 5 minutes before and after the event.

Note: The Video Inspection layout depends on the configuration and information available in Elkron-ONE. A floor plan is included if the camera generating the event is placed on an uploaded floor plan. Related cameras are included if their viewing cones contain the device that generated the event. Similarly, the Information Viewer is included only if the Information section in Device Management is populated for the device that generated the event.

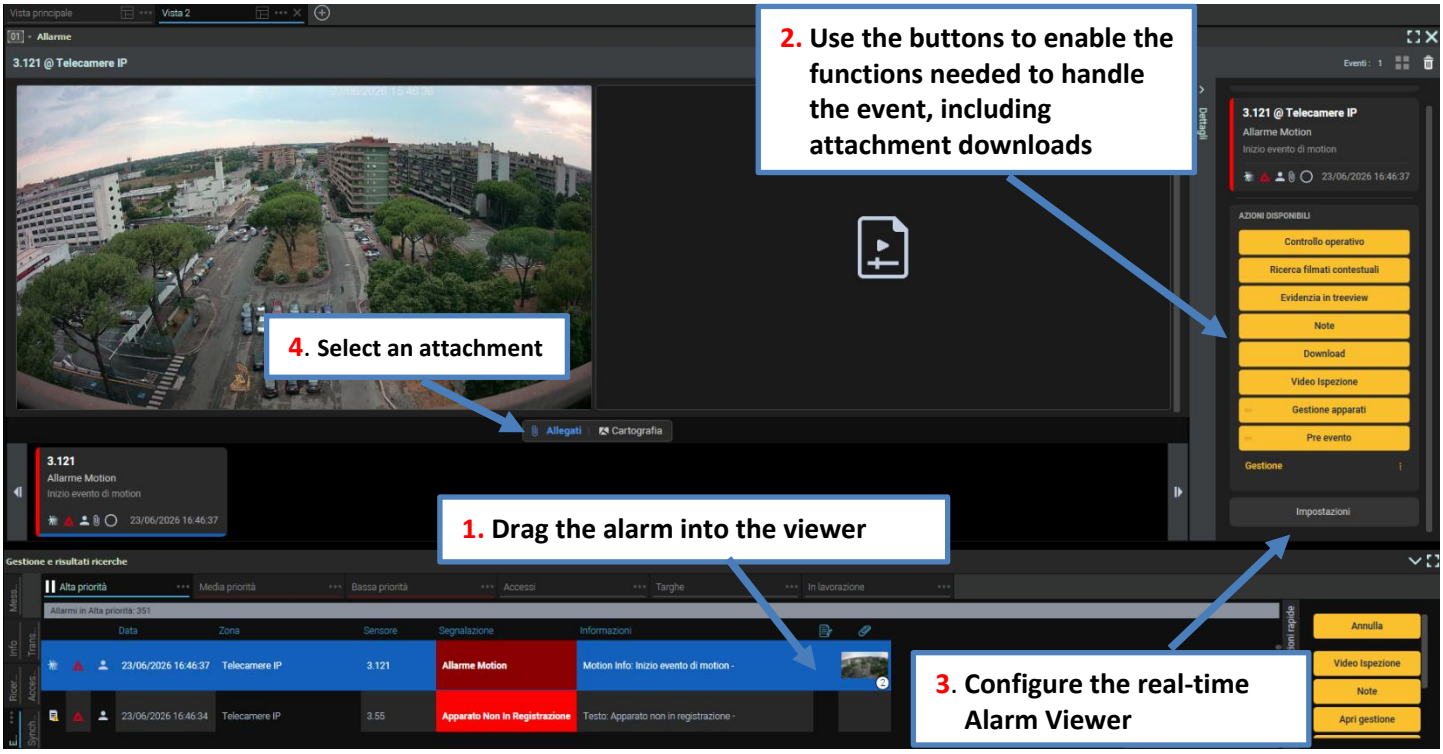
VIEWING ALARM ATTACHMENTS

Click an attachment image to open an enlarged preview. The preview can be resized and zoomed.



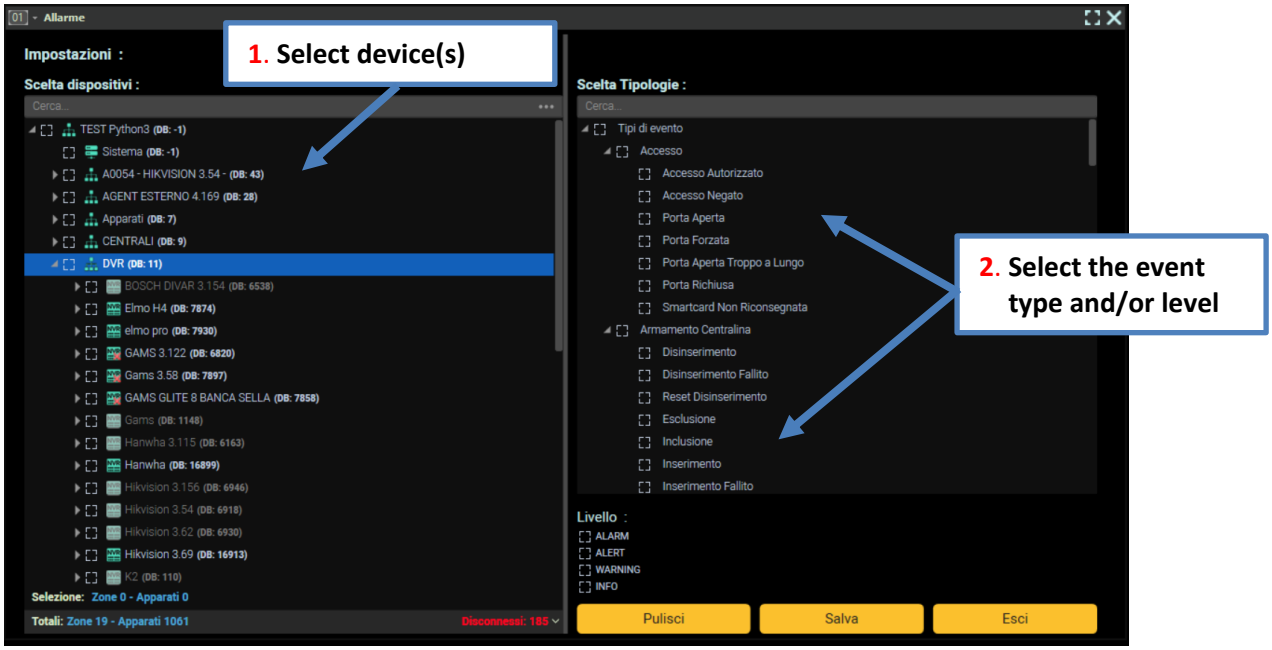
VIEWING ALARM DETAILS

To view alarm details, drag the alarm into a viewer from the alarm queue or alarm search results. The viewer displays the alarm type, the name of the device that generated it, the acquisition date and time and any associated images.

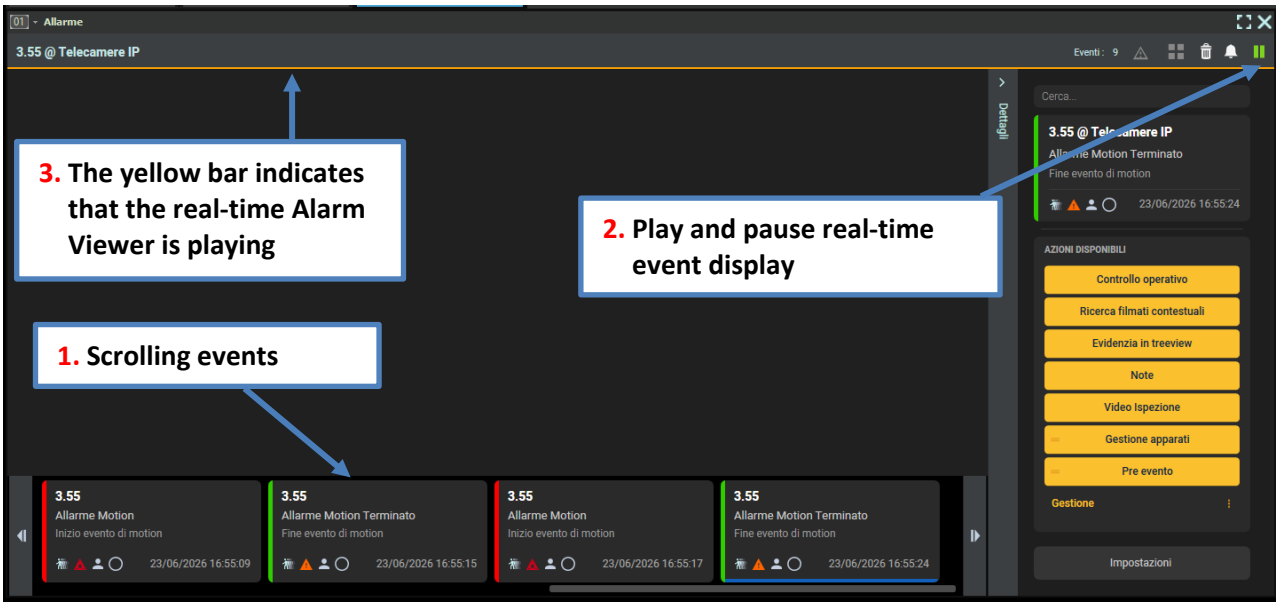


3. Real-time: the image shows how to configure real-time display of alarms acquired from one or more devices.



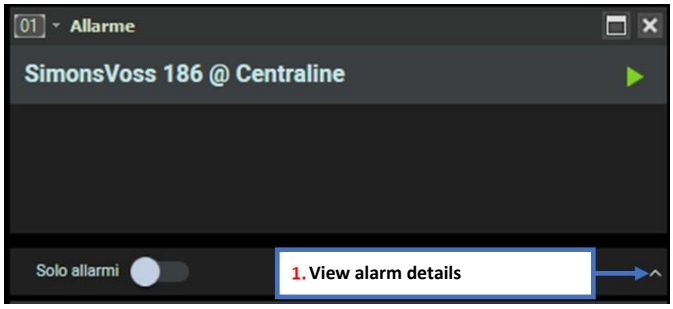


Incoming alarms scroll through the viewer, showing their management status, alarm type, originating device, date and time.

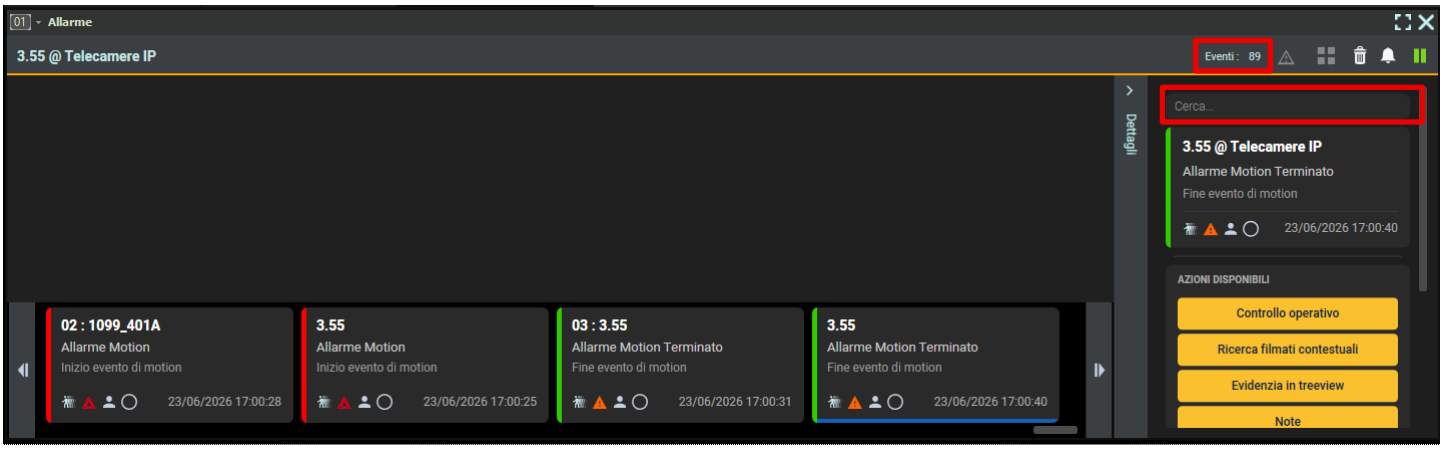


Note: Real-time mode can also be enabled by dragging an alarm tab into the viewer.

If the display area contains several viewers, click the button shown in the figure to view alarm details.



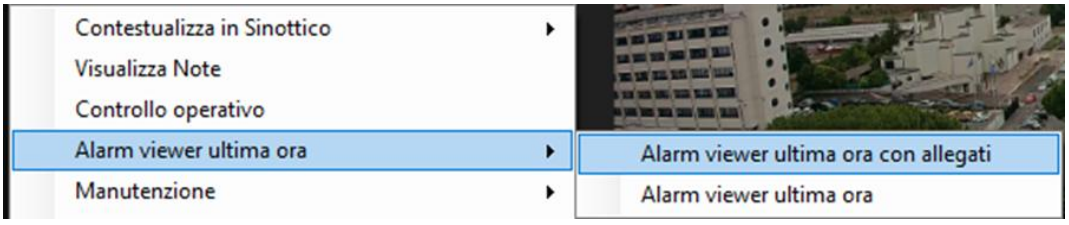
Searches can be performed directly in the alarm grid by filtering any field. The total number of events in the Alarm Viewer is also displayed. The event counter updates when the text search filter is applied.



Note: The Alarm Viewer automatically pauses whenever an event is selected for management.

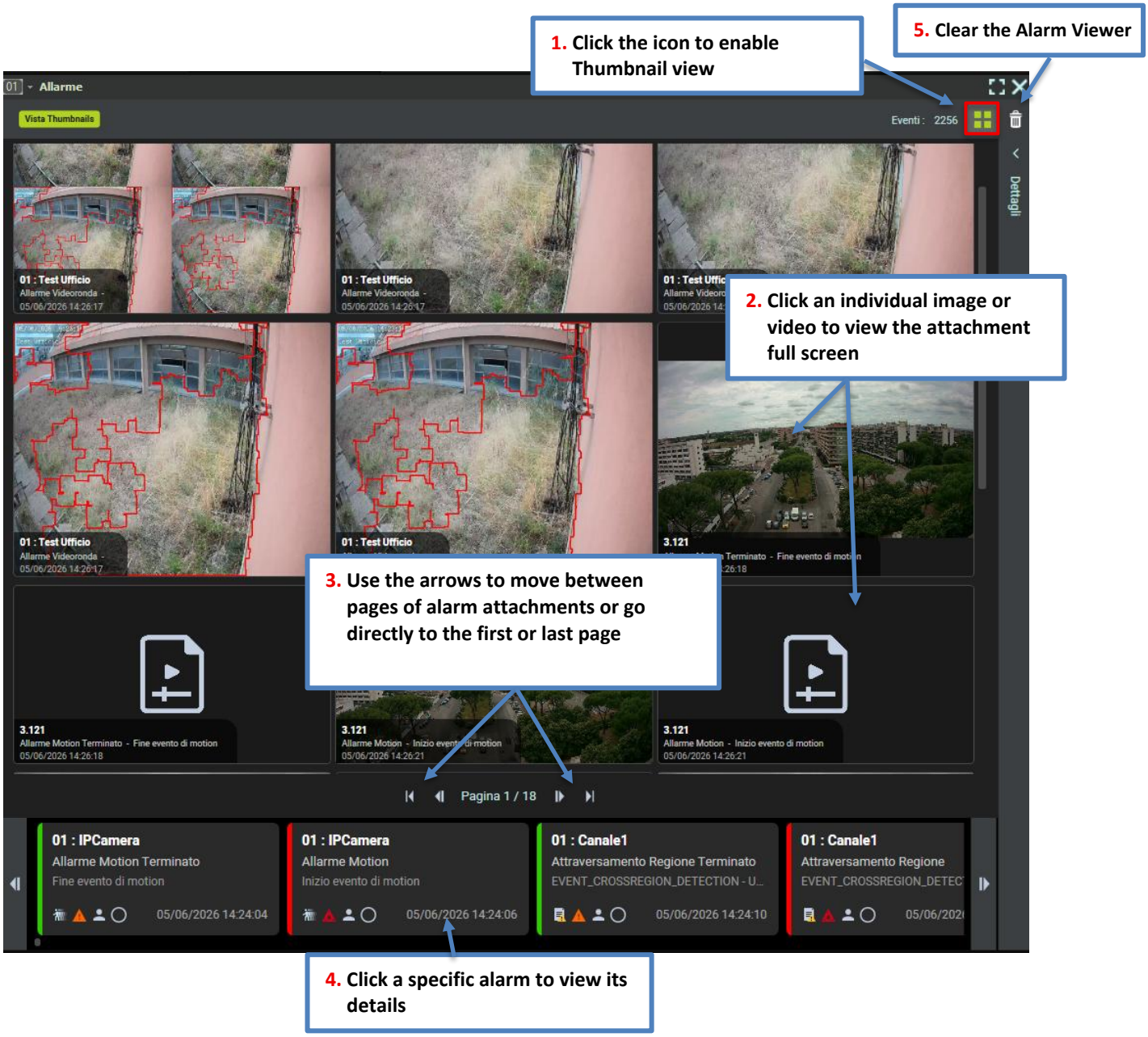
The Alarm Viewer can also be opened directly with the last hour's events already loaded, for faster management without configuring a dedicated viewer.

In addition to loading the previous 24 hours of events from Operational Control or the Event Grid, depending on the existing configuration, right-click a device in the tree view and select *"Alarm viewer ultima ora"* (Last Hour Alarm Viewer) to display events as shown above. To display only alarms with attachments, select *"Alarm viewer ultima ora con allegati"* (Last Hour Alarm Viewer with Attachments).



Thumbnail view

The Alarm Viewer can display several alarm attachments at once, helping users identify false alarms quickly without scrolling through images individually. Click the button in the top-right corner to enable Thumbnails mode.



CLOSE EVENT AND SEND TO DAILY REPORT

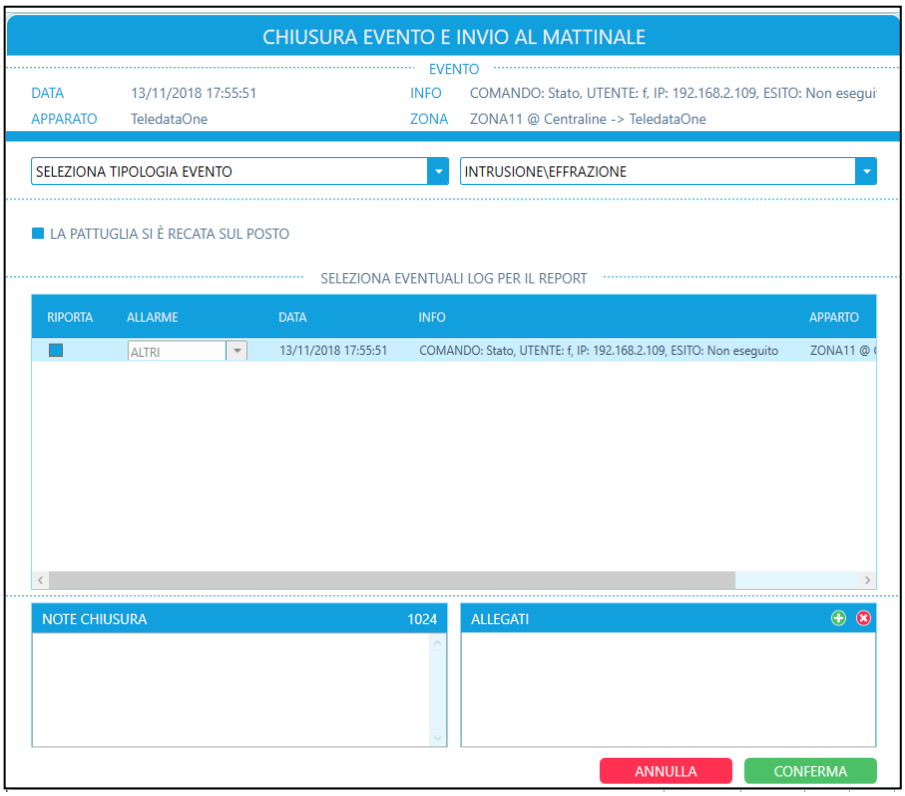
The Daily Report groups alarms handled within a specified period. It consists of Event Records, each containing a set of handled alarms sent by a device. For example, an unknown person entering an area without authorisation may trigger several sensors connected to the same intrusion alarm control panel. An Event Record can group these alarms from that control panel.

To create a Daily Report, follow the steps below in two stages:

- Stage 1 – Create an Event Record
- Stage 2 – Find the Event Record and Create the Daily Report

Stage 1 – Create an Event Record

- Select an alarm from an alarm view.
- Take responsibility for the alarm by clicking **Gestione** (Manage).
- Click **Apri (Open).**
- Select **Manage** again, then **Close with Daily Report.**



The screen shows information about the selected event:

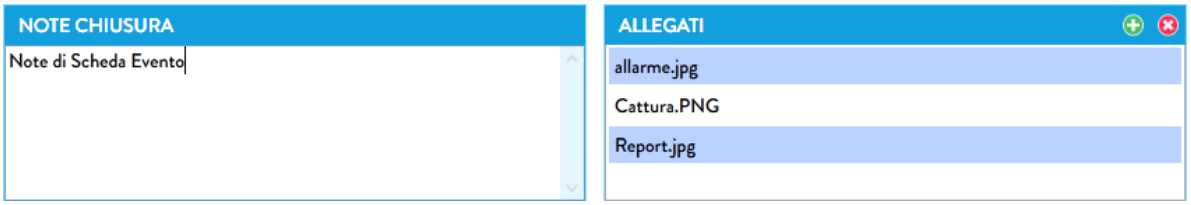
- Date: the date and time of the selected alarm.
- Info: contains the same information as the corresponding column on the alarm tab.
- Device: the control panel that generated the alarm.
- Zone: the zone containing the control panel or device.

The event type and its cause can be specified. If a patrol attended the site, its arrival date and time can be entered
by selecting its checkbox.

An event may be linked to other events. In this case, select several alarms using the checkboxes in the **Select Any Logs for the Report** area.



A comment can also be entered in **Closing Notes,** and images can be attached.

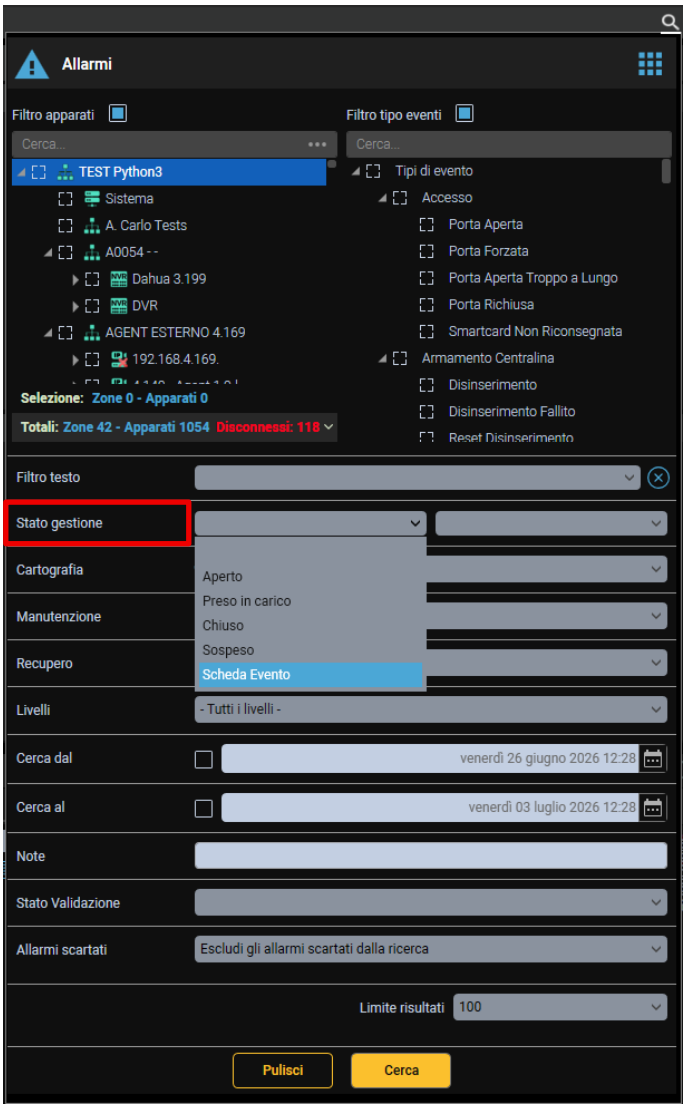


Click **Confirm** to finish creating the note.

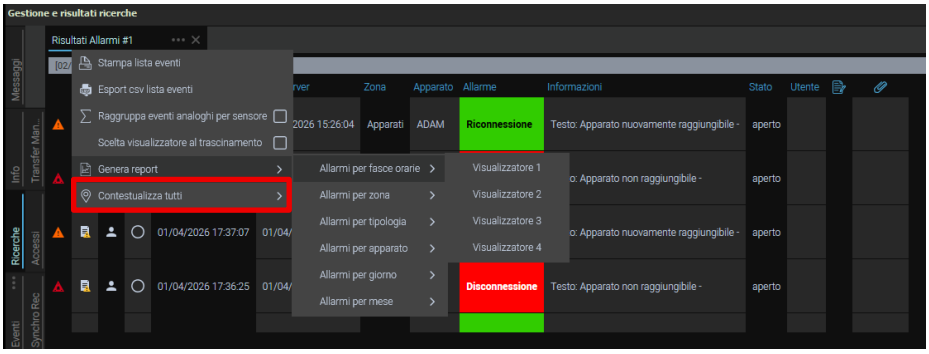


Stage 2 – Find the Event Record and Create the Daily Report

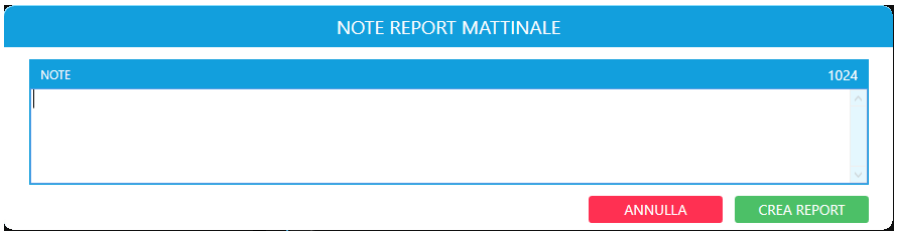
Once Event Records have been created, find them using **Alarm Search** by selecting “Event Record” under Management Status. Results can also be filtered by zone and time period, based on the event opening date:



The search results show Event Records in a table. Use the button highlighted in the figure to create the Daily Report:

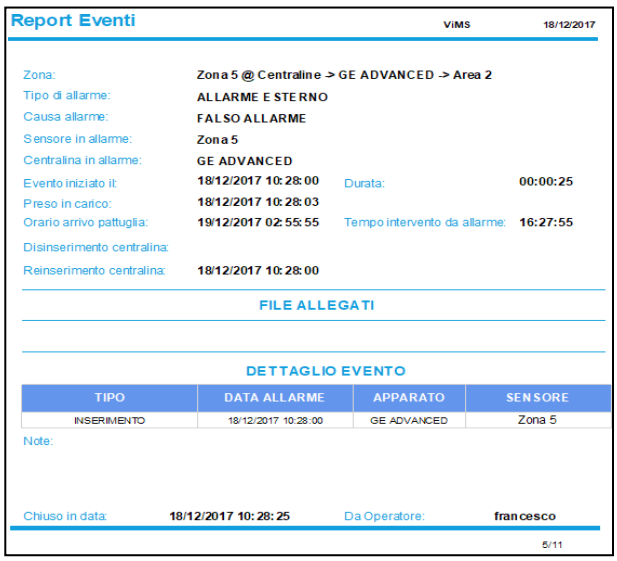


The operator can enter notes before generating the report. Then select **Create Report.**

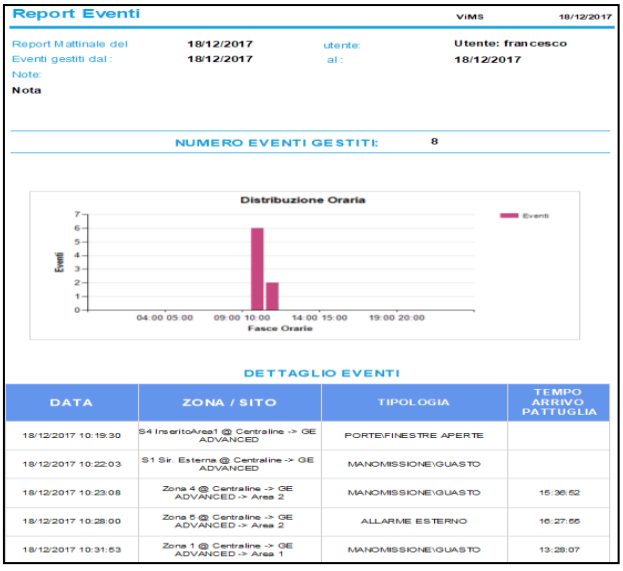


The report includes all Event Records on the search tab, structured as follows:

1. General information about the Daily Report:
    - Creation date.
    - User who created it.
    - Period during which the events occurred.
    - Notes (optional).
    - Number of events handled.
    - Chart showing events by time of day.
    - List of included events.



- Any attached files.
- Details of each displayed event, based on the information entered in stage 1.



SEARCH DAILY REPORTS

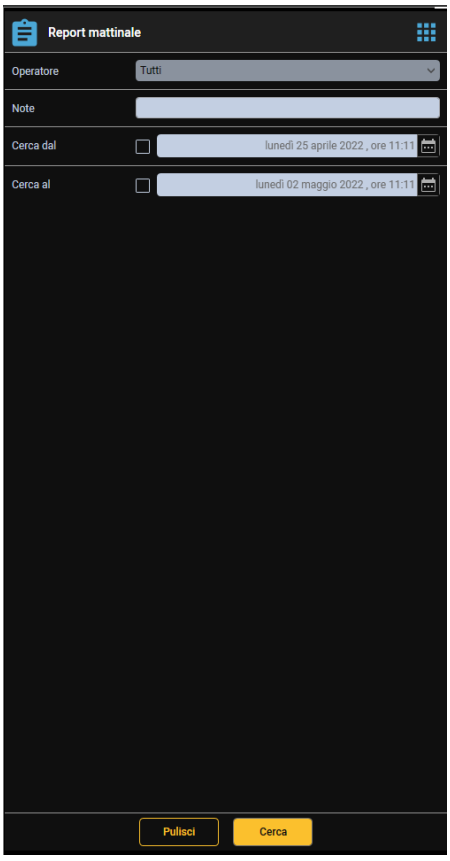
1. Open the advanced search panel using the button 
2. Select “Daily Report”:



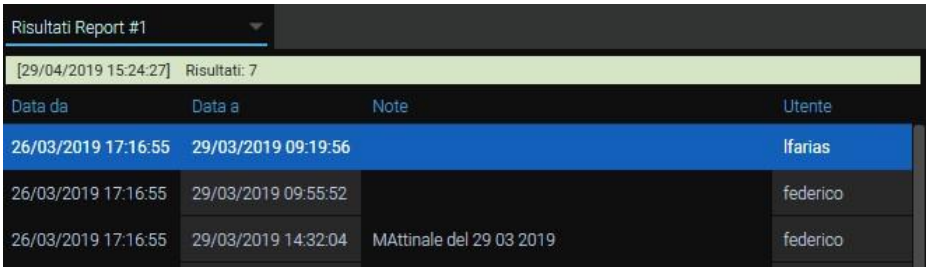
3. Set the required filters:
   - **Operator:** select the operators to include in the search. The list contains operators in the same group as the user currently logged into the system.

   - **Notes:** enter text to search for in the notes of existing Daily Reports.
   - **Search From/To:** specify the search period.

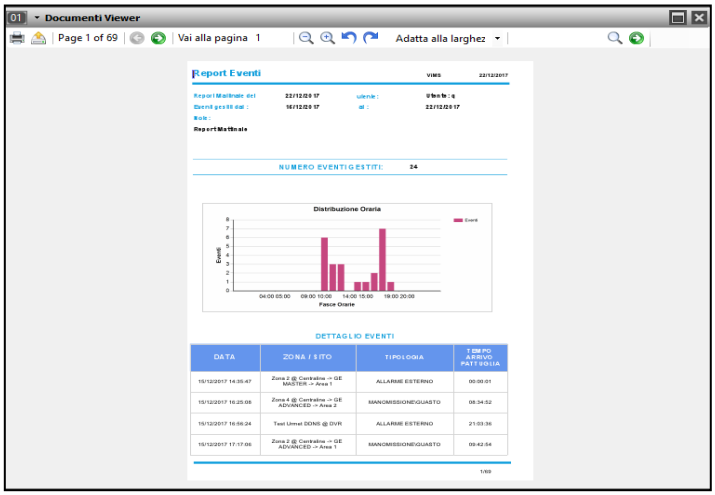
4. Start the search using the **Search** button:



The results are displayed in a table.



View report details: drag the report into a viewer. Use the controls to print it, save it locally, navigate its pages, adjust zoom and rotation, and search for specific text within the document.



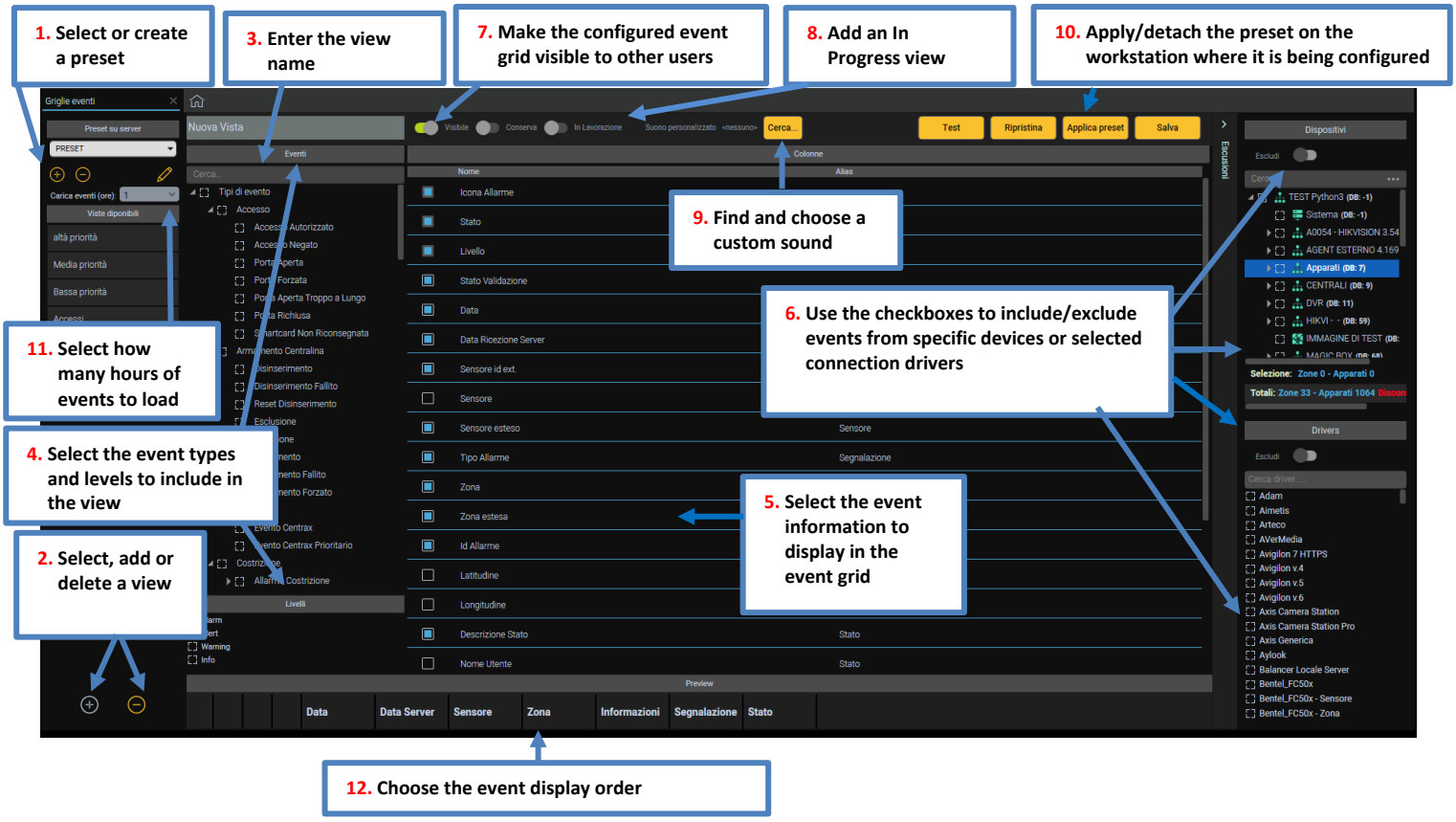
Export a report: right-click and select Download.



CONFIGURING ALARM VIEWS

The events managed by Elkron-ONE are grouped into configurable views, such as High Priority and Medium Priority:

The image shows the *Event Grids* section used to manage configurable views:



3. Name

The view name must be unique. To create an **In Progress** view, select its checkbox. The system automatically selects all available alarm types.

Only one **In Progress** view can exist in the alarm area. If this view already exists, the checkbox is disabled.

4. Alarm types

Select the alarm types to include in the view and choose the information to display for each type: Events, Name and Alias.

4. Alarm level

Select the alarm level: Alarm, Alert, Warning or Info.

6. Drivers

Alarms can be filtered for devices with a particular driver. Select one or more drivers and use the corresponding checkbox to specify which to exclude.

6. Devices

Using the Exclude checkbox, the user can:

a. **include specific devices:** clear **Select All** and select the devices to include;

b. **exclude specific devices:** select **Exclude** and select the devices to exclude.

Note: In both cases, selecting a zone directly includes or excludes all devices in that zone with one click.

9. Sound

Upload a sound using the Browse button and associate it with the view. It plays whenever the system receives a report in the new view.

11. Saving

The new view appears in the **Available Views** list. Select its checkbox to display it in the Alarm area.

12. Column order

The columns area shows how the new view will be displayed and allows the column order to be changed.

12. Column management.

Specify which alarm queue column will display each item of information.



The **Heading** is the column name in the alarm queue and can be renamed by the user.

Each information item can have its own column, in which case the heading must be unique. Alternatively, several items can share a column, in which case all items to be grouped must have the same label.

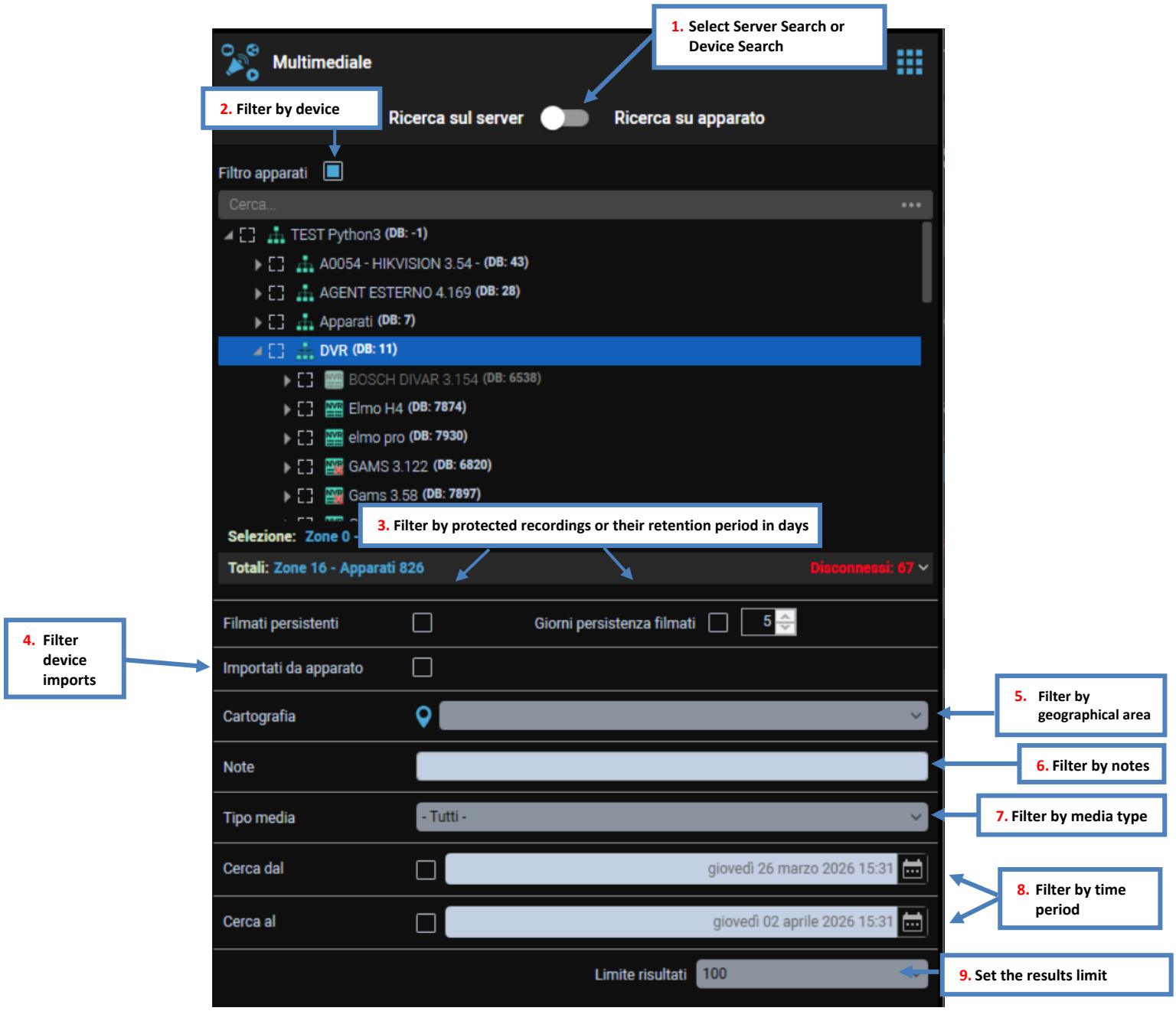
SEARCHING AND EXPORTING DATA

All data archived in Elkron-ONE can be searched for viewing, management and export. The advanced search function provides filters for selecting specific data.

