



## Plugin Manual



---

### Revision Table

Rev.	Date	Changes
1.0.0.0	31/10/2024	Manual first public issue

---

### Acronyms

- **dll** dynamic-link library
- **ES** XProtect Event Server
- **FW** Firmware
- **GUID** Globally Unique Identifier
- **MC** XProtect Management Client
- **MIP** Milestone Integration Platform
- **MS** XProtect Management Server
- **RS** XProtect Recording Server
- **SC** XProtect Smart Client
- **URL** Uniform Resource Locator

---

## Contents

---

<b>1</b>	<b>Intro</b> .....	<b>4</b>
<b>2</b>	<b>Administration (MC)</b> .....	<b>5</b>
	2.1 Creating a new Server.....	5
	2.2 Triggering Events.....	9
	2.3 Managed Analytics Events.....	9
	2.4 Options.....	11
<b>3</b>	<b>Operations (SC)</b> .....	<b>12</b>
	3.1 Dedicated Workspace.....	12
	3.2 Graphic Maps.....	13
	3.3 Views.....	14
	3.4 Event Notifications.....	15
	3.5 Analytics Events.....	18
<b>4</b>	<b>Plugin Installation</b> .....	<b>20</b>

## 1 Intro

This document describes the activities to be performed for using the iDefender plugin. It is divided into two distinct sections:

- Administration (MC), where all the operations necessary to correctly configure the plugin are illustrated
- Operation (SC), where all the features available to Users are described

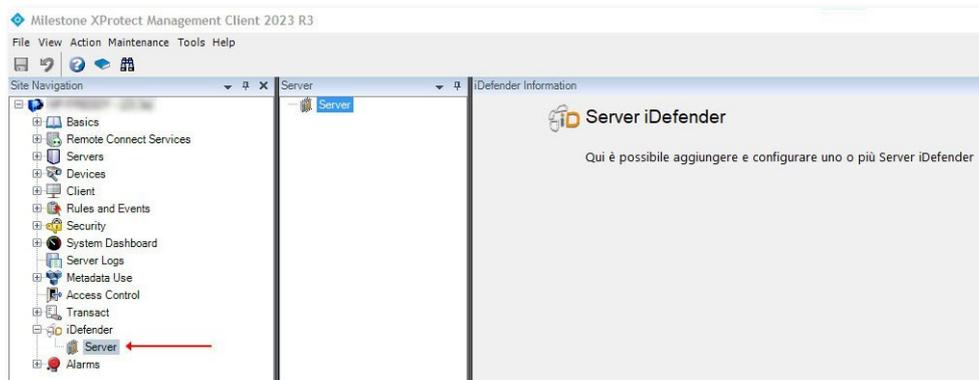
## 2 Administration (MC)

The Plugin is able to manage one or more iDefender servers, for each of them the following information is required:

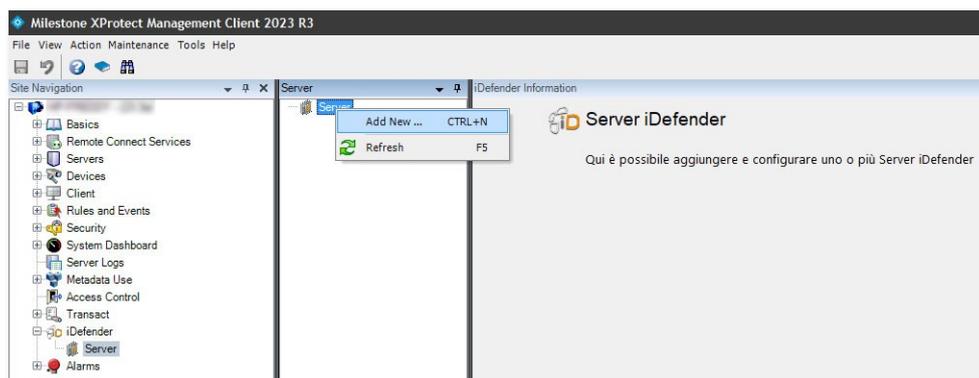
- Networking Parameters
- Server ID
- Server Name
- List of Controlled XProtect Cameras

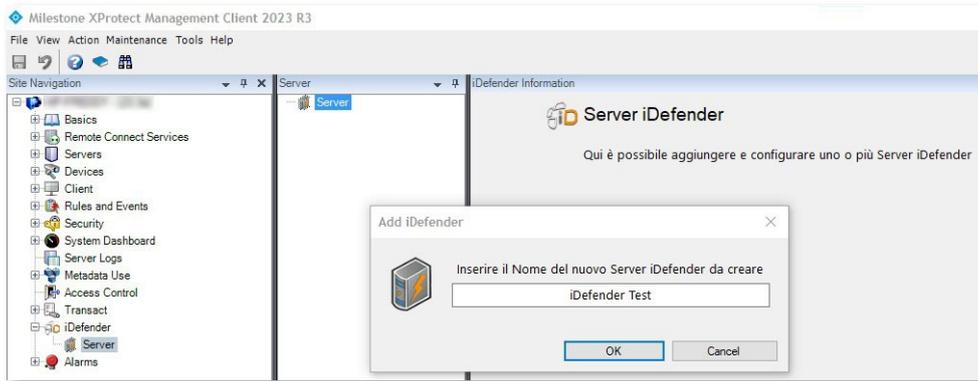
### 2.1 Creating a new Server

After starting the MC select the Plugin Server icon to add the servers to configure.

