Honeywell

THE POWER OF **CONNECTED**

MAXPRO® NVR 4.5

Installation and Configuration Guide

This page is intentionally left blank.

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 30	Updated document for 4.5 Release

This page is intentionally left blank.

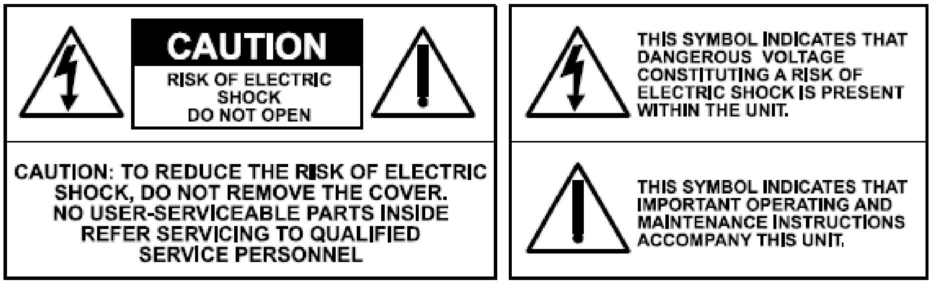
Table of Contents

This page is intentionally left blank

List of Figures

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.

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.

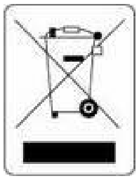
In the event you have a problem with any Honeywell product, please call Technical Support at 1-800-323-4576 (North America only) for assistance or to request a **Return Merchandise Authorization (RMA)** number.

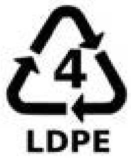
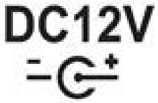
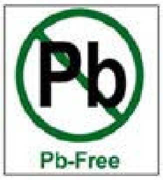
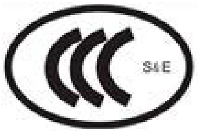
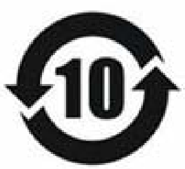
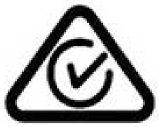
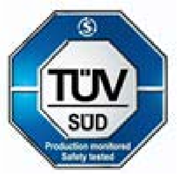
Be sure to have the model number, serial number, and the nature of the problem available for the technical service representative.

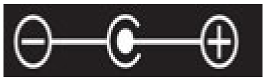
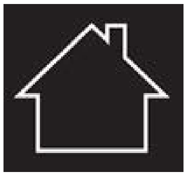
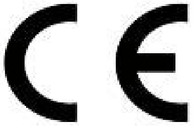
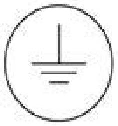
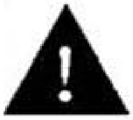
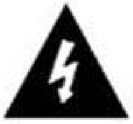
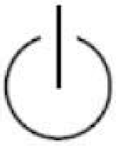
Prior authorization must be obtained for all returns, exchanges, or credits. **Items shipped to Honeywell without a clearly identified Return Merchandise Authorization (RMA) number may be refused.**

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.
	The LDPE symbol. This symbol indicates that this product is made of Low-Density Polyethylene (LDPE).
	The Direct Current symbol. This symbol indicates that the product operates from a 12 V direct current.
	The Lead-free symbol. This symbol indicates that the product does not contain lead (Pb).
	The CCC compliance logo. This logo indicates that the product conforms with the China Compulsory Certification guidelines.
	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.
	The TUV Lab symbol. This symbol indicates that the product has been safety tested by the TUV Lab.

Symbol	Explanation
	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.

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
- Configuring MAXPRO NVR
- Configuring Web Client
- Installing and Configuring MAXPRO NVR Mobile App
- Securing MAXPRO NVR

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.

No	Chapter	Description
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	MAXPRO NVR Web Client	Describes the procedures to install and configure the MAXPRO NVR Web Client.
9	MAXPRO NVR Mobile App	Describes the procedures to install and configure the MAXPRO NVR Mobile App.
10	Securing MAXPRO NVR	Describes the mandatory security settings that needs to be performed on MAXPRO NVR.
11	Appendix A	Describes the procedures to customize MAXPRO NVR Single-box Turnkey solutions and setting up the Antivirus software on MAXPRO NVRs.
12	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).

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	800-16422V5-A	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
Swiss721 BT	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.

Font	What it represents	Example
	Heading	**Installation**
Italic	Cross-reference to external source	Refer to the ***System Administrator Guide.***
	Cross-reference within document	See Installation.

This page is intentionally left blank

1

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 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 or 64 channels while allowing for up to 64 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**
Description	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 64	4, 8, 16, 32 or 64
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 - 12 TB, internal fixed	1 - 24 TB removable bays	Up to 48 TB RAID 5/6, removable bays	1 - 12 TB internal fixed	1 - 36 TB, removable bays	Up to 48 TB 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.

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.

.

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 processors. This feature allows a user to render high resolution cameras while optimizing the CPU consumption.

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 the 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 synched 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 Changing the Registry value for On Demand live streaming and How to Enable Video on demand feature in MAXPRO NVR section for more information.

Profile-G or Edge Syn 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 Mercury model cameras.

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.

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.

MAXPRO NVR Typical System Architecture

MAXPRO NVR Standalone System Diagram

The following figure illustrates the MAXPRO NVR SE system architecture.

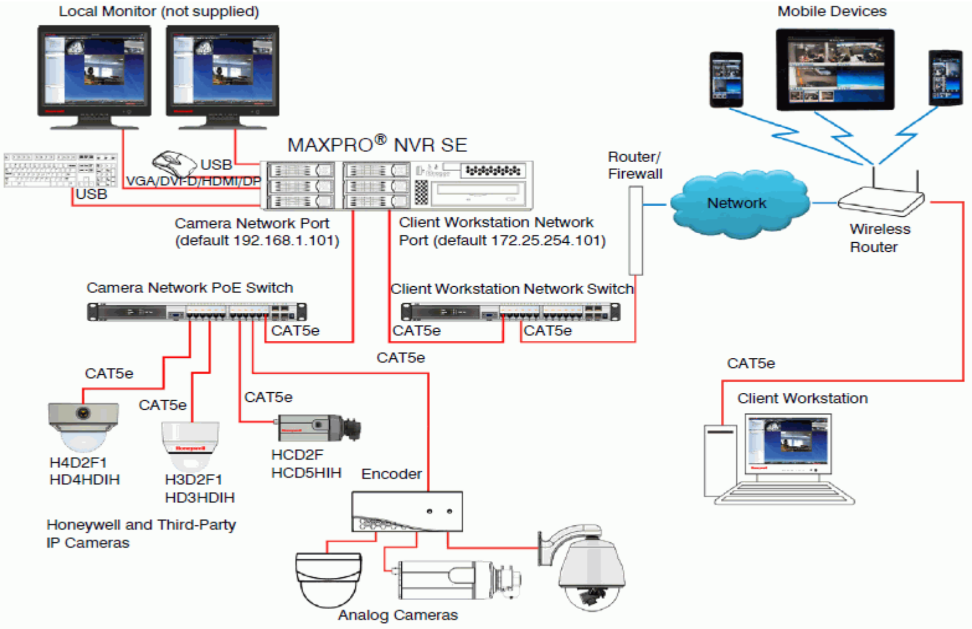


Figure 1-1 MAXPRO NVR SE System Diagram

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.

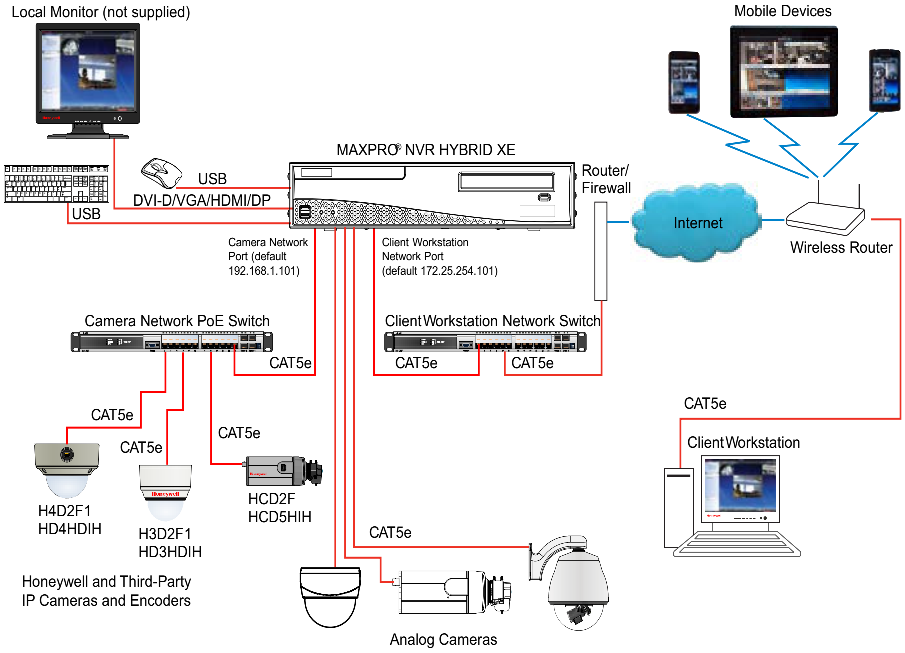


Figure 1-2 MAXPRO NVR HYBRID XE Standalone System Architecture

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.

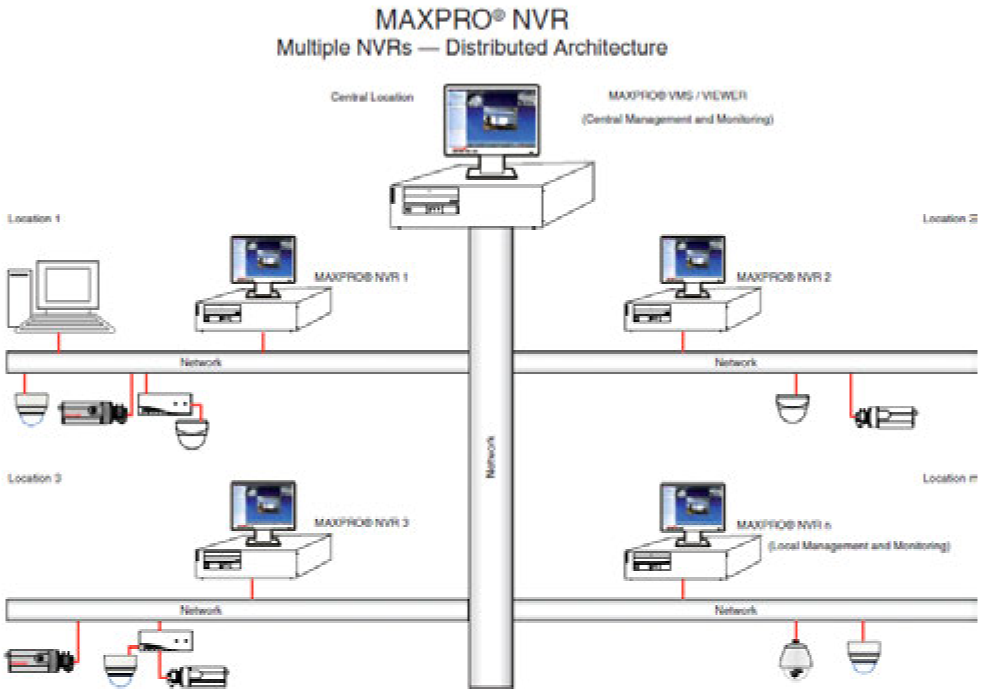


Figure 1-3 MAXPRO NVR Distributed System Architecture

This page is intentionally left blank

2

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 39 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 44 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:

1. The server and client computers meet the minimum hardware and software requirements.
2. Installing the MAXPRO NVR software.

See the MAXPRO NVR Software Installation section on page 58 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 Configuring MAXPRO NVR section on page 111 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 183 for information on how to perform the verification.

3

SETTING UP THE MAXPRO NVR

Chapter 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 39.
- For setting up the MAXPRO NVR Software-Only solution, see the Setting up the MAXPRO NVR Software-Only Solution section on page 44.
- For setting up a peripheral Joystick Controller, see the Connecting the Joystick Controller section on page 54.

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.

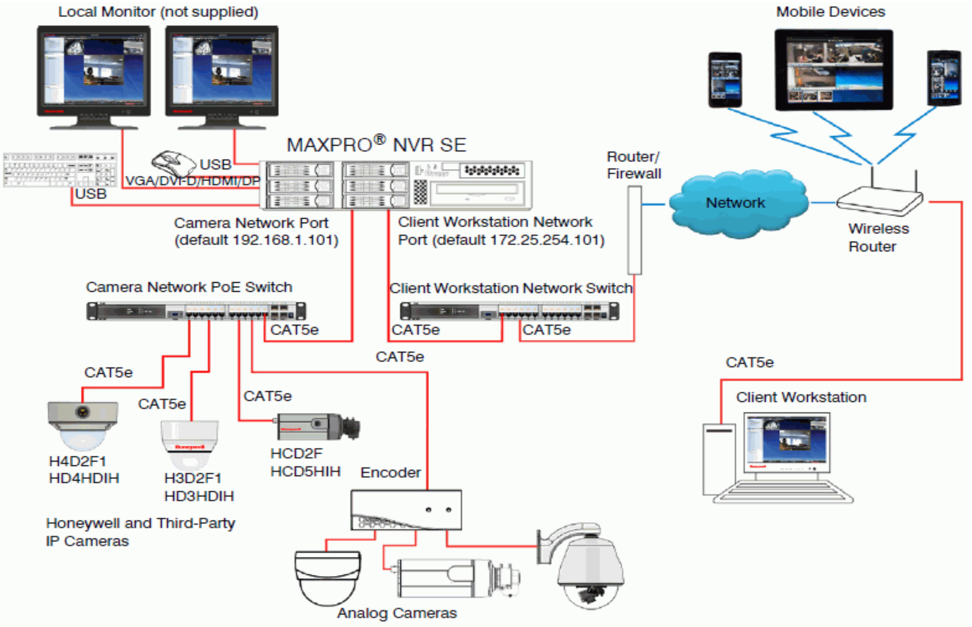


Figure 3-1 Typical MAXPRO NVR System Diagram

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.

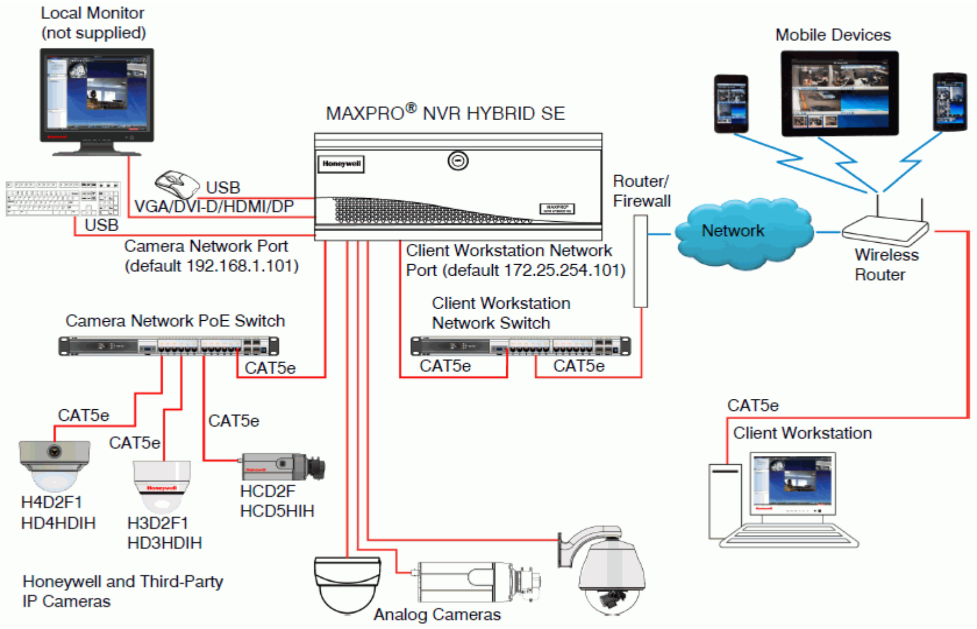


Figure 3-2 Typical MAXPRO NVR Hybrid System Diagram

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 46 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.honeywellvideo.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

1. Turn on camera(s) and other hardware connected to the MAXPRO NVR unit.
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.
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 225 for more information.

To turn off the power for MAXPRO NVR

1. Close the MAXPRO NVR application.
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

1. Click the network icon in the notification area, click **Open Network and Sharing Center** (See Figure 3-3), and then click **Change adapter settings**.

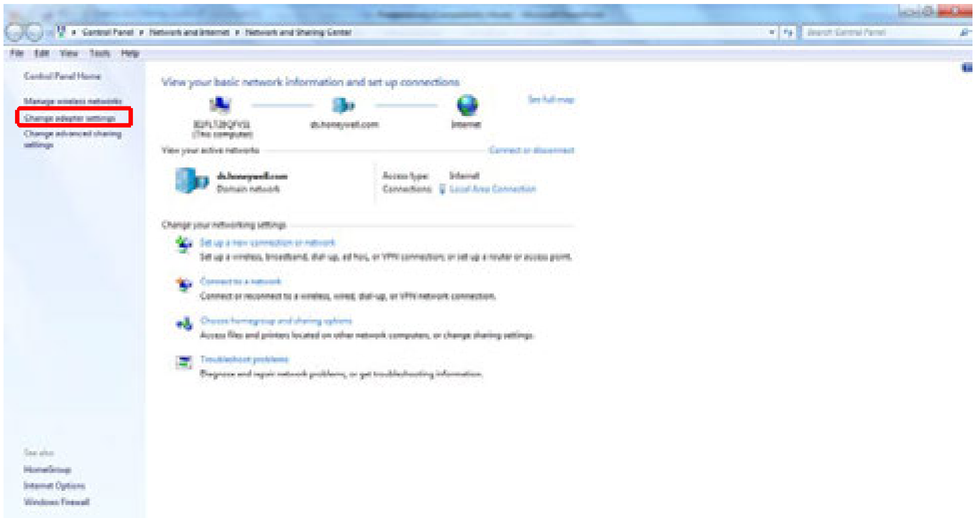
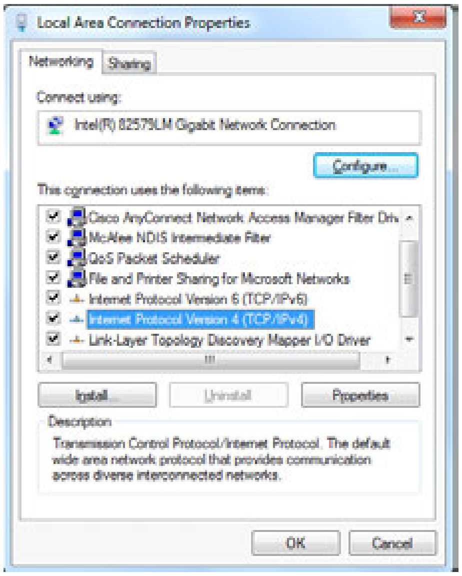

Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
(This computer)
Internet
View your active networks
Connect or disconnect
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.
See also
HomeGroup
Internet Options
Windows Firewall

Figure 3-3 Network and Sharing Center

2. Right-click **Camera Network** or **Client Workstation Network**, and then click **Properties**. The **Local Area Connection Properties** dialog box (Similar to Figure 3-4) 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.

Figure 3-4 LAN Properties

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

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

1. Click **Start**, right-click **Computer**, and then click **Properties**. The **System** window appears.
2. Click **Advanced system settings**. The **System Properties** dialog box appears.
3. Click the **Computer Name** tab, and then click **Change...**
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: < >;: " * + = \ | ?.
5. After changing the computer name, you are prompted to restart the computer.
6. Navigate to the **C:\Program Files\Honeywell\MaxproNVR\TrinityFramework\bin** folder, and then double-click **MaxProNVRMachineNameUtility.exe** to open the Maxpro NVR Utility.
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

1. Right-click on the Windows desktop and select **Screen resolution**.
2. Select the appropriate **Resolution**.
3. Click **OK** to save the setting and close the dialog box.

Configuring Display Setting from the Control Panel

1. Click **Start** > **Control Panel**, to open the Windows control panel screen.
2. Under **Appearance and Personalization**, click **Adjust screen resolution**.
3. Select the appropriate **Resolution**.
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.

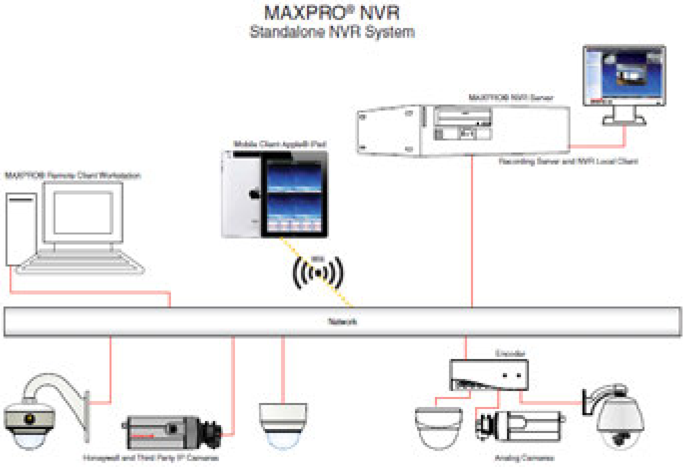

MAXPRO® NVR
Standalone NVR System
MAXPRO® NVR Server
Recording Server and NVR Local Client
Mobile Client Apple® iPad
MAXPRO® Remote Client Workstation
Network
Encoder
Honeywell and Third Party IP Cameras
Analog Cameras

Figure 3-5 MAXPRO NVR Software Solution Standalone System

MAXPRO NVR Software Solution Distributed System

The following figure illustrates the MAXPRO NVR Distributed system.

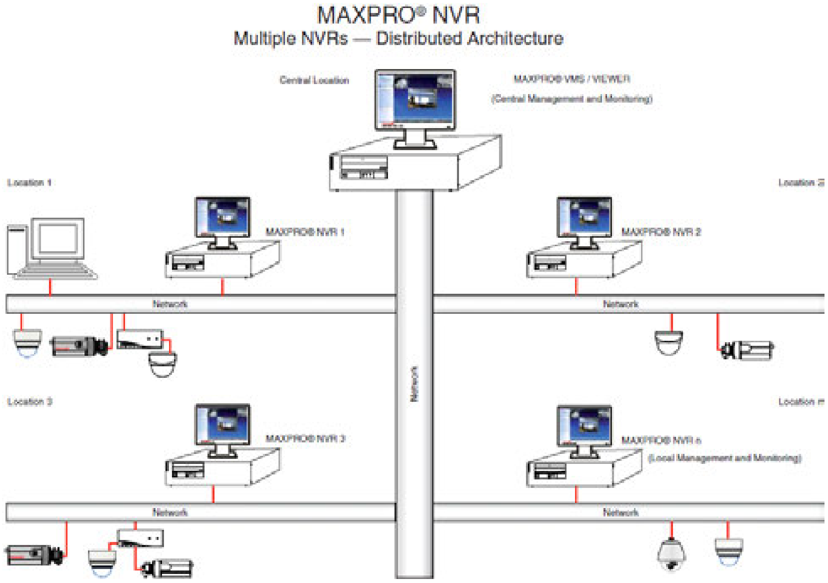


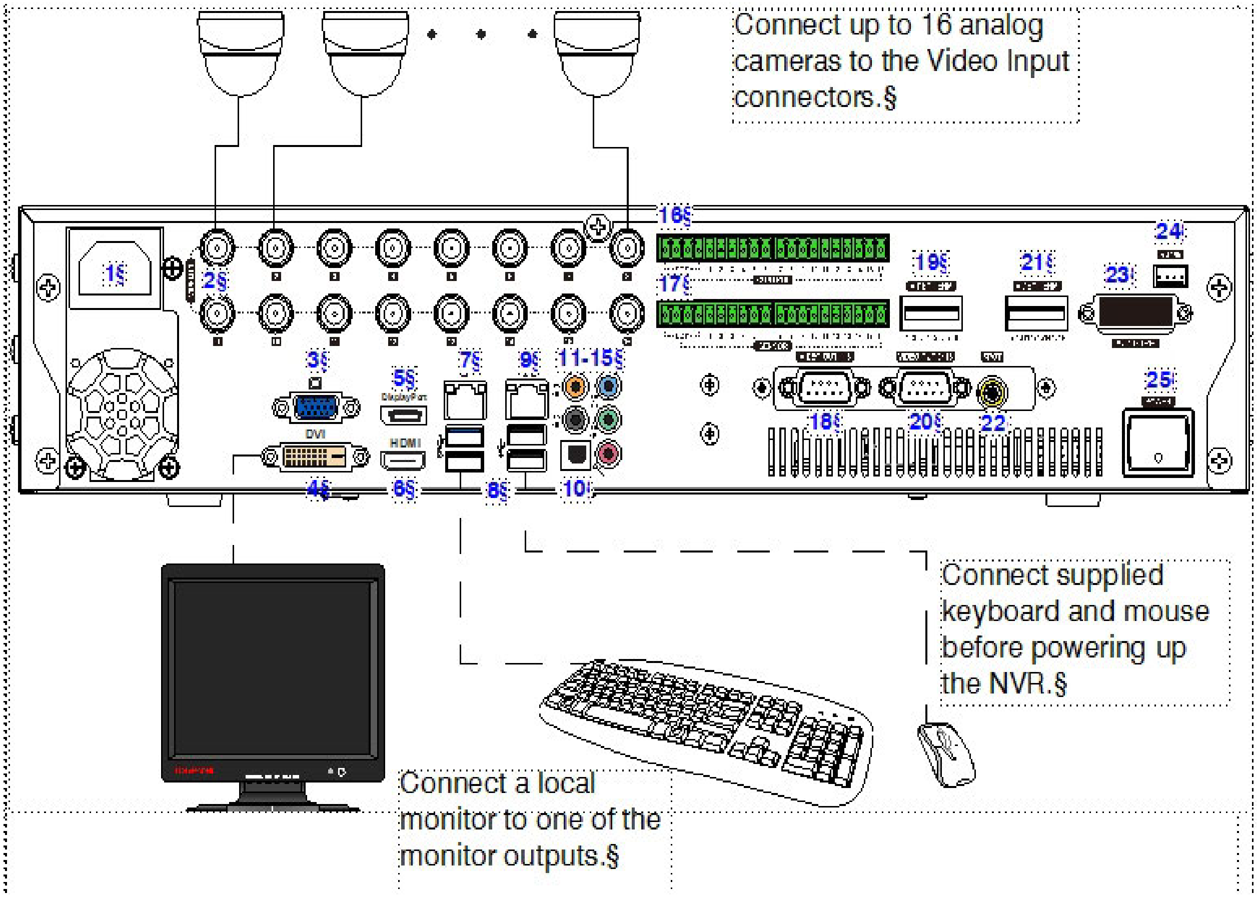
Figure 3-6   MAXPRO NVR Software Solution Distributed System

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.

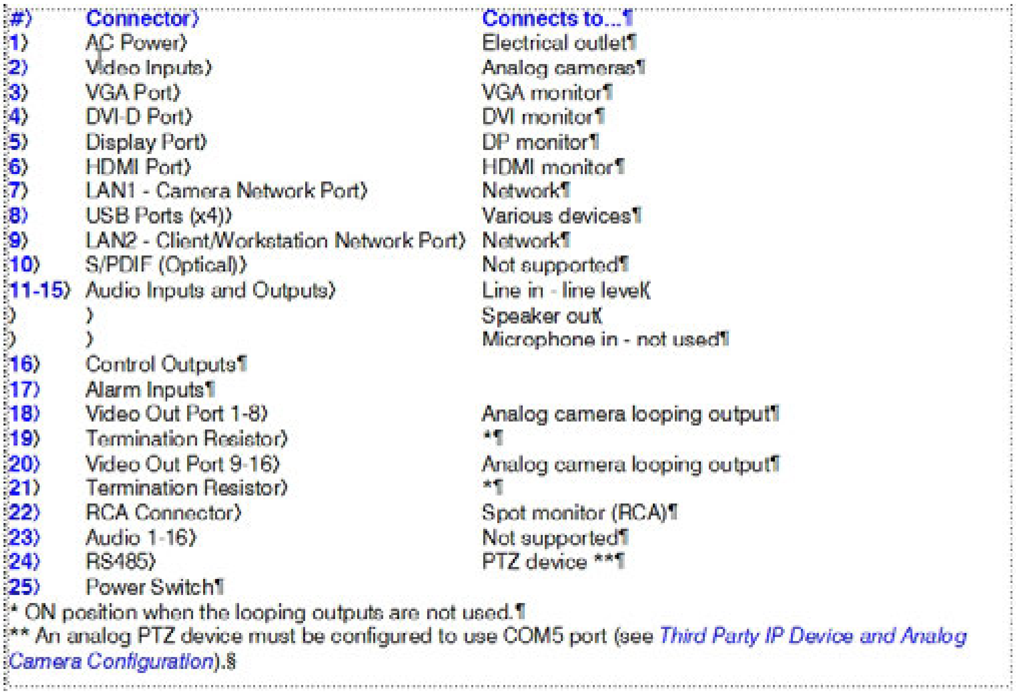
Hybrid XE Connections



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

Connect supplied keyboard and mouse before powering up the NVR.

Connect a local monitor to one of the monitor outputs.



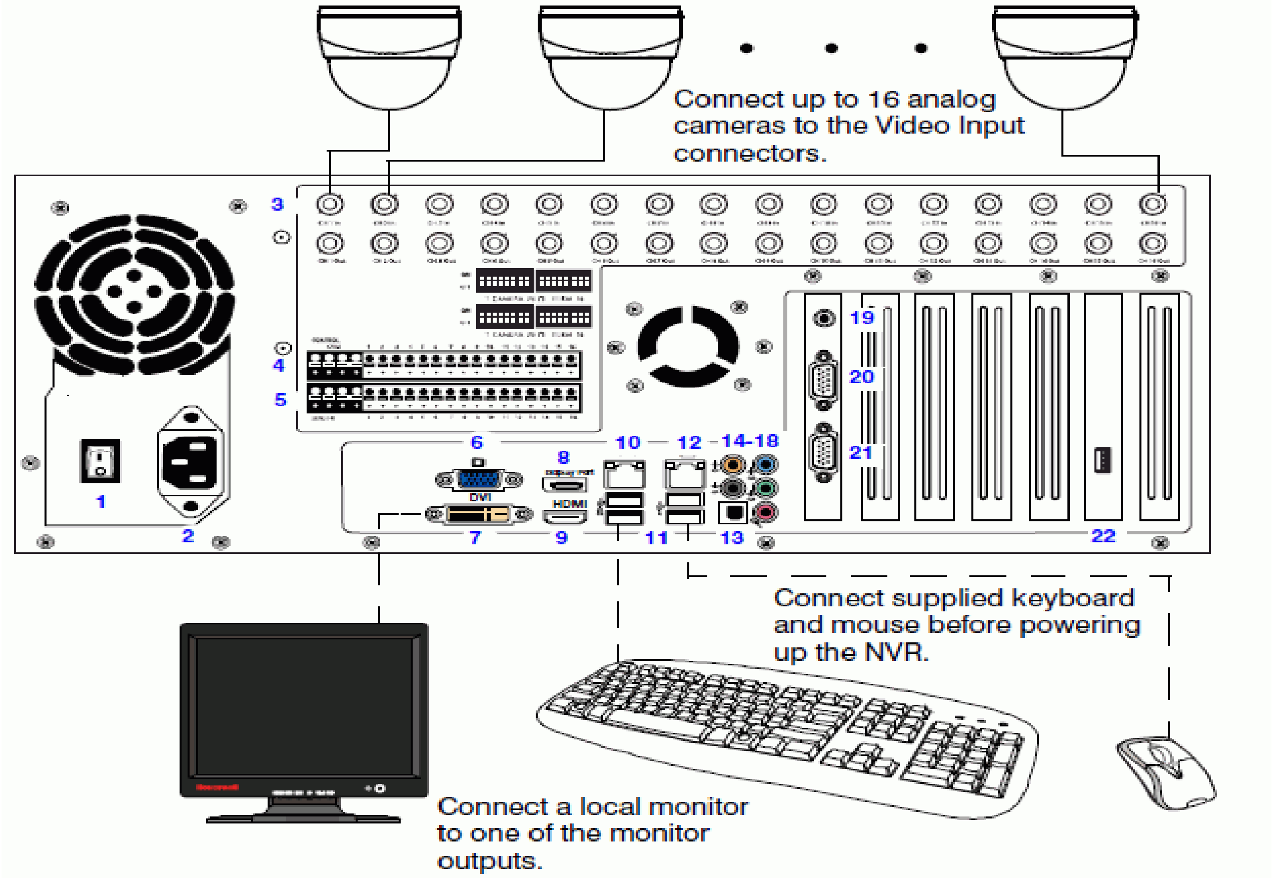
#	Connector	Connects to...
1	AC Power	Electrical outlet
2	Video Inputs	Analog cameras
3	VGA Port	VGA monitor
4	DVI-D Port	DVI monitor
5	Display Port	DP monitor
6	HDMI Port	HDMI monitor
7	LAN1 - Camera Network Port	Network
8	USB Ports (x4)	Various devices
9	LAN2 - Client/Workstation Network Port	Network
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*).

Figure 3-7 Hybrid XE Connections

Hybrid SE Connections



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

Connect supplied keyboard and mouse before powering up the NVR.

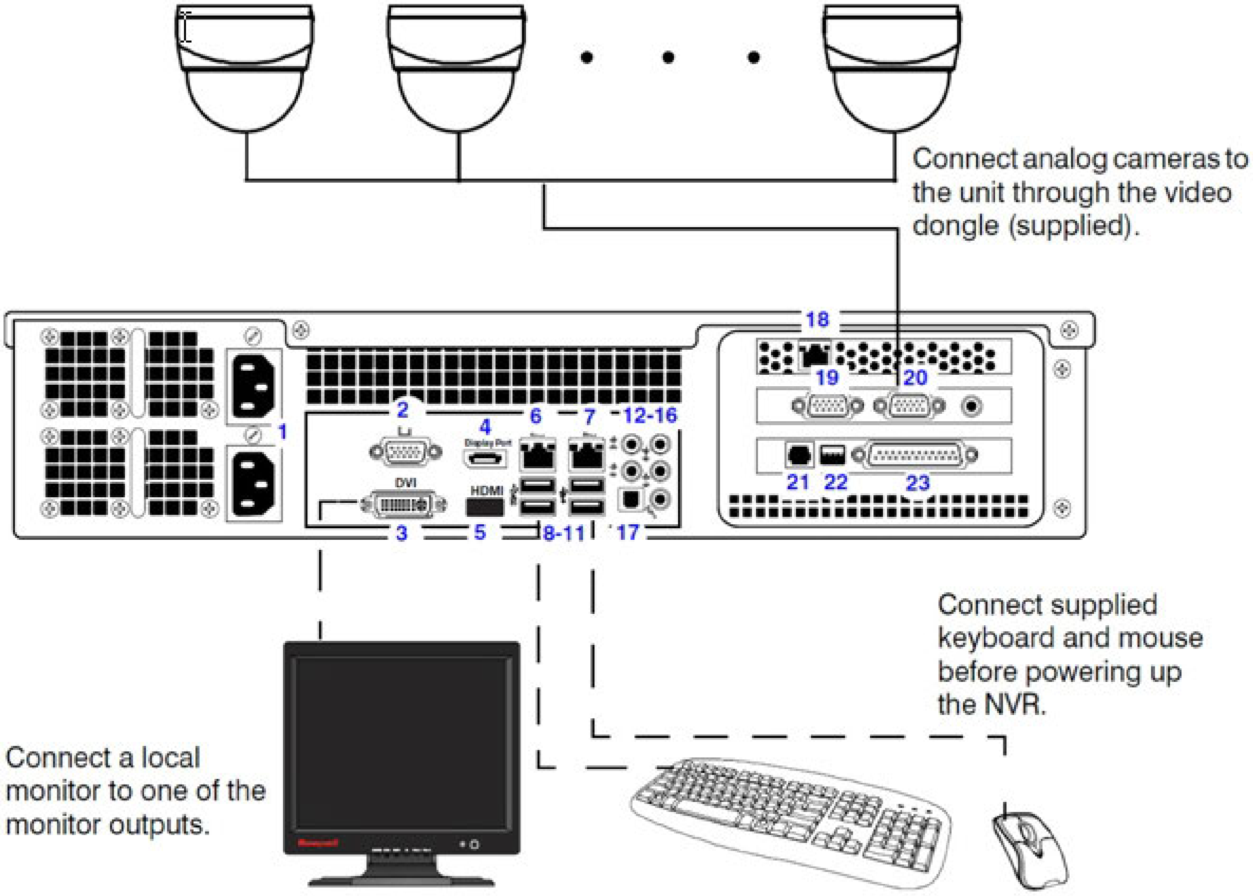
Connect a local monitor to one of the monitor outputs.

#	Connector	Connects to...
1	Power Switch	
2	AC Power	Electrical outlet
3	Video Inputs, Outputs (BNC)	Analog cameras
4	Control Outputs	
5	Alarm Inputs	
6	VGA Port	VGA monitor
7	DVI-D Port	Monitor
8	Display Port	Monitor
9	HDMI Port	HDMI monitor
10	LAN1 - Camera Network Port	Network
11	USB Ports (x4)	Various devices
12	LAN2 - Client/Workstation Network Port	Network
13	S/PDIF (Optical)	Not supported
14-18	Audio Inputs and Outputs	Line in - line level Speaker out Microphone in - not used
19	RCA Connector	Sport monitor (RCA)
20	Video Out Port 1–8	Analog camera looping output
21	Video Out Port 9–16	Analog camera looping output
22	RS485	PTZ device *

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

Figure 3-8 Hybrid SE Connections

Hybrid PE Connections



Connect analog cameras to the unit through the video dongle (supplied).

Connect supplied keyboard and mouse before powering up the NVR.

Connect a local monitor to one of the monitor outputs.

#	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*).

Figure 3-9 Hybrid PE Connections

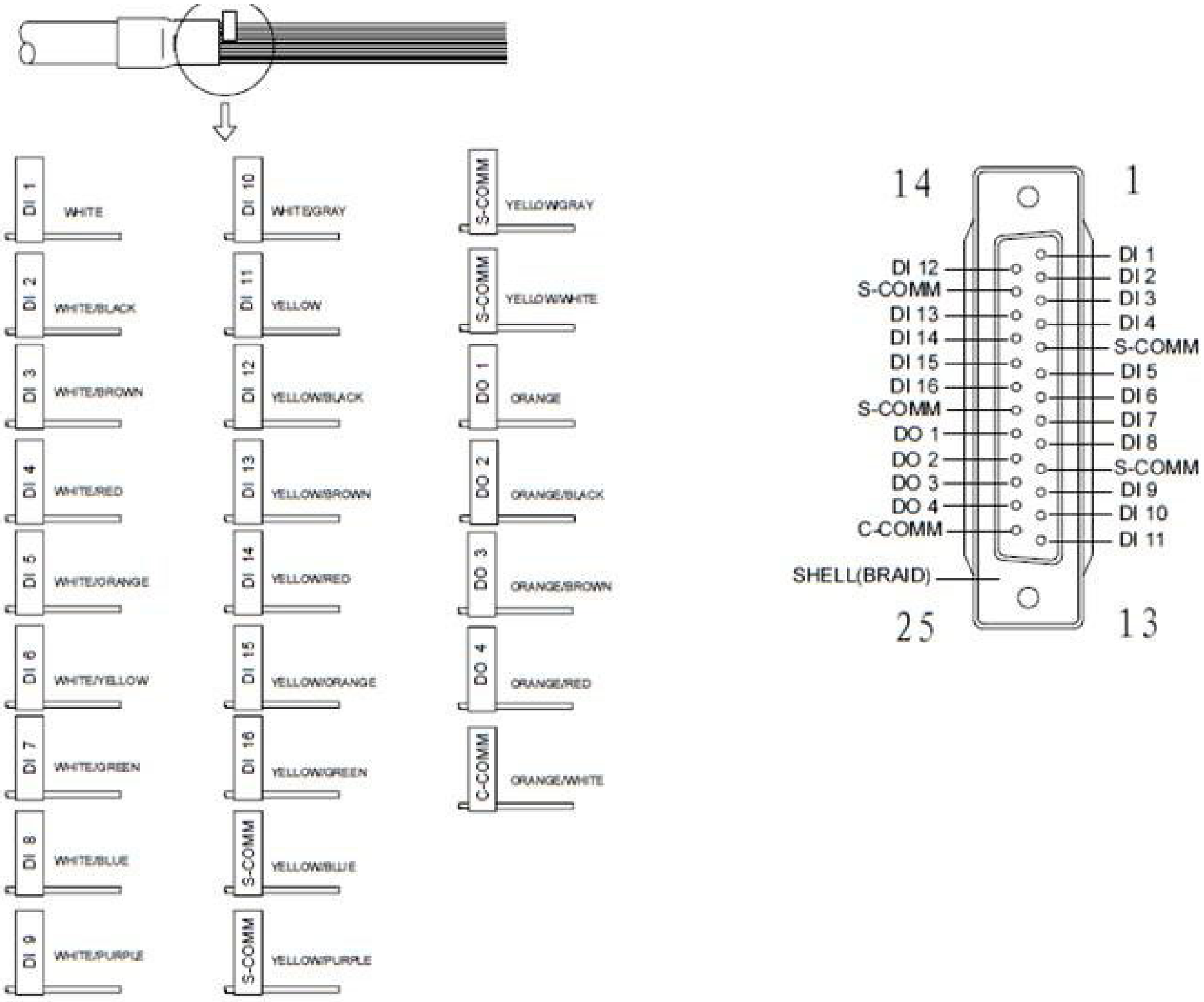


Figure 3-10 Input and Output Ports For MAXPRO NVR Hybrid PE

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.

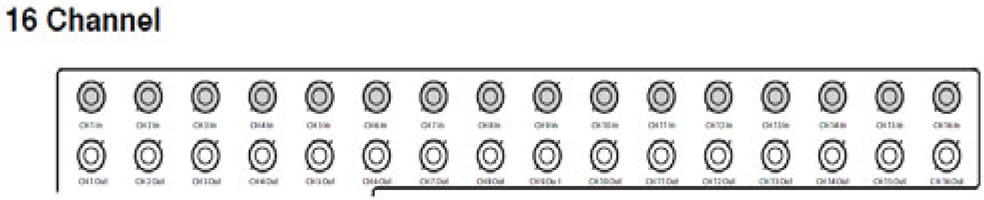


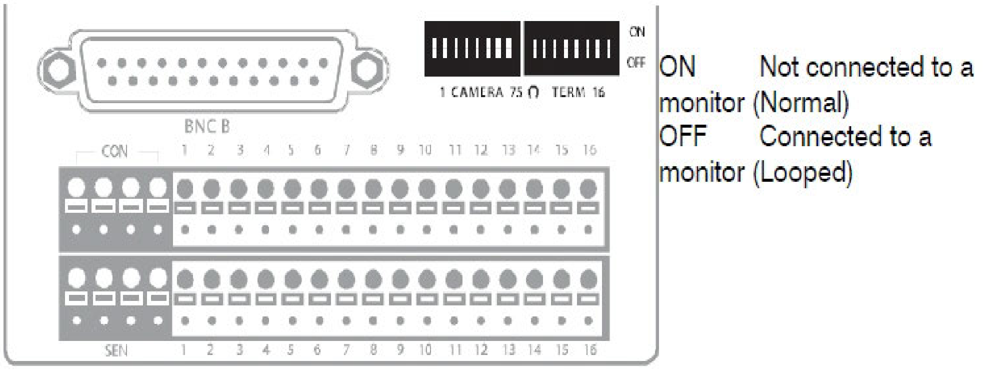
Figure 3-11 Connecting a Video Source

Note: The video inputs are 75 Ώ 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)

Figure 3-12 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.

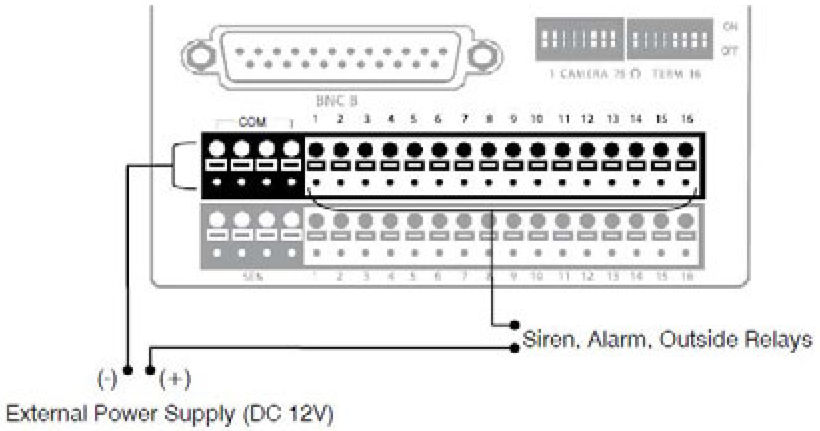


Figure 3-13 Control Outputs

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.

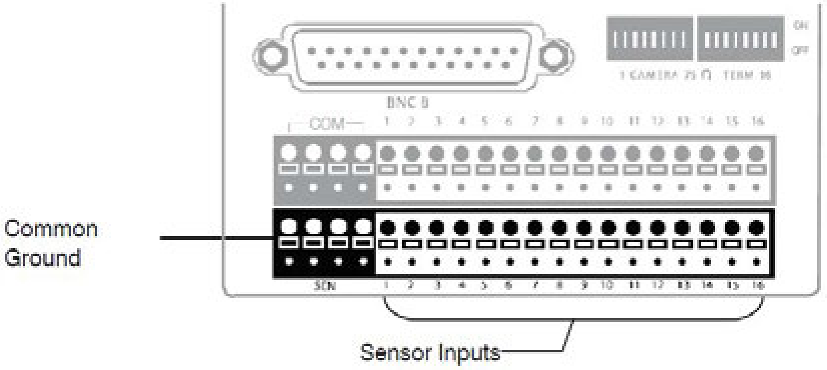


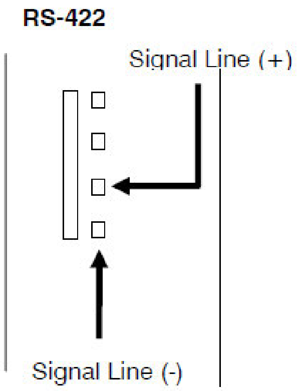
Figure 3-14 Connecting Sensors

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



1. Locate the PTZ adapter cable.
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-.
3. Connect the other end of the adapter to the XVR unit as shown.
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.

Figure 3-15 4-Pin Adapter

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.

1. Power-on the UltraKey Plus keyboard.
2. Press the **Menu** key on the LCD.
3. Press the **MAX-1000 Setup** key on the LCD. The **Left**, **Up**, **Right**, and **Down** buttons appear on the LCD.
4. Press the **Ent** hard key located on the right side of the UltraKey Plus keyboard.
5. Enter the default PIN password **1234**.
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?

1. Press the **Menu** key on the LCD.
2. Press the **MAX-1000 Setup** key on the LCD. The **Left**, **Up**, **Right**, and **Down** buttons appear on the LCD.
3. Press the **Down** key.
4. Press the **Ent** hard key twice located on the right side of the UltraKey Plus keyboard. The log off confirmation message appears.
5. Press the **Ent** hard key.

4

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® 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 NVR before installing MAXPRO NVR software.
- Microsoft® Windows® Server 2008 R2 Standard, Service pack 1 or Windows Server 2012 R2 Standard 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.

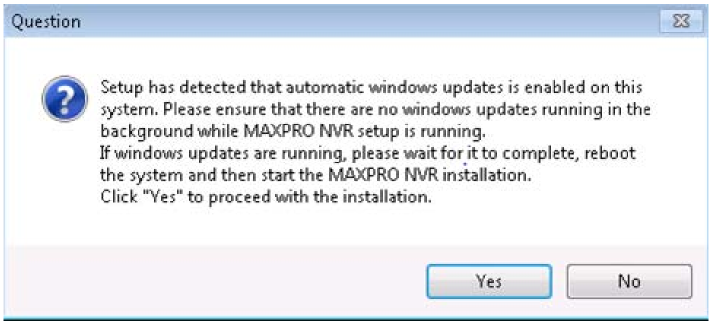
Please refer to the *Microsoft® Windows Patches Tested with MAXPRO®NVR* document for further details on Windows updates that have been tested with the current software version shipping with MAXPRO NVRs.

Before you Begin - Recommended Partition Arrangement for NVR Server

It is recommended to create a separate partition of 50 GB or higher size for Metadata storage preferably on the non-OS hard drive in the NVR Server system. Metadata storage path can be selected during the install and changed from the default path on the OS partition.

Before you Begin - Windows Updates

If Windows updates are enabled in your system, then Figure 4-1 warning message appears and the installation continues.

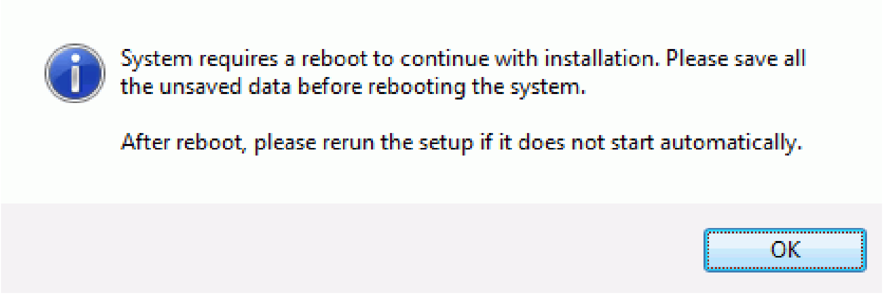


Question

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.

Figure 4-1 Automatic Windows Update Enabled Warning Message

If any pending reboot is there due to windows updates, then Figure 4-2 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.

Figure 4-2 Pending Reboot Error Message

If:

- TrinityBackupScheduler is created manually before the MAXPRO NVR installation
- you have uninstalled MAXPRO NVR (Build 22 or lesser version)

And If

- if scheduled task is already present in the machine.

Then:

- the MAXPRO NVR Server installation will fail to create "TrinityBackupScheduler". In this case, it is recommended that you delete the Scheduled task before starting the installation.

To delete the Scheduled task manually or using Cmd prompt

- Manually: **Control Panel->System and Security->Administrative Tools->Task Scheduler->Task Scheduler Library->Delete** TrinityBackupScheduler OR
- Through Cmd Prompt: **C:\windows\system32\"SchTasks.exe" /Delete /TN "TrinityBackupScheduler" /F**

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.

1. Click **Start** -> **Run** -> type **DFRGUI**.
2. In the **Disk Defragmenter** dialog click **Configure Schedule**
3. Click to clear the **Run on the schedule (recommended)** check box.
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.**
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

1. Turn off the Protection settings for all the drives including OS installed drive in **My Computer** -> **Properties** -> **Advanced System Settings** -> **System Protection** tab.
2. Select the drive under **Protection settings** and click **Configure**.
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 logon 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 226
- Step 6: Disable the Administrator Account, page 230.

MAXPRO NVR Software Installation

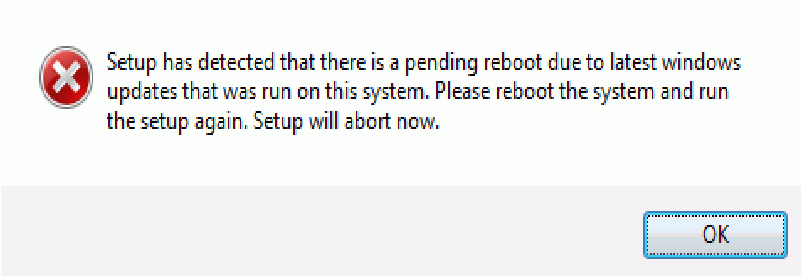
To complete the MAXPRO NVR software installation follow the procedures in these sections:

1. First, How to Install MAXPRO NVR section on page 58
2. Choose the installation that best suits your requirements, and follow the appropriate steps.
   - Full Installation section on page 62 : Full installation can be selected to install the Server and Client on the same system.
   - Client Installation section on page 68 : Client installation can be selected to install MAXPRO NVR desktop client on the client workstations.

How to Install MAXPRO NVR

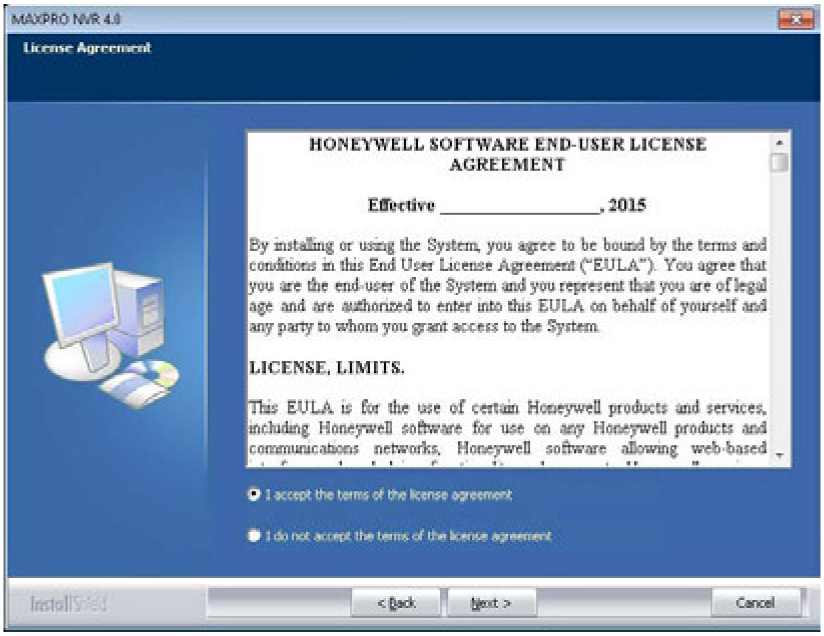
1. Insert the MAXPRO NVR 4.0 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse the DVD drive, and double-click **setup.exe**. A dialog box appears with the question - “Do you want to validate the setup before continuing MAXPRO NVR 4.0 installation ?”, 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 appears.

Note If any reboot is pending 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.

2. Click **Next**. The License Agreement screen appears. See Figure 4-3.



MAXPRO NVR 4.0

License Agreement

HONEYWELL SOFTWARE END-USER LICENSE AGREEMENT

Effective ________________, 2015

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.

LICENSE, LIMITS.

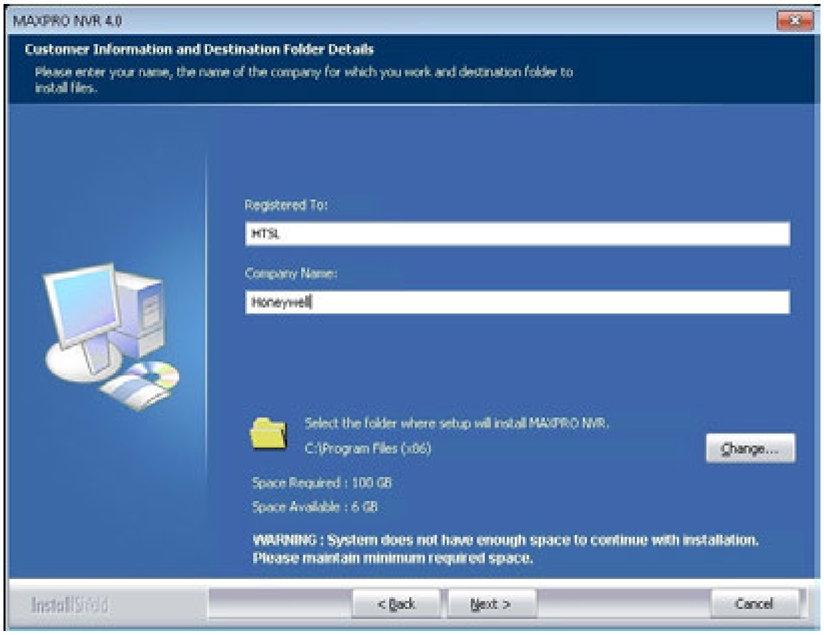
This EULA is for the use of certain Honeywell products and services, including Honeywell software for use on any Honeywell products and communications networks, Honeywell software allowing web-based

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Figure 4-3 License Agreement

3. Read the license agreement, and then select **I accept the terms of the license agreement**. Click **Next** to accept the license agreement, the Customer Information screen (Figure 4-4) appears.



MAXPRO NVR 4.0

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: HTSL

Company Name: Honeywell

Select the folder where setup will install MAXPRO NVR.
C:\Program Files (x86)

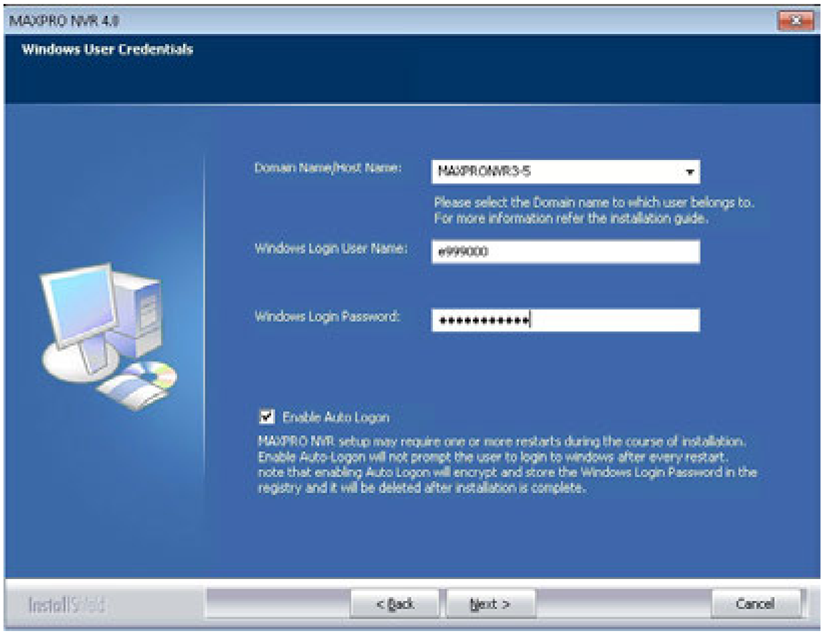
Space Required : 100 GB
Space Available : 6 GB

WARNING : System does not have enough space to continue with installation. Please maintain minimum required space.

Figure 4-4 Customer Information and Destination Folder details

4. Type your **Registered To** name.
5. Type your **Company Name**.
6. Click **Change** if you want to change the destination folder, and then select the folder where MAXPRO NVR must be installed.

7. Click **Next**. The **Windows User Credentials** screen (Figure 4-5) appears.



MAXPRO NVR 4.0

Windows User Credentials

Domain Name/Host Name: MAXPRONVR3-5

Please select the Domain name to which user belongs to.
For more information refer the installation guide.

Windows Login User Name: e999000

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.

Figure 4-5   Validation of User Credentials

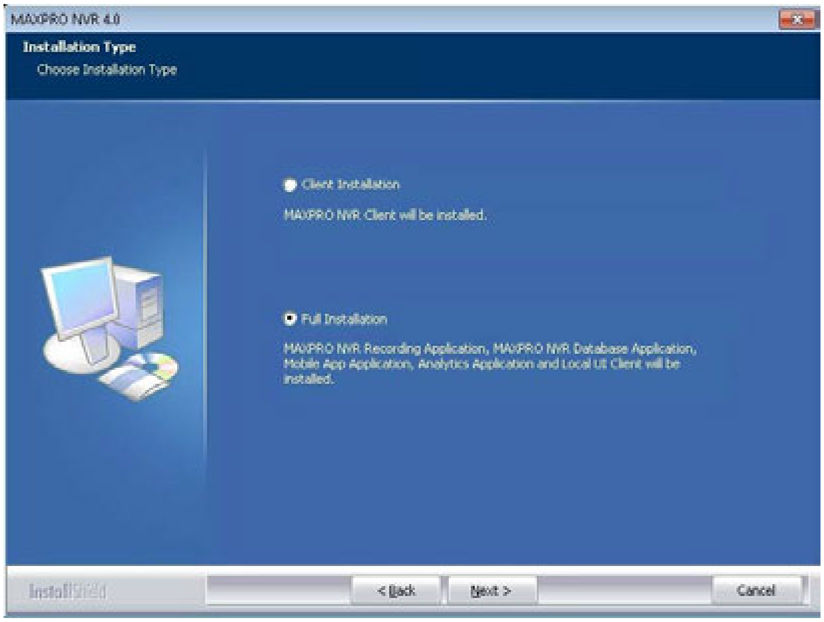
8. Select your **Domain Name**/**Host Name** from the domains drop-down list..

9. Type your **Windows User Name**.

10. Type your **Windows Password**.

Note: Use the newly created Administrator user account as explained in Before you Begin - Changing the default Windows Administrator Account Created By NVR, page 58.

11. Click **Next**. A message “Enabling Auto Log on is not secure as the Password will be stored in the Registry. Do you want to continue” appears. Click **Yes** to open the Choose Installation Type screen (Figure 4-6).



MAXPRO NVR 4.0

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.

Figure 4-6 Choose Installation Type

12. Select the **Client Installation** or **Full Installation** as it applies to your system installation. (See Table 4-1 for more information).

Table 4-1 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 Full Installation section on page 62 for more information.
Client Installation	Installs Client, Trinity Framework, and Adapters. See the Client Installation section on page 68 for more information.

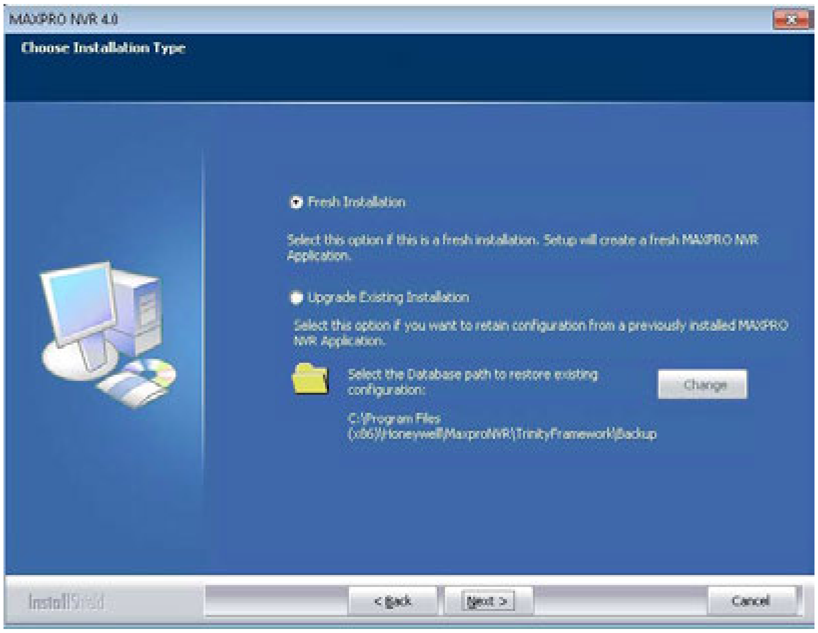
Full Installation

MAXPRO NVR 4.0 Full installation can be selected to install the Server and Client on the same system.

Note: Full Installation is only needed for Software solutions.

To perform a full installation

1. Perform steps 1 through 14 of How to Install MAXPRO NVR section on page 58, and then select the Full Installation option in the Installation Type screen (Figure 4-6). appears.
2. Click **Next**. The **Choose Installation Type** screen appears (Figure 4-7).



MAXPRO NVR 4.0

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)\Honeywell\MaxproNVR\TrinityFramework\Backup

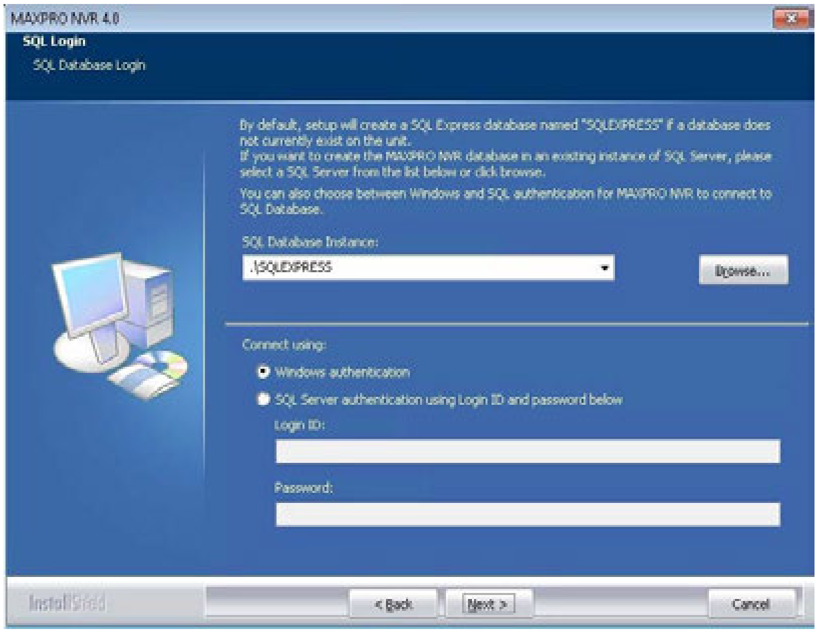
Figure 4-7 Choose Installation Type

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 (Figure 4-8).

   Or

   - **Upgrade\Retain**: 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 (Figure 4-8).



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:

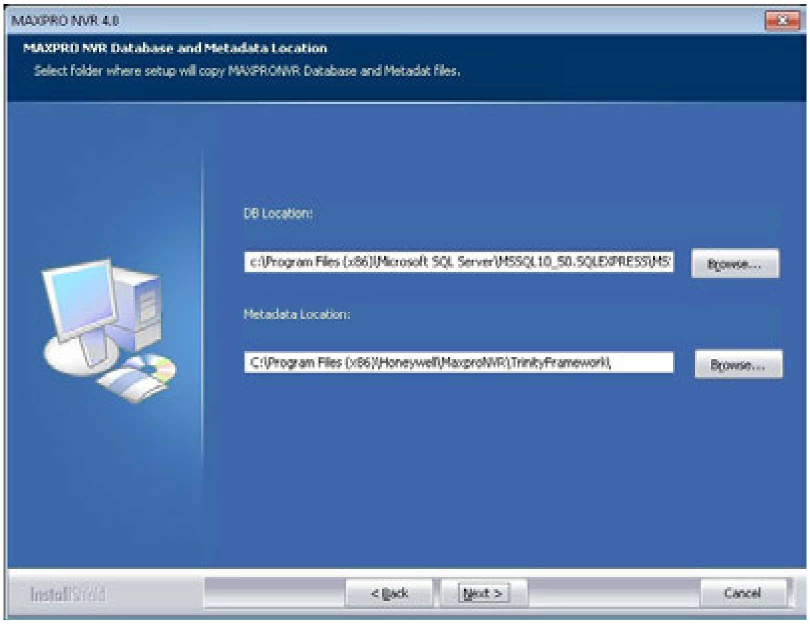
Figure 4-8 Database Server Log on

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.

6. Click **Next**. The SQL credentials validation status appears. After successful validation, the Choose Database and Metadata Location screen appears (Figure 4-9).



MAXPRO NVR Database and Metadata Location

Select folder where setup will copy MAXPRONVR Database and Metadat files.

DB Location:

c:\Program Files (x86)\Microsoft SQL Server\MSSQL10_50.SQLEXPRESS\MS

Metadata Location:

C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework\

Figure 4-9 Choose location for MAXPRO NVR database and Metadata Path

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

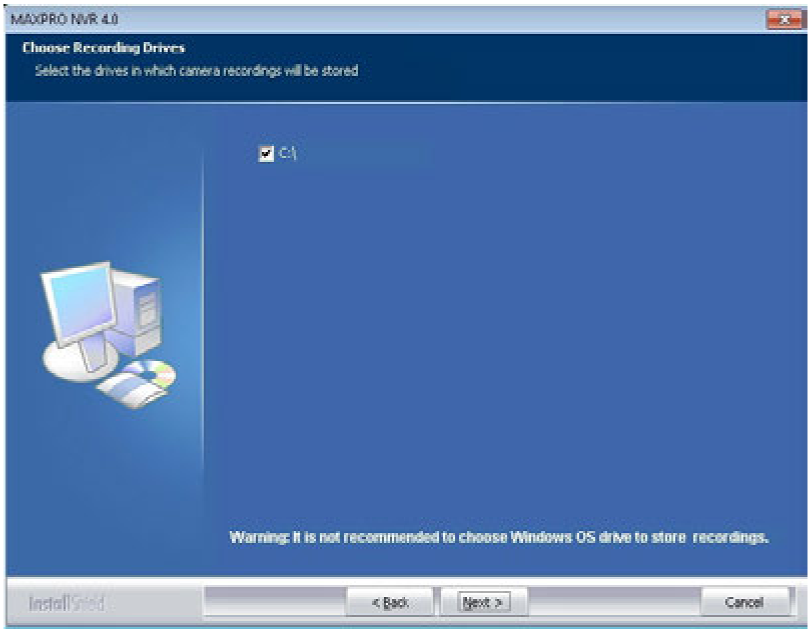
   - **For Fresh installation of a MAXPRO NVR Database**: The default path where the MAXPRO NVR database is created automatically displays for a MAXPRO NVR database fresh installation. Click **Next** to use the default path or click **Browse** to select a new path if necessary and then click **Next.** The **Choose Recording Drives** screen (Figure 4-10) 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. If you

     - Click **Yes**. The Localization Support screen (Figure 4-11) appears.
     - Click **No**. The Choose Recording Drives screen (Figure 4-10) appears.

   - Click **Browse** to select a new path for Metadata if required and then click **Next**. The Choose Recording Drives screen (Figure 4-10) appears.

Note: Metadata path can be changed from the default location to a separate Metadata partition as recommended in the Before you Begin section.



MAXPRO NVR 4.0

Choose Recording Drives

Select the drives in which camera recordings will be stored

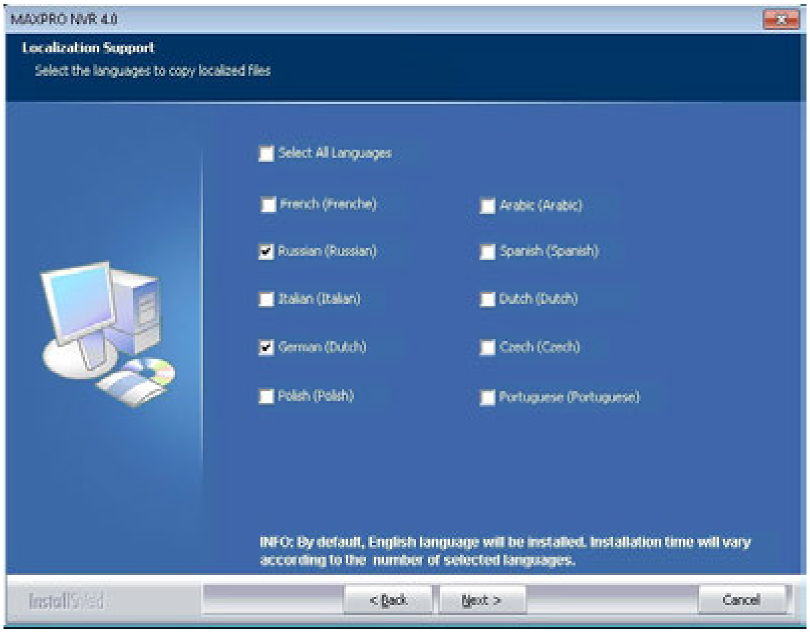
☑ C:\

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

Figure 4-10 Choose Recording Drives

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 (Figure 4-11) 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 4.0

Localization Support

Select the languages to copy localized files

□ Select All Languages

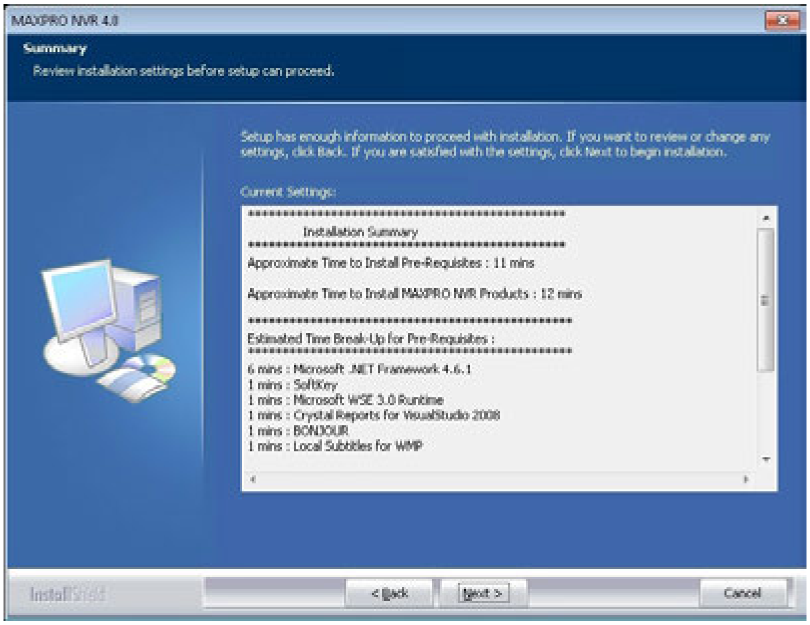
□ French (Frenche)	□ Arabic (Arabic)
☑ Russian (Russian)	□ Spanish (Spanish)
□ Italian (Italian)	□ Dutch (Dutch)
☑ German (Dutch)	□ Czech (Czech)
□ Polish (Polish)	□ Portuguese (Portuguese)

INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.

Figure 4-11 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.

9. Select the languages in which you want to install MAXPRO NVR and then click **Next**. The **Installation Summary** screen (Figure 4-12) 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.

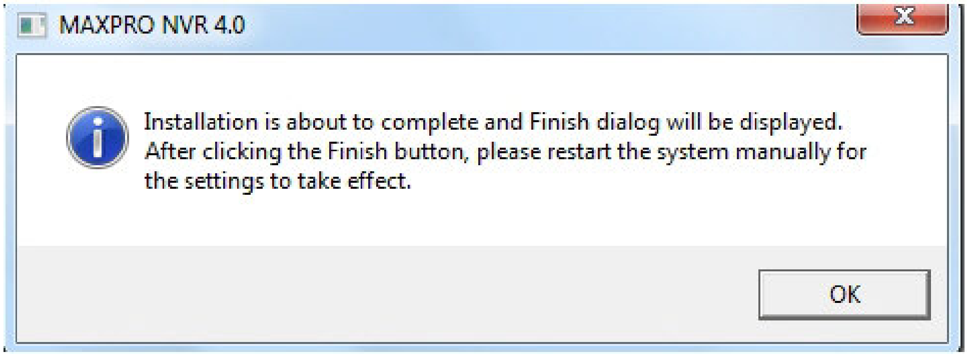
Current Settings:

```
*************************************************
          Installation Summary
*************************************************
Approximate Time to Install Pre-Requisites : 11 mins

Approximate Time to Install MAXPRO NVR Products : 12 mins

**************************************************
Estimated Time Break-Up for Pre-Requisites :
**************************************************
6 mins : Microsoft .NET Framework 4.6.1
1 mins : SoftKey
1 mins : Microsoft WSE 3.0 Runtime
1 mins : Crystal Reports for VisualStudio 2008
1 mins : BONJOUR
1 mins : Local Subtitles for WMP
```

Figure 4-12 Summary

10. The approximate time for installing the prerequisites and MAXPRO NVR Products displays. If you want to change any settings, click **Back**, else click **Next**.

11. When the installation is about to complete, the following message is displayed.

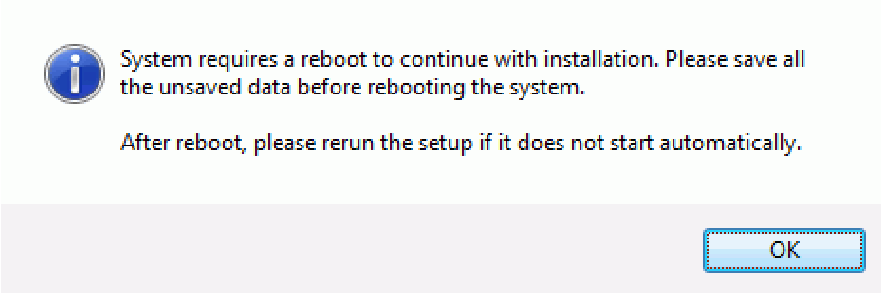


Installation is about to complete and Finish dialog will be displayed. After clicking the Finish button, please restart the system manually for the settings to take effect.

12. 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 11 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.

Figure 4-13 Reboot prompt

13. Click **OK** to complete the MAXPRO NVR installation.

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 a fresh installation scenario, 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.