Server multimedia search

Users with the required permission can open the panel shown below by clicking the magnifying glass in the top-right corner:





Searches for multimedia recordings on the server can be filtered by:

2- Devices: searches the database only for files from the selected devices. Select the Device Filter checkbox, then select the individual devices. Selecting a zone automatically includes all devices in that area. Use the **Filter** for large tree views.

Note: Search results also include data acquired before removal from devices subsequently removed from the system.

3- Protected files: searches only files marked as protected from deletion.

4- Imported from device: searches only files stored in the device's local memory on an SD card.

Note: If **Edge Storage** is enabled in Camera Configuration, recordings on the SD card are aligned with those on the server. For example, if camera-to-server connectivity problems caused a recording gap, this alignment can automatically retrieve the missing footage from the SD card.

5- Map selection: searches only data from devices located inside or on the boundary of the selected geographical area. The button  opens the map selection area.

Note: Map selections apply only to the current connection session of the specific client. All areas entered are removed from the system when the client closes.

6- Notes: searches only files with associated notes matching the entered text.

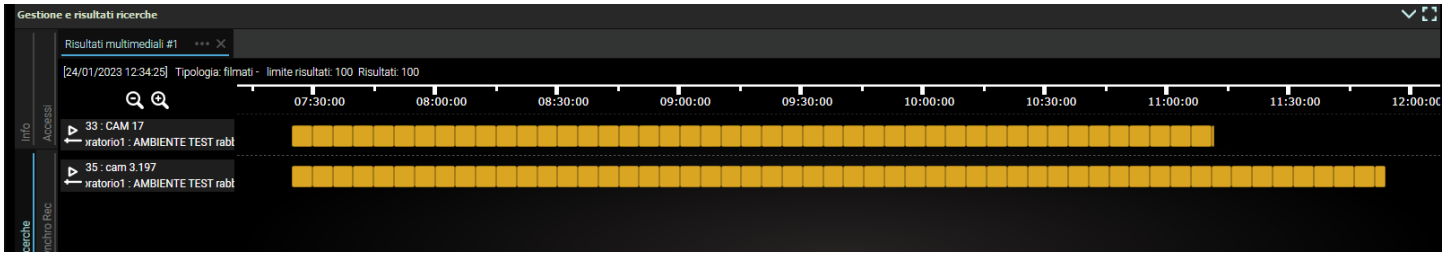
7- Media type: searches Videos, Photos, Audio or Documents.

8- Time period: searches data acquired during the specified period. Select the **Search From** and/or **Search To** checkboxes and choose the dates. The start date must be earlier than the end date. By default, the period covers the last ten days.

9- Results limit: returns the most recent 100 (default), 500, 1000 or 2000 results.

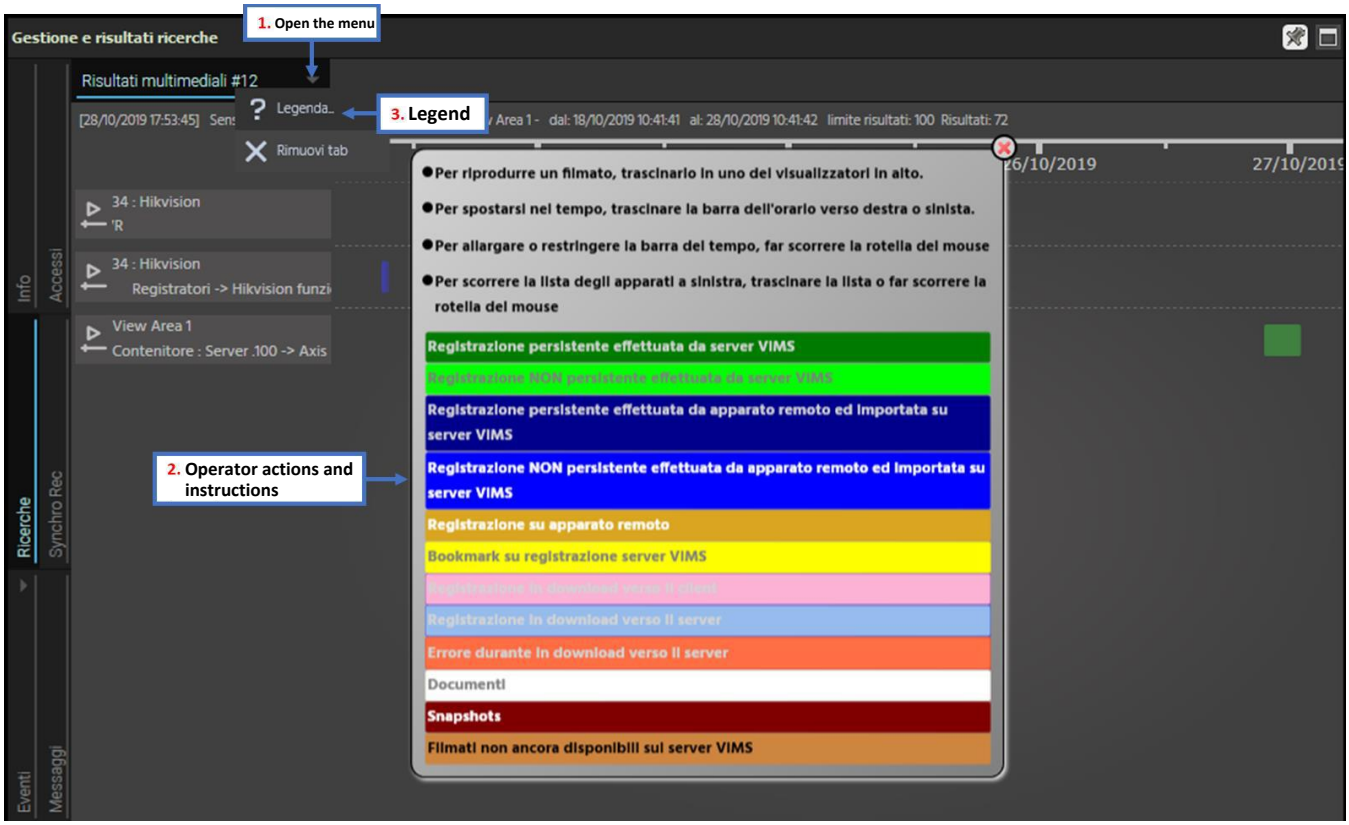
Viewing recorded footage

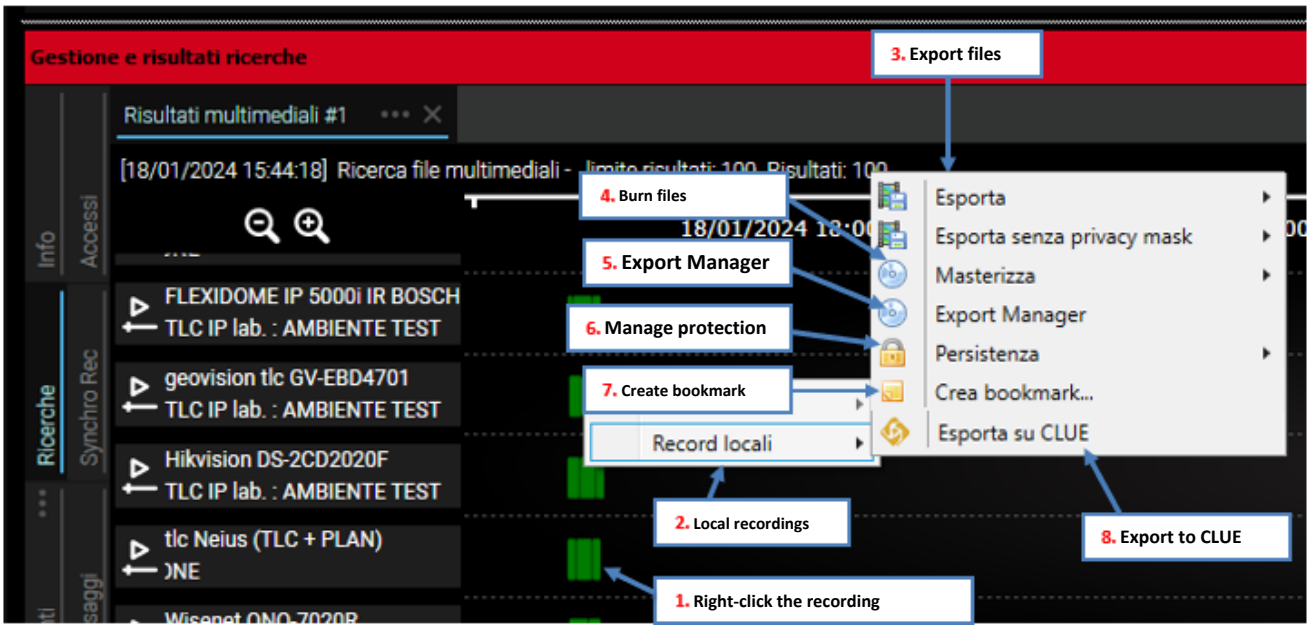
For each camera, the search results show all recordings available within the selected period. To view a recording, drag the required segment into a viewer. The playback controls are the same as those described in the **Live Video, Recordings and Playback Timeline** section:



Note: Use the mouse wheel or zoom in/out buttons to navigate the recording timeline.

The **Legend** shows the available user operations and file notifications, identified by colour:

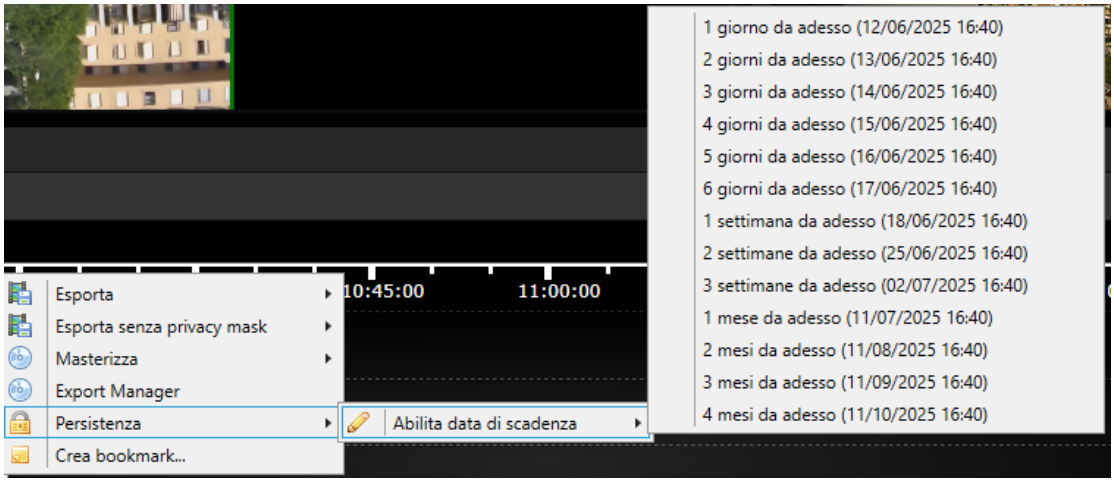




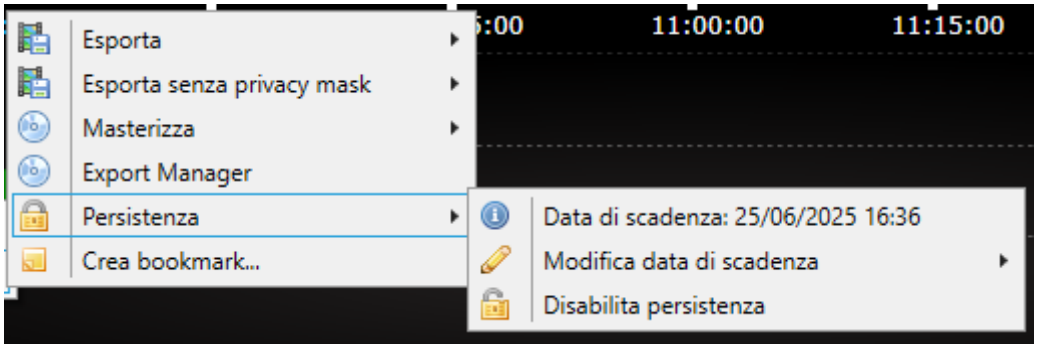
The image shows the actions available for recordings.

3. **File export**
   - **Export:** saves the selected file locally in *.mkv or .mp4 format.*
   - **Export without privacy masks:** saves the recording locally without privacy masks.

4. **Burn:** see Exporting and Burning with MultiViewer.
5. **Export Manager:** see Export Manager.
6. **Protection**
   Unprotected recordings:
   - **Enable expiry date:** protects the selected file from deletion for a specified period, for both IP camera recordings and recordings transferred to the server. The system cannot delete the protected file during this period, even after the normal retention limit expires. This limit is the number of days recordings are kept, depending on available storage space. Protected files are highlighted in darker green and blue. Note: The retention period for recordings imported to the server is configurable in Admin Web. For IP camera recordings, the retention period is configurable in *System Settings.*



Protected recordings:



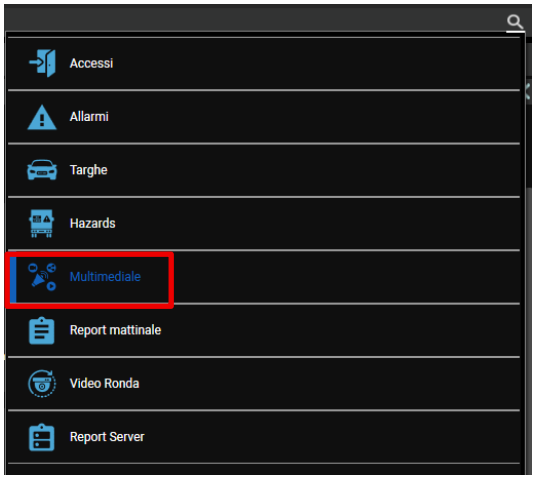
- **Expiry date:** shows the current expiry date of the file's retention protection.
- **Change expiry date:** replaces the current expiry date of the file's retention protection with a new date.
- **Disable protection:** removes the file's protection from deletion.

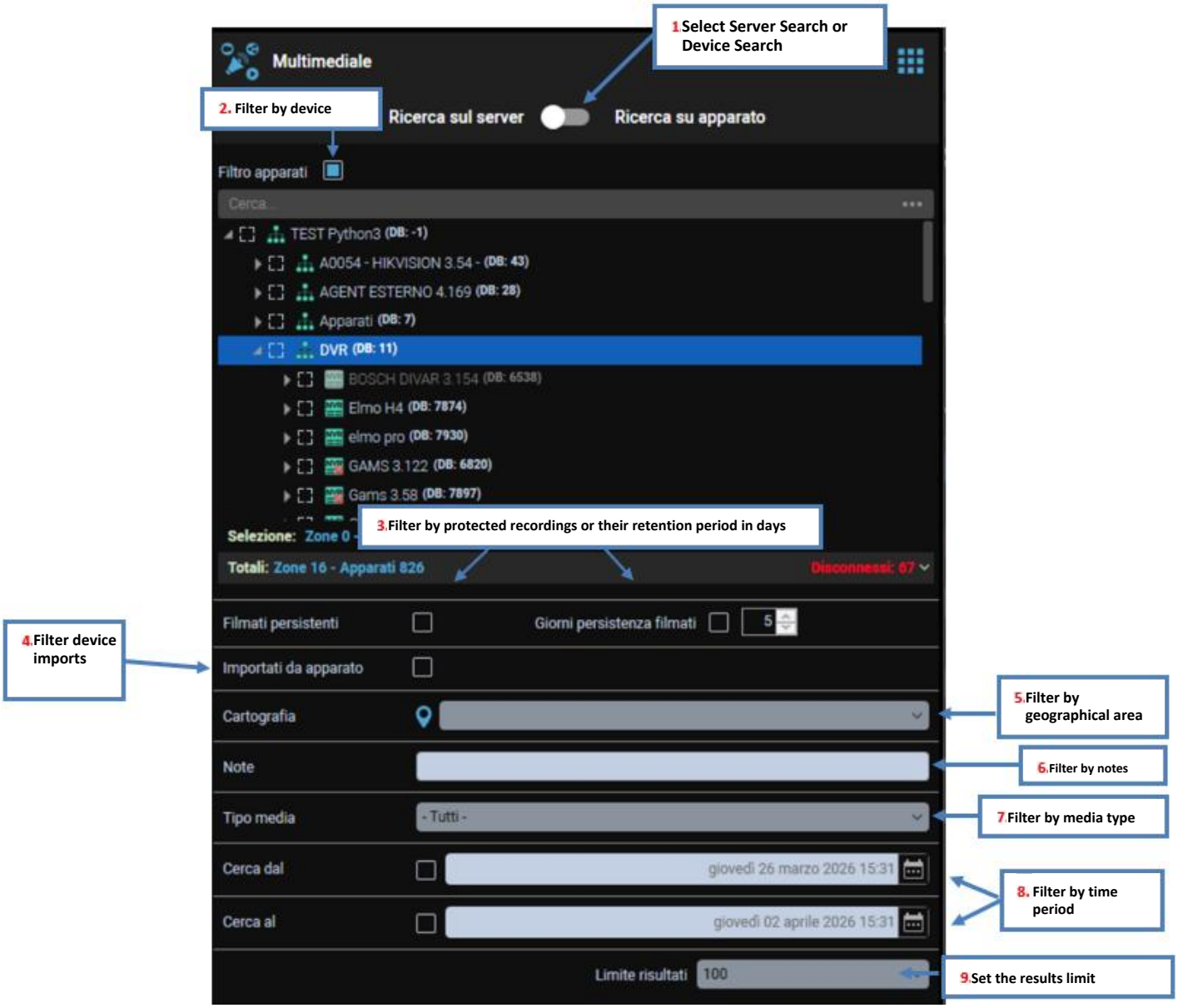
Note: To change a file's retention protection, the user must have the “Change retention protection even for another user's files” permission.

7. **Create bookmark:** adds notes to multimedia files:

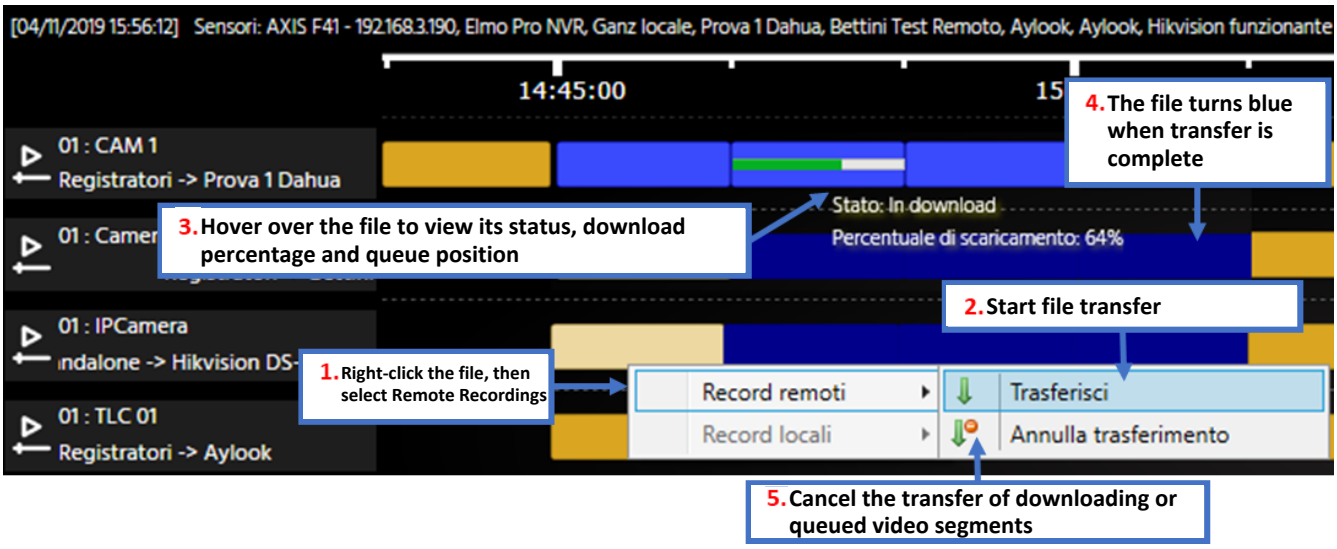


Searching for multimedia files on a device





The search filters are the same as those described for multimedia searches on the server. Results show files recorded on the device. To export a recording, first transfer it from the device's memory to the system server, as shown in the image.
Recordings transferred to the Elkron-ONE server also appear in server multimedia search results.



Event search

All alarms archived in Elkron-ONE can be searched for viewing, management and export. The advanced search function provides filters for selecting specific alarms.



1- Filter by device: searches the database only for data acquired from the selected devices. Select the **Device Filter** checkbox, then select individual devices. Selecting a zone automatically includes all devices in that area. Use the **Filter** for large tree views.

2- Filter by event type: searches by the event type selected for the device specified in Device Filter.

3- Filter by geographical area: searches only data from devices inside or on the boundary of the selected geographical area. The button  opens the map selection area.

4- Filter by alarm level: searches only the selected alarm level: Alarm, Alert, Warning, Info.

5- Filter by time period: searches data acquired during the specified period. Select the **Search From** and/or **Search To** checkboxes and choose the dates. The start date must always be earlier than the end date. By default, the period covers the last ten days.

6- Notes: searches only alarms with associated notes matching the entered text.

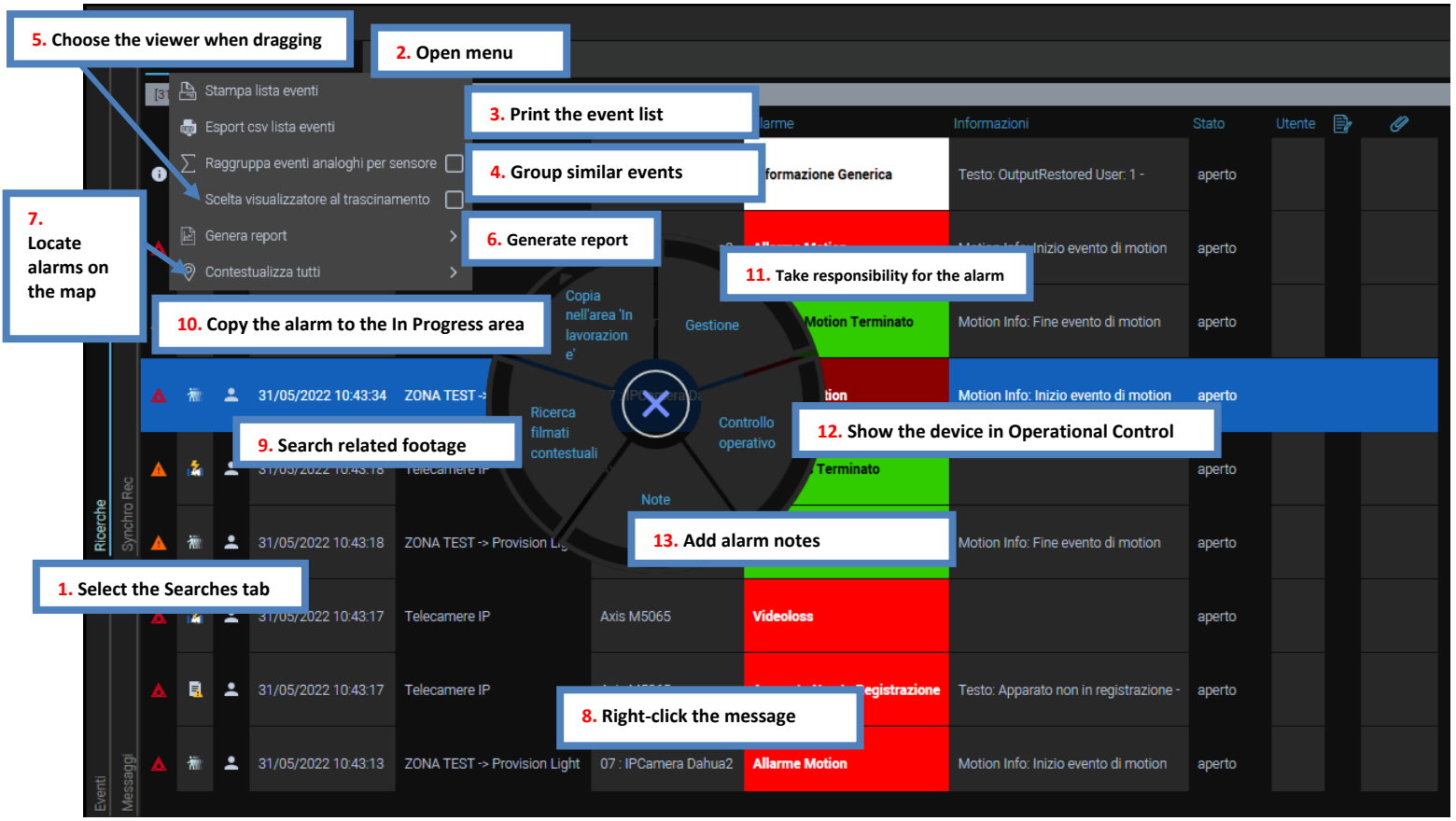
7- Filter by validation status: searches alarms whose validation is not performed, completed, positive, negative or in progress.

8- Filter by discarded alarms: three options are available: *Include discarded alarms in search,* which returns all alarms including discarded ones; *Search only discarded alarms,* which returns only discarded alarms; and *Exclude discarded alarms from search,* which returns only alarms actually notified.

9- Results limit: returns the most recent 100 (default), 500, 1000 or 2000 results.

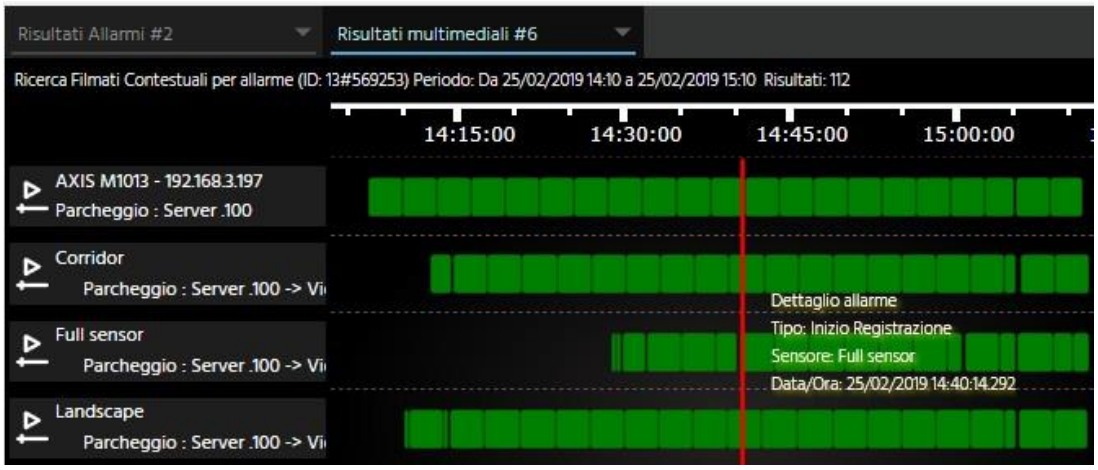
Search results are displayed in a table in the **Management and Search Results** area. They include the event date and time, originating device, event type details, management status and the presence of notes or attached files.

The image shows all actions available on the search results:



The results can be used to search for related footage from cameras in the same zone as the device that generated the alarm.

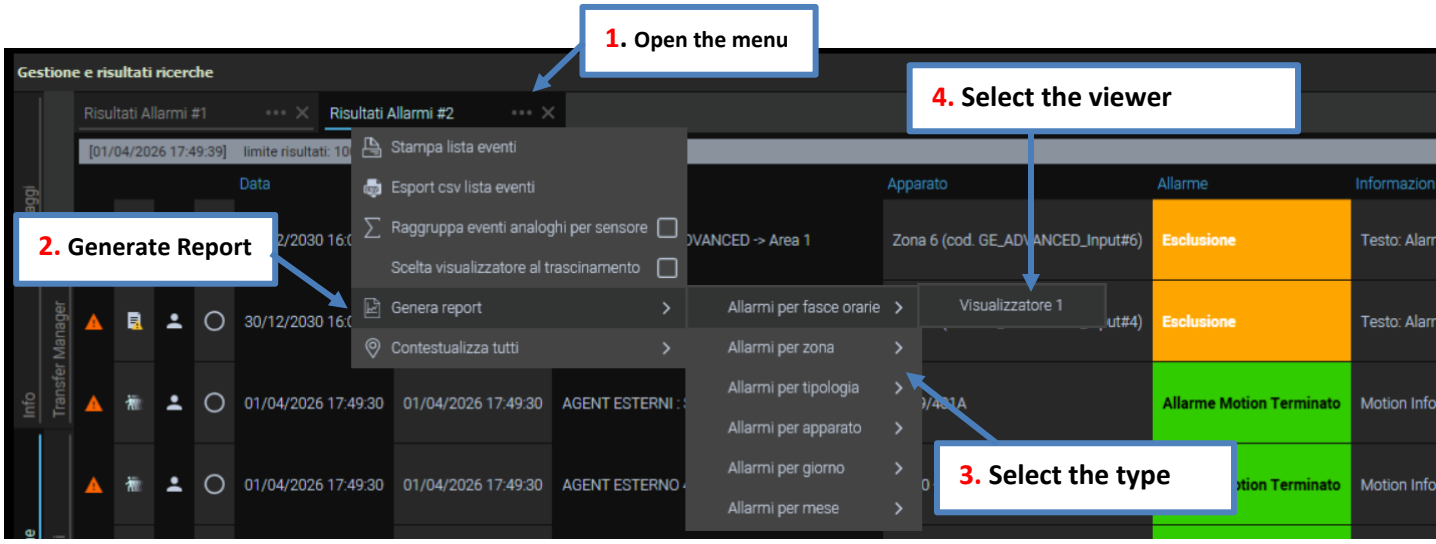
A red bar highlights the alarm. Hover over it to display the details.



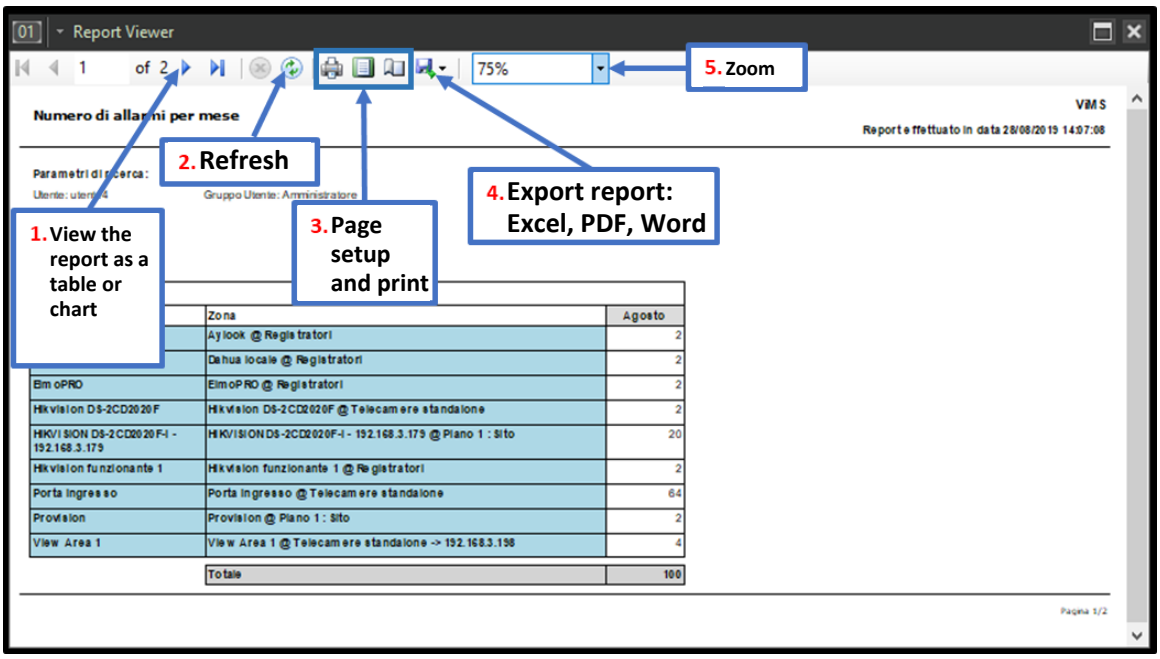
SEARCH RESULT REPORTS

Elkron-ONE provides statistical analysis of events to help assess operational situations. Reports are generated from data stored by the system. Different report types are available according to the data category:

- **Event Reports:** alarms by time slot - alarms by zone - alarms by type - alarms by device - alarms by day - alarms by month.
- **Access Reports:** access recognition errors - access passage volume - access alarms.

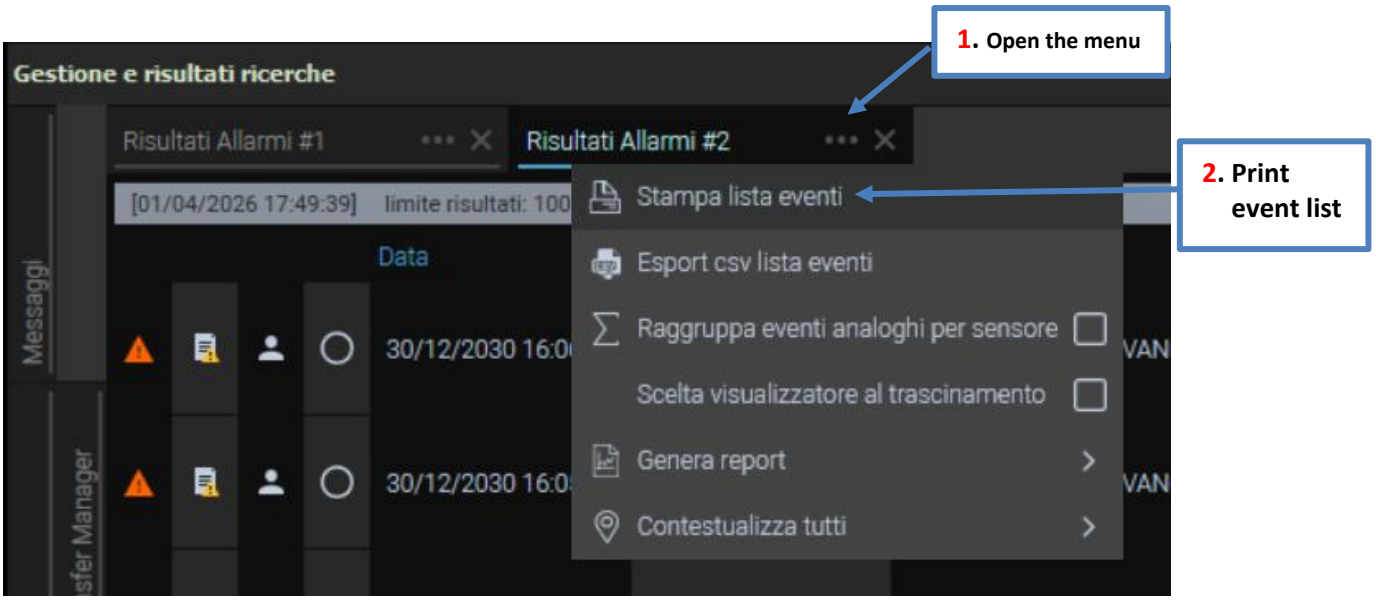


The report viewer provides controls to display charts, zoom, print and export reports.



PRINTING DATA

Elkron-ONE can print data managed by the system: the real-time alarm queue, search results and the internal message list. The image shows how to access printing.



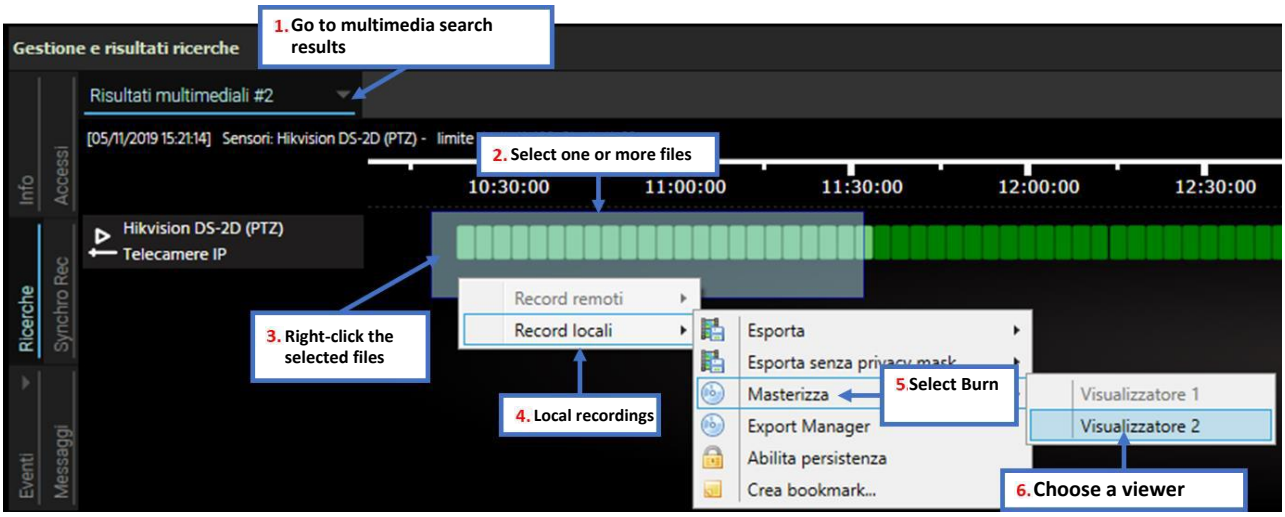
EXPORTING DATA

Elkron-ONE provides advanced functions for exporting database records to local storage or burning them to CD/DVD or USB storage. Transferred files can be viewed with a dedicated application without additional software. Export Manager is also available for bulk exports of audio and video files using configurable formats.

Exporting and burning with MultiViewer

The images show the steps for exporting or burning files.

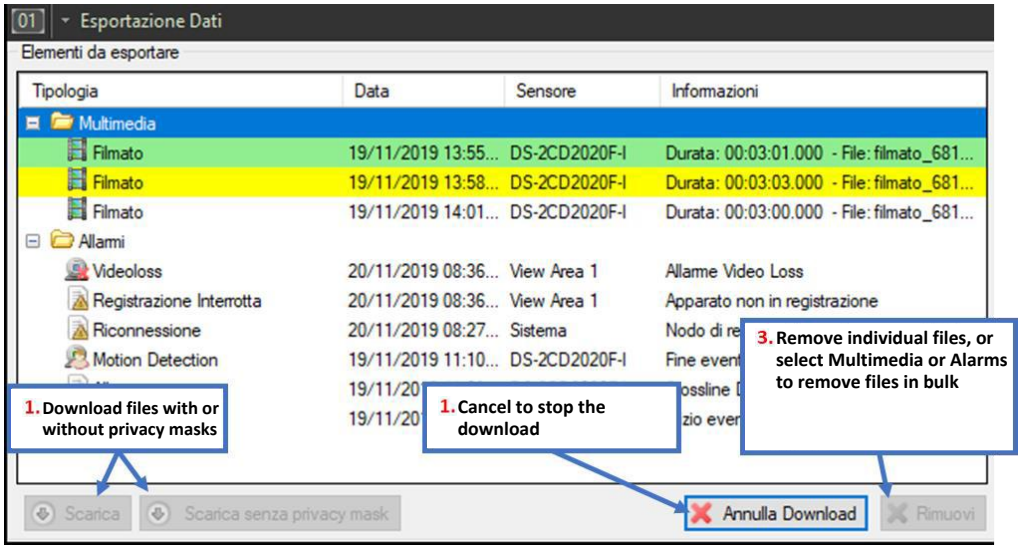
- **Select the files to export or burn**



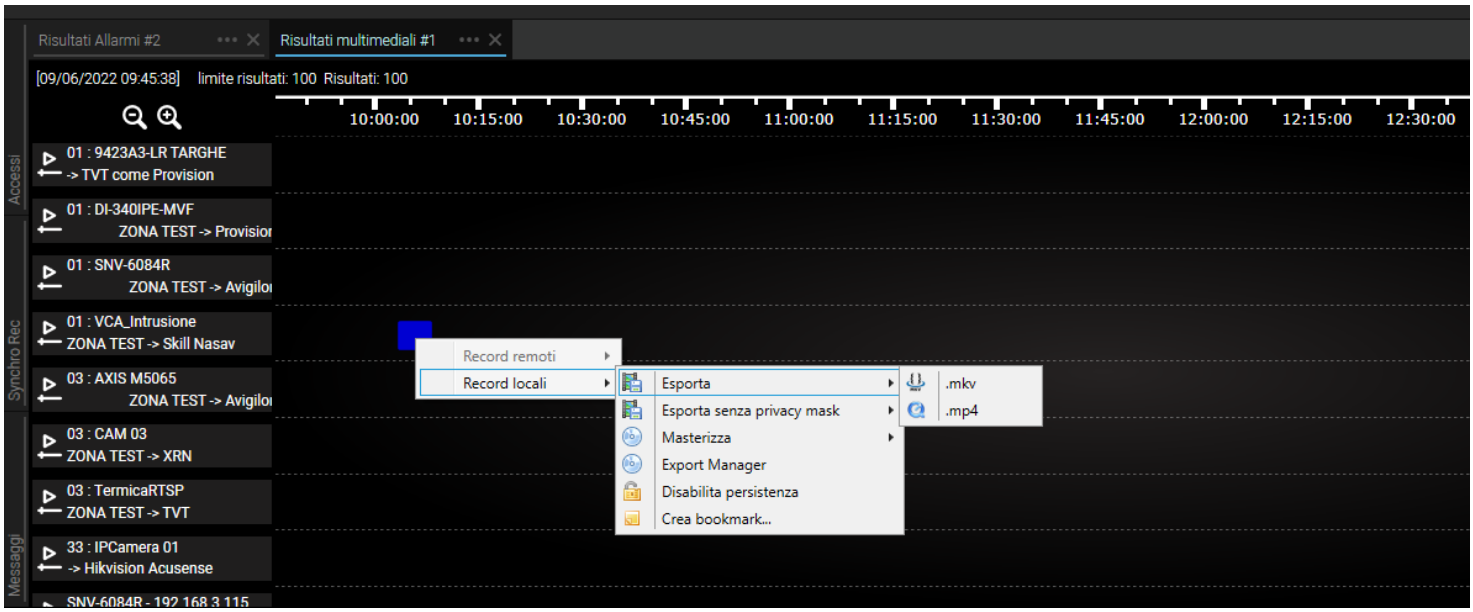
- **Download the files to export or burn**
  Selected files are added to the export panel. If it is already open, drag individual recordings into it. Alarms can be dragged individually or added in bulk by dragging the search tab into the export panel.

