Honeywell | THE FUTURE IS WHAT WE MAKE IT

MAXPRO®NVR 6.7

Installation and Configuration Guide

Installation & Configuration Guide

Revisions

Issue	Date	Description
1.0 Rev D	Mar, 2014	Updated document for 3.1 Build 65 Rev C
1.0 Rev E	Aug, 2014	Updated document for 3.1 SP1
2.0 Rev A	Aug, 2015	Updated document for 3.5
3.0 Rev A	August, 2016	Updated document for 4.0 Release
800-16419V4-A	Feb, 2017	Updated document for 4.1 Release
800-16419V5-A	August 2017	Updated document for 4.5 Release
800-16419V5-B	November 2017	Updated document for 4.7 Release
800-16419V5-C	February, 2018	Updated document for 4.9 Release
800-16419V5-D	June, 2018	Updated document for 5.0 Release
800-16419V5-E	September, 2018	Updated document for 5.0 T Patch Release
800-16419V5-F	October, 2018	Updated document for 5.0 SP1 Release
800-16419V5-G	February, 2019	Updated document for 5.5 Release
800-16419V5-J	May, 2019	Updated document for 5.6 Release
800-26013-A	November 2019	Updated document for 6.0 Release
800-26013-B	August 2020	Updated document for 6.3 Release
800-26013-C	February 2021	Updated document for 6.7 Release

TABLE OF CONTENTS

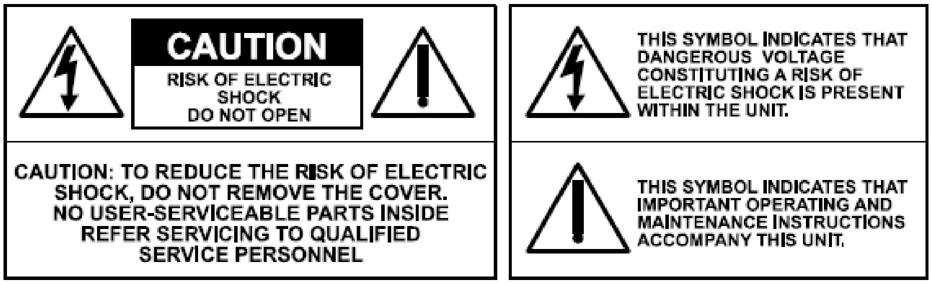
This page is intentionally left blank

LIST OF FIGURES

This page was intentionally left blank

PRECAUTIONS

Cautions and Warnings



CAUTION

RISK OF ELECTRIC SHOCK DO NOT OPEN

CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE THE COVER. NO USER-SERVICEABLE PARTS INSIDE REFER SERVICING TO QUALIFIED SERVICE PERSONNEL

THIS SYMBOL INDICATES THAT DANGEROUS VOLTAGE CONSTITUTING A RISK OF ELECTRIC SHOCK IS PRESENT WITHIN THE UNIT.

THIS SYMBOL INDICATES THAT IMPORTANT OPERATING AND MAINTENANCE INSTRUCTIONS ACCOMPANY THIS UNIT.

Installation and servicing should be performed only by qualified and experienced technicians to conform to all local codes and to maintain your warranty.

WEEE (Waste Electrical and Electronic Equipment). Correct disposal of this product (applicable in the European Union and other European countries with separate collection systems). This product should be disposed of, at the end of its useful life, as per applicable local laws, regulations, and procedures.

FCC Compliance Statement

Information to the User: This equipment has been tested and found to comply with the limits for a Class A digital device. Pursuant to Part 15 of the FCC Rules, these limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la Classe B est conforme à la norme NMB-003 du Canada.

Personal Data Storage

Please be aware that this product can store personal data.

Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner ("data subjects") rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the GDPR website of the EU: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Important Safeguards

1. Read Instructions

All the safety and operating instructions should be read before the appliance is operated.

2. Retain Instructions

The safety and operating instructions should be retained for future reference.

3. Cleaning

Unplug this equipment from the wall outlet before cleaning it. Do not use liquid aerosol cleaners. Use a damp soft cloth for cleaning.

4. Attachments

Never add any attachments and/or equipment without the approval of the manufacturer as such additions may result in the risk of fire, electric shock, or other personal injury.

5. Water and/or Moisture

Do not use this equipment near water or in contact with water.

6. Ventilation

Place this equipment only in an upright position. Ensure product ventilation openings are not obstructed.

7. Accessories

Do not place this equipment on an unstable cart, stand, or table. The equipment may fall, causing serious injury to a child or adult, and serious damage to the equipment. Wall or shelf mounting should follow the manufacturer's instructions, and should use a mounting kit approved by the manufacturer.

This equipment and cart combination should be moved with care. Quick stops, excessive force, and uneven surfaces may cause the equipment and cart combination to overturn.

8. Power Sources

This equipment should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power, please consult your equipment dealer or local power company.

9. Power Cords

Operator or installer must remove power, BNC, alarm, and other connections before moving the equipment.

10. Lightning

For added protection for this equipment during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet and disconnect the antenna or cable system. This will prevent damage to the equipment due to lightning and power-line surges.

11. Overloading

Do not overload wall outlets and extension cords to avoid the risk of fire or electric shock.

12. Objects and Liquids

Never push objects of any kind through openings of this equipment as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the equipment.

13. Servicing

Do not attempt to service this equipment yourself. Refer all servicing to qualified service personnel.

14. Damage Requiring Service

Unplug this equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:

- When the power-supply cord or the plug has been damaged
- If liquid is spilled or objects have fallen into the equipment
- If the equipment has been exposed to rain or water

- If the equipment does not operate normally by following the operating instructions, adjust only those controls that are covered by the operating instructions as an improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the equipment to its normal operation.
- If the equipment has been dropped or the cabinet damaged
- When the equipment exhibits a distinct change in performance-this indicates a need for service.

15. Replacement Parts

When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or that have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock, or other hazards.

16. Safety Check

Upon completion of any service or repairs to this equipment, ask the service technician to perform safety checks to determine that the equipment is in proper operating condition.

17. Field Installation

This installation should be made by a qualified service person and should conform to all local codes.

18. Correct Batteries

⚠ **Warning: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.**

19. Operating Temperature

An operating temperature range is specified so that the customer and installer may determine a suitable operating environment for the equipment.

20. Elevated Operating Ambient Temperature

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the specified operating temperature range.

21. Reduced Air Flow

Installation of the equipment in the rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.

22. Mechanical Loading

Mounting of the equipment in the rack should be such that a hazardous condition is not caused by uneven mechanical loading.

23. Circuit Overloading

Consideration should be given to connection of the equipment to supply circuit and the effect that overloading of circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

24. Reliable Earthing (Grounding)

Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Warranty and Service

Subject to the terms and conditions listed on the Product warranty, during the warranty period Honeywell will repair or replace, at its sole option, free of charge, any defective products returned prepaid.

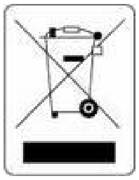
In the event you have a problem with any Honeywell product, please call Technical Support at 1-800-323-4576 (North America only) for assistance or to request a Return Merchandise Authorization (RMA) number.

Be sure to have the model number, serial number, and the nature of the problem available for the technical service representative.

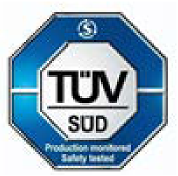
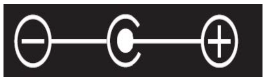
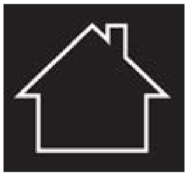
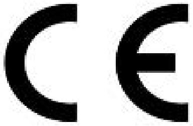
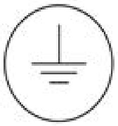
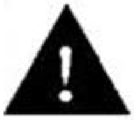
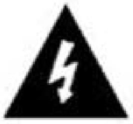
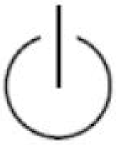
Prior authorization must be obtained for all returns, exchanges, or credits. Items shipped to Honeywell without a clearly identified Return Merchandise Authorization (RMA) number may be refused.

List of Symbols

The following is a list of symbols that might appear on the NVR.

Symbol	Explanation
	The WEEE symbol. This symbol indicates that when the end-user wishes to discard this product, it must be sent to separate collection facilities for recovery and recycling. By separating this product from other household-type waste, the volume of waste sent to incinerators or landfills will be reduced, and thus natural resources will be conserved.
	The UL compliance logo. This logo indicates that the product has been tested and is listed by the Underwriters Laboratories.
	The FCC compliance logo. This logo indicates that the product conforms to Federal Communication’s Commission compliance standards.

Symbol	Explanation
⎓	The direct current symbol. This symbol indicates that the power input/output for the product is direct current.
∼	The alternating current symbol. This symbol indicates that the power input/output for the product is alternating current.
♴ LDPE	The LDPE symbol. This symbol indicates that this product is made of Low-Density Polyethylene (LDPE).
DC12V −⊙+	The Direct Current symbol. This symbol indicates that the product operates from a 12 V direct current.
Pb Pb-Free	The Lead-free symbol. This symbol indicates that the product does not contain lead (Pb).
CCC S&E	The CCC compliance logo. This logo indicates that the product conforms with the China Compulsory Certification guidelines.
10	The Environment Friendly Use-period symbol. This symbol indicates the length of time that this electronic product can used without harming the environment.
✓	The RCM Compliance symbol. This symbol indicates that the product conforms with the Australian RCM guidelines.

Symbol	Explanation
	The TUV Lab symbol. This symbol indicates that the product has been safety tested by the TUV Lab.
	The Direct Current symbol. This Direct Current symbol indicates that the product operates direct current.
	This symbol indicates that the product is to be used indoors.
	The CE Compliance logo. This logo indicates that the product conforms to the relevant guidelines/standards for the European Union harmonization legislation.
	The Protective Earth symbol. This symbol indicates that the marked terminal is intended for connection to the protective earth/grounding conductor.
	This symbol is used to direct attention to important information.
	This symbol warns that the corresponding action could result in an electric shock.
	This symbol indicates On/Standby functionality of the corresponding control/button/ switch.

This page is intentionally left blank

CHAPTER

1 ABOUT THIS GUIDE

Overview

This guide describes the procedures and guidelines for installing, configuring and using the MAXPRO® NVR system.

Intended Audience

This document is intended for field and commissioning engineers.

Scope

This guide describes the installation and configuration procedures for both the MAXPRO NVR turnkey boxed solutions (MAXPRO NVR XE, SE, PE and MAXPRO NVR Hybrid XE, SE, PE models) and MAXPRO NVR software-only solution. This guide covers the following four major sections:

- Installing MAXPRO NVR
- Logging in and Familiarizing NVR
- Configuring MAXPRO NVR
- Upgrading MAXPRO NVR
- Configuring Web Client
- Installing and Configuring MAXPRO NVR Mobile App

Overview Of Contents

The following table describes the detailed structure and the contents of each chapter in this guide.

No	Chapter	Description
1	Introduction to MAXPRO NVR	Introduces the MAXPRO NVR system and types of Video surveillance solutions.
2	Commissioning MAXPRO NVR	Describes the commissioning procedures for the MAXPRO NVR system.
3	Setting up the MAXPRO NVR	Describes the tasks to set up the: • MAXPRO NVR Single Box solutions. • MAXPRO NVR Software-Only solution.
4	Installing the NVR Software	Describes the procedures to install the MAXPRO NVR software.
5	Logging on and Getting Started	Describes how to log on and gives an overview of the MAXPRO NVR.
6	Configuring MAXPRO NVR	Describes the tasks for configuring the MAXPRO NVR.
7	Verifying the Configuration	Describes the tasks to verify the MAXPRO NVR configuration.
8	Upgrade MAXPRO NVR Software	Describes how to upgrade MAXPRO NVR
9	MAXPRO NVR Web Client	Describes the procedures to install and configure the MAXPRO NVR Web Client.
10	MAXPRO NVR Mobile App	Describes the procedures to install and configure the MAXPRO NVR Mobile App.
12	Appendix A	Describes the procedures to customize MAXPRO NVR Single-box Turnkey solutions and setting up the Anti virus software on MAXPRO NVRs.
13	Appendix B	Describes the Image Stream Combinations and Device Characteristics of Oncam Grandeye Cameras, Configuring VMD Settings and Motion-based Recording, Event and Alarm Types and MAXPRO® NVRs - AXIS Camera/Encoders Discovery and Configuration (using ONVIF).
14	Patches Released on Top of NVR 4.0	Lists the various patches that are released on top of MAXPRO NVR 4.0. It also explains the enhancements that you can experience after installing the specific patch.

Related Documents

This document listed in the table serves as a necessary prerequisite for understanding MAXPRO NVR.

Document title	Part number	Description
MAXPRO NVR Operator's Guide	800-26014-C	This document is written for everyday MAXPRO NVR users who perform the basic video surveillance operations.

Typographical Conventions

This guide uses the following typographical conventions.

Font	What it represents	Example
Honeywell Sans Medium	Words or characters that you must type. The word "enter" is used if you must type text and then press the Enter or Return key.	Enter the **password**.
	Menu titles and other items you select	Double-click **Open** from the **File** menu.
	Buttons you click to perform actions	Click **Exit** to close the program.
Honeywell Cond Extrabold	Heading	Installation
Honeywell Sans Extrabold (Italic)	Cross-reference to external source	Refer to the ***MAXPRO® NVR Installation and Configuration Guide***.
Honeywell Sans (Italic)	Cross-reference within the guide	See *Installation*.

This page is intentionally left blank

CHAPTER

2 INTRODUCTION TO MAXPRO®NVR

Overview

Honeywell's MAXPRO® NVR line includes turnkey solutions—NVR (XE, SE, PE) with 8 to 64 channels and NVR Hybrid (XE, SE, PE) with 16 to 64 channels—and software solutions that range from 4 to 64 and 128 channels. It supports ONVIF Profile S and PSIA interoperability standards, RTSP, native integration for third-party cameras—including 360° camera support—and encoders from Honeywell, Axis and other manufacturers, making it a truly open system. MAXPRO NVR provides easy to use desktop clients, web clients and mobile apps. The advanced IP video capabilities make MAXPRO NVRs easy-to-install with 3-clicks* to live video and easy-to-use with features such as Video Surround, Calendar Search, SMART Motion Search and SMART VMD for every day security users as well as advanced video surveillance users.

* - With default settings and in a local area network for specific models.

MAXPRO NVR Turnkey Boxed Solutions

Honeywell's MAXPRO NVRs offer ideal solutions from entry to enterprise IP video surveillance systems. Supporting Honeywell's high definition (HD) cameras and broad integration with third-party IP cameras and encoders. The MAXPRO family of NVRs is a powerful HD IP recording and security monitoring system for a variety of applications. MAXPRO NVR comes pre-installed with the required software and pre-licensed with the required channels depending on the MAXPRO NVR model you purchase.

MAXPRO NVR Software Only Solution

Honeywell's MAXPRO NVR Software is a flexible, scalable and open IP video surveillance system. Supporting Honeywell's high definition (HD) cameras and broad integration with third party IP cameras and encoders, the MAXPRO NVR family is a powerful, high definition IP recording and security monitoring system for a variety of applications. MAXPRO NVR Software solution ensures flexibility for end-user IT departments when the choosing NVR hardware to deploy and end users will find it as easy as a simple DVR to configure and operate.

MAXPRO NVR Software is an open platform that supports broad third party device integrations with support for PSIA and ONVIF Profile S standards, real time streaming protocol (RTSP) standard and native device integrations. MAXPRO NVR provides easy-to-use desktop, web clients and mobile apps. MAXPRO NVR Software comes with all required software applications and a license for 4, 8, 16, 32, 64 or 128 channels while allowing for up to 128 cameras as your system grows. Minimum hardware specifications for different levels of recording and monitoring performance are provided for IT departments to choose the appropriate hardware platform for their system. This, along with quick and easy commissioning wizards for discovery and system configuration, makes installing HD IP systems quick and efficient without requiring any IP expertise. Simple and logical configuration pages make setup a breeze even for the novice installer. The following table describes the software solutions available.

MAXPRO NVR Family

The following table describes the various MAXPRO NVR Hybrid and MAXPRO NVR offerings that are available.

	 MAXPRO NVR Hybrid XE (Xpress Edition)	 **MAXPRO NVR Hybrid SE (Standard Edition)**	 **MAXPRO NVR Hybrid PE (Professional Edition)**	 **MAXPRO NVR XE (Xpress Edition)**	 **MAXPRO NVR SE (Standard Edition)**	 **MAXPRO NVR PE (Professional Edition)**	 **MAXPRO NVR Software**
Descriptio n	Simple, affordable NVR Hybrid	Flexible, scalable NVR Hybrid	Enterprise class NVR Hybrid	Simple, affordable NVR	Flexible, scalable NVR	Enterprise class NVR	Flexible, software only NVR
Channels	16 Analog or 16 IP	16 Analog and 48 IP or only 64 IP	16 Analog and 48 IP or only 64 IP	8 or 16	Up to 64	Up to 128	4, 8, 16, 32, 64 or 128
Maximum Frame Rate							Server hardware dependent- Minimum hardware specs recommended for various fps
at 4CIF/ VGA IP	480 fps (16 ch IP)	1920 fps (64 ch IP)	1920 fps (64 ch IP)	480 fps	1920 fps	1920 fps	
at 720p IP	480 fps (16 ch IP)	1920 fps (64 ch IP)	1920 fps (64 ch IP)	480 fps	1920 fps	1920 fps	
at 1080p IP (4 Mbps bitrate)	480 fps (16 ch IP)	1280 fps (64 ch IP)	1920 fps (64 ch IP)	480 fps	1280 fps	1920 fps	
at CIF or 4CIF/D1 Analog	480 fps CIF or 120 fps 4CIF/D1 (16 ch Analog)	480 fps CIF or 120 fps 4CIF/D1 (16 ch Analog)	480 fps CIF or 120 fps 4CIF/D1 (16 ch Analog)				
Storage	1 - 16 TB, internal fixed	1 - 24 TB removable bays	Up to 68 TB RAID 5/ 6, removable bays	1 - 12 TB internal fixed	1 - 48 TB, removable bays	Up to 68TB RAID 5/ 6, removable bays	Server hardware dependent
Form Factor	Desktop	Workstation/Server	Server	Desktop	Workstation/Server	Server	Server hardware dependent

Note: *The product options available in your region may vary, please contact your local Honeywell representative for more information.*

MAXPRO NVR Features

MAXPRO NVR (Turnkey NVR/Hybrid boxes - XE, SE, PE and Software only solution) offers the following key features that differentiate it from other IP video surveillance systems.

Mask Compliance Detection

Mask Compliance Detection feature detects the people who are with and without Masks in a given scene. This feature detects in a real time scenario and generates an event for People with/without mask. It helps in monitoring the people those who are violating the compliance of not wearing a mask in public places. This feature requires dedicated license to configure and use.

Social Distancing Violation Detection

Social Distancing Violation detection feature detects distance between two people and raises an alarm if the social distance norm is violated. This feature helps to ensure social distancing is followed in your premises. This feature requires dedicated license to configure and use.

Alarms for both Mask Detection and Social Distancing

Following are the list of alarms that are generated in NVR for Mask and Social Distancing detection features:

- Person Detected with Mask
- Person Detected without Mask
- Social Distancing Violation
- Non- Compliant Social Distancing Regions

Operating Conditions

There are various recommendation with respect to operating conditions for both Mask Detection and Social Distancing to give good results. It is recommended to refer these operating conditions before using these feature.

Non-Compliant Social Distancing Regions

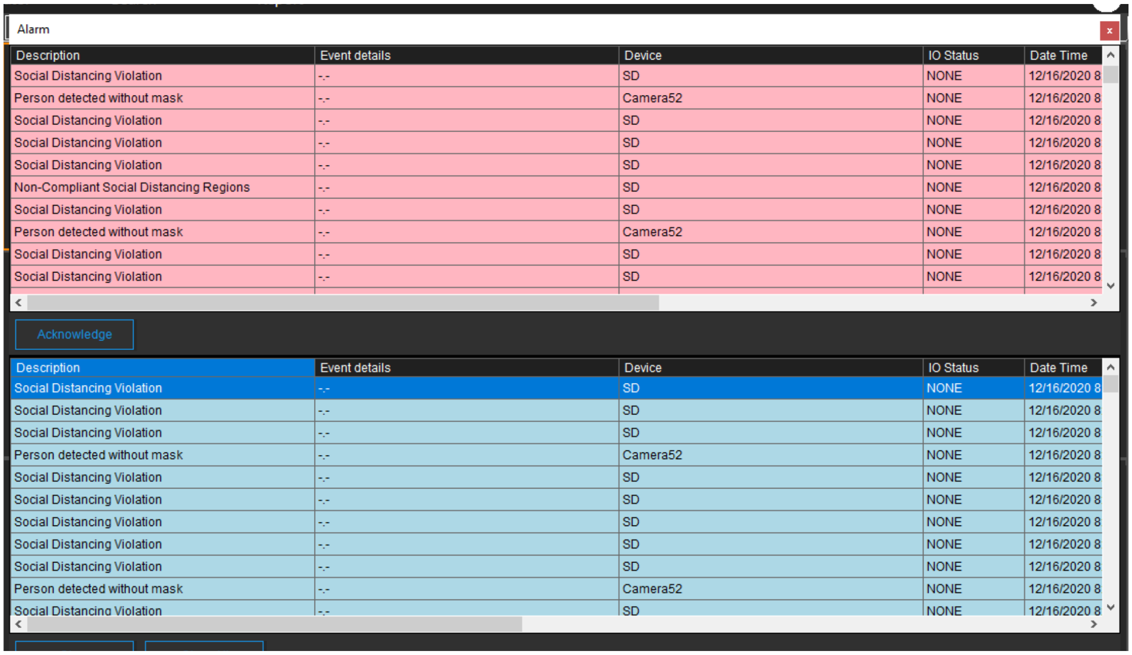
This feature helps user to identify the areas in which the sub regions/areas of camera views where the most number of Non-complaint social Distancing violations are happening.

In order to generate this alarm, user need to create at least one region. The system monitors the Social distancing violations and then monitors in to each region how many social distancing violations are occurred. The algorithm calculates the most violated regions and raises an alarm. This alarm is displayed in percentage of violation for a given time. This alarm is generated periodically every 5 hours (Configurable See Configuring Social Distancing ROI Duration and Show section). A maximum of 6 ROI's can be created.

Note: *User has to configure the Social Distancing first in order to configure this alarm.*

Analytic Alarms in NVR

The below screen displays the list of alarms that are generated in NVR for Mask Detection, Social Distancing violation and Non-Complaint Social Distancing Region features.



Alarm

Description	Event details	Device	IO Status	Date Time
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Person detected without mask	-.-	Camera52	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Non-Compliant Social Distancing Regions	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Person detected without mask	-.-	Camera52	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8

Description	Event details	Device	IO Status	Date Time
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Person detected without mask	-.-	Camera52	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8
Person detected without mask	-.-	Camera52	NONE	12/16/2020 8
Social Distancing Violation	-.-	SD	NONE	12/16/2020 8

Scalable Analytics Server

This feature is introduced to manage the load on a NVR box while rendering analytics based cameras. Earlier only one local analytics server was available for multiple cameras that support analytics. This results in high consumption of CPU and low rendering capability of live video in NVR cameras.

Scalability feature helps customer to share the analytics server load on different remote machines and utilize the analytic algorithms efficiently. User can map the required cameras to each remote server and view the alarms in VMS,

A new tab named Analytics Server is introduced under Configurator tab to add additional analytics server and to choose the one while configuring Social Distancing, Mask compliance and SVMD features. This provides flexibility and increases the processing time to manage the load over analytics server when configuring multiple features.

- A maximum of 5 Analytics Remote boxes can be added under this tab.
- For each Analytics Remote box, 4 camera with 30 FPS and up to 8 cameras with 5 FPS can be assigned

Bulk configurations of cameras from NVR

This feature allows you to perform Bulk camera configuration for main and sub stream's, to ease the effort of configuring multiple cameras at the customer site. This feature improves the productivity for dealers and system integrators while configuring many NVRs. The configuration of cameras from the NVR is done one by one today (either post discovery or manual addition). This leads to higher lead time to configure and setup customer sites.

You can perform the following using Bulk configuration screen:

- General Settings
- Schedule Settings
- Preference Settings
- Stream Settings including child stream configurations specific to camera model
- SVMD Configuration

Bi-Directional Audio Support for MAXPRO NVR

This feature helps an operator to send Bi-directional audio warnings/messages to any audio output of cameras from MAXPRO VMS machines. Currently Mic and speech is supported from VMS viewer only.

This feature supports standard audio Codec format G.711 ulaw and only Honeywell ONVIF Camera model are supported.

Only Honeywell ONVIF Camera models are supported.
Only fixed G.711 ulaw Codec format is supported.
Mutlistream is supported, but can be enabled in only one stream at a time.
It is recommended for the user to enable and speak for one camera at a time.

Series 60 Camera Integration

MAXPRO VMS R670 supports Series 60 Camera integration with MAXPRO NVR 6.7 recorder. The following tables explain the list of supported camera models, and events/alarms supported.

Type	Camera Models	Firmware Details
Premium Model	HC60W35R2	Honeywell_60-Series_IPC_HC60WXXRX_V1.0.21.20200828
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	
Series60 IR PTZ	HC60WZ5R30	
Series30	HC30W25R3-12V	

Support for Ex-Proof Camera models

MAXPRO NVR 6.7 supports Ex-Proof Camera integration. The following tables explain the list of supported camera models, Codec and Resolutions supported.

Camera Models	Codec & FPS Supported	Resolutions Supported
HEIPTZ-2201W-IR	H264, H265, MPEG FPS: 50 for PAL FPS: 50 for NTSC	1920 x 1080, 1280 x 960, 1280 x 720, 704 x 576, 640 x 480, 352 x 288
HEICC-2301T	H264, H265, MPEG FPS: 50 for PAL FPS: 60 for NTSC	1920 x 1080, 1280 x 960, 1280 x 720, 704 x 480, 640 x 480, 352 x 240

Enhancements in FishEye camera Dewarping Support

This enhancement for FishEye camera allows you to view/perform the following

- When one of the Quad-view column display 360º view then the user can select a designated location to display for the rest of the 3 columns.
- Allow PTZ function during live-view and playback.
- Enable PTZ operation on Quad-view setting & Dewarped image.
- Oncam GPU rendering support

This improvement is supported only to the following camera models:

- HC12-IEC1-O: C-12 Indoor Camera
- HC12-OPC1-O: C-12 Outdoor Plus Camera

Refer to the MAXPRO NVR 6.7 Operator Guide on how to configure and use this feature

Mask Compliance Detection

Mask Compliance Detection feature detects the people who are with and without Masks in a given scene. This feature detects in a real time scenario and generates an event for People with/without mask. It helps in monitoring the people those who are violating the compliance of not wearing a mask in public places. This feature requires dedicated license to configure and use. Refer to the MAXPRO NVR 6.7 Operators Guide on how to configure and use this feature.

Social Distancing Violation Detection

Social Distancing Violation detection feature detects distance between two people and raises an alarm if the social distance norm is violated. This feature helps to ensure social distancing is followed in your premises. This feature requires dedicated license to configure and use. Refer to the MAXPRO NVR 6.7 Operators Guide on how to configure and use this feature

Alarms for both Mask Detection and Social Distancing

Following are the list of alarms that are generated in NVR for Mask and Social Distancing detection features:

- Person Detected with Mask
- Person Detected without Mask
- Social Distancing Violation

Operating Conditions

There are various recommendation with respect to operating conditions for both Mask Detection and Social Distancing to give good results. It is recommended to refer these operating conditions before using these feature.

Recommended Operating Conditions For Mask Detection

Mask Detection algorithm is developed to detect people who are with and without Masks in live video.

This section provides recommended specifications that can provide good or better mask detection accuracies.

Recommended Operating Conditions

Parameter	Specification
Camera height from the ground	8 – 10 feet

Camera field of view and orientation/tilt	Mounting should be suitable to obtain frontal face images. H-FOV should not more than 60 degrees. Ceiling mounted or overhead mounted cameras which have near vertical view of faces looking down is not recommended for the application. Bright light in the background or sunlight which results in poor image quality of face in not recommended. Wide angle camera with long field of view is not recommended.
Image quality	Full HD 2M pixel camera video streams with high bitrate (5 to 8 Mbps for 30fps) with no blur and good focus. For 3MP cameras the recommended bit rate 10 to 15 Mbps. Good quality video encoding should be used (H.264/H.265)
Illumination	100-150 lux (uniform illumination on both sides of face)
Face pose for MD	Frontal pose can have +/-45 deg variation
Detection Distances	Maximum distance from camera 15 feet along the ground. Highly preferred that people enter into the field of view from distances not more than 15 feet and there is no clutter or moving objects (prefer a static background such a wall so that false detections are avoided)

Configuration parameters:

Parameter	**Specification**
Minimum Size of the face with Mask	50 x 50 Pixels
Minimum Confidence level recommended	50%

Note: *To avoid false alarm please follow the operating condition and keep the confidant level more the 80%.*

Recommended Operating Conditions For Distancing Violation detection

This section provides specifications of the conditions that can provide a good or better social distancing solution with respect to camera placement and operating conditions requirements.

Required operating conditions can be divided in two sections as explained:

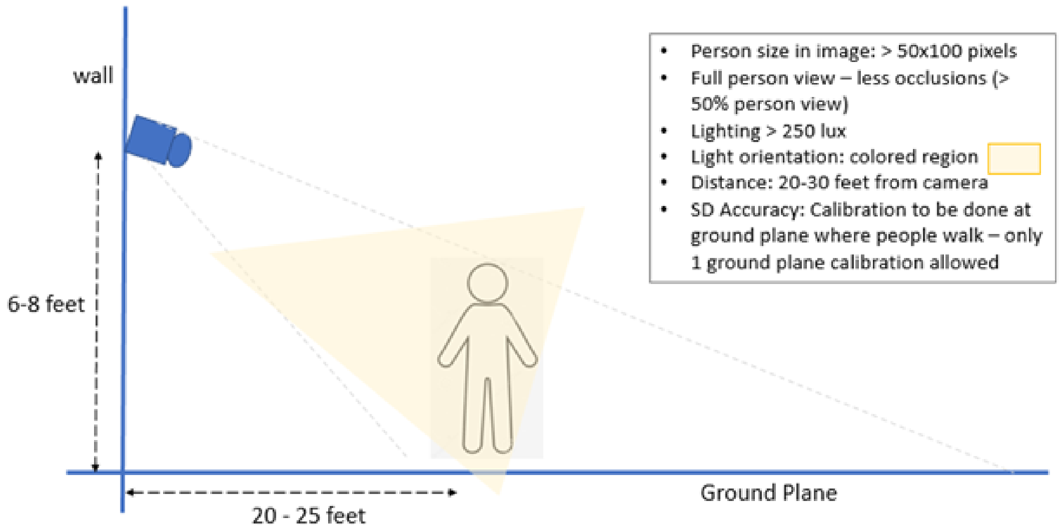
- Conditions for person detection
- Conditions for calibration selection of ground plane.

Person Detection Conditions

Below figures explains different preferred camera placements and conditions for person detection. It is to be noted that the numbers given in the figures are approximate and can vary:

Placement 1: Normal Perspective View

Placement 1: Normal Perspective View



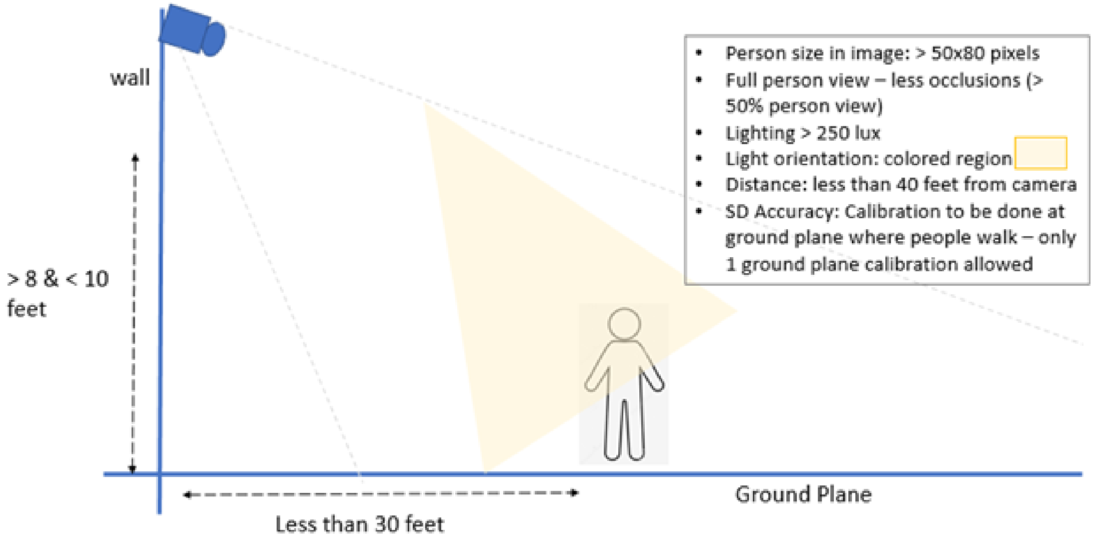
- Person size in image: > 50x100 pixels
- Full person view – less occlusions (> 50% person view)
- Lighting > 250 lux
- Light orientation: colored region
- Distance: 20-30 feet from camera
- SD Accuracy: Calibration to be done at ground plane where people walk – only 1 ground plane calibration allowed

This placement explains that the person recognition can be good till around 30 feet, when the camera placement is < 8 feet (given that average height of person is between 5-6 feet), and when the person is at approximately 20-30 feet from the camera. Also, lighting should be > 250 lux and the light should be falling on the person with no back lighting for better accuracies.

Placement 2: Camera at a higher height or ceiling height

This placement explains the configuration wherein the camera is placed at a much higher height than the person.

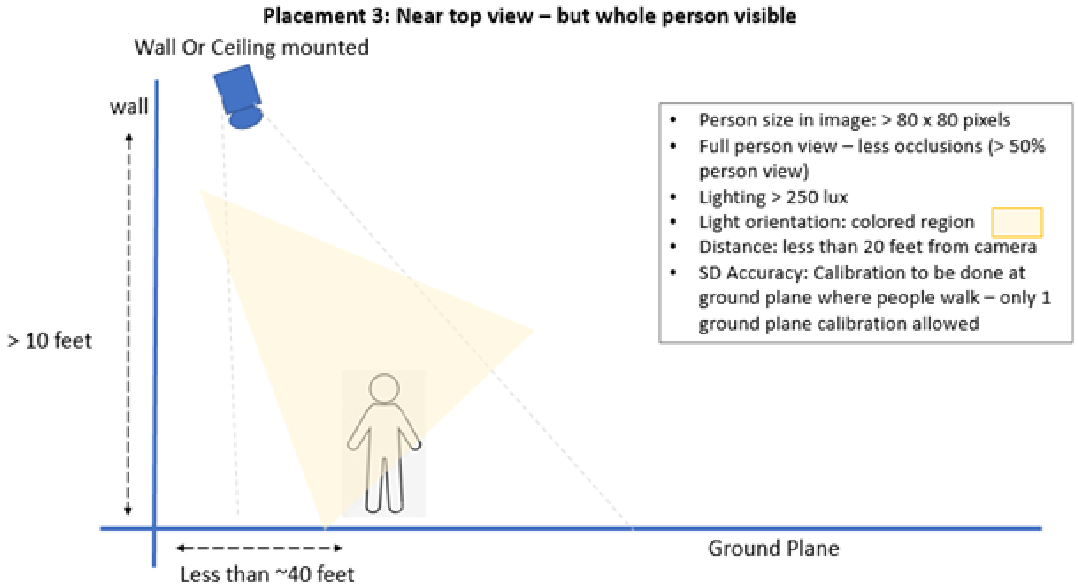
Placement2: Camera Placed at higher heights and looking sharply down to the ground plane



- Person size in image: > 50x80 pixels
- Full person view – less occlusions (> 50% person view)
- Lighting > 250 lux
- Light orientation: colored region
- Distance: less than 40 feet from camera
- SD Accuracy: Calibration to be done at ground plane where people walk – only 1 ground plane calibration allowed

If the camera height is as shown in the above figure, the FR accuracies can be reduced with distance. But at lesser distances from camera (<10-12 feet), FR can be accurate enough. Again, adequate amount of light falling on the face for good features is an important requirement.

Placement 3: Camera at higher height from the ground


Placement 3: Near top view – but whole person visible
Wall Or Ceiling mounted
wall
> 10 feet
Less than ~40 feet
Ground Plane
Person size in image: > 80 x 80 pixels
Full person view – less occlusions (> 50% person view)
Lighting > 250 lux
Light orientation: colored region
Distance: less than 20 feet from camera
SD Accuracy: Calibration to be done at ground plane where people walk – only 1 ground plane calibration allowed

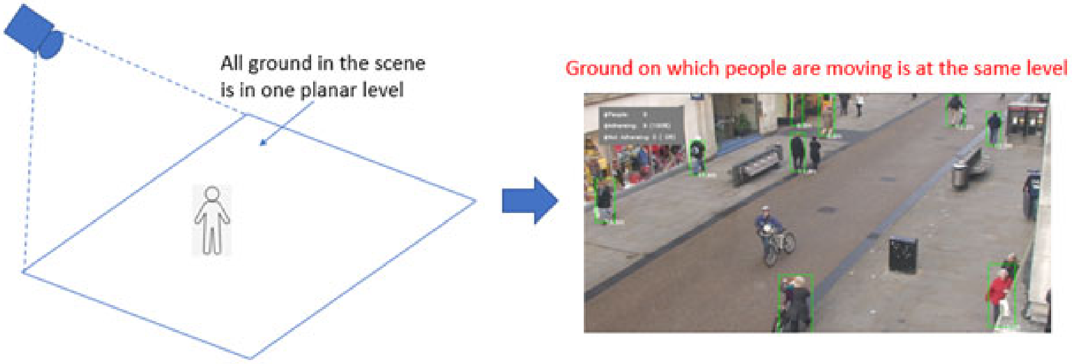
In this placement the camera height is nearly overhead, the person detection model is not tested when there is just head and shoulders view in the video stream. It is recommended that silhouette of the person is seen.

Calibration Conditions

Calibration is the most important step for distance measurement between two people. The primary requirement of this step is that the ground plane on which distances between people are measured and the ground plane that is calibrated should be the same. Details of this statement in form of figures are given in this section.

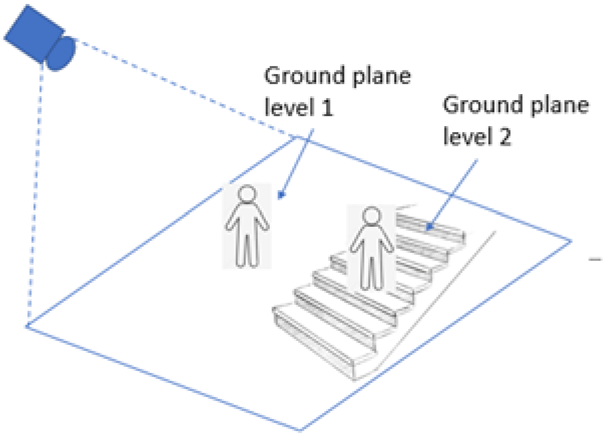
Condition 1: Camera Perspective View with one ground plane

This condition details the meaning of ground plane being at the same level. The level of the ground where people are moving and the measurement for social distancing should be one planar level. This is the most important requirement for accuracies of calibration. The configuration is done on Ground Plane Level 1 and Social distancing output will be done on this plane only. Stairs are not counted for the solution.


All ground in the scene is in one planar level
Ground on which people are moving is at the same level

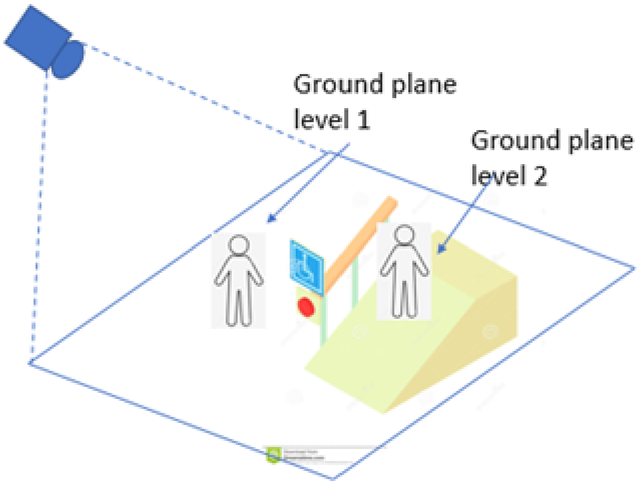
Condition 2: Multiple ground planes

This conditions gives the sketch wherein there are people moving on the pathway (one ground plane level) and a staircase too. The staircase is of different ground plane level when compared to the pathway ground nearby. Hence the current solution calibration can be done on the pathway and NOT on the stairs. Our solution will not address output for people on the stairs



Condition 3: Multiple Ground Planes with slope as the second plane

This condition explains a sketch wherein the stairs in Condition 2 is replaced by a slope. Even in this situation, our solution will not give correct results on the slope. The calibration needs to be done on Ground Plane 1 and results also will be for ground plane 1.



Note: *In registry there is an option to change at what distance Social Distancing alarm should be generated. For example: 4 ft, 10 ft.*

Support for Remote Analytics Server

MAXPRO R670 release support for Remote analytics Server configuration for Mask, Social Distancing and SVMD on i8700 & 9700 Machines. This configuration is required if the existing systems are not capable to take up the load of Analytics and to avoid overshoot of system resources memory. See Configuring Remote Analytics Server section for more information.

Note: *Analytics server is supported only on Windows 10 OS platform.*

Series 60 Camera Integration

MAXPRO VMS R630 supports Series 60 Camera integration with MAXPRO NVR 6.7 recorder. The following tables explain the list of supported camera models, and events/alarms supported.

Type	Camera Models	Firmware Details

Premium Model	HC60W35R2	Honeywell_60-Series_IPC_HC60WXXRX_V1.0.21.20200828
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	

Supported Events/Alarms

Series 60 Camera models support the following events/alarms:

Event
Tampering
Image too bright
Image too dark
Image too blur event
Motion Detection
Intrusion Detection
Loitering Detection
Line crossing Detection
Unattended Object Detection
Missing Object Detection
Face Detection

Supported key Features

- HTTPS integration: The camera supports complete HTTPS protocol while integrating with NVR.
- Smart Stream III
  - Smart Codec
  - Smart FPS
  - Dynamic intra Frame Period (DIF)
- Alarms
- Profile S compliant
- Multicast
- Edge Sync Recording Support
- Full Encrypted Communication (including Encrypted Profile G communication)

Thermal Camera Integration - HRCF-FD384H/HRCF-FD640H

MAXPRO R630 supports integration of Silent Sentinel and Thermal Cameras. Following are the cameras and firmware details:

Type	Camera Model	Firmware Details
Silent Sentinel	HRCF-FD640H	V4 : v1.0.1D20200603
	HRCF-FD384H	
Thermal Camera	HVCT-B4010I	V5.5.26 build 200514
	HVCT-B4020I	
	HVCT-D4010I	

Refer the MAXPRO integration with MODUM Technical Notes for detailed information on the how to integrate the HRCF-FD384H/HRCF-FD640H Thermal cameras with MAXPRO NVR.

SSA - Software Service Agreement for MAXPRO

Software Service Agreement (SSA) is a flexible version specific licensing process which allows a user to get the support on the MAXPRO VMS licenses across multiple versions. From 6.0 release user need to buy a valid license to upgrade or for fresh installation. In addition user can buy SSA support license for a specific duration which helps to get support from Honeywell.

Please contact Honeywell Customer support. See the back cover for the contact information in respective regions.Licensing changes for Software Service Agreement.

NDAA Series 30 camera Integration in MAXPRO NVR & VMS

Series 30 Camera integration is supported in 6.0 release with MAXPRO NVR recorder. The following tables explain the list of supported camera models, firmware version and events.

Note: *FishEye camera does not support HTTPS.*

#	Camera Models	Firmware Details
1	HC30W42R3	v1.0.18.20190523 Note: If a camera has older firmware, please upgrade to the above firmware version and perform factory default once.
2	HC30W45R3	
3	HC30W45R2	
4	HC30WB2R1	
5	HC30WB5R1	
6	HC30WB5R2	
7	HC30WE2R3	
8	HC30WE5R3	
9	HC30WE5R2	
10	HC30WF5R1	

Supported Events

Series 30 Camera models support the following events:

Event
Motion Detection
Tamper
Image too blur
Image too dark
Image too bright
People Detection
Intrusion

Supported key Features

- Smart Stream III
  - Smart Codec
  - Smart FPS
  - Dynamic intra Frame Period (DIF)
- HTTPS
- Alarms
- Profile S compliant

- Multicast

MPEG2 Encoder Support with MAXPRO NVR and VMS

NVR 6.0 supports legacy MPEG2 Encoders with Live and playback, Alarms and VMS in VMS functionalities. The following encoders are supported.

- ENC8M2
- VE8M2

Supported Firmware Version: 1.2.261

Additional Cameras Support

In addition to above HC Series 30 cameras, NVR 6.0 supports the below camera models:

- H4W8GR4IN
- H4W8GR1IN

Supported Codec Formats: H.265, H.264, H.264H, H.264B, MJPEG.

Additional Resolution Support

For HFD6GR1 model camera, following additional resolutions are supported:

- 2432 x 1216
- 1920 x 1080
- 960 x 480
- 640 x 320
- 512 x 256

Video Guard service for SIRA compliance

MAXPRO NVR 6.0 release supports SIRA compliance with Video Guard Agent. This is to meet the specifications defined as part of the City wide Surveillance initiative by the Security Industry Regulatory Agency (SIRA) of Dubai, UAE, and being adopted across Middle-East countries.

New Features in NVR 5.6

Support for Equip series V2 Cameras

The following is the list of Equip Series V2 camera integration is supported in MAXPRO VMS:

Note: *Recommended to use NVR 5.6 and above to connect to the below camera firmware.*

#	Camera Model	Type
1	H2W2GR1	WDR cameras
2	H3W2GR1V	
3	H3W4GR1V	
4	H4W2GR1V	
5	H4W4GR1V	
6	HBW2GR1V	
7	HBW2GR3V	
8	HBW4GR1V	
9	HCW2GV	
10	H4L2GR1V	Ultra Low Light
11	HCL2GV	
12	HBL2GR1V	

The below table details the Firmware version compatible with the NVR 5.6 Build 572:

Camera Model	Firmware	Web Version	Onvif Version	ISOM Version	Xtralis Intrusion	Xtralis Loitering	Intrusion Detection	Loitering Detection	Trigger Line Detection
Equip S Series V2 Firmware version					VA Packages				
Ultra Low Light	1.00000000.18, 2019-04-23 Or above.	3.2.1.722805	16.1.2	1.3.1, 2019-04-21	1.01.19	1.01.19	1.0.8, 2019-01-15	1.0.8, 2019-01-15	1.0.8 2019-01-15
WDR cameras	1.00000000.18, 2019-04-09 Or above.	3.2.1.716054	16.12	1.3.1, 2019-04-04					

The above Equip S Series V2 Firmware version supports the following features:

- New VA events added with Annotation support
  - Xtralis IntrusionTrace™
  - Xtralis LoiterTrace™

- Intrusion Detection
- Loitering Detection
- Trigger Line Detection

Note: *Annotation feature is supported only with Xtralis XO package.*

- Profile -G Edge Sync recording
- Mulitcast

Support for HRHQ104 DVR

NVR 5.6 supports HRHQ104/108/116 DVR (V1.00.00HW001.1.190422) as 4/8/16ch encoders

Support for smooth Rendering at VMS

NVR 5.6 Build 570 installation is mandatory for smooth reverse playback in MAX-PRO VMS.

New Features in NVR 5.5

Analytics Annotations Support

Camera built in Annotations feature helps to trace and locate the moving subjects in live/recorded video and generates an alarm if intrusion or loitering is detected. After this feature is enabled in NVR, subjects in video when found in Region Of Interest, is bounded by rectangle box and on alarm conditions, it will be signified with a change in color of bounding box.

Annotation support for Intrusion Trace and Loiter Trace in Live and Playback video is supported with only Equip-S Series specific cameras

See Annotations section on how to configure this feature.

Enhancements in Video connection

Improvements in video connection from Viewer.

New features in NVR 5.0

Patches Merged in SP1

5.0 T Patch

- Refer to the 800-22559V1-E_MAXPRO NVR_5.0_T Patch_Whats_New_Release_Notes for complete information on new features in 5.0 T Patch.

Windows Expiry Patch

This patch is to make MAXPRO VMS application not to apply password expiry option for windows users. Refer to the MAXPRO® VMS_ Windows Expiry_Patch_Release Notes for detailed information.

Archival Improvements

Include Archived Clips

This feature allows user to search Archived clips including the recording clips. User needs to select Include Archived Clips check box under Filter area while searching for recorded clips. Based on the search criteria the archived clips are displayed in Grey color. When user drag and drop the archived clips in to the panel then camera name and clips status as REC is displayed. Refer to the *MAXPRO® NVR Operator Guide* for complete details on how to search for Archived clips.

Note: *If user selects Include archived clip check box and then search for archived clips, it displays only auto archived clips. It will not display the manually archived clips.*

Primary and Archived Location

The Archived clips in the Result window also displays the location of Archived clip as explained below.

- Archived: The clip is available in Archived path
- Primary, Archived: The clips is available in both primary storage and Archived path

Camera Name & Clip status

In Viewer screen following are the improvements:

- Under Snapshots/clips, the folder naming structure is changed to camera name.
- When a user drag and drops a archived clip into panel, the archival camera name with clip status Rec is displayed.
- If Archived clips are played in MAXPRO clip player then the camera name and clip status is also displayed.

Archival Schedule Check box

Ensure Clip scheduled for archival are not deleted until archived check box is introduced in System tab > Archival Schedule to ensure that clips will not be deleted by the system until it is archived. The following are the benefits if user selects this check box.

- If the clip deletion schedule is reached for a specific clip then this feature will retry and archive the clip.

This check box settings is applicable for the following:

- Integrity services
- Neo Deletion Scheduled
- Disk Space Full
- Distress deletion

Archival Clip and Deletion Retry

This feature is introduced to allow user to configure the Archival and Deletion retry settings in the config file available in bin folder. For any reason if the archival drive disconnects then based on the config file settings the:

- Archival clip retry feature will help to get the pending archival clips.
- Deletion clip retry feature will retry the process and deletes the clips.

The default value for retry process is set to 4. User can set the required number for archival and deletion retry process.

See How to configure the Archival and Deletion retry settings section on how to set the retry process.

Validation Message For Network Credentials

If user adds a Network Drive for Archival without Domain, Username and Password then a validation message is displayed to provide the network credentials.

Disabled Password Never Expires

In User tab, if IS Windows user check box is selected then the Password Never Expire check box is disabled and it cannot be cleared. This ensures that for a Windows user the password will never expiries.

Playing archived clips through Client machine

User was unable to access and play the archived clips from NVR server machine. If user drag and drops the archived clips into the viewer then an error message is displayed.

User needs to have the privileges to access the archived clips from remote NVR clients. Refer to the See Playing archived clips through Client machine for complete details of the possible combinations to play the archived clips from client machine.

See Different Scenarios to playback Archived Clip section to playback Archived clips.

Improved GPU rendering

GPU Rendering capability is now enhanced to handle the camera video packets along with decompression technique. User can view smooth and clear live video through GPU rendering. User should modify the registry value in client or server machine to enable GPU rendering mode. See Improved GPU Rendering section on page 242 for more information.

GPU Rendering Combinations

The below table explains the combination settings between Enabling GPU Rendering option in Preference tab and Registry settings.

IF	And If	Then
User enables Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 1	Both Decompression and Rendering will be processed through in GPU mode.
User enables Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 0	Decompression process will happen through GPU and Rendering will be processed in CPU mode.
user does not select Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 1	Both decompression and Rendering will be processed through CPU.

60FPS support for EQUIP-S 1080P cameras

EQUIP-S 1080 P Model cameras are now supported with 60FPS rendering through GPU Rendering Mode. The following are the list of cameras support 60 FPS.

Note: *Cameras beyond 1080 resolution will not support 60 FPS rendering.*

- H4L2GR1V
- HBL2GR1V
- HCL2GV
- H4W2GR1V
- HBW2GR1V
- HBW2GR3V
- H3W2GR1V
- HCW2GV
- H2W2GR1

NAS Recording support

Network Attached Storage (NAS) external drive is now supported for recording video clips along with other drives in MAXPRO NVR. This helps user to extend the storage capacity to save the recordings. User needs to configure the directory and user permission in respective NAS web page to use this feature. See Guidelines to configure NAS Drive for Recording section on page 245 for complete information

Note: *If customer is using Infotrend NAS then they have to create the user inside the NAS box. The username could be NVR-Admin or Administrator.*

Video Anonymization

This feature allows user to configure or mask identifiable objects based on the scene environment. It provides flexibility to choose and configure the required camera based on the mounting position. User need to select the required Environment from the Stream Preferences Settings based on the camera mounting position. The following are the options supported. See Video Anonymization section on page 239 for more information on how to configure based on scene environment.

- Variable Scene: If the scene contains both stationary and moving people or objects then select this option to anonymize the objects in the scene.
- High Motion Scene: To anonymize the objects in high motion in the scene.
- Still Scene: To anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

Installation

- NVR 5.0 Installation is supported for Windows 2016 OS (Server).

Introduced the following new services

- TrinityIntegrity Service: A service that runs in background and ensures all the system data is synchronized. As part of 5.0 release it includes features such as Delete Orphan Data and Drive Feature. See Integrity Service Settings section for more information.
- Trinityupdate Service: A service introduced to scale recording capacity on demand and to enable necessary steps required for additional recording services.
- NeoStorageserver3 and NeoStorageserver4: These services are to support 128 channels in a system and starts automatically after a user crosses 64 and 96 channels respectively. These services will stop when user deletes the cameras and the count goes less than <64 and <97 respectively.

Support for 128 Channel

Additional 64 channels are provided with the existing 64 channels, resulting in a total of 128 channels in NVR Software and PE RAID System. User needs to buy license for the additional channels. If only Encoders are added in the system then without additional license user can add up to 128 Channels. However, adding additional channels depends on the type of encoder.

Privacy Protection Settings (GDPR)

Anonymization Support

Anonymization feature is to help the business owner to meet the EU GDPR compliance standards easily. The objective of this feature is to hide the identifiable personal data or personal identity in a video surveillance system using masking techniques. This feature is specific to European Union region and valid license is required to enable this feature.

Anonymization at NVR level can be set in Configurator > Systems tab and only an Administrator can use this feature and grant access in User tab. This feature can also be enabled at camera level under Stream >Preferences tab. EquIP Series cameras are supported by this feature.

To mask the identifiable objects based on the scene environment, see How to Anonymize objects based on Environment section on page 240 for more information.

The Anonymization feature supports two types of masking:

- Blur: Blurs the region
- Pixelize: Pixelizes the region

Four Eye Authentication Support

This feature is also part of Privacy Protection setting and to meet the EU GDPR compliance standards easily. This feature is to restrict all users in a surveillance system to perform Playback operation. While performing playback operation at least two people from different roles should authenticate. For an Administrator, user authentication is not required and can do any playback operation. For an operator user, a popup is displayed and an Administrator user or any other User with different role needs to authenticate to perform playback operation.

In MAXPRO NVR, a check box is introduced to enable this feature in Systems tab. By default this check box is not selected. User need to obtain valid license to enable this feature.

The following table explains the Four Eye Authentication based on the user and roles

User	Authenticating User	Valid Authentication
Operator	Administrator Or any other user with different role	Yes

Operator	Operator	No
Operator	Operator 2	Yes

Clip Export with Anonymization support

Anonymization feature is supported for both Playback and Clip Export operation.

Note: *If a user exports a clip with Anonymization using Clip Export option then only WMV format is supported.*

Password Complexity and Expiry Enhancements

The following are the enhancements:

- Improved change of password security by introducing complexity requirements. The following are the password requirements.
- The password should have a minimum length of 12 characters.
- The password should consist of at least one number, one uppercase letter and one special character
- If user changes the password, it will expire for every 90 days. Earlier it was no expiry
- If user wants to set the password which should never expire then navigate to Configurator > Users tab. Select the Password Never Expire check box for the specific user.
- User is notified with the message Your Password will expire in no.of days on the top right corner of the screen.
- If Admin password is expired then the administrator can use the Change Password feature in NVR log in screen to create a new one.

Note: *Only administrator will have access to user screen and can change the password for operator. Operator should contact administrator for changing the password and settings.*

In Upgrade Scenario

If user upgrades to NVR 5.0 then the password complexity requirements will be applicable.

In Fresh Installation Scenario

In case of Fresh Installation, the following are the recommendations:

- Only default username is displayed and the password field will be blank
- User must create new password
- In Create New Password dialog box, leave the Old Password field blanks and proceed.

UI Improvements

For better user experience and accessibility the following features are rearranged in Systems tab

- Archival Schedule
- In camera level added after 30 minutes (s) as a new entry.
- Edge Sync Settings
- Privacy Protection Settings

Improvements in Status Monitor

- Additional status message Database Connection lost is included. This will help user to know the status of database connection.
- Color Indications:
- Green: Everything is Fine
- Blinking between Yellow and Green: Not Recording
- Blinking between Yellow and Red: Database Connection Lost

System and Performance Improvements

- There is no Metadata from 5.0 Release onwards.
- No separate drive is required for Metadata
- New Recording file system with no Index files except PassIndex is introduced and it is for per camera and per drive.
- Plug-in a new recording drive which can have recordings of another 5.0 NVR, and play the same recordings by adding the same Unique Number of the camera.
- Supports backward compatibility (5.0 version can play till 4.9 version recordings (With Metadata) including 5.0 recordings). No recording loss in user’s perspective.
- Recording, Retrieval and Recycle features will have no dependency on index files.
- PassIndex only use as catalyst
- New naming convention for Segment files (Num_StartTime_EndTime)
- Access recordings directly from recording drive
- Each recording drive is self sufficient
- XML Corruption recovery
- Auto recovery of corrupted XMLs by NEO on the run
- No functionality loss

Integrity Service Settings

This is a new a service that runs in background and ensure all system data to be synchronized. Following are the features this service provides as part of 5.0 release.

Step 1. Delete Orphan Data: In this feature, system will find and clean up orphan clips from file system or DB. Orphan data will be identified based on camera configured deletion settings.

Step 2. Drive Feature: In this feature, Drive Full Scan is performed until a new fixed drive is detected in NVR system. Based on the scan result, data sync up or orphan data clean up process is initiated using the current camera configuration or if the camera is not found then, by default the data after 30 days will be deleted.

For Example: If NVR 1 is down due to some technical issues, then the hard disk of NVR 1 can be used in NVR2. NVR2 initiates the scan, detects the drives and displays the recordings of NVR 1.

- Running on schedule base is same as windows scheduler.
- Has capability to process deleted camera's data for Orphan deletion.

Step 3. Schedule of when to start the service can be configured.

Step 4. Allows Neo to recycle data first (since by default it deletes clips with retention period + 24 hours)

New EquIP 1080p and 4MP Camera Integration

Step 1. Configuration is done through Honeywell proprietary ISOM APIs

Step 2. After integrating the new EquIP Camera, system will be able to perform the following

- H.264, H.265 and MJPEG coded support
- HTTPS support

Step 3. New events supported: With the EquIP series camera integration the following events are generated.

- Abandoned Object detection
- Object Missing detected
- Trigger Line detection

The following EquIP series Camera models are supported using ISOM API's

#	Camera Model	Description	Firmware Details
1	H4L2GR1V	2MP Lowlight outdoor dome	Version: 1.000.0000.10, Build Date: 2018-05-29 ISOM Version 1.2.1_Build 20180529 VA Package Version: 1.0.8_build20180529
2	HBL2GR1V	2MP Lowlight IR bullet	
3	HCL2GV	2MP Lowlight box camera	

#	Camera Model	Description	Firmware Details
4	H4W2GR1V	2MP WDR outdoor dome	Version: 1.000.0000.9, Build Date: 2018-05-25 ISOM Version: V 1.2.1_Build 20180524
5	H4W4GR1V	4MP WDR outdoor dome	
6	HBW2GR1V	2MP WDR bullet, 2.7-13.5mm	
7	HBW2GR3V	2MP WDR bullet, 5-60mm	
8	H3W2GR1V	2MP WDR indoor dome	
9	H3W4GR1V	4MP WDR indoor dome	
10	HCW2GV	2MP WDR box camera	
11	H2W2GR1	2MP Pancake camera	

RTSP H.265 Support

- Any H.265 URL can be added and streamed with Generic-RTSP streamer name.

Enhancements in MAXPRO Mobile APP

- Introduced new Mobile app versions
- For Andriod: 1.3.0 (100030004)
- For IOS: 1.3.0 (100030001)
- New Supported OS: minSDKVersion = 21
- Finger Print Authentication is supported for Android version of MAXPRO Mobile app. However, this feature is available on Fingerprint supported devices.

Limitation with Privacy Protection Settings

- If Anonymization is enabled in NVR application, then user will not be able to see the video in MAXPRO mobile app/Web client. An error message is displayed.
- If Four Eye Authentication option is enabled in NVR application then user will not be able to view playback video in MAXPRO mobile app/Web client.

Grand Eye New Evolution support

EVO18 0 and EVO12

Industry Standards

MAXPRO NVR is an open platform and supports broad third party device integrations with support for PSIA and ONVIF Profile S standards, Real Time Streaming Protocol (RTSP) standard and native device integrations.

Flexible Licensing

MAXPRO NVR comes with all required software applications and licenses.

Role Based Operator Privileges

MAXPRO NVR offers role-based operator privileges supporting Windows and Local users. You can add up to 1024 users under the Users tab.

Easy Configuration

A quick and easy 3-click* wizard to set up the system with auto-configuration and auto-discovery of IP cameras, recording and monitoring configuration, makes installing HD IP systems quick and efficient without requiring any IP expertise. Simple and logical configuration pages make setup a breeze, even for the novice installer.

* - With default settings and in a local area network for specific models.

64 channel Support

MAXPRO NVR (SE, PE), Hybrid NVR (SE, PE) and Software only solution now support 64 channels. You can connect up to 64 cameras based on your type of solution.

Auto Discovery

Discovering the IP cameras in the network is now simpler with the enhanced auto discovery interface. You can define the IP range to search for the cameras in the network and also camera credentials can be set at once for the newly discovered cameras.

MultiStream

MAXPRO NVR provides you with the flexibility to add multiple streams with different resolutions on a single camera. Depending on the type of camera you can add and configure additional streams and can define the Video Quality Settings, Recording Settings, and Stream Preference settings. Based on your requirements you can view or render different resolutions on a single camera. It also allows you to set various parameters for your recording, including audio.

Third Party ONVIF Profile G supported cameras:

Following new Third Party ONVIF compliance Profile-G cameras are now supported in NVR 4.7.

Profile G Cameras	Camera Type	Firmware Details
Tyco	ADCi350-B111	V3.1.0 170215
Samsung	QNO-7010R	1.04_170224
Panasonic	WV-SFV631L	2.41

MAXPRO Web Configurator

Enhanced the Web configurator user interface with new themes, for a better user experience while configuring the System, Server and Security configurations for Web client and mobile.

New Deletion Schedule

Introduced new deletion schedule where user can now retrieve the recordings of the last 5 years.

GPU Rendering Support

Cost-effective enhanced HD video rendering on remote desktop clients with support for monitoring of up to 18 1080p HD cameras in real time (30 fps) with no-time-lapse using the GPU capabilities of built-in processor graphics with Intel® 4th generation and above processors. This feature allows a user to render high resolution cameras while optimizing the CPU consumption. To know about improvised GPU rendering capability, see Improved GPU Rendering section on page 242 section.

Analog Capture Card Support

MAXPRO NVR Hybrid supports an Analog Capture card through which you can manually add 16 analog cameras. Each capture card comes with 16-channel support and allows you to manage the analog cameras.

User-Friendly and Feature-Rich User Interface

The MAXPRO NVR user interface is based on Honeywell's flagship MAXPRO® VMS user interface which offers a feature-rich user experience. Utilization of this familiar interface allows for the “Learn One, Know Them All” concept that ensures familiarity across a broad range of Honeywell products.

MAXPRO Status Monitor

MAXPRO Status Monitor is a brand new application in NVR V4.0 release that helps you to search and monitor the NVR's (System or Recording Engine) in the current network. You can monitor a single system/recording engine or multiple systems/ recording engines at once. This application is installed along with the NVR 4.0 software update and can be accessed on the desktop.

You can manually add or auto search for NVRs and then connect to a single or multiple NVRs (System or Recording Engine) to monitor the status of various parameters.

For a system you can monitor parameters such as CPU Consumption, Average Disk Queue Length, Disk Write/Read and so on, depending upon the NVR connected.

For a Recording engine you can monitor parameters such as Total FPS Received/ Recorded, Total Bitrate Received/Recorded, Total Active Cameras and so on.

Recording and Playback Operations

MAXPRO NVR supports simultaneous recording, live and playback viewing, search and system management of all supported IP cameras including HD formats in a single server instance.

On Demand live Streaming (VOD)

On Demand Live Streaming feature allows you to configure and store recordings at camera level. Later the recordings at the camera level can be synchronized back to view in NVR viewer. This avoids persistent stream recording. MAXPRO NVR configured as On Demand Live Streamer streams video from camera, only when a client request a live stream for viewing. When all the clients close the particular camera, then streaming from the camera is stopped.

The NVR configured as On Demand streamer supports only Sync back edge recording.

On Demand live streaming is compatible from MAXPRO NVR Viewer, MAXPRO NVR Web Clients and MAXPRO NVR Mobile app clients.

In your PC, by default On demand Live Streaming registry value is set to zero (disabled). User needs to change the value to 1 to use this feature. See How to Enable Video on demand feature in MAXPRO NVR section for more information.

Recording support in On Demand video Streaming: It is also an add-on for the existing Edge Sync Recording feature. This feature helps user to enable recording during on demand video streaming. A check box is introduced in Configurator > System tab to enable this feature. Earlier only live video was supported.

Profile-G or Edge Sync Support

Profile-G or Edge Sync feature allows you to synchronize the recordings from the camera SD card to NVR. Camera SD card contains recordings that are configured on demand. This features enables the user to playback only those recording which are saved on demand in the SD card. User can enable the edge syn feature in Camera page and configure the day and time for synchronizing in System window to get the recordings from the camera. Edge Sync feature is applicable only to the cameras with SD card. This feature is supported only for New EquIP Series model cameras.

Automatic Retry clips is an add-on for the existing Edge Sync Recording feature. This feature is meant to retry and download the failed clips. It allows user to configure various parameters in the config file to avoid clips download failure. If any clips fails to download then based on the user configuration auto retry feature downloads the clips to NVR.

Low bandwidth Stream Settings:

Use Low Resolution Stream: This feature is to view the low resolution video in any format of salvo layout. User needs to configure the low resolution (for any Primary or secondary stream) in MAXPRO NVR camera page. For the following scenario under which you can use this option:

- For a specific site if you want to use the Low Resolution stream option then you need to configure the stream settings in the camera tab. See Recommendation to use Low bandwidth stream option section for more information.

Note: *If you want to set the bit-rate value for a low bandwidth site then you can set this value in the camera web page*

Receive Only I Frame/Low Bandwidth Streaming: This feature is applicable only for the sites with Low bandwidth. It allows user to receive and view only I Frame considering the bandwidth at the site. This feature is only supported for MAXPRO NVR.

Use Extended time Outs: This helps in increasing the default time outs for NVR connections, stream connections and snapshots retrieval. This feature is only supported for MAXPRO NVR.

Optimize Stream Usage Settings:

Enable Stream Switch: Enable stream switch automatically switches between low and high resolution streams in the salvo layout based on the users selection. User should have minimum two streams available to use this feature. By default camera will stream in high resolution video in single salvo layout and the same camera when it is drag and dropped in multiple salvo, it streams with low resolution video. This feature is only supported for MAXPRO NVR.

Enriched Video Viewing Experience

MAXPRO NVR offers an enriched video viewing experience through the intuitive video rendering engine that optimizes CPU utilization by altering the video frame rate.

Efficient Event and Alarm Viewing Capability

MAXPRO NVR provides the ability to investigate events and alarms by simultaneously viewing alarm videos at various stages. For every alarm, users can view the video captured during pre-alarm, on-alarm, and post-alarm, and also view live video from the camera which triggered the alarm.

Simultaneous Video Recording and Video Viewing

MAXPRO NVR supports multiple simultaneous operations such as video recording and video viewing or alarm monitoring on the server unit without the need for an additional workstation. It also provides the option of remote monitoring clients. You can view live video while simultaneously performing searches.

Video Motion Detection (VMD) Support

MAXPRO NVR supports both camera-based and server-based video motion detection (VMD). Camera-based VMD support depends on the integration method and the motion detection performance depends on camera analytics. Server-based VMD (SMART VMD) is supported for all video devices supported by NVR, and is based on Honeywell Active Alert analytics algorithms supporting object-based motion detection with reduced false alarms.

Search

MAXPRO NVR supports multiple search features: Timeline Search, Preview Search, Alarm/Events Search, Calendar Search and SMART Motion Search.

SMART Motion Search

SMART Motion Search feature allows you to search for a missing object by searching on motion in recorded video within a short span of time. This feature overcomes the traditional way of searching an object in recorded videos. It also provides you with before and after recordings of a missing object.

360 Immersive Experience (Dewarping) Support

MAXPRO NVR supports client side dewarping integration with Oncam Grandeye and Immervision 360 applications.

New EquIP Series Camera Models Support

Additional 8 new EquIP camera models are now supported (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D, HDZ302DIN). In addition the following are the advanced features that are offered through these cameras:

- Intrusion trace (Need to purchase separate license to enable this feature in camera)
- Face Detection
- Audio Detection (For cameras with Built-in Microphone or External Microphone)
- SD Card Failure

New high performance and specialty EquIP Camera Support

- HM4L8GR1: 8 MP IR Rugged Multi-Imager Dome
- HMBL8GR1: 8 MP IR Rugged Multi-Imager Bullet
- H4L6GR2: Low-Light 6 MP IR Rugged Dome
- HBL6GR2: Low-Light 6 MP IR Rugged Bullet
- HEPB302W01A04: 1080p 30x Explosion-Proof IP Camera, 4 m cable
- HEPB302W01A10: 1080p 30x Explosion-Proof IP Camera, 10 m cable
- HTMZ160T302W: Dual Sensor Thermal/Visual IP PTZ Camera

3D Positioning

3D Positioning feature enables you to view a specific object in a live video in 3-dimensional view. On a live video you need to draw a region to view a specific object. This feature is supported only with New EquIP PTZ (HDZ302DE, HDZ302D, HDZ302DIN) camera models.

New EquIP Camera Model Dewarping

New EquIP FishEye Camera (HFD6GR1) is capable of delivering FishEye view of the surrounding and which can also be Dewarped to different view types depending on the mounting position.

H.265 Codec Support

H265 codec type is now supported to optimize the storage requirements for higher solution cameras. H265 is only supported for New EquIP model cameras (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D and HDZ302DIN). H.265 cameras supports GPU based Rendering. Now you can render upto 23 H.265 cameras with 1080P Resolution at 30 FPS/30 GOP.

Limitations of H.265 Codec Type:

- H.265 is not supported in MAXPRO Mobile app

- H.265 is not supported in Web client

Meta Data Conversion Utility

Meta data conversion utility allows you to replace or update the unique system ID number of the recorded clips and Meta data details for all or specific cameras. This utility helps you to retain your recorded clips and Meta data details during Failover /Failback operations. This allows a user to effectively playback the recorded clip without loss of video.

Multi-language Support

MAXPRO NVR supports multiple languages such as English, French, Arabic, Russian, Spanish, Italian, Dutch, German, Czechoslovakian, Portuguese and Polish. English is the default language.

Keyboard Support

MAXPRO NVR supports industry standard Honeywell keyboards connected over Ethernet such as UltraKey Plus and UltraKey Lite

Clip Export

MAXPRO NVR supports exporting clips with audio in - WMV, ASF and Honeywell MPVC formats. It also supports exporting still images/snapshots in .BMP format. The clips can be signed with digital signatures to ensure authenticity.

MAXPRO NVR Clip Player

MAXPRO NVR Clip Player is a Honeywell proprietary clip player designed to only playback exported MAXPRO Video Container format (MPVC) clips. This clip player is part of the NVR 4.0 package and can be accessed in the NVR installation folder.

Email Notification

MAXPRO NVR supports email notification on camera, system and operator events.

Video Surround Feature

MAXPRO NVR offers Video Surround, which provides the ability to track subjects of interest as they move between areas covered by adjacent cameras. Simply double-click on the panel where the subject is currently visible to track the subject.

Profile Cameras

Multi-zoom views on HD video and support for Profile cameras to create virtual cameras by digitally zooming into the field of view. Example: Zoom in on a cash register in one view of the HD camera and at the same time monitor the cash operator in the zoom out view of the HD camera

Reports

Using the MAXPRO NVR, you can generate Event History and Operator Log reports, each of which has its own significance. These reports can be exported in PDF, Crystal Reports, Excel and Word formats.

Integration Capability

Multiple MAXPRO NVRs can be deployed for system expansion using a distributed architecture and integrated with the MAXPRO Viewer multi-site software or MAXPRO VMS enterprise video management system. MAXPRO also integrates with WIN-PAK® and Pro-Watch® Access Control Systems.

Audio

MAXPRO NVR supports 1-way audio (camera to NVR) for specific IP cameras. Please refer to the MAXPRO NVR compatibility list at www.security.honeywell.com/hota/compatibility/index.html for the models supported.

Web Client

The MAXPRO NVR Web Client allows you to remotely access the MAXPRO NVR server using a web browser like Internet Explorer and perform video surveillance. It gives you the flexibility to view live video and perform the basic video surveillance functions remotely over the web. MAXPRO NVR Web Client supports viewing the live video, viewing Recorded Video (Playback), taking a Snapshot and viewing Presets.

Archival

This feature enables you to archive the recorded video from the system manually or automatically to a NAS or SAN disk. You can define a specific schedule to archive the recordings periodically or you can manually archive whenever required. For both cases you should configure the archival disk/drive in the Configurator > Disk tab. To configure NAS for recording, see Guidelines to configure NAS Drive for Recording section on page 245 for complete information.

Mobile Apps

MAXPRO NVR supports mobile monitoring clients on iOS and Android with MAXPRO NVR Mobile apps. The apps can be used to perform common daily tasks such as viewing live video, zooming in for full screen viewing, playback or searching for video by date and time, perform PTZ control through presets, monitor & manage alarms and taking a snapshot of a video frame. Recent enhancements also include One configuration for both Local and Remote server connection, Fingerprint Authentication login is support (only for IOS devices), Digital Zoom (only for IOS devices), HIS Streaming and HTTPS support

Advanced Security

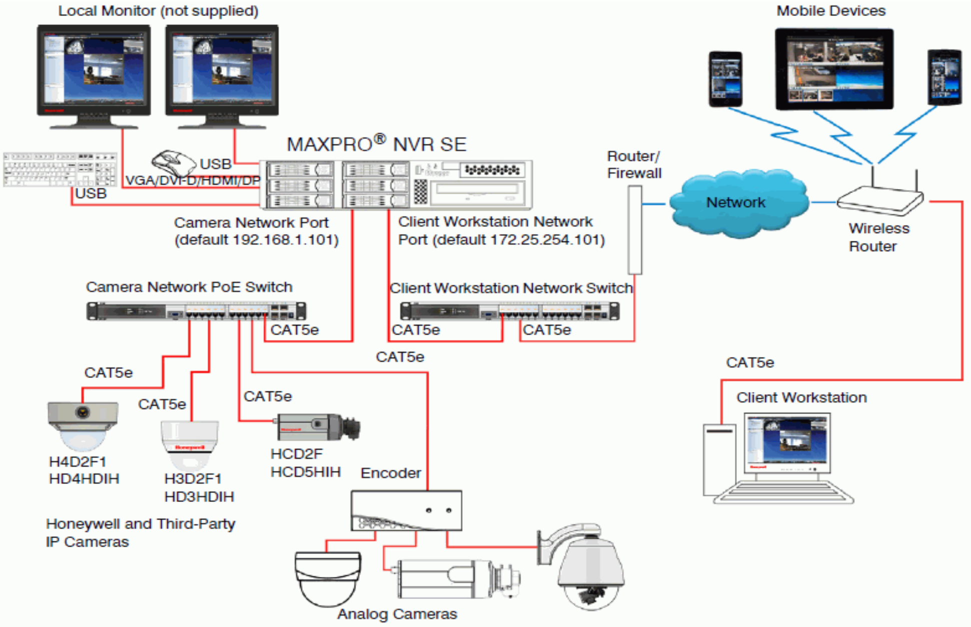
MAXPRO NVR supports advanced security features with encryption support for communication between desktop client to NVR and secure https login for the Web Client and Mobile App.

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*

MAXPRO NVR Typical System Architecture

MAXPRO NVR Standalone System Diagram

The following figure illustrates the MAXPRO NVR SE system architecture.

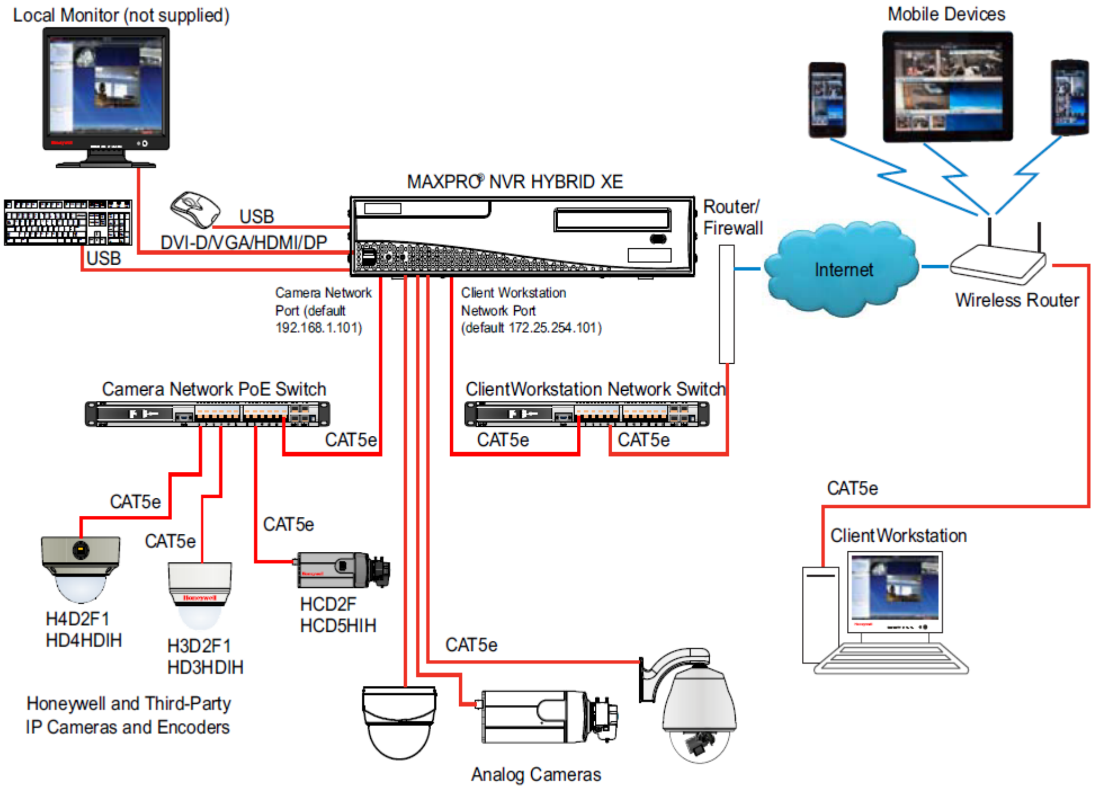


MAXPRO NVR SE System Diagram

Note: *The NVR SE box in the above system diagram is used as an example of a typical system. Other System diagrams for NVRs (XE, PE and Software only) look similar to the NVR SE and will only have minor differences.*

MAXPRO NVR Hybrid Standalone System Diagram

The following figure illustrates the MAXPRO NVR HYBRID XE Standalone system architecture.

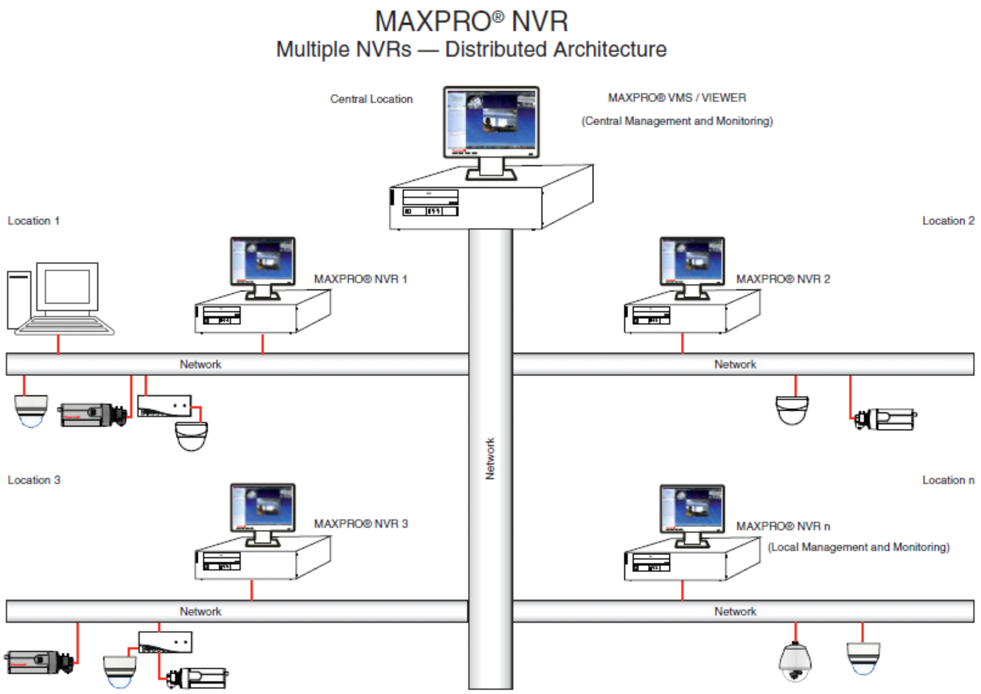


MAXPRO NVR HYBRID XE Standalone System Architecture

Note: *The Hybrid NVR XE box in the above system diagram box is used as an example of a typical system. Other system diagrams for Hybrid NVRs (SE, PE) look similar to the Hybrid NVR XE and will only have minor differences.*

MAXPRO NVR Distributed System Architecture

The following figure illustrates the MAXPRO NVR distributed system architecture.



MAXPRO NVR Distributed System Architecture

This page is intentionally left blank

CHAPTER

3 COMMISSIONING MAXPRO NVR

Overview of Commissioning Procedure

Commissioning is the process of setting up the MAXPRO NVR system hardware, installing the software and configuring the NVR system. At the end of the commissioning process, the MAXPRO NVR system is equipped for use by operators to perform video surveillance operations.

Steps in the Commissioning Procedure

The process of commissioning involves the following phases.

- Setting up the MAXPRO NVR system
- Installing the Software in the Server and Client Computers
- Configuring the MAXPRO NVR
- Verifying the Configuration

Setting up the MAXPRO NVR

Setting up the MAXPRO NVR involves:

- Determining the number of MAXPRO NVR server and client computers at the location.
- Choosing the desired MAXPRO NVR system architecture.
- Connecting the monitors to the MAXPRO NVR. After connecting the monitors, configure the monitor display properties.
- Connecting the keyboards (for example, Ultrakey) to the MAXPRO NVR unit.

See the Setting up the MAXPRO NVR Turnkey Box Solutions section on page 83 for information on how to setup the MAXPRO NVR XE/SE/PE or MAXPRO NVR Hybrid XE/SE/PE system.

See the Setting up the MAXPRO NVR Software-Only Solution section on page 89 for information on how to setup the MAXPRO NVR Software installed on a 3rd party Server.

Installing the Software in the Server and Client Computers

Note: *Full/Fresh installation is NOT required on Honeywell's boxed solutions: MAXPRO NVR XE, SE, PE and MAXPRO NVR Hybrid XE, SE, PE. Fresh client installation is only required on client computers.*

The following steps are involved to install the MAXPRO NVR software on a 3rd party hardware:

Step 1. The server and client computers meet the minimum hardware and software requirements.

Step 2. Installing the MAXPRO NVR software.

Caution: Don't install any Email client on the MAXPRO NVR server machine.

See the MAXPRO NVR Software Installation section on page 104 for information on software requirements and installation instructions for the MAXPRO NVR software.

Configuring the MAXPRO NVR

In this phase, you need to configure the MAXPRO NVR through the user interface. Configuring MAXPRO NVR includes the following:

- Configuring the Honeywell cameras with MAXPRO NVR Wizard
- Configuring the system level settings
- Configuring the disk management settings
- Configuring the schedule based recording for cameras
- Performing user administration

See the In this chapter... section on page 153 for information on how to configure the MAXPRO NVR system.

Verifying the Configuration

Verifying the configuration involves checking whether the surveillance operations can be performed using MAXPRO NVR. Surveillance operations include: viewing the live video, performing the pan, tilt, and zoom on the video, and starting the video recording.

See the Verifying the Configuration section on page 305 for information on how to perform the verification.

CHAPTER

4 SETTING UP THE MAXPRO NVR

Overview

This chapter describes the settings for setting up the MAXPRO NVR system.

- For setting up the MAXPRO NVR Single-box solution, see the Setting up the MAXPRO NVR Turnkey Box Solutions section on page 83.
- For setting up the MAXPRO NVR Software-Only solution, see the Setting up the MAXPRO NVR Software-Only Solution section on page 89.
- For setting up a peripheral Joystick Controller, see the Connecting the Joystick Controller section on page 99.

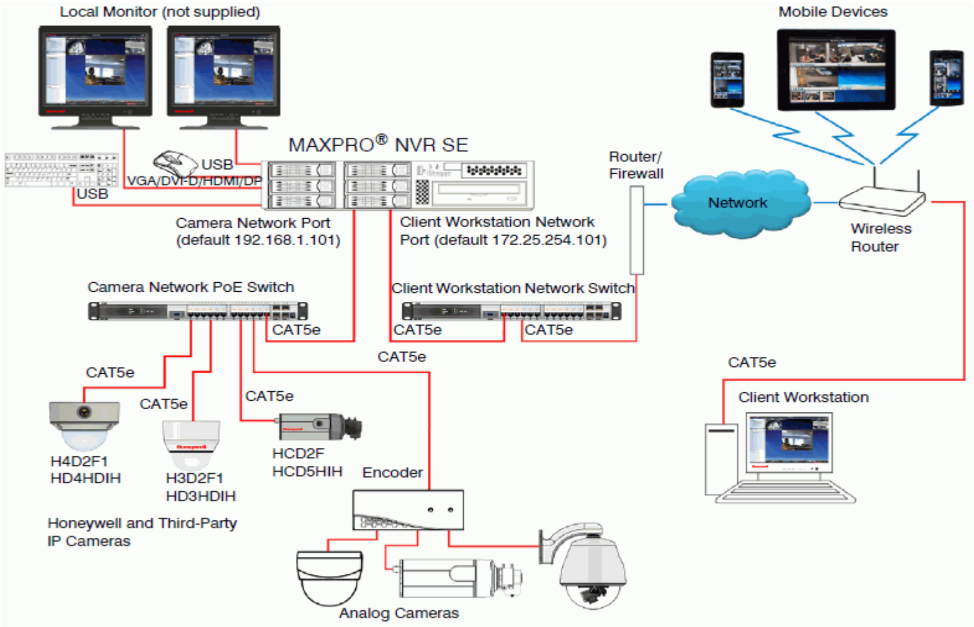
Setting up the MAXPRO NVR Turnkey Box Solutions

Setting up the MAXPRO NVR unit and client computers is the first phase in the commissioning process.

Refer to the specific *MAXPRO NVR Data Sheet* on Honeywell Video web site. (www.honeywellvideo.com) for information on hardware specifications for the MAXPRO NVR unit.

Typical MAXPRO NVR System Diagram

The following figure illustrates the MAXPRO NVR SE system diagram.

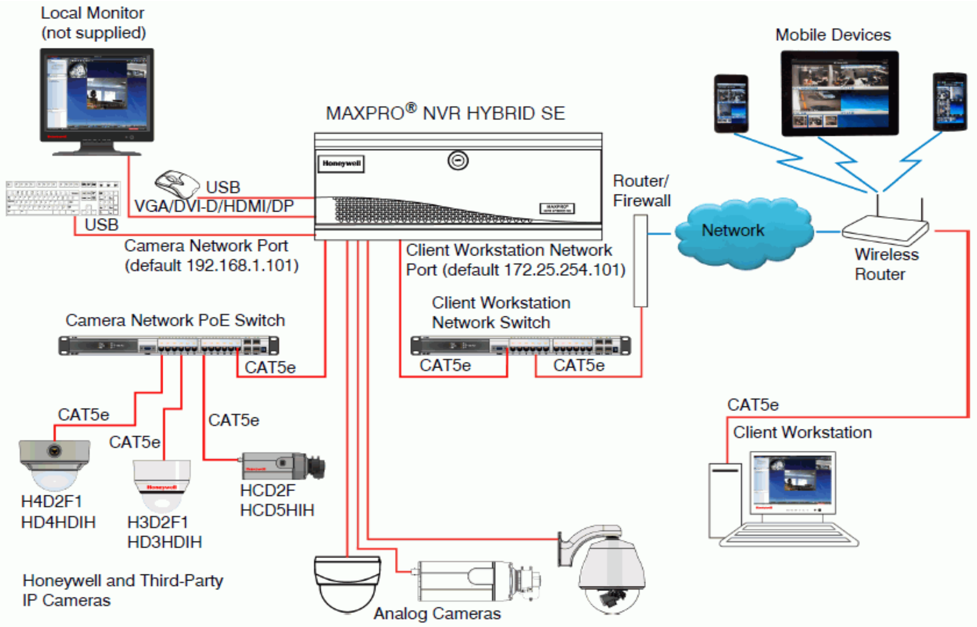


Typical MAXPRO NVR System Diagram

Note: *In the above system diagram NVR SE box is used as an example of a typical system. Other System diagrams for NVRs (XE, PE and Software only) look similar to the NVR SE and will have minor differences.*

Typical MAXPRO NVR Hybrid System Diagram

The following figure illustrates the MAXPRO NVR Hybrid system diagram.



Typical MAXPRO NVR Hybrid System Diagram

Note: *In the above system diagram Hybrid NVR SE box is used as an example of a typical system. Other system diagrams for Hybrid NVRs (XE, PE) look similar to the NVR Hybrid SE and will have minor differences.*

See MAXPRO NVR Hybrid Connections section on page 90 for rear panel connectors to connect analog video source, looping outputs and IOs.

Connecting the Monitors

Connect one or more local monitors to one of the monitor connections on the back panel of your MAXPRO NVR unit. The number of monitors that you can connect to the MAXPRO NVR unit varies based on the NVR Edition you purchase. Refer to the specific *MAXPRO NVR Data Sheet* on Honeywell Video web site (www.honeywell-video.com) for more information.

Powering on the MAXPRO NVR Unit

Note: *Honeywell recommends using an Uninterrupted Power Supply (UPS) for the MAXPRO NVR unit and the cameras. Powering the cameras and unit from a UPS ensures that the MAXPRO NVR unit can continue to record video during a power outage or during transient power events. If you need to monitor video during a power outage, consider a UPS for the client workstations as well.*

To power on the MAXPRO NVR unit

Step 1. Turn on camera(s) and other hardware connected to the MAXPRO NVR unit.

Step 2. Press and hold the power button on front of the MAXPRO NVR unit. The power button turns “blue” after the MAXPRO NVR unit is turned on.

Step 3. After powering on the unit, you are prompted to log on. For MAXPRO NVR turnkey units shipped with v4.0 or later version, the default Windows desktop login user has user name: NVR-Admin, password: Password$123. The user name and password are case sensitive. You will be prompted to create a new password the first time that you log in. After logging on, the MAXPRO NVR Wizard automatically starts up but may take two minutes to initiate.

Note: *Honeywell recommends to disable the Administrator User account and create a new Administrator User account. See* Securing MAXPRO NVR *section on page* 299 *for more information.*

To turn off the power for MAXPRO NVR

Step 1. Close the MAXPRO NVR application.

Step 2. Click Start>Shut Down. Wait for the MAXPRO NVR unit to shut down.

Changing the MAXPRO NVR IP Address and Machine Name

Your MAXPRO NVR unit has pre-configured network ports with the following default IP addresses:

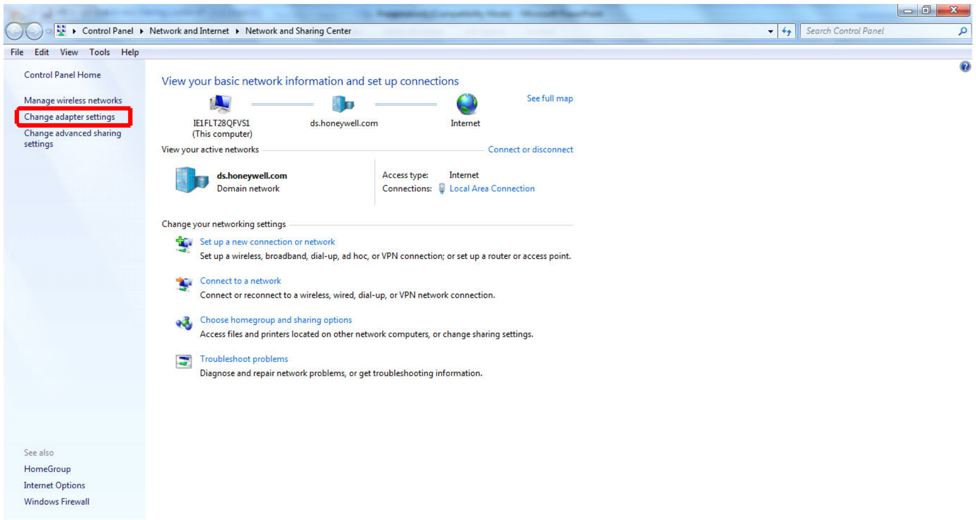
- 192.168.1.101 for NIC1 (Camera Network)
- 172.25.254.101 for NIC2 (Client Workstation Network)

Note: *NIC2 may not be available on all NVR options, please refer to the data sheet for more information.*

If more than one MAXPRO NVR unit is on the same network, you must assign a unique IP address and computer name to each unit (the default name is MAXPRO-NVR).

Changing the IP address

Step 1. Click the network icon in the notification area, click Open Network and Sharing Center (See Typical MAXPRO NVR Hybrid System Diagram), and then click Change adapter settings.



View your basic network information and set up connections

View your active networks

ds.honeywell.com
Domain network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

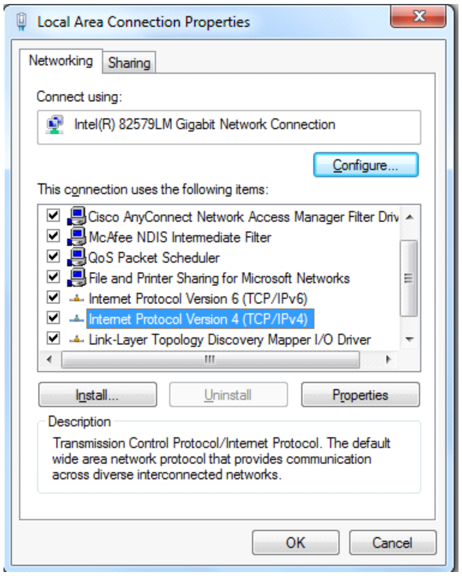
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Network and Sharing Center

Step 2. Right-click Camera Network or Client Workstation Network, and then click Properties. The Local Area Connection Properties dialog box (Similar to MAXPRO NVR Software Solution Distributed System) appears.



Connect using:
Intel(R) 82579LM Gigabit Network Connection

This connection uses the following items:

- ☑ Cisco AnyConnect Network Access Manager Filter Driv
- ☑ McAfee NDIS Intermediate Filter
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

LAN Properties

Step 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties.

Step 4. Click Use the following IP address, and then, in the IP address, Subnet mask, and Default gateway boxes, type the IP address settings.

Step 5. Click Use the following DNS server addresses, and then, in the Preferred DNS server and Alternate DNS server boxes, type the addresses of the primary and secondary DNS servers.

Changing the computer name

Step 1. Click Start, right-click Computer, and then click Properties. The System window appears.

Step 2. Click Advanced system settings. The System Properties dialog box appears.

Step 3. Click the Computer Name tab, and then click Change...

Step 4. In Computer name, delete the old computer name, type a new computer name, and then click OK. The name cannot contain spaces or all numbers or any of the following characters: < >;: " * + = \ | ?.

Step 5. After changing the computer name, you are prompted to restart the computer.

Step 6. Navigate to the C:\Program Files\Honeywell\MaxproNVR\TrinityFramework\bin folder, and then double-click MaxProNVRMachineNameUtility.exe to open the Maxpro NVR Utility.

Step 7. The new computer name automatically appears in the Machine Name field. If it does not, enter the name manually and click Update. The message `Machine Name Updated Successfully` appears when the update is complete.

Configuring the Monitor Display Properties

The recommended display settings for the monitor are dialog box resolution of 1280 x 1024 pixels and color quality of 65K colors non-interlaced. The display settings can be configured from the Windows control panel or from the Windows desktop through the context menu.

Configuring Display Settings for the Context Menu

Step 1. Right-click on the Windows desktop and select Screen resolution.

Step 2. Select the appropriate Resolution.

Step 3. Click OK to save the setting and close the dialog box.

Configuring Display Setting from the Control Panel

Step 1. Click Start > Control Panel, to open the Windows control panel screen.

Step 2. Under Appearance and Personalization, click Adjust screen resolution.

Step 3. Select the appropriate Resolution.

Step 4. Click OK to save the setting and close the dialog box.

Setting up the MAXPRO NVR Software-Only Solution

Setting up the MAXPRO NVR server and client computers is the first phase in the commissioning process.

Before you Begin

Determine the following at the location.

- Number of server and client computers required.
- Hardware configuration of the computers.
- Number of peripheral devices such as joystick controllers (Ultrakey keyboard), and other devices that are needed.

Hardware Specifications

The MAXPRO NVR server and client computers must meet the minimum hardware specifications, refer to the *MAXPRO NVR Software Data Sheet* for more information.

MAXPRO NVR Software System Architecture

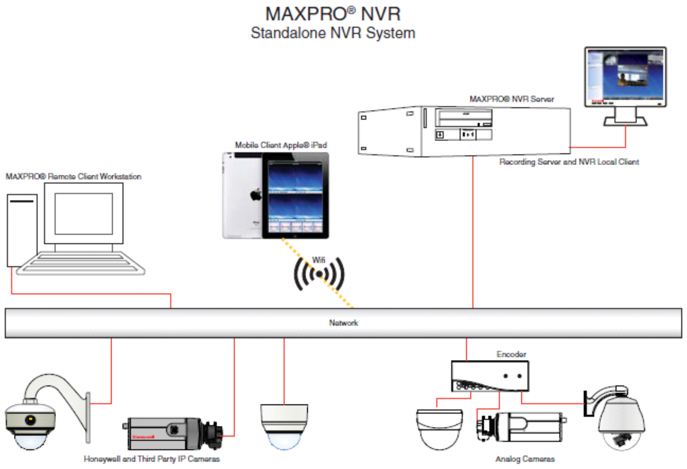
MAXPRO NVR software solution can be set up in the following two ways:

- Standalone System
- Distributed System

Corresponding system architectures are displayed below

MAXPRO NVR Software Solution Standalone System

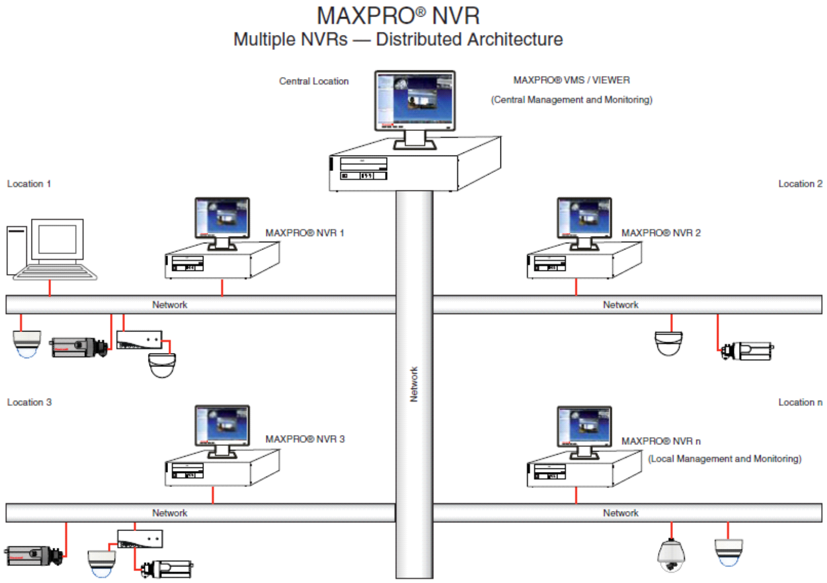
The following figure illustrates the MAXPRO NVR Standalone system.


MAXPRO® NVR
Standalone NVR System
MAXPRO® NVR Server
Recording Server and NVR Local Client
Mobile Client Apple® iPad
MAXPRO® Remote Client Workstation
Wifi
Network
Encoder
Honeywell and Third Party IP Cameras
Analog Cameras

MAXPRO NVR Software Solution Standalone System

MAXPRO NVR Software Solution Distributed System

The following figure illustrates the MAXPRO NVR Distributed system.



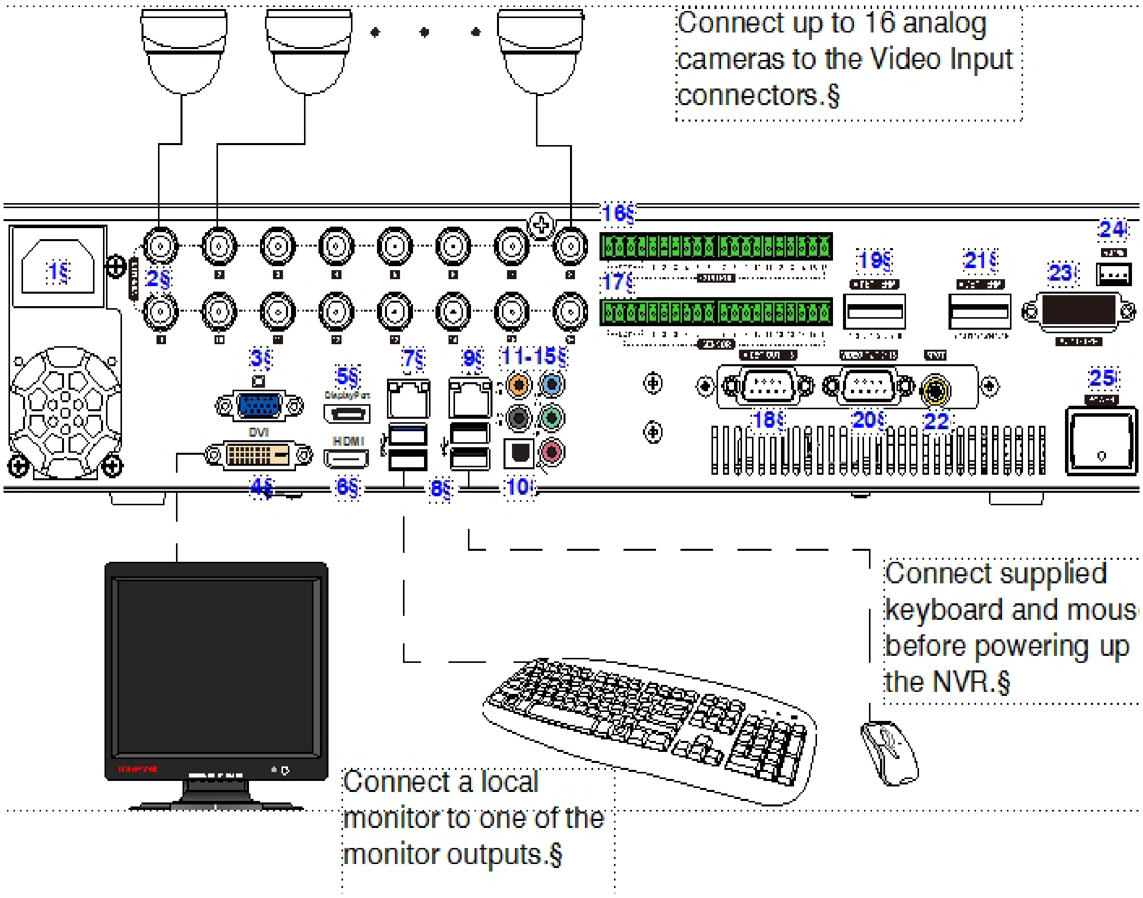
MAXPRO NVR Software Solution Distributed System

MAXPRO NVR Hybrid Connections

Rear Panel Connectors

The rear panel of the NVR contains the connectors used for attaching cameras, sensors, and relays to the NVR. Below are the diagrams that outline the location and connections of Hybrid XE, SE and PE connectors and also the Input and Output Ports For MAXPRO NVR Hybrid PE.

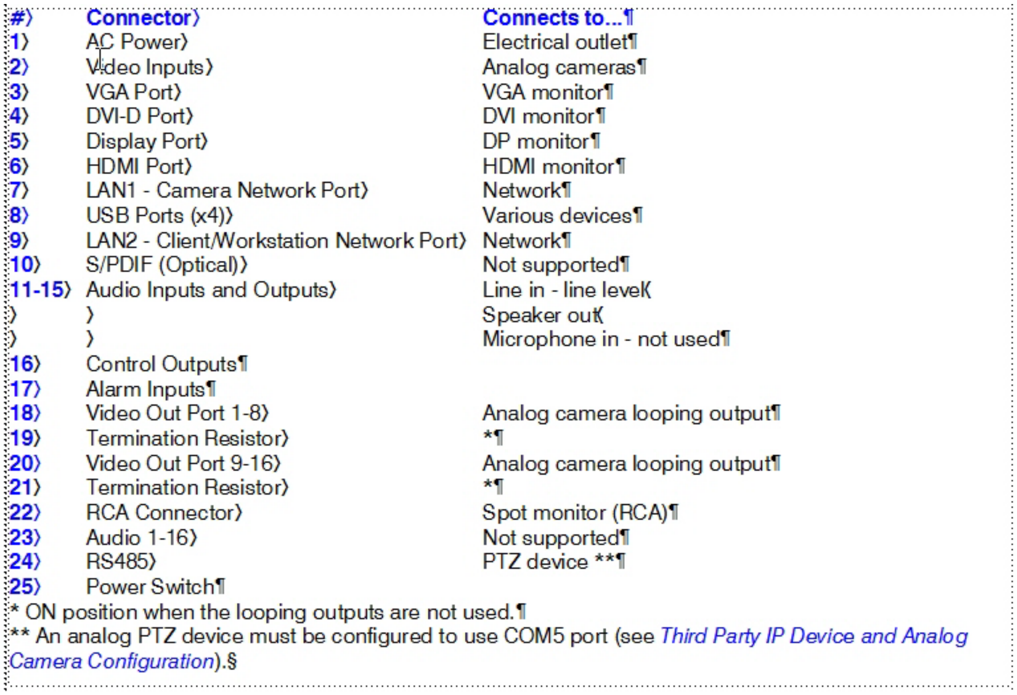
Hybrid XE Connections



Connect up to 16 analog cameras to the Video Input connectors.§

Connect supplied keyboard and mous before powering up the NVR.§

Connect a local monitor to one of the monitor outputs.§



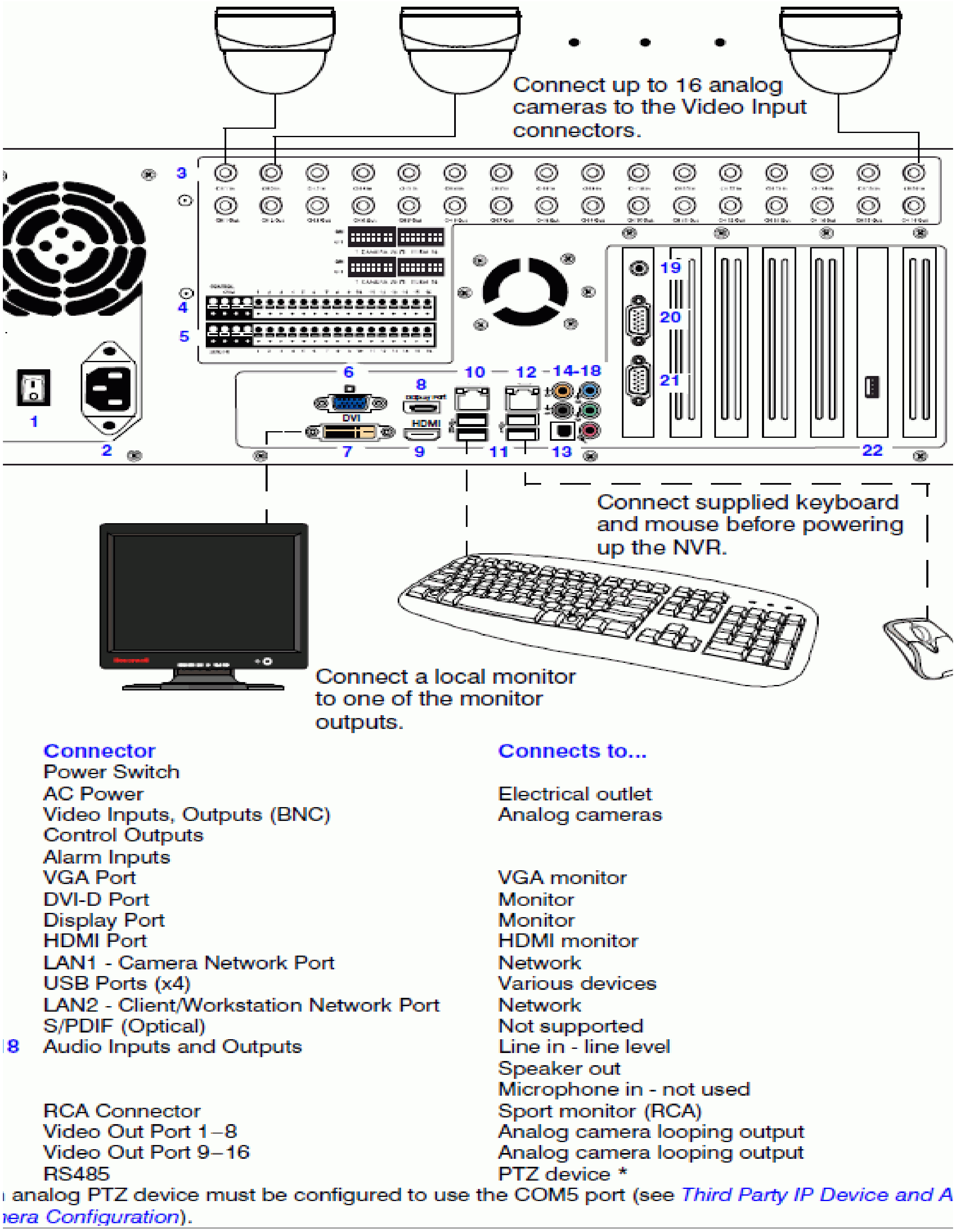
#	Connector	Connects to...
1	AC Power	Electrical outlet
2	Video Inputs	Analog cameras
3	VGA Port	VGA monitor
4	DVI-D Port	DVI monitor
5	Display Port	DP monitor
6	HDMI Port	HDMI monitor
7	LAN1 - Camera Network Port	Network
8	USB Ports (x4)	Various devices
9	LAN2 - Client/Workstation Network Port	Network
10	S/PDIF (Optical)	Not supported
11-15	Audio Inputs and Outputs	Line in - line level
		Speaker out
		Microphone in - not used
16	Control Outputs	
17	Alarm Inputs	
18	Video Out Port 1-8	Analog camera looping output
19	Termination Resistor	*
20	Video Out Port 9-16	Analog camera looping output
21	Termination Resistor	*
22	RCA Connector	Spot monitor (RCA)
23	Audio 1-16	Not supported
24	RS485	PTZ device **
25	Power Switch	

* ON position when the looping outputs are not used.

** An analog PTZ device must be configured to use COM5 port (see *Third Party IP Device and Analog Camera Configuration*).

Hybrid XE Connections

Hybrid SE Connections

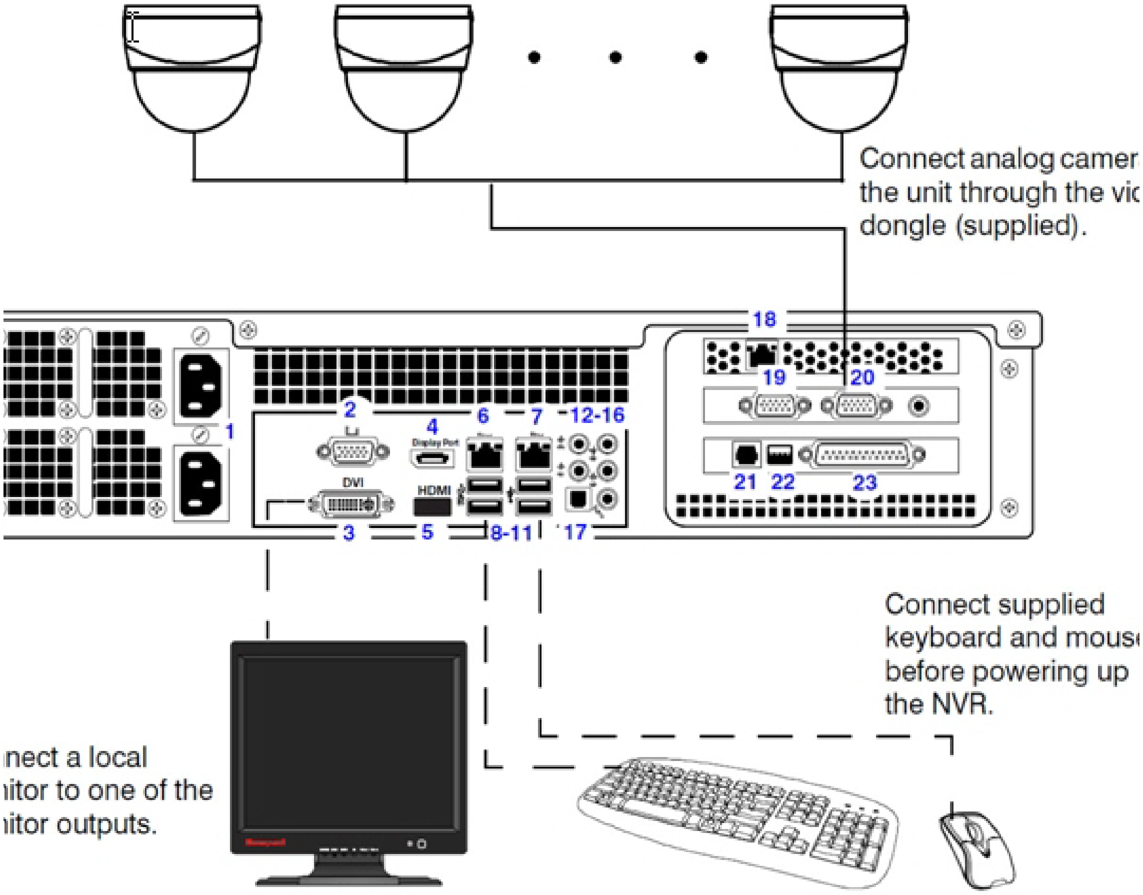

Connect up to 16 analog cameras to the Video Input connectors.
3
4
5
1
2
6
7
8
9
10
11
12
13
14-18
19
20
21
22
DVI
HDMI
Connect supplied keyboard and mouse before powering up the NVR.
Connect a local monitor to one of the monitor outputs.

	Connector	Connects to...
	Power Switch	
	AC Power	Electrical outlet
	Video Inputs, Outputs (BNC)	Analog cameras
	Control Outputs	
	Alarm Inputs	
	VGA Port	VGA monitor
	DVI-D Port	Monitor
	Display Port	Monitor
	HDMI Port	HDMI monitor
	LAN1 - Camera Network Port	Network
	USB Ports (x4)	Various devices
	LAN2 - Client/Workstation Network Port	Network
	S/PDIF (Optical)	Not supported
8	Audio Inputs and Outputs	Line in - line level
		Speaker out
		Microphone in - not used
	RCA Connector	Sport monitor (RCA)
	Video Out Port 1–8	Analog camera looping output
	Video Out Port 9–16	Analog camera looping output
	RS485	PTZ device *

analog PTZ device must be configured to use the COM5 port (see *Third Party IP Device and A* *era Configuration*).

Hybrid SE Connections

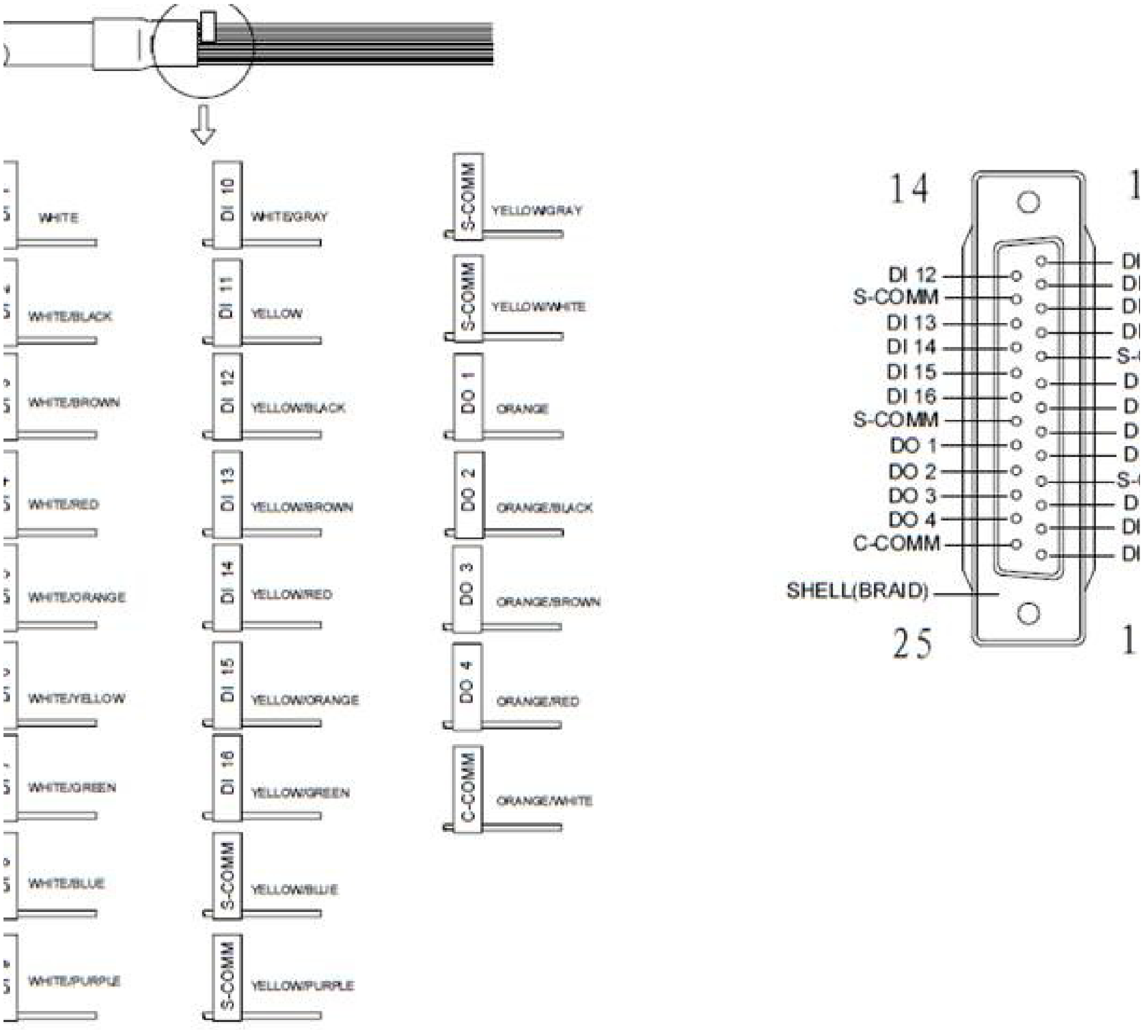
Hybrid PE Connections



#	Connector	Connects to...
1	AC Power (x2)	Electrical outlet
2	VGA Port	VGA monitor
3	DVI-D Port	Monitor
4	Display Port	Monitor
5	HDMI	Not supported
6	LAN1 - Camera Network Port	Network
7	LAN2 - Client Workstation Network Port	Network
8-11	USB Ports (x4)	Various devices
12-16	Audio inputs and outputs	Line in - line level Speaker out Microphone in - not used
17	S/PDIF (Optical)	
18	RAID Management Port	RAID device
19	Video Input 1-8	Cameras
20	Video Input 9-16	Cameras
21	Not used	
22	RS485	PTZ device *
23	Input and Output Ports	Alarm inputs and Control outputs

* An analog PTZ device must be configured to use the COM4 port (see *Third Party Device Configuration*).

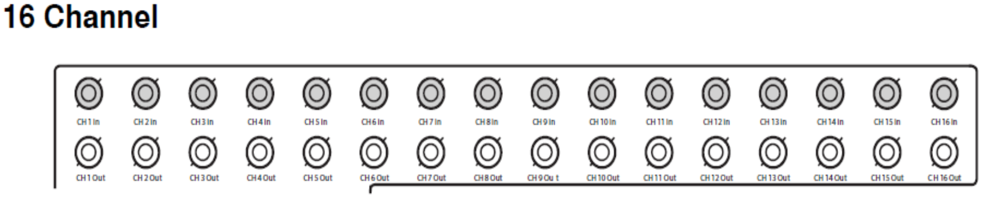
Hybrid PE Connections



Input and Output Ports For MAXPRO NVR Hybrid PE

Connecting a Video Source

There are different types of Video Sources that can be plugged into the NVR including DVD players, VHS players, and CCTV Cameras. Hybrid XE, SE and PE support 16 channel analog video source. The connectors use the BNC standard.



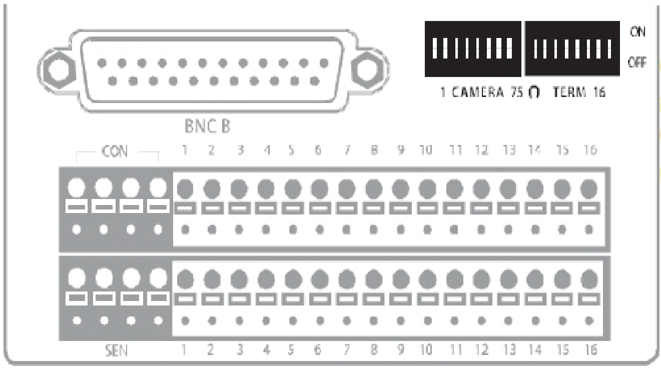
Connecting a Video Source

Note: *The video inputs are 75 Ω BNC connectors. Plug one end into the video source (DVD, Camera, etc.) and plug the other end into the desired BNC input on the NVR.*

Looping Output Termination

If the image appears distorted or virtually un-viewable, turn the termination resister to the ON position, making it terminated. When it is necessary to terminate a looping output, the NVR has built-in termination that allows users to select individual outputs. It is not always necessary to terminate the output; it depends on the device to which you are connecting. As a rule, if the image appears distorted or virtually un-viewable, it likely needs to be terminated.

Note: *Please refer to the specific Hybrid unit data sheet for more information on number of looping outputs supported on a specific unit.*



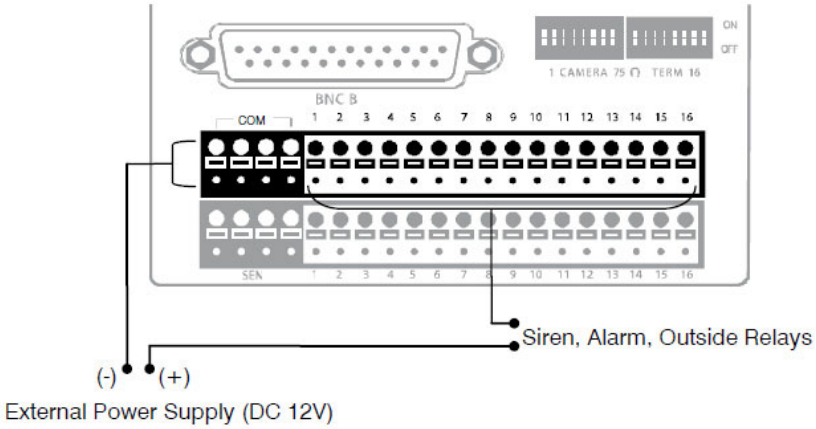
ON Not connected to a monitor (Normal)
OFF Connected to a monitor (Looped)

Looping Output Termination

Note: *Always leave the dip switch set to the ON position when the Looping Outputs are not used and only the installer should decide to turn it ON /OFF.*

Connecting Control Outputs

Each NVR Hybrid has Control Outputs. These outputs can be used to trigger devices such as Sirens, Phone Dialers, Lights, and any other relay activated device. There is no power supplied to the ports. Use an external power supply if necessary.



Control Outputs

Use 12V, below 300mA. For controlling lights or other devices, use another external relay.

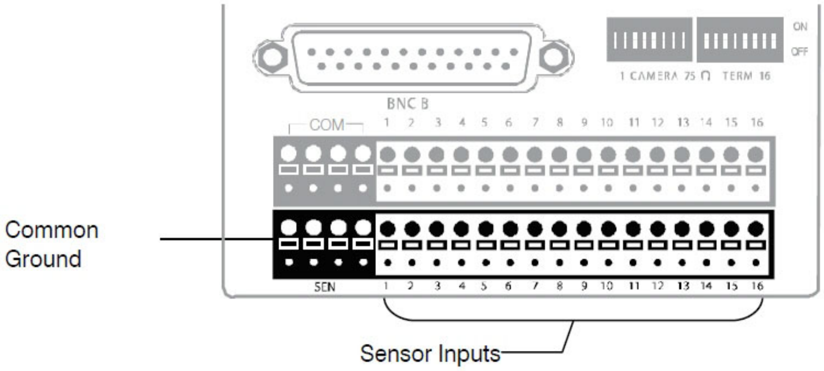
- Maximum voltage is 24V AC @ 1 amp
- Output uses a Form C Relay

Note: *Please refer to the specific Hybrid unit data sheet for more information on number of control outputs supported on a specific unit.*

Connecting Sensors

Each NVR Hybrid has Sensor inputs. These inputs can be used with devices such as infrared devices, motion device, glass breakage alarms, door and window trips, and so on. The Sensors can be set to Normally Open or Normally Closed inside the software.

There are Common Grounds (-) and sensor inputs (+). There is no power supplied to the ports so an external power supply must be used if power is necessary.



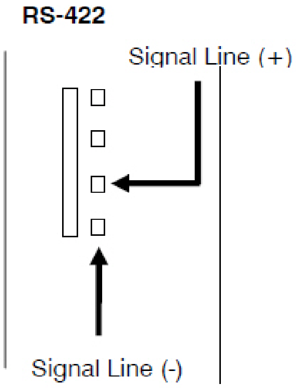
Connecting Sensors

Note: *Please refer to the specific Hybrid unit data sheet for more information on number of sensor inputs supported on a specific unit.*

Connecting an Analog PTZ Camera

Setting up a PTZ Camera is simple. The NVR Hybrid comes pre-assembled with an internal PTZ adapter. The cabling may be run up to 4,000 ft using 22 Gauge Twisted Pair. It is important to understand how the PTZ connects to the NVR. The NVR outputs an RS-232 signal and converts in to an RS-422/485 signal which is then sent to the PTZ camera.

Attaching the 4-Pin Adapter



4-Pin Adapter

Step 1.Locate the PTZ adapter cable.

Step 2.Connect the wires of the PTZ adapter to the PTZ camera. The yellow wire should connect to the RX+ on the camera and the orange wire should connect to the RX-.

Step 3.Connect the other end of the adapter to the XVR unit as shown.

Step 4.Assign the PTZ camera an ID number in PTZ Setup that coincides with the number assigned to the camera. This is normally done utilizing a dip-switch configuration method on the addressable dome. For Example: If the camera is plugged into input number 5, set the PTZ unit to ID number 5.

Connecting the Joystick Controller

Joystick Controllers (Ultrakey Plus or Ultrakey Lite over Ethernet) can be connected to MAXPRO NVR without any configuration.

Honeywell UltraKey joystick controller is an industry-leading approach to intelligent, user-friendly control of video management systems. Using the UltraKey keyboard, you can perform actions such as selecting a panel, PTZ operations, selecting a video source such as a camera, and others in the Viewer tab.

Connecting a Joystick Controller to MAXPRO NVR

To connect a Joystick Controller to MAXPRO NVR

- The UltraKey can be connected through the Ethernet. Set the UltraKey IP Address and System Controller (IP Address of MAXPRO NVR) through the UltraKey configuration settings. Refer to the *UltraKey manual* for more information.

How to log on to the UltraKey Plus keyboard?

First time users of MAXPRO NVR must explicitly log on to UltraKey Plus keyboard in order to use MAXPRO NVR.

Step 1. Power-on the UltraKey Plus keyboard.

Step 2. Press the Menu key on the LCD.

Step 3. Press the MAX-1000 Setup key on the LCD. The Left, Up, Right, and Down buttons appear on the LCD.

Step 4. Press the Ent hard key located on the right side of the UltraKey Plus keyboard.

Step 5. Enter the default PIN password 1234.

Step 6. Press Ent. The UltraKey Plus keyboard is now ready for use for performing the video management functions.

How to log off from the UltraKey Plus keyboard?

Step 1. Press the Menu key on the LCD.

Step 2. Press the MAX-1000 Setup key on the LCD. The Left, Up, Right, and Down buttons appear on the LCD.

Step 3. Press the Down key.

Step 4. Press the Ent hard key twice located on the right side of the UltraKey Plus keyboard. The log off confirmation message appears.

Step 5. Press the Ent hard key.

NetBIOS Naming Convention Limitations

This section describes the naming conventions for computer accounts in Microsoft Windows, NetBIOS domain names, DNS domain names, Active Directory sites, and organizational units (OUs) that are defined in the Active Directory directory service.

For MAXPRO NVR

In remote connection scenario, the NVR Hostname will be more than 15 characters. However, NetBIOS naming convention supports only 15 characters for hostname.

- If user is trying to connect to a database and if it failing, then ensure that the hostname of the computer is not more than 15 characters.

Refer the following Microsoft web page of more details on NetBIOS limitations.

https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

CHAPTER

5 INSTALLING THE NVR SOFTWARE

Overview

This chapter describes the procedures for installing the MAXPRO NVR software. Follow the appropriate section in this chapter to complete your MAXPRO NVR software installation.

Caution: For Honeywell's turnkey box solutions, MAXPRO NVR XE/SE/PE and MAXPRO NVR Hybrid XE/SE/PE, the server and client software required is pre-installed on the box. The instructions in this chapter for Server software fresh installation are NOT applicable for the turnkey box solutions. On the NVR and Hybrid NVR box solutions, only the installation upgrade process might apply depending on the existing software version on the unit. For client workstations, the client installation procedure is applicable.

Before you Begin

The client and server computers must meet the hardware and software specifications listed in the respective NVR Data Sheet.

MAXPRO NVR Software - Operating System Prerequisites

Before you install Honeywell MAXPRO NVR software, please note the MAXPRO NVR Server and Client operating system requirements listed in the following section.

- MAXPRO NVR Server

The computer that is designated as the server must run on one of the following operating systems:

- Microsoft® Windows® 8.1 Professional 64-bit or Windows 10 Professional 64-bit must be installed on the NVR before installing MAXPRO NVR software.

- Microsoft® Windows® Server 2008 R2 Standard, Service pack 1 or Windows Server 2012 R2 Standard or Windows Server 2016 must be installed on the NVR before installing MAXPRO NVR Software.
- MAXPRO NVR Client Workstation

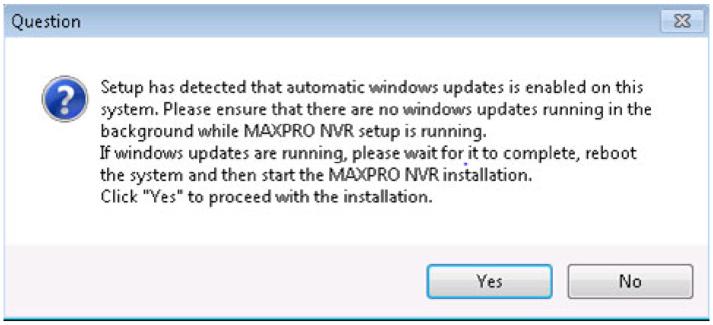
The computer that is designated as the client workstation must run on one of the following operating systems:

- Microsoft® Windows® 7 Professional 32-bit / 64-bit, Service pack 1 or Windows 8.1 Professional 32-bit/64-bit or Windows 10 Professional 32-bit/ 64-bit must be installed on the workstation before installing MAXPRO NVR client software.

Please refer to the *Microsoft® Windows Patches Tested with MAXPRO®NVR* document for further details on Windows updates that have been tested with the current software version shipping with MAXPRO NVRs.

Before you Begin - Windows Updates

If Windows updates are enabled in your system, then Figure warning message appears and the installation continues.

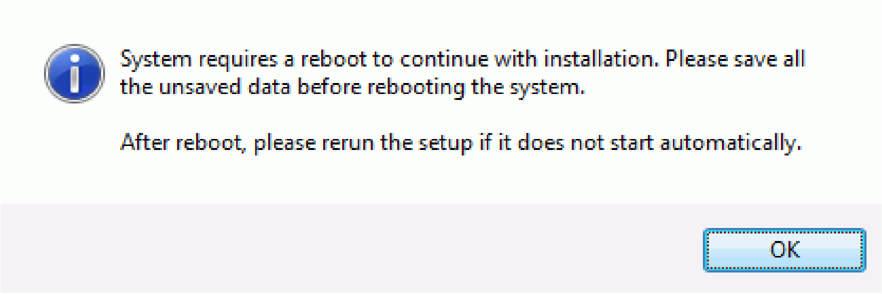


Question

Setup has detected that automatic windows updates is enabled on this system. Please ensure that there are no windows updates running in the background while MAXPRO NVR setup is running.
If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR installation.
Click "Yes" to proceed with the installation.

Automatic Windows Update Enabled Warning Message

If any pending reboot is there due to windows updates, then Figure error message appears, and the installation stops. Please ensure that you reboot your computer after the Windows updates are finished.



System requires a reboot to continue with installation. Please save all the unsaved data before rebooting the system.

After reboot, please rerun the setup if it does not start automatically.

Pending Reboot Error Message

Note: *Ensure that services.msc console is closed before Installing or upgrading the MAXPRO NVR.*

Before you Begin - Disable Defragmentation

Before starting the installation of MAXPRO NVR, it is recommended that you disable Defragmentation.

Step 1. Click Start -> Run -> type DFRGUI.

Step 2. In the Disk Defragmenter dialog click Configure Schedule

Step 3. Click to clear the Run on the schedule (recommended) check box.

Step 4. Click Start, (Right-click) Computer-> Manage, select Task scheduler ->Task scheduler library -> Microsoft -> Windows -> Defrag. Right-click on the ScheduleDefrag and then select Disable.

Step 5. Perform the following steps to make changes in the Registry Settings to disable defragmentation at boot time:

a. Open the Registry Editor. Navigate to HKEY_LOCAL_MACHINE> SOFTWARE> Microsoft> Dfrg> BootOptimizeFunction.

b. Right-click on the keyword "Enable" and then click Edit.

c. In the Value Data field type, N and then click OK.

d. Right-click on the keyword "Optimizecomplete" and then click Edit.

e. In the Value Data field, replace Yes with No. (case sensitive) Click OK.

f. Close the Registry Editor. The changes take effect when Windows is restarted.

Before you Begin - Disable Volume Shadow Copy, Windows Backup Services

Step 1. Turn off the Protection settings for all the drives including OS installed drive in My Computer -> Properties -> Advanced System Settings -> System Protection tab.

Step 2. Select the drive under Protection settings and click Configure.

Step 3. Under Restore Settings select Turn off system protection and click OK.

Before you Begin - Changing the default Windows Administrator Account Created By NVR

Honeywell recommends to login with new Administrator user account for installing MAXPRO NVR. To create a new Administrator user account and to disable the default Administrator account, perform the following two steps as explained in:

- Step 1: Create a new user account with administrator privileges, page 300
- Step 6: Disable the Administrator Account, page 304.

Before you Begin - Installed SQL Service Pack on older SQL Server versions

Install the SQL Service Pack on older SQL Server versions (any SQL version below 2016) to work with MAXPRO VMS. Refer to the ***800-26010-A - Securing MAXPRO VMS-NVR Technical Notes*** for more information.

