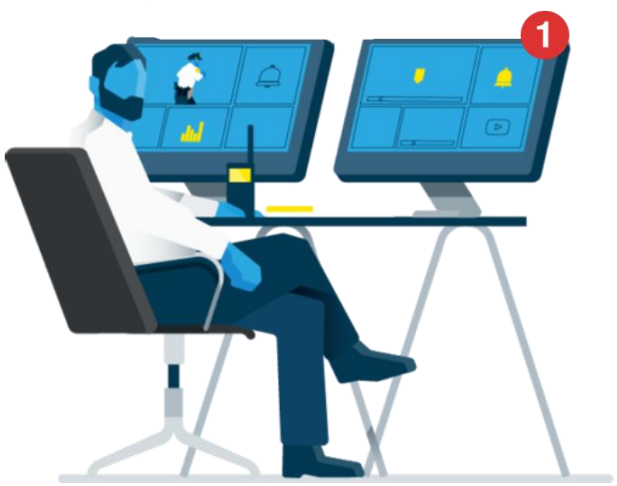
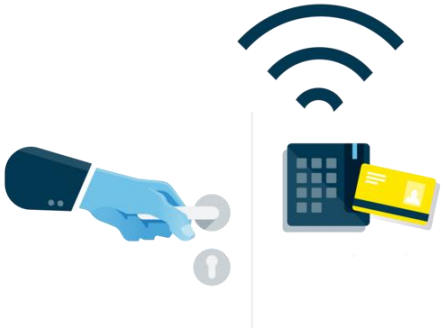
Nova networks





milestone VERIFIED

# InovaLink FEA – User Manual

# Contents

# InovaLink Introduction

InovaLink is a plug-in with the objective of linking Eden Innovations OPTIMA Box access control software, with Milestone XProtect VMS, in order to connect the alarm functions within XProtect with the alarms generated in the OPTIMA Box.

The plug-in is configured by a system administrator in the XProtect Management Client. The administrator establishes the connection with the related OPTIMA Box. With a valid connection, the OPTIMA Box elements are added to the Milestone XProtect System. The system administrator can then create a new alarm in the Alarm Definitions based on any of the events that are launched by the OPTIMA Box.

In the Smart Client, users are notified of any alarms (created by the system administrator). They can get more information using the Alarm Manager plug-in and by enabling the “Tag” column in the Alarm Data Settings.

# Installation and Deployment

## Prerequisites

The InovaLink plug-in must be installed on the machines running Milestone Systems XProtect Management Client and Milestone Systems XProtect Event Server.

This product only works with Eden Innovations OPTIMA Box.

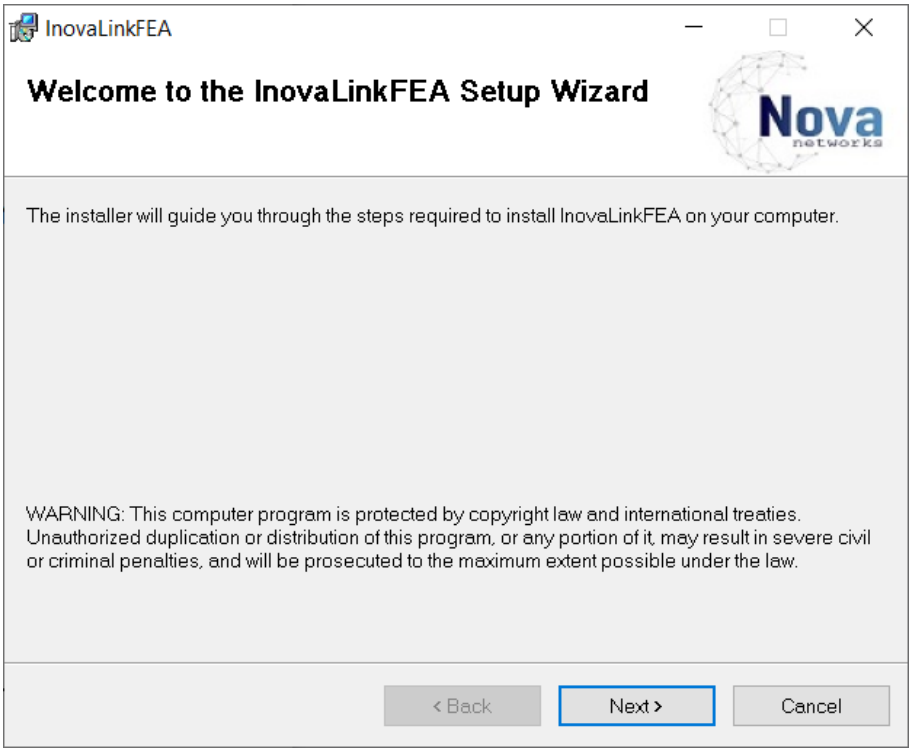
**The InovaLink plug-in requires a valid XProtect Software License Code.**

