lares 4.0 MIP Plugin Administrator Manual





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

Сор	yrig	ht and D	isclaimer		4
Plu	gin L	icense			4
Cor	vent	tions			5
Pro	toco	ls and Po	orts Used		5
Acr	onyr	ns			5
1	Intr	·o			6
	1.1	Plugin A	Architectu	ıre	6
	1.2	Plugin l	anguage		7
2	Plu	gin Insta	llation		8
3	Plu	gin Conf	iguration		9
	3.1	Configu	iration W	orkflow	9
	3.2	Adding	a Securit	y Panel	
		3.2.1	Configu	rations Download	11
			3.2.1.1	IP Zone Triggers	
				3.2.1.1.1 Rules for the Activation of User Events	
			3.2.1.2	Verification and Customization of the Objects controlled by the Security Panel	
	3.3	Alarm (Configura	tion	
	3.4	Assigni	ng Access	Rights to Users	19
	3.5	Positio	ning of Ob	jects on Graphic Maps	20
		3.5.1	Status D	Display Parameter Settings	22
	3.6	Event L	og Retent	ion	23
4	Auc	lit Log			



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 overlange with the SDr
HTTPS	443	Data exchange with the SPS
HTTP	69	Sending Commands to internally managed IP Zones
HTTP	8080	Conding Commands to ID Zanas managed through IBT norts
HTTPS	8443	Sending Commands to IP zones managed through for ports

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

at Clien File Edit View Action Tools Help 🗟 🤊 🕜 🗢 🛱 - 0 X - 13 milestone | XProtect[®] Basics Remote Connect Services
 Servers
 Devices 4.0 KS Client
 Rules and Events This Plugin allows the integration of the Ksenia Security "lares 4.0" family Intrusion Security Panels on the XProtect Platform. Security Security
 System Dashboard
 Server Logs
 Wetadata Use Version: 0.0.0.0 - © Copyright Ksenia Security 2020-2030. All rights reserved Access Control 40 Kser Iares 4.0" family Security Panels Partitions enia Output Scenarios E & Alarms security innovation

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.

Enter the Name of the new Security Panel to be created
New Security Panel

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.

		New Security Panel	
eneral	Peripherals IP Zone Tri	iggers	
	IP Address	192.168.170.33	
	Security Protocol	TLS O NO	
	User PIN	•••••	
	Installer PIN	•••••	
c	heck Connection	Panel Conf	iguration
	FW Version		7
			-
	MAC Address		



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.

		New Security Panel	
eneral	Peripherals IP Zo	one Triggers	
	IP Address	192.168.170.33	
	Security Protocol	TLS O NO	
	User PIN	•••••	
	Installer PIN	•••••	
c	heck Connection	Downloa Panel Co	d/Update nfiguration
c	heck Connection	Downloa Panel Co Iares 4.0 40IP wis	id/Update nfiguration
C	heck Connection Model FW Version	Downloa Panel Co lares 4.0 40IP wis 1.68.26	d/Update nfiguration
C	Model FW Version MAC Address	Downloa Panel Co lares 4.0 40IP w/s 1.68.26 A4-58-0F-94-44-E6	id/Update nfiguration

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.

lements	Actual	Previous
utput	4	0
artitions	2	0
enarios	6	0
eripherals	8	0

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.



		New Security Panel
Gene	ral Peripherals IP Z	one Triggers
ID	Description	Туре
1	ergo S 1	ERGOS
1	auxi relè/auxi-L 1	AUXIRELE
2	auxi 2	AUXI
3	auxi-HT	AUXIHT
4	auxi-HL	AUXIHL
1	poli 1	POLI
2	nanus 2	NANUS
1	Sirena Wls	IMAGO

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.



			New Security	Panel		
eneral	Peripherals	IP Zone Trigg	jers			
	Zone			User-defined E	Events	
Zor	a IP		Sblocco Canc	ello Carraio		× 🗙
			Attivazione Sir	ena		
			Accensione Lu	a allo Carraio		_

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.