MAXPRO NVR Software Installation

To complete the MAXPRO NVR software installation follow the procedures in these sections:

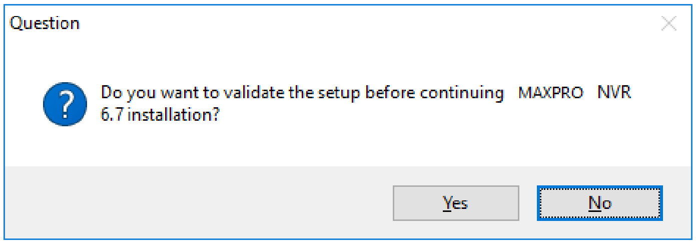
Step 1. First complete, How to Install MAXPRO NVR

Step 2. Choose the installation that best suits your requirements, and follow the appropriate steps.

- Full Installation: Full installation can be selected to install the Server and Client on the same system.
- Client Installation: Client installation can be selected to install MAXPRO NVR desktop client on the client workstations.

How to Install MAXPRO NVR

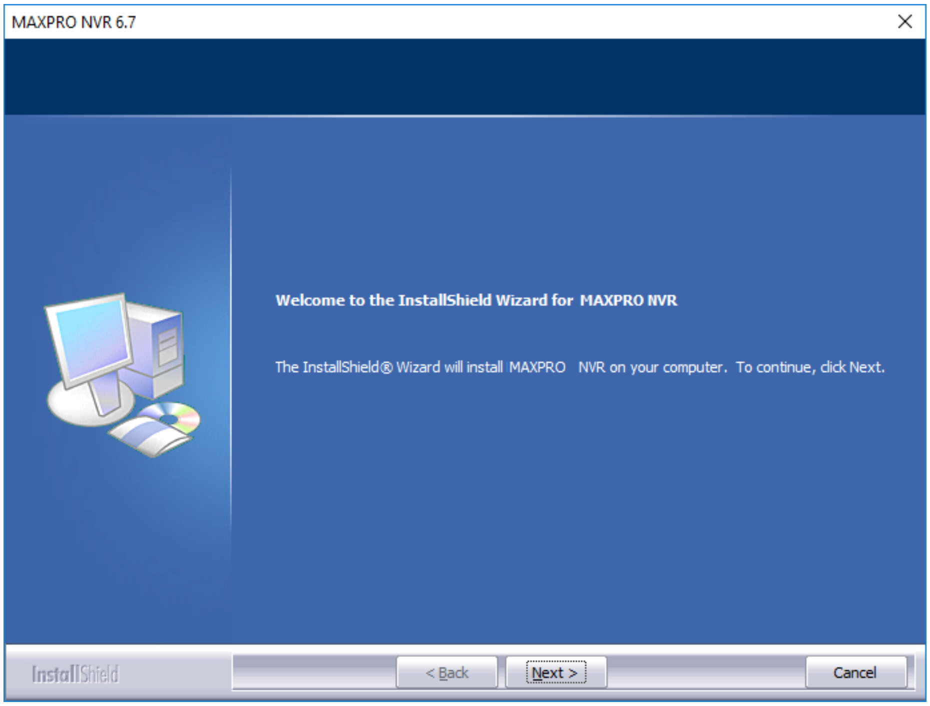
1. Insert the MAXPRO NVR 6.7 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse the DVD drive, and double-click setup.exe. A message box appears as shown below.



Question

Do you want to validate the setup before continuing MAXPRO NVR 6.7 installation?

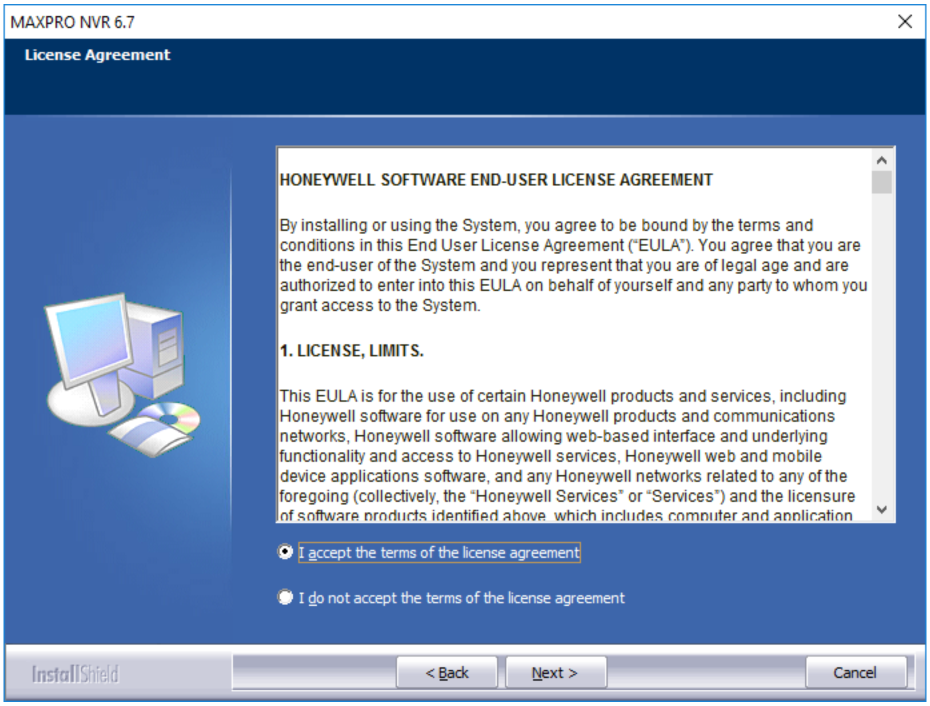
2. Click Yes to validate the setup files are not corrupted before continuing the installation and click No to skip the validation to continue the setup. The Welcome installation wizard appears as shown below.



Welcome to the InstallShield Wizard for MAXPRO NVR

The InstallShield® Wizard will install MAXPRO NVR on your computer. To continue, click Next.

3. Click Next. The License Agreement screen appears.



HONEYWELL SOFTWARE END-USER LICENSE AGREEMENT

By installing or using the System, you agree to be bound by the terms and conditions in this End User License Agreement ("EULA"). You agree that you are the end-user of the System and you represent that you are of legal age and are authorized to enter into this EULA on behalf of yourself and any party to whom you grant access to the System.

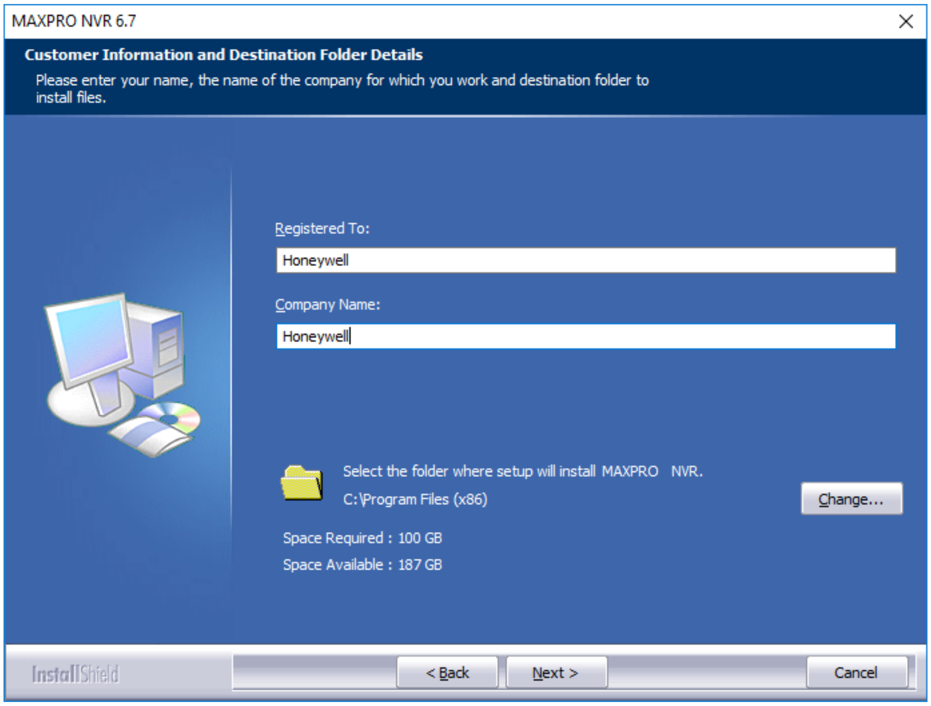
1. LICENSE, LIMITS.

This EULA is for the use of certain Honeywell products and services, including Honeywell software for use on any Honeywell products and communications networks, Honeywell software allowing web-based interface and underlying functionality and access to Honeywell services, Honeywell web and mobile device applications software, and any Honeywell networks related to any of the foregoing (collectively, the "Honeywell Services" or "Services") and the licensure of software products identified above, which includes computer and application

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

4. Read the license agreement, and then select I accept the terms of the license agreement. Click Next, the Customer Information screen appears.



MAXPRO NVR 6.7

Customer Information and Destination Folder Details

Please enter your name, the name of the company for which you work and destination folder to install files.

Registered To: Honeywell

Company Name: Honeywell

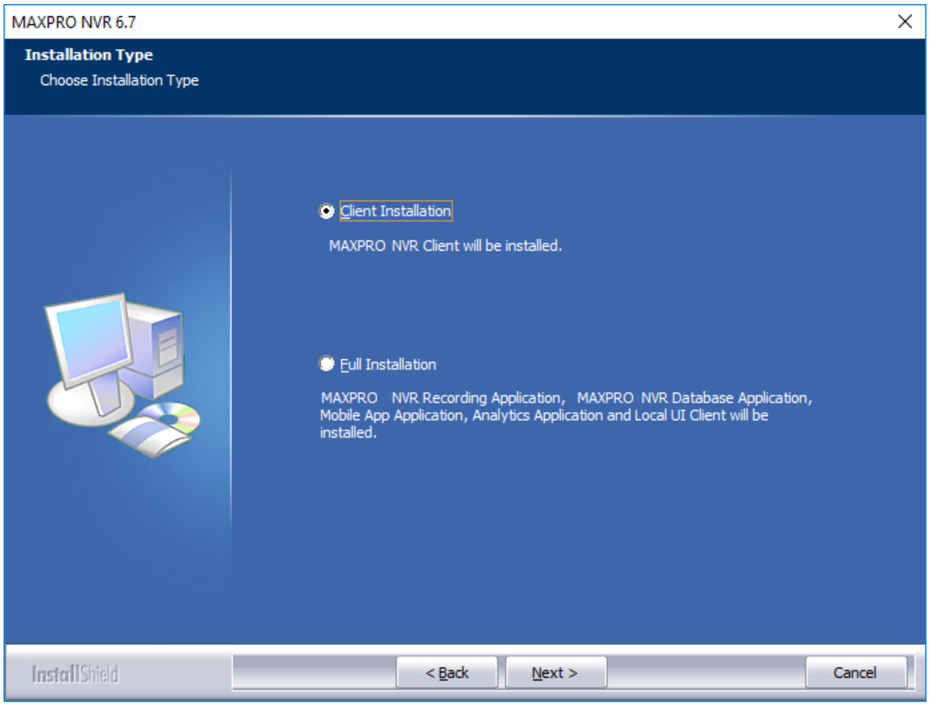
Select the folder where setup will install MAXPRO NVR.

C:\Program Files (x86)

Space Required : 100 GB

Space Available : 187 GB

5. Type your Registered To name.
6. Type your Company Name.
7. Click Change if you want to change the destination folder, and then select the folder where MAXPRO NVR must be installed.
8. Click Next. The Choose Installation Type wizard is displayed.



MAXPRO NVR 6.7

Installation Type

Choose Installation Type

● Client Installation

MAXPRO NVR Client will be installed.

○ Full Installation

MAXPRO NVR Recording Application, MAXPRO NVR Database Application, Mobile App Application, Analytics Application and Local UI Client will be installed.

9. Select the Client Installation or Full Installation as it applies to your system installation.

Select Features to Install

Full Installation Note: Full Installation is only needed for Software solutions.	Installs Trinity Framework, MAXPRO NVR Recording Application, MAXPRO NVR Database Application, Mobile App Application, Analytics Application and MAXPRO NVR Client on the same computer. See the See "Full Installation" on page 107 for more information.
Client Installation	Installs Client, Trinity Framework, and Adapters. See the See "Client Installation" on page 114 for more information.

Full Installation

MAXPRO NVR 6.7 Full installation can be selected to install the Server and Client on the same system.

Note: *Full Installation is only needed for Software solutions. Don't install any Email client on the MAXPRO NVR server machine.*

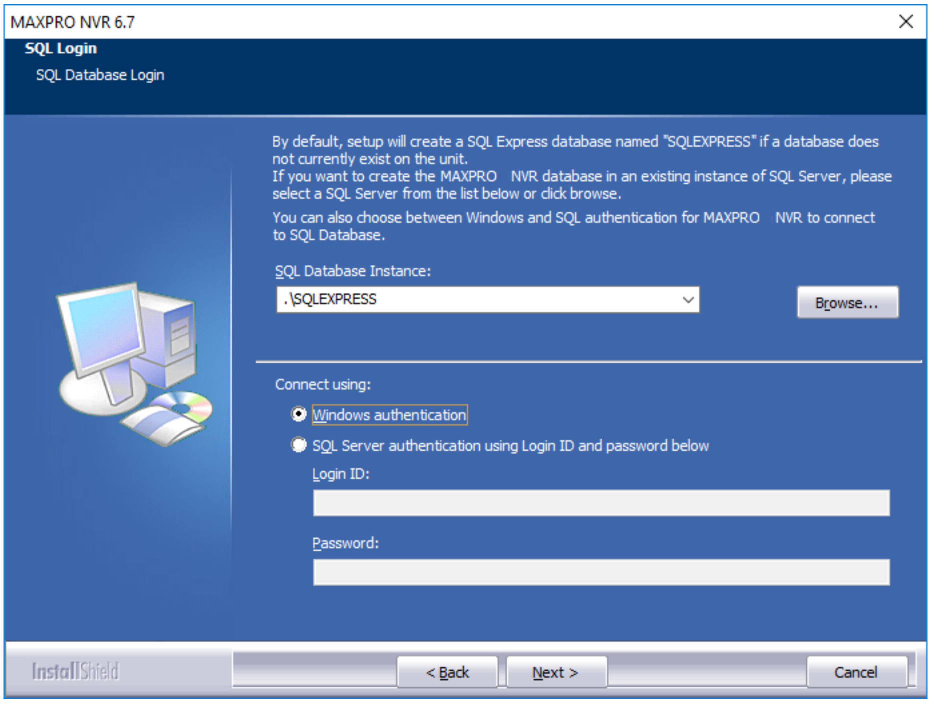
To perform a full installation

1. Perform steps 1 through 9 of How to Install MAXPRO NVR, and then select the Full Installation option in the Choose Installation Type screen appears.
2. Click Next. The Choose Installation Type screen appears.
3. You have two options to choose from:

- Fresh Installation: Select this option if you are installing MAXPRO NVR for the first time and then click Next. The SQL Login screen appears.

Or

- Upgrade Existing Installation: Select this option if you want to retain/restore the configuration settings from a backup of the previously installed version of MAXPRO NVR and click Next. The SQL Login screen appears.



MAXPRO NVR 6.7

SQL Login

SQL Database Login

By default, setup will create a SQL Express database named "SQLEXPRESS" if a database does not currently exist on the unit.
If you want to create the MAXPRO NVR database in an existing instance of SQL Server, please select a SQL Server from the list below or click browse.

You can also choose between Windows and SQL authentication for MAXPRO NVR to connect to SQL Database.

SQL Database Instance: .\SQLEXPRESS

Connect using:

● Windows authentication

○ SQL Server authentication using Login ID and password below

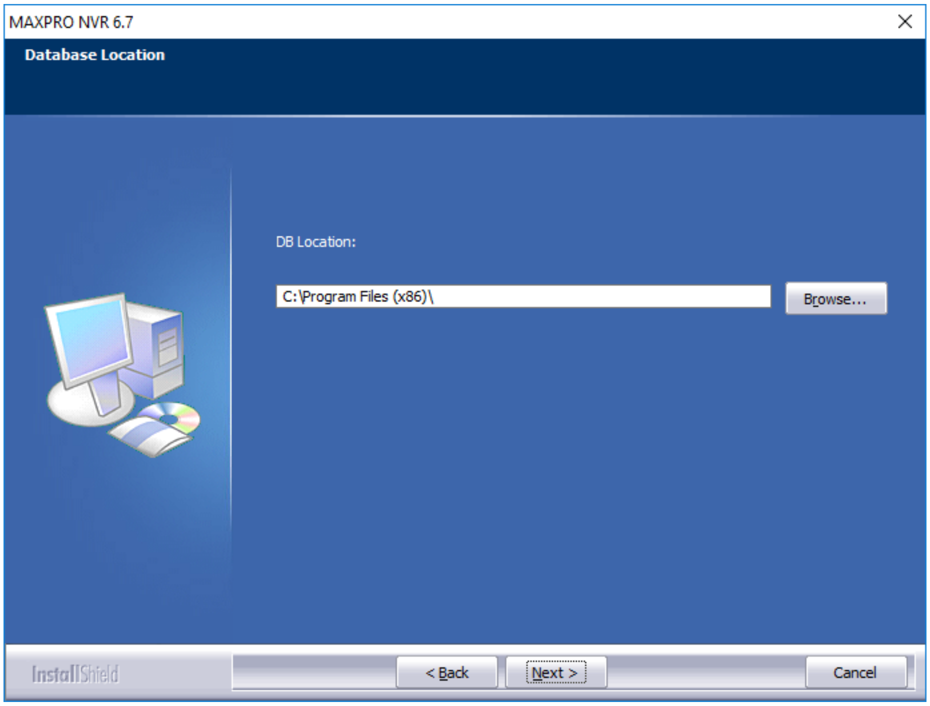
Login ID:

Password:

4. Click Browse, and then select any existing SQL database server instance, such as the existing SQL database server instance on the same network. If you do not want to select an existing database server instance, proceed to step 5.
5. Select Connect using option as Windows authentication or SQL Server authentication. If you select SQL Sever authentication, type the Log on ID and Password.

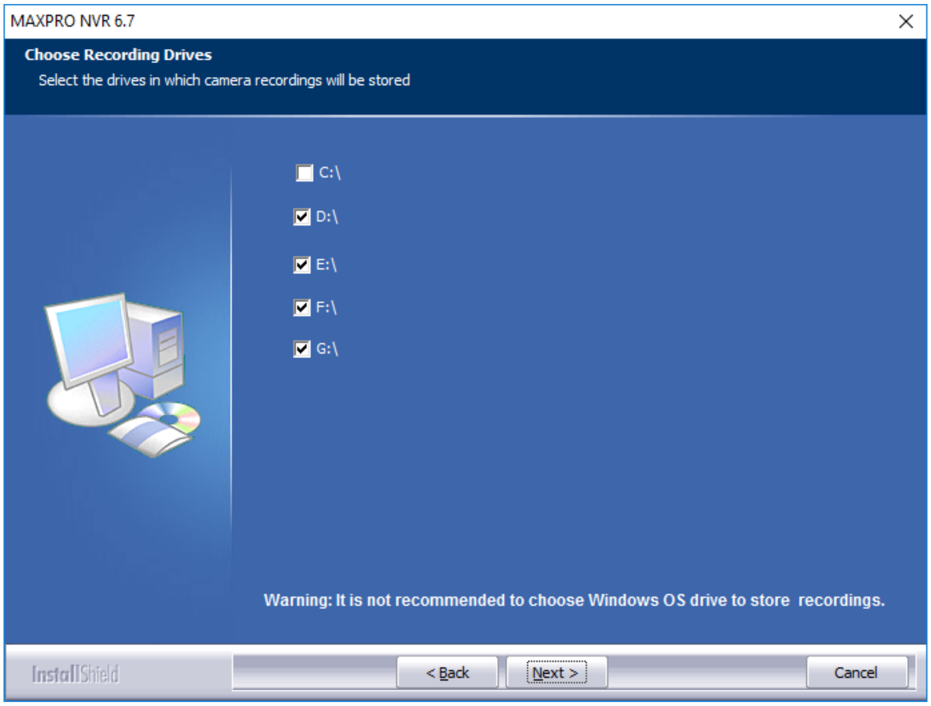
Note: *If you are installing MAXPRO NVR on a new computer that does not have SQL Server 2012 Express installed, you will be prompted to install it. Follow the on-screen instructions to complete the installation. In addition VC++ 2008 redistributable will be installed as a prerequisite as part of MAXPRO NVR installation.Refer What' New Release Notes for more information on issues.*

6. Click Next. The SQL credentials validation status appears. After successful validation, the Choose Database Location screen appears.



7. There are two scenarios that are possible here, depending on your installation type:

- For Fresh installation of a MAXPRO NVR Database: The default path where the MAXPRO NVR database is created automatically displays for a MAXPRO NVR database fresh installation. Click Next to use the default path or click Browse to select a new path if necessary and then click Next. The Choose Recording Drives screen appears.
- To retain the existing MAXPRO NVR Database: The path where the MAXPRO NVR database is saved for a previously installed version of the MAXPRO NVR software automatically displays. Click Next. A message “Trinity Database file already exists. Do you want to retain the database” appears shown below. If you
  - Click Yes. The Localization Support screen appears.
  - Click No. The Choose Recording Drives screen appears.


MAXPRO NVR 6.7

Choose Recording Drives

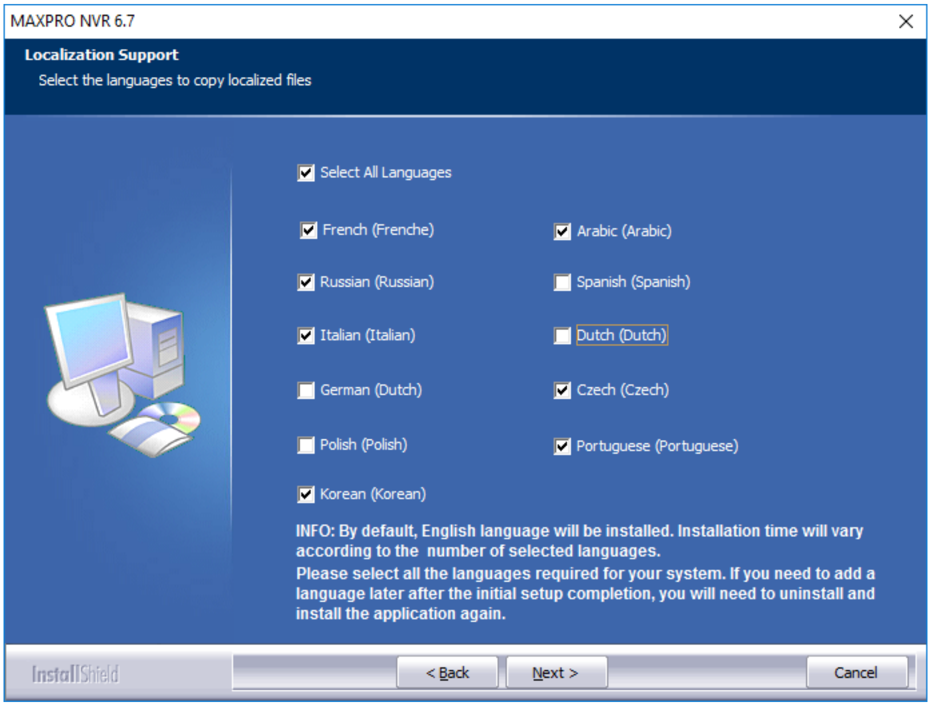
Select the drives in which camera recordings will be stored

□ C:\
☑ D:\
☑ E:\
☑ F:\
☑ G:\

Warning: It is not recommended to choose Windows OS drive to store recordings.

8. Select the drive check box for the drive on which to save the camera recordings (to use as a video storage drive) and click Next. The Localization Support screen appears.

Caution: It is recommended that you do not choose the operating system drive for saving the camera recordings (as a video storage drive). Selecting an Operating System drive for video storage can lead to system instability and crash.


MAXPRO NVR 6.7

Localization Support

Select the languages to copy localized files

☑ Select All Languages

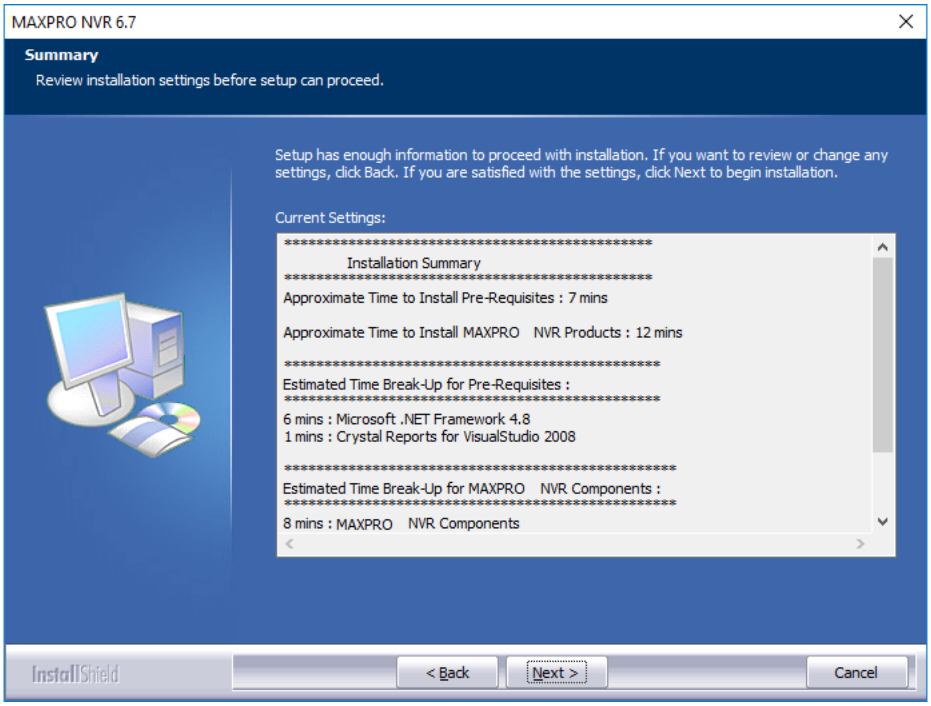
☑ French (Frenche)
☑ Arabic (Arabic)
☑ Russian (Russian)
□ Spanish (Spanish)
☑ Italian (Italian)
□ Dutch (Dutch)
□ German (Dutch)
☑ Czech (Czech)
□ Polish (Polish)
☑ Portuguese (Portuguese)
☑ Korean (Korean)

INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.
Please select all the languages required for your system. If you need to add a language later after the initial setup completion, you will need to uninstall and install the application again.

Caution: By Default, English language will be installed. Please ensure to select all the languages required for your system. If an additional language is required after the installation is completed, the software will need to be uninstalled and installed again.

Note: *Only English language will be supported/installed in Beta release.*

9. Select the languages in which you want to install MAXPRO NVR and then click Next. The Installation Summary screen appears.



MAXPRO NVR 6.7

Summary

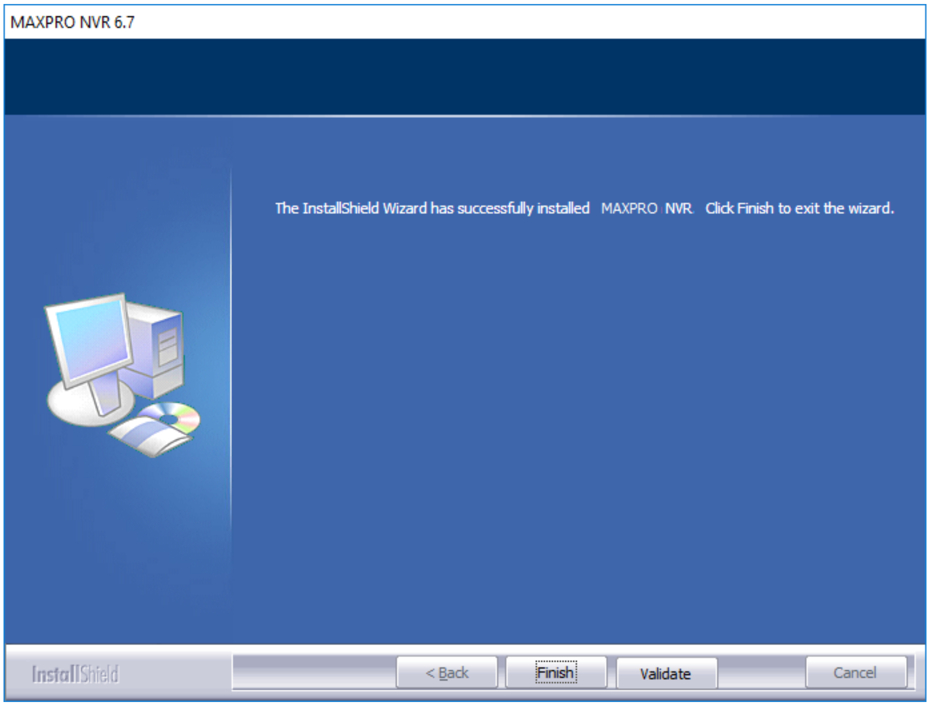
Review installation settings before setup can proceed.

Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

```
**************************************************
          Installation Summary
**************************************************
Approximate Time to Install Pre-Requisites : 7 mins

Approximate Time to Install MAXPRO   NVR Products : 12 mins

***************************************************
Estimated Time Break-Up for Pre-Requisites :
***************************************************
6 mins : Microsoft .NET Framework 4.8
1 mins : Crystal Reports for VisualStudio 2008

*****************************************************
Estimated Time Break-Up for MAXPRO   NVR Components :
*****************************************************
8 mins : MAXPRO   NVR Components
```

10. If you want to change any settings, click Back, else click Next. When the installation is complete, the following message is displayed. The approximate time for installing the prerequisites and MAXPRO NVR Products displays.


MAXPRO NVR 6.7

The InstallShield Wizard has successfully installed MAXPRO NVR. Click Finish to exit the wizard.

11. Click OK. The Finish dialog appears with the options to Validate and to Finish the installation.
    - Click Validate to verify the installed files on your NVR. If there are no errors then a message appears - Setup has been validated successfully without any error. Click here to view report. If there are errors, the message shows there are errors and the report can be reviewed to identify the error and contact Honeywell technical support if required to correct them on reinstall.
    - Click Finish. The installation wizard starts all the services which may take a few minutes. After the wizard closes, as mentioned in step 10 it is recommended to Restart the system manually for the changes to take effect. If you are prompted to reboot the system then a confirmation message is displayed.
12. Click OK to complete the MAXPRO NVR installation.

Installing Web Client

By default MAXPRO NVR 6.7 installs the Web Client component on your machine. It also installs the MAXPROWEBConfigurator utility to change or update the system and server configuration. If you want to access the MAXPRO NVR Server using Web Client remotely through a supported web browser then you should install Silverlight on the remote machine.

Caution: For better security, close the browser upon logout.

Prerequisites to access MAXPRO NVR Server through Web Client

The following are the prerequisites to access the MAXPRO NVR server through Web Client:

- Silverlight: Ensure that Silverlight version 5 and above is installed on your machine. If you don't have the Silverlight plug-in on your machine, you can download it from the following Microsoft link. http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx

Note: *Silverlight plug-in is not supported by Chrome version 42.x or above and Microsoft Edge browser.*

- Web Browsers Supported on Windows Systems: Ensure that at least one of the following supported web browsers are installed on your PC:
  - Internet Explorer version 8 or above
  - Firefox version 15.0.1 or above
  - Chrome version 32.x to 41.x only.

Note: *MAXPRO NVR Web Client is only supported for the below Web Browsers on Windows 10 with Silverlight plug-in installed:*

- Internet Explorer version 11 or above
- Firefox version 40 or above

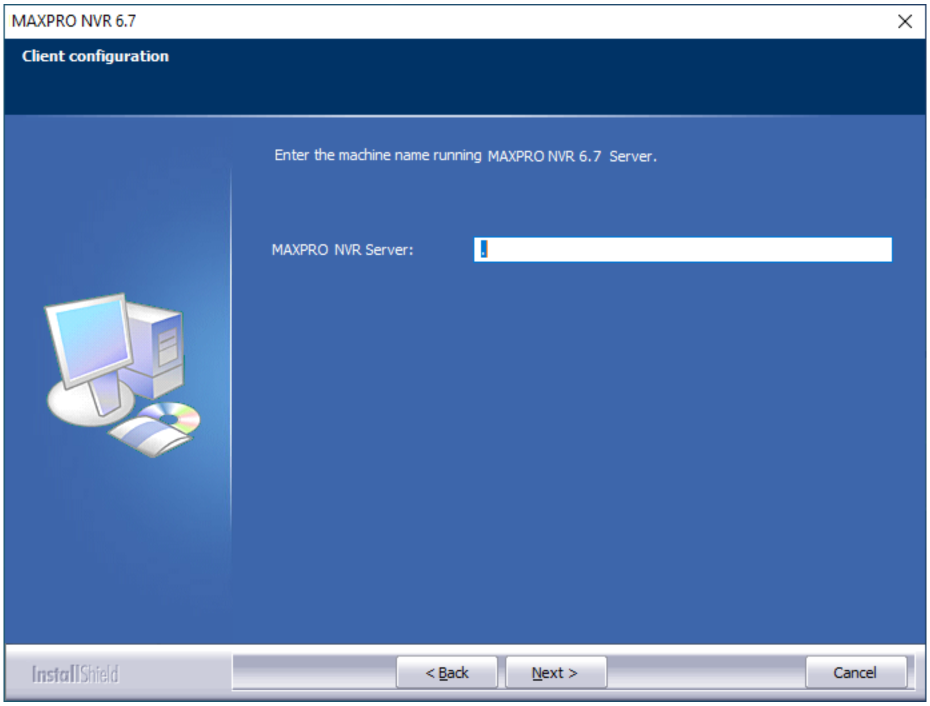
Caution: For better security, close the browser upon logout.

- Web Browsers Supported on MAC systems: Not supported.

Client Installation

MAXPRO NVR 6.7 Client installation gives you an option to install MAXPRO NVR Client on the client workstations.

1. Select Client Installation in Choose Installation Type screen and then click Next. The Client Configuration screen appears.



MAXPRO NVR 6.7

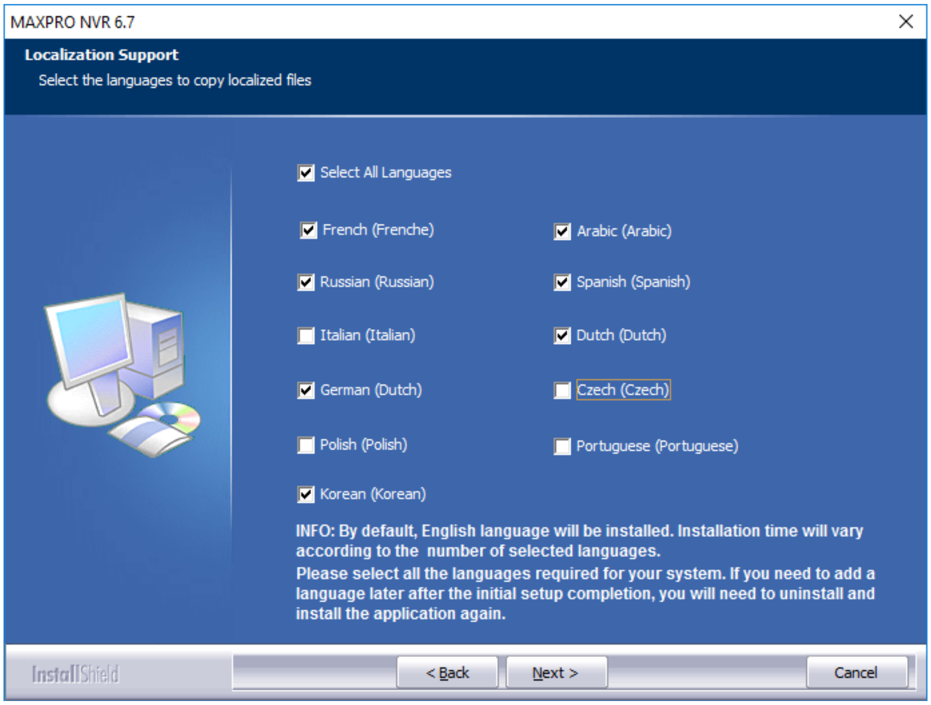
Client configuration

Enter the machine name running MAXPRO NVR 6.7 Server.

MAXPRO NVR Server: .

2. Type the MAXPRO NVR Server name or IP address, and then click Next. The Localization Support screen appears.

Note: *If you do not know the server name or if the server is not accessible, then type the local host/computer name. The server name can be changed after the installation in the Client.*



MAXPRO NVR 6.7

Localization Support

Select the languages to copy localized files

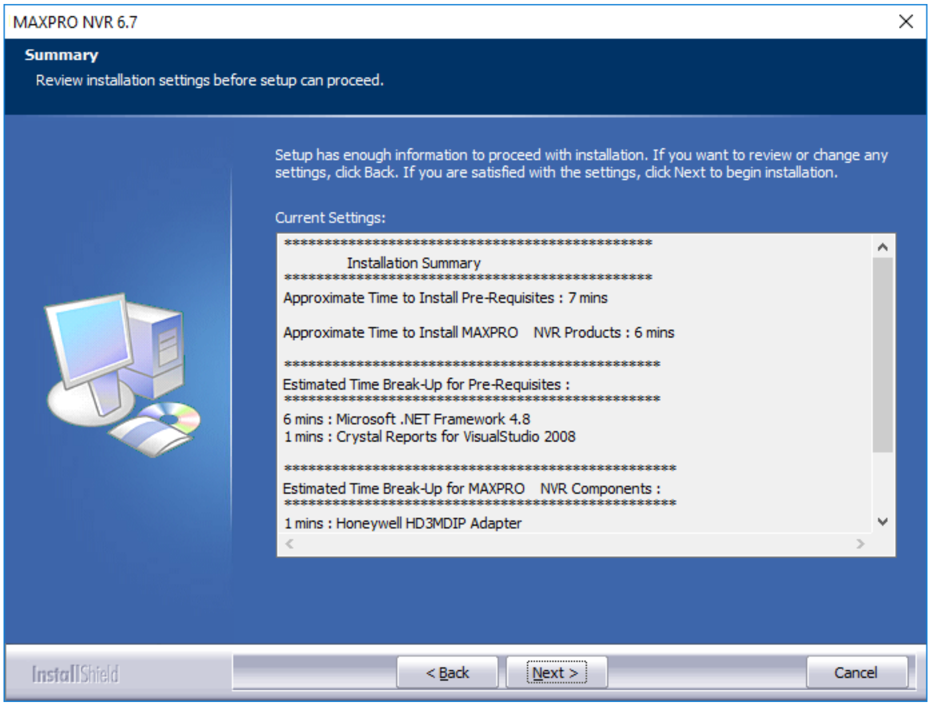
☑ Select All Languages

☑ French (Frenche)	☑ Arabic (Arabic)
☑ Russian (Russian)	☑ Spanish (Spanish)
□ Italian (Italian)	☑ Dutch (Dutch)
☑ German (Dutch)	□ Czech (Czech)
□ Polish (Polish)	□ Portuguese (Portuguese)
☑ Korean (Korean)	

INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.
Please select all the languages required for your system. If you need to add a language later after the initial setup completion, you will need to uninstall and install the application again.

Caution: By Default, English language will be installed. Please ensure to select all the languages required for your system. If an additional language is required after the installation is completed, the software will need to be uninstalled and installed again.

3. Select the languages in which you want to install MAXPRO NVR and then click Next. The Installation Summary screen appears.



MAXPRO NVR 6.7

Summary

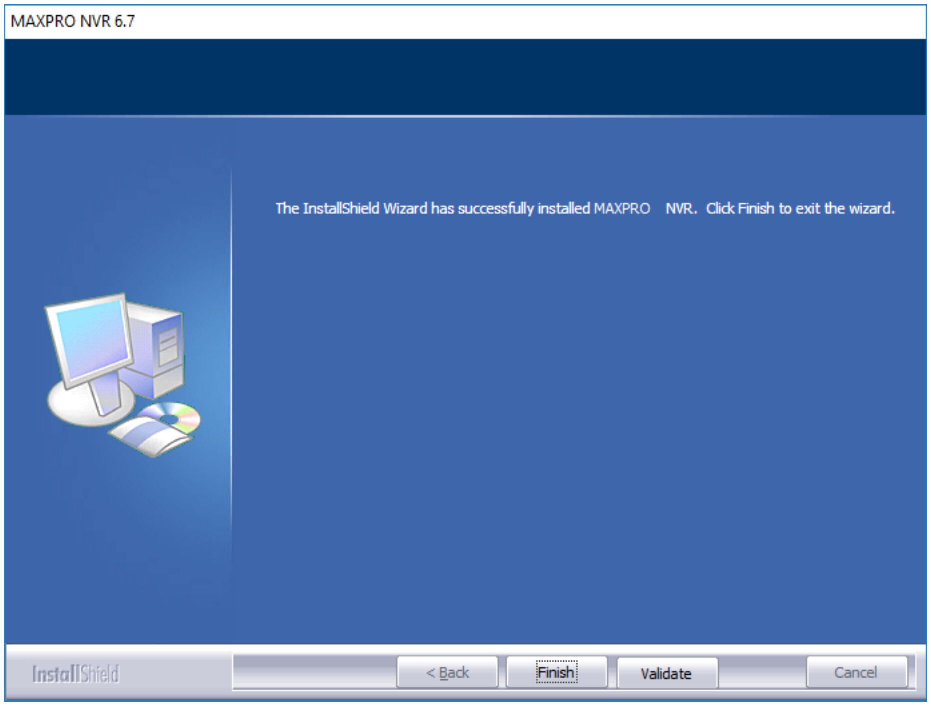
Review installation settings before setup can proceed.

Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

```
****************************************************
         Installation Summary
****************************************************
Approximate Time to Install Pre-Requisites : 7 mins

Approximate Time to Install MAXPRO   NVR Products : 6 mins

*****************************************************
Estimated Time Break-Up for Pre-Requisites :
*****************************************************
6 mins : Microsoft .NET Framework 4.8
1 mins : Crystal Reports for VisualStudio 2008

*******************************************************
Estimated Time Break-Up for MAXPRO   NVR Components :
*******************************************************
1 mins : Honeywell HD3MDIP Adapter
```

4. If you want to review or change any settings click Back, otherwise click Next. The setup status of various components appears.When the installation is complete, the following message is displayed.



MAXPRO NVR 6.7

The InstallShield Wizard has successfully installed MAXPRO   NVR. Click Finish to exit the wizard.

5. Click OK. The Finish dialog appears. Click Finish. The installation wizard starts all the services which may take a few minutes. After the wizard closes, it is

recommended to Restart the system manually for the changes to take effect. If you are prompted to reboot the system then the reboot message is displayed.

6. Click OK to complete the MAXPRO NVR Client installation.

Uninstalling MAXPRO NVR

To uninstall MAXPRO NVR, choose any of the following uninstall procedures that best suit your requirement.

- Client uninstall
- Full uninstall

Client Uninstall

Choose this option to uninstall MAXPRO NVR Client components.

To uninstall the client

Step 1. Go to Control Panel->Programs and Features, select the MAXPRO NVR Client and click uninstall.

Or

Insert the MAXPRO NVR setup DVD in the DVD drive, browse the DVD drive, and then double-click Setup.exe.

Or

Go to the MAXPRO NVR setup folder on your computer, and then double-click Setup.exe. The uninstall wizard starts.

Step 2. Click Next. The message “Do you want to completely remove the selected application and all of its features” appears. The uninstall status of various components appears.

Step 3. Click Finish. You are prompted to reboot your computer to complete the uninstall procedure.

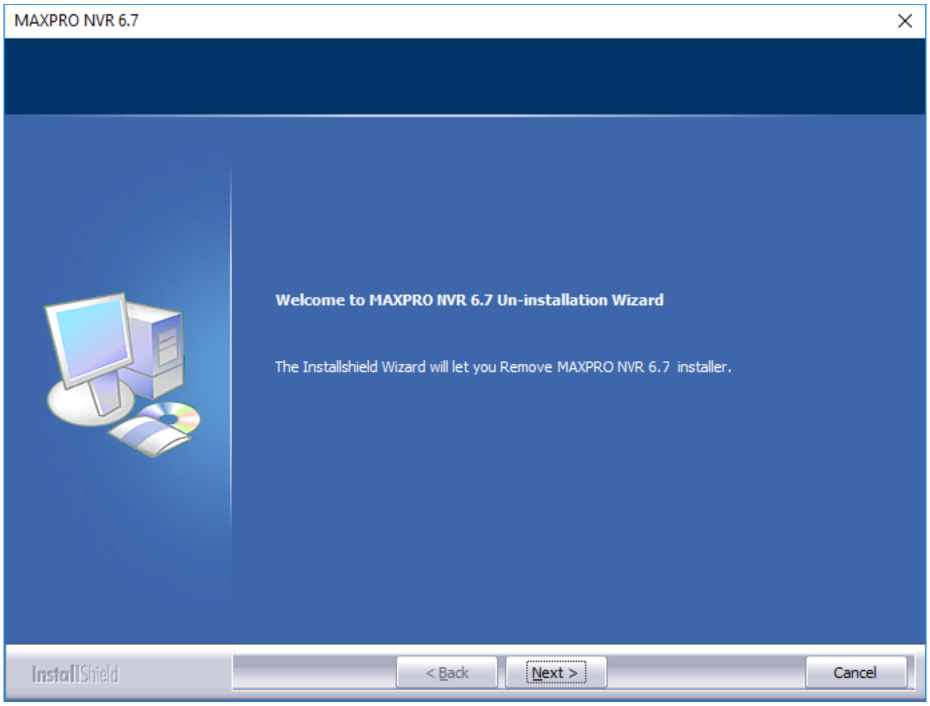
Full Uninstall

The following components are uninstalled: MAXPRO NVR Server and Client components. You can choose the option to retain a backup of database and clip (recording) metadata as per your input during the full uninstall process.

To perform full uninstall

Step 1. Go to Control Panel->Programs and Features, select MAXPRO NVR 6.7 and click uninstall.
Or
Insert the MAXPRO NVR setup DVD in the DVD drive, browse the DVD drive, and then double-click Setup.exe.

Or
Go to the MAXPRO NVR setup folder on your computer, and then double-click Setup.exe. The uninstall Welcome wizard is displayed.

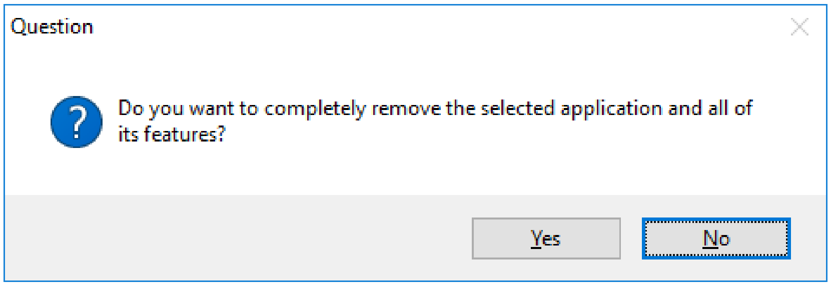


MAXPRO NVR 6.7

Welcome to MAXPRO NVR 6.7 Un-installation Wizard

The Installshield Wizard will let you Remove MAXPRO NVR 6.7 installer.

A message Do you want to completely remove the selected application and all of its feature? is displayed.Click Yes or No as applicable.



Question

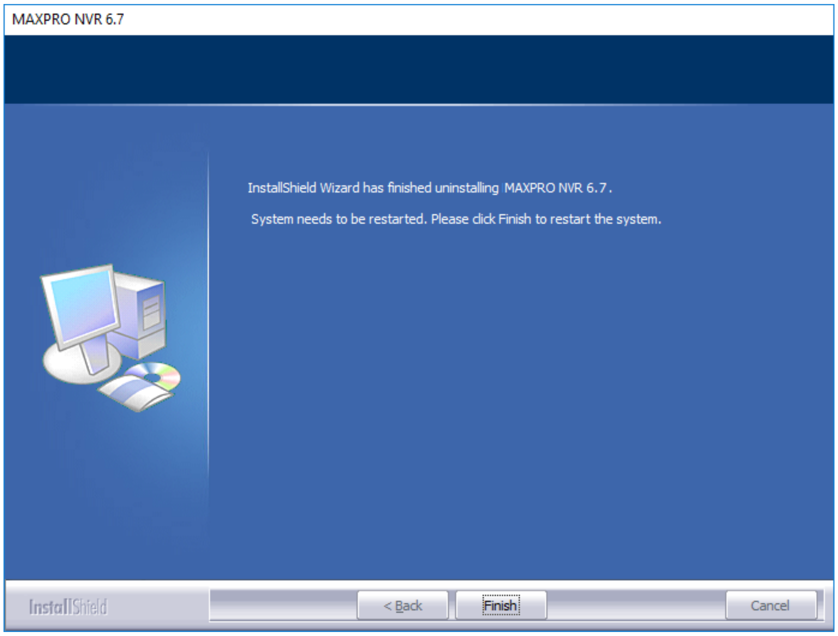
Do you want to completely remove the selected application and all of its features?

Step 2. Click Yes. The Restoring Trinity Database screen is displayed.

Step 3. Click Yes or No as applicable.

- If you click “Yes” and then click Browse to specify a new path for backup location for storing the database. Click Next, the database is retained for future installations of MAXPRO NVR. The uninstall status of various componentsappears and uninstallation finish screen appears.

- If you click “No” and then click Yes to confirm deleting the Trinity database. The database is deleted. The uninstall status of various components appears and uninstallation finish screen appears.



InstallShield Wizard has finished uninstalling MAXPRO NVR 6.7.

System needs to be restarted. Please click Finish to restart the system.

Installation Finish

Step 4. Click Finish. The uninstall wizard closes and you are prompted to reboot your computer.

NetBIOS Naming Convention Limitations

This section describes the naming conventions for computer accounts in Microsoft Windows, NetBIOS domain names, DNS domain names, Active Directory sites, and organizational units (OUs) that are defined in the Active Directory directory service.

For MAXPRO NVR

In remote connection scenario, the NVR Hostname will be more than 15 characters. However, NetBIOS naming convention supports only 15 characters for hostname.

- If user is trying to connect to a database and if it failing, then ensure that the hostname of the computer is not more than 15 characters.

Refer the following Microsoft web page of more details on NetBIOS limitations.

https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

This page is intentionally left blank

CHAPTER

6 LOGGING ON AND GETTING STARTED

In this chapter...

Logging on Using Profiles

The MAXPRO NVR server addresses are saved in profiles. You need to select the profile before logging on. You can set a profile as the default profile. When a profile is set as the default, you do not need to select the profile each time you log on to MAXPRO NVR. You can also modify and delete profiles.

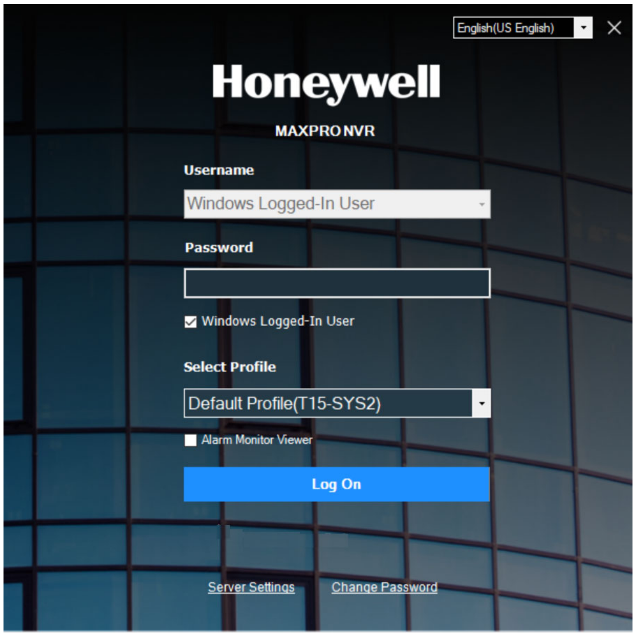
Logging on to MAXPRO NVR

Caution: On Honeywell provided systems shipped with v4.0 or later version, a default Windows user: NVR-Admin with password: Password$123 is already configured and hence you are automatically logged on. Honeywell recommends you to create and use a new Administrator account to install and logon to MAXPRO NVR. See Securing MAXPRO NVR **section on page** 299 **for more information. Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.**

Step 1. Double-click on the desktop. The Log On dialog box appears.

Or

Click Start -> Programs -> Honeywell -> MAXPRO NVR. The Log On dialog box (MAXPRO NVR Log on dialog box) appears.



English(US English)

Honeywell

MAXPRO NVR

Username

Windows Logged-In User

Password

☑ Windows Logged-In User

Select Profile

Default Profile(T15-SYS2)

□ Alarm Monitor Viewer

Log On

Server Settings

Change Password

MAXPRO NVR Log on dialog box

Step 2. Click the Language option, and then select the required language from the drop-down list. The supported languages (selected during installation) are Arabic, Czechoslovakian, Dutch, Polish, Portuguese, French, German, Russian, Italian, Spanish, Korean and English. The default language is English (US English).

Step 3. Clear the Windows Logged-In User check box and then enter your Username. The default user name is admin. Honeywell recommends to create a new NVR user (See Adding a User) in the Configurator tab and use the same to logon.

Step 4. Type your Password. The default password is trinity.

Note: *Honeywell recommends you to change the default Password before you logon to MAXPRO VMS. See Changing the Default Password section to change the password. See* Securing MAXPRO NVR *chapter for more details on security settings. See* Password Complexity and Expiry Enhancements *section for more information on password setting.*

Note: *Select the Windows Logged-In User check box for logging on using the Windows authentication (uses current logged in Windows account credentials). If the Windows Logged-In User check box is cleared, the MAXPRO NVR user name and password is used for authentication. Ensure that you avoid using the @ character in your password. Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.*

Step 5. If there is no profile set as default, then select the Profile corresponding to the MAXPRO NVR server to which you want to connect.

Note: *Set profiles if you have multiple MAXPRO NVRs and use the drop-down to choose which NVR you would like to connect to.*

Step 6. Click Login. The Viewer tab appears.

Tips for Logging on

- Click the Language option, and then select the required language from the drop-down list. The supported languages are Arabic, Czechoslovakian, Dutch, Polish, Portuguese, French, German, Russian, Italian, Spanish, and English. The default language is English (US English).
- Select the Windows Logged-In User check box for logging on using the Windows authentication (uses current logged in Windows account credentials). If the Windows Logged-In User check box is cleared, the MAXPRO NVR user name and password is used for authentication.
- Ensure that you avoid using the @ character in your password.
- Set profiles if you have multiple MAXPRO NVRs and use the drop-down list to choose which NVR you would like to connect to.
- Select the Display Video on Alarm check box to display the viewer as an alarm monitor.

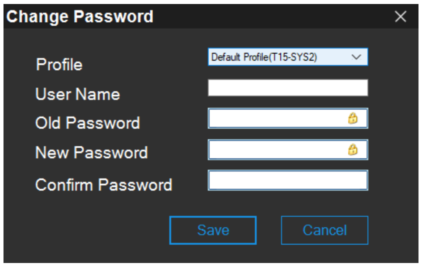
Note: *Alarm monitor supports pop-up of camera associated to IO events only. Pop-up on motion alarms is not currently supported.*

Changing the Default Password

Honeywell recommends you to change the default password and create a new password before logging on to MAXPRO NVR software. See Securing MAXPRO NVR for more security settings.

To change the default password:

Step 1. In the NVR login screen, click Change Password. The Change Password dialog box appears.



Change Password

Profile: Default Profile(T15-SYS2)

User Name

Old Password

New Password

Confirm Password

Step 2. Select the Profile from the drop-down list for which you want to change the password.

Step 3. Type the Username. For Fresh installation admin is the user name.

Step 4. Type the Old Password.

Note: *Old password is blank for Fresh installations. In upgrade scenarios, enter the old password which is configured before upgrading. See* Securing MAXPRO NVR *for more security settings. See* Password Complexity and Expiry Enhancements *section for more information on password setting*

Step 5. Type the New password. See Password Requirement .

Step 6. Type the new password once again to Confirm Password.

Step 7. Click Save.

Password Requirement

Ensure that the new password must meet the following requirements.

1. Minimum length – 12 and Maximum length – 20
2. Password should consists one number, one uppercase letter and one special character.
   a. Number– a digit zero through nine in any script except ideographic scripts.
   b. Uppercase letter – any kind of letter from any language which has uppercase variant.
   c. Special character – any kind of punctuation character – any kind of hyphen, dash, opening bracket, closing bracket, quotes, underscore etc

Configuring MAXPRO NVR Windows/ Desktop Client

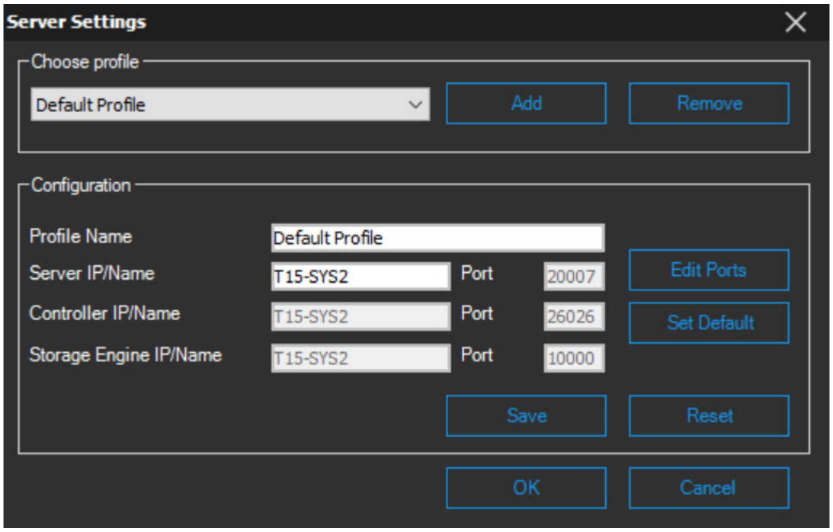
Managing Profiles

Saving a Server Address in a Profile

To save a server address

Step 1. In the client workstation, double-click the icon on the desktop to display the Log On dialog box.

Step 2. Click Server Settings. The Server Settings dialog box appears (Server Settings dialog box).



Server Settings

Choose profile: Default Profile

Configuration

Profile Name: Default Profile

Server IP/Name: T15-SYS2 Port 20007

Controller IP/Name: T15-SYS2 Port 26026

Storage Engine IP/Name: T15-SYS2 Port 10000

Server Settings dialog box

Step 3. Click Add.

Step 4. Type the Profile Name to identify the profile.

Step 5. Type the Server IP/Name (numerical IP address or the network name of the MAXPRO NVR server).

Step 6. Click Save.

Step 7. Click OK. The server address is saved in the profile.

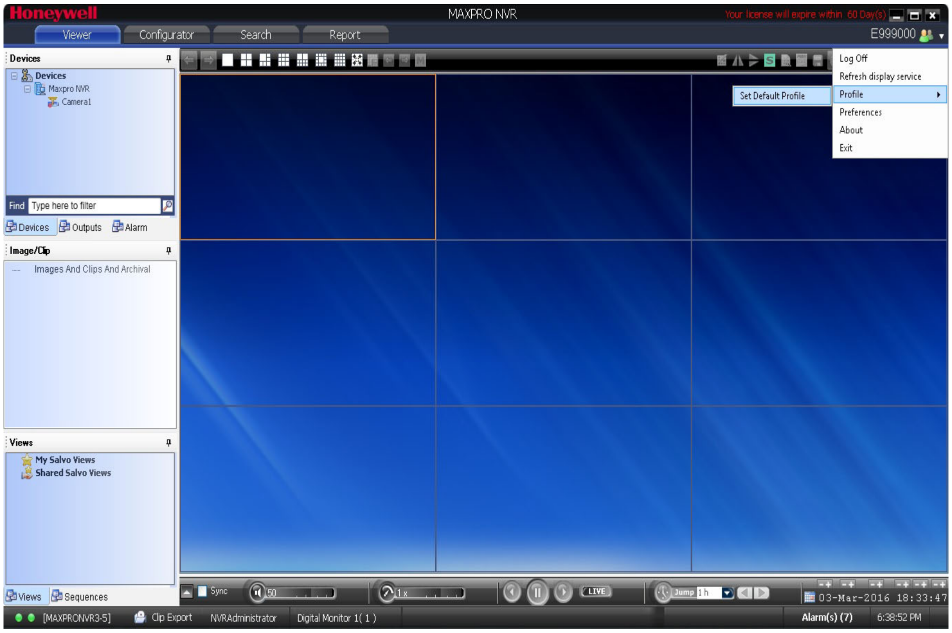
Tip: You can click Set Default in the server settings dialog box to set the profile as the default profile.

Setting the Default Profile

To set the default profile

Step 1. Select the profile you want to set as default before logging on to the MAXPRO NVR.

Step 2. In the User menu, , click Profiles > Set Default Profile. The profile is set as the default profile. The default profile appears selected in the Profile box in the Log On dialog box.



Setting the Default Profile

Modifying a Profile

You can modify the profile name and the server address saved in the profile.

To modify a profile

Step 1. In the client workstation, double-click the icon on the desktop to display the Log On dialog box.

Step 2. Click Server Settings. The Server Settings dialog box appears.

Step 3. In the Choose Profile box, select the profile you want to modify. The profile details appear under Configuration in the Server Settings dialog box.

Step 4. Change the Profile Name, as applicable.

Step 5. Change the Server IP/Name, as applicable.

Step 6. Click Save.

Step 7. Click OK. The profile is modified.

Deleting a Profile

Step 1. In the client workstation, double-click the icon on the desktop to display the Log On dialog box.

Step 2. Click Server Settings. The Server Settings dialog box appears.

Step 3. In the Choose Profile box, select the profile you want to delete.

Step 4. Click Remove.

Step 5. Click OK. The profile is deleted.

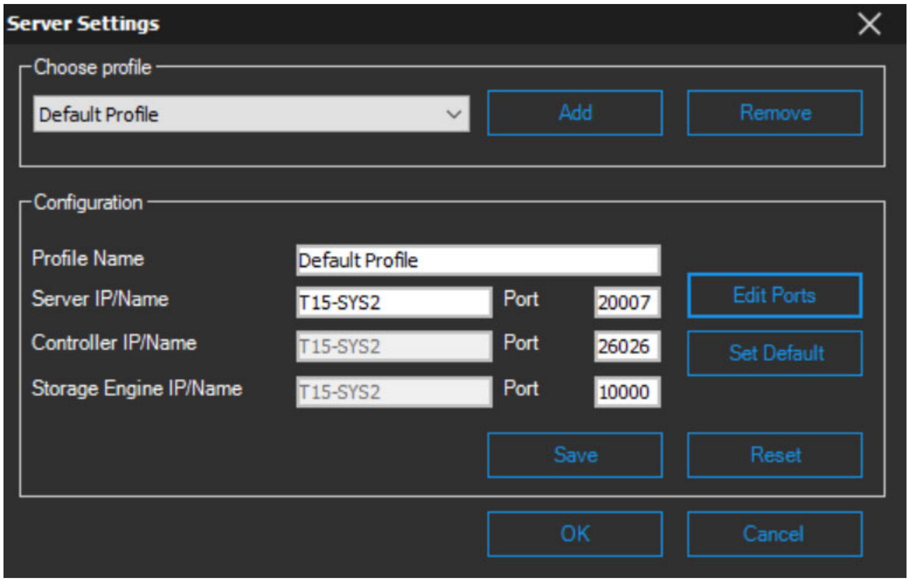
Editing the Ports

The MAXPRO NVR user interface includes a provision to modify the port number used by MAXPRO NVR client to connect to the following components:

- Trinity Server
- Trinity Controller
- NeoEngine Server

To edit the ports:

Step 1. In the Server Settings dialog box, click Edit Ports. The port numbers associated to Server IP/Name, Controller IP/Name and Storage Engine IP/Name are enabled for editing.



Choose profile: Default Profile

Profile Name	Default Profile		
Server IP/Name	T15-SYS2	Port	20007
Controller IP/Name	T15-SYS2	Port	26026
Storage Engine IP/Name	T15-SYS2	Port	10000

Editing the Ports

Step 2. Change the port numbers, as applicable.

Step 3. Click Save.

Note: *Port 20000 is used for ONVIF discovery.*

Port Forwarding

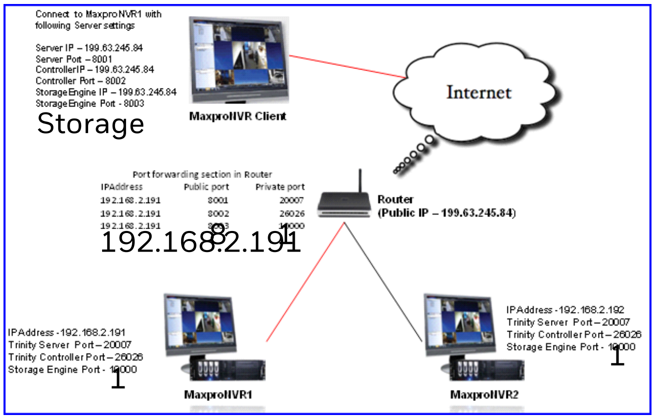
The Port Forwarding feature is generally used when an Internet client wants to connect to a particular NVR in a private Local Area Network (LAN). This feature is enabled by defining port forwarding rules in the Router. By defining these rules, you can send data using the range of ports on the internet side to a port and IP addresses on the private LAN network.

Scenarios of Port Forwarding

Note: *The scenarios described in the subsequent sections, only cover port forwarding required for the NVR client to connect to the NVR. For using MAXPRO NVR Mobile and MAXPRO NVR Web Client from the Internet, the port used by Web Server on the NVRs (Default Ports: 80, 443) should also be set up for port forwarding. See the* Changing Default Port 443 for the MAXPRO Web Client and MAXPRO Mobile app *section on page* 366 *for further details.*
It is not recommended to access NVR Client via Internet. Only NVR Web client and Mobile client is recommended to access via Internet.

Scenario1- Services mapped to different ports

Two NVRs in a private LAN are configured behind the router, and all the services on the NVRs are running on the default ports. In the router's port forwarding section you need to map the ports for each of the services running in the NVRs. An internet MAXPRO NVR client can connect to a NVR, by specifying the public IP address given to the router and corresponding ports mapped in the port forwarding table in the router.



Connect to MaxproNVR1 with following Server settings

Server IP – 199.63.245.84
Server Port – 8001
ControllerIP – 199.63.245.84
Controller Port – 8002
StorageEngine IP – 199.63.245.84
StorageEngine Port - 8003

Port forwarding section in Router

IPAddress	Public port	Private port
192.168.2.191	8001	20007
192.168.2.191	8002	26026
192.168.2.191	8003	10000

IPAddress -192.168.2.191
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000

IPAddress -192.168.2.192
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000

Port Forwarding Scenario 1

In the above figure:

MAXPRO NVR 1 and MAXPRO NVR 2 have the default port numbers, 20007, 26026, 10000, 10010 configured for the following services respectively:

- Trinity Server
- Trinity Controller
- Storage Engine (NEOStorageServer, NEOStorageServer2)

In the router's port forwarding table, the default ports numbers for these services are mapped to the public port numbers (8001, 8002, 8003, 8004) of the router.

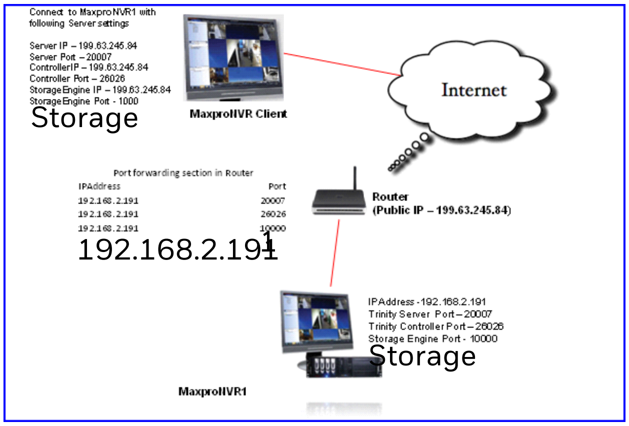
An external MAXPRO NVR client can access MAXPRO NVRs using the following settings:

- Server IP: 199.63.245.84
- Server Port: 8001
- Controller IP: 199.63.245.84
- Controller Port: 8002
- Storage Engine IP: 199.63.245.84
- Storage Engine Ports: 8003, 8004

Note: *The mapping of the ports 8001, 8002, 8003, 8004 to the respective NVR IP and ports (20007, 26026, 10000, 10010) helps an external MAXPRO NVR desktop Client to connect to the MAXPRO NVR system.*

Scenario 2: Services mapped to existing ports

A single NVR is configured behind the router, and all the services on the NVR are running on the default ports. In the router's port forwarding section specify the default ports. The Internet client can just specify the public IP Address and default ports to connect to the NVR. The drawback of mapping to the same ports is that only one NVR can be behind the router.



Connect to MaxproNVR1 with following Server settings

Server IP – 199.63.245.84
Server Port – 20007
ControllerIP – 199.63.245.84
Controller Port – 26026
StorageEngine IP – 199.63.245.84
StorageEngine Port - 1000

Port forwarding section in Router

IPAddress	Port
192.168.2.191	20007
192.168.2.191	26026
192.168.2.191	10000

IPAddress - 192.168.2.191
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000

Port Forwarding scenario 2

In the above figure:

There is a single MAXPRO NVR 1 with the default port numbers, 20007, 26026, 10000, 10010 configured for the following services respectively:

- Trinity Server
- Trinity Controller
- Storage Engine (NEOStorageServer, NEOStorageServer2)

In the router's port forwarding table, the default ports numbers for these services are specified.

An external MAXPRO NVR client can access the MAXPRO NVRs using the following settings:

- Server IP: 199.63.245.84
- Server Port: 20007
- Controller IP: 199.63.245.84
- Controller Port: 26026
- Storage Engine IP: 199.63.245.84
- Storage Engine Ports:10000 and 10010

Note: *In these scenarios, as ports are not mapped in the router, you can connect to only one MAXPRO NVR from an external MAXPRO NVR desktop Client.*

Getting to Know the MAXPRO NVR User Interface

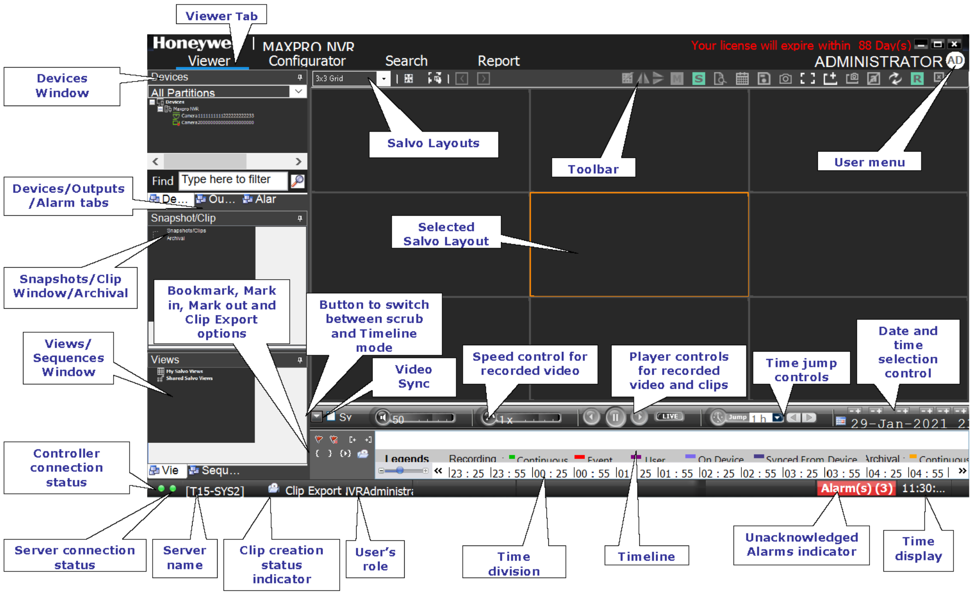
The user interface of MAXPRO NVR is easy-to-use with its intuitive icons and user-friendly features. You can configure the devices in the video surveillance network through the MAXPRO NVR user interface. The user interface consists of tabs, tree-structures, status bar, floating windows, and icons. On opening the user interface, you see the following four tabs: Viewer, Configurator, Search and Report. Based on the tab you select, windows, tree structures, and other settings relevant to the tab appear on the screen.

A status bar is displayed at the bottom of the user interface. The status bar displays: the connection status with the MAXPRO NVR server and controller, the status of clip creation, the role of the user, the number of unacknowledged alarms, and the time.

Note: *The tabs that are displayed in MAXPRO NVR User Interface is dependent on the user roles and privileges.*

Viewer Tab

Figure illustrates the Viewer tab.



Viewer tab

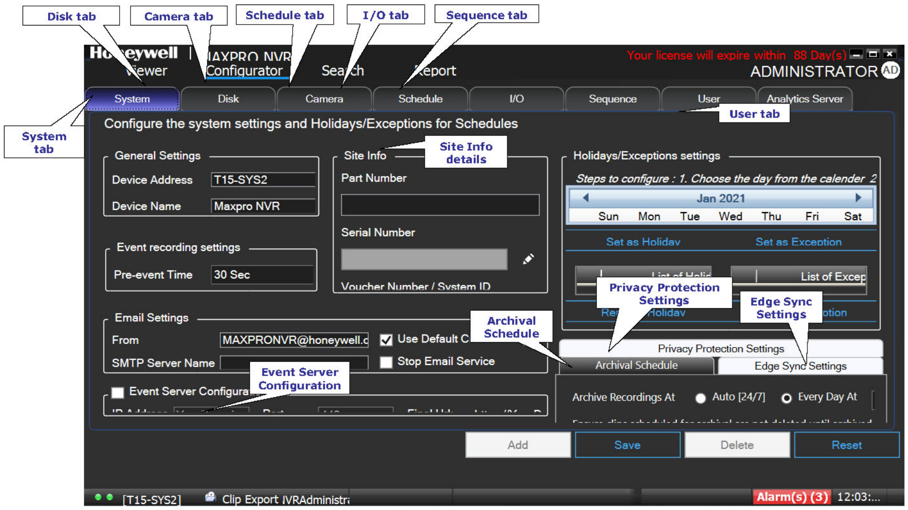
The following components are displayed on the Viewer tab screen.

Component	Description
Devices/Site window	A floating window that displays the recorders and cameras in a tree structure. You can select one or more devices from the **Devices** window to view its video in the Salvo Layout. Refer *MAXPRO® NVR Operator's Guide* for more information. Intellisense search The Intellisense search option simplifies the search for cameras. Intellisense search supports wild characters while searching. Refer *MAXPRO® NVR Operator's Guide* for more information.
Alarm window	Click to display a floating window that lists the alarms. You can acknowledge and clear the alarms from this window. Refer Alarms section in *MAXPRO® NVR Operator's Guide* for more information.
Snapshot/Clip/ Archival window	Click to display a floating window that lists the images and clips in a tree structure. You can select the images, clips and Archival clips to view. Refer Snapshot and Clips section in *MAXPRO® NVR Operator's Guide* for more information.
Sequences window	Click to display a floating window that lists the sequences. You can play the sequence using the play sequence action. See the Configuring the Sequences section on page 220.

Component	Description
Views window	A floating window that lists the salvo views. The **View** window consists of **My Salvo Views** and **Shared Salvo views**. Refer Salvo View section in *MAXPRO® NVR Operator's Guide* for more information.
Salvo Layout	An arrangement of panels in which video is displayed. Refer Salvo Layouts and Panels section in *MAXPRO® NVR Operator's Guide* for more information.
Timeline window	A window that enables you to view video from a specified date and time. Refer Video Recording and Viewing section in *MAXPRO® NVR Operator's Guide*.

Configurator Tab

Figure illustrates the Configurator tab.



Configure the system settings and Holidays/Exceptions for Schedules

General Settings

Device Address: T15-SYS2

Device Name: Maxpro NVR

Event recording settings

Pre-event Time: 30 Sec

Site Info

Part Number

Serial Number

Voucher Number / System ID

Holidays/Exceptions settings

Steps to configure : 1. Choose the day from the calender 2

Jan 2021

Sun Mon Tue Wed Thu Fri Sat

Set as Holiday   Set as Exception

List of Holid   List of Excep

Email Settings

From: MAXPRONVR@honeywell.c

SMTP Server Name

☑ Use Default C

□ Stop Email Service

□ Event Server Configura

Privacy Protection Settings

Archival Schedule

Edge Sync Settings

Archive Recordings At ● Auto [24/7] ○ Every Day At

[T15-SYS2] Clip Export IVRAdministra

Configurator tab

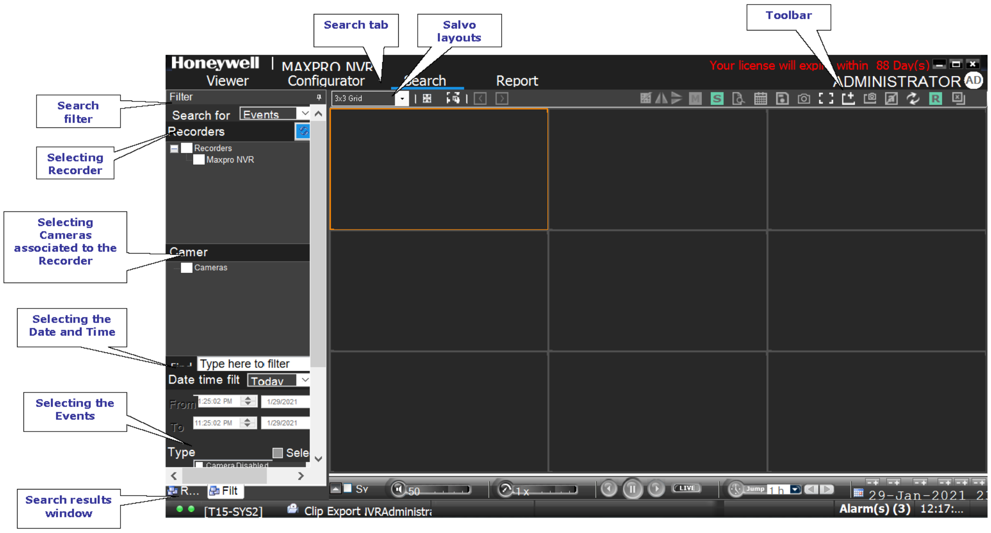
The settings in the Configurator tab enable you to add and configure the video devices and set up the MAXPRO NVR system.

Components	Description
System tab	Helps you to configure the system level settings, Site information, Archival Schedule/deletion, Holidays/Exceptions settings, Event Server Configuration and Edge Syn Settings for MAXPRO NVR.
Disk tab	Helps you to configure the disk settings for video storage.

Components	Description
Camera tab	Helps you to configure the camera settings.
Schedules tab	Helps you to configure the schedules for recording video.
IO tab	Helps you to configure the input and output for a camera.
Sequence tab	Helps you to select a sequence of cameras for live video.
User tab	Helps in user administration.

Search Tab

Figure illustrates the Search tab.

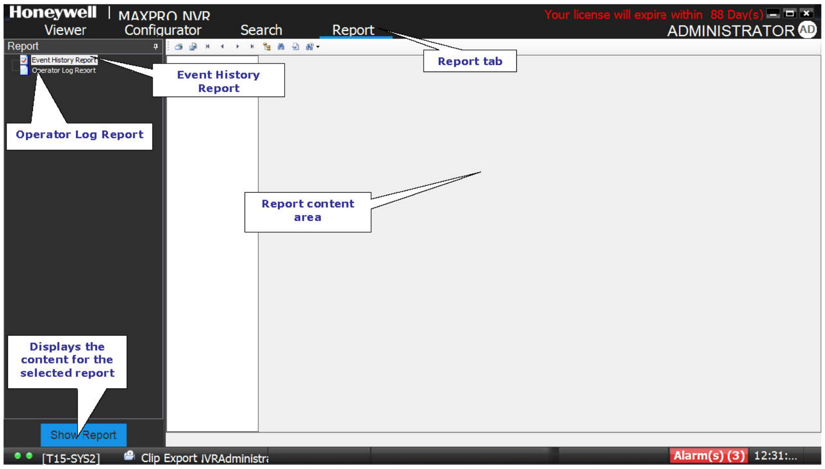


Search tab

You can search for recorded video and events in MAXPRO NVR from the Search tab.

Report Tab

Figure illustrates the Report tab.



Report tab

Setting Preferences

The Preferences option in the User menu enables you to configure the general settings and the On Screen Display (OSD) settings. On the General Settings tab, you can configure the frame rate for panels that are not selected in the salvo layout, the video rendering settings, the video to be displayed for alarms, and the alarm threshold settings. The OSD settings can be configured to change the font properties such as type, color, and size for the text that appears over the video displayed in a panel.

You can also select the default values for the general and OSD settings using the Preferences option.

MAXPRO NVR supports three modes of encryption between client and server. On the Advance Settings tab you can select the options such as Default Encryption, Windows Authentication Encryption and Certificate Based Encryption under the Application Security Settings for secure communication.

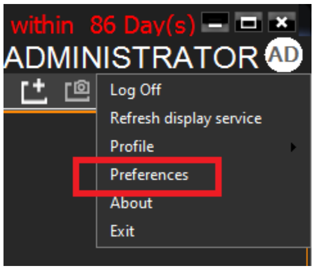
Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*

Settings for Video Rendering

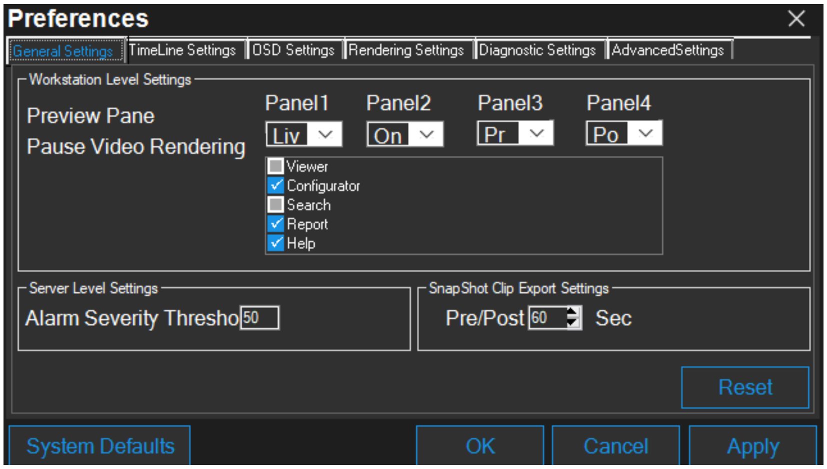
There are two types of rendering modes, Default and No Video Display. The Default rendering is the recommended mode which enables the user to view live video from multiple cameras at optimum quality. Selecting No Video Display means that no video is displayed. You can also set the frame rate for panels that are not selected in the salvo layout. The frame rate for the panels that are not selected can be set to improve the video signal transmission over lower bandwidth networks.

To select the video rendering option

Step 1. Click the Preferences option in the user menu.



The Preferences dialog box appears. By default, the General Settings tab (General Settings tab) is selected.



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Liv	On	Pr	Po

Pause Video Rendering

☐ Viewer
☑ Configurator
☐ Search
☑ Report
☑ Help

Server Level Settings

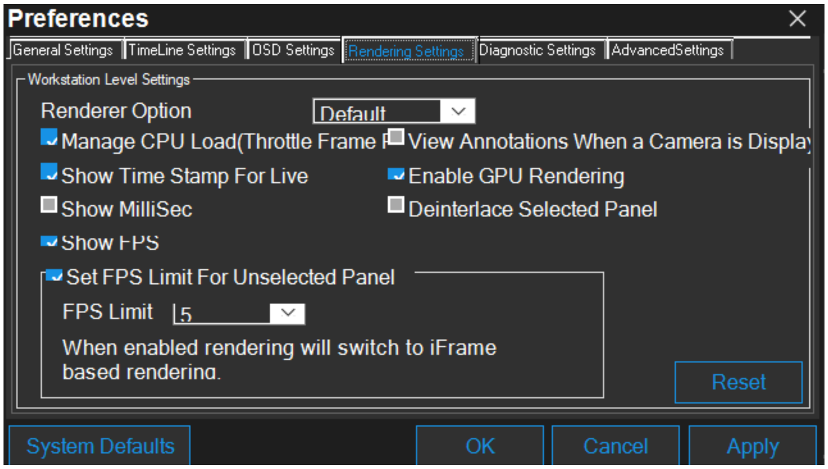
Alarm Severity Thresho 50

SnapShot Clip Export Settings

Pre/Post 60 Sec

General Settings tab

Step 2. Click the Rendering Settings tab (Rendering Settings tab).



Workstation Level Settings

Renderer Option: Default

☑ Manage CPU Load(Throttle Frame F

☐ View Annotations When a Camera is Display

☑ Show Time Stamp For Live

☑ Enable GPU Rendering

☐ Show MilliSec

☐ Deinterlace Selected Panel

☑ Show FPS

☑ Set FPS Limit For Unselected Panel

FPS Limit: 5

When enabled rendering will switch to iFrame based rendering.

Rendering Settings tab

Step 3. Select the Renderer Option (Default/No Video Display) for video rendering.

Step 4. Select the Mange CPU Load (Throttle Frame Rate) check box if you want to throttle the frame rate if the CPU usage reaches 90 per cent.

Step 5. Select the Show Time Stamp For Live check box if you want the camera name and time to be displayed on the live video.

Step 6. Select Show Milli Sec check box if you want the milliseconds to be displayed in the timestamp on video.

Step 7. Select Show FPS check box if you want the frames per second to be displayed on video.

Step 8. Select the Deinterlace Selected Panel check box if you want to deinterlace the selected panel.

Step 9. Select the check box beside Set FPS Limit For Unselected Panel.

Step 10. Select the FPS Limit. The default frame rate is 5 fps and is the recommended setting for unselected panels.

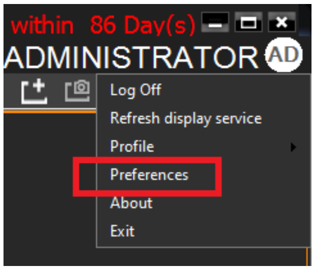
Step 11. Click Apply.

Step 12. Click OK to close the dialog box.

Rendering Settings for a GPU system

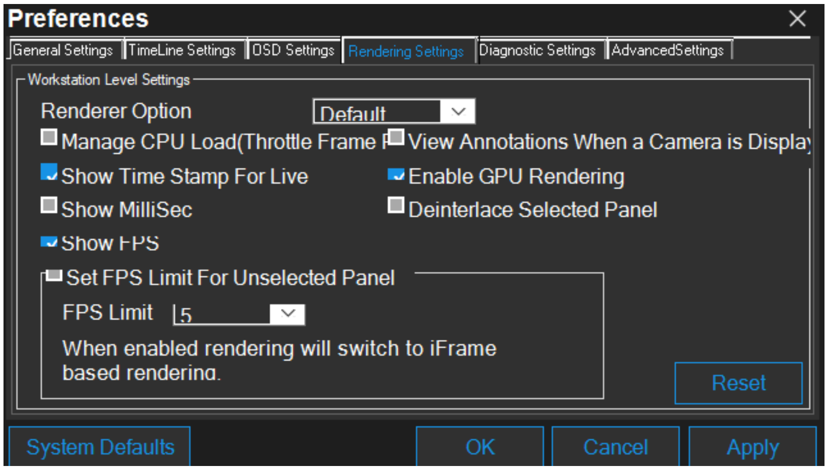
To avail GPU rendering (30 fps in your salvo view) you need to configure the video rendering settings under Workstation Level Settings. You can render up to 18 cameras at 1080P resolution 30fps on a client machine with recommended workstation specifications (refer to NVR data sheet for specifications). To know about improvised GPU rendering capability, see Improved GPU Rendering section on page 242 section.

Step 1. Click the Preferences option in the user menu.



The Preferences dialog box appears. By default, the General Settings tab is selected.

Step 2. Click the Rendering Settings tab (Rendering Settings tab).



Workstation Level Settings

Renderer Option: Default

□ Manage CPU Load(Throttle Frame F

□ View Annotations When a Camera is Display

☑ Show Time Stamp For Live

☑ Enable GPU Rendering

□ Show MilliSec

□ Deinterlace Selected Panel

☑ Show FPS

□ Set FPS Limit For Unselected Panel

FPS Limit: 5

When enabled rendering will switch to iFrame based rendering.

Rendering Settings tab

Step 3. Clear the following check boxes:
By default these two check boxes are selected.

- Mange CPU Load (Throttle Frame Rate)
- Set FPS Limit For Unselected Panel

Step 4. Click Apply.

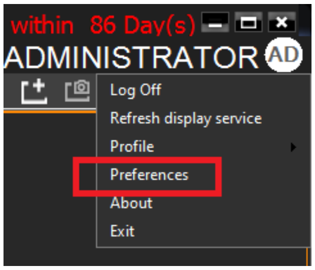
Step 5. Click OK to close the dialog box.

Pausing the Video Rendering

You can pause the video rendering to momentarily stop the rendering of video when a tab that does not display video is selected (for example, when the Report tab is selected, the video rendering can be paused to improve the application performance). The rendering of video starts again when you select a different tab in the user interface.

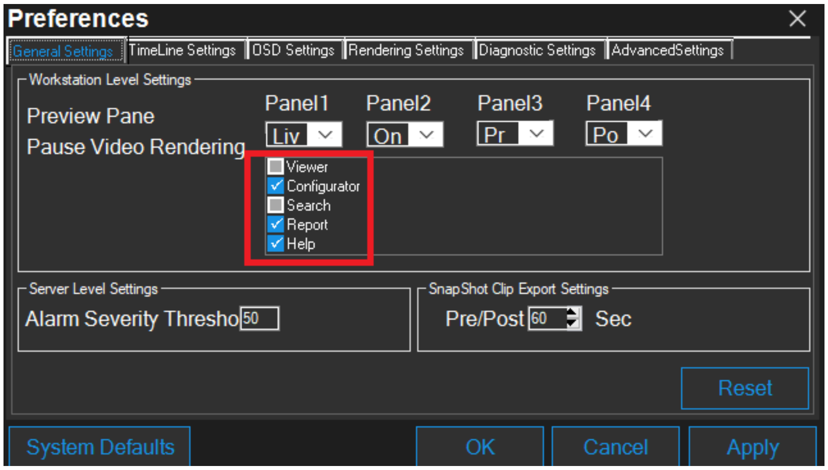
To select the tab which pauses video rendering

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box appears. By default, the General Settings tab is selected.

Step 2. For Pause Video Rendering, select the check box next to the tab names that you want to select (Settings for pausing the Video Rendering).



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Liv	On	Pr	Po

Pause Video Rendering

□ Viewer
☑ Configurator
□ Search
☑ Report
☑ Help

Server Level Settings

Alarm Severity Thresho 50

SnapShot Clip Export Settings

Pre/Post 60 Sec

Settings for pausing the Video Rendering

Step 3. Click Apply.

Step 4. Click OK to close the dialog box.

Settings for Alarm Preview Pane

When the video related to an alarm is played from the Alarm window, the salvo layout changes to a four panel layout. You can define the video display for each panel namely, Pre Alarm, Post Alarm, Live, and On Alarm. The following table defines these options.

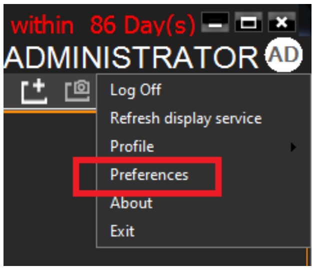
Option	Description
Pre Alarm	The video before the occurrence of the event that triggered the alarm is played.
Post Alarm	The video after the occurrence of the event that triggered the alarm is played.
Live	Live video is played.

Option	Description
On Alarm	The video is played from the occurrence of the event that triggered the alarm.

Note: *You can view video related to alarms for the cameras connected to MAXPRO NVR. For Pre Alarm, Post Alarm, and On Alarm, the video is played only when the video recording pertaining to the date and time of alarm is available.*

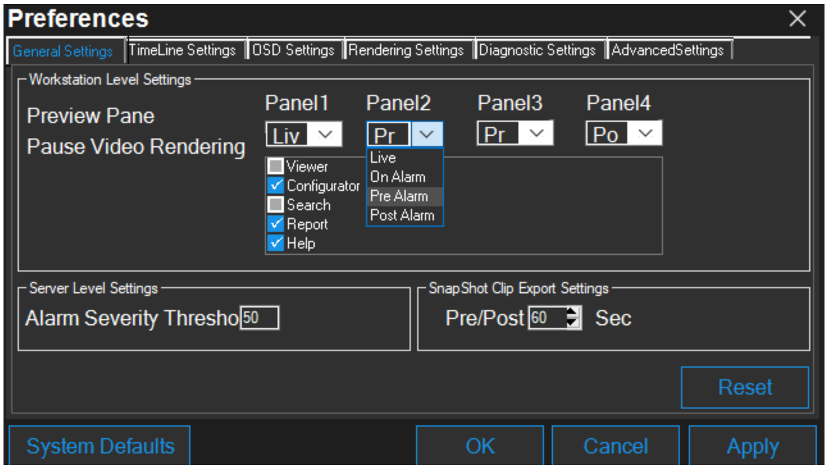
To define the video display for each preview panel

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box appears. By default, the General Settings tab is selected (Settings for the Alarm Preview Pane).

Step 2. Select the video option for each panel corresponding to Preview Pane. When you select Pre Alarm and Post Alarm, a dialog box appears. Select the time in seconds for which you want to view video related to pre alarm and post alarm in the dialog box and click OK.



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Liv	Pr	Pr	Po

Pause Video Rendering

☐ Viewer
☑ Configurator
☐ Search
☑ Report
☑ Help

Server Level Settings

Alarm Severity Thresho 50

SnapShot Clip Export Settings

Pre/Post 60 Sec

Settings for the Alarm Preview Pane

Step 3. Click Apply.

Step 4. Click OK to close the dialog box.

Setting the Alarm Threshold Value

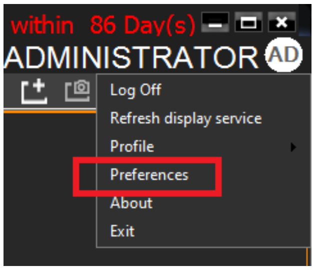
Each event type supported in the NVR has a pre-defined Severity Level value associated to it. When the event occurs, the value is compared with the value in the Alarm Severity Threshold box in the Preferences dialog box. The alarm is triggered only when the Severity Level value is greater than the Alarm Severity Threshold value. See Appendix B, Event and Alarm Types section on page 417 for default Event and Alarm types and their severity levels for Camera, Recorder and SMART VMD.

For example, the alarm is triggered if the Severity Level for an event is 50 and the Alarm Severity Threshold value is 40.

Note: *Severity level for alarms are displayed in the Alarm window Refer the Alarms section in MAXPRO® NVR Operator's Guide for more information.*

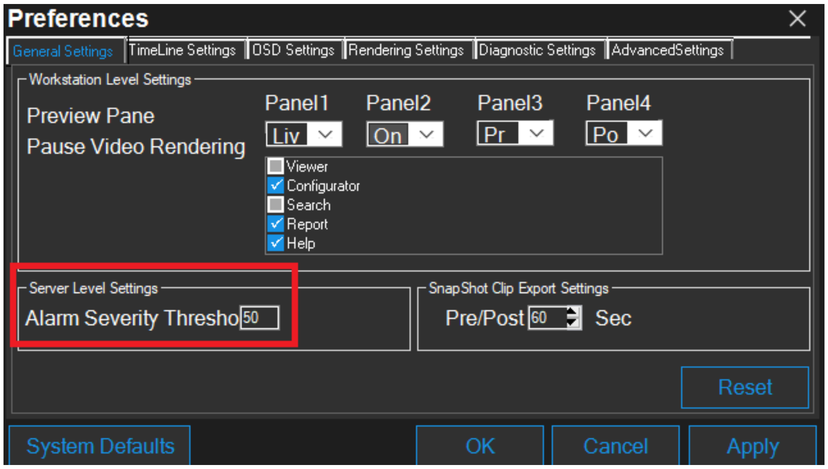
To set the Alarm Severity Threshold value

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box appears. By default, the General Settings tab is selected (Setting the Alarm Threshold).

Step 2. Under Server Level Settings, type an Alarm Severity Threshold.



Preview Pane: Liv | On | Pr | Po

Pause Video Rendering:

□ Viewer
☑ Configurator
□ Search
☑ Report
☑ Help

Alarm Severity Thresho 50

Pre/Post 60 Sec

Setting the Alarm Threshold

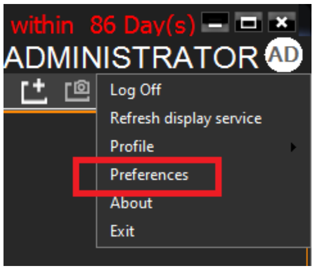
Step 3. Click Apply.

Step 4. Click OK to close the dialog box.

Configuring the Snapshot Clip Export Settings

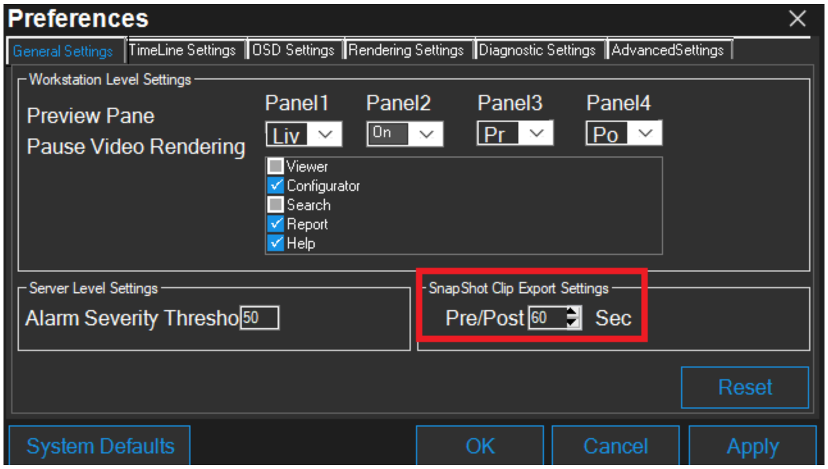
You can configure the time interval for the exported snapshot.

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box appears. By default, the General Settings tab is selected (Settings for SnapShot Clip Export).

Step 2. Under SnapShot Clip Export Settings, select the Clip Export time in seconds.



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Liv	On	Pr	Po

Pause Video Rendering

- ☐ Viewer
- ☑ Configurator
- ☐ Search
- ☑ Report
- ☑ Help

Server Level Settings

Alarm Severity Thresho 50

SnapShot Clip Export Settings

Pre/Post 60 Sec

Settings for SnapShot Clip Export

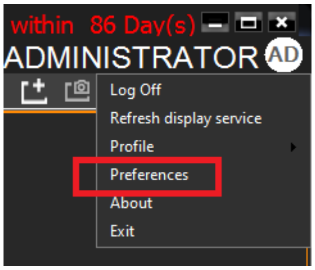
Step 3. Click Apply.

Step 4. Click OK to close the dialog box.

Configuring the OSD Settings

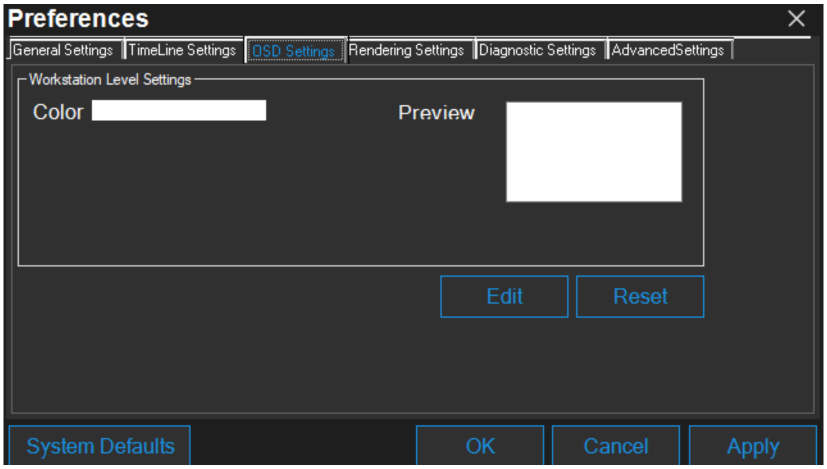
You can configure the OSD settings to change the properties such as type, color, and size of the text that appears over the video displayed in a panel.

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box (OSD Settings tab) appears.

Step 2. Click the OSD Settings tab.



OSD Settings tab

Step 3. Click Edit and select the font and color properties in the dialog box.

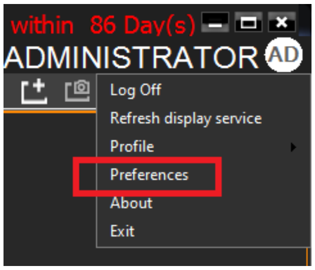
Step 4. Click OK to close the font properties dialog box.

Step 5. Click Apply in the Preferences dialog box.

Step 6. Click OK to close the Preferences dialog box.

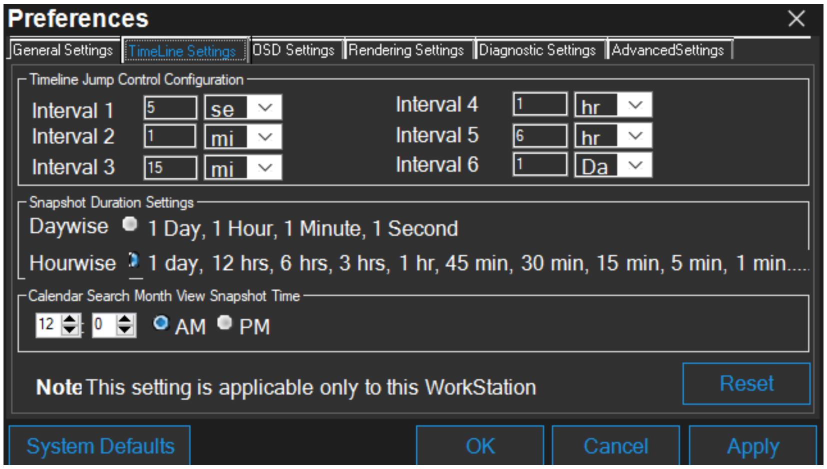
Configuring the Timeline Settings

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box (Timeline Settings tab) appears.

Step 2. Click the Timeline Settings tab.



Preferences

General Settings | TimeLine Settings | OSD Settings | Rendering Settings | Diagnostic Settings | AdvancedSettings

Timeline Jump Control Configuration

Interval 1: 5 se
Interval 2: 1 mi
Interval 3: 15 mi
Interval 4: 1 hr
Interval 5: 6 hr
Interval 6: 1 Da

Snapshot Duration Settings

Daywise ○ 1 Day, 1 Hour, 1 Minute, 1 Second

Hourwise ● 1 day, 12 hrs, 6 hrs, 3 hrs, 1 hr, 45 min, 30 min, 15 min, 5 min, 1 min....

Calendar Search Month View Snapshot Time

12 : 0 ● AM ○ PM

Note This setting is applicable only to this WorkStation

Timeline Settings tab

Step 3. Under Timeline Jump Control Configuration, set the time for the intervals (Interval 1 to Interval 6) as applicable.

Step 4. Under Snapshot Duration Settings, select the Daywise or Hourwise option button as applicable.

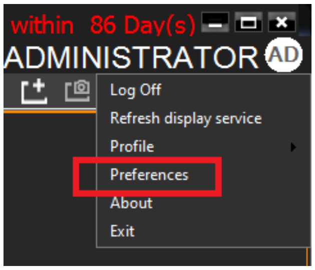
Step 5. Under Calendar Search Month View Snapshot Time, type the preferred time and seconds and then click AM or PM as applicable.

Step 6. Click Apply.

Step 7. Click OK to close the Preferences dialog box.

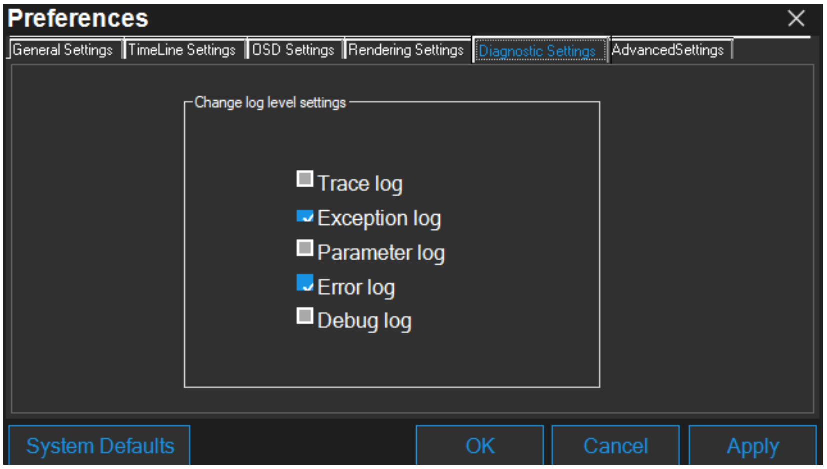
Configuring the Diagnostic Settings

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box (Diagnostic Settings tab) appears.

Step 2. Click the Diagnostic Settings tab.



Change log level settings

- □ Trace log
- ☑ Exception log
- □ Parameter log
- ☑ Error log
- □ Debug log

Diagnostic Settings tab

Step 3. Under Change log level settings, select the check boxes corresponding to logs as applicable.

Step 4. Click Apply.

Step 5. Click OK to close the Preferences dialog box.

Configuring the Advanced Settings

Encryption secures the communication between server and client. You can encrypt the data between client to server using encryption feature. MAXPRO NVR supports three types of encryption modes to communicate with NVR box through client. Each encryption has specific pre-requisites. The following are the pre-requisites for each encryption mode.

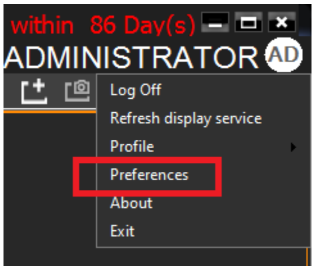
- Default Encryption: None
- Windows Authentication Encryption:
- System clock time should be synced between client and server machine. It also recommended to use the time sync utility to sync the time between client and server.
- Workgroup: If the machines are in workgroup then the password used by a client to log on as a windows user should be the same as Server PC.
- Domain User: All valid domain users are allowed to log on.
- Certificate Based Encryption (Recommended):
- System clock time should be in sync between client and server machine. It is also recommended to use the time sync utility to sync the time between client and server.
- Certificate needs to be installed in all Client and Server PCs. A client without a certificate is not allowed to log on.
- Internet connection is required to Install the certificate.

- Certificate Based Encryption works across workgroup and domain.

Note: *VeriSign Class 3 Code Signing 2010 CA issued certificate is tested for certificate based encryption. Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*

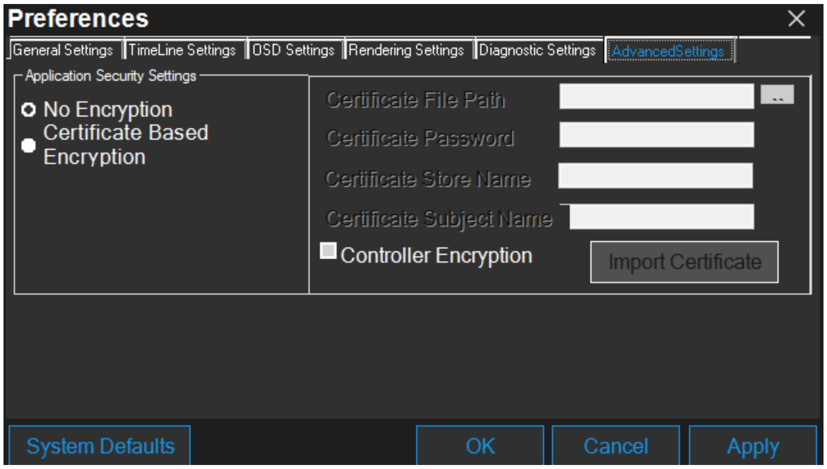
To configure the Advanced settings

Step 1. Click the Preferences option in the User menu.



The Preferences dialog box (Advanced Settings Tab) appears.

Step 2. Click the Advanced Settings tab.



Advanced Settings Tab

Step 3. Click Certificate Based Encryption option (Recommended), a certificate is used for encrypting the data between client and server. To encrypt the data using Certificate Based Encryption, perform the following:

d. Browse the certificate (.pfx file).

e. Type the Certificate Password and then click the Import Certificate button to import the certificate.

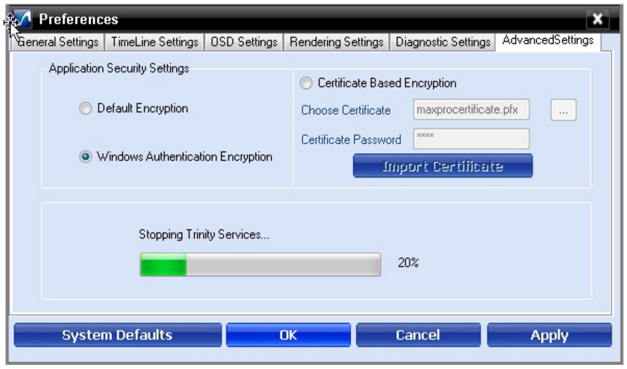
Tip: You can also import the certificate from the following link: http://technet.microsoft.com/en-us/library/cc776889(v=ws.10).aspx

Or

Under Application Security Settings, select the Default Encryption or Windows Authentication Encryption options as applicable.

Note: *Honeywell recommends you to opt for Certificate Based Encryption and use a valid certificate from a Certificate Authority. The CA certificate would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes on how to Secure Communication between Client and Server for MAXPRO NVR & VMS section.*

Step 1. Click OK. A services restarting progress bar is displayed. Its takes several minutes to restart all the services.



Application Security Settings

○ Default Encryption

● Windows Authentication Encryption

○ Certificate Based Encryption

Choose Certificate: maxprocertificate.pfx

Certificate Password: ****

Stopping Trinity Services...

20%

Advance Settings Tab Service Restart

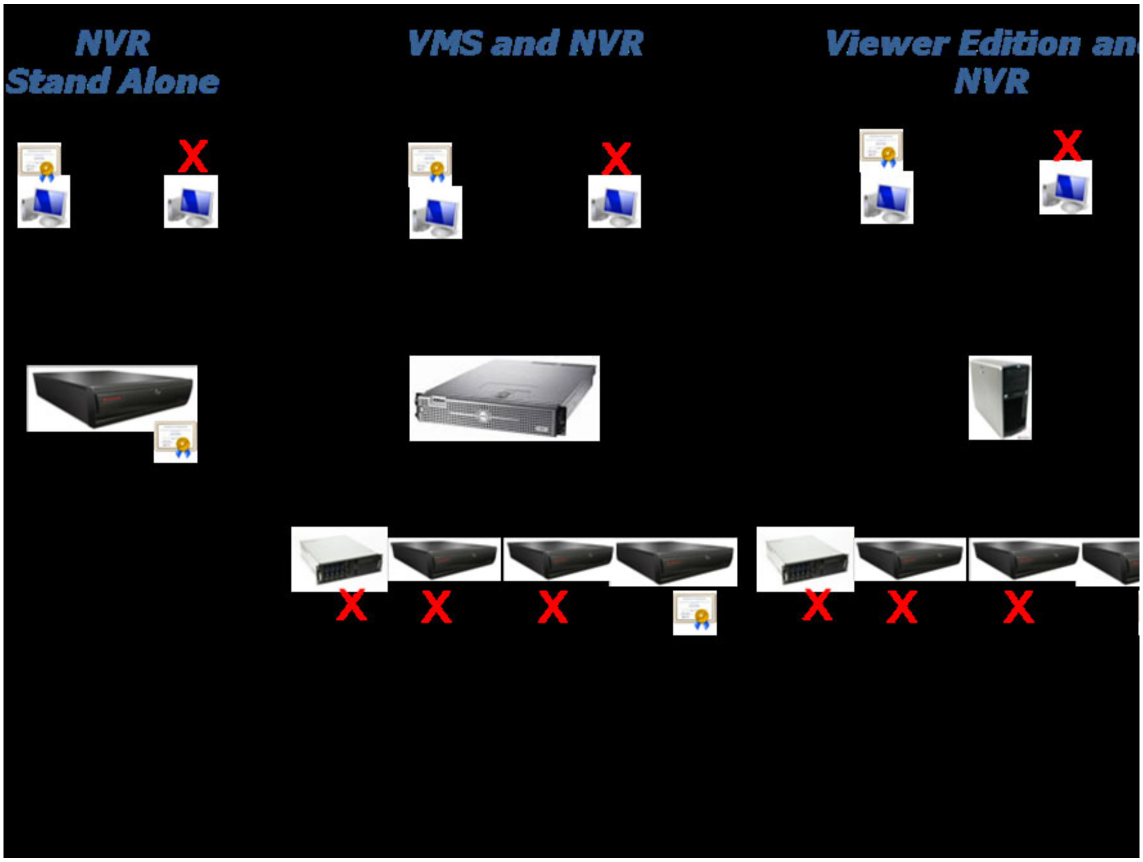
Note: *All services will be restarted and all clients will be auto-reconnected.*

Step 2. Click Apply to close the Preferences dialog box.

Encryption Certificate deployment scenario

The following figures depicts the Encryption certificate deployment scenarios:

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*



Configuring the Default Settings

Step 1. Click Reset to apply default settings while setting preferences.

Step 2. Click System Defaults to apply the system default settings while setting preferences.

Licensing Information

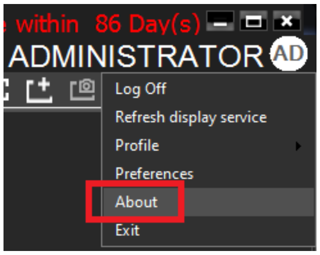
Viewing the Version and License Information of MAXPRO NVR

Caution: Honeywell's turnkey box solutions come pre-licensed or included with all the camera licenses. This varies for MAXPRO NVR models, please refer to the respective data sheets.

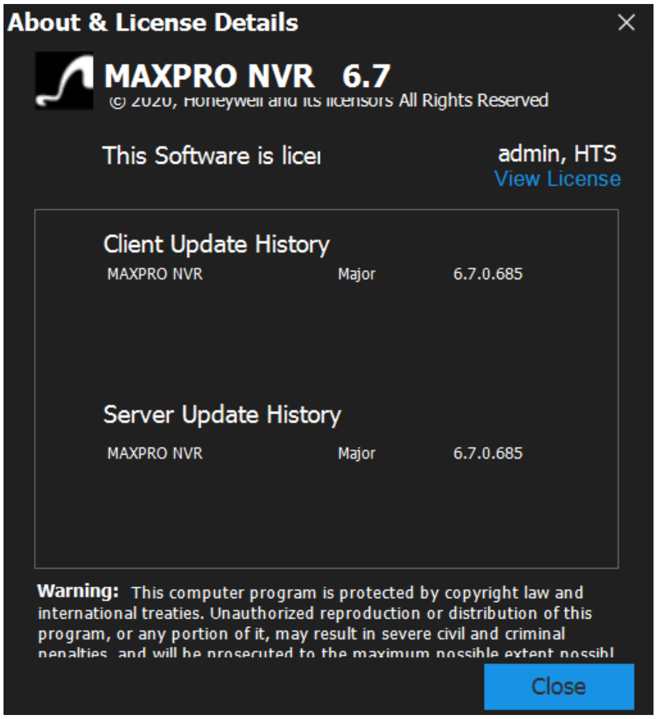
The MAXPRO NVR Software license has a 60-day activation period. During this trial period NVR allows you to add up to 64 cameras. To continue using the software beyond the first 60 days, you must register the software. On registration, the license is limited to the number of camera licenses purchased with the software.

You can view the version and license information of MAXPRO NVR software from the User menu.

Step 1. From the User menu on the top right, click About from the drop-down list.



The version information of MAXPRO NVR appears Figure .



About & License Details

MAXPRO NVR 6.7

© 2020, Honeywell and its licensors All Rights Reserved

This Software is licei admin, HTS

View License

Client Update History

MAXPRO NVR Major 6.7.0.685

Server Update History

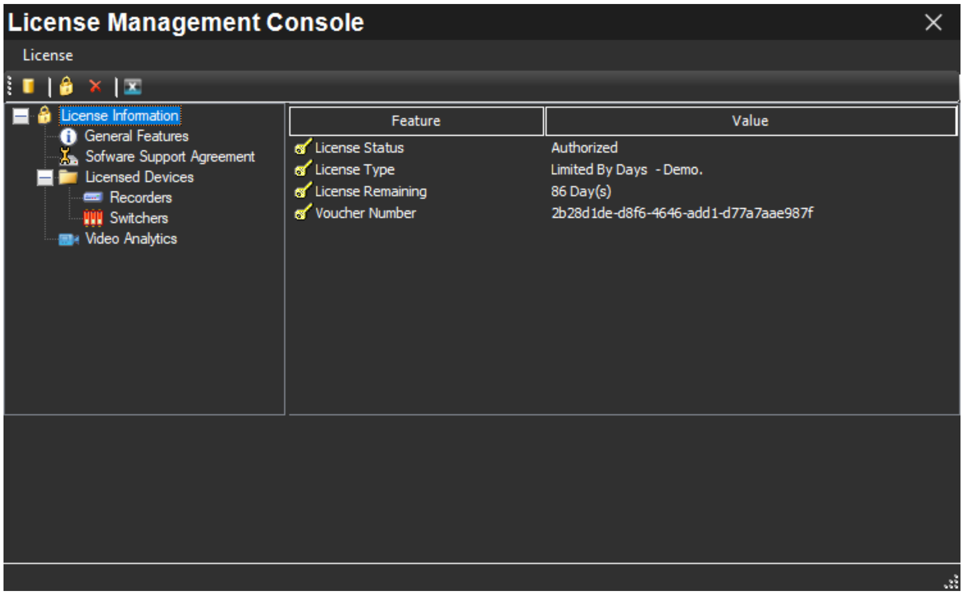
MAXPRO NVR Major 6.7.0.685

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum possible extent possibl

Close

About MAXPRO NVR

Step 2. Click the License option. The License Management Console dialog box Figure appears.



Feature	Value
License Status	Authorized
License Type	Limited By Days - Demo.
License Remaining	86 Day(s)
Voucher Number	2b28d1de-d8f6-4646-add1-d77a7aae987f

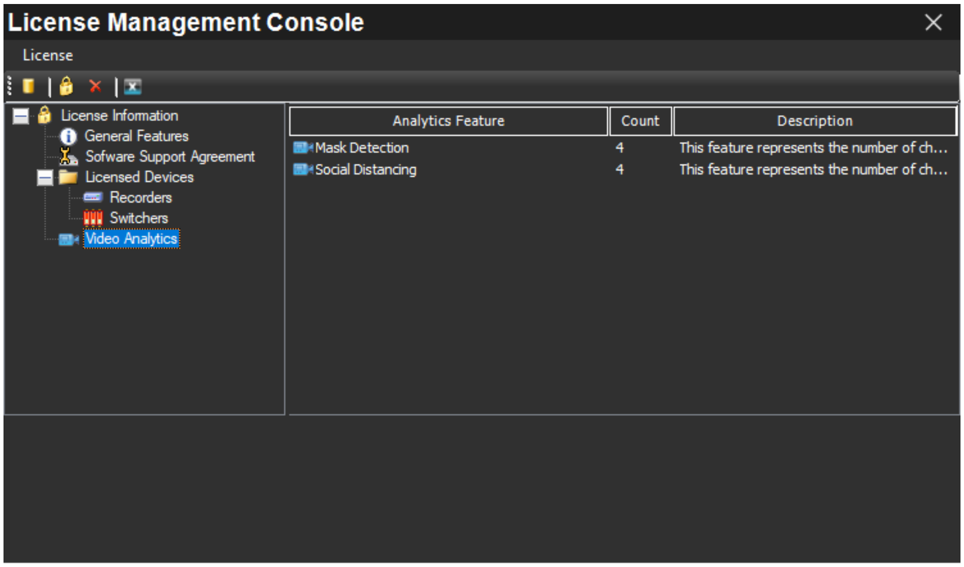
License Management Console

The License Management Console dialog box displays the number of days remaining in the 60-day activation period since the software was installed. You must purchase the license to continue using MAXPRO NVR.

License Type is shown as Permanent if your NVR has been licensed. General Features shows the license information on number of channels and clients.

Video Analytics License

Below sample images represents with video analytics licenses for Mask and Social Distancing Detection feature.



Analytics Feature	Count	Description
Mask Detection	4	This feature represents the number of ch...
Social Distancing	4	This feature represents the number of ch...

Registration and Licensing

Registering the software only requires the Host ID file from the server system. This is a unique ID generated for the NVR Server. Click the drum icon to create a Host ID. You are prompted to select the path where you want to generate the Host ID (HID) file, and then click OK. Save the file to a USB flash drive or hard drive.

Refer to the *MAXPRO NVR Quick Start Guide* for detailed information on registration and licensing of Software only NVR.

Completing the Licensing

After you receive the license certificate, perform the following steps to license the NVR.

Step 1. Download the License Certificate file and save it to a USB flash drive.

Step 2. Launch MAXPRO NVR on the MAXPRO NVR Server.

Step 3. From the User menu, click About.

Step 4. On the MAXPRO® NVR dialog box, click License.

Step 5. On the License Management Console dialog box, select Install License in the License drop-down list.

Step 6. The New License Configuration Wizard launches. Click Next.

Step 7. On the Locate Your License File dialog box, click Browse to locate your license certificate (for example, on the USB flash drive), and then click Next.

Step 8. The License Comparison dialog box displays the details of the existing license and the newly procured license. Compare the Existing License and the Selected License columns corresponding to General Features and Devices. When you are satisfied, click Next.

Note: *Any discrepancy in the license must be reported to Honeywell Sales Support. For example, the Maximum supported cameras row under the Selected License column displays the number of cameras for which the license is purchased. If the number of cameras is less or more than the number of cameras for which the license was purchased, contact Honeywell Sales Support immediately.*

Step 9. On the Device Configuration Changes dialog box, check that the details are accurate, and then click Next.

Step 10. On the Confirm New License dialog, click Finish.

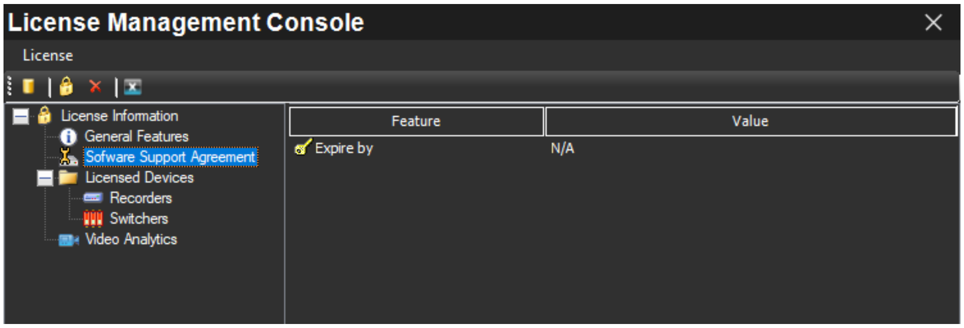
Step 11. On the New License Configuration Wizard dialog box, click Yes.

SSA - Software Service Agreement for MAXPRO

Software Service Agreement (SSA) is a flexible version specific licensing process which allows a user to get the support on the MAXPRO NVR licenses across multiple versions. From 6.0 release user need to buy a valid license to upgrade or for fresh installation. In addition, user can buy SSA support license for a specific duration which helps to get support from Honeywell.Please contact Honeywell Customer support. See the back cover for the contact information in respective regions.

Note: *license is valid only for a specific release. When applied, on a wrong version, the license will be rejected. For example if you install 5.0 license on a 6.0 installed machine, then a message* ***Selected license is invalid for MAXPRO NVR 6.0. Please select correct license file*** *is displayed.*

To install the procured license see Registration and Licensing for more information. Once the SSA license is procured and installed, the License console Management window displays the SSA info entry with validity as shown in the below example.



Feature	Value
Expire by	N/A

Analytics License

In some scenario if user changes the Mask and Social Distancing camera license then there will not be any impact on Analytics service about the number of camera count.

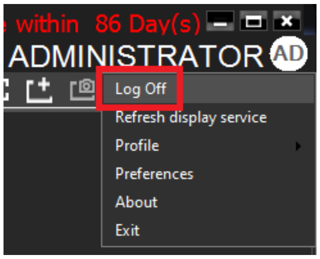
For example: If you have 5 Mask /Social Distancing camera license and if you change it to 2 camera license then the alarms from the unlicensed 3 cameras will be generated in NVR for mask and social distancing until the configuration is modified.

Once the camera configuration is changed then the unlicensed camera will not function as Analytics camera and Mask/social distancing alarms will not be generated.

Logging off

You can log off from MAXPRO NVR from the User menu. The name of the currently connected user is displayed as the User menu on the top right of each screen.

Step 1. Click the User menu. The user menu options appear.

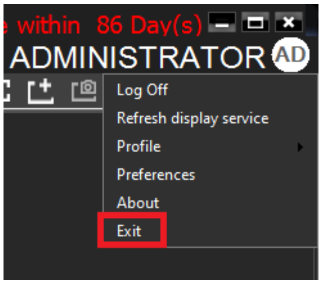


Step 2. Click Log Off. The Log on dialog box appears after logging off from MAXPRO NVR.

Closing the MAXPRO®NVR User Interface

You can close the MAXPRO NVR user interface from the User menu. The name of the currently connected user is displayed as the User menu on the top right of each screen.

Step 1. Click the User menu. The user menu options appear.



Step 2. Click Exit. A dialog box appears prompting you to confirm the action.

Step 3. Click Yes.

CHAPTER

7 CONFIGURING MAXPRO NVR

In this chapter...

Overview

Configuring MAXPRO NVR involves setting up the system to perform video surveillance and IP recording operations. This is the most important phase for commissioning MAXPRO NVR system as it involves setting up the MAXPRO NVR IP address, organizing devices, users, and roles. The MAXPRO NVR configuration task is performed only by the user having the NVR Administrator role. This is the initial task performed after the setting up the MAXPRO NVR system.

Caution: Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.

Note: *For a user having the Operator role, the contents in this chapter serve as a reference.*

MAXPRO NVR configuration involves the following tasks:

- Configuring the Honeywell cameras with MAXPRO NVR Wizard.
- Configuring the System settings
- Configuring the Disk settings
- Configuring the Cameras
- Adding IP Cameras / Encoders
- Manually adding cameras
- Discovering and Adding Third Party PSIA, ONVIF and AXIS Cameras
- Discovering and Adding Multi-channel Encoders
- Adding FLIR Camera
- Adding RTSP Cameras/Encoders

- Adding Streams
- Configuring the Input and Output for an IP camera
- Configuring 360/180 Cameras
- Managing Analog Cameras
- Configuring Analog Cameras
- Configuring the Input and Output for an Analog camera
- Server VMD (SMART VMD)
- Updating the Cameras
- Deleting the Cameras
- Configuring the Schedules
- Configuring the Sequences
- Performing User administration

Before you Begin

- Ensure that you have completed MAXPRO NVR server and client hardware setup and software installation.

Firewall Settings

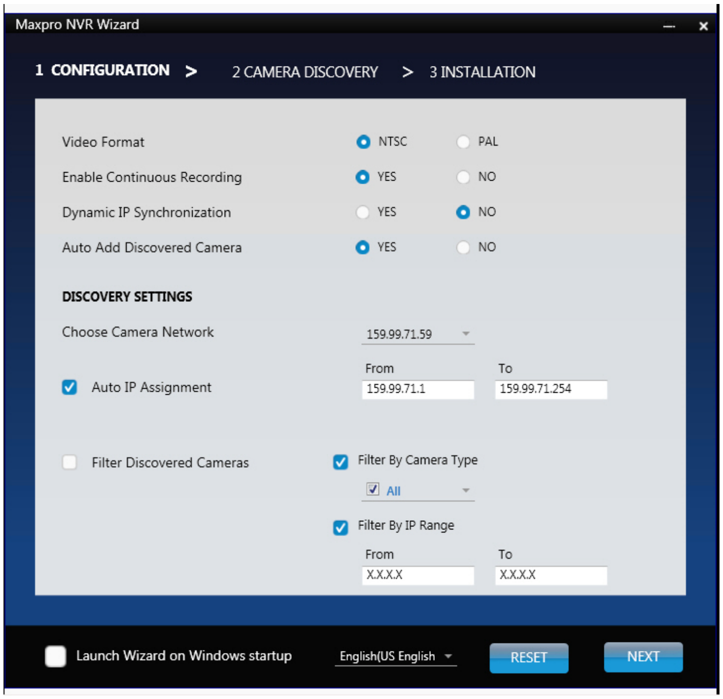
Caution: The Firewall settings are pre-configured for boxed solutions – MAXPRO NVR XE, SE, PE and MAXPRO NVR Hybrid XE, SE, PE. For MAXPRO NVR Software-Only solution, the Firewall settings are automatically configured during the installation process.

Configuring the Honeywell cameras with MAXPRO NVR Wizard

MAXPRO NVR Wizard is an easy three-step* procedure to live video for Honeywell devices. This wizard automatically starts each time you power on the MAXPRO NVR system.

(* 3 clicks with default settings and in a local area network for specific models)

Step 1. The CONFIGURATION page appears.



Video Format ● NTSC ○ PAL

Enable Continuous Recording ● YES ○ NO

Dynamic IP Synchronization ○ YES ● NO

Auto Add Discovered Camera ● YES ○ NO

DISCOVERY SETTINGS

Choose Camera Network 159.99.71.59

☑ Auto IP Assignment From 159.99.71.1 To 159.99.71.254

□ Filter Discovered Cameras

☑ Filter By Camera Type ☑ All

☑ Filter By IP Range From X.X.X.X To X.X.X.X

□ Launch Wizard on Windows startup English(US English

CONFIGURATION page

- If you want to change the default settings, select YES or NO corresponding to the fields listed in the following table or click STEP 2 to accept the default settings, and proceed to the CAMERA DISCOVERY page in step 2.

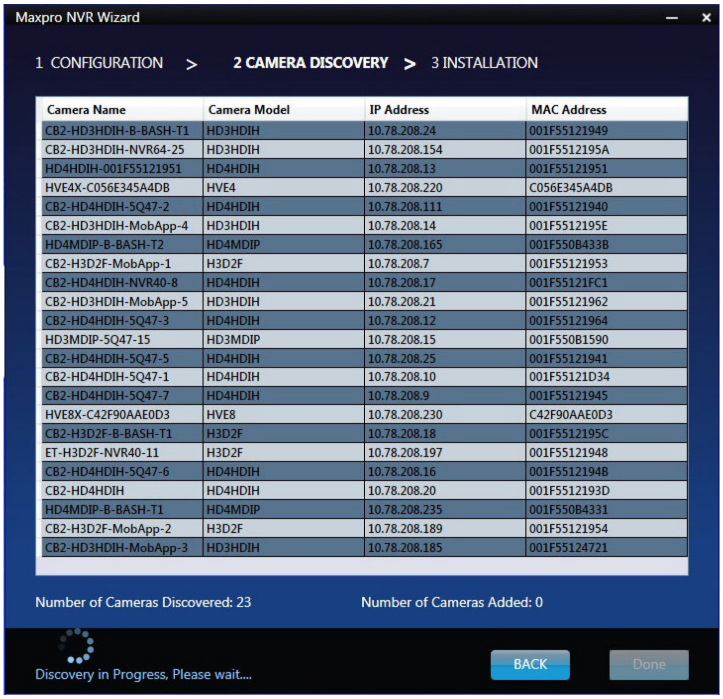
Field	**Description**
CONFIGURATION SETTINGS	
Video Format	Select “NTSC” or “PAL” based on your region.
Enable Continuous Recording	Start recording as soon as soon as the camera is added. 24/7 continuous recording is enabled for all the cameras.
Dynamic IP Synchronization	MAXPRO NVR software automatically synchronizes any change in the camera’s IP address. For example. if a camera is restarted, and a new IP is associated to the camera, then the MAXPRO NVR software automatically detects the changed IP address and synchronizes it to the camera so that live viewing and recording is not disturbed.
Auto Add Discovered Camera	Any newly connected camera is automatically discovered and added to the camera’s list.

Field	Description
DISCOVERY SETTINGS	
Choose Camera Network	Enables you to choose your camera network from the drop-down list. Click the refresh icon ↻ to refresh the drop-down list.
Auto IP Assignment	Assigns a valid address to cameras with Automatic Private IP Addressing (APIPA). Note: Use this option only if you do not have a DHCP server and want to assign an IP address in your computer network range to the cameras.
	Range for IP Assignment: The MAXPRO NVR system automatically detects all the cameras in this range on the network. From, To: Type the IP range.
Filter Discovered Cameras	Enables you to filter the discovered cameras based on the camera model and IP range.
	• Filter By Camera Type: Select this check box and then select a camera model from the drop-down list by clicking the respective check boxes. • Filter By IP Range: Select this check box and then type the IP range in From and To.

- Select the required language from the drop-down list. The supported languages are Arabic, Czechoslovakian, Dutch, French, German, Russian, Italian, Polish, Portuguese, Spanish, and English. The default language is English (US English).
- Select the Launch Wizard on Windows startup check box to launch the wizard automatically each time you start Windows.

Note: *Click RESET to restore the default settings for each of the fields listed in the above table.*

Step 2. The CAMERA DISCOVERY page appears.



Camera Name	Camera Model	IP Address	MAC Address
CB2-HD3HDIH-B-BASH-T1	HD3HDIH	10.78.208.24	001F55121949
CB2-HD3HDIH-NVR64-25	HD3HDIH	10.78.208.154	001F5512195A
HD4HDIH-001F55121951	HD4HDIH	10.78.208.13	001F55121951
HVE4X-C056E345A4DB	HVE4	10.78.208.220	C056E345A4DB
CB2-HD4HDIH-5Q47-2	HD4HDIH	10.78.208.111	001F55121940
CB2-HD3HDIH-MobApp-4	HD3HDIH	10.78.208.14	001F5512195E
HD4MDIP-B-BASH-T2	HD4MDIP	10.78.208.165	001F550B433B
CB2-H3D2F-MobApp-1	H3D2F	10.78.208.7	001F55121953
CB2-HD4HDIH-NVR40-8	HD4HDIH	10.78.208.17	001F55121FC1
CB2-HD3HDIH-MobApp-5	HD3HDIH	10.78.208.21	001F55121962
CB2-HD4HDIH-5Q47-3	HD4HDIH	10.78.208.12	001F55121964
HD3MDIP-5Q47-15	HD3MDIP	10.78.208.15	001F550B1590
CB2-HD4HDIH-5Q47-5	HD4HDIH	10.78.208.25	001F55121941
CB2-HD4HDIH-5Q47-1	HD4HDIH	10.78.208.10	001F55121D34
CB2-HD4HDIH-5Q47-7	HD4HDIH	10.78.208.9	001F55121945
HVE8X-C42F90AAE0D3	HVE8	10.78.208.230	C42F90AAE0D3
CB2-H3D2F-B-BASH-T1	H3D2F	10.78.208.18	001F5512195C
ET-H3D2F-NVR40-11	H3D2F	10.78.208.197	001F55121948
CB2-HD4HDIH-5Q47-6	HD4HDIH	10.78.208.16	001F5512194B
CB2-HD4HDIH	HD4HDIH	10.78.208.20	001F5512193D
HD4MDIP-B-BASH-T1	HD4MDIP	10.78.208.235	001F550B4331
CB2-H3D2F-MobApp-2	H3D2F	10.78.208.189	001F55121954
CB2-HD3HDIH-MobApp-3	HD3HDIH	10.78.208.185	001F55124721

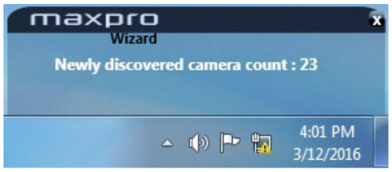
Number of Cameras Discovered: 23

Number of Cameras Added: 0

Discovery in Progress, Please wait....

CAMERA DISCOVERY page

- All the settings that you have saved on the CONFIGURATION page are listed, along with the discovered cameras. As each connected camera is discovered (notice the message that displays on the lower right of your monitor) it is added to the list. This list disappears as the cameras are added to the MAXPRO NVR software.

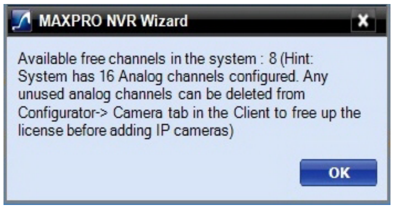


Newly discovered camera count : 23

Discovered Cameras

Note: *The ADD button on the CAMERA DISCOVERY page appears only if you have selected “NO” corresponding to Auto Add Discovered Camera in the CONFIGURATION page. Select the check boxes corresponding to a camera from the discovered list, and then click ADD button to add the discovered cameras of your choice to the MAXPRO NVR software.*

- A MAXPRO NVR Wizard pop-up message appears detailing the available free channels in the system on NVR Hybrid units if there are analog cameras (pre-configured or added manually). It also gives you a hint about deleting the unused analog channels to add IP cameras. Click OK to continue.