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**

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

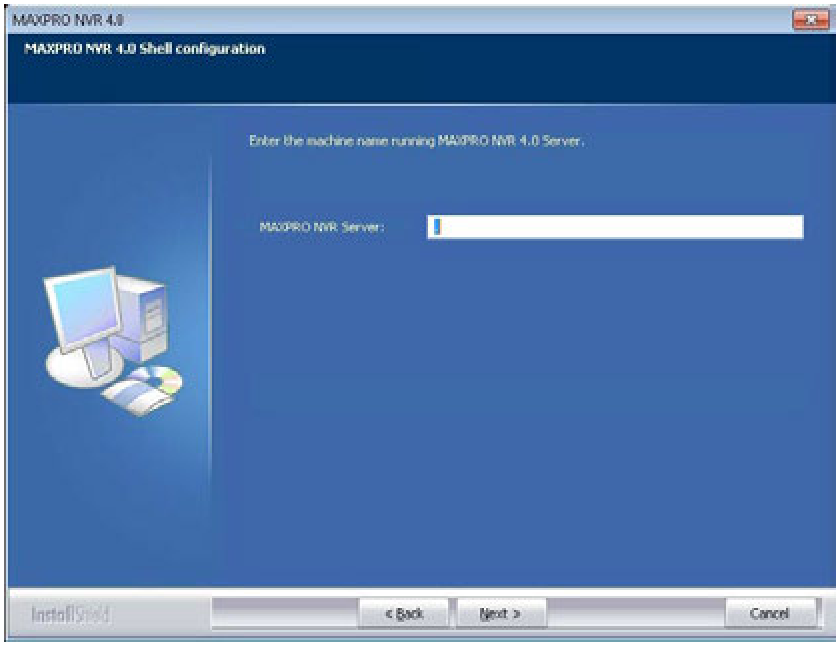
- Internet Explorer version 11 or above
- Firefox version 40 or above

- **Web Browsers Supported on MAC systems**: Not supported.

Client Installation

MAXPRO NVR 4.0 Client installation gives you an option to install MAXPRO NVR Client on the client workstations.

1. Select **Client Installation** in Figure 4-6 and click **Next**. The Client Configuration screen (Figure 4-14) appears.


MAXPRO NVR 4.0

MAXPRO NVR 4.0 Shell configuration

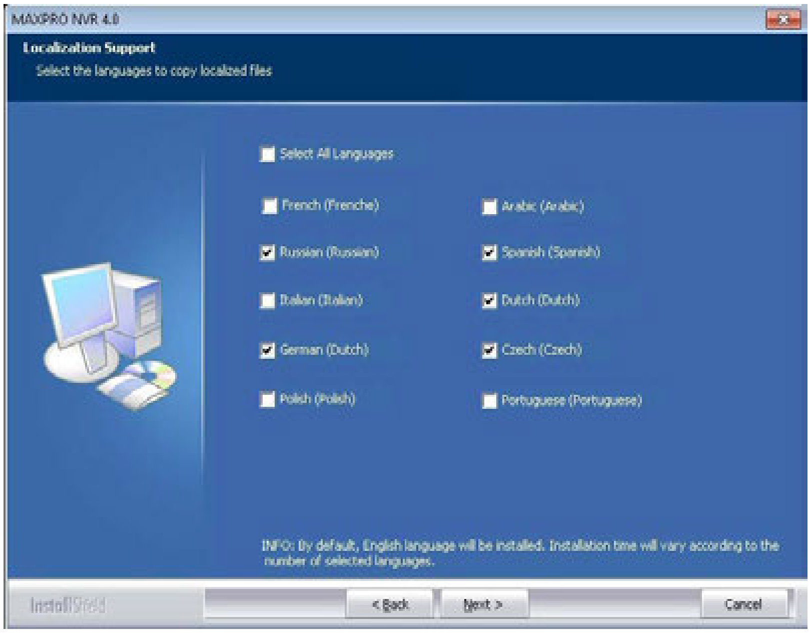
Enter the machine name running MAXPRO NVR 4.0 Server.

MAXPRO NVR Server:

Figure 4-14 MAXPRO NVR 4.0 Client Configuration

2. Type the **MAXPRO NVR Server** name or IP address, and then click **Next**. The **Localization Support** screen (Figure 4-15) 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 4.0

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)

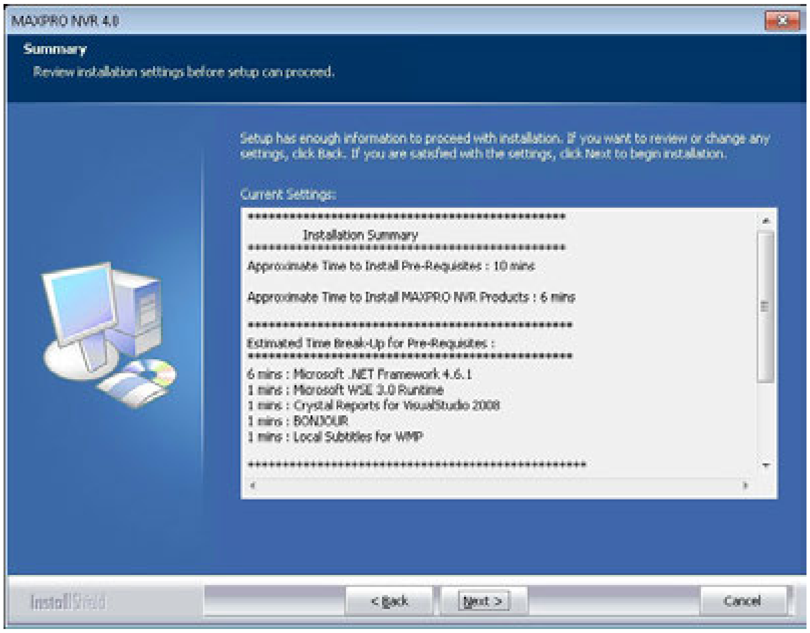
□ Polish (Polish)   □ Portuguese (Portuguese)

INFO: By default, English language will be installed. Installation time will vary according to the number of selected languages.

Figure 4-15 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.

3. Select the languages in which you want to install MAXPRO NVR and then click **Next**. The **Installation Summary** screen (Figure 4-16) 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.

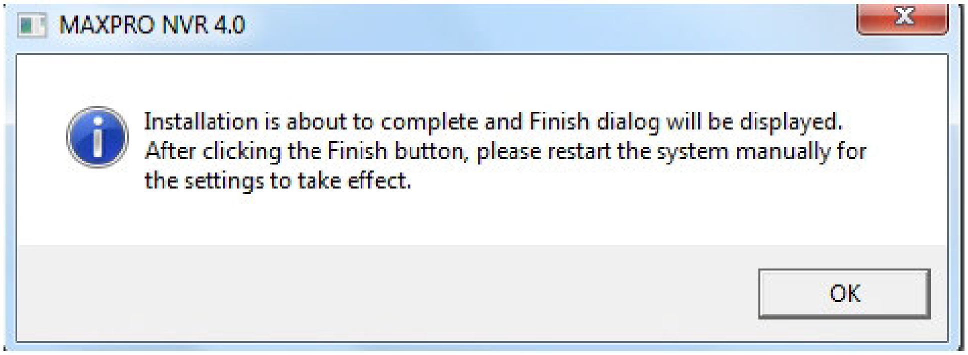
Current Settings:

```
**********************************************
          Installation Summary
**********************************************
Approximate Time to Install Pre-Requisites : 10 mins

Approximate Time to Install MAXPRO NVR Products : 6 mins

***********************************************
Estimated Time Break-Up for Pre-Requisites :
***********************************************
6 mins : Microsoft .NET Framework 4.6.1
1 mins : Microsoft WSE 3.0 Runtime
1 mins : Crystal Reports for VisualStudio 2008
1 mins : BONJOUR
1 mins : Local Subtitles for WMP

*************************************************
```

Figure 4-16 Summary

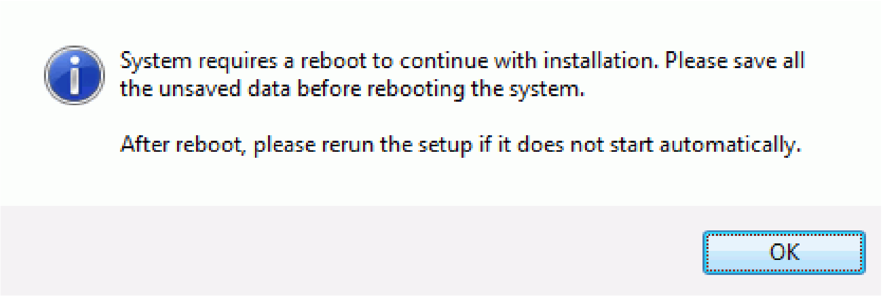
4. If you want to review or change any settings click **Back**, otherwise click **Next.** The setup status of various components appears.

5. When the installation 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.

6. 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, as mentioned in step 5 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.

Figure 4-17 Reboot prompt

7. 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

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.
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.
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

1. Go to **Control Panel->Programs and Features**, select **MAXPRO NVR 4.0** and click **uninstall**.

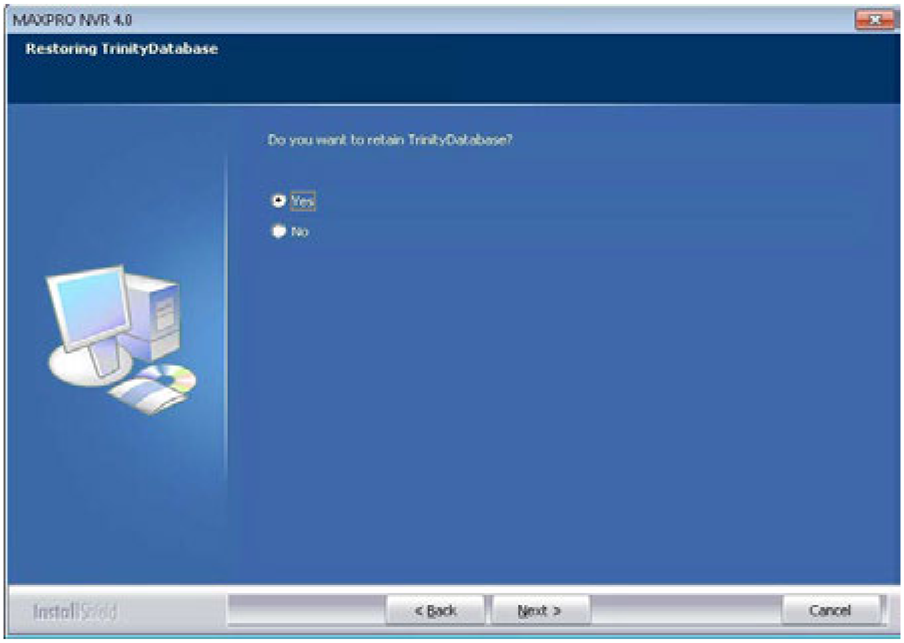
   Or

   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.
   A message **Do you want to completely remove the selected application and all of its feature?** is displayed.Click **Yes** or **No** as applicable. If you click **Yes,** Figure 4-18 is displayed.

2. Click **Next**. The Restoring Trinity Database (Figure 4-18) appears.



MAXPRO NVR 4.0

Restoring TrinityDatabase

Do you want to retain TrinityDatabase?

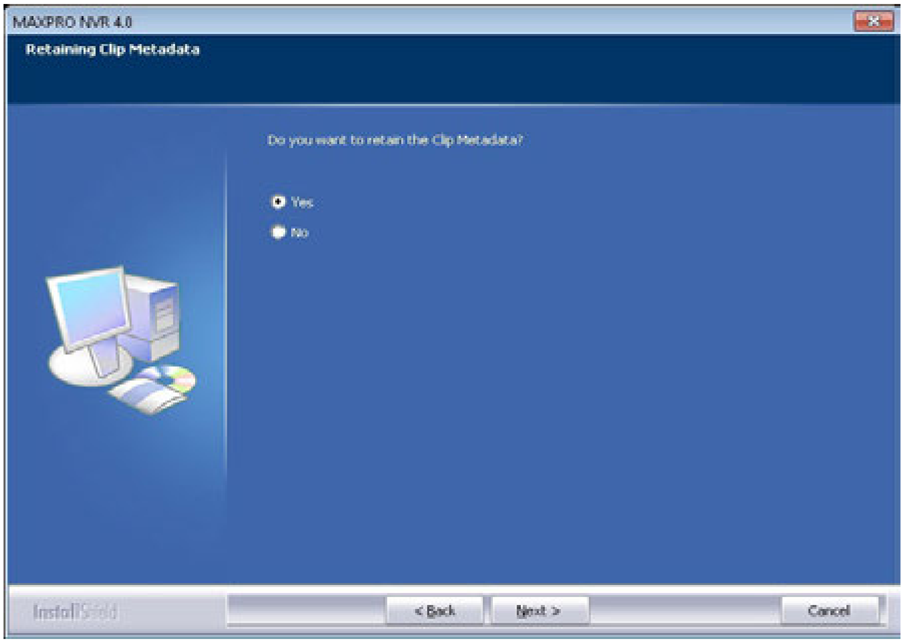
● Yes
○ No

Figure 4-18 Retaining Trinity Database

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 Retaining Clip Metadata (Figure 4-19) appears. Go to step **4**.

- 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. Go to step **6**.



MAXPRO NVR 4.0

Retaining Clip Metadata

Do you want to retain the Clip Metadata?

● Yes
○ No

Figure 4-19 Retaining Clip (Recording) Metadata

4. Click **Yes** or **No** as applicable.

   - If you click “**Yes”** and then click **Next,** the clip (recording) metadata path is retained for future installations of MAXPRO NVR.

   - If you click “**No**” and then click **Next**, the clip (recording) metadata path is deleted. The uninstall status of various components appears. Go to step **6**.

5. Click **Finish**. The uninstall wizard closes and you are prompted to reboot your computer
6. Click **OK** to complete the uninstall procedure.

Note: The Database and Clip (recording) Metadata backup taken during the uninstall process can be used for future installations. This backup does not include Video storage drive’s data.

Upgrading MAXPRO NVR

This section describes about the various ways to upgrade MAXPRO NVR. The following are the upgrade scenarios covered in this section:

- To upgrade to MAXPRO NVR 4.0
- Upgrading to MAXPRO NVR 4.1Build 123 Rev B
- Upgrading to MAXPRO NVR 4.5 Build 159

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 57.

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.

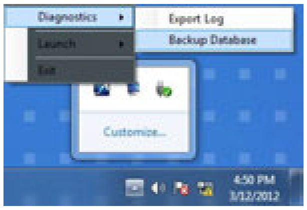


Figure 4-20 Taking Database backup using the MAXPRO NVR Agent

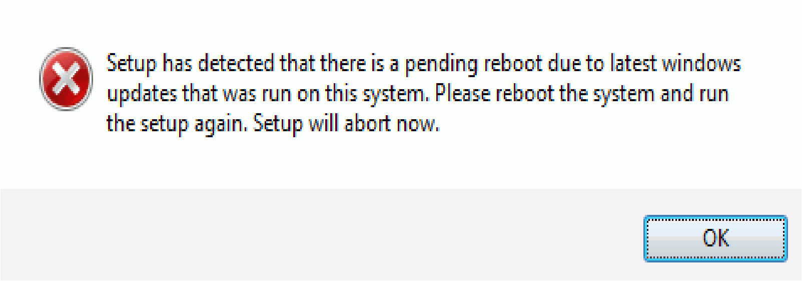
Note: In MAXPRO NVR 3.1 or later version, a new scheduled backup mechanism is added which will retain the last 7 days of Database Backup. In case of upgrade, if the backup is set in the system already then same backup drives are maintained in the configuration and used in the new backup mechanism.
Or
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.

To upgrade to MAXPRO NVR 4.0

1. Insert the MAXPRO NVR 4.0 setup DVD in the DVD drive, browse the DVD drive, and then double-click **setup.exe**

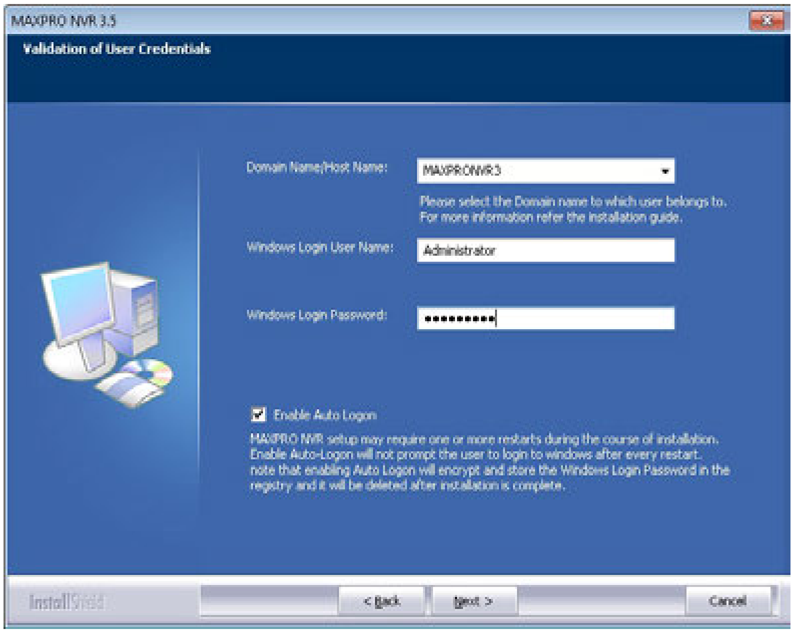
   Or
   Go to the MAXPRO NVR setup folder on your computer, and then double-click **setup.exe**. A dialog box appears with the question - “Do you want to validate the setup before continuing MAXPRO NVR 4.0 installation ?”, click **Yes** to validate the setup files are not corrupted before continuing the 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.

2. Click **Next**. The Validation of User Credentials (Figure 4-21) 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

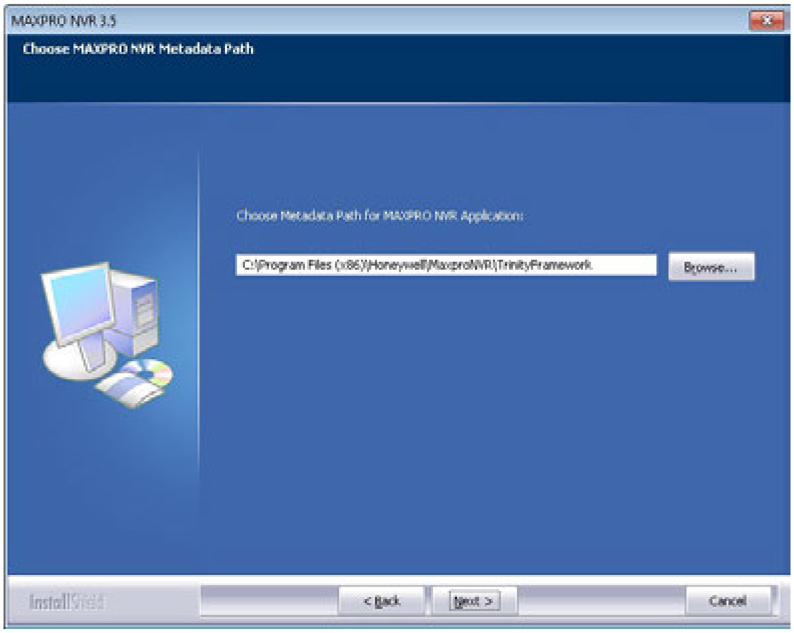
MAXPRO NVR setup may require one or more restarts during the course of installation. Enable Auto-Logon will not prompt the user to login to windows after every restart. note that enabling Auto Logon will encrypt and store the Windows Login Password in the registry and it will be deleted after installation is complete.

Figure 4-21 Validation of User Credentials

3. Select your **Domain Name**/**Host Name**.
4. Type your **Windows User Name**.
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 58.

6. Click **Next**. The Choose Metadata Path (Figure 4-22) appears.



MAXPRO NVR 3.5

Choose MAXPRO NVR Metadata Path

Choose Metadata Path for MAXPRO NVR Application:

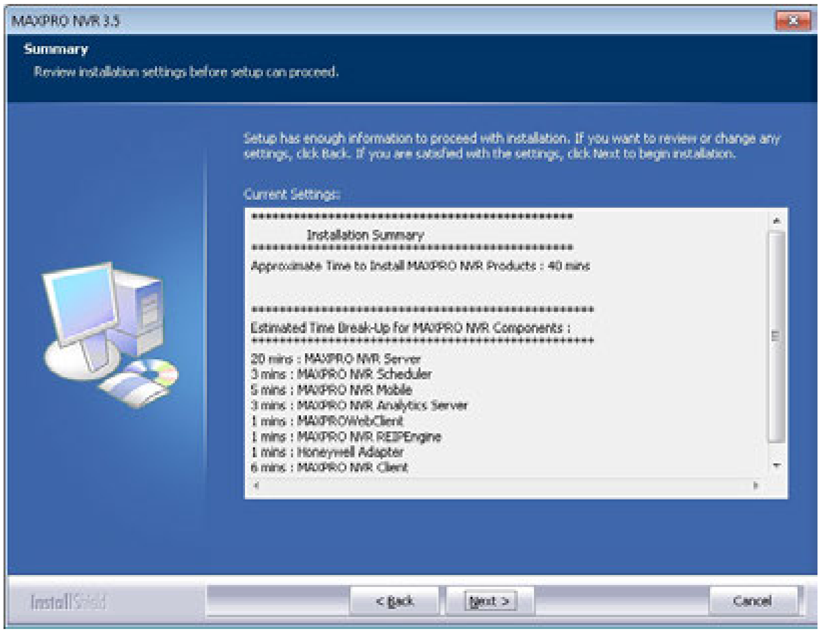
C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework

Figure 4-22 Choose Metadata Path

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.

8. Click **Next**. The summary screen (Figure 4-23) 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:

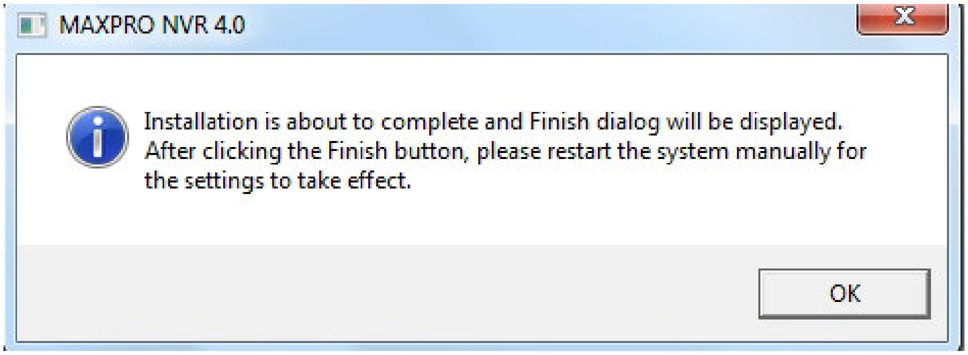
```
**************************************************
          Installation Summary
**************************************************
Approximate Time to Install MAXPRO NVR Products : 40 mins


*****************************************************
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
```

Figure 4-23 Summary

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.

10. When the upgrade is about to complete, the following message is displayed.

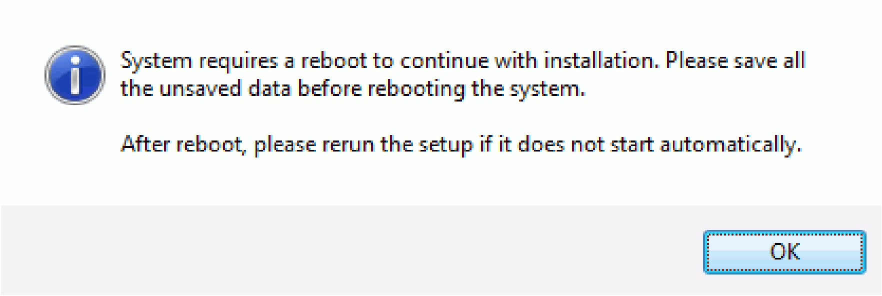


Installation is about to complete and Finish dialog will be displayed. After clicking the Finish button, please restart the system manually for the settings to take effect.

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.

Figure 4-24 Reboot prompt

12. Click **OK** to complete the MAXPRO NVR upgrade.

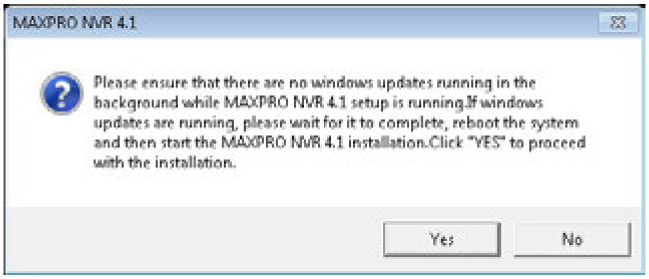
Upgrading to MAXPRO NVR 4.1Build 123 Rev B

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

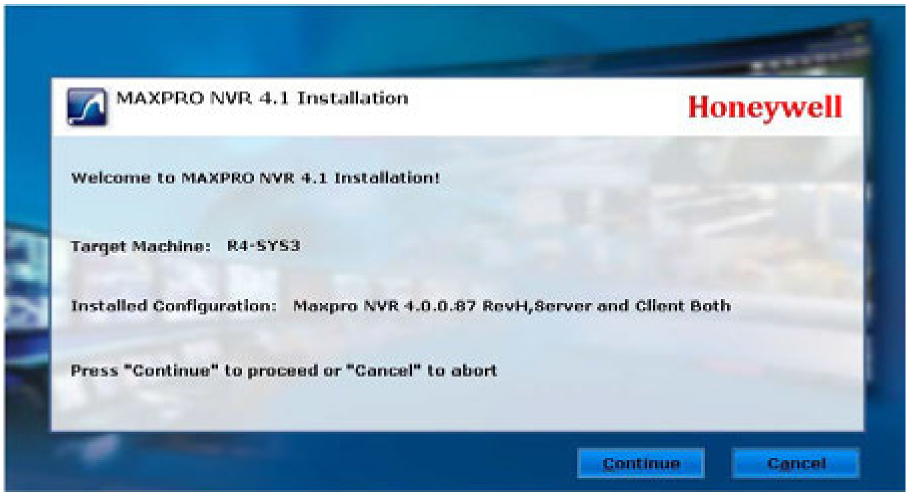
1. Double click **MAXPRO NVR 4.1 Setup.exe**. The WinRAR self extracts the files and displays the Windows update message.



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.

2. Click **Yes** to proceed, the installation wizard starts and the **Welcome** page appears.


MAXPRO NVR 4.1 Installation

Welcome to MAXPRO NVR 4.1 Installation!

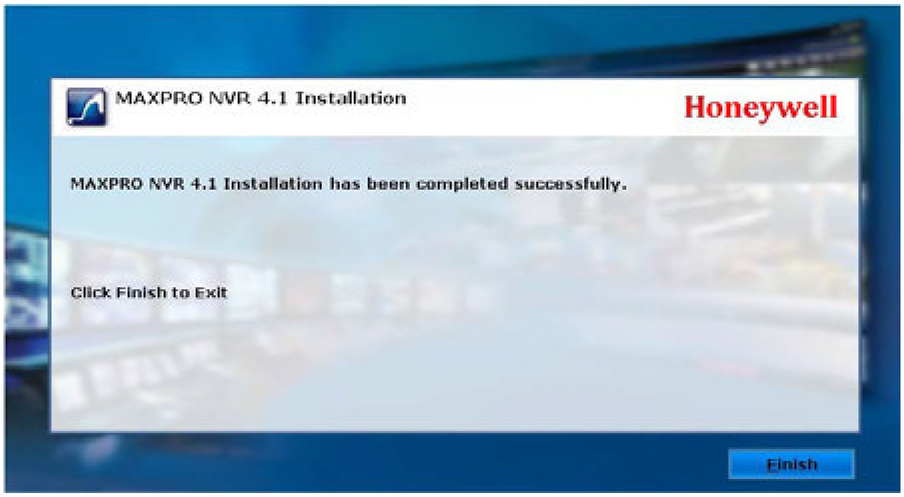
Target Machine: R4-SYS3

Installed Configuration: Maxpro NVR 4.0.0.87 RevH,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Figure 4-25 Welcome Wizard

3. Click **Continue** to start the installation. After the installation is finished, the following page appears.


MAXPRO NVR 4.1 Installation

MAXPRO NVR 4.1 Installation has been completed successfully.

Click Finish to Exit

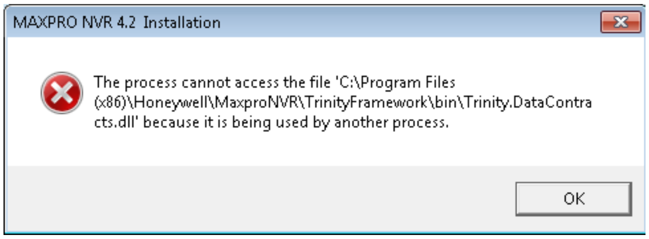
Figure 4-26 Installation Complete

4. Click **Finish** to complete the installation and close the wizard.

Upgrading to MAXPRO NVR 4.5 Build 161

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

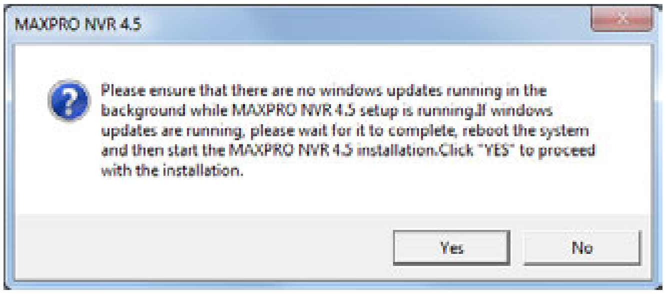
The process cannot access the file 'C:\Program Files (x86)\Honeywell\MaxproNVR\TrinityFramework\bin\Trinity.DataContracts.dll' because it is being used by another process.

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

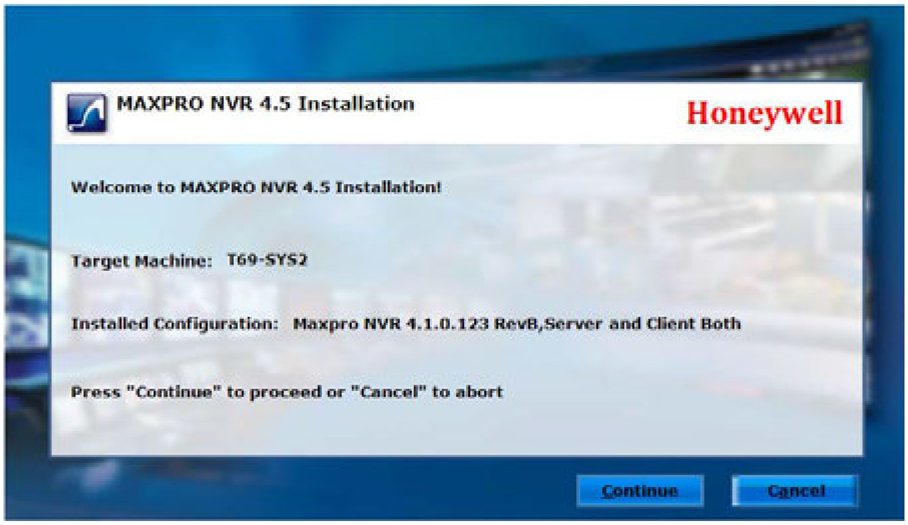
To upgrade to MAXPRO NVR 4.5 Service Pack

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.

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!

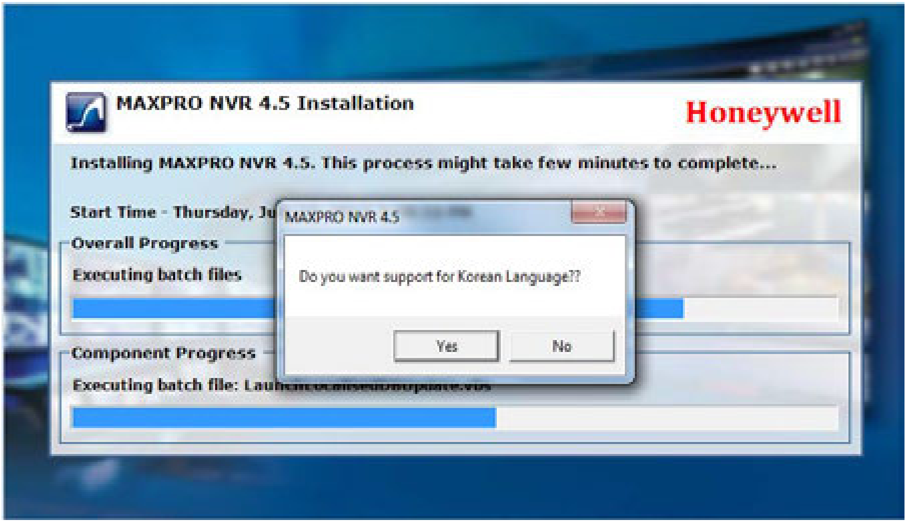
Target Machine: T69-SYS2

Installed Configuration: Maxpro NVR 4.1.0.123 RevB,Server and Client Both

Press "Continue" to proceed or "Cancel" to abort

Figure 4-27 Welcome Wizard

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

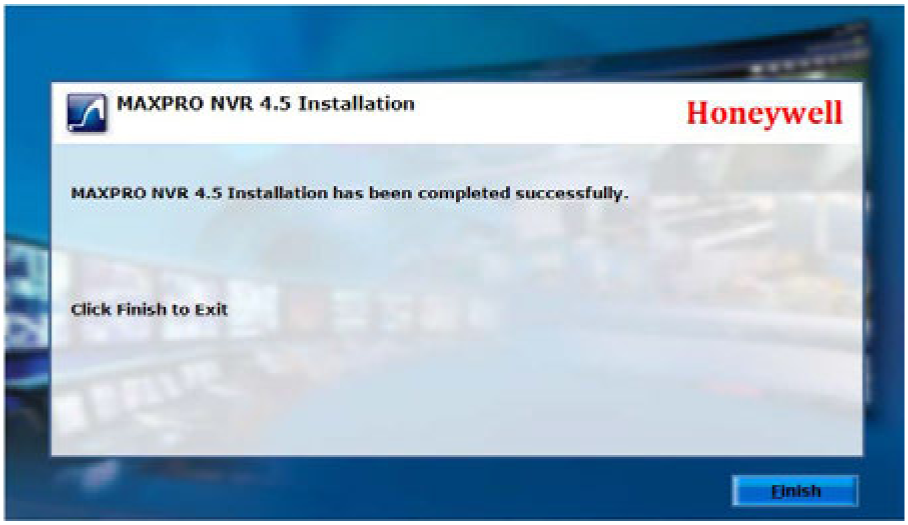
Executing batch file: Lau

MAXPRO NVR 4.5

Do you want support for Korean Language??

Figure 4-28 Installation Complete

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 has been completed successfully.

Click Finish to Exit

5. Click **Finish** to complete the installation and close the wizard.

This page is intentionally left blank

5

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.

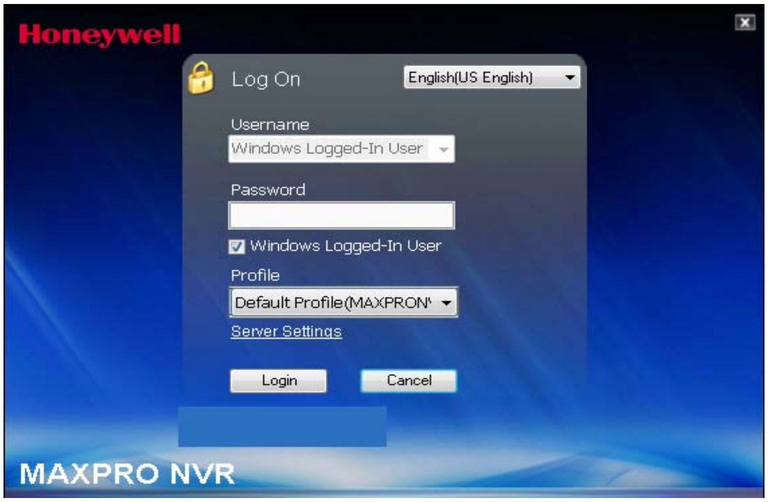
Logging on to MAXPRO NVR

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 MAXPRO NVR. See Securing MAXPRO NVR section on page 225 section for more information.

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

   Or

Click **Start -> Programs -> Honeywell -> MAXPRO NVR**. The **Log On** dialog box (Figure 5-1) appears.



English(US English)

Username: Windows Logged-In User

Password:

☑ Windows Logged-In User

Profile: Default Profile(MAXPRON'

Figure 5-1 MAXPRO NVR Log on dialog box

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, and English. The default language is **English (US English)**.
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.
4. 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 Use**r 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.

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.

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.

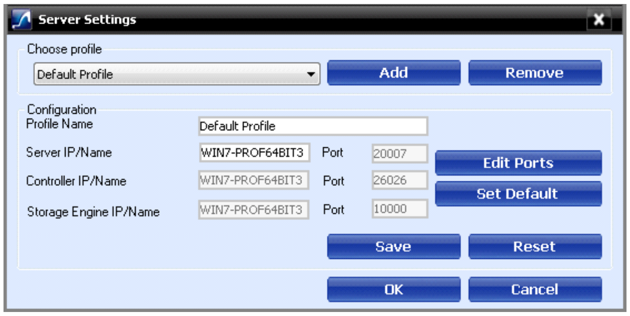
Configuring MAXPRO NVR Windows/ Desktop Client

Managing Profiles

Saving a Server Address in a Profile

To save a server address

1. In the client workstation, double-click the icon on the desktop to display the **Log On** dialog box.
2. Click **Server Settings**. The **Server Settings** dialog box appears (Figure 5-2).


Server Settings

Choose profile: Default Profile

Configuration
Profile Name: Default Profile
Server IP/Name: WIN7-PROF64BIT3 Port 20007
Controller IP/Name: WIN7-PROF64BIT3 Port 26026
Storage Engine IP/Name: WIN7-PROF64BIT3 Port 10000

Figure 5-2 Server Settings dialog box

3. Click **Add.**
4. Type the **Profile Name** to identify the profile.

5. Type the **Server IP**/**Name** (numerical IP address or the network name of the MAXPRO NVR server).
6. Click **Save**.
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

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

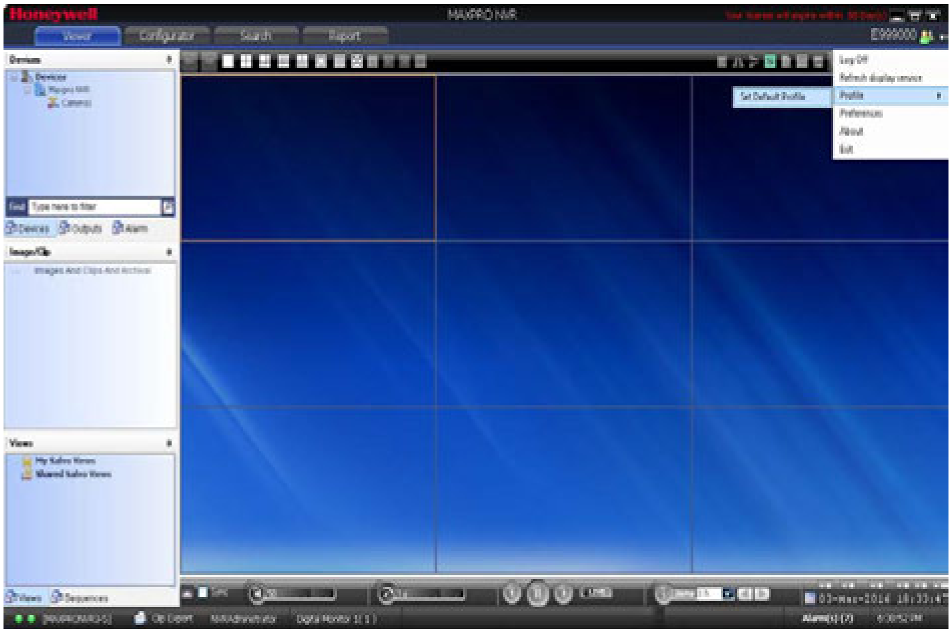


Figure 5-3 Setting the Default Profile

Modifying a Profile

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

To modify a profile

1. In the client workstation, double-click the icon on the desktop to display the **Log On** dialog box.
2. Click **Server Settings**. The **Server Settings** dialog box appears.
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.
4. Change the **Profile Name,** as applicable.
5. Change the **Server IP**/**Name**, as applicable.
6. Click **Save**.
7. Click **OK**. The profile is modified.

Deleting a Profile

1. In the client workstation, double-click the icon on the desktop to display the **Log On** dialog box.
2. Click **Server Settings**. The **Server Settings** dialog box appears.
3. In the **Choose Profile** box, select the profile you want to delete.
4. Click **Remove**.
5. Click **OK**. The profile is deleted.

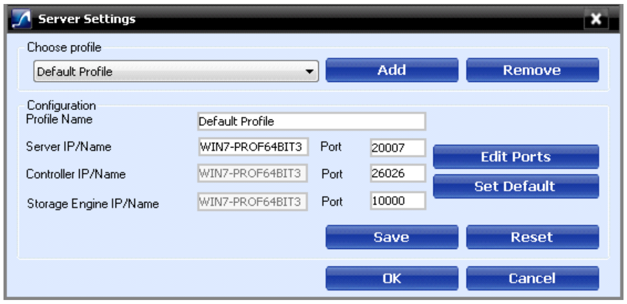
Editing the Ports

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:

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.


Server Settings

Choose profile: Default Profile

Configuration
Profile Name: Default Profile
Server IP/Name: WIN7-PROF64BIT3 Port 20007
Controller IP/Name: WIN7-PROF64BIT3 Port 26026
Storage Engine IP/Name: WIN7-PROF64BIT3 Port 10000

Figure 5-4 Editing the Ports

2. Change the port numbers, as applicable.
3. Click **Save**.

Note: Port 20000 is used for ONVIF discovery.

Port Forwarding

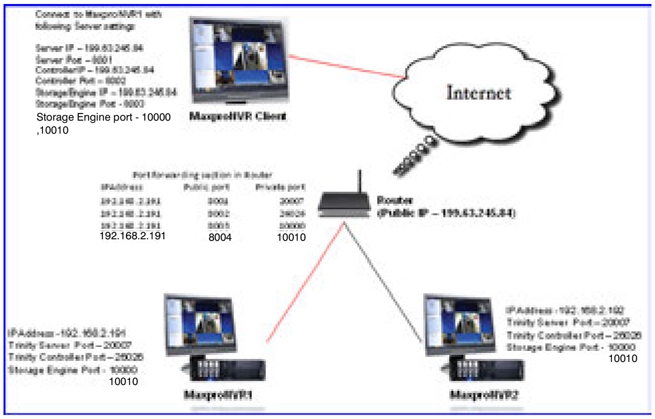
The Port Forwarding feature is generally used when an Internet client wants to connect to a particular NVR in a private Local Area Network (LAN). This feature is enabled by defining port forwarding rules in the Router. By defining these rules, you can send data using the range of ports on the internet 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 201 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
Storage Engine port - 10000 ,10010

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
192.168.2.191	8004	10010

IPAddress - 192.168.2.191
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000
10010

IPAddress - 192.168.2.192
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000
10010

Figure 5-5 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.

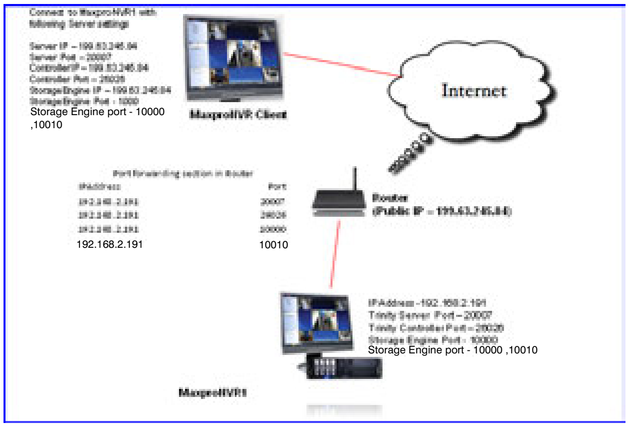

Connect to MaxproNVR1 with
following Server settings
Server IP – 199.63.245.84
Server Port – 20007
Controller IP – 199.63.245.84
Controller Port – 26026
StorageEngine IP – 199.63.245.84
StorageEngine Port - 1000
Storage Engine port - 10000
,10010
MaxproNVR Client
Internet
Port forwarding section in Router
IPAddress
Port
192.168.2.191
20007
192.168.2.191
26026
192.168.2.191
10000
192.168.2.191
10010
Router
(Public IP – 199.63.245.84)
IPAddress -192.168.2.191
Trinity Server Port – 20007
Trinity Controller Port – 26026
Storage Engine Port - 10000
Storage Engine port - 10000 ,10010
MaxproNVR1

Figure 5-6 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 5-7 illustrates the **Viewer** tab.

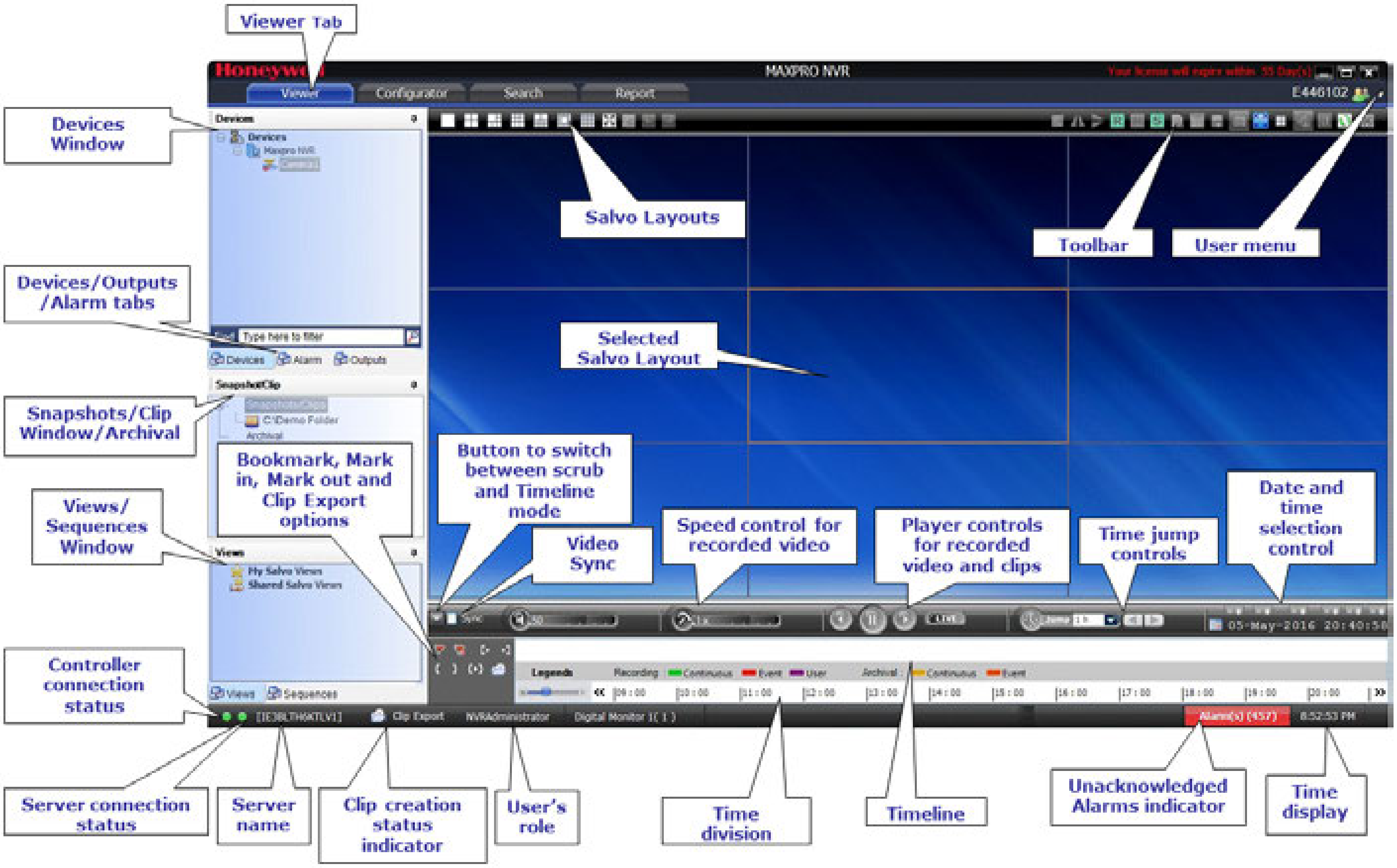

Viewer Tab
MAXPRO NVR
Viewer
Configurator
Search
Report
Devices Window
Devices/Outputs /Alarm tabs
Snapshots/Clip Window/Archival
Bookmark, Mark in, Mark out and Clip Export options
Views/ Sequences Window
Controller connection status
Salvo Layouts
Toolbar
User menu
Selected Salvo Layout
Button to switch between scrub and Timeline mode
Video Sync
Speed control for recorded video
Player controls for recorded video and clips
Time jump controls
Date and time selection control
Server connection status
Server name
Clip creation status indicator
User's role
Time division
Timeline
Unacknowledged Alarms indicator
Time display

Figure 5-7 Viewer tab

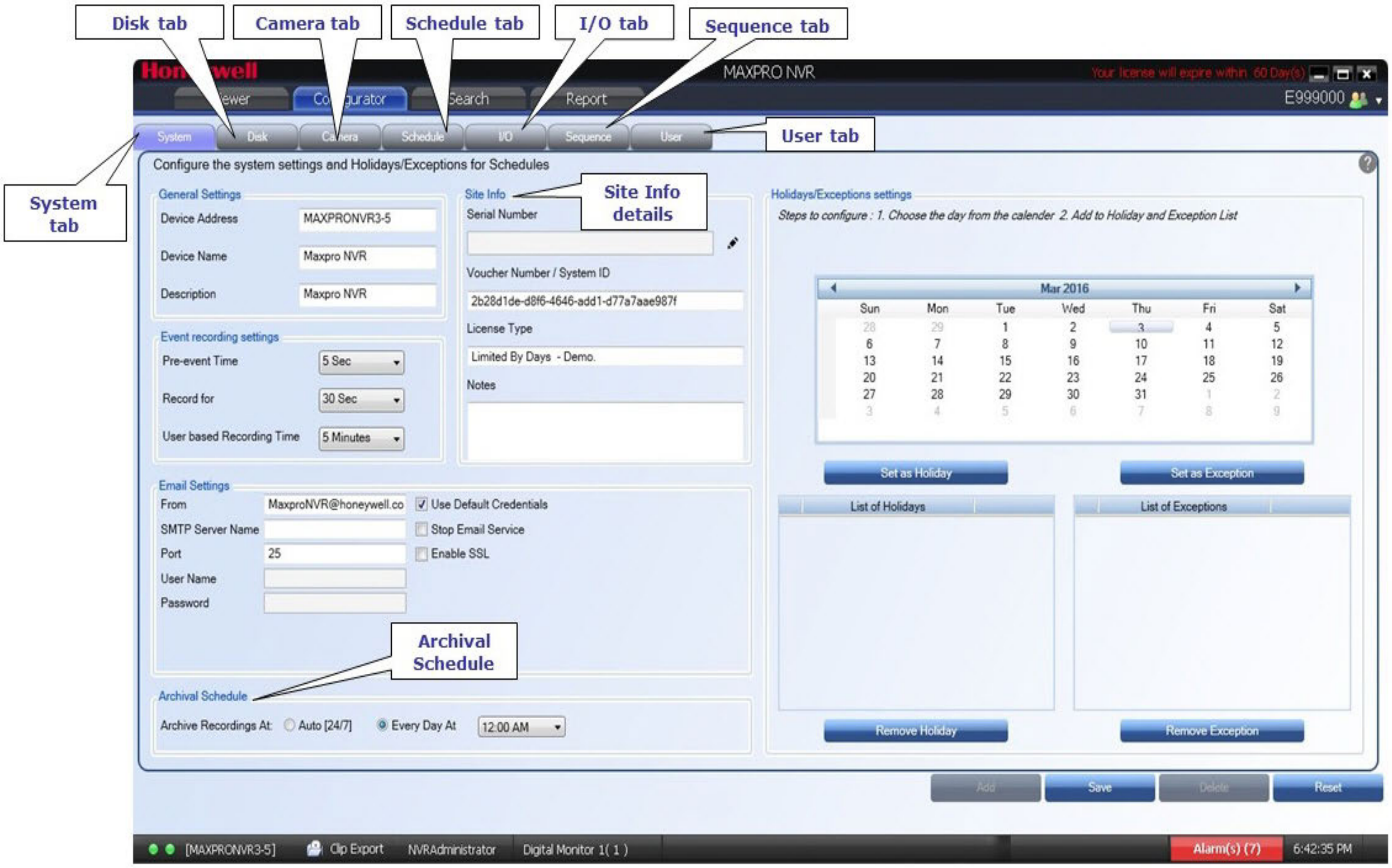
The following components are displayed on the Viewer tab screen.

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.

Component	Description
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 and 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 176.
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 5-8 illustrates the **Configurator** tab.



Configure the system settings and Holidays/Exceptions for Schedules

General Settings

- Device Address: MAXPRONVR3-5
- Device Name: Maxpro NVR
- Description: Maxpro NVR

Event recording settings

- Pre-event Time: 5 Sec
- Record for: 30 Sec
- User based Recording Time: 5 Minutes

Site Info

- Serial Number:
- Voucher Number / System ID: 2b28d1de-d8f6-4646-add1-d77a7aae987f
- License Type: Limited By Days - Demo.
- Notes:

Email Settings

- From: MaxproNVR@honeywell.co
- SMTP Server Name:
- Port: 25
- User Name:
- Password:
- ☑ Use Default Credentials
- □ Stop Email Service
- □ Enable SSL

Archival Schedule

Archive Recordings At: ○ Auto [24/7] ● Every Day At 12:00 AM

Holidays/Exceptions settings

Steps to configure : 1. Choose the day from the calender 2. Add to Holiday and Exception List

Figure 5-8 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 and Holidays/Exceptions settings for MAXPRO NVR.
Disk tab	Helps you to configure the disk settings for video storage.
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 5-9 illustrates the **Search** tab.

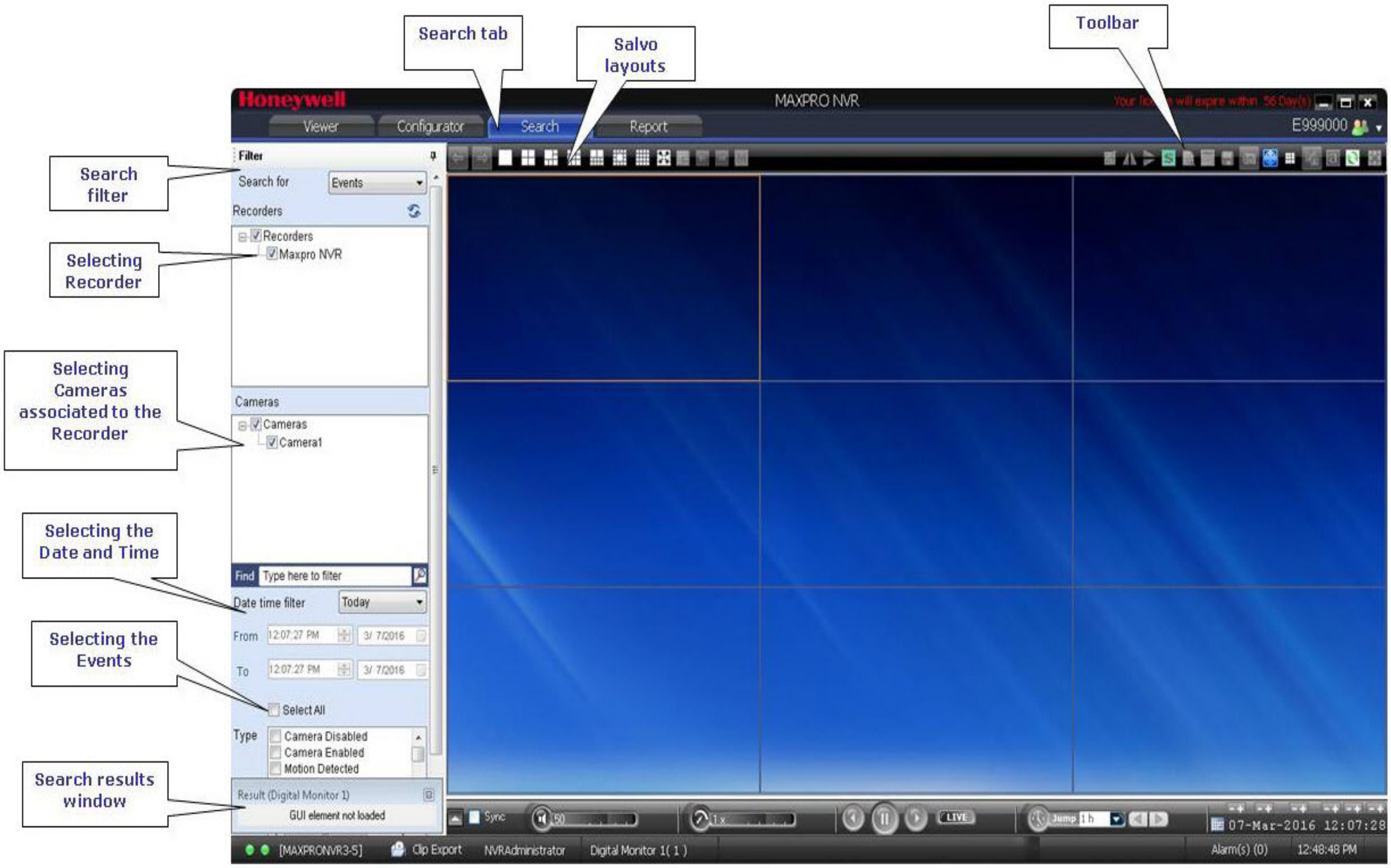


Figure 5-9 Search tab

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

Report Tab

Figure 5-10 illustrates the **Report** tab.

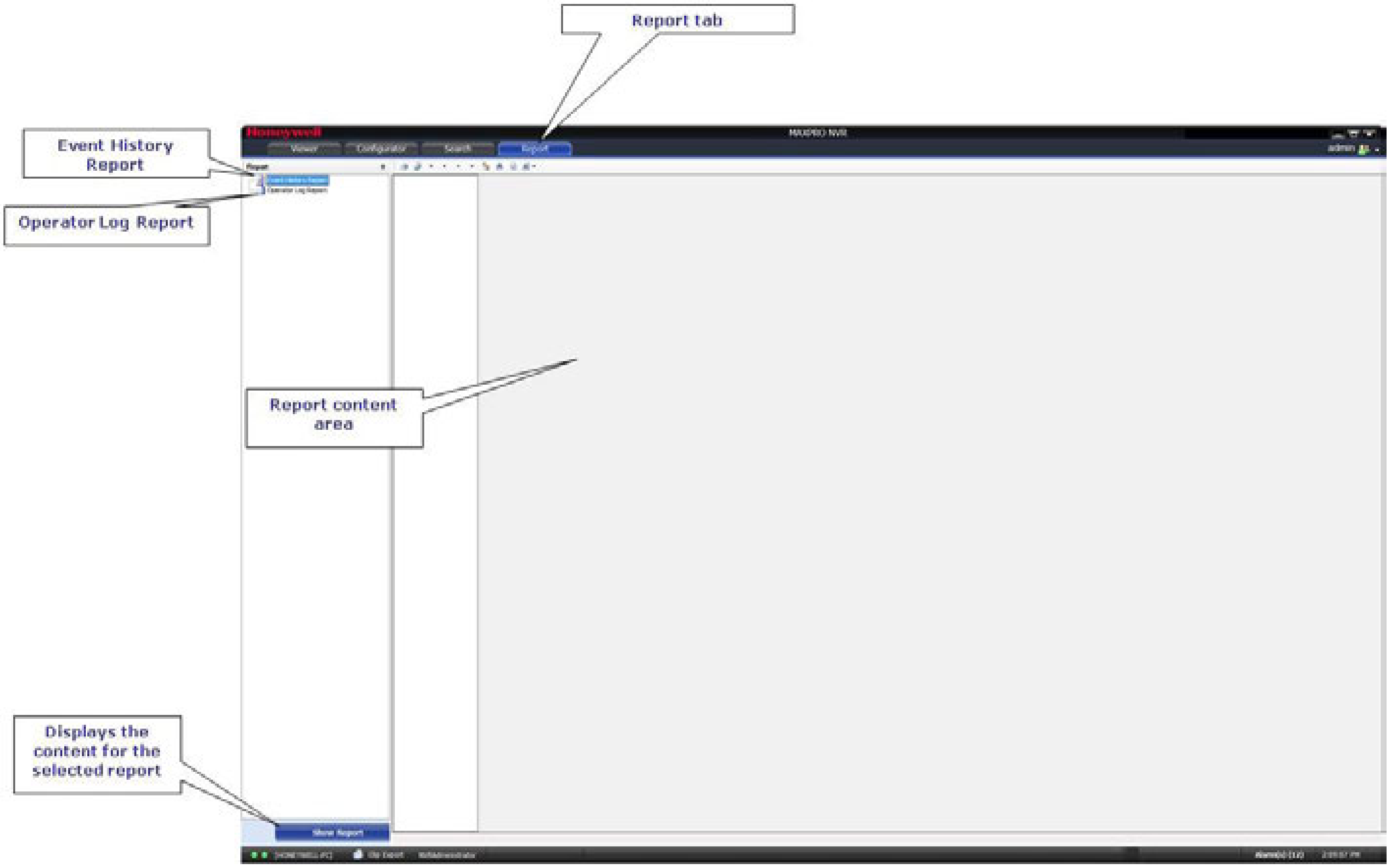


Figure 5-10 Report tab

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.

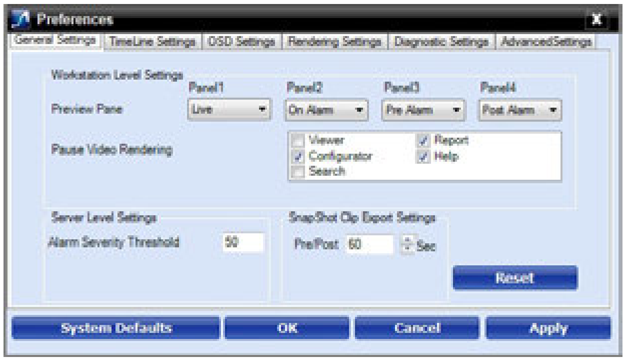
MAXPRO NVR supports three modes of encryption between client and server. On the Advance Settings tab you can select the options such as Default Encryption, Windows Authentication Encryption and Certificate Based Encryption under the Application Security Settings for secure communication.

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

1. Click the **Preferences** option in the user menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab (Figure 5-11) is selected.



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Live	On Alarm	Pre Alarm	Post Alarm

Pause Video Rendering: □ Viewer ☑ Configurator □ Search ☑ Report ☑ Help

Server Level Settings

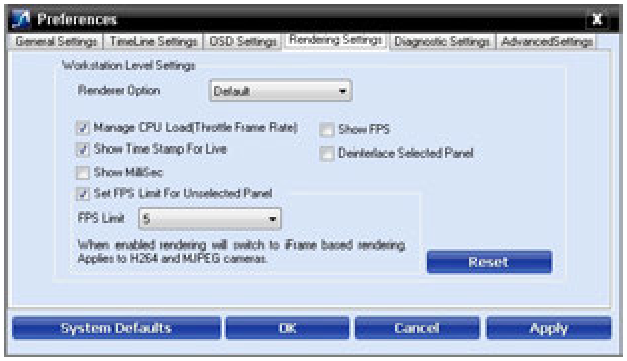
Alarm Severity Threshold 50

SnapShot Clip Export Settings

Pre/Post 60 Sec

Figure 5-11 General Settings tab

2. Click the **Rendering Settings** tab (Figure 5-12).



Workstation Level Settings

Renderer Option Default

☑ Manage CPU Load(Throttle Frame Rate)
☑ Show Time Stamp For Live
□ Show MilliSec
☑ Set FPS Limit For Unselected Panel
□ Show FPS
□ Deinterlace Selected Panel

FPS Limit 5

When enabled rendering will switch to iFrame based rendering.
Applies to H264 and MJPEG cameras.

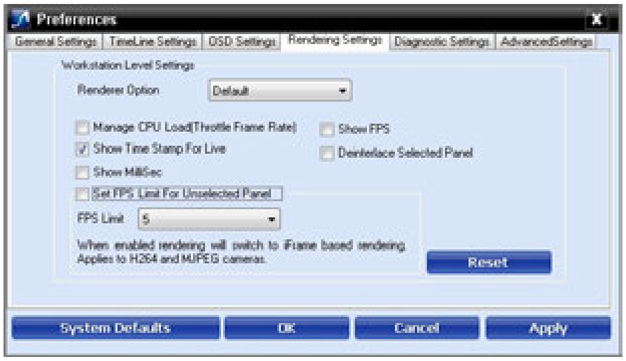
Figure 5-12 Rendering Settings tab

3. Select the **Renderer Option (Default/No Video Display)** for video rendering.
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.
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.
6. Select **Show MilliSec** check box if you want the milliseconds to be displayed in the timestamp on video.
7. Select **Show FPS** check box if you want the frames per second to be displayed on video.
8. Select the **Deinterlace Selected Panel** check box if you want to deinterlace the selected panel.
9. Select the check box beside **Set FPS Limit For Unselected Panel**.
10. Select the **FPS Limit**. The default frame rate is 5 fps and is the recommended setting for unselected panels.
11. Click **Apply**.
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).

1. Click the **Preferences** option in the user menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab is selected.
2. Click the **Rendering Settings** tab (Figure 5-13).



Workstation Level Settings

Renderer Option: Default

□ Manage CPU Load(Throttle Frame Rate)
☑ Show Time Stamp For Live
□ Show MilliSec
□ Set FPS Limit For Unselected Panel
□ Show FPS
□ Deinterlace Selected Panel

FPS Limit: 5

When enabled rendering will switch to iFrame based rendering.
Applies to H264 and MJPEG cameras.

Figure 5-13 Rendering Settings tab

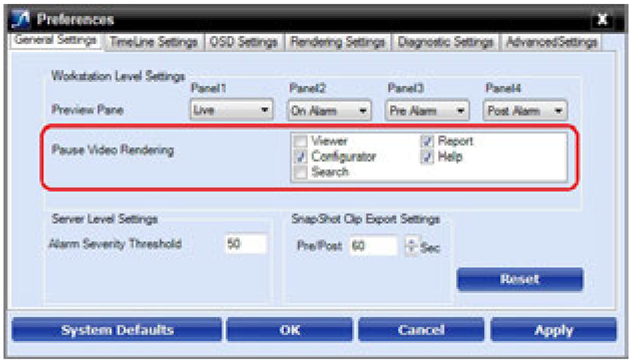
3. Clear the following check boxes:
   By default these two check boxes are selected.
   - Mange CPU Load (Throttle Frame Rate)
   - Set FPS Limit For Unselected Panel
4. Click **Apply**.
5. Click **OK** to close the dialog box.

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

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab is selected.
2. For **Pause Video Rendering**, select the check box next to the tab names that you want to select (Figure 5-14).



Preview Pane: Panel1 Live; Panel2 On Alarm; Panel3 Pre Alarm; Panel4 Post Alarm

Pause Video Rendering: ☐ Viewer ☑ Configurator ☐ Search ☑ Report ☑ Help

Alarm Severity Threshold: 50

Pre/Post: 60 Sec

Figure 5-14 Settings for pausing the Video Rendering

3. Click **Apply**.
4. Click **OK** to close the dialog box.

Settings for Alarm Preview Pane

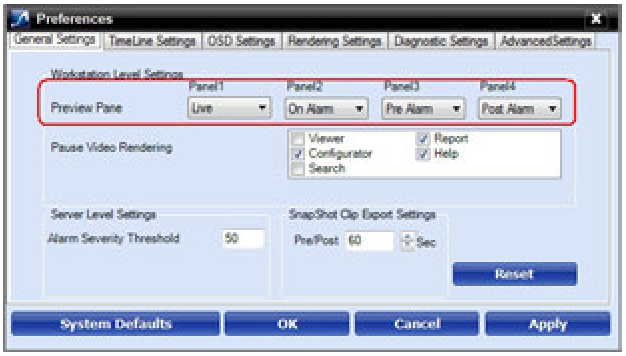
When the video related to an alarm is played from the **Alarm** window, the salvo layout changes to a four panel layout. You can define the video display for each panel namely, Pre Alarm, Post Alarm, Live, and On Alarm. The following table defines these options.

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.
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

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab is selected (Figure 5-15).
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	Live	On Alarm	Pre Alarm	Post Alarm

Pause Video Rendering: □ Viewer ☑ Configurator □ Search ☑ Report ☑ Help

Server Level Settings
Alarm Severity Threshold 50

SnapShot Clip Export Settings
Pre/Post 60 Sec

Figure 5-15 Settings for the Alarm Preview Pane

3. Click **Apply**.
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 304 for default Event and Alarm types and their severity levels for Camera, Recorder and SMART VMD.

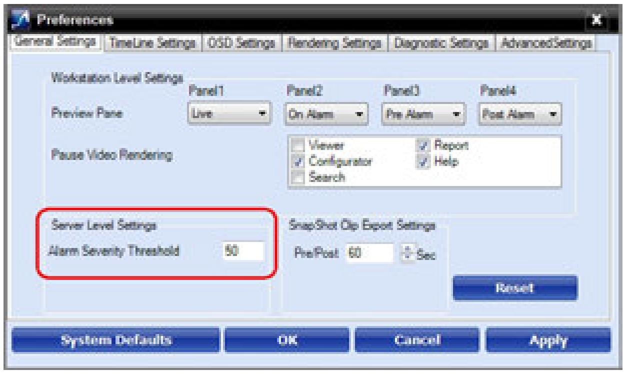
For example, the alarm is triggered if the **Severity Level** for an event is 50 and the **Alarm Severity Threshold** value is 40.

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

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab is selected (Figure 5-16).

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



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Live	On Alarm	Pre Alarm	Post Alarm

Pause Video Rendering: ☐ Viewer ☑ Configurator ☐ Search ☑ Report ☑ Help

Server Level Settings
Alarm Severity Threshold 50

SnapShot Clip Export Settings
Pre/Post 60 Sec

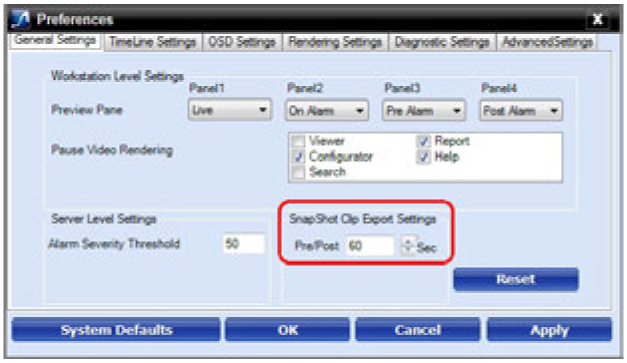
Figure 5-16 Setting the Alarm Threshold

3. Click **Apply**.
4. Click **OK** to close the dialog box.

Configuring the Snapshot Clip Export Settings

You can configure the time interval for the exported snapshot.

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box appears. By default, the **General Settings** tab is selected (Figure 5-17).
2. Under **SnapShot Clip Export Settings,** select the **Clip Export** time in seconds.



Workstation Level Settings

	Panel1	Panel2	Panel3	Panel4
Preview Pane	Live	On Alarm	Pre Alarm	Post Alarm

Pause Video Rendering: ☐ Viewer ☑ Configurator ☐ Search ☑ Report ☑ Help

Server Level Settings
Alarm Severity Threshold 50

SnapShot Clip Export Settings
Pre/Post 60 Sec

Figure 5-17 Settings for SnapShot Clip Export

3. Click **Apply**.
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.

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box (Figure 5-18) appears.

2. Click the **OSD Settings** tab.

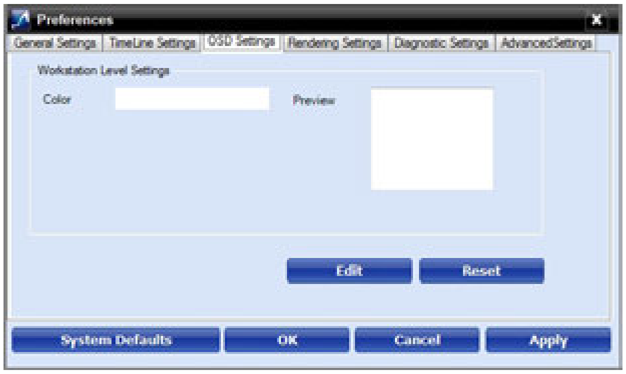
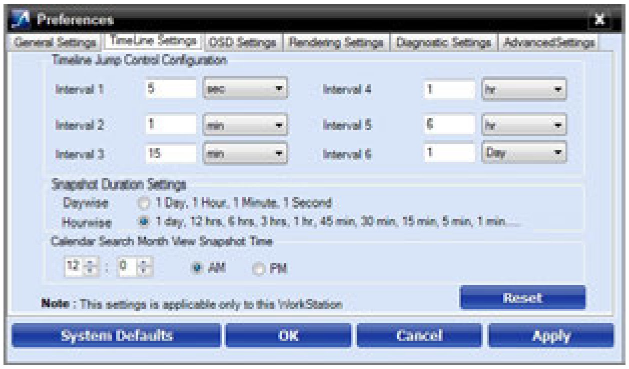


Figure 5-18 OSD Settings tab

3. Click **Edit** and select the font and color properties in the dialog box.
4. Click **OK** to close the font properties dialog box.
5. Click **Apply** in the **Preferences** dialog box.
6. Click **OK** to close the **Preferences** dialog box.

Configuring the Timeline Settings

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box (Figure 5-19) appears.
2. Click the **Timeline Settings** tab.



Timeline Jump Control Configuration

Interval 1	5	sec	Interval 4	1	hr
Interval 2	1	min	Interval 5	6	hr
Interval 3	15	min	Interval 6	1	Day

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

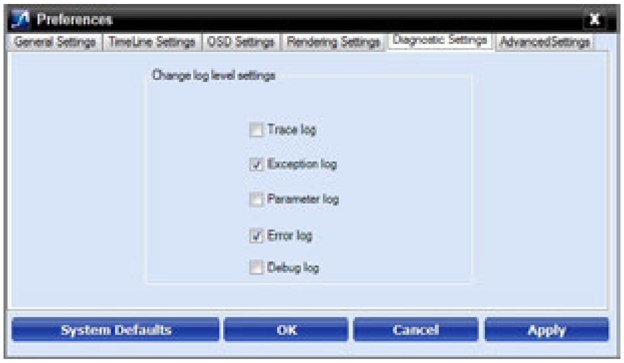
Note : This settings is applicable only to this WorkStation

Figure 5-19 Timeline Settings tab

3. Under **Timeline Jump Control Configuration**, set the time for the intervals (**Interval 1** to **Interval 6**) as applicable.
4. Under **Snapshot Duration Settings**, select the **Daywise** or **Hourwise** option button as applicable.
5. Under **Calendar Search Month View Snapshot Time**, type the preferred time and seconds and then click **AM** or **PM** as applicable.
6. Click **Apply**.
7. Click **OK** to close the **Preferences** dialog box.

Configuring the Diagnostic Settings

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box (Figure 5-20) appears.
2. Click the **Diagnostic Settings** tab.



Change log level settings

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

Figure 5-20 Diagnostic Settings tab

3. Under **Change log level settings**, select the check boxes corresponding to logs as applicable.
4. Click **Apply**.
5. Click **OK** to close the **Preferences** dialog box.

Configuring the Advanced Settings

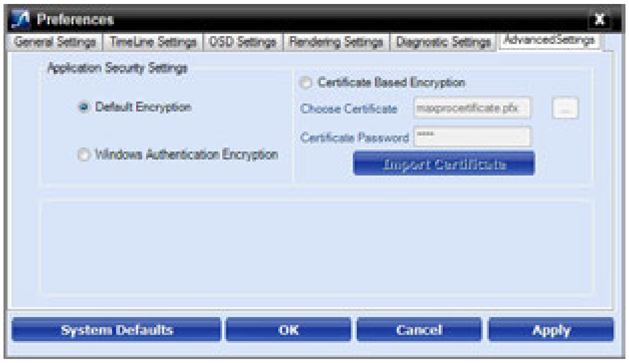
Encryption secures the communication between server and client. You can encrypt the data between client to server using encryption feature. MAXPRO NVR supports three types of encryption modes to communicate with NVR box through client. Each encryption has specific pre-requisites. The following are the 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**:
  - System clock time should be synced 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.

To configure the Advanced settings

1. Click the **Preferences** option in the **User** menu, . The **Preferences** dialog box (Figure 5-21) appears.
2. Click the **Advanced Settings** tab.



