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!"

June 2023

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

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

Summary

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

Table of Contents

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

1. System Overview

BTX™ (Bridge to Milestone XProtect) is a middleware application. It monitors real-time event and alarm data streams from third-party systems such as Video Analytics, Access Control, Sensors, Security and Building Automation, SIP phone systems, and software applications.

BTX analyzes incoming data, then based on user-defined rules and schedules, transforms that data into XProtect to ...

- Generate Alarms with Video Bookmarks.
- Generate Events with Video Bookmarks.
- Trigger User-defined Alarms. (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)

BTX stores and tags the originating event and alarm data, along with relevant metadata, in the XProtect database.

With BTX, XProtect becomes a “single-pane of glass” to monitor a wide variety to security systems while serving as a repository database for pertinent third-party security data. Smart Client operators can readily access third-party metadata by using event / alarm search filters or the XProtect “Reports” feature.

BTX improves situational awareness in *real-time* by making alarms from third-party systems *pop* in Milestone XProtect, while also capturing important data to improve video surveillance review and analysis.

1.1. System Requirements

The BTX system requirements are conventional and lightweight.

- Windows 10. **Windows 7 version available for older versions of XProtect.*
- BTX is lightweight software - low disk usage / low RAM consumption / minimal CPU usage.
  - 350MB disk space.
  - 50MB 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 current with latest versions of XProtect.

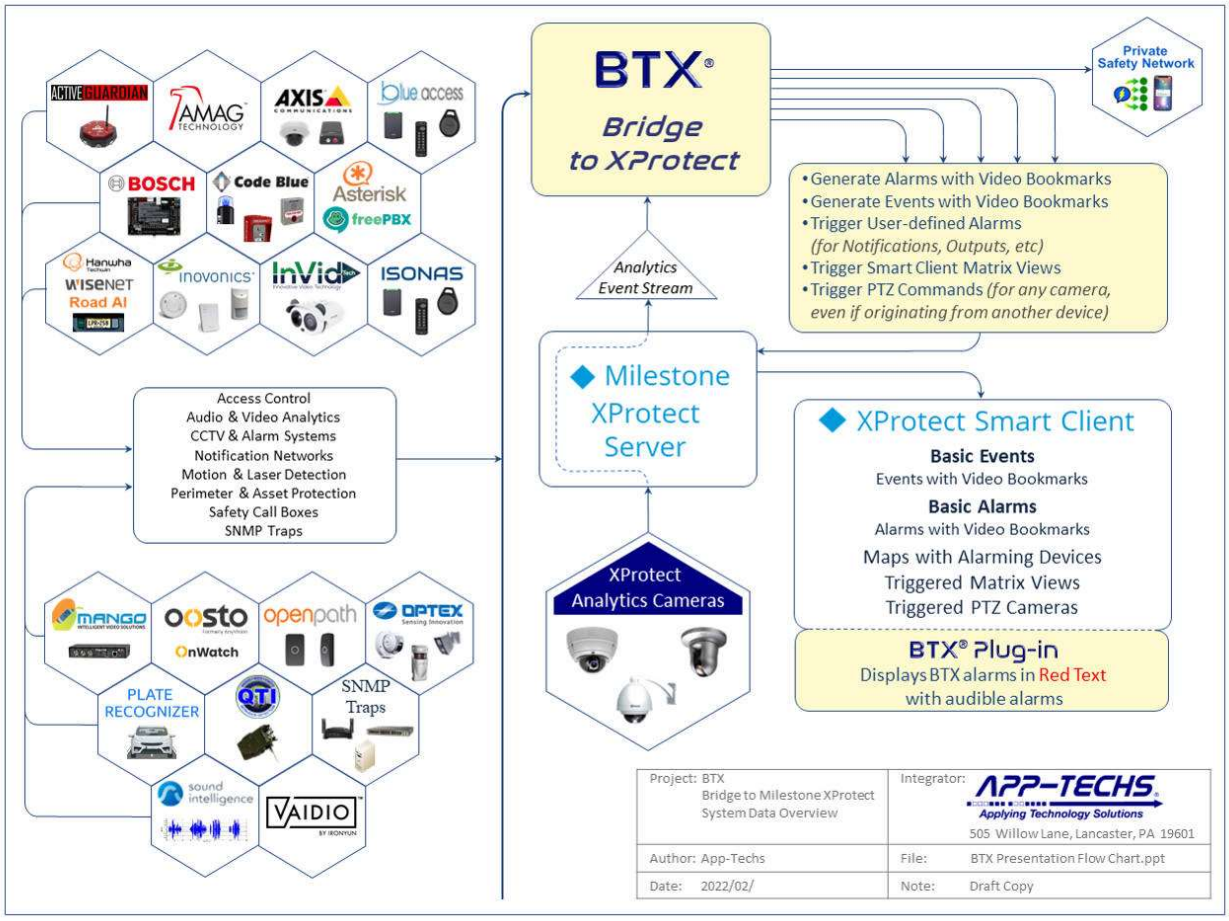
1.2. Features

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

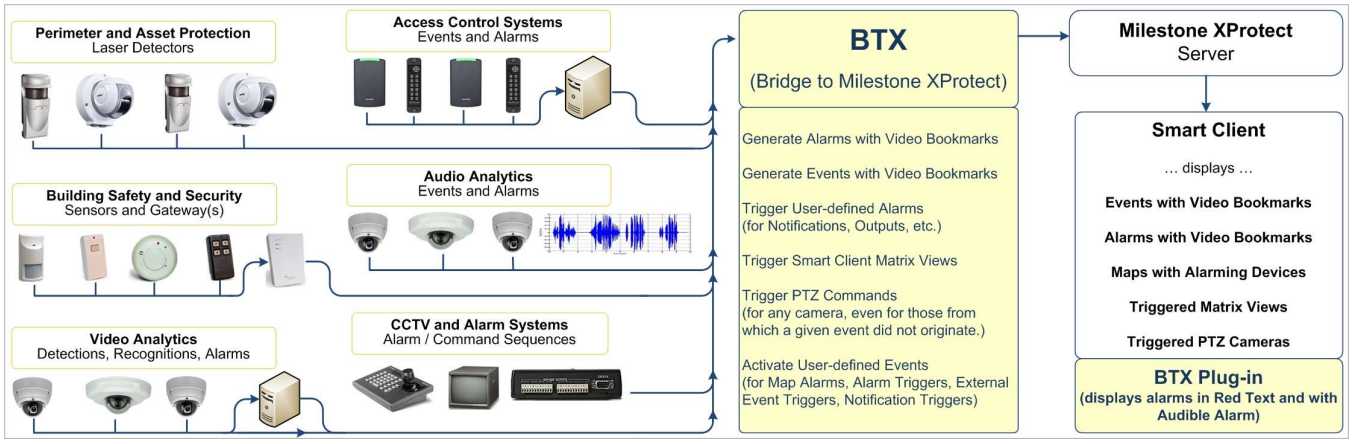
- **RECEIVE** third-party data in a variety of formats, including TCP, HTTP Post, UDP, Serial, SNMP Traps, and other protocols.
- **FILTER** third-party alarms by alarm keyword and/or device of origin
- **ASSOCIATE** XProtect cameras / devices to specific third-party devices.
- **GENERATE** XProtect events and / or alarms with Video Bookmarks.
- **DEBOUNCE** frequent or over-active third-party alarm messages, reducing false-positives and operator alarm fatigue.
- **SCHEDULE** alarms to be active at different times of the day.
- **TRIGGER** XProtect user-defined events (for text & email notifications, relays and digital outputs, and Smart Wall commands)
- **FIRE** 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.
- **ACKNOWLEDGE** XProtect alarms based on third-party keyword matches.
- **GROUP** multiple alarms into a single, master alarm with "Double-knock".
- **DISPLAY** third-party video analytics snapshots directly in the XProtect Smart Client.
- **STORE** relevant third-party data directly in the XProtect alarm record database
- **SEARCH** supplemental third-party detection / device data in the XProtect Smart Client.
- **MONITOR** device /sensor status with App-Tech’s Situational Awareness plug-in.
- **INTEGRATE** with other systems, such as the Private Safety Network mass notification system

2. Data Flow

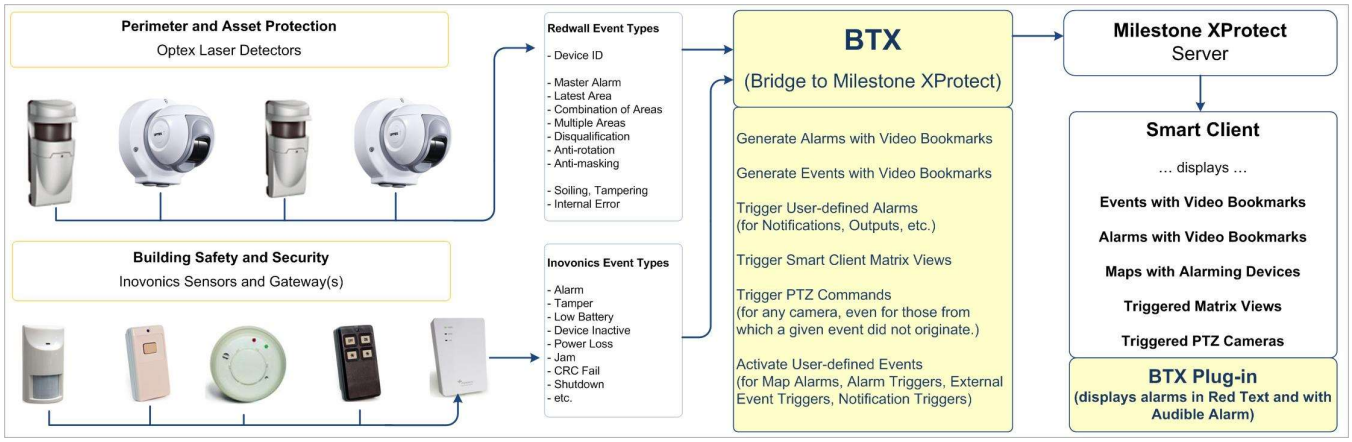
2.1. Overview



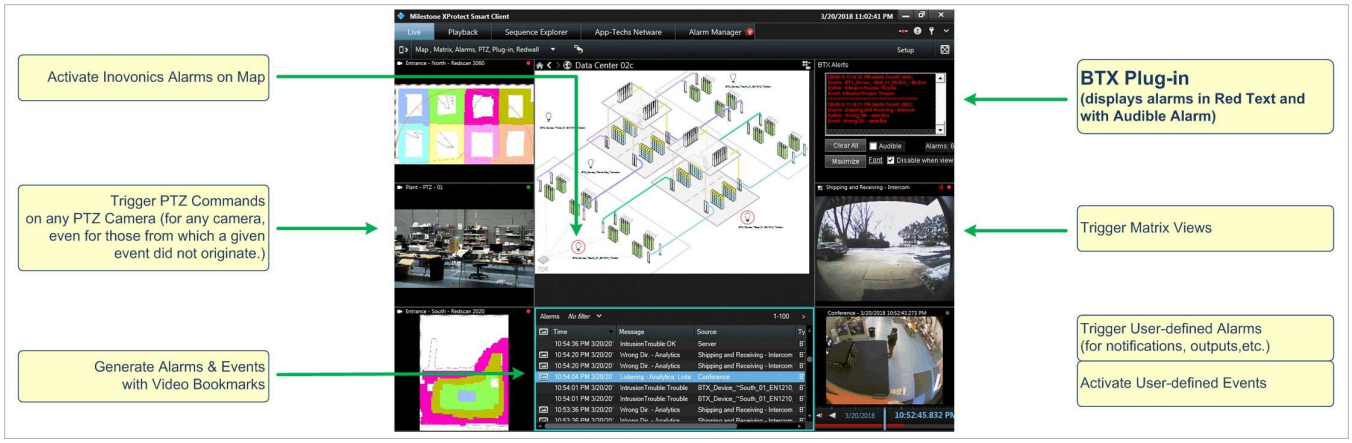
2.2. BTX Receives Third-party Events and Alarms



