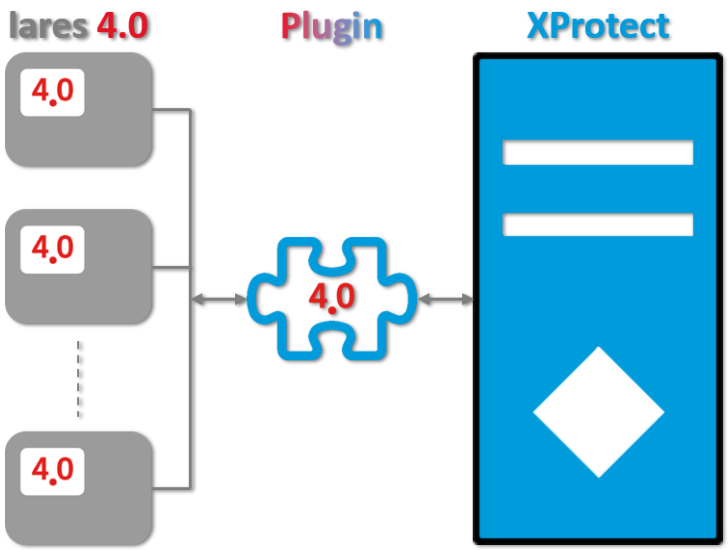
# lares 4.0 MIP Plugin

# Manuale Installazione e Programmazione




Ksenia®
security innovation

www.kseniasecurity.com

Il contenuto del presente documento viene fornito unicamente a scopo informativo, è soggetto a modifica senza preavviso e non deve essere interpretato come un impegno da parte di Ksenia Security.

**INDICE**

Copyright e Limitazioni di Responsabilità ..... 4
Licenza d'Uso del Plugin ..... 4
Convenzioni ..... 5
Protocolli e Porte Utilizzate ..... 5
Acronimi ..... 5

**1 Introduzione ..... 6**
1.1 Architettura del Plugin ..... 6
1.2 Lingua Utilizzata dal Plugin ..... 7

**2 Installazione del Plugin ..... 8**
2.1 Registrazione del certificato radice ..... 8

**3 Configurazione del Plugin ..... 10**
3.1 Workflow di Configurazione ..... 10
3.2 Aggiunta di una Centrale ..... 11
3.2.1 Download delle Configurazioni ..... 13
3.2.1.1 Trigger delle Zone IP ..... 14
3.2.1.1.1 Regole per l'Attivazione degli Eventi Utente ..... 16
3.2.1.2 Verifica e Personalizzazione degli Oggetti controllati dalla Centrale ..... 19
3.3 Configurazione degli Allarmi ..... 20
3.4 Assegnazione Diritti di Accesso agli Utenti ..... 21
3.5 Posizionamento degli Oggetti sulle Mappe Grafiche ..... 22
3.5.1 Impostazioni Parametri Visualizzazione Stato ..... 24
3.6 Durata Conservazione Registro Eventi ..... 25

**4 Log delle Attività ..... 26**

# Copyright e Limitazioni di Responsabilità

© Copyright Ksenia Security 2021-2030. Tutti i diritti sono riservati.

## Limitazioni di Responsabilità

Questo documento è destinato esclusivamente a scopi di informazioni generali del Plugin in oggetto e la sua applicazione alla Piattaforma Milestone XProtect, della quale è richiesta almeno una conoscenza di base.

Qualsiasi rischio derivante dall'uso di queste informazioni e/o del Plugin stesso è di competenza del destinatario che non potrà in alcun caso rivalersi sul Produttore.

Tutti i riferimenti a impianti, persone e organizzazioni utilizzati nel documento sono fittizi e qualsiasi somiglianza con situazioni reali è puramente casuale e non intenzionale.

Ksenia Security si riserva il diritto di apportare modifiche al Plugin senza alcun preavviso.

# Licenza d'Uso del Plugin

Il Plugin implementa la gestione della licenza d'uso conforme ai requisiti del Licensing Framework di Milestone, in modo tale che la specifica licenza rappresenti una estensione della licenza base della Piattaforma, definita SLC (Software License Code). Lo schema di licenza si basa sulla quantità di Licenze; i diversi Pannelli di Sicurezza della famiglia lares 4.0 hanno pesi differenti a seconda della capacità, la somma dei pesi degli SP da gestire non può superare la quantità totale di Licenze. I pesi delle varie centrali della famiglia sono i seguenti.

| Tipo di Centrale | Peso Licenza |
|---|---|
| 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 |

Si raccomanda, pertanto, prima di iniziare le attività di configurazione descritte di seguito, di verificare tramite l'apposita sezione "Informazioni sulla licenza" del MC la disponibilità di una licenza che consenta di configurare quanto ci si accinge a fare, per evitare che la configurazione consentita sia parziale e debba essere interrotta prima del completamento.

**Attenzione! Nel caso in cui si voglia sostituire una centrale lares 4.0 già acquisita nel sistema, indipendentemente dal peso della sua licenza, prima di configurare la nuova occorre disabilitare e/o cancellare quella esistente per liberare le licenze occupate. Le licenze sono gestite dalla piattaforma Milestone e non direttamente dal plugin.**

## Convenzioni

Nel presente documento sono utilizzate le seguenti definizioni:

- **CENTRALE**: la centrale della famiglia lares 4.0 a cui fa capo l'impianto periferico o parte di esso
- **SISTEMA**: l'insieme della centrale, schede periferiche e oggetti gestiti (zone, partizioni, out, scenari, etc.)

Per convenzione il nome del Sistema coincide con quello della Centrale.

## Protocolli e Porte Utilizzate

Il protocollo utilizzato dalle centrali è WEB Socket e può essere utilizzato sia in chiaro che criptato. Se si utilizza il protocollo sicuro (TPS), la centrale funge da server e il plugin deve solo riconoscere e accettare il certificato digitale.

La tabella seguente illustra i protocolli e le porte utilizzati in diverse occasioni.

| Protocollo | Porta | Uso |
|---|---|---|
| HTTP | 80 | Scambio di dati con le Centrali |
| HTTPS | 443 | |
| HTTP | 69 | Invio Comandi alle Zone IP interne |
| HTTP | 8080 | Invio Comandi alle Zone IP gestite attraverso porte IoT |
| HTTPS | 8443 | |

**NOTA IMPORTANTE!**
In caso di centrale con accesso limitato ad Internet (rete protetta dietro firewall), verificare e aggiornare le regole del firewall perché permettano alla centrale di raggiungere:

a. Porta remota: **9443**
b. Protocollo: TCP
c. URL: api.kseniasecureweb.com/*

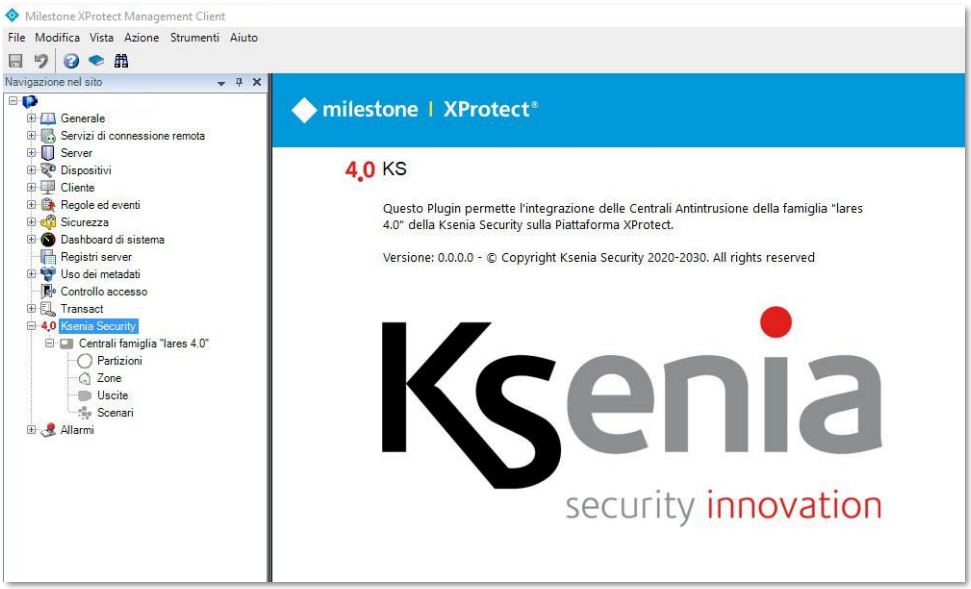
Inoltre, il Plugin utilizza il Ping per verificare se c'è connettività con gli End Point, quindi la risposta deve sempre essere abilitata.

## Acronimi

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

# 1 Introduzione

Questo Plugin è stato sviluppato allo scopo di integrare le centrali della famiglia “lares 4.0” sulla piattaforma VMS XProtect di Milestone.

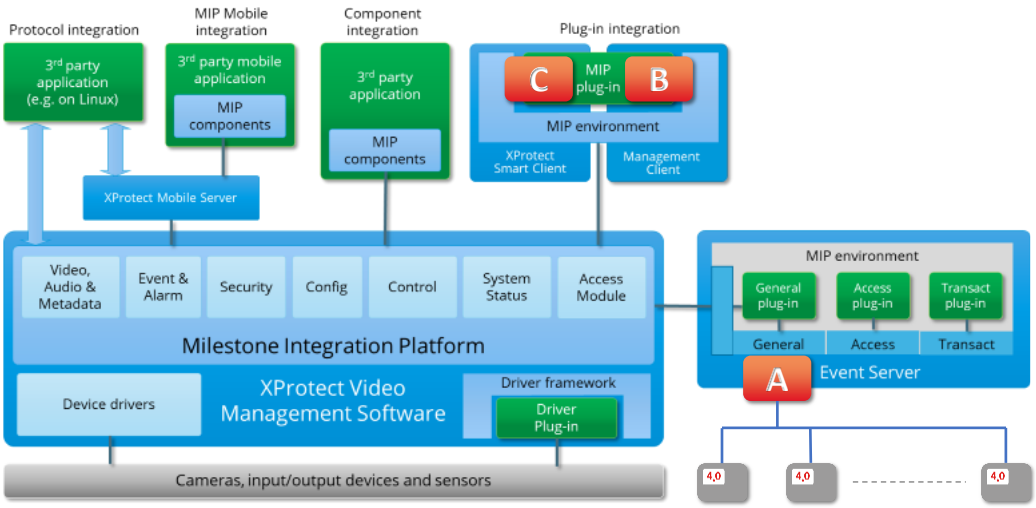



Il Plugin è in grado di controllare completamente, dalla Piattaforma dove è installato, un numero virtualmente illimitato di centrali della famiglia raggiungibili tramite rete.

