Video Services

User Guide

Confidential-Permaconn Installer Use Only

PERMACONN™

The leader in wireless security

RDDCO Pty. Ltd.
Unit 3/9-11 South Street
Rydalmere NSW 2116
+61 2 9352 1777
www.permaconn.com

Table of Contents

Table of Contents 1
Video Services Overview 2
Video Verification 2
Virtual Patrol 4
Delivering Video to a Third Party 5
Archiving and Retrieval of Footage 5
Permaconn Video Plans 6
Video Bundle Plans with PM54 6
Video Naked Plans with BYO Data 7
Installation and Set-up 9
What you need 9
Camera/NVR Preparation 9
Set-up with PM54 Bundle 10
Video Verification Rule Setup 18
Virtual Patrol Rule Setup 20
Set-up with other remote network access 21
Troubleshooting 23
Appendix A – Supported NVRs and Cameras 26
Appendix B – Special Video Service Event Codes 27

Video Services Overview

Permaconn offers the following two video capture services:

- Video Verification
- Virtual Patrol

The purpose and use case of each are described in the following paragraphs.
Note that this document replaces the document previously titled "Video Verification User Manual".

Video Verification

Purpose

Video Verification enables a monitoring station operator to review images or CCTV footage when an alarm event is received by the automation software. The Permaconn Video Verification service is delivered using existing Permaconn infrastructure and does not require any additional software in the monitoring station.

When the alarm panel sends a burglary event, the Permaconn Video Verification remotely connects to the NVR or camera and fetches the video clip or still image from the linked camera. The system then delivers an extended contact ID event to the monitoring station's automation software. The operator simply clicks on the video verification URL link which opens the video clip in default desktop browser (Internet Explorer, Chrome etc.). This allows the monitoring station operator to quickly review video footage and decide if it is a genuine false alarm.

Brief Description

Permaconn's Video Verification service works by pairing an alarm system with a Permaconn Communicator and an NVR (or IP Cameras). Individual cameras are paired with alarm zones, so that only the specific footage from a triggered zone is sent to monitoring station. When an alarm is triggered only the relevant footage or image will be sent back to base.

Permaconn's Video Verification is easiest to configure when connecting the NVR or cameras directly to the Permaconn PM54 however, the system will also work with the Permaconn communicator if the NVR and/or camera is reachable from the Internet.

Operation of Video Verification During an Alarm

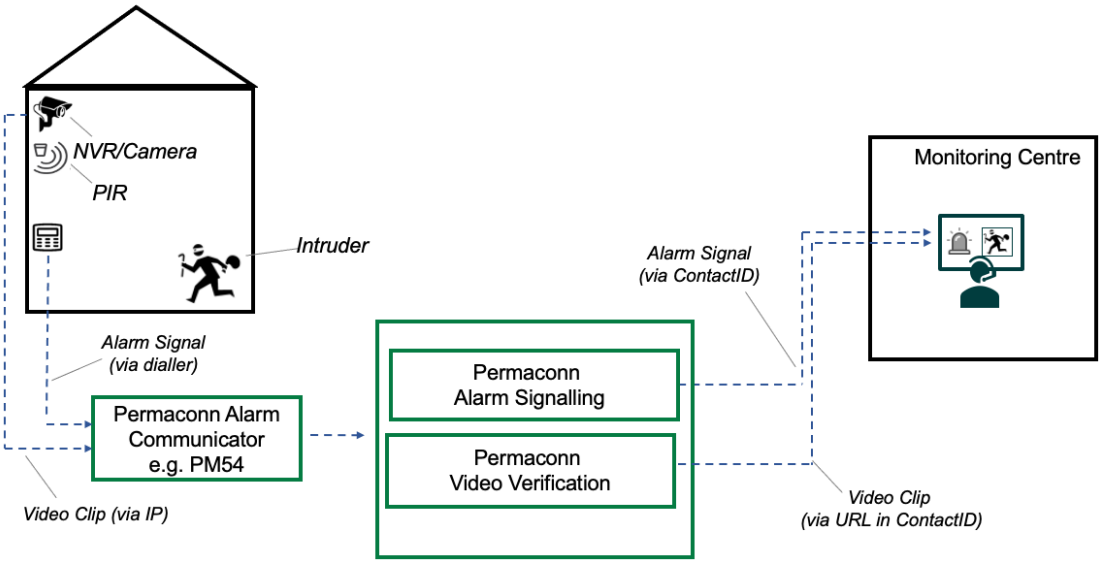

Figure 1 – Overview of Video Verification of an Alarm Event

When an alarm event is detected, it will trigger the following sequence of events:

1. The alarm panel will send the alarm event to the monitoring station via the Permaconn communicator.

2. The Video Verification service will identify the zone that triggered the alarm and look up the camera paired to that zone.

3. The Video Verification service will connect to the NVR or camera to retrieve the footage.

    a. If using an NVR, the system will retrieve a short video clip from the most recent motion-capture video recording from the relevant camera.

    b. If using a stand-alone camera with no storage, the system will commence the live capture of the real time video stream.

4. The Video Verification service will store the video clip in the Permaconn cloud and generate a secret URL link to the video.

5. The Video Verification service will send a follow-up extended ContactID event (Event code E720 – Video Verification Event) to the monitoring station containing the link to the video footage.

6. The monitoring station operator can view the video footage by clicking on the link.

7. Repeated violations of the same zone, or violation of other zones will repeat the above sequence until the number of clips reaches the pre-configured Maximum Clip Limit (typically six clips per alarm event)

Notes on Video Clip Timing for Video Verification

The exact timing of the video clip will differ whether it is using an NVR or a standalone camera.

NVR

Most modern NVR systems are triggered to record video when it detects motion. The time that the camera detects motion and the time the alarm system detects a zone violation will differ depending on the specifics of the on-site installation.

For example, depending on where the camera is located relative to the PIR sensor, a burglary alarm triggered by the PIR may occur some seconds after the camera detects an intruder entering the field of view.

The Permaconn Video Service will retrieve the video footage from when the camera detected motion, even if this precedes the actual alarm event by up to 120 seconds.

Stand-alone Camera

Stand-alone cameras don't typically have internal storage. In this case the Video Verification service will connect to the camera and commence the capture of the live video from the moment the burglary alarm is detected.

There is a meaningful delay between when a zone is violated and when the alarm panel delivers the ContactID message to the monitoring station of up to 30 seconds. Depending on the placement of the camera in relation to the zone sensor, this delay may allow the intruder to move out of the frame of the camera before the recording commences. It is for this reason that Permaconn recommends using an NVR where possible.

Virtual Patrol

Purpose

Virtual patrol allows a monitoring centre to capture and view images or CCTV footage at selected times of the day. This could potentially replace a guard doing a physical patrol or it can be used in applications where there is a requirement to check the CCTV footage on a regular basis.

Like video verification, the system delivers an extended contact Id event to the monitoring station's automation software, with an embedded URL that the operator can simply click to view the video clip.

Brief Description

Permaconn's Virtual Patrol works by setting up a schedule, combined with an NVR/Camera, that captures an image or video clip at preconfigured times of the day and on specific days of the week. When combining the service with an NVR, the NVR should be setup for constant recording instead of motion detect.

Like Video Verification, the setup requires a Permaconn PM54 if the Cameras/NVR is not accessible from the internet.

Delivering Video to a Third Party

The video clip viewed by the monitoring station operator can be sent to a third party such as the customer, Police, or a patrol guard by copying the URL and sending it via email or text message.

Note: Take note who you share the video link with. While the secret link is complex, anyone who knows the link can view and/or save the footage without requiring a username or password.

Archiving and Retrieval of Footage

The video clips are stored on the Permaconn servers for 30-days before being archived to long-term cold storage for five years.

