ACTIVITYDETECTION EDGE 3.0

VMS integration

Revision 1

© 2018 ACIC sa/nv. All rights reserved.

ACIC sa / nv
Parc Initialis
Boulevard Initialis 28
B-7000 Mons
Belgium

support@acic.eu

www.acic.eu

Tel. : +32 65 39 43 80
Fax : +32 65 39 43 81

TVA/BTW : BE 0861 141 650

Document history

Revision	Date	Comment
1	11/2019	First revision

Intended audience

This document is addressed to installers, integrators and technicians who need to implement the ACIC ActivityDetection Edge 3.0 product. This version of the video analysis is designed to be installed in an Axis product, but the configuration and operating concepts are identical to the server version. The associated documents are thus:

- ActivityDetection 3.0, configuration
- ActivityDetection Edge 3.0, user guide

Getting technical support

You can ask your questions or post your comments and suggestions to ACIC at the following address: support@acic.eu. Don't forget to detail the information on the product you own (firmware number) and your details so that we can reply to you.

Warnings

The product brands used in this document may be trademarks or brands registered by their respective owners.

Table of contents

1 Introduction 5

2 Integration with the VMS Milestone XProtect 6

2.1 Installation of the plug-in 7
2.1.1 Download the program 7
2.1.2 Installing the program 7

2.2 Using the plugin suite 10
2.2.1 Configuration in XProtect Administration Application / Management Client 10
2.2.2 Event reporting 11
2.2.3 Embedding of graphics data in the Smart Client 11

3 Integration with Genetec Security Center 13

3.1 Installation of the gateway 14
3.1.1 Download the program 14
3.1.2 Installing the program 14

3.2 Using the gateway 15
3.2.1 About Security Center certificates 15
3.2.2 General configuration 15
3.2.3 Events reporting 16

3.3 ACIC Security Center Service services supervision 17

3.4 Security Center Plugin deployment and configuration 21
3.4.1 Installation of the ACIC Security Center Plugin 21
3.4.1.1 Prerequisites 21
3.4.1.2 Download the program 22
3.4.1.3 Installing the program 22
3.4.2 Displaying the overlays 23
3.4.2.1 The statistics panel 24
3.4.3 Executing the plugin with a non-administrator account 25
3.4.4 Troubleshooting 26
3.4.5 Known issues 27

4 Integration with SeeTec 28

4.1 Configuration of SeeTec 28

4.2 Configuring the camera 28

5 ExacqVision integration 29

6 Axis Camera Station Integration 32

7 Generic integration 35

8 Miscellaneous integrations 36

8.1 Axis rule engine 36

1 Introduction

The ACIC ActivityDetection Edge product is an embarked video processing application mainly used for the detection of activity in secure areas. Its functions are as follows:

- To detect the crossing of one or several virtual lines.
- To detect the entry of an object in a zone.
- To detect the parcel deposition and/or collection in a zone.
- To filter detections in function of size, speed or presence time.

This document provides the instructions for the integration of this product with Video Management Systems (VMS). An integration provides at least the communication of the detection events to the VMS, and also, in some cases, the display of graphics information on the video.

For this product version, compatible VMS are:

- Genetec Security Center
- Milestone XProtect
- Seetec
- ExacqVision
- Axis Camera Station

Moreover, another document (“ACIC API 1.2”) explains the ACIC generic API for the streaming of detection metadatas. Such a protocol can be used to integrate ACIC analytics with third party products.

2 Integration with the VMS Milestone XProtect

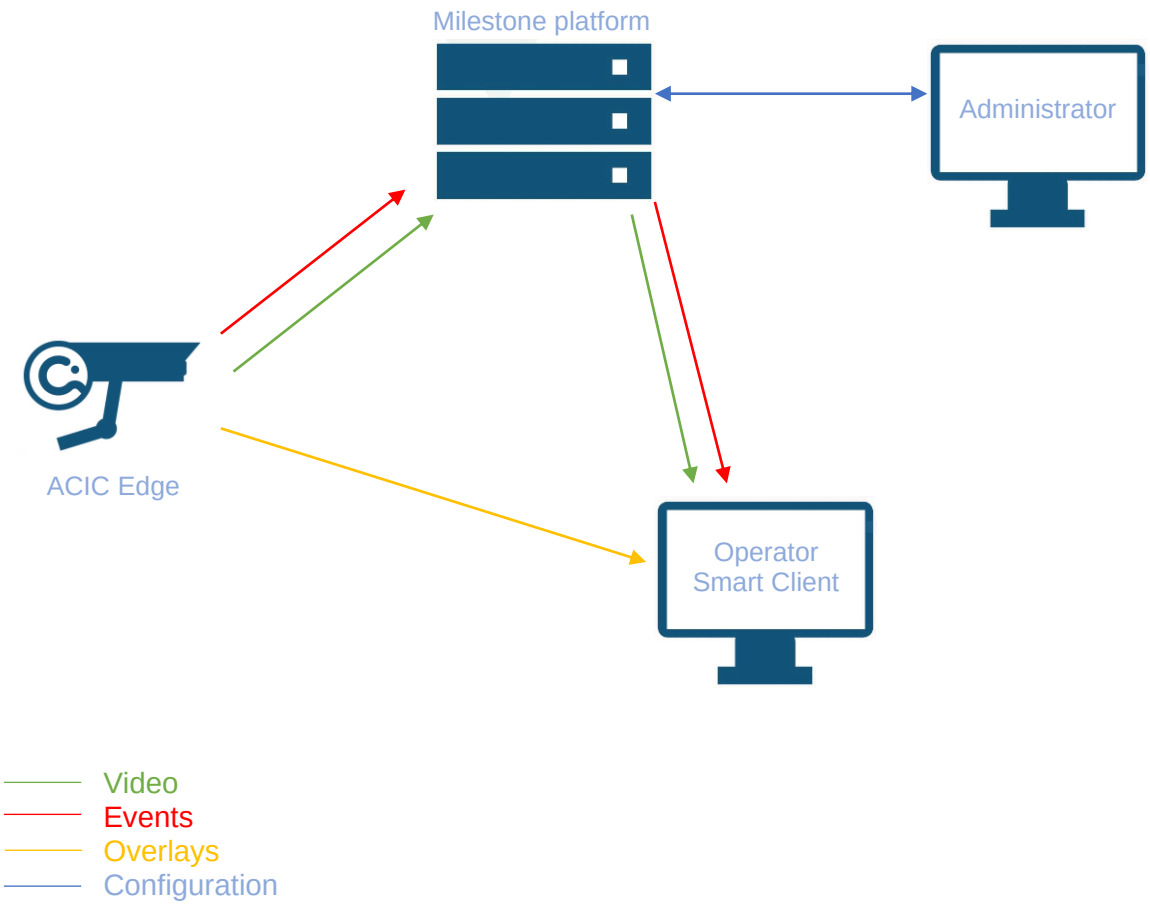
Milestone XProtect is a VMS made by Milestone System (http://www.milestonesys.com/).

The integration provides:

- automatic reporting of all events to "Analytics Events" in the VMS
- the embedding of "live" and “replay” graphics data on the videos displayed in the Smart Client (this is called video analytics overlays).

The integration is a plugin type integration. Its configuration is as simple as clicking on a button each time some cameras have been added to the VMS. The program is executed directly within the Milestone XProtect applications as indicated in the following figure.

- Milestone platform: the plugin collects the information on cameras known to Milestone from it. Moreover, the plugin collects the ACIC events from the camera and inserts them as "Analytic Events" in Milestone.
- XProtect Smart Client: the plugin provides embedding of the "live" graphics data on the videos displayed.



Note:
- The functionalities available may depend on the VMS version

Compatibility:
- Milestone XProtect Corporate 2013 (6.0a) or higher
- Milestone XProtect Expert 2013 (6.0a) or higher
- Milestone XProtect Enterprise 2013 (8.5e) or higher
- Milestone XProtect Professional 2013 (8.5e) or higher
- Milestone XProtect Professional+ 2017 R2 (11.2a) or higher
- Milestone XProtect Express 2014 (8.6a) or higher
- Milestone XProtect Express+ 2017 R2 (11.2a) or higher
- Milestone XProtect SmartClient 2013 or higher
- ACIC Analytics software with MIP (Milestone Integration Plateform) 3.0 support or higher

2.1 Installation of the plug-in

The steps for installing this suite of plugins are:

2.1.1 Download the program

Download the installation program for "ACIC XProtect Plugin" on the secure ACIC website or get it from your distributor.

Note: The 32 bits version of Milestone XProtect applications require the 32 bits version of "ACIC XProtect Plugin" while the 64 bits version of Milestone XProtect applications require the 64 bits version of "ACIC XProtect Plugin". Both versions can be installed on the same host.

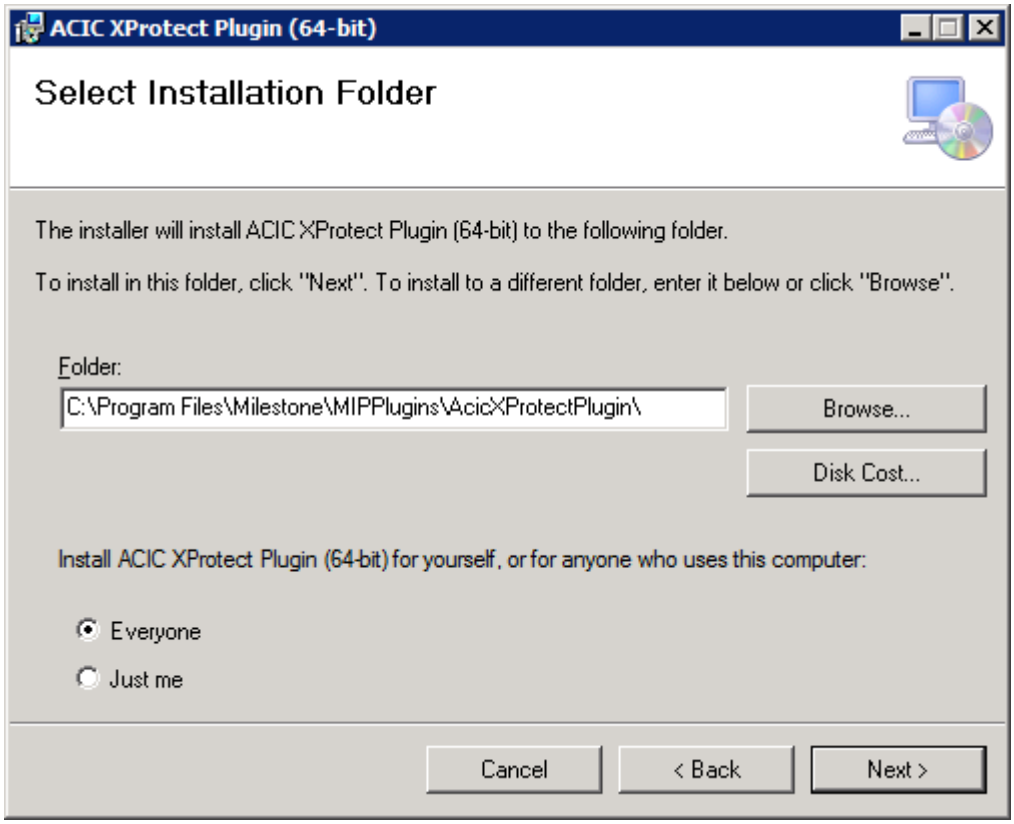
2.1.2 Installing the program

The "ACIC XProtect Plugin" program must be installed on the server on which the Milestone XProtect Event Server is installed and on any other machine where the Milestone Smart Client is used.