**Please note that the product will not work until a Product license is activated.**

# Installation Procedure

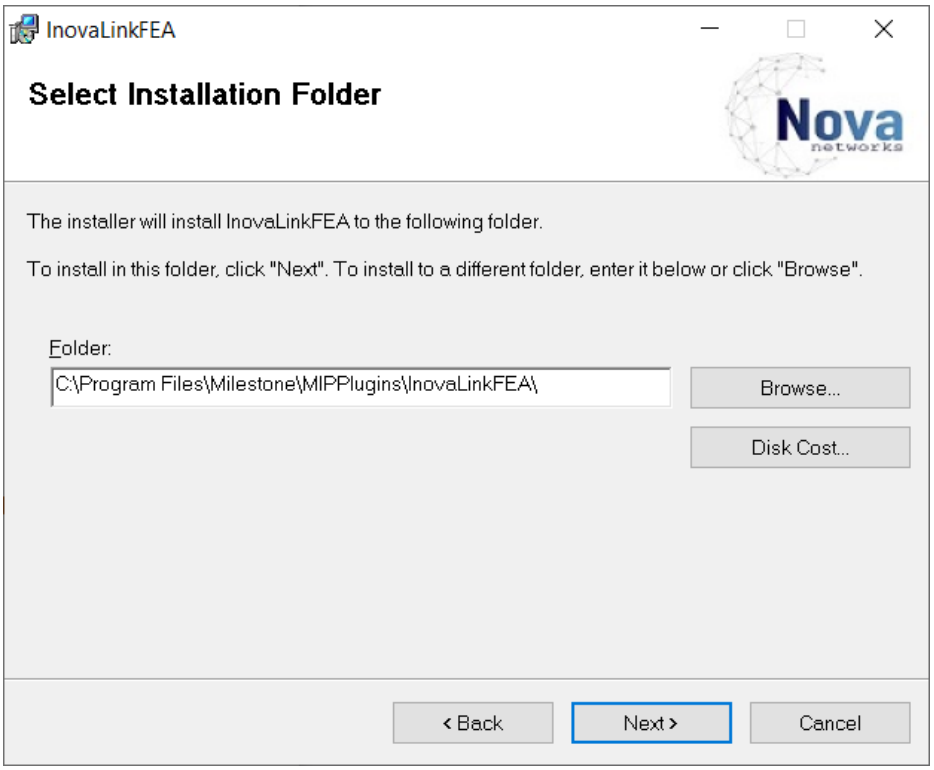
## Install the Management Client Plug-in

1. Double-click the executable program file of *InovaLinkFEA-mngt-plugin* to enter the welcome page of the Setup Wizard.



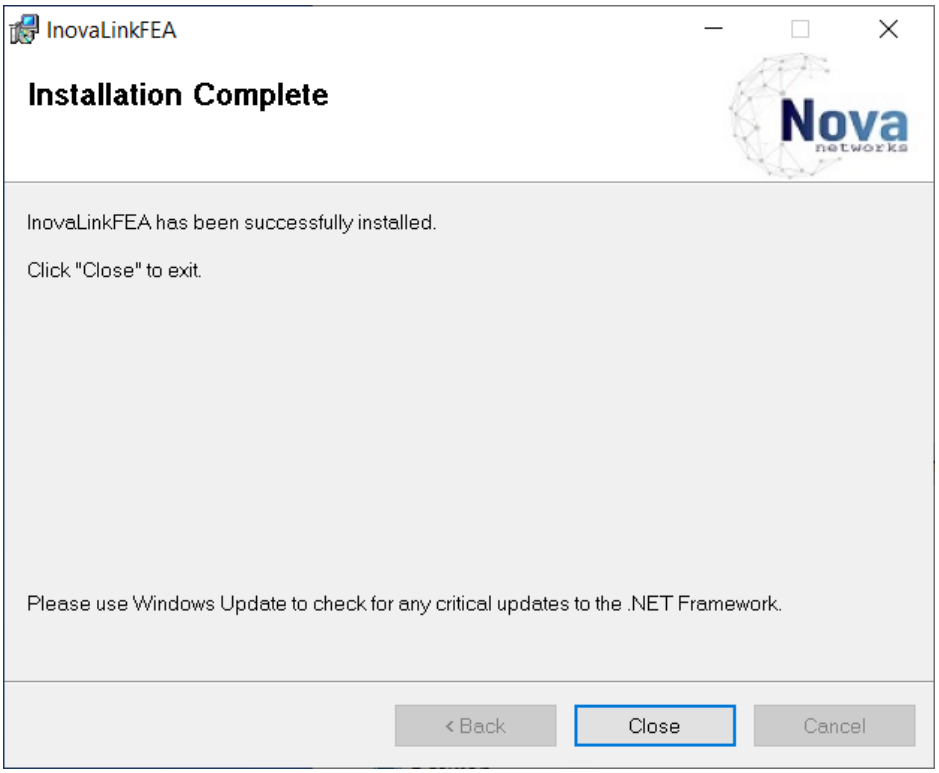

2. Click **Next** to start the setup wizard.

3. The plug-in must be installed in the corresponding Milestone MIPPlugins folder. The default path is “C:\Program Files\Milestone\MIPPlugins”. Click **Change** to select a proper directory as the installation location.




4. Optional: Click **Back** to review or change any of the installation settings.

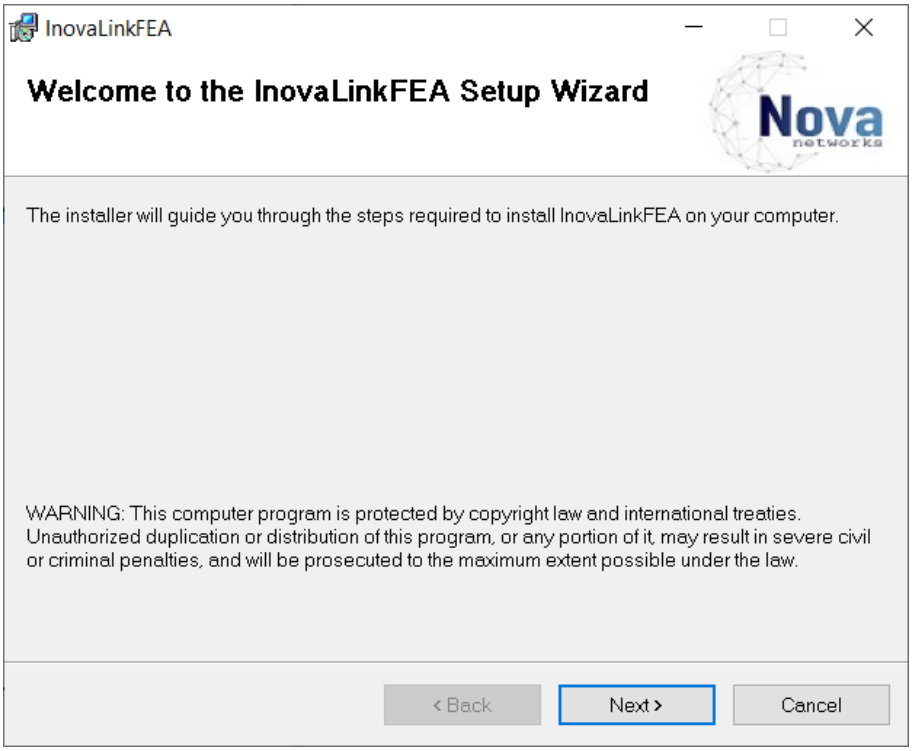
5. Click **Next** to start the installation. After starting installation, a progress bar will appear to show the installation status. Click **Cancel** to interrupt the installation process if needed.