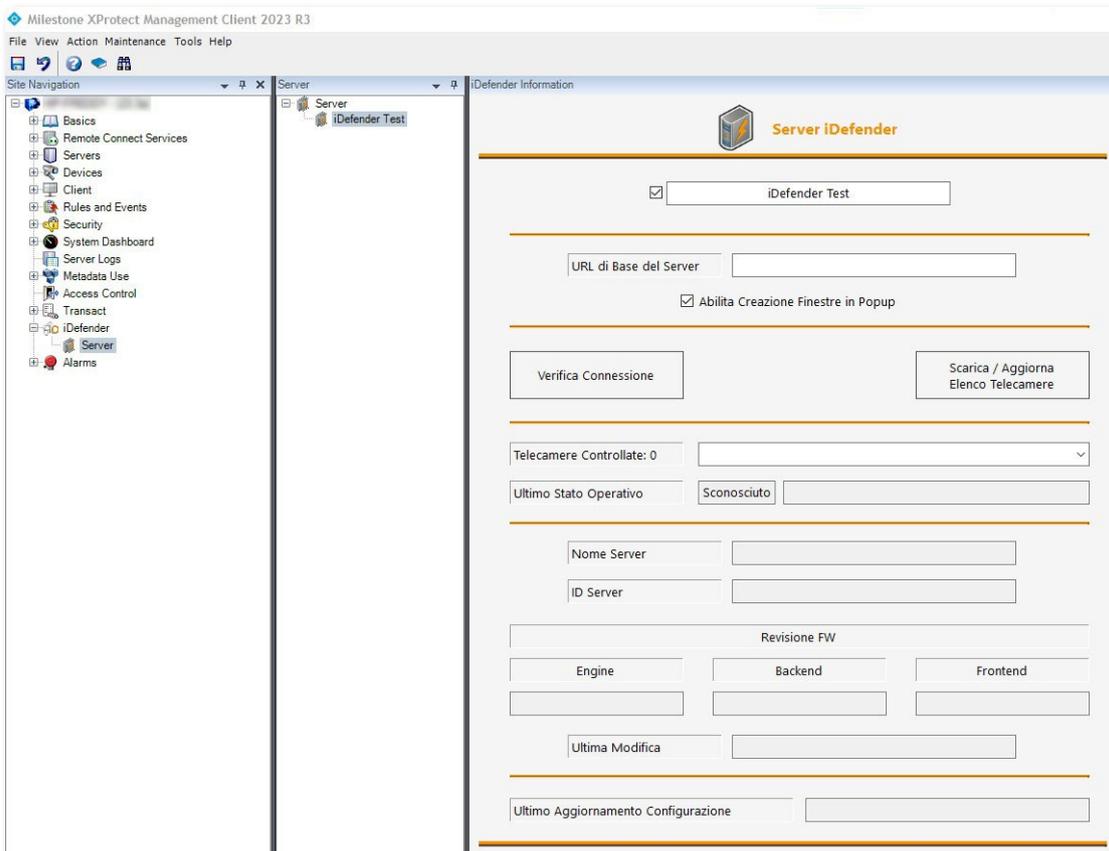


Right-click on the Server icon and select "Add New ...".



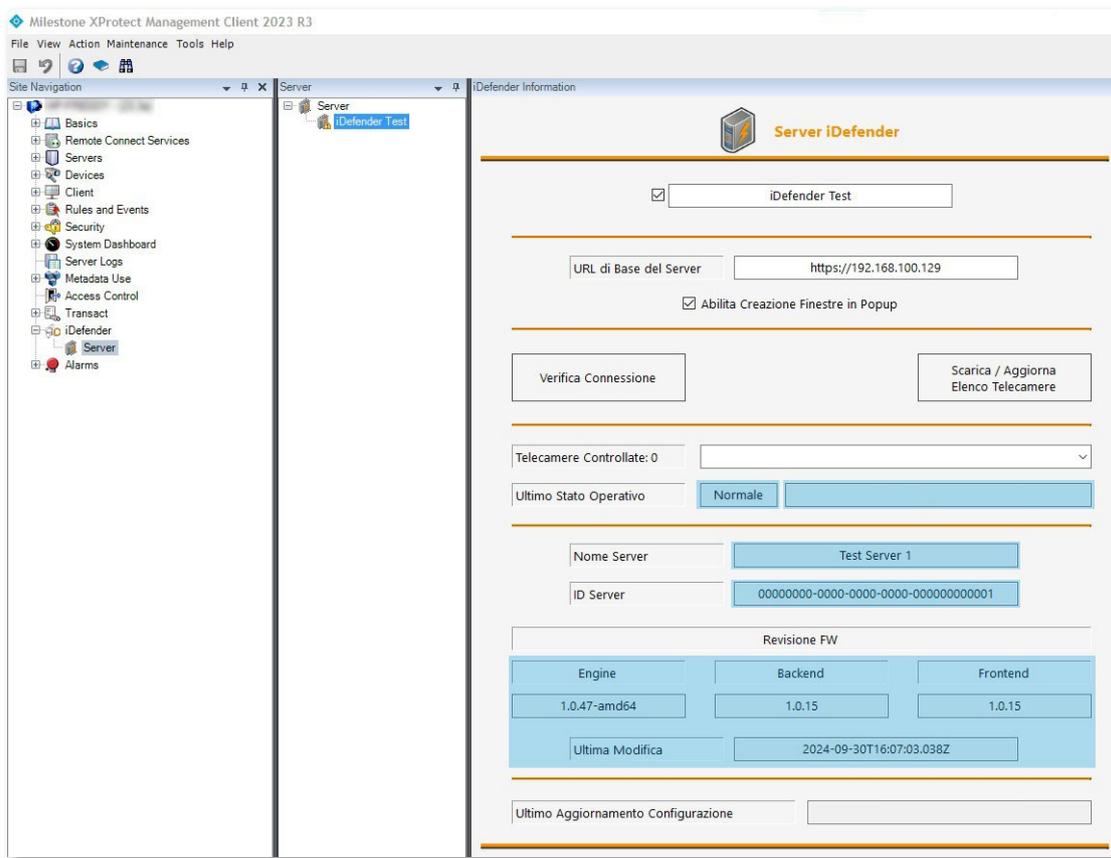


Enter the name of the server you want to create in the box. If the name is not already used, the configuration window for the newly created server will open.