Files are transferred to a temporary storage area on the local PC, usually C:\Windows\Temp.

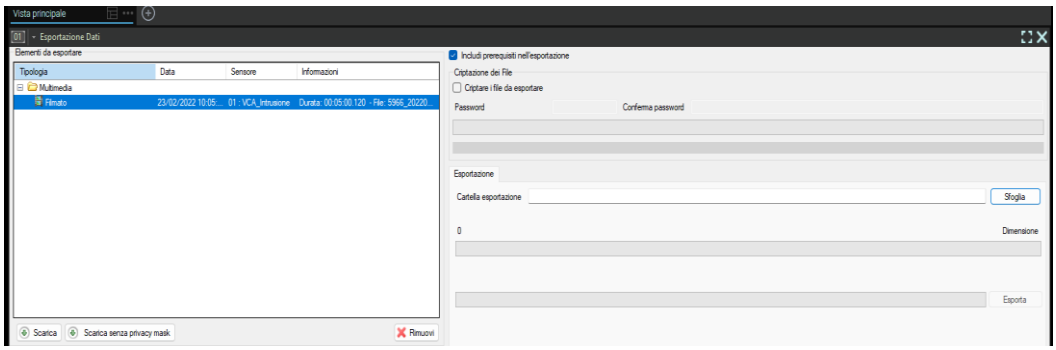
Downloads have three possible states: **green** for successful, **yellow** for in progress and **red** for failed. Before exporting or burning, remove any files that failed to download correctly, highlighted in red.



- **Start exporting the files**



- **Start burning the files**



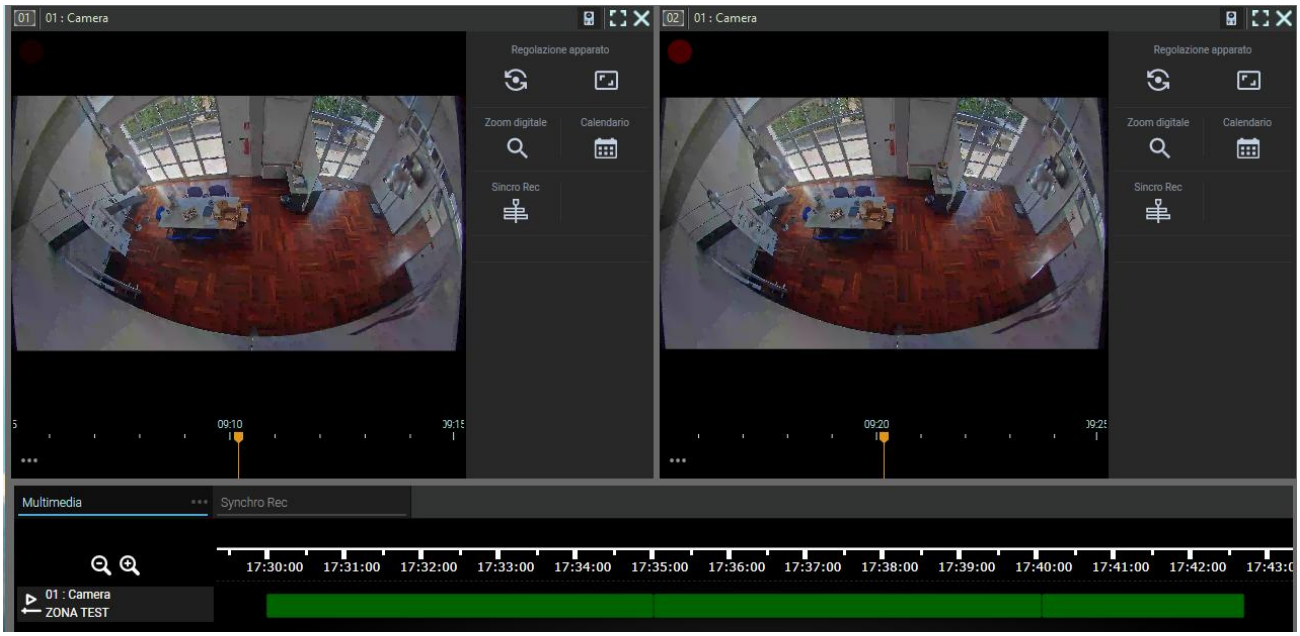
- **View the exported or burned files**

To view the files, launch **MultiViewer** from the export folder.



If the files were encrypted, the password used during encryption is requested. MultiViewer then decrypts the exported files. The user is also asked to validate the exported files to check for falsification or tampering. Depending on the number of files, this may take several minutes.

If validation is skipped, MultiViewer opens immediately.

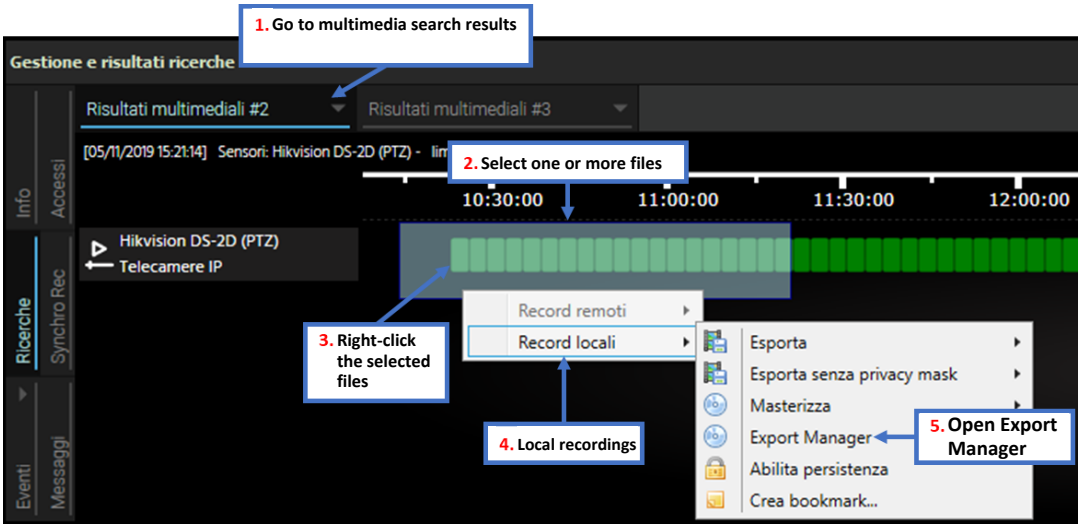


MultiViewer has two viewers for displaying data grouped into themed tabs. Drag and drop exported files into the viewers to display them.

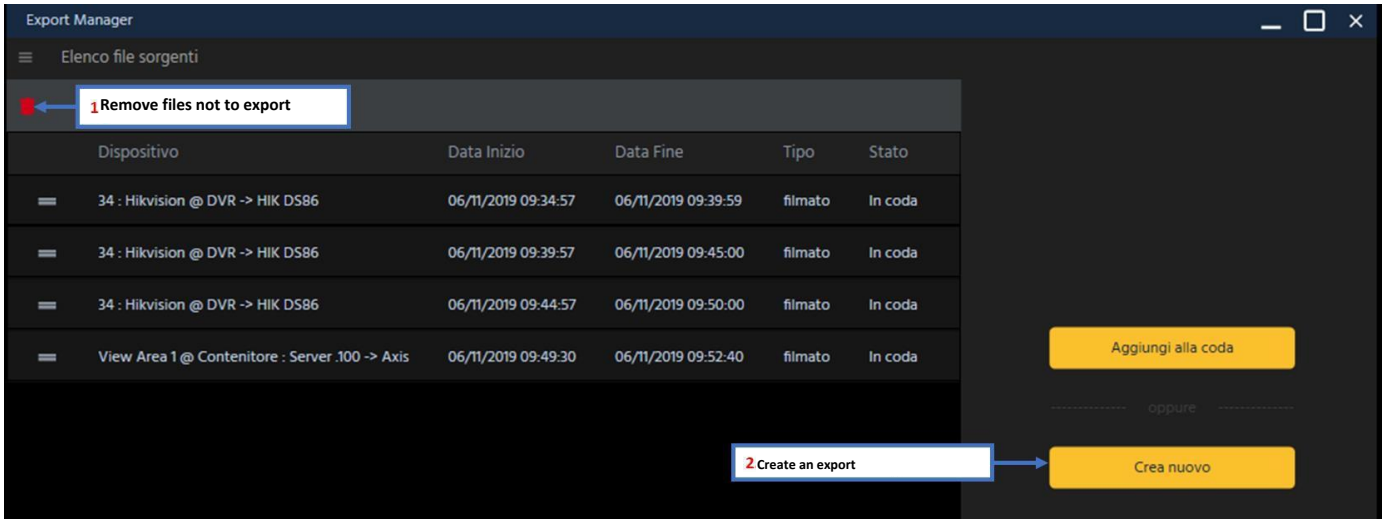
Export Manager

The images show the steps for exporting files.

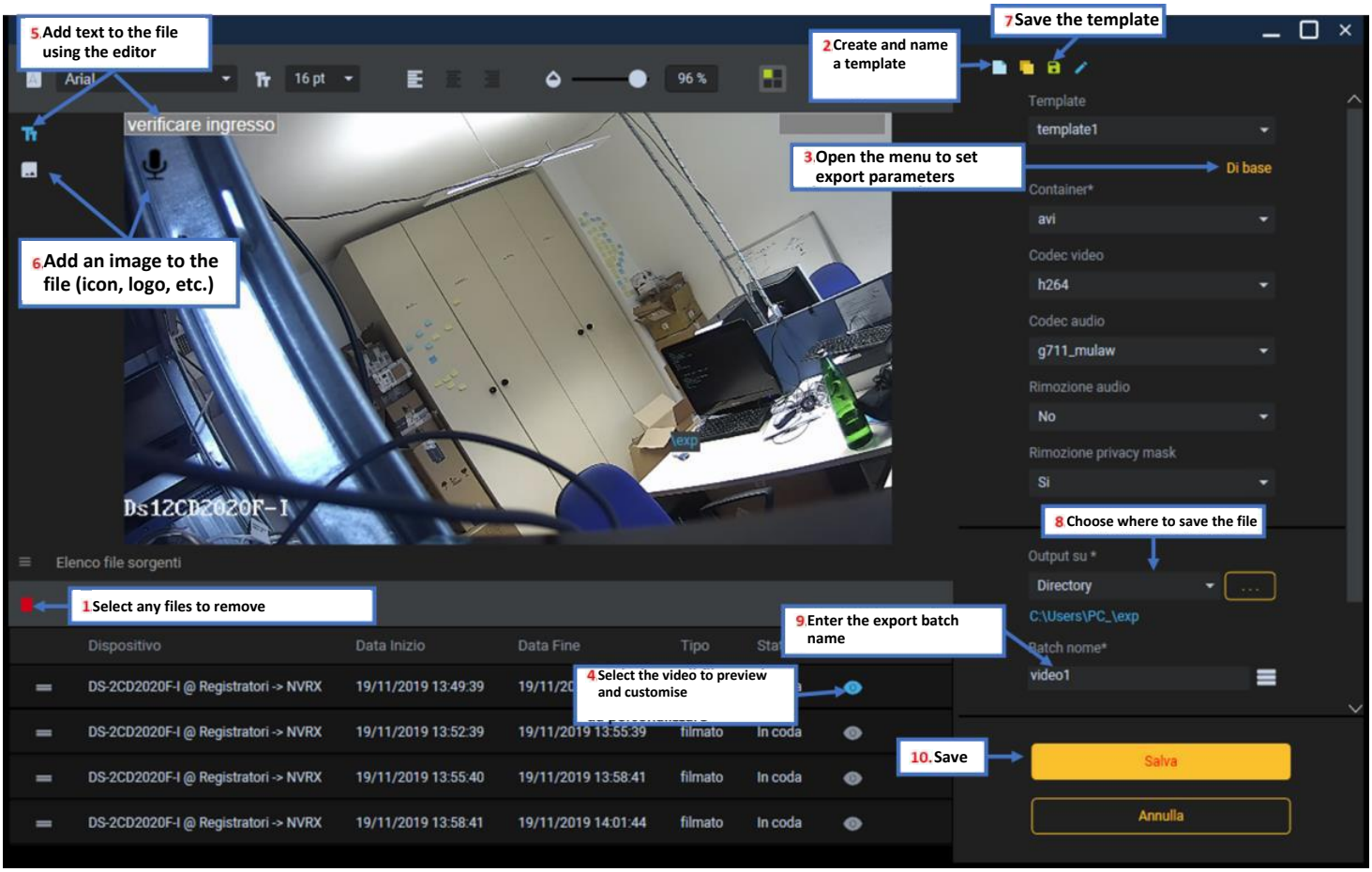
- **Add the files to Export Manager.**



- **Create the export batch.**



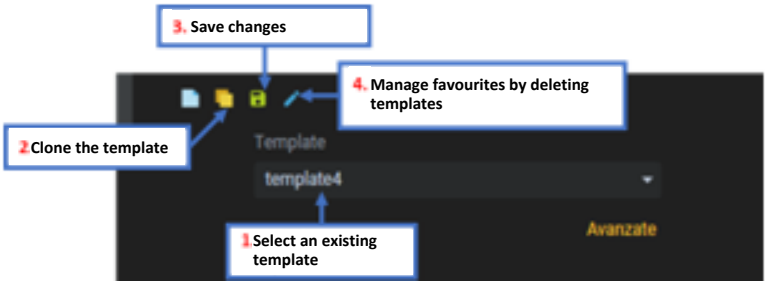
- **Customise the export by creating a new export template.**



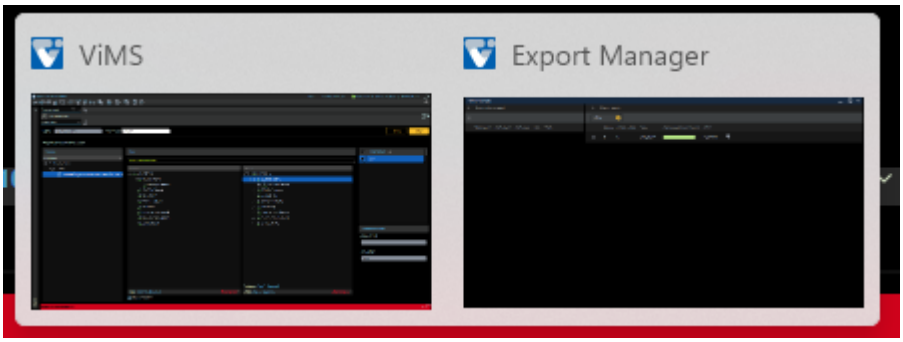
3. Advanced: configurable parameters:

- ✓ **Container:** a file format that can hold different types of data compressed using audio/video codecs.
- ✓ **Video codec.**
- ✓ **Audio codec.**
- ✓ **Remove audio:** removes audio when selected.
- ✓ **Remove privacy masks:** users with the required permission can remove privacy masks from the export.

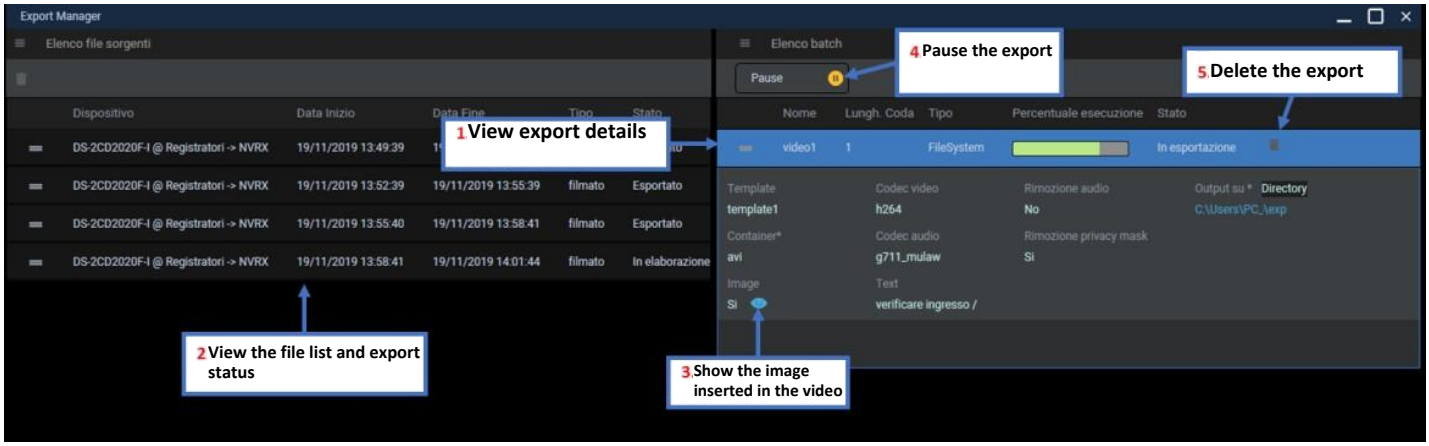
Alternatively, use existing templates. The image shows how to use saved templates, clone a template to retain some settings while changing others, or delete previously saved templates.



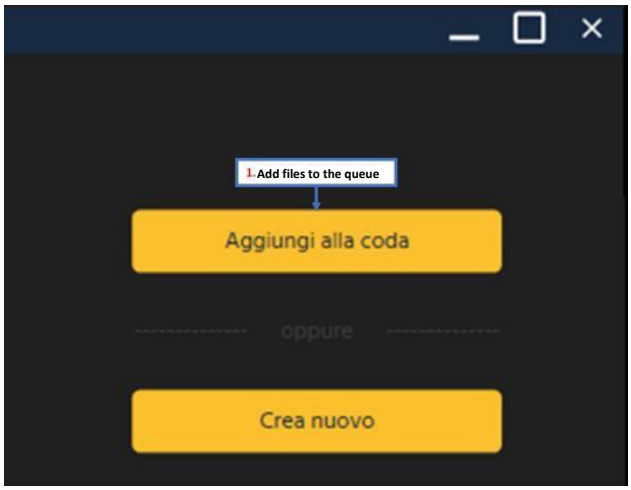
If Export Manager is minimised, use its dedicated window to reopen it.

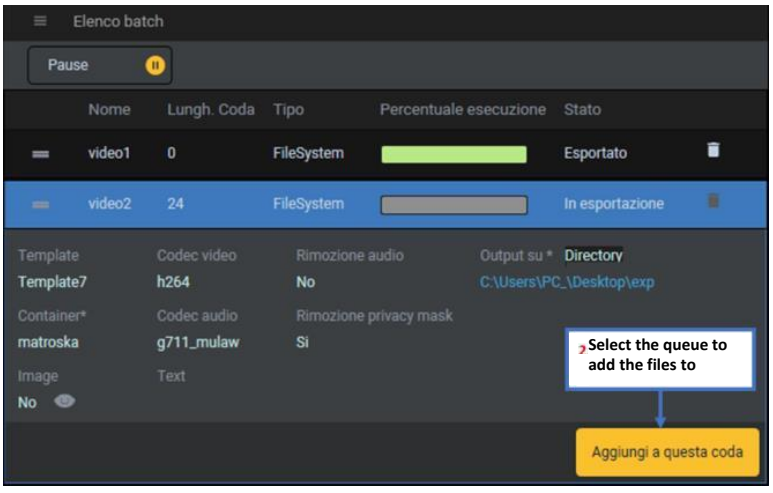


- **Start exporting the files.**



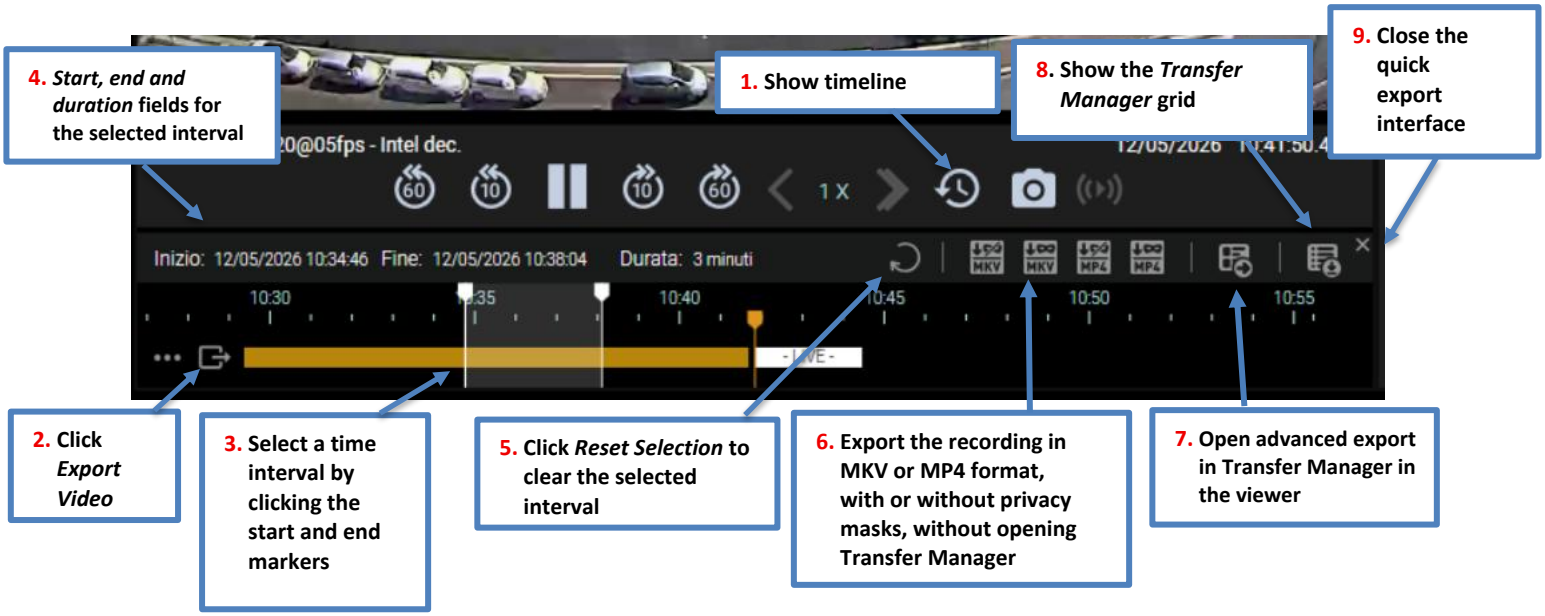
- **Adding files to a queue already being processed by Export Manager.**





Quick export

To export a recording quickly, follow the steps shown in the image below.



Quick video export is available in VideoViewer, Video Browser and Synchro Rec. In Synchro Rec, the same recording period can be exported from several cameras simultaneously. All sections use the buttons described above. For Synchro Rec, opening advanced export from Transfer Manager always uses the viewer for the first camera in the list.

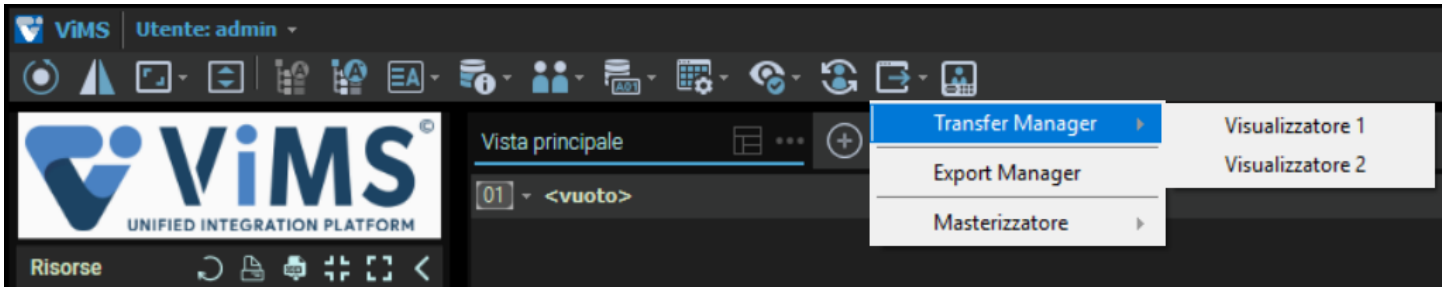
Note: Quick export requires the *"Allow the user to view recordings"* permission.

This function is supported by server versions that include Transfer Manager, from **v. 6.0.5.0.**

Transfer Manager

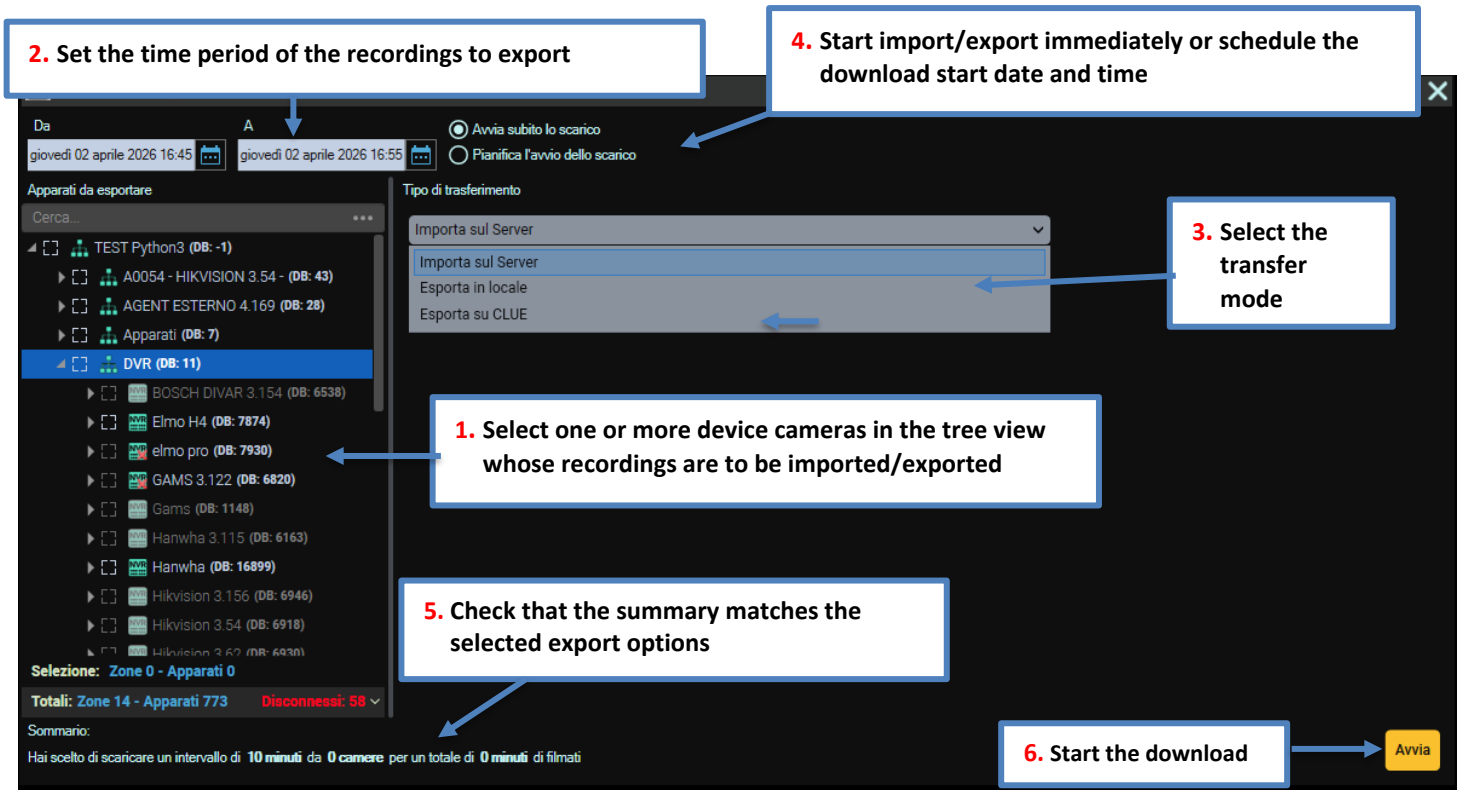
Transfer Manager transfers recordings to the server and exports server data to local storage. The images show how to open Transfer Manager and download video files.

- **Click the Import/Export icon to open Transfer Manager in a viewer**

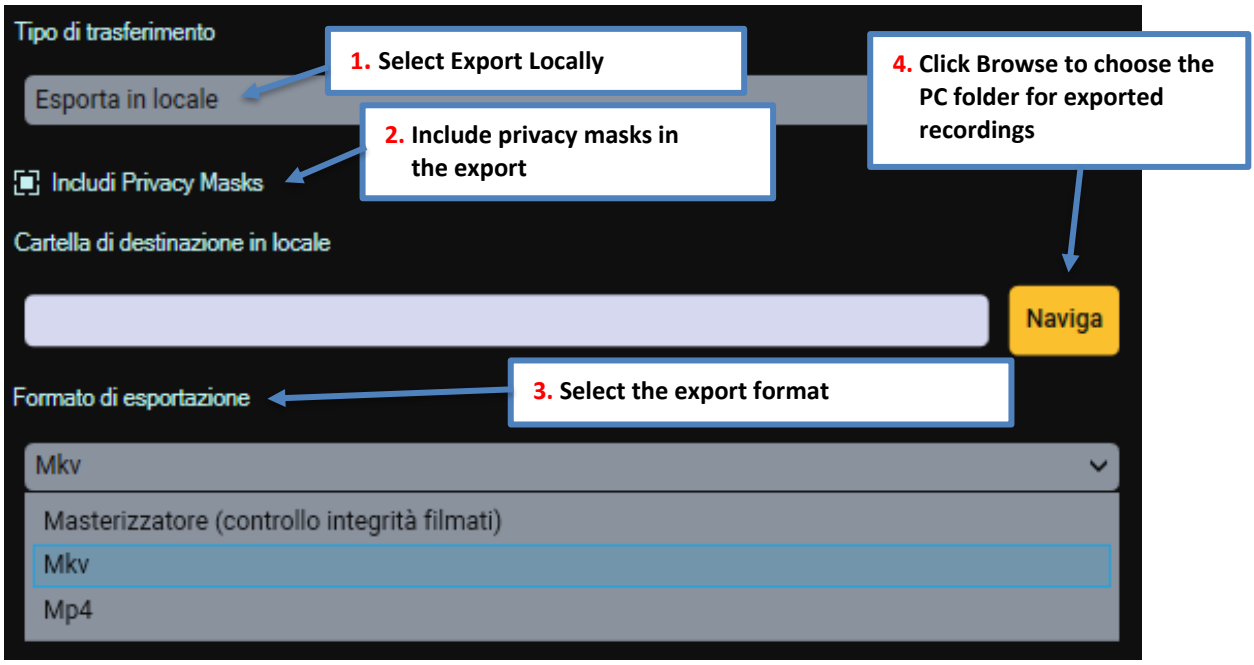


- **Download the files to import to the server or export locally**

Local export always begins by importing the recording to the server. Once this is complete, the second stage, export to local storage, starts automatically.



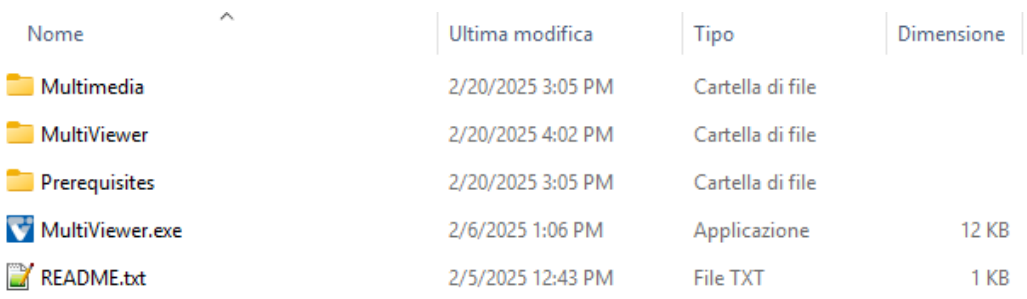
- **If local export is selected (3), choose the recording export format**



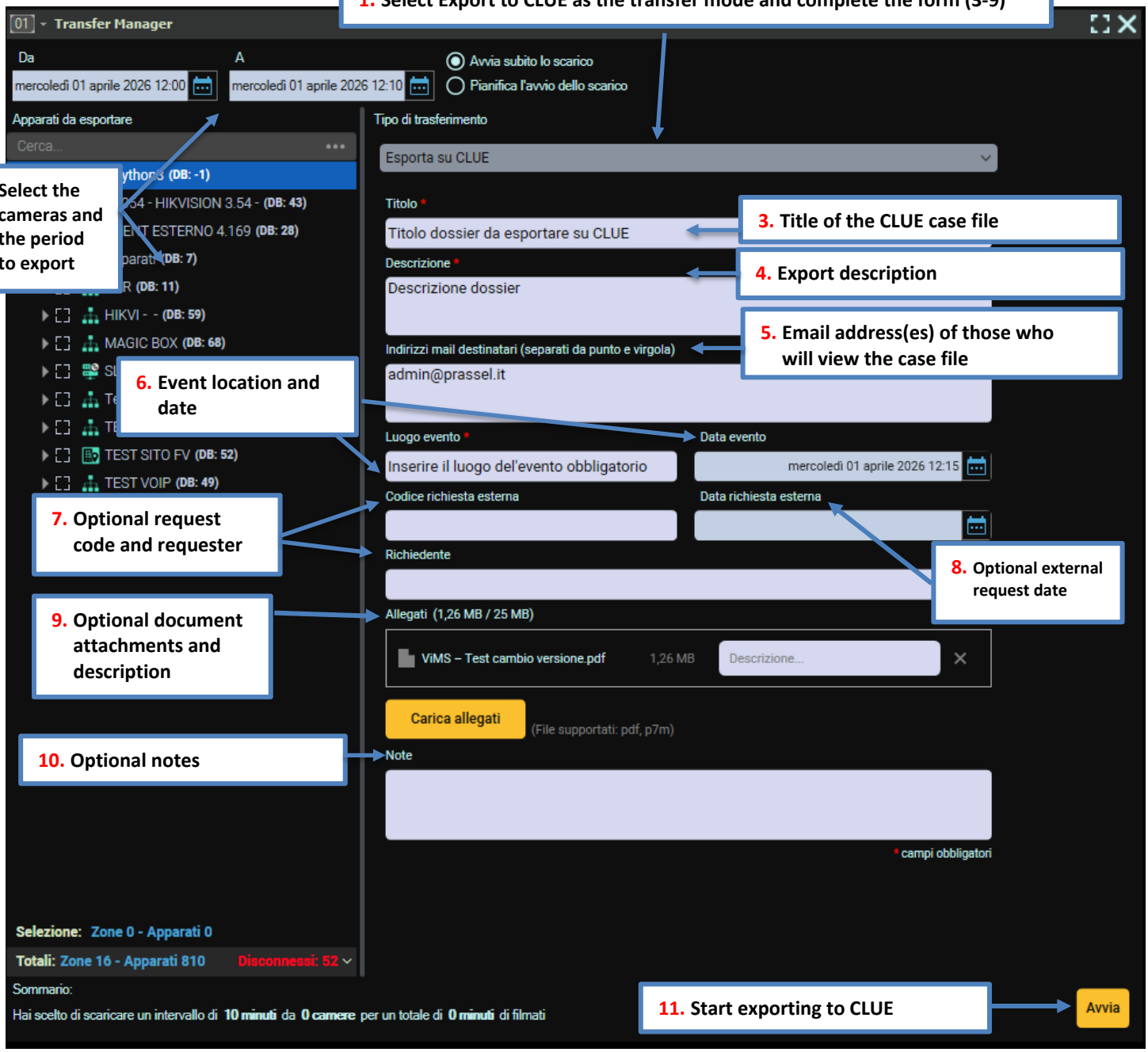
- **For Burner (MultiViewer), choose whether to enable an encryption password and include prerequisites in the export (selected by default)**



Note: If prerequisites are included, a *Prerequisites* folder is created inside the MultiViewer installation folder.



- **If Export to CLUE is selected (3), complete the form for creating the CLUE case file**

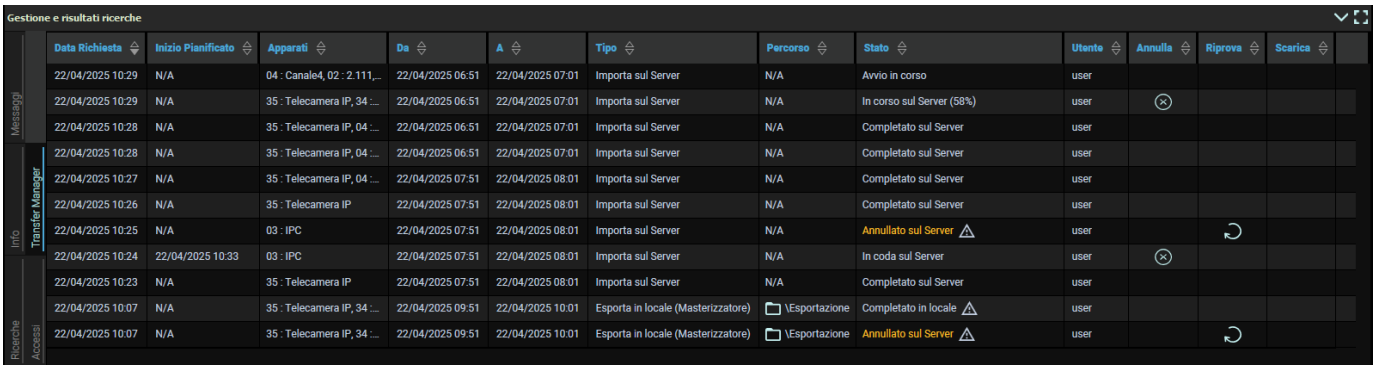


5) Recipient addresses for the case file in CLUE are mandatory by default. From server version 6.0.7.0, a server-side setting can make this field optional. If no recipient is added, the case file is available in CLUE only to account managers, as an In Progress case file.

8) Attachments can be uploaded only in *.pdf* and *.p7m* formats. The maximum upload size is 25 MB and the maximum number is 100.

Note: From client version 6.0.7.0, Export to CLUE is no longer available in multimedia search and is available only in Transfer Manager.

When export starts, the event grid automatically switches to the Transfer Manager tab, showing the status of all started, cancelled or ongoing tasks:



Each task has the following columns:

- **Request Date:** the download start date and time.
- **Scheduled Start:** if populated, the scheduled date and time for downloading camera recordings.
- **Devices:** the cameras selected for export.
- **From/To:** the period being downloaded.
- **Type:** the transfer type and, for local export, the selected export format.

- **Path:** the selected export folder.
- **Status:** the current download status. The triangle explains any import/export errors.

- **User:** the name of the user who started the download.
- **Cancel:** cancels a transfer in progress.
- **Retry:** attempts the download again if it was cancelled or failed.

- **Download:** manually starts the local download if it did not complete correctly, for example because the client was closed while the task was transferring data to the server.

As described above, the current download status appears in the grid's *Status* column. The following legend describes the possible statuses and colours.

COLOUR	STATUS
White	Recordings are downloaded **without errors**
Yellow	**Errors occurred during download**
Red	The recording download **failed**

Status of tasks transferring to the server

- **Starting:** import to the server is starting.
- **Completed on Server:** import to the server completed without errors.
- **Completed on Server, with Errors:** import to the server completed, but some chunks failed.
- **In Progress on Server:** download to the server is in progress, with the percentage displayed.
- **In Progress on Server, with Errors:** download to the server is in progress, but some chunks failed.

- **Queued on Server:** when downloading several channels from the same device, they are queued and their queue positions are shown.
- **Cancelled on Server:** a user cancelled the server download.
- **Failed on Server:** transfer to the server failed, for example because all chunks failed or communication with DVR Proxy failed.

Status of local export tasks

- **Completed Locally:** local export completed without errors.
- **Completed on CLUE:** export succeeded and the CLUE case file was created. Note: If a tooltip is still present in this state, the error relates to stage 1, transfer to the server, rather than export to CLUE.

- **Completed Locally, with Errors:** local download completed, but some chunks failed.

- **Completed on CLUE, with Errors:** export completed, but some chunks failed.

- **In Progress Locally:** local download is in progress, with the percentage displayed.
- **In Progress Locally, with Errors:** local download is in progress, but some chunks failed.

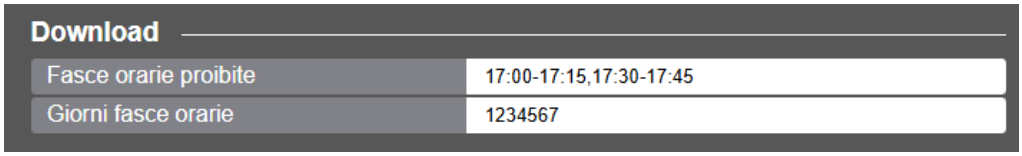
- **In Progress on CLUE:** download to CLUE is in progress, with the percentage displayed.
- **In Progress on CLUE, with Errors:** download to CLUE is in progress, but some chunks failed.
- **Queued Locally:** when downloading several channels from the same device, they are queued and their queue positions are shown.
- **Queued on CLUE:** multiple downloads to CLUE are queued.
- **Failed Locally:** local export failed, for example because all chunks failed or the client was restarted.
- **Failed on CLUE:** export to CLUE failed, for example because all chunks failed or the client was restarted.

