BTX™

"Bridge to XProtect"

for

Milestone XProtect

Integration with

Third-party Systems

User Guide

"Enable your video surveillance operator to monitor and control your security system!"

January 2025

App-Techs Corp.
505 Willow Lane
Lancaster, PA 17601 USA

Telephone: 717-735-0848
Fax: 717-735-0851
Web: www.app-techs.com
Email: sales@app-techs.com

Summary

This document provides a basic overview as well as installation and operating instructions for the BTX™ software package.

Table of Contents

1. System Overview

BTX™ (Bridge to Milestone XProtect) is a communication bridge / middleware that transforms events and alarms from third-party systems into a variety of actions in Milestone XProtect.

BTX works by receiving real-time event and alarm data streams from third-party systems such as video analytics, access control, sensors, security and building automation equipment, SIP phone systems, and software applications. It receives event data in a variety of protocols and converts this data into a variety of actions in XProtect.

Incoming data is received, transposed, and analyzed. Then, based on user-defined settings, filters, and schedules, BTX transforms this data into XProtect to ...

- Generate Alarms with Video Bookmarks.
- Generate Events with Video Bookmarks.
- Debounce, i.e. filter or ignore, repetitive or over-active alarms.
- Schedule alarm time-of-day intervals.
- Tag Searchable Bookmarks.
- Trigger User-defined Events. (for Text and Email Notifications, Relays and Digital Outputs, and other functions)
- Trigger Smart Client Matrix Views.
- Trigger PTZ Commands. (for any camera, even for those from which a given event did not originate)
- Relay analytics snapshots and other relevant metadata into the XProtect Smart Client.
- Rename third-party alarms to convey site-specific, situational specific details to the Smart Client operator.

All of this functionality is accomplished without the use of XProtect plug-ins, and without requiring a technician to define an elaborate set of XProtect generic events, rules, and alarm definitions in the XProtect Management Client.

With BTX, it is possible integrate dozens, or hundreds, of third-party devices with XProtect in just a few minutes.

The simplicity and utility of BTX improves *real-time* situational awareness by making third-party events and alarms *pop* in Milestone XProtect, while also capturing and reporting event metadata data to better inform security operators.

BTX integrates with over 30+ sensors, devices, and systems. One instance of BTX can simultaneously receive and manage alarms from any number of systems of devices. There is no limit to the number of devices one can integrate with BTX, and no additional licensing is required to integrate with any additional third-party sub-system.

1.1. System Requirements

The BTX system requirements are conventional and lightweight.

- Windows 10, 11. **Windows 7 version available for older versions of XProtect.*
- Microsoft .net framework 4.8.0 or higher.
- BTX is lightweight software - low disk usage / low RAM consumption / minimal CPU usage.
    - 350MB disk space.
    - 100MB RAM.
- Typically install on the same server as the Milestone XProtect Management Service.
- Run as desktop application during configuration phase, then switch to Windows service version for production.
- Supplemental Upgrade Protection (SUP) available to keep BTX current with the latest version releases for XProtect.

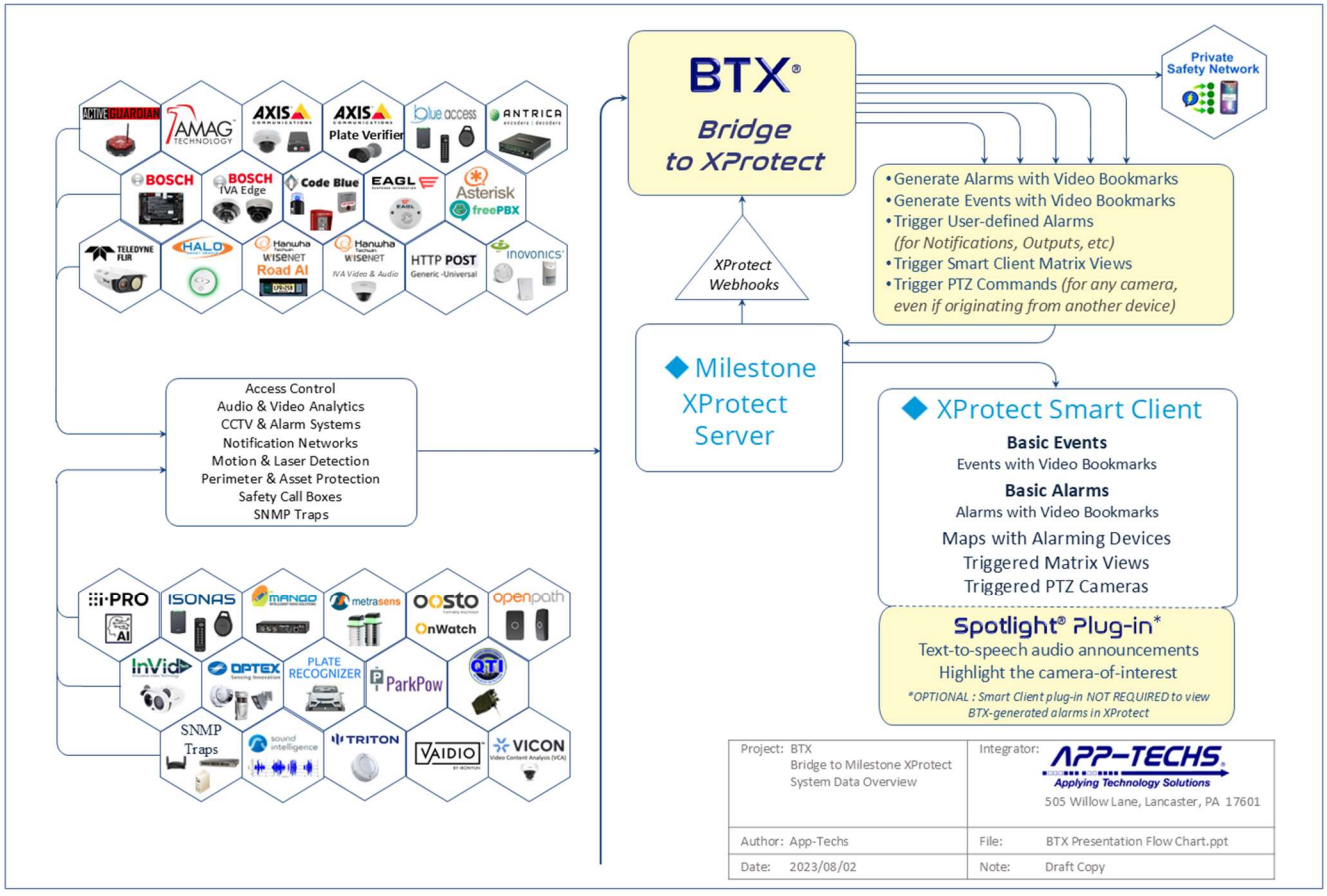
1.2. BTX Features

BTX provides the following features to transform third-party alarms into* action* in Milestone XProtect.

- **RECEIVE** third-party data in a variety of formats, including TCP, HTTP Post, UDP, Serial, SNMP Traps, and other protocols.
- **FILTER** third-party alarms by alarm keyword and/or device of origin
- **ASSOCIATE** XProtect cameras / devices to specific third-party devices.
- **GENERATE** XProtect events and / or alarm records.
- **DEBOUNCE** frequent or over-active third-party alarm messages, reducing false-positives and operator alarm fatigue.
- **SEARCH** third-party events and alarms as XProtect Bookmarks.
- **SCHEDULE** alarms to be active at different times of the day.
- **TRIGGER** XProtect user-defined events (for text & email notifications, relays and digital outputs, Smart Wall commands, etc.)
- **CALL UP** Smart Client matrix views.
- **ACTIVATE** PTZ Commands (for any camera, even for those from which a given event did not originate).
- **RENAME** XProtect event / alarm messages to by easily understood by the Smart Client operator.
- **DISPLAY** third-party video analytics snapshots directly in the XProtect Smart Client.
- **STORE** relevant third-party data directly in the XProtect alarm record database
- **MONITOR** device /sensor status with App-Tech's Situational Awareness plug-in.
- **INTEGRATE** with other systems, such as the mass notification and incident management systems

2. Data Flow

2.1. Overview



3. Installation

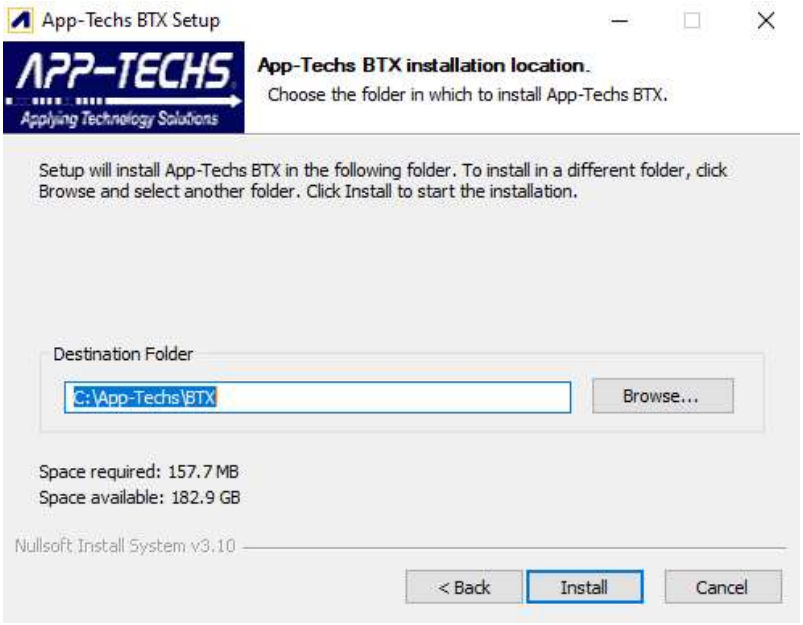
3.1. BTX Server

The BTX Server runs on any server which has network connectivity with XProtect and the third-party system(s) of interest.

It is typically installed on the same server as the main XProtect services.

3.2. Core Application

Run the installer for the BTX core application. Choose the installation folder.

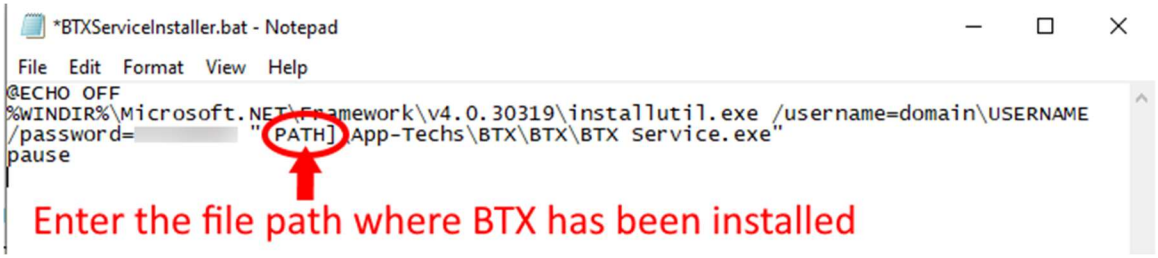


3.3. Windows Service Installation

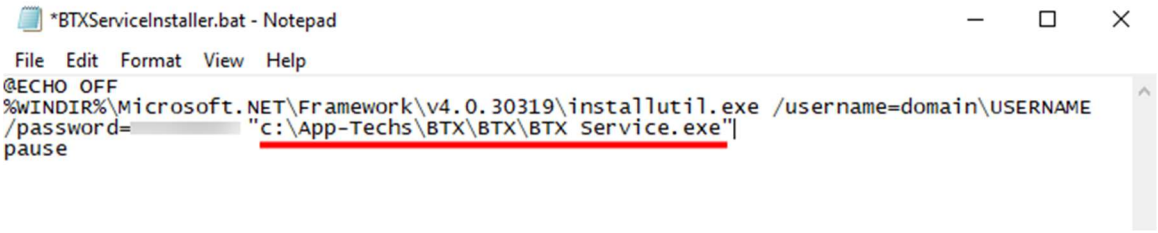
Navigate to the location of the directory where BTX was installed. Locate the file "BTXServiceInstaller.bat" in the BTX/BTX folder

`Ex. C:\App-Techs\BTX\BTX\BTXServiceInstaller.bat`

Open the \BTXServiceInstaller.bat file in notepad. Edit the file path to indicate the installation location:

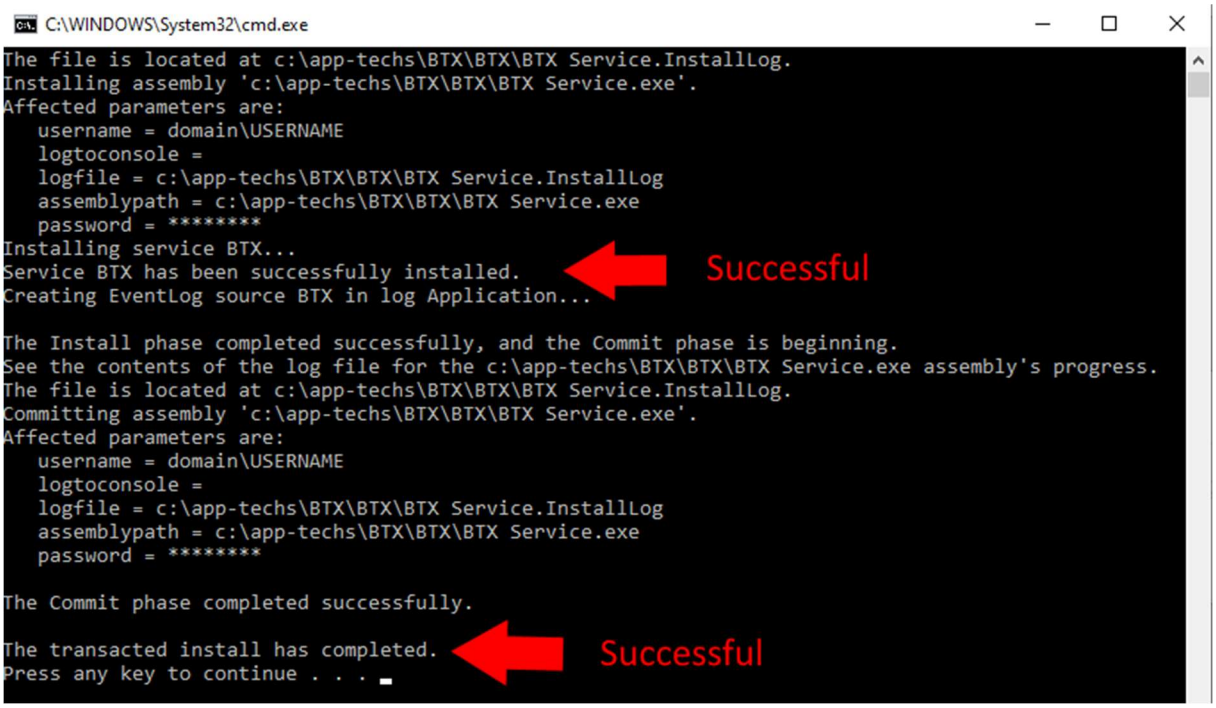


Below is an example:



Save the file while making sure it remains a *.bat file.

RUN AS ADMIN the `BTXServiceInstaller.bat` batch file.



The BTX Service version is now successfully installed. If errors occur in the service installation process, contact App-Techs support.

4. BTX Initial Setup

4.1. Run BTX.exe as a desktop application

To launch BTX, from the Windows "Start" menu, select …
- All Programs
  - App-Techs Directory
    - BTX (Bridge to XProtect)

Alternatively, the default file path for BTX.exe to is:
`C:\app-techs\BTX\core\BTX.exe`

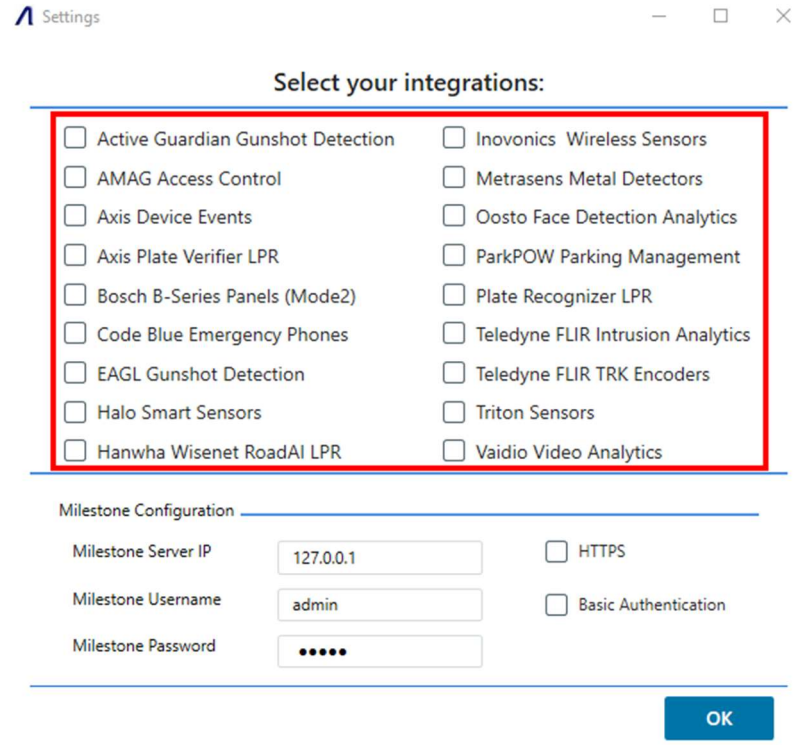
4.2. Activate your BTX License

Upon launch, a license key is required. Enter your license key.

If you do not have a license key, use the "Copy" button to save your MAC address. Contact App-Techs at support@app-techs.com to request a license key. Be sure to include your MAC address with your license request.

4.3. Choose your third-party integration.

Select any number of integrations to pre-load alarm settings into BTX.
NOTE: If the preferred integration is not on this list, proceed without checking any boxes; BTX includes the ability to create custom integration configurations in subsequent sections.

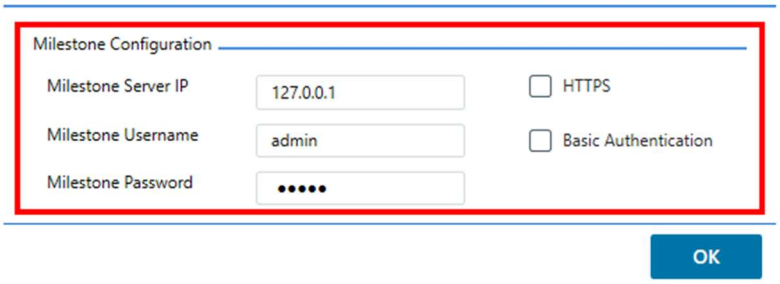


4.4. Enter Milestone XProtect server information.

Enter the correct network and authentication settings to establish a connection with the XProtect Management Server.

The XProtect username used to authenticate must have sufficient privileges in the XProtect Management Client “Roles” menu to view all cameras and to write alarm records. It is strongly recommended to provide this user with admin-level privileges. Either windows users or basic users may be used.