Nel rispetto dei diritti di accesso alle singole entità stabiliti tramite il menù dei Ruoli, il Plugin è in grado di ricevere dalle centrali controllate qualsiasi cosa accada sul relativo impianto, così come inviare tutti i comandi permessi agli Utenti (set, reset, arm, disarm, etc.).

## 1.1 Architettura del Plugin

La figura seguente illustra l’architettura del Plugin.



Il Plugin è sostanzialmente composto da tre parti distinte, ciascuna con propri compiti specifici, e si differenzia, per alcune particolarità da quelli tradizionali indicati in figura come MIP plug-in.

La parte tradizionale è composta dalle componenti B e C che operano rispettivamente in ambiente MC e SC; la prima per la gestione delle Configurazioni, descritta nel presente manuale e la seconda per la gestione Operativa degli impianti, descritta nel Manuale Utente.

A queste due componenti se ne aggiunge una terza, definita A in figura, che opera in background, in abbinamento all'Event Server da cui viene avviata, e funge da server nei confronti delle componenti B e C. Tale architettura offre i seguenti vantaggi:

- È solo la componente A a colloquiare con le centrali in campo garantendo quindi un numero virtualmente infinito di Client connessi contemporaneamente, superando il limite max di 5 permessi da ciascuna centrale
- La componente A è sempre attiva, anche se non ci sono client connessi, quindi quando l'utente effettua una connessione sulla piattaforma, tipicamente con lo SC, riceve tutte le informazioni di quanto accaduto quando il sistema non era presidiato
- Nel caso si effettuino modifiche alle configurazioni di una centrale la stessa notifica l'evento con un messaggio dedicato che, intercettato dalla componente A, causa la rilettura delle configurazioni e l'aggiornamento degli stati, senza alcun intervento da parte dell'Utente tramite il MC

## 1.2 Lingua Utilizzata dal Plugin

La versione attuale implementa la gestione delle lingue Italiana e Inglese, la cui scelta è automaticamente legata alla lingua scelta per i Client (MC e SC).

Se la lingua scelta per i client è Italiano o Inglese il Plugin utilizzerà l'una o l'altra (anche differenti tra loro), per qualsiasi altra lingua scelta il Plugin utilizzerà la lingua Inglese.

# 2 Installazione del Plugin

Il Plugin dispone di una propria procedura di installazione che crea la specifica cartella di destinazione, copiandoci all'interno tutti i file necessari al corretto funzionamento.

La cartella di destinazione proposta è C:\Programmi\Milestone\MIPPlugins\KS; la cartella finale KS può essere modificata in fase di installazione stessa, sebbene sia consigliato utilizzare il nome proposto.

In caso di aggiornamenti la procedura provvederà alla rimozione della vecchia versione prima di installare la nuova.

## 2.1 Registrazione del certificato radice

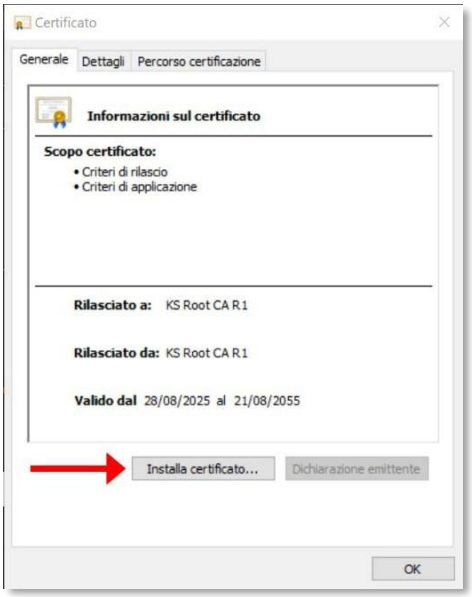
**A partire dalla versione firmware 2.1.X delle centrali lares 4.0**, per la comunicazione con la piattaforma milestone XProtect è richiesto, oltre alla normale installazione del plugin, la registrazione del certificato radice sul server, al fine di garantire la compatibilità tra i sistemi e consentire l'utilizzo del protocollo cifrato TLS.

**La procedura descritta di seguito costituisce quindi un'attività aggiuntiva rispetto all'installazione già consolidata e deve essere eseguita nei casi in cui si operi su centrali con versione firmware uguale o superiore alla 2.1.X**.

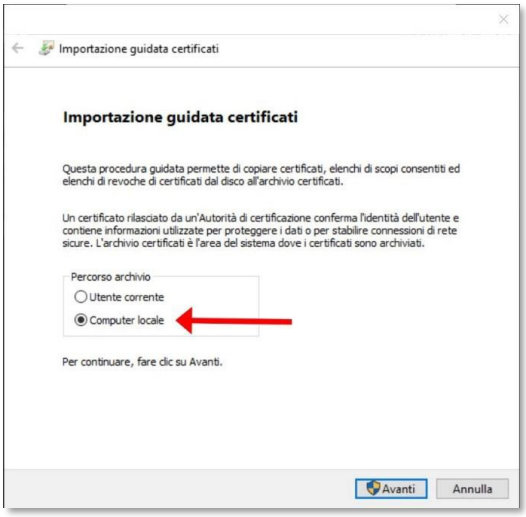
Per il corretto funzionamento della verifica della catena dei certificati, il certificato radice deve essere registrato nello store "Computer locale" del server e non nello store "Utente corrente".

Di seguito i passaggi della registrazione:

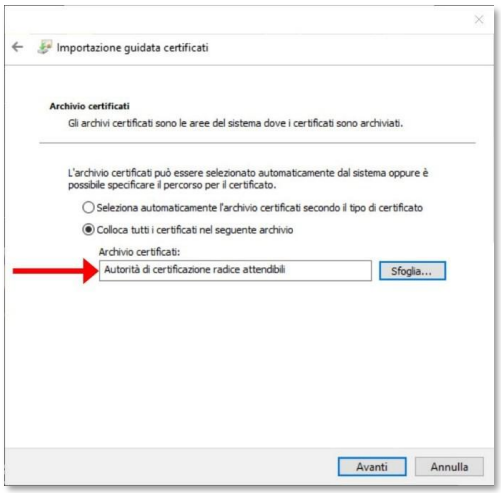
1. Eseguire doppio click sul file **Certificato Radice KS-Root-CA-R1-cert.crt** appena scaricato, quindi cliccare sul bottone "Installa certificato…"



