VMS Gateway

Integration & Configuration Guide

Milestone XProtect®

Version 1.13

August 27, 2019

This Guide

This integration guide describes the steps for setting up and ensuring communication between the AnyVision Better Tomorrow, VMS Gateway, and Milestone XProtect®, a third-party video management system for IP surveillance.

Table of Contents

List of Tables

List of Figures

Important Notice

The information specified herein constitutes proprietary and confidential information of AnyVision.

The information specified herein is provided solely for your internal use and you shall not disclose the Information to any third party. Unauthorized use or disclosure of such information would cause irreparable harm to AnyVision.

The information specified herein is provided "as is" and AnyVision makes no representations or warranties of any kind, express or implied, with respect to the information in this publication, and specifically disclaims implied warranties of accuracy, completeness, merchantability, title, non-infringement and/or fitness for a particular purpose.

AnyVision reserves the right to make changes in or to the said information, or any part thereof, in its sole judgment, without the requirement of giving any notice prior to or after making such changes to the information.

Use, copying and distribution of any AnyVision software described in this publication require an applicable software license.

All product names, logos and brands are property of their respective owners. All company, product and service names used in this website are for identification purposes only.

The AnyVision logo is a trademark of AnyVision.

1. Milestone VMS—AnyVision: Integration Overview

1.1. About this Integration Guide

VMS Gateway is an AnyVision component that enables Better Tomorrow to connect with third-party VMS clients and receive from them video for security monitoring and forensic analytics.

VMS stands for Video Management System. A VMS is a security camera component that collects video from cameras and various devices. A VMS records and stores video to storage devices, and provides an interface for viewing live video, while providing access to recorded video.

This guide describes the steps for integrating the three key components making up the VMS environment. Topics include:

- Installing the **VMS Gateway** and configuring the **VMS** client;
- Ensuring correct configuration of components and the ability to import video for analytics by **Better Tomorrow (BT)**;
- Confirming that the VMS client, through the VMS GW, is able to send events to and alarms to AnyVision BT regarding recognition of faces.

VMS integration ensures that AnyVision Better Tomorrow, VMS Gateway computer, and Milestone XProtect® video management software are installed, configured, and able to communicate with one another. Once these components are integrated and configured, AnyVision BT can detect faces, enabling Milestone XProtect to issue alarms, generate events, and monitor security.

See Figure 1 in section 2.3, Architecture, for a high-level visualization of the above components.

IMPORTANT

This document illustrates and explains the full procedure for a fresh installation of video management system, end-to-end. If your VMS has already been configured, fully or partially, some of the procedures, steps, or parameter definitions might not be applicable.

1.2. Purpose and Scope

This guide describes how to install the VMS Gateway and Milestone XProtect video management software and configure AnyVision Better Tomorrow to communicate with third-party video cameras. Here is a brief summary of what you'll find in the sections that follow.

TABLE 1. SECTION SUMMARY

Section 2, About the VMS Gateway	Describes the capabilities, components, and architecture of AnyVision's VMS Gateway, and prerequisite steps to ensure a smooth integration process
Section 3, VMS Integration	
Section 3.1, Process Flow	Provides a workflow walking you through the end-to-end VMS integration process
Section 3.2, Gateway and Management Setup	Describes Gateway and video management software installation, ensuring ANV-client connectivity, and configuring the VMS Gateway
Section 3.3, Importing Video for Analytics	Describes how to configure AnyVision BT, including server settings, and camera selection for live video and forensic import
Section 3.4, Managing Alarms	Describes how to validate integration by sanity checking that live image display occurs in the third-party VMS, that BT can communicate with VMS, and that VMS can issue alarms

1.3. Concepts, Terms, and Abbreviations

Familiarity with the terms, concepts, and abbreviations appearing below could prove useful in helping ease the process of performing integration of AnyVision Better Tomorrow, VMS Gateway, and third-party video management products.

TABLE 2. CONCEPTS, TERMS, AND ABBREVIATIONS

Term, Concept, or Abbreviation	Meaning
ANV	AnyVision
API	Application Programming Interface
BT	Better Tomorrow. AnyVision's tactical application for facial recognition that enables detecting, identifying, and obtaining real-time alerts about POIs
GW	Gateway
POI	Person of Interest
RTSP	Real Time Streaming Protocol
SDK	Software Development Kit
V2C	Vendor to Customer
VMS	Video Management System

2. About the VMS Gateway

This section introduces the VMS Gateway in detail, describing its:

- Capabilities (see section 2.1);
- Components (see section 2.2);
- Architecture (see section 2.3);
- System Requirements (see section 2.4).

Taking care to ensure all the items above are in place, from the outset, can best ensure a smooth integration process.

2.1. Capabilities

AnyVision VMS Gateway features the following capabilities. The VMS GW facilitates:

- Importing a list of cameras from the video management software; the BT dashboard displays these devices for selection.
- Obtaining camera names from the VMS, enabling integration engineers and security personnel to identify particular devices in the third-party video management software.
- Receiving video from selected cameras, enabling facial analysis by BT.
    - Live video: interpreting real-time video received by BT from cameras deployed in live surveillance environments;
    - Forensics: analyzing pre-recorded video transferred offline from the VMS to AnyVision BT, based on a specified camera and date-time range.
- Sending events to the VMS. For instance, facial alarms and alert messages triggered by identification of POI in a live video stream, or in playback of offline video.

2.2. Components

The key components operating in the VMS Gateway environment are the following:

- AnyVision Better Tomorrow, running on Ubuntu version 18.04 (BT version 1.20 or later);
- VMS Gateway, running on Windows 10 Professional and Enterprise editions (English only);
- Milestone XProtect, video management software.

2.3. Architecture

Figure 1 below depicts AnyVision VMS Gateway's architecture, and the exchange of data between the system's components.

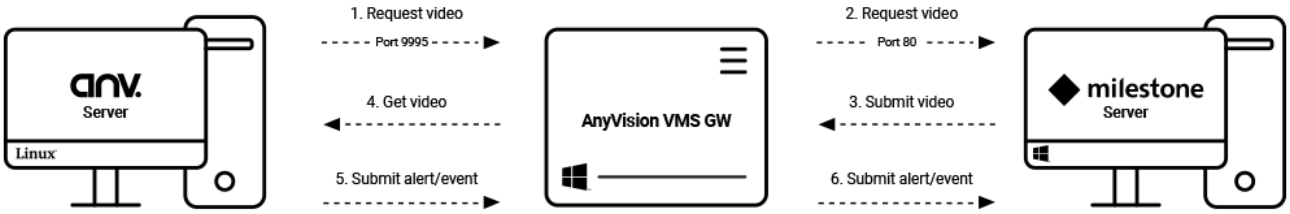

FIGURE 1. ANYVISION VMS GATEWAY. SYSTEM ARCHITECTURE

The following describes the process flow depicted above. Numbers relate to the steps indicated in the flow.

1. AnyVision BT Server contacts, via port 9995 and AnyVision API, AnyVision VMS Gateway, with a request for video (live or forensic).
2. AnyVision VMS Gateway, via port 80 and 3rd party API, passes that request along to Milestone XProtect.
3. Milestone XProtect, through the inverse pathway, returns the video to the AnyVision VMS Gateway.
4. The AnyVision VMS Gateway passes that video to AnyVision BT for analysis.

5. When a face is detected (recognized or unknown), AnyVision BT declares an event and informs the AnyVision VMS Gateway. The information contained in this event is based on data received from cameras and 3rd party security management software.
6. The AnyVision VMS Gateway passes POI alert information to Milestone XProtect.

