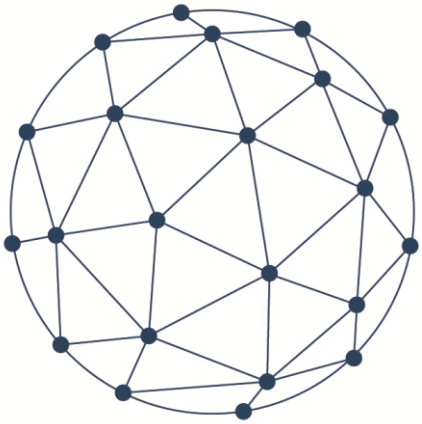


SGSE

Soluciones Globales de Seguridad Electrónica

AEOS INTRUSION MONITOR

Installer and user manual

Content

1. Document versions

Version	Date	Author	Description
1.0	01/2022	SDA	First version of the document

2. Introduction

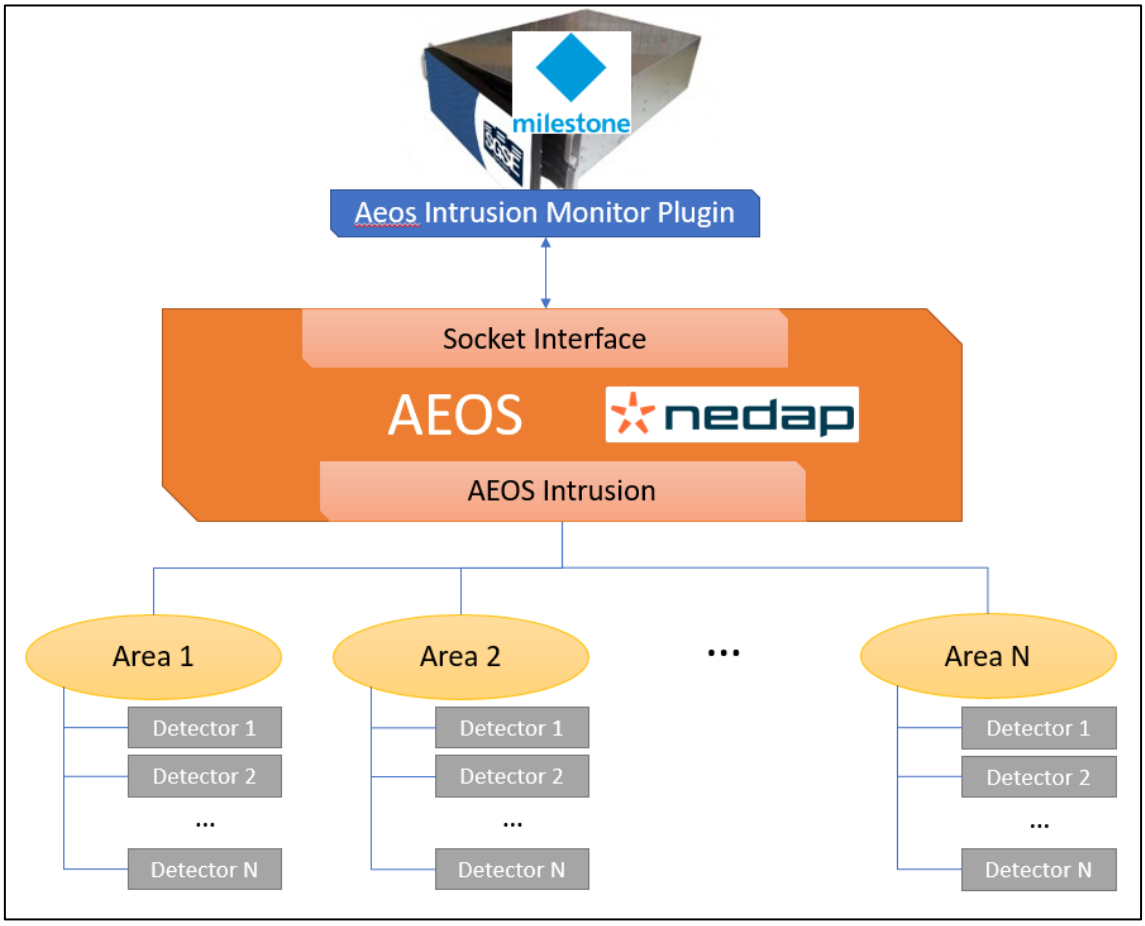
The purpose of this document is to explain the operation, installation and use of the software solution called "*AEOS Intrusion Monitor*".

This solution consists of a plugin that allows to monitor and interact with AEOS Intrusion solution (by Nedap), from the user interface and the working environment of the XProtect® platform, by Milestone.

In this way, the monitoring of the intrusion system is available together with the advantages of the XProtect® VMS for video and alarm management. CCTV and intrusion in a single interface.

3. Architecture

The architecture of the solution is described in the scheme below:



Through the Ethernet network, the plugin connects with the AEOS system through its *Socket Interface* API. AEOS must be properly configured to accept connections and requests from the plugin.

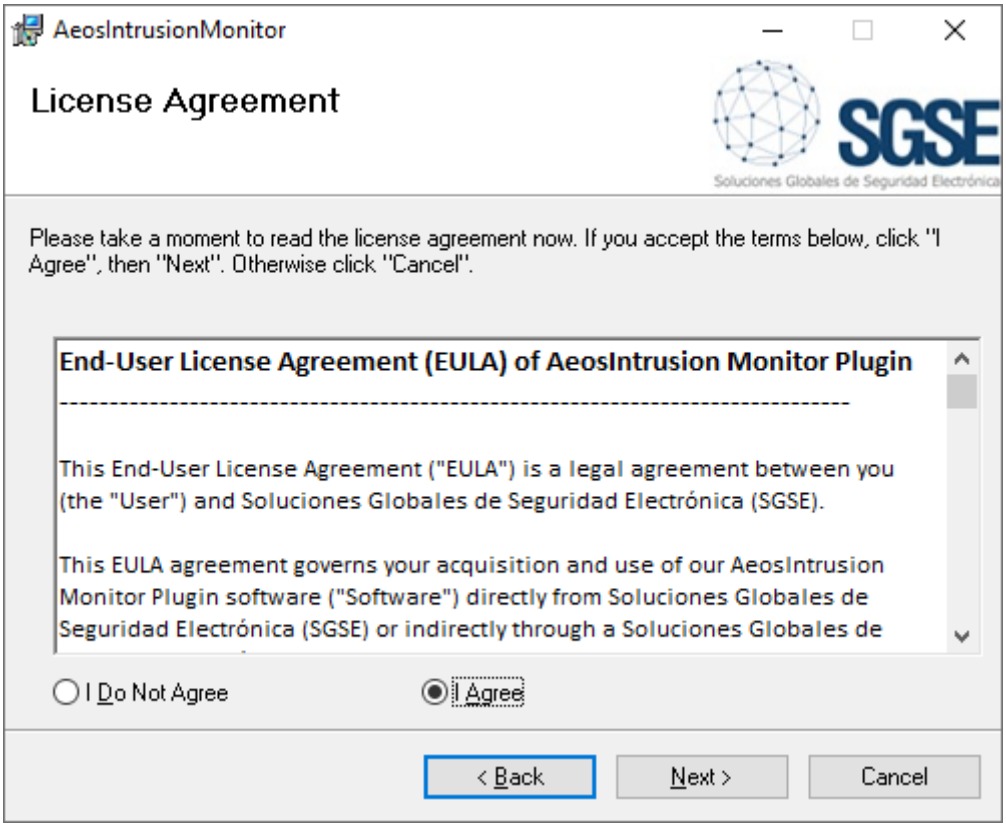
Once the communication is established, the plugin will import the AEOS Intrusion configuration (areas and detectors) and create the corresponding items in Milestone. The connection is kept open to:

- ✓ Send commands to the AEOS Intrusion system.
- ✓ Update the icons of Milestone items to show the current state of the intrusion system.
- ✓ Trigger intrusion related events in Milestone as they happen in the AEOS Intrusion system.

