SecurSys

Event Sensors

MIP Plugin

Rev. 3.0.1.0

User Guide

Revision Table

Rev.	Date	Changes
3.0.1.0	05/08/2019	Plugin revision first public issue

Sommario

1 Copyright and Disclaimer

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.

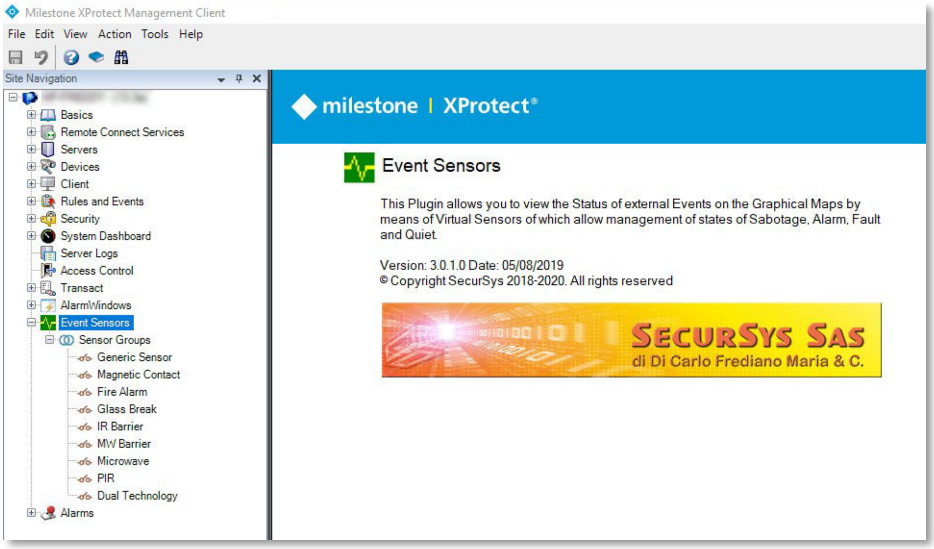
All references to systems, people and organizations used in the document are dummy and any resemblance to real situations is purely random and unintended.

SecurSys reserves the right to make changes to the Plugin without notice.

2 Intro

This Plugin was developed in order to facilitate the operational management, on the XProtect VMS platform, of intrusion systems that do not have a specific integration plugin but use External Events to communicate status changes.

It adds to the XProtect Platform a certain number of types of virtual sensors, 9 in the current version, which can be associated with the Events related to the external system and positioned on the graphic maps, to allow security officers to locate the origin and type of the events themselves.



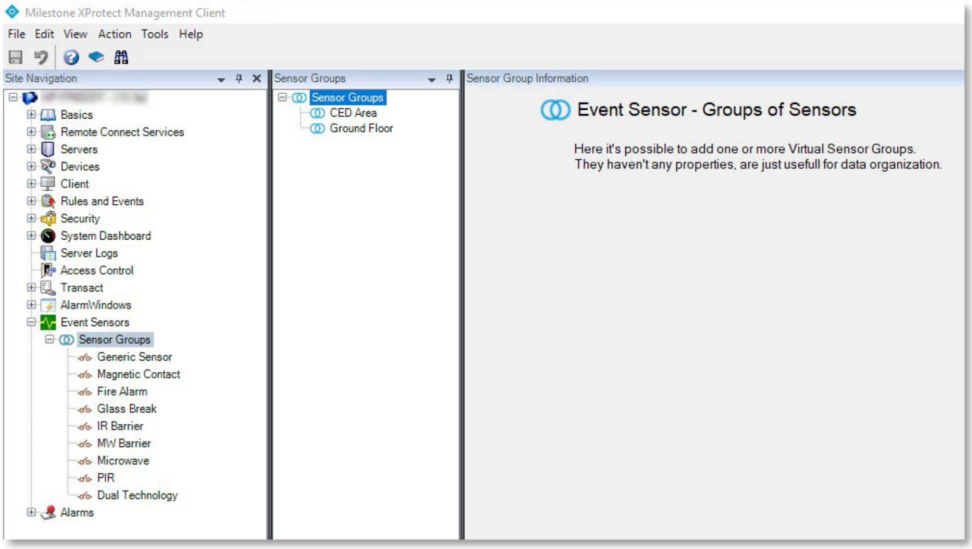
Event Sensors

This Plugin allows you to view the Status of external Events on the Graphical Maps by means of Virtual Sensors of which allow management of states of Sabotage, Alarm, Fault and Quiet.

Version: 3.0.1.0 Date: 05/08/2019
© Copyright SecurSys 2018-2020. All rights reserved

The Virtual Sensors belong to Groups that do not have any operational properties, but help to organize the sensors themselves. For example, it is convenient to create as many Groups as there are graphical maps so that each Group contains all the sensors to be positioned on the relative map.

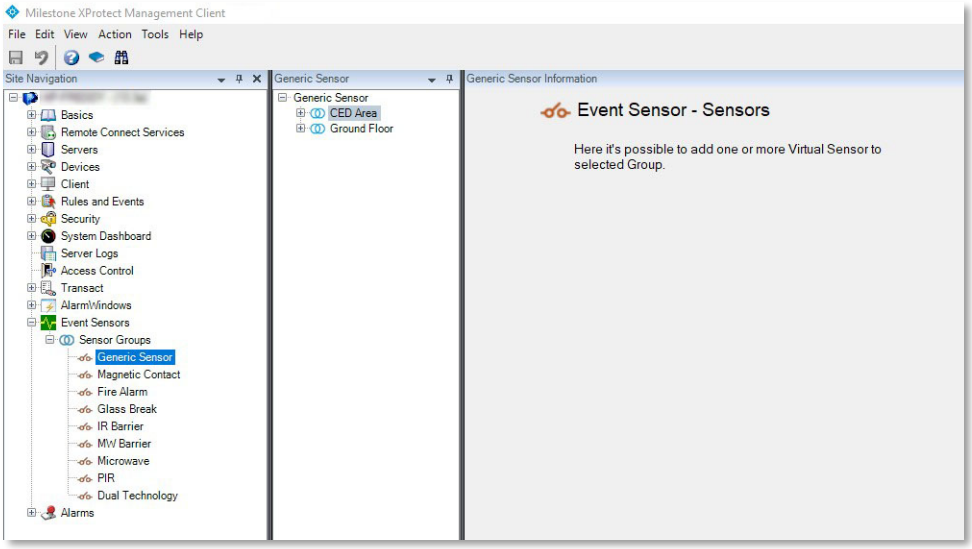
Groups are identified by the icon .



Event Sensor - Groups of Sensors

Here it's possible to add one or more Virtual Sensor Groups.
They haven't any properties, are just usefull for data organization.

Once the Groups have been created, the desired number of Virtual Sensors can be associated with them, on the Management Client the Virtual Sensors are identified by the icon .



Event Sensor - Sensors

Here it's possible to add one or more Virtual Sensor to
selected Group.

2.1 Plugin Evolution

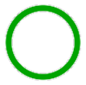
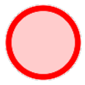
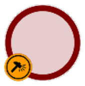
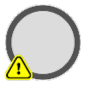
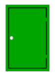
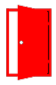
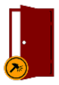
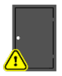
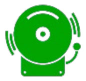
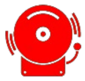
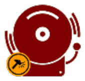
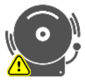
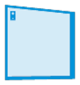
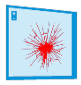
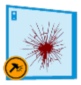
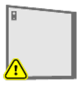
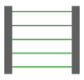
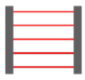
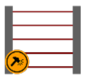
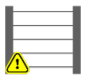
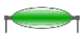
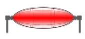
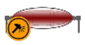
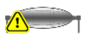
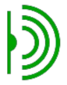
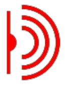
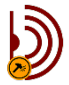
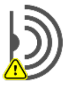
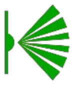
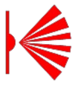
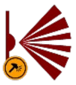
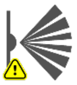
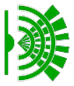
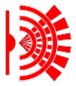
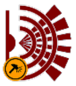
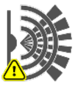
The Rev. 1.0 of the Plugin managed a single type of sensor which had only two states, Alarm and Quiet, with their icon maps, in order to graphically illustrate the state itself.

Rev. 2.0 of the Plugin brought to 9 the different types of sensors (magnetic contact, PIR, dual technology, etc.), each with its own pair of status icons, to allow a more immediate and detailed interpretation of the events.

Rev. 3.0 brings to 4 the operating states of the sensors, Alarm, Sabotage, Fault and Rest, and related status icons, to allow the complete management of intrusion systems compliant with Security Grade 4 of the reference standard CEI EN 50131.

2.2 Graphic Representation of Virtual Sensors

The following table shows the icons that can be used on the graphic maps of the platform, for each of the current types and relative operating states.