6. Click **Finish** to complete the installation after the progress is ended.

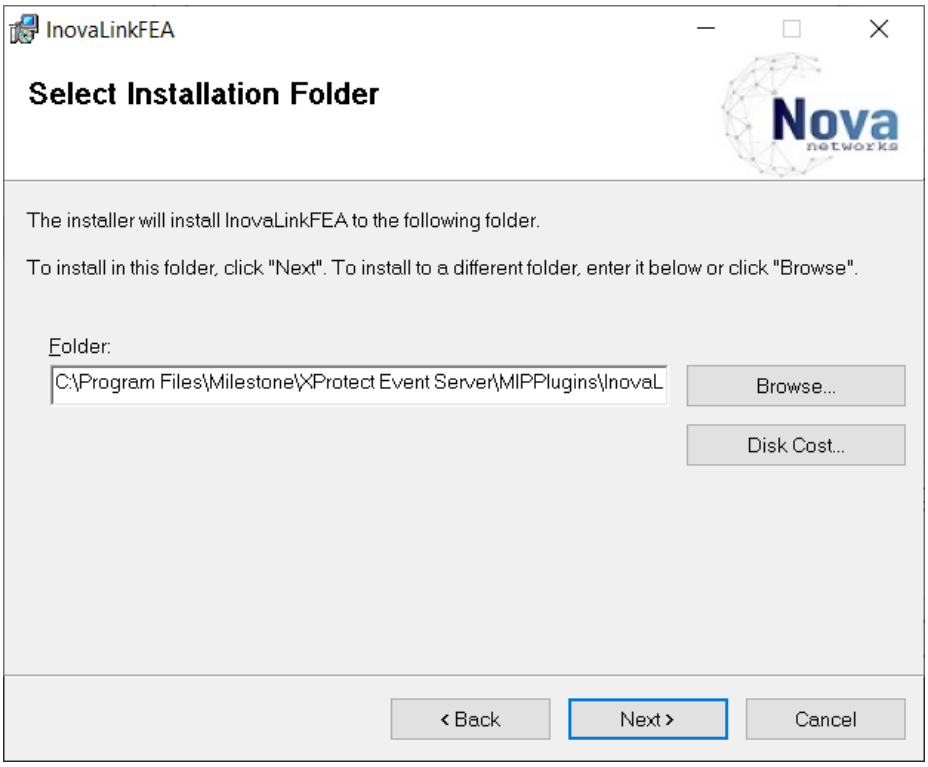
## Install the Service Plug-in in the Event Server

1. Double-click the executable program file of *InovaLinkFEA-server-plugin* to enter the welcome page of the Setup Wizard.



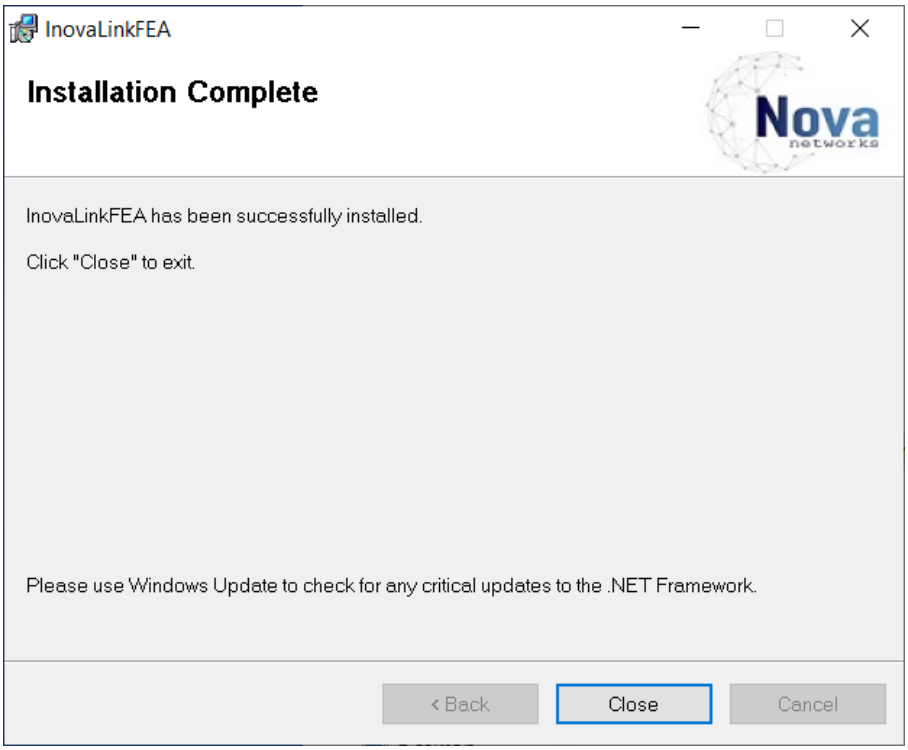

2. Click **Next** to start the setup wizard.

3. The plug-in must be installed in the corresponding Milestone MIPPlugins folder. The default path is “C:\Program Files\Milestone\XProtect Event Server\MIPPlugins”. Click **Change** to select a proper directory as the installation location.