The VMS Gateway is a service provided by AnyVision. Ordinarily, VMS Gateway runs on the VMS computer. However, occasionally, a third-party might choose to deploy the VMS Gateway on a separate, dedicated machine.

2.4. System Requirements

Table 3, below, covers prerequisites, software, applications, and configuration that must be in place for AnyVision VMS Gateway to install, launch, and function together with Milestone XProtect. These include the following component categories:

- AnyVision BT
- Client hardware and infrastructure
- Client software and VMS

Before getting started with the VMS integration, be sure these requirements, as well as the proper versions, are in place.

TABLE 3. SYSTEM REQUIREMENTS

Category	Component/ Prerequisite	Versions	Remarks
AnyVision	Microsoft Visual C++ installation	2010 Redistribution Package (x86)	▪ Essential for installation of the VMS GW service! ▪ The GW can be installed on the VMS computer, or on a dedicated machine. ▪ The installation pack is available by Internet download.
	BT Dashboard	1.20+	Access available via AnyVision Support.
	Milestone VMS GW installation file: VMSGateway.Setup	Milestone 1.8.0	Access available via AnyVision Support.
	Ubuntu	18.02	

Category	Component/ Prerequisite	Versions	Remarks
Client Hardware and Infrastructure	Cameras	Various, depending on manufacturer.	▪ All cameras deployed in the system must connect directly to the VMS, not from behind a VPN or via an alternative means of connection. ▪ All cameras in the VMS environment must have an identical username and password.
Client Software and VMS	VMS	2019 R3	▪ The correct OS and client SDK versions are essential for installing, configuring, and operating Milestone XProtect software in a VMS GW environment. ▪ RTSP is obtained by the SDK. ▪ Make certain that proper versions are installed. ▪ Other versions might not work for Milestone VMS!
	Milestone license	Contact software vendor	
	ONVIF Bridges	2019	
	Windows	Win10 OS PRO, English only	

3. VMS Integration

3.1. Process Flow

What follows in Figure 2, below, illustrates at an abstract level the activities a security integration engineer performs when setting up AnyVision's VMS Gateway environment. The different colors indicate the particular components—or combination of components—involved in each step of the process.

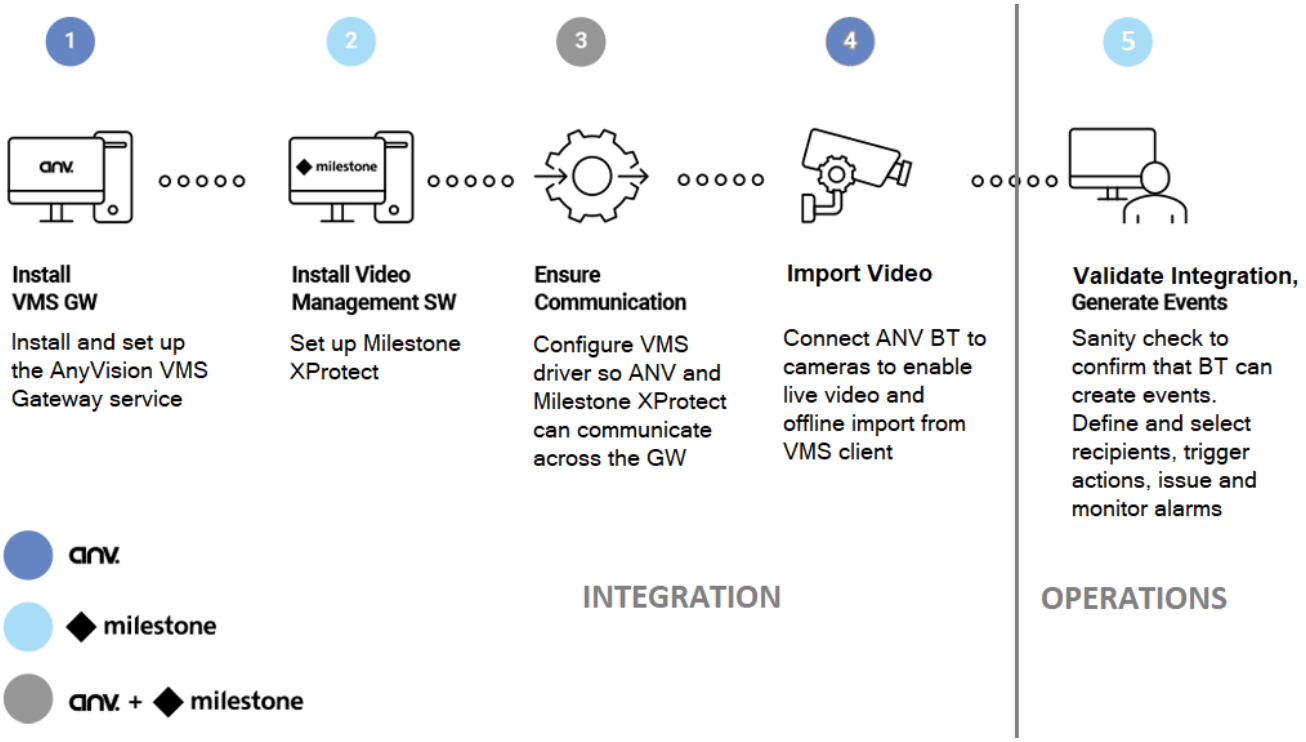

FIGURE 2. PROCESS FLOW

For instructions on installing and configuring the end-to-end VMS and validating the integration, read the following sections.

- Installing the Gateway (see section 3.2.1);
- Installing security and video software (see section 3.2.2);
- Adding cameras and connecting to live video (see section 3.3.1);
- Transferring offline video for forensic analysis (see section 3.3.2);
- Validating integration and monitoring system activity (see section 3.4).

3.2. Gateway and Management Setup

Setting up the VMS Gateway and security management software takes place on the VMS computer. This involves the following activities:

- Installing the VMS Gateway (see section 3.2.1);
- Installing security management software (see section 3.2.2).

3.2.1. Installing the VMS Gateway

This sub-section explains how to install and set up the AnyVision VMS Gateway Service. Note that this procedure will also install Mongo DB on your system.

Note: The VMS Gateway can be installed on the same computer as the VMS security client software, or on a separate machine. The procedure detailed below covers both scenarios.

To install the gateway service:

1. Obtain access to the AnyVision VMS Gateway installation file by contacting your AnyVision Support representative. Request the executable (EXE) file.
2. Run the file **VMSGateway.Setup.exe**.

   This step requires Administrator permissions.