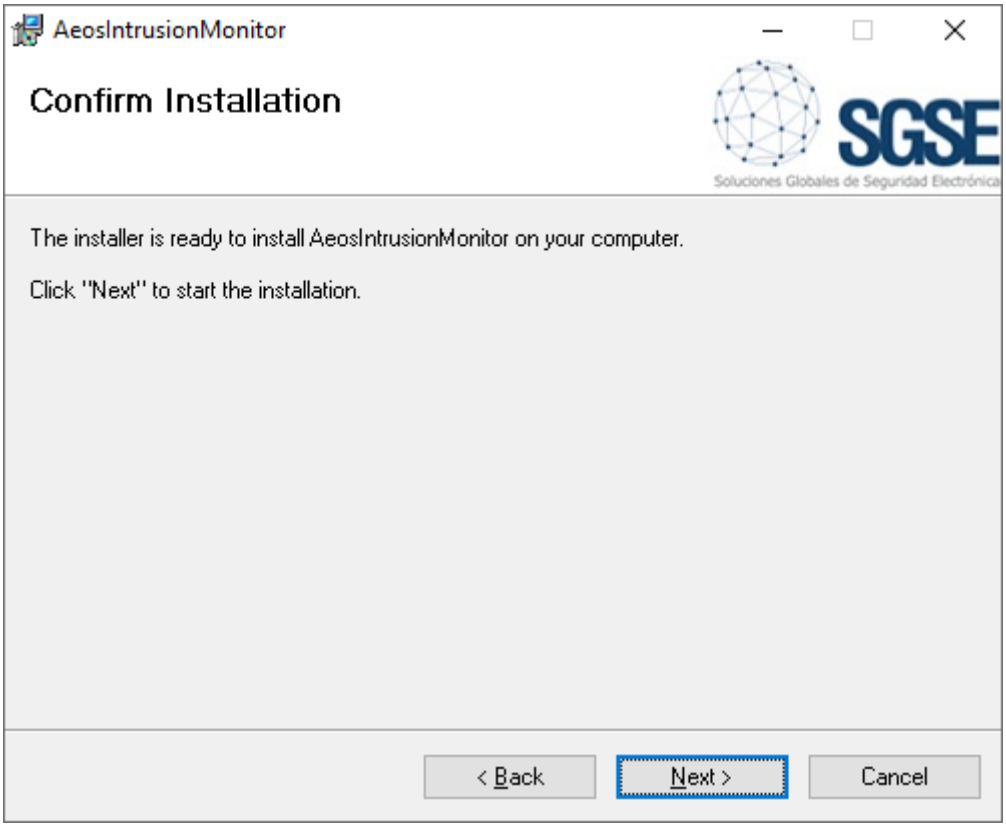
4. Installation

To install the plugin, simply execute with administrator rights the installer "AEOS Intrusion Monitor Installer.msi" provided by SGSE or downloaded from the Milestone Marketplace. The process is automatic. Throughout the different screens of the installer, we will only have to accept the End User License Agreement, a mandatory condition to be able to use the plugin.

Click “Next >” to start the installation process.

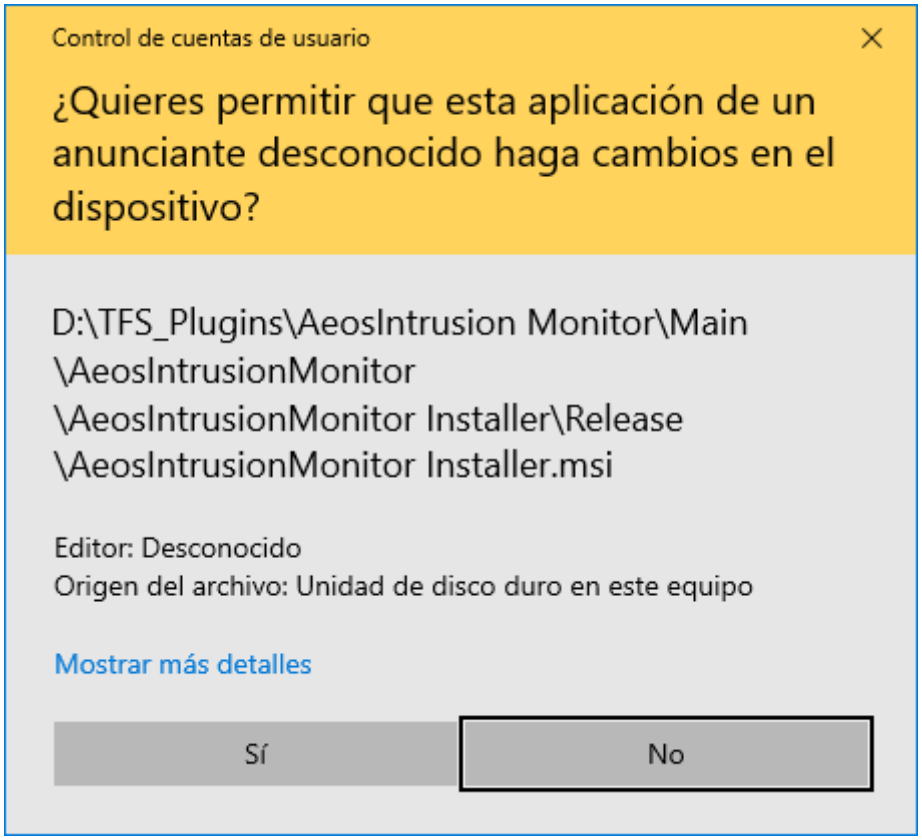


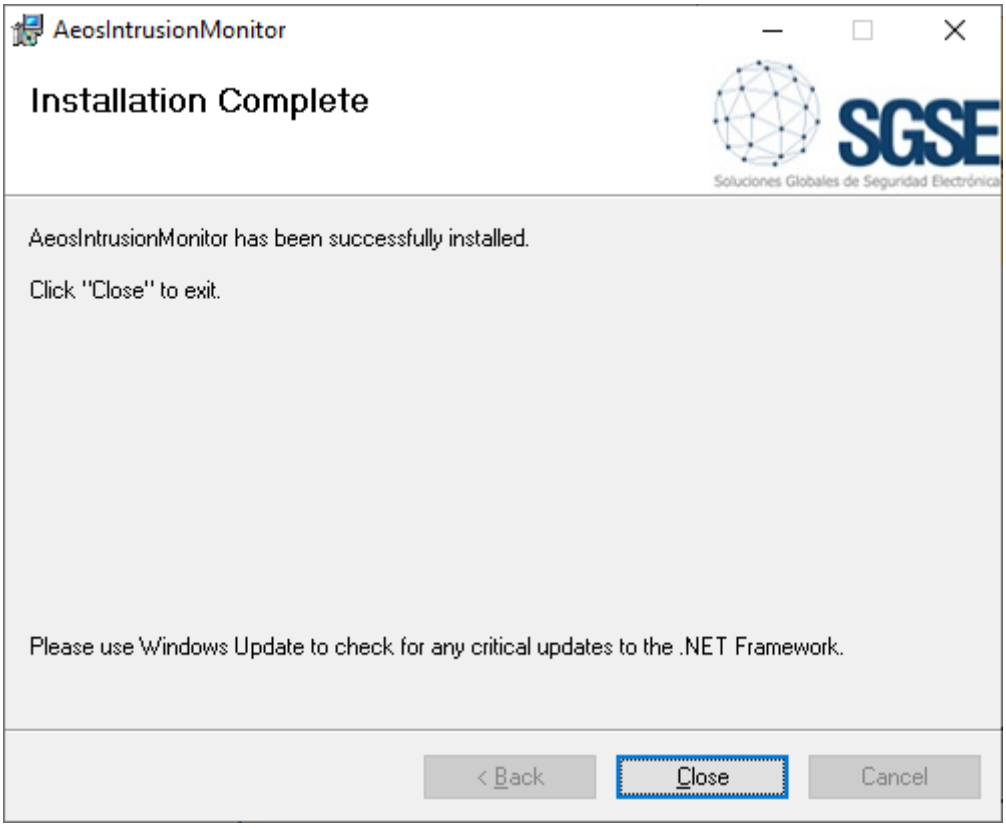
You will have to read and accept the End User License Agreement to proceed with installation.



Click “Next >” to proceed and install the plugin files.

If Windows User Account Control is enabled, you may have to allow the installer to go ahead with installation.





Once the process is finished, you can click “Close”. The plugin is already installed!

