BTX™

"Bridge to XProtect"

for

Milestone XProtect

and

Third-party Systems

User Guide

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

March 2019

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, Security and Building Automation.

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. Data Flow

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 into the XProtect database. As such, Smart Client users can search and filter reports by Event and Alarm Keywords, external / third-party Device Name, originating Date and Time, and even the raw Incoming Message String.

1.3. Features

BTX device-specific configuration options include:

- Counters - to de-bounce high event and alarm rates, and reduce false-positives
- Timers - to throttle over-frequent event alarm rates, and reduce false-positives
- Schedules - to define specific time periods within which incoming events and alarms should be processed

BTX "double-knock" configuration options include:

- Groups - combine events and alarms for any combination of devices, to produce a single event or alarm
- (Instead of generating many single events. This function is important, because it facilitates validation of any single alarm, and eliminates false alarms)
- Double-knock Timers - to specify time periods within which all devices in a given group must generate an alarm in order to produce a single master alarm

1.4. Components

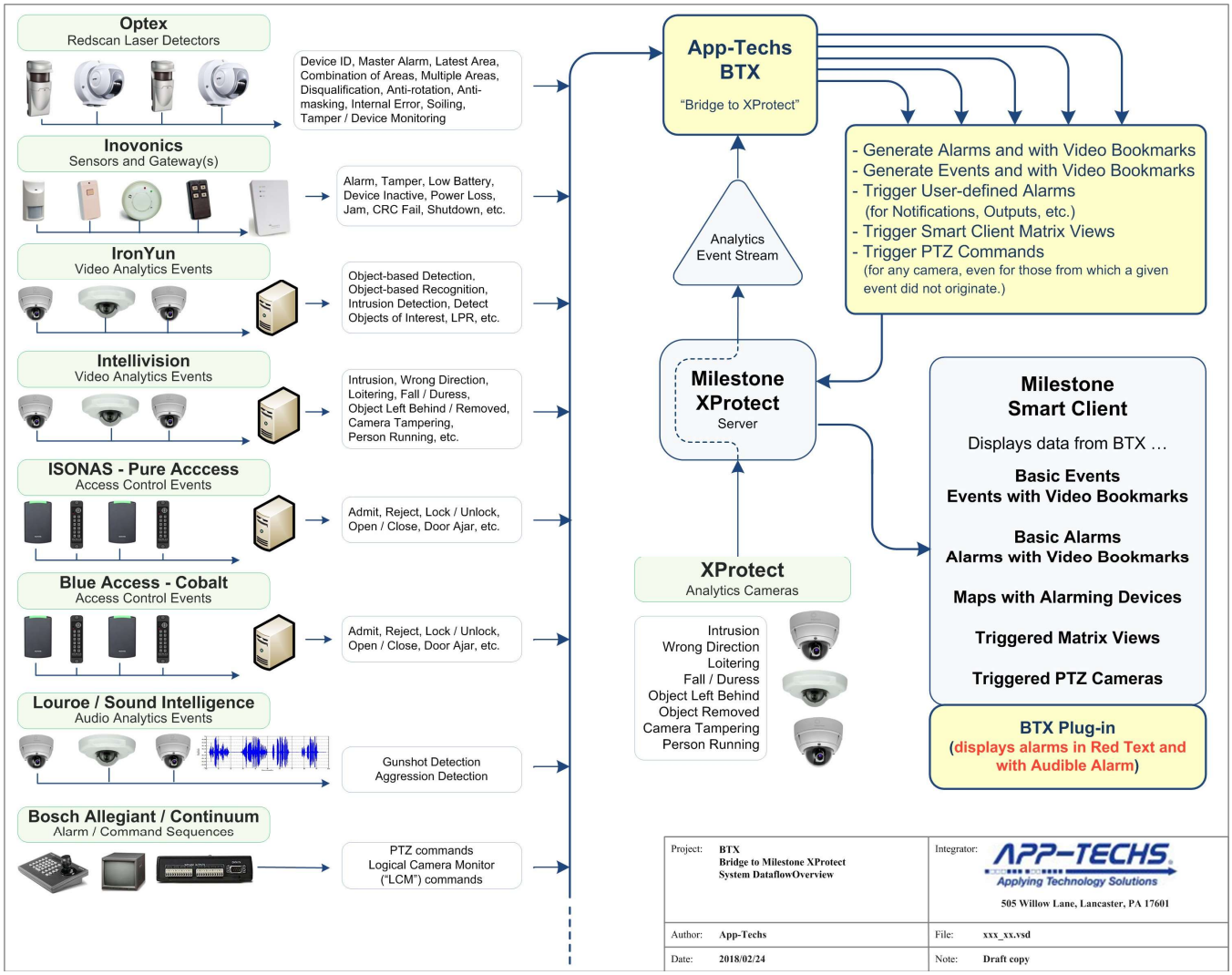
BTX is comprised of three primary components:

- Base System
  - The "**Bridge Server"** facilitates communication between third-party systems and XProtect.
    - Mates with many systems, without need for additional "adapters".
    - Runs on Windows desktop or in the background as a Windows service.
  - The Smart Client operator **Alarm Monitor** plug-in presents users with notification of alarms in real-time.
    - Display alarm contents in red text.
    - Runs in a cell of any standard "view".
    - Installs under the "MIP Plug-ins" directory of each user's workstation.
      - Normally C:\Program Files\Milestone\XProtect Smart Client\MIPPlugins.
  - The Smart Client operator **Alarm Schedule Modifier** plug-in users modify the alarm arm / disarm schedule.
    - Runs in a custom "workspace" (tab) of the Smart Client.
    - Installs under the "MIP Plug-ins" directory of each user's workstation.
      - Normally C:\Program Files\Milestone\XProtect Smart Client\MIPPlugins.