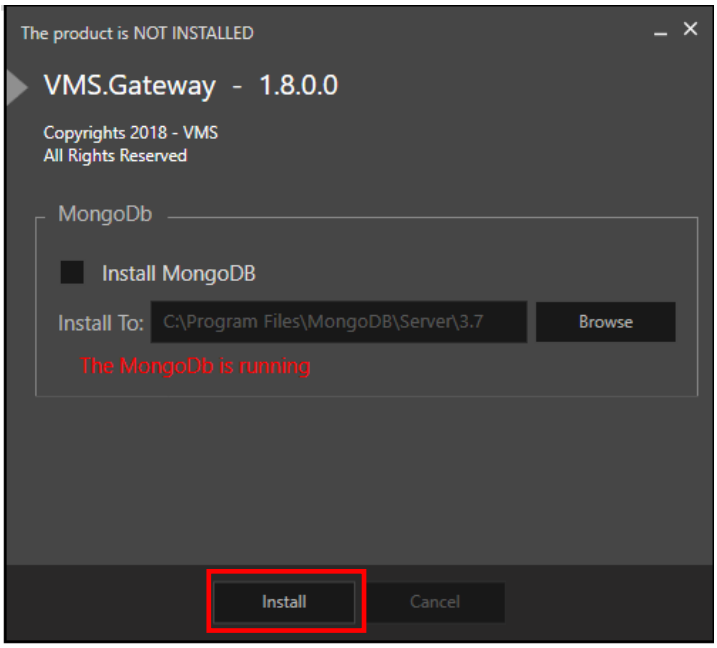

FIGURE 3. VMS GATEWAY. INSTALLATION SCREEN

The VMS Gateway installation opening screen is displayed.

Note: If MongoDB is already installed on the VMS Gateway computer, then remove selection from the MongoDB checkbox.

3. Click **Install**.

4. Once installation has completed successfully, in Windows, open Services. Access this facility by clicking the Windows button, scrolling down the Start menu, and selecting **Windows Administrative Tools > Services**.

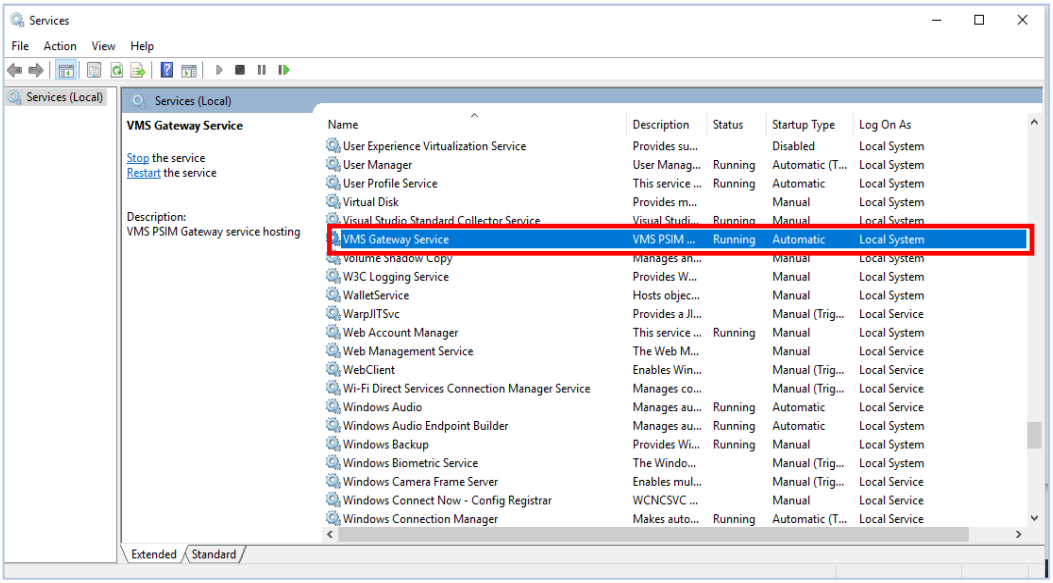

FIGURE 4. WINDOWS SERVICES. VMS GATEWAY (WITH STATUS AS RUNNING)

Note: The above step requires administrator permissions. To gain access, right-click on VMS Gateway; in the popup menu, choose **Run as Administrator**.

5. Check whether a VMS Gateway service is running. If the service is not running, then start it by right-clicking, and in the popup menu, choosing **Start**.

6. Check to see whether MongoDB service is running. Perform this step by running the following URL in your browser: **127.0.0.1:27017**.

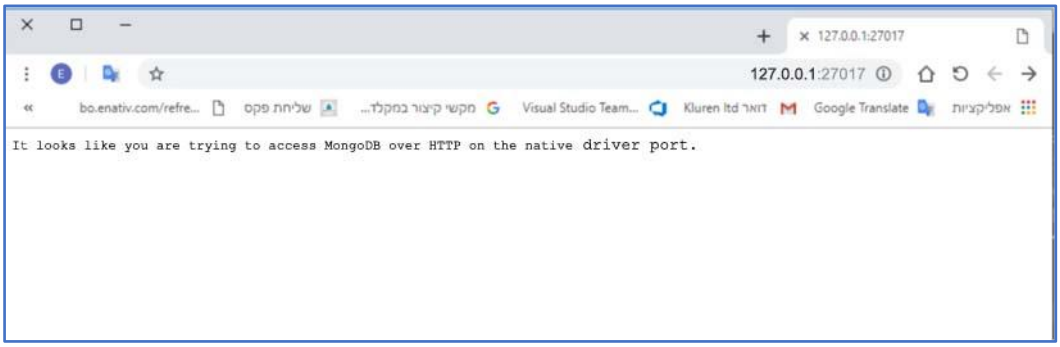

FIGURE 5. MONGODB CONFIRMATION

7. Confirm that the following expression is displayed in the browser:

   "**It looks like you are trying to access MongoDB over HTTP on the native driver port**."

8. Verify that the firewall is inbound, and that Outbound Rules for **port 9995** is open.

   Note: The method for performing this test differs between devices.

3.2.2. Installing Video Management Software

This sub-section explains how to install and set up Milestone XProtect video management software, and how to ensure it integrates with AnyVision BT. This involves:

- Adding video cameras (see section 3.2.2.1);
- Creating an ONVIF Bridge User (see section 3.2.2.2).

3.2.2.1. Adding Video Cameras

This sub-section explains how, in the Milestone XProtect Management client, to add video cameras.

To add video cameras:

1. In the Milestone XProtect Management client, open the recording server contextual menu.
2. Right click on your recording server and select **Add Hardware**.