NOTE: if you have installed the plugin while Milestone XProtect was operating, then a restart of the Event Server and any client applications (Management Client, Smart Client) will be required.

5. Licensing

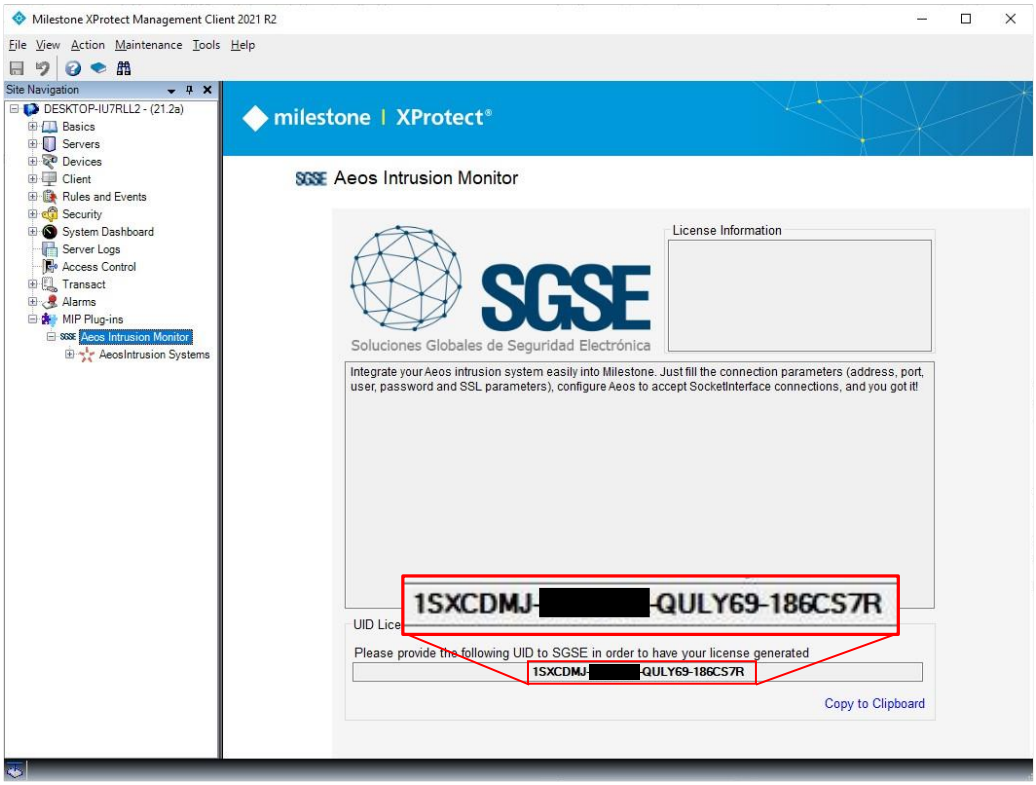
The plugin needs a license to run. Each AEOS system must be licensed. These licenses are generated by SGSE. The procedure to obtain the license file corresponding to the acquired license is described below. The license is also related to the number of detectors that exist in the AEOS Intrusion systems.

5.1 Getting a UID

In order to generate the license, you must provide the corresponding UID. This UID is a unique identifier to which the license is bound.

To get this code, you have to run XProtect® Management Client after installing the plugin and go to the corresponding menu item (*MIP Plugins > AeosIntrusion Monitor*).

In that screen, when the plugin is not licensed, you will see the corresponding UID.



Please provide this UID to SGSE, and you will get your license file generated.

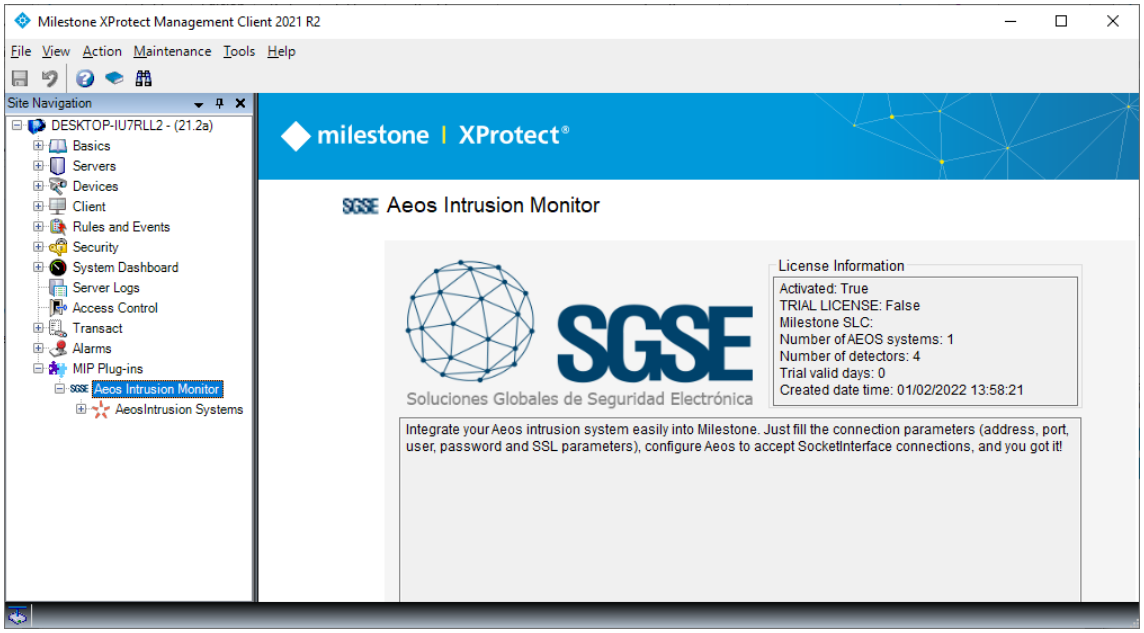
5.2 Applying the license

Please copy the license file "*Licencia.lic*" into the plugin folder. By default:

```
C:\Program Files\Milestone\MIPPlugins\AeosIntrusionMonitor\
```

After applying the license, Event Server must be restarted so that changes take effect, and we can use the plugin.

Once the license is applied, the Management Client interface will show the license information:



5.3 Workstations (only SmartClient)

To generate the UID in a workstation where you don't have XProtect® Management Client, but you will be only using SmartClient instead, you will have to use the SGSE tool, "*UID Generator*" to obtain the UID.

Please, contact SGSE support to get this tool.

6. Configuration

6.1 AEOS configuration

The AEOS Intrusion Monitor plugin makes use of the AEOS API "Socket Interface". For the plugin to work properly, some configuration must be done in the AEOS system.

6.1.1 Enable Socket Interface

In order to enable AEOS Socket Interface API, you have to configure the *aeos.properties* file.

1. Open the *aeos.properties* file (...\AEOS\AEserver\standalone\configuration).
2. Search for the following section:

```
#####################################
# aeos.service.InterfaceService
#####################################
aeos.service.InterfaceService.Port=8035
aeos.service.InterfaceService.UseSSL=false
aeos.service.InterfaceService.SSLClientAuth=false
aeos.service.InterfaceService.SocketTimeoutSeconds=0
aeos.service.InterfaceService.DelegateSubscriptions=true
aeos.service.InterfaceService.RMITimeoutMinutes=480
```

3. Check the following parameters:
    a. Port number: The AEOS interface service is listening on a port for socket connections. The port number is 8035 by default. If needed, you can change this number. This port will be needed in the plugin configuration.
    b. UseSSL (SSL/TLS connection): Set this value to true if you want to use a SSL/TLS secure connection with the AEOS Socket Interface. Make sure the correct SSL/TLS certificate is installed at the external system side of the connection. Without the correct certificate, the SSL/TLS secure connection will not work.
    c. RMITimeout: This is the timeout setting for RMIAdapter connections. After this timeout, the session of a logged-in user becomes invalid. On access, an exception is thrown. This timeout is set in minutes. The default value is 480 minutes (8 hours). You can change this value to your own preference. When the value is set to 0, the sessions will not expire at all.

