



**BTX<sup>™</sup>**

**“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!”*

This document, together with its attachments, if any, contains information that is privileged, confidential, or otherwise protected. Please refrain from dissemination, distribution or copying of this document without prior written permission from App-Techs.

January 2025

First Edition Copyright © June, 2013, App-Techs Corporation

“BTX” is a trademark of App-Techs Corporation.

Other trademarks belong to their respective Owners.

All Rights Reserved

## 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 .....	3
1.1. System Requirements .....	3
1.2. BTX Features .....	4
2. Data Flow .....	4
2.1. Overview .....	4
3. Installation .....	5
3.1. BTX Server .....	5
3.2. Core Application .....	5
3.3. Windows Service Installation .....	6
4. BTX Initial Setup .....	7
4.1. Run BTX.exe as a desktop application .....	7
4.2. Activate your BTX License .....	7
4.3. Choose your third-party integration .....	7
4.4. Enter Milestone XProtect server information .....	8
4.4.1. XProtect Authentication Success – “Connected” .....	8
4.4.2. XProtect Authentication Success – “Disconnected” .....	9
5. BTX Settings .....	11
5.1. Inbound Configuration .....	11
5.2. Outbound Configuration .....	11
5.3. Refresh XProtect Data .....	11
6. Basic Alarm Setup – Associate third-party alarms with XProtect Cameras .....	12
6.1. Alarm Data Overview .....	12
6.2. Define Alarm Actions .....	13
6.3. Define Alarm Keyword Actions .....	14
6.3.1. Alarm Keyword Specificity .....	15
6.4. Choose your preferred actions in Milestone XProtect: .....	17
6.5. Associate Analytic Devices with Milestone Camera(s) .....	19
6.6. Configure Device Specific Actions in XProtect .....	21
7. Testing and Evaluating Integration Configuration .....	22
7.1. Send SAMPLE third-party events to test integration configuration. ....	22
7.2. Evaluating the BTX Log View and Log Files .....	23
7.3. Review Alarm Results in the XProtect Smart Client .....	24
7.4. Review Searchable Bookmarks .....	25
8. Milestone Settings – User-Defined Events, Rules, and Live Matrix Views .....	27
8.1. Overview .....	27
8.2. Trigger XProtect User-defined events. ....	27
8.2.1. Create User-defined Events in XProtect .....	27
8.2.2. Refresh Management Server Configuration in BTX. ....	28
8.3. Trigger XProtect User-defined events in BTX. ....	28
8.3.1. Trigger Action in XProtect using XProtect Rules .....	29
8.4. Trigger XProtect Live Matrix Views .....	30
8.4.1. Refresh Management Server Configuration in BTX. ....	30
8.4.2. Trigger XProtect Live Matrix View with BTX. ....	31
9. Third-party Integrations - General .....	32
9.1. Overview .....	32
9.2. Third-party integration subsystems .....	32
9.3. Formatting TCP messages for BTX .....	32
9.4. Third-party Integration Example – Axis Device Events .....	33
10. Third-party Integrations – IronYun Vaidio Video Analytics .....	36
10.1. Vaidio Alert Configuration .....	36
10.2. Auto-Associate Vaidio cameras with XProtect cameras .....	38
10.3. Configure BTX to relay Vaidio alerts to XProtect .....	39
10.4. Create list specific actions for Vaidio License Plate Recognition (LPR) and Face Recognition detections. ....	42
11. BTX FAQ .....	45
12. Legal .....	46
12.1. Trademarks .....	46

---

12.2. Licenses and Copyrights.....	46
12.3. Surveillance Privacy.....	46
12.4. Disclaimer .....	46

## 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.
  - o 350MB disk space.
  - o 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.

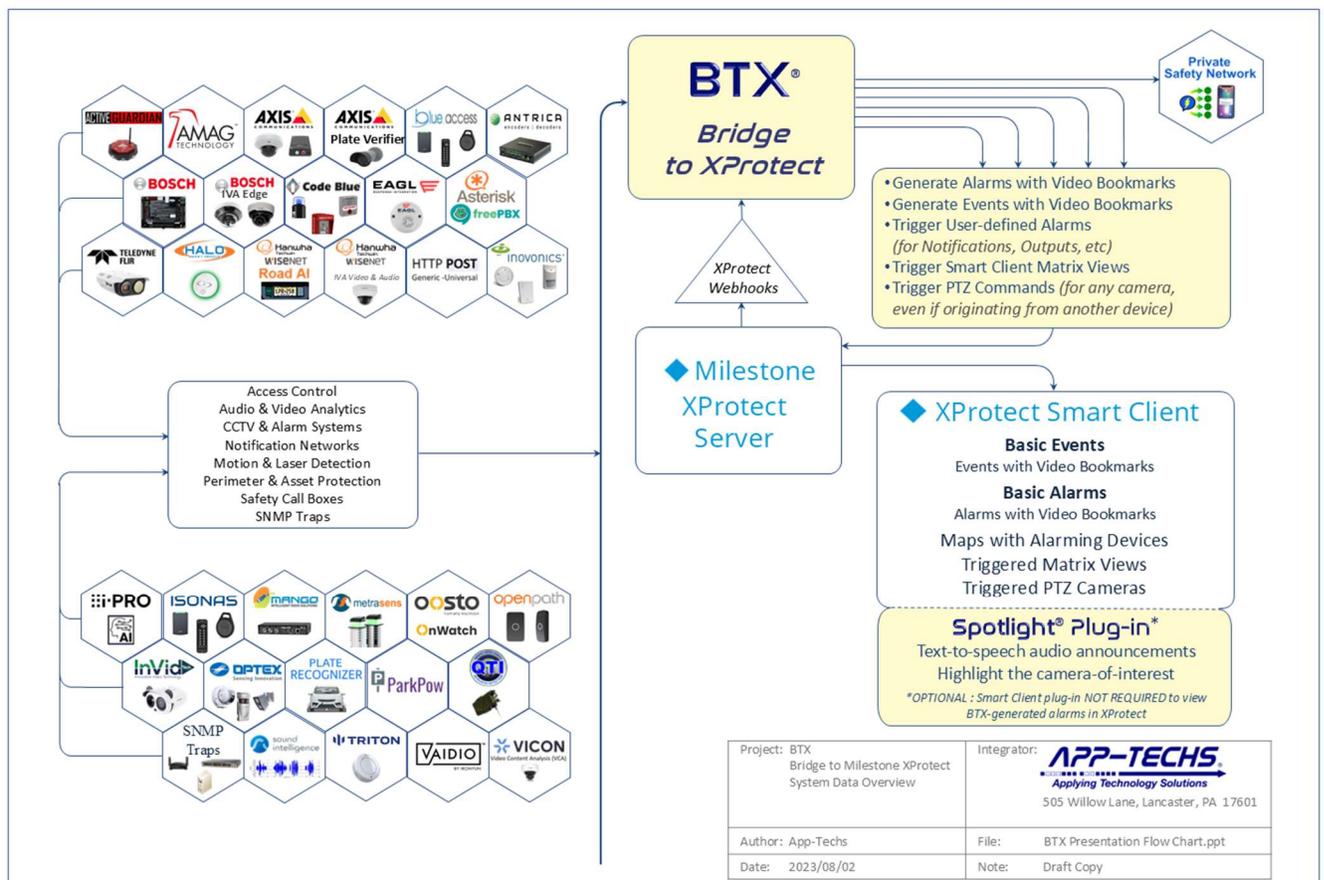
## 1.2. BTX Features

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 be 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

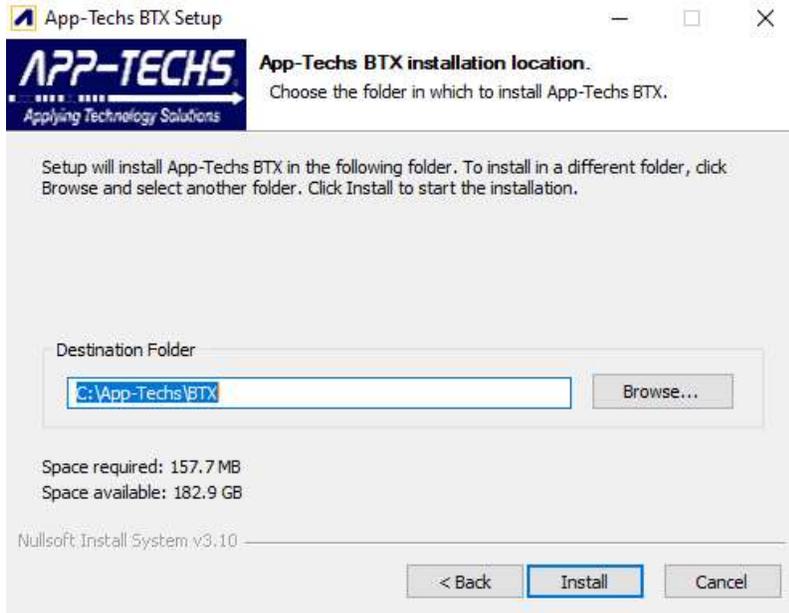
#### 3.1. BTX Server

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

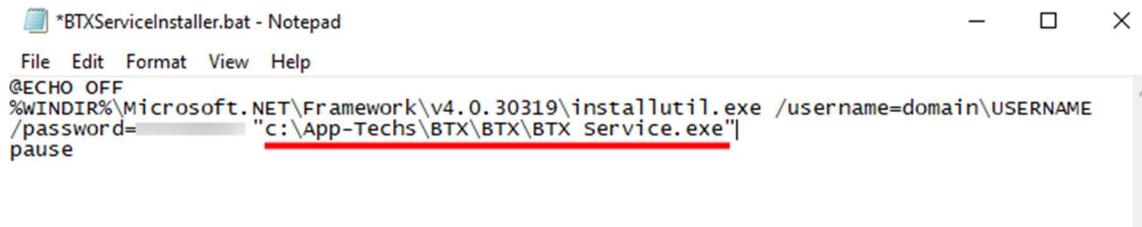
Navigate to the location of the directory where BTX was installed. Locate the file “BTXServiceInstaller.bat” in the BTX/BTX folder

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

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

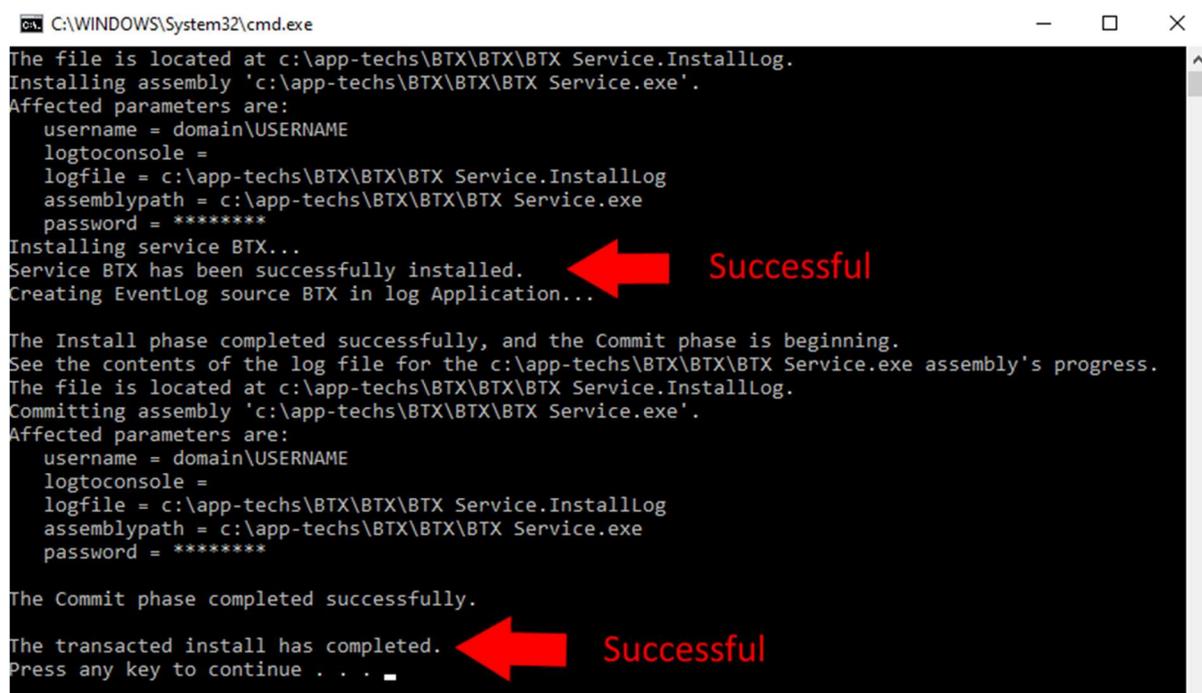


Below is an example:



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.