MAXPRO NVR Wizard

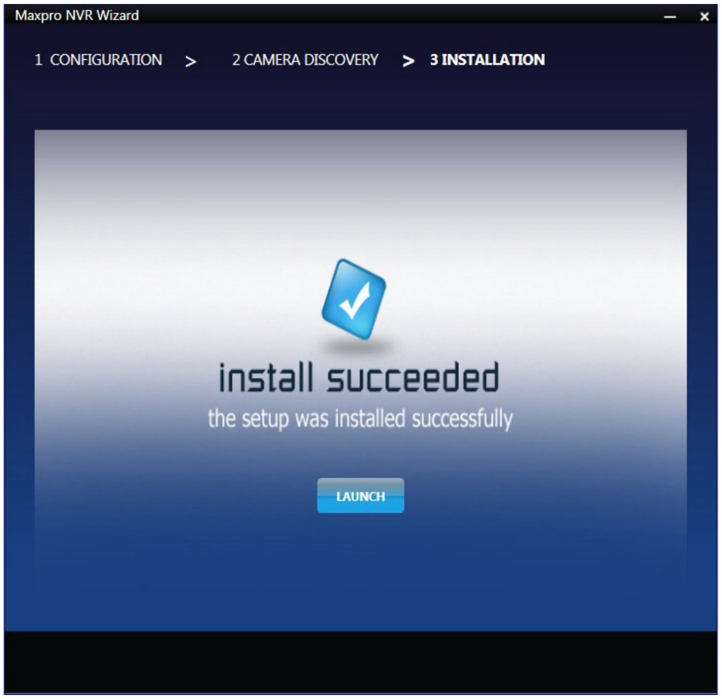
Available free channels in the system : 8 (Hint: System has 16 Analog channels configured. Any unused analog channels can be deleted from Configurator-> Camera tab in the Client to free up the license before adding IP cameras)

- Click BACK to return to the CONFIGURATION page or click DONE when the number of cameras discovered equals the number of connected cameras.

Caution: Only Honeywell IP cameras and HVE encoders (except Honeywell Performance Series and New equIP® Series IP cameras) are discovered and added in the MAXPRO NVR Wizard. To discover and add other third party PSIA/ONVIF compliant cameras, see the Discovering and Adding Third Party ONVIF and AXIS Cameras **section on page** 184**. For adding and configuring third party RTSP cameras, the RTSP settings must be specified, see** Adding RTSP Cameras/Encoders **section on page** 188**.**

Note: *MAXPRO NVR Wizard discovers only 1 channel for multi-channel Encoders and allows you to add only 1 channel from the wizard that is first channel. You can add the additional channels from the Camera tab.*

Step 3. The INSTALLATION page appears.



Maxpro NVR Wizard
1 CONFIGURATION > 2 CAMERA DISCOVERY > 3 INSTALLATION
install succeeded
the setup was installed successfully
LAUNCH

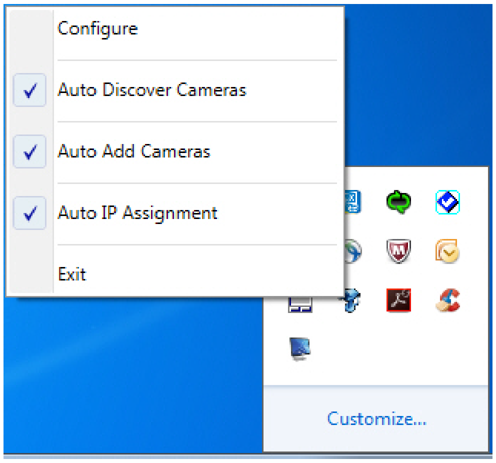
INSTALLATION page

- Click LAUNCH. The MAXPRO NVR Log On dialog appears. Please wait while the system logs you on automatically as a Windows Logged-In User. MAXPRO NVR launches and the Viewer tab appears. The Devices window on the left pane lists all the discovered network cameras.

Video is visible as soon as the cameras are dragged and dropped into the panels (also known as Salvo Layouts) on the Viewer. Refer Live Video section in *MAXPRO® NVR Operator's Guide* for more information.

MAXPRO NVR Wizard Settings on the Task bar

If you right-click the MAXPRO NVR Wizard on the Task bar, a shortcut menu appears with a list of quick configuration settings.



MAXPRO NVR Wizard Task bar Settings

Setting	Select..
Configure	To open the Configuration page.
Auto Discover Cameras	To automatically discover the cameras.
Auto Add Cameras	To automatically add the discovered cameras to the list.
Auto IP Assignment	To assign a valid address to cameras with Automatic Private IP Addressing (APIPA).
Exit	To close the MAXPRO NVR Wizard.

Navigating to Configurator tab

Step 1. Double-click the icon on your desktop. The MAXPRO NVR Log On dialog box appears.

Caution: Only on the Honeywell provided systems shipped with v4.0 or later version has a default Windows user name, NVR-Admin and password Password$123 is already configured and hence you automatically log in. Honeywell recommends you to create and use a new Administrator account to install and configure MAXPRO NVR. See Before you Begin - Changing the default Windows Administrator Account Created By NVR**, page** 103 **section for more information.**

Step 2. Clear the Windows Logged-In User check box and then type the Username. The default user name is admin.

Step 3. Type your Password. The default password is trinity.

Note: *Select the Windows Logged-In User check box for logging on using the Windows authentication (uses current logged in Windows account credentials). If the Windows Logged-In User check box is cleared, the MAXPRO NVR user name and password is used for authentication. If there is no profile set as default, then select the Profile corresponding to the MAXPRO NVR server to which you want to connect.*

Tip: Set profiles if you have multiple MAXPRO NVR units and use the drop-down to choose which NVR unit you would like to connect to.

Step 4. Select the Display Video on Alarm check box to display the viewer as an alarm monitor.

Note: *Alarm monitor supports pop-up of camera associated to IO events only. Pop-up on motion alarms is not currently supported.*

Step 5. Click Login. The Viewer screen appears by default.

Step 6. Click the Configurator tab to open the Configurator screen. The System page opens by default.

Configuring the System Settings

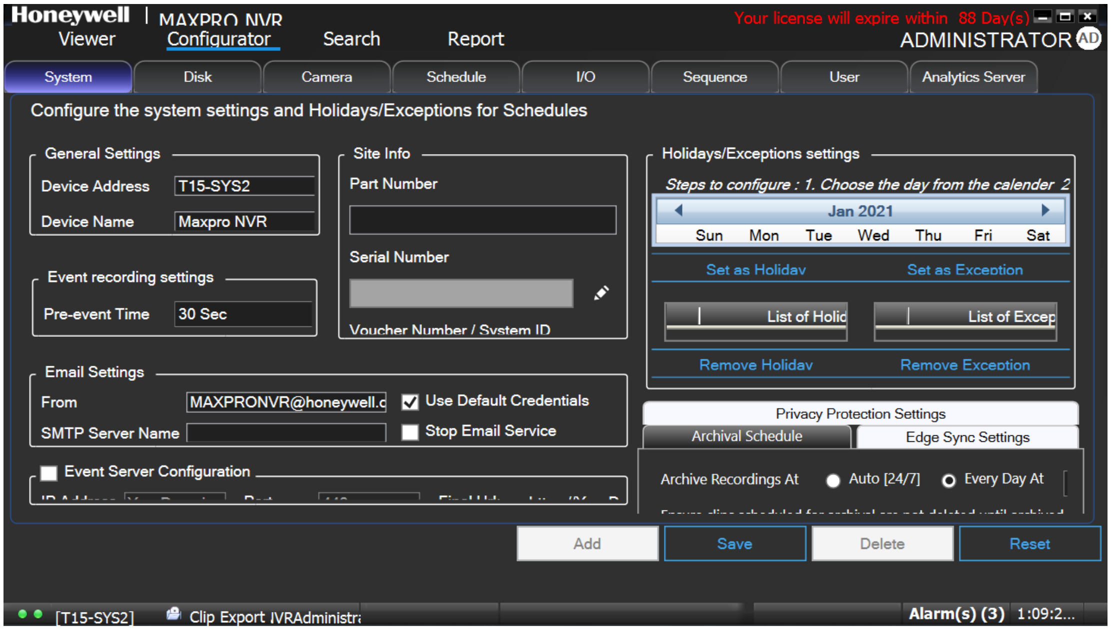
The System settings help in configuring the following:

- General System Settings - enable configuring the device name, device description, and device address for MAXPRO NVR.
- Event Recording Settings - enable configuring the times associated to event and user based recording.
- Email Settings - enable configuring the SMTP server settings for e-mail communication of events.
- Site Info - enable configuring and displaying the Site info and License type information.

- Archival Schedule - enable configuring the archive schedule for the recordings.
- Edge Sync Settings: allows you to sync and back fill the recordings from camera SD card to NVR. You can configure when to sync or back fill.
- Privacy Protection Settings: enables user to configure the type of masking in live video.See Privacy Protection Settings (GDPR Favored) for complete information.
- Holiday/Exception Settings for Schedules - enable configuring the holidays and exceptions for schedule based recording.

To view the system settings

- Click the Configurator tab. The System page appears by default.



Device Address T15-SYS2

Device Name Maxpro NVR

Pre-event Time 30 Sec

From MAXPRONVR@honeywell.c ☑ Use Default Credentials

□ Stop Email Service

□ Event Server Configuration

Archive Recordings At ● Auto [24/7] ○ Every Day At

System page

Configuring General Settings

The general settings enable configuring of the device address, device name, and device description for MAXPRO NVR.

Under General Settings

- The Device Address displays by default. You can type a new device address as applicable.
- The Device Name displays by default. You can type a new device name as applicable.
- The Description of the device displays by default. You can type a new description as applicable.

Tip: The information in the Device Address and the Device Name fields is mandatory. Device Address must be set to the machine name or IP address of the NVR for the system to work properly.

Event Recording Settings

The event recording settings enable configuring of the times associated to video motion detection and user based recording.

Under Event Recording Settings

- The Pre-event Time (the length of time (in seconds) recording takes place before motion is detected) and displays by default. Select a new Pre-event Time as applicable. You can set this value from NONE to 15 seconds. The default Pre-event Time is 5 seconds.
- The default Record for time is 30 seconds. This is the amount of time that the NVR records or boosts recording frame rate after the motion event trigger time. You can set this value from 5 seconds to 5 minutes.

Note: *Honeywell recommends that you retain the default setting of 30 seconds to get optimal recorded time on an event.*

- The User based Recording Time (duration for which the recording is done after the user action) displays by default. Select a new User based Recording Time as applicable. The user based recording is the recording initiated by the user manually and is applicable for all the cameras connected to MAXPRO NVR.
  To start user based recording
  Right-click the panel displaying live video and click Start Recording.
  To stop the recording
  Right-click the panel displaying live video and click Stop Recording.

Email Settings

The email settings enable configuring of the SMTP server settings for email communication of events.

Under Email Settings

- Type the From address
- Type the SMTP Server Name.
- The Port displays by default. Type a new Port number as applicable.
- Type the User Name of the user.
- Type the Password of the user.
- Select the Use Default Credentials check box if you want to use the credentials that are used while logging on.

- Select the Stop Email Service check box, if you do not want to send an email from the configured settings.
- Select the Enable SSL check box.

Site Info Settings

Site Info settings allows you to quickly provide or refer the information related to Part Number, Serial Number, Voucher Number/System ID and the type of license being used to a support focal.

Note: *For MAXPRO NVR turnkey solutions shipped with v4.0 or later version, the Site Info details are configured in the factory.*

Under Site Info

- Type the Part Number of the NVR box. If the field is empty, the part number can be input without any credentials. To modify the Part Number, click ✎ and then type the factory password provided by Honeywell Technical Support.
- Type the Serial Number. To modify the Serial Number, click ✎ and then type the factory password provided by Honeywell Technical Support.
- The Voucher Number/System ID is displayed by default and it is non-editable.
- The License Type details are displayed by default and it is non-editable.
- Under Notes type any required information regarding the site based on your requirements.

Archival Schedule Settings

The Archival Schedule settings enables you to configure the archiving schedule for your recordings. Ensure that the storage drive (NAS or SAN or USB) is configured in Disk tab and select the Drive Purpose as Archival. See Configuring the Disk Management Settings section on page 167 for more information. To configure NAS drive for recording, see Guidelines to configure NAS Drive for Recording section on page 245 for complete information.

Under Archival Schedule

- Click Auto [24/7] option to archive the recordings automatically 24/7.
  Or
  Click Every Day at option to select the required time for archival from the drop-down list.
- Select Ensure Clip scheduled for archival are not deleted until archived check box to ensure that clips will not be deleted by the system until it is

archived. If the clip deletion schedule is reached for a specific clip then this feature will retry and archive the clip.

Note: *The default Archival Schedule configured and recommended is Every Day at 12:00 AM. This is recommended versus the Auto [24/7] option for optimal performance and load on NVR.*

The default Archival Schedule configured and recommended is Every Day at 12:00 AM. This is recommended versus the Auto [24/7] option for optimal performance and load on NVR.

Edge Sync Settings

Edge Sync settings enables you to set the schedule for synchronizing the recordings from the camera SD card. This feature is supported for Profile-G compliant cameras where the recordings are stored at the camera level.

Under Edge Sync Recording at:

- Click Every option and then select the time in minutes or hours to synchronize the recordings.
  Or
  Click Every Day at option to set the specific time in hours during which the synchronizing should trigger.
- Limit Past Sync: This option allows you to set number of days passed for which you want system to sync the recordings from camera. For example - if you set 10 days, then system will sync the recording within last 10 days from camera.

Manual Archival

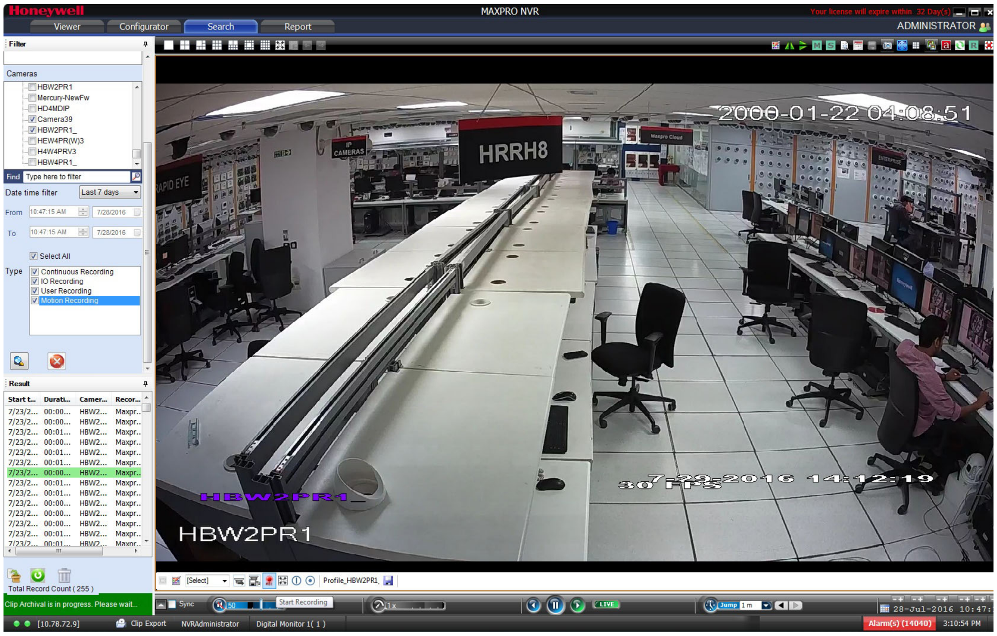
Manual archive can be performed in Search tab. You need to search and then archive the required recording. Before performing the manual archive ensure that you configure the drive in Disk tab and select the Drive Purpose as Archival. See Configuring the Disk Management Settings section on page 167.

To perform manual archive:

Step 1. Navigate to Search tab and search the required Recording. Refer *MAXPRO NVR Operator's Guide*, How to search for recorder video and events section for more information. The recorded video is searched based on the search conditions. The search results are listed in the Results window.

Step 2. In the Results pane, select the required recording from the list of recording. Press Ctrl to select multiple recordings.

Step 3. Click ![] at the bottom of the pane. The Clip Archival is in progress. Please Wait... message is displayed Archive Progress.



Filter

Cameras

- □ HBW2PR1
- □ Mercury-NewFw
- □ HD4MDIP
- ☑ Camera39
- ☑ HBW2PR1_
- □ HEW4PR(W)3
- □ H4W4PRV3
- □ HBW4PR1_

Find: Type here to filter

Date time filter: Last 7 days

From: 10:47:15 AM 7/28/2016

To: 10:47:15 AM 7/28/2016

☑ Select All

Type:
- ☑ Continuous Recording
- ☑ IO Recording
- ☑ User Recording
- ☑ Motion Recording

Result

Start t...	Durati...	Camer...	Recor...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...

Total Record Count (255)

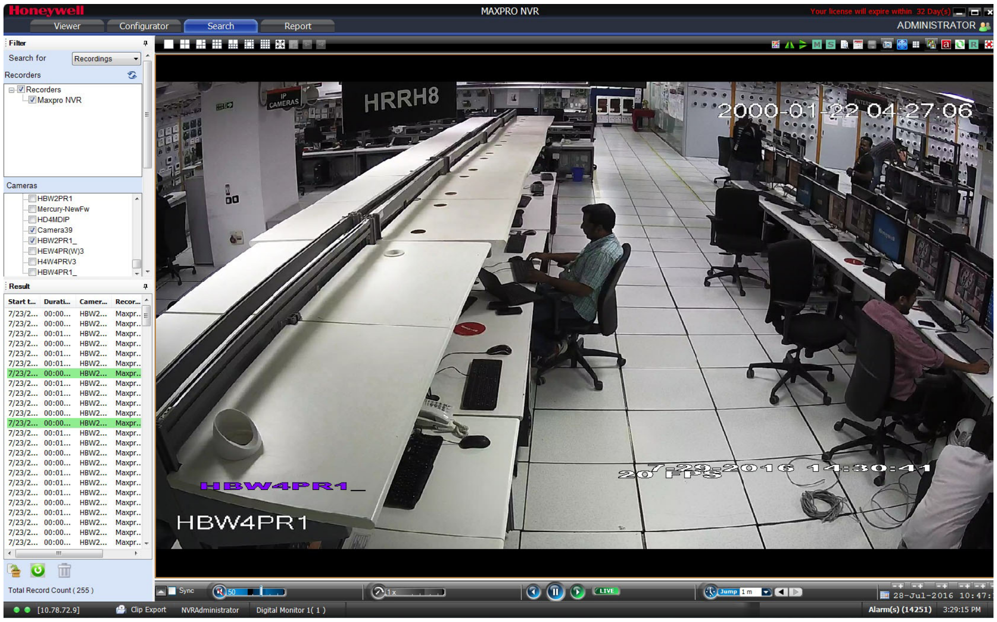
Clip Archival is in progress. Please wait...

[10.78.72.9] Clip Export NVRAdministrator Digital Monitor 1(1)

Archive Progress

Note: *If the Archival type Disks is not configured then you cannot archive the clips manually and Failed to archive clip message is displayed.*

Once the Manual Archive is success then the selected clips are displayed in Green color (Archive Progress) and a Manual archival folder is created automatically for the respective camera. If it fails then the selected clips are displayed in Pink color.



Filter

Search for: Recordings

Recorders

- ☑ Recorders
  - ☑ Maxpro NVR

Cameras

- □ HBW2PR1
- □ Mercury-NewFw
- □ HD4MDIP
- ☑ Camera39
- ☑ HBW2PR1_
- □ HEW4PR(W)3
- □ H4W4PRV3
- □ HBW4PR1_

Result

Start t...	Durati...	Camer...	Recor...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:01...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...
7/23/2...	00:00...	HBW2...	Maxpr...

Total Record Count (255)

[10.78.72.9] Clip Export NVRAdministrator Digital Monitor 1(1)

Holidays/Exceptions Settings

The holidays/exceptions settings enable setting of the holiday and exceptions for schedule based video recording.

Step 1. Under Holidays/Exceptions

To set holidays and exceptions

- Select a day from the calendar, and click Set as Holiday to set the selected day as a holiday. The selected holiday displays under List of Holidays.
- Select a day from the calendar, and click Set as Exception to set the selected day as a exception. The selected exception displays under List of Exceptions.

To remove holidays and exceptions

- Under List of Holidays, select the check box for the holiday you want to remove, and then click Remove Holiday.
- Select the check box for the exception you want to remove, and click Remove Exception.

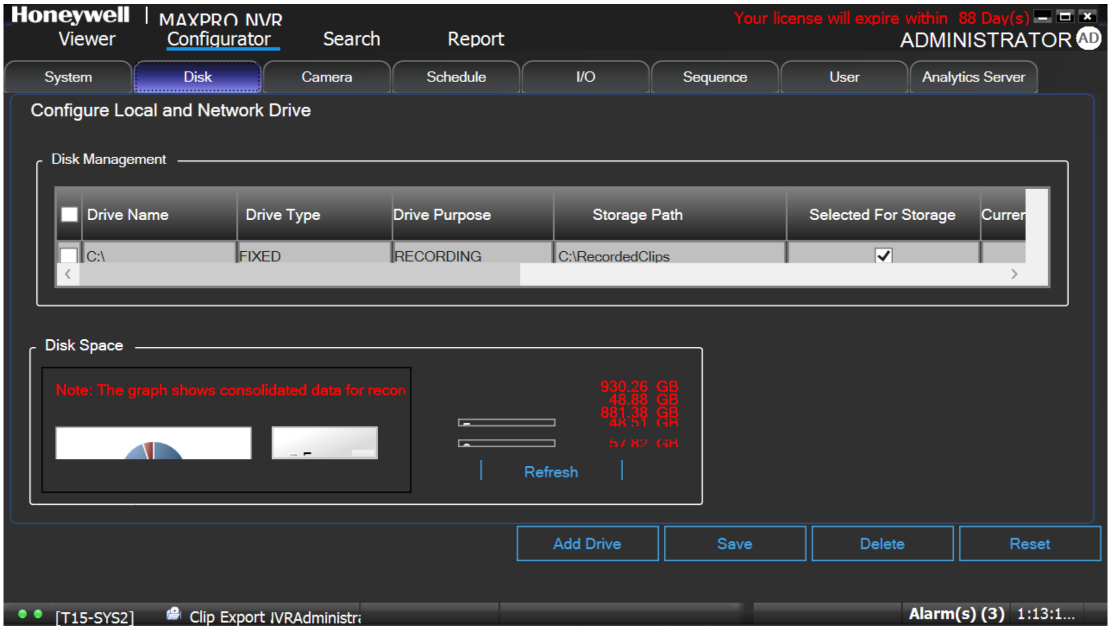
Step 2. Click Save to save the information or click Reset to clear the information entered.

Configuring the Disk Management Settings

Disk Management helps you to configure the disk settings for saving the recorded video. All the drives available on the MAXPRO NVR system are automatically added in the Disk Management page. To configure NAS drive for recording, see Guidelines to configure NAS Drive for Recording section on page 245 for complete information.

Step 1.	Click the Configurator tab. The System page displays by default.

Step 2.	Click the Disk tab to open the Disk Management page.



Your license will expire within 88 Day(s)

Configure Local and Network Drive

□ Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For Storage	Curren
□ C:\	FIXED	RECORDING	C:\RecordedClips	☑	

Note: The graph shows consolidated data for recon

Disk Management page

All the drives available on the MAXPRO NVR system are listed.

By default, the check boxes corresponding to all the drives except C:\ are selected. C:\ is reserved for the Operating System data.

Caution: It is recommended that you do not choose the operating system drive for saving the camera recordings (as a video storage drive). Selecting an Operating System drive for video storage can lead to system instability.

Step 3.	The following information displays under Disk Management.

- Drive Name - displays the drive name such as C:\, D:\ and so on.
- Drive Type - displays the drive type (Fixed or Network). To configure NAS drive for recording, see Guidelines to configure NAS Drive for Recording section on page 245 for complete information.
- Drive Purpose - displays the purpose of the drive (Recording/ Archival)

Note: *For Manual or Auto Archiving, ensure that you configure the Drive and select the Drive purpose option as Archival.*

Tip: By default, only the fixed drives are listed. See step 5 to explicitly add a network drive or fixed drive.

- Storage Path - displays the default storage path for saving the recorded video. You can type a new path for saving the recorded video.

- Selected for Storage - By default, this check box is selected for all the fixed drives that are listed except C: To disable video recording on a particular drive, clear the Select for Storage check box corresponding to the drive.
- Total Space (GB) - displays the total space available on the drive.
- Free Space (GB) - displays the free space available on the drive.
- Current Recording Drive - displays a status indicator indicating that recording is taking place on the drive. “Green” indicates that current recorded video is saved on the drive.
- NAS Domain - displays the domain name of NAS
- NAS Username - Type the username to access the NAS

Note: *If the domain, username and password mismatches with the external drive (NAS) credentials then TotalSpace(GB) column displays Invalid Drive message.To configure NAS drive for recording, see* Guidelines to configure NAS Drive for Recording *section on page* 245 *for complete information. If user adds a Network Drive for Archival without Domain, Username and Password then a validation message is displayed to provide the network credentials.*

- NAS Password - Type the password to access the NAS. If you select the NAS as the recording drive then ensure to follow the below.
- We should not use “-” during the share folder creation.
- If we select the shared drive for Recording, In NAS need to be create user say Administrator or NVR-admin with same password, where NVR services is running.
- If Neo services is running with “NVRservicesuser”, since we do not know the password of this user (due to Cyber security) even though if we are creating user in NAS, Recording will not work.

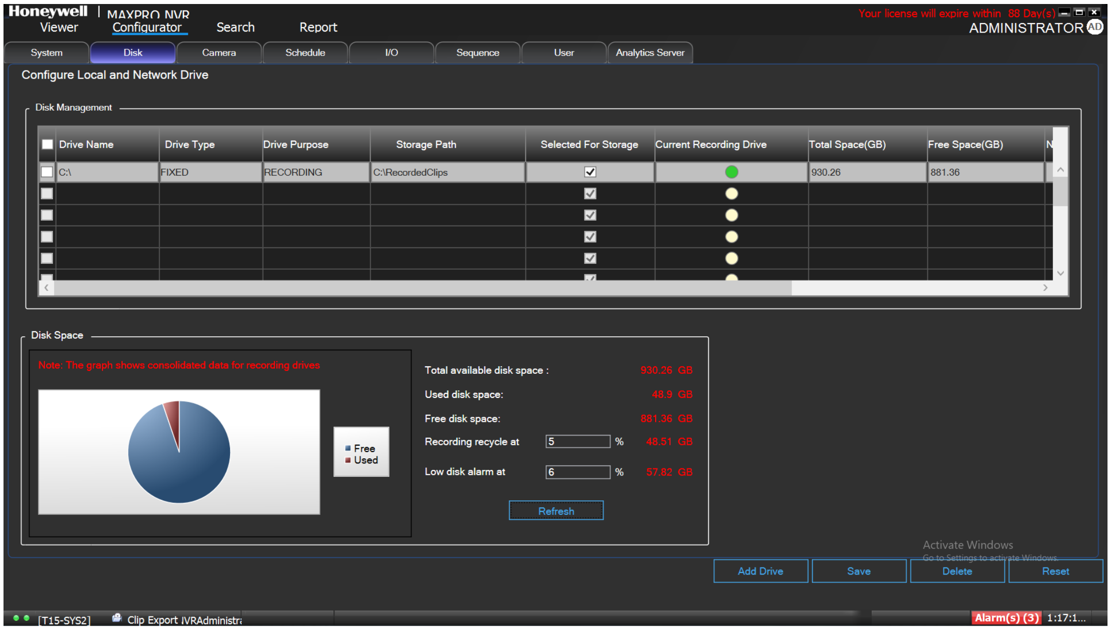
Step 4. Under Disk Space

The overall drive statistics specified for the recorded video at any point of time is indicated by the following fields:

- Total available disk space - displays the total storage space available on the drives used for saving the recorded video.
- Used non video disk space - displays the disk space used by non video data on the drives.
- Used video disk space - displays the disk space on the drives used for saving the recorded video.
- Free disk space - displays the free disk space available on the drives.

Note: *The statistics provided in the Disk Space section does not include Archival drives.*

You can also view a graphical illustration of the drive statistics with legends for each of the above fields.



Configure Local and Network Drive

Disk Management

□	Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For Storage	Current Recording Drive	Total Space(GB)	Free Space(GB)	N
□	C:\	FIXED	RECORDING	C:\RecordedClips	☑	●	930.26	881.36	
□					☑	○			
□					☑	○			
□					☑	○			
□					☑	○			

Disk Space

Note: The graph shows consolidated data for recording drives

Total available disk space : 930.26 GB

Used disk space: 48.9 GB

Free disk space: 881.36 GB

Recording recycle at 5 % 48.51 GB

Low disk alarm at 6 % 57.82 GB

Graphical Illustration

- In the Recording recycle at box, type a value. The Recording recycle refers to a state when the oldest video recordings are automatically deleted, if there is no disk space on the drives for new video recordings.
- In the Low disk alarm at box, type a value. The Low disk alarm refers to a state when the space on the drives for video storage is nearing the maximum size of the drives.

Caution: The Low disk alarm at value must be always greater than the Recording recycle at value.

Tip: Click Refresh to refresh the information under Disk Space at any point in time.

Step 5. Click Add Drive to add a fixed drive or a network drive.

- The fixed drive that you are adding must be available on the MAXPRO NVR system, else an “Invalid Drive” text displays in the Total Space (GB) column.
- Add Network Drive using map drive as \\Drivename\Folder.
- Add a network drive path in the following format: \\<IP address >\<folder name> for example, \\192.168.1.12\Recorded Clips.

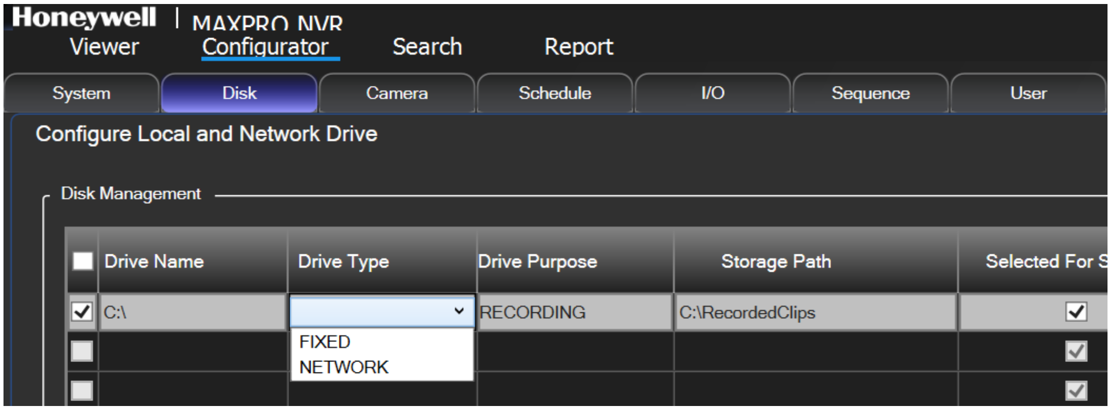
Note: *The Network drive added must be valid with proper folder permissions set for the installed default user, else an Invalid Drive text displays in the Total Space (GB) column.*

Caution: Please exercise caution while using a network drive as a Recording type video storage drive, since network interruptions and network performance can lead to loss of video recordings.

Step 6. Click Save to save the information or click Reset to clear the information entered.

Removing a drive

Step 1. Select the check box corresponding to the drive you want to remove as shown below.



☐	Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For S
☑	C:\		RECORDING	C:\RecordedClips	☑
☐					☑
☐					☑

Drive Type

Step 2. From the Drive Type drop-down list, select Network and then click Delete. By default Fixed drive is selected. If you try to delete the Fixed drive then a message Only Network Drives can be Deleted is displayed.

Caution: Do not delete all drives from the system otherwise user will not get an option to add the drives again. Contact to Honeywell technical support in case of this scenario.

Configuring the Cameras

Cameras are sources for a video input in MAXPRO NVR. The maximum number of cameras that can be configured in MAXPRO NVR depends on the model and for each camera you can also add multiple streams depending on the camera type. You can add the following types of cameras:

- IP Cameras/Encoders: MAXPRO NVR can automatically discovers these devices in the network and adds it to the MAXPRO NVR user interface. See the Adding IP Cameras / Encoders section on page 172 for more information.
- Analog Cameras: User is required to manually add these cameras to the respective channel and configure the camera. See the Adding/Deleting Analog Cameras section on page 202 for more information. The maximum number of analog cameras that you can configure in MAXPRO NVR Hybrid series (XE, SE, PE) is 16.

Adding IP Cameras / Encoders

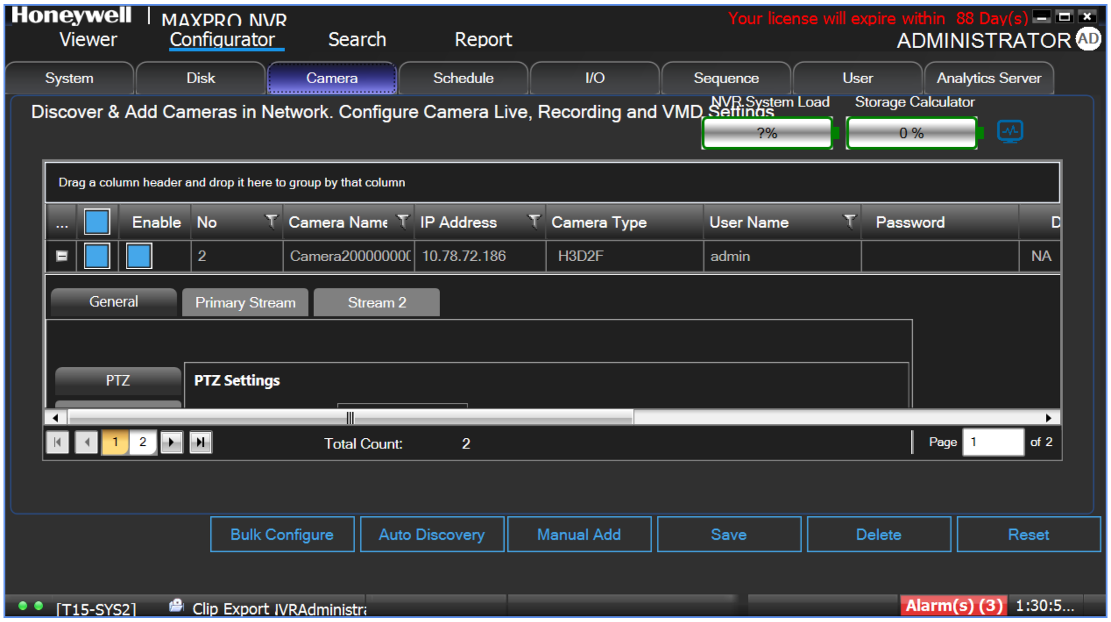
The MAXPRO NVR Wizard automatically discovers Honeywell cameras in the network and adds it to the MAXPRO NVR user interface. Alternatively, you can also discover and add all the supported cameras in MAXPRO NVR in the Camera page.

Note: *It is not recommended to add Encoder/Multi-channel video stream across NEO storage.*

To add IP cameras

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to open the Camera page.



Your license will expire within 88 Day(s)

Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

NVR System Load ?%

Storage Calculator 0 %

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	D
⊟	□	□	2	Camera20000000(	10.78.72.186	H3D2F	admin		NA

Total Count: 2

Page 1 of 2

Camera page

Note: *All Honeywell cameras that are discovered and added using the MAXPRO NVR Wizard appear in the Camera page when you first open it.*

Step 3. Click the Auto Discovery button, the Auto Discovery screen is displayed.

- Click Start Discovery to discover the cameras in the network. By default, the cameras discovered are displayed under Cameras Discovered pane.
  The cameras are added based on the IP range and Video Format settings. See the Configuring the Auto Discovery Settings section on page 180 for more information. Only device integrations with auto discovery support are discovered automatically in the NVR. All other devices need to be added manually.
- To add only specific cameras, select the required camera check boxes and then click Add Cameras. The selected cameras appear under the Camera pane.

Note: *The cameras added will have the default parameters for all their settings.*

Step 4. Under the Camera screen, select a camera to change the default parameters for the following settings.

- Enable/Disable - Enables or disables a camera for recording and live video. By default the check box corresponding to a camera to enable live video preview is selected. To disable live video preview, clear the check box corresponding to a camera. The live video appears under Preview at the bottom right corner of the camera General/Primary Stream page See the Configuring the Camera Properties section on page 176 for more information.
- Number - Displays the camera number. You cannot modify the camera number.
- Camera Name - Displays the camera name. You can type a new camera name limited to a maximum of 50 alphanumeric characters.
- IP Address - Displays the IP address of the camera. You can type the new IP address for the camera as applicable. The IP address should include the Port number 80. For example if the IP address is 111.221.0.333 then you should add the port number (80) as 111.222.0.333:80.
- Camera Type - Displays the type of camera.

Note:

- For the camera type, “Generic - RTSP, you must specify the RTSP settings for the camera in the camera properties. See the Adding RTSP Cameras/Encoders section on page 188 for more information.
- To add the discovered multi-channel encoders, see the Discovering and Adding Multi-channel Encoders section on page 185.

Note:

- User Name- Displays the default user name, “admin” for the camera. You can type a new user name for the camera as applicable. Change this only if the user has been changed on the camera.
- Password - Displays the password, if any, for the camera. You can type a new password for the camera as applicable. Change this only if the password has been changed on the camera.

Caution: The camera Username and Password in the NVR needs to match the username and password configured on the device for the NVR to be able to connect to the camera and get video.

- Device Stream No - Displays the channel ID. You cannot modify this field.
- Unique System No - Display the unique camera ID. You can modify and assign a new number as applicable.

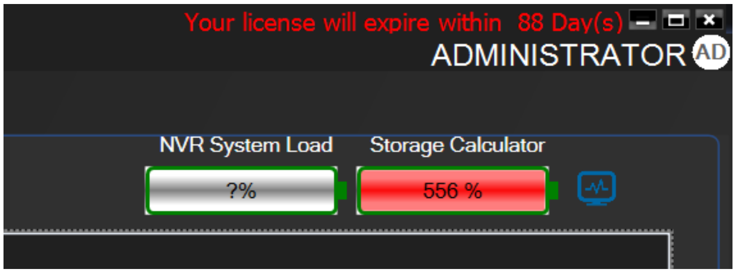
Note:

- Unique System Number can be used to assign a unique camera number across all your NVRs. This helps in having an unique camera number in your entire system.

- Unique System Number should not be modified for the NVRs upgraded from older versions to 4.0.
- For fresh installation of 4.0 we recommend the Unique System Number should be updated when the camera is added to the NVR system. If the Unique System Number is modified later then the older recording cannot be retrieved.
- Unique system Number can be discovered as callup number in VMS based on the user configuration in VMS discovery window.

Note:

- Stream Count - Displays the number of streams associated with the camera. By default it displays 1. if a additional stream is added then the stream count increases. Multistream or Dual stream is not supported for encoders.
- NVR System Load, Storage Calculator -


Your license will expire within 88 Day(s)

- NVR System Load provides system load estimate based on the estimation of recording bit rate of cameras currently configured on your NVR versus maximum recording bit rate supported for the NVR in graphical manner (Percentage load is displayed and the indicator changes to red if the load is above the limit).

Tip: Hover the mouse over the NVR System Load indicator for more details.

Note:

- Part Number of your NVR system should be entered in the System tab for the Maximum estimate to be shown in the System Load. Please reopen the NVR client after updating the part number, if the part number is updated after opening the client.
- NVR System Load is based on the recording bit rate only and does not include archival recording.
- Maximum Bit Rate is based on the part number entered in System tab and Current Bit Rate Estimate is based on the cameras configured in the NVR.
- For Software only NVR System, 4 Mbps bit rate per camera license is assumed to calculate the Maximum Bit Rate but the maximum bit rate supported can vary based on your NVR Server hardware specification.
- The Current Bit Rate Estimate is based on the estimated bit rate value for configured cameras based on standard conditions and can vary based on your site environment. All the estimated bit rate calculations are based on

fixed bit rate (Mbps) and might vary based on the site environment if the camera is set to VBR (variable bit rate) mode.

- It is very important to stay within the estimator guidelines to ensure the MAXPRO NVR will operate normally.
- Over configuration of the system can lead to unsatisfactory performance.

Note:

- Storage Calculator provides recording storage estimate based on the recording configuration (bit rate estimate of cameras, recording schedule and retention) of current cameras on NVR versus the maximum Recording storage drive space supported by the NVR in graphical manner (Percentage recording storage estimate is displayed and the indicator changes to red if the storage estimated is above the NVR recording storage capacity).

Tip: Hover the mouse over the Storage Calculator indicator for more details.

Note:

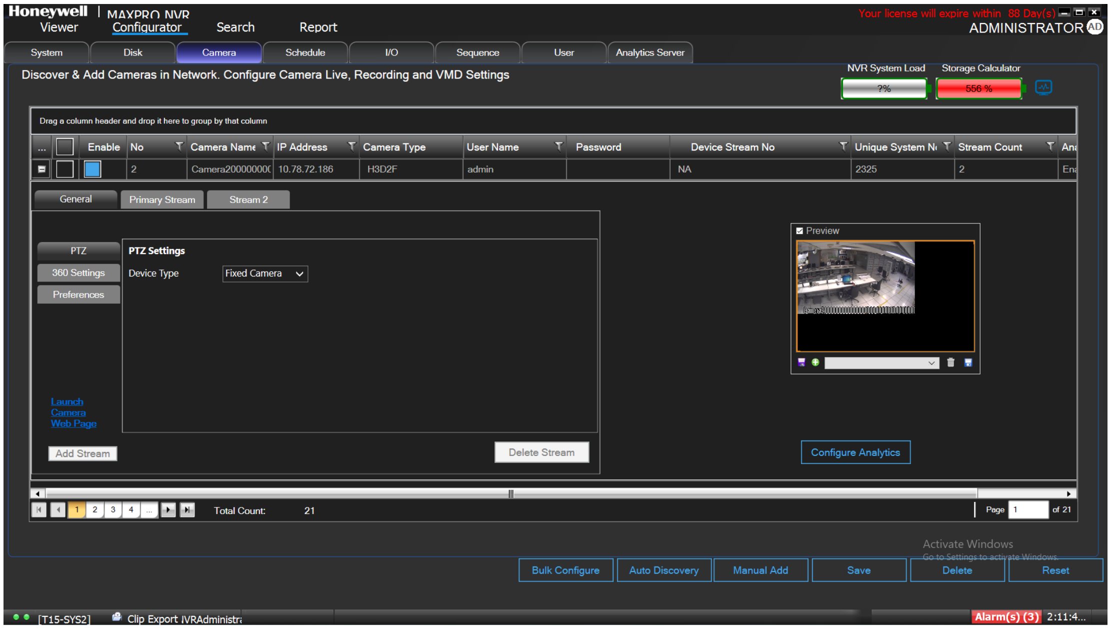
- Archival storage calculations is not included in the estimation.
- This is an estimate for reference purpose only. While providing a reasonable storage estimate it should not be inferred that the results are absolute and will apply to all the systems and locations.
- Recording bit-rate and duration can be dramatically effected by PTZ cameras, higher levels of activity, image quality, light levels and noise.
- All the Estimator calculations are based on the fixed bit rate (Mbps) and might vary based on the site environment if the camera is set to VBR (variable bit rate) mode.

Note:

Tip: Click on the Status Monitor icon 🖥 to launch status monitor. Refer to the ***MAXPRO NVR Operator’s Guide*** for more information on using MAXPRO Status Monitor.

Configuring the Camera Properties

Step 1. For the required camera, click ⊞ on the left corner to open the camera properties pane see the Figure .



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count	An
⊟	□	■	2	Camera20000000(	10.78.72.186	H3D2F	admin		NA	2325	2	Ena

PTZ Settings

Device Type: Fixed Camera

Camera Properties pane

Step 2. Click Launch Camera Web Page to launch the web page for the camera. Use the camera's web page to view IP and firmware settings, bit rate statistics, camera exposure, day night and white balance settings, and set up video motion detection and other analytic events.

Step 3. Under General > PTZ > PTZ Settings

- Device Type - Select whether the camera is a PTZ or fixed.
- PTZ Sensitivity - Select the PTZ Sensitivity for PTZ camera. Available PTZ options are: Minimum, Low, Normal, High and Maximum.

Note: *The PTZ Sensitivity field is not available for fixed cameras.*

Step 4. Under General > 360 Settings

Note: *If Camera Type is OnCam Grandeye Fisheye (OnCam-GE-***-Fisheye), the 360 Settings tab does not display Enable Panamorph, Immervision settings and shows Enable Dewarping, OnCam Grandeye settings.*

- Enable Panamorph: Select the Enable Panomorph check box to enable the Panomorph feature.
- Mounting position: Select the Mounting Position. You have three options to choose from: Wall, Ceiling, and Ground.
- Modes: Select the Mode for the camera. The available modes are PTZ Mode, Quad Mode, and Perimeter Mode. The default mode is PTZ Mode

- Lens ID: Select the Lens ID for the camera. The supported lens ids from v3.5 or later are A0**V, A0IFV, A0NKV, A1UST, A8TRT, B0QQV, B4QQV, B5SST, B6SST and B8QQT. By default A0**V Lens

Caution: Only Immervision certified camera models can support this feature enabled. Before configuring this feature, please check whether your camera has the Panomorph lens.

Note:

- To view live video from Immervision certified cameras, Refer Video Viewing Options from Immervision Enabled Cameras section in *MAXPRO NVR Operator's Guide*.
- The recommended Aspect Ratio for Immervision Certified cameras is 4:3.

Note:

- Enable Dewarping: Select the Enable Dewarping check box to enable the dewarping feature for OnCam Grandeye fisheye cameras.
- Mounting position: Select the Mounting Position. You have three options to choose from: Wall, Ceiling, and Ground.
- Modes: Select the Mode for the camera. The available modes are Virtual camera view, Panorama 2x180 views, Panorama 1x360 view and Panorama 1x180 view.

Note: *To view live video from OnCam Grandeye cameras, Refer Video Viewing Options from OnCam Grandeye Cameras section in MAXPRO® NVR Operator's Guide.*

Step 5. Under General > Preference > Stream Preference Settings

- Live - Select the preferred stream of the camera which you want to use for streaming live video.
- Continuous - Select the preferred stream of the camera which you want to record continuously.
- Event Recording - Select the preferred stream of the camera which you want to record on events.
- Mobile/Web - Select the preferred stream of the camera which you want to use for streaming in Mobile/Web application.
- Anonymization Algorithm: Select the preferred algorithm option to anonymize the live video scene based on the environment.The available options are:
- Variable Scene: If the scene contains both stationary and moving people or objects then select this option to anonymize the objects in the scene.
- High Motion Scene: To anonymize the objects in high motion in the scene.
- Still Scene: To anonymize the objects in a scene where the scene predominantly contains stationary people and objects.
- High Resolution - Select the preferred stream of the camera which you want to categorize as High Resolution stream.

- Low Resolution - Select the preferred stream of the camera which you want to categorize as Low Resolution stream.

Note: *The stream selected as Low Resolution settings will be used in SMART VMD.*

- Multicast Enabled - Select this check box to enable the Multicast feature for the camera. After selecting the check box enter the following details:
- Multicast Address: Type the Multicast IP address.
- Multicast Port: Type the Multicast IP Port number.

Step 6. Under Primary Stream > Recording > Video Quality Settings

- Resolution - The Resolution is defaulted to a fixed value based on the camera model (for example, HD3MDIP model defaults to 1280 x 720 resolution).
- Frame Rate - Select the FPS for a camera. FPS refers to the number of pictures displayed in exactly one second. FPS is a measure of how much information is used to store and display motion video. The term applies to digital video. Each frame is a still image; displaying frames in quick succession creates the illusion of motion.

Note: *30 FPS is the maximum frame rate in NTSC format and 25 FPS is the maximum frame rate in PAL format supported by MAXPRO NVR.*

Ensure that you set the Primary stream for recording which is 720p resolution and secondary stream for Live which is 4CIF. See Recommended stream Settings *section for more information.*

You can set the Bit rate value in the specific camera web page.

- Video Codec Type - Select the Codec type for the camera. The available options are H.264, H.265 and MJPEG. H.265 cameras can render in both CPU and GPU modes. To know about improvised GPU rendering capability, To know about improvised GPU rendering capability, see Improved GPU Rendering section on page 242 section.

Limitations of H.265 Codec Type:

- H.265 is not supported in MAXPRO Mobile app
- H.265 is not supported in Web client.

Note: *Only HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D and HDZ302DIN model cameras support H.265 Codec type.*

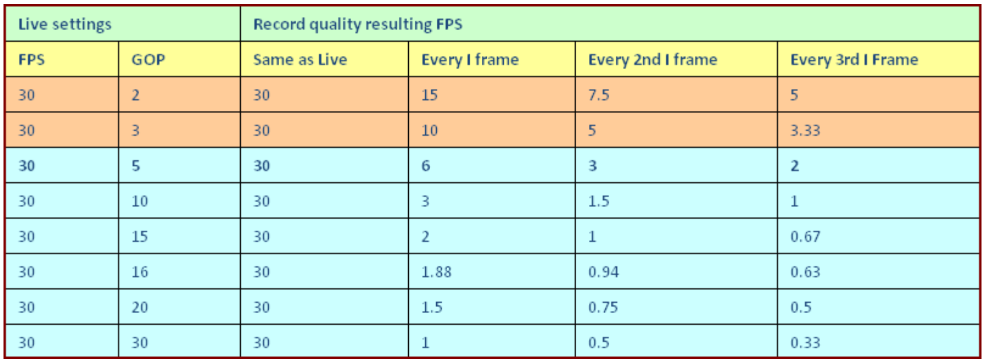
- Compression Level - The Compression Level is defaulted to “Medium”. You can select a new Compression ratio as applicable.
- GOP - The GOP is defaulted to “5”. Type a new GOP as applicable. Group of Pictures (GOP) are individual frames (number of pictures) that are grouped together and played back for viewing. A GOP consists of “IFrame” picture type that represents a fixed image independent of other picture types. Each GOP begins with this type of picture.

- Video Format - Select the Video Format (NTSC or PAL). The NTSC and PAL are the widely used video formats.
- Streaming Mode - The Streaming Mode is defaulted to UDP. You can select TCP streaming mode as applicable. The Streaming Mode is supported only for specific models of Honeywell, AXIS and ONVIF Cameras.
- Continuous - Select the FPS for Continuous recording.
- Event - Select the FPS for Event based recording.

Live/Recording Quality can be varied by controlling GOP. The formula for this is calculated as follows: Recording Quality resulting FPS = Live FPS/(GOP*I Frame Number for recording).

For example, in the following table if Live FPS is configured as “30” and Continuous recording is set to record “Every I frame” and Event recording is set to “Same as Live” with GOP value set to “5”, the result is 6 FPS continuous recording quality and 30 FPS event recording quality.

Note: *GOP value below 5 may not be achieved from all the cameras.*



Live settings		Record quality resulting FPS			
FPS	GOP	Same as Live	Every I frame	Every 2nd I frame	Every 3rd I Frame
30	2	30	15	7.5	5
30	3	30	10	5	3.33
30	**5**	**30**	**6**	**3**	**2**
30	10	30	3	1.5	1
30	15	30	2	1	0.67
30	16	30	1.88	0.94	0.63
30	20	30	1.5	0.75	0.5
30	30	30	1	0.5	0.33

- Enable Edge Sync- This option is supported for Profile-G compliant cameras and used for checking whether the camera is really Profile-G compliant. Click the Get Configuration button, if the camera is a Profile-G compliant camera then the Get Configuration button disappears and Enable Edge Sync check box is enabled. Select the check box and then Sync/view the recordings using Edge Sync Settings option from the Systems tab.
  If the camera is not Profile-G compliant then NVR application displays Edge Sync not supported or enabled for this device message at the bottom.

Step 7. If audio is supported for the camera then Enable Audio check is displayed. Select the check box to enable audio. 1-way audio (camera to NVR) is supported for specific IP cameras. Please visit URL: http://www.security.honeywell.com/hota/ for the compatibility list and the models supported.

Note: *Profile-G compliant camera time should be in sync with NVR time.*
Ensure you configure the NTP server to avoid Time Sync related issues.

Step 8. Under Primary Stream > Schedules:

- Recording Settings:

    - Continuous Recording - All cameras added are defaulted to “24/7” recording. You can choose a different option from the drop-down list.
    - Event Based Recording - This is “None” by default. Select an option from the drop-down if you want to do motion/event based recording.
- Recording Deletion Settings:
    - Type the required number (Days) for the Continuous Recording video deletion duration.
    - Type the required number (Days) for the Event Recording video deletion duration.

Note: *If user is upgrading from 6.0 to 6.3 then whatever value user selected in 6.0 will be converted to days in 6.3. Similarly if user un installs 6.3 then the value entered is mapped to nearest bigger number in the drop down list.*

- Archive Recording Older Than:
    - Continuous - This is “None” by default. Select an option from the drop-down if you want to archive the continuous recording.
    - Event - This is “None” by default. Select an option from the drop-down if you want to archive the event recording.
- Delete Archived Recording After:
    - Continuous Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived continuous recording can be deleted.
    - Event Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived event recording can be deleted.

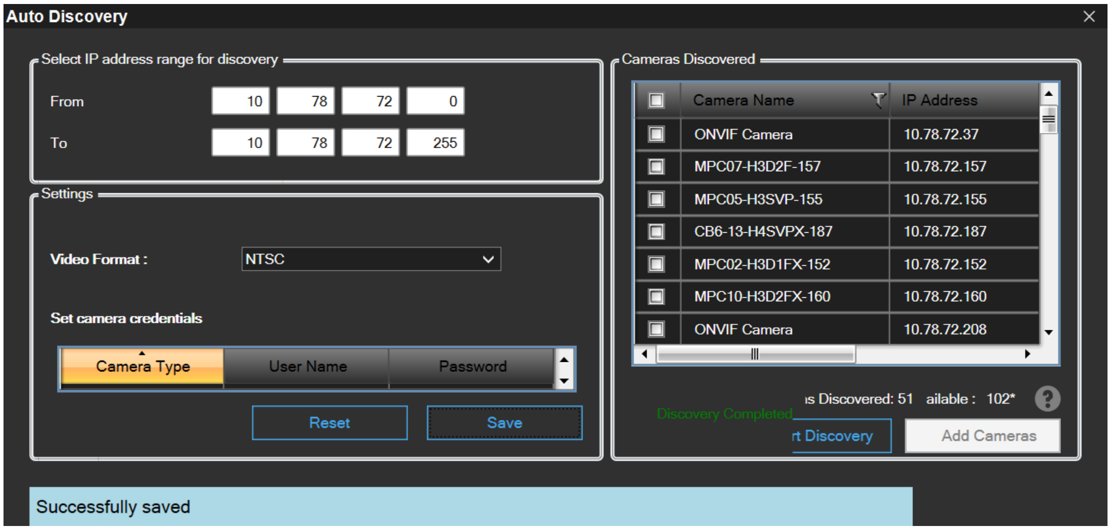
Step 9. Under Primary Stream > Preferences > Stream Preferences Settings. See step 5 for more information.

Step 10. Click Save.

Configuring the Auto Discovery Settings

The Auto Discovery Settings enable you to select the IP address range for discovery, set the video format (NTSC/PAL), username and password of a camera as it is being added to the NVR from the Discovery window. The Username and Password set for the camera in MAXPRO NVR must match the username and password on the camera (actual device) to stream video into MAXPRO NVR. See the Figure .

Note: *Auto Discovery Settings are only applicable for Honeywell, AXIS and ONVIF cameras.*



From: 10 . 78 . 72 . 0

To: 10 . 78 . 72 . 255

Video Format : NTSC

	Camera Name	IP Address
□	ONVIF Camera	10.78.72.37
□	MPC07-H3D2F-157	10.78.72.157
□	MPC05-H3SVP-155	10.78.72.155
□	CB6-13-H4SVPX-187	10.78.72.187
□	MPC02-H3D1FX-152	10.78.72.152
□	MPC10-H3D2FX-160	10.78.72.160
□	ONVIF Camera	10.78.72.208

Discovery Completed

ıs Discovered: 51 ailable : 102*

Successfully saved

Auto Discovery Window

To configure the Auto Discovery Settings

- On the Camera page, click the Auto Discovery button, the Auto Discovery screen appears. Perform the following:
- Under Select the IP Address range for discovery, type and set the IP address in From and To fields.
- Under Settings, select “NTSC” or “PAL” from Video Format list.
- Under Set camera credentials
- Type a Username for the camera.
- Type a Password for the camera.

Note: *You cannot edit the Camera Type field. The cameras credentials settings provides the username and password for Honeywell (for models already added in NVR database), AXIS (for models already added in NVR database) and ONVIF cameras discovery and addition. If a Honeywell or AXIS ONVIF model that is not already added in NVR database is discovered, then the camera credentials set for ONVIF is used for discovery and addition. You can find all the models that are already added in NVR database by checking the models listed in the Camera Type drop-down in the Camera tab.*

- Click Apply to save the changes or click Reset to clear the information entered. The username and password entered is applicable for all NTSC or PAL cameras. However, the username and password can be changed while configuring a particular camera.

Adding Additional Streams for a Camera

MAXPRO NVR V4.0 supports adding multiple streams for a single camera. The number of streams that can be added depends on the model of the camera. You can also configure each stream for a specific device based on your need. For example you can configure the first stream for Live recording and the second stream for event based recording. Multistream or Dual stream is not supported for encoders.

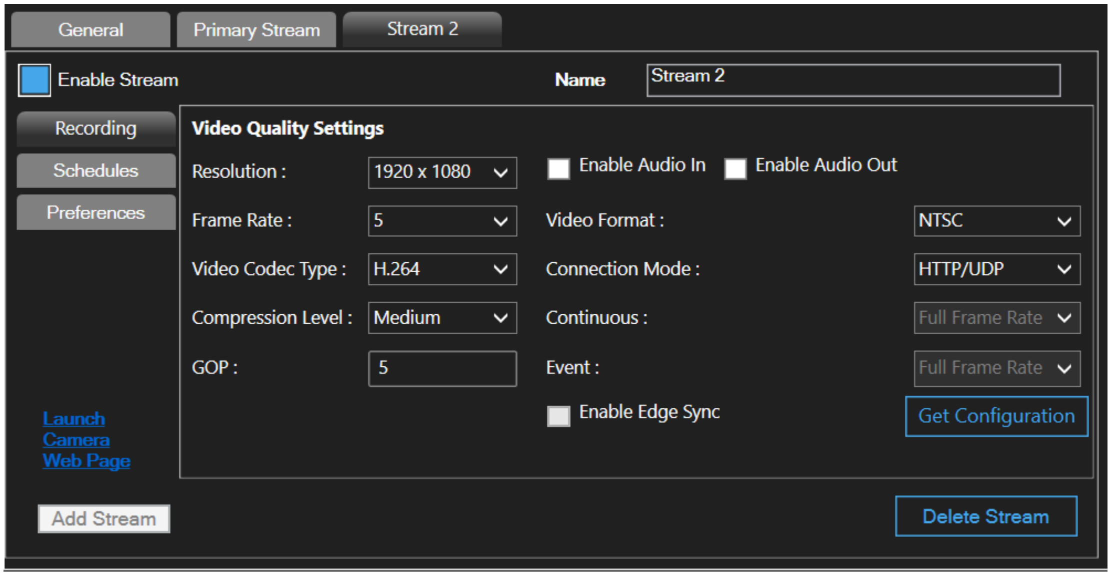
Note: *It is not recommended to add Encoder/Multi-channel video stream across NEO storage.*

To configure the additional streams for a camera

Step 1. Click the Camera tab, the camera page is displayed with the list of cameras discovered.

Step 2. For the required camera, click ⊞ on the left corner, the camera properties pane is displayed see the Figure .

Step 3. Click the Add Stream button, an additional stream (Stream 2) is added see the Figure .



■ Enable Stream

Name: Stream 2

Video Quality Settings

Resolution : 1920 x 1080

Frame Rate : 5

Video Codec Type : H.264

Compression Level : Medium

GOP : 5

□ Enable Audio In □ Enable Audio Out

Video Format : NTSC

Connection Mode : HTTP/UDP

Continuous : Full Frame Rate

Event : Full Frame Rate

□ Enable Edge Sync

Adding Stream

Note:

- Based on the type of camera the Add Stream button is enabled/disabled. If the camera supports additional streams then the Add Stream button is enabled. You can add streams until the button is enabled.
- System stream limit is 128. This is the maximum number of streams that can be added including multi-stream for cameras and multi-channel encoders or multi-imager 180/360 cameras. Multistream or Dual stream is not supported for encoders.

Note:

Step 4. Under Stream 2:

- Type the required Name for the additional stream.
- Select Enable Stream check box to enable the stream Or clear the check box to disable this stream.

Step 5. For the Stream 2 Recording, Schedules, Preference settings, repeat step 6 through step 10 of Configuring the Camera Properties section on page 176. Similarly you can add and configure multiple streams for a camera.

Note: *Ensure that the Resolution and FPS should match with the Camera and the NVR secondary stream settings, else live video can not be displayed.*

Ensure that you set the Primary stream for recording which is 720p resolution and secondary stream for Live which is 4CIF. See Recommended stream Settings *section for more information.*

You can set the Bit rate value in the specific camera web page.

Deleting Additional Streams

Step 1. For the required camera, click ⊞ on the left corner, the camera properties pane is displayed see the Figure .

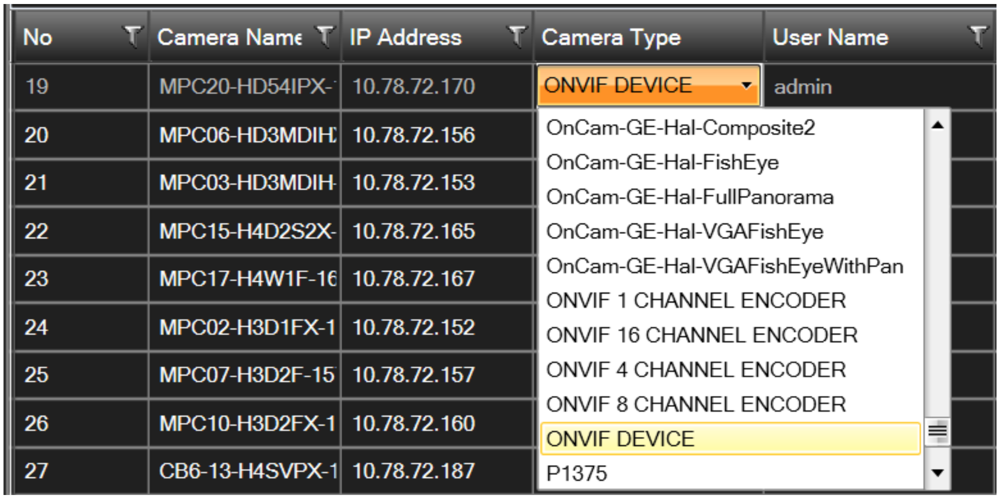
Note: *If an additional stream is added then only the Delete Stream button is enabled.*

Step 2. Click the required stream tab (For example Stream 1, 2, 3) and then click the Delete Stream button. A confirmation message Do you really want to delete the stream? is displayed at the bottom of the screen.

Step 3. Click Yes to delete Or click No to cancel. If you delete the primary stream then all the configured child streams will be deleted.

Discovering and Adding Third Party ONVIF and AXIS Cameras

The third party ONVIF and AXIS cameras that are discovered in the MAXPRO NVR user interface do not display the model name. However, the Camera Type field associated to the ONVIF and AXIS cameras displays “ONVIF DEVICE” and “No Streamer Type” in the Camera Discovered pane on the Auto Discovery screen.



No	Camera Name	IP Address	Camera Type	User Name
19	MPC20-HD54IPX-	10.78.72.170	ONVIF DEVICE	admin
20	MPC06-HD3MDIH	10.78.72.156		
21	MPC03-HD3MDIH-	10.78.72.153		
22	MPC15-H4D2S2X-	10.78.72.165		
23	MPC17-H4W1F-16	10.78.72.167		
24	MPC02-H3D1FX-1	10.78.72.152		
25	MPC07-H3D2F-15	10.78.72.157		
26	MPC10-H3D2FX-1	10.78.72.160		
27	CB6-13-H4SVPX-1	10.78.72.187		

Camera Type field displaying “ONVIF DEVICE” for a ONVIF camera

You must add the discovered camera(s) using the Add Cameras button to view the model name(s). After adding the camera(s), you can view the model name(s) from the Camera Type
drop-down list in the left pane of the Camera page.

AXIS and ONVIF cameras also support the TCP and UDP based streaming modes. You can choose the required streaming mode during the configuration depending upon what camera supports.

Tip: To discover and configure the AXIS Camera/Encoders as an ONVIF device in MAXPRO NVRs, see Appendix B MAXPRO®NVRs - AXIS Camera/Encoders Discovery and Configuration (using ONVIF) section on page 425.

To add third party ONVIF cameras in MAXPRO NVR through Auto Discovery

Step 1. In the Camera page, click the Auto Discovery button. After the discovery select the required check boxes of third party ONVIF cameras.

Step 2. Under Settings, select the Video Format from the drop-down list.

Step 3. Under Set camera credentials, type the User Name and Password of the third party ONVIF camera.

Step 4. Click Save.

Step 5. Click the Add Cameras button to add the camera.

Tip: After adding a third party ONVIF camera model using Auto Discovery, you can also manually add a new third party ONVIF camera. Click the **Manual Add** button located at the bottom of the **Camera** page and then select the model from the **Camera Type** drop-down list.

Adding ONVIF devices manually when Auto discovery is not supported

MAXPRO NVR v3.5 or later supports manual addition of ONVIF cameras and encoders with the support of additional device types - ONVIF DEVICE (for cameras) and ONVIF ENCODER DEVICE (for encoders).

To manually add ONVIF devices in MAXPRO NVR when Auto Discovery is not supported

Note: *Manual addition is recommended only when auto discovery is not supported in case of camera/encoder streaming across subnets.*

Step 1. Click Manual Add. A new camera is added in the camera pane.

- From the Camera Type drop-down list, select the required ONVIF DEVICE (for cameras) or ONVIF 1/4/8/16 CHANNEL ENCODER DEVICE (for encoders) option.

Step 2. Type the Camera Name and IP Address.

Step 3. Type the User Name and Password of the ONVIF device.

Step 4. Under camera properties pane, configure the General and Primary Stream settings.

Note: *For streaming to start, the (Resolution and FPS) in camera properties pane should be set to match the values supported by the camera/encoder.*

Step 5. Click Save.

Discovering and Adding Multi-channel Encoders

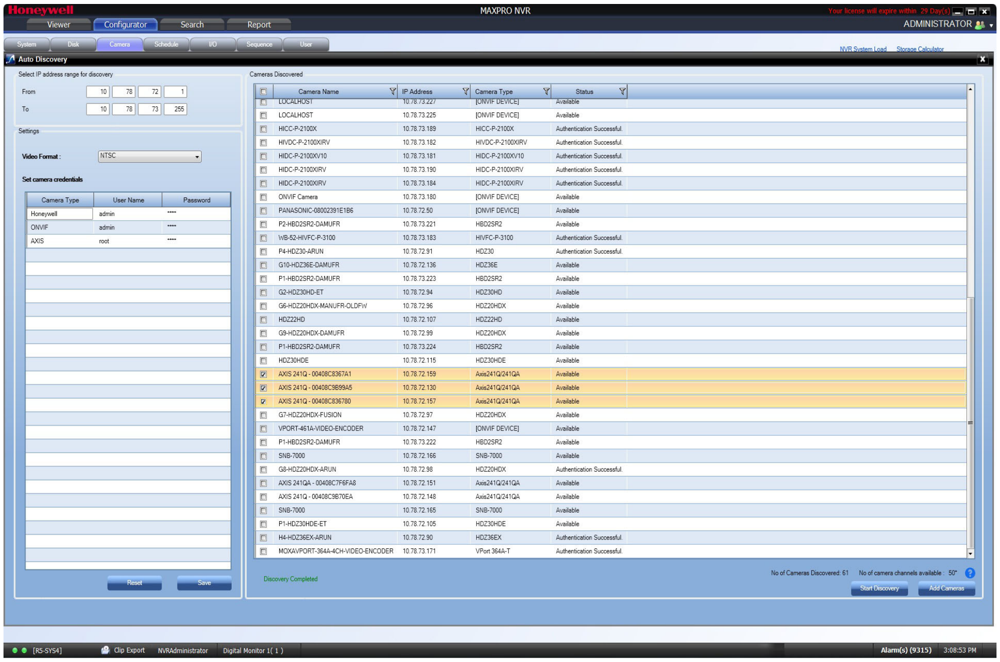
An Encoder connects to an analog camera using a coaxial cable and converts analog video streams to digital video streams, which can be sent over an IP network. Multistream or Dual stream is not supported for encoders.

Each encoder varies based on the number of channels (cameras) supported. Please visit URL: http://www.security.honeywell.com/hota/ for the most up to date list of encoders supported by MAXPRO NVR.

MAXPRO NVR automatically discovers its supported encoders and displays them in the Camera Discovered pane as shown below.

Note: *It is not recommended to add Encoder/Multi-channel video stream across NEO storage.*

.



Select IP address range for discovery

From 10 78 72 1

To 10 78 73 255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

Cameras Discovered

☐	Camera Name	IP Address	Camera Type	Status
☐	LOCALHOST	10.78.73.227	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.225	[ONVIF DEVICE]	Available
☐	HICC-P-2100X	10.78.73.189	HICC-P-2100X	Authentication Successful.
☐	HIVDC-P-2100XIRV	10.78.73.182	HIVDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XV10	10.78.73.181	HIDC-P-2100XV10	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.190	HIDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.184	HIDC-P-2100XIRV	Authentication Successful.
☐	ONVIF Camera	10.78.73.180	[ONVIF DEVICE]	Available
☐	PANASONIC-08002391E1B6	10.78.72.50	[ONVIF DEVICE]	Available
☐	P2-HBD2SR2-DAMUFR	10.78.73.221	HBD2SR2	Available
☐	WB-52-HIVFC-P-3100	10.78.73.183	HIVFC-P-3100	Authentication Successful.
☐	P4-HDZ30-ARUN	10.78.72.91	HDZ30	Authentication Successful.
☐	G10-HDZ36E-DAMUFR	10.78.72.136	HDZ36E	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.223	HBD2SR2	Available
☐	G2-HDZ30HD-ET	10.78.72.94	HDZ30HD	Available
☐	G6-HDZ20HDX-MANUFR-OLDFW	10.78.72.96	HDZ20HDX	Available
☐	HDZ22HD	10.78.72.107	HDZ22HD	Available
☐	G9-HDZ20HDX-DAMUFR	10.78.72.99	HDZ20HDX	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.224	HBD2SR2	Available
☐	HDZ30HDE	10.78.72.115	HDZ30HDE	Available
☑	AXIS 241Q - 00408C8367A1	10.78.72.159	Axis241Q/241QA	Available
☑	AXIS 241Q - 00408C9B99A5	10.78.72.130	Axis241Q/241QA	Available
☑	AXIS 241Q - 00408C836780	10.78.72.157	Axis241Q/241QA	Available
☐	G7-HDZ20HDX-FUSION	10.78.72.97	HDZ20HDX	Available
☐	VPORT-461A-VIDEO-ENCODER	10.78.72.147	[ONVIF DEVICE]	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.222	HBD2SR2	Available
☐	SNB-7000	10.78.72.166	SNB-7000	Available
☐	G8-HDZ20HDX-ARUN	10.78.72.98	HDZ20HDX	Authentication Successful.
☐	AXIS 241QA - 00408C7F6FA8	10.78.72.151	Axis241Q/241QA	Available
☐	AXIS 241Q - 00408C9B70EA	10.78.72.148	Axis241Q/241QA	Available
☐	SNB-7000	10.78.72.165	SNB-7000	Available
☐	P1-HDZ30HDE-ET	10.78.72.105	HDZ30HDE	Available
☐	H4-HDZ36EX-ARUN	10.78.72.90	HDZ36EX	Authentication Successful.
☐	MOXAVPORT-364A-4CH-VIDEO-ENCODER	10.78.73.171	VPort 364A-T	Authentication Successful.

Discovery Completed

No of Cameras Discovered: 61   No of camera channels available : 50*

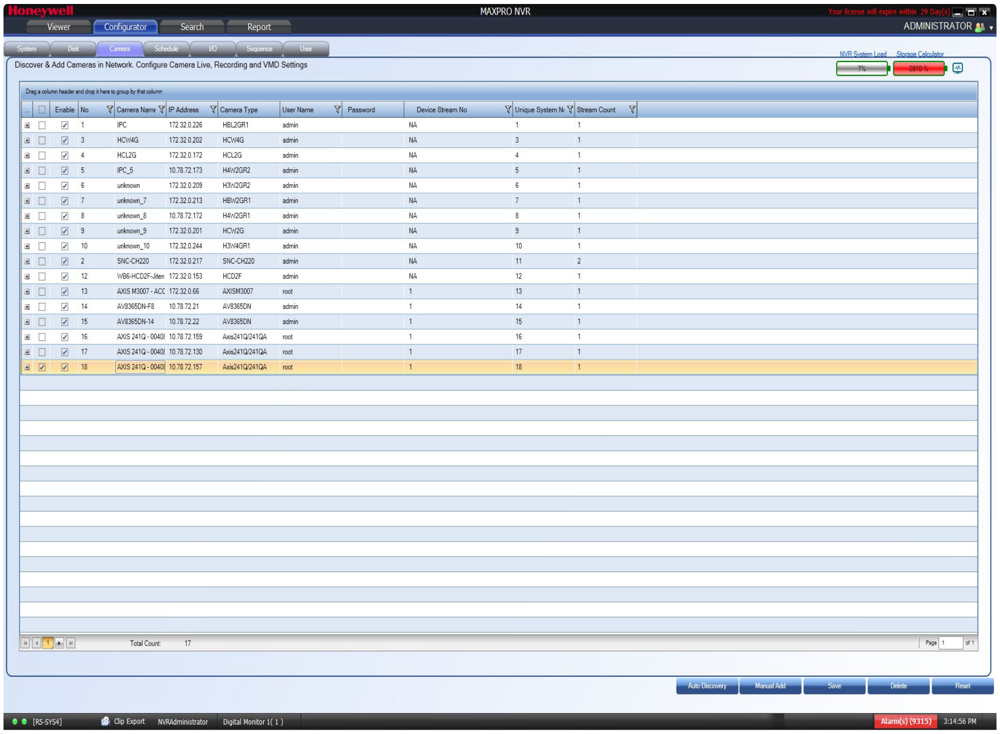
Encoder discovery

The encoder is discovered as a single device in the Cameras Discovered pane, and “n” number of cameras (where n is the number of channels supported by the encoder) are added under Camera as shown in the following figure.

Note:

- For AXIS encoders, n+1 streams are typically added (might vary by models) with 1 additional stream providing the matrix view of all cameras. This matrix view added can be deleted if it is not required by the user.
  To discover and configure the AXIS Camera/Encoders as an ONVIF device in MAXPRO NVRs, see Appendix B MAXPRO®NVRs - AXIS Camera/Encoders Discovery and Configuration (using ONVIF) section on page 425.
- For multi-channel encoders and multi-imager 180/360 cameras with single IP, only one channel license is consumed. Maximum System limit is 64 cameras including, the cameras connected through encoders and the cameras/streams connected from the multi-imager is 180/360 cameras. Multistream or Dual stream is not supported for encoders.

Note:



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	1	IPC	172.32.0.226	HBL2GR1	admin		NA	1	1
⊞	□	☑	3	HCW4G	172.32.0.202	HCW4G	admin		NA	3	1
⊞	□	☑	4	HCL2G	172.32.0.172	HCL2G	admin		NA	4	1
⊞	□	☑	5	IPC_5	10.78.72.173	H4W2GR2	admin		NA	5	1
⊞	□	☑	6	unknown	172.32.0.209	H3W2GR2	admin		NA	6	1
⊞	□	☑	7	unknown_7	172.32.0.213	HBW2GR1	admin		NA	7	1
⊞	□	☑	8	unknown_8	10.78.72.172	H4W2GR1	admin		NA	8	1
⊞	□	☑	9	unknown_9	172.32.0.201	HCW2G	admin		NA	9	1
⊞	□	☑	10	unknown_10	172.32.0.244	H3W4GR1	admin		NA	10	1
⊞	□	☑	2	SNC-CH220	172.32.0.217	SNC-CH220	admin		NA	11	2
⊞	□	☑	12	WB6-HCD2F-Jiten	172.32.0.153	HCD2F	admin		NA	12	1
⊞	□	☑	13	AXIS M3007 - ACC	172.32.0.66	AXISM3007	root		1	13	1
⊞	□	☑	14	AV8365DN-F8	10.78.72.21	AV8365DN	admin		1	14	1
⊞	□	☑	15	AV8365DN-14	10.78.72.22	AV8365DN	admin		1	15	1
⊞	□	☑	16	AXIS 241Q - 00408	10.78.72.159	Axis241Q/241QA	root		1	16	1
⊞	□	☑	17	AXIS 241Q - 00408	10.78.72.130	Axis241Q/241QA	root		1	17	1
⊞	☑	☑	18	AXIS 241Q - 00408	10.78.72.157	Axis241Q/241QA	root		1	18	1

Total Count: 17

Page 1 of 1

Adding the Encoder

Note: *The Video Channel Number field can be modified, but it is recommended that you do not change the information in this field.*

Adding FLIR Camera

The FLIR cameras are not discovered automatically in MAXRPRO NVR; hence you must add these cameras manually. The IP address of the FLIR camera should include the port number 8081 (default ONVIF port used by camera). For example: xxx.xxx.xxx:8081.

To add FLIR Camera in MAXPRO NVR

Step 1. In MAXPRO NVR, click the Configurator tab. The System page displays by default.

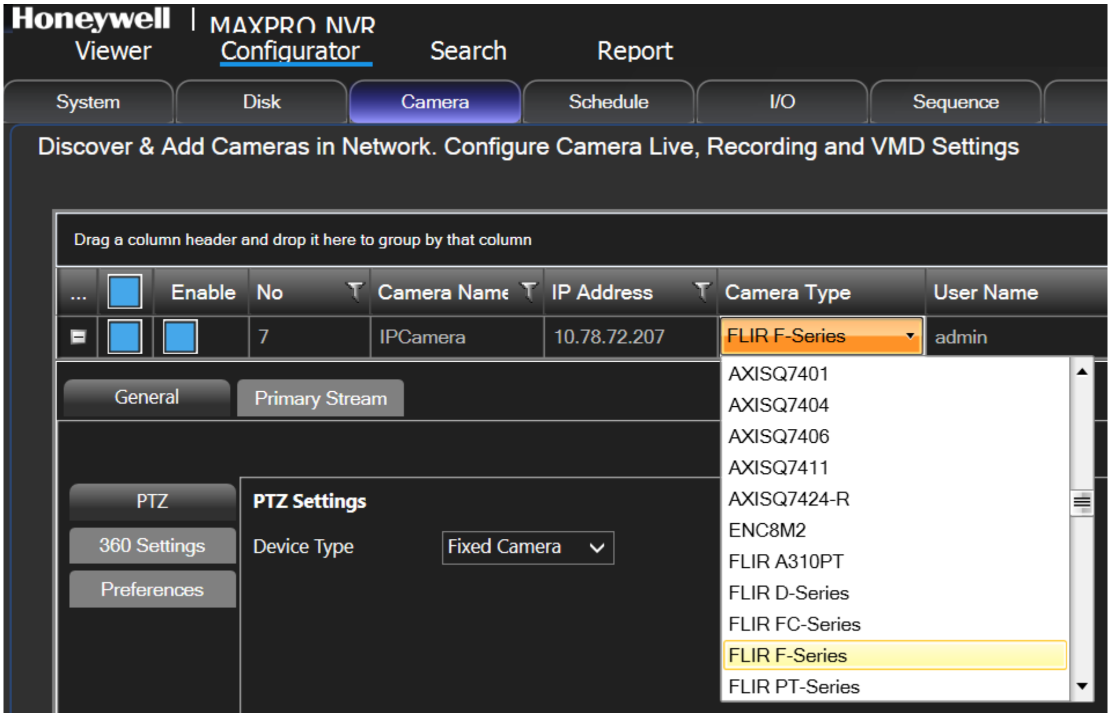
Step 2. Click the Camera tab to open the Camera page.

Step 3. Click Manual Add. A new camera is added under Camera list.

Step 4. Type the required Camera Name.

Step 5. Type the IP Address of the camera as shown in figure. The IP address should include the Port number 8081. For example if the IP address is 111.221.0.333 then you should add the port number (8081) as 111.222.0.333:8081.

Step 6. Select the required FLIR Series model camera from the Camera Type drop-down list as shown below (the Figure) for example FLIR F-Series).



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name
⊟	□	□	7	IPCamera	10.78.72.207	FLIR F-Series	admin

PTZ Settings

Device Type: Fixed Camera

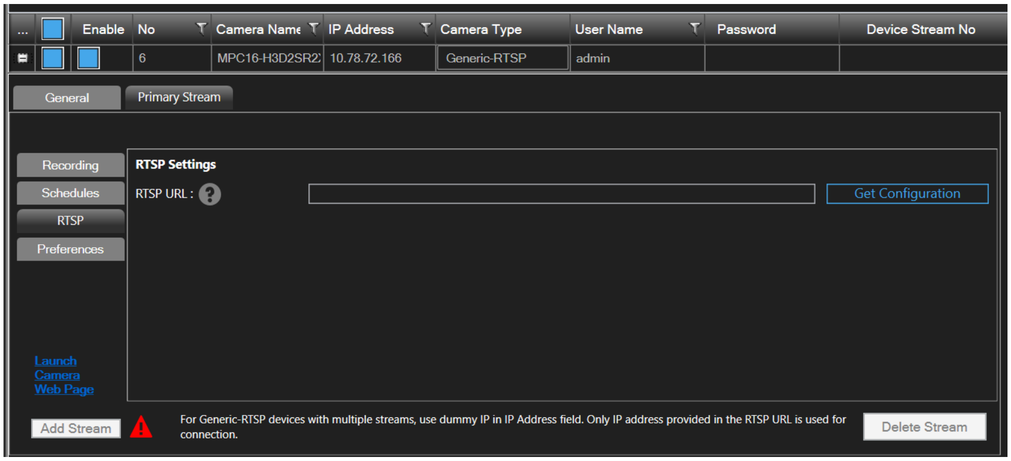
Adding FLIR Model Camera

Step 7. Scroll right to manually type the User Name and Password. The default user name is admin and password is admin.

Step 8. Click Save.

Adding RTSP Cameras/Encoders

Real Time Streaming Protocol (RTSP) is a control protocol for streaming video over the Internet. It allows you to select the TCP or UDP based streaming modes depending upon what the camera supports. For the camera type “Generic RTSP”, you must specify the following RTSP setting.



...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No
⊟	□	□	6	MPC16-H3D2SR2	10.78.72.166	Generic-RTSP	admin		

RTSP Settings

RTSP URL :

For Generic-RTSP devices with multiple streams, use dummy IP in IP Address field. Only IP address provided in the RTSP URL is used for connection.

RTSP Settings

- Type the RTSP URL. Click ? for help on RTSP URLs format that can be assigned to different camera types.

Note: *The Help that opens lists only a few manufacturers. Most cameras are RTSP, and all RTSP third party cameras can be configured. If the RTSP URL format for a particular camera type is not listed in the Help, then the URL format can be obtained from the camera manufacturer.*

- Click Get Configuration to get the resolution and compression format for the camera.
- For RTSP, all settings such as FPS must be configured on the camera web page, and the default port 554 must be used.
- If "Get Configuration" fails, a message appears to choose the compression and resolution. You must go to the Camera web page and set both of them, and then configure the same settings in MAXPRO NVR.

Step 9. Click Save.

Tip: If a particular camera is not discovered by the system, you can add it manually by clicking **Manual Add**.

Configuring the Input and Output for an IP Camera

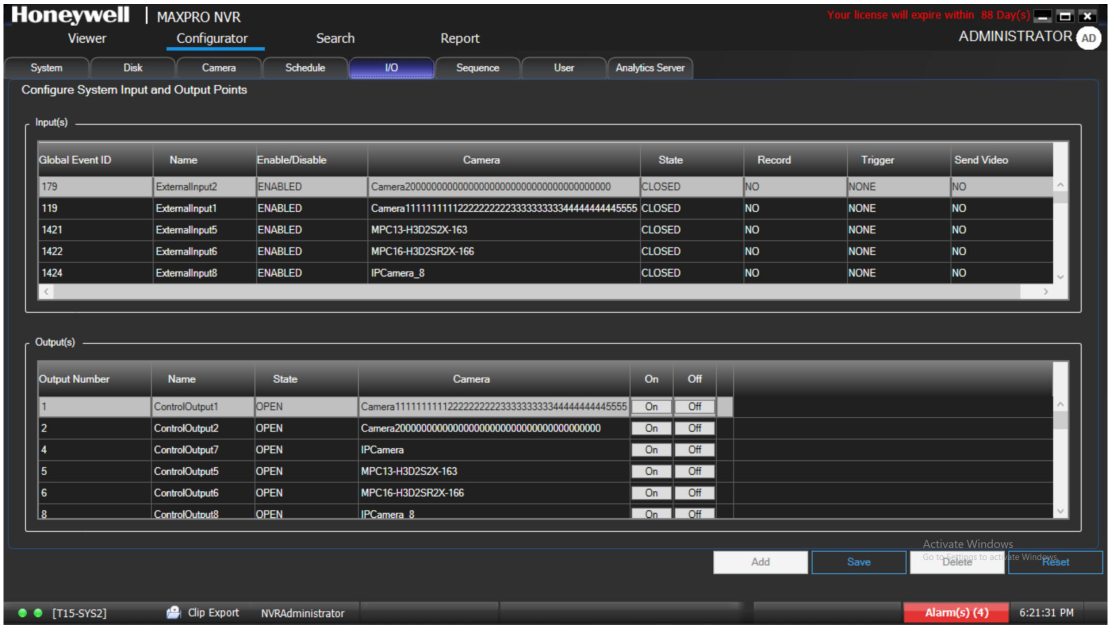
Most IP cameras have a monitor input and a control output that can be configured. For example the input of the camera could be connected to a motion detector and the output of the camera to a door opener. Once configured, movement detected at the door would trigger the door to be opened. For electrical characteristics of the input and output refer to the camera documentation.

In MAXPRO NVR, the inputs and outputs of a camera are configured by default in the database while adding a camera if the integration supports it (Refer to compatibility list on HOTA for the models with support for IO with MAXPRO NVR and the no of IOs supported by each model). MAXPRO NVR has a specialized interface that lists the inputs and outputs associated to the configured cameras.

To configure input and output

Step 1. Click the Configurator tab. The System page (the Figure) displays by default.

Step 2. Click the I/O tab.



Configure System Input and Output Points

Input(s)

Global Event ID	Name	Enable/Disable	Camera	State	Record	Trigger	Send Video
179	ExternalInput2	ENABLED	Camera200000000000000000000000000000000000000	CLOSED	NO	NONE	NO
119	ExternalInput1	ENABLED	Camera1111111111222222222233333333334444444444555	CLOSED	NO	NONE	NO
1421	ExternalInput5	ENABLED	MPC13-H3D2S2X-163	CLOSED	NO	NONE	NO
1422	ExternalInput6	ENABLED	MPC16-H3D2SR2X-166	CLOSED	NO	NONE	NO
1424	ExternalInput8	ENABLED	IPCamera_8	CLOSED	NO	NONE	NO

Output(s)

Output Number	Name	State	Camera	On	Off
1	ControlOutput1	OPEN	Camera1111111111222222222233333333334444444444555	On	Off
2	ControlOutput2	OPEN	Camera200000000000000000000000000000000000000	On	Off
4	ControlOutput7	OPEN	IPCamera	On	Off
5	ControlOutput5	OPEN	MPC13-H3D2S2X-163	On	Off
6	ControlOutput6	OPEN	MPC16-H3D2SR2X-166	On	Off
8	ControlOutput8	OPEN	IPCamera_8	On	Off

IO page

Step 3. The Input(s) pane lists the inputs for the configured cameras. Select the appropriate options in the fields as explained in the following table.

Field	Description
Global Event ID	Unique event ID
Name	External input name.
Enable/Disable	Enables or Disables the input.
Camera	Displays the associated camera name.
State (CLOSED/ OPEN)	The default option is CLOSED. Defines the normal (non-alarm or non-active) state of the input. For example a normally closed input would have its input terminal normally connected to common or ground. To activate the normally closed input, the input needs to be opened (connection to ground or common removed). For example: A magnetic door switch raises alarm if the contacts are open when the door opens.
Record (No/Yes)	The default option is No. If set to Yes recording will starts when an input is activated. **Note** Recording is based on the time you set under **System** tab > **Event recording settings**. You can specify the **Pre-event time** and **Record For** time to record the video.

Field	Description
Trigger (NONE/ ControlOutput)	The default option is NONE. If a control output is selected, then the selected output is activated when the corresponding input activates. **Note** A cameras input can only activate the same cameras output.
Send Alarm Monitor (NO/YES)	The default option is No. If set to YES, video will pop up in the viewer when an input is activated. Ensure that "Display Video on Alarm" check box is selected in the MAXPRO NVR Log on dialog box.

Step 4. The Output(s) pane lists the outputs for the configured cameras. Select the appropriate options in the fields as explained in the following table. Or you can also access the Output tab in Viewer screen.

Field	Description
Output Number	Control output number.
Name	Control output name.
State (CLOSED/ OPEN)	The default option is OPEN. Defines the normal (non-alarm or non-active) state of the output relay contacts.
Camera	Displays the associated camera name.
ON/OFF	Manual control of the output. Click ON to close the relay contacts. Click OFF to open the relay contacts.

Step 5. In the Output(s) pane, select an output and then click On to turn on the relay manually or Click Off to turn off the relay manually.

Step 6. Click Save or click Reset to undo the changes.

To trigger the output from viewer screen:

Step 1. Click the Viewer tab.

Step 2. On the left pane, click Outputs tab, the list of camera outputs are displayed in Sites.

Step 3. Right-click the required camera output and then set ON or OFF.

Configuring 360/180 Cameras

Configuring the Panomorph Settings for the Cameras with Immervision Support

ImmerVision's Panomorph lens enables 360 degree Field of View (FOV). This lens is compatible with industry standard analog and IP cameras.

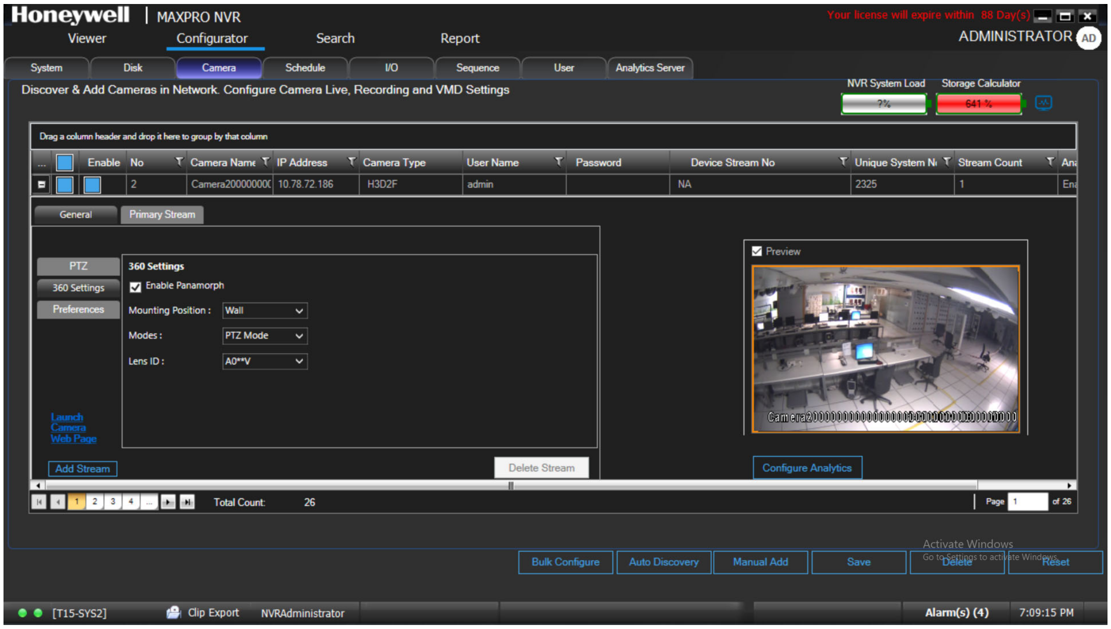
By using the Panomorph lens with your IP/ Analog camera, you can:

- View live, record and playback the complete 360x180 FOV.
- Eliminate blind spots in the FOV.
- Increase the video surveillance coverage.
- Detect, track and analyze throughout the entire area.
- Playback the recorded video with digital watermark for evidence purposes.

Caution: Only Immervision certified camera models can support this feature enabled. Before configuring this feature, please check whether your camera has the Panomorph lens.

To configure Panomorph settings

Step 1. On the Camera page, for the required camera, click ⊞ on the left corner to open the camera properties pane see the Figure .



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...		Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count	Ana
⊟	■	■	2	Camera20000000(	10.78.72.186	H3D2F	admin		NA	2325	1	Ena

360 Settings

☑ Enable Panamorph

Mounting Position : Wall

Modes : PTZ Mode

Lens ID : A0**V

Total Count: 26

Panomorph Settings

Step 2. Under General > 360 Settings

- Select the Enable Panomorph check box to enable the Panomorph feature.
- Select the Mounting Position. You have three options to choose from: Wall, Ceiling, and Ground.

- Select the Mode for the camera. The available modes are PTZ Mode, Quad Mode, and Perimeter Mode. The default mode is PTZ Mode.
- Select the Lens ID for the camera. The supported lens ids in v3.5 or later are A0**V, A0IFV, A0NKV, A1UST, A8TRT, B0QQV, B4QQV, B5SST, B6SST and B8QQT. By default A0**V Lens ID is selected. For Sony 360 camera the A8TRT lens ID is selected automatically.

Step 3. Click Save.

Note:

- To view live video from Immervision certified cameras, Refer Video Viewing Options from Immervision Enabled Cameras section in *MAXPRO® NVR Operator's Guide.*
- The recommended Aspect Ratio for Immervision Certified cameras is 4:3.

Configuring Oncam Grandeye Cameras

The integration of the unique 360-degree Oncam Grandeye H.264 IP cameras in MAXPRO NVR enables video surveillance, acquisition and tracking that identifies suspicious behavior enabling the interrogation and verification of a potential threat. This in-turn provides the necessary intelligence needed to make a measured response to any critical situation. Grandeye's customized security solutions are designed to address to meet all of today's security and liability requirements.

MAXPRO NVR supports only Oncam Grandeye H.264 Evolution camera.

The Evolution series cameras support the following views, that help in effective video surveillance of a site:

- Evolution - FishEye(OnCam-GE-Evo-Fisheye)
- Virtual Camera View
- Panorama 2x 180 views
- Panorama 1x 360 view
- Panorama 1x 180 view

Adding Oncam Grandeye Cameras

The Oncam Grandeye cameras are not discovered automatically in MAXRPRO NVR, hence you must add these cameras manually.

Note: *For Evolution cameras, please first set the active camera stream (resolution) on the camera web page. Select the same settings as camera active stream in the NVR-camera properties pane for video to be displayed.*

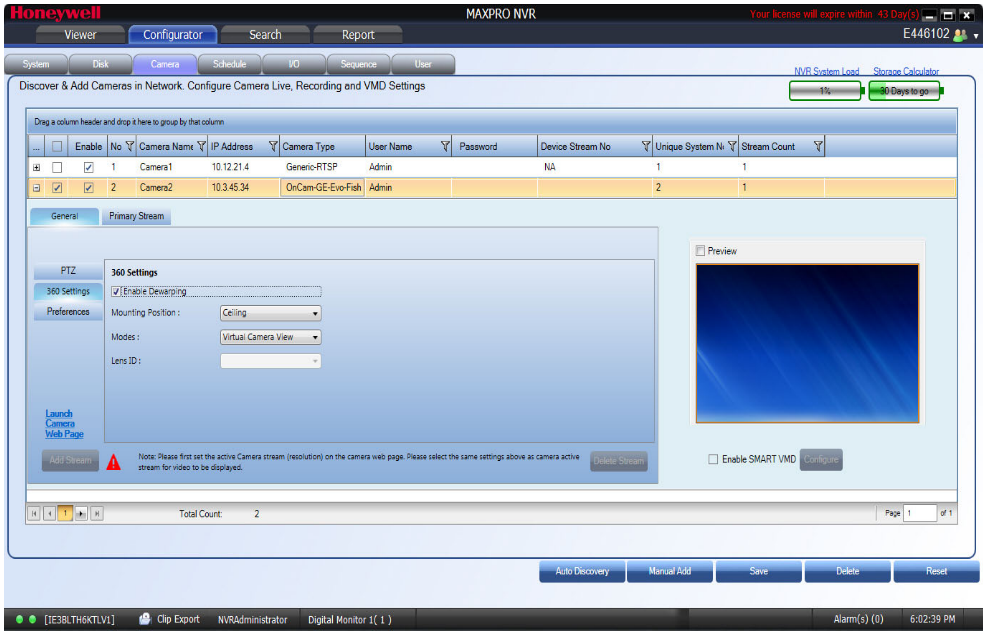
To add Oncam Grandeye cameras

Step 1. On the Camera page, click Manual Add.

Step 2. Enter the following information:

- Camera Name
- IP address
- Camera Type
- User Name - Type the default user name, “admin”.
- Password - Type the default password, “admin”.
- Device Stream Number (Defaulted)
- Unique System Number
- Stream Count (Defaulted)

Step 3. Click ⊞ to open the camera properties pane see the Figure .:



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	1	Camera1	10.12.21.4	Generic-RTSP	Admin		NA	1	1
⊟	☑	☑	2	Camera2	10.3.45.34	OnCam-GE-Evo-Fish	Admin			2	1

360 Settings

☑ Enable Dewarping

Mounting Position : Ceiling

Modes : Virtual Camera View

Lens ID :

Note: Please first set the active Camera stream (resolution) on the camera web page. Please select the same settings above as camera active stream for video to be displayed.

□ Enable SMART VMD

Total Count: 2

Page 1 of 1

Grandeye Dewarping Settings

Step 4. Under General > 360 Settings

- Select the Enable Dewarping check box to enable the dewarping settings.

Note: *For the streamers other than GrandEye, the Enable Panorama options are not visible.*

- Select the Mounting Position. The available options are Wall, Ceiling and Ground.
- Select the Modes. The available options are Virtual Camera View, Panorama 2x 180 views, Panorama 1x 360 view, and Panorama 1x 180 view. The Mounting Position and Modes are only applicable to Evolution cameras.

Step 5. Click Save.

Image Stream Combinations for Oncam Grandeye Cameras

Evolution camera works best when configured with a particular resolution and fps. See the Image Stream Combinations for Oncam Grandeye Cameras section on page 409 in Appendix B for the optimum resolution and fps configurations for each of the cameras.

Viewing Live Video from Oncam Grandeye Cameras

Refer Video Viewing Options from Oncam Grandeye Cameras section in *MAXPRO® NVR Operator's Guide.*

Device Characteristics of Oncam Grandeye Cameras

See Appendix B, Device Characteristics of Oncam Grandeye Cameras section on page 409.

Adding Axis 360/180 Camera

To add Axis 360/180 camera

Note: *v3.1 SP1 or later supports discovering and adding Axis 360/180 models. Earlier these were supported through RTSP only in v3.1 or lower versions.*

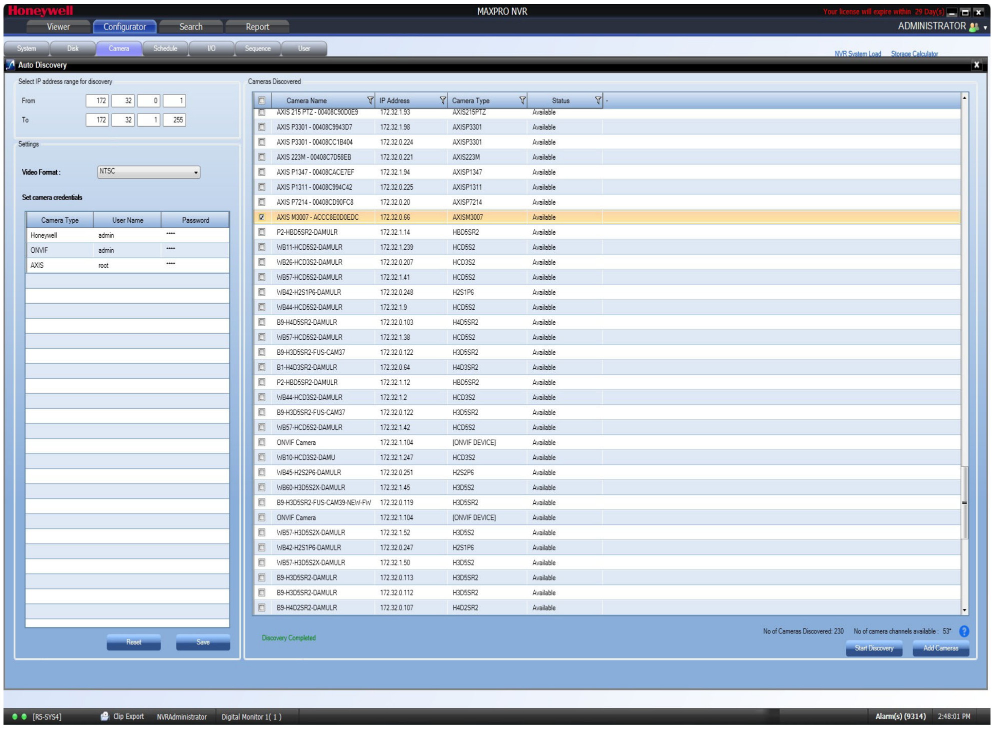
Step 1. In MAXPRO NVR, click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to open the Camera page.

Step 3. Click Auto Discovery button. The Auto Discovery screen is displayed and the discovery starts by default.

- If discovery is stopped then click Start Discovery to discover the cameras in the network. The cameras are added based on the IP range and Video Format settings. See the Configuring the Auto Discovery Settings section on page 180 for more information. Only device integrations with auto discovery support are discovered automatically in the NVR. All other devices need to be added manually. For Axis M3007-PV and M3027-PVE model cameras, ONVIF should be enabled on the camera prior to discovery. see Appendix B, MAXPRO®NVRs - AXIS Camera/Encoders Discovery and Configuration (using ONVIF) section on page 425.

Step 4. After the discovery, to add the Axis 360/180 camera models, select the check boxes of Axis 360/180 camera model as shown in the Figure . Axis 360/180 cameras are listed in the discovery pane with their model numbers for example Axis M3007 and so on.



Honeywell

MAXPRO NVR

Your license will expire within 29 Day(s)

Auto Discovery

Select IP address range for discovery

From	172	32	0	1
To	172	32	1	255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

Cameras Discovered

□	Camera Name	IP Address	Camera Type	Status
□	AXIS 215 PTZ - 00408C90D0E9	172.32.1.93	AXIS215PTZ	Available
□	AXIS P3301 - 00408C9943D7	172.32.1.98	AXISP3301	Available
□	AXIS P3301 - 00408CC1B404	172.32.0.224	AXISP3301	Available
□	AXIS 223M - 00408C7D58EB	172.32.0.221	AXIS223M	Available
□	AXIS P1347 - 00408CACE7EF	172.32.1.94	AXISP1347	Available
□	AXIS P1311 - 00408C994C42	172.32.0.225	AXISP1311	Available
□	AXIS P7214 - 00408CD90FC8	172.32.0.20	AXISP7214	Available
☑	AXIS M3007 - ACCC8E0D0EDC	172.32.0.66	AXISM3007	Available
□	P2-HBD5SR2-DAMULR	172.32.1.14	HBD5SR2	Available
□	WB11-HCD5S2-DAMULR	172.32.1.239	HCD5S2	Available
□	WB26-HCD3S2-DAMULR	172.32.0.207	HCD3S2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.41	HCD5S2	Available
□	WB42-H2S1P6-DAMULR	172.32.0.248	H2S1P6	Available
□	WB44-HCD5S2-DAMULR	172.32.1.9	HCD5S2	Available
□	B9-H4D5SR2-DAMULR	172.32.0.103	H4D5SR2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.38	HCD5S2	Available
□	B9-H3D5SR2-FUS-CAM37	172.32.0.122	H3D5SR2	Available
□	B1-H4D3SR2-DAMULR	172.32.0.64	H4D3SR2	Available
□	P2-HBD5SR2-DAMULR	172.32.1.12	HBD5SR2	Available
□	WB44-HCD3S2-DAMULR	172.32.1.2	HCD3S2	Available
□	B9-H3D5SR2-FUS-CAM37	172.32.0.122	H3D5SR2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.42	HCD5S2	Available
□	ONVIF Camera	172.32.1.104	[ONVIF DEVICE]	Available
□	WB10-HCD3S2-DAMU	172.32.1.247	HCD3S2	Available
□	WB45-H2S2P6-DAMULR	172.32.0.251	H2S2P6	Available
□	WB60-H3D5S2X-DAMULR	172.32.1.45	H3D5S2	Available
□	B9-H3D5SR2-FUS-CAM39-NEW-FW	172.32.0.119	H3D5SR2	Available
□	ONVIF Camera	172.32.1.104	[ONVIF DEVICE]	Available
□	WB57-H3D5S2X-DAMULR	172.32.1.52	H3D5S2	Available
□	WB42-H2S1P6-DAMULR	172.32.0.247	H2S1P6	Available
□	WB57-H3D5S2X-DAMULR	172.32.1.50	H3D5S2	Available
□	B9-H3D5SR2-DAMULR	172.32.0.113	H3D5SR2	Available
□	B9-H3D5SR2-DAMULR	172.32.0.112	H3D5SR2	Available
□	B9-H4D2SR2-DAMULR	172.32.0.107	H4D2SR2	Available

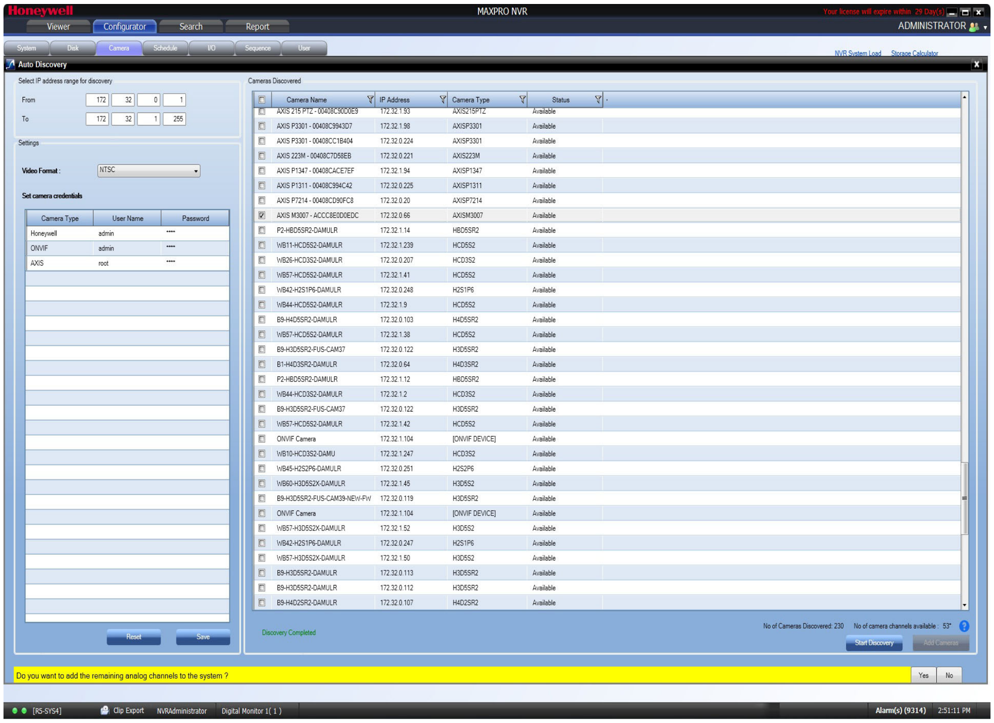
Discovery Completed

No of Cameras Discovered: 230 No of camera channels available : 53*

● ● [R5-SYS4] Clip Export NVRAdministrator Digital Monitor 1(1) Alarm(s) (9314) 2:48:01 PM

Discovering AXIS 360 Camera

Step 5. Click Add Cameras. A message Do you want to add the remaining analog channels to the system? is displayed at the bottom of the screen as shown in the Figure .



Honeywell

MAXPRO NVR

Your license will expire within 29 Day(s)

Auto Discovery

Select IP address range for discovery

From	172	32	0	1
To	172	32	1	255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

Cameras Discovered

□	Camera Name	IP Address	Camera Type	Status
□	AXIS 215 PTZ - 00408C90D0E9	172.32.1.93	AXIS215PTZ	Available
□	AXIS P3301 - 00408C9943D7	172.32.1.98	AXISP3301	Available
□	AXIS P3301 - 00408CC1B404	172.32.0.224	AXISP3301	Available
□	AXIS 223M - 00408C7D58EB	172.32.0.221	AXIS223M	Available
□	AXIS P1347 - 00408CACE7EF	172.32.1.94	AXISP1347	Available
□	AXIS P1311 - 00408C994C42	172.32.0.225	AXISP1311	Available
□	AXIS P7214 - 00408CD90FC8	172.32.0.20	AXISP7214	Available
☑	AXIS M3007 - ACCC8E0D0EDC	172.32.0.66	AXISM3007	Available
□	P2-HBD5SR2-DAMULR	172.32.1.14	HBD5SR2	Available
□	WB11-HCD5S2-DAMULR	172.32.1.239	HCD5S2	Available
□	WB26-HCD3S2-DAMULR	172.32.0.207	HCD3S2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.41	HCD5S2	Available
□	WB42-H2S1P6-DAMULR	172.32.0.248	H2S1P6	Available
□	WB44-HCD5S2-DAMULR	172.32.1.9	HCD5S2	Available
□	B9-H4D5SR2-DAMULR	172.32.0.103	H4D5SR2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.38	HCD5S2	Available
□	B9-H3D5SR2-FUS-CAM37	172.32.0.122	H3D5SR2	Available
□	B1-H4D3SR2-DAMULR	172.32.0.64	H4D3SR2	Available
□	P2-HBD5SR2-DAMULR	172.32.1.12	HBD5SR2	Available
□	WB44-HCD3S2-DAMULR	172.32.1.2	HCD3S2	Available
□	B9-H3D5SR2-FUS-CAM37	172.32.0.122	H3D5SR2	Available
□	WB57-HCD5S2-DAMULR	172.32.1.42	HCD5S2	Available
□	ONVIF Camera	172.32.1.104	[ONVIF DEVICE]	Available
□	WB10-HCD3S2-DAMU	172.32.1.247	HCD3S2	Available
□	WB45-H2S2P6-DAMULR	172.32.0.251	H2S2P6	Available
□	WB60-H3D5S2X-DAMULR	172.32.1.45	H3D5S2	Available
□	B9-H3D5SR2-FUS-CAM39-NEW-FW	172.32.0.119	H3D5SR2	Available
□	ONVIF Camera	172.32.1.104	[ONVIF DEVICE]	Available
□	WB57-H3D5S2X-DAMULR	172.32.1.52	H3D5S2	Available
□	WB42-H2S1P6-DAMULR	172.32.0.247	H2S1P6	Available
□	WB57-H3D5S2X-DAMULR	172.32.1.50	H3D5S2	Available
□	B9-H3D5SR2-DAMULR	172.32.0.113	H3D5SR2	Available
□	B9-H3D5SR2-DAMULR	172.32.0.112	H3D5SR2	Available
□	B9-H4D2SR2-DAMULR	172.32.0.107	H4D2SR2	Available

Discovery Completed

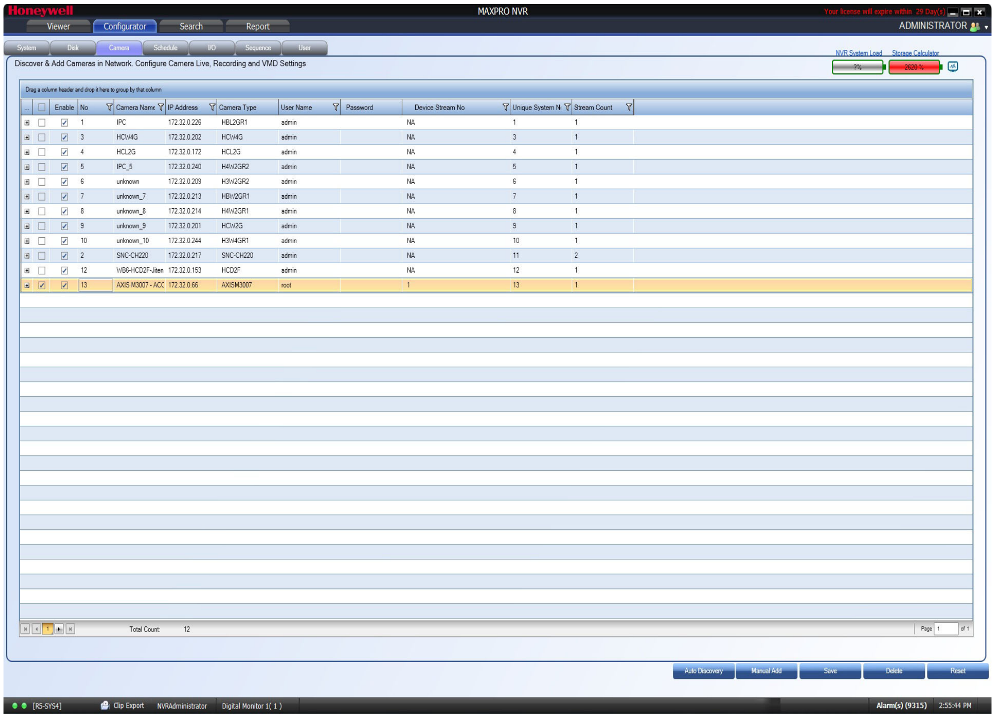
No of Cameras Discovered: 230 No of camera channels available : 53*

Do you want to add the remaining analog channels to the system ?

● ● [R5-SYS4] Clip Export NVRAdministrator Digital Monitor 1(1) Alarm(s) (9314) 2:51:11 PM

Adding Remaining Axis Channels

Step 6. Click Yes to add the remaining channels. The list of channels associated with the camera is added in the Camera list as shown in the Figure .



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System No	Stream Count
⊞	□	☑	1	IPC	172.32.0.226	HBL2GR1	admin		NA	1	1
⊞	□	☑	3	HCW4G	172.32.0.202	HCW4G	admin		NA	3	1
⊞	□	☑	4	HCL2G	172.32.0.172	HCL2G	admin		NA	4	1
⊞	□	☑	5	IPC_5	172.32.0.240	H4W2GR2	admin		NA	5	1
⊞	□	☑	6	unknown	172.32.0.209	H3W2GR2	admin		NA	6	1
⊞	□	☑	7	unknown_7	172.32.0.213	HBW2GR1	admin		NA	7	1
⊞	□	☑	8	unknown_8	172.32.0.214	H4W2GR1	admin		NA	8	1
⊞	□	☑	9	unknown_9	172.32.0.201	HCW2G	admin		NA	9	1
⊞	□	☑	10	unknown_10	172.32.0.244	H3W4GR1	admin		NA	10	1
⊞	□	☑	2	SNC-CH220	172.32.0.217	SNC-CH220	admin		NA	11	2
⊞	□	☑	12	WB6-HCD2F-Jiten	172.32.0.153	HCD2F	admin		NA	12	1
⊞	☑	☑	13	AXIS M3007 - ACC	172.32.0.66	AXISM3007	root		1	13	1

Total Count: 12

AXIS Channels

Note: *Depending on the mounting position, the Axis 360/180 camera (this does not apply to AXIS multi-imager cameras) supports eight or less video streams with one stream per channel added. Each channel added consumes 1 channel license. For Encoders if you add 4 channels then it will consumes 1 channel license.*

By default, the Axis 360/180 camera adds eight channels under camera list covering below views. Views which are not required for your specific application can be deleted. To reclaim the used channel license, select the specific channel in the list and then click Delete.

1. Overview: A non-dewarped 360° view

2. Panorama: One dewarped 180° panoramic view

3. Double Panorama: Two dewarped 180° panoramic views (Not available when the camera is mounted on a wall)

4. Quad View: Four dewarped 90° views, one for each direction (Not available when the camera is mounted on a wall)

5. View Area 1: A dewarped 90° view with PTZ (pan/tilt/zoom) functionality

6. View Area 2: A dewarped 90° view with PTZ (pan/tilt/zoom) functionality

7. View Area 3: A dewarped 90° view with PTZ (pan/tilt/zoom) functionality

8. View Area 4: A dewarped 90° view with PTZ (pan/tilt/zoom) functionality

Adding Arecont 360/180 Camera

To add Arecont 360/180 Camera in MAXPRO NVR

Note:

- v3.1 SP1 or later supports discovering and adding certain Arecont 360/180 model cameras. These were supported through RTSP only in v3.1 or lower versions.
- For multi-channel encoders and multi-imager 180/360 cameras with single IP, only one channel license is consumed. Maximum System limit is 64 cameras including, the cameras connected through encoders and the cameras/streams connected from the multi-imager is 180/360 cameras.

Note:

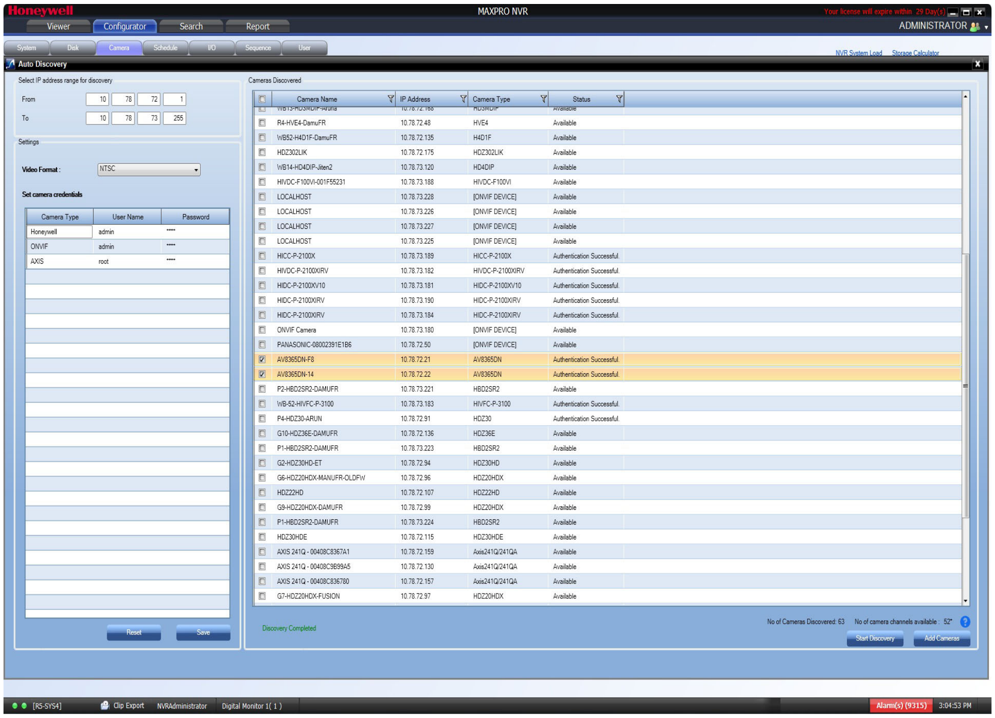
Step 1. In MAXPRO NVR, click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to open the Camera page.

Step 3. Click Auto Discovery button. The Auto Discovery screen is displayed and the discovery starts by default. If discovery is stopped then click Start Discovery to discover the cameras in the network. The cameras are added based on the IP range and Video Format settings. See the Configuring the Auto Discovery Settings section on page 180 for more information.

Step 4. After the discovery, to add the Arecont 360/180 camera models, select the check boxes corresponding to Arecont 360/180 camera models as shown in the figure Adding Arecont 360 Model Camera.

Note: *Arecont 360/180 cameras are listed in the discovery pane with their model numbers for example AV8365DN-F8.*



Select IP address range for discovery

From 10 78 72 1

To 10 78 73 255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

Cameras Discovered

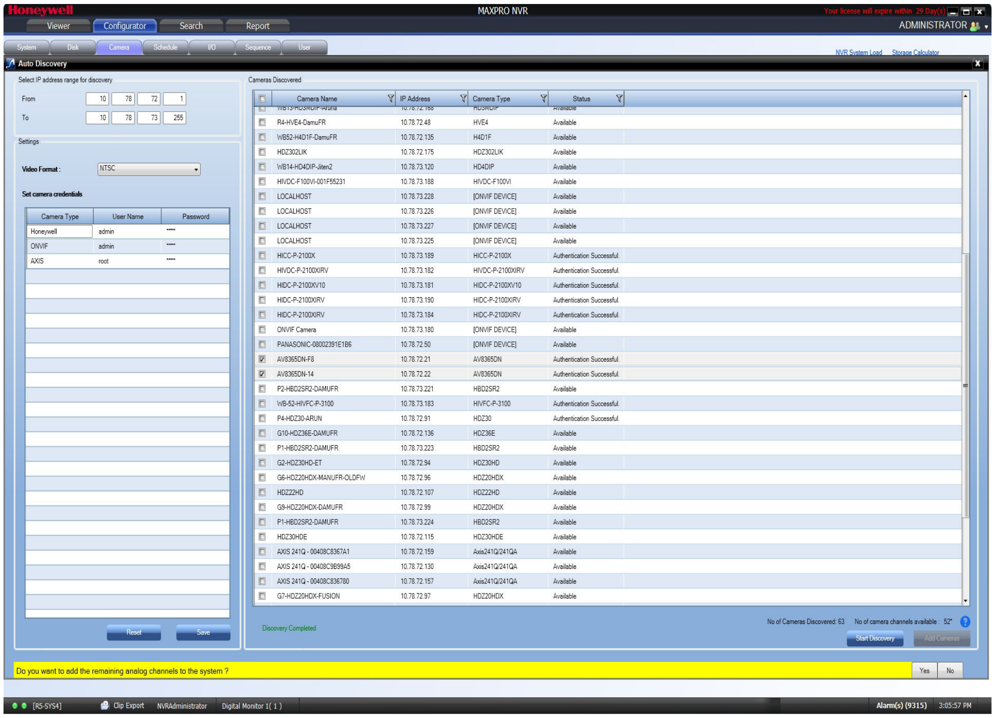
☐	Camera Name	IP Address	Camera Type	Status
☐	WB13-HD3MDIP-Aruna	10.78.72.168	HD3MDIP	Available
☐	R4-HVE4-DamuFR	10.78.72.48	HVE4	Available
☐	WB52-H4D1F-DamuFR	10.78.72.135	H4D1F	Available
☐	HDZ302LIK	10.78.72.175	HDZ302LIK	Available
☐	WB14-HD4DIP-Jiten2	10.78.73.120	HD4DIP	Available
☐	HIVDC-F100VI-001F55231	10.78.73.188	HIVDC-F100VI	Available
☐	LOCALHOST	10.78.73.228	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.226	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.227	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.225	[ONVIF DEVICE]	Available
☐	HICC-P-2100X	10.78.73.189	HICC-P-2100X	Authentication Successful.
☐	HIVDC-P-2100XIRV	10.78.73.182	HIVDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XV10	10.78.73.181	HIDC-P-2100XV10	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.190	HIDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.184	HIDC-P-2100XIRV	Authentication Successful.
☐	ONVIF Camera	10.78.73.180	[ONVIF DEVICE]	Available
☐	PANASONIC-08002391E1B6	10.78.72.50	[ONVIF DEVICE]	Available
☑	AV8365DN-F8	10.78.72.21	AV8365DN	Authentication Successful.
☑	AV8365DN-14	10.78.72.22	AV8365DN	Authentication Successful.
☐	P2-HBD2SR2-DAMUFR	10.78.73.221	HBD2SR2	Available
☐	WB-52-HIVFC-P-3100	10.78.73.183	HIVFC-P-3100	Authentication Successful.
☐	P4-HDZ30-ARUN	10.78.72.91	HDZ30	Authentication Successful.
☐	G10-HDZ36E-DAMUFR	10.78.72.136	HDZ36E	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.223	HBD2SR2	Available
☐	G2-HDZ30HD-ET	10.78.72.94	HDZ30HD	Available
☐	G6-HDZ20HDX-MANUFR-OLDFW	10.78.72.96	HDZ20HDX	Available
☐	HDZ22HD	10.78.72.107	HDZ22HD	Available
☐	G9-HDZ20HDX-DAMUFR	10.78.72.99	HDZ20HDX	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.224	HBD2SR2	Available
☐	HDZ30HDE	10.78.72.115	HDZ30HDE	Available
☐	AXIS 241Q - 00408C8367A1	10.78.72.159	Axis241Q/241QA	Available
☐	AXIS 241Q - 00408C9B99A5	10.78.72.130	Axis241Q/241QA	Available
☐	AXIS 241Q - 00408C836780	10.78.72.157	Axis241Q/241QA	Available
☐	G7-HDZ20HDX-FUSION	10.78.72.97	HDZ20HDX	Available

Discovery Completed

No of Cameras Discovered: 63 No of camera channels available : 52*

Adding Arecont 360 Model Camera

Step 5. Click Add Camera. A message Do you want to add the remaining analog channels to the system? is displayed at the bottom of the screen as shown below.



Select IP address range for discovery

From	10	78	72	1
To	10	78	73	255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

Reset Save

Cameras Discovered

☐	Camera Name	IP Address	Camera Type	Status
☐	WB13-HD3MDIP-Aruna	10.78.72.168	HD3MDIP	Available
☐	R4-HVE4-DamuFR	10.78.72.48	HVE4	Available
☐	WB52-H4D1F-DamuFR	10.78.72.135	H4D1F	Available
☐	HDZ302LIK	10.78.72.175	HDZ302LIK	Available
☐	WB14-HD4DIP-Jiten2	10.78.73.120	HD4DIP	Available
☐	HIVDC-F100VI-001F55231	10.78.73.188	HIVDC-F100VI	Available
☐	LOCALHOST	10.78.73.228	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.226	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.227	[ONVIF DEVICE]	Available
☐	LOCALHOST	10.78.73.225	[ONVIF DEVICE]	Available
☐	HICC-P-2100X	10.78.73.189	HICC-P-2100X	Authentication Successful.
☐	HIVDC-P-2100XIRV	10.78.73.182	HIVDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XV10	10.78.73.181	HIDC-P-2100XV10	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.190	HIDC-P-2100XIRV	Authentication Successful.
☐	HIDC-P-2100XIRV	10.78.73.184	HIDC-P-2100XIRV	Authentication Successful.
☐	ONVIF Camera	10.78.73.180	[ONVIF DEVICE]	Available
☐	PANASONIC-08002391E1B6	10.78.72.50	[ONVIF DEVICE]	Available
☑	AV8365DN-F8	10.78.72.21	AV8365DN	Authentication Successful.
☑	AV8365DN-14	10.78.72.22	AV8365DN	Authentication Successful.
☐	P2-HBD2SR2-DAMUFR	10.78.73.221	HBD2SR2	Available
☐	WB-52-HIVFC-P-3100	10.78.73.183	HIVFC-P-3100	Authentication Successful.
☐	P4-HDZ30-ARUN	10.78.72.91	HDZ30	Authentication Successful.
☐	G10-HDZ36E-DAMUFR	10.78.72.136	HDZ36E	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.223	HBD2SR2	Available
☐	G2-HDZ30HD-ET	10.78.72.94	HDZ30HD	Available
☐	G6-HDZ20HDX-MANUFR-OLDFW	10.78.72.96	HDZ20HDX	Available
☐	HDZ22HD	10.78.72.107	HDZ22HD	Available
☐	G9-HDZ20HDX-DAMUFR	10.78.72.99	HDZ20HDX	Available
☐	P1-HBD2SR2-DAMUFR	10.78.73.224	HBD2SR2	Available
☐	HDZ30HDE	10.78.72.115	HDZ30HDE	Available
☐	AXIS 241Q - 00408C8367A1	10.78.72.159	Axis241Q/241QA	Available
☐	AXIS 241Q - 00408C9B99A5	10.78.72.130	Axis241Q/241QA	Available
☐	AXIS 241Q - 00408C836780	10.78.72.157	Axis241Q/241QA	Available
☐	G7-HDZ20HDX-FUSION	10.78.72.97	HDZ20HDX	Available

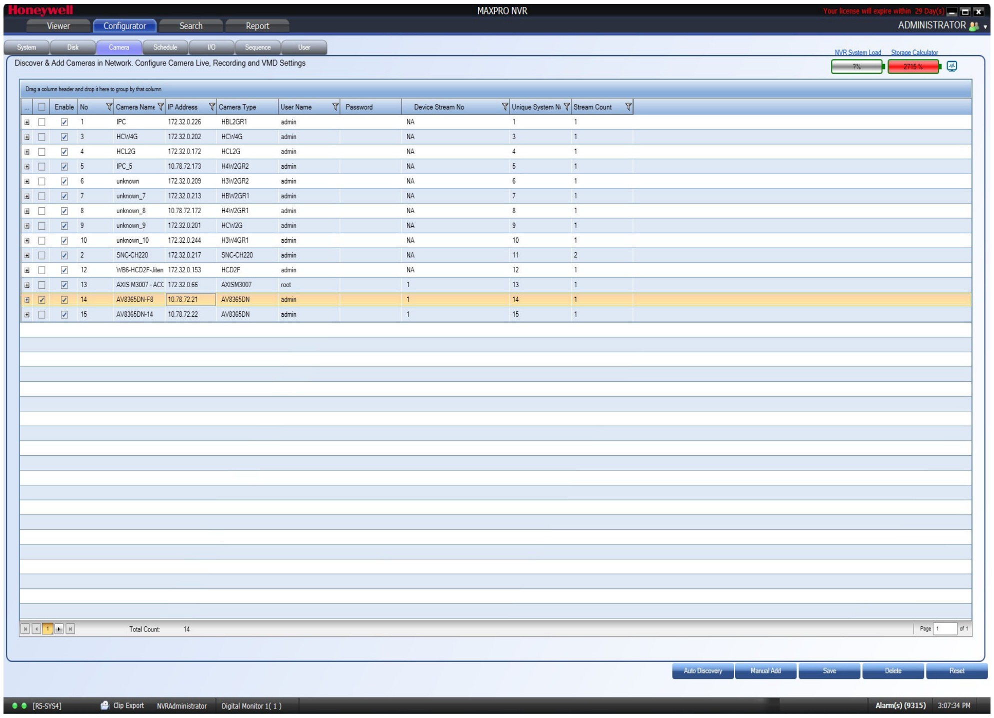
Discovery Completed

No of Cameras Discovered: 63 No of camera channels available : 52*

Do you want to add the remaining analog channels to the system ?

Adding Remaining Arecont channels

Step 6. Click Yes to add the remaining analog channels. The list of channels associated with the Arecont 360 camera is added in the Camera list as shown below. By default the Arecont 360 camera adds four channels under camera list.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	☐	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	☐	☑	1	IPC	172.32.0.226	HBL2GR1	admin		NA	1	1
⊞	☐	☑	3	HCW4G	172.32.0.202	HCW4G	admin		NA	3	1
⊞	☐	☑	4	HCL2G	172.32.0.172	HCL2G	admin		NA	4	1
⊞	☐	☑	5	IPC_5	10.78.72.173	H4W2GR2	admin		NA	5	1
⊞	☐	☑	6	unknown	172.32.0.209	H3W2GR2	admin		NA	6	1
⊞	☐	☑	7	unknown_7	172.32.0.213	HBW2GR1	admin		NA	7	1
⊞	☐	☑	8	unknown_8	10.78.72.172	H4W2GR1	admin		NA	8	1
⊞	☐	☑	9	unknown_9	172.32.0.201	HCW2G	admin		NA	9	1
⊞	☐	☑	10	unknown_10	172.32.0.244	H3W4GR1	admin		NA	10	1
⊞	☐	☑	2	SNC-CH220	172.32.0.217	SNC-CH220	admin		NA	11	2
⊞	☐	☑	12	WB6-HCD2F-Jiten	172.32.0.153	HCD2F	admin		NA	12	1
⊞	☐	☑	13	AXIS M3007 - ACC	172.32.0.66	AXISM3007	root		1	13	1
⊞	☑	☑	14	AV8365DN-F8	10.78.72.21	AV8365DN	admin		1	14	1
⊞	☐	☑	15	AV8365DN-14	10.78.72.22	AV8365DN	admin		1	15	1

Total Count: 14

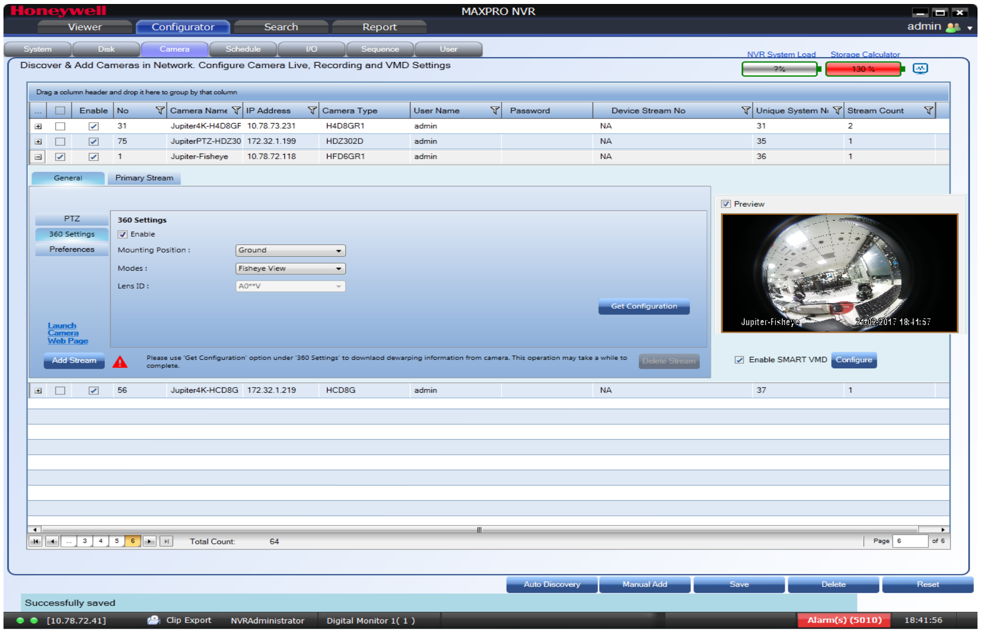
Page 1 of 1

Configuring the New EquIP Model Camera for Dewarping

To dewarp the New EquIP model camera

Step 1. Add the New EquIP Fisheye Model (HFD6GR1) camera.

Step 2. On the Camera page, for the New EquIP Fisheye Model (HFD6GR1) camera, click ⊞ on the left corner to open the camera properties pane.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	31	Jupiter4K-H4D8GF	10.78.73.231	H4D8GR1	admin		NA	31	2
⊞	□	☑	75	JupiterPTZ-HDZ30	172.32.1.199	HDZ302D	admin		NA	35	1
⊟	☑	☑	1	Jupiter-Fisheye	10.78.72.118	HFD6GR1	admin		NA	36	1
⊞	□	☑	56	Jupiter4K-HCD8G	172.32.1.219	HCD8G	admin		NA	37	1

360 Settings

☑ Enable

Mounting Position : Ground

Modes : Fisheye View

Lens ID : A0**V

Please use 'Get Configuration' option under '360 Settings' to downlaod dewarping information from camera. This operation may take a while to complete.

☑ Preview

☑ Enable SMART VMD

Total Count: 64

Successfully saved

EquIP- Fisheye camera Settings

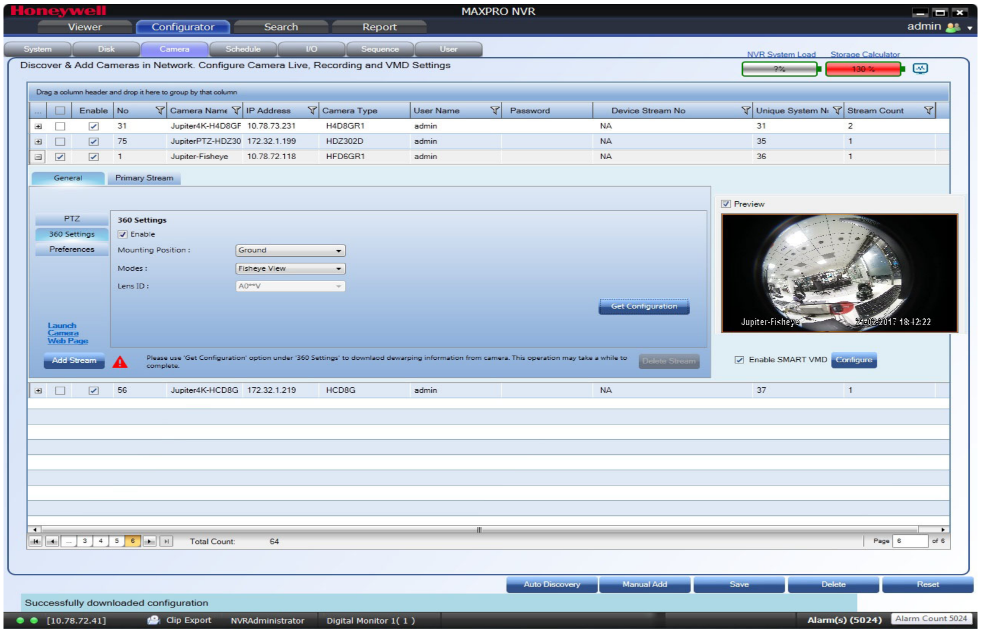
Step 3. Under General > 360 Settings, select the Enable check box to enable the dewarping feature.