When you've changed these settings:

1. Save the aeos.properties file.
2. Restart the AEOS application server.

6.1.2 Create user with required permissions

A user role can be defined that is allowed to execute only functions belonging to the Socket interface. To achieve this, log in to the AEOS maintenance interface and go to **Management/System users/Maintain user role**. Create a new role or assign the functions related to the Socket-connection (as listed below) to an existing role:

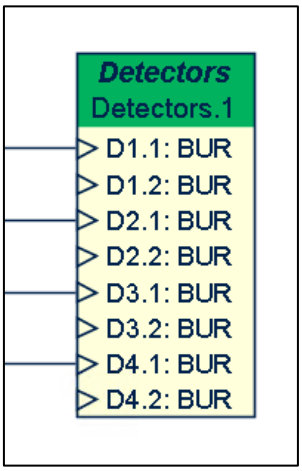
- Configuration, Socketconnection, Commands
- Configuration, Socketconecction, Events

Finally, assign this user role to a user. This user with its password will be needed in the plugin configuration.

For more information on the Socket Interface configuration, please refer to the *"AEOS Socket Interface Installation and Configuration"* manual.

6.1.3 Define Detectors (AEmon)

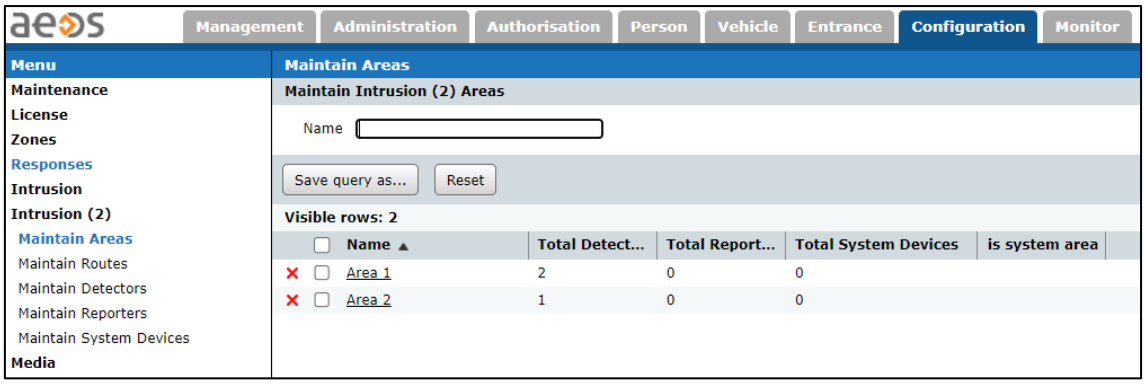
Using the AEmon tool, define intrusion system Detectors using **Intrusion > Detectors** behaviour components. For more information about AEOS Intrusion setup and configuration, please refer to the "*AEOS – Intrusion Installation and configuration*" manual or to your Nedap distributor.

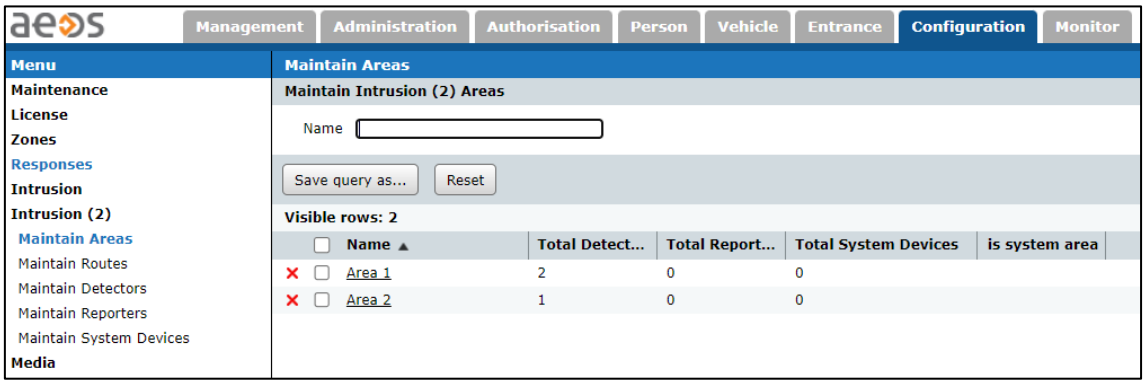


NOTE: apart from the detector AEbc themselves, it is necessary to add a *TaggedServiceManager* for the Socket Interface to report the intrusion elements to the plugin.

6.1.4 Create Intrusion Areas (AEOS Administration web)

Using the AEOS administration web interface, create intrusion areas and assign them the defined detectors.





For more information on the Intrusion system configuration, please refer to the "*AEOS – Intrusion Installation and Configuration*" manual.

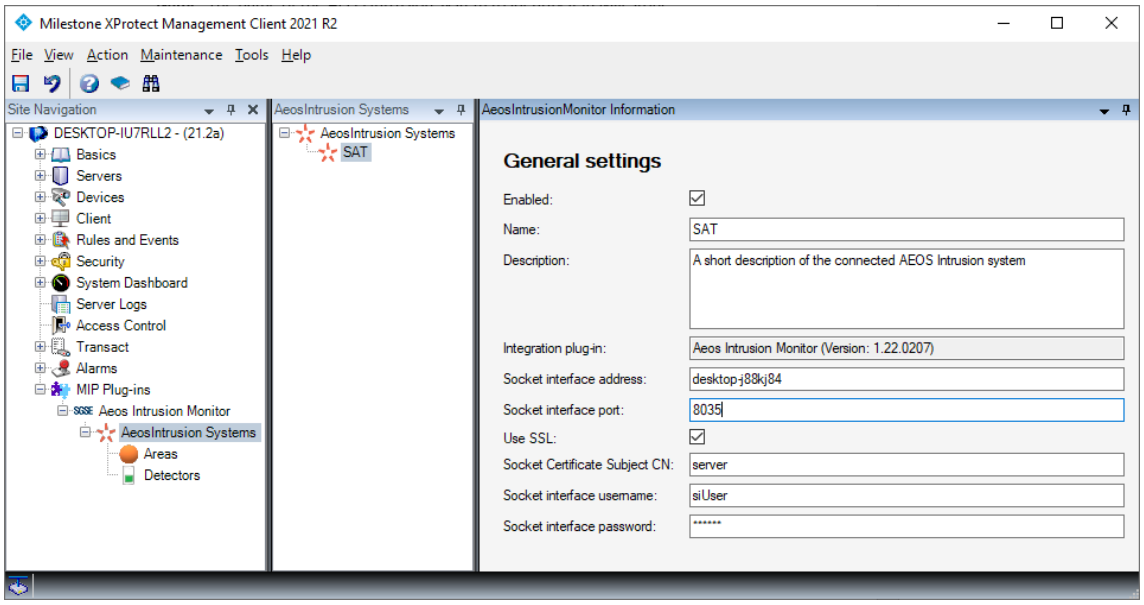
6.2 Plugin configuration

6.2.1 Set up connection

From the plugin side, we will have to set the configuration to connect to the AEOS Intrusion system. This connection set up must match and will depends on the configuration at the AEOS server side.

The required parameters are shown in the picture below and are the following:

- **Enabled**: Use this checkbox to enable or disable the interaction with the AEOS Intrusion system in Milestone.
- **Name**: The name of the AEOS Intrusion system to identify it in Milestone.
- **Description**: A description of the AEOS intrusion system.
- **Socket interface address**: The hostname or the IP address of the AEOS server where the socket interface API is listening.
- **Socket interface port**: The port in which the socket interface is listening.
- **Use SSL**: Use this checkbox to tell the plugin if SSL is used in the connection to the socket interface.
- **Socket Certificate Subject CN**: In case of using SSL, this field must contain the Common Name that appears in the AEOS server SSL certificate.
- **Socket interface username**: The username to log in into AEOS through the socket interface.
- **Socket interface password**: The password of the user used to log in into AEOS through the socket interface.



Once the plugin has been properly configured, it automatically retrieves the areas and detectors defined in AEOS Intrusion and creates the corresponding items in Milestone (data refresh by pressing F5 might be required to see the items in the Management Client).