**Select your integrations:**

<input type="checkbox"/> Active Guardian Gunshot Detection	<input type="checkbox"/> Inovonics Wireless Sensors
<input type="checkbox"/> AMAG Access Control	<input type="checkbox"/> Metrasens Metal Detectors
<input type="checkbox"/> Axis Device Events	<input type="checkbox"/> Oosto Face Detection Analytics
<input type="checkbox"/> Axis Plate Verifier LPR	<input type="checkbox"/> ParkPOW Parking Management
<input type="checkbox"/> Bosch B-Series Panels (Mode2)	<input type="checkbox"/> Plate Recognizer LPR
<input type="checkbox"/> Code Blue Emergency Phones	<input type="checkbox"/> Teledyne FLIR Intrusion Analytics
<input type="checkbox"/> EAGL Gunshot Detection	<input type="checkbox"/> Teledyne FLIR TRK Encoders
<input type="checkbox"/> Halo Smart Sensors	<input type="checkbox"/> Triton Sensors
<input type="checkbox"/> Hanwha Wisenet RoadAI LPR	<input type="checkbox"/> Vaidio Video Analytics

**Milestone Configuration**

Milestone Server IP:   HTTPS

Milestone Username:   Basic Authentication

Milestone Password:

**OK**

#### 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”.

Milestone Configuration

Milestone Server IP: 127.0.0.1  HTTPS

Milestone Username: admin  Basic Authentication

Milestone Password: •••••

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.

Bridge to XProtect

Log View Devices Settings About

```
13:31:57: Using ini file at: C:\App-Techs\BTX\Third-party\BTXV2\Config.ini
13:31:57: Authenticating SDK.
13:31:58: Connected to the Configuration API.
13:31:58: SDK Authenticated.
13:31:58:
13:31:58: Fetching Cameras...
13:31:59: Fetching User Defined Events...
13:31:59: Fetching Matrices...
13:31:59: Listening on port 7227...
```

Clear Log Open Log File TCP Test SEND

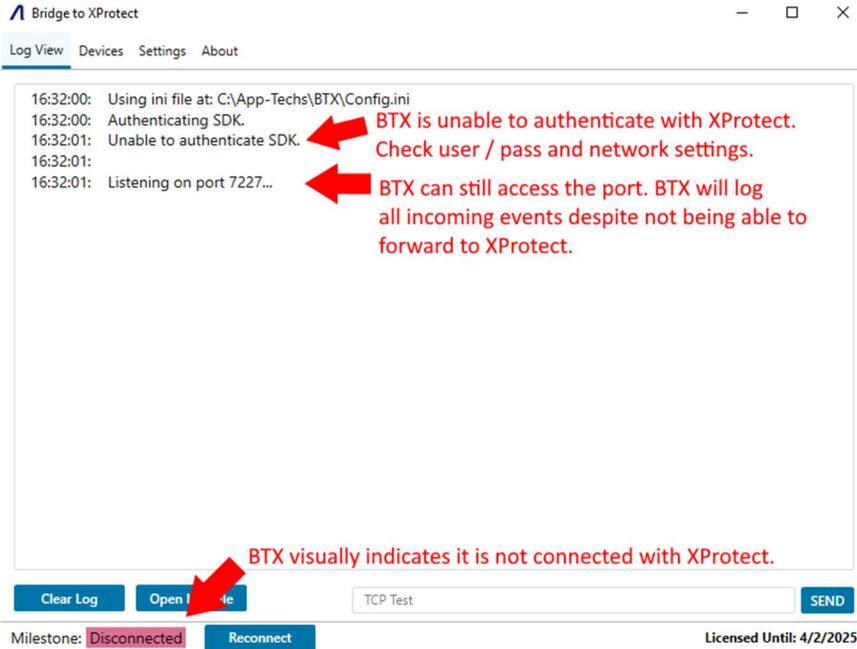
Milestone: Connected

Licensed Until: 3/27/2025

#### 4.4.2. XProtect Authentication Success – “Disconnected”

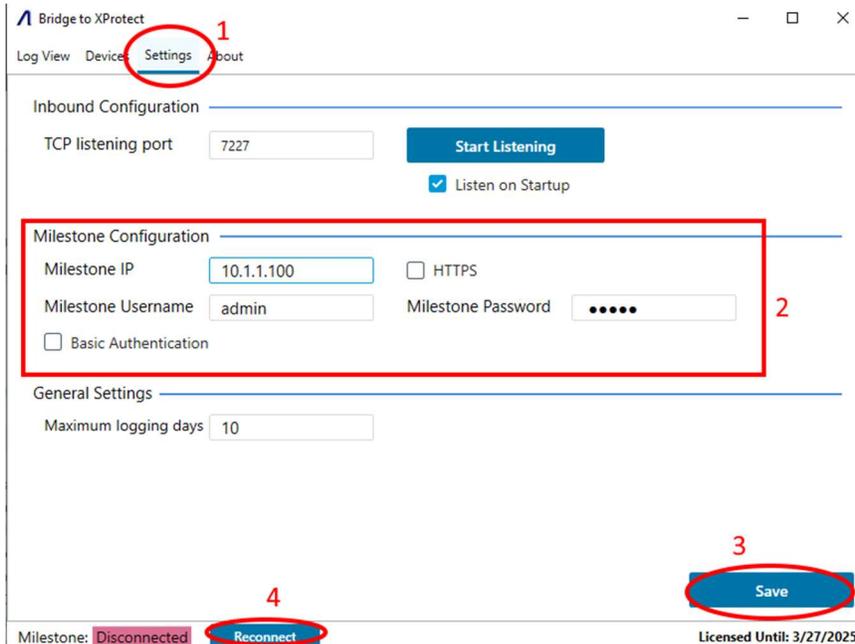
The BTX “Log View” provides information on BTX connectivity status.

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.

Bridge to XProtect

Log View Devices Settings About

```
14:28:13: Fetching User Defined Events...
14:28:13: Unable to fetch User Defined Events.
14:28:13: Fetching Matrices...
14:28:13: Unable to fetch Matrices.
15:05:16:
15:05:16: Authenticating SDK.
15:05:31: Unable to authenticate SDK.
15:05:31:
15:05:31: Fetching Cameras...
15:05:31: Fetching User Defined Events...
15:05:31: Unable to fetch User Defined Events.
15:05:31: Fetching Matrices...
15:05:31: Unable to fetch Matrices.
15:05:46:
15:05:46: Authenticating SDK.
15:05:47: Connected to the Configuration API.
15:05:47: SDK Authenticated.
15:05:47:
15:05:47: Fetching Cameras...
15:05:48: Fetching User Defined Events...
15:05:48: Fetching Matrices...
15:05:48: Listening on port 7227...
```

Clear Log Open Log File TCP Test SEND

Milestone: Connected Licensed Until: 3/27/2025

## 5. BTX Settings

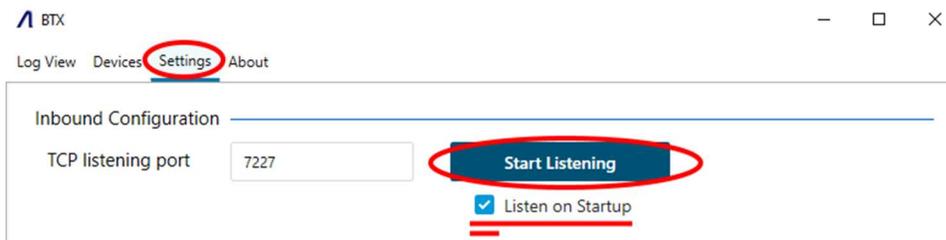
### 5.1. Inbound Configuration

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.

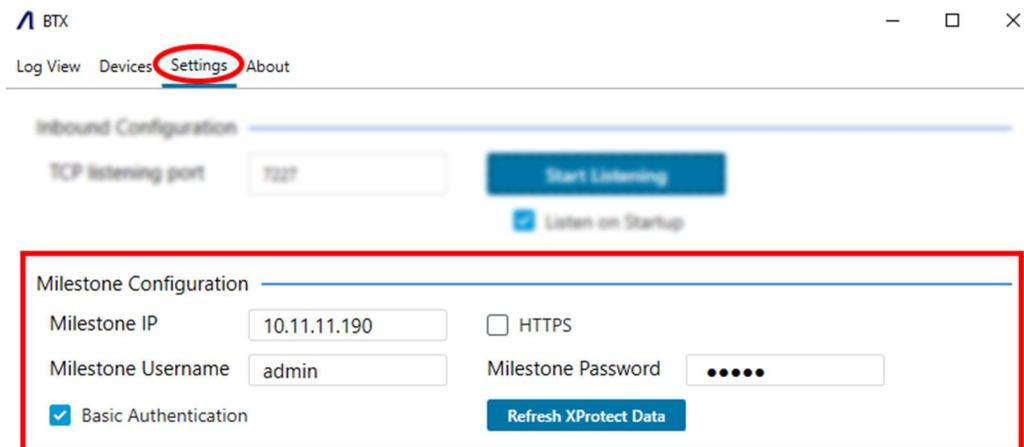
To start actively listening for events from third-party systems, click the “Start Listening” button.

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

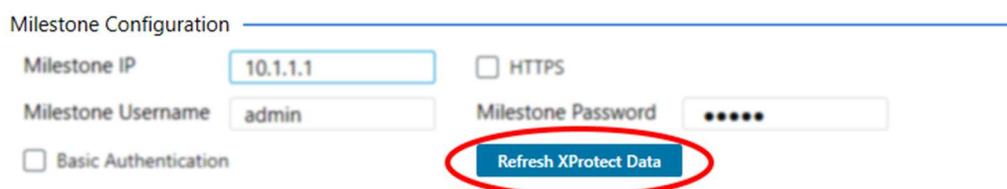
In the event the XProtect network address or user / pass has changed, update your server settings and click the “Save” button/



### 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.

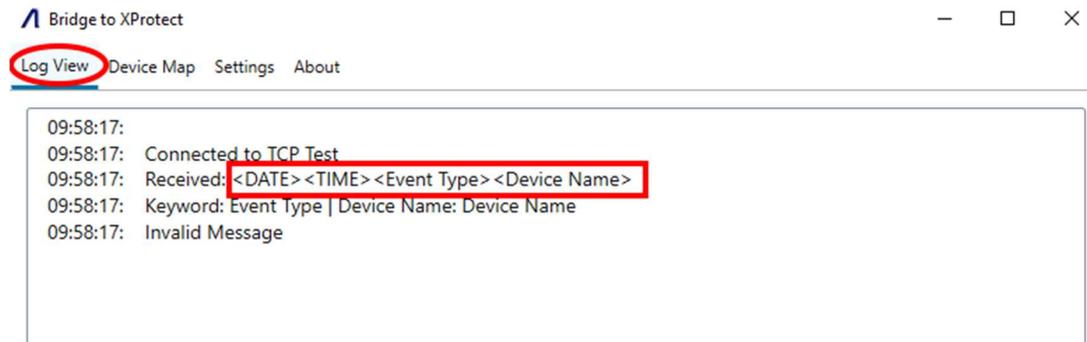
**Parameter #3:** <Event Type> - Reported event type.

**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.

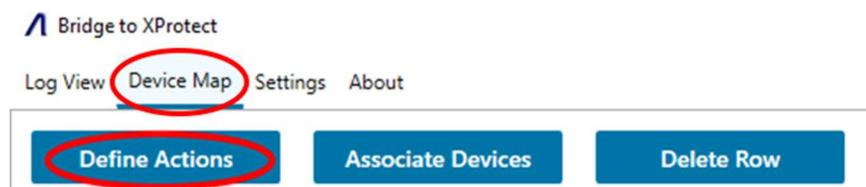
By requiring an **alarm keyword** match, BTX filters incoming messages based on type, identifying events of security interest while logging and ignoring banal or non-security-related events.