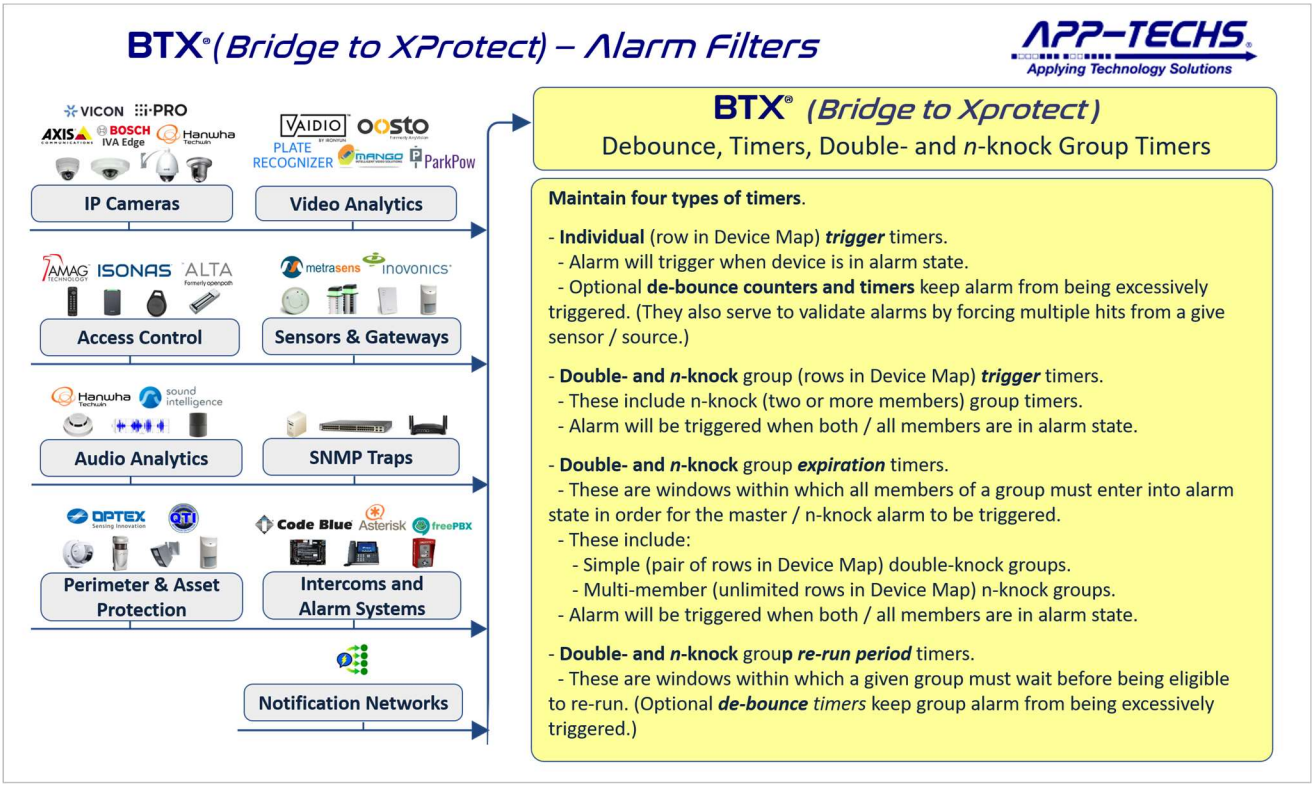
2.3. BTX Filters and Classifies Events and Alarms



2.4. BTX Integrates with Smart Client Maps



2.5. BTX Consolidates Alarms into Double-knock and n-Knock Groups



3. Installation

3.1. BTX Server

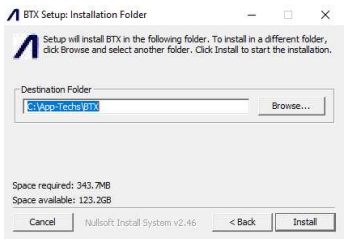
The BTX Server runs on any server which has network connectivity with XProtect and the third-party system(s) of interest.

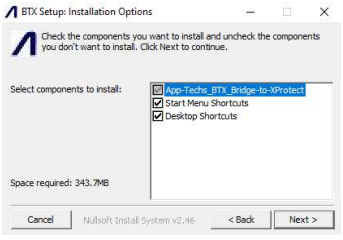
It is typically installed on the same server as the main XProtect services.

3.2. Core Application

Run the installer for the BTX core application. The four step process is illustrated below: (1) Installation Options; (2) Installation Folder Choice; (3) Installation Progress; and (4) Installation Complete.

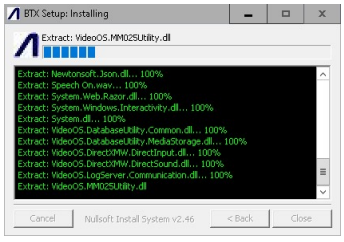
1

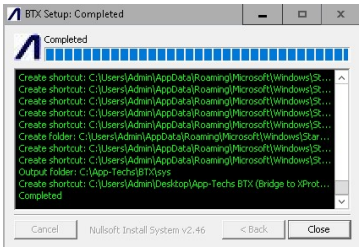




2

3





4

3.3. Windows Service Installation

Use the Windows Start menu and navigate to App-Techs > BTX (Bridge to XProtect) > 3. Setup > 1a. Install BTX Service (ADMIN)

RUN AS ADMIN.

You can also install the service with the command line below. Be sure to RUN AS ADMIN.

- C:\App-Techs\BTX\sys>BTX_util.bat InstallSrvc

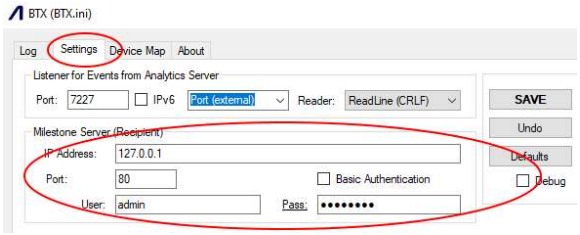
4. Configuration – Establish XProtect Connectivity

4.1. Connect BTX with Milestone

To launch BTX, from the Windows "Start" menu, select …
- All Programs
  - BTX (Bridge to XProtect)
    - Lauch BTX (Desktop for Configuration)

**Note: If an "Invalid License Key" error message is received, call or email App-Techs.

In BTX, select the "Settings" tab to set up the network connection with Milestone.

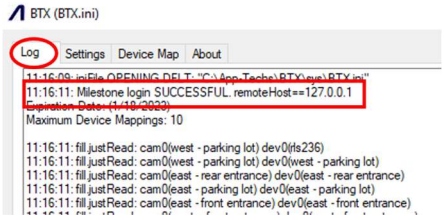


Enter the correct network configuration settings to authenticate BTX with the XProtect Management Server.

After configuring the connection settings, click the "SAVE" button in the top-right corner before exiting.

Exit BTX, then restart desktop application to initiate its connection with the designated XProtect system.

Log messages visible on the *Log* tab will indicate if BTX successfully authenticated with XProtect.



If unsuccessful, check your username / password. Verify the user profile has administrative privileges in the XProtect Management Client.

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

5.1. Alarm Data Overview

To transform third-party alarm data into XProtect alarm records, BTX looks for four critical pieces of information:

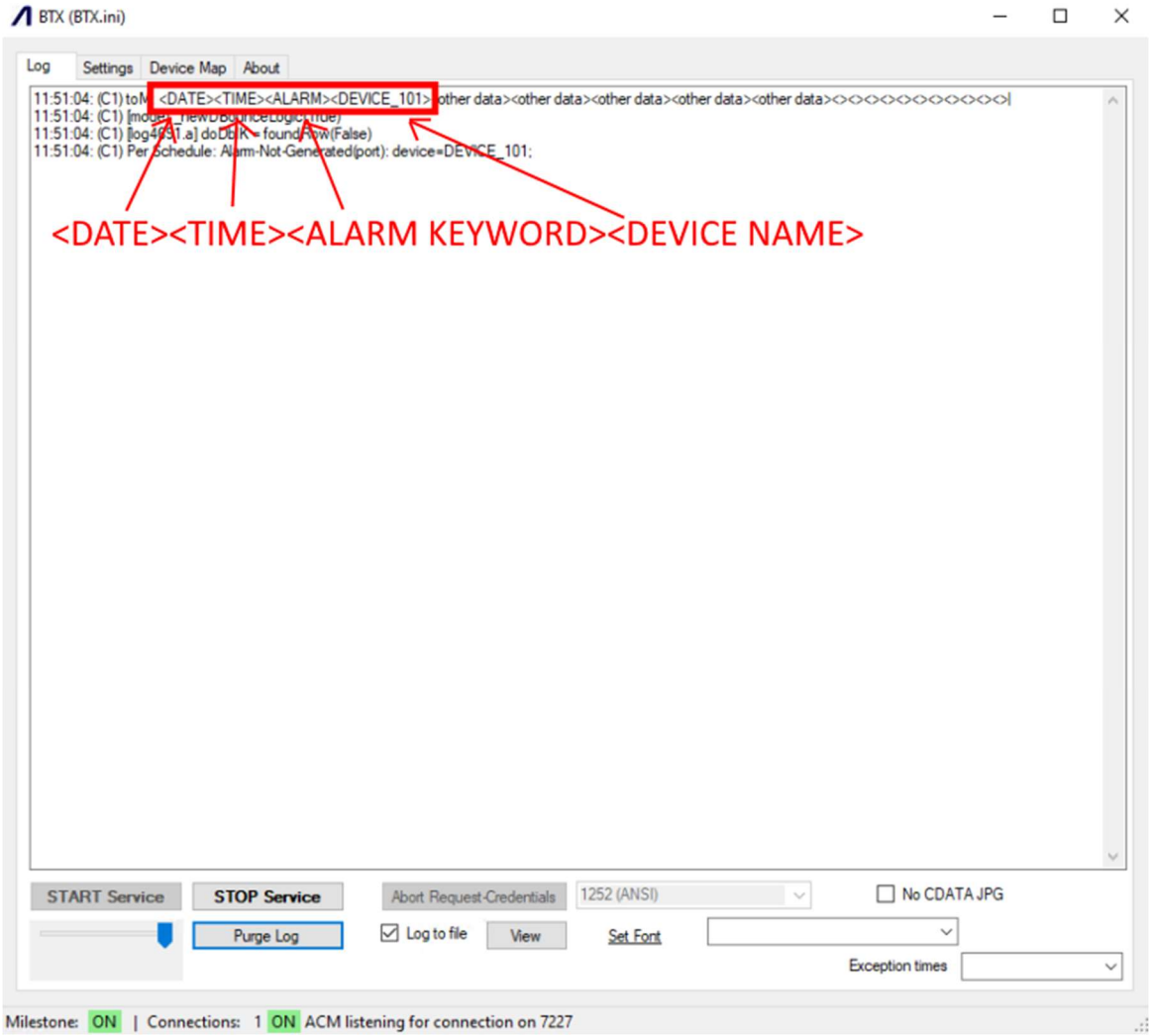
1) DATE
2) TIME
3) ALARM KEYWORD / NATURE OF EVENT
4) DEVICE NAME

By convention, BTX receives and displays third-party data in the following format:

<DATE><TIME><ALARM KEYWORD><DEVICE NAME><other data><other data><other data><other data><other data>|
Parameter #1 Parameter #2 Parameter #3 Parameter #4 [... optional data ....]

Almost all BTX core features are derived from these four key parameters. Since DATE and TIME can be optionally over-ridden (substituted by system time), the ALARM KEYWORD and DEVICE NAME are typically the most important and most often-used parameters in the configuration process.

Below is an example of an alarm received by BTX on the "Log" tab. Understanding this data convention will help make the configuration process easier and more user-friendly.



5.2. Specify Alarm Keywords

BTX provides the flexibility to filter which third-party alarm messages are sent to XProtect. With a positive ALARM KEYWORD match, BTX will initiate the process of generating a XProtect alarm. Non-keyword match messages are logged, but typically no action is taken in XProtect.

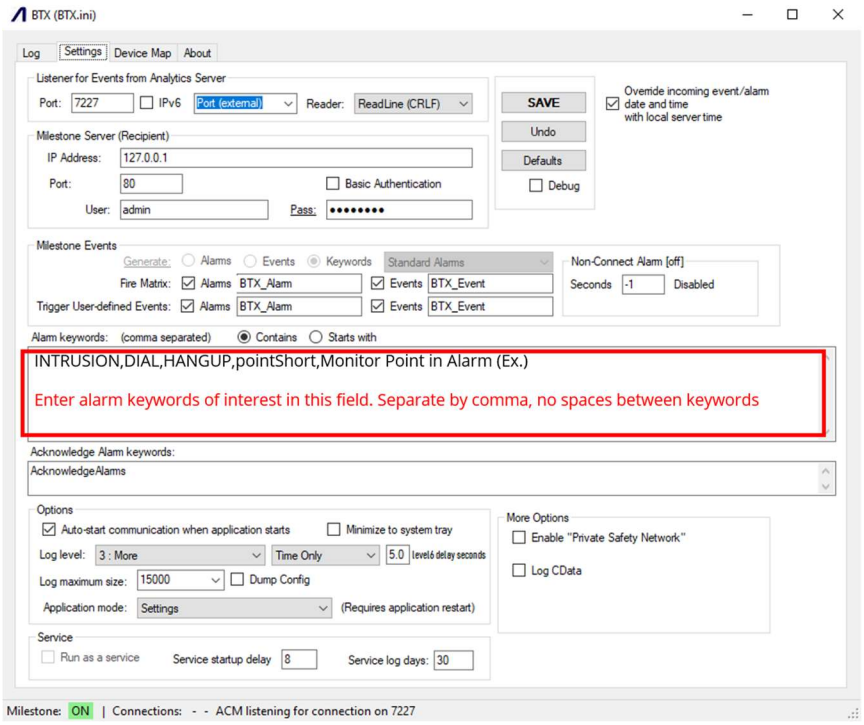
Using BTX's default configuration, an ALARM KEYWORD match is required to initiate a XProtect Event and/or Alarm Record.