4. Optional: Click **Back** to review or change any of the installation settings.

5. Click **Next** to start the installation. After starting installation, a progress bar will appear to show the installation status. Click **Cancel** to interrupt the installation process if needed.




6. Click **Finish** to complete the installation after the progress is ended.

# Configuration

## OPTIMA Box Token

Accessing the OPTIMA Box with a valid account, enables the user to generate a third-party system connection. In this case, the program will be accessing the OPTIMA Box via the API.

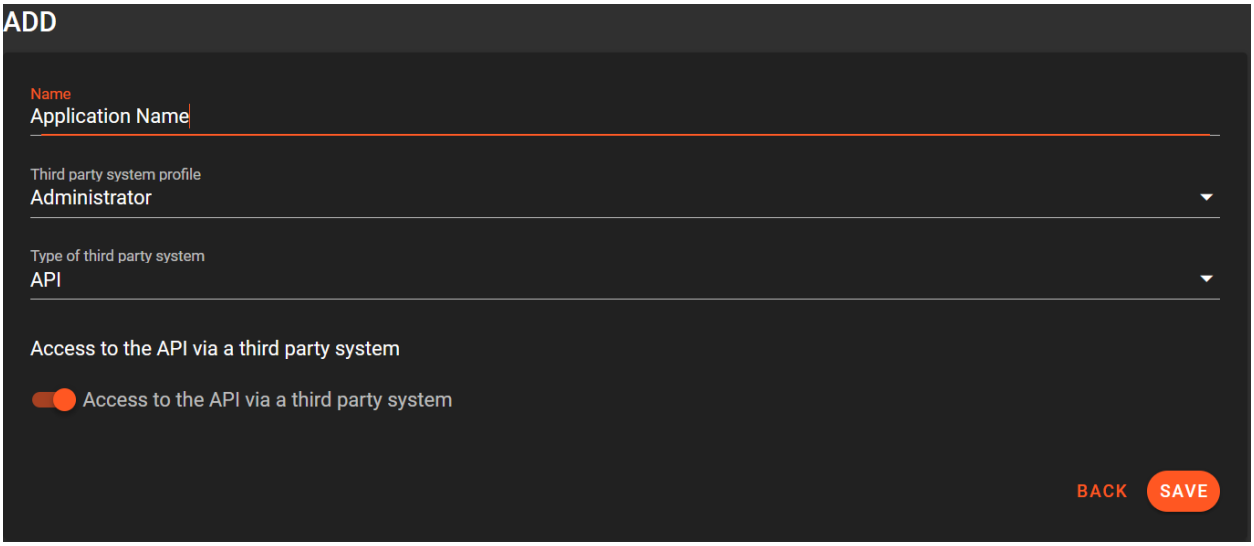



Figure 1 - Third-Party Configuration for OPTIMA Box

Clicking in *Save* shows another menu, where the user obtains information about the security token. There is no need to generate multiple tokens for an OPTIMA Box, although the communication between XProtect and the OPTIMA Box will work with any of the security tokens generated.

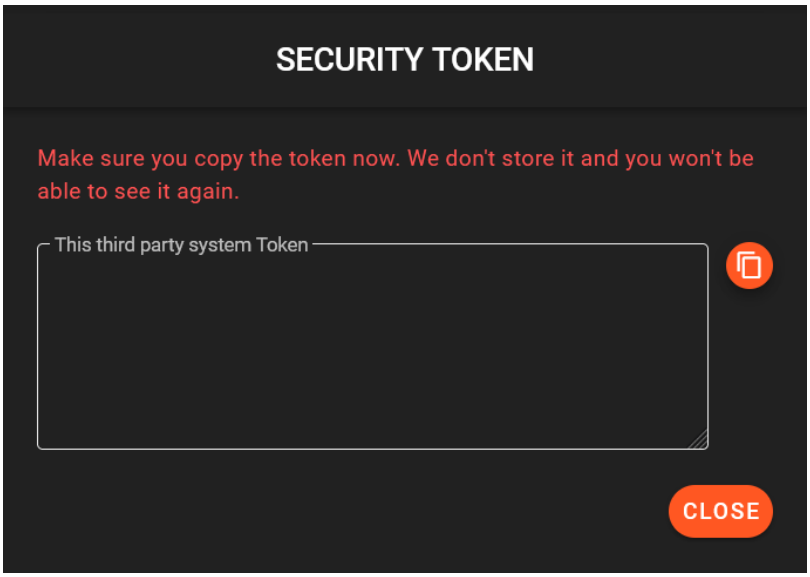



Figure 2 - OPTIMA Box Security Token Generation

Every time any changes are made to the configuration in the XProtect System, the administrator must copy and paste the token in the User Control, in order to update the information between the program and the OPTIMA Box.

## Management Client

In the Management Client the system administrator establishes a connection with an OPTIMA Box. Upon successful connection, the elements managed by the OPTIMA Box are added to the Milestone Systems VMS. The system administrator creates a new OPTIMA Box connection by creating a new OPTIMA Box Item in the InovaLink FEA plug-in node in the MIP Plug-ins.

The system administrator is only able to create and edit OPTIMA Box Items, as the hability to create new Items is not enabled for the Liguard and Reader elements. The system administrator can, however, delete Liguard and Reader Items that should not figure in the Milestone XProtect VMS.

Once an OPTIMA Box Item is created, a user control menu appears, where the administrator fills in the **OPTIMA Box IP address**, the **third-party connection token** issued by the OPTIMA Box to validate the connection and selects **if HTTPS protocol is enabled**, as well as the **communication port**.