Step 4. Under General > 360 Settings

- Select the Mounting Position. You have three options to choose from: Wall, Ceiling, and Ground. Based on the mounting position the views are displayed.

Step 5. Click the Get Configuration button. The dewarping configuration takes a while to download the dewarping configuration. A message Successfully downloaded configuration is displayed in the bottom of the camera screen.

Note: *For each Mounting Position, you need to click Get Configuration button to download the corresponding configuration.*



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	31	Jupiter4K-H4D8GF	10.78.73.231	H4D8GR1	admin		NA	31	2
⊞	□	☑	75	JupiterPTZ-HDZ30	172.32.1.199	HDZ302D	admin		NA	35	1
⊟	☑	☑	1	Jupiter-Fisheye	10.78.72.118	HFD6GR1	admin		NA	36	1
⊞	□	☑	56	Jupiter4K-HCD8G	172.32.1.219	HCD8G	admin		NA	37	1

360 Settings

☑ Enable

Mounting Position : Ground

Modes : Fisheye View

Lens ID : A0**V

Please use 'Get Configuration' option under '360 Settings' to downlaod dewarping information from camera. This operation may take a while to complete.

☑ Enable SMART VMD

... 3 4 5 6 Total Count: 64 Page 6 of 6

Successfully downloaded configuration

[10.78.72.41] NVRAdministrator Digital Monitor 1(1) Alarm(s) (5024) Alarm Count 5024

Dewarping Success Message

Step 6. After successful download of configuration, click Save.

Step 7. Under General > 360 Settings

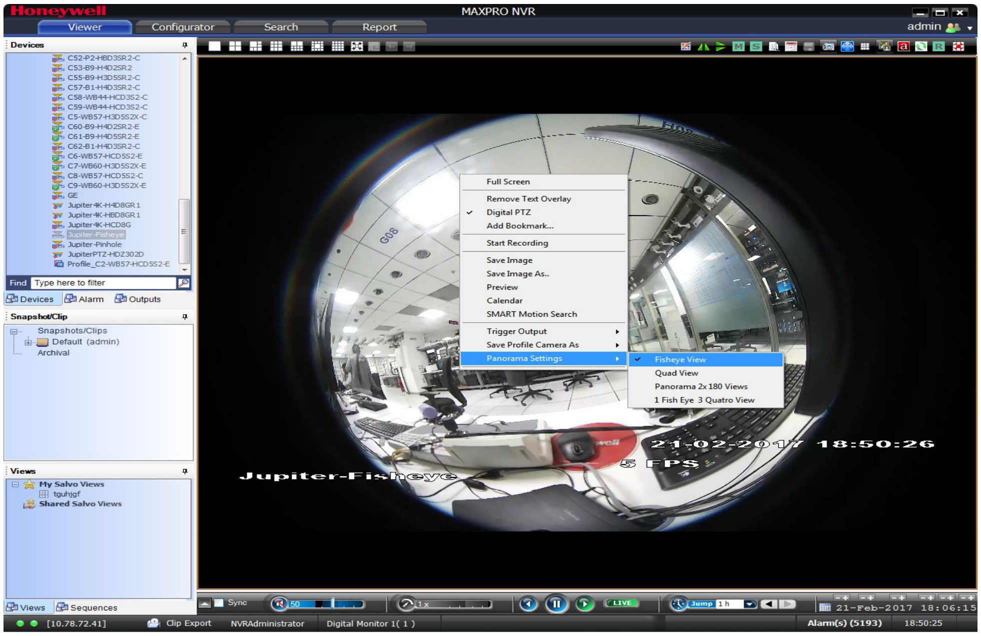
- Select the Mounting Position. You have three options to choose from: Wall, Ceiling, and Ground. Based on the mounting position the views are displayed.
- Select the Mode for the camera. The available modes are FishEye Mode, Quad Mode, and Perimeter Mode. The default mode is FishEye Mode.

Note: *Based on the Mounting Position the modes/views are displayed.*

- Lens ID for the camera is disabled.

Step 8. Click Save to complete the configuration.

Step 9. In Viewer, drag and drop the EquIP Fisheye Model (HFD6GR1) camera and then right-click to view the Dewarping options as shown below. For various Dewarped views refer to the *MAXPRO® NVR Operator's Guide*.



Dewarped Views List

Managing Analog Cameras

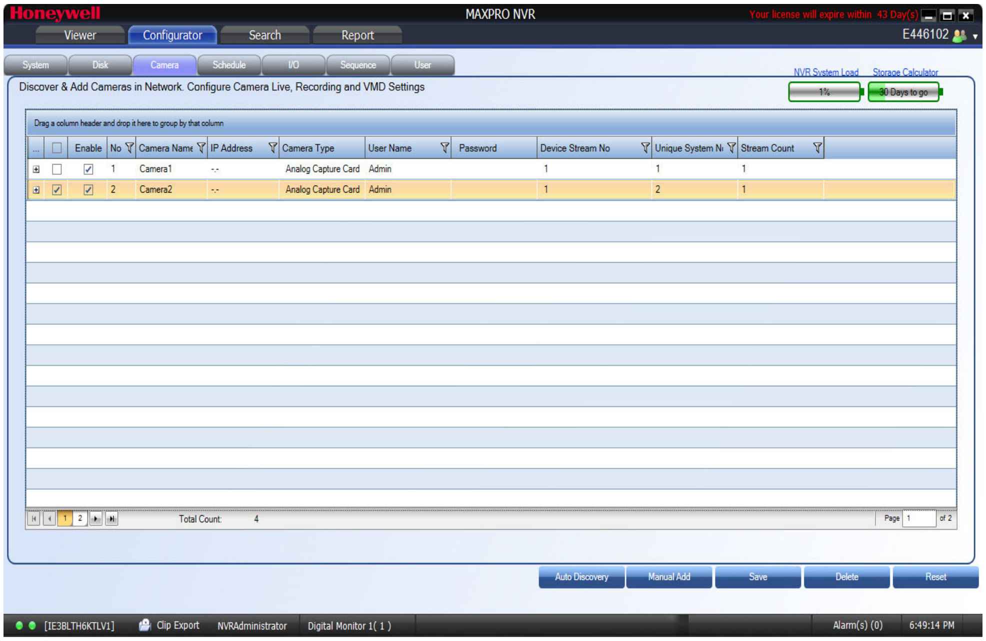
MAXPRO NVR Hybrid now supports Analog Capture card through which you can connect up to 16 analog cameras. Refer to MAXPRO NVR Hybrid Connections section on page 90 that depict the MAXPRO NVR Hybrid SE, XE and PE box with analog capture card.

Adding/Deleting Analog Cameras

Step 1. Connect the required number of cameras manually to analog capture card. The maximum number of analog cameras can be connected is 16.

Step 2. Click the Configurator tab. The System page displays by default.

Step 3. Click the Camera tab to open the Camera page. All analog cameras that are pre-configured in the factory image appear in the Camera page when you first open it.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	1	Camera1	-.-	Analog Capture Card	Admin		1	1	1
⊞	☑	☑	2	Camera2	-.-	Analog Capture Card	Admin		1	2	1

Total Count: 4

Page 1 of 2

Adding or Deleting Analog Camera

Step 4. Click Manual Add. A new camera is added in the camera pane.

- Under Camera Type - Displays the type of camera. Select the Analog Capture Card option to add analog cameras.

To delete Analog Camera

Step 1. Select the required analog camera channel check box.

Step 2. Click Delete. A confirmation message appears “Do you really want to delete camera(s)”

Step 3. Click Yes to delete.

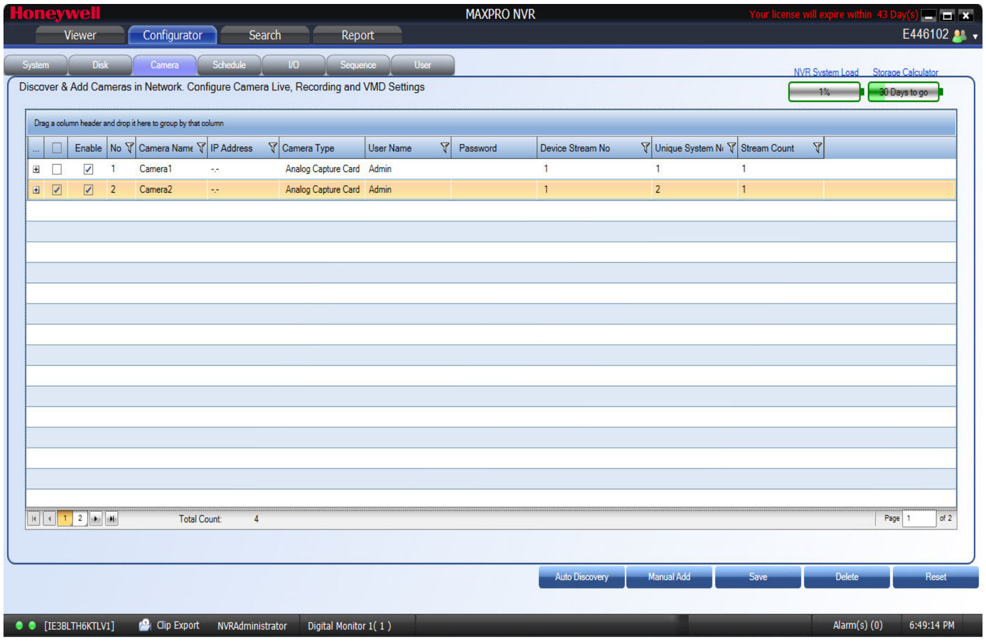
Configuring Analog Cameras

Pre-requisite to configure analog cameras: Ensure that you connect the required number of cameras manually to the analog capture card and then perform the below steps.

To configure analog cameras

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to open the Camera page.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	1	Camera1	-.-	Analog Capture Card	Admin		1	1	1
⊞	☑	☑	2	Camera2	-.-	Analog Capture Card	Admin		1	2	1

1 2 Total Count: 4 Page 1 of 2

Camera page

Note: *All analog cameras that are pre-configured in the factory image appear in the Camera page when you first open it.*

Step 3. Under the Camera pane, select a camera to change the default parameters for the following settings.

- Enable/Disable - Enables or disables a camera for recording and live video. By default the check box corresponding to a camera to enable live video preview is selected. To disable live video preview, clear the check box corresponding to a camera. The live video appears under Video Preview at the bottom right corner of the Camera page.
- Number - Displays the camera number. You cannot modify the camera number.

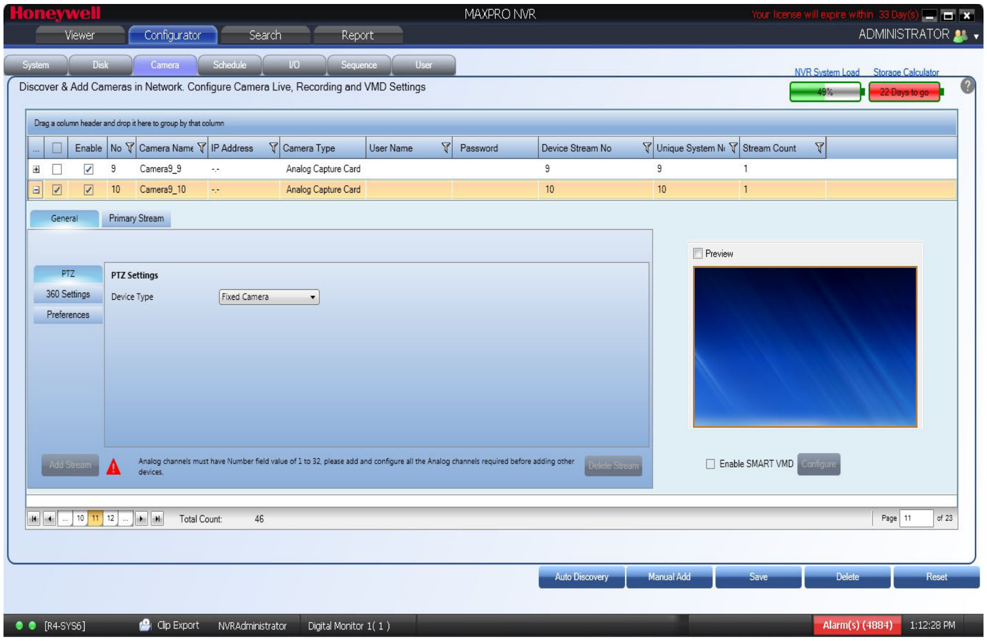
Note: *Analog channels must have Number field value of 1 to 32, please add and configure all the analog channels required before adding other devices.*

- Camera Name - Displays the camera name. You can type a new camera name limited to a maximum of 50 alphanumeric characters.
- IP Address - This is -.- by default for analog cameras. You can provide any valid IP if required.
- Camera Type - Displays the type of camera. Select the Analog Capture Card option to add analog cameras.
- User Name: Displays the default user name, “Admin” for the camera. You can type a new user name for the camera as applicable. Change this only if the user has been changed on the camera.

- Password: Displays the password, if any, for the camera. You can type a new password for the camera as applicable. Change this only if the password has been changed on the camera.
- Device Stream No: Displays the channel ID. You cannot modify this field.
- Unique System No: Display the unique camera ID. You can modify and assign a new number as applicable.
- Stream Count: Displays the number of streams associated with the camera. Analog cameras does not support additional streams. By default it displays 1.

Tip: Based on the Analog Capture Card model, system will prompt a message to add all supported channels by default. Click Yes to add all supported channels or No to add only 1 channel.

Step 4. For the required camera, click ⊞ on the left corner to open the camera properties pane see the Figure .



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

...	☐	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	☐	☑	9	Camera9_9	-.-	Analog Capture Card			9	9	1
⊟	☑	☑	10	Camera9_10	-.-	Analog Capture Card			10	10	1

PTZ Settings

Device Type: Fixed Camera

Analog channels must have Number field value of 1 to 32, please add and configure all the Analog channels required before adding other devices.

Camera properties pane

Note: *The camera properties pane is disabled when there are no cameras available in the system.*

Step 5. Under General > PTZ > PTZ Settings

- Device Type - Select whether the camera is a PTZ or Fixed. By default, ACUIX cameras are PTZ enabled. See Advanced PTZ Settings
- PTZ Sensitivity - Select the PTZ Sensitivity for PTZ camera. Available PTZ options are: Minimum, Low, Normal, High and Maximum.

Note: *The PTZ Sensitivity field is not available for fixed cameras.*

Step 6. Under Primary Stream > Recording > Video Quality Settings

- Resolution - The Resolution is defaulted to a fixed value based on the camera model (for example, HD3MDIP model defaults to 1280 x 720 resolution).
- Frame Rate - Select the FPS for a camera. FPS refers to the number of pictures displayed in exactly one second. FPS is a measure of how much information is used to store and display motion video. The term applies to digital video. Each frame is a still image; displaying frames in quick succession creates the illusion of motion.

Note: *30 FPS is the maximum frame rate in NTSC format and 25 FPS is the maximum frame rate in PAL format supported by MAXPRO NVR.*

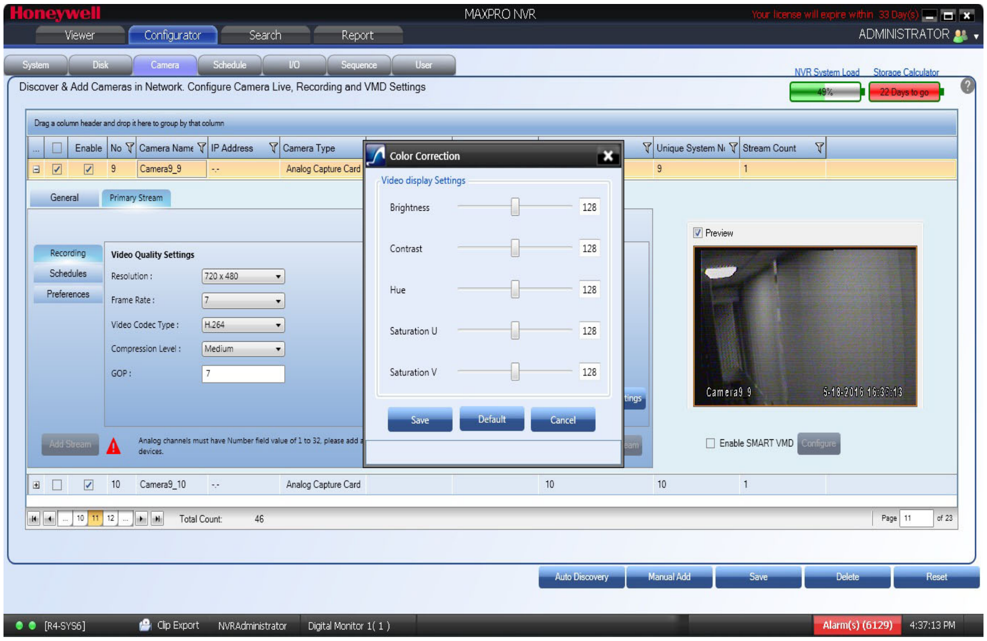
- Video Codec Type - Select the Codec type for the camera.
- Compression Level - The Compression Level is defaulted to “Medium”. You can select a new Compression ratio as applicable.
- GOP - The GOP value is proportional to Frame Rate value. If you set the Frame Rate value as 15 then the GOP value is updated to 15. You can also type a new GOP as applicable.
  Group of Pictures (GOP) are individual frames (number of pictures) that are grouped together and played back for viewing. A GOP consists of “IFrame” picture type that represents a fixed image independent of other picture types. Each GOP begins with this type of picture.

Note: *It is recommended to maintain the same GOP value as Frame Rate value.*

- Video Format - Select the Video Format (NTSC or PAL). The NTSC and PAL are the widely used video formats.
- Streaming Mode - The Streaming Mode is defaulted to UDP. You can select TCP streaming mode as applicable. The Streaming Mode is supported only for AXIS and ONVIF Cameras.
- Continuous - Select the FPS for Continuous recording.
- Event - Select the FPS for Event based recording.

Step 7. Click Video Display Settings. The Color Correction dialog box appears.

Note: *The Video Display Settings feature is available only on the desktop local client on the NVR Hybrid Server machine.*



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type			Unique System N	Stream Count
⊟	☑	☑	9	Camera9_9	-.-	Analog Capture Card			9	1
⊞	□	☑	10	Camera9_10	-.-	Analog Capture Card		10	10	1

Total Count: 46 | Page 11 of 23

Video Quality Settings

Resolution : 720 x 480

Frame Rate : 7

Video Codec Type : H.264

Compression Level : Medium

GOP : 7

Analog channels must have Number field value of 1 to 32, please add a devices.

□ Enable SMART VMD Configure

Color Correction

Video display Settings

Brightness	128
Contrast	128
Hue	128
Saturation U	128
Saturation V	128

Save | Default | Cancel

Color Correction dialog box

Step 8. Under Video Display Settings

- Move the slider right or left to increase or decrease the Brightness, Contrast, Hue, Saturation U and Saturation V.
  Or
  Type the required value in the respective boxes to adjust the video display settings.
  Or
  Click Default to set the default values.

Step 9. Click Save to save the display settings.

Step 10. Under Primary Stream > Schedules

- Recording Settings:
- Continuous Recording - All cameras added are defaulted to “24/7” recording. You can choose a different option from the drop-down list.
- Event Based Recording - This is “None” by default. Select an option from the drop-down if you want to do motion based recording.
- Recording Deletion Settings:
- Select the Event Recording clip deletion duration.
- Select the Continuous Recording clip deletion duration.
- Archive Recording Older Than:
- Continuous - This is “None” by default. Select an option from the drop-down if you want to archive the continuous recording.
- Event - This is “None” by default. Select an option from the drop-down if you want to archive the event recording.

- Delete Archived Recording After:
- Continuous Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived continuous recording can be deleted.
- Event Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived event recording can be deleted.

Step 11. Under Primary Stream > Preferences > Stream Preferences Settings. See step 5 for more information.

Step 12. Click Save.

PTZ Settings for Analog Camera

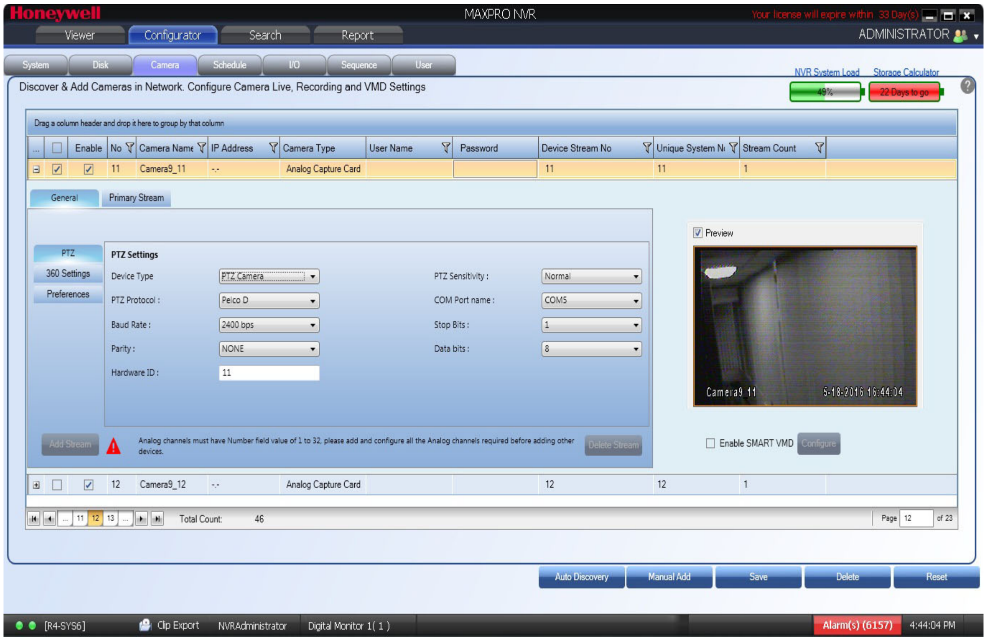
MAXPRO NVR now supports the advanced PTZ settings for an analog PTZ camera.

Note: *Advanced PTZ settings are available only for analog PTZ cameras.*

To set the PTZ settings

Step 1. Select the required analog PTZ camera from the camera pane.

Step 2. Click ⊞ on the left corner to open the camera properties pane.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊟	☑	☑	11	Camera9_11	-.-	Analog Capture Card			11	11	1
⊞	□	☑	12	Camera9_12	-.-	Analog Capture Card			12	12	1

PTZ Settings

Device Type	PTZ Camera	PTZ Sensitivity :	Normal
PTZ Protocol :	Pelco D	COM Port name :	COM5
Baud Rate :	2400 bps	Stop Bits :	1
Parity :	NONE	Data bits :	8
Hardware ID :	11		

Analog channels must have Number field value of 1 to 32, please add and configure all the Analog channels required before adding other devices.

☑ Preview

Camera9 11 5-18-2016 16:44:04

□ Enable SMART VMD

Total Count: 46

Page 12 of 23

[R4-SYS6] NVRAdministrator Digital Monitor 1(1) Alarm(s) (6157) 4:44:04 PM

Camera properties pane

Step 3. Under General > PTZ > PTZ Settings

- Device Type - Select the camera as a PTZ camera. The PTZ settings are displayed.
- Select the PTZ Protocol. Available PTZ Protocol options are VCL, Pelco P, Pelco D, Maxpro, GE Kalatel.

Note: *Vicon protocol is not supported in this release.*

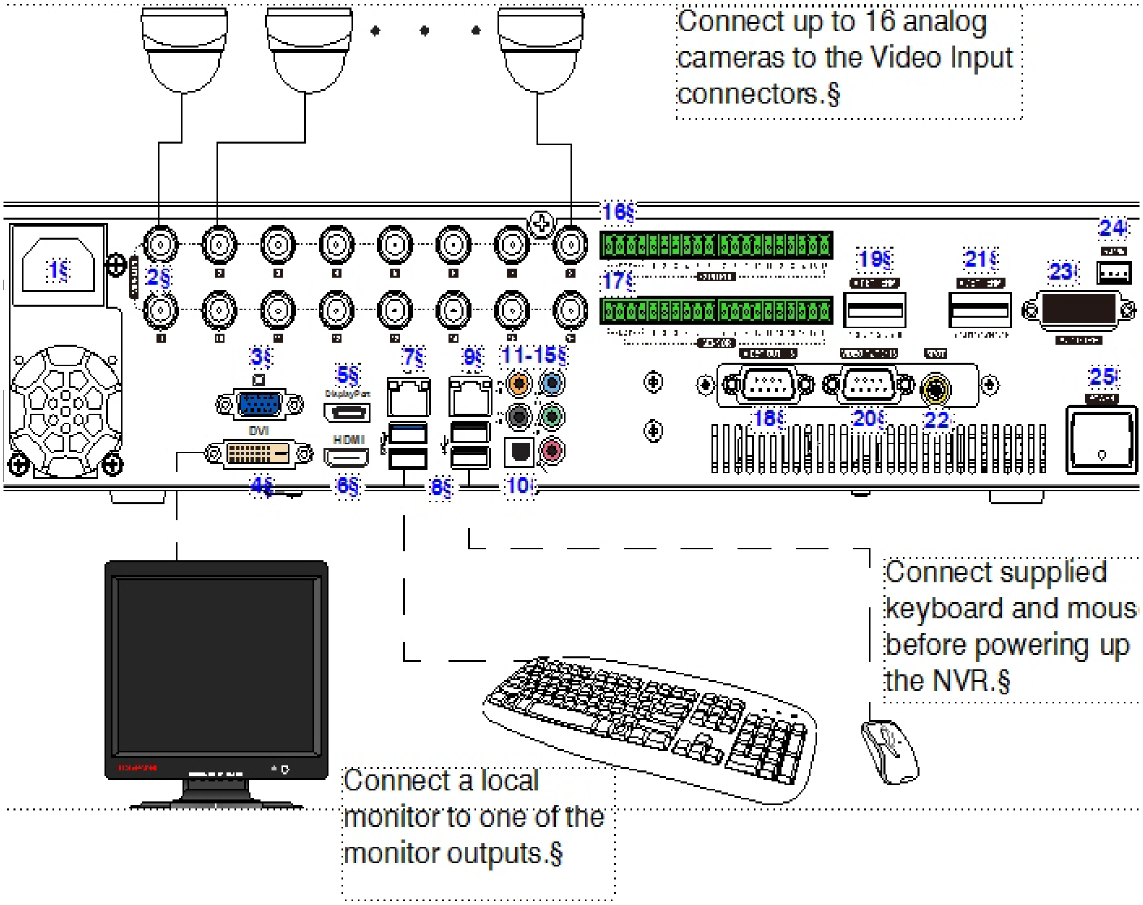
- Select the required Baud Rate. Available Baud Rates options are 110, 300,600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 56000, 57600, 115200, 128000, 256000.
- Select the Parity. Available Parity options are ODD and EVEN
- Type the Hardware ID, if the analog camera type is a PTZ camera. The hardware ID is based on the PTZ Protocol.
- Select the PTZ Sensitivity for a PTZ camera. Available PTZ options are: Low, Normal, High and Maximum.
- Select the COM Port name. Available COM Port names options are COM 1 and NONE For Hybrid PE, COM Port names are COM1, COM2, COM3, COM4 and NONE. Select COM 4 for analog PTZ control.
- Select the Stop Bits. Available stop bits options are 1 and 2.
- Select the Data Bits. Available data bits options are 7 and 8.

Step 4. Click Save.

Configuring the Input and Output for an Analog Camera

The input and output hardware configuration for an analog camera in MAXPRO NVR Hybrid is configured by default and when you add an analog camera, then by default the camera is mapped to their respective input and output ports. The first input/output port is mapped to the first camera, similarly the second camera is mapped to the second input/output port of the box and so on. The input output combinations cannot be mapped to any other analog or IP camera other than the default configuration.

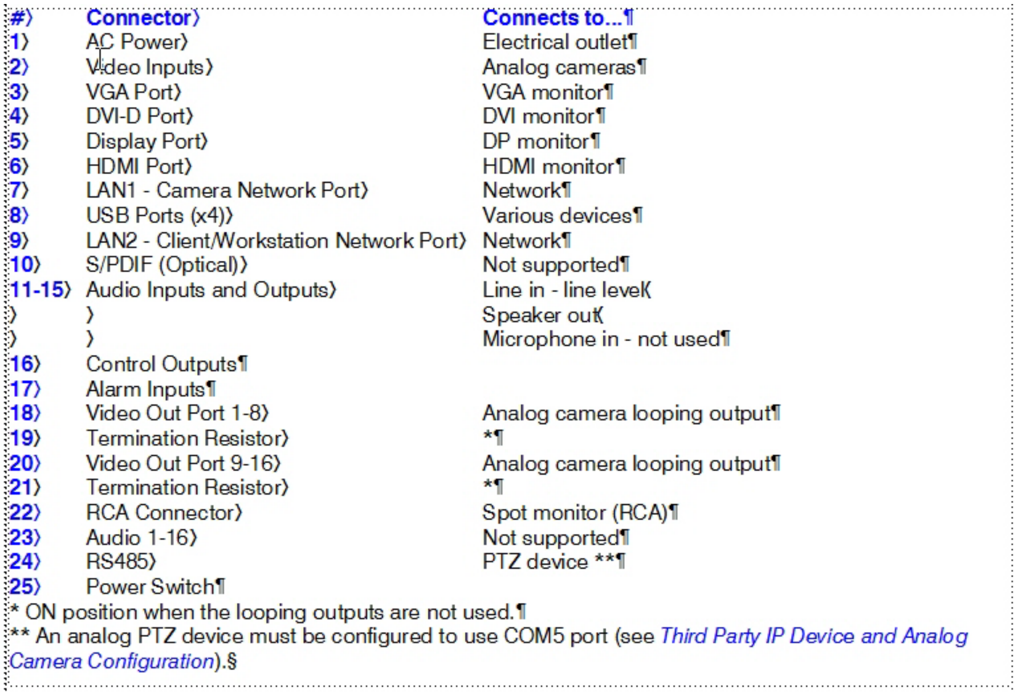
The below figures depicts the typical input and output ports (Highlighted in Red) and RS-485 connectors for MAXPRO NVR Hybrid XE, SE and PE Box. The SENSOR is the input port and CONTROL is the output port for both Hybrid XE (See the figure Input and Output Ports For MAXPRO NVR Hybrid XE) and SE Box (See the figure Input and Output Ports For MAXPRO NVR Hybrid SE). The detailed input and output ports for NVR Hybrid PE box is shown in Input and Output Ports For MAXPRO NVR Hybrid PE.



Connect up to 16 analog cameras to the Video Input connectors.§

Connect supplied keyboard and mous before powering up the NVR.§

Connect a local monitor to one of the monitor outputs.§

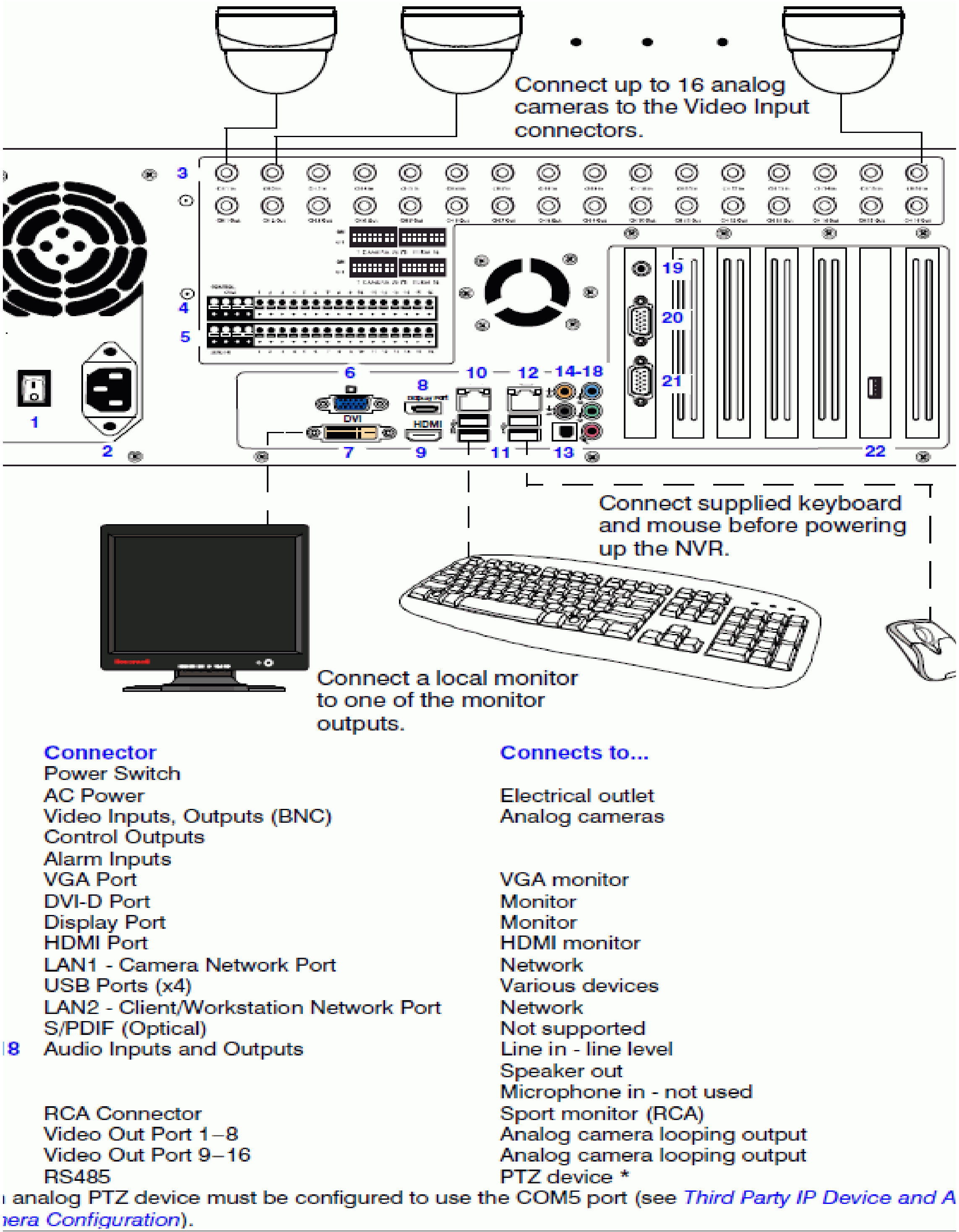


#	Connector	Connects to...¶
1	AC Power	Electrical outlet¶
2	Video Inputs	Analog cameras¶
3	VGA Port	VGA monitor¶
4	DVI-D Port	DVI monitor¶
5	Display Port	DP monitor¶
6	HDMI Port	HDMI monitor¶
7	LAN1 - Camera Network Port	Network¶
8	USB Ports (x4)	Various devices¶
9	LAN2 - Client/Workstation Network Port	Network¶
10	S/PDIF (Optical)	Not supported¶
11-15	Audio Inputs and Outputs	Line in - line level(
		Speaker out(
		Microphone in - not used¶
16	Control Outputs¶	
17	Alarm Inputs¶	
18	Video Out Port 1-8	Analog camera looping output¶
19	Termination Resistor	*¶
20	Video Out Port 9-16	Analog camera looping output¶
21	Termination Resistor	*¶
22	RCA Connector	Spot monitor (RCA)¶
23	Audio 1-16	Not supported¶
24	RS485	PTZ device **¶
25	Power Switch¶	

* ON position when the looping outputs are not used.¶

** An analog PTZ device must be configured to use COM5 port (see *Third Party IP Device and Analog Camera Configuration*).§

Input and Output Ports For MAXPRO NVR Hybrid XE



Connect up to 16 analog cameras to the Video Input connectors.

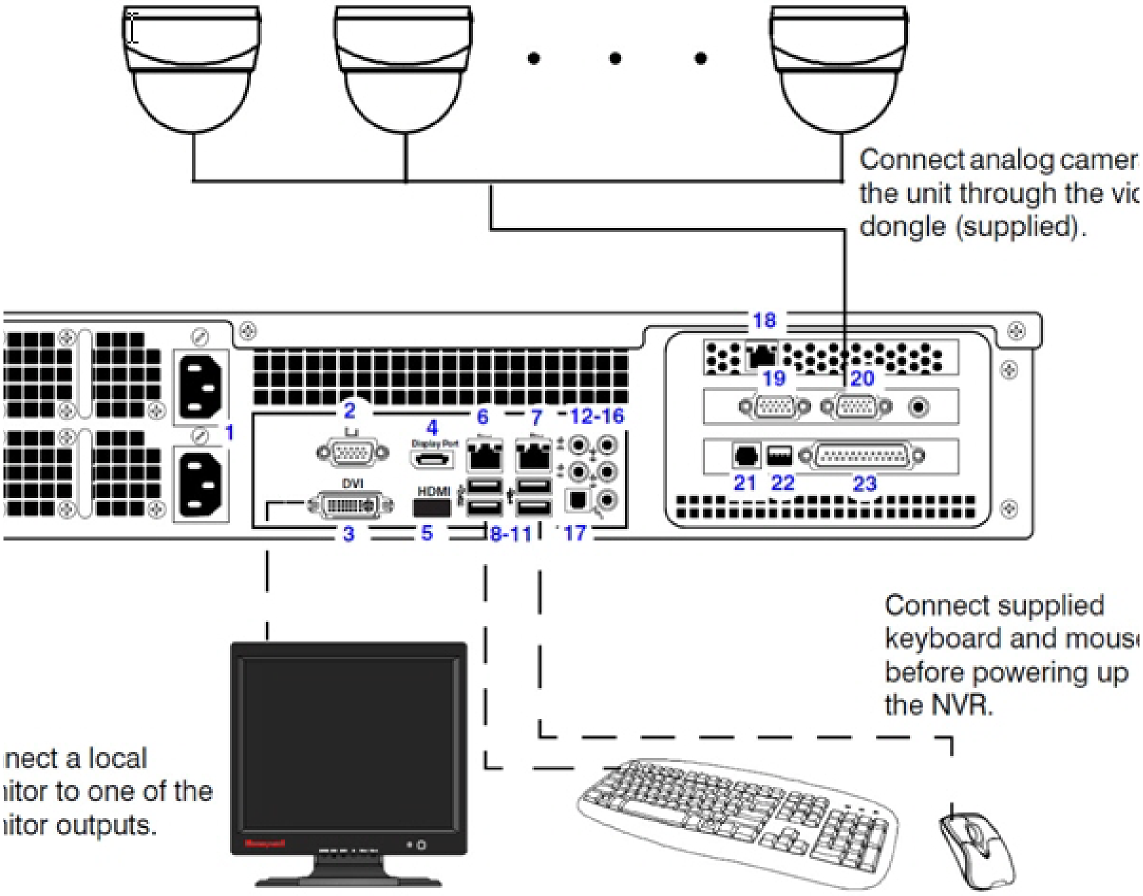
Connect supplied keyboard and mouse before powering up the NVR.

Connect a local monitor to one of the monitor outputs.

	Connector	Connects to...
	Power Switch	
	AC Power	Electrical outlet
	Video Inputs, Outputs (BNC)	Analog cameras
	Control Outputs	
	Alarm Inputs	
	VGA Port	VGA monitor
	DVI-D Port	Monitor
	Display Port	Monitor
	HDMI Port	HDMI monitor
	LAN1 - Camera Network Port	Network
	USB Ports (x4)	Various devices
	LAN2 - Client/Workstation Network Port	Network
	S/PDIF (Optical)	Not supported
8	Audio Inputs and Outputs	Line in - line level Speaker out Microphone in - not used
	RCA Connector	Sport monitor (RCA)
	Video Out Port 1–8	Analog camera looping output
	Video Out Port 9–16	Analog camera looping output
	RS485	PTZ device *

analog PTZ device must be configured to use the COM5 port (see *Third Party IP Device and A era Configuration*).

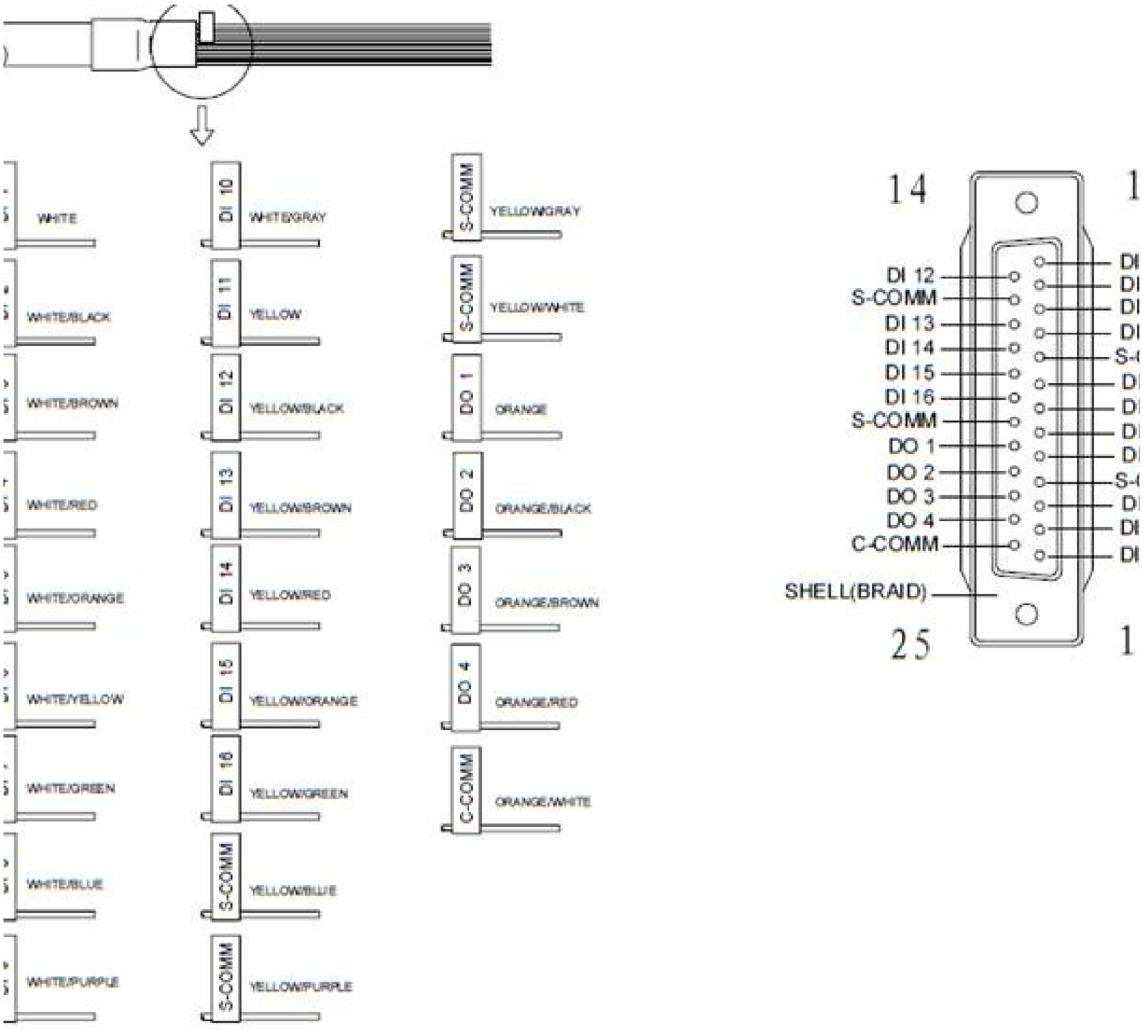
Input and Output Ports For MAXPRO NVR Hybrid SE



#	Connector	Connects to...
1	AC Power (x2)	Electrical outlet
2	VGA Port	VGA monitor
3	DVI-D Port	Monitor
4	Display Port	Monitor
5	HDMI	Not supported
6	LAN1 - Camera Network Port	Network
7	LAN2 - Client Workstation Network Port	Network
8-11	USB Ports (x4)	Various devices
12-16	Audio inputs and outputs	Line in - line level Speaker out Microphone in - not used
17	S/PDIF (Optical)	
18	RAID Management Port	RAID device
19	Video Input 1-8	Cameras
20	Video Input 9-16	Cameras
21	Not used	
22	RS485	PTZ device *
23	Input and Output Ports	Alarm inputs and Control outputs

* An analog PTZ device must be configured to use the COM4 port (see *Third Party Device Configuration*).

MAXPRO NVR Hybrid PE Rear View



Input and Output Ports For MAXPRO NVR Hybrid PE

Spot Monitoring

The Spot Monitoring feature allows you to view the live video of analog cameras from the box. You need to connect a physical monitor to the RCA port on Hybrid boxes to view the live video.

Server VMD (SMART VMD)

Video Motion Detection (VMD) is a built-in intelligent feature that enables you to configure motion detection for the live video streamed by MAXPRO NVR using its connected cameras. Configuring motion detection involves defining one or more Region of Interest (ROI) in the field of view. Regions are drawn in the field of view to specify where the motion should be detected or excluded.

The Server VMD running on the MAXPRO NVR provides superior performance comparing to regular VMD, due to its capability to differentiate real object motion from:

- Image or camera noises
- Irrelevant motion due to weather (example: rain, snow)
- Lighting changes

Few cameras have built-in VMD capabilities. There is a provision included in the MAXPRO NVR user interface to manually configure VMD (known as Server-based VMD) for the cameras that do not have the VMD feature built-in them.

Caution: At a time, a camera can be configured only with built-in (camera based VMD) or the Server VMD (SMART VMD). If both are enabled then only SMART VMD alarms will be displayed to user and built-in (camera based VMD) alarms will be ignored.

SMART VMD-Technology Overview

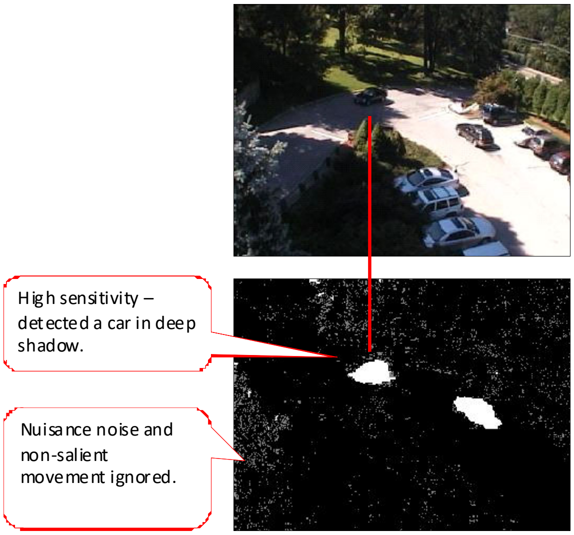
SMART VMD uses the same detection module as full analytics.

SAMRT VMD	Traditional VMD (Cameras and Head-ends)
• Object based- triggers alarms based on moving objects. • Ignores changes in lighting, video noise, and rain. • Ignores other false alarm triggers that affect pixel-based VMD. • Processing at lower frame rate, simple object validation: low CPU requirements.	• Pixel based - compares image pixels, detects changes with a single threshold. • Does not adapt to changing environment. • Susceptible to nuisance alarms from illumination changes, rain, moving trees.

Detection of Relevant Motion

- Statistical modeling to maintain high detection sensitivity, while filtering out non-salient motion.

- Significant improvement over standard video motion detection.


High sensitivity – detected a car in deep shadow.
Nuisance noise and non-salient movement ignored.

Detection of relevant motion

To configure SMART VMD

Note: *Before enabling Server VMD for a camera configured to stream H.264 or MPEG4 video, please ensure that the GOP size is set to be smaller or equal to the stream frame rate. For objects that do not persist in the region till the stream contains at least 1 iFrame, SMART VMD ignores as noise to reduce false alarms. Example: Insect flying in front of a camera. It is recommended that you configure large enough regions to capture relevant motion in the area of interest. Server VMD is not supported on 360 camera (fisheye or panomorph) views.*

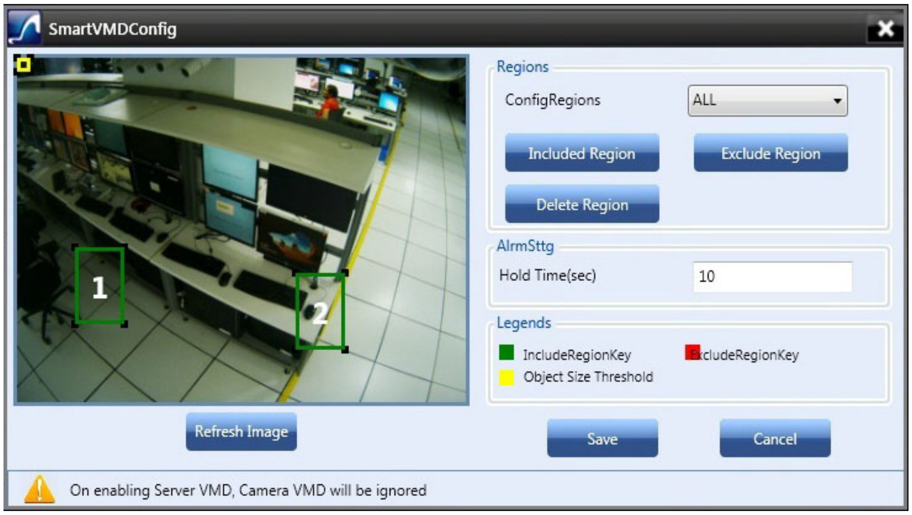
Step 1. Select the Enable SMART VMD check box.

Step 2. Click Configure. The SMART VMD Configuration dialog box appears (see SMART VMD Configuration).

Step 3. Click Include Region and a new include region (in green) appears. On the field of view, click and drag the corners of the rectangle to position and resize the region where you want the motion to be detected. Repeat the operation to include more regions.

Step 4. Click Exclude Region and a new exclude region (in red) appears. On the field of view, click and drag the corners of the rectangle to position and resize the region where you do not want motion to be detected. Repeat the operation to exclude more regions.

Step 5. To delete a region, select the region from the Configured Regions drop-down list, then click Delete Region.



ConfigRegions: ALL

Hold Time(sec): 10

🟩 IncludeRegionKey 🟥 ExcludeRegionKey

🟨 Object Size Threshold

⚠ On enabling Server VMD, Camera VMD will be ignored

SMART VMD Configuration

Note:

- You can draw a maximum of 10 ROIs (includes Include and Exclude regions).
- Include regions are shown as green rectangles and Exclude regions are shown in red rectangles in the field of view.
- Each region is assigned a unique identifier number for easy identification.
- The Exclude region overwrites the Include region. No motion is detected in the area that is inside any of the exclusion regions.

Note:

Step 6. Under Alarm Settings

- Type the Hold Time (sec). This indicates the hold time for the motion video after the detected motion stops. When motion is detected and motion video has started being recorded, if motion stops briefly and then resumes within Hold Time (sec), no “Motion stopped” event is generated. This brief gap in detected motion is ignored and motion triggered recording continues without interruption. On the other hand, if motion stops and no new motion is detected within Hold Time (sec), then the “Motion stopped” event is reported. Motion triggered recording is then stopped after additional Post-Alarm duration. The Hold Time range is 0 to 30 seconds.
- The Object Size Threshold (the minimum object size required to trigger an alarm) is displayed as a yellow rectangle in the field of view. Click and drag the corners of the rectangle to resize the minimum object size for motion detection.

Note: *The Object Size Threshold is a universal threshold across the entire image. By default, the Object Size Threshold is set to the smallest size, and therefore even very small motions trigger an alarm. This may not be appropriate for all sites and cameras, and the yellow rectangle size should be adjusted if the default size is not adequate.*

Tip: Click the Refresh Image button to refresh the video.

Step 7. Click Save to save the changes or click Cancel to abort the changes.

Updating the Cameras

You can modify the settings of a camera to change the camera name, IP address, camera type, fixed/PTZ, advanced camera settings, and so on. You can update the camera settings only if you have admin rights.

To update a camera

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to navigate to the Camera page. The list of cameras configured are displayed.

Step 3. Select the row corresponding to the camera you want to modify.

Step 4. Change the settings such as camera name, IP address, and so on.

Step 5. Click Save.

Deleting the Cameras

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to navigate to the Camera page.

Step 3. Select the check box corresponding to the camera you want to delete.

Step 4. Click Delete. A confirmation message appears at the bottom of the display area.

Step 5. Click Yes. The selected camera is deleted.

Configuring the Schedules

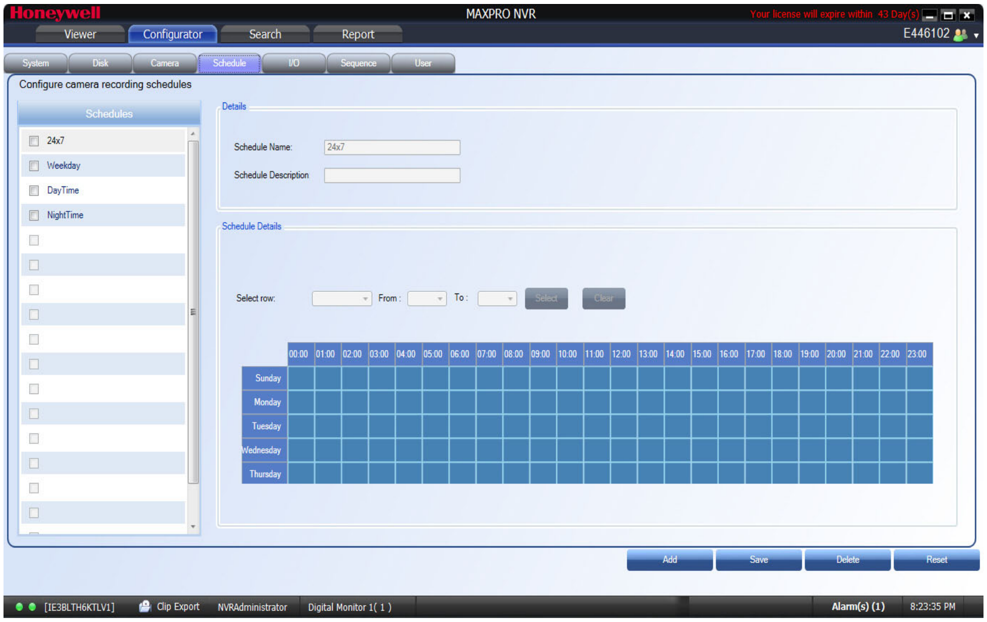
A schedule defines the date and times when continuous recording and video analytics (motion detection) functions are enabled for a camera. You can create schedules for camera(s) to record video at recurring intervals for continuous recording or event based recording (for example, motion event). There are four default schedules: 24 x 7, Weekday, DayTime, NightTime.

Creating a Schedule

You can create schedules for the camera to record video at recurring intervals.

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Schedule tab to navigate to the Schedule page. By default MAXPRO NVR supports the following 4 default schedules: 24 x 7, Weekday, DayTime, and NightTime.



Your license will expire within 43 Day(s)

Configure camera recording schedules

□ 24x7
□ Weekday
□ DayTime
□ NightTime

Schedule Name: 24x7

Schedule Description:

Select row: From : To :

[IE3BLTH6KTLV1] NVRAdministrator Digital Monitor 1(1)

Schedule page

Note: *You cannot modify/delete any of the default schedules.*

Step 3. Click Add to create a new schedule.

Step 4. Configure the schedule details as listed in the following table.

Type	Setting
Schedule Name	The schedule name appears by default. You can type a new schedule name as applicable.
Schedule Description	Type the schedule description.
Schedule settings	
Select row	Select the day of the week.
From	Select the from date.
To	Select the to date.
Select	Click Select. The schedule details entered appear under Scheduler Settings.
Clear	Click Clear to clear the information entered.

Step 5. Click Save or click Reset to undo the changes. You can create a maximum of 50 schedules in MAXPRO NVR.

Deleting a Schedule

You can delete a schedule for the camera when you do not want to record video at recurring intervals.

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Schedule tab to navigate to the Schedule page.

Step 3. Under Schedules, select the schedule you want to delete from the list. The schedule's details appear.

Step 4. Click Delete, and then click Yes in response to the confirmation message.

Configuring the Sequences

A sequence is a set of live video streamed one after the other from cameras for a specified time interval. You can select the cameras or presets to be included in a sequence and also specify the time interval for which the video from each camera or preset must be displayed. Presets must be defined for the cameras before including them in the sequence.

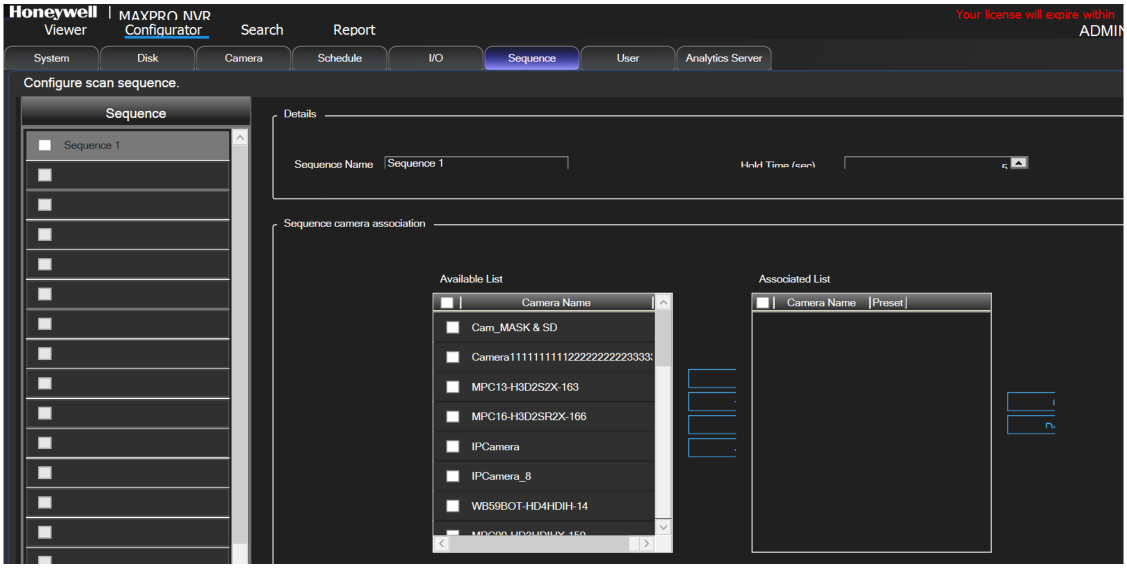
Creating a Sequence

You can create a sequence to display video that is captured from different cameras connected to MAXPRO NVR. You can add a maximum of 50 sequences in MAXPRO NVR.

To create a sequence

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Sequence tab to navigate to the Sequence page.



Configure scan sequence.

Sequence

□ Sequence 1

Sequence Name: Sequence 1

Hold Time (sec): 5

Available List:

□ Cam_MASK & SD
□ Camera1111111111222222222223333
□ MPC13-H3D2S2X-163
□ MPC16-H3D2SR2X-166
□ IPCamera
□ IPCamera_8
□ WB59BOT-HD4HDIH-14
□ MPC00-HD2HDIHX-150

Sequence page

Step 3. Click Add.

Step 4. Under Details

- The Sequence Name appears by default. You can type a new Sequence Name as applicable. The Sequence Name is limited to a maximum of 18 alphanumeric characters.
- The Hold Time (Sec) box appears by default. You can type or select a new Hold Time (Sec) for the camera to display video before advancing to the next camera.

Step 5. Under Sequence camera Association

- Select the check box corresponding to the camera that must be included in the sequence under the Available List, and then click >. The selected camera appears under the Associated List.
- Click >> to move all the cameras to the Associated List.
- Select the check boxes corresponding to the camera that you do not want to include in the sequence under the Associated List and then click <. The selected camera appears under the Available List.
- Click << to move all the cameras to the Available List.
- To include presets in the sequence, select the preset number from the drop-down list under the Preset column next to a camera. The video from each camera in the list is displayed sequentially.

Note: *The drop-down list is not visible in the Preset column for a fixed camera.*

Step 6. Click Save.

Rearranging the Cameras In the Sequence

You can rearrange the cameras and presets in the sequence. When you rearrange them, the sequence of live video streaming from each of the cameras is altered based on the rearrangement.

To rearrange the cameras

Step 1. Select the check box corresponding to the camera you want to rearrange inside the sequence.

Step 2. Click Up to move the camera one row up, or click Down to move the camera one row down.

Step 3. Click Save.

Removing Presets from a Sequence

You can remove a preset when you do not want it to be associated with a sequence.

To remove presets from a camera

Step 1. In the Preset column, do not select any preset from the drop-down list.

Step 2. Click Save.

Updating a Sequence

Updating a sequence allows you to change the sequence of video display from cameras.

To update a sequence

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Sequence tab to navigate to the Sequence page.

Step 3. Select the check box corresponding to the sequence you want to update.

Step 4. You can change the sequence name, dwell time and sequence of the cameras.

Step 5. Click Save.

Deleting a Sequence

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Sequence tab to navigate to the Sequence page.

Step 3. Select the check box corresponding to the sequence you want to delete.

Step 4. Click Delete. A confirmation message appears on the top of the display area.

Step 5. Click Yes.

Performing User Administration

A user in MAXPRO NVR is responsible for performing various operations like viewing video, reporting alarms, and other video surveillance tasks. You can create two types of users in MAXPRO NVR: System Local User and Windows User.

Caution: Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.

System Local User

A System local user can access only MAXPRO NVR Client. This user may not have access to a client workstation.

Windows User

A Windows user can access a client workstation and also MAXPRO NVR Client.

Users and Roles

Roles are provided to a user. These roles comprise a set of privileges. When a user is associated to a role, the privileges that are available for the role are also assigned to the user.

The various roles available in MAXPRO NVR are as follows:

- NVR Administrator
- Operator
- Supervisor
- Internet Operator
- Live View Operator

For MAXPRO NVR Software-Only Solution

The first time MAXPRO NVR is installed, two default users are created.

- admin/trinity - Non-Windows user. Honeywell recommends to create a new NVR user (See Adding a User) in the Configurator tab and use the same to logon.
- Installed user - Windows user. You enter the credentials for this user while installing the MAXPRO NVR software.

For MAXPRO NVR Turnkey (XE,SE,PE) Solution

There are 3 default users created for NVR turnkey units shipped with v4.0 or later version.

- admin/trinity - Non-Windows user. Honeywell recommends to create a new NVR user (See Adding a User) in the Configurator tab and use the same to logon.
- NVR-Admin/Password$123- Windows user.
- NVRServiceUser - Windows non-interactive user used for NVR Services.

Note: *For a Windows user, Honeywell recommends to disable the default Administrator User account and create a new Administrator User account. See* Securing MAXPRO NVR *section on page* 299 *for more information. Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.*

The following table lists the various user roles and the privileges applicable to the

	Viewer	**Configurator**	**Search**	**Report**
NVR Administrator	X	X	X	X
Operator	X	-	-	-
Supervisor	X	-	X	X
Internet Operator	X	-	-	-
Live View Operator	X	-	-	-

role.

Legend

- "X" indicates that the user's role has access to the privilege.
- "-" indicates that the user's role does not have access to the privilege.

Note:

- The Internet Operator role is optimized for remote monitoring at lower bandwidths (minimum bandwidth requirements still apply to be able to stream required video data)
- The Live View Operator role can only access live video, and does not have access to playback operations.

Note:

When you install MAXPRO NVR for the first time, a default user named "admin" is created. The admin user is assigned the role "NVRAdministrator". Only the user having "NVRAdministrator" privilege can add new users, assign roles to the added users, add or modify the privileges to the users, and perform various configurations in MAXPRO NVR.

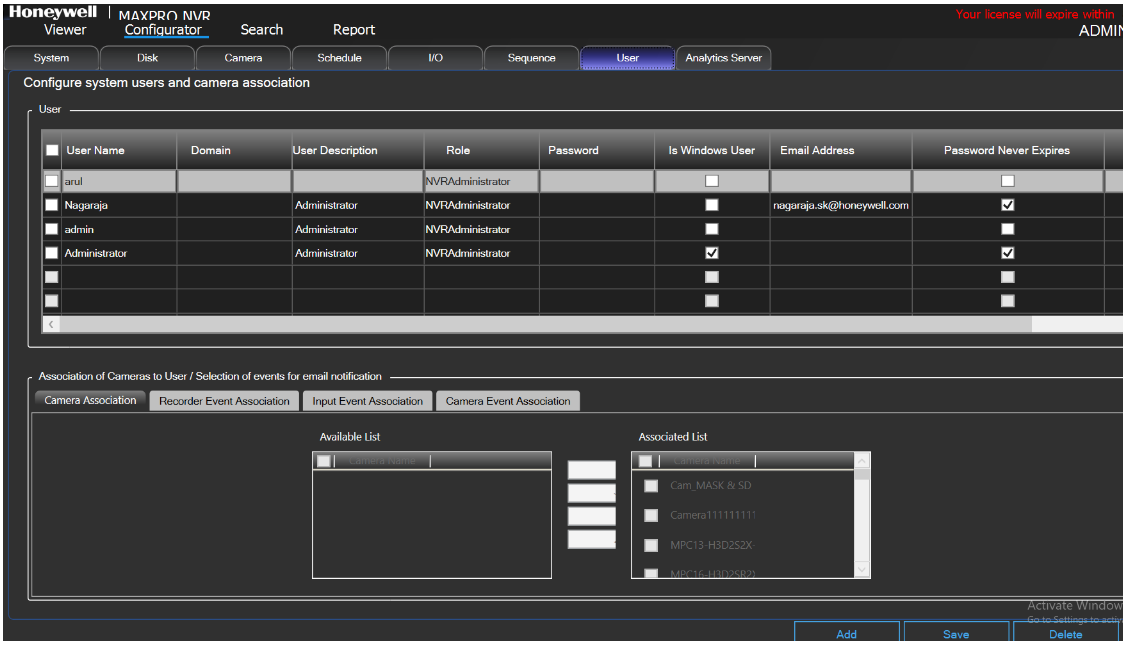
Adding a User

You can add a user by providing a unique user name and a password. Only the "NVR Administrator role" user can add a new user in MAXPRO NVR. You can add up to 1024 users in MAXPRO NVR. After you add a new user, you can assign a role to it.

To add a user

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the User tab to navigate to the User page.



Configure system users and camera association

User

□ User Name	Domain	User Description	Role	Password	Is Windows User	Email Address	Password Never Expires
□ arul			NVRAdministrator		□		□
□ Nagaraja		Administrator	NVRAdministrator		□	nagaraja.sk@honeywell.com	☑
□ admin		Administrator	NVRAdministrator		□		□
□ Administrator		Administrator	NVRAdministrator		☑		☑
□					□		□
□					□		□

Association of Cameras to User / Selection of events for email notification

Available List

□ Camera Name

Associated List

□ Camera Name
□ Cam_MASK & SD
□ Camera111111111
□ MPC13-H3D2S2X-
□ MPC16-H3D2SR2)

User page

Step 3. Click Add. A new row is created with a default set of values for the user.

Step 4. Under the User Name column, the default user name is displayed. You can type a new user name as applicable.

Step 5. Under the Domain column, type the Windows domain name if the user is a Window's user and is part of a Window's domain network.

Step 6. Under the User Description column, type a description for the user.

Step 7. Under the Role column, select the role you want to assign to the user from the drop-down list.

Step 8. Under the Password column, type the user's password.

Note: *Minimum length of the password is 6 characters. While adding a User, if the password of other users added before 3.1 release is less than 6 characters then an error message is displayed and all passwords need to be updated to meet the minimum requirement.*

Step 9. Under the IsWindowsUser column, select the check box if the user is a Window's user. if IS Windows user check box is selected then the Password Never Expire check box is disabled and it cannot be cleared. This ensures that for a Windows user the password will never expiries.

Step 10. Under the Email Address column, type the user's email address.

Step 11. Under Password Never Expires, select the check box to ensure that the user password never expires.

Note: *If IS Windows user check box is selected then the Password Never Expire check box is disabled and it cannot be cleared. This ensures that for a Windows user the password will never expiries.*

Step 12. Under Anonymization, select the check to anonymize the live video for the specific user. See Privacy Protection Settings (GDPR Favored) for complete information on Anonymization feature.

Step 13. Click the Camera Association tab to associate cameras to the user.

- To associate one camera at a time, under the Available List, select a camera and then click >. The selected camera appears under the Associated List.
- Click >> to associate all cameras to the Associated List.
- To remove an associated camera, under the Associated List, select a camera and then click <. The selected camera appears under the Available List.
- Click << to disassociate all the cameras to the Available List.

Step 14. Click the Recorder Event Association tab to associate recorder events to the user.

- To associate one particular event, under the Available List, select the check box corresponding to the event and then click >. The select recorder event appears under the Associated List.
- Click >> to associate all events to the Associated List.
- To remove an event, under the Associated List, select a check box corresponding to the event and then click <. The selected event appears under the Available List.

- Click << to disassociate all the events to the Available List.

Step 15. Click the Input Event Association tab to associate input events to the user.

- To associate one particular input event, under the Available List, select the check box corresponding to the input event and then click >. The selected input event appears under the Associated List.
- Click >> to associate all the input events to the Associated List.
- To remove an input event, under the Associated List, select a check box corresponding to the input event and then click <. The selected input event appears under the Available List.
- Click << to disassociate all the input events to the Available List.

Step 16. Click the Camera Event Association tab to associate camera events to the user.

- To associate one particular event, under the Available List, select the check box corresponding to the event and then click >. The select camera event appears under the Associated List.
- Click >> to associate all the camera events to the Associated List.
- To remove an event, under Associated List, select a check box corresponding to the event and then click <. The selected camera event appears under the Available List.
- Click << to disassociate all the camera events to the Available List.

Step 17. Click Save to save the information.

Note: *You can add a maximum of 1024 users in MAXPRO NVR.*

Updating a User

You can modify the settings of a user to change the user ID, password, role, description, IsWindowsUser flag, and email address. You can update user settings only if you have admin rights.

Note: *Minimum length of the password is 6 characters. While adding a User, if the password of other users added before 3.1 release is less than 6 characters then an error message is displayed and all passwords need to be updated to meet the minimum requirement.*

To update a user

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the User tab to navigate to the User page.

Step 3. Select the check box corresponding to the user you want to modify.

Step 4. Change the settings such as user name, user description, and so on.

Step 5. Click Save.

Deleting a User

You can remove a user from MAXPRO NVR. When you delete a user, all the associations made to the user are also removed.

To delete a user

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the User tab to navigate to the User page.

Step 3. Select the check box corresponding to the user you want to delete.

Step 4. Click Delete. A confirmation message appears at the bottom of the display area.

Step 5. Click Yes.

Recommended stream Settings

To view the video streaming in NVR you must configure the primary stream for recording and secondary stream for live video streaming in both Camera tab and Web Page. If the configuration in NVR camera tab and specific Camera web page is different then the video is not displayed.

To configure the Primary and secondary stream settings:

Step 1. In NVR Camera tab, set the Primary Stream for recording that is for high resolution.

Step 2. Set the Secondary stream for Live video streaming that is low resolution.

Note: *Set the Primary stream for recording which is 720p resolution and secondary stream for Live which is 4CIF.*

Step 3. Launch the specific camera web page and then ensure that the same camera parameters are set in web page.

Recommendation to use Low bandwidth stream option

Before enabling the Use Low resolution stream option in MAXPRO VMS you need to perform the following:

Step 1. In MAXPRO NVR Camera tab > Primary/Secondary Stream > Preference, select the Secondary stream from the Low resolution drop down.

Note: *Set the Primary stream for recording which is 720p resolution and secondary stream for Live which is 4CIF.*

Step 2. In MAXPRO VMS > Preferences > Advanced Tab > Low Bandwidth Stream Settings, select the Use Low Resolution Stream check box.

The below table explains the parameter that you can set for Primary and Secondary Streams.

Primary /Main Stream		Secondary /Sub Stream
Codec Format	H.264B	H.264B
Resolution	720 P (1280 x 720)	VGA (640x480)
FPS	12	5
Bit Rate Type	CBR	CBR
Bit Rate	640 - 720	192

Automatic Retry for Backfilled Clips

Perform the steps in the order as mentioned below:

Step 1. Upgrade MAXPRO NVR

Step 2. Configure the Automatic Retry parameter values

Upgrade MAXPRO NVR

MAXPRO NVR 4.9 Build 204:

Upgrade is supported from MAXPRO NVR v4.0 Build 87 Rev H, v4.0 Build 97 Rev B, V4.1 Build 123 Rev B, v4.5 Build 162, MAXPRO NVR v4.7 Build 188 to MAXPRO NVR 4.9 Build 204. This update applies to the MAXPRO Family - Turnkey NVR and NVR Hybrid solutions (XE, SE, PE) and Software only.

Note: *For unsupported lower versions, first upgrade to 4.0 87 Rev H and then apply the NVR v4.9 Build 204 patch.*

Step 1. Install the MAXPRO NVR 4.9 Build 204.

Step 2. Navigate to C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework\bin\ and then access the TrinityBackfillService.exe.config file.

Step 3. In the config file, locate Inside app setting section.

Step 4. Change the value = 1 for <add key="StreamOverTCP" value="0"/> parameter.

⚠ **Caution: If user fails to change the XML value from UDP to TCP then it will cause multiple clips synchronization failure.**

Configure the Automatic Retry parameter values

To configure the Retry parameter details

Step 1. Navigate to C:\Program Files (x86)\Honeywell\MaxproNVR\Trinity-Framework\bin\ and then access the TrinityBackfillService.exe.config file.

Step 2. In the config file, locate Inside app setting section and its values as shown below.

- <add key="DownloadRetryCount" value="0"/>
- <add key="FailClip_RetryInterval" value="06:00"/>
- <add key="FailClip_RetryCount" value="3"/>
- <add key="FailClip_ConfigRefreshInterval" value="1"/>
- <add key="FailClip_StartTimeOnServiceStart" value="00:00"/>
- <add key="NoOfFailedClipsPerBatch" value="10" />
- <add key="ClipDownloadTimeoutMultiplier" value="1.5" />

Step 3. Change the values as mentioned in the below table. The values shown below are default values and user can change based on there requirement.

Parameter Value to change	Description
"DownloadRetryCount" value="0"	Immediate number of consecutive retries for a failed clips.
"FailClip_RetryInterval" value="06:00"	Number of Schedule retries the pooling interval. The default value is set to 6 hours. For every 6 hours once MAXPRO NVR will retry to download the failed clips
"FailClip_RetryCount" value="3"	Number of Schedule retries for automatic retry. The default value is set to 3. For example if the clip is failed, the first retry is attempted after 6 hours consecutively for 3 times.
"FailClip_ConfigRefreshInterval" value="1"	This key helps user to set the configuration change refreshing interval for above auto retry changes. For example: FailClip_RetryInterval value change will be activated after ConfigRefreshInterval time reaches without service restart. The default value is set to 1 second.

Parameter Value to change	Description
"FailClip_StartTimeOnServiceStart" value="00:00"	This key will decide from when the Fail Retry should start after starting the service. This is the reference point to FailClip_RetryInterval" value. Retry operation triggers after StartTimeOnServiceStart value.
"NoOfFailedClipsPerBatch" value="10"	Number of clips to retry with a given camera before attempting the retry on another cameras. Once all the cameras are done with retry then the control comes back to the first camera and fetches the number of clips mentioned for retry.
"ClipDownloadTimeoutMultiplier" value="1.5"	A Multiplier factor to the Maximum Time (actual Clip playback duration or 10min, whichever is higher) until that the backfill service waits to Timeout for downloading a clip.

Step 4. Click Close to close the config file.

Enable Recording During On Demand Streaming

This feature helps user to enable recording during on demand video streaming. Earlier only live video was supported.

For Event Based recording with ON demand streaming, Continuous Recording Schedule option should be selected as None and Event based recording should be configured as 24/7 with condition that there will not be pre event recording only post event recording exists.

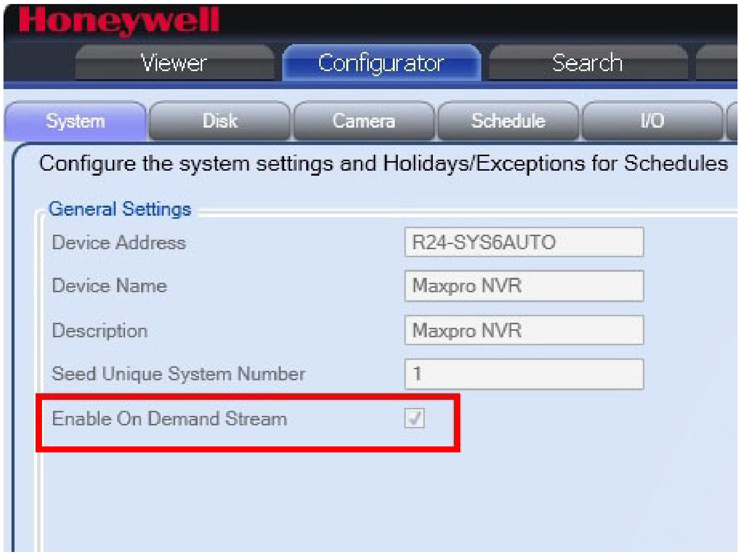
Note: *To set event based On Demand streaming recording, Continuous Recording Schedule option should be selected as None and Event based recording should be configured as 24/7, However, there will not be pre event recording only post event recording exists.*

User should associate alarms to the required camera(s), prior enabling On Demand stream option.

Step 1. Log on to MAXPRO NVR.

Step 2. Navigate to Configurator > System tab.

Step 3. Select Enable On Demand Stream check box as highlighted below.



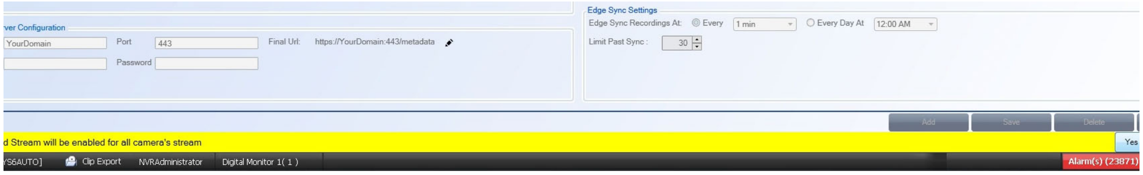
Configure the system settings and Holidays/Exceptions for Schedules

General Settings

Device Address	R24-SYS6AUTO
Device Name	Maxpro NVR
Description	Maxpro NVR
Seed Unique System Number	1
Enable On Demand Stream	☑

Enable On Demand

Step 4. Click Save. A message id displayed as shown below.



ver Configuration

YourDomain Port 443 Final Url: https://YourDomain:443/metadata

Password

Edge Sync Settings

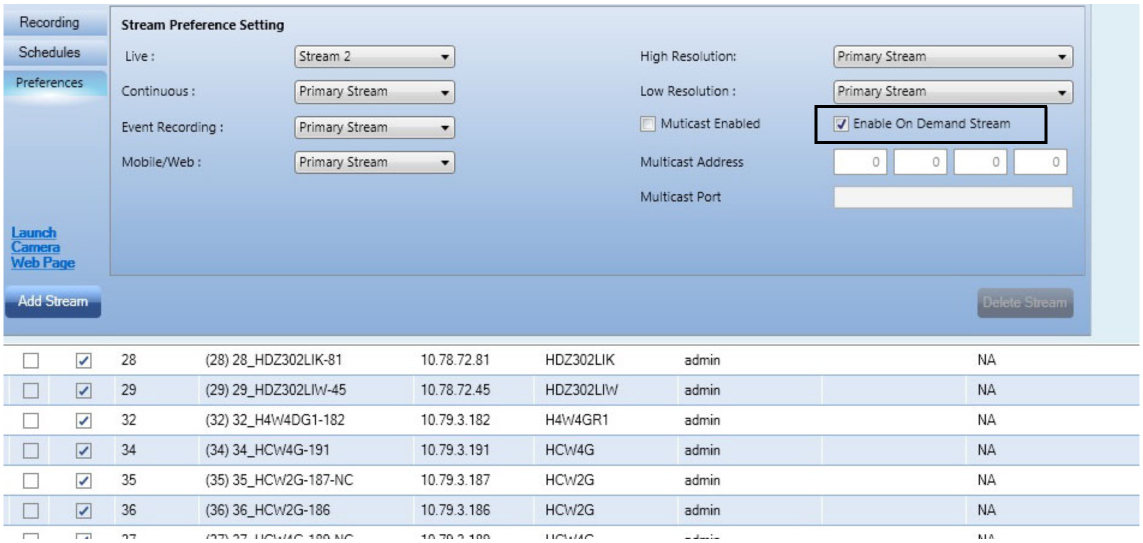
Edge Sync Recordings At: ● Every 1 min ○ Every Day At 12:00 AM

Limit Past Sync : 30

d Stream will be enabled for all camera's stream

YS6AUTO]

Note: *If you enable On Demand Stream feature in Systems tab then it will be enabled for all the camera in NVR. If you want to disable On Demand Stream feature for the required camera then go to required camera settings > Preferences tab and then clear the On Demand Stream check box as shown below. Click Save once done.*



Stream Preference Setting

Live : Stream 2

Continuous : Primary Stream

Event Recording : Primary Stream

Mobile/Web : Primary Stream

High Resolution: Primary Stream

Low Resolution : Primary Stream

□ Muticast Enabled

☑ Enable On Demand Stream

Multicast Address 0 0 0 0

Multicast Port

□	☑	28	(28) 28_HDZ302LIK-81	10.78.72.81	HDZ302LIK	admin		NA
□	☑	29	(29) 29_HDZ302LIW-45	10.78.72.45	HDZ302LIW	admin		NA
□	☑	32	(32) 32_H4W4DG1-182	10.79.3.182	H4W4GR1	admin		NA
□	☑	34	(34) 34_HCW4G-191	10.79.3.191	HCW4G	admin		NA
□	☑	35	(35) 35_HCW2G-187-NC	10.79.3.187	HCW2G	admin		NA
□	☑	36	(36) 36_HCW2G-186	10.79.3.186	HCW2G	admin		NA

Privacy Protection Settings (GDPR Favored)

Anonymization

Anonymization feature is to help the business owner to meet the EU GDPR compliance standards easily. The objective of this feature is to hide the identifiable personal data or personal identity in a video surveillance system using masking techniques. You can even configure the masking type based on the scene environment. This feature is specific to European union region and valid license is required to enable this feature. Only an Administrator can use this feature and grant access in User tab. EquIP Series cameras are supported for this feature. To mask the identifiable objects based on the scene environment, see How to Anonymize objects based on Environment section on page 240 for more information.

The following Camera association and type of masking is supported:

- Blur
- Pixelize

Four Eye Authentication

This feature is also part of Privacy Protection setting and to meet the EU GDPR compliance standards easily. This feature is to restrict all users in a surveillance system to perform Playback operation. While performing playback operation at least two people from different roles should authenticate. For an Administrator, user authentication is not required and can do any playback operation.

For an operator user, a popup is displayed and an Administrator user or any other User with different role needs to authenticate to perform playback operation. By default this option is not selected. User need to obtain valid license to enable this feature.

The following table explains the Four eye authentication based on the user and roles:

User	Authenticating User	Valid Authentication
Operator	Administrator Or any other user with different role	Yes
Operator	Operator	No
Operator	Operator 2	Yes

Clip Export Option

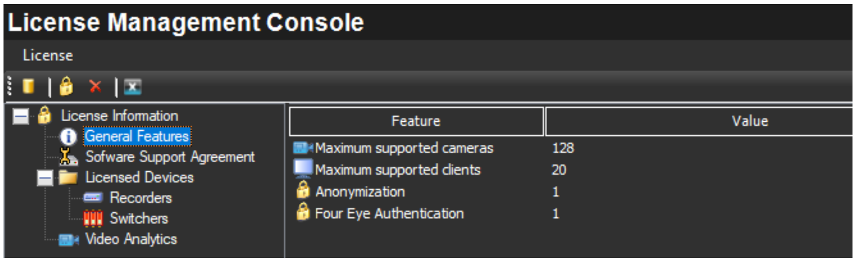
Clip export with Anonymization is supported: Anonymization feature is supported in both Playback and Clip Export operation. Refer *MAXPRO® NVR Operator's Guide* on how to export a clip.

Note: *If a user exports a Anonymized clip then only WMV format is supported.*

Licensing

Both Anonymization and Four Eye Authentication (GDPR Favored) features are license based. Contact Honeywell Tech support, see the back cover for contact information.

Once the license is enabled the entries for both the features are displayed in License Management Console > Privileges screen as shown below.



Feature	Value
Maximum supported cameras	128
Maximum supported clients	20
Anonymization	1
Four Eye Authentication	1

License Privacy protection Settings

How to enable Anonymization

Note: *To mask the identifiable objects based on the scene environment, see* How to Anonymize objects based on Environment *section on page* 240 *for more information.*

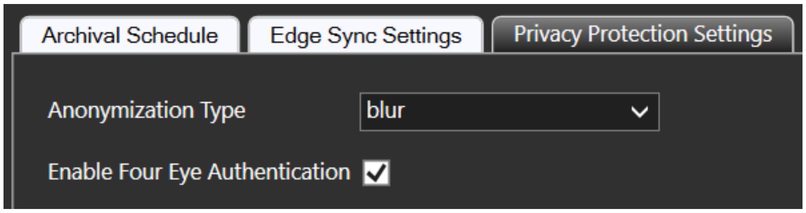
At System Level

Note: *Only Administrator can use this feature and provide access to an operator.*

Step 1. In Configurator > System tab, navigate to Privacy Protection Setting tab.

Step 2. From the Anonymization type drop down, select the masking type. The available options are:

- Blur: Blurs the Identifiable object
- Pixelize: Pixelizes the Identifiable object



Anonymization Type: blur

Enable Four Eye Authentication ☑

Privacy protection Settings

At Camera Level

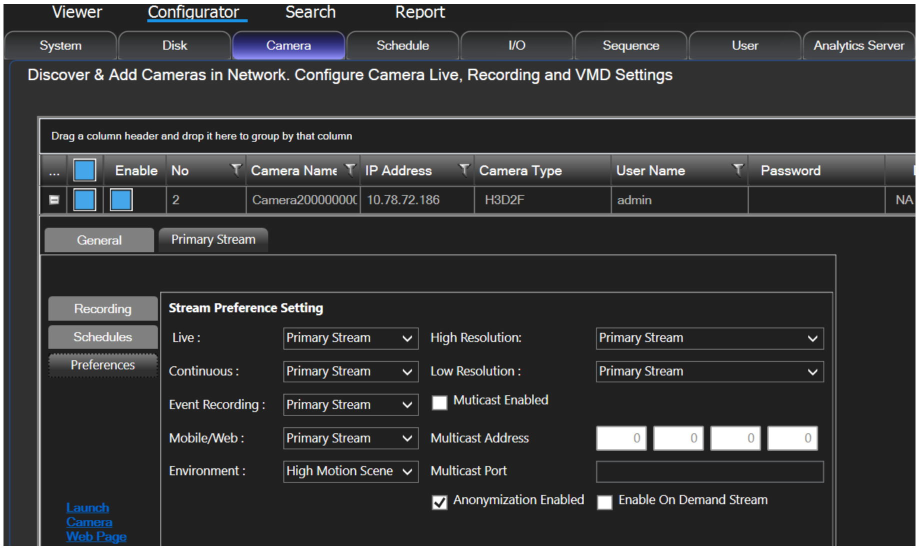
At camera level user can enable or disable the Anonymization based on the requirement.

Step 1. In Configurator > Camera tab, navigate to the camera properties for the specific camera.

Step 2. Under Primary Stream > Preference tab, select the Anonymization Enabled check box as shown below. By default it is not selected.

Step 3. Environment: Select the preferred Environment option to anonymize the live video scene based on the scene environment.The available options are:

- Variable Scene: If the scene contains both stationary and moving people or objects then select this option to anonymize the objects in the scene.
- High Motion Scene: To anonymize the objects in high motion in the scene.
- Still Scene: To anonymize the objects in a scene where the scene predominantly contains stationary people and objects.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...		Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	
⊟	■	■	2	Camera20000000(	10.78.72.186	H3D2F	admin		NA

Stream Preference Setting

Live :	Primary Stream	High Resolution:	Primary Stream
Continuous :	Primary Stream	Low Resolution :	Primary Stream
Event Recording :	Primary Stream	□ Muticast Enabled	
Mobile/Web :	Primary Stream	Multicast Address	0 . 0 . 0 . 0
Environment :	High Motion Scene	Multicast Port	
		☑ Anonymization Enabled	□ Enable On Demand Stream

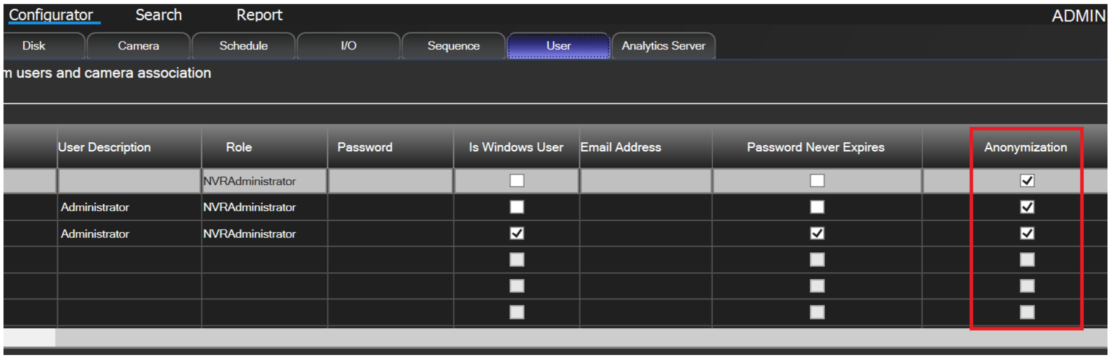
Anonymization Camera Level

At User level

An Administrator can enable Anonymization for a specific user in Users tab. The corresponding user will be able to view only anonymized video.

Step 1. Navigate to Configurator > User tab.

Step 2. For the required User, select the Anonymization check box as shown below. By default it is Enabled for all the operators.



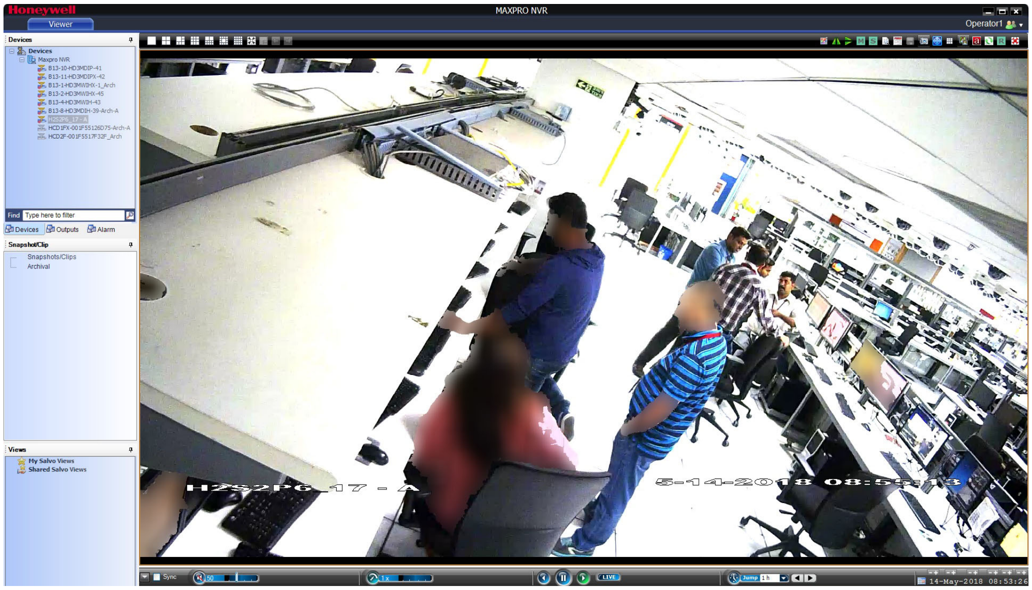
	User Description	Role	Password	Is Windows User	Email Address	Password Never Expires	Anonymization
		NVRAdministrator		□		□	☑
	Administrator	NVRAdministrator		□		□	☑
	Administrator	NVRAdministrator		☑		☑	☑
				□		□	□
				□		□	□
				□		□	□

Anonymization at User level

How to view Anonymized video

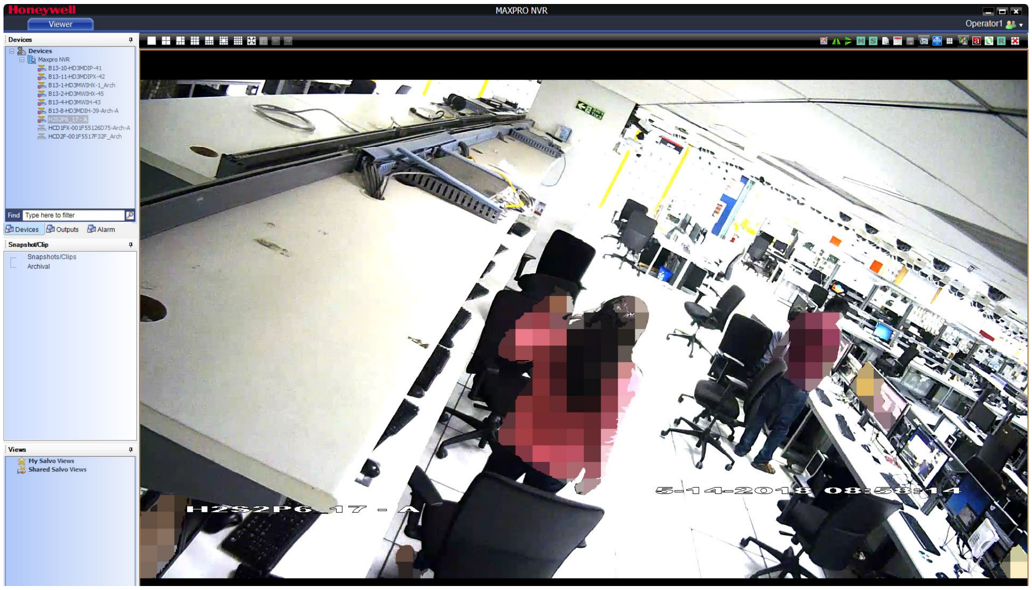
- An Administrator should have grant permission to an operator to view the Anonymized video.
- After selecting the type of Anonymization from the drop down, drag and drop the required camera on to the video panel. Following images displays the types of anonymization.

For Blur



Blur View

For Pixelize



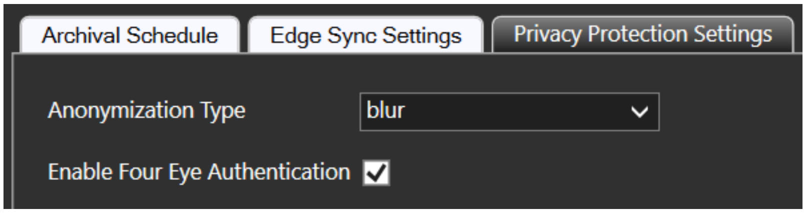
Pixelize Views

How to enable Four Eye Authentication

Step 1. Under Configurator > System tab, navigate to Privacy Protection Setting tab.

Step 2. Select the Enable Four Eye Authentication check box as show below.

Note: *Once this option is enabled it will be applicable to entire NVR system. By default this check box is not selected. User need to obtain valid license to enable this feature.*



Anonymization Type: blur

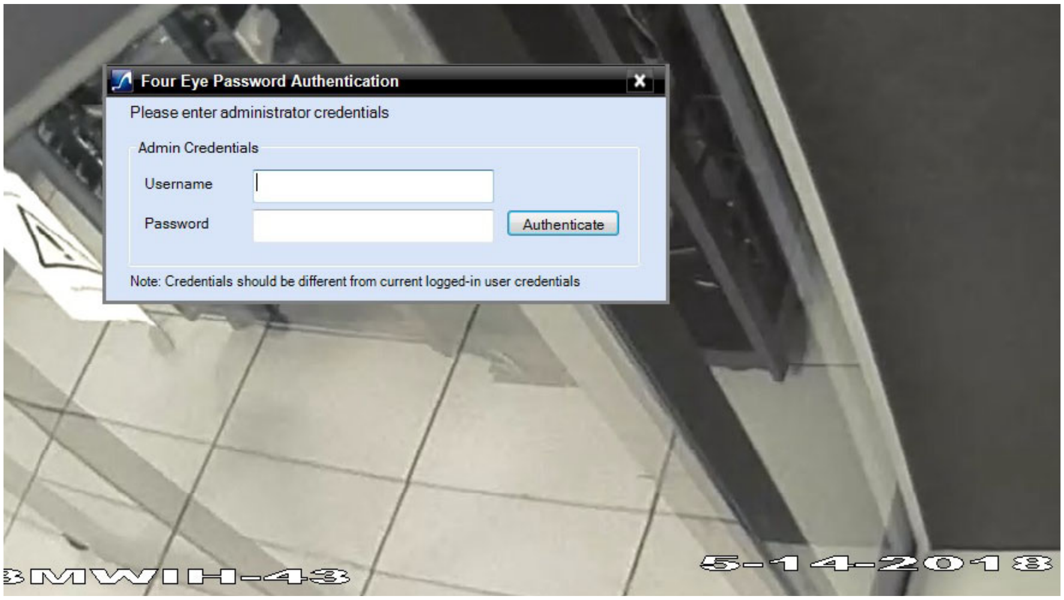
Enable Four Eye Authentication ☑

Enable Four Eye

How Four Eye Authentication feature Works

For an Non Administrator user

Step 1. When an Non Administrator user tries to perform a playback operation then the following dialog box appears on th screen.



Four Eye Password Authentication

Please enter administrator credentials

Admin Credentials

Username

Password

Note: Credentials should be different from current logged-in user credentials

Four Eye Authentication

Step 2. Enter the credentials of Administrator user or a User from different role.

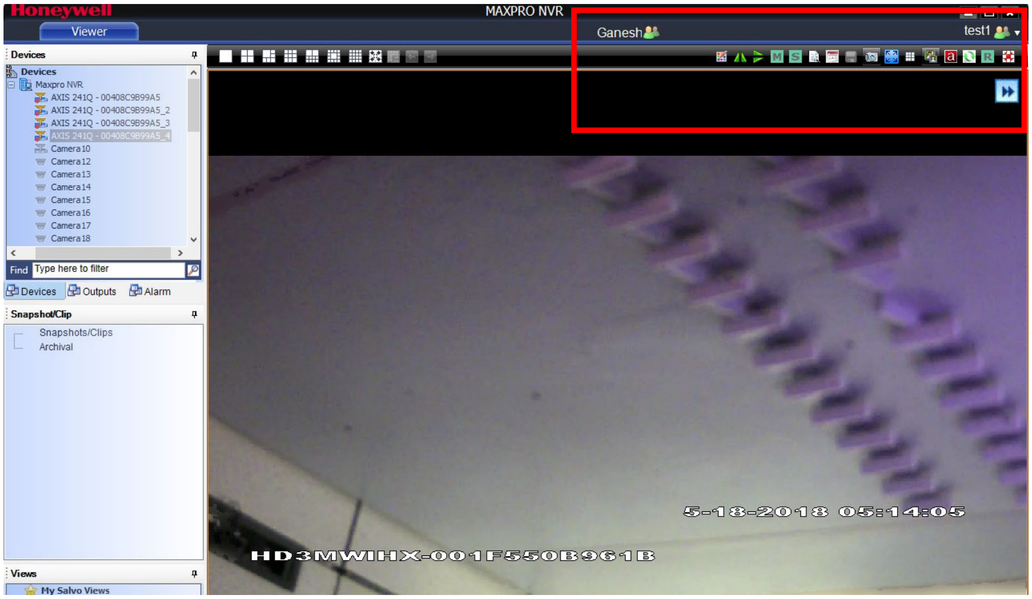
Note: *For authentication, the logged in user and the Administrator user should not be of same role.*

The following table explains the Four eye authentication based on the user and roles

User	Authenticating User	Valid Authentication
Operator	Administrator Or any other user with different role	Yes
Operator	Operator	No
Operator	Operator 2	Yes

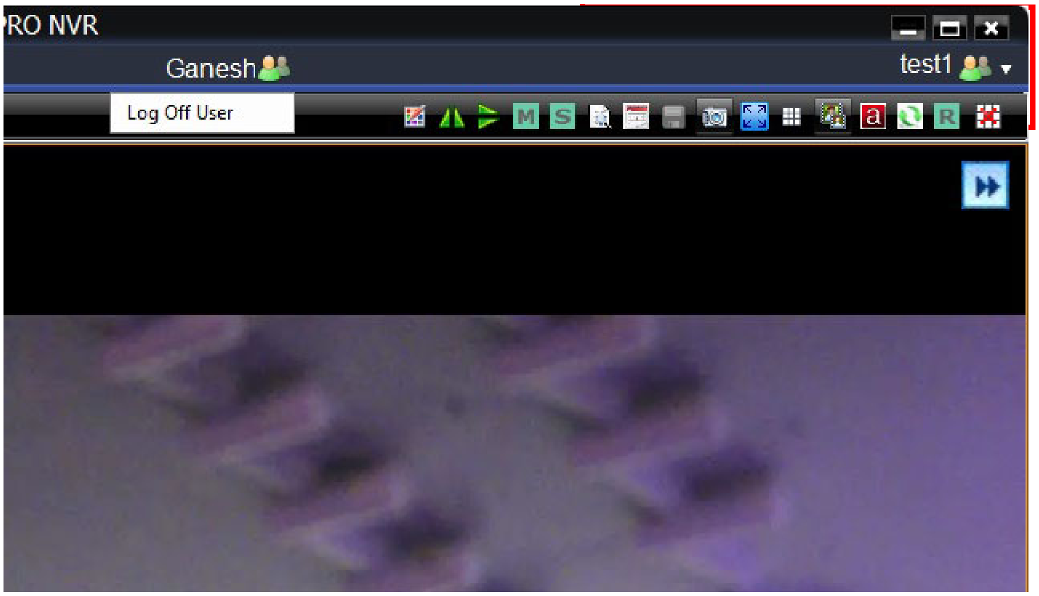
Step 3. Click the Authenticate button to view the playback video. After authentication the Four eye authenticated user and logged in user icons are displayed on the top of the screen as highlighted below. For example: In the below image for a test1 user, an administrator authenticates and the corresponding users are created.

- Until the four eye authenticated user is logged in, the operator can perform any playback operation.



Four Eye Authentication Success

- If the four eye authenticated user logs off as highlighted below then again for any playback operation the Admin authentication is required.



Authenticating User

Video Anonymization

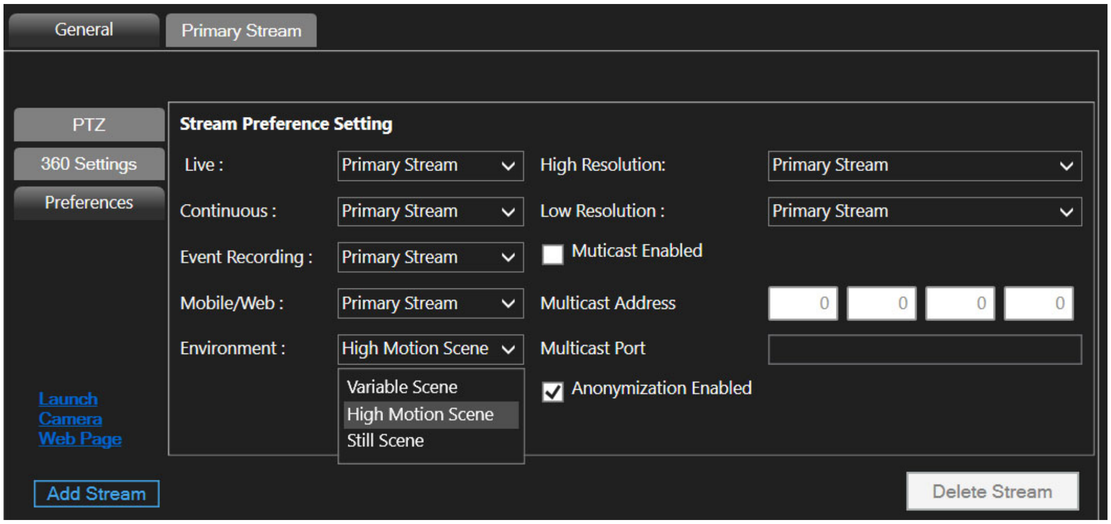
This feature allows user to configure or mask identifiable objects based on the scene environment. It provides flexibility to choose and configure the required camera based on the mounting position. The following are the options supported.

- Variable Scene: If the scene contains both stationary and moving people or objects then select this option to anonymize the objects in the scene.
- High Motion Scene: To anonymize the objects in high motion in the scene.
- Still Scene: To anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

How to Anonymize objects based on Environment

Step 1. For the required camera, click on the left corner to open the camera properties pane.

Step 2. Click General > Preference > Stream Preference Settings as shown below.



Stream Preference Setting

Live : Primary Stream

Continuous : Primary Stream

Event Recording : Primary Stream

Mobile/Web : Primary Stream

Environment : High Motion Scene

High Resolution: Primary Stream

Low Resolution : Primary Stream

☐ Muticast Enabled

Multicast Address 0 0 0 0

Multicast Port

☑ Anonymization Enabled

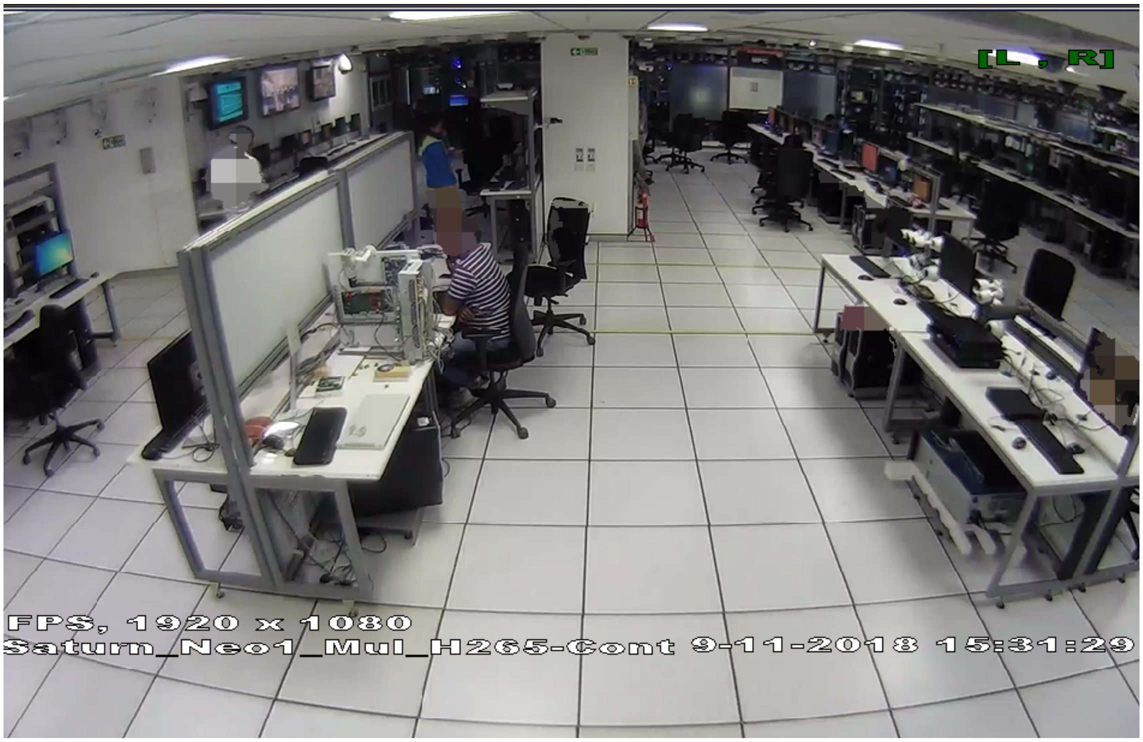
Step 3. Under Environment, select the preferred option. The available options are:

Options	Description
Variable Scene	Select this option if the scene contains both stationary and moving people or objects.
High Motion Scene	Select if you want to anonymize the objects in high motion scene
Still Scene	Select to anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

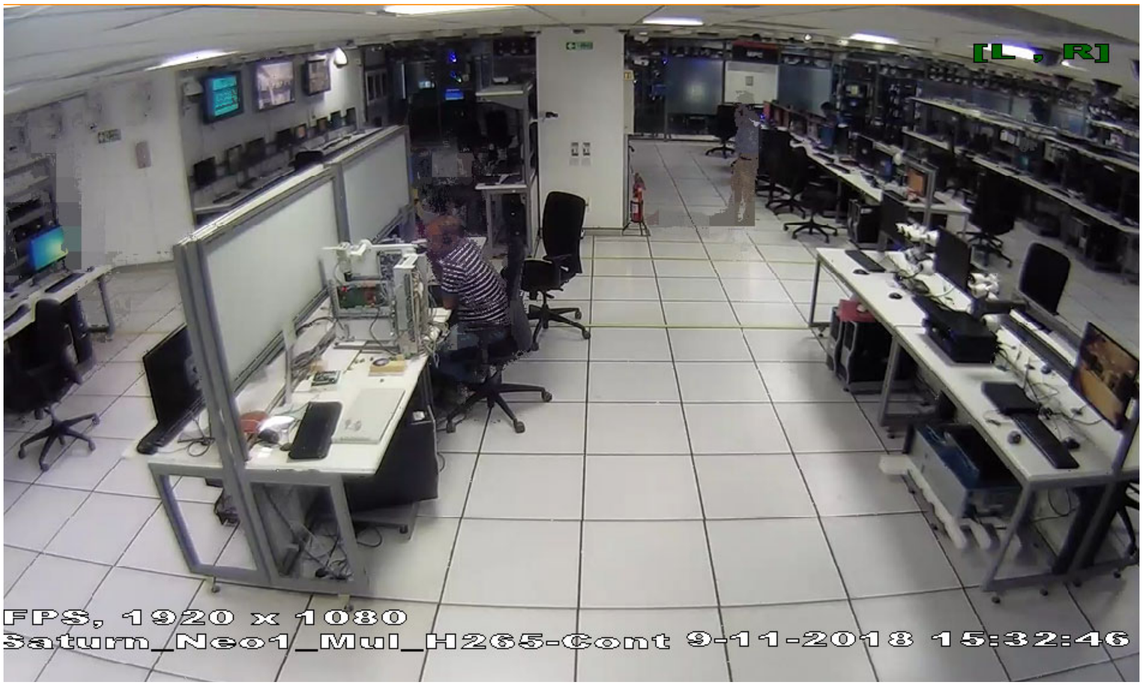
Step 4. Click Save.

Following images display the type of video anonymization scenes based on the environment selection in NVR.

For Variable Scene



For High Motion Scene



For Still Scene

Improved GPU Rendering

GPU Rendering capability is now enhanced to handle the camera video packets along with decompression technique. This helps the system not to depend on CPU for rendering video. User can view smooth and clear live video through GPU rendering. User should modify the registry value in client or server machine to enable GPU rendering mode.

Note: *The following list of camera models/machine will not render in GPU mode:*

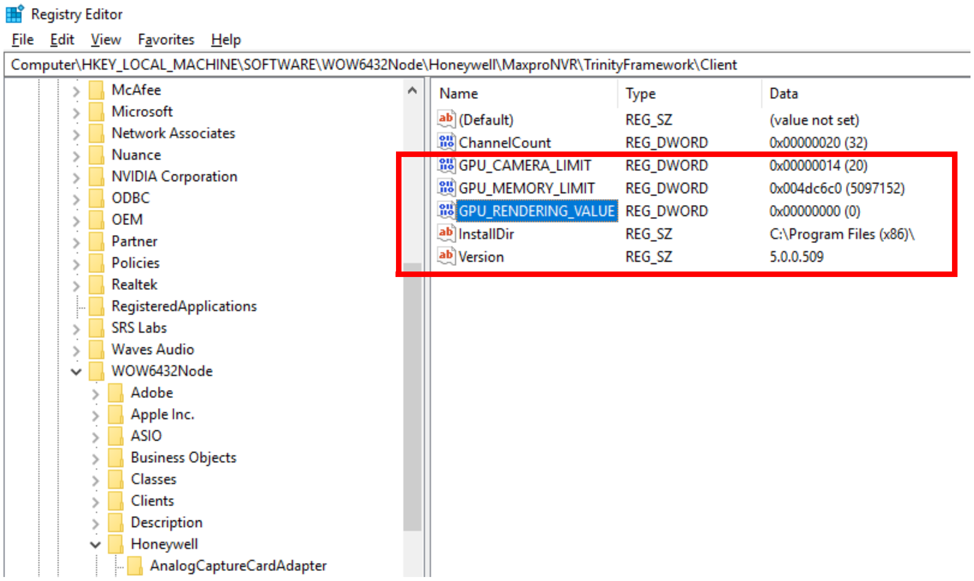
- GrandEye Camera Models
- Dewarping Camera Models
- Anonymizaion enabled cameras
- Analog Cameras
- 32 bit processor rendering client machine

Settings for Rendering Video through GPU

Note: *Ensure that user has enabled the Enable GPU Rendering check box in Preferences > Rendering options tab to render video through GPU.*

Step 1. In a client or server machine, open the Registry Editor.

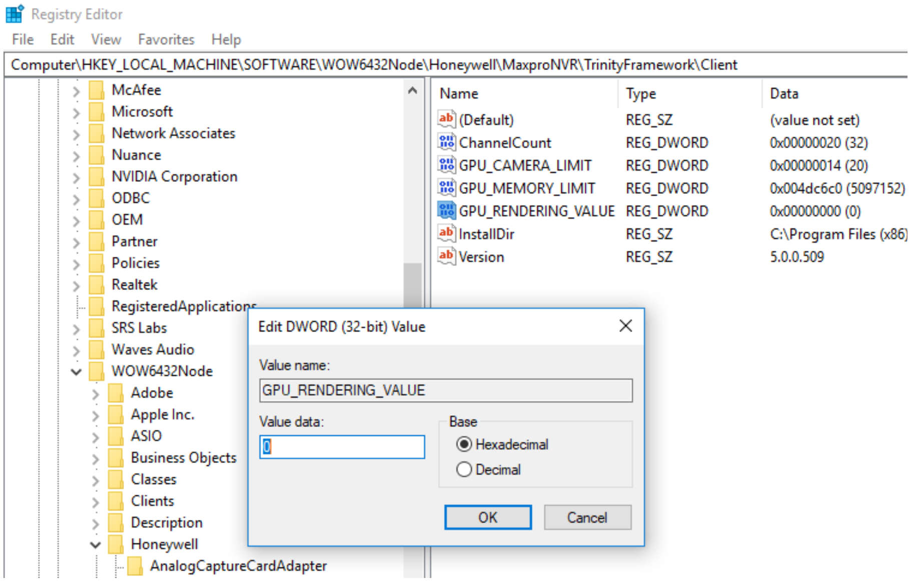
Step 2. Navigate to the path HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\MaxproNVR\TrinityFramework\Client as shown below.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\MaxproNVR\TrinityFramework\Client

Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelCount	REG_DWORD	0x00000020 (32)
GPU_CAMERA_LIMIT	REG_DWORD	0x00000014 (20)
GPU_MEMORY_LIMIT	REG_DWORD	0x004dc6c0 (5097152)
GPU_RENDERING_VALUE	REG_DWORD	0x00000000 (0)
InstallDir	REG_SZ	C:\Program Files (x86)\
Version	REG_SZ	5.0.0.509

Step 3. On the left pane, double-click GPU_RENDERING_VALUE. The Edit DWORD value dialog appears as shown below.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\MaxproNVR\TrinityFramework\Client

Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelCount	REG_DWORD	0x00000020 (32)
GPU_CAMERA_LIMIT	REG_DWORD	0x00000014 (20)
GPU_MEMORY_LIMIT	REG_DWORD	0x004dc6c0 (5097152)
GPU_RENDERING_VALUE	REG_DWORD	0x00000000 (0)
InstallDir	REG_SZ	C:\Program Files (x86)
Version	REG_SZ	5.0.0.509

Edit DWORD (32-bit) Value

Value name: GPU_RENDERING_VALUE

Value data: 0

Base: ● Hexadecimal ○ Decimal

Step 4. Modify the value to 1 in Value data box.

Note: *If the Value data flag is set to 0 then rendering will happen through CPU mode.*

Step 5. Click OK. Drag and drop the cameras required cameras on to the panel to view the improvised GPU rendering mode.

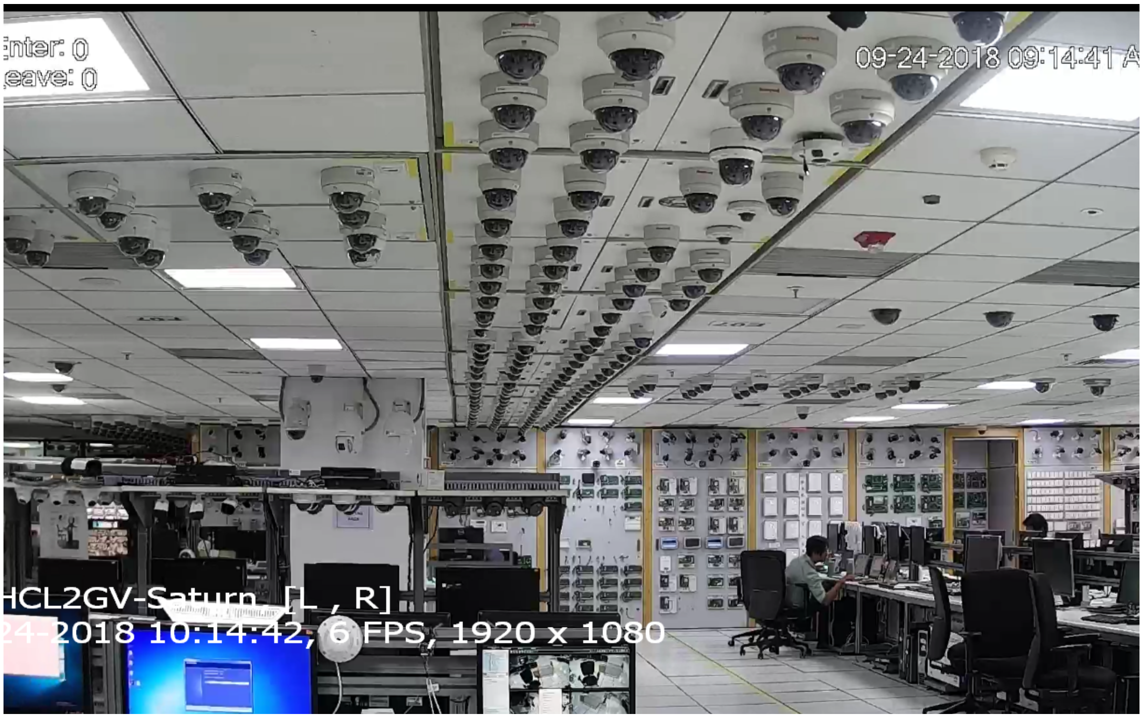
GPU Rendering Combinations

The below table explains the combination settings between Enable GPU Rendering option and Registry settings.

IF	And If	Then
User enables Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 1	Both Decompression and Rendering will be processed through in GPU mode.
User enables Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 0	Decompression process will happen through GPU and Rendering will be processed in CPU mode.
user does not select Enable GPU Rendering check box in Preferences > Rendering options tab	user sets GPU_Rendering_Value flag to 1	Both decompression and Rendering will be processed through CPU.

How to identify if a camera is Rendering in GPU Mode

After Enabling GPU: The font and clarity of live video is displayed as shown below.



Guidelines to configure NAS Drive for Recording

Step 1: Create Directory in NAS

Note: *The steps described below may vary from one NAS to another.*

Step 1. Logon to respective NAS web page

Step 2. Click Settings > Privilege. The Privilege page is displayed.

Step 3. Click Shared Folders > Add. The Add/Edit folder page is displayed.

Step 4. Under General provide the following information for new directory

- Folder Name: Tye the name of folder to store recording
- Description: Type the description if required
- Location: Select the required location to store
- Protocol: Select CIFS/SMB protocol

Step 5. Click the Save button. The new folder directory is created and displayed under shared folder.

Step 2: Map the User details with NVR User

Note: *The steps described below may vary from one NAS to another.*

Step 1. Click Settings > Privilege. The Privilege page is displayed.

Step 2. Click User tab and then Add. The Add User page is displayed.

Step 3. Under Add User Provide the details for the following:

- Username: Provide the same Username of NVR NeoStorageServer
- Password: Provide the same password of NVR NeoStorageServer
- Re-enter the password
- Description: provide the description of the user
- Group: configure the group to which the user belongs to.
- Home Directory: Select the required Home directory
- Password Expiration: set the required password expiration duration.
- Click Quota tab to set the quota details

Step 4. Click OK. The newly created user is displayed under list of users pane.

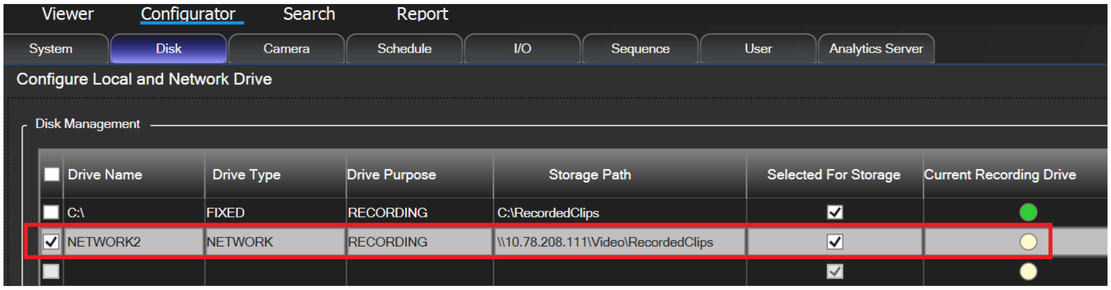
Note: *If customer is using Infotrend NAS then they have to create the user inside the NAS box. The username could be NVR-Admin or Administrator.*

Step 3: Configure the NAS Drive in NVR

Step 1. Click the Configurator tab. The System page displays by default.

Step 2. Click the Disk tab to open the Disk Management page

Step 3. Click Add Drive to add a network drive. A new drive row is added with Network as shown below.



☐	Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For Storage	Current Recording Drive
☐	C:\	FIXED	RECORDING	C:\RecordedClips	☑	●
☑	NETWORK2	NETWORK	RECORDING	\\10.78.208.111\Video\RecordedClips	☑	○
☐					☑	○

Step 4. Under Disk Management, select the following information:

- Drive Name - Select the Network drive.
- Drive Type - Select Network.
- Drive Purpose - Select Recording. By default Recording is selected

Note: *If you select Archival as Drive Purpose then you have to provide the details for NAS Domain, NAS Username and NAS Password. If user adds a Network Drive for Archival without Domain, Username and Password then a validation message is displayed to provide the network credentials.*

Step 5. In Storage Path, add a network drive path in the following format: \\<IP address >\<folder name> For example, \\192.168.1.12\Test.

Step 6. Click the Save button. The Network Drive path will be appended with RecordedClips folder. The complete path is displayed as \\<IP address >\<folder name>\RecordedClips. If the NAS drive is Selected for Storage then the Current Recording Drive turns to Green.

QNAP NAS for Recording

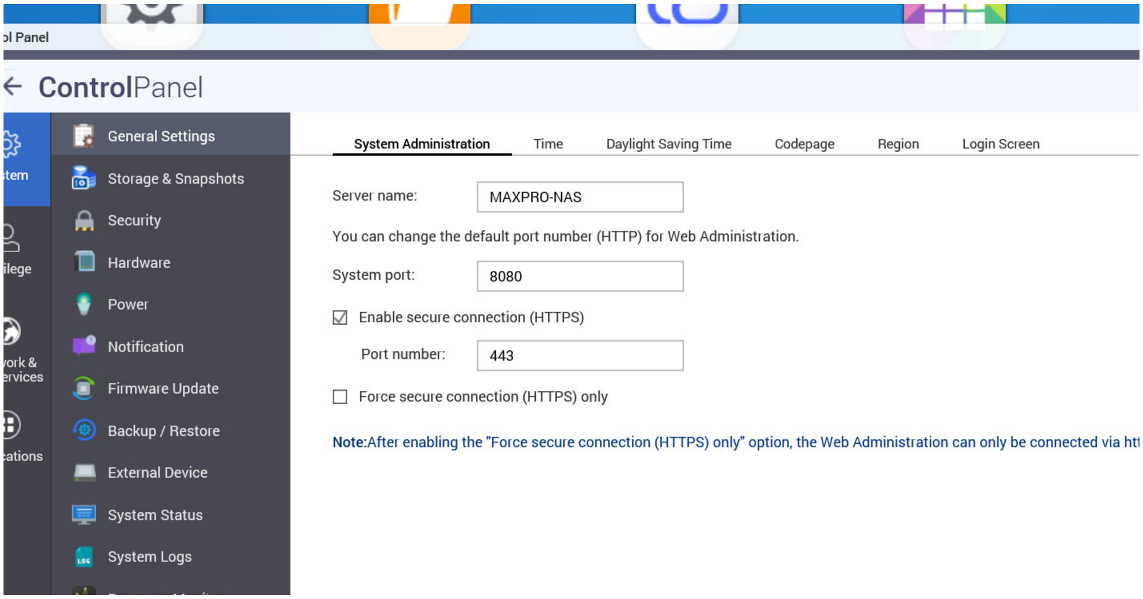
When user configures the QNAP NAS for recording, then recycle function is not happening. QNAP is creating Recycle bin folder in shared folders. The deleted clips are being stored in recycle bin which is available on the same shared folder.

To avoid QNAP creating Recycle bin folder in shared folder user needs to disable the Enable Network Recycle Bin check box option.

To disable Network Recycle Bin option

Step 1. Logon to QNAP NAS web page.

Step 2. Click Control Panel > System. The System page is displayed as shown below.



Server name: MAXPRO-NAS

You can change the default port number (HTTP) for Web Administration.

System port: 8080

☑ Enable secure connection (HTTPS)

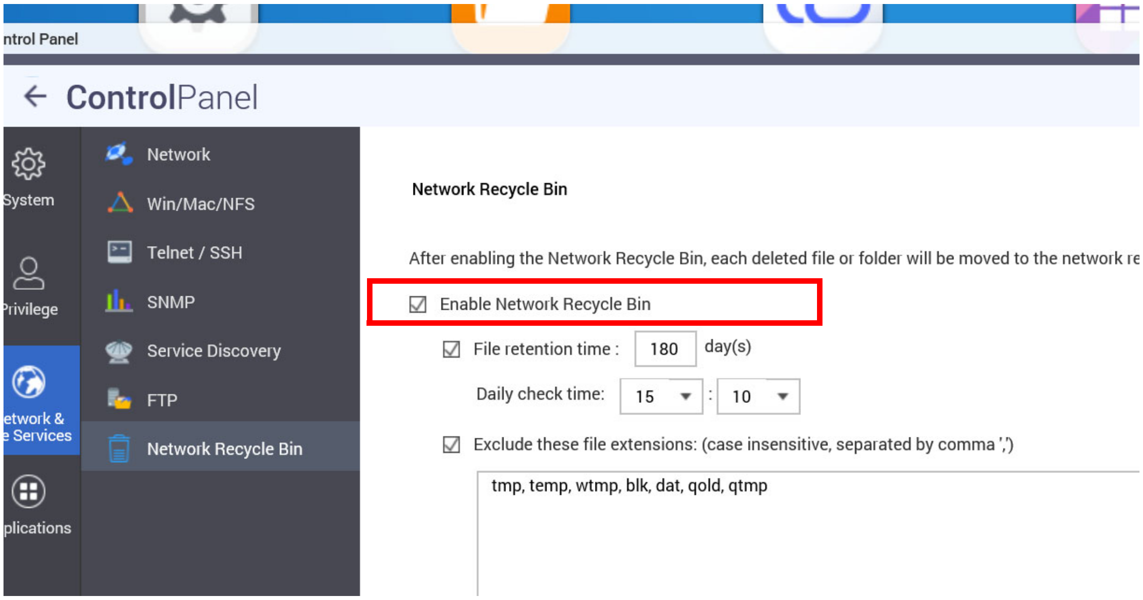
Port number: 443

□ Force secure connection (HTTPS) only

Note:After enabling the "Force secure connection (HTTPS) only" option, the Web Administration can only be connected via htt

Step 3. Navigate to Network & File Services > Network Recycle Bin. The Network Recycle Bin page is displayed.

Step 4. Clear the Enable Network Recycle Bin check box as highlighted below.



Network Recycle Bin

After enabling the Network Recycle Bin, each deleted file or folder will be moved to the network re

☑ Enable Network Recycle Bin

☑ File retention time : 180 day(s)

Daily check time: 15 : 10

☑ Exclude these file extensions: (case insensitive, separated by comma ',')

tmp, temp, wtmp, blk, dat, qold, qtmp

Step 5. Click Apply to save the changes.

Limitations in Configuring NAS for recording

- User should not use “-”, “@” (Hyphen/At the Rate) during the share folder creation
- If user selects the NAS drive for Recording, then in NAS Web page user need to be create user with same credentials as NVR NeoStorageServer services.

For example if NVR service is running with credentials Administrator or NVR-admin then the same user should be created in NAS web page.

- If Neo service is running with “NVRservicesuser” credentials then it is important to have same credentials for NAS User. If different user credentials are created in NAS then recording will not work.
- If user adds multiple directories from same NAS into NVR then the available space will be incorrect (it will add NAS space for every such directory added)
- In Disk management window, after configuring the storage path for NAS drive, the Total Space (GB) columns displays Invalid Drive. For NVR to show the drive details the recording has to switch to the NAS drive.
- If customer is using Infotrend NAS then they have to create the user inside the NAS box. The username could be NVR-Admin or Administrator.

Playing archived clips through Client machine

Pre-requisite

User was unable to access and play the archived clips from NVR server machine. If user drag and drops the archived clips into the viewer then an error message is displayed.

User needs to have the below privileges to access the archived clips from remote NVR clients. Below table details out the possible combinations to play the archived clips from client machine.

- Scenario 1: If user has configured Fixed drive in NVR Server For Archival.

Configured Archival path NVR Server	Then Client should have access to this path	Description
NVR Server (10.78.34.100): D:\archival	\\10.78.34.100\D $\archival	User can access with this admin share only if the logged in user of NVR client is a local administrator in NVR server.

- Scenario 2: If user has configured shared path in NVR Server for archival then user need to configure the Archival drive as UNC path.

Configured Archival path NVR Server	Then Client should have access to this path (Read Only access)
NVR Server \\10.78.34.100\archival	\\10.78.34.100\archival

How to achieve the above Scenario 2 in Domain Environment

- NVR Server and NVR client should be added to the same domain environment

Refer the Windows specific documentation on how to configure the NVR Server and NVR client to the same domain controller.

- Add two user in the Domain Controller as mentioned below
- Add one Domain user as the Local Administrator in NVR Server
- Add another Domain user as a local Administrator in NVR Client (Check whether it is only local administrator or less privileges access)

How to achieve Scenario 2 in Work group

- Scenario 3: If user using NAS drive

If NVR Server Path (using NAS as archival location):	The Client path to access
\\10.78.34.200\NVR_A_ARCHIVAL	\\10.78.34.200\NVR_A_ARCHIVAL

- Scenario 4: If user using SAN then client can be accessed as mentioned in Scenario 1 above.

Different Scenarios to playback Archived Clip

Clip does not exist or you do not have the permission to view it” message is displayed if user drag and drop a archived clip on a salvo. This is because of the client machine has no access to the Archived shared path. Access permission to Archival shared drive should be granted to client machine also.

Below table explains various scenarios in which the archived clip is playable. User needs to perform suitable scenario settings to avoid the error message and playback the clip.

If NVR Server Credentials	then NVR Client Credentials	If Shared Drive Credentials are	If Drive Type is	Playback Supported	Workaround if Playback Fails
Administrator, Password1	Administrator, Password1	NA	Fixed	Yes	None
Administrator, Password1	Administrator, Password2	NA	Fixed	No	None

If NVR Server Credentials	then NVR Client Credentials	If Shared Drive Credentials are	If Drive Type is	Playback Supported	Workaround if Playback Fails
Administrator, Password1	NVR-admin, Password1	NA	Fixed	No	**Workaround for Client** - In fixed path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	MaxproNVR, Password1	NA	Fixed	No	**Workaround for Client** - In fixed path, machine need to create the Client user name with same password and provide (Read) permission for the drive or folder.
Administrator, Password1	Administrator, Password1	Administrator, Password1	Shared	Yes	NA
Administrator, Password1	Administrator, Password1	NVR-admin, Password1	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	NVR-admin, Password1	Administrator, Password1	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	NVR-admin, Password1	NVR-admin, Password1	Shared	Yes	In server machine it will not stream
NVR-admin, Password1	Administrator, Password1	NVR-admin, Password1	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	Administrator, Password2	Administrator, Password2	Shared	Yes	None
Administrator, Password2	Administrator, Password2	Administrator, Password1	Shared	No	None

If NVR Server Credentials	then NVR Client Credentials	If Shared Drive Credentials are	If Drive Type is	Playback Supported	Workaround if Playback Fails
Administrator, Password1	Administrator, Password2	NVR-admin, Password1	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	NVR-admin, Password1	Administrator ,Password2	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
Administrator, Password1	NVR-admin,Password1	NVR-admin, Password2	Shared	Yes	NA
NVR-admin,Password1	Administrator, Password1	Administrator, Password2	Shared	No	None
NVR-admin,Password1	Administrator, Password1	NVR-admin, Password2	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.
NVR-admin,Password1	NVR-admin,Password2	Administrator, Password1	Shared	No	**Workaround for Client** - In Shared path, machine need to create the Client user name with same password and provide (Read) permission for the Archival drive or folder.

How to configure the Archival and Deletion retry settings

Recommendations:

Honeywell recommends before configuring Archival Clip and Deletion Retry settings ensure that the following parameters are set based on the site requirement:

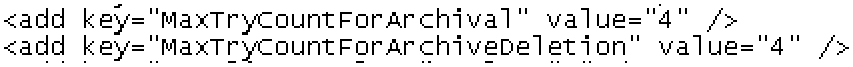
- The default value for DiskAlarmThresholdInGB is 100: This indicates when the available free space in archival location is less than 100 GB then an alarm is triggered.
- The default value for DiskRecyclingInGB is 30: This indicates if the available free space is below 30 GB, then the older archived clips are recycled to create space for the newly archiving clips.
- The default value for DiskSwitchLimitINGB is 5: This indicates if the available free space in the archival location goes less than 5 GB then Low Disk Space

alarm is triggered and the archival process will be attempted to next available archival location if configured.

Step 1. Navigate to C:\Program Files (x86)\Honeywell\MaxproNVR\Trinity-Framework\bin\TrinityArchival.exe.config.

Step 2. Right-click and open with Notepad.

Step 3. Scroll down to locate the below two values and change the count value for each parameter based on the requirement. The default value is 4.



```
<add key="MaxTryCountForArchival" value="4" />
<add key="MaxTryCountForArchiveDeletion" value="4" />
```

- If Value is set to 0 = Indefinite tries
- If Value is set to > than 0 = Indicated the number of attempts to archive or delete the archived clips respectively.

Note: *Archival/Deletion Retry settings will be moved to default count value if user upgrades to future versions of VMS/NVR.*

Annotations

Introduction

Annotation feature helps to trace and locate the moving subjects in live/recorded video and generates an alarm if intrusion or loitering is detected. After this feature is enabled in NVR, subjects in video when found in Region Of Interest, is bounded by rectangle box and on alarm conditions, it will be signified with a change in color of bounding box. This helps the operator to quickly trace the direction of the moving subject.

Equip-S series camera supports Annotation feature along with Intrusion trace and Loitering Trace alarms. These alarms are in-built with Equip-S series camera and are made available by installing required analytics licenses.

Annotation with Intrusion Trace alarm: This feature helps in detecting a subject, if it enters a predefined restricted area. The system will annotate and detects the object with Green rectangular box. If the object is detected in the restricted area then the annotated Green rectangular box turns to Red and an alarm is generated.

Annotation with Loitering Trace alarm: This feature helps in detecting an object If loitering beyond the specified duration of time in a predefined region. The subjects is bounded by the box along with the duration (time in seconds) for which it is identified in the region of interest. If the subject is loitering in the region beyond a predefined time then the annotation boxes turns to Red and an alarm is generated.