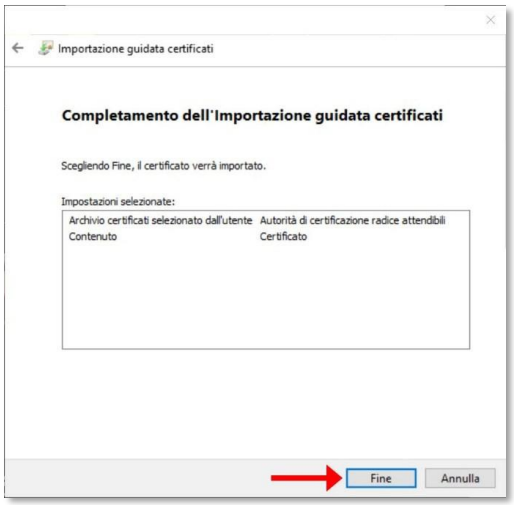

2. Selezione dello Store "Computer locale"




3. Selezione archivio “Autorità di certificazione radice attendibili”



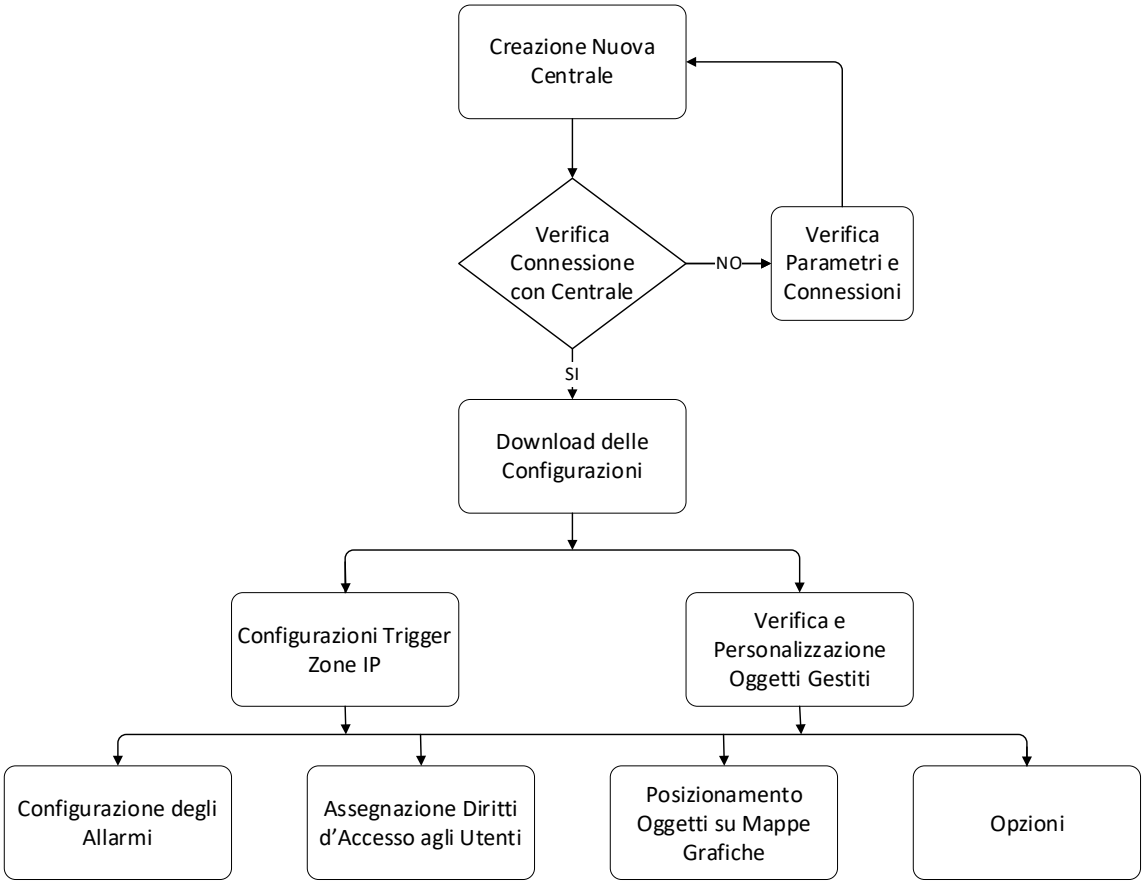

4. Completamento dell’operazione



# 3 Configurazione del Plugin

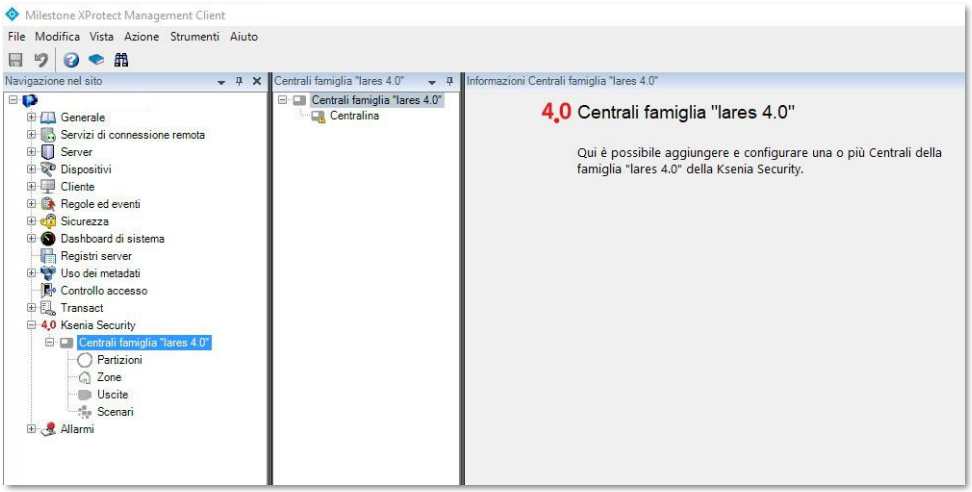
In questo capitolo sono descritti tutti i passaggi necessari alla completa configurazione del Plugin. Per facilitare il compito nel prossimo paragrafo sono riportati tutti gli step necessari alla configurazione completa.

## 3.1 Workflow di Configurazione

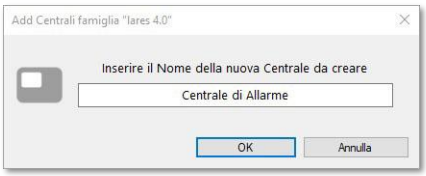


## 3.2 Aggiunta di una Centrale

Come prima operazione è necessario creare una nuova centrale da aggiungere alle configurazioni, per farlo selezionare la riga delle Centrali famiglia “lares 4.0” dell’albero di navigazione quindi fare click con il destro sulla stessa riga del blocco centrale, oppure utilizzare la combinazione CTRL+N.



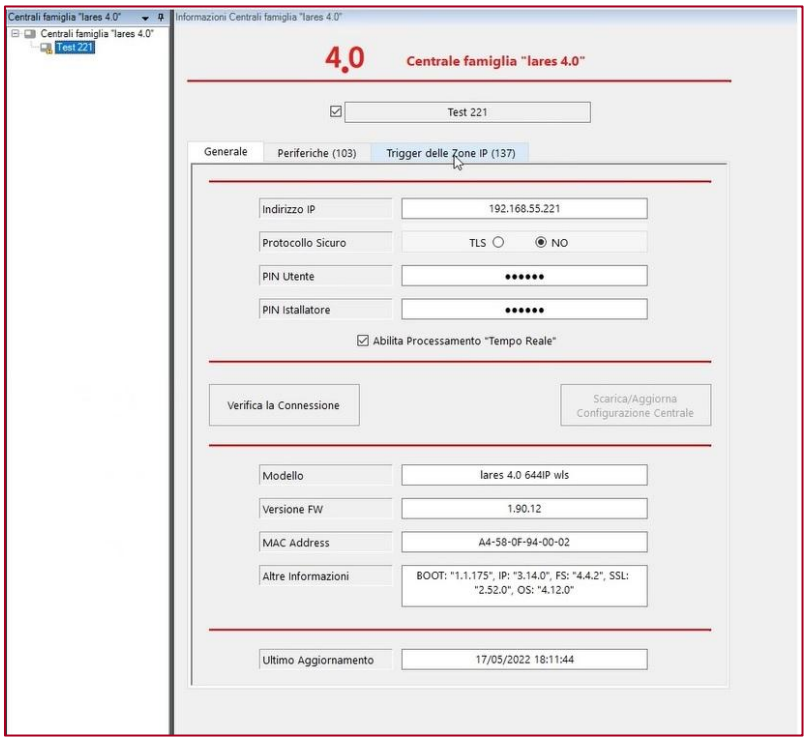

Apparirà la finestra per l’inserimento del nome da assegnare alla nuova centrale; non è consentito inserire un nome già utilizzato, senza differenziare maiuscole/minuscole.




Una volta confermato il nome della centrale apparirà la schermata di inserimento dei parametri di collegamento (Indirizzo IP, tipo di Protocollo, PIN Utente e Installatore).




Dopo l'inserimento dei parametri è possibile verificare la raggiungibilità della nuova centrale utilizzando il tasto "Verifica la Connessione". Se è tutto OK si popoleranno i campi sottostanti il tasto utilizzato.




**ATTENZIONE** – la verifica della connessione non utilizza alcuno dei PIN immessi, pertanto non ne garantisce la correttezza. Tali PIN sono utilizzati nella fase successiva di download delle configurazioni.

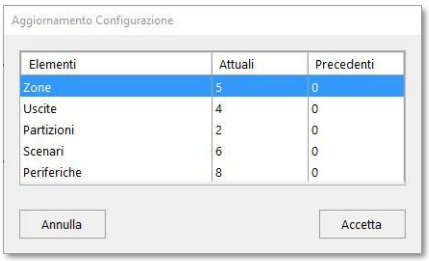
Il pannello di creazione di una nuova centrale contiene, tra le altre, le seguenti informazioni aggiunte con il rilascio del Plugin di Milestone a maggio 2022:

1. Nuova flag "**Abilita processamento Tempo reale**" (abilitata di default):
   l'opzione abilitata permette di visualizzare in tempo reale le variazioni di stato di tutte le zone anche ad impianto disinserito.
   In caso di grandi impianti che gestiscono un numero elevato di zone, da cui possono provenire frequenti variazioni di stato con zona disinserita, si consiglia di disabilitare la flag per migliorare le prestazioni del sistema; in tal modo vengono visualizzate le variazioni solo agli allarmi effettivi. Ovviamente ad impianto disinserito continuano ad essere gestiti gli allarmi generati da zone 24h.
2. Numero delle **Periferiche** (accanto al nome del Tab):
   dopo aver cliccato sul tasto "Scarica/Aggiorna Configurazione Centrale", viene visualizzato il numero totale delle periferiche presenti in configurazione.
3. Numero dei **Trigger delle zone IP** (accanto al nome del Tab):
   dopo aver cliccato sul tasto "Scarica/Aggiorna Configurazione Centrale", viene visualizzato il numero totale delle zone IP presenti in configurazione.

### 3.2.1 Download delle Configurazioni

Quando si ha la garanzia di raggiungibilità della Centrale si abilita il tasto di download delle configurazioni ed è possibile procedere con tale operazione.

L'operazione può durare da alcuni secondi ad alcuni minuti in funzione dell'equipaggiamento della centrale, al termine viene presentata una finestra di riepilogo degli elementi presenti nella configurazione con i quantitativi appena letti e le differenze rispetto al precedente download.




Se si accetta la configurazione appena scaricata il SW provvede alla creazione di tutti gli Item MIP (centrale, zone, out, etc.) registrandoli nel DB della piattaforma.

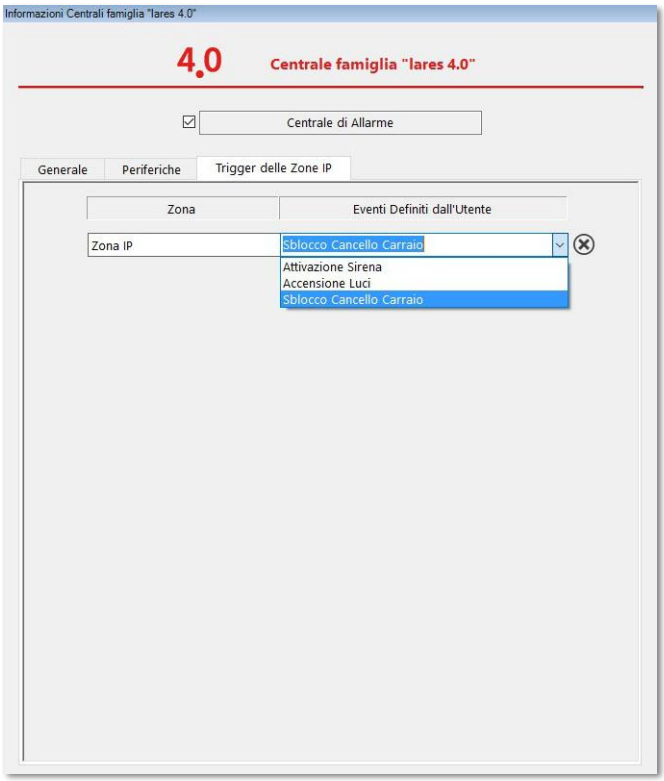
A questo punto è possibile verificare l'elenco delle Periferiche collegate alla Centrale.