Application Security Settings

● Default Encryption

○ Windows Authentication Encryption

○ Certificate Based Encryption

Choose Certificate: maxprocertificate.pfx

Certificate Password: ****

Figure 5-21 Advanced Settings Tab

3. Under Application Security Settings, select the **Default Encryption** or **Windows Authentication Encryption** option button as applicable.
   Or

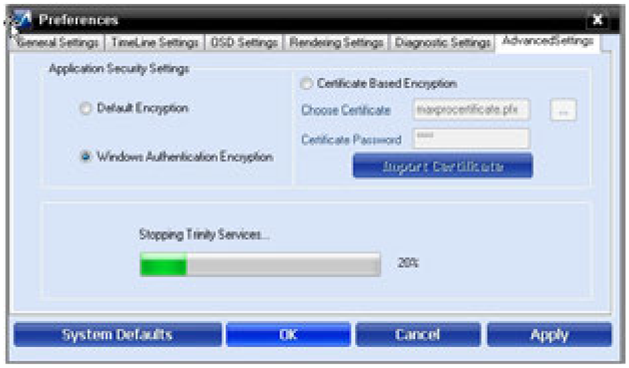
If you select the **Certificate Based Encryption** option button, then a certificate is used for encrypting the data between client and server. To encrypt the data using **Certificate Based Encryption,** perform the following:

a. Browse the certificate (.pfx file).

b. 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

4. 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%

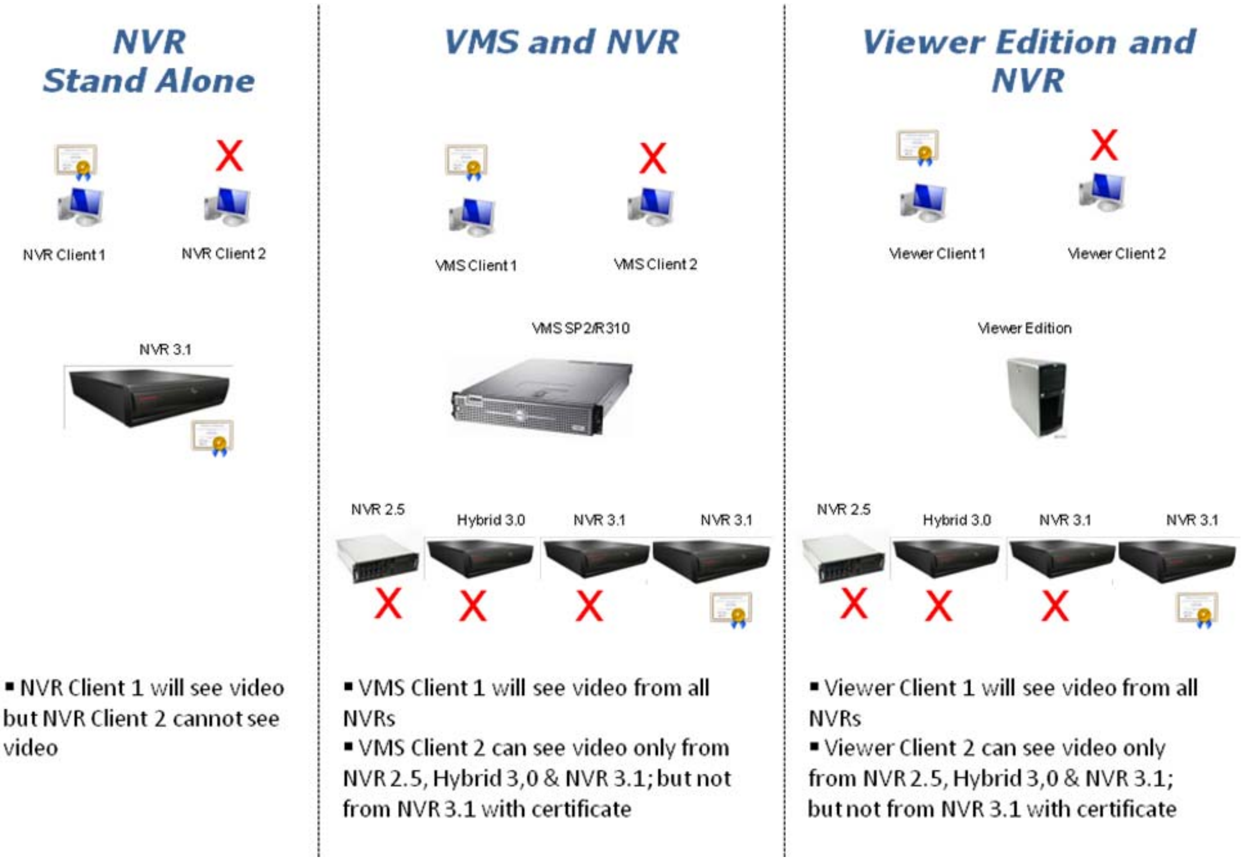
Figure 5-22 Advance Settings Tab Service Restart

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

5. Click **Apply** to close the **Preferences** dialog box.

Encryption Certificate deployment scenario

The following figures depicts the Encryption certificate deployment scenarios:



- NVR Client 1 will see video but NVR Client 2 cannot see video

- VMS Client 1 will see video from all NVRs
- VMS Client 2 can see video only from NVR 2.5, Hybrid 3,0 & NVR 3.1; but not from NVR 3.1 with certificate

- Viewer Client 1 will see video from all NVRs
- Viewer Client 2 can see video only from NVR 2.5, Hybrid 3,0 & NVR 3.1; but not from NVR 3.1 with certificate

Configuring the Default Settings

1. Click **Reset** to apply default settings while setting preferences.
2. Click **System Defaults** to apply the system default settings while setting preferences.

Licensing Information

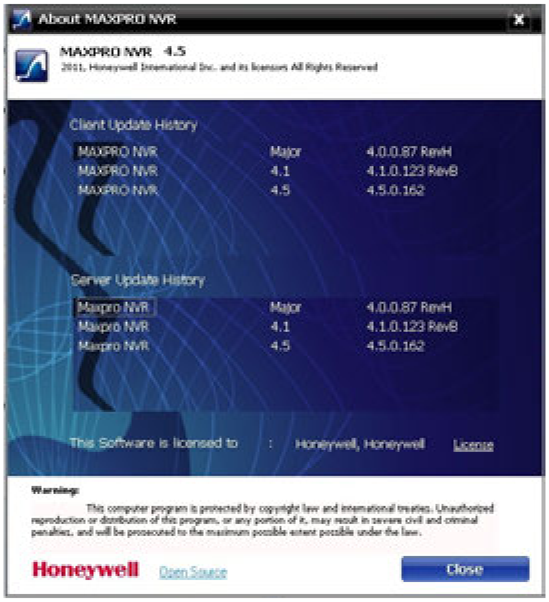
Viewing the Version and License Information of MAXPRO NVR

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.

1. From the **User menu** on the top right, click **About** from the drop-down list. The version information of MAXPRO NVR appears Figure 5-23.



About MAXPRO NVR

MAXPRO NVR 4.5
2011, Honeywell International Inc. and its licensors All Rights Reserved

Client Update History

MAXPRO NVR	Major	4.0.0.87 RevH
MAXPRO NVR	4.1	4.1.0.123 RevB
MAXPRO NVR	4.5	4.5.0.162

Server Update History

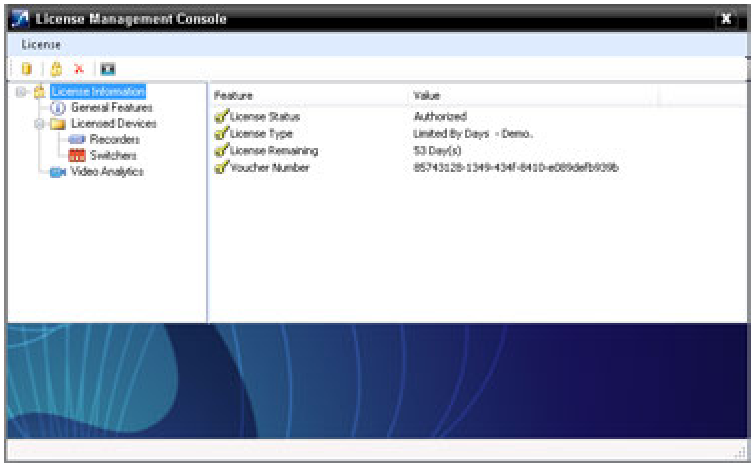
Maxpro NVR	Major	4.0.0.87 RevH
Maxpro NVR	4.1	4.1.0.123 RevB
Maxpro NVR	4.5	4.5.0.162

This Software is licensed to : Honeywell, Honeywell License

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 possible under the law.

Figure 5-23 About MAXPRO NVR

2. Click the **License** option. The **License Management Console** dialog box Figure 5-24 appears.



Feature	Value
License Status	Authorized
License Type	Limited By Days - Demo.
License Remaining	53 Day(s)
Voucher Number	85743128-1349-434f-8410-e089defb939b

Figure 5-24 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.

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 Getting Started 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.

1. Download the License Certificate file and save it to a USB flash drive.
2. Launch MAXPRO NVR on the MAXPRO NVR Server.
3. From the **User** menu, click **About**.
4. On the **MAXPRO® NVR** dialog box, click **License**.
5. On the **License Management Console** dialog box, select **Install License** in the **License** drop-down list.
6. The **New License Configuration Wizard** launches. Click **Next**.
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**.
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.

9. On the **Device Configuration Changes** dialog box, check that the details are accurate, and then click **Next**.
10. On the **Confirm New License** dialog, click **Finish**.
11. On the **New License Configuration Wizard** dialog box, click **Yes**.

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.

1. Click the **User** menu, . The user menu options appear.
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.

1. Click the **User** menu, . The user menu options appear.
2. Click **Exit**. A dialog box appears prompting you to confirm the action.
3. Click **Yes**.

This page is intentionally left blank.

6

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.

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

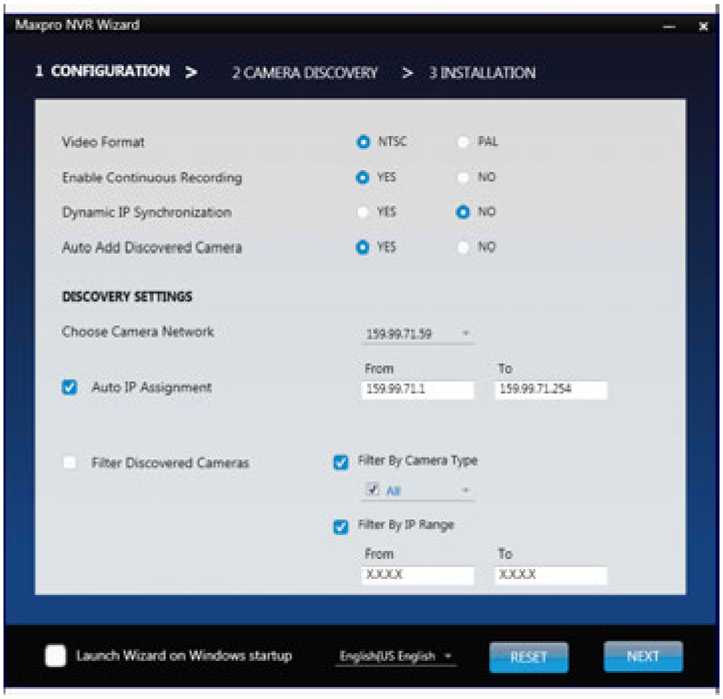
Caution: The Firewall settings are pre-configured for boxed solutions – MAXPRO NVR XE, SE, PE and MAXPRO NVR Hybrid XE, SE, PE. For MAXPRO NVR Software-Only solution, the Firewall settings are automatically configured during the installation process.

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)

1. **Step 1** - The **CONFIGURATION** page (Figure 6-1) 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

Figure 6-1 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.

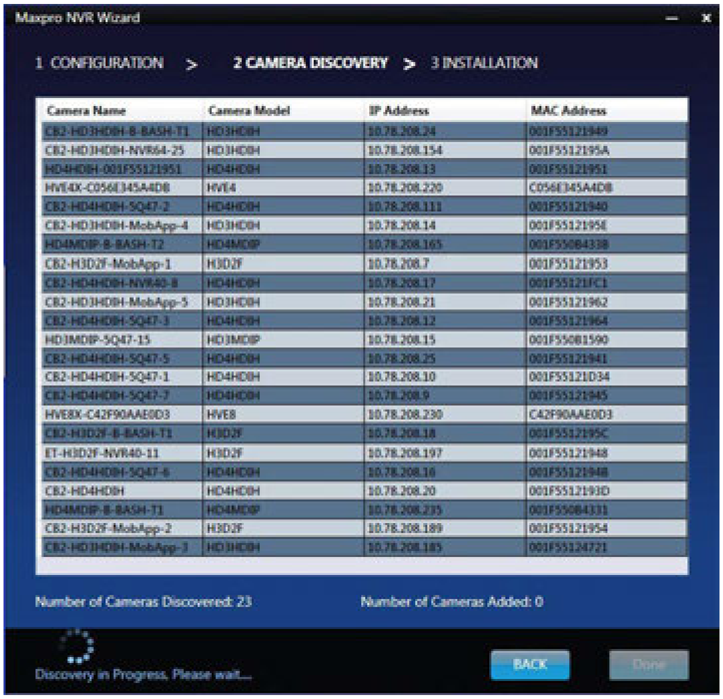
Field	Description
CONFIGURATION SETTINGS	
Video Format	Select “NTSC” or “PAL” based on your region.

Field	Description
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.
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.

2. Step 2 - The **CAMERA DISCOVERY** page (Figure 6-2) appears.



Camera Name	Camera Model	IP Address	MAC Address
CB2-HD3HD0H-8-BASH-T1	HD3HD0H	10.78.208.24	001F55121949
CB2-HD3HD0H-NVR64-25	HD3HD0H	10.78.208.154	001F5512195A
HD4HD0H-001F55121951	HD4HD0H	10.78.208.13	001F55121951
HVE4X-C056E345A4D8	HVE4	10.78.208.220	C056E345A4D8
CB2-HD4HD0H-5Q47-2	HD4HD0H	10.78.208.111	001F55121940
CB2-HD3HD0H-MobApp-4	HD3HD0H	10.78.208.14	001F5512195E
HD4MDIP-8-BASH-T2	HD4MDIP	10.78.208.165	001F550B433B
CB2-H3D2F-MobApp-1	H3D2F	10.78.208.7	001F55121953
CB2-HD4HD0H-NVR40-8	HD4HD0H	10.78.208.17	001F55121FC1
CB2-HD3HD0H-MobApp-5	HD3HD0H	10.78.208.21	001F55121962
CB2-HD4HD0H-5Q47-3	HD4HD0H	10.78.208.12	001F55121964
HD3MDIP-5Q47-15	HD3MDIP	10.78.208.15	001F550B1590
CB2-HD4HD0H-5Q47-5	HD4HD0H	10.78.208.25	001F55121941
CB2-HD4HD0H-5Q47-1	HD4HD0H	10.78.208.10	001F55121D34
CB2-HD4HD0H-5Q47-7	HD4HD0H	10.78.208.9	001F55121945
HVE8X-C42F90AAE0D3	HVE8	10.78.208.230	C42F90AAE0D3
CB2-H3D2F-8-BASH-T1	H3D2F	10.78.208.18	001F5512195C
ET-H3D2F-NVR40-11	H3D2F	10.78.208.197	001F55121948
CB2-HD4HD0H-5Q47-6	HD4HD0H	10.78.208.16	001F55121948
CB2-HD4HD0H	HD4HD0H	10.78.208.20	001F5512193D
HD4MDIP-8-BASH-T1	HD4MDIP	10.78.208.235	001F550B4331
CB2-H3D2F-MobApp-2	H3D2F	10.78.208.189	001F55121954
CB2-HD3HD0H-MobApp-3	HD3HD0H	10.78.208.185	001F55124721

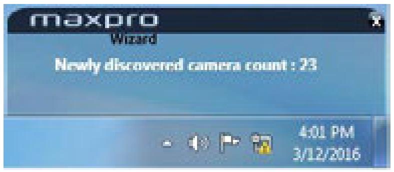
Number of Cameras Discovered: 23

Number of Cameras Added: 0

Discovery in Progress, Please wait...

Figure 6-2 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.

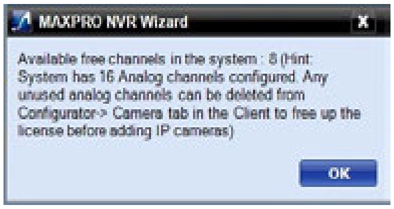


Newly discovered camera count : 23

Figure 6-3 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.



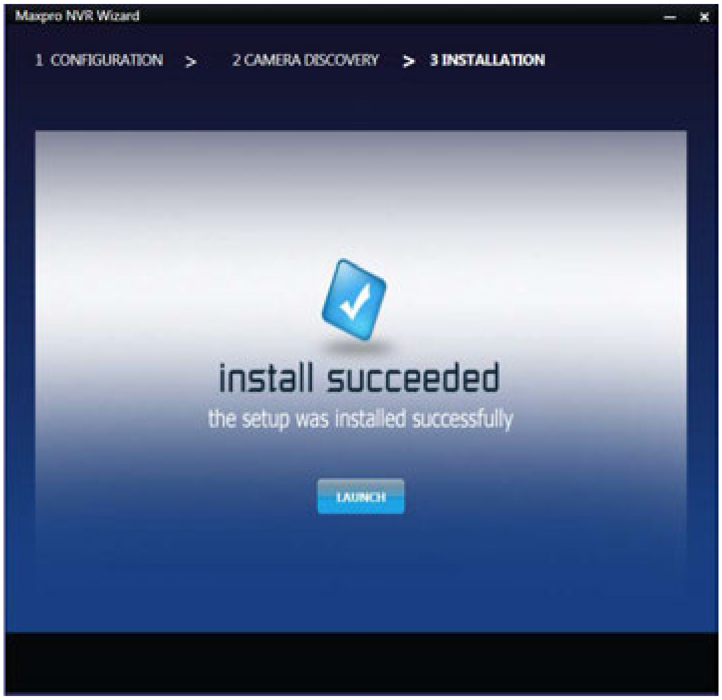
Available free channels in the system : 8 (Hint: System has 16 Analog channels configured. Any unused analog channels can be deleted from Configurator-> Camera tab in the Client to free up the license before adding IP cameras)

- 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 140. For adding and configuring third party RTSP cameras, the RTSP settings must be specified, see Adding RTSP Cameras/Encoders section on page 144.

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.

3. Step 3 - The **INSTALLATION** page (Figure 6-4) appears.



install succeeded

the setup was installed successfully

Figure 6-4 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.

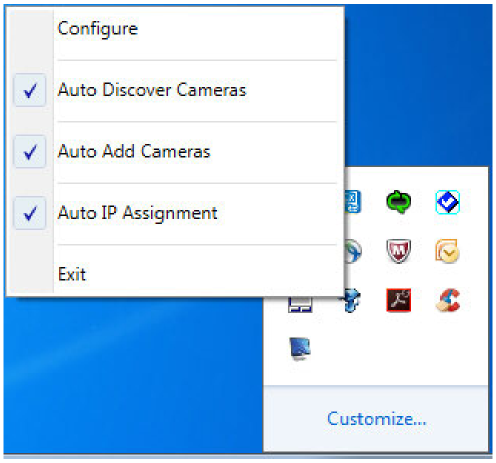


Figure 6-5 MAXPRO NVR Wizard Task bar Settings

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

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 58 section for more information.

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

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.

5. Click **Login**. The **Viewer** screen appears by default.
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.
- **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.
- **Site Info** - enable configuring and displaying the Site info and License type 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 (Figure 6-6) appears by default.

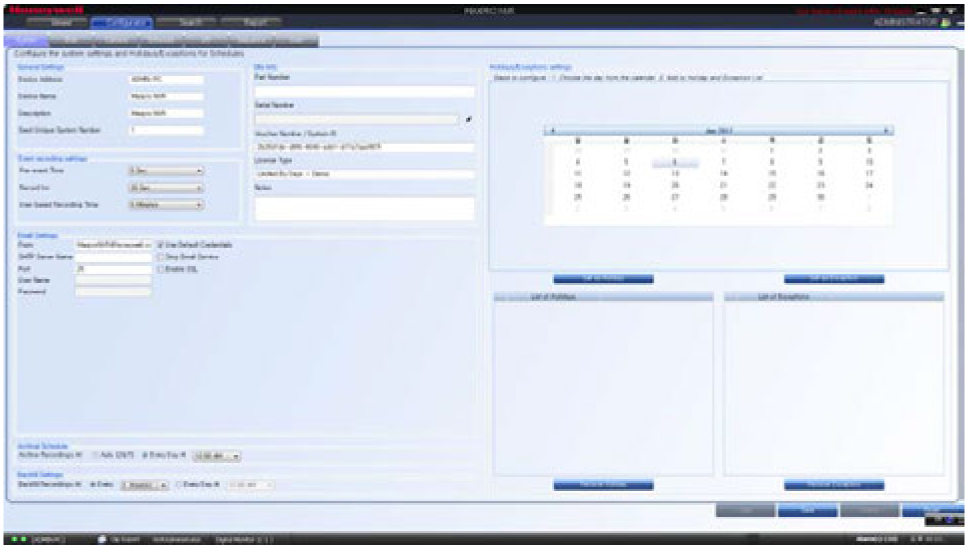


Figure 6-6 System page

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.

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 124 for more 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.

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 stop the synchronizing process at certain point of time. You can set time in minutes. The synchronizing process starts once it overshoots the limit time.

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 124.

To perform manual archive:

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

3. Click at the bottom of the pane. The **Clip Archival is in progress**. **Please Wait..**. message is displayed Figure 6-7.

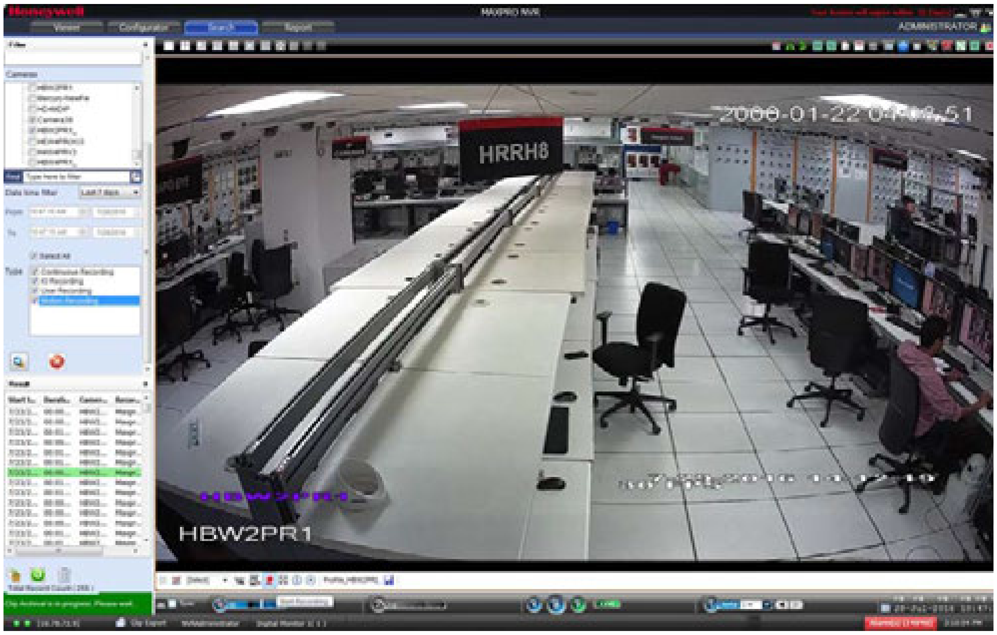


Figure 6-7 Archive Progress

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 (Figure 6-7) and a **Manual** archival folder is created automatically for the respective camera. If it fails then the selected clips are displayed in **Pink** color.

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.

Holidays/Exceptions Settings

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

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

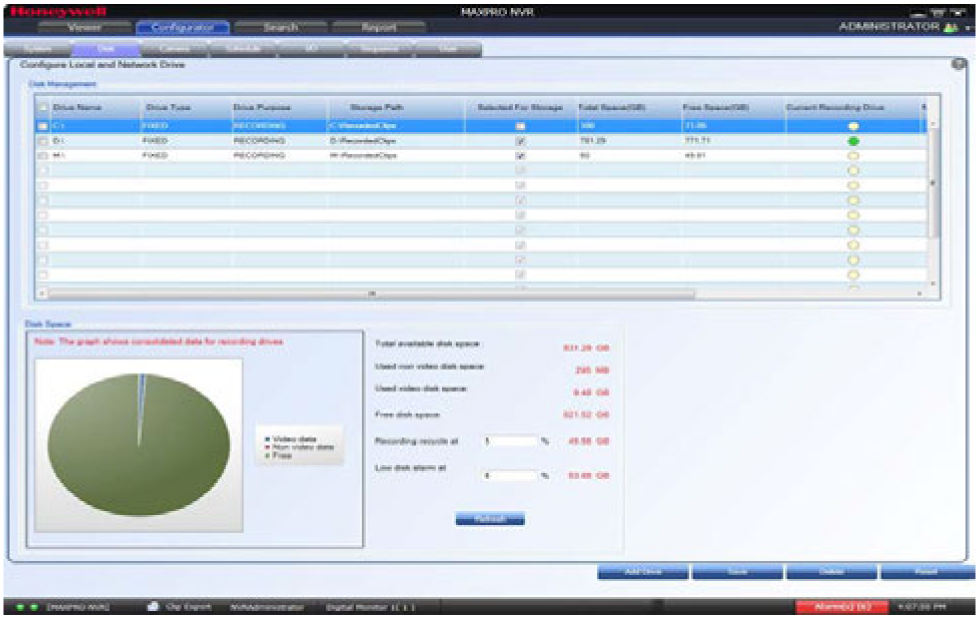
- Under **List of Holidays**, select the check box for the holiday you want to remove, and then click **Remove Holiday**.
- Select the check box for the exception you want to remove, and click **Remove Exception**.

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.

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Disk** tab to open the **Disk Management** page Figure 6-8.



☐	Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For Storage	Total Space(GB)	Free Space(GB)	Current Recording Drive
☐	C:\	FIXED	RECORDING	C:\RecordedClips	☐	100	71.06	○
☐	D:\	FIXED	RECORDING	D:\RecordedClips	☑	781.29	771.71	●
☐	H:\	FIXED	RECORDING	H:\RecordedClips	☑	50	49.81	○

Total available disk space 831.29 GB
Used non video disk space 295 MB
Used video disk space 9.48 GB
Free disk space 821.52 GB
Recording recycle at 5 % 49.58 GB
Low disk alarm at 6 % 53.68 GB

Figure 6-8 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.

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).
   - **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.

- **NAS Password** - Type the password to access the NAS

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 see Figure 6-9.

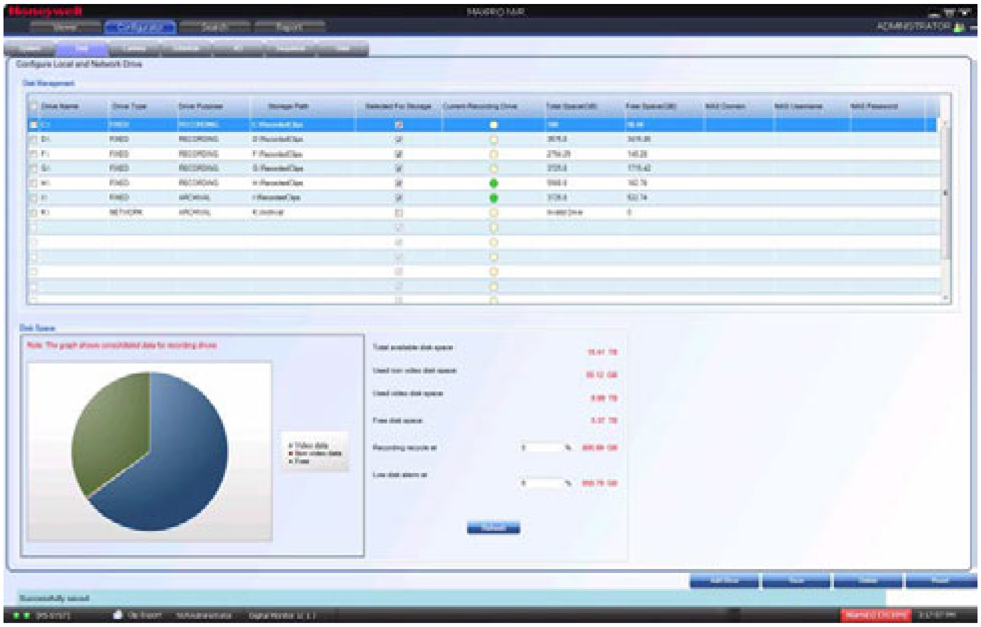


Figure 6-9 Graphical Illustration

- 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.

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 a network drive in the following format: \\**<IP address >****<folder name>** for example, \\**192.168.1.12****Recorded Clips**.

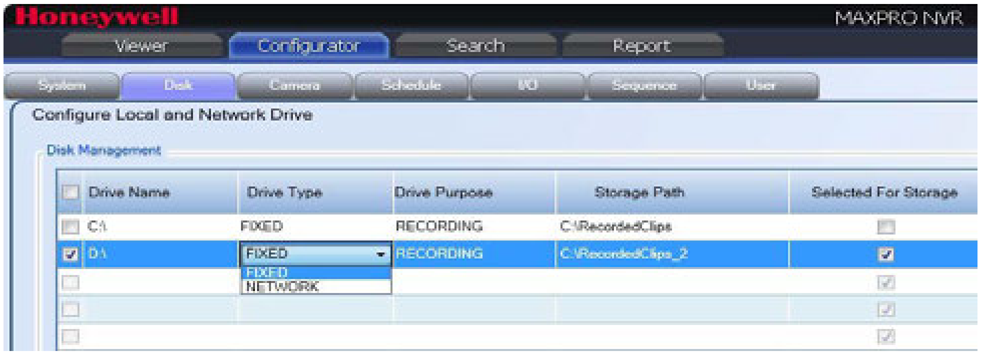
Note: The Network drive added must be valid with proper folder permissions set for the installed default user, else an **Invalid Drive** text displays in the **Total Space (GB)** column.

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.

6. Click **Save** to save the information or click **Reset** to clear the information entered.

Removing a drive

1. Select the check box corresponding to the drive you want to remove as shown in Figure 6-9.



Configure Local and Network Drive

Disk Management

□	Drive Name	Drive Type	Drive Purpose	Storage Path	Selected For Storage
□	C:\	FIXED	RECORDING	C:\RecordedClips	□
☑	D:\	FIXED FIXED NETWORK	RECORDING	C:\RecordedClips_2	☑
□					☑
□					☑
□					☑

Figure 6-10 Drive Type

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:

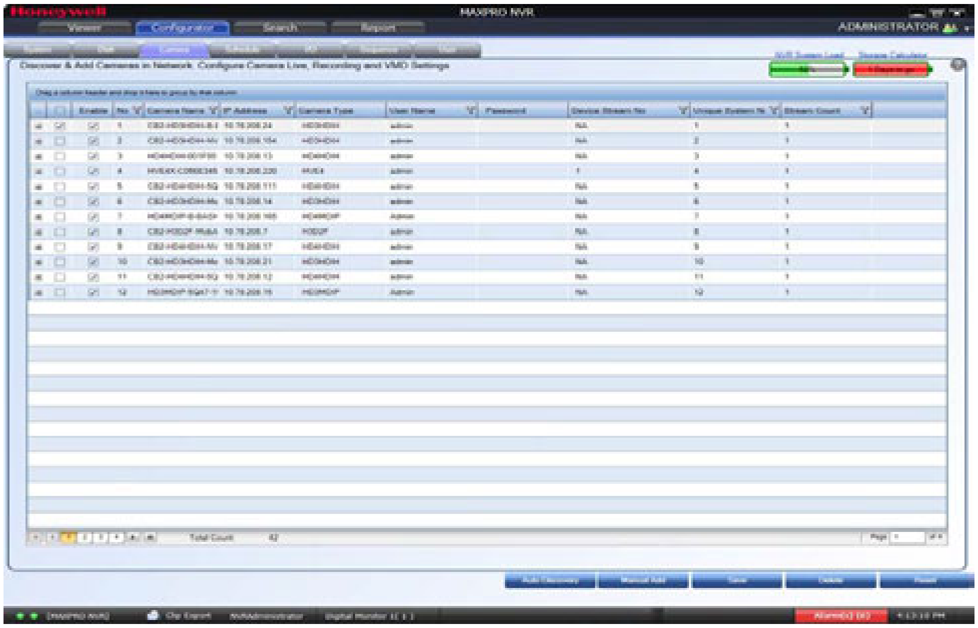
- **IP Cameras**/**Encoders**: MAXPRO NVR can automatically discovers these devices in the network and adds it to the MAXPRO NVR user interface. See the Adding IP Cameras / Encoders section on page 128 for more information.
- **Analog Cameras**: User is required to manually add these cameras to the respective channel and configure the camera. See the Adding/Deleting Analog Cameras section on page 159 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.

To add IP cameras

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to open the **Camera** page Figure 6-11.


Honeywell
MAXPRO NVR
Viewer
Configurator
Search
Report
ADMINISTRATOR
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
Total Count
Auto Discovery
Manual Add
Save
Delete
Reset

	☐	Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
	☑	☑	1	[illegible]	10.78.208.24	HD3HDH	admin		NA	1	1
	☐	☑	2	[illegible]	10.78.208.154	HD3HDH	admin		NA	2	1
	☐	☑	3	[illegible]	10.78.208.13	HD4HDH	admin		NA	3	1
	☐	☑	4	[illegible]	10.78.208.220	HVE4	admin		1	4	1
	☐	☑	5	[illegible]	10.78.208.111	HD4HDH	admin		NA	5	1
	☐	☑	6	[illegible]	10.78.208.14	HD3HDH	admin		NA	6	1
	☐	☑	7	[illegible]	10.78.208.105	HD4MDIP	Admin		NA	7	1
	☐	☑	8	[illegible]	10.78.208.7	HD2P	admin		NA	8	1
	☐	☑	9	[illegible]	10.78.208.17	HD4HDH	admin		NA	9	1
	☐	☑	10	[illegible]	10.78.208.21	HD3HDH	admin		NA	10	1
	☐	☑	11	[illegible]	10.78.208.12	HD4HDH	admin		NA	11	1
	☐	☑	12	[illegible]	10.78.208.15	HD3MDIP	Admin		NA	12	1

Figure 6-11 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.

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 136 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.

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 Camera Properties section on page 132 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 144 for more information.
- To add the discovered multi-channel encoders, see the Discovering and Adding Multi-channel Encoders section on page 141.

- **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.

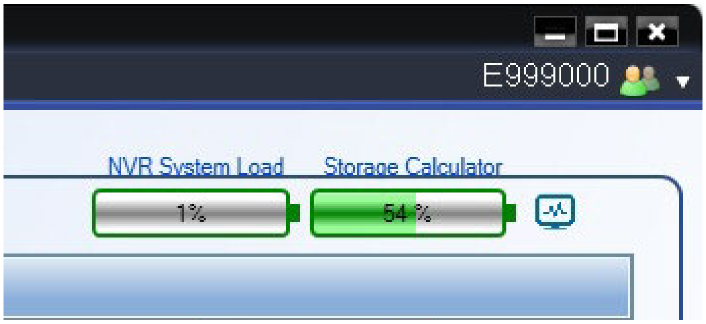
- **Device Stream No** - Displays the channel ID. You cannot modify this field.
- **Unique System No** - Display the unique camera ID. You can modify and assign a new number as applicable.

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.

- **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** -



  - **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.

- **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.

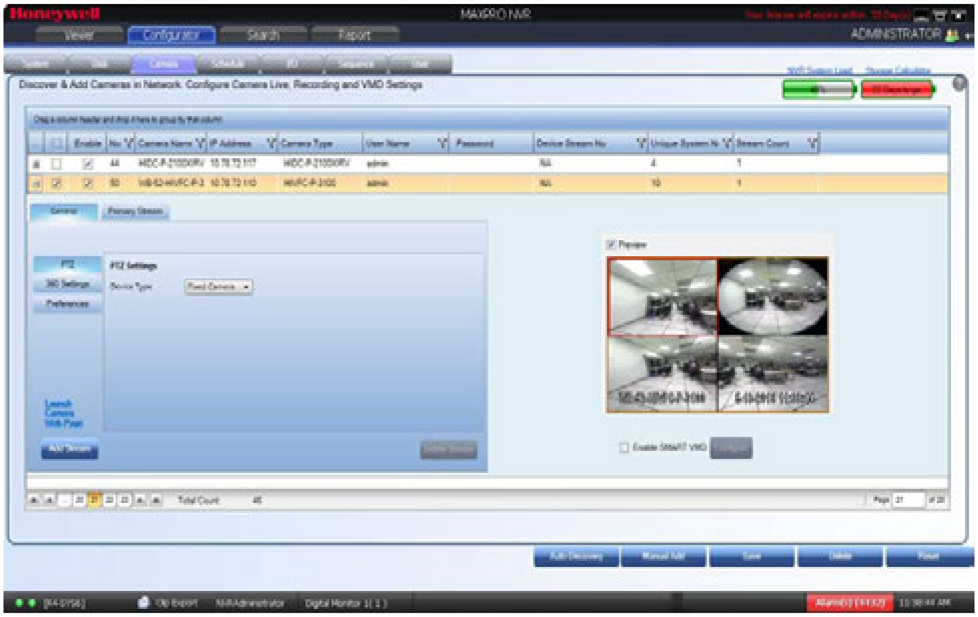
Note:

- 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.

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 Camera Properties

5. For the required camera, click ⊞ on the left corner to open the camera properties pane see Figure 6-12.



		Enable	No	Camera Name	IP Address	Camera Type	User Name	Password	Device Stream No	Unique System N	Stream Count
⊞	□	☑	44	HDC-P-2100DRV	10.78.72.117	HDC-P-2100DRV	admin		NA	4	1
⊟	☑	☑	50	[illegible]	10.78.72.110	[illegible]	admin		NA	10	1

Figure 6-12 Camera Properties pane

6. 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.

7. 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.

8. 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 **AO**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.

- **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***.

9. 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.
   - **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.

10. 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.

Limitations of H.265 Codec Type:

- H.265 is not supported in MAXPRO Mobile app
- H.265 is not supported in Web client.

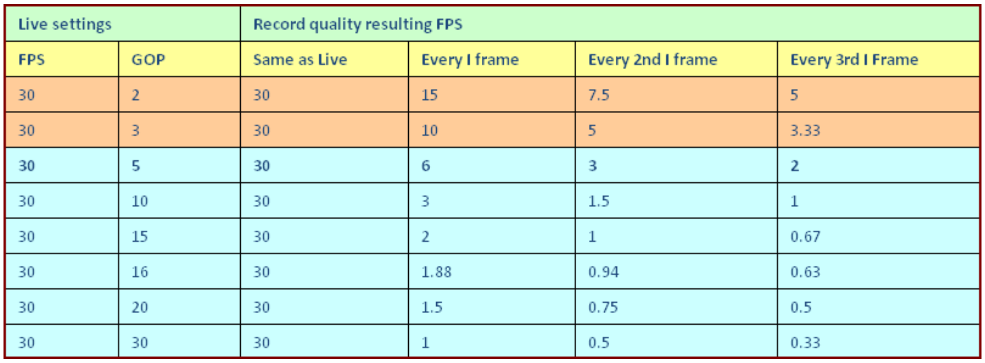
Note: Only HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D and HDZ302DIN model cameras support H.265 Codec type.

- **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.

- 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.

11. 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:**
        - Select the **Event Recording** video deletion duration.
        - Select the **Continuous Recording** video 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.
12. Under **Primary Stream > Preferences > Stream Preferences Settings.** See step 9 for more information.
13. 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 Figure 6-13.

Note: Auto Discovery Settings are only applicable for Honeywell, AXIS and ONVIF cameras.

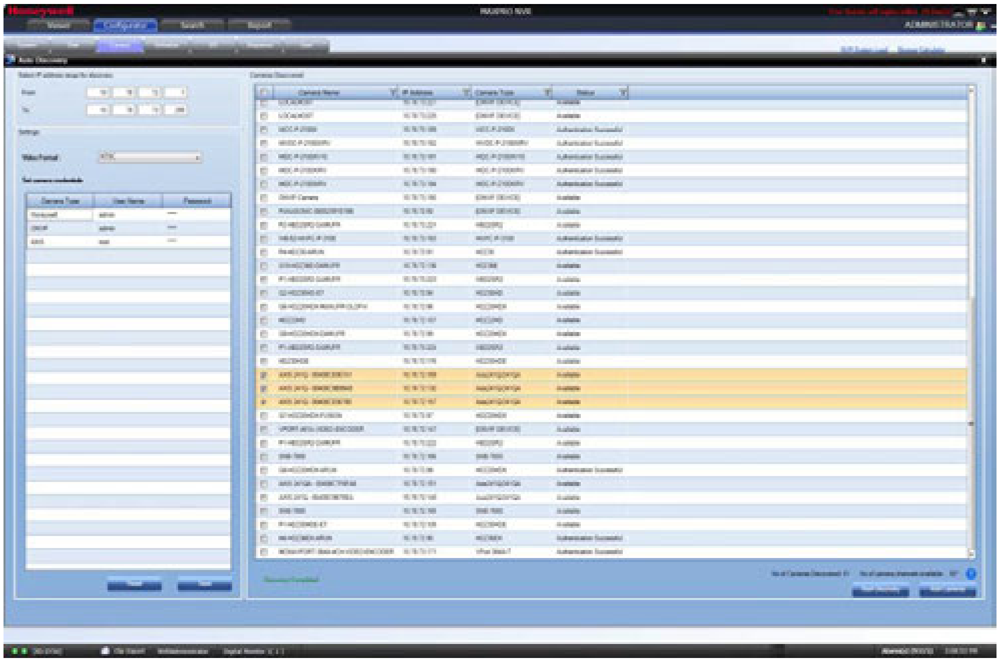


Figure 6-13 Auto Discovery Window

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.

To configure the additional streams for a camera

1. Click the **Camera** tab, the camera page is displayed with the list of cameras discovered.
2. For the required camera, click ⊞ on the left corner, the camera properties pane is displayed see Figure 6-14.

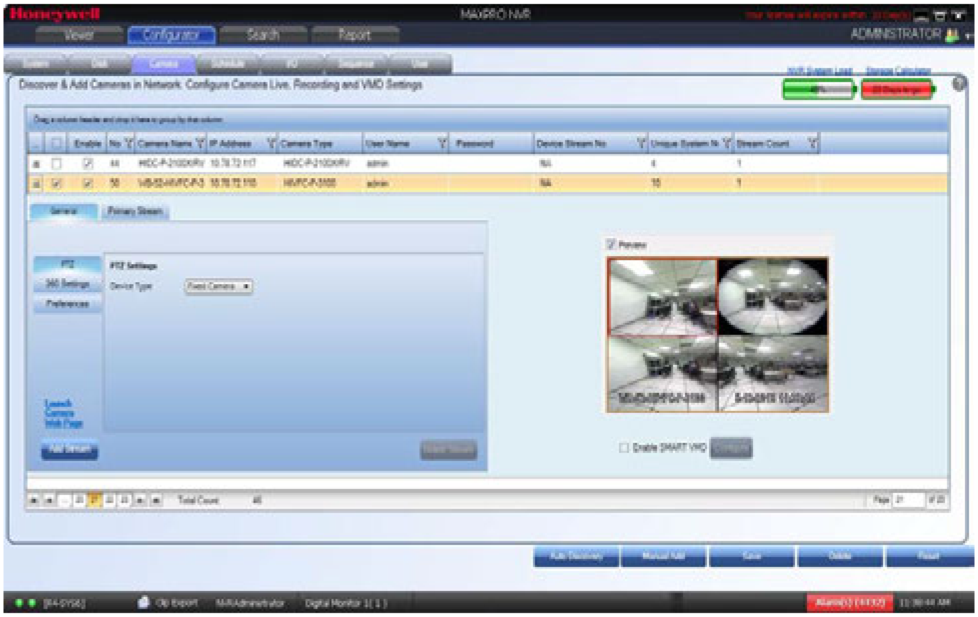


Figure 6-14 Camera Properties Pane

3. Click the **Add Stream** button, an additional stream (Stream 2) is added see Figure 6-15.

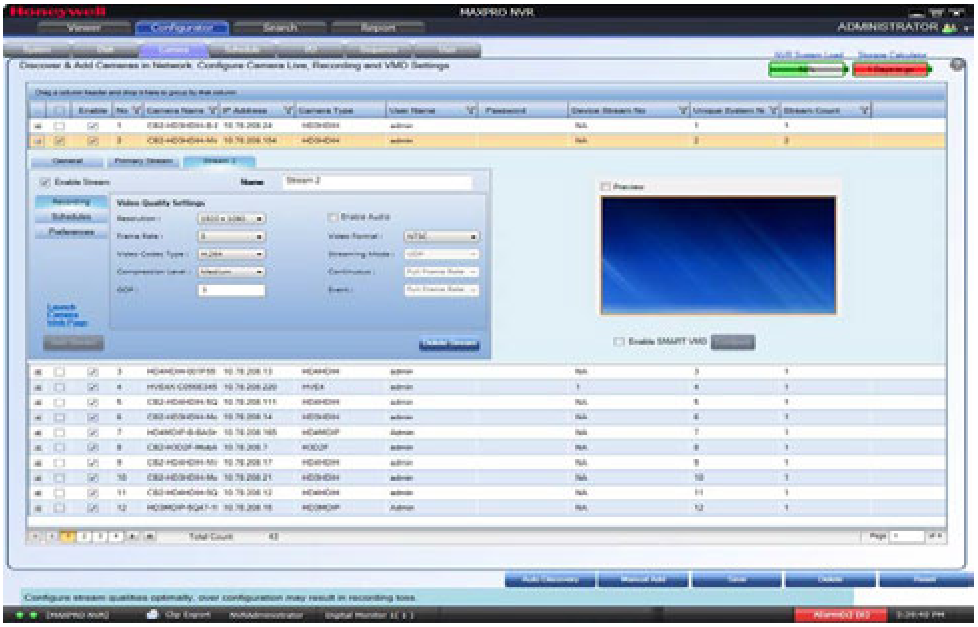


Figure 6-15 Adding Stream

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 encorders.

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.
5. For the Stream 2 **Recording, Schedules, Preference** settings, repeat step 10 through step 13 of Configuring Camera Properties section on page 132. Similarly you can add and configure multiple streams for a camera.

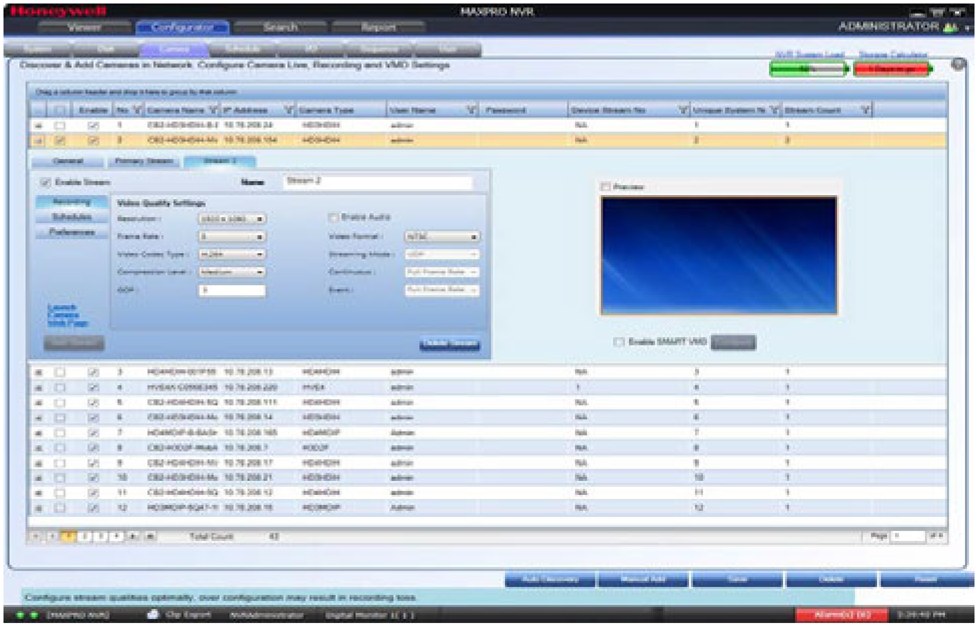
Note: Ensure that the Resolution and FPS should match with the Camera and the NVR secondary stream settings, else live video can not be displayed.

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

1. For the required camera, click ⊞ on the left corner, the camera properties pane is displayed see Figure 6-14.



Note: If an additional stream is added then only the **Delete Stream** button is enabled.

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.
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.

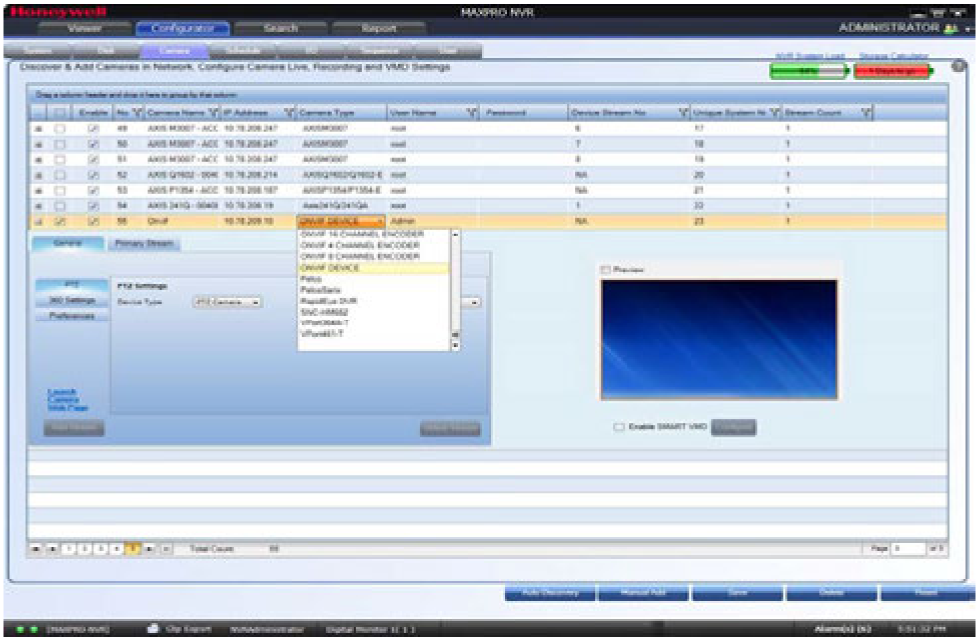


Figure 6-16 Camera Type field displaying "ONVIF DEVICE" for a ONVIF camera

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 306.

To add third party ONVIF cameras in MAXPRO NVR through Auto Discovery

1. In the **Camera** page, click the **Auto Discovery** button. After the discovery select the required check boxes of third party ONVIF cameras.
2. Under **Settings**, select the **Video Format** from the drop-down list.
3. Under **Set camera credentials,** type the **User Name** and **Password** of the third party ONVIF camera.
4. Click **Save**.
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.

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.
2. Type the **Camera Name** and **IP Address**.
3. Type the **User Name** and **Password** of the ONVIF device.
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.

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 encorders.

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 in the Figure 6-17.

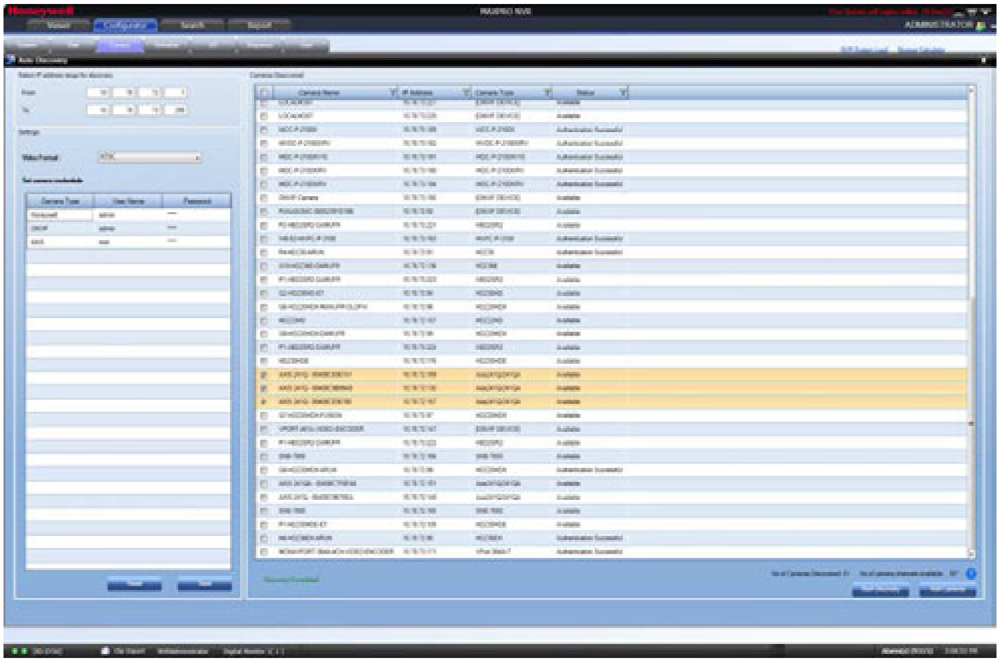


Figure 6-17 Encoder discovery

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 306.
- 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 encorders.

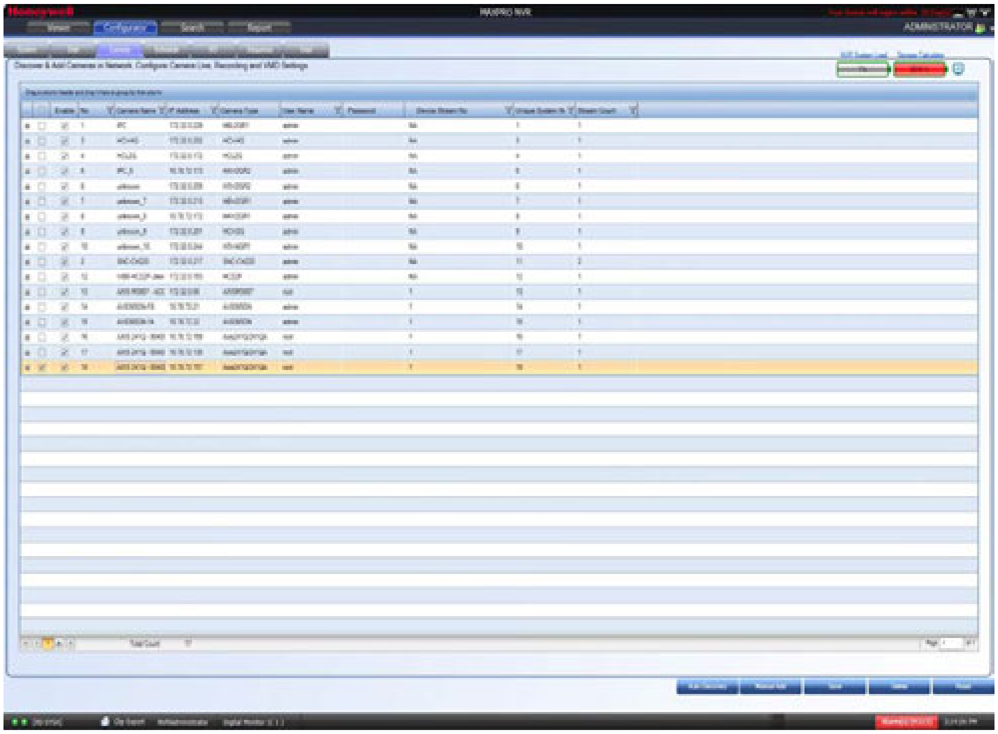


Figure 6-18 Adding the Encoder

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

1. In MAXPRO NVR, click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to open the **Camera** page.
3. Click **Manual Add**. A new camera is added under **Camera** list.
4. Type the required **Camera Name**.
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.
6. Select the required FLIR Series model camera from the **Camera Type** drop-down list as shown below (Figure 6-19) for example **FLIR F-Series**).

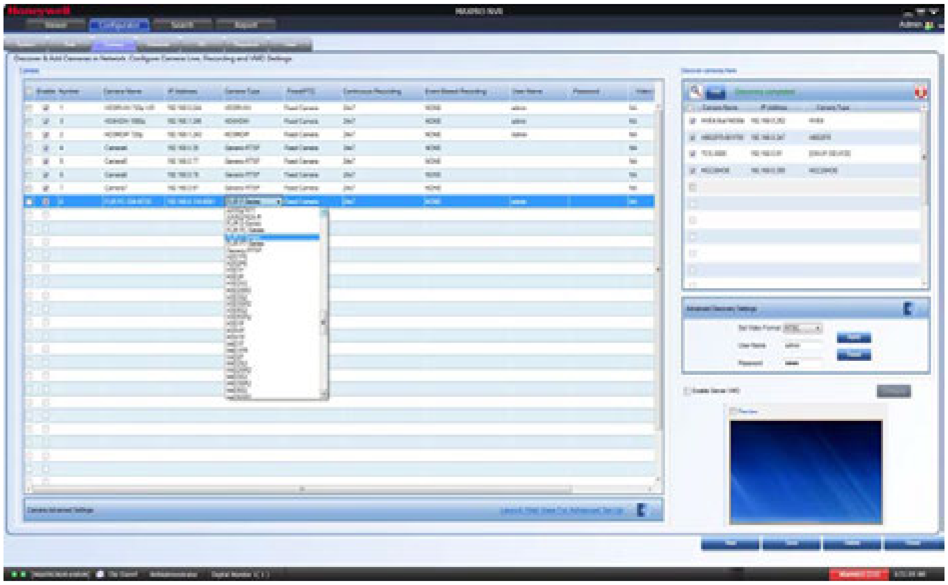


Figure 6-19 Adding FLIR Model Camera

7. Scroll right to manually type the **User Name** and **Password**. The default user name is **admin** and password is **admin**.

8. Click **Save**. A new FLIR series camera is added as shown below (Figure 6-20).

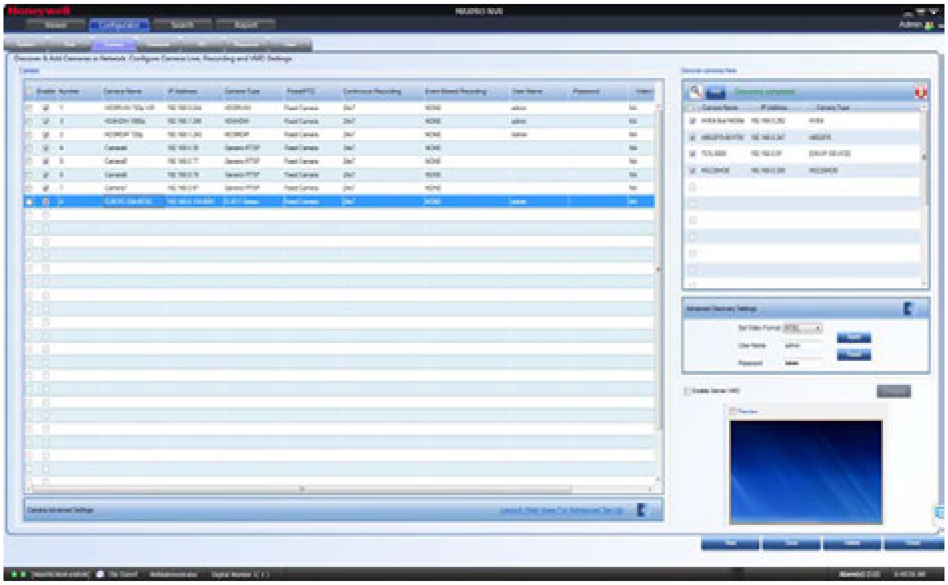
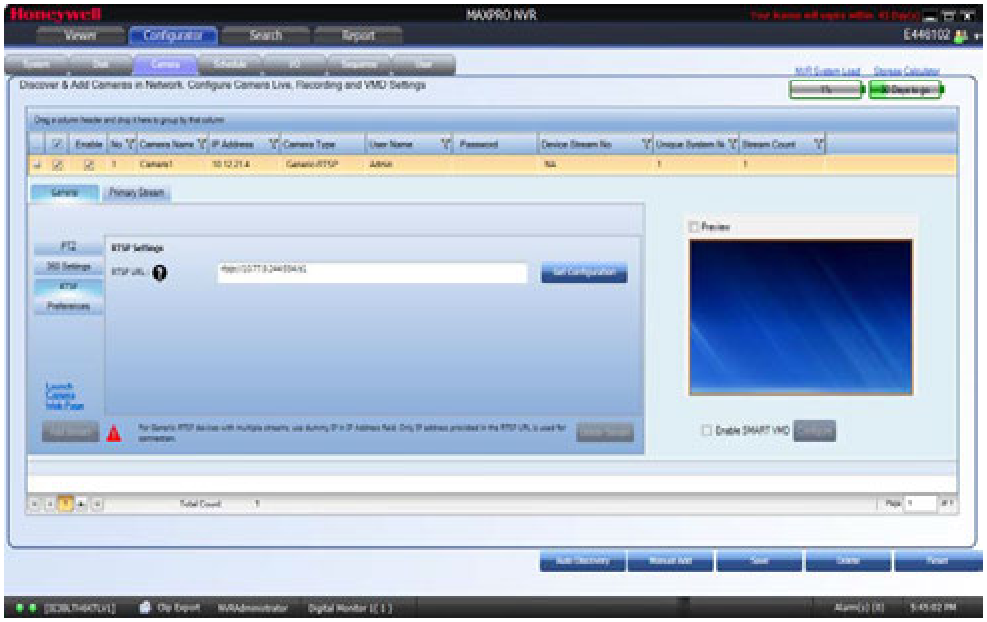


Figure 6-20 Saving FLIR Camera

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.



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 №	Stream Count
	☑	☑	1	Camera1	10.12.21.4	Generic RTSP	Admin		NA	1	1

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.

Total Count 1

Figure 6-21 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.

9. Click **Save**.

Tip: If a particular camera is not discovered by the system, you can add it manually by clicking **Manual Add**.

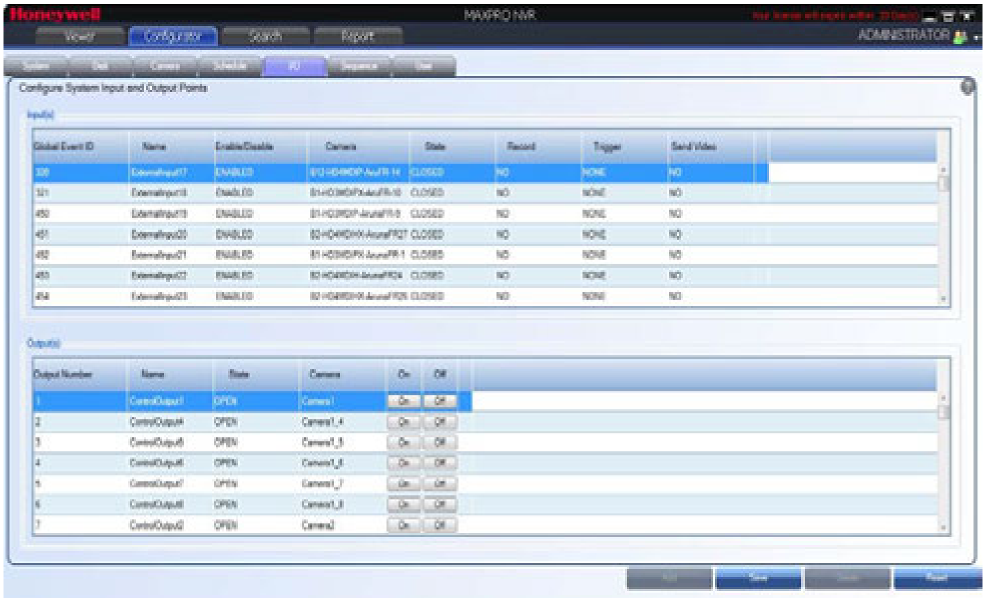
Configuring the Input and Output for an IP Camera

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

1. Click the **Configurator** tab. The **System** page (Figure 6-22) displays by default.
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
330	ExternalInput17	ENABLED	[illegible]	CLOSED	NO	NONE	NO
321	ExternalInput18	ENABLED	[illegible]	CLOSED	NO	NONE	NO
450	ExternalInput19	ENABLED	[illegible]	CLOSED	NO	NONE	NO
451	ExternalInput20	ENABLED	[illegible]	CLOSED	NO	NONE	NO
452	ExternalInput21	ENABLED	[illegible]	CLOSED	NO	NONE	NO
453	ExternalInput22	ENABLED	[illegible]	CLOSED	NO	NONE	NO
454	ExternalInput23	ENABLED	[illegible]	CLOSED	NO	NONE	NO

Output(s)

Output Number	Name	State	Camera	On	Off
1	ControlOutput1	OPEN	Camera1	On	Off
2	ControlOutput4	OPEN	Camera1_4	On	Off
3	ControlOutput5	OPEN	Camera1_5	On	Off
4	ControlOutput6	OPEN	Camera1_6	On	Off
5	ControlOutput7	OPEN	Camera1_7	On	Off
6	ControlOutput8	OPEN	Camera1_8	On	Off
7	ControlOutput2	OPEN	Camera2	On	Off

Figure 6-22 IO page

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.
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.

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.

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.
6. Click **Save** or click **Reset** to undo the changes.

To trigger the output from viewer screen:

1. Click the **Viewer** tab.
2. On the left pane, click **Outputs** tab, the list of camera outputs are displayed in **Sites**.
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

1. On the **Camera** page, for the required camera, click ⊞ on the left corner to open the camera properties pane see Figure 6-12.

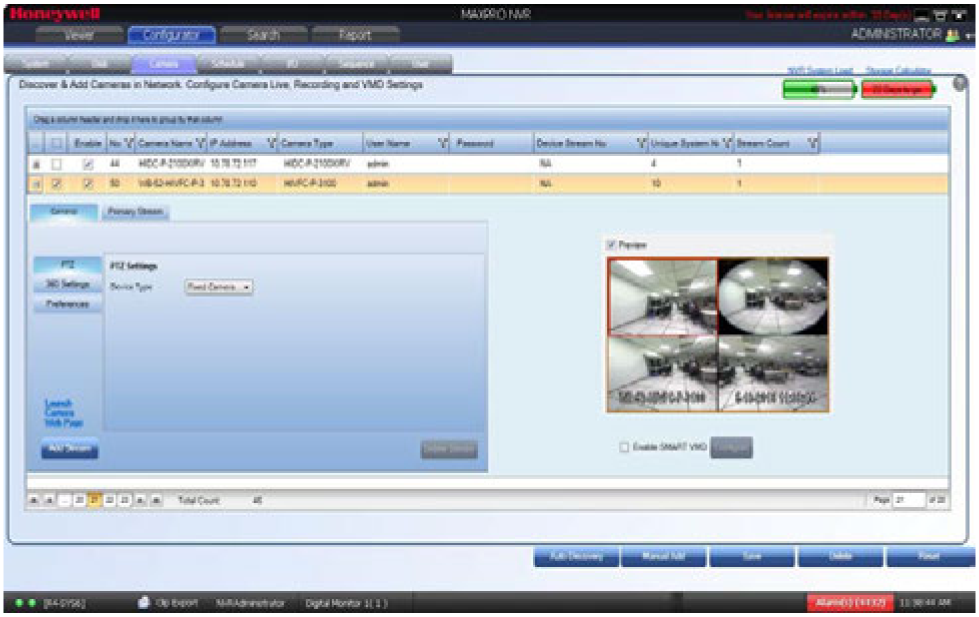


Figure 6-23 Panomorph Settings

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 AO**V Lens ID is selected. For Sony 360 camera the A8TRT lens ID is selected automatically.
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

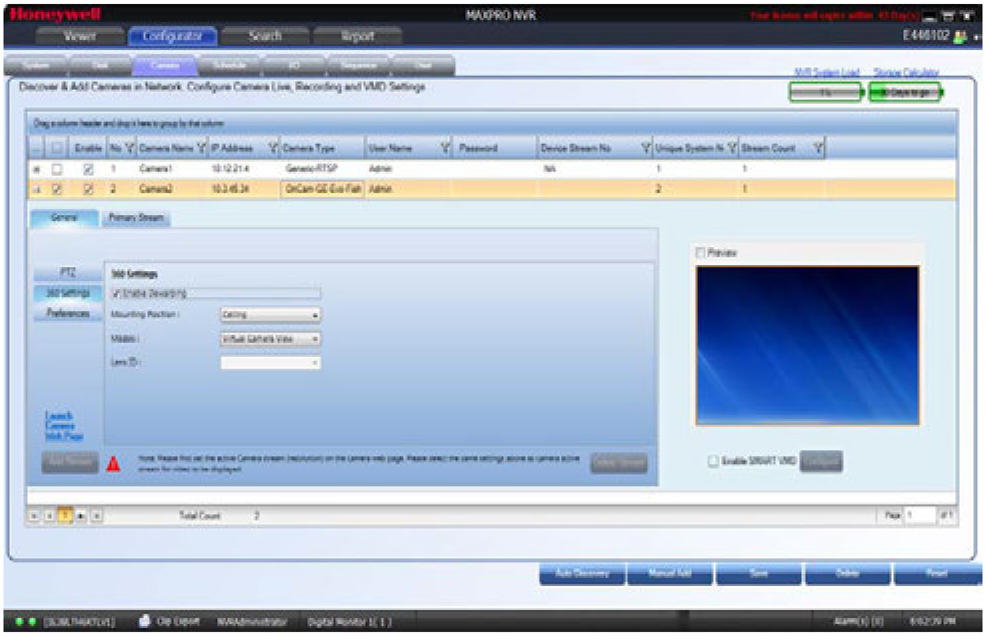
The Oncam Grandeye cameras are not discovered automatically in MAXRPRO NVR, hence you must add these cameras manually.

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

1. On the **Camera** page, click **Manual Add**.
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)

3. Click ⊞ to open the camera properties pane see Figure 6-24.:



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	10.3.45.24	OnCam GE Evo Fish	Admin			2	1

360 Settings

☑ Enable Dewarping

Mounting Position : Ceiling

Modes : Virtual Camera View

Lens ID :

Figure 6-24 Grandeye Dewarping Settings

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.

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 297 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 297.

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.

1. In MAXPRO NVR, click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to open the **Camera** page.
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 136 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 306.
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 Figure 6-25. Axis 360/180 cameras are listed in the discovery pane with their model numbers for example Axis M3007 and so on.

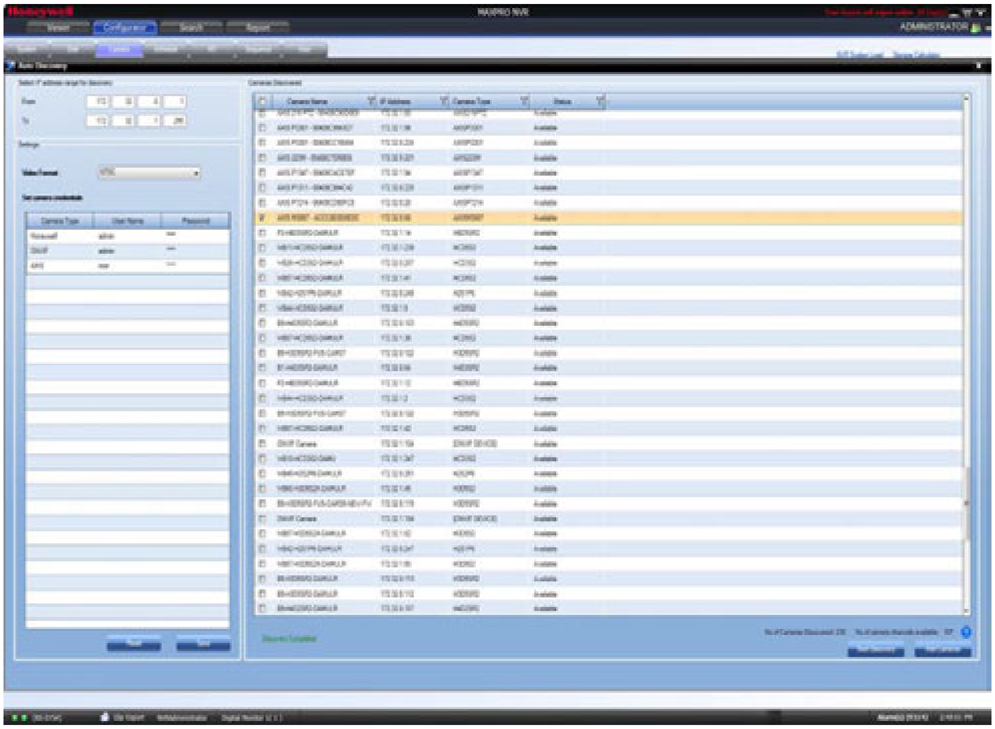


Figure 6-25 Discovering AXIS 360 Camera

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 Figure 6-26.

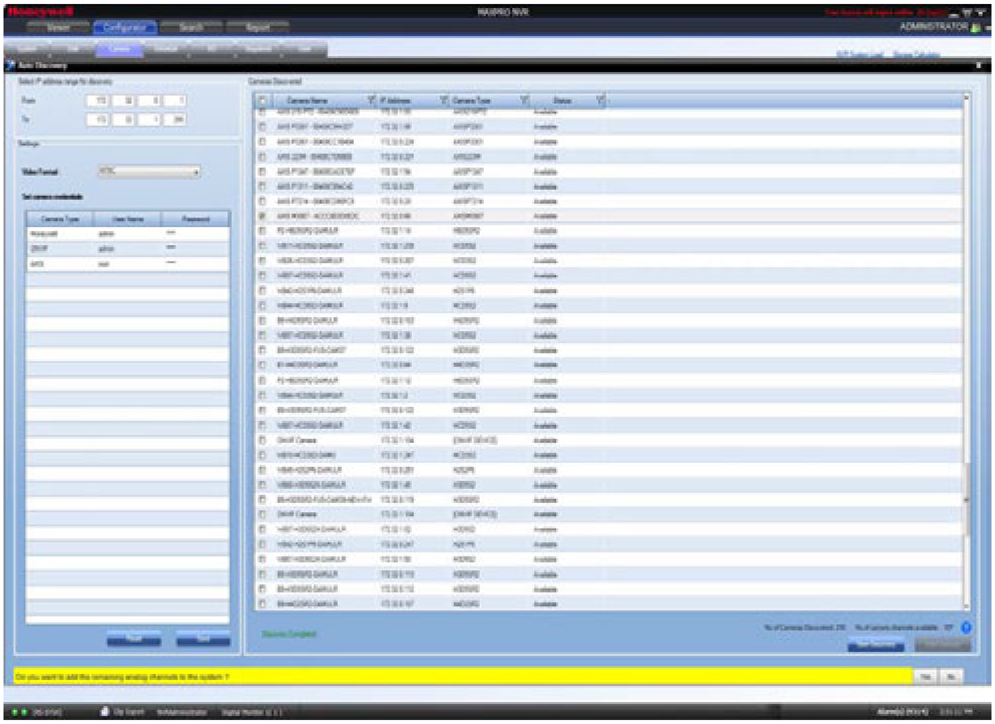


Figure 6-26 Adding Remaining Axis Channels

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 Figure 6-27.

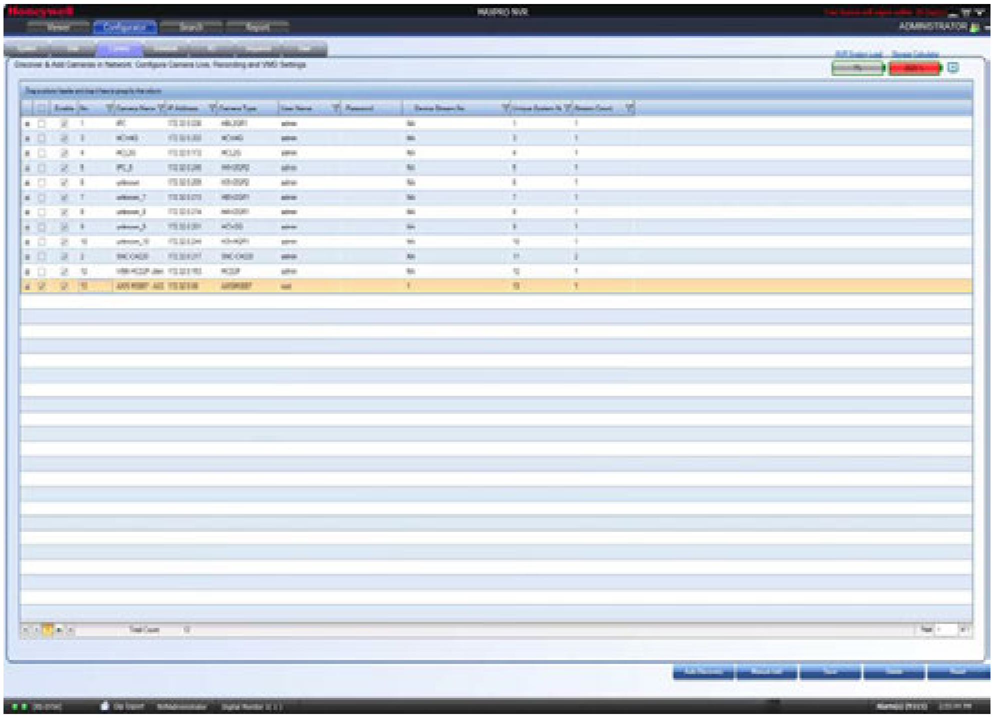


Figure 6-27 AXIS Channels

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.

1. In MAXPRO NVR, click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to open the **Camera** page.
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 136 for more information.
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 Figure 6-28.

Note: Arecont 360/180 cameras are listed in the discovery pane with their model numbers for example **AV8365DN-F8**.

