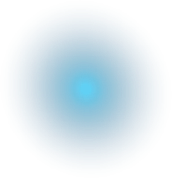
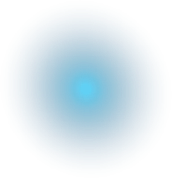
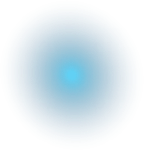
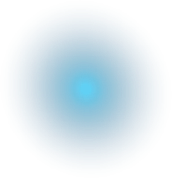
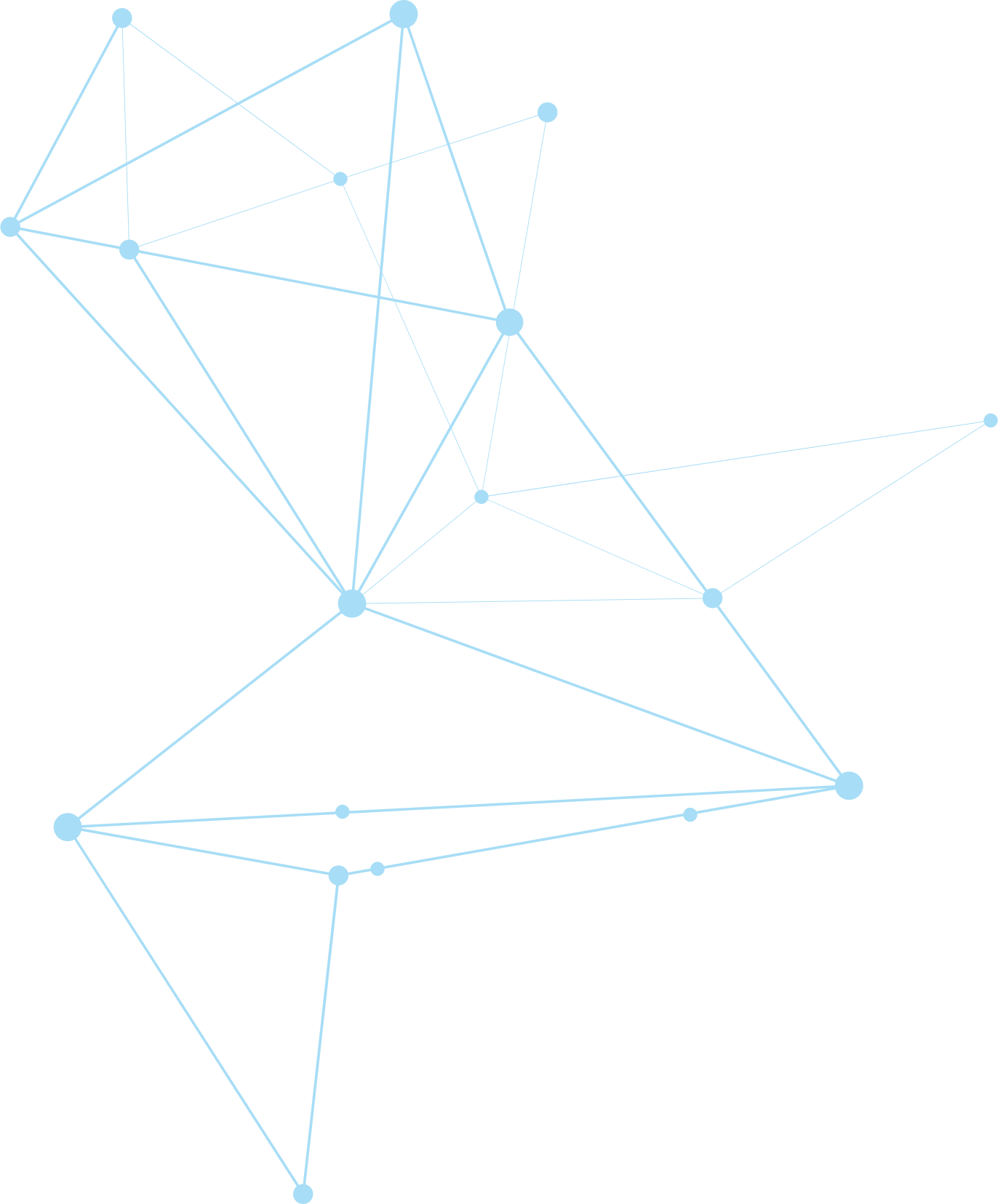
****

VMS

Gateway



Integration Guide for Milestone

Video Management System

Version 1.06 May 29, 2019

Table of Contents

This Guide

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

[1. Milestone VMS—AnyVision: Integration Overview 5](#_Toc10041574)

[1.1. About this Integration Guide 5](#_Toc10041575)

[1.2. Purpose and Scope 6](#_Toc10041576)

[1.3. Concepts, Terms, and Abbreviations 6](#_Toc10041577)

[2. About the VMS Gateway 8](#_Toc10041578)

[2.1. Capabilities 8](#_Toc10041580)

[2.2. Components 9](#_Toc10041581)

[2.3. Architecture 9](#_Toc10041582)

[2.4. System Requirements 10](#_Toc10041583)

[3. VMS Integration 12](#_Toc10041584)

[3.1. Process Flow 12](#_Toc10041589)

[3.2. Gateway and Management Setup 13](#_Toc10041590)

[3.2.1. Installing the VMS Gateway 13](#_Toc10041591)

[3.2.2. Installing Security Management Software 15](#_Toc10041592)

[3.2.3. Configuring the VMS Driver 23](#_Toc10041593)

[3.3. Connect Cameras: Server Configuration 24](#_Toc10041594)

[3.3.1. Defining Server Settings and Selecting Cameras 24](#_Toc10041595)

[3.3.2. Defining General Settings 26](#_Toc10041596)

[3.4. Define MIPs, Verify Image Display 28](#_Toc10041597)

[3.4.1. Troubleshooting MIP Drivers 28](#_Toc10041598)

[3.4.2. Managing Alarms 30](#_Toc10041599)

[Index 31](#_Toc10041600)

List of Tables

Table 1. Section Summary 6

Table 2. Concepts, Terms, and Abbreviations 6

Table 3. System Requirements 10

List of Figures

Figure 1. AnyVision VMS Gateway. System Architecture 9

Figure 2. Process Flow 12

Figure 3. VMS Gateway. Installation Screen 13

Figure 4. Windows Services. VMS Gateway (with Status as Running) 14

Figure 5. MongoDB Confirmation 14

Figure 6. Contextual Menu. Add Hardware 15

Figure 7. Management Client. Properties 16

Figure 8. VMS Gateway Configuration. Site Navigation 17

Figure 9. VMS Gateway Configuration. ONVIF Bridges 17

Figure 10. Management Client. Recording Servers 18

Figure 11. VMS Gateway Configuration. Adding Hardware 19

Figure 12. Add User. Set Credentials 19

Figure 13. Camera Hardware. Select Device Drivers 20

Figure 14. Hardware Devices. Associate IP Addresses 20

Figure 15. Hardware Devices. Associate Metadata Ports 21

Figure 16. Hardware Devices. Assign Devices to Groups 21

Figure 17. Metadata Definitions 22

Figure 18. Assign Metadata to Cameras 22

Figure 19. “Bounding Box” Providers List 23

Figure 20. AnyVision Configuration. Settings 25

Figure 21. AnyVision. VMS Settings 25

Figure 22. Select Camera Names 26

Figure 23. Import Cameras 26

Figure 24. Create a Camera Group 27

Figure 25. Management Client. Navigation Pane 28

Figure 26. Management Client. Recording Servers 29

Figure 27. Management Client. MIP Driver Menu 29

Figure 28. Milestone XProtect. Live Panel 30

Important Notice

Copyright © 2019 AnyVision. All rights reserved.

