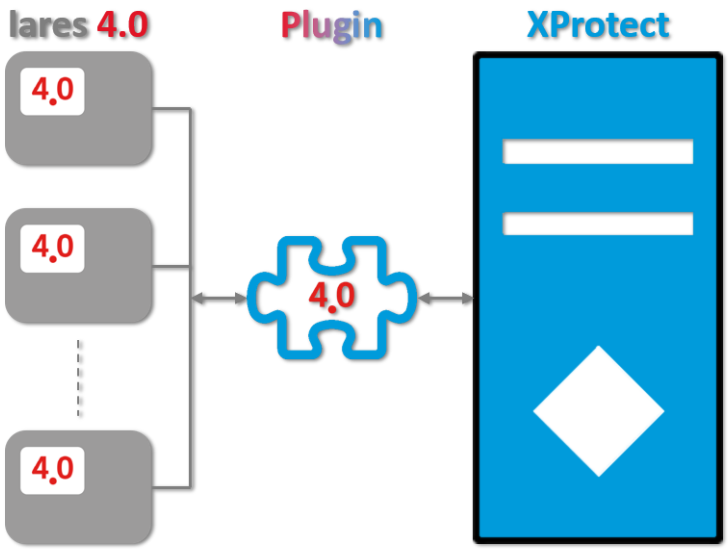
lares 4.0 MIP Plugin

Administrator Manual



Ksenia®
security innovation

www.kseniasecurity.com

The content of this document is provided for informational purposes only, is subject to change without notice and should not be construed as a commitment by Ksenia Security.

Summary

Copyright and Disclaimer

© Copyright Ksenia Security 2021-2030. All rights are reserved.

Disclaimer

This document is intended for general information purposes only of the Plugin and its application to the Milestone XProtect Platform, of which at least basic knowledge is required.

Any risk deriving from the use of this information and/or the Plugin itself is the responsibility of the recipient who cannot in any case claim the Manufacturer.

All references to systems, people and organizations used in the document are dummy and any resemblance to real situations is purely random and unintended.

Ksenia Security reserves the right to make changes to the Plugin without notice.

Plugin License

License management complies with the requirements of the Milestone Licensing Framework; therefore, the specific license represents an extension of the basic license of the Platform, defined SLC (Software License Code).

The licensing scheme is based on the quantity of Licenses; the different Security Panels of the lares 4.0 family have different weights depending on the capacity, the sum of the weights of the SPs to be managed cannot exceed the total quantity of Licenses. The weights of the various security panels of the family are as follows.

Security Panel Type	License Weight
lares 4.0 16IP	1
lares 4.0 40IP	2
lares 4.0 40IP WLS	2
lares 4.0 WLS 96	2
lares 4.0 140IP WLS	4
lares 4.0 644IP WLS	8

It is therefore recommended, before starting the configuration activities described below, to check the availability of a license through the appropriate "License Information" section of the MC that allows you to configure what you are about to do, to prevent the allowed configuration is partial and must be aborted before completion.

Conventions

The following definitions are used in this document:

- **SECURITY PANEL**: the security panel of the lares 4.0 family to which the peripheral system or part of it belongs
- **SYSTEM**: the set of security panel, peripheral cards and managed objects (zones, partitions, outs, scenarios, etc.)

By convention, the name of the system coincides with that of the security panel.

Protocols and Ports Used

The protocol used by the SPs is WEB Socket and can be used both in clear and encrypted. If the secure protocol (TPS) is used, the control panel acts as a server and the plugin must only recognize and accept the digital certificate.

The following table illustrates the protocols and ports used on different occasions.

Protocol	Port	Use
HTTP	80	Data exchange with the SPs
HTTPS	443	
HTTP	69	Sending Commands to internally managed IP Zones
HTTP	8080	Sending Commands to IP Zones managed through IoT ports
HTTPS	8443	

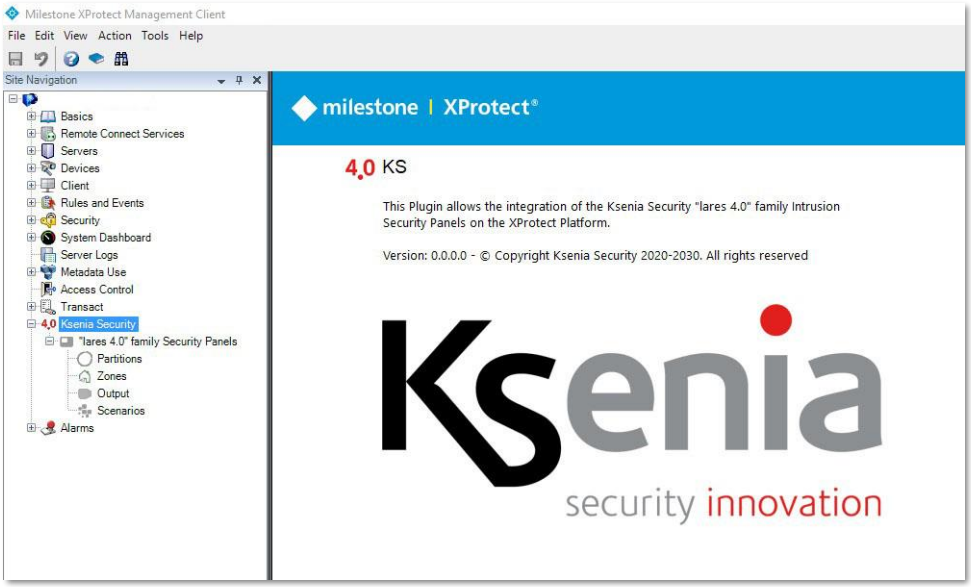
Furthermore, the Plugin uses Ping to verify if there is connectivity with the End Points, whose response must therefore be enabled.

Acronyms

- **DB** Database
- **ES** Event Server
- **MC** Management Client
- **SC** Smart Client
- **SW** Software
- **VMS** Video Management System

1 Intro

This Plugin was developed in order to integrate the security panels of the "lares 4.0" family on Milestone's XProtect VMS platform.

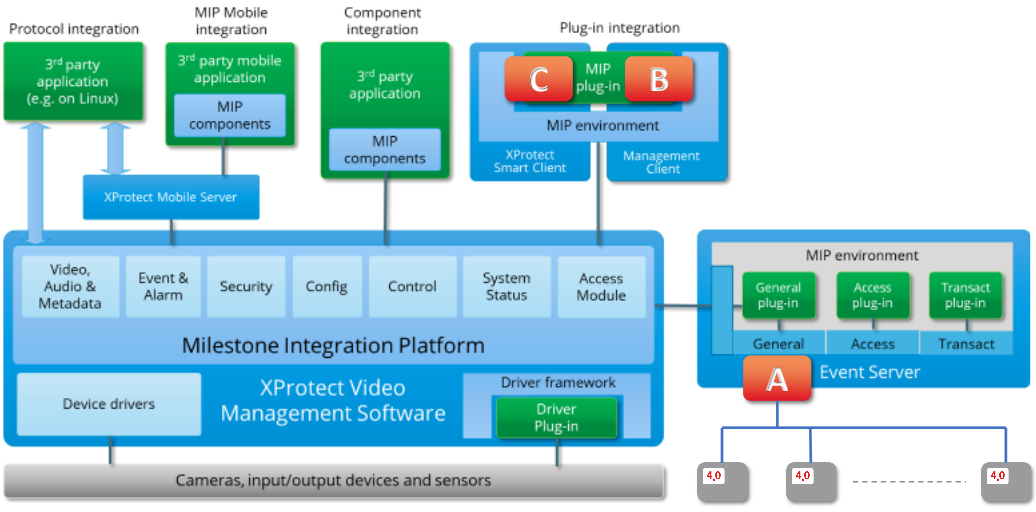


The Plugin is able to completely control, from the Platform where it is installed, a virtually unlimited number of security panels of the family reachable via the network.

In compliance with the access rights to the individual entities established through the Roles menu, the Plugin is able to receive from the controlled units whatever happens on the relevant system, as well as send all the commands allowed to the Users (set, reset, arm, disarm, etc.).

1.1 Plugin Architecture

The following figure illustrates Plugin's Architecture.



The Plugin is basically composed of three distinct parts, each with its own specific tasks, and differs, for some particularities, from the traditional ones indicated in the figure as MIP plug-in.

The traditional part is made up of components B and C which operate respectively in the MC and SC environment; the first for the management of the Configurations, described in this manual, and the second for the Operational management of the Systems, described in the User Manual.