Configuring prohibited time periods

Prohibited time periods can be configured on the server to block camera downloads for users without the *"Allow importing recordings from devices during prohibited periods"* permission.

Configure these in the Download section of AdminWeb. In *Prohibited Time Periods,* enter one or more periods during which downloads are blocked, using the format "HH:MM-HH:MM";

in *Time Period Days,* enter the weekdays on which the restriction applies, using the format "1356", where 1=Monday, 2=Tuesday, etc.



If a download is in progress when a prohibited period starts, it is interrupted and resumes only after that period ends.
Users without the *"Allow managing imports for the user's group"* permission can see only their own downloads, not those started by other users in the same group.

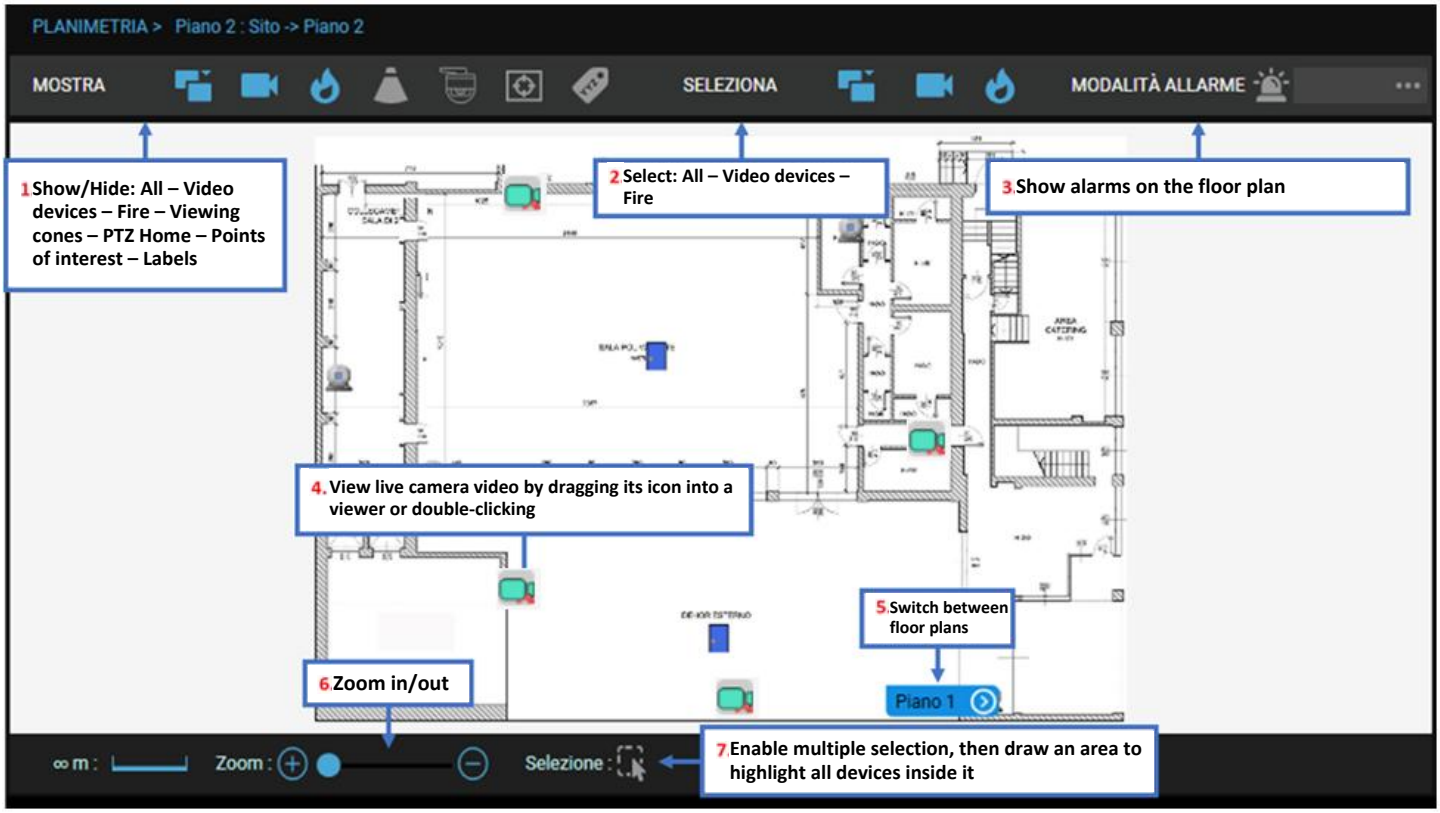
Note: The Transfer Manager grid refresh interval, in minutes, is configurable in the client configuration file using the *TransferManagerGridPollingIntervalInMinutes* parameter.

FLOOR PLANS

Elkron-ONE supports security device management using floor plans in *.jpg/.pn./.gif* formats. Any device in the resource tree can be placed on a floor plan to show its physical location and allow direct interaction, such as viewing live camera video with one click. Device display can be filtered, and alarms or critical events can be highlighted immediately on the floor plan. Floor plans can be customised with titles, text boxes and symbols. Multilevel navigation can be configured for quick movement between floor plans, including following events across different physical areas.

Navigating a floor plan

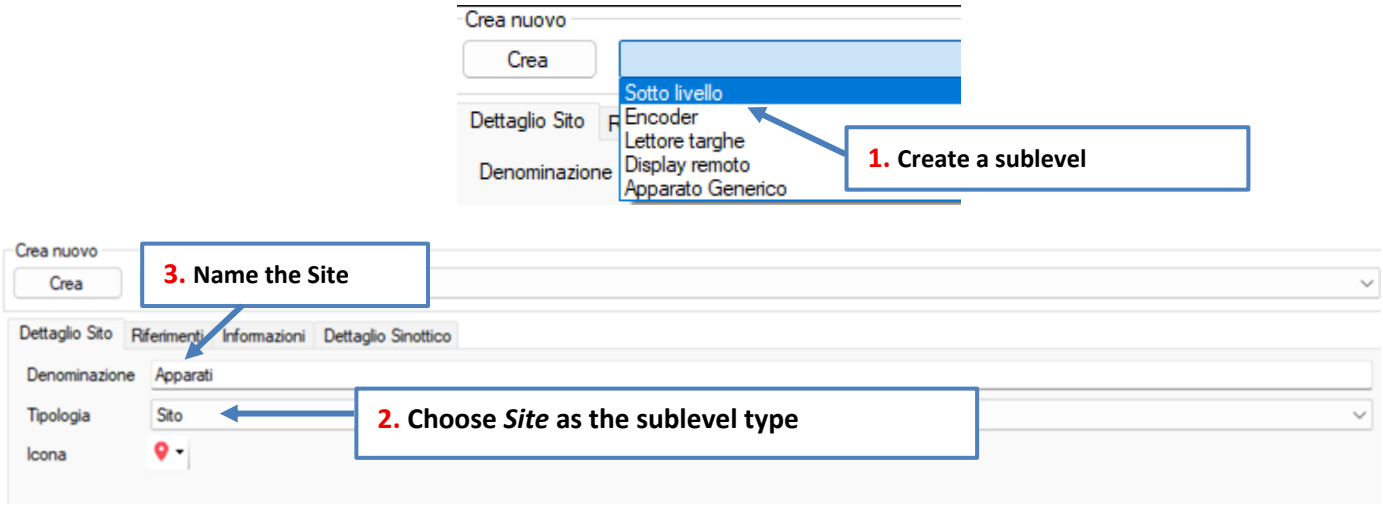
To view a floor plan, drag its icon from the resource tree into a viewer. The image describes the available functions.



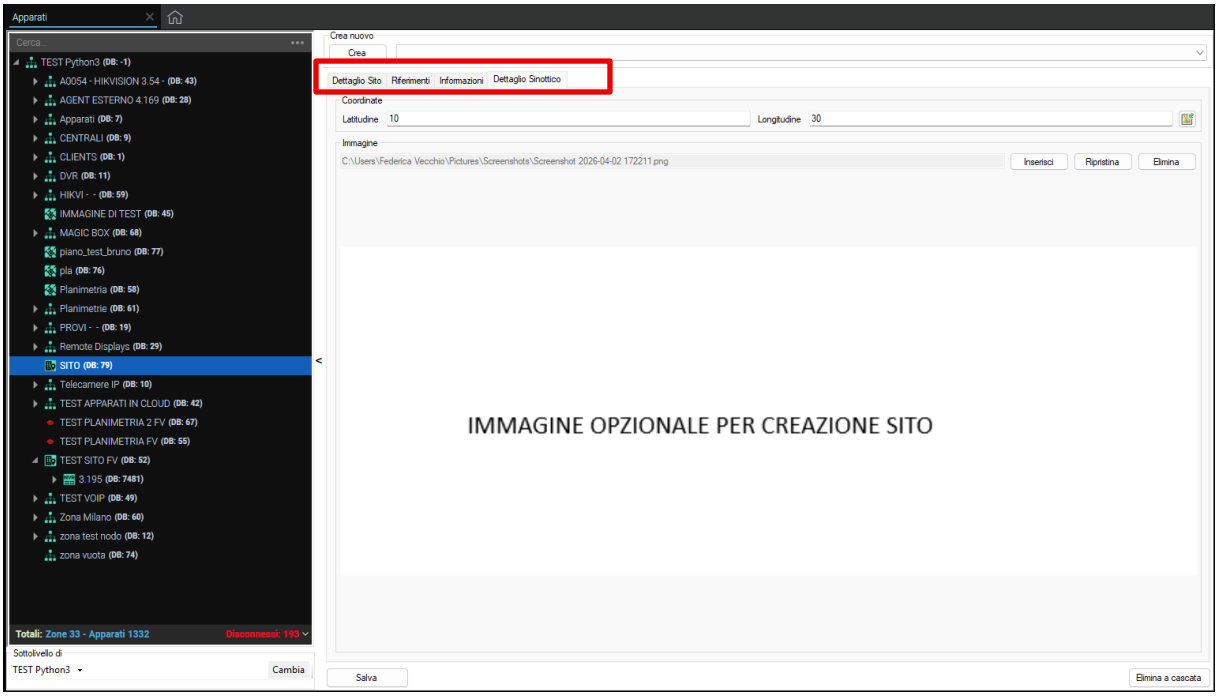
SITES

Elkron-ONE can organise tree view zones using sublevels called Sites. These act as zone containers, useful for grouping report and dashboard data, for example to create separate charts for larger areas.

Creating a site



A Site can be positioned on the map by assigning latitude and longitude, and an image can be associated with it. Map coordinates and the image are added through the *Overview Details* section in Device Management or through the Floor Plan and Site Management module.



VOIP MODULE

The **VoIP** module lets the Elkron-ONE client function as a VoIP SIP device. It can make and receive calls to and from other Elkron-ONE VoIP client workstations and VoIP devices in the tree view, such as video door phones.

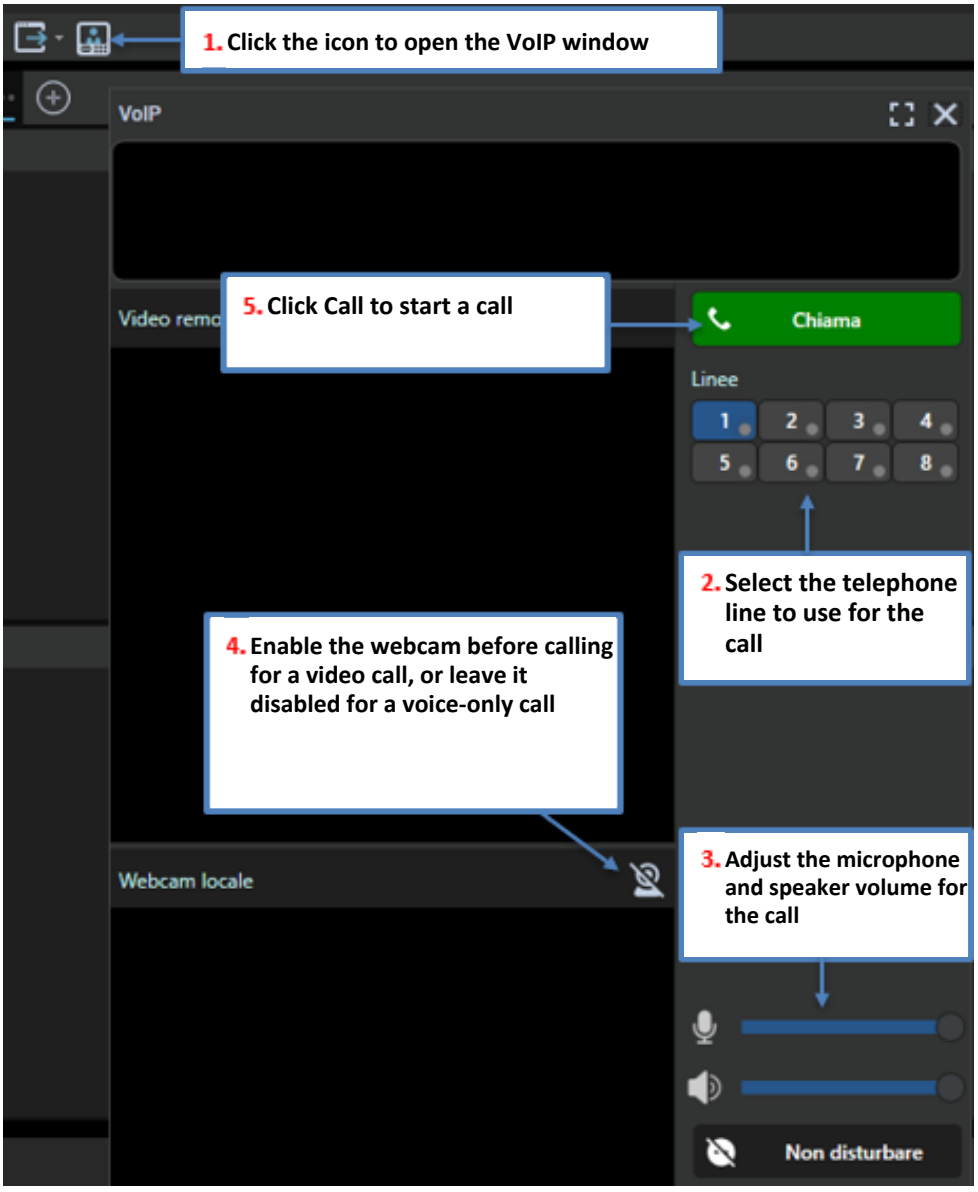
Making a call

VoIP calls in Elkron-ONE can be started in three ways:

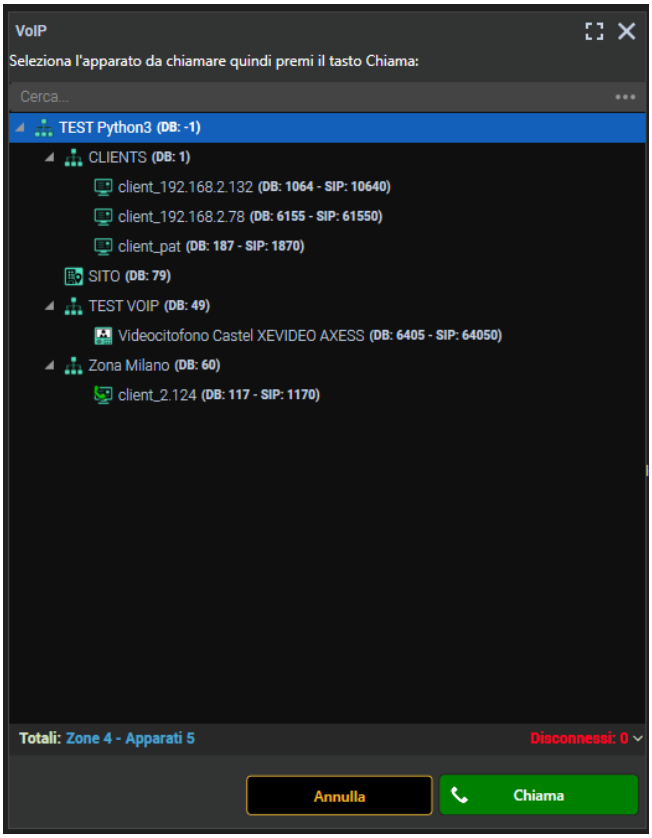
1. from the dedicated **VoIP window;**
2. from the **tree view context menu;**
3. from the **floor plan context menu.**

The 3 methods are described below.

1. ***Calling from the VoIP window***

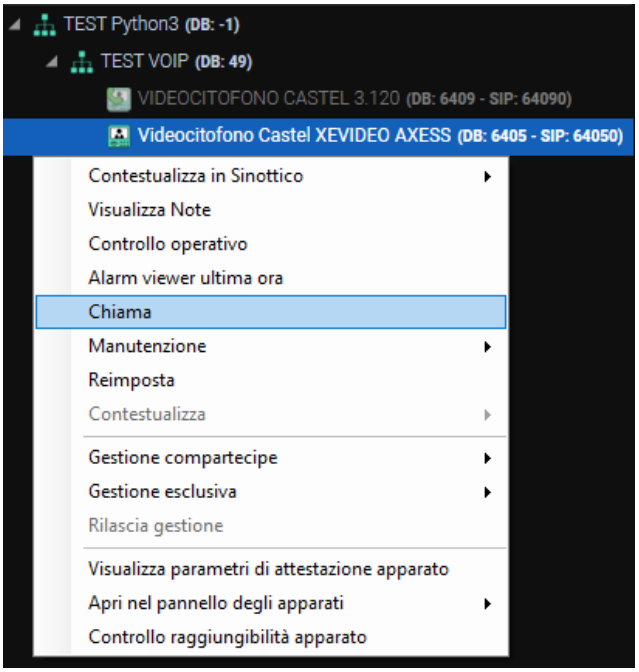


After starting a call from the window, the tree view opens so that a client or VoIP device available to receive calls can be selected:



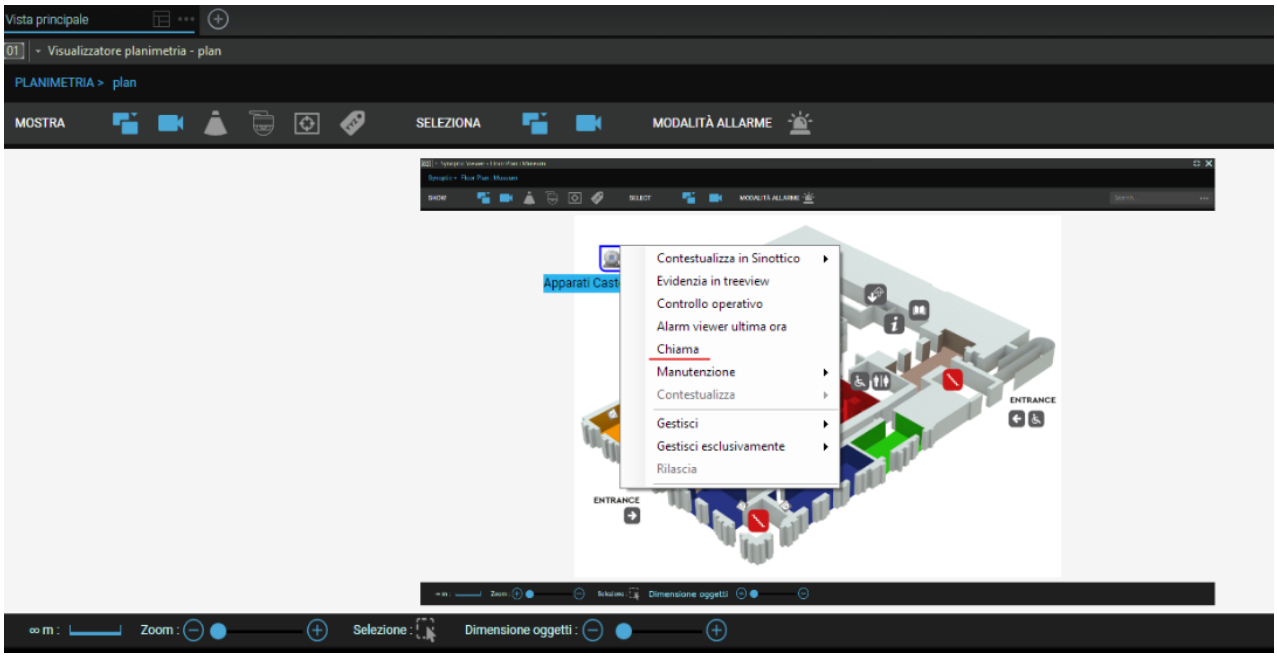
2. ***Calling from the tree view context menu***

The second method is to use *Call* in the tree view. This option appears only for devices supporting VoIP SIP.



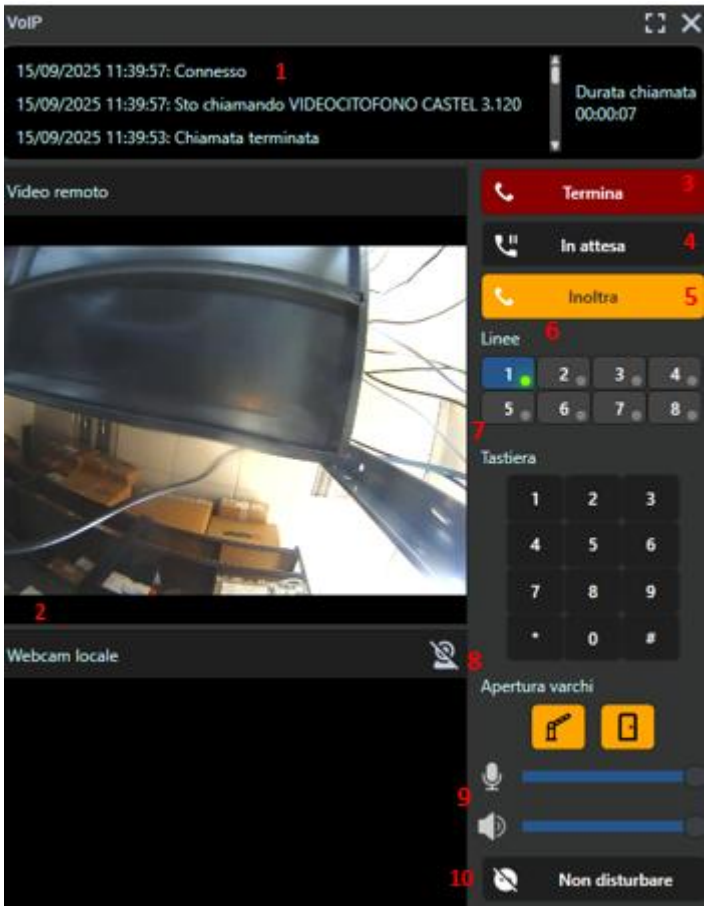
3. Calling from the floor plan context menu

After a VoIP device is added to a floor plan, it can be called directly from its context menu. *Call* appears in the drop-down menu only for VoIP devices.



Call in progress

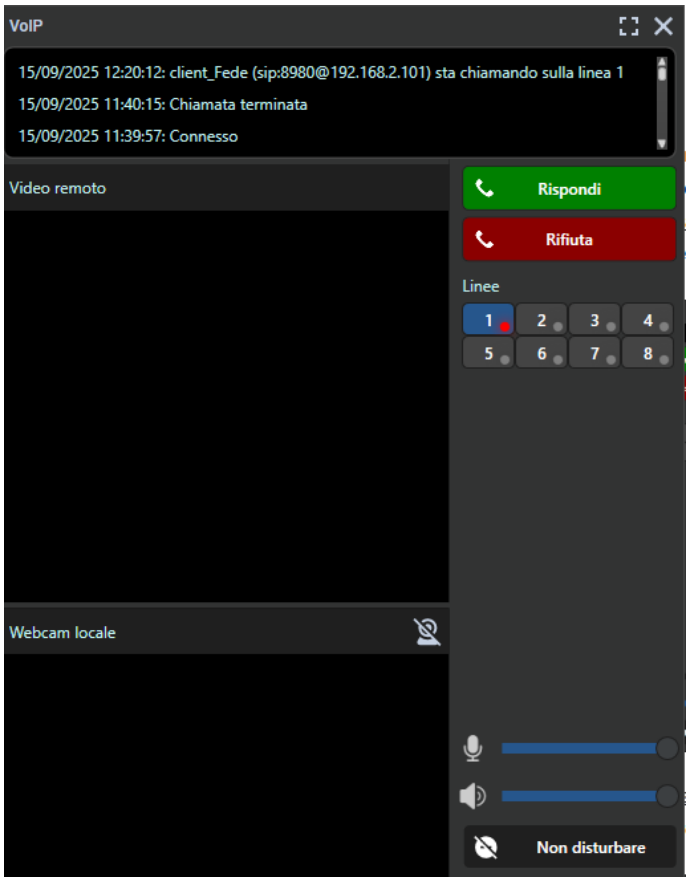
When the called person or VoIP device answers, communication is established and the call-in-progress interface opens:



1. The **status bar** shows the call operation history;
2. The **local webcam and remote video** of call participants;
3. The **End** button terminates a call;
4. The **Hold** button puts a call on hold; to resume it, click the **Resume** button.
5. The **Forward** button forwards the call to a third party;
6. The **eight telephone lines** available for a call;
7. The **keypad** sends DTMF tones to the server, after configuring the actions on the device;
8. **Gate and door release** buttons open the two entrances, if supported and configured on the called device;
9. **Sliders** adjust the microphone and speaker volumes during the call;
10. The **Do Not Disturb** button enables DND to reject all incoming calls.

Managing a call

1. **Answering or rejecting a call:** when a call is received, the VoIP window opens automatically on the called person's client and the ringtone plays. A red LED identifies the line receiving the call. Click *Answer* or *Reject* to answer or reject the call.



2. **Forwarding a call:** after answering or starting a call, it can be forwarded to another user by clicking **Forward.** The tree view opens automatically to select the destination device or Elkron-ONE client. If forwarding succeeds, the current line is released.

Note: An incoming call can always be received on another line during an active call. Switching to that line to answer or reject the incoming call automatically puts the active call on hold. A flashing yellow LED indicates the held line.

Icons

The following table summarises the possible telephone line LED states.

Telephone line LED	Status
	Telephone line available
	Telephone line in use and on hold
	Incoming call on the telephone line
	Active call on the telephone line

The button that opens the VoIP window and the VoIP devices/clients in the tree view also update their icons to reflect the current status. The following table illustrates these states.

VoIP window	VoIP device	Status
		No active call
		Call in progress
		Call on hold
	/	**Do Not Disturb** enabled
/		Ringing

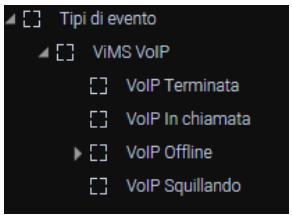
Client settings for the microphone, speaker and webcam

Client Settings includes a section for selecting the audio and video configurations used for VoIP voice and video calls. For details, see *Client Settings.*

VoIP event reception and server logging

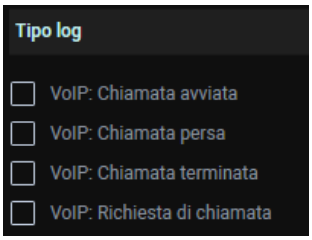
The server generates the following events and logs for Elkron-ONE VoIP operations. Events are generated when:

- a VoIP device goes online or offline on Asterisk;
- a device rings, is in a call or ends a call.



Logs are generated for:

- a call being started and the originating user, for Elkron-ONE clients;
- a call ending, including its duration;
- a call being accepted;
- a missed call.



Part III ADMINISTRATION

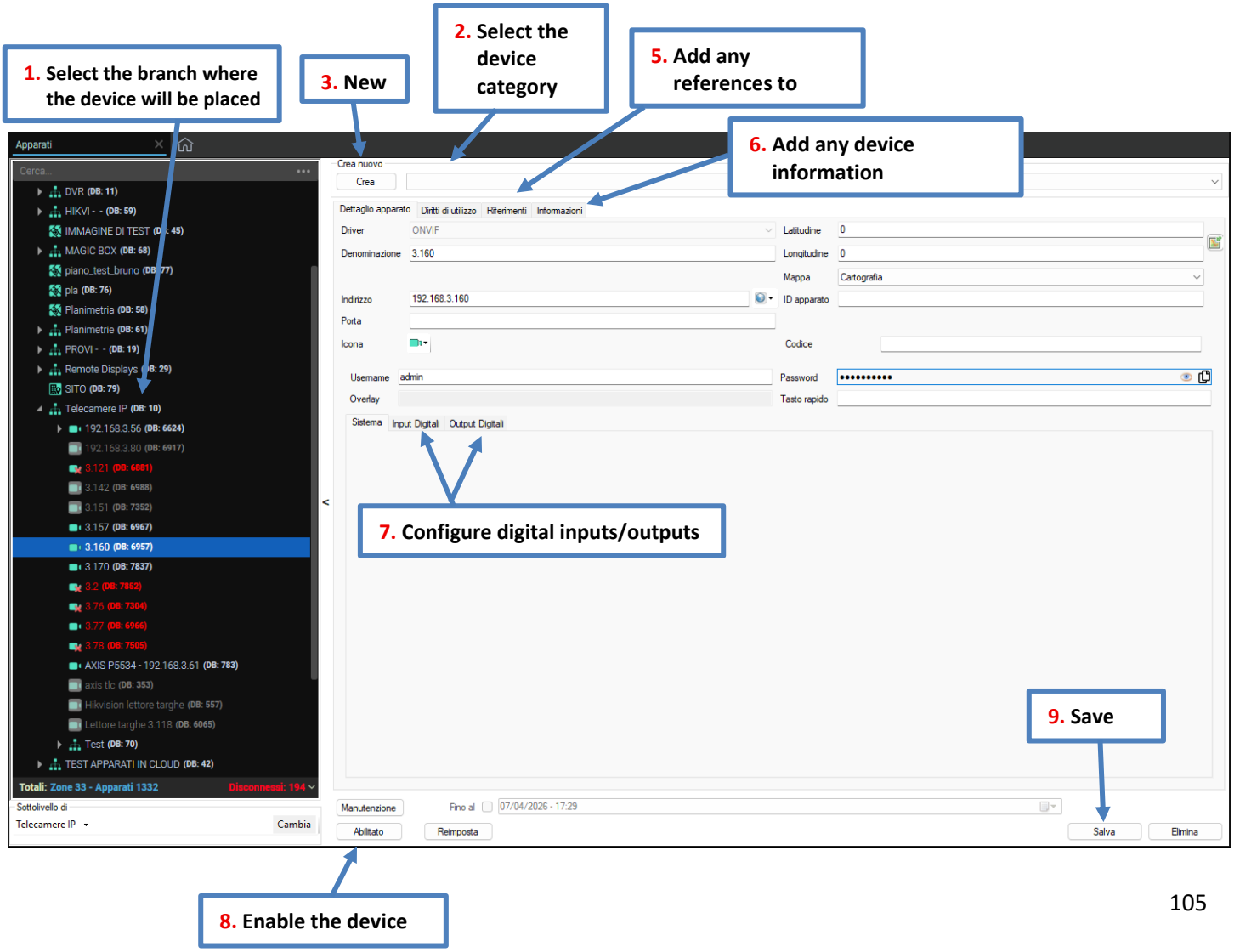
DEVICE MANAGEMENT

Elkron-ONE includes a dedicated module for adding devices to the system and configuring their operation.



Configuring a device

The image shows how to configure a device. The parameters described depend on the driver hardware characteristics and the functions supported by the device.

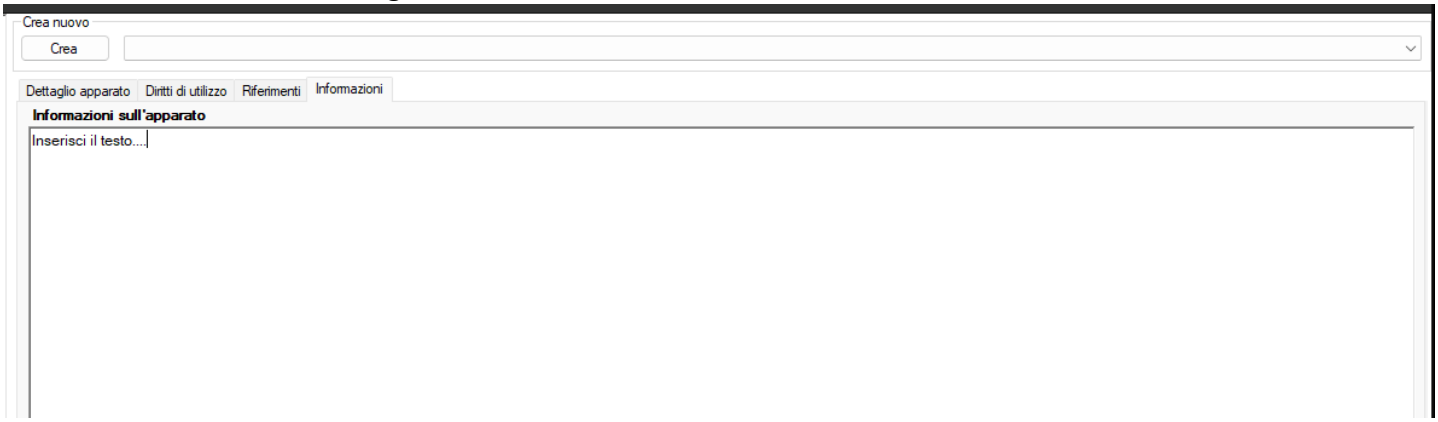


4. Device details:

- **Driver:** device type *(mandatory).*
- **Name:** the name assigned to the device *(mandatory).*
- **Address:** the IP address assigned to the detector *(mandatory).*
- **Port:** the connection port number.
- **Device ID:** assigns an identifier to the device.
- **Icon:** assigns an icon to the device.
- **Code:** an additional identifier for classifying devices in the tree view.
- **Username and Password:** the device access credentials.
- **Shortcut key:** manages the device using the keyboard.
- **Automatically record transmitted video:** enables automatic video stream recording.

- **Latitude and Longitude:** if these fields are blank, the system automatically enters zero. To enter latitude and longitude values instead,
  hold down Ctrl and click the device's intended position on the map.
  The system stores the latitude and longitude values. In the Device Management panel, click this button  to insert the stored coordinates automatically. Alternatively, enter the longitude and latitude manually.

5. Information: the image shows how to add device information.



8. Digital inputs/outputs

Examples of digital inputs:

- **Tamper:** enclosure open;
- **Power:** electrical connection lost;
- **Temperature:** critical temperature levels.

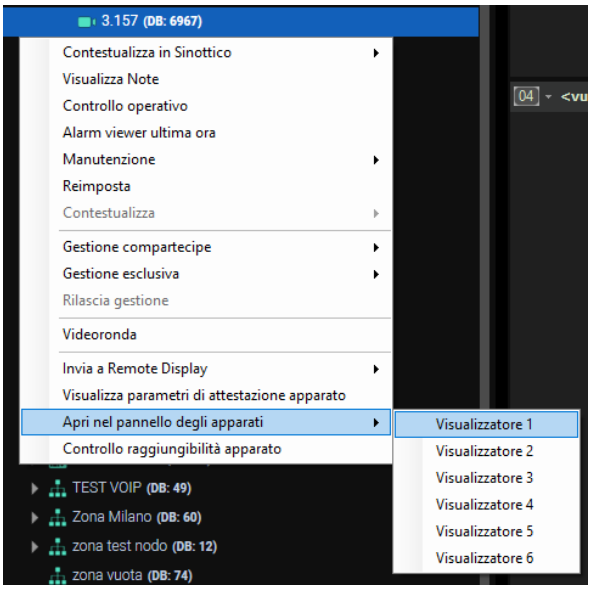
Input and *output* labels can be renamed for all devices, including disabled devices.

9. Enable/disable a device: disabled devices are shown in grey

in the tree view.  The management operations available for active devices cannot be performed on them, but data acquired while they were operational can still be viewed. For unreachable devices, the system shows  the date from which the device has been unavailable and the reason.

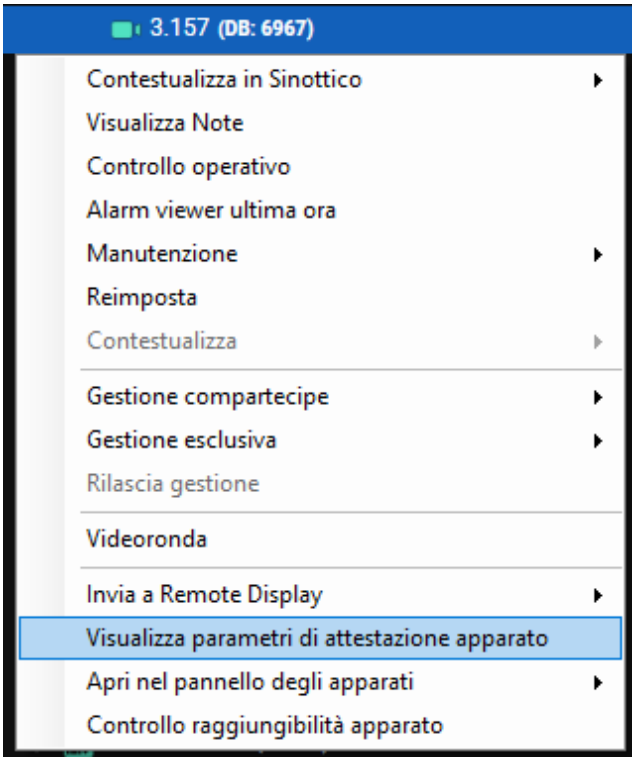


A device's configuration can also be opened directly without using the Administration panel. Select “Open in Device Panel”, available to all administrators and users with Device Management permission.



Viewing device connection parameters

Users who do not manage devices can still view a device's connection parameters using “View Device Connection Parameters” in the tree view context menu. This option is enabled for users with Device Management permission and/or *permission to view device technical information.*

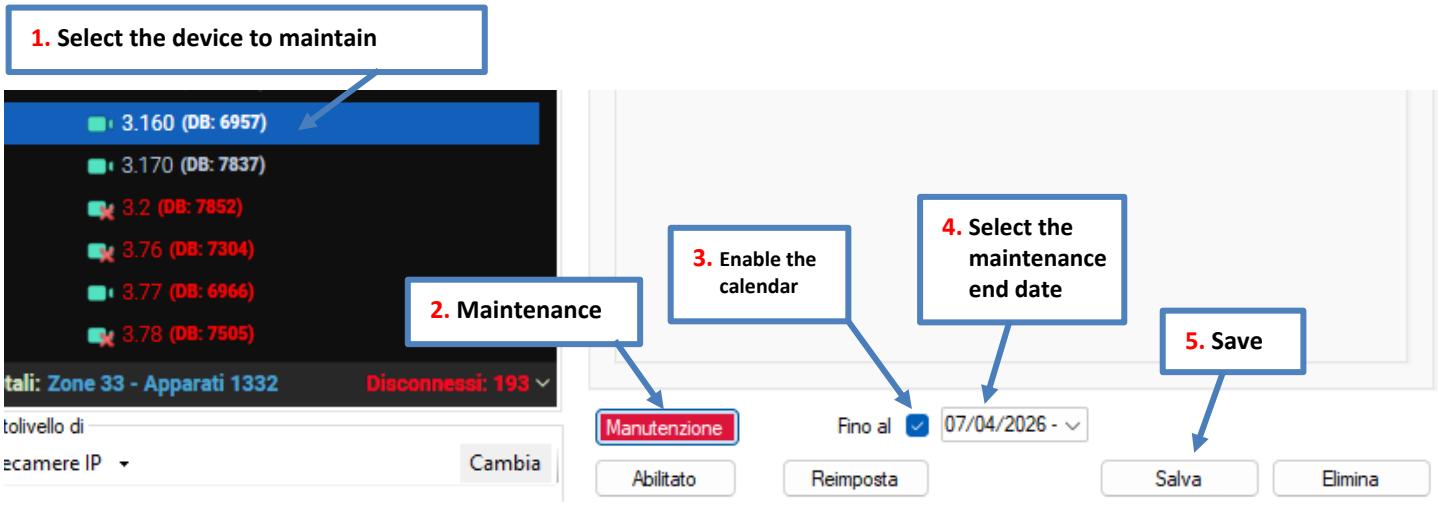


Selecting the option opens a pop-up showing the device's technical information:



Placing a device under maintenance

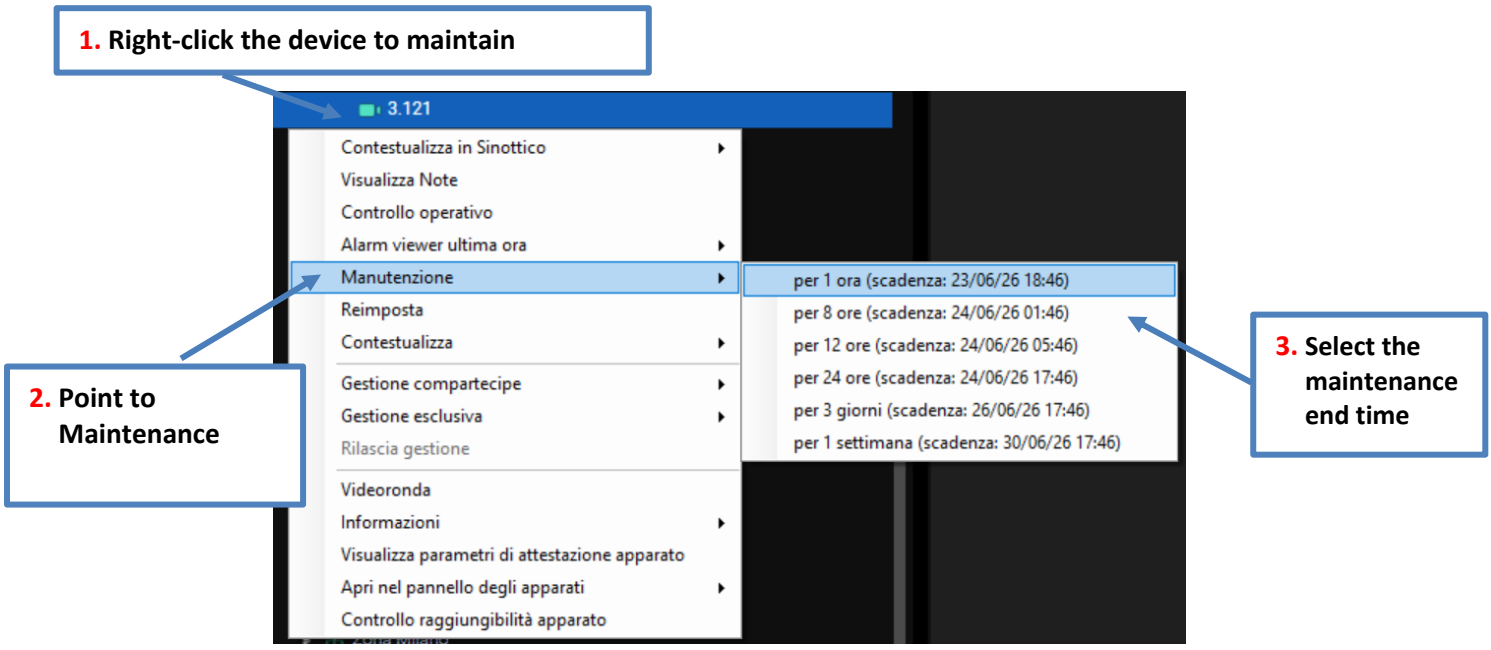
The image shows how to mark a device as under maintenance.