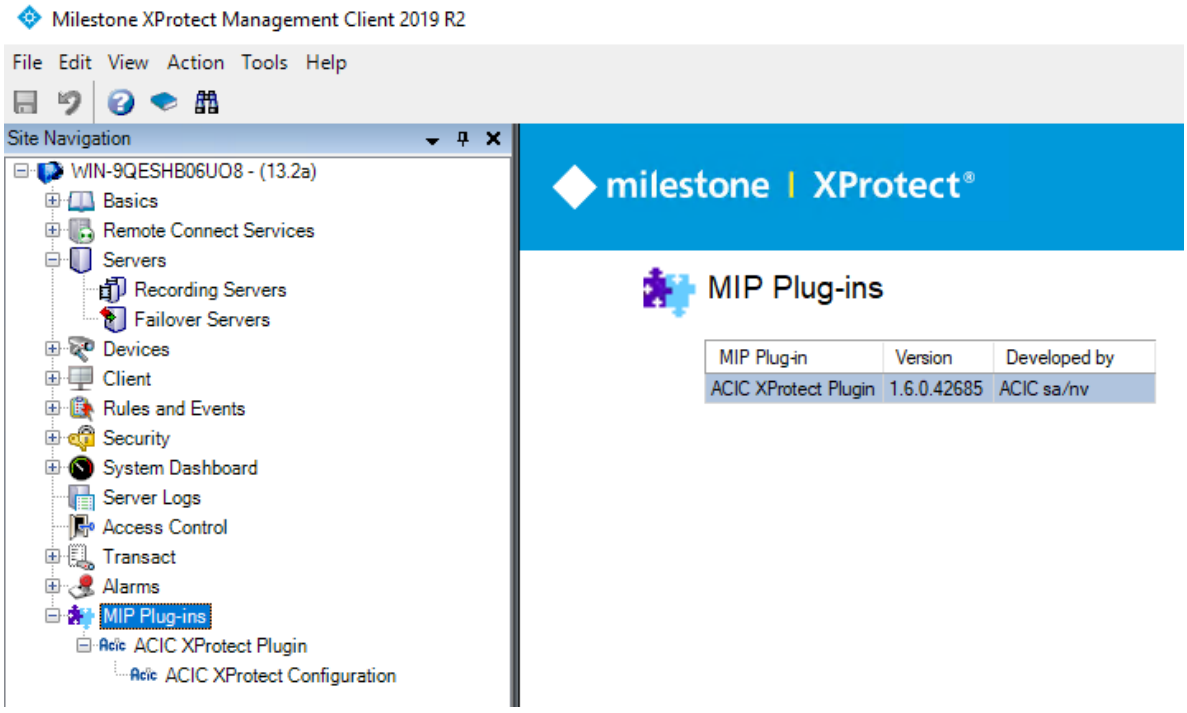
Note: When the Milestone XProtect application is deployed on several servers (e.g. several events servers), "ACIC XProtect Plugin" must be deployed on each server.

Launch the installation and follow the instructions. The program must be installed in the MIPPlugins folder under the Milestone installation directory. It is recommended to install the program for all users.

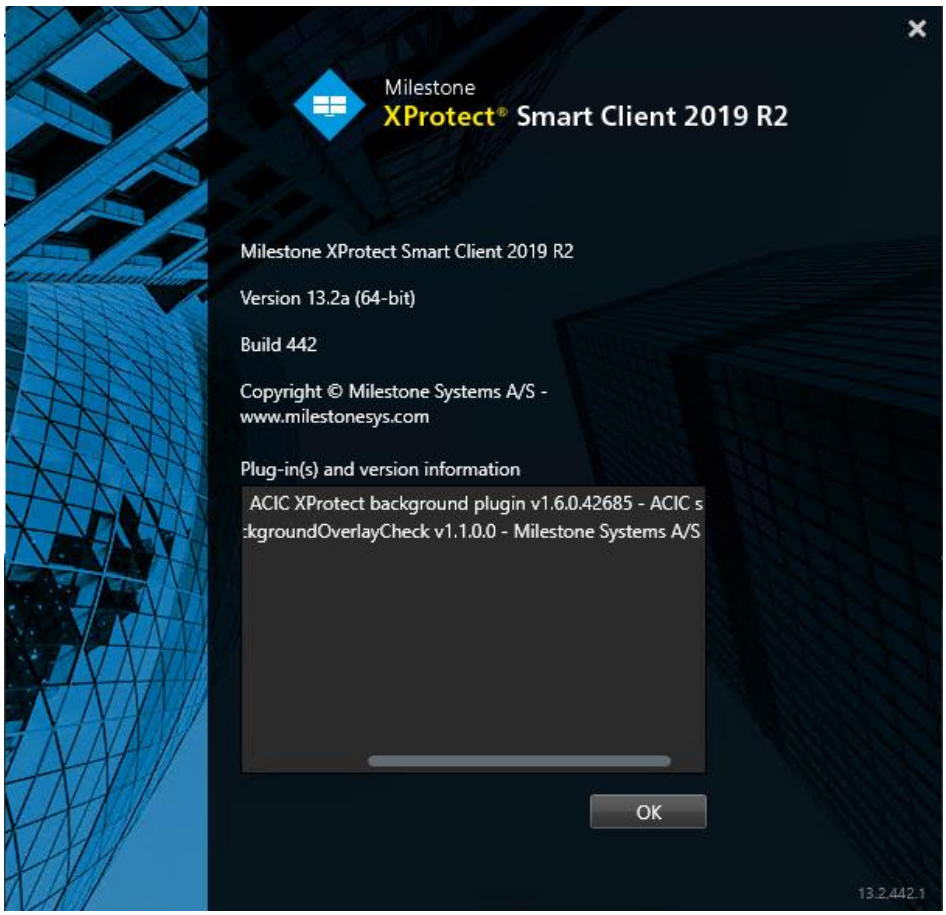
For a standard installation of Milestone XProtect, you don't have to change any settings.



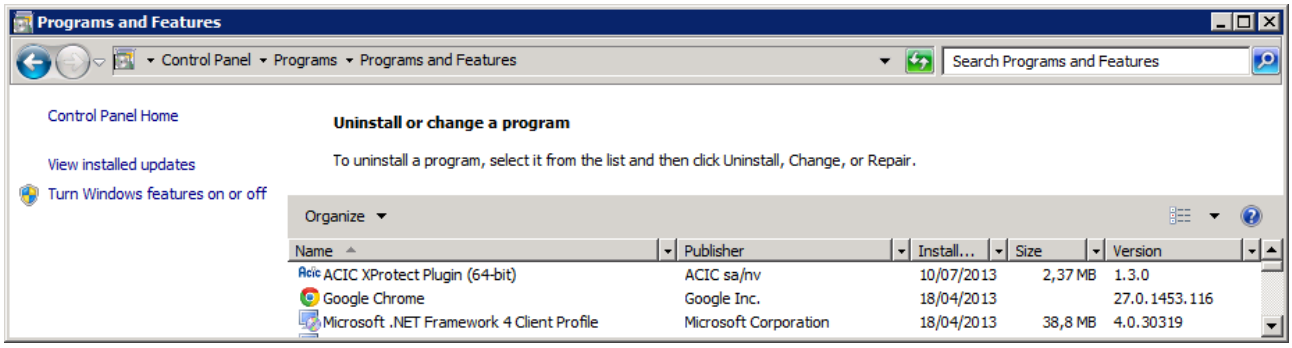
You can check the installed version in the administration tool:



For the Smart Client, the version can be checked in the About menu:



For a XProtect Events Server executing on a remote machine, the only way to check the installation is to check the version in the Windows programs manager.



2.2 Using the plugin suite

2.2.1 Configuration in XProtect Administration Application / Management Client

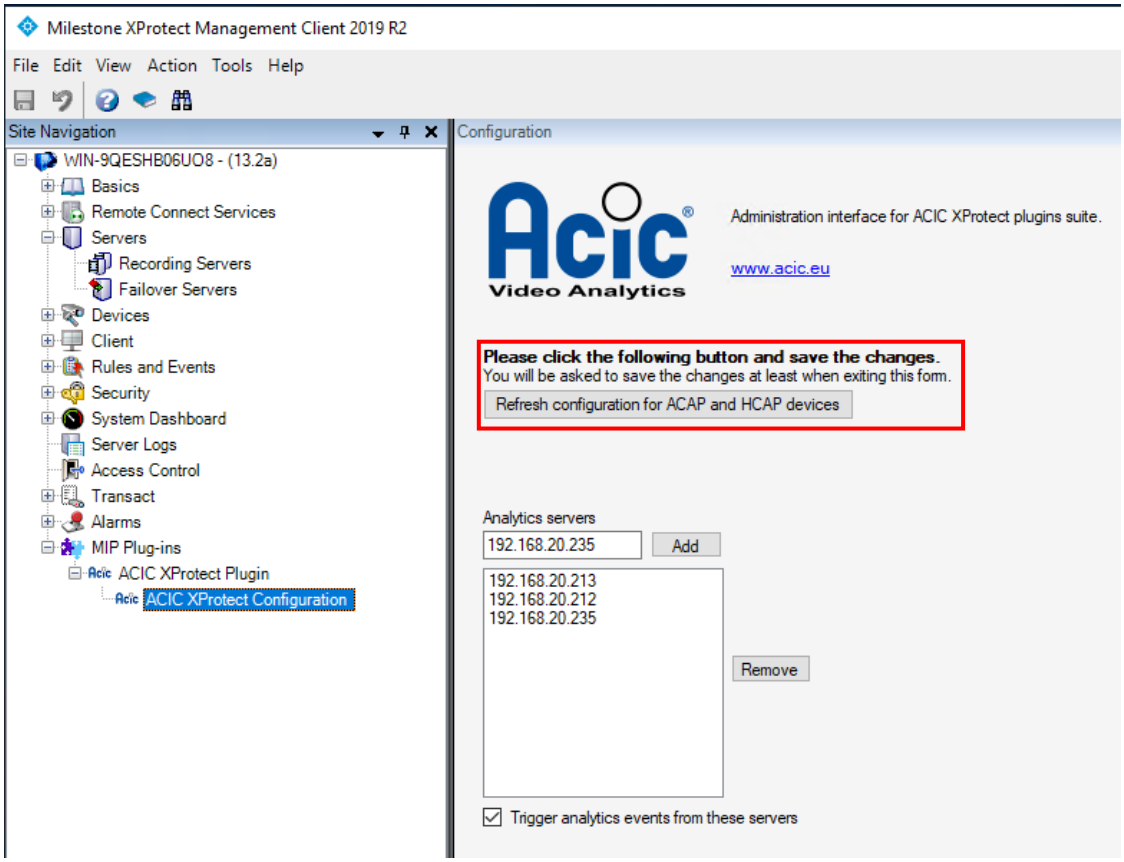
The illustration below shows the interesting part of the plugin configuration for edge ACIC video analytics applications.

In order for the plugin to identify the cameras with edge analytics, it is just required to click on the “Refresh configuration for ACAP devices” button and save the changes. You will be asked to save the changes at least when exiting the plugin configuration.

The list of cameras able to host an ACIC edge application is compiled when saving the plugin configuration changes. Event reporting and graphics data embedding are done for these cameras only!

In order for the changes in the Milestone XProtect configuration tool to be applied, they must be saved, and the services must be rebooted[1].

When a camera is added to or deleted from the Milestone XProtect administration tool, the XProtect Events Server is notified within approximately one minute. It is also necessary to reboot the Smart Client for that changes to be taken into account.



1 See Milestone XProtect user documentation

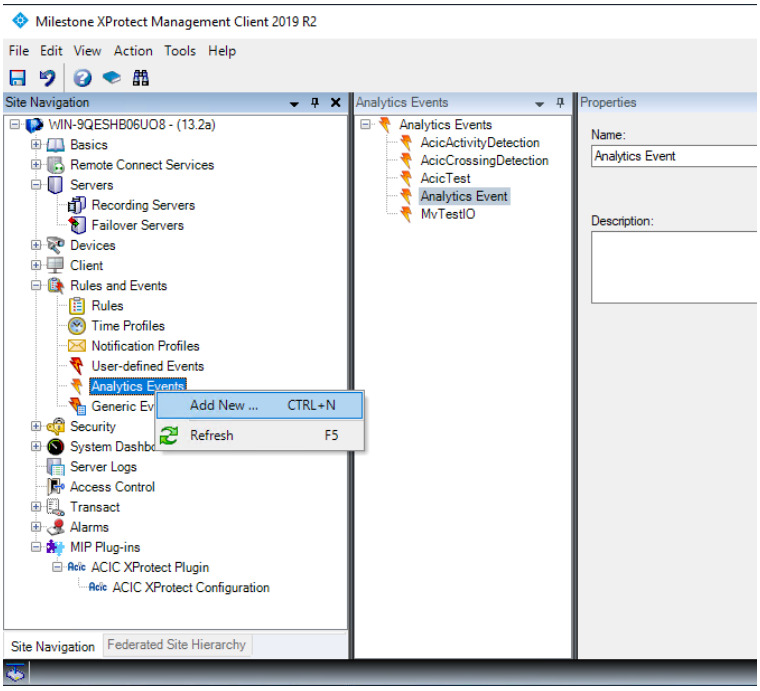
2.2.2 Event reporting

All ACIC events are automatically sent to Milestone as "Analytics Events". The source camera is automatically associated with each event transmitted.

To use these events, in the Milestone XProtect administration tool, you need to:

1. Declare an Analytics event bearing the same name as the ACIC event. The list of ActivityDetection events is:
   - AcicActivityDetection: detection of activity in a zone
   - AcicCrossingDetection: crossing of a single virtual line
   - AcicMultipleCrossingDetection: crossing of several virtual lines
   - AcicStationaryDetection: detection of stationary object
   - AcicMotionDetection: movement detection
   - AcicPTZPreset_i: activation du preset PTZ i
   - AcicTest: test event generated on request
2. Declare an alarm using this event.

For events with a duration (for example ActivityDetection), only the start of the event is sent to the VMS.



Note: XProtect Event Servers must be restarted after the plugin installation since the plugins are only loaded when the XProtect Event Server service is starting.

2.2.3 Embedding of graphics data in the Smart Client

The illustration below shows the embedding of "Live" graphics data in the Smart Client.