Note: *Currently Annotation feature works with only with old GPU rendering modes.*

Annotation feature is supported with the following camera models and firmware version:

S.No	Camera Model	Firmware	Loiter	Intrusion
1	H4D8GR1	2.420.HW00.9, Build Date: 2018-12-17	V1.20.60	V1.20.60
2	HCD8G			
3	HBD8GR1			
4	HFD6GR1	1.000.HW00.9, Build Date: 2018-12-17	V1.20.60	V1.20.60
5	HFD8GR1			
6	HDZ302DE	1.000.0043.3, Build Date: 2019-01-07	V1.20.60	V1.20.60
7	HDZ302D			
8	HDZ302DIN			

Note: *The PTZ Model cameras (HDZ302DE, HDZ302D, HDZ302DIN) after the firmware upgrade will be compatible with MAXPRO NVR T-Patch 532 and above versions.*

How to get/configure Annotation Feature

To get and use the Annotation feature in MAXPRO NVR/VMS, user needs to perform the following configurations in the order as mention below:

1. Upgrade the Camera Firmware
2. Install the VA packages
    c. Remove Old VA Package
    d. Upgrade to Latest VA Package

3. Obtain the License to use Annotation feature

4. Configure and Enable Annotation in NVR

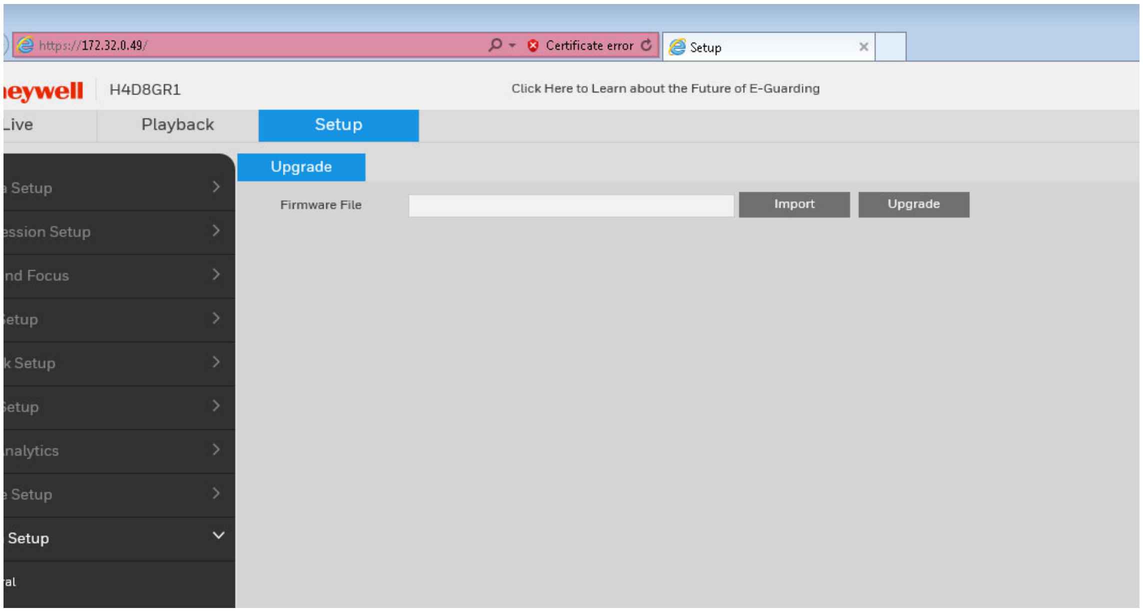
5. Enable Annotations in VMS

Upgrade the Camera Firmware

Step 1. Launch the Equip-S series model camera web page and then click on Setup tab.

Step 2. Check the existing version of Firmware in Information > Version page.

Step 3. In the left pane, navigate to System Setup > Upgrade. The Firmware Upgrade page is displayed as shown below.



Step 4. Click the Import button and then browse the Firmware to import.

Step 5. Click Upgrade. Once the upgrade complete, Firmware Upgrade successful message is displayed.

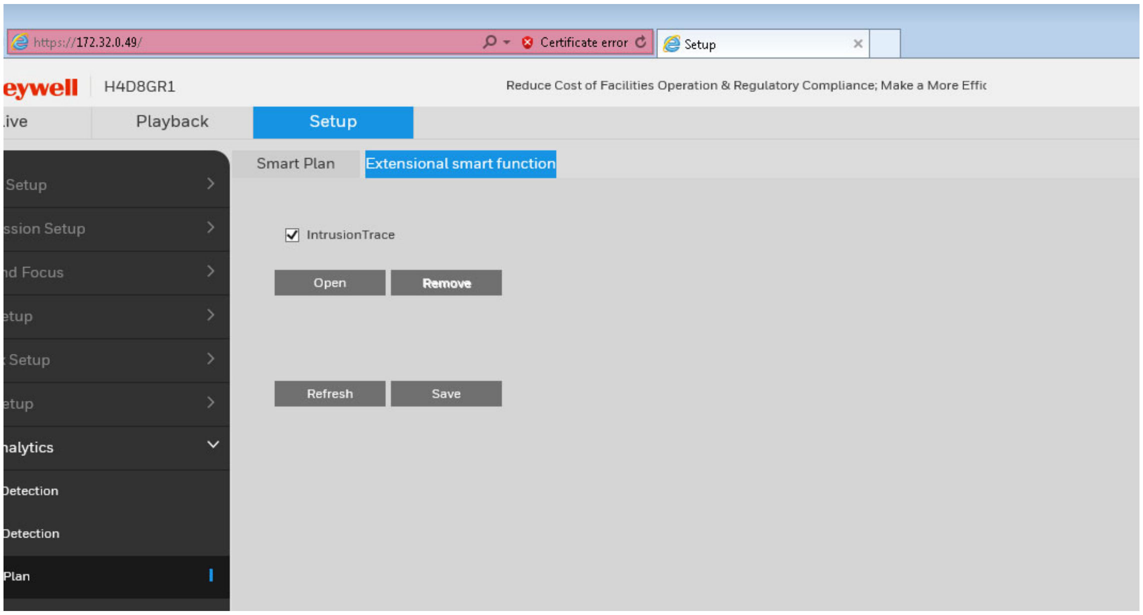
Install the VA packages

Remove Old VA Package

If the existing VA package is old then:

Step 1. Navigate to Video Analytics > Smart Plan. The Smart Plan page is displayed.

Step 2. Click on the Extensional Smart function tab as shown below.



Step 3. Click Remove to remove the old VA package. Clear the alarm check box and then and save. Once it is saved click remove button, otherwise remove button will be in disable state only. Vice versa, it should be selected and saved to open VA Webpage.

Step 4. Repeat the step 1 through step 3 to remove the old VA package of Loitering trace.

Upgrade to Latest VA Packages

Step 1. In th same camera web-page, navigate to System Setup > Upgrade. The Firmware Upgrade page is displayed as shown below.

Step 2. Click the Import button and then browse the latest VA packages (Intrusion trace and Loitering trace) to import.

Step 3. Click Upgrade. Once the upgrade complete, VA package upgrade successful message is displayed.

Enable Extensional Smart Function

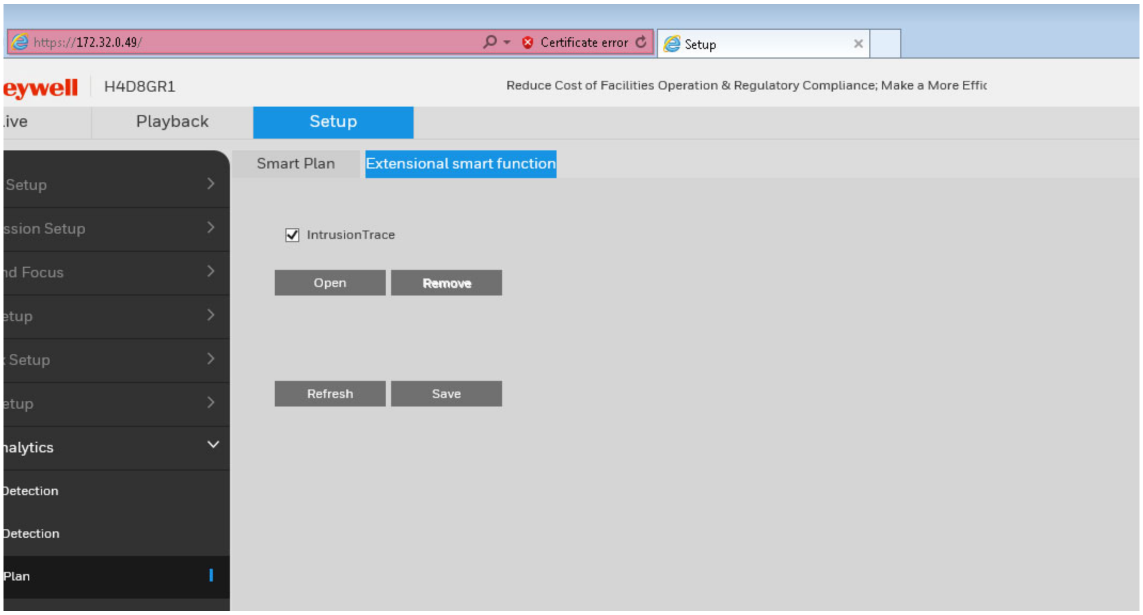
Step 1. Navigate to Video Analytics > Smart Plan. The Smart Plan page is displayed.

Step 2. If the Extensional Smart function is off, click to turn ON to configure and use Annotation feature.

Obtain the License and install

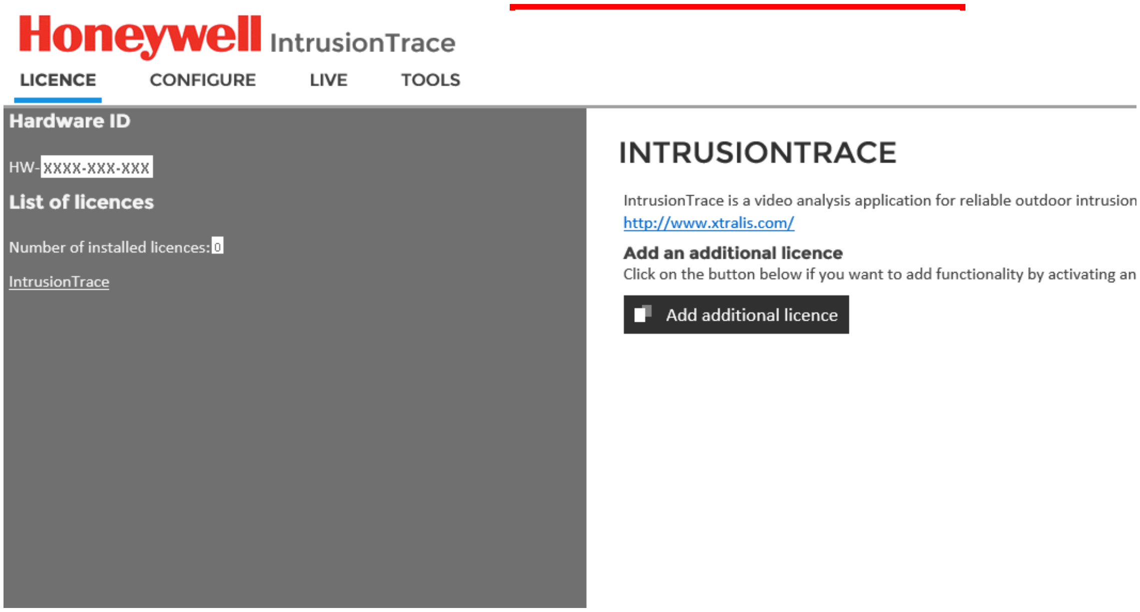
Step 1. Contact Honeywell Technical Support to obtain the license for Intrusion Trace and Loitering Trace features.

Step 2. In the Extensional Smart function page, for a specific feature, click the Open button. For example Intrusion Trace as shown below.



The Honeywell Video Analytics page is displayed.

For Intrusion trace



Hardware ID

HW-XXXX-XXX-XXX

List of licences

Number of installed licences: 0

IntrusionTrace

INTRUSIONTRACE

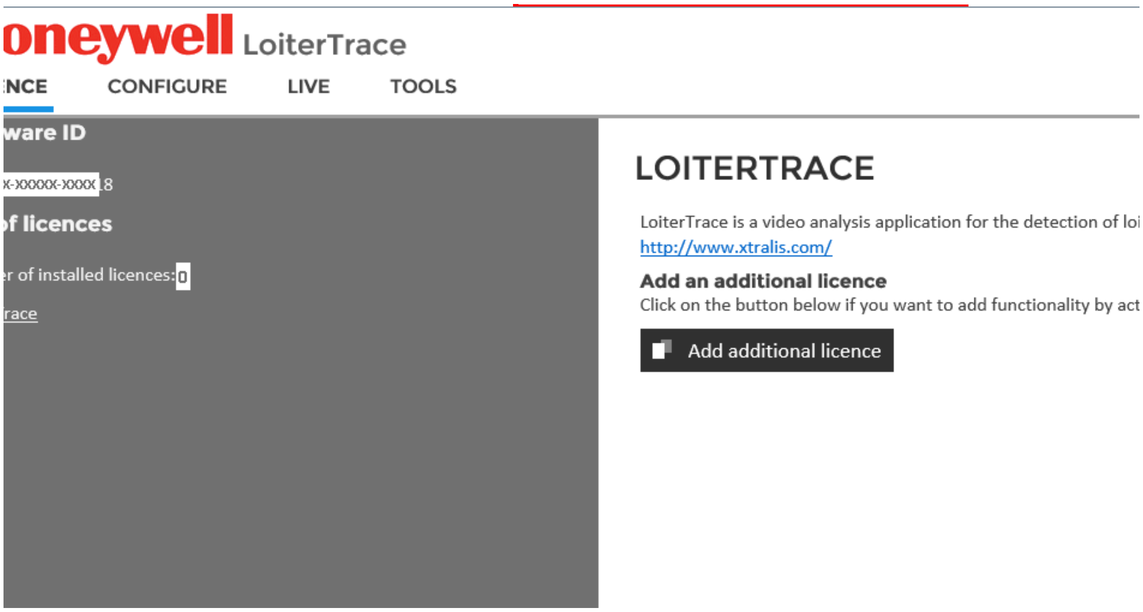
IntrusionTrace is a video analysis application for reliable outdoor intrusion

http://www.xtralis.com/

Add an additional licence

Click on the button below if you want to add functionality by activating an

For Loitering Trace



ware ID

X-XXXXX-XXXX 18

f licences

r of installed licences: 0

race

LOITERTRACE

LoiterTrace is a video analysis application for the detection of loi

http://www.xtralis.com/

Add an additional licence

Click on the button below if you want to add functionality by act

Step 1. Click on Add Additional License button.

Step 2. Enter the license key and then click OK to activate.

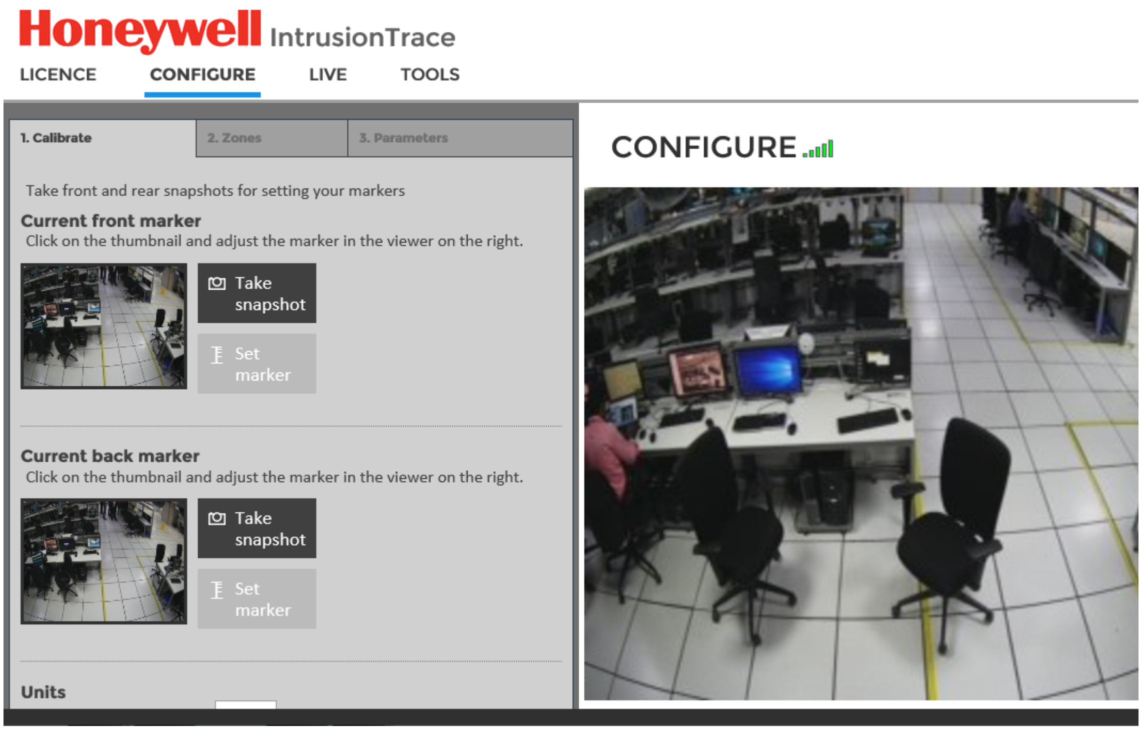
Configuring Intrusion trace

Pre-requisite:

Before you configure the Intrusion trace feature ensure you have:

a. Upgraded the camera firmware.
b. Upgraded the Intrusion trace VA package
c. Obtained and installed the required license

Step 1. Click on the Configure tab, the Configure page is displayed as shown below. By default the Calibrate tab is selected.



Take front and rear snapshots for setting your markers

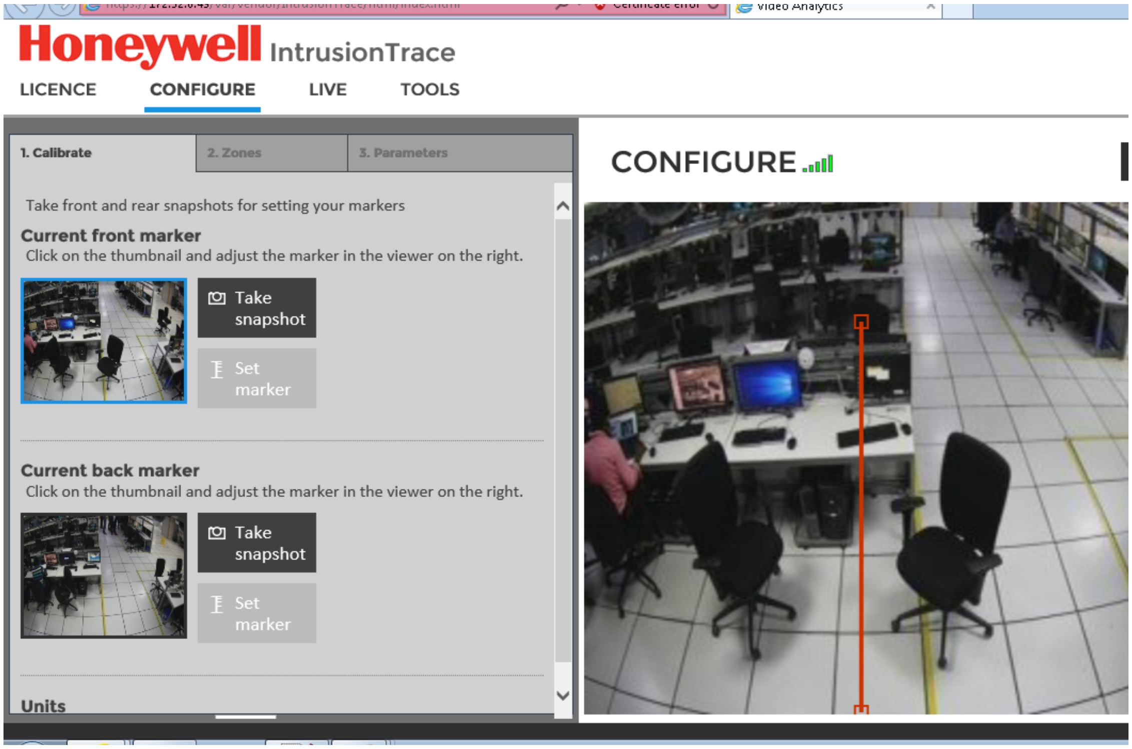
Current front marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Current back marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Step 2. Click on Take Snapshot, read and perform the on screen instructions to adjust the current front marker as shown below.



Take front and rear snapshots for setting your markers

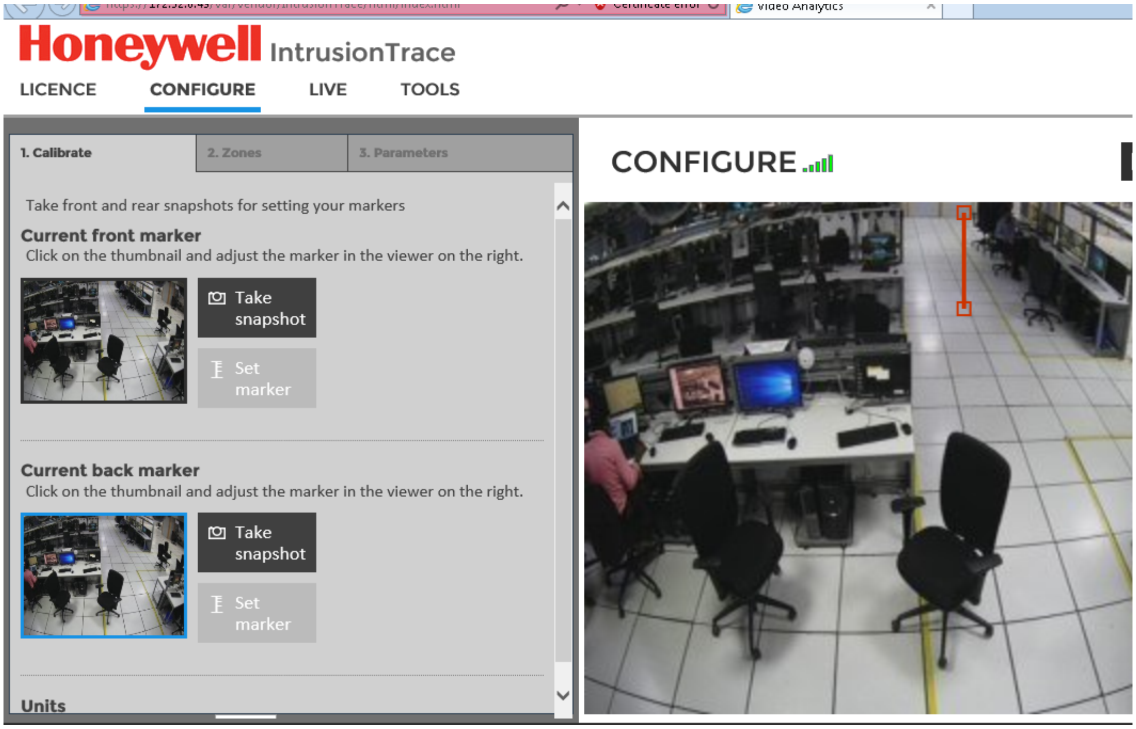
Current front marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Current back marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Step 3. Under Current back marker, click on Take Snapshot, read and perform the on screen instructions to adjust the current back marker as shown below.



Take front and rear snapshots for setting your markers

Current front marker

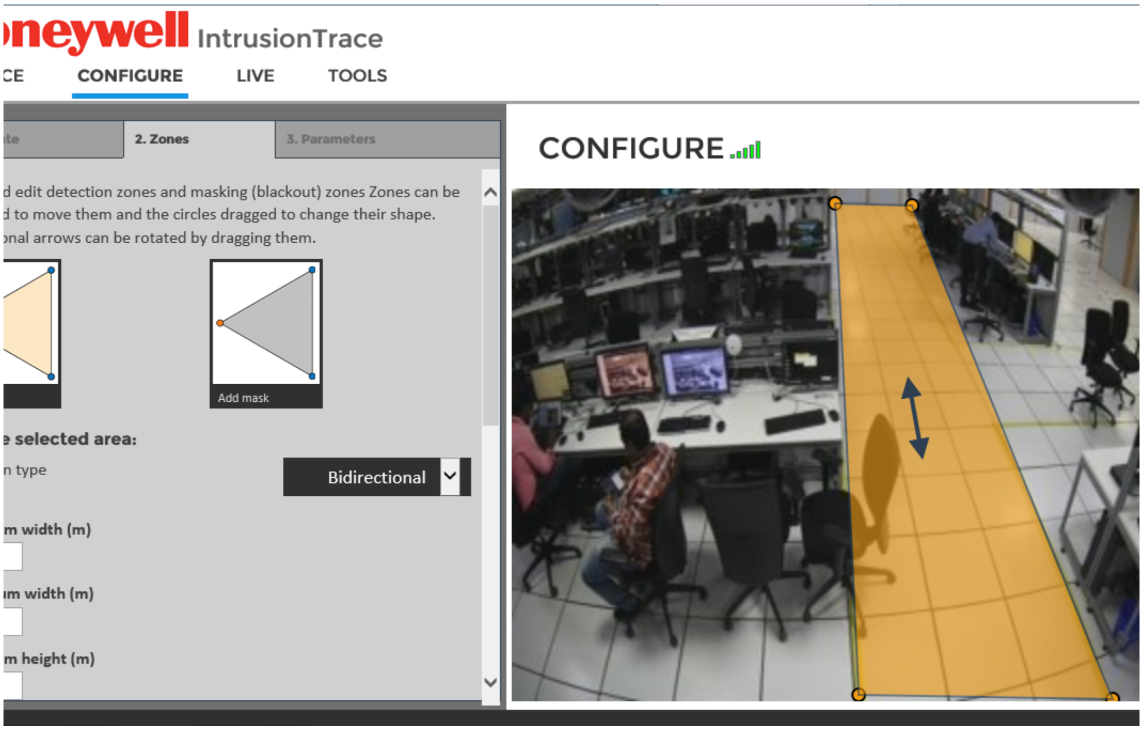
Click on the thumbnail and adjust the marker in the viewer on the right.

Current back marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Step 4. Once done, click Save in the bottom of the page. Data saved successfully message is displayed.

Step 5. Click on Zones and then click on Add area to add define the area for intrusion trace. This will be the area under which an alarm is generated if an object is detected. User can define multiple zones.



d edit detection zones and masking (blackout) zones Zones can be d to move them and the circles dragged to change their shape. onal arrows can be rotated by dragging them.

e selected area:

n type Bidirectional

m width (m)

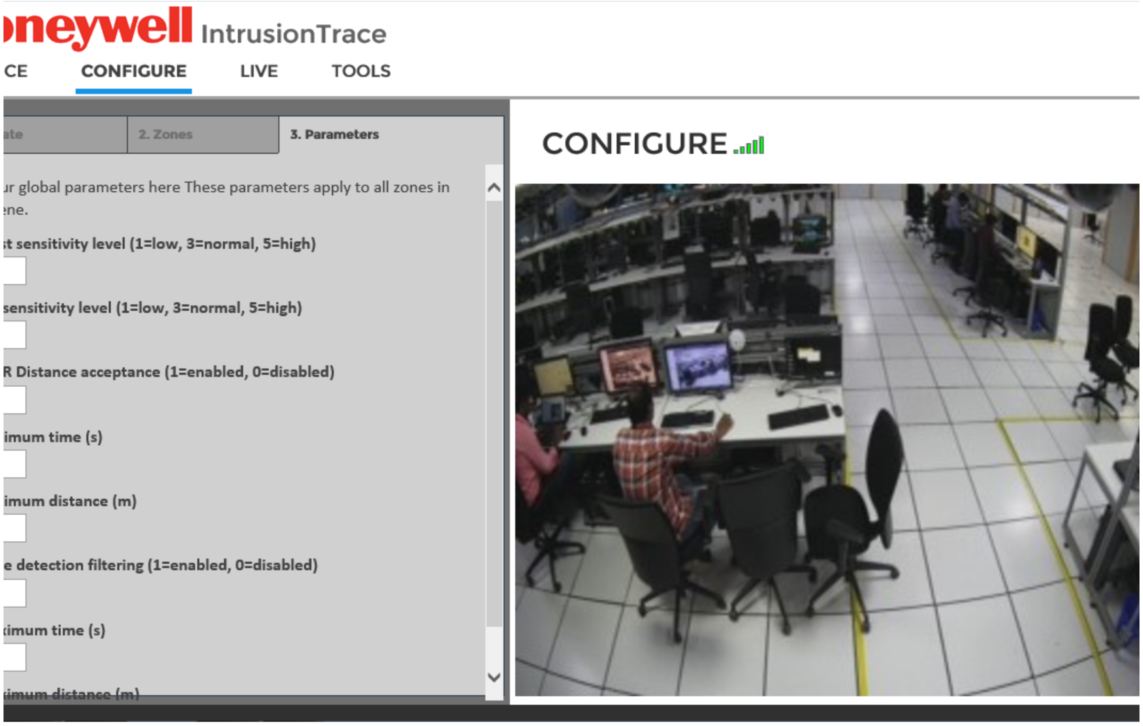
im width (m)

m height (m)

Step 6. Read the on screen instructions and set the parameters for the zone such as Minimum width, Maximum width, Minimum height, Maximum height, Minimum area, Maximum area, Minimum speed, Maximum speed, Time and Distance acceptance, minimum time and minimum distance.

Step 7. Click Save at the bottom of the page. Data Saved successfully message is displayed.

Step 8. Click on Parameters and set the parameter for all the defined zones as shown below.



ur global parameters here These parameters apply to all zones in ne.

t sensitivity level (1=low, 3=normal, 5=high)

sensitivity level (1=low, 3=normal, 5=high)

R Distance acceptance (1=enabled, 0=disabled)

imum time (s)

imum distance (m)

e detection filtering (1=enabled, 0=disabled)

imum time (s)

imum distance (m)

Step 9. Click Save at the bottom of the page. Data Saved successfully message is displayed.

Step 10. Click on the Live tab to view the configured intrusion feature.

Configuring Loitering trace

Pre-requisite:

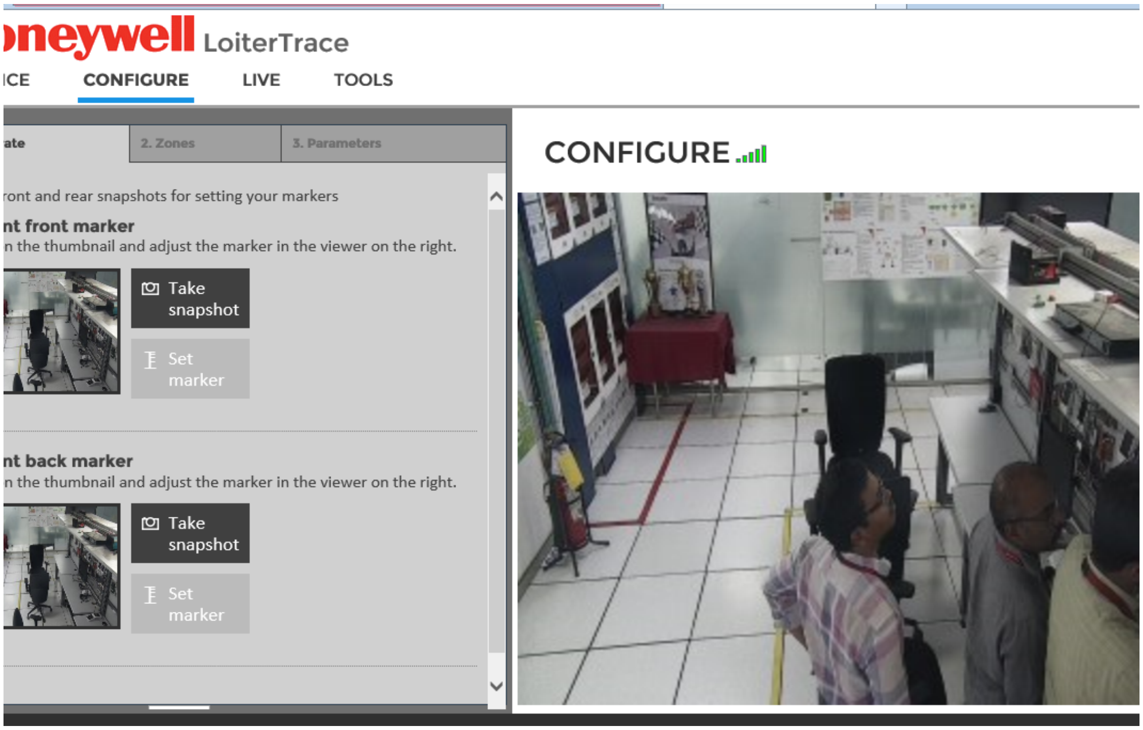
Before you configure the Loitering trace feature ensure you have:

a. Upgraded the camera firmware

b. Upgraded the Loitering trace VA package

c. Obtained and installed the required license.

Step 1. Click on the Configure tab, the Configure page is displayed as shown below. By default the Calibrate tab is selected.



ront and rear snapshots for setting your markers

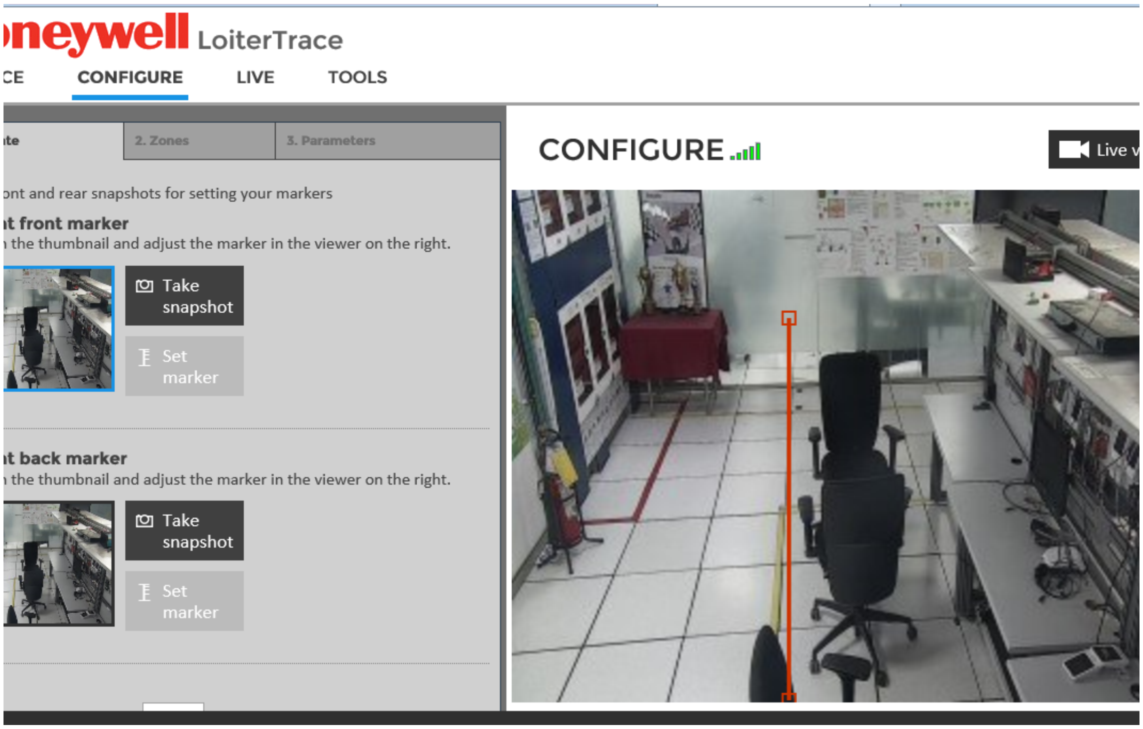
nt front marker

n the thumbnail and adjust the marker in the viewer on the right.

nt back marker

n the thumbnail and adjust the marker in the viewer on the right.

Step 2. Click on Take Snapshot, read and perform the on screen instructions to adjust the current front marker as shown below.



ont and rear snapshots for setting your markers

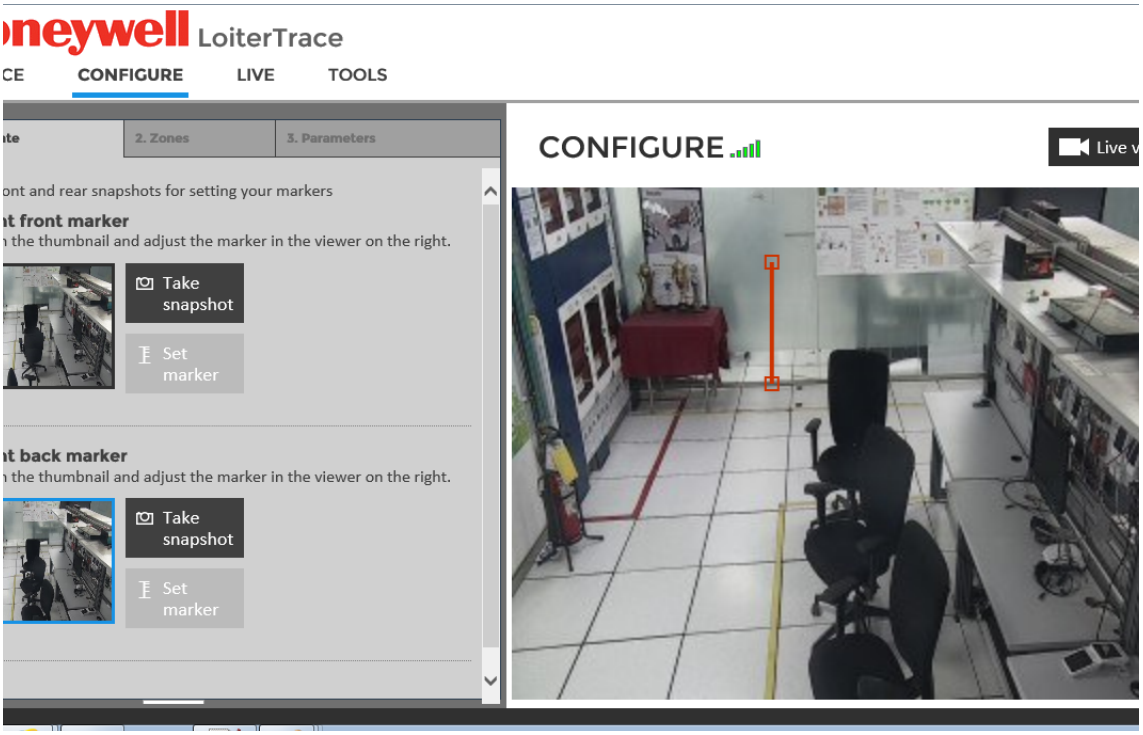
it front marker

i the thumbnail and adjust the marker in the viewer on the right.

it back marker

i the thumbnail and adjust the marker in the viewer on the right.

Step 3. Under Current back marker, click on Take Snapshot, read and perform the on screen instructions to adjust the current back marker as shown below.



ont and rear snapshots for setting your markers

t front marker

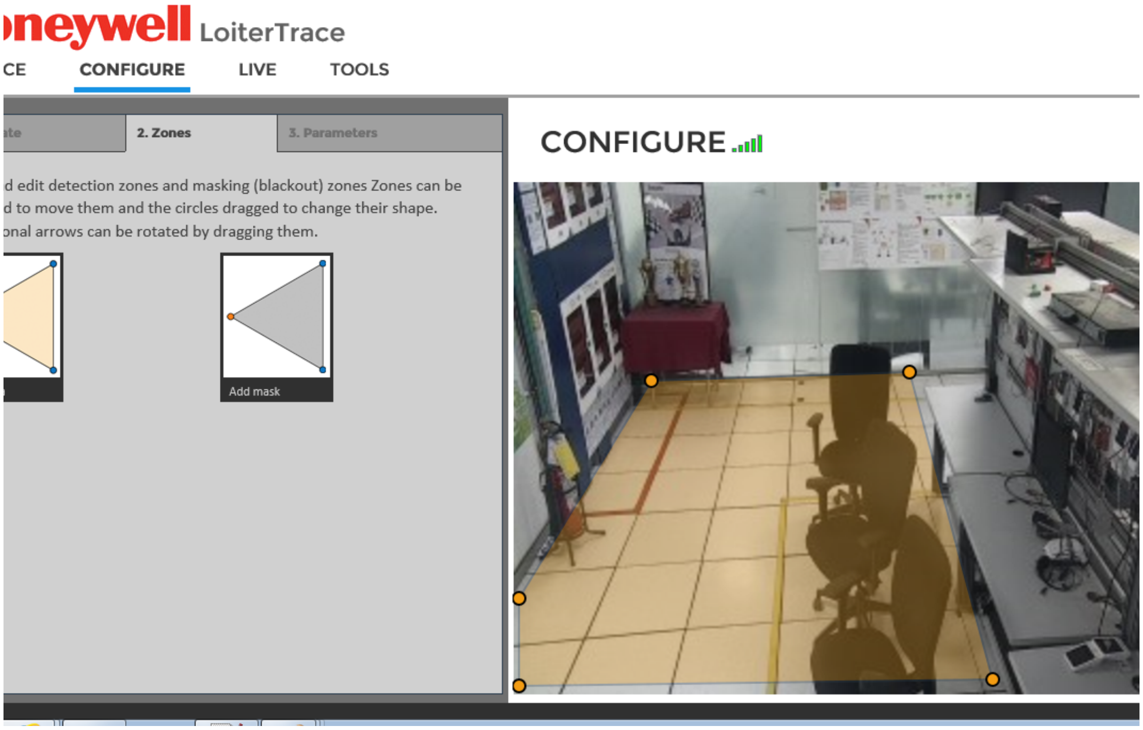
the thumbnail and adjust the marker in the viewer on the right.

t back marker

the thumbnail and adjust the marker in the viewer on the right.

Step 4. Once done, click Save in the bottom of the page. Data saved successfully message is displayed.

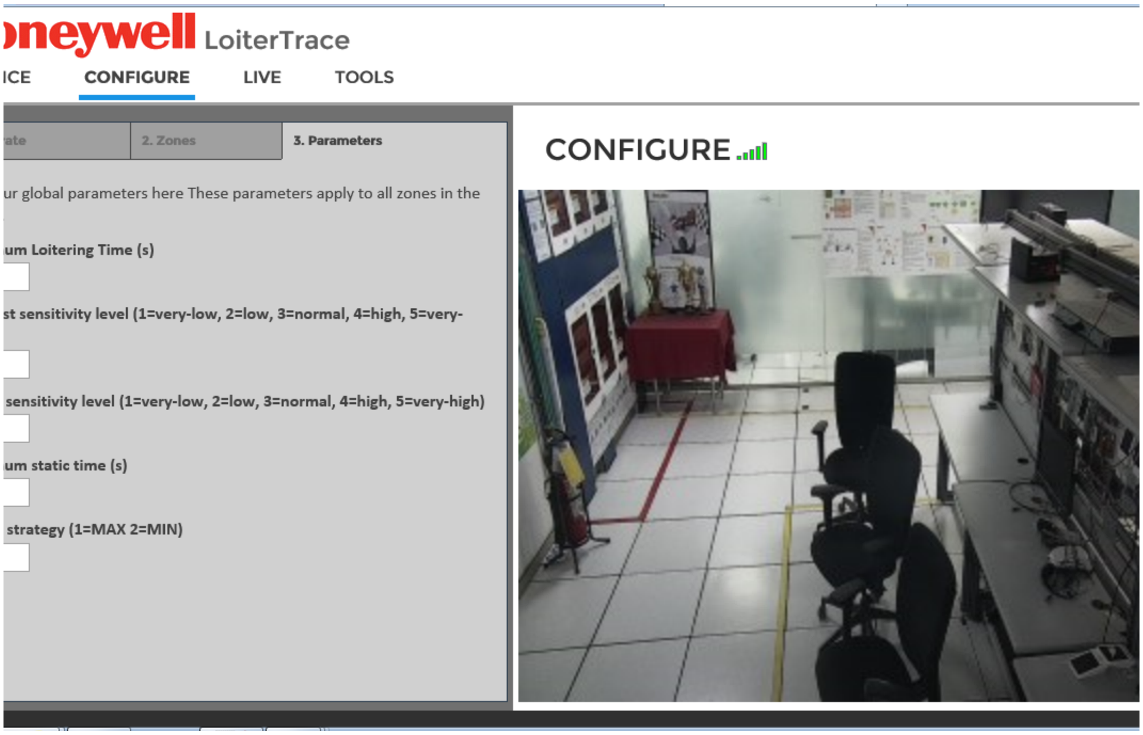
Step 5. Click on Zones and then click on Add area to add define the area for loitering trace. This will be the area under which an alarm is generated if an object found loitering more than the predefined time (Maximum Loitering time). User can define multiple zones.



d edit detection zones and masking (blackout) zones Zones can be
d to move them and the circles dragged to change their shape.
onal arrows can be rotated by dragging them.

Step 6. Click Save at the bottom of the page. Data Saved successfully message is displayed.

Step 7. Click on Parameters and set the parameter for all the defined zones. Such as maximum Loitering Time, Contrast sensitivity level, Object sensitivity level, Maximum static time and Times Strategy as shown below.



ur global parameters here These parameters apply to all zones in the

um Loitering Time (s)

st sensitivity level (1=very-low, 2=low, 3=normal, 4=high, 5=very-

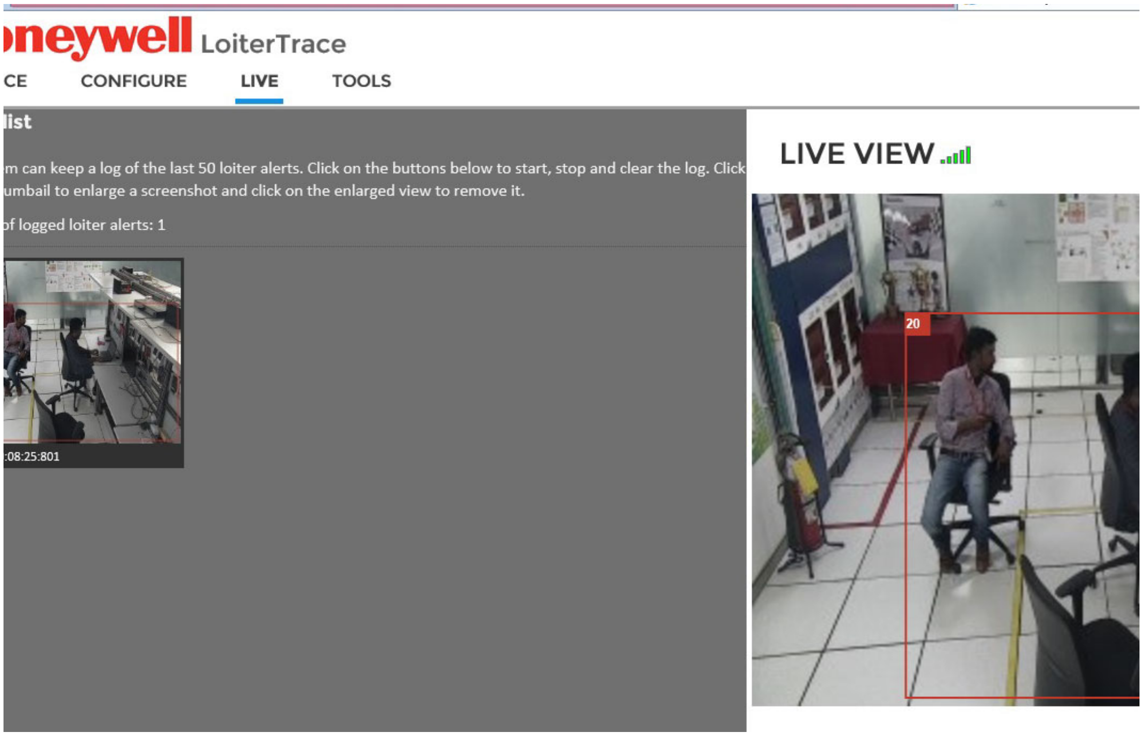
sensitivity level (1=very-low, 2=low, 3=normal, 4=high, 5=very-high)

um static time (s)

strategy (1=MAX 2=MIN)

Step 8. Click Save at the bottom of the page. Data Saved successfully message is displayed.

Step 9. Click on the Live tab to view the configured Loitering feature. In camera web page user can see the loiter alarm in the list as shown below.



m can keep a log of the last 50 loiter alerts. Click on the buttons below to start, stop and clear the log. Click umbail to enlarge a screenshot and click on the enlarged view to remove it.

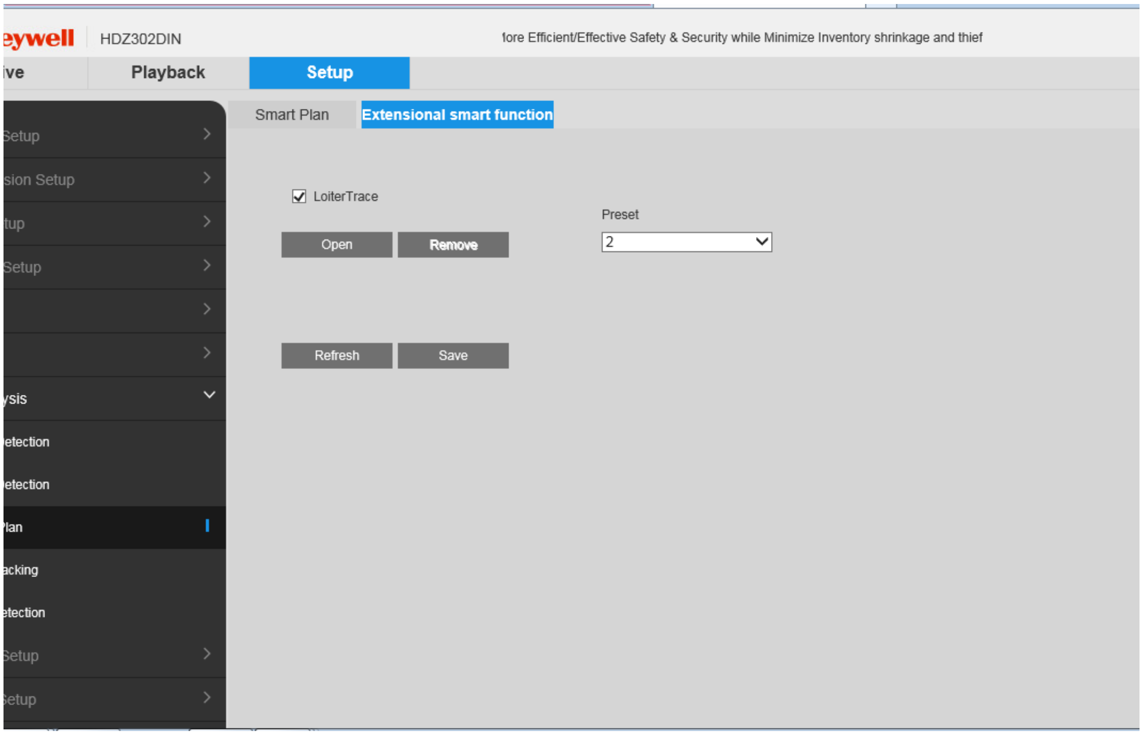
of logged loiter alerts: 1

Loitering Trace with PTZ Camera

For a PTZ camera Loitering trace should be configured with a predefined preset. If a camera has multiple presets then in camera web page the specific preset should be selected and saved in order to view the same in NVR.

However, Annotation will work with in the preset defined. if there is a minor variation beyond the preset area then Annotations will not be displayed.

The preset should be selected in camera web page > IVS Analysis > Smart Plan > Extensional Smart function > Preset as shown below.



☑ LoiterTrace

Preset 2

Configure and Enable Annotation in NVR

Annotation in NVR can be enabled if it is already configured in the supported camera web page. Equip-S series camera supports Annotation with Intrusion Trace and Loitering Trace.

Ensure you have completed the following in camera web page before enabling Annotation in NVR.

a. Upgraded the camera firmware

b. Upgraded the Intrusion and Loitering VA package

c. Obtained and installed the required license

d. Configured Intrusion and Loitering Trace features

How to enable Annotation in NVR

In Camera Web Page

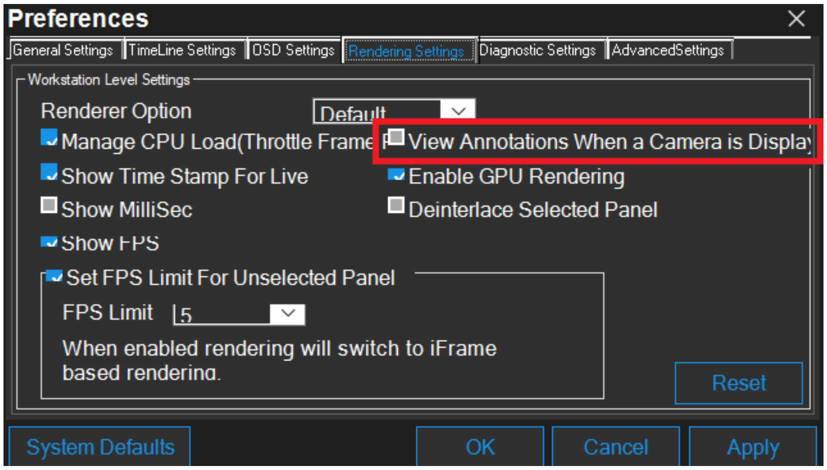
Step 1. Navigate to Video Analytics > Smart Plan. The Smart Plan page is displayed.

Step 2. If the Extensional Smart function is off, click to turn ON.

Step 3. Select the Intrusion Trace or Loitering Trace check box to enable Annotation.

In Preference Box

- In Preference > Rendering Setting tab, select the View Annotations when a camera is displayed check box to enable annotations for all the supported cameras (Equip-S Series)



Preferences

Workstation Level Settings

Renderer Option: Default

☑ Manage CPU Load(Throttle Frame R

☐ View Annotations When a Camera is Display

☑ Show Time Stamp For Live

☑ Enable GPU Rendering

☐ Show MilliSec

☐ Deinterlace Selected Panel

☑ Show FPS

☑ Set FPS Limit For Unselected Panel

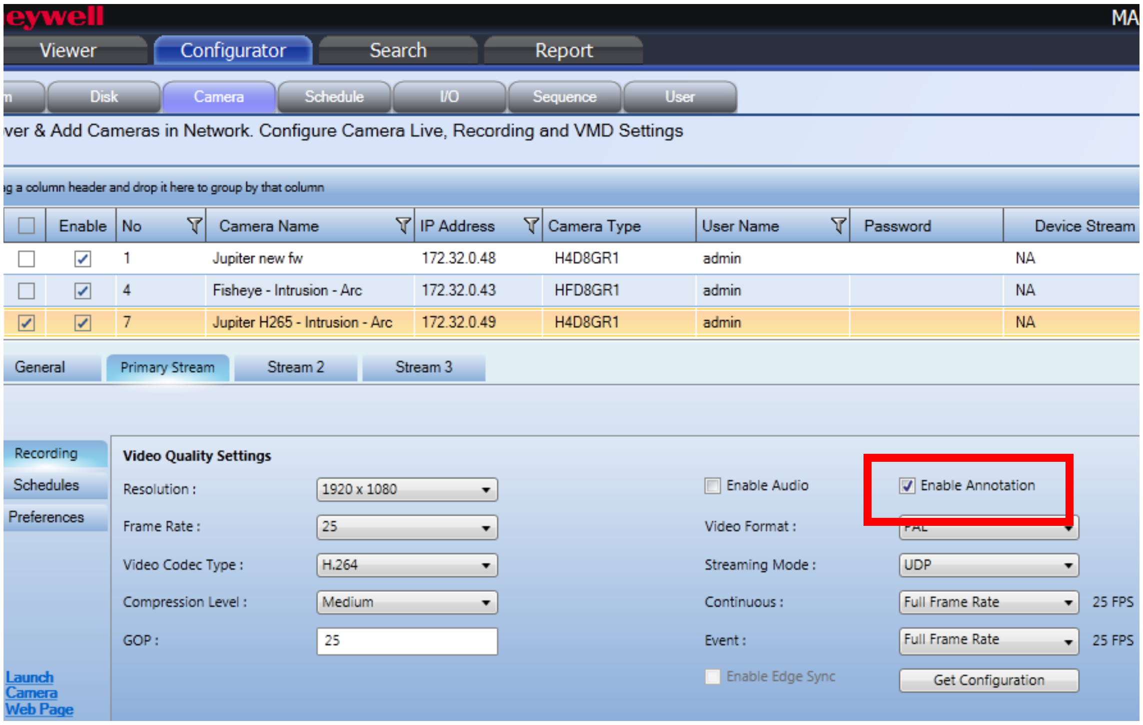
FPS Limit: 5

When enabled rendering will switch to iFrame based rendering.

- In Camera Properties, navigate to any stream and then select the Enable Annotation check box for the particular stream.

Note: *For Sub stream 2 Annotation will not work, if the resolution is taken form camera sub stream 2. This is a camera side limitation.*

For PTZ camera based on the Preset selection, annotation will not work if there is a slight movement beyond the defined preset.



ver & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

g a column header and drop it here to group by that column

☐	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream
☐	☑	1	Jupiter new fw	172.32.0.48	H4D8GR1	admin		NA
☐	☑	4	Fisheye - Intrusion - Arc	172.32.0.43	HFD8GR1	admin		NA
☑	☑	7	Jupiter H265 - Intrusion - Arc	172.32.0.49	H4D8GR1	admin		NA

Video Quality Settings

Resolution : 1920 x 1080

Frame Rate : 25

Video Codec Type : H.264

Compression Level : Medium

GOP : 25

☐ Enable Audio

☑ Enable Annotation

Video Format : PAL

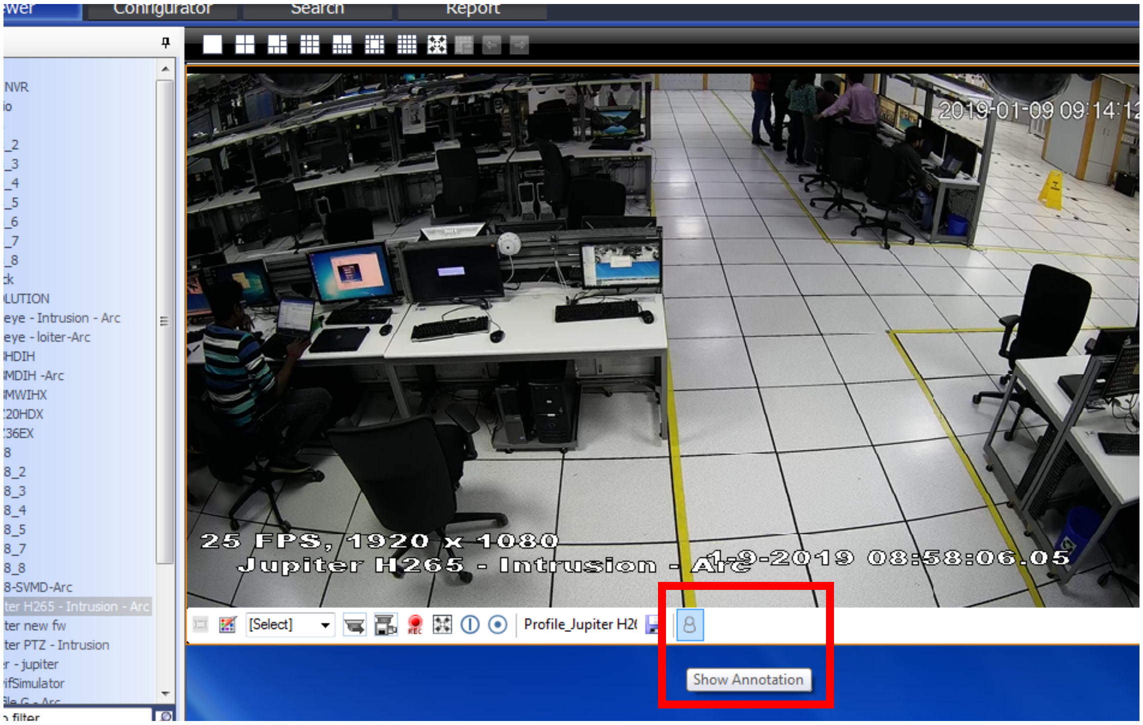
Streaming Mode : UDP

Continuous : Full Frame Rate 25 FPS

Event : Full Frame Rate 25 FPS

☐ Enable Edge Sync

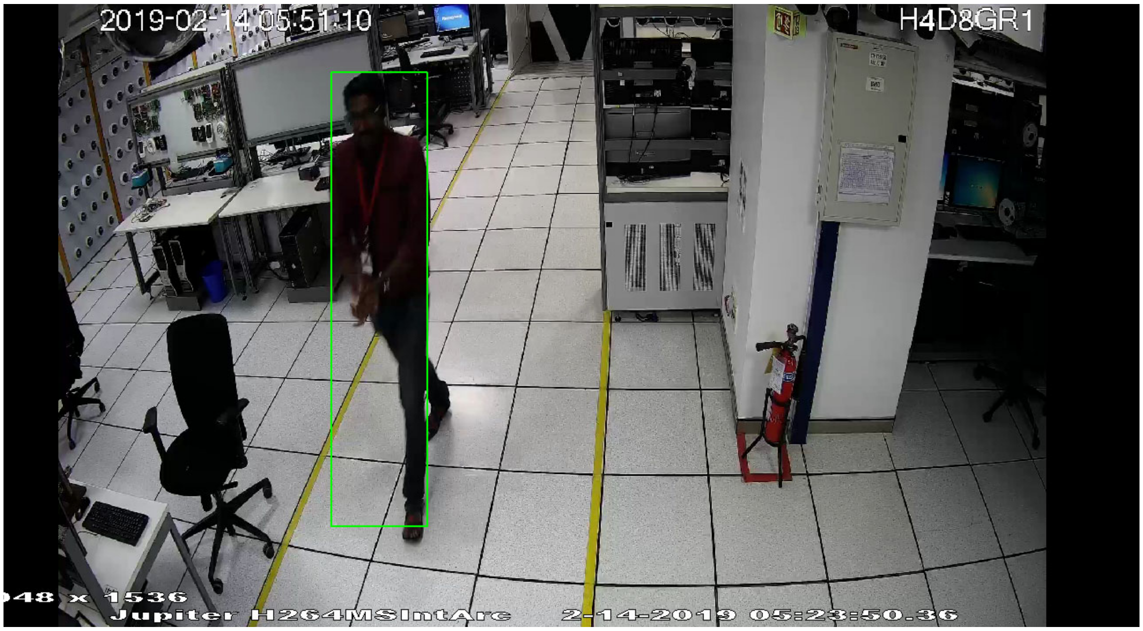
- In Video panel, hover the mouse in the bottom of the panel to view the options and then click on Show Annotations for that particular camera as shown below. You can also click th same icon to Hide annotation s only for that camera.



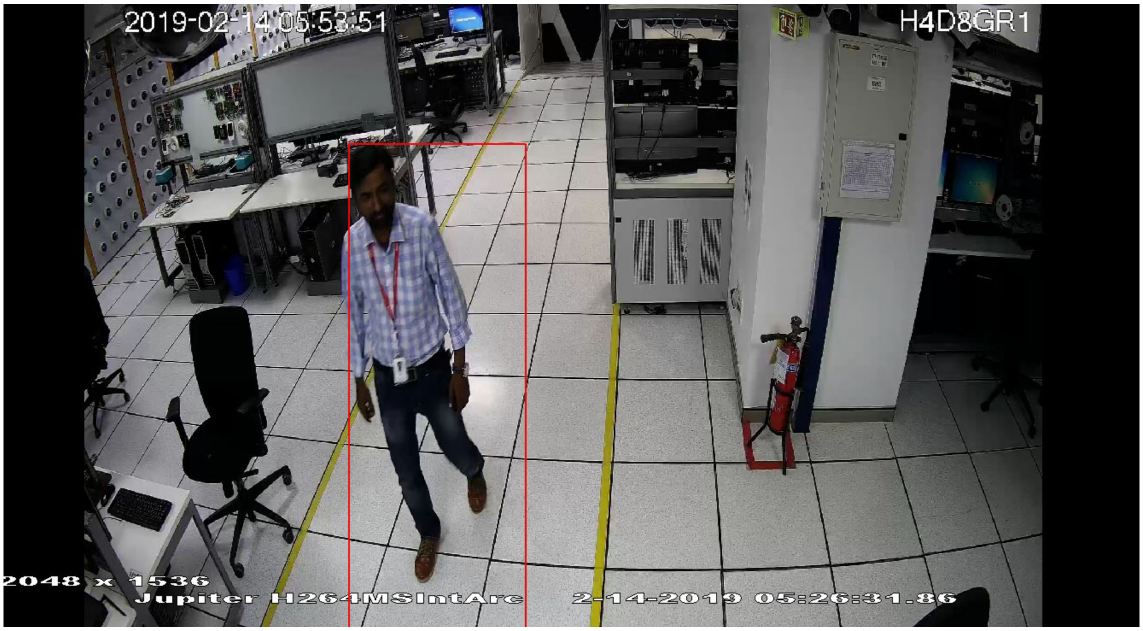
Annotation with Intrusion Trace in VMS/NVR (Live/playback)

After the Annotation feature is enabled for Intrusion trace, rectangular bounding boxes will be accompanied with any moving object in the scene. If any object is moving within the predefine area then the object is highlighted with Red rectangular box and an alarm is generated a shown below.

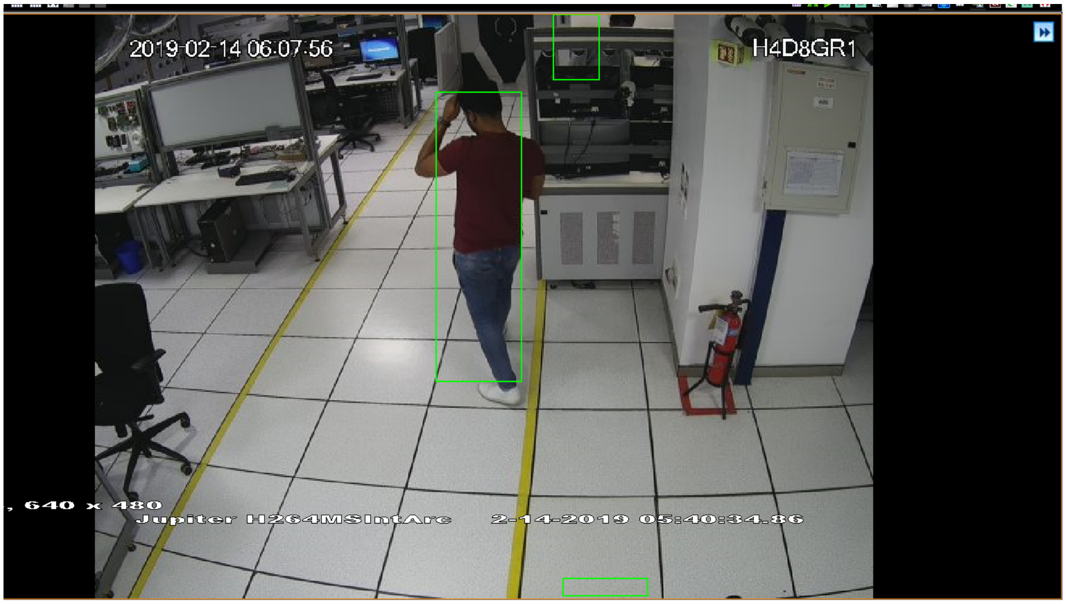
Annotation with Intrusion Trace (Live) with out alarm



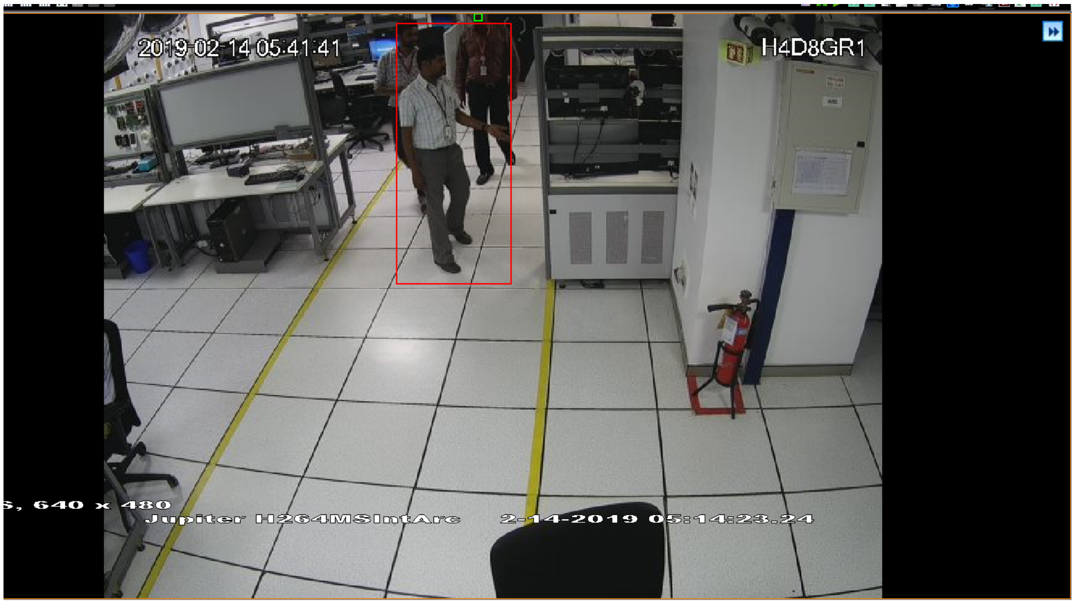
Annotation with Intrusion Trace (Live) with alarm



Annotation with Intrusion Trace (Playback) Without alarm



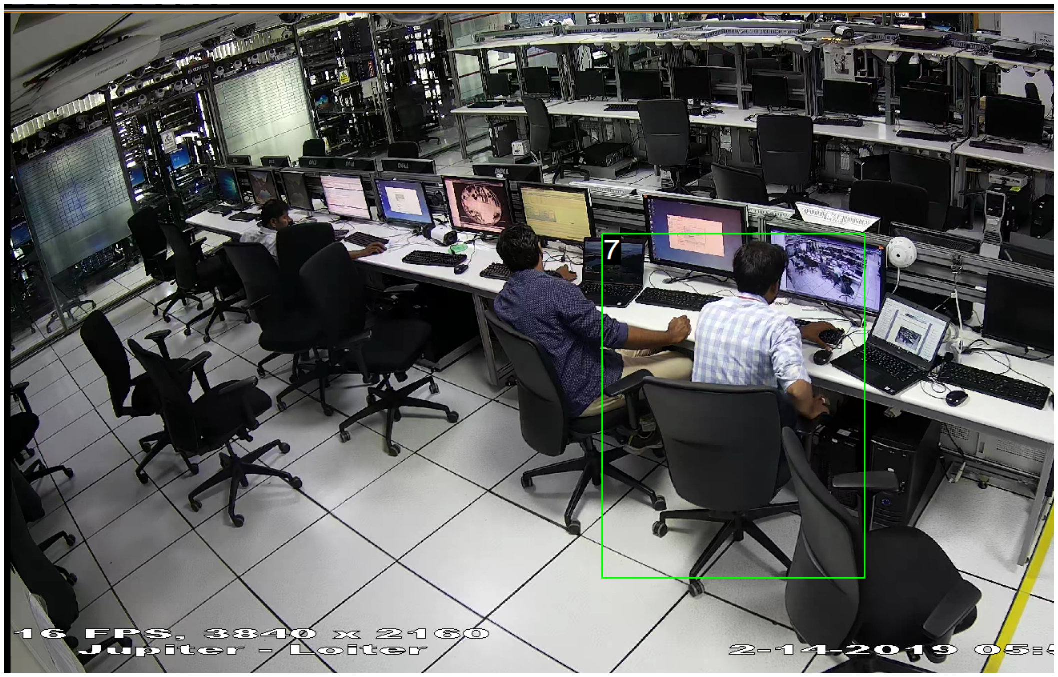
Annotation with Intrusion Trace (Playback) With alarm



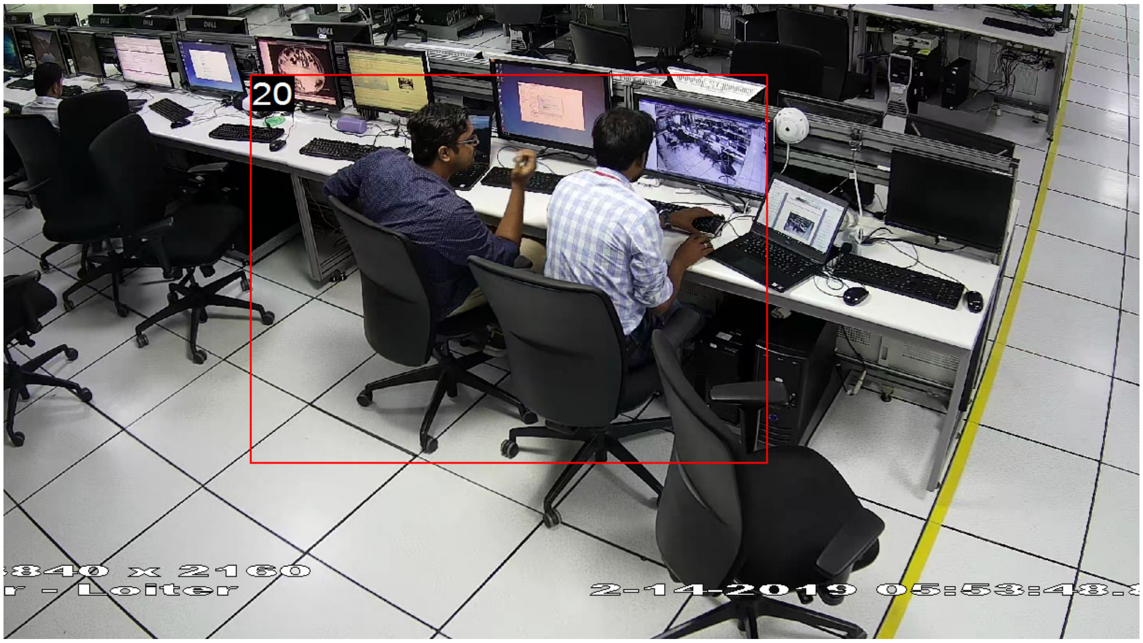
Annotation with Loitering Trace in VMS/NVR (Live/playback)

If an object loiters with in the predefined zone then a Green colored rectangular bounding box are displayed. If the same object loiters beyond the Maximum Loitering Time, then the object will be highlighted with Red Rectangular box as shown below.

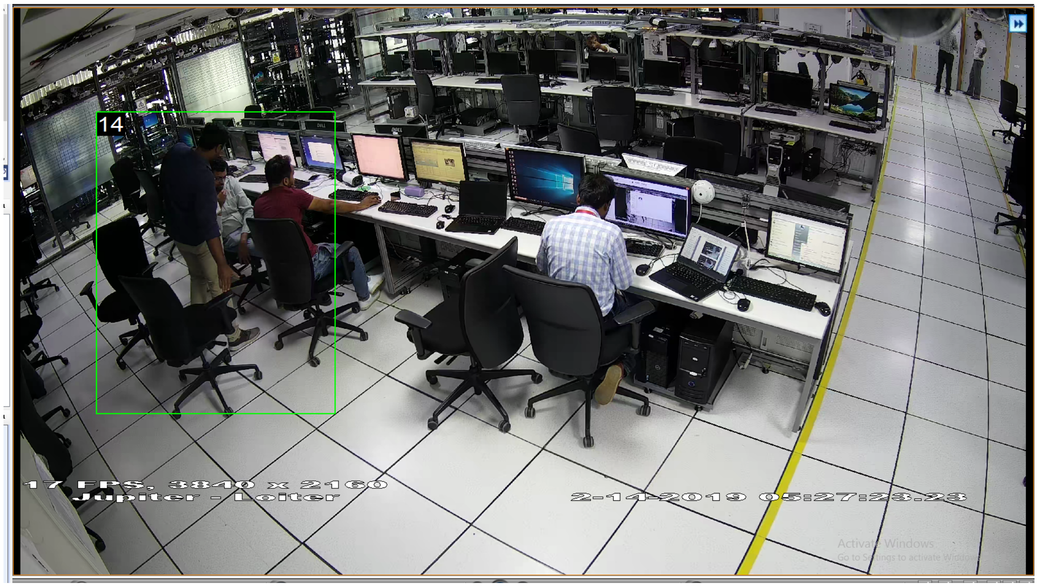
Object with in the Maximum Loitering Time (Live)



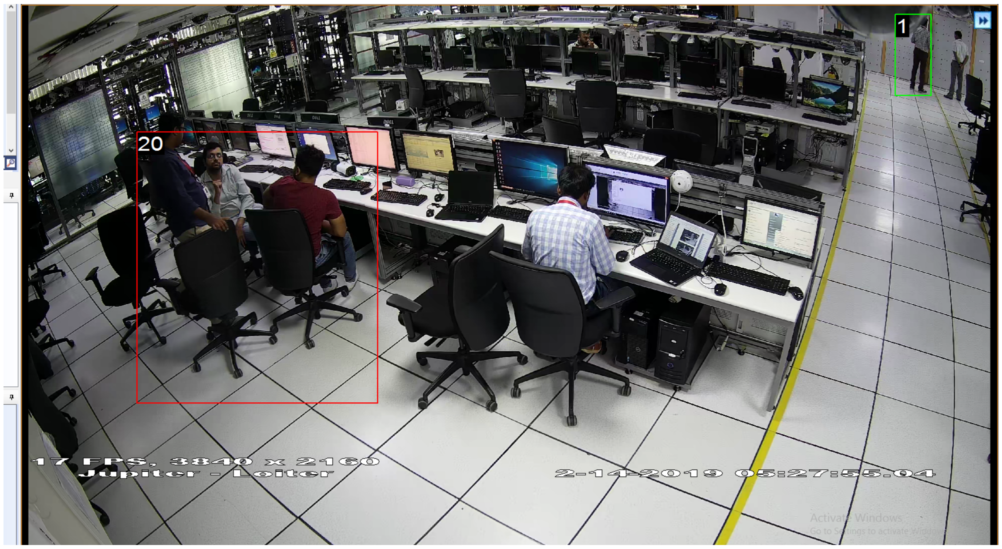
Object beyond the Maximum Loitering Time (Live)



Loitering Trace in Playback without alarm



Loitering Trace in Playback with alarm



Snapshots with Annotations

- Capturing snapshots with Annotation bounding box in Live and Recorded video is supported. User can find the captured snapshots under Snapshots/ Clips pane.

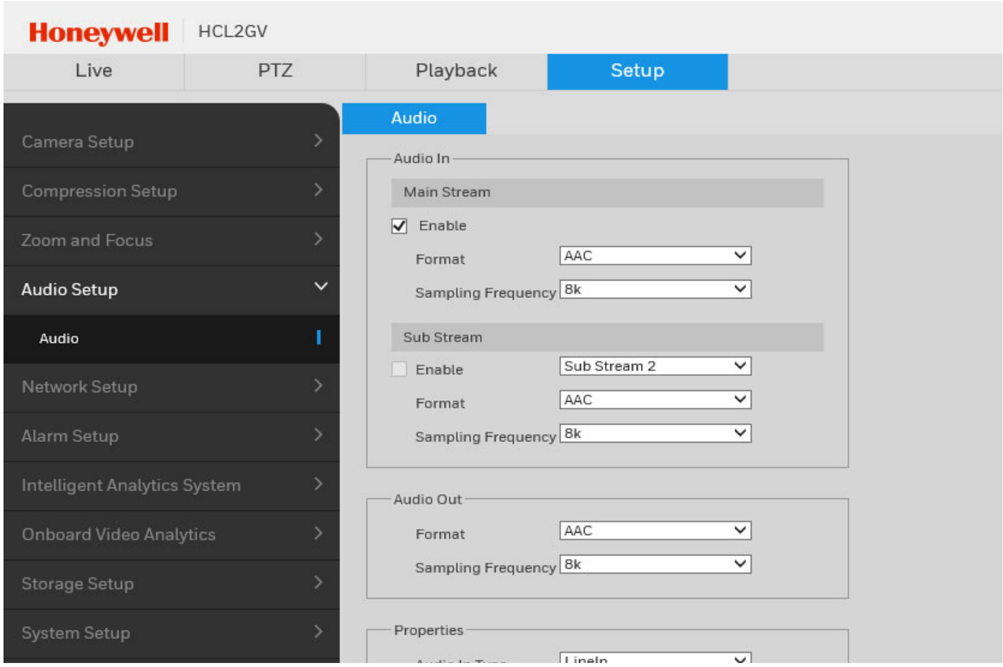
Setting the Audio Codec in Camera Web Page

Latest version of Equip S Series V2 camera firmware will not render video in NVR with the previous versions of MAXPRO NVR 5.0/5.5. To overcome this issue user need to set the Audio codec for all the streams to AAC in the specific camera web page.

How to set the Audio Codec

Step 1. Logon to specific camera web page (for ex HBW4GR1V).

Step 2. Navigate to Setup > Audio Setup > Audio. The Audio settings are displayed on the left pane as shown below.



Audio In

Main Stream

☑ Enable

Format: AAC

Sampling Frequency: 8k

Sub Stream

□ Enable: Sub Stream 2

Format: AAC

Sampling Frequency: 8k

Audio Out

Format: AAC

Sampling Frequency: 8k

Properties

Audio In Type: LineIn

Step 3. Under Audio In area > Main Stream, select AAC from the Format drop-down list.

Step 4. Under Sub Stream, select the Enable check box.

Step 5. Select the required Sub Stream from the drop down list and then select AAC option from the Format drop-down list.

Step 6. Under Audio Out area, select AAC from the Format drop-down list.

Step 7. Click Save.

Video Guard service for SIRA compliance

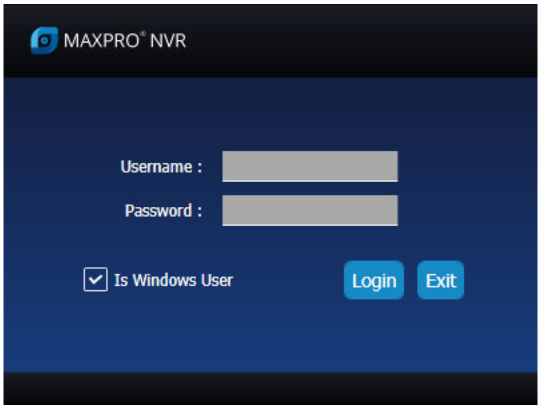
MAXPRO R600 release supports SIRA compliance with Video Guard Device Integration. This is to meet the specifications defined as part of the City wide Surveillance initiative by the Security Industry Regulatory Agency (SIRA) of Dubai, UAE, and being adopted across Middle-East countries.

User can run this service in NVR box to be in compliant with SIRA standards. To enable the service user needs to use MAXPRO Video Guard Configurator available in Bin folder. This configurator connects to MAXPRO NVR, sends the recorder information to video guard systems and synchronize the heartbeat messages (Polling) and system time.

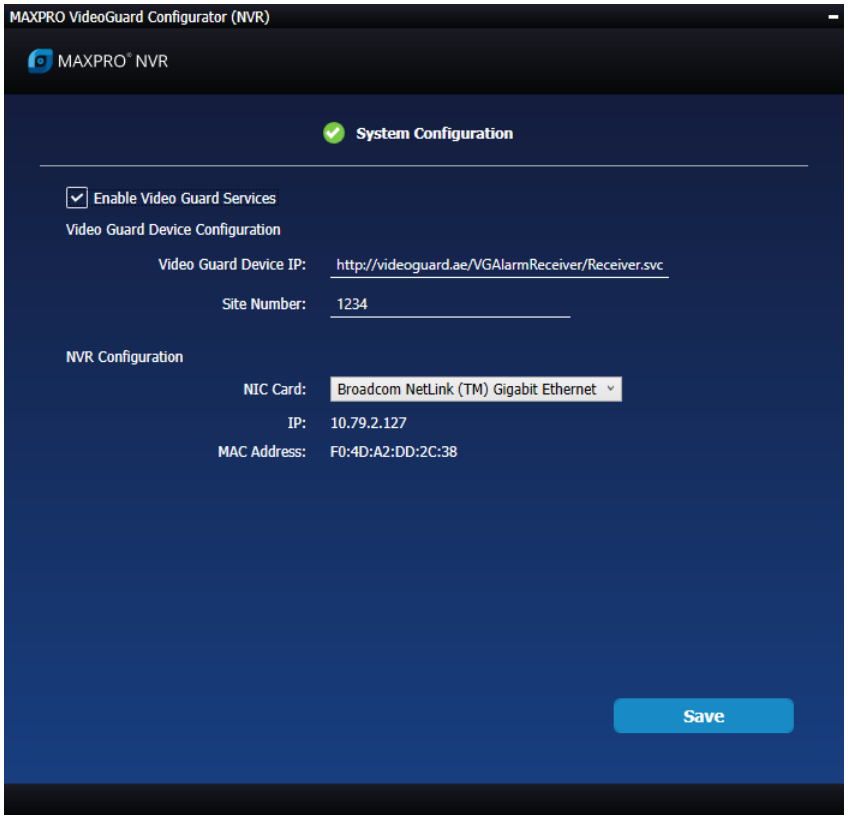
Note: *Network time sync should be disabled when NVR is configured to communicate with Video Guard device.*
It is required to restart NEO engine once the timezone is changed by Video Guard service.

How to run the WCF service using MAXPRO Video Guard Configurator

1. Navigate to MAXPRO NVR Bin folder and then locate the MAXPRO Video Guard Configurator.exe.
2. Double-click the exe. A login window is displayed as shown below.



3. Type the Username and Password in the box provided.
   Or
   Select Is Window User check box to login using windows credentials.
4. Click the Login button. The MAXPRO Video Guard Configurator application is displayed as shown below.



☑ Enable Video Guard Services

Video Guard Device Configuration

Video Guard Device IP: http://videoguard.ae/VGAlarmReceiver/Receiver.svc

Site Number: 1234

NVR Configuration

NIC Card: Broadcom NetLink (TM) Gigabit Ethernet

IP: 10.79.2.127

MAC Address: F0:4D:A2:DD:2C:38

5. Select the Enable Video Guard Services check box. By default it is cleared.
6. Under Video Guard Device Configuration:
   - Type the Video Guard Device IP
   - Type the Site Number
7. Under NVR Configuration:
   - Select the NIC card from the drop down list
8. Click the Save button.

NDAA HC Series 30 Camera Support

The following tables explain the list of supported camera models, firmware version and events supported with Series 30 cameras.

Note: *Series 30 camera should be discovered with correct user name and password else the camera can lock out for 5 minutes.*

.

#	Camera Models	Firmware Details
1	HC30W42R3	v1.0.18.20190523 Note: If a camera has older firmware, please upgrade to this version or above and perform factory default once
2	HC30W45R3	
3	HC30W45R2	
4	HC30WB2R1	
5	HC30WB5R1	
6	HC30WB5R2	
7	HC30WE2R3	
8	HC30WE5R3	
9	HC30WE5R2	
10	HC30WF5R1	

Supported Events

The following events are support with Series 30 Camera Integration.:

Event
Motion Detection
Tamper Detection
Image too blur
Image too dark
Image too bright
People Detection
Intrusion

Series 30 Cameras Features

HC Series 30 cameras supports the following features.

- Smart Stream III
  - Smart Codec
  - Smart FPS
  - Dynamic intra Frame Period (DIF)
- HTTPS

Note: *HC30WF5R1 model camera does not support HTTPS.*

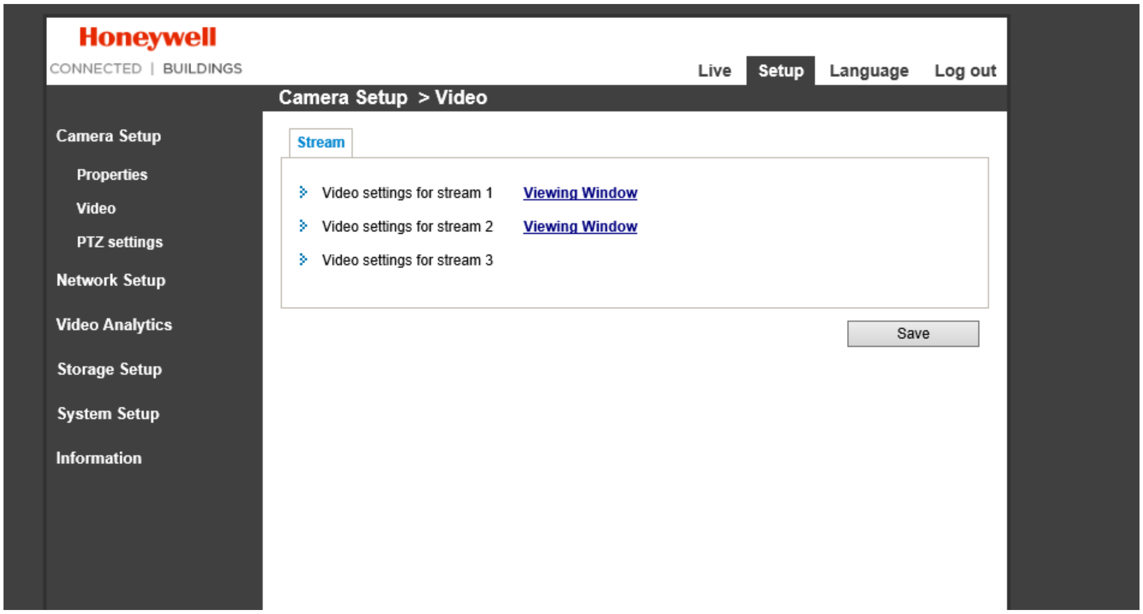
- Alarms
- Profile S compliant
- Multicast

User need to configure the below Smart Stream III features at camera side to use it in NVR. These features helps the end user to reduce the bandwidth usage in the network. Once these features are configured user can add or discover the camera in NVR for surveillance purpose.

- Smart Codec: Based on region of interest in the scene the code format is automatically applied. The user can adjust the quality balance between ROI (Region of Interest) and non-ROI area. It is applicable only for H.264 and H.265 codec format. See How to configure Smart Codec.
- Smart FPS: Dynamically manages and adjust the FPS based on the motion in the scene. If there is a high motion in the scene then higher FPS is utilized and vice versa. See How to Enable Smart FPS
- DIF (Dynamic intra Frame Period): Automatically adjusts the I frame interval time from 1 up to 10 seconds based on the motion in scene. See How to Enable DIF
- HTTPS: Allows user to enable secure communication for video over the network using secure protocol. See How to enable Https for series 30 Cameras

How to configure Smart Codec

1. Log on to the HC30 Series camera.
2. Click the Setup tab. The General Settings page is displayed.
3. On the left pane, navigate to Camera Setup > Video. The Stream list is displayed o the right pane as shown below.



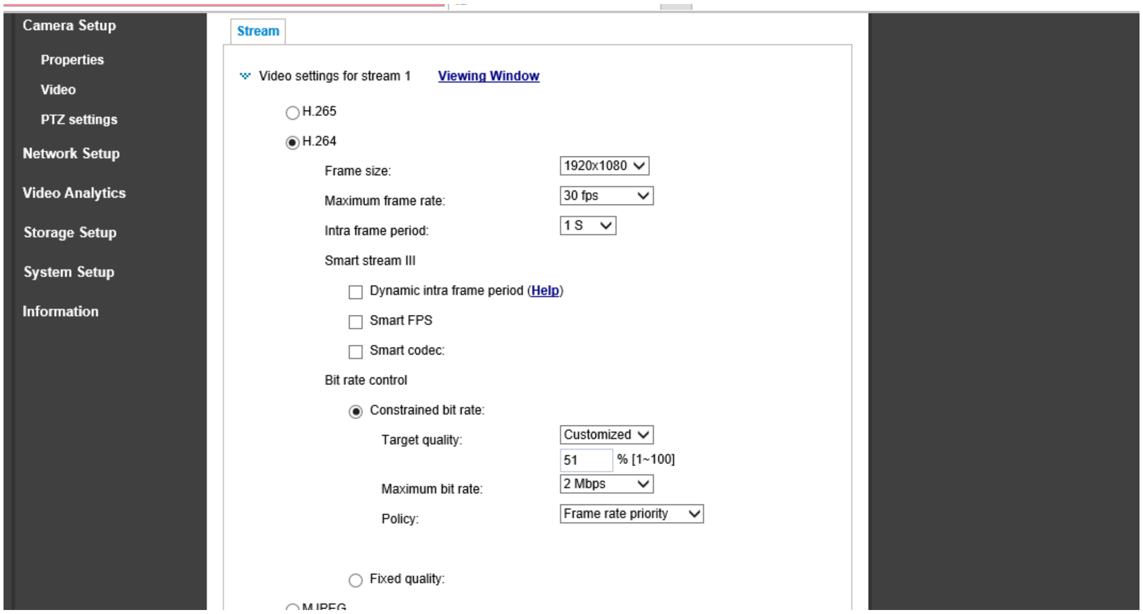
Camera Setup > Video

Video settings for stream 1 Viewing Window

Video settings for stream 2 Viewing Window

Video settings for stream 3

4. Click Video Settings for Stream 1. The Stream setting page is displayed.



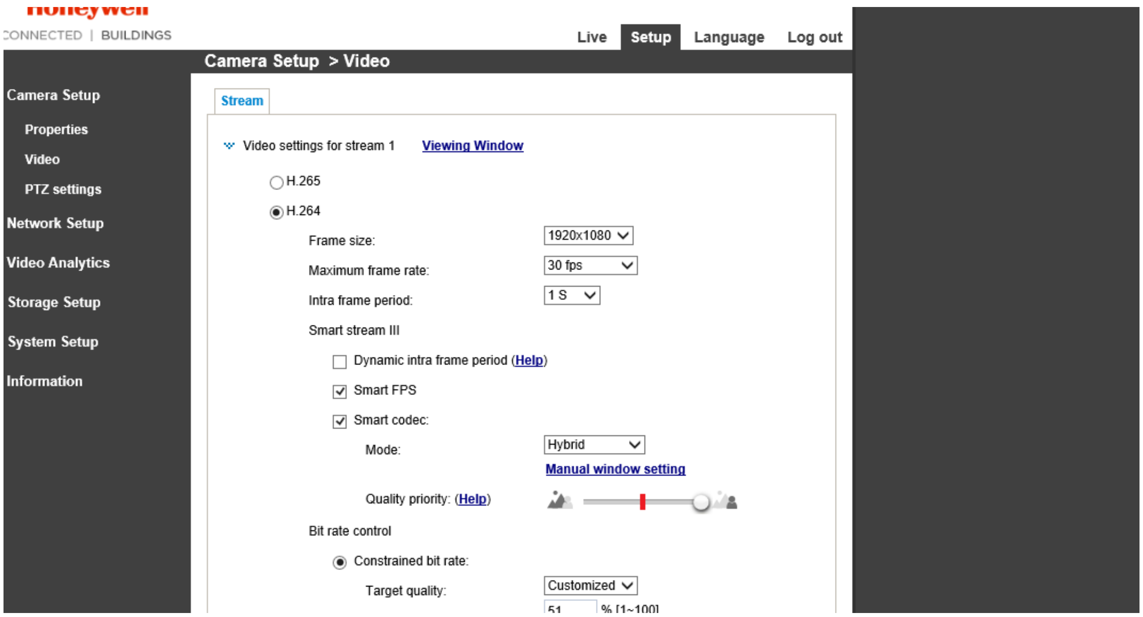
Video settings for stream 1

○ H.265
● H.264

Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S
Smart stream III
□ Dynamic intra frame period (Help)
□ Smart FPS
□ Smart codec:
Bit rate control
● Constrained bit rate:
Target quality: Customized
51 % [1~100]
Maximum bit rate: 2 Mbps
Policy: Frame rate priority
○ Fixed quality:
○ MJPEG

5. Select the Codec format. Only H.265 and H.264 is supported. The corresponding settings are displayed.

6. Under Smart Stream III, select the Smart Codec check box. The Mode and Quality Priority options are displayed as shown below.



Video settings for stream 1

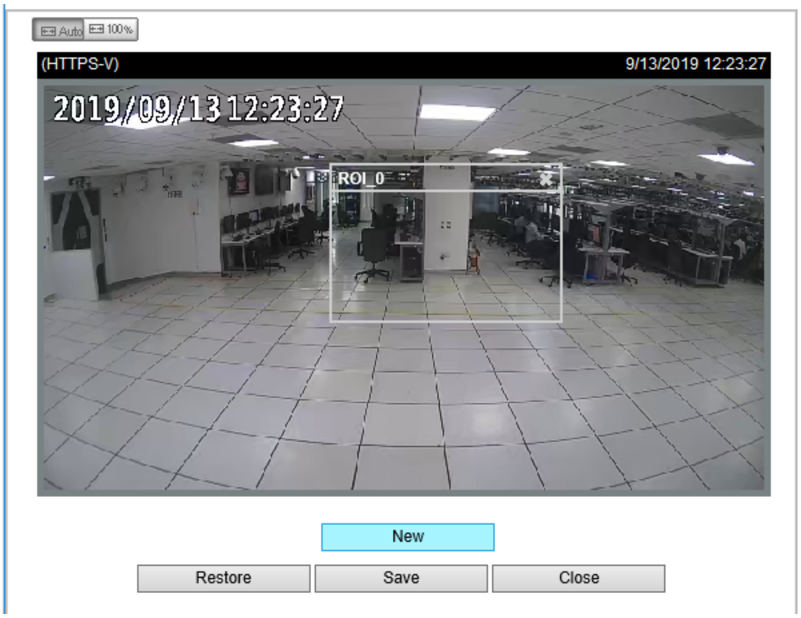
○ H.265
● H.264

Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S
Smart stream III
□ Dynamic intra frame period (Help)
☑ Smart FPS
☑ Smart codec:
Mode: Hybrid
Quality priority: (Help)
Bit rate control
● Constrained bit rate:
Target quality: Customized
51 % [1~100]

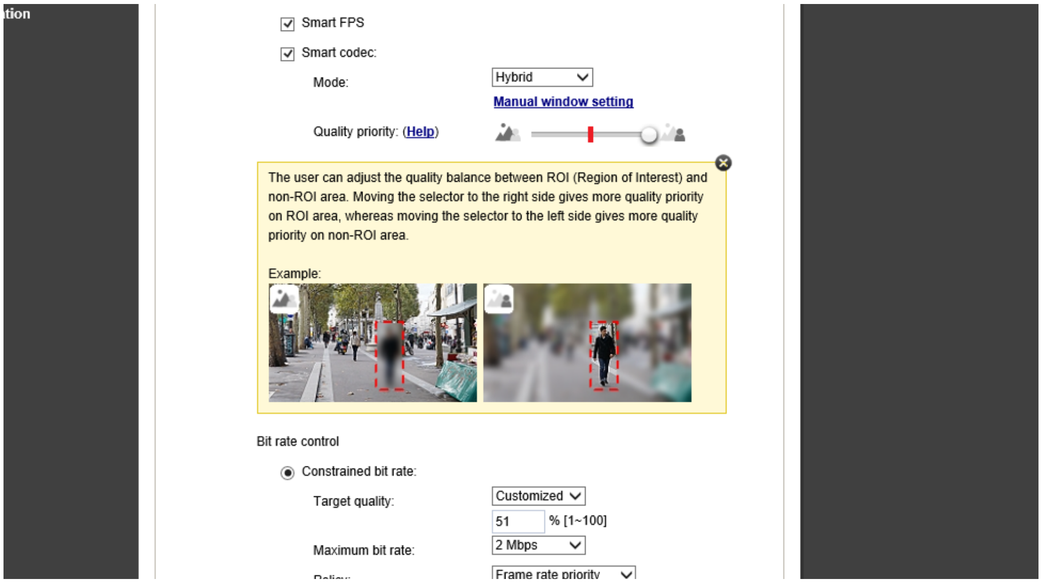
7. Select the required Mode from the drop-down list. The available options are
   - Auto tracking: Automatically sets the ROI and non ROI area for smart codec
   - Manual: Manually need to define the ROI and non ROI area for smart codec
   - Hybrid: Automatically sets the ROI and non ROI area for smart codec

To manually set the mode:

1. Select Manual option from the Mode drop-down list.
2. Click the Manual Window Settings. The video rendering page is displayed.



3. Click the New button to define or add new ROI and then click Save.
4. Click Close to complete defining ROI.
5. Under Quality Priority, move the slider left or right accordingly to balance the quality between ROI and non ROI region as shown below. Refer the camera page help for more details.



☑ Smart FPS

☑ Smart codec:

Mode: Hybrid

Manual window setting

Quality priority: (Help)

The user can adjust the quality balance between ROI (Region of Interest) and non-ROI area. Moving the selector to the right side gives more quality priority on ROI area, whereas moving the selector to the left side gives more quality priority on non-ROI area.

Example:

Bit rate control

● Constrained bit rate:

Target quality: Customized

51 % [1~100]

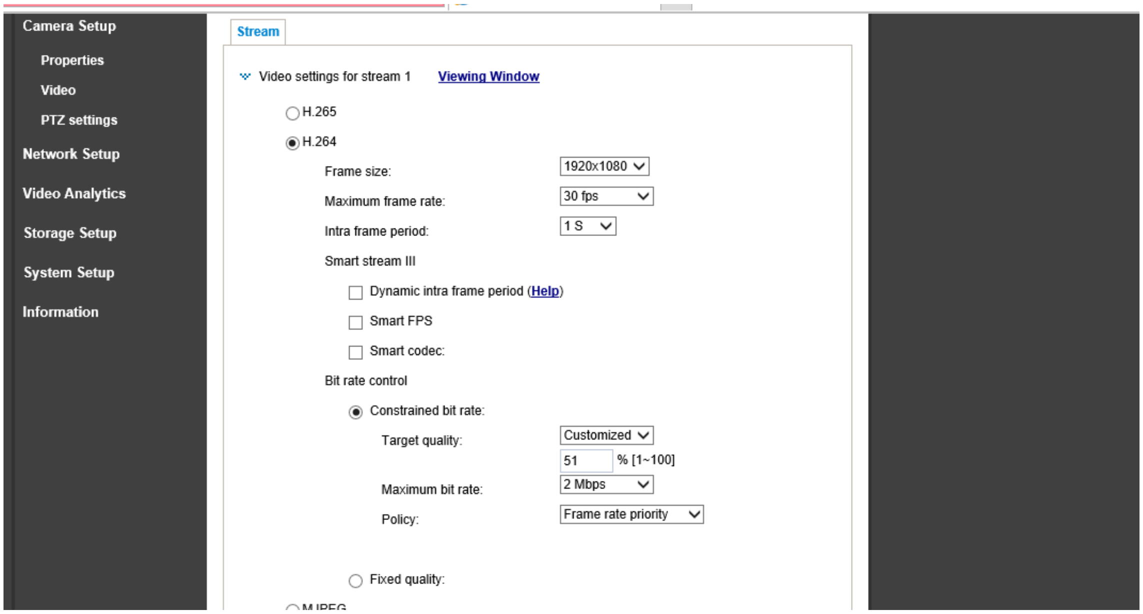
Maximum bit rate: 2 Mbps

Policy: Frame rate priority

6. Click Save to complete the configuration. Similarly configure the Smart Codec manually for other streams.

How to Enable Smart FPS

1. In the camera web page, click Setup > Camera Setup > Video > Video Settings for Stream 1. The Stream setting page is displayed.



Video settings for stream 1

○ H.265
● H.264

Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S

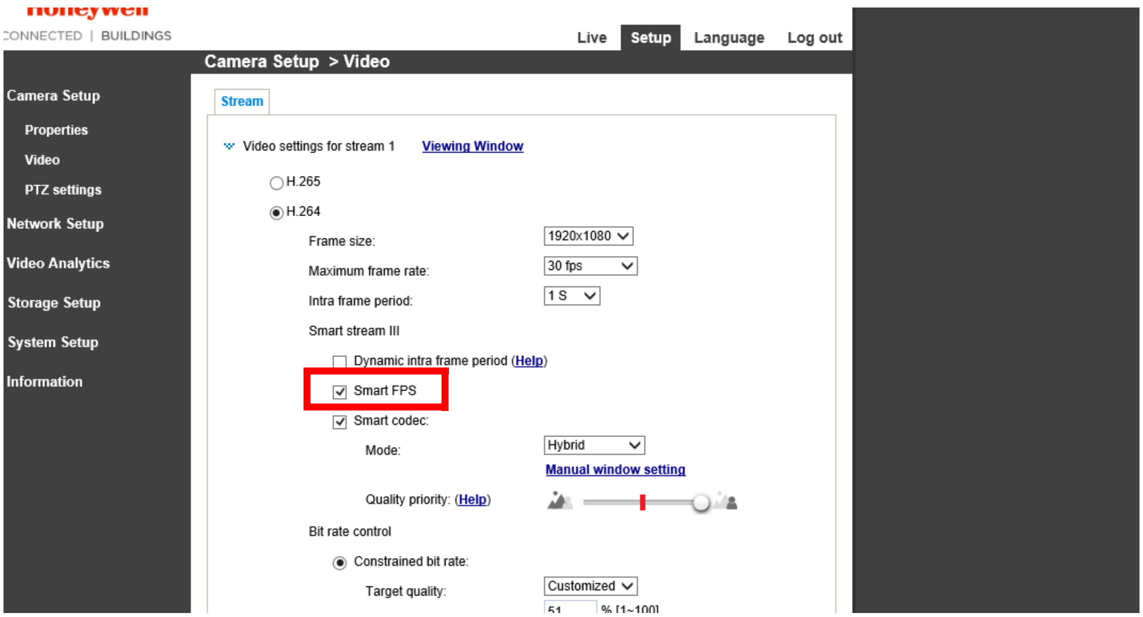
Smart stream III
□ Dynamic intra frame period (Help)
□ Smart FPS
□ Smart codec:

Bit rate control
● Constrained bit rate:
Target quality: Customized
51 % [1~100]
Maximum bit rate: 2 Mbps
Policy: Frame rate priority

○ Fixed quality:

○ M JPEG

2. Under Smart Stream III, select the Smart FPS check box as highlighted below.



Video settings for stream 1

○ H.265
● H.264

Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S

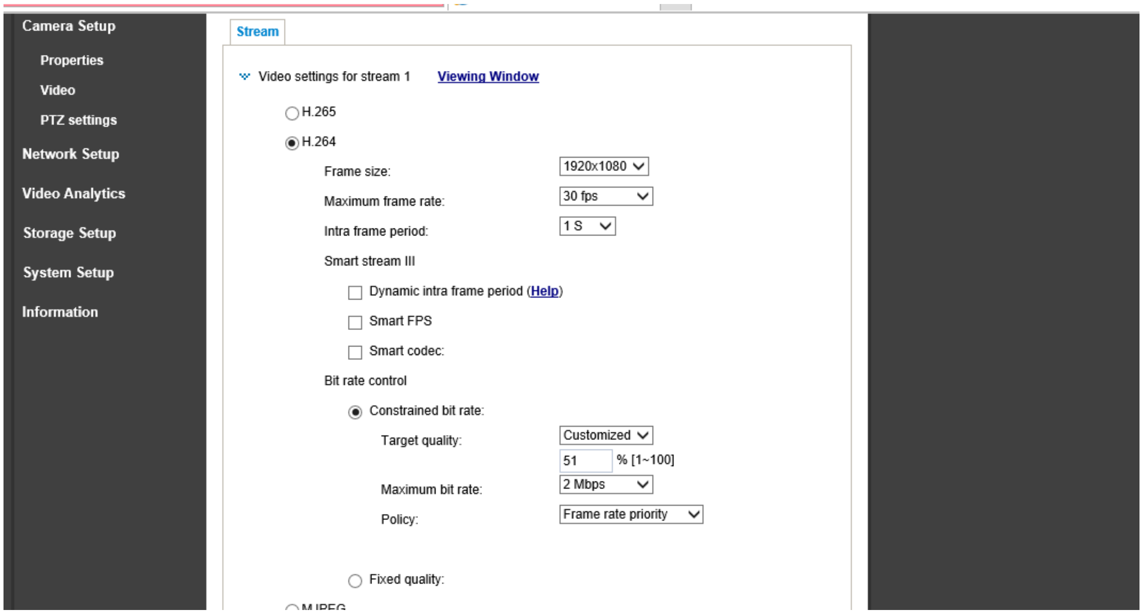
Smart stream III
□ Dynamic intra frame period (Help)
☑ Smart FPS
☑ Smart codec:
Mode: Hybrid
Quality priority: (Help)

Bit rate control
● Constrained bit rate:
Target quality: Customized
51 % [1~100]

3. Click Save. Similarly enable the Smart FPS manually for other streams

How to Enable DIF

1. In the camera web page, click Setup > Camera Setup > Video > Video Settings for Stream 1. The Stream setting page is displayed.



Video settings for stream 1

○ H.265

● H.264

Frame size: 1920x1080

Maximum frame rate: 30 fps

Intra frame period: 1 S

Smart stream III

□ Dynamic intra frame period (Help)

□ Smart FPS

□ Smart codec:

Bit rate control

● Constrained bit rate:

Target quality: Customized

51 % [1~100]

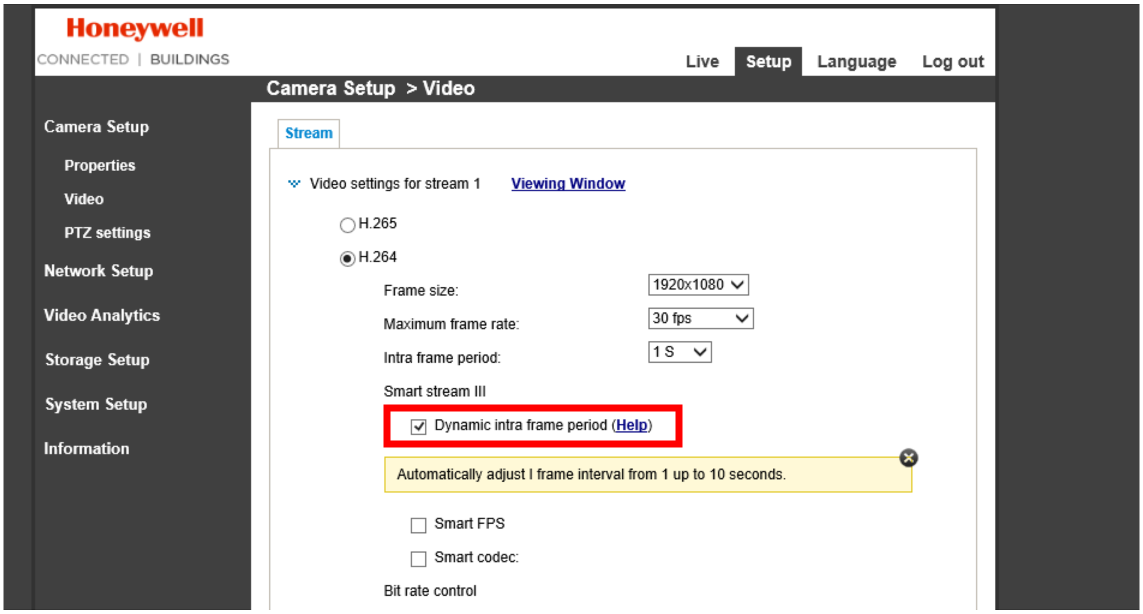
Maximum bit rate: 2 Mbps

Policy: Frame rate priority

○ Fixed quality:

○ MJPEG

2. Under Smart Stream III, select the Dynamic intra frame period check box as highlighted below. Refer the camera help for more details.



Video settings for stream 1

○ H.265

● H.264

Frame size: 1920x1080

Maximum frame rate: 30 fps

Intra frame period: 1 S

Smart stream III

☑ Dynamic intra frame period (Help)

Automatically adjust I frame interval from 1 up to 10 seconds.

□ Smart FPS

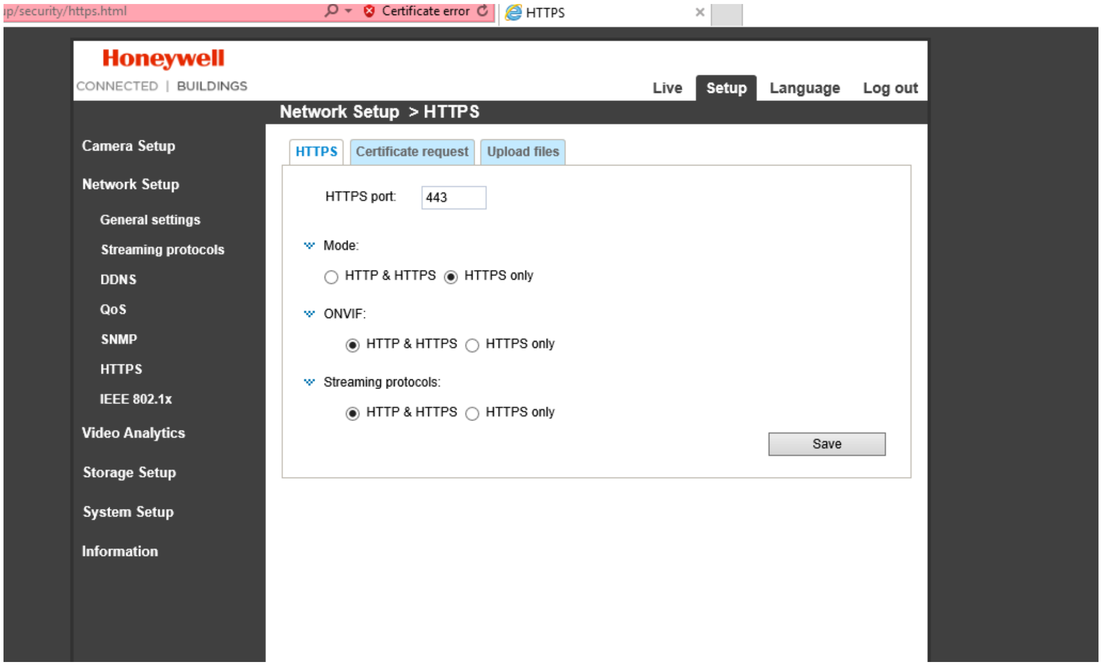
□ Smart codec:

Bit rate control

3. Click Save to complete enabling. Similarly enable the DIF manually for other streams

How to enable Https for series 30 Cameras

1. Log on to the HC30 Series camera.
2. Click the Setup tab. The General Settings page is displayed.
3. On the left pane, navigate to Network Setup > HTTPS. The HTTPS tab is displayed on the right pane as shown below.



HTTPS port: 443

Mode:

○ HTTP & HTTPS ● HTTPS only

ONVIF:

● HTTP & HTTPS ○ HTTPS only

Streaming protocols:

● HTTP & HTTPS ○ HTTPS only

4. Under Mode, click HTTPS only option.
5. Under ONVIF, click HTTP & HTTPS option.
6. Under Streaming protocols, click HTTP & HTTPS option.

Note: *Ensure that you select the options as mentioned above to secure the communication. HC30WF5R1 model camera does not support HTTPS.*

7. Click Save to complete.

Event Settings

Refer the HC Series 30 camera help on how to configure the events.

MPEG2 Encoder Support

NVR 6.0 release supports legacy MPEG2 Encoders with Live and playback, Alarms and VMS in VMS functionalities. The following encoders are supported.

- ENC8M2
- VE8M2

Supported Firmware Version: 1.2.261

Supported Features are:

- Live
- Playback
- Export

Note: *It is not recommended to add Encoder/Multi-channel video stream across NEO storage.*

Multicast Streaming IP for Encoder

MAXPRO NVR 6.0 supports multicast streaming IP configuration for encoders. User can assign a IP to view the encoder streams in multiple NVR clients.

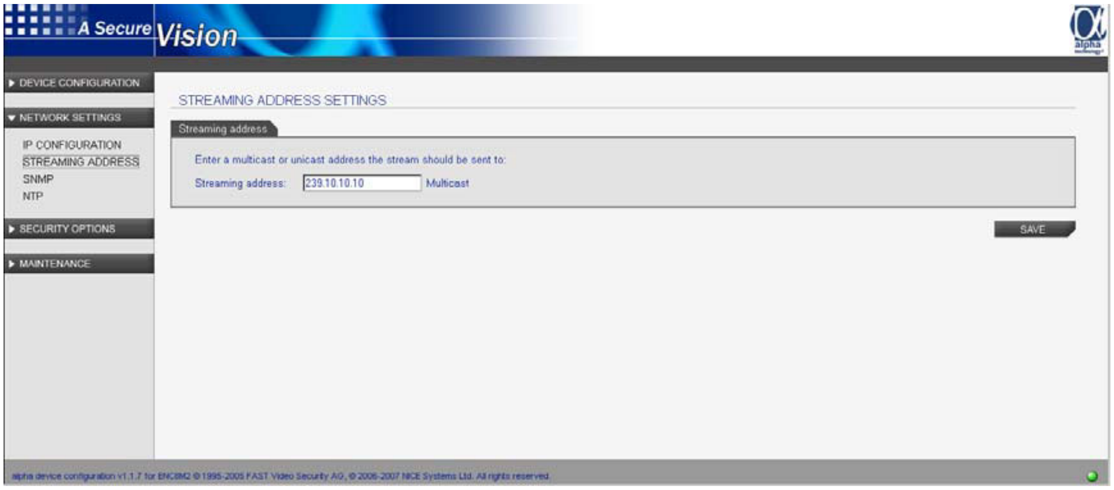
How to configure Multicast IP for ENC Encoder

Multicast Streaming IP address can be set in two ways:

- Using Encoder Web page
- Using VX Manager

Using Encoder webpage

1. Launch the Encoder (ENC8M2 or VE8M2) web page.
2. On the left pane, navigate to Network Settings node > Streaming Address. The Streaming Address Settings page is displayed on the right pane.



STREAMING ADDRESS SETTINGS

Streaming address

Enter a multicast or unicast address the stream should be sent to:

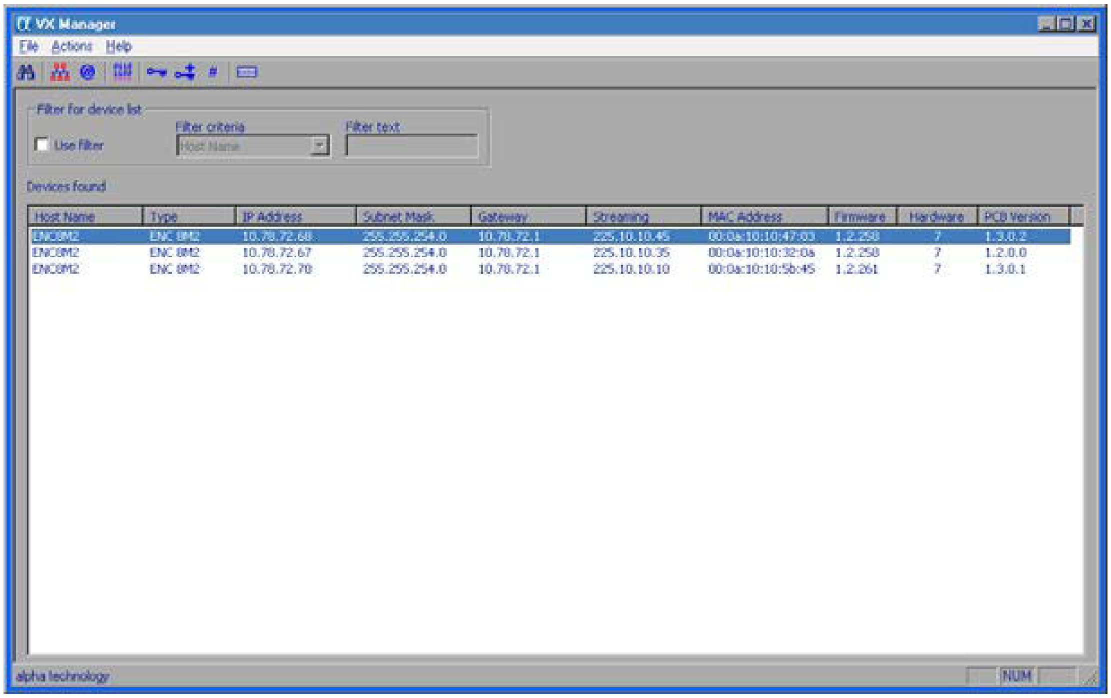
Streaming address: 239.10.10.10 Multicast

alpha device configuration v1.1.7 for ENC8M2 ©1995-2005 FAST Video Security AG, ©2006-2007 NICE Systems Ltd. All rights reserved.

3. In the Streaming Address Multicast box, type the multicasting IP address.

Note: *Unicast streaming IP address is not supported.*

1. Launch the VX Manager and discover the required encoder as shown below.



Filter for device list

□ Use filter

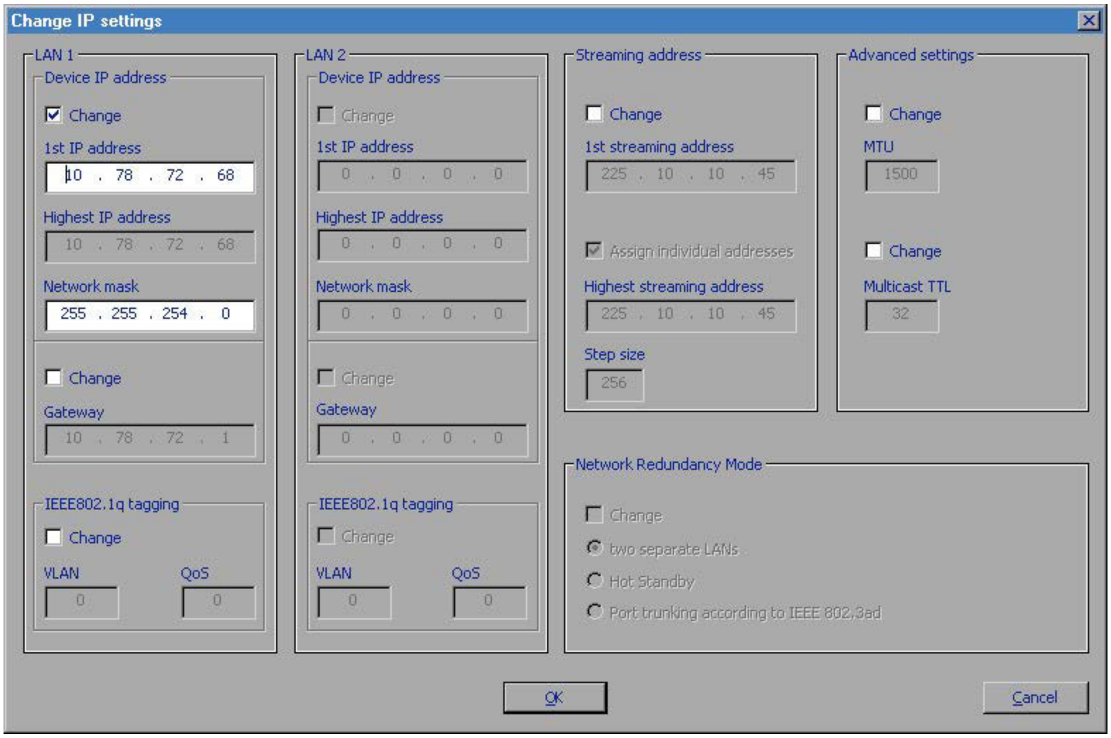
Filter criteria: Host Name

Filter text:

Devices found

Host Name	Type	IP Address	Subnet Mask	Gateway	Streaming	MAC Address	Firmware	Hardware	PCB Version
ENC8M2	ENC 8M2	10.78.72.68	255.255.254.0	10.78.72.1	225.10.10.45	00:0a:10:10:47:03	1.2.258	7	1.3.0.2
ENC8M2	ENC 8M2	10.78.72.67	255.255.254.0	10.78.72.1	225.10.10.35	00:0a:10:10:32:0a	1.2.258	7	1.2.0.0
ENC8M2	ENC 8M2	10.78.72.70	255.255.254.0	10.78.72.1	225.10.10.10	00:0a:10:10:5b:45	1.2.261	7	1.3.0.1

2. Right-click on the required encoder and then click IP Settings. The Change IP Settings dialog box is displayed.



LAN 1

Device IP address

☑ Change

1st IP address: 10 . 78 . 72 . 68

Highest IP address: 10 . 78 . 72 . 68

Network mask: 255 . 255 . 254 . 0

□ Change

Gateway: 10 . 78 . 72 . 1

IEEE802.1q tagging

□ Change

VLAN: 0 QoS: 0

LAN 2

Device IP address

□ Change

1st IP address: 0 . 0 . 0 . 0

Highest IP address: 0 . 0 . 0 . 0

Network mask: 0 . 0 . 0 . 0

□ Change

Gateway: 0 . 0 . 0 . 0

IEEE802.1q tagging

□ Change

VLAN: 0 QoS: 0

Streaming address

□ Change

1st streaming address: 225 . 10 . 10 . 45

☑ Assign individual addresses

Highest streaming address: 225 . 10 . 10 . 45

Step size: 256

Advanced settings

□ Change

MTU: 1500

□ Change

Multicast TTL: 32

Network Redundancy Mode

□ Change

● two separate LANs

○ Hot Standby

○ Port trunking according to IEEE 802.3ad

3. Under Streaming address area, select the Change check box to enable the 1st streaming address box.
4. Type the required multicast streaming IP address and then click OK. The Password box is displayed.
5. Type the password and then click OK. The IP address is updated and an Update Results status box is displayed.
6. Click OK to complete. Similarly you can change or assign the new IP address.
7. Add the encoder manually in NVR for video streaming.

Configuring Remote Analytics Server

This section explains how to configure the remote analytics server for Mask and Social Distancing. It also explains how to revert a remote server machine.

Scalable Analytics Server

This feature is introduced to manage the load on a NVR box while rendering analytics based cameras. Earlier only one local analytics server was available for multiple cameras that support analytics. This results in high consumption of CPU and low rendering capability of live video in NVR cameras.

Scalability feature helps customer to share the analytics server load on different remote machines and utilize the analytic algorithms efficiently. User can map the required cameras to each remote server and view the alarms in VMS,

A new tab named Analytics Server is introduced under Configurator tab to add additional analytics server and to choose the one while configuring Social Distancing, Mask compliance and SVMD features. This provides flexibility and increases the processing time to manage the load over analytics server when configuring multiple features.

- A maximum of 5 Analytics Remote boxes can be added under this tab.
- For each Analytics Remote box, 4 camera with 30 FPS and up to 8 cameras with 5 FPS can be assigned

Note: *If Mask & Social Distancing alarms are not coming after upgrading the NVR machine from previous market released version to current version (6.7) within stipulated time(15 Mins) then user need to restart the machine.*

Converting a NVR Machine to a Analytics Remote Server

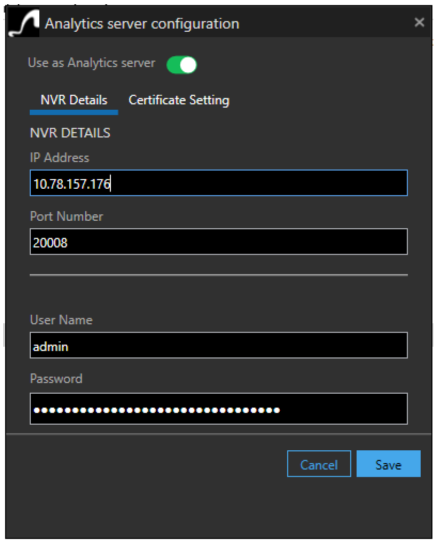
Any NVR machine can be converted into a Remote Analytics server to balance the analytics camera load on CPU. User need to ensure the below to convert a NVR machine to Analytics Server

- It should be an NVR machine without cameras. No cameras should be added
- All Neo services should be in stop state to minimize the load on analytic server.
- If you are using remote analytics servers, then ensure to enable encryption in remote analytics box as well. It is recommend to use different certificates for encryption. See How to Encrypt the Remote Analytic Server secion.

In order to do ease the above steps for user, MaproNvrAnalyticServerConfigUtility is introduced. User can configure this in Remote machine to convert it to analytics server machine.

How to configure Analytics Server

1. In Remote NVR machine, navigate to NVR Bin folder and locate MaproNvrAnalyticServerConfigUtility.
2. Run the Utility in Administrator mode. The Analytics Server Configuration dialog box appears.



Use as Analytics server: on

NVR DETAILS

IP Address: 10.78.157.176

Port Number: 20008

User Name: admin

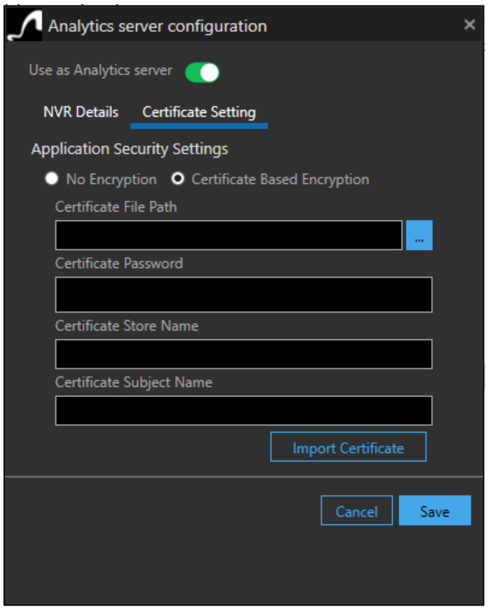
Password: ••••••••••••••••••••••••••••••••

3. Click the “Use as Analytics Server” toggle button to enable.
4. Under NVR Details, type the following details as explained below:
   - IP Address: This is IP address of the NVR machine where analytic cameras are added
   - Port Number of the NVR machine
   - User name and Password of the NVR machine
5. Click Save to complete the configuration.

Note: *If Mask & Social Distancing alarms are not coming in NVR machine from the remote analytic server even after applying the encryption, then user need to reapply the encryption certificate again in remote analytic server.*

How to Encrypt the Remote Analytic Server

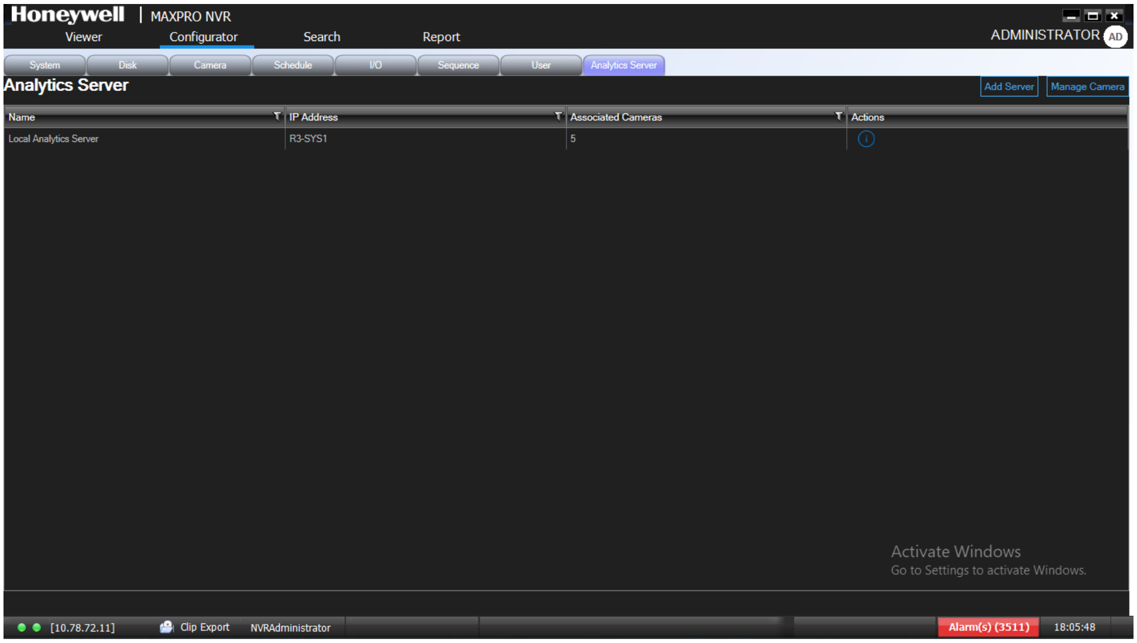
1. In Remote NVR machine, navigate to NVR Bin folder and locate MaproNvrAnalyticServerConfigUtility.
2. Run the Utility in Administrator mode. The Analytics Server Configuration dialog box appears.



3. Click the “Use as Analytics Server” toggle button to enable.
4. Click the Certificate Setting tab.
5. Under Application Security, click the Certificate Based Encryption option.
6. Type the following details as explained below:
    - Certificate File Path: Browse to select the certificate.
    - Certificate Password: Type the certificate Password
    - Certificate Store Name: Type the certificate Store Name
    - Certificate Subject Name: Type the certificate subject name
7. Click Import Certificate button.
8. Click Save to complete the configuration.

How to Add Analytics Server in NVR Machine

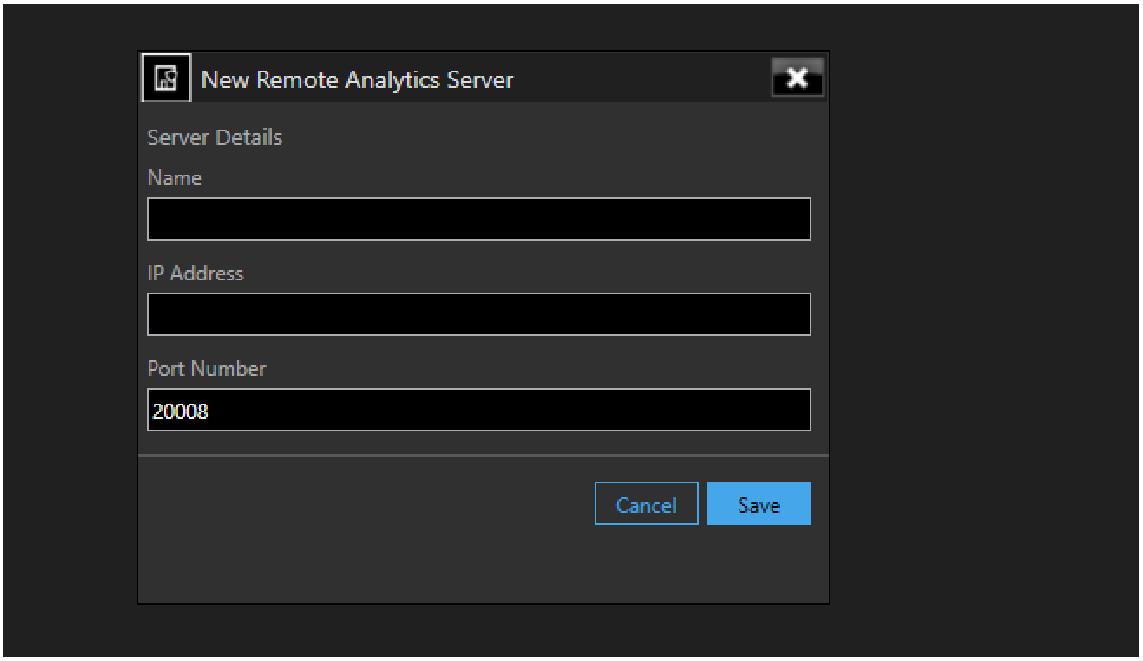
1. In the Configurator > Camera tab, click the Analytics Server tab. The Analytics Server screen is displayed with the list of analytics server already configured.



Analytics Server

Name	IP Address	Associated Cameras	Actions
Local Analytics Server	R3-SYS1	5	ⓘ

2. Click Add Server from the right most corner of the screen.



New Remote Analytics Server

Server Details

Name

IP Address

Port Number

20008

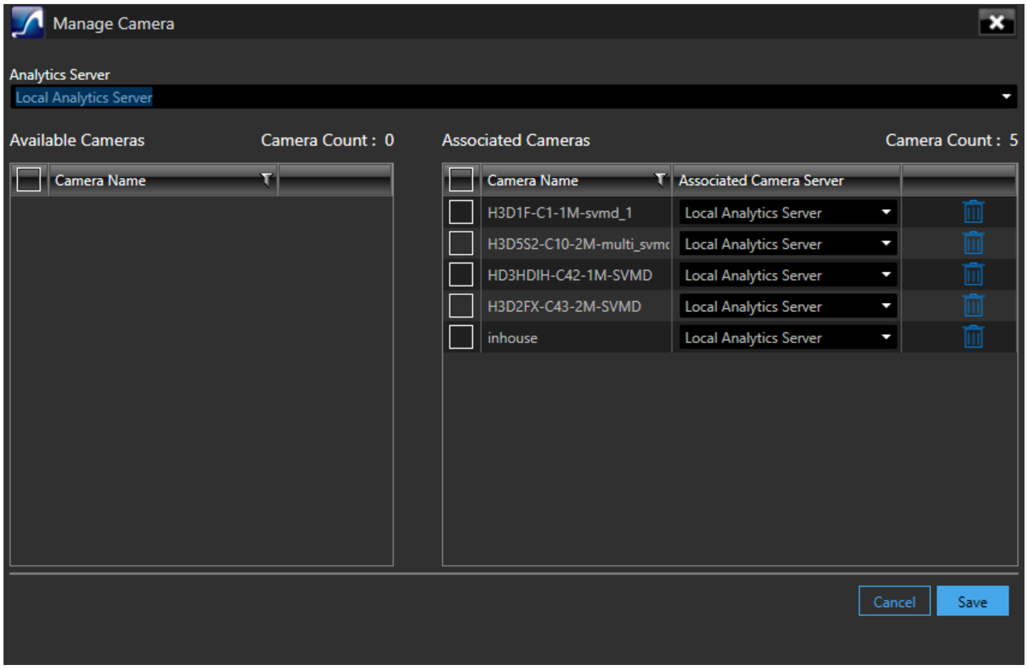
3. For the New Remote Analytics Server provide Server Name, IP Address and Port Number of the server.

4. Click Save to add the new analytics server.

Manging Cameras for Analytics Server

This window allows you to assign analytics server to multiple cameras in bulk. If you have multiple analytics server then you can associate specific cameras to view the alarms accordingly.

1. In the Analytics Server screen, click Manage Cameras from the right most corner of the screen. The Manage Camera dialog box is displayed.