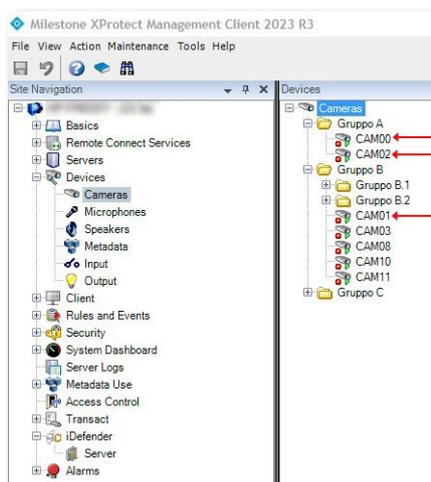
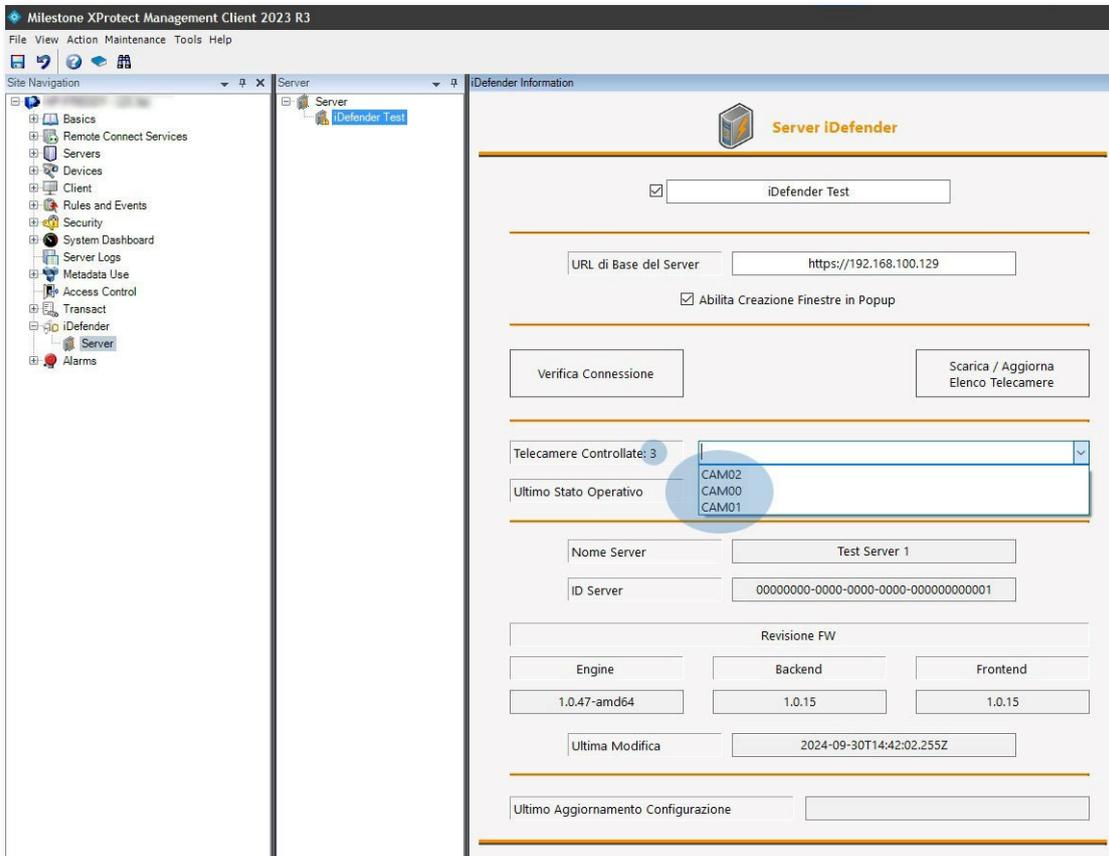
First you need to enter the Server URL then click on the left button "Check Connection", if the address is correct and the server is online it will respond with the following information:

- Name
- ID
- Operational Status and description of the reason in case of Critical or Error status
- FW Revision Information



If everything is OK you should now click on the right button to download the list of XProtect cameras controlled by the Server.

The Server responds with a list of camera GUIDs, then the plugin checks that those GUIDs correspond to cameras on the Platform.

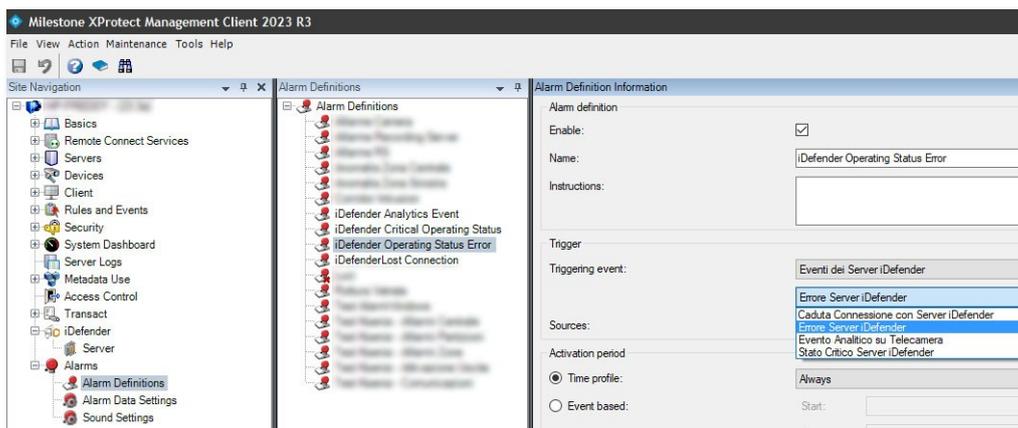


The last field at the bottom "Last Configuration Update" refers to the MIP Item.

## 2.2 Triggering Events

The Plugin is able to manage 4 types of Triggers that can be used to activate Alarms and/or other specific Events, these are:

- Lost Connection
- Critical Operating Status
- Operating Status Error
- Analytics Event



The Source of the first three triggers is obviously the Server while the last one are Cameras. BE CAREFUL: The Analytics Events trigger does not distinguish between the type of Event detected, it is triggered by any type.

## 2.3 Managed Analytics Events

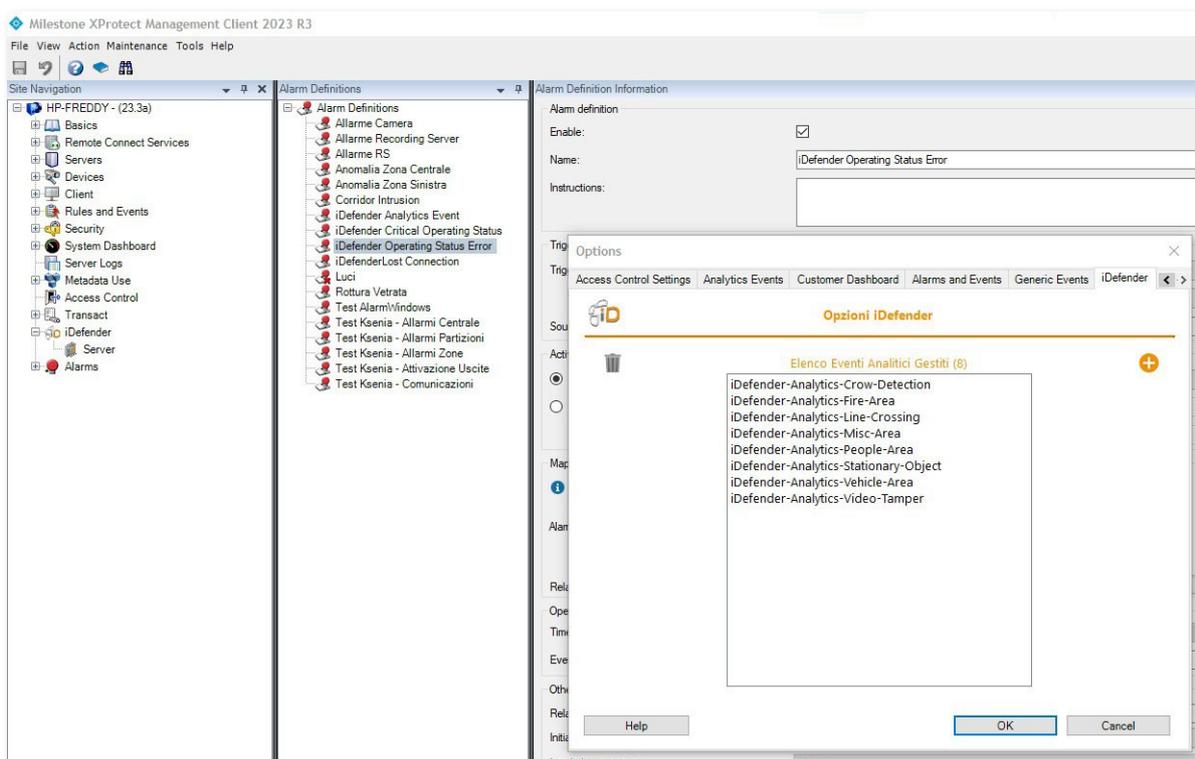
The iDefender Server is capable of detecting and managing a wide range of events, among which:

- **vehicle-area:** detection of vehicles in a specified area, this could include unauthorized vehicles entering restricted zones
- **people-area:** identification of people within certain areas, which can help detect intrusions or movement in sensitive locations
- **fire-area:** detection of fire or the presence of smoke in a monitored area, enabling rapid response to potential fire hazards
- **misc-area:** monitoring for miscellaneous objects or activities that may not fall into predefined categories but are deemed of interest
- **line-crossing:** detection of objects or people crossing a defined line or boundary, which is often used for perimeter security
- **stationary-object:** recognition of objects that remain stationary in a defined area for a specific duration, potentially indicating abandoned items or hazards

- **crowd-detection:** detection of crowd formation or unusual gatherings of people, which may indicate public safety issues or unauthorized assembly
- **video-tamper:** detection of video tampering, such as camera occlusion, defocusing, or other interference that may compromise video integrity.

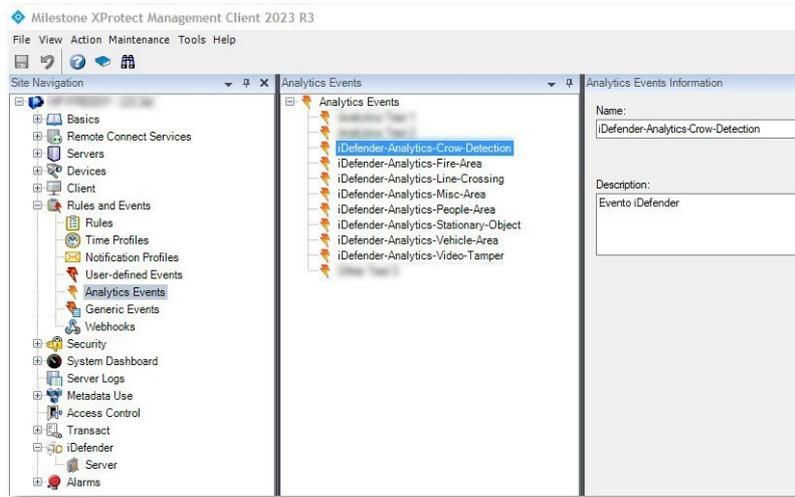
In order to have triggers for specific Events managed by the Server, it is necessary to create related Analytics Events on the Platform that will be activated by the Plugin.

To achieve this goal, you need to use the specific Tab in the Options menu.

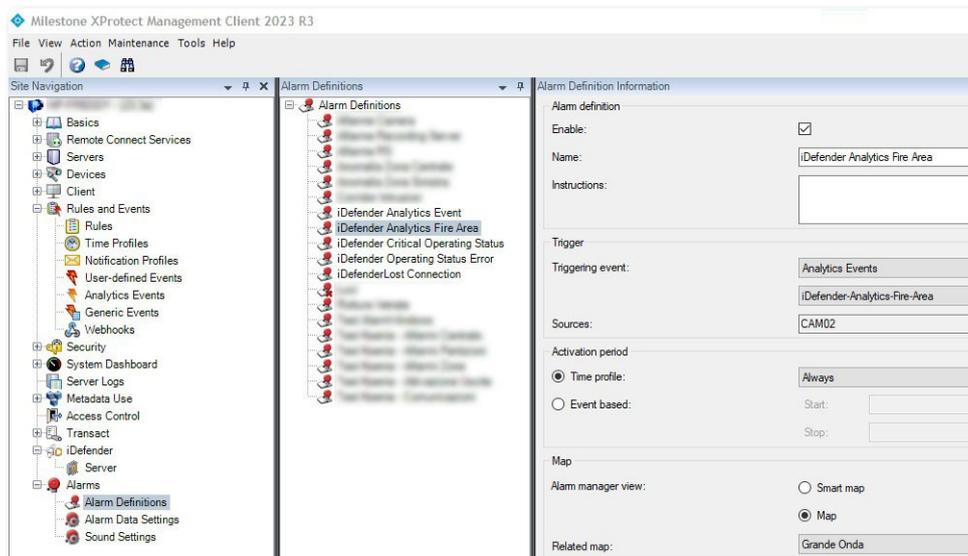


The ones shown are the default, but you can delete and/or add others.

When you save these Rules parameters, the Plugin creates (with the same name) the related Analytics Events on the Platform.



This allows you to configure Alarms for the specific Analytics Event.



## 2.4 Options

There are two checkboxes in the Server page, the one next to the Name represents the Enabled Status of the MIP Item, while the other, when active (default), causes on reception of an Analytics Event from the Server a Floating Window opening with the images, live and playback, of the camera involved.

### 3 Operations (SC)

The Plugin associates a set of Graphic Map Icons with iDefender Server Items that visually represent their current state.