For each camera displayed in "Live" mode, the graphical metadata (graphical overlays) can be visible if this camera executes the ActivityDetection application.

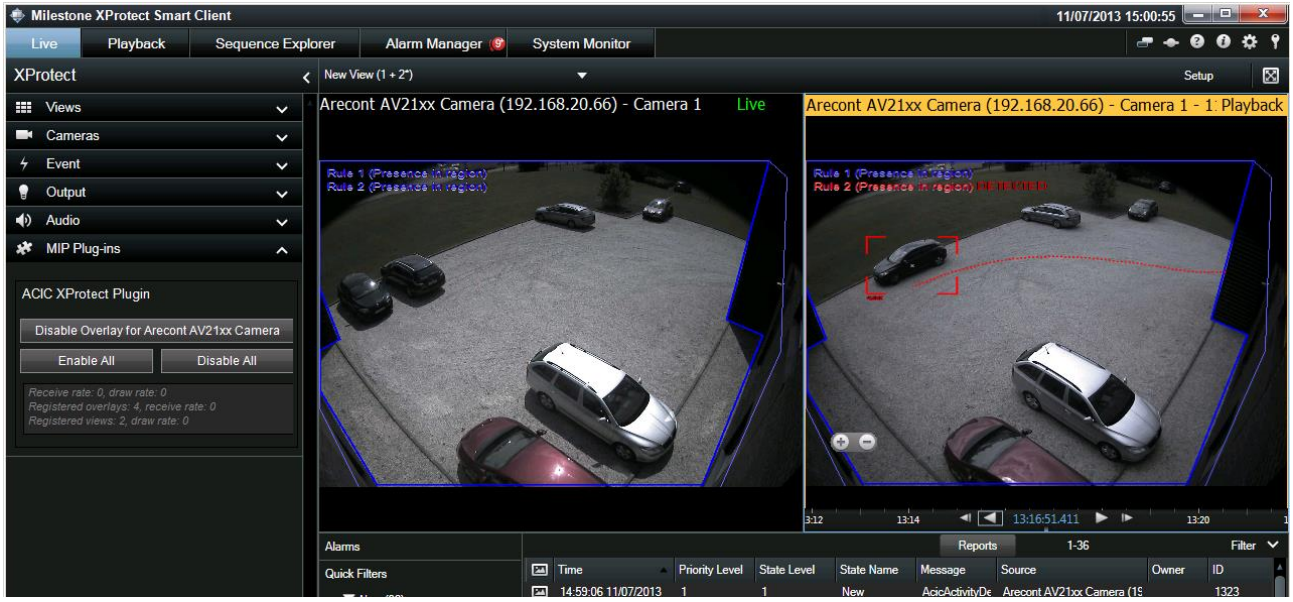
Some statistics are also provided for reference, such as:

- The flow of graphical data received and displayed for the selected camera.

- The number of cameras displayed producing a graphical data flow and the overall flow of this data.
- The number of views displayed and the overall display flow.

Note: The graphical data flow can be null in normal operation since graphics data are only sent when they change.

Known problem: to display the statistics of a camera that has just been slide over the currently selected view, you must temporarily select another view before you can select this camera. The Milestone development tools do not currently provide a solution to this problem.



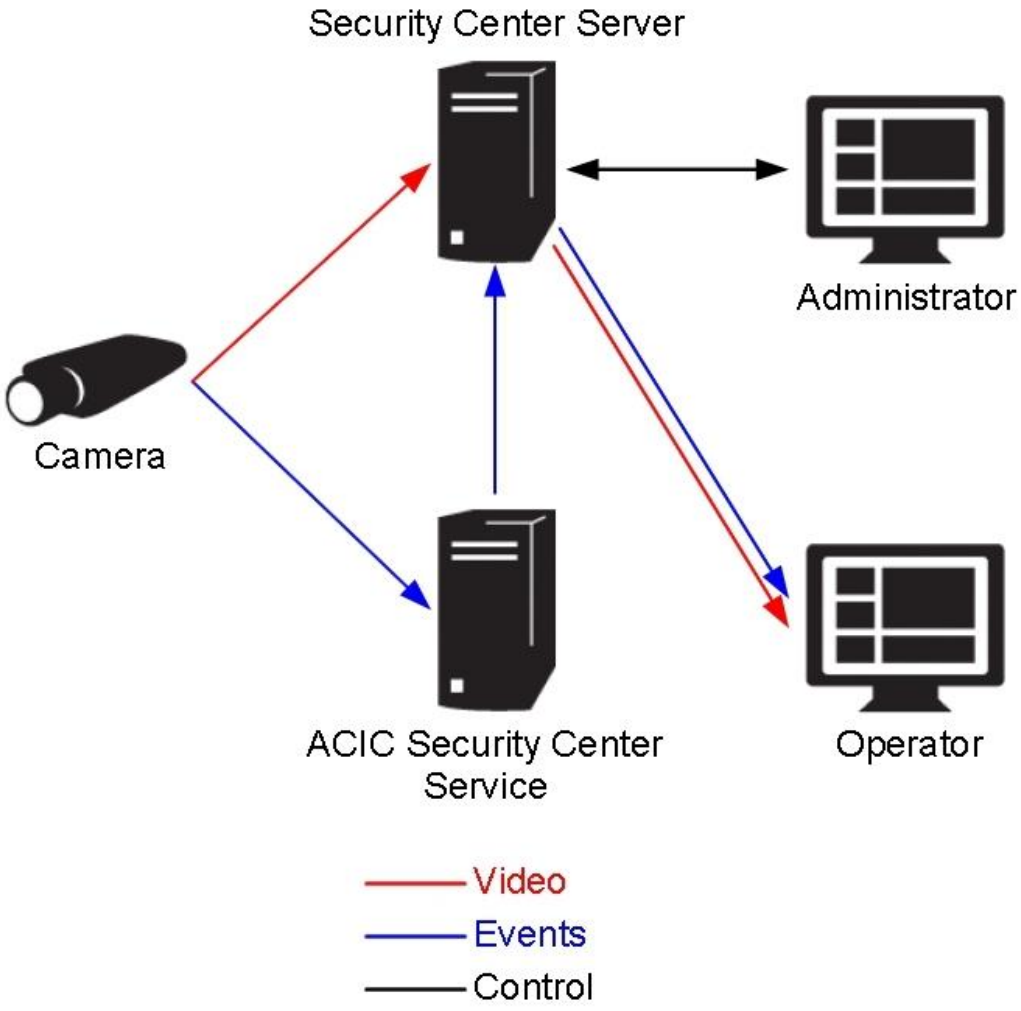
3 Integration with Genetec Security Center

Genetec Security Center is a VMS made by Genetec Inc. (http://www.genetec.com).

The integration provides:

- automatic reporting of all events to "Custom Events" in the VMS.
- video analytics overlays over live and replayed video in Security Desk (on version 5.2 or later)

The integration uses a Windows service component acting as a gateway between ACIC video analytics and the VMS.



Compatibility:

- Security Center 5.2 and above

Genetec Certificate:

*The integration between ACIC and Genetec requires a specific Genetec certificate. The certificate reference is **GSC-1SDK-ACIC-SCGateway**, it must be ordered from your Genetec dealer. Without that certificate, the ACIC integration service will not be able to connect to Security Center service. One certificate is used for each instance of ACIC Security Center service, whatever the number of cameras handled by the services.*

3.1 Installation of the gateway

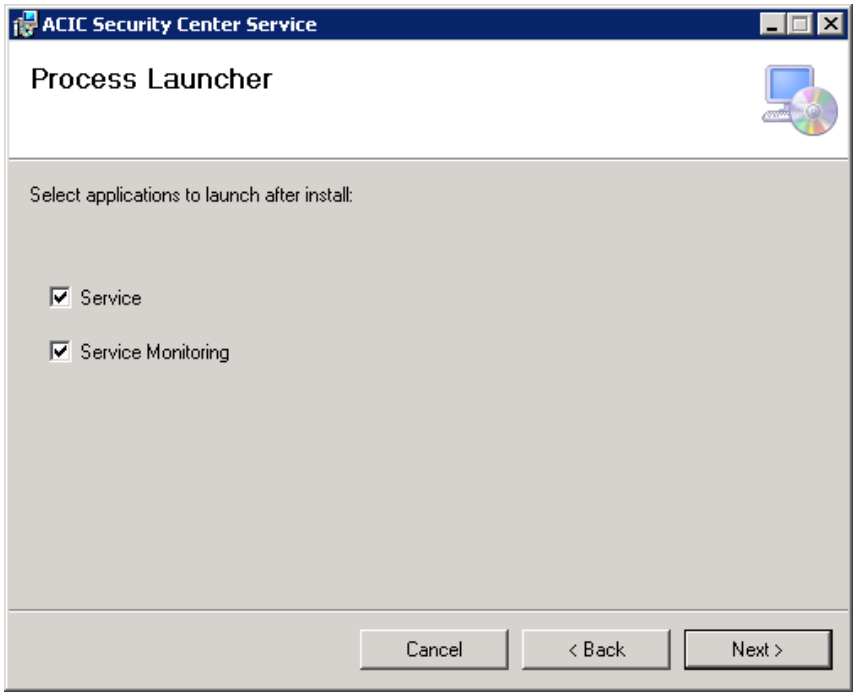
The steps for installing the gateway (ACIC security center service) are:

3.1.1 Download the program

Download the installation program for "ACIC Security Center Service" on the secure ACIC website or get it from your distributor.

3.1.2 Installing the program

The "ACIC Security Center Service" program can be installed on any recent Windows machine (with support for .NET 4.0) including the one running Security Center. Launch the installation and follow the instructions.



You can check the installed version in the about menu of the ACIC Security Center Service management tool as well as in the Windows program manager.

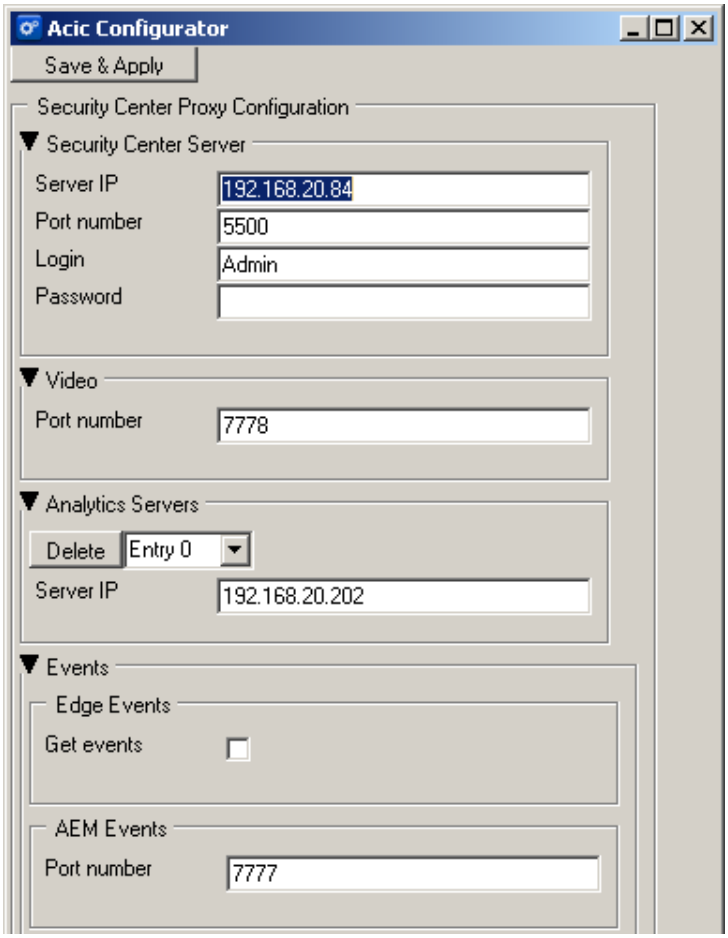
3.2 Using the gateway

3.2.1 About Security Center certificates

To use the gateway, you need to install the appropriate Security Center certificate in your Security Center server. You can order our gateway certificate with the specific part number GSC-1SDK-ACIC-SCGateway.

3.2.2 General configuration

The gateway must be configured with the appropriate credentials to be able to connect to Security Center. This is done through a simple management tool that can be accessed through an icon in the Windows notification area when launched.
It is required to fill in the “Security Center Server” section to fit the Security Center configuration. The port numbers in the “Video” and “AEM Events” sections must also be set although they are not used for an Edge setup.



In the ACIC Security Center Service management tool, it is required to configure the following information.

- The Security Center Server section provides the necessary data to be able to connect to Security Center Server.

- The Video and Analytics Servers sections are only used with server-based video analytics and should not be completed for Edge analytics.
- The Edge Events section allows to enable the automatic acquisition of events emitted by ACIC Analytics running on the Axis Cameras known from the Security Center Server. This must be checked for Edge analytics.
- The AEM Events port number is mainly for compatibility with old ACIC video analytics solutions.