Analytics Server: Local Analytics Server

Available Cameras — Camera Count : 0

□	Camera Name	

Associated Cameras — Camera Count : 5

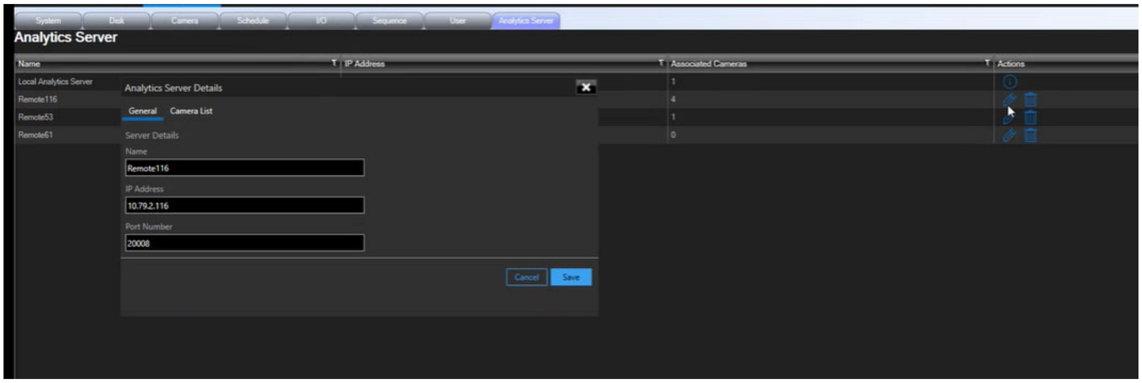
□	Camera Name	Associated Camera Server	
□	H3D1F-C1-1M-svmd_1	Local Analytics Server	🗑
□	H3D5S2-C10-2M-multi_svmc	Local Analytics Server	🗑
□	HD3HDIH-C42-1M-SVMD	Local Analytics Server	🗑
□	H3D2FX-C43-2M-SVMD	Local Analytics Server	🗑
□	inhouse	Local Analytics Server	🗑

2. From the Analytics Server drop-down, select the required server. This selection applies to all the cameras that will be associated in next steps.
3. From the Available Cameras pane, select the required camera check boxes to associate
4. Click Save. The selected cameras are displayed in Associated Cameras pane.

Note: *If you want to assign a different analytic server to a specific camera, then under Associated Cameras > Associated Camera Server, select the required server from the drop down list.*

Editing Remote Analytics Server Details

1. In the list of Analytics Server, click . The Analytics Server Details box is displayed. By default General tab is displayed.



Name	IP Address	Associated Cameras	Actions
Local Analytics Server		1	
Remote116		4	
Remote53		1	
Remote61		0	

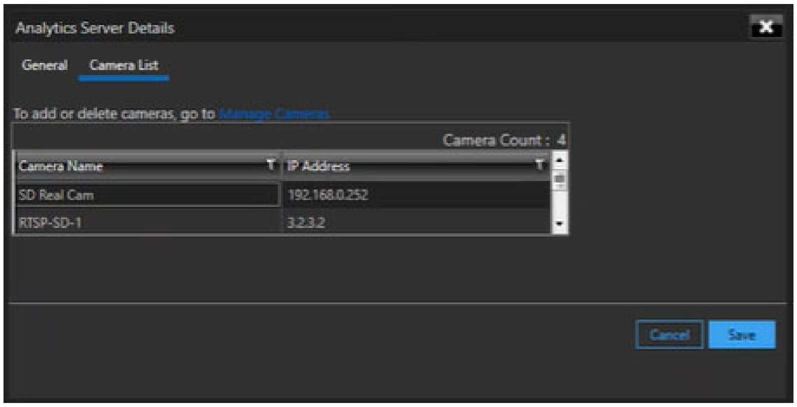
Name: Remote116

IP Address: 10.79.2.116

Port Number: 20008

2. Under Server Details, edit the Name, IP Address and Port number of the NVR machine.

3. Click Camera tab to view the list of cameras associated.



To add or delete cameras, go to Manage Cameras

Camera Count : 4

Camera Name	IP Address
SD Real Cam	192.168.0.252
RTSP-SD-1	3.2.3.2

4. To add or delete the associated cameras, then click the Manage Camera link to view the Manage Camera dialog box, See Manging Cameras for Analytics Server section.

5. Click Save.

Bulk configurations of cameras from NVR

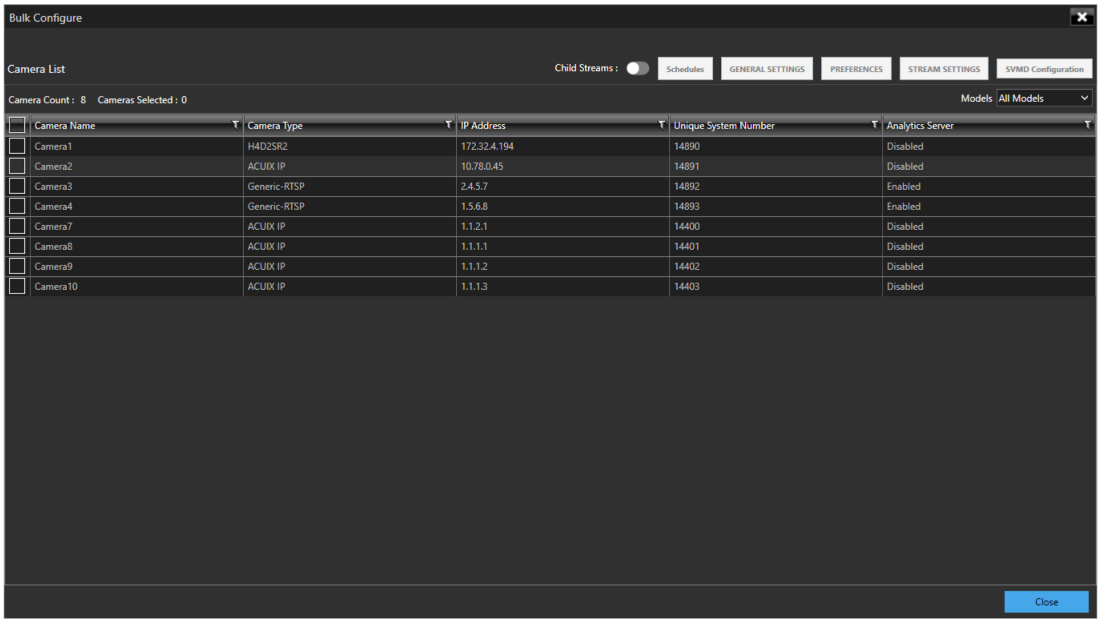
This feature allows you to perform Bulk camera configuration for main and sub stream’s, to ease the effort of configuring multiple cameras at the customer site. This feature improves the productivity for dealers and system integrators while configuring many NVRs. The configuration of cameras from the NVR is done one by one today (either post discovery or manual addition). This leads to higher lead time to configure and setup customer sites.

You can perform the following using Bulk configuration screen:

- General Settings
- Schedule Settings
- Preference Settings
- Stream Settings including child stream configurations specific to camera model
- SVMD Configuration

How to configure General Settings for cameras in bulk

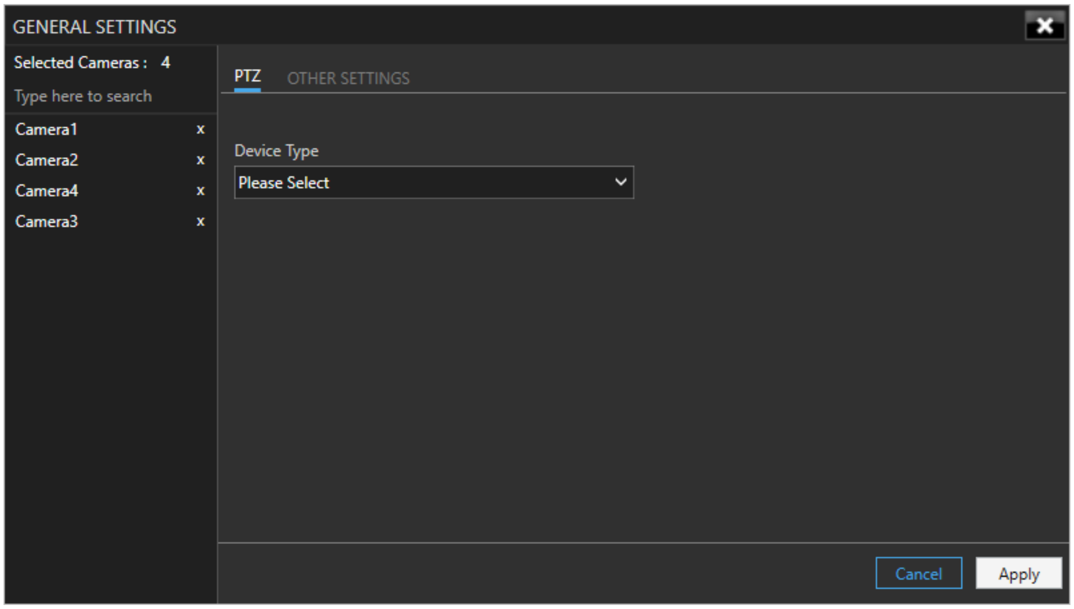
1. In the camera tab, click Bulk Configure button at the bottom of the screen. The Bulk Configure screen is displayed.



Camera Count : 8 Cameras Selected : 0

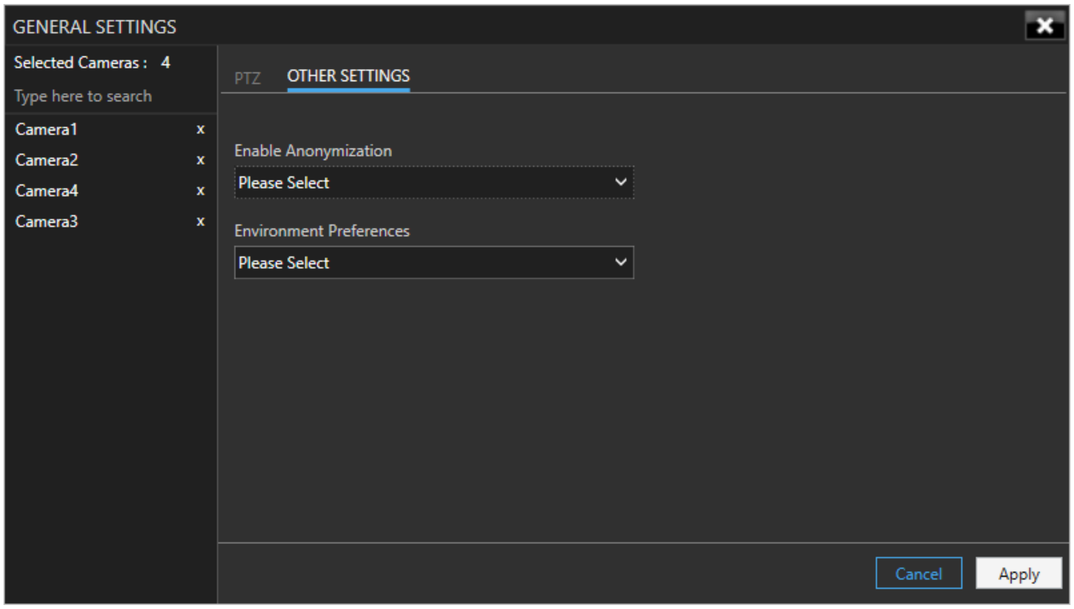
□	Camera Name	Camera Type	IP Address	Unique System Number	Analytics Server
□	Camera1	H4D2SR2	172.32.4.194	14890	Disabled
□	Camera2	ACUIX IP	10.78.0.45	14891	Disabled
□	Camera3	Generic-RTSP	2.4.5.7	14892	Enabled
□	Camera4	Generic-RTSP	1.5.6.8	14893	Enabled
□	Camera7	ACUIX IP	1.1.2.1	14400	Disabled
□	Camera8	ACUIX IP	1.1.1.1	14401	Disabled
□	Camera9	ACUIX IP	1.1.1.2	14402	Disabled
□	Camera10	ACUIX IP	1.1.1.3	14403	Disabled

2. Select the required number of camera check boxes and then click the General Setting button. The General Setting dialog box is displayed.



Note: *The Stream Settings and Preferences buttons will be enabled while configuring Child Streams. User need to enable Child Streams toggle button to configure streams.*

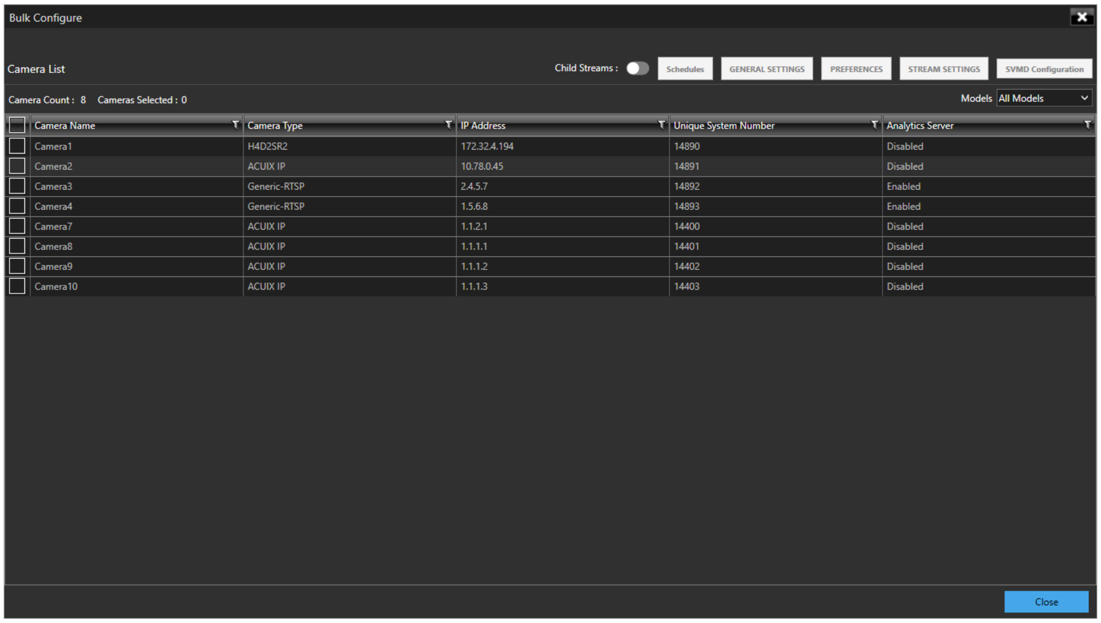
3. In PTZ tab, select the Device Type from the drop down list.
4. Click Other Settings tab, select Enable Anonymization and Environment Preferences options from the drop-down list.



5. Click Apply to complete general settings for the selected cameras.

How to configure Schedule Settings for cameras in Bulk

1. Navigate to the Bulk Configure screen.



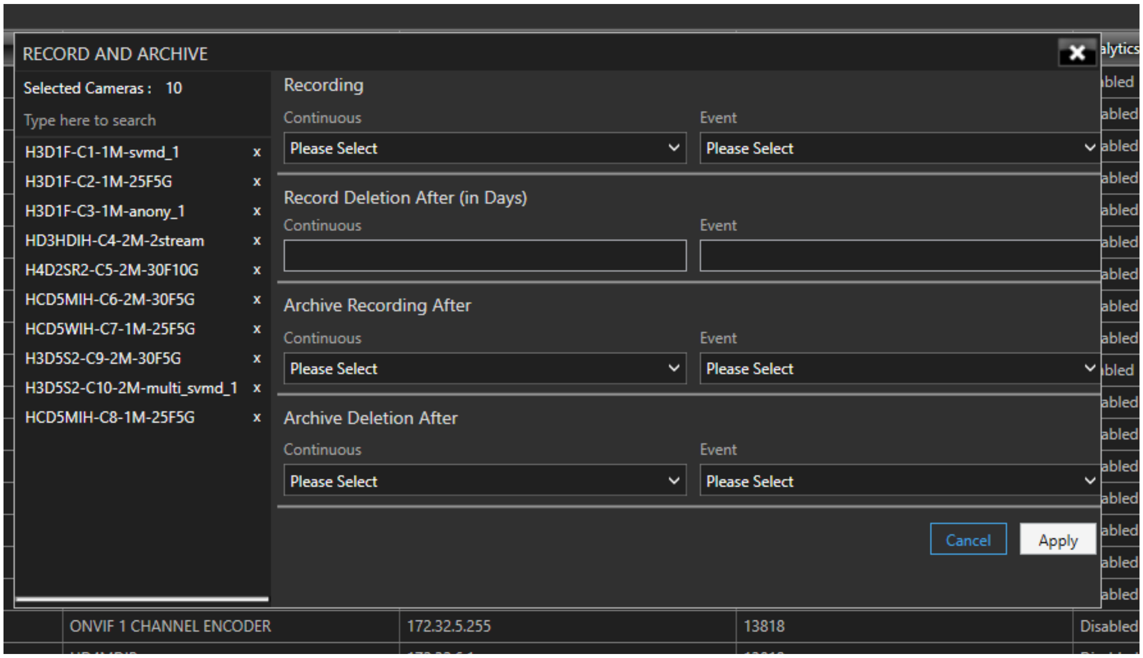
Bulk Configure

Camera List

Camera Count : 8   Cameras Selected : 0

□	Camera Name	Camera Type	IP Address	Unique System Number	Analytics Server
□	Camera1	H4D2SR2	172.32.4.194	14890	Disabled
□	Camera2	ACUIX IP	10.78.0.45	14891	Disabled
□	Camera3	Generic-RTSP	2.4.5.7	14892	Enabled
□	Camera4	Generic-RTSP	1.5.6.8	14893	Enabled
□	Camera7	ACUIX IP	1.1.2.1	14400	Disabled
□	Camera8	ACUIX IP	1.1.1.1	14401	Disabled
□	Camera9	ACUIX IP	1.1.1.2	14402	Disabled
□	Camera10	ACUIX IP	1.1.1.3	14403	Disabled

2. Select the required number of camera check boxes and then click the Schedule button. The Schedule dialog box is displayed.



RECORD AND ARCHIVE

Selected Cameras : 10

Type here to search

- H3D1F-C1-1M-svmd_1 x
- H3D1F-C2-1M-25F5G x
- H3D1F-C3-1M-anony_1 x
- HD3HDIH-C4-2M-2stream x
- H4D2SR2-C5-2M-30F10G x
- HCD5MIH-C6-2M-30F5G x
- HCD5WIH-C7-1M-25F5G x
- H3D5S2-C9-2M-30F5G x
- H3D5S2-C10-2M-multi_svmd_1 x
- HCD5MIH-C8-1M-25F5G x

Recording

Continuous: Please Select   Event: Please Select

Record Deletion After (in Days)

Continuous: Event:

Archive Recording After

Continuous: Please Select   Event: Please Select

Archive Deletion After

Continuous: Please Select   Event: Please Select

3. On Selected camera pane, the list of selected camera are displayed. You can also search and remove the cameras from here.

4. Select and enter the following as explained below:

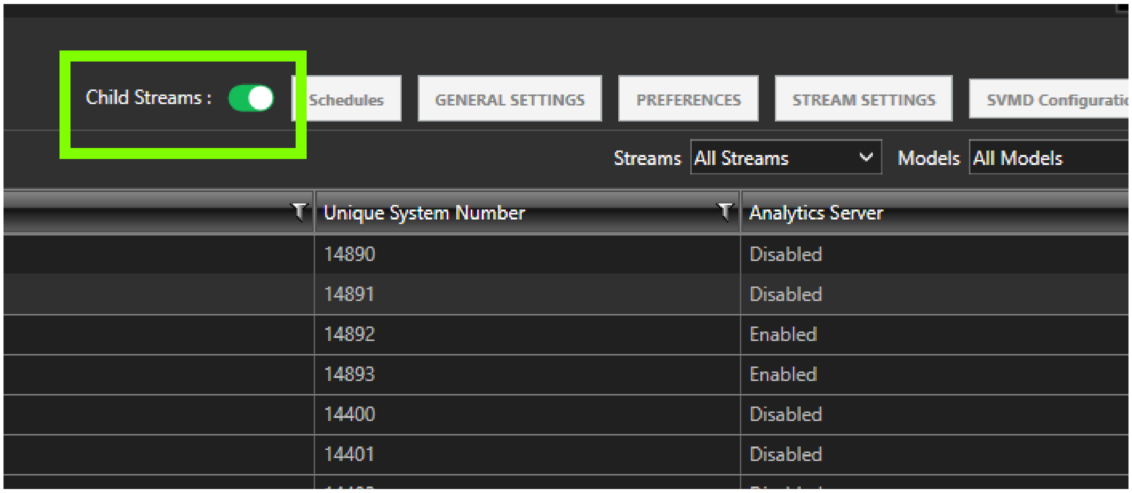
- Continuous - Select the FPS for Continuous recording.
- Event - Select the FPS for Event based recording.
- Recording Deletion After (In Days):
  - Select the Event Recording video deletion duration.
  - Select the Continuous Recording video deletion duration.
- Archive Recording After:
  - Continuous - This is “None” by default. Select an option from the drop-down if you want to archive the continuous recording.
  - Event - This is “None” by default. Select an option from the drop-down if you want to archive the event recording.
- Archive Deletion After Recording After:
  - Continuous Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived continuous recording can be deleted.
  - Event Recording - This is “365 Days” by default. Select the number of days from the drop-down after which the archived event recording can be deleted

5. Click Apply to complete the configuration.

How to configure Preferences for cameras in Bulk

Note: *Preferences setting is applicable only to the specific stream index. User has to select same stream either stream 1 2 or 3 and then click preference to apply settings .*

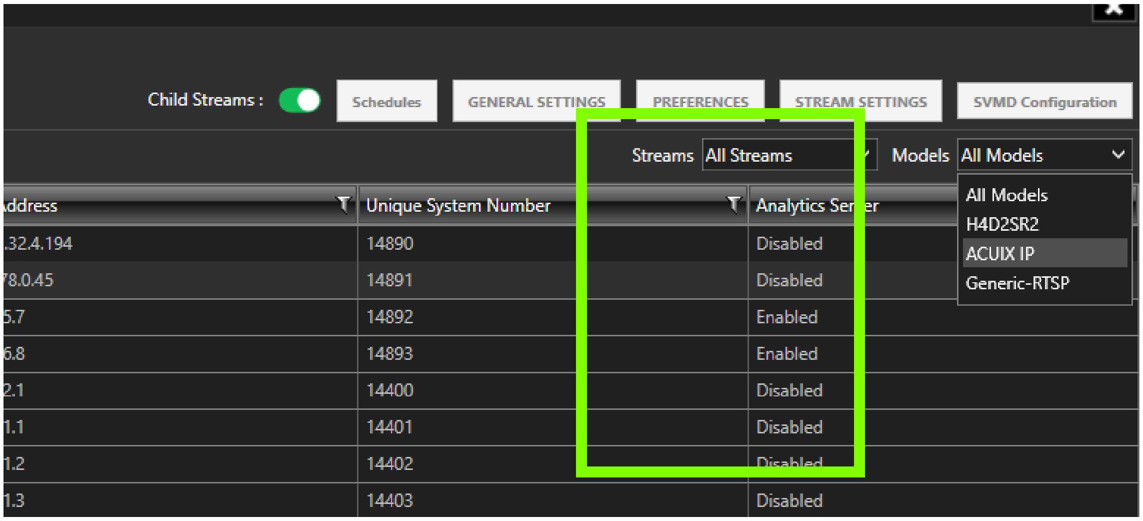
1. Navigate to the Bulk Configure screen and then enable the Child Streams toggle button as shown below.



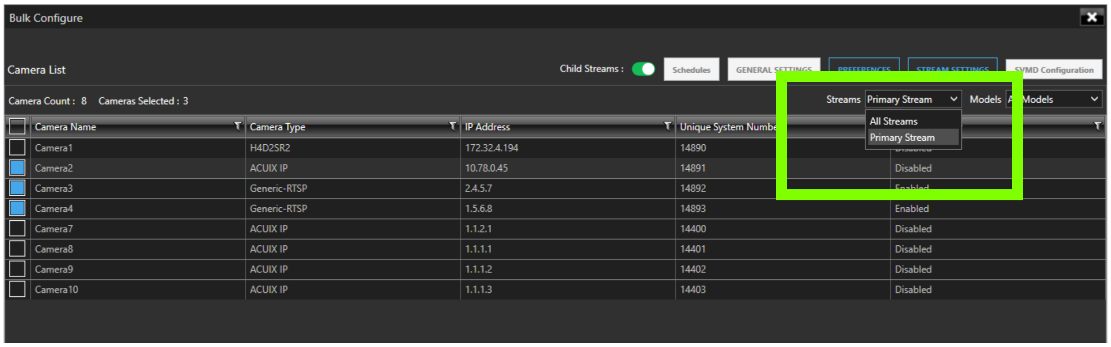
Streams All Streams Models All Models

	Unique System Number	Analytics Server
	14890	Disabled
	14891	Disabled
	14892	Enabled
	14893	Enabled
	14400	Disabled
	14401	Disabled

2. Select the required cameras of same stream.
   Or
   Select the required stream from the Streams drop-down list as shown below.



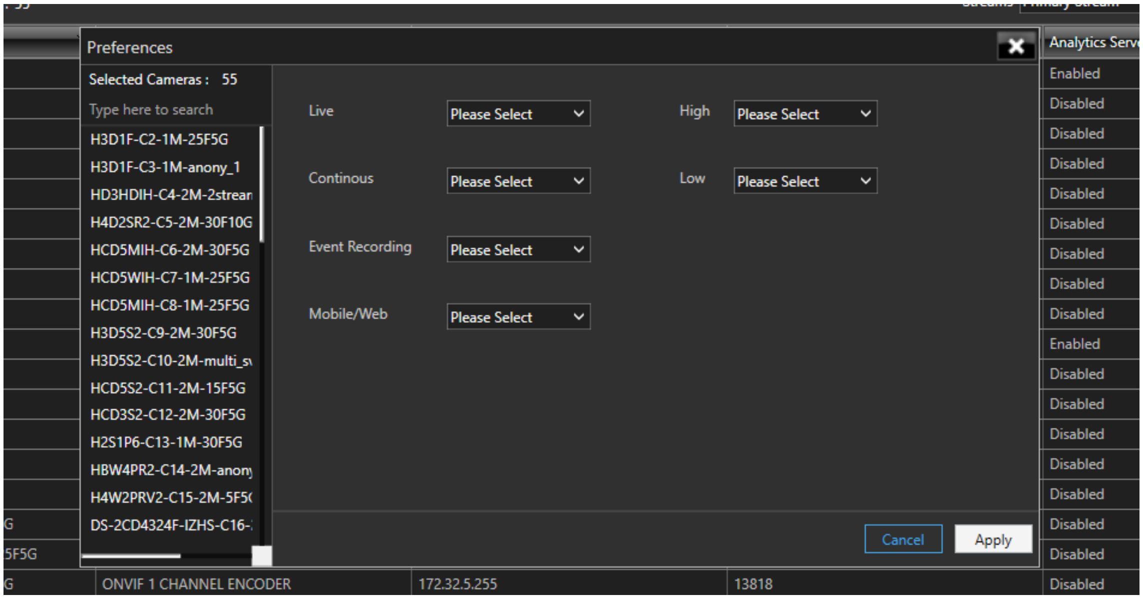
ddress	Unique System Number	Analytics Ser er
.32.4.194	14890	Disabled
78.0.45	14891	Disabled
5.7	14892	Enabled
6.8	14893	Enabled
2.1	14400	Disabled
1.1	14401	Disabled
1.2	14402	Disabled
1.3	14403	Disabled



Camera Count : 8   Cameras Selected : 3

☐	Camera Name	Camera Type	IP Address	Unique System Numbe	
☐	Camera1	H4D2SR2	172.32.4.194	14890	Disabled
☑	Camera2	ACUIX IP	10.78.0.45	14891	Disabled
☑	Camera3	Generic-RTSP	2.4.5.7	14892	Enabled
☑	Camera4	Generic-RTSP	1.5.6.8	14893	Enabled
☐	Camera7	ACUIX IP	1.1.2.1	14400	Disabled
☐	Camera8	ACUIX IP	1.1.1.1	14401	Disabled
☐	Camera9	ACUIX IP	1.1.1.2	14402	Disabled
☐	Camera10	ACUIX IP	1.1.1.3	14403	Disabled

3. Click the Preferences button. The Preferences dialog box is displayed.



Selected Cameras : 55

Type here to search

- H3D1F-C2-1M-25F5G
- H3D1F-C3-1M-anony_1
- HD3HDIH-C4-2M-2strean
- H4D2SR2-C5-2M-30F10G
- HCD5MIH-C6-2M-30F5G
- HCD5WIH-C7-1M-25F5G
- HCD5MIH-C8-1M-25F5G
- H3D5S2-C9-2M-30F5G
- H3D5S2-C10-2M-multi_s
- HCD5S2-C11-2M-15F5G
- HCD3S2-C12-2M-30F5G
- H2S1P6-C13-1M-30F5G
- HBW4PR2-C14-2M-anony
- H4W2PRV2-C15-2M-5F5(
- DS-2CD4324F-IZHS-C16-

Live: Please Select

Continous: Please Select

Event Recording: Please Select

Mobile/Web: Please Select

High: Please Select

Low: Please Select

4. On Selected camera pane, the list of selected camera are displayed. You can also search and remove the cameras from here

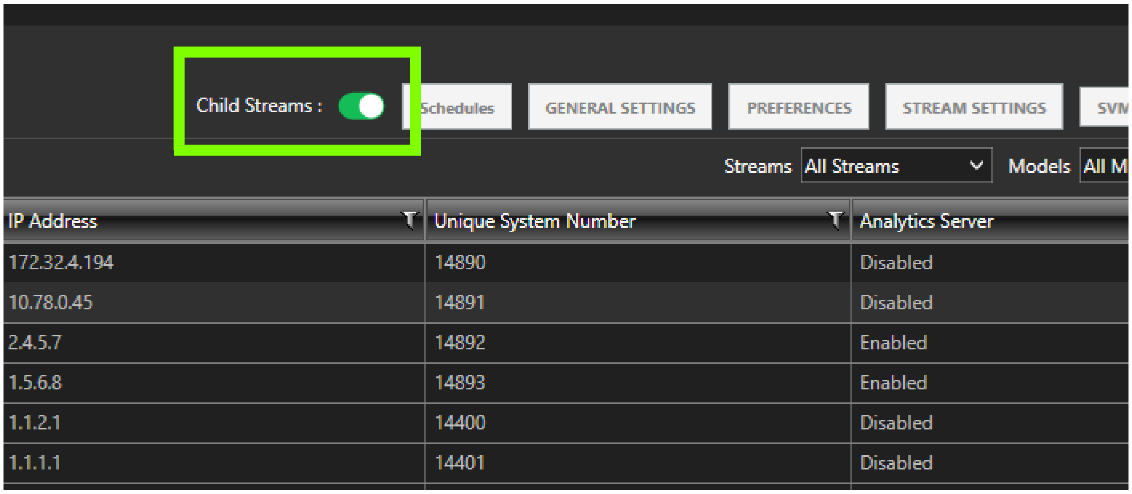
5. Perform the following as explained below:

- Live - Select the preferred stream of the camera which you want to use for streaming live video.
- Continuous - Select the preferred stream of the camera which you want to record continuously.
- Event Recording - Select the preferred stream of the camera which you want to record on events.
- Mobile/Web - Select the preferred stream of the camera which you want to use for streaming in Mobile/Web application.
- High - Select the preferred stream of the camera which you want to categorize as High Resolution stream.
- Low - Select the preferred stream of the camera which you want to categorize as Low Resolution stream.
- Click Apply to complete the configuration

How to configure Stream Settings for cameras in Bulk

Note: *Stream setting is applicable only to the specific camera models. User need to select the camera models which supports multiple streams.*

1. Navigate to the Bulk Configure screen and then enable the Child Streams toggle button as shown below.

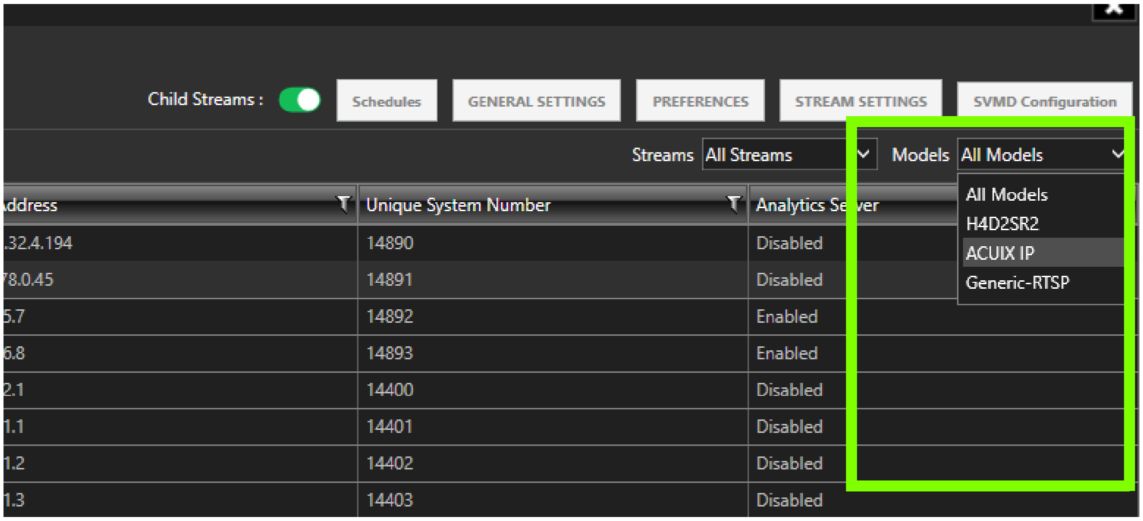


Streams All Streams Models All M

IP Address	Unique System Number	Analytics Server
172.32.4.194	14890	Disabled
10.78.0.45	14891	Disabled
2.4.5.7	14892	Enabled
1.5.6.8	14893	Enabled
1.1.2.1	14400	Disabled
1.1.1.1	14401	Disabled

2. Select the required cameras of same model.
   Or
   Select the required model of camera from the Model drop-down list a shown below.

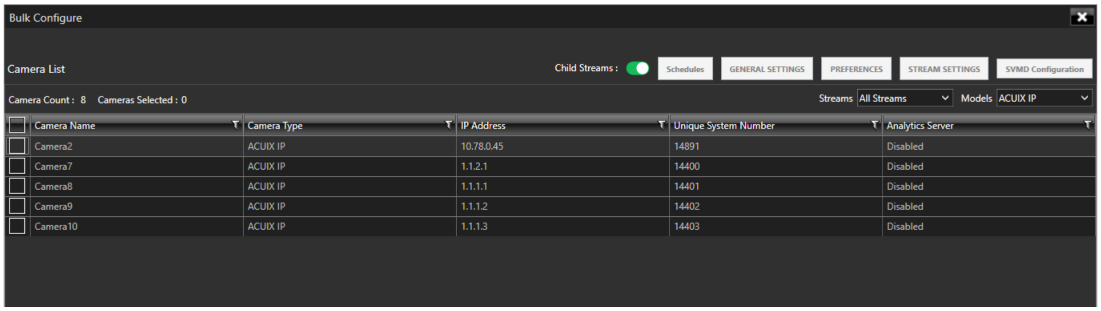
Note: *If cameras with different models are selected then a message, Stream of same model should be selected is displayed at the bottom of the screen. Click OK to proceed.*



Streams All Streams Models All Models

ddress	Unique System Number	Analytics Server
.32.4.194	14890	Disabled
78.0.45	14891	Disabled
5.7	14892	Enabled
6.8	14893	Enabled
2.1	14400	Disabled
1.1	14401	Disabled
1.2	14402	Disabled
1.3	14403	Disabled

The selected models are displayed as shown below:



Bulk Configure

Camera List

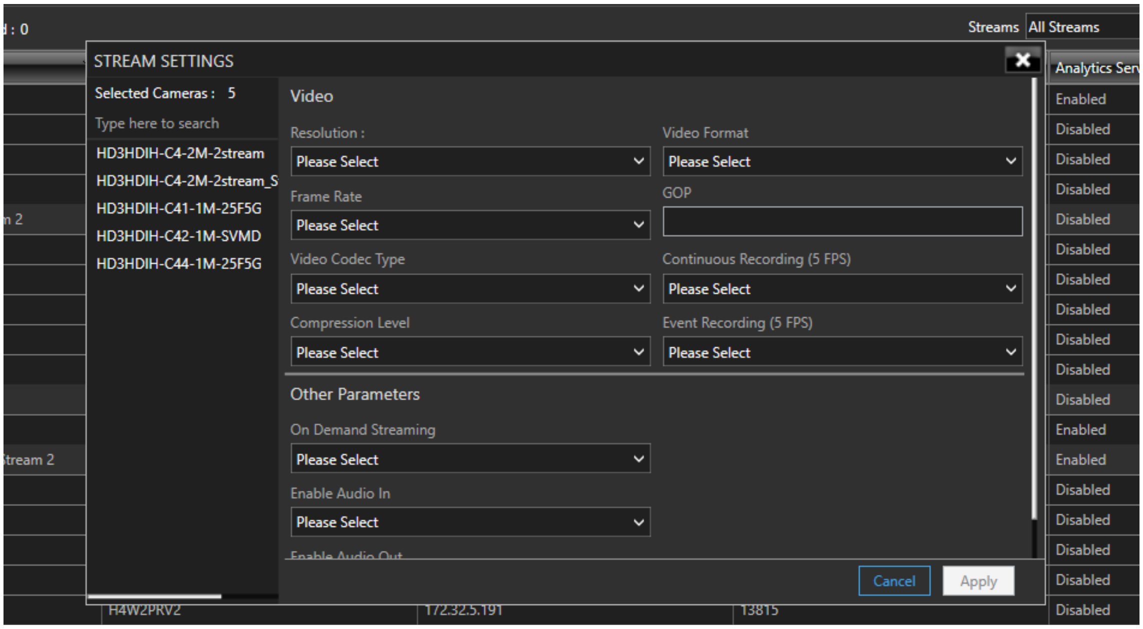
Child Streams : ● Schedules | GENERAL SETTINGS | PREFERENCES | STREAM SETTINGS | SVMD Configuration

Camera Count : 8 Cameras Selected : 0

Streams: All Streams Models: ACUIX IP

□	Camera Name	Camera Type	IP Address	Unique System Number	Analytics Server
□	Camera2	ACUIX IP	10.78.0.45	14891	Disabled
□	Camera7	ACUIX IP	1.1.2.1	14400	Disabled
□	Camera8	ACUIX IP	1.1.1.1	14401	Disabled
□	Camera9	ACUIX IP	1.1.1.2	14402	Disabled
□	Camera10	ACUIX IP	1.1.1.3	14403	Disabled

3. Click the Stream Setting button. The Stream Setting dialog box is displayed.



STREAM SETTINGS

Selected Cameras : 5

Type here to search

- HD3HDIH-C4-2M-2stream
- HD3HDIH-C4-2M-2stream_S
- HD3HDIH-C41-1M-25F5G
- HD3HDIH-C42-1M-SVMD
- HD3HDIH-C44-1M-25F5G

Video

Resolution : Please Select

Video Format: Please Select

Frame Rate: Please Select

GOP:

Video Codec Type: Please Select

Continuous Recording (5 FPS): Please Select

Compression Level: Please Select

Event Recording (5 FPS): Please Select

Other Parameters

On Demand Streaming: Please Select

Enable Audio In: Please Select

Enable Audio Out

Cancel | Apply

4. On Selected camera pane, the list of selected camera are displayed. You can also search and remove the cameras from here

5. Under Video configure the following as explained below:

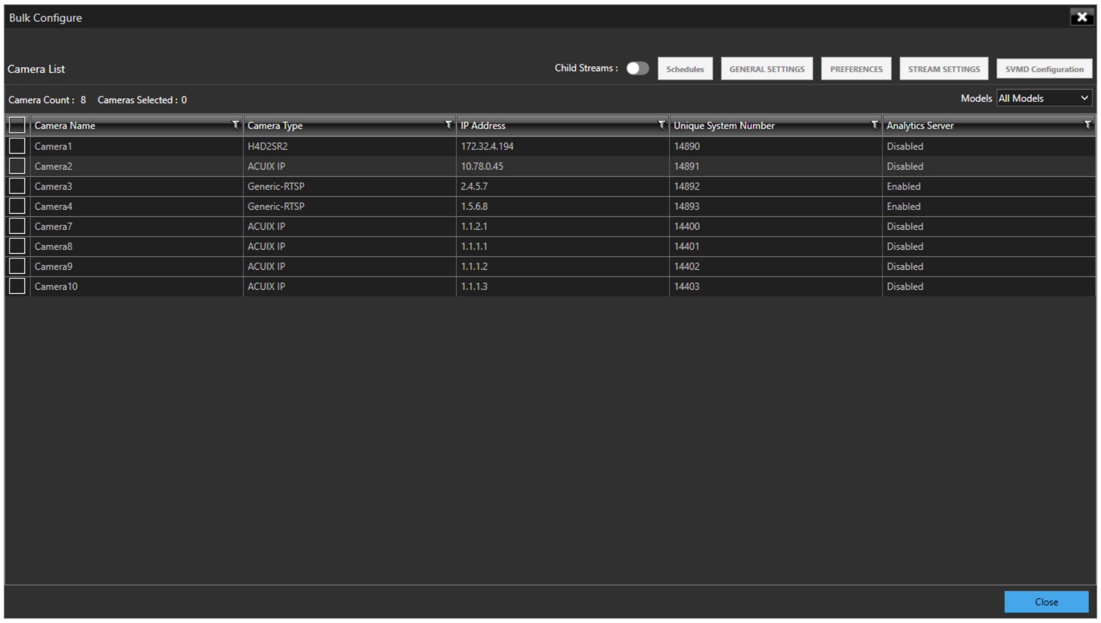
- Resolution - The Resolution is defaulted based on the camera model (for example, HD3MDIP model defaults to 1280 x 720 resolution).
- Frame Rate - Select the FPS for a camera. FPS refers to the number of pictures displayed in exactly one second. FPS is a measure of how much information is used to store and display motion video. The term applies to digital video. Each frame is a still image; displaying frames in quick succession creates the illusion of motion.
- Video Codec Type - Select the Codec type for the camera. This is populated based on the camera model selected. H.265 cameras can render in both CPU and GPU modes.
- Compression Level - The Compression Level is defaulted to “Medium”. You can select a new Compression ratio as applicable.

- Video Format - Select the Video Format (NTSC or PAL). The NTSC and PAL are the widely used video formats.
- GOP - Type a new GOP as applicable. Group of Pictures (GOP) are individual frames (number of pictures) that are grouped together and played back for viewing. A GOP consists of “IFrame” picture type that represents a fixed image independent of other picture types. Each GOP begins with this type of picture.
- Continuous Recording (5 FPS) - Select the FPS for Continuous recording.
- Event Recording (5 FPS) - Select the FPS for Event based recording.
- Under Other Parameters
  - Select the On Demand Streaming options from the drop-down list.
  - Enable Audio In/Out: This is for audio supported camera. Select the required In and Out option from the drop-down list.

6. Click Apply to complete the configuration

How to configure SVMD for cameras in bulk

1. Navigate to the Bulk Configure screen.

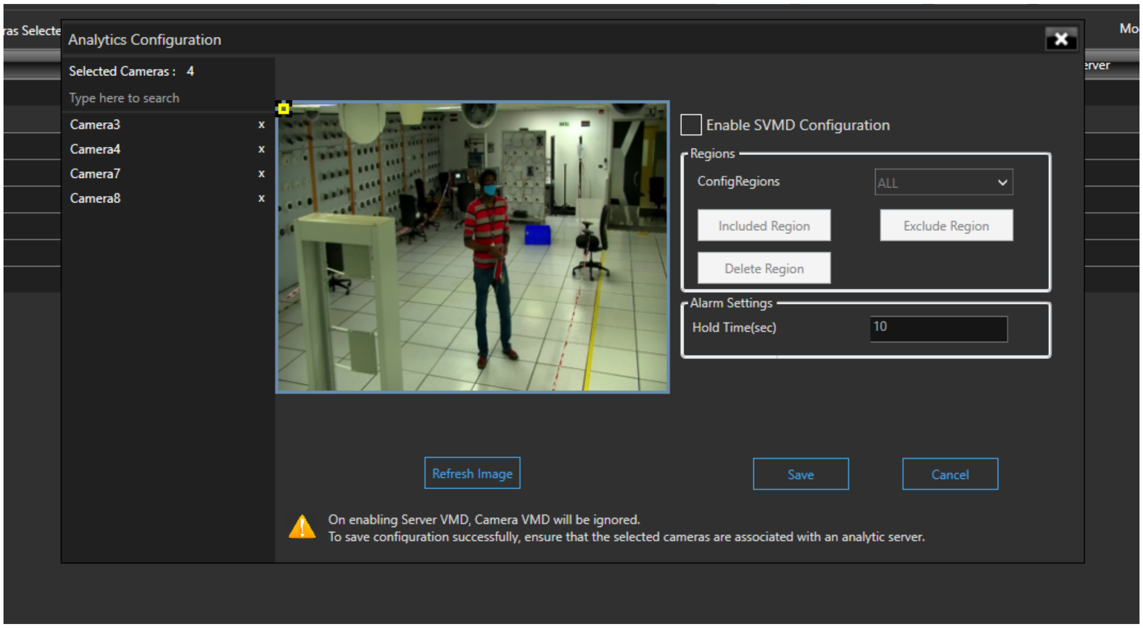


Camera Count : 8 Cameras Selected : 0

Models All Models

□	Camera Name	Camera Type	IP Address	Unique System Number	Analytics Server
□	Camera1	H4D2SR2	172.32.4.194	14890	Disabled
□	Camera2	ACUIX IP	10.78.0.45	14891	Disabled
□	Camera3	Generic-RTSP	2.4.5.7	14892	Enabled
□	Camera4	Generic-RTSP	1.5.6.8	14893	Enabled
□	Camera7	ACUIX IP	1.1.2.1	14400	Disabled
□	Camera8	ACUIX IP	1.1.1.1	14401	Disabled
□	Camera9	ACUIX IP	1.1.1.2	14402	Disabled
□	Camera10	ACUIX IP	1.1.1.3	14403	Disabled

2. Select the required number of camera check boxes and then click the SVMD Configuration button. The Analytics Configuration dialog box is displayed.



Selected Cameras : 4

Camera3 x
Camera4 x
Camera7 x
Camera8 x

□ Enable SVMD Configuration

ConfigRegions: ALL

Hold Time(sec): 10

On enabling Server VMD, Camera VMD will be ignored.
To save configuration successfully, ensure that the selected cameras are associated with an analytic server.

Note: *The Image what u see here is from first camera of NVR*
Only Enable SVMD and Region configuration can be done in this dialog box. Associating cameras to Analytics server has to be done from either camera configuration window or from Analytics Server tab.

3. Select the Enable SVMD Configuration check box
4. Under Regions, click the Include Region button to create required numbers of region(s) on the image.
5. Select the required region to display from the Region drop-down. Available options are All, None or (Region 1, 2, 3 and so on). Configure the Object size threshold if required.
6. If you want to exclude any region then select the region using mouse and then click Exclude Region button.
7. Under Alarm Settings, set the Alarm Hod time in seconds.
8. Click Save to complete the configuration.

Bi-Directional Audio Support for MAXPRO NVR

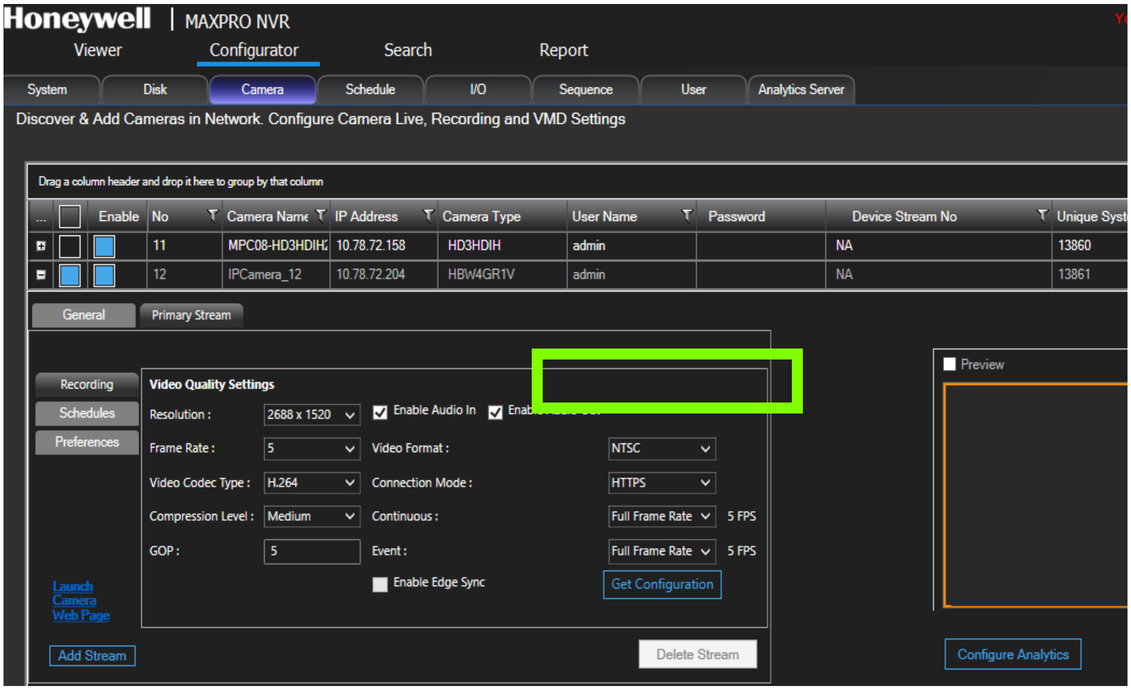
This feature helps an operator to send Bi-directional audio warnings/messages to any audio output of cameras from MAXPRO VMS machines. Currently Mic and speech is supported from VMS viewer only.

This feature supports standard audio Codec format G.711 ulaw and only Honeywell ONVIF Camera model are supported.

Note: *Only Honeywell ONVIF Camera models are supported.*
Only fixed G.711 ulaw Codec format is supported.
Mutlistream is supported, but can be enabled in only one stream at a time.
It is recommended for the user to enable and speak for one camera at a time.
Windows 2016, 2019 windows server machines are not supported for beta release.

How to configure Bi-Directional Audio for a camera

1. In NVR, for a Honeywell Onvif camera, navigate to Camera properties > Primary Stream > Recording tab.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

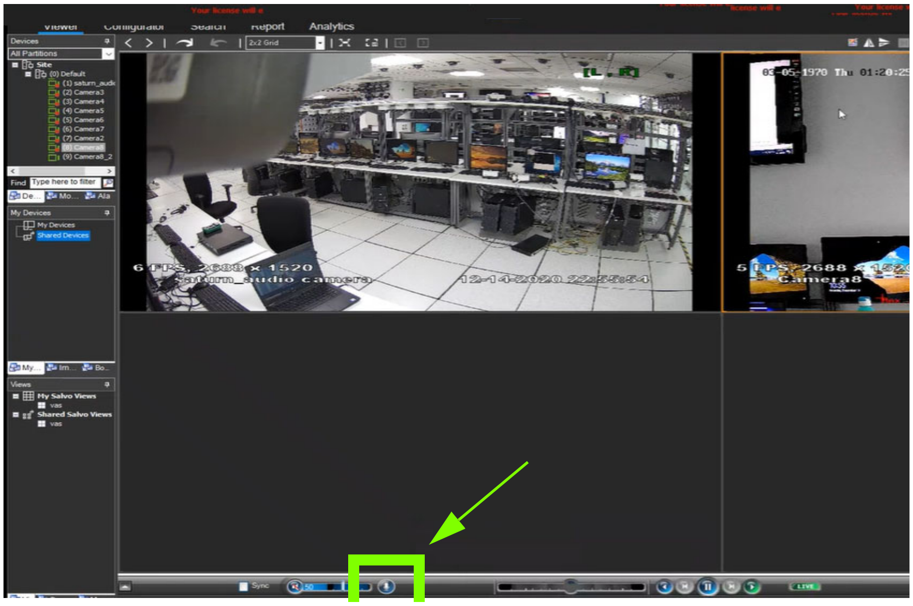
Drag a column header and drop it here to group by that column

...	☐	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique Syst
⊞	☐	■	11	MPC08-HD3HDIH	10.78.72.158	HD3HDIH	admin		NA	13860
⊟	■	■	12	IPCamera_12	10.78.72.204	HBW4GR1V	admin		NA	13861

Video Quality Settings

Resolution :	2688 x 1520	☑ Enable Audio In	☑ Enab
Frame Rate :	5	Video Format :	NTSC
Video Codec Type :	H.264	Connection Mode :	HTTPS
Compression Level :	Medium	Continuous :	Full Frame Rate 5 FPS
GOP :	5	Event :	Full Frame Rate 5 FPS
		☐ Enable Edge Sync	

2. For a specific stream, select the Enable Audio In/Out check boxes as explained below:
   - Enable Audio In: Camera to VMS Operator
   - Enable Audio Out: Operator to camera connected with speakers.
3. In VMS > Viewer screen. select the audio enabled camera in the panel (One at a time) and then enable the Mic button on the Timeline bar to speak and Disable the Mic button to end the speech as highlighted below.



Limitation

- AAC compression format is not supported for Audio Out from MAXPRO NVR. It is recommended to configure G711 u law as Audio Out compression format in the camera webpage.
- From NVR to VMS, user will notice a latency of 1.5 Seconds in audio.

Series 60 Camera Integration

MAXPRO VMS R670 supports Series 60 Camera integration with MAXPRO NVR 6.7 recorder. The following tables explain the list of supported camera models, and events/alarms supported.

Type	Camera Models	Firmware Details
Premium Model	HC60W35R2	Honeywell_60-Series_IPC_HC60WXXRX_V1.0.21.20200828
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	

Series60 IR PTZ	HC60WZ5R30	
Series30	HC30W25R3-12V	

Configuring Social Distancing ROI Duration and Show

User can configure the Registry entries to increase the duration of alarms generation for a specific time and highlight the same using color indication.

Following are the two parameters that are allowed to configure:

- sdGraphicROIDuration : The Non-complaint Social Distancing Regions alarm is generated for every 5 hours (By Default). The Value of this key is in Minutes (By Default 300 Mins (5 hours))
- sdGraphicROIShow: This key is used for displaying when alarm occurs then in live view user can see the regions in specific color coding based on number of violations occurred. For example
- the highest violated region more than 80% is RED
- 20 to 80 percent region violated is YELLOW
- the succeeding less value (Les than 0) is displayed in GREEN

Perform the below steps to modify the values:

1. Navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\TrinityFramework\RenderingServer
2. Locate sdGraphicROIDuration and then change the value (By Default 300 Mins (5 hours)).
3. Locate the sdGraphicROIShow and then change the color code value.

This page is intentionally left blank

CHAPTER

7 VERIFYING THE CONFIGURATION

Overview

Verifying the configuration of the MAXPRO NVR is the final phase in the commissioning process. In this phase, you need to verify the working of the MAXPRO NVR.

Before you Begin

Ensure that the configuration of MAXPRO NVR is complete.

Activities to Perform in this Phase

In this phase, using the MAXPRO NVR user interface, check for the following one after the other.

- Connection with the MAXPRO NVR sever (logging on)
- Camera listing in the devices window
- Live video display from cameras
- Playback of recorded video
- Inserting comments and marking the point of interest using the bookmark feature in Timeline window
- Playback of loop (mark in and mark out feature) in Timeline window
- Panning, tilting, and zooming functions
- Acknowledgment of alarms and clearing of alarms
- Image creation
- Clip creation
- Video from the surrounding cameras (video pursuit or surrounding cameras feature in MAXPRO NVR)
- Saving the salvo layout using the salvo view feature
- Searching recorded video in MAXPRO NVR

- Generating and viewing the event and operator log report

Checking the Connection with the MAXPRO NVRServer

The MAXPRO NVR server addresses are stored in profiles. You can save the address of each server in profiles from the Log On dialog box that appears when you start MAXPRO NVR.

To connect to a MAXPRO NVR server from the client computer

Step 1. In the Username box, type the user name. The default user name is “admin”.

Step 2. In the Password box, type the password. The default password is “trinity”.

Note: *Honeywell recommends to create a new NVR user (See Adding a User) in the Configurator tab and use the same to logon.*

Step 3. In the Profile box, select the profile in which the server address is saved.

Step 4. Click Login. The Viewer Screen appears.

You can set a profile as the default profile. When a profile is set as default, you need not select the profile each time you log on to MAXPRO NVR. You can also modify and delete profiles.

Note: *See the Configuring MAXPRO NVR Windows/ Desktop Client section on page 124 for more information on how to save server addresses in profiles, how to set a profile as default profile, and how to modify and delete the profiles.*

Checking the Device listing in the Devices Window

By default, the Viewer tab is selected when you log on to MAXPRO NVR. The Devices window in the Viewer tab lists the IP cameras connected to and discovered by MAXPRO NVR.

See the Getting to Know the MAXPRO NVR User Interface section on page 130 for more information on the Device window.

Checking the Acknowledgment and Clearing of Alarms

Clicking the Alarms tab next to the Device tab opens the Alarms window that lists all the alarms in a floating window. You can acknowledge and clear the alarms.

Alarms notify the occurrence of events to the operators. You can configure alarms to be triggered when events such as recorder disk space nearing full, motion detection, and others happen. The events that trigger an alarm can be selected while configuring the recorders, cameras, and switchers. The events can be associated to event groups.

Each alarm goes through the following states.

New or Unacknowledged

When an alarm is triggered it appears in the Alarm window. You can click the Alarm tab to view the Alarm window. The state of the alarm after it is triggered is referred to as unacknowledged. You can view the list of all the unacknowledged alarms in a table in the Alarm window.

See the Getting to Know the MAXPRO NVR User Interface section on page 130 for more information on the Alarms.

Checking the Live Video from Cameras

To ensure that all the cameras are connected and functioning properly, you need to check for live video from them.

To select the cameras and view live video

- Double-click a camera in the Devices window.
  Or
  You can also drag a camera to a panel in the salvo layout. The panel starts displaying live video.

You can select multiple cameras and view live video in different panels of the salvo layout.

See the Getting to Know the MAXPRO NVR User Interface section on page 130 for more information on how to view live video from cameras.

Checking the Playback of Recorded Video

To playback video, the recording from the camera must be available and the recording settings for the camera must be configured. Recorded video can be played from the Timeline window.

The following operations can be performed on the recorded video.

- Playing recorded video using the timeline
- Playing recorded video using Mark In and Mark Out points in timeline
- Marking points of interest in the timeline using bookmarks

Refer to the *MAXPRO® NVR Operator's Guide* for more information on how to configure the recording settings for the cameras connected to MAXPRO NVR.

Checking the Panning, Tilting, and Zooming

Using the digital PTZ feature in MAXPRO NVR, you can perform panning and tilting on live and recorded video and clips. The digital PTZ feature when enabled allows you to perform panning and tilting on the video display that is zoomed or enlarged in a panel.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on PTZ.

Checking the Creation of Images

A frame of video displayed in the panel can be saved as an image. The image can be saved in Bitmapped Graphics (BMP), Joint Photographic Experts Group (JPG) format, Portable Graphics format (PNG), and Graphics Interchange Format (GIF).

Only the images saved in the Snapshots/Clips folder at the location in the hard drive in which MAXPRO NVR files are installed can be viewed in the Snapshot/ Clip window.

You can double-click the image view option in the site window to view images on the salvo layout. You can view the images in the form of thumbnails or filmstrip. You can also select the image size large, medium, and small as per the requirement.

For example, X:\ProgramFiles\Honeywell\TrinityFramework\Snapshots/Clips. Here, X: is the hard drive.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on creating the images.

Checking the Creation of Clips

You can create clips from recorded video. These clips can be saved with digital signatures. Digital signatures ensure authenticity of clips. Digital signatures are primarily used to authenticate videos that are produced in courts as evidence. A digital signature generates a unique string for the clip using algorithms recommended by the W3C. The World Wide Web Consortium (W3C) is an international consortium where member organizations, a full-time staff, and the public work together to develop Web standards. If the video in the clip is modified, a verification check for the unique string fails indicating that the content is tampered. When a clip is saved with the digital signature, a package file with the .PKG extension is created to save the clip.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on creating clips.

Checking the Salvo View Feature

A salvo layout that is customized based on the preferences of the operators is referred to as a salvo view. Cameras and scan sequences that are selected frequently and the preferred salvo layout can be saved as a salvo view.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on how to create, select, and manage salvo views.

Checking the Search for Recorded Video in MAXPRO NVR

Operators can search for recorded video from cameras connected to MAXPRO NVR. The search results can be filtered based on conditions like video recorded today, yesterday, and others.

You can search for recorded video from the Search tab.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on how to search for recorded video, and how to play the search results.

Checking the Generation of Event History/ Operator Log Report

Two types of reports, namely event history report and operator log report, can be generated.

The event history report can be generated for cameras, monitors, and recorders. The event history report lists the events related to a device during a time period. For example, for a camera, you can generate the event history report to know the occurrence of events like enabling of camera motion detection, starting of background recording, and so on.

The operator log report can be generated to view the activities performed by users. The operator log report lists the activities performed by users during a time period. For example, creating clips, adding bookmarks.

You can generate reports from the Report tab.

Refer to the *MAXPRO® NVR Operator's Guide* for more information on how to generate and view the reports.

This page is intentionally left blank.

CHAPTER

8 UPGRADE MAXPRO NVR SOFTWARE

Overview

This chapter describes the procedures to upgrade the MAXPRO NVR software. Follow the appropriate section in this chapter to upgrade your MAXPRO NVR software.

The following are the upgrade scenarios covered:

- Upgrade to MAXPRO NVR 6.7 Build 687
- Upgrade to MAXPRO NVR 6.3 Build 643
- Upgrade to MAXPRO NVR 6.0 Build 622
- Upgrade to MAXPRO NVR 5.6 (Build 572)
- Upgrade to MAXPRO NVR 5.5 (Build 558)
- Upgrade to MAXPRO NVR 5.0 SP1(Build 532)
- Upgrade to MAXPRO NVR 5.0 Build 522(T Patch)
- Upgrade to MAXPRO NVR 5.0 Build 509 Rev D
- Upgrade to MAXPRO NVR 4.9 Build 204
- Upgrade to MAXPRO NVR 4.7 Build 188
- Upgrade to MAXPRO NVR 4.5 Build 162
- Upgrade to MAXPRO NVR 4.1 Build 123 Rev B
- Upgrade to MAXPRO NVR 4.0

Note: *Downgrade to previous version of NVR is only supported if user has restored the Database backup during installation. For example: If user upgrades from 4.1 to 5.0 and if for any reason uninstalls the 5.0 build then, 4.1 installation will also be uninstalled from the machine. If user has restored the DB backup during 5.0 installation then downgrade (4.1) build will be available..*

Upgrade to MAXPRO NVR 6.7 Build 687

Upgrade to 6.7 is supported from th e following build only:

- MAXPRO® NVR 6.3 Build 643
- MAXPRO® NVR 6.0 Build 622

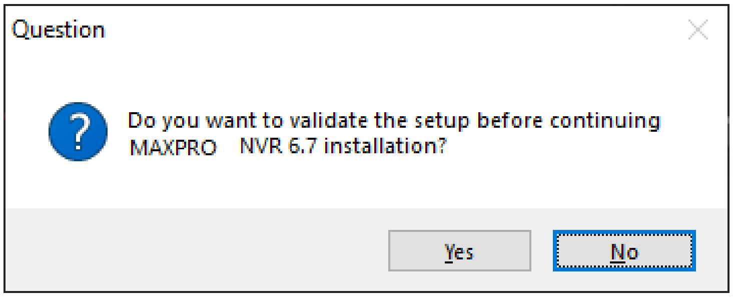
Below tables explains the upgrade support to MAXPRO and Pro-Watch R670:

Upgrade Support	MNVR/MVMS 670	Retain License	Change to Demo License
MNVR/MVMS 600	✓	✓	✗
MNVR/MVMS 630	✓	✓	✗
PNVR/PVMS 650	✗	NA	NA
PNVR/PVMS 650 SP1	✗	NA	NA

Upgrade Support	PWNVR/PWVMS 670	Retain License	Change to Demo License
MNVR/MVMS 600	✓	✗	✓
MNVR/MVMS 630	✓	✗	✓
PWNVR/PWVMS 650	✓	✓	✗
PWNVR/PWVMS 650 SP1	✓	✓	✗

To upgrade to NVR 6.7:

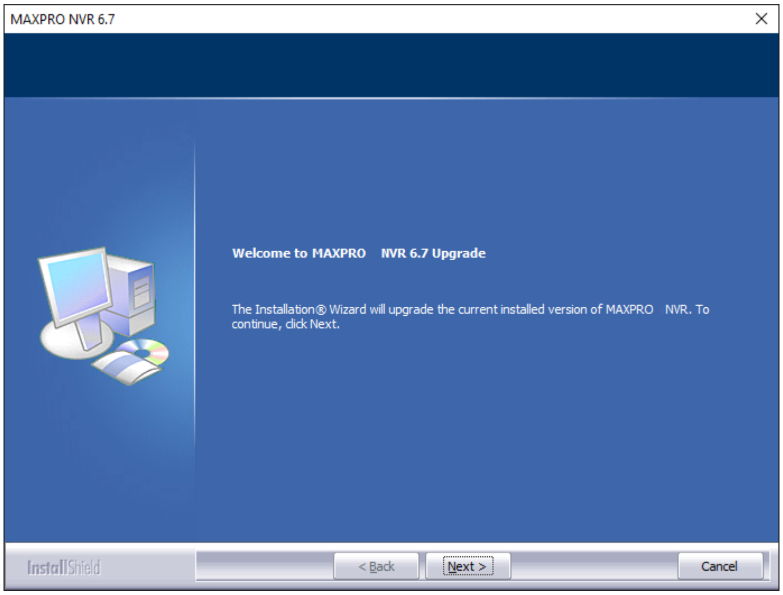
Step 1. Insert the MAXPRO NVR 6.7 setup DVD in the DVD drive, browse the DVD drive, and then double-click setup.exe. A dialog box appears with the question - "Do you want to validate the setup before continuing MAXPRO NVR 6.7 installation?".



Question

Do you want to validate the setup before continuing MAXPRO NVR 6.7 installation?

Step 2. Click Yes to validate the setup files are not corrupted before continuing the installation and click No to skip the validation to continue the setup. The installation wizard starts and the Welcome screen appears.



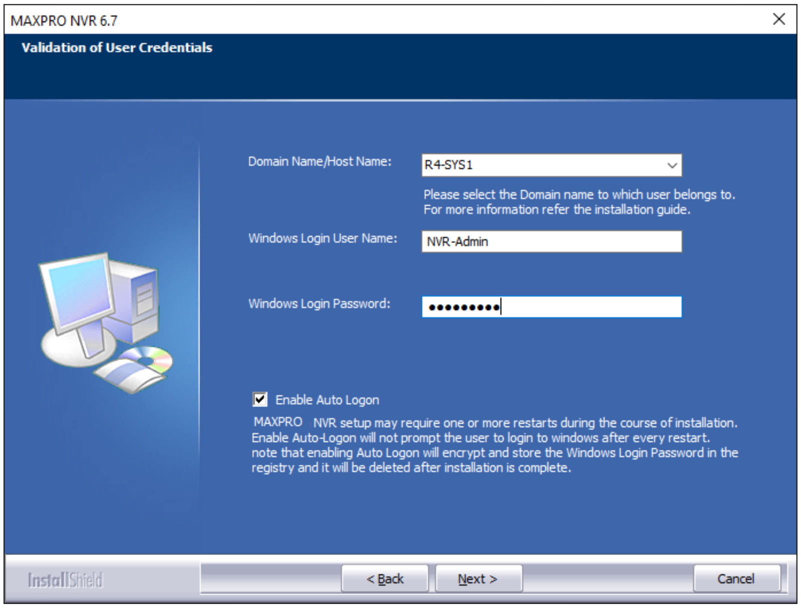
MAXPRO NVR 6.7

Welcome to MAXPRO NVR 6.7 Upgrade

The Installation® Wizard will upgrade the current installed version of MAXPRO NVR. To continue, click Next.

Welcome Wizard

Step 3. Click Next. The Validation of User Credentials appears.



MAXPRO NVR 6.7

Validation of User Credentials

Domain Name/Host Name: R4-SYS1

Please select the Domain name to which user belongs to. For more information refer the installation guide.

Windows Login User Name: NVR-Admin

Windows Login Password: ●●●●●●●●●

☑ Enable Auto Logon

MAXPRO NVR setup may require one or more restarts during the course of installation. Enable Auto-Logon will not prompt the user to login to windows after every restart. note that enabling Auto Logon will encrypt and store the Windows Login Password in the registry and it will be deleted after installation is complete.

Validation of User Credentials

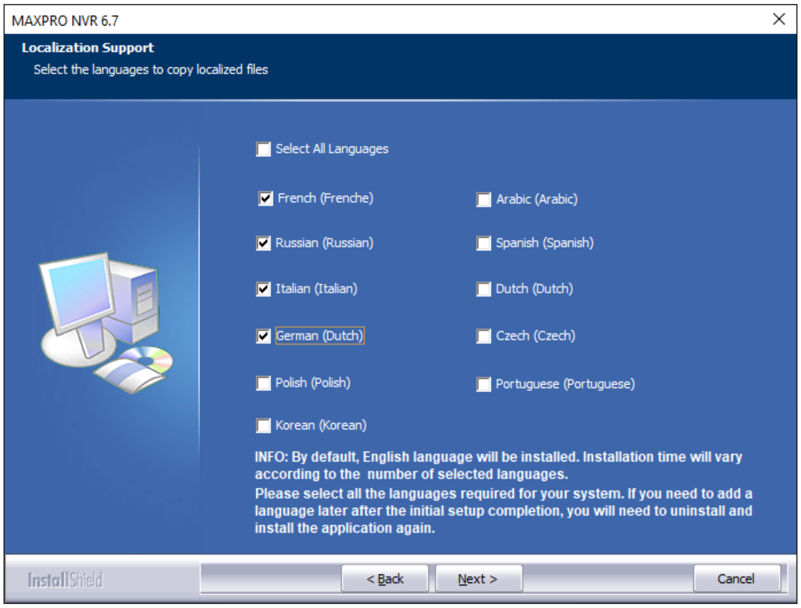
Step 4. Select your Domain Name/Host Name.

Step 5. Type your Windows User Name.

Step 6. Type your Windows Password.

Note: *Honeywell recommends to use the newly created Administrator user account as explained in* Before you Begin - Changing the default Windows Administrator Account Created By NVR, *page* 103.

Step 7. Click Next. The Localization Support wizard appears.



MAXPRO NVR 6.7

Localization Support

Select the languages to copy localized files

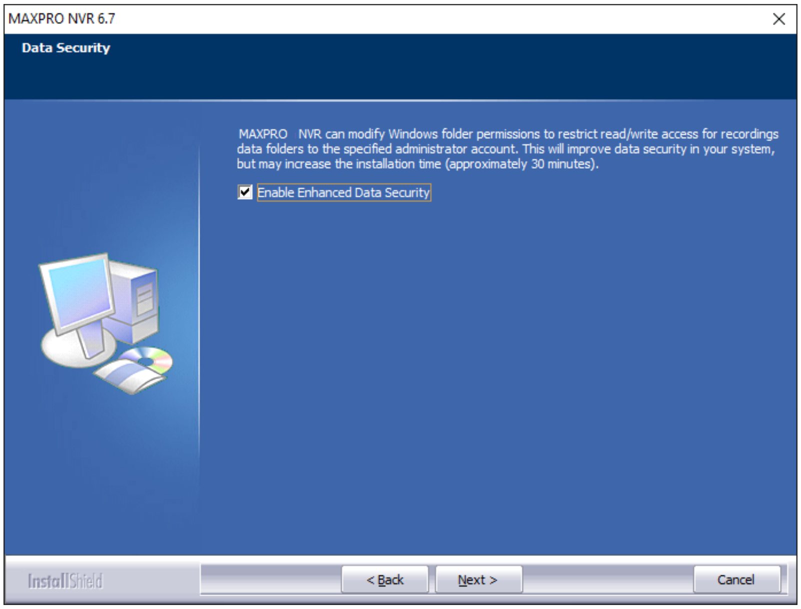
- □ Select All Languages
- ☑ French (Frenche)
- ☑ Russian (Russian)
- ☑ Italian (Italian)
- ☑ German (Dutch)
- □ Polish (Polish)
- □ Korean (Korean)
- □ Arabic (Arabic)
- □ Spanish (Spanish)
- □ Dutch (Dutch)
- □ Czech (Czech)
- □ Portuguese (Portuguese)

INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.
Please select all the languages required for your system. If you need to add a language later after the initial setup completion, you will need to uninstall and install the application again.

Localization Support

Caution: By Default, English language will be installed. Please ensure to select all the languages required for your system. If an additional language is required after the installation is completed, the software will need to be uninstalled and installed again.

Step 8. Select the languages in which you want to upgrade MAXPRO NVR and then click Next. The Data Security Wizard appears.



MAXPRO NVR 6.7

Data Security

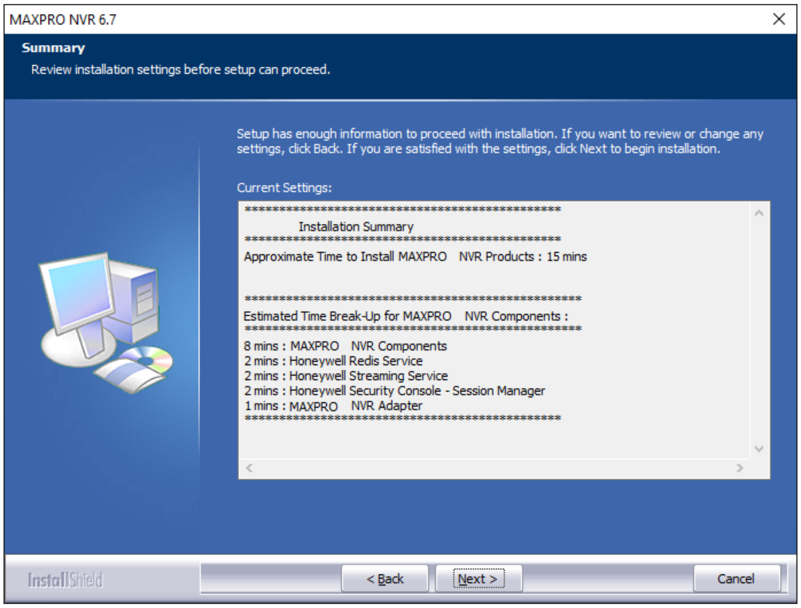
MAXPRO NVR can modify Windows folder permissions to restrict read/write access for recordings data folders to the specified administrator account. This will improve data security in your system, but may increase the installation time (approximately 30 minutes).

☑ Enable Enhanced Data Security

Data Security

Step 9. Select the Enable Enhanced Data Security check box to improve data security in your system.

Step 10. Click Next. The Summary wizard appears.



Summary

Review installation settings before setup can proceed.

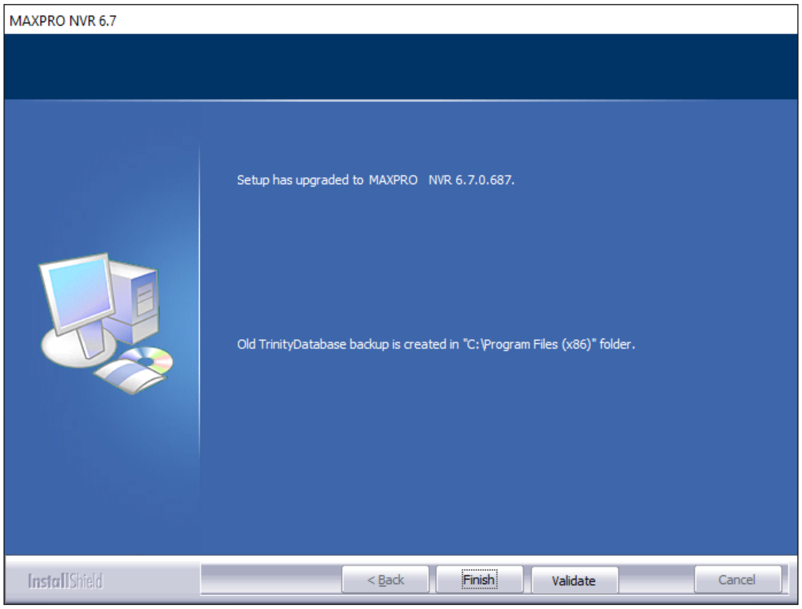
Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

```
**************************************************
          Installation Summary
**************************************************
Approximate Time to Install MAXPRO   NVR Products : 15 mins


******************************************************
Estimated Time Break-Up for MAXPRO   NVR Components :
******************************************************
8 mins : MAXPRO   NVR Components
2 mins : Honeywell Redis Service
2 mins : Honeywell Streaming Service
2 mins : Honeywell Security Console - Session Manager
1 mins : MAXPRO   NVR Adapter
**************************************************
```

Upgrade Summary

Step 11. Click Next. The upgrade status of various components appears. Once the upgrade is complete, the Finish dialog appears.



Setup has upgraded to MAXPRO   NVR 6.7.0.687.

Old TrinityDatabase backup is created in "C:\Program Files (x86)" folder.

Upgrade Finish

Step 12. Click Finish to complete the upgrade.

Upgrade to MAXPRO NVR 6.3 Build 643

Upgrade to 6.3 is supported from th e following build only:

- MAXPRO® NVR 6.0- Build 622

To upgrade to MAXPRO_NVR_6.3:

Step 1. Browse to the setup folder and double-click MAXPRO_NVR_ 6.3 Setup.exe. The installer extracts the setup files and a confirmation message is displayed to disable the Automatic Windows updates.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed.

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 6.0 Build 622

Upgrade to 6.0 is supported as explained below:

- MAXPRO® NVR 6.0- Build 615
- MAXPRO® NVR 6.0- Build 612
- MAXPRO® NVR 5.6- Build 583
- MAXPRO® NVR 5.6- Build 572
- MAXPRO® NVR 5.5- Build 560
- MAXPRO® NVR 5.5- Build 559
- MAXPRO® NVR 5.0 SP1- Build B532
- MAXPRO® NVR 5.0_T patch Build 522
- MAXPRO® NVR 5.0 Build 509 Rev D

Before Upgrading

Caution: If user had configured the Network drive as Recording drive in the previous version of NVR, then after upgrading to 6.0 Build XXXX, none of the cameras will display video. Ensure that you delete/modify the Network path configured as Recording drive and then upgrade.

Pre-requisite

Before upgrading to MAXPRO NVR 6.0, user must install the below SQL service pack for successful upgrade. Refer to the ***800-26010-A - Securing MAXPRO VMS-NVR Technical Notes*** for more information on how to download and install the below service pack.

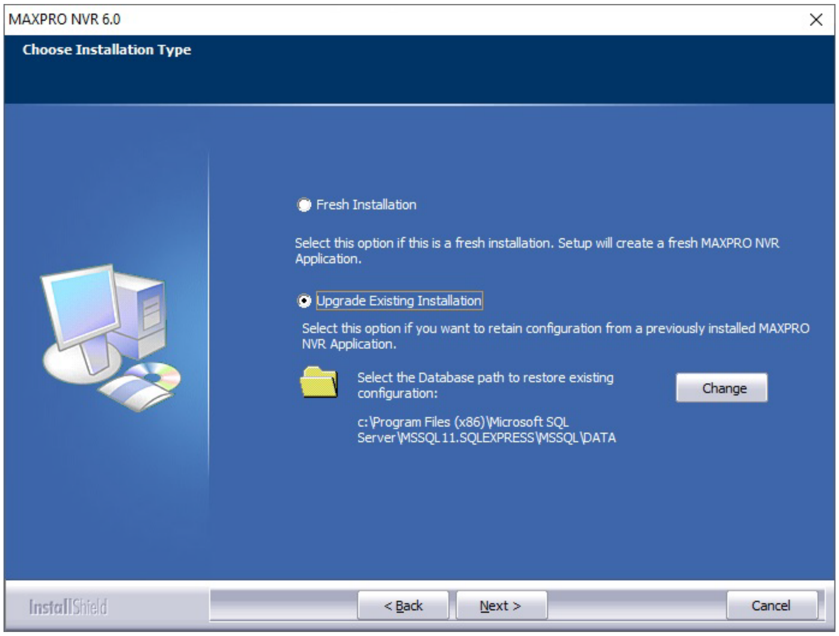
- SQL2012SP4

To upgrade to NVR 6.0:

Step 1. Insert the MAXPRO NVR 6.0 setup DVD in the DVD drive, browse the DVD drive, and then double-click setup.exe

Or

Go to the MAXPRO NVR setup folder on your computer, and then double-click setup.exe. In Choose Installation Type wizard, click Upgrade Existing Installation option.



MAXPRO NVR 6.0

Choose Installation Type

○ Fresh Installation

Select this option if this is a fresh installation. Setup will create a fresh MAXPRO NVR Application.

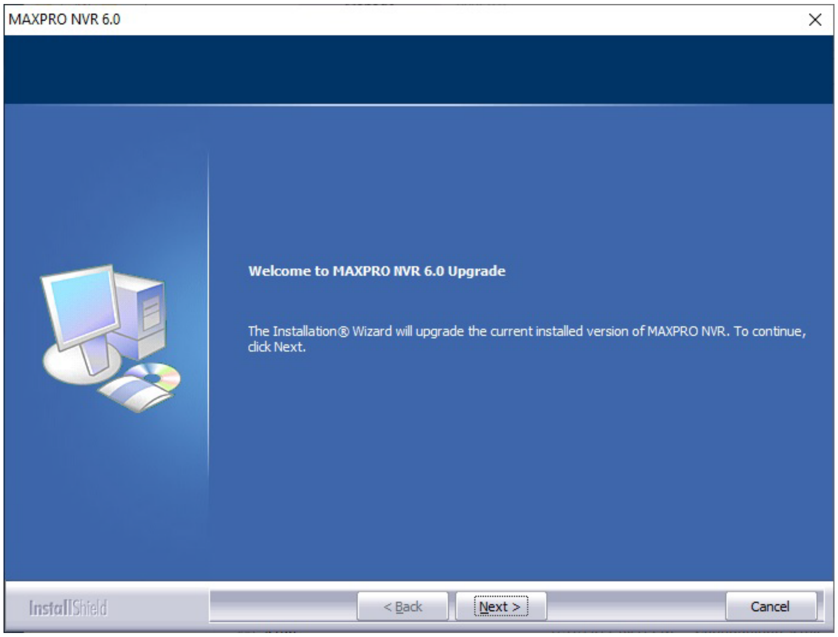
● Upgrade Existing Installation

Select this option if you want to retain configuration from a previously installed MAXPRO NVR Application.

Select the Database path to restore existing configuration:

c:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA

Step 2. Click Next. A dialog box appears with the question - “Do you want to validate the setup before continuing MAXPRO NVR 6.0 installation?”, click Yes to validate the setup files are not corrupted before continuing the installation and click No to skip the validation to continue the setup. The installation wizard starts and the Welcome screen appears.

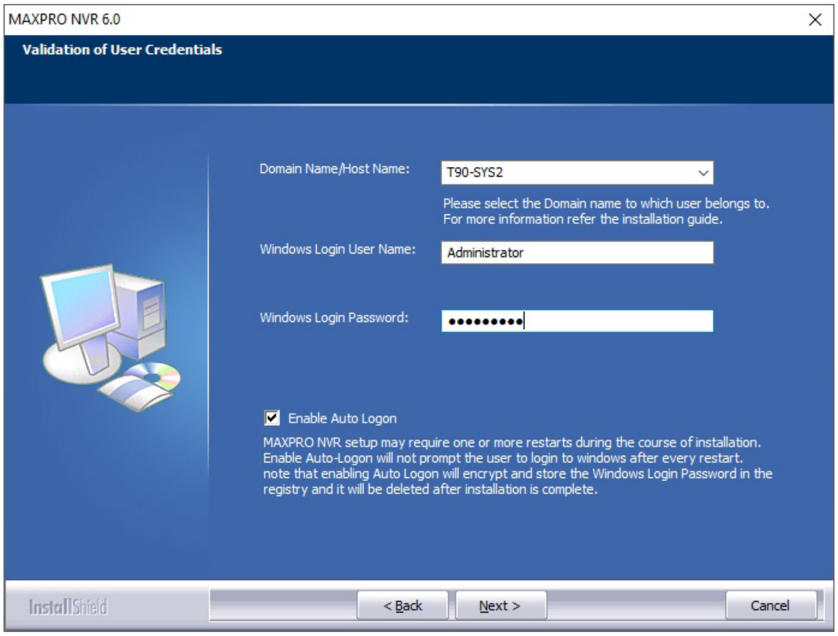


Welcome to MAXPRO NVR 6.0 Upgrade

The Installation® Wizard will upgrade the current installed version of MAXPRO NVR. To continue, click Next.

Welcome Wizard

Step 3. Click Next. The Validation of User Credentials appears.



Validation of User Credentials

Domain Name/Host Name: T90-SYS2

Please select the Domain name to which user belongs to.
For more information refer the installation guide.

Windows Login User Name: Administrator

Windows Login Password: ●●●●●●●●●●

☑ Enable Auto Logon

MAXPRO NVR setup may require one or more restarts during the course of installation.
Enable Auto-Logon will not prompt the user to login to windows after every restart.
note that enabling Auto Logon will encrypt and store the Windows Login Password in the registry and it will be deleted after installation is complete.

Validation of User Credentials

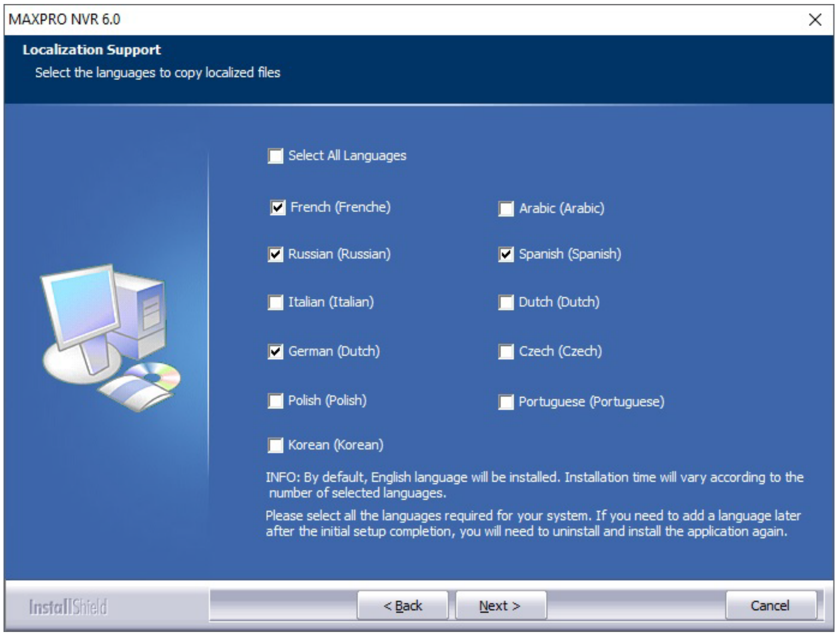
Step 4. Select your Domain Name/Host Name.

Step 5. Type your Windows User Name.

Step 6. Type your Windows Password.

Note: *Honeywell recommends to use the newly created Administrator user account as explained in* Before you Begin - Changing the default Windows Administrator Account Created By NVR, *page* 103.

Step 7. Click Next. The Localization Support wizard appears.



MAXPRO NVR 6.0

Localization Support

Select the languages to copy localized files

□ Select All Languages

☑ French (Frenche) □ Arabic (Arabic)

☑ Russian (Russian) ☑ Spanish (Spanish)

□ Italian (Italian) □ Dutch (Dutch)

☑ German (Dutch) □ Czech (Czech)

□ Polish (Polish) □ Portuguese (Portuguese)

□ Korean (Korean)

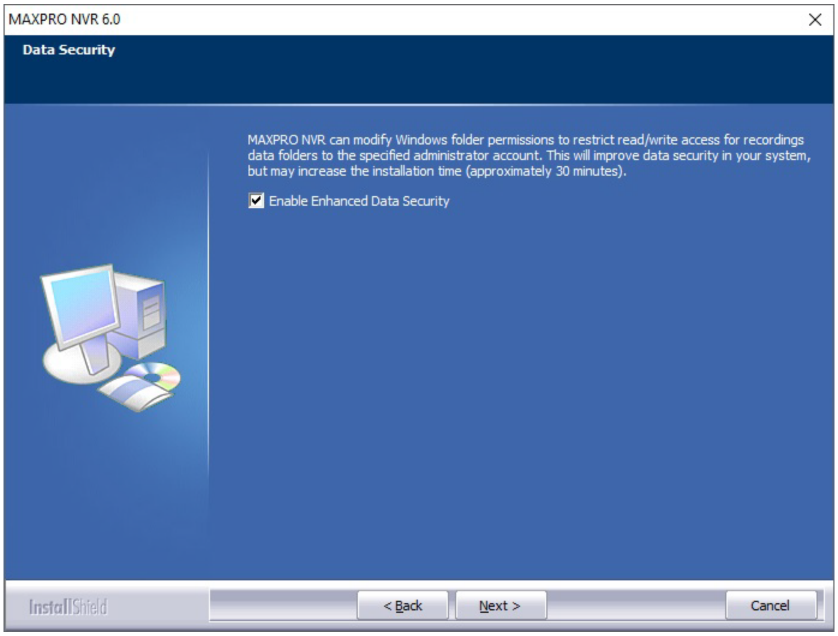
INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.

Please select all the languages required for your system. If you need to add a language later after the initial setup completion, you will need to uninstall and install the application again.

Localization Support

Caution: By Default, English language will be installed. Please ensure to select all the languages required for your system. If an additional language is required after the installation is completed, the software will need to be uninstalled and installed again.

Step 8. Select the languages in which you want to upgrade MAXPRO NVR and then click Next. The Data Security Wizard appears.



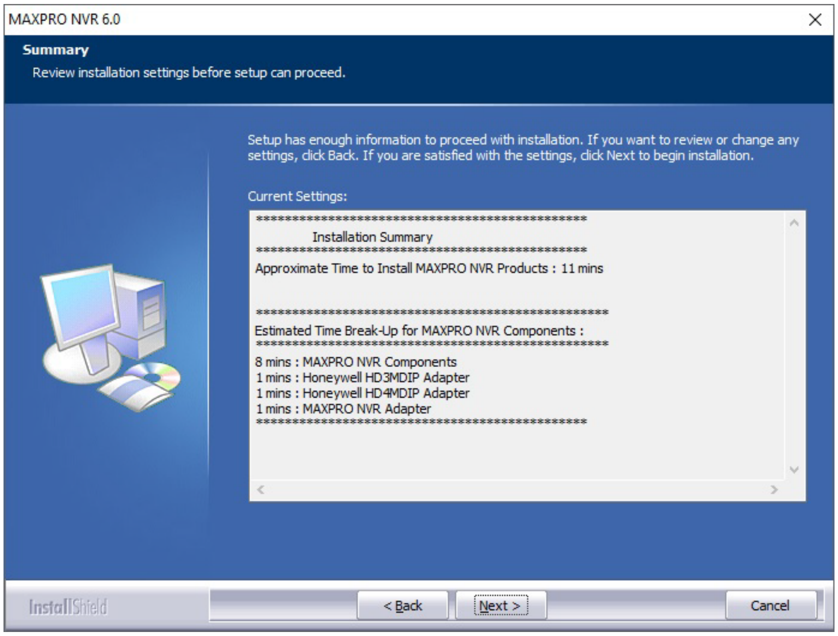
MAXPRO NVR can modify Windows folder permissions to restrict read/write access for recordings data folders to the specified administrator account. This will improve data security in your system, but may increase the installation time (approximately 30 minutes).

☑ Enable Enhanced Data Security

Data Security

Step 9. Select the Enable Enhanced Data Security check box to improve data security in your system.

Step 10. Click Next. The Summary wizard appears.



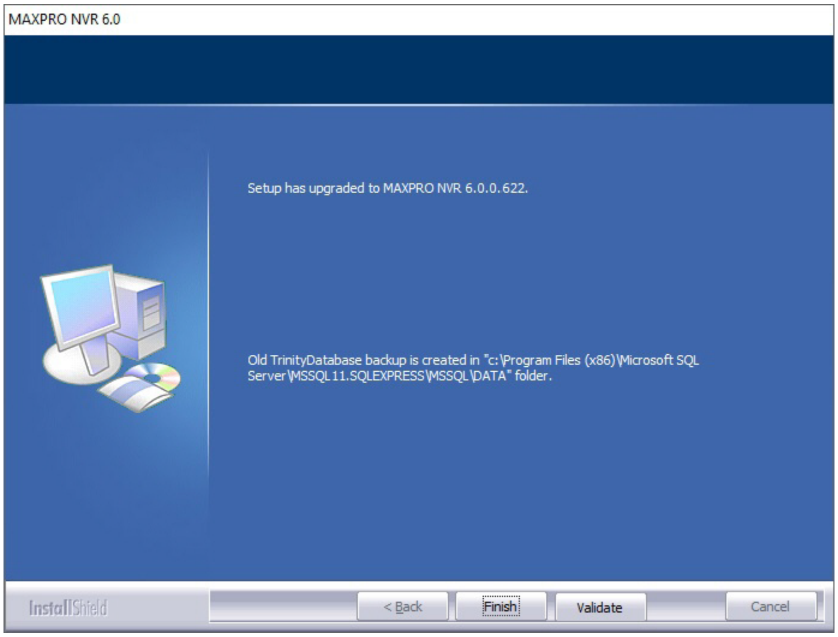
Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

```
**************************************************
          Installation Summary
**************************************************
Approximate Time to Install MAXPRO NVR Products : 11 mins


******************************************************
Estimated Time Break-Up for MAXPRO NVR Components :
******************************************************
8 mins : MAXPRO NVR Components
1 mins : Honeywell HD3MDIP Adapter
1 mins : Honeywell HD4MDIP Adapter
1 mins : MAXPRO NVR Adapter
**************************************************
```

Upgrade Summary

Step 11. Click Next. The upgrade status of various components appears. Once the upgrade is complete, the Finish dialog appears.


MAXPRO NVR 6.0

Setup has upgraded to MAXPRO NVR 6.0.0.622.

Old TrinityDatabase backup is created in "c:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA" folder.

Upgrade Finish

Step 12. Click Finish to complete the upgrade.

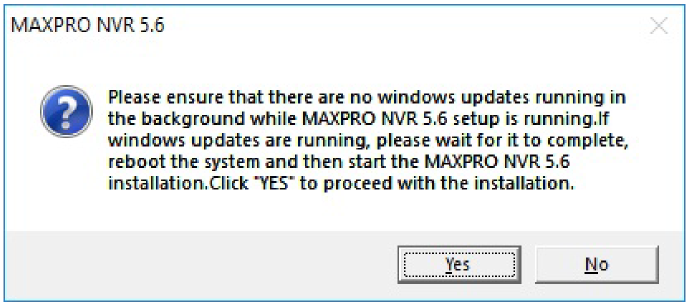
Upgrade to MAXPRO NVR 5.6 (Build 572)

Upgrade to NVR 5.6 Build 572 is supported from the following builds only.

- MAXPRO NVR v5.0 Build 509 Rev D
- MAXPRO NVR 5.0_T patch Build 522
- MAXPRO NVR 5.0 SP1 Build 532
- MAXPRO NVR 5.5 Build 558

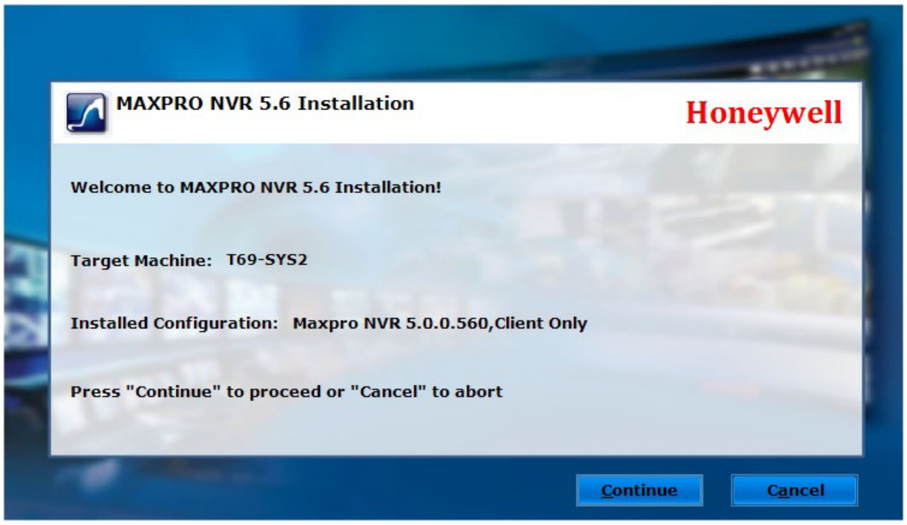
To upgrade to MAXPRO_NVR_5.6:

Step 1. Browse to the setup folder and double-click MAXPRO_NVR_ 5.6 Setup.exe. The installer extracts the setup files and a confirmation message is displayed to disable the Automatic Windows updates as shown below.


MAXPRO NVR 5.6

Please ensure that there are no windows updates running in the background while MAXPRO NVR 5.6 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 5.6 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 5.6 Installation

Welcome to MAXPRO NVR 5.6 Installation!

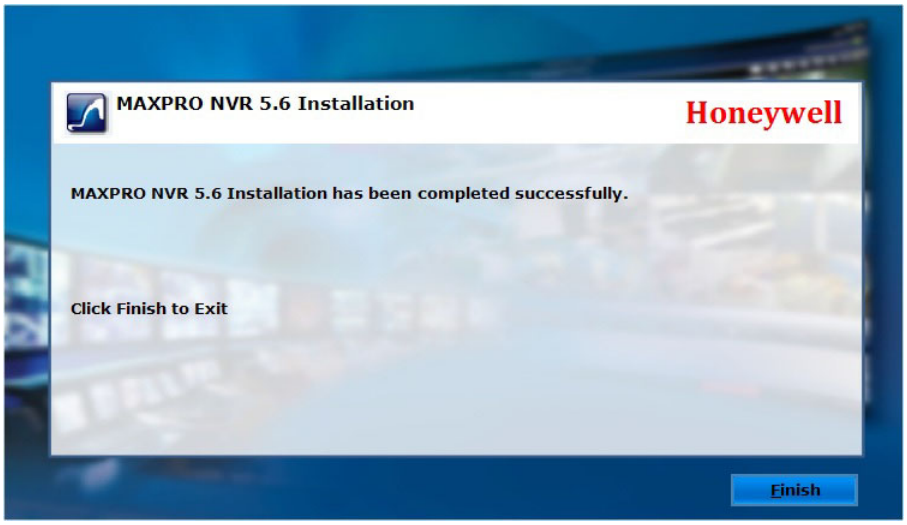
Target Machine: T69-SYS2

Installed Configuration: Maxpro NVR 5.0.0.560,Client Only

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed as shown below.



MAXPRO NVR 5.6 Installation

MAXPRO NVR 5.6 Installation has been completed successfully.

Click Finish to Exit

Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 5.5 (Build 558)

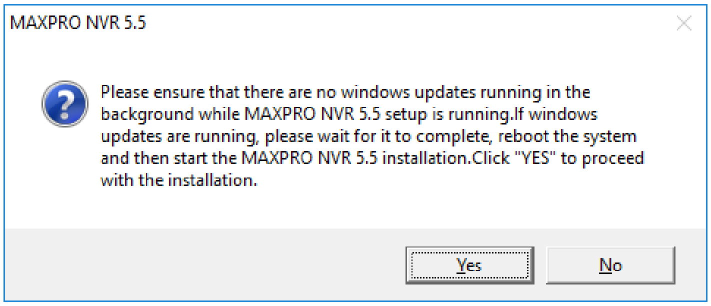
Upgrade to NVR 5.5 Build 558 is supported from the following builds only.

- MAXPRO NVR v5.0 Build 509 Rev D
- MAXPRO NVR 5.0_T patch Build 522

- MAXPRO NVR 5.0 SP1 Build 532

To upgrade to MAXPRO_NVR_5.5:

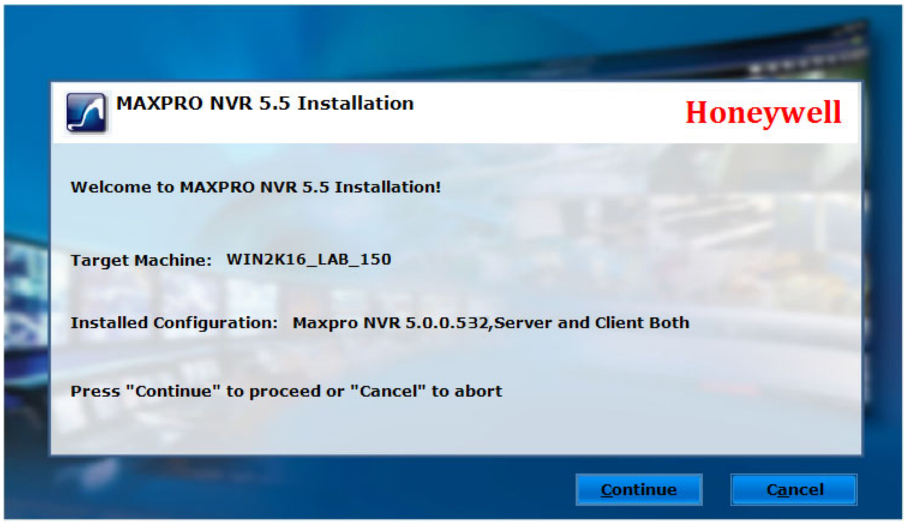
Step 1. Browse to the setup folder and double-click MAXPRO_NVR_ 5.5 Setup.exe. The installer extracts the setup files and a confirmation message is displayed to disable the Automatic Windows updates as shown below.



MAXPRO NVR 5.5

Please ensure that there are no windows updates running in the background while MAXPRO NVR 5.5 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 5.5 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 5.5 Installation

Welcome to MAXPRO NVR 5.5 Installation!

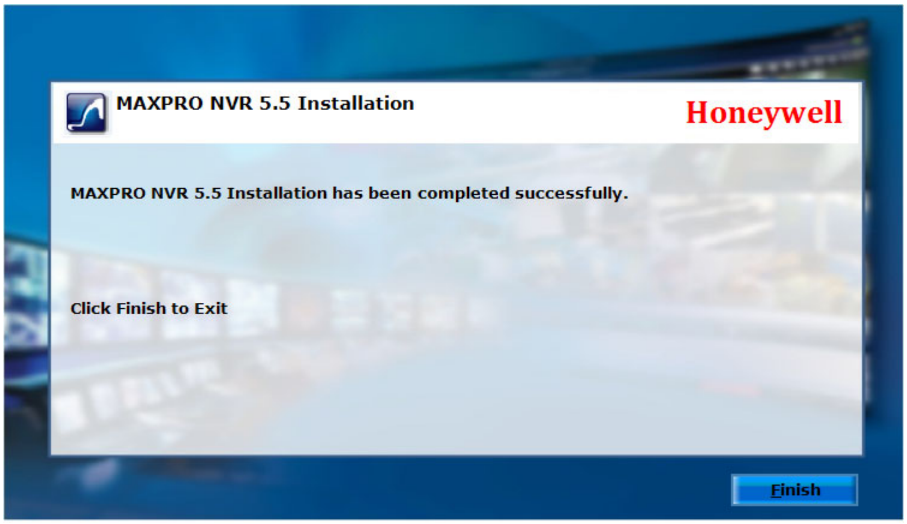
Target Machine: WIN2K16_LAB_150

Installed Configuration: Maxpro NVR 5.0.0.532,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed as shown below.



MAXPRO NVR 5.5 Installation has been completed successfully.

Click Finish to Exit

Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 5.0 SP1(Build 532)

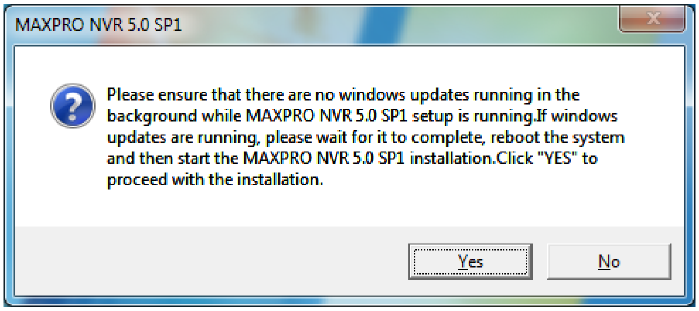
Upgrade to 5.0 Service Pack 1 is supported from the following builds only.

- MAXPRO NVR v5.0 Build 509 Rev D
- MAXPRO_NVR_ 5.0_T patch Build 522

Note: *If SP1 is installed on top of 5.0 Build 509 Rev D then MAXPRO_NVR_ 5.0_T patch Build 522 is installed internally.*

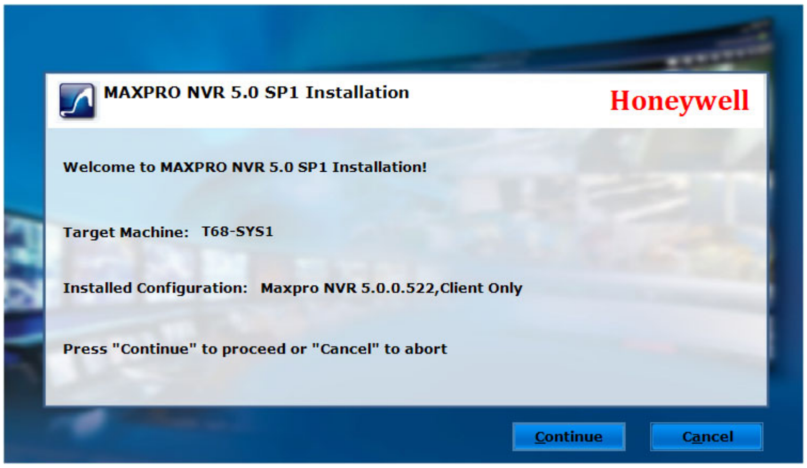
To upgrade to MAXPRO_NVR_ R500_SP1

Step 1. Double click MAXPRO_NVR_ R500_SP1 Setup.exe. The installer extracts the files and displays the Windows update message.



Please ensure that there are no windows updates running in the background while MAXPRO NVR 5.0 SP1 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 5.0 SP1 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 5.0 SP1 Installation

Welcome to MAXPRO NVR 5.0 SP1 Installation!

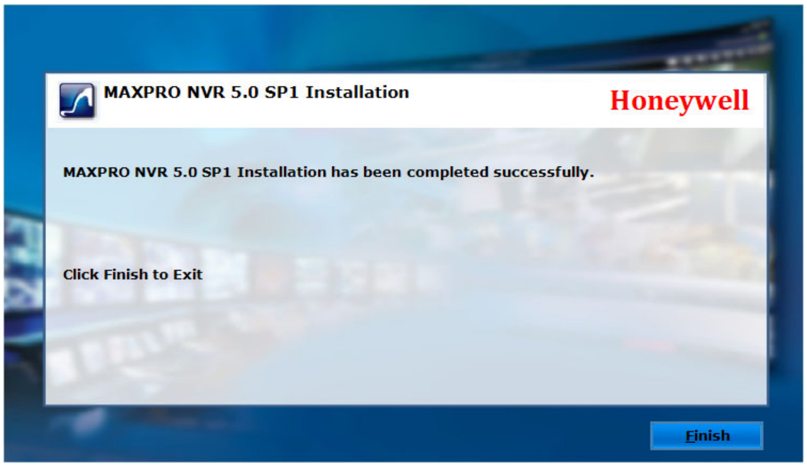
Target Machine: T68-SYS1

Installed Configuration: Maxpro NVR 5.0.0.522,Client Only

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed as shown below.



MAXPRO NVR 5.0 SP1 Installation

MAXPRO NVR 5.0 SP1 Installation has been completed successfully.

Click Finish to Exit

Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Uninstalling SP1

In Add/Remove program windows there will be two entries as:

- MAXPRO_NVR_ 5.0_T patch Build 522
- MAXPRO_NVR_ 5.0 SP1 Build 531

If user wants to go back to v5.0 Build 509 Rev D then from Add/Remove Program window uninstall the applications in the order as mentioned below:

Step 1. Uninstall SP1

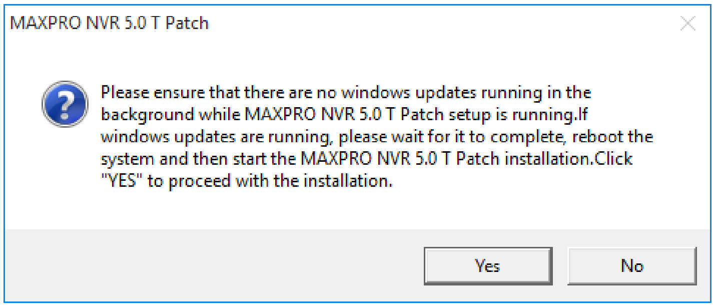
Step 2. Uninstall 5.0_T patch Build 522

Upgrade to MAXPRO NVR 5.0 Build 522(T Patch)

Upgrade to 5.0 T patch is supported from v5.0 Build 509 to MAXPRO NVR 5.0 Build 522 only.

To upgrade to MAXPRO_NVR_ R500_T patch

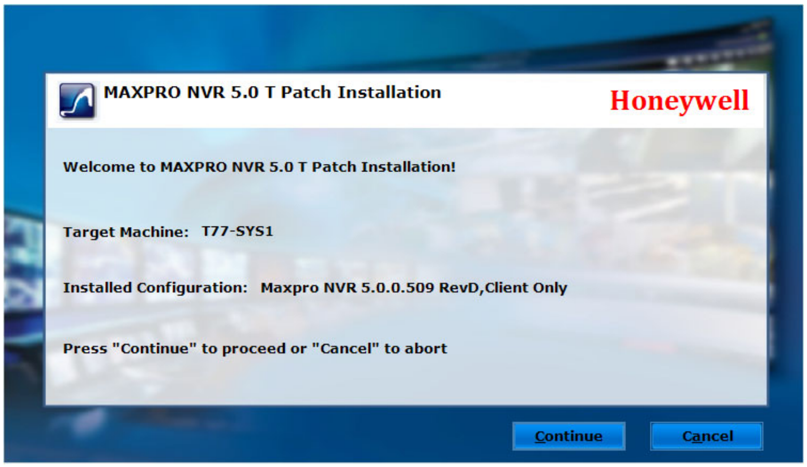
Step 1. Double click MAXPRO_NVR_ R500_T patch Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



MAXPRO NVR 5.0 T Patch

Please ensure that there are no windows updates running in the background while MAXPRO NVR 5.0 T Patch setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 5.0 T Patch installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 5.0 T Patch Installation

Welcome to MAXPRO NVR 5.0 T Patch Installation!

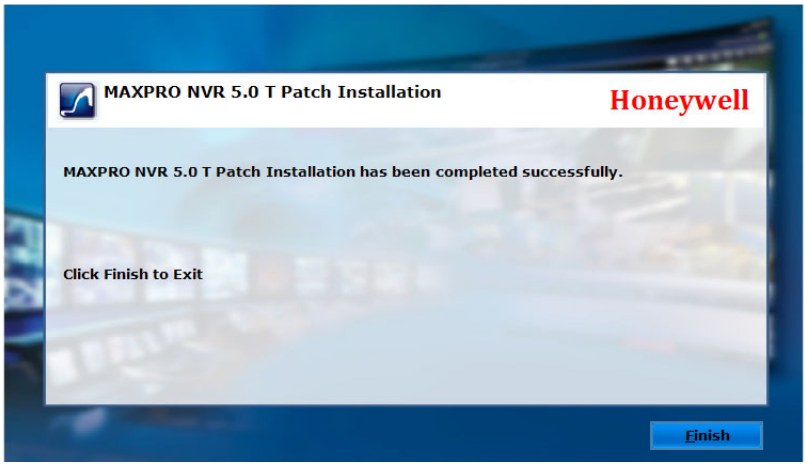
Target Machine: T77-SYS1

Installed Configuration: Maxpro NVR 5.0.0.509 RevD,Client Only

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed as shown below.


MAXPRO NVR 5.0 T Patch Installation

MAXPRO NVR 5.0 T Patch Installation has been completed successfully.

Click Finish to Exit

Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 5.0 Build 509 Rev D

Upgrade to 5.0 is supported as explained below:

- From v4.0 Build 87 Rev H to MAXPRO NVR 5.0 Build 509 Rev D
- From NVR 4.1 Build 123 Rev B to NVR 5.0 Build 509 Rev D
- From NVR 4.5 Build 162 Rev B to NVR 5.0 Build 509 Rev D
- From NVR 4.7 Build 188 to NVR 5.0 Build 509 Rev D
- From NVR 4.9 Build 204 to NVR 5.0 Build 509 Rev D

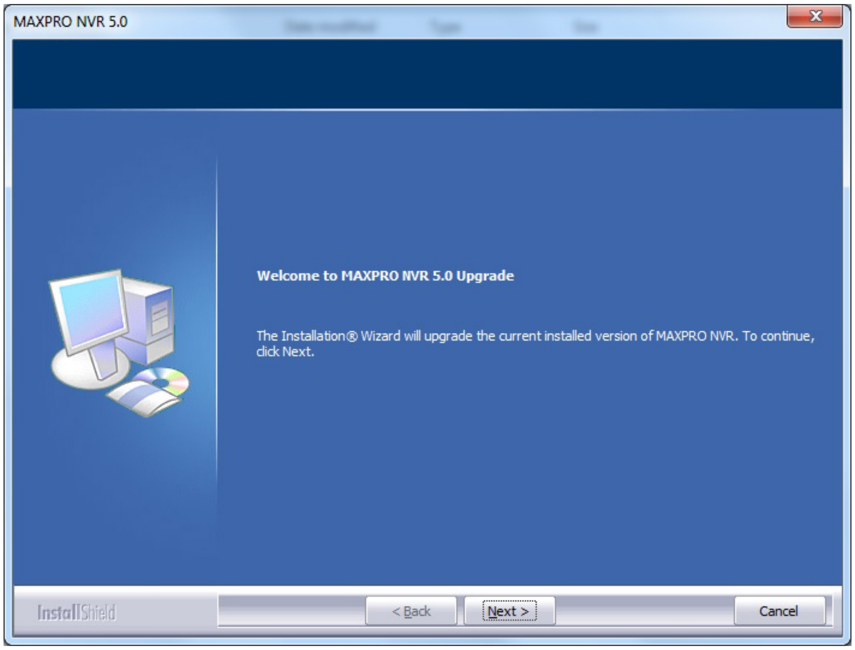
Before Upgrading

Caution: If user had configured the Network drive as Recording drive in the previous version of NVR, then after upgrading to 5.0 Build 509, none of the cameras will display video. Ensure that you delete/modify the Network path configured as Recording drive and then upgrade.

To upgrade to NVR 5.0:

Step 1. Insert the MAXPRO NVR 5.0 setup DVD in the DVD drive, browse the DVD drive, and then double-click setup.exe

Or
Go to the MAXPRO NVR setup folder on your computer, and then double-click setup.exe. A dialog box appears with the question - “Do you want to validate the setup before continuing MAXPRO NVR 5.0 installation?”, click Yes to validate the setup files are not corrupted before continuing the installation and click No to skip the validation to continue the setup. The installation wizard starts and the Welcome screen appears.

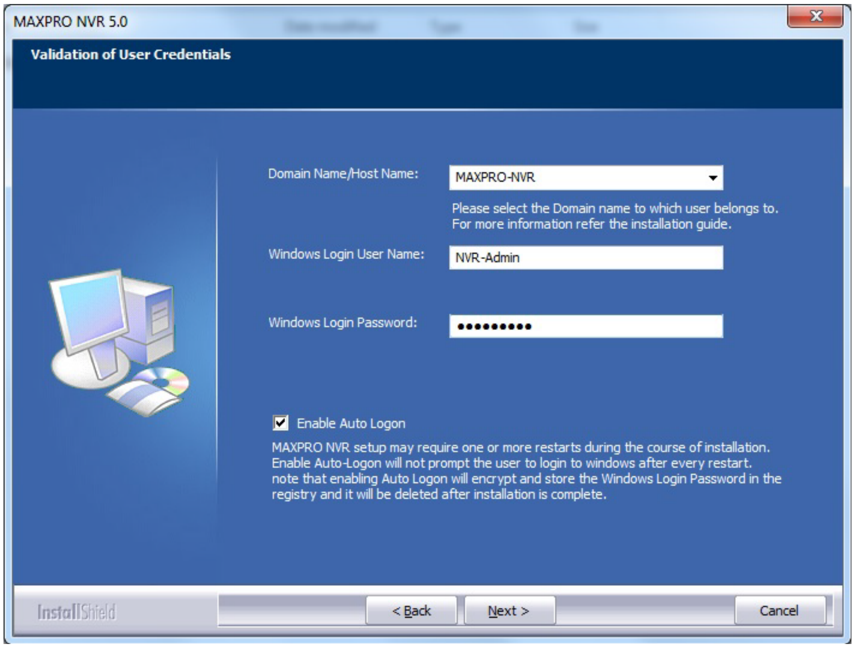

MAXPRO NVR 5.0

Welcome to MAXPRO NVR 5.0 Upgrade

The Installation® Wizard will upgrade the current installed version of MAXPRO NVR. To continue, click Next.

Welcome Wizard

Step 2. Click Next. The Validation of User Credentials appears.


MAXPRO NVR 5.0

Validation of User Credentials

Domain Name/Host Name: MAXPRO-NVR

Please select the Domain name to which user belongs to.
For more information refer the installation guide.

Windows Login User Name: NVR-Admin

Windows Login Password: •••••••••

☑ Enable Auto Logon

MAXPRO NVR setup may require one or more restarts during the course of installation. Enable Auto-Logon will not prompt the user to login to windows after every restart. note that enabling Auto Logon will encrypt and store the Windows Login Password in the registry and it will be deleted after installation is complete.

Validation of User Credentials

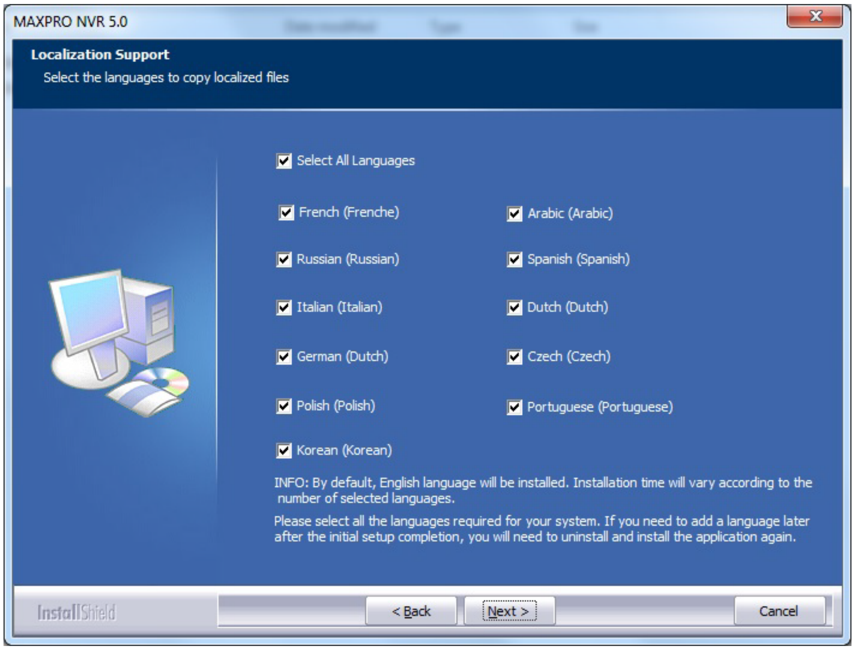
Step 3. Select your Domain Name/Host Name.

Step 4. Type your Windows User Name.

Step 5. Type your Windows Password.

Note: *Honeywell recommends to use the newly created Administrator user account as explained in* Before you Begin - Changing the default Windows Administrator Account Created By NVR, *page* 103*.*

Step 6. Click Next. The Localization Support wizard (Figure) appears.



Localization Support

Select the languages to copy localized files

☑ Select All Languages

☑ French (Frenche)

☑ Arabic (Arabic)

☑ Russian (Russian)

☑ Spanish (Spanish)

☑ Italian (Italian)

☑ Dutch (Dutch)

☑ German (Dutch)

☑ Czech (Czech)

☑ Polish (Polish)

☑ Portuguese (Portuguese)

☑ Korean (Korean)

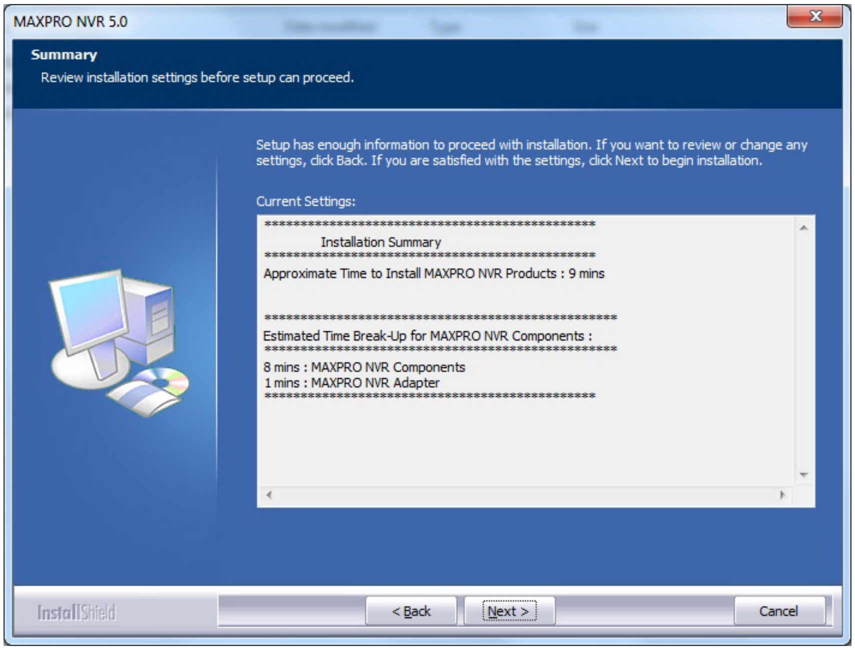
INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.

Please select all the languages required for your system. If you need to add a language later after the initial setup completion, you will need to uninstall and install the application again.

Localization Support

Caution: By Default, English language will be installed. Please ensure to select all the languages required for your system. If an additional language is required after the installation is completed, the software will need to be uninstalled and installed again.

Step 7. Select the languages in which you want to upgrade MAXPRO NVR and then click Next. The Summary screen appears.



MAXPRO NVR 5.0

Summary

Review installation settings before setup can proceed.

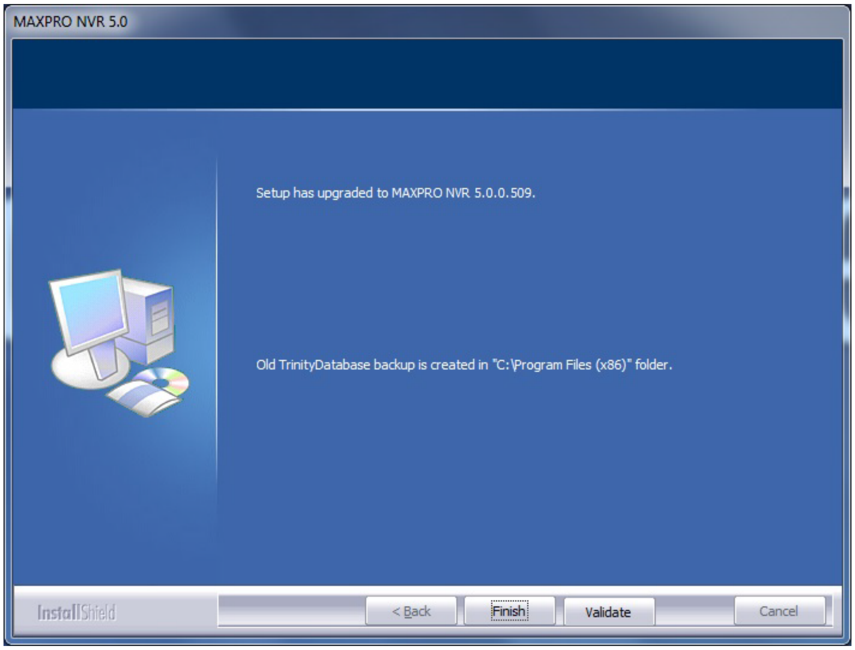
Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

```
************************************************
          Installation Summary
************************************************
Approximate Time to Install MAXPRO NVR Products : 9 mins


***************************************************
Estimated Time Break-Up for MAXPRO NVR Components :
***************************************************
8 mins : MAXPRO NVR Components
1 mins : MAXPRO NVR Adapter
************************************************
```

Summary

Step 8. Click Next. The upgrade status of various components appears. Once the upgrade is complete, the Finish dialog appears.



MAXPRO NVR 5.0

Setup has upgraded to MAXPRO NVR 5.0.0.509.

Old TrinityDatabase backup is created in "C:\Program Files (x86)" folder.

Upgrade Finish

Step 9. Click Finish to complete the upgrade.

Note: *While upgrading the client to 5.0, a System Warning dialog with Unknown Hard Error message is displayed*
Cause: This issue may occur due to conflict between third party applications or due to system file corruption.
Solution: Refer and perform the steps as explained in the Microsoft link https://answers.microsoft.com/en-us/windows/forum/windows_8-performance/explorerexe-system-warning-dialog-with-unknown/4c0be311-c9d5-46e7-b352-c8656f5c0226?auth=1

Or

https://www.drivethelife.com/windows-10/fix-unknown-hard-error-windows-10.html

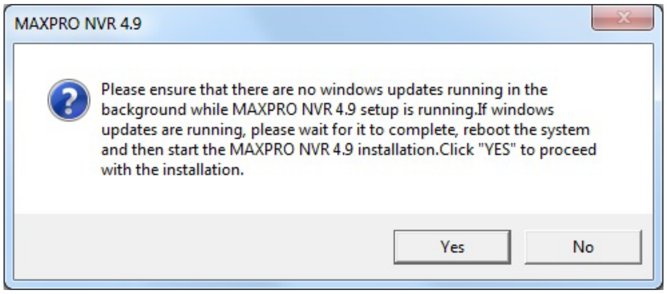
Upgrade to MAXPRO NVR 4.9 Build 204

Upgrade to 4.9 is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.9 Build 204
- From NVR 4.0 97 Rev B to NVR 4.9 Build 204
- From NVR 4.1 Build 123 Rev B to NVR 4.9 Build 204
- From NVR 4.5 Build 162 Rev B to NVR 4.9 Build 204
- From NVR 4.7 Build 188 to NVR 4.9 Build 204

To upgrade to MAXPRO NVR 4.9 Service Pack

Step 1. Double click MAXPRO NVR 4.9 Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



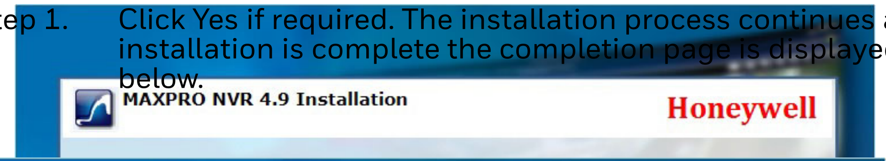
MAXPRO NVR 4.9

Please ensure that there are no windows updates running in the background while MAXPRO NVR 4.9 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 4.9 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.

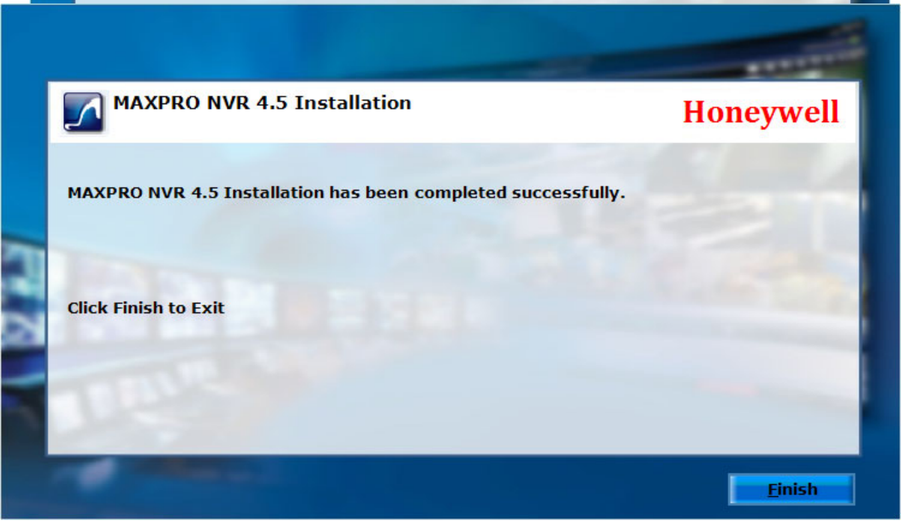
Installation Complete

Step 1. Click Yes if required. The installation process continues and once the installation is complete the completion page is displayed as shown below.



MAXPRO NVR 4.9 Installation

Honeywell



MAXPRO NVR 4.5 Installation

Honeywell

MAXPRO NVR 4.5 Installation has been completed successfully.

Click Finish to Exit

W

S process pletion page is

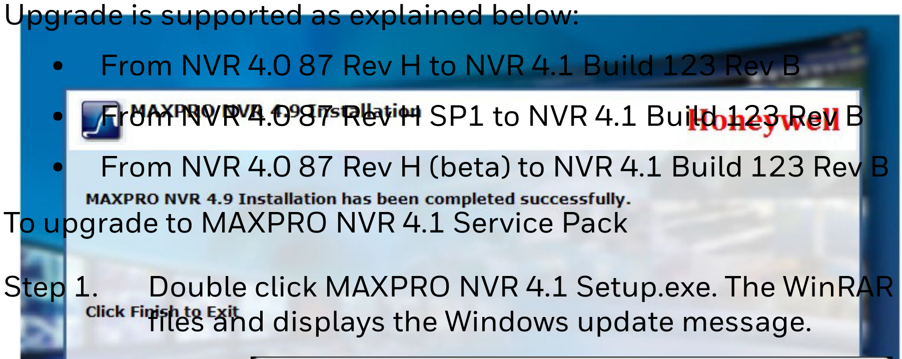
Note: *If Korean language is not installed in your previous build (such as NVR 4.5 Build 162 or 4.7 Build 188) then a confirmation message to support Korean Language is displayed. Click Yes if required.*

Step 2. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 4.1 Build 123 Rev B

Upgrade is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H SP1 to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H (beta) to NVR 4.1 Build 123 Rev B



MAXPRO NVR 4.9 Installation

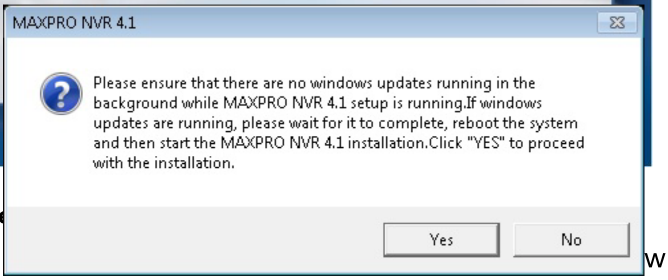
Honeywell

MAXPRO NVR 4.9 Installation has been completed successfully.

Click Finish to Exit

To upgrade to MAXPRO NVR 4.1 Service Pack

Step 1. Double click MAXPRO NVR 4.1 Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



MAXPRO NVR 4.1

Please ensure that there are no windows updates running in the background while MAXPRO NVR 4.1 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 4.1 installation.Click "YES" to proceed with the installation.

Installation Complete

Step 4. Click Fi wizard.

Upgrade to MAXPRO NVR 4.7 Build 188

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.

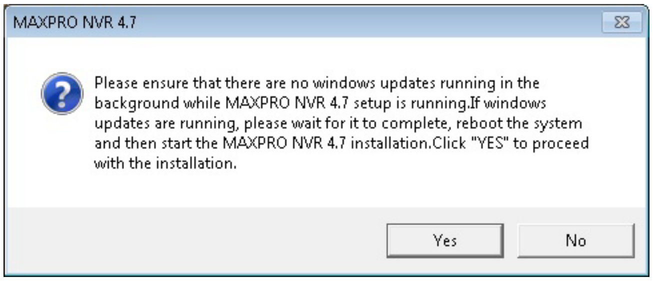
Direct Upgrade to 4.7 is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.7 Build 188
- From NVR 4.0 97 Rev B to NVR 4.7 Build 188

- From NVR 4.1 Build 123 Rev B to NVR 4.7 Build 188
- From NVR 4.5 Build 162 Rev B to NVR 4.7 Build 188

To upgrade to MAXPRO NVR 4.7 Service Pack

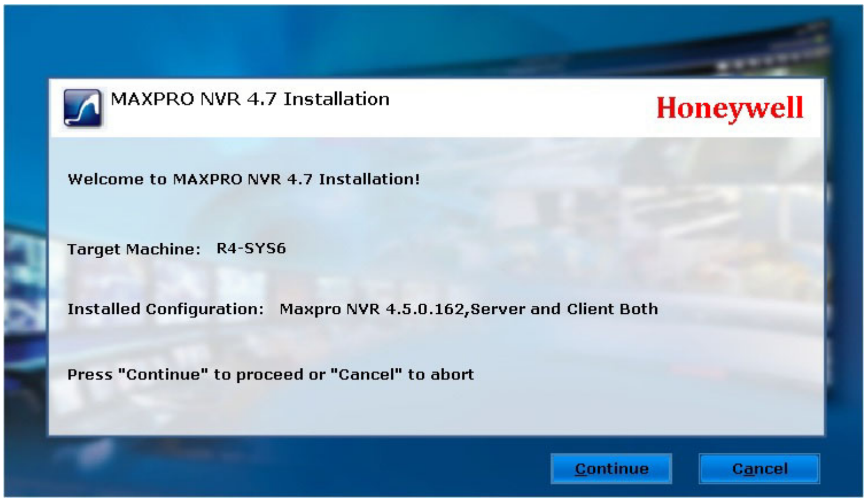
Step 1. Double click MAXPRO NVR 4.7 Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



MAXPRO NVR 4.7

Please ensure that there are no windows updates running in the background while MAXPRO NVR 4.7 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 4.7 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 4.7 Installation

Welcome to MAXPRO NVR 4.7 Installation!

Target Machine: R4-SYS6

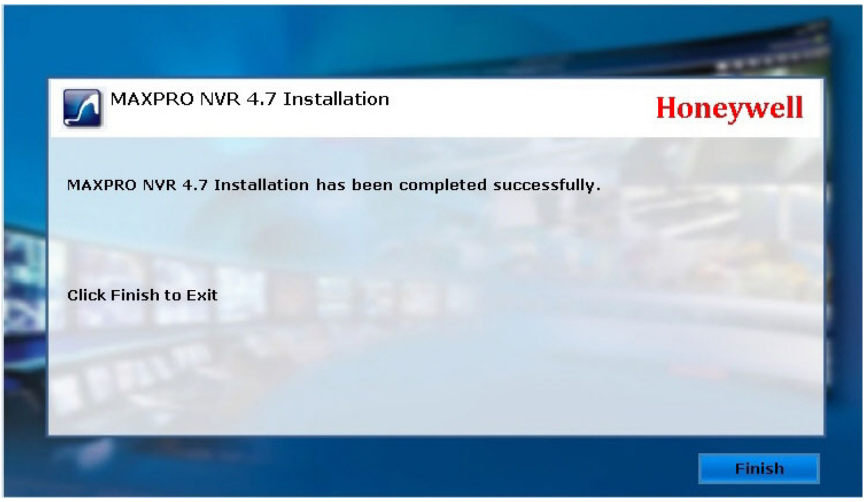
Installed Configuration: Maxpro NVR 4.5.0.162,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. The installation process continues and once the installation is complete the completion page is displayed as shown below.

Note: *If Korean language is not installed in your previous build (such as NVR 4.5 Build 162) then a confirmation message to support Korean Language is displayed. Click Yes if required.*


MAXPRO NVR 4.7 Installation

MAXPRO NVR 4.7 Installation has been completed successfully.

Click Finish to Exit

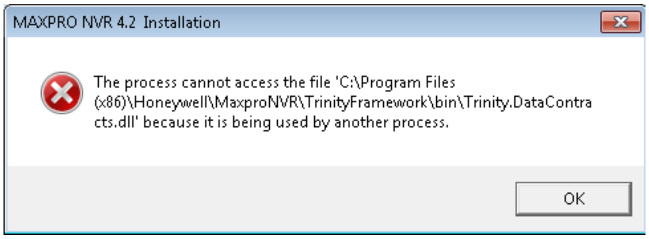
Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 4.5 Build 162

Pre-requisites

Before installing NVR 4.5 build 162 Service pack, ensure that all other applications in the PC is closed. If any application is still running then Process can not access the file message is displayed as shown below.