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.

# Milestone VMS—AnyVision: Integration Overview

**01**

## About this Integration Guide

This guide describes the steps for integrating the various components making up the VMS environment. 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.

VMS integration ensures that the AnyVision Server, 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 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. |

## Purpose and Scope

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

Table . 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 | 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 database connectivity, and configuring the VMS Gateway |
| **Section ‎3.3,** Connect Cameras: Server Configuration | Describes how to configure AnyVision server, including server’s settings, camera selection, and general settings |
| **Section ‎3.4,** Define MIPs, Verify Image Display | Describes how to troubleshoot MIP drivers and ensure live image display in the third-party video management system |

## 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 Server, VMS Gateway, and third-party video management products.

Table . Concepts, Terms, and Abbreviations

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

# About the VMS Gateway

**02**

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.



## Capabilities

AnyVision VMS Gateway features the following capabilities:

* Imports a list of cameras from the video management software; the BT dashboard displays these devices for selection.
* Obtains camera names from the VMS, enabling integration engineers and security personnel to identify particular devices in the third-party video management software.
* Takes live video from a selected camera, enabling, for example, triggering of video playbacks.
* Sends events and alerts to the VMS, for instance, facial alarms.
* Furthermore, by requesting video start and end times, AnyVision VMS Gateway performs forensic functions by transferring offline video from the VMS to AnyVision servers.

## Components

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

* AnyVision Server, 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.

## Architecture

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

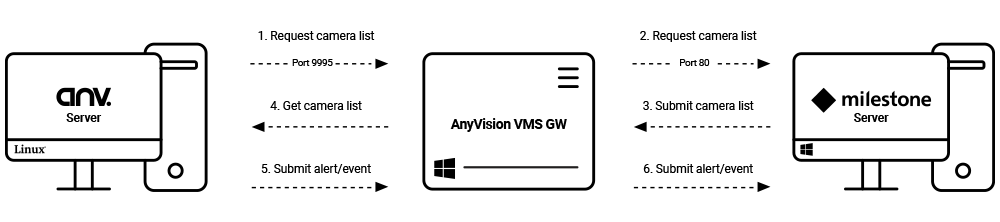


Figure 1. AnyVision VMS Gateway. System Architecture

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

1. AnyVision’s Server contacts, via port 9995 and AnyVision API, AnyVision VMS Gateway, with a request for a list of cameras.
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 camera list to the AnyVision VMS Gateway.
4. The AnyVision VMS Gateway passes that camera list to the AnyVision Server.
5. When an unknown face is detected, the AnyVision Server 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.

Note that the VMS Gateway is a service provided by AnyVision. Ordinarily, VMS Gateway runs on the VMS computer. However, there are situations where a third-party might choose to deploy the VMS Gateway on a separate, dedicated machine.

## 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
* 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 1.7.8+ | Access available via AnyVision Support. |
|  | Ubuntu | 18.02 |  |
| **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 | 2017 R3 | * The correct OS and SDK versions are essential for installing, configuring, and operating Milestone XProtect software in a VMS GW environment. * Make certain that proper versions are installed. * Other versions might not work for Milestone VMS! |
| MIP SDK installation | 2017 |
| Milestone license | Contact software vendor |
| ONVIF Bridges | 2017 |
| Windows | Win10 OS PRO, English only |

# VMS Integration

**03**



## Process Flow

What follows in Figure , below, illustrates at an abstract level the activities a security integration engineer performs when setting up AnyVision’s VMS Gateway environment.

A close up of a logo

Description automatically generated

Figure 2. Process Flow

## Gateway and Management Setup

Setting up the VMS Gateway and security management software entails the following activities:

* Installing the VMS Gateway (see section ‎3.2.1);
* Installing security management software (see section ‎3.2.2);
* Configuring the VMS driver (see section ‎3.2.3).

### Installing the VMS Gateway

This sub-section explains how to install and set up the AnyVision VMS Gateway Service.

**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. To gain access, go to **Services**, right-click on **VMS Gateway**; then, in the popup menu, choose **Administrator**.

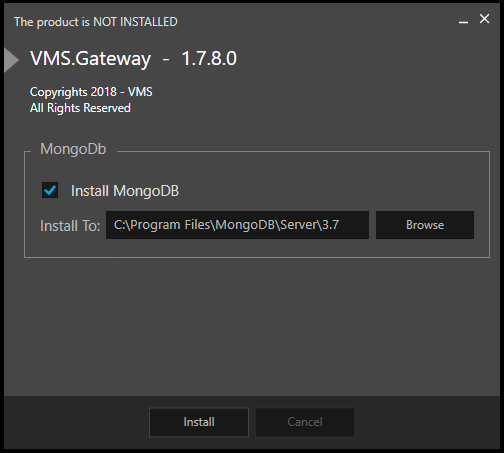


Figure 3. VMS Gateway. Installation Screen

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.

1. Click **Install**.
2. In both of the setup screens that follow, click **Next**.
3. 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**.

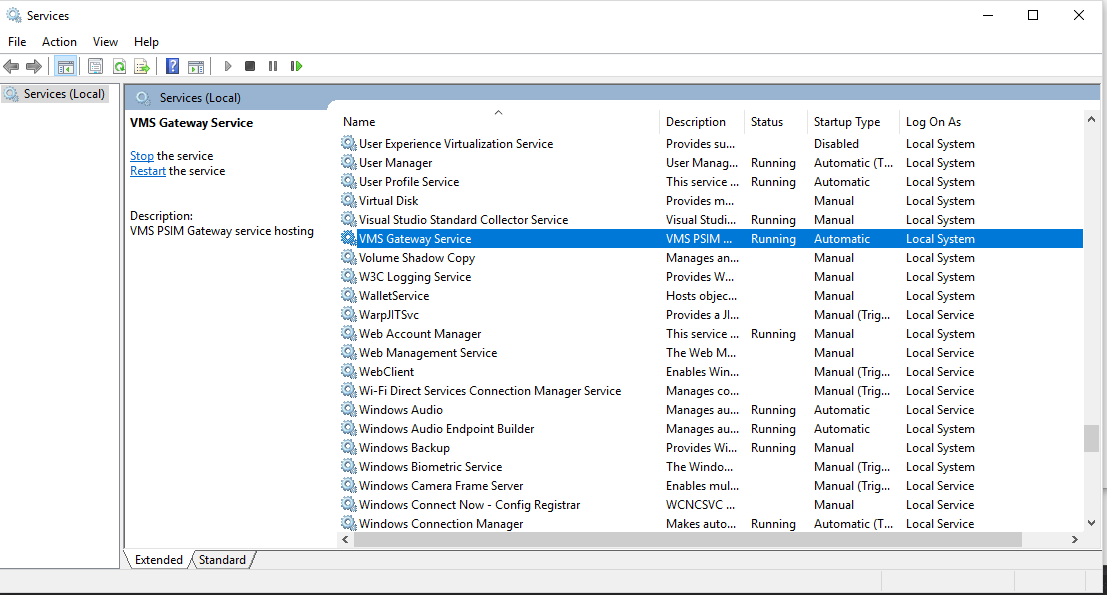


Figure 4. Windows Services. VMS Gateway (with Status as Running)

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

1. 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.
2. Check to see whether MongoDB service is running. Perform this step by running the following URL in your browser: **127.0.0.1:27017**.