Devices under maintenance are identified in the tree view by this icon . After maintenance expires, the system automatically marks the device as available again. If the device becomes available before the scheduled date, the operator can make it available manually using the red **Maintenance** button, followed by **Save.**

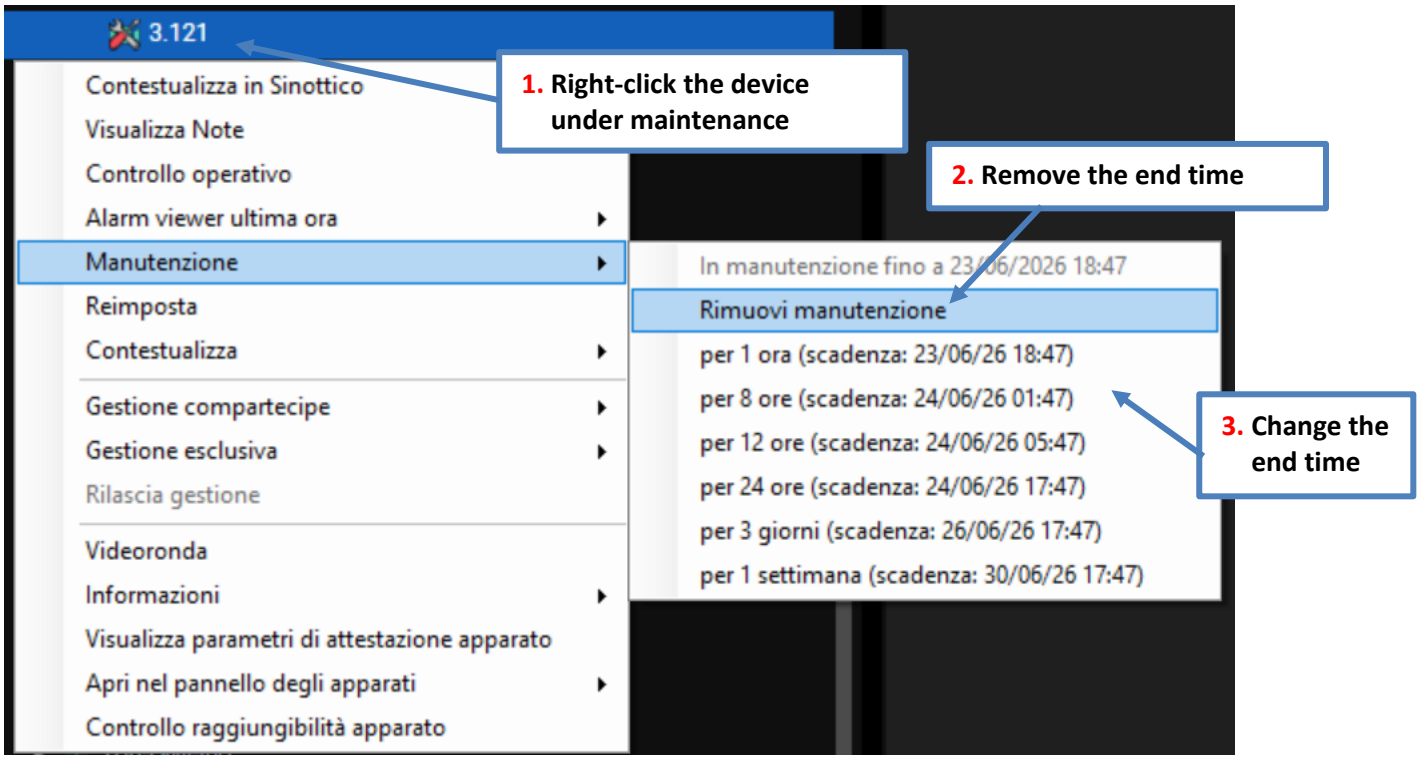
A device can also be placed under maintenance from the tree view:

1. **Right-click the device to maintain in the tree view**
2. Point to **Maintenance**
3. Select the **device maintenance period**



Once a device is under maintenance, you can:

1. **View the previously set end time**
2. **Remove the previously set end time**
3. **Change the end time**



Maintenance can also be applied to individual sublevels, such as channels or detectors, using the methods described above.

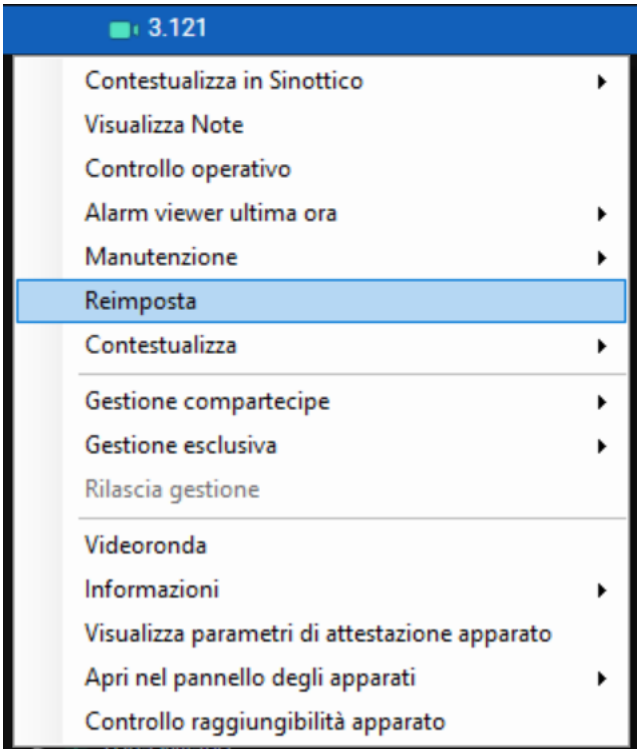
Note: To set maintenance from the tree view, the user needs *Device Management* permission and/or *permission to place a device under maintenance.*

Resetting a device

The image shows how to refresh the device settings, for example when channels are added to an existing device or other changes are made on the device.

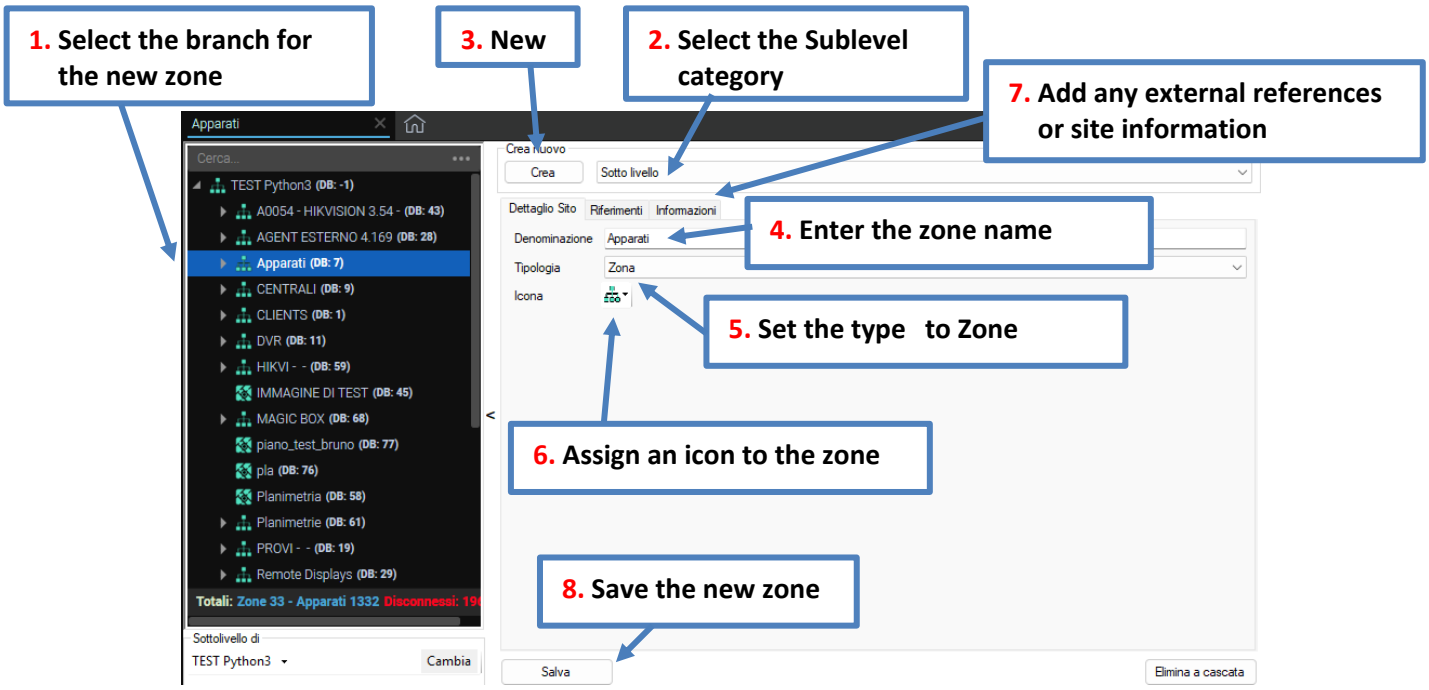


A device can be reset directly using Reset in the tree view. This option is enabled for users with *Device Management* permission and/or *permission to send the Reset command to devices* from the tree view.



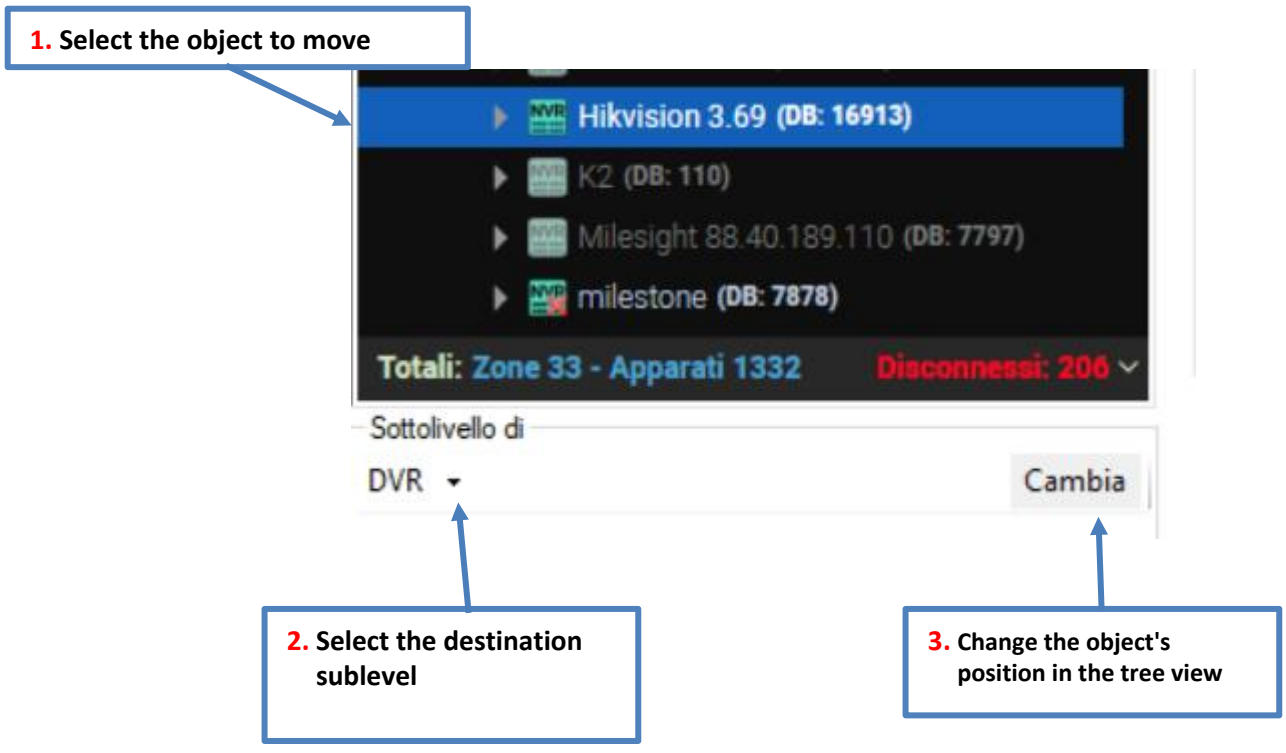
Configuring a zone

The image shows how to add a zone to the Elkron-ONE tree view:



Moving objects in the tree view

The image shows how to move a device or zone in the tree view.



Deleting objects from the tree view

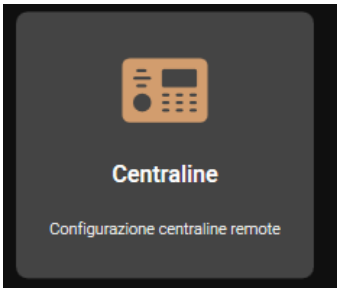
The two images show how to delete a zone together with all its devices and sublevels, or delete an individual device.





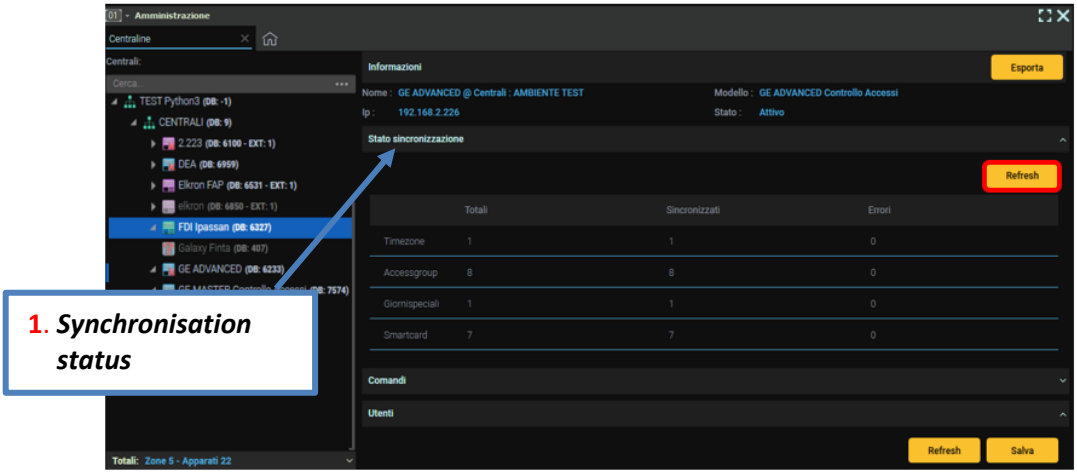
CONTROL PANELS

Elkron-ONE includes a section, accessible from the administration panel, for viewing control panel information and managing its operation.

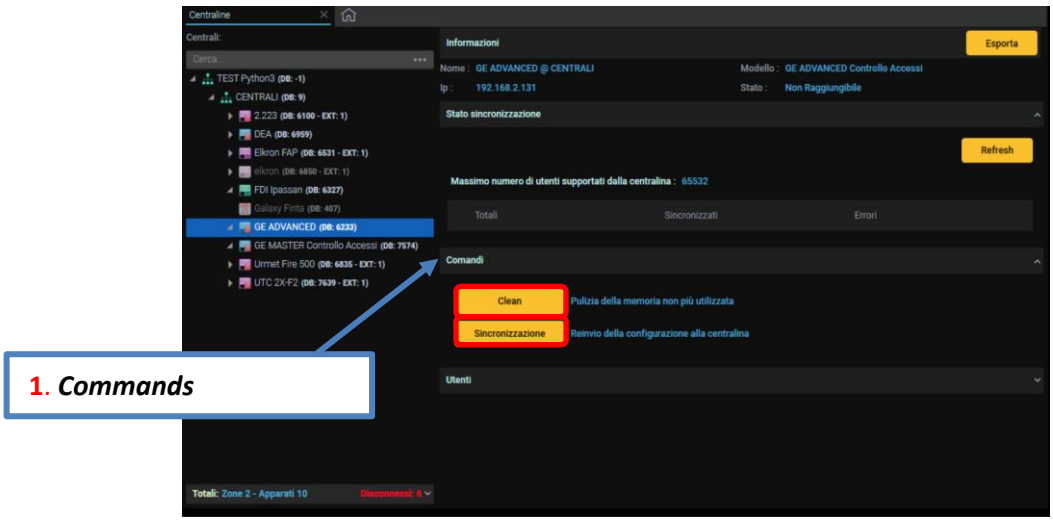


Select a device in the tree view to display the control panel's name, IP address, model and status. Depending on its type and supported functions, remote commands can be sent to the control panel and its users can be managed:

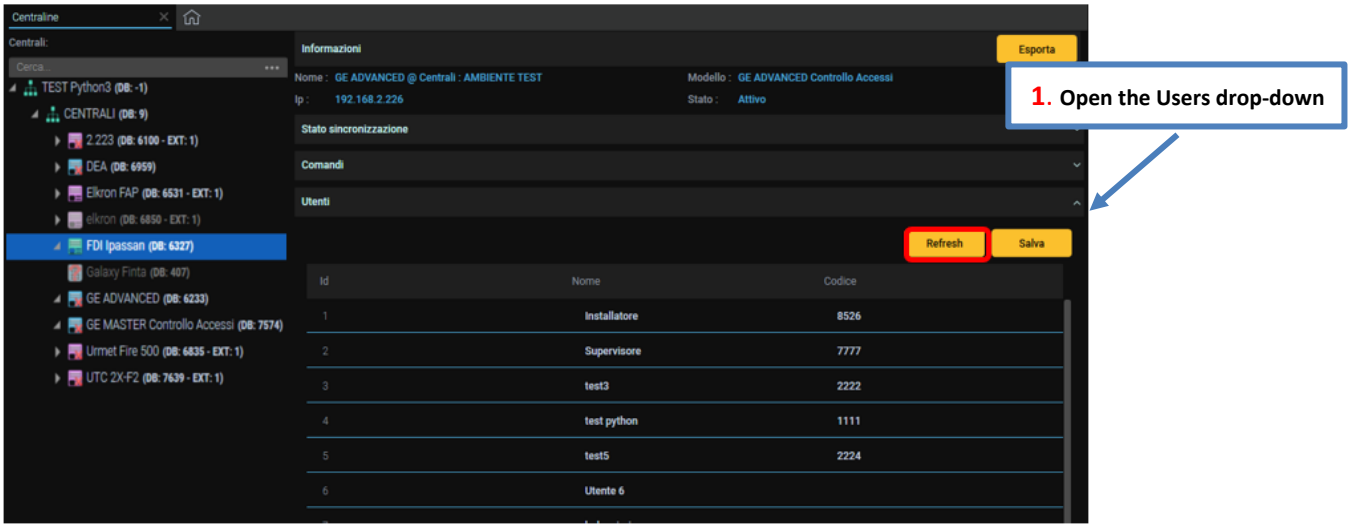
- **Refresh:** updates the synchronisation status between the control panel and Elkron-ONE.



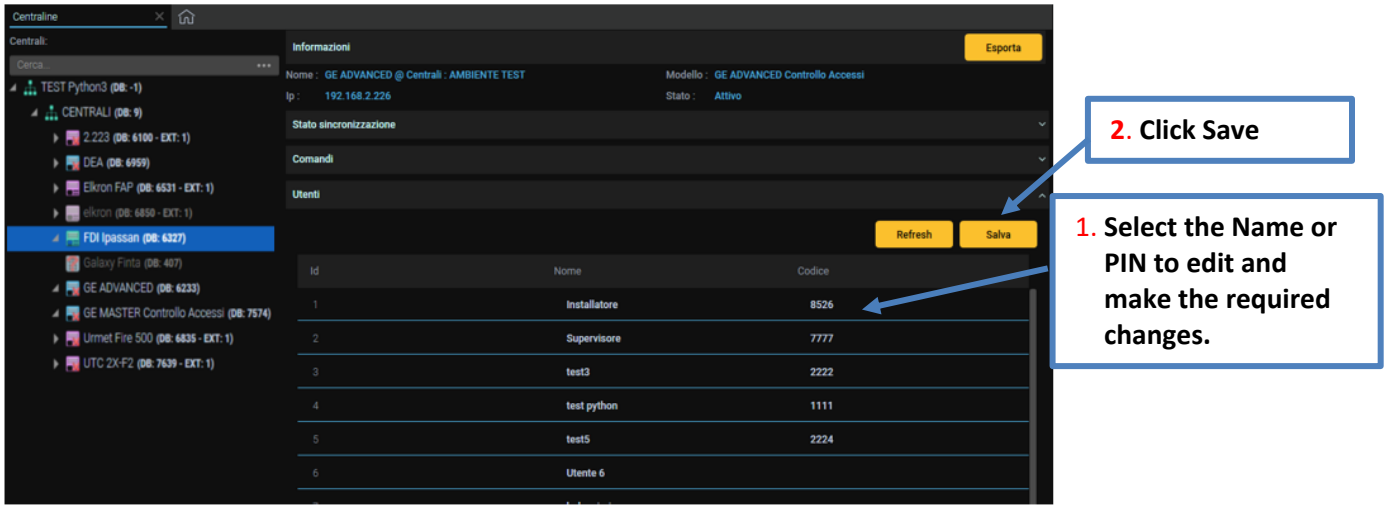
- **Clean:** frees unused memory on the control panel.
- **Synchronisation:** resends the configuration to the control panel.



- **Refresh:** updates/requests the control panel user list.

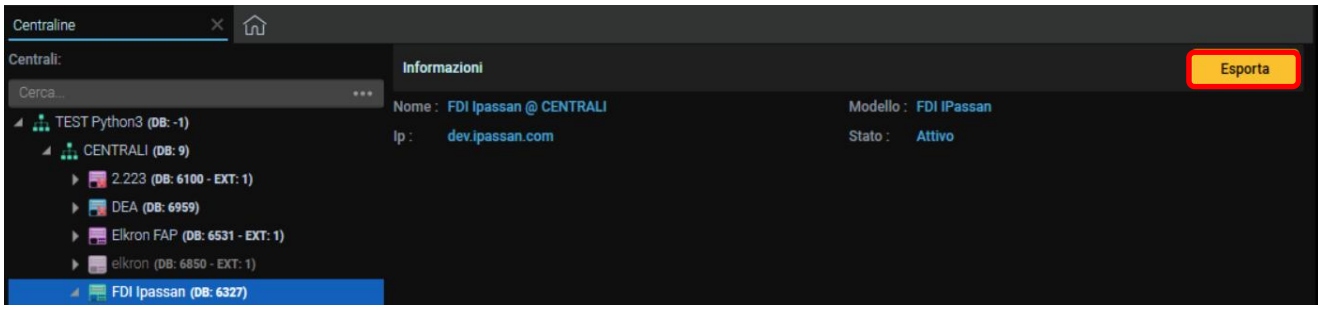


- **Edit a user:** select the user to edit and save the changes.



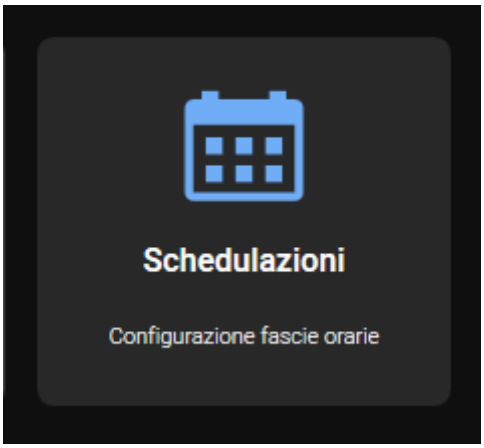
Note: Changing the Installer PIN, generally used to connect the control panel, may require its corresponding credentials to be updated in Device Management.

- **Export:** copies control panel information and its user list, if available, to the PC clipboard for pasting into a text file.

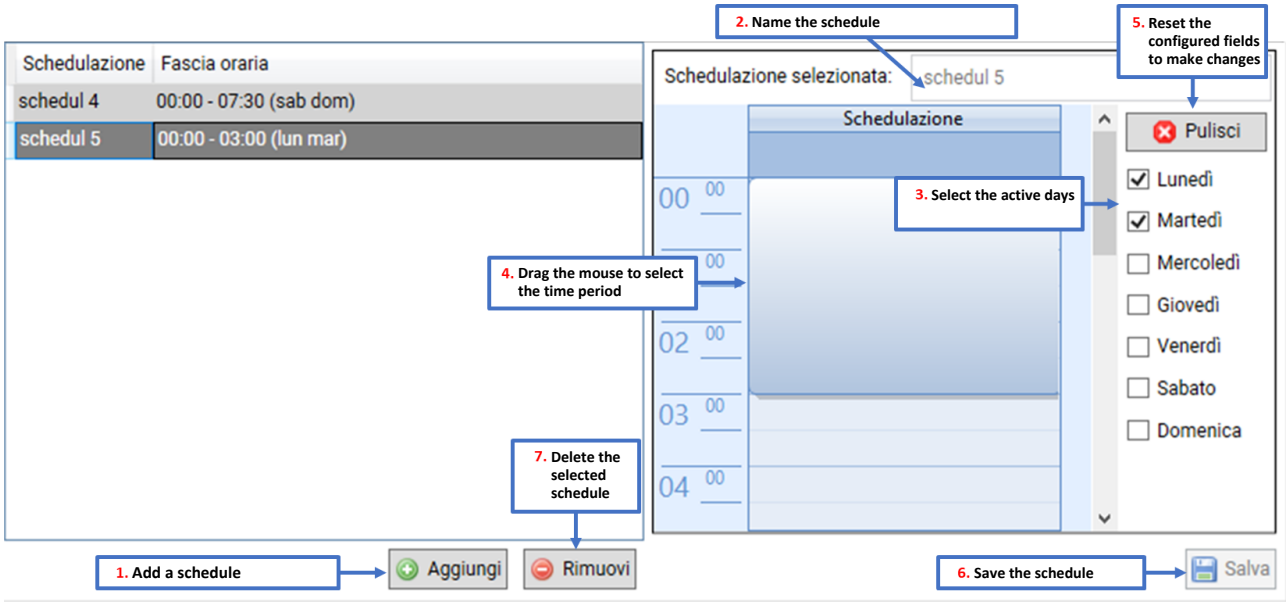


SCHEDULES

Elkron-ONE includes a section for configuring time periods.
These time periods schedule camera processes,
such as starting recording at a specific time of day.

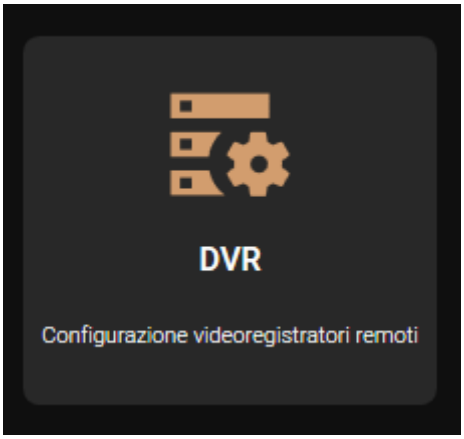


The image shows how to configure a time period.

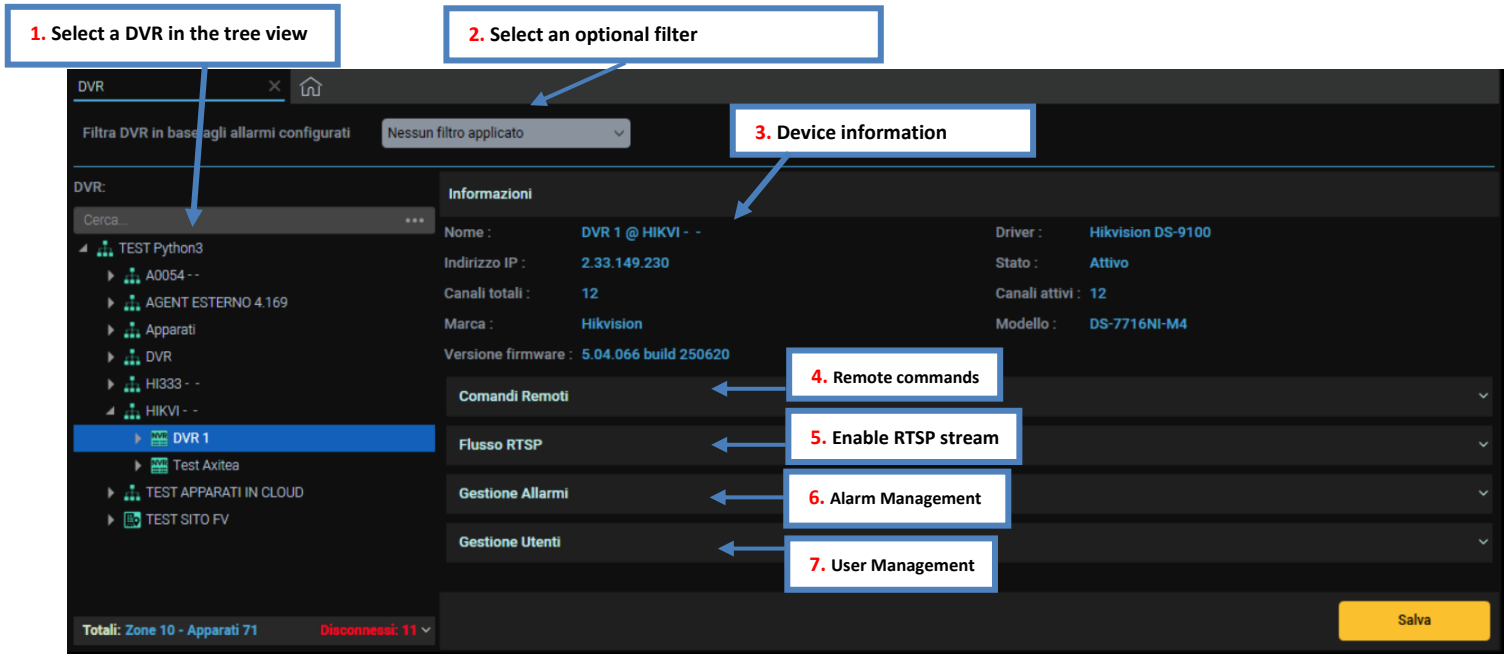


DVR MANAGEMENT

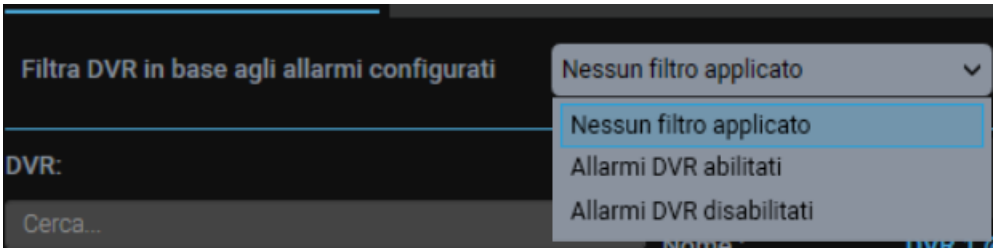
Elkron-ONE provides full management of DVR devices, remote commands, alarms and users with access to device recordings.



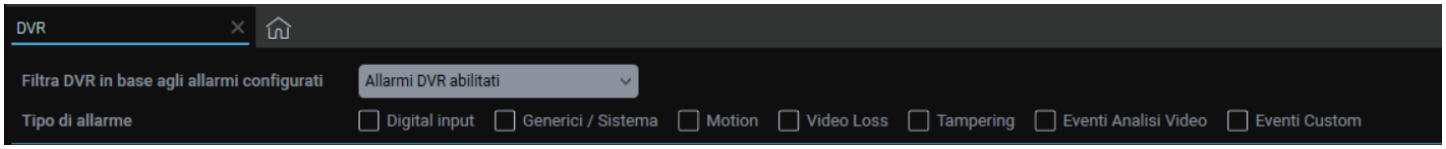
The tree view displays all DVRs connected to the system. Select a DVR to view its details and access the operations described below:



2. **FILTER DVRs BY CONFIGURED ALARMS:** filter DVRs by their alarm status, enabled or disabled, using the corresponding filter in the drop-down menu.



Selecting the *DVR Alarms Enabled* filter also allows DVRs to be searched by active alarm category.

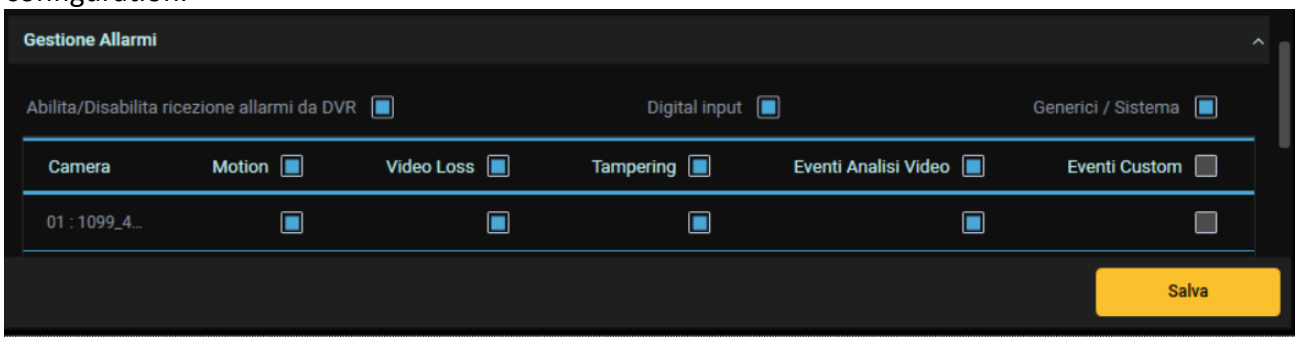


3. **INFORMATION:** displays the selected DVR's name and zone, model, IP address, total and active; status.

4. **REMOTE COMMANDS**
   a) **Set NTP:** synchronises the device time with the server. b) **Restart:** restarts the device, interrupting all recording transfers to the server and all live video views. c) **Shut Down:** switches off the device.

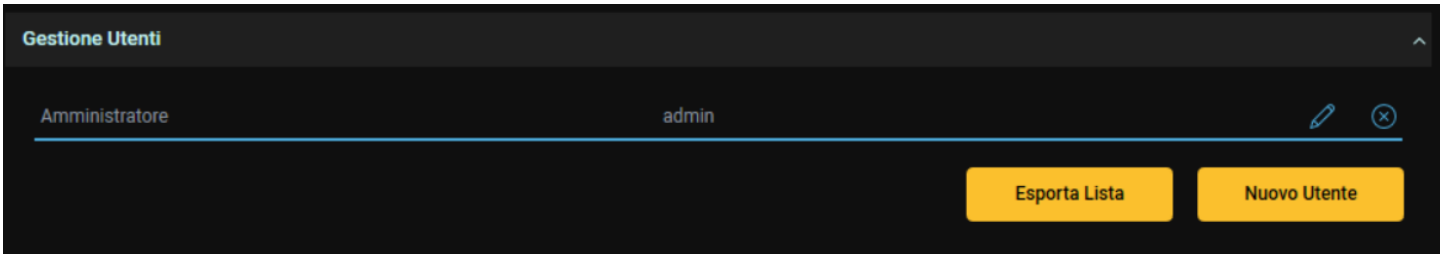
5. **RTSP STREAM:** select the checkbox to view live video through the RTSP stream.

6. **ALARM MANAGEMENT:** to enable or disable specific DVR alarms, for Digital Input and/or General System reports, select the relevant checkboxes and save the configuration.



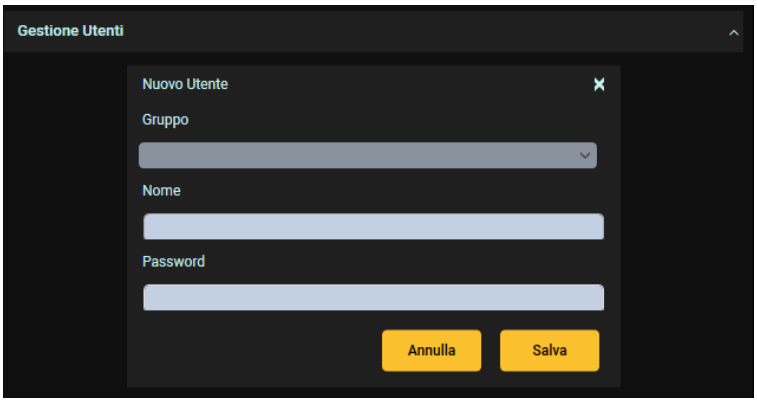
7. **USER MANAGEMENT:** displays users with access to recordings from the selected DVR. Users are listed by Name and assigned Group.

Four buttons are available for the corresponding actions.



a. **Export List:** copies the table to the system clipboard. b. The data can then be pasted into external applications (CTRL+V). c. **New User:** adds a user by entering

group, name and password.

d. 

e. **Change Password:** changes the selected user's password. f. **Delete User:** deletes the selected user.

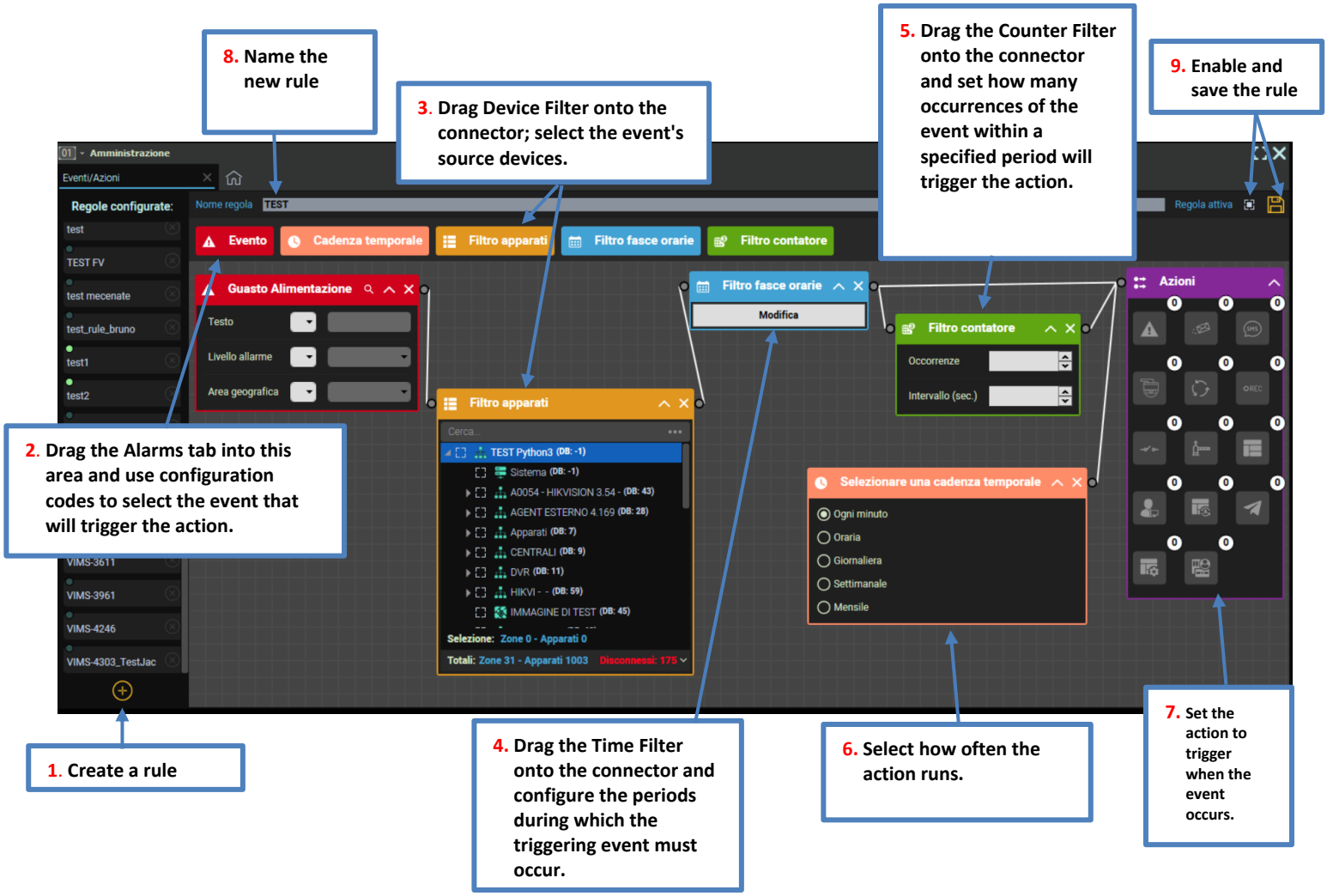
EVENTS – ACTIONS

Elkron-ONE includes a module for configuring operating rules that trigger one or more actions when a specific event occurs, either directly or subject to defined conditions. For example, a motion event from a particular camera during a specified time period can cause the system to send an alert, an SMS to selected operators, an email, or several actions together.



Creating a rule

The image shows how to configure a new rule.



Configure Event: after the event type is selected, the Alarms tab connects automatically to the Actions tab through the grey connector, creating a direct condition. Refine the alarm type using the following codes.