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.

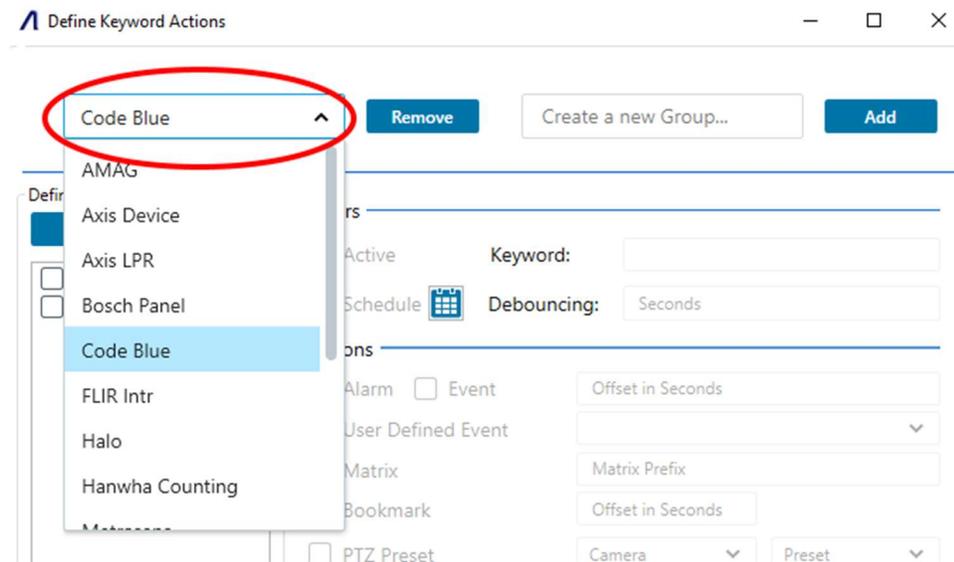
## 6.2. Define Alarm Actions.

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.

Code Blue [Remove] [Create a new Group...] [Add]

Define Keyword Actions [Add] [Remove]

- DIAL
- HANGUP

Filters

Active Keyword:

Schedule [Calendar Icon] Debounce:

Actions

Alarm  Event

User-Defined Event

Matrix

Bookmark

PTZ Preset

Data

Replacement Message

Appended Message

Associated Cameras

System Time  Map Guid

[Cancel] [Save]

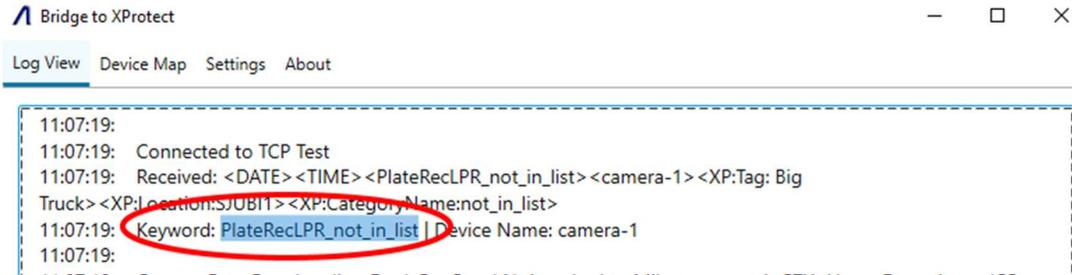
### 6.3.1. Alarm Keyword Specificity

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

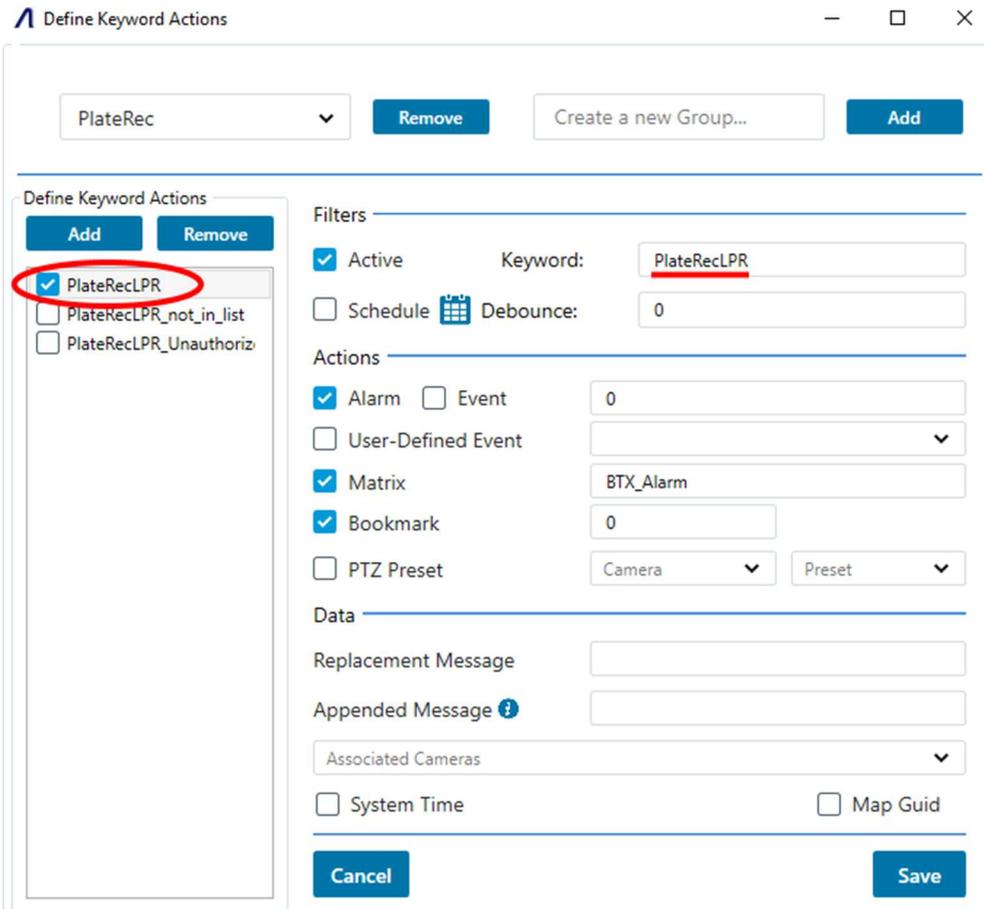
However, in some cases, defining a more specific alarm keyword can provide more granular control over what actions are taken in XProtect.

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.

**Filters**

Active      Keyword:

Schedule Debounce:

**Actions**

Alarm    Event     

User-Defined Event     

Matrix     

Bookmark     

PTZ Preset

**Data**

Replacement Message     

Appended Message     

Associated Cameras     

System Time       Map Guid

Cancel

Save

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.

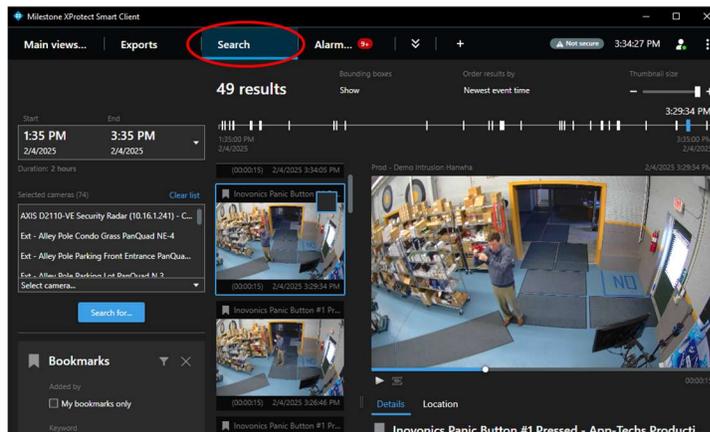
**Event** [Checkbox]: Generate a XProtect event record.

**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.



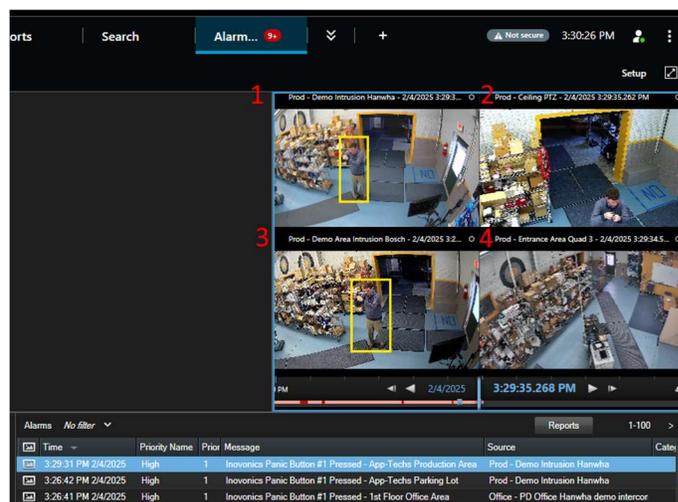
**PTZ Preset** [Checkbox + dropdown]: Option to trigger a PTZ preset on any PTZ camera when a keyword match occurs.

**Data:**

**Replacement Message** [Text field]: When generating a XProtect event / alarm record, 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.



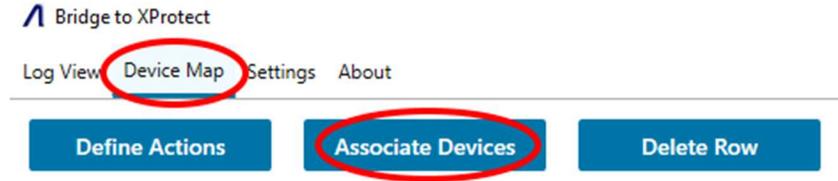
**System Time** [Checkbox]: Overwrite the event time reported by the device with the XProtect system time. This can be used to compensate for device time drift and other factors.

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

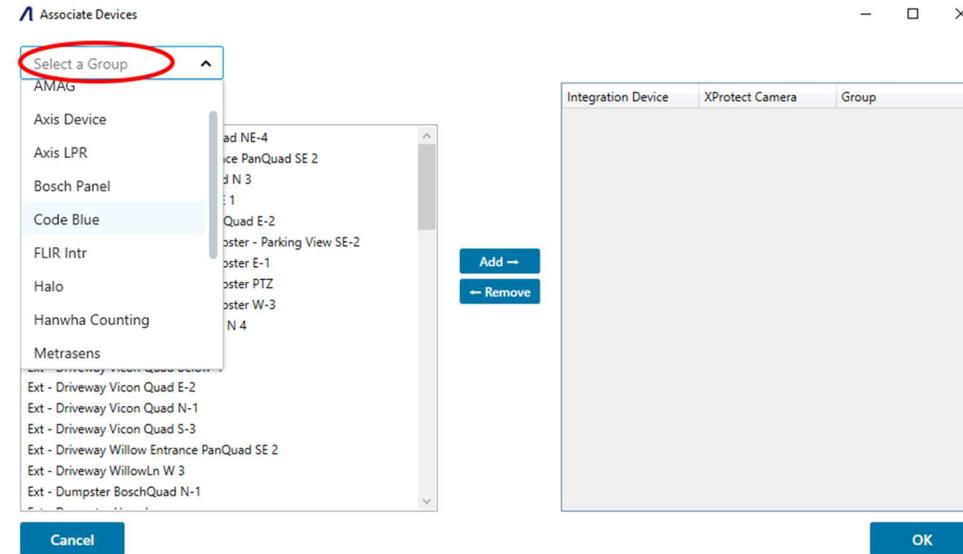
Click "Save" to save your settings for each defined keyword actions.