To these two components is added a third, defined A in the figure, which operates in the background, in conjunction with the Event Server from which it is started, and acts as a server for components B and C. This architecture offers the following advantages:

- Only component A communicates with the security panels in the field, thus guaranteeing a virtually infinite number of clients connected at the same time, exceeding the maximum limit of 5 permissions from each control panel
- Component A is always active, even if there are no connected clients, so when the user makes a connection on the platform, typically with the SC, he receives all the information of what happened when the system was unattended
- If changes are made to the configurations of a security panel, the same notifies the event with a dedicated message which, intercepted by component A, causes the configurations to be re-read and the statuses updated, without any intervention by the User via the MC

1.2 Plugin Language

The current version implements Italian and English languages management, the choice of which is automatically linked to the language chosen for the Clients (MC and SC).

If the language chosen for the clients is Italian or English, the Plugin will use one or the other (even different from each other), for any other language chosen the Plugin will use the English language.

2 Plugin Installation

The Plugin has its own installation procedure that creates the specific destination folder, copying all the files necessary for proper operation.

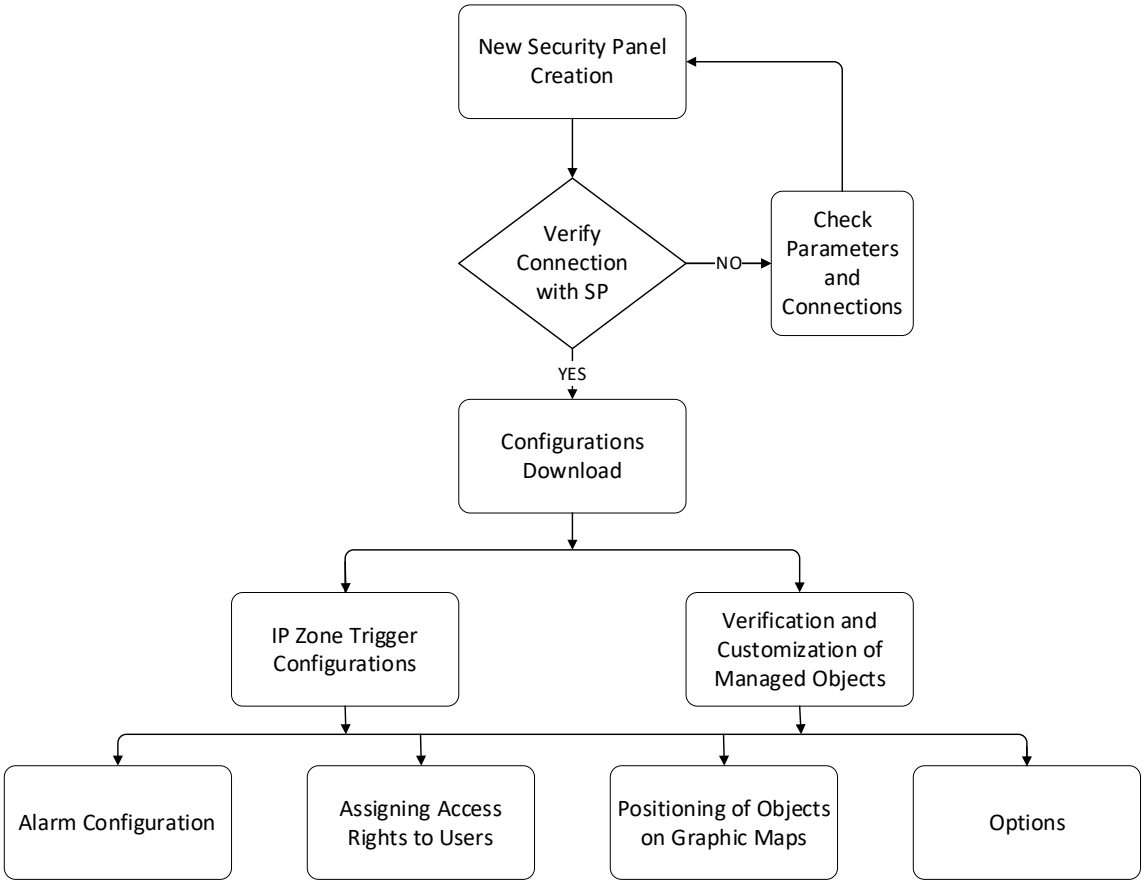
The proposed destination folder is C:\Program Files\Milestone\MIPPlugins\KS; the final KS folder can be changed during the installation itself, although it is recommended to use the proposed name.

In case of updates, the procedure will remove the old version before installing the new one.

3 Plugin Configuration

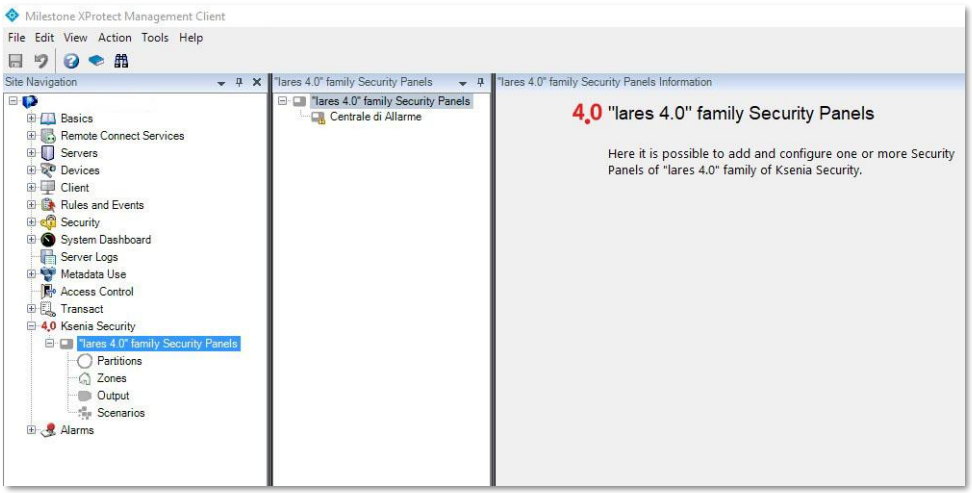
This chapter describes all the steps necessary for the complete configuration of the Plugin. To facilitate the task, all the steps necessary for the complete configuration are illustrated in the next paragraph.

3.1 Configuration Workflow



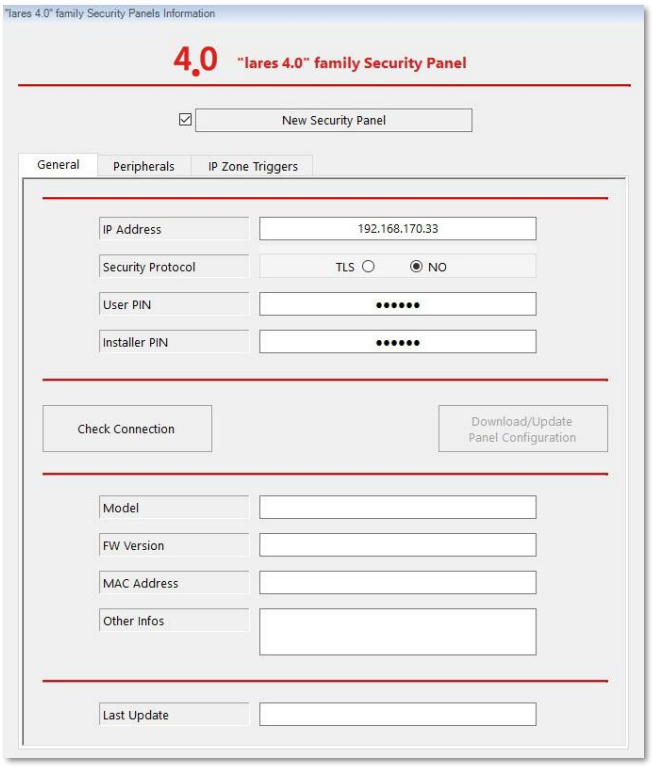
3.2 Adding a Security Panel

As a first operation it is necessary to create a new Security Panel to add to the configurations, to do so select the row of the "lares 4.0" family Security Panels in the navigation tree then right-click on the same line as the central block, or use the combination CTRL+N.