The video footage can be retrieved during the first 30 days using the URL delivered to the monitoring station. This video clip can be saved from the browser to disk, allowing the monitoring station to archive this file according to their own procedures.

If more than 30-days have elapsed the monitoring station can request that Permaconn retrieve this footage from cold storage for a nominal fee.

Permaconn will store video footage for 5 years, after which point footage will be permanently deleted.

Permaconn Video Plans

Permaconn has designed a variety of Video plans to make the selection and use of the service as easy as possible.

Video Bundle Plans with PM54

Video Bundle plans are the simplest way to use the Video service. This approach uses the Permaconn PM54 communicator to provide both the alarm signalling and the Internet connection with sufficient data to upload the video clips.

- Sizing is based on 30-second Full HD video clips. Longer clips or 4K video will reduce the number of clips available before hitting the data limit.
- Cameras must be configured to record using the H.264 video codec format. Most internet browsers do not yet support the newer H.265 and so will not be visible to the monitoring station operator.

These bundles come in four sizes:

Video Plan Name	Data and Clip Allowance per month
Small	**24** Full HD video clips at 30-second each to a maximum of data usage 480MB.
Medium	**48** Full HD video clips at 30-second each to a maximum of data usage 960MB.
Large	**96** Full HD video clips at 30-second each to a maximum of data usage 1.9GB.
Extra Large	**192** Full HD video clips at 30-second each to a maximum of data usage 3.8GB.

Data/Clip Allocation Top-Ups

If a Video service exceeds the maximum data usage threshold, the video service will cease to operate, and no further video clips will be captured. Alarm signalling will continue to operate as per normal.

Usage notification messages will be sent to the monitoring station at the following thresholds:

- 70% of data consumed.
- 80% of data consumed

- 95% of data consumed
- 100% of data consumed. Video service is suspended.

The notification messages are sent in the form of events to the monitoring station, and as emails to both the administrator/s of the monitoring centre and/or bureau.

Video top-ups are available at any time through the Atlas portal and can either be adding another plan of the same or smaller size (e.g., if on a Medium plan, adding another Medium or Small plan for the remainder of the month) or an upgrade of the service to the next size up. (e.g., upgrade to a Large plan).

Video Naked Plans with BYO Data

In some applications, the data allowances in the Bundle Plans described above might not be suitable. In this case, Permaconn also provides "Naked" Video Plans which requires some other form of Internet connection to allow the Service to reach the NVR or cameras.

The Internet connection could be the corporate WAN, so long as the appropriate firewall rules can be configured to allow remote access to the NVR and camera, and the connection has sufficient bandwidth to stream the video clips in real time. Alternatively, a PM54 with a standard data plan (1GB, 10GB etc.) may also be used.

Unlike Bundle Plans, Naked plans do not include any data. The amount of data used for video will measure and capped based on the plan's allowance.

Video Plan Name	Clip allowance per month
Naked Small	**24** Full HD video clips at 30-second each to a maximum of data usage 480MB.
Naked Medium	**48** Full HD video clips at 30-second each to a maximum of data usage 960MB.
Naked Large	**96** Full HD video clips at 30-second each to a maximum of data usage 1.9GB.
Naked Extra Large	**192** Full HD video clips at 30-second each to a maximum of data usage 3.8GB.

Notes on Video Clip sizing

- Sizing is based on 30-second Full HD video clips. Longer clips or 4K video will reduce the number of clips available before hitting the allowed disk storage limit.

- Cameras must be configured to record using the H.264 video codec format. Most internet browsers do not yet support the newer H.265 and so will not be visible to the monitoring station operator.

Data/Clip Allocation Top-Ups

If a Video service exceeds the maximum data usage threshold, the video service will cease to operate, and no further video clips will be captured. Alarm signalling will continue to operate as per normal.

Usage notification messages will be sent to the monitoring station at the following thresholds:

- 70% of allowed video data used
- 80% of allowed video data used
- 95% of allowed video data used
- 100% of allowed video data used. Video service is suspended.

The notification messages are sent in the form of events to the monitoring station, and as emails to both the administrator/s of the monitoring centre and/or bureau.

Video top-ups are available at any time through the Atlas portal and can either be adding another plan of the same or smaller size (e.g., if on a Naked Medium plan, adding another Naked Medium or Naked Small plan for the remainder of the month) or an upgrade of the service to the next size up. (e.g., upgrade to a Naked Large plan)

Installation and Set-up

What you need

To set up the Video Service you will need:

1. A Permaconn Communicator (connected to an alarm system for video verification)
2. An NVR or Camera on the supported list (Appendix A)
3. Remote access to the NVR or camera

Camera/NVR Preparation

1. Consult the manufacturer user manual on how to connect and configure your device.
2. For security reasons it is recommended that the default password be changed. This is a required step on most cameras/NVRs during initial setup.
3. Once inside the configuration, configure the date and time on the device, either manually or via NTP.
4. Browse to the location where the video encoding settings are configured. Select the desired resolution. Take note that a higher resolution will result in more data usage and so therefore fewer available clips per month.
5. Ensure the video encoding is set to **H.264**.
6. If using an NVR configured to record on motion detect, ensure that the pre-record buffer is less than the duration of the video clip, e.g., if configuring the device to retrieve a 30 second clip, the pre-record buffer should ideally be less than 20 seconds to ensure that the event that triggered the alarm is captured in the clip.
7. If connecting to the camera/NVR via the PM54 (as described in the next section), browse to the network settings on the device. Give the device a **static IP**. Ensure that the device subnet is the same as the PM54 LAN subnet. The PM54 LAN subnet can be determined by performing a device ping from Atlas and navigating to the LAN section of the IP tab. The default is 192.168.111.x

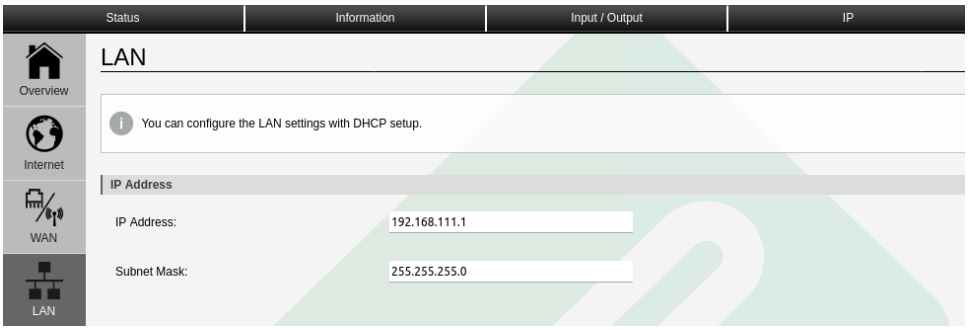

Figure 1 – Locating the LAN subnet of the PM54

Set-up with PM54 Bundle

Activate the PM54 with Video Service

While activating a PM54, there is checkbox option to add on Video Service (see figure 2 below).

1. Tick the checkbox for Video Service (Figure 2 below). Ticking this box enables access to the Video plans fields.

2. Select the desired Video Plan:

    a. Select a Bundle Plan if using the PM54 data purely for the Video Service.

    b. Select a Naked plan if using your own internet connection (through the PM54's WAN connection) or if you require additional data on top of the video service data.