#### 3.2.1.1 Trigger delle Zone IP

Le centrali della famiglia lares 4.0 dispongono di particolari Zone virtuali definite “Zone IP”, poiché le stesse sono attivabili tramite specifici comandi di rete. Il Plugin provvede all’invio automatico di tali comandi quando si verificano “Eventi definiti dall’Utente” configurati come Trigger di tali Zone.

Per procedere con l’assegnazione dei Trigger è pertanto necessario aver definito un Evento Utente per ciascuno dei Trigger da assegnare; fatto ciò è possibile assegnare un Trigger a ciascuna Zona IP presente nella configurazione.

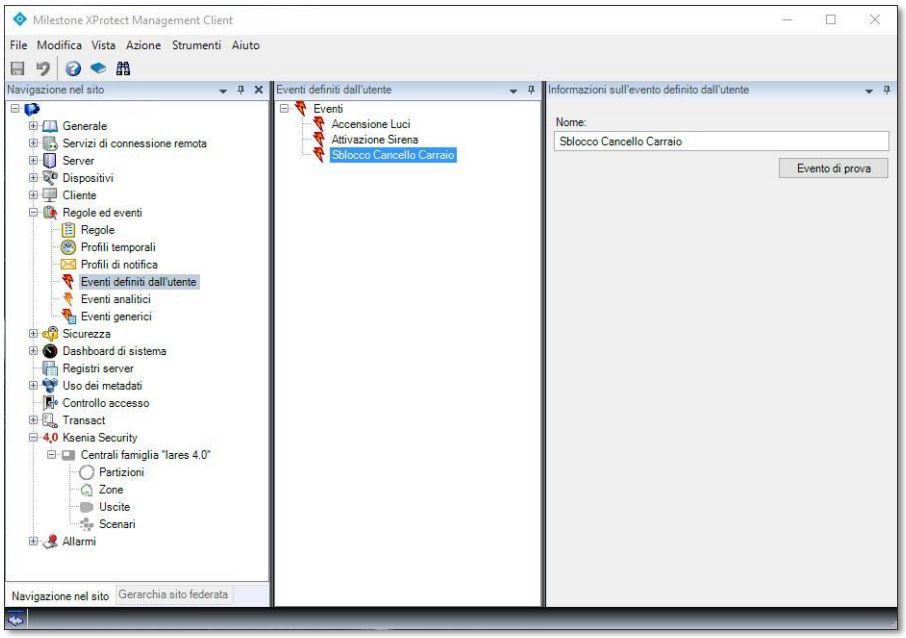



Nell'esempio precedente sono stati definiti 3 Eventi Utente, rispettivamente "Attivazione Sirena", "Accensione Luci" e "Sblocco Cancello Carraio"; quest'ultimo viene assegnato come Trigger all'unica Zona IP presente.

Nel caso siano presenti più Zone IP compariranno le relative righe per l'assegnazione dei rispettivi Trigger. Naturalmente le assegnazioni dei Trigger sono facoltative e devono essere configurate solo se si intende sfruttare tali automatismi.

**ATTENZIONE** – non è possibile utilizzare lo stesso Evento per più Trigger, ossia associare lo stesso Evento a più Zone IP; nel caso si desideri attivare più Zone IP quando accade qualcosa gestito dalla Piattaforma, come illustrato di seguito, è necessario che quello che accade attivi tanti Eventi Utente quante sono le Zone IP da attivare.

È noto che gli "Eventi definiti dall'Utente" sono delle semplici etichette testuali, come illustrato di seguito.




Affinché tali Eventi siano attivati dalla Piattaforma è necessario definire una o più Regole che a loro volta fungono da Trigger degli Eventi stessi.

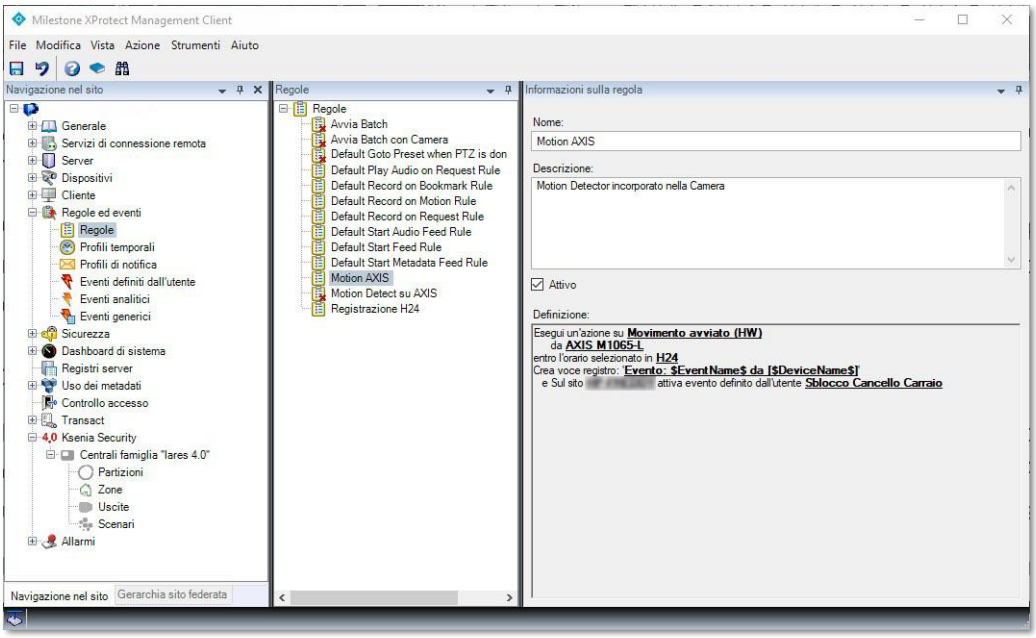
Grazie comunque alla presenza, per ciascun Evento, del tasto “Evento di prova” è possibile verificare in qualsiasi momento la corretta esecuzione del meccanismo; tale tasto infatti attiva lo specifico Evento che, se programmato come Trigger di una Zona IP, ne causerà a sua volta l’attivazione.

#### 3.2.1.1.1 Regole per l’Attivazione degli Eventi Utente

Per attivare un Evento Utente è necessario programmare una Regola che provvede ad attivarlo. È possibile fare in modo che più Regole abbiano la stessa origine per fare in modo che tale origine attivi più Zone IP, così come è possibile definire una Regola che abbia più origini per fare in modo che più origini attivino una stessa Zona IP.

La programmazione delle Regole viene effettuata utilizzando il motore di workflow presente sulla piattaforma che offre, di fatto, una infinità di combinazioni sia per quanto riguarda l’origine, sia le condizioni in cui si trova la Piattaforma.

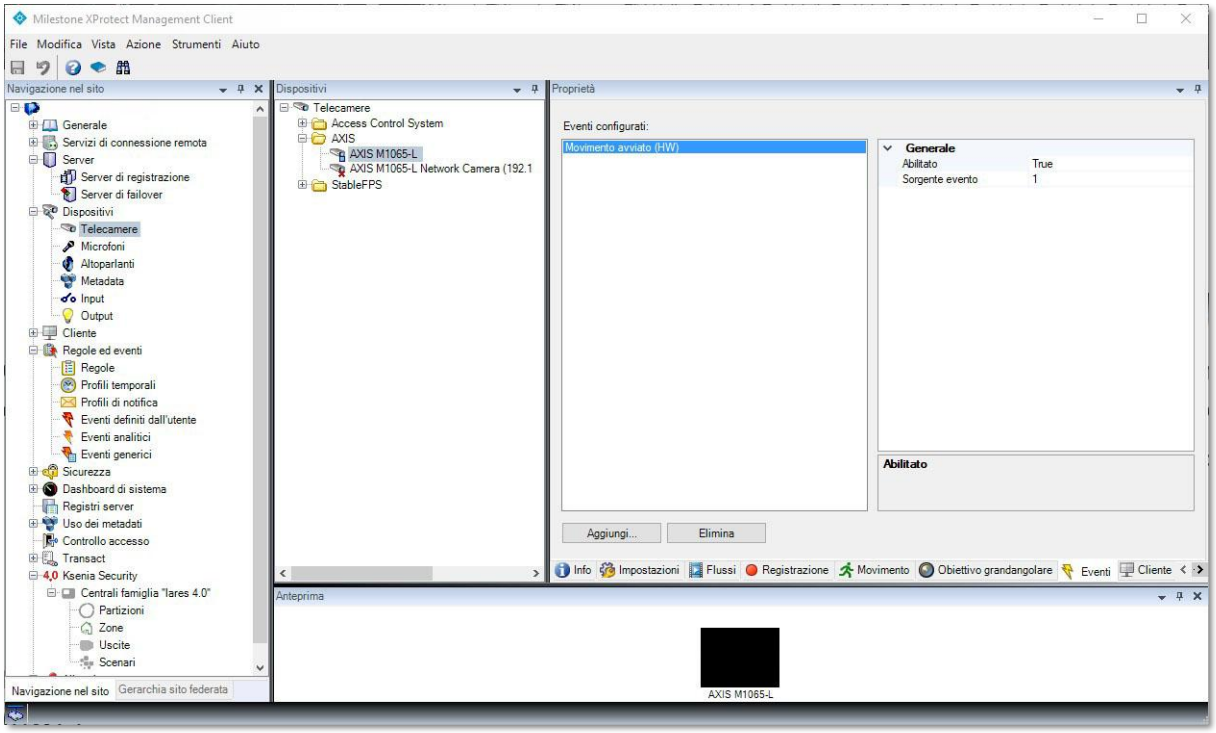
Di seguito alcuni esempi di Regole che attivano Eventi Utente; per una descrizione più dettagliata si rimanda alla specifica documentazione Milestone.