File Edit View Action Tools Help	Milestone XProtect Management Client			22		×
Image: Ster Nervated Ster Hersechy Image: Ster Nervated Ster Hersechy	File Edit View Action Tools Help					
Sine Navigabon • 0 X Basics Rules Ba	🖬 🤊 🕝 🗢 🛍					
Image: Series	Site Navigation 👻 🕂 🗙	Rules 🚽 🦊	Rule Information			₩ Ĥ
Ste Navigation Federated Site Hierarchy c >	Basics Basics	Rules Rules Avria Batch Avria	Name: Motion AXIS Description: Motion Detector on board Camera Image: State of the	raio		× >
	Site Navigation Federated Site Hierarchy	< >	1	_	_	

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)"

Milestone XProtect Management Client			– D X
File Edit View Action Tools Help			
目 9 2 ◆ 曲			
Site Navigation	Devices v 4	Properties	- 4
Site Revigation	Decides v v Concess Control System Control	Configured events: Motion Stated (HW)	General Enabled True Event source 1
Analytics Events Generic Events Generic Events Governity System Dashboard 		Add Delete	Enabled
E C Transact		A Info Ca Settings T Streams A Record & Motion A Fisheve	ens 🐘 Evente 🥅 Client 🎟 Privacy masking
G 4.0 Ksenia Security	· · · · · · · · · · · · · · · · · · ·	To the streams and the cord of	
Tares 4.0" family Security Panels O Partitions O Jones Output Scenarios	Preview		~ ‡ >
Site Navigation Federated Site Hierarchy		AXIS M1065-L	



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.

					2.4	
ame:	Test Rule					
escription:						
tive:						
		Ste	p 1: Type of rule			_
Select the rule	type you want to e	create				
Perform an	action on <event></event>	>				
Perform an	action in a time in action on a krecu	nterval arring time>				
		and and a				
Edit the rule de	scription (click a	n underlined item)				
Edit the rule de Perform an actio	scription (click an non <u>event</u>	n underlined item)	nt server	 		
Edit the rule de Perform an actio from <u>devic</u> i	scription (click a n on <u>event</u> es/recording se	n underlined item) erver/managemei	nt server	 		
Edit the rule de Perform an actio from <u>device</u>	scription (click an In on <u>event</u> es/recording se	n underlined item) erver/managemei	nt server	 		
Edit the rule de Perform an actic from <u>device</u>	scription (click ar in on <u>event</u> ss/recording se	n underlined item) erver/managemen	nt server	 		
Edit the rule de Perform an actio from <u>device</u>	scription (click a in on <u>event</u> es/recording se	n underlined item) erver/managemen	nt server	 		
Edit the rule de Perform an actic from <u>devic</u>	scription (click ar n on <u>event</u> es/recording se	n underlined item) erver/managemen	nt server	 		
Edit the rule de Perform an actio from <u>devic</u>	scription (click ar n on <u>event</u> ss/recording se	n underlined item) erver/managemen	at server	 		
Edit the rule de Perform an actic from <u>devic</u>	scription (click ar in on <u>event</u> ss/recording se	n underlined item) erver/managemen	nl server			









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

Milestone XProtect Management Client				- 6 >
File Edit View Action Tools Help				
🗄 🤊 🥝 🗢 🕅				
Site Navigation 👻 🕈 🗙	Alarm Definitions 👻 🤑	Alarm Definition Information		-
C C C C C C C C C C C C	Atem Definitions Corridor Intrusion Forced Entry Rotura Vetrata Server Failure Test Kaenia - Allarmi Centrale Test Kaenia - Allarmi Partizioni	Nam definition Enable: Name: Instructions:	2 Tet Kenis - Klani Zove	~
	Test Kaenia - Anivazione Usche Test Kaenia - Comunicazioni	Trigger Triggering event:	Tures 4.0° fandy Security Panel Events	~
Access Control Access Control Access Control Access Control Access Control Access Control		Sources:	Awms comis Awms Secury Parels Rems Active	
Tares 4.0° family Security Panels O Partitions Zones Dutput Encounter		Activation period Time profile: Event based:	Anonales Fattors Anonales Cantos Pante Communicators Scrutz Panels Olgafick Antra Anonales Olgafick Antra Anona	
Alarms Alarm Definitions Alarm Definitions		Мар	Stop	Select
		Aam manager view:	Start ras ® Mae Tatoh Rana	
		Constant and the same land		
		Time lint:	1 minute	~
		Events trggered		Seed_
		Other		
		Related cameras:	CAM05	Select
		Initial alarm owner:	Guarda (basc) guarda)	~
		Initial alarm priority:	1: High	~
		Aam category:	Infrusione	~
		Events tragened by alarm		Select
		Acto close alarm: Alarm assignable to Administrators:		
Site Navigation Federaled Site Hierarchy				

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.