Once the configuration is complete and applied, start the service if it is not already running and check in the logs if the connection with Security Center is successful.

3.2.3 Events reporting

For the automatic reporting of ACIC events, you have to check the “Get events” box in the “Events” section.

All ACIC events are automatically sent to Security Center as "Custom Events". The source camera is always associated with each output events.

The “Event Rules” section is optional and allows to personalize the translation from ACIC events to Security Center Custom Events. Each rule can be understood like: For each event with the name “Event name”, send a custom event to Security Center with name “Output name” and description “Output description”. The description can be set up with the content of the ACIC event parameters.

ACIC events that have no associated rule are sent to Security Center with “Output name” being the Event name and description “%name% at %time%”.

To use these events, in Security Center Config Tool, we need to:

1. Declare a Custom Event bearing the appropriate name (“Output name” used in rules or ACIC event name, e.g. AcicActivityDetection). The list of ActivityDetection events is:
   - AcicActivityDetection: detection of activity in a zone
   - AcicCrossingDetection: crossing of a single virtual line
   - AcicMultipleCrossingDetection: crossing of several virtual lines
   - AcicStationaryDetection: detection of stationary object
   - AcicMotionDetection: movement detection
   - AcicPTZPreset_i : activation of PTZ preset i
   - AcicTest: test event generated on request
2. Declare an alarm using this Custom Event.
3. Optionnaly, use a Security Center macro to process this custom event and exploit its description string.

For events with a duration (for example ActivityDetection), only the start of the event is sent to the VMS.

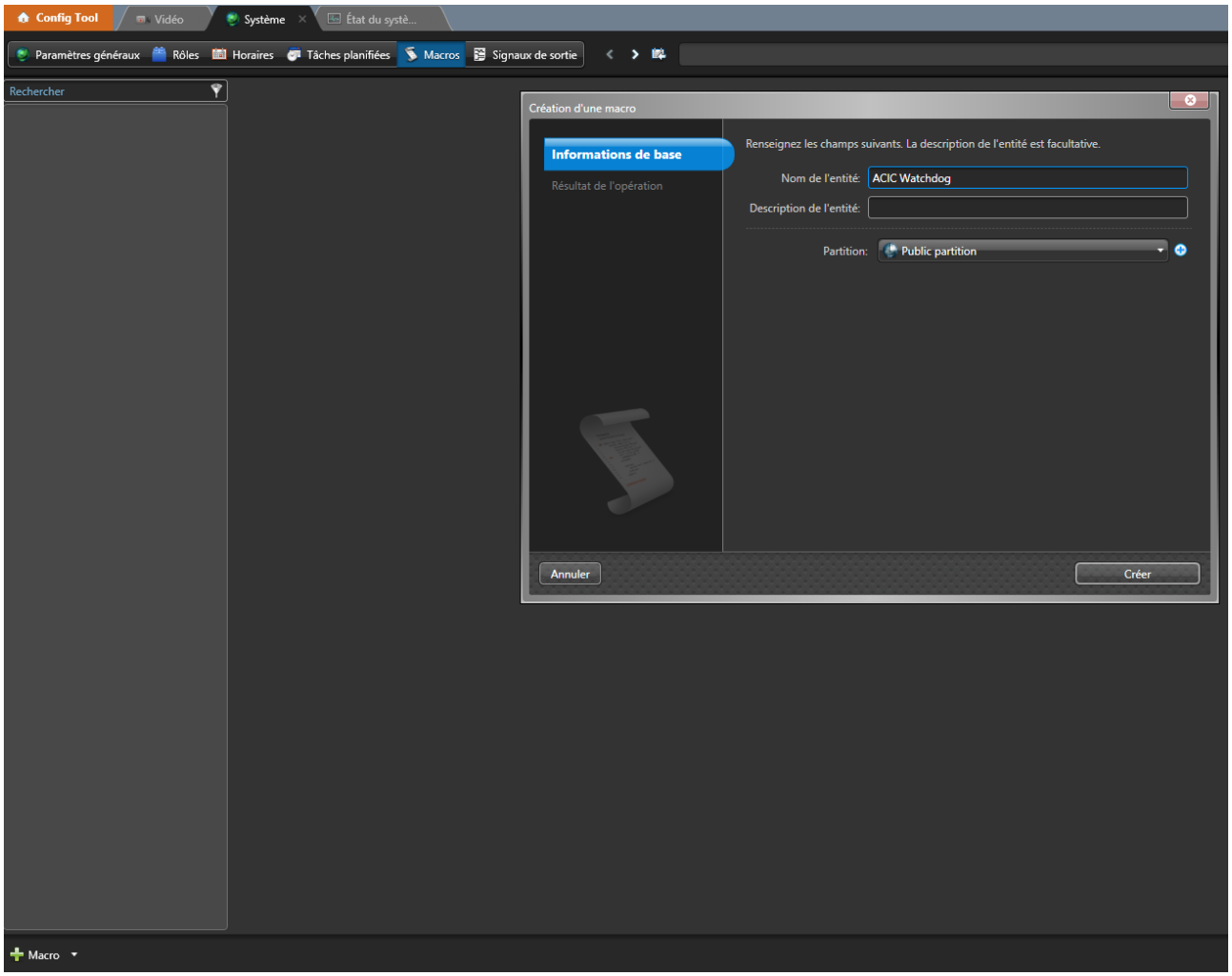
3.3 ACIC Security Center Service services supervision

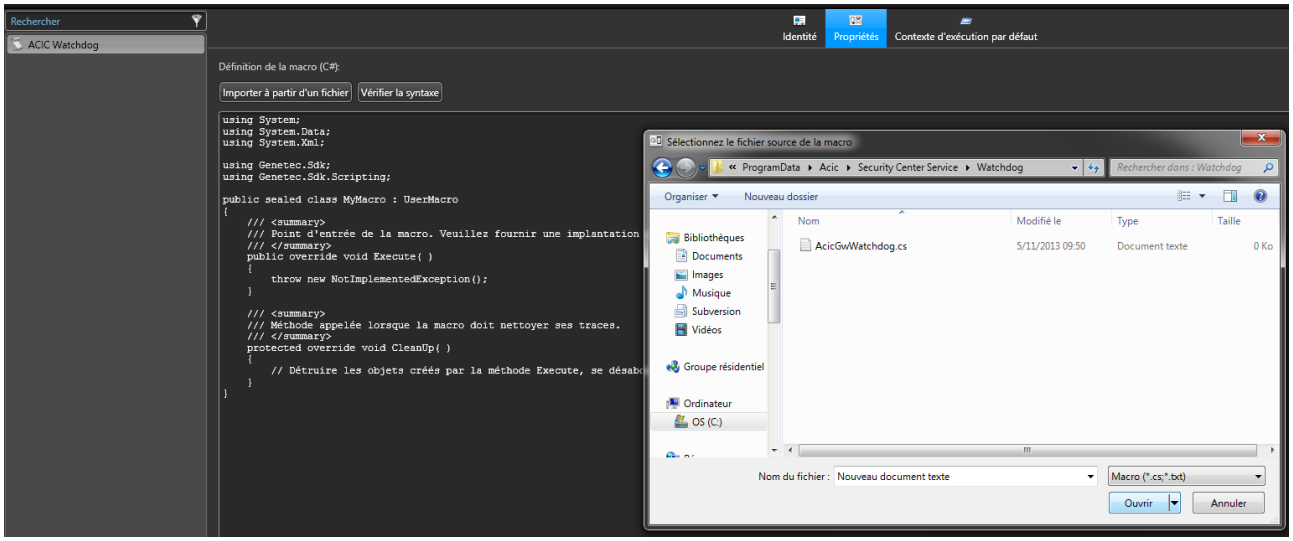
You can monitor ACIC Security Center services to raise supervision events for the availability and unavailability of each service instance. For that, you need to import a macro in Security Center ConfigTool. This macro can be found in the package named ACICSecurityCenterServiceWatchdog_1_0.zip available on the secure part of ACIC web site or through your dealer.

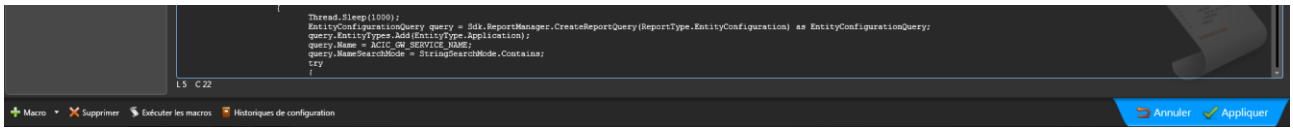
Open Security Center ConfigTool and select the **System** task. Go then to the **Macros** menu and click on **+** as illustrated here after. Name the entity ACIC Watchdog and validate by clicking the **Create** button.

Click then on **Import from file** in the **Properties** menu and select AcicGwWatchdog.cs which is in the AcicSecurityCenterServiceWatchdog_1_0.zip package.

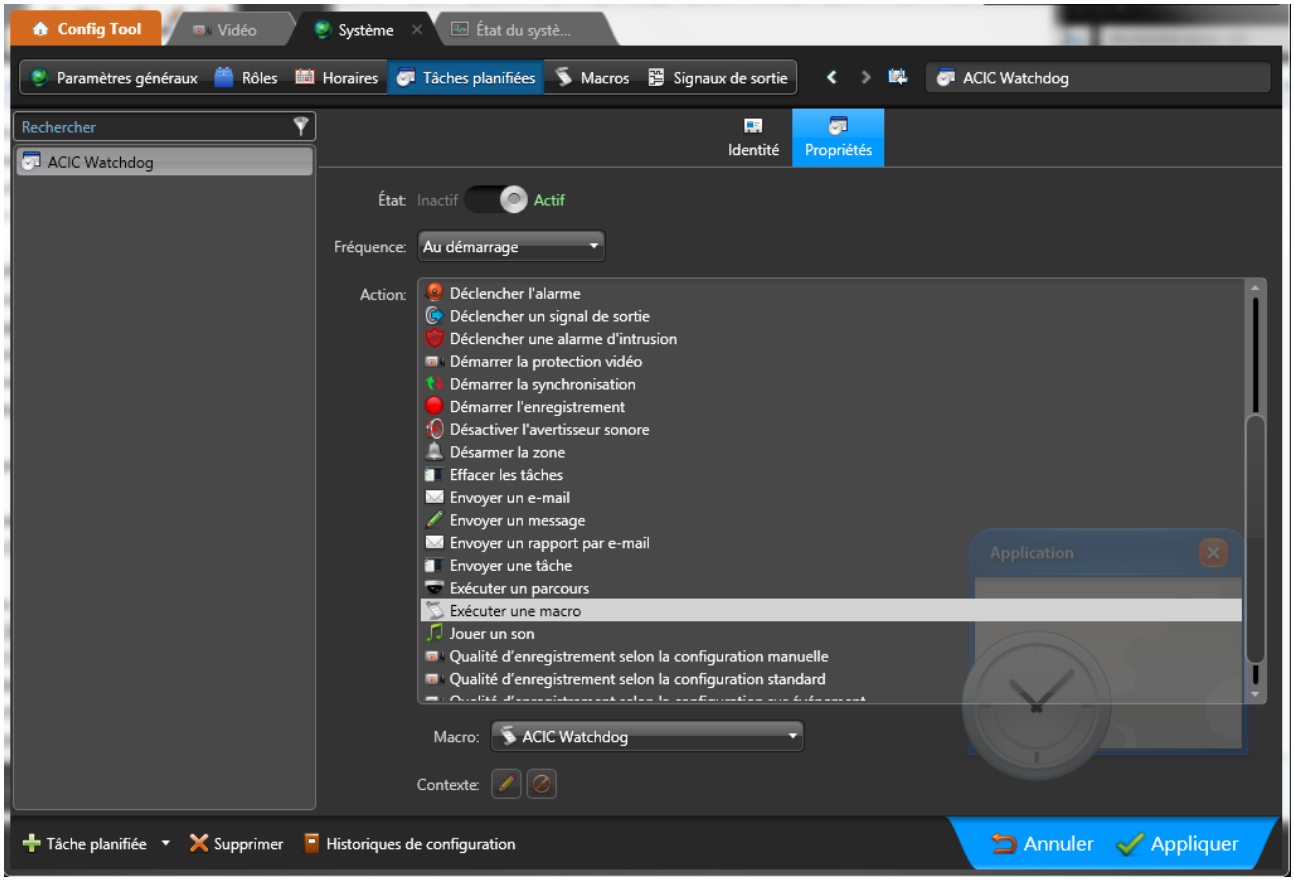
Click then **Apply**.







To get the watchdog macro started when Security Center starts, you need to create a scheduled task. In Security Center ConfigTool, under the **System** task, select the **Scheduled tasks** menu. Click on the **+** button to add a task and name it ACIC Watchdog. In the task properties, set the status to **Active**, set Recurrence to **On startup**, choose action **Run a macro**, then select the **ACIC Watchdog** macro – see illustration here after. To validate the changes, click **Apply**.