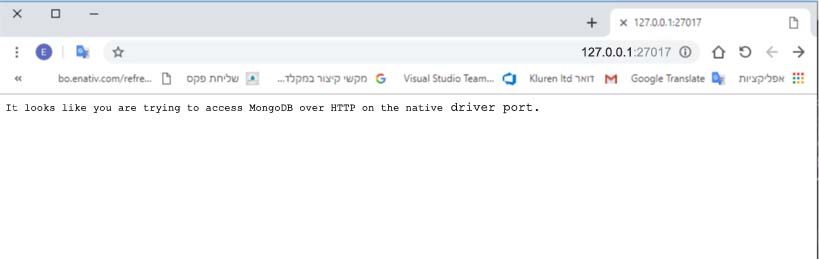


Figure 5. MongoDB Confirmation

1. 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**."
2. 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.

### Installing Security 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:

* Configuring video (see section ‎3.2.2.1);
* Creating an ONVIF Bridge User (see section ‎3.2.2.2);
* Configuring metadata (see section ‎3.2.2.3);
* Assigning metadata ports (see section ‎3.2.2.4).

#### Video Configuration

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

**To add video cameras:**

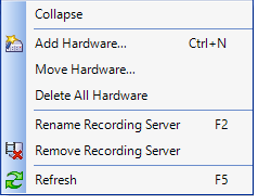
1. In the Milestone XProtect Management client, open the recording server contextual menu.
2. Click **Add Hardware**.   
     
   

Figure 6. Contextual Menu. Add Hardware

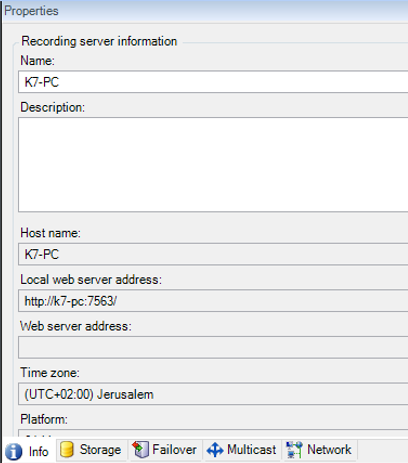
1. For each camera you wish to add, fill out the relevant information in the appropriate fields in the Properties pane.  
     
   

Figure 7. Management Client. Properties

Once you have added the cameras, the next stage is to add metadata sources. This enables detection overlays in surveillance images, and allows receiving events from AnyVision BT.

#### Creating an ONVIF Bridge User

Setting up ONVIF Bridges is part of installing Milestone XProtect.

**To install and set up Milestone XProtect:**

1. Run installations for the following programs:

* MIPSDK;
* ONVIF BRIDGES.

**Note**: The installation process differs among various devices.

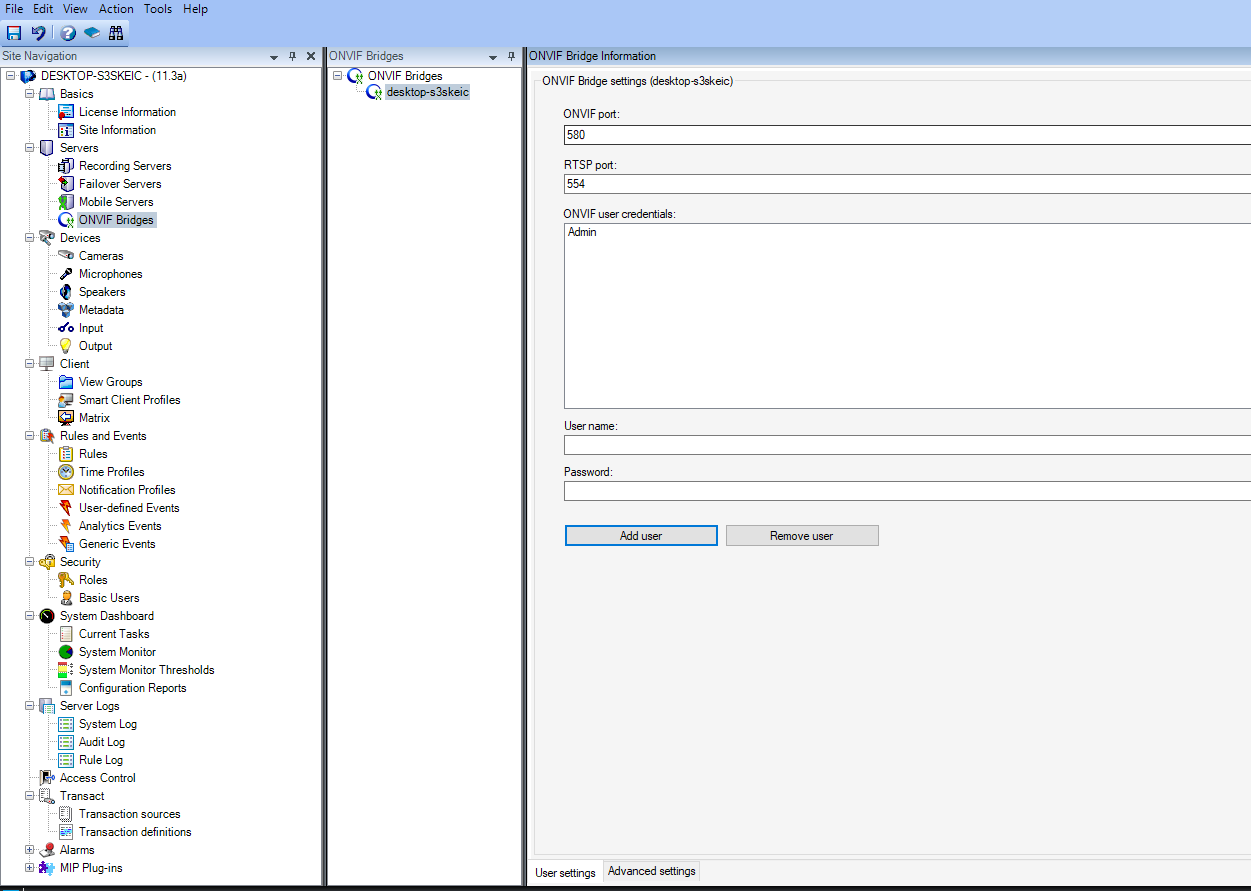
1. In the **Management Client** application, create a new **ONVIF Bridges** user.
   1. In the **Site Navigation** pane, select **ONVIF Bridges**.   
        