MAXPRO NVR 4.2 Installation

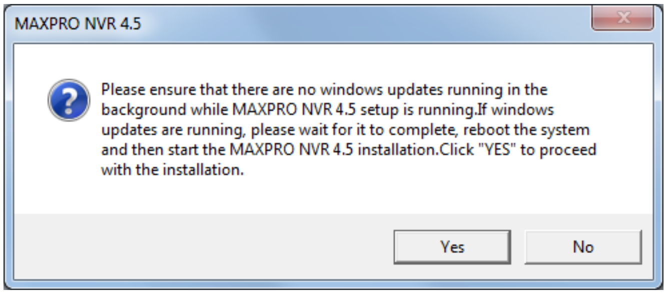
The process cannot access the file 'C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework\bin\Trinity.DataContracts.dll' because it is being used by another process.

Upgrade is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H SP1 to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H (beta) to NVR 4.1 Build 123 Rev B
- From NVR 4.1 Build 123 Rev B to NVR 4.5 Build 162

To upgrade to MAXPRO NVR 4.5 Service Pack

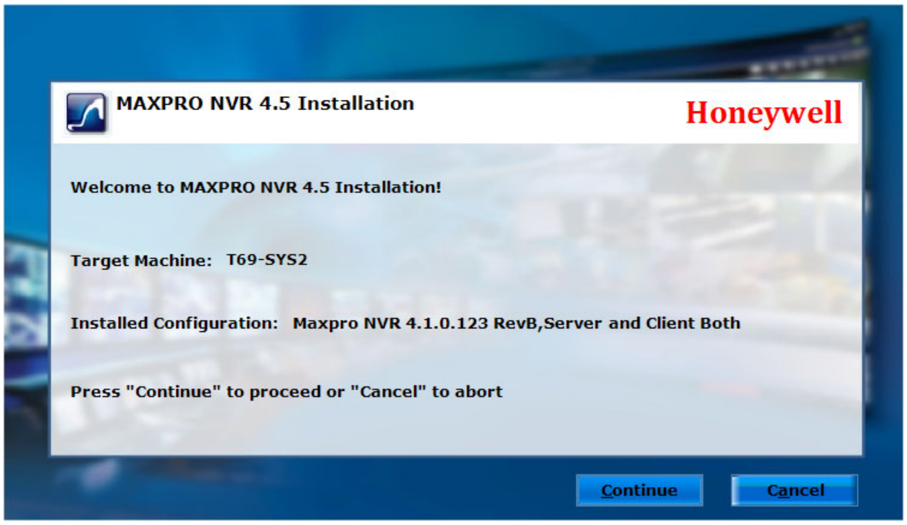
Step 1. Double click MAXPRO NVR 4.5 Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



MAXPRO NVR 4.5

Please ensure that there are no windows updates running in the background while MAXPRO NVR 4.5 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 4.5 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.



MAXPRO NVR 4.5 Installation

Welcome to MAXPRO NVR 4.5 Installation!

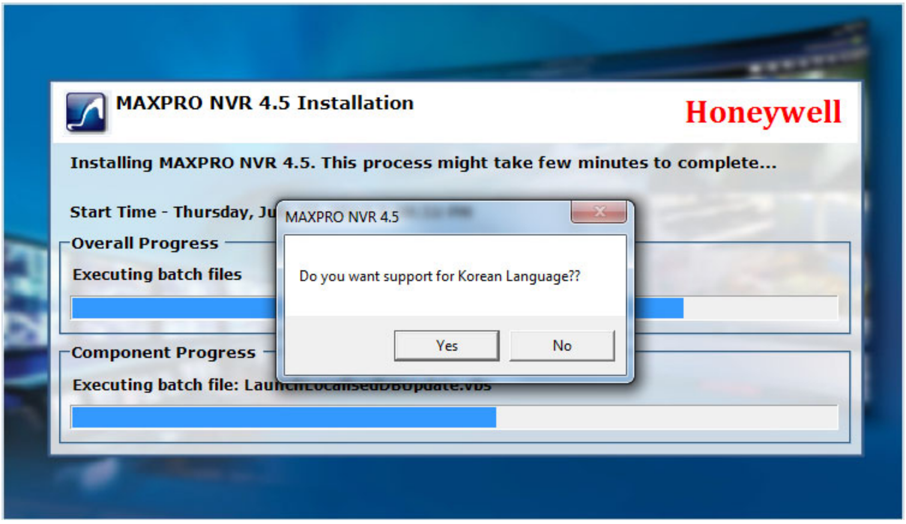
Target Machine: T69-SYS2

Installed Configuration: Maxpro NVR 4.1.0.123 RevB,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. A confirmation message to support Korean Language is displayed as shown below.



MAXPRO NVR 4.5 Installation

Installing MAXPRO NVR 4.5. This process might take few minutes to complete...

Start Time - Thursday, Ju

Overall Progress

Executing batch files

Component Progress

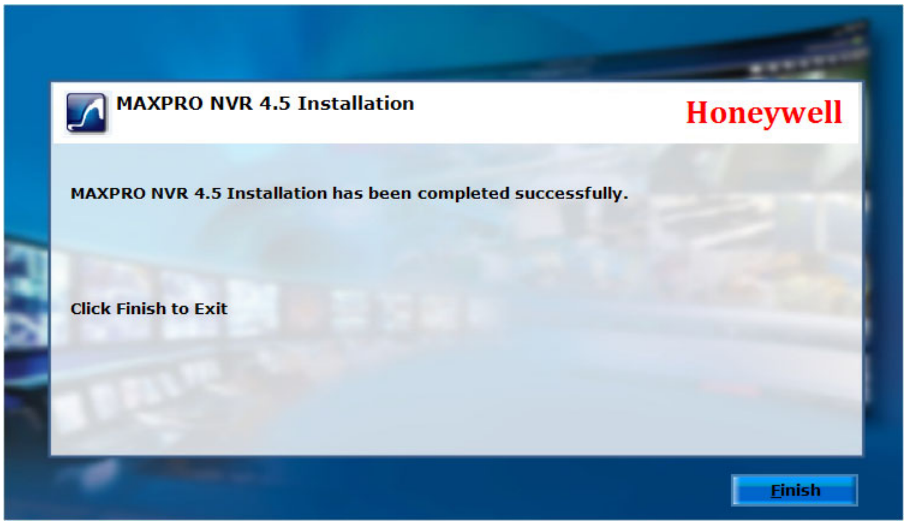
Executing batch file: Lau

MAXPRO NVR 4.5

Do you want support for Korean Language??

Installation Complete

Step 4. Click Yes if required. The installation process continues and once the installation is complete the completion page is displayed as shown below.



MAXPRO NVR 4.5 Installation

MAXPRO NVR 4.5 Installation has been completed successfully.

Click Finish to Exit

Step 5. Click Finish to complete the installation and close the wizard.

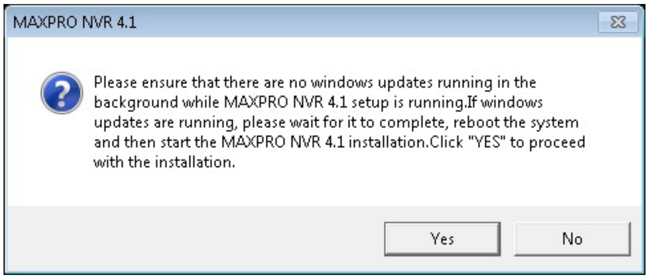
Upgrade to MAXPRO NVR 4.1 Build 123 Rev B

Upgrade is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H SP1 to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H (beta) to NVR 4.1 Build 123 Rev B

To upgrade to MAXPRO NVR 4.1 Service Pack

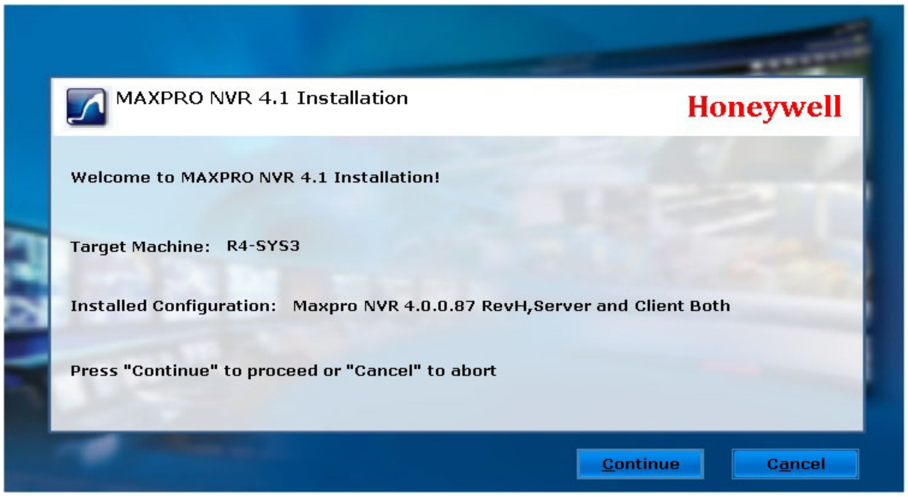
Step 1. Double click MAXPRO NVR 4.1 Setup.exe. The WinRAR self extracts the files and displays the Windows update message.



MAXPRO NVR 4.1

Please ensure that there are no windows updates running in the background while MAXPRO NVR 4.1 setup is running.If windows updates are running, please wait for it to complete, reboot the system and then start the MAXPRO NVR 4.1 installation.Click "YES" to proceed with the installation.

Step 2. Click Yes to proceed, the installation wizard starts and the Welcome page appears.


MAXPRO NVR 4.1 Installation

Honeywell

Welcome to MAXPRO NVR 4.1 Installation!

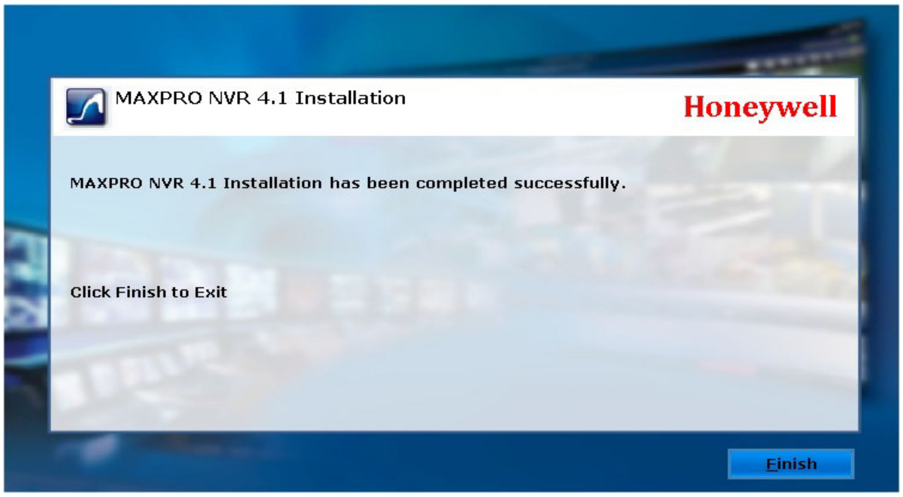
Target Machine: R4-SYS3

Installed Configuration: Maxpro NVR 4.0.0.87 RevH,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Welcome Wizard

Step 3. Click Continue to start the installation. After the installation is finished, the following page appears.


MAXPRO NVR 4.1 Installation

Honeywell

MAXPRO NVR 4.1 Installation has been completed successfully.

Click Finish to Exit

Installation Complete

Step 4. Click Finish to complete the installation and close the wizard.

Upgrade to MAXPRO NVR 4.0

Upgrade is supported from MAXPRO NVR 3.1 SP1 or later version to MAXPRO NVR 4.0 Build 87 Rev H.

If you are upgrading from a version lower than 3.1 SP1 to MAXPRO NVR 4.0 then an error message is displayed. Upgrade to v3.1 SP1 Build 70C on top of the lower versions and then upgrade to NVR 4.0 Build 87 Rev H.

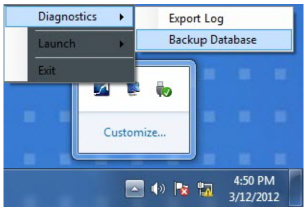
Note: *Ensure that Services.msc console is closed before Installing or upgrading the MAXPRO NVR. See the* Before you Begin - Disable Defragmentation *section on page* 103.

If you are upgrading to MAXPRO NVR 4.1 Build 123 Rev B then upgrade is supported as explained below:

- From NVR 4.0 87 Rev H to NVR 4.1 Build 123 Rev B
- From NVR 4.0 87 Rev H SP1 to NVR 4.1Build 123 Rev B
- From NVR 4.0 87 Rev H (beta) to NVR 4.1 Build 123 Rev B

Taking the Database Backup

Honeywell recommends database backup before running the upgrade. Database backup can be done from MAXPRO NVR Agent.



Taking Database backup using the MAXPRO NVR Agent

Note: *In MAXPRO NVR 3.1 or later version, a new scheduled backup mechanism is added which will retain the last 7 days of Database Backup. In case of upgrade, if the backup is set in the system already then same backup drives are maintained in the configuration and used in the new backup mechanism.*
Or
If the backup is not set then by default the first recording drive is selected for database backup according to the alphabetical order. If you want to change the drive then edit the TakeNVRbackup.bat file which is available in C:\Install\BackupData and mention the required drive name.

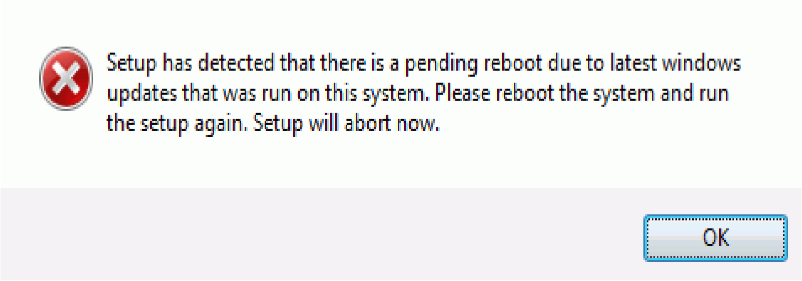
How to upgrade to MAXPRO NVR 4.0

Step 1. Insert the MAXPRO NVR 4.0 setup DVD in the DVD drive, browse the DVD drive, and then double-click setup.exe

Or
Go to the MAXPRO NVR setup folder on your computer, and then double-click setup.exe. A dialog box appears with the question - “Do you want to validate the setup before continuing MAXPRO NVR 4.0 installation?”, click Yes to validate the

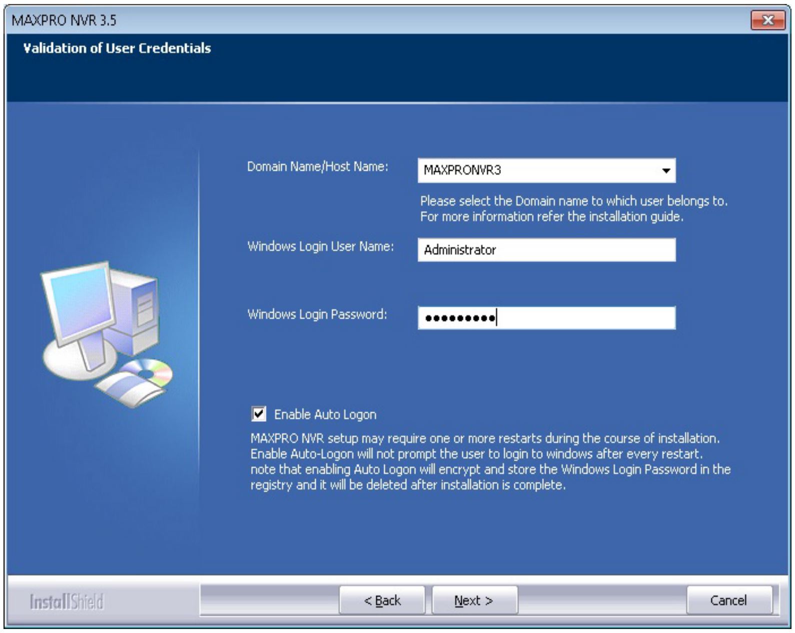
setup files are not corrupted before continuing the installation and click No to skip the validation to continue the setup. The installation wizard starts and the Welcome screen appears.

Note: *If any pending reboot is there due to windows updates, the following error message appears, and the installation stops. Please ensure that you reboot your computer and run the setup again.*



Setup has detected that there is a pending reboot due to latest windows updates that was run on this system. Please reboot the system and run the setup again. Setup will abort now.

Step 2. Click Next. The Validation of User Credentials appears.



MAXPRO NVR 3.5

Validation of User Credentials

Domain Name/Host Name: MAXPRONVR3

Please select the Domain name to which user belongs to.
For more information refer the installation guide.

Windows Login User Name: Administrator

Windows Login Password: •••••••••

☑ Enable Auto Logon

MAXPRO NVR setup may require one or more restarts during the course of installation. Enable Auto-Logon will not prompt the user to login to windows after every restart. note that enabling Auto Logon will encrypt and store the Windows Login Password in the registry and it will be deleted after installation is complete.

Validation of User Credentials

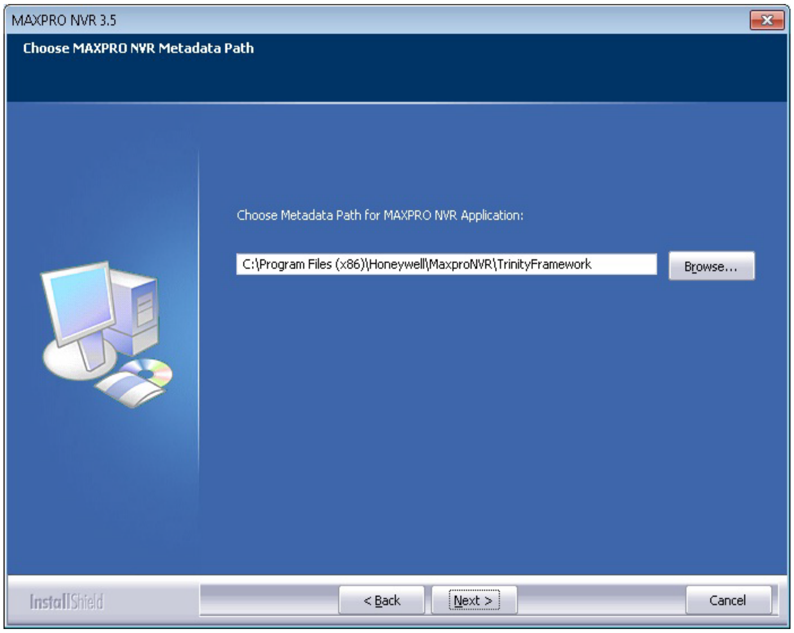
Step 3. Select your Domain Name/Host Name.

Step 4. Type your Windows User Name.

Step 5. Type your Windows Password.

Note: *Honeywell recommends to use the newly created Administrator user account as explained in* Before you Begin - Changing the default Windows Administrator Account Created By NVR, *page* 103.

Step 6. Click Next. The Choose Metadata Path appears.



MAXPRO NVR 3.5

Choose MAXPRO NVR Metadata Path

Choose Metadata Path for MAXPRO NVR Application:

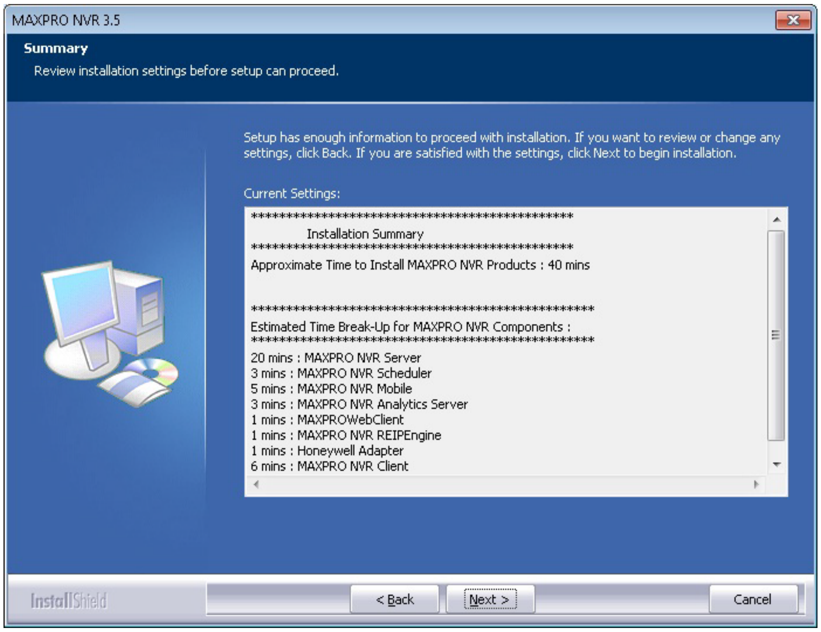
C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework

Choose Metadata Path

Step 7. Click Browse to specify a new path for Metadata in NVR Application.

Note: *If you want to move your metadata to a non-OS partition then please choose the appropriate path. Upgrade will move the metadata accordingly.*

Step 8. Click Next. The summary screen appears.



MAXPRO NVR 3.5

Summary

Review installation settings before setup can proceed.

Setup has enough information to proceed with installation. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin installation.

Current Settings:

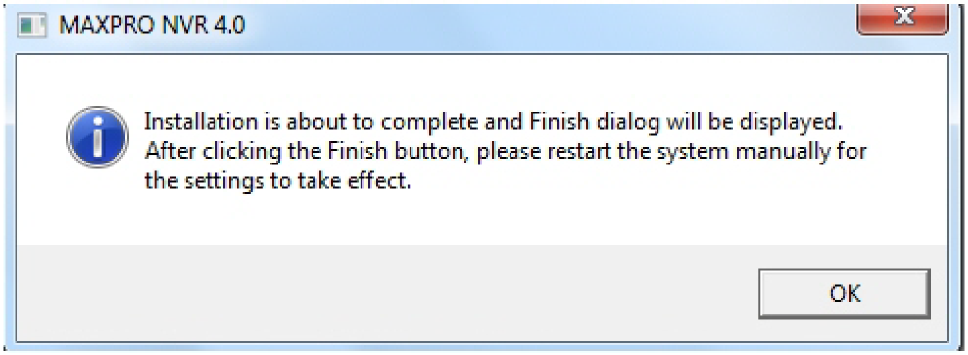
```
*************************************************
        Installation Summary
*************************************************
Approximate Time to Install MAXPRO NVR Products : 40 mins


****************************************************
Estimated Time Break-Up for MAXPRO NVR Components :
****************************************************
20 mins : MAXPRO NVR Server
3 mins : MAXPRO NVR Scheduler
5 mins : MAXPRO NVR Mobile
3 mins : MAXPRO NVR Analytics Server
1 mins : MAXPROWebClient
1 mins : MAXPRO NVR REIPEngine
1 mins : Honeywell Adapter
6 mins : MAXPRO NVR Client
```

Summary

Step 9. Click Next. The upgrade status of various components appears.

Note: *During upgrade, SQL Server 2008 Express is not upgraded to SQL Server 2012 Express to reduce upgrade time and only the Trinity database is updated with changes required for v4.0.*

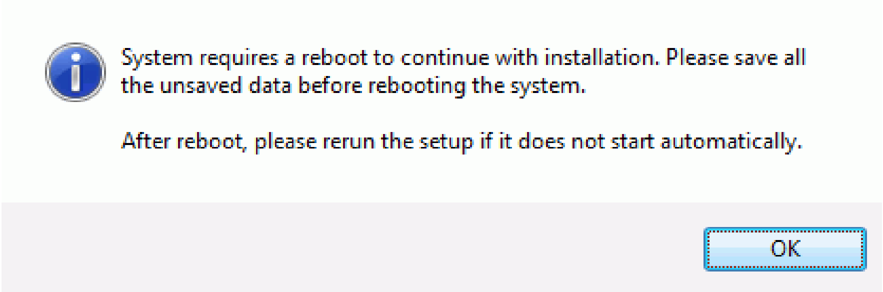
Step 10. When the upgrade is about to complete, the following message is displayed.



Installation is about to complete and Finish dialog will be displayed. After clicking the Finish button, please restart the system manually for the settings to take effect.

Step 11. Click OK. The Finish dialog appears with the options to Validate and to Finish the installation.

- Click Validate to verify the installed files on your NVR. If there are no errors then a message appears – Setup has been validated successfully without any error. Click here to view report. If there are errors, the message shows there are errors and the report can be reviewed to identify the error and contact Honeywell technical support if required to correct them on reinstall.
- Click Finish. The installation wizard starts all the services which may take a few minutes. After the wizard closes, as mentioned in step 10 it is recommended to Restart the system manually for the changes to take effect. If you are prompted to reboot the system then the following message is displayed.


System requires a reboot to continue with installation. Please save all the unsaved data before rebooting the system.

After reboot, please rerun the setup if it does not start automatically.

Reboot prompt

Step 12. Click OK to complete the MAXPRO NVR upgrade.

This page is intentionally left blank

CHAPTER

9 MAXPRO NVR WEB CLIENT

In this chapter...

Introducing Web Client

The MAXPRO NVR Web Client allows you to remotely access the MAXPRO NVR server and perform video surveillance using a web browser such as Internet Explorer. It gives you the flexibility to view live video and perform the basic video surveillance functions remotely over the web.

MAXPRO NVR Web client is available with MAXPRO NVR 4.0. By default MAXPRO NVR installs the Web client and MAXPRO Web Configurator along with the NVR 4.0 installation. You can use the web client once you have installed the NVR 4.0.

MAXPRO NVR Web Client functions involve the following tasks:

- Viewing the live video
- Viewing Recorded Video (Playback)
- Taking Snapshot
- Viewing Presets

Limitation with Privacy Protection Settings

- Anonymization is not supported in Web. If user is tries to see Anonymized video and also camera Anonymized option is enabled then an error message “Trying to access Anonymized Stream” is displayed.
- When an Operator (non-admin) logs into the Web Client and tries to view playback for any video then an error message “Four Eye authentication Privilege Failure” is displayed.

Installing Web Client

By default MAXPRO NVR 4.0 installs the Web Client component on your machine. It also installs the MaxproWEBConfigurator utility to change or update the system and server configuration. If you want to access the MAXPRO NVR Server using Web Client remotely through a supported web browser then you should install Silverlight on the remote machine.

Prerequisites to access MAXPRO NVR Server through Web Client

The following are the prerequisites to access the MAXPRO NVR server through Web Client.

- Silverlight: Ensure that Silverlight version 5 and above is installed on your machine. If you don't have the Silverlight plug-in on your machine, you can download it from the following Microsoft link. http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx

Caution: For better security, close the browser upon logout.

Note: *Silverlight plug-in is not supported by Chrome version 42.x or above and Microsoft Edge browser.*

- Web Browsers Supported on Windows Systems: Ensure that at least one of the following supported web browsers are installed on your PC:
- Internet Explorer version 8 or above
- Firefox version 15.0.1 or above
- Chrome version 32.x to 41.x only.

Note: *MAXPRO NVR Web Client is only supported by below Web Browsers on Windows 10 with Silverlight plug-in installed*

- Internet Explorer version 11 or above
- Firefox version 40 or above

Note:

- Web Browsers Supported on MAC systems: Not supported.

Setting the MAXPRO Web Configurator

By default MAXPRO NVR installs the Web Configurator and 📹 is displayed on your desktop.

MAXPRO NVR Web Configurator is a utility and it allows you to perform the following:

Step 1. System Configuration

Step 2. Server Configuration

Step 3. Security Configuration

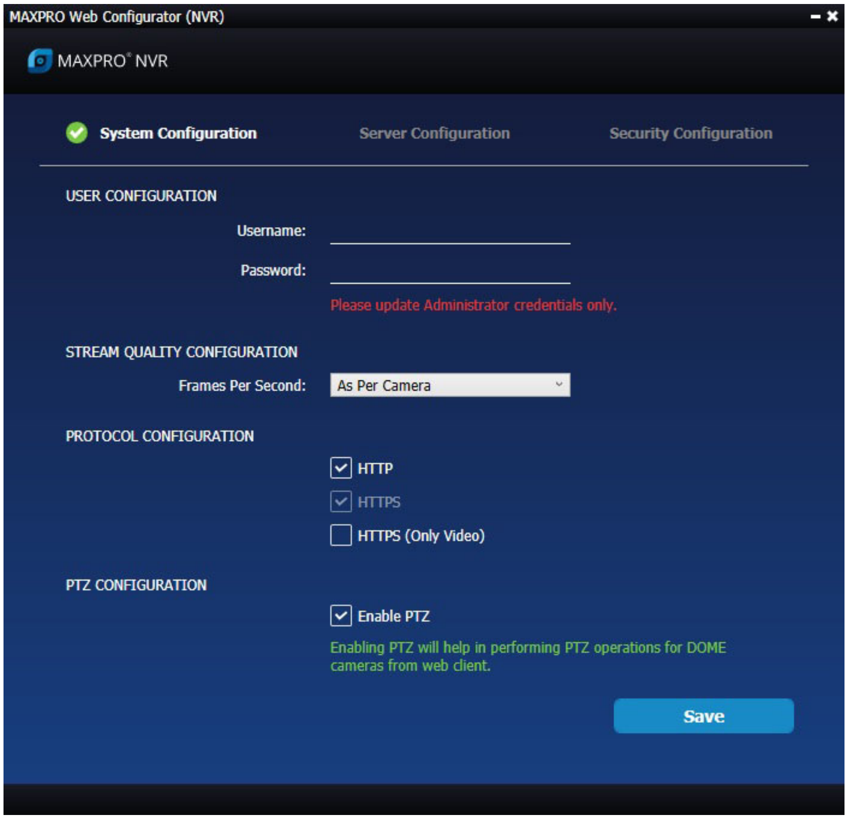
System Configuration tab: The system configuration tab allows you to update the administrator user credentials and the FPS for a better Stream quality. It also allows you to set the protocol for secure communication.

Server Configuration tab: The server configuration tab allows you to update the Web Server and MAXPRO NVR Server IP details.

Security Configuration tab: The Security Configuration tab automates the manual process of Creating Self Signed Certificate, Installing the Certificate, Binding the generated certificate with https and registers the same with IIS to use the same. It also allows you to configure the Silverlight control to access a service in another domain.

To set the Web Configurator

Step 1. Double-click on the desktop. The MAXPRO Web Configurator dialog box appears. By default the System Configuration tab is selected.



MAXPRO Web Configurator (NVR)

MAXPRO® NVR

✓ System Configuration | Server Configuration | Security Configuration

USER CONFIGURATION

Username:

Password:

Please update Administrator credentials only.

STREAM QUALITY CONFIGURATION

Frames Per Second: As Per Camera

PROTOCOL CONFIGURATION

☑ HTTP

☑ HTTPS

☐ HTTPS (Only Video)

PTZ CONFIGURATION

☑ Enable PTZ

Enabling PTZ will help in performing PTZ operations for DOME cameras from web client.

Save

MAXPRO WebConfigurator

Step 2. Under User Configuration: When the (non-window) Administrator log on name and password is changed then you can update the credentials of MAXPRO NVR Web Client to log on.

- Type the Username and Password and then click Update.

Note: *You can update only the NVRAdministrator credentials used by the Web Server. If you are changing the default administrator user credentials (admin/trinity) in NVR through the desktop client, then you should change and update the credentials in MaxproWEBConfigurator as well for Web Server to communicate with NVR and Web Clients.*

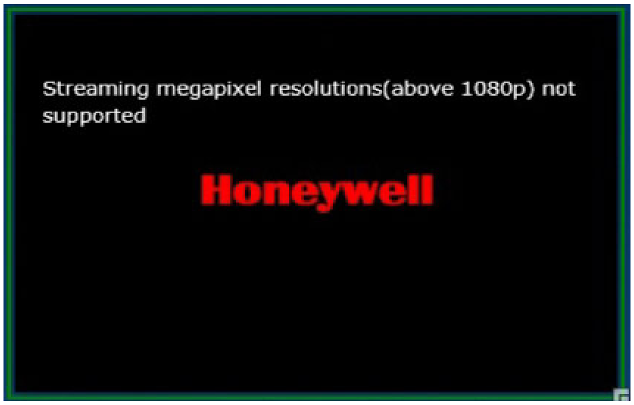
The Administrator credentials used by the Web Server should be configured as a non-Windows Administrator user in the MAXPRO NVR through the desktop client. As a good security practice, it is recommended to update the default credentials on your system.

Step 3. Under Stream Quality Configuration:

- Select the required Frames Per Second options as applicable and then click Save. The available options are:

- As Per Frame: Select this option to view the video as per the camera stream settings. If the camera supports 30 frames per second to stream the video then you can view 30 frames per second and accordingly your bandwidth is consumed. By default As Per Frame option is selected and it is recommended not to change this option, because this provides you with the best quality video.
- Only IFrame: select this option if your bandwidth is low and if you want to view only one IFrame per second.

Note: *MAXPRO NVR Web Client supports streaming quality resolution up to 1080p. Cameras configured above 1080p resolution are not supported. If you drag and drop a camera configured with megapixel resolutions (above 1080p) then a message appears and video is not displayed as shown below.*



Streaming megapixel resolutions(above 1080p) not supported

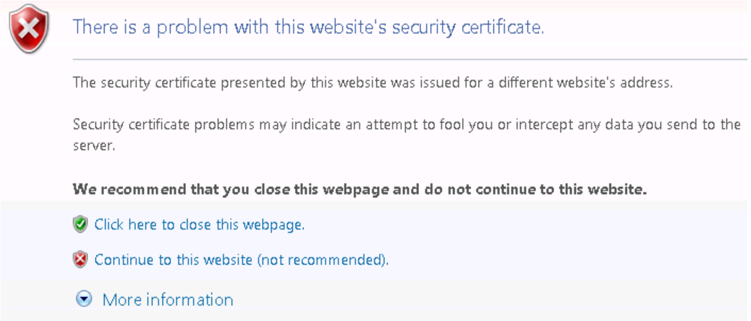
Step 4. Under Protocol Configuration:

- Click the appropriate Protocol options for secure communication. The available options are HTTP, HTTPS, HTTPS (Only Video). By default HTTP and HTTPS protocol is selected.

Note:

- Video to the Web Client is always transmitted over HTTP. Non-video data is transmitted over HTTPS/HTTP based on the protocol configuration settings.
- Please ensure ports required for both video and non-video data is considered in any port forwarding settings.

Note: *If you want to access the web client using secured connection then click the HTTPS option. When you access the MAXPRO NVR server using the URL https://<MAXPRO NVR Server IP or Machine /Computer name>/MAXPROWEB/ then the following message is displayed. Click Continue to this website to proceed. It is recommended to verify the certificate to check whether it is issued by a valid Certificate Authority. See* Viewing the Certificate Information *for more information.*



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

The above message appears by default when you access the NVR server for the first time. Honeywell recommends you to buy a Domain Name specific certificate, create it and then install it. See the Creating Self Signed Certificate *section on page* 351 *and* Installing the Certificate *section on page* 355 *for more information. Or You can use the MAXPRO Web Configurator utility to create the Self Signed Certificate.*
Or
You can create a self signed certificate and then install it. See the Creating Self Signed Certificate *section on page* 351 *and* Installing the Certificate *section on page* 355 *for more information.*
The above settings are applicable to Internet Explorer, Chrome, Firefox and Safari web browsers. These settings are valid if the web client is accessed using the Domain/Host Name. If you access the web client using the IP then the above settings are not valid.

Caution: For better security, close the browser upon logout.

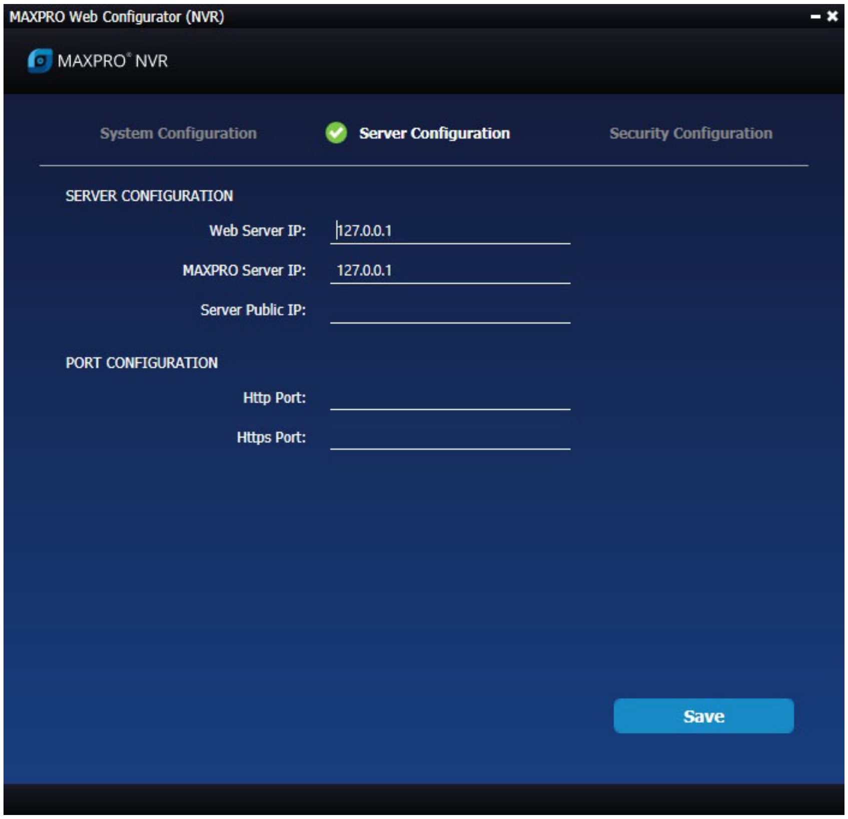
Step 5. Under PTZ Configuration:

- Select the Enable PTZ check box to perform PTZ operations on a PTZ camera from Web Client.

Note: *PTZ feature is not supported and It is not recommended to use this feature in the current release. Enabling PTZ will help in performing PTZ operations fro DOME cameras from web client.*

Step 6. Click Save.

Step 7. Click the Server Configuration tab. The Server Configuration screen appears.



SERVER CONFIGURATION

Web Server IP: 127.0.0.1

MAXPRO Server IP: 127.0.0.1

Server Public IP:

PORT CONFIGURATION

Http Port:

Https Port:

MAXPROWebConfigurator-Server Configuration

Note: *By default the Web Server and the MAXPRO Server is installed on the NVR server machine and the IPs are set by default to local IP or computer/machine name. If it is not set by default in your system then it is recommended to change these settings to NVR Server (local) computer/machine name. For Honeywell supplied NVR boxes, default computer/machine name is MAXPRO-NVR and can be updated in the configuration from the tool.*

Step 8. Under Server Configuration:

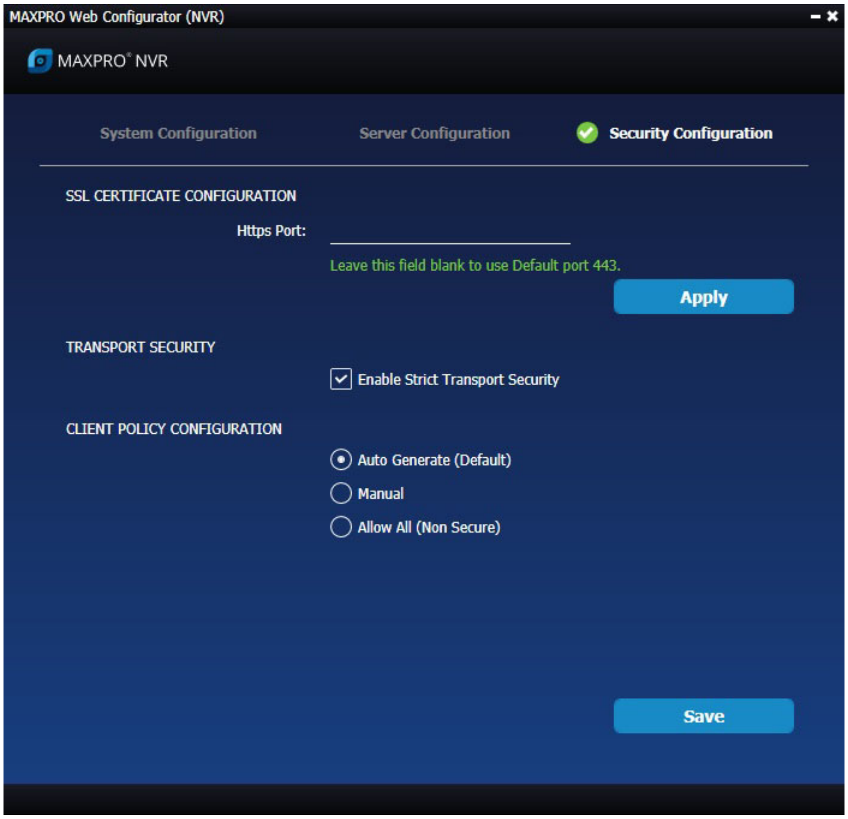
- Web Server IP: If the MAXPRO NVR server computer/machine name or IP (as applicable) is changed then you should change the Web Server IP. Type the new computer/machine name or IP (as applicable) in this box and then click Update.
- MAXPRO Server IP: If the MAXPRO NVR server computer/machine name or IP (as applicable) is changed then you should change the MAXPRO Server IP. Type the new computer/machine name or IP (as applicable) in this box and then click Update. Both Web Server IP and MAXPRO Server IP should be same.
- Server Public IP: If you want to host the MAXPRO Web client via internet (or Public) then you need to provide the Public Server IP.Type the new Public IP (as applicable) in this box and then click Update.

Step 9. Under Port Configuration:

- Http Port: If you want to change the http default port 80 to some other port number then type the required port number and click Apply.
- Https Port: If you want to change the https default port 443 to some other port number then type the required port number and click Apply.
  Port change option in the Configurator tool is available from 3.1 Build 65 Rev C or higher version.

Step 10. Click Save.

Step 11. Click the Security Configuration tab. The Security Configuration screen appears.



MAXPRO Web Configurator (NVR)

MAXPRO® NVR

System Configuration | Server Configuration | ✓ Security Configuration

SSL CERTIFICATE CONFIGURATION

Https Port: ______

Leave this field blank to use Default port 443.

TRANSPORT SECURITY

☑ Enable Strict Transport Security

CLIENT POLICY CONFIGURATION

● Auto Generate (Default)

○ Manual

○ Allow All (Non Secure)

MAXPROWebConfigurator-Security Configuration

Step 12. Under SSL Certificate Configuration:

- Type the Port number in the box provided if the Https binding is other than 443 and then click Apply. The default port is 443.

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*

Step 13. Under Transport Security, select the Enable Strict Transport Security check box to avoid or protect from hacking.

Step 14. Under Client Policy Configuration: Allows you to modify the C:\inetpub\wwwroot\clientaccesspolicy.xml & C:\inetpub\wwwroot\crossdomain.xml file.

- Click the required Client Policy option. The available options are
- Auto Generate (Default): This options makes entries to the above files such that the local Silverlight application (Web client) is able to make request to local ISOM.
- Manual: If Web Client and ISOM are on different machine or any other Silverlight application is trying to access ISOM then the above xml file need to be modified. Choose manual to make the modification manually. For more information on configuring Cross Domain or Client Access Policy browse the below websites: http://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html https://msdn.microsoft.com/library/cc197955(v=vs.95).aspx
- Allow All (non Secure): Non secure mode. If you want to allow all Silverlight clients to connect to ISOM hosted on the machine then you can click this option. Use with caution. This options also helps to troubleshoot the wrong configurations by providing full access temporarily.

Note: *Auto mode is flexible and is the recommended mode.*

Caution: Ensure that you exercise caution while choosing the options other than the Default.

Step 15. Click Save.

Creating Self Signed Certificate

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. See* Procuring and Installing CA Certificate *section. Or Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for security settings.*

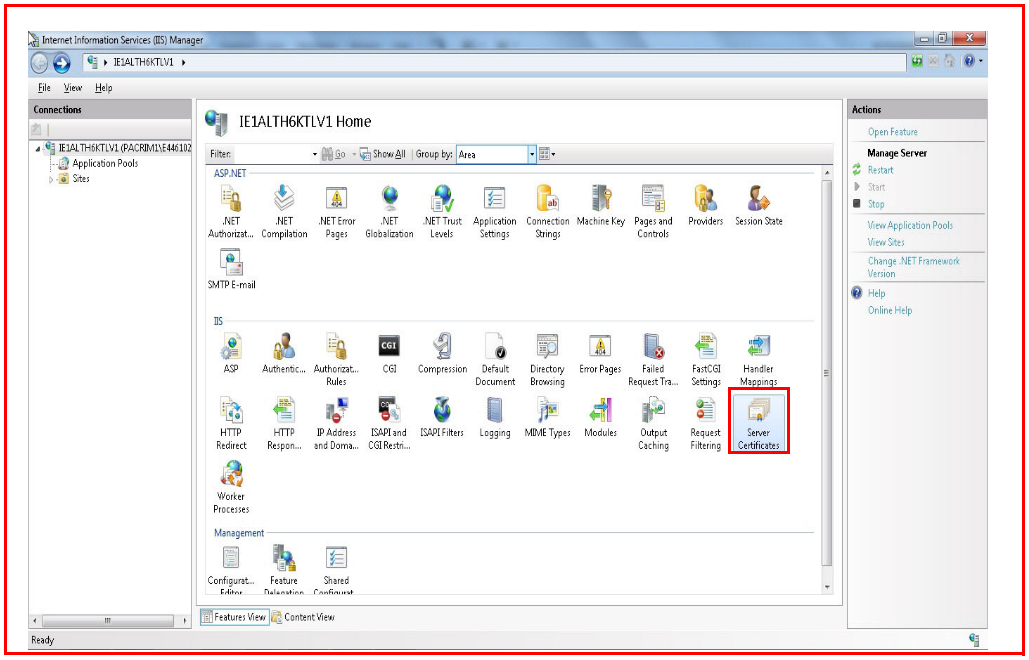
Self signed certificate is required if you want to access the MAXPRO NVR server using your domain name. You should create a certificate, bind it to the https and then install the certificate to access the server using the web browser (Internet Explorer, Chrome, Firefox and Safari).

To create self signed certificate

Step 1. Open the Internet Information Manager (IIS) window.

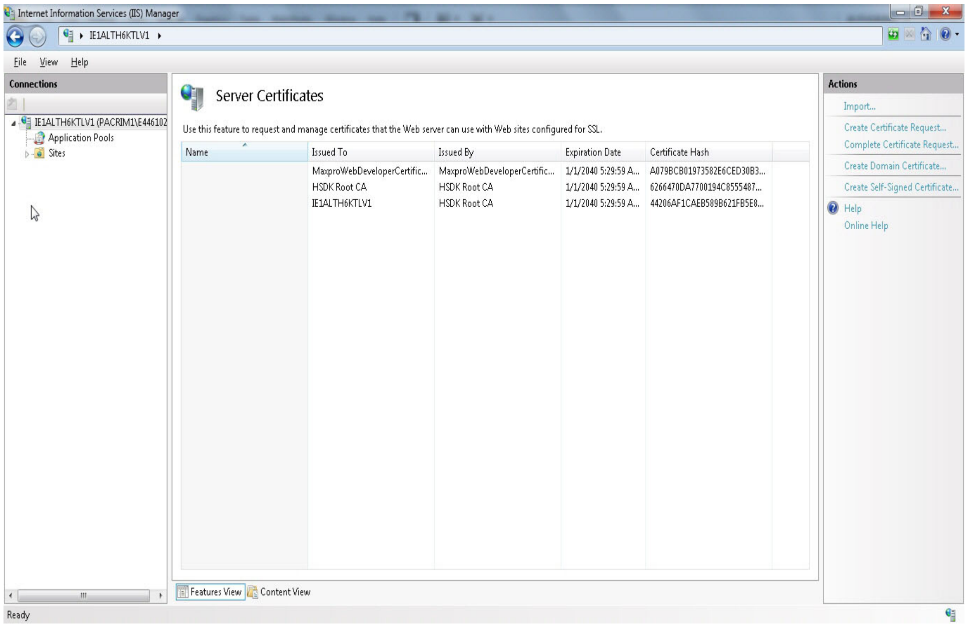
Step 2. Select the server node under Connections pane.

Step 3. Under IIS, double click the Server Certificate option Figure .



Home

The Server Certificate window is displayed.


Internet Information Services (IIS) Manager
IE1ALTH6KTLV1
File View Help
Connections
IE1ALTH6KTLV1 (PACRIM1\E446102
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Features View
Content View
Ready

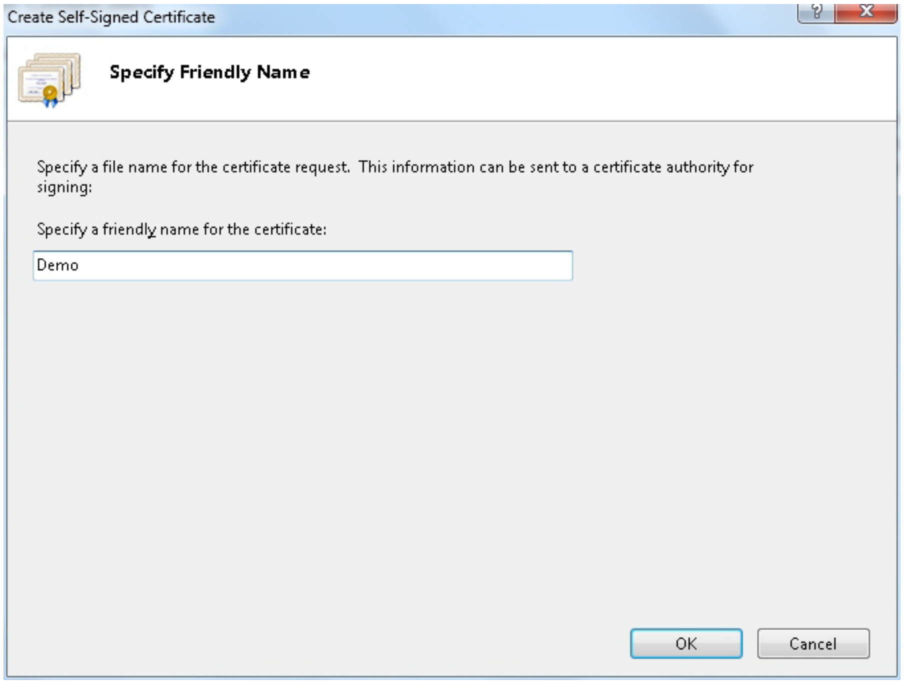
Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
	MaxproWebDeveloperCertific...	MaxproWebDeveloperCertific...	1/1/2040 5:29:59 A...	A079BCB01973582E6CED30B3...
	HSDK Root CA	HSDK Root CA	1/1/2040 5:29:59 A...	6266470DA7700194C8555487...
	IE1ALTH6KTLV1	HSDK Root CA	1/1/2040 5:29:59 A...	44206AF1CAEB589B621FB5E8...

Server Certificate

Step 4. Click the Create Self-Signed Certificate on the right-most pane. The Specify Friendly Name dialog appears.



Specify Friendly Name

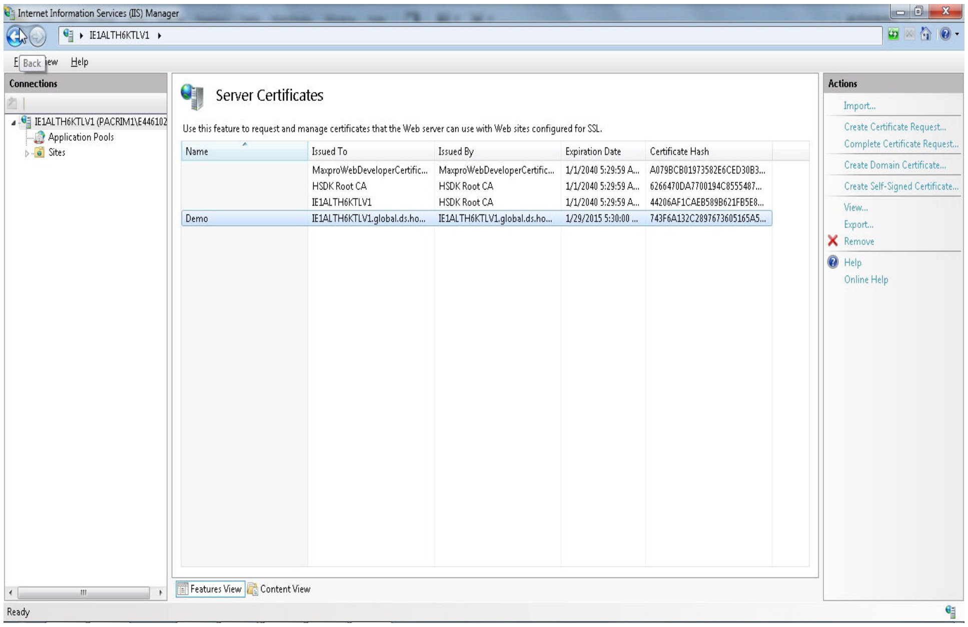
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Demo

Specify Friendly Name

Step 5. Type a friendly name for the certificate and then click OK. A new certificate is generated and listed under server certificates list as shown below:


Internet Information Services (IIS) Manager
IE1ALTH6KTLV1
Back
Help
Connections
IE1ALTH6KTLV1 (PACRIM1\E446102
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Features View
Content View
Ready

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
	MaxproWebDeveloperCertific...	MaxproWebDeveloperCertific...	1/1/2040 5:29:59 A...	A079BCB01973582E6CED30B3...
	HSDK Root CA	HSDK Root CA	1/1/2040 5:29:59 A...	6266470DA7700194C8555487...
	IE1ALTH6KTLV1	HSDK Root CA	1/1/2040 5:29:59 A...	44206AF1CAEB589B621FB5E8...
Demo	IE1ALTH6KTLV1.global.ds.ho...	IE1ALTH6KTLV1.global.ds.ho...	1/29/2015 5:30:00 ...	743F6A132C2897673605165A5...

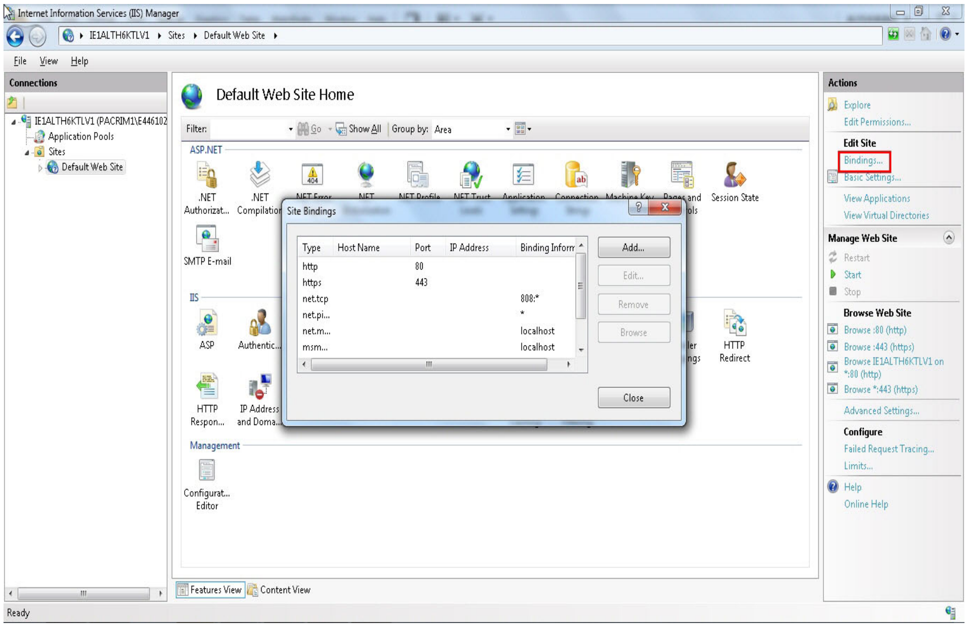
Generated Certificate

Binding the generated certificate with https

Step 1. In the Internet Information Manager (IIS) window, expand the server node under Connections pane.

Step 2. Navigate to Sites > Default Web Site.

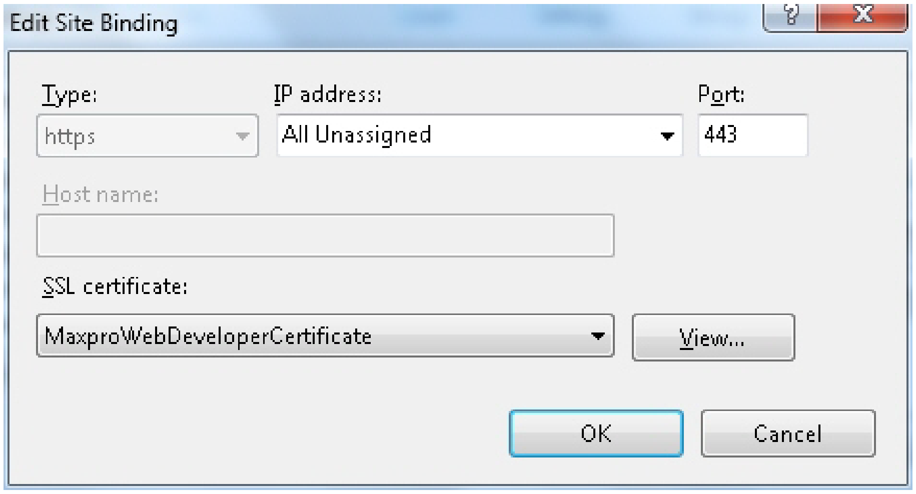
Step 3. Click Bindings in the right-most pane. The Site Bindings dialog appears.



Type	Host Name	Port	IP Address	Binding Inform
http		80		
https		443		
net.tcp				808:*
net.pi...				*
net.m...				localhost
msm...				localhost

Site Bindings Dialog

Step 4. Select the type as https and then click Edit. The Edit Site Bindings dialog appears.



Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: MaxproWebDeveloperCertificate

Edit Site Bindings

Step 5. Select the Demo SSL certificate from the SSL Certificate drop-down list.

Step 6. Select All Unassigned from the IP Address drop-down list.

Note: *Ensure that you select All Unassigned option from the IP Address drop-down list and the port should be 443.*

Step 7. Type the port number as 443.

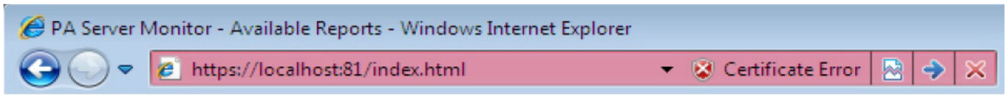
Step 8. Click OK.

Installing the Certificate

Once you have created a self signed certificate you need to install the certificate in the Internet Explorer on machines accessing the web client. If you do not install the certificate then the web browser displays the following error as shown in the figure Certificate Error.

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. See* Procuring and Installing CA Certificate *section.*

Caution: For better security, close the browser upon logout.

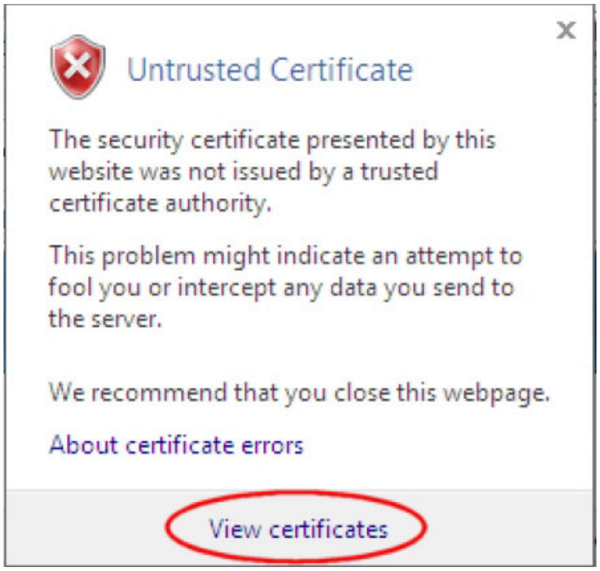


PA Server Monitor - Available Reports - Windows Internet Explorer

https://localhost:81/index.html

Certificate Error

To view the error details, click on the Certificate Error message. A Untrusted Certificate message box is displayed as shown below:



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

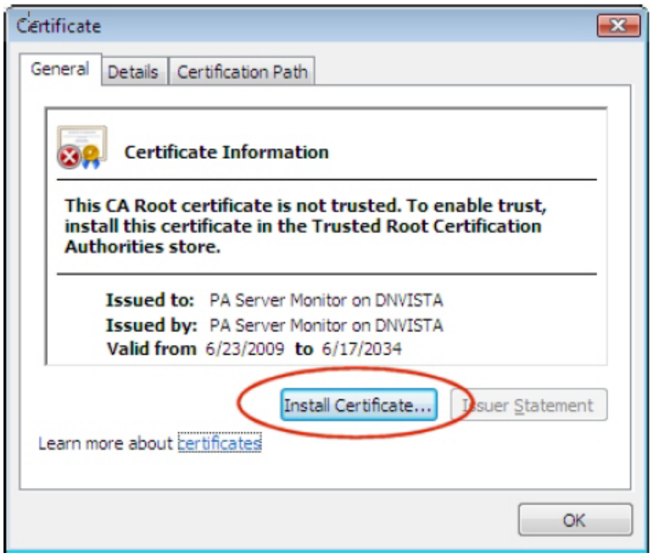
We recommend that you close this webpage.

Untrusted Certificate

To install the certificate

Step 1. Click View Certificate as shown in the figure Untrusted Certificate. The Certificate dialog box appears as below.

Tip: You can install the certificate using Internet Explorer. Once the installation is done you can access the MAXPRO NVR server using other browsers on the same machine using your domain name.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: PA Server Monitor on DNVISTA

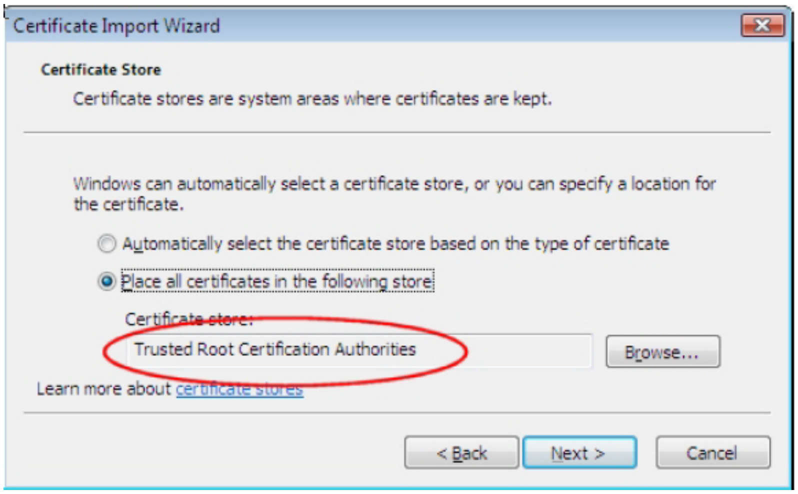
Issued by: PA Server Monitor on DNVISTA

Valid from 6/23/2009 to 6/17/2034

Learn more about certificates

Certificate

Step 2. Click the Install Certificate button. Certificate Import Wizard dialog box appears.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

Certificate Import Wizard

Step 3. Click the Browse button and then select the Trusted Certificate Authorities option.

Step 4. Click Next until Finish button is displayed.

Step 5. Click the Finish button. A confirmation message “you want to add the new certificate” is displayed.

Procuring and Installing CA Certificate

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. Refer to the 800-23557-E - Securing MAXPRO VMS_NVR Technical Notes for more security settings.*

Installing an SSL Certificate in Windows Server 2008 (IIS 7.0)

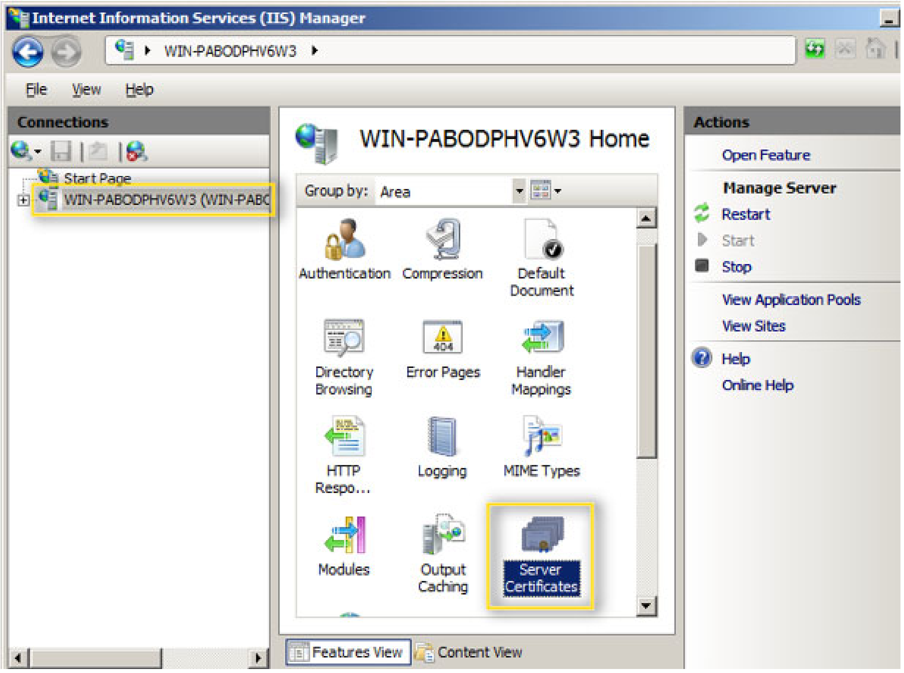
Windows Server 2008 includes Internet Information Services (IIS) 7.0. This new version makes several big changes in the way that SSL certificates are generated, making it much easier than previous versions of IIS. In addition to the new method of requesting and installing SSL certificates, IIS 7 includes the ability to:

- Request more than one SSL certificate at a time
- Import, export, and renew SSL certificates easily in IIS
- Quickly create a self-signed certificate for testing

Create the Certificate Signing Request

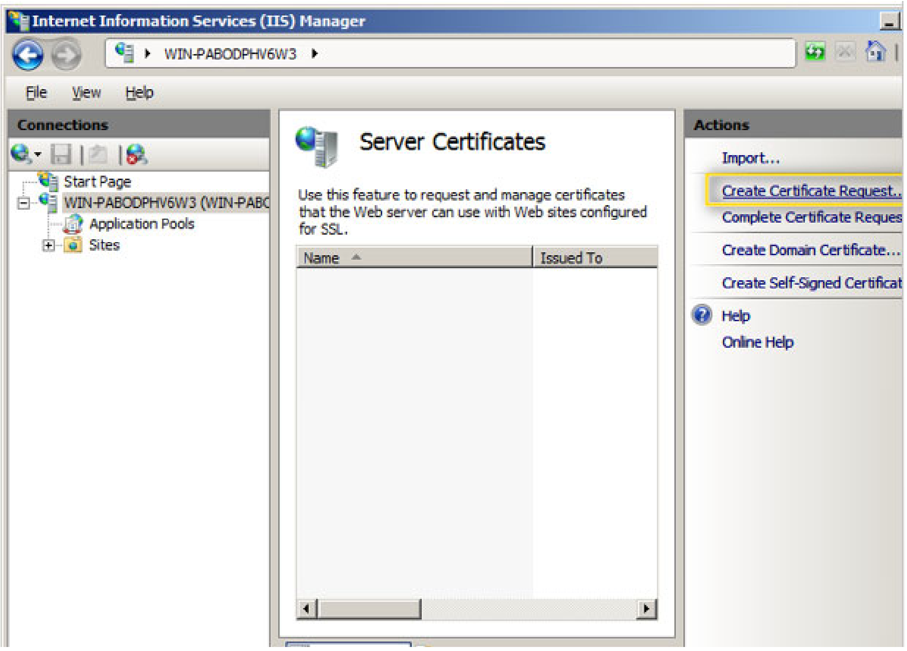
The first step in ordering an SSL certificate is generating a Certificate Signing Request. This is very easy to do in IIS7 using the following instructions. perform the below steps to create the Certificate Signing Request:

Step 1. Click on the Start menu, go to Administrative Tools, and then click on Internet Information Services (IIS) Manager. The IIS manger window is displayed.



IIS Home

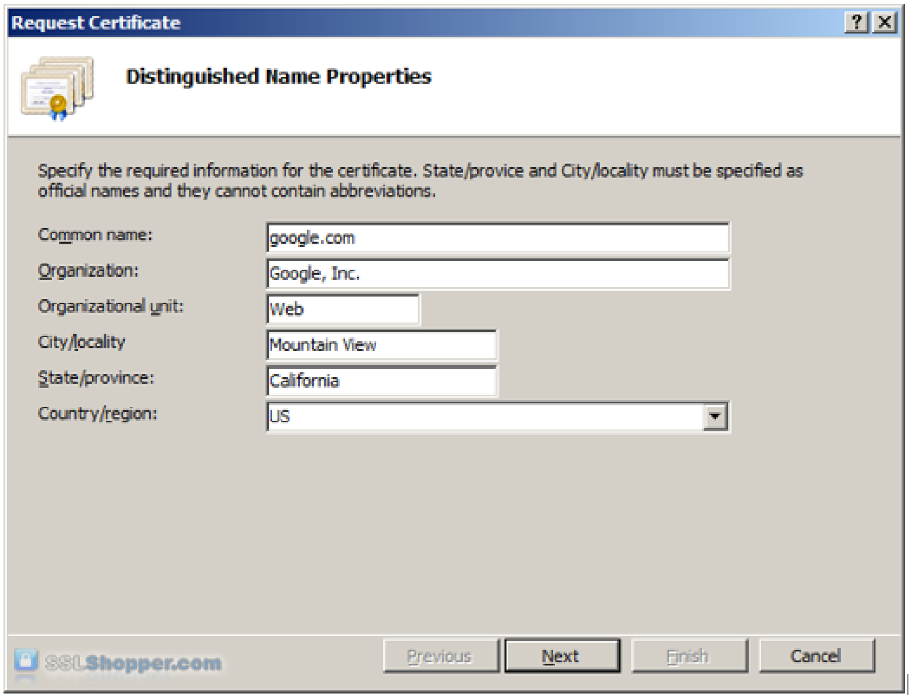
Step 2. Click on the name of the server in the Connections pane on the left. Double-click on Server Certificates.


Internet Information Services (IIS) Manager
WIN-PABODPHV6W3
File
View
Help
Connections
Start Page
WIN-PABODPHV6W3 (WIN-PABC
Application Pools
Sites
Server Certificates
Name
Issued To
Actions
Import...
Create Certificate Request...
Complete Certificate Reques
Create Domain Certificate...
Create Self-Signed Certificat
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Create Certificate Request

Step 3. In the Actions pane on the right, click on Create Certificate Request. The Request Certificate dialog box appears.



Specify the required information for the certificate. State/provice and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	google.com
Organization:	Google, Inc.
Organizational unit:	Web
City/locality	Mountain View
State/province:	California
Country/region:	US

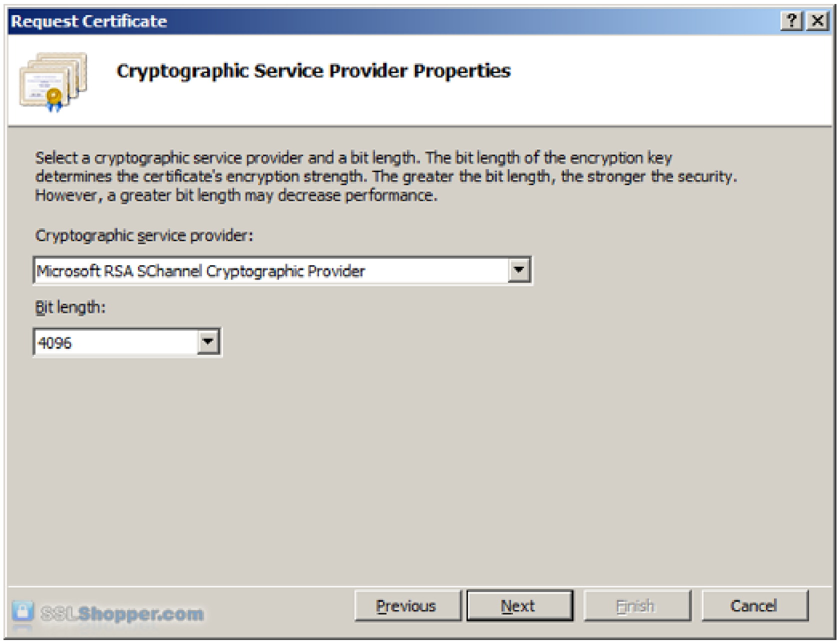
Request Certificate

Step 4. Enter all of the following information about your company and the domain you are securing and then click Next.

Name	Description	Examples
Common Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser or you will receive a name mismatch error.	*.google.com mail.google.com
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Google Inc.
Organizational Unit	The division of your organization handling the certificate. (Most CAs don't validate this field)	IT Web
City/Locality	The city where your organization is located.	Mountain View
State/province	The state/region where your organization is located. This shouldn't be abbreviated.	California

Name	Description	Examples
Country/ Region	The two-letter ISO code for the country where your organization is location.	US GB

Step 5. Leave the default Cryptographic Service Provider. Increase the Bit length to 2048 bit or higher. Click Next.



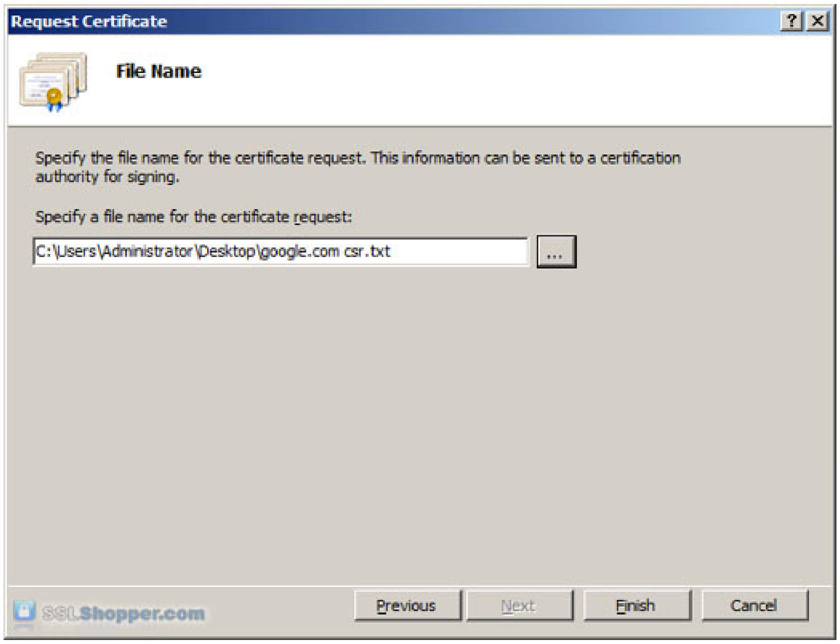
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 4096

Request Certificate

Step 6. Click the button with the three dots and enter a location and filename where you want to save the CSR file. Click Finish.



Request Certificate

File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\google.com csr.txt

Request Certificate

Step 7. Once you have generated a CSR you can use it to order the certificate from a certificate authority. If you don't already have a favorite, you can compare SSL features from each provider using our SSL Wizard or by comparing cheap SSL certificates, Wildcard Certificates, or EV certificates. Once you paste the contents of the CSR and complete the ordering process, your order is validated, and you will receive the SSL certificate file.

Installing the Certificate

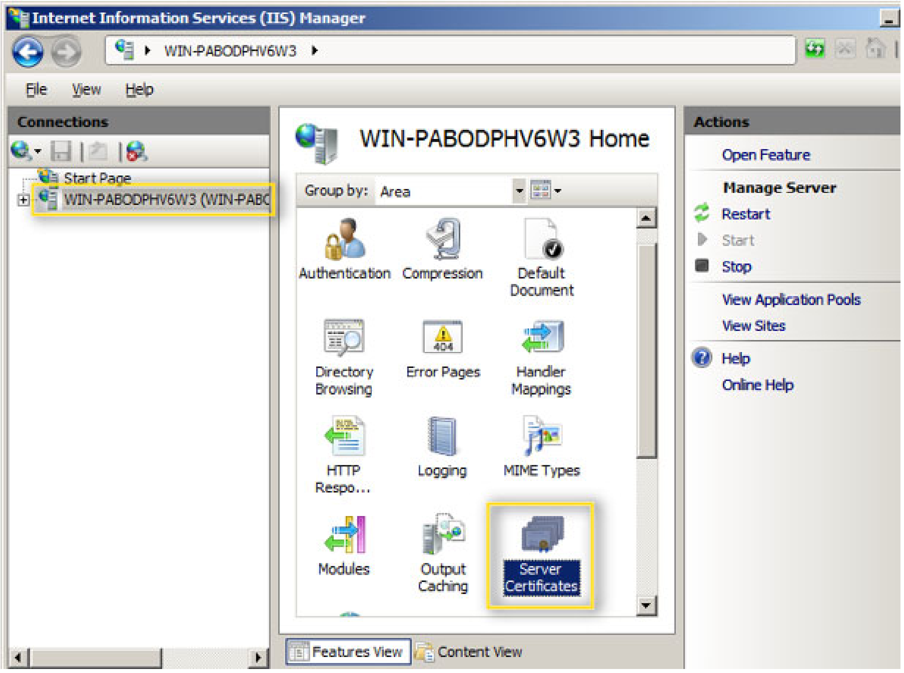
To install your newly acquired SSL certificate in IIS 7, first copy the file somewhere on the server and then follow these instructions:

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate See* Procuring and Installing CA Certificate *section.*

To install the certificate

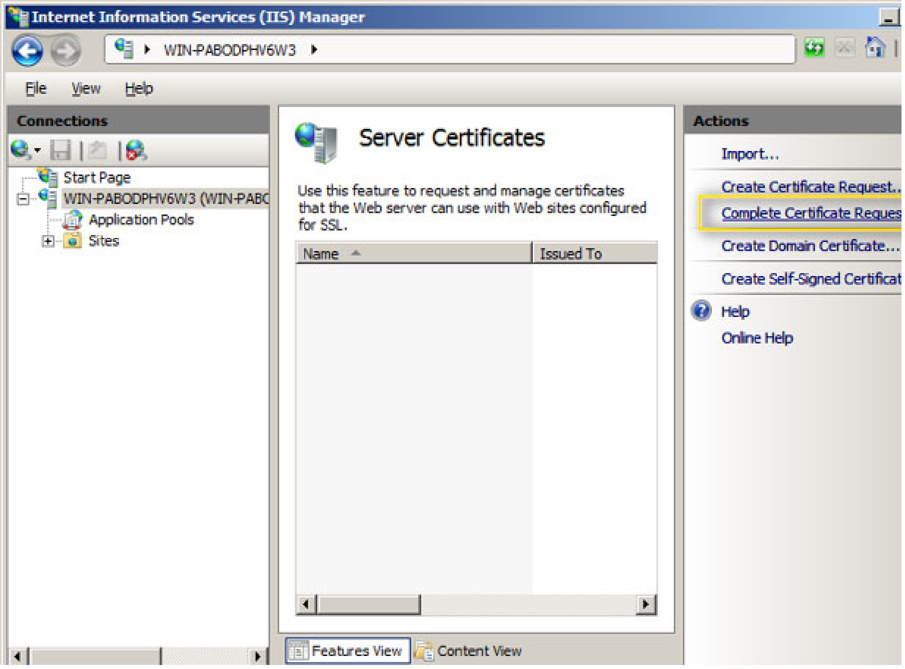
Step 1. Click on the Start menu, go to Administrative Tools, and click on Internet Information Services (IIS) Manager.

Step 2. Click on the name of the server in the Connections column on the left. Double-click on Server Certificates.



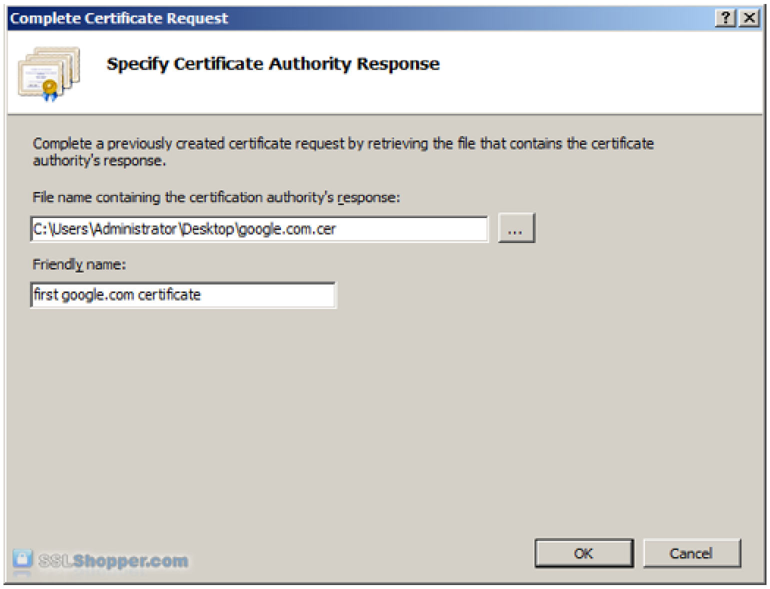
IIS Manger

Step 3. In the Actions column on the right, click on Complete Certificate Request...as shown below.


Internet Information Services (IIS) Manager
WIN-PABODPHV6W3
File
View
Help
Connections
Start Page
WIN-PABODPHV6W3 (WIN-PABC
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.
Name
Issued To
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Reques
Create Domain Certificate...
Create Self-Signed Certificat
Help
Online Help

IIS Manger

Step 4. Click the button with the three dots and select the server certificate that you received from the certificate authority. If the certificate doesn't have a .cer file extension, select to view all types. Enter any friendly name you want so you can keep track of the certificate on this server. Click OK.



Complete Certificate Request

Specify Certificate Authority Response

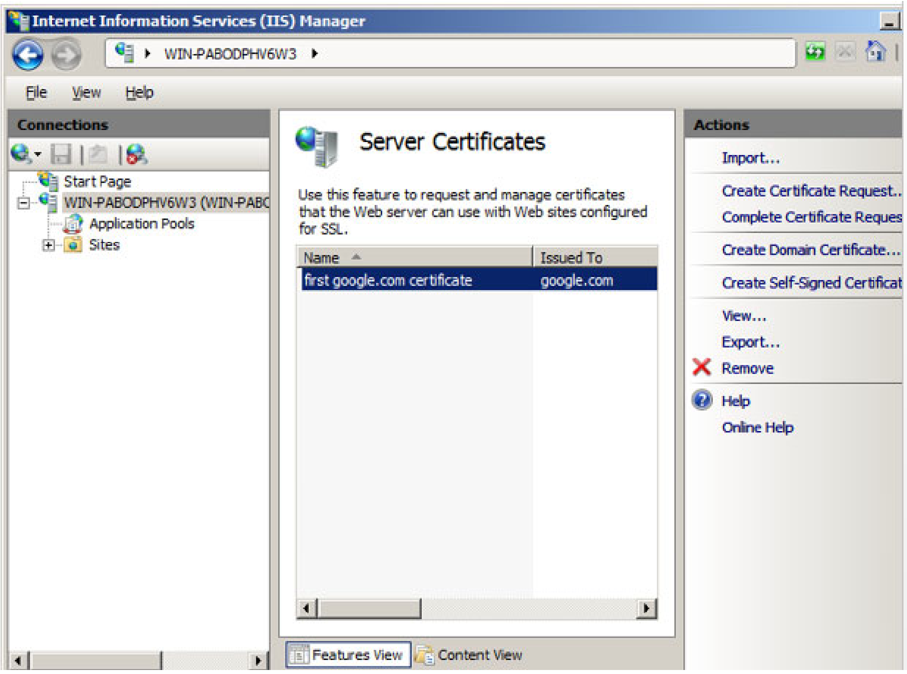
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\Users\Administrator\Desktop\google.com.cer

Friendly name: first google.com certificate

Complete Certificate request

Step 5. If successful, you will see your newly installed certificate in the list. If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate. Contact your certificate authority if you have problems with this.



Internet Information Services (IIS) Manager

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To
first google.com certificate	google.com

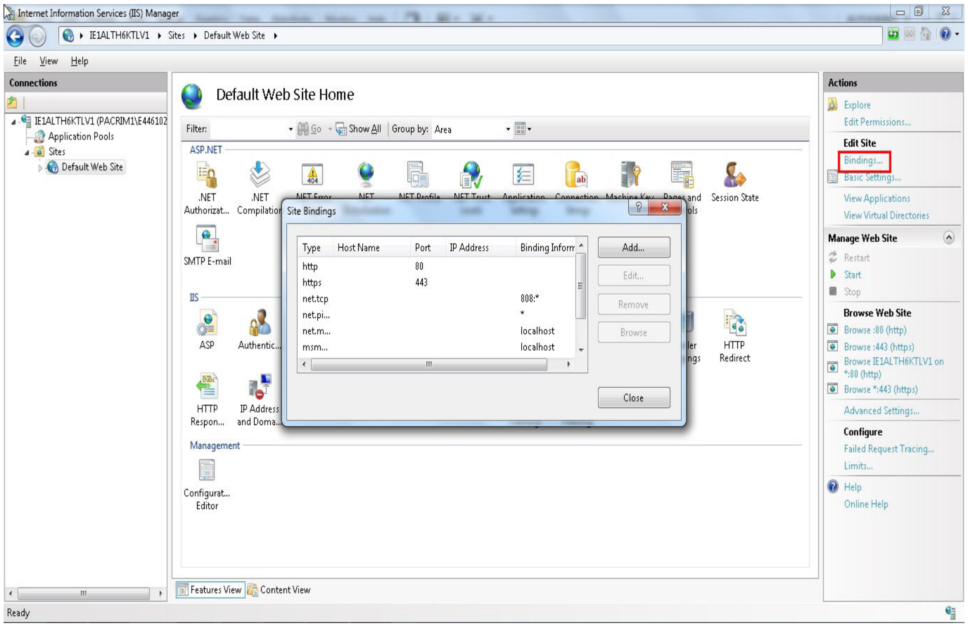
IIS manger-Server Certificate

Bind the Certificate to a website

Step 1. In the Internet Information Manager (IIS) window, expand the server node under Connections pane.

Step 2. Navigate to Sites > Default Web Site.

Step 3. Click Bindings in the right-most pane. The Site Bindings dialog appears.

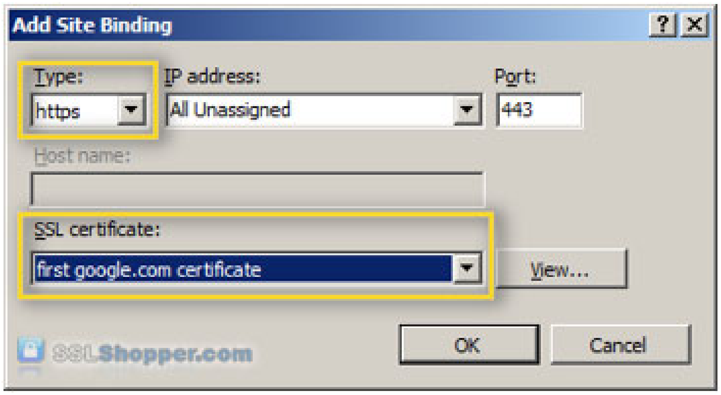


Type	Host Name	Port	IP Address	Binding Inforr
http		80		
https		443		
net.tcp				808:*
net.pi...				*
net.m...				localhost
msm...				localhost

Site Bindings Dialog

Step 4. Click on the Add...button

Step 5. Change the Type to https and then select the SSL certificate that you just installed. Click OK.



Type: https

IP address: All Unassigned

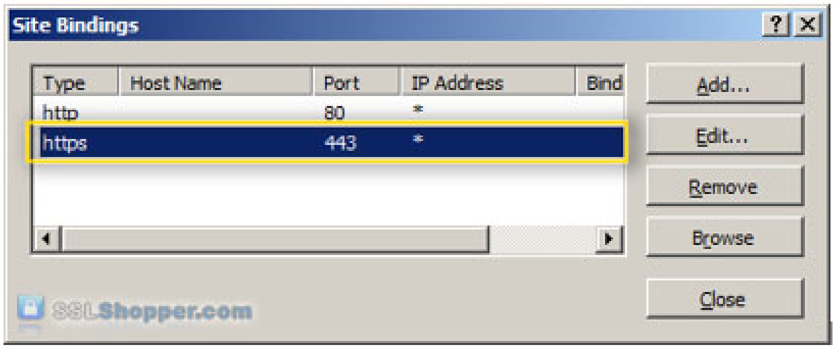
Port: 443

Host name:

SSL certificate: first google.com certificate

Add Site Bindings

Step 6. You will now see the binding for port 443 listed. Click Close.



Site Bindings

Type	Host Name	Port	IP Address	Bind
http		80	*	
https		443	*	

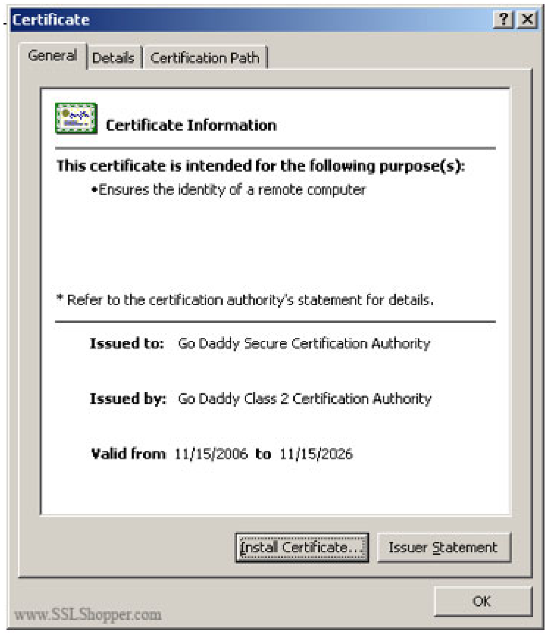
Install any Intermediate Certificates

Most SSL providers issue server certificates off of an Intermediate certificate so you will need to install this Intermediate certificate to the server as well or your visitors will receive a Certificate Not Trusted Error. You can install each Intermediate certificate (sometimes there is more than one) using these instructions:

Step 1. Download the intermediate certificate to a folder on the server.

Step 2. Double click the certificate to open the certificate details.

Step 3. At the bottom of the General tab, click the Install Certificate button to start the certificate import wizard. Click Next.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

•Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

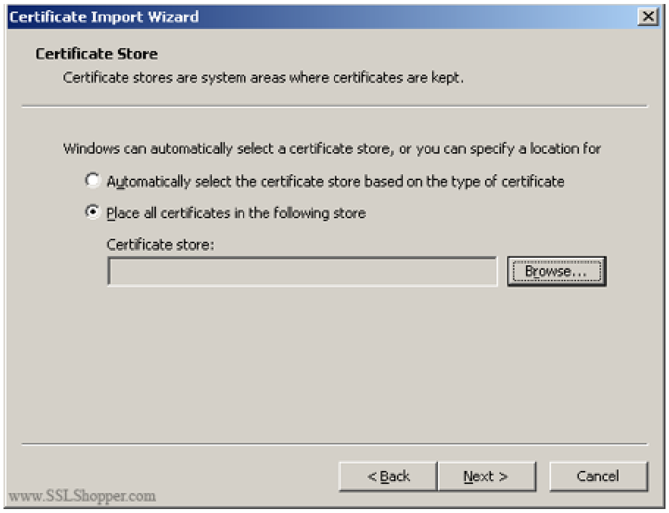
Issued to: Go Daddy Secure Certification Authority

Issued by: Go Daddy Class 2 Certification Authority

Valid from 11/15/2006 to 11/15/2026

Certificate

Step 4. Select Place all certificates in the following store and click Browse.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

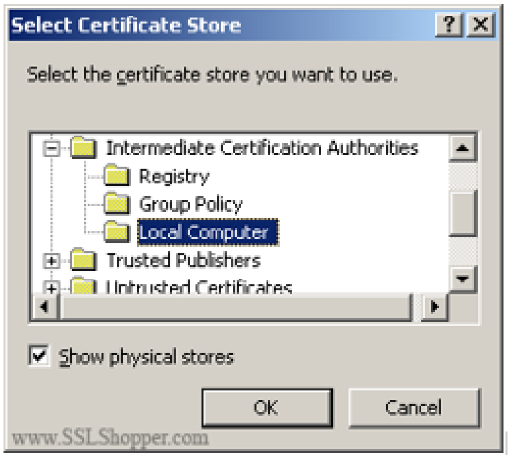
● Place all certificates in the following store

Certificate store:

Certificate Import Wizard

Step 5. Check the Show physical stores checkbox, then expand the Intermediate Certification Authorities folder, select the Local Computer folder beneath it. Click OK.

Step 6. Click Next, then Finish to finish installing the intermediate certificate.



Select Certificate Store

Select the certificate store you want to use.

☑ Show physical stores

Changing Default Port 443 for the MAXPRO Web Client and MAXPRO Mobile app

Changing the default Port 443 for the MAXPRO Web Client and MAXPRO Mobile app is a two step process:

- Changing the port 443 on the MAXPRO NVR.
- Changing the port in the MAXPRO Mobile app and MAXPRO Web Client.

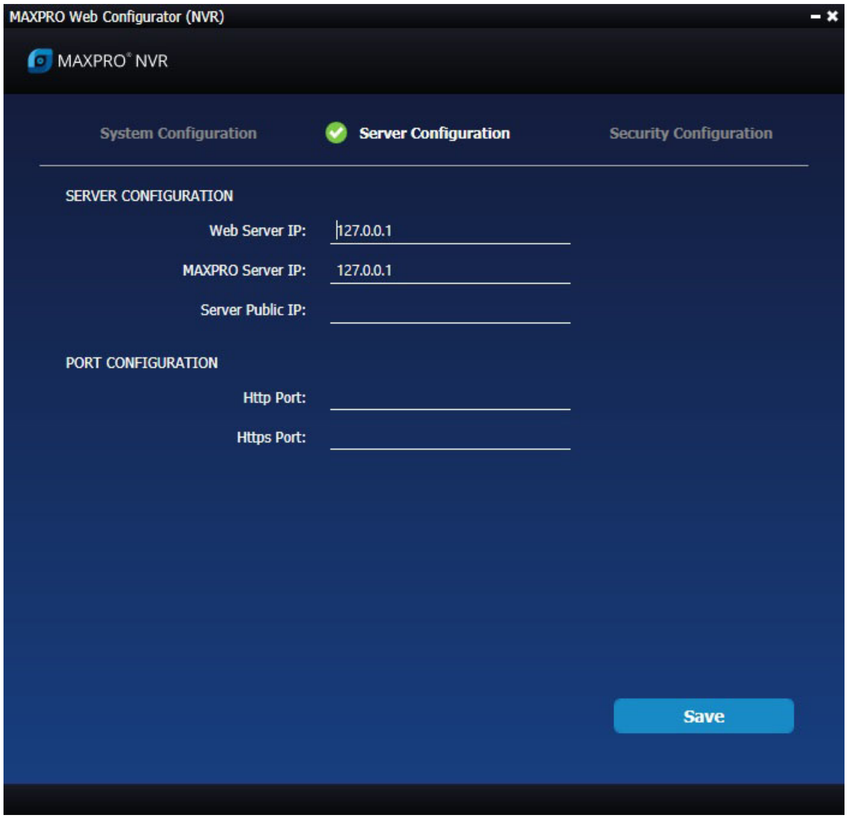
Note: *MAXPRO NVR Web Client and MAXPRO Mobile app share a common port. Different ports cannot be assigned to the Web Client and Mobile app.*

Step 1: Changing the Default Port 443 on the MAXPRO NVR

By default, Port 443 is configured for the MAXPRO Web Client and MAXPRO Mobile app to connect to the NVR. If you need to modify the default port, perform the following procedure. If you require further assistance, please contact your Network Administrator.

Step 1. Double-click on the desktop. The MAXPRO Web Configurator dialog box appears. By default the System Configuration tab is selected.

Step 2. Click the Server Configuration tab the following screen appears.



SERVER CONFIGURATION

Web Server IP: 127.0.0.1

MAXPRO Server IP: 127.0.0.1

Server Public IP:

PORT CONFIGURATION

Http Port:

Https Port:

Server Configuration

Step 3. Under Port Configuration:

- Http Port: If you want to change the http default port 80 to some other port number then type the required port number and click Apply.
- Https Port: If you want to change the https default port 443 to some other port number then type the required port number and click Apply.

Note: *Port change option in the configurator tool is available from 3.1 Build 65 Rev C or higher version.*

Step 2: Changing the Port in the MAXPRO Web Client and MAXPRO Mobile app

Step 1. Launch MAXPRO Mobile by tapping on your mobile device.

Step 2. Before you log on: Tap + in the right hand side to add NVR

Step 3. Add the MAXPRO NVR Server:

- Select whether you want to connect through Remote network or Local network
- In the name field, enter the name (For example Demo/Site name) for the NVR.
- In the IP Address field, type the IP address/Host Name of the unit
- Type the Port number. The default port number is 443.
- Tap Add.

To change the port in MAXPRO NVR Web Client:

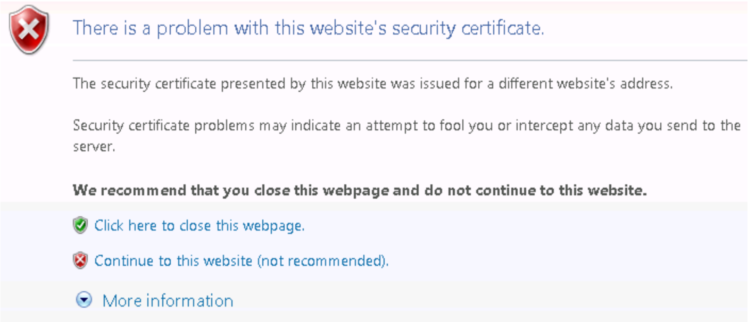
- Type the URL https://<MAXPRO NVR Server IP or Computer/Machine name>:<PORT>/MAXPROWEB/ in your web browser and then press Enter. The log In page appears.

Note: *<MAXPRO NVR Server IP or Computer/Machine name> needs to be replaced by the IP address or Computer/Machine name (as applicable) of the MAXPRO NVR Server machine on which both the Web Server and the NVR Server are installed by default. <PORT> needs to be replaced by the new port. For example: if the port is changed to 1024 with the steps above, enter the URL as https://74.x.x.x:1024/MAXPROWEB/*

Caution: For better security, close the browser upon logout.

Viewing the Certificate Information

If you see the below security message then it may not be from the valid certificate authority and it would be the case of self signed. It is recommended to exercise caution and verify the certificate and check whether the certificate details are matching with the server machine.



There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

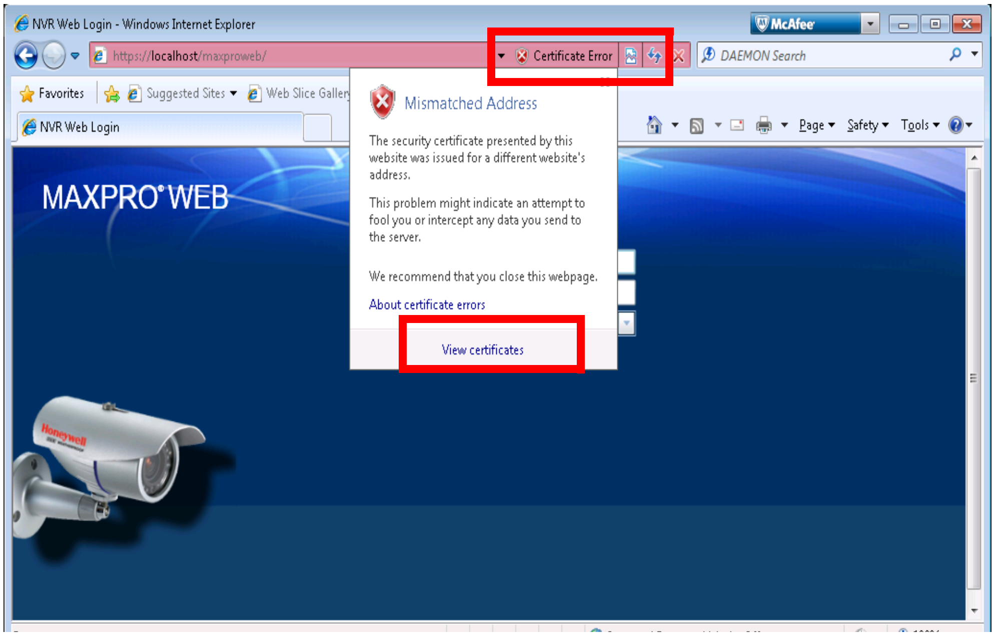
Continue to this website (not recommended).

More information

To verify the certificate details:

Step 1. Click Continue to this web site (not recommended) link to proceed. The NVR Web Login page is displayed.

Step 2. Click Certificate Error as shown below. The Mismatch Address pop up message is displayed.



Mismatched Address

The security certificate presented by this website was issued for a different website's address.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

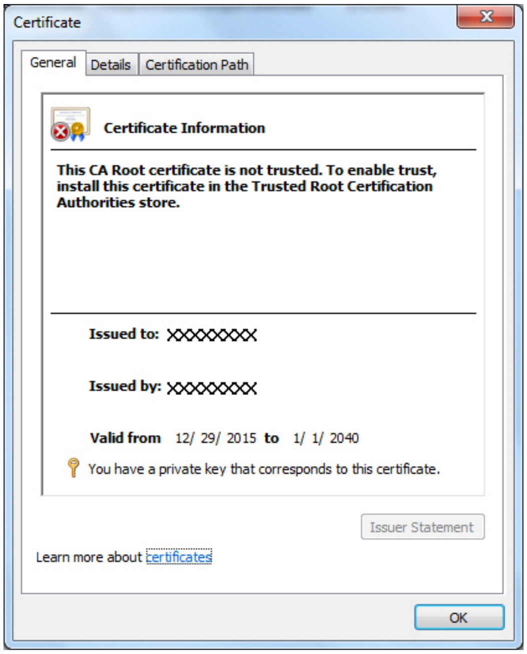
We recommend that you close this webpage.

About certificate errors

View certificates

Program Maintenance

Step 3. Click View Certificate. The Certificate dialog box is displayed.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: XXXXXXXX

Issued by: XXXXXXXX

Valid from 12/ 29/ 2015 **to** 1/ 1/ 2040

You have a private key that corresponds to this certificate.

Learn more about certificates

Certificate dialog

Step 4. Verify the following fields to check whether it is matching with the details of Server machine.

- Issued to

- Issued By
- Valid From

Step 5. Click the Details tab and then check other details.

⚠ **Caution: For better security, close the browser upon logout.**

CHAPTER

10 MAXPRO NVR MOBILE APP

Introduction

This chapter describes how to connect to a MAXPRO® NVR using the MAXPRO®NVR Mobile app on an Apple® or Android™ mobile devices. It also covers how to install the app and creating the users for the MAXPRO NVR Mobile app.

With MAXPRO NVR Mobile App, you can perform every day video surveillance tasks such as:

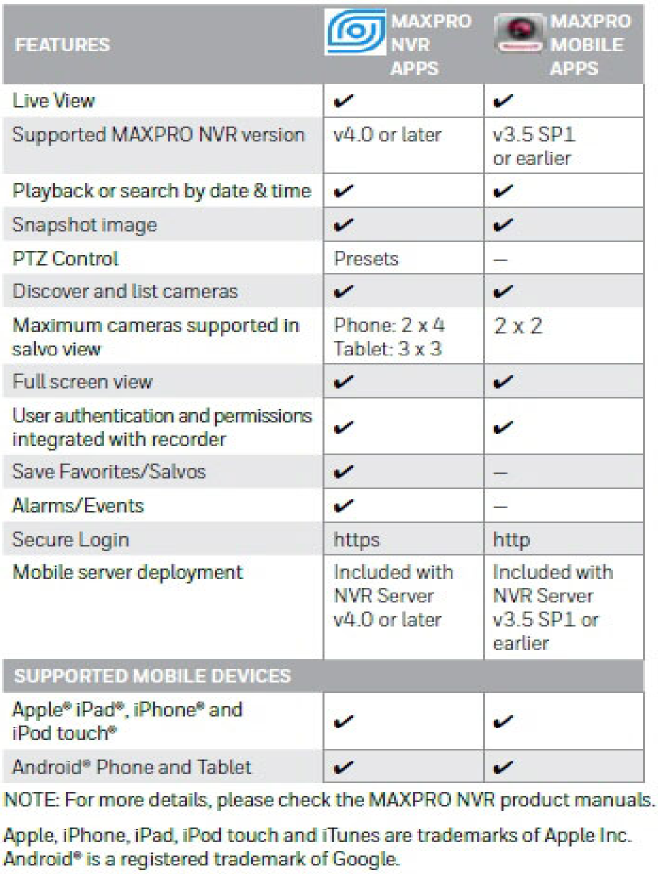
- Configure and Logon using Touch ID (For Fingerprint recognition supported mobile device only). Fingerprint Authentication login is supported for both Android and IOS devices.
- HIS Streaming support where you can view live video if you have not installed valid/trusted certificate.
- One time configuration for both Local and Remote connection.
- Live video view to monitor your house, facility, customers or employees.
- Digital zoom in and zoom out for full screen view in landscape or portrait.
- Playback or search for recorded video by date and time.
- Take a snapshot of a live or recorded video frame and use as an image.
- Create favorite salvos (cameras up to 3x3 on tablets and 2x4 on phones per salvo).
- Perform PTZ control through Presets.
- Monitor & Manage Alarms.
- Search for MAXPRO NVR and download the FREE app at the Apple® iTunes® App Store or Google Play. For NVR 3.5 SP1 or older version search for: MAXPRO Mobile.

Enhancements in NVR 5.0 Release

- Support for New Mobile app versions
- For Android: 1.3.0 (100030004)

- For IOS: 1.3.0 (100030001)
- New Supported OS: minSDKVersion = 21

The following table explains the features available in MAXPRO NVR Apps and MAXPRO Mobile Apps:



FEATURES	MAXPRO NVR APPS	MAXPRO MOBILE APPS
Live View	✔	✔
Supported MAXPRO NVR version	v4.0 or later	v3.5 SP1 or earlier
Playback or search by date & time	✔	✔
Snapshot image	✔	✔
PTZ Control	Presets	–
Discover and list cameras	✔	✔
Maximum cameras supported in salvo view	Phone: 2 x 4 Tablet: 3 x 3	2 x 2
Full screen view	✔	✔
User authentication and permissions integrated with recorder	✔	✔
Save Favorites/Salvos	✔	–
Alarms/Events	✔	–
Secure Login	https	http
Mobile server deployment	Included with NVR Server v4.0 or later	Included with NVR Server v3.5 SP1 or earlier
SUPPORTED MOBILE DEVICES		
Apple® iPad®, iPhone® and iPod touch®	✔	✔
Android® Phone and Tablet	✔	✔

NOTE: For more details, please check the MAXPRO NVR product manuals.

Apple, iPhone, iPad, iPod touch and iTunes are trademarks of Apple Inc.
Android® is a registered trademark of Google.

MAXPRO NVR Mobile app Installation

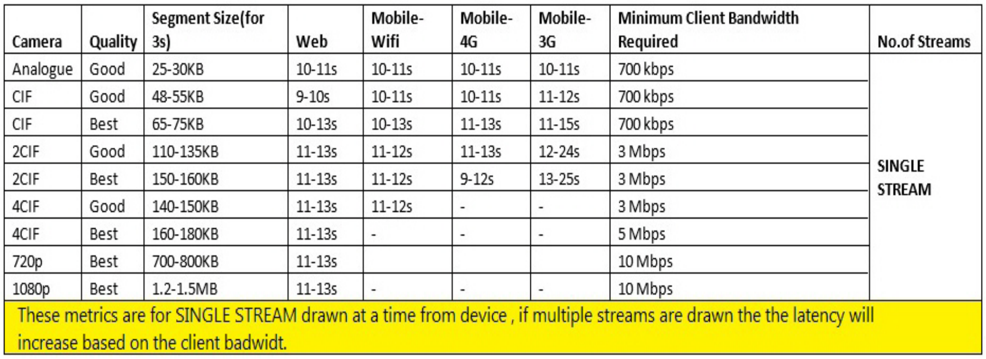
The MAXPRO NVR Mobile app is compatible with MAXPRO NVR v4.0 or later versions.

Minimum Requirements

The MAXPRO NVR Mobile app minimum requirements are:

- Apple iPad, iPhone, and iPod touch running IOS 8 and later
- Android phones and tablets running v4.4 and later
- Internet connection to the MAXPRO NVR
- Wifi or 3G/4G connection for the Apple or Android device

The following table depicts the minimum bandwidth required for MAXPRO NVR mobile app to function normally:

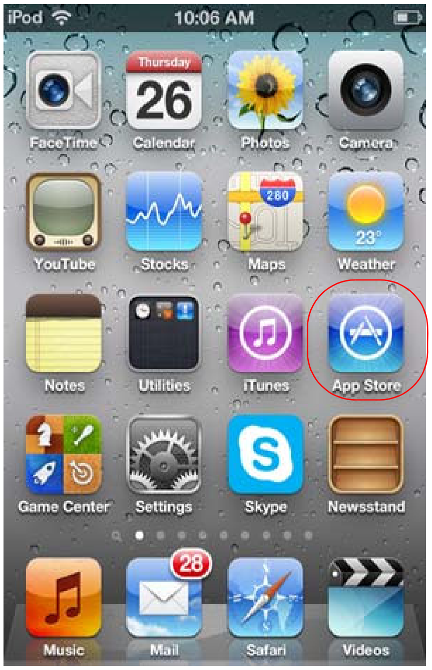
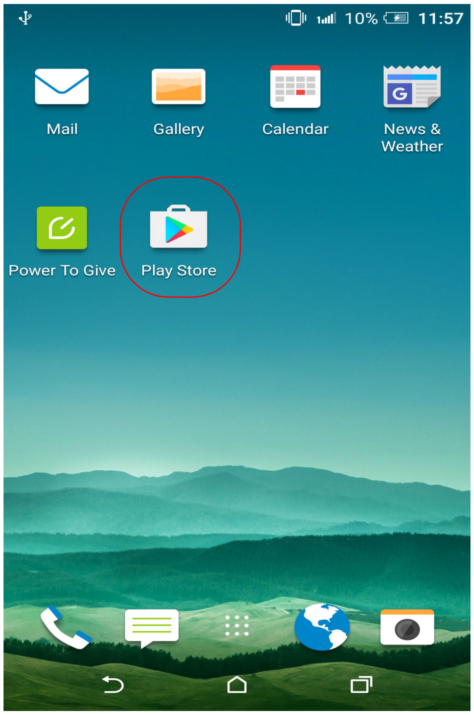


Camera	Quality	Segment Size(for 3s)	Web	Mobile-Wifi	Mobile-4G	Mobile-3G	Minimum Client Bandwidth Required	No.of Streams
Analogue	Good	25-30KB	10-11s	10-11s	10-11s	10-11s	700 kbps	SINGLE STREAM
CIF	Good	48-55KB	9-10s	10-11s	10-11s	11-12s	700 kbps	
CIF	Best	65-75KB	10-13s	10-13s	11-13s	11-15s	700 kbps	
2CIF	Good	110-135KB	11-13s	11-12s	11-13s	12-24s	3 Mbps	
2CIF	Best	150-160KB	11-13s	11-12s	9-12s	13-25s	3 Mbps	
4CIF	Good	140-150KB	11-13s	11-12s	-	-	3 Mbps	
4CIF	Best	160-180KB	11-13s	-	-	-	5 Mbps	
720p	Best	700-800KB	11-13s				10 Mbps	
1080p	Best	1.2-1.5MB	11-13s	-	-	-	10 Mbps	

These metrics are for SINGLE STREAM drawn at a time from device , if multiple streams are drawn the the latency will increase based on the client badwidt.

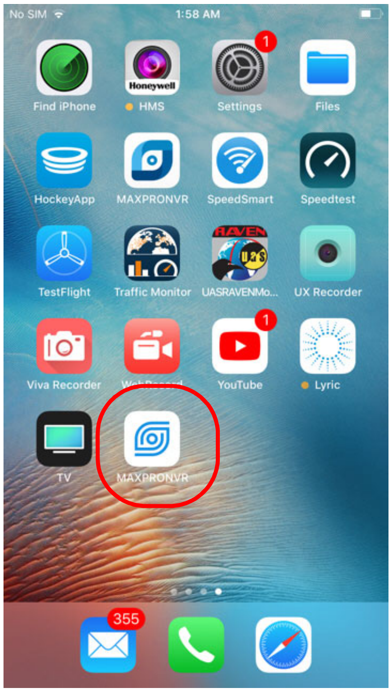
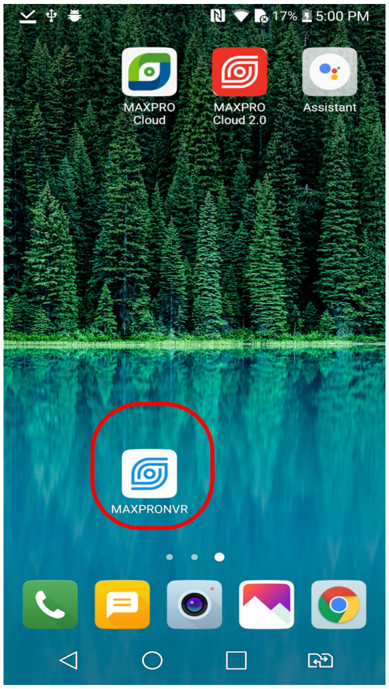
Installing the MAXPRO NVR Mobile app

Step 1. Download the app by searching for MAXPRO NVR Mobile from the appropriate mobile app store, either the Apple App Store or the Google Play Store (https://play.google.com/).

Apple mobile device	Android mobile device
	

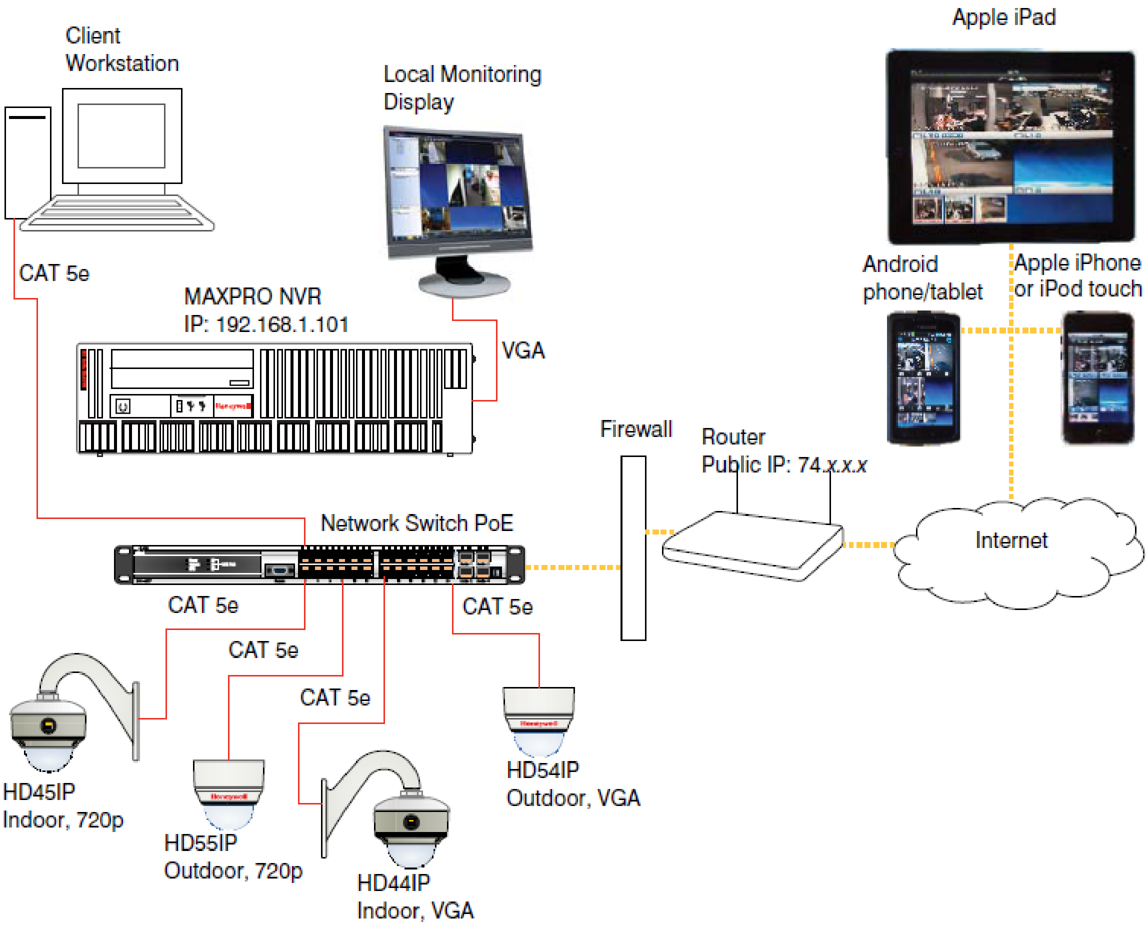
Step 2. When the application is successfully installed, the Honeywell MAXPRO

Mobile icon appears on the device.

Apple mobile device	Android mobile device
	

Typical Network Configuration and Settings

The System Diagram figure shows a typical system setup. In applications where the mobile device connects to the MAXPRO NVR through a public router, you must configure port forwarding on the router as shown in the port forwarding table. Please contact your Network Administrator for assistance.



System Diagram

Up to three mobile devices can be used simultaneously to view video from the NVR.

Note:

- The default ports for the Mobile app on MAXPRO NVR is 80 and 443. See the ***Changing Default Port 443 for the MAXPRO Web Client and MAXPRO Mobile app*** section on page ***366*** for instructions on how to change the port number if Port 80, 443 is already used or if there is more than one MAXPRO NVR behind the router in the network.
- Video to the Mobile app is always transmitted over HTTP and Non-video data is always transmitted over HTTPS.
- Please ensure ports required for both video and non-video data are considered in any port forwarding settings required.

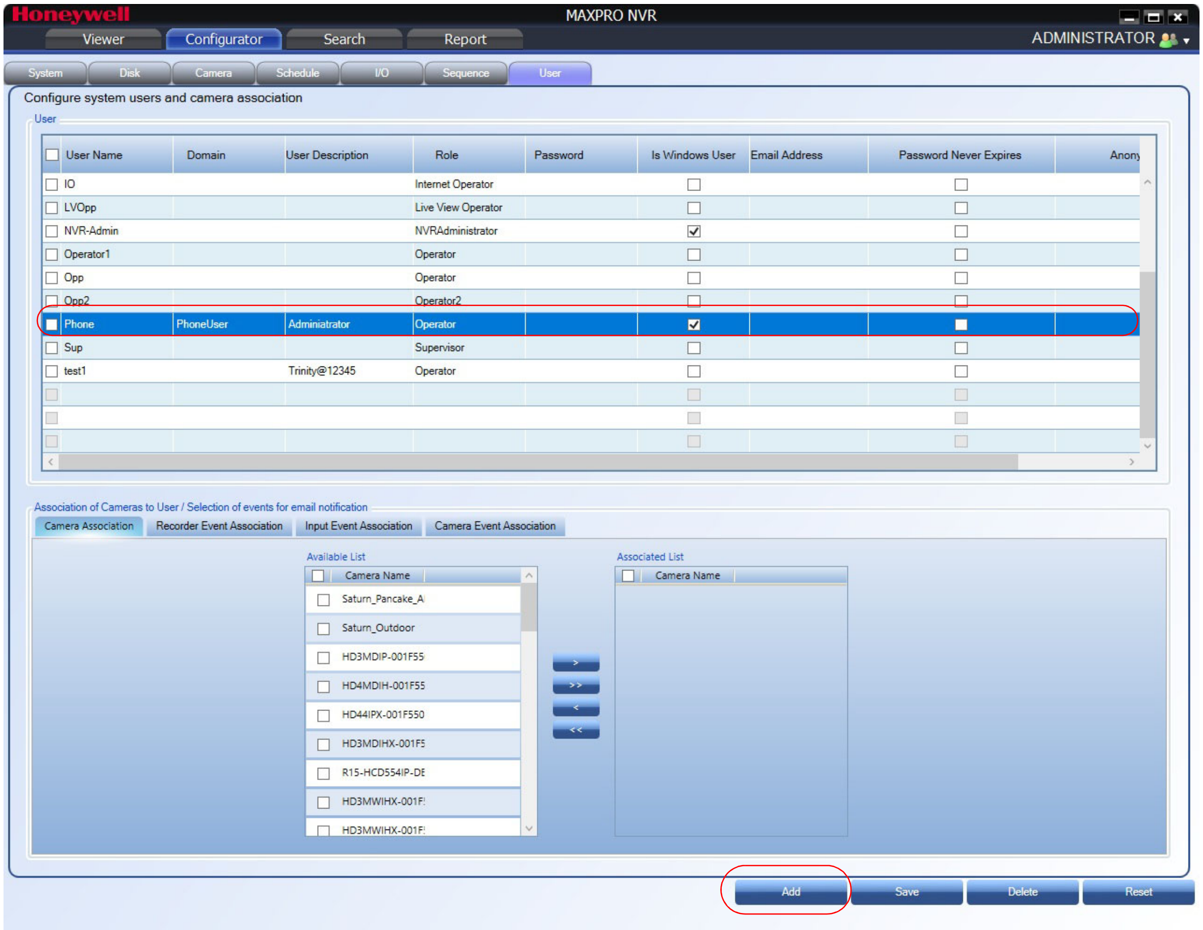
Public Router IP Address	External Port	MAXPRO NVR IP Address	Internal Port
74.xxx	80	192.168.1.101	80
74.xxx	443	192.168.1.101	443

Creating Users for the MAXPRO NVR Mobile app

The MAXPRO NVR Mobile app uses a non-Windows authentication. You need to create non-Windows users in NVR to allow access from authorized mobile device users.

Step 1. Launch MAXPRO NVR (double-click the MAXPRO NVR icon on your desktop).

Step 2. On the Configurator tab, select the User tab, then click Add at the bottom.



Configure system users and camera association

User

□	User Name	Domain	User Description	Role	Password	Is Windows User	Email Address	Password Never Expires	Anony
□	IO			Internet Operator		□		□	
□	LVOpp			Live View Operator		□		□	
□	NVR-Admin			NVRAdministrator		☑		□	
□	Operator1			Operator		□		□	
□	Opp			Operator		□		□	
□	Opp2			Operator2		□		□	
□	Phone	PhoneUser	Adminiatrator	Operator		☑		□	
□	Sup			Supervisor		□		□	
□	test1		Trinity@12345	Operator		□		□	
□						□		□	
□						□		□	
□						□		□	

Available List

□	Camera Name
□	Saturn_Pancake_A
□	Saturn_Outdoor
□	HD3MDIP-001F55
□	HD4MDIH-001F55
□	HD44IPX-001F550
□	HD3MDIHX-001F5
□	R15-HCD554IP-DE
□	HD3MWIHX-001F
□	HD3MWIHX-001F

Associated List

□	Camera Name

- Double-click User in the User Name column. Type in a name for the MAXPRO Mobile user. This is the name that will be used to log on to the mobile device to connect to the MAXPRO NVR.
- (Optional) Double-click in the User Description column to add an appropriate description (for example, Mobile app operator).
- In the Role drop-down list, select the appropriate user permission (for example, Operator, as shown above).
- Select the Password Never Expire check box if you do not want to change the password periodically.

- Select Anonymization Check box to use the Privacy Protection feature (GDPR Favored). See Privacy Protection Settings section for more information.

Limitation with Privacy Protection Settings

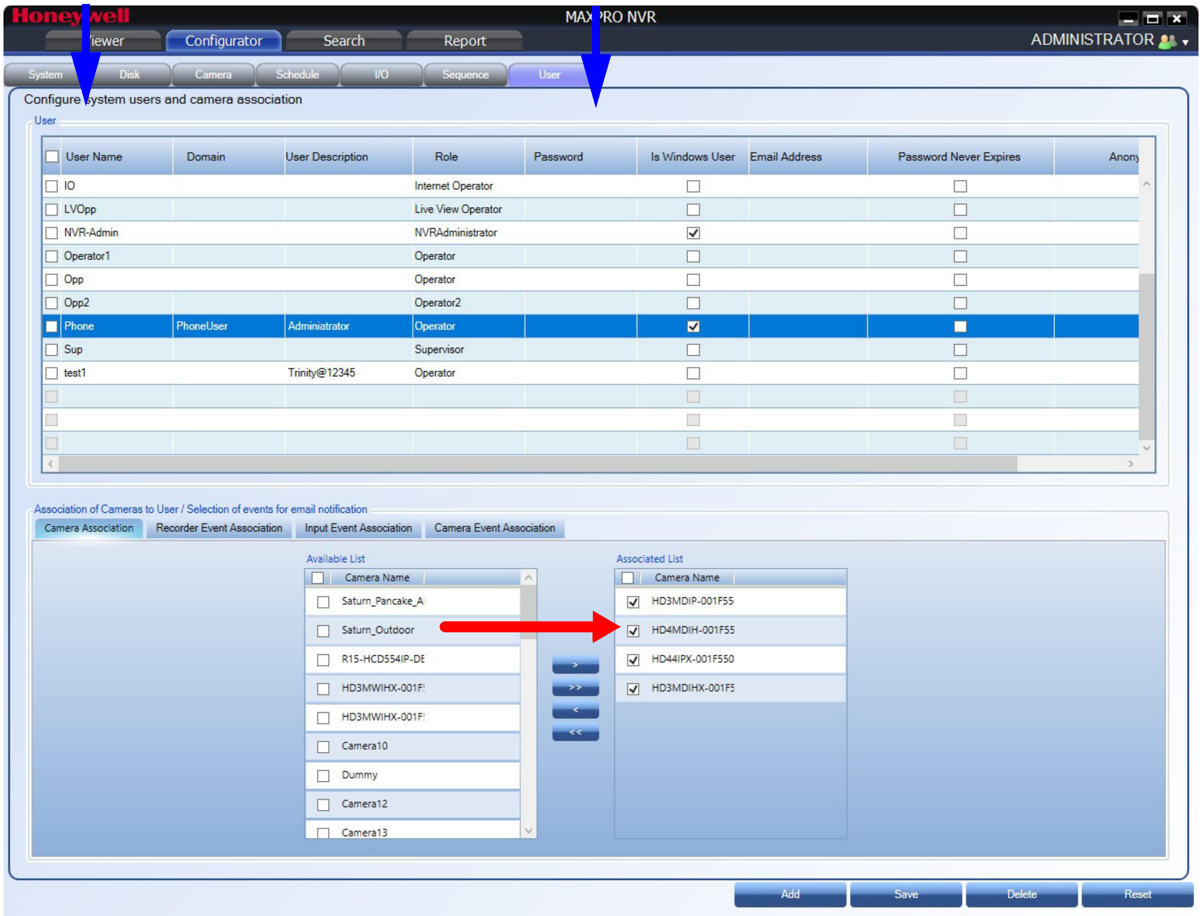
- If Anonymization is enabled in NVR application, then user will not be able to see the video in MAXPRO mobile app/Web client. An error message is displayed.
- Anonymization is not supported in Web. If user is tries to see Anonymized video and also camera Anonymized option is enabled then an error message "Trying to access Anonymized Stream" is displayed.
- If Four Eye Authentication option is enabled in NVR application then user will not be able to view playback video in MAXPRO mobile app/Web client
- When an Operator (non-admin) logs into the Web Client and tries to view playback for any video then an error message "Four Eye authentication Privilege Failure" is displayed.

Selecting the Cameras to be Remotely Viewed

Step 1. Provide access for the MAXPRO Mobile user to selected cameras, as required.

- Select the required cameras in the Available List, then click the right arrow to move them to the Associated List.

- Click Save.



Configure system users and camera association

User

☐	User Name	Domain	User Description	Role	Password	Is Windows User	Email Address	Password Never Expires	Anony
☐	IO			Internet Operator		☐		☐	
☐	LVOpp			Live View Operator		☐		☐	
☐	NVR-Admin			NVRAdministrator		☑		☐	
☐	Operator1			Operator		☐		☐	
☐	Opp			Operator		☐		☐	
☐	Opp2			Operator2		☐		☐	
☐	Phone	PhoneUser	Adminiatrator	Operator		☑		☐	
☐	Sup			Supervisor		☐		☐	
☐	test1		Trinity@12345	Operator		☐		☐	

Association of Cameras to User / Selection of events for email notification

Available List

☐	Camera Name
☐	Saturn_Pancake_A
☐	Saturn_Outdoor
☐	R15-HCD554IP-DE
☐	HD3MWIHX-001F
☐	HD3MWIHX-001F
☐	Camera10
☐	Dummy
☐	Camera12
☐	Camera13

Associated List

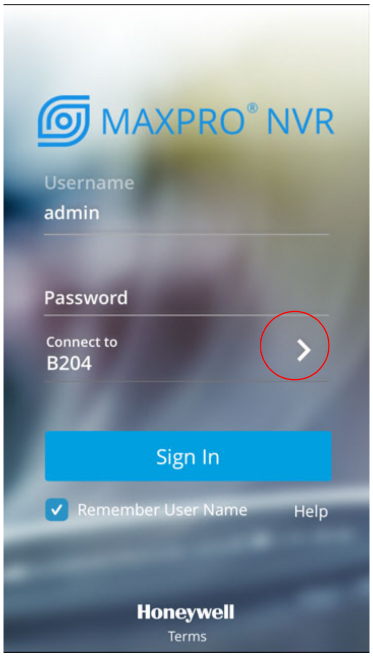
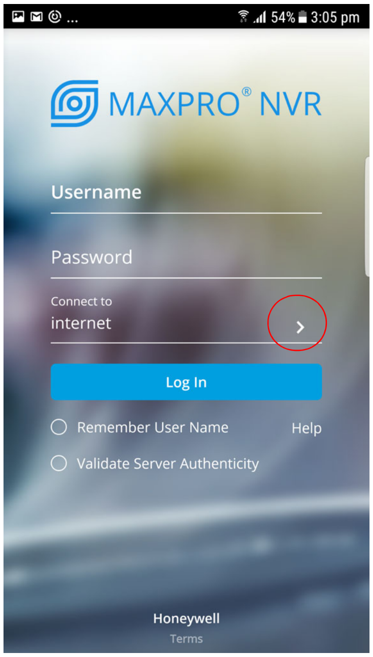
☐	Camera Name
☑	HD3MDIP-001F55
☑	HD4MDIH-001F55
☑	HD44IPX-001F550
☑	HD3MDIHX-001F5

Adding the MAXPRO NVR to the MAXPRO NVR Mobile app

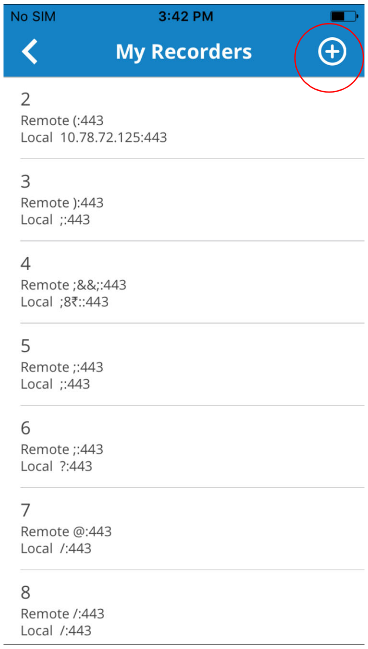
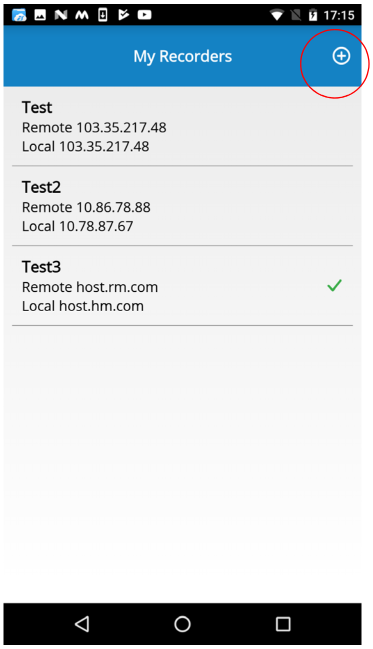
In the MAXPRO NVR Mobile app, you must add the MAXPRO NVR so that you can view video.

Step 1. Launch MAXPRO NVR Mobile by tapping MAXPRONVR on your mobile device.

Step 2. Before you log on: Tap > in the right hand side to view the available NVRs or to add new NVR.

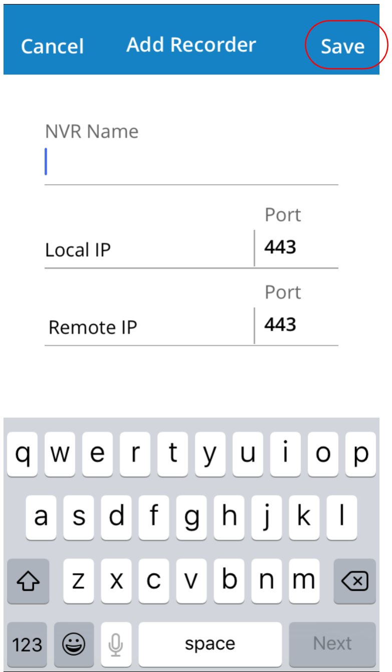
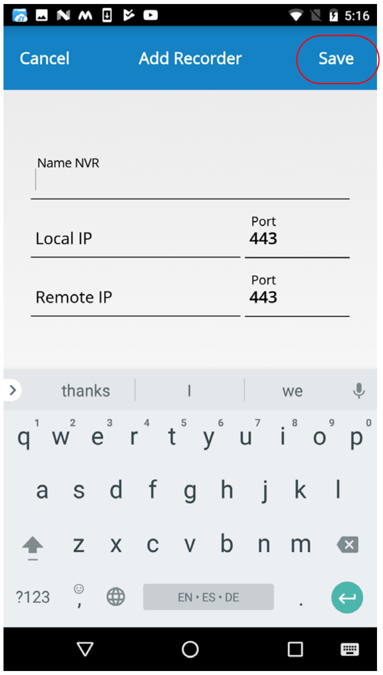
Apple mobile device	Android mobile device
 MAXPRO® NVR Username admin Password Connect to B204 Sign In ☑ Remember User Name Help Honeywell Terms	 54% 3:05 pm MAXPRO® NVR Username Password Connect to internet Log In ○ Remember User Name Help ○ Validate Server Authenticity Honeywell Terms

In the Add Recorder screen:

Apple mobile device	Android mobile device
Tap ⊕ to add a new NVR Recorder.  No SIM 3:42 PM My Recorders 2 Remote (:443 Local 10.78.72.125:443 3 Remote):443 Local ;:443 4 Remote ;&&;:443 Local ;8₹::443 5 Remote ;:443 Local ;:443 6 Remote ;:443 Local ?:443 7 Remote @:443 Local /:443 8 Remote /:443 Local /:443	Tap ⊕ to add a new NVR Recorder  17:15 My Recorders Test Remote 103.35.217.48 Local 103.35.217.48 Test2 Remote 10.86.78.88 Local 10.78.87.67 Test3 ✓ Remote host.rm.com Local host.hm.com

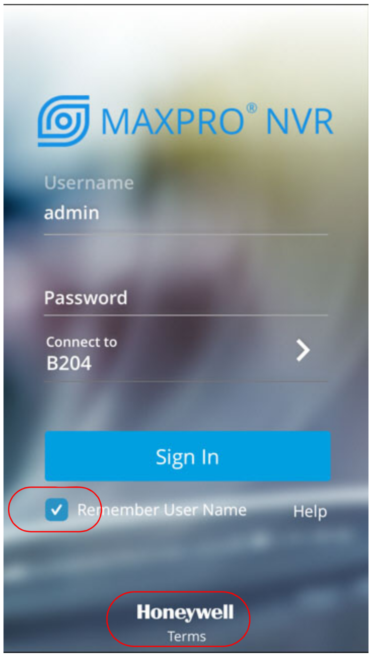
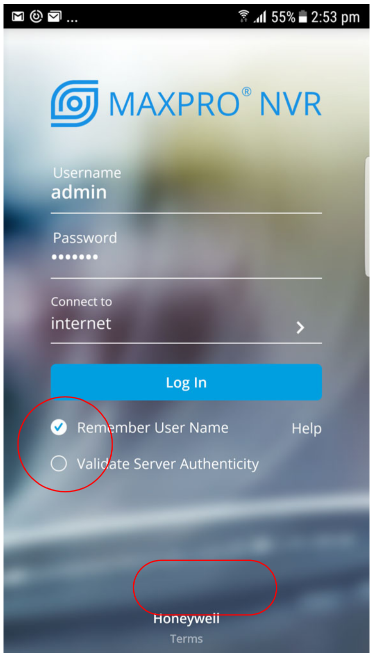
- In the NVR Name field, type the name (For example Demo/Site name) for the NVR.
- In the Local IP field, type the local IP address/Host name of the unit.
- In the Remote IP field, type the remote IP address/Host name of the unit.

- Type the Port number. The default port number is 443.

Apple mobile device	Android mobile device
Tap Save to complete adding NVR Recorder.  NVR Name Local IP Port 443 Remote IP Port 443	Tap Save to complete adding NVR Recorder.  Name NVR Local IP Port 443 Remote IP Port 443

Step 3. Log on: You can Log on in two ways, Manual and Finger Print Touch ID. (Finger Print Touch ID logon is supported only for IOS devices).