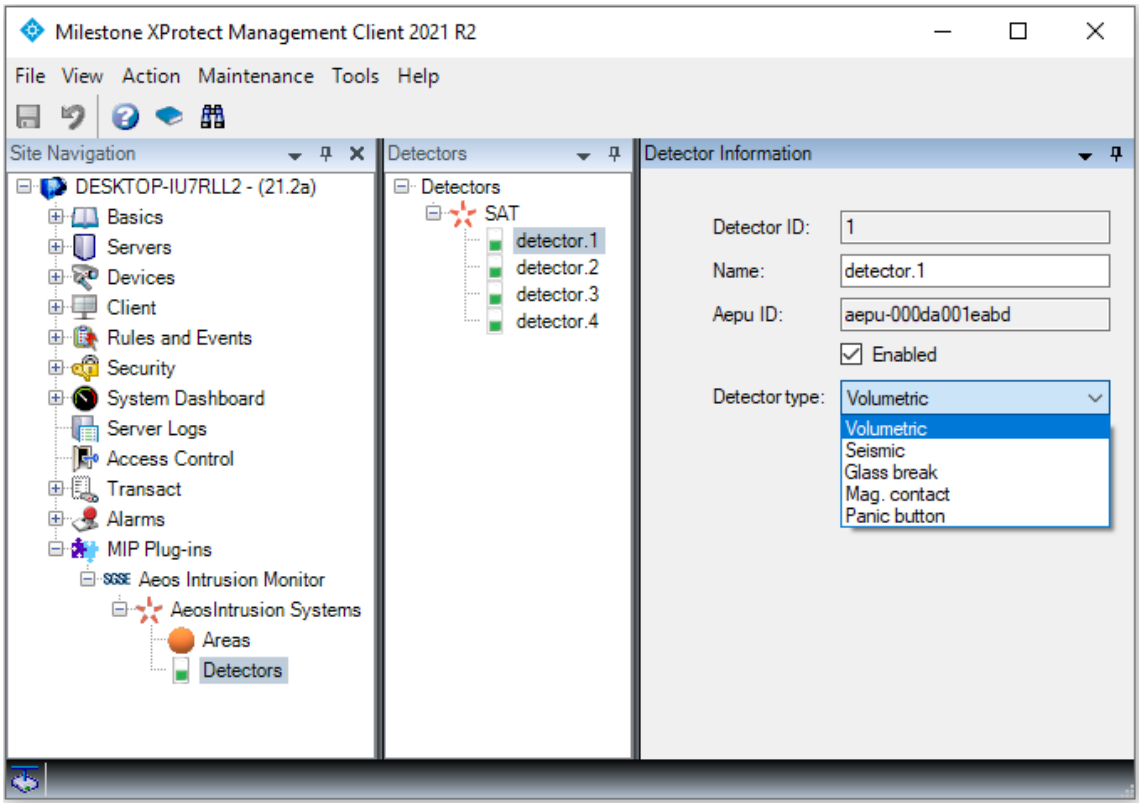
No further configuration is required for the plugin to operate, although some fine tuning might be wanted for the operators to have a better idea of the intrusion system and to get a completely useful integration, like specifying the kind of detectors or defining the alarms that must be triggered upon receiving AEOS intrusion related events.

6.2.2 Detector type

The default icon for detectors is a volumetric detector. The plugin allows the user to define the type of detector by selecting from a set of kinds. This will change the icons of the detectors on the Smart Client maps.

To change the detector type, just go to the detector item itself in the Management Client and then select the detector type from the drop-down selectable options. The available detector kinds are:

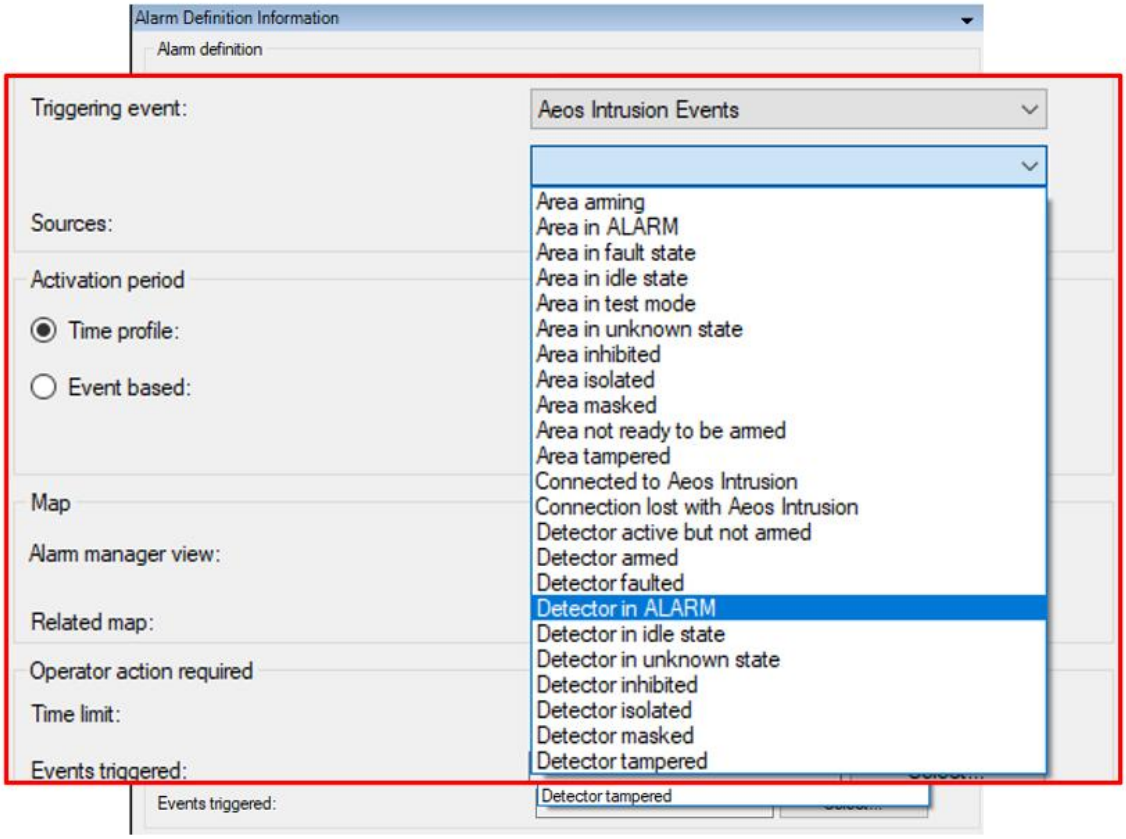
- Volumetric (PIR) – Default value
- Seismic
- Glass break
- Magnetic contact
- Panic button



From this page you can also see which AEpu the detector is associated to in AEOS, and change the name of the detector in Milestone, for a better understanding of the operator.

6.2.3 Alarms definition

The plugin defines a set of events that are triggered by the AEOS Intrusion integration. These events can be used to define which of them, when triggered from specific sources, must be considered as alarms. You just have to go to the "Alarm definition" section, within Management Client, and create a new alarm whose triggering event is an event from the *AEOS Intrusion Events* group and specify the item(s) from which you want this event to be considered as an alarm.



The available events are listed in the following section.

As an example, you can define an alarm in Milestone when the “Detector in ALARM” event is triggered from any detector (selecting all detectors). This way, whenever any detector goes into alarmed state in AEOS Intrusion systems, an alarm will be fired in Milestone.