### 6.5. Associate Analytic Devices with Milestone Camera(s)

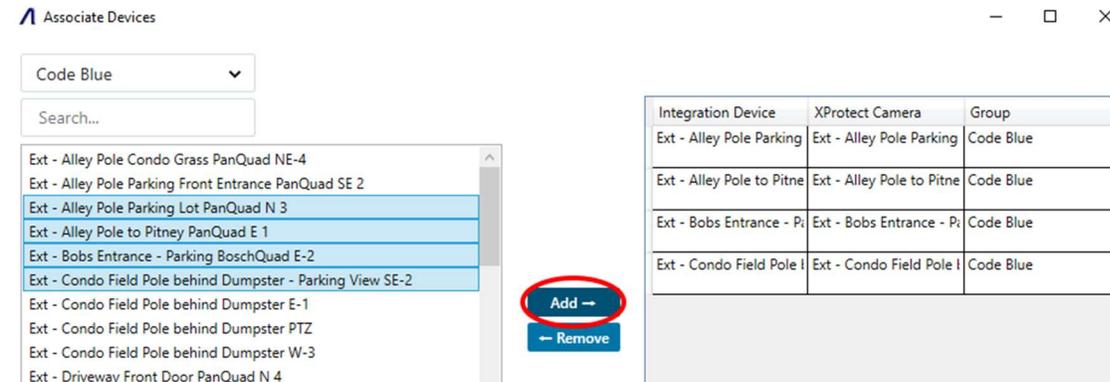
Go to the “Device Map” tab, and click the “Associate Actions” button:



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.

**Associate Devices**

Code Blue

Search XProtect Cameras...

- AXIS D2110-VE Security Radar (10.16.1.241) - Camera 1
- BWC-01 (B8A44F80910D) - Camera 1
- Ext - Alley Pole Condo Grass PanQuad NE-4
- Ext - Alley Pole Parking Front Entrance PanQuad SE 2
- Ext - Alley Pole Parking Lot PanQuad N 3
- Ext - Alley Pole to Pitney PanQuad E 1
- Ext - Bobs Entrance - Parking BoschQuad E-2
- Ext - Condo Field Pole behind Dumpster - Parking View SE-2
- Ext - Condo Field Pole behind Dumpster E-1
- Ext - Condo Field Pole behind Dumpster PTZ
- Ext - Condo Field Pole behind Dumpster W-3
- Ext - Driveway Front Door PanQuad N 4
- Ext - Driveway PanQuad E 1
- Ext - Driveway Vicon Quad Below-4
- Ext - Driveway Vicon Quad E-2
- Ext - Driveway Vicon Quad N-1
- Ext - Driveway Vicon Quad S-3
- Ext - Driveway Willow Entrance PanQuad SE 2

Add →

← Remove

Associate the 3rd-party device name with its XProtect camera by typing **HERE**

Integration Device	XProtect Camera	Group
Type 3rd-Party Device Name HERE	Ext - Alley Pole Parkin	Code Blue
CodeBlue102	Ext - Alley Pole to Pitn	Code Blue
CodeBlue103	Ext - Bobs Entrance - I	Code Blue
Codeblue104	Ext - Condo Field Pole	Code Blue

Cancel

OK

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.

Bridge to XProtect

Log View **Device Map** Settings About

Define Actions Associate Devices Delete Row Search... Code Blue

Found	Group	Active	Integration Device	XProtect Camera	GUID
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue101	Ext - Alley Pole to Pitney PanQuad E 1	f0bb6343-887c-43c7-8871-d8d7f52
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue102	Ext - Bobs Entrance - Parking BoschQuad E-2	0e4e733f-ed5f-4e4d-8d5b-bbdc44
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue103	Ext - Condo Field Pole behind Dumpster - Parking View SE-2	584a31d9-c051-4763-9c16-657776
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue104	Ext - Alley Pole Parking Lot PanQuad N 3	70ba2cef-01d1-4b30-8693-90c690

Keyword Actions

Add Remove

DIAL  
 HANGUP

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.

Bridge to XProtect

Log View **Device Map** Settings About

Define Actions Associate Devices Delete Row Search... Code Blue

Found	Group	Active	Integration Device	XProtect Camera	GUID
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue101	Ext - Alley Pole to Pitney PanQuad E 1	f0bb6343-887c-43c7-8871-d8d7f52
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue102	Ext - Bobs Entrance - Parking BoschQuad E-2	0e4e733f-ed5f-4e4d-8d5b-bbdc44
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue103	Ext - Condo Field Pole behind Dumpster - Parking View SE-2	584a31d9-c051-4763-9c16-657776
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue104	Ext - Alley Pole Parking Lot PanQuad N 3	70ba2cef-01d1-4b30-8693-90c690

Keyword Actions

Add Remove

DIAL  
 HANGUP

Filters

Active Keyword: DIAL

Schedule Debouncing: Seconds

Actions

Alarm  Event Offset in Seconds

User Defined Event

Matrix BTX\_Alarm

Bookmark Offset in Seconds

PTZ Preset Camera Preset

Data

Replacement Message

Appended Message

Associate Camera  System Time  Map Guid

Cancel Save

Milestone: Connected

Licensed Until: 4/2/2025

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.

The screenshot shows the Bridge to XProtect application window. The 'Log View' tab is active, displaying a log with the following entries:

```
14:05:09:
14:05:09: Connected to TCP Test
14:05:09: Received: <DATE><TIME><DIAL><CodeBlue 101>
14:05:09: Keyword: DIAL | Device Name: CodeBlue 101
14:05:09:
14:05:09: Alarm DIAL sent to Milestone.
14:05:10: Created Bookmark DIAL.
```

A red arrow points from the log entry to a text input field at the bottom of the window. The input field contains the text: `<DATE><TIME><DIAL><CodeBlue 101>`. A red circle highlights a 'SEND' button to the right of the input field.

Annotations in red text:

- Copy (CTRL-C) a previously received third-party event message.
- Paste (CTRL-V) to mimic the event without needing to physically trigger an event on the device.

At the bottom of the window, the status bar shows 'Milestone: Connected' and 'Licensed Until: 02/06/2030'.

## 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.

The screenshot shows the Bridge to XProtect application window. The 'Log View' tab is active, displaying a log entry for 12:02:59. The log text is as follows:

```

12:02:59:
12:02:59: Connected to TCP Test
12:02:59: Received: <01/03/2025> <07:37:26> <RoadAI_not_in_list> <EmergencyEntrance> <XP:Tag:US-PA SUV NONE Mercedes-Benz GL-Class
> <XP:Location:MNC8305> <XP:CategoryName:not_in_list>
12:02:59: Keyword: RoadAI_not_in_list | Device Name: EmergencyEntrance
12:02:59:
12:02:59: Triggered PTZ Preset home.
12:02:59: Alarm RoadAI_not_in_list_MNC8305 sent to Milestone.
12:02:59: User Defined Event BTX_LPR_Unauthorized Vehicle sent to Milestone.
12:02:59: Created Bookmark RoadAI_not_in_list_MNC8305.
12:02:59: Camera LPR - New Hanwha Demo pushed to Milestone matrix BTX_Alarm_DemoArea_155
12:02:59: Camera LPR - New Hanwha Demo pushed to Milestone matrix BTX_Alarm_148
12:02:59: Camera LPR - New Hanwha Demo pushed to Milestone matrix BTX_Alarm_Information - Push to SC on 134 (PD Workstation)
12:02:59: Camera LPR - New Hanwha Demo pushed to Milestone matrix BTX_Alarm - Push to 190
  
```

A red box highlights the actions taken in XProtect, starting from 'Triggered PTZ Preset home.' to 'Camera LPR - New Hanwha Demo pushed to Milestone matrix BTX\_Alarm - Push to 190'. A red arrow points to the 'Open Log File' button at the bottom of the interface, with the text 'The today's log file can be opened and evaluated by clicking here.' next to it.

Below the log view, the status is 'Milestone: Connected' and 'Licensed Until: 4/2/2025'. There are buttons for 'Clear Log' and 'Open Log File', and a search field containing 'nz GL-Class > <XP:Location:MNC8305> <XP:CategoryName:not\_in\_list>' with a 'SEND' button.

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

The screenshot shows the Bridge to XProtect application window. The 'Log View' tab is active, displaying a log entry for 12:12:22. The log text is as follows:

```

12:12:22:
12:12:22: Connected to TCP Test
12:12:22: Received: <01/03/2025> <07:37:26> <LPR_not_in_list> <EmergencyEntrance> <XP:Tag:US-PA SUV NONE Mercedes-Benz GL-Class
> <XP:Location:MNC8305> <XP:CategoryName:not_in_list>
12:12:22: Keyword: LPR_not_in_list | Device Name: EmergencyEntrance
12:12:22: Keyword LPR_not_in_list not found in device EmergencyEntrance's profiles
  
```

A red box highlights the final log entry: '12:12:22: Keyword LPR\_not\_in\_list not found in device EmergencyEntrance's profiles'.

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

The screenshot shows the Bridge to XProtect application window. The 'Log View' tab is active, displaying a log entry for 12:15:36. The log text is as follows:

```

12:15:36:
12:15:36: Connected to TCP Test
12:15:36: Received: <01/03/2025> <07:37:26> <Road_not_in_list> <DeviceTEST1> <XP:Tag:US-PA SUV NONE Mercedes-Benz GL-Class
> <XP:Location:MNC8305> <XP:CategoryName:not_in_list>
12:15:36: Keyword: Road_not_in_list | Device Name: DeviceTEST1
  
```

The device name 'DeviceTEST1' is underlined in the log entry.

### 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.

The screenshot displays the Milestone XProtect Smart Client interface. The top navigation bar includes '2 x 2 Alarm Testing', 'Exports', 'Search', and 'Alarm Manager 9+'. The main area is divided into several sections:

- Events Log:** A table listing events with columns for Time, Message, Source, and ID. A red arrow points to the entry '12:40:30 PM 1/3/2025 External Event' from 'BTX\_Code Blue Device 89'. A yellow callout box with the text 'User-defined Event triggered' is overlaid on this row.
- Alarms Log:** A table listing alarms with columns for Time, Message, Source, Owner, and ID. A red arrow points to the entry '12:40:31 PM 1/3/2025 Code Blue DIAL\_89' from 'Office - PD Axis Demo Cars'. A yellow callout box with the text 'Alarm record generated' is overlaid on this row.
- Map View:** A satellite map titled 'App-Techs\_floor\_plan2' showing a building layout. A red circle on the map is highlighted with a red arrow, and a yellow callout box with the text 'Map icon indicates alarm' is overlaid on it.
- Video Playback:** A video player showing a man in a light blue shirt holding a blue folder. A yellow callout box with the text 'View Video Bookmark' is overlaid on the video.

At the bottom of the interface, there are 'PLAYBACK' and 'LIVE' buttons.

## 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.

The screenshot shows the XProtect interface with the 'Device Map' tab selected. A table lists devices with columns for Found, Group, Active, Integration Device, XProtect Camera, and GUID. The 'Keyword Actions' panel on the right shows the configuration for the 'DIAL' keyword, with the 'Bookmark' option checked. The 'Filters' section shows 'Active' checked and 'Keyword' set to 'DIAL'. The 'Actions' section has 'Alarm' checked and 'Event' unchecked. The 'Data' section has 'Replacement Message' and 'Appended Message' fields.

Found	Group	Active	Integration Device	XProtect Camera	GUID
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	89	Office - PD Axis Demo Camera	2cc1d115-99d0-4099-
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue101	Ext - Alley Pole to Pitney PanQuad E 1	f0bb6343-887c-43c7-
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue102	Ext - Bobs Entrance - Parking BoschQuad E-2	0e4e733f-ed5f-4e4d-
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue103	Ext - Condo Field Pole behind Dumpster - Parking View SE-2	584a31d9-c051-4763-
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue104	Ext - Alley Pole Parking Lot PanQuad N 3	70ba2cef-01d1-4630-

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.

The screenshot shows the XProtect Smart Client search interface. The 'Search' tab is selected, and the search results show 4 results. The search criteria are 'Code Blue DIAL\_89'. The search results are displayed as a list of cameras and a video thumbnail. The 'Bookmarks' option is selected in the search filter, and the 'New search' button is highlighted.

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.

The screenshot displays the Milestone XProtect Smart Client interface. At the top, the 'Search' tab is highlighted with a red circle. Below the navigation bar, the search results section shows '4 results' for a time range from 10:58 AM to 12:58 PM on 1/3/2025. A list of selected cameras is visible on the left. A 'Bookmarks' overlay is shown in the bottom-left corner, with a red arrow pointing to the 'Keyword' field containing '89'. A yellow callout box on the right explains that this field uses CONTAINS logic for partial keyword matches.