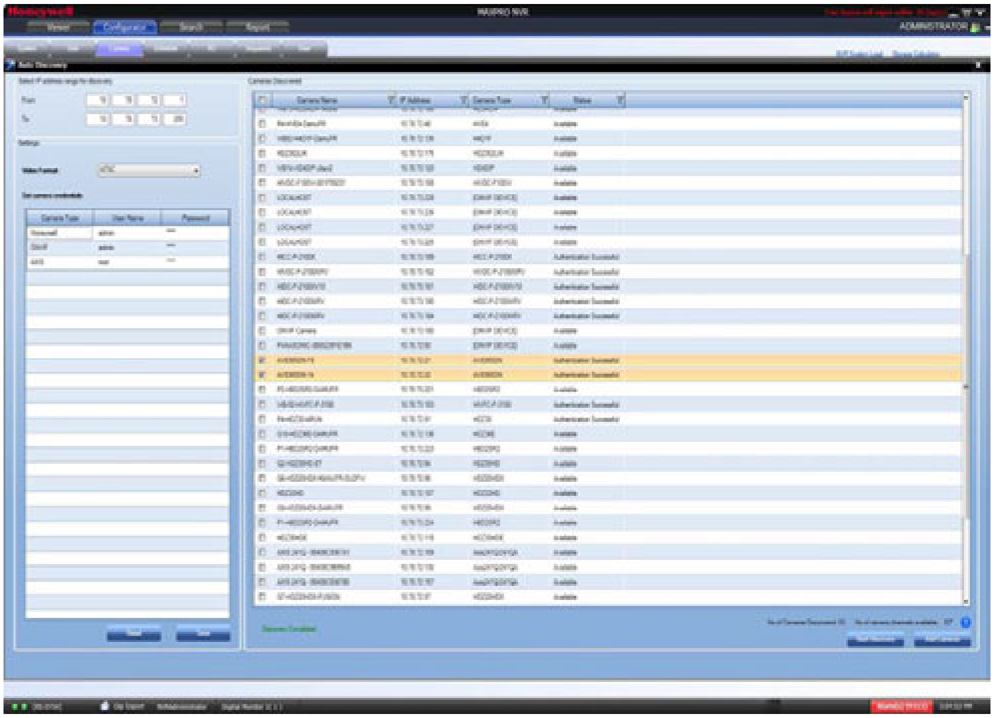
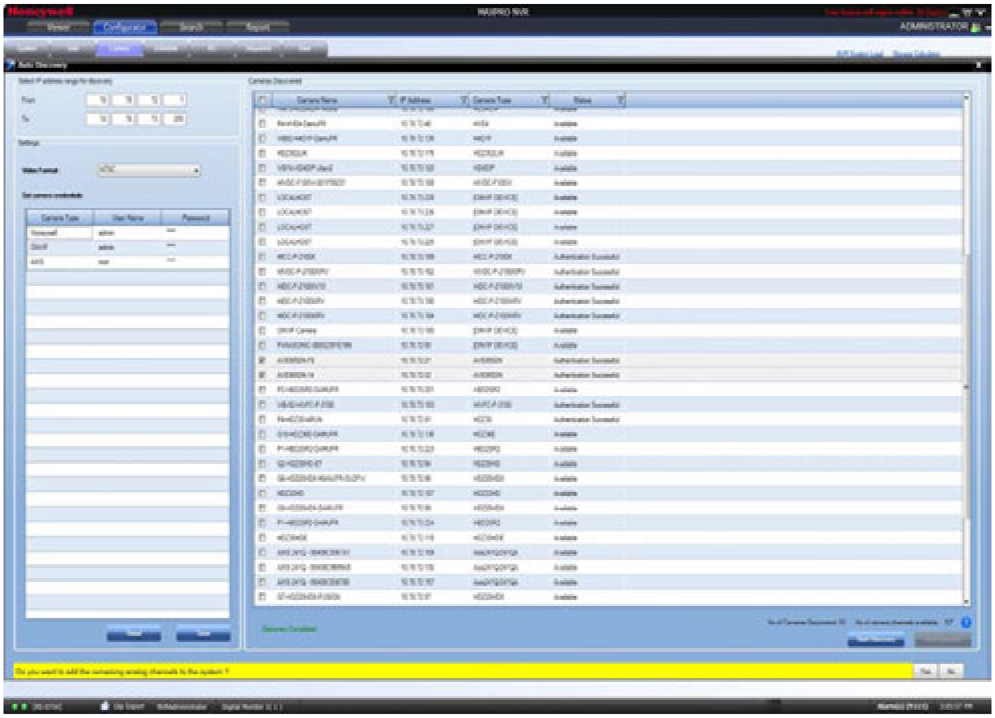


Figure 6-28 Adding Arecont 360 Model Camera

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 in Figure 6-29



Do you want to add the remaining analog channels to the system ?

Figure 6-29 Adding Remaining Arecont channels

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.

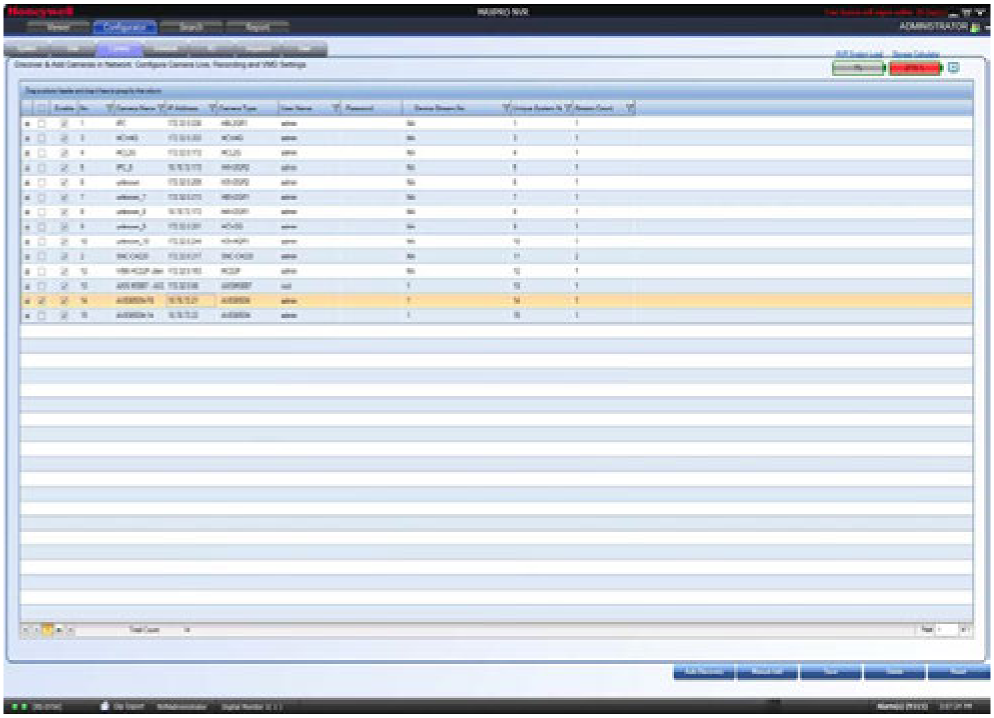


Figure 6-30 Arecont Channels

Configuring the New EquIP Model Camera for Dewarping

To dewarp the New EquIP model camera

1. Add the New EquIP Fisheye Model (HFD6GR1) camera.

2. On the **Camera** page, for the New EquIP Fisheye Model (HFD6GR1) camera, click ⊞ on the left corner to open the camera properties pane see Figure 6-12.

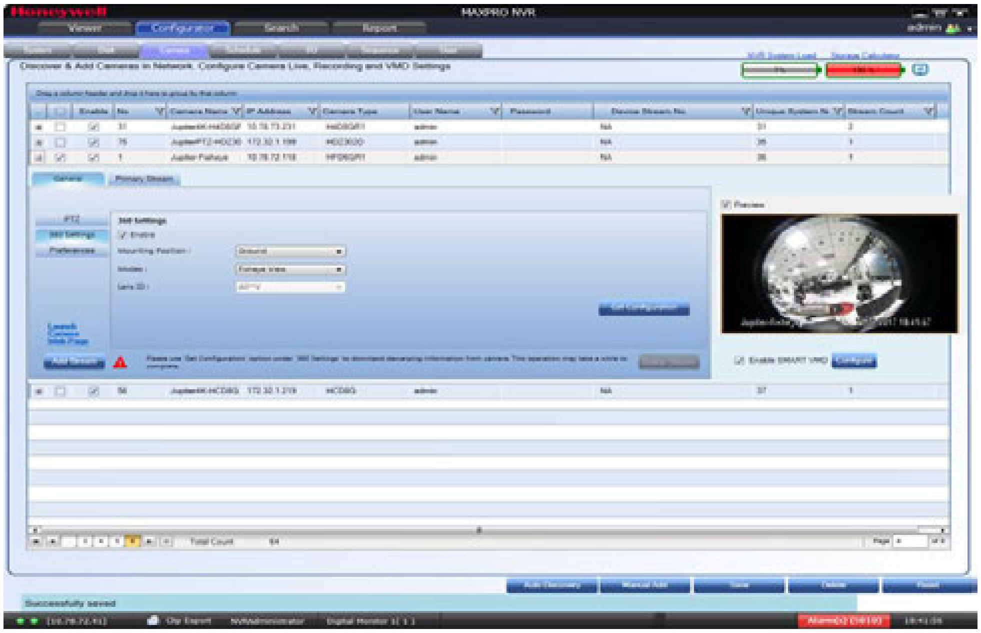


Figure 6-31 EquIP- Fisheye camera Settings

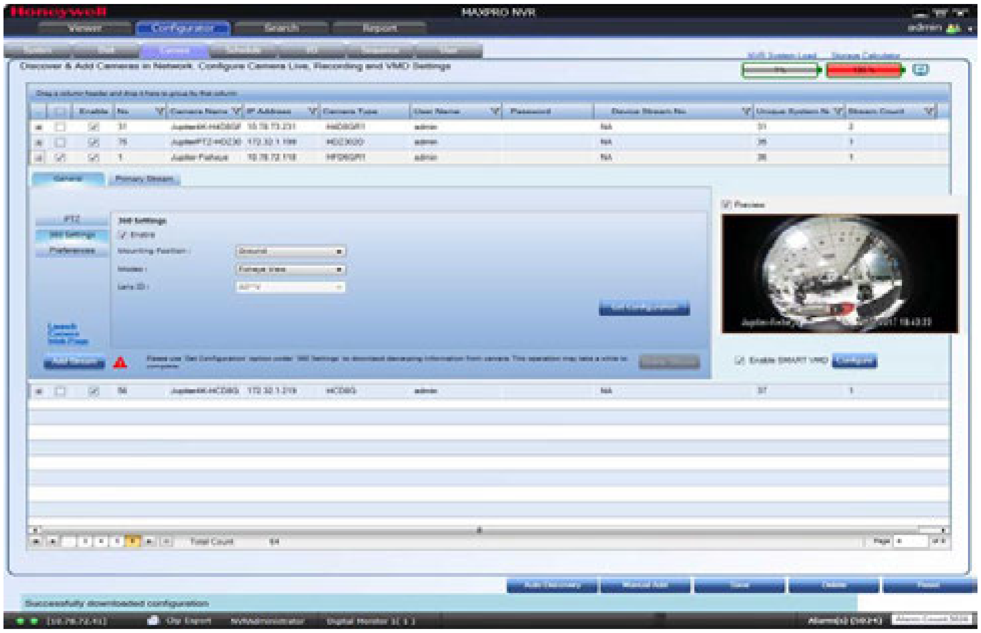
3. Under **General** > **360 Settings,** select the **Enable** check box to enable the dewarping feature.

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.

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

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

Successfully downloaded configuration

Figure 3-7 Dewarping Success Message

6. After successful download of configuration, click **Save**.

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.

8. Click **Save** to complete the configuration.

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 MAXPRO NVR Operator Guide.

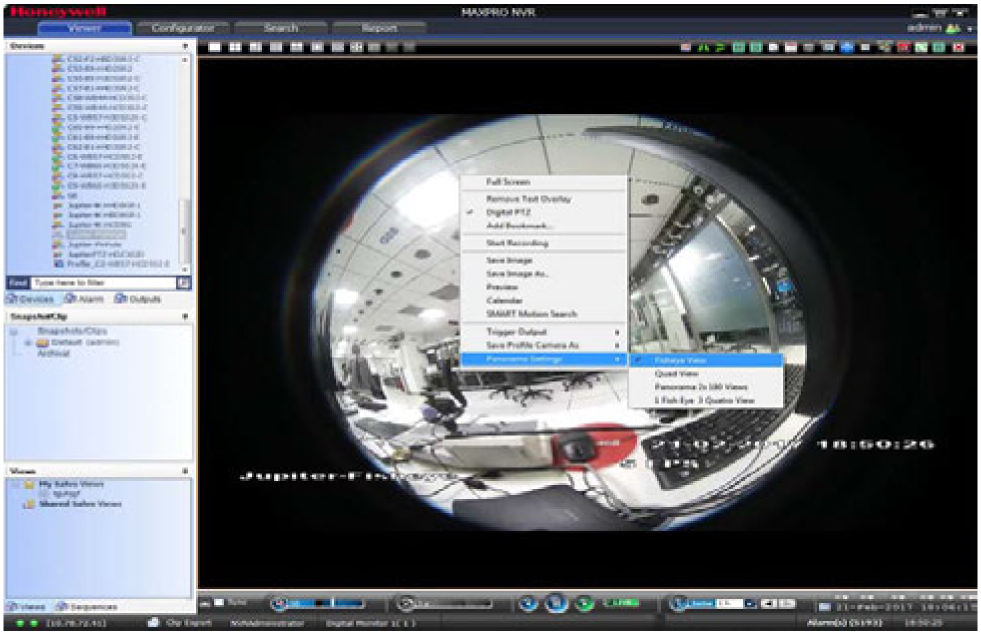


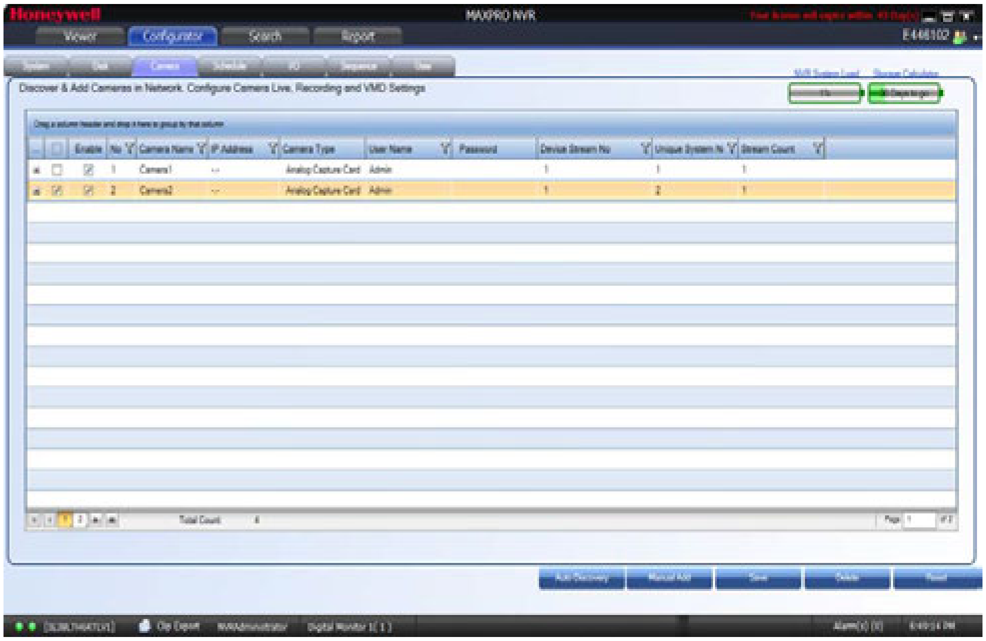
Figure 3-8 Dewarped Views List

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 46 that depict the MAXPRO NVR Hybrid SE, XE and PE box with analog capture card.

Adding/Deleting Analog Cameras

1. Connect the required number of cameras manually to analog capture card. The maximum number of analog cameras can be connected is 16.
2. Click the **Configurator** tab. The **System** page displays by default.
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

	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

Figure 6-1 Adding or Deleting Analog Camera

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

1. Select the required analog camera channel check box.
2. Click **Delete**. A confirmation message appears “Do you really want to delete camera(s)”
3. Click **Yes** to delete.

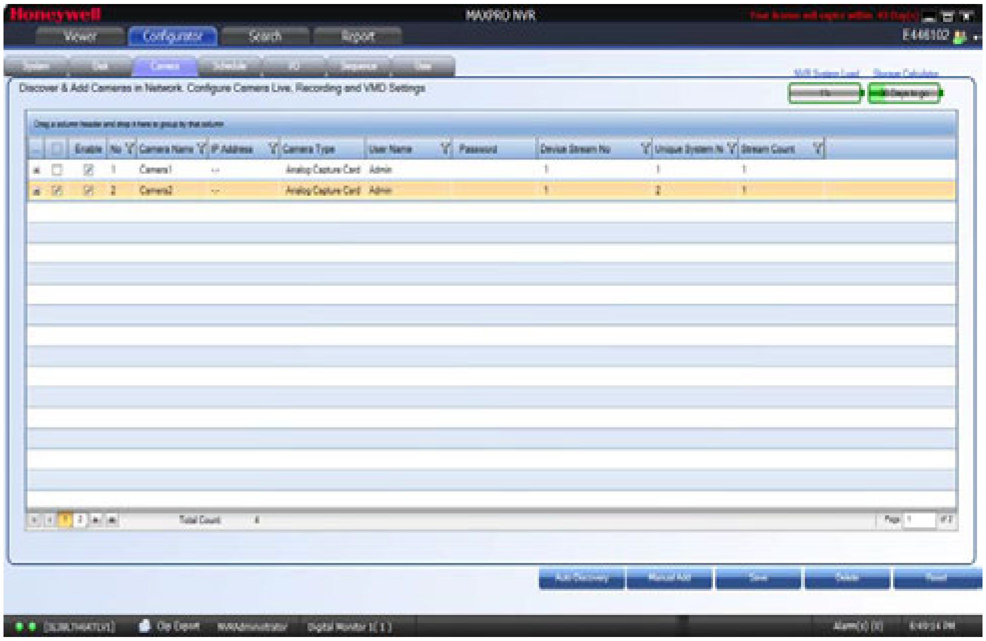
Configuring Analog Cameras

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

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

2. Click the **Camera** tab to open the **Camera** page.



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	--	Analog Capture Card	Admin		1	1	1
	☑	☑	2	Camera2	--	Analog Capture Card	Admin		1	2	1

Figure 6-2 Camera page

Note: All analog cameras that are pre-configured in the factory image appear in the Camera page when you first open it.

3. Under the **Camera** pane, select a camera to change the default parameters for the following settings.

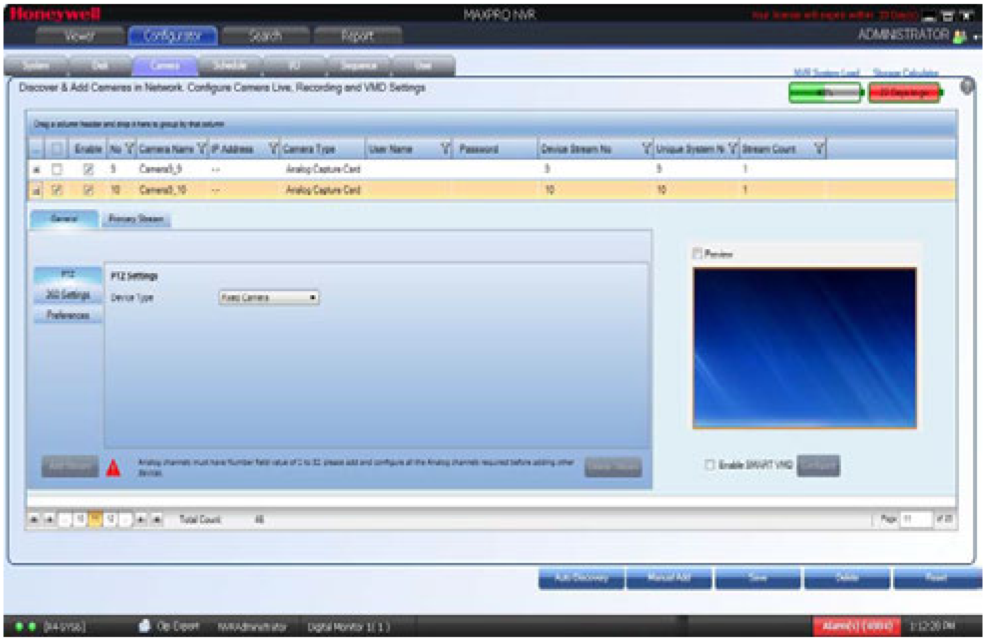
   - **Enable**/**Disable** - Enables or disables a camera for recording and live video. By default the check box corresponding to a camera to enable live video preview is selected. To disable live video preview, clear the check box corresponding to a camera. The live video appears under **Video Preview** 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.

4. For the required camera, click ⊞ on the left corner to open the camera properties pane see Figure 6-12.



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 No	Stream Count
☐	☑	5	Camera5_5	-.-	Analog Capture Card			5	5	1
☑	☑	10	Camera5_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.

Total Count 46

Figure 6-3 Camera properties pane

Note: The camera properties pane is disabled when there are no cameras available in the system.

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.

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.

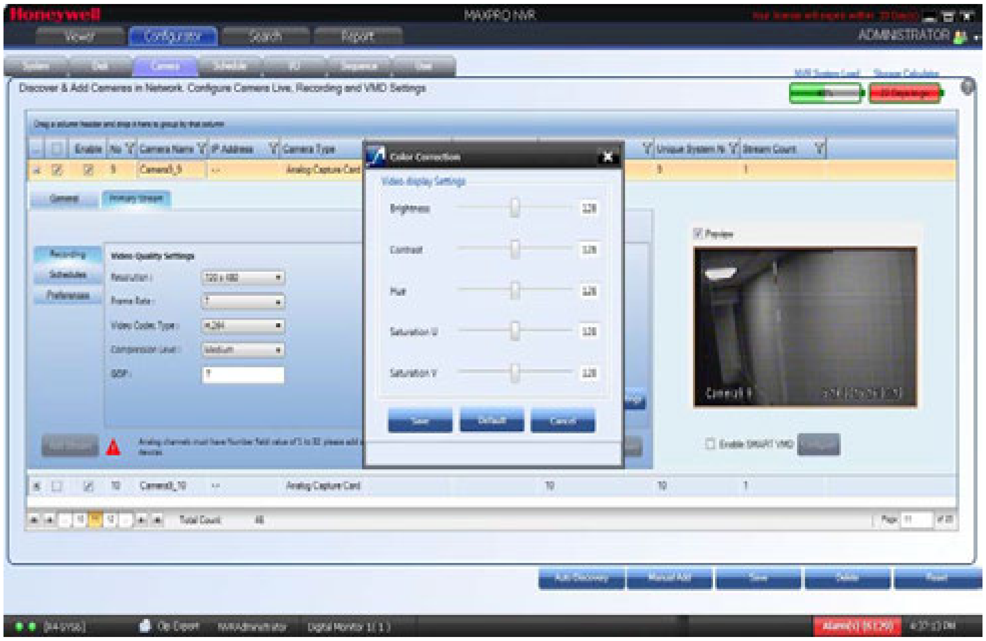
- **Video Codec Type** - Select the Codec type for the camera.
- **Compression Level** - The **Compression Level** is defaulted to “Medium”. You can select a new Compression ratio as applicable.
- **GOP** - The **GOP** value is proportional to **Frame Rate** value. If you set the Frame Rate value as 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.

7. Click **Video Display Settings**. The **Color Correction** dialog box appears Figure 6-4.

Note: The **Video Display Settings** feature is available only on the desktop local client on the NVR Hybrid Server machine.



Color Correction

Video display Settings

Brightness	128
Contrast	128
Hue	128
Saturation U	128
Saturation V	128

Figure 6-4 Color Correction dialog box

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.
9. Click **Save** to save the display settings.

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.
11. Under **Primary Stream** > **Preferences** > **Stream Preferences Settings.** See step 9 for more information.
12. Click **Save**.

PTZ Settings for Analog Camera

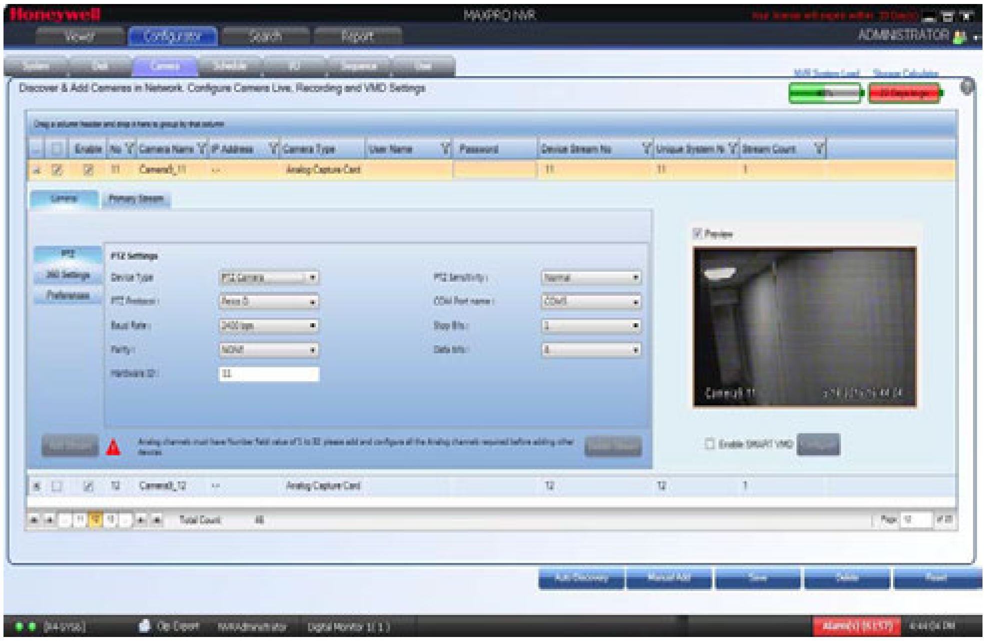
MAXPRO NVR now supports the advanced PTZ settings for an analog PTZ camera.

Note: Advanced PTZ settings are available only for analog PTZ cameras.

To set the PTZ settings

1. Select the required analog PTZ camera from the camera pane.

2. Click ⊞ on the left corner to open the camera properties pane see Figure 6-12.



PTZ Settings

Device Type: PTZ Camera

PTZ Protocol: Pelco D

Baud Rate: 2400 bps

Parity: NONE

Hardware ID: 11

PTZ Sensitivity: Normal

COM Port name: COM5

Stop Bits: 1

Data bits: 8

☐ Enable SMART VMD

Figure 6-5 Camera properties pane

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**.

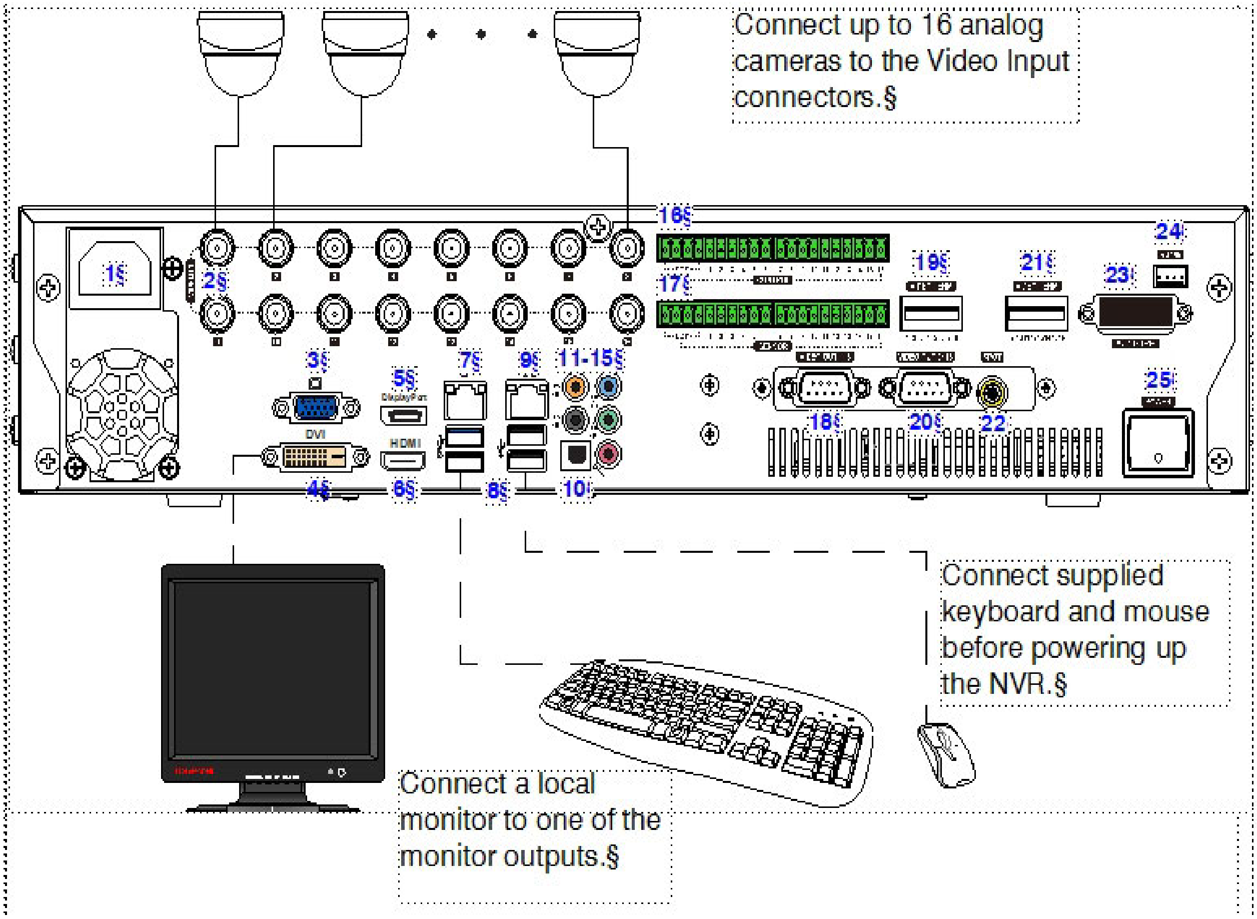
Note: Vicon protocol is not supported in this release.

   - 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.
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.

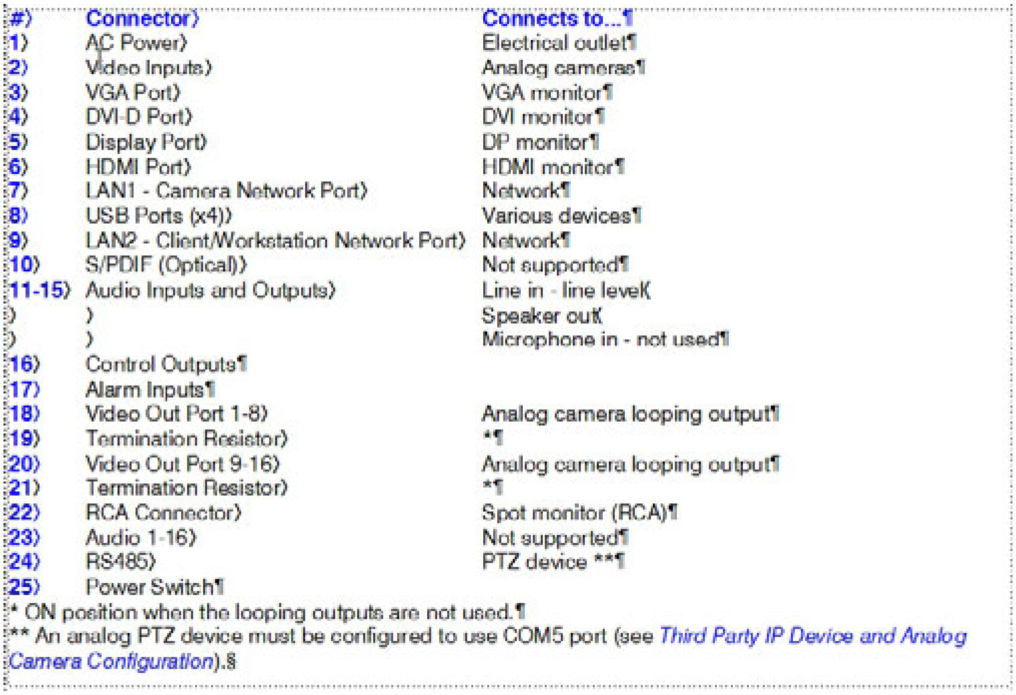
The below figures depicts the typical input and output ports (Highlighted in Red) and RS-485 connectors for MAXPRO NVR Hybrid XE, SE and PE Box. The **SENSOR** is the input port and **CONTROL** is the output port for both Hybrid XE Figure 6-6 and SE Box Figure 6-7. The detailed input and output ports for NVR Hybrid PE box is shown in Figure 6-9.



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.§

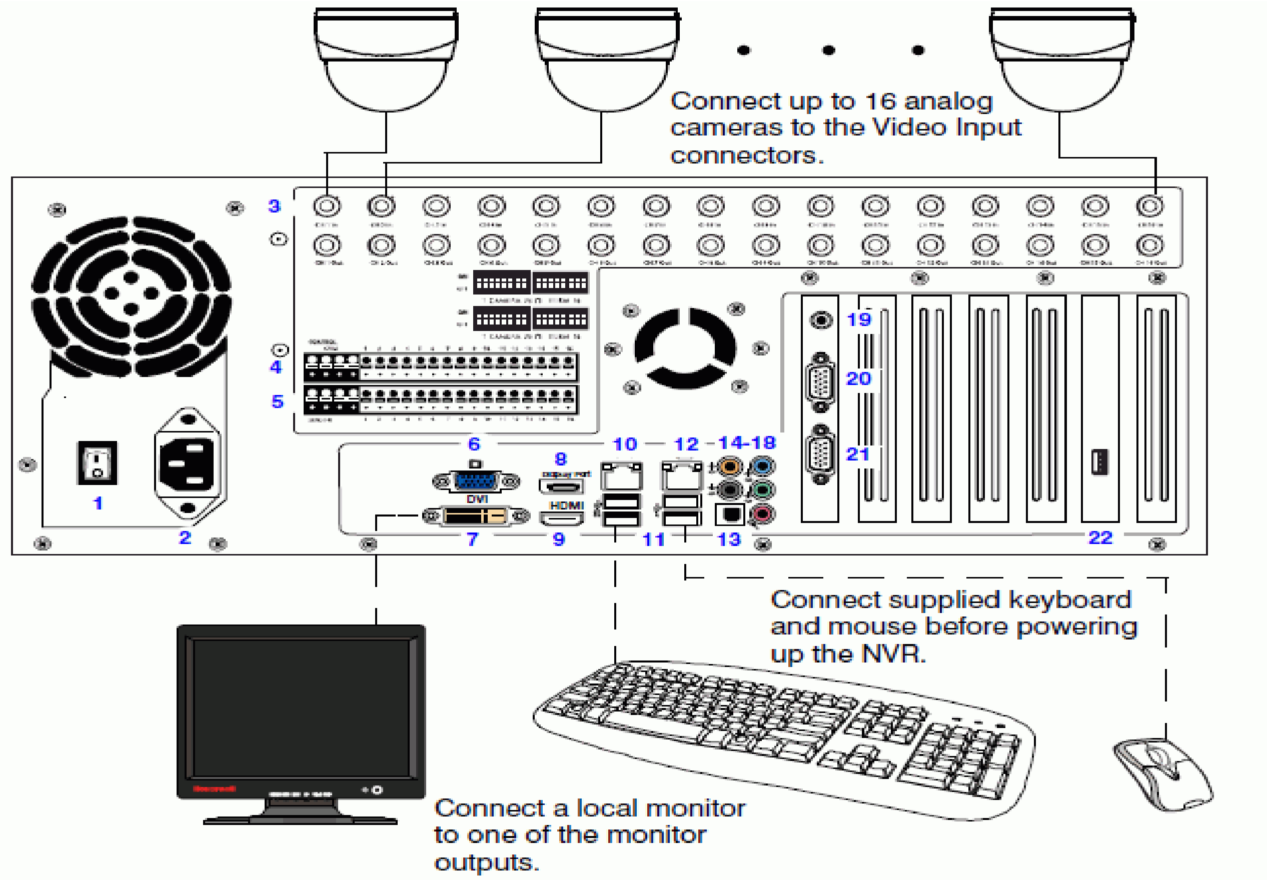


#	Connector	Connects to...
1	AC Power	Electrical outlet
2	Video Inputs	Analog cameras
3	VGA Port	VGA monitor
4	DVI-D Port	DVI monitor
5	Display Port	DP monitor
6	HDMI Port	HDMI monitor
7	LAN1 - Camera Network Port	Network
8	USB Ports (x4)	Various devices
9	LAN2 - Client/Workstation Network Port	Network
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*).

Figure 6-6 Input and Output Ports For MAXPRO NVR Hybrid XE



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

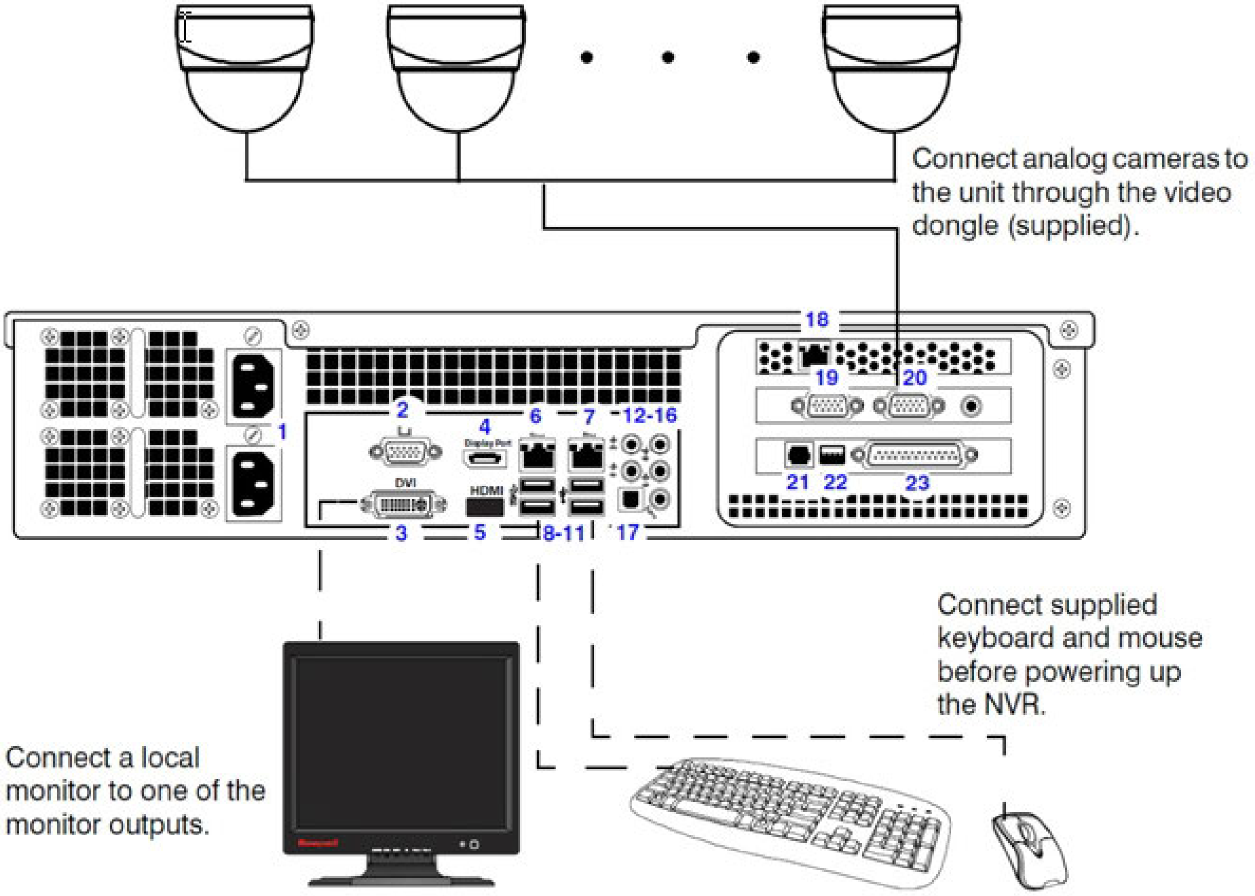
Connect supplied keyboard and mouse before powering up the NVR.

Connect a local monitor to one of the monitor outputs.

#	Connector	Connects to...
1	Power Switch	
2	AC Power	Electrical outlet
3	Video Inputs, Outputs (BNC)	Analog cameras
4	Control Outputs	
5	Alarm Inputs	
6	VGA Port	VGA monitor
7	DVI-D Port	Monitor
8	Display Port	Monitor
9	HDMI Port	HDMI monitor
10	LAN1 - Camera Network Port	Network
11	USB Ports (x4)	Various devices
12	LAN2 - Client/Workstation Network Port	Network
13	S/PDIF (Optical)	Not supported
14-18	Audio Inputs and Outputs	Line in - line level Speaker out Microphone in - not used
19	RCA Connector	Sport monitor (RCA)
20	Video Out Port 1–8	Analog camera looping output
21	Video Out Port 9–16	Analog camera looping output
22	RS485	PTZ device *

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

Figure 6-7 Input and Output Ports For MAXPRO NVR Hybrid SE



Connect analog cameras to the unit through the video dongle (supplied).

Connect supplied keyboard and mouse before powering up the NVR.

Connect a local monitor to one of the monitor outputs.

#	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*).

Figure 6-8 MAXPRO NVR Hybrid PE Rear View

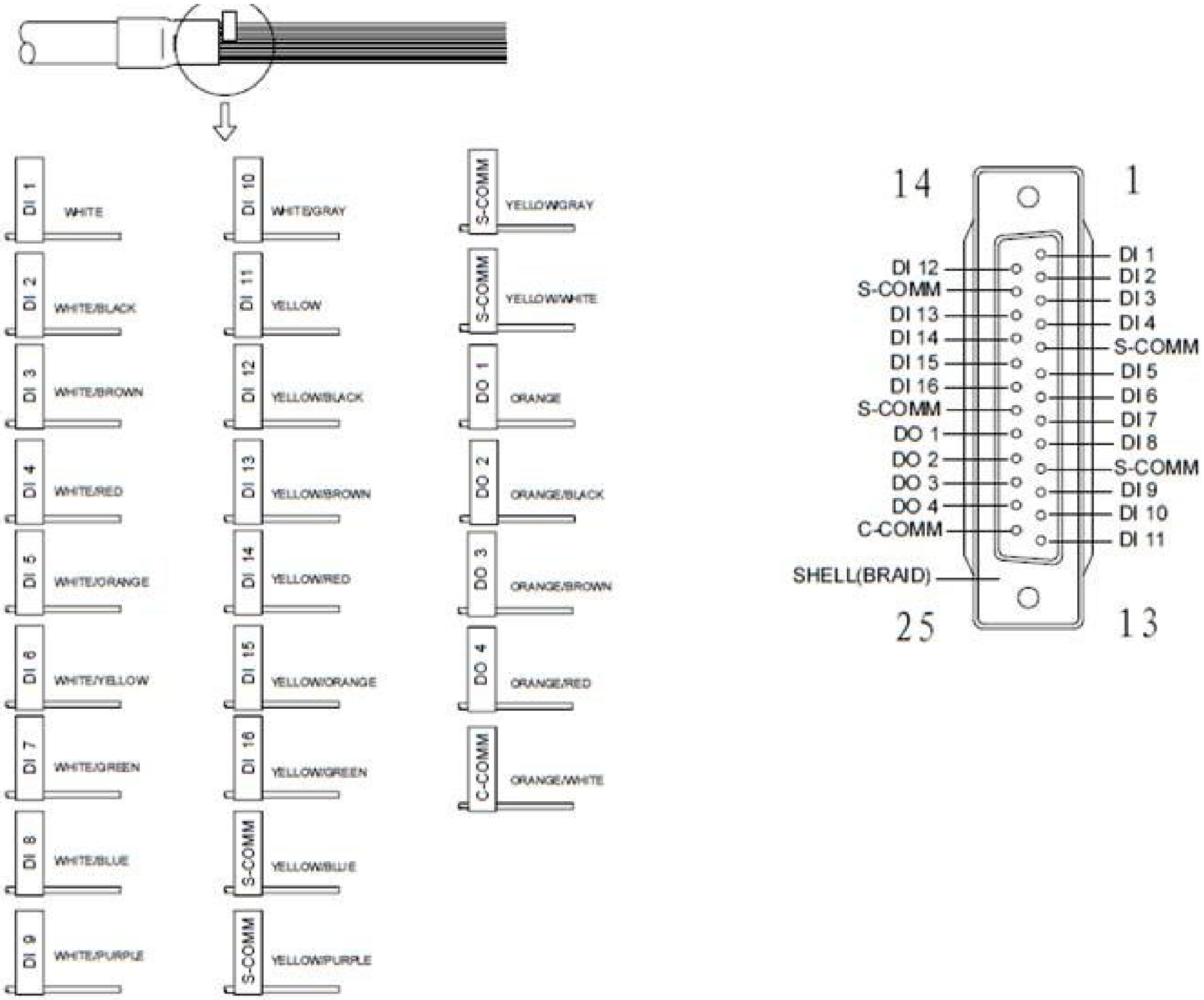


Figure 6-9 Input and Output Ports For MAXPRO NVR Hybrid PE

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.

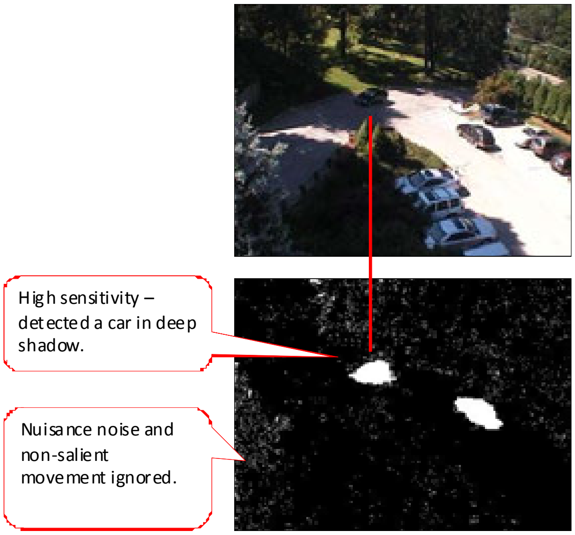
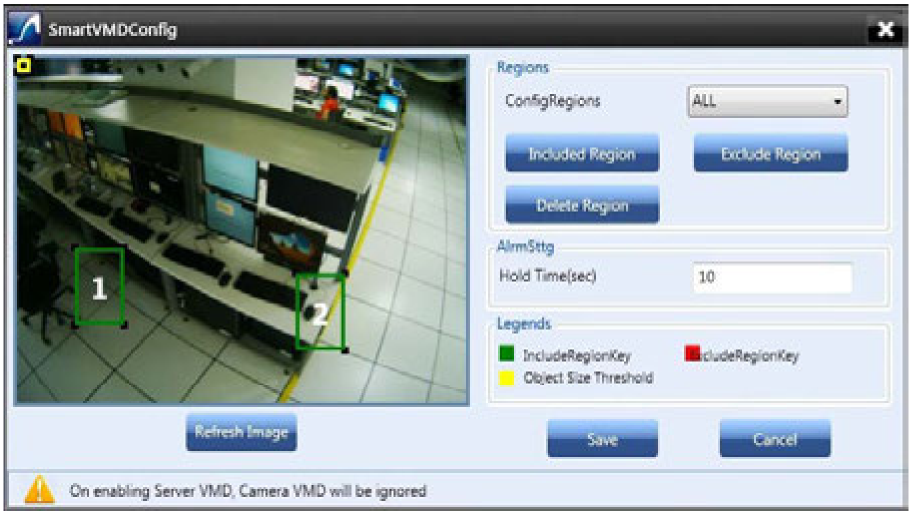

High sensitivity – detected a car in deep shadow.
Nuisance noise and non-salient movement ignored.

Figure 6-10 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.

1. Select the **Enable SMART VMD** check box.
2. Click **Configure**. The **SMART VMD Configuration** dialog box appears (see Figure 6-40).
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.
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.
5. To delete a region, select the region from the Configured Regions drop-down list, then click **Delete Region**.



Regions

ConfigRegions: ALL

AlrmSttg

Hold Time(sec): 10

Legends

🟩 IncludeRegionKey 🟥cludeRegionKey

🟨 Object Size Threshold

⚠ On enabling Server VMD, Camera VMD will be ignored

Figure 6-11 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.

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.

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

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to navigate to the **Camera** page. The list of cameras configured are displayed.
3. Select the row corresponding to the camera you want to modify.
4. Change the settings such as camera name, IP address, and so on.
5. Click **Save**.

Deleting the Cameras

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to navigate to the **Camera** page.
3. Select the check box corresponding to the camera you want to delete.
4. Click **Delete**. A confirmation message appears at the bottom of the display area.
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.

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

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** **(**see Figure 6-12).

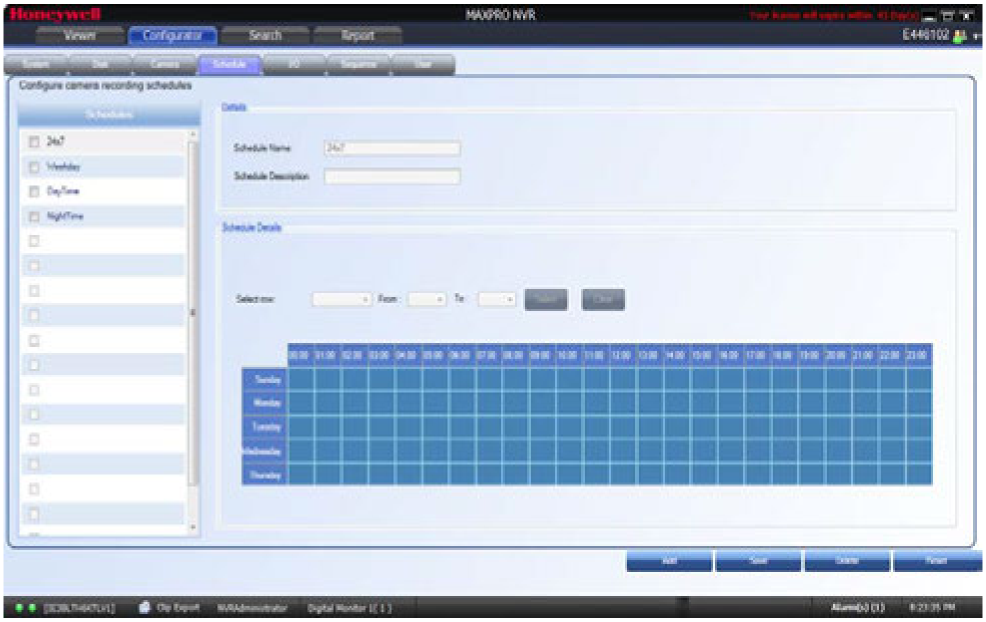


Figure 6-12 Schedule page

Note: You cannot modify/delete any of the default schedules.

3. Click **Add** to create a new schedule.
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.

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.

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Schedule** tab to navigate to the **Schedule** page.
3. Under **Schedules**, select the schedule you want to delete from the list. The schedule's details appear.
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

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Sequence** tab to navigate to the **Sequence** page.

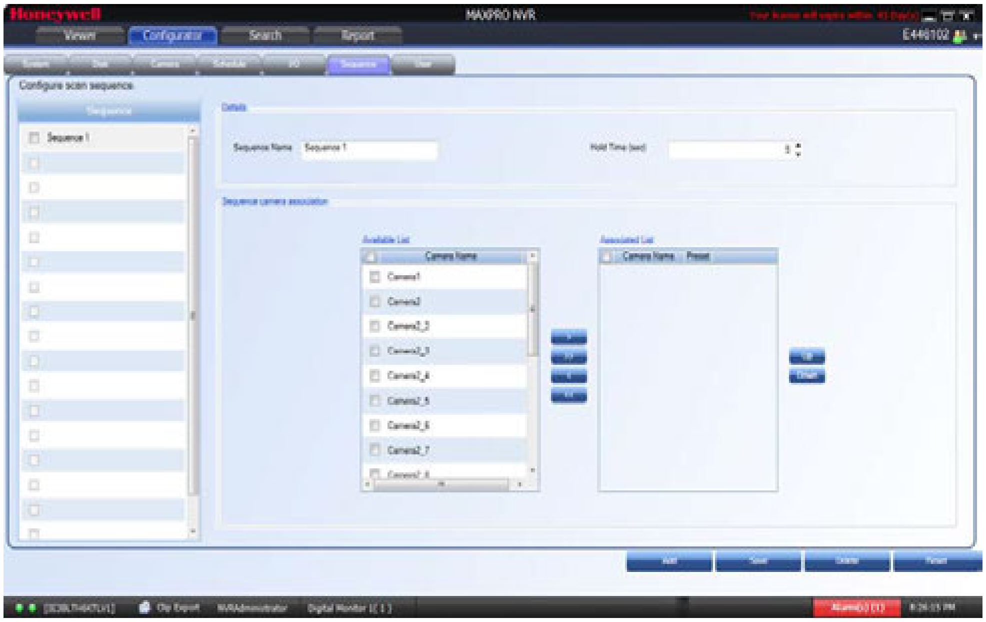


Figure 6-13 Sequence page

3. Click **Add**.

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.
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.

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

1. Select the check box corresponding to the camera you want to rearrange inside the sequence.
2. Click **Up** to move the camera one row up, or click **Down** to move the camera one row down.
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

1. In the **Preset** column, do not select any preset from the drop-down list.
2. Click **Save**.

Updating a Sequence

Updating a sequence allows you to change the sequence of video display from cameras.

To update a sequence

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Sequence** tab to navigate to the **Sequence** page.
3. Select the check box corresponding to the sequence you want to update.
4. You can change the sequence name, dwell time and sequence of the cameras.
5. Click **Save**.

Deleting a Sequence

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **Sequence** tab to navigate to the **Sequence** page.
3. Select the check box corresponding to the sequence you want to delete.
4. Click **Delete**. A confirmation message appears on the top of the display area.
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.

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 225 for more information.

The following table lists the various user roles and the privileges applicable to the role.

	Viewer	Configurator	Search	Report
NVR Administrator	X	X	X	X
Operator	X	-	-	-
Supervisor	X	-	X	X
Internet Operator	X	-	-	-
Live View Operator	X	-	-	-

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.

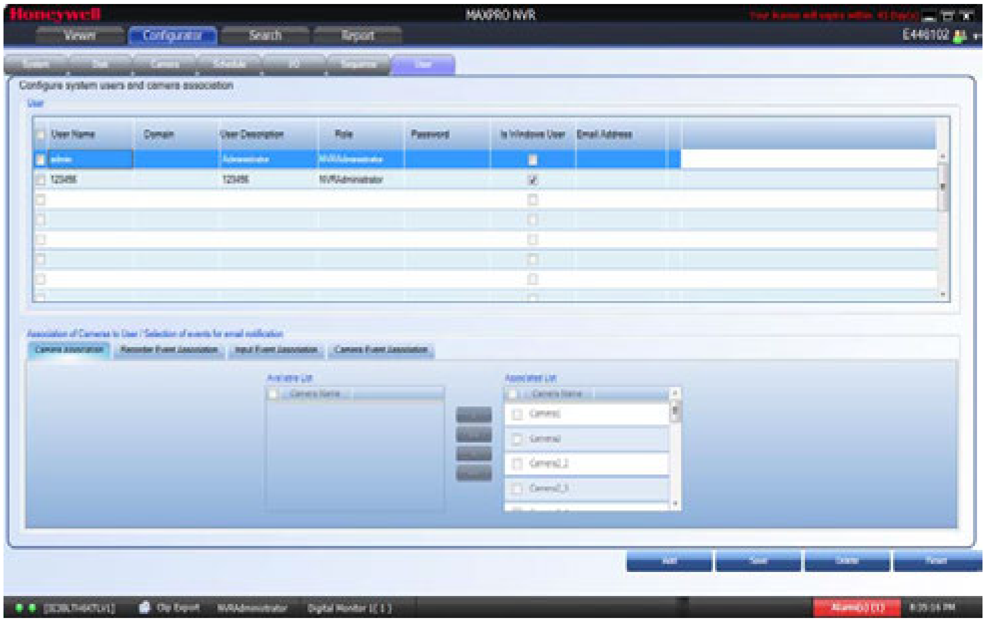
When you install MAXPRO NVR for the first time, a default user named "admin" is created. The admin user is assigned the role "NVRAdministrator". Only the user having "NVRAdministrator" privilege can add new users, assign roles to the added users, add or modify the privileges to the users, and perform 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

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **User** tab to navigate to the **User** page Figure 6-14.



	User Name	Domain	User Description	Role	Password	Is Windows User	Email Address
□	admin		Administrator	NVRAdministrator		□	
□	123456		123456	NVRAdministrator		☑	
□						□	
□						□	
□						□	
□						□	
□						□	

Figure 6-14 User page

3. Click **Add**. A new row is created with a default set of values for the user.
4. Under the **User Name** column, the default user name is displayed. You can type a new user name as applicable.
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.
6. Under the **User Description** column, type a description for the user.
7. Under the **Role** column, select the role you want to assign to the user from the drop-down list.
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.

9. Under the **IsWindowsUser** column, select the check box if the user is a Window's user.
10. Under the **Email Address** column, type the user's email address.

11. 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**.
12. 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**.
13. 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**.
14. 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**.
15. 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

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **User** tab to navigate to the **User** page.
3. Select the check box corresponding to the user you want to modify.
4. Change the settings such as user name, user description, and so on.
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

1. Click the **Configurator** tab. The **System** page displays by default.
2. Click the **User** tab to navigate to the User page.
3. Select the check box corresponding to the user you want to delete.
4. Click **Delete**. A confirmation message appears at the bottom of the display area.
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:

1. In NVR Camera tab, set the Primary Stream for recording that is for high resolution.
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.

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:

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.

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

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
- Acknowledgement 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 NVR Server

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

1. In the **Username** box, type the user name. The default user name is “**admin**”.
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.

3. In the **Profile** box, select the profile in which the server address is saved.
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 87 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 92 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 92 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 92 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.

8

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

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**

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

- **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:

1. System Configuration
2. Server Configuration
3. Security Configuration

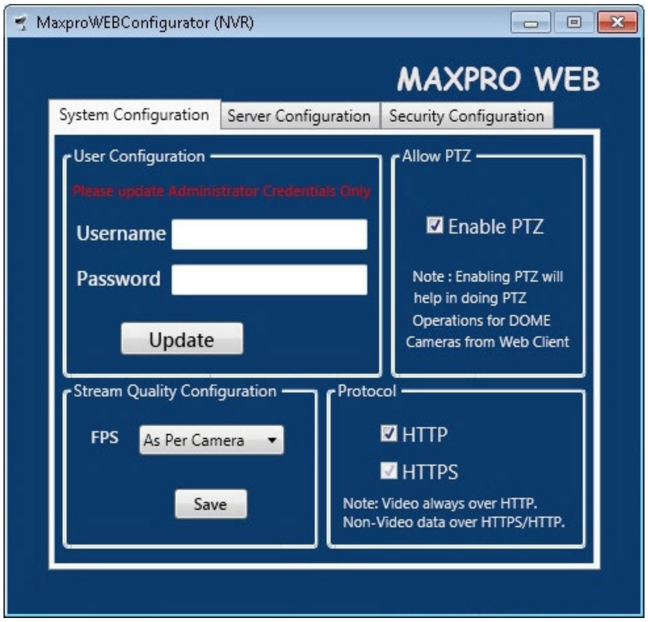
System Configuration tab: The system configuration tab allows you to update the administrator user credentials and the FPS for a better Stream quality. It also allows you to set the protocol for secure communication.

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

1. Double-click on the desktop. The **MAXPRO Web Configurator** dialog box Figure 8-1 appears. By default the **System Configuration** tab is selected.



Please update Administrator Credentials Only

☑ Enable PTZ

Note : Enabling PTZ will help in doing PTZ Operations for DOME Cameras from Web Client

FPS: As Per Camera

☑ HTTP

☑ HTTPS

Note: Video always over HTTP.
Non-Video data over HTTPS/HTTP.

Figure 8-1 MAXPRO WebConfigurator

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.

3. Under **Allow PTZ**:

   - Select the **Enable PTZ** check box to perform PTZ operations on a PTZ camera from Web Client.

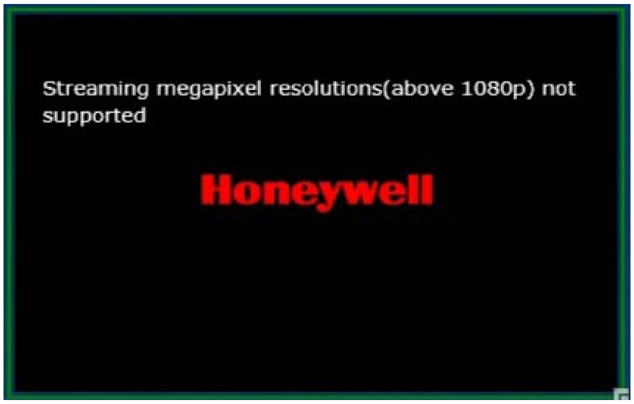
Note: PTZ feature is not supported and It is not recommended to use this feature in the current release.

4. Under **Stream Quality Configuration**:

   - Select the required **FPS** 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

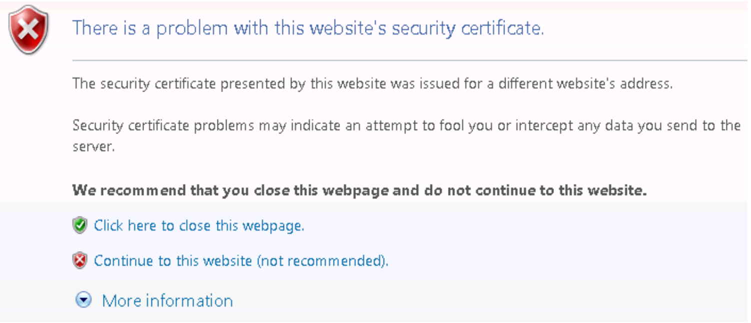
5. Under **Protocol**:

   - Click the appropriate **Protocol** options for secure communication. The available options are **HTTP** and **HTTPS**. By default **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 are considered in any port forwarding settings required.

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 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 196 and Installing the Certificate section on page 200 for more information. Or You can use the MAXPROWeb 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 196 and Installing the Certificate section on page 200 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.

6. Click the **Server Configuration** tab**.** The **Server Configuration** screen (Figure 8-2) appears.

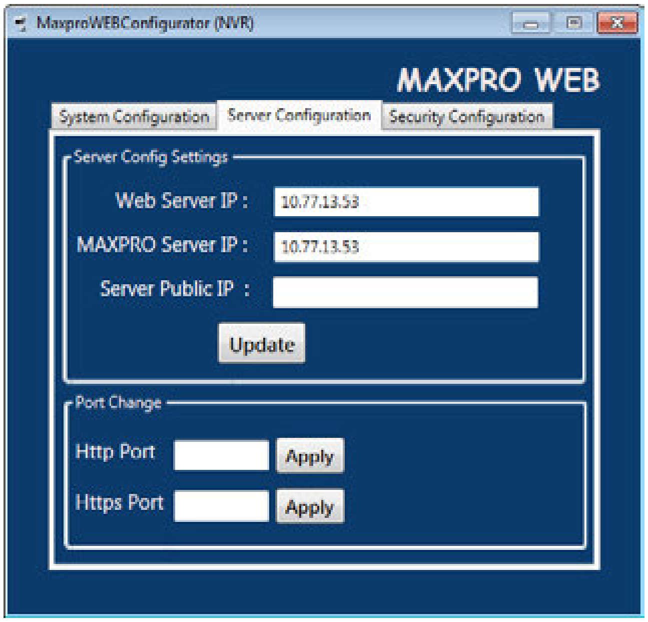


Figure 8-2 MAXPROWebConfigurator-Server Configuration

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.

7. Under **Server Config Settings**:

   - **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**.

8. Under **Port Change**:

   - **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.

9. Click the **Security Configuration** tab**.** The **Security Configuration** screen (Figure 8-2) appears.

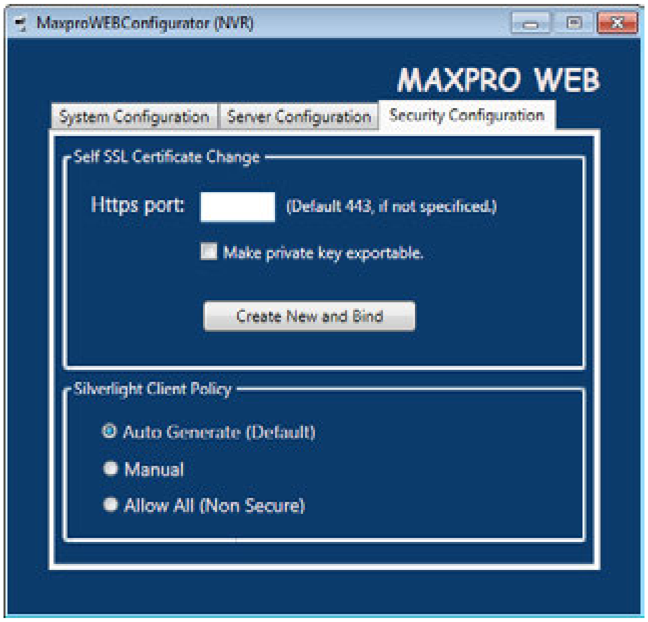

MaxproWEBConfigurator (NVR)
MAXPRO WEB
System Configuration
Server Configuration
Security Configuration
Self SSL Certificate Change
Https port:
(Default 443, if not specificed.)
□ Make private key exportable.
Create New and Bind
Silverlight Client Policy
● Auto Generate (Default)
○ Manual
○ Allow All (Non Secure)

Figure 8-3 MAXPROWebConfigurator-Security Configuration

10. Under **Self SSL Certificate Change**:

    - Type the **Port number** in the box provided if the Https binding is other than 443. The default port is 443.
    - Select the **Make private key exportable** check box to make the private key of the SSL Certificate.
    - Click **Create New and Bind** button.

11. Under **Silverlight Client Policy**: Allows you to modify the C:\inetpub\wwwroot\clientaccesspolicy.xml & C:\inetpub\wwwroot\crossdomain.xml file.

    - Click the required Silverlight 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.

12. Click X to close the MaxproWebConfigurator.

Creating Self Signed Certificate

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

1. Open the **Internet Information Manager** (IIS) window.
2. Select the server node under **Connections** pane.
3. Under **IIS**, double click the **Server Certificate** option Figure 8-4.

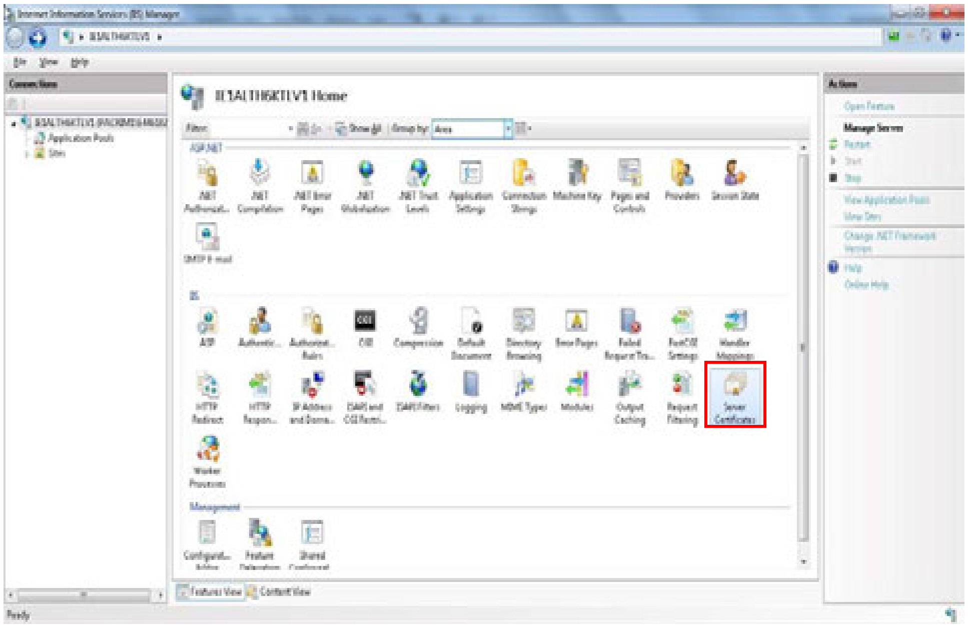
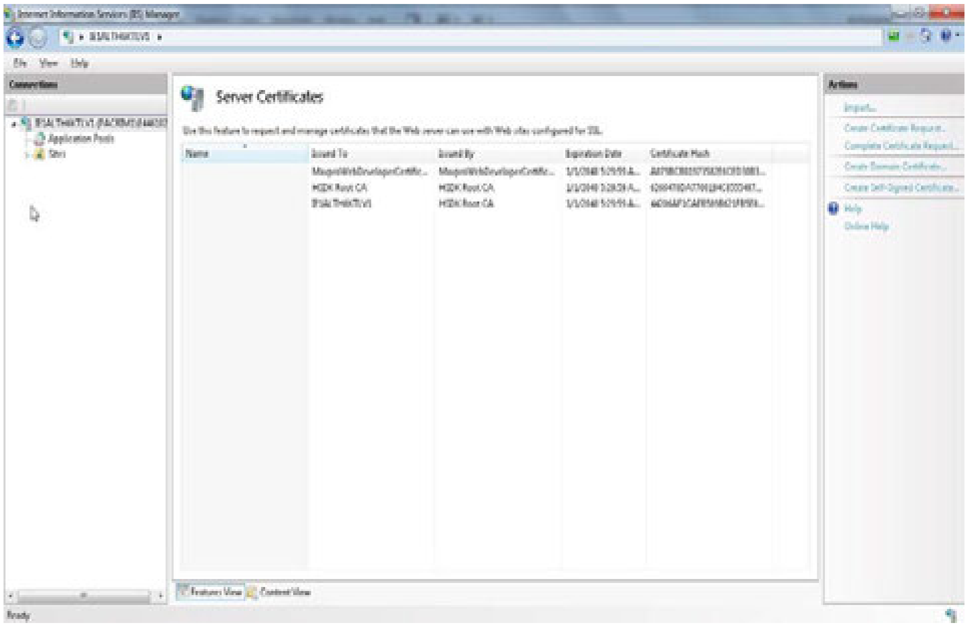


Figure 8-4 Home

The **Server Certificate** window is displayed Figure 8-5.



Server Certificates

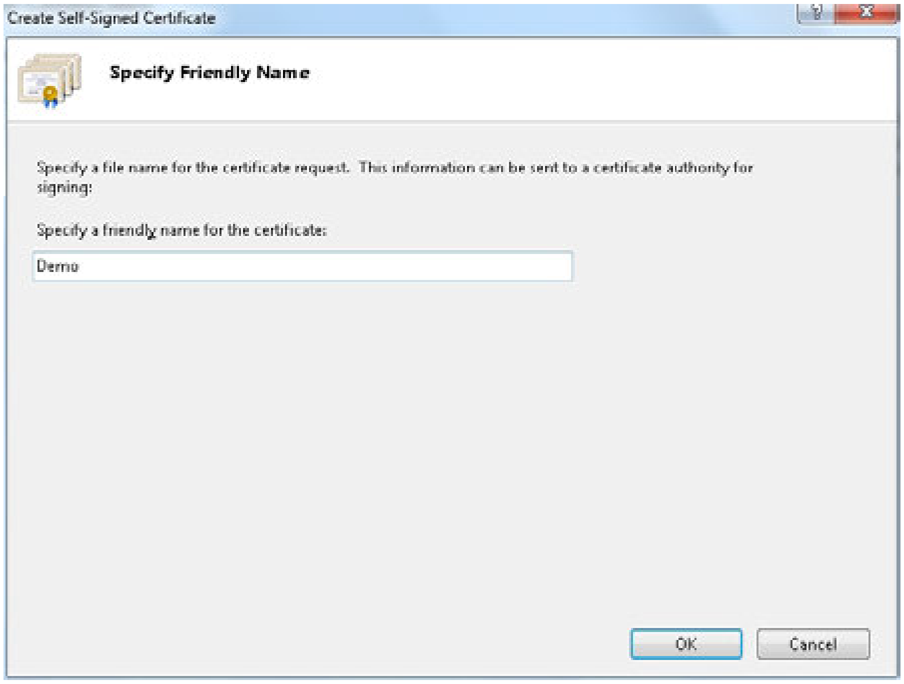
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash
	MaxproWebDeveloperCertific...	MaxproWebDeveloperCertific...	[illegible]	[illegible]
	HSDK Root CA	HSDK Root CA	[illegible]	[illegible]
	[illegible]	HSDK Root CA	[illegible]	[illegible]

Internet Information Services (IIS) Manager
File
View
Help
Connections
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

Figure 8-5 Server Certificate

4. Click the Create **Self-Signed Certificate** on the right-most pane. The **Specify Friendly Name** dialog appears Figure 8-6.



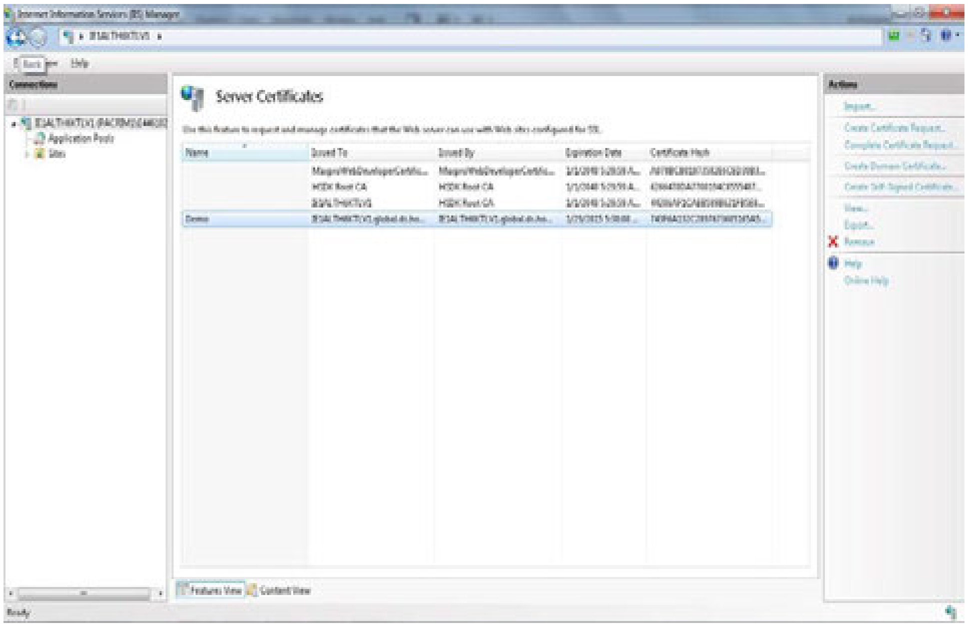
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Demo

Figure 8-6 Specify Friendly Name

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 in Figure 8-7.