Sensor Type	STATE			
	Quite	Alarm	Tampering	Failure
Generic				
Magnetic Contact				
Fire Alarm				
Glass Break				
IR Barrier				
MW Barrier				
Microwave				
PIR				
Dual Technology				

2.3 Sensors Operating Status Management and Relative Priorities

The following priorities are used to manage the operating states of the sensors (from the highest to the lowest):

- Failure
- Tampering
- Alarm
- Quiet

This implies, regardless of the starting state:

- When a failure activation event is received, the virtual sensor assumes this state and any subsequent communication (tamper, alarm, etc.) is ignored (a faulty sensor can provide false signals) until the fault deactivation event is received
- When a Tampering activation event is received, the virtual sensor assumes this status and any subsequent Alarm communication is ignored, but obviously not the Failure one, until the Sabotage deactivation event is received
- The Alarm condition is therefore considered only in the absence of Failure and Tampering
- The condition of Quite implies the complete absence of the other 3

2.3.1 Smart Client Contextual Menus

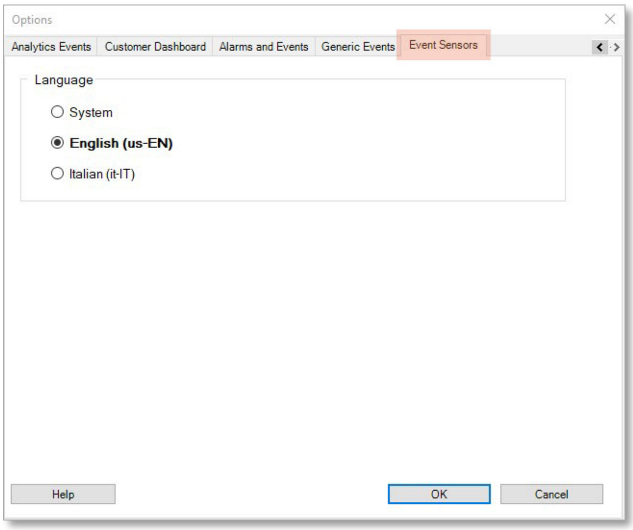
Since this Plugin operates in the conditions in which the exchange of information takes place only from the intrusion system to the XProtect Platform, status misalignments may occur, eg. from the fault condition of a sensor, one passes to the normal one without sending the message corresponding to the deactivation of the fault. For this reason, on the Smart Client there are 4 contextual menu items (right click of the mouse) whose actions force the desired state in order to realign the two systems. The following icons are associated with these menu items:

- ➡ Set Failure State
- ➡ Set Tampering State
- ➡ Set Alarm State
- ➡ Set Quiet State

2.3.2 Plugin Language

The current version implements the management of the Italian and English languages, the choice of which can be linked to the language used by the Clients or set by the User.

This is because part of the displayed messages is managed by the Event Server whose language is the same of the Operating System, it could therefore happen that with an OS in English and the 2 Clients in Italian, part of the messages will be in English and part in Italian. To avoid this, you can choose one of the 2 languages, through one of the Management Client options tabs, as shown below.



Language

○ System

● English (us-EN)

○ Italian (it-IT)

If you choose the System option, the messages generated by the Clients will be in the same language chosen for the Clients, while those generated by the Event Server is the language of the Operating System.

3 Plugin Installation

The plugin consists of only 3 files:

- Plugin.def
- EventSensors.dll
- EventSensors.dll.config

The first is the plugin definition file, which is essential for its functioning.

The second contains the executable code of the plugin with all the resources incorporated (graphics and languages).

The third contains additional system configuration parameters to those accessible through the Management client. These parameters will be illustrated in the chapter on the Operation of the plugin itself.

The plugin does not have its own installation procedure, it is sufficient to create a folder with any name, but the name EventSensors is strongly recommended to facilitate the search, within which to copy the aforementioned 3 files.

The installation folder must be created as a sub-folder of "MIPPlugins", which is itself a sub-folder of the XProtect Platform installation folder. If the installation of the Platform was performed with the standard procedure, the following 2 alternatives are possible:

1. 64bit installation:

   the Platform is installed in the C:\Program Files\Milestone folder, then the plugin

   C:\Program Files\Milestone\MIPPlugins\EventSensors

2. 32bit installation:

   the Platform is installed in the C:\Program Files (86)\Milestone, then the plugin

   C:\Program Files (86)\Milestone\MIPPlugins\EventSensors

4 Plugin Configuration

The plugin configuration is mainly carried out through the Management Client, with the exception of the positioning of the Virtual Sensors on the graphic maps, which is done through the Smart Client.

Before proceeding with the configuration, it is essential to prepare some elements of the system used as parameters of the Virtual Sensors.

The complete logical flow of the various operations to be performed is as follows:

1. Configure all the "Generic Events" that correspond, for each Real Sensor of the Burglar Alarm system, to the Activation and Deactivation messages of Alarm, Tamper and Failure states (or only the subset managed by the system); these must be associated with the Virtual Sensors managed by the Plugin
2. Configure the Groups of Sensors and related Virtual Sensors belonging to them
3. Configure the System Alarms whose activation events are linked to the different Virtual Sensors
4. Place the Virtual Sensors on the System Graphic Maps

The Management Client is used for the first 3 points, the Smart Client for the last.

4.1 Configuration of Generic Events

For a detailed description, refer to the specific documentation of the XProtect Platform.

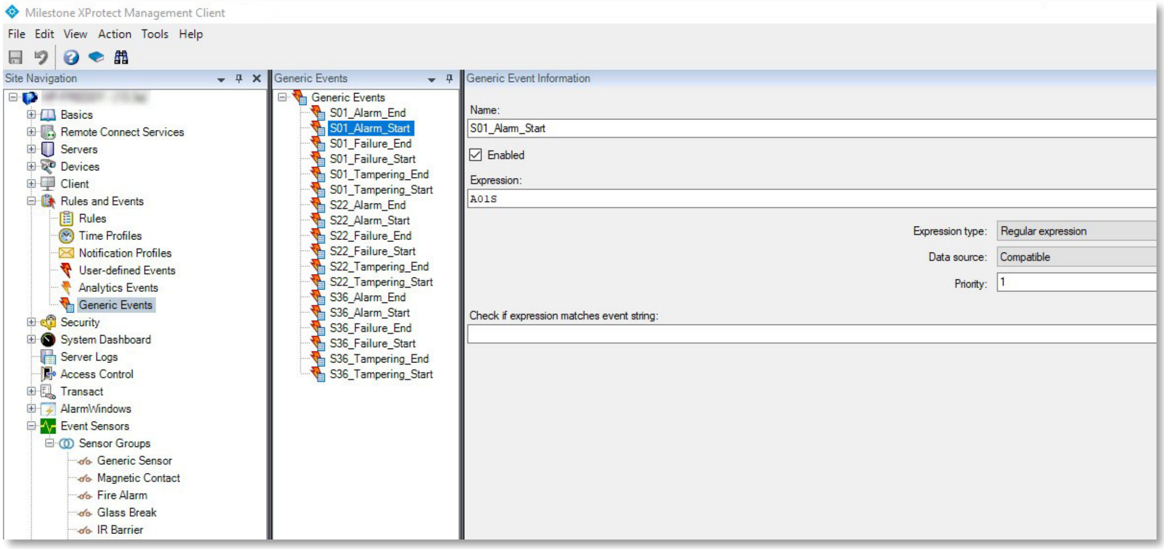
Below are example screenshots of a hypothetical configuration of Generic Events. In the following examples, the following conventions are assumed:

- 3 different sensors are involved whose external device (for example an intrusion panel) identifies with 01, 22 and 36
- When the status of each sensor changes, the external device sends the following message over the network to the XProtect Platform

  [A | F | T]nn[S | E]

  where A = Alarm, F = Failure and T = Tampering (Tampering), nn is the sensor index and the last field S = Start, E = End; for example the beginning of the Sabotage of the sensor 45 will be

  T45S



Name: S01_Alarm_Start

☑ Enabled

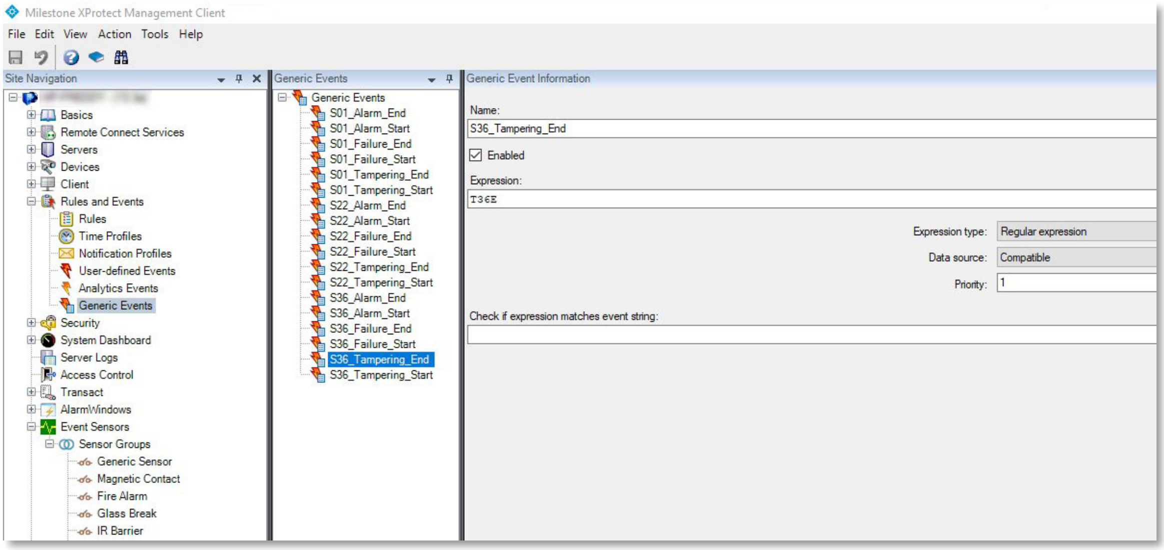
Expression: A01S

Expression type: Regular expression

Data source: Compatible

Priority: 1

Check if expression matches event string:



Name: S36_Tampering_End

☑ Enabled

Expression: T36E

Expression type: Regular expression

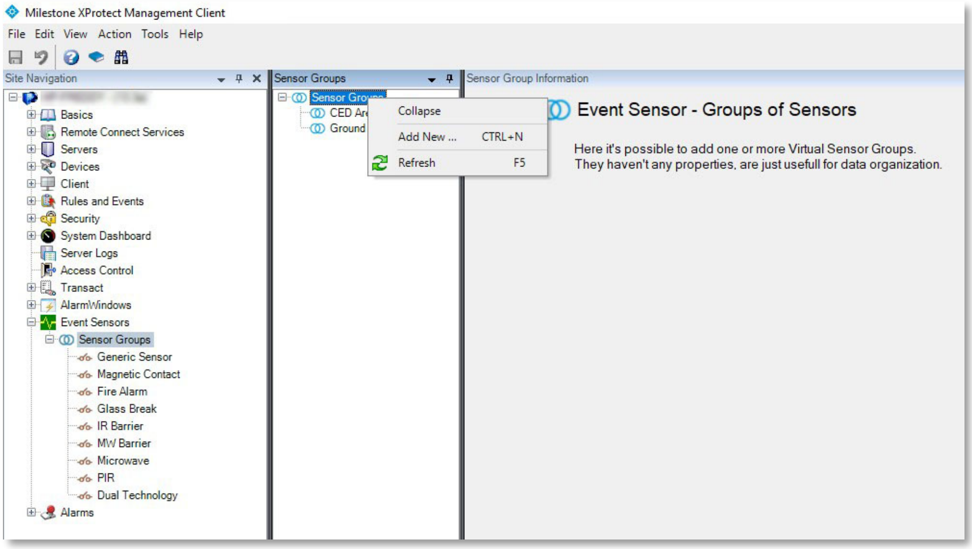
Data source: Compatible

Priority: 1

Check if expression matches event string:

4.2 Groups and Virtual Sensors Configuration

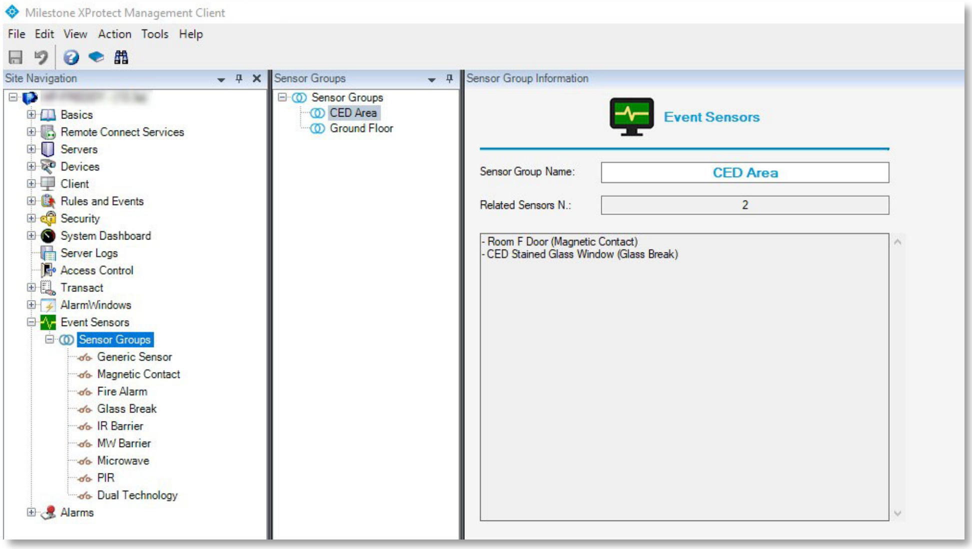
Before creating the Virtual Sensors it is necessary to create the Groups that collect them. To do this, simply open the plugin tree, select the Groups node then right-click on the root node and select the item "Add new ...".



Event Sensor - Groups of Sensors

Here it's possible to add one or more Virtual Sensor Groups. They haven't any properties, are just usefull for data organization.

If, on the contrary, an existing group is selected, the plugin shows the quantity of Virtual Sensors associated with it and the relative type.

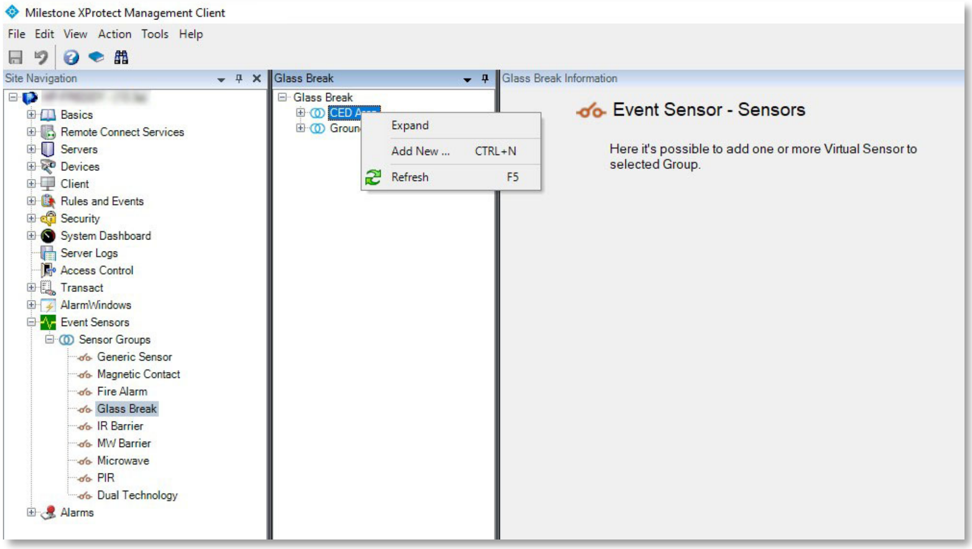


Sensor Group Name: CED Area

Related Sensors N.: 2

- Room F Door (Magnetic Contact)
- CED Stained Glass Window (Glass Break)

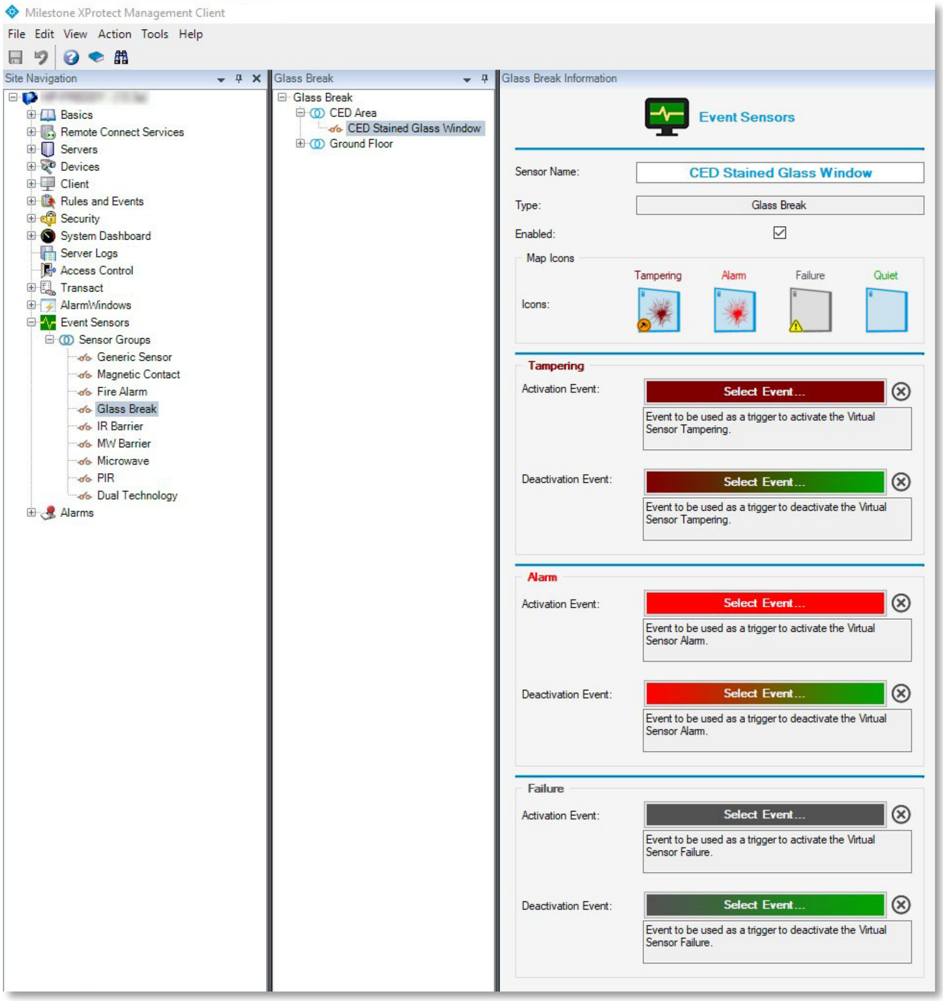
After creating the Groups, you can populate them by creating the sensors that belong to them. To do this, select the type of sensor you want to create on the plugin tree, then in the central part select the Group to which you want to associate the sensor, click the right button of the mouse, and select the item "Add new ...".



Event Sensor - Sensors

Here it's possible to add one or more Virtual Sensor to selected Group.

At this point, all the parameters that regulate the behavior of the Virtual Sensor during creation must be configured.



Sensor Name: CED Stained Glass Window

Type: Glass Break

Enabled: ☑

Tampering

Activation Event: Select Event...

Event to be used as a trigger to activate the Virtual Sensor Tampering.

Deactivation Event: Select Event...

Event to be used as a trigger to deactivate the Virtual Sensor Tampering.

Alarm

Activation Event: Select Event...

Event to be used as a trigger to activate the Virtual Sensor Alarm.

Deactivation Event: Select Event...

Event to be used as a trigger to deactivate the Virtual Sensor Alarm.

Failure

Activation Event: Select Event...

Event to be used as a trigger to activate the Virtual Sensor Failure.