**Search for BTX-generated bookmarks by typing the alarm keyword here.**

**This field uses CONTAINS logic, so a partial keyword match is sufficient.**

## 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.

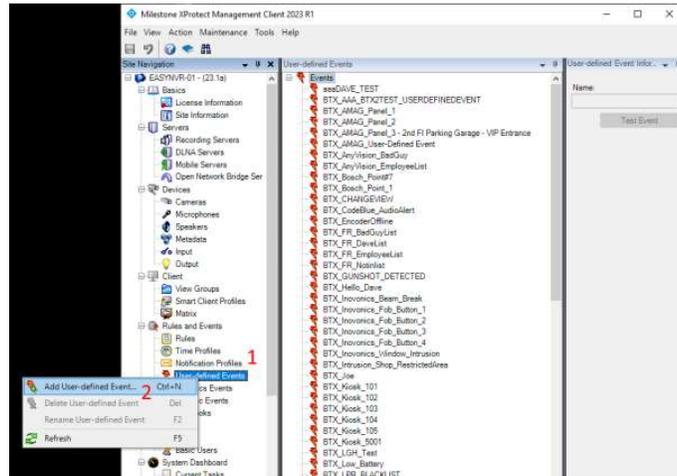
### 8.2. Trigger XProtect User-defined events.

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.

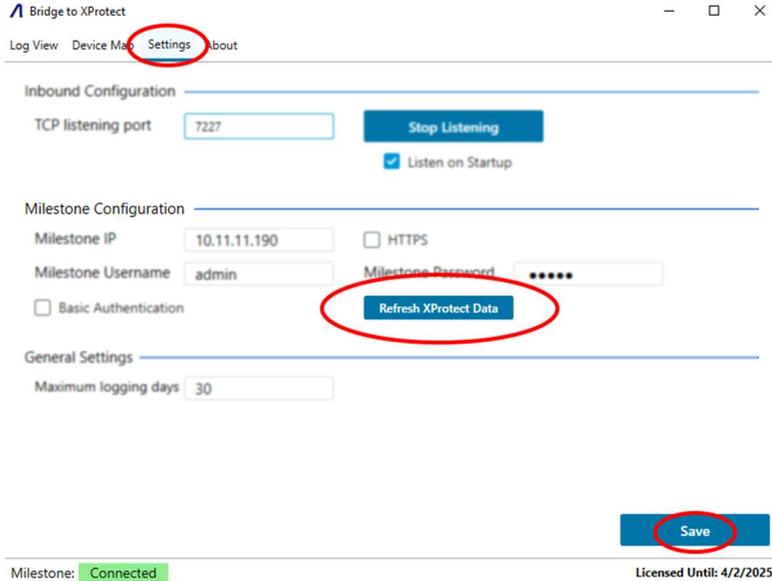


Be sure to click “Save” in XProtect.

### 8.2.2. Refresh Management Server Configuration in BTX.

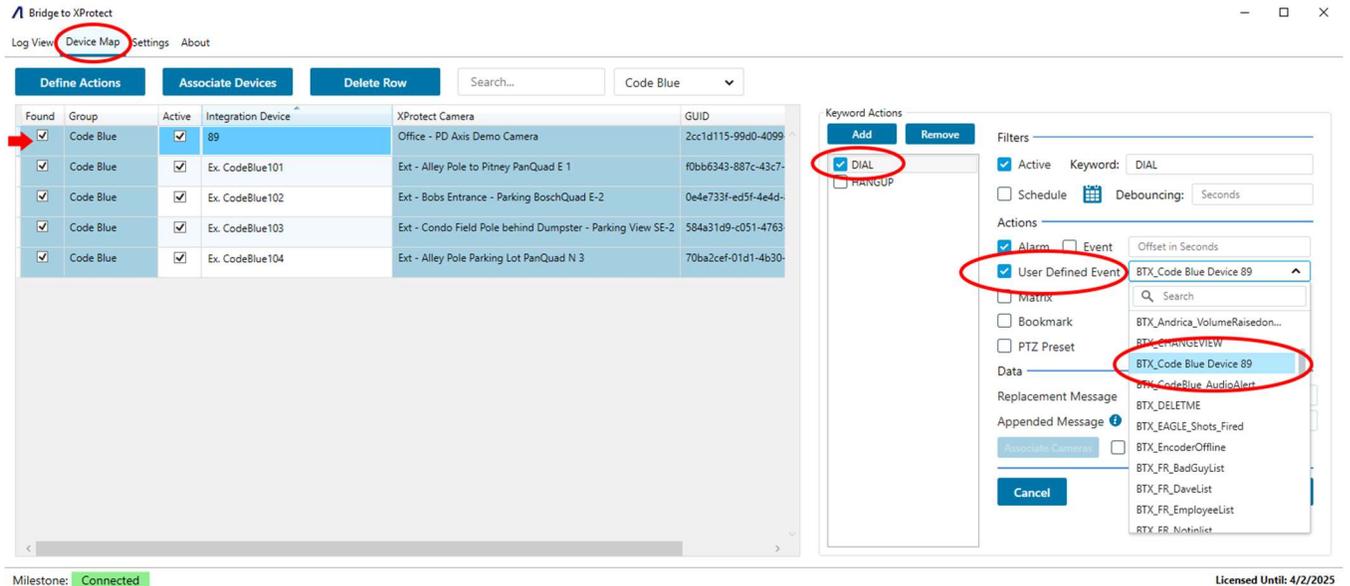
If you create new User-defined events in the XProtect Management Client, BTX must be re-refreshed to update its stored information.

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:



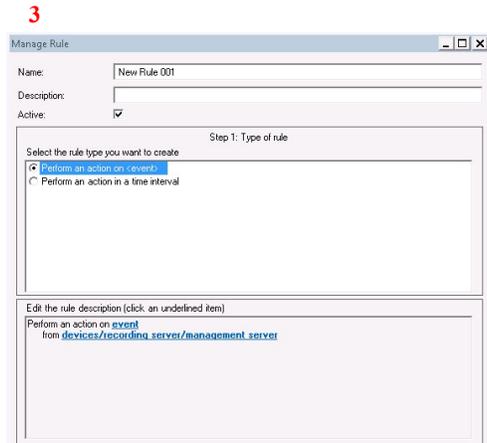
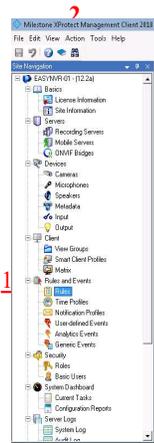
### 8.3.1. Trigger Action in XProtect using XProtect Rules

#### 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....

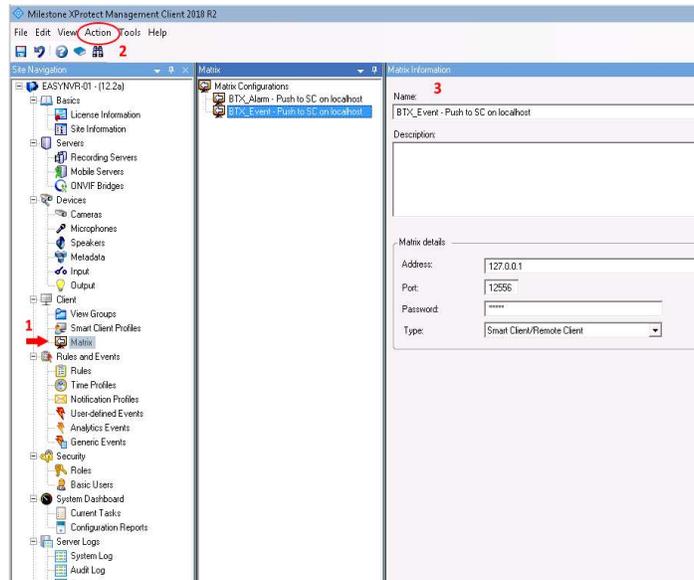
3 Follow the steps in the Manage Rule tool to create a rule that associates any specified User-defined Event with a desired action.



## 8.4. Trigger XProtect Live Matrix Views

To configure a Matrix Display in XProtect:

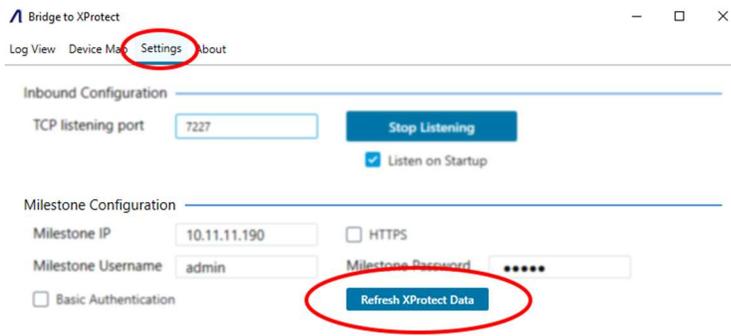
- 1 In the XProtect Management Client, go to the Site Navigation bar on the left-hand side toolbar and select *Matrix*.
- 2 From the file menu, select Action → Add Matrix....
- 3 Save Settings in XProtect.



### 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.

The screenshot shows the 'Bridge to XProtect' software interface. The 'Device Map' tab is active, displaying a table of devices. A red arrow points to the first row of the table. The 'Keyword Actions' panel on the right is open, showing the configuration for a 'DIAL' keyword. The 'Matrix' action is selected, and the 'Matrix' field is set to 'BTX\_Alarm'. The 'Save' button is circled in red.

Found	Group	Active	Integration Device	XProtect Camera	GUID
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	89	Office - PD Axis Demo Camera	2cc1d
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue101	Ext - Alley Pole to Pitney PanQuad E 1	f0bb6
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue102	Ext - Bobs Entrance - Parking BoschQuad E-2	0e4e7
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue103	Ext - Condo Field Pole behind Dumpster - Parking View SE-2	584a3
<input checked="" type="checkbox"/>	Code Blue	<input checked="" type="checkbox"/>	Ex. CodeBlue104	Ext - Alley Pole Parking Lot PanQuad N 3	70ba2

Keyword Actions:

- DIAL
- HANGUP

Filters:

- Active Keyword: DIAL
- Schedule
- Debouncing: Seconds

Actions:

- Alarm
- Event
- User Defined Event: BTX Code Blue Camera 89
- Matrix: BTX\_Alarm
- Bookmark
- PTZ Preset

Data:

- Replacement Message
- Appended Message: [Source]
- System Time
- Map Guid

Buttons: Cancel, Save

Milestone: Connected Licensed Until: 4/2/2025

## 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”

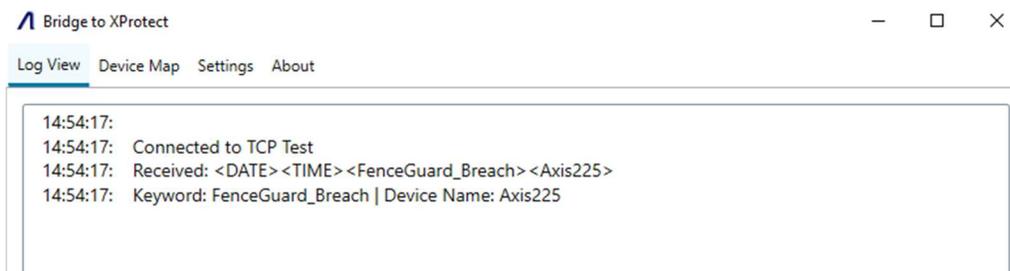
AXIS P3225-LV Mk II Network Camera

The screenshot shows the configuration interface for an Axis P3225-LV Mk II Network Camera. The 'Rules' tab is selected and circled with a red '3'. A rule named 'To BTX' is configured with the following settings:

- Use this rule:** Checked
- Name:** To BTX
- Wait between actions (max 23:59:59):** 00:00:00
- Condition:** Fence Guard: Any Profile
- Action:** Send notification through TCP (circled with a red '4')
- Recipient:** BTX 190 (circled with a red '4')
- Message:** <DATE><TIME><FenceGuard\_Breach><Axis225> (circled with a red '4')

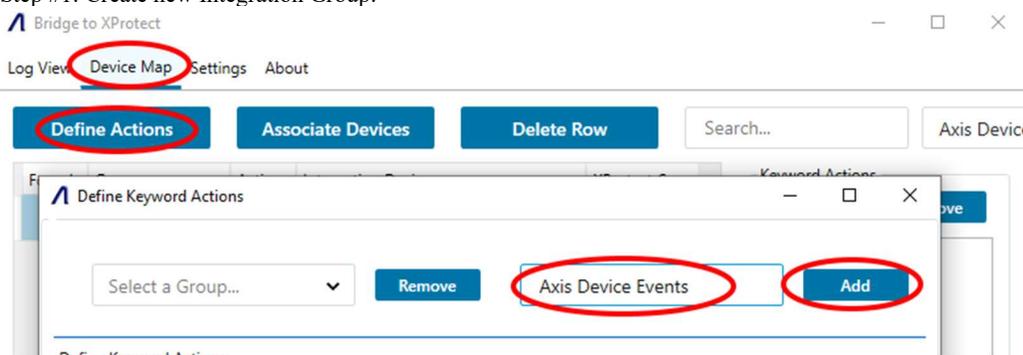
At the bottom of the interface, the 'System' menu is circled with a red '1', and the 'Events' icon is circled with a red '2'.