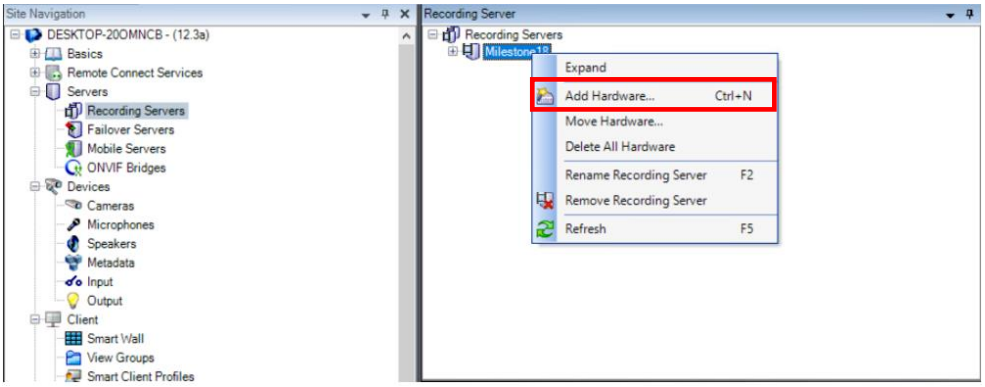

FIGURE 6. CONTEXTUAL MENU. ADD HARDWARE

3. For each camera you wish to add, fill out the relevant information in the appropriate fields in the Properties pane.

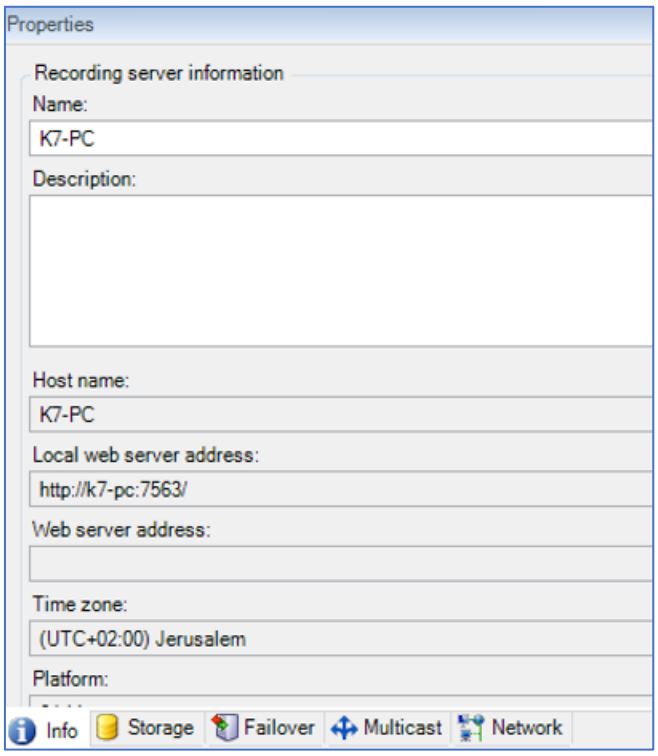

FIGURE 7. MANAGEMENT CLIENT. PROPERTIES

Once you have added the cameras, the next stage is to create an ONVIF Bridge user.

3.2.2.2. Creating an ONVIF Bridge User

Setting up ONVIF Bridges is part of installing Milestone XProtect.

To install and set up Milestone XProtect:

1. Run the installation program for ONVIF BRIDGES.

   Note: The installation process differs among various devices.

2. In the **Management Client** application, create a new **ONVIF Bridges** user.

a. In the **Site Navigation** pane, select **ONVIF Bridges**.

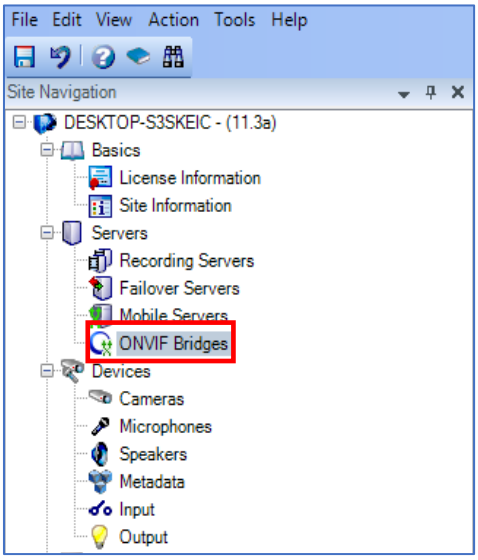

FIGURE 8. VMS GATEWAY CONFIGURATION. SITE NAVIGATION

b. In the **ONVIF Bridge Information** pane, fill in the following user information; then, click **Add User**.

- Username = User name of the VMS;
- Password = Password of the VMS.

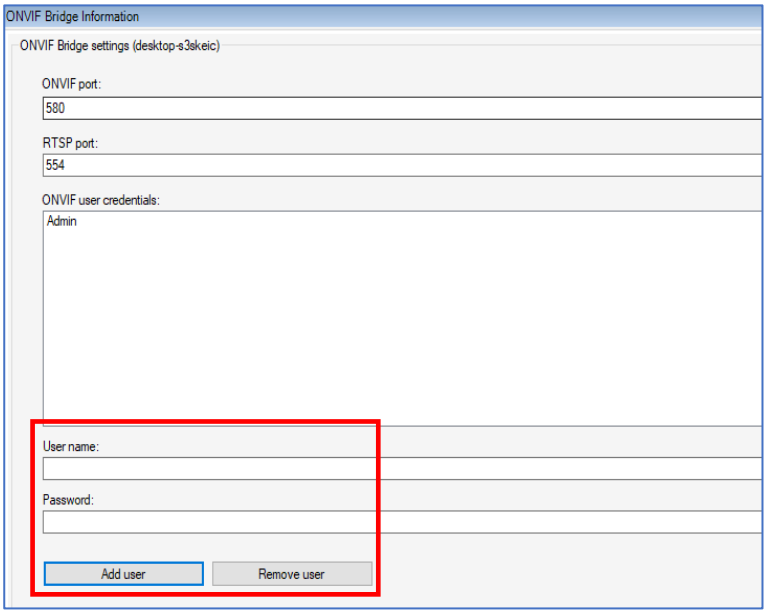

FIGURE 9. VMS GATEWAY CONFIGURATION. ONVIF BRIDGES

Note: The user must have administrator privileges. If you wish to modify the above values, be sure to do so in the VMS Gateway configuration file.

Once the ONVIF Bridge and user information are in place, you can begin importing video for analytics.

3.2.3. Configuring the VMS Driver

This segment of the Gateway configuration involves editing the VMS driver's configuration file.

Note: The VMS application must be installed on the same computer on which the VMS Gateway Service is running.

To configure the VMS driver:

1. If you are running VMS Gateway version 1.8.0 or above, go to the **C:\Program Files (x86)\VMS\VMS.Gateway\Plugins** directory and open the **VMS.Driver.Milestone.dll.config** file.

   If you are running a VMS Gateway version lower than 1.8.0, go to the **C:\Program Files (x86)\VMS\VMS.Gateway\Plugins\Milestone** directory and open the **VMS.Driver.Milestone.dll.config** file.

2. Define the following parameters, as follows:

   a) **Username** = take the value for this credential from the VMS.

   b) **Password** = take the value for this credential from the VMS.

   c) **IP Address** = the network location of the computer on which the VMS is running.

   d) **Port** = the port on which the VMS is running.

   e) **Username ONVIF** = The username defined in section 3.2.2.2.

   f) **Password ONVIF** = The password defined in section 3.2.2.2

   g) **Trigger Alarm with Event** = if you wish to attach an alarm when sending an event, set to **True**; otherwise, set to **False.**

   h) **Show Instruction** = if you wish to display the instruction of an alarm, set to **True**; otherwise, set to **False.**

   i) **ONVIF Port** = obtain the port of the ONVIF bridge from the XProtect Management Client application.

   j) **ONVIF FTP Address** = ONVIF bridge's IP address.

   k) **Analytics Event Name** = name of the analytics event set in management client application.

Assuming all the above steps in this section have been performed successfully, the Milestone XProtect client will display all the cameras tracked by AnyVision BT.

Once the VMS driver is configured, continue to the next sub-section to configure the Milestone Analytics Event.

3.2.4. Configuring the Analytics Event

With the security management software now installed and VMS driver configured, you are now ready to go ahead and configure the Milestone Analytics Event.

To configure the Analytics Event:

1. In Milestone XProtect, Open the Management client.
2. In the Navigation pane, open **Rules and Events** and select **Analytics Events**.
3. Under the **Analytics Event** list, create a new event.