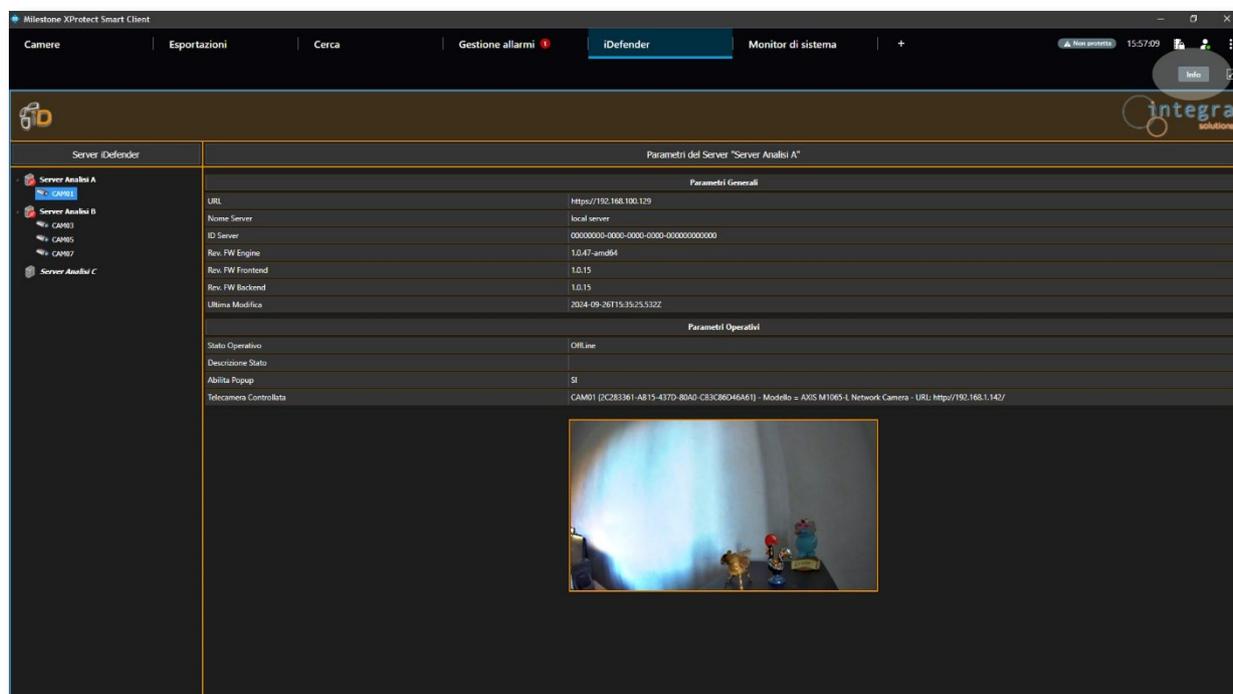
The icon set is as follows:

Disabled	Normal	Offline	Critical	Error
				

We assume that whoever created the System Configuration has included the necessary Graphical Maps by placing the iDefender Server Icons on them.

#### 3.1 Dedicated Workspace

The Plugin has its own Workspace where, for each server present, the Status and Operational information are listed, including the list of controlled cameras.



When you select one of the cameras in the lists, its live stream is displayed.

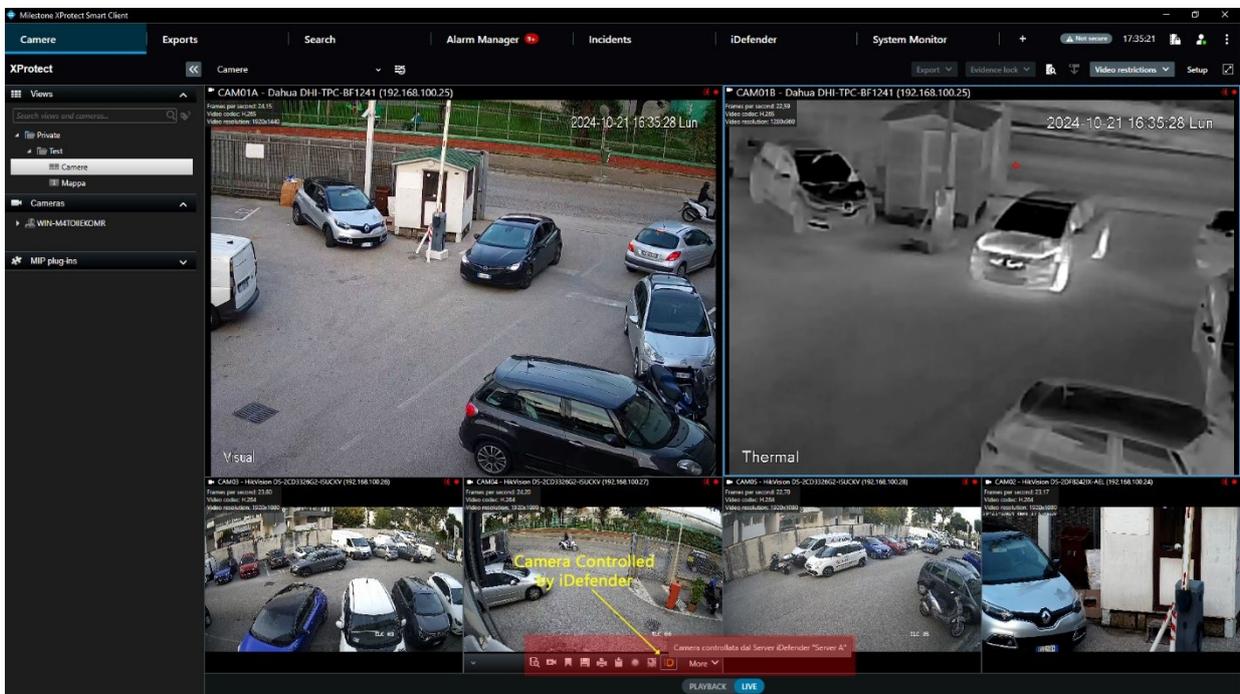
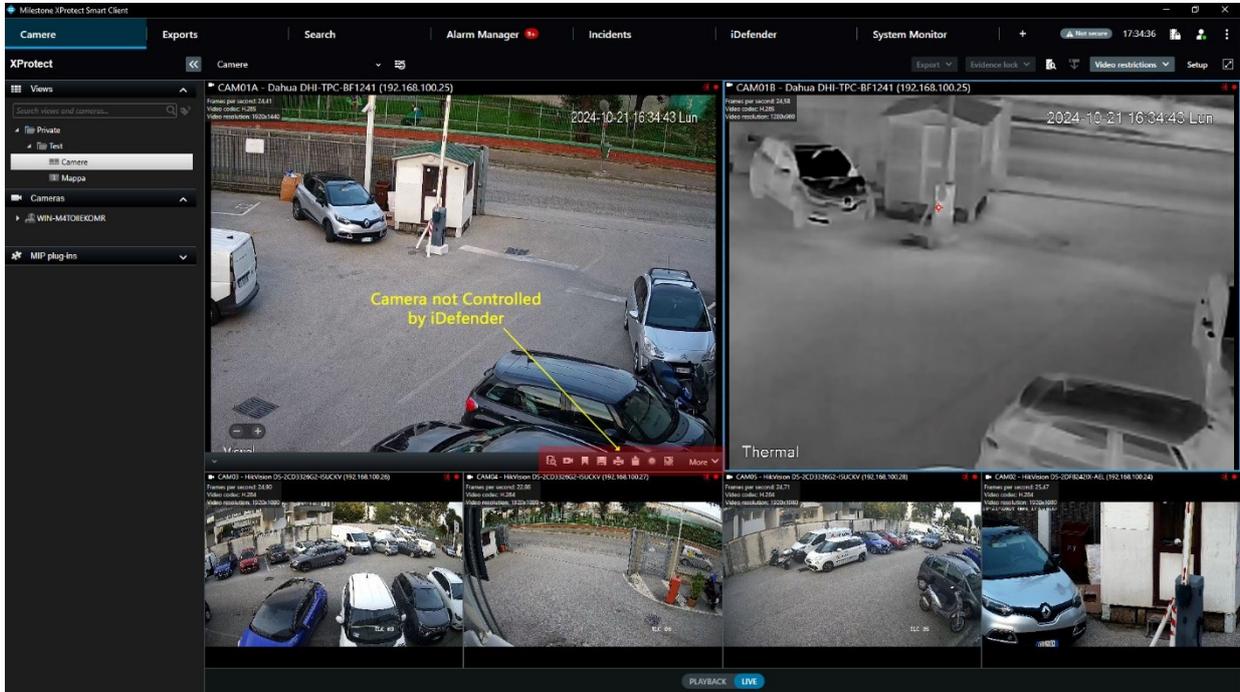
### 3.2 Graphic Maps