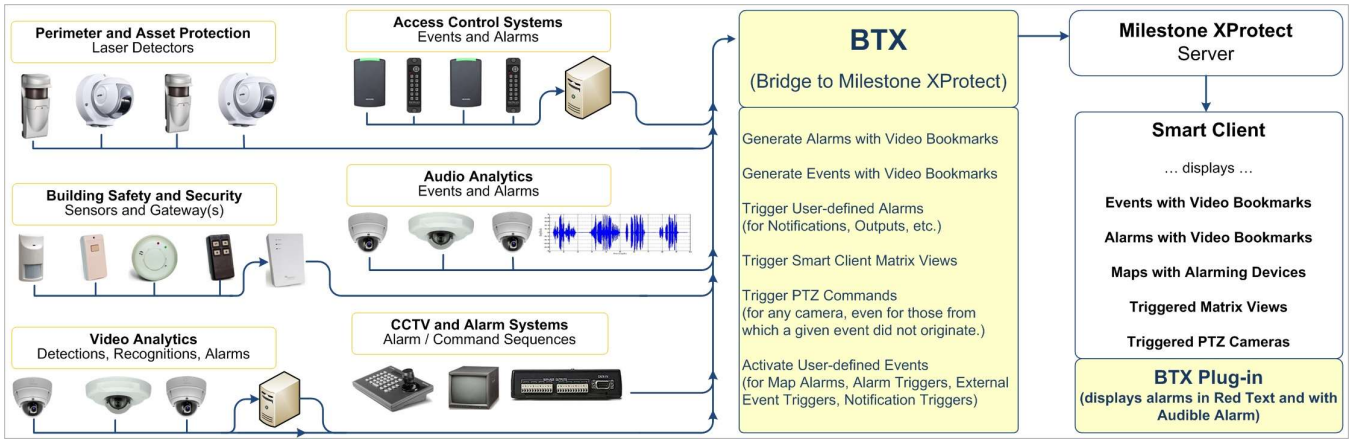
- Add-on Modules
  - The "**Inovonics Connector"** facilitates communication between Inovonics Gateways and BTX.
    - Included with Base System.
    - Mates with many systems, without need for additional "adapters".
    - Optionally sends events directly to XProtect "Generic Events", without BTX.
    - Runs on Windows desktop or in the background as a Windows service.

2. Data Flow

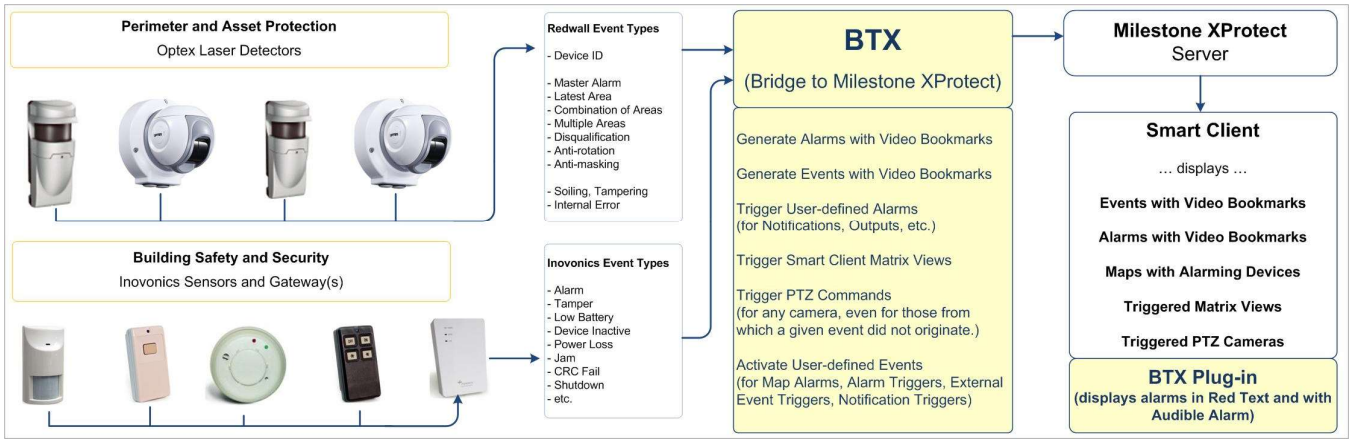
2.1. Overview



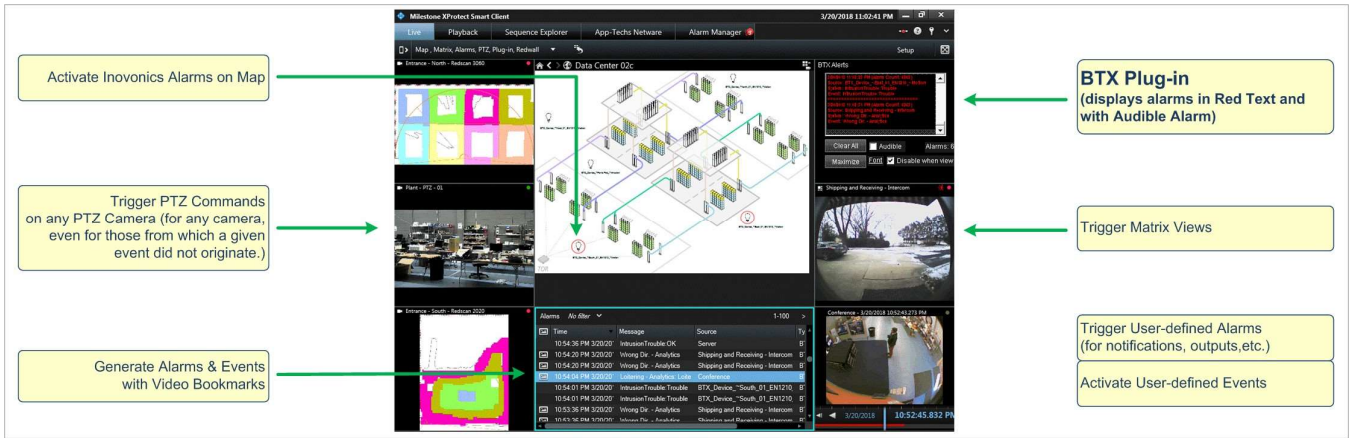
2.2. BTX Receives Third-party Events and Alarms



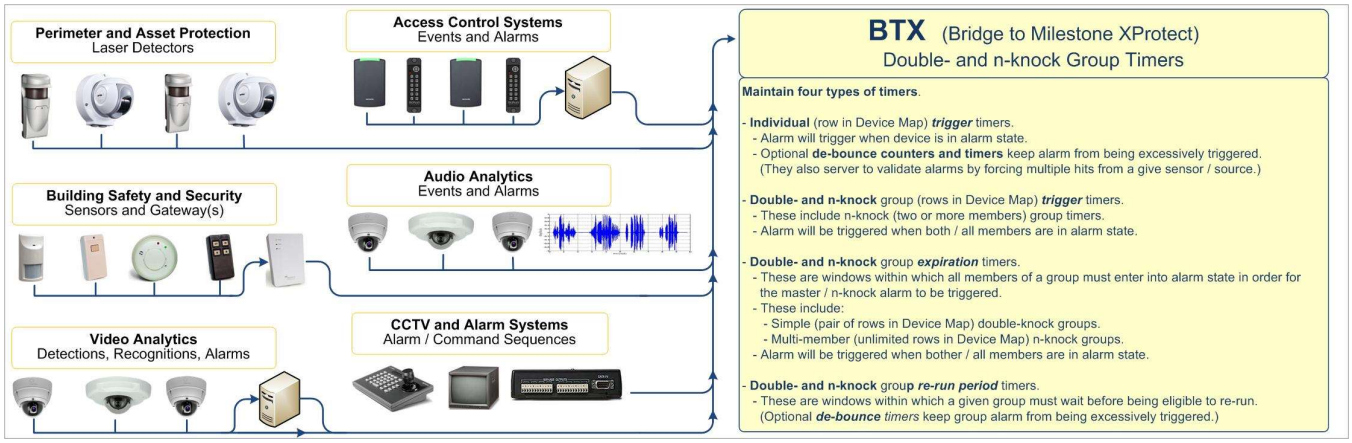
2.3. BTX Filters and Classifies Events and Alarms



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

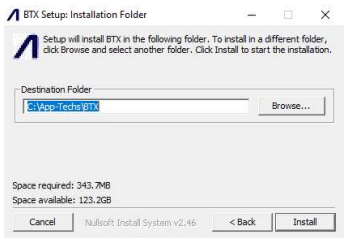
The BTX Server runs on any server which has network connectivity with XProtect and the third-party system(s) of interest.

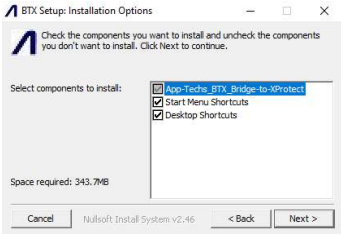
It is typically installed on the same server as the main XProtect services.

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.

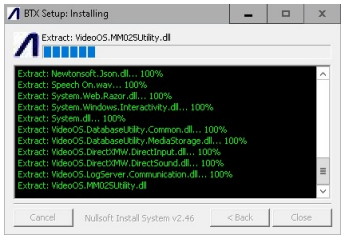
1

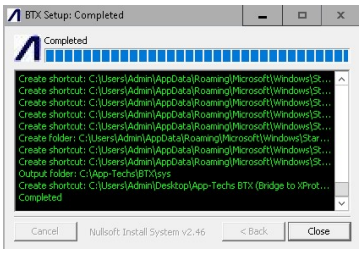




2

3





4

3.3. Smart Client Plug-In

Contact App-Techs for copies of the plug-in download files.

Once files are downloaded, decompress and copy files to the following directory on the workstation c:/ drive:

- C:\ Program Files\Milestone\XProtect Smart Client\MIPPlugins

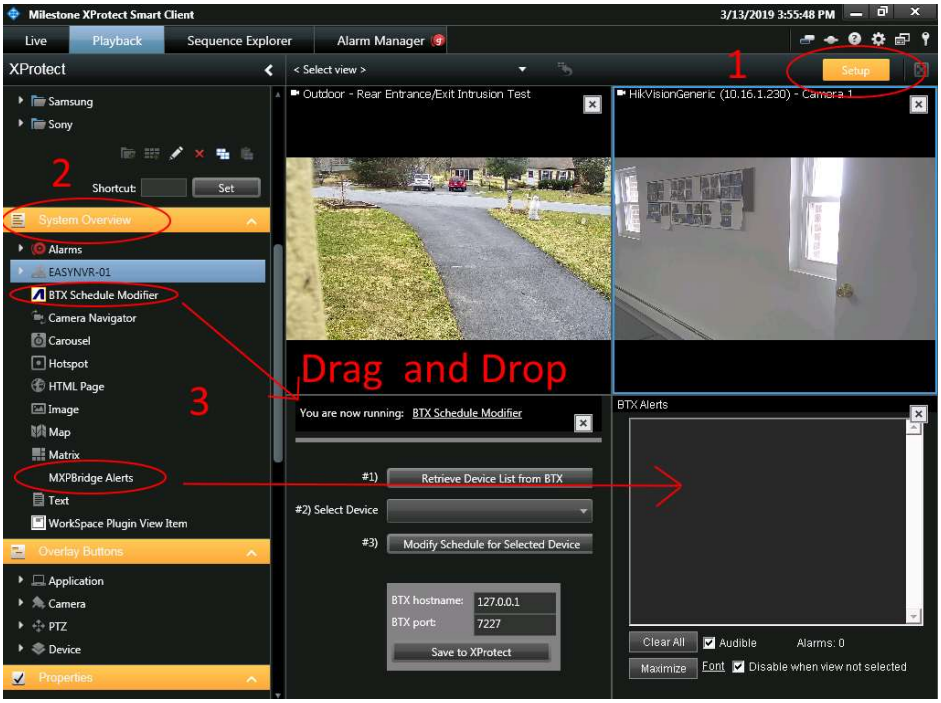
*** Please note that Milestone could be stored in the local Program Files (x86) folder, in which case copy files to the following directory:

- C:\ Program Files (x86)\Milestone\XProtect Smart Client\MIPPlugins

Once the files are copied, close any running versions of the Milestone Smart Client and restart.

1) Upon restart, enter Milestone's Setup mode.
2) Choose a view where the plug-in will be displayted.
3) In the "System Overview" section located in the left-hand tool bar, drag-and-drop "BTX Schedule Monitor" and "MXP Bridge" options into the desired Smart Client window.
4) Exit Setup.

Here is a screenshot in Milestone's Setup mode:



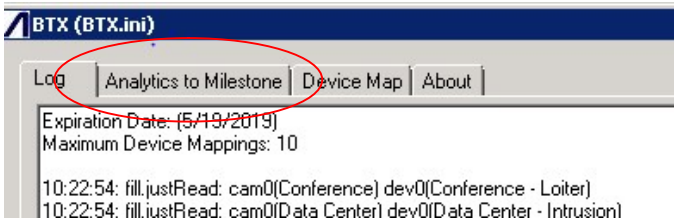
4. Configuration

4.1. Connect BTX with Milestone

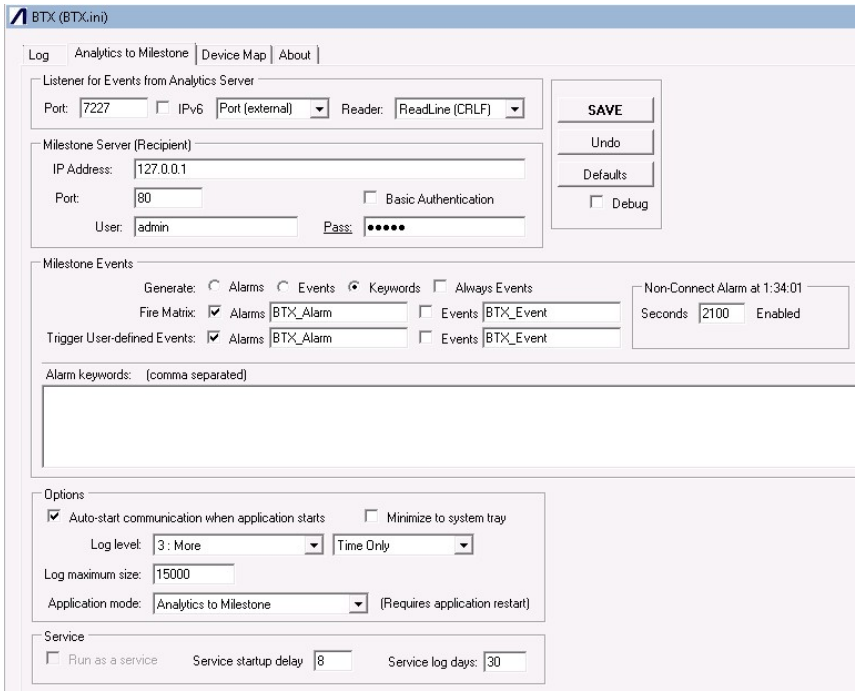
To launch BTX, from the Windows "Start" menu, select …
- All Programs
  - BTX (Bridge to XProtect)
    - Lauch BTX (Desktop for Configuration)

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

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



Enter the correct network configuration settings to connect BTX with Milestone.



4.2. User Field Entry List

Listener for Events from Analytics Server
- Port – Default = 7227 – BTX listens on this port for incoming events and alarms from third-party systems.
- IPV6 – Default = Not checked.
- Reader – Default = CR/LF. Do not change unless specifically required.

Milestone Server
- IP Address: Milestone server IP address and port number. Enter Milestone server admin user/password, NOT the Milestone Smart Client user/pass.

Milestone Events
- Use default settings unless specifically required.

Alarm Keywords
- Specify keywords used in the transaction data for each analytics (third-party) device.
    - Call App-Techs sales for a list of keywords used by the analytics device(s).

Options
- Do not change unless specifically required.

Service
- Do not change unless specifically required.

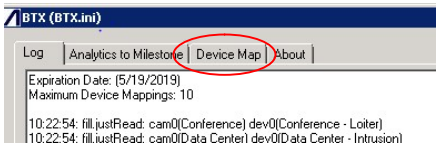
After configuring the network settings, click the “SAVE” button in the top-right corner before exiting.

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

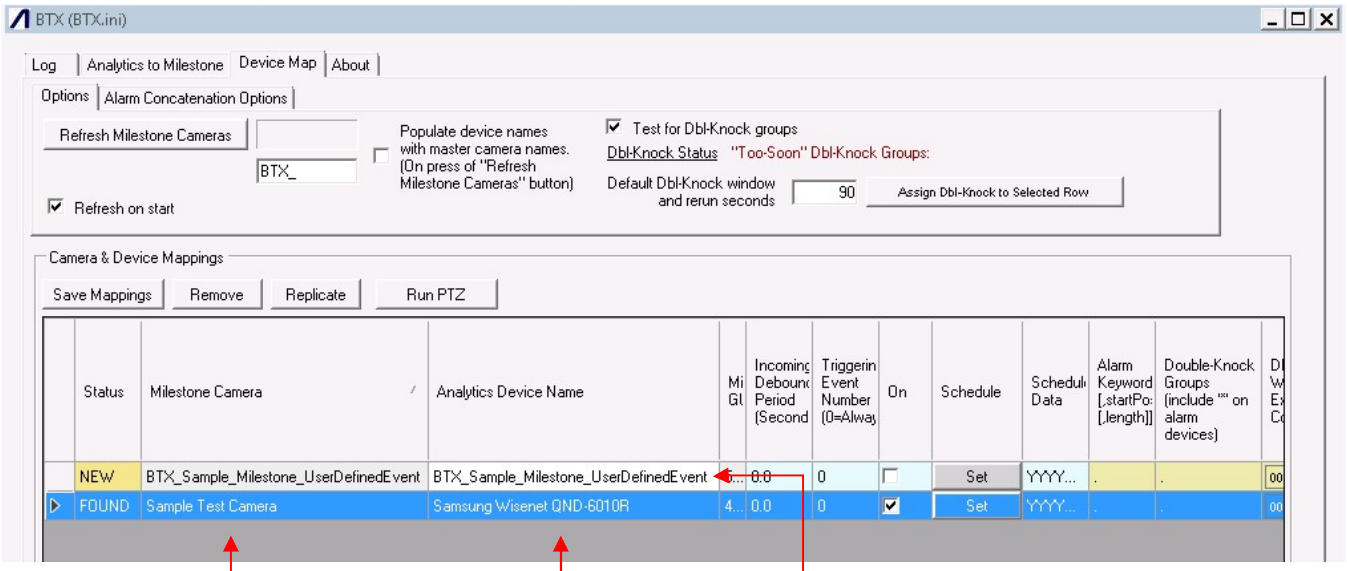
5. Device and Event/Alarm Setup – Basic Functionality

5.1. Associate Analytic Devices with Milestone Camera(s) / User-defined Events(s)

After restarting BTX, click on the "Device Map" tab. Each time BTX is restarted, it automatically scans the Milestone server and compiles an updated list of all active cameras/devices AND user-defined events.



The screen should resemble the following:



The *Milestone Camera* column includes all camera names listed in Milestone AND all user-defined events listed in the Milestone Management Client. **Since this information is imported directly from Milestone, THIS COLUMN CANNOT BE EDITED.**

The *Analytics Device* column is **EDITABLE**. This is where the user associates a third-party analytics device(s) to Milestone cameras and/or User-defined events.

Any User-defined events created in Milestone will be given its own column on BTX "Device Map" tab. Associate the device to the User-defined Event by typing the analytics device name here as specified in the transaction data.

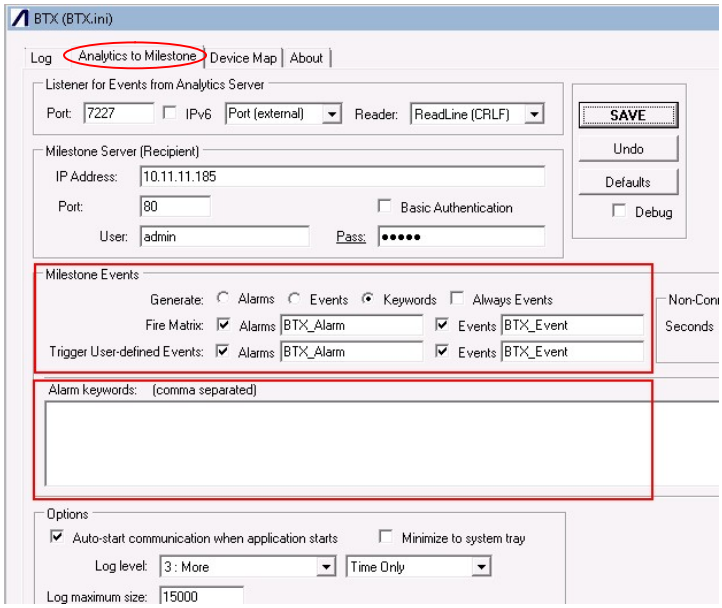
IMPORTANT: To associate the analytics device name (as reported in the transaction data sent to BTX) with a Milestone camera or user-defined event, enter the analytics device name into the *Analytics Device Name* column. (Additional information on User-defined Events is covered in Section 7.2.)

> *Explanation: If an analytics device is using the feed from a Milestone device to identify security events and alarms, it is important to re-associate the analyzed data back with the camera as it is known in Milestone. In many cases, the analytics device assigns a different name than what is listed in Milestone. To compensate, enter the analytics device name as specified in the transaction data into the *Analytics Device Name* column.

Click "Save Mappings" to save settings.

5.2. Managing Events and Alarms

Now that an association has been created between the analytics device and a Milestone Camera, return to the *Analytics to Milestone* tab.



The recommended presets are shown above.

- The Generate: ⊙ Keywords is the most common option. Use default settings unless specifically required.
- Fire Matrix: Milestone initiates a matrix firing when BTX generates an event and/or alarm record.
- Trigger User-defined Events: Milestone will execute pre-configured User-defined Events when BTX generates an event and/or alarm record.

Enter all alerts keywords that will be received in the transaction data from the third-party analytics device into the "Alarm keywords" text box. Separate with a comma without any spaces. If the user does not have a list of keywords used by the third-party analytics device in the transaction data, contact App-Techs tech support.

> Note: By entering third-party device keywords into the "Alarm keywords" field, BTX will define all subsequent matches from incoming transaction data as alarm records to be sent to Milestone.

Click "SAVE" to save settings.

6. Device and Alarm Setup – Advanced Functionality

6.1. Events and Alarm Definitions

When a third-party analytics device reports transaction data, BTX gives users the ability to control whether incidences will be reported to Milestone as an event record or an alarm record.

Event Record

- An Event Record is typically categorized as a security occurrence that has happened under "allowed" circumstances. An example of this would be an authorized person swiping an access card at a door reader.

- In this instance, users typically log an Event Record for tracking purposes. In BTX, transaction data categorized as an event will be reported to Milestone as an Event Record. BTX is configured to trigger an event matrix view in Milestone when an event is logged.

- Since Event Records tag ordinary security occurrences, BTX will report an Event Record to Milestone. By default, an Event Record will not trigger User-defined Events. Triggering is typically reserved for Alarm Records (see below). However, BTX's "Event Triggering" functionality (see Section 6.4) does provide an option to trigger a User-Defined Events with an Event Record (See Section 6.4).

Alarm Record

- An Alarm Record is categorized as a security incident when something happens that is not allowed. An example of this would be if someone tries to access a door they are not allowed to enter.

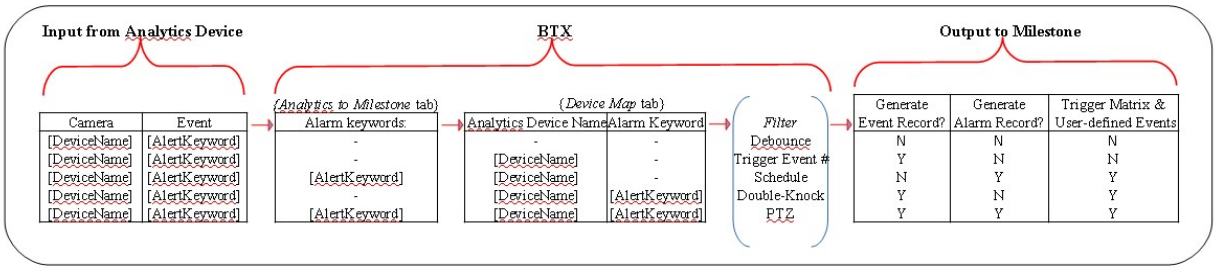
- In BTX, transaction data from a third party device that contains a keyword match in the "Alarm keywords" field (located on the *Analytics to Milestone* tab) will be reported to Milestone as an Alarm Record and will subsequently trigger an Alarm Matrix view and all user-defined events associated with the device.

- BTX filters can be used to control the rate at which Alarm Records are reported to Milestone.

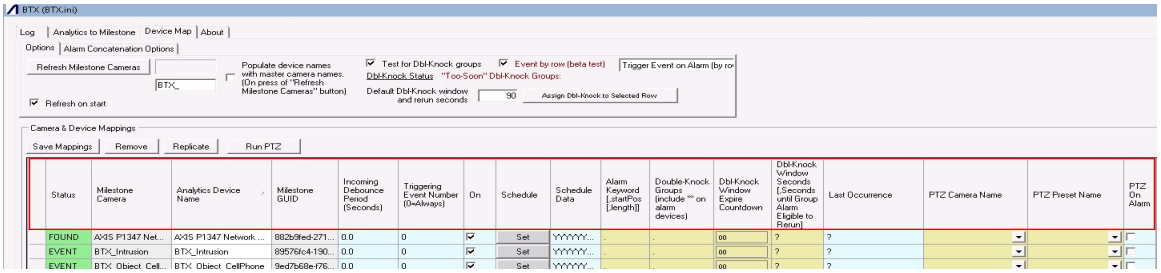
6.2. Summary of BTX Process Flow for Generating Events and Alarms in Milestone

The table below shows the process by which BTX generates Milestone outputs from incoming third-party transaction data when using the Generate: ⊙ Keywords default setting. Note that the " BTX Alarm keywords" field on the *Analytics to Milestone* tab and the "Alarm Keyword" column on to the *Device Map* tab are the two key fields that determine the following: 1) whether an event or alarm record are sent to Milestone, and 2) whether BTX triggers a User-defined Event(s).

Transaction data sent from third-party analytics device:
Ex: <Date><Time><DeviceName><AlertKeyword>



6.3. 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.
  - FOUND – A active device imported from the Milestone device list
  - NEW – A user-defined event that is newly recognized by BTX.
  - INI – An inactive device imported from the Milestone device list
  - EVENT – A User-defined event that has been associated with an analytics device name

- 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

- A label for all camera names and user-defined events listed in Milestone. Since this column is data imported from Milestone, it cannot be edited.

Analytics Device Name

- The *Analytics Device* column is editable. Associate to third-party analytics device to Milestone cameras and/or User-defined Events by typing the analytics device name here as specified in the transaction data.

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 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 debounce period.

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 minimizing false-positives and managing high incoming alert rates.

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.

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

6.4. Highlighted BTX Filtering Options

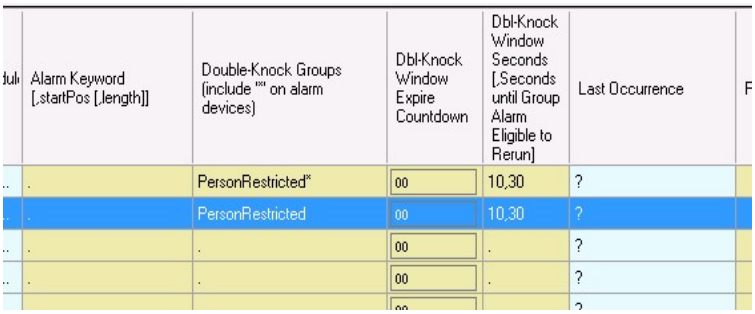
Debounce
- The "Incoming Debounce Period (Seconds)" column allows the user to throttle high event and alarm creation rates. This can be useful when a third-party device reports multiple, redundant alarms for a singular security event. By employing the debounce filter, BTX creates only one event and/or alarm record in Milestone 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 Milestone 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 Milestone 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 with a 30 second time window.



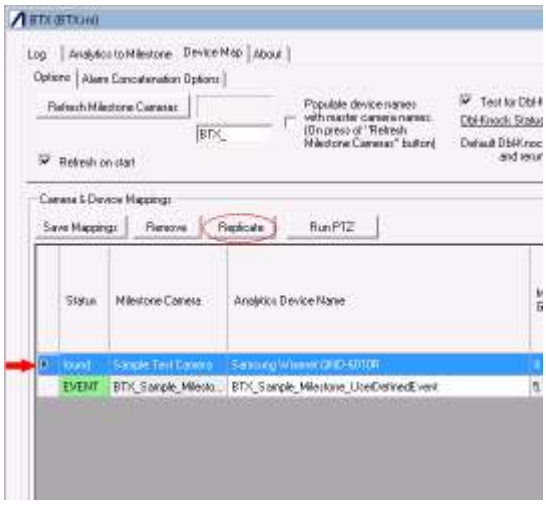
	Alarm Keyword [,startPos [,length]]	Double-Knock Groups (include "*" on alarm devices)	Dbl-Knock Window Expire Countdown	Dbl-Knock Window Seconds [,Seconds until Group Alarm Eligible to Rerun]	Last Occurrence	F
..	.	PersonRestricted*	00	10,30	?	
..	.	PersonRestricted	00	10,30	?	
..	.	.	00	.	?	
..	.	.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

PTZ

- Additional information will be published in a future manual. Please call App-Techs with any questions about the PTZ feature.

6.5. Replicate *Device Map* Columns

To associate multiple analytic devices to a single Milestone device or User-defined event, use the "Replicate" button to create a new column. Enter a new *Analytics Device Name* in the newly created column.

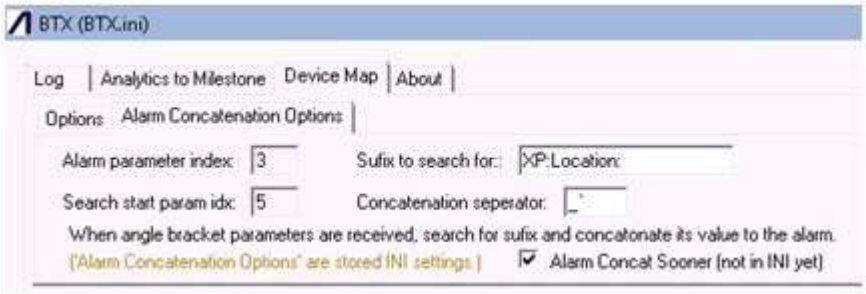


Click "Save Mappings" save settings.

6.6. **Concatenate**

Concatenation allows users to join two separate transaction 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 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 5th 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 Milestone 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 *Analytics to Milestone* tab.

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

7.1. Overview

User-defined events in Milestone link Event and Alarm Records to additional security actions performed by either Milestone and/or third-party devices.

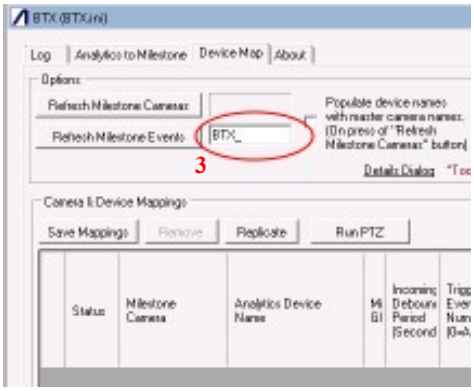
- When launched, BTX scans the Milestone Management Client for all user-defined events that begin with the prefix "BTX_" (by default) and displays each User-defined Event as a row in the BTX *Device Map* tab.
- Users then associate a third-party analytics device with the User-defined Event by editing the "Analytics Device Name" column.
- The "Replicate" feature can be used to associate multiple analytic devices to a single User-defined Event (see Section 6.5).
- Any incoming data categorized by BTX as an alarm or event-trigger (see section 6.4) will trigger a User-defined Event associated with the analytics device.
- Once a User-defined Event is triggered, the Milestone *Rules* tool controls what additional actions are executed by Milestone and/or third-party devices.

7.2. Create User-defined Events in Milestone

1 In the Milestone 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 Be sure your User-defined Event name begins with the prefix specified in the field located on the *Device Map* tab in BTX. The default is "BTX_". This is the text string BTX searches for when auto-generating a list of Milestone User-defined Events.



4 Enter name of User-defined Event.

Be sure to click "Save" in Milestone. 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 Milestone cameras.

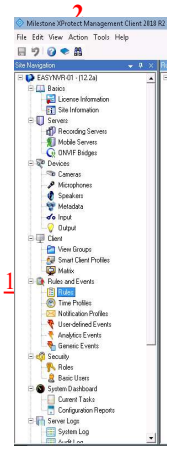
7.3. Link *User-defined Events* to *Rules* in Milestone

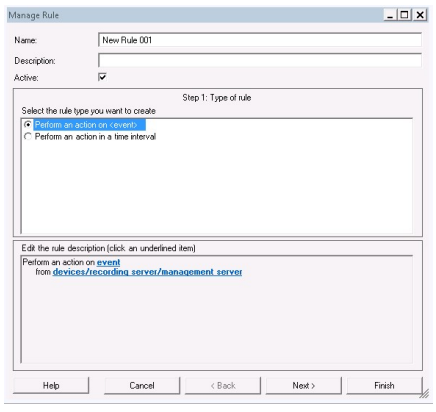
Trigger Action using Milestone Rules

1 In the Milestone 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 Milestone is being used to receive video from any camera at a location of an alarm or event.

- The Milestone 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.

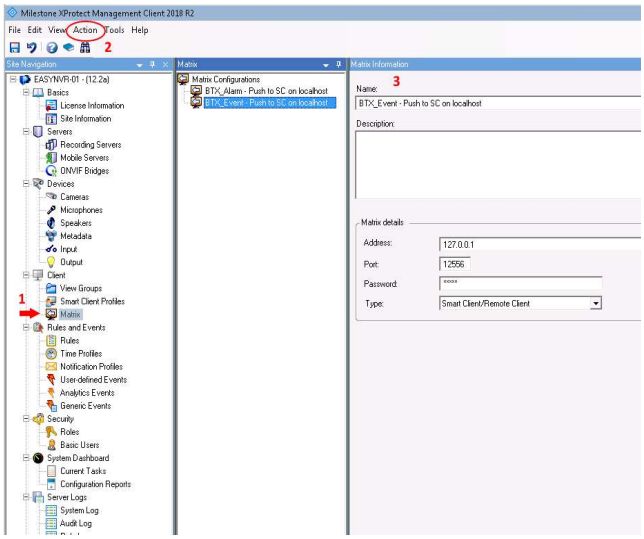
- Another valuable feature of the Milestone Smart Client (only available when using Milestone XProtect Enterprise, Expert, and Corporate) is the alarm manager. This allows the user to view a list of alarms and escalate/manage them. In the alarm manager, an alarm can be forwarded to a manager or other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

To configure a Matrix Display:

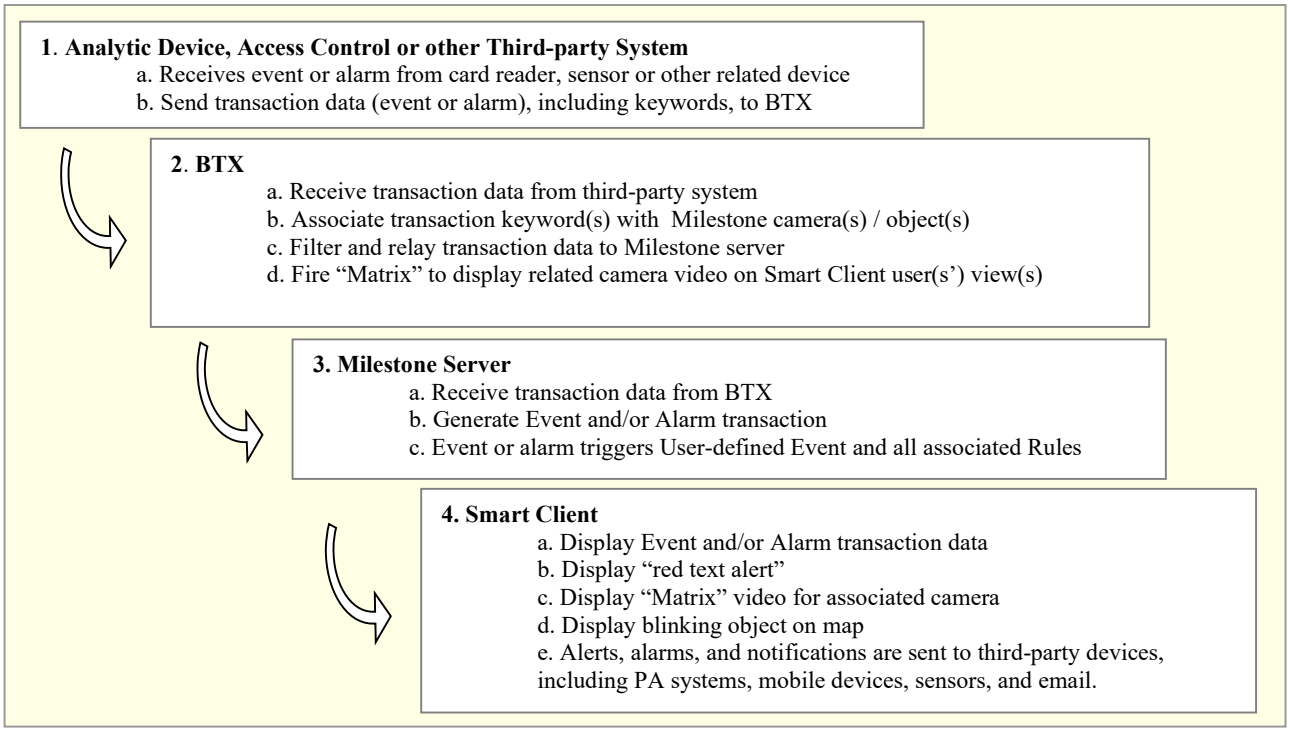
1 In the Milestone XProtect Management Client, go to the Site Navigation bar on the left hand side of the screen and select *Matrix*.

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. Summary - Typical Event / Alarm Sequence



8. Legal

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.