3. If a Naked pack was selected, select the appropriate data pack according to your data requirements.

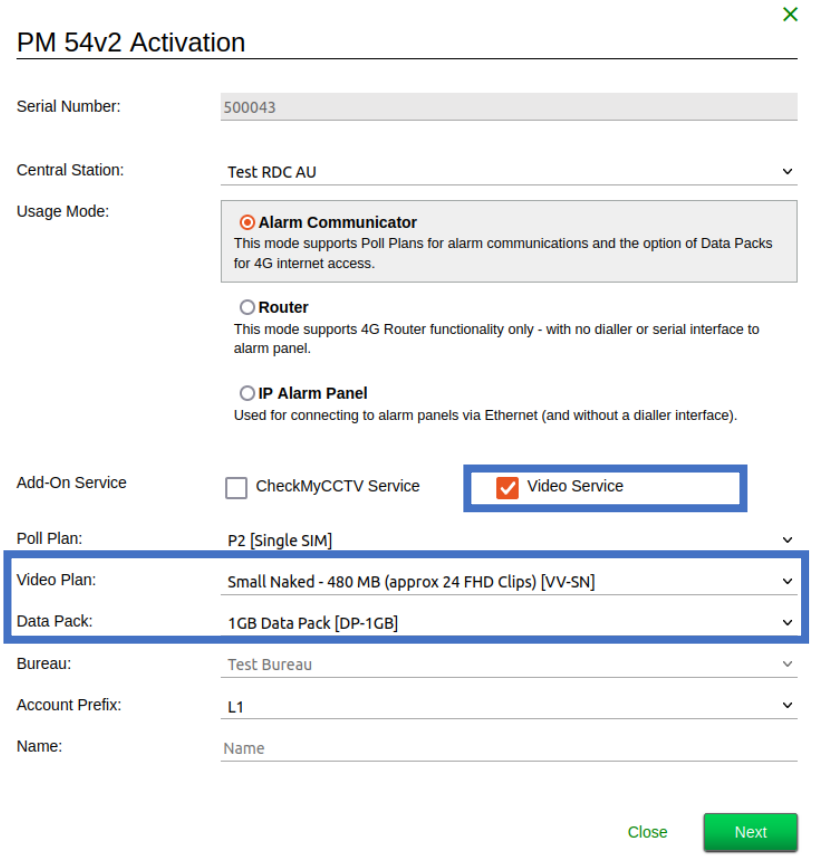

Figure 2 – Video Add-On service on PM54 Activation Screen

Configure the Video Service Options

Navigate to the fleet tab and search for your Permaconn device.

Click on the option button to the left of the device number and select "Video Configuration" from the pop-up menu.