The following screenshot shows the Plugin's functionality in relation to Graphic Maps. Right-clicking on the icon gives access to the context menu, including "Status Details"



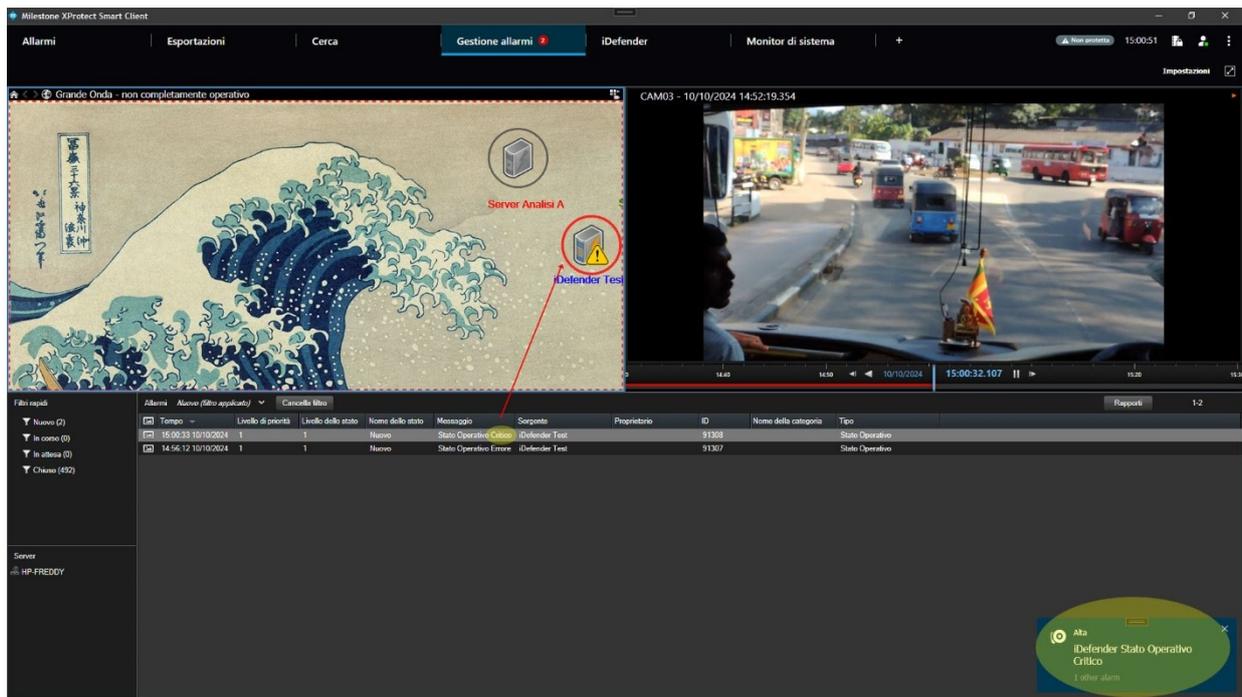
### 3.3 Views

When using SC Views, the plugin adds a small icon to the toolbar of those containing server-controlled cameras, indicating which server is controlling the camera.



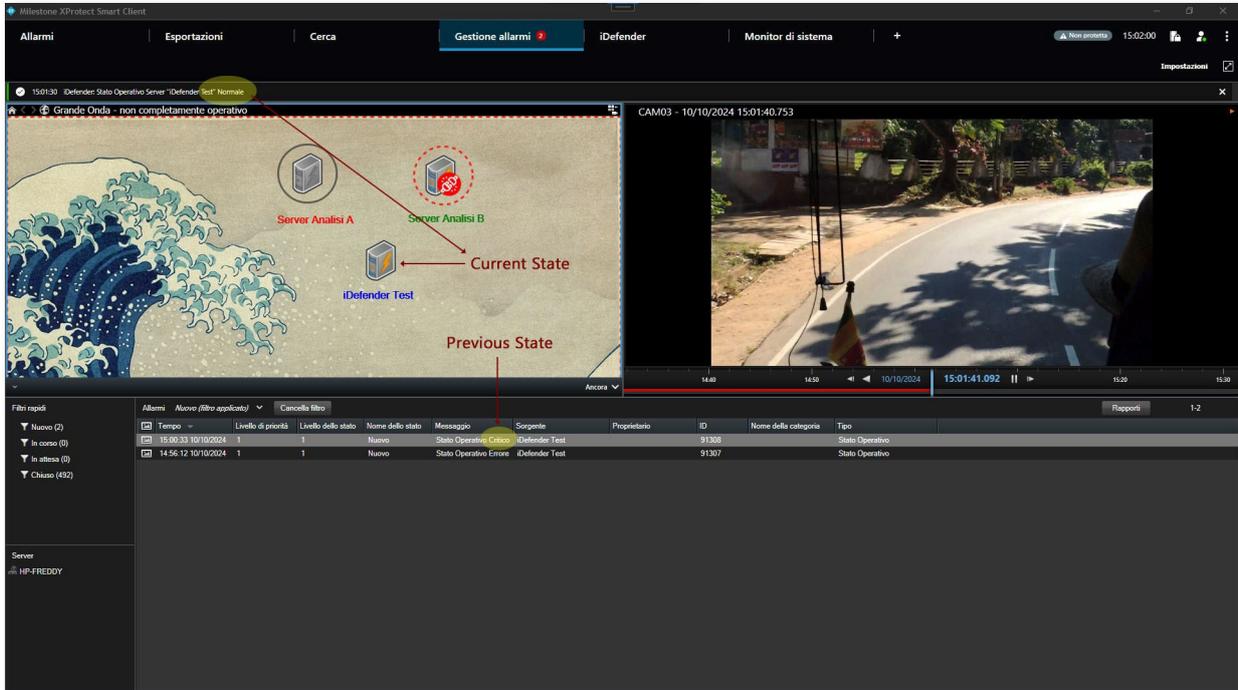
### 3.4 Event Notifications

When one of the 4 types of Events managed by the Plugin occurs (Offline, Critical, Error, Analytics), if the related Alarms have been configured, the event reports are those typical of the Platform, including Toast Message (bottom right corner) if Alarm Desktop Notification has been enabled.