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

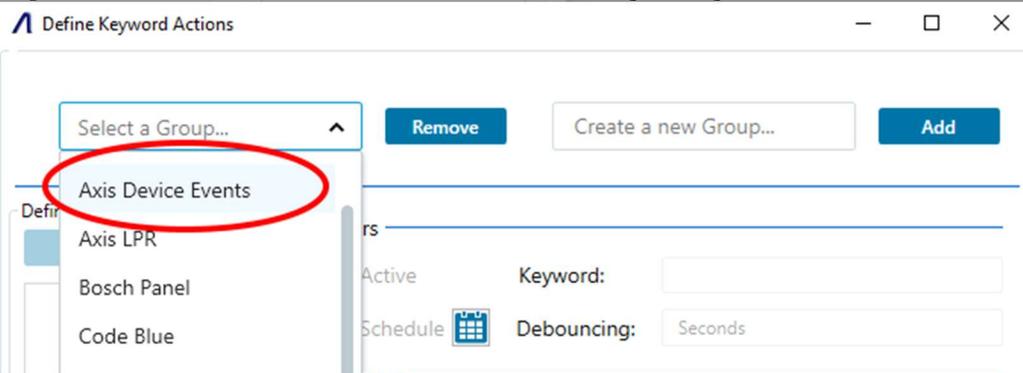


With the alarm keyword: “FenceGuard\_Breach” and device name: “Axis 225”, BTX can easily be configured to integrate this Axis device event with XProtect.

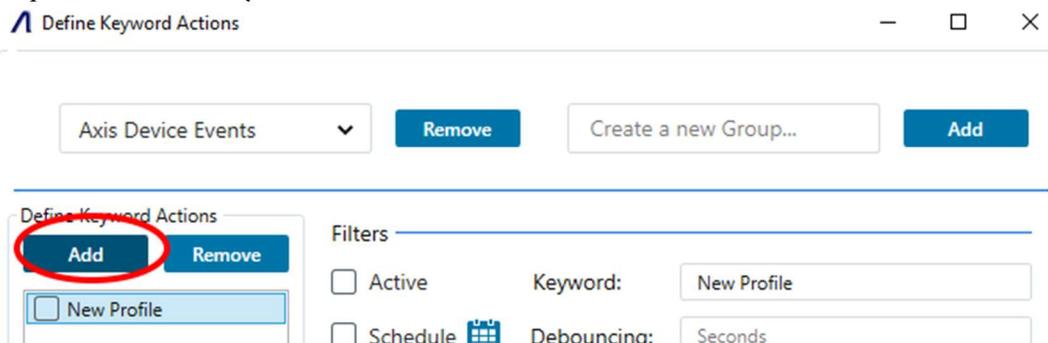
Step #1: Create new Integration Group.



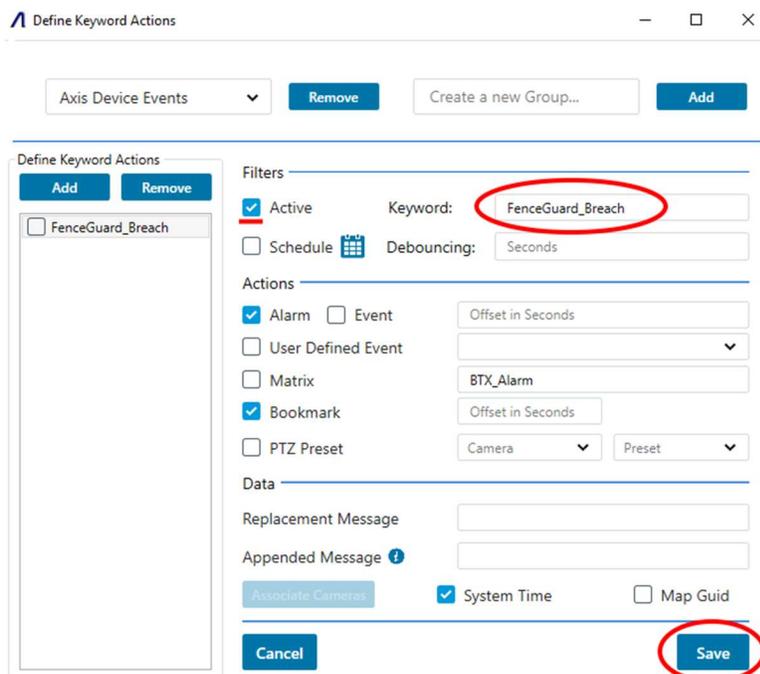
Step #2: Select the “Axis Device Events” from the “Select a Group ...” dropdown menu.



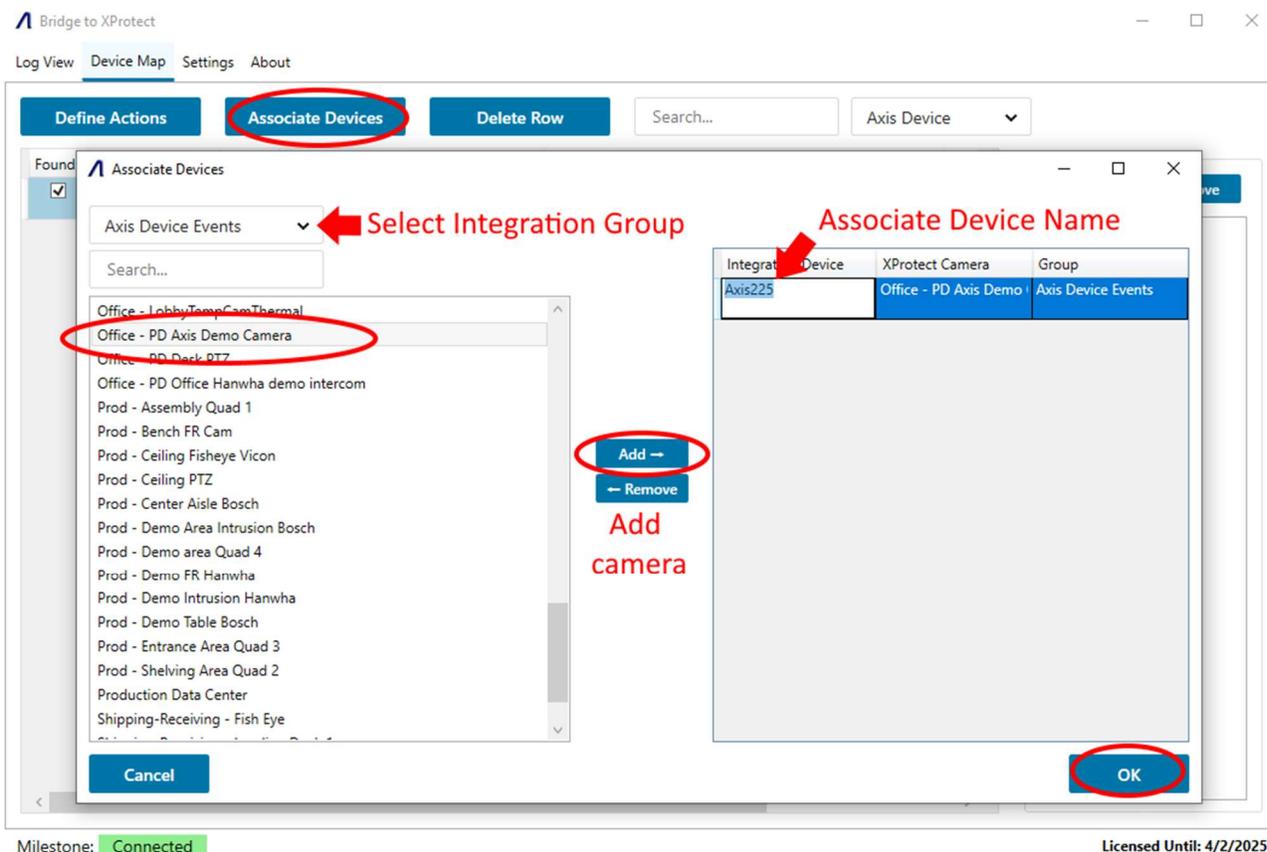
Step #3: Define a new Keyword Action.



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.

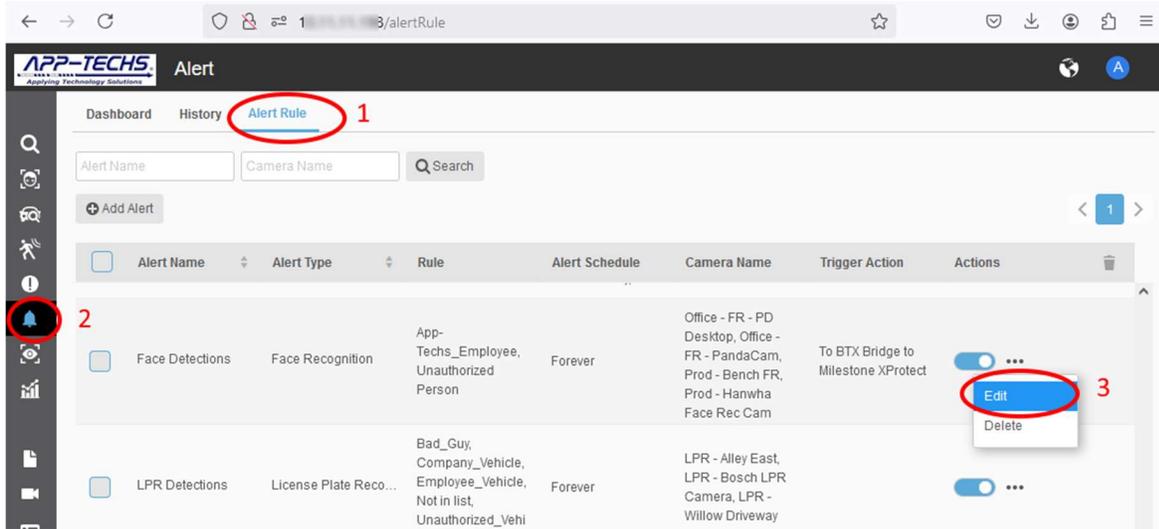


## 10. Third-party Integrations – IronYun Vaidio Video Analytics

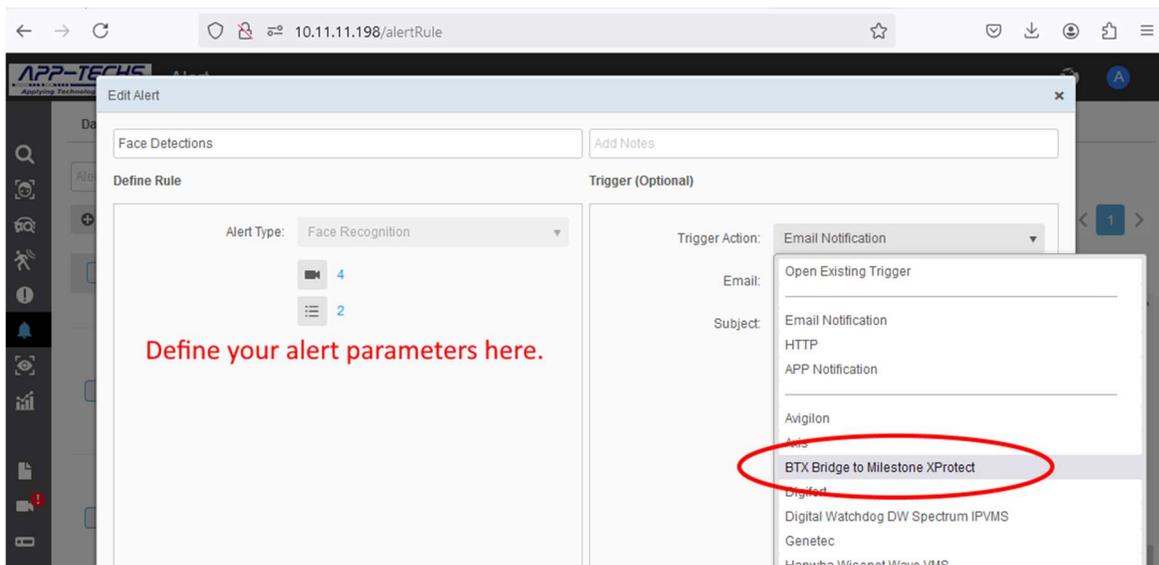
BTX serves as the middleware to relay Vaidio live analytics alerts to Milestone XProtect. Users have ample control over what actions are taken in Milestone XProtect when a Vaidio alert-of-interest occurs.