To specify third-party ALARM KEYWORDS of interest, return to the *Settings* tab.

Enter all ALARM KEYWORDS of interest that will be sent by the third-party device(s) in the "Alarm keywords" text box. Separate keywords with a comma without any spaces.

Note the "Contains" and "Starts with" radio button. This can be used to add specificity to what constitutes an alarm keyword match.

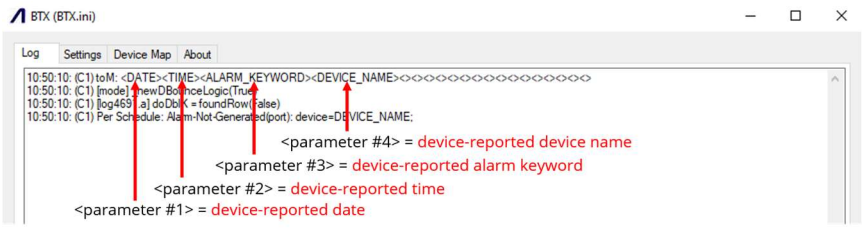
To ignore certain alarm messages from third-party devices, simply DO NOT include those **ALARM KEYWORDS** in the "Alarm keyword:" text field.



Click "Save".

Unsure of the third-party device ALARM KEYWORD? Generate a test alarm on the third-party device, and then go to the BTX *Log* tab.

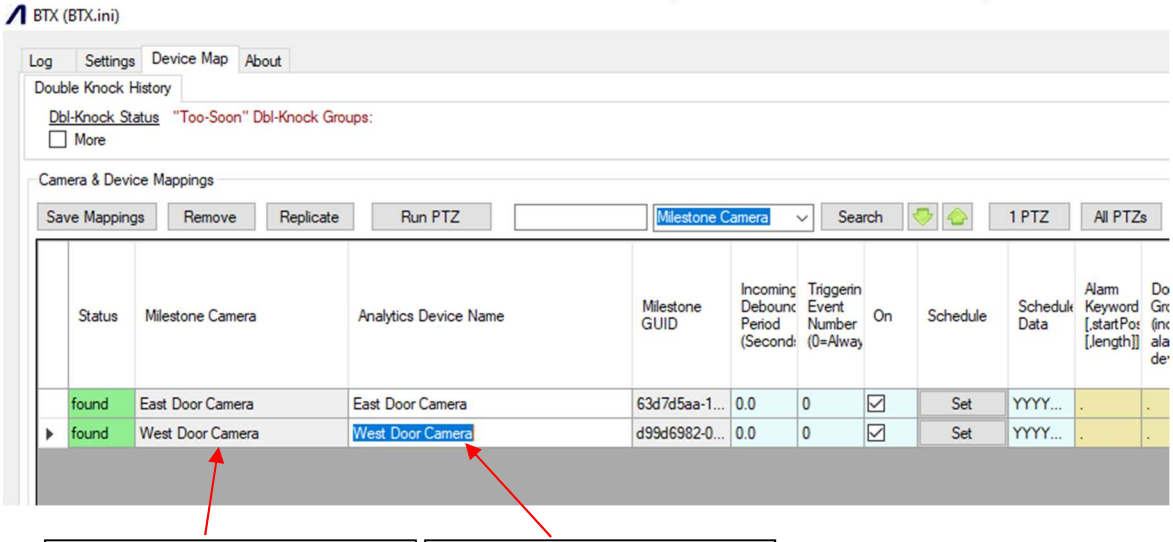
- Parameter #3 of the incoming alarm message is the **ALARM KEYWORD**.
- Copy the full or partial contents of Parameter #3. Return to the *Settings* tab, paste the keyword within the "Alarm keywords:" text field.
- Click "Save".



5.3. Associate Analytic Devices with Milestone Camera(s)

Go to the BTX "Device Map" tab.

If user authentication with XProtect is successful, the BTX *Device Map* tab will resemble the following:



The *Milestone Camera* column is a list of all XProtect cameras enabled in the Management Client. **Since this information is imported directly from XProtect, this column CANNOT BE EDITED.**

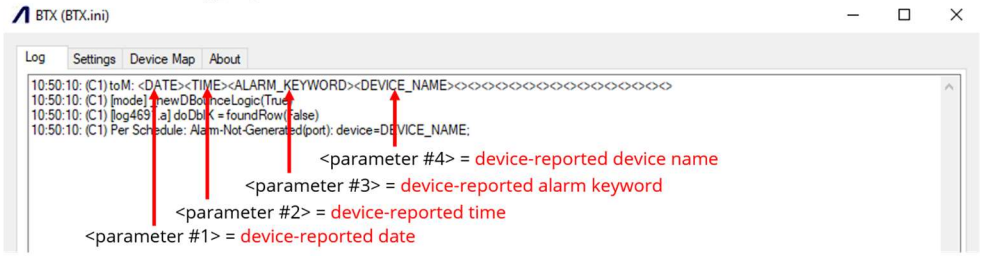
The *Analytics Device* column field is **EDITABLE**. This field is where the user associates a third-party DEVICE NAME to its corresponding Milestone camera.

To associate a third-party device with a Milestone camera.

- (1) Referencing the *Milestone Camera* column, choose the row containing the XProtect camera you would like to associate with the third-party device.
- (2) In the corresponding *Analytics Device Name* cell, click to edit the text. Enter the third-party device name exactly as it is listed in Parameter #4 of the incoming alarm message. An exact DEVICE NAME match is required; partial matches are insufficient.
- (3) Click "Save Mappings" to save settings.
- (4) Rows may be replicated to map any number third-party devices to any number of XProtect cameras.

Unsure of the third-party DEVICE NAME? Generate a test alarm on the third-party device, and the go to the BTX *Log* tab.

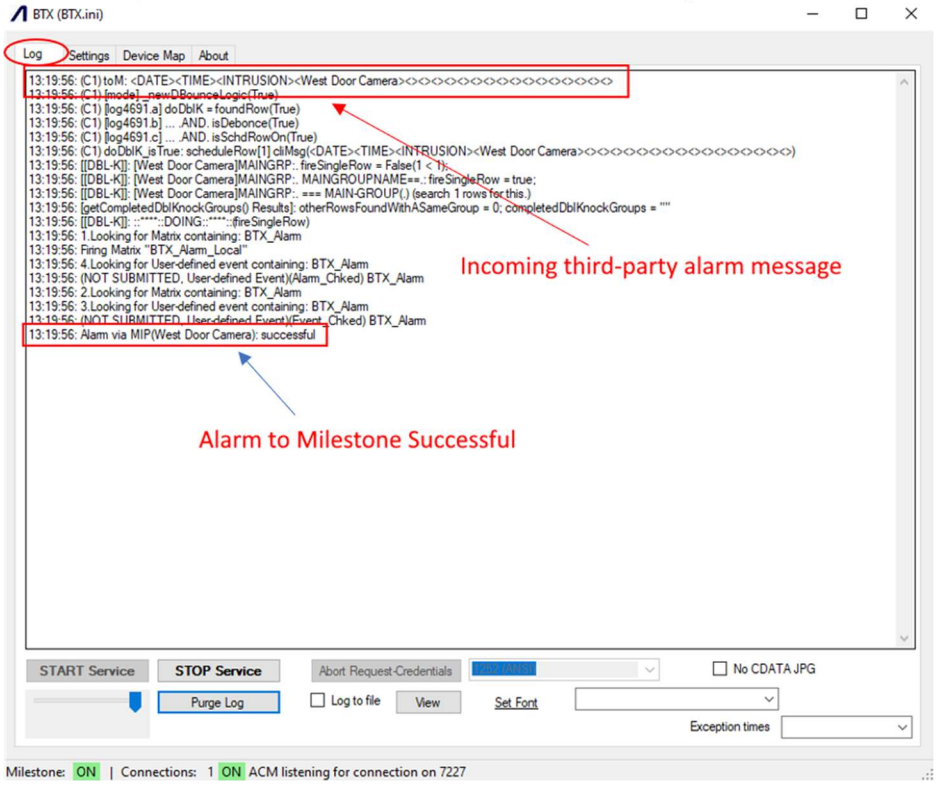
- Parameter #4 of the incoming alarm message will indicate the third-party DEVICE NAME.
- Copy the contents of parameter #4. Return to the *Device Map* tab, paste the device name within the *Analytics Device Name* field.
- Click "Save Mappings".



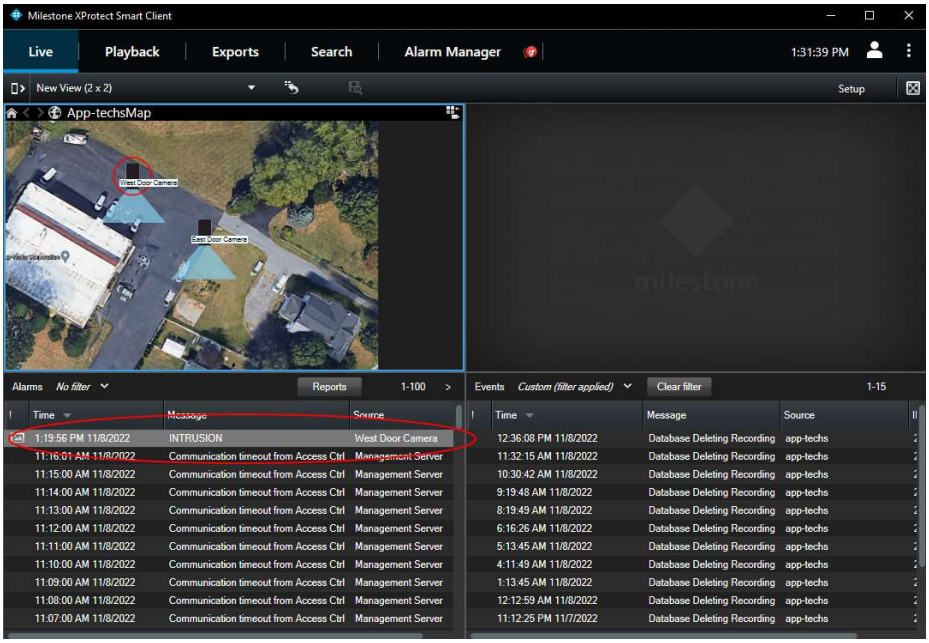
5.4. Test and confirm third-party alarms delivered to XProtect.

With BTX's default settings, an incoming alarm message that contains (1) an ALARM KEYWORD match on the *Settings* tab and (2) a properly associated DEVICE NAME match on the *Device Map* will result in an alarm being sent to XProtect.

Check the Log tab to confirm an "Alarm via MIP" confirmation message.



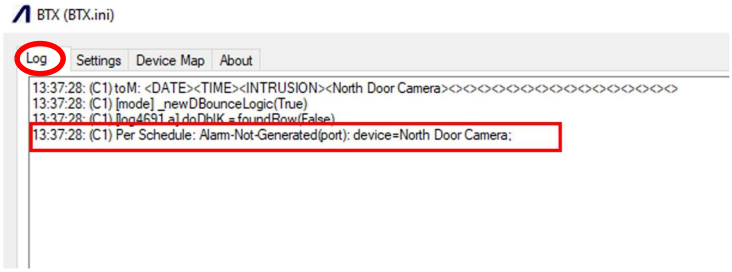
Delivery can also be confirmed by checking the alarm list in the XProtect Smart Client



5.5. Troubleshooting third-party alarms delivered to XProtect.

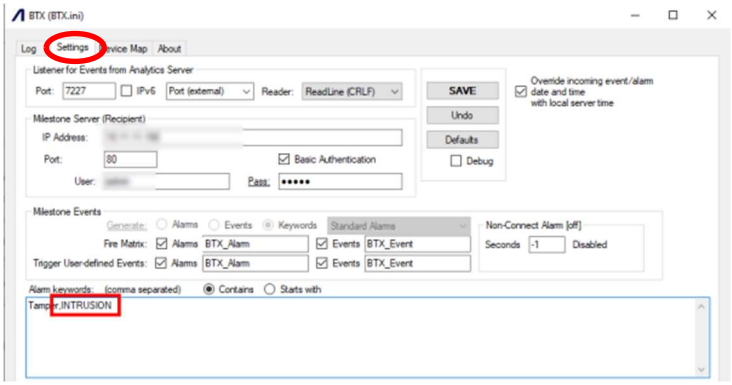
Incoming third-party alarms that do not meet the criteria of either an ALARM KEYWORD or a DEVICE NAME match will be logged by BTX, but no action will be taken in XProtect.