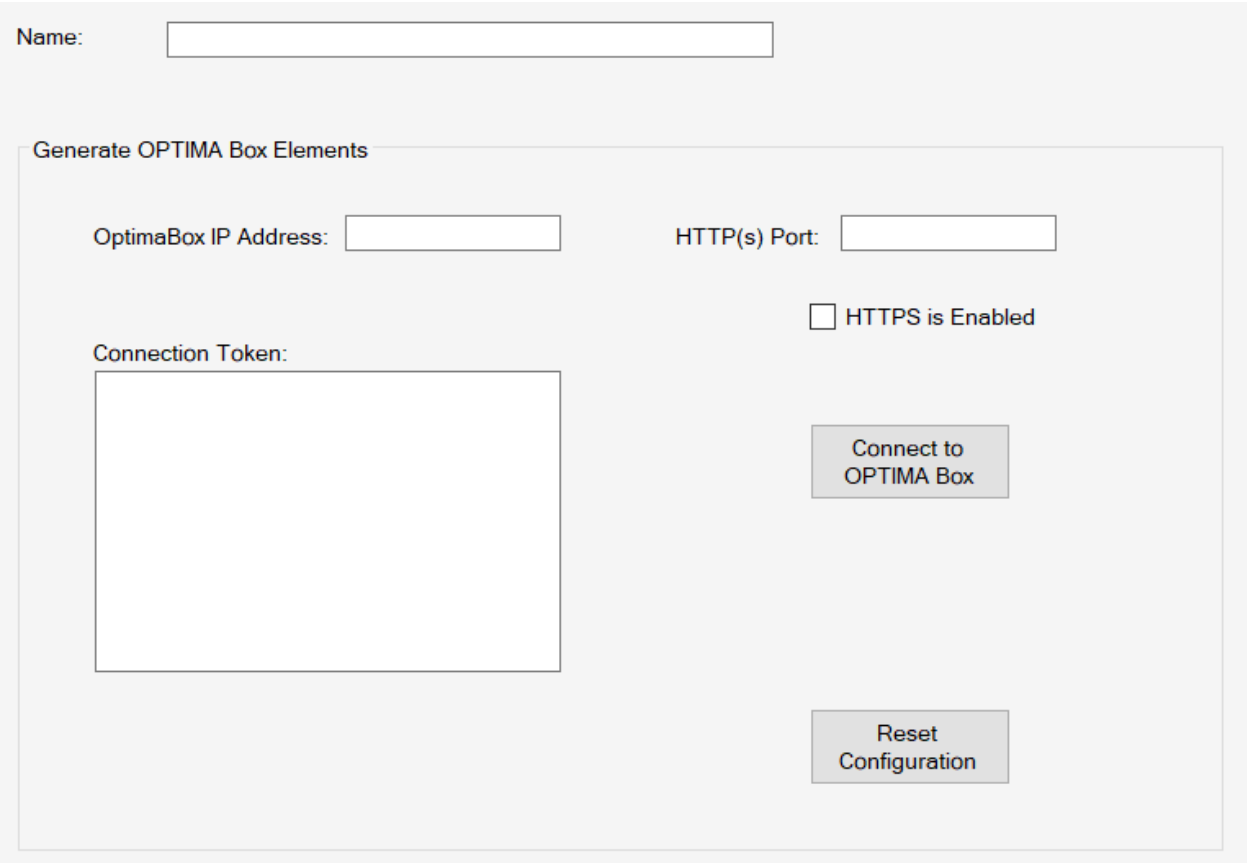



Figure 3 - InovaLink FEA User Control Menu

## User control functions

There are two buttons: *Connect to OPTIMA Box* and *Reset Configuration*.

By clicking *Connect to OPTIMA Box*, if all the information previously specified is correctly inserted, it connects to the OPTIMA Box and fetches the elements in it to make them available in the Milestone XProtect VMS. This button can also be used to update any changes done in the OPTIMA Box after having already created elements in the Milestone XProtect VMS.

The button *Reset Configuration* is to be used strictly in the case that a malfunction happens creating the elements, or there is no longer need to connect to the OPTIMA Box, and the system administrator needs to delete the Item from the database. Any alarm definition will in turn cease to have the associated elements and instead will show *Unknown Item*.

**Every time a system administrator proceeds to make a change in the configuration of the OPTIMA Box connection in the Management Client, it needs to insert the OPTIMA Box third-party connection token to validate the action completely.**

**After any changes are made to the plug-in configuration in the Management Client, please restart the Event Server for it to take into account the changes made.**

# Alarm Definitions

In the *Alarm Definitions* the system administrator is able to select in the *Trigger* menu the Events that cause the alarm. There are three different elements that produce events: the OPTIMA Box, connected Liguards and connected Readers. As it will be further explained, the system administrator can define what degree of specificity the alarms hold by selecting which events will be launched.

## OPTIMA Box Events

The system administrator can select a triggering event for when the connection is lost to the OPTIMA Box. The “Source” can be any of the existing and valid OPTIMA Box connections. This is the only event associated with the OPTIMA Box element.

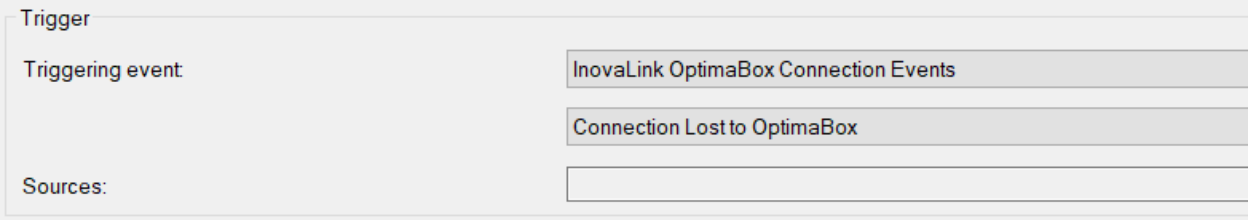



Figure 4 - Selection of triggering event for the OPTIMA Box

## Liguard Events

Liguard Events have two different types of events: “Single” and “All”. The system administrator can therefore select to only launch alarms for a specific event launched by a Liguard or to launch alarms for any event produced by a certain Liguard. In the Sources menu the administrator selects which elements from the OPTIMA Box are responsible for the selected event.