=	Equal to
!=	Unequal
C	Contains
!C	Does not contain

2.4. 5. Configure Filters: place filters on the connector line so that they are inserted automatically into the flow. To delete a connection, double-click the connector to highlight it in blue, then press Delete. To create a connection, drag the mouse from one green dot to the other.

6. Configure Action: several actions can be triggered by the defined event. Each action can be configured from scratch or selected from existing actions. If no name is assigned, the system names the rule sequentially by default, for example ALLARME1, ALLARME2, etc.

- **Generate alarms:** displays the alarm on the *High Priority* tab as an *Automatic Event.*
- **Send email:** email addresses are configured in *User Management* records.
- **Send SMS:** mobile numbers are configured in *User Management* records.
- **Move camera to a configured PTZ preset:** presets are configured in *Camera Configuration.*
- **Activate a configured Guard Tour:** guard tours are configured in *Camera Configuration.*

- **Record streams from video devices:** IP cameras whose recording is to be started/stopped must be set to *External Request* in *Camera Configuration.*
- **Activate a digital output:** digital outputs are configured in *Device Management.*
- **Execute remote device commands:** available commands depend on the selected device type.

- **Open a configured client layout:** layouts are configured in *Configured Layout Management.*
- **Open a configured device on clients:** select individual recipients or user groups for whom the selected camera view will open when the event occurs.
- **Open an automatic layout:** select recipients or user groups for one of these video behaviours: *Go to Live, Go to Alarm Date,* or *Go to Alarm Date Minus N Seconds.*

- **Send a Telegram message:** configure event messages by entering the details in the Telegram section of AdminWeb. For more information, see the guide *"Telegram - Integration in Elkron-ONE for Receiving*

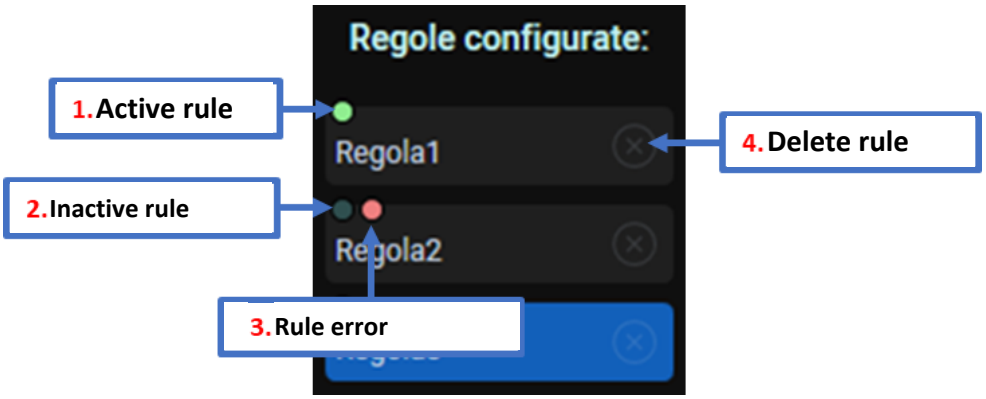
Events”.

- **Open a configured automatic layout:** select recipients or user groups for a layout containing one or more of the following: video from devices whose viewing cones cover the alarm point; live streams from devices in the detector's zone; live video from the device that generated the event; the overview containing the detector; the device's Info Viewer; and its AlarmViewer in Real Time or Received Alarm mode.

- **Manage device control:** select one or more devices to place under exclusive, shared or shared control by a user group, for a fixed or indefinite period.

Managing configured rules

The image shows the status of configured rules and how to delete them. A rule error may occur, for example, if its devices have been deleted.



USER ACCOUNTS

Elkron-ONE provides flexible user profile management for assigning the available functions to users.

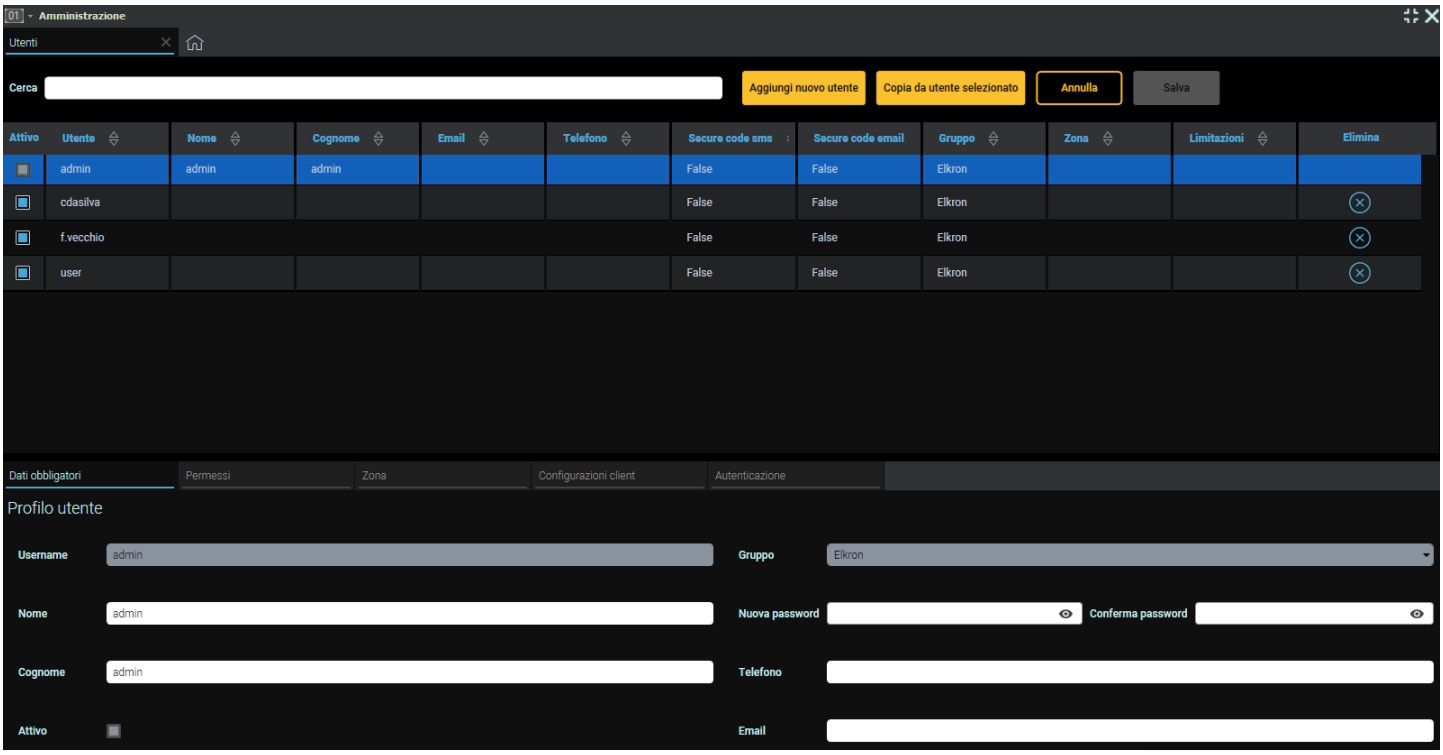
These operations are available in the Users section of the administration panel:



USER MANAGEMENT

Creating a user

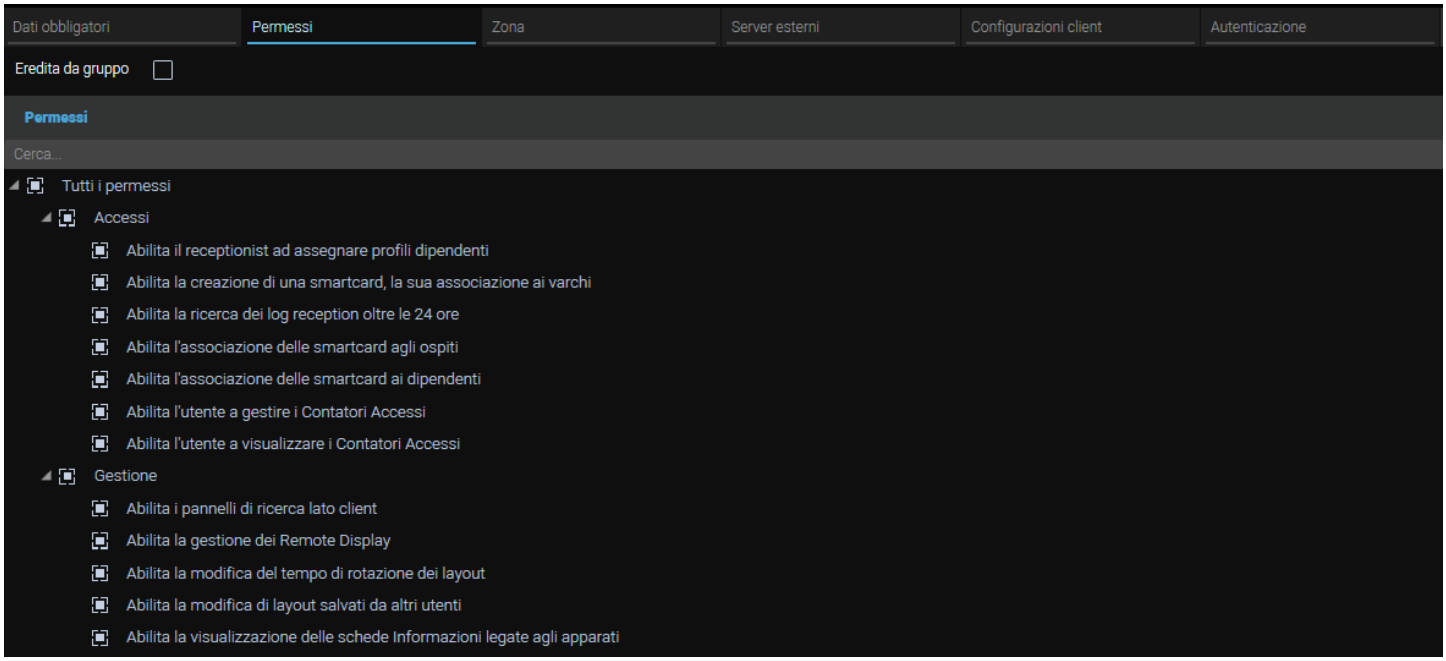
The image shows how to create a user. Steps 6, 7, 8 and 9 are optional.



1. **Account details:** Username, Password and Group are mandatory. Select a group from existing groups or create a new one (see **User Group Management).** Assigning

a group gives the user all that group's attributes, such as permissions and zones, etc.

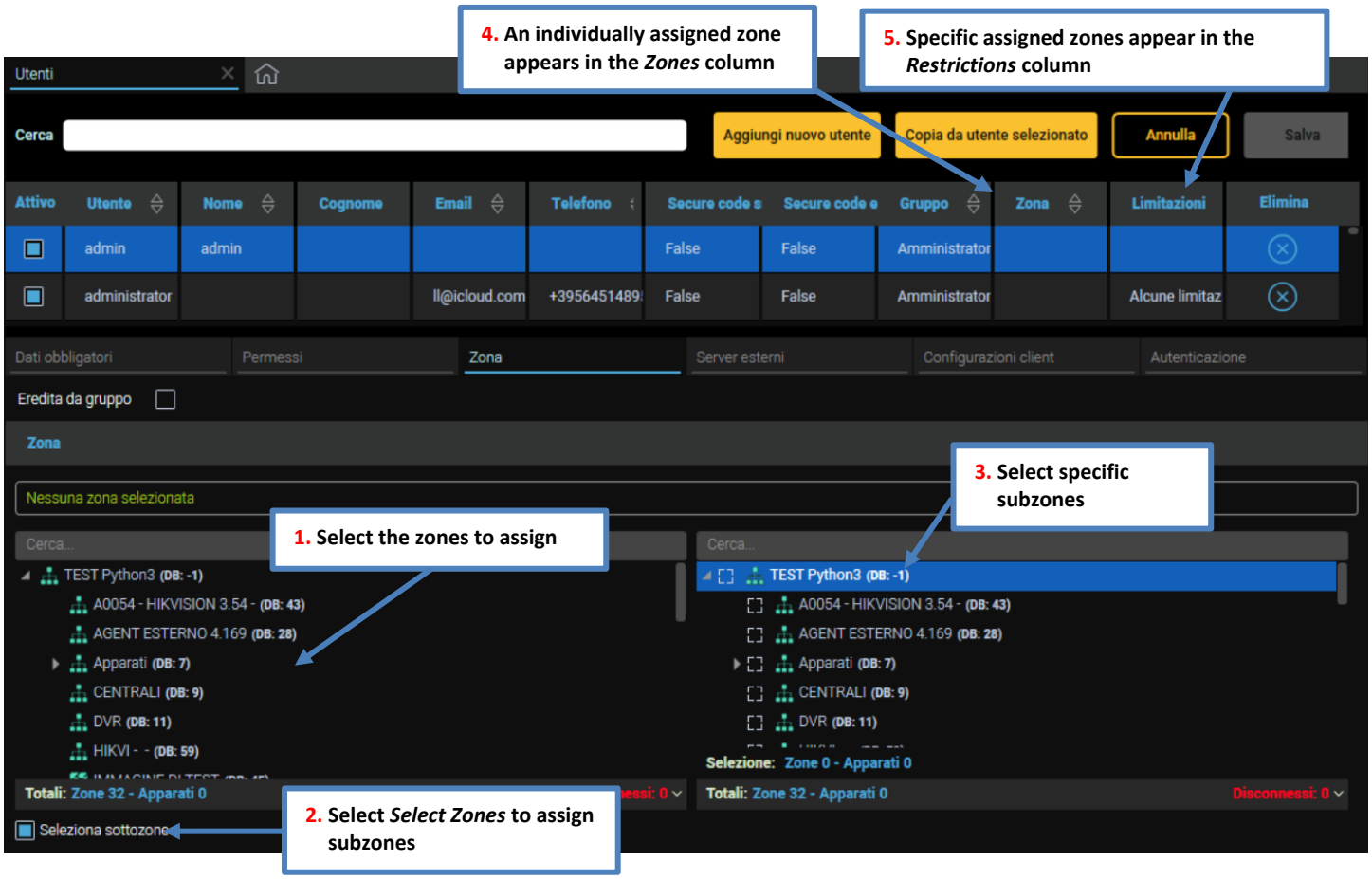
2. **Permissions:** select those to enable for the user or select Inherit from Group to acquire them automatically from the assigned group.



The appendix explains the access granted by individual permissions.

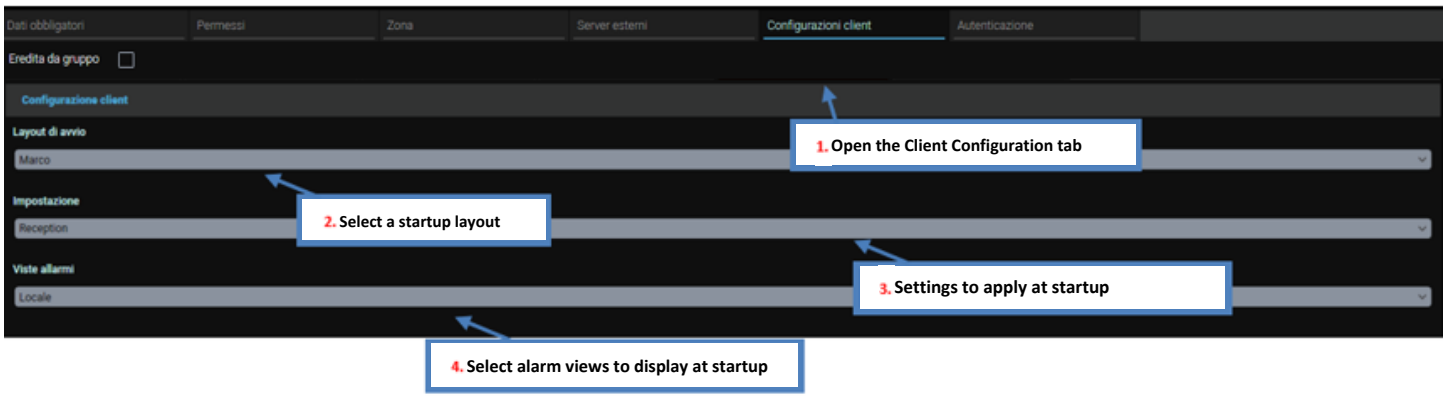
Note: View Local Blacklist and Add/Edit Local Blacklist can be enabled only together with *Show Licence Plate Passage Alarms.* Therefore, Show Licence Plate Passage Alarms can be disabled only after Add/Edit Local Blacklist and View Local Blacklist have been disabled.

3. **Zones:** the user sees only the assigned zone or zones and the devices they contain. Viewing zones can also be inherited directly from the assigned group by enabling the corresponding checkbox. The image shows how to assign zones to the new user.



4. **Client configurations:** the image shows how to assign a specific client configuration to the user, defining the startup layout, settings and alarm views displayed after login. Client configurations can also be inherited directly from the user's group by enabling the corresponding checkbox.

Startup layouts include only global layouts, shared layouts and layouts belonging to the user's group.



Note: Managing layouts requires the Allow Managing Layouts permission. Without it, users can only view the layout tree and activate shared layouts.

5. **Authentication:** binds the user account to the IP address of the user's computer.

Existing user details can be edited, deleted or copied.

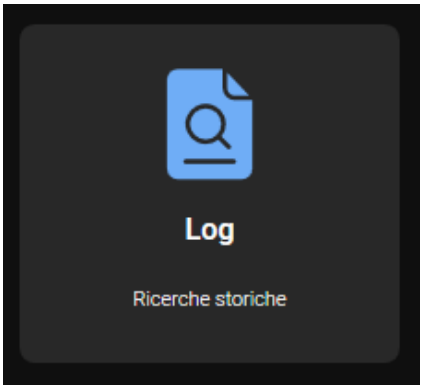
- To **edit** a user, select the account, make changes and save. If the affected user is logged in, one of these messages appears:
  - ✓ **User Disabled:** the account has been deactivated and can no longer access the system.
  - ✓ **User Permissions Changed:** the user's permissions have changed.

In all cases, the user is disconnected from the system. Log in again to regain access.

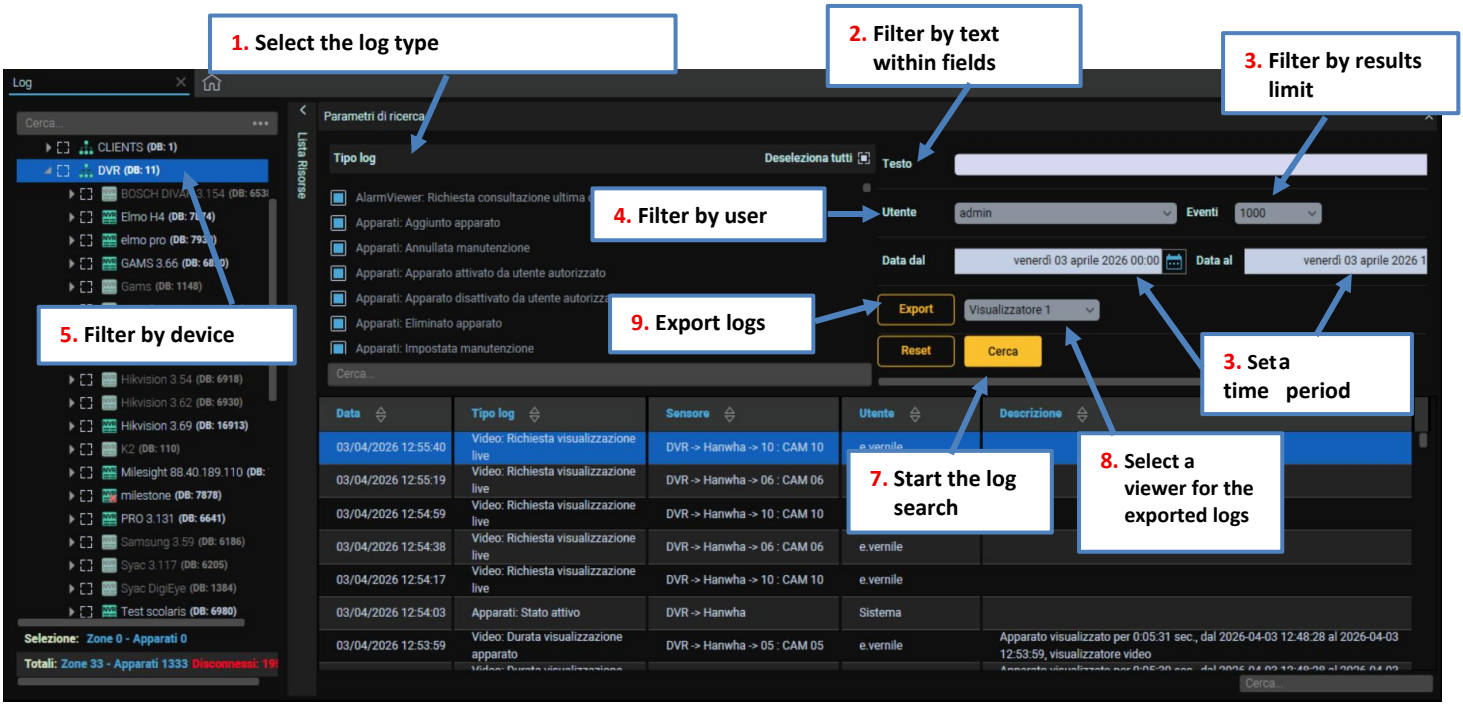
- To **delete** a user, click the red x  and confirm.
- To **copy** details from an existing account, select the source user and click Copy from Selected User.

LOG MANAGEMENT

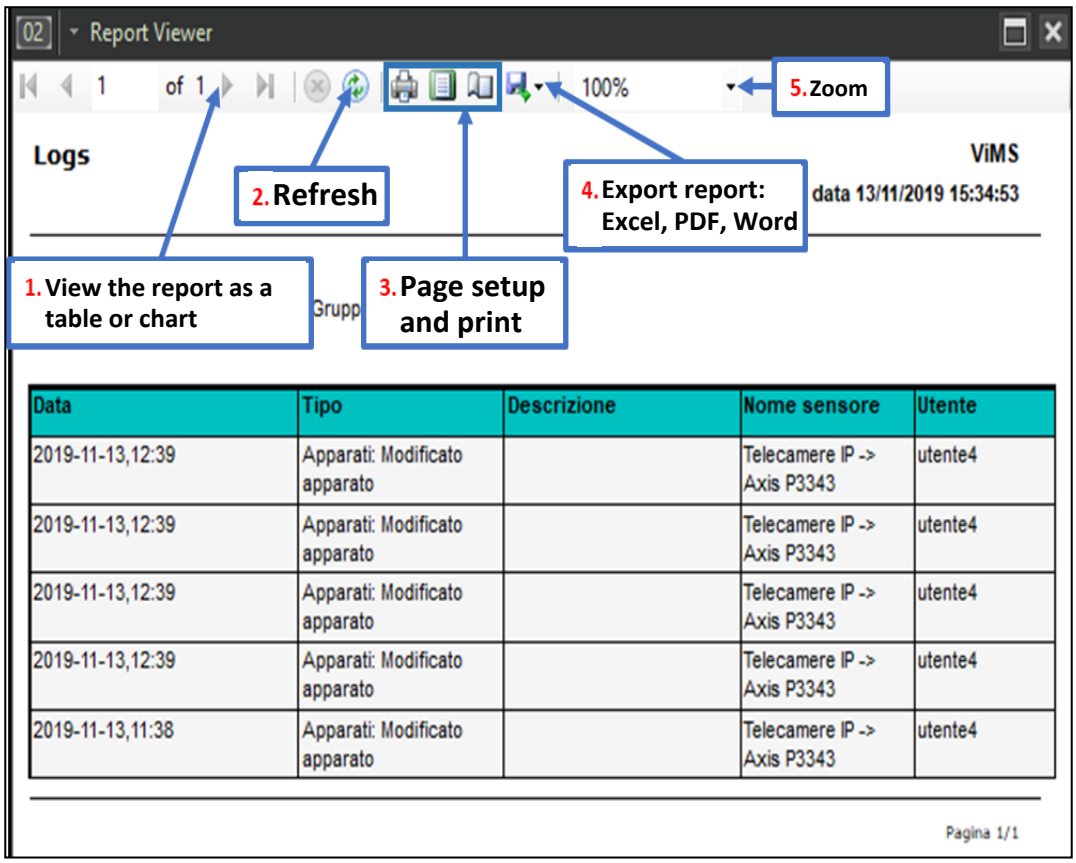
Users can view a chronological record of all activities performed while using and managing the system. Open the administration panel and select Logs:



Start a search directly to view the most recent 100 logs for the current day, or use filters to find specific logs. The image shows how to search logs and export the results as a report.



The report viewer provides controls to display charts, zoom, print and export reports.

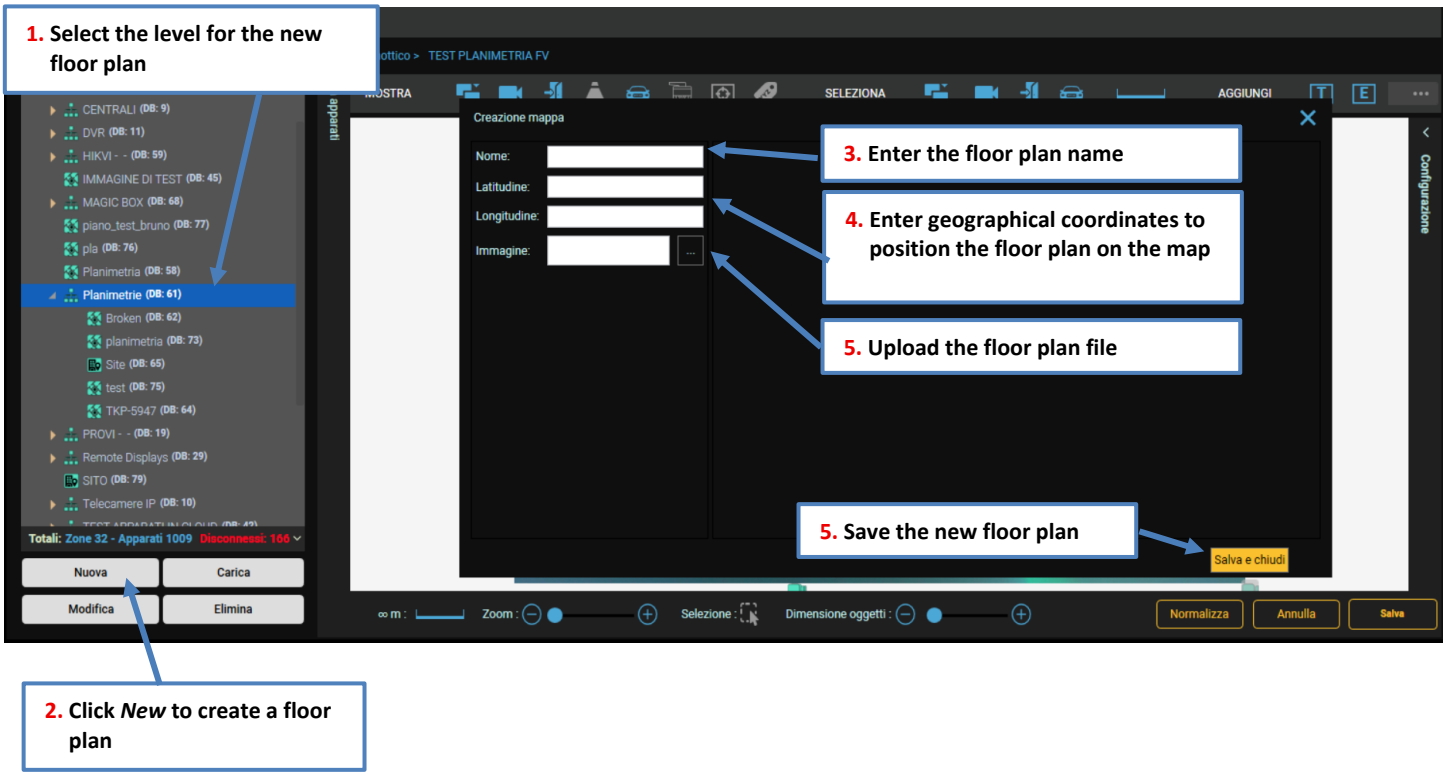


FLOOR PLAN AND SITE MANAGEMENT

Floor plan and site management is reserved for administrators. It includes creating floor plans, editing sites with an associated image, configuring devices within them, and editing or deleting existing floor plans. Open the administration panel and select Floor Plans.

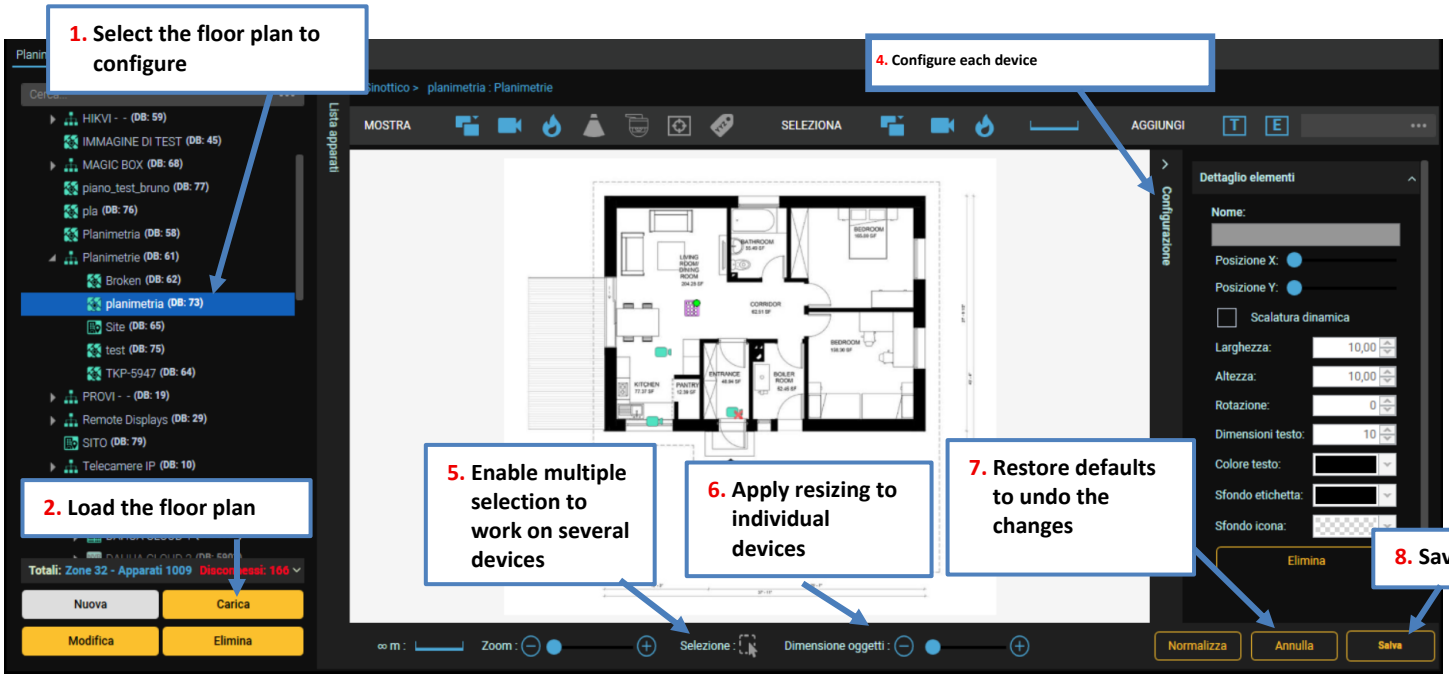


Creating a floor plan



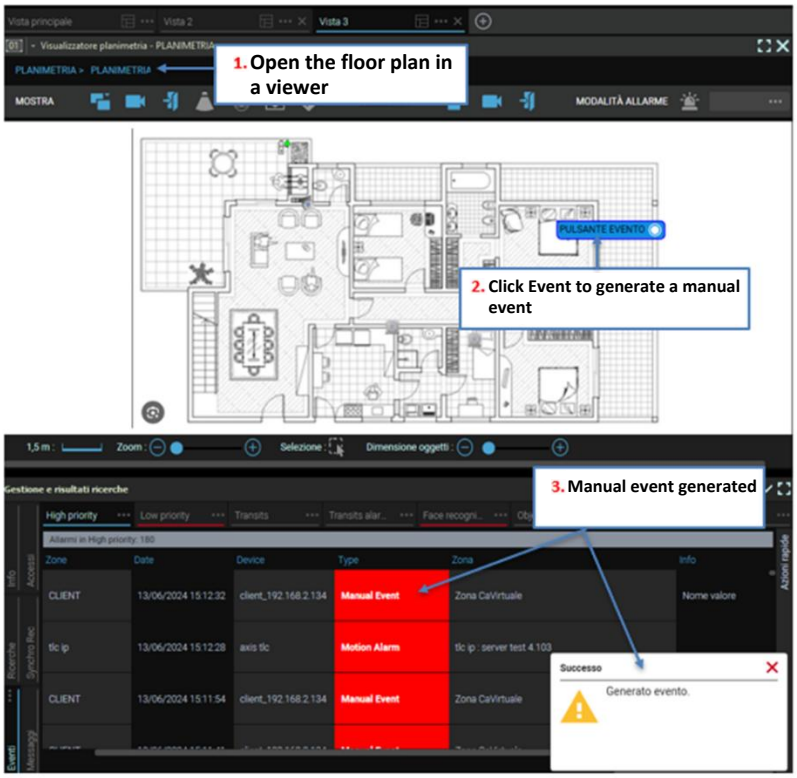
Loading a floor plan or site and configuring its devices

The image below illustrates the floor plan configuration tools.



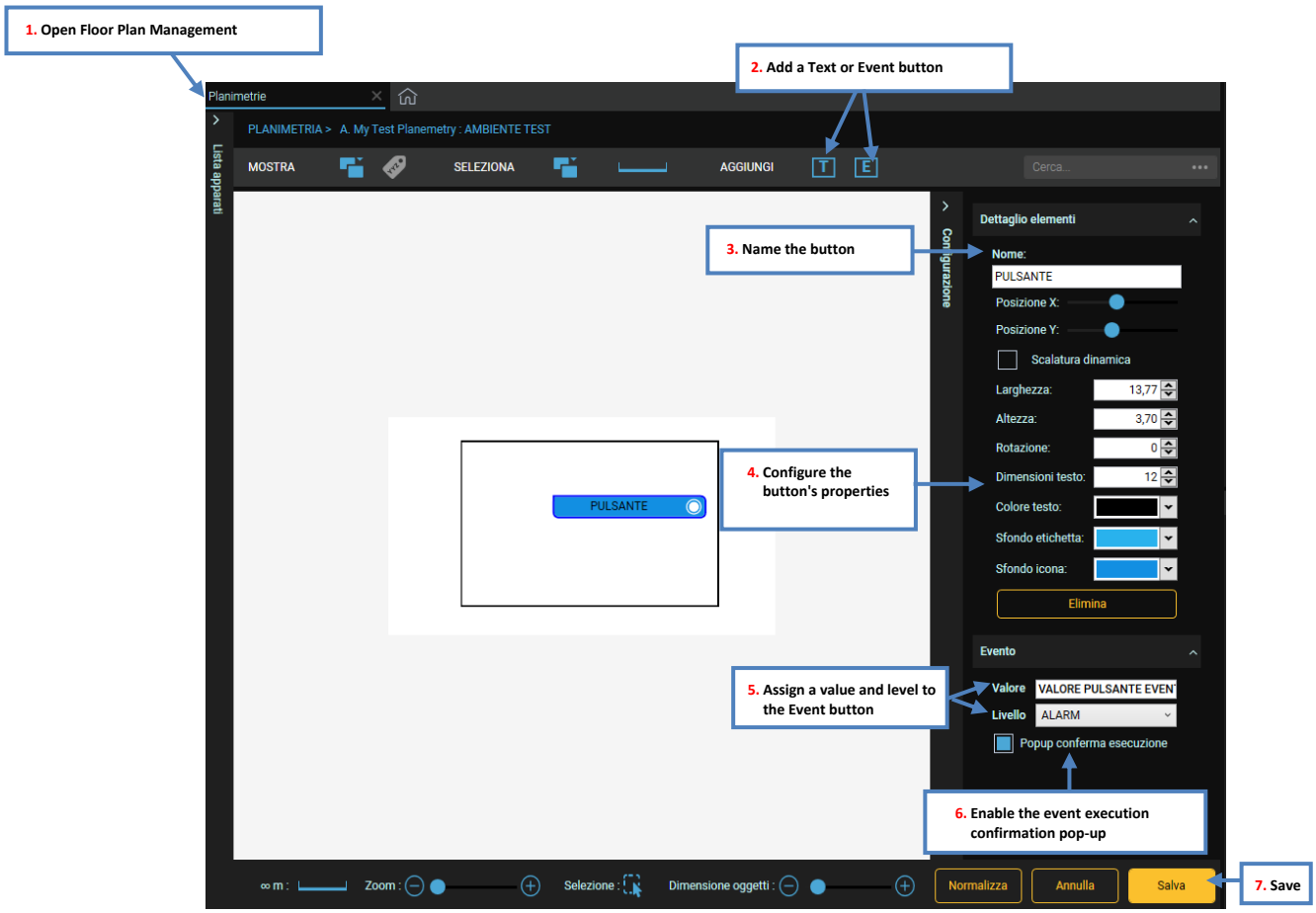
Note: Sites can contain only floor plans, not other sites. Floor plans can contain other floor plans, but not sites.

Once the *Event* button (10) is created, users can generate a Manual Event by clicking the button on the floor plan, following the steps shown below.



Configuring a floor plan button

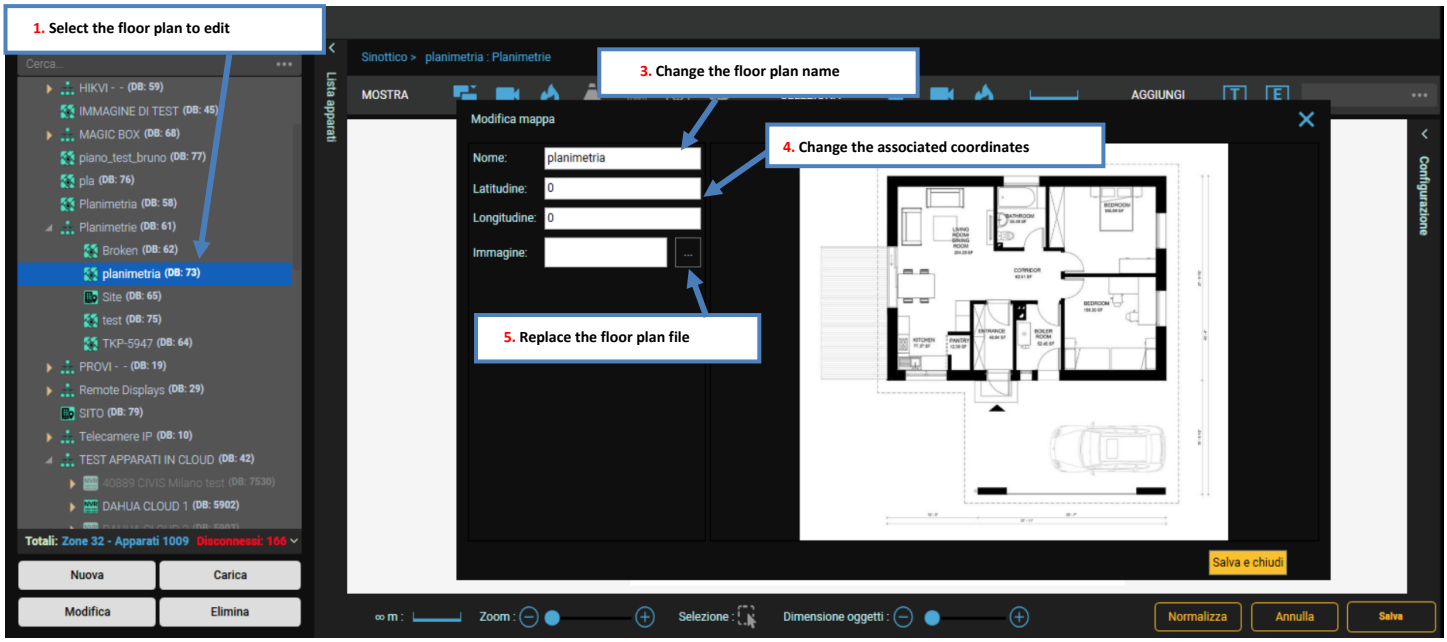
Follow the steps below to configure a Text button (1- 4) or an Event button (1- 6) on the floor plan.



This function allows users to perform multiple actions with one click, after creating a suitable rule in Events/Actions. The following section provides an example of an event/action rule using a Manual Event.