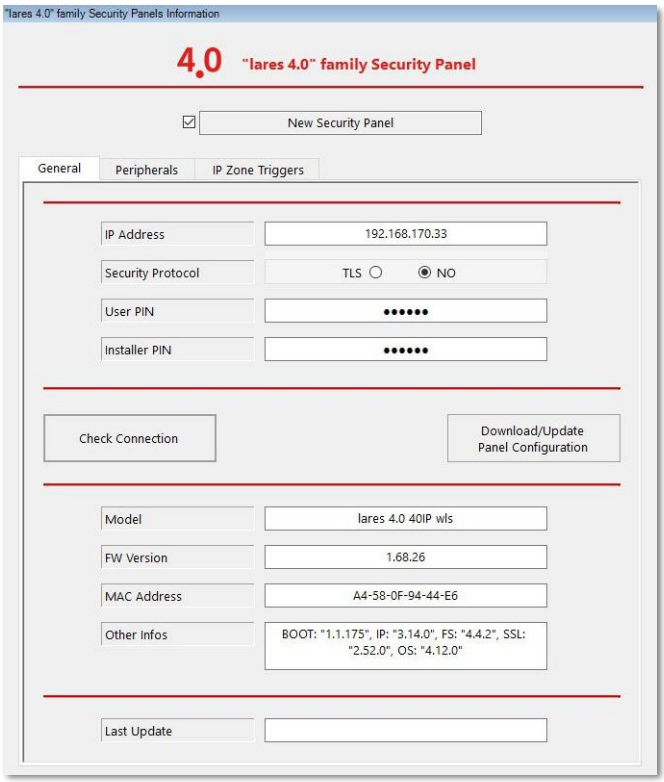


The window for entering the name to be assigned to the new control unit will appear; it is not allowed to insert a name that has already been used, without differentiating case.

Once the control panel name has been confirmed, the screen for entering the connection parameters (IP address, type of protocol, user and installer PIN) will appear.



After entering the parameters, you can check the reachability of the new Security Panel using the "Check Connection" button. If everything is OK, the fields below the button used will be filled.

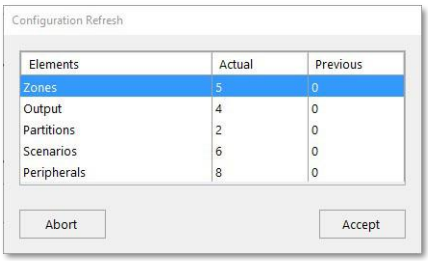


WARNING – Connection verification does not use any of the PINs entered, therefore it does not guarantee their correctness. These PINs are used in the subsequent configuration download phase.

3.2.1 Configurations Download

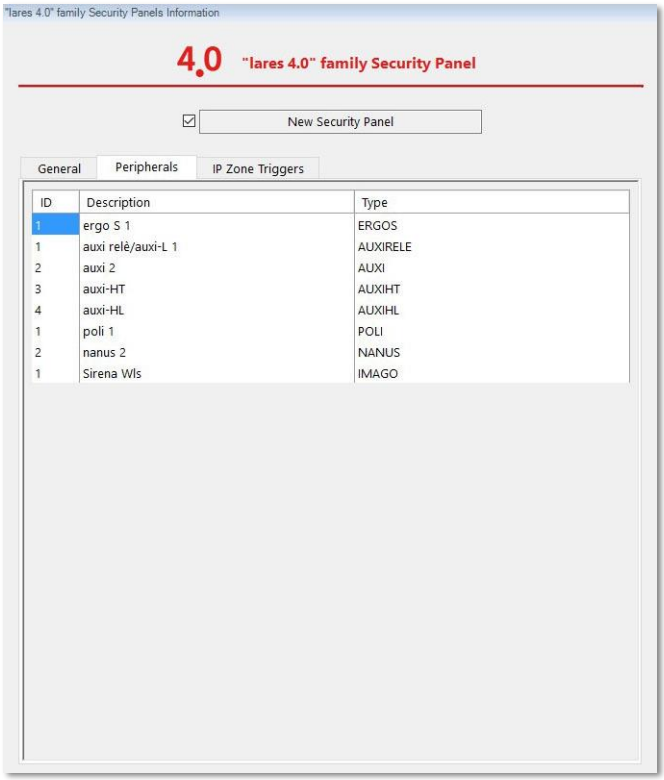
When the Security Panel connection is guaranteed, the configuration download button will be enabled and it will be possible to proceed with this operation.

The operation can last from a few seconds to a few minutes depending on the Security Panel's equipment, at the end a summary window of the elements present in the configuration is showed with the quantities just read and the differences compared to the previous download.



If you accept the configuration just downloaded, the SW creates all the MIP Items (security panel, zones, out, etc.) by registering them in the Platform DB.

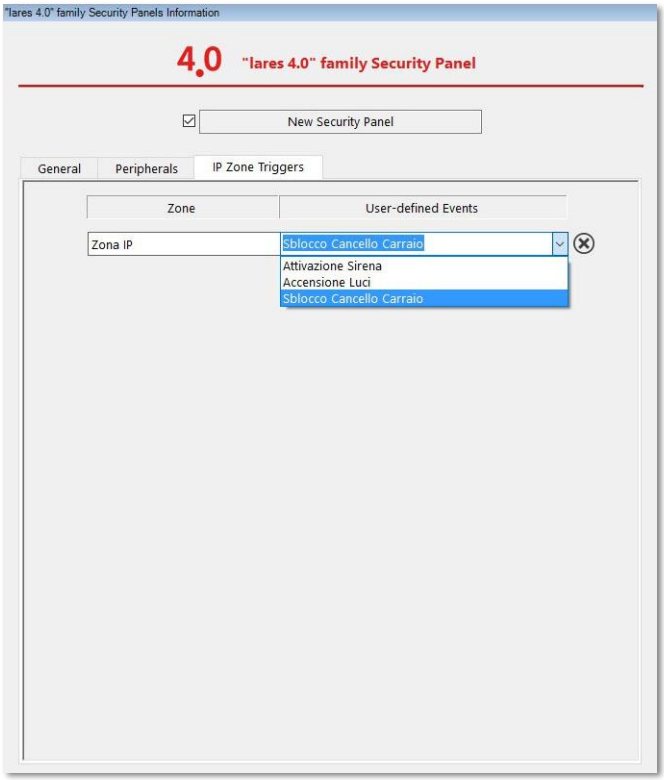
Now it is possible to verify the list of peripherals connected to the Security Panel.



3.2.1.1 IP Zone Triggers

The security panels of the lares 4.0 family have special virtual zones defined as “IP Zones”, since they can be activated via specific network commands. The Plugin automatically sends these commands when "User-Defined Events" configured as Triggers of these Zones occurs.

To proceed with the assignment of the Triggers it is therefore necessary to have defined an User Event for each of the Triggers to be assigned; only after it is possible to assign a Trigger to each IP Zone present in the configuration.

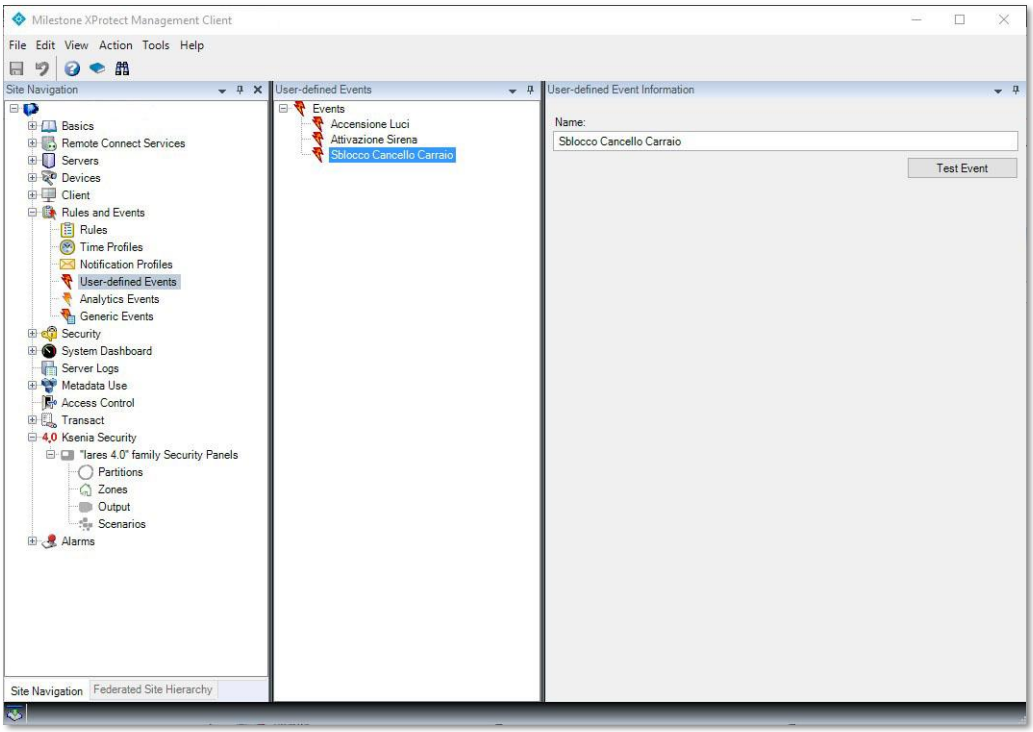


In the previous example, 3 User Events were defined, respectively “Attivazione Sirena” (Siren Activation), “Accensione Luci” (Turning on the Lights) and “Sblocco Cancello Carraio” (Driveway Gate Unlock); the latter is assigned as a Trigger to the only IP Zone present.