### 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.



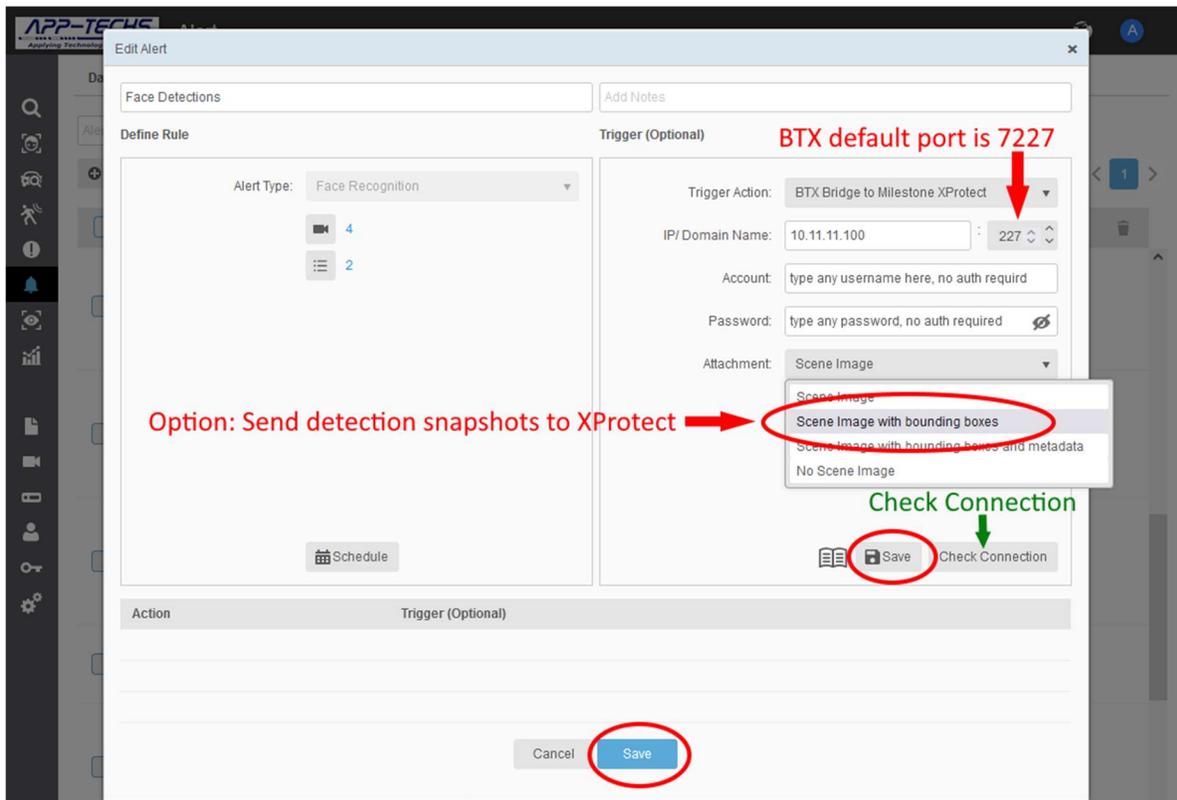
After configuring your preferred alert parameters, select “BTX Bridge to XProtect” from the “Trigger Action:” dropdown menu.



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.



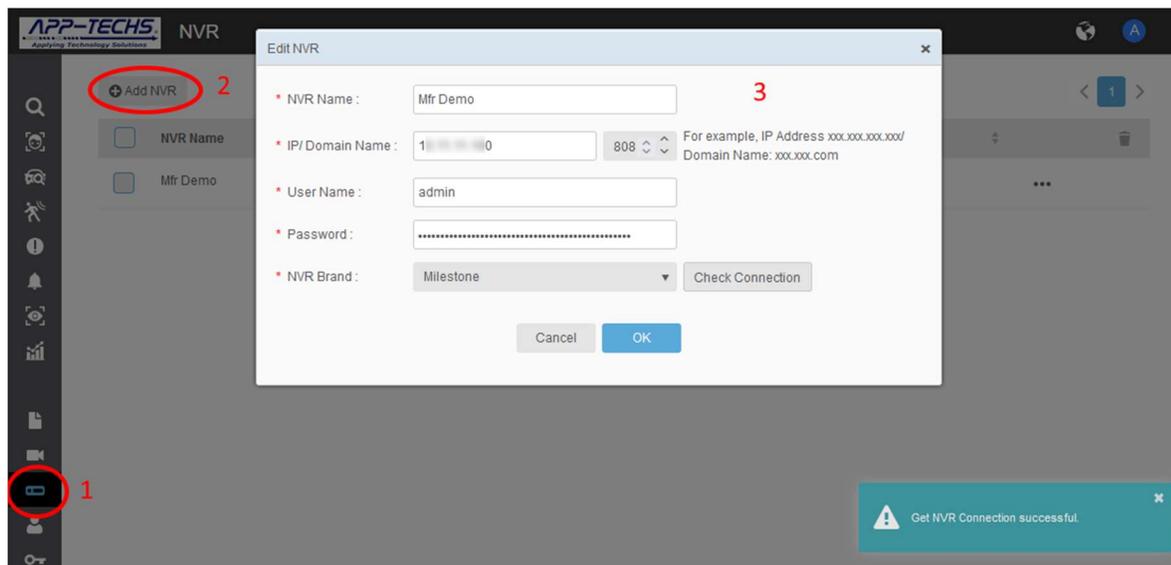
When “Check Connection” test succeeds, Vaidio alerts will be received by BTX.

## 10.2. Auto-Associate Vaidio cameras with XProtect cameras.

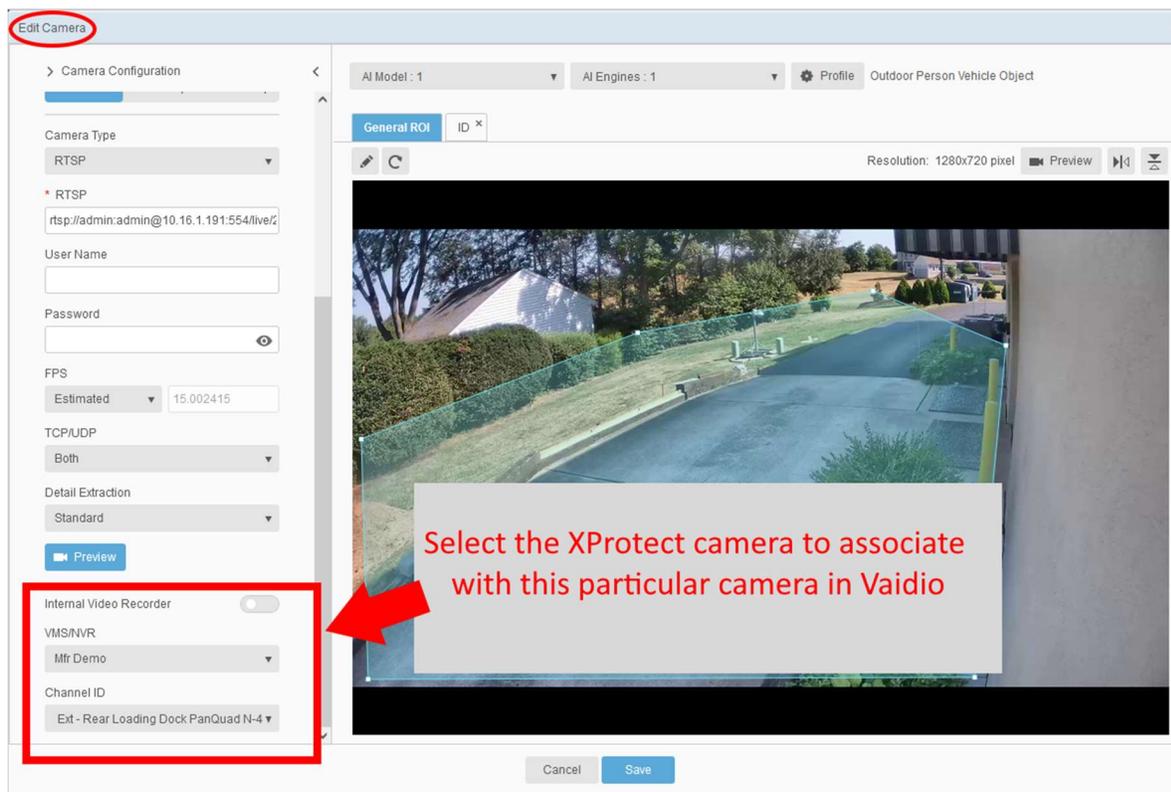
If the XProtect system has an active Mobile Server Service, a user can associate a Vaidio camera with its XProtect counterpart within the Vaidio UI.

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.

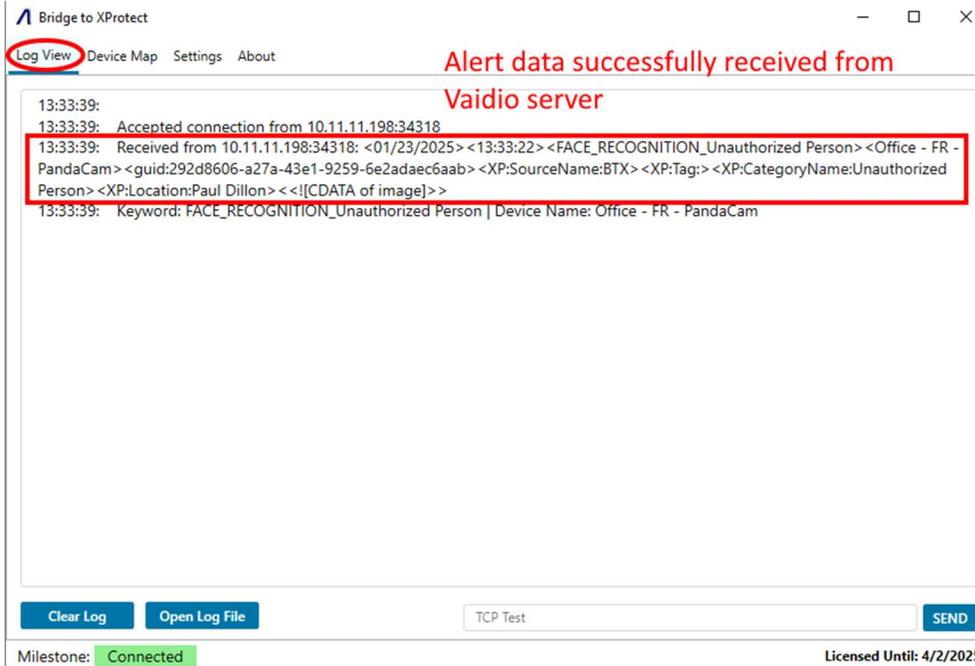


Step #2: In the Vaidio “Edit Cameras” menu, use the left-hand tool bar to select a XProtect camera to associate with the Vaidio camera. Complete this step for each camera in the Vaidio system.