      

Figure 8. VMS Gateway Configuration. Site Navigation

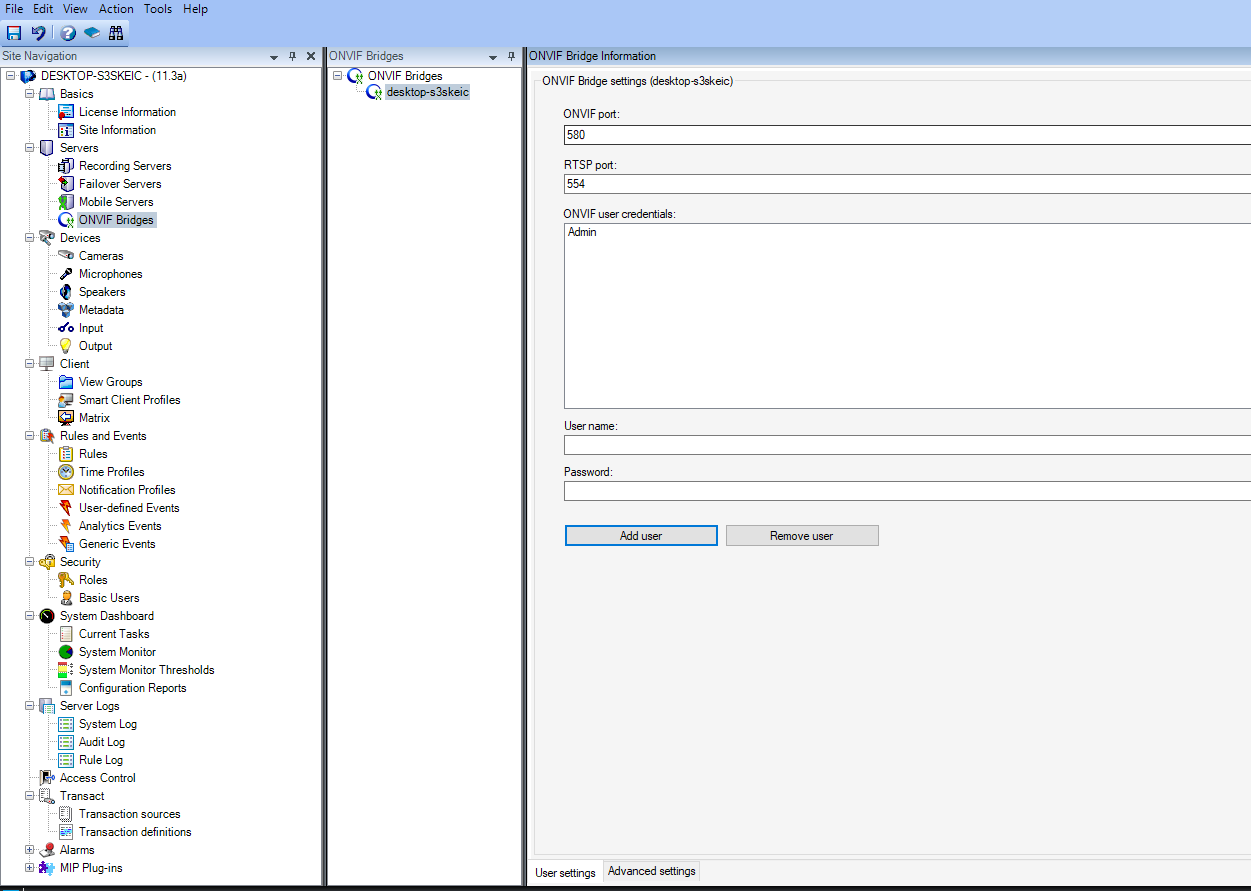
* 1. In the **ONVIF Bridge Information** pane, fill in the following user information; then, click **Add User**.
* Username = **Admin**;
* Password = **1234**.  
  

Figure 9. VMS Gateway Configuration. ONVIF Bridges

**Note**: If you wish to modify the above values, be sure to do so in the VMS Gateway configuration file.

#### Configuring Metadata

For each camera operating in the Milestone XProtect ecosystem, metadata configuration adds and initializes metadata hardware. Before performing this procedure, make sure the AnyVision Gateway hosting service is running.

**Note**: Only after all the cameras have been added can you configure the metadata.

**To configure metadata:**

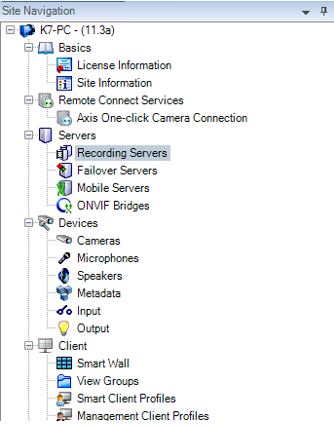
1. Launch the Milestone XProtect Management client.
2. Make sure the AnyVision Gateway hosting service is running.   
     
   

Figure 10. Management Client. Recording Servers

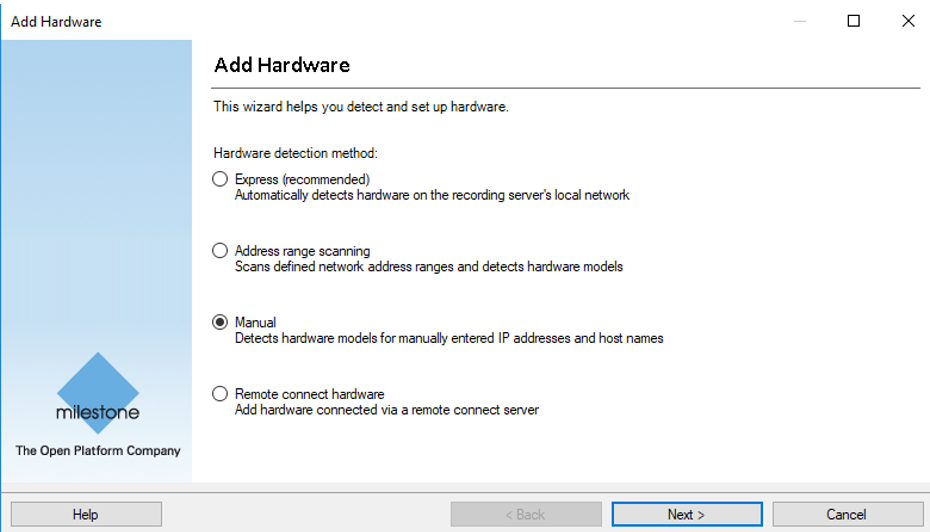
1. In **Site Navigation**, right-click **Recording Servers** and choose **Add Hardware**.   
     