If there are multiple IP Zones, the relevant lines will appear for the assignment of the respective Triggers. Of course, Trigger assignments are optional and must be configured only if you want to take advantage of these automatisms.

WARNING – it is not possible to use the same Event for multiple Triggers, that is to associate the same Event to multiple IP Zones; if you need to activate multiple IP Zones when some situation managed by the Platform occurs, as illustrated below, such situation must activate as many User Events as there are IP Zones to be triggered.

It is known that "User-Defined Events" are simple textual labels, as illustrated below.



In order for these Events to be activated by the Platform, it is necessary to define one or more Rules which in turn act as Triggers for the Events themselves.

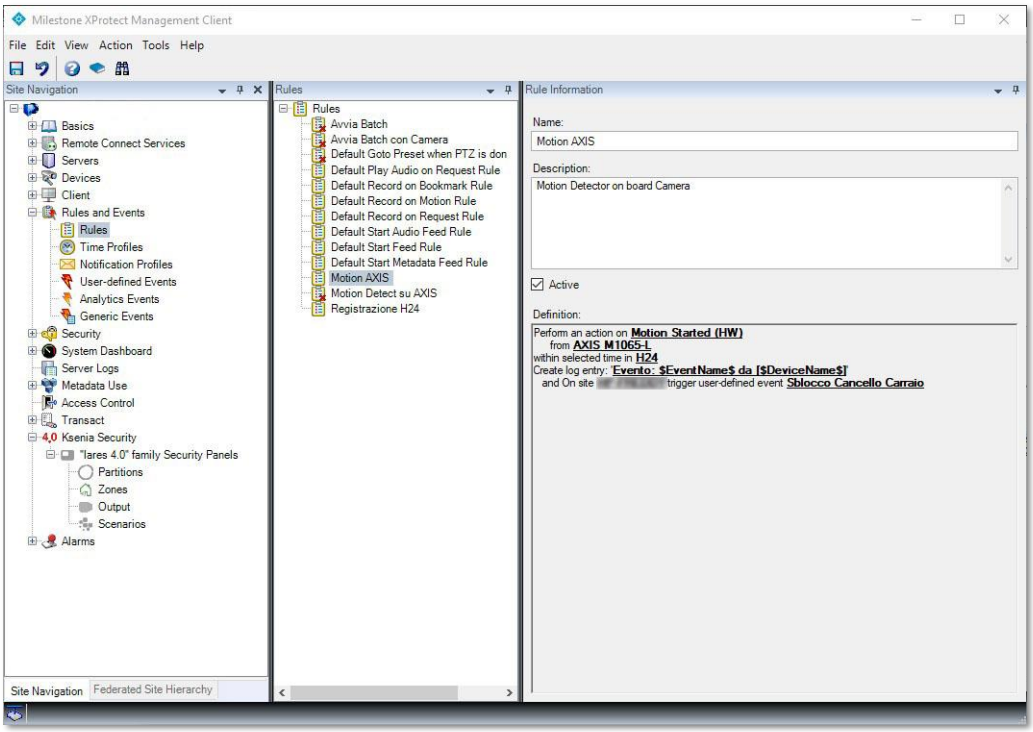
However, thanks to the presence, for each Event, of the "Test Event" button, it is possible to check the correct execution of the mechanism at any time; this button in fact activates the specific Event which, if programmed as a Trigger of an IP Zone, will in turn cause its activation.

3.2.1.1.1 Rules for the Activation of User Events

To activate a User Event, it is necessary to program a Rule that activates it. It is possible to have several Rules with the same origin in order to have this source activate multiple IP Zones; it is also possible to define a Rule that has multiple origins to have several sources activate the same IP Zone.

The programming of the Rules is carried out using the workflow engine present on the platform which offers an infinite number of combinations both in terms of the origin and the conditions in which the Platform is operating.

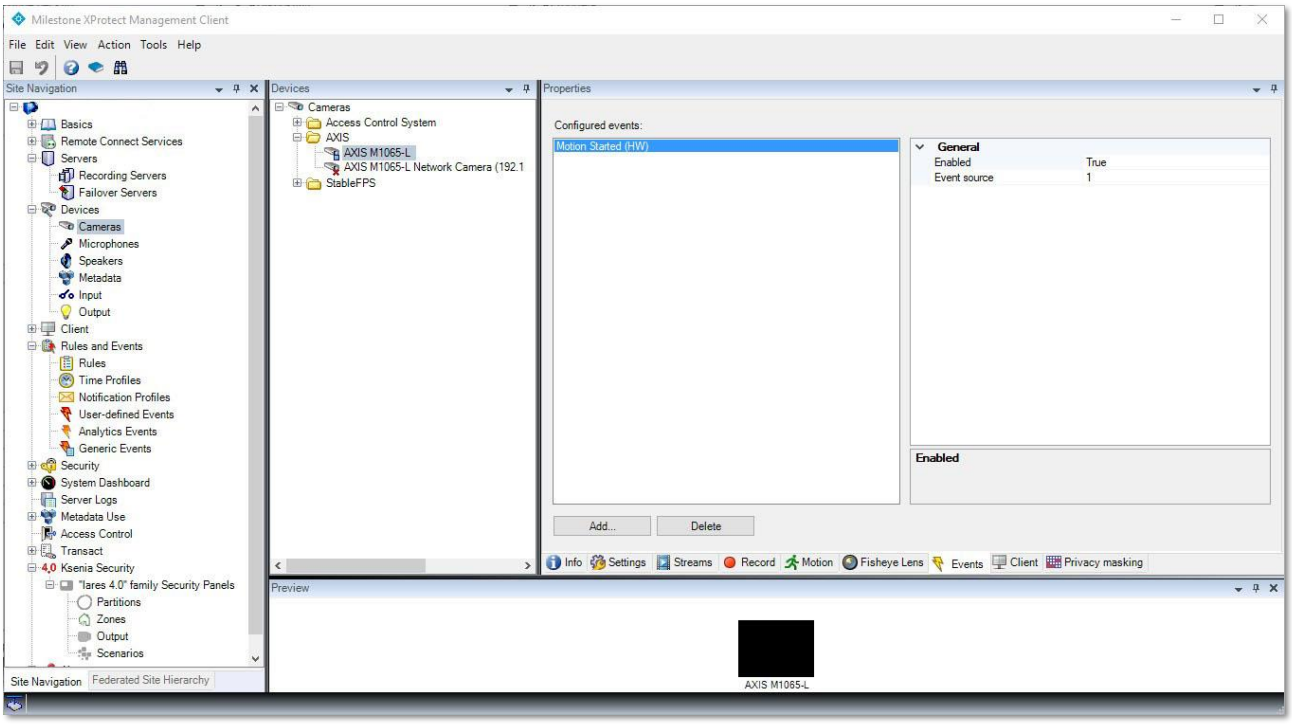
Hereafter some examples of Rules that activate User Events; for a more detailed description, please refer to the specific Milestone documentation.



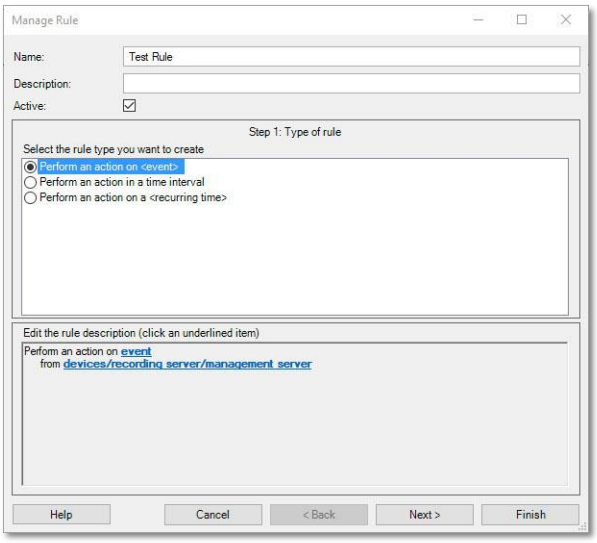
This Rule is activated, without any Hourly restrictions (Time Profile H24), when the algorithm on board the AXIS M1065-L camera detects movement and communicates it to the Platform. The Rule performs 2 distinct actions:

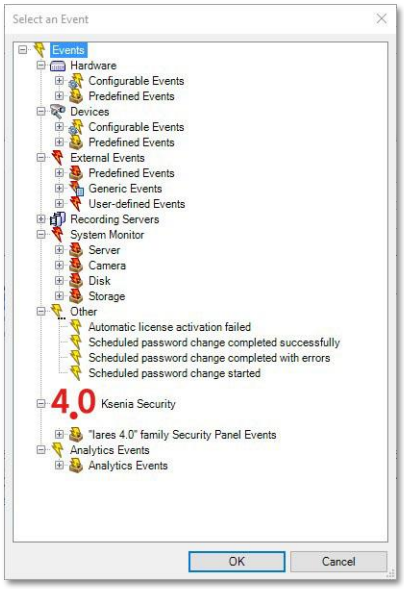
- Create a specific entry in the Register called "Rule-Triggered Logs", the purpose of which is basically diagnostic and is useful for verifying whether activation took place under the required conditions
- Activates the User-defined Event called “Sblocco Cancello Carraio” (Driveway Gate Unlock) which, according to the programming shown above, causes the activation of the IP Zone. In the case of Federated Architecture, it is even possible to define on which of the Federated Sites the User Event should be activated

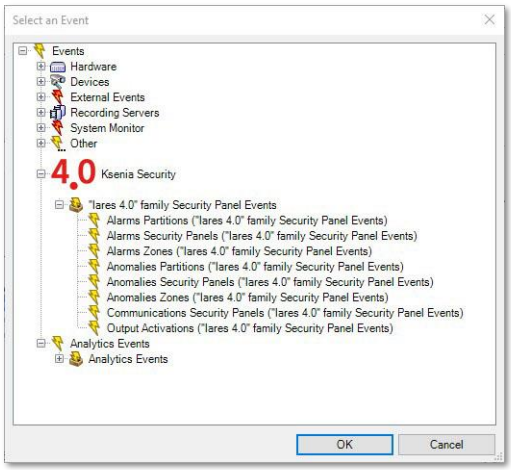
To complete the description below how to make the specific camera generate "Motion Started (HW)"

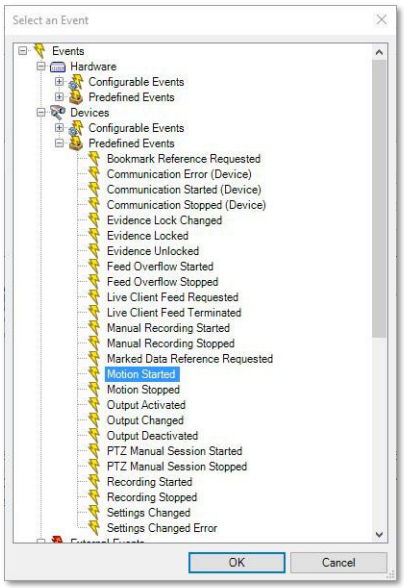


Below are some screenshots that illustrate the potential of the Platform workflow engine, therefore the potential available to create Rules that activate specific User Events, including all those generated by the Security Panels.



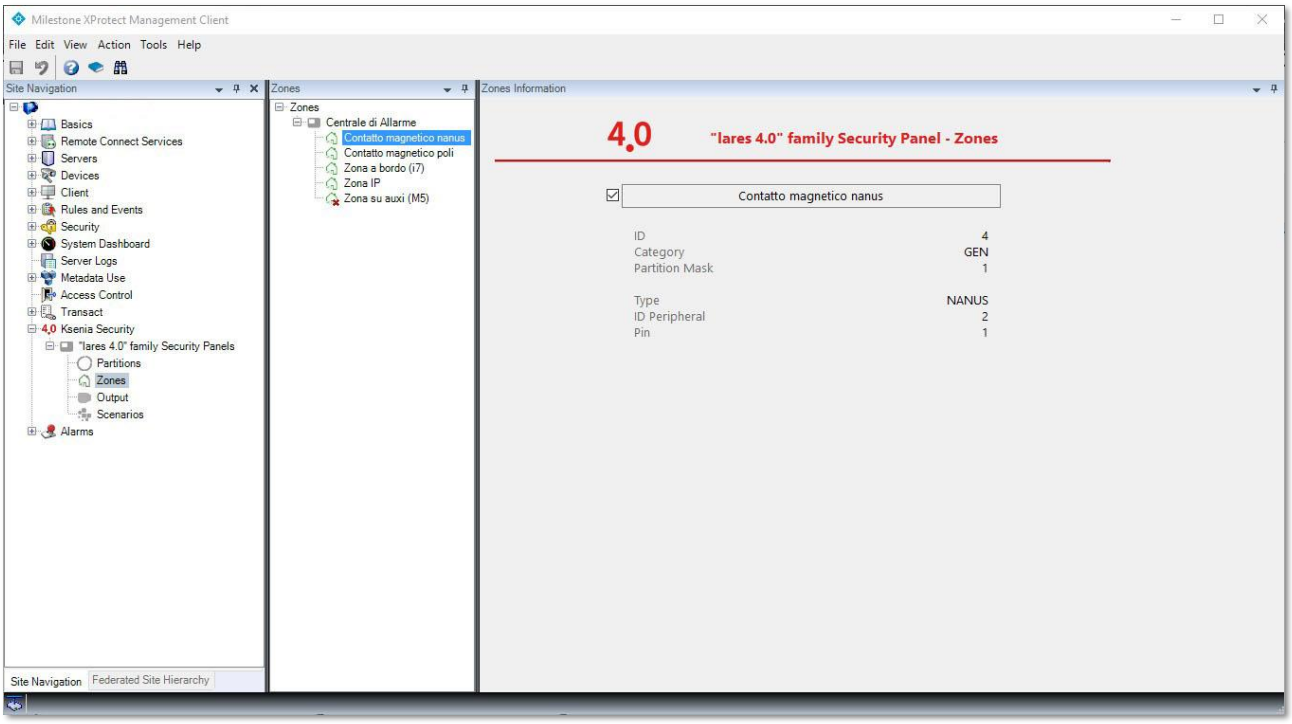


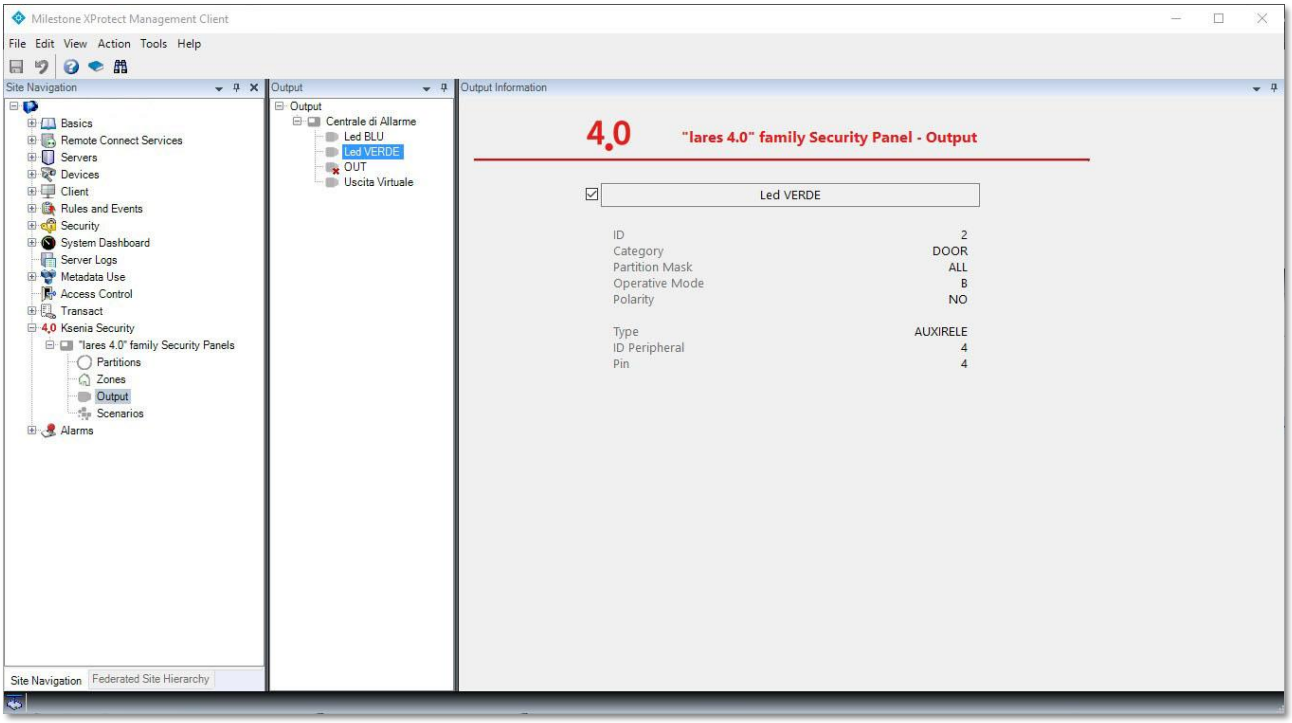




3.2.1.2 Verification and Customization of the Objects controlled by the Security Panel

After downloading the configurations and accepting the result, as reported, the SW creates the MIP Items associated with the Security Panel; these can now be consulted and partially modified.