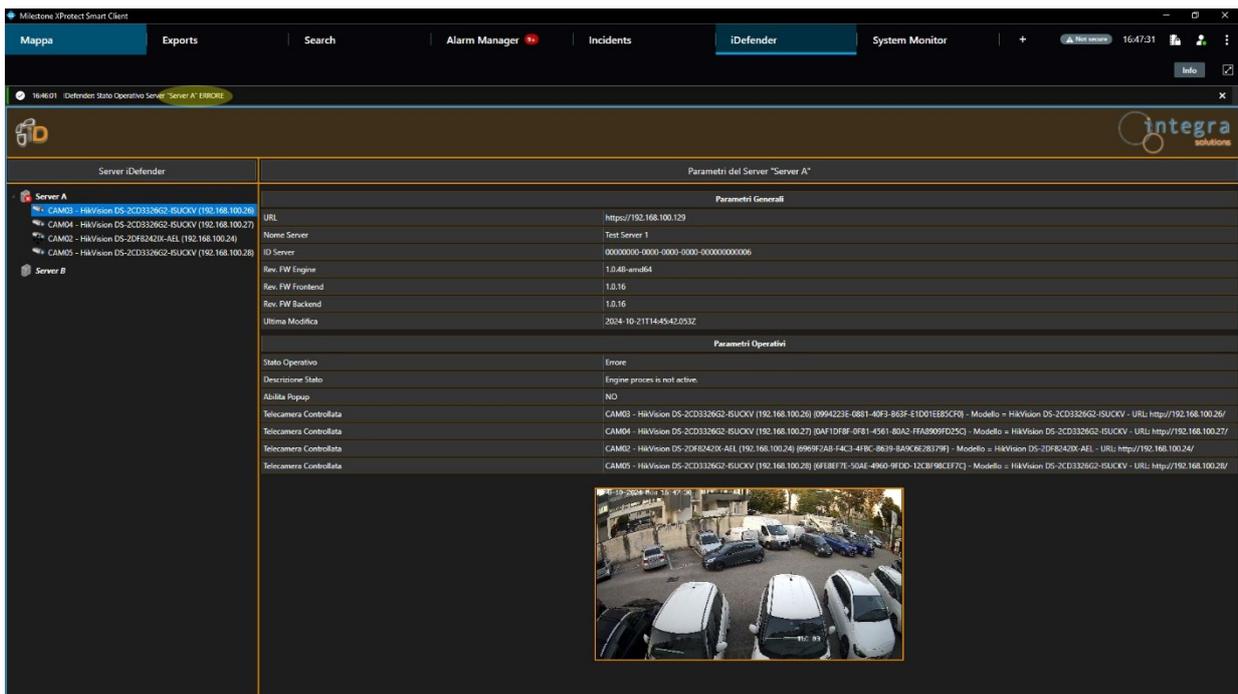
The Server icon change according to new State.

In addition to the normal Notifications, the Plugin, every time an Item changes status, sends a message to the SC Info Toolbar with the information on what happened, then updates the Operating Status and Icon accordingly.

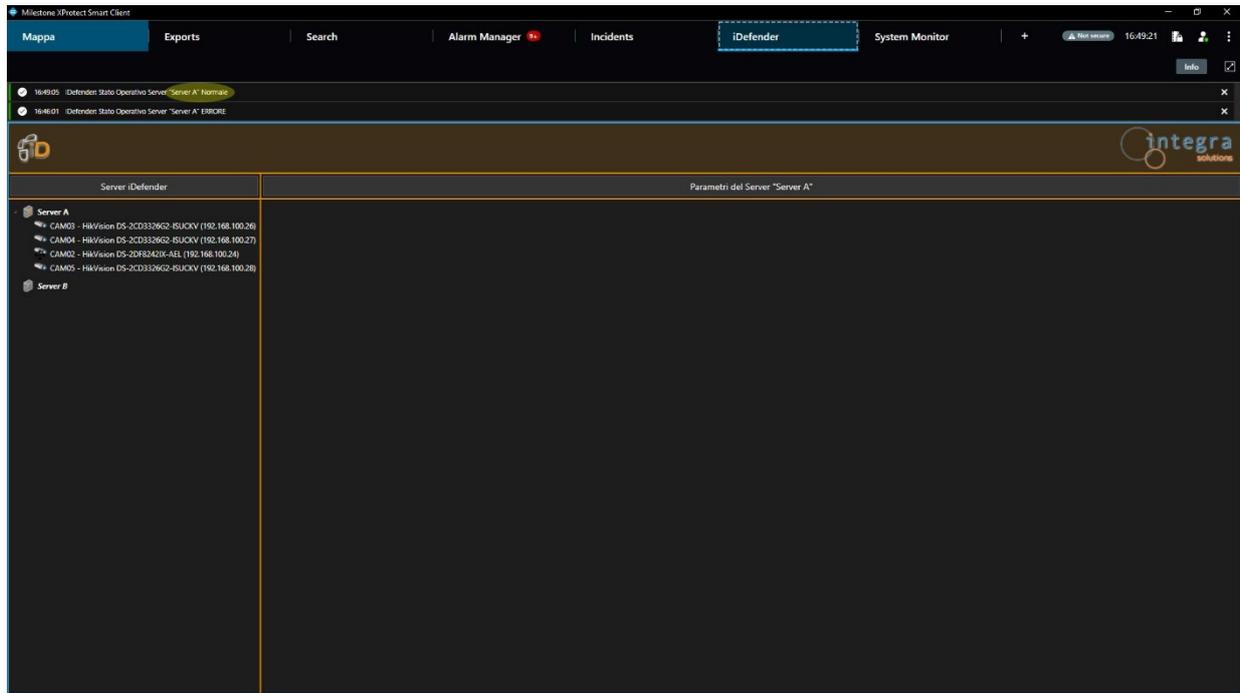


Such additional Notifications may be sufficient for some types of Events, e.g. Critical Status or Error, avoiding the need to program Alarms. The messages on the Info bar can be several and remain until the User deletes them.

Here are a couple of examples. The first is the Error Operation Status notification ...



...then the return to Normality.