- For Manual Logon:
- In the Username field enter the name that was created for the mobile device user in MAXPRO NVR (see the ***Creating Users for the MAXPRO NVR Mobile app*** section on page ***377***).
- In the Password field enter the appropriate password.
- Under Connect to, ensure that your Recorder is selected or tap > to connect to a different recorder.
- Select the Remember User Name check box If you want the app to remember the User Name for your future login.
- (Only for Android Devices): Select the Validate Server Authenticity check box If you want to validate the server.
- Tap on Terms at the bottom of the screen to read the EULA terms and conditions.

Apple mobile device	Android mobile device
Tap **Sign In.**	Tap **Log In**.
 MAXPRO® NVR Username admin Password Connect to B204 Sign In ☑ Remember User Name Help Honeywell Terms	 55% 2:53 pm MAXPRO® NVR Username admin Password ••••••• Connect to internet Log In ✓ Remember User Name Help ○ Validate Server Authenticity Honeywell Terms

- For Touch ID logon, see ***Logon using Touch ID (Fingerprint Authenticated)*** for more information.

Logon using Touch ID (Fingerprint Authenticated)

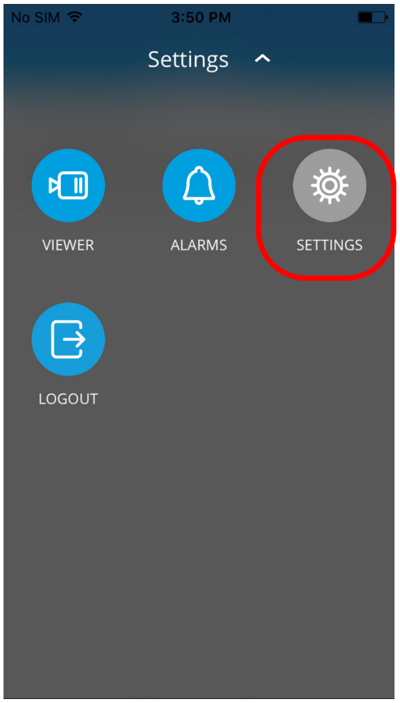
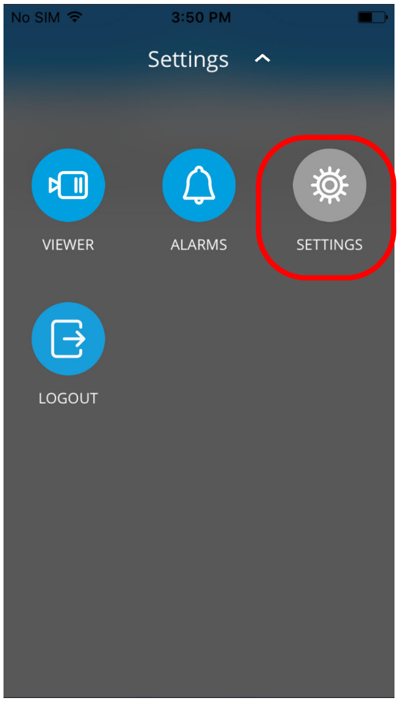
Touch ID logon (For Fingerprint recognition supported mobile device only): This feature is supported for fingerprint secured Android and IOS mobile devices. Maximum of 5 users fingerprints can be configured per mobile device. The first login should be manual login and you need to enter the credentials manually. After that, the succeeding logins can be based on fingerprint authentication. The Fingerprint authentication logon option is displayed after the first manual logon. You can see the fingerprint icon on the bottom left corner of the login screen. Touch ID logon feature is supported for both Android and IOS devices.To use the Touch ID logon facility user needs to verify the Touch ID

Verifying the Touch ID

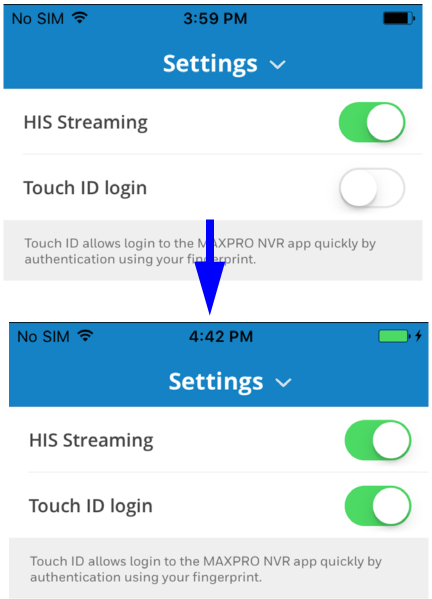
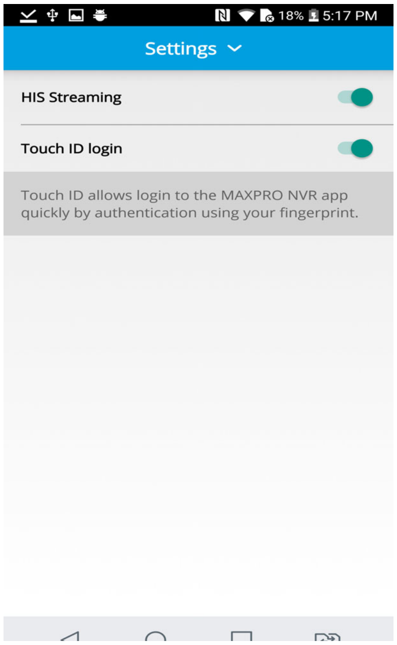
Pre-requisite:

To verify the Touch ID configuration, it is assumed that the user should have configured the Fingerprint authentication under Settings to unlock the mobile. Refer corresponding Mobile (IOS) user manuals to set the Fingerprint based authentication to unlock.

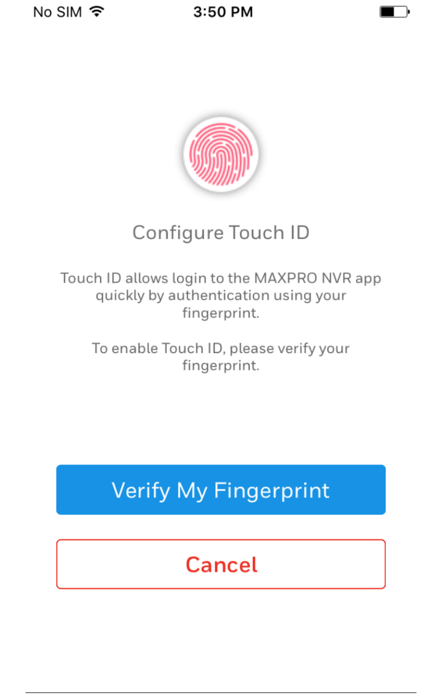
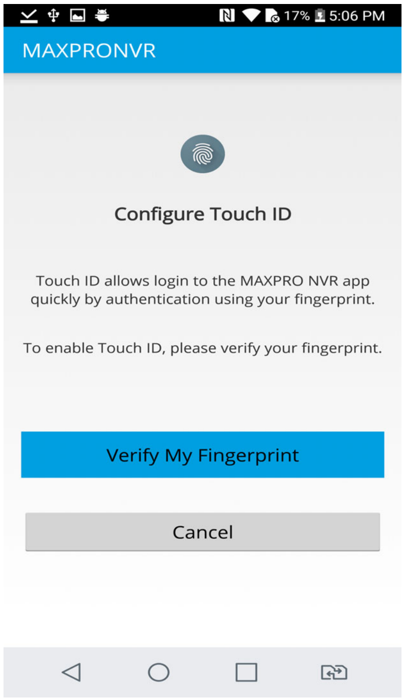
Step 1. Manually logon to the MAXPRO app and then navigate to Settings screen as shown below.

Apple mobile device	Android mobile device
Tap Settings.	
 No SIM 3:50 PM Settings VIEWER ALARMS SETTINGS LOGOUT	 No SIM 3:50 PM Settings VIEWER ALARMS SETTINGS LOGOUT

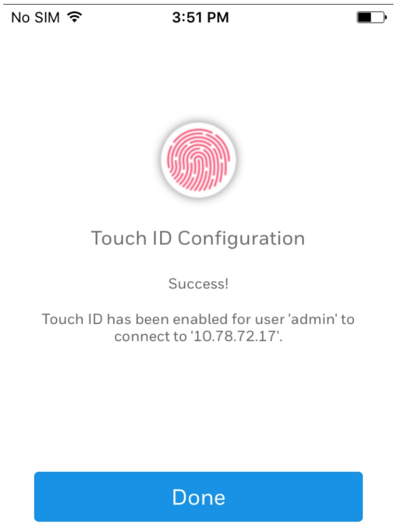
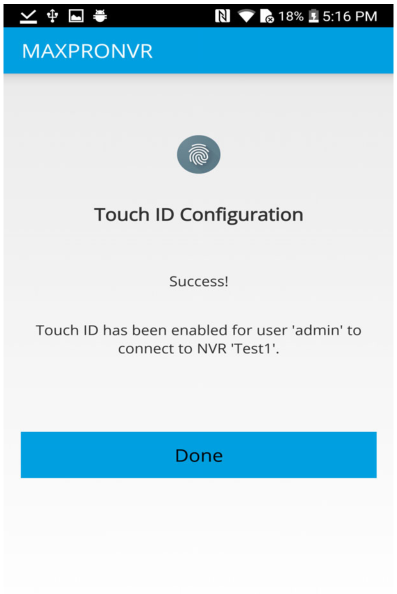
Step 2. Tap the toggle button to turn on the Touch ID Login as shown below.

Apple mobile device	Android mobile device
 No SIM 3:59 PM Settings HIS Streaming Touch ID login Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint. No SIM 4:42 PM Settings HIS Streaming Touch ID login Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint.	 18% 5:17 PM Settings HIS Streaming Touch ID login Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint.

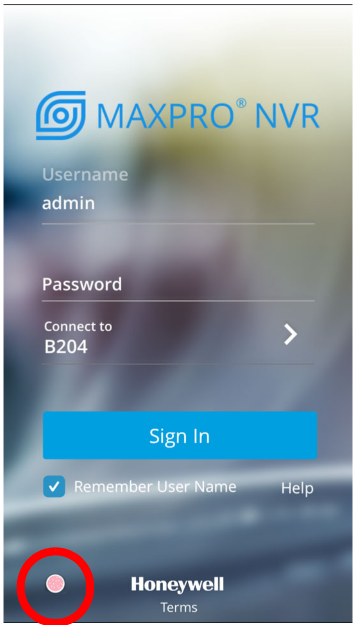
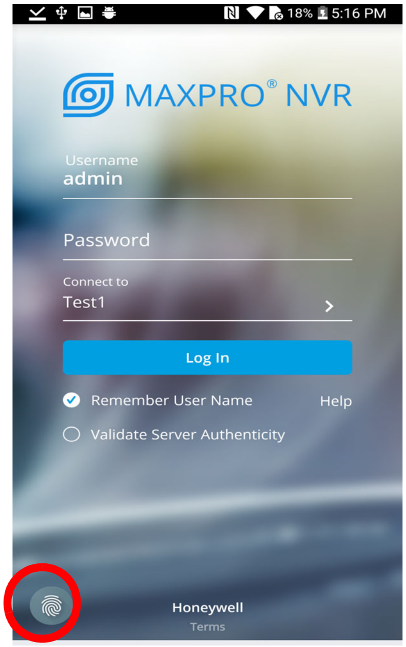
Step 3. Once the Touch ID login is ON, the Configure Touch ID screen is displayed as shown below.

Apple mobile device	Android mobile device
Tap Verify My Fingerprint to start verifying the fingerprint.  Configure Touch ID Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint. To enable Touch ID, please verify your fingerprint.	Tap Verify My Fingerprint to start verifying the fingerprint.  Configure Touch ID Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint. To enable Touch ID, please verify your fingerprint.

Step 4. Follow the instructions on the screen during the verification process. You need to touch and hold the Home button multiple times to verify the fingerprint. If the verification is successful then the Success message is displayed as shown.

Apple mobile device	Android mobile device
Tap Done to complete.  No SIM 3:51 PM Touch ID Configuration Success! Touch ID has been enabled for user 'admin' to connect to '10.78.72.17'. 	Tap Done to complete.  18% 5:16 PM MAXPRONVR Touch ID Configuration Success! Touch ID has been enabled for user 'admin' to connect to NVR 'Test1'.

Step 5. Tap Done to complete the configuration. Fingerprint authentication option is now displayed as highlighted below.

Apple mobile device	Android mobile device
 MAXPRO® NVR Username admin Password Connect to B204 ☑ Remember User Name Help Honeywell Terms	 18% 5:16 PM MAXPRO® NVR Username admin Password Connect to Test1 ☑ Remember User Name Help ○ Validate Server Authenticity Honeywell Terms

Step 6. Place your finger on the Fingerprint icon as highlighted above. You will be logged in to MAXPRO app.

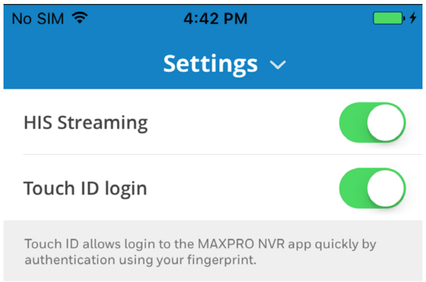
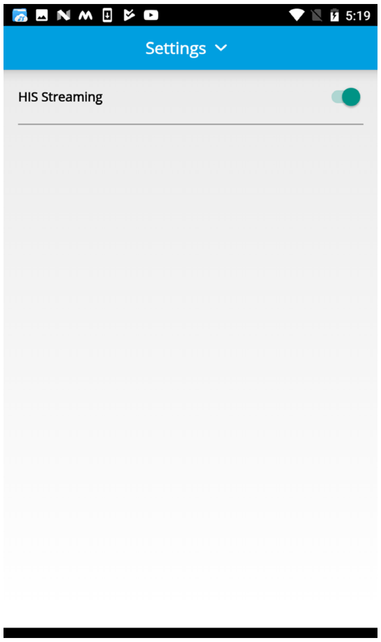
Note: *Ensure that the first logon should be Manual logon.*

Enable HIS Streaming

HIS Streaming feature allows you to view the live video even if you dont have valid certificate installed on the server for secure connection. You can still view the live video frame by frame to ensure you are surveillance process is smooth and continuous. By default HIS Streaming feature is enabled in the app. This feature detects your trusted certificate status automatically and intimates if you are viewing live video through HIS Streaming. You can use HIS streaming in the following scenarios:

- if you have not installed valid/trusted certificate on the Server.
- if your trusted certificate is expired.

By default HIS Streaming is enabled in Settings screen as shown below.

Apple mobile device	Android mobile device
 No SIM 4:42 PM Settings HIS Streaming Touch ID login Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint.	 5:19 Settings HIS Streaming

Adding Multiple NVR Recorders

To add additional NVR on the mobile app:

Note: *Maximum 20 NVR configurations are allowed.*

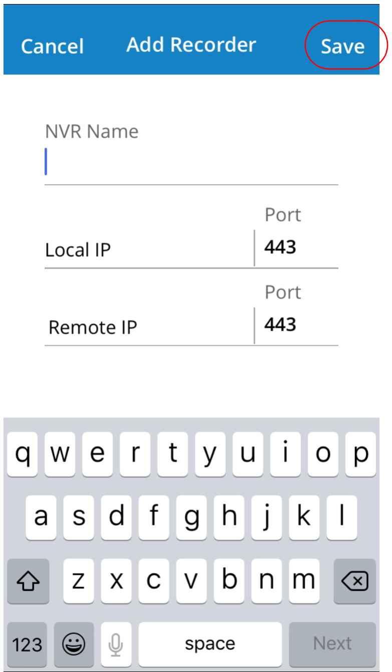
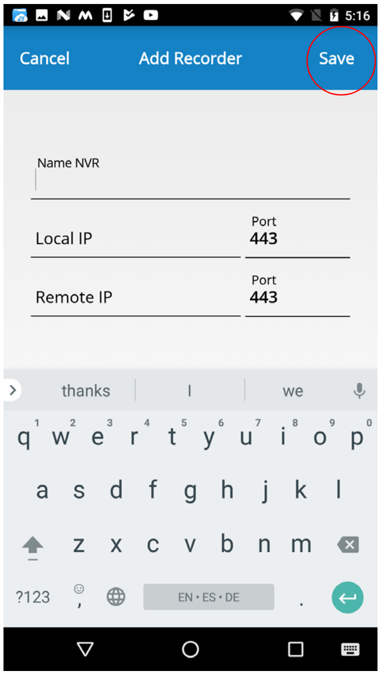
Step 1. Tap > on the login screen. The list of already saved NVRs under My Recorders screen is displayed.

Step 2. Tap ⊕. The Add Recorder screen is displayed.

Step 3. Add the MAXPRO NVR Recorder as follows:

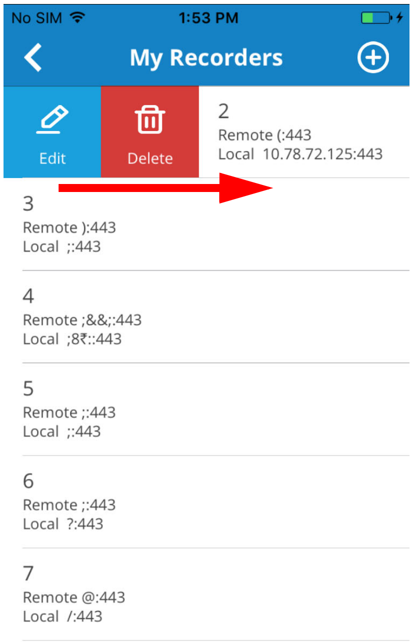
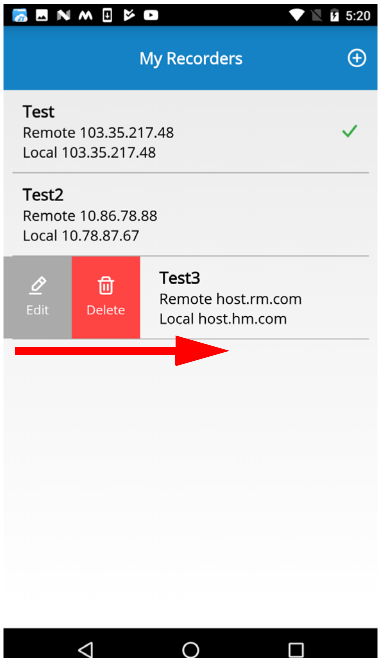
- In the NVR Name field, type the name (For example Demo/Site name) for the NVR.
- In the Local IP field, type the local IP address/Host name of the unit.
- In the Remote IP field, type the remote IP address/Host name of the unit.
- Type the Port number. The default port number is 443.

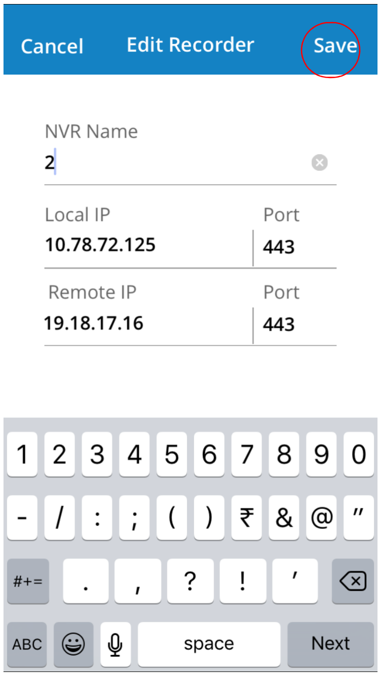
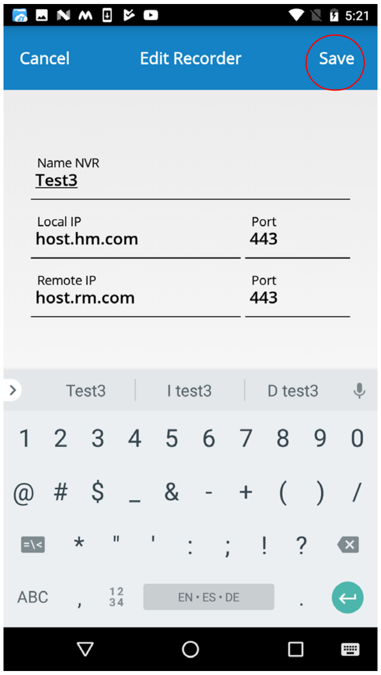
Step 4. Repeat the step 1 through step 3 to add multiple NVR Recorders.

Apple mobile device	**Android mobile device**
Tap Save to complete adding NVR Recorder.  NVR Name Local IP — Port 443 Remote IP — Port 443	Tap Save to complete adding NVR Recorder.  Name NVR Local IP — Port 443 Remote IP — Port 443

Editing NVR Recorder Details

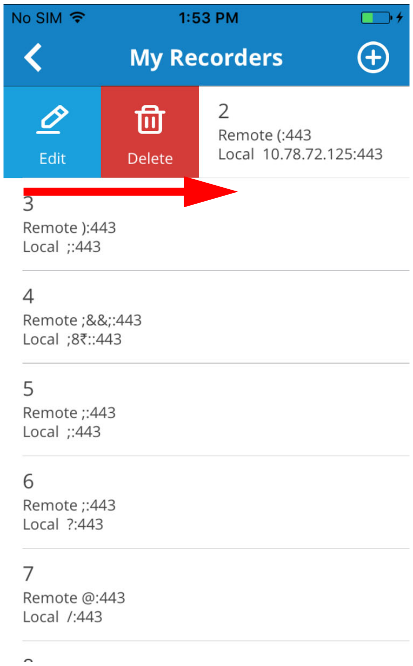
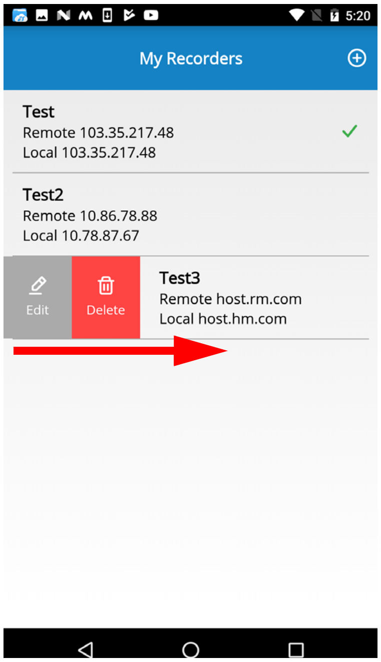
To edit the NVR Recorder details:

Apple mobile device	Android mobile device
Tap >. The already saved NVRs are displayed. On the required NVR recorder, gently swipe to right-side. The **Edit** and **Delete** options are displayed as shown.  No SIM 1:53 PM My Recorders Edit Delete 2 Remote (:443 Local 10.78.72.125:443 3 Remote):443 Local ;:443 4 Remote ;&&;:443 Local ;8₹::443 5 Remote ;:443 Local ;:443 6 Remote ;:443 Local ?:443 7 Remote @:443 Local /:443	Tap >. The already saved NVRs are displayed On the required NVR recorder, gently swipe to right-side. The **Edit** and **Delete** options are displayed as shown.  5:20 My Recorders Test Remote 103.35.217.48 Local 103.35.217.48 ✓ Test2 Remote 10.86.78.88 Local 10.78.87.67 Edit Delete Test3 Remote host.rm.com Local host.hm.com

Apple mobile device	Android mobile device
Tap on **Edit**. The **Edit Recorder** screen is displayed. Modify the required details. Tap **Save** once you modify the details.  Cancel Edit Recorder Save 1 2 3 4 5 6 7 8 9 0 - / : ; ( ) ₹ & @ " #+= . , ? ! ' ABC space Next NVR Name: 2 Local IP: 10.78.72.125 Port: 443 Remote IP: 19.18.17.16 Port: 443	Tap on **Edit**. The **Edit Recorder** screen is displayed. Modify the required details. Tap **Save** once you modify the details.  5:21 Cancel Edit Recorder Save Test3 I test3 D test3 1 2 3 4 5 6 7 8 9 0 @ # $ _ & - + ( ) / * " ' : ; ! ? ABC , 12 34 EN • ES • DE . Name NVR: Test3 Local IP: host.hm.com Port: 443 Remote IP: host.rm.com Port: 443

Deleting the Saved NVR Recorders

To delete the saved NVR Recorders:

Apple mobile device	Android mobile device
Tap ❯. The already saved NVRs are displayed. On the required NVR recorder, gently swipe to right-side. The **Edit** and **Delete** options are displayed as shown. Tap **Delete** to delete the existing NVR server. A warning message is displayed. Tap **Yes** to delete Or Tap **Cancel** to retain.  2 Remote (:443 Local 10.78.72.125:443 3 Remote):443 Local ;:443 4 Remote ;&&;:443 Local ;8₹::443 5 Remote ;:443 Local ;:443 6 Remote ;:443 Local ?:443 7 Remote @:443 Local /:443	Tap ❯. The already saved NVRs are displayed. On the required NVR recorder, gently swipe to right-side. The **Edit** and **Delete** options are displayed as shown. Tap **Delete** to delete the existing NVR server. A warning message is displayed. Tap **Yes** to delete Or Tap **Cancel** to retain.  Test Remote 103.35.217.48 Local 103.35.217.48 ✓ Test2 Remote 10.86.78.88 Local 10.78.87.67 Test3 Remote host.rm.com Local host.hm.com

Changing Default Port 443

To change the default Port 443 for the MAXPRO Web Client and MAXPRO NVR Mobile app, see the ***Changing Default Port 443 for the MAXPRO Web Client and MAXPRO Mobile app*** section on page ***366*** for more information.

Note: *Honeywell recommends you to use a valid certificate from a Certificate Authority that would ensure robust security along with integrity and authenticity, instead of using self-signed certificate. See **Procuring and Installing CA Certificate** section.*

Limitation with Privacy Protection Settings in MAXPRO Mobile App

- If Anonymization is enabled in NVR application then user will not be able to see the video in MAXPRO mobile app/Web client and an error message is displayed.

- If Four eye authentication option is enabled in NVR application then user will not be able to view playback video in MAXPRO mobile app/Web client.

This page is intentionally left blank

APPENDIX

A

APPENDIX A

Customizing IP Address and Machine Name and Scheduling Metadata and Database Backup

Changing the Default IP address and Machine Name

See the Changing the MAXPRO NVR IP Address and Machine Name section on page 86 for more information.

Scheduled Metadata and Database Backup

A common batch file is created for taking the scheduled metadata and database backup.

The following sections describe the procedures to setup scheduled metadata and database backup.

Note: *It is recommended to set up scheduled backups of Metadata and Database with the below steps if they are not already configured on your NVR. The backups can be used to recover a system anytime later in case of a failure or if the OS drive is reimaged with a recovery disk, please contact Technical Support for assistance. Please note the below steps do not include backup or recovery of the Video Storage drives containing the raw video data. Below is the recommended configuration:*

a. Separate Metadata partition (For example M:) of 50 GB or higher size on the non-OS hard drive. Metadata can be pointed to the separate partition during the install/upgrade.

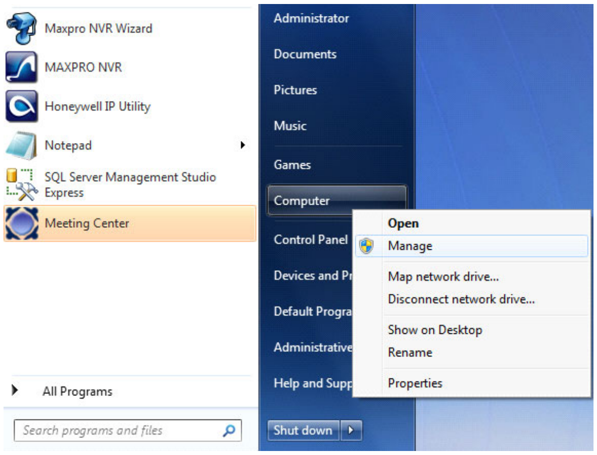
b. The database backup is recommended to be pointed to the Metadata partition.

c. The Metadata backup is recommended to be pointed to the OS partition.

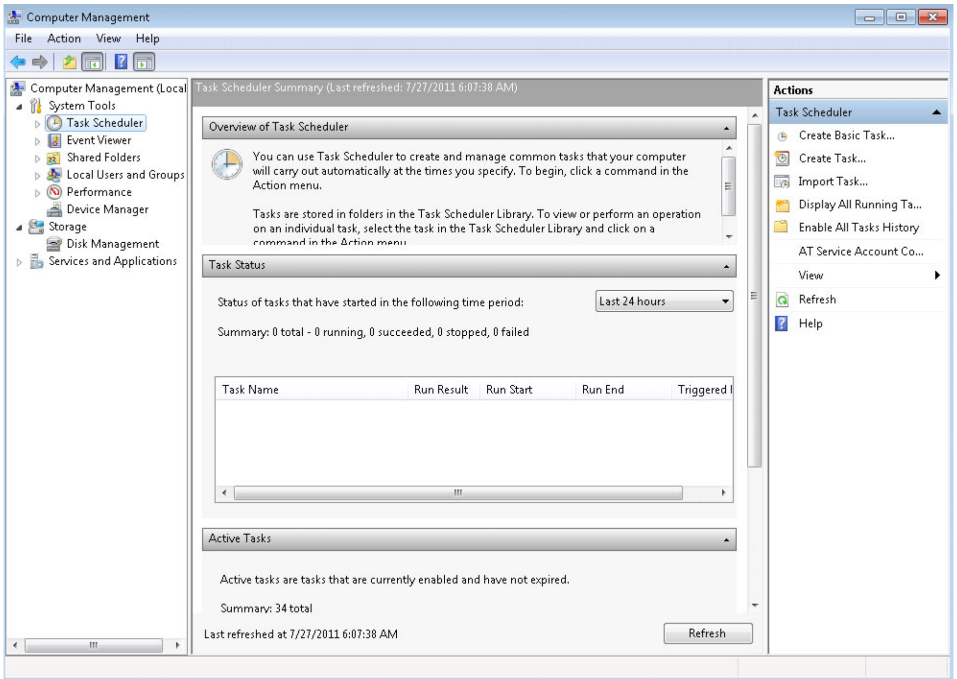
Scheduled Task for Backing up the Metadata and Database

In this scenario, create a scheduled task that helps in taking either a daily backup or a weekly backup or a monthly back up of the metadata based on your requirement.

Step 1. On the Microsoft Windows® 7 computer, right-click the Computer option, and click Manage in the context menu as shown in the following figure.



The Computer Management window appears.



You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Status of tasks that have started in the following time period:

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

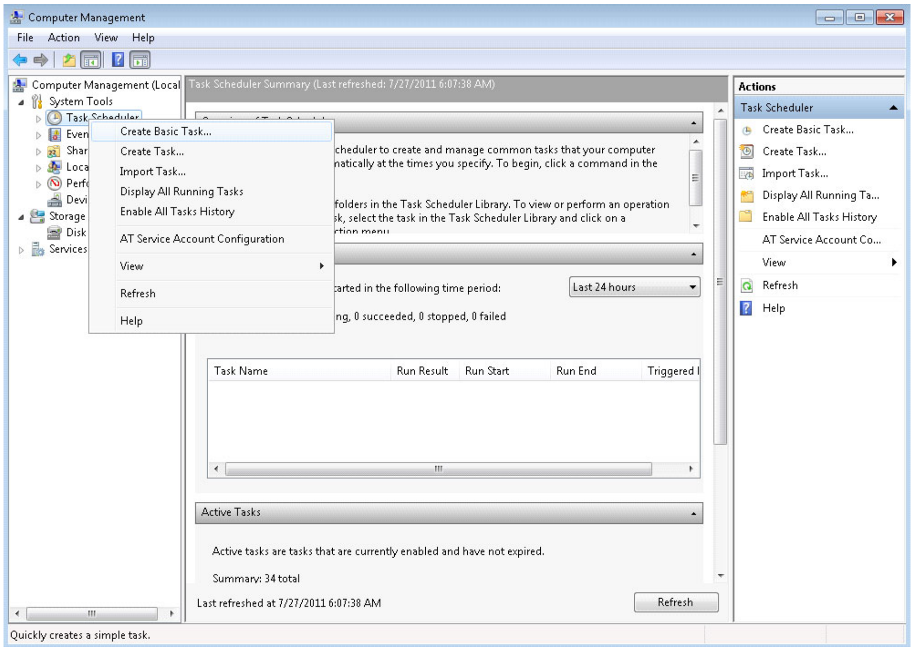
Active tasks are tasks that are currently enabled and have not expired.

Summary: 34 total

Last refreshed at 7/27/2011 6:07:38 AM

Computer Management

Step 2. Right-click Task Scheduler on the left pane, and click Create Basic Task in the context menu as shown in the following figure.



cheduler to create and manage common tasks that your computer natically at the times you specify. To begin, click a command in the

folders in the Task Scheduler Library. To view or perform an operation sk, select the task in the Task Scheduler Library and click on a ction menu

arted in the following time period:

ng, 0 succeeded, 0 stopped, 0 failed

Active tasks are tasks that are currently enabled and have not expired.

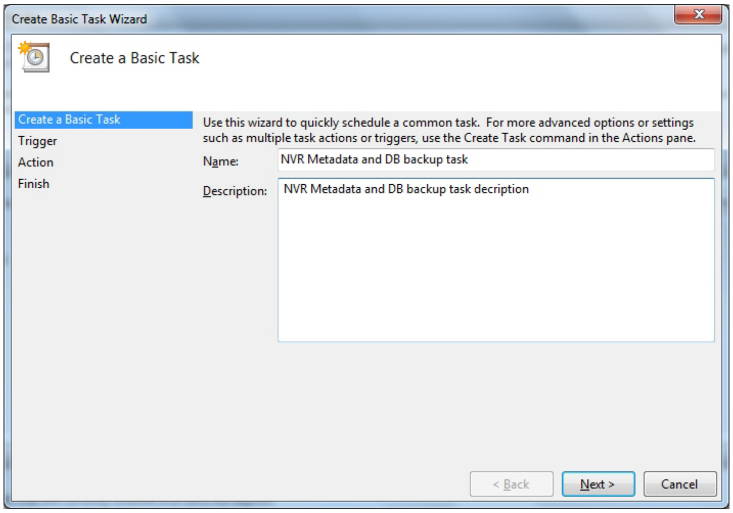
Summary: 34 total

Last refreshed at 7/27/2011 6:07:38 AM

Quickly creates a simple task.

Task Scheduler

The Create a Basic Task dialog box appears.



Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

Name: NVR Metadata and DB backup task

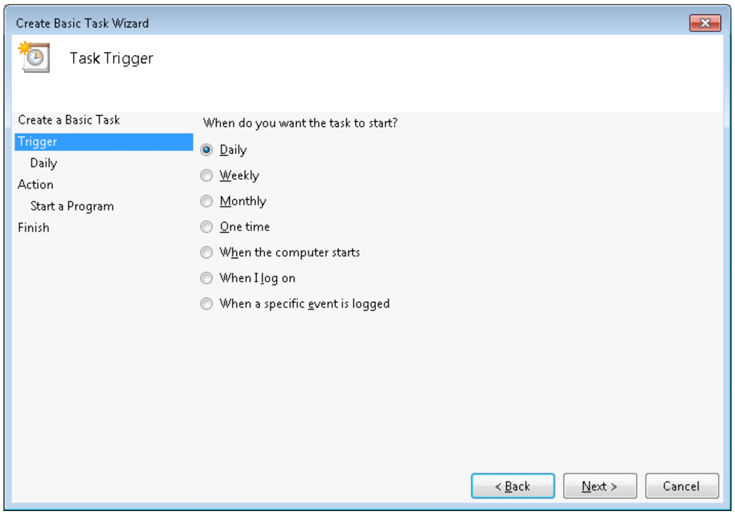
Description: NVR Metadata and DB backup task decription

Create Basic Task

Step 3. Type the Name of the task.

Step 4. Type a Description for the task.

Step 5. Click Next. The Task Trigger dialog box appears.



Create Basic Task Wizard

Task Trigger

Create a Basic Task
Trigger
Daily
Action
Start a Program
Finish

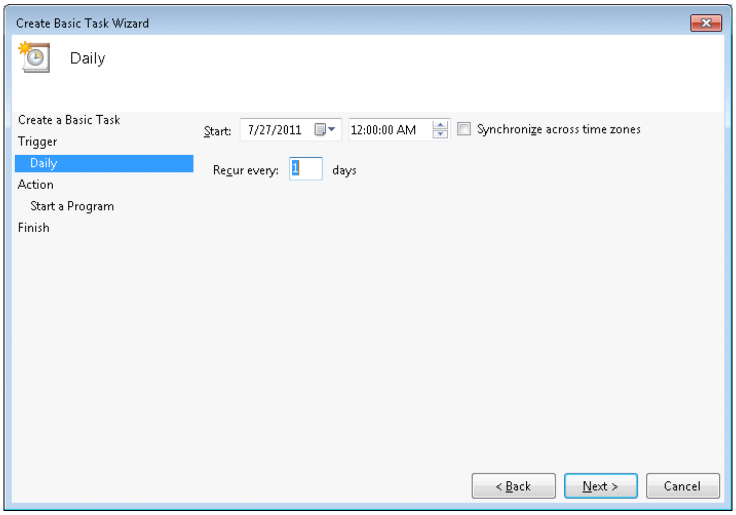
When do you want the task to start?

● Daily
○ Weekly
○ Monthly
○ One time
○ When the computer starts
○ When I log on
○ When a specific event is logged

Task Trigger

Step 6. Select the Daily option. You can select other options based on your requirement.

Step 7. Click Next. The Daily dialog box appears.



Create Basic Task Wizard

Daily

Create a Basic Task
Trigger
Daily
Action
Start a Program
Finish

Start: 7/27/2011 12:00:00 AM □ Synchronize across time zones

Recur every: 1 days

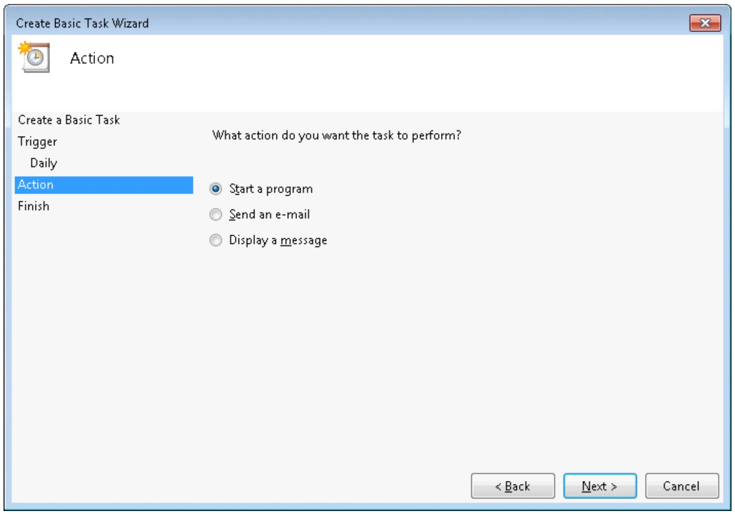
Daily Dialog

Step 8. In the Start box, select the start date and time of the task.

Step 9. Select the Synchronize across time zones check box to synchronize the time across different time zones.

Step 10. Type the days in Recur every, to run the task periodically.

Step 11. Click Next. The Action dialog box appears.



What action do you want the task to perform?

● Start a program

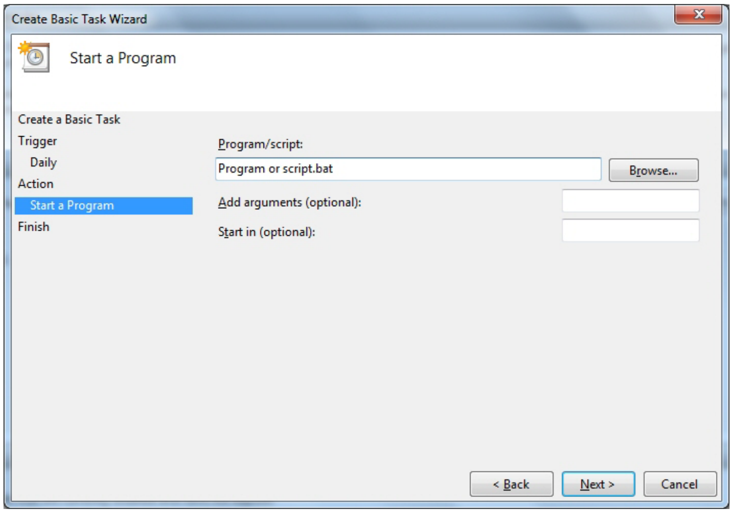
○ Send an e-mail

○ Display a message

Action dialog

Step 12. Select the Start a Program option.

Step 13. Click Next. The Start a Program dialog box appears.



Program/script: Program or script.bat

Add arguments (optional):

Start in (optional):

Start a Program

Step 14. Select the Program/script that is required to run the task. Click Browse and choose the .bat file - TakeNVRBackup.bat.

TakeNVRbackup.bat file is available in the path C:\Install\BackupData for NVRs with v3.5 or later version.

Note: *Please save the batch file (if you make any changes) in the following location: C:\Install\BackupData\TakeNVRBackup.bat. The following are the two new entries in the .bat file set BackupDBDrive=M: set BackupMetaDataDrive=C. By default the Backup Database (BackupDB) is stored in M drive and the Metadata (BackupMetaData) is stored in C drive. It is recommended to choose M and C drive for DB and Metadata backup, but you can choose your own drives (for example: E, D, H drives) to store the backup file.*

```
@echo off
echo
*****************************************************************
echoBatch File to take MAXPRONVR Metadata and Database Backup
echo
*****************************************************************
REM
*****************************************************************
REM To Change the Backup Drive please change the value below
set BackupDBDrive=M:
set BackupMetaDataDrive=C:
REM
*****************************************************************
```

Note: *To change the Backup Drive, change the value of set BackupDBDrive=D:\.*

Step 15. Click Next after you have selected the above batch file. The Summary dialog box appears.

Step 16. Verify the information, and then click Finish.

Meta Data Conversion Utility

Meta data conversion utility is used for updating the unique ID number of a camera in a primary/redundant box. You can use this utility only if you are opting for Redundancy feature.

You need to run this utility before configuring the Redundancy feature in MAXPRO VMS and ensure that all the Primary NVR boxes are updated with proper unique IDs for the cameras.

This utility updates the unique system ID number of the recorded clips and Meta data details for all or specific cameras. It retains your recorded clips and Meta data details during Failover /Failback operations. This allows a user to effectively playback the recorded clip without loss of video. You can also define a new Unique ID for all or required cameras based on the existing Unique IDs.

Meta data conversion utility is available in Bin folder of the installation path and you need to run this utility in each NVR box individually to update the unique system number. This utility is applicable only for existing MAXPRO NVR 4.0 Build 87 H solution box.

Offline Mode

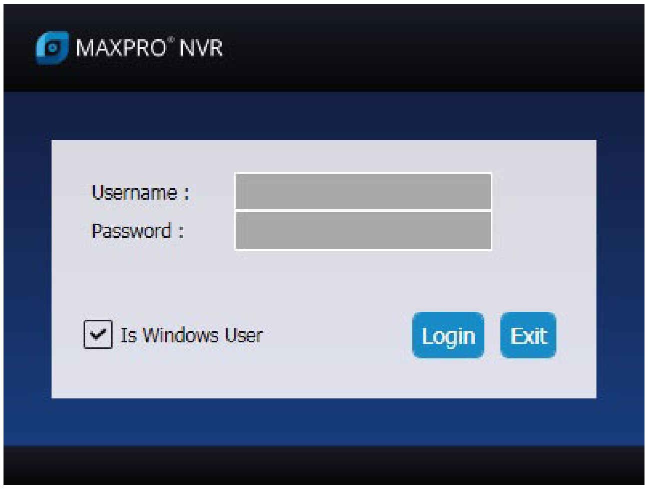
You can also use this utility to synchronize the Unique ID in offline mode for specific cameras. Offline Mode option enables you to update the unique ID manually if you have modified/updated the unique ID only in one NVR box (such as Primary box). To synchronize the unique ID number in both the primary and redundant box you need to run this utility in the Redundant NVR box.

For example for an existing Redundancy User: After Failover/Failback operation, if you have modified/updated the Unique ID in Primary box and the same in not updated in the Redundant box then you cannot playback the clips when the system was in Failover/Failback mode. You need to run this utility in the Redundant box in order to synchronize the IDs and to playback the clips without interruption. See How to update the Unique ID in Offline Mode section on page 404.

How to access the Meta Data Conversion Utility

To access the Meta Data Conversion Utility

Step 1. Navigate to the MAXPRO NVR 4.0 installation path (C:\Program Files (x86)\Honeywell\TrinityFramework\Bin) folder and then click the Meta Data Conversion Utility. The login screen appears as shown below.

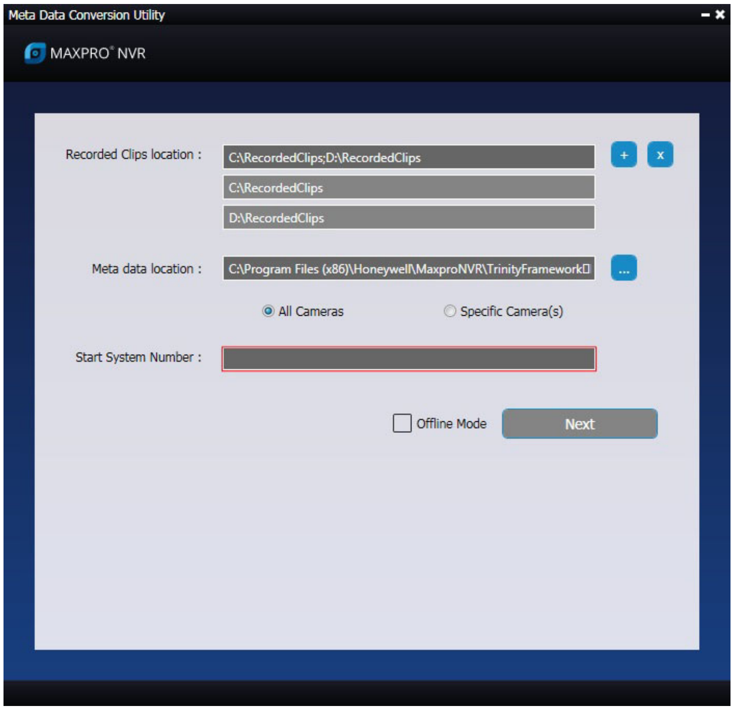


Meta Data Conversion Utility Login

Step 2. Type the Username and Password in box provided.
Or
Select the Is Windows User to login using windows default credentials.

Note: *Select the Is Windows User check box for logging on using the Windows authentication (uses current logged in Windows account credentials). If the Is Windows User check box is cleared, the MAXPRO NVR user name and password is used for authentication. Ensure that you avoid using the @ character in your password.*

Step 3. Click Login. The Meta Data Conversion Utility home screen appears a shown below.



Meta Data Conversion Utility

MAXPRO® NVR

Recorded Clips location : C:\RecordedClips;D:\RecordedClips

C:\RecordedClips

D:\RecordedClips

Meta data location : C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework\

● All Cameras ○ Specific Camera(s)

Start System Number :

□ Offline Mode

Meta Data Conversion Utility

Updating the Unique system ID for all Cameras

To update the Unique system ID for all cameras

Step 1. Access and launch the Meta Data Conversion Utility as explained in How to access the Meta Data Conversion Utility section on page 401. By default the Recorded Clips Location and Meta data location is updated with your default path.

Step 2. Click + to add additional location for Recorded Clips Location.
Or

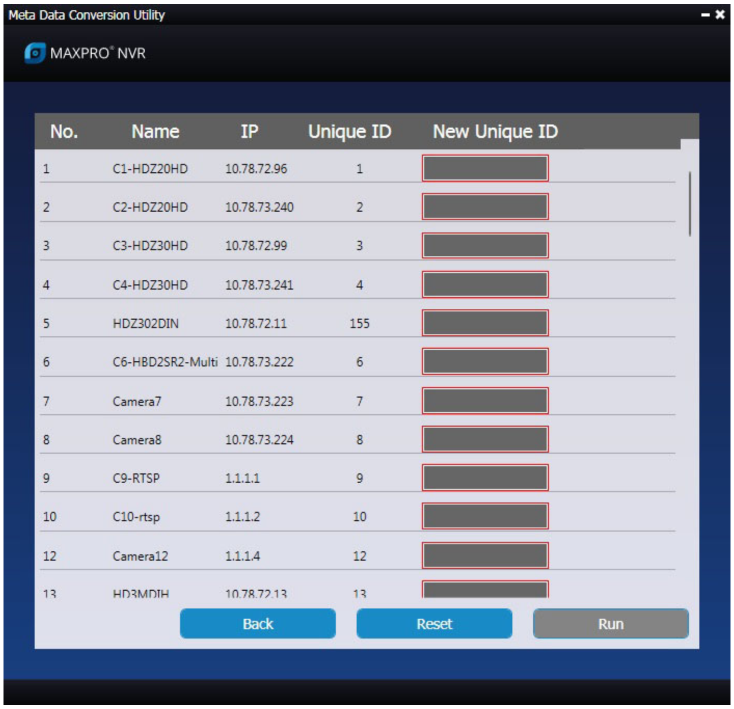
Click x to delete any Recorded Clips Location.

Step 3. Click ... to browse and update the existing Meta data path.

Step 4. Click All Cameras option.

Step 5. In the Start System Number box, type the starting number for all the cameras.

Step 6. Click Next. The next screen for the utility is displayed and the New Unique ID for all the cameras is updated automatically from the start number defined as shown below.



No.	Name	IP	Unique ID	New Unique ID
1	C1-HDZ20HD	10.78.72.96	1	
2	C2-HDZ20HD	10.78.73.240	2	
3	C3-HDZ30HD	10.78.72.99	3	
4	C4-HDZ30HD	10.78.73.241	4	
5	HDZ302DIN	10.78.72.11	155	
6	C6-HBD2SR2-Multi	10.78.73.222	6	
7	Camera7	10.78.73.223	7	
8	Camera8	10.78.73.224	8	
9	C9-RTSP	1.1.1.1	9	
10	C10-rtsp	1.1.1.2	10	
12	Camera12	1.1.1.4	12	
13	HD3MDIH	10.78.72.13	13	

Define Unique ID screen

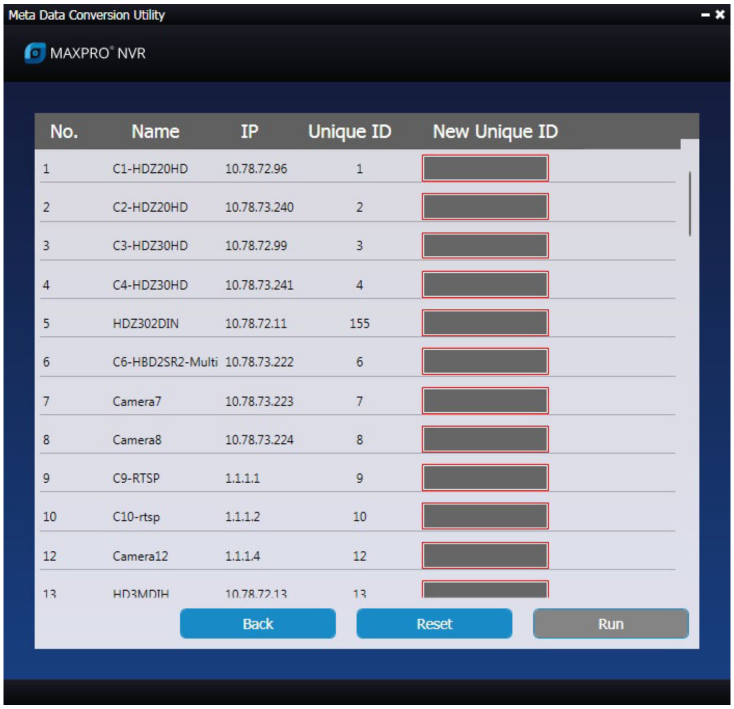
Step 7. Click Run to execute the utility.
Or
Click Back togo back to home screen to change the settings.

Updating the Unique system ID for Specific Cameras

To update the Unique system ID for Specific Cameras

Step 1. Perform step 1 through step 3 of Updating the Unique system ID for all Cameras section on page 402.

Step 2. Click Specific Camera(s) option, and then click Next. The next screen for the utility is displayed and the New Unique ID column for all the cameras is displayed blank as shown below.



No.	Name	IP	Unique ID	New Unique ID
1	C1-HDZ20HD	10.78.72.96	1	
2	C2-HDZ20HD	10.78.73.240	2	
3	C3-HDZ30HD	10.78.72.99	3	
4	C4-HDZ30HD	10.78.73.241	4	
5	HDZ302DIN	10.78.72.11	155	
6	C6-HBD2SR2-Multi	10.78.73.222	6	
7	Camera7	10.78.73.223	7	
8	Camera8	10.78.73.224	8	
9	C9-RTSP	1.1.1.1	9	
10	C10-rtsp	1.1.1.2	10	
12	Camera12	1.1.1.4	12	
13	HD3MDIH	10.78.72.13	13	

Updating Unique ID

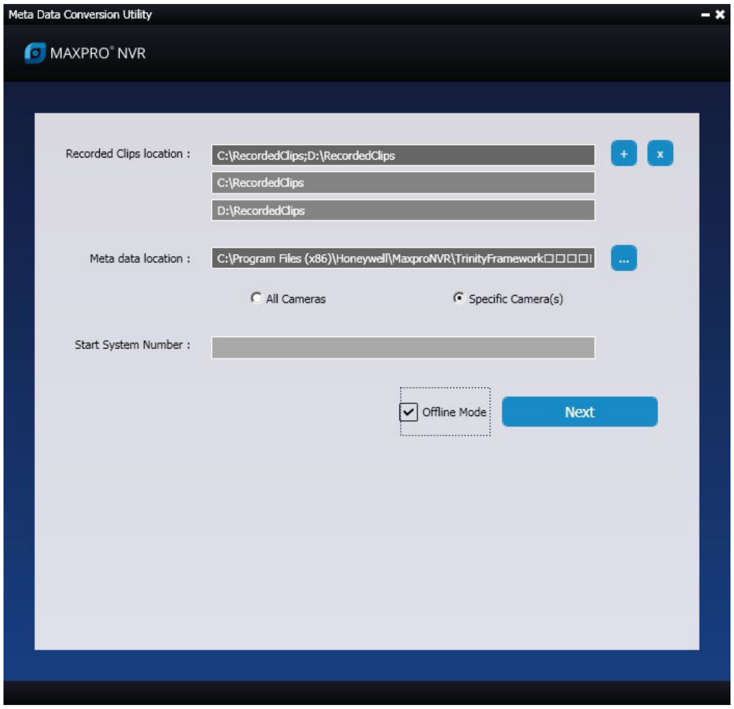
Step 3. Scroll up and down to view the specific cameras and then type the required New Unique ID in the corresponding box.

Step 4. Click Run to execute the utility.
Or
Click Reset to reset all ID.

How to update the Unique ID in Offline Mode

To update the unique ID in offline mode

Step 1. In the Meta Data Conversion Utility home page, click Specific Camera(s) option, and then select the Offline Mode check box as shown below.



Recorded Clips location : C:\RecordedClips;D:\RecordedClips
C:\RecordedClips
D:\RecordedClips

Meta data location : C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework□□□□I

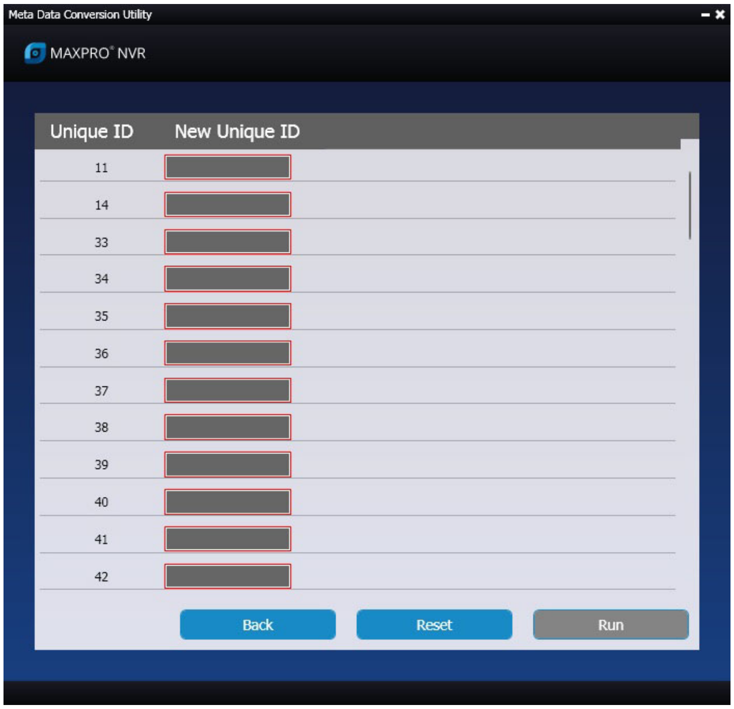
○ All Cameras ● Specific Camera(s)

Start System Number :

☑ Offline Mode

Offline Mode

Step 2. Click Next. The next screen for the utility is displayed and the New Unique ID column for all the cameras is displayed blank as shown below.



Unique ID	New Unique ID
11	
14	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	

Offline Updating Unique ID

Step 3. Scroll up and down to view the specific cameras to update the unique ID and then type the required New Unique ID in the corresponding box.

Step 4. Click Run to execute the utility.
Or
Click Reset to reset all ID.

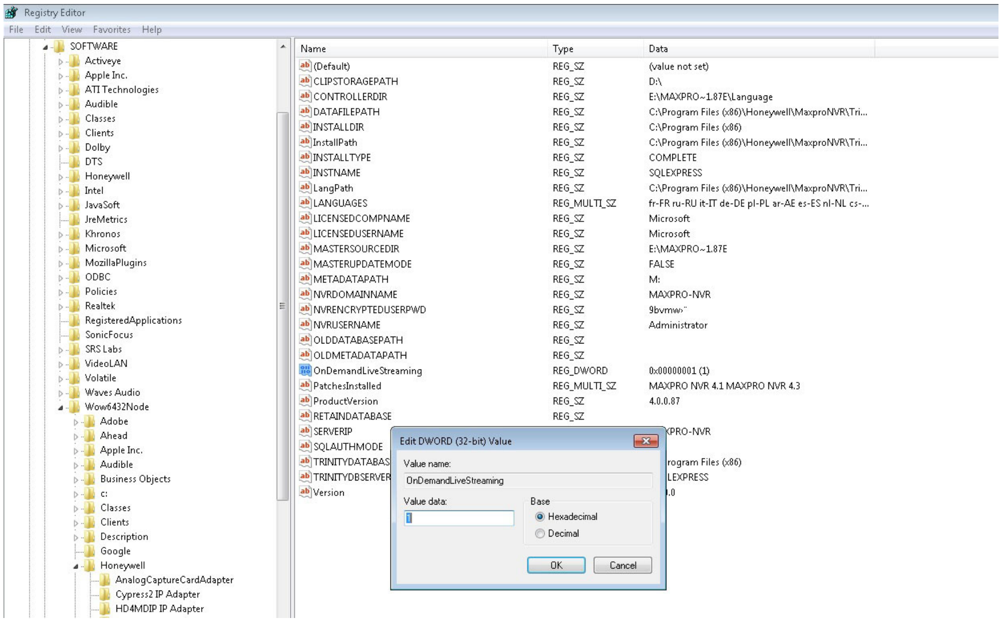
How to Enable Video on demand feature in MAXPRO NVR

Step 1. Launch the Registry Editor Window.

Step 2. Navigate to the below registry path HKEY_LOCAL_MACHINE->SOFTWARE->Wow6432Node->Honeywell->MaxproNVR->TrinityFramework.

Step 3. Locate OnDemandLiveStreaming parameter and in the Data column.

Step 4. By default value is 0 means its not enabled, If user want to enable Video on demand feature it must be set to 1 as shown below. Change the 0x00000000 (0) value to 0x00000000 (1)



Name	Type	Data
(Default)	REG_SZ	(value not set)
CLIPSTORAGEPATH	REG_SZ	D:\
CONTROLLERDIR	REG_SZ	E:\MAXPRO~1.87E\Language
DATAFILEPATH	REG_SZ	C:\Program Files (x86)\Honeywell\MaxproNVR\Tri...
INSTALLDIR	REG_SZ	C:\Program Files (x86)
InstallPath	REG_SZ	C:\Program Files (x86)\Honeywell\MaxproNVR\Tri...
INSTALLTYPE	REG_SZ	COMPLETE
INSTNAME	REG_SZ	SQLEXPRESS
LangPath	REG_SZ	C:\Program Files (x86)\Honeywell\MaxproNVR\Tri...
LANGUAGES	REG_MULTI_SZ	fr-FR ru-RU it-IT de-DE pl-PL ar-AE es-ES nl-NL cs-...
LICENSEDCOMPNAME	REG_SZ	Microsoft
LICENSEDUSERNAME	REG_SZ	Microsoft
MASTERSOURCEDIR	REG_SZ	E:\MAXPRO~1.87E
MASTERUPDATEMODE	REG_SZ	FALSE
METADATAPATH	REG_SZ	M:
NVRDOMAINNAME	REG_SZ	MAXPRO-NVR
NVRENCRYPTEDUSERPWD	REG_SZ	9bvmw›¨
NVRUSERNAME	REG_SZ	Administrator
OLDDATABASEPATH	REG_SZ	
OLDMETADATAPATH	REG_SZ	
OnDemandLiveStreaming	REG_DWORD	0x00000001 (1)
PatchesInstalled	REG_MULTI_SZ	MAXPRO NVR 4.1 MAXPRO NVR 4.3
ProductVersion	REG_SZ	4.0.0.87
RETAINDATABASE	REG_SZ	
SERVERIP		XPRO-NVR
SQLAUTHMODE		
TRINITYDATABAS		rogram Files (x86)
TRINITYDBSERVER		LEXPRESS
Version		.0

Edit DWORD (32-bit) Value

Value name: OnDemandLiveStreaming

Value data: 1

Base

● Hexadecimal

○ Decimal

Step 5. Restart the PC and both the NEO (NEO 1 and 2) services for the changes to take effect.

Note: *In VMS no need to perform any settings or config changes to enable VOD feature. No recordings will take place in NVR once Video On Demand feature is enabled.*

How to Enable the Camera Stream

To Enable/Disable cameras and Enable Camera stream Redirect to NVR in ISOM

Step 1. Navigate the path in NVR C:\Program Files (x86)\Honeywell\UVISOM.

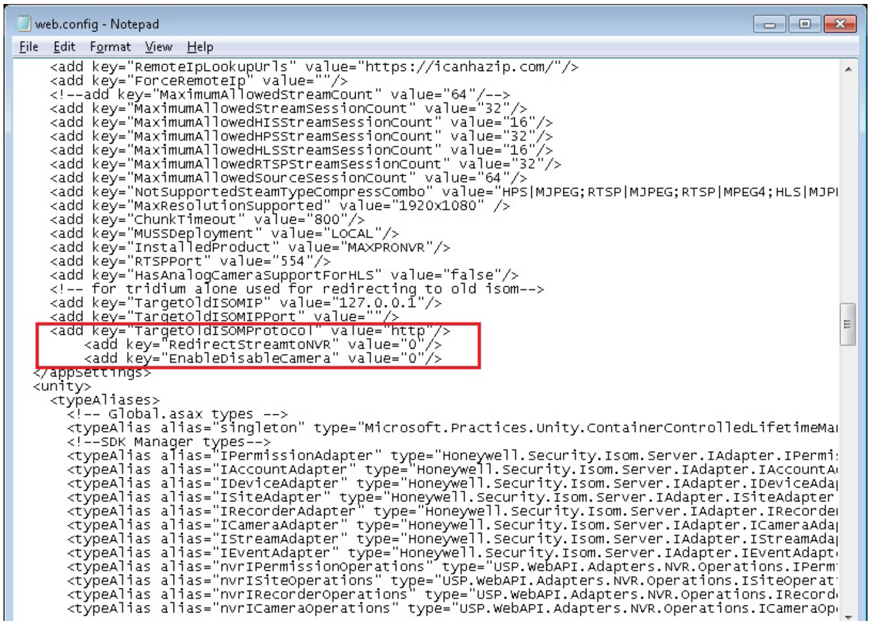
Step 2. Open web.config file in notepad and check the below 2 entries:

<add key="RedirectStreamtoNVR" value="0"/>

<add key="EnableDisableCamera" value="0"/>

Step 3. By default both are set to "0". means it is disabled. To enable the feature change the value from 0 to 1 as highlighted below.

Note: *Once Video On Demand is configured to be used in MAXPRO NVR then Enable/ Disable camera feature can be turned off.*



```
    <add key="RemoteIpLookupUrls" value="https://icanhazip.com/"/>
    <add key="ForceRemoteIp" value=""/>
    <!--add key="MaximumAllowedStreamCount" value="64"/-->
    <add key="MaximumAllowedStreamSessionCount" value="32"/>
    <add key="MaximumAllowedHISStreamSessionCount" value="16"/>
    <add key="MaximumAllowedHPSStreamSessionCount" value="32"/>
    <add key="MaximumAllowedHLSStreamSessionCount" value="16"/>
    <add key="MaximumAllowedRTSPStreamSessionCount" value="32"/>
    <add key="MaximumAllowedSourceSessionCount" value="64"/>
    <add key="NotSupportedSteamTypeCompressCombo" value="HPS|MJPEG;RTSP|MJPEG;RTSP|MPEG4;HLS|MJPI
    <add key="MaxResolutionSupported" value="1920x1080" />
    <add key="ChunkTimeout" value="800"/>
    <add key="MUSSDeployment" value="LOCAL"/>
    <add key="InstalledProduct" value="MAXPRONVR"/>
    <add key="RTSPPort" value="554"/>
    <add key="HasAnalogCameraSupportForHLS" value="false"/>
    <!-- for tridium alone used for redirecting to old isom-->
    <add key="TargetOldISOMIP" value="127.0.0.1"/>
    <add key="TargetOldISOMIPPort" value=""/>
    <add key="TargetOldISOMProtocol" value="http"/>
        <add key="RedirectStreamtoNVR" value="0"/>
        <add key="EnableDisableCamera" value="0"/>
  </appSettings>
  <unity>
    <typeAliases>
      <!-- Global.asax types -->
      <typeAlias alias="singleton" type="Microsoft.Practices.Unity.ContainerControlledLifetimeMa
      <!--SDK Manager types-->
      <typeAlias alias="IPermissionAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IPermi
      <typeAlias alias="IAccountAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IAccountA
      <typeAlias alias="IDeviceAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IDeviceAda
      <typeAlias alias="ISiteAdapter" type="Honeywell.Security.Isom.Server.IAdapter.ISiteAdapter
      <typeAlias alias="IRecorderAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IRecorde
      <typeAlias alias="ICameraAdapter" type="Honeywell.Security.Isom.Server.IAdapter.ICameraAda
      <typeAlias alias="IStreamAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IStreamAda
      <typeAlias alias="IEventAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IEventAdapt
      <typeAlias alias="nvrIPermissionOperations" type="USP.WebAPI.Adapters.NVR.Operations.IPerm
      <typeAlias alias="nvrISiteOperations" type="USP.WebAPI.Adapters.NVR.Operations.ISiteOperat
      <typeAlias alias="nvrIRecorderOperations" type="USP.WebAPI.Adapters.NVR.Operations.IRecord
      <typeAlias alias="nvrICameraOperations" type="USP.WebAPI.Adapters.NVR.Operations.ICameraOp
```

To enable this feature in MAXPRO VMS Server then perform the following steps:

Step 1. Navigate the path in VMS C:\Program Files (x86)\Honeywell\UVISOM.

Step 2. Repeat the step 2 to step 3 of How to Enable the Camera Stream section.

Note: *Make sure MAXPRO Web client is working.*

APPENDIX

B

APPENDIX B

Image Stream Combinations for Oncam Grandeye Cameras

For Oncam Grandeye Evolution Cameras

Camera Type	Resolution	Best fps (MAX)(H.264)
Evolution	1056x960	15
	2144x1944	10
	1448x1360	15
	528x480	15

Device Characteristics of Oncam Grandeye Cameras

Characteristic	Camera Type	Comments
Camera provides variable fps. Example: For highest resolution, 2144x1944, maximum fps a camera can provide is 3. On several occasions, it is seen that fps varies from 1 to 3, and very rarely a camera provides 3 fps.	Halocam	As per Grandeye, fps varies and cannot go beyond the maximum value, 3. This is the design specific behavior of the camera.

Characteristic	Camera Type	Comments
Camera provides variable fps. Example: For highest resolution, 2144x1944, maximum fps a camera can provide is 10. On several occasions, it is seen that fps varies from 6 to 10, and very rarely a camera provides 10 fps.	Evolution	As per Grandeye, fps varies and cannot go beyond the maximum value 10. This is the design specific behavior of the camera.
Before streaming, the active Camera stream (Resolution) must be set in the Camera Web page. In MAXPRO NVR, if you do not select the active stream, video is not displayed.	Evolution	As per Grandeye this is the design specific behavior of the camera.

VMD Settings and Motion-based Recording Configuration

VMD setup consists of:

- Event-based recording configuration on MAXPRO NVRs.
- Server VMD (SMART VMD) settings on all video devices supported in MAXPRO NVR.
- Built-in VMD (Camera based VMD) settings on Honeywell IP cameras.

Overview of MAXPRO NVR Recording Options

Each IP camera configured in the NVR can be set for Continuous (background) recording, event-based recording, or both.

When using event-based recording, Honeywell recommends that you:

- Set up recording on events at a higher frame rate
- Set up continuous (background) recording at a lower frame rate

Continuous (background) recording at a lower frame rate and event-based recording with boosted higher frame rate ensure that:

- Video recording is not missed in the event that the motion is not sufficient to trigger a VMD event on the camera; that is, the motion does not meet the configured VMD threshold on the camera.
- Video records longer than pre and post event recording with the lower frame rate; that is, Continuous (background) recorded video provides better forensics.

MAXPRO NVR supports recording at different frame rates for each camera using a single live stream from the camera and recording quality settings. The NVR Recording Quality Setting options for Continuous (background) and Event recording are:

- Same as Live
- Every IFrame
- Every Second IFrame
- Every Third IFrame.

Example:

For a camera configured in the NVR with these settings:

- FPS = 5
- GOP = 5
- Record Quality Setting: Background/Continuous Recording = Every IFrame
- Event Based Recording = Same as Live

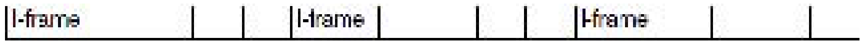
The result is a Continuous (background) record rate of 1 FPS and a boosted event-based record rate of 5 FPS.

Note:

- A combination of continuous and event-based recording from a camera can be achieved using the relationship between Frames Per Second (FPS) and Group Of Pictures (GOP).
- FPS is a measure of the images every second from the camera, while GOP determines how frames are sequenced.
- Every GOP starts with an I-frame (full image) and is followed by smaller images which are relative to the images preceding it. So, for a GOP of 5 there will be one I-frame for every 5 frames.

Note:

The following figure shows an example of three seconds of video at 5 FPS and 5 GOP.



I-frame Example

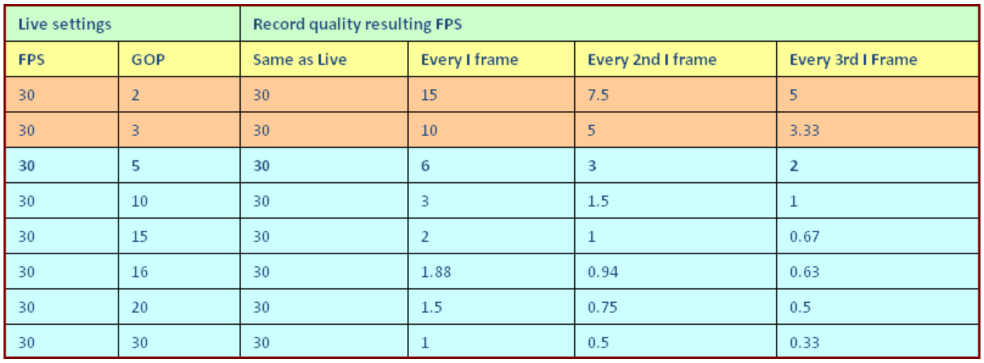
The NVR record Quality Settings for Continuous (background) and Event recording can be used to achieve different level of FPS by selecting one of the following options.

- Same as Live: Every frame is recorded (5 FPS in the example)

- Every I-frame: Every I-frame is recorded (1 FPS in the example)
- Every Second Iframe: Every second I-frame is recorded (1 frame every 2 seconds in the example)
- Every Third Iframe: Every third I-frame is recorded (1 frame every 3 seconds in the example)

For more detailed information on the relationship between FPS and GOP and example settings to achieve different frame rates, refer to the table below:

Note: *GOP value below 5 may not be achieved from all the cameras.*



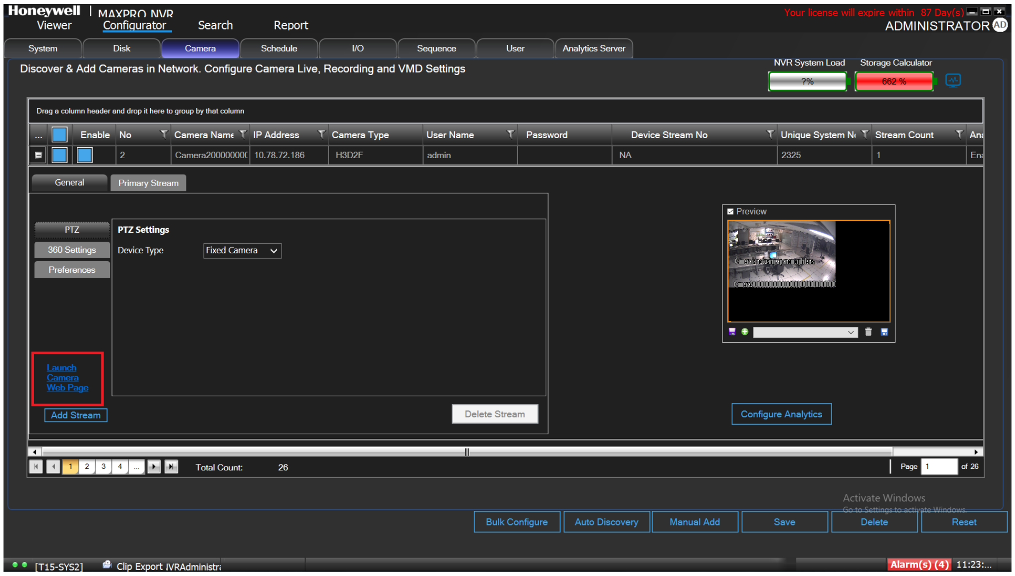
Live settings		Record quality resulting FPS			
FPS	GOP	Same as Live	Every I frame	Every 2nd I frame	Every 3rd I Frame
30	2	30	15	7.5	5
30	3	30	10	5	3.33
30	**5**	**30**	**6**	**3**	**2**
30	10	30	3	1.5	1
30	15	30	2	1	0.67
30	16	30	1.88	0.94	0.63
30	20	30	1.5	0.75	0.5
30	30	30	1	0.5	0.33

Configuring the Pre and Post Event Recording Settings

See the ***Event Recording Settings*** section on page ***163*** for more information on configuring the pre and post event recording settings.

Configuring Camera Settings for VMD-Based Recording

Step 1. Click the Configurator tab and then the Camera tab to open the Camera configuration page.



Discover & Add Cameras in Network. Configure Camera Live, Recording and VMD Settings

Drag a column header and drop it here to group by that column

...	□	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count	Ana
⊟	□	□	2	Camera20000000(	10.78.72.186	H3D2F	admin		NA	2325	1	Ena

PTZ Settings

Device Type: Fixed Camera

Total Count: 26

Page 1 of 26

Camera configuration page

- For built-in (Camera-based) VMD configuration, open the camera web page by clicking Launch Web View for Advanced Setup. See the ***Configuring Built-in VMD*** section on page ***414*** for more information.

- For Server-based VMD (SMART VMD) configuration, select the Enable SMART VMD check box and click Configure. See the ***Server VMD (SMART VMD)*** section on page ***414*** for more information.

Note: *Built-in (Camera-based) VMD support in NVR is based on the type of device integration and may not be supported for all devices. Please refer to the MAXPRO NVR compatibility list on HOTA website (http://www.security.honeywell.com/hota/) for details. Server VMD (SMART VMD) is supported for all video devices supported by NVR.*

Step 2. Select a camera to configure the following items in the Camera pane:

- Continuous Recording (default=24x7): In the Continuous Recording drop-down list, select the appropriate value. Honeywell recommends 24x7 for continuous recording. There are several standard options for scheduled recording. You can define additional schedules in the Schedules tab.

- Event Based Recording (default=NONE): In the Event based Recording drop-down list, select the appropriate value. Select a setting other than NONE to activate event-based recording. The typical setting would be 24x7. There are also several standard options for scheduled recording. You can define additional schedules in the Schedules tab.

Server VMD (SMART VMD)

See the ***Server VMD (SMART VMD)*** section on page ***414*** for more information.

Configuring Built-in VMD

To Congfigure Camera based VMD on Honeywell IP Cameras:

Use the Camera Web Client to configure VMD on the camera itself.

For motion detection, an Administrator can enable and configure up to five zones within a scene. The enabled and configured zones are monitored for motion.

Step 1. Click the Video Analytics tab.

Step 2. Click the Region drop-down list in the Video Motion Detection pane, then select a region from the five available.

Step 3. Click the VMD drop-down arrow, and then select Enable.

Step 4. The regions appear as colored rectangles in their default positions. Click and drag the box to resize and place it over the camera image. This box is the region of interest.

Step 5. Click Motion Threshold and then select the sensitivity level:

- Low (30%) (most sensitive)
- Medium (50%)
- High (80%) (least sensitive).

It is recommended that you use the medium sensitivity at 50% as the initial setting. It can be further adjusted as explained in ***Fine Tuning the Video Motion Detection*** section on page ***414***.

Step 6. Click Apply.

Note:

- To ensure that the VMD settings have been applied, navigate to another tab, and then back to the Video Settings tab. Check the VMD settings for the changes you made.
- In the unlikely event that the VMD settings are not applied, please try to log off from the software and log on again. Then repeat step 1 through step 5 above.

Disabling Motion Detection

To disable a zone, click the VMD drop-down arrow and then select Disable.

Fine Tuning the Video Motion Detection

For optimum results, adjust the VMD configuration to match the camera field of view, regions of interest and other factors. The recommended configuration procedure is:

Step 1. Identify areas in the image where motion detection alarms should be triggered. In some applications, motion anywhere in the image needs to be reported. In other applications, you may wish to monitor specific areas such as doors, parking lot entrances, or other areas of interest.

Step 2. Select one of the five available regions for each area of interest and draw the
region-of-interest box for that region to fully cover the area of interest.

Tip: The camera only measures motion inside the drawn box. For example, a person or vehicle moving along the boundary of the box may or may not trigger an alarm, because their motion is only partially evaluated. Therefore, it is important to adjust the region-of-interest boxes to fully cover the required areas of interest.

Step 3. Test your initial configuration setup by observing VMD performance to ensure that relevant scene motion triggers alarms and to ensure that the camera is not reporting false alarms (such as VMD alarms triggered due to image noise). In cameras with a wide field of view, or when activity happens far away from the camera, people and vehicles may appear rather small in the image. In such cases, it may not be possible to apply a single area of interest to the whole field of view to reliably detect motion. In such cases, Honeywell recommends covering the camera view with multiple, smaller region-of-interest boxes, concentrating on specific areas where motion alarms are important, such as entrances, restricted access areas, and so on.

Step 4. Use the medium sensitivity of 50% as the initial setting. You can adjust this further if required.

Note: *Observe VMD performance in all expected lighting conditions after the initial configuration is applied. Ensure that relevant scene motion triggers alarms and ensure that the camera is not reporting false alarms (such as VMD alarms triggered due to image noise).*

Increasing VMD Sensitivity

If the relevant scene motion does not trigger VMD alarms, try the following adjustments to increase VMD sensitivity.

- Decrease the sensitivity level from 80% to 50%, or from 50% to 30%. This change causes smaller objects to trigger alarms and it requires smaller contrast level to report an alarm. This should be the primary adjustment mechanism.
- Reduce the size of the region-of-interest box and, if needed, add more regions. Note that this adjustment causes smaller objects to also trigger VMD alarms.

Tip: After VMD sensitivity is increased, observe the performance in other lighting conditions in case further tuning is required to prevent false alarms.

Decreasing VMD Sensitivity

If VMD alarms are triggered even when there is no motion and no significant changes in the video, try the following adjustments to decrease VMD sensitivity.

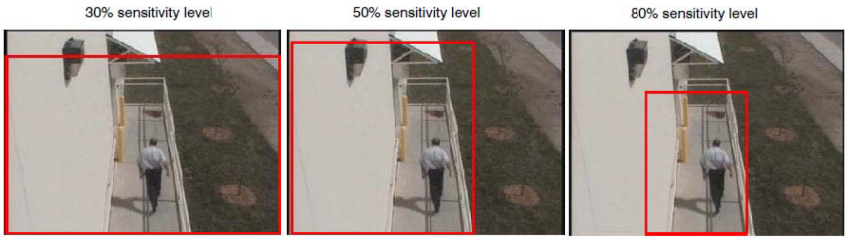
- Increase the sensitivity level from 30% to 50%, or from 50% to 80%. This primary adjustment mechanism increases the required contrast level (or amount of noise) required to trigger an alarm. Higher sensitivity levels also require larger amounts of motion to be observed before a VMD alarm is triggered.
- Increase the size of the region-of-interest box. This adjustment prevents smaller objects (or smaller areas of noise) from triggering VMD alarms.

VMD Configuration Examples

The sensitivity level examples below are provided only for illustration. Other factors such as lighting level, contrast, and image noise may affect VMD performance and may require further tuning adjustments as described above.

Normal Field of View

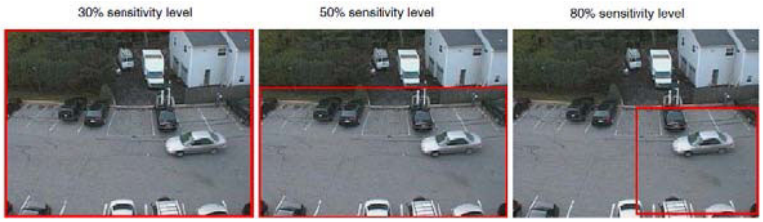
In a normal field of view, with a person walking in front of the camera, the maximum recommended region-of-interest box sizes would be as shown by the red boxes.



Sensitivity Level Comparison: Normal Field of View

Wide Field of View

In a wide field of view camera, the car shown below (Sensitivity Level Comparison: Wide Field of View)would be expected to trigger a VMD alarm if the VMD region-of-interest box is not larger than indicated by the red box.



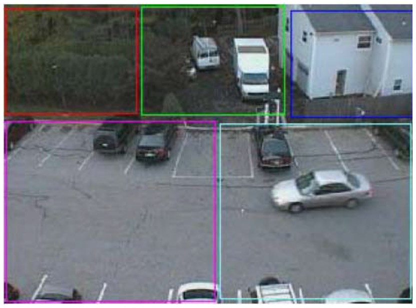
Sensitivity Level Comparison: Wide Field of View

Combination Field of View

For cameras with a wide-angle field of view covering a large outdoor scene, people who walk far away from the camera might appear rather small in the image. If motion needs to be detected in the entire field of view, the following region-of-interest box configuration is recommended.

- Three smaller boxes, set to 30% sensitivity, covering the upper portion of the image where people appear small.
- Two larger boxes, set to 50% sensitivity, covering the lower portion of the image where objects appear larger.

Combination Field of View Example illustrates a typical region-of-interest box configuration in a combination field of view.



Combination Field of View Example

Event and Alarm Types

This section describes about the various default Event and Alarm types with severity level for Camera, Recorder and SMART VMD.

Camera Level Events and Alarm types

The following table displays the 17 default camera level Events and Alarm types with description and severity level.

The EventSeverity level above 50 is an alarm and below 50 is an event.

See the ***Setting the Alarm Threshold Value*** section on page ***140*** to set the Alarm Severity Threshold value.

EventID	EventDescription	EventSeverity
3	Camera User Recording Started	20
4	Camera User Recording Completed	20
5	Camera Disconnected	40
6	Camera Connected	40
7	Camera Continuous Recording Disabled	20
8	Camera Continuous Recording Enabled	20
9	Camera Event Recording Started	30
10	Camera Event Recording Completed	30

EventID	EventDescription	EventSeverity
11	Camera Disabled	20
12	Camera Enabled	20
13	Camera User Recording Error	30
14	Camera NoMotion Detected	40
15	Camera Motion Detected	40
16	Camera Motion Started	40
17	Camera Motion Stopped	30
18	Camera Motion Stopped in all regions	10
139	ExternalInput2	40

Video Analytics Events

The following table displays the 5 default Video Analytics Events with description and severity level. New EquIP series model cameras (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D, HDZ302DIN) generates the following events.

Note: *User need to configure the following events in the camera web page to view in the Alarms window.*

EventID	EventDescription	EventSeverity
2066	Face Detected	40
	Tamper Detected	
	Audio Detected	
	Device SD Card Full	
	Device SD Card Failure	

Recorder Level Events and Alarm types

The following table displays the 4 default Recorder level Events and Alarm types with description and severity level.

EventID	EventDescription	EventSeverity
1	Recorder Connected	70
2	Recorder Disconnected	70
22	Low disk space	70
27	Missing Storage Drive	50

EventID	EventDescription	EventSeverity
33	Low Archival Disk Space	70
34	Missing Archival Drive	50

SMART VMD Level Events and Alarm types

The following table displays the default SMART VMD level Events and Alarm types with description and severity level.

EventID	Event Description	EventSeverity
28	SMART VMD Connected	40
29	SMART VMD Disconnected	40

Configuring Loitering & Intrusion Trace Alarms

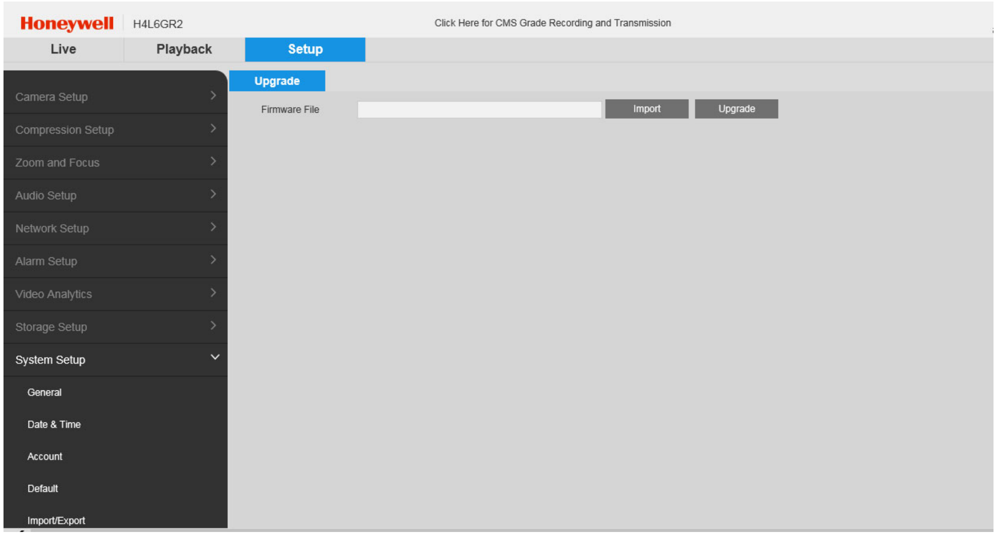
H4L6GR2 and HBL6GR2 camera models support both Intrusion Trace and Loitering Trace Alarms. User needs to configure these alarms in specific camera web page. You need to first upgrade the firmware of the camera and then configure the alarms.

How to upgrade the Firmware of a camera

Step 1. Launch the required camera web page.

Step 2. Click the Setup tab.

Step 3. On the left pane, navigate to System Setup > Upgrade. The Upgrade page is displayed as shown below.



Upgrade Firmware - Setup Page

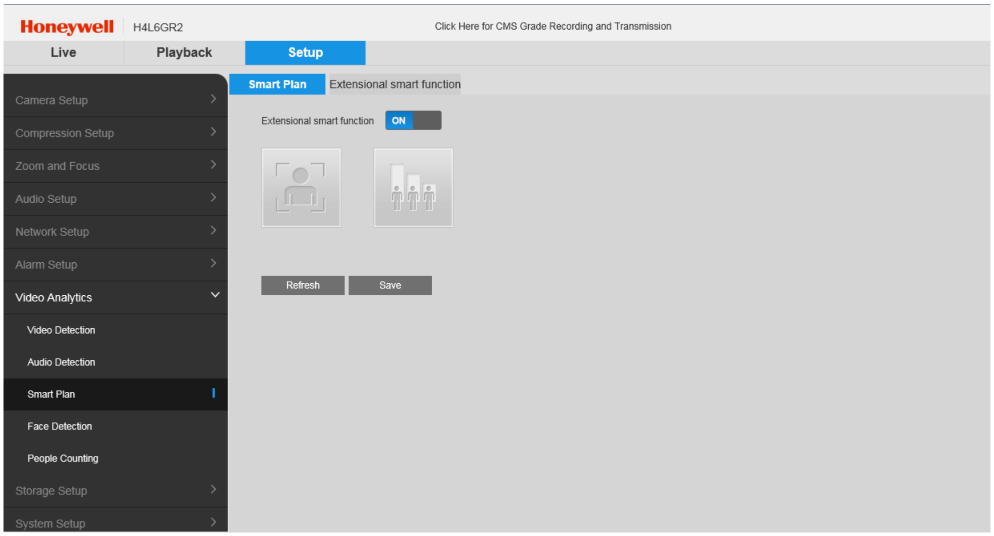
Step 4. Click Import to import the Latest Firmware file and then click Upgrade.

How to configure Loitering Trace Alarm

Note: *You can configure and use only one alarm license at once. If you want to view another type of alarm then uninstall the previous firmware, install the required firmware and then configure the alarm.*

Tip: The below procedure is also applicable to configure the Intrusion Trace Alarms.

Step 1. After the camera firmware upgrade is done, in the camera web page navigate to Video Analytics > Smart Plan. The Smart Plan page is displayed on the left side as shown below.

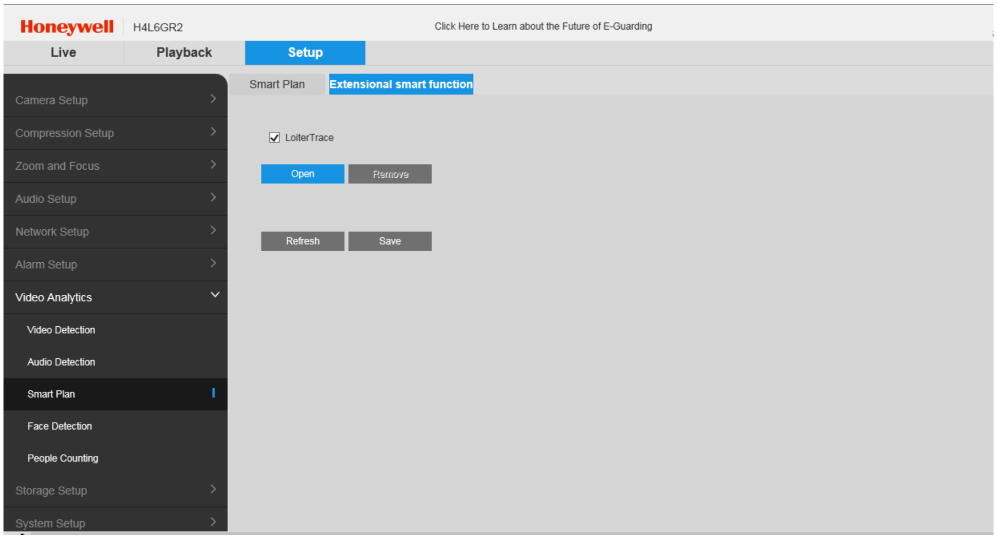


Extensional smart function ON

Smart Plan Setup Page

Step 2. Under Smart Plan, turn ON the Extensional smart function option. The Extensional smart function tab is enabled.

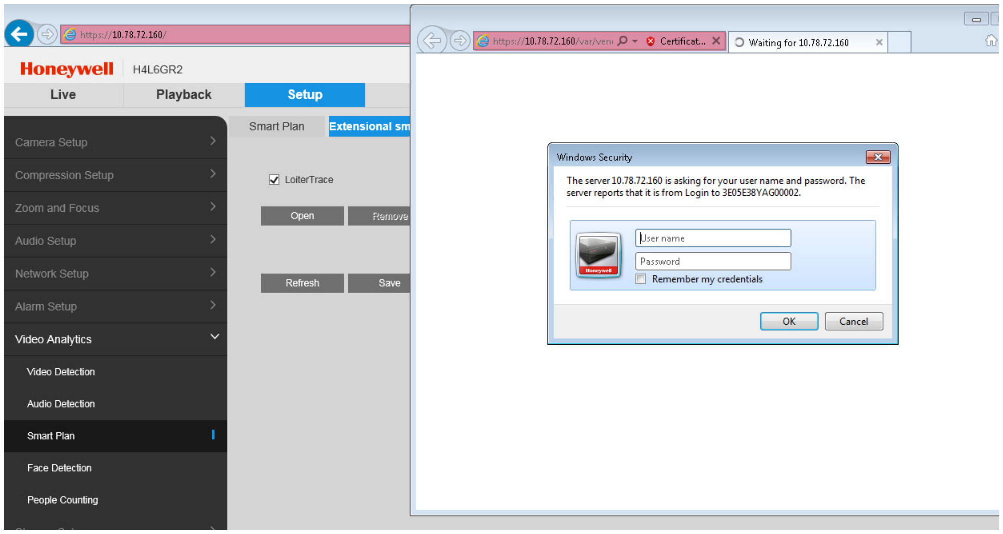
Step 3. Click the Extensional smart function tab to view the LoiterTrace alarms as shown below.



☑ LoiterTrace

Extensional smart function page

Step 4. Click Open. The Xtralis authentication window is displayed as shown below.

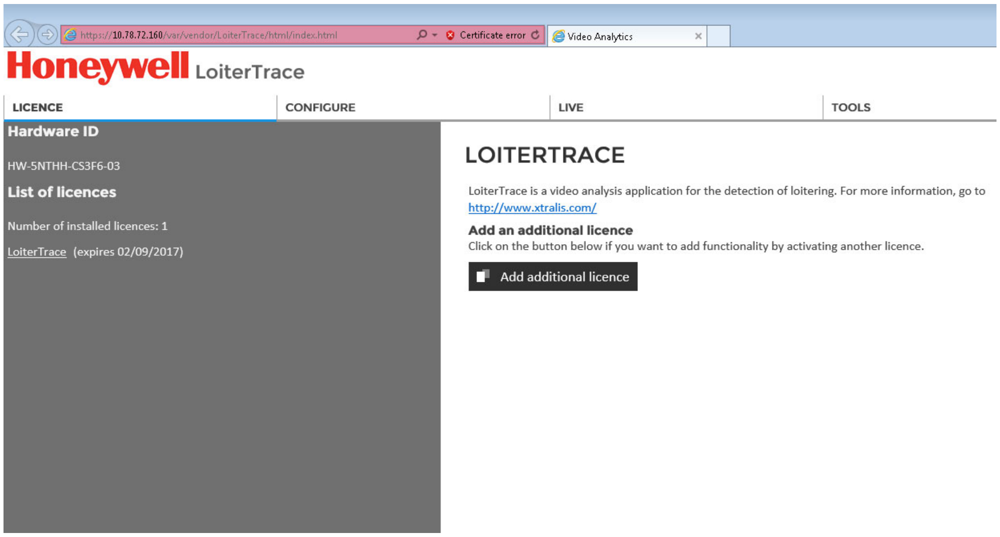


☑ LoiterTrace

The server 10.78.72.160 is asking for your user name and password. The server reports that it is from Login to 3E05E38YAG00002.

Xtralis Login

Step 5. Enter the credentials and then click OK. The LoiterTrace page is displayed as shown below.



Hardware ID

HW-5NTHH-CS3F6-03

List of licences

Number of installed licences: 1

LoiterTrace (expires 02/09/2017)

LOITERTRACE

LoiterTrace is a video analysis application for the detection of loitering. For more information, go to http://www.xtralis.com/

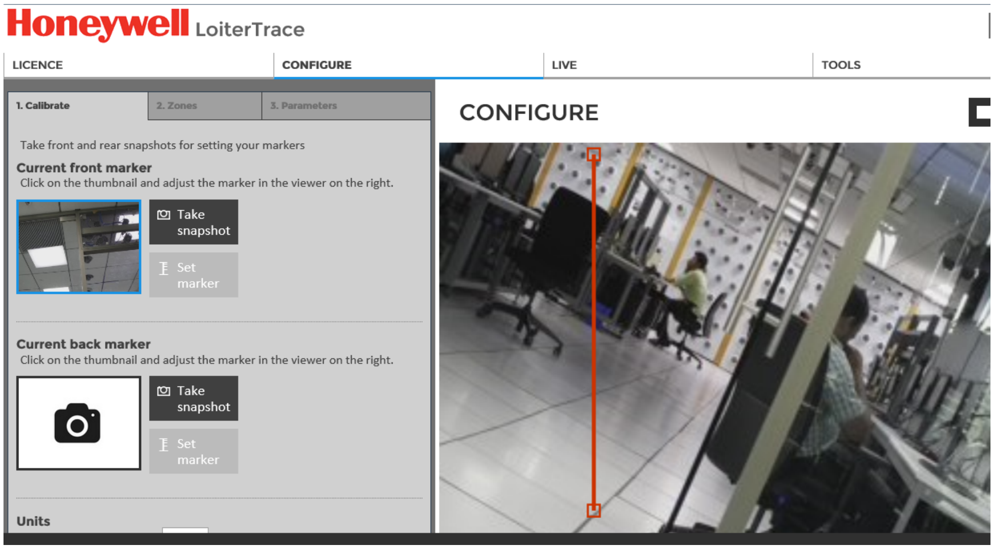
Add an additional licence

Click on the button below if you want to add functionality by activating another licence.

Loiter Trace Page

Step 6. Under Configure > Calibrate tab:

a. Click Take Snapshot under Current front marker to take the snapshot and adjust the viewer on the right pane as shown below.



Take front and rear snapshots for setting your markers

Current front marker

Click on the thumbnail and adjust the marker in the viewer on the right.

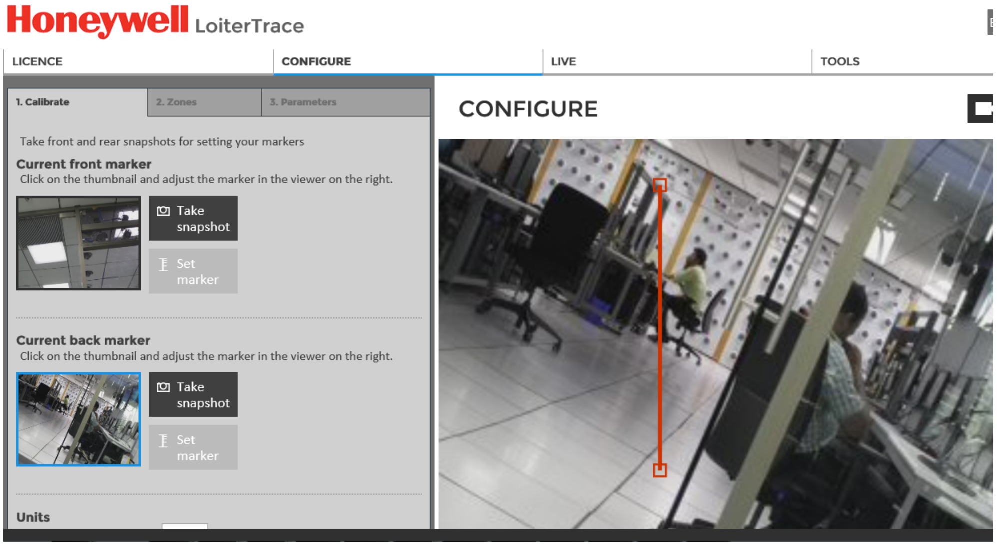
Current back marker

Click on the thumbnail and adjust the marker in the viewer on the right.

CONFIGURE

Loiter Trace Configuration

b. Click Take Snapshot under Current back marker to take the snapshot and adjust the viewer on the right pane as shown below



Take front and rear snapshots for setting your markers

Current front marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Current back marker

Click on the thumbnail and adjust the marker in the viewer on the right.

Loiter Trace - Calibrate

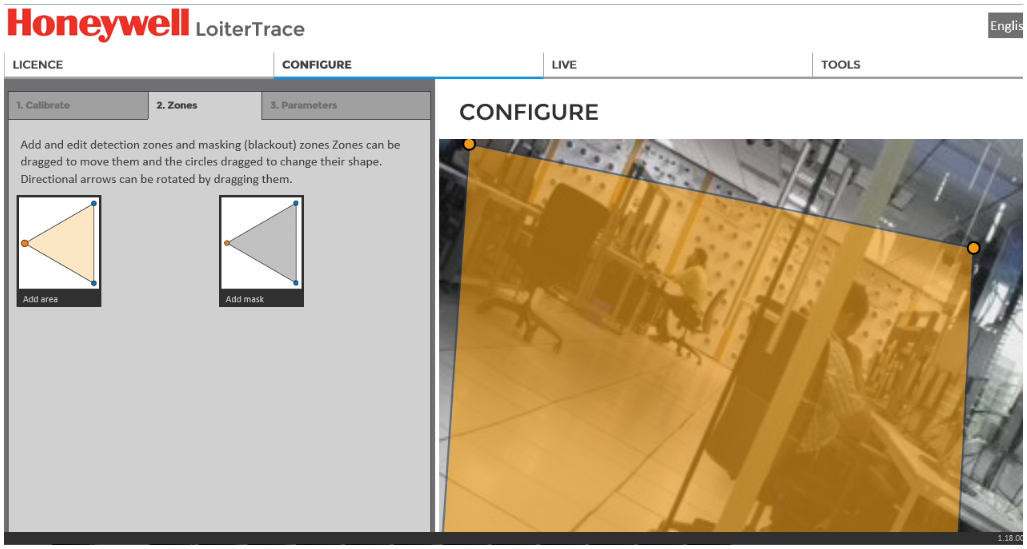
c. Click Save once done.

Step 1. Under Configure > Zones tab:

a. Add and edit the detection zones and masking zones.

b. Drag to move the zones and circles to change the shapes as shown below.

c. Click Save once done.

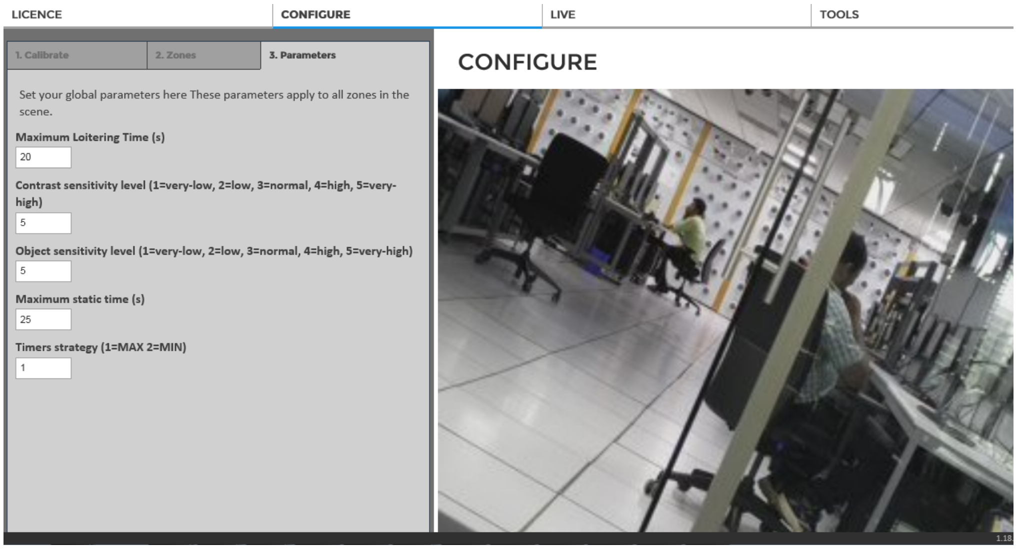


Add and edit detection zones and masking (blackout) zones Zones can be dragged to move them and the circles dragged to change their shape. Directional arrows can be rotated by dragging them.

Loiter Trace - Zones

Step 1. Under Configure > Parameters tab:

a. Set the global parameters as shown below.



Set your global parameters here These parameters apply to all zones in the scene.

Maximum Loitering Time (s)
20

Contrast sensitivity level (1=very-low, 2=low, 3=normal, 4=high, 5=very-high)
5

Object sensitivity level (1=very-low, 2=low, 3=normal, 4=high, 5=very-high)
5

Maximum static time (s)
25

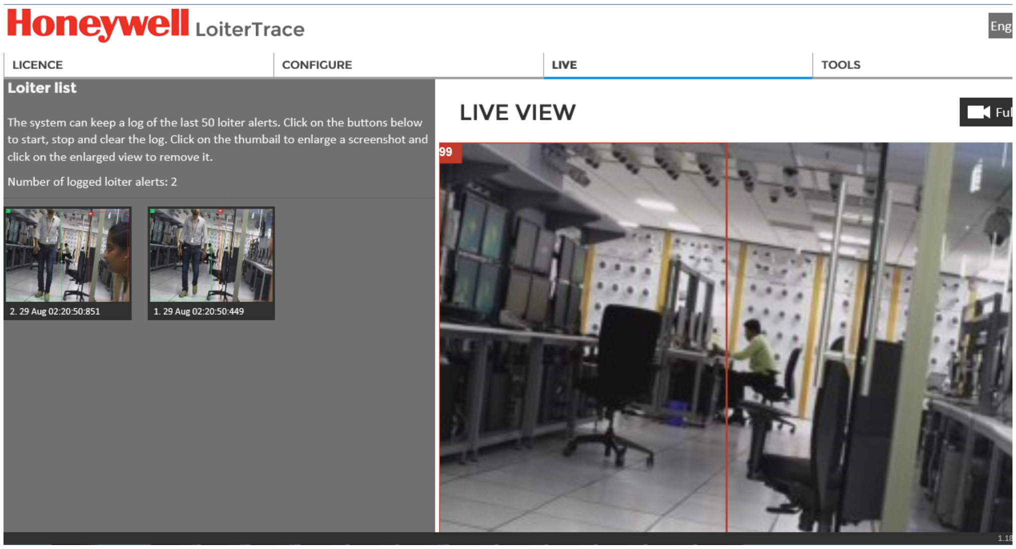
Timers strategy (1=MAX 2=MIN)
1

Loiter Trace - Parameters

b. Click Save once done.

Step 1. Once the configuration is done, click the Live tab. The Live View tab is displayed.

Step 2. Click Start Loiter Logging button at the bottom of page to start loitering process. Based on the global parameters set the loiter alarms are generated and displayed on the left pane as shown below. These alarms are also generated in MAXPRO NVR > Alarms window.
Similarly you can configure the Intrusion Trace Alarms.



Loiter list

The system can keep a log of the last 50 loiter alerts. Click on the buttons below to start, stop and clear the log. Click on the thumbail to enlarge a screenshot and click on the enlarged view to remove it.

Number of logged loiter alerts: 2

2. 29 Aug 02:20:50:851

1. 29 Aug 02:20:50:449

Loiter Trace - Live View Logs

MAXPRO®NVRs - AXIS Camera/Encoders Discovery and Configuration (using ONVIF)

This section describes the steps to discover and configure the AXIS Camera/ Encoders as an ONVIF device in MAXPRO NVRs.

If you have questions concerning this document, please contact Honeywell Technical Support. See the back cover for contact information.

Step 1: Enable ONVIF Web Service on AXIS Camera/Encoder

Scenario Description

If you are unable to discover AXIS cameras/encoders using ONVIF compliance standard in MAXPRO® NVR, ensure that ONVIF Web service is enabled and set up on the AXIS device.

The above scenario is noticed if you log on to the camera web page (for example to set the IP address on the AXIS device) prior to discovering and configuring the device in NVR through ONVIF; as a result the ONVIF Webservice gets disabled automatically.

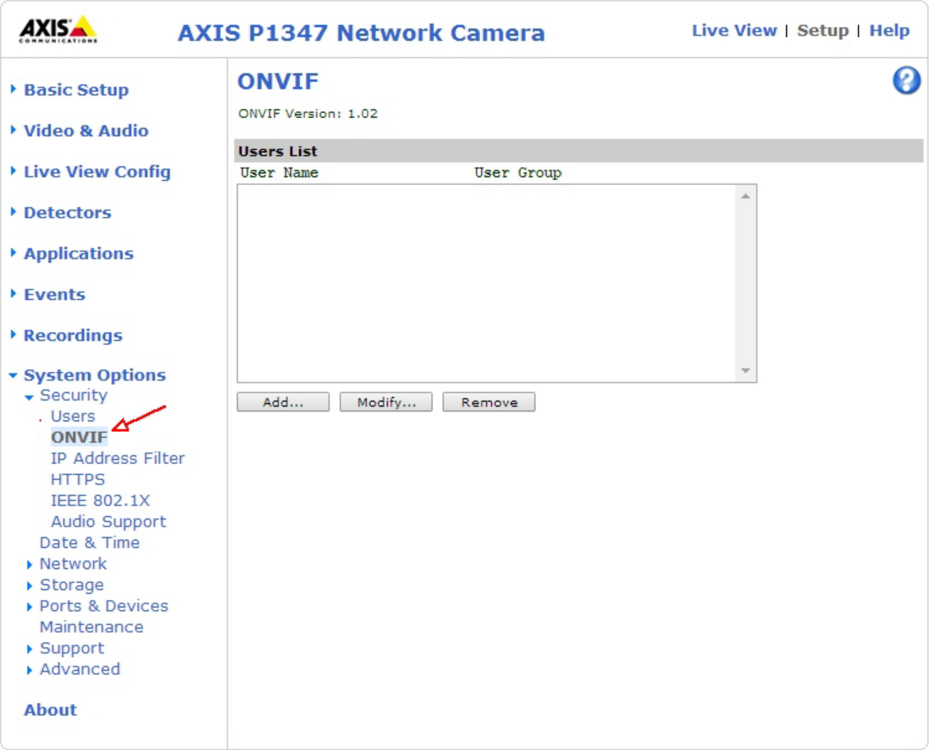
Perform the steps in ***Option 1: Add a ONVIF user in the camera web page.*** section on page ***426***. or ***Option 2: Reset to factory default settings*** section on page ***427*** to enable ONVIF on the AXIS devices.

Note: *AXIS P1347 Network Camera is used as an example to show the steps required. Perform similar steps for other AXIS ONVIF devices.*

Option 1: Add a ONVIF user in the camera web page.

Step 1. Log on to the AXIS camera web page. The AXIS camera home page appears with live video.

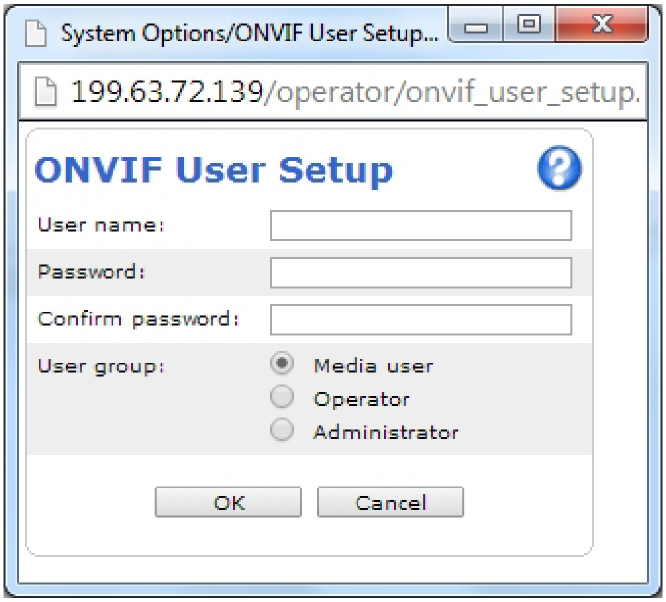
Step 2. Click Setup and then navigate to System Options > ONVIF. The User List dialog box appears.



ONVIF Version: 1.02

User List

Step 3. Click the Add button. The ONVIF User Setup dialog box appears (see *Figure*).


System Options/ONVIF User Setup...
199.63.72.139/operator/onvif_user_setup.
ONVIF User Setup
User name:
Password:
Confirm password:
OK
Cancel

User group: ● Media user ○ Operator ○ Administrator

ONVIF User Setup

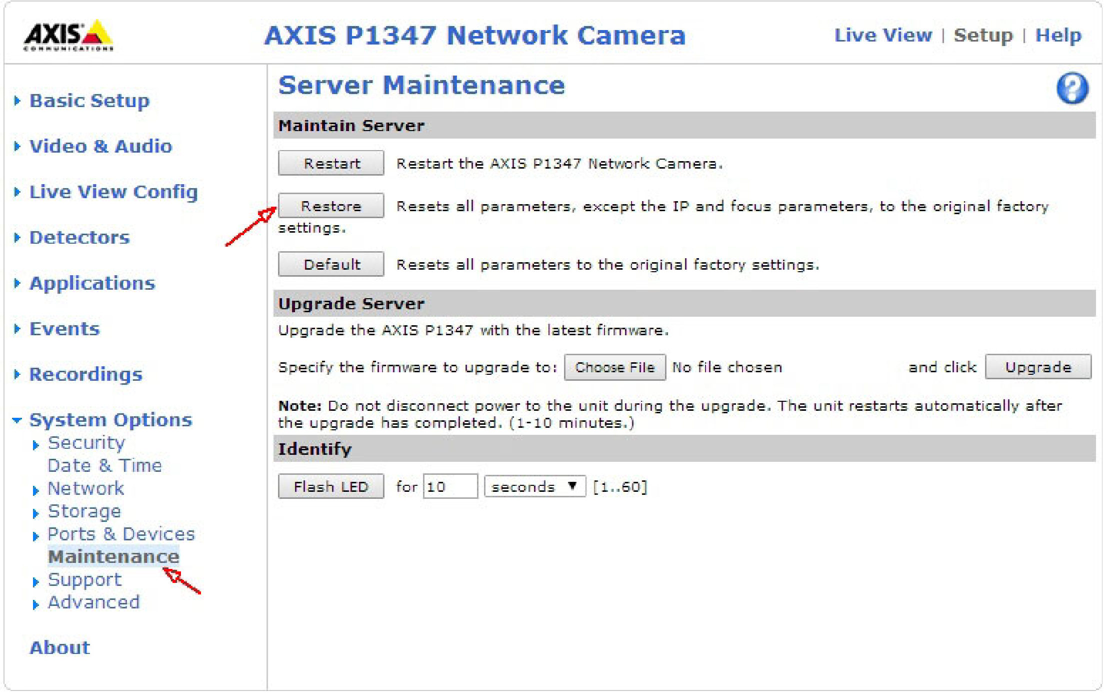
Step 4. Type the user name and password in the respective boxes.

Step 5. Confirm the password and then click OK. The newly added user is displayed in the User List box. Ensure that you enter the same User name and Password in MAXPRO® NVR Discovery (Advance Settings) dialog box.

Option 2: Reset to factory default settings

Step 1. Log on to the AXIS camera web page. The AXIS camera home page appears with live video.

Step 2. Click Setup and then navigate to System Options > Maintenance. The Server Maintenance page appears.



Server Maintenance

Maintain Server

Restart the AXIS P1347 Network Camera.

Resets all parameters, except the IP and focus parameters, to the original factory settings.

Resets all parameters to the original factory settings.

Upgrade Server

Upgrade the AXIS P1347 with the latest firmware.

Specify the firmware to upgrade to: No file chosen and click

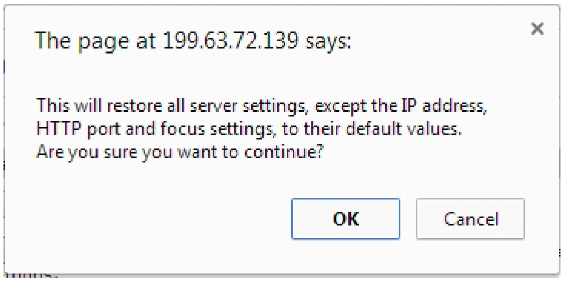
Note: Do not disconnect power to the unit during the upgrade. The unit restarts automatically after the upgrade has completed. (1-10 minutes.)

Identify

for 10 seconds [1..60]

Server Maintenance

Step 3. In the Maintain Server area, click Restore. A confirmation box appears.



The page at 199.63.72.139 says:

This will restore all server settings, except the IP address, HTTP port and focus settings, to their default values. Are you sure you want to continue?

Step 4. Click OK.

Note: *Restore operation resets all the parameters, except the IP and focus parameters, to the original factory settings.*

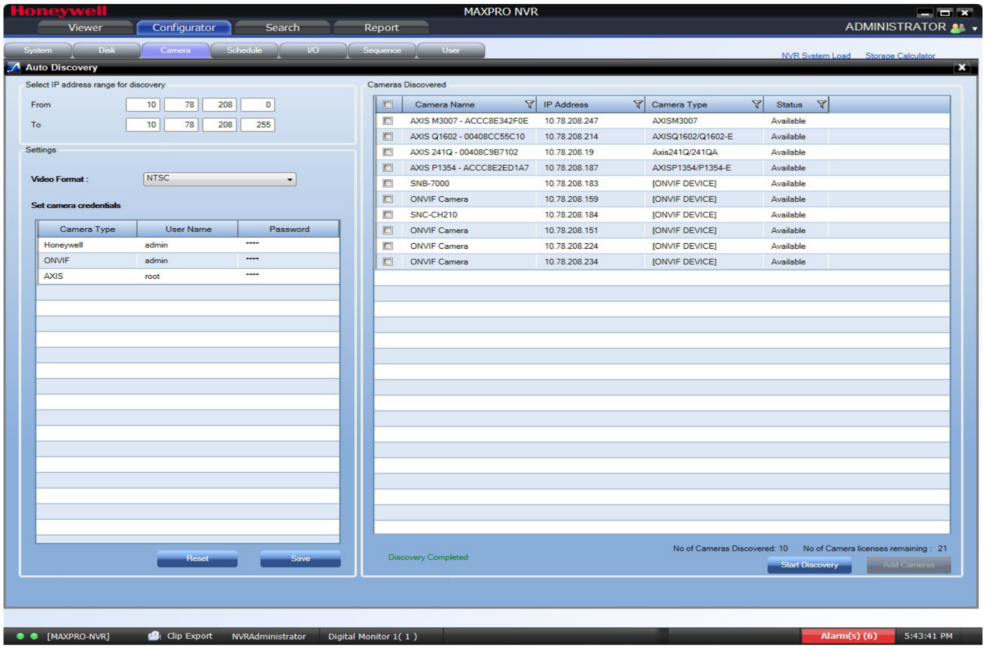
Step 5. Add and discover the AXIS camera in MAXPRO NVR using the default user name root and password pass.

Step 2: Discover and Configure the AXIS Camera/Encoder in MAXPRO® NVR

Step 1. In MAXPRO NVR, click the Configurator tab. The System page displays by default.

Step 2. Click the Camera tab to open the Camera page.

Step 3. Click the Auto Discovery button, the Auto Discovery screen is displayed.



Select IP address range for discovery

From	10	78	208	0
To	10	78	208	255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	----
ONVIF	admin	----
AXIS	root	----

Cameras Discovered

□	Camera Name	IP Address	Camera Type	Status
□	AXIS M3007 - ACCC8E342F0E	10.78.208.247	AXISM3007	Available
□	AXIS Q1602 - 00408CC55C10	10.78.208.214	AXISQ1602/Q1602-E	Available
□	AXIS 241Q - 00408C9B7102	10.78.208.19	Axis241Q/241QA	Available
□	AXIS P1354 - ACCC8E2ED1A7	10.78.208.187	AXISP1354/P1354-E	Available
□	SNB-7000	10.78.208.183	[ONVIF DEVICE]	Available
□	ONVIF Camera	10.78.208.159	[ONVIF DEVICE]	Available
□	SNC-CH210	10.78.208.184	[ONVIF DEVICE]	Available
□	ONVIF Camera	10.78.208.151	[ONVIF DEVICE]	Available
□	ONVIF Camera	10.78.208.224	[ONVIF DEVICE]	Available
□	ONVIF Camera	10.78.208.234	[ONVIF DEVICE]	Available

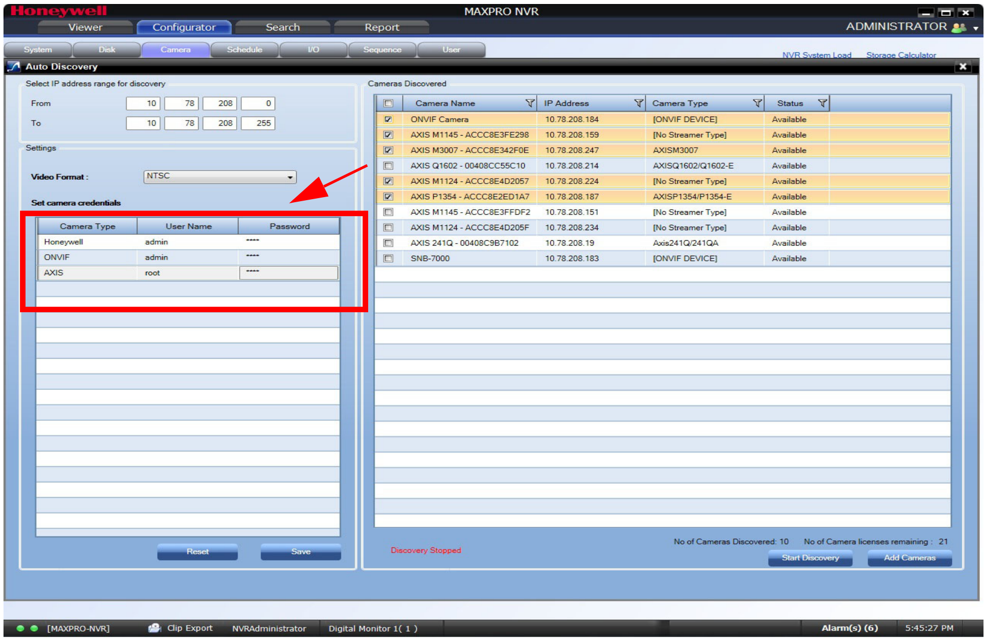
No of Cameras Discovered: 10 No of Camera licenses remaining : 21

Discovery Completed

Step 4. After the discovery, to add the AXIS cameras, first clear the check boxes corresponding to all other cameras other than AXIS cameras.

Step 5. Select a AXIS camera that you want to add under. type the User Name and Password of the third party AXIS camera as shown in the following figure.See the ***Configuring the Auto Discovery Settings*** section on page ***180*** for more information.

Note: *The default user name is root and password is pass.*



Select IP address range for discovery

From	10	78	208	0
To	10	78	208	255

Settings

Video Format : NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	----
ONVIF	admin	----
AXIS	root	----

Cameras Discovered

□	Camera Name	IP Address	Camera Type	Status
☑	ONVIF Camera	10.78.208.184	[ONVIF DEVICE]	Available
☑	AXIS M1145 - ACCC8E3FE298	10.78.208.159	[No Streamer Type]	Available
☑	AXIS M3007 - ACCC8E342F0E	10.78.208.247	AXISM3007	Available
□	AXIS Q1602 - 00408CC55C10	10.78.208.214	AXISQ1602/Q1602-E	Available
☑	AXIS M1124 - ACCC8E4D2057	10.78.208.224	[No Streamer Type]	Available
☑	AXIS P1354 - ACCC8E2ED1A7	10.78.208.187	AXISP1354/P1354-E	Available
□	AXIS M1145 - ACCC8E3FFDF2	10.78.208.151	[No Streamer Type]	Available
□	AXIS M1124 - ACCC8E4D205F	10.78.208.234	[No Streamer Type]	Available
□	AXIS 241Q - 00408C9B7102	10.78.208.19	Axis241Q/241QA	Available
□	SNB-7000	10.78.208.183	[ONVIF DEVICE]	Available

No of Cameras Discovered: 10 No of Camera licenses remaining : 21

Discovery Stopped

Axis Credentials

Step 6. Click Apply.

Step 7. In the Discover cameras here area, click Add to add the camera.

APPENDIX

C PATCHES RELEASED ON TOP OF NVR 4.0

Overview

This chapter lists the various patches that are released on top of MAXPRO NVR 4.0. It also explains the enhancements that you can experience after installing the specific patch.

In this chapter...

AXIS Patch

Patch Version: (Build 87H_T2 patch)

Installation: To be installed on top of MAXPRO NVR 4.0

Issues Fixed

The following are the issues fixed in this patch:

- AXIS camera stops responding after upgrading the firmware version to 6.30.1. This issues is fixed by providing AXIS new Firmware support 6.XXXX.
- Fixed the SMART VMD Issue: Recording is not in progress for the cameras which are configured only for motion based recording. However, motion based alarms are generated.

Skylake Patch

Patch Version: (NVR 4.0 SP1 Build 97)

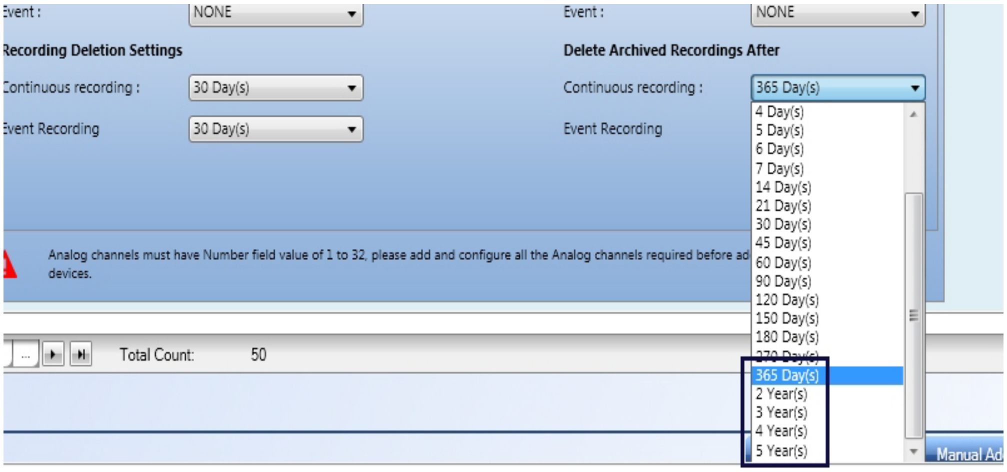
Installation: To be installed on top of MAXPRO NVR 4.0

Release Highlights:

This Patch includes the following enhancements:

Step 1. Supports Sky-Lake Processor

Step 2. For Archival under Delete Archived Recordings After > Continuous recording drop-down, new deletion schedules are implemented such as 2,3,4 and 5 years as highlighted below.



Event : NONE

Recording Deletion Settings

Continuous recording : 30 Day(s)

Event Recording 30 Day(s)

Event : NONE

Delete Archived Recordings After

Continuous recording : 365 Day(s)

Event Recording

Analog channels must have Number field value of 1 to 32, please add and configure all the Analog channels required before ad devices.

Total Count: 50

Step 3. Updated the Resolutions for Equip S2 series (HICC-2500MI, HIVDC-2500MI) cameras.

Step 4. Updated the Number of Streams [3 Streams] for Equip S2 series (HICC-2500MI, HIVDC-2500MI) cameras.

Step 5. Support for 15 Performance series camera s models.

Step 6. Limit for Rendering Camera can be increased in Registry. The default value is 20. See ***How to increase the Limit for Rendering Camera*** section for more information.

Issues Fixed

The following are the issues fixed in this patch:

Step 1. Sandy-Bridge Issue: Provided the support to disable the GPU Rendering feature from Preferences dialog box. See ***How to Disable the GPU Rendering*** section for more information.

Step 2. I18N: Fixed the issue: Values are not displaying in the Archival drop-down list in Polish language

Step 3. Fixed the Clip Player Day light Saving Time issue

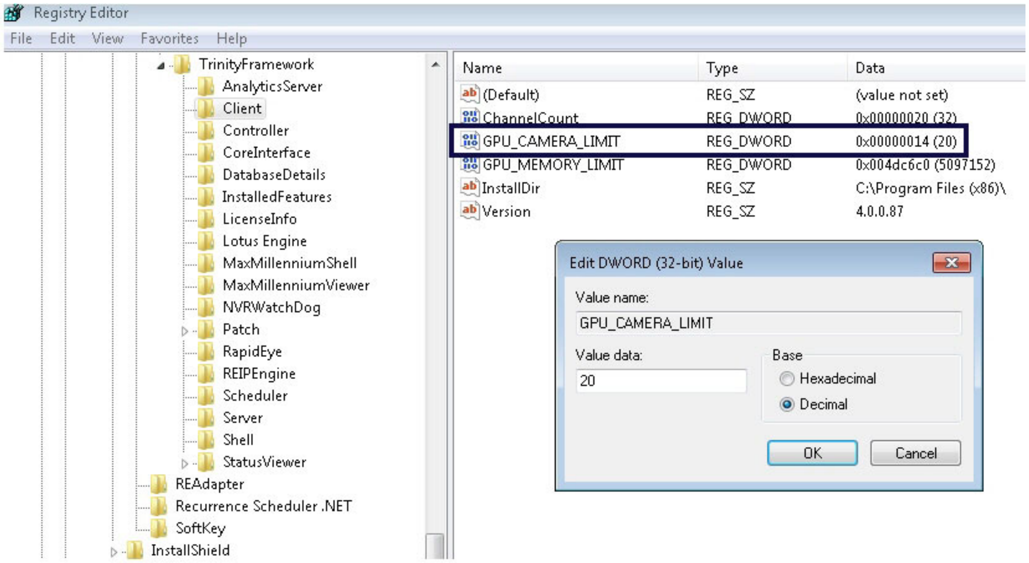
Step 4. T2 Patch changes - Axis v6.0 support and fixed the SVMD issue

Step 5. Fixed the Incorrect GPU driver installation and the cameras are not rendering issue.

How to increase the Limit for Rendering Camera

Step 1. Open the Registry Editor window.

Step 2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Honeywell\MaxproNVR\TrinityFramework\Client and then double-click GPU_CAMERA_LIMIT on the right pane. The Edit DWORD dialog box appears as shown below.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelCount	REG_DWORD	0x00000020 (32)
GPU_CAMERA_LIMIT	REG_DWORD	0x00000014 (20)
GPU_MEMORY_LIMIT	REG_DWORD	0x004dc6c0 (5097152)
InstallDir	REG_SZ	C:\Program Files (x86)\
Version	REG_SZ	4.0.0.87

Edit DWORD (32-bit) Value

Value name: GPU_CAMERA_LIMIT

Value data: 20

Base

○ Hexadecimal

● Decimal

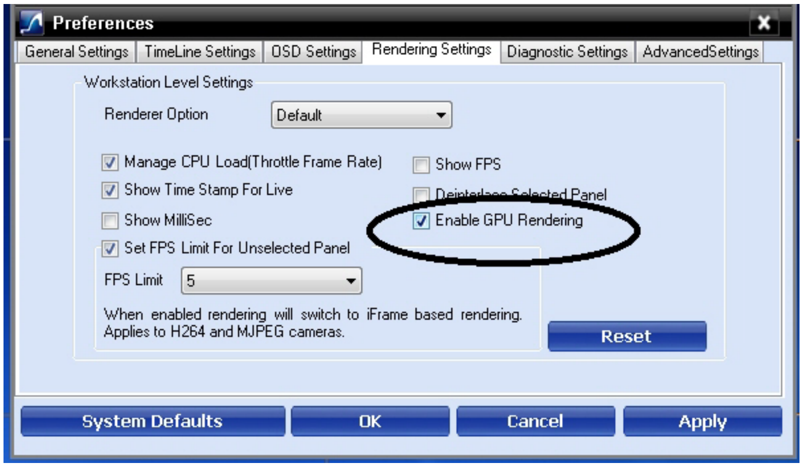
OK Cancel

Step 3. In the Value data field, modify the value based on your requirement and then click OK. The default value is 20.

How to Disable the GPU Rendering

Step 1. Click the Preferences option in the user menu. The Preferences dialog box is displayed. By default, the General Settings tab is selected.

Step 2. Click the Rendering Settings tab as shown below.



Renderer Option: Default

☑ Manage CPU Load(Throttle Frame Rate)

☑ Show Time Stamp For Live

□ Show MilliSec

☑ Set FPS Limit For Unselected Panel

FPS Limit: 5

When enabled rendering will switch to iFrame based rendering. Applies to H264 and MJPEG cameras.

□ Show FPS

□ Deinterlace Selected Panel

☑ Enable GPU Rendering

Step 3. Select the Enable GPU Rendering check box to enable and to render video using GPU.
OR
Clear the Enable GPU Rendering check box to disable GPU Rendering.

INDEX

Honeywell Building Technologies - Security Americas (Head Office)

Honeywell Commercial Security
715 Peachtree St. NE
Atlanta, GA 30308
www.security.honeywell.com/
☎ +1 800 323 4576

Honeywell Building Technologies - Security Mexico

Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,
CP 0121, CDMX, Mexico.
Colombia: Edificio Punto 99, Carrera 11a.
98-50, Piso 7, Bogota, Colombia.
clarsupport@honeywell.com
☎ 01.800.083.59.25
www.honeywell.com

Honeywell Colombia SAS

Carrera 11A # 98-50
Edificio Punto 99, Piso 7, Bogotá DC
Colombia

Honeywell Building Technologies – Security Middle East/N. Africa

Emaar Business Park, Sheikh Zayed Road
Building No. 2, 2nd floor, 201
Post Office Box 232362
Dubai, United Arab Emirates
☎: +971 44541704
www.honeywell.com/security/me

Honeywell Building Technologies – Security Europe/South Africa

Aston Fields Road, Whitehouse Industrial Estate
Runcorn, WA7 3DL,
United Kingdom
www.honeywell.com/security/uk
☎ 08448 000 235

Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961,
1117 CE Schiphol-Oost, Netherlands
www.security.honeywell.com/nl
☎ +31 (0) 299 410 200

Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14 72458 Albstadt, Germany
www.security.honeywell.de
☎ +49 (0) 7431 801-0

Honeywell Building Technologies – Security France

Immeuble Lavoisier
Parc de Haute Technologie 3-7 rue Georges Besse 92160 Antony, France
www.security.honeywell.com/fr
☎ +33 (0) 1 40 96 20 50

Honeywell Building Technologies – Security & Fire (Pacific)

Honeywell Ltd. 9 Columbia Way, BAULKHAM HILLS NSW 2153
Visit: www.honeywellsecurity.com.au, Email: hsf.comms.pacific@Honeywell.com
☎ Tech Support: Australia: 1300 220 345, New Zealand: +64 9 623 5050

Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22, 20097 San Donato Milanese (MI), ITALY
www.security.honeywell.com/it

Honeywell Commercial Security - España

Josefa Valcárcel, 24
28027 - Madrid
España
www.honeywell.com
☎ +34 902 667 800

Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow, UI, Kiev 7 Russia
www.security.honeywell.com/ru
☎ +7 (495) 797-93-71

Honeywell Building Technologies – Security Asia Pacific

Building #1, 555 Huanke Road,
Zhang Jiang Hi-Tech Park Pudong New Area,
Shanghai, 201203, China
www.asia.security.honeywell.com
☎ 400 840 2233

Honeywell Building Technologies – Security and Fire (ASEAN)

Honeywell International Sdn Bhd
Level 25, UOA Corp Tower, Lobby B
Avenue 10, The Vertical, Bangsar South City
59200, Kuala Lumpur, Malaysia
Visit Partner Connect: www.partnerconnect.honeywell.com
Email: buildings.asean@honeywell.com

Technical support (Small & Medium Business):

Vietnam:☎ +84 4 4458 3369
Thailand:☎ +66 2 0182439
Indonesia:☎ +62 21 2188 9000
Malaysia:☎ +60 3 7624 1530
Singapore:☎ +65 3158 6830
Philippines:☎ +63 2 231 3380

Honeywell Home and Building Technologies (India)

HBT India Buildings
Unitech Trade Centre, 5th Floor,
Sector – 43, Block C, Sushant Lok Phase – 1,
Gurgaon – 122002, Haryana, India
Visit Partner Connect: www.partnerconnect.honeywell.com
Email: HBT-IndiaBuildings@honeywell.com
Toll Free No: 1-800-103-0339
☎ +91 124 4975000

Honeywell Building Technologies – Security and Fire (Korea)

Honeywell Co., Ltd. (Korea)
5F SangAm IT Tower,
434, Worldcup Buk-ro, Mapo-gu,
Seoul 03922, Korea
Visit: http://www.honeywell.com
Email: info.security@honeywell.com
Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779
☎ +82-2-799-6114

Honeywell | THE FUTURE IS WHAT WE MAKE IT

Document: 800-26013-C - MAXPRO®NVR 6.7 Installation and Configuration Guide – 2/2021

www.honeywell.com/security
+1 800 323 4576 (North America only)
https//honeywellsystems.com/ss/techsupp/index.html

www.honeywell.com/security/uk
+44 (0) 1928 754 028 (Europe only)
https//honeywellsystems.com/ss/techsupp/index.html