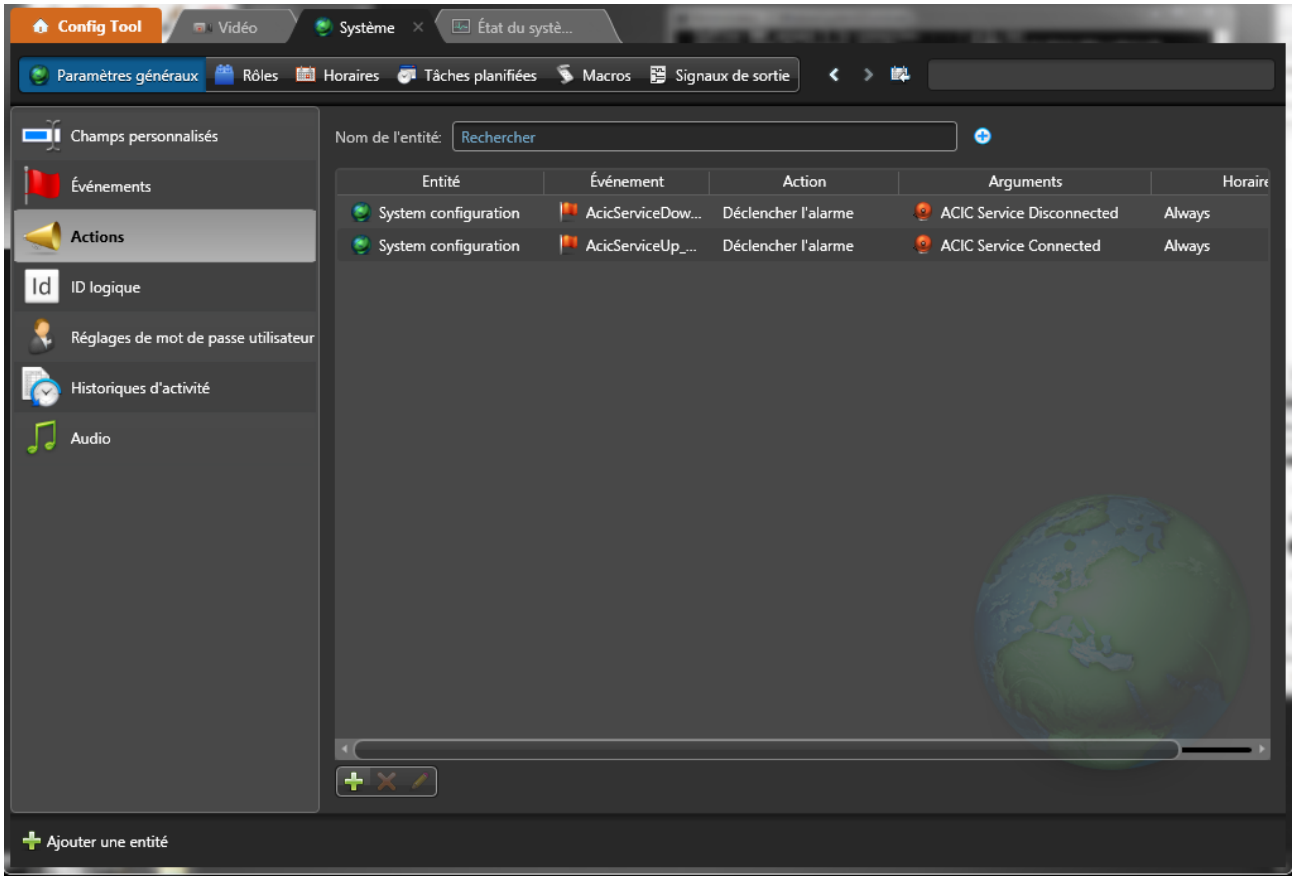


Once installed, the macro will detect arrivals and departures of ACIC Security Center Services and will emit supervision events with respective names **AcicServiceUp_<name>** and **AcicServiceDown_<name>** where <name> is the host name where the service runs. These events are automatically created by the macro when it detects a new service.

Supervision events exploitation

In Security Center ConfigTool create two alarms: ACIC Service connected and ACIC Service disconnected. Choose the targets of the alarm, e.g. the administrator. These alarms will be raised when receiving the macro events (see here after).

Create two actions for each ACIC service that raise these alarms. In the Security Center ConfigTool, **System > General settings > Actions**, click on the button **+**. Select the **System** entity, choose the source event within the ones defined by the macro and set **Trigger alarm** with the alarms previously defined.



These alarms will have their source event name postfixed with the host name where the involved service runs.

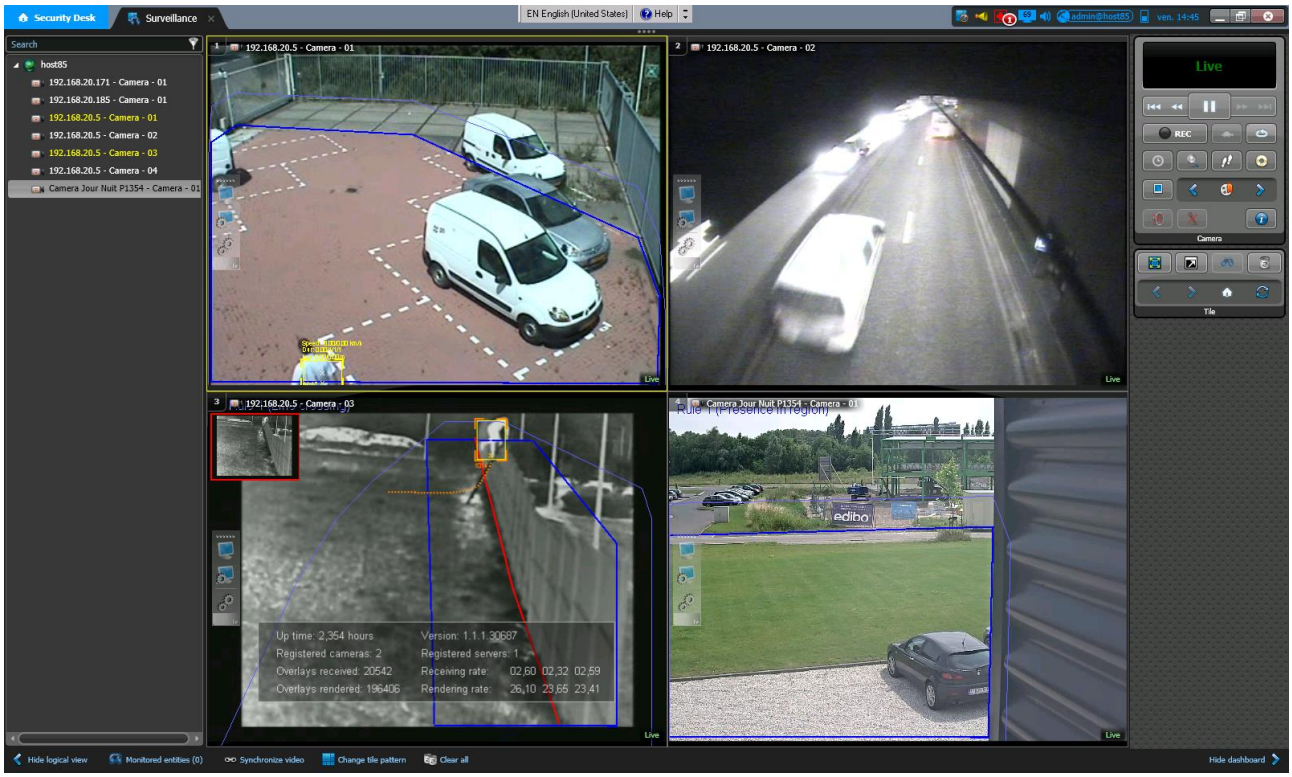
Please see Genetec documentation for more notification possibilities.

3.4 Security Center Plugin deployment and configuration

Note: If the version of the ACIC Security Center service is equal to or higher than 3.0, this part is no longer needed as the overlays will be handled directly from the Genetec server.

The ACIC Security Center Plugin is required to display real time overlays in Security Desk application.

Overlays are graphical layers generated by ACIC video analytics, showing information like detection, positions of mobiles, counting statistics ... They can be displayed over each camera that has been analyzed by ACIC software.



3.4.1 Installation of the ACIC Security Center Plugin

3.4.1.1 Prerequisites

The ACIC Security Center Plugin is compatible with Security Desk 5.2 and higher.
For the plugin to be able to retrieve overlays sent by ACIC's analytics server, you must install the ACIC Security Center Service.

Each Security Desk running with the ACIC plugin consumes an ACIC-Genetec certificate. The ***GSC-1SDK-ACIC-SCGateway*** certificate must be ordered from Genetec.

3.4.1.2 Download the program

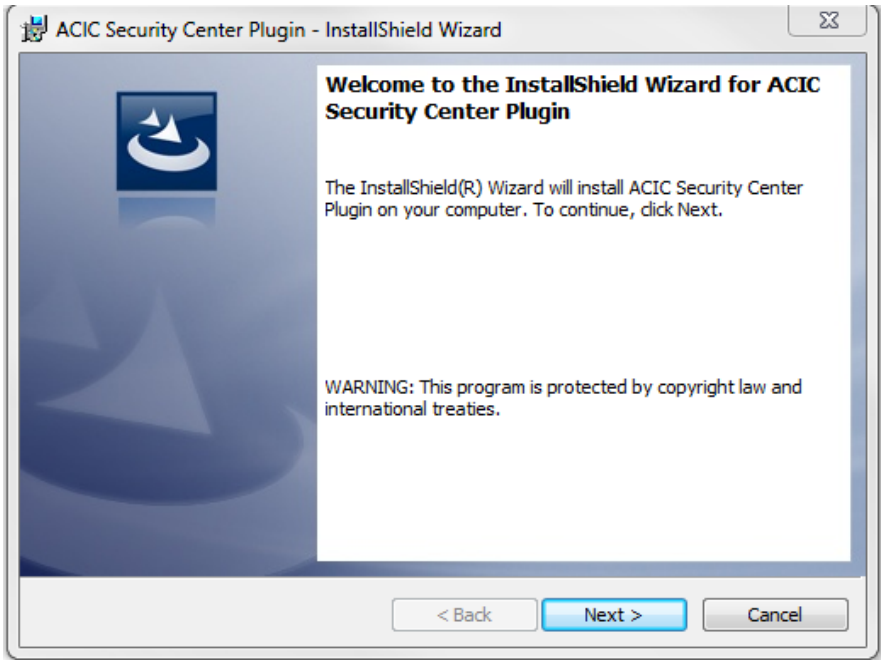
Download the installation program for "ACIC Security Center Plugin" on the secure ACIC website or get it from your distributor.

3.4.1.3 Installing the program

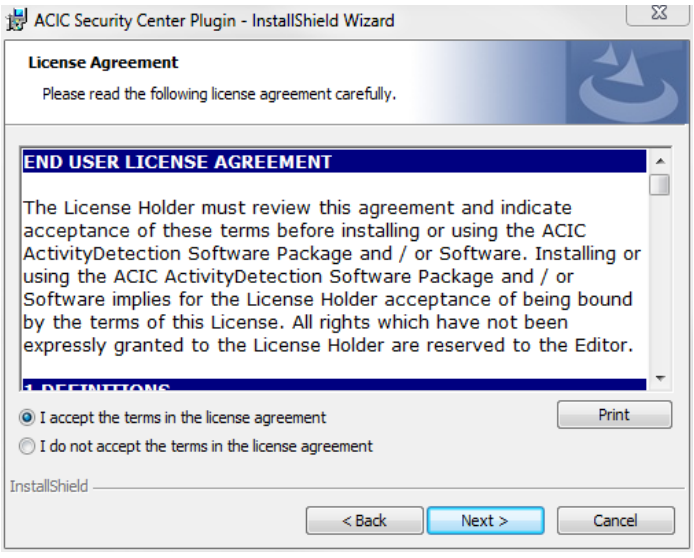
The ACIC Security Center Plugin must be installed on each computer where a Security Desk Client may be used.