This may look like the following:

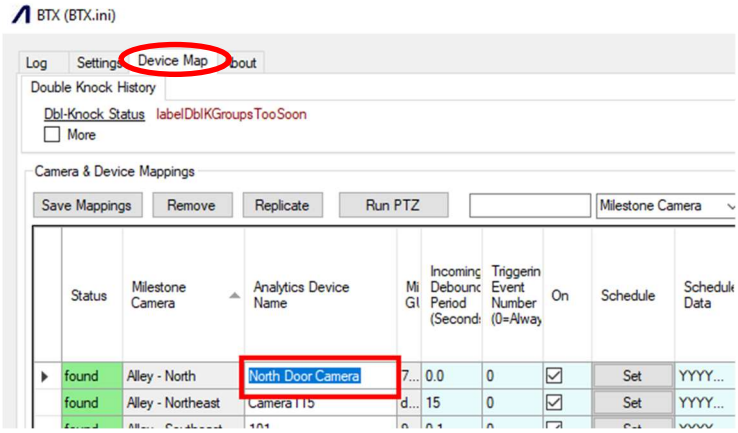


In the figure above, a third-party alarm was received by BTX, but it lacked the configuration necessary to generate an alarm in XProtect.

If you fail to properly generate an alarm record in XProtect, first check the "Alarm keywords:" text field on the BTX *Settings* tab. Make sure the keyword in question – in this case "INTRUSION" - has been added to the Alarm keywords field. Also check to make sure to separate keywords with a comma without any spaces in between keywords. (keyword1,keyword2,keyword3,etc)



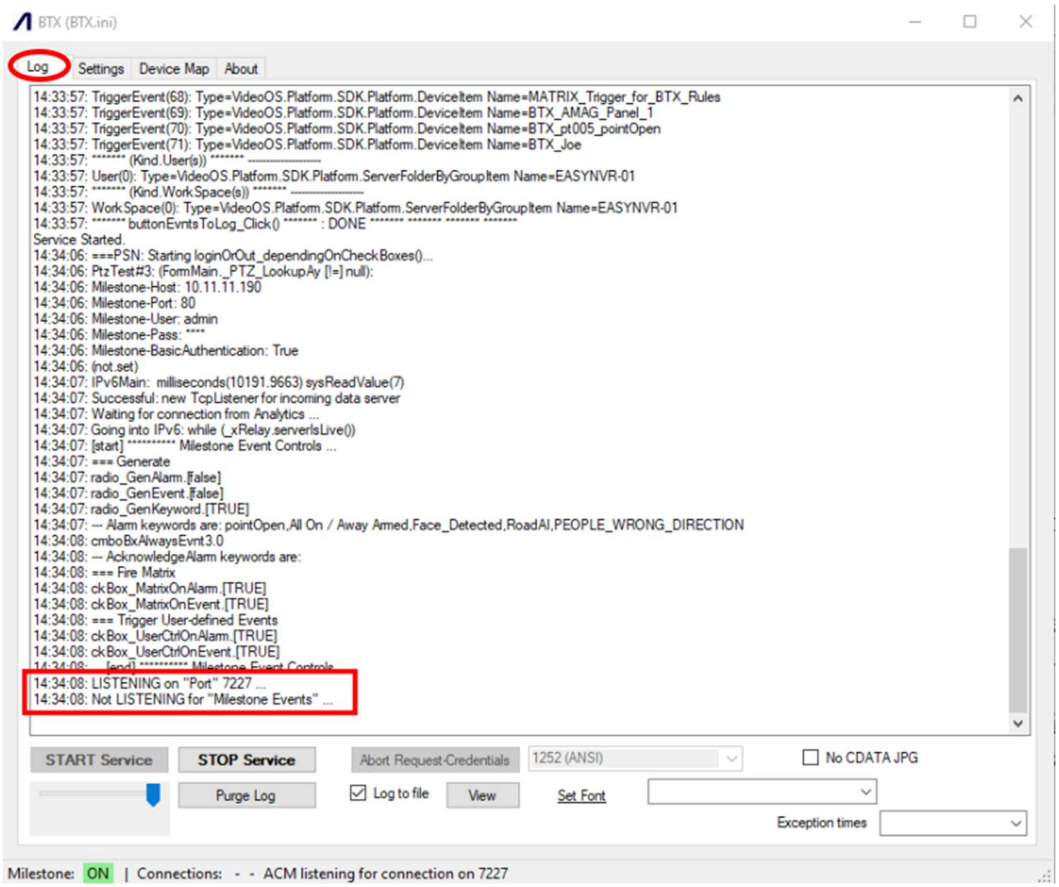
Next, check the *Device Map* tab to make sure you properly associated the third-party device name – in this case "North Door Camera" to the correct Milestone camera. Check for typos or incorrect entries; an exact DEVICE NAME match is required.



In most cases, a simple re-check of these two parameters will result in an alarm being sent to XProtect.

6. Device and Alarm Setup – BTX Features Explained

6.1. Log Tab



Start Service / Stop Service Buttons

RARELY USED. These buttons open and close the receiving port for incoming TCP messages.
These buttons DO NOT START and STOP the Windows Service feature of BTX.

Purge Log Button

This button purges the log visible in the BTX "Log" tab. It will NOT purge alarm records from the BTX log file. This button can be used helpful when generating test alarms; it makes it easier visually to confirm the arrival of new logs without requiring scrolling.

Log to File ☑ Checkbox

CHECKED STRONGLY RECOMMENDED. This instructs BTX to writer incoming alarm messages to the BTX log file. When not checked, you will have no searchable records to forensically confirm if an alarm message was received by BTX and what action was taken.

View Button (View Log File)

Click to view the full BTX log file in Windows Notepad.

Set Font

Not common. Used only in the case of certain integrations.

Exception times

Not common. Used only in the case of certain integrations.

Milestone ON

This confirms BTX successfully authenticated with XProtect. Unsuccessful authentications will appear as Milestone OFF.

Milestone: ON | Connections: - - ACM listening for connection on 7227 - BTX has properly authenticated with XProtect.

Milestone: OFF | Connections: - - ACM listening for connection on 7227 - BTX is NOT authenticated and cannot send alarms to XProtect.

Connections: -- ACM listening for connection on 7227

Milestone: ON | Connections: OFF ACM listening for connection on 7227

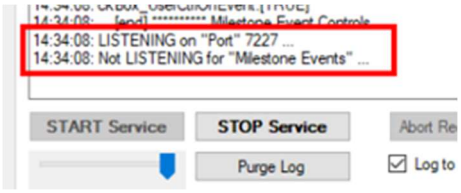
The *"Connections: OFF ACM listening for connection on 7227"* indicator is normal, and should not be interpreted as a malfunction or mis-configuration in BTX.

OFF indicates that BTX is not currently configured to receive ACM (Access Control Module) events from XProtect. If your integration is not related to access control, this indicator is irrelevant, and BTX is functioning properly.

If the XProtect on which BTX is installed has an active ACM license, this field will appear as:

Milestone: ON | Connections: 1 ON ACM listening for connection on 7227

SPECIAL NOTE: Interpreting log messages

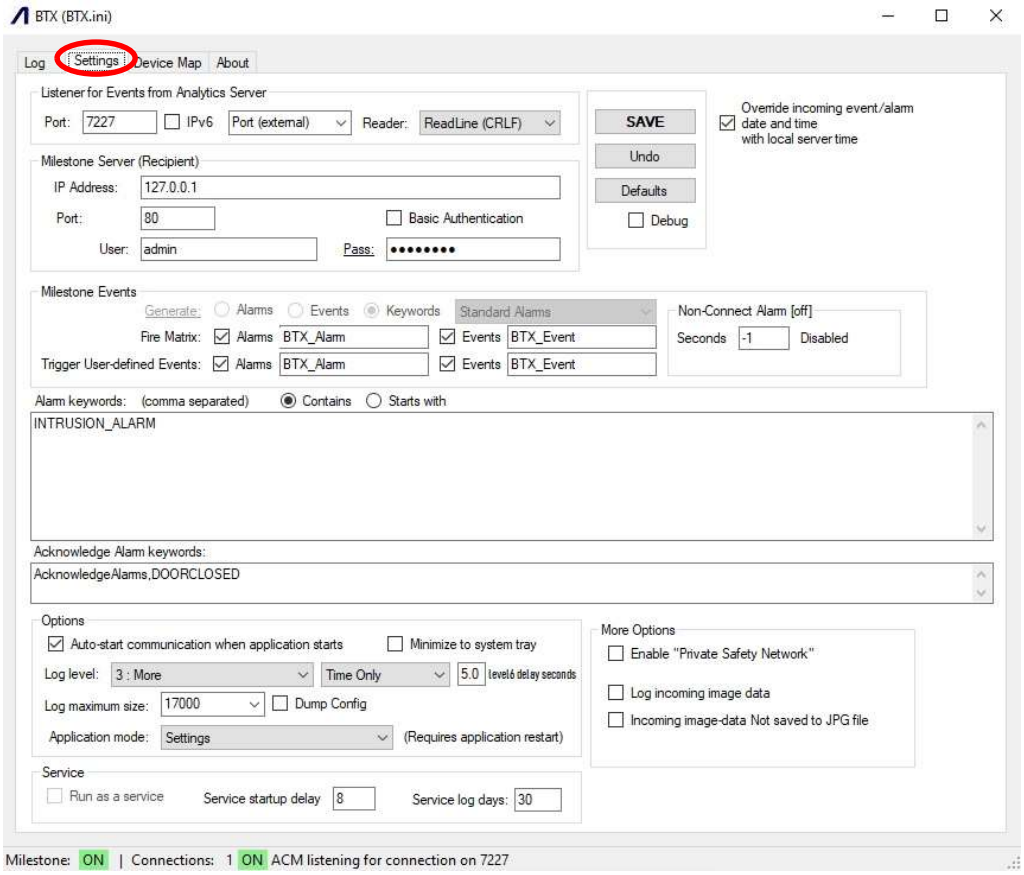


LISTENING on "Port" 7227 indicates BTX is listening for incoming alarm messages on "Port" 7227.

Not LISTENING for "Milestone Events" indicates that BTX is not currently configured to *receive* access control data from XProtect.

The **Not LISTENING for "Milestone Events"** message is normal. It should NOT be interpreted as BTX not functioning properly. This message only pertains to ACM (Access Control Module) integrations using BTX, and is irrelevant for typical "one-way" integrations.

6.2. Settings Tab



Listener for event from Analytics Server

Port
Default listening "Port" is 7227, but may optionally be changed by the user.

IPv6
Use IPv6. The unchecked default is IPv4.

Reader
BTX data handling settings. Default is "*ReadLine (CRLF)*." DO NOT CHANGE unless instructed to do so by App-Techs technical support.

Save
Save Settings.

Undo
Undo Settings.

Defaults
Sets BTX to its default settings.

Override incoming event/alarm date and time with local time server ☑ Checkbox
Substitute the date and time as reported by the third-party device with the system time on which BTX resides. Unchecking this box allows you to bookmark a XProtect alarm to the third-party device's reported time. Checking the box optionally over-rides the device time and substitute the BTX system time. This feature is useful in the case of third-party devices that are not time-synced or report incorrect time, which can result in alarms being incorrectly bookmarked and not synced correctly with video playback.

Milestone Server (Recipient)

IP Address
Enter IP address of XProtect Management server.

Port
Enter correct XProtect port number

Basic Authentication ☑ Checkbox
Toggles between using XProtect's Windows User and Basic User authentication methods.

User
XProtect username

Pass
XProtect password

Milestone Events

Fire Matrix: ☑ Checkbox
BTX provides the option to fire live matrix commands when generating XProtect alarms and / or events.

☑ **-** Default Setting. Provides the option to send or suppress Matrix commands for events and / or alarms.
☐ will suppress all matrix commands to sent to XProtect

BTX_Alarm, BTX_Event (text field):
This provides the user with the ability to define a MASTER matrix command. When any alarm or event is generated in XProtect, BTX will automatically fire ALL matrix profiles as defined in the XProtect Management Client that begin with this prefix. Default prefixes are "BTX_Alarm" and "BTX_Event".