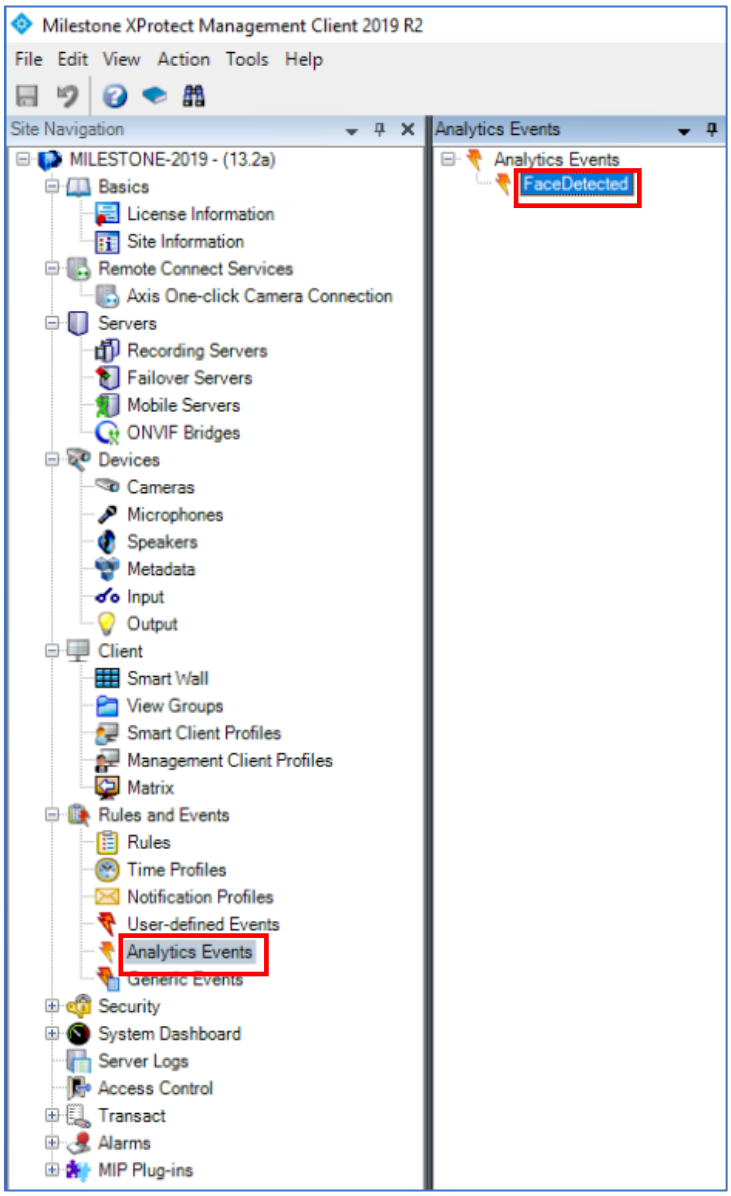

FIGURE 10. MILESTONE MANAGEMENT CLIENT. ANALYTICS EVENT

4. Copy the event name, exactly as it appears in the Management UI, to the **AnalyticsEventName** property in the VMS.Driver.Milestone.dll configuration file.

3.3. Importing Video for Analytics

There are two key aspects to communication between AnyVision BT and the VMS client:

- Connecting to live video (see section 3.3.1);
- Transferring offline video from the VMS to AnyVision BT (see section 3.3.2).

For both the live and offline scenarios, you acquire video in AnyVision BT via the settings window.

3.3.1. Connecting to Live Video

The procedure below explains how to configure AnyVision BT settings and select cameras for live video import.

To select cameras for live video import:

1. In AnyVision BT, click the **Configuration** ( ) icon to open the **Settings** window.

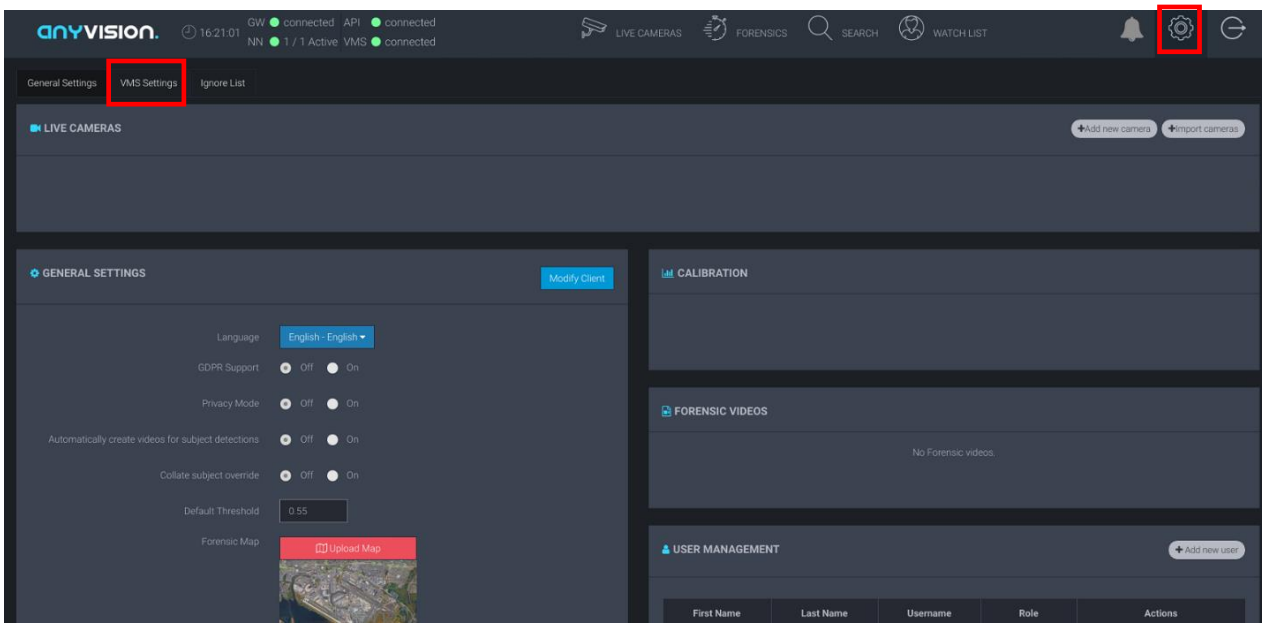

FIGURE 11. ANYVISION CONFIGURATION. SETTINGS

2. Toward the top of the screen, click the **VMS Setting tab**.

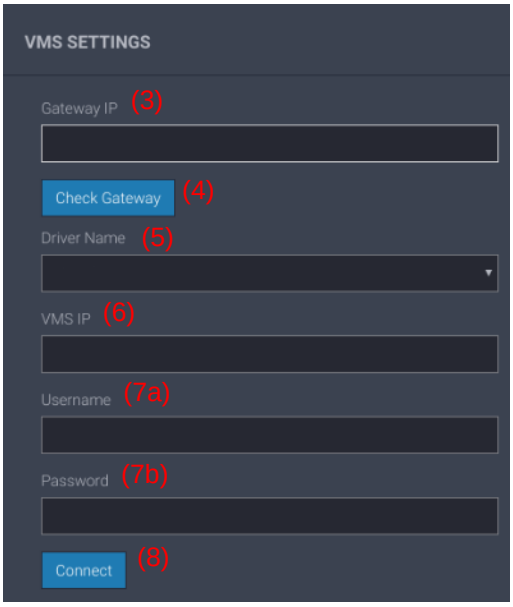

FIGURE 12. ANYVISION. VMS SETTINGS

The Gateway IP is an internal interface that communicates with the SDKs of third-party VMSes.

3. In the **Gateway IP** field, enter the IP address of the VMS Gateway. This field is essential for enabling a 3rd-party VMS to communicate with the VMS Gateway.
4. Click **Check Gateway** to ensure connectivity.

   If the VMS provider, in this case, Milestone, appears among the options in the Driver Name menu, a working connection is in place.
5. In **Driver Name**, open the menu and select the name of the driver to which you would like to connect. In this case, choose **Milestone**.
6. In **VMS IP**, specify the IP address of the VMS Gateway.
7. In the remaining fields, enter the VMS' **Username** and **Password**.
8. To connect with the VMS using the values you specified, click **Connect**.

   A list of cameras associated with the selected VMS is displayed.

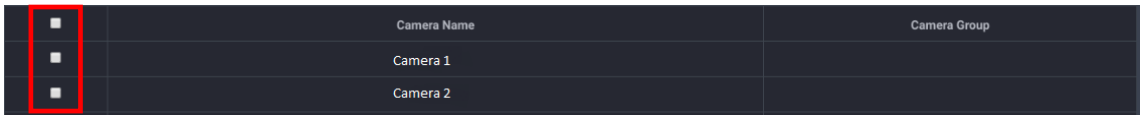

FIGURE 13. SELECT CAMERA NAMES

9. For each camera you wish to add to your system, select the corresponding checkbox and click **Import Cameras**.

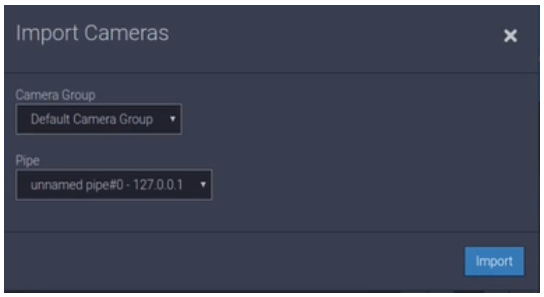

FIGURE 14. IMPORT CAMERAS

10. Select the **Camera Group** and **Pipe**.

    Note: Camera groups are defined in BT, where unique settings are assigned to parameters, per group.

11. In the **Import Cameras** dialog, click **Import**.

    For the cameras belonging to a camera group, parameters are set in VMS. Once you import a camera group, those parameters are transferred to BT, where they will be available for selection.

    BT generates new cameras with the relevant parameters of those cameras imported from the VMS. These parameters include camera name, RTSP URL, username and password. The remaining parameters use default parameters.

    You edit the parameters of new cameras in General Settings.

12. Toward the top of the AnyVision Settings screen, click the **General Settings** tab.

13. Review the settings of the recently added cameras by selecting a camera group and clicking its corresponding **Edit** button.

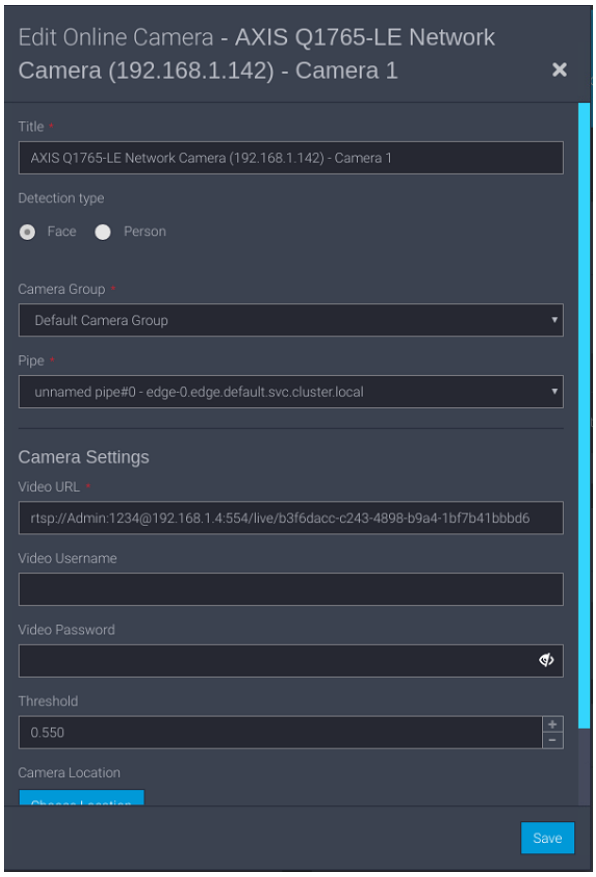

FIGURE 15. EDIT A CAMERA GROUP

Your system is now ready to detect faces and, when appropriate, generate alarms to notify security monitors regarding persons of interest!

3.3.2. Importing Forensic Video

Through the Milestone UI and AnyVision BT dashboard, you can request video residing in the VMS for analysis and interpretation. Through the import of offline video from the VMS, AnyVision BT can perform forensic investigation functions on the captured video.

To transfer offline video:

1. In the client UI, go to the playback view, select a camera, and pick a starting point in the video timeline.
2. Begin playing the video.
3. In AnyVision BT, click **FORENSICS**.

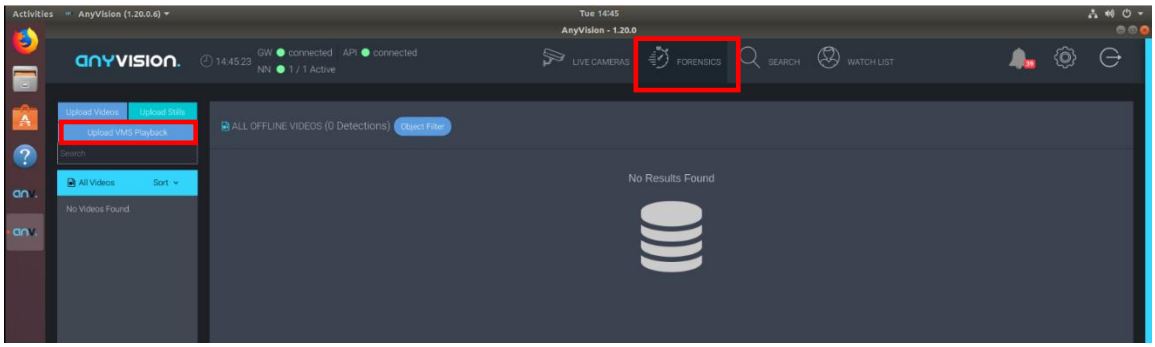

FIGURE 16. ANYVISION UI. FORENSICS VIEW

4. In the left-side navigation pane, click **Upload VMS Playback**.

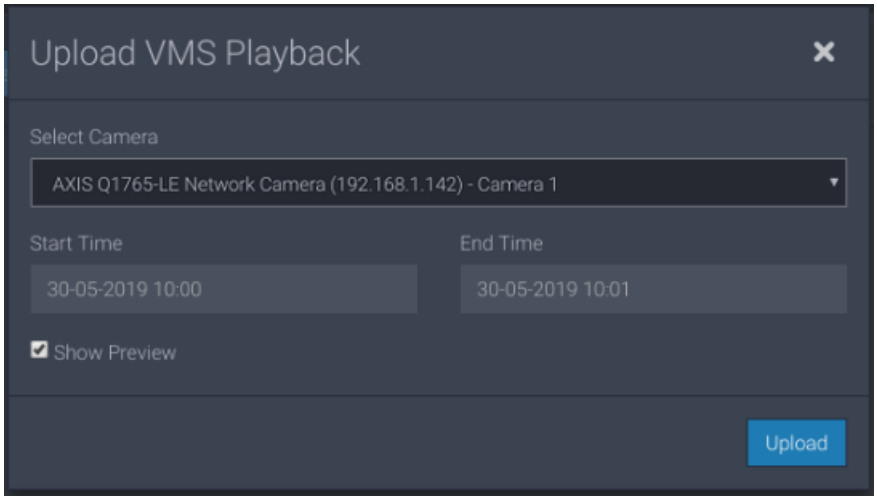

FIGURE 17. ANYVISION UI. UPLOAD VMS PLAYBACK

5. Open the **Select Camera** menu and choose a video camera.
6. Click on the **Start Time** field; from the calendar, select a starting date, and then, from the list of available times, click your start time selection.
7. From the **End Time** field, do the same as described in step #6 for your ending date and time.
8. Click **Upload**.

   The selected segment uploads to AnyVision BT, which inspects the imported video. BT scans for faces and generates alerts, which it submits to the client VMS.

   A preview window is displayed.

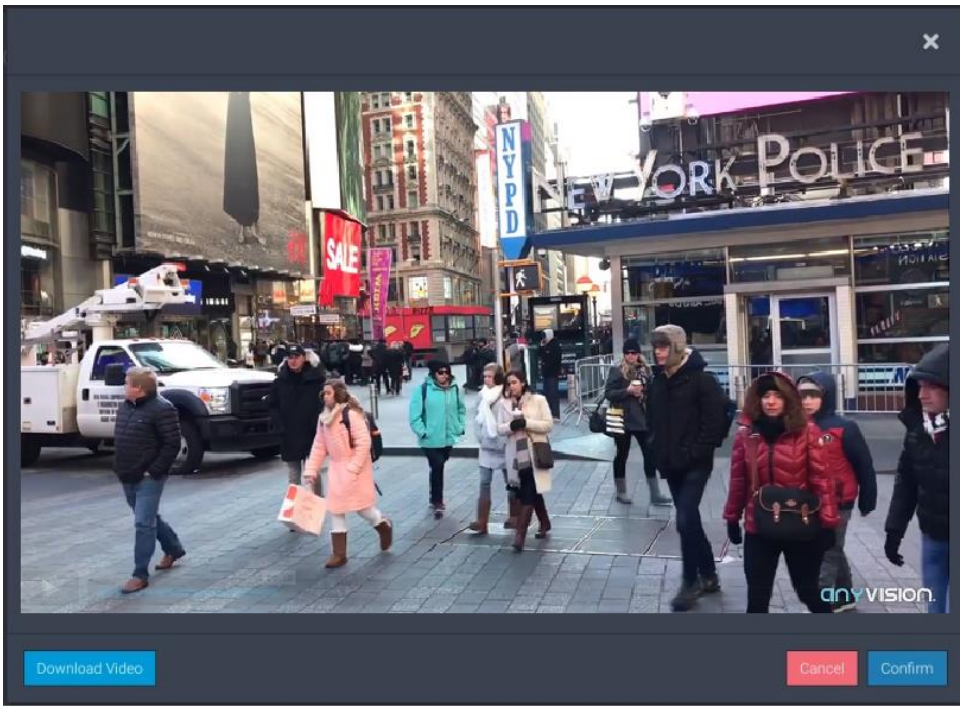

FIGURE 18. ANYVISION UI. PLAY UPLOADED VIDEO

9. To save the selected video segment to AnyVision BT, click **Confirm**.

   Alternatively, to remove the video segment, click **Cancel**.

10. If you wish to save the video segment to the computer's desktop, click **Download Video**.

Your system is now ready to perform forensic analysis of recorded video! Continue to section 3.4 to generate alarms.

3.4. Managing Alarms

This section explains how to validate integration by sanity checking that the three components—BT, VMS GW, and VMS client—are installed, properly configured, and connecting to video. This validation step is performed by setting up alarms and issuing alarms using the VMS client.

The following topics are covered:

- Confirming BT Communication with VMS (see section 3.4.1);
- Monitoring System Activity (see section 3.4.2).

3.4.1. Confirming BT Communication with VMS

Once you have verified that BT can import live stream and forensic video from VMS, you can confirm that BT is issuing to VMS AI regarding facial identification.

When VMS receives intelligence from BT with regard to identified faces (recognized and unknown), BT could prompt an event. That BT event appears, in the VMS UI, as an alarm or event in the VMS UI.

This sub-section describes how to confirm that BT is communicating with VMS and providing actionable information in the manner of AI-prompted events.

To confirm BT-VMS communication:

1. In AnyVision BT, open the **Live Cameras** view.

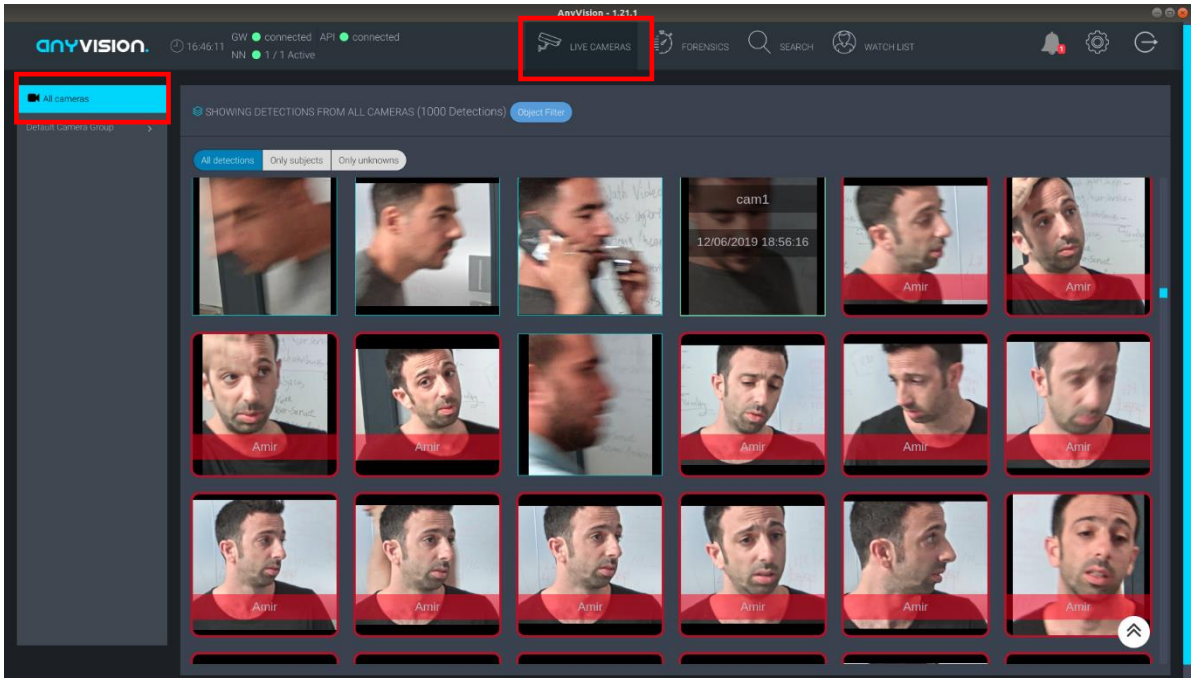

FIGURE 19. ANYVISION BT. LIVE CAMERAS VIEW

2. In the navigation pane, select **All Cameras**.

   Alternatively, select a Camera Group, or in the main window, use the Object Filter and buttons to limit the display of facial detection to a subset of cameras.

   When BT detects a face, it issues an event to the VMS containing a description of the POI. An event contains the following fields:

   - Name
   - Class
   - Type
   - Suspect ID
   - Suspect Group ID
   - Message
   - Time

3. Open the **Smart Client** application.
4. Click on the **Alarm Manager** tab.
5. Point your mouse to the bottom of the window and click; then choose **Setup**.
6. Choose **Alarm** or **Event**.

The Milestone XProtect UI displays an image similar to the following:

- For an event:

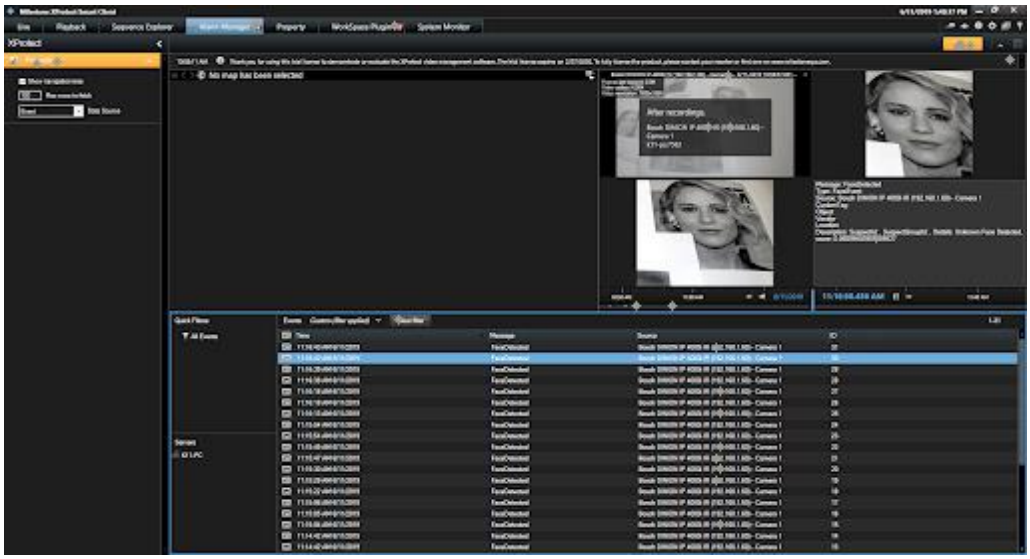

FIGURE 20. MILESTONE EVENT SCREEN

- For an alarm:

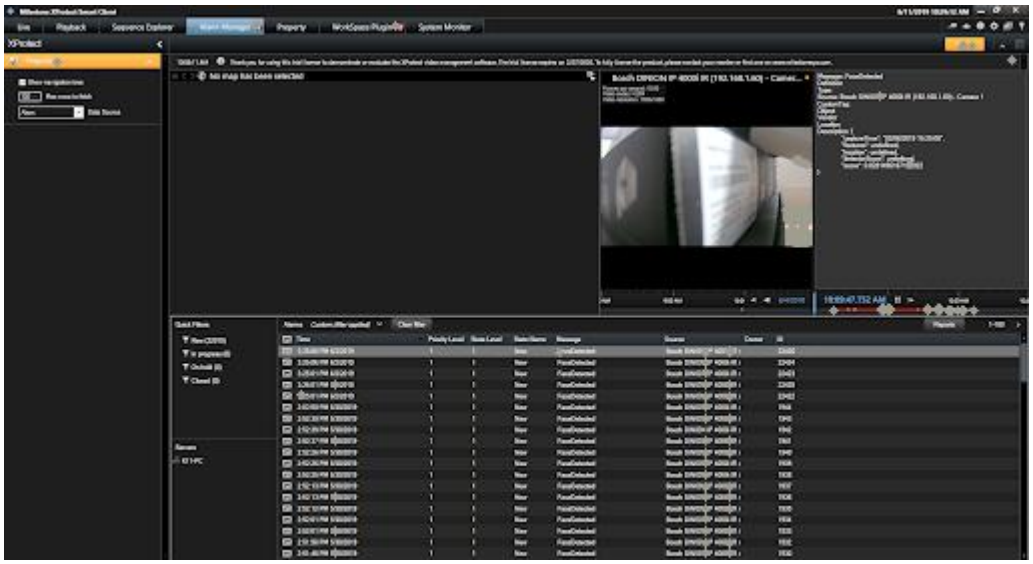

FIGURE 21. MILESTONE ALARM SCREEN

Now that you have confirmed BT is issuing AI-prompted events to the VMS, you can go ahead and manage those events and alarms using the VMS UI.

Refer to Milestone documentation for instructions on monitoring live system activity, managing alarms, and playing back incidents.

3.4.2. Monitoring System Activity

Once the VMS and Gateway configurations are in place, communication confirmed, you can begin monitoring system activity.

To monitor system activity:

In Milestone XProtect, select the Live panel and verify display of a live image.

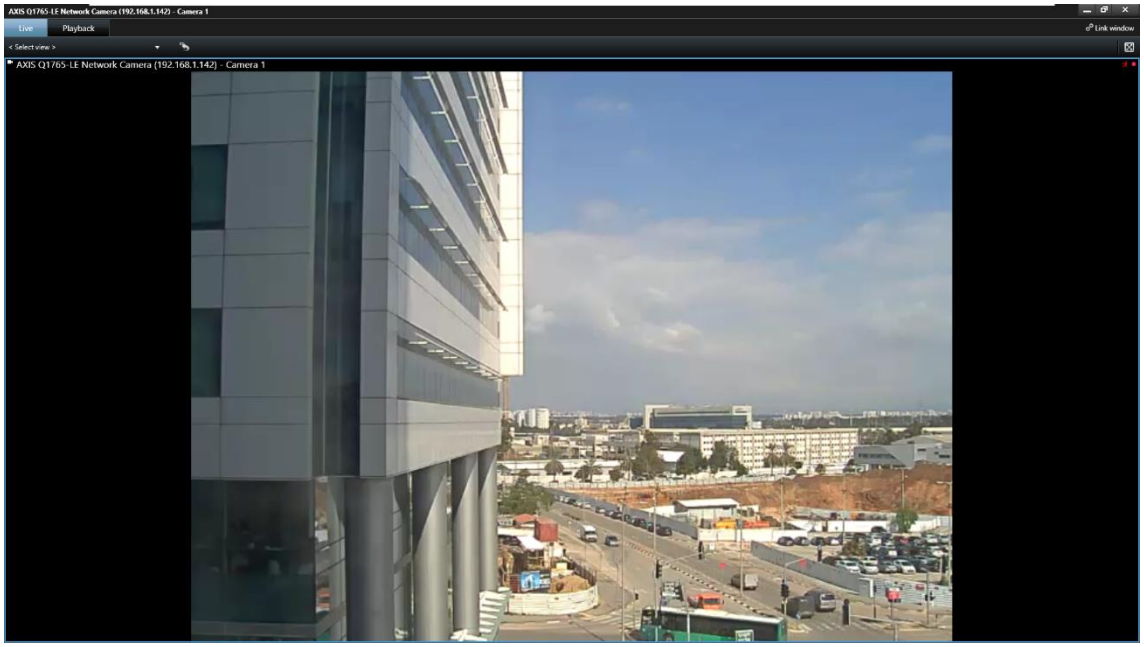

FIGURE 22. MILESTONE XPROTECT. LIVE PANEL

Refer to Milestone documentation for instructions on monitoring live system activity, managing alarms, and playing back incidents.

Index