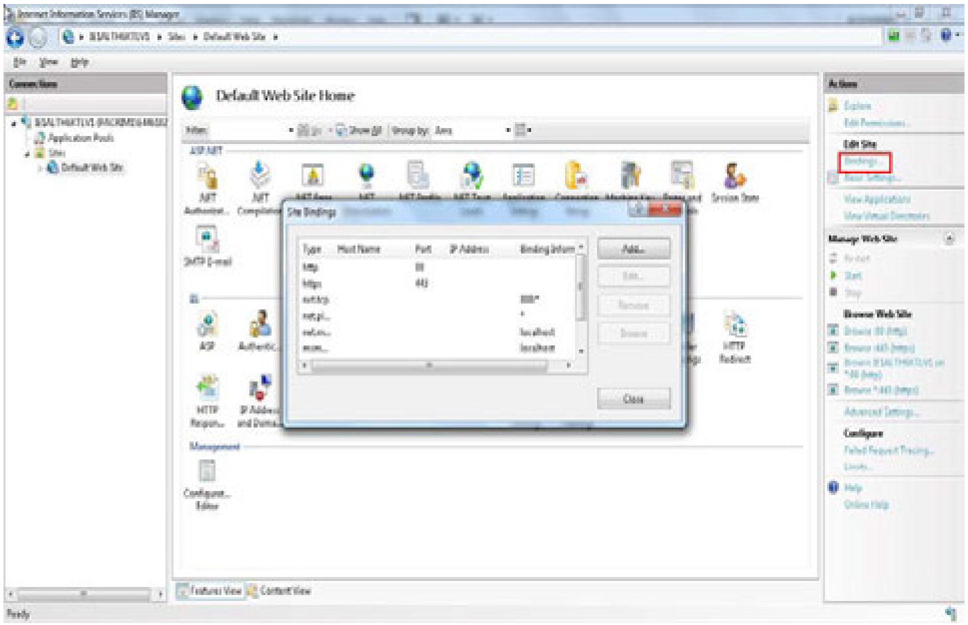

Internet Information Services (IIS) Manager
Back
Help
Connections
Application Pools
Sites
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Features View
Content View
Ready

Name	Issued To	Issued By	Expiration Date	Certificate Hash
	MaxproWebDeveloperCertific...	MaxproWebDeveloperCertific...	[illegible]	[illegible]
	HSDK Root CA	HSDK Root CA	[illegible]	[illegible]
	[illegible]	HSDK Root CA	[illegible]	[illegible]
Demo	[illegible].global.ds.ho...	[illegible].global.ds.ho...	[illegible]	[illegible]

Figure 8-7 Generated Certificate

Binding the generated certificate with https

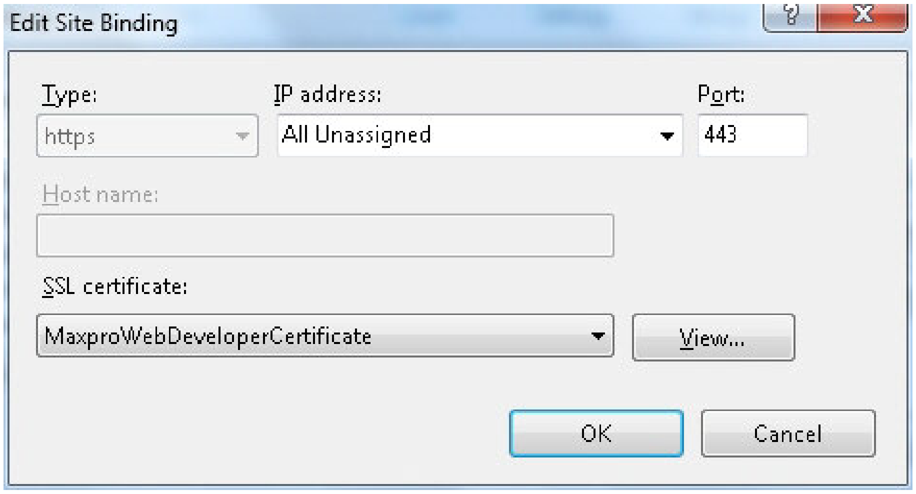
1. In the **Internet Information Manager** (IIS) window, expand the server node under **Connections** pane.
2. Navigate to **Sites > Default Web Site**.
3. Click **Bindings** in the right-most pane. The **Site Bindings** dialog appears Figure 8-8.



Type	Host Name	Port	IP Address	Binding Inform...
http		80		
https		443		
net.tcp				808:*
net.pi...				*
net.m...				localhost
msm...				localhost

Figure 8-8 Site Bindings Dialog

4. Select the type as **https** and then click **Edit**. The **Edit Site Bindings** dialog appears Figure 8-9.



Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: MaxproWebDeveloperCertificate

Figure 8-9 Edit Site Bindings

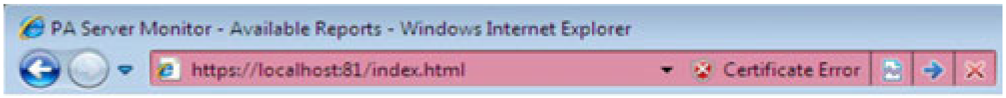
5. Select the **Demo** SSL certificate from the **SSL Certificate** drop-down list.
6. Select **All Unassigned** from the **IP Address** drop-down list.

Note: Ensure that you select All Unassigned option from the IP Address drop-down list and the port should be 443.

7. Type the port number as **443**.
8. Click **OK**.

Installing the Certificate

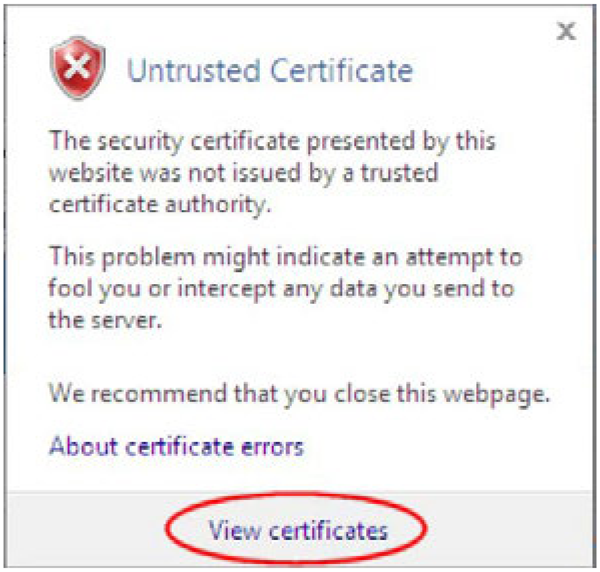
Once you have created a self signed certificate you need to install the certificate in the Internet Explorer on machines accessing the web client. If you do not install the certificate then the web browser displays the following error Figure 8-10.


PA Server Monitor - Available Reports - Windows Internet Explorer

https://localhost:81/index.html

Figure 8-10 Certificate Error

To view the error details, click on the **Certificate Error** message. A **Untrusted Certificate** message box is displayed as shown below Figure 8-11.


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.

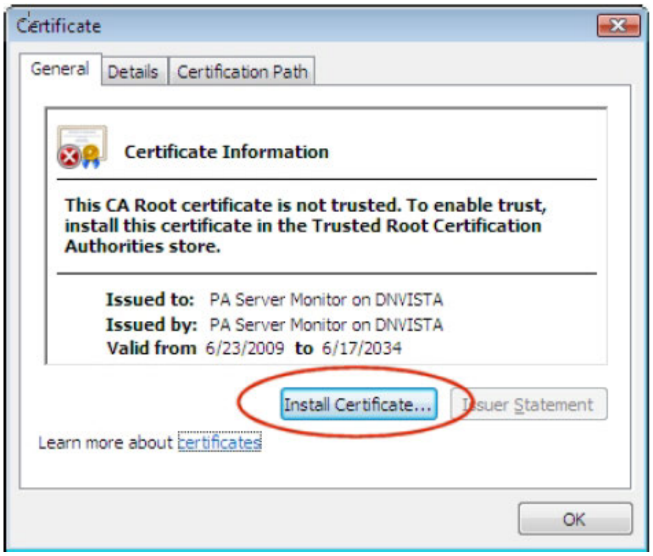
We recommend that you close this webpage.

Figure 8-11 Untrusted Certificate

To install the certificate

1. Click **View Certificate** as shown in Figure 8-11. The **Certificate** dialog box appears Figure 8-12.

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.

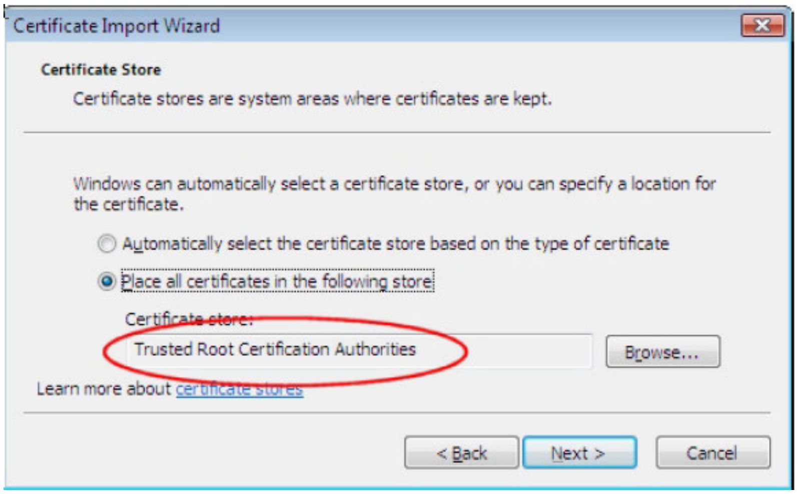
Issued to: PA Server Monitor on DNVISTA

Issued by: PA Server Monitor on DNVISTA

Valid from 6/23/2009 **to** 6/17/2034

Figure 8-12 Certificate

2. Click the **Install Certificate** button. **Certificate Import Wizard** dialog box appears Figure 8-13.


Certificate Import Wizard
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

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

Figure 8-13 Certificate Import Wizard

3. Click the **Browse** button and then select the **Trusted Certificate Authorities** option.
4. Click **Next** until **Finish** button is displayed.
5. Click the **Finish** button. A confirmation message “**you want to add the new certificate**” is displayed.

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:

1. Changing the port 443 on the MAXPRO NVR.

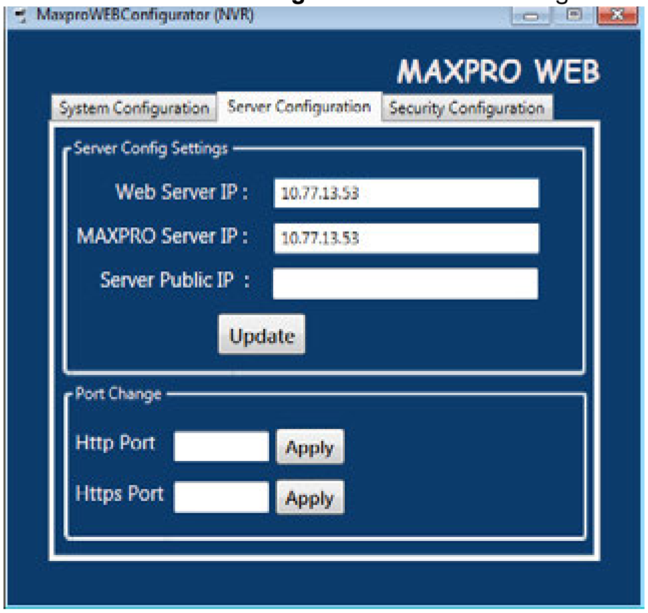
6. Changing the port in the MAXPRO Mobile app and MAXPRO Web Client.

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.

1. Double-click on the desktop. The **MAXPRO Web Configurator** dialog box appears. By default the **System Configuration** tab is selected.
2. Click the **Server Configuration** tab the following screen appears Figure 8-14.



Server Config Settings

Web Server IP : 10.77.13.53

MAXPRO Server IP : 10.77.13.53

Server Public IP :

Port Change

Http Port

Https Port

Figure 8-14 Server Configuration

3. Under **Port Change**:

- **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

1. Launch MAXPRO Mobile by tapping on your mobile device.
2. Before you log on: Tap + in the right hand side to add NVR
2. 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**.

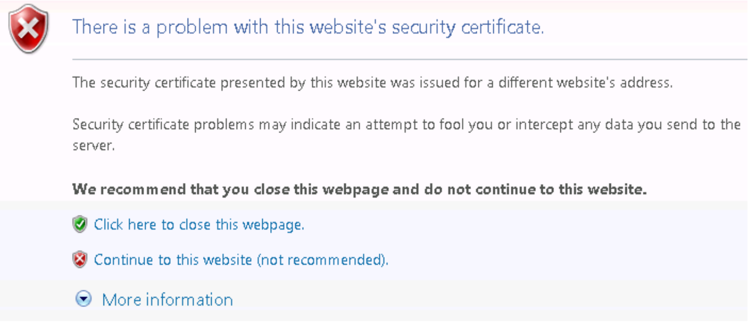
To change the port in MAXPRO NVR Web Client:

- 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**/

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.

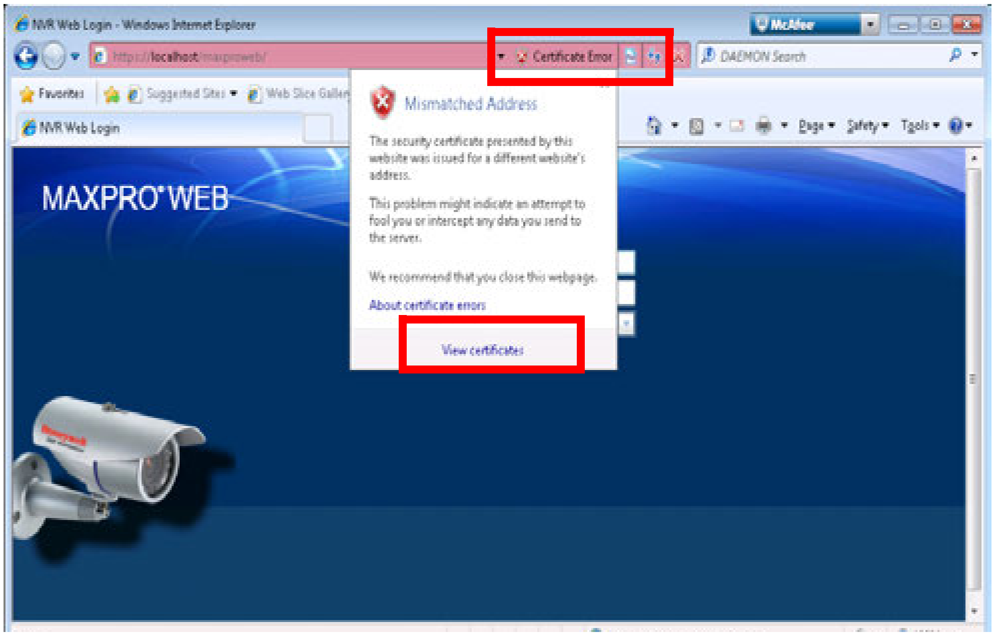
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

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:

1. Click **Continue to this web site (not recommended)** link to proceed. The NVR Web Login page is displayed.
2. Click **Certificate Error** as shown below. The **Mismatch Address** pop up message is displayed.



Mismatched Address

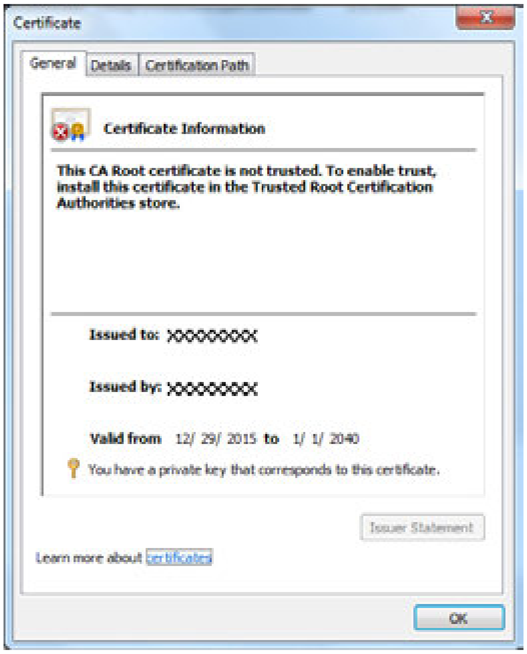
The security certificate presented by this website was issued for a different website's address.

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.

Figure 8-15 Program Maintenance

3. Click **View Certificate**. The Certificate dialog box is displayed.



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

Figure 8-16 Certificate dialog

4. Verify the following fields to check whether it is matching with the details of Server machine.
    - Issued to
    - Issued By
    - Valid From
5. Click the **Details** tab and then check other details.

This page is intentionally left blank.

MAXPRO NVR Mobile App

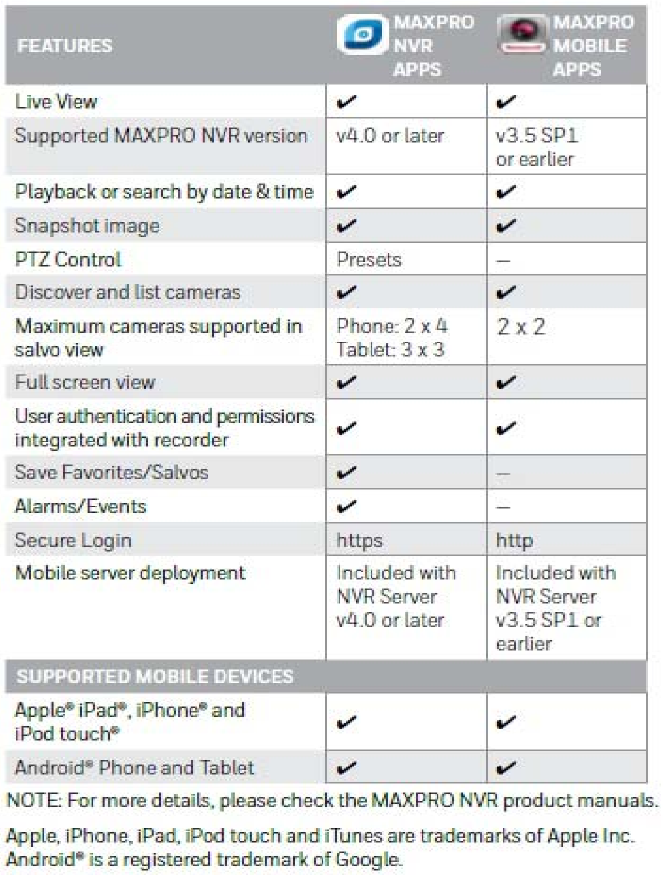
Introduction

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 only for 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.

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

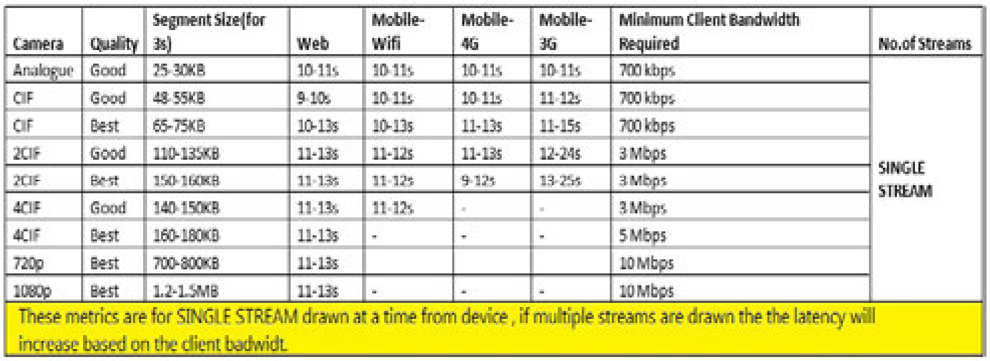
The MAXPRO NVR Mobile app is compatible with MAXPRO NVR v4.0 or later versions.

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:

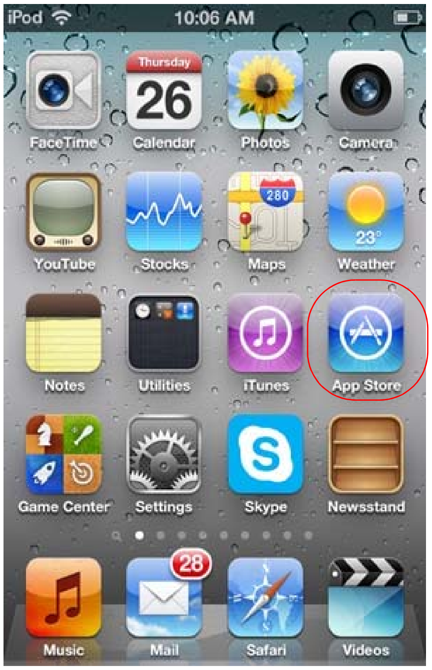
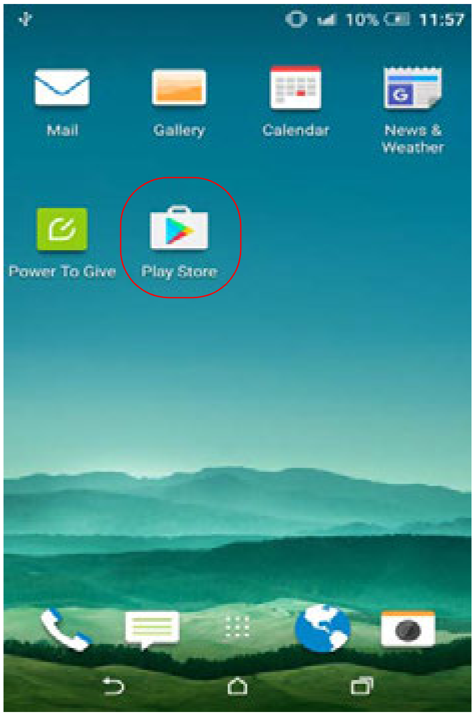


Camera	Quality	Segment Size(for 3s)	Web	Mobile-Wifi	Mobile-4G	Mobile-3G	Minimum Client Bandwidth Required	No.of Streams
Analogue	Good	25-30KB	10-11s	10-11s	10-11s	10-11s	700 kbps	SINGLE STREAM
CIF	Good	48-55KB	9-10s	10-11s	10-11s	11-12s	700 kbps	
CIF	Best	65-75KB	10-13s	10-13s	11-13s	11-15s	700 kbps	
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	

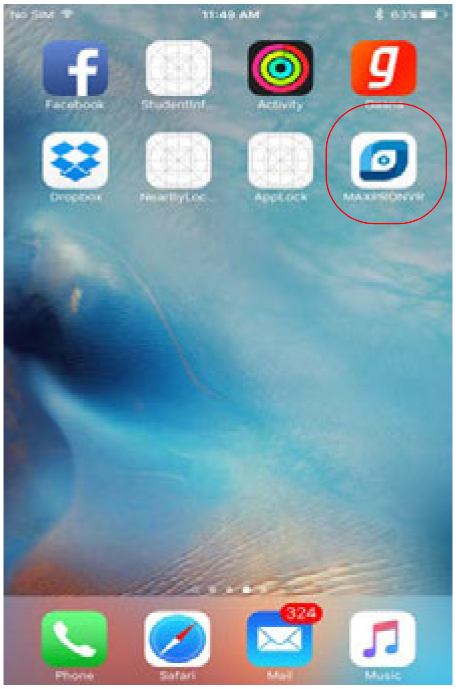
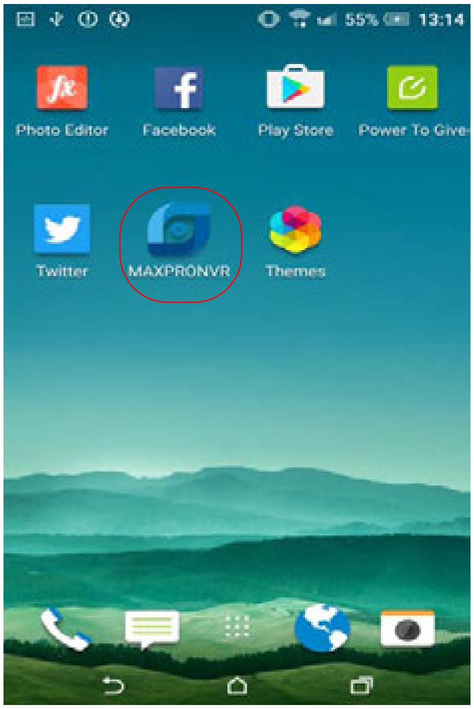
These metrics are for SINGLE STREAM drawn at a time from device , if multiple streams are drawn the the latency will increase based on the client badwidt.

Installing the MAXPRO NVR Mobile app

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
	

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

Figure 9-1 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 ***Table 1-1***. Please contact your Network Administrator for assistance.

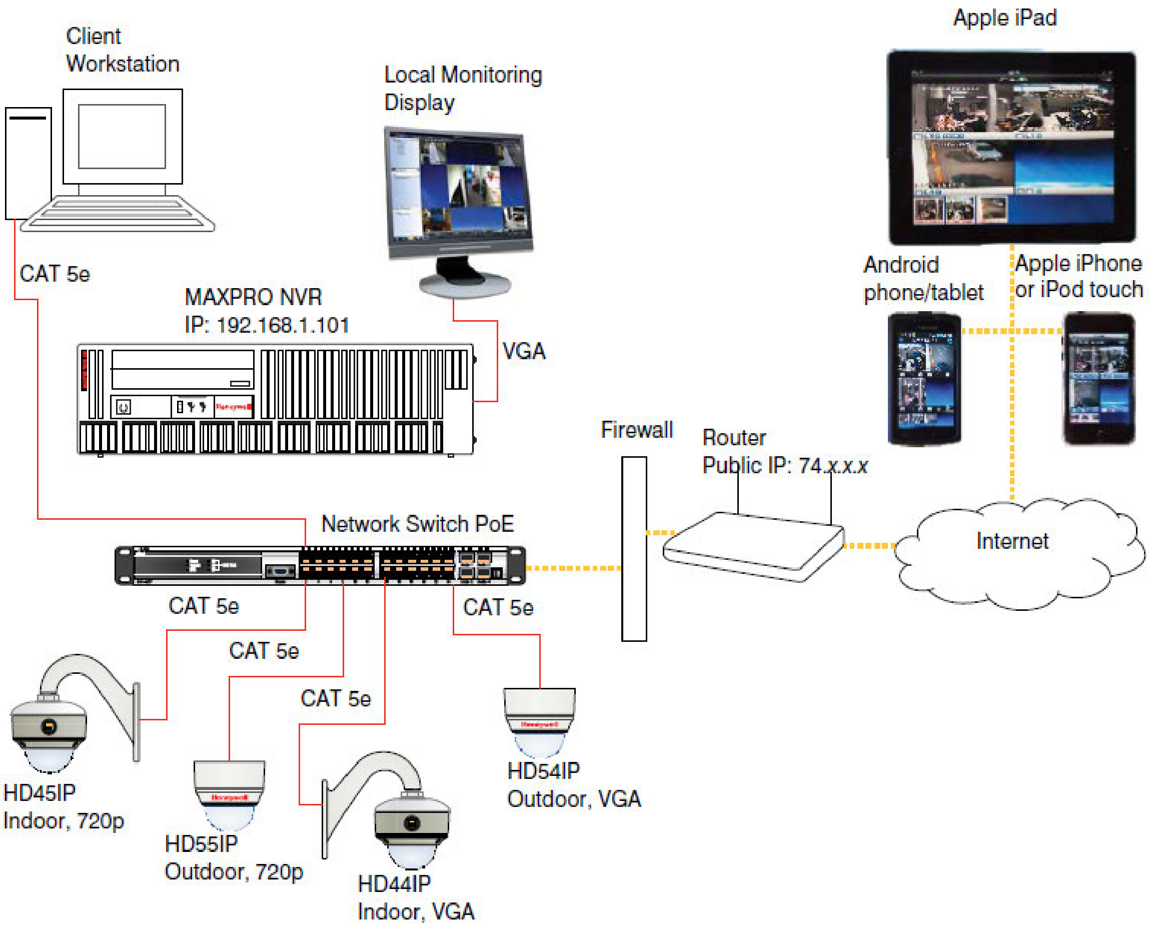


Figure 9-1 System Diagram

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 ***201*** 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.

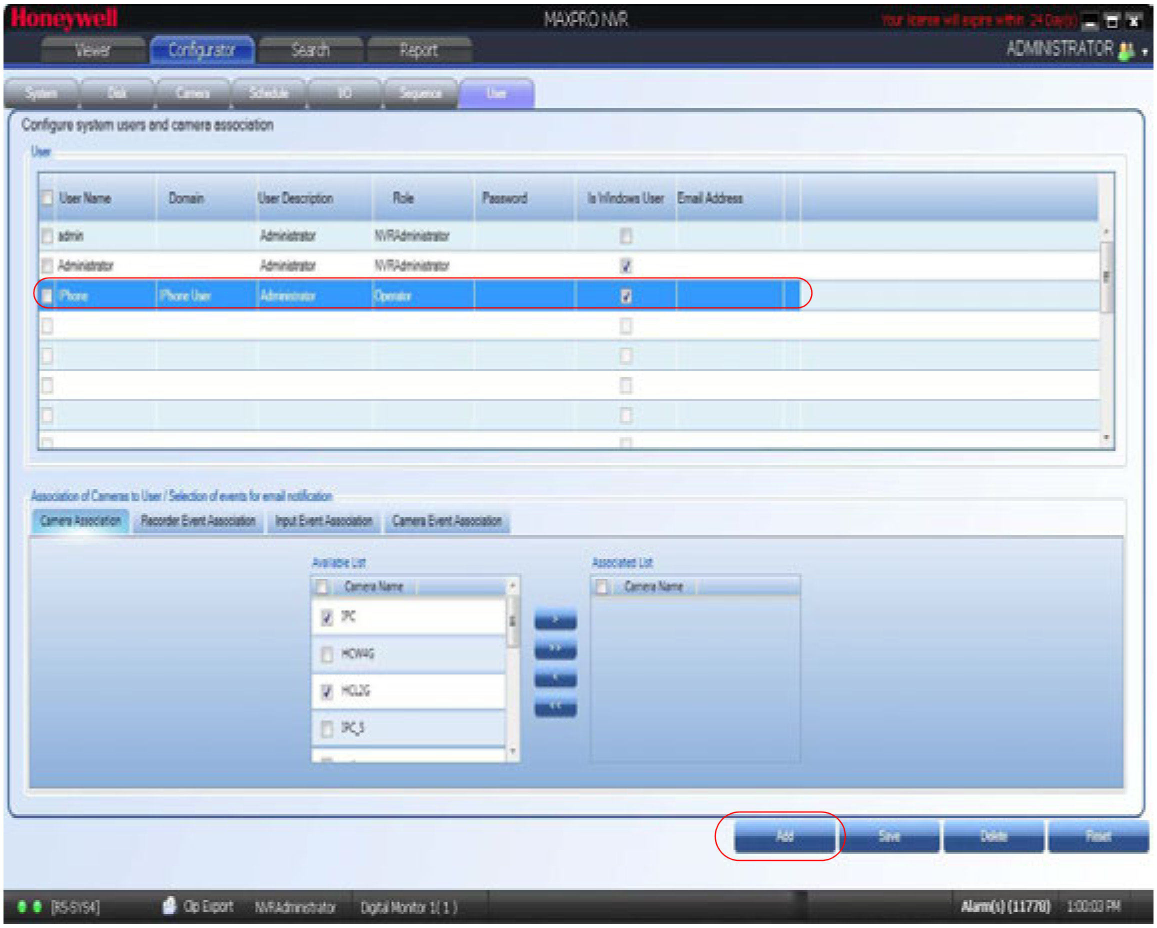
Table 1-1 Port Forwarding

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.

1. Launch MAXPRO NVR (double-click the MAXPRO NVR icon on your desktop).
2. On the **Configurator** tab, select the **User** tab, then click **Add** at the bottom.



Configure system users and camera association

User

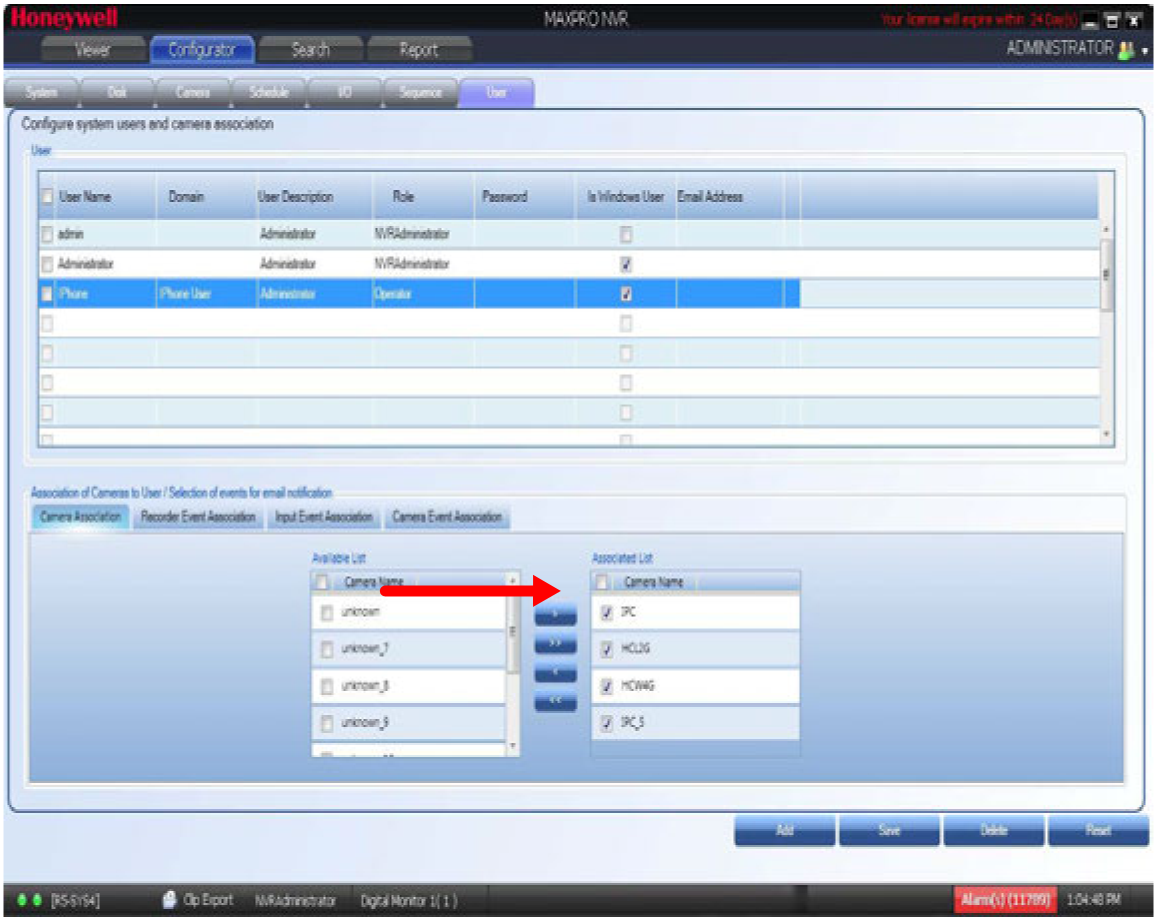
User Name	Domain	User Description	Role	Password	Is Windows User	Email Address
admin		Administrator	NVRAdministrator		□	
Administrator		Administrator	NVRAdministrator		☑	
Phone	Phone User	Administrator	Operator		☑	

Camera Name
☑ IPC
□ HCW4G
☑ HCL2G
□ IPC_5

- Double-click **User2** 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).

Selecting the Cameras to be Remotely Viewed

3. 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
□	admin		Administrator	NVRAdministrator		□	
□	Administrator		Administrator	NVRAdministrator		☑	
□	Phone	Phone User	Administrator	Operator		☑	
□						□	
□						□	
□						□	
□						□	

Association of Cameras to User / Selection of events for email notification

Available List

□	Camera Name
□	unknown
□	unknown_7
□	unknown_8
□	unknown_9

Associated List

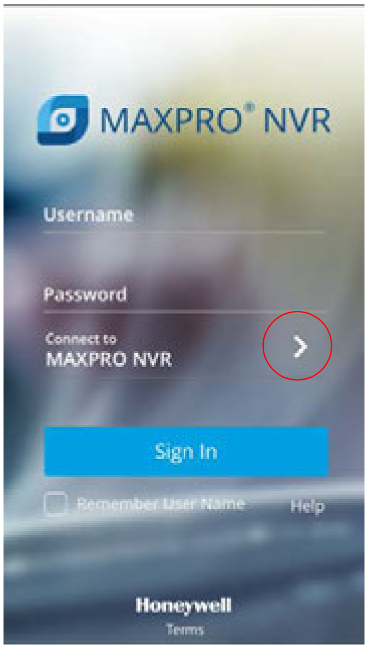
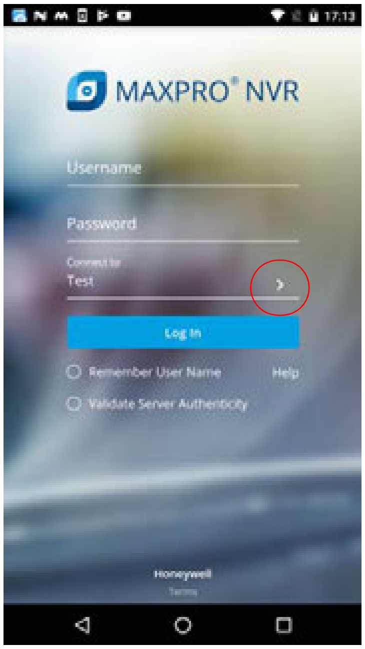
□	Camera Name
☑	IPC
☑	HCL2G
☑	HCW4G
☑	IPC_5

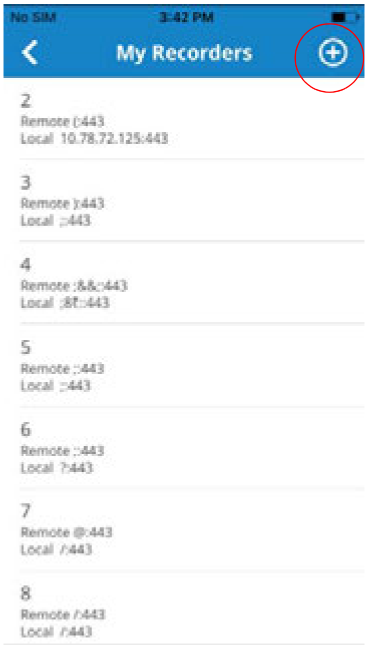
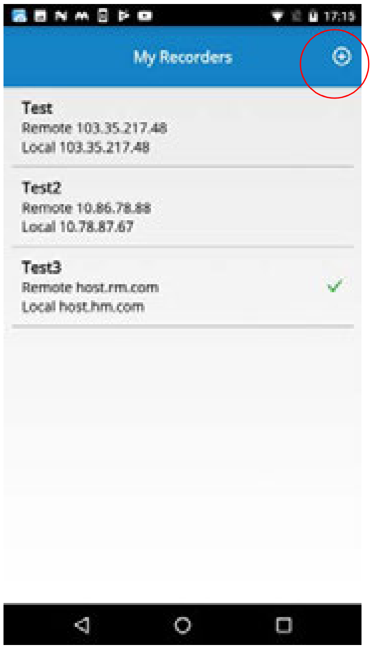
Adding the MAXPRO NVR to the MAXPRO NVR Mobile app

In the MAXPRO NVR Mobile app, you must add the MAXPRO NVR so that you can view video.

1. Launch MAXPRO NVR Mobile by tapping on your mobile device.

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
	

Apple mobile device	Android mobile device
Tap ⊕ to add a new NVR Recorder.	Tap ⊕ to add a new NVR Recorder
	

2
Remote (:443
Local 10.78.72.125:443

3
Remote):443
Local ;:443

4
Remote :&&;:443
Local ;8f;:443

5
Remote ;:443
Local ;:443

6
Remote ;:443
Local ?:443

7
Remote @:443
Local /:443

8
Remote /:443
Local /:443

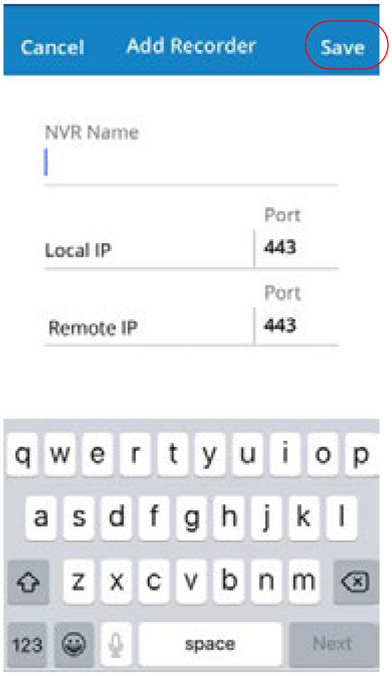
Test
Remote 103.35.217.48
Local 103.35.217.48

Test2
Remote 10.86.78.88
Local 10.78.87.67

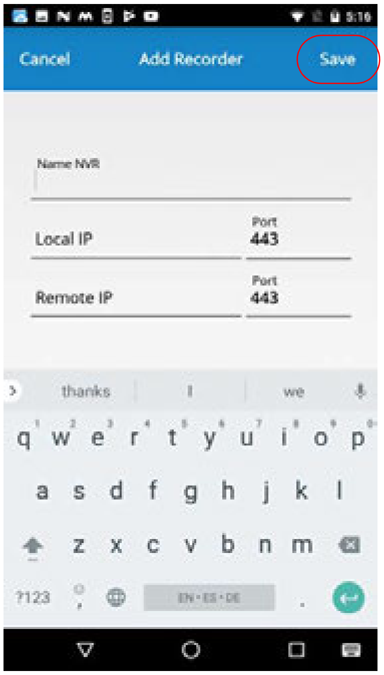
Test3 ✓
Remote host.rm.com
Local host.hm.com

3. In the Add Recorder screen:
    - 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.

<table>
<tr><th>Apple mobile device</th><th>Android mobile device</th></tr>
<tr><td>
Tap <b>Save</b> to complete adding NVR Recorder.

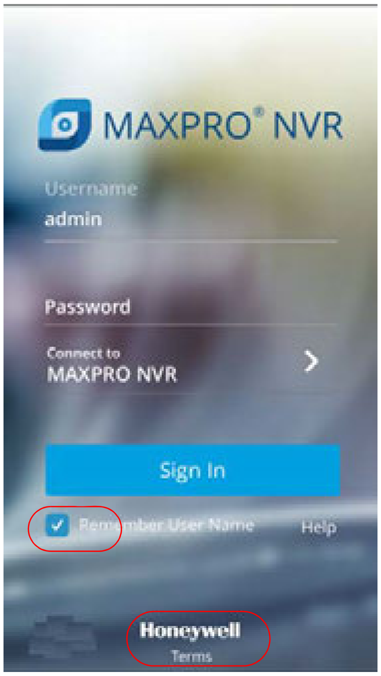
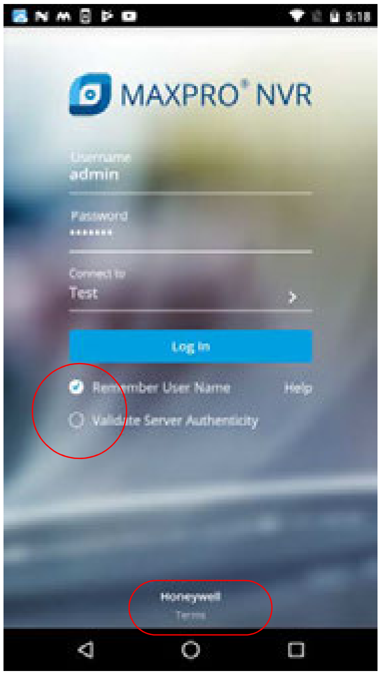


</td><td>
Tap <b>Save</b> to complete adding NVR Recorder.



</td></tr>
</table>

4. **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 ***212***).
        - 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 MAXPRO NVR Sign In ☑ Remember User Name Help Honeywell Terms	 MAXPRO® NVR Username admin Password ••••••• Connect to Test 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 IOS mobile devices only. 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 only for IOS devices.

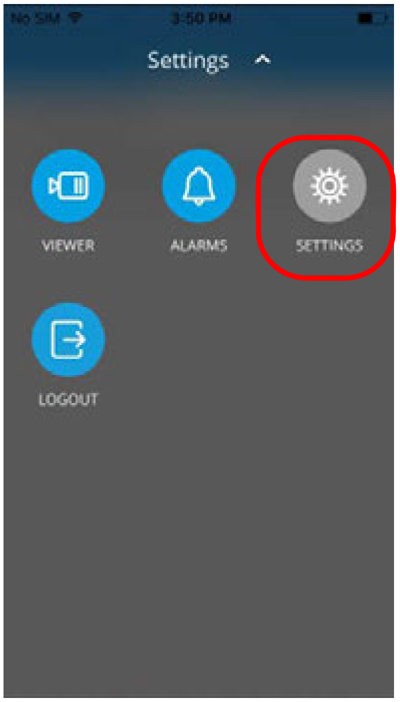
To use the Touch ID logon facility user needs to verify the Touch ID

Verifying the Touch ID

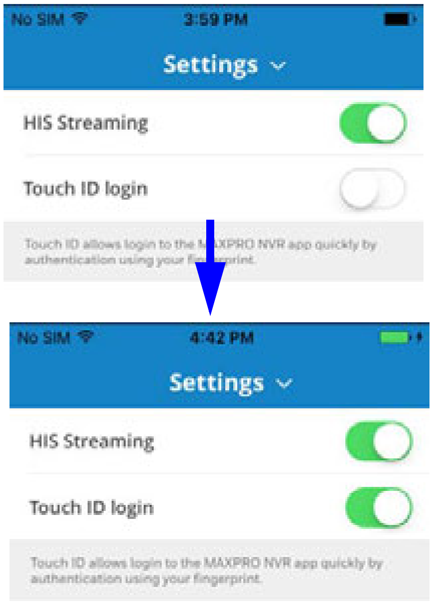
Pre-requisite:

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.

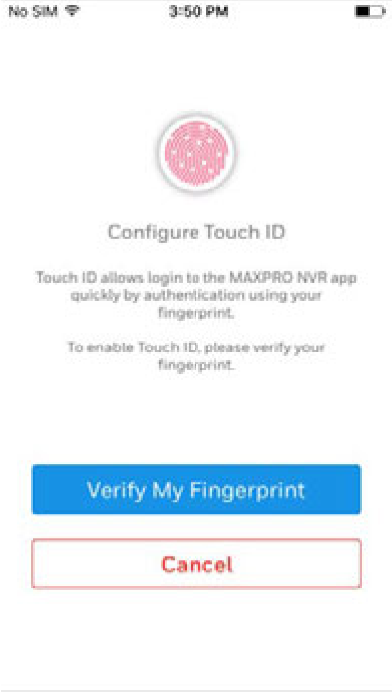
1. Manually logon to the MAXPRO app and then navigate to **Settings** screen as shown below

Apple mobile device	Android mobile device
Tap **Settings**.  No SIM 3:50 PM Settings VIEWER ALARMS SETTINGS LOGOUT	Supported in Next Release.

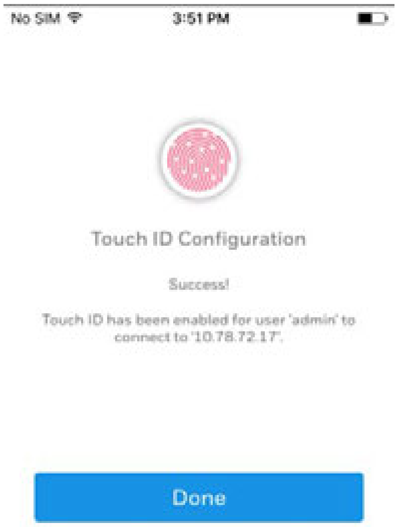
2. Tap the toggle button to turn on the **Touch ID Login** as shown below.

Apple mobile device	Android mobile device
 HIS Streaming ● Touch ID login ○ Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint. HIS Streaming ● Touch ID login ● Touch ID allows login to the MAXPRO NVR app quickly by authentication using your fingerprint.	Supported in Next Release.

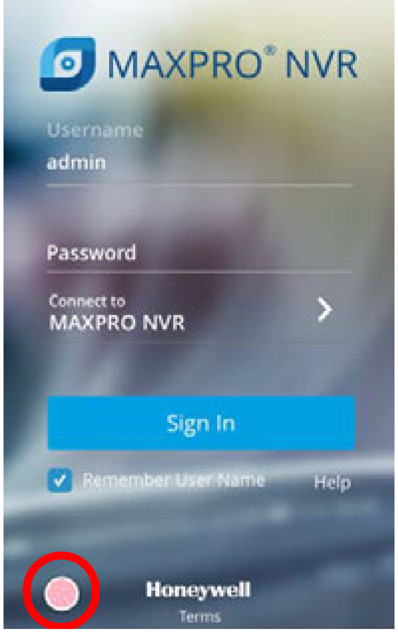
Once the Touch ID login is **ON**, the **Configure Touch ID** screen is displayed as shown below.

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. 	Supported in Next Release.

3. 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.  Touch ID Configuration Success! Touch ID has been enabled for user 'admin' to connect to '10.78.72.17'. 	Supported in Next Release.

4. Tap **Done** to complete the configuration. Fingerprint authentication option is now displayed as highlighted below.

Apple mobile device	Android mobile device
 Username admin Password Connect to MAXPRO NVR Sign In ☑ Remember User Name Help	Supported in Next Release.

5. Place your finger on the Fingerprint icon as highlighted above. You will be logged in to MAXPRO app.

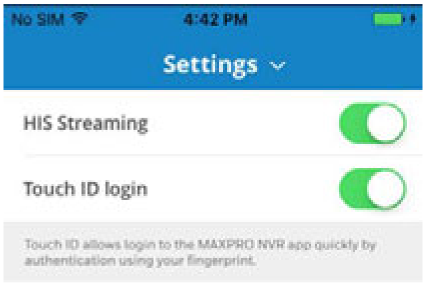
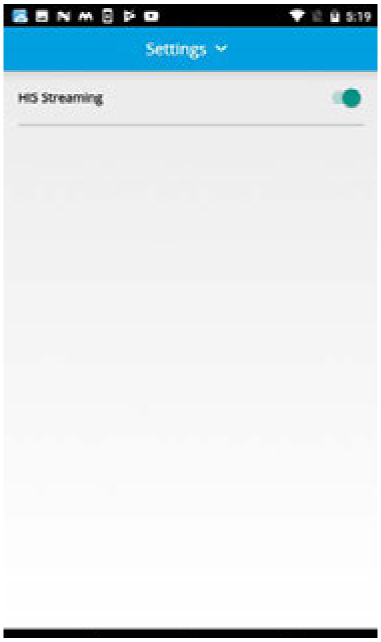
Note: Ensure that the first logon should be Manual logon.

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

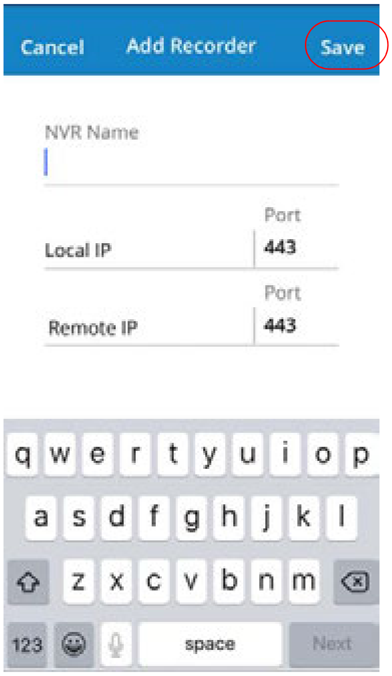
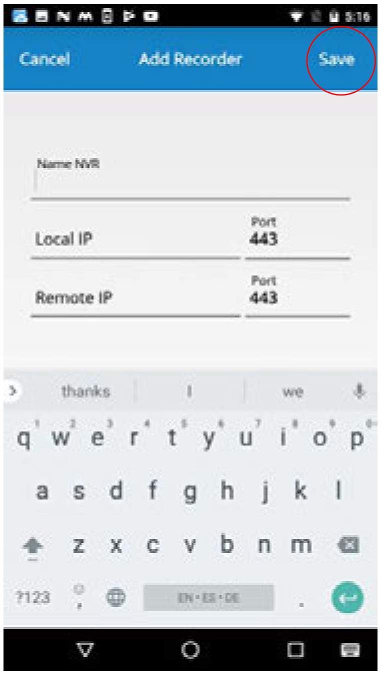
Adding Multiple NVR Recorders

To add additional NVR on the mobile app:

Note: Maximum 20 NVR configurations are allowed.

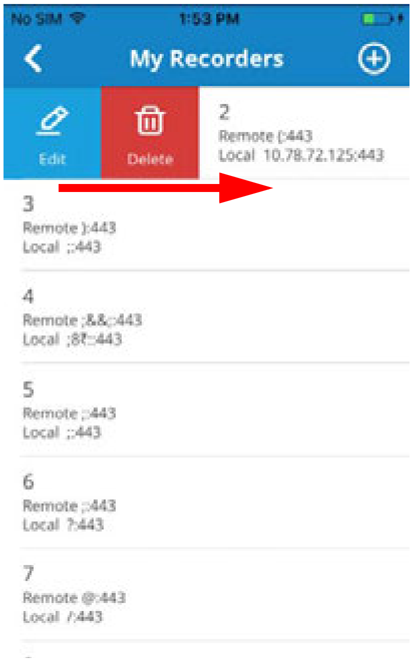
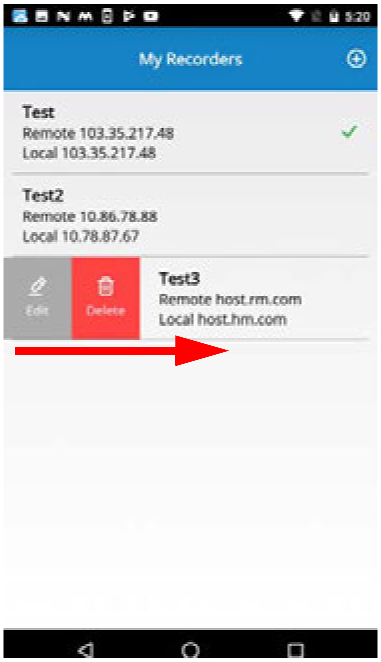
1. Tap › on the login screen. The list of already saved NVRs under **My Recorders** screen is displayed.
2. Tap ⊕. The **Add Recorder** screen is displayed.
3. Add the MAXPRO NVR Recorder as follows:
   - In the **NVR Name** field, type the name (For example Demo/Site name) for the NVR.
   - In the **Local 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.

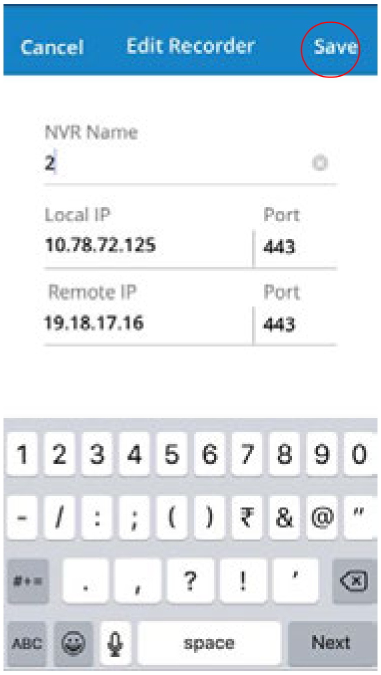
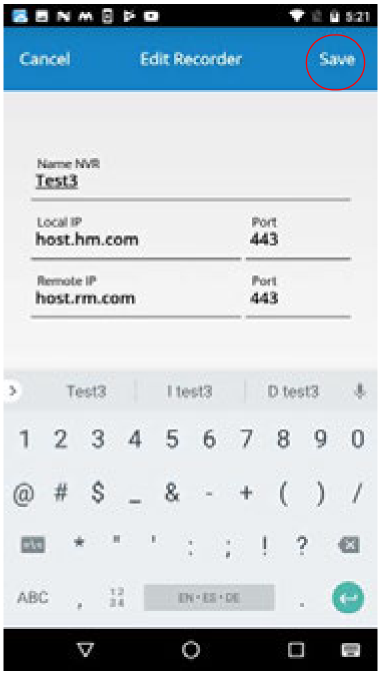
4. Repeat the step 1 through step 3 to add multiple NVR Recorders.

Apple mobile device	Android mobile device
Tap **Save** to complete adding NVR Recorder.  Cancel Add Recorder Save NVR Name Local IP Port 443 Remote IP Port 443 q w e r t y u i o p a s d f g h j k l z x c v b n m 123 space Next	Tap **Save** to complete adding NVR Recorder.  Cancel Add Recorder Save Name NVR Local IP Port 443 Remote IP Port 443 5:16 thanks I we q w e r t y u i o p a s d f g h j k l z x c v b n m ?123 EN • ES • DE

Editing NVR Recorder Details

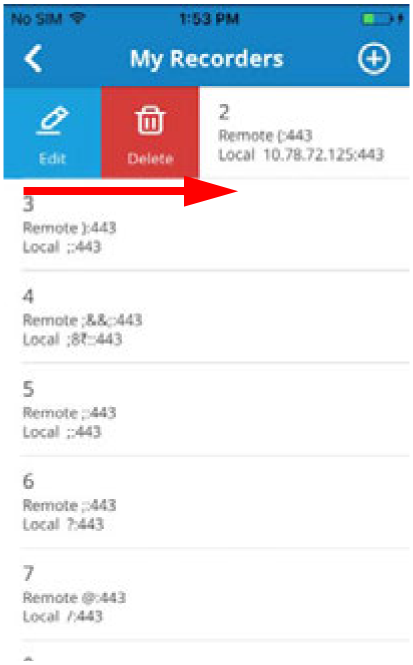
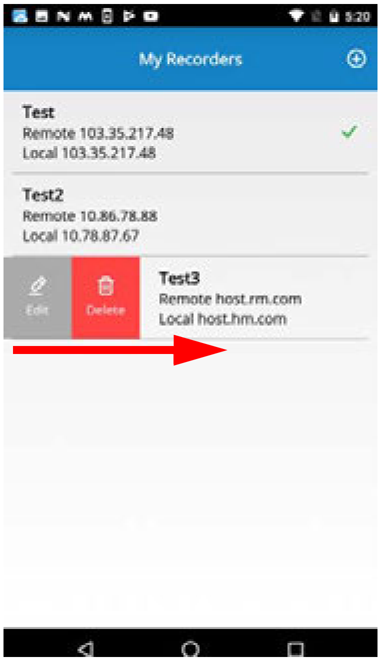
To edit the NVR Recorder details:

Apple mobile device	Android mobile device
Tap ❯. The already saved NVRs are displayed.	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.	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	 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.	Tap on **Edit**. The **Edit Recorder** screen is displayed. Modify the required details. Tap **Save** once you modify the details.
 NVR Name: 2 Local IP: 10.78.72.125 Port: 443 Remote IP: 19.18.17.16 Port: 443	 Cancel Edit Recorder Save Test3 I test3 D test3 ABC 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.	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	 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 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 ***201*** for more information.

10

SECURING MAXPRO NVR

Introduction

This chapter explains about the mandatory security settings that needs to be performed on MAXPRO NVR. This chapter includes:

- Changing the Default Windows Administrator Account Created By NVR
- Enabling Remote Desktop
- Changing the default Windows Password for Windows Logon user on MAXPRO NVR
- Changing the Windows Password for NVRServiceUser on MAXPRO NVR
- Setting Up Antivirus Software for MAXPRO NVRs
- IPsec Policies for Secured Video Data Transmission

Note: The instructions below assumes turnkey NVR/Hybrid XE,SE,PE units shipped with v4.0 or later version from factory.

Changing the Default Windows Administrator Account Created By NVR

Honeywell recommends to create and use a new Administrator and Service User account to install and configure MAXPRO NVR. NVRServiceUser is used as the logon account for all the NVR services. Perform the following 9 steps in the order as mentioned to change the default windows administrator account created by NVR.

When you turn on the machine (for turnkey NVRs shipped with v4.0 or later version from factory), **NVR-Admin** is the user what you see. logon with the default password **Password$123**. You are prompted to change the password.

Note: You must change the Password for the **Administrator** user. Ensure that you create a strong password for both **Administrator** and **Service User** account.

Step 1: Create a new user account with administrator privileges

1. Click **Start** and navigate to **Control Panel** > **All Control Panel Items** > **User Accounts**. The make changes to your use account screen appears.
2. Click **Manage Another account**/**Manage User Account** link. The **choose the account you would like to change** screen appears.
3. Click C**reate a New Account**. The **Name the account and choose the account type** screen appears.
4. Type the **New account name** in the box provided. (For example **NVRTestUser**)
5. Click the **Administrator** option and then click the **Create Account** button. the newly created account is displayed under **choose the account you would like to change** screen.

Creating a Password for the new account.

1. In the **choose the account you would like to change** screen, click the newly created account. (For example **NVRTestUser**). The **Make changes to xxxxx account** screen appears.
2. Click **Create a Password**. The **Create a password for xxxxx account** screen appears.
3. Type the **New Password** in the box provided.
4. Confirm the **Password** in the box provided.
5. Type a **Password Hint** (Optional).
6. Click **Create Password** button.

Step 2: Creating a user in NVR User's tab

1. Launch the MAXPRO NVR application in the machine with Administrator user.
2. Go to **Configurator** > **User** tab and create a user with the new account details.
3. Type the following:
   - **UserName**: Provide the username (For example: **NVRTestUser**) of the new account created in Step 1: Create a new user account with administrator privileges.
   - **User Description**; Provide the description as Administrator.
   - **Role**: Provide the role as **NVRAdministrator**.
   - **Password**: If you select the **Is Window User** check box then you don't have to provide the new password created.
   - Select the **Is Window User** check box for the new user.
4. Click **Save** and close the MAXPRO NVR application.

Step 3: Create a new Service User and Deny log on

1. Click **Start** and navigate to **Control Panel> All Control Panel Items> User Accounts**. The make changes to your use account screen appears.
2. Click **Manage Another account**/**Manage User Account** link. The **choose the account you would like to change** screen appears.
3. Click **Create a New Account**. The **Name the account and choose the account type** screen appears.
4. Type the **New account name** in the box provided. (For example **NVRServiceUser2**)
5. Click the **Administrator** option and then click the **Create Account** button. the newly created account is displayed under **choose the account you would like to change** screen.

Creating a Password for the new Service User account.

Note: By default the password for NVRServiceUser is **tZN"&4x!sF**.

1. In the **choose the account you would like to change** screen, click the newly created account. (For example **NVRServiceUser2**). The **Make changes to xxxxx account** screen appears.
2. Click **Create a Password**. The **Create a password for xxxxx account** screen appears.
3. Type the **New Password** in the box provided.
4. Confirm the **Password** in the box provided.
5. Type a **Password Hint** (Optional).
6. Click **Create Password** button.

Denying Log on

1. In **Run** command window, type secpol.msc. The **Local Security Policy** window is displayed.
2. In the **Console** tree, double-click **Local Policies**, and then click **User Rights Assignments**.
3. In the **Details** pane, double-click **deny log on locally**.
4. Click **Add User or Group** and then add the appropriate account (**NVR Service user)** to the list of accounts that possess the **Logon as** a service right.
5. Click **Apply** and then click **OK**.

Creating a user in NVR User's tab

1. Launch the MAXPRO NVR application in the machine.
2. Go to **Configurator** > **User** tab and create a user with the new account details.

3. Type the following:

    - **UserName**: Provide the username (For example: **NVRServiceUser2**) of the new account created in Step 3: Create a new Service User and Deny log on.
    - **User Description**; Provide the description as Administrator.
    - **Role**: Provide the role as **NVRAdministrator**.
    - **Password**: If you select the **Is Window User** check box then you don't have to provide the new password created.
    - Select the **Is Window User** check box for the new user (For example: **NVRServiceUser2**).

4. Click **Save** and close the MAXPRO NVR application.

Step 4: Update the NVR services with new Service user account Credentials

1. Launch the **Services** (**Run** > **Services.msc**.) window and **Stop** the following services in the order mentioned:
    - NeoStorageExtWDService
    - NEOStorageServer
    - NEOStorageServer2
    - TrinityArchival (Applicable only for 4.0 Release version)
    - TrinityController
    - TrinitySmart VMD services
    - TrinityServer
2. Right-click on **TrinityServer** service and then click **Properties**. The **TrinityServer Properties** dialog appears.
3. Click the **Logon** tab.
4. Under **This account** option:
    - Replace the **Username** from **./Administrator** to **./NVRServiceUser2** which is created in Step 3: Create a new Service User and Deny log on in Section .
    - Type the **Password** which is created in **Creating password for the new account** section.
    - Confirm the **Password**.
5. Click **Apply** and then click **OK**.

Note If you are changing the username of a service for the first time then a service Pop message **The account xxxx has been granted the Log On As a service right** is displayed. Click **OK** to proceed.

6. Similarly repeat steps 2 through step 5 to update the account details for the following services.
   - TrinitySmart VMD services
   - TrinityController
   - TrinityArchival (Applicable only for 4.0 Release version)
   - NeoStorageExtWDService
   - NEOStorageServer
   - NEOStorageServer2
7. After updating account details, restart the following services in the order mentioned.
   - TrinityServer
   - TrinitySmart VMD services
   - TrinityController
   - TrinityArchival (Applicable only for 4.0 Release version)
   - NeoStorageExtWDService
   - NEOStorageServer
   - NEOStorageServer2

Step 5: Updating the Application pools in IIS

1. Launch the Internet **Information Services (IIS) Manager** window. (Run > Inetmgr).
2. Under **Connections** pane expand the main node and then click the **Application pools** node.The list of application pools are displayed in the Application Pools pane.
3. Click **ISOM_Application** and then under **Actions** pane > **Edit Application Pool**, click **Advanced Settings** link. The **Advanced Settings** dialog appears.
4. Under **Process Model** node, click **Identity** and then click the browse button,. The **Application Pool Identity** dialog appears.
5. Under **Custom account** option, click the **Set** button. The **Set Credentials** dialog is displayed.
6. Type the **User name** (For example: **NVRServiceUser2**), **Password** which is created in Step 3: Create a new Service User and Deny log on in Section and then **Confirm the Password**. Click **OK**.
7. Click **OK** in the **Application Pool Identity** box and **Advanced Settings** box.
8. Under **Connections** pane expand the **Sites** node and then navigate to **Default Web site** > **Live** node.
9. Under **Actions** pane > **Manage Application**/**Browse Application**, click **Advanced Settings** link. The **Advanced Settings** dialog appears.
10. Under **General**, click **Physical Path Credentials** and then click the browse button. The **Connect as** dialog appears.
11. Under **Specific User** option, click the **Set** button. The **Set Credentials** dialog is displayed.
12. Type the **User name** (For example: **NVRServiceUser2**), **Password** which is created in Step 3: Create a new Service User and Deny log on in Section and then **Confirm the Password**. Click **OK**.
13. Click **OK** in the **Connect as** box and Advanced Settings box.

14. Similarly repeat the step 8 through step 13 for the following application under **Sites > Default Web site** node.
    - MaxproWeb
    - MediaConverter
    - Playback
    - ISOM
15. Logoff and logon once again to the machine with above created account credentials.
16. In the **Run** command box type the **IISreset** command to rest the IIS services.

Step 6: Disable the Administrator Account

1. Logon to the machine with newly created account in step 1
2. Launch **Computer Management** window or Click **Start** and right-click **Computer** to choose **Manage**. The **Computer Management** window is displayed.
3. Under **Computer Management** node, click **Local Users and Groups** > **Users**. The corresponding users are displayed in the middle pane.
4. Right-click on the **Administrator** and then select **Properties**. The **Administrator Properties** dialog is displayed.
5. In the **General** tab, select the **Account is disabled** check box.
6. Click **Apply** and then click **OK**.

Below steps should be performed only on NVR 4.0 embedded box shipped from Honeywell:

7. Right-click on the **NVRTestUser** (Applicable only in **4.0** Release version) and then select **Properties**. The **NVRTestUser Properties** dialog is displayed.
8. In the **General** tab, select the **Account is disabled** check box.
9. Click **Apply** and then click **OK**.
10. Restart the machine and then Logon with the new user credentials.

Step 7: Restart all the services

- Check if all the below services are running after restarting the machine. Ensure that you manually restart if any of the service is stopped.
    - TrinityServer
    - TrinitySmart VMD services
    - TrinityController
    - TrinityArchival (Applicable only for 4.0 Release version)
    - NeoStorageExtWDService
    - NEOStorageServer
    - NEOStorageServer2

Note When you logon as a new user, all the MAXPRO NVR shortcuts will not be displayed and you need to copy the shortcuts from Administrator account to new user account (**NVRTestUser).**

Step 8: Copy MAXPRO NVR Desktop Shortcuts from Administrator to NVRTestUser

After you logon as a new user the following shortcuts will not be available on the desktop. You need to manually copy all the desktop shortcuts from Administrator account to new user account (**NVRTestUser).**

Note These shortcuts are applicable only for Server machines.

- MAXPRO NVR
- MAXPRO NVR Web Client
- MAXPRO NVR Wizard
- MAXPROClipPlayer.exe (Applicable only in **4.0** Release version)
- MAXPRONVRStatusMonitor.exe (Applicable only in **4.0** Release version)
- Honeywell Device Search Utility
- Honeywell IP Utility
- Web Configurator Utility
- Ultrakey Configurator Utility

To Copy the MAXPRO NVR Desktop Shortcuts from Administrator to NVRTestUser:

1. In Server machine, navigate to **C:\User\Public\Desktop** and **C:\User\Administrator\Desktop** and then copy the following shortcuts.
   - MAXPRO NVR
   - MAXPRO NVR Web Client
   - MAXPRO NVR Wizard
   - MAXPROClipPlayer.exe (Applicable only in **4.0** Release version)
   - MAXPRONVRStatusMonitor.exe (Applicable only in **4.0** Release version)
   - Honeywell Device Search Utility
   - Honeywell IP Utility
   - Web Configurator Utility
   - Ultrakey Configurator Utility
2. Paste the above copied shortcuts to **C:\User\NVRTestUser\Desktop**.

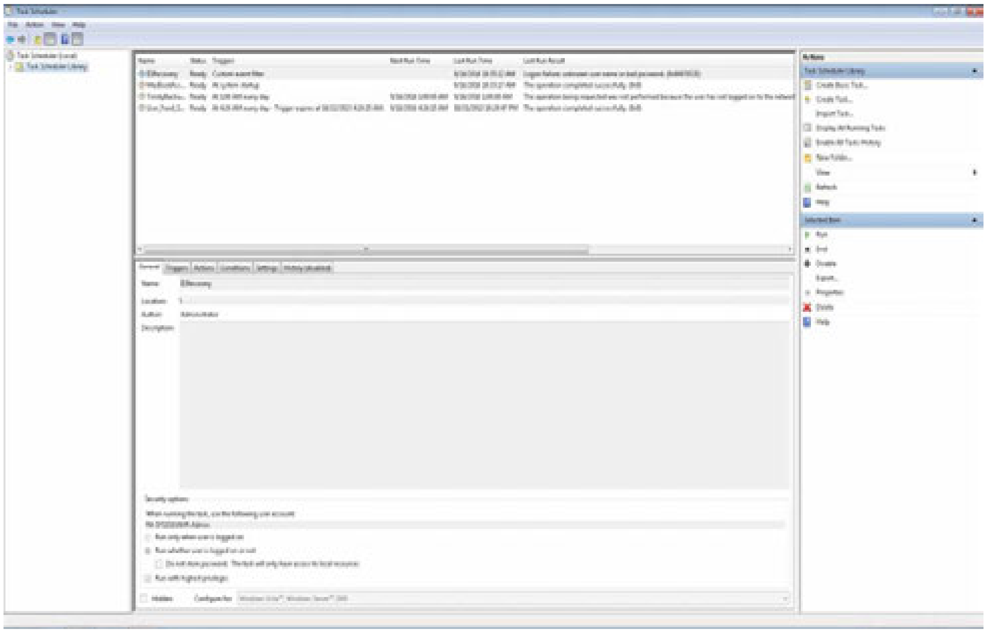
Step 9: Update the user credentials of Task Schedules with new user account (For EX: NVRTestUser)

After performing the above 8 steps, you need to update the user name and password of the following **Task Schedules** with new user account created in Step 1: Create a new user account with administrator privileges section on page 226:

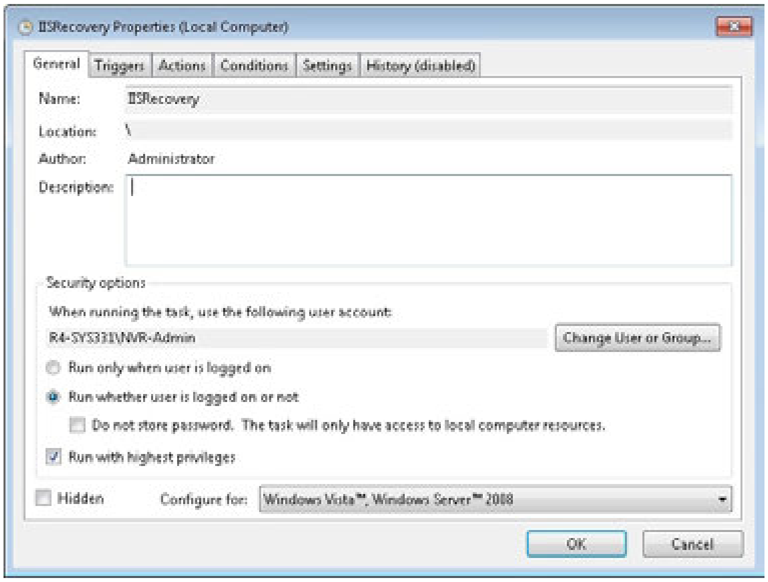
- IISRecovery
- MaxBootAssistant
- TrinityBackupScheduler

To update the Task Schedule credentials:

1. Click **Start** > **Run**. In **Run** command window, type **Taskschd.msc**. The **Task Scheduler** window is displayed.
2. Navigate to **Task Scheduler Library** node on the left pane. The task schedules are displayed on the right pane as shown below.



3. Right click **IISRecovery** and then select **Properties**. The **IISRecovery Properties** dialog box appears as shown below. By default the **General** tab is selected.



Name: IISRecovery

Location: \

Author: Administrator

Description:

Security options

When running the task, use the following user account:

R4-SYS331\NVR-Admin

○ Run only when user is logged on

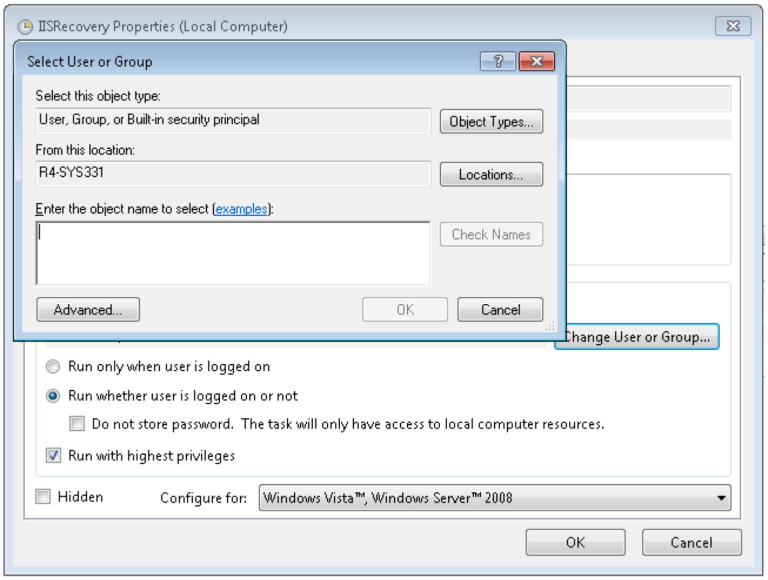
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

4. Click the **Change User or Group** button. The **Select User or Group** dialog box appears.



Select this object type:

User, Group, or Built-in security principal

From this location:

R4-SYS331

Enter the object name to select (examples):

○ Run only when user is logged on

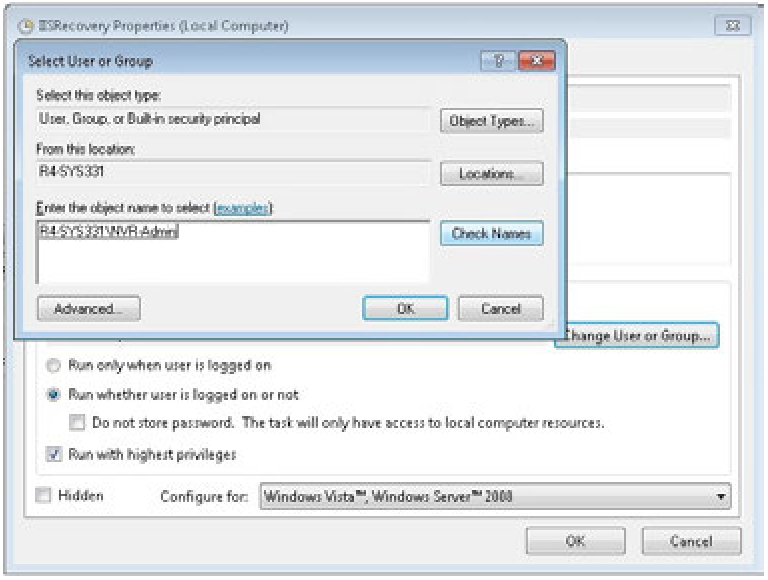
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

5. Under **Enter the Object name to select**, type the Windows Logon user name created in Step 1: Create a new user account with administrator privileges section on page 226 and then click **Check Names**. The System name and Username is displayed (For Example: T69-SYSS\NVR-Admin as shown below.



Select this object type:
User, Group, or Built-in security principal

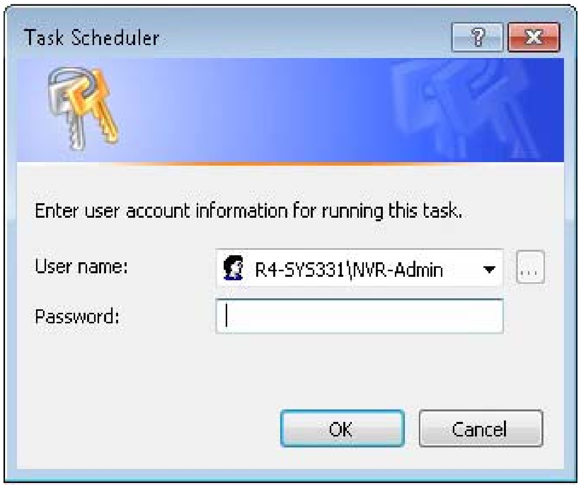
From this location:
R4-SYS331

Enter the object name to select (examples):
R4-SYS331\NVR-Admin

○ Run only when user is logged on
● Run whether user is logged on or not
□ Do not store password. The task will only have access to local computer resources.
☑ Run with highest privileges
□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

6. Click **OK** in Select User or Group window.

7. Click **OK** in IISRecovery Properties dialog box. A **Task Scheduler** window appears and prompts you to enter the Password as shown below.