Trigger User Defined Events: ☑ Checkbox
BTX provides the option to trigger user-defined events when generating XProtect alarms and / or events. NOTE: user-defined events are configured and mapped on the "Device Map" tab.

☑ **-** Default Setting. BTX will trigger configured user-defined events when generating and XProtect Alarm and / or event record.
☐ will suppress all user-defined event commands to XProtect.

BTX_Alarm, BTX_Event (text field):
This provides the user with the ability to define a MASTER user-defined event command. When BTX sends any alarm or event to XProtect, BTX will automatically fire ALL user-defined events as defined in the XProtect Management Client that that begin with the prefix "BTX_Alarm" or "BTX_Event".

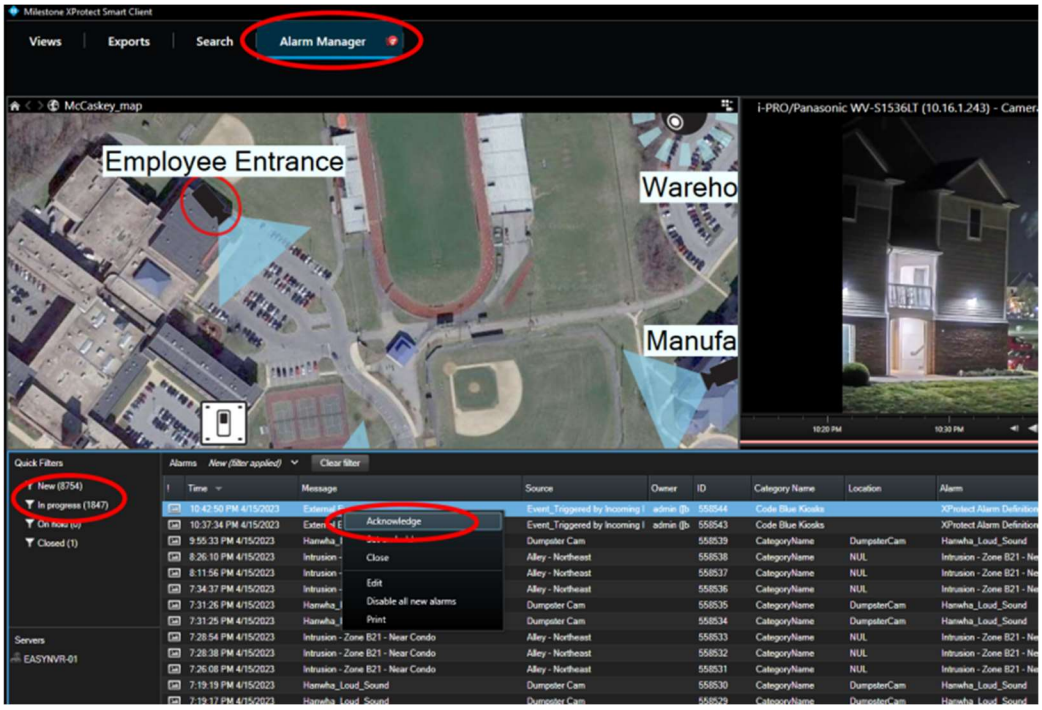
Alarm keywords: (comma separated) ⭘ Contains ○ Starts with
Optionally parse keyword matches by alarm keywords that either "contain" or "starts with" a particular character string.

Alarm keywords (text field)
This text field is where the user specifies which alarm keyword matches should be passed to XProtect. An incoming alarm message that does NOT contain a character string match in this text field will result in the alarm message being logged as received and ignored.

Acknowledge Alarm Keywords: (Text field)

An alarm keyword match in this field will cause BTX to send a command to Milestone to change the status of alarm from “New” to “In Progress” in the XProtect Smart Client

By acknowledging the alarm, it will also stop associated camera icons from blinking red on any map in the Smart Client Alarm Manager.



Options

Auto-start communication when application starts ☑ Checkbox

By default, this box is checked. If not checked, the BTX service will not start communicating automatically upon reboot. DO NOT UNCHECK unless in the case of special circumstances.

Minimize to system tray: **☑ Checkbox**

Creates an icon in the system try when the BTX application is running. Default is unchecked. Although useful in some circumstances, users may forget BTX is minimized in the system tray. This may cause users to open several instances of BTX, which can negatively impact the proper function of BTX.

Log Level: (Drop-down)

Control the amount of information that is stored by BTX in the log file. Default is log level 3.

Log Time

Control display of Date / Time in log file.

Dump Config

Output the config file to the directory.

Application Mode: (dropdown)

Default is "Settings." DO NOT CHANGE unless you are deploying a special access control integration. Changing this setting will result in BTX not functioning properly with most third-party integrations

SERVICE

Do not use unless running a legacy version of BTX.

More Options

Private Safety Network ☐ Checkbox

To enable features for use with the Private Safety Network mass notification system. Default is unchecked.

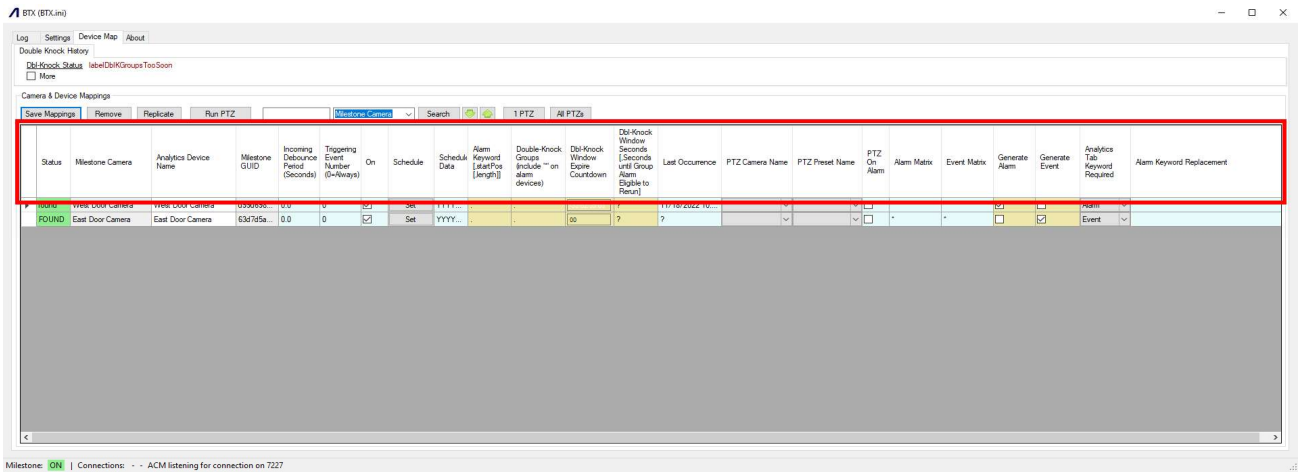
Log incoming image data ☐ Checkbox

Saves video analytics snapshots sent to BTX as JPEG files to c:\app-techs\files\BTX\sys. For diagnostic / testing purposes only. Rarely used. Default is unchecked.

Incoming image-data NOT saved to JPG file ☐ Checkbox

Saves image data in the BTX log as Base64-encoded characters. For diagnostic / testing purposes only. Rarely used. Default is unchecked.

6.3. Device Map Tab



Save Mappings (Button)

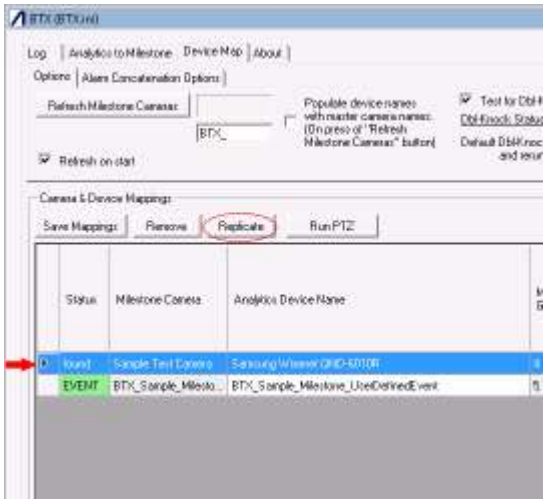
Save current configuration. Commits settings to the *.ini file. Be sure to click this button after making configuration changes to BTX.

Remove (Button)

Allows you to delete a row in the BTX Device Map. Click on the row to highlight, and then click “Remove” to delete. Click “Save Settings” to preserve your new settings.

Replicate (Button)

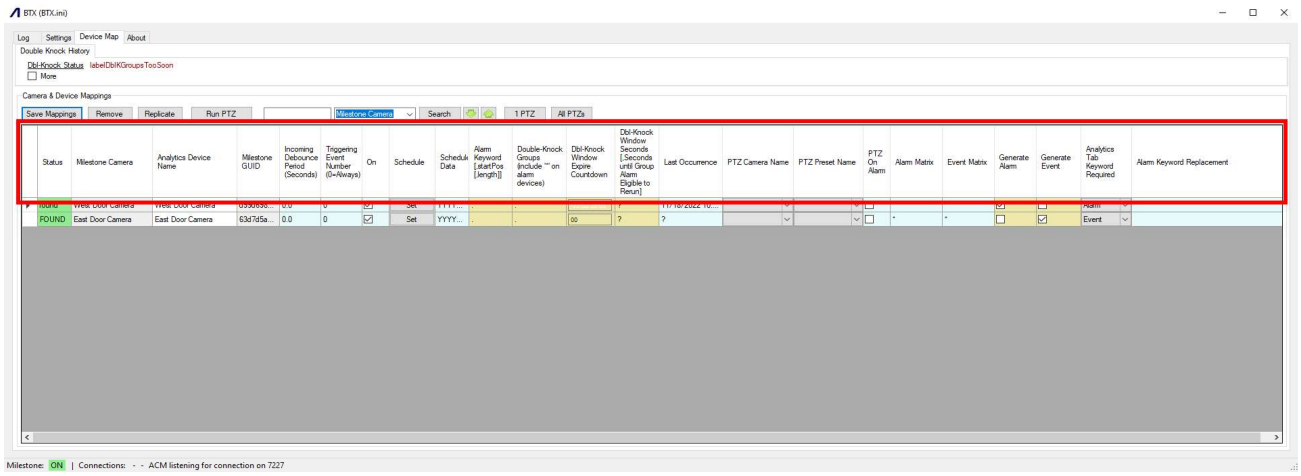
Allows you to copy a row in the BTX Device Map. Click on the row to highlight, and then click “Replicate” to copy. After making configuration changes to new row, click “Save Settings” to preserve your new settings.



Run PTZ Command

Execute the PTZ preset of the highlighted row. A means of testing the settings without generating a test alarm.

6.1. Device Map Filters (by Column)

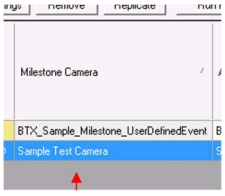


Each column located on the *Device Maps* tab represents either a label or filter for any event or alarm record created by BTX. Event and alarm records are filtered in order from left to right.

Status

- A label classifying the status of a device or user-defined event. This field cannot by edited. This indicates BTX connection status to XProtect cameras and user-defined events.
- INI Camera is listed as discovered by BTX in previous sessions, but has been either removed or disabled in XProtect.
- found The BTX .ini config file has a previous record of a XProtect camera. Camera is online and matched with previous record.
- EVENT The BTX .ini config file has a previous record of the user-defined event, and the event remains active in XProtect.
- NEW A new camera or user-defined event has been discovered by BTX. Click “Save Mappings” to commit the record to the the btx.ini file.
- Status labels displayed in CAPS indicate a device or event that has not been edited in BTX. Once a row has been edited and changes saved, the status will be shown in lower case letters.

Milestone Camera Name



This column lists all XProtect cameras and user-defined events beginning with “BTX_” as defined in the XProtect Management server.

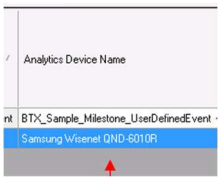
This field cannot be edited by design. It represents the item(s) to which the third-party devices will be associated to.

The column may be sorted alphabetically by clicking on the header row.

Analytics Device Name

The *Analytics Device* column is EDITABLE. To associate the analytics device name (as reported in the transaction data sent to BTX) with a Milestone camera or user-defined event, enter the analytics device name into the *Analytics Device Name* column. (Additional information on User-defined Events is covered in Section 7.2.)

-



The default field value is a simply replica of the "Milestone Camera" column.

The column may be sorted alphabetically by clicking on the header row.