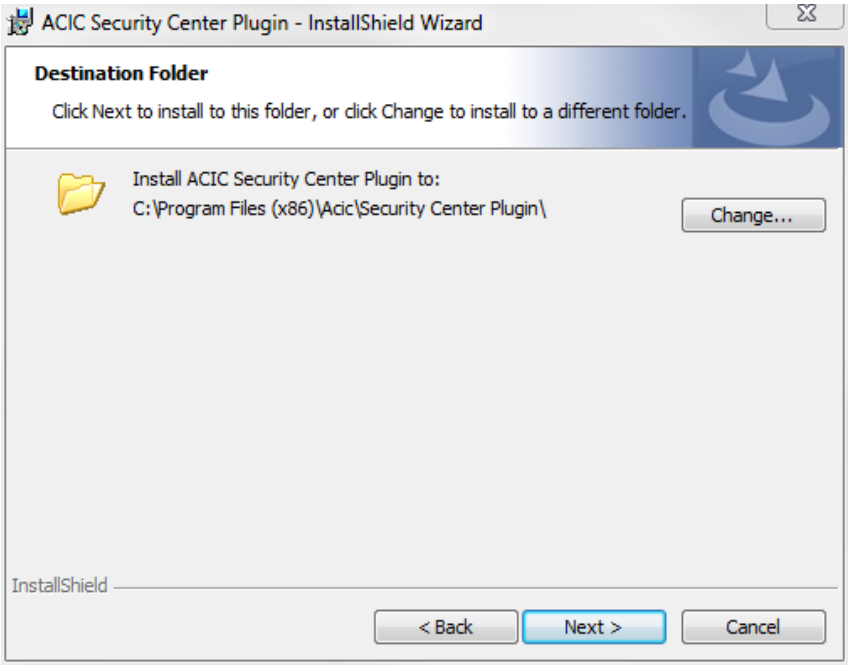
Launch the installation and follow the instructions. The program is by default installed in the Program Files directory under \Acic\Security Center Plugin\.

For a standard installation, you don't need to change any settings.



For the plugin to be installed on the target machine, you have to read and accept the ACIC licensing terms as shown below.





3.4.2 Displaying the overlays

If everything is well configured and the camera is recognized as an ACIC compatible video source, the ACIC overlay toolbar will appear in the left side of the tile.

This button enables or disables the ACIC overlays on the current tile view.

This button activates or removes the support for the ACIC overlays (effective on all tiles)

This menu enables or disables the statistics panel on the current tile view.

Illustration 1: Security Center Plugin controls

3.4.2.1 The statistics panel

The statistics panel is a tool that give information about version, up-time, number of registered cameras and server, receiving and rendering rate. The window appears in the bottom of the tile view as a semitransparent panel.

Up time: Time interval representing the tile view lifespan. The tile view is reused by Security Desk between tabs thus the tile is not attached to a dedicated video source.

Version: The ACIC Security Center plugin version. This version have to be transmitted to the support team in case of any problem.

Registered cameras: Numbers of camera from which the plugin try to acquire meta data.

Registered servers: Numbers of server from which the plugin try to acquire meta data. The servers are configured in the ACIC Security Center Service[2] – see Illustration 2: ACIC XProtect Plugin installation options.

Overlays received: Total number of overlays received, for the video source currently displayed, since the tile view creation. Because overlays are incremental, they are transmitted only when they change. A rapid variation of this number involves a high dynamic scene.

Receiving rate: The statistics given in the receiving rate are composed of 3 columns representing the average values of overlays received per seconds computed (from left to right) on the last 10 seconds, 1 minute and 10 minutes.

Overlays rendered: Total number of overlays drawn on this tile view. When displaying the statistics panel, the overlay rendered increase drastically to update the statistics panel itself. When the statistics are hidden the overlay are rendering only when they changed.

Rendering rate: The statistics given in the rendering rate are composed of 3 columns representing

2 Several servers may be processed by one gateway

the average values of overlays drawn per seconds computed (from left to right) on the last 10 seconds, 1 minute and 10 minutes.

Illustration 2: Statistics panel

3.4.3 Executing the plugin with a non-administrator account

By default, the plugin cannot display overlays from ACIC Analytics servers except if the Security Desk is running with administrator privileges. This is due to the fact that the plugin must be able to read the custom field “ACIC Servers List” configured by the ACIC Security Center Service. This problem is not present when the plugin displays data from Edge video sources.

The Genetec Custom Fields are only viewable by administrator or privileged accounts but you can change the permissions of custom fields to allow specific users and/or a groups access.

Should you wish to use the plugin with a non-administrator account, follow these steps:

1) Login to the Config Tool with the administrator account.
2) In the System > General settings > Custom fields panel, edit the ACIC Servers List custom field.
3) In the bottom panel named “Security”, add all users or groups authorized to use the ACIC plugin.
4) Apply the changes and restart all the running Security Desk instances.

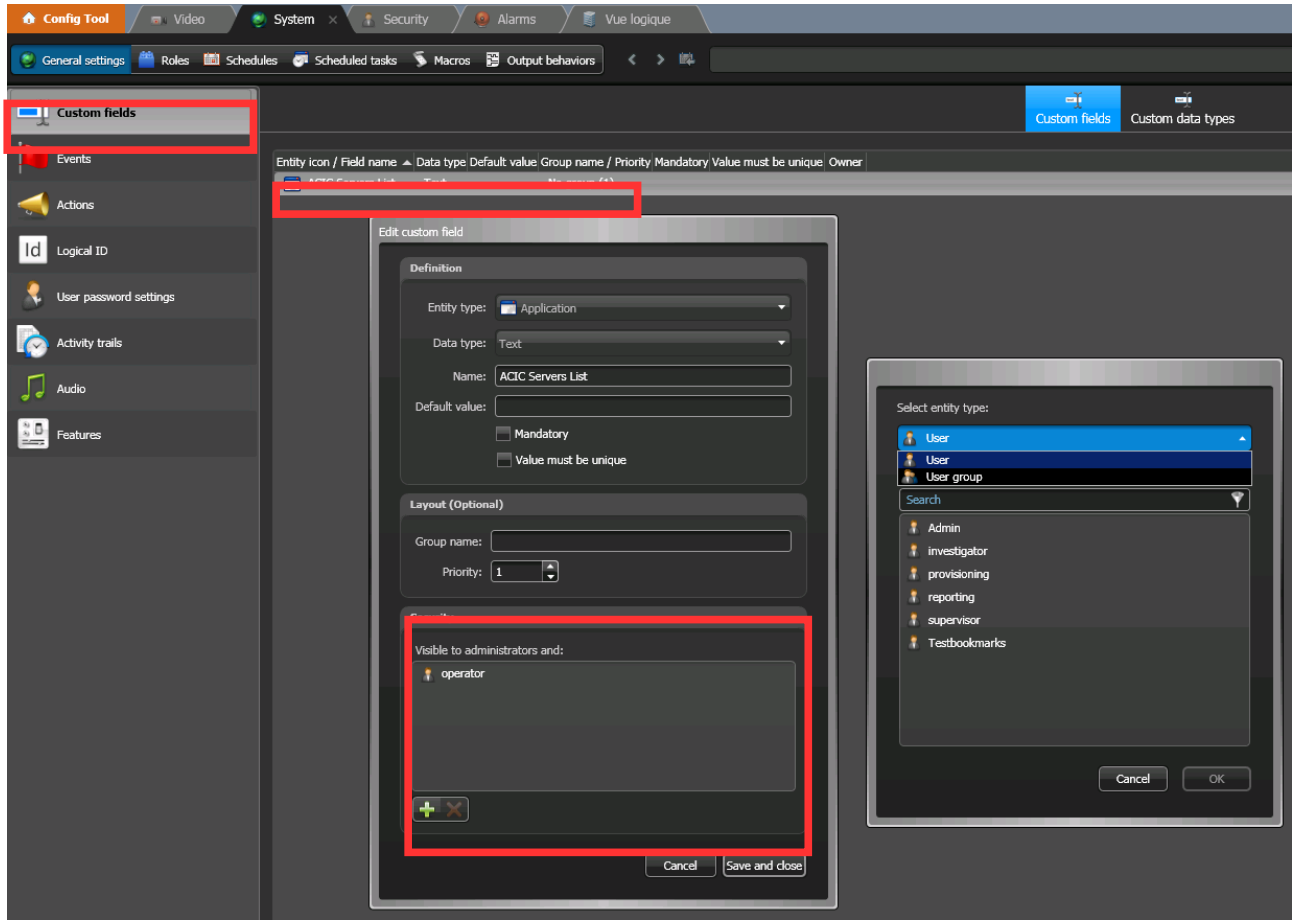


Illustration 3: Executing the plugin with non-administrator account

3.4.4 Troubleshooting

1) The ACIC overlay tool bar is not visible.

This is probably because the tile view is not loaded by Security Center. To be sure, open the Logs file located at %APPDATA%\Acic\Security Center Plugin\Logs. If the log file does not exist or the content is out of date, the plugin is not loaded, it could be a problem of:

- Security Center version, only versions 5.2 or above are supported.
- Certificate. Like other features, the ACIC Security Center plugin needs the Gentec GSC-1SDK-ACIC-SCGateway certificate. A certificate is required for each running Security Desk that use the plugin.

2) The tool bar appears only in some tile view.

The tile for which the tool bar does not appears are not considered as a valid ACIC analytics compliant source.

2.1) The source is an ACAP/Edge camera:

→ Check if the software is correctly installed on the camera and is up to date.

2.2) The source is processed by an ACIC server:

→ Check if the ACIC Security Center Service is started.

→ Check if the analytics server is setup in the ACIC Security Center Service configuration.

→ Check if the corresponding analytics stream is supplied with video stream.

→ If the ACIC server streams is taken directly from the camera, check if the External ID match the ID given by Security Center.

3.4.5 Known issues

The zoom is not applied to the ACIC overlays. This issue is due to a feature that is not implemented by the Genetec Security Center SDK.

4 Integration with SeeTec

The integration with SeeTec (http://www.seetec.eu/) provides reporting of the events generated by the ActivityDetection Edge application to the VMS and creation of the associated alarms.

4.1 Configuration of SeeTec

To receive events and generate alarms, a TCP communication reception component must be added in the SeeTec system.

Add the TCP integration component in SeeTec:

1. Launch the SeeTec client, **SeeTec Surveillance** and authenticate
2. Go into **Configuration Mode** (**File** menu, **Configuration Mode**)
3. Select **Hardware** in the left panel, click on **New**
4. Choose a name for the new hardware, then select **"3rd Party Interface"** for the **Manufacturer** field and **"Seetec Network I/O"** as **Type**. Leave the other fields at their original value
5. Select the new entry under **Hardware** in the left panel and in the right panel select **Inputs** and click on **"Edit..."** to the right of the **"Change number of inputs"** field
6. Create an appropriate number of inputs, generally per type of event to be received from a camera with the ActivityDetection Edge program.
   SeeTec will create the number of TCP inputs requested in the above point. For each input, we need to configure the TCP reception port. Choose a different port per input and this port cannot already be in use by another program on the SeeTec system host.
7. Per line of input settings, give a name to the input in the **Name** field and enter a port value in the **Port** field. Refer to the SeeTec documentation for the meaning of the other fields. In the context of the integration with the ActivityDetection Edge program, they can conserve their default value.
8. Click on **Apply** to confirm

Once the TCP inputs have been created following the above procedure, these inputs can serve in SeeTec alarm scenarios as alarm start or end events. Refer to the SeeTec documentation for the creation and editing of alarm scenarios.

4.2 Configuring the camera

To activate the TCP inputs in SeeTec, new TCP addressees must be configured on the camera with the SeeTec system as destination and the values configured for the inputs in stage **7** of **Erreur ! Source du renvoi introuvable.** as destination ports.

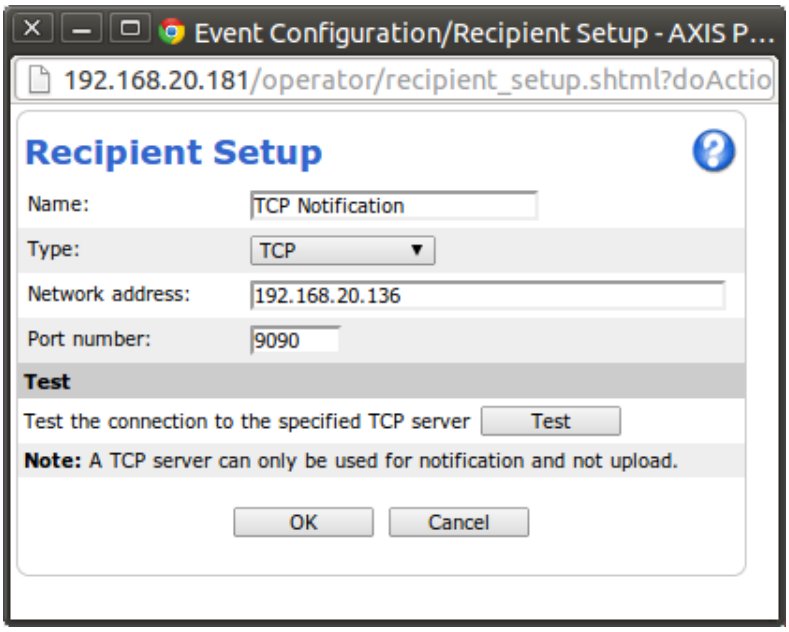
Refer to chapter **Erreur ! Source du renvoi introuvable.** of this document and to the Axis documentation for the creation of new TCP addresses.