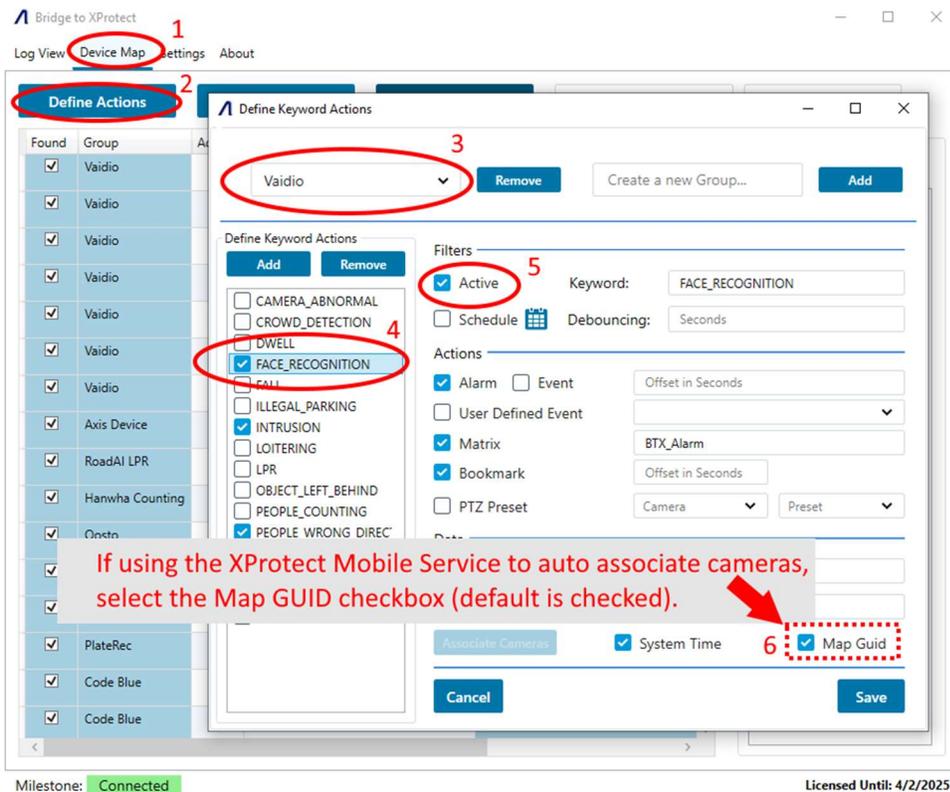
### 10.3. Configure BTX to relay Vaidio alerts to XProtect.

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



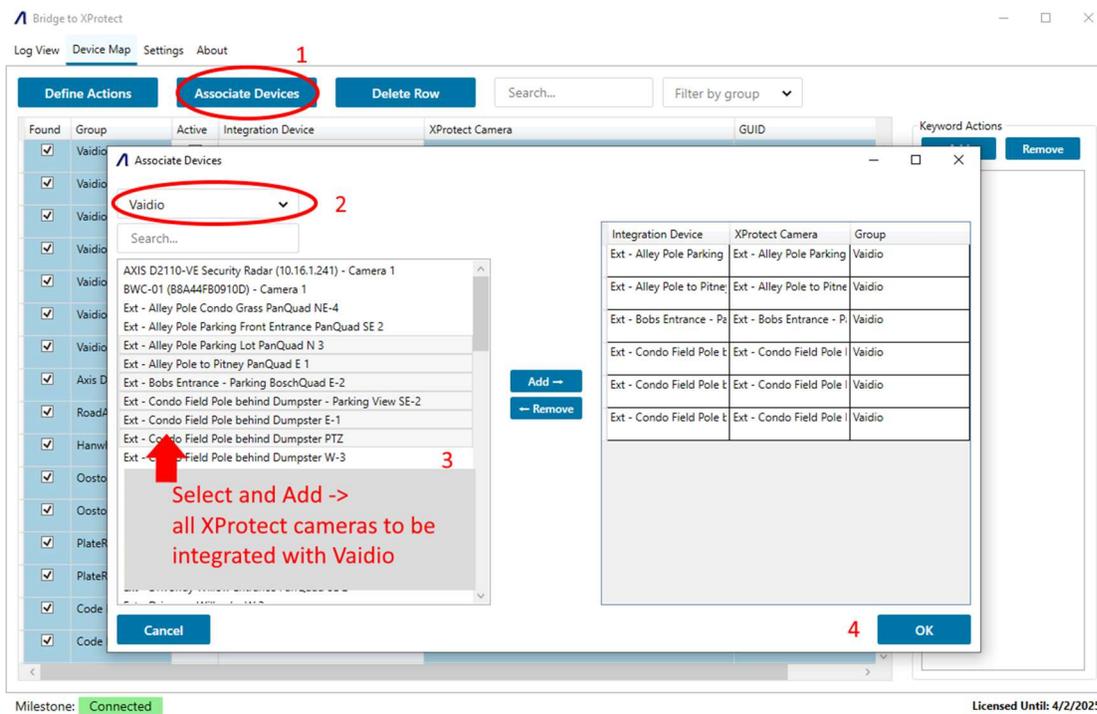
Go to the “Device Map” tab and select “Define Actions.” From the “Select a Group” dropdown menu, choose “Vaidio.”

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.

**Associate Devices**

Vaidio

Search...

- AXIS D2110-VE Security Radar (10.16.1.241) - Camera 1
- BWC-01 (B8A44FB0910D) - Camera 1
- Ext - Alley Pole Condo Grass PanQuad NE-4
- Ext - Alley Pole Parking Front Entrance PanQuad SE 2
- Ext - Alley Pole Parking Lot PanQuad N 3
- Ext - Alley Pole to Pitney PanQuad E 1
- Ext - Bobs Entrance - Parking BoschQuad E-2
- Ext - Condo Field Pole behind Dumpster - Parking View SE-2
- Ext - Condo Field Pole behind Dumpster E-1
- Ext - Condo Field Pole behind Dumpster PTZ
- Ext - Condo Field Pole behind Dumpster W-3
- Ext - Driveway Front Door PanQuad N 4
- Ext - Driveway PanQuad E 1
- Ext - Driveway Vicon Quad Below-4
- Ext - Driveway Vicon Quad E-2
- Ext - Driveway Vicon Quad N-1
- Ext - Driveway Vicon Quad S-3
- Ext - Driveway Willow Entrance PanQuad SE 2

**Type camera name as entered in Vaidio HERE**

Integration Device	XProtect Camera	Group
VaidioDevice001	Ext - Alley Pole Parking Lot P	Vaidio
Ext - Alley Pole to Pitney PanC	Ext - Alley Pole to Pitney Pan	Vaidio
Ext - Bobs Entrance - Parking	Ext - Bobs Entrance - Parking	Vaidio
Ext - Condo Field Pole behind	Ext - Condo Field Pole behin	Vaidio
Ext - Condo Field Pole behind	Ext - Condo Field Pole behin	Vaidio
Ext - Condo Field Pole behind	Ext - Condo Field Pole behin	Vaidio

Buttons: Add →, ← Remove, Cancel, OK

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”

Define Keyword Actions

Vaidio Remove Create a new Group... Add

Define Keyword Actions

Add Remove

- CAMERA\_ABNORMAL
- CROWD\_DETECTION
- DWELL
- FACE\_RECOGNITION
- FACE\_RECOGNITION\_Unauthorized
- FALL
- ILLEGAL\_PARKING
- INTRUSION

Filters

Active Keyword: FACE\_RECOGNITION\_Unauthorized

Schedule Debounce: Seconds

Actions

Alarm  Event Offset in Seconds

User-Defined Event

Matrix BTX\_Alarm

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.**

Define Keyword Actions

Vaidio [Remove] Create a new Group... [Add]

Define Keyword Actions

**Filters**

Active Keyword: FACE\_RECOGNITION\_Employee

Schedule Debouncing: Seconds

**Actions**

Alarm  Event Offset in Seconds

User Defined Event BTX\_FR\_EmployeeList

Matrix BTX\_Alarm

Bookmark Offset in Seconds

PTZ Preset Camera Preset

**Data**

Define Keyword Actions

CAMERA\_ABNORMAL

CROWD\_DETECTION

DWELL

FACE\_RECOGNITION

FACE\_RECOGNITION\_Em

FACE\_RECOGNITION\_Un

FALL

ILLEGAL\_PARKING

INTRUSION

LOITERING

LPR

PEOPLE\_COUNTING

PEOPLE\_WRONG\_DIREC

**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.”**

Define Keyword Actions

Vaidio [Remove] Create a new Group... [Add]

Define Keyword Actions

**Filters**

Active Keyword: FACE\_RECOGNITION\_Unauthorized

Schedule Debouncing: Seconds

**Actions**

Alarm  Event Offset in Seconds

User Defined Event BTX\_FR\_BadGuyList

Matrix BTX\_Alarm

Bookmark Offset in Seconds

PTZ Preset Camera Preset

**Data**

Define Keyword Actions

CAMERA\_ABNORMAL

CROWD\_DETECTION

DWELL

FACE\_RECOGNITION

FACE\_RECOGNITION\_Em

FACE\_RECOGNITION\_Un

FALL

ILLEGAL\_PARKING

INTRUSION

LOITERING

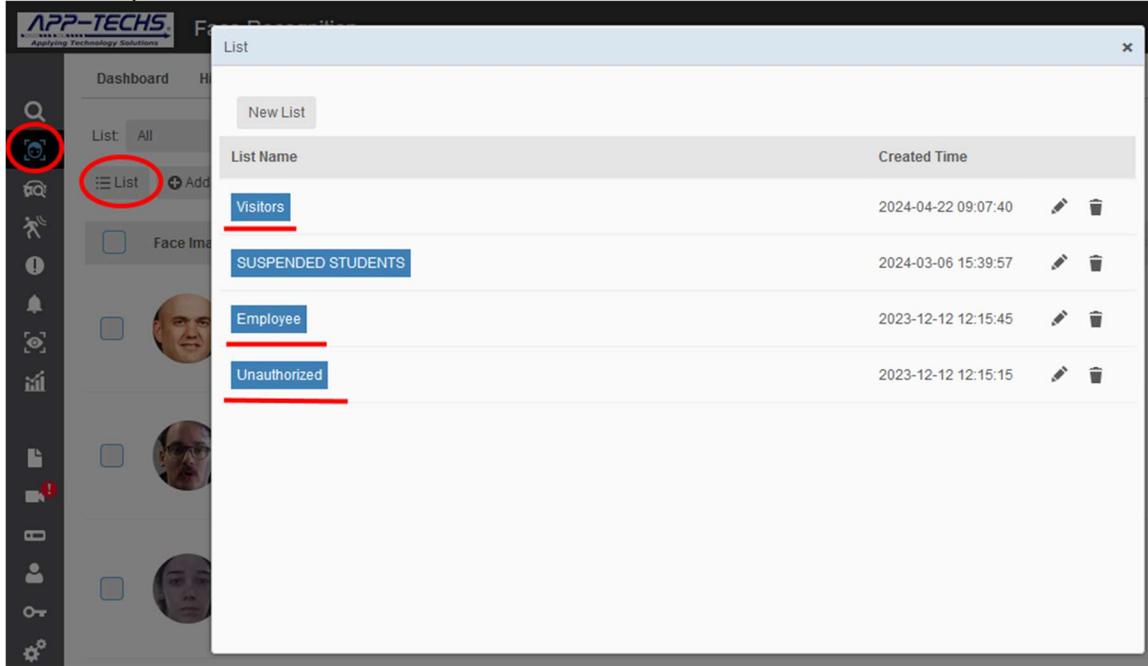
LPR

PEOPLE\_COUNTING

PEOPLE\_WRONG\_DIREC

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

Copyright © 2012 App-Techs Corp., First Edition, First Printing: October 2011

All rights reserved. No part of this publication may be stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of App-Techs, Corp. This document is printed in the United States of America.

DMap, EasyNVR and the App-Techs logo are trademarks of App-Techs, Corp. All other trademarks, trade names, company names and product names contained in this document are registered trademarks or trademarks of their respective owners.

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.