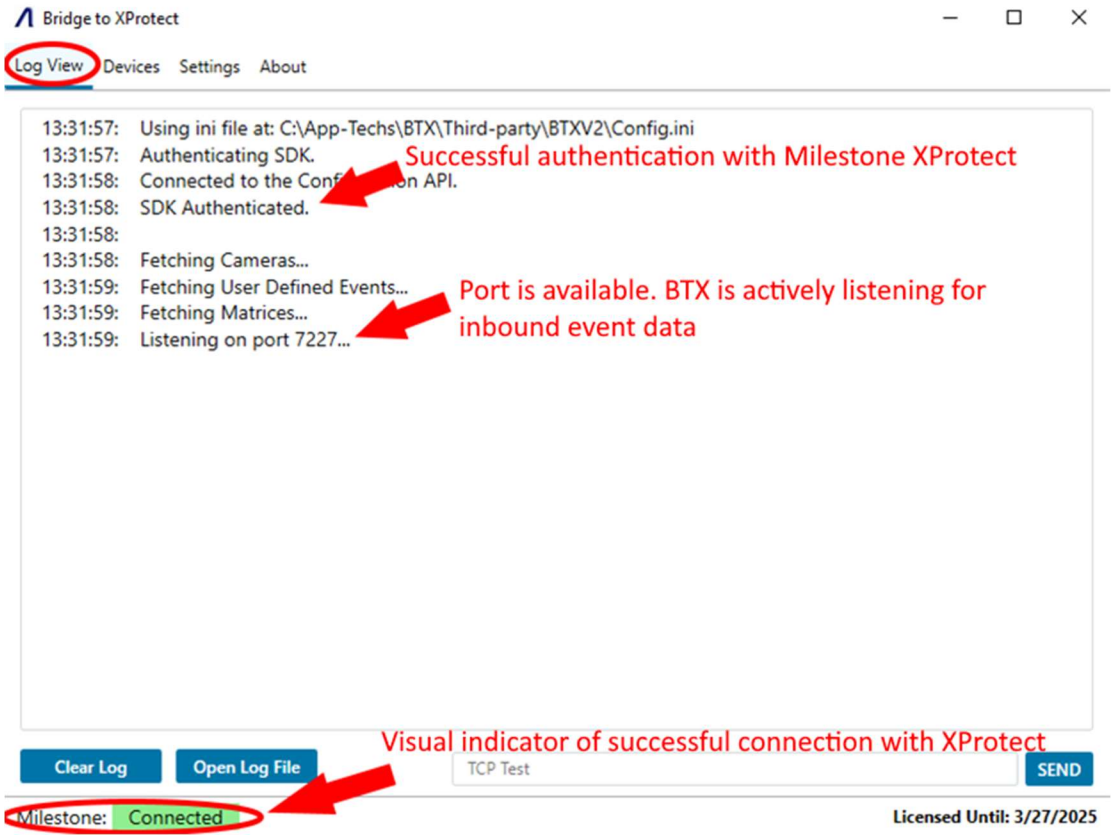
After configuring the connection settings, click the “OK”.



4.4.1. XProtect Authentication Success – “Connected”

If BTX can successfully authenticate with Milestone XProtect, a green “Connected” will appear in the lower-left.

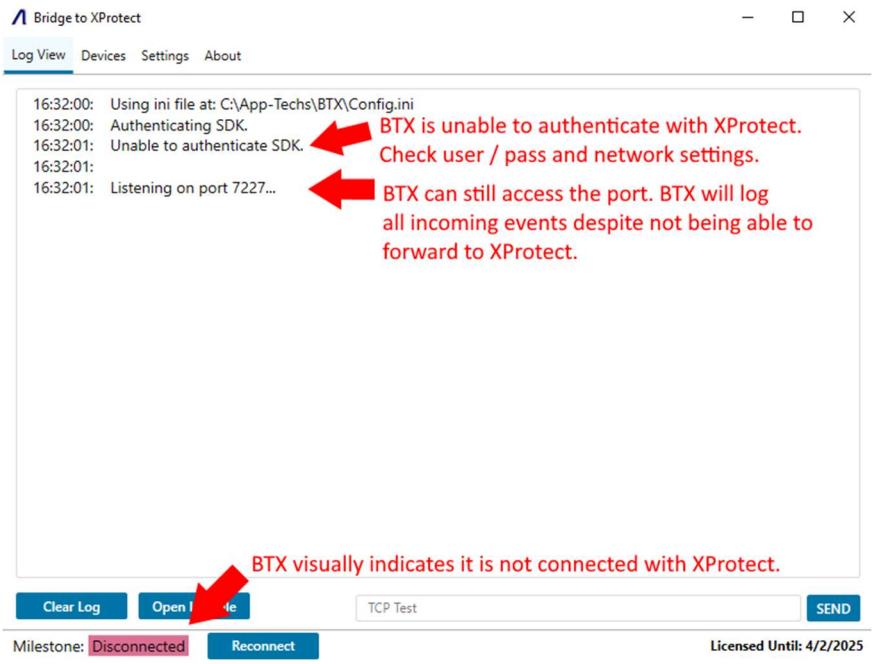
Note the log view provides information on connectivity status.



4.4.2. XProtect Authentication Success – "Disconnected"

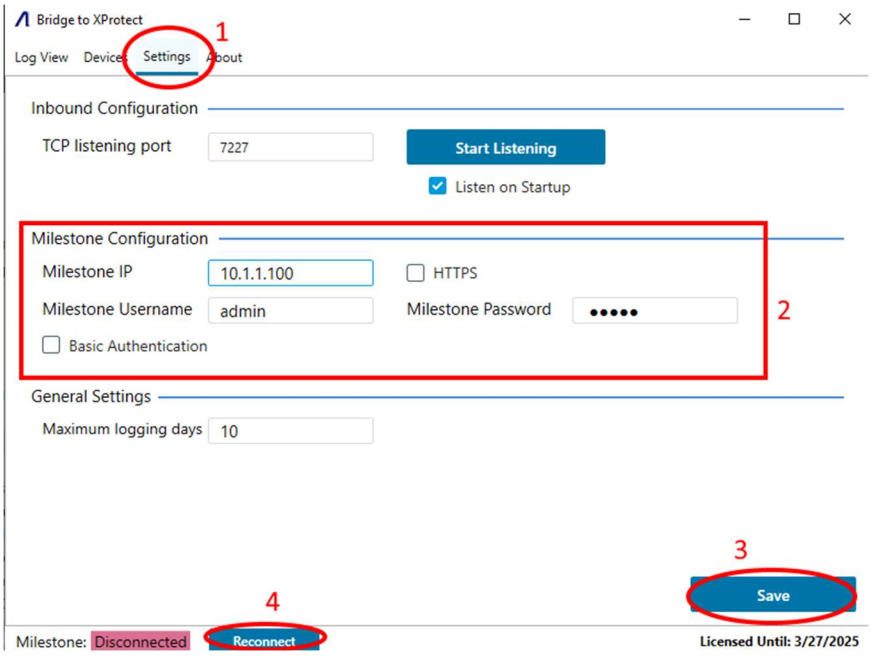
The BTX "Log View" provides information on BTX connectivity status.

If authentication to XProtect was unsuccessful, check your username / password. Verify the user profile has administrative privileges in the XProtect Management Client. Check your network settings to determine if BTX can access the XProtect Management Server over the LAN.

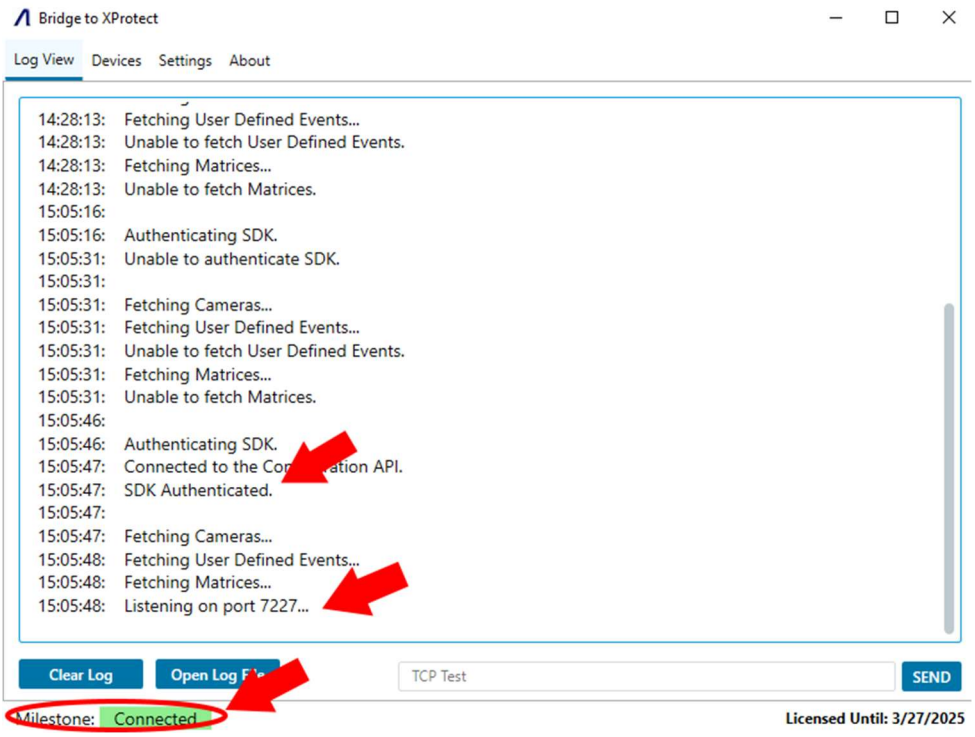


Re-try authenticating with XProtect by going to the BTX "Settings" tab. Re-enter your server address and credentials. Click "Save."

Then press "Reconnect"



The "Log View" will verify if the new server address and / or credentials successfully authenticated with XProtect.



5. BTX Settings

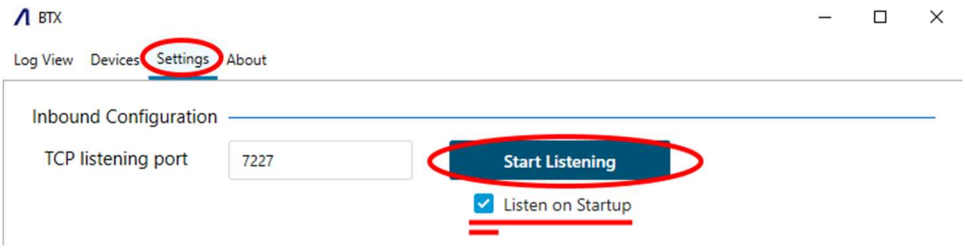
5.1. Inbound Configuration

The BTX core application receives third-party data in the form of TCP messages. Default listening port is 7227. Optionally change the port number if that port is being used by another application.

Check firewall settings to verify the server can accept inbound TCP messages on the listening port (default=7227). It is common for users to create a firewall "inbound rule" to allow traffic sent from third-party devices / systems.

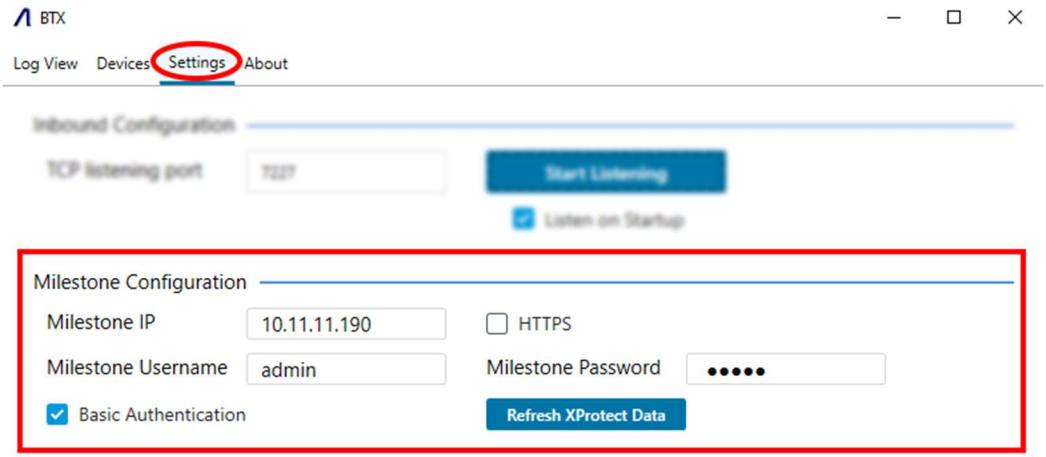
To start actively listening for events from third-party systems, click the "Start Listening" button.

It is strongly recommended to set BTX to "Listen on Startup", as indicated by the checkbox below. When starting / re-starting BTX in the future, BTX will automatically begin listening for incoming alarms, without the need to manually activate BTX.



5.2. Outbound Configuration

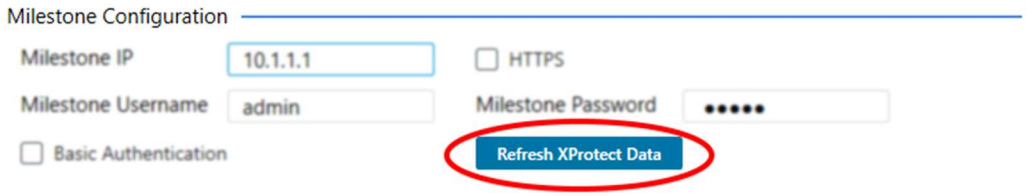
In the event the XProtect network address or user / pass has changed, update your server settings and click the "Save" button/



5.3. Refresh XProtect Data

If changes are made to the XProtect Management Server configuration, such the addition of XProtect cameras, user-defined events, ptz presets, or matrix profiles, the "Refresh XProtect Data" will retrieve these new settings from the server.

NOTE: BTX automatically updates its server information when restarted. The "Refresh XProtect Data" is only required if changes have been made while BTX is open as a desktop application.



6. Basic Alarm Setup – Associate third-party alarms with XProtect Cameras

6.1. Alarm Data Overview

BTX uses three key pieces of information to associate inbound third-party event data to XProtect cameras and devices:

(1) the **date / time** of the event; - i.e, WHEN the event occurred.
(2) the **alarm keyword**; - i.e, WHAT type of event occurred.
(3) the **third-party device name**. - i.e, WHERE the event occurred.

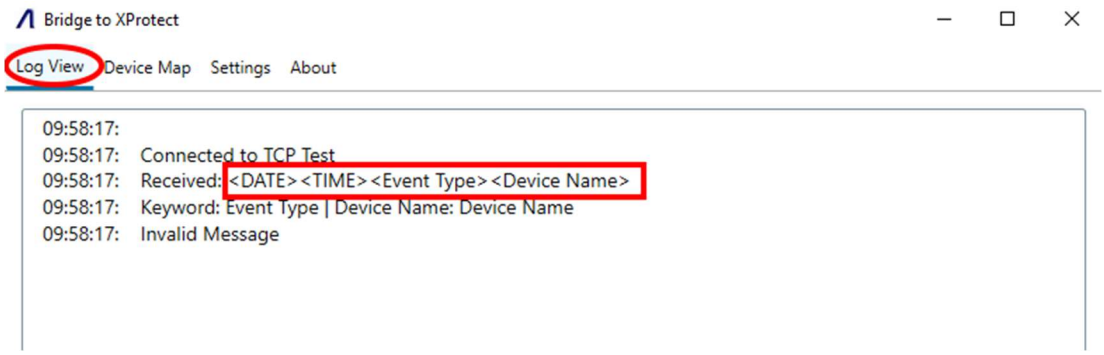
By convention, BTX receives event data via TCP in the following format:

<DATE><TIME><Event Type><Third-party device name>

Parameter #1: <DATE> - Reported date of event.
Parameter #2: <TIME> - Reported time of event.
Parameter #3: <Event Type> - Reported event type.
Parameter #4: <Third-party device name> - Reported device name.
Parameter #5+: <other metadata> - This data may be useful, but is not required to map events in XProtect.

Parameters #1-4 contain all the information needed to map incoming third-party alarms with XProtect. Incoming alarm messages may contain additional parameters, but these function as optional event metadata.

The "Log View" tab displays incoming third-party event data in real-time. The log windows displays the contents of the incoming TCP message as shown below:



When BTX receives an incoming third-party event, the "Log View" tab will assist the user by clearly indicating the **alarm keyword** and **third-party device name** as shown below.

The core function of BTX is to allow the user to define if an **alarm keyword** *AND* **third-party device name** match qualifies as an event-of-interest that merits forwarding to XProtect.

BTX does not automatically forward all alarms to Milestone XProtect. This is by design. Many third-party systems release many different types of event messages, only some that may be of security interest.

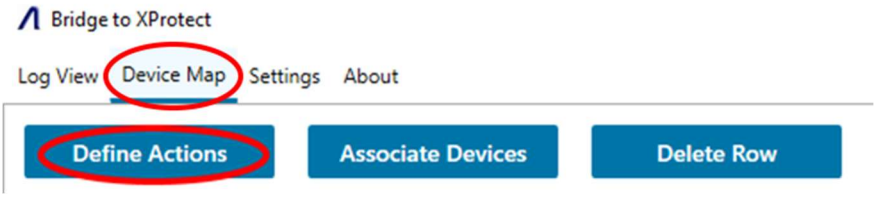
By requiring an **alarm keyword** match, BTX filters incoming messages based on type, identifying events of security interest while logging and ignoring banal or non-security-related events.

Once BTX establishes an **alarm keyword** match, BTX will then need to pair (or associate) the reported **third-party device name** with its XProtect camera counterpart.

When there is a positive match of both **alarm keyword** and the **third-party device name**, BTX will execute the user's preferred actions in XProtect, and thus the third-party event is associated with video in Milestone XProtect.

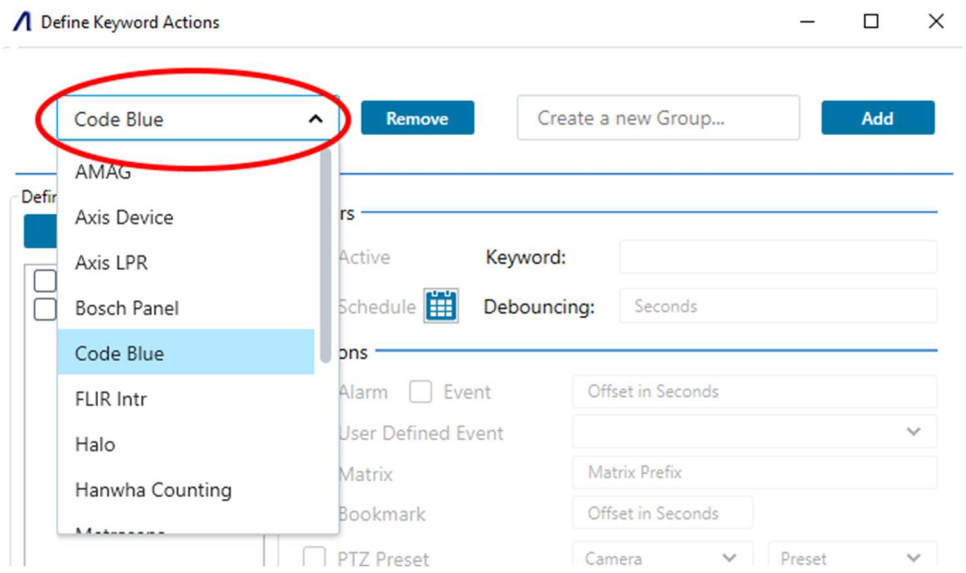
6.2. Define Alarm Actions.

To establish an **alarm keyword** match in XProtect, go to the "Device Map" tab, and click the "Define Actions" button in the top-left corner of the tab.



Select an integration group from the drop-down, or create a new group.

Groups are a way of organizing and saving pre-defined **alarm keyword** templates. This allows the user to rapidly apply alarm settings to many third-party devices without the need to manually configure settings for each device individually.