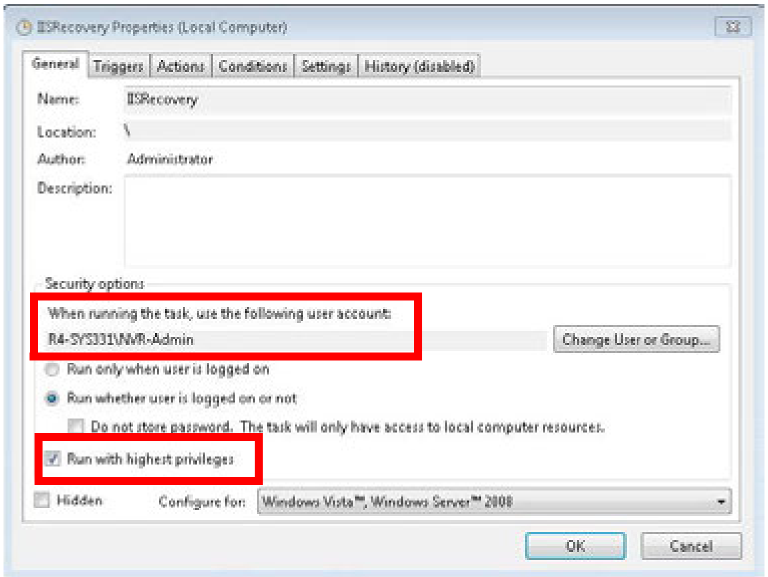
Enter user account information for running this task.

User name: R4-SYS331\NVR-Admin

Password:

8. Type the Windows Logon **Password** created in Step 1: Create a new user account with administrator privileges section on page 226 and then click **OK**. The updated credentials are displayed under **General Tab** > **Security Options** area as highlighted below.

9. Select the **Run with highest privileges** check box and then click **OK** to complete.


IISRecovery Properties (Local Computer)

Name: IISRecovery

Location: \

Author: Administrator

Description:

Security options

When running the task, use the following user account:

R4-SYS331\NVR-Admin

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

10. Similarly repeat the step 3 through step 7 for "MaxBootAssistant" and "TrinityBackupScheduler" and update the credentials.

Enabling Remote Desktop

By default NVR 4.0 turnkey units will have the Remote Desktop option disabled. Perform the the below steps in the order to enable remote desktop.

- Enable remote desktop services
- Enable remote desktop option

Safety Precautions for Enabling Remote Desktop

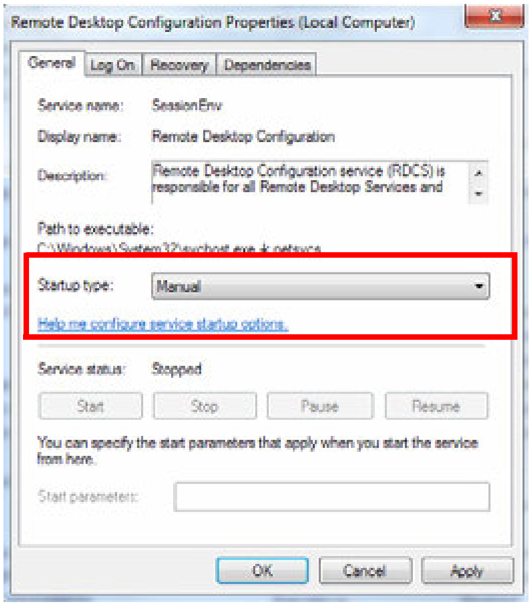
- NVR should never be used directly over the internet. Ensure that you always establish a connection with VPN first and then access NVR through the VPN.
- Ensure that NVR with Remote Desktop Enabled must have Antivirus software installed and maintained up to date. See Setting Up Antivirus Software for MAXPRO NVRs to configure the antivirus software.
- Ensure that all the security patches are up to date in your PC.

WARNING! **Running remote desktop services or Terminal Server makes your system vulnerable to network attacks from malicious entities. This is especially true if your NVR is made accessible over the internet. Please understand the risks involved with this and enable it only if absolutely necessary.**

To enable remote desktop services

1. In the **Run** command window, type **services.msc** and then click **OK**. The **Service** window appears.

2. From the list of services, locate **Remote Desktop Configuration (SessionEnv)**.
3. Right-click **Remote Desktop Configuration (SessionEnv)** and then click **Properties**. The **Properties** dialog box is displayed.By default the **General** tab is selected.
4. Select **Manual** from the **Start type** drop-down list as shown below and then click **OK**.


Remote Desktop Configuration Properties (Local Computer)

Service name: SessionEnv

Display name: Remote Desktop Configuration

Description: Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and

Path to executable:
C:\Windows\System32\svchost.exe -k netsvcs

Startup type: Manual

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

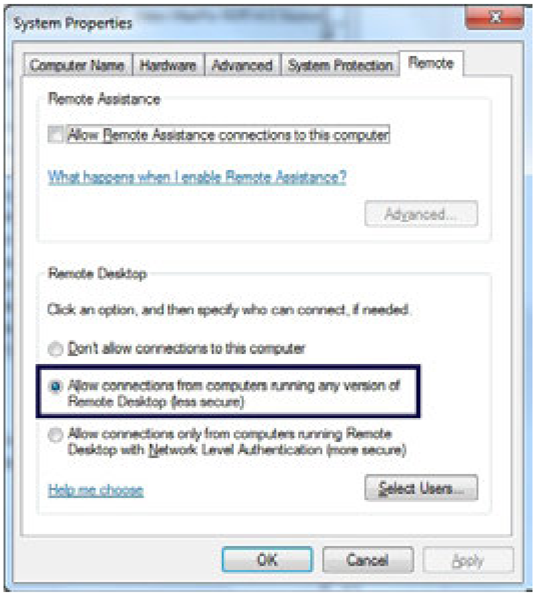
Start parameters:

Figure 6-1 Properties Dialog

5. Similarly from the list of services, locate **Remote Desktop Services (TermService) service** and **Remote Desktop Services UserMode Port Redirector (UmRdpService) service**.
6. Repeat the step 3 and step 4 to enable remote desktop.

To enable remote desktop option

1. Click **Start > Computer**. Right click on **Computer** and then select **Properties**. The Control Panel Home screen appears.
2. Click **Remote settings** on the left pane. The **System Properties** dialog box appears as shown below.



Remote Assistance

□ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

Figure A-2 System Properties

3. Under **Remote Desktop**, ensure that **Allow connections from computers running any version of Remote Desktop (less secure)** option is selected and then click **OK**.

Changing the default Windows Password for Windows Logon user on MAXPRO NVR

Note: For Honeywell turnkey box solutions (XE, SE, PE) with v4.0 or later shipped from factory, the default Windows user name is **NVR-Admin** and Windows password is **Password$123**.

You can customize and change the default password.

To change the default password

1. Change the Windows password. Perform the steps as explained in the Step1: Changing the Windows password section on page 239.
2. After changing the Windows password you should update the user credentials of Task Schedules with the new username/password created. See Step 9: Update the user credentials of Task Schedules with new user account (For EX: NVRTestUser) section on page 232.

Changing the Windows Password for NVRServiceUser on MAXPRO NVR

Note: For Honeywell turnkey box solutions (XE, SE, PE) with v4.0 or later shipped from factory, the default service user name is **NVRServiceUser** and Windows password is **tZN"&4x!sF**.

You can customize and change the default password.

To change the default password

1. Change the Windows password. See the Step1: Changing the Windows password section on page 239.

After changing the Windows password, perform the following:

2. Change the password for the following MAXPRO NVR Services. See the Step 2: Changing the NEOStorageServer, NEOStorageServer2, Trinity Smart VMD Service, TrinityServer, TrinityController passwords, and TrinityArchival. section on page 239.
   - NEOStorageServer
   - NEOStorageServer2
   - TrinityServer
   - TrinityController
   - Trinity Smart VMD Service
   - TrinityArchival

3. Reset the Cache Credentials for MAXPRO Web in Internet Information Services (IIS) Manager. See the Step 3: Resetting the Cache Credentials for MAXPRO Web in Internet Information Services (IIS) Manager section on page 240.

Note: Ensure that passwords set for the MAXPRO Web in IIS, NEOStorageServer, NEOStorageServer2, TrinityServer, TrinityController and Trinity Smart VMD Service should match with the Windows password.

Step1: Changing the Windows password

1. Press **Ctrl**+**Alt**+**Del** and click **Change a password**...
2. Click the **Administrator/NVRServiceUser**.
3. Type the **Old password**, **New password** and **Confirm password**.

Step 2: Changing the NEOStorageServer, NEOStorageServer2, Trinity Smart VMD Service, TrinityServer, TrinityController passwords, and TrinityArchival.

1. Click **Start**>**Control Panel**>**Administrative Tools**> **Services**. A list of services are displayed Figure A-3.

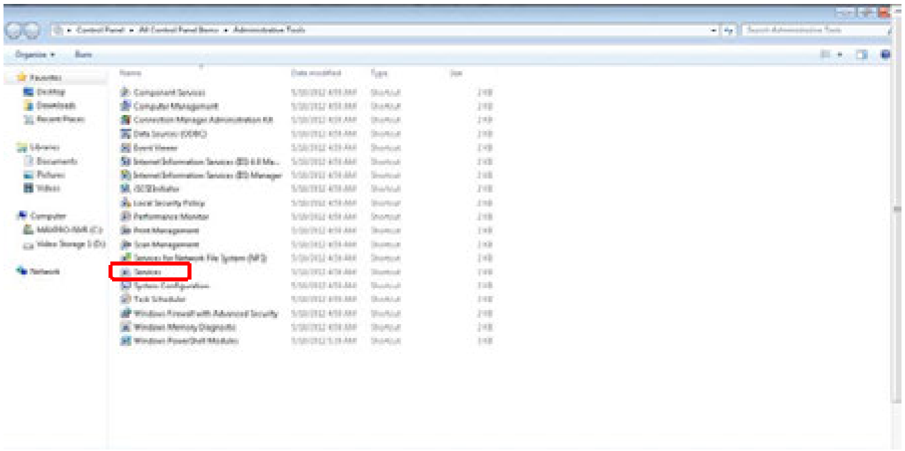


Figure A-3 Application Tools

2. Double-click **Services**. The **Services** window appears Figure A-4

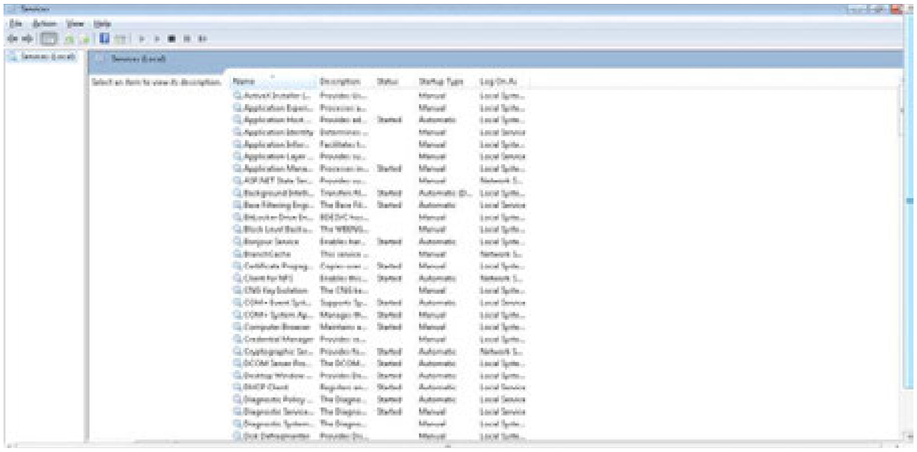


Figure A-4 Services

3. Right-click the **NEOStorageServer** service and click **Properties**. The **NEOStorage Server Properties** dialog box appears Figure A-5.

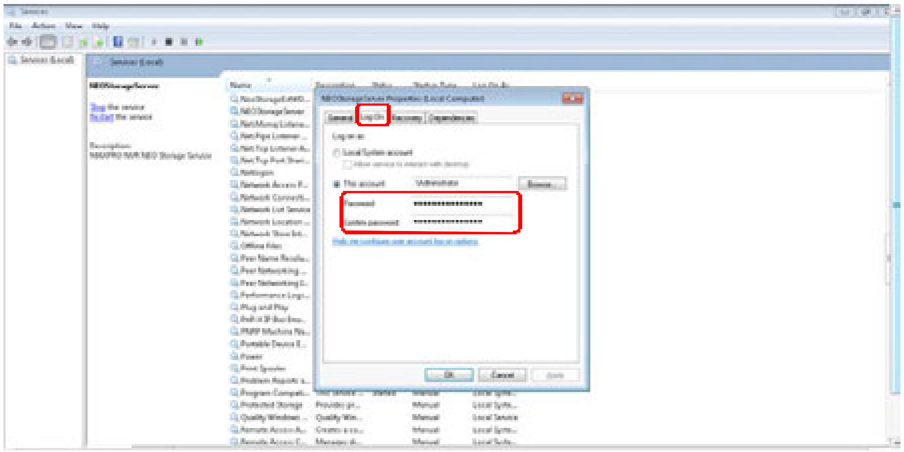


Figure A-5 NEOStorage Engine Properties

4. Click the **Log On** tab.

5. Type the new password in **Password**.

6. Type the new password again in **Confirm Password**.

7. Click **OK**. Follow the similar procedure to change the password for the NeoStorageServer2, Trinity Smart VMD Service, TrinityServer, TrinityController and TrinityArchival services.

8. Restart all the services manually one by one in order to apply the new changes.

9. Launch the MAXPRO NVR desktop client, and verify if the system is running after changing the password.

Step 3: Resetting the Cache Credentials for MAXPRO Web in Internet Information Services (IIS) Manager

1. Click **Start>Control Panel>Administrative Tools> Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** window is displayed.

2. In the **Connection** pane, navigate to **Machine name** > **Sites**> **Default Web Site** > **MaxproWeb**. The **MaxproWeb Home** screen is displayed Figure A-6.

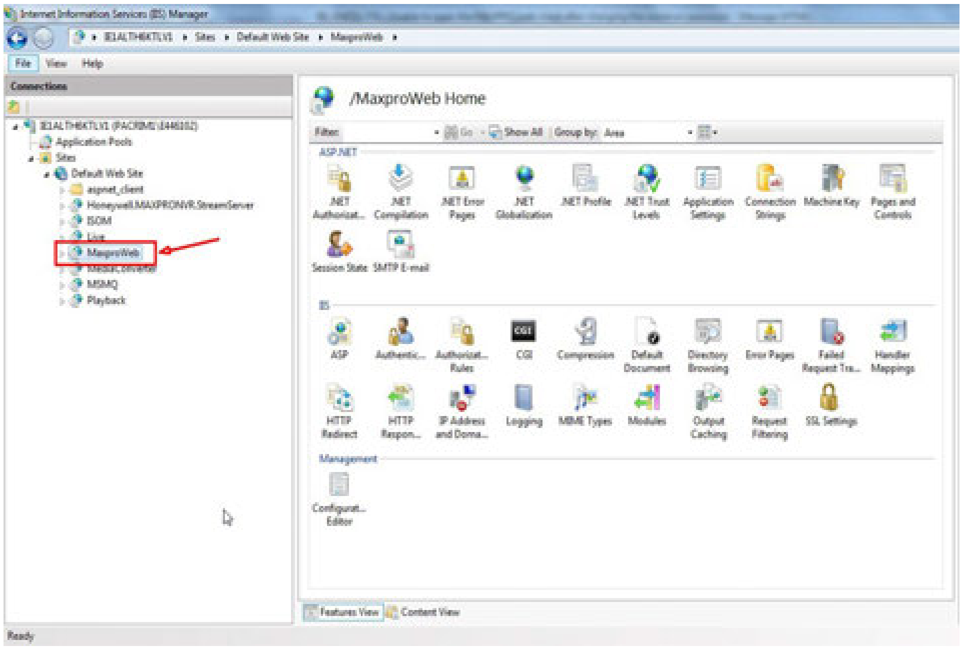
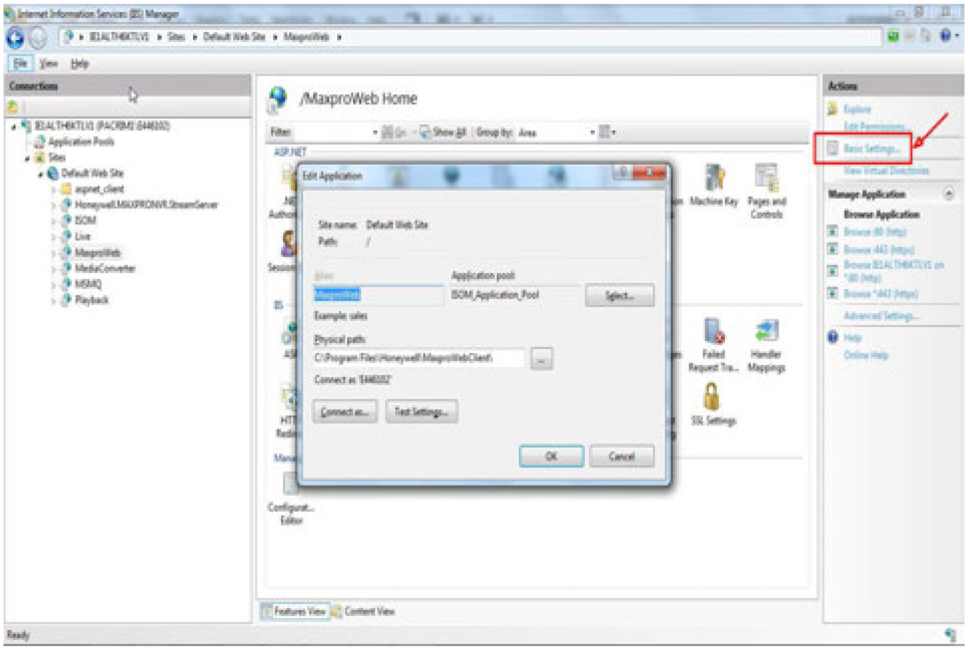


Figure A-6 MAXPRO Web Home page

3. In the **Actions** pane, click **Basic Settings**. The **Edit Application** dialog box appears Figure A-7.



Edit Application

Site name: Default Web Site
Path: /

Alias:
MaxproWeb

Application pool:
ISOM_Application_Pool

Select...

Example: sales

Physical path:
C:\Program Files\Honeywell\MaxproWebClient\

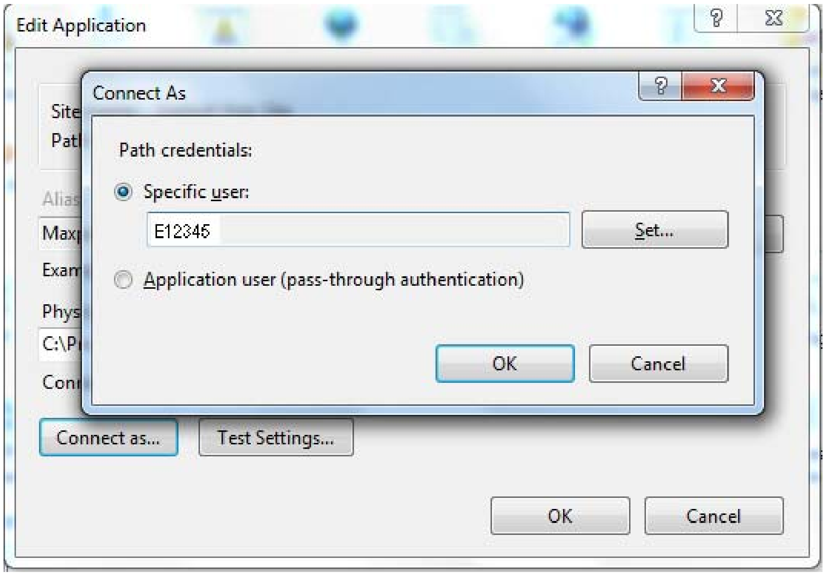
Connect as 'E446102'

Connect as...
Test Settings...

OK
Cancel

Figure A-7 Edit Application Dialog

4. Click **Connect as...**, the **Connect As** dialog appears Figure A-8.



Path credentials:

● Specific user: E12345

○ Application user (pass-through authentication)

Figure A-8 Connect As Dialog

5. Click **Set**. The **Set Credentials** dialog appears Figure A-9.

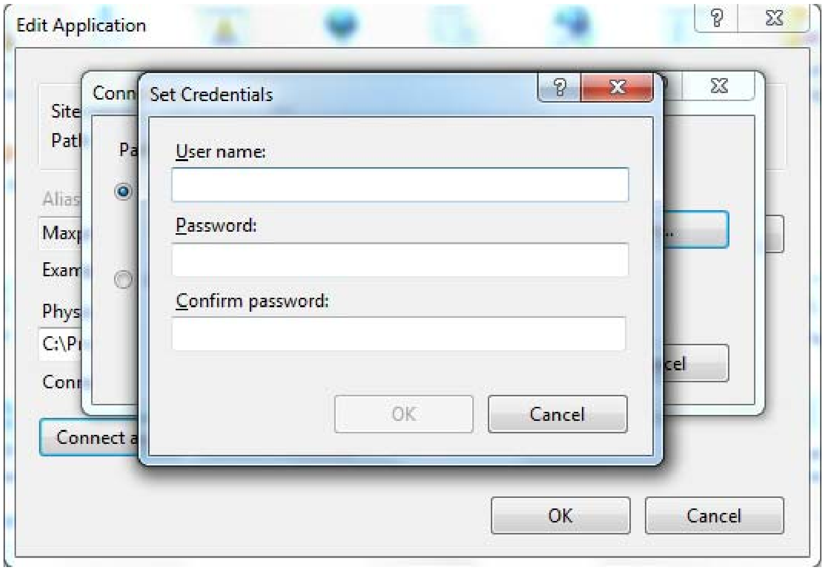


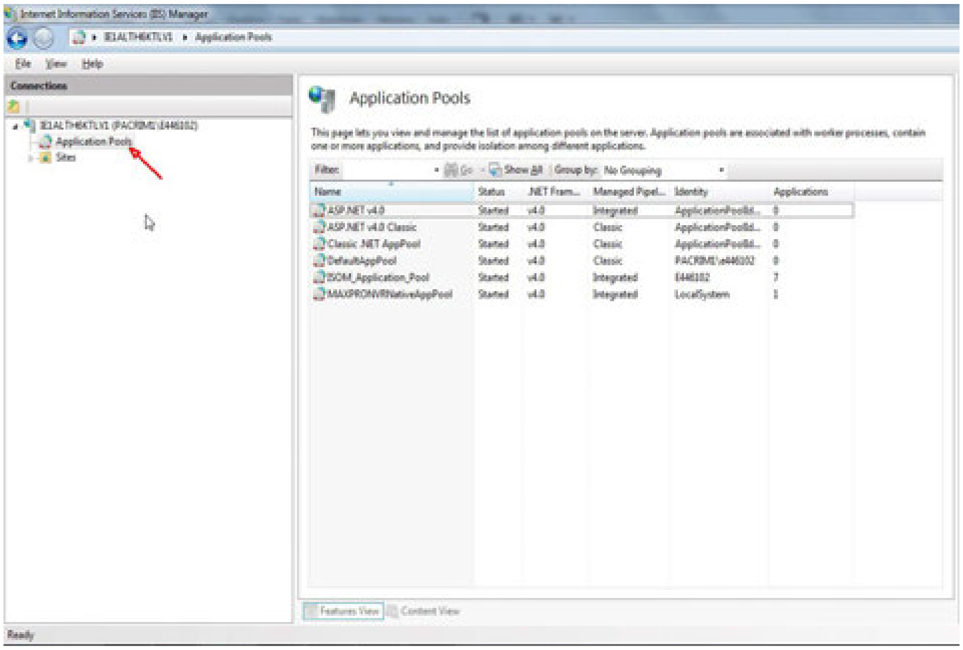
Figure A-9 Set Credentials Dialog

6. Type the **User name** in the box provided.
7. Type the new **Password** in the box provided.
8. Confirm the password and then click **OK**. Similarly perform the above steps to reset the cache password for other applications that uses the user credentials to authenticate.

To reset the Cache credentials for Application Pools, perform the following:

1. Click **Start**>**Control Panel**>**Administrative Tools**> **Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** window is displayed.

2. In the **Connection** pane, navigate to **Application Pools.** The **Application pools** screen is displayed Figure A-10.


Internet Information Services (IIS) Manager
IE1ALTH6KTLV1 ▸ Application Pools
File View Help
Connections
IE1ALTH6KTLV1 (PACRIM1\E446102)
Application Pools
Sites
Features View
Content View
Ready

Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

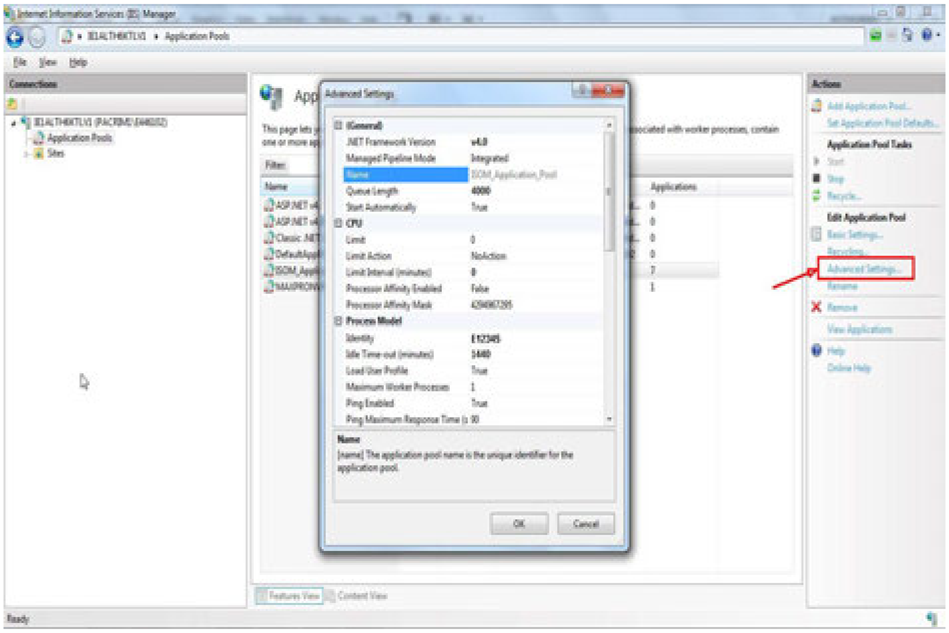
Filter: Go Show All Group by: No Grouping

Name	Status	.NET Fram...	Managed Pipel...	Identity	Applications
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolId...	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
Classic .NET AppPool	Started	v4.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Classic	PACRIM1\e446102	0
ISOM_Application_Pool	Started	v4.0	Integrated	E446102	7
MAXPRONVRNativeAppPool	Started	v4.0	Integrated	LocalSystem	1

Figure A-10 Application pools screen

3. In the **Application pools** pane, select **ISOM_Application_pool**.

4. In the **Actions pane** > **Edit Application Pool**, click **Advanced Settings**. The **Advanced Settings** dialog box appears Figure A-11.



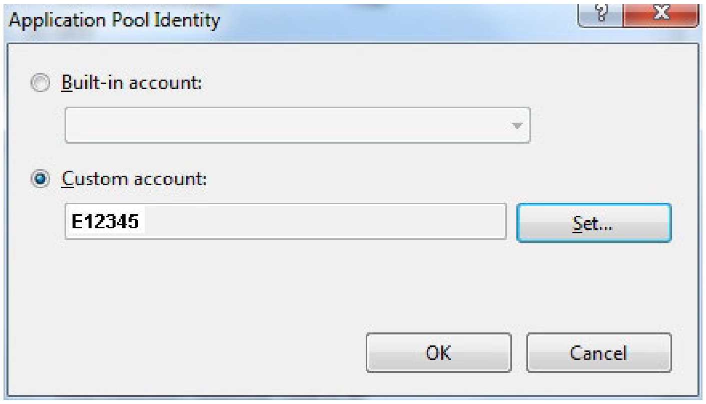
Advanced Settings

(General)	
.NET Framework Version	v4.0
Managed Pipeline Mode	Integrated
Name	ISOM_Application_Pool
Queue Length	4000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	0
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	E12345
Idle Time-out (minutes)	1440
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (s	90

Name
[name] The application pool name is the unique identifier for the application pool.

Figure A-11 Advanced Settings Dialog

5. In the **Process Model**, select **Identity** and then click ... . The **Application Pool Identity** dialog box appears Figure A-12.



○ Built-in account:

● Custom account: E12345

Figure A-12 Advanced Settings - Application Pool Identity Dialog

6. Click **Set**. The **Set Credentials** box appears Figure A-13.

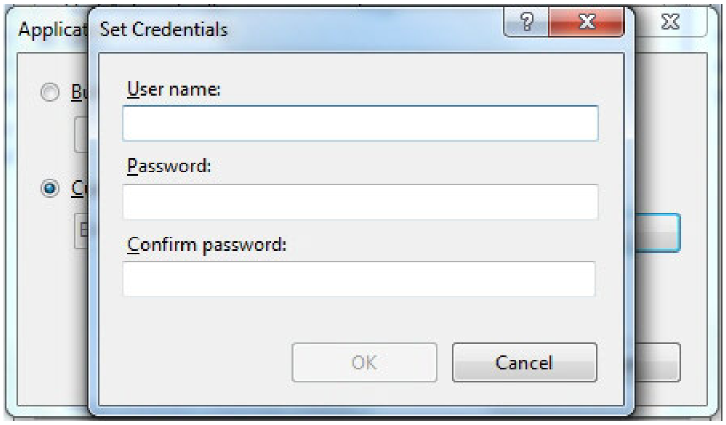


Figure A-13 Set Credentials box

7. Type the **User name** in the box provided.
8. Type the new **Password** in the box provided.
9. Confirm the password and then click **OK**.
Open the MAXPRO NVR Web Client from your browser and verify that the logging on to web client works, if a non-Windows MAXPRO NVR user configured in the NVR system.

Setting Up Antivirus Software for MAXPRO NVRs

Honeywell supports installing the following Antivirus software on MAXPRO NVRs. The following Antivirus applications have been tested, and function well with the MAXPRO NVR operational parameters.

- McAfee VirusScan Version 8.8, McAfee Antispyware
- Microsoft Security Essentials
- Symantec AntiVirus Edition 2008 (Norton), 2010, 2013
- Sophos v7.3.0
- AVG v8.5.409

Auto-protection and Auto-updates

Auto-protection (Live file-system protection) is recommended along with auto-updating through the Internet or a Network Virus Definition Server. When using auto-update, it may be necessary to reboot the NVR for some of the patches/updates to take effect. This is not normally needed during standard virus definition updates; however, occasionally Antivirus Software Engine updates trigger that require system reboots. In this scenario, it is suggested that, if the Antivirus software is installed and configured on an NVR system, auto-updates are disabled and updates need to be done manually by the operator to manage the reboots.

IMPORTANT! Do Not Schedule DATA Drive Scans

Do not set the Antivirus software to run any scheduled hard disk scans of DATA (Video Storage) drives. This can hinder the performance of the NVR unit and cause other potential problems. In particular:

- The NVR software is CPU and Memory dependant. Having antivirus software scan DATA (Video Storage) drives while recording video can cause degradation of recording performance.
- Scanning DATA (Video Storage) drives can also create a problem due to the DATA files constantly being updated and written to. The virus software will attempt to re-scan these files after each data change as video is being saved.

IPsec Policies for Secured Video Data Transmission

This section describes how to create highly secured network connections using the IPsec policies for secure video data transmission. The recommended types of policies are:

- Unrestricted
- Blocked
- Secured

User needs create these 3 types of policies depending upon the network devices. The detail explanation is given below.

Unrestricted Network

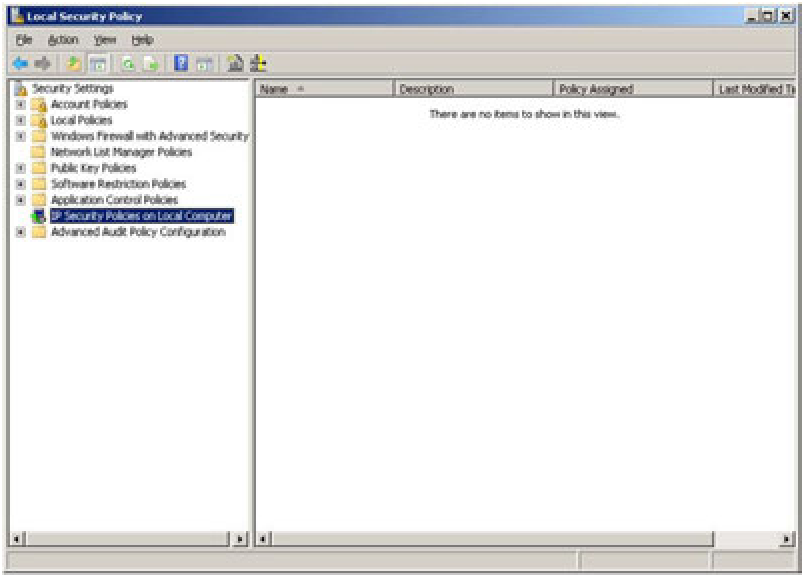
Unrestricted network is for connecting within your control (inside LAN), so that you need not perform any security settings for communication between the network devices. This also applies to devices which cannot establish IPsec communication.

Example where unrestricted network will be required is as follows:

- Connections between cameras and recorder (MAXPRO NVR)
- Connections between Ultra key, Joysticks keyboards to Recorders (MAXPRO NVR) and Video Management Solutions (MAXPRO VMS)

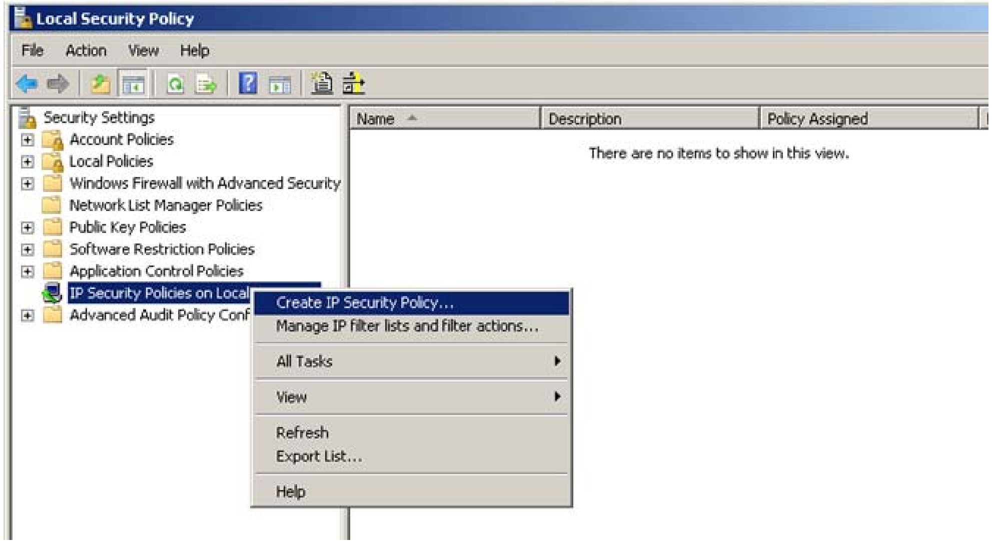
How to configure Unrestricted connections rule

1. In Run command box type **secpol.msc** and then click **OK**. The **Local Security Policy** window is displayed as shown below.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Name
Description
Policy Assigned
Last Modified Ti

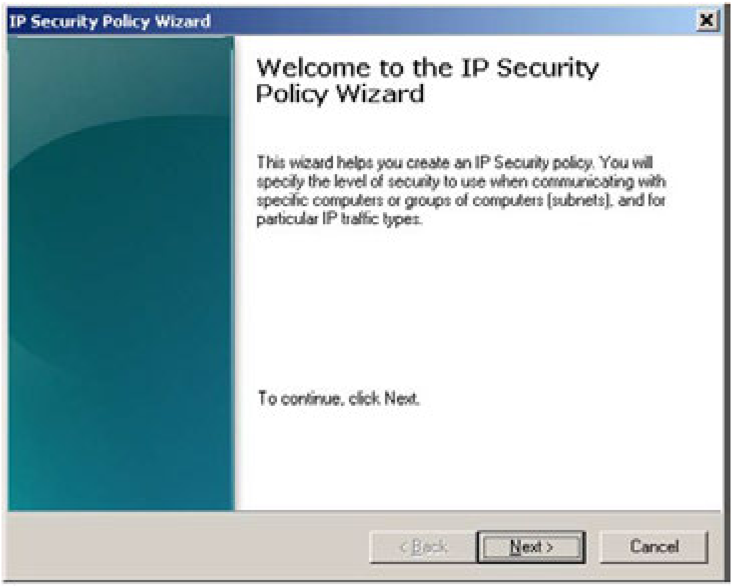
There are no items to show in this view.

2. Under **Security Settings** pane, right click on **IP Security Policies on Local Computer** and then select **Create IP Security Policy** as shown below.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Conf
Name
Description
Policy Assigned
Create IP Security Policy...
Manage IP filter lists and filter actions...
All Tasks
View
Refresh
Export List...
Help

There are no items to show in this view.

The **IP Security Policy Wizard** appears as shown below.

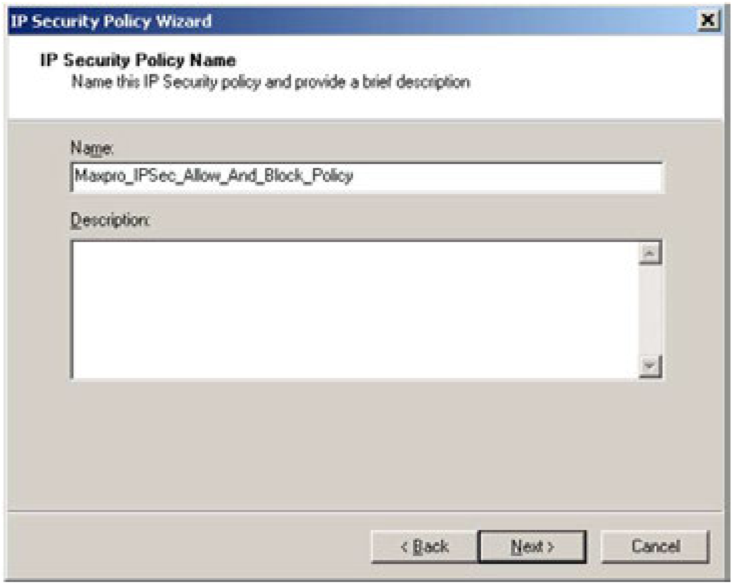


Welcome to the IP Security Policy Wizard

This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.

To continue, click Next.

3. Click **Next**. The **IP Security Policy Name** wizard appears.



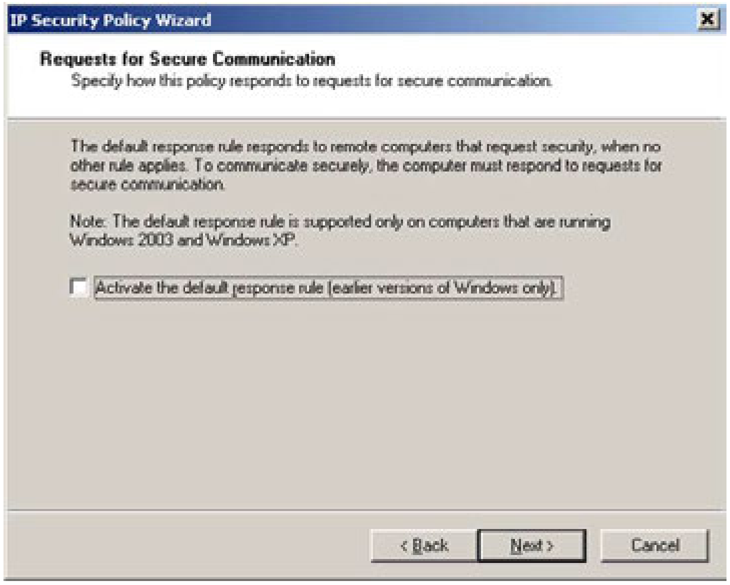
IP Security Policy Wizard

IP Security Policy Name
Name this IP Security policy and provide a brief description

Name:
Maxpro_IPSec_Allow_And_Block_Policy

Description:

4. Type the policy name as **Maxpro_IPSec_Allow_And_Block_Policy** and then click **Next**. **Request for Secure Communication** wizard appears.



IP Security Policy Wizard

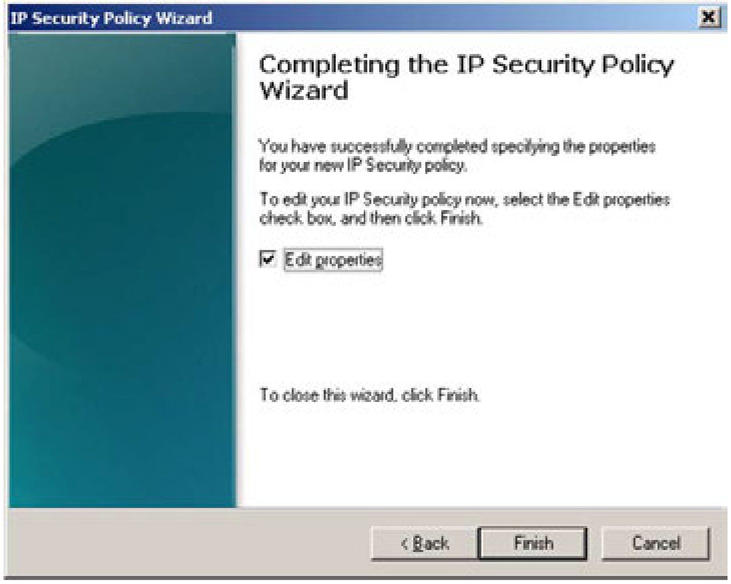
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.

□ Activate the default response rule (earlier versions of Windows only).

5. Select the **Activate the default response rule (earlier versions of Window only)** check box if required and then click **Next**. **Completing the IP Security Policy Wizard** appears.



Completing the IP Security Policy Wizard

You have successfully completed specifying the properties for your new IP Security policy.

To edit your IP Security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

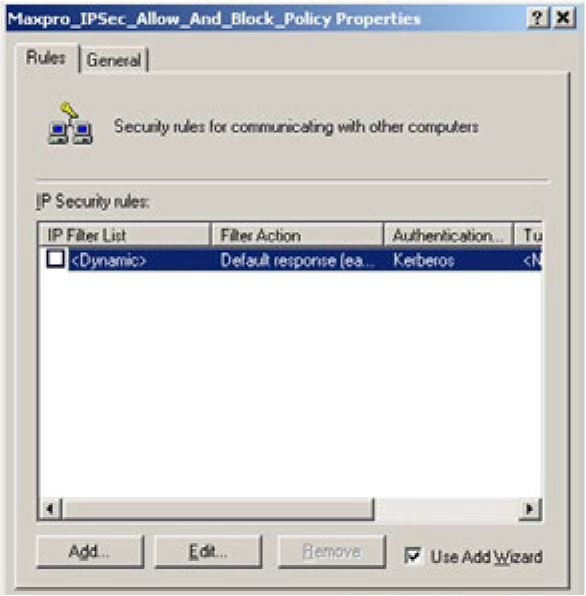
To close this wizard, click Finish.

6. Select the **Edit Properties** check box and then click **Finish**. The IP Security Policy will be created.

Creating an IP Filter list

To create IP Filter:

1. Click **Add** in **Maxpro_IPSec_Allow_And_Block_Policy_Properties** dialog box.



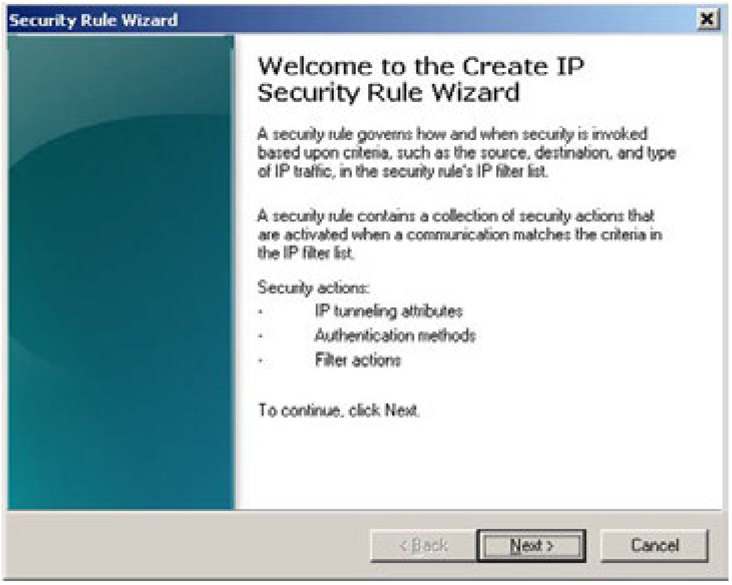
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default response (ea...	Kerberos	<N

☑ Use Add Wizard

The Welcome wizard is displayed. Click **Next**.



Security Rule Wizard

Welcome to the Create IP Security Rule Wizard

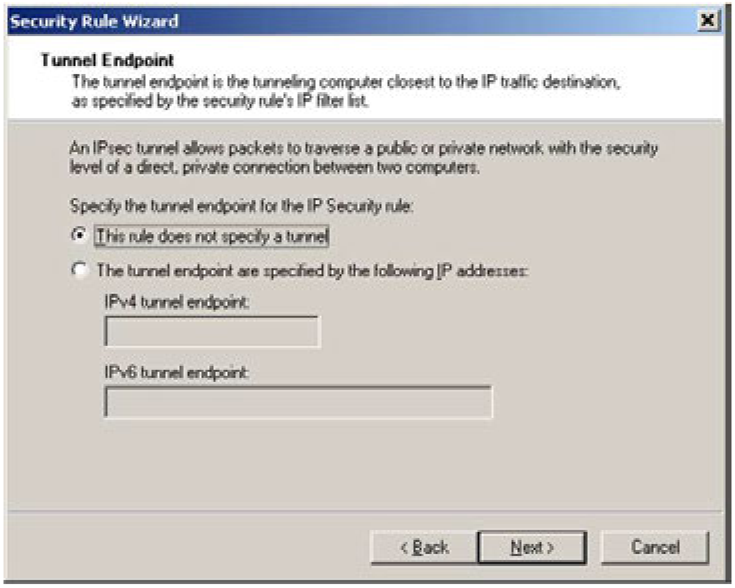
A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:
- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

2. Click **Next**. The **Tunnel Endpoint** wizard is displayed.



Security Rule Wizard

Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPsec tunnel allows packets to traverse a public or private network with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP Security rule:

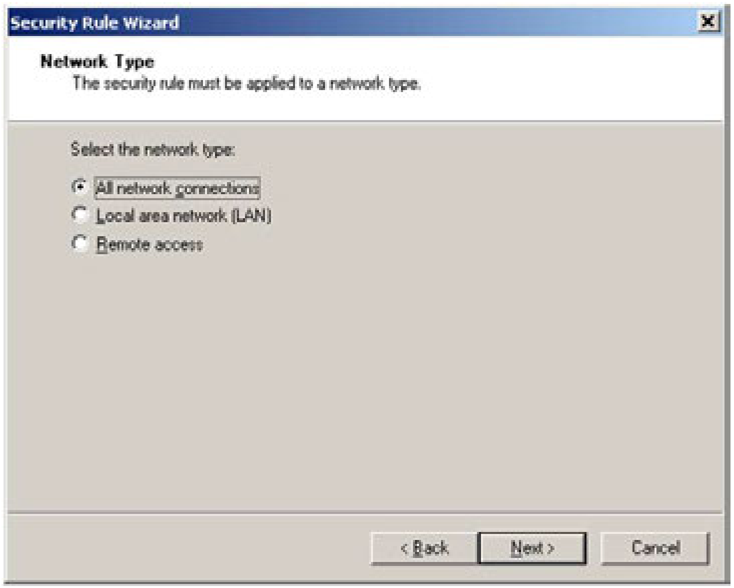
● This rule does not specify a tunnel

○ The tunnel endpoint are specified by the following IP addresses:

IPv4 tunnel endpoint:

IPv6 tunnel endpoint:

3. Click **Next**. The **Network Type** wizard is displayed.



Security Rule Wizard

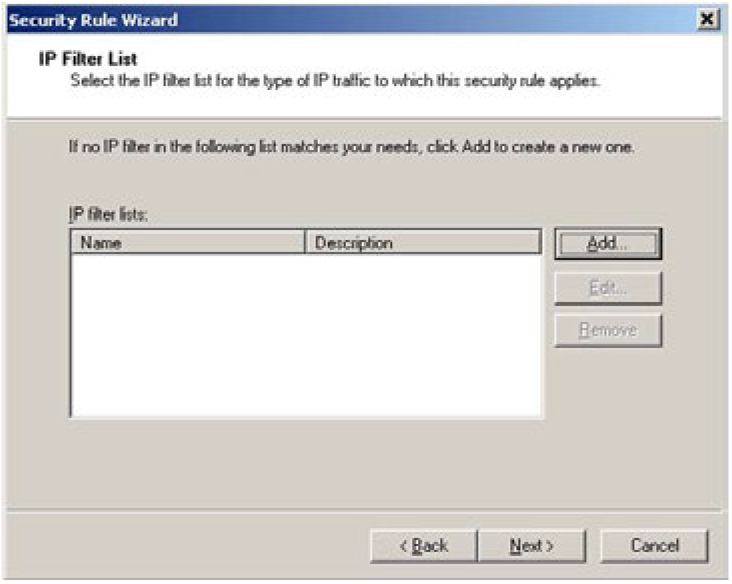
Network Type

The security rule must be applied to a network type.

Select the network type:

● All network connections
○ Local area network (LAN)
○ Remote access

4. Ensure that **All networks Connections** option is selected and then click **Next**. The **IP Filter List** wizard is displayed.



Security Rule Wizard

IP Filter List

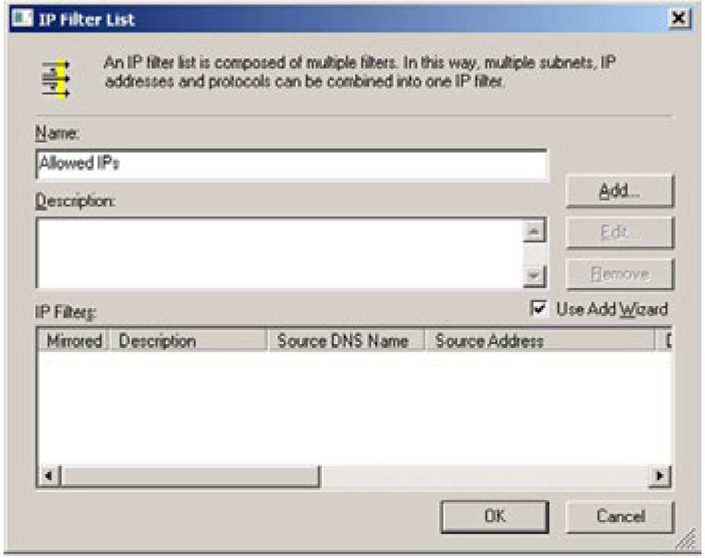
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description

5. Click **Add**. The **IP Filter List** dialog box appears.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

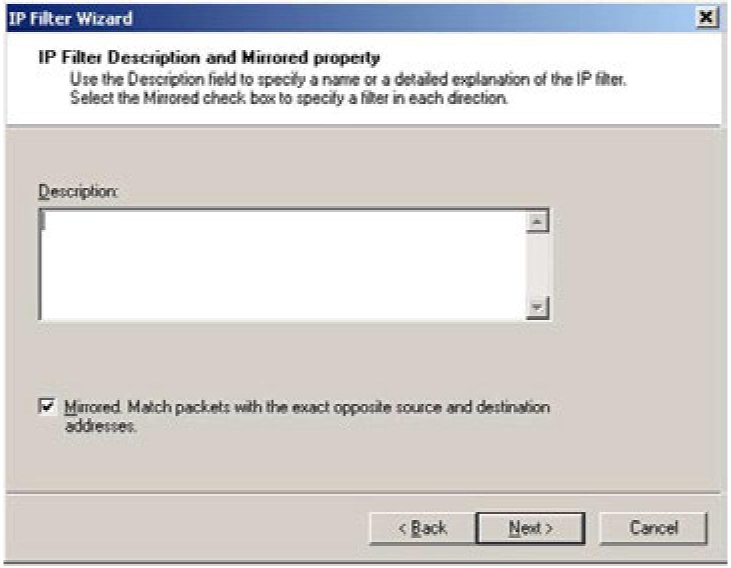
Name: Allowed IPs

Description:

IP Filters:

☑ Use Add Wizard

6. Type the **Name** for a filter and then click **Add** to add the required IPs in the filter. The **IP Filter Description and Mirrored Property** wizard appears.



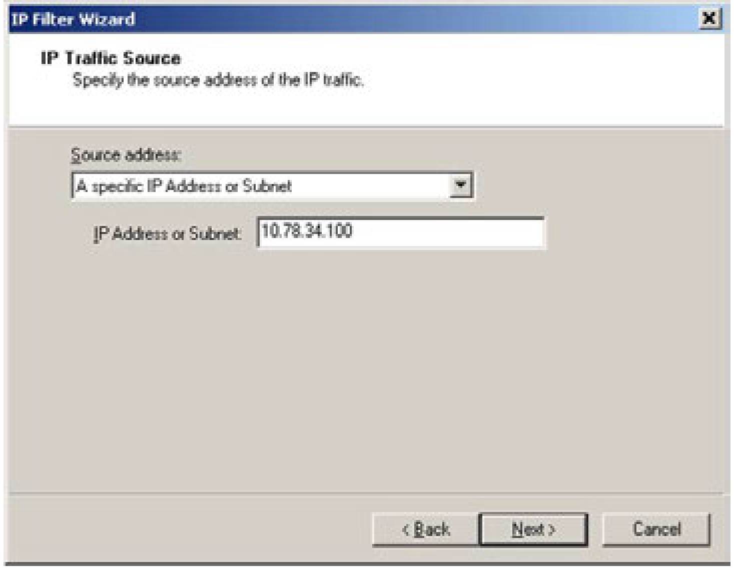
IP Filter Description and Mirrored property

Use the Description field to specify a name or a detailed explanation of the IP filter.
Select the Mirrored check box to specify a filter in each direction.

Description:

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

7. Type the **Description** and then click **Next**. The **IP Traffic Source** wizard appears.



IP Filter Wizard

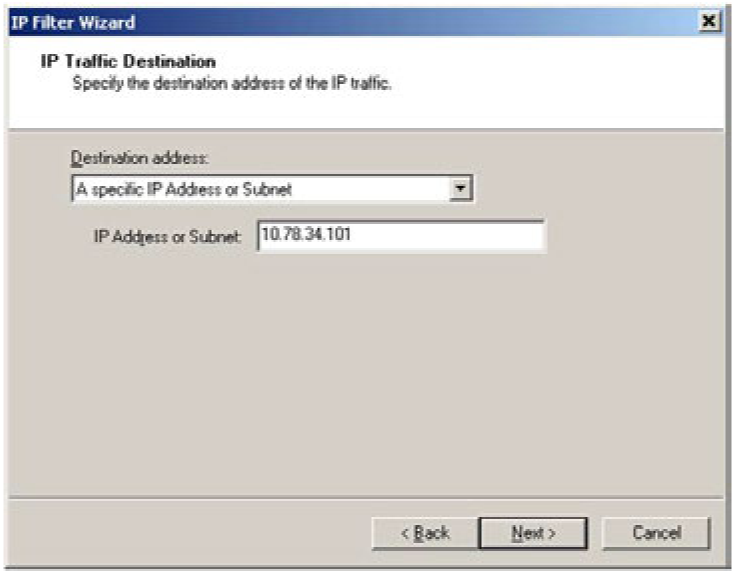
IP Traffic Source

Specify the source address of the IP traffic.

Source address: A specific IP Address or Subnet

IP Address or Subnet: 10.78.34.100

8. Select the **Source address** from the drop-down list.
9. Type the **IP Address or Subnet** of this MAXPRO machine and then click **Next**. The **IP Traffic Destination** wizard appears.



IP Filter Wizard

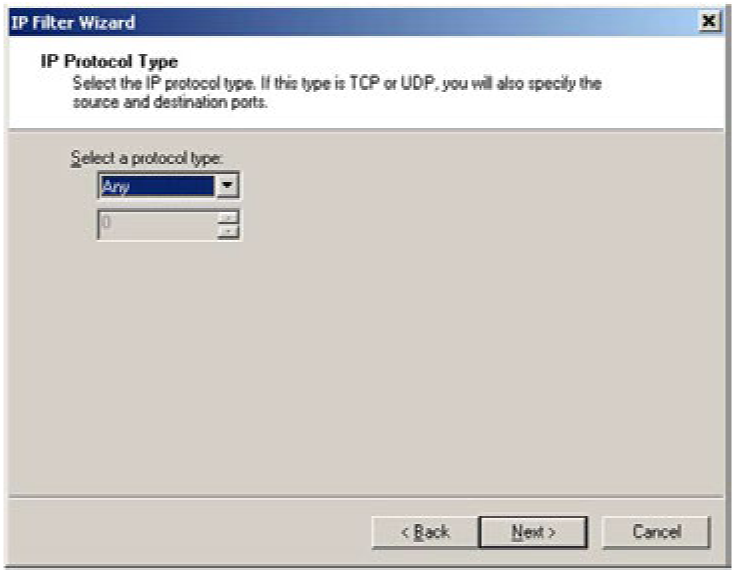
IP Traffic Destination

Specify the destination address of the IP traffic.

Destination address: A specific IP Address or Subnet

IP Address or Subnet: 10.78.34.101

10. Select the **Destination address** from the drop-down list.
11. Type the **IP Address or Subnet** of this MAXPRO machine and then click **Next**. The **IP Protocol Type** wizard appears.



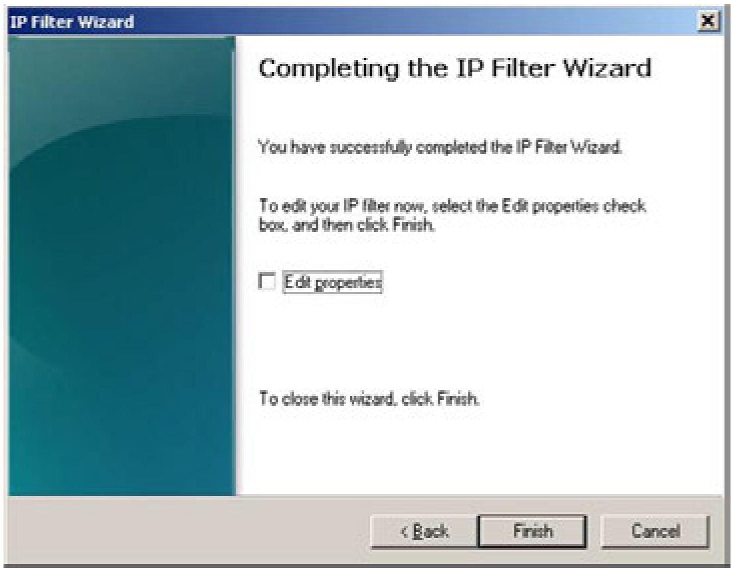
IP Filter Wizard

IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type: Any

12. Select the **Protocol Type** from the drop-down list and then click **Next**. **Completing the IP Filter Wizard** is displayed.



IP Filter Wizard

Completing the IP Filter Wizard

You have successfully completed the IP Filter Wizard.

To edit your IP filter now, select the Edit properties check box, and then click Finish.

☐ Edit properties

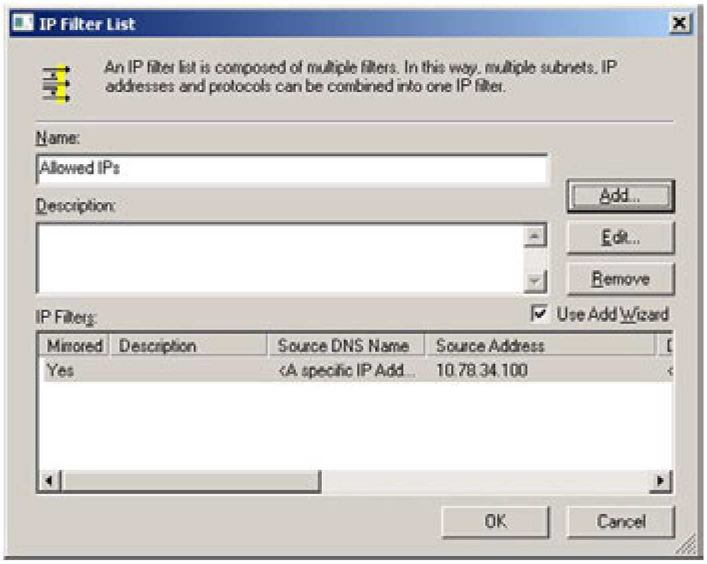
To close this wizard, click Finish.

13. Select the **Edit Properties** check box and then click **Finish**.

Add the required Unrestricted Network devices and Subnets in the IP Filter

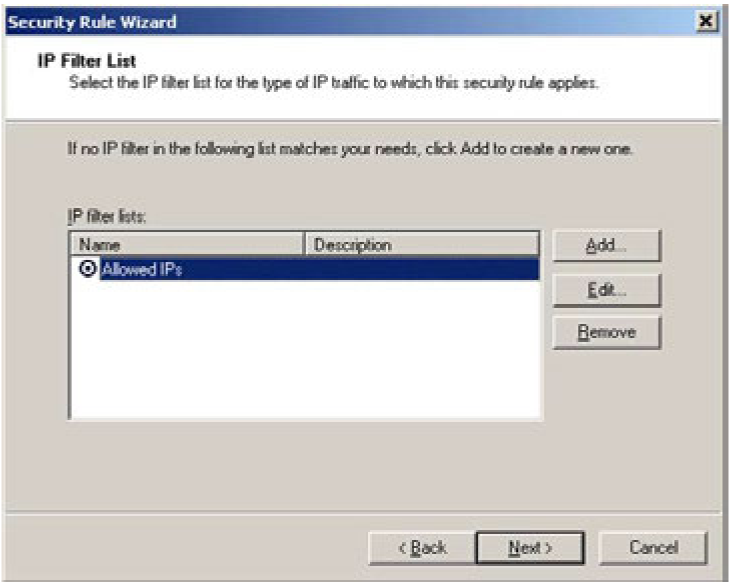
To add the required Unrestricted Network devices and subnets in the IP Filter:

1. Click **Add** in the IP Filter dialog box. The

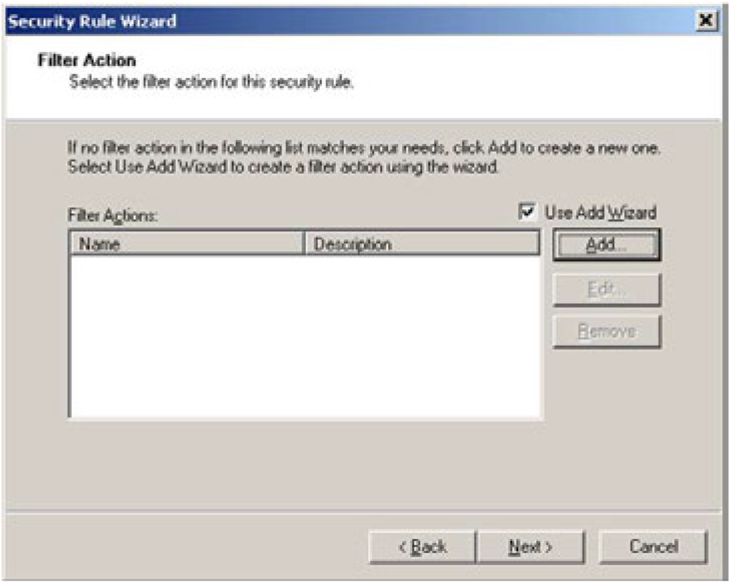

IP Filter List
An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
Allowed IPs
Description:
Add...
Edit...
Remove
IP Filters:
☑ Use Add Wizard
OK
Cancel

Mirrored	Description	Source DNS Name	Source Address
Yes		<A specific IP Add...	10.78.34.100

2. Click **Add**. The **Security Rule** Wizard appears with the list of IP Filters.


Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
◉ Allowed IPs
Add...
Edit...
Remove
< Back
Next >
Cancel

3. Under **IP filters list,** select the IP Filter created in previous step and then click **Next**. The **Filter Action** wizard appears.



Security Rule Wizard

Filter Action

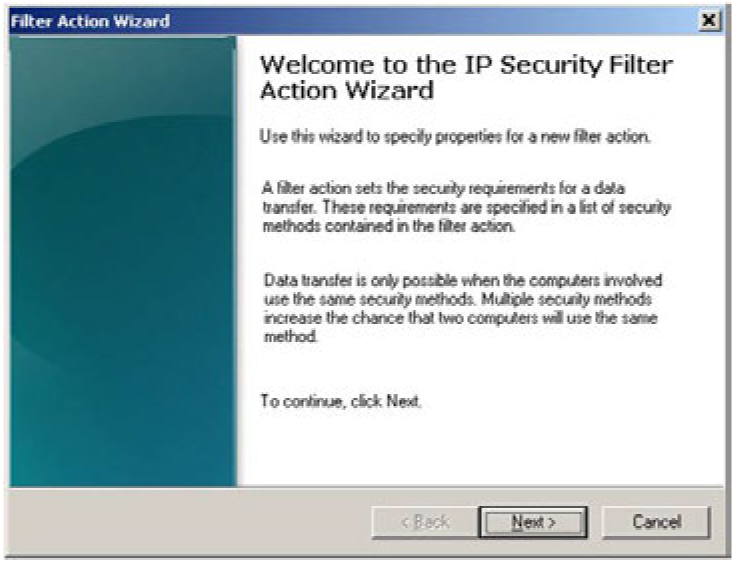
Select the filter action for this security rule.

If no filter action in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions: ☑ Use Add Wizard

Name	Description

4. Click the **Add** button to create IPsec filter to allow connections without any restrictions. The IPSec Welcome Wizard appears.



Filter Action Wizard

Welcome to the IP Security Filter Action Wizard

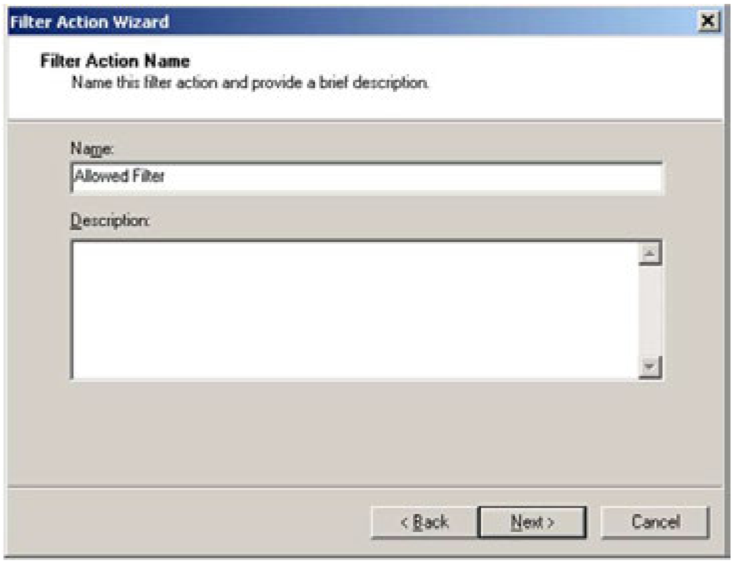
Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

5. Click **Next**. The **Filter Action Name** wizard is displayed.



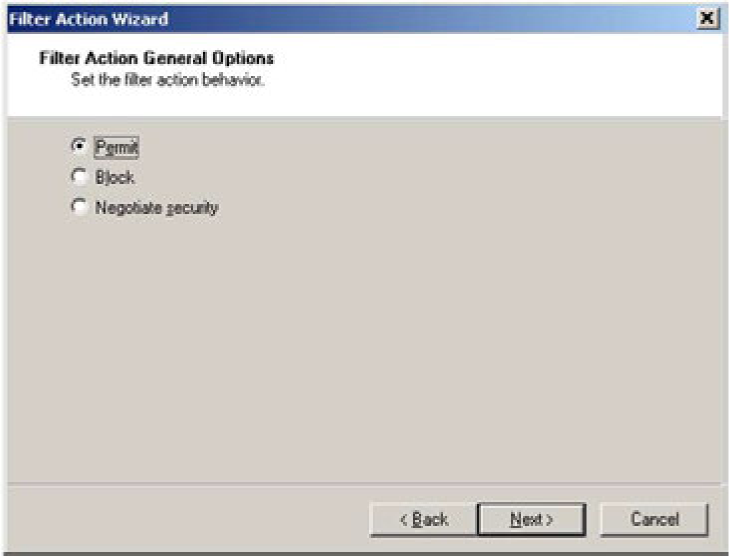
Filter Action Wizard

Filter Action Name
Name this filter action and provide a brief description.

Name: Allowed Filter

Description:

6. Type the **Name** for filter and then click **Next**. The **Filter Action General Options** wizard is displayed.

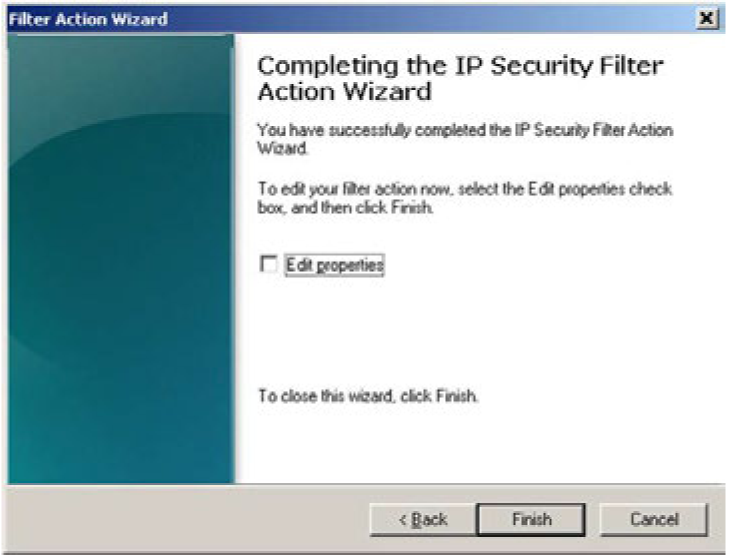


Filter Action Wizard

Filter Action General Options
Set the filter action behavior.

● Permit
○ Block
○ Negotiate security

7. Click the **Permit** option and then click **Next**. The IPSec Filter Action wizard appears.



Filter Action Wizard

Completing the IP Security Filter Action Wizard

You have successfully completed the IP Security Filter Action Wizard.

To edit your filter action now, select the Edit properties check box, and then click Finish.

□ Edit properties

To close this wizard, click Finish.

8. Select the **Edit Properties** check box if required and then click **Finish**.

TBD

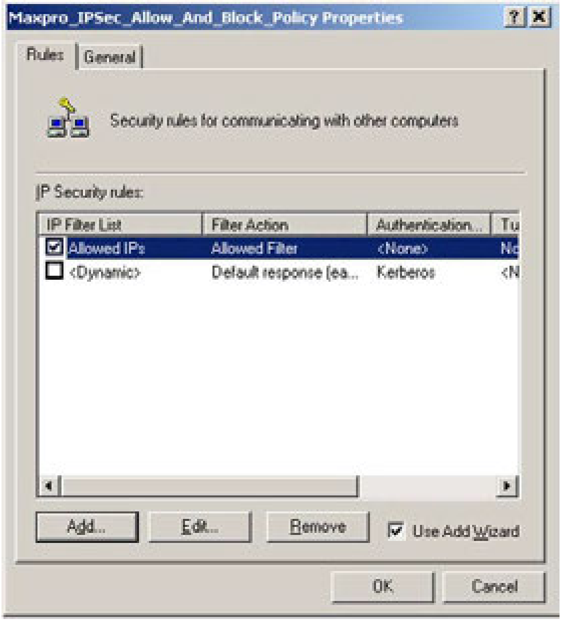
Blocked Network Devices

User can configure Blocked connections for all the IP address and can allow only the ones which are in Unrestricted (Permitted) devices lists to connect to the MAXPRO machine.

To configure blocked connections rule for all the IP address:

1. Click **Add** in **Maxpro_IPSec_Allow_And_Block_Policy_Properties** dialog box.

   See TBA to Open **Maxpro_IPSec_Allow_And_Block_Policy_Properties** dialog**.**



Maxpro_IPSec_Allow_And_Block_Policy Properties

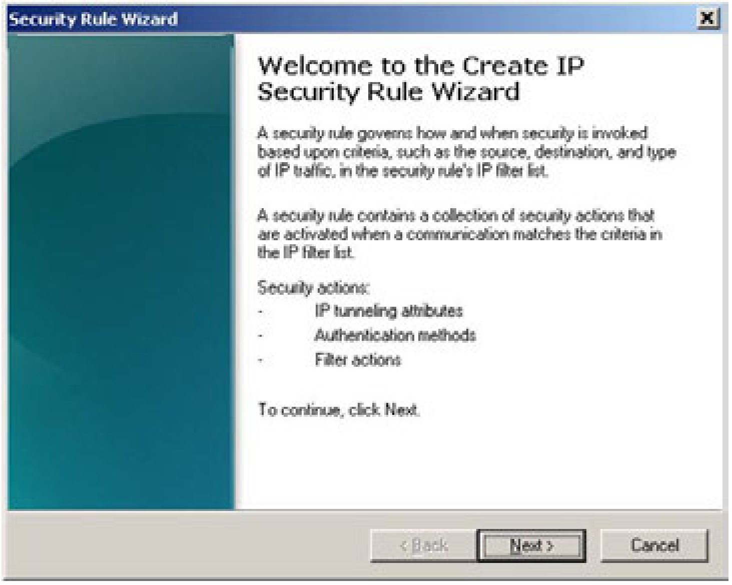
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ Allowed IPs	Allowed Filter	<None>	No
□ <Dynamic>	Default response (ea...	Kerberos	<N

☑ Use Add Wizard

The Welcome wizard to create IP Security Rule appears.



Welcome to the Create IP Security Rule Wizard

A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.

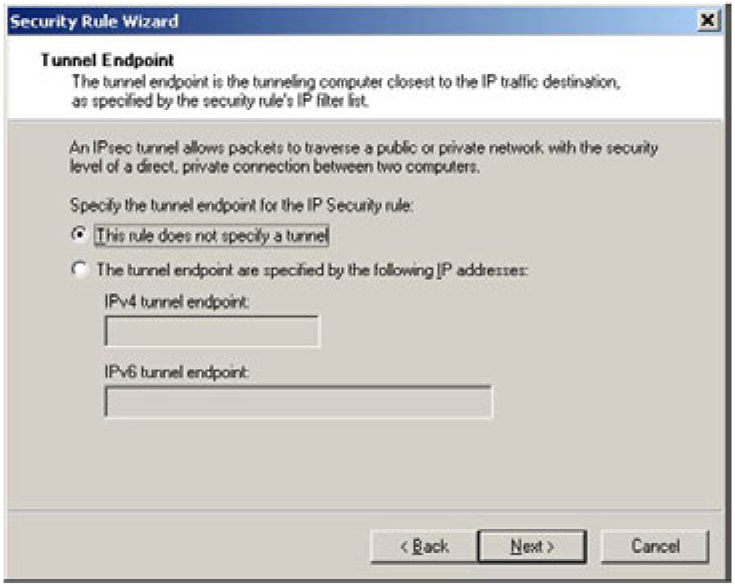
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.

Security actions:

- IP tunneling attributes
- Authentication methods
- Filter actions

To continue, click Next.