6.2.4 Rules – events

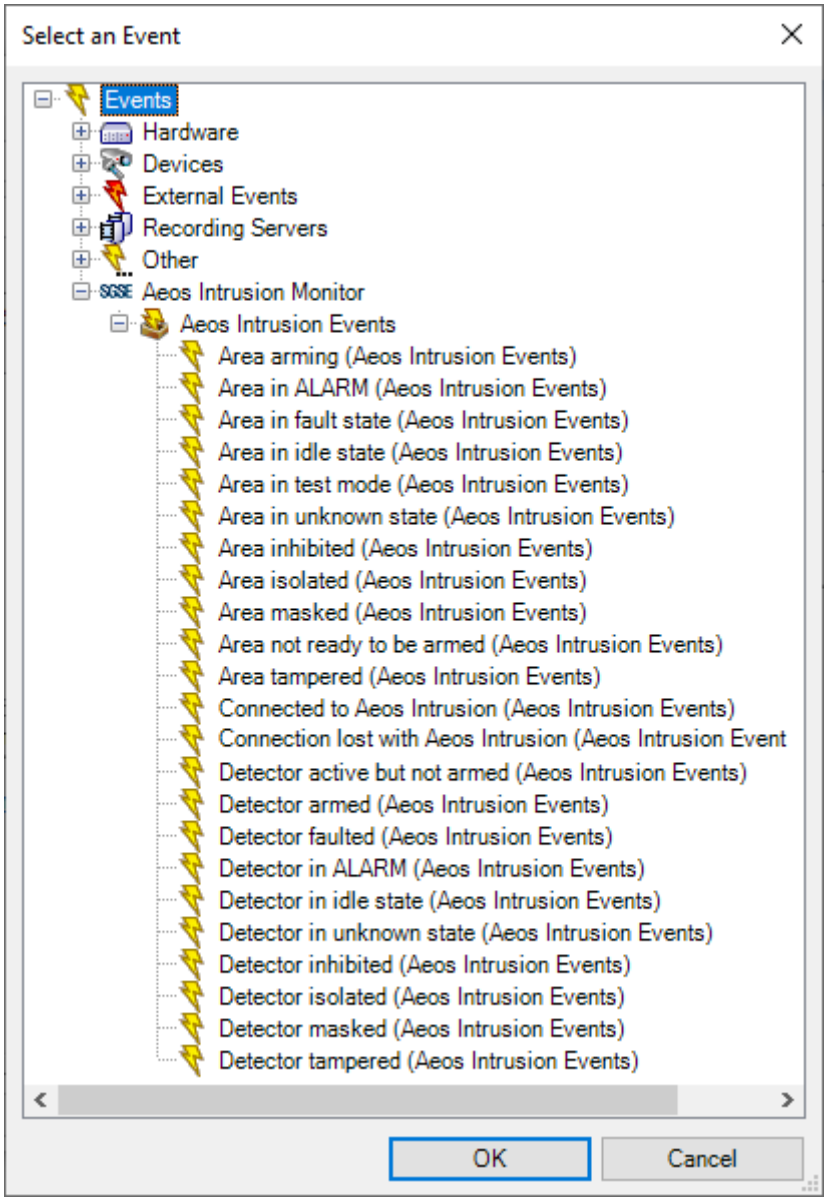
The same events that can be defined as alarms, can also be used to trigger rules in Milestone. Just create a rule and select as “Triggering event” an event from those added by the plugin.

The events that are currently supported by the plugin are:

- Area arming
- Area in ALARM
- Area in fault state
- Area in idle state
- Area in test mode
- Area in unknown state
- Area inhibited
- Area isolated
- Area masked
- Area not ready to be armed
- Area tampered
- Connection established to AEOS Intrusion system

- Connection lost with AEOS Intrusion system
- Detector active but nor armed
- Detector armed
- Detector faulted
- Detector in ALARM
- Detector in idle state
- Detector in unknown state
- Detector inhibited
- Detector isolated
- Detector masked
- Detector tampered

As an example, you may want to move a PTZ camera to a specific preset when one of the detectors, let's say, back corridor, is active (it is detecting something) but the area is not armed, so it's not an alarm. Then you can create a rule so that the "Detector active but not armed" event coming from the detector located at the back corridor is the triggering event, and as an action you move the associated PTZ camera to the preset that looks at the back corridor.



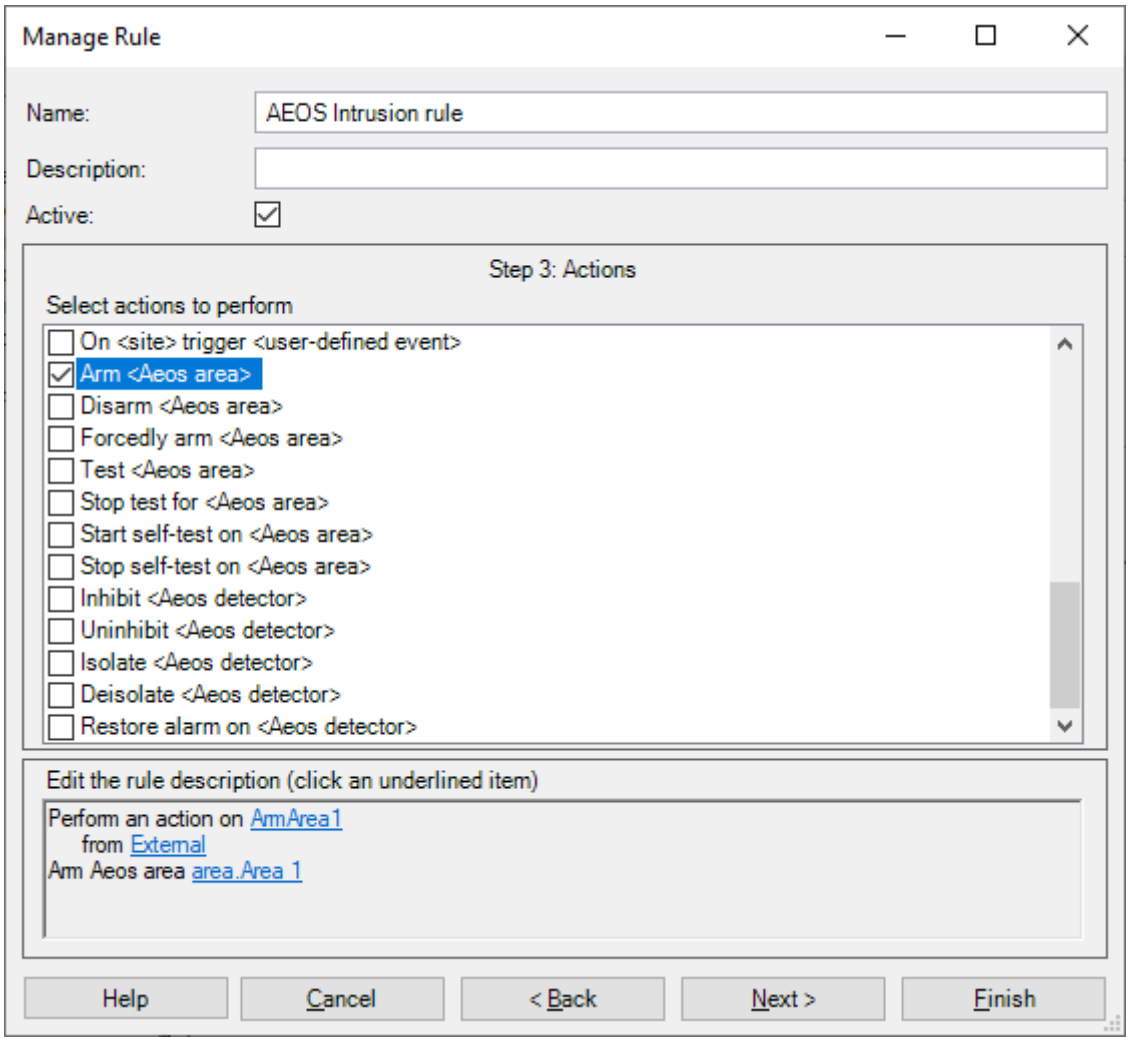
6.2.5 Rules – Actions

The plugin also adds Actions to be performed into the AEOS Intrusion system when a defined rule is triggered by any event in Milestone.

You can define rules to perform the following actions on the AEOS Intrusion system:

- Arm an area
- Disarm an area
- Forcedly arm an area
- Test an area
- Stop test on an area
- Start self-test on an area
- Stop self-test on an area
- Inhibit a detector
- Disinhibit a detector
- Isolate a detector

- Deisolate a detector
- Restore alarms on a detector



6.2.6 Role permissions

Milestone allows you to assign roles to users and give them specific permissions. The AEOS Intrusion plugin adds the possibility of assigning permissions on the different elements of the AEOS intrusion system, by group of by specific element. Specific permission can also be defined.