   

Figure 11. VMS Gateway Configuration. Adding Hardware

1. In the Add Hardware wizard, select **Manual**; click **Next**.
2. Add a user with the following credentials (use the MIP password):

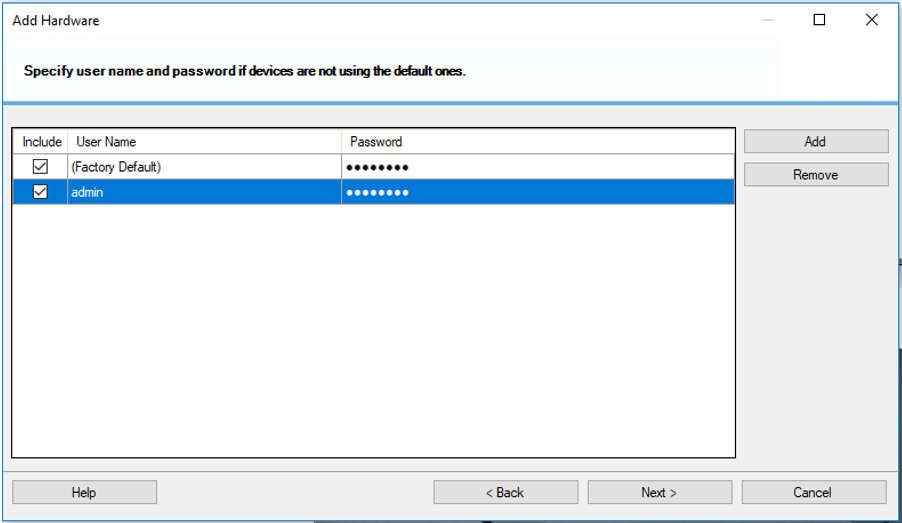
* User = **admin**;
* Password = **1234**.   
  

Figure 12. Add User. Set Credentials

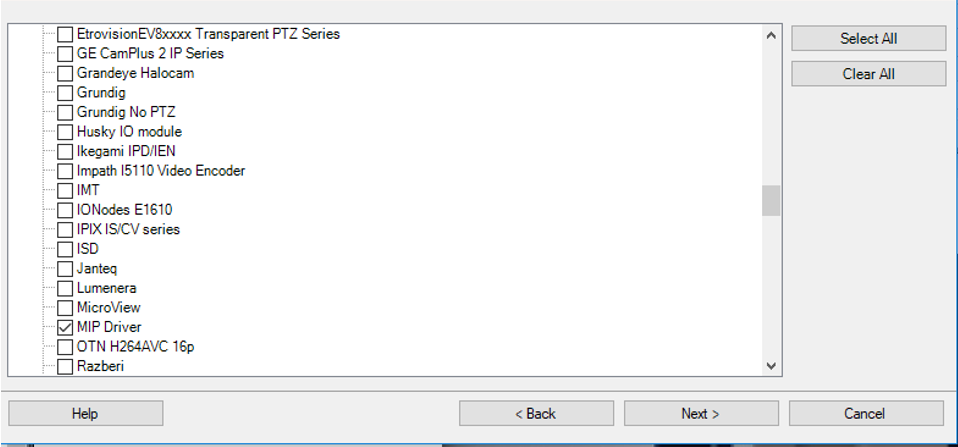
1. Click **Next**.
2. For the various camera hardware devices, select drivers. In the drivers list, select the **MIP Driver** (only).   
     
   

Figure 13. Camera Hardware. Select Device Drivers

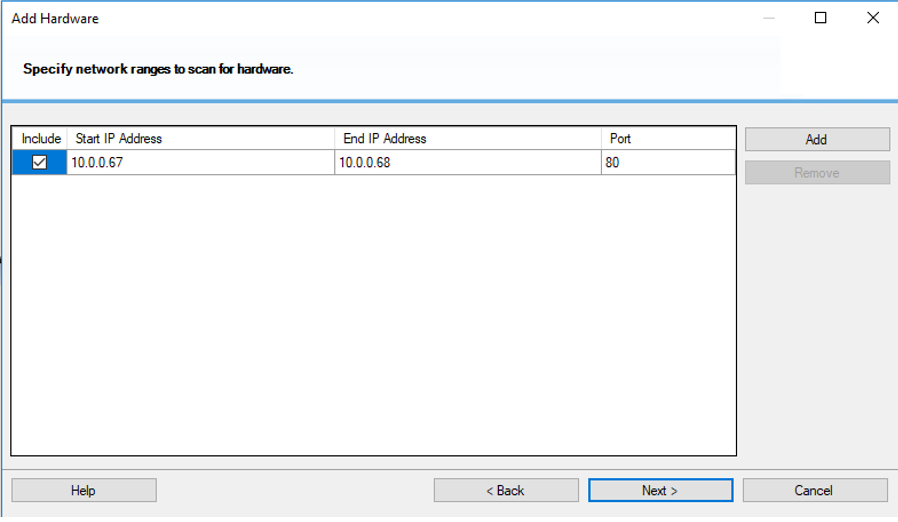
1. Click **Next**.
2. For the various hardware devices, associate the relevant IP address and port **52123**; click **Next**.   
     
   

Figure 14. Hardware Devices. Associate IP Addresses

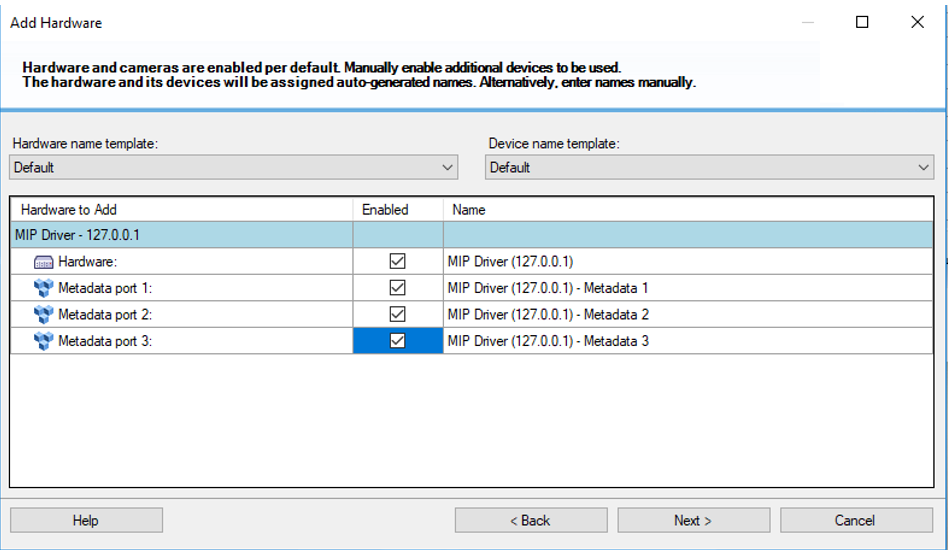
1. Select all relevant metadata ports (one per camera); click **Next**.   
     
   

Figure 15. Hardware Devices. Associate Metadata Ports

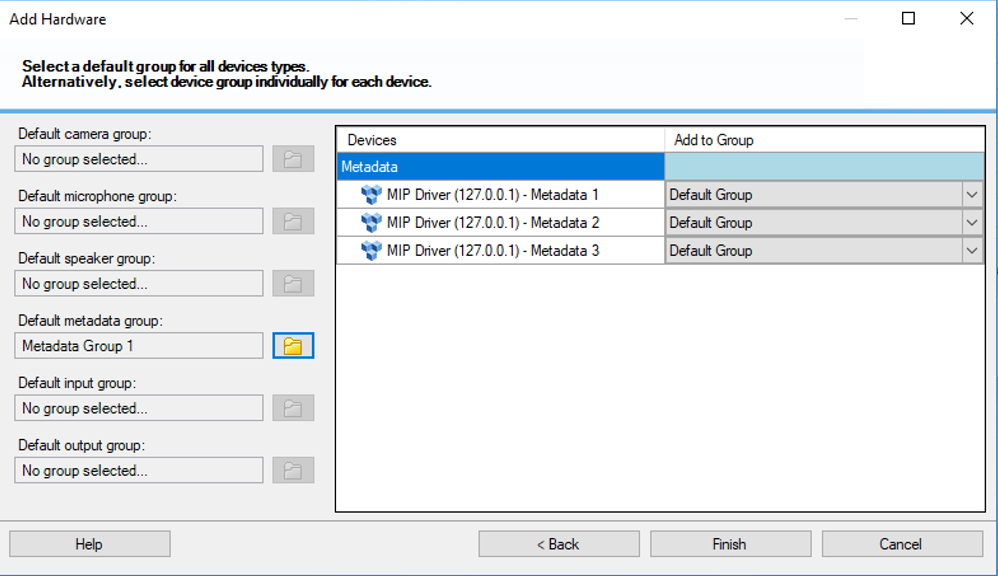
1. Assign the metadata devices to a group; click **Finish**.   
     