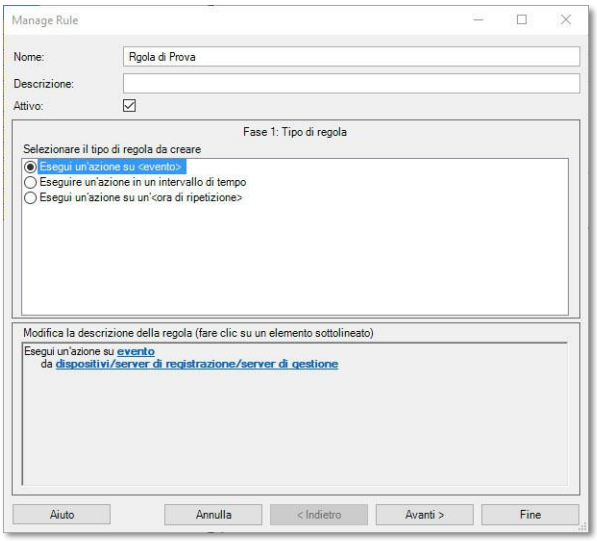

Questa Regola viene attivata, senza alcuna restrizione Oraria (Profilo Temporale H24), quando l'algoritmo a bordo della camera AXIS M1065-L rileva movimento e lo comunica alla Piattaforma. La Regola compie 2 distinte azioni:

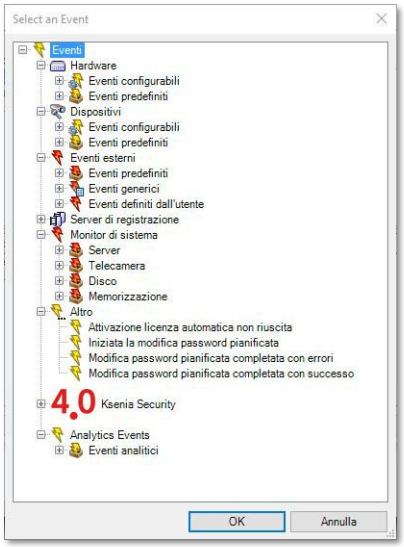
- Crea una specifica voce nel Registro chiamato "Registri attivati da regole", il cui scopo è fondamentalmente diagnostico e torna utile per verificare se l'attivazione è avvenuta nelle condizioni richieste
- Attiva l'Evento definito dall'Utente chiamato "Sblocco Cancello Carraio" che, in base alle programmazioni mostrate in precedenza, causa l'attivazione della Zona IP. Nel caso di Architettura Federata è possibile perfino definire su quale dei Siti Federati debba essere attivato l'Evento Utente

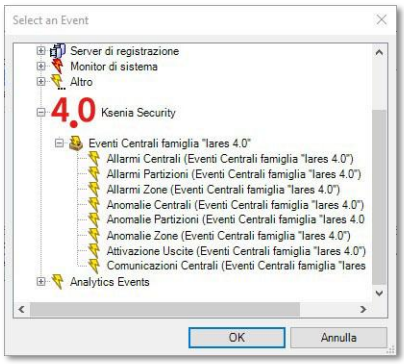
Per completare la descrizione di seguito come fare in modo che la specifica telecamera generi "Movimento avviato (HW)".

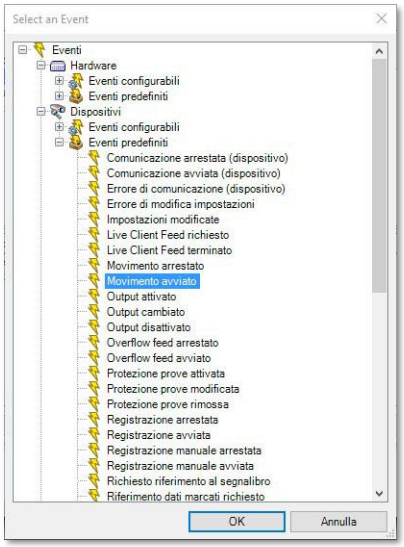


Di seguito alcune schermate che illustrano le potenzialità del motore di workflow della Piattaforma, quindi le potenzialità di cui si dispone per creare Regole che attivino specifici Eventi Utente tra i quali anche tutti quelli generati dalla Centrale.



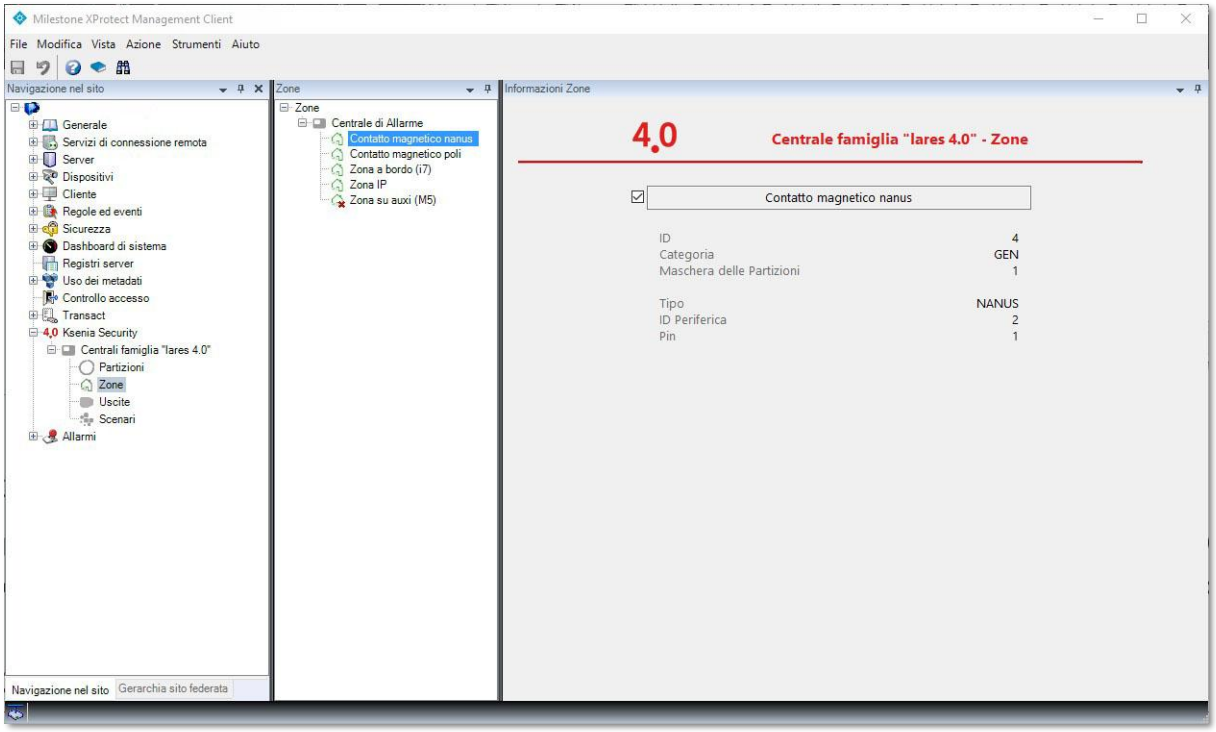



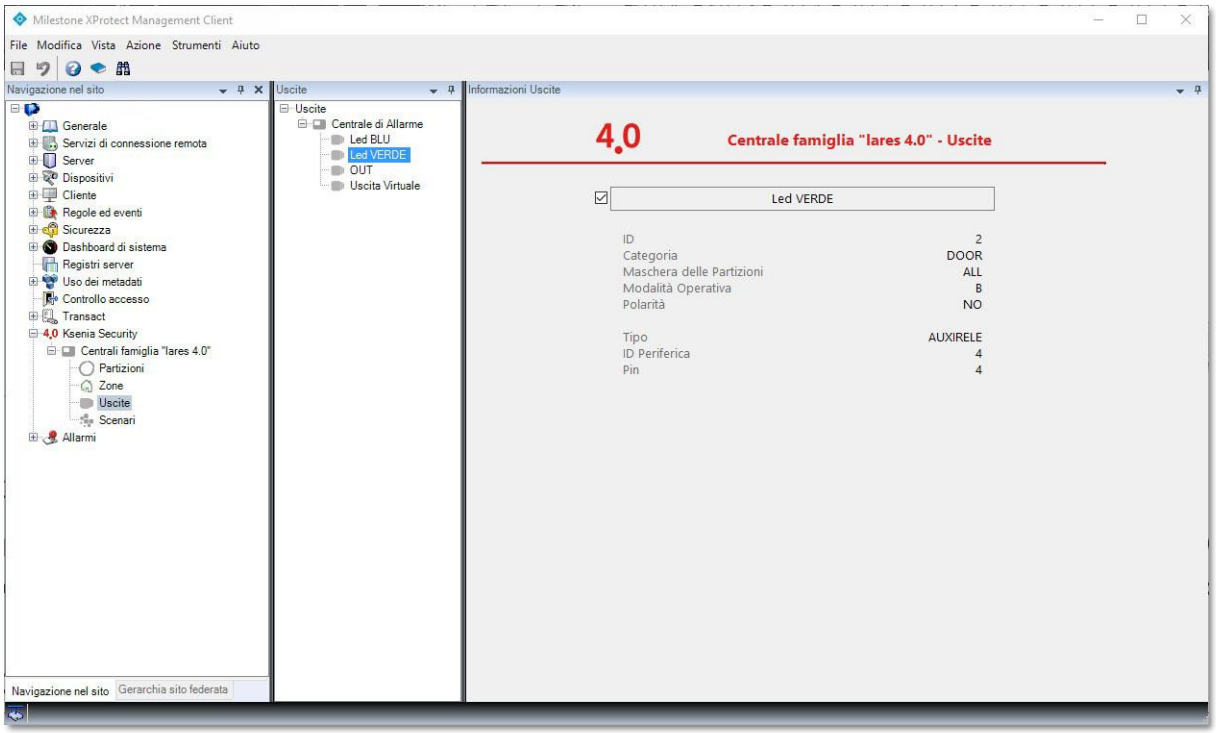



### 3.2.1.2 Verifica e Personalizzazione degli Oggetti controllati dalla Centrale

Dopo aver effettuato il download delle configurazioni ed aver accettato il risultato, come riferito, il SW provvede alla creazione degli Item MIP associati alla Centrale; questi possono ora essere consultati e parzialmente modificati.