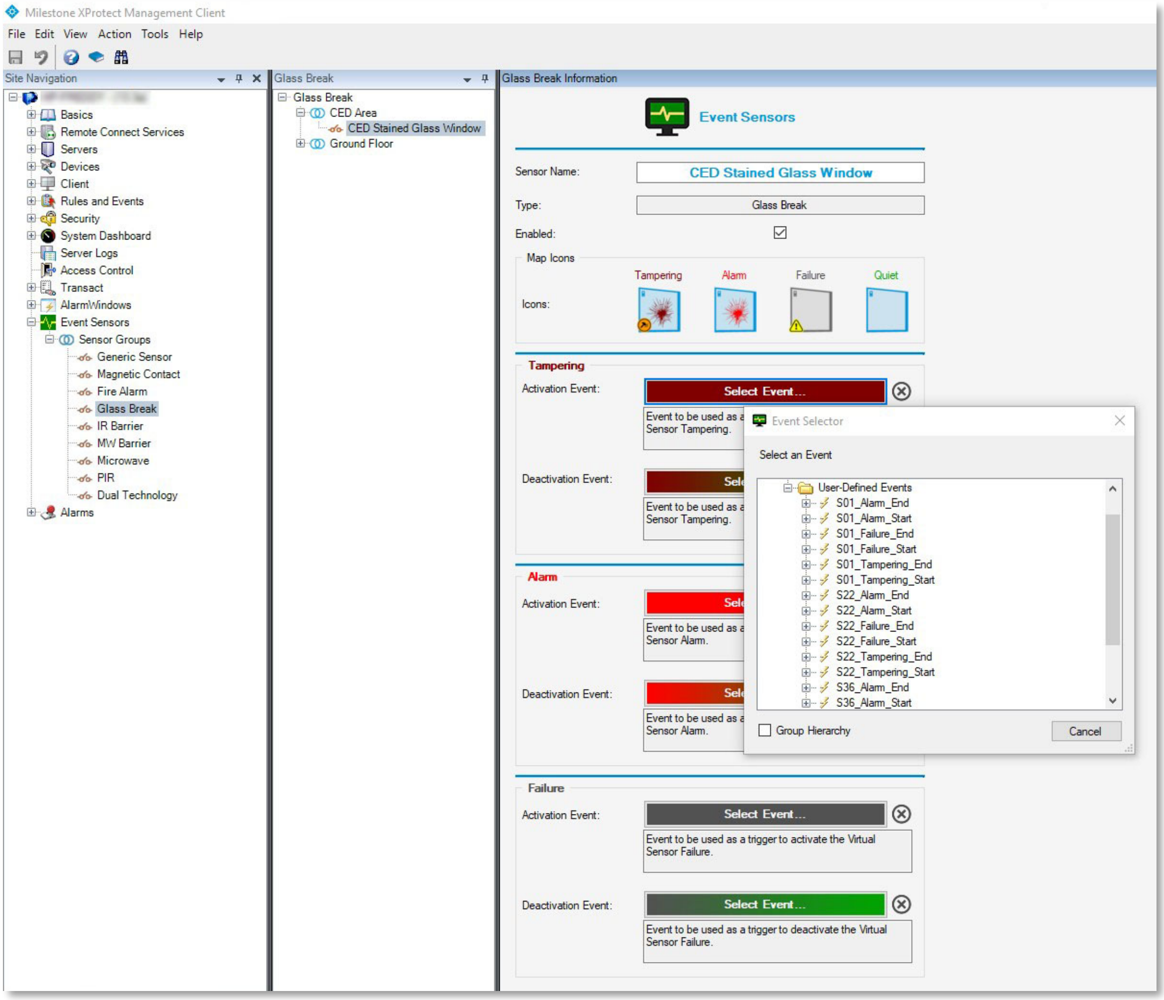
Deactivation Event: Select Event...

Event to be used as a trigger to deactivate the Virtual Sensor Failure.

First, give the Virtual Sensor a name ("CED Stained Glass Window" in the previous example).

WARNING – the XProtect Platform distinguishes the various elements by their own unique ID (not visible) and not by name; this implies that it is possible to create more sensors with the same name and the plugin will still work correctly, but it is obviously possible that this will create confusion for the staff in charge, therefore it is strongly not recommended to do so.

After the name it is necessary to associate the 3 states of Tampering, Alarm and Failure with the external Events that correspond to the Activation and Deactivation messages of these states. To do this, simply click on the relative button (colored), a window for selecting external events will open, simply click on the one you want to associate it with the sensor.



Sensor Name: CED Stained Glass Window

Type: Glass Break

Enabled: ☑

Map Icons

Icons: Tampering Alarm Failure Quiet

Tampering

Activation Event: Select Event...

Event to be used as a Sensor Tampering.

Deactivation Event: Sel

Event to be used as a Sensor Tampering.

Alarm

Activation Event: Sel

Event to be used as a Sensor Alarm.

Deactivation Event: Sel

Event to be used as a Sensor Alarm.

Failure

Activation Event: Select Event...

Event to be used as a trigger to activate the Virtual Sensor Failure.

Deactivation Event: Select Event...

Event to be used as a trigger to deactivate the Virtual Sensor Failure.

Event Selector

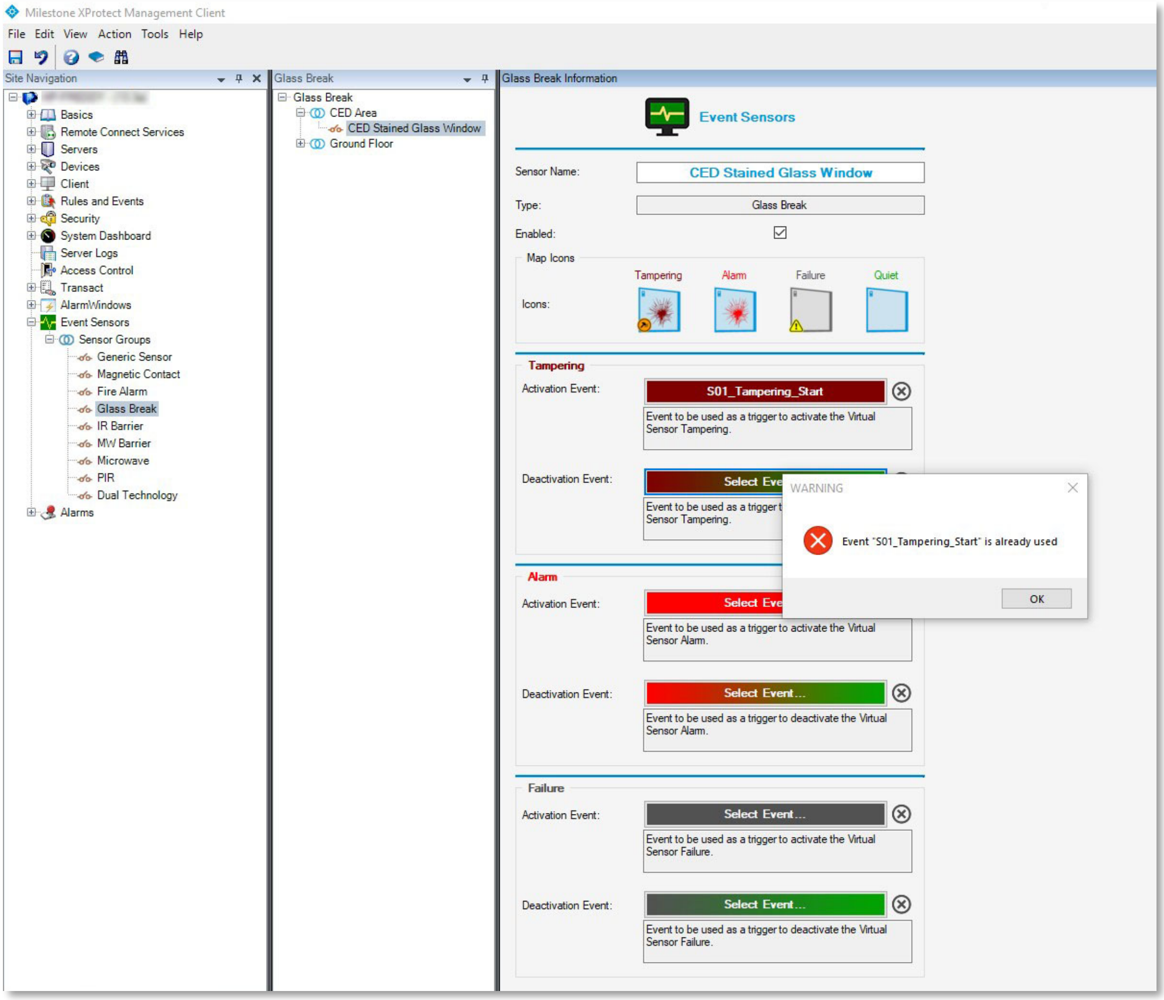
Select an Event

User-Defined Events
S01_Alarm_End
S01_Alarm_Start
S01_Failure_End
S01_Failure_Start
S01_Tampering_End
S01_Tampering_Start
S22_Alarm_End
S22_Alarm_Start
S22_Failure_End
S22_Failure_Start
S22_Tampering_End
S22_Tampering_Start
S36_Alarm_End
S36_Alarm_Start

☐ Group Hierarchy

Cancel

WARNING – it is not possible to select an already associated external event as this would create an unsolvable ambiguity on which sensor/state to activate upon receipt of the message. The plugin prevents this.



Sensor Name: CED Stained Glass Window

Type: Glass Break

Enabled: ☑

Activation Event: S01_Tampering_Start

Event to be used as a trigger to activate the Virtual Sensor Tampering.

Deactivation Event:

Event to be used as a trigger to deactivate the Virtual Sensor Tampering.

Event "S01_Tampering_Start" is already used

Activation Event:

Event to be used as a trigger to activate the Virtual Sensor Alarm.

Deactivation Event:

Event to be used as a trigger to deactivate the Virtual Sensor Alarm.

Activation Event:

Event to be used as a trigger to activate the Virtual Sensor Failure.