   

Figure 16. Hardware Devices. Assign Devices to Groups

When the wizard has completed, you then need to assign a metadata port to a camera, as a one-to-one relationship.

#### Assigning Metadata Ports

Once you have configured the system’s camera metadata, go ahead and assign metadata ports to cameras.

**To configure metadata:**

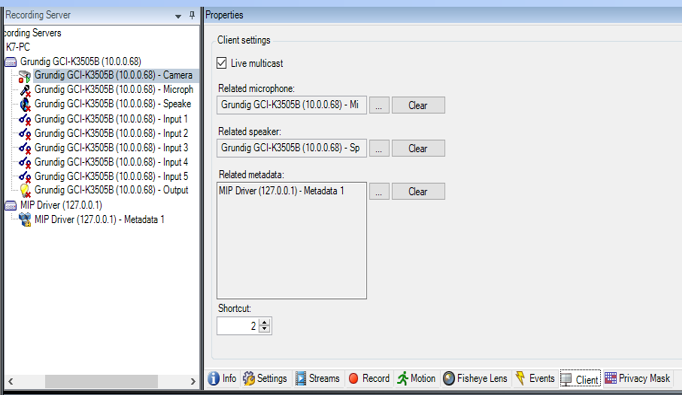
1. Return to Site Navigation and create a new camera group; add to that group the camera(s) you defined above (see section ‎3.2.2.3, above).
2. In **Management Client Application**, add hardware metadata (with user = **admin**, password = **1234**).   
     
   

Figure 17. Metadata Definitions

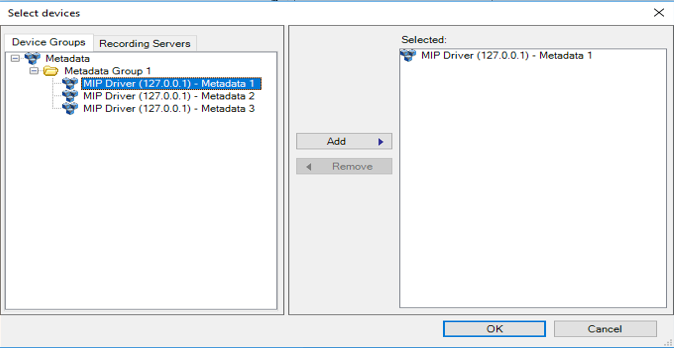
1. Click the **Client** button; under **Related Metadata**, declare metadata definitions for the various cameras.   
     
   

Figure 18. Assign Metadata to Cameras

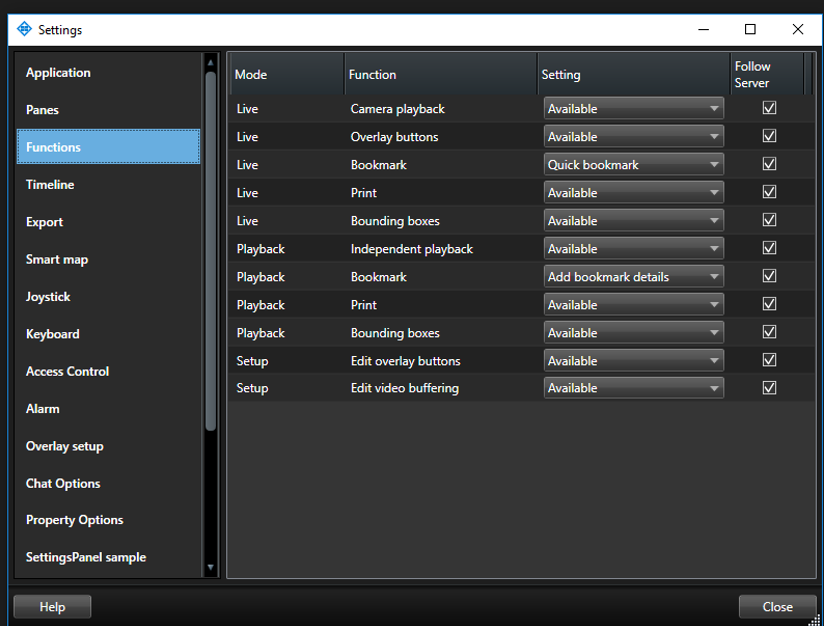
1. Add **Metadata 1** and assign it to **Camera 1**; click **OK**.  
     
   For each camera, repeat steps ‎3 and ‎4, above.
2. To request service, use the camera’s unique identifier, for instance:  
   Camera 1 = Grundig GCI-K3505B (10.0.0.68).
3. Start the smart client and choose the relevant camera. In setup mode, verify that bonding boxes are enabled, and that the new metadata device is present in the “Bounding Box” Providers list.   
     
   

Figure 19. “Bounding Box” Providers List

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. These include detection bounding boxes and generated events.

Once the security management software is installed, continue to the next section to ensure connection with the VMS Gateway driver.

### Configuring the VMS Driver

With connectivity now established, you can go ahead and verify communication. This segment of the Gateway configuration involves editing the VMS driver's .dll file.

**To configure the VMS driver:**

1. Once the VMS Gateway has been installed, go to the **C:\Program Files (x86)\VMS\VMS.Gateway\Plugins** directory, and open the **VMS.Driver.Milestone.dll.config** file.
2. Using a text editor, define the following parameters, as follows:
3. **Username** = take the value for this credential from the VMS.
4. **Password** = take the value for this credential from the VMS.
5. **IP Address** = the network location of the computer on which the VMS is running.
6. **Username ONVIF** = the camera’s username: **onvif**.
7. **Password ONVIF** = the camera’s password: **onvif**.
8. Restart the VMS service by opening **Windows** > **Services**; then close the service and restart it. Alternatively, you could perform this step by simply restarting the computer.

## Connect Cameras: Server Configuration

There are key two steps involved in configuring the AnyVision VMS Server to work with Milestone video devices:

* Defining Server Settings and Selecting Cameras (see ‎3.3.1);
* Defining General Settings (see ‎3.3.2).

You configure the AnyVision Server using the settings window.

### Defining Server Settings and Selecting Cameras

The procedure below explains how to configure Server settings and select cameras.