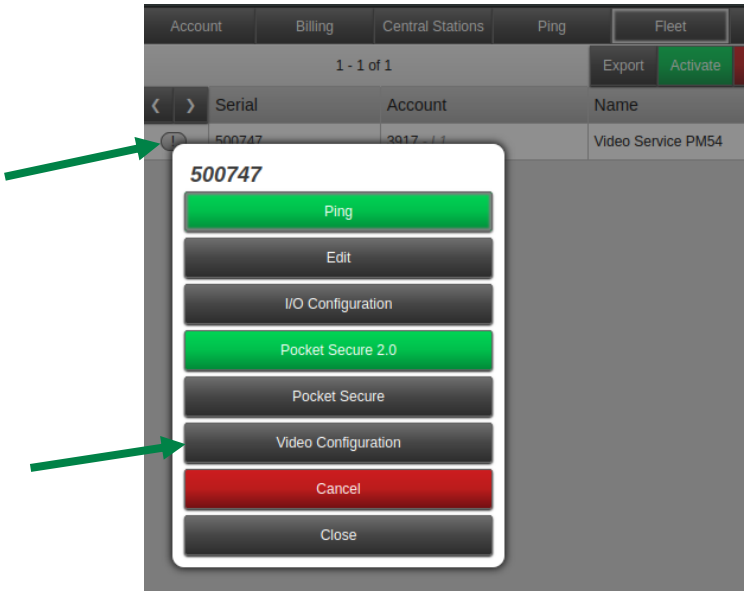

Figure 3 – Video Configuration selection on the fleet tab

Adding an NVR or Camera

1. Select "Add Device" to add your camera/NVR connection details.

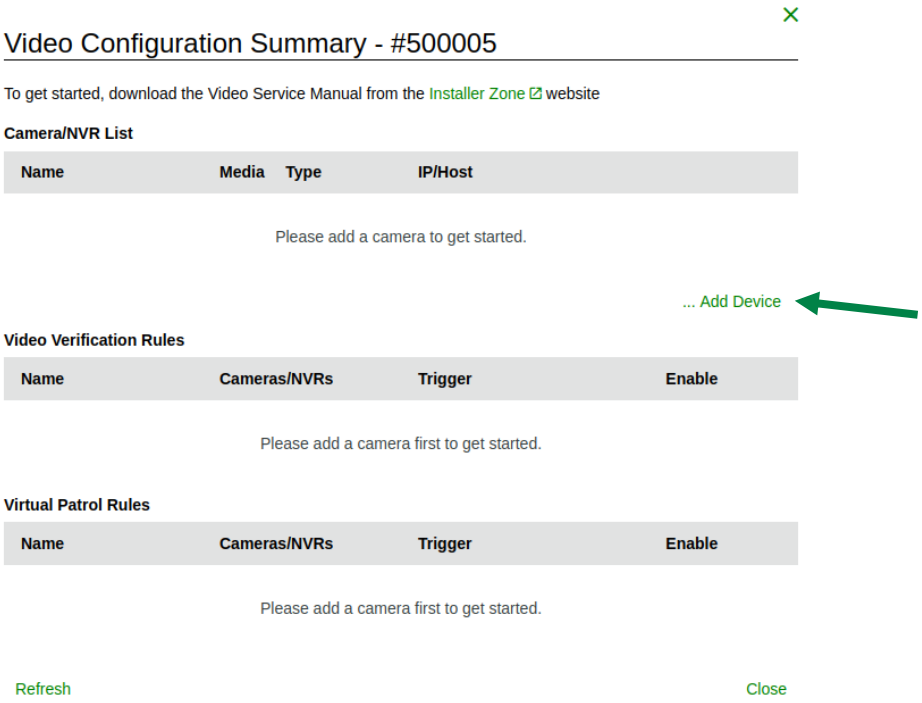

Figure 4 – Video Configuration Summary form

2. Select whether to add a camera or NVR

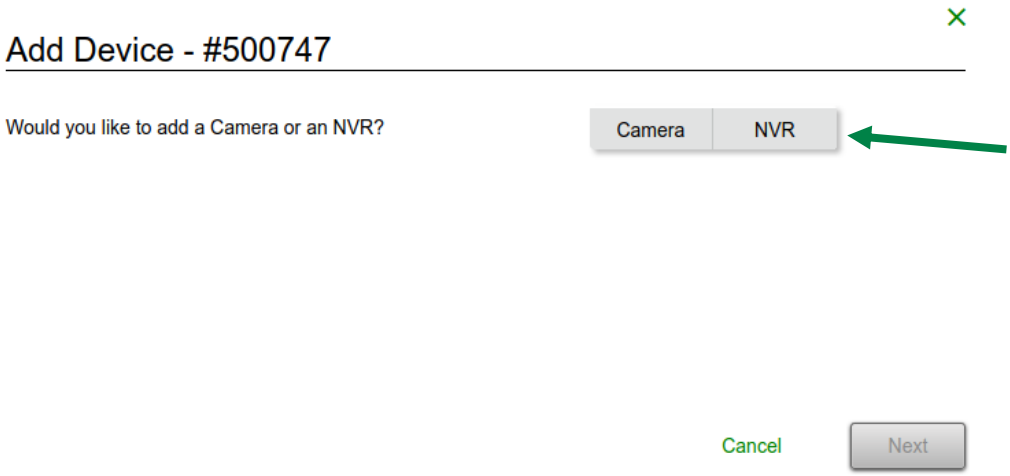

Figure 5 – Device type selection

Adding an NVR

1. Select make of NVR from the list.

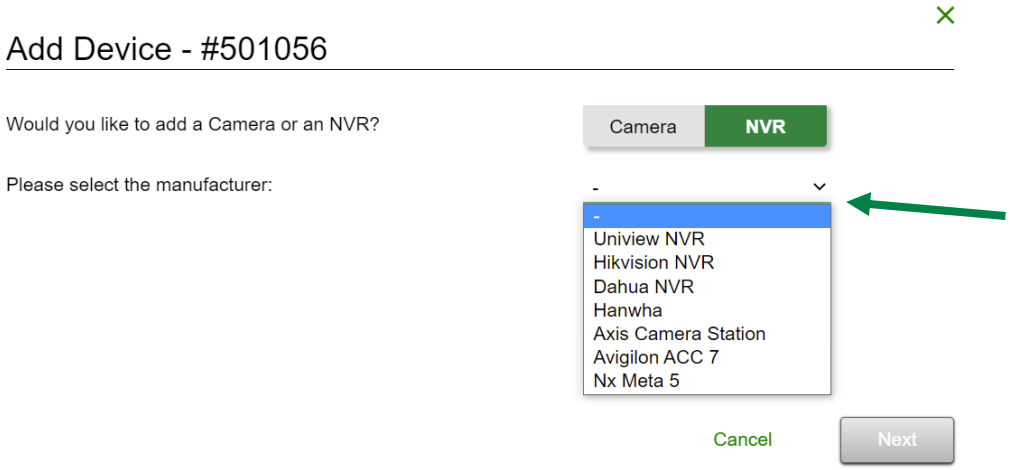

Figure 5 – NVR manufacturer selection options

Adding a camera

1. Select whether you would like to manually configure the IP details or whether you would like the PM54 to try and detect the camera.

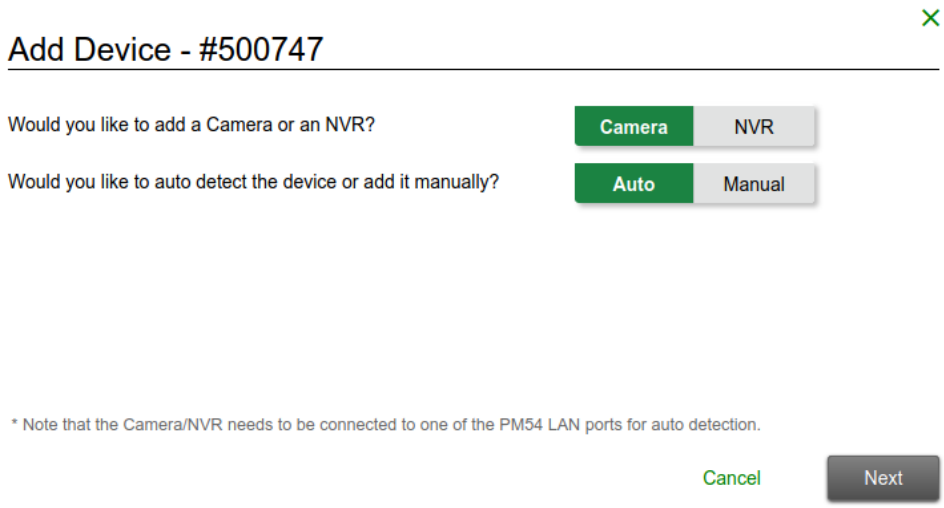

Figure 6 – Options for adding a camera

Autodetect Camera

1. On auto detect, the pm54 will scan the network for any cameras and present the list of detected cameras for selection.

2. Should the desired camera not be present in the list, there is an option to "Retry" or select "Close".

3. When "Close" is pressed, the Camera Configuration form will load, where the IP details can be entered manually.

4. When pressing "Select" next to the desired camera, the Camera Configuration form will show, preloaded with the detected IP details.

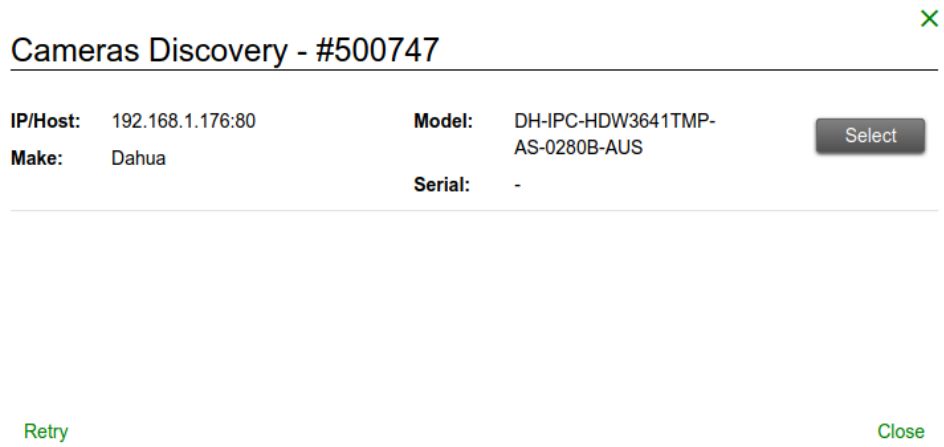

Figure 7 – List of Cameras detected during Cameras Discovery

Manually configure camera

1. When selecting "Manual" configuration or the camera from the Camera Discovery form, the Camera/NVR configuration will be shown where all the details required to connect to the camera can be entered.

2. The format of the clip and duration of the video can be selected.

3. After entering the details of the camera, the "Test Configuration" button should be pressed to confirm that the configuration details have been entered correctly and the server can communicate with the Camera.

4. Note that the Test configuration will only work for video when 10 sec duration is selected. Once it has been confirmed that the video works, the desired duration should be selected before pressing the save button.

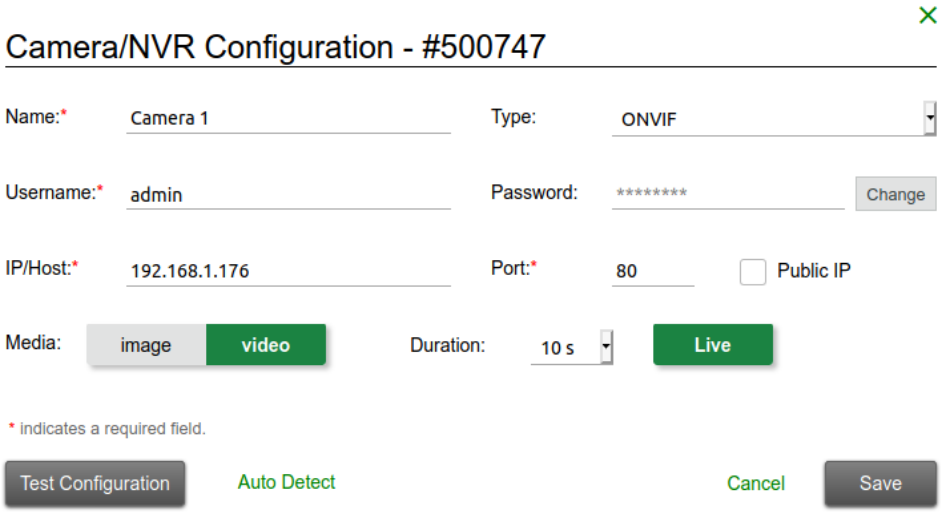

Figure 8 – Camera Configuration Form

Configuring the NVR

Dahua, Uniview, Hanwha or Hikvision NVR

For Dahua, Uniview, Hanwha or Hikvision NVRs complete the authentication and IP details and select the port number on the NVR where the desired camera is connected.