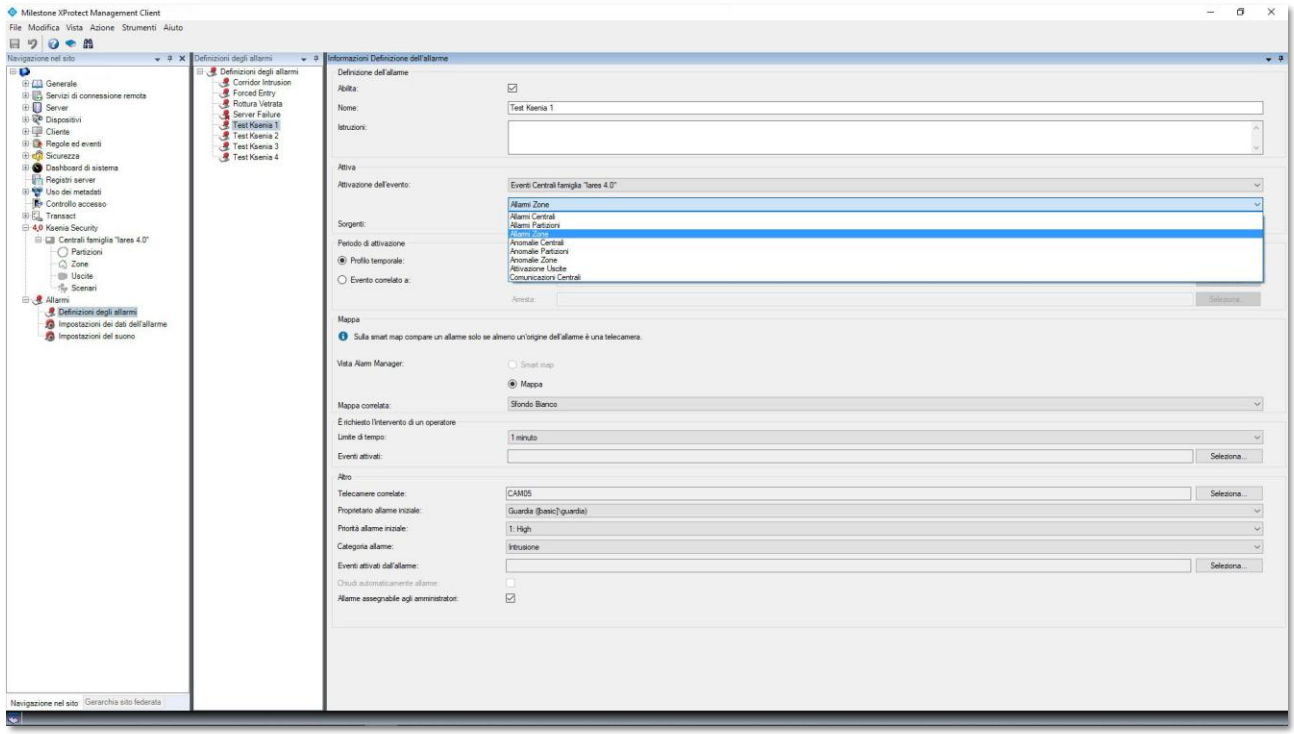

Come appare evidente dalle immagini è possibile solo abilitare o meno l'Item, tutti gli altri parametri devono essere modificati sulla Centrale, compreso il Nome utilizzato.

## 3.3 Configurazione degli Allarmi

Una volta terminata l'attività di configurazione è possibile procedere con la configurazione degli Allarmi e le altre configurazioni descritte di seguito.

Per la generazione degli Allarmi il Plugin mette a disposizione i seguenti eventi:

- Eventi Centrali famiglia "lares 4.0"
  - Allarmi Centrali
  - Allarmi Partizioni
  - Allarmi Zone
  - Anomalie Centrali
  - Anomalie Partizioni
  - Anomalie Zone
  - Attivazione Uscite
  - Comunicazioni Centrali

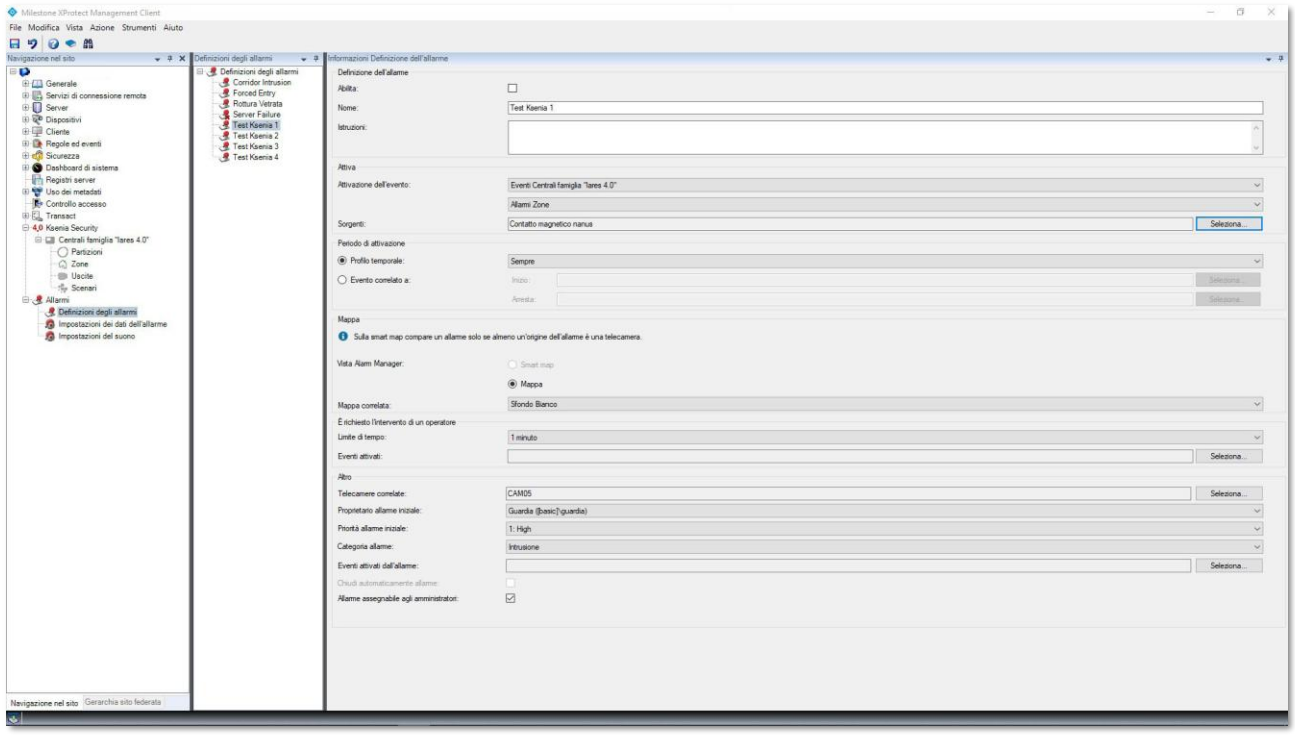



Gli Eventi definiti Anomalie rappresentano sia i Sabotaggi che i Guasti, nel caso della Centrale questi ultimi sono di diverse origini, tra le quali la Scomparsa delle Periferiche, la sezione di Alimentazione (Batteria Bassa o Guasta, Tensione Bassa, etc.).

È anche possibile generare gli Allarmi quando vengono attivate delle Uscite e quando ci sono problemi alle Comunicazioni, sia tra Plugin e Centrale, sia tra Centrale e altri dispositivi.

Di seguito un esempio di Allarme generato dall'allarme della Zona "Contatto magnetico nanus".