Milestone Camera Name

- A label for the GUID assigned by Milestone to a device or user-defined event. Since this column is data imported from Milestone, it is for reference and cannot be edited.

Incoming Debounce Period (Seconds)

- A filter that throttles high event and alarm creation rates. Prevents redundancy and reduces false-positives by reporting only one event or alarm record per a user-defined debounce period. The default value is 0.0 seconds.

Triggering Event Number

- A count threshold requiring a certain number of alerts from a single analytics device before generating an event or alarm record. This feature is useful for reducing false-positives and managing high rates of incoming alarms.

On

- Activate or de-activate event or alarm record(s) being sent to Milestone for a given device or user-defined event.

Schedule

- Set a time period for a device or User-defined event. Use the "Set" button to make any schedule changes.

Schedule Data

- A text representation of the schedule. Do not manually edit; use Schedule "Set" functionality.

Alarm Keyword

- This column enables BTX's "Event Trigger" capability, which allows an event record to trigger User-defined Events (as opposed to an alarm record). Enter the device's alert keyword as specified in the transaction data into this column. This feature provides additional flexibility to customize user-defined events. Additional information on event triggering can be found in section 6.2.

Double-Knock Groups

- The double-knock feature is a way to require BTX to require concurrent alerts from two or more third-party analytic devices (i.e., devices represented as different columns on the *Device Map* tab) before generating an event or alarm record in Milestone. This feature adds device redundancy to incoming alerts to minimize false-positives and provide redundant confirmation.

-

Dbl-Knock Countdown

- Visual representation of your Double Knock Window. This field cannot by edited.

Double-Knock Window Seconds

- Set the time window (in seconds) in which a second analytics device can corroborate an event or alarm record reported from a primary analytics device. By using a separating comma, users can also specify a debounce period for Double-Knock alarm generation (which prevents high alarm generation rates).

PTZ Camera

- To trigger a PTZ response from an event or alarm record generated by BTX, specify the device name here.

PTZ Preset

- Enter PTZ present name here.

PTZ on Alarm

- Activate or de-activate PTZ feature.

Alarm Matrix
- This feature allows you to fire a subgroup of Matrix profiles. In this field, specify a Matrix profile prefix beginning with "BTX_[Enter Sub-group here]". When a Device Map row sends an alarm to XProtect, it will fire all XProtect Matrix profiles beginning with the prefix you entered. An example would be if you had two buildings, and you only wanted devices from Building A to trigger matrix profiles on XProtect Smart Client workstations also located in Building A. In this case, one would go to the "Matrix Profiles" menu in XProtect Management Client, and define a series of Matrix profiles beginning with the prefix "BTX_BuildingA_[type any additional information here]". Close BTX and restart so BTX can identify the new Matrix profiles you created in the XProtect Management Client. Now go to the Device Map tab and specify all the rows that are to fire these matrix profiles by including the prefix "BTX_BuildingA" in this Alarm field.

Event Matrix
- Same features listed as above, except triggered when BTX sends event records to BTX.

Generate Alarm (checkbox)
- Indicate if you want BTX to send an Alarm Record to XProtect.

Generate Event (checkbox)
- Indicate if you want BTX to send an Event Record to XProtect.

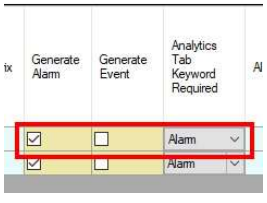
Analytics Tab Keyword Required (dropdown)
- This feature provides a method to specify if you want to require an ALARM KEYWORD match (as specified on the "Settings" tab) as a condition for generating events and alarms in XProtect.

- In summary, when using this dropdown, ask the following question, "Do I want to require a keyword match in order to generate an XPRotect Alarm or Event Record?"
    - Generate alarm on keyword match: Choose "Alarm" in dropdown and check "Generate Alarm" checkbox.
    - Generate event on keyword match: Choose "Event" in dropdown and check "Generate Event" checkbox.
    - Generate an alarm + event on keyword match: Choose "Both" and check both the "Generate Alarm" checkbox and "Generate Event" checkbox.
    - Generate alarm on keyword match, pass all other third-party messages as event records to XProtect: Choose "Alarm" in dropdown, and check both the "Generate Alarm" checkbox and "Generate Event" checkbox.
        - Translation: "I want to require a keyword match for alarms, but I do not want to require a keyword match to generate events.
    - Generate an alarm for all messages from a device: Choose "Neither" in dropdown, but only check both the "Generate Alarm" checkbox.
    - Other permutations may be useful, but are generally uncommon.

Why does BTX provide so many event and alarm options? Because third-party systems have a broad array of alarm types and conditions, and this provides maximum flexibility to control what actions are sent to XProtect.

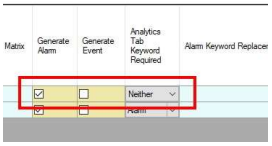
Example Setting #1: You are integrating a panic button device with XProtect. Device "0:1:Panic Button Door" outputs "PANIC BUTTON PUSH" when activated. The device also reports regular heartbeats, low-battery alarms, and systems diagnostic information. In this case, you only want PANIC BUTTON PUSH alarms to be sent to XProtect.

Here are your settings:



Example #2: An analytics device has over a dozen different detection types, which can be adaptively changed by the user in the analytics UI. Regardless of user settings, you want BTX to pass ALL detections reported by the analytics device as Alarm Records in XProtect.

In this case, your setting would be the following:



Alarm Keyword Replacement

- This allows you to replace the message field that will be displayed in the XProtect Smart Client when the BTX row sends an event / alarm to XProtect. This is a means of creating user-defined messages that can be easily understood by a XProtect Smart Client operator. In some cases, alarm messages sent from third-party devices contain cryptic information. For example, a panic button alarm may be received by BTX as "IntrusionAlarm:Intrusion;SCICode:1;SCI:ALARM 1;ID:0002". However, by using this field, you can replace this cryptic message to read "Panic Button Pushed", or whatever message is most useful, in the XProtect Smart Client.

After filters have been configured, be sure to click "Save Mappings."

6.2. Highlighted BTX Filtering Options

Debounce

- The "Incoming Debounce Period (Seconds)" column allows the user to throttle high event and alarm creation rates. This can be useful when a third-party device reports multiple, redundant alarms for a singular security event. By employing the debounce filter, BTX creates only one event and/or alarm record in XProtect per debounce period, regardless of the number of alerts received from the analytics device. Enter a time period in (seconds) in this column to activate the debounce feature.

Triggering Event Number

- Use this column to require BTX to receive a specified number of third-party device alerts before generating an event and/or alarm record in Milestone. By setting a trigger number, the user can increase event/alarm confidence, reduce false-positives, and compensate for the sensitivity of third-party devices.

Event Triggers

- In certain cases, users may want a XProtect event record (as opposed to an alarm record) to trigger a user-defined event. By entering a third-party device keyword in the "Alarm Keyword" column the *Device Maps* tab, any transaction data containing the keyword entered in this column will generate an event record AND trigger matrix views and associated user-defined events.

    - Be sure to exclude the alert keyword from the "Alarm keywords" field on the *Analytics to Milestone* tab (or else BTX will report it as an Alarm Record.).

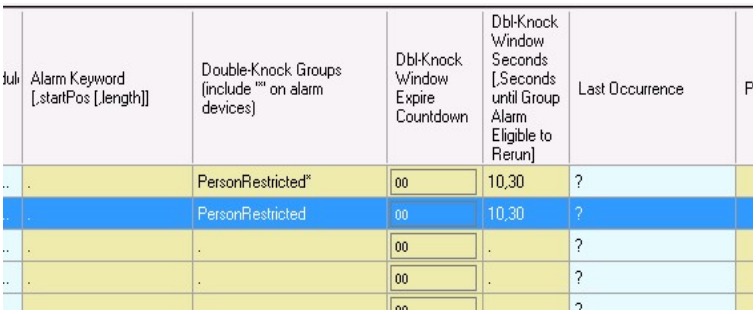
Double-Knock

- This feature is useful if users want multiple devices to confirm a single security incident before an alarm is triggered. As an example, perhaps one would like a motion sensor and camera analytic device to confirm the presence of a person in a restricted area. When using Double-Knock, an alarm will only be sent to XProtect if BTX receives transaction data from the motion sensor AND from the camera analytics device. If transaction data is received from only one device, no alarm will be generated.

    - To activate the double-knock feature, create a keyword and enter it in the "Dbl-Knock Groups" column in a row that contains one of the analytics devices.
    - Type the same keyword into a second row (or third, etc) that contains a secondary, confirming analytics device.
    - If the user only wants to trigger one alarm for a Double-Knock group, then include an asterisk (*) after the keyword in the row of the primary device.
    - Set your Double-Knock window (in seconds). An alarm will only be generated if all grouped devices report transaction data within the Double-Knock window. The default setting is 90 seconds.
    - To throttle high Double-knock alarm rates, use a comma (,) after the Double-Knock window and enter the desired debounce period (in seconds). BTX will generate only one alarm record within the specified debounce period.

- Example: Double Knock

- In the example below, the Double-Knock group "PersonRestricted" has been created with a Double-Knock window of 10 seconds and a debounce period of 30 seconds. In this scenario, if transaction data is received from both devices within 10 seconds, BTX will generate an alarm record (or an event record). To prohibit high-frequency and/or repetitive alarm records, a debounce period of 30 seconds (,30) was added to the "Double-Knock Window Seconds" column so that only one alarm record is reported to Milestone within a 30 second time window.

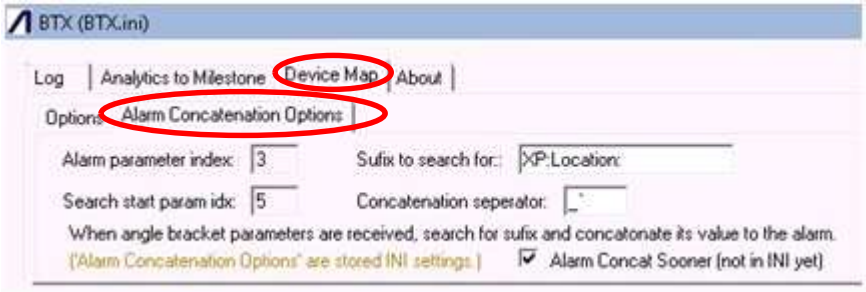


	Alarm Keyword [,startPos [,length]]	Double-Knock Groups (include "" on alarm devices)	Dbl-Knock Window Expire Countdown	Dbl-Knock Window Seconds [,Seconds until Group Alarm Eligible to Rerun]	Last Occurrence	P
..	.	PersonRestricted"	00	10,30	?	
..	.	PersonRestricted	00	10,30	?	
..	.	.	00	.	?	
..	.	.	00	.	?	

6.3. **Concatenate**

Concatenation allows users to merge two separate alarm data fields to create a custom alarm keyword. This is useful feature if the analytics device uses a separate data field to report different variations of an alarm type or category.

To activate concatenation, check the "Alarm Concat Sooner" checkbox and set your fields. Ex. below:



In the example above, BTX will execute the following steps:

1. Search for suffix "XP:Location:" in the 5^{th} through the n^{th} fields
   - **Suffix to search for** = XP:Location:
   - **Search start param idx** = 5
2. If text match, copy text in field after suffix
3. Merge copied text with the contents of 3rd field, separated by _`
   - **Alarm parameter index** = 3
   - **Concatenation separator** = _`
4. Generate a revised transaction data string. New 3rd field = [Previous text in 3rd field] +[_`] + [text after XP:Location:]
5. Search revised 3rd data field for Alarm keyword match
   - **Alarm keyword**=[Text in 3rd field] +[_`] + [text after XP:Location:]
6. If alarm keyword match, generate an alarm record in XProtect and trigger associated User-defined events.
7. Save settings.

Note: Make sure to add the concatenated alarm keyword to your list of alarm keywords in the BTX *Settings* tab.

7. Milestone Settings – User-Defined Events, Rules, and Matrices

7.1. Overview

User-defined events in XProtect are used to trigger "Rules" which initiate additional security actions third-party devices.