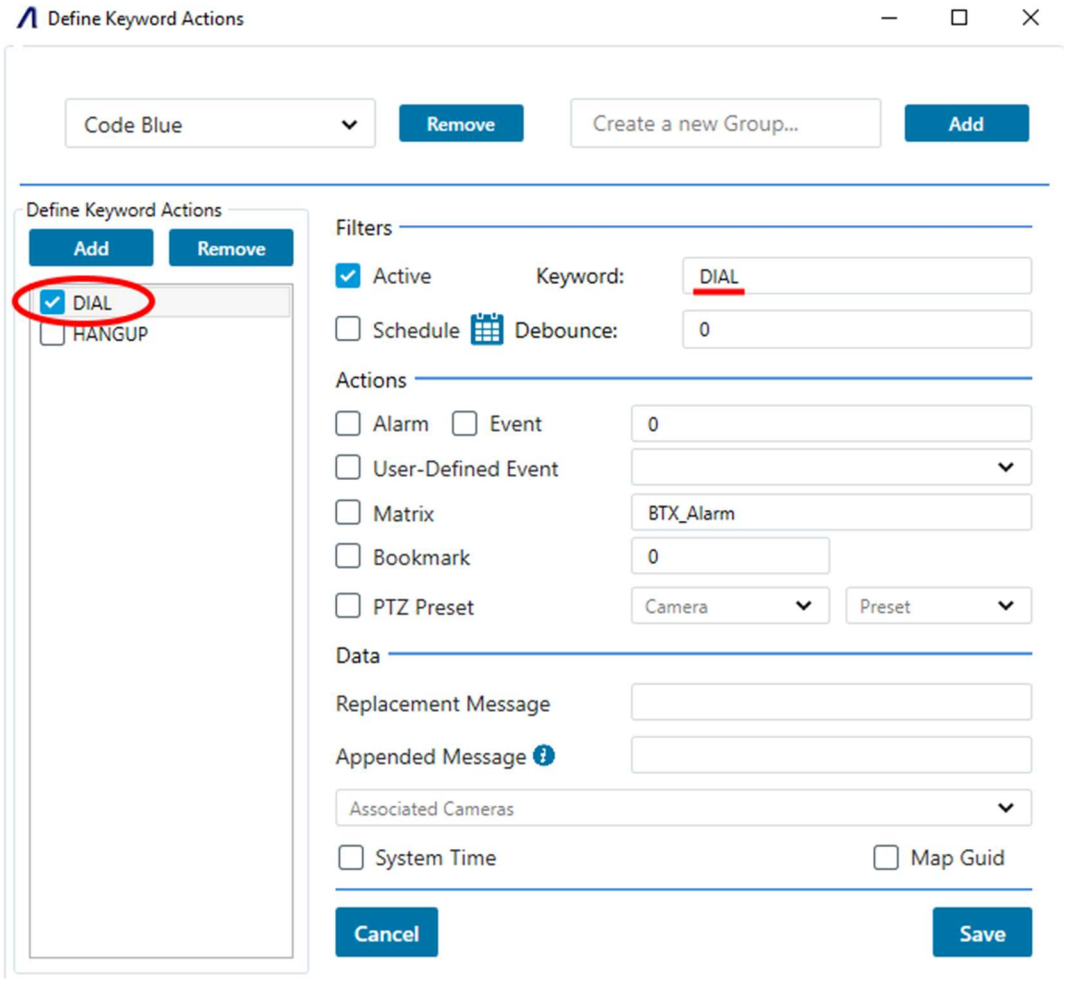
6.3. Define Alarm Keyword Actions.

In the “Define Keyword Actions” section, highlight a pre-configured “Define Keyword Action,” or press “ADD” to create a new one.

On the right-hand side, edit or enter the “Keyword:” field. This field is critical; it is where the user defines if an incoming **alarm keyword** qualifies as event-of-interest to send to XProtect.

By default, the “Keyword” field uses CONTAINS logic to determine an **alarm keyword** match, i.e., if the incoming event message contains “DIAL” [case-sensitive!], then execute the subsequent actions in XProtect.

Check the “Active” checkbox to tell BTX to begin actively listening for this alarm keyword type.



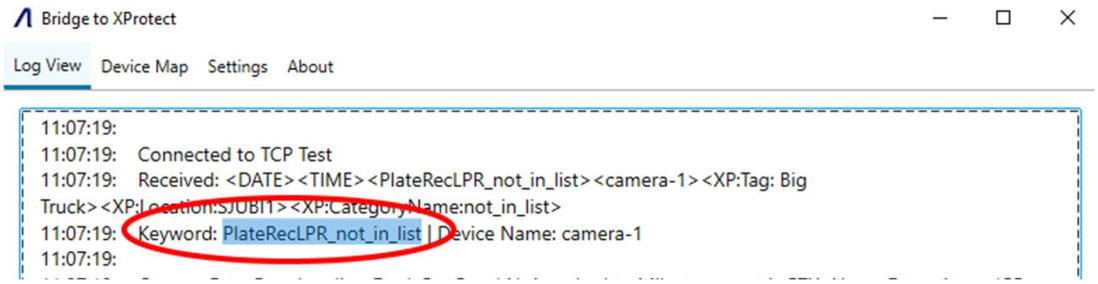
6.3.1. Alarm Keyword Specificity

In the case of many integrations, a partial **alarm keyword** match is all that is required to integrate a third-party event with XProtect.

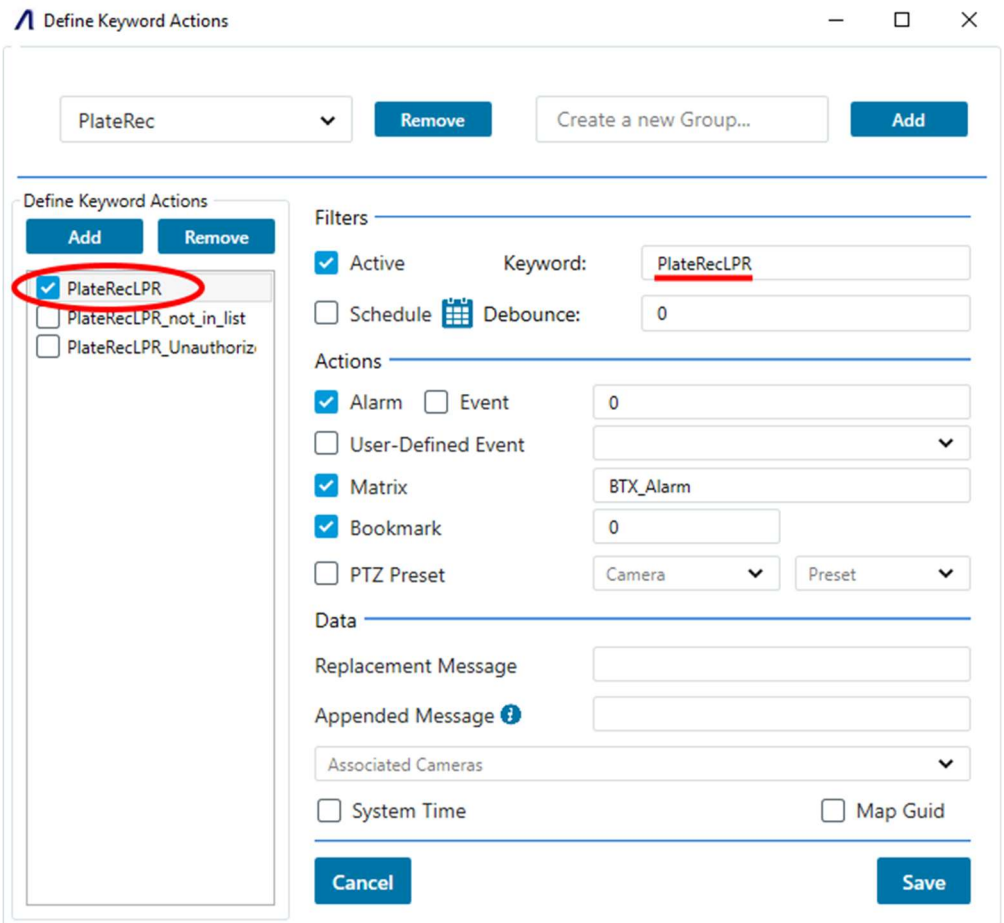
However, in some cases, defining a more specific alarm keyword can provide more granular control over what actions are taken in XProtect.

In the example below, BTX received an incoming third-party event with the **alarm keyword**, "PlateRecLPR_not_in_list."

- The character string "PlateRecLPR" is a generic identifier; "_not_in_list" indicates a specific type of event. In this case, the alarm keyword event indicates that a license plate did not match with a list and is therefore an unknown plate.



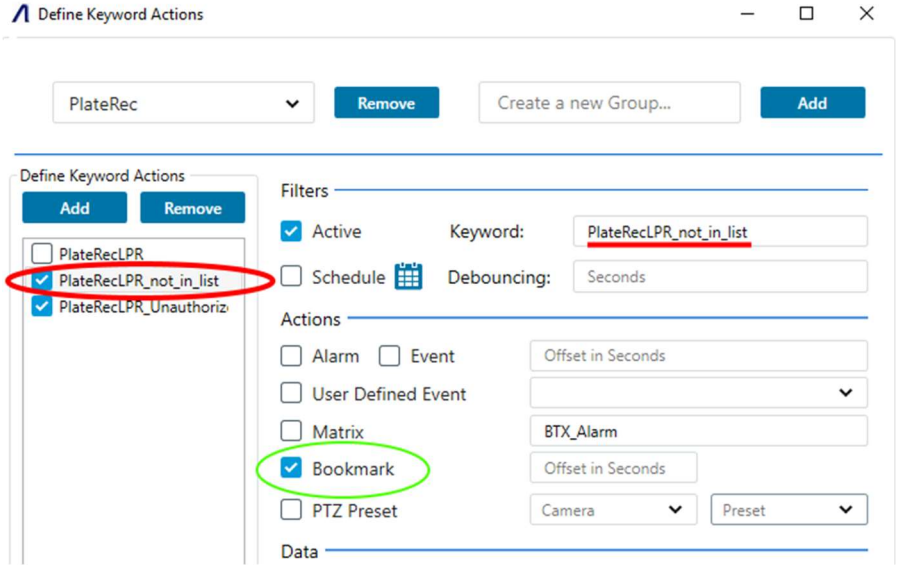
If the aim is to send ALL license plate detections to XProtect, i.e. all alarms keywords that CONTAIN "PlateRecLPR", then defining a partial **alarm keyword** match as "PlateRecLPR" will suffice.



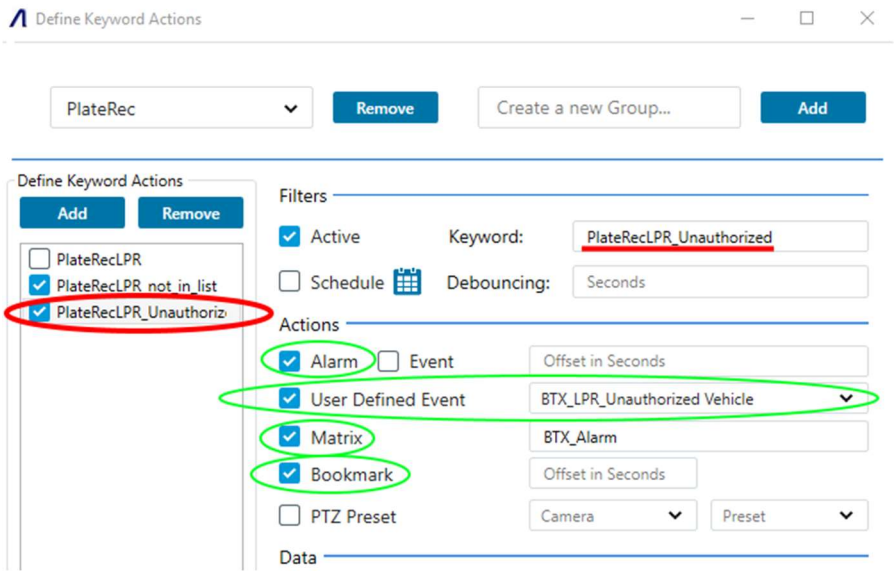
However, if the user prefers certain actions in XProtect based on plate list type, then the BTX user must define a more specific keyword match.

Click the ADD button in the "Define Keyword Actions" section to create a more specific keyword. De-activate or remove the generic "PlateRecLPR" Keyword Action.

Ex: When keyword CONTAINS "PlateRecLPR_not_in_list", only generate a XProtect bookmark.

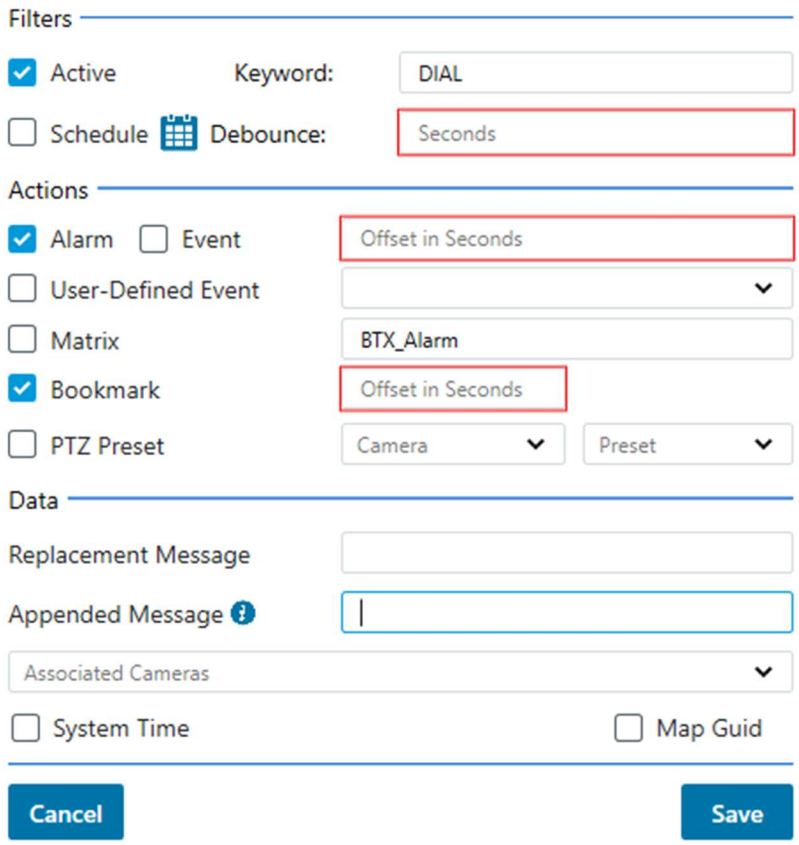


Ex: When keyword CONTAINS "PlateRecLPR_Unauthorized", generate a XProtect alarm + bookmark, trigger the User-defined event "BTX_Alarm_Unauthorized", and fire all live Matrix profiles that start with "BTX_Alarm."



6.4. Choose your preferred actions in Milestone XProtect:

Select the filters and actions to occur when an **alarm keyword** match occurs.



Below is a description of each function can trigger when a keyword match occurs.

Filters:

Keyword [Text field]: A character string match is required to qualify an inbound third-party event as an event-of-interest. This field uses CONTAINS logic. If the alarm keyword being sent by the third-party device CONTAINS a character string match in this field, BTX will execute subsequent actions in XProtect as specified by the user.

Active [Checkbox]: Enables / disables the Keyword Action. If disabled, BTX will not execute the specified actions in Milestone XProtect.

Schedule [Menu]: Specify a time of day/week by which BTX will execute actions in XProtect. This is useful if certain alarms are only of interest at certain times, such as during the evening / night, or during non-work hours.

Debounce [Numeric Text field]: Default = 0 seconds. Ignore repeat alarms over a set time period (in seconds). This is useful if a third-party device reports over-active or repetitive alarms. By ignoring repeat alarms, the user can avoid spamming Milestone with redundant alarm records that are of no security value.

Actions:

Alarm [Checkbox]: Generate a XProtect alarm record.

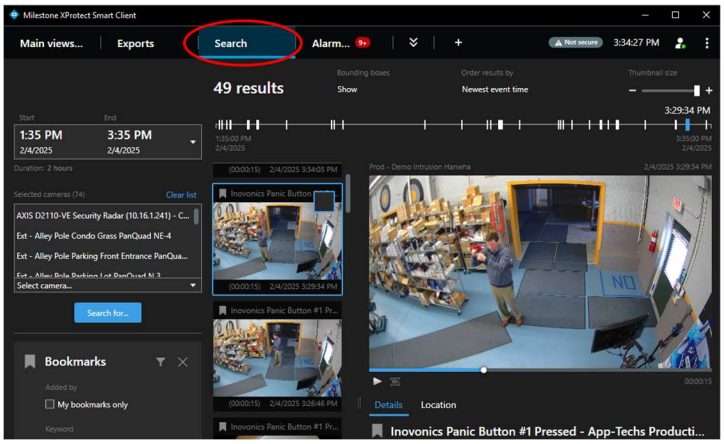
Event [Checkbox]: Generate a XProtect event record.

Offset [Numeric Text field]: Default = 0 seconds. Option to modify the alarm / event record timestamp by *-x* or *+x* seconds to correct a misalignment of third-party devices' reported event time with the actual event time. (Applies to both Alarm and Events)

User-defined Event [Checkbox + dropdown]: Option to trigger a XProtect user-defined event when a keyword match occurs.

Matrix [Checkbox + dropdown]: Option to trigger all XProtect Matrix Profiles that START WITH the text string entered in this field.

Bookmark [Checkbox + Numeric Text Field]: Option to write a searchable bookmark, viewable in the XProtect Smart Client "Search" tab. Includes the option to alter the bookmark time stamp by *-x* or *+x* seconds to correct for any misalignment of third-party devices' reported event time with the actual event time.



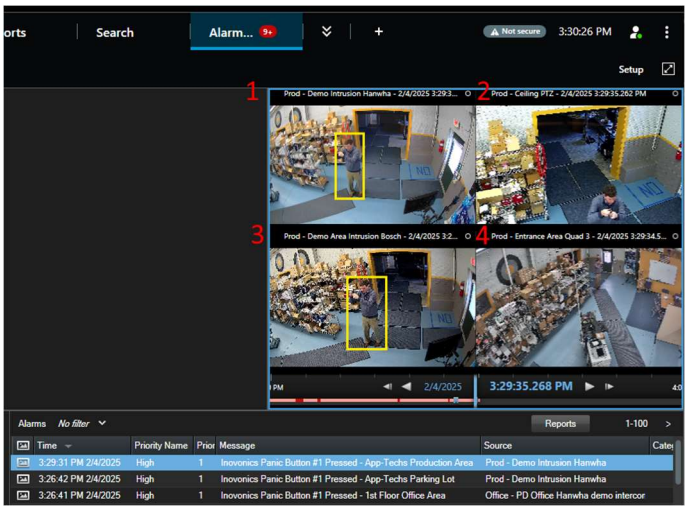
PTZ Preset [Checkbox + dropdown]: Option to trigger a PTZ preset on any PTZ camera when a keyword match occurs.

Data:

Replacement Message [Text field]: When generating a XProtect event / alarm record, BTX replace the alarm keyword reported by the third-party device with the contents of this field.

Appended Message [Text field]: When generating a XProtect event / alarm record, add the contents of this field to the tail of the alarm message.

Associated Cameras [Dropdown]: Optionally choose to associate additional XProtect cameras with a XProtect event or alarm record. This provides additional situational awareness when the primary associated camera lacks sufficient FOV coverage to view with event.



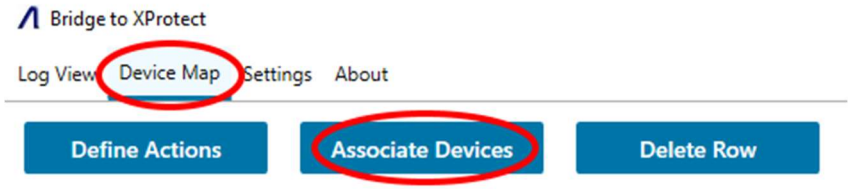
System Time [Checkbox]: Overwrite the event time reported by the device with the XProtect system time. This can be used to compensate for device time drift and other factors.

Map GUID [Checkbox]:: For Vaidio Video Analytics integration only: Automatically use the reported XProtect GUID to associate the device with its XProtect counterpart.

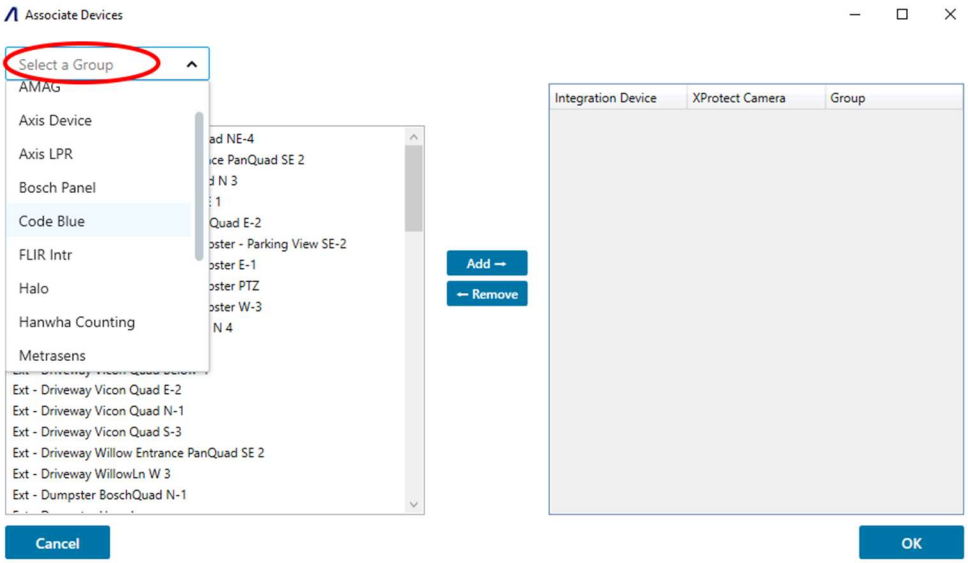
Click "Save" to save your settings for each defined keyword actions.