Selecting a specific alarm means that only that alarm from the Liguard will be notified in the Smart Client.

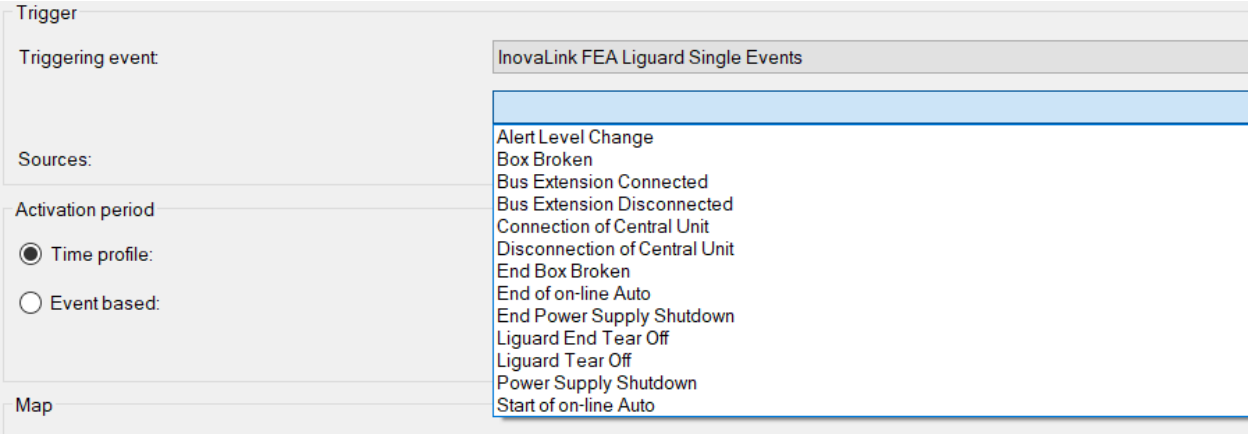



Figure 5 - Liguard Single Events Menu

Otherwise, selecting all events will notify the Smart Client user of any event produced by the Liguard.

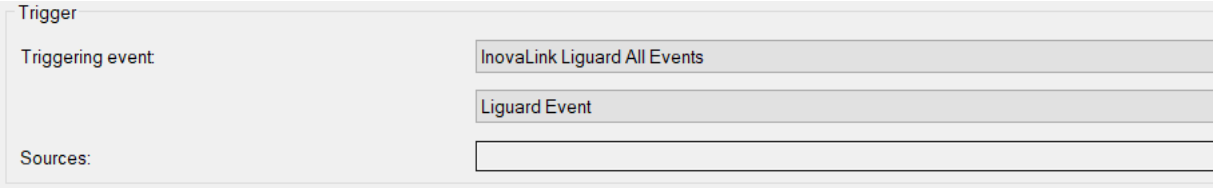



Figure 6 - Liguard All Events Menu

## Reader Events

As with the Liguard Events, Reader Events also have the “Single” and “All” events. As there is a large quantity of Events associated with the Readers, it is recommended to select specific events for the alarms including Readers.

Selecting a specific alarm means that only that alarm from the Reader will be notified in the Smart Client.