1 C + M				
ation - 4 3	Alarm Definitions - 0	Alarm Definition Information		
	🕞 🧶 Alarm Definitions	Nam definition		
Basics Remote Connect Services Servers	Forced Entry	Enable:		
	Rottura Vetrata	Name:	Test Kseria - Alami Zone	
Devices	Server Failure			
Client	Test Ksenia - Allarmi Partizioni	instructions:		
Rules and Events	Test Ksenia - Allarmi Zone			
System Dashboard	Test Ksenia - Admazione Osche	Trigger		
Server Logs		Trippering event:	Tares 4.0° family Security Panel Events	
Metadata Use	1			
Transact			Nattrs Jones	
B Ksenia Security	1	Sources:	Contatio magnetico nanus	Select
I Iares 4.0" family Security Panels	1	Activation period		
O Partitions	1	Time profile:	News	
Dutput	1	O E-millioned		
tily Scenarios			5000.	
Alarms			Step	Silent's
Alexa Data Satisara		Map		
	1		Map	
			® Map	
		Related map:	Map Stock Banco	
		Related map: Operator action required	Map Storedo Banco	
		Related map: Operator action required Time limit	@ Map Bindo Banco 1 minde	
		Related map: Operator action required Time limit: Events triggered:	@ Map Stroke Banco 1 minde	Select_
		Related map: Operator action required Time limit Events triggered: Other	Mup Sinds Bance Timule	Select_
		Related map: Operator action required Time Inst Events triggered Other Related commas:	Map Binds Bancs Initial CM05	Select_
		Related map: Operator action required Time line: Events triggered. Other Related commens. Initial atom conner.	Map Strado Banco Innute CMMS CuMdS Guarda (Banc)quarda)	Select_
		Rolated map: Opentier action required Time Init: Events Higgered: Other Rolated camerums: Initial dammerer. Initial dam pointy:	Kup Since Innute CM05 Guarda SancQuarda) 1 Hyb	Select_
		Related map: Operator Action required Time limit : Events Mogened : Other Related commiss: Initial Jamin conver Initial Jamin conver Initial Jamin printy; Adam cetegoy;	Kup Map Map Map Map Ininde CM05 CM05 Canda Base(gunde) Hph Hum Hum	Select_
		Related map: Openitor action required Time Int I: Events Higgened Other Related commens: Initial dama pointy; Alien colorgoy; Events Higgened by dama;	Kup Sinch Banco Innute CM05 Guarda Sasciparda I Hph Itatore I Hph Itatore I Hph Itatore I Hph Itato	Select_
		Related map: Constant action regulared Time linit; Event togened: Other Related commas: Initial adam protects; Valid adam protects; Alam contegory; Event togened by adam;: Alam contegory;	Kup Brick Banco Initude CM05 Cauda (Basc)quarta) Huture Huture tutore Cutors tutore Cutors	Select_
		Robert map: Openitor action required Time Int. I: Events Miggend: Other Robert commens: Hold allen openity: Allen openity: Events Miggene by alem: Allen say allen be Adventeration:		Select.
		Related map: Openizer action required Time linet: Events folgement: Other Related comments: Indial alam pointy; Aiem category: Events folgement by alam; Alacid ana film: Alam assignable for Administrators:		Seed
		Related map: Concertor Action required Time Init: Events Mogened: Other Related communic Initial Jama contern: Initial Jama pointy: Adm categoy: Events Mogened by Jama: Adm assignable to Administratory:	@ Nap @inde Banco Innute CMOS Guada §asc(parts) 1 Hpi Hutane 	Select
		Related map: Openitor action regulated Time last: Events higgened: Other Related commans: India dama pointy: Admin conter; Nation actiopopy: Events inggened by adm: Admin assignable to Administrators;	@ Nap @Inste Inste CM05 Guoda Sactguarda) 1 Hgia Huane 	Select.
		Related map: Constant action regulared Time linet : Event toggenet : Other Related commas: Hold after openet: Hold after openet: Anno collegops : Event toggenet by alem: Also chan alems: Also man assignable to Administrators:	@ Nap Ørde Bance I sinde CMMS Ganda (basc)queda) I hju Hausee I I hju I hju I hju I hju I hju	Select.
		Related map: Openitor action required Time Init: Events higgened: Other Related commans: Initial dama pointry: Admin category: Events higgened by dama: Admin assignable to Administratory:	@ Nap [Strote Bance Immate [Select.
		Related map: Constat Action regulared Time link : Event togenet: Other Related commas: Initial adam points; Adam contegory : Event togenet by adam: Adam segnable to Administratory :	@ Nap @ Map @ Map I minde CM05 Gardis (basc) Querta) 1. Haj Wituppe Wituppe I I I I I I I I I I I I I	Select_