6.5. Associate Analytic Devices with Milestone Camera(s)

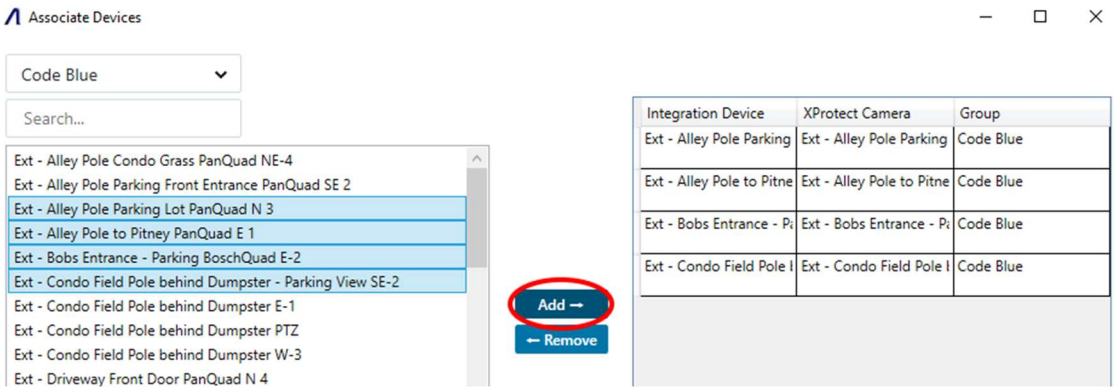
Go to the “Device Map” tab, and click the “Associate Actions” button:



Select an integration group:

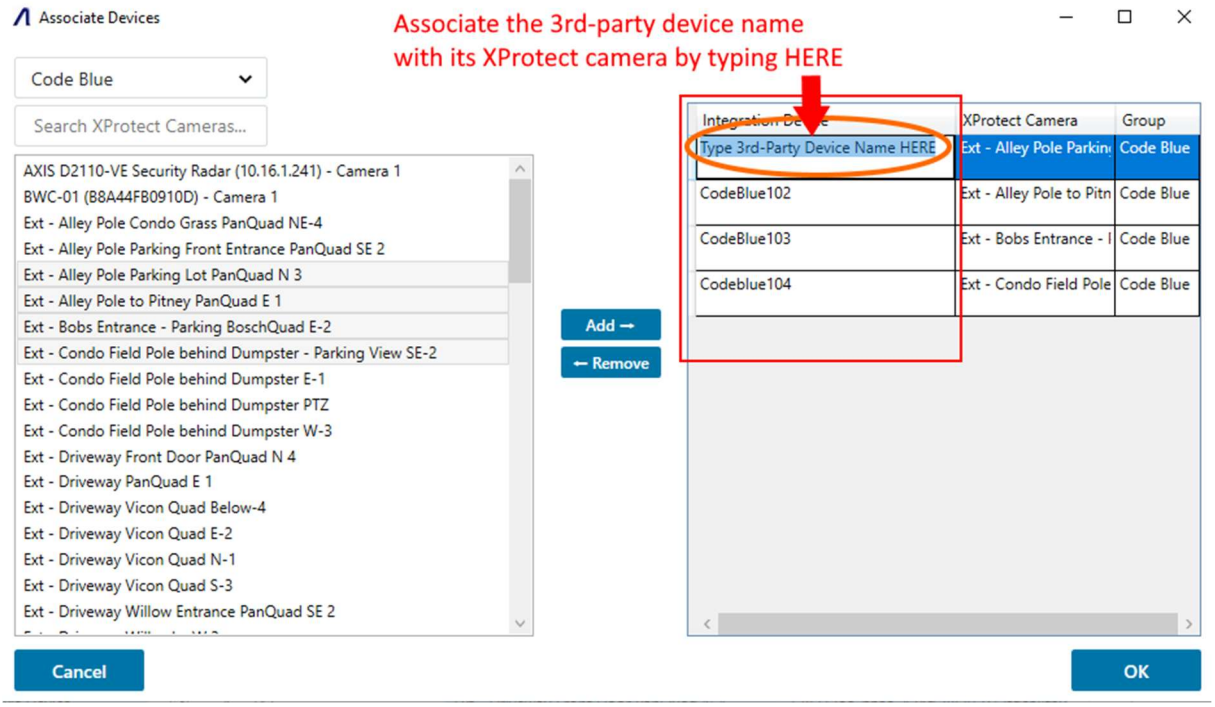


Choose the XProtect cameras from the dropdown you would like to associate with third-party device:.



Click “Add”.

In the “Analytics Device” Column, enter the third-party device name next to its XProtect counterpart.



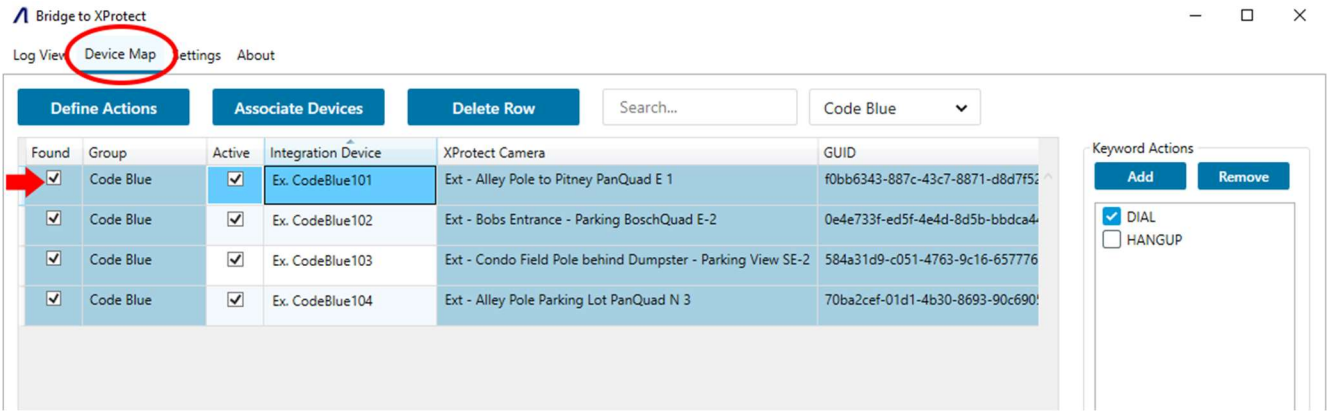
Click “OK” to save settings.

6.6. Configure Device Specific Actions in XProtect.

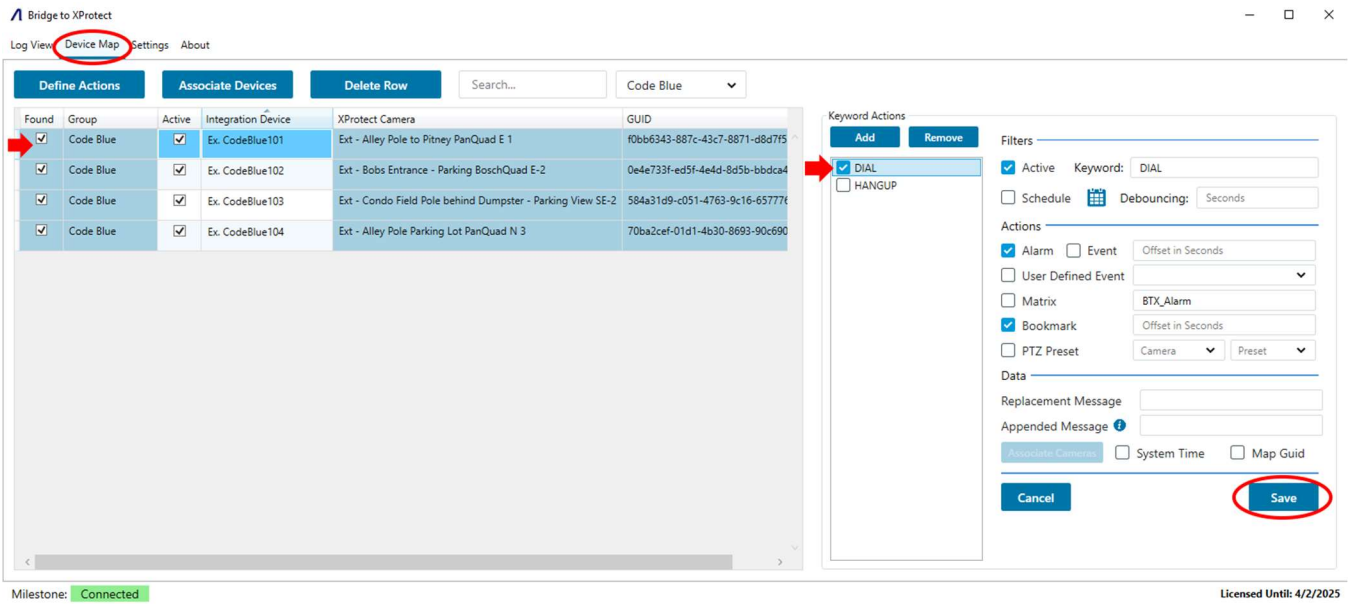
Once third-party devices have been associated with XProtect cameras, they are added as rows to the “Device Map” grid.

The “Device Map” displays to the user what actions will be taken in XProtect when an alarm keyword match occurs on each specific third-party device.

To edit settings at the device-level, highlight a row and click on a specific Keyword Action.



Edit your settings. By editing the settings, the user will only change the keyword settings for this device. These settings will **NOT** apply to other devices on the table.



NOTE: Regarding **device-specific** actions, BTX allows the user very granular control over what actions in XProtect will be taken on each specific third-party device.

There are many instances where the user may want different actions to occur in XProtect based on certain events occurring on a particular third-party device.

A good example of this is with PTZ presets. If integrating 40 motion sensor devices, each motion sensor will likely require its own PTZ command, based on the proximity of the nearest PTZ camera.

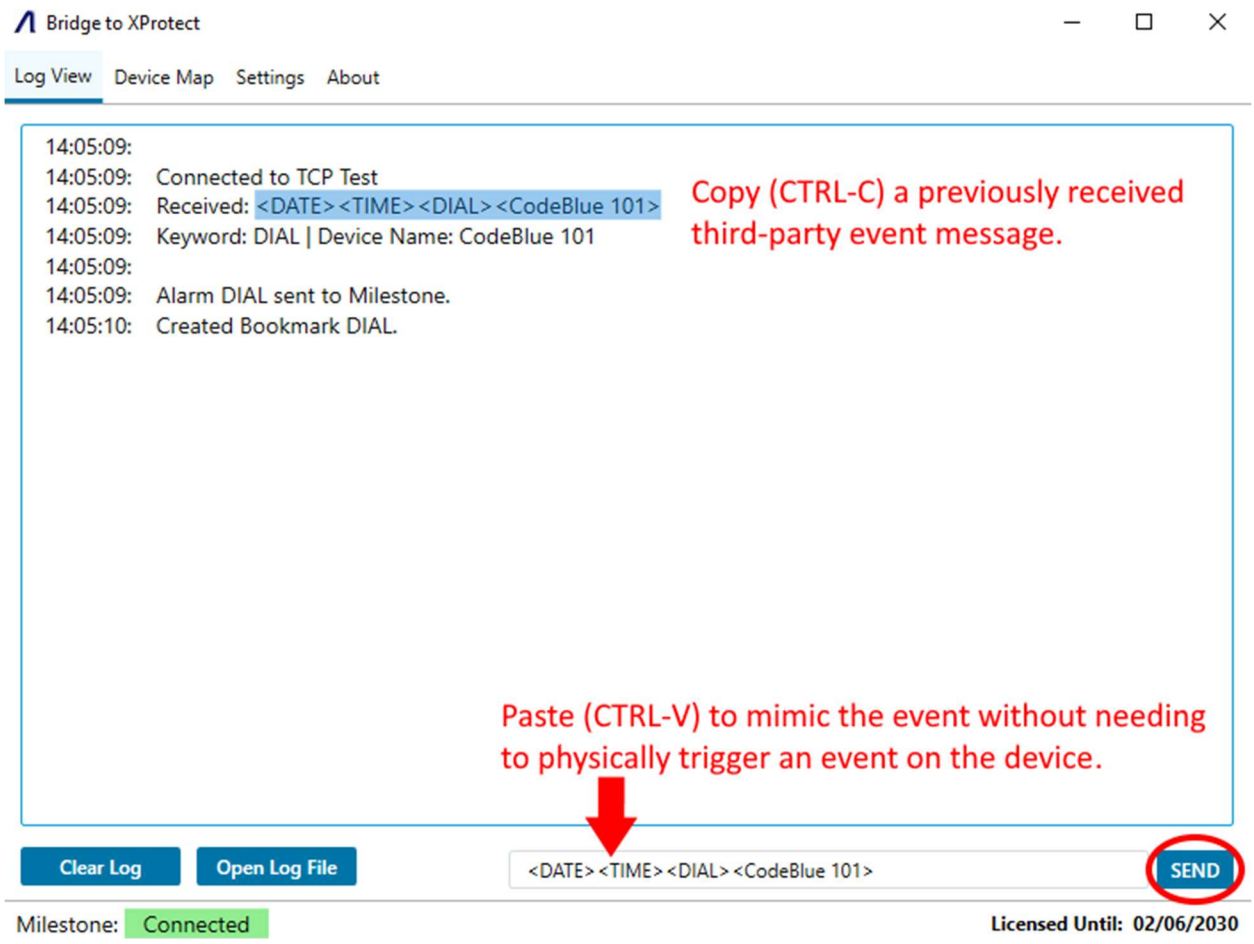
7. Testing and Evaluating Integration Configuration

7.1. Send SAMPLE third-party events to test integration configuration.

Go to the “Log View” tab.

Use the “TCP Test” field to mimic a sample third-party event message.

Third-party events previously received by BTX can be copied from the “Log View” tab or the log file and resent to BTX as test events by using the “TCP Test” feature.



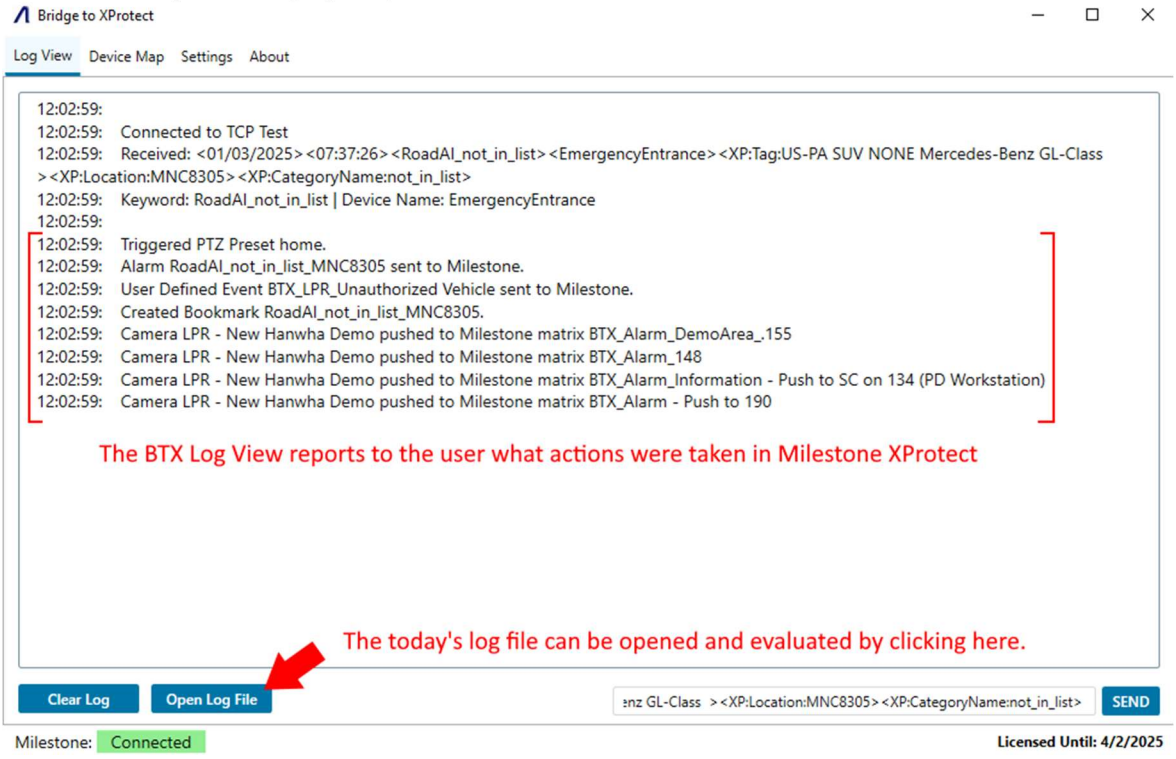
7.2. Evaluating the BTX Log View and Log Files

BTX logs all received third-party events and subsequent actions taken in XProtect.

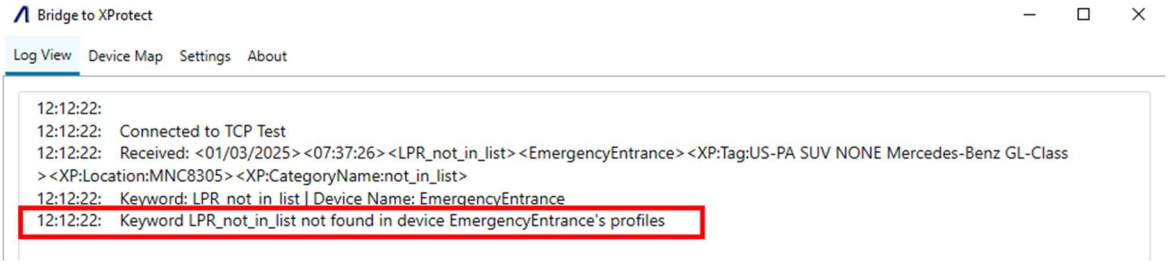
While open as a Desktop Application, the user can view the most recently received third-party events in the "Log View" tab. Today's log file can also be opened by clicking "Open Log File" button.

To access previous log files, use Windows explorer and navigate to:
`C:\App-Techs\BTX\logs` [*default file path*]

Below is an example of the log reporting a successful alarm sent to XProtect and the actions taken in XProtect.



Below is an example of a third-party event in which BTX did not detect an alarm keyword match.