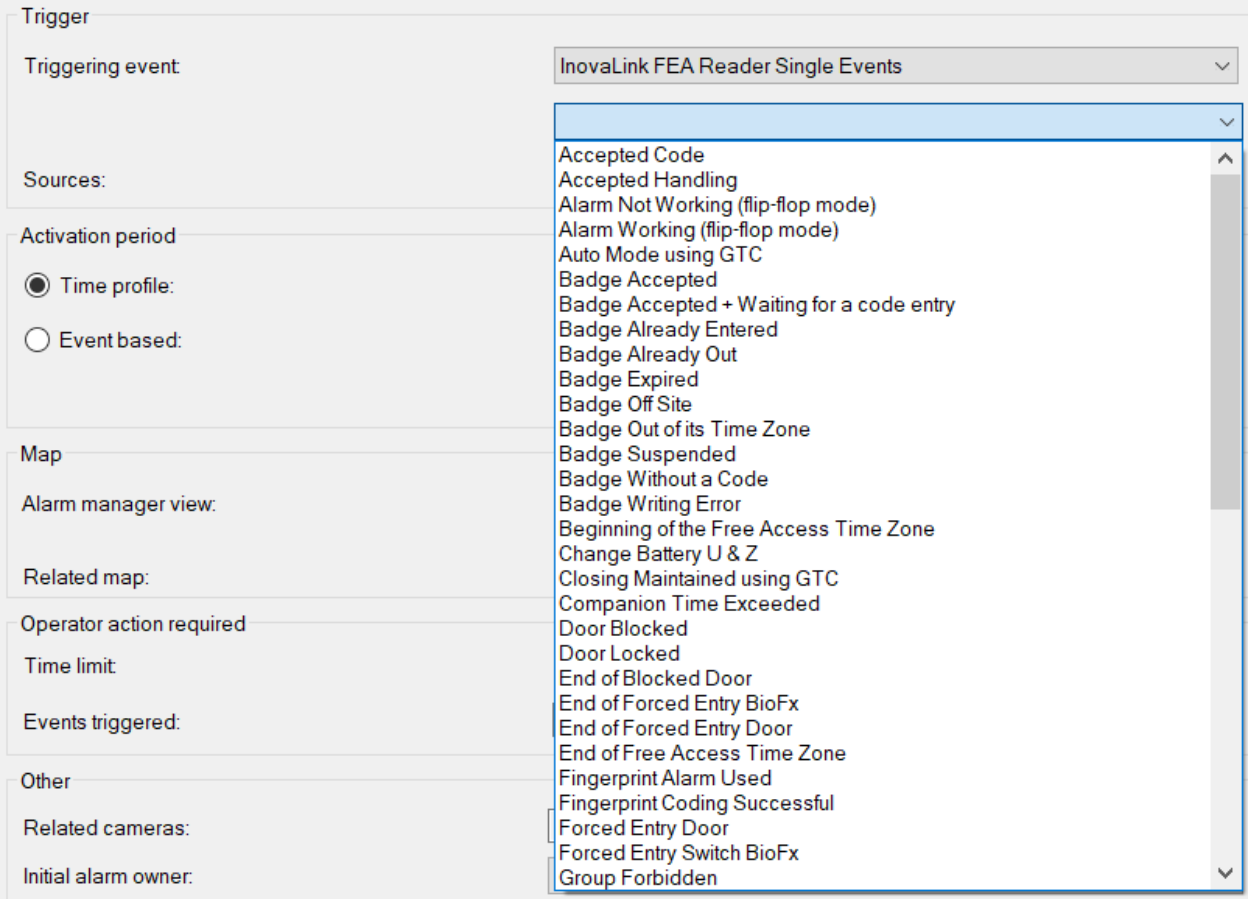



Figure 7 - Reader Single Events Menu

Otherwise, selecting all events will notify the Smart Client user of any event produced by the Reader.

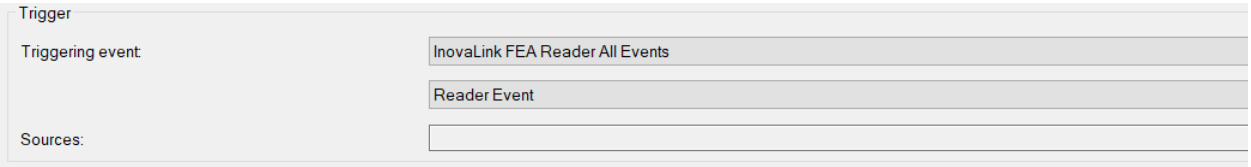



Figure 8 - Reader All Events Menu

## Smart Client Alarm View

Using the Alarm Manager plug-in from Milestone Systems a user can check the alarm notifications. Here the user can handle the alarms that the system administrator has defined.

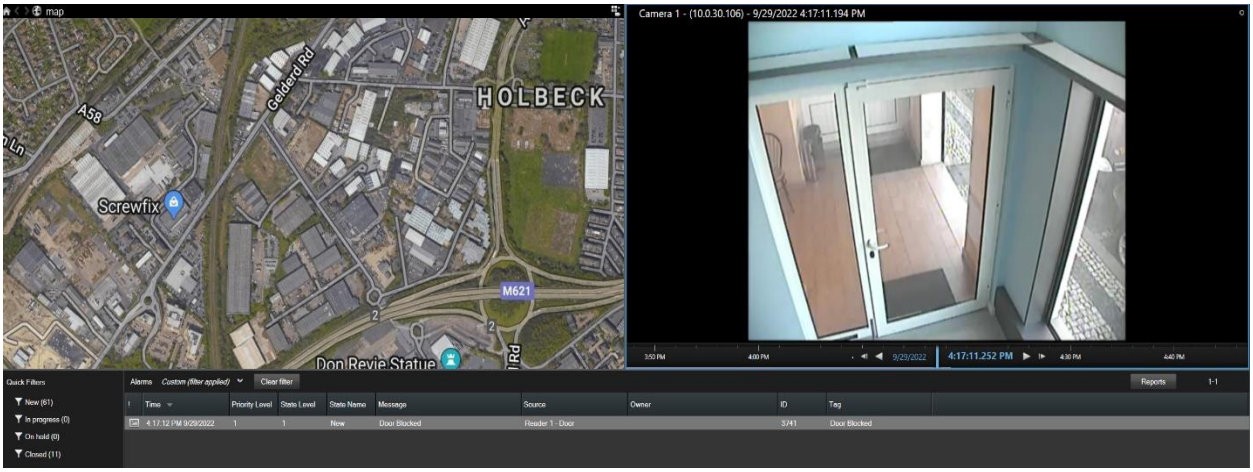



Figure 9 - Alarm Manager User Interface, an event is selected and the corresponding map and camera are displayed

In the Alarm Manager, when double-clicking in an alarm, a new window pops up with more information about the alarm.