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.

Milestone XProtect Management Client		- 0 ×
File Edit View Action Tools Help		
m 10 - M		
8 7 V 8		
Site Navigation + 4 X	Roles • 9	Role Settings
	Name	MP conflue retions
(i) (iii) Basics	Administrators (Administrators have co	ren overlige som
FI IIB Remote Connect Services	Core	E-40 Karnia Security
E Servere	Coop -	Image 4.0" family Security Panels
(i) ER Dunians	The Employees	iai La Centras a Alame
in EP crime	Security Guarda	B Partitions
in the class	-	Service Performediate
er or Rules and Events		
Erecta Security		
The Holes		Control to manufactor and
Basic Users		Cona a bords (7)
(i) System Dashboard		Can P
Server Logs		Zone su auto (MS)
🕀 🌄 Metadata Use		E Dutot
Access Control	1	- m Led BLU
(i) [], Transact	1	D Led VERDE
4.0 Ksenia Security	1	TUO
E Tares 4 0' family Security Panels	1	III Uscta Vituale
- O Partitiona	1	🗁 🎰 Serrarioa
0.7000		- 1 Accendi Led Verde
Ci zones		- 15 Commuta Led BLU
i output		fair Dishostmento
tige Scenarios		- is insense
🖽 🍕 Alarma		- Te Reset Alarri
		Tiu Spegni Led Verde
	1	
	1	
	1	
	1	
	1	
	1	
	1	
	1	
	1	Security settings for: Tares 4.0" family Security Panels
	1	Conjustion of Operating States
	1	Command Execution
	1	
	1	
	1	
	1	
	1	
	1	
Site Navigation Federated Site Hierarchy		🚺 info 🥰 Users and Groups 🚡 Overall Security 👰 Device 🏟 PTZ 🤹 Speech 🙀 Remote Recordings 🇮 Smart Wall 🎈 External Events 🚳 View Group 🚺 Servers 🔯 Matrix 🏓 Aarms 🕷 Access Control 🚚 UPR 約 MIP



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.

Attention ne	eded		
Color	Line	Width	Indication speed
		▼ 3	▼ Moderate ▼
Not operatio	onal		
Color	Line	Width	Indication speed
		→ 3	▼ Moderate ▼
Alarms			
Color	Line	Width	Indication speed
		- 4	▼ Moderate ▼
lgnored stat	us		
Color	Line	Width	Indication speed
		₹ 2	▼ Fixed ▼
Disabled			
Color	Line	Width	Indication speed
		- 3	- Fixed -

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).

ptions					×
nalytics Events	Customer Dashboard	Alarms and Events	Generic Events	KS - lares 4.0	< .
Events Ret	ention Time				
O 2 Week	s				
1 Mont	h				
O 2 Month	s				
O 3 Month	s				
Help				OK	Cancel

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.