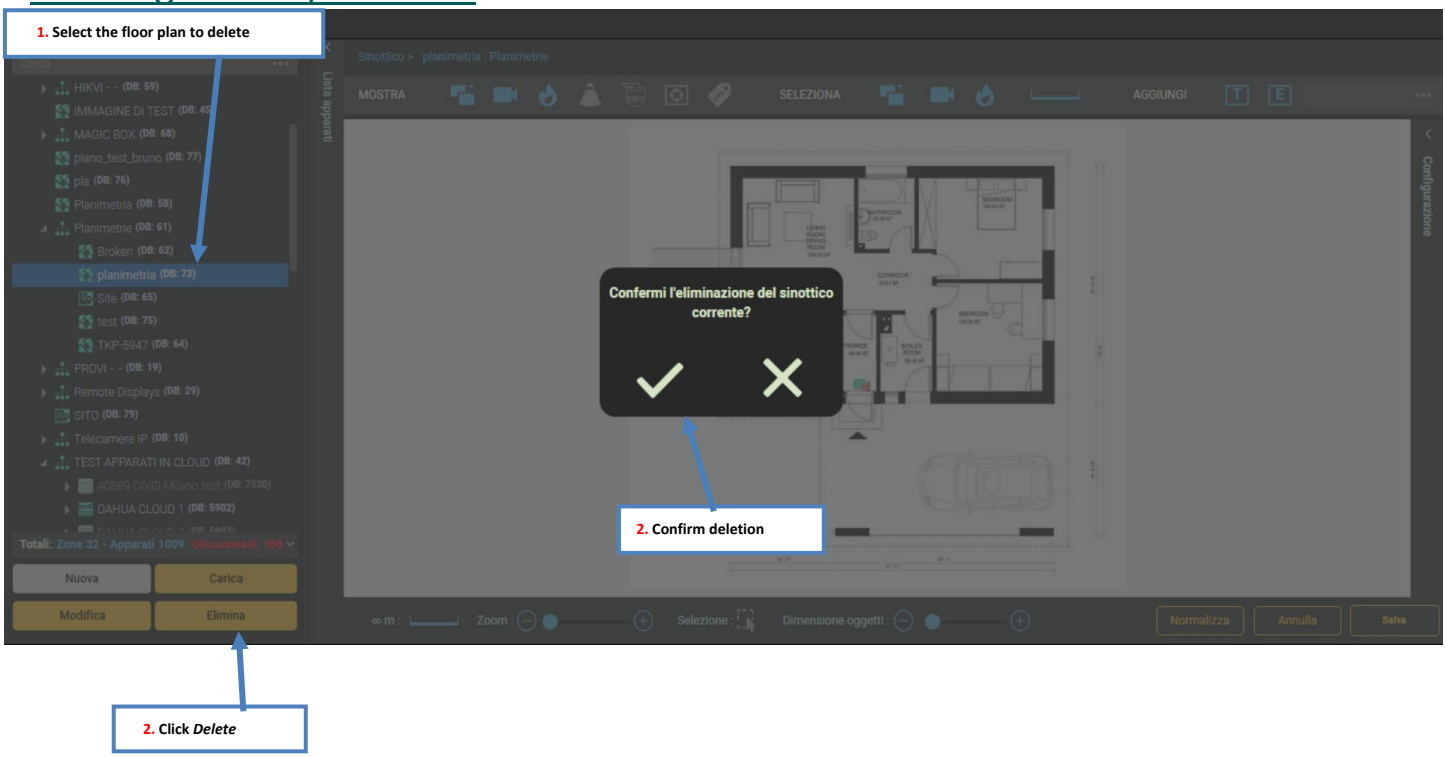
Editing a floor plan

A floor plan can be edited by changing its name, geographical coordinates or file.



To edit devices on a floor plan, load the floor plan and use the tools described above.

Deleting a floor plan



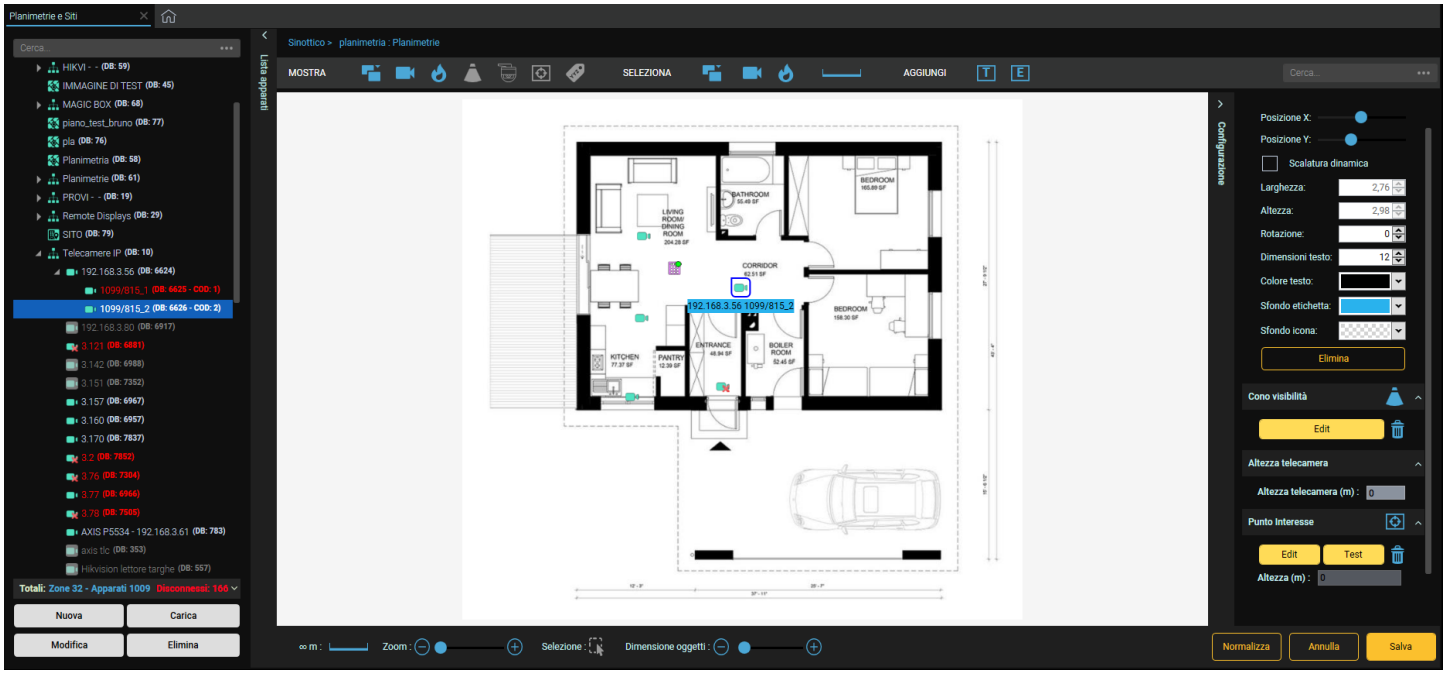
ACTIVE VIDEO SURVEILLANCE

Elkron-ONE provides active video surveillance, allowing one or more devices on a floor plan to be configured to respond to events at points of interest. Devices whose fields of view cover the relevant point are directed towards it, and the system generates an alarm.

Open the administration panel and select Floor Plans to access this function.

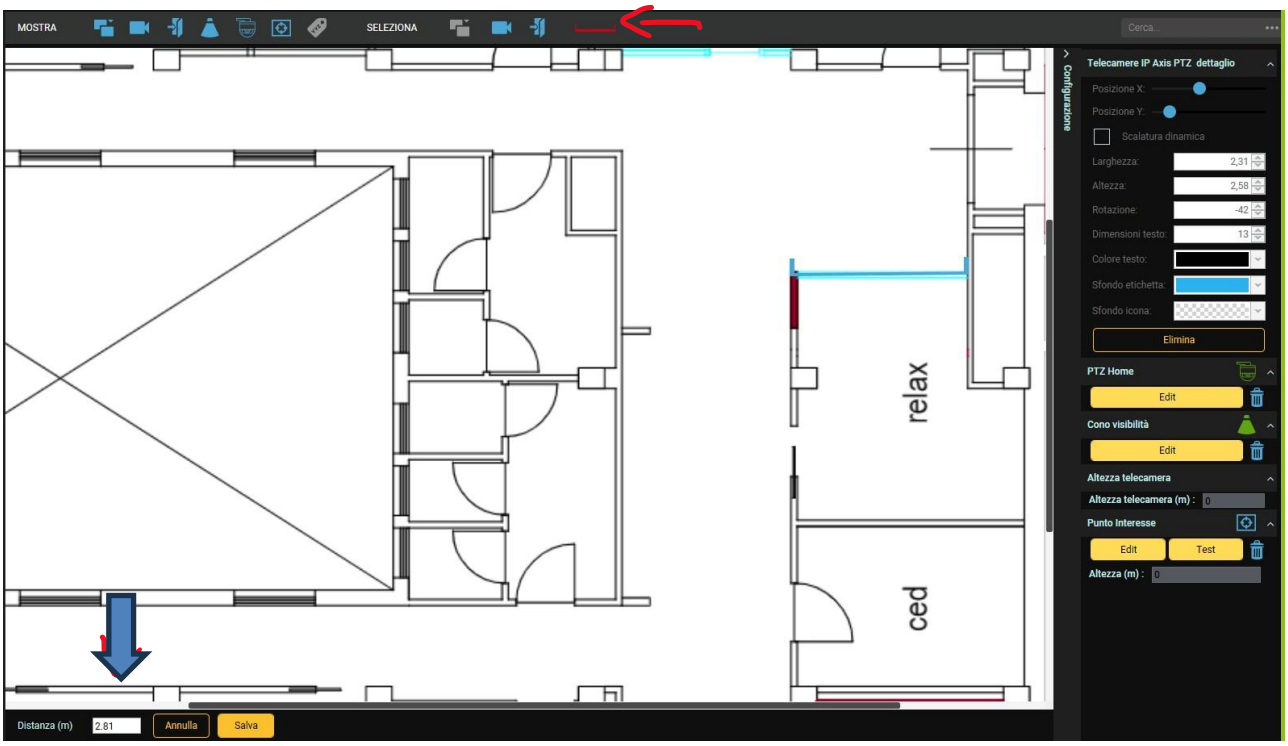


Load the floor plan, then drag a camera onto it and place it at the required position.

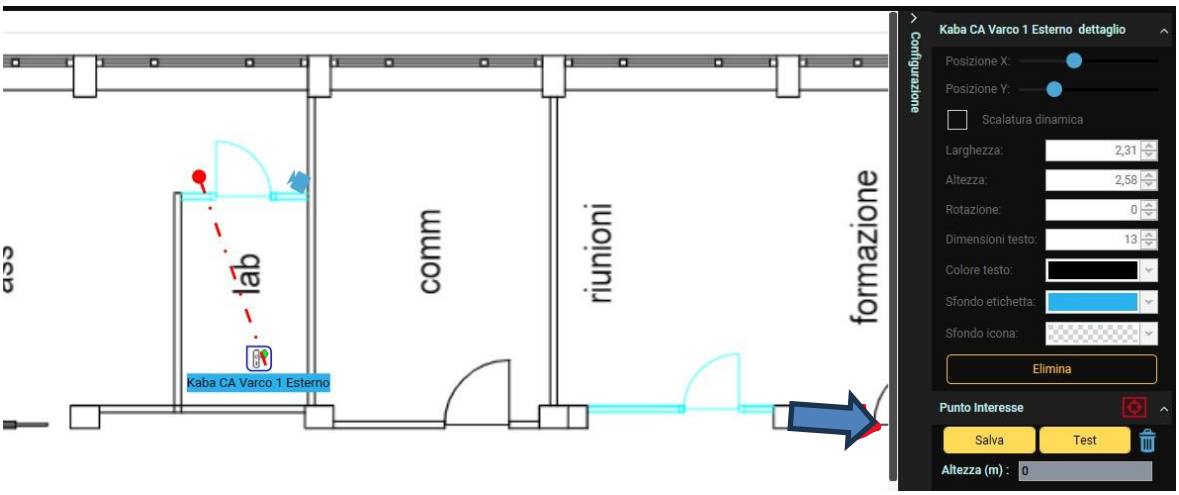


First configure the floor plan scale to relate image pixels to the actual dimensions of the area.

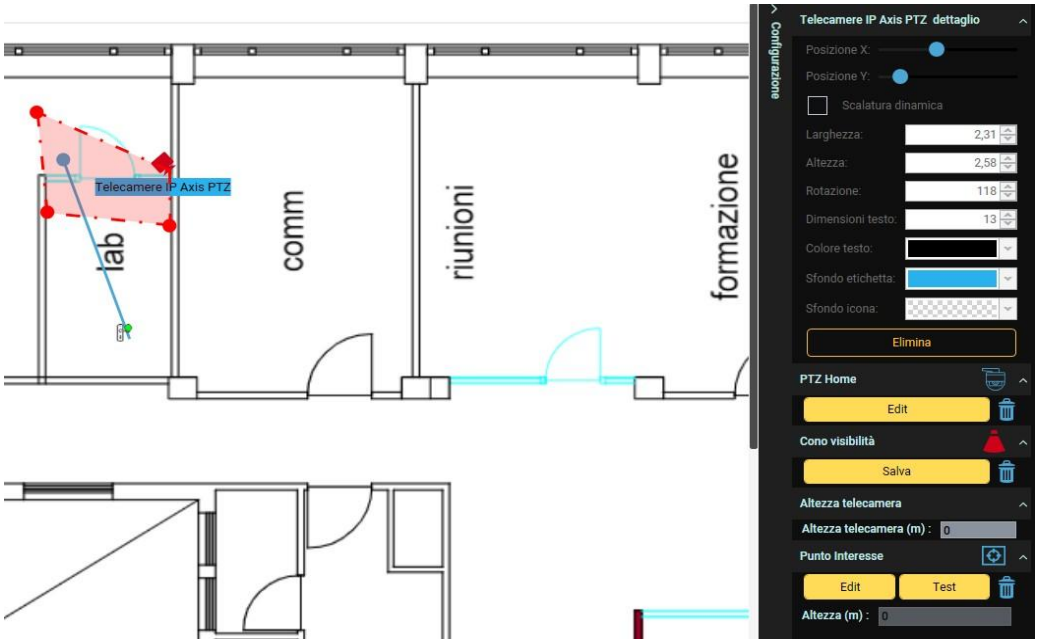
Position the scale indicator over a floor plan feature with known real-world dimensions. Enter its length in metres and save the configuration.



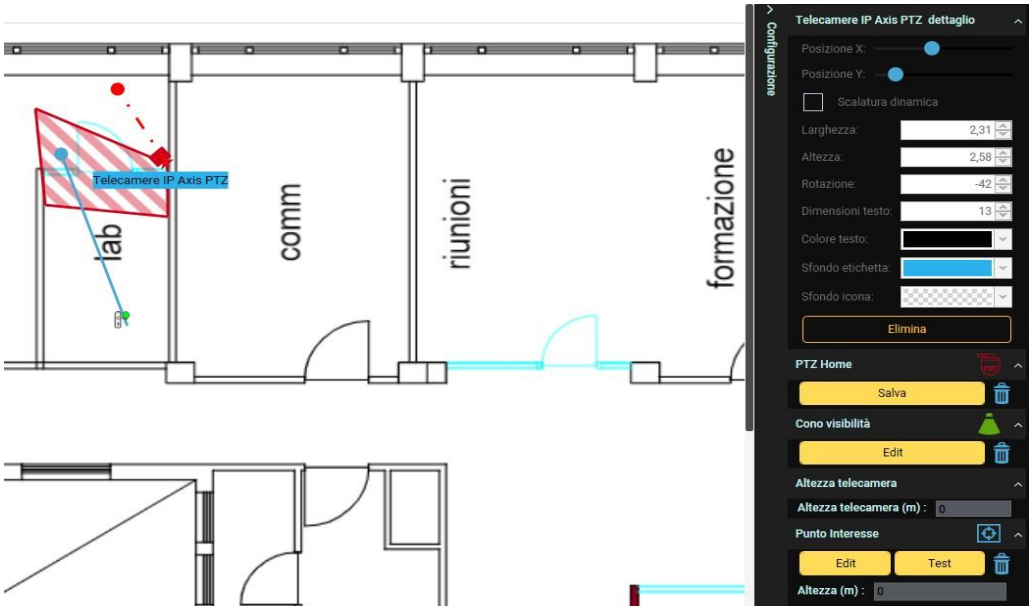
Then configure the point of interest for the intrusion, fire or access control detector.



The detector's point of interest must lie within the camera's coverage cone. Double-click a segment to add a side to the polygon; right-click to edit the area.

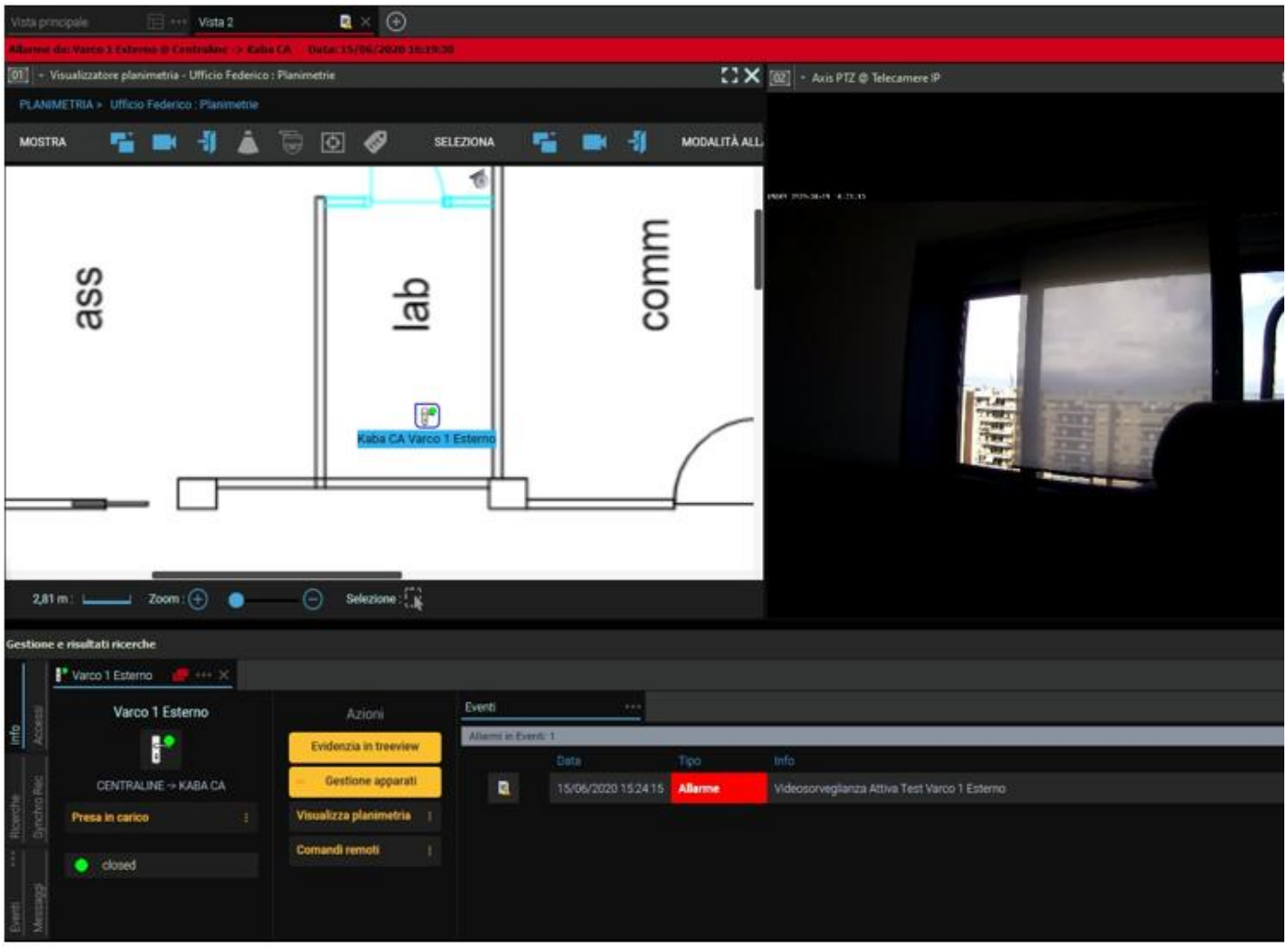


Configure PTZ Home to set the reference point used for rotating PTZ cameras.



After configuring all elements, run a test to check that the expected alarm is generated.

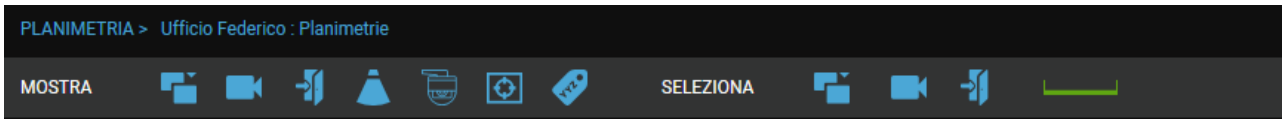
The layout shows the floor plan in one viewer, the camera image in another and the generated alarm in the lower area.



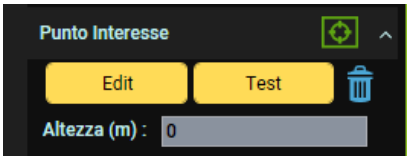
The image shows the configured scale indicator, zoom controls and multiple selection controls.

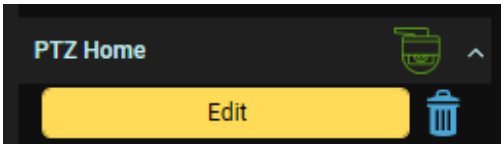


The image shows filters for displaying or hiding cameras, access control devices, coverage cones, number plate readers, PTZ cameras, points of interest and labels on the floor plan. The same toolbar includes filters for selecting cameras or access control devices.



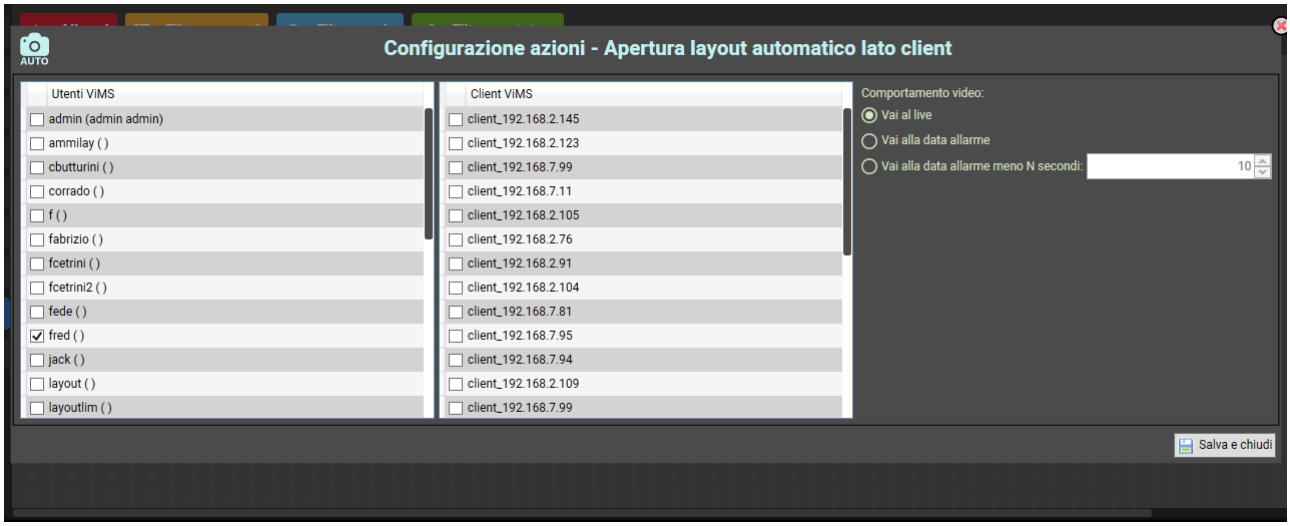
Green icons indicate configured items. The three images show, in order, the point of interest, PTZ Home and scale.







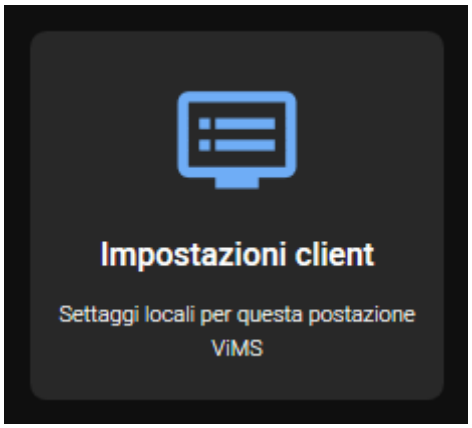
In the administration panel's Events/Actions section, a rule can be configured to open the layout automatically with live video by default, at the exact alarm time, or a specified number of seconds before the alarm.



CLIENT SETTINGS

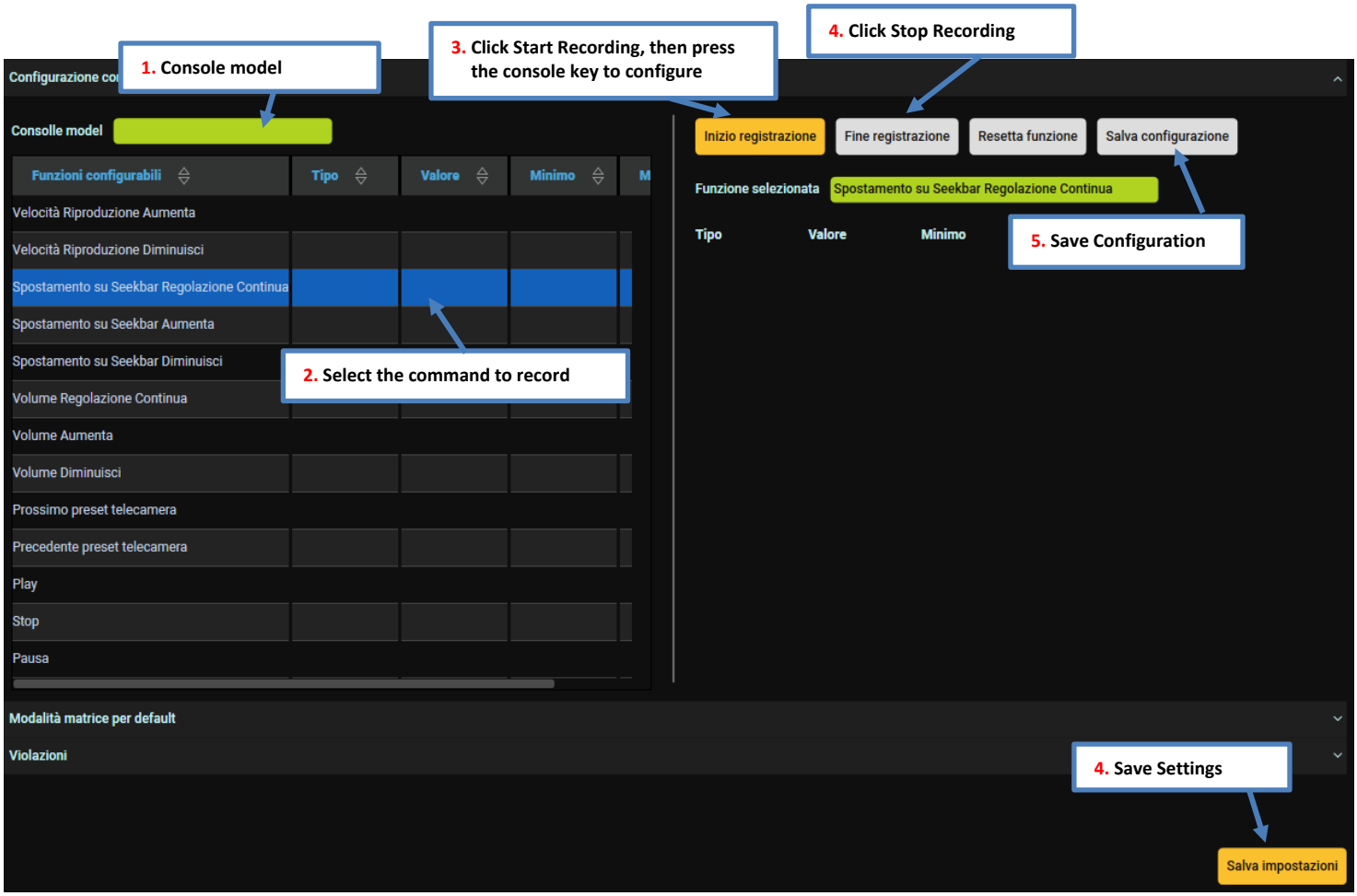
Elkron-ONE includes local settings for each client workstation. Client Settings are shared by all Windows users with access to the workstation, so each Elkron-ONE user does not need to reconfigure the player or console. Settings are saved in separate files under:

C:\ProgramData\Elkron-ONE\Elkron-ONE_CFG

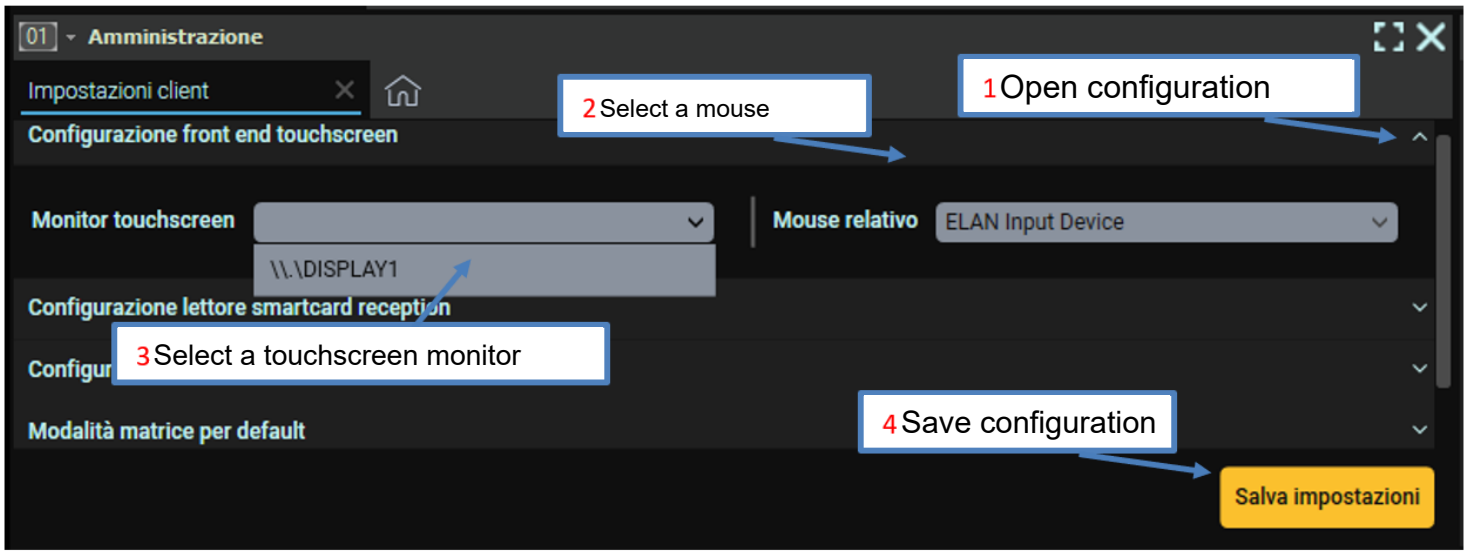


CONSOLE/JOYSTICK CONFIGURATION

Connect the console to the PC and check that its model appears in the corresponding Client Settings area. Follow the steps shown below:

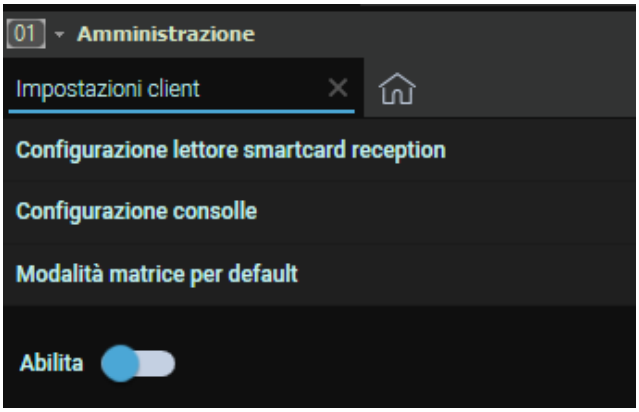


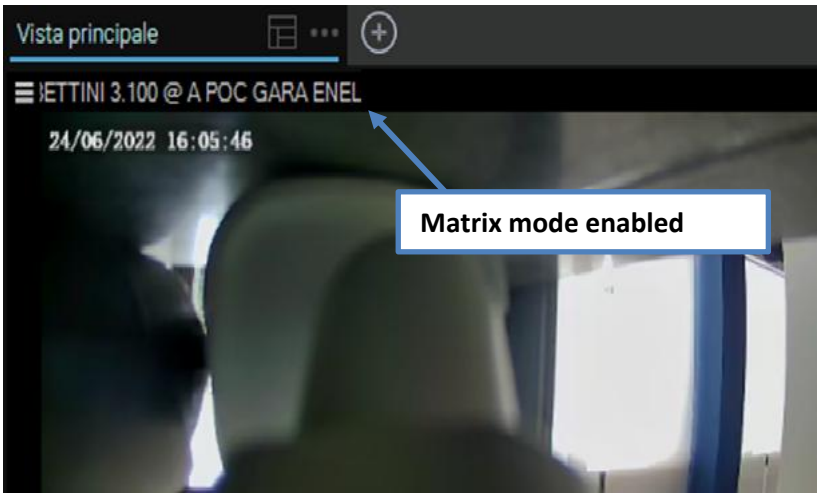
TOUCHSCREEN FRONT END CONFIGURATION

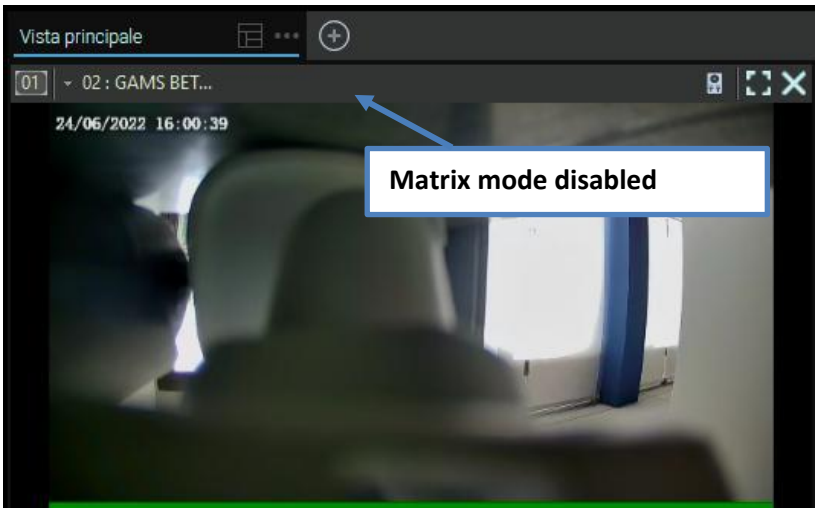


MATRIX MODE CONFIGURATION

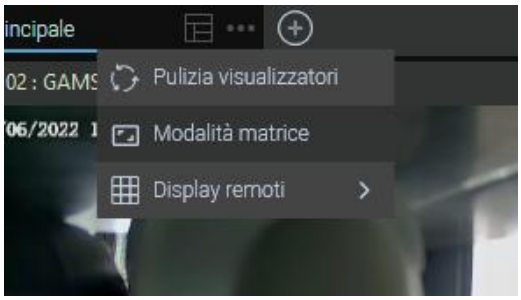
Client Settings can define whether the matrix at the top of viewers is shown by default. Hiding it can be useful when viewers display video streams.





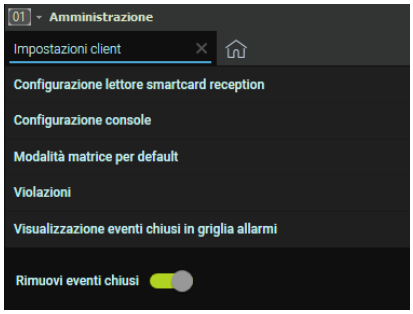


The mode of each individual viewer can also be enabled or disabled as shown below:



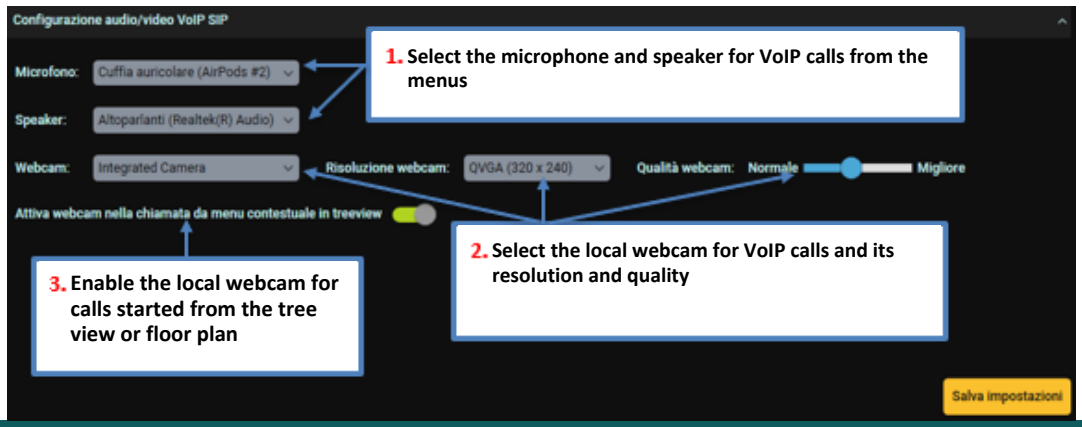
REMOVING CLOSED EVENTS FROM THE EVENT GRID

Client Settings can enable the default removal of closed events from the alarm grid after they have been handled.



VOIP SIP AUDIO/VIDEO CONFIGURATION

Client Settings includes a dedicated section for selecting the audio and video configurations used for VoIP voice and video calls.



Note: If no microphone and/or speaker is detected, the VoIP module will not work. Connect a microphone/speaker and restart the client.

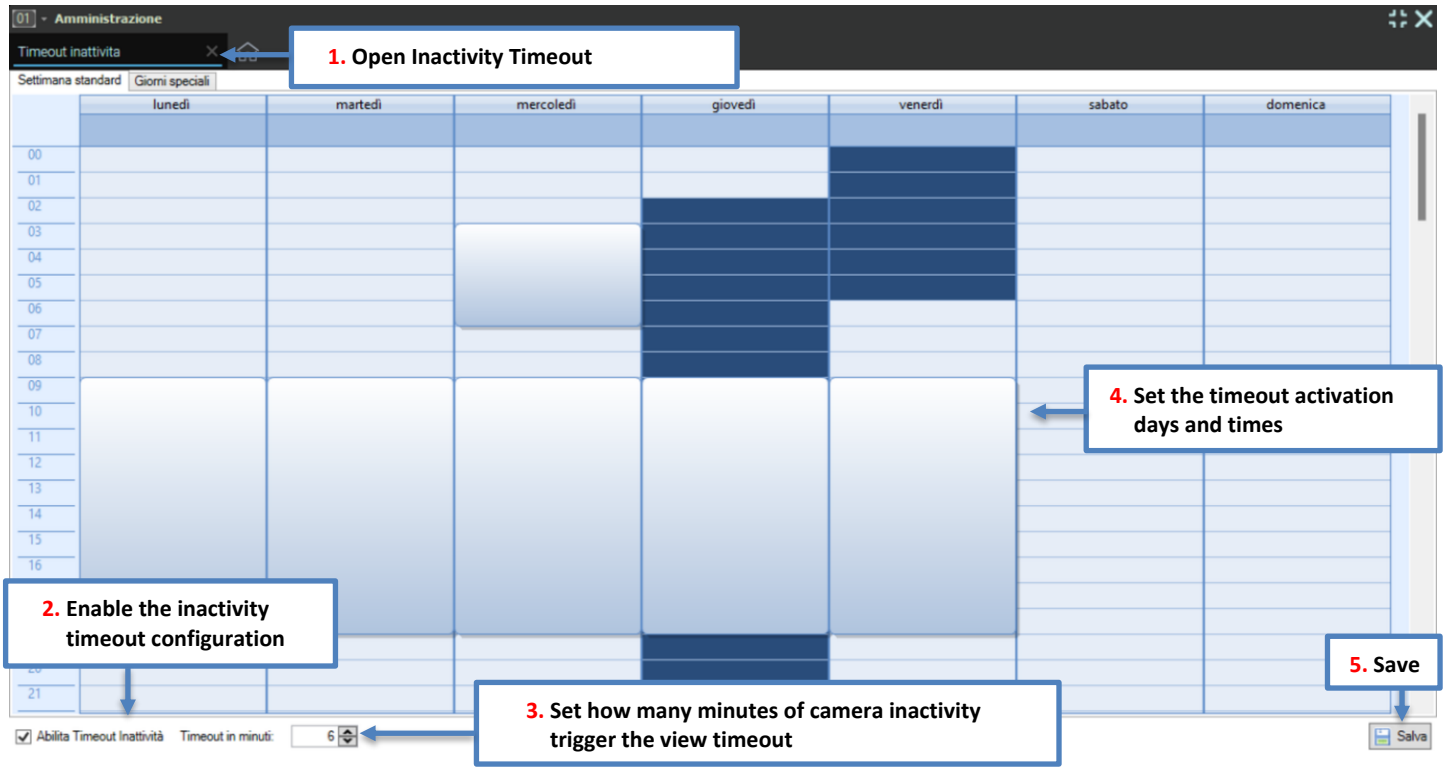
INACTIVITY TIMEOUT

Elkron-ONE includes a section for configuring the inactivity timeout. Open the administration panel and select the panel shown below.



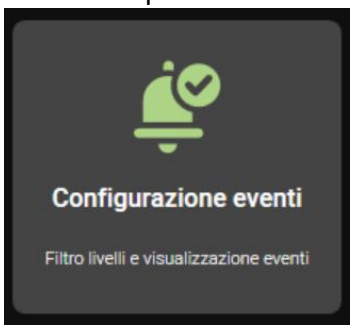
Configuring the inactivity timeout

This function times out camera display in a view after a specified period of inactivity. Follow the steps shown in the image to configure it.