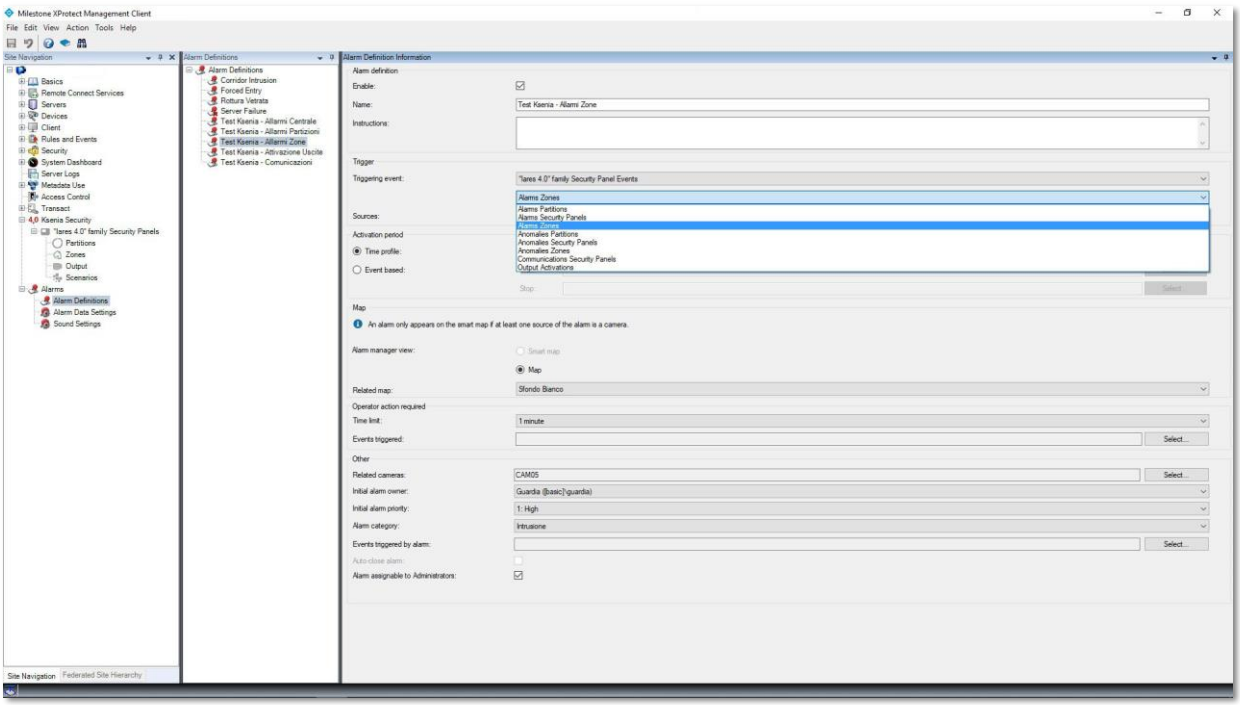
As is evident from the images, it is only possible to enable or disable the Item, all other parameters must be changed on the Security Panel, including the Name used.

3.3 Alarm Configuration

Once the configuration activity is complete, it is possible to proceed with the configuration of the Alarms and the other configurations described below.

For the generation of Alarms, the Plugin provides the following events:

- "lares 4.0" family Security Panel Events
  - Alarms Partitions
  - Alarms Security Panels
  - Alarms Zones
  - Anomalies Partitions
  - Anomalies Security Panels
  - Anomalies Zones
  - Communications Security Panels
  - Outputs Activations

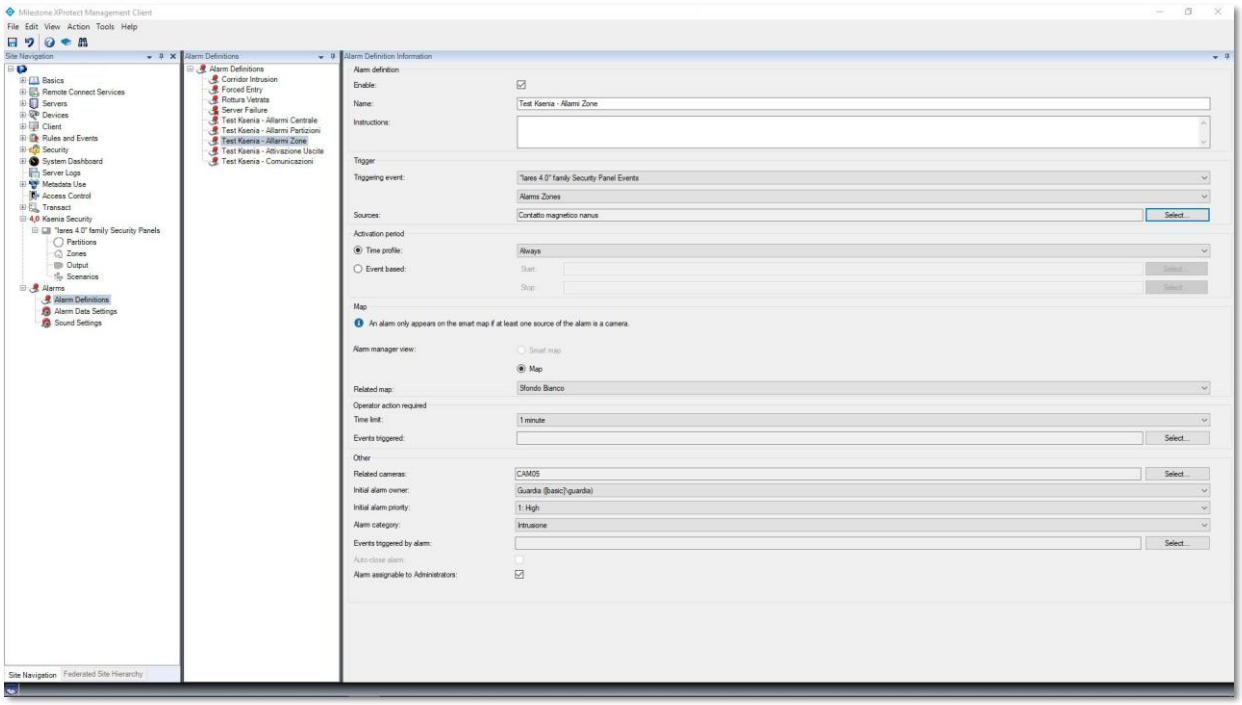


The Events defined Anomalies represent both the Tampering and the Faults, in the case of the Security Panels the latter have different origins, including Peripherals Lost, Power section (Low or Faulty Battery, Low Voltage, etc.).

It is also possible to generate Alarms when Outputs are activated and when there are problems with Communications, both between Plugin and SP, and between SP and other devices.

Below is an example of an alarm generated by the "Contatto magnetico nanus" Zone Alarm.