2. Click **Next**. The **Tunnel Endpoint** dialog appears.



Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPsec tunnel allows packets to traverse a public or private network with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP Security rule:

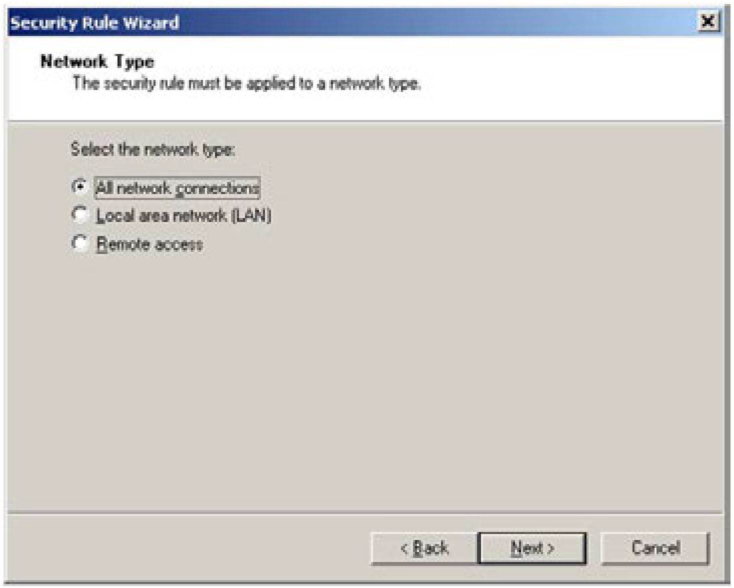
● This rule does not specify a tunnel

○ The tunnel endpoint are specified by the following IP addresses:

IPv4 tunnel endpoint:

IPv6 tunnel endpoint:

3. Click **This rule does not specify a tunnel** option and then click **Next**. The **Network Type** dialog appears.



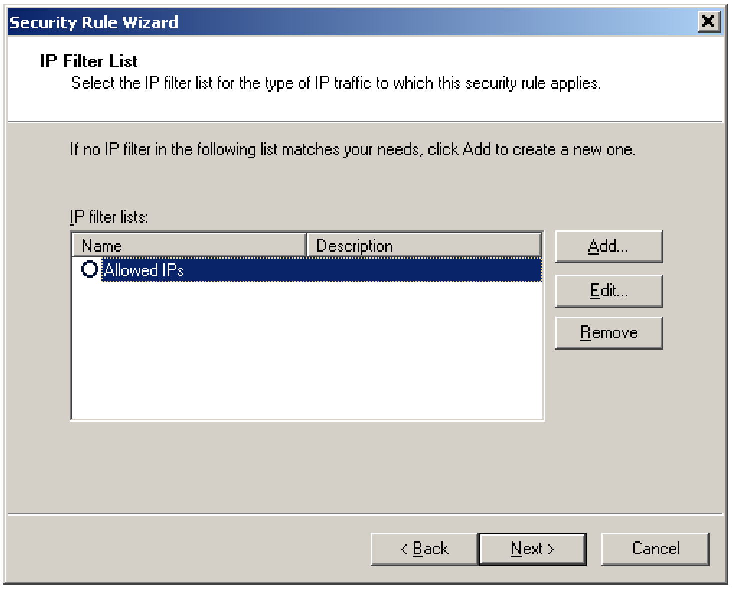
Security Rule Wizard

Network Type
The security rule must be applied to a network type.

Select the network type:

- ● All network connections
- ○ Local area network (LAN)
- ○ Remote access

4. Select network type as **All networks Connections** and then click **Next**. The **IP Filter List** dialog appears.



Security Rule Wizard

IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

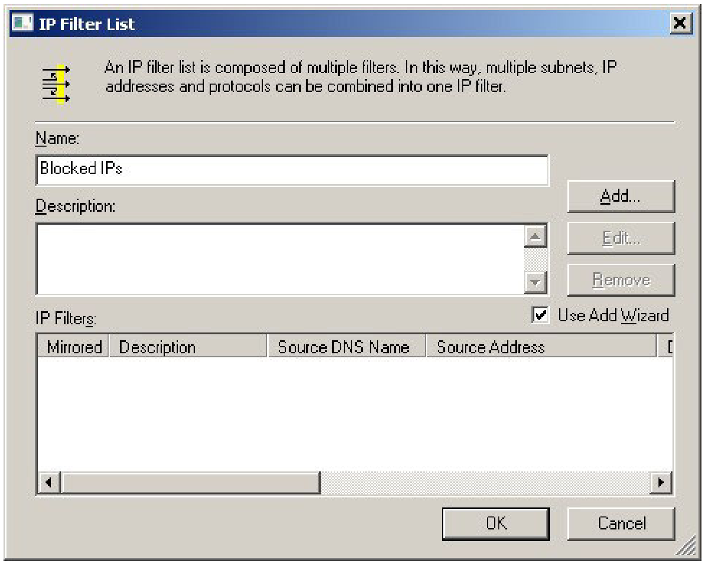
Name	Description
● Allowed IPs	

5. Create a new **IP Filter List** for Blocked IPs**.**

Creating an IP Filter List

To create IP Filter:

a. Click **Add** in **IP Filter List** dialog. The IP Filter List dialog appears.



IP Filter List

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

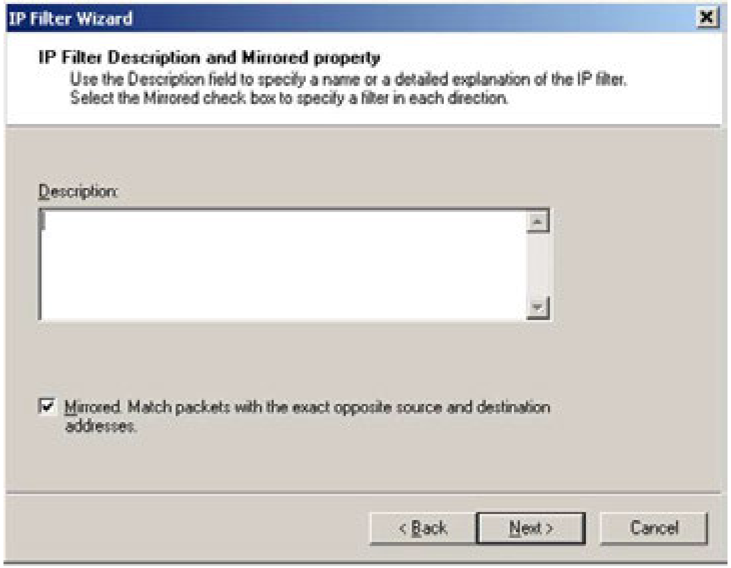
Name: Blocked IPs

Description:

IP Filters: ☑ Use Add Wizard

Mirrored	Description	Source DNS Name	Source Address	D

b. Type a **Name** for the filter. Select **Use ADD Wizard** check box and then click **Add**. The **IP Filter Description and Mirrored Property** dialog appears.



IP Filter Wizard

IP Filter Description and Mirrored property

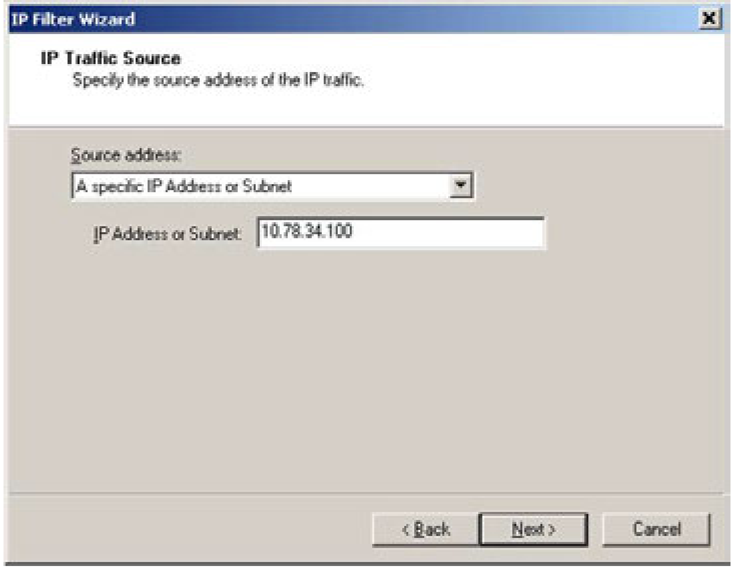
Use the Description field to specify a name or a detailed explanation of the IP filter. Select the Mirrored check box to specify a filter in each direction.

Description:

☑ Mirrored. Match packets with the exact opposite source and destination addresses.

c. Type the **Description** and select **"Mirrored. Match packets with exact opposite source and destination addresses"**. Click **Next**.

The **IP Traffic Source** dialog appears.



IP Filter Wizard

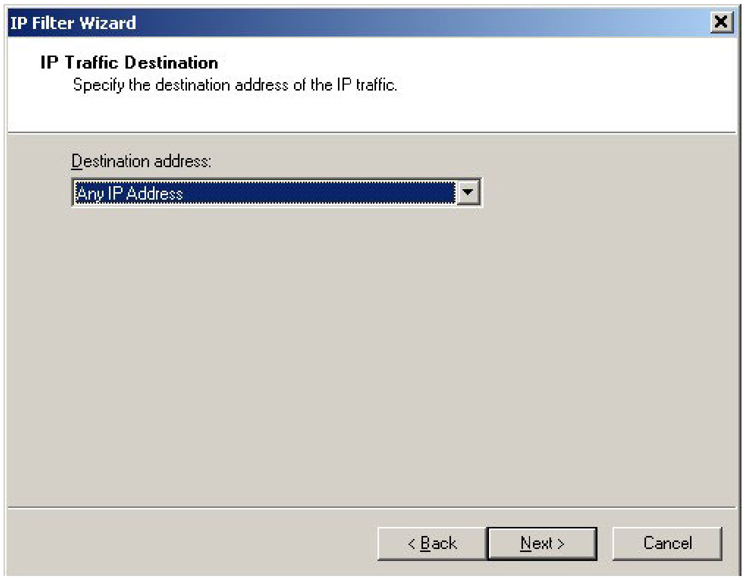
IP Traffic Source
Specify the source address of the IP traffic.

Source address: A specific IP Address or Subnet

IP Address or Subnet: 10.78.34.100

d. Select the **Source address** as **“A specific IP Address or Subnet”** from the drop-down list.

e. Type the **IP Address or Subnet** of the MAXPRO machine and then click **Next**. The **IP Traffic Destination** dialog appears.



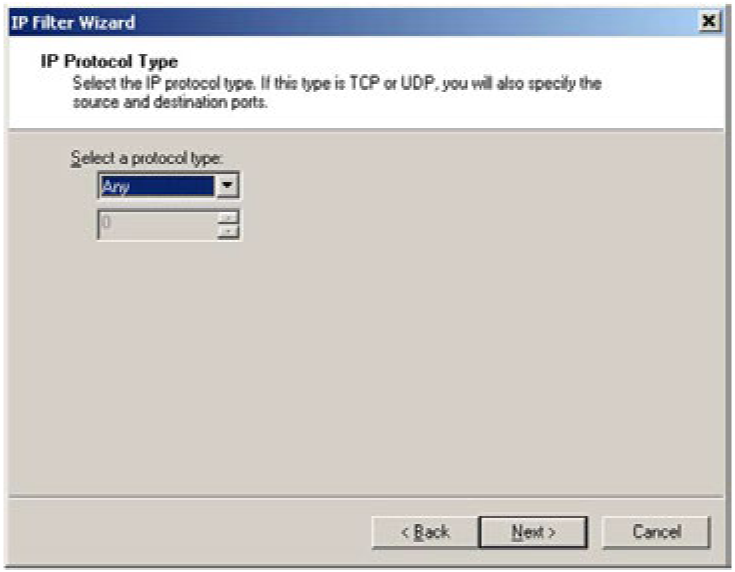
IP Filter Wizard

IP Traffic Destination
Specify the destination address of the IP traffic.

Destination address: Any IP Address

f. Select the **Destination address** as **“Any IP Address”** from the drop-down list. Click **Next**.

The **IP Filter Wizard** appears.



IP Filter Wizard

IP Protocol Type

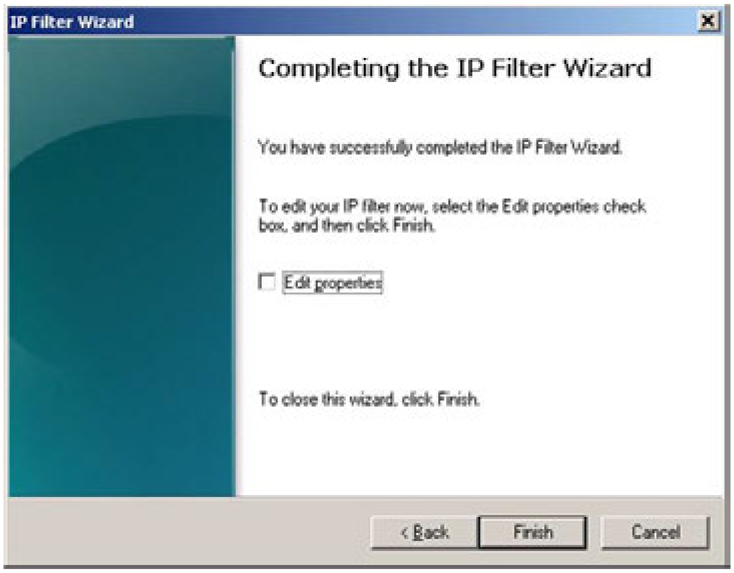
Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

Select a protocol type:

Any

0

g. Select the **Protocol Type** as **"Any"** from the drop-down list and then click **Next**. **Completing the IP Filter Wizard** dialog appears.



IP Filter Wizard

Completing the IP Filter Wizard

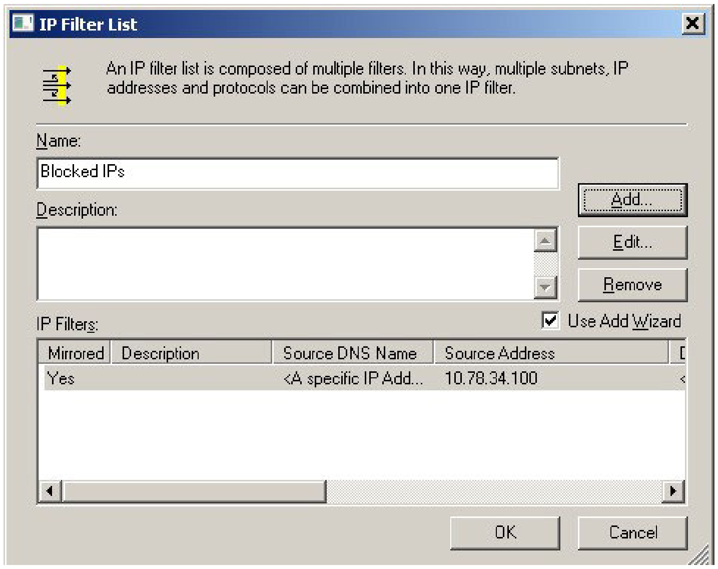
You have successfully completed the IP Filter Wizard.

To edit your IP filter now, select the Edit properties check box, and then click Finish.

□ Edit properties

To close this wizard, click Finish.

h. Clear **Edit Properties** check box and then click **Finish**. **IP Filter List** dialog appears.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: Blocked IPs

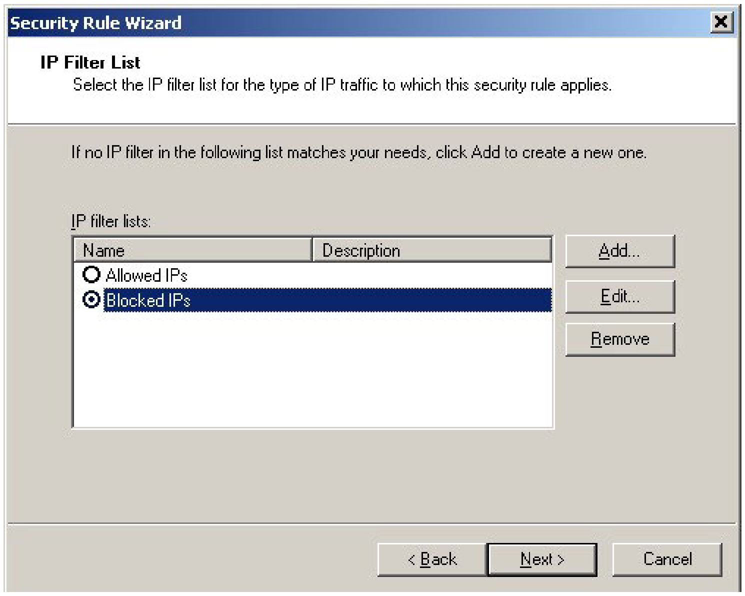
Description:

IP Filters: ☑ Use Add Wizard

Mirrored	Description	Source DNS Name	Source Address	D
Yes		<A specific IP Add...	10.78.34.100	<

i. Click **OK.**

6. Continued from step 5, The **Security Rule Wizard** appears.



IP Filter List

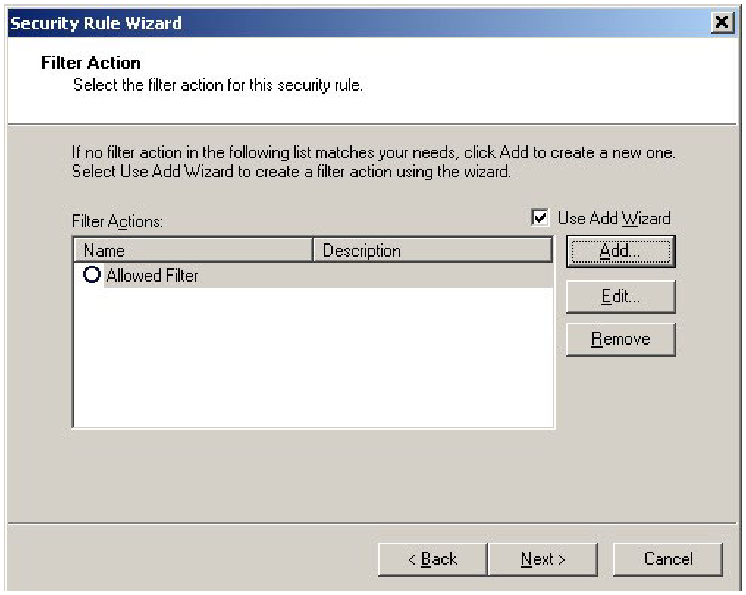
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ Allowed IPs	
● Blocked IPs	

7. Select **Blocked IPs** and then Click **Next. Filter Action** dialog appears.


Security Rule Wizard

Filter Action
Select the filter action for this security rule.

If no filter action in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

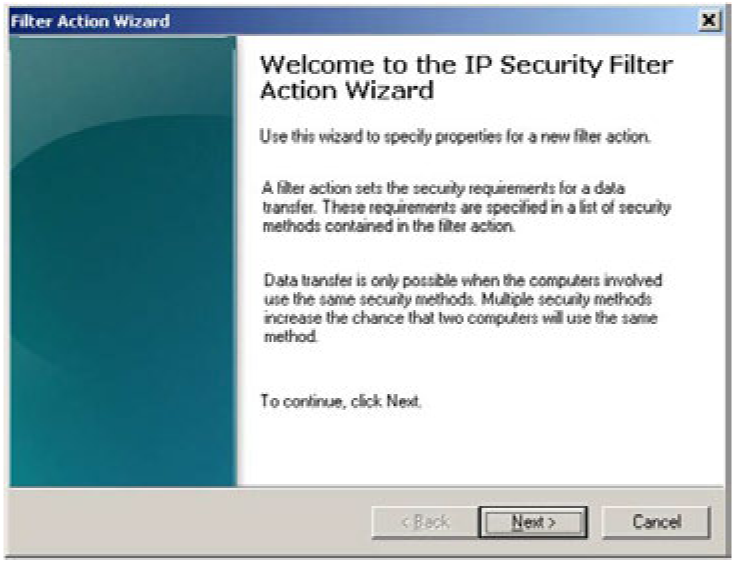
☑ Use Add Wizard

Name	Description
○ Allowed Filter	

8. Create a new **IPsec Filter Action** for blocked connections.

Creating IPsec Filter Action

a. Click **Add** in **Filter Action** dialog. The IPSec Welcome Wizard appears.


Filter Action Wizard

Welcome to the IP Security Filter Action Wizard

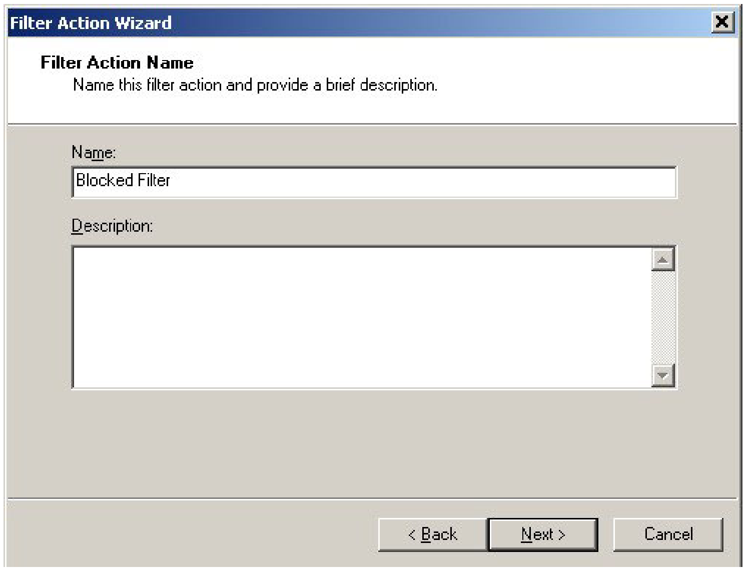
Use this wizard to specify properties for a new filter action.

A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.

Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.

To continue, click Next.

b. Click **Next**. The **Filter Action Name** dialog appears.



Filter Action Name

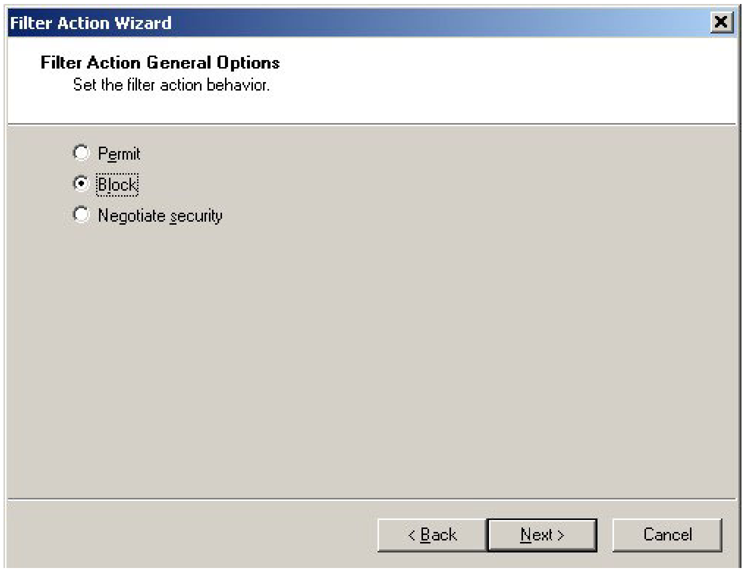
Name this filter action and provide a brief description.

Name:

Blocked Filter

Description:

c. Type a **Name** for the filter and then click **Next**. The **Filter Action General Options** dialog appears.



Filter Action General Options

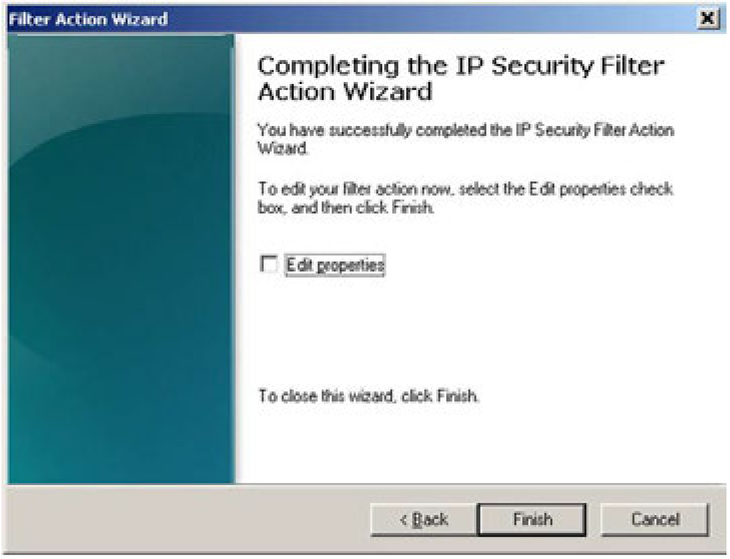
Set the filter action behavior.

○ Permit

● Block

○ Negotiate security

d. Select **"Block"** option and then click **Next**. **Completing the IP Security Filter Action Wizard** dialog appears.



Filter Action Wizard

Completing the IP Security Filter Action Wizard

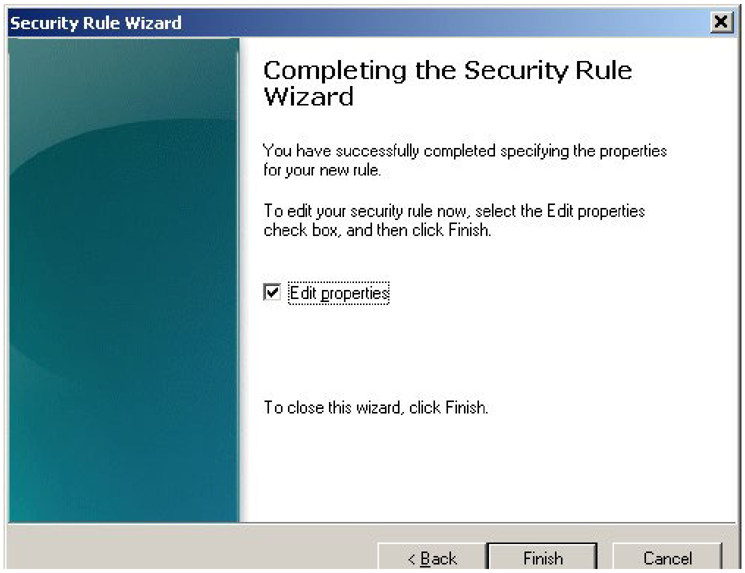
You have successfully completed the IP Security Filter Action Wizard.

To edit your filter action now, select the Edit properties check box, and then click Finish.

☐ Edit properties

To close this wizard, click Finish.

e. Clear **Edit Properties** check box and then click **Finish**. **Filter Action** dialog appears.



Security Rule Wizard

Completing the Security Rule Wizard

You have successfully completed specifying the properties for your new rule.

To edit your security rule now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, click Finish.

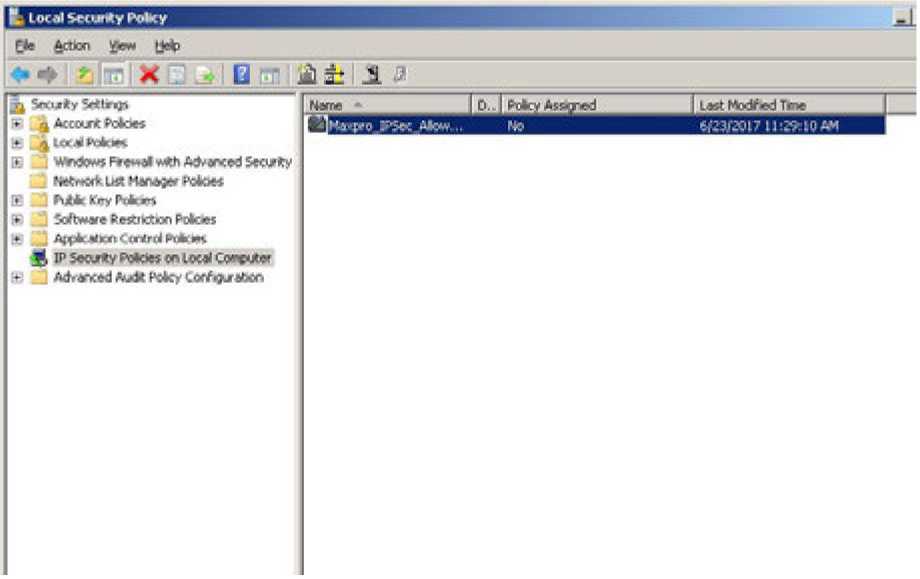
Continued from step 8

9. Select **Edit properties** and the click **Finish.**

10. **TBA**

Assign the Policy

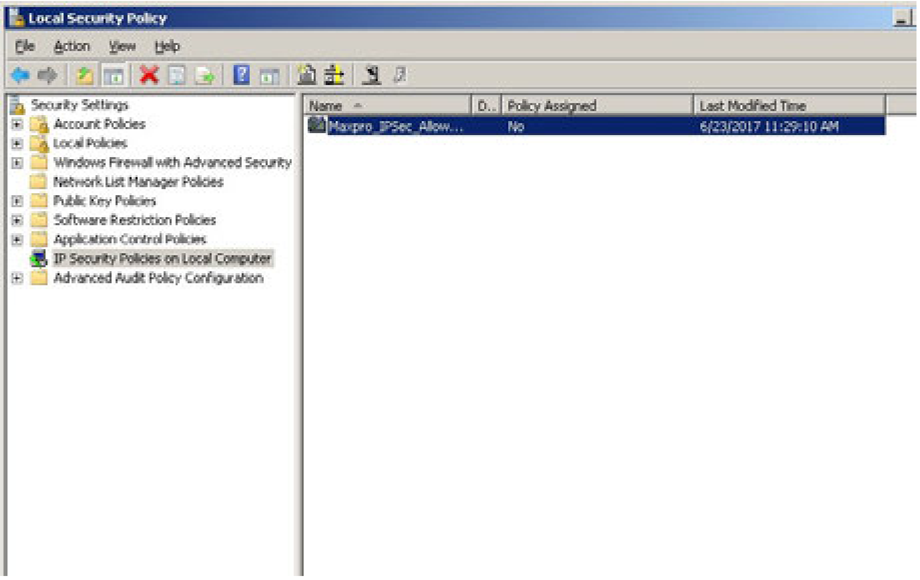
1. In Run command box type **secpol.msc** and then click **OK**. The **Local Security Policy** window is displayed as shown below.



- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Name	D..	Policy Assigned	Last Modified Time
Maxpro_IPSec_Allow...		No	6/23/2017 11:29:10 AM

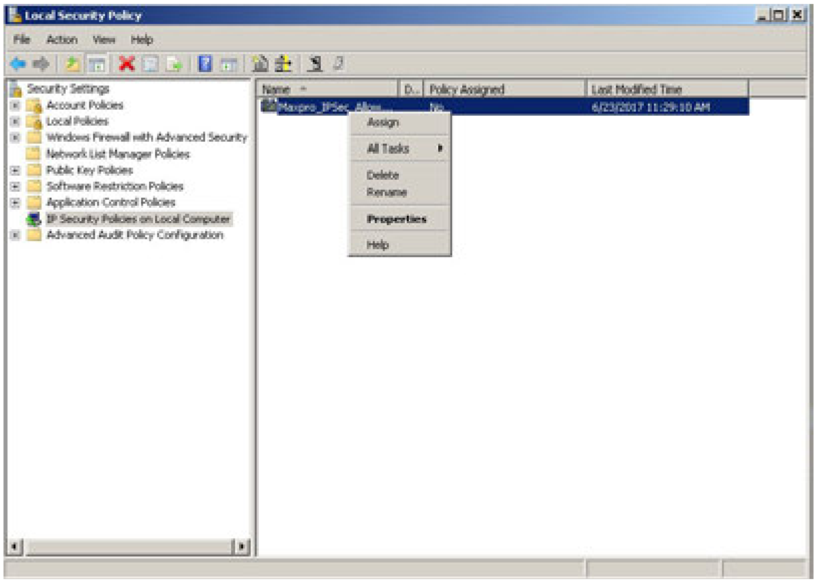
2. Under **Security Settings** pane, Click on **IP Security Policies on Local Computer**.



- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Name	D..	Policy Assigned	Last Modified Time
Maxpro_IPSec_Allow...		No	6/23/2017 11:29:10 AM

3. Right Click on **"Maxpro_IPSec_Allow_And_Block_Policy"** and click **Assign.**



4. IPsec Policy for Blocked and Unblocked Communication is created.

Secured Network.

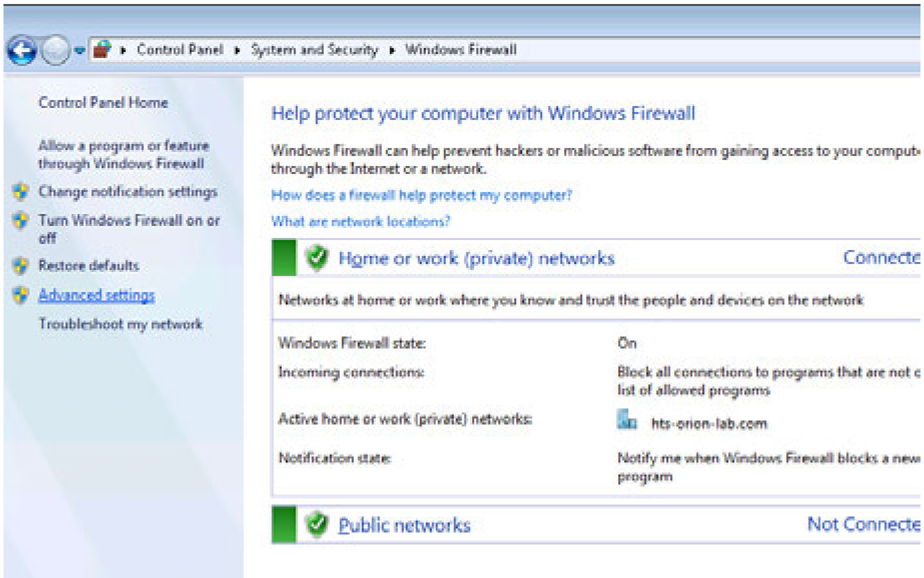
Secured connection is applicable between MAXPRO Machines as listed below:

- Maxpro VMS Server - Maxpro NVR Server
- Maxpro VMS Server - Maxpro VMS Client
- Maxpro NVR Server - Maxpro NVR Client

To establish Secured communication between MAXPRO Machines (IPsec secured communication) using AES/3DES for Encryption and SHA1/MD5 for Integrity, create IPSec policy with Windows Firewall policy

Creating IPSec policy with Windows Firewall policy.

1. In Run command box type **firewall.cpl** and then click **OK**. The Windows Firewall window appears.


Control Panel ▸ System and Security ▸ Windows Firewall
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
How does a firewall help protect my computer?
What are network locations?

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your comput through the Internet or a network.

Home or work (private) networks — Connecte

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

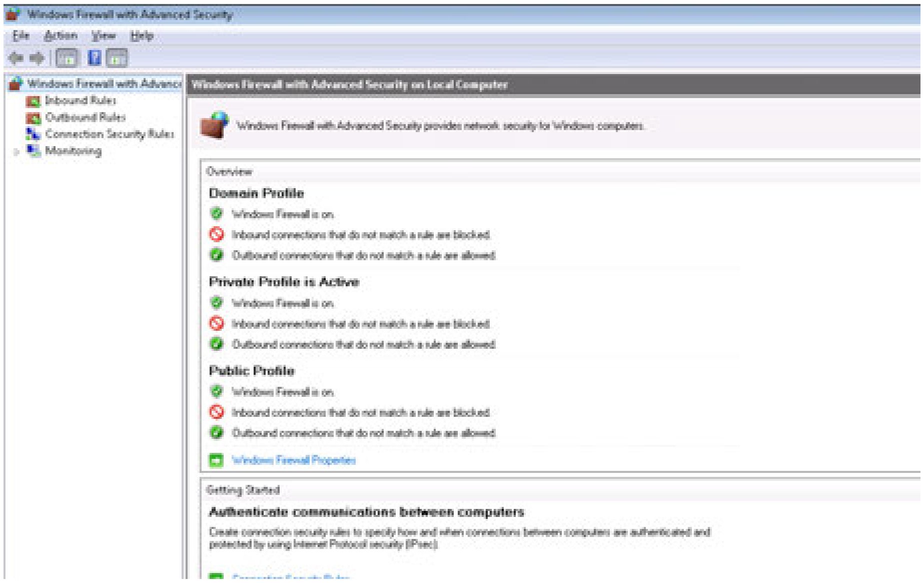
Incoming connections: Block all connections to programs that are not c list of allowed programs

Active home or work (private) networks: hts-orion-lab.com

Notification state: Notify me when Windows Firewall blocks a new program

Public networks — Not Connecte

2. On left Pane, click **Advanced settings**. the **Windows Firewall with advanced settings** dialog appears


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall Properties

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile

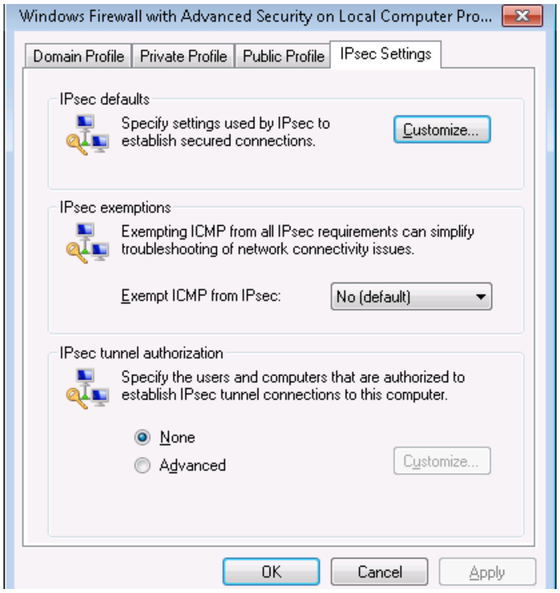
- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

3. Click **Windows Firewall Properties,** the **Properties** dialog appears**.**



IPsec defaults

Specify settings used by IPsec to establish secured connections.

IPsec exemptions

Exempting ICMP from all IPsec requirements can simplify troubleshooting of network connectivity issues.

Exempt ICMP from IPsec: No (default)

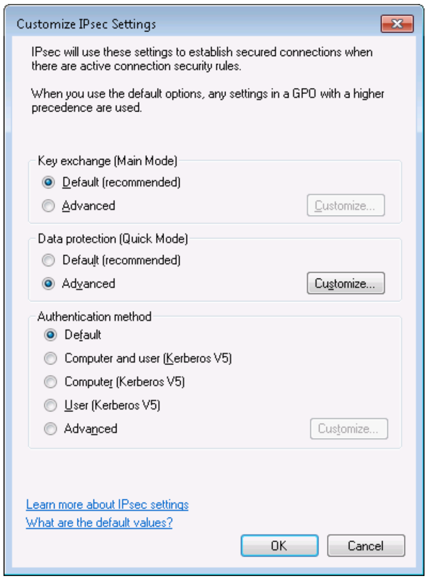
IPsec tunnel authorization

Specify the users and computers that are authorized to establish IPsec tunnel connections to this computer.

● None

○ Advanced

4. In IPsec Settings tab, click the **Customize** button. The Customize IPsec Settings dialog box appears.



IPsec will use these settings to establish secured connections when there are active connection security rules.

When you use the default options, any settings in a GPO with a higher precedence are used.

Key exchange (Main Mode)

● Default (recommended)

○ Advanced

Data protection (Quick Mode)

○ Default (recommended)

● Advanced

Authentication method

● Default

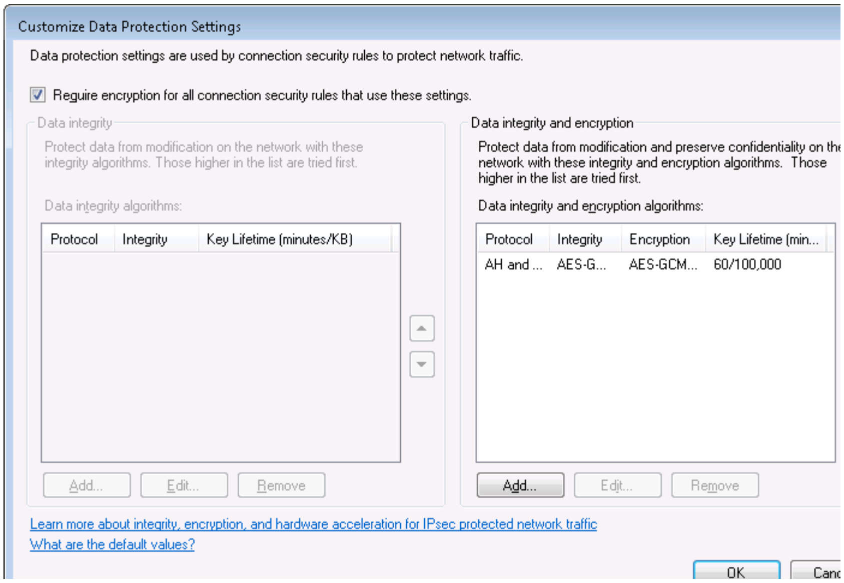
○ Computer and user (Kerberos V5)

○ Computer (Kerberos V5)

○ User (Kerberos V5)

○ Advanced

5. Under **“Data Protection”** select **Advanced** and click **Customize.Customize Data Protection Settings** dialog appears.



Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☑ Require encryption for all connection security rules that use these settings.

Data integrity

Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)

Data integrity and encryption

Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

Data integrity and encryption algorithms:

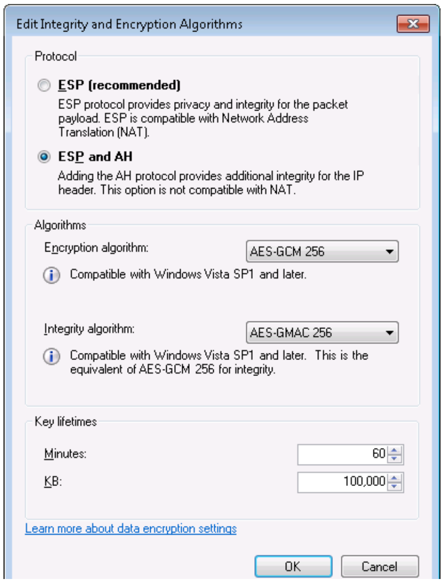
Protocol	Integrity	Encryption	Key Lifetime (min...
AH and ...	AES-G...	AES-GCM...	60/100,000

Learn more about integrity, encryption, and hardware acceleration for IPsec protected network traffic

What are the default values?

6. Select **Require encryption for all connections security rules that use these settings.** Remove all the **Data Integrity and Encryption protocols**.

7. Under **Data Integrity and encryption algorithms** click **Add. Edit Integrity and Encryption Algorithms** dialog appears.



Edit Integrity and Encryption Algorithms

Protocol

○ **ESP (recommended)**
ESP protocol provides privacy and integrity for the packet payload. ESP is compatible with Network Address Translation (NAT).

● **ESP and AH**
Adding the AH protocol provides additional integrity for the IP header. This option is not compatible with NAT.

Algorithms

Encryption algorithm: AES-GCM 256

Compatible with Windows Vista SP1 and later.

Integrity algorithm: AES-GMAC 256

Compatible with Windows Vista SP1 and later. This is the equivalent of AES-GCM 256 for integrity.

Key lifetimes

Minutes: 60

KB: 100,000

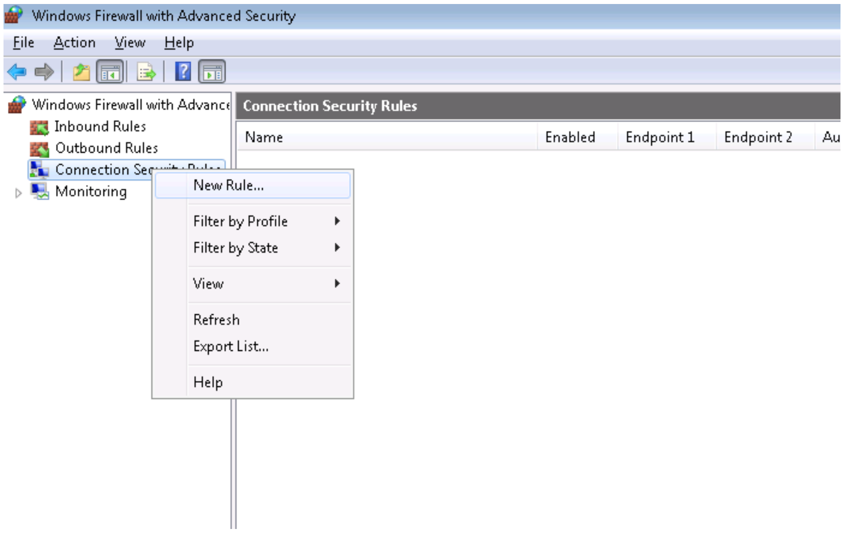
Learn more about data encryption settings

8. Select **Protocol, Algorithms and Key lifetimes** as shown in the above screen and then click **OK.**

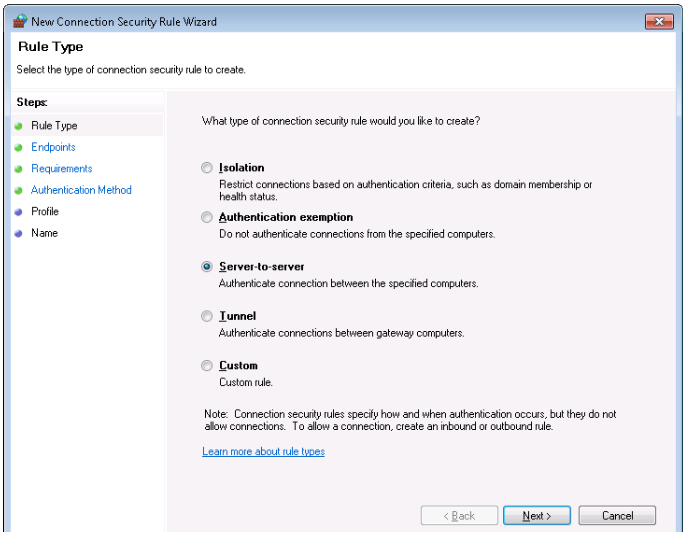
9. Click **OK** in **Customize Data Protection Settings** dialog.

Create a rule to use the IPsec security settings.

1. In **Windows Firewall with advanced settings** dialog, select **Connection Security Rule and right click.**



2. Select **New rule. New Connection Security Rule Wizard** dialog appears.


New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:
- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

○ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.

○ **Authentication exemption**
Do not authenticate connections from the specified computers.

● **Server-to-server**
Authenticate connection between the specified computers.

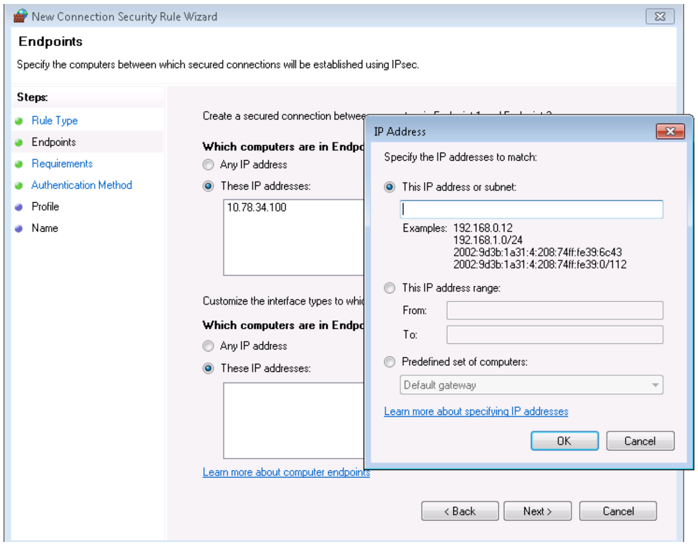
○ **Tunnel**
Authenticate connections between gateway computers.

○ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

3. Select **Rule type** as **server to server.** Click **Next.** The **IP Address** dialog box appears as shown below.



New Connection Security Rule Wizard

Endpoints

Specify the computers between which secured connections will be established using IPsec.

Steps:
- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Create a secured connection betwee

Which computers are in Endpo
○ Any IP address
● These IP addresses:
10.78.34.100

Customize the interface types to whic

Which computers are in Endpo
○ Any IP address
● These IP addresses:

IP Address

Specify the IP addresses to match:

● This IP address or subnet:

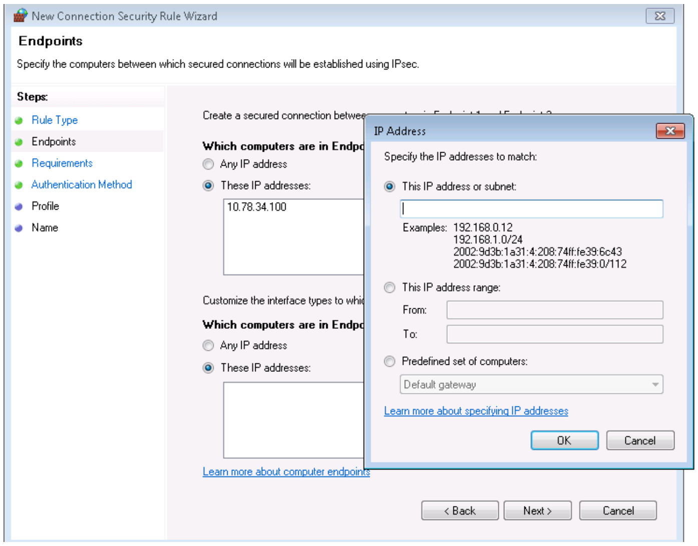
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:
From:
To:

○ Predefined set of computers:
Default gateway

Learn more about specifying IP addresses
OK
Cancel
Learn more about computer endpoints
< Back
Next >
Cancel

4. Select “**These IP Addresses”** under **Which Computers are in Endpoint 1.**
   a. Click **Add** to add IPs to the list.
   b. Type the required **IP** under “**This IP address or subnet”** and then click **OK.**



New Connection Security Rule Wizard

Endpoints

Specify the computers between which secured connections will be established using IPsec.

Steps:
- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Create a secured connection betwee

Which computers are in Endpo
○ Any IP address
● These IP addresses:
10.78.34.100

Customize the interface types to whic

Which computers are in Endpo
○ Any IP address
● These IP addresses:

IP Address

Specify the IP addresses to match:

● This IP address or subnet:

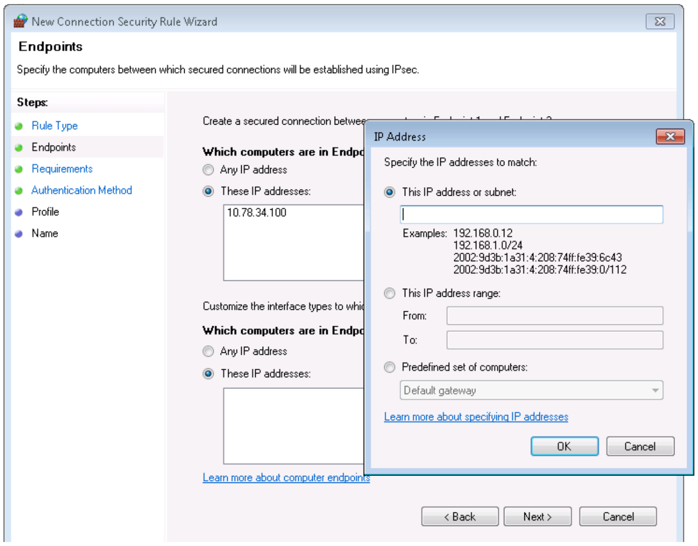
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:
From:
To:

○ Predefined set of computers:
Default gateway

Learn more about specifying IP addresses
OK
Cancel
Learn more about computer endpoints
< Back
Next >
Cancel

5. Select **These IP Addresses** under **“Which Computers are in Endpoint 2”**
   a. Click Add to add IPs to the list.
   b. Type the required IP under “**This IP address or subnet**” and then click **OK.**



New Connection Security Rule Wizard

Endpoints

Specify the computers between which secured connections will be established using IPsec.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Create a secured connection betwee

Which computers are in Endpo

○ Any IP address

● These IP addresses:

10.78.34.100

Customize the interface types to whic

Which computers are in Endpo

○ Any IP address

● These IP addresses:

Learn more about computer endpoints

< Back | Next > | Cancel

IP Address

Specify the IP addresses to match:

● This IP address or subnet:

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

From:

To:

○ Predefined set of computers:

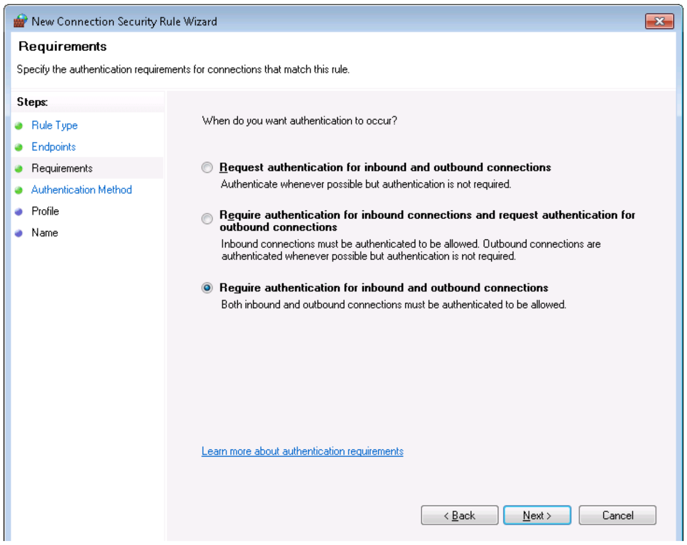
Default gateway

Learn more about specifying IP addresses

OK | Cancel

Note: For Endpoint 1 add machine IP where the rule is being created. Add all the other MAXPRO machines as Endpoint 2

6. Click **Next**. The **Requirements** screen appears.



New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

When do you want authentication to occur?

○ **Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.

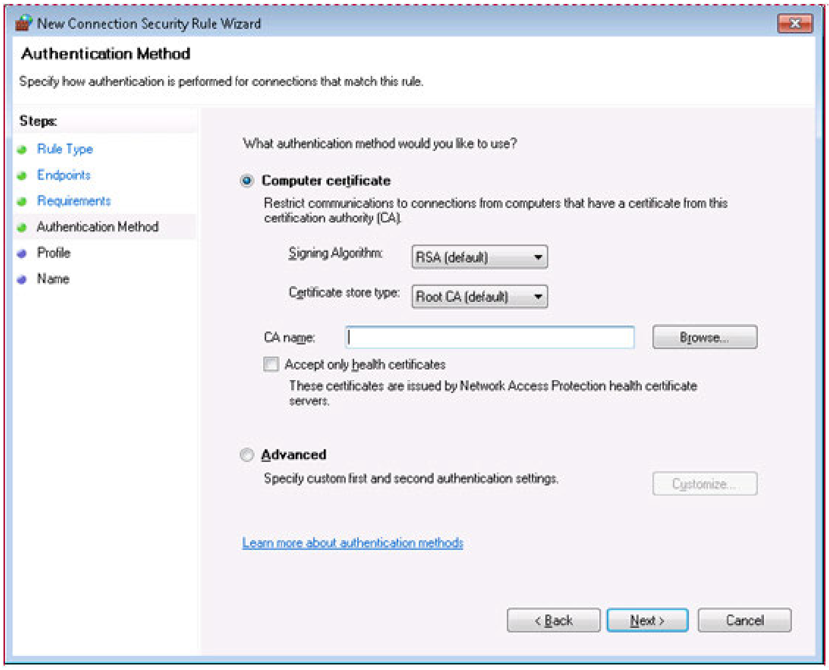
○ **Require authentication for inbound connections and request authentication for outbound connections**
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.

● **Require authentication for inbound and outbound connections**
Both inbound and outbound connections must be authenticated to be allowed.

Learn more about authentication requirements

< Back | Next > | Cancel

7. Ensure **Require authentication for inbound and outbound connections** option is selected and then click **Next.** The **Authentication method** screen appears.



Authentication Method

Specify how authentication is performed for connections that match this rule.

What authentication method would you like to use?

● Computer certificate

Restrict communications to connections from computers that have a certificate from this certification authority (CA).

Signing Algorithm: RSA (default)

Certificate store type: Root CA (default)

CA name:

□ Accept only health certificates

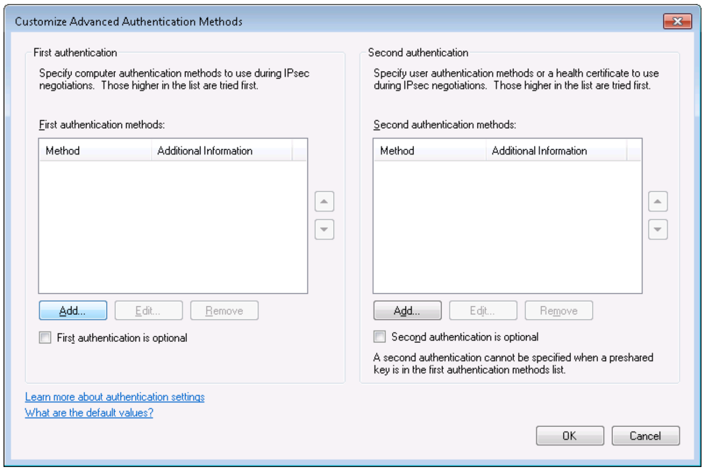
These certificates are issued by Network Access Protection health certificate servers.

○ Advanced

Specify custom first and second authentication settings.

Learn more about authentication methods

8. Under **Authentication Method** select **Advanced** and then click **Customize.**
   Customize Advanced Authentication Methods dialog appears.



Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

□ First authentication is optional

Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first.

Second authentication methods:

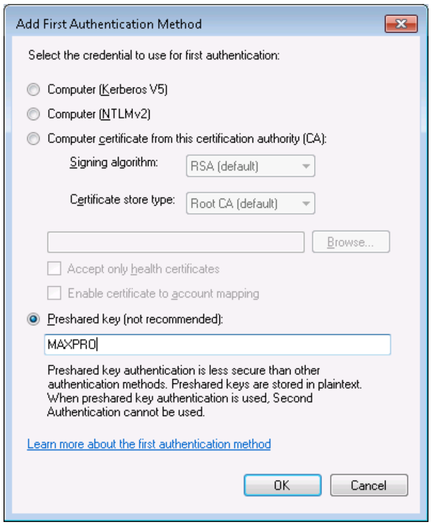
□ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

Learn more about authentication settings

What are the default values?

a. Click **ADD. Add First Authentication Method** dialog appears.



Add First Authentication Method

Select the credential to use for first authentication:

○ Computer (Kerberos V5)

○ Computer (NTLMv2)

○ Computer certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

□ Accept only health certificates

□ Enable certificate to account mapping

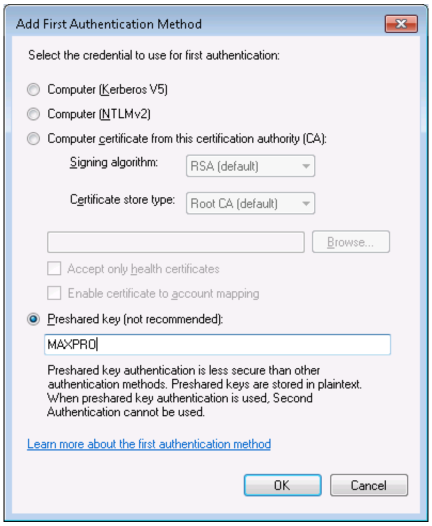
● Preshared key (not recommended):

MAXPRO

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

b. Select **Preshared Key.**

c. Type a **Key.** Example **"MAXPRO"**



Add First Authentication Method

Select the credential to use for first authentication:

○ Computer (Kerberos V5)

○ Computer (NTLMv2)

○ Computer certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

□ Accept only health certificates

□ Enable certificate to account mapping

● Preshared key (not recommended):

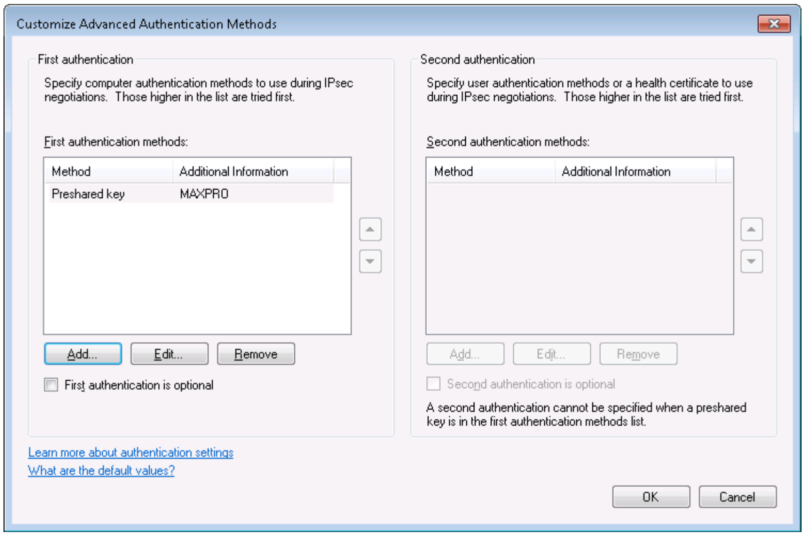
MAXPRO

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

Note: Select Computers (Kerberos v5) if using a Trusted Domain.

d. Click **OK.**

9. Click **OK** in **Customize Advanced Authentication Methods.**



Customize Advanced Authentication Methods

First authentication

Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
Preshared key	MAXPRO

☐ First authentication is optional

Second authentication

Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first.

Second authentication methods:

Method	Additional Information

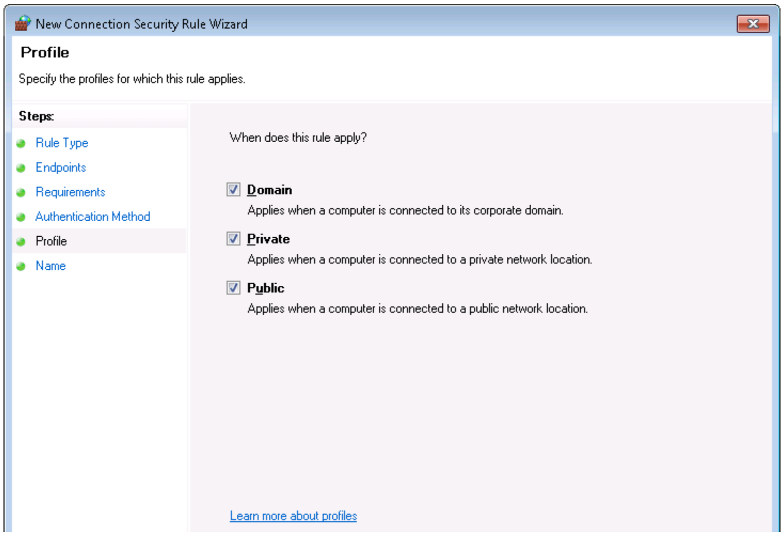
☐ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

Learn more about authentication settings
What are the default values?

Note: It is recommended to use CA certificate based Authentication

10. Click **Next.** The **Profile** screen appears.



New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

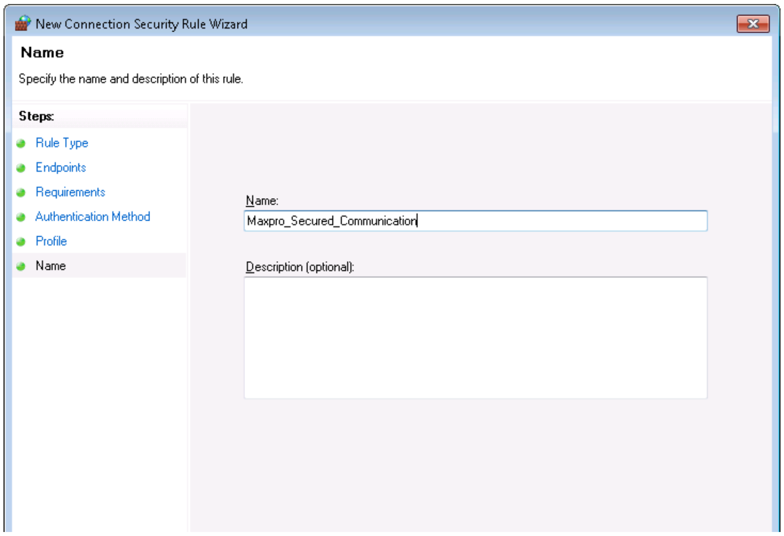
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Learn more about profiles

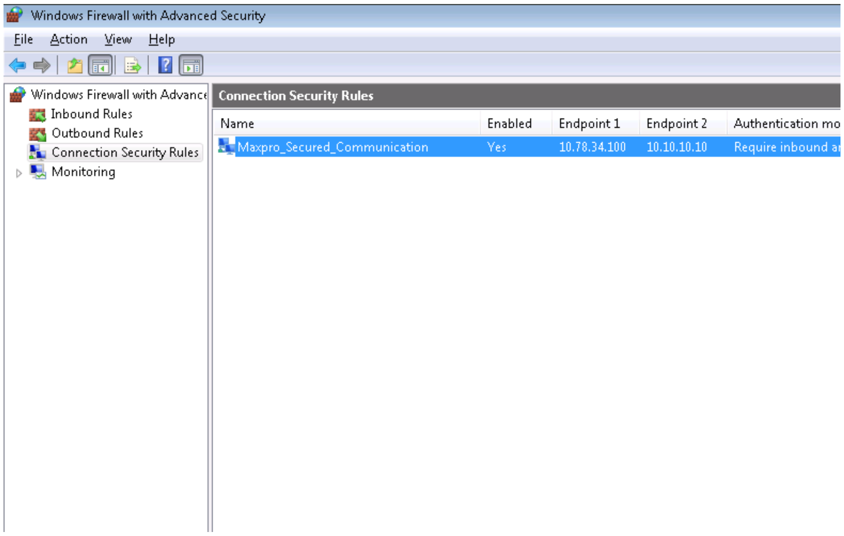
11. Select all network locations under **Profile** and then click **Next.** The **Name** screen appears.


New Connection Security Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Endpoints
Requirements
Authentication Method
Profile
Name

Name: Maxpro_Secured_Communication

Description (optional):

12. Type a **Name** for the Rule and then click **Finish.**The Rule is created.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Connection Security Rules

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mo
Maxpro_Secured_Communication	Yes	10.78.34.100	10.10.10.10	Require inbound a

Note: If the rule is not enabled, right click on the rule and click **Enable.**

Note: Create and enable a similar rule for all Maxpro machines participating in the secured communication.

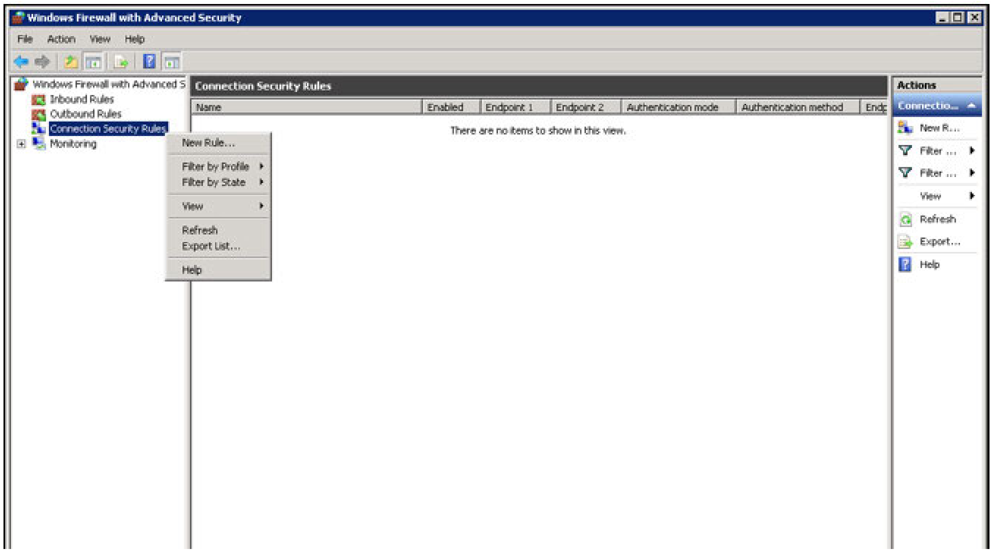
Note: If a secured rule is created on only one end point, there will not be any communication between the machine with rule and machine without rule.

Special Exception for IPSec policy (Local Machine)

This section explains about creating a rule for Special Exception on Windows Server and Client Machines:

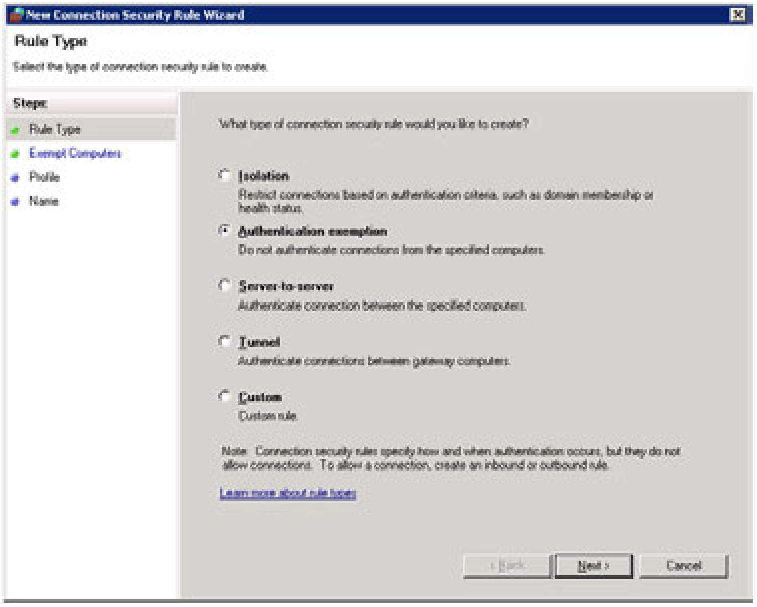
To create rule for Special Exception on Windows Server and Client Machines:

1. In the **Windows Firewall with Advanced Security** window, right-click on **Connection Security Rules** and then select **New Rule** as shown below.



There are no items to show in this view.

The **New Connection Security Rule Wizard** is displayed as shown below.



Rule Type

Select the type of connection security rule to create.

What type of connection security rule would you like to create?

○ Isolation
Restrict connections based on authentication criteria, such as domain membership or health status.

● Authentication exemption
Do not authenticate connections from the specified computers.

○ Server-to-server
Authenticate connection between the specified computers.

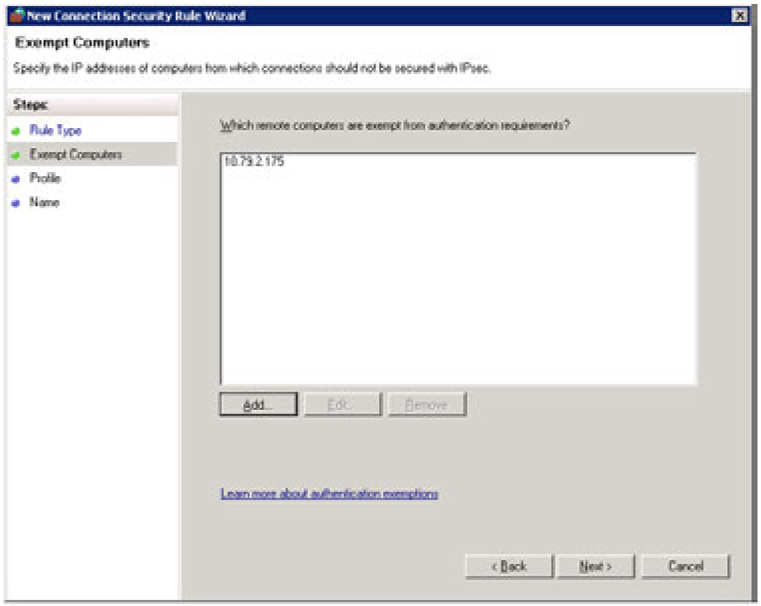
○ Tunnel
Authenticate connections between gateway computers.

○ Custom
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

Learn more about rule types

2. Click **Authentication exemption** option and then click **Next**. The **Exempt Computers** dialog appears.



New Connection Security Rule Wizard

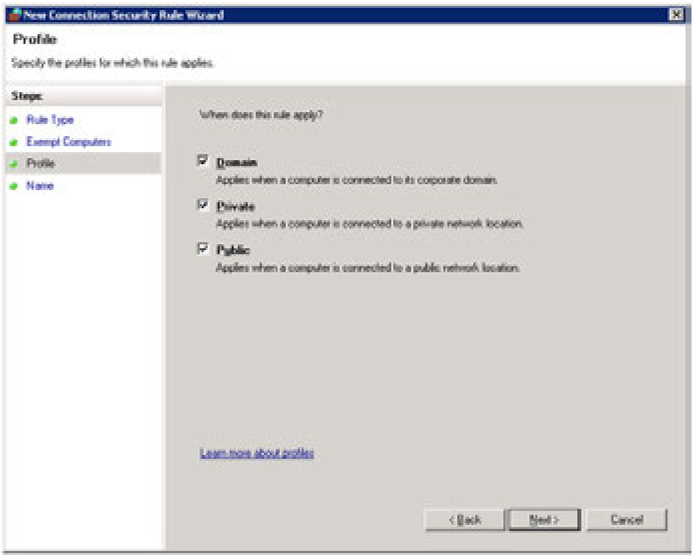
Exempt Computers

Specify the IP addresses of computers from which connections should not be secured with IPsec.

Which remote computers are exempt from authentication requirements?

10.79.2.175

3. Click **Add**, to add the **Local Machine IP** and then click **Next**. The **Profile** dialog appears.



New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

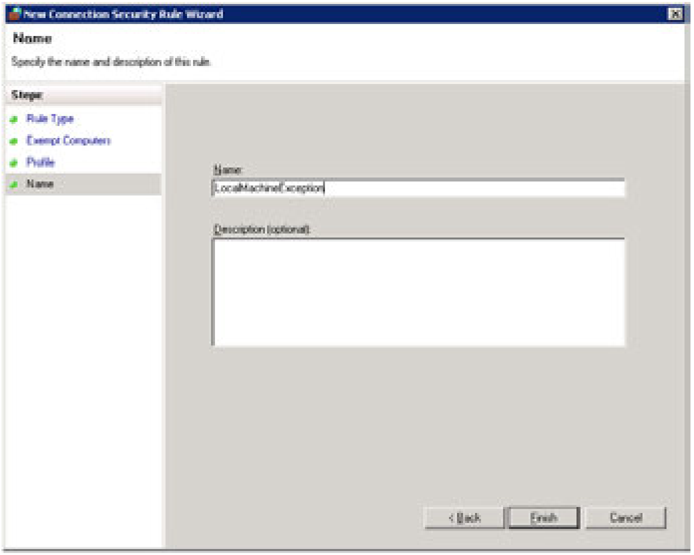
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

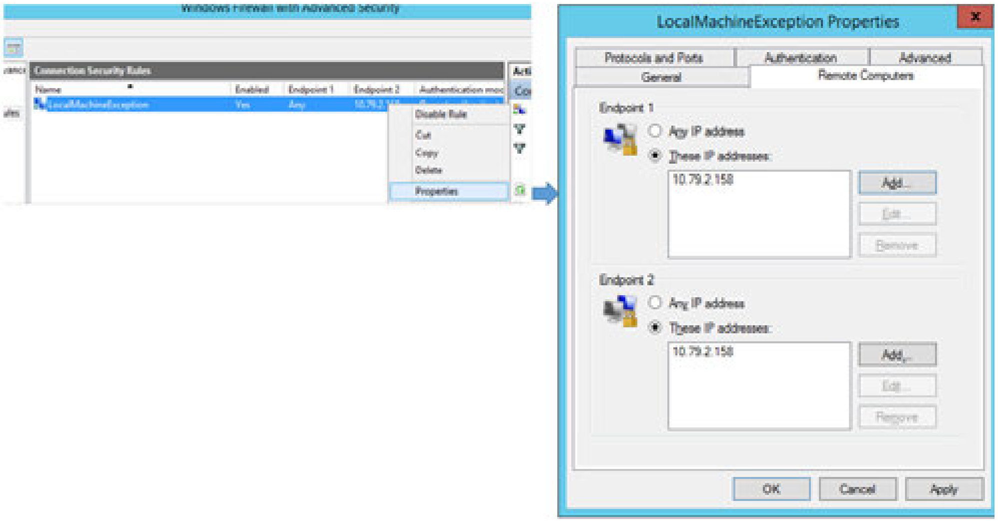
4. Under **When dose this rule apply?**, select the **Domain**, **Private** and **Public** check boxes.
5. Click **Next**. The **Name** dialog box appears.



Name: LocalMachineException

6. Type the **Name** for the rule in the box provided and then click **Finish**.

7. Under **Connection Security Rule**, right-click on the rule created and then select **Properties** as shown below.



Name	Enabled	Endpoint 1	Endpoint 2	Authentication mod
LocalMachineException	Yes	Any	10.79.2.158	

Endpoint 1
○ Any IP address
● These IP addresses:
10.79.2.158

Endpoint 2
○ Any IP address
● These IP addresses:
10.79.2.158

8. In the **Properties** dialog box, navigate to **Remote Computers** tab as shown in the above figure.

9. Verify the IP address and ensure that **These IP addresses** option is selected as shown above.

10. Click **Apply** and then click **OK**.

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 41 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.

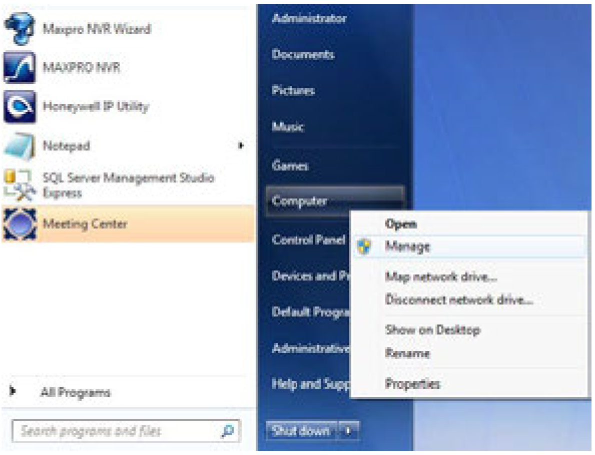
b. The database backup is recommended to be pointed to the Metadata partition.

c. The Metadata backup is recommended to be pointed to the OS partition.