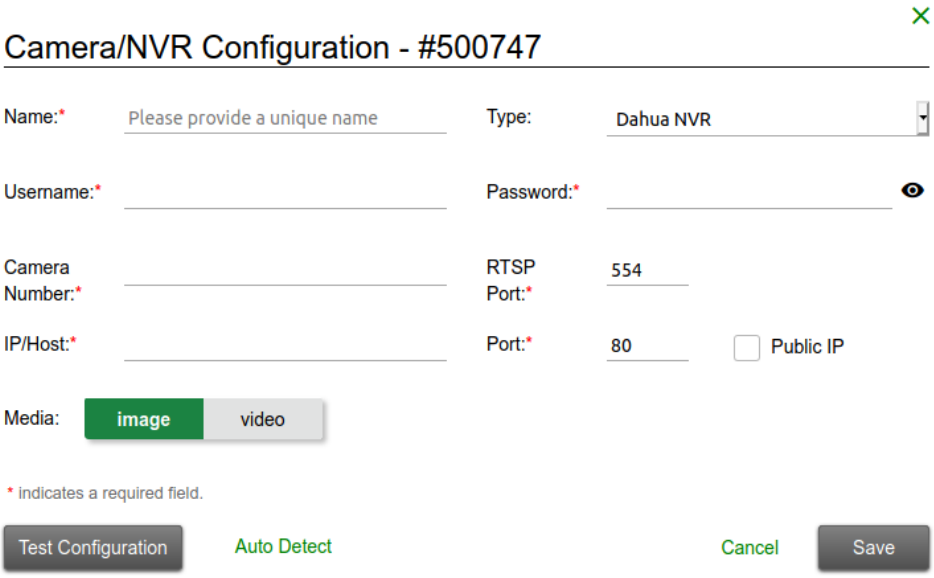

Figure 9 – NVR Configuration Form for Dahua NVR

Axis Camera Station

For Axis configuration, provide the serial/MAC of the camera that can be found in the Camera Station software instead.

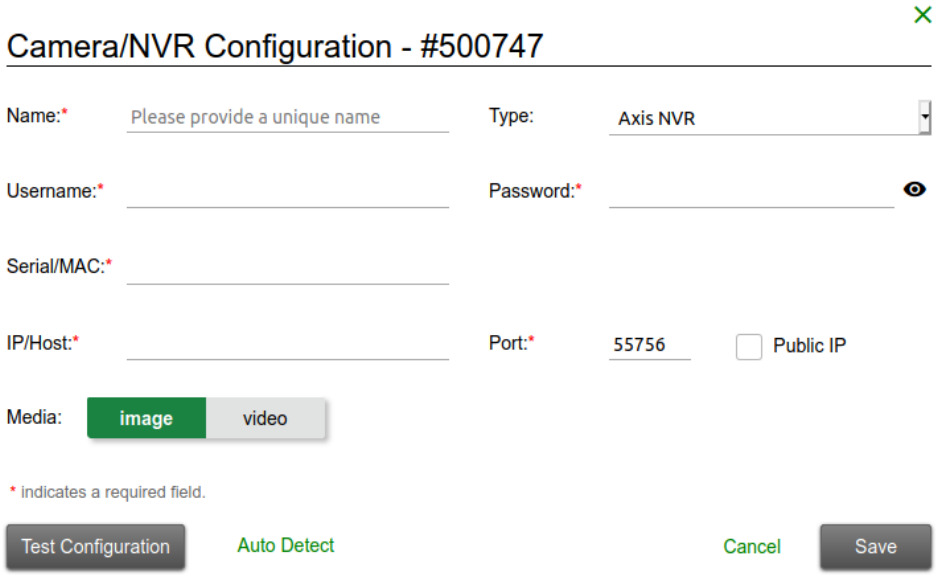

Figure 10 – NVR Configuration Form for Axis Camera Station

Avigilon ACC 7

The setup for interfacing with an Avigilon ACC 7 requires both the site name and the MAC Address of the camera.

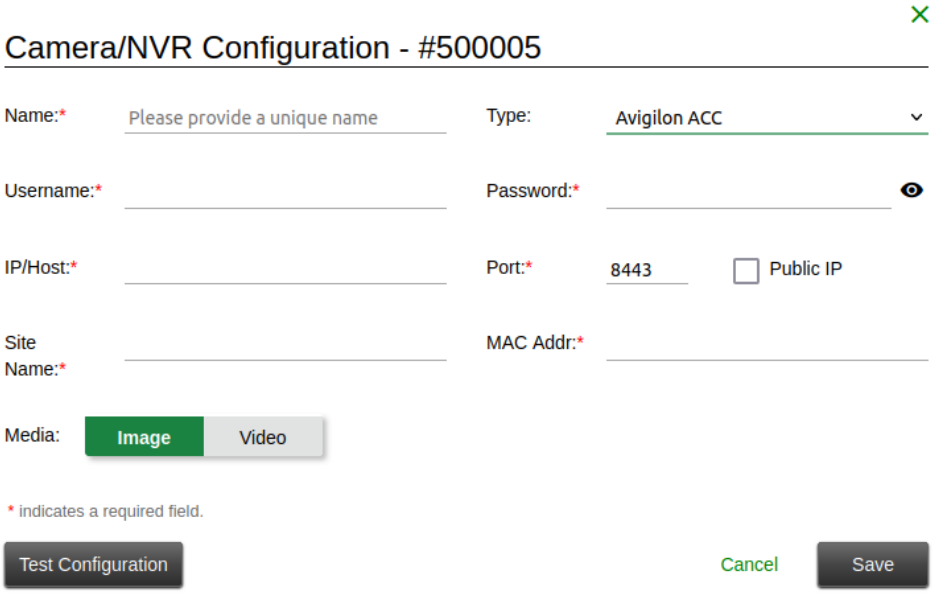

Figure 11 – NVR Configuration Form for Avigilon ACC 7

Nx Witness\Meta 5

For Nx configuration, provide the camera ID that can be found in the Nx Witness\Meta software. Note that only Nx Witness\Meta version 5.0 and later is supported.

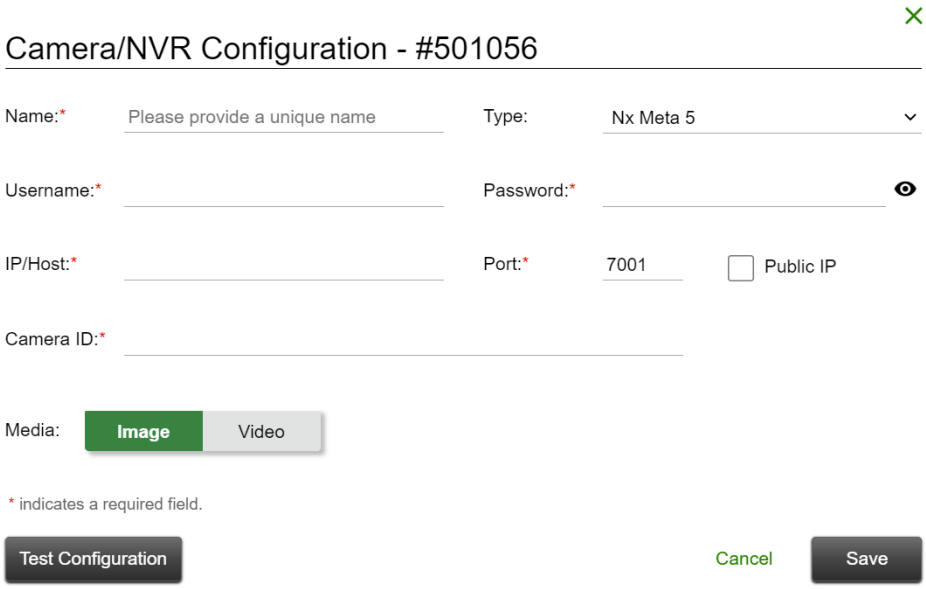

Figure 12 – NVR Configuration Form for NX Witness\Meta

Video Verification Rule Setup

The video verification rule setup can be accessed from the Video Configuration Summary form.