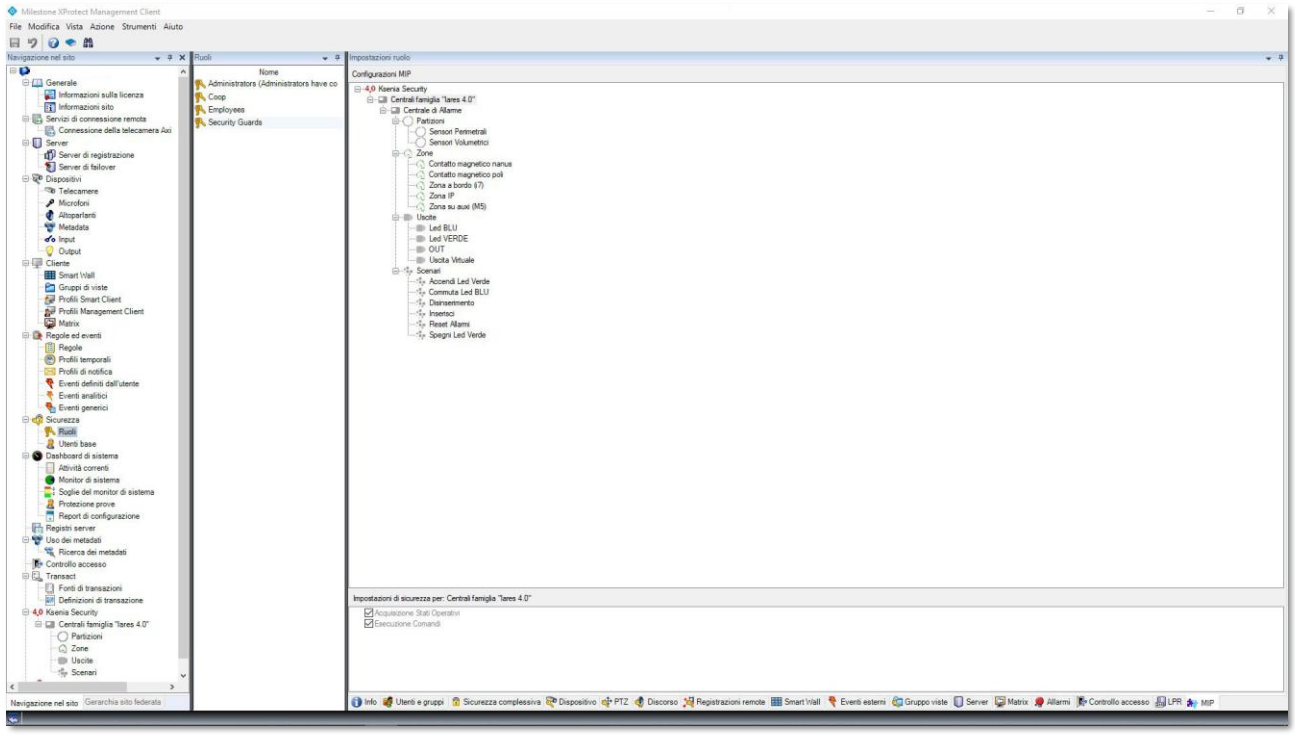
Per i vari parametri configurabili si rimanda alla specifica documentazione Milestone.



## 3.4 Assegnazione Diritti di Accesso agli Utenti

Per tutti gli elementi che compongono il Sistema è possibile assegnare i Diritti di Accesso ai Profili degli Utenti, fatta eccezione, come regola di base della Piattaforma, ai profili di Amministrazione che possiede sempre tutti i Diritti.

Per default tutti i Diritti sono abilitati per tutti i Profili, ma è possibile personalizzarli tramite l'apposito menù "Ruoli"; di seguito una schermata che ne illustra le varie opzioni.



L'assegnazione dei Diritti è gerarchica, intendendo con ciò che una data assegnazione a un dato livello si propaga su tutti gli elementi dei sottolivelli, ma è sempre possibile personalizzare i livelli sottostanti per fare in modo che gli Utenti siano autorizzati ai soli elementi di cui hanno competenza; per esempio inibendo il completo accesso a uno o più Scenari.

Esistono due soli tipi di Diritto d'Accesso, quello in cosiddetta Lettura, identificato con la definizione "Acquisizione Stati Operativi" e l'altro in Scrittura, definito "Esecuzione Comandi".

ATTENZIONE – la mancata abilitazione al Diritto in Lettura esclude automaticamente quello in Scrittura, indipendentemente dalla presenza del segno di spunta su quest'ultimo.

Se non si abilita il Diritto il Lettura a un dato Profilo tutti gli Utenti con tale Profilo non vedranno l'elemento in oggetto, non riceveranno alcuna segnalazione da esso originata e, ovviamente, non potranno eseguire alcuna azione che coinvolga tale elemento.

La mancata abilitazione del Diritto in Scrittura, come da definizione, impedisce agli Utenti di eseguire comandi sui relativi Item (set/reset, arm/disarm, etc.). Nel caso un Utente non abilitato provi ad eseguire un dato comando comparirà un messaggio che indica la motivazione della mancata esecuzione.

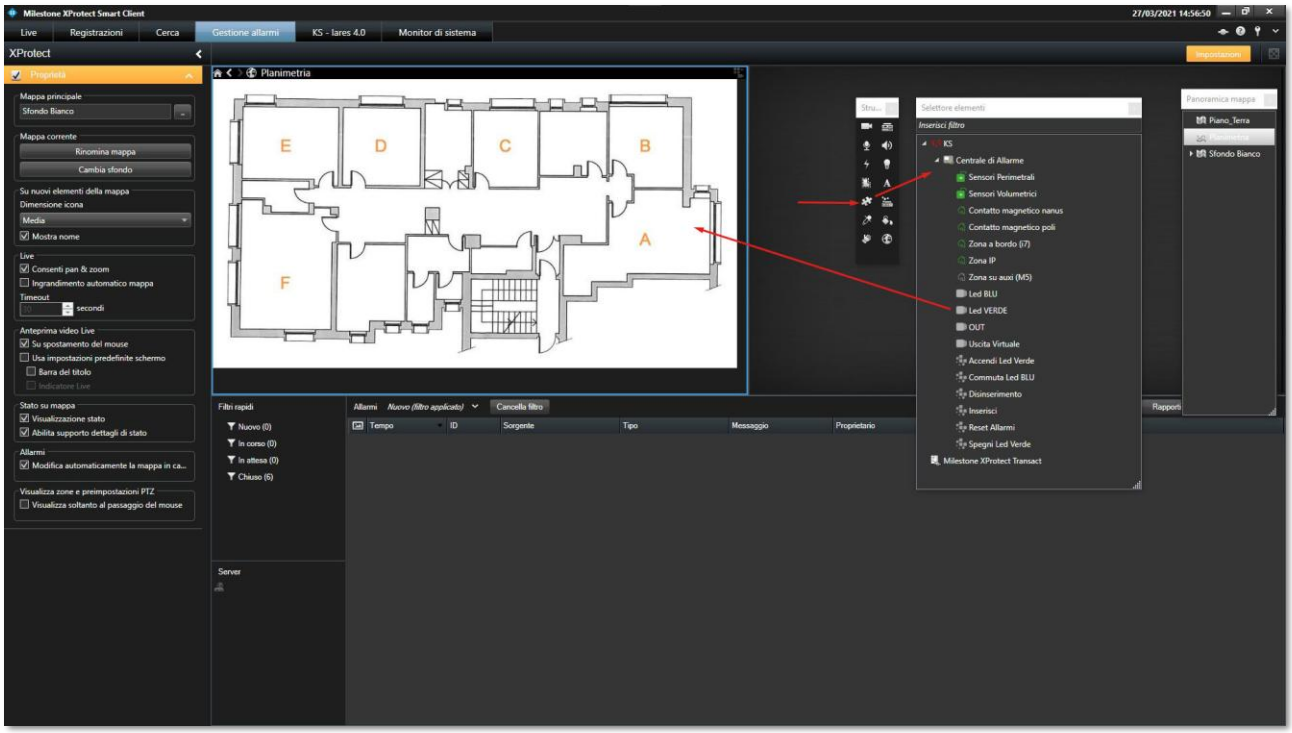
## 3.5 Posizionamento degli Oggetti sulle Mappe Grafiche

Per completare la configurazione di un Sistema (Centrale e suoi elementi) e rendere fruibili le varie funzionalità messe a disposizione dalla Piattaforma è necessaria la creazione di Mappe Grafiche (non obbligatoriamente utilizzabili ma decisamente opportuno) sulle quali posizionare gli elementi che costituiscono l'Impianto da controllare.

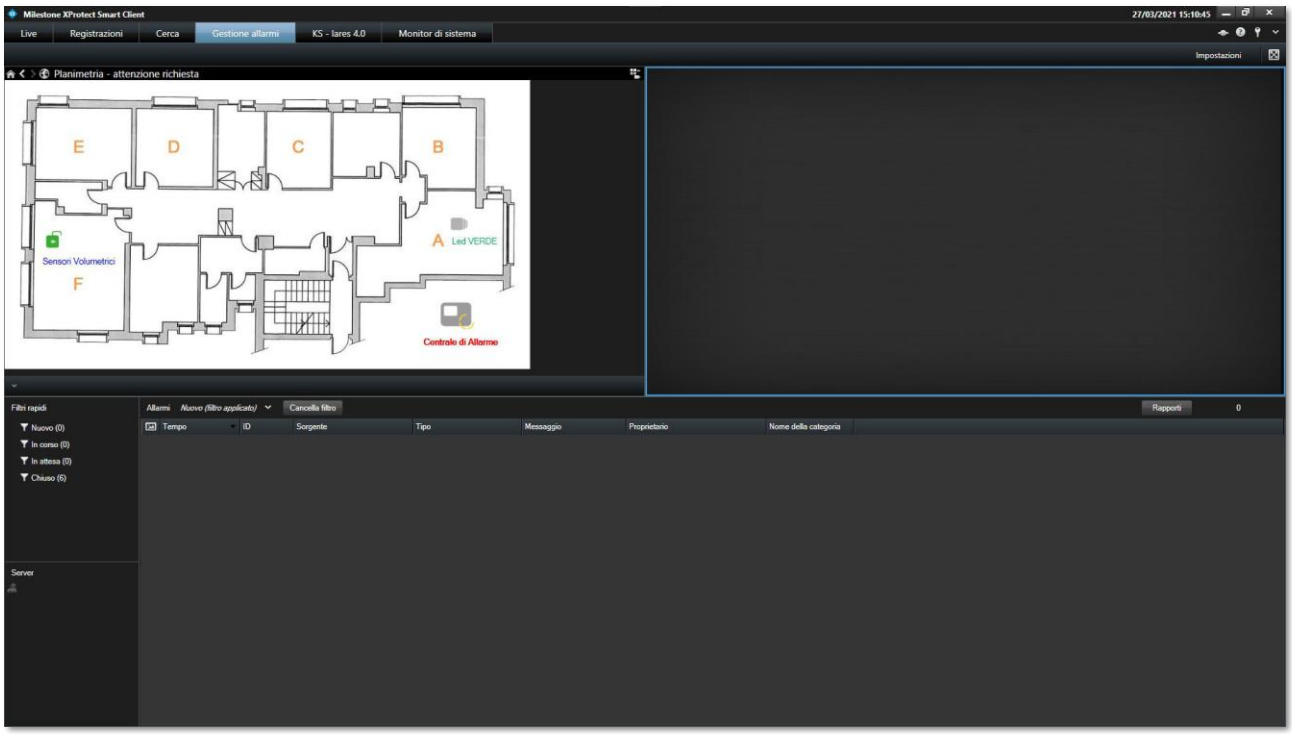
Nel seguito si farà riferimento alle Mappe Grafiche tradizionali, ma quanto illustrato è analogamente applicabile alle cosiddette Smart Map.