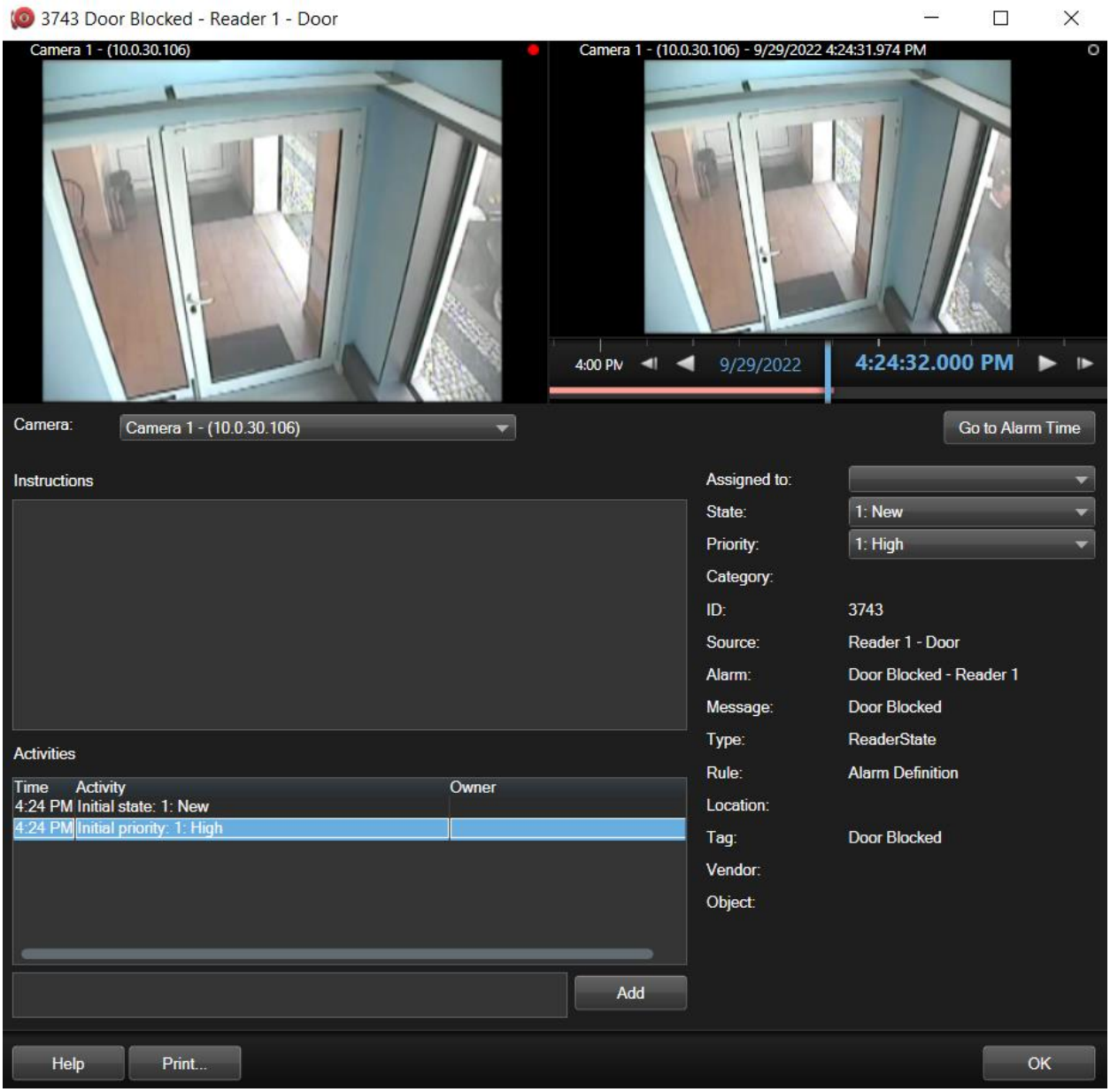



Figure 10 - Selected alarm complete information

It is advised that the system administrator add the “Tag” column to the *Selected Columns* in the Alarm List Configuration found in the Alarm Data Settings in the Management Client. This gives more information about the alarm, especially when capturing all events occurring in a given Reader or Liguard.

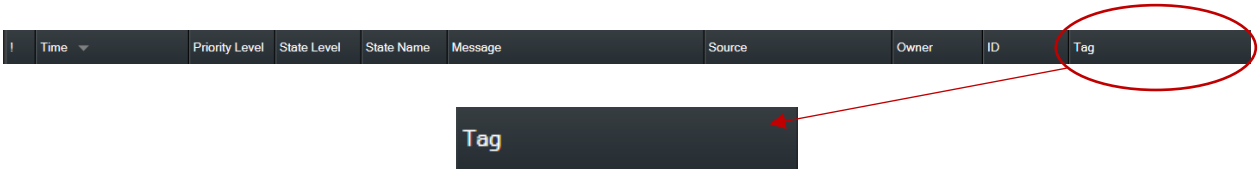



Figure 11 - Tag Column in the Alarm Manager Menu

# Appendix A. Reader Events

**Table 1 - Reader Events Table**

| READER EVENTS | |
|---|---|
| Accepted Code | Left key press SOWIT |
| Accepted handling | License plate recognized, awaiting for a badge |
| Alarm not working (flip-flop mode) | Maximum number of allowed passages reached |
| Alarm working (flip-flop mode) | Mistake in badge format |
| Auto mode using GTC | No Battery |
| Badge accepted | No condition |
| Badge accepted + Waiting for a code entry | No vehicle was detected |
| Badge already entered | Opening maintained using GTC |
| Badge already out | Opening using GTC |
| Badge expired | Prohibited |
| Badge off site | Push button opening |
| Badge out of its time zone | Right key press SOWIT |
| Badge suspended | Sensor obstructed |
| Badge without a code | Setting alarm on/off |
| Badge writing error | Stolen badge |
| Beginning of the free access time zone | Time out for code entry |
| Change battery U & Z | Transit time exceeded |
| Closing maintained using GTC | Unknown plate |
| Companion time exceeded | Unrecognized badge |
| Door blocked | User without fingerprint |
| Door locked | Waiting for a fingerprint |
| End of blocked door | Waiting for a handling |
| End of forced entry BioFx | Weak battery |
| End of forced entry Door | Wrong code |
| End of free access time zone | Wrong fingerprint |
| Fingerprint alarm used | Wrong handling |
| Fingerprint coding successful | Wrong reseller badge |
| Forced entry Door | |
| Forced entry switch BioFx | |
| Group forbidden | |
| Incorrect badge | |
| Invalid door for this badge | |
| Keypad locked | |
| Keypad no longer locked | |

# Appendix B. Liguard Events

**Table 2 - Liguard Events Table**

| LIGUARD EVENTS | |
|---|---|
| Alert level change | End of on-line Auto |
| Box Broken | End power supply shut down |
| Bus extension connected | Liguard End Tear-Off |
| Bus extension disconnected | Liguard Tear-Off |
| Connection of Central Unit | Power supply shut down |
| Disconnection of Central Unit | Start of on-line Auto |
| End Box Broken | |


contact@novanetworks.tech

www.novanetworks.tech