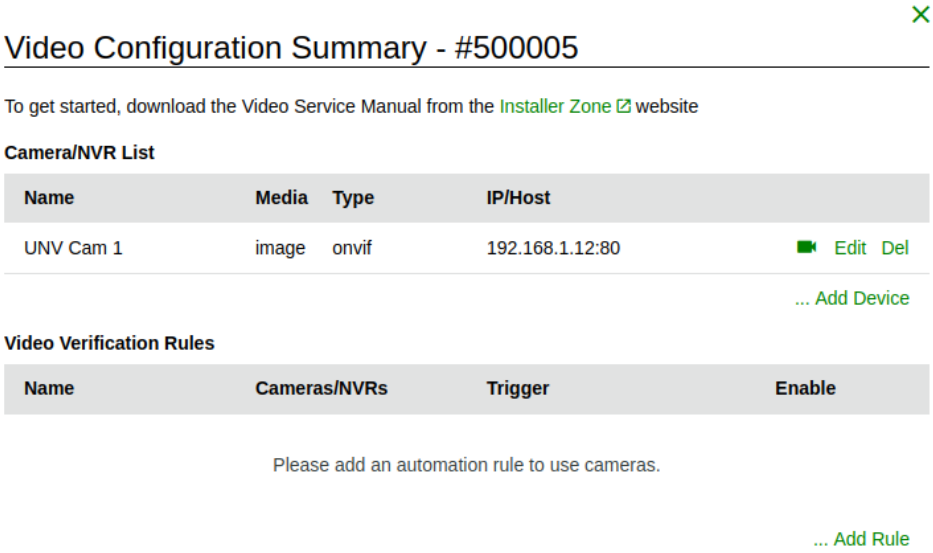

Figure 13 – Video Verification Form showing option to add a rule

The video verification system provides 2 options to trigger a capture:

1. Alarm panel event: The system will perform a capture after the alarm panel sent an event. For alarm events, this is paired with a zone or partition.
2. PM54 Input: The system can also be configured to perform a capture if a change on the input is detected on the pm54.

Pair to Zone

1. After at least one camera or NVR configuration has been saved, video verification rules can be added which will control when a capture will be performed.

2. Add the desired cameras or NVRs that are associated with the zone.

3. Select Capture Trigger “On Event” and select the “Alarm” checkbox.

4. Add the desired zones or partitions.

5. Additionally, emails addresses can be added to the rule, which will receive a link to the captured video in the email whenever the rule is triggered.

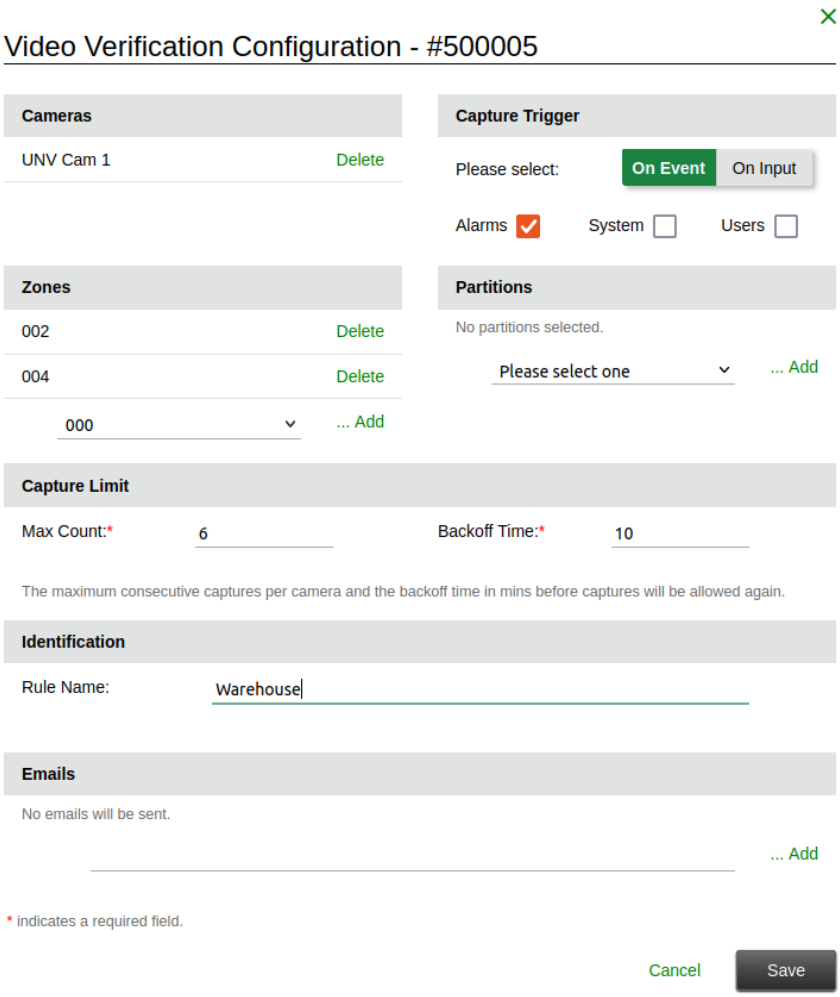

Figure 14 – Video Verification Alarm Trigger Setup

Set capture limit

Depending on the installation, an alarm panel can continue to send burglary events whenever the PIR triggers. To prevent the system from taking excessive captures, and thus exhausting the data plan, the rule can be configured to stop capturing after a certain number of clips and only resume once the alarm panel stops transmitting these burglary events. The backoff time after which the system will start acting on events again can be configured.

Input triggered capture

1. Add the desired cameras or NVRs that are associated with the pm54 inputs.
2. Select Capture Trigger “On Input” and select which input or inputs will trigger the capture.
3. Select the condition for the capture:
    a. Capture only when the input is triggered, and the panel is armed (Will report only if a burglary event is sent by the panel).

b. Capture at any time the input is triggered regardless of the state of the alarm panel (24 hours)