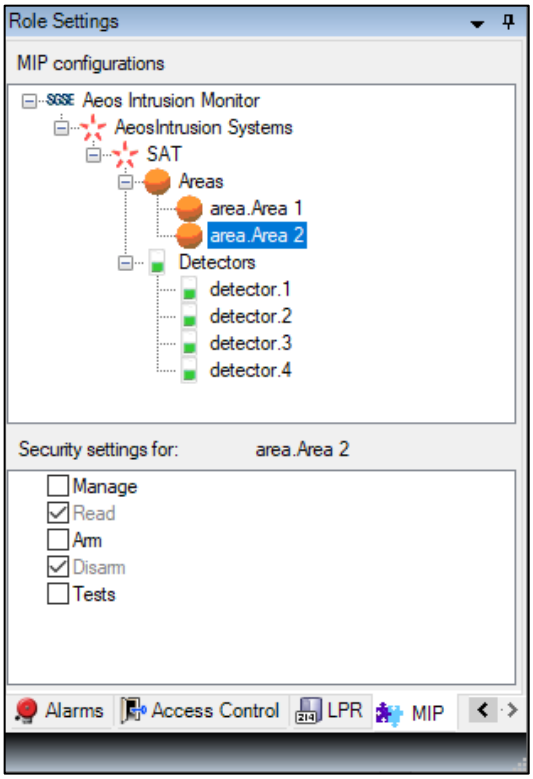
You can define the generic read permissions, so that the user can see the elements and their related alarms. And to define how the users in the role can interact with the intrusion elements, you have separated permissions to choose from.

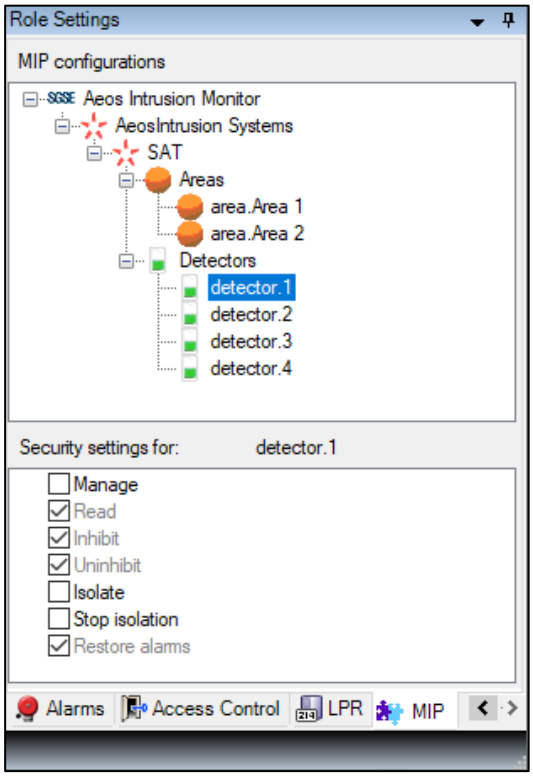
For areas, you can specify the following specific permissions:

- Arm
- Disarm
- Tests

For detectors, you can specify the following specific permissions:

- Inhibit
- Disinhibit
- Isolate
- Deisolate
- Restore alarms





7. Operation

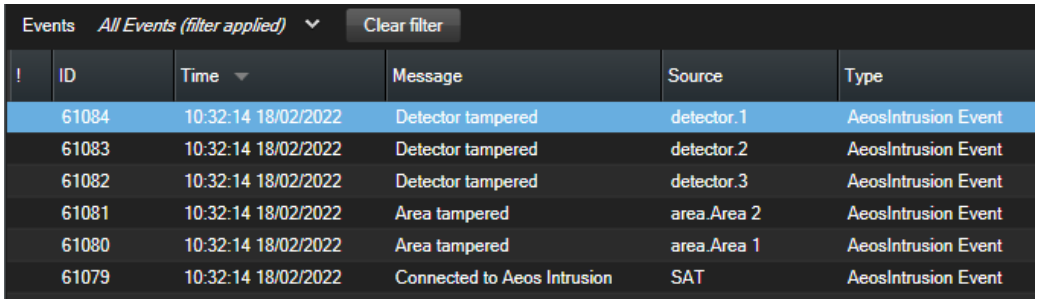
The AEOS Intrusion Monitor plugin allows you to monitor and interact with AEOS Intrusion systems. Interaction can be automatically performed through rules, as described before, or manually by the operator. Monitoring and every manual interaction is performed from the Smart Client, which is the standard user interface in Milestone XProtect®.

By using User-defined events with rules, and alarms, monitoring and interaction can also be done through other interfaces (Web Client, Mobile App), although not all the features are available using these interfaces (like maps or side panel tree view), as explained in section 7.4.

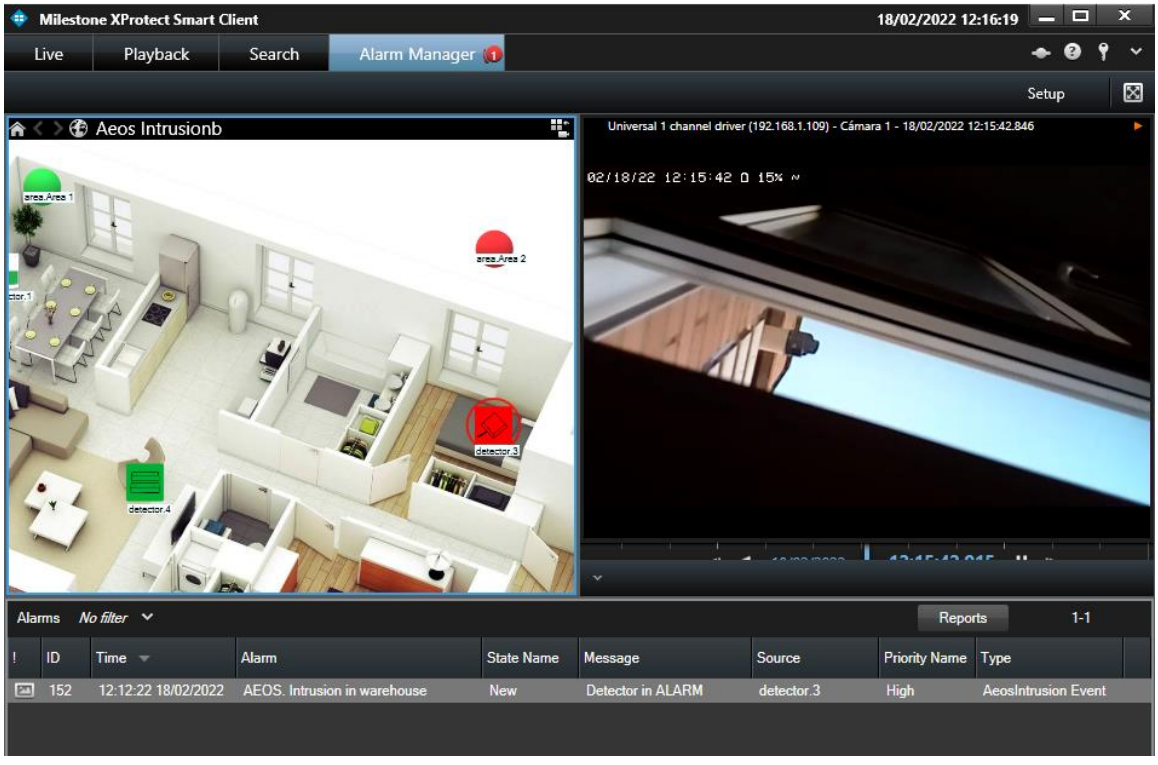
The operator can interact with the AEOS Intrusion system and send commands to the areas or to the detectors.

7.1 Event/alarm viewer and Alarm Manager

From the standard events and alarms viewer, defined alarms and events coming from the AEOS Intrusion system can be viewed and managed.