5 ExacqVision integration

ExacqVision is a multi-camera and multi-platform VMS from Exacq Technologies : www.exacq.com. Detection events of ActivityDetection Edge can be transmitted to the VMS using TCP notifications available in Axis camera.

The setup procedure is as follow:

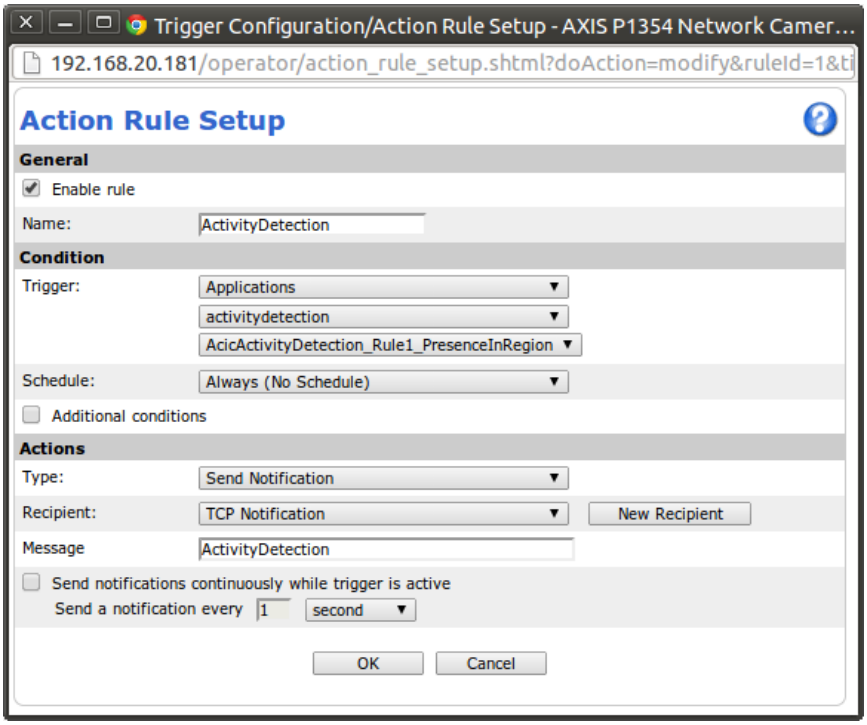
Create a new Recipient in the Axis configuration interface (Events section), with TCP type, the address of the ExacqVision server and an unused port.

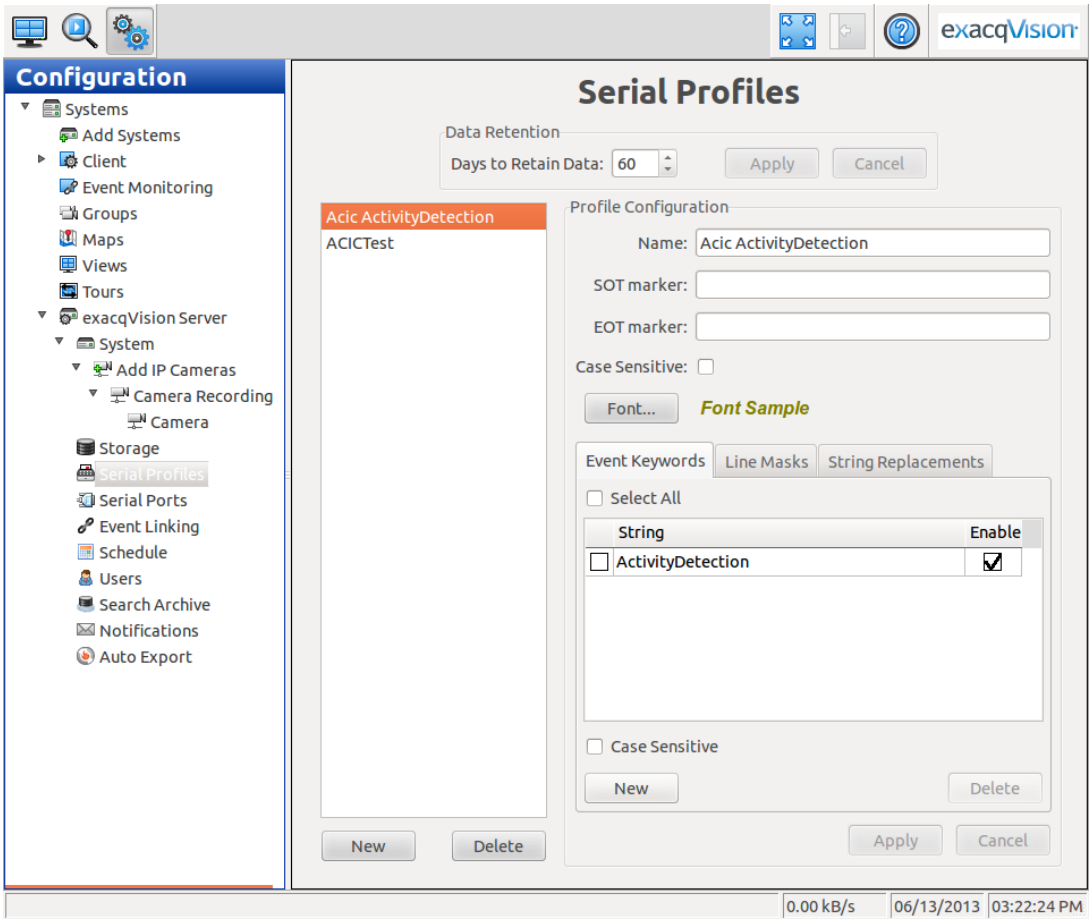


Add an action rule for each event that need to be sent to ExacqVision.

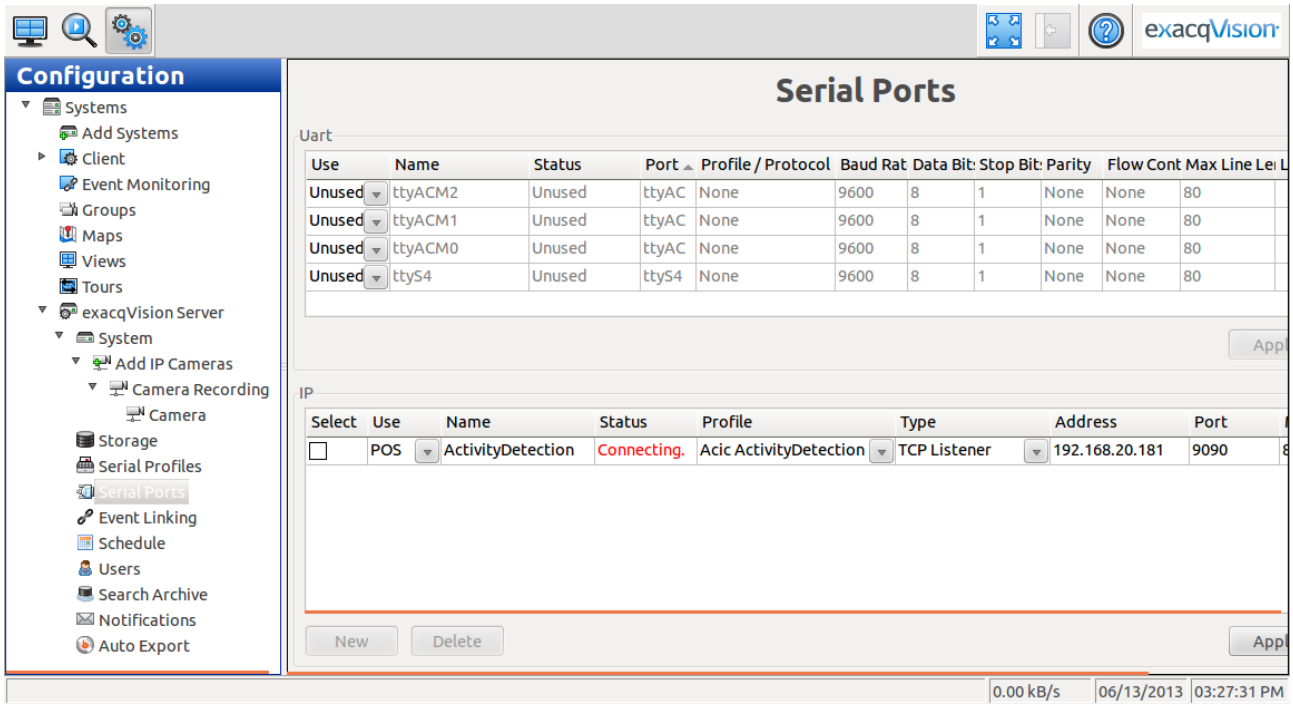
In addition to the regular triggers, created for each detection rule, there is a special “AcicTest” trigger. That trigger is generated by the button on the “***main page***” of ActivityDetection application.

Select TCP Notification as the Action for the rule. The given Message will be send to Exacq using that TCP connexion and must be specific for the selected event (so we can create condition at the reception of the message).



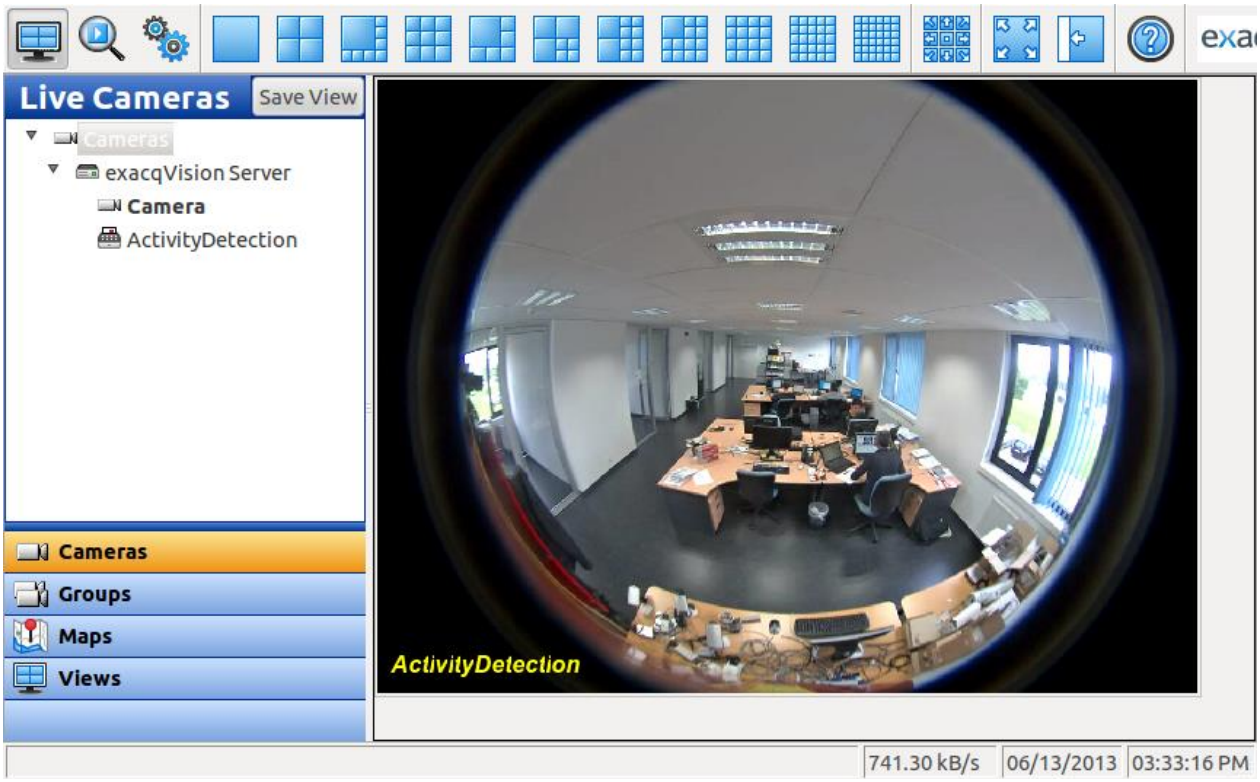


Using the ExacqVision configuration interface, you have to create one or several "***Serial Profile***" for the expected messages. For example, with the keyword "ActivityDetection" as shown above.



Then, a "***Serial Port***" of type « ***TCP Listener*** » must be added. It will create a server listening to the given port (e.g 9090). The IP of the camera (the emitter) must be given. Receiving data will be

forwarded to the Serial Profile for parsing.