**To configure Server settings and select cameras:**

1. Click the **Configuration** () icon to open the **Settings** window.

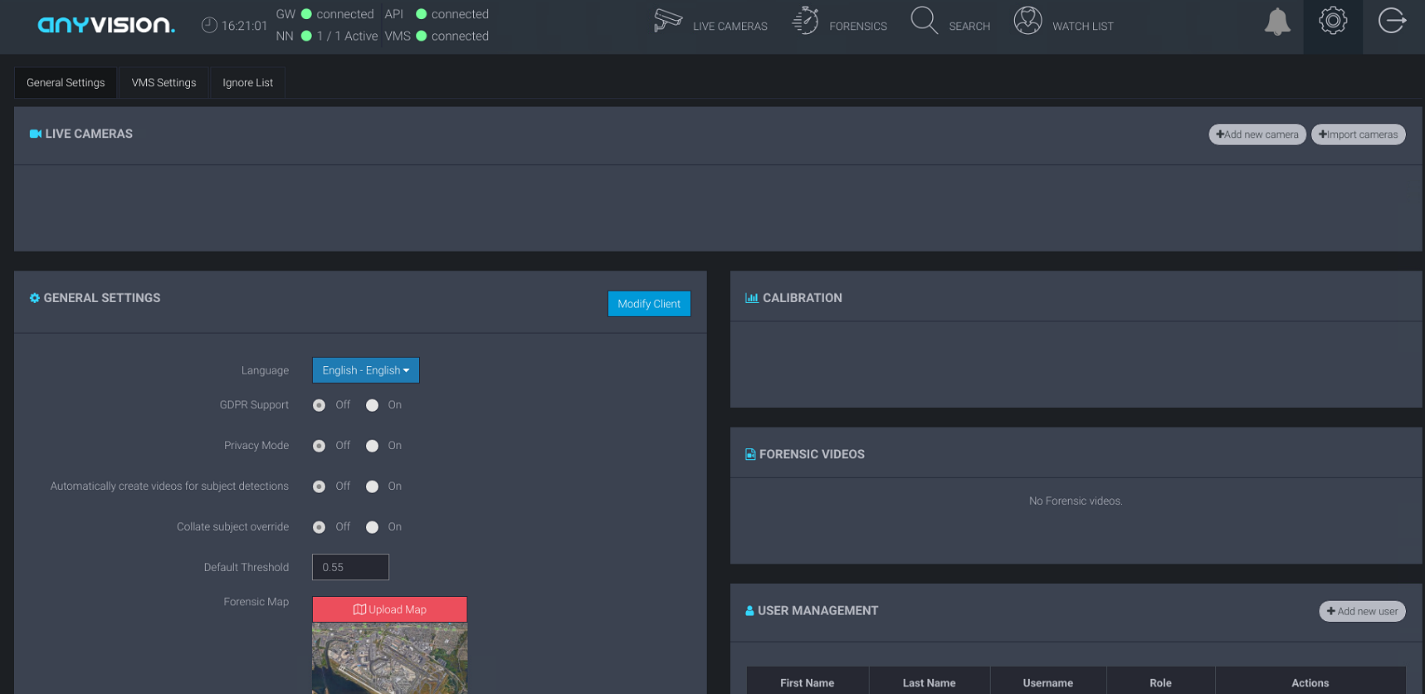


Figure 20. AnyVision Configuration. Settings

1. Toward the top of the screen, click the **VMS Setting tab**.   
     
   The Gateway IP is an internal interface that communicates with the SDKs of third-party VMSes.  
     
   A screenshot of a cell phone

   Description automatically generated

(3)

(4)

(6)

(7a)

(8)

(5)

(7b)

Figure 21. AnyVision. VMS Settings

1. In the **Gateway IP** field, enter the IP address of the Gateway.
2. Click **Check Gateway** to ensure connectivity.
3. 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**.
4. In **VMS IP**, specify the IP address of the VMS Gateway.
5. In the remaining fields, enter the VMS' **Username** and **Password**.
6. To connect with the VMS using the values you specified, click **Connect**.   
     
   A list of cameras associated with the selected VMS is displayed.

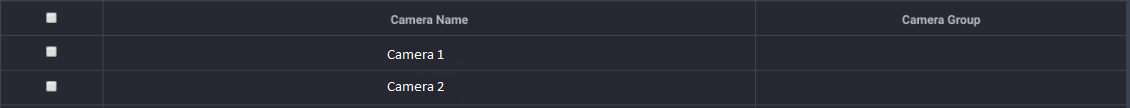


Figure 22. Select Camera Names

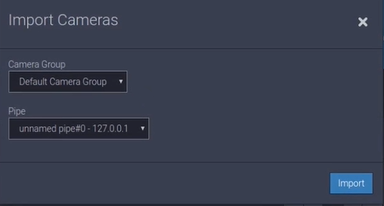
1. For each camera you wish to add to your system, select the corresponding checkbox and click **Import Cameras**.
2. Select the **Camera Group** and **Pipe**.   
     
   

Figure 23. Import Cameras

1. Click **Import**.

### Defining General Settings

The procedure that follows describes how to define the Server’s general parameter settings.

**To define general settings:**

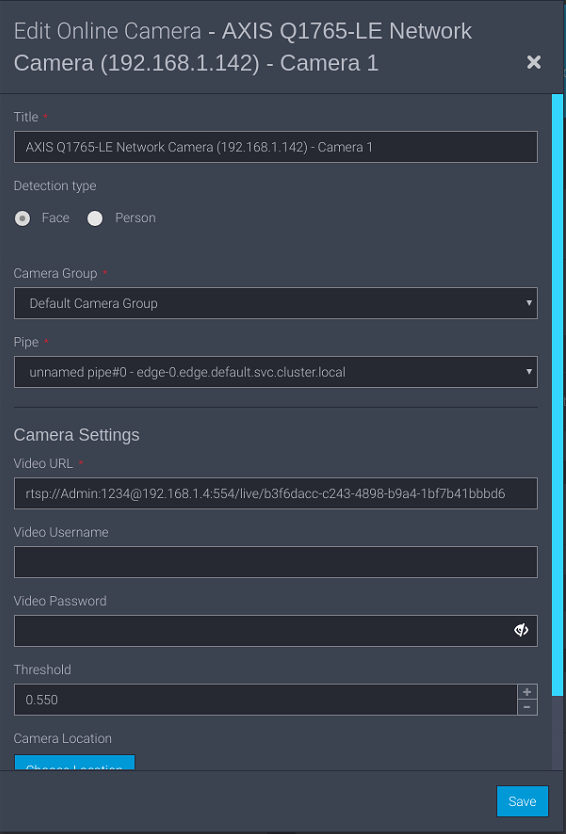
1. Toward the top of the AnyVision Settings screen, click the **General Settings** tab.
2. Review the settings of the recently added cameras by selecting a camera and clicking its corresponding **Edit** button.   
     
   

Figure 24. Create a Camera Group

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

## Define MIPs, Verify Image Display

This section explains how to troubleshoot potential issues stemming from incorrectly defined MIP drivers. The correct MIP drivers and settings are necessary in order for the VMS Gateway to communicate with an external system. Once MIP support is in place, you can verify image display and begin managing alarms with Milestone XProtect. The following topics are covered:

* Troubleshooting MIP drivers (see section ‎3.4.1);
* Managing alarms (see section ‎3.4.2);

### Troubleshooting MIP Drivers

Sending events externally from Milestone XProtect requires VMS support of the MIP driver being utilized. MIP support is necessary in order to enable the camera to display an image.