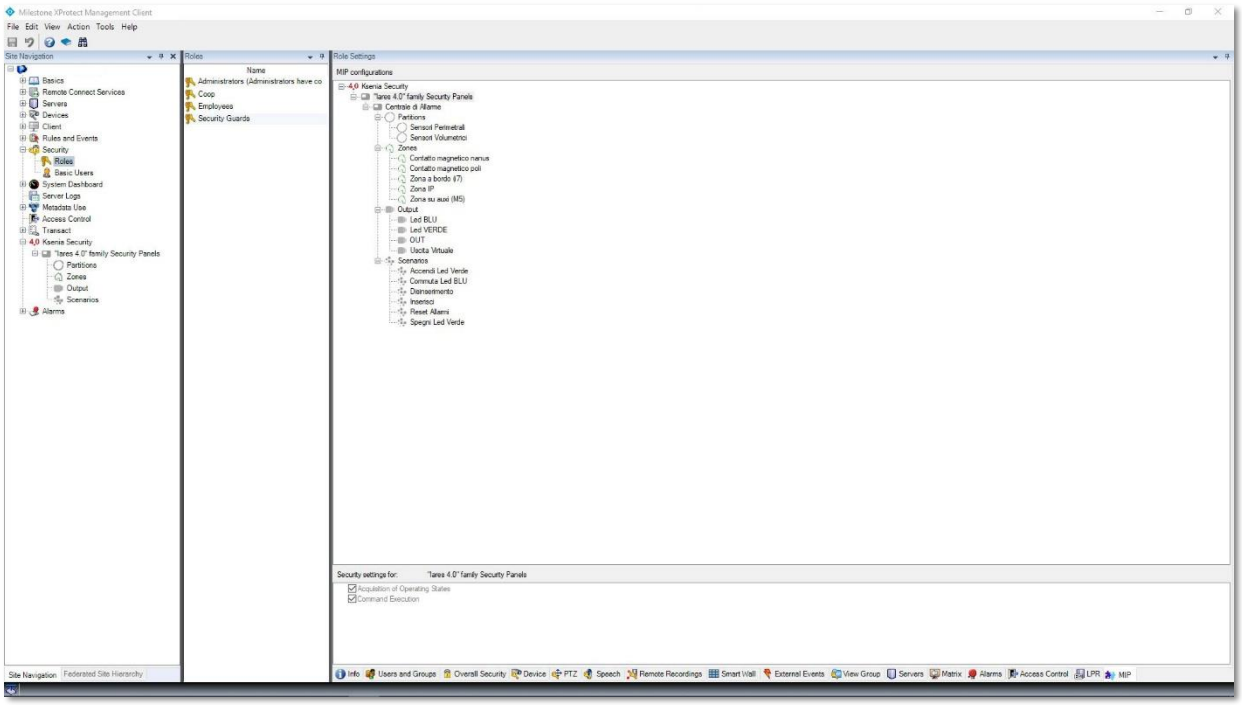
For the various configurable parameters, refer to the specific Milestone documentation.



3.4 Assigning Access Rights to Users

For all the elements that make up the System, it is possible to assign Access Rights to User Profiles, with the exception, as a basic rule of the Platform, to Administration profiles which always have all the Rights.

By default, all Rights are enabled for all Profiles, but you can customize them using the appropriate "Roles" menu; below is a screen that illustrates the various options.



The assignment of Rights is hierarchical, meaning by this that a given assignment to a given level spreads over all the elements of the sub-levels, but it is always possible to customize the underlying levels to ensure that Users are authorized only to the elements of which they have competence; for example, by inhibiting complete access to one or more Scenarios.

There are only two types of Access Rights, the one so-called Reading, identified with the definition "Acquisition of Operating States" and the other for Writing, called "Commands Execution".

WARNING – missing Reading Right automatically excludes Writing Right, regardless of the presence of the check mark on the latter.

If Reading Right of a given Profile is not enabled, all Users with that Profile will not see the item in question, will not receive any notification originating from it and, obviously, will not be able to perform any action involving this item.

Missing Writing Right, as per definition, prevents Users from executing commands on the related Items (set/reset, arm/disarm, etc.). If a non-enabled user tries to execute a given command, a message will appear indicating the reason for refusal.

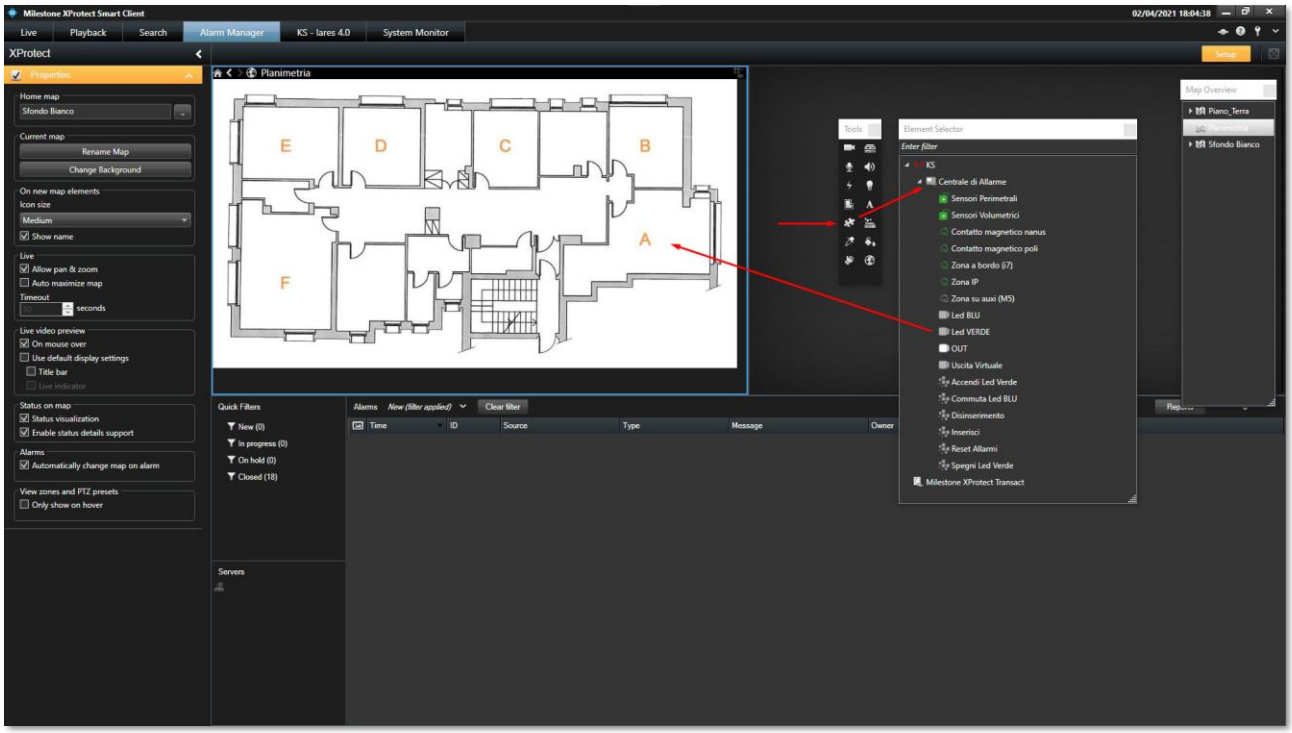
3.5 Positioning of Objects on Graphic Maps

To complete the configuration of a System (security panel and related elements) and make the various functions made available by the Platform usable, it is necessary to create Graphic Maps (not necessarily usable but definitely appropriate) on which to place the elements that make up the System to be to controlled.

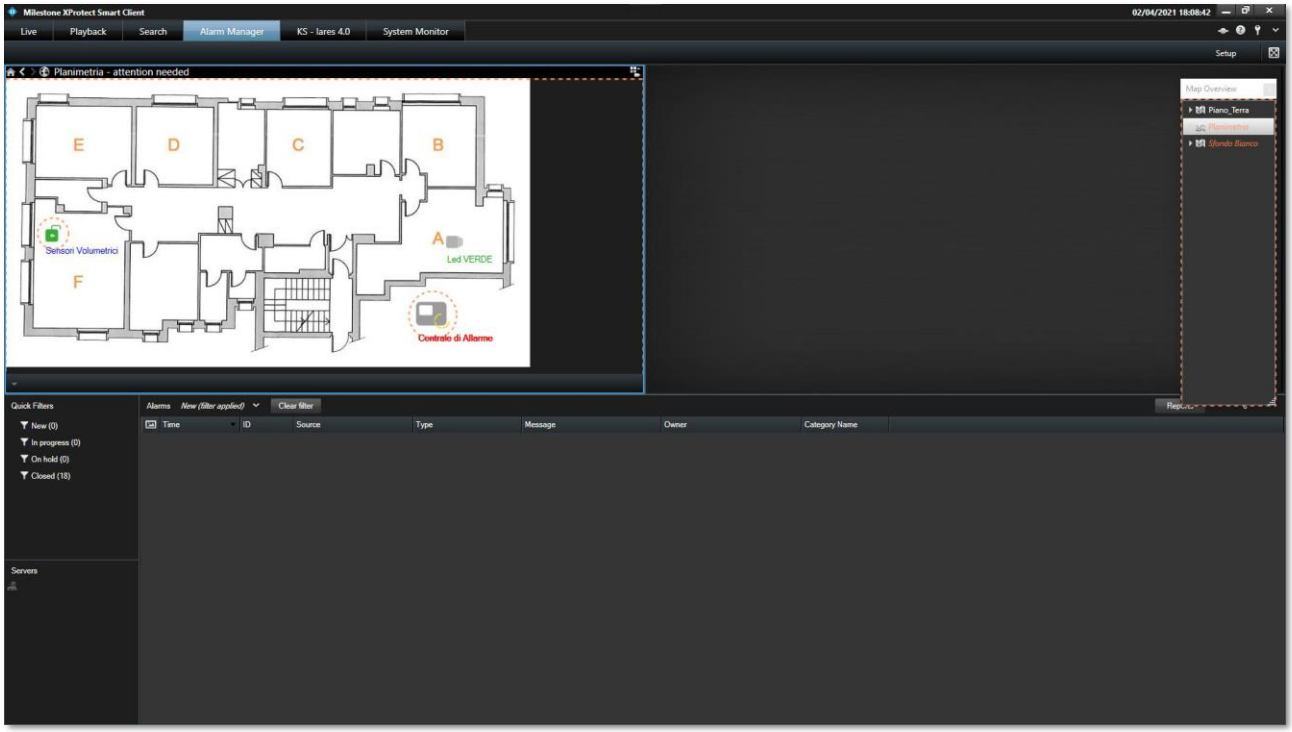
In the following reference will be made to traditional Graphic Maps, but what is illustrated is similarly applicable to the so-called Smart Maps.