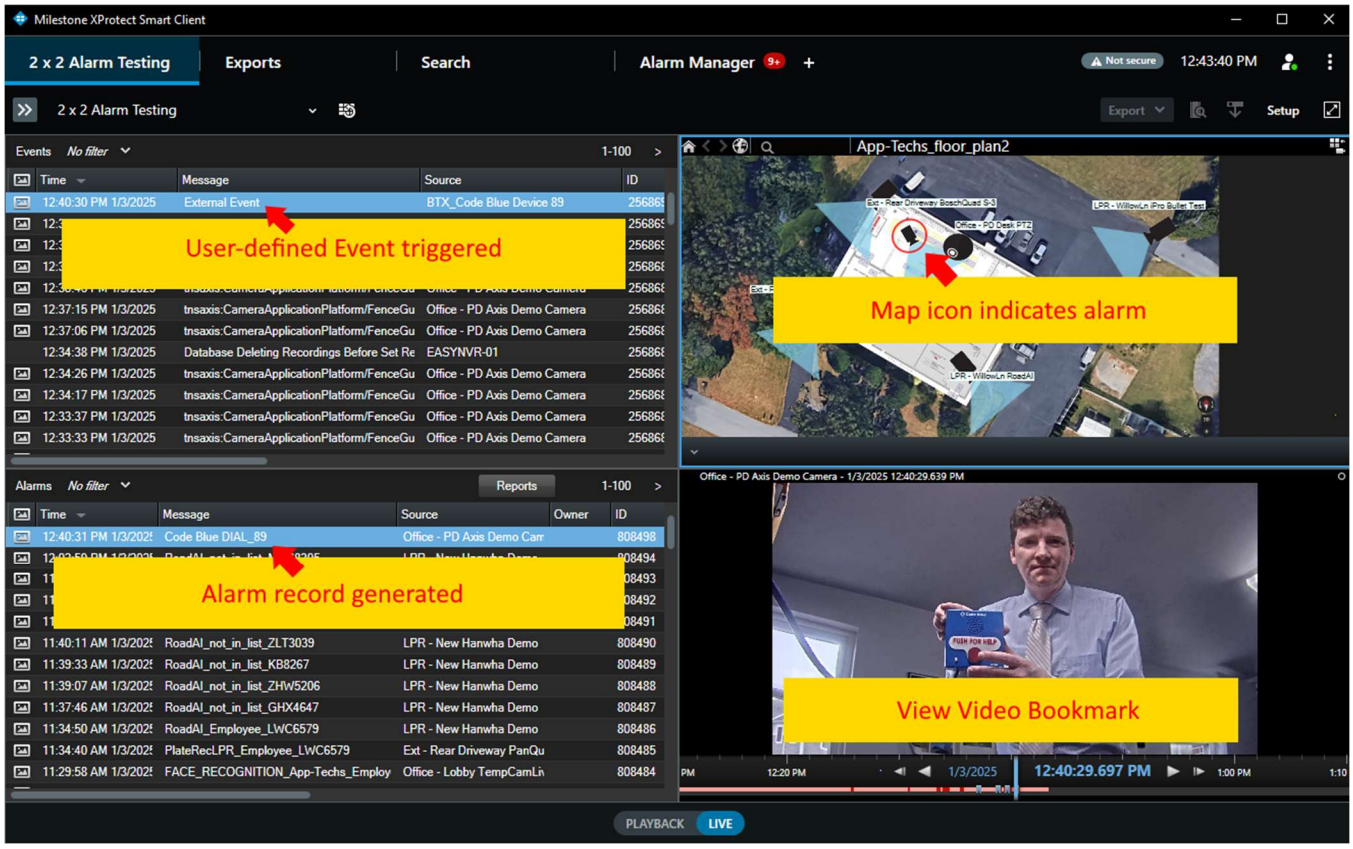


Below is an example of a third-party event in which BTX did not detect a third-party device name match.

7.3. Review Alarm Results in the XProtect Smart Client.

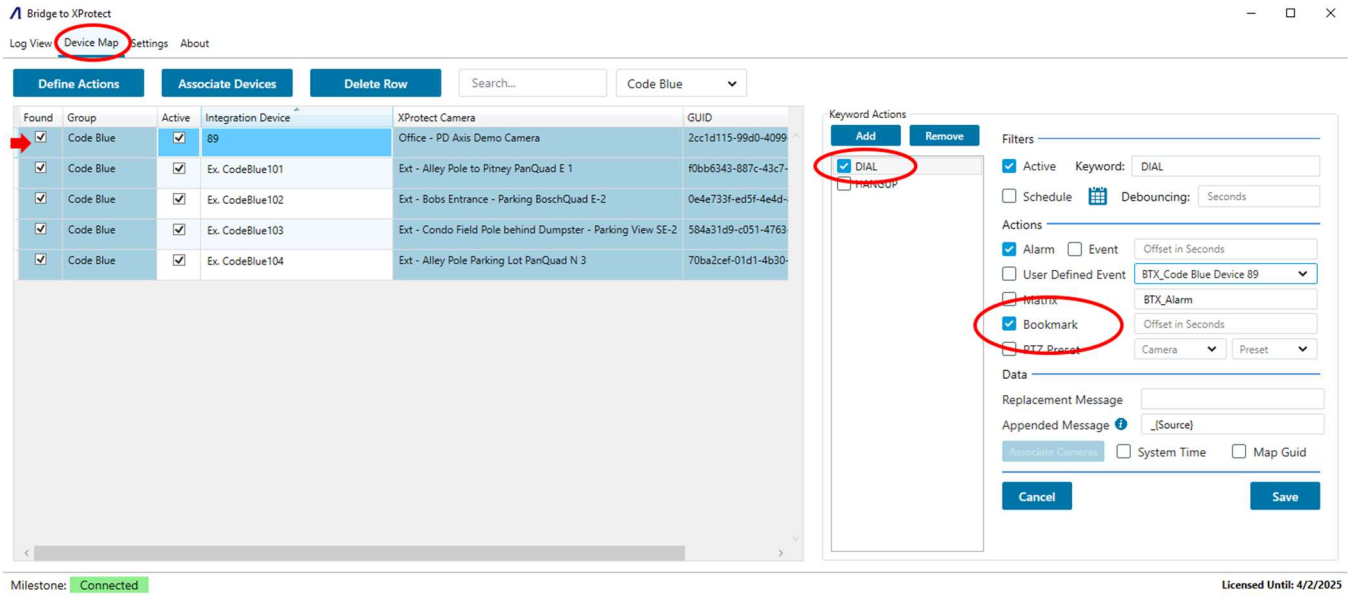
With successful configuration, a BTX user can review the actions taken in the XProtect Smart Client.

For alarms, go to the Smart Client alarm manager tab to confirm events and alarms are successfully being sent by BTX.



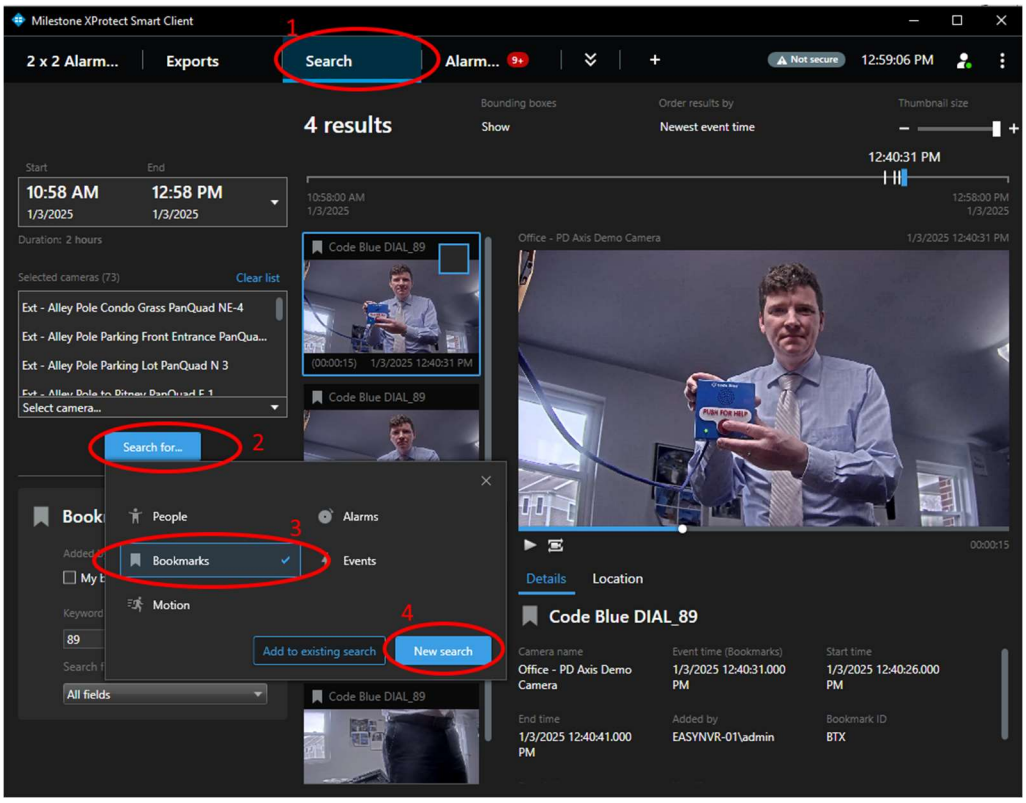
7.4. Review Searchable Bookmarks

To review search bookmarks in the XProtect, be sure the Bookmark option was selected in BTX for a given alarm keyword / third-party device.

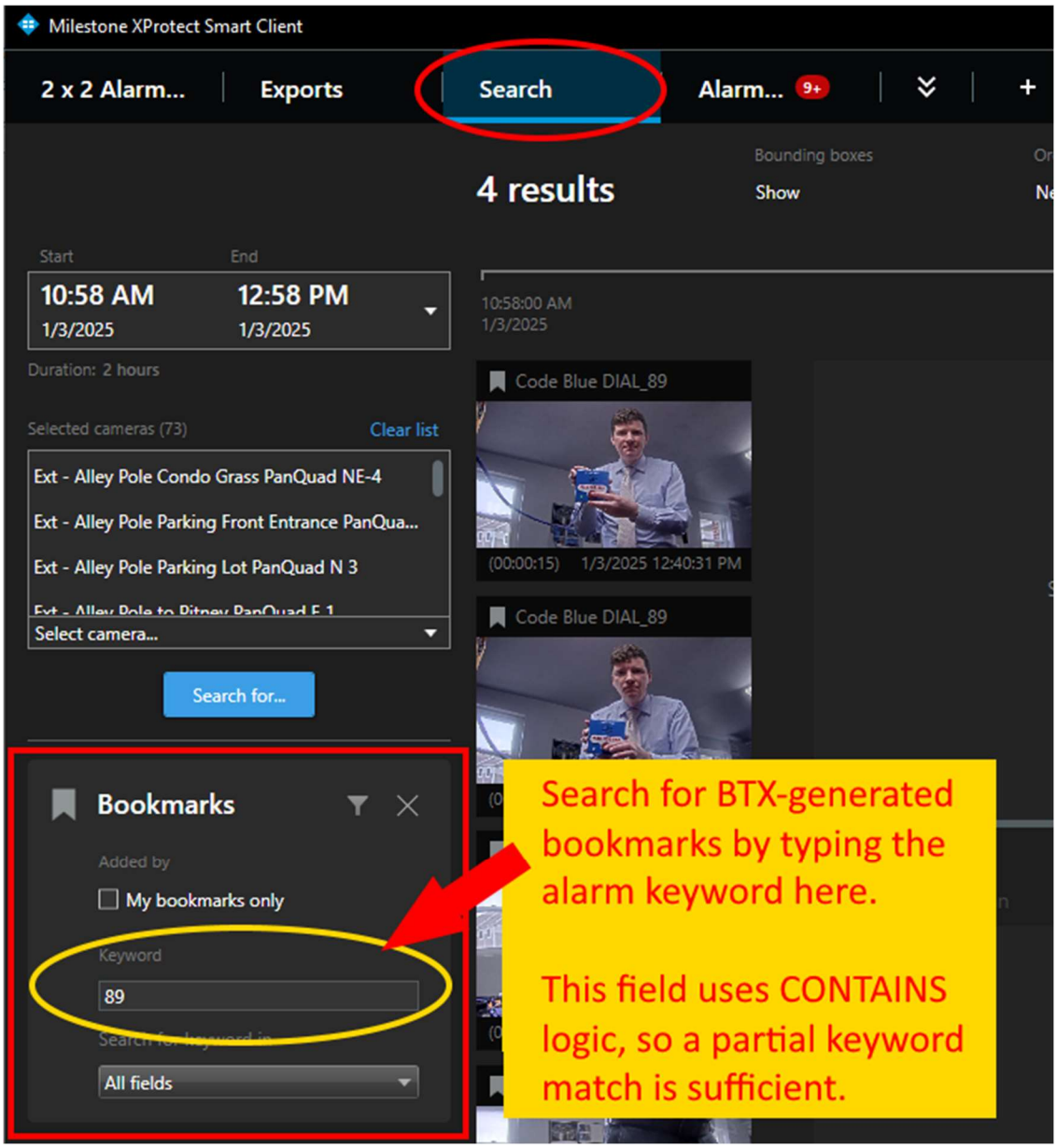


To search bookmarks, go to:

1) XProtect Smart Client “Search” tab,
2) Select Cameras,
3) Choose “Bookmarks” Option,
4) Click “New Search”,
5) Type search criteria. BTX bookmarks are searchable as character string matches. In XProtect, partial matches are sufficient.



Note: XProtect user permissions may limit access to the Search tab, or prevent viewing of bookmarks on given XProtect cameras and devices. Check your user privileges before evaluating integration results from BTX.



8. **Milestone Settings – User-Defined Events, Rules, and Live Matrix Views**

8.1. Overview

BTX requires very little configuration in the XProtect Management Client to trigger various security and display actions in XProtect. However, a few features require some minor setup in the Management Client so that BTX can trigger the preferred action.

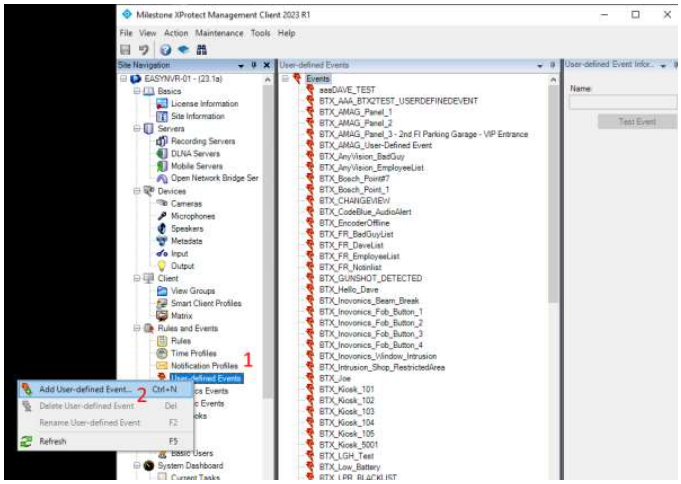
8.2. Trigger XProtect User-defined events.

User-defined events in XProtect are used to trigger "Rules" which initiate additional security actions third-party devices. Security responses, including email notification, I/O commands, and Smart Wall presets, are controlled via XProtect Rules.

8.2.1. Create User-defined Events in XProtect

1 In the XProtect Management Client, go to the Site Navigation bar on the left hand side of the screen and select *User-defined Events*.

2 From the file menu, select Action->Add User-defined Event….



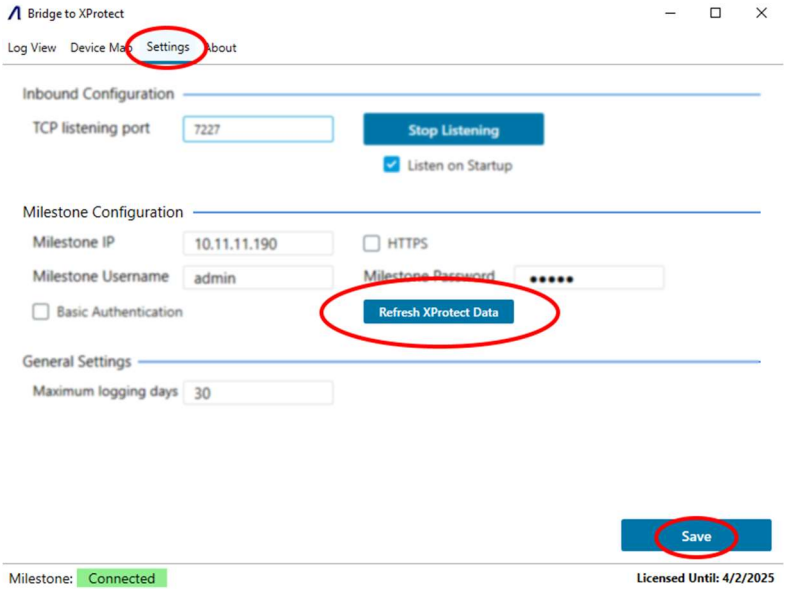
3 Enter name of User-defined Event.

Be sure to click "Save" in XProtect.

8.2.2. Refresh Management Server Configuration in BTX.

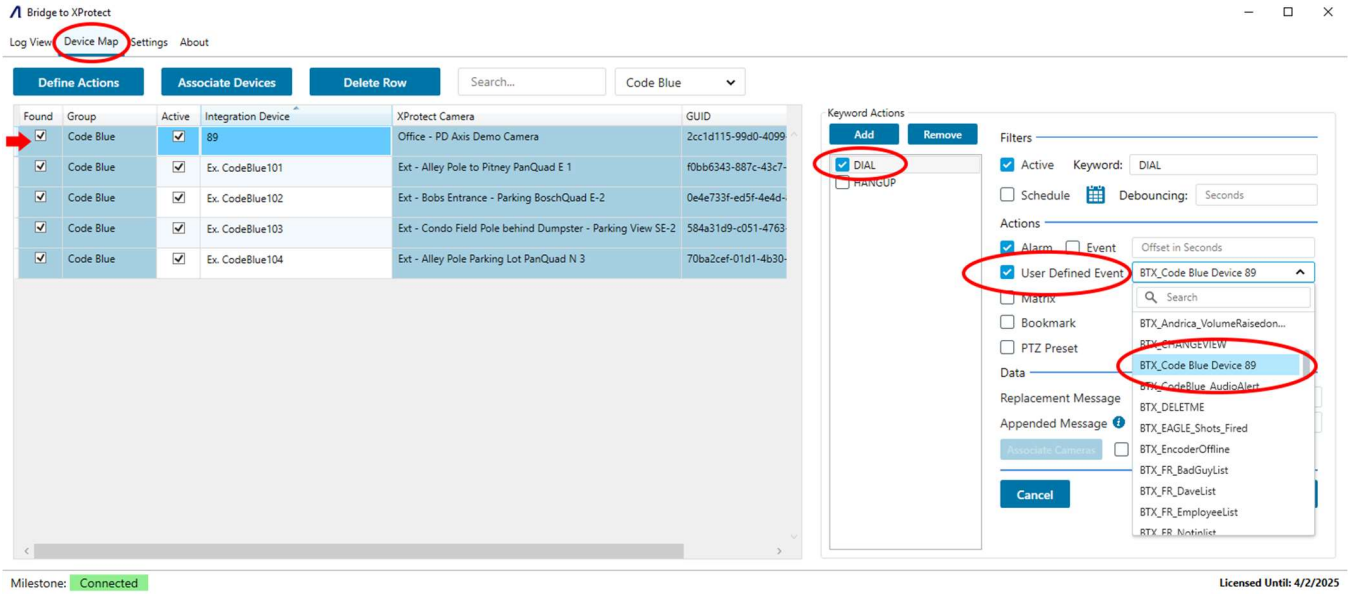
If you create new User-defined events in the XProtect Management Client, BTX must be re-refreshed to update its stored information.

To refresh XProtect settings in BTX, go to the "Settings" tab → "Refresh XProtect Data



8.3. Trigger XProtect User-defined events in BTX.

In BTX, User-defined events can be associated with given alarm keyword / third-party device as shown below:



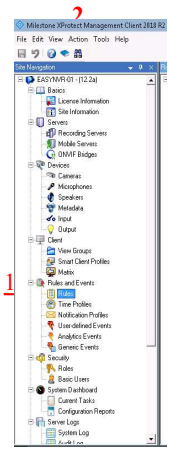
8.3.1. Trigger Action in XProtect using XProtect Rules

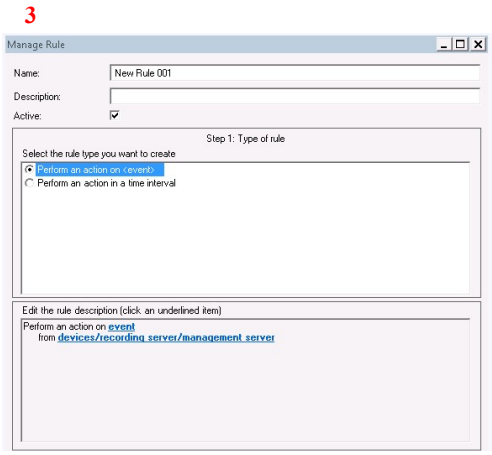
Trigger Action using XProtect Rules

1 In the XProtect Management Client, go to the Site Navigation bar on the left hand side of the screen and select *Rules*.