**To adjust MIP driver settings:**

1. After defining the MIP driver, in the Milestone XProtect Management Client, go to the navigation pane.

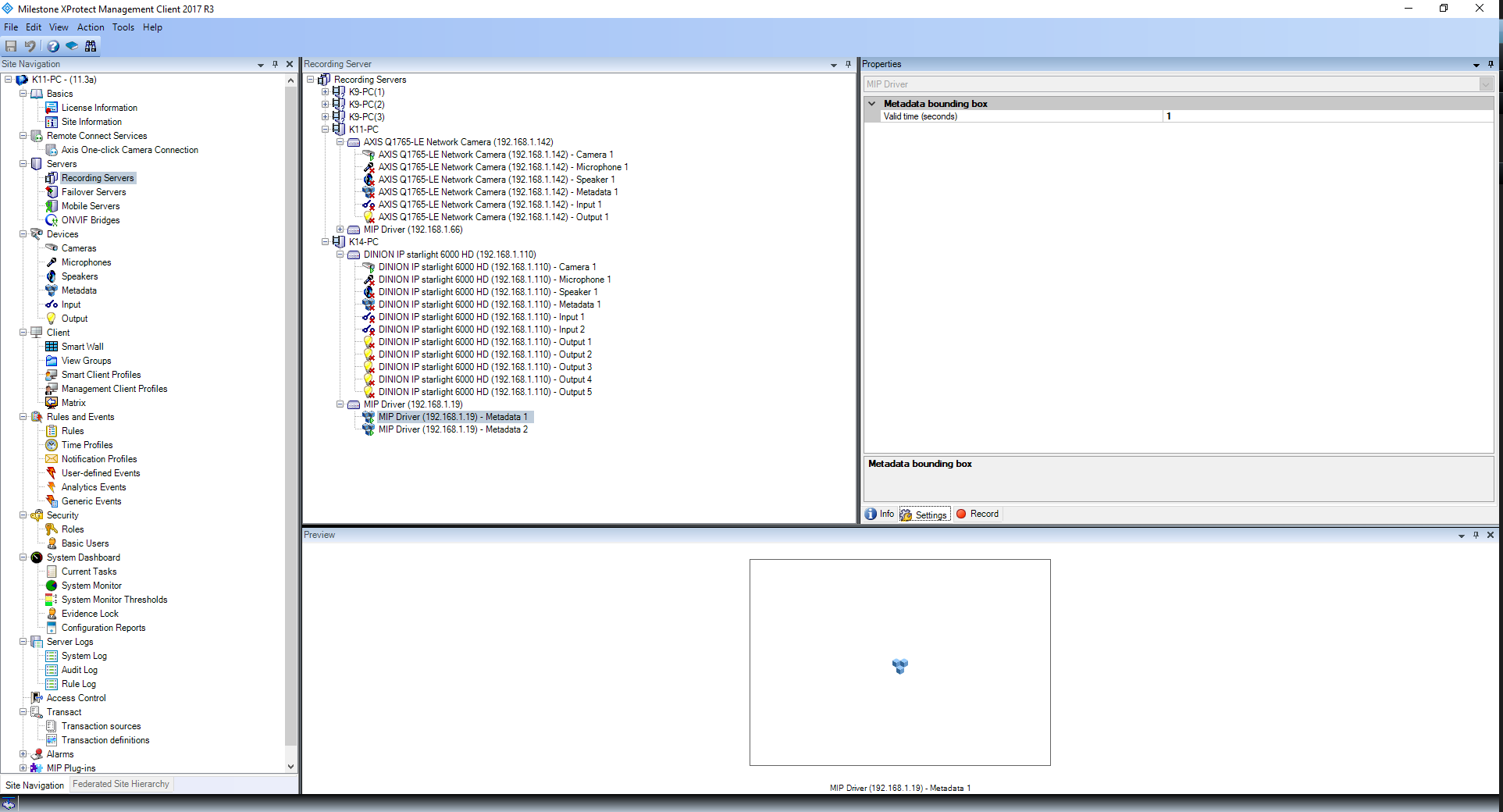


Figure 25. Management Client. Navigation Pane

1. Choose **Servers** > **Recording Servers**.   
     
   

Figure 26. Management Client. Recording Servers

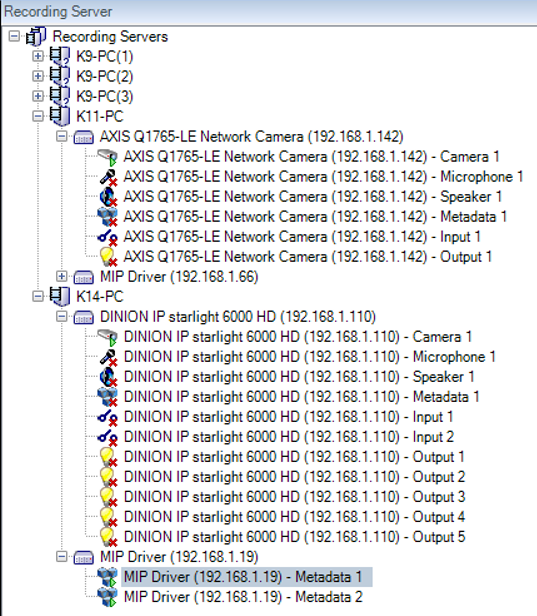
1. Under **Recording Servers**, expand the MIP Driver menu and choose a relevant server.   
     
   

Figure 27. Management Client. MIP Driver Menu

1. Under **Properties**, click **Settings**; in **Metadata Bounding Box** > **Settings** > **Valid Time**, specify **1**.   
     
   The RTSP is obtained by the SDK.

### Managing Alarms

Once the VMS and Gateway configurations are in place, communication confirmed, and MIP drivers updated, you can begin managing alarms.

**To manage alarms:**

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



Figure 28. Milestone XProtect. Live Panel

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

# Index

A

Alarm management, 30

Alarms, 30; issuing, 5, 28

Archiecture. *See* VMS Gateway, architecture

C

Camera groups, 15, 26

Capabilities. *See* VMS Gateway, capabilities

Components. *See* VMS Gateway, components

Control software, installation, 15

E

Events: generating, 28

F

Facial detection, 5

H

Hardware. See Camera groups

M

Metadata: bounding, 29; configuration, 18; ports, 21; related, 22

MIPSDK, 16

O

ONVIF Bridges, 16

P

Ports: 9995, 24

R

Requirements: client hardware, 10; infrastructure, 10; VMS, 10

Requirments: AnyVision, 10

S

Security management: installation, 15

Security, monitoring, 5

T

TCP, 24

U

Ubuntu, 9

UDP, 24

V

Video management: configuration, 15; installation, 15

VMS: driver installation, 23; environment, 5

VMS Gateway: architecture, 9; capabilities, 8; components, 9; installation, 13; requirements, 10

VMS integration: end-to-end process, 12

VMS Server: camera selection, 24; configuration, 24; general settings, 26

W

Windows 10, 9

Workflow. *See* VMS Integration Process, end-to-end