System logs A	Audit logs	Rule-triggered logs											Expo
01/04/202	21 17:28 - (02/04/2021 17:28 ∨	Category	~	Permission	~	Source type	✓ Source name	~	User	~	User location	✓ 152 e
Local time		Message text					Permission	Category	Source ty	pe	Source name	User	User location
02/04/2021 15:05:1	15	KS: Security Panel Config	uation Download				Granted	Management	Device		New Security Panel	NP-FREEDOWN-Market	fe80: 25f9:226d:2173:493
02/04/2021 13:45:0	:02	User successfully logged	n				Granted	Security	Server		HP-PREDEV	NT AUTHORITY/SERVIZIO	E fe80::25f9:226d:2173:493
02/04/2021 12:50:5	:52	KS: New Security Panel (onfiguration				Granted	Management	Device		New Security Panel	of PRESS Press	fe80::25f9:226d:2173:493
02/04/2021 12:41:4	:49	KS: User Logged IN (MC)					Granted	Security	Device		MP-PRODUCT N	NOT A TRACE OF TAXABLE PARTY.	fe80: 25f9 226d 2173:493
System logs A	Audit logs	Rule-triggered logs											Expo
System logs A	Audit logs 21 17:52 - (Rule-triggered logs	Category	~	Permission	~	Source type	V Source name	~	User	~]	User location	Expc
System logs A	Audit logs 21 17:52 - (Rule-triggered logs 02/04/2021 17:52 V	Category	~	Permission	*]	Source type	V Source name	~	User	~	User location	⊂ Expc
System logs A	Audit logs 21 17:52 - (Rule-triggered logs 02/04/2021 17:52 ~ Message text	Category	~	Permission	~	Source type Permission	 ✓ Source name Category 	∽ Source t₀	User	✓ Source name	User location	V 157 e
System logs A 01/04/202 Local time 02/04/2021 17:52:2	Audit logs 21 17:52 - (:25	Rule-triggered logs 02/04/2021 17:52 ~ Message text KS: User Logged OUT (S	Category	~]	Permission	~	Source type Permission Granted	 Source name Category Security 	Source to Device	User	Source name localhost	User location User	 Expc 157 e User location fe80-25f9-226d-2173.493
System logs A 01/04/202 Local time 02/04/2021 17:52:2 02/04/2021 17:52:2	Audit logs 21 17:52 - (:25 :23	Rule-triggered logs 02/04/2021 17:52 ~ Message text KS: User Logged OUT (S User successfully logged	Category) aut	~	Permission	~	Source type Permission Granted Granted	 Source name Category Security Security 	Source to Device Server	User	Source name localhost	User location User	 Expc 157 e User location fe80-25f9-226d-2173.493 fe80-25f9-226d-2173.493
System logs System logs Collocal time 02/04/2021 17:52: 02/04/2021 17:52: 02	Audit logs 21 17:52 - (225 23 :03	Rule-triggered logs 02/04/2021 17:52 V Message text KS: User Logged OUT (S User successfully logged User has accessed logs. Log type: Audit Ime: 2021-04-01 15:52:(Category) sut 1 to 2021-04-02 15:52:01 (UTC tir	~]	Permission	~	Source type Permission Granted Granted Granted	Source name Category Security Security Log read	Source ty Device Server Audit	User	Source name localhost	User location User	Expc 157 e User location 1680-259-2264 2173.493 1680-259 2264 2173.493 1680-259 2264 2173.493
System logs A 01/04/202 Local time 02/04/2021 17:52:0 02/04/2021 17:52:0 02/04/2021 17:52:0 02/04/2021 17:51:4	Audit logs 21 17:52 - (:25 :23 :03 :40	Rule-triggered logs 02/04/2021 17:52 ~ Message text KS: User Logged OUT (S User successfully logged User has accessed logs. Time: 2021-04-01 15:52(Jam list viewing stoppe	Category 2) 34 1 to 2021-04-02 15:52:01 (UTC tir	~]	Permission	~	Source type Permission Granted Granted Granted	Source name Category Security Log read Unknown	Source to Device Server Audit Alarms	User	Source name localhost	User location User	 Expc 157 e User location 460: 2545 2264 2173.493 460: 2545 2264 2173.493 460: 2545 2264 2173.493 460: 2545 2264 2173.493