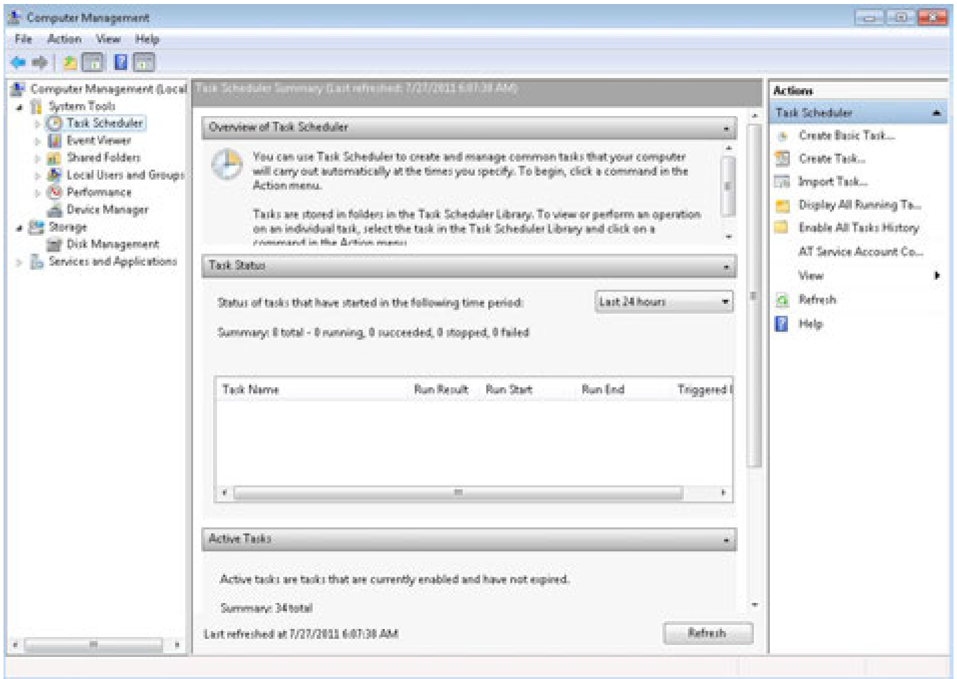
Scheduled Task for Backing up the Metadata and Database

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.

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 Figure A-1.



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: Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

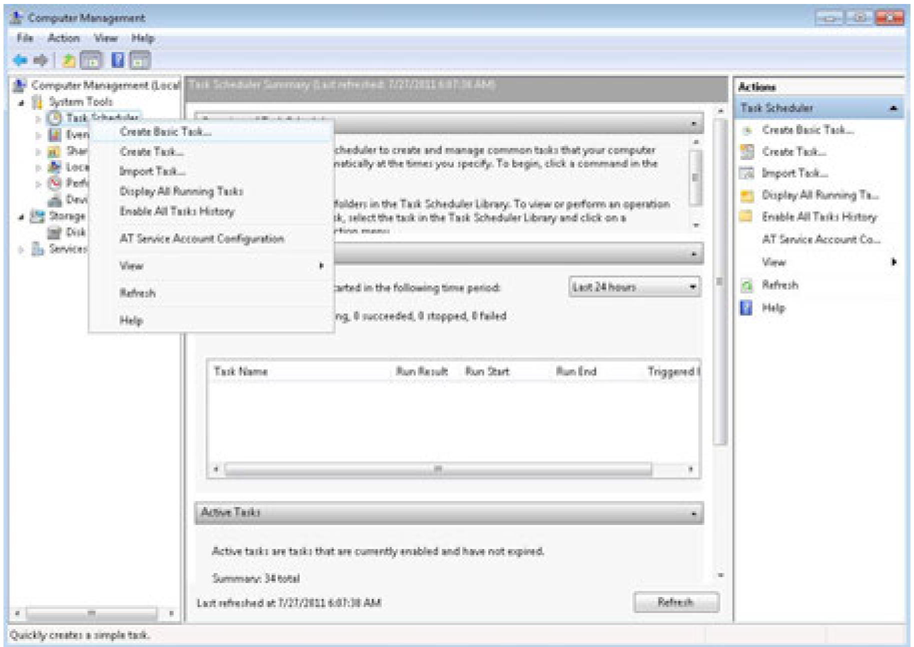
Active tasks are tasks that are currently enabled and have not expired.

Summary: 34 total

Last refreshed at 7/27/2011 6:07:38 AM

Figure A-1 Computer Management

2. Right-click **Task Scheduler** on the left pane, and click **Create Basic Task** in the context menu as shown in the following figure Figure A-2.



Task Scheduler Summary (Last refreshed: 7/27/2011 6:07:38 AM)

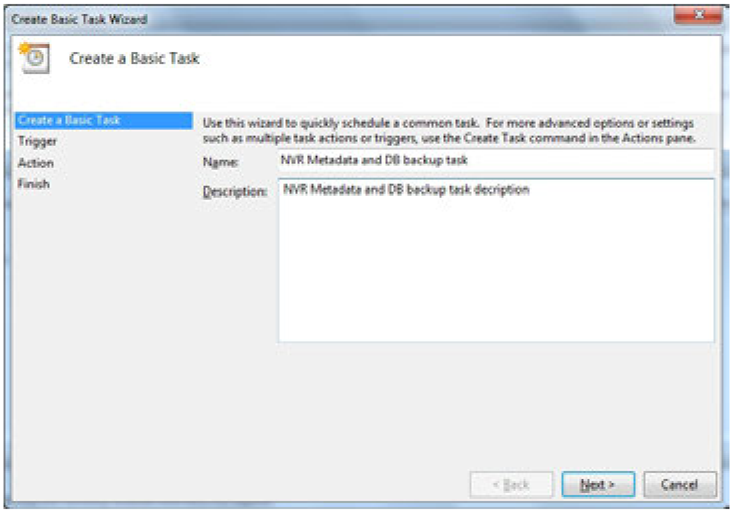
Active tasks are tasks that are currently enabled and have not expired.

Summary: 34 total

Last refreshed at 7/27/2011 6:07:38 AM

Figure A-2 Task Scheduler

The **Create a Basic Task** dialog box appears Figure A-3.



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

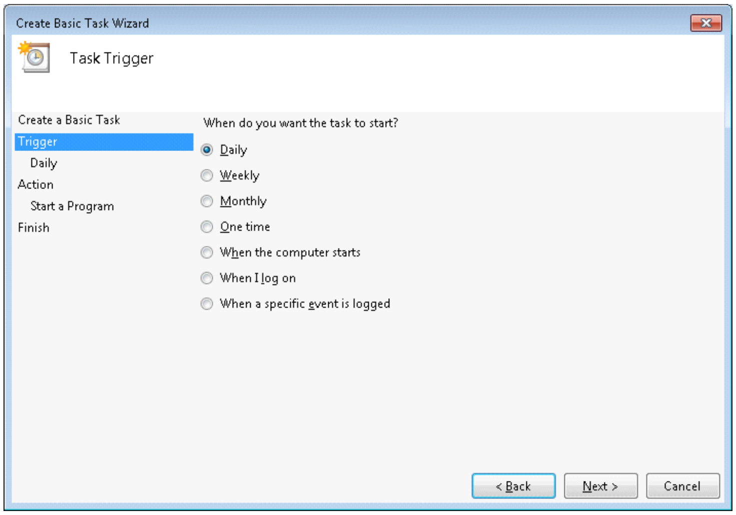
Description: NVR Metadata and DB backup task decription

Figure A-3 Create Basic Task

3. Type the **Name** of the task.

4. Type a **Description** for the task.

5. Click **Next**. The **Task Trigger** dialog box appears Figure A-4.



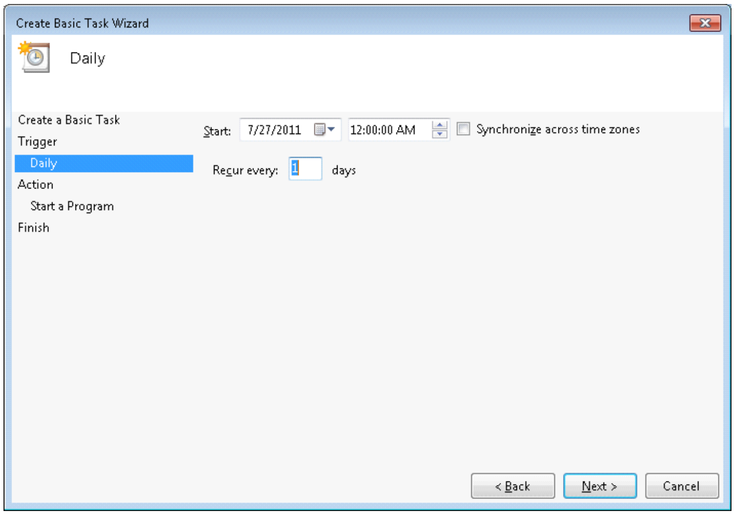
When do you want the task to start?

● Daily
○ Weekly
○ Monthly
○ One time
○ When the computer starts
○ When I log on
○ When a specific event is logged

Figure A-4 Task Trigger

6. Select the **Daily** option. You can select other options based on your requirement.

7. Click **Next**. The **Daily** dialog box appears Figure A-5.



Start: 7/27/2011 12:00:00 AM □ Synchronize across time zones

Recur every: 1 days

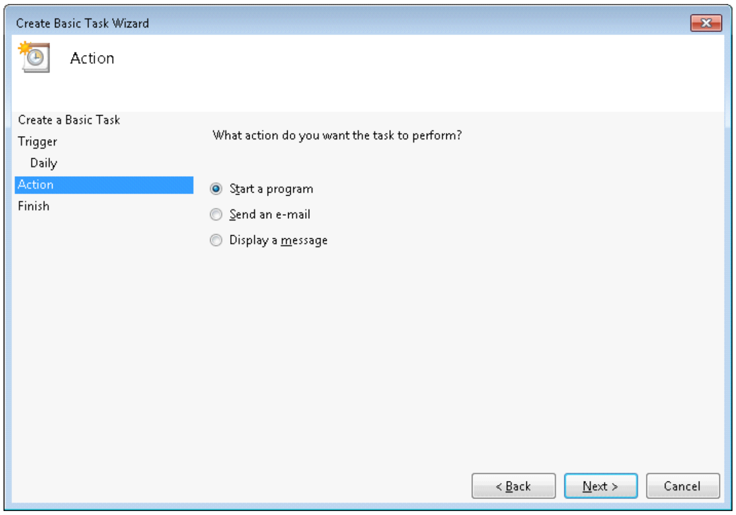
Figure A-5 Daily Dialog

8. In the **Start** box, select the start date and time of the task.

9. Select the **Synchronize across time zones** check box to synchronize the time across different time zones.

10. Type the days in **Recur every**, to run the task periodically.

11. Click **Next.** The **Action** dialog box appears Figure A-5.



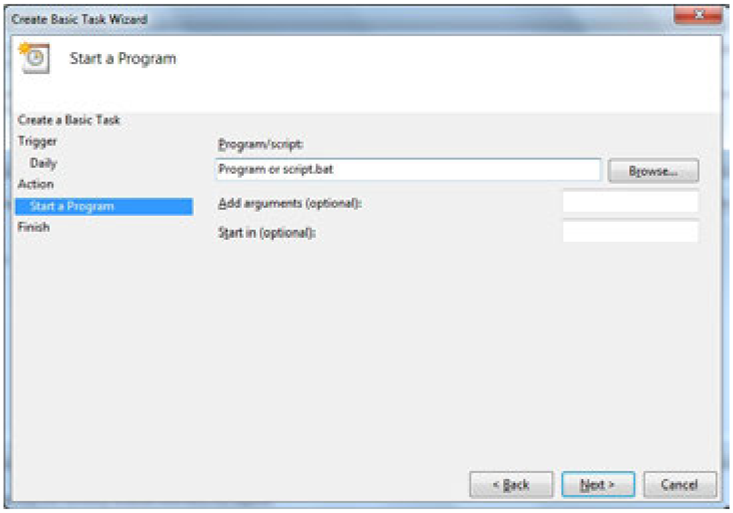
What action do you want the task to perform?

● Start a program
○ Send an e-mail
○ Display a message

Figure A-6 Action dialog

12. Select the **Start a Program** option.

13. Click **Next**. The **Start a Program** dialog box appears Figure A-7.



Program/script:
Program or script.bat
Add arguments (optional):
Start in (optional):

Figure A-7 Start a Program

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:\.**

15. Click **Next** after you have selected the above batch file. The **Summary** dialog box appears.
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 292.

How to access the Meta Data Conversion Utility

To access the Meta Data Conversion Utility

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.

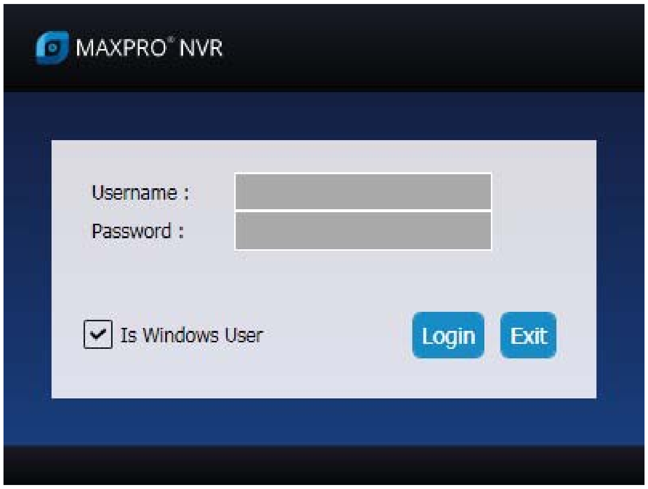
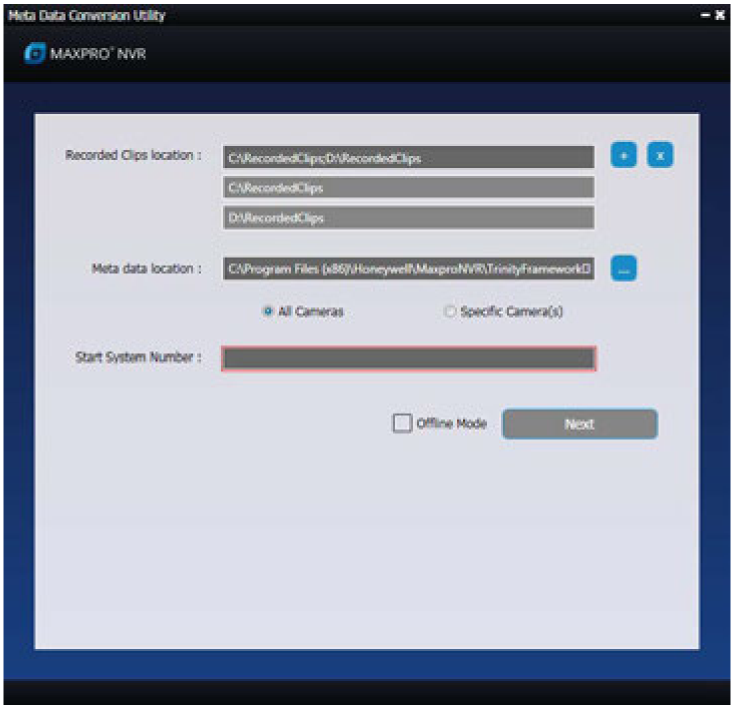


Figure A-8 Meta Data Conversion Utility Login

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.

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\TrinityFrameworkD

● All Cameras ○ Specific Camera(s)

Start System Number :

□ Offline Mode

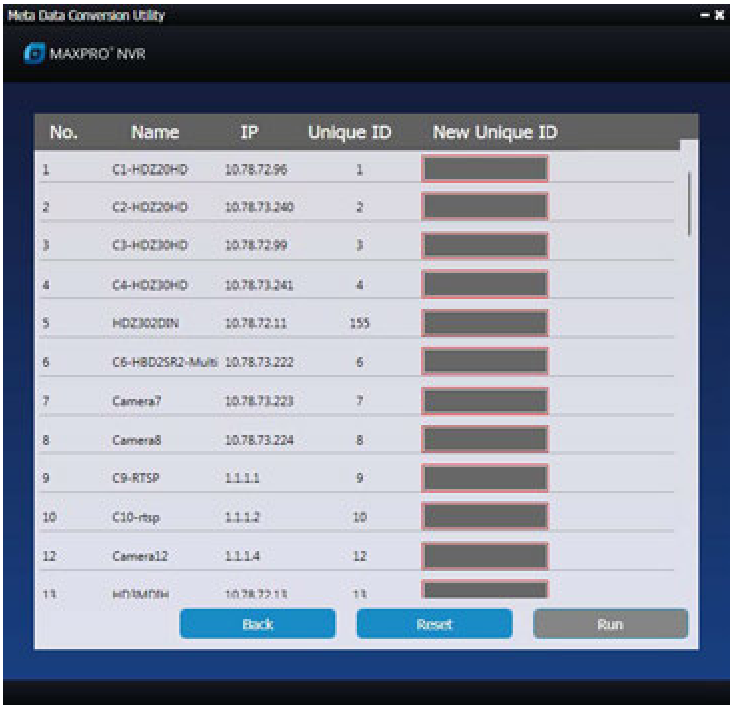
Figure A-9 Meta Data Conversion Utility

Updating the Unique system ID for all Cameras

To update the Unique system ID for all cameras

1. Access and launch the Meta Data Conversion Utility as explained in How to access the Meta Data Conversion Utility section on page 289. By default the Recorded Clips Location and Meta data location is updated with your default path.
2. Click + to add additional location for Recorded Clips Location.
   Or

   Click x to delete any Recorded Clips Location.
3. Click ... to browse and update the existing Meta data path.
4. Click **All Cameras** option.
5. In the **Start System Number** box, type the starting number for all the cameras.
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	

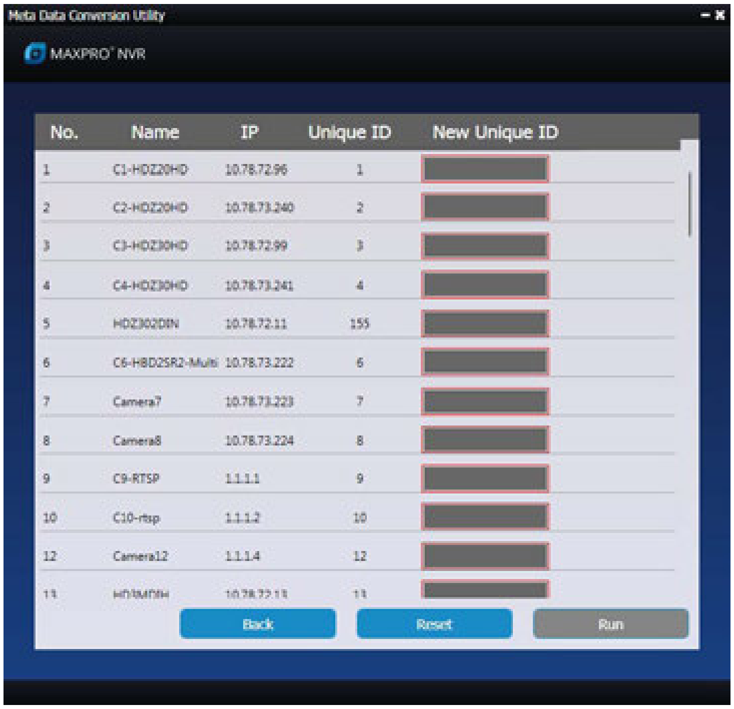
Figure A-10 Define Unique ID screen

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

1. Perform step 1 through step 3 of Updating the Unique system ID for all Cameras section on page 290.
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	

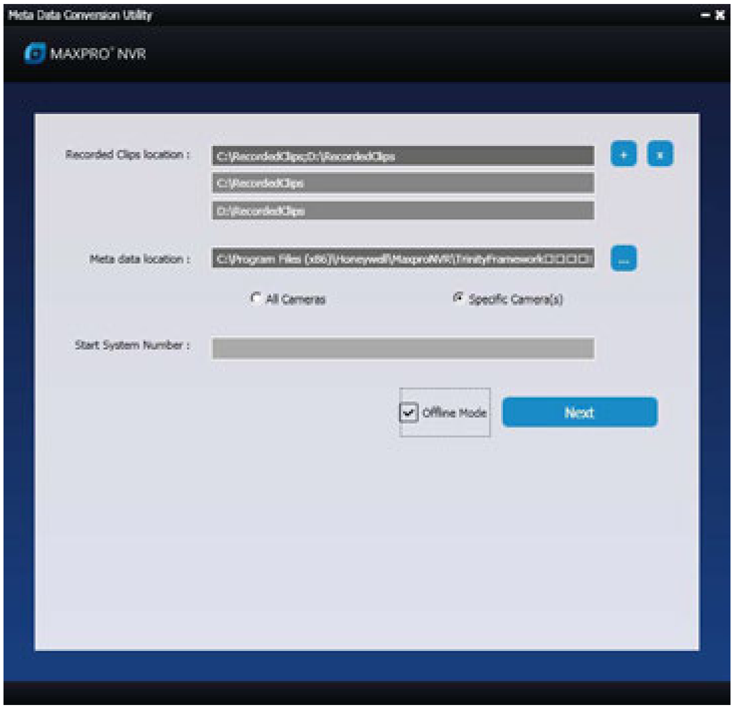
Figure A-11 Updating Unique ID

3. Scroll up and down to view the specific cameras and then type the required **New Unique ID** in the corresponding box.
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

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.



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□□□□□

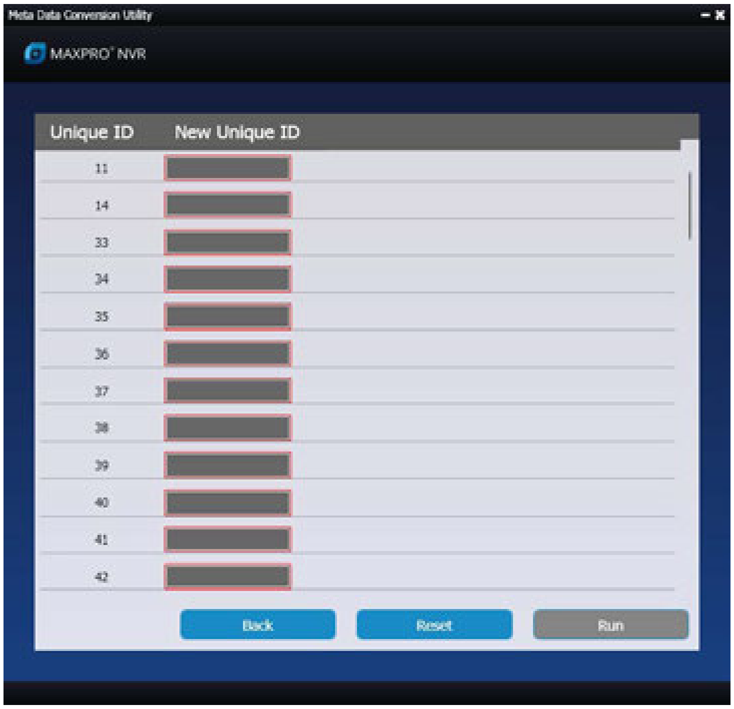
○ All Cameras ● Specific Camera(s)

Start System Number :

☑ Offline Mode

Figure A-12 Offline Mode

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.



Meta Data Conversion Utility

MAXPRO® NVR

Unique ID	New Unique ID
11	
14	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	

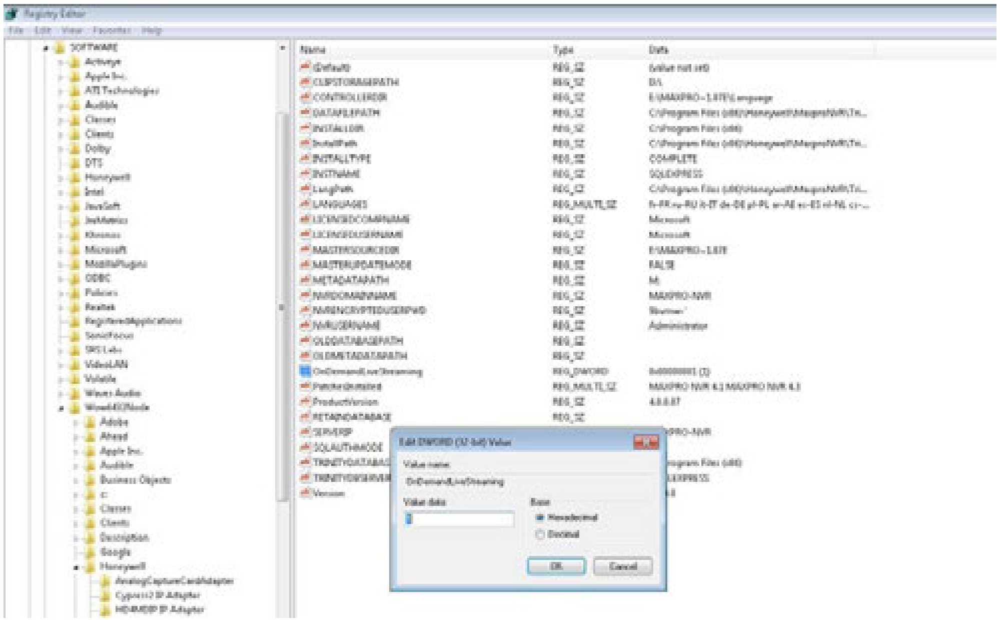
Figure A-13 Offline Updating Unique ID

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.

4. Click **Run** to execute the utility.
   Or
   Click **Reset** to reset all ID.

How to Enable Video on demand feature in MAXPRO NVR

1. Launch the **Registry Editor** Window.
2. Navigate to the below registry path **HKEY_LOCAL_MACHINE->SOFTWARE->Wow6432Node->Honeywell->MaxproNVR->TrinityFramework.**
3. Locate **OnDemandLiveStreaming** parameter and in the Data column.
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-...
LICENSEDCOMPANYNAME	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	[illegible]
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		...PRO-NVR
SQLAUTHMODE		
TRINITYDATABAS...		...rogram Files (x86)
TRINITYDBSERVER...		...LEXPRESS
Version		...4.0

Edit DWORD (32-bit) Value

Value name:
OnDemandLiveStreaming

Value data: 1

Base
● Hexadecimal
○ Decimal

OK Cancel

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 allow Enable/Disable of cameras and Enable Camera stream Redirect to NVR in ISOM

1. Navigate the path in NVR **C:\Program Files (x86)****Honeywell****UVISOM.**

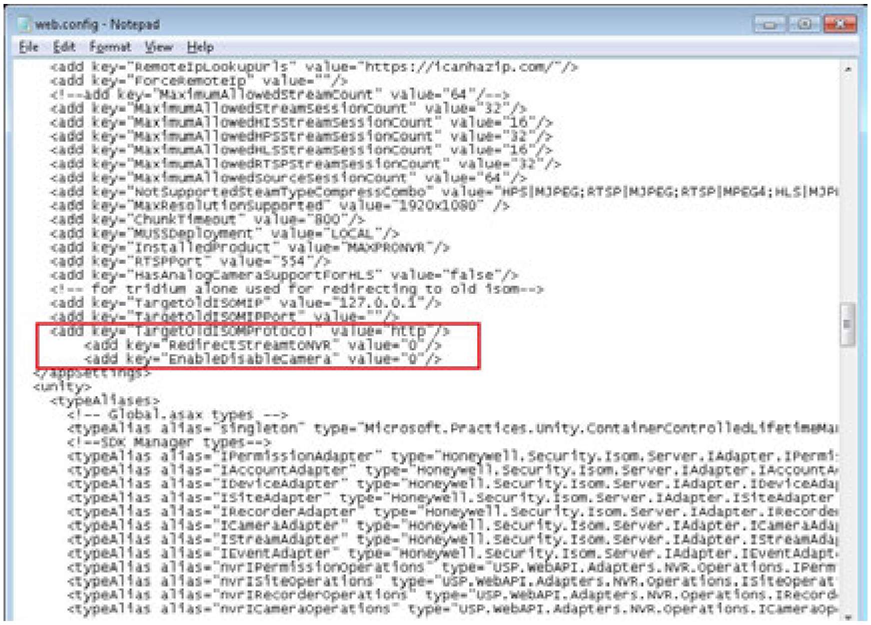
2. Open web.config file in notepad and check the below 2 entries:

   <add key="RedirectStreamtoNVR" value="0"/>

   <add key="EnableDisableCamera" value="0"/>

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|MJP
    <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:

1. Navigate the path in VMS **C:\Program Files (x86)\Honeywell\UVISOM.**

2. Repeat the step 2 to step 3 of How to allow Enable/Disable of cameras and Enable Camera stream Redirect to NVR in ISOM section.

Note: Make sure MAXPRO Web client is working.

This page is intentionally left blank.

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.
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.

The following figure shows an example of three seconds of video at 5 FPS and 5 GOP.

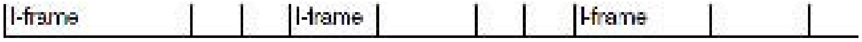


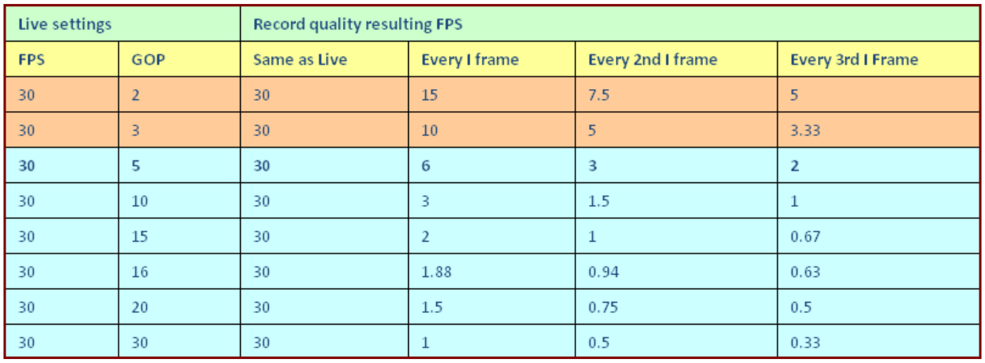
Figure B-1 I-frame Example

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 ***120*** for more information on configuring the pre and post event recording settings.

Configuring Camera Settings for VMD-Based Recording

1. Click the **Configurator** tab and then the **Camera** tab to open the **Camera configuration** page (***Figure B-2***).

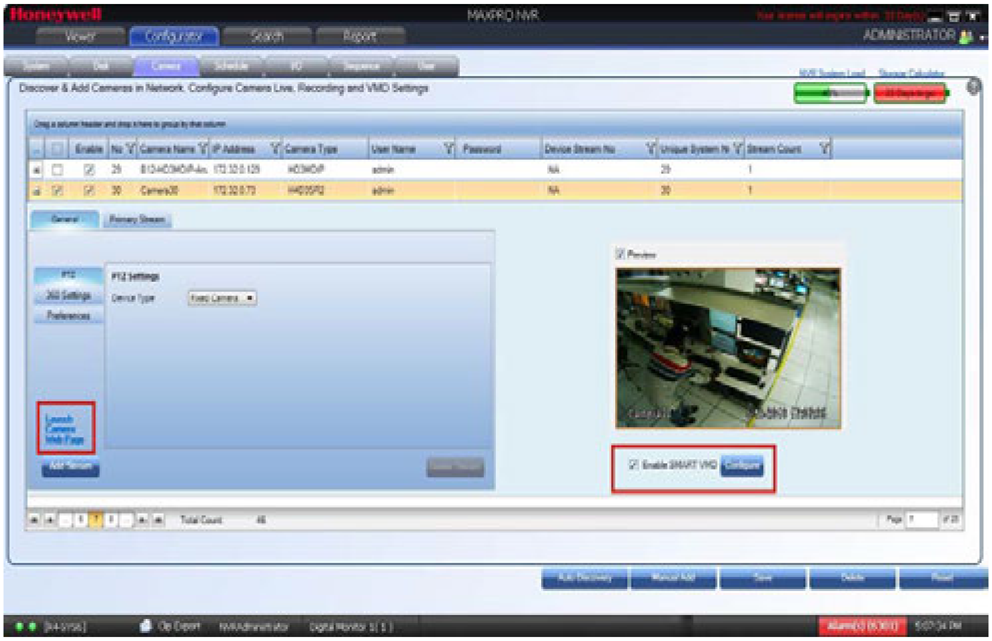


Figure B-2 Camera configuration page

- 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 (Camera based VMD) on Honeywell IP Cameras*** section on page ***301*** 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 ***301*** 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.

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 ***301*** for more information.

Configuring Built-in VMD (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.

1. Click the **Video Analytics** tab.
2. Click the **Region** drop-down list in the **Video Motion Detection** pane, then select a region from the five available.
3. Click the **VMD** drop-down arrow, and then select **Enable**.
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.
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 ***302***.

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:

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.
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.

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.
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 in ***Figure B-3***.

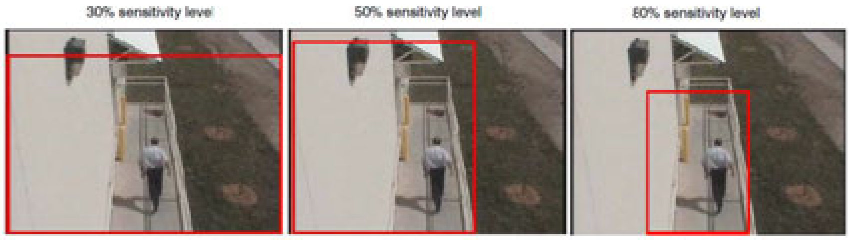


Figure B-3 Sensitivity Level Comparison: Normal Field of View

Wide Field of View

In a wide field of view camera, the car shown below (***Figure B-4***)would be expected to trigger a VMD alarm if the VMD region-of-interest box is not larger than indicated by the red box.

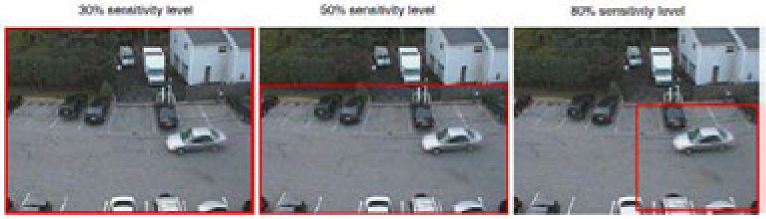


Figure B-4 Sensitivity Level Comparison: Wide Field of View

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.

Figure B-5 illustrates a typical region-of-interest box configuration in a combination field of view.

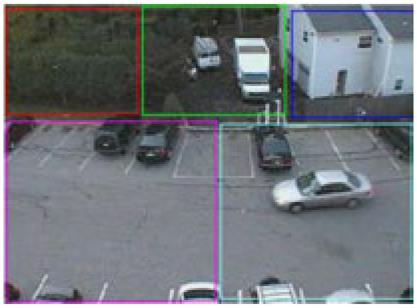


Figure B-5 Combination Field of View Example

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 ***101*** 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
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

EventID	EventDescription	EventSeverity
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
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

1. Launch the required camera web page.
2. Click the **Setup** tab.
3. On the left pane, navigate to **System Setup** > **Upgrade**. The **Upgrade** page is displayed as shown below.

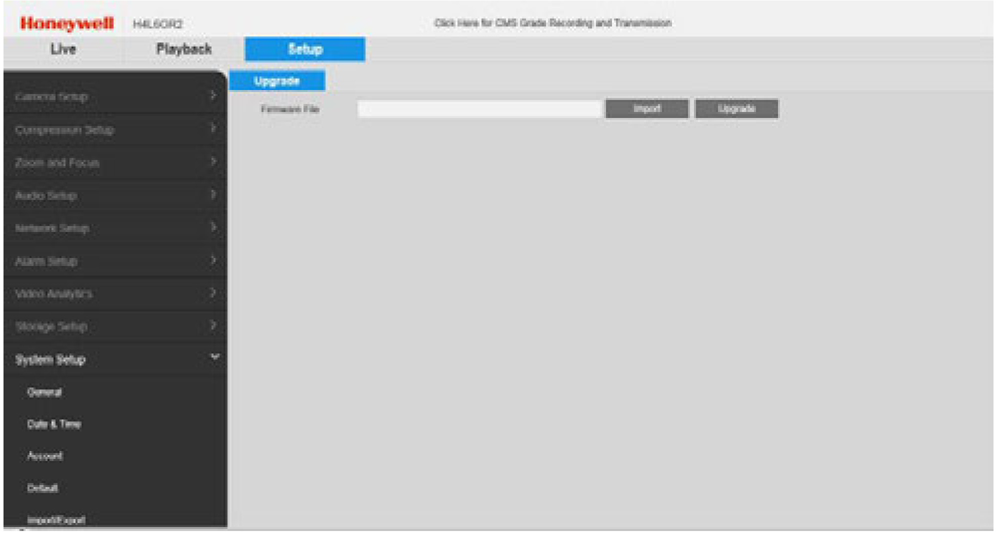


Figure B-6 Upgrade Firmware - Setup Page

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.

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.

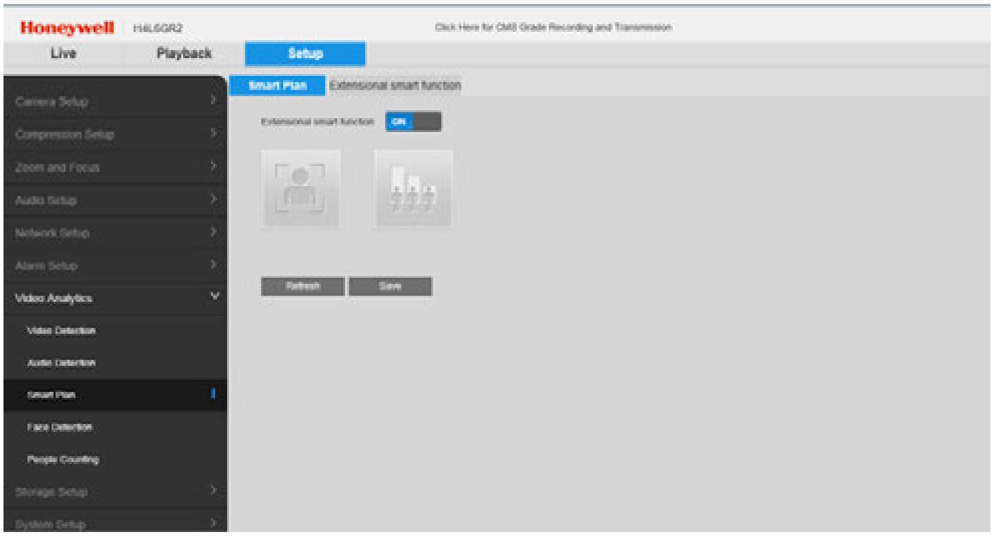


Figure B-7 Smart Plan Setup Page

2. Under Smart Plan, turn **ON** the Extensional smart function option. The Extensional smart function tab is enabled.
3. Click the **Extensional smart function** tab to view the **LoiterTrace** alarms as shown below.

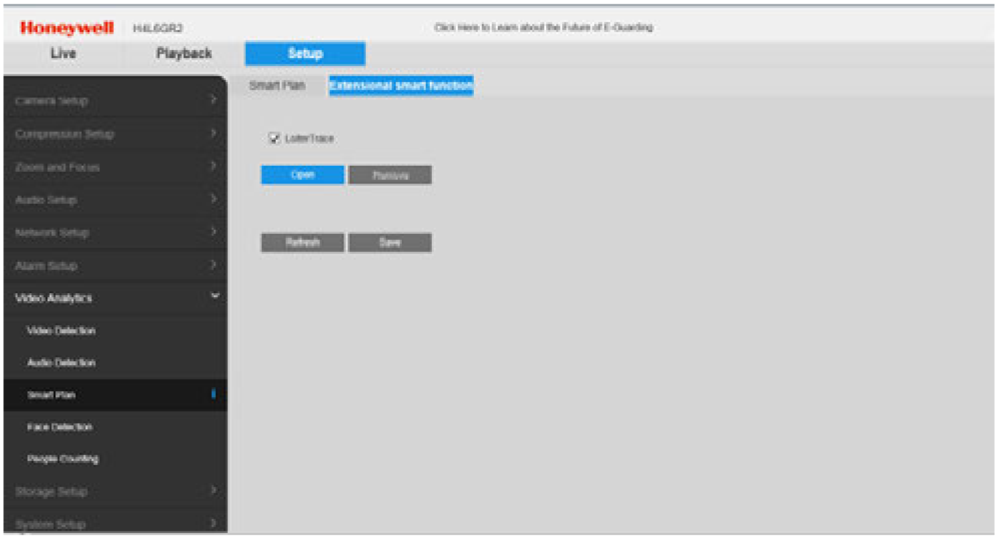
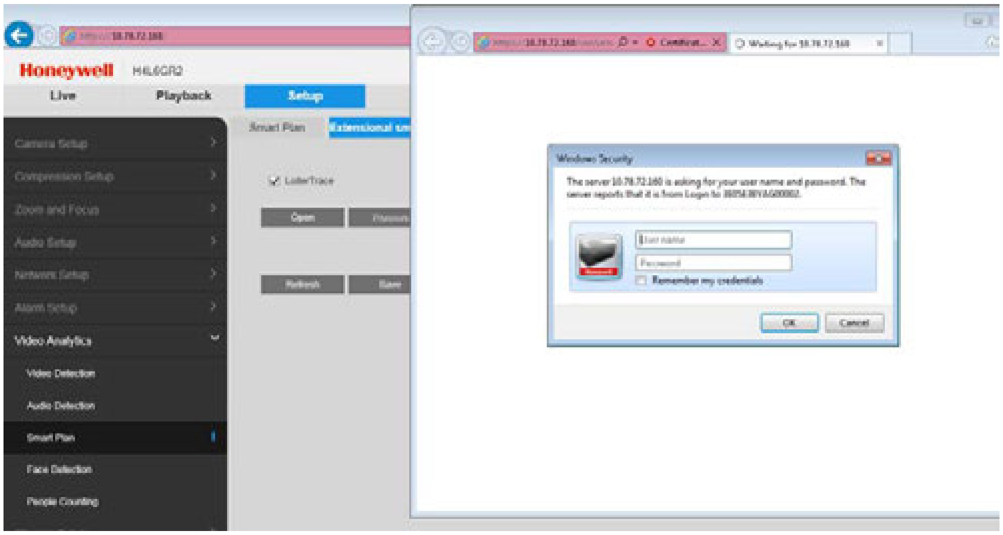


Figure B-8 Extensional smart function page

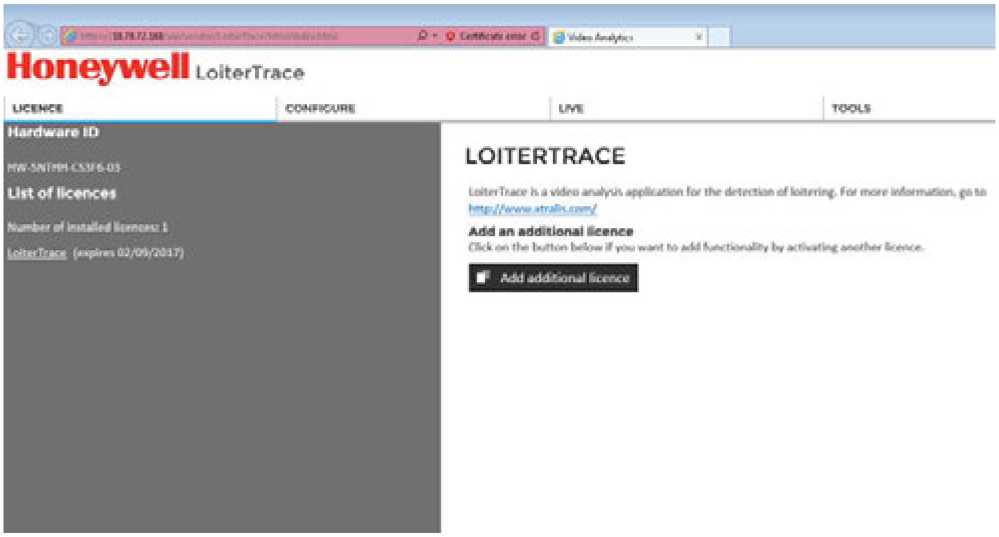
4. Click **Open**. The Xtralis authentication window is displayed as shown below.



The server 10.78.72.160 is asking for your user name and password. The server reports that it is from Login to [illegible].

Figure B-9 Xtralis Login

5. Enter the credentials and then click OK. The LoiterTrace page is displayed as shown below.



Hardware ID

MW-5NTHM-C53F6-03

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/

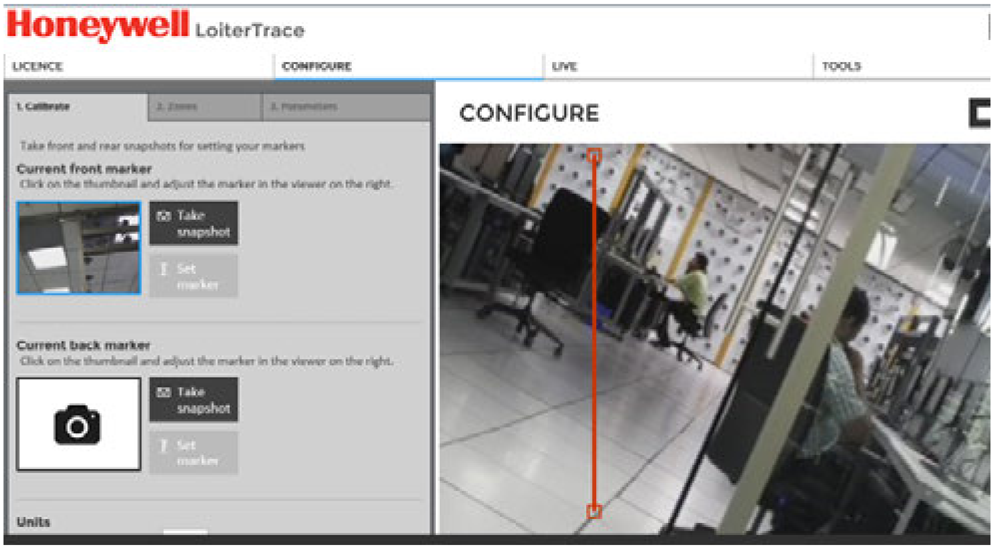
Add an additional licence

Click on the button below if you want to add functionality by activating another licence.

Figure B-10 Loiter Trace Page

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.



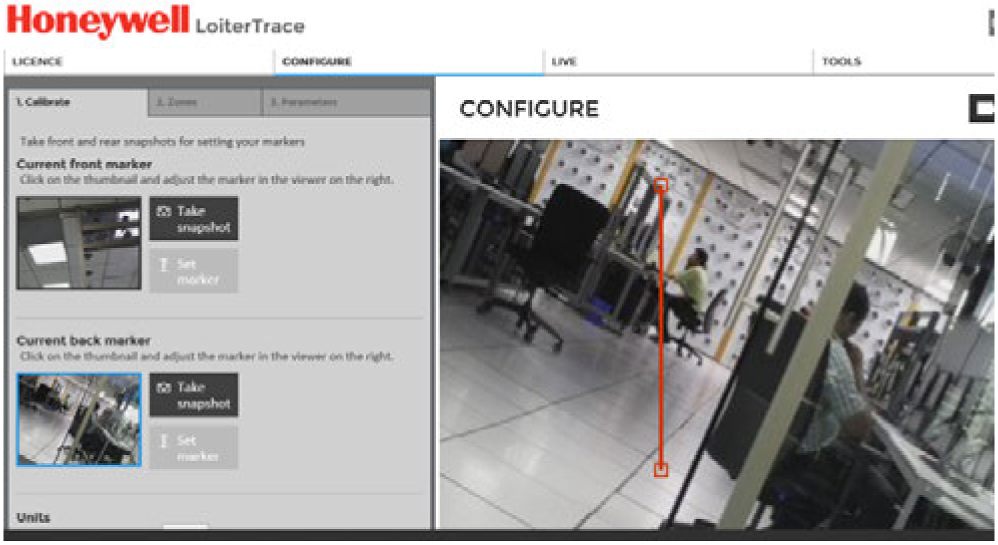
Take front and rear snapshots for setting your markers

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.

Figure B-11 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.

Figure B-12 Loiter Trace - Calibrate

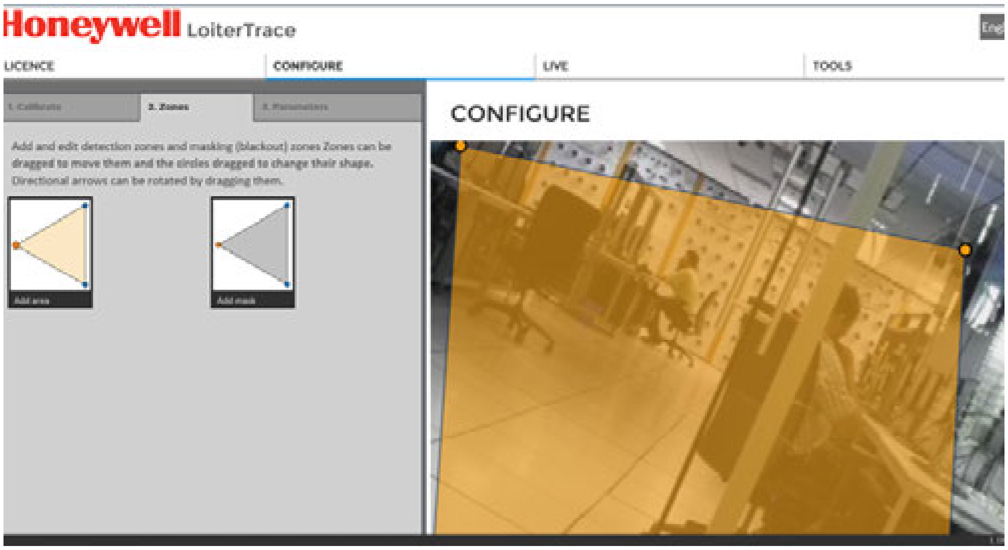
c. Click **Save** once done.

7. 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.

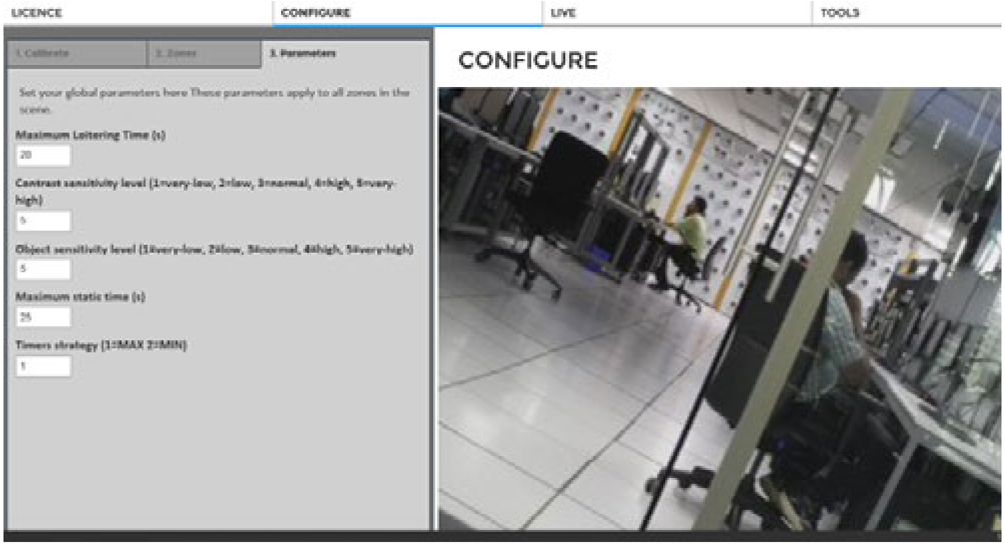


Add and edit detection zones and masking (blackout) zones Zones can be dragged to move them and the circles dragged to change their shape. Directional arrows can be rotated by dragging them.

Figure B-13 Loiter Trace - Zones

8. 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

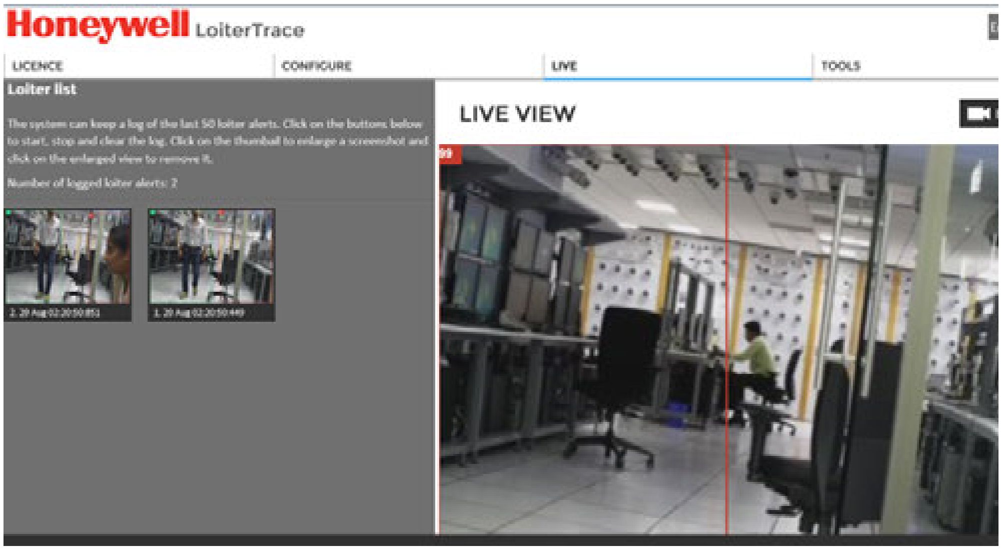
Timers strategy (1=MAX 2=MIN)
1

Figure B-14 Loiter Trace - Parameters

   b. Click **Save** once done.

9. Once the configuration is done, click the Live tab. The Live View tab is displayed.

10. 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. 20 Aug 02:20:50:851

1. 20 Aug 02:20:50:449

Figure B-15 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.

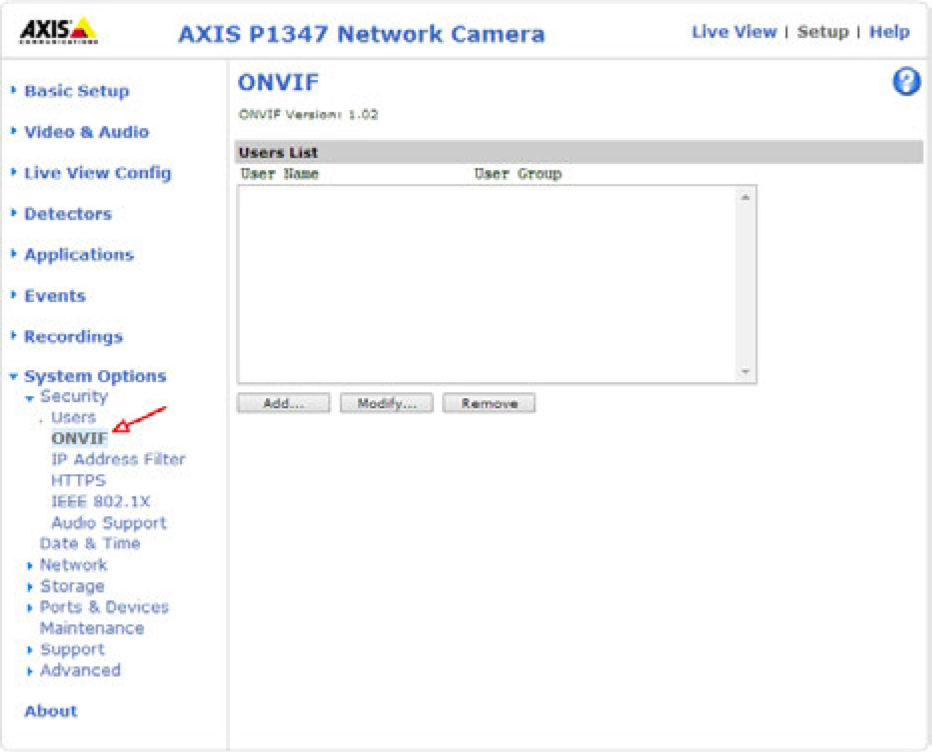
The above scenario is noticed if you log on to the camera web page (for example to set the IP address on the AXIS device) prior to discovering and configuring the device in NVR through ONVIF; as a result the ONVIF Webservice gets disabled automatically.

Perform the steps in ***Option 1: Add a ONVIF user in the camera web page.*** section on page ***306***. or ***Option 2: Reset to factory default settings*** section on page ***308*** 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.

1. Log on to the AXIS camera web page. The AXIS camera home page appears with live video.
2. Click **Setup** and then navigate to **System Options** > **ONVIF**. The **User List** dialog box appears (see ***Figure B-6***).



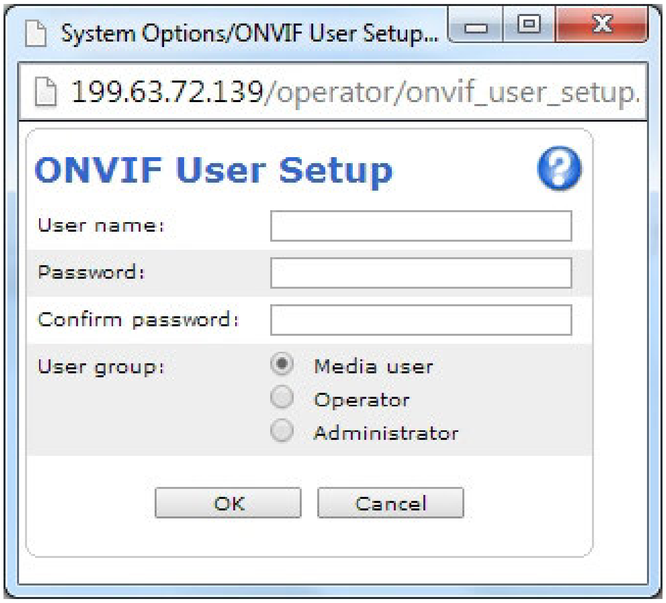
ONVIF

ONVIF Version: 1.02

Users List	
User Name	User Group

Figure B-16 User List

3. Click the **Add** button. The **ONVIF User Setup** dialog box appears (see ***Figure B-7***).


System Options/ONVIF User Setup...
199.63.72.139/operator/onvif_user_setup.
OK
Cancel

ONVIF User Setup

User name:

Password:

Confirm password:

User group: ● Media user ○ Operator ○ Administrator

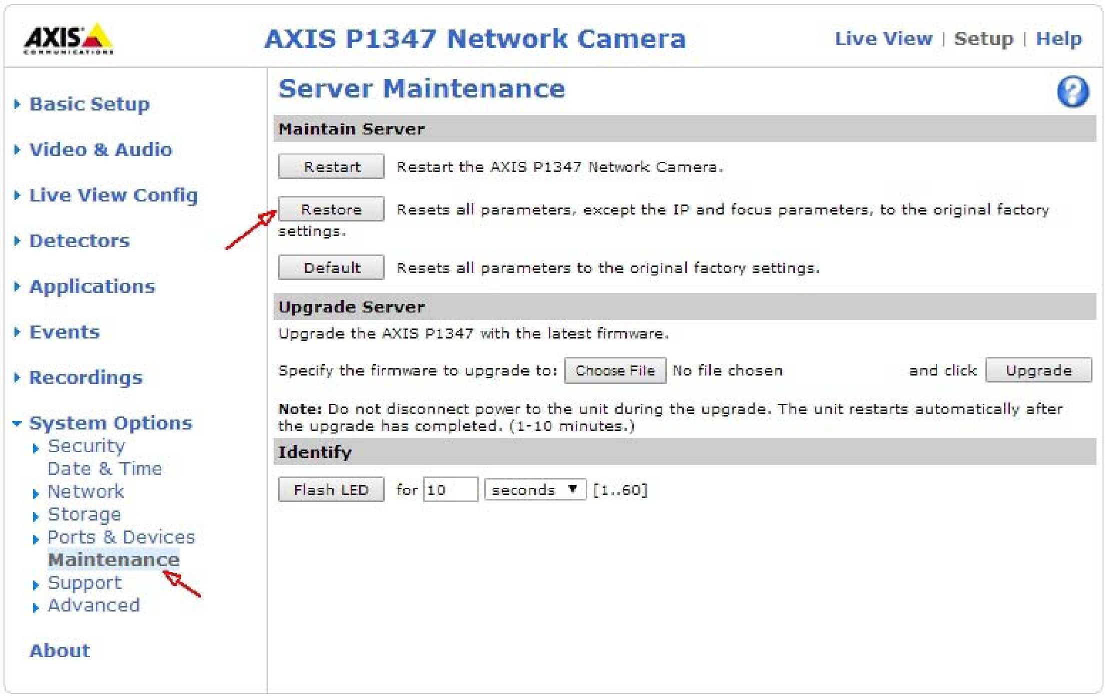
Figure B-17 ONVIF User Setup

4. Type the **user name** and **password** in the respective boxes.

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

1. Log on to the AXIS camera web page. The AXIS camera home page appears with live video.
2. Click **Setup** and then navigate to **System Options** > **Maintenance.** The **Server Maintenance** page appears (see *Figure B-8*).



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 the AXIS P1347 with the latest firmware.

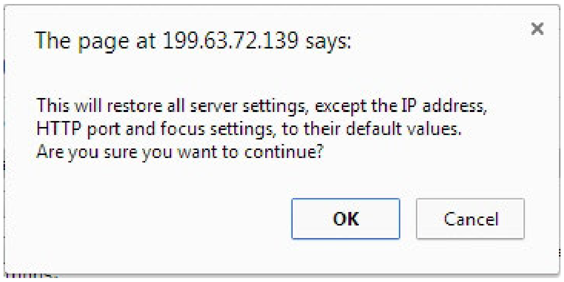
Specify the firmware to upgrade to: No file chosen and click

Note: Do not disconnect power to the unit during the upgrade. The unit restarts automatically after the upgrade has completed. (1-10 minutes.)

for 10 seconds [1..60]

Figure B-18 Server Maintenance

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?

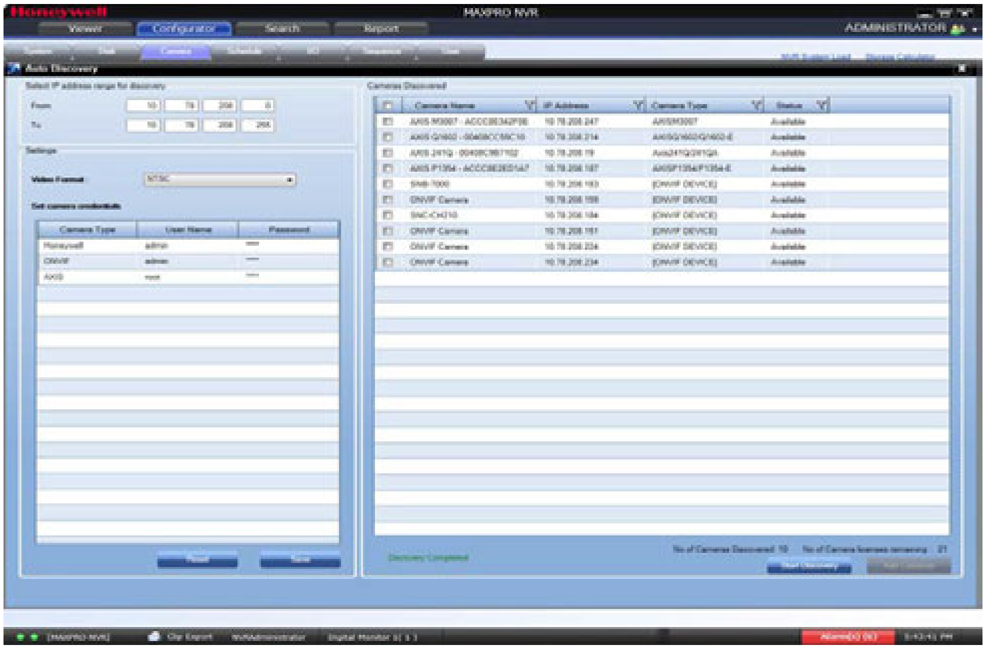
4. Click **OK**.

Note: **Restore** operation resets all the parameters, except the IP and focus parameters, to the original factory settings.

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

1. In MAXPRO NVR, click the **Configurator** tab. The **System** page displays by default.
2. Click the **Camera** tab to open the **Camera** page.
3. Click the **Auto Discovery** button, the Auto Discovery screen is displayed.



From 10 78 208 0
To 10 78 208 255

Video Format: NTSC

Set camera credentials

Camera Type	User Name	Password
Honeywell	admin	****
ONVIF	admin	****
AXIS	root	****

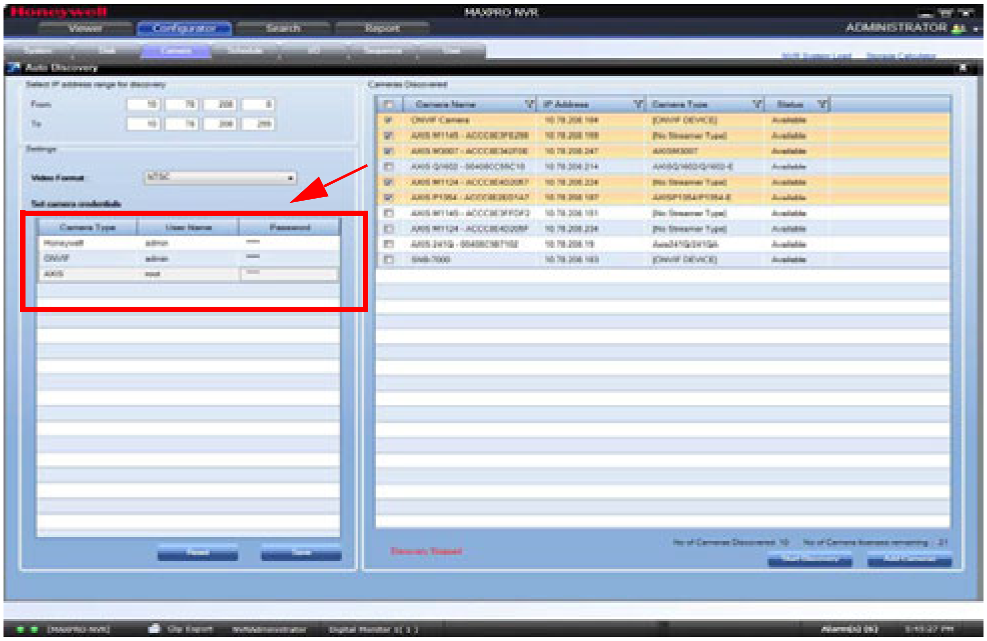
☐	Camera Name	IP Address	Camera Type	Status
☐	AXIS M3007 - ACCC8E342F08	10.78.208.247	AXISM3007	Available
☐	AXIS Q1602 - 00408CC58C10	10.78.208.214	AXISQ1602/Q1602-E	Available
☐	AXIS 241Q - 00408C9B7102	10.78.208.19	Axis241Q/241QA	Available
☐	AXIS P1354 - ACCC8E2ED1A7	10.78.208.187	AXISP1354/P1354-E	Available
☐	SNB-7000	10.78.208.183	[ONVIF DEVICE]	Available
☐	ONVIF Camera	10.78.208.198	[ONVIF DEVICE]	Available
☐	SNC-CH210	10.78.208.184	[ONVIF DEVICE]	Available
☐	ONVIF Camera	10.78.208.181	[ONVIF DEVICE]	Available
☐	ONVIF Camera	10.78.208.224	[ONVIF DEVICE]	Available
☐	ONVIF Camera	10.78.208.234	[ONVIF DEVICE]	Available

Discovery Completed

No of Cameras Discovered 10 No of Camera licenses remaining 21

4. After the discovery, to add the AXIS cameras, first clear the check boxes corresponding to all other cameras other than AXIS cameras.
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 ***136*** 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	10.78.208.188	[No Streamer Type]	Available
☑	AXIS M3007 - ACCC8E342F08	10.78.208.247	AXISM3007	Available
☐	AXIS Q1602 - 00408CC95C18	10.78.208.214	AXISQ1602/Q1602-E	Available
☑	AXIS M1124 - ACCC8E4D2087	10.78.208.224	[No Streamer Type]	Available
☑	AXIS P1354 - ACCC8E3ED1A7	10.78.208.187	AXISP1354/P1354-E	Available
☐	AXIS M1145 - ACCC8E3FFDF2	10.78.208.151	[No Streamer Type]	Available
☐	AXIS M1124 - ACCC8E4D208F	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

Discovery Stopped

No of Cameras Discovered: 10 No of Camera licenses remaining : 21

[MAXPRO-NVR] Clip Export NVRAdministrator Digital Monitor 1(1) Alarm(s) (6) 5:15:27 PM

Figure B-19 Axis Credentials

6. Click **Apply**.
7. In the **Discover cameras here** area, click **Add** to add the camera.

This page is intentionally left blank

C

Appendix C

Patches Released on Top of NVR 4.0

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

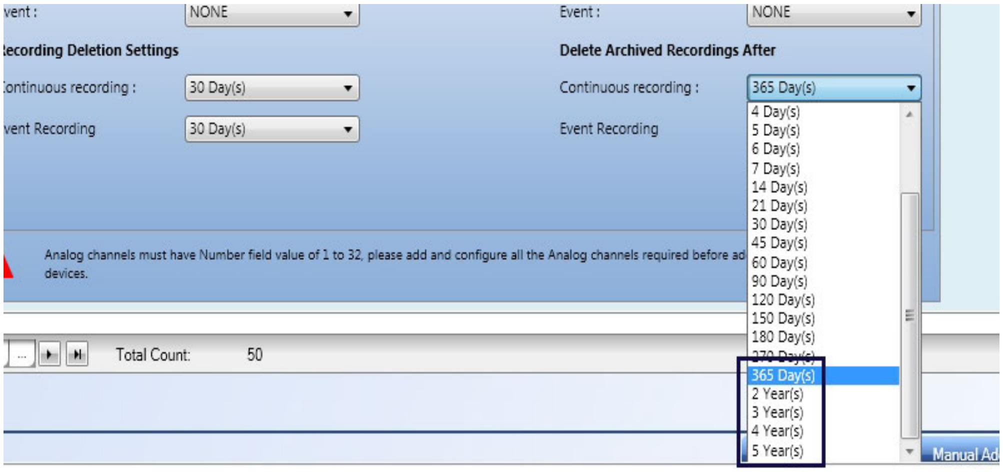
Patch Version: (NVR 4.0 SP1 Build 97)

Installation: To be installed on top of MAXPRO NVR 4.0

RELEASE HIGHLIGHTS:

This Patch includes the following enhancements:

1. Supports Sky-Lake Processor
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.



vent : NONE

ecording Deletion Settings

ontinuous recording : 30 Day(s)

vent 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

3. Updated the Resolutions for Equip S2 series (HICC-2500MI, HIVDC-2500MI) cameras.
4. Updated the Number of Streams [3 Streams] for Equip S2 series (HICC-2500MI, HIVDC-2500MI) cameras.
5. Support for 15 Performance series camera s models.
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.

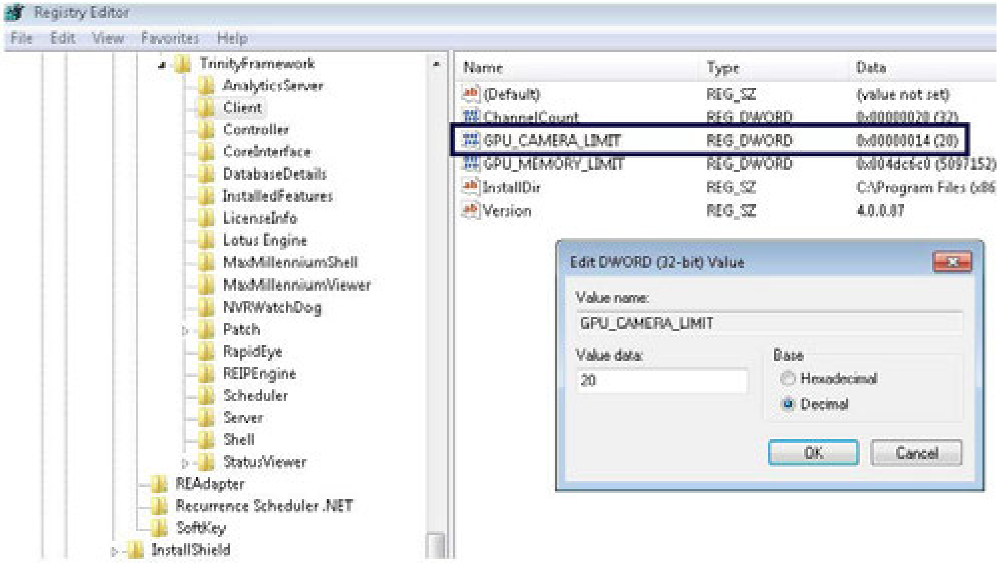
ISSUES FIXED

The following are the issues fixed in this patch:

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.
2. I18N: Fixed the issue: Values are not displaying in the Archival drop-down list in Polish language
3. Fixed the Clip Player Day light Saving Time issue
4. T2 Patch changes - Axis v6.0 support and fixed the SVMD issue
5. Fixed the Incorrect GPU driver installation and the cameras are not rendering issue.

How to increase the Limit for Rendering Camera

1. Open the **Registry Editor** window.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Honeywell\MaxproNVR\Trinity Framework\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

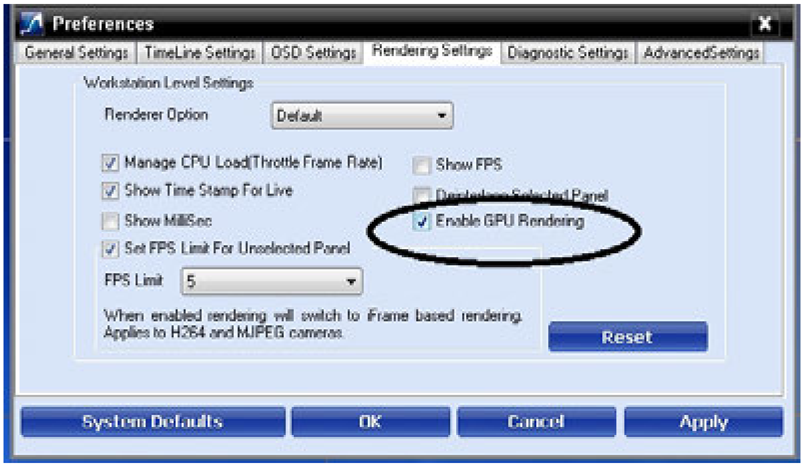
Value data: 20

Base: ○ Hexadecimal ● Decimal

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

1. Click the **Preferences** option in the user menu. The **Preferences** dialog box is displayed. By default, the **General Settings** tab is selected.
2. Click the **Rendering Settings** tab as shown below.



Workstation Level Settings

Renderer Option: Default

☑ Manage CPU Load(Throttle Frame Rate)
☐ Show FPS
☑ Show Time Stamp For Live
☐ Deinterlace Selected Panel
☐ Show MilliSec
☑ Enable GPU Rendering
☑ Set FPS Limit For Unselected Panel

FPS Limit: 5

When enabled rendering will switch to Iframe based rendering. Applies to H264 and MJPEG cameras.

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.

This page is intentionally left blank

Index

Contact Information

Honeywell Security and Fire Americas (Head Office)
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299, USA
www.honeywell.com/security
☎ +1 800 323 4576

Honeywell Security and Fire Europe/South Africa
Aston Fields Road, Whitehouse Industrial Estate
Runcorn, WA7 3DL, United Kingdom
www.honeywell.com/security/uk
☎ +44 (0) 1928 754 028

Honeywell Security and Fire Americas Caribbean/Latin America
9315 NW 112th Ave.
Miami, FL 33178, USA
www.honeywell.com/security/clar
☎ +1 305 805 8188

Honeywell Security and Fire Pacific
Level 3, 2 Richardson Place
North Ryde, NSW 2113, Australia
www.asia.security.honeywell.com
☎ +61 2 9353 7000

Honeywell Security and Fire Asia
35F Tower A, City Center, 100 Zun Yi Road
Shanghai 200051, China
www.asia.security.honeywell.com
☎ +86 21 5257 4568

Honeywell Security and Fire Middle East/N. Africa
Emaar Business Park, Sheikh Zayed Road
Building No. 2, Office No. 30
Post Office Box 232362
Dubai, United Arab Emirates
www.honeywell.com/security/me
☎ +971 (0) 4 450 5800

Honeywell Security and Fire Northern Europe
Ampèrestraat 41
1446 TR Purmerend, The Netherlands
www.honeywell.com/security/nl
☎ +31 (0) 299 410 200

Honeywell Security and Fire Deutschland
Johannes-Mauthe-Straße 14
D-72458 Albstadt, Germany
www.honeywell.com/security/de
☎ +49 (0) 7431 801-0

Honeywell Security and Fire France
Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
www.honeywell.com/security/fr
☎ +33 (0) 1 40 96 20 50

Honeywell Security and Fire Italia SpA
Via della Resistenza 53/59
20090 Buccinasco
Milan, Italy
www.honeywell.com/security/it
☎ +39 (0) 2 4888 051

Honeywell Security and Fire España
Avenida de Italia, n° 7, 2ª planta
C.T. Coslada
28821 Coslada, Madrid, Spain
www.honeywell.com/security/es
☎ +34 902 667 800

Honeywell Security & Fire Pacific
Unit 5, 24-28 River Rd West,
Parramatta NSW - 2150 , Australia
www.honeywellsecurity.com.au
HSFPAC.Support@honeywell.com
Ph: 1800 220 345

Honeywell
THE POWER OF **CONNECTED**

www.honeywellvideo.com
+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

Document 800-16419V5 – Rev A – 08/2017