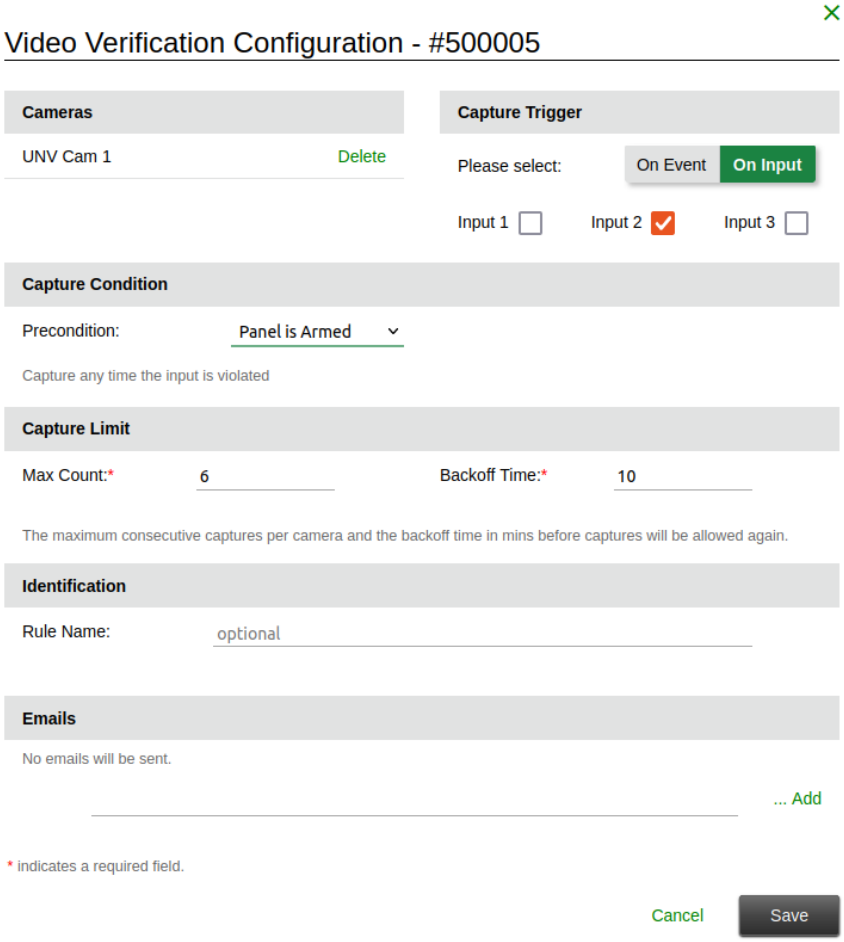

Figure 15 – Video Verification Input Trigger Setup

Virtual Patrol Rule Setup

Follow the following steps to setup a virtual patrol schedule

1. Add the desired cameras or NVRs that are associated with the virtual patrol.
2. Select a virtual zone that will be associated with this rule (optional).
3. Select the day of week when the capture will occur.
4. Select the time zone and add the times of the day when the rule will be triggered.

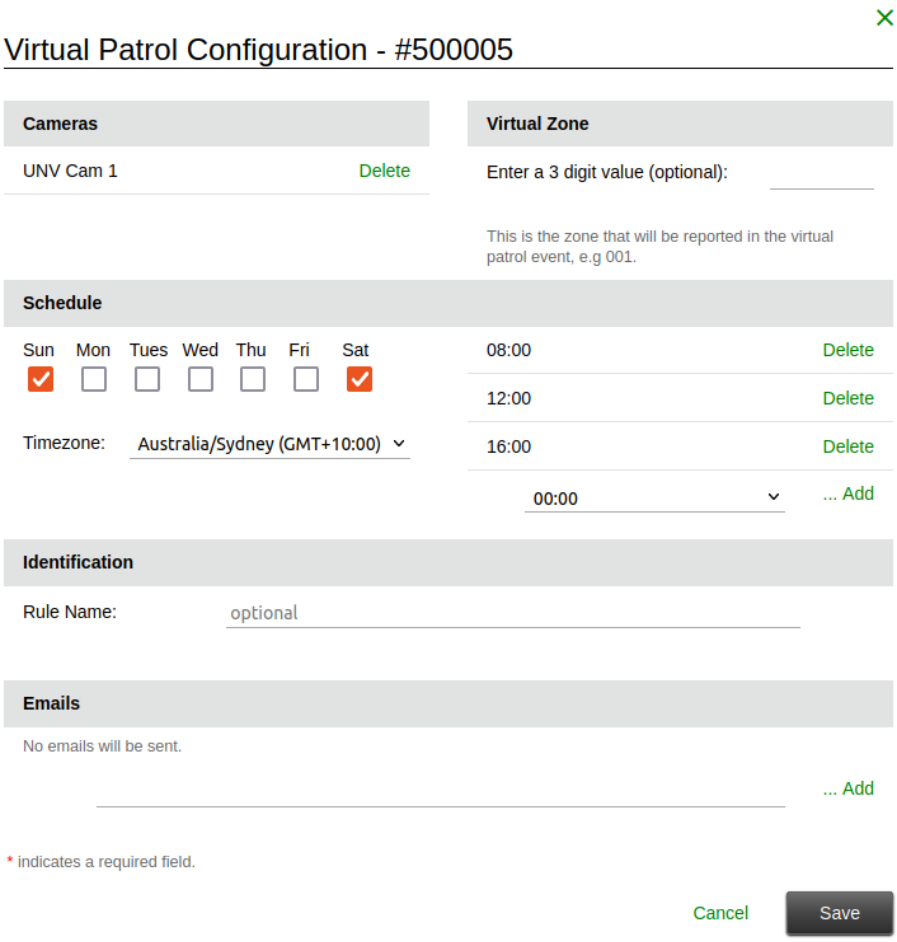

Figure 16 – Virtual Patrol Setup

Set-up with other remote network access

It is possible to connect to a camera or NVR provided that the device is publicly accessible from the Permaconn Video Service server. To do this, the premises need a public routable IP from their ISP and the necessary port forwards need to be configured on the router.

The firewall will need to be configured to allow inbound connections from the following Permaconn Video Service servers IP Addresses and ports:

- 13.237.40.185
- 3.105.66.86
- 52.65.49.151
- 54.79.47.99

Ports:

- Port 80 is typically the default for an NVR, but this is configurable on the NVR, so the same port must be configured in Atlas and on the firewall.

Configuration is the same as the setup for connecting through the PM54, but on the camera configuration, the “Public IP” checkbox must be ticked.

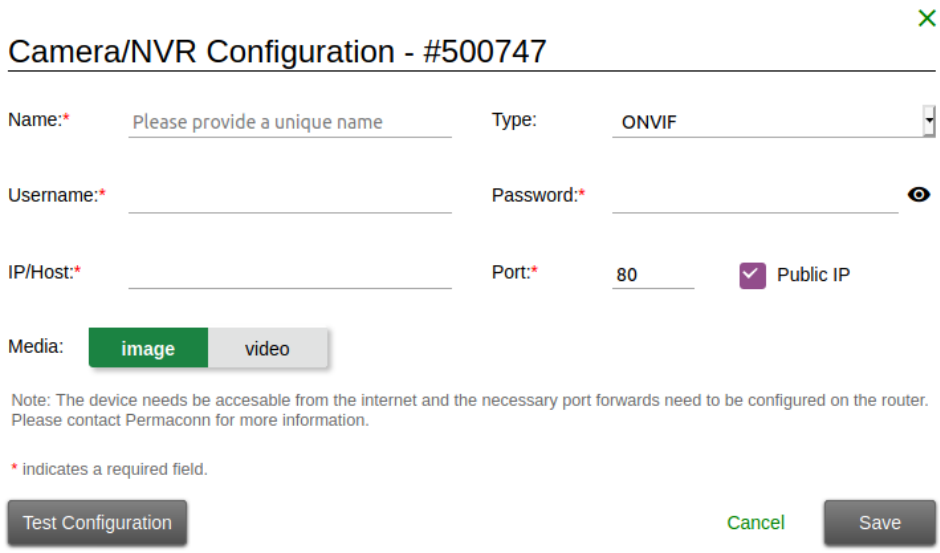

Figure 17 – Configuring a camera with a public IP address.

Notes on Firewall Rules

For the Video service to contact the NVR, the firewall needs to allow connections to the NVR ports.

Troubleshooting

When testing the configuration, the reason for the failure will be displayed on the status box.