Deactivation Event:

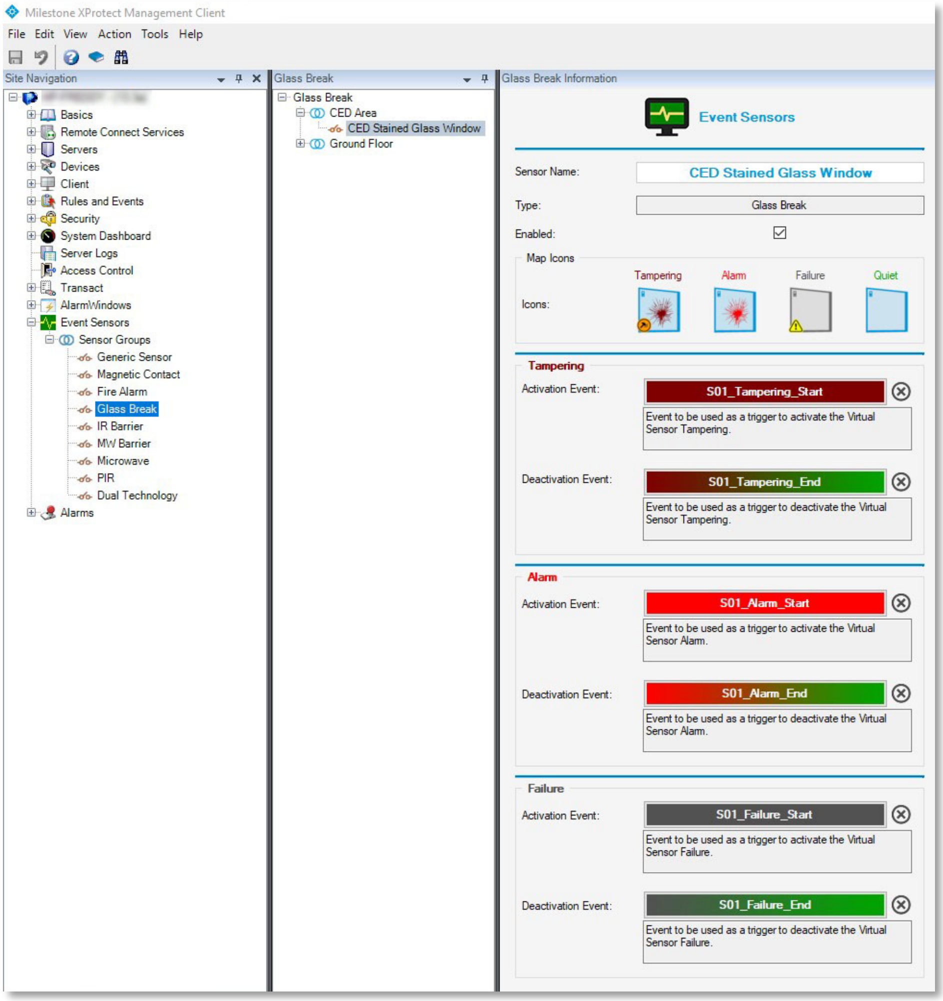
Event to be used as a trigger to deactivate the Virtual Sensor Failure.

The icon ⊗ next to each event association button removes the link between the specific external event and the sensor. It is the only way to do this if you have selected an incorrect event. ATTENTION: to permanently remove the event/sensor association, the sensor configuration must be saved.

It is not essential to configure all the associations, it is sufficient to do so for all the reports managed by the intrusion system. For example, if the system does not reach Safety Grade 4 of the reference standard, it means that it is unable to manage the "Sensor Failure" condition, in this case the "Failure" block can be left empty.

Of course, each activation event (eg. Tampering) must correspond to a Deactivation event (return to quite), if this is not the case, the plugin is still able to activate the configured Alarms, but the subsequent quite condition must be forced manually via contextual menus.

Below is the example of Sensor 01, "CED Stained Glass Window", fully configured.



Sensor Name: CED Stained Glass Window

Type: Glass Break

Enabled: ☑

Map Icons

Icons: Tampering, Alarm, Failure, Quiet

Tampering

Activation Event: S01_Tampering_Start

Event to be used as a trigger to activate the Virtual Sensor Tampering.

Deactivation Event: S01_Tampering_End

Event to be used as a trigger to deactivate the Virtual Sensor Tampering.

Alarm

Activation Event: S01_Alarm_Start

Event to be used as a trigger to activate the Virtual Sensor Alarm.

Deactivation Event: S01_Alarm_End

Event to be used as a trigger to deactivate the Virtual Sensor Alarm.

Failure

Activation Event: S01_Failure_Start

Event to be used as a trigger to activate the Virtual Sensor Failure.

Deactivation Event: S01_Failure_End

Event to be used as a trigger to deactivate the Virtual Sensor Failure.

Note that the Virtual Sensor can be disabled, if necessary, by removing the check in the appropriate box.

At this point, it is necessary to highlight a "strange" behavior of the XProtect Platform: when the plugin intercepts an activation event of its competence, it generates a system event corresponding to a "New Alarm", the Platform consequently generates an Alarm condition with the “New” status which, among other things, implies the activation of the flashing red circle around the sensor that originated it.

When the plugin intercepts, for the same sensor, the deactivation event, in addition to changing the icon that represents the new status of the sensor, it could send to the platform an event similar to the previous one but with the status "On Hold"(1), if the operator has not yet acknowledged the event, or with the status "Closed" if the acknowledgment had been made.

Unfortunately, the Platform removes the flashing red circle from any state change of the alarm, even if it has not yet been acknowledged. There is therefore a risk that with a pending alarm (New), if the "On Hold" status is forced when the deactivation event is received, with consequent removal of the flashing red circle, the operator could completely miss the event.

For this reason, in the EventSensors.dll.config configuration file there is a global parameter that inhibits or not the alarm change status, while the change of the status icon takes place anyway. The parameter (in XML) is:

key="ChangeAlarmState" value="False"

which corresponds to avoid sending the alarm status change command to the Platform, in order to keep the flashing red circle. Any value other than False, on the contrary, implies sending the command to change the alarm state.

Although the default seems the most obvious choice, the end user can decide at any time to alter this behavior.

WARNING: any parameter modification must be made with the two Clients closed and the Event Server disabled, otherwise the change will take effect only at the next restart of the Platform.

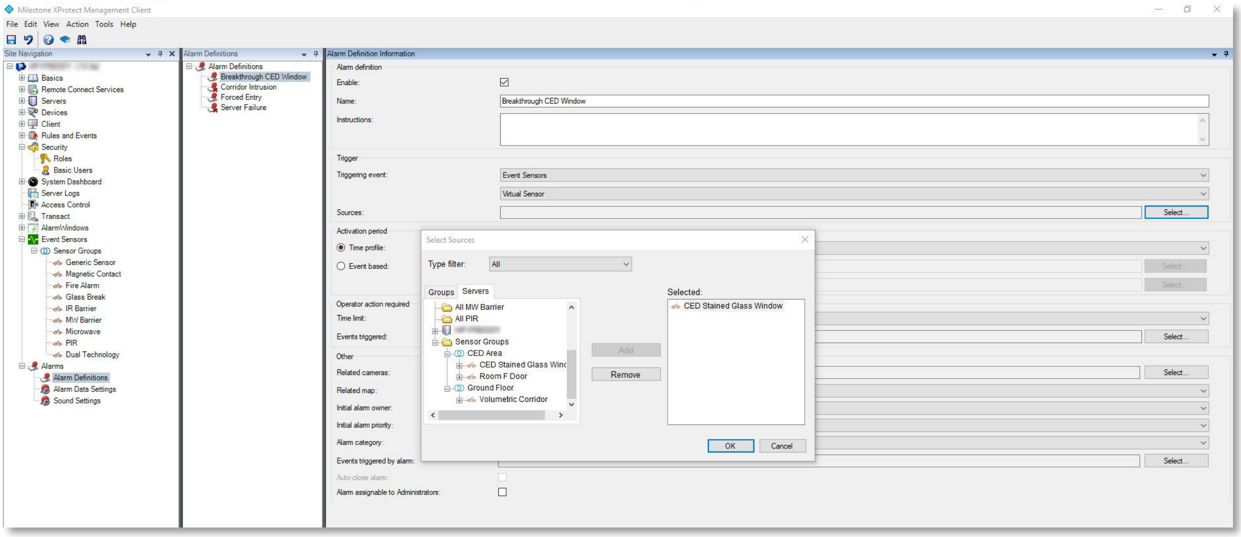
4.3 Alarm Configuration

For a detailed description, refer to the specific documentation of the XProtect Platform.

Below are example screenshots of a hypothetical Alarm Configuration.

(1) The "On Hold" status corresponds to the condition in which the sensor has returned to the quiet state, but the operator has yet to acknowledge the event. On the contrary, the "In Progress" status corresponds to the condition in which the operator has acknowledged but the sensor is still excited.

WARNING – although it is possible to create an Alarm with the same name as a Virtual Sensor (eg. Garage Access Door), it is essential to avoid doing so because when an external sensor activation event occurs, the System generates the "Garage Access Door" alarm message, and the Plugin that intercepts it generates in turn a Change State (and relative icon) with the same name. Although everything works correctly since the two messages are produced in successive times, 2 messages with the same name but different actions are registered in the System DB, and this creates ambiguity; with the growth of these situations, the Event Server, committed to trying to resolve these ambiguities, begins to manifest incorrect behaviors, among which, the most frequent is that, in the start-up phase, to remain in the Starting state, without ever reaching the state of complete operation.