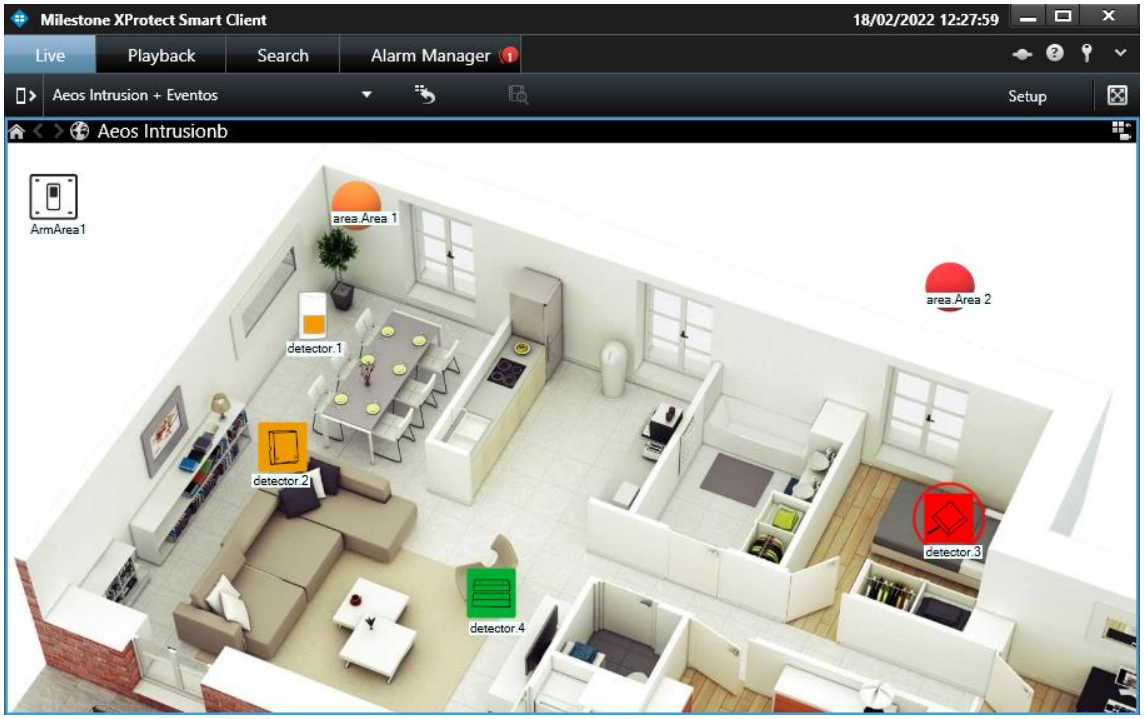
Alarms can also be managed as any other Milestone alarm using the Alarm Manager.



7.2 Maps

Icons corresponding to areas and detectors can be added to any XProtect® map on Smart Client.

The icon of each area and detector will show the state of the corresponding intrusion element according to the colour legend referenced below.



Icons for areas are the following:

Colour	Icon	Meaning
Green		**Idle**: The area is OK, it is not armed and there is no problem.
Orange		**Armed**: The area is OK and armed.
Red		**Alarm**: The area is in alarmed state.
Dark green		**Not ready to arm**: The area is not ready to be armed. Probably an associated detector is active.
Blue		**Inhibited or isolated**: The area is inhibited or isolated.
Magenta		**Masked or tampered**: The area is masked or tampered.
Yellow		**Fault**: The area is in fault state
Gray		**Disabled or unknown**: The area has been disabled in Milestone or the state is unknown.
Green/Orange		**Test**: The area is in test mode

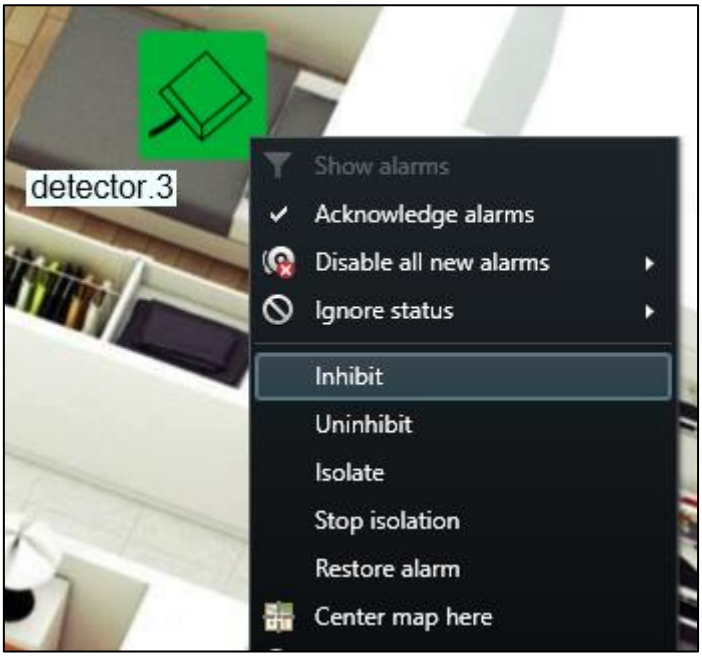
The detector icons also represent the selected detector type during the configuration. Icons for detectors are the following:

Colour	Volumetric	Seismic	Glass break	Magnetic Contact	Panic button	Status
Green						**Idle**
Orange						**Armed**
Red						**Alarm**
Dark green						**Active but nor armed**
Blue						**Inhibited or isolated**
Magenta						**Masked or tampered**
Yellow						**Fault**
Gray						**Unknown or disabled**

The icons also let you interact with the corresponding item, through their context menu (secondary button of the mouse).

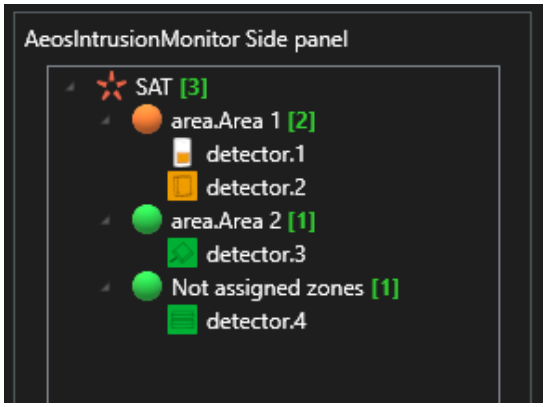
This way, you can interact with areas to arm, disarm, forcedly arm, test, stop test, start self-test or stop self-test:

And with detectors to inhibit, disinhibit, isolate, deisolate or restore alarms:



7.3 Side panel tree view

To have a quick overview of the system in every moment, you can see the areas and their associated detectors in the side panel tree view.



The icons represent their state, as they do on the maps, and allow you to directly interact with them, performing the same commands that can be performed through the context menu of each item.

7.4 Web client and Milestone Mobile

These two interfaces do not support all the functionalities of the AEOS Intrusion plugin, like maps or the side panel tree view.

However, it is still possible to monitor and interact with the AEOS Intrusion system through these interfaces. Alarms defined in the systems can be received in any of these interfaces, so you can monitor the system through its alarms.

By using User-defined events to trigger rules performing actions on the AEOS Intrusion system, interaction can also be done through these interfaces, as user-defined events can be triggered from both the Web Client and the Milestone Mobile.

8. Troubleshooting

Problem	Possible reasons and solutions
There is no connection with AEOS	Verify the network connection. Verify the Socket Interface configuration. Verify that the plugin configuration matches Socket Interface configuration. Verify the user rights in AEOS. Restart Event Server.
You can see nothing related to the plugin	Restart application and/or Event Server. Verify that the product is licensed.
Areas have a tampered state for a connection lost.	Go into AEOS status administration page and restore the areas state. Restore alarms on the detectors of this area that might be on a tampered state.
You cannot perform actions on elements	Verify your Milestone user's roles and permissions. You should receive a response message telling you why you cannot perform that action.
The status of a detector is not being updated.	Probably the detector is not assigned to an area. Changes on state of detectors that are not assigned to an intrusion area are not reported by AEOS. Restart Event Server.
Management Client and Smart Client on separate PCs do not show anything about the plugin.	The plugin requires the main Event Server license, but any PC running Smart Client or Management Client also needs a licence file to run. Ask SGSE for these files, specifying that they are client licenses with: - the required UID, - the PC it is for (as you identify it) - the main license info (UID, SLC, site name).

If you need further assistance, please collect logs and specify the problem you have as clearly as possible, describing the problem itself, the situation in which it happens, etc.

Relevant logs can be accessed in the following folders:

- C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs\
- C:\ProgramData\Milestone\XProtect Smart Client (if logs are enabled in Smart Client)
- C:\ProgramData\SGSE\AeosIntrusionMonitor\Logs

If you need support related to the plugin, please contact SGSE at sat@sgse.eu for technical issues or info@sgse.eu for commercial issues.

If you need support related to a general Milestone issue, please contact Milestone support (https://www.milestonesys.com/es/support/) or your Milestone provider.

If you need support related to AEOS configuration or AEOS Intrusion system, please contact Nedap support or your AEOS provider.