These operations must of course be carried out by means of the Smart Client (although these are still Configurations), using a User Profile that allows access to the Settings sections.

Therefore, by selecting the Settings Menu in the Alarms workspace (the same can be performed on the live and/or recorded video workspaces), you select the desired map, then the "Add plug-in element" section, all the elements of the System appear which can be positioned, using drag & drop, on the selected map.



The same operation must be carried out for all elements found within the map; below is an example where a Security Panel (Centrale di Allarme), a Partition (Sensori Volumetrici) and an Output (Led Verde) have been positioned on the map.



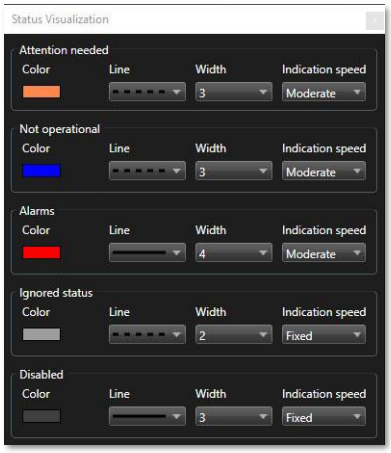
For more details on the positioning of MIP Items on maps, please refer to the specific Milestone documentation.

3.5.1 Status Display Parameter Settings

The Items positioned on the maps provide the Platform with information on their Operating Status according with what is managed by XProtect, in particular, in addition to the Alarm and Quiet states, they are able to communicate the Disabling and Anomaly states.

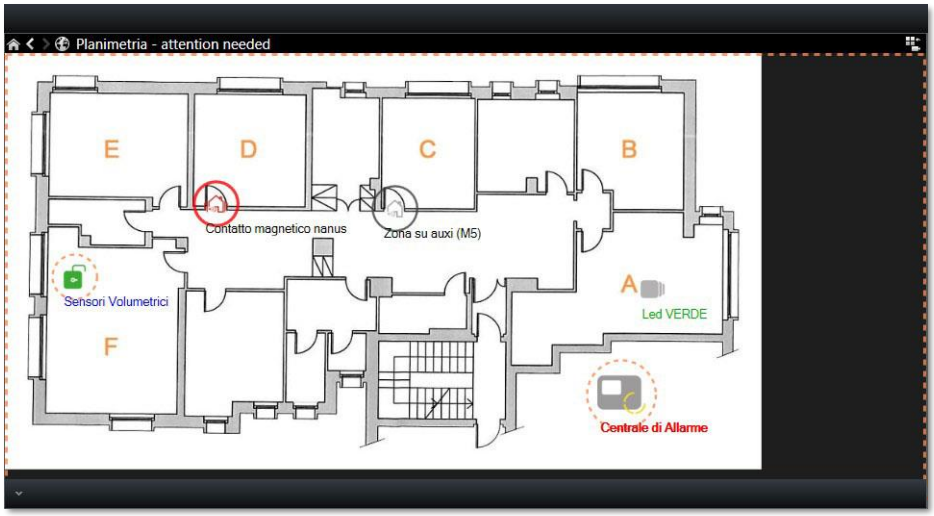
The Platform allows you to associate the different operating states with specific graphic representations of the same by means of circles surrounding the icon of the item on the maps that can have different color, thickness, hatching and flashing speed, to be immediately identified.

It is possible to customize these circles, during the Setup phase, by accessing the Status Visualization menu, shown below.



The Plugin, as above mentioned, in addition to the Alarm and Quiet states, also manages those of "Attention Needed", "Not Operational" and "Disabled"; the second refers to the Offline Control Units while the last obviously refers to an Item that is not enabled on the MC, while the first is linked to the managed Anomalies which, as for the generation of alarms, can be Faults, Tampering condition of "System not Armed" (totally or partially). Of course, this last state may be desired (eg. volumetric sensors in a busy area during the day), but it can be useful for Operators to check, with a glance, the arming status.

Below is an example of a graphical representation of the operating states based on the settings shown in the previous image.



The situation illustrated is the following:

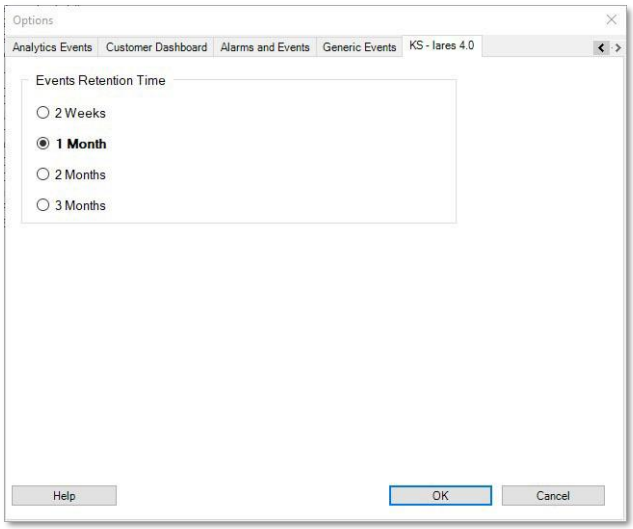
- The "Sensori Volumetrici" Partition is circled in Orange (flashing) since it is Disarmed (not active)
- The “Contatto magnetico nanus” Zone is circled in Red (flashing) because it is in Alarm

- The Zone "Zona su auxi (M5)" is circled in Gray (fixed) because the Item is disabled
- The Security Panel is circled in Orange (flashing) because it is in Battery Fault state
- The Output "Led Verde" is not circled because the Item is in a quiet condition

Finally, it should be noted that the presence of Items with Anomalies (Orange circle) causes the entire map to be surrounded by an Analogous box (Orange flashes) appending after the map title the sentence "attention needed".

3.6 Event Log Retention

Using the Tools => Options menu and selecting the “KS - lares 4.0” tab, you can access the Plugin Options section where you can set the storage duration of the Event Logs (displayed with the SC).

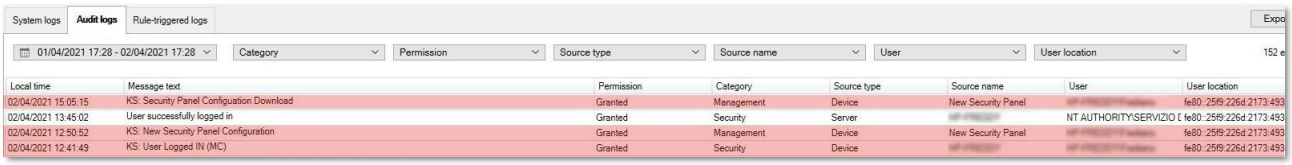


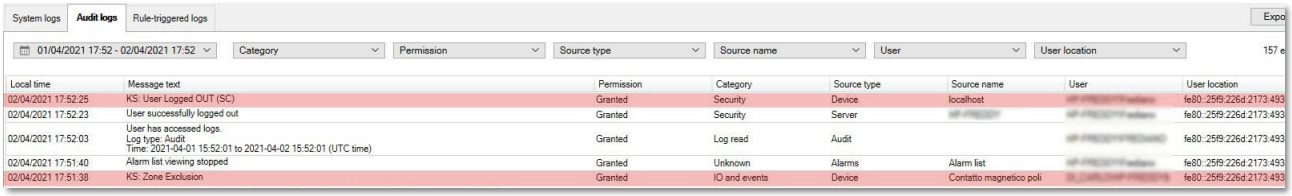
The default value is 1 Month, but 2 Weeks, 2 and 3 Months can also be selected. At the end of the period, the oldest Events are automatically deleted by the SC.

4 Audit Log

The Plugin records all User activities in the Platform Log called "Audit Logs", both for Configuration and for Commands executed on System Elements.

For immediate viewing of these messages, the convention is used that each of them begins with "KS:", as in the following examples, the first referring to the creation of the SP called “New Security Panel” with the MC and the second to inclusion of the “contatto magnetico poli” Zone with the SC.






Ksenia®
security innovation