



Metrasens Ultra™

Integration with Milestone XProtect

User Guide

*Keep people, property, and sensitive information safe
by accurately detecting ferrous threat objects
and receiving detection alarms
in Milestone XProtect*

August 2023

First Edition Copyright © August 2023, App-Techs Corporation.
“Spotlight” and the App-Techs logo are trademarks of App-Techs Corporation.
Other trademarks belong to their respective Owners.
All Rights Reserved

Summary

This document provides a basic overview, installation, and operating instructions for the Metrasens Ultra™ integration with Milestone XProtect.

Table of Contents

1. Metrasens Ultra™ Milestone XProtect Integration..... 3
 1.1. Product Summary 3
 1.2. Basic Data Flow 3
 1.3. Data Flow Diagram 3
 1.4. Integration Features 4
 1.5. Installation 4
 1.6. Run the BTX Metrasens Listener (“BML”) as a Windows Scheduled Task 4
 2. BTX Metrasens Listener (“BML”) Setup and Configuration..... 5
 2.1. Configure the BML to connect with Metrasens Ultra™ detection units..... 5
 2.2. Configure connection to the BTX (Bridge-to-XProtect)..... 6
 2.3. Confirm the BML connection with BTX..... 6
 3. Configure Bridge-to-XProtect (“BTX”) to Integrate Metrasens Device Events with Milestone XProtect 7
 4. Metrasens Listener Settings 7
 4.1. Device Entry and Detection Filter Options..... 7
 4.2. Alarm Parameter, Logging, and Edge Device Health Monitoring Settings 8
 5. FAQ 9
 5.1. Can the integration run in the background? 9
 5.2. Can multiple Metrasens Ultra™ devices be mapped to a single XProtect camera / device? 9
 6. Legal 10
 6.1. Surveillance Privacy 10
 6.2. Disclaimer 10

1. Metrasens Ultra™ Milestone XProtect Integration

1.1. Product Summary

Metrasens Ultra™ Advanced Detection Technology accurately detects ferrous threat objects, inclusive of both weapons and data recording devices as small as MicroSD cards.

With Bridge-to-XProtect (“BTX”), alarms from Metrasens Ultra™ detection units become visual and audible alerts in the XProtect Smart Client.

BTX receives, filters, classifies detections from any number of Metrasens Ultra™ devices. Based on user-defined settings and filters, BTX transforms the Ultra™ detections into XProtect event and/or alarm records with video bookmarks. The integration provides real-time situational awareness for XProtect Smart Client operators and retroactive video evidence review capabilities.

The integration requires no management / event server plug-ins and little to no settings changes in the XProtect Management Client.

BTX brings the added safety of Metrasens Ultra™ to your Milestone XProtect VMS.

1.2. Basic Data Flow

BTX uses a sub-system called the **BTX Metrasens Listener (“BML”)** to establish a secure connection with the Metrasens Ultra™ detection unit.

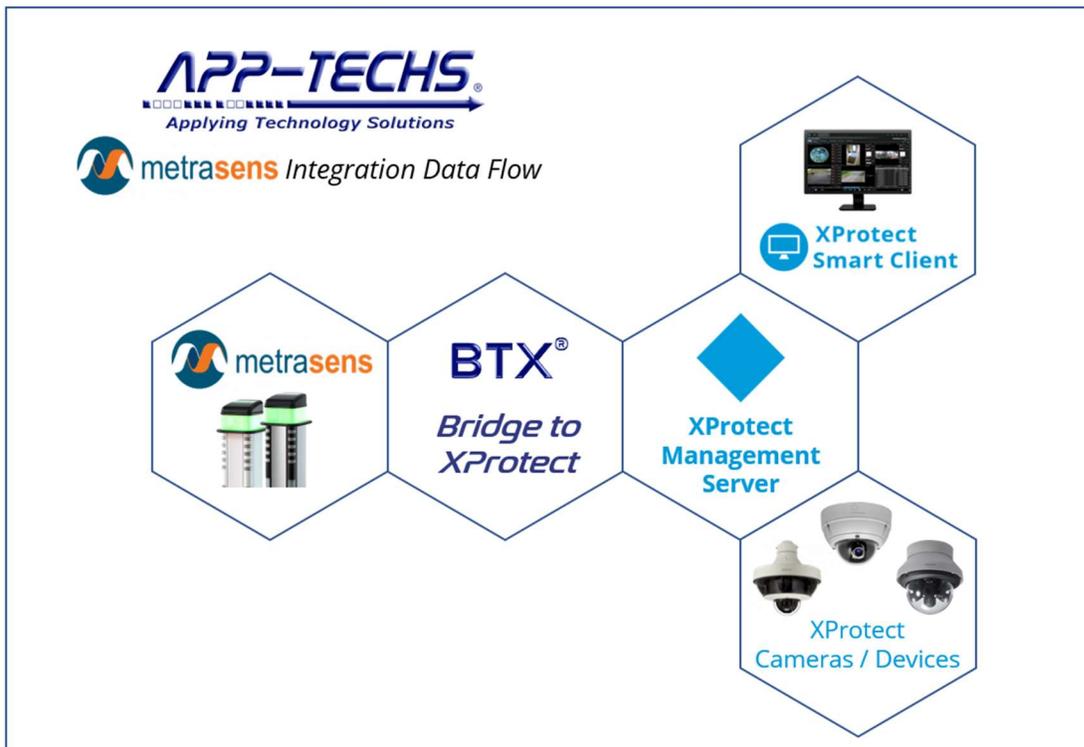
The BML receives Metrasens Ultra™ detection data in real-time. User-defined filters classify the incoming detections, and qualifying alarms are forwarded to BTX. Non-qualifying alarms are logged as “received” and then ignored.

In BTX, qualifying alarms are easily associated with XProtect cameras and forwarded to XProtect as event or alarm records with Video Bookmarks.

BTX provides additional features to activate PTZ presets, display live matrix views, and fire XProtect user-defined events with minimal configuration required in the XProtect Management Client.

The result: a qualifying Metrasens Ultra™ detection triggers immediate security action in Milestone XProtect.

1.3. Data Flow Diagram



1.4. Integration Features

The Metrasens Ultra™ integration with BTX provides the following functionality for use with Milestone XProtect:

- **ASSOCIATE** Metrasens Ultra™ detections to any number of XProtect Cameras.
- **GENERATE** event and/or alarm records with Video Bookmarks.
- **FILTER** device events by source, signal strength, and detection zone.
- **TRIGGER** XProtect user-defined events to activate rules, notifications, announcements, strobes, and other security actions.
- **DISPLAY** XProtect Smart Client live matrix views when a device is activated.
- **CREATE** situation-specific, site specific alarm names and messages for easy understanding and action.
- **SEARCH** detection metadata in the Smart Client.
- **MONITOR** the online / offline status of Metrasens Ultra devices for added reliability and safety.

1.5. Installation

BTX and the BML are typically installed on the Milestone XProtect Management Server.

After installing BTX, the BML can be found in the following directory:

- C:\App-Techs\BTX\Third-party\Metrasens

To configure, run

- "MetrasensToBTX.exe" (BTX Metrasens Listener) as a desktop application.

The BML itself does not require licensing. However, BTX requires a valid license to receive Metrasens Ultra™ alarms and send them to Milestone XProtect.

1.6. Run the BTX Metrasens Listener ("BML") as a Windows Scheduled Task

Once devices are configured, "MetrasensToBTX.exe" (BML) may be run in the background as a Scheduled Task. To set up as a schedule task, follow the directions below.

- Open the Task Scheduler on the system that will be running the MetrasensToBTX.exe application.
- In the Actions pane on the right, click Import Task.
- Navigate to the following file and select it:
 - o C:\App-Techs\BTX\Third-party\Metrasense\MetrasensToBTX_TaskScheduler.xml
- Select the Change User or Group ... button.
 - o Specify the user that you wish to run this task and click "Check Names" to verify the user and then click OK to close the selection.
 - o If you have located the application in the default location, no other modifications should be necessary.
- Click OK to finish creating the task and supply the password for the user specified.

The scheduled task will run at start-up or it can be manually run by clicking the "Run" button in the Actions pane. Optionally, start and stop the scheduled service from a command line:

Run Task

```
schtasks /run /TN "MetrasensToBTX_TaskScheduler.xml"
```

End Task

```
schtasks /end /TN "MetrasensToBTX_TaskScheduler.xml"
```

2. BTX Metrasens Listener (“BML”) Setup and Configuration

The BML is a sub-system that communicates with Metrasens Ultra™ detection units. It establishes a secure connection and detects changes to the device’s current state.

Based on user-defined settings, qualifying detections are forwarded to BTX. Non-qualifying alarms are logged as “received” and then ignored. BTX provides the user-interface to associate Metrasens Ultra™ devices with XProtect cameras.

2.1. Configure the BML to connect with Metrasens Ultra™ detection units.

Open the BML as a Desktop application.

- C:\App-Techs\BTX\Third-party\metrasens\MetrasensToBTX.exe

Go to the “Detectors” tab.

Enter the preferred device name, IP address, and device credentials for each Metrasens Ultra™ detection unit. Optionally, add qualifying filters.

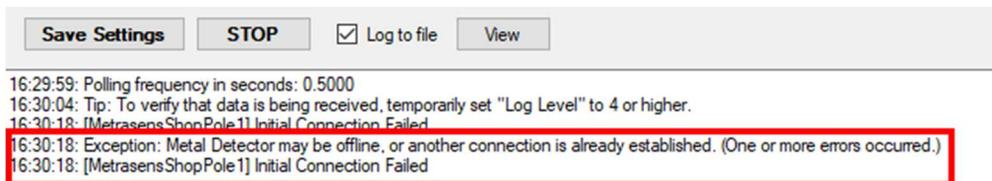
Device Id	Uri Prefix	Uri Suffix	Signal Op	Signal Strength	Zone	User	Password
NW_Entry1	https://10.11.11.204	system:detectors	>=	3	1,2,3,4,5	user	password
Name	Device IP			Filters		user / pass	

Click “Save Settings.”

To test connections, click the “Start” Button and generate a test alarm. If the connection is successful, the log window will display a device event message.



If the connection fails, the log will report a Lost Connection message.



Check your IP address, device credentials, and network / firewall and retry.

2.2. Configure connection to the BTX (Bridge-to-XProtect)

In the “Output to BTX” section, enter the IP address of the server where BTX is installed (typically 127.0.0.1. Default BTX port is 7227).

Save settings.

2.3. Confirm the BML connection with BTX.

Generate a test Metrasens Ultra™ detection and check the BML log window to confirm the event was relayed to BTX.

To confirm the device event is successfully received by BTX (Bridge-to-XProtect), open BTX and check the log window. With proper configuration, the BTX log window will also display the event data as received from the BML in real-time.

3. Configure Bridge-to-XProtect (“BTX”) to Integrate Metrasens Device Events with Milestone XProtect

Refer to the BTX User Manual for instructions on associating Metrasens Ultra™ detection events with XProtect cameras and sending events and alarms to Milestone XProtect.

The BTX User Manual can be found in the following directory:

- C:\App-Techs\BTX\doc

4. BTX Metrasens Listener (“BML”) Settings

4.1. Device Entry and Detection Filter Options

Detectors Settings											
	Active	Connection Status	Description	Device Id	Uri Prefix	Uri Suffix	Signal Op	Signal Strength	Zone	User	Password
	<input checked="" type="checkbox"/>	Connected	Northwest Lobby	NW_Entry1	https://10.1.2.100	https://10.1.2.100	>=	3	1,2,3,4,5	user1	pass1
	<input checked="" type="checkbox"/>		Southwest Lobby	SW_Lobby1	https://10.1.2.101	https://10.1.2.101	>=	1	1,2,3,4,5	user2	pass2
	<input type="checkbox"/>		Southwest Lobby2	SW_Lobby2	http://10.16.1.102	https://10.16.1.102	>=	1	1,2,3,4,5	user3	user3
*	<input type="checkbox"/>										

Active (checkbox) – On / off toggle for monitoring for individual devices. Box must be checked to receive detections from an edge device.

Connection Status (Status) – Not editable. Displays if the listener is actively connected to an edge device.

Description (text field) – Add useful notes. This field is not used as part of the integration with XProtect.

Device Id (text field) – This field is sent to BTX as the Device Name. This field is used in BTX “Device Map” tab to associate Metrasens Ultra™ edge devices with XProtect cameras.

URI Prefix (text field) – Do not change unless instructed to by App-Techs. Changes to the field will prevent connection to the edge device.

URI Suffix (text field) – Do not change unless instructed to by App-Techs. Changes to the field will prevent connection to the edge device.

Signal Op (dropdown) – Filtering option related to Signal Strength text field. Ex. *“Qualify detections with a signal strength of 3 or greater as alarms to be sent to BTX. Detections of signal strength 1 or 2 will be logged and ignored.”*

Signal Strength (text field) – Enter a value between 1-5.

Zone (text field) - Filtering option related to Zone. Zone is the vertical sensor location. Possible zone options are 1-5. 1 is at floor-level, 5 is at head-level. Omit a zone to ignore detections from this region.

User (text field) – Enter Metrasens Ultra™ device username for authentication.

Password (text field) - Enter Metrasens Ultra™ device password for authentication.

4.2. Alarm Parameter, Logging, and Edge Device Health Monitoring Settings

Alarm Message

Alarm message:

Include Signal Strength in alarm message

Include Location Zone in alarm message

Polling Parameters

Polling frequency in seconds:

Retry frequency in seconds:

Offline Seconds until BTX Alert:

Offline message keyword:

Miscellaneous

Log maximum size: Auto-Start active detectors

Log level:

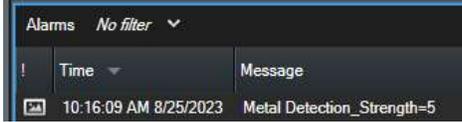
BTX Alarm date:

Log days: Format JSON to Log

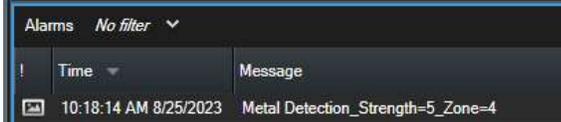
Alarm message (text field) – User can define the alarm message to appear in the XProtect Smart Client Alarm List. Default is “Metal Detection.”



Include Signal Strength in alarm message (checkbox) – Option to report signal strength as part of the alarm message in the XProtect Smart Client Alarm List.



Include Location Zone in alarm message (checkbox) – Option to report zone as part of the alarm message in the XProtect Smart Client Alarm List.



Polling Frequency in seconds – Default is 0.5 seconds. Controls how often the BML polls the status of edge device.

Retry frequency in seconds – Default is 30 seconds. If the connection to the edge device is lost or severed, the BLM will automatically attempt to reconnect.

Offline Seconds until BTX Alert – Default is 60 seconds. If the BLM cannot re-establish a connection with the edge device within this period, the Metrasens listener will send an alarm message, which BTX can forward to XProtect to trigger notifications.

Offline message keyword (textbox) – User can define the alarm message to appear in the XProtect Smart Client Alarm List when a device is reported as offline.

Log Max Size (dropdown) – Limit log file size.

Log Level (Dropdown) – Limit log messages to device events only (log level 3 or lower), or monitor polling status for testing (log level 4 or 5)

Auto-Start active detectors (checkbox) – Default is checked. If unchecked, when the Metrasens Listener is run a scheduled task, it will not automatically begin monitoring devices.

Log Level (Dropdown) – Limit log messages to device events only (log level 3 or lower), or monitor polling status for testing (log level 4 or 5).

BTX Alarm date: (Dropdown) – Report the detection date and time to XProtect AS REPORTED BY the edge device, or optionally ignore the device time and substitute the listener’s SYSTEM TIME.

Log days: Choose how long to store log files locally.

Format JSON to log (checkbox) – For diagnostic purposes. Reports device events in a more readable format in the log file.

5. FAQ

5.1. Can the integration run in the background?

A: Yes. Section 1.6 above details how the BML can be run as Windows Scheduled Task. When running as a scheduled task, make sure the **Auto-Start active detectors checkbox** is checked.

5.2. Can multiple Metrasens Ultra™ devices be mapped to a single XProtect camera / device?

A: Yes. In BTX, open the “Device Map” tab and simply replicate a row that corresponds to the XProtect camera device in question and add the second device to the newly-created row. Click save. PTZ presets can be mapped for each device. Refer to the BTX User Manual for additional information.

6. Legal

6.1. 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.

6.2. Disclaimer

Copyright © 2023 App-Techs Corp., First Edition, First Printing: October 2023.

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.

Spotlight™, BTX™, BIX™, Latest Alarm™, and the App-Techs 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.