2 From the file menu, select Action →Add Rule….

3 Follow the steps in the Manage Rule tool to create a rule that associates any specified User-defined Event with a desired action.





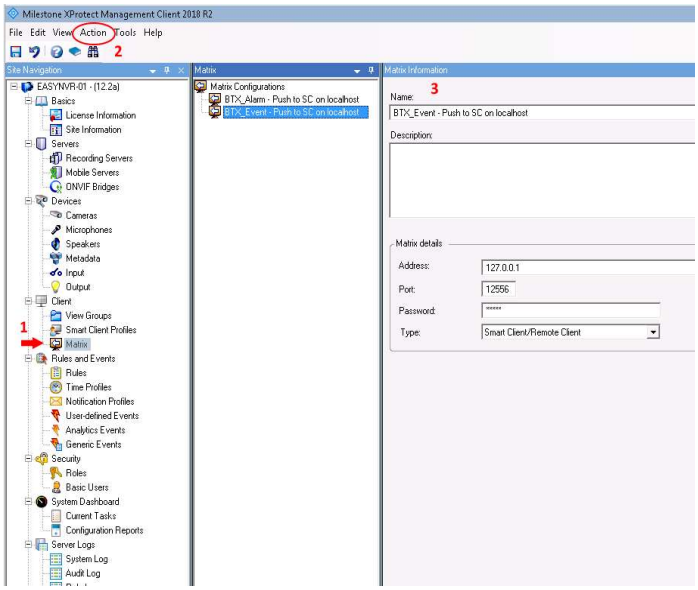
8.4. Trigger XProtect Live Matrix Views

To configure a Matrix Display in XProtect:

1 In the XProtect Management Client, go to the Site Navigation bar on the left-hand side toolbar and select *Matrix*.

2 From the file menu, select Action → Add Matrix….

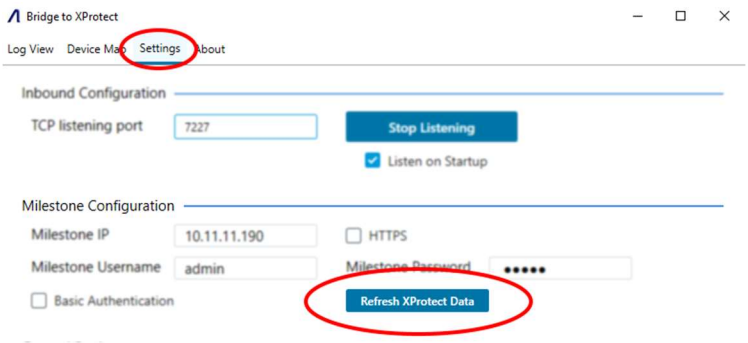
3 Save Settings in XProtect.



8.4.1. Refresh Management Server Configuration in BTX.

If you create new Matrix Profiles in the XProtect Management Client, BTX must be re-refreshed to update its stored information.

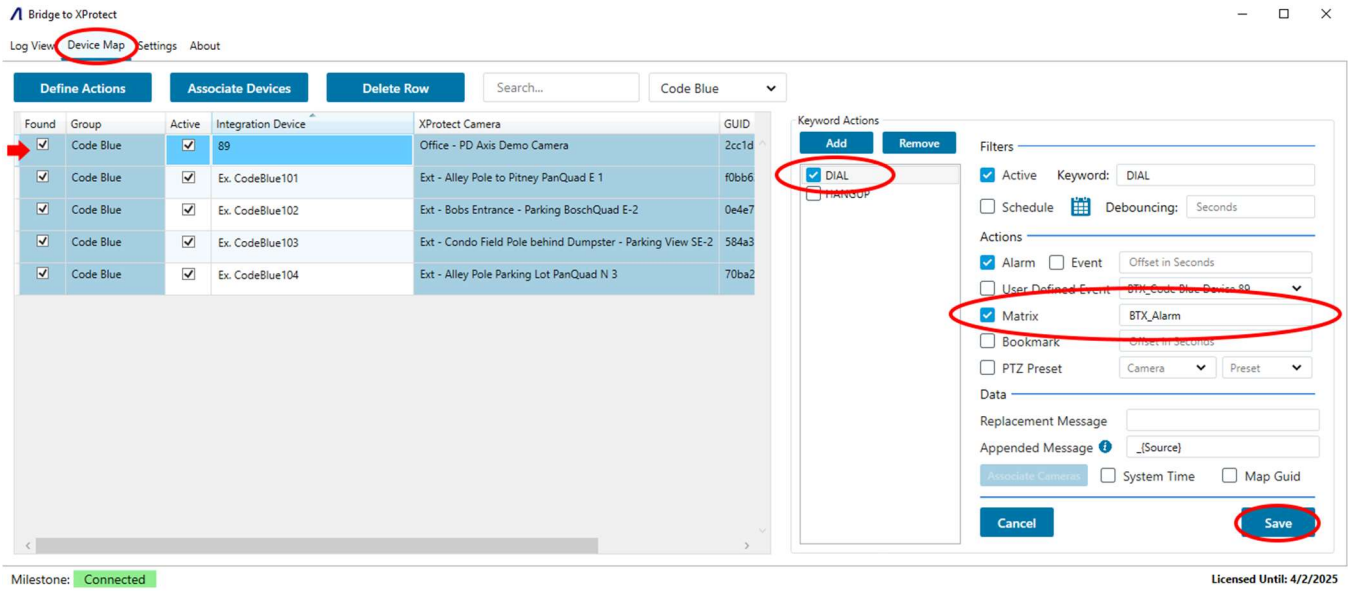
To refresh XProtect settings in BTX, go to the "Settings" tab → "Refresh XProtect Data."



8.4.2. Trigger XProtect Live Matrix View with BTX.

In BTX, XProtect live matrix views events can be associated with given alarm keyword / third-party device as shown below:

Note: The Matrix textbox in BTX uses *STARTS WITH* logic. As such, in the example below, BTX will trigger all XProtect Matrix profiles that *START WITH* "BTX_Alarm". This logic is useful if you want certain alarms to trigger certain sets of Matrix Profiles.



9. Third-party Integrations - General

9.1. Overview

BTX receives third-party alarm message via TCP to default port 7227. If the third-party device allows you to specify a TCP output when an event-of-interest occurs, BTX can integrate the device with Milestone XProtect.

9.2. Third-party integration subsystems

Not all third-party devices provide the option to send user-defined TCP messages. In this case, BTX uses sub-systems to receive messages in other protocols / formats and convert them into a TCP message.

BTX third-party sub-systems are located in the following directory:

c:\app-techs\BTX\Third-party

If an integration requires a sub-system, instructions are included in the sub-system folder.

9.3. Formatting TCP messages for BTX.

BTX uses the format below to receive and process third-party alarms.

```
<DATE><TIME><ALARM KEYWORD><DEVICE NAME>
Parameter #1
        Parameter #2
                Parameter #3
                                Parameter #4
```

If the third-party device allows you to specify the TCP message to be sent, use this format to construct the alarm messages to be forwarded to XProtect.

will now associate all Vaidio alerts occurring on “VaidioDevice001” to the corresponding XProtect camera.

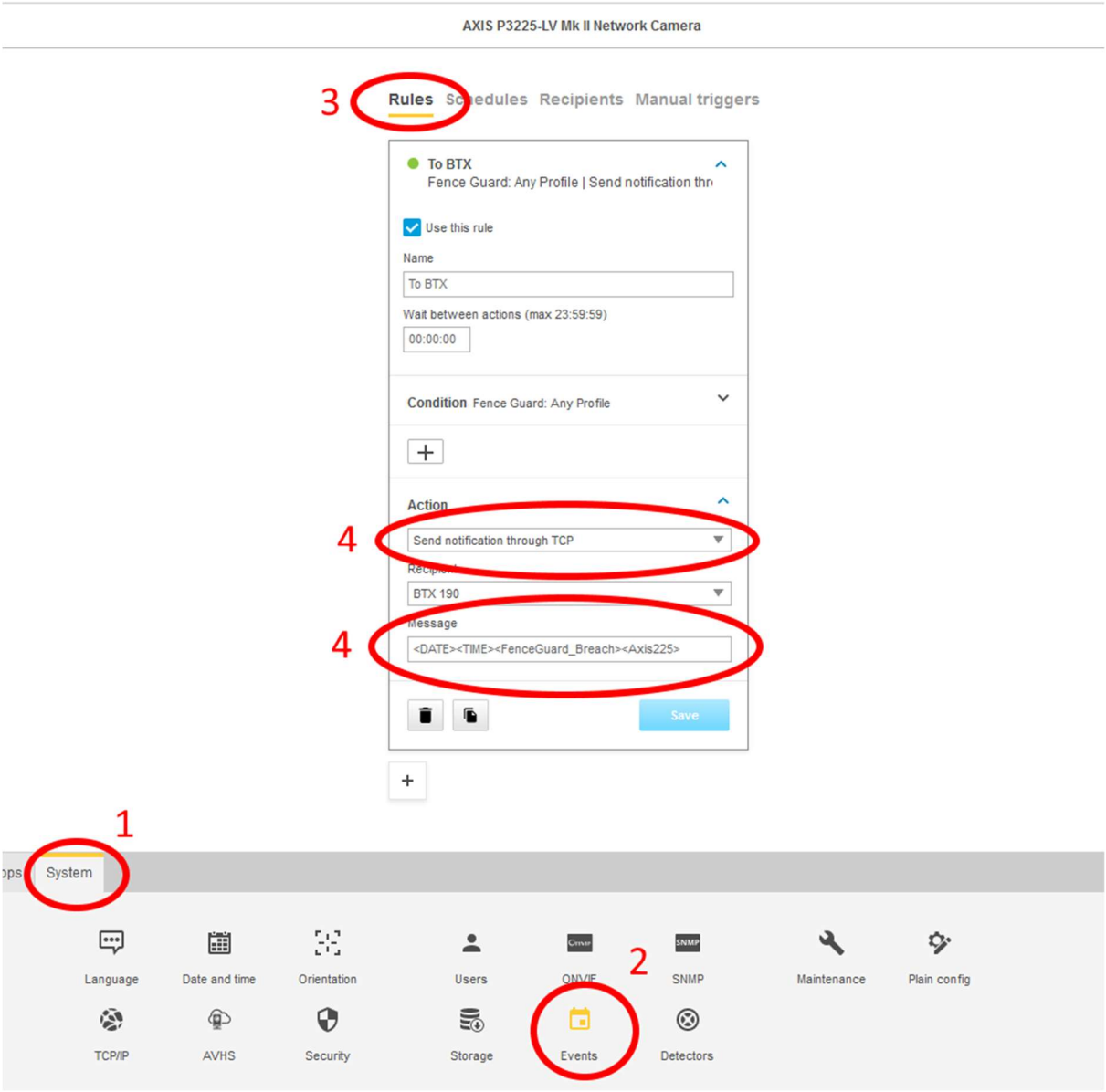
9.4. Third-party Integration Example – Axis Device Events

Axis devices provide a method to send outbound TCP message when device events-of-interest occur. BTX can receive this message and integrate the event with XProtect.

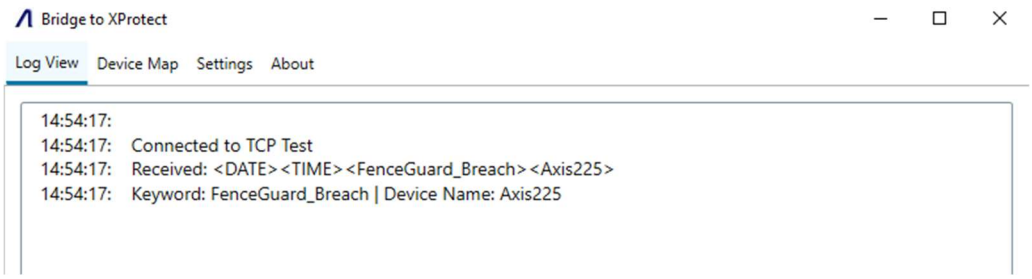
Note: Check network and firewall settings to confirm the third-party device can communicate with BTX over port: 7227 *(default)*.

Use the format above to construct a preferred alarm string.

In this case, the **ALARM KEYWORD** is “FenceGuard_Breach” and the **DEVICE NAME** is “Axis225”

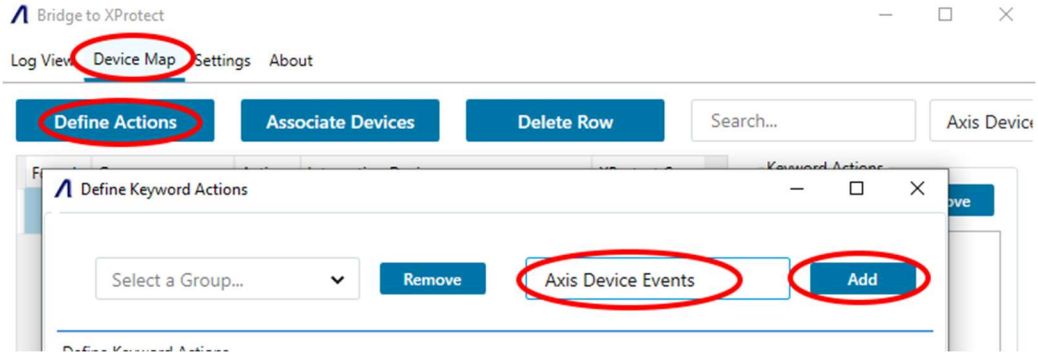


When a “FenceGuard_Breach” is received by BTX from the Axis device, it will be displayed as the following:

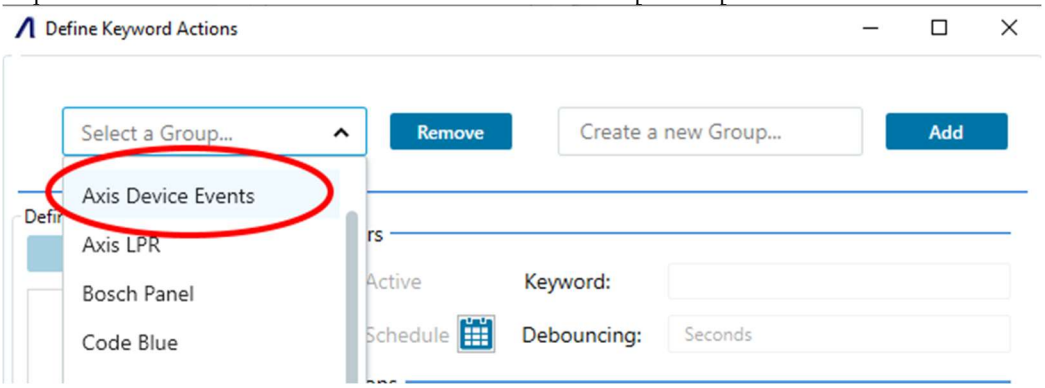


With the alarm keyword: “FenceGuard_Breach” and device name: “Axis 225”, BTX can easily be configured to integrate this Axis device event with XProtect.

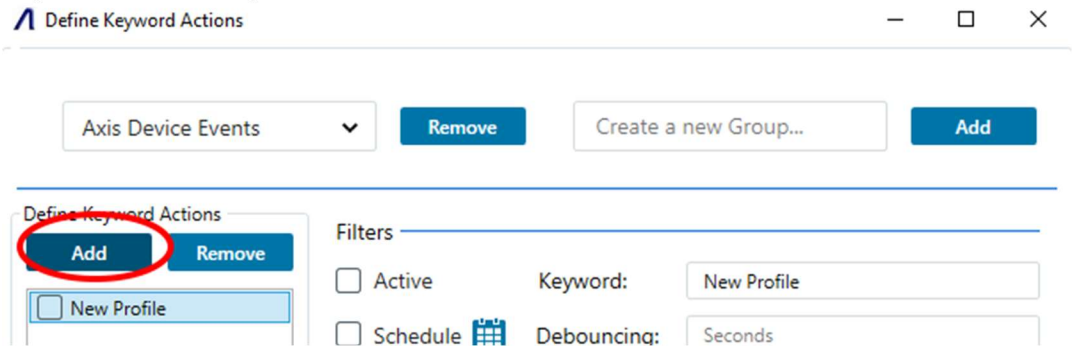
Step #1: Create new Integration Group.



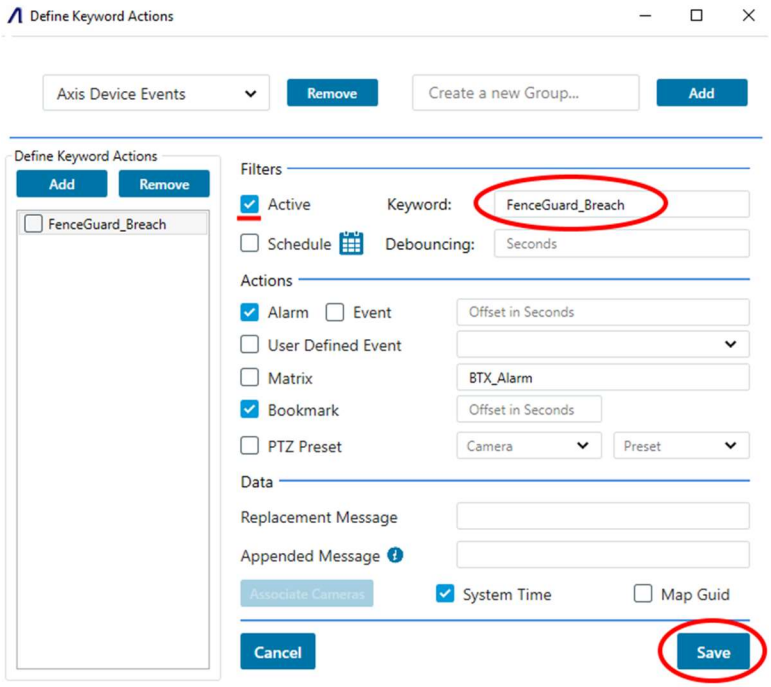
Step #2: Select the “Axis Device Events” from the “Select a Group ...” dropdown menu.



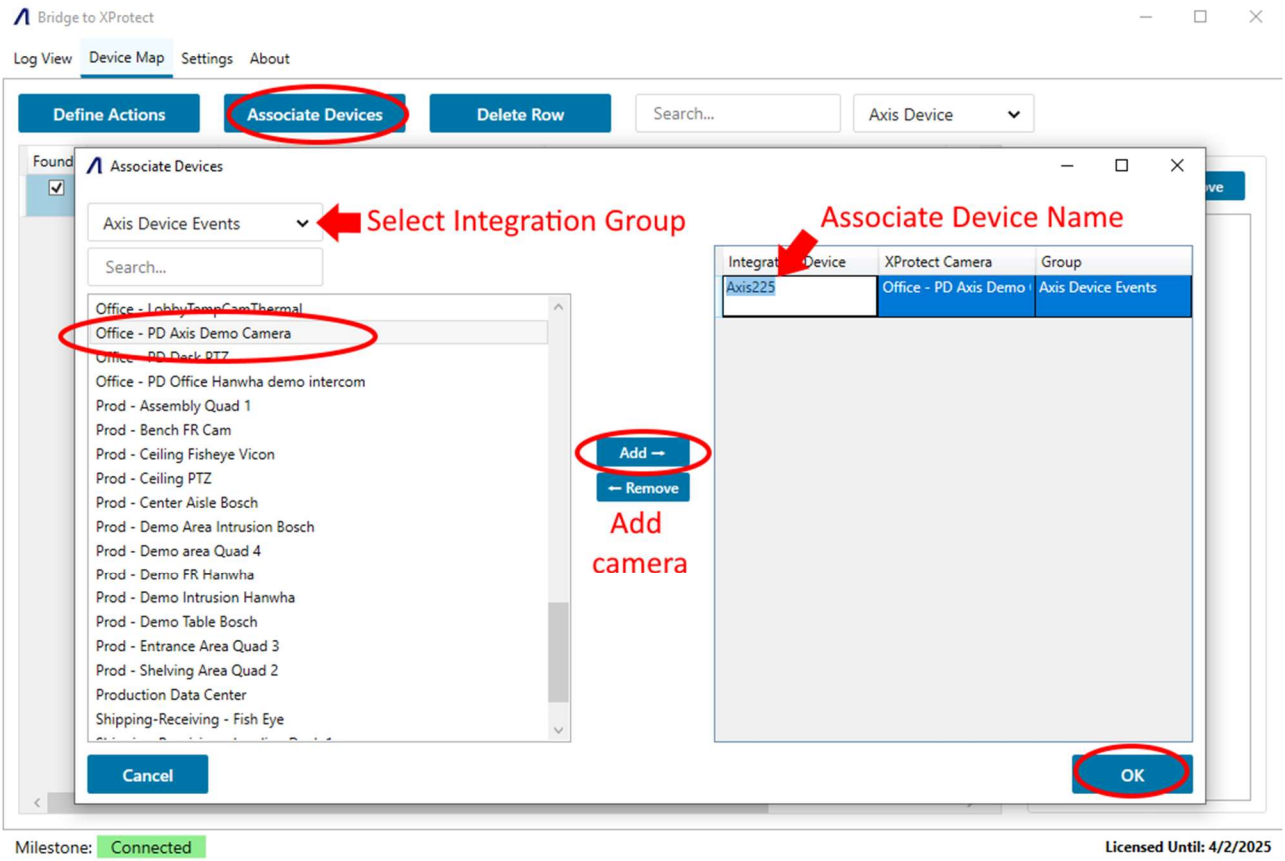
Step #3: Define a new Keyword Action.