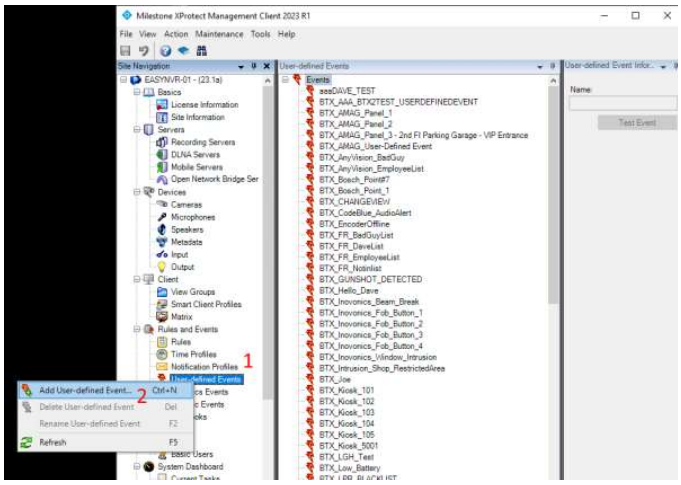
- When launched, BTX scans the XProtect Management Client for all user-defined events that begin with the prefix "BTX_" (by default) and displays each User-defined Event as a row in the BTX *Device Map* tab.
- Users then associate a third-party analytics device with the User-defined Event by editing the "Analytics Device Name" column .
- The "Replicate" feature can be used to associate multiple analytic devices to a single User-defined Event (see Section 6.3).
- Any incoming data categorized by BTX as an alarm or event-trigger will trigger a User-defined Event associated with the analytics device.
- Once a User-defined Event is triggered, the XProtect *Rules* tool controls what additional actions are executed by XProtect and/or third-party devices.
-

7.2. 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….

! Be sure your User-defined Event name begins with "BTX_". This is the text string BTX searches for when auto-generating a list of XProtect User-defined Events.



3 Enter name of User-defined Event.

Be sure to click "Save" in XProtect. Close BTX and restart it to repopulate the list of Milestone Cameras and User-defined events. New User-defined event should now show up in the Device Map tab as a column with a status listed as NEW. Edit the "Analytics Device Name" column to associate newly created user-defined events to analytic devices and XProtect cameras.

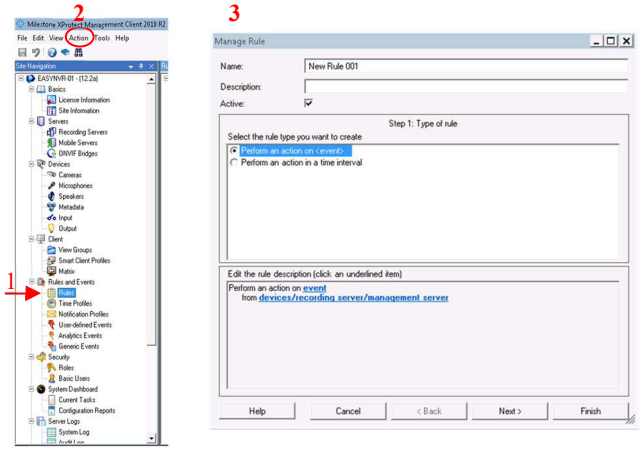
7.3. Link *User-defined Events* to *Rules* in XProtect

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.



7.4. Configuring Matrix Displays

A matrix can be setup no matter what version of XProtect is being used to receive video from any camera at a location of an alarm or event.

- The XProtect Smart Client has the ability to do filtered searches and easily find video from an alarm/event that happened on a certain day, or search out when a certain person went into a certain door at a certain time.

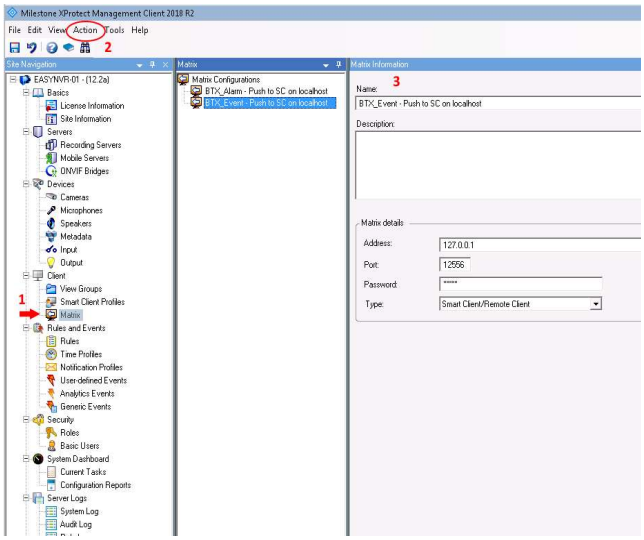
- Another useful feature of the XProtect Smart Client (only available when using Milestone XProtect Enterprise, Expert, and Corporate) is the alarm manager. This allows the user to view a list of alarms and escalate/manage them. In the alarm manager, an alarm can be forwarded to a manager or other personnel for appropriate action to be taken.

To configure a Matrix Display:

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

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

3 Be sure your Matrix name begins with "BTX_Alarm" or "BTX_Event". This is the text string BTX searches for when pushing out matrix views. You can add a new Matrix if you want to push events and alarms to different workstations.



7.5. Send Test Alarms to BTX with PuTTY

PuTTY can be used to send sample third-party alarms to BTX.

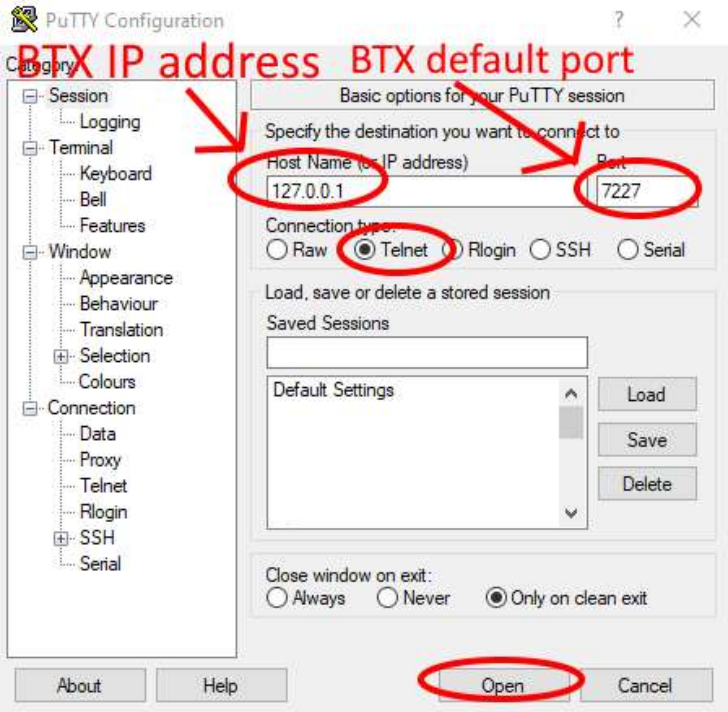
This allows you to mimic incoming third-party alarms without having to physically trip a device alarm.

This is very helpful to test your BTX configuration, and also to test your XProtect Management Client / XProtect Smart Client setup.

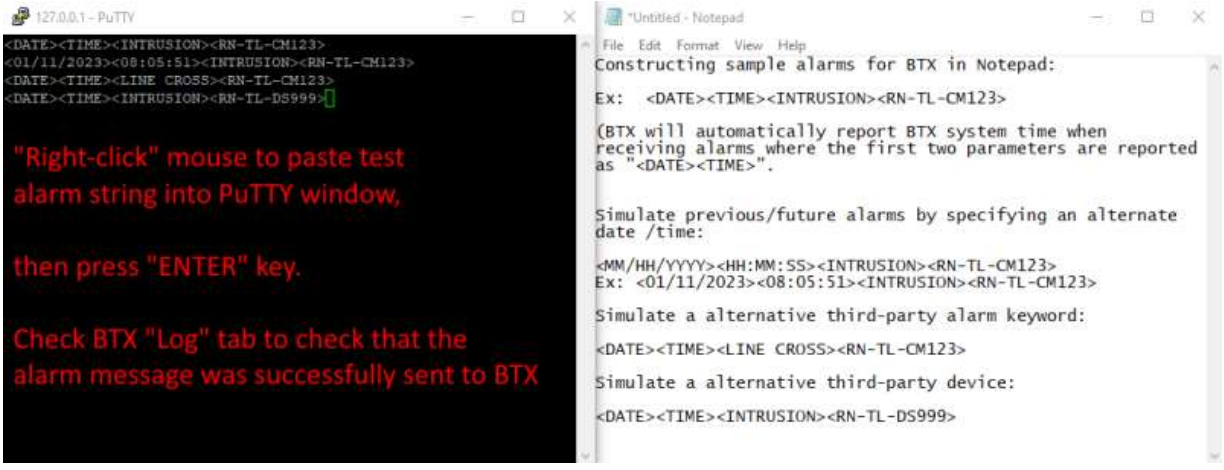
Steps to send test / sample alarms to BTX:

1) Download PuTTy: (https://www.putty.org/)

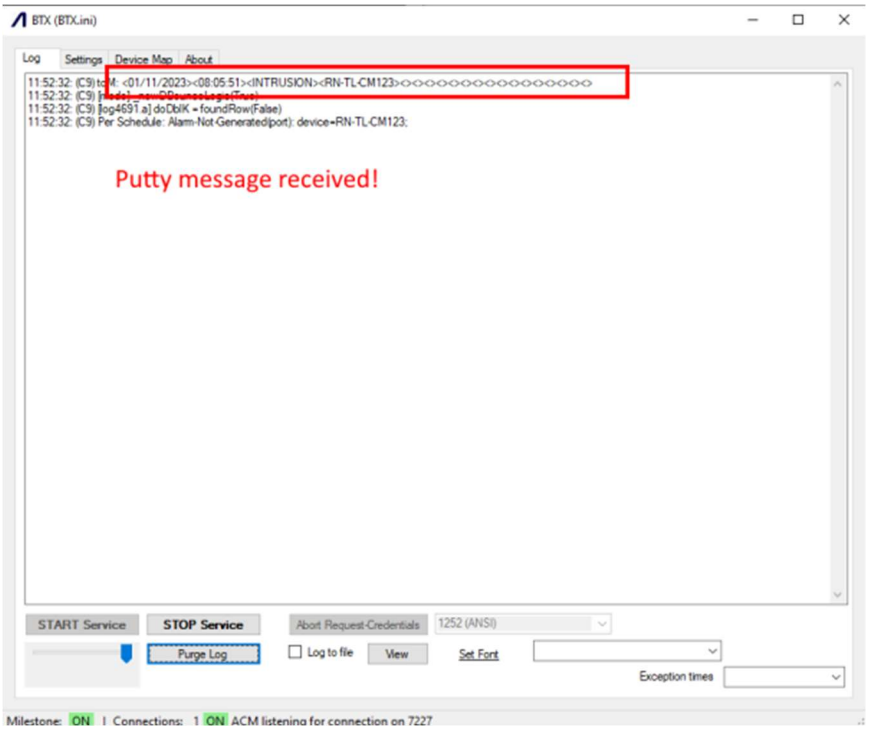
2) Configure PuTTY:



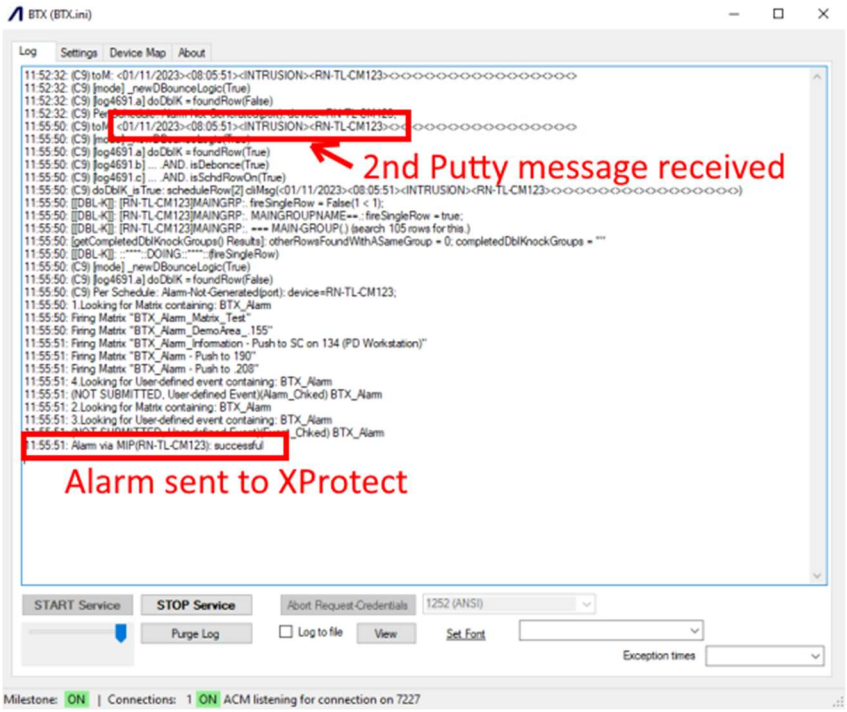
3) Send sample alarm in PuTTY:



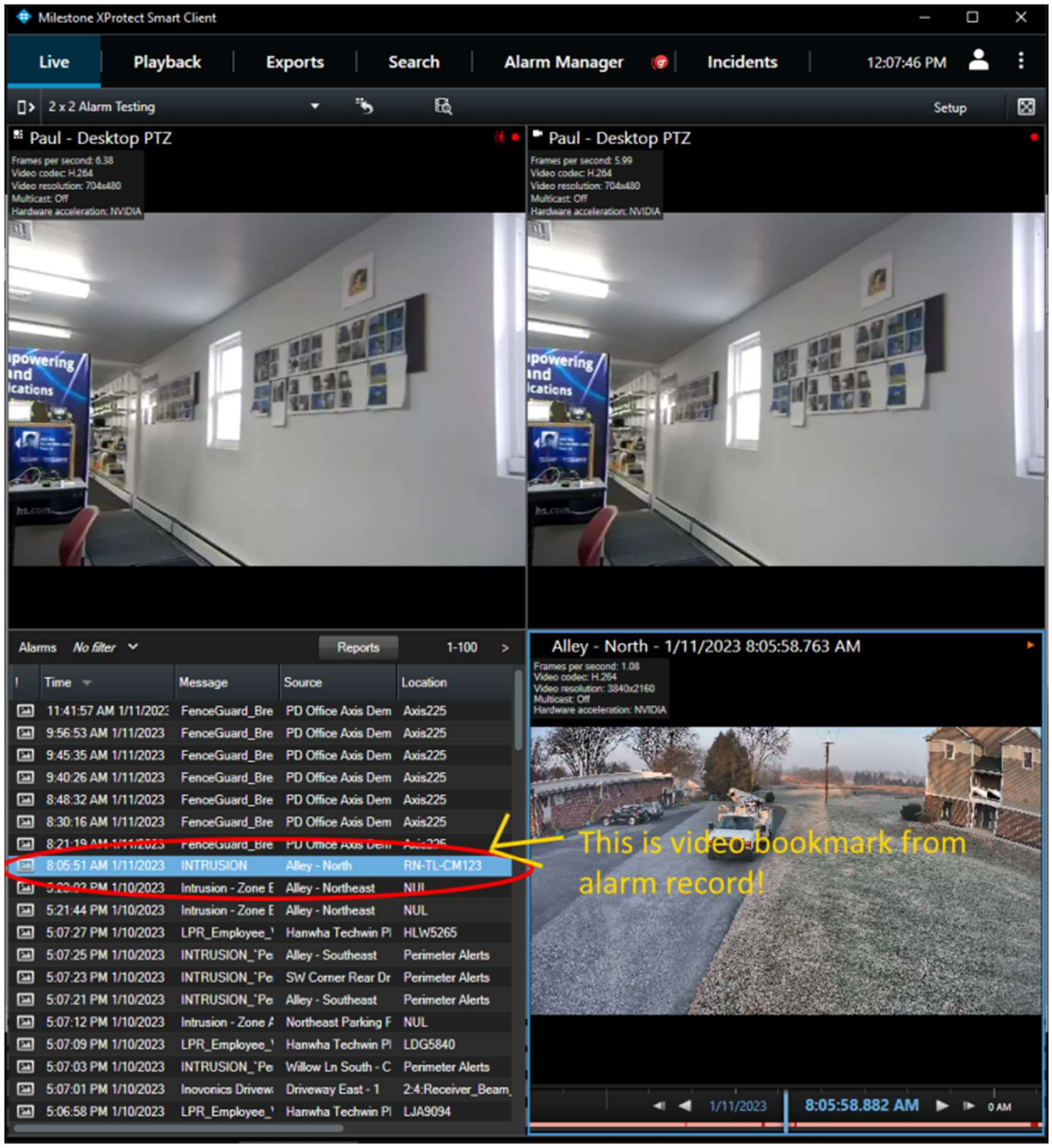
4) Confirmed PuTTY alarm message received in BTX:



5) If necessary, check to make sure your BTX alarm keyword(s) and device mappings are properly configured to generate an alarm in XProtect for the incoming PuTTy message. Resend message in PuTTY. If your BTX configuration is proper, the BTX log will indicate an alarm was successfully sent to XProtect.



6) Confirm the success sample test / alarm output in the XProtect Smart Client:



8. Third-party Integrations

8.1. Overview

BTX receives third-party alarm message via TCP to default port 7227. BTX uses the format below to receive and process third-party alarms (See section 5.1).

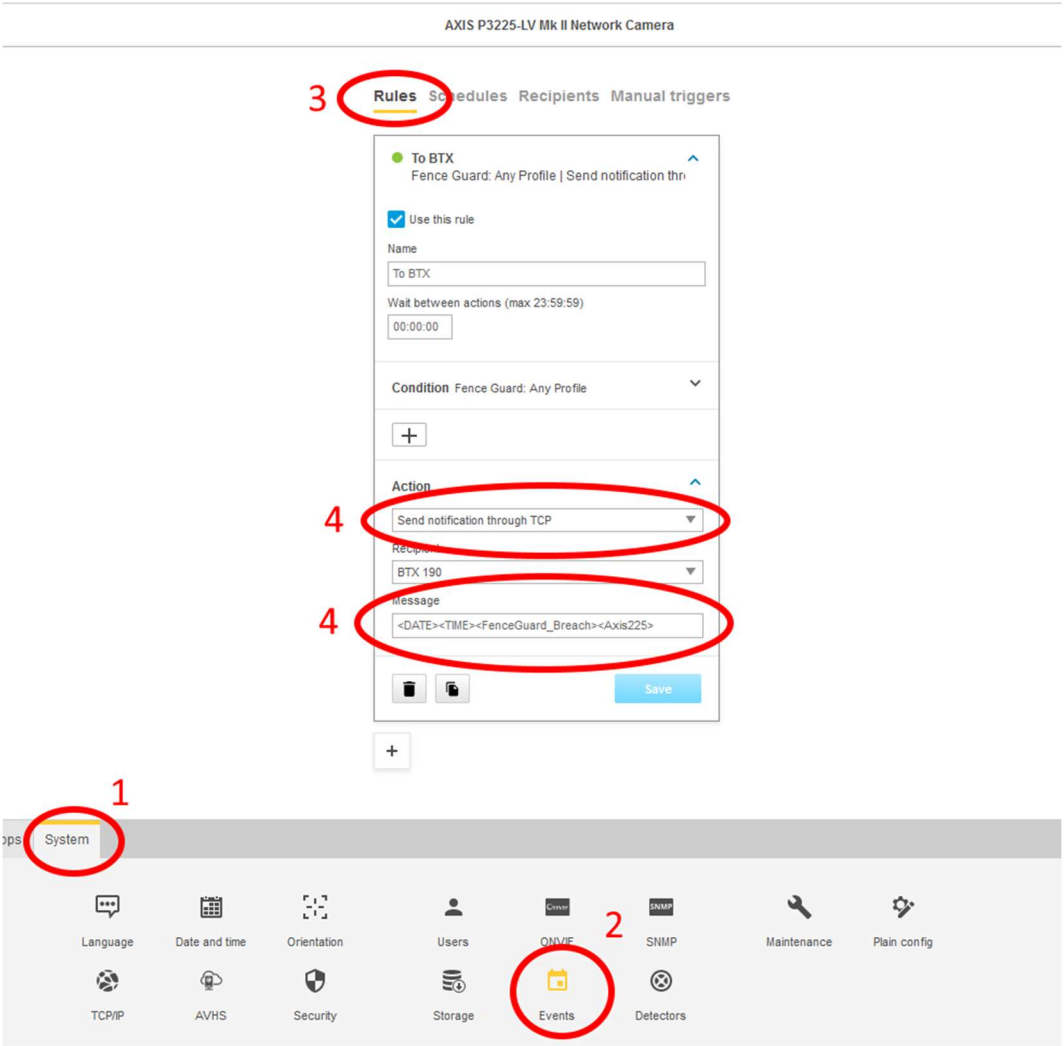
<DATE><TIME><ALARM KEYWORD><DEVICE NAME>
Parameter #1 Parameter #2 Parameter #3 Parameter #4

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.

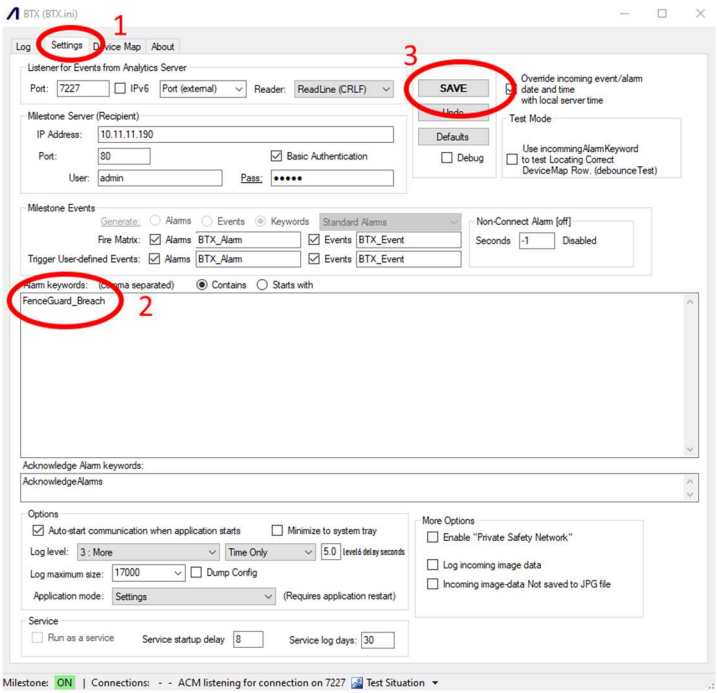
Example: Axis Devices

Axis devices provide a method to send TCP message when device events occur. Use the format above to construct a preferred alarm string.

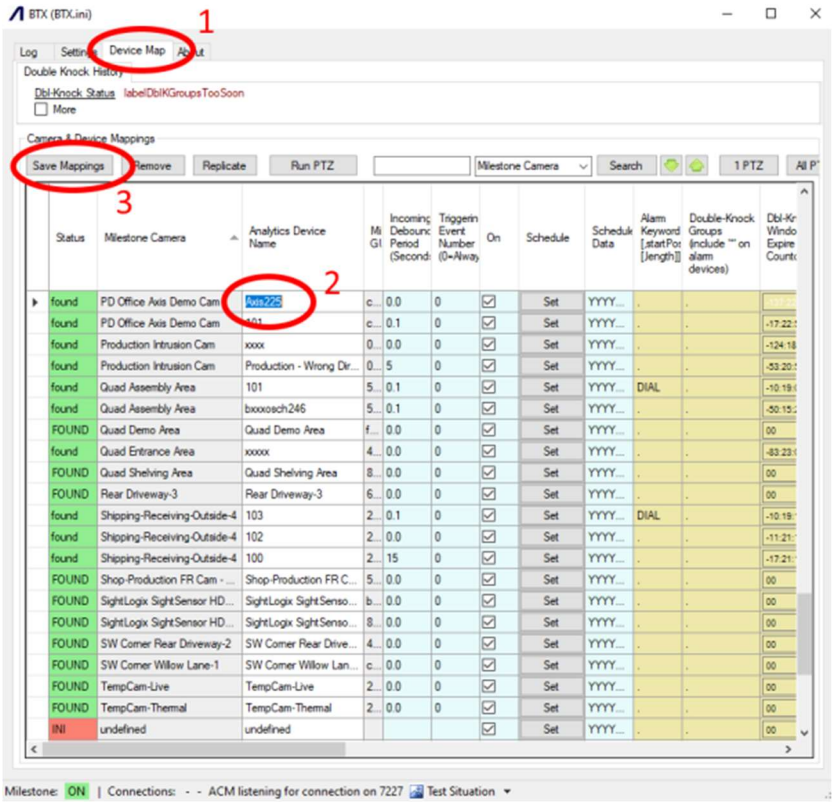
In this case, the **ALARM KEYWORD** is "FenceGuard_Breach" and the **DEVICE NAME** is "Axis225"



To generate alarm in XProtect, add the **ALARM KEYWORD**, "FenceGuard_Breach", to the *Alarm keywords:* field on the BTX Settings tab.



Then associate your DEVICE NAME, "Axis225" to the corresponding device in XProtect by going to the *Device Map* tab and editing the "Analytics Device Name" column.



When this event occurs on the Axis device, BTX will now generate an alarm record with Video Bookmark in XProtect.

8.2. 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 forum or posted on the BTX knowledgebase.

9. Legal

9.1. 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.

9.2. 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.

9.3. 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.

9.4. Disclaimer

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.