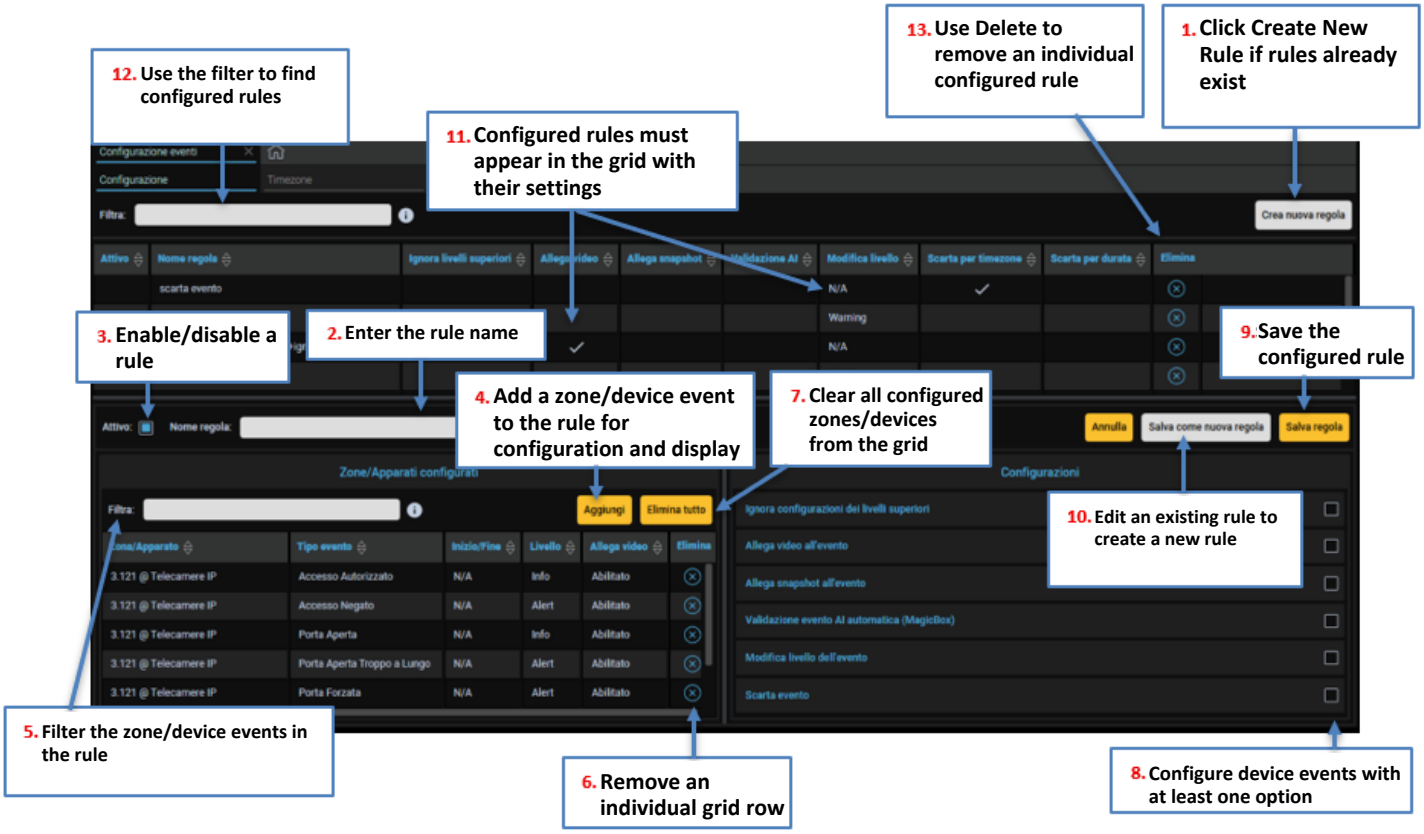
EVENT CONFIGURATION

Event filtering is available from the Administration panel.



This module applies specific settings to one or more events within the same rule.

Follow these steps to use the function.



The following settings can be applied to a rule:

- **Ignore higher-level settings:** ignores settings applied to hierarchically higher elements or devices;
- **Attach snapshot to event:** attaches a snapshot to the received event;
- **Attach video to event:** attaches video to the received event;

Note: For DVR/NVR devices, video attachments can be configured only if the device supports RTSP streaming and the stream is enabled.

- **Automatic AI event validation (Magic Box):** starts automatic AI validation of the rule's events. Set the recording period to analyse using *"Analysis interval: x seconds before and x seconds after the event".* Analysis can also include the first 5 devices in the same zone by enabling *"Include the first 5 devices in the same zone".*

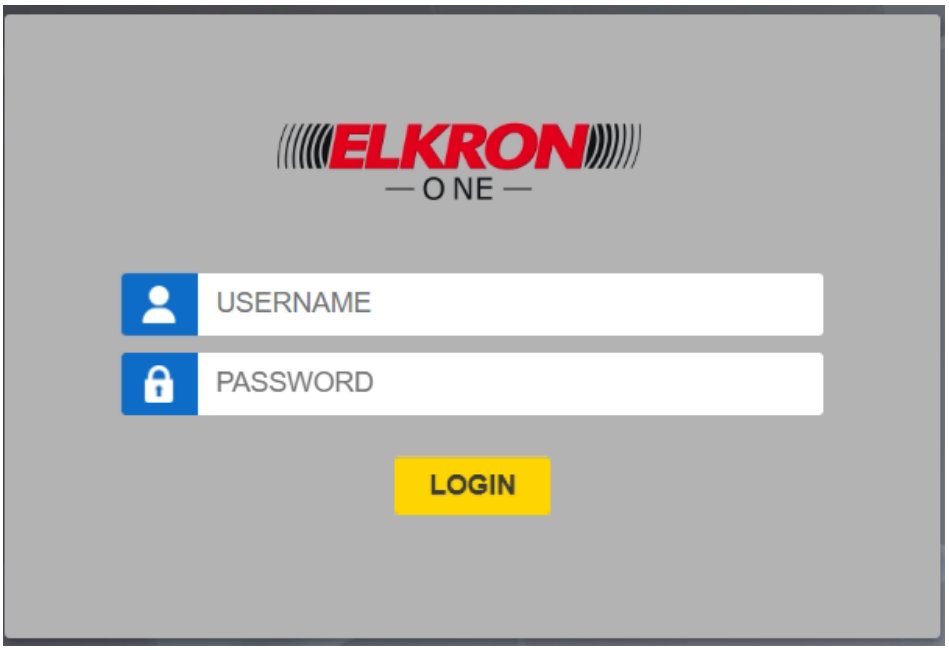
- **Change Level:** filters incoming events in the alarm grid by changing their notification level. For example, a Motion Detection start event can be changed from Alarm to Warning.

- **Discard Event:** discards specific alarms by device, event tag and
  time period during which the event should not be displayed.
  Configure the time periods and special days for discarding the event on the **Timezone** tab.

WEB ADMIN

Admin Web is the Elkron-ONE server administration panel for configuring Elkron-ONE, its associated services and operational functions. It centralises system management to help control, update and maintain the platform. Follow these steps to log in:

1. Enter the IP address in the browser address bar. The following screen appears:

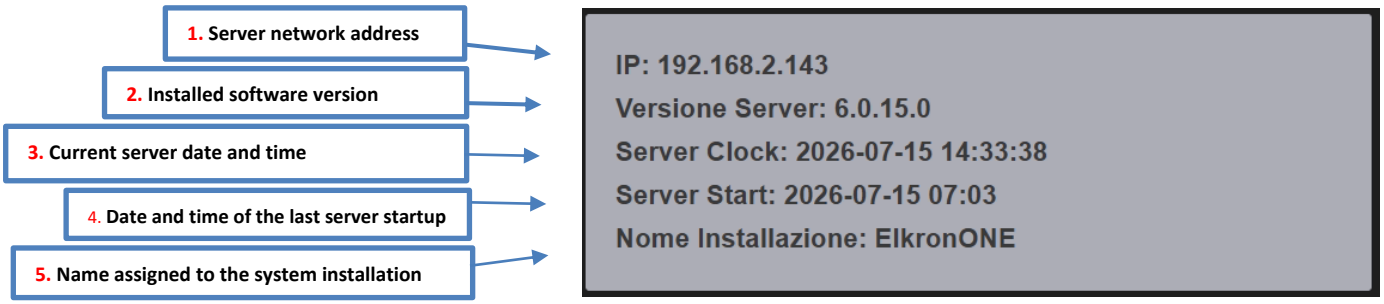


2. Enter your username and password in the corresponding fields and log in.

The Admin Web page contains the sections described below.

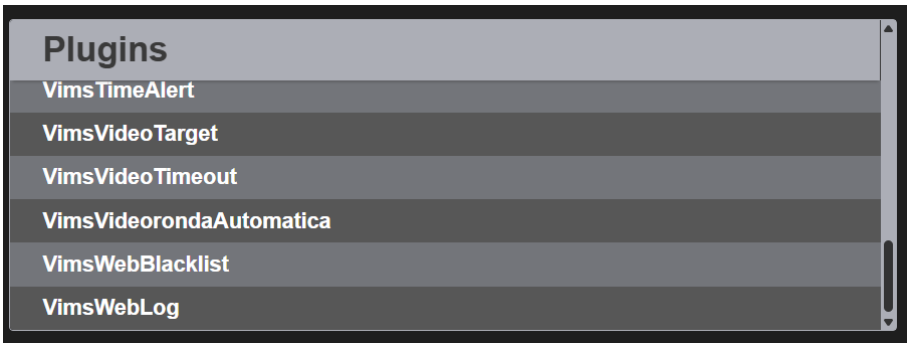
Server information

Server Information shows the system's main identification and operating details.



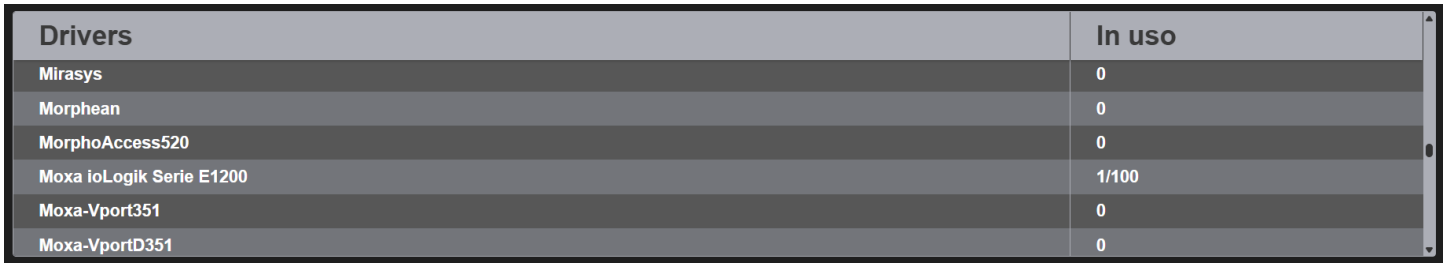
Plugins

Plugins lists all available plugins loaded by the system. Plugins extend platform functions and integrate third-party devices, services and applications.



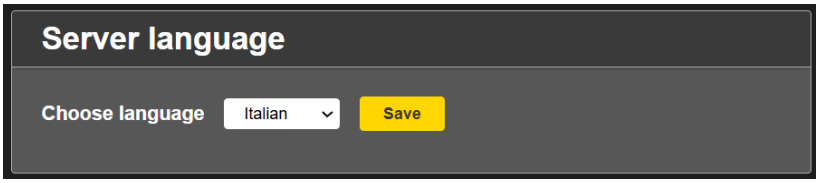
Drivers

Drivers shows the drivers supported by the system. Each driver displays the number of instances in use compared with the maximum available, providing a quick overview of resource and integration usage.



Server language

Server Language selects the administration interface language from a drop-down menu. Select the language and click Save to apply the change.



Clock settings

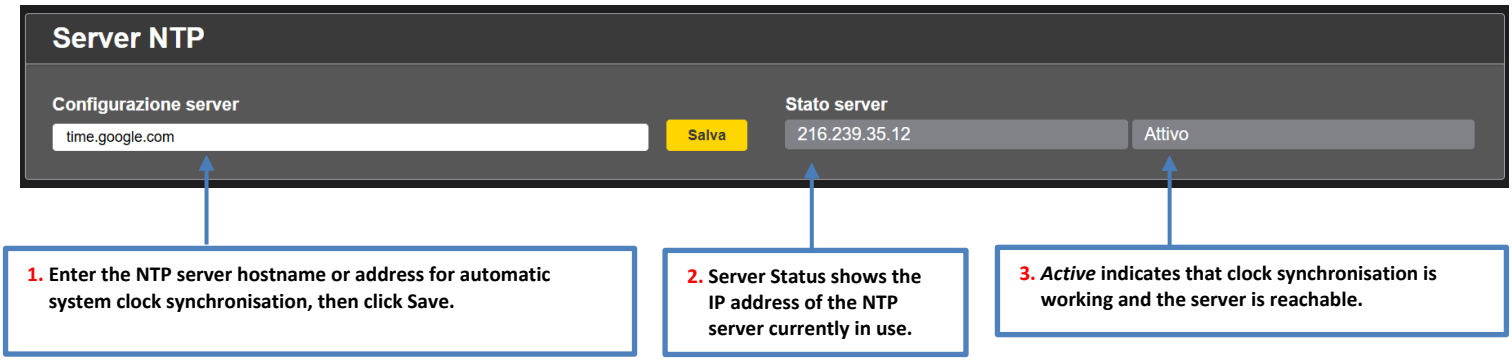
Clock Settings shows the current server date and time. These can be changed manually using the corresponding fields and saving:



Changing the system clock affects functions that use time references, including event recording, logs and schedules.

NTP server

NTP Server configures a server for clock synchronisation using Network Time Protocol.

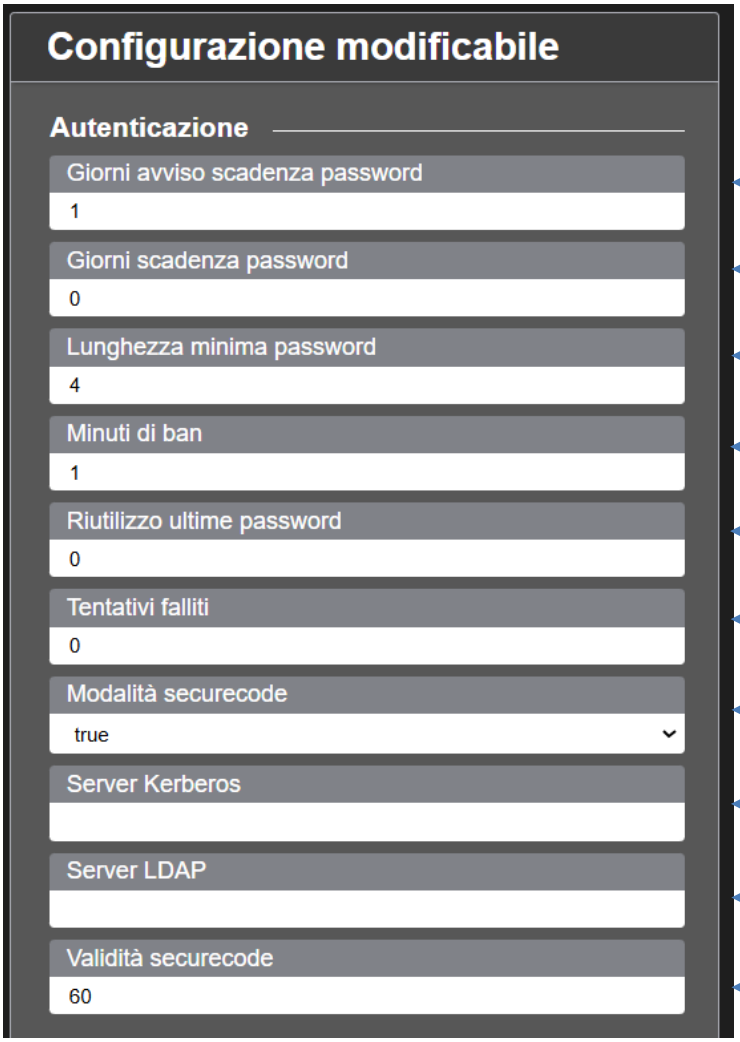


Editable configuration:

Editable Configuration allows administrators to define general ELKRON-ONE operating parameters, including user authentication, notifications, cloud integrations, communication services and event management.

- ### Authentication

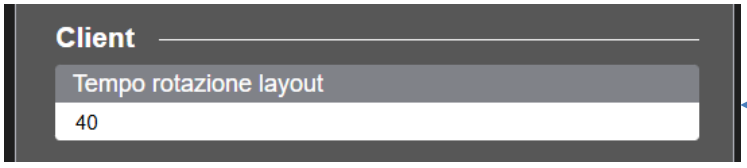
  Authentication contains user account and access security parameters.



1. Number of days before password expiry when the user starts receiving warnings.
2. Password validity period in days. Enter 0 for no expiry.
3. Minimum number of password characters.
4. Account lockout duration after exceeding the permitted login attempts.
5. Number of previous passwords that cannot be reused.
6. Maximum number of failed login attempts before lockout.
7. Enables an additional security code, such as a second authentication factor or temporary code.
8. Kerberos server address for centralised authentication.
9. LDAP server address for corporate directory authentication.
10. SecureCode validity period in seconds.

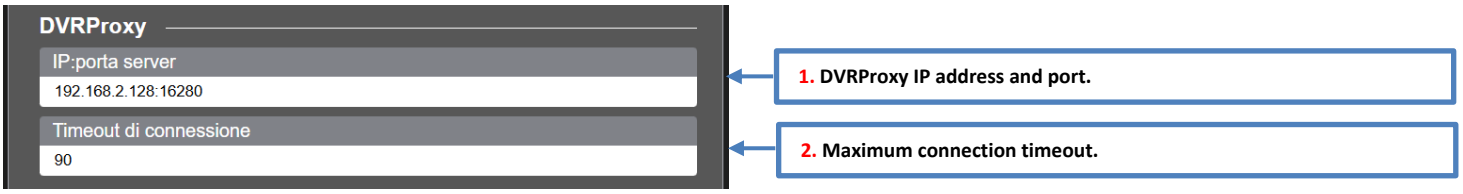
- ### Client

  Client contains user interface parameters.

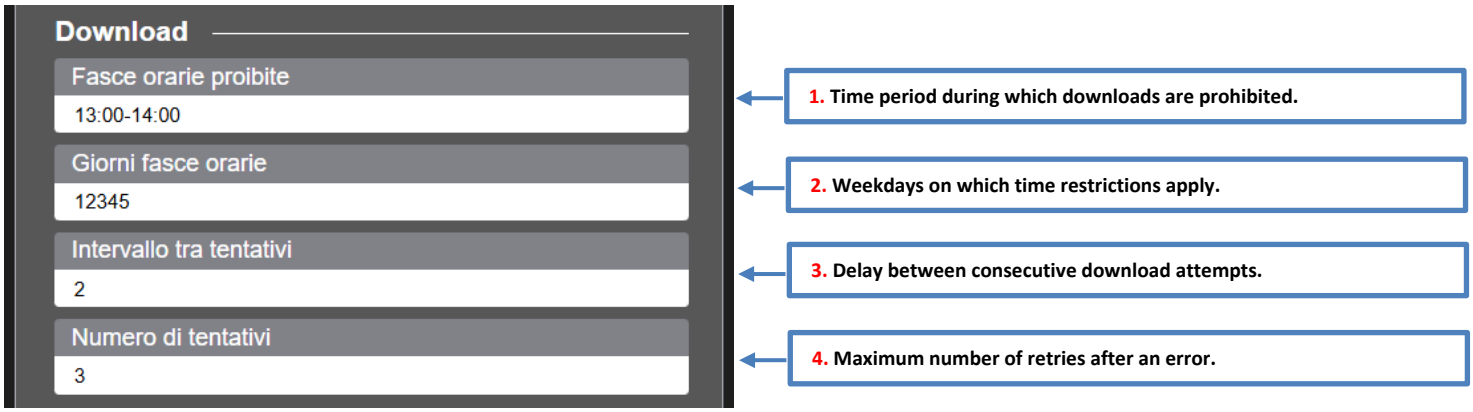


1. Interval in seconds for automatically rotating layouts or displayed screens.

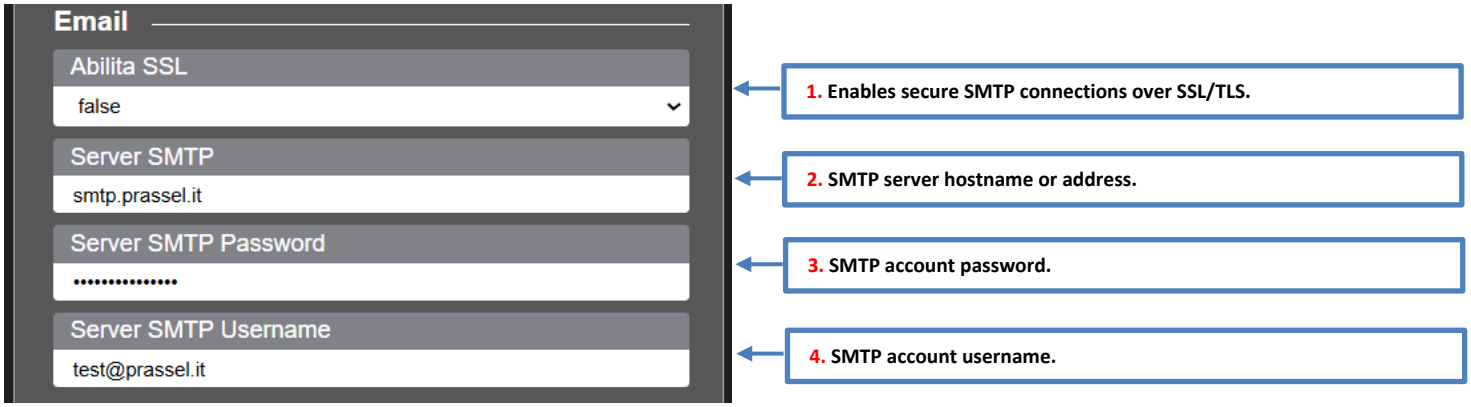
- **DVRProxy**
  DvrProxy configures the DVR Proxy parameters used by the Elkron-ONE server to communicate with DVRs.



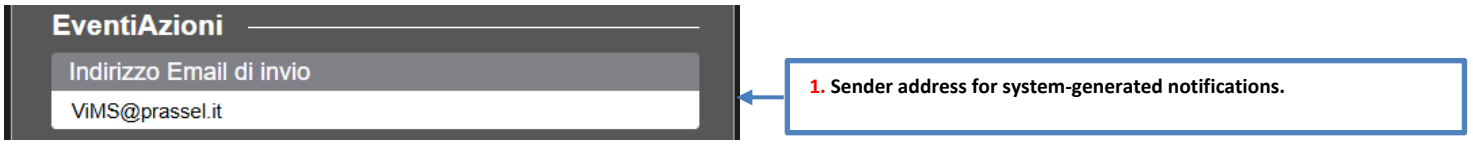
- **Download**
  Download configures the time periods for automatic downloads.



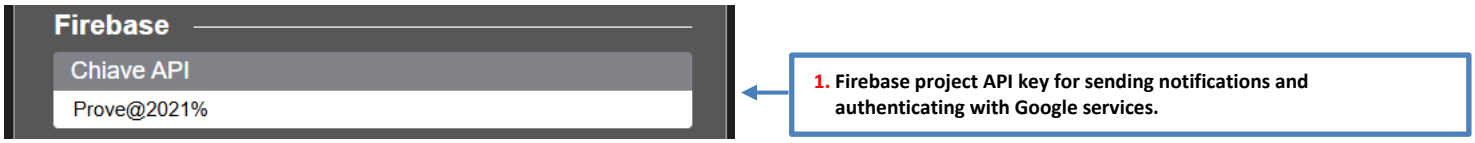
- **Email**
  Email configures the email service.



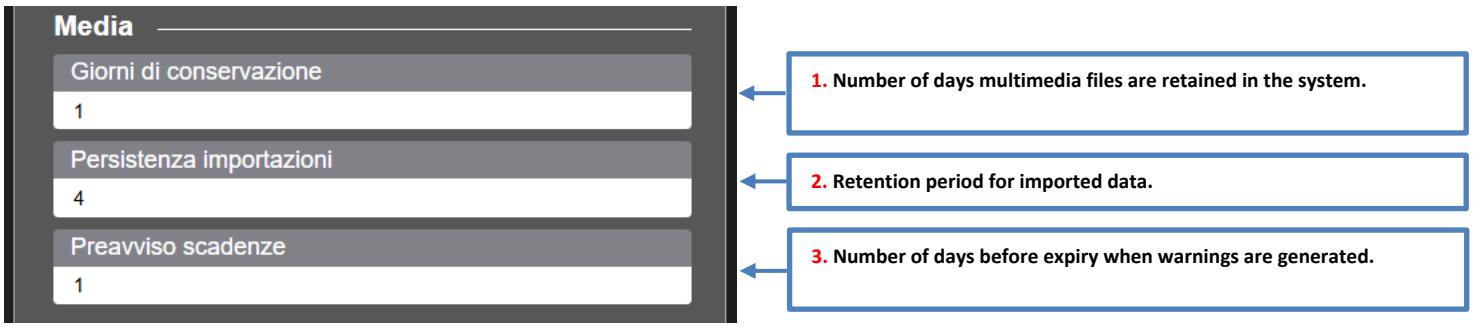
- **Events/Actions**
  Events/Actions configures automatic event notifications.



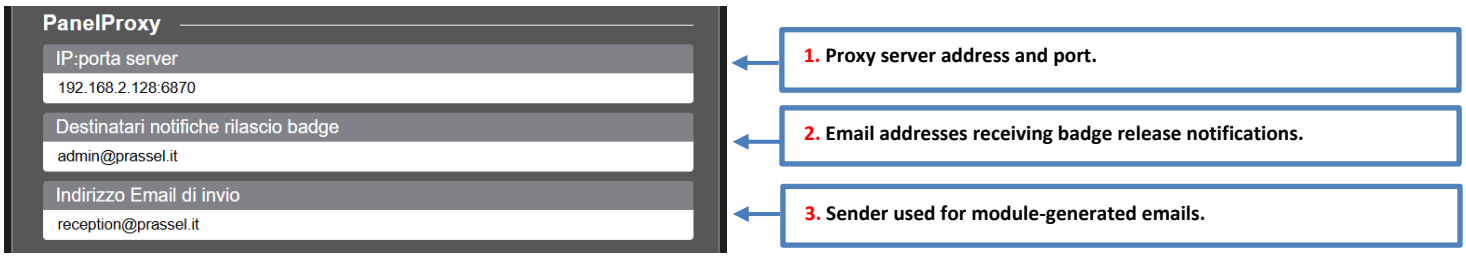
- **Firebase**
  Firebase contains the *Firebase* service settings for push notifications and cloud services.



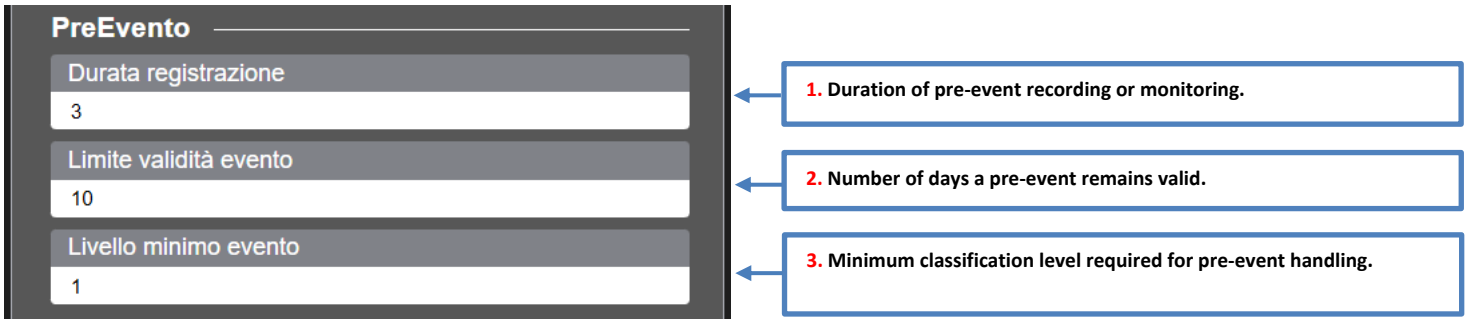
- **Media**
  Media configures multimedia content management and retention.



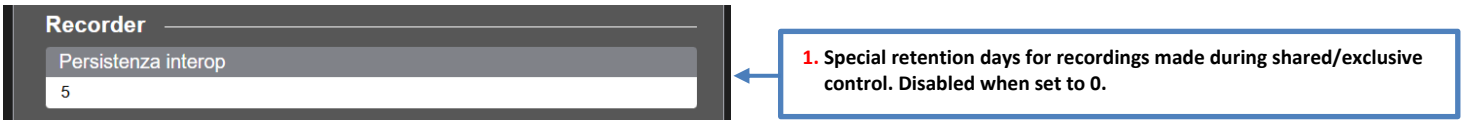
- **PanelProxy**
  PanelProxy configures the Panel Proxy parameters used by the Elkron-ONE server.



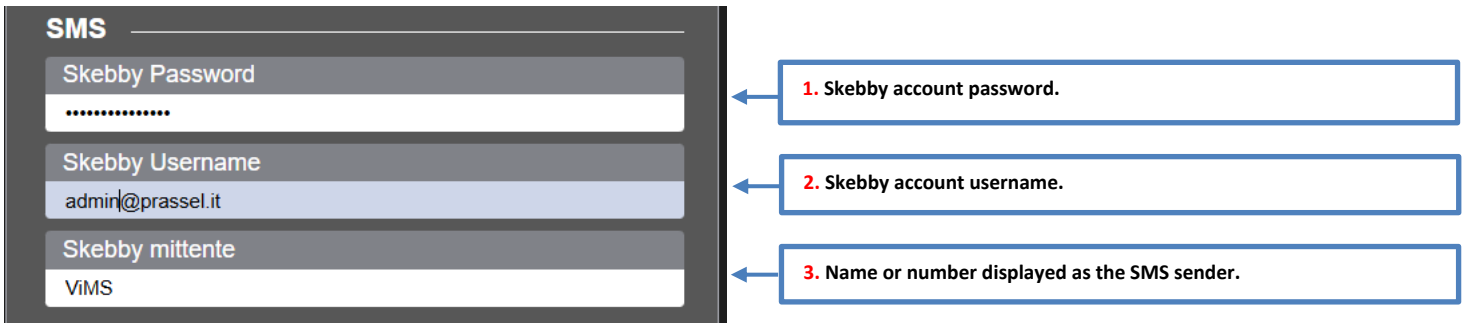
- **Pre-Event**
  Pre-Event contains pre-event configuration parameters.



- **Recorder**
  Recorder configures recording systems.

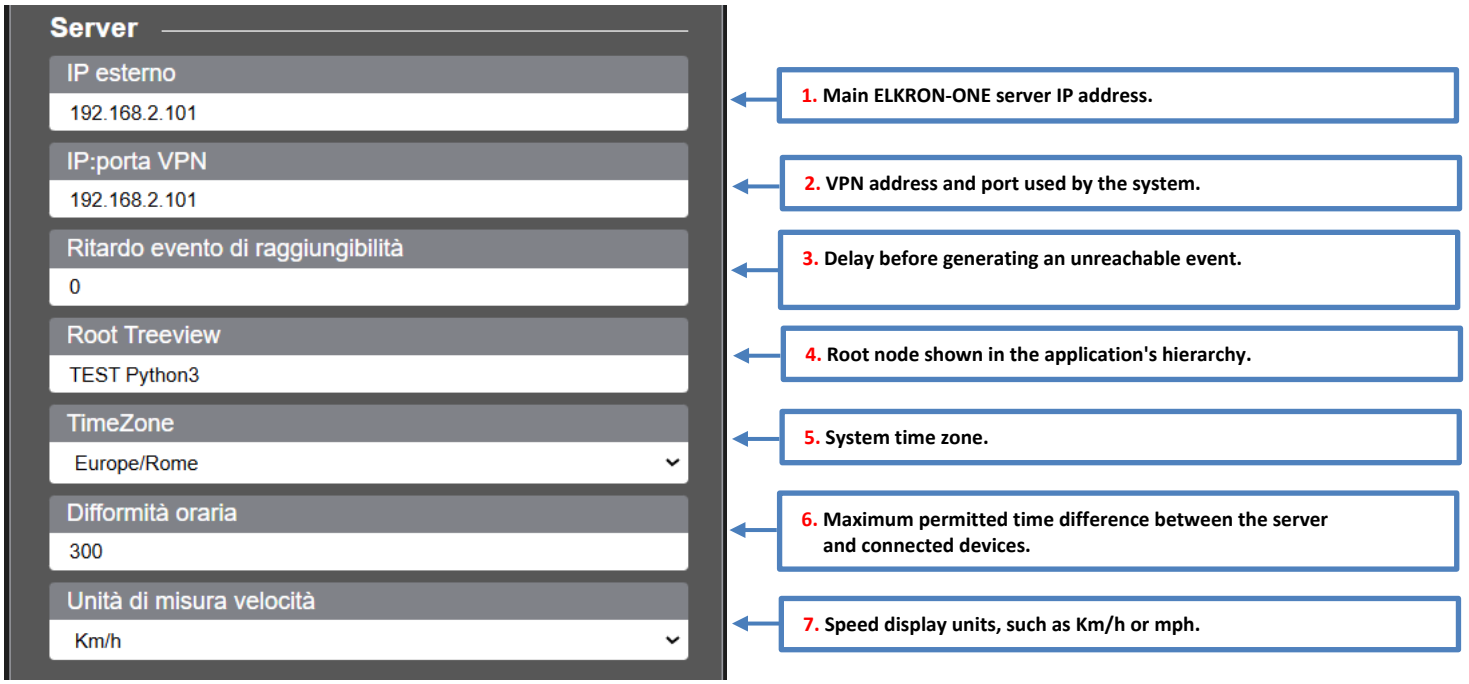


- **SMS**
  SMS configures the SMS gateway.



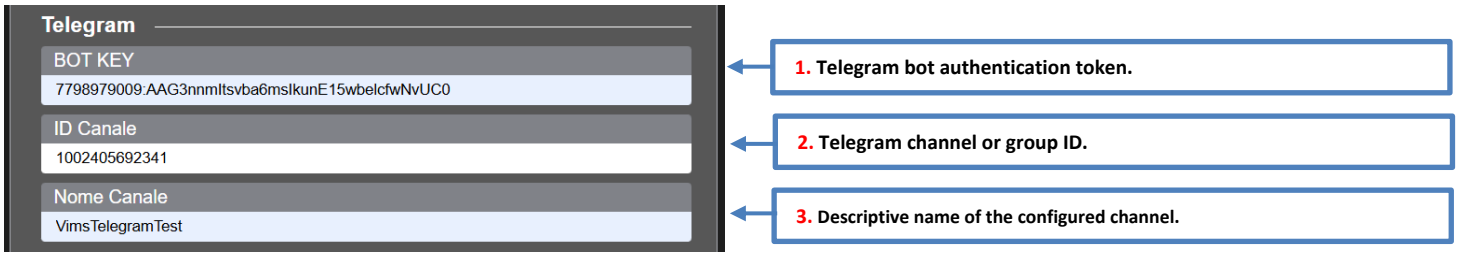
- **Server**

  Server contains general ELKRON-ONE application server parameters.



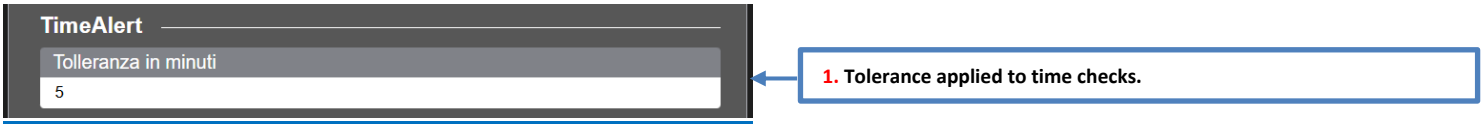
- **Telegram**

  Telegram configures Telegram notifications.



- **TimeAlert**

  TimeAlert contains time period and anomaly monitoring parameters.



Permission to edit *Admin Web:*
Editable Configuration contains parameters affecting the general operation of ELKRON-ONE and its integrations. These may therefore be changed only by System Administrators or users with specific advanced configuration permissions assigned by the organisation. Users without the required privileges can view the information but cannot change it.

Saving *Admin Web* changes:
After changing configuration parameters, click *Save.* Changes are applied only after saving. Leaving the screen without saving discards all changes.

USER PERMISSIONS

Elkron-ONE groups user permissions into functional categories. Each contains authorisations defining the operations a user can perform in the application.

The available permission categories and their meanings are described below:

MANAGEMENT

- ***Enable client-side search panels***
  Users can search by topic using the search panels on the client's System Bar: Access, Alarms, Licence Plates, Hazards, Multimedia, Daily Report, Video Patrol and Server Reports.

- ***Enable layout rotation interval changes***
  Allows the user to set the layout rotation interval in seconds in the layout patrolling settings.

- ***Allow editing layouts saved by other users***
  Allows access to and editing of layouts previously saved by other users in the client's Layouts section.

- ***Allow viewing device Information tabs***
  Allows users to view specific device information by right-clicking the device and selecting View Information directly in the resource tree.

- ***Allow sending remote commands to devices***
  Allows users to send remote commands such as *Set NTP, Restart* and *Shut Down.*

- ***Allow managing layouts***
  Allows users to configure viewing layouts that can be saved and quickly recalled. Users can choose the number and type of viewers and the data to display within them.

- ***Allow placing devices under maintenance***
  Allows users to place a device under maintenance or remove it from maintenance directly from the resource tree.

- ***Allow moving PTZ cameras***
  Allows users to move a PTZ camera while viewing it.

- ***Allow restarting server services***
  Allows users to restart any service from *Server Diagnostics* in the Administration panel.

- ***Allow event searches***
  Allows users to search recorded system events, view information and filter it using the available criteria.

- ***Allow viewing device technical information***
  Allows users to view a device's connection parameters using *View Device Connection Parameters* in the tree view.

- ***Allow sending the Reset command to devices***
  Allows users to reset a device directly from the tree view context menu without using the Administration panel.

- ***Force taking/releasing device control***
  Allows users to force taking and releasing control of devices.

- ***Show alarms sent by devices***
  Allows users to view device alarms in the client's Management and Search Results area. The alarms shown are those configured for the specific device.

- ***Allow taking/releasing device control***
  Allows users to manage interoperability only from the main Elkron-ONE tree view and *Usage Rights* in Device Management.

- ***Print and burn data***
  Allows users to print system data such as the real-time alarm queue, search results and the internal message list.

SYSTEM

- ***Enable the Voice Recording module***
  Allows users to enable Voice Recording from *Client Settings.*

- ***Allow adding or removing system icons***
  Allows users to add or remove system icons through User Icons.

- ***Allow assigning icons to devices***
  Allows users to assign existing icons to devices available on the client through User Icons.

- ***Allow changing local settings***
  Allows users to configure workstation settings through *Client Settings,* including the reception smartcard reader, console key functions and default Matrix mode.

- ***Allow managing event configuration***
  Allows users to define and edit the parameters and settings governing system events.

- ***View logs***
  Allows users to view the chronological record of activities performed while using the system. Start a search to view logs quickly, using filters to find those of interest.

- ***View free NVR space***
  Allows users to check the free space available for recordings through the system bar.

- ***View connected users***
  Allows users to view current session users through the corresponding button on the client's system bar, including their login, username and group.

- ***Device Management***
  Allows users to manage client-connected devices and configure their operation through *Devices.*
  Parameters depend on driver hardware characteristics and device-supported functions.

- ***Manage automatic alarm time periods***
  Allows users to configure automatic alarms for a specific period on Event Configuration, selecting the zone or device, event type and handling configuration.

- ***Manage server interoperability***
  Allows management of remote server links and remote access through *Multilink.* In server interoperability, the Master can see the Slaves, but not vice versa.

- ***Manage SCNTT***
  Enabling *Manage SCNTT* allows users to exchange licence plate identification information with CEN.

- ***Manage overviews***
  Allows users to configure overview maps through *Floor Plans.* Floor plans support .jpg/png/.gif formats. Device display can be filtered and specific alarms or events highlighted on the floor plan.

- ***User Management***
  Allows flexible user profile management for assigning available functions. User groups can also be created with privileges that can be assigned to individual users.

- ***Manage event views***
  Allows users to create and edit event views and configure event display and filtering criteria.

- ***Prevent deleting non-empty zones***
  With this permission enabled, the user cannot prevent deletion of a non-empty zone in the client's resource tree.

VIDEO

- ***Allow viewing live video streams***
  Allows users to view live streams from devices such as IP cameras, DVRs and NVRs in the Viewing and Control panel.

- ***Allow managing the user's group imports***
  Allows users to view and manage Transfer Manager downloads started by other users in the same group.

- ***Allow importing device recordings during prohibited periods***
  Allows users to start Transfer Manager downloads during periods configured as prohibited.

- ***Allow changing Video Patrol configuration***
  Allows users to view and manage the Video Patrol module in the Administration panel.

- ***Allow hiding privacy masks***
  Allows users to hide privacy masks on a camera's video stream.

- ***Allow viewing recordings***
  Allows users to search through the corresponding button in the Viewing and Control panel. Multimedia Search can find recordings on both devices and the server.

- ***Allow viewing event-related recordings***
  Allows users to view recordings before an event, according to the server's Pre-Event settings.

- ***Allow enabling/disabling Video Patrol from the tree view***
  Allows users to enable or disable a channel's configured Video Patrol directly from the tree view context menu without opening the Video Patrol module.

- ***Allow advanced recording analysis***
  Allows users to perform advanced analysis of recordings archived in the system.

- ***Change retention protection even for another user's files***
  After selecting a recording, users can enable retention protection for another system user's file. This marks the file as protected from system deletion even after the configured retention limit expires. Protection can also be disabled, allowing the file to be deleted.

- ***Recording restrictions: unrestricted access to all imported recordings***
  Allows the control room to view server-imported recordings even after authorisation expires. This permission depends on *Recording Restrictions: View Only the Authorised Time Period.*

- ***Recording restrictions: grant viewing permission for the user's zone***
  Allows the store manager to authorise a control room user to view recordings from devices in the manager's zone.

- ***Recording restrictions: grant permission for a time period***
  Allows the store manager to select the recording period (From/To) accessible to the control room.

- ***Recording restrictions: view only the authorised time period***
  Allows control room users to access recordings authorised by the store manager. This permission depends on *Allow Viewing Recordings.*

Elkron is a trademark of Urmet S.p.A.
distributed by Urmet Solutions GLT s.r.l.

Via Bologna, 188 C
10154 Torino (Italy)

(+39) 011 39 86 711
info@elkron.it
www.elkron.com

follow us