Step #4: Define an “Alarm Keyword” match and choose preferred actions in XProtect.



Step #5: Associate the Axis Device with its XProtect counterpart. A “FenceGuard_Breach” event on device “Axis225” is now integrated with Milestone XProtect.

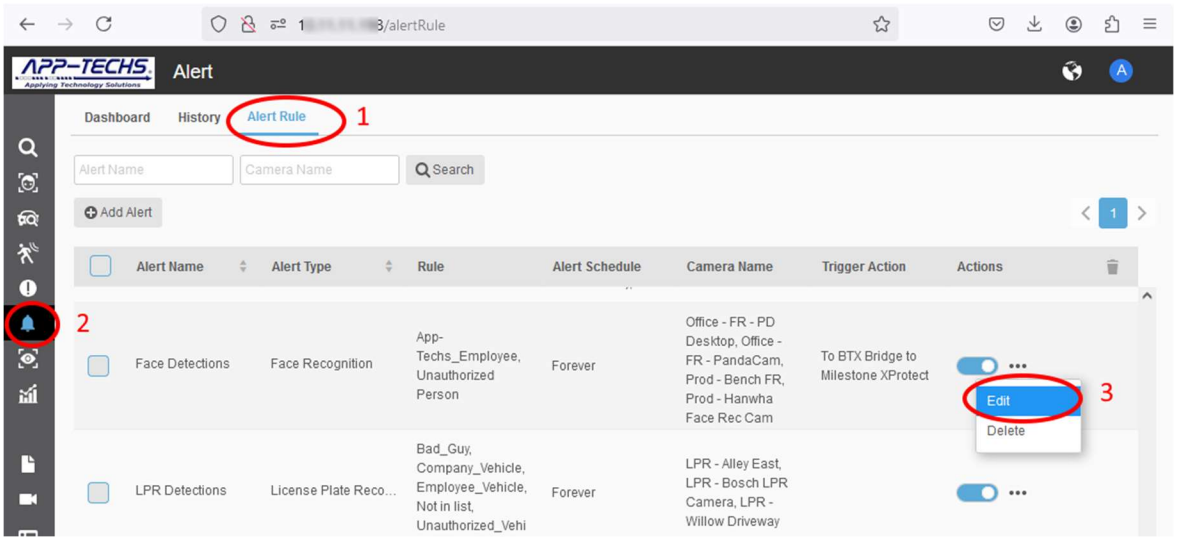


10. Third-party Integrations – IronYun Vaidio Video Analytics

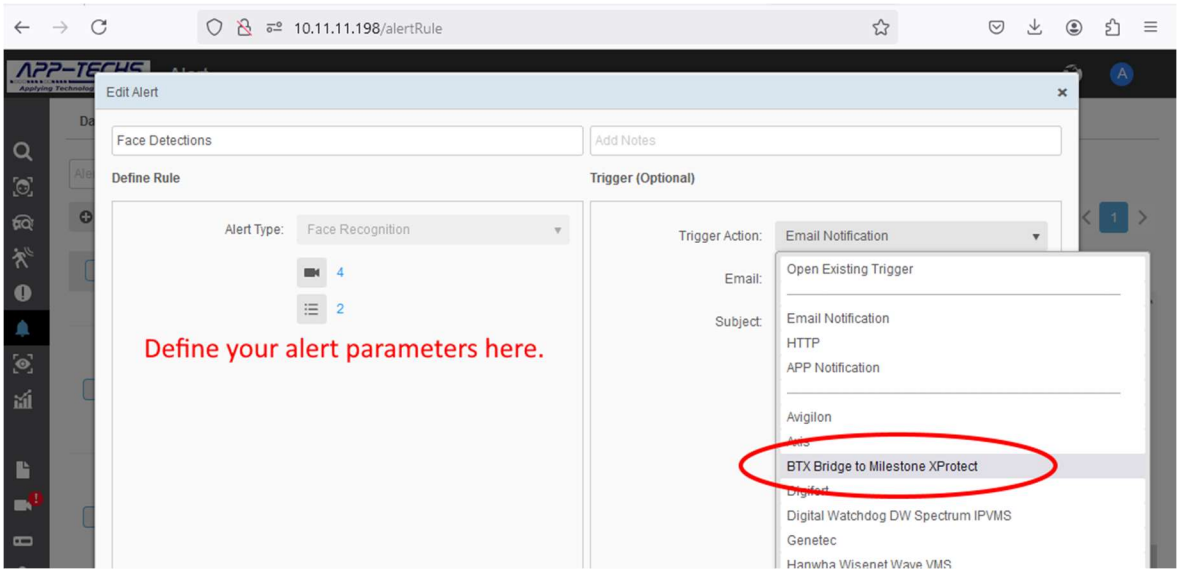
BTX serves as the middleware to relay Vaidio live analytics alerts to Milestone XProtect. Users have ample control over what actions are taken in Milestone XProtect when a Vaidio alert-of-interest occurs.

10.1. Vaidio Alert Configuration

Navigate to the Vaidio Alert menu and go to the "Alert Rule" sub-tab. Choose to add an alert or edit an existing one.



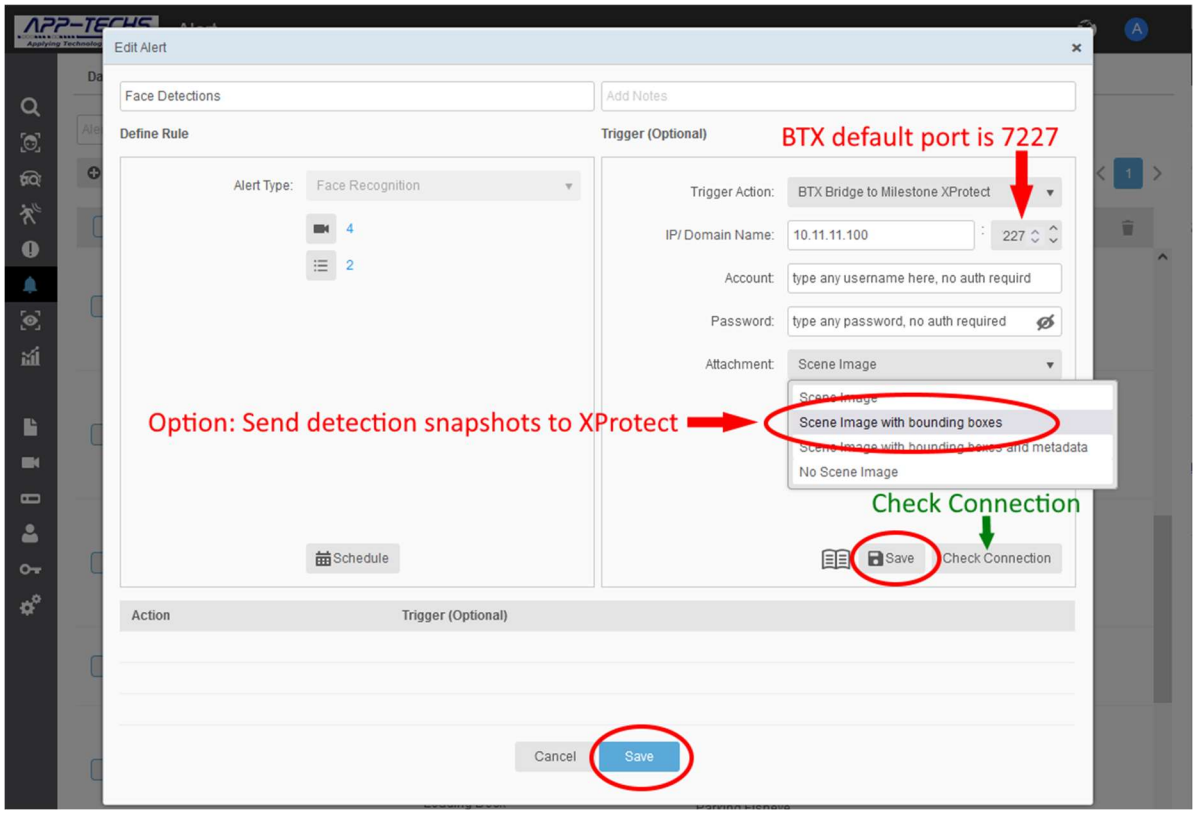
After configuring your preferred alert parameters, select "BTX Bridge to XProtect" from the "Trigger Action:" dropdown menu.



Enter settings to direct Vaidio alert events to a running instance of BTX.

1. Make sure BTX.exe is running on its server so it can receive data.
2. Enter IP address of the server where BTX resides.
3. Enter BTX listening port #. Default is 7227.
4. Enter any username. BTX does not require authentication, so type any value in this field.
5. Enter any password. BTX does not require authentication, so type any value in this field.
6. Optionally choose to send detection snapshots to XProtect.
7. Check connection to verify network path.
8. Save Trigger settings.
9. Save Alert settings.

If the “Check Connection” test fails, check firewall settings on the server where BTX resides and allow inbound TCP traffic on port: 7227 (default). Also check to make sure the Vaidio server has a network pathway to the BTX server.



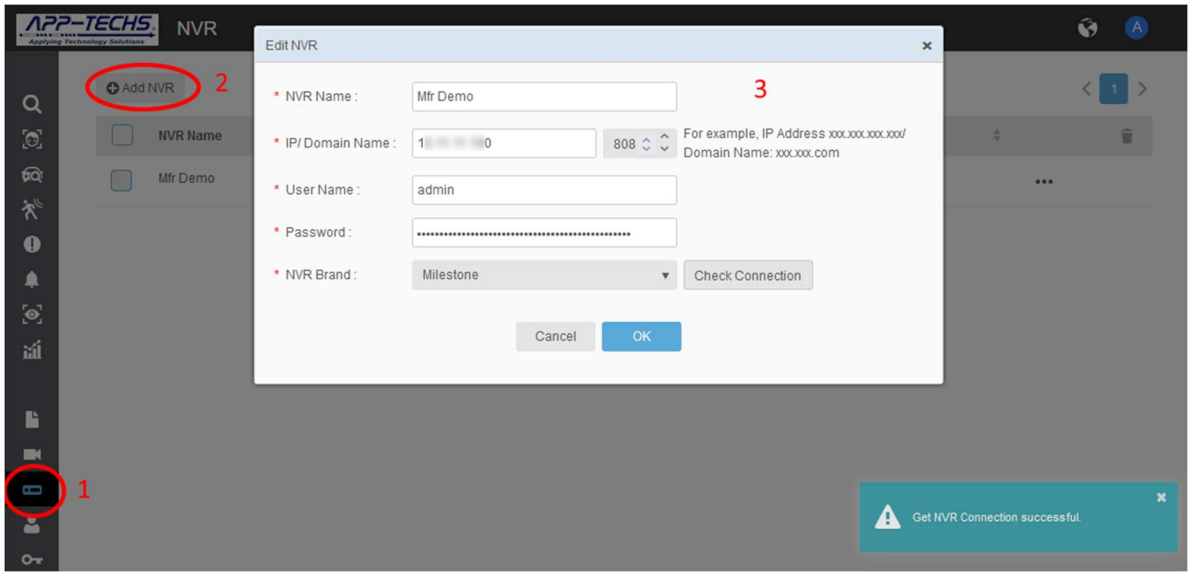
When “Check Connection” test succeeds, Vaidio alerts will be received by BTX.

10.2. Auto-Associate Vaidio cameras with XProtect cameras.

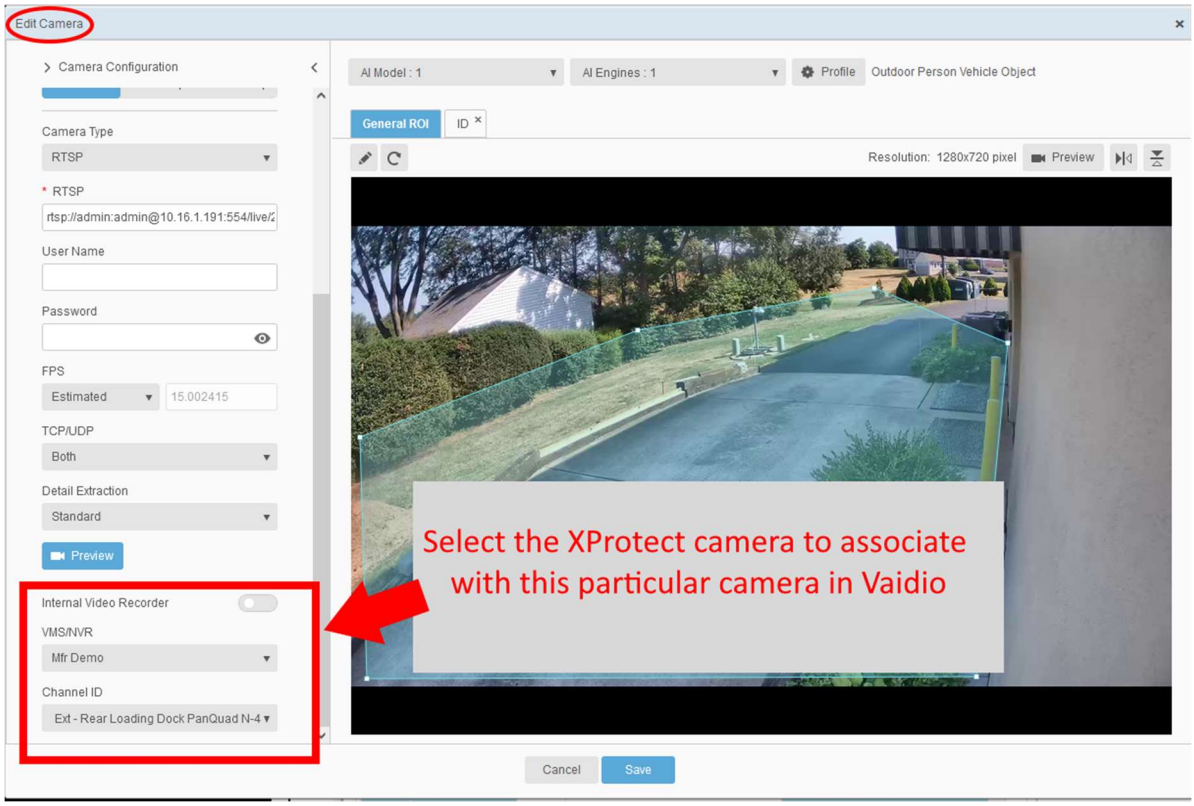
If the XProtect system has an active Mobile Server Service, a user can associate a Vaidio camera with its XProtect counterpart within the Vaidio UI.

If the XProtect system does not have a mobile server installed, a manual method of associating cameras is described in Section 10.3.

Step #1: Add the Milestone Mobile Server as an “NVR” instance in XProtect.

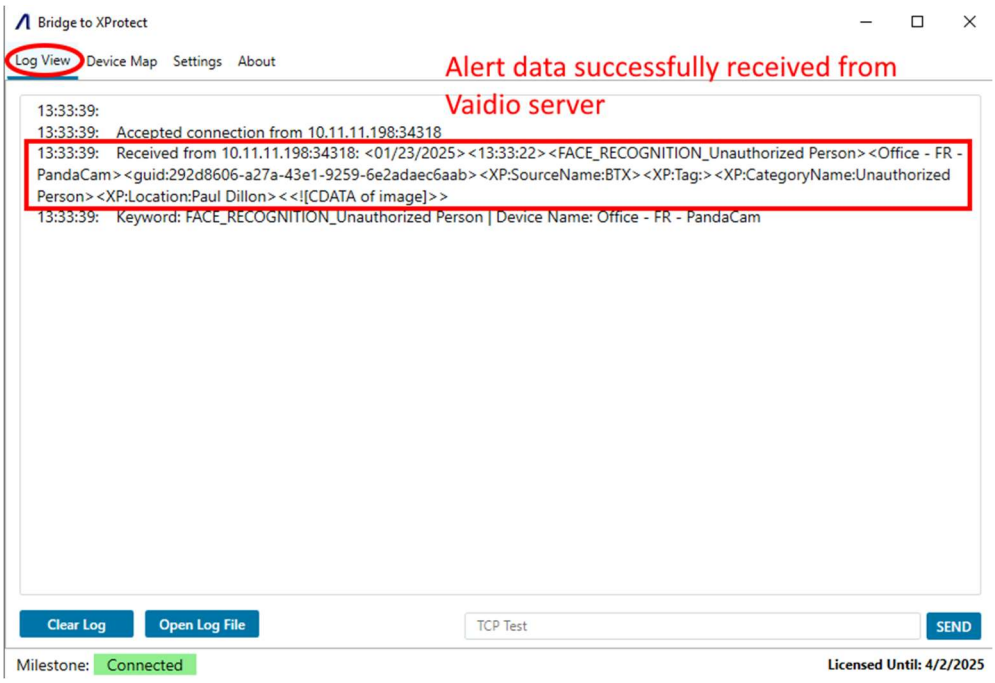


Step #2: In the Vaidio “Edit Cameras” menu, use the left-hand tool bar to select a XProtect camera to associate with the Vaidio camera. Complete this step for each camera in the Vaidio system.



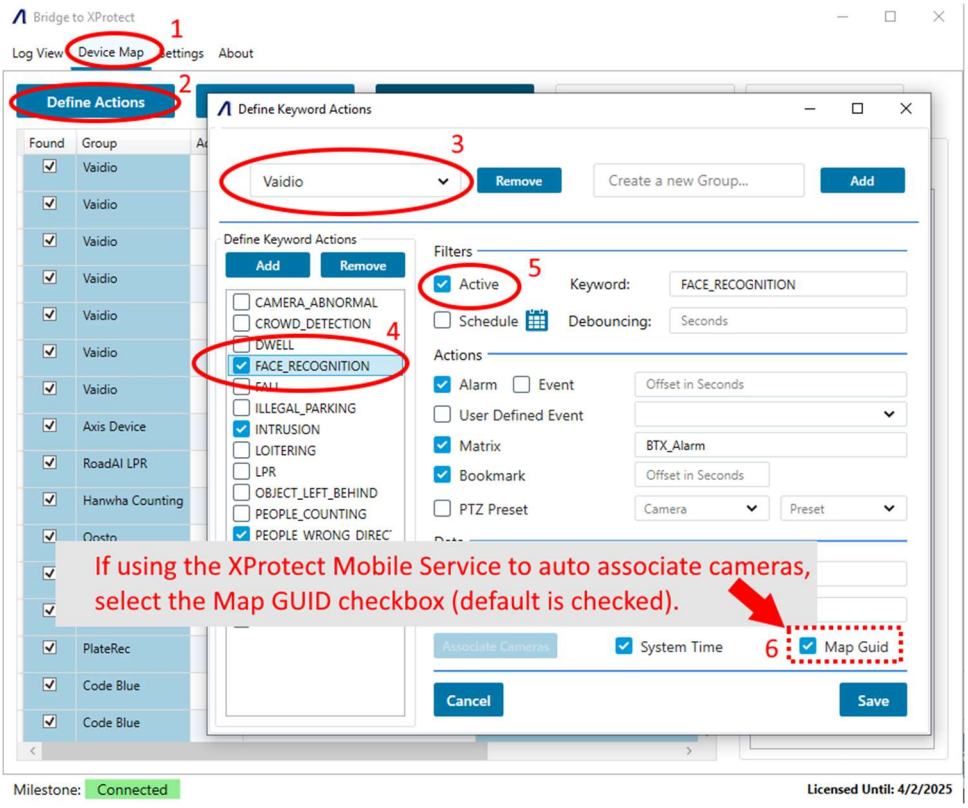
10.3. Configure BTX to relay Vaidio alerts to XProtect.