Alarm Definition Information

Alarm definition

Enable: ☑

Name: Breakthrough CED Window

Instructions:

Trigger

Triggering event: Event Sensors

Virtual Sensor

Sources:

Activation period

● Time profile:

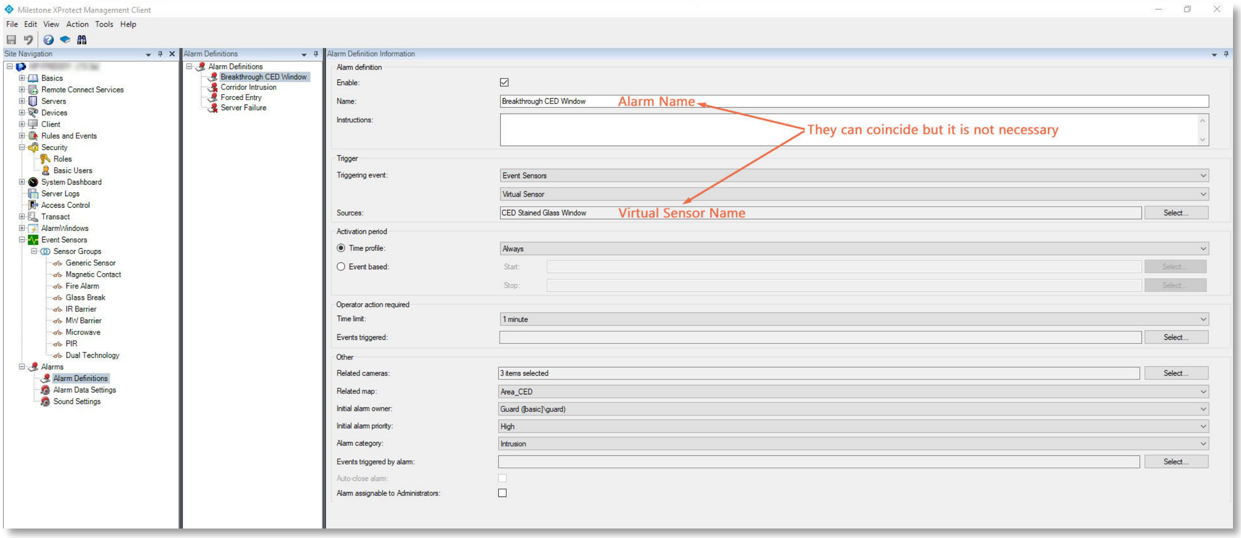
○ Event based:

Select Sources

Type filter: All

Selected: CED Stained Glass Window

Alarm assignable to Administrators: □



Alarm Definition Information

Alarm definition

Enable: ☑

Name: Breakthrough CED Window

Alarm Name

They can coincide but it is not necessary

Instructions:

Trigger

Triggering event: Event Sensors

Virtual Sensor

Sources: CED Stained Glass Window

Virtual Sensor Name

Activation period

● Time profile: Always

○ Event based: Start: Stop:

Operator action required

Time limit: 1 minute

Events triggered:

Other

Related cameras: 3 items selected

Related map: Area_CED

Initial alarm owner: Guard ([basic]\guard)

Initial alarm priority: High

Alarm category: Intrusion

Events triggered by alarm:

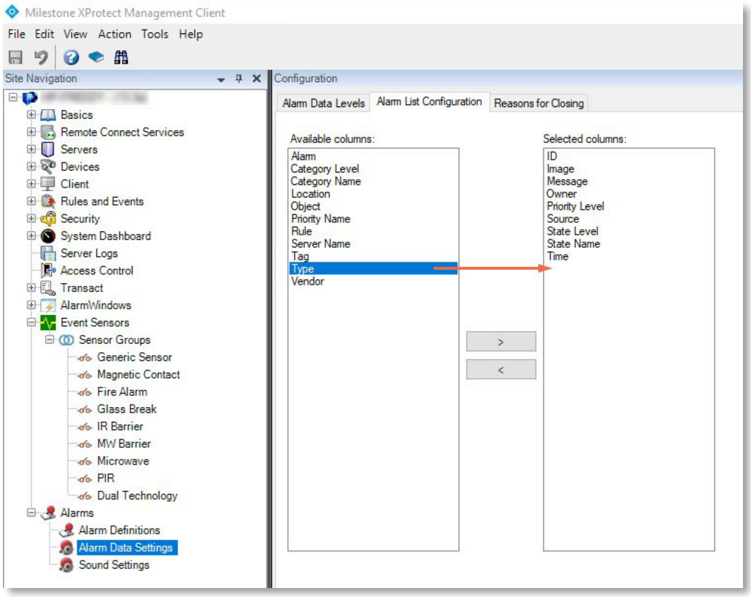
Auto-close alarm: □

Alarm assignable to Administrators: □

4.3.1 Tips

To improve the identification of the Alarms on the Smart Client it is suggested to add, and make visible, an additional column to the list of Smart Client alarms.

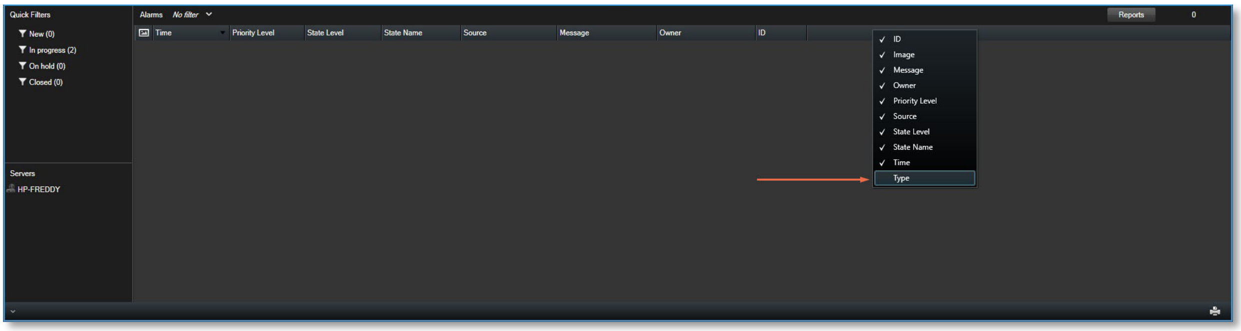
To do this, you must first activate the use of the new column via the Management Client; select "Alarm data settings", then the "Alarm list configuration" tab and add "Type" to the "Selected columns".

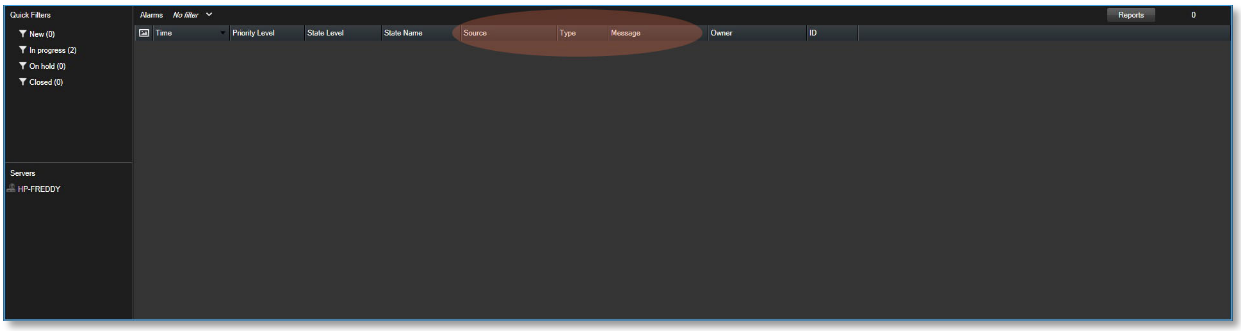


Available columns:
Alarm
Category Level
Category Name
Location
Object
Priority Name
Rule
Server Name
Tag
Type
Vendor

Selected columns:
ID
Image
Message
Owner
Priority Level
Source
State Level
State Name
Time

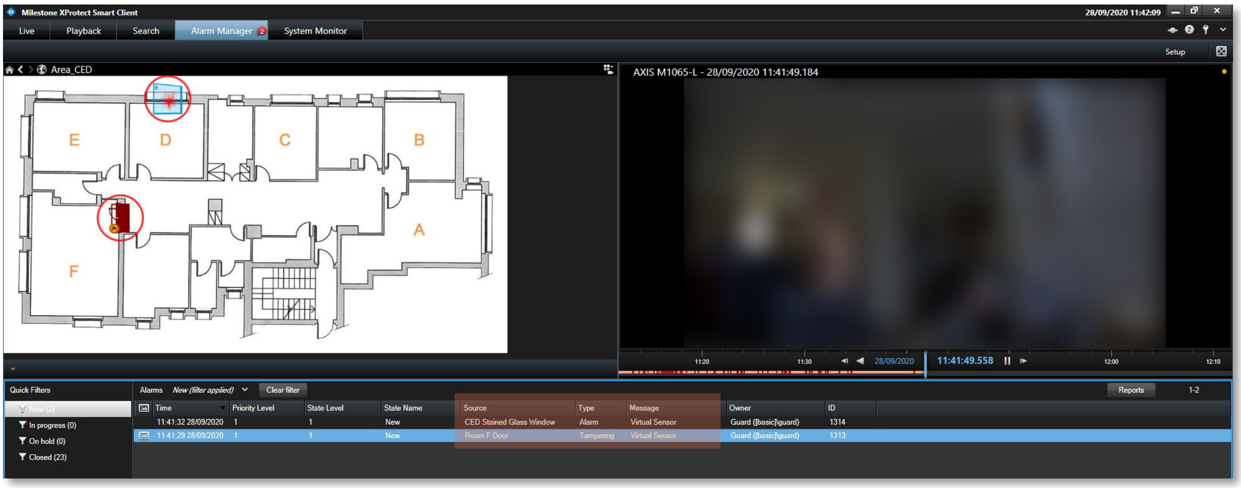
On the Smart Client alarm list, click the right mouse button and activate the display of the "Type" column, then drag the columns so that the "Source" - "Type" – "Message" columns are positioned consecutively.





Time	Priority Level	State Level	State Name	Source	Type	Message	Owner	ID

Whit this arrangement, when an alarm occurs, the 3 highlighted columns report complete information on the type of event that occurred. The added "Type" column naturally reports the type of event detected (Tamper, Alarm, Fault) to which the specific icon of the specific Virtual Sensor corresponds.

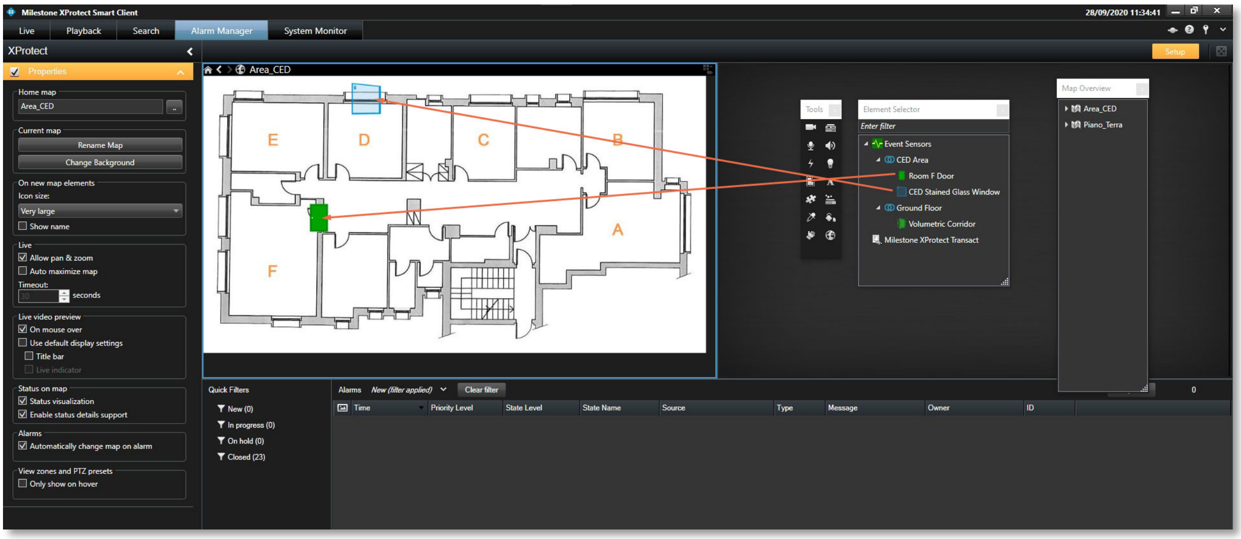


Time	Priority Level	State Level	State Name	Source	Type	Message	Owner	ID
11:41:32 28/09/2020	1	1	New	CED Stained Glass Window	Alarm	Virtual Sensor	Guard ([basic]\guard)	1314
11:41:29 28/09/2020	1	1	New	Room F Door	Tampering	Virtual Sensor	Guard ([basic]\guard)	1313

4.4 Positioning of Virtual Sensor Icons on Graphic Maps

For a detailed description, refer to the specific documentation of the XProtect Platform.

Below are example screenshots of the positioning of the Virtual Sensors on Maps.



☑ Properties

Home map: Area_CED

Current map
Rename Map
Change Background

On new map elements
Icon size: Very large
☐ Show name

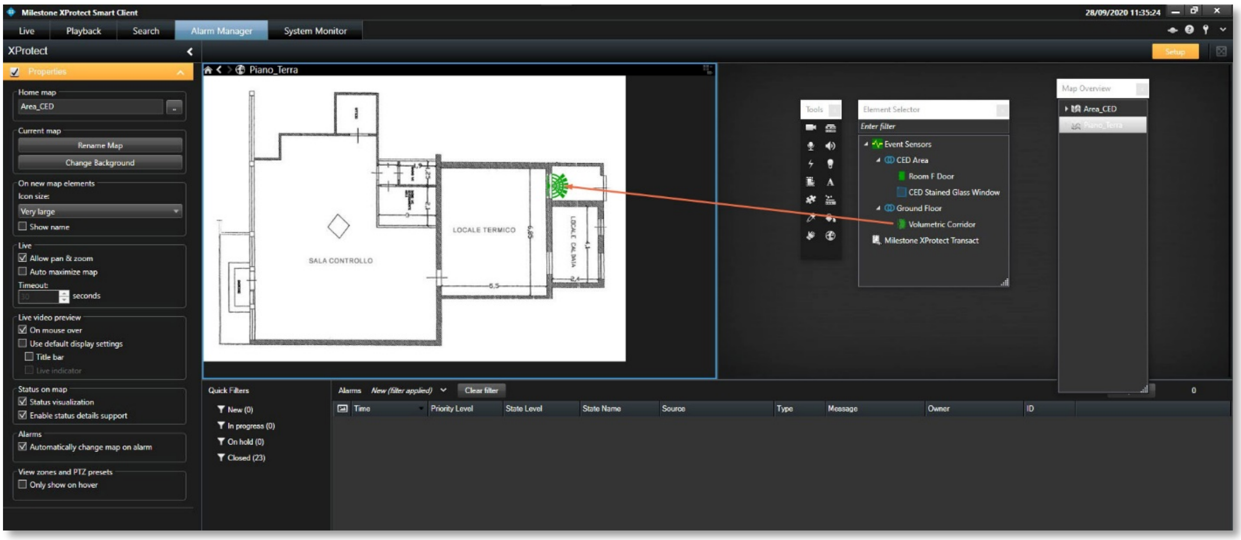
Live
☑ Allow pan & zoom
☐ Auto maximize map
Timeout: 30 seconds

Live video preview
☑ On mouse over
☐ Use default display settings
☐ Title bar
☐ Live indicator

Status on map
☑ Status visualization
☑ Enable status details support

Alarms
☑ Automatically change map on alarm

View zones and PTZ presets
☐ Only show on hover



☑ Properties

Home map: Area_CED

Current map
Rename Map
Change Background

On new map elements
Icon size: Very large
☐ Show name

Live
☑ Allow pan & zoom
☐ Auto maximize map
Timeout: 30 seconds

Live video preview
☑ On mouse over
☐ Use default display settings
☐ Title bar
☐ Live indicator

Status on map
☑ Status visualization
☑ Enable status details support

Alarms
☑ Automatically change map on alarm

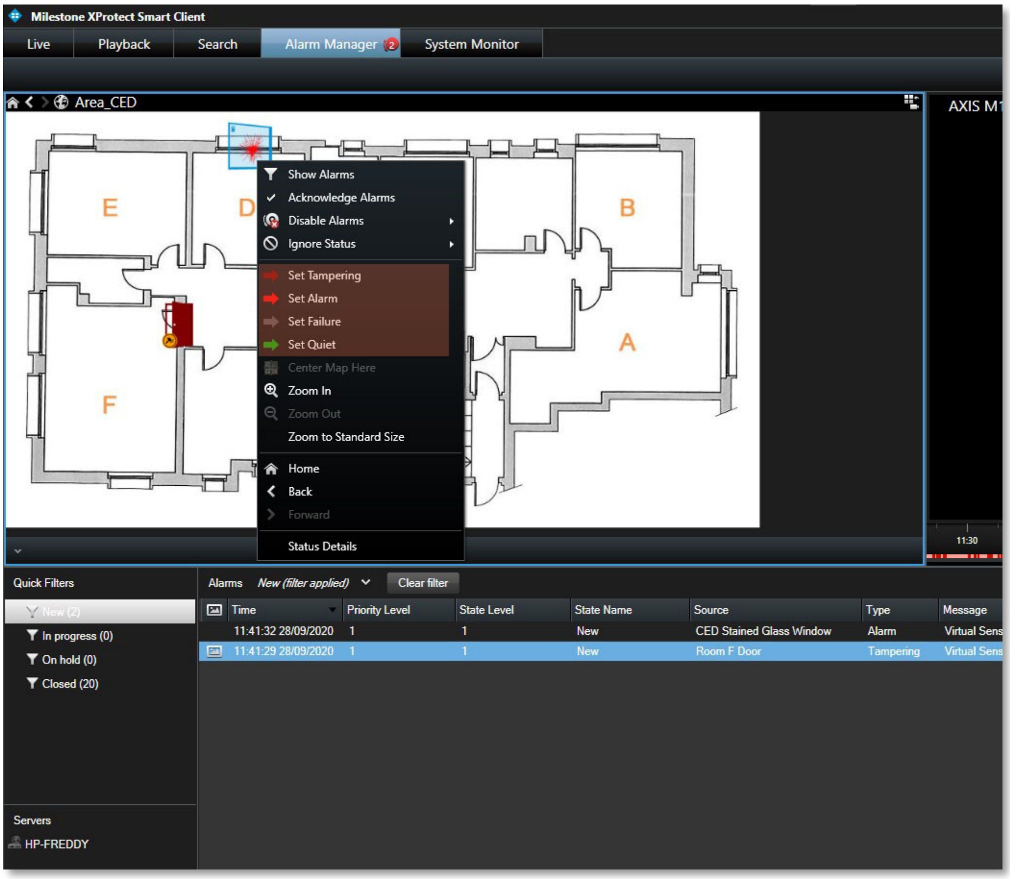
View zones and PTZ presets
☐ Only show on hover

5 Plugin Operational Management

At this point, if the configuration has been performed correctly, the plugin is fully operational and able to carry out their work independently, as shown in the previous image on page 20.

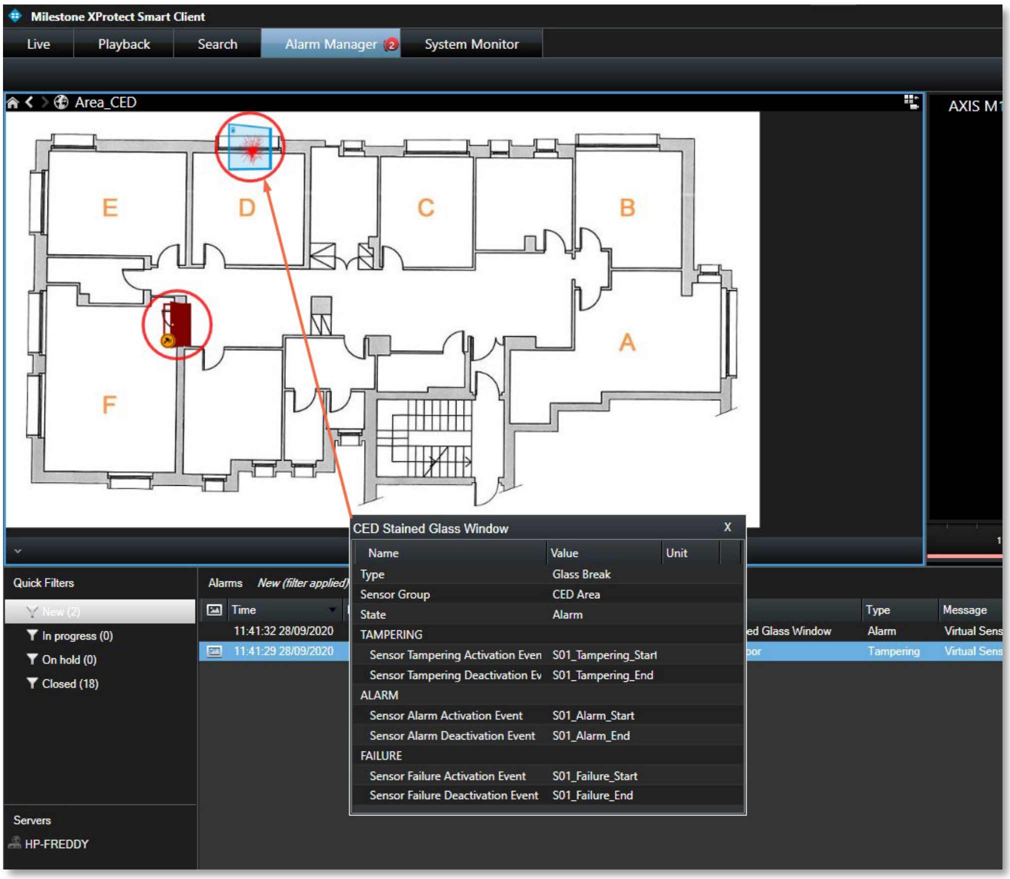
The only feature not yet illustrated is the one that shows detailed information of the individual sensors by acting directly on the icon on the maps.

Selecting a sensor and click with the right mouse button in order to bring up the contextual menu of that element (the same applies to any other type of element managed by the platform).



Time	Priority Level	State Level	State Name	Source	Type	Message
11:41:32 28/09/2020	1	1	New	CED Stained Glass Window	Alarm	Virtual Sens
11:41:29 28/09/2020	1	1	New	Room F Door	Tampering	Virtual Sens

To be noted the Commands to force the sensor status with the arrow icons shown above. Select the last item "Status Details" to get detailed information on the selected item and the following is obtained.



Time		Type	Message
11:41:32 28/09/2020	ed Glass Window	Alarm	Virtual Sens
11:41:29 28/09/2020	oor	Tampering	Virtual Sens

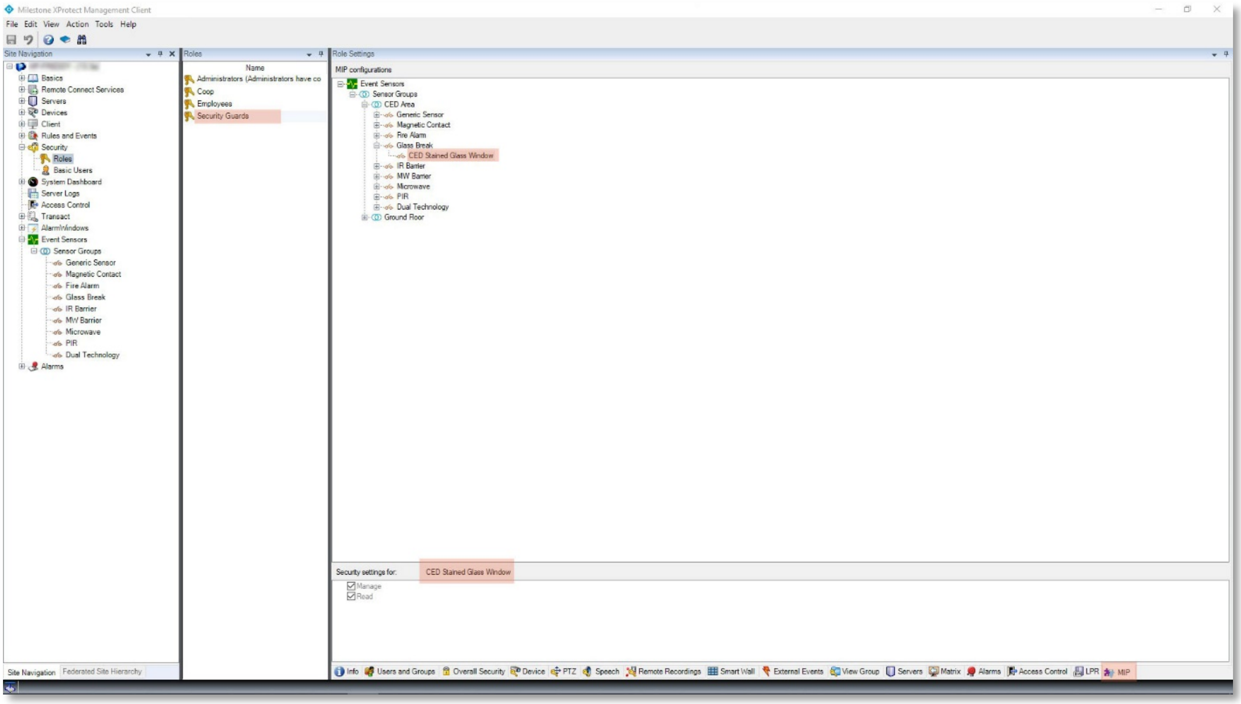
CED Stained Glass Window

Name	Value	Unit
Type	Glass Break	
Sensor Group	CED Area	
State	Alarm	
TAMPERING		
Sensor Tampering Activation Even	S01_Tampering_Start	
Sensor Tampering Deactivation Ev	S01_Tampering_End	
ALARM		
Sensor Alarm Activation Event	S01_Alarm_Start	
Sensor Alarm Deactivation Event	S01_Alarm_End	
FAILURE		
Sensor Failure Activation Event	S01_Failure_Start	
Sensor Failure Deactivation Event	S01_Failure_End	

with the specific window showing the Type, the Parent Group and the current State of the Virtual Sensor, as well as all the External Events associated with it.

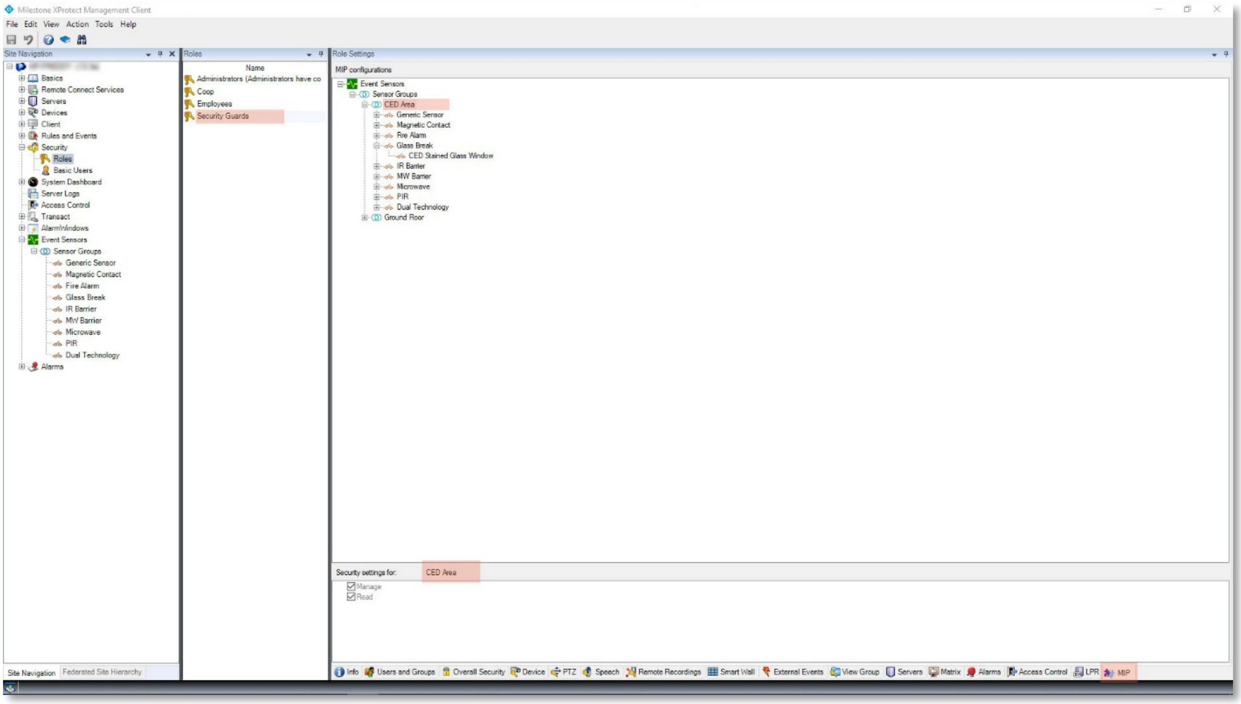
6 Virtual Sensor Access Control List

The plugin allows you to specify the Access Permissions to the Virtual Sensors to be associated with the User Profiles. The Permissions can be assigned both individually to the Virtual Sensors and to all those belonging to a Group by acting on it, as shown in the following images.



Security settings for: CED Stained Glass Window

☑ Manage
☑ Read



Security settings for: CED Area

☑ Manage
☑ Read

By default, all operations are allowed to all User Profiles. If Manage is disabled, Users of the selected Profile are prevented from executing the Commands (status change) present in the Contextual Menus; also disabling Read Only prevents the complete visibility of the Virtual Sensors.

7 Application 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 manageable Virtual Sensors.

milestone

TECHNOLOGY
PARTNER

SECURSYS