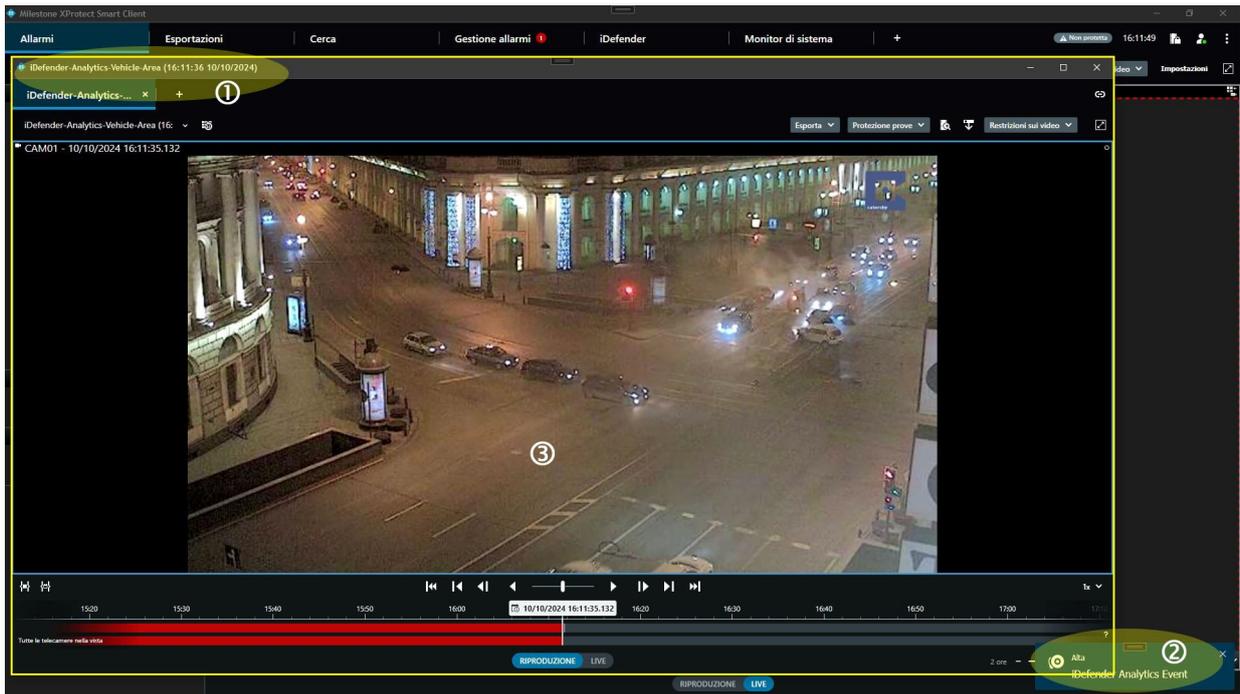


### 3.5 Analytics Events

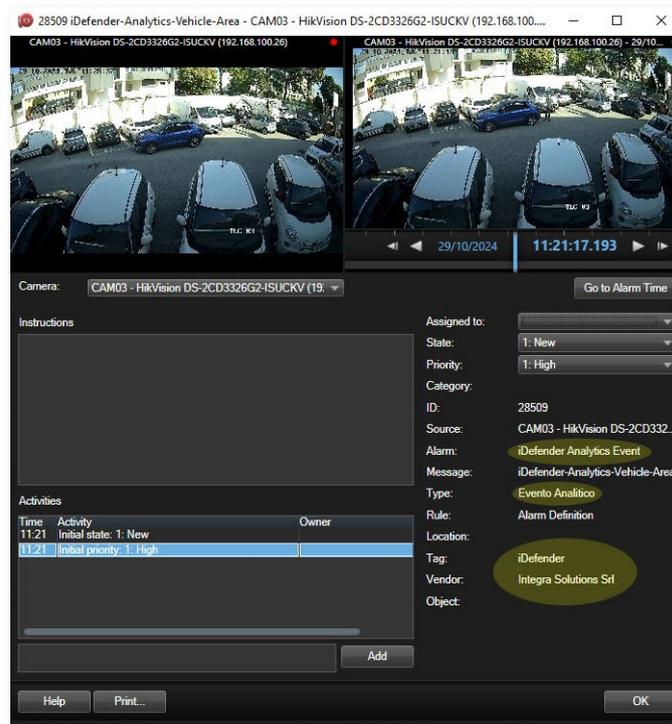
The management of Analytics Events presents one more option, in terms of Notifications, compared to what we have seen so far: the opening of a popup window with live/playback images from the camera in question, so when an Analytics Event occurs Notifications are:

- Message for the SC Info Bar (always)
- Alarm Activation (if configured and enabled)
- Floating Window opening (if enabled)

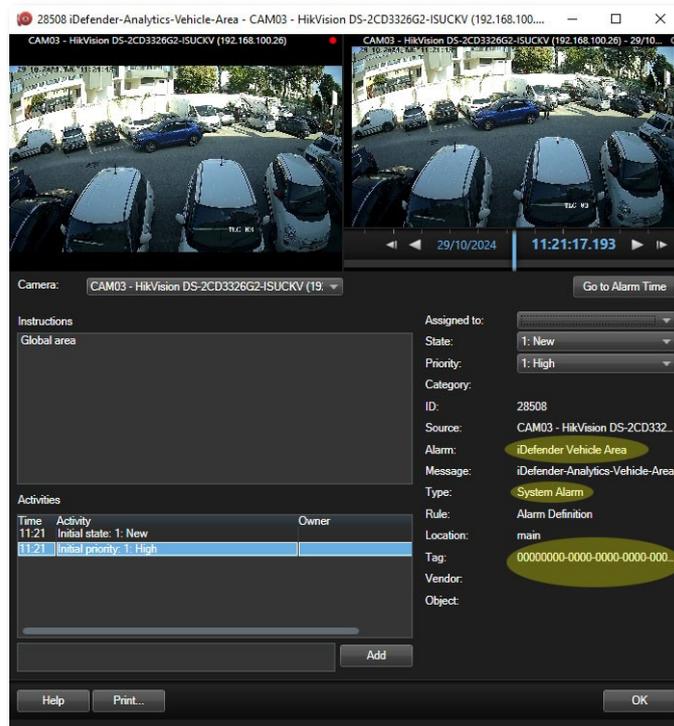
Alarms and Floating Windows can be enabled independently of each other.



This snapshot is an Analytics Event (Vehicle Area) with ① Info Bar Notification, ② Alarm (and Toast Notification) and ③ Floating Windows (yellow highlighted), while the following is 'normal' Alarm window.



Now the same Alarm generated by an Analytic Event and not by the Plugin.



## 4 Plugin Installation

The Plugin has its own installation procedure which suggests creating the iDefender folder in the MIPPlugins folder.

The contents of the Plugin folder are as follows:

- Plugin.def
- iDefender.dll
- Newtonsoft.Json.dll

additionally, after startup, the Plugin creates a log file called iDefender.log in that folder.

**WARNING:** To replace the dll, in case of updates, you must first stop ES and then restart it.

---

END OF DOCUMENT

---