Queste operazioni devono naturalmente essere effettuate per mezzo dello Smart Client (sebbene si tratti ancora di Configurazioni), utilizzando un Profilo Utente che consenta l'accesso alle sezioni di Impostazioni.

Selezionando dunque il Menù Impostazioni nel workspace degli Allarmi (lo stesso può essere eseguito sui workspace dei filmati dal vivo e/o registrati) si seleziona la mappa desiderata, quindi la sezione "Aggiungi elemento plug-in", compaiono tutti gli elementi dell'Impianto che possono essere posizionati, utilizzando il drag&drop, sulla mappa selezionata.




La stessa operazione deve essere ripetuta per tutti gli elementi che si trovano all'interno della mappa; di seguito un esempio dove sono stati posizionati sulla mappa una Centrale (Centrale d'Allarme), una Partizione (Sensori Volumetrici) e un'Uscita (Led Verde).



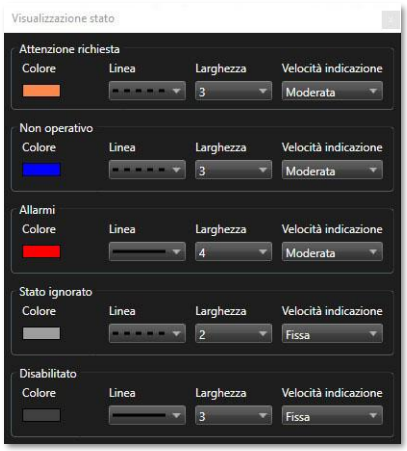

Per maggiori dettagli sul posizionamento su mappe degli Item MIP si rimanda all'apposita documentazione Milestone.

### 3.5.1 Impostazioni Parametri Visualizzazione Stato

Gli Item posizionati sulle mappe forniscono alla Piattaforma informazioni sul proprio Stato Operativo in linea con quanto gestito da XProtect, in particolare, oltre agli stati di Allarme e Riposo, sono in grado di comunicare gli stati di Disabilitazione e Anomalia.

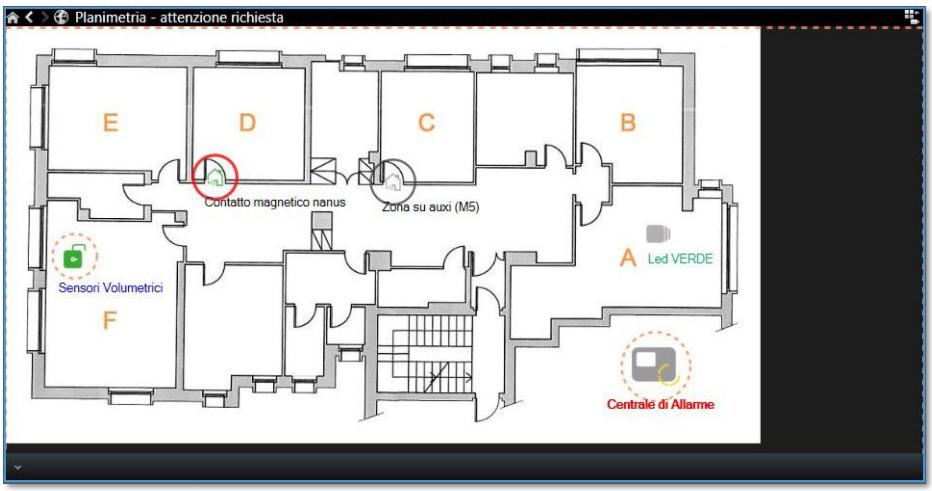
La Piattaforma permette di associare ai diversi stati operativi delle specifiche rappresentazioni grafiche degli stessi per mezzo di cerchi che circondano l'icona dell'item sulle mappe che possono avere colore, spessore, tratteggio e velocità di lampeggio differenti, per essere immediatamente identificati.

È possibile personalizzare tali cerchi, in fase di Impostazione, accedendo al menù Visualizzazione stato, mostrato di seguito.




Il Plugin, come detto, oltre agli stati di Allarme e Riposo, gestisce anche quelli di "Attenzione Richiesta", "Non Operativo" e "Disabilitato"; il secondo è riferito alle Centrali non in linea mentre l'ultimo è ovviamente riferito a un Item che non risulta abilitato sul MC, mentre il primo è legato alle Anomalie gestite che, come per la generazione degli allarmi, possono essere Guasti, Sabotaggi e la condizione di "Impianto non Inserito" (totalmente o parzialmente). Naturalmente questo ultimo stato può essere voluto (es. l'antipermanenza in una zona frequentata durante il giorno), ma può tornare utile agli Operatori per verificare, con un colpo d'occhio, lo stato di inserimento.

Di seguito un esempio di rappresentazione grafica degli stati operativi basati sulle impostazioni illustrate nell'immagine precedente.




La situazione illustrata è la seguente:

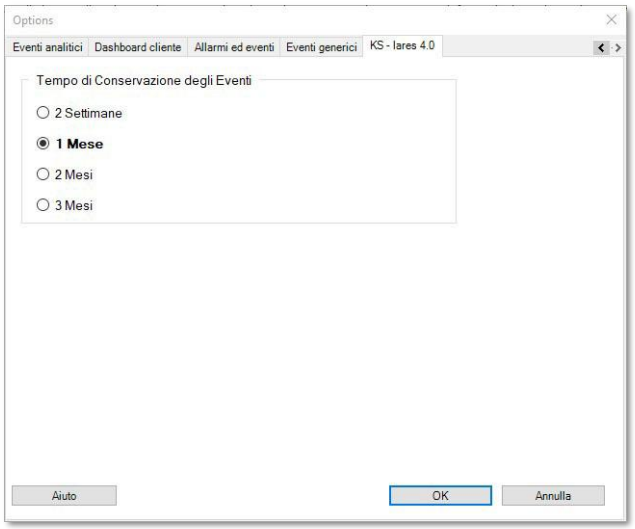
- La Partizione "Sensori Volumetrici" è cerchiata di Arancio (lampeggiante) poiché risulta Disarmata (non attiva)
- La Zona "Contatto magnetico nanus" è cerchiata di Rosso (lampeggiante) perché in Allarme

- La Zona “Zona su auxi (M5)” è cerchiata di Grigio (fisso) perché l’Item è disabilitato
- La Centrale di Allarme è cerchiata di Arancio (lampeggiante) perché è in Guasto Batteria
- L’Uscita “Led Verde”, infine, non è cerchiata perché l’Item è in condizione di riposo

In ultimo da notare che la presenza di Item con Anomalie (cerchio Arancio) fa sì che l’intera mappa sia circondata da un riquadro Analogo (Arancio lampeggiate) e presenta la dicitura, dopo il titolo della mappa, “attenzione richiesta”.

## 3.6 Durata Conservazione Registro Eventi

Utilizzando il menù Strumenti => Opzioni e selezionando il tab “KS – lares 4.0” si accede alla sezione delle Opzioni del Plugin dove è possibile stabilire la durata di conservazione dei Registro degli Eventi (visualizzati con lo SC).

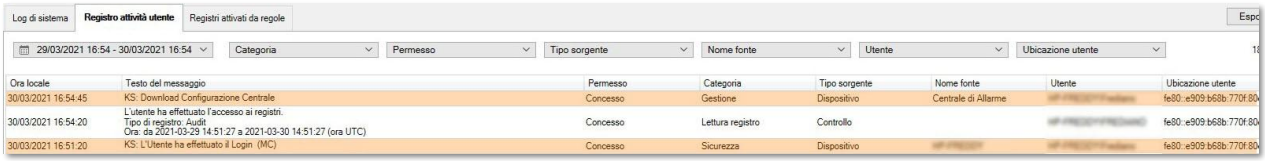


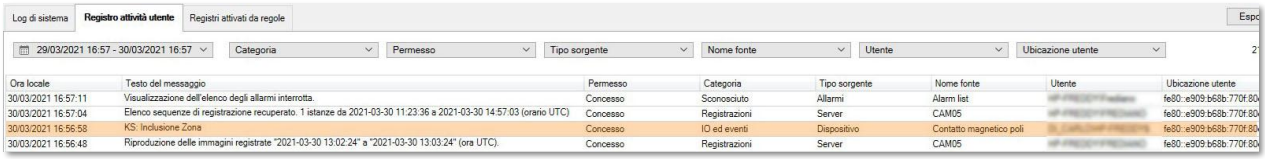

Il valore di default è 1 Mese, ma è possibile selezionare anche 2 Settimane, 2 e 3 Mesi. Allo scadere del periodo gli Eventi più vecchi sono cancellati automaticamente dallo SC.

# 4 Log delle Attività

Il Plugin registra tutte le attività degli Utenti nel Registro della Piattaforma chiamato “Registro attività utente”, siano esse di Configurazione che i Comandi eseguiti sugli Elementi dei Sistemi.

Per una immediata presa visione di tali messaggi è utilizzata la convenzione che ciascuno di essi inizia con “KS:”, come negli esempi seguenti, il primo riferito all’aggiornamento delle Configurazioni della Centrale “Centrale di Allarme” con il MC e il secondo all’inclusione della Zona “contatto magnetico poli” con lo SC.






cod. R28020.100 04/2026