The BTX "Log View" tab will display Vaidio alert data received by BTX.



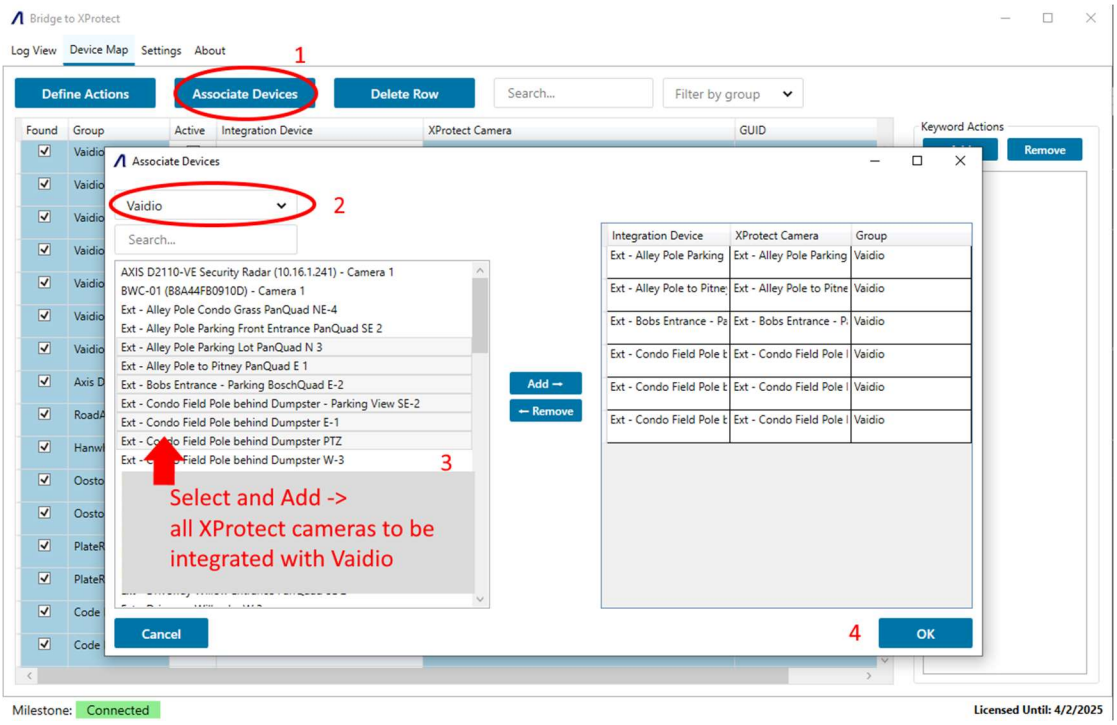
Go to the "Device Map" tab and select "Define Actions." From the "Select a Group" dropdown menu, choose "Vaidio."

For each keyword type, choose the preferred actions in XProtect when a Vaidio event containing a keyword match occurs.

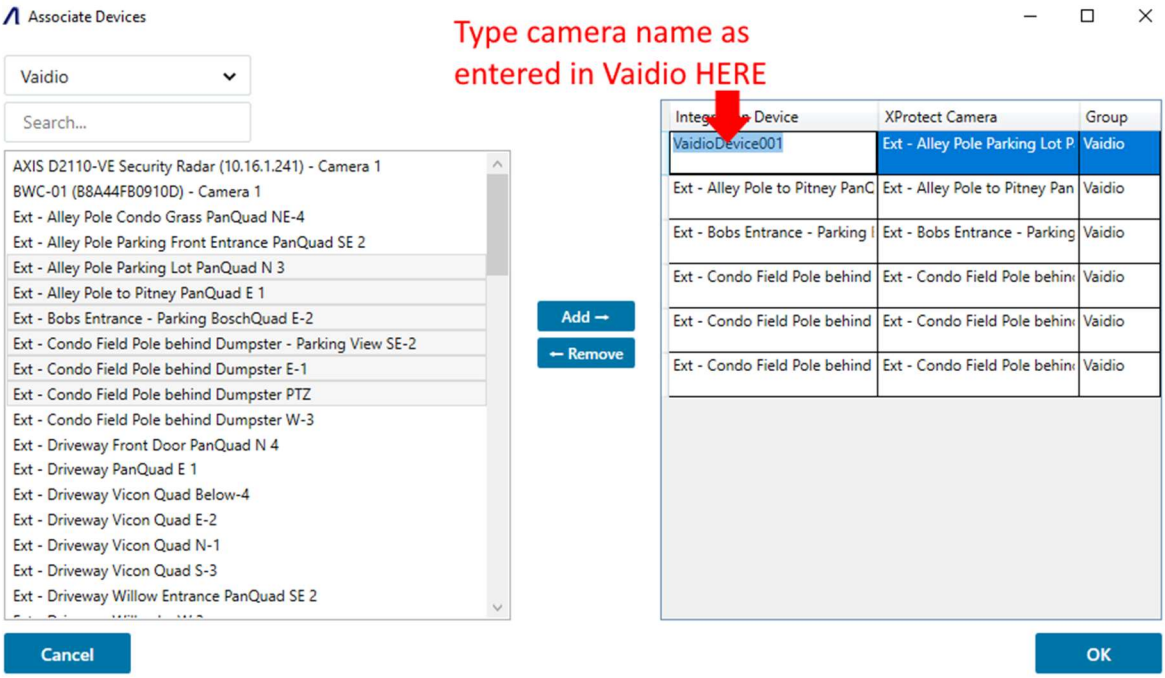


Go to the “Device Map” tab and select “Associate Devices.”

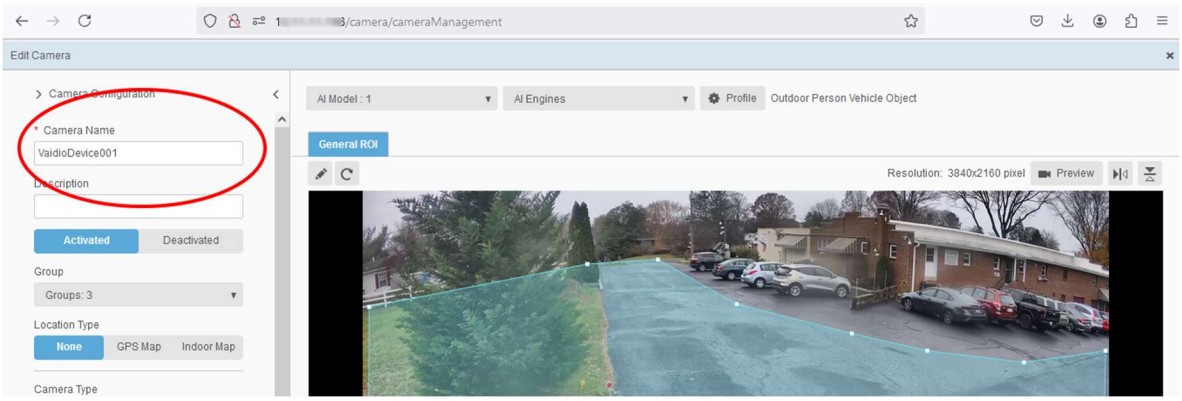
If auto-associating cameras as described in Section 10.2, select from the list of XProtect cameras to be integrated with Vaidio and press “ADD →”. Press “OK”. Vaidio events are now integrated with Milestone XProtect.



If manually associating Vaidio device name with XProtect cameras, edit the “Integration Device Column” so that the device name in this column matches the camera name in Vaidio.



The camera name as entered in the Vaidio UI is the field shown below:



Click OK. Vaidio events are now integrated with Milestone XProtect.

10.4. Create list specific actions for Vaidio License Plate Recognition (LPR) and Face Recognition detections.

There are many scenarios where a BTX user may want to trigger specific actions in XProtect based on the detection list. This applies specifically to the Vaidio face recognition and license plate recognition (LPR) analytics. As an example, a user may want trigger a XProtect user-defined event to unlock a door for detected individuals on the "Employee" list, but generate an alarm for individuals on the "Unauthorized" list.

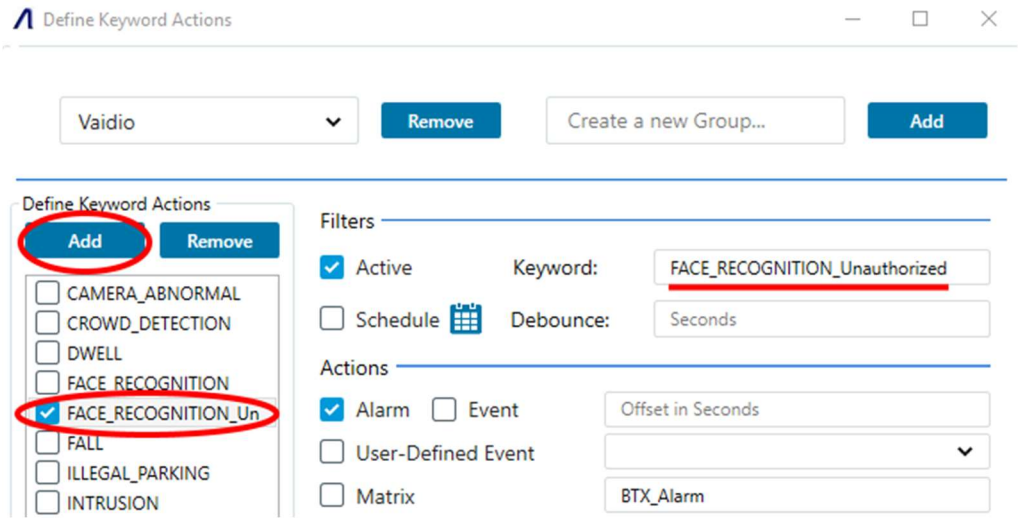
BTX makes this simple to do by allowing users to trigger action based on a more specific alarm keyword type.

To setup list-specific actions in BTX, go to the "Device Map" tab, select "Device Actions", and choose "Vaidio" from the "Select a Group ..." dropdown.

With its default settings, BTX will consider ALL received Vaidio alerts containing the alarm keyword "FACE_RECOGNITION" or "LPR" as qualifying as an alarm keyword match.

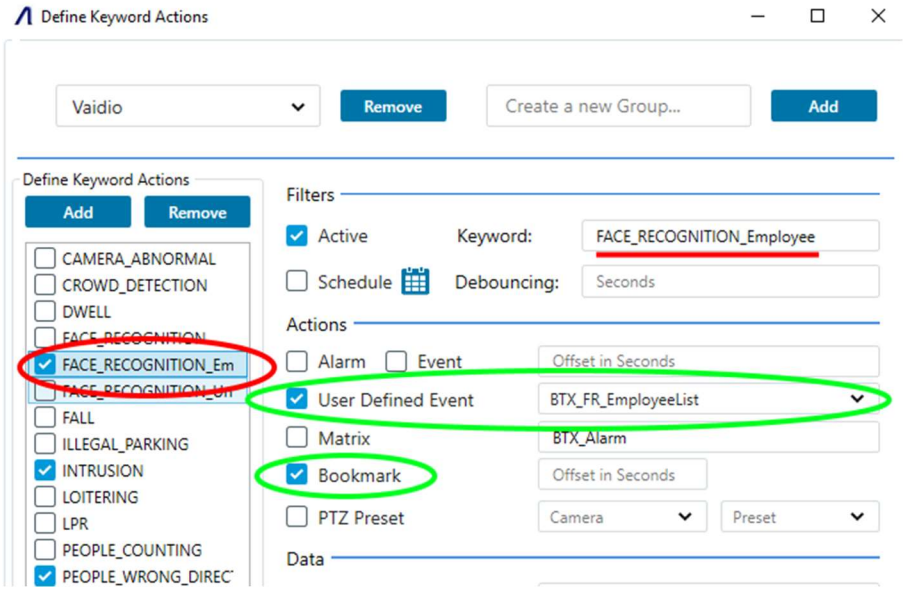
Deactivate the default "Face Recognition" alarm keyword and click ADD to define a new keyword action.

Click "Add" to define a new Keyword Action and create a new entry with a keyword containing a Vaidio list name.
Ex. "FACE_RECOGNITION_Unauthorized"

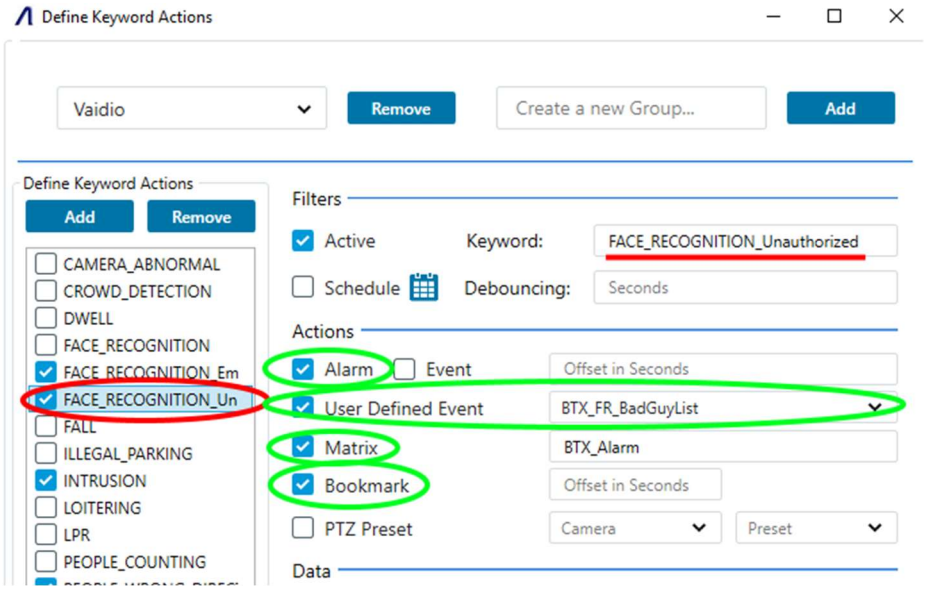


BTX will now trigger trigger actions in XProtect only if the Vaidio alert contains the "Unauthorized" list type.

Ex: When keyword CONTAINS "FACE_RECOGNITION_Employee", generate a XProtect bookmark and trigger the User-defined event.

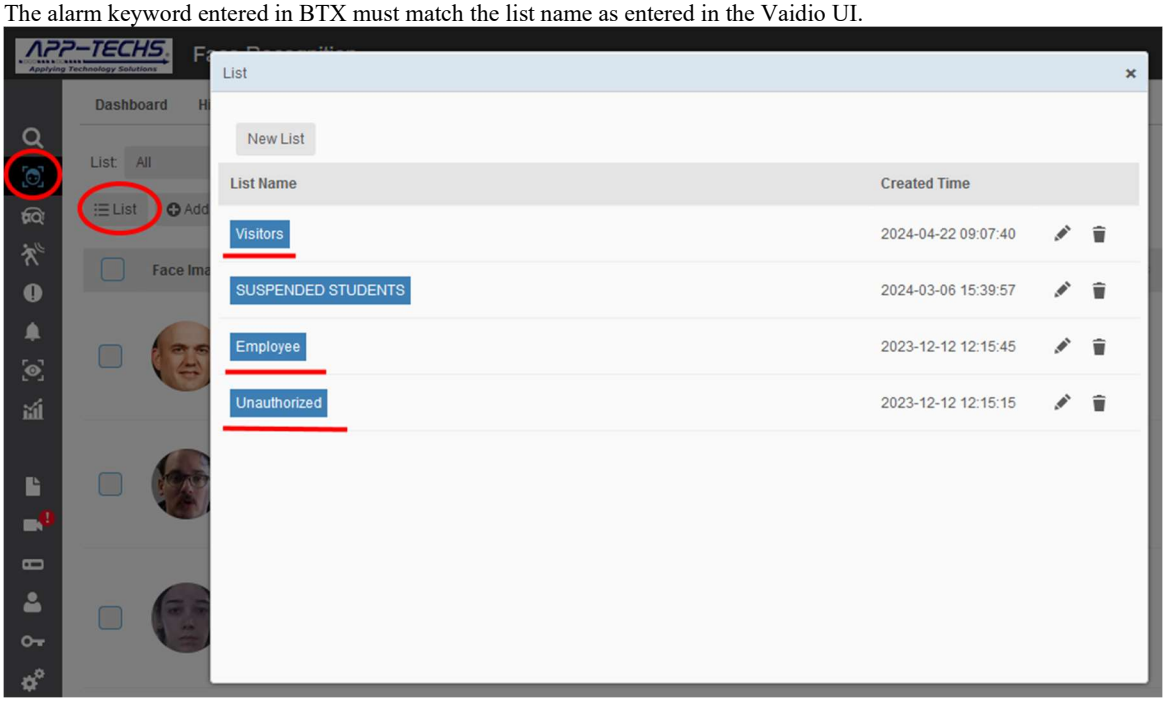


Ex: When keyword CONTAINS "FACE_RECOGNITION_Unauthorized", generate a XProtect alarm + bookmark, trigger the User-defined event "BTX_FR_BadGuyList", and fire all live Matrix profiles that start with "BTX_Alarm."



Please note that any alarms containing another list type, ex. “Visitors,” will now have to be defined in BTX to qualify as an alarm keyword match.

The alarm keyword entered in BTX must match the list name as entered in the Vaidio UI.



11. **BTX FAQ**

Q: BTX connection settings appear correct, but the Log View indicates that I am not receiving any alarm data from my third-party devices. What could be the cause?

A: The most common fixes for this issue is to check if the third-party devices are on the same network subnet as BTX, or if there is a verified network path between the third-party device and BTX. Try pinging the device from the server on which BTX is installed. If pinging the device is unsuccessful, check your network settings, or contact a network administrator to establish a network pathway between the device and BTX.

Another common fix is to check your server's firewall settings. Because BTX requires receiving inbound TCP messages on port 7227, it is common for the Windows Firewall or Anti-virus software to block this traffic unless a rule specifically authorized this traffic. Try temporarily disabling your firewall to see if traffic appears. If so, adjust firewall rules / settings to allow traffic when it is enabled.

12. Legal

12.1. Trademarks

DMap™, SWIM™ and the App-Techs logo are trademarks of App-Techs Corp.

All other trademarks mentioned in this document belong to their respective owners.

12.2. Licenses and Copyrights

DMap includes software developed by App-Techs. Refer to the DMap Installation Guide for the full text of DMap Software License, Copyright and Warranty details.

12.3. Surveillance Privacy

Always use discretion when installing video and / or surveillance equipment especially when there is perceived privacy, or an expectation of privacy. Inquire regarding federal, state and / or local regulation applicable to the lawful installation of video and / or audio recording or surveillance equipment. Party consent may be required.

12.4. Disclaimer

App-Techs has made every effort to provide accurate and reliable information. However, App-Techs does not warrant that the contents of this document will meet your requirements; or that the operation of your system will be uninterrupted or error free before, during or after execution of any instructions; or that the content itself is in fact accurate or reliable.

In no event will App-Techs be liable to you for any damages, including any lost profits, lost savings or other incidental or consequential damages arising out of the use or inability to use the contents of this document, even if App-Techs has been advised of the possibility of such damages, or for any claim by any other party.

App-Techs Corp. reserves the right to make adjustments to this document without prior notification.