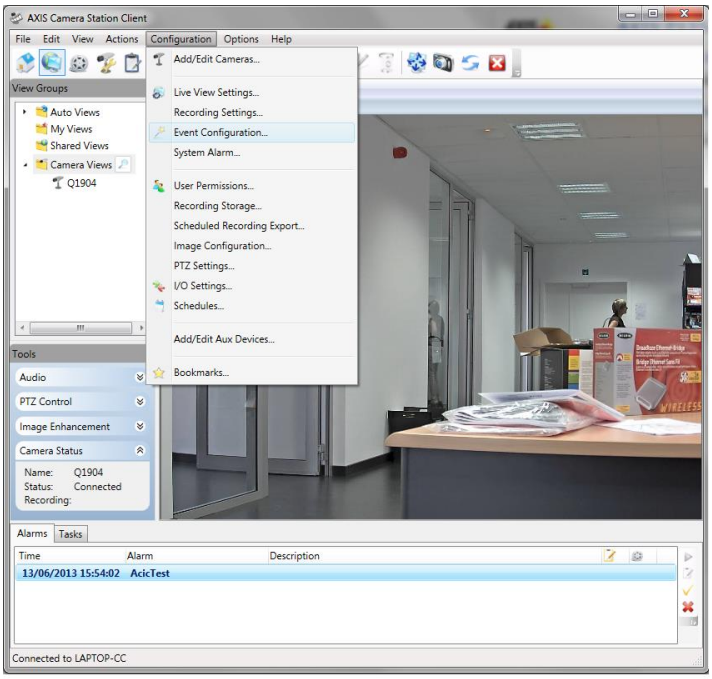


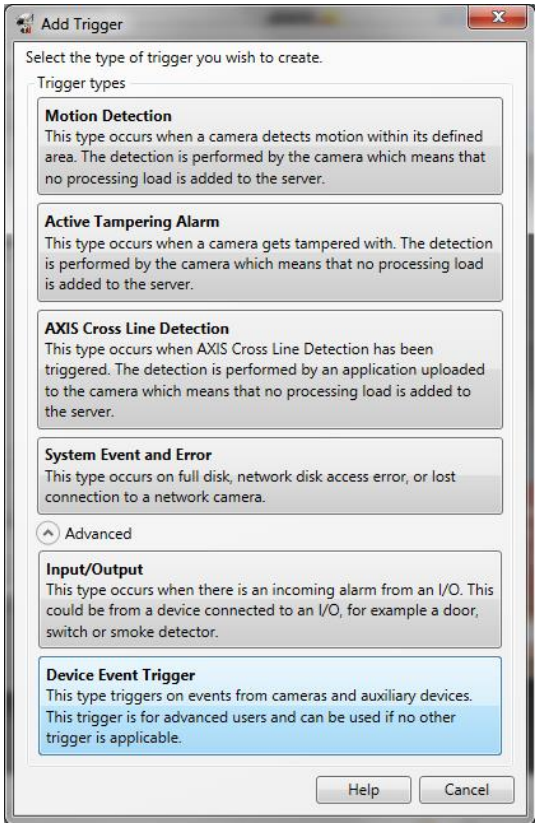
In the ExacqVision live view, it is now possible to show alarms. The serial profile(s) are displayed on the left panel and can be drag dropped on a video view. These alarm data are also recorded and can be reviewed synchronized with the video.

6 Axis Camera Station Integration

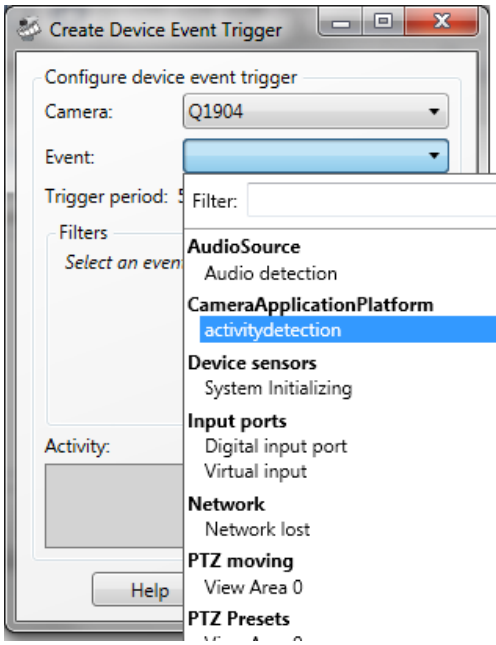
Axis Camera Station is a VMS from Axis found at http://www.axis.com/products/cam_station_software/index.htm.
If a camera is loaded with ACIC ActivityDetection Edge, detection events will be automatically visible in that VMS. No configuration is required on the camera side. The following procedure explains how to configure Axis Camera Station to use ACIC analytics event.

In the VMS, call the Event Configuration panel.

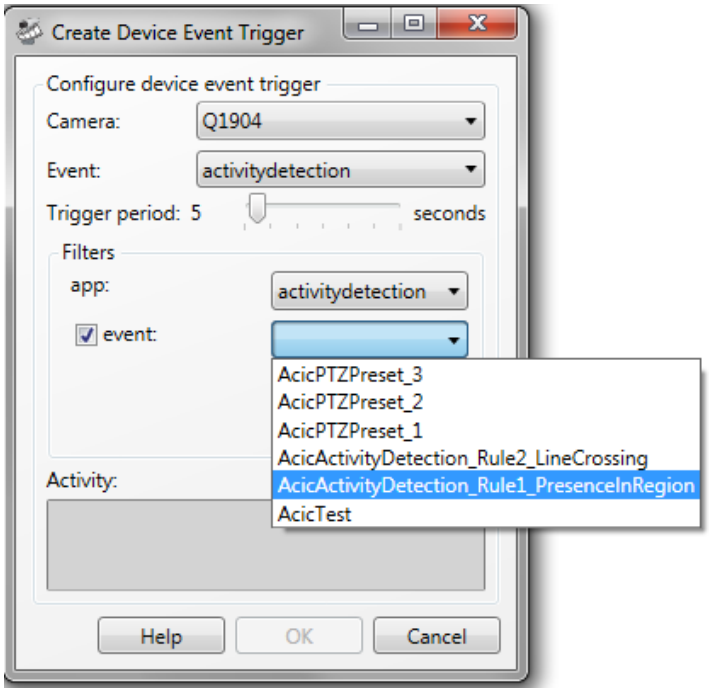




Choose « Device Event Trigger » as trigger type.

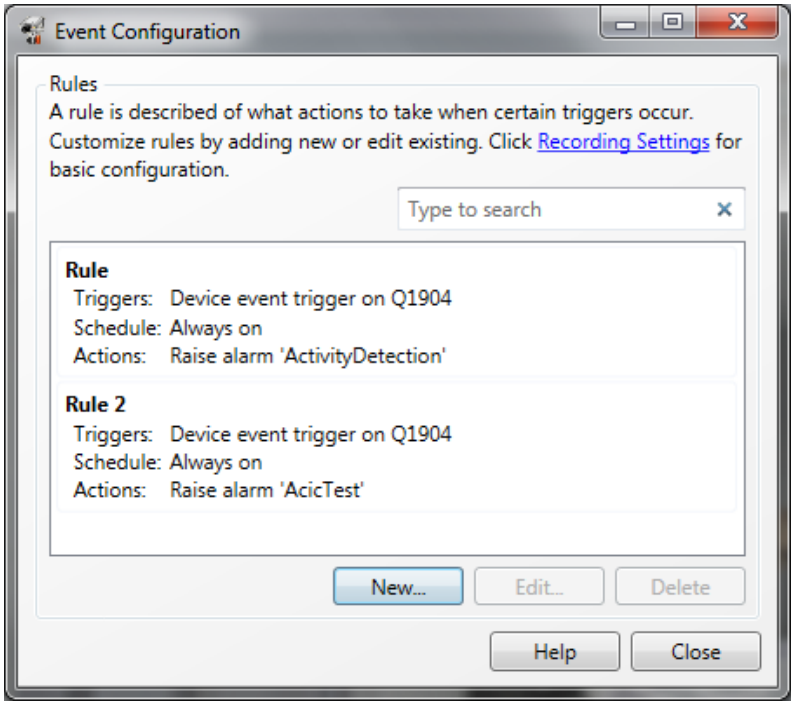


Choose « Camera Application Platform » as event source. The ACAP application name, ActivityDetection, should be in the list.

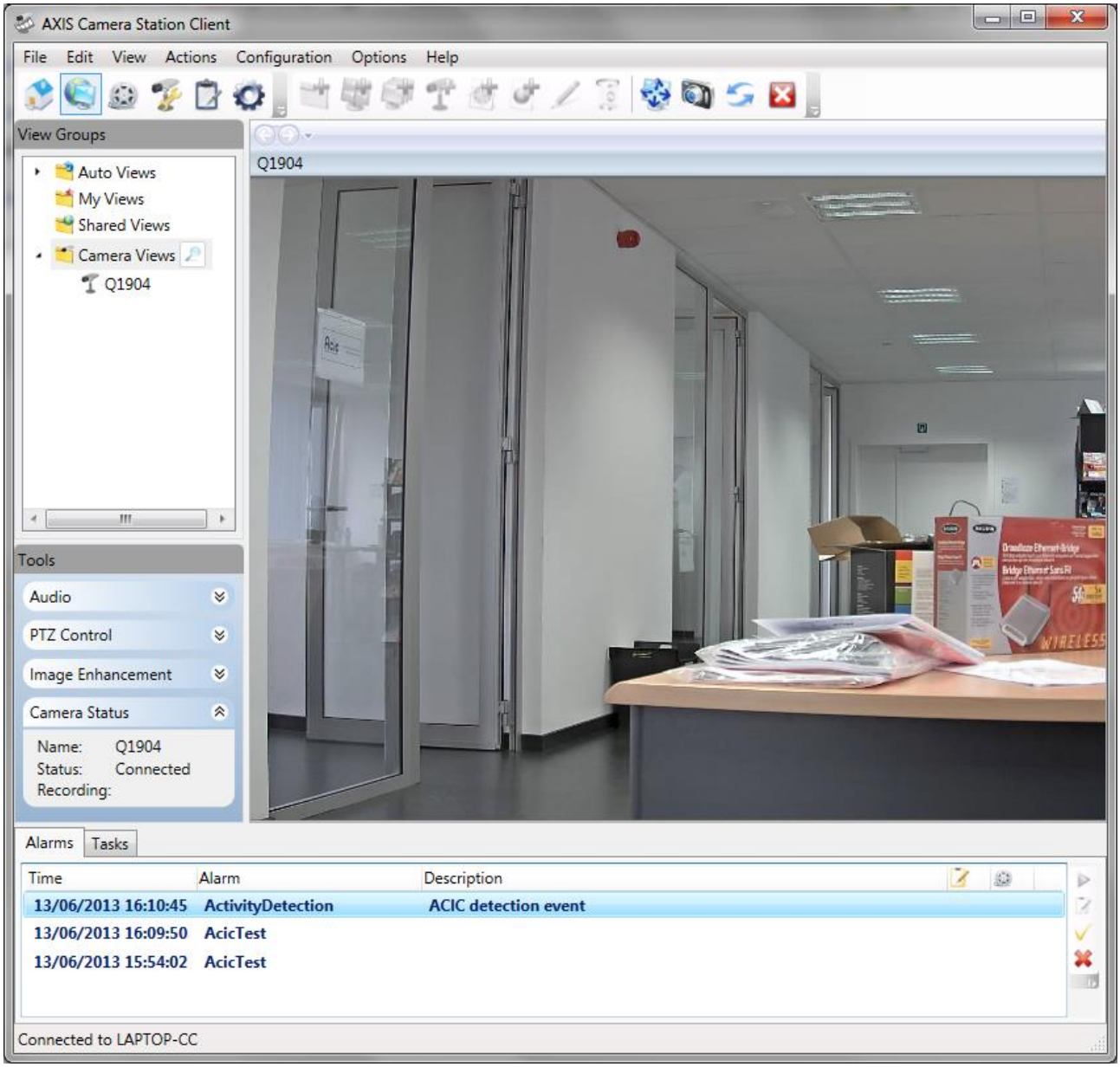


For that event source, a list of currently available events is presented. So, a specific ACIC event (detection rule, PTZ preset, test) can be selected for that rule.

Finally, after selecting an action (« ***Raise an alarm*** » here), the rule's configuration is complete and the process active.



Alarms are directly displayed on the bottom panel of the Axis Camera Station client. As many rules as necessary can be created. A test rule, using the ACIC event "***AcicTest***", is a convenient way to check the system communication.



7 Generic integration

The ActivityDetection Edge program has a multi-part HTTP protocol (http://en.wikipedia.org/wiki/MIME) for the dissemination of graphics events and meta data.
The URL to use is the following:

http://<ip of the camera>/local/activitydetection/streaming.cgi?<query string>

Parameters are available in <*query string*> to customize the stream format and content. That genetic interface is presented in detail in the "***ACIC API 1.2, metadata streaming***" document. That protocol can be use in Edge and Server ACIC products.

8 Miscellaneous integrations

8.1 Axis rule engine

ACIC ActivityDetection Edge events can be used to trigger actions in the Axis rule engine embedded in each camera. Refer to the Axis documentation for more information on the Axis rule engine.

Caveat : Due to a bug in Axis VAPIX, a call to port.cgi cannot have a delay between actions of more than 5 seconds. If the I/O must remain in a state for more than 5 seconds before returning to its initial state (“pulse”), you must use a manual trigger to return to the opposite state.