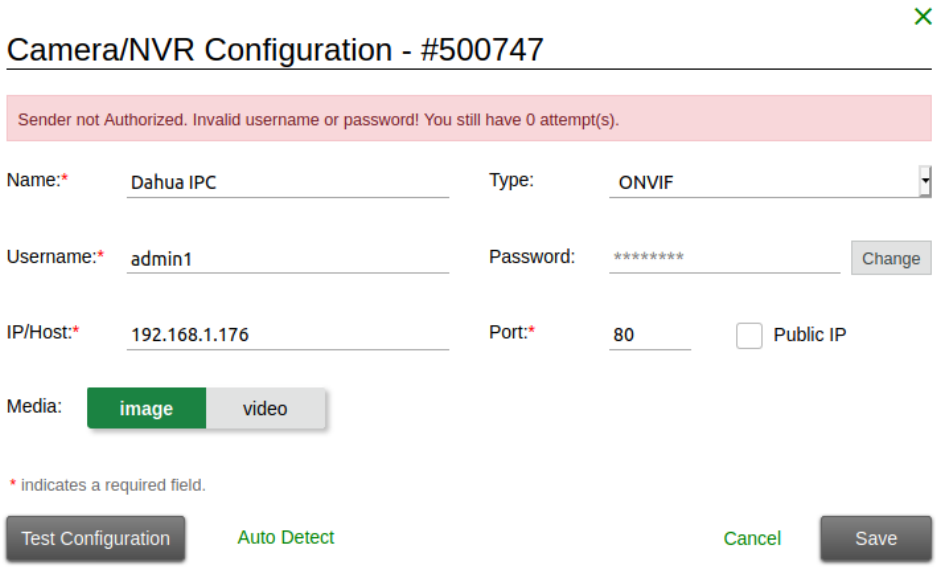

Figure 18 – Configuration test failed due to invalid username.

Unable to connect to the device IP and port.

1. Ensure that the camera/NVR is connected in the LAN1 or LAN2 port of the PM54 and that the device is powered.

2. Verify that the PM54 can detect the device by:

    a. Inspect the LAN1/LAN2 port on the PM54 and verify that the LAN indicator LEDs are blinking.

    b. You can also navigate to the Ping->IP->Overview page on Atlas and verify that the connected LAN port has a green checkbox.

    c. Click on the green number next to the "Active Clients" as shown in the figure below to bring up a list of LAN clients.

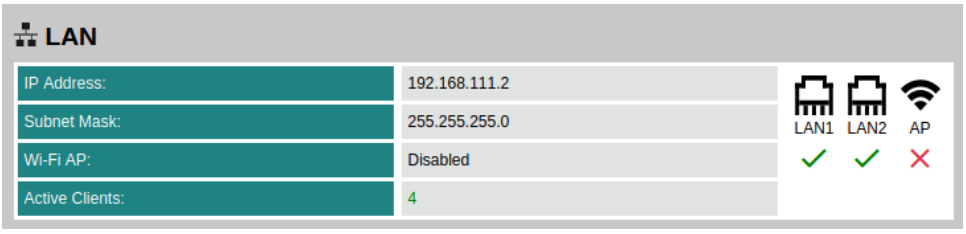

Figure 19 – LAN section of PM54 Ping IP Overview Page.

d. Verify that the IP address of the camera/NVR is listed in the active client list.

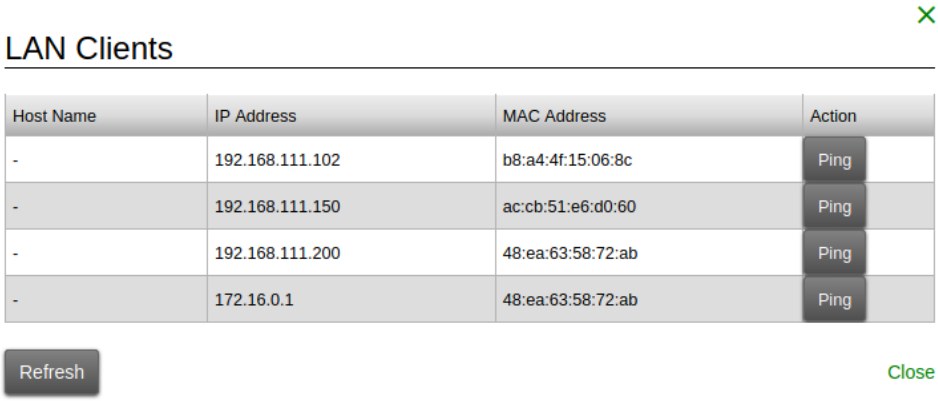

Figure 20 – List of active LAN clients.

e. Ping the device. If the ping is successful, verify that the ports in the camera/NVR matches the ports on the camera configuration page.

f. If the IP address of the camera/NVR changed, it means that the camera/NVR was configured to use DHCP. In this case log into the camera/NVR and set the IP address to static.

Camera Image failed

1. Some cameras require that you enable ONVIF protocol, ensure that if the camera/NVR has this as a configurable option, that it is selected and ensure that the username/password matches the configuration of the camera configuration page.

2. Some cameras do not support ONVIF snapshot or require it to be manually enabled. In this case, either enable the option, or try getting the video instead.

Hikvision NVR

1. For the Video Service server to connect to a Hikvision NVR, the NVR needs to support ISAPI protocol and the protocol needs to be enabled on the Integration Protocol tab in the Configuration->Network-> Advanced Settings page.

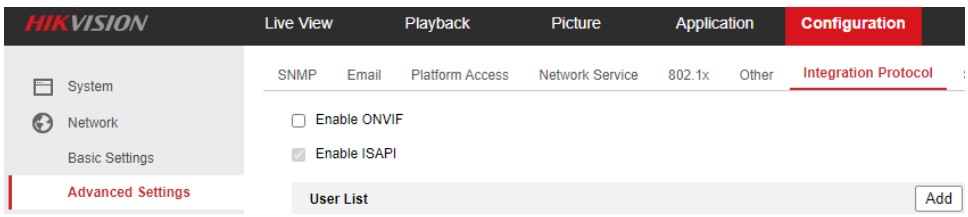

Figure 21 – Hikvision ISAPI enable.

Video Not playing in Chrome Browser

1. In Chrome, go to Chrome Menu > Settings > Advanced. Under System, disable Use hardware acceleration when available

Appendix A – Supported NVRs and Cameras

The following devices have been tested and confirmed to work with the solution:

Manufacturer	Model	Type
Axis	Q1604	IP Camera
	P3245-LVE	IP Camera
	S2208	NVR
Dahua	HDW3641TMP	IP Camera
	HDW3549HP	IP Camera
Hikvision	DS-2CD2342WD	IP Camera
	DS-7608NI-I2 / 8P	NVR
Milesight	MS-C2975-PB	IP Camera
Uniview	IPC3635ER3-DUPZ	IP Camera
	IPC3615ER3-ADUPF40	IP Camera
	IPC322SR3-VSF28W-D	IP Camera
	NVR301-08-P8	NVR
Vivotek	VC8101	IP Camera
	MS8391	IP Camera
Dahua	NVR4108HS-8P-4KS2	NVR
Avigilon	ACC 7	Video Management Software
Nx	Witness / Meta 5.0	Video Management Software

Note: This list is subject to change as more NVRs/Cameras are tested and confirmed.

Please contact Permaconn to check if your devices are supported.

Appendix B – Special Video Service Event Codes

The following events codes are transmitted to the monitoring centres as part of the video service:

Event ID	Event Type	Partition	Zone	Description
306	E Only	0	967	Programming change to Permaconn Video service
356	E / R	0	967	Permaconn Video Service - Offline
688	E Only	0	970	Permaconn Video Data usage has reached 70%
688	E Only	0	980	Permaconn Video Data usage has reached 80%
688	E Only	0	995	Permaconn Video Data usage has reached 95%
688	E Only	0	999	Permaconn Video Data usage has reached 100%
720	E Only	Any	Any	Video Verification - Capture Successful – Check hyperlink
721	E Only	Any	Any	Video Verification - Capture Failed
722	E Only	Any	Any	Video Verification Swinger Shutdown. Maximum number of events has been triggered. VV rule will reset after swinger shutdown time has expired
723	E Only	Any	Any	Virtual Patrol - Capture Successful – Check hyperlink
724	E Only	Any	Any